The LAFN User's Guide

Apr 13, 2012

Doug Hardie
Systems Administrator

Table of Contents

Revision History

1 Oct 1999 .....Initial Release

20 Mar 2000 .....Added non-profit and classroom account information.

6 Jun 2000 .....Added personal web pages. Updated non-profit account information. Added section on Connection Problems.

15 Jun 2000.....Updated the spam information section.

22 Jun 2000.....Updated the personal web pages to show automatic establishment.

1 Jul 2000.....Added more information on uploading personal web pages.

28 Jul 2000.....Correct PMB number.

15 Aug 2000 .....Add user spam block options.

9 Sep 2000.....Added Secure LAFN User Services

25 Nov 2000.....Corrected non-profit paragraph error.

18 Jan 2001 .....Corrected User ID requirements.

14 Feb 2001 .....Update CD systems supported list.

9 Apr 2001 .....Add spam blocking notification.

10 Jun 2001.....Added new spam bypass option. Cleanup.

18 Jul 2001.....Added section on User Computer Protection.

2 Nov 2001 .....Conversion to Managed Modems and personal firewalls.

12 Nov 2001.....Update contact information and User Services.

4 Jan 2002 .....Update ftp.

13 Feb 2002 .....Permit ftp across the internet, clarify the spam blocking options.

25 Feb 2002.....Added section on handling received spam.

17 Mar 2002 .....Corrected URL for full news service. Updated e-mail section for SSL and frozen mailboxes.

7 Aug 2002 .....Added information news group and status web page.

9 Sep 2002 .....Updated session limits for the 4 hour sessions and included a section on requesting e-mail bypasses.

24 Oct 2002 .....Added alternate notifications.

30 Oct 2002 .....Update DNS addresses.

9 Nov 2002 .....Added Disposable E-mail Addresses.

20 Nov 2002 .....Added new use for disposable addresses.

27 Nov 2002.....Text improvements.

31 Jan 2003 .....Remove LAFN CD

12 Feb 2003.....Added User Domains and corrected some information on dial-in numbers.

30 Mar 2003 .....Removed fee amounts to reduce future updates.

13 Apr 2003 .....Removed the User Agreement and point to its web location.

19 Apr 2003.....Added ftp-ssl and ftp-tls information. Added section on mail-lists and mail relays.

27 Apr 2003 .....Updated user training.

21 Jun 2003.....Cleanup of numerous sections.

28 Aug 2003 .....Added section on Remote E-Mail access.

6 Dec 2003.....Added information on SlipStream and Extended dial-in services.

22 May 2004.....News posting e-mail address policy. Added info on spam blocking.

2 Jun 2004.....Updated the Personal Web Space sizes.

29 Dec 2004 .....Conversion and general updates.

13 Apr 2005 .....Revision of the spam blocking options and addition of Mail Server Bayesian Filtering.

7 Dec 2005 .....Correct ftp example and update FileZilla information.

11 Apr 2006 .....Updated spam bypass information.

22 Jul 2006.....Remove mailing address and point to User Services for that information. Added DSL account information.

16 Oct 2006 .....Added features for changing family account ids and bypass requests via User Services.

2 Nov 2006 .....Correct windows for renewal and removal to match LAFN policy.

7 Feb 2007.....Add TMDA Spam Blocking Option. Updated DSL information.

15 May 2007.....Update DNS server information.

21 May 2007.....Correct PWP size to 20 MB.

9 Jan 2008.....Added information on account renewal and connection services.

17 Apr 2008 .....Updated numerous sections to clean up language and correct minor errors.

4 Oct 2008 .....Update the termination of disposable e-mail addresses for DSL users.

20 Oct 2008 .....Added Spam Firewall and reorganized the spam blocking sections.

4 Sep 2009.....Added section on PWP Passwords.

6 Mar 2010 .....Add information on fetch and cyberduck.

26 Apr 2010 .....Change in the answering machine's number.

13 Apr 2012 .....Change the 888 number references to the answering machine.

The LAFN User's Guide

The LAFN system is designed to provide Internet Services to our users. These services incorporate many different features that require configuration or procedures to use effectively. The User's Guide is the reference for LAFN services for users. The LAFN is not a static system but evolves with the availability of new technology. As a result, this document will evolve as new features and services are made available. In addition, we want to improve this document to make it helpful for users. Please send any corrections, or suggestions for improvement to ops@lafn.org.

The LAFN Charter

Los Angeles Free-Net's mission is to provide low-cost Internet accounts. LAFN provides individual Internet accounts and other types of accounts for non-profit organizations and classrooms.

To be able to offer internet services at this price, LAFN uses its computer and Internet bandwidth resources at or near capacity-levels. Also, LAFN restricts computing, storage, and Internet bandwidth-intensive services that it offers. For example, LAFN doesn't offer full Usenet newsgroups. As a result, LAFN operates with less equipment and bandwidth per user, and passes the savings to its users in the form of lower user fees.

The LAFN Organization

The LAFN is a non-profit corporation that is run by a Steering Committee. The officials of the LAFN consist of the President, the Chief Financial Officer, and the Secretary. The steering committee establishes the rules of operation and manages the operation of the LAFN.

In addition to the steering committee, LAFN has two groups of volunteers who administer daily operations. The registrars manage the LAFN user accounts. They activate, reregister, and deactivate accounts in accordance with LAFN policy. The mentors provide technical assistance to the users to assist them in using the LAFN services.

Virtually all of LAFN is staffed by volunteers. The Steering Committee, the registrars, the mentors, and most staff members are volunteers who are donating their time to enable LAFN to achieve its goals.

LAFN maintains a mail box and an answering machine. There is no office that is staffed by people. Volunteers receive the mail from the mail box and distribute it to the registrars and staff as appropriate. Likewise phone calls are periodically retrieved from the answering machine and distributed to the mentors. See the Contacting LAFN section later in this guide for details on those services.

What makes LAFN different from full-service ISPs

LAFN does not provide full internet services. For example, bandwidth to the internet is limited. Internet bandwidth is the most expensive portion of the LAFN operations. We cannot provide adequate bandwidth to support all of ours users for unlimited duration connections. We generally have about half the number of simultaneous dial-in connections that a full-service ISP would have.

LAFN restricts most connections in California to one hour. Longer sessions are available as described in the Session Limits section. A user can immediately redial when a session ends. However, the use of automatic reconnection is not permitted. LAFN is designed for personal use, not unattended use. Each line is intended to support 15 to 20 users. By limiting the sessions, we reduce the number of dial-in lines that are required and the load on the internet connection. This approach prevents a user from being locked out for extended periods. LAFN does monitor usage and notifies users who are abusing the dial-in service.

LAFN users are directly connected to the Internet while on-line. This means that configuration of the various Internet clients is simple, but the user's computer must be properly secured to prevent hackers from accessing information or taking over the computer. This is addressed in detail later in this document.

LAFN actively rejects spam e-mail. We do not have the disk space available to handle the volume of spam that is received daily. As a result, you may have desired messages spam blocked. There are a number of approaches you can use to address these issues. See the sections below on spam blocking for information on the available options.

LAFN does not have a full-time staff available for immediate consultation. Our staff is almost exclusively volunteers who work when they have time available.

LAFN does not maintain an office. Our equipment is located in a very small closet that is shared with another organization.

LAFN does not provide guaranteed service. LAFN should not be used for situations that required immediate accessibility, such as on-line stock trading. LAFN provides approximately 1 dial-in line for every 20 active users. Full-service ISPs typically provide 1 line for every 4 users with the corresponding increase in costs. Busy signals will occasionally be encountered with LAFN. In addition, we do not provide any redundant equipment so equipment failures will result in outages that could last a few days.

The LAFN User's Agreement

The LAFN User's Agreement defines the rules and procedures for proper usage of the LAFN accounts. In order to receive an LAFN account, a user must agree to the LAFN User's Agreement. Violation of the terms of the agreement are grounds for immediate termination of the account without refund of any fees paid. The current User Agreement

is found at http://admin.lafn.org:8000/lafn/users/agreement.html or via a link on our home page.

Establishing an Account

Accounts are established via the LAFN web. It can be accessed from the Internet via http://www.lafn.org. Or, with a computer that has PPP available, dial one of the numbers listed in the Telephone exchange listings on the LAFN web page: http://www.lafn.org. Use the user id of "visitor". No password is required. Then go to the URL http://www.lafn.org.

Personal Accounts

Personal Accounts are established by a new user registering on the LAFN web registration system. The user will be shown the LAFN User's Agreement and must agree to it before registering. New users must select a user id that is unique and complete the entire registration form.

While a user may use nicknames for their e-mail names, real names must be used when registering. Also, the date of birth is used if a user forgets or otherwise needs LAFN to create a new password for them.

Personal Accounts can have dial-in and/or DSL access.

Once a new registration is accepted by LAFN, the user has 60 days to mail the contribution to LAFN to complete the activation of the account. Since the user id has been reserved and cannot be used by another user, after 60 days the registration will be deleted if payment has not been received to free up the user id for a paying user.

Accounts are registered for one year from the date the contribution is processed by LAFN. The user can check the account status by trying to connect to LAFN using the new user id and password. If the connection does not establish then the account is not activated. If the account does not become active within 3 weeks from the date of registration, contact LAFN using via the answering machine as described in the Contacting LAFN section and provide us the details of the user id, the date it was registered, and the date, name, and check number.

Personal accounts are also provided Personal Web Pages. See the Personal Web Page section below for the details.

Family Accounts

Family accounts are additional e-mail addresses intended for family members of a LAFN user. Now it is possible for family members to have their own e-mail addresses. Family accounts do not have any dial-in capability. The term runs concurrently with the primary account. When the primary account is renewed, you

must include the fee for each Family E-mail Account and identify each along with the primary account.

Each account initially has a name derived from the primary account. For example, if the primary account is aa100, the first family account would be aa100-1, the second aa100-2 etc. Or if your id is xyz then the first family account would be xyz-1, the second xyz-2 etc. Once the family account has been created, the user can log in to User Services with that ID and password and change the family account id to any desired and available id. The designation of Family Accounts to specific family members is the family's responsibility.

Family accounts can be established when the primary account is registered. There is a place in the registration form to enter the number of desired family accounts. The registration system will provide the payment information.

Family accounts can also be established after the primary account exists by going to User Services and selecting the link for Adding New Features to Your Account. There you can establish new features such as family accounts and pay by check or credit card. The web page provides the details for both. The initial passwords for the Family Accounts will be the same as for the primary account. To set up the mail reader for the Family Accounts, you will need to use the new Family Account ID with the password of the primary account. The passwords can be changed as described below.

To change the password for a Family Account, you use LAFN User Services. See the instructions in the section Changing Your Password.

The primary account-holder is responsible for informing the family account member(s) of the LAFN User Agreement and the Acceptable Use Policy. Family accounts that violate the rules, like all other LAFN accounts, are subject to termination.

Family Accounts terminate with the primary account. If the primary account is renewed without the Family Accounts, the Family Accounts will expire.

Affiliate Accounts

Affiliate accounts are additional e-mail accounts that are available to non-profit organizations. These accounts are functionally the same as family accounts and are handled the same by the system.

Classroom Accounts

Pre-K through community college public and private schools in the LA Free-Net's local dial-in area are entitled to classroom accounts at no cost. If requested, a WWW Home Page can be granted. We expect sponsors to have individual accounts on the LA Free-Net and to encourage their staff, students, and their families to join the LA Free-Net.

Classroom accounts can only have dial-in service.

To register a classroom account, go to the LAFN home web page and follow the user registration link. In the Welcome to LAFN page is a link to Classroom accounts. Click on that to go to the classroom account description and click on the link in that page. Fill out the form and submit the letter as directed.

Rules for Using Classroom Accounts

1. A Classroom account must be used only in the room designated in the registration for that account and only when the students are under the direct supervision of a responsible adult.
2. Students are forbidden to know the password for the account. Only the responsible adult may use the user ID and password to make the connection to the LA Free-Net. The password should be changed frequently to protect the integrity of the account.
3. Students are not permitted to use a classroom account when they are not in the classroom and under the direct supervision of a responsible adult. If students have access to a different computer and modem, they must register for personal accounts of their own.
4. Students (and adult supervisors) must understand and abide by the LA Free-Net User Agreement and Acceptable Use Policy. All students and their parents are urged to sign a written agreement which includes the Acceptable Use Policy.
5. Only one session at a time is permitted. Multiple logins using the same user ID and password are forbidden. Additional classroom accounts must be requested by on-line registration.
6. Failure to observe these rules may lead to the revocation of the classroom account.

Non-profit Organization Accounts

Non-profit organizations have the following:

1. A WWW Home Page on the LA Free-Net.
2. A user account.
3. One Affiliate account. Additional Affiliate accounts are available.

Because the LA Free-Net is an all-volunteer non-profit organization, it is hoped that non-profit organizations will encourage their members to join the LA Free-Net. This gives full use of the LA Free-Net services and sustains the LA Free-Net.

Non-profit account id's need to be 14 characters or less so that the affiliate account id can be properly created.

To register a non-profit account, go to the LAFN home web page and follow the user registration link. In the Welcome to LAFN page is a link to non-profit organization accounts. Click on that to go to the non-profit organization account description and click on the link in that page. Fill out the form and submit the e-mail as directed.

Non-profit accounts can have dial-in and/or DSL service.

Student Accounts

LAFN is currently able to offer student accounts for K-12 students and their families. The procedures for registering for a student account are on the LAFN web page for new account registration.

Student accounts can only have dial-in service.

Renewing an Account

At approximately 60 days before an account expires, an e-mail will be sent to the user describing the renewal process. Likewise at approximately 30 days before expiration another e-mail will be sent. If renewal payment is received during the period from 60 days before expiration until 90 days after expiration, the account will be renewed for one year from the original expiration date.

Thirty days after the expiration date, the account will be disabled. All e-mail and personal web page files will be deleted. No new e-mail will be accepted for the account. It will be returned to the sender as undeliverable. The user's record will be retained and the account can still be renewed. If renewal payment is received after 90 days beyond expiration, the account will be renewed for one year from the date payment is processed.

Renewal of classroom and student accounts can be accomplished by sending a notice to ops@lafn.org that states that the account is still in use and the original criteria for the account are still met. Student accounts renewals need to include the school and grade.

LAFN also provides for the renewal e-mails to be sent to an alternate notification address. While the intent of alternate notification was to provide notification to another person who is assisting the user to avoid loss of service, some users have found it helpful to have the notices delivered to an alternate address of their own. To establish an alternate notification address, go to User Services and use the account record update function.

Account Expiration and Grace Period

When the expiration date for the account arrives, if the account has not been renewed any DSL service will be immediately terminated. Please note, that if you renew an account after the expiration date, there will be a week or two delay for the processing of the DSL re-establishment with the providers. LAFN automatically provides a 30 day grace period after the expiration date where the account and dial-in services remain available for use.

Please keep in mind that if you are renewing by check, there are some significant processing time involved.

Account Termination

When the 30 day grace period expires, if the account has not been renewed, it will be permanently removed from the system. All mail and personal web pages will be deleted. While we may be able to restore the personal web pages, your mailbox is not saved. It's contents cannot be retrieved. LAFN does not recommend using your mailbox for long term storage of e-mail.

One year after expiration if payment has not been received for renewal, the user's record will be deleted from the system. This will free up the user id so that it can be used by another user. If a renewal payment is received after the one year period, LAFN will contact the user who will then have to create a new registration as the original registration no longer exists.

Dial-in Service

The LAFN dial-in service uses a form of managed modems where the user's connection is via a service that provides the Internet connection directly from the Remote Access Server that provides the dial-in connection. As a result, we tend to avoid the congestion that occurs with a common access point.

LAFN provides three different dial-in services: Regular, SlipStream, and Extended. When you sign up for an account you have to pick one of the dial-in services. The features and areas of coverage are different for the three services. See the Frequently Asked Questions on our web page or the Add Features to My Account in User Services for details on the dial-in services costs and areas of coverage. User Services will let you switch between the services.

Regular Dial-in Service

Regular dial-in service is only available in California. It has session limits (see the section below on session limits) and you may not use automatic reconnection with Regular dial-in service. Classroom and Student accounts are only permitted to use Regular dial-in service.

SlipStream Dial-in Service

SlipStream dial-in service has session limits (see the section below on session limits) and you may not use automatic reconnection with SlipStream dial-in service.

SlipStream service provides a caching server and uses a newer compression algorithm on the dial-up line to speed up access to web pages and downloads. The improvement in download times is dependent on a number of factors. In addition, you have the ability to set the amount of reduction to use for images on web pages.

Using a higher compression will give more reduction in transfer times. To use SlipStream dial-in service you first have to download the SlipStream client from the LAFN web page. Then you have to start the SlipStream client before establishing the connection to LAFN. SlipStream clients are only available for some OSs. Check the LAFN web pages when signing up for SlipStream service, or in User Services for Adding new Features to your account for the complete details on which OSs are supported and the various requirements and restrictions on the service.

Extended Dial-in Service

Extended dial-in service is available in a number of states including California. It is the only service available outside California. We anticipate the area of coverage to be expanded in the next couple years. Extended dial-in service does not have any session limits and automatic reconnections are permitted. However, there is a limit of 400 hours connection time each calendar month. If you are connected for over 400 hours in a month, your account will be reduced by a month for each additional 400 hours.

When using Extended dial-in service, you must use SMTP-AUTH to provide authentication information when sending e-mail. In addition, LAFN strongly recommends the use of STARTTLS to provide encryption of the authentication information while its being sent across the internet. See the Frequently Asked Questions (FAQ) on our web page for instructions on configuring SMTP-AUTH and STARTTLS.

Usenet News service is available with Extended dial-in service. The news client must be configured to provide authentication.

Phone Numbers

The phone number list is too large to be included in the User's Guide. Basically the service area is all of California and most areas in 45 other states. For the complete phone number list, go to the LAFN web page at http://www.lafn.org. There you will find the numbers for each of the three dial-in services. The number finder URL in that page provides numbers for California. You enter the area code and the first 3 digits of your phone number. It will then show the numbers that should be toll free for you. Please remember that you need to check them out with your phone company as the rate structure sometimes changes.

Please note, it is the user's responsibility to select a phone number that does not have a toll, or long distance, charge. LAFN and our dial-in service are not responsible for any long-distance or tolls you encounter when using our services. Toll call charges can build up rapidly when using the internet. If you need assistance in determining if a number is toll free, contact your local phone company. The information provided by LAFN in this regard is intended to assist in the selection process but cannot be guaranteed accurate for all cases. Do note that

sometimes a ZUM toll call will be listed as a "local" call. Technically ZUM calls are local, but they still incur a charge and are not free.

Session Limits

Regular and SlipStream Dial-in services have session limits. LAFN sessions are established based on the time you connect to LAFN. Four hour sessions are provided when you connect between midnight and 4 am daily. Two hour sessions are provided if connect between 4 am and 6 am daily or anytime after 4 am on weekends. Otherwise the session is one hour. Please note that the session limit is established when you connect. If you connect at 11:30 p.m. you will not get a 4 hour session.

In addition there is a 15 minute inactivity time-out. If there is no network traffic during a 15 minute period, you will be disconnected. Please note, that most POP mail clients download all the e-mail first then let you read it. Generally they don't send responses immediately but queue them up for later transmission. Hence, you can easily spend 15 minutes reading and replying to e-mail without sending any traffic on the line.

Connection Problems

Connections to LAFN normally should last until the session limit is exceeded. However, sometimes there are situations that cause connections to be terminated early. If you are experiencing unexpected disconnects over multiple days, then you should investigate the cause. Go to http://www.lafn.org/admin/problems.html for a description on how to investigate the cause of the problem.

DSL Service

DSL Service is available in portions of the LAFN coverage area. There are multiple classes of DSL service depending on the desired line speed. Not all classes are available in all areas. The specifics on the DSL classes and costs are in the FAQ as they tend to change periodically. LAFN is trying to establish DSL service in other areas and bulletins will be issued as we are able to create new services. The cost of DSL service includes regular dial-in service. Extended and Slip-Stream are also available at an additional cost.

DSL connections use dynamic IP addresses. Static IP addresses are possible, but the cost to LAFN is a bit outrageous. If there is a real demand, we might offer static IP. However, its primary use is for business level service which LAFN does not offer.

Changing Connection Services

Dial-in and DSL services can be added and changed through User Services. In addition to one-time payment by check and by PayPal, LAFN provides for a monthly or quarterly

payment by credit card using PayPal. These options will be displayed when they are available in User Services.

When you add or change services, the remaining credit on your existing account is computed based on the time remaining until expiration. This is then subtracted from the next payment. If you are using a one-time payment, the account is renewed for a year from the date of payment. If you are using a monthly or quarterly payment, the credit is subtracted from the first payment. Because of the transcation costs from PayPal and the limitations of their services, monthly and quarterly payments can not be used in all situations.

Accounts Without Connection Services

If you do not require a connection service (dial-in or DSL), then you can remove both of those services from your account and save money. Non-connection accounts are intended for those who have high-speed connections not provided by LAFN. These accounts provide all of the LAFN Internet Services described below.

LAFN Internet Services

LAFN provides a number of internet related services to its users. This section describes those services and the limitations LAFN places on their use.

Domain Name Service (DNS)

Domain Name Service provides the mechanism to enable your computer to locate our server and internet resources. You must have at least one DNS server configured. However, it would be best to configure at least two so that you do not lose access to services if one of our DNS servers happens to be down. It is best to use the DNS servers that the Remote Access Servers will dynamically assign. They will respond much quicker as they require less Internet traffic. Most versions of Windows 95/98 and MacOS 8 and later systems support dynamically assigned DNS addresses. If you need to manually enter DNS addresses, you should use the following:

Sacramento Area
ns1.o1.com 66.81.0.251 (primary DNS)
ns2.o1.com 66.81.0.252 (secondary DNS)

San Jose Area
ns1.o1.com 69.19.189.116 (primary DNS)
ns2.o1.com 66.81.0.252 (secondary DNS)

Los Angeles Area

ns1.o1.com 69.19.190.116 (primary DNS)
ns2.o1.com 66.81.0.252 (secondary DNS)

E-mail

E-mail services are provided to LAFN users. LAFN currently provides a POP mail server for received e-mail and a SMTP mail server for sending e-mail.

Received e-mail is accessed via a POP client that is configured to connect to mail.lafn.org. The user id must be configured to your LAFN user id. For example, if your LAFN user id is bc979, then you would configure the mail user id as bc979, not bc979@lafn.org. The latter will not work. The password you use to connect to LAFN is the password for receiving e-mail.

Your mail client must be configured to delete e-mail from the server. LAFN does not have disk space to hold large mail files for our users. We require that e-mail be regularly retrieved from the server. There is no enforced limit on the size of the mailbox or messages other than you have to be able to download it during a session. LAFN relies on our users to keep their mailboxes from exhausting server space.

Mail lists can generate volumes of e-mail that can overload our server. If you subscribe to mail lists, you need to be careful to ensure they do not result in large mail files while you are on vacation. You may need to sign off the mail list during periods when you will not be able to regularly access e-mail. Please see the LAFN User's Agreement.

E-mail to be sent should be configured to be sent to smtp.lafn.org. Your user id and password are required via SMTP-AUTH to be able to send mail through our server. In addition, you should be aware that the SMTP-AUTH protocol does not protect the user id and password. They are sent in the clear. You should use STARTTLS to encrypt the user id and password. The configuration instructions in the Frequently Asked Questions on our web page show how to setup mail with both SMTP-AUTH and STARTTLS. We recommend the use of both in all cases. Please see Delays in Sending E-mail below for information on response times.

Occasionally you may receive an e-mail that is too large to download in a session. When that occurs you are unable to access e-mail behind it and your mailbox is effectively frozen. There are two ways to get this resolved. The quickest is to go to www.lafn.org and select the Remote Mail function. Login using your user id and password. That will provide a listing of the messages in the mailbox. You can use the delete function to delete the message without having to download it. The other approach is to send ops@lafn.org a request to delete it.

The standard POP mail transfer protocol requires your user id and password to be sure we are sending you the proper mail. Those are sent in the clear such that anyone monitoring the network will see your id and password. They will then be able to become you to our system. LAFN also provides POP service with SSL. This

is just like the SSL used for web pages. It encrypts the information as it is sent across the networks so that it cannot be read by someone monitoring the network. Unfortunately there are two ways to use SSL with e-mail.

The old, non-standard approach uses SSL on port 995. This approach is used by older mail clients that have not adopted RFC 2595 yet. These are fairly common. Typical among these is Outlook Express. Some e-mail clients do support RFC 2595 and they work differently. They use port 110 which is the standard POP3 port. The Frequently Asked Questions on our web page include in section 2 the instructions for the most popular mail clients for configuring with SSL and SMTP-AUTH. If you are having trouble getting those to work, one thing worth trying is to change the port to 995 or 110 and try both setups. One should work.

Remote E-Mail Access

There are several approaches available to access your E-Mail when away from home. If you have access to a computer that is connected to the internet and has a web browser you can go to www.lafn.org and select the link for Remote Mail. You login with your user id and password and you have access to your mail through a very simple, web based mail client. Please note that while this client provides most of the services of a normal mail client, it is very slow. Be sure to use only its buttons. Do not use the browser's back button or reload button as you can easily corrupt your mailbox. Remote Mail does not automatically delete messages so you will be able to retrieve them when you return home.

The other option if you have your computer with you is to configure the send mail server to use password authentication with your user id and password. The technical name for this service is smtp-auth. Not all mail clients support smtp-auth. Some use earlier protocols that are not supported by LAFN. The use of SSL with smtp-auth is somewhat problematic. We have not been able to get consistent results with that combination. All the tests we have run have the user id and password encrypted when sent using smtp-auth. There are instructions for some mail clients for the configuration of smtp-auth in the Frequently Asked Questions on our web page.

Some ISPs (e.g., Earthlink) block access to the standard smtp port, 25. As a result smtp-auth will not work. This blocking prevents many forms of spam from being sent by their users. The result may be a connection that fails to complete, or an error message back to you. If you encounter this problem, switch to port 26 on smtp.lafn.org. It should not be blocked. Generally it is possible to use smtp-auth on port 26 as your normal smtp configuration, even from home. Its not required when dialed into LAFN but would save changing configurations when operating away from home.

Smtp-auth is also usable by high-bandwidth connections (i.e., Cable and DSL). This enables those users to use LAFN as their primary mail server.

System Bulletins

System Bulletins are the mechanism by which LAFN provides information to its users. System Bulletins are distributed in e-mail messages when a user accesses their e-mail. The POP mail server formats them as e-mail and sends them to the user's e-mail client. There is no way to limit distribution or to forward them outside of LAFN since they are not e-mail - they just look like e-mail.

Protection from Spam E-mail

LAFN uses a multi-pronged approach to protection from spam. Basically there are 3 phases of spam protection. All e-mail received by LAFN must go through the Spam Firewall to eliminate mail servers that do not operate properly. LAFN only accepts e-mail from properly operated mail servers. Then a virus check is done on the e-mail. Any messages containing viruses are deleted. Finally each individual user has spam blocking options (regular spam blocking, no spam blocking, TMDA, or DSPAM).

The Spam Firewall

The Spam Firewall blocks incoming mail from Mail Transfer Agents (MTA) that have not shown that the operate in accordance with the RFCs. Hence there is nothing being received by our mail server from those MTAs. There is no way to know who the spam was from or addressed to as that information is never received. Once a MTA has identified itself as operating in accordance with the RFCs the mail it sends gets delivered directly to the recipient's mailbox. The delivery time is now actually a bit faster than before. Previously the volume of spam was such that the mail server had to shutdown incoming connections to process the backlog. This delayed both spam in desired email. Now the server is basically running at idle and will not need to shutdown the connections. Incoming mail gets through much faster.

To delineate the effects of the Spam Firewall in more detail, we need to elaborate on the concept of MTA. Every ISP operates at least one MTA. LAFN actually has 4 of them: the incoming mail server, the outgoing mail server, one used by the staff for special functions, and one for testing software. Only the first two are used by users. Larger ISPs will have multiple MTAs. It makes the job of managing and handling email easier when you process large amounts of email. Each MTA is identified by its IP address. The name of the server is not important, only the IP address. When a user sends mail, their ISP designates one of the MTAs to accept the message and then route it to the destination MTA. For mail addressed to LAFN users, the destination MTA is our incoming mail server.

MTAs directly contact the destination MTA and try to deliver the email. However, there can be a number of reasons why the originating MTA is unable to contact the destination MTA at a point in time. Some of those are:

- There is an internet link in the path between them that is down or congested.
- The destination MTA itself may be down for maintenance.
- The destination MTA may have disabled incoming connections because its overloaded.

If the originating MTA is unable to contact the destination MTA then it just queues the email and waits about 30 minutes and tries again then. The queue time is generally configurable but the RFCs are strongly recommending at least 30 minutes. Under "normal" conditions, it is quite often that the initial MTA connection cannot be completed and the message has to be queued. For the last couple years our incoming mail server is frequently disabling incoming mail for short periods because of the spam workload. The email system is designed to handle this as best as is possible with the existing internet structure. However, it is quite unreasonable to expect the mail system to delver email immediately. There are actually a fairly large number of MTAs that queue every message and send them later. This was quite common when the internet links were dial-up lines and the cost depended on the time of day. MTAs would routinely queue email and send it during the evenings when the cost was lower.

While that specific situation is quite rare today, the links that make up the internet are paid for by companies that need to use them for their own business. They are making any spare bandwidth available to the rest of the internet. It is not uncommon for those links to have priorities based on data type. Email is almost always the lowest priority. Video conferences and things like that are generally given a much higher priority. Email delays are normal.

The Spam Firewall identifies MTAs that do not follow the RFCs by delaying the very first email we receive from the MTA. Basically it responds that the MTA is not available. Thus the originating MTA has to queue the message and try again. When they try again, after 20 minutes from the first try, then we whitelist their IP address and deliver that message and all subsequent emails from that MTA immediately. This detects MTAs that do not queue messages. Spammers don't want to spend the money and time on queueing spam. Queueing requires additional disk space and bandwidth. Both of those are reasonable expensive in high volume. Spammers get paid by volume. They need to process as quickly as possible.

LAFN retains an MTA on the whitelist as long as it receives another email within 72 days. The norm for this is 30 days, but we have stretched it out because there are a number of users on monthly maillists. Often those maillists do not come out on schedule but may be delayed. To avoid those MTAs having to go through the delay again, we use 76 days. Thats probably too big, but we are going to monitor usage and see what happens.

There have been some concern expressed about delays to regularly received email. As described above, that will not occur. Only the first email from a MTA will be delayed. Once the first one has been accepted any email from that MTA to any LAFN user will be directly delivered. Only if we do not receive an email from that MTA in 76 days will it be removed from the whitelist.

Virus Blocking

LAFN uses virus blocking on all incoming e-mail after it has been through the first step. Each e-mail is checked against the known viruses. If a virus is detected, the e-mail is discarded. The virus definitions are updated several times daily. However, there may be a time period between when a virus first is released and when it is identified and a detection method created. During that time we will not be able to detect them. Hence, it is still advisable to keep your own virus checker up to date and run it often.

The developers of the virus database also include definitions for some spam. Likewise those will be discarded when detected.

User Spam Blocking

E-mails after passing this far are subjected to the spam blocking options available to users. Users can select in User Services between: default spam blocking, no spam blocking, TMDA, and DSPAM. No single approach is best for everyone. Users should familiarize themselves with the options and their benefits and select the one best suited to their needs.

User Spam Blocking Options

Even though LAFN blocks spam, there will be times when you receive an objectionable e-mail

The number of ISPs being blocked because of spam problems seems to be growing. As a result the blocks are preventing mail from some of our users correspondents from being accepted by LAFN. LAFN accounts are normally configured for spam blocking as described above. LAFN users encountering problems with their correspondents being blocked can select three alternate forms of spam blocking: individual blocking bypass, forwarding service, or complete removal of spam blocking.

Default Spam Blocking

Default spam blocking is the most aggressive blocking approach available. It is the default because of the large number of Student Accounts that we provide. It is not necessarily the best approach for all users. There are several options available with default spam blocking: Spam blocking notification and Bypasses. If you are using default spam blocking we strongly recommend enabling Spam blocking notification in User services.

LAFN is subject to Denial of Service (DOS) attacks, particularly from high-bandwidth Internet sites. DOS attacks not only disrupt LAFN's Internet connection, which, for example, prevents users from browsing the WWW, but also disrupt LAFN's servers.

When an e-mail message is blocked, LAFN returns a message to the originator that contains a URL describing why the e-mail was block, and how to go about resolving the problem, e.g.,

```
Mail from 216.192.16.16 refused, see http://
    www.lafn.org/blockedmail.html
```

The originator of the message needs to contact their ISP administrators with that information and request that the spam problem be resolved. The URL includes information for the administrators on how to get the block removed.

Imagine, for example, someone with a 1.5 megabit-per-second connection forcing unwanted packets down your 56 kilobit-per-second dial-up connection while you were logged in. The unwanted packets would disrupt your connection and use of your computer. The same results occur when a high-bandwidth Internet site launches a DOS attack against LAFN. The e-mailing of mass distribution advertising becomes an effective DOS attack on LAFN because they can deny LAFN users the ability to use the internet resources. The use of mass distribution e-mail is increasing because it is a very cheap form of advertising and has proven effective in the adult business sector.

When a DOS attack is identified, LAFN blocks routing to the IP address of the DOS attack, and sends e-mail to the IP address block owner. In most cases, LAFN gets a response within 24 hours (many in less than 60 minutes!), The problem is resolved, and the IP address block removed.

LAFN will block spam with the least possible blocking of other users of he involved ISP. For example, if a spammer is stupid enough to use the same return address on spam mail, we will only block that address. However, many ISPs operate open relays which permit the spammers to route their spam through relay such that it appears to come from a normal user of that ISP. About all we can do in that situation is block the Mail Transfer Agent

(MTA) that has the open relay. There is no way to distinguish spam from legitimate e-mail arriving from that MTA.

Generally spam blocking is done by the IP address of the MTA. We cannot tell for sure which ISPs might use that MTA. In addition many ISPs will use multiple MTAs so that blocking will appear to be inconsistent. Sometimes a user of that ISP will be assigned the MTA that is blocked. Then mail will not be received. Other times they will be assigned an MTA that is not blocked. In those situations the mail will be received.

LAFN uses both external and internal resources to combat spam mail DOS attacks. The external resources currently include the following which are used by numerous ISPs:

```
http://maps.vix.com/rbl/
http://maps.vix.com/dul/
http://relays.radparker.com/
```

When LAFN is under massive spam mail DOS attacks, the following additional external resources are used:

```
http://www.orbs.org/
http://www.imrss.org/
```

LAFN contributes its DOS information to the above Internet-wide databases.

In summary, LAFN takes any and all steps necessary to prevent DOS attacks from disrupting its services or its Internet connectivity. LAFN also uses from and contributes to Internet-wide anti-spam databases. LAFN notifies the source of the DOS attack of it's actions, and, in the case of blocked mail, returns a notice to the sender describing how to resolve the problem.

Default spam blocking is based on our users notifying us when that occurs. You need to send the complete message along with full headers to unblock@zook.lafn.org. We will then initiate blocking of that spam. Please note that the headers you normally see for a message are highly abbreviated. It normally takes additional actions to have the full headers displayed. If you need instructions, see The Frequently Asked Questions on the LAFN web page. Full headers look like:

```
Return-Path: <root@mindworkshop.com>
Received: from mindworkshop.com (mindworkshop.com
    [216.208.127.226])
    by zoon.lafn.org (8.11.3/8.11.3) with ESMTP id
    g86HvYm65829
    for <bc979@lafn.org>; Fri, 6 Sep 2002 10:57:34
    -0700 (PDT)
    (envelope-from root@mindworkshop.com)
```

```
Received: (from root@localhost)
    by mindworkshop.com (8.11.6/8.11.6) id
    g86HvWA28525;
    Fri, 6 Sep 2002 13:57:32 -0400
Date: Fri, 6 Sep 2002 13:57:32 -0400
Message-Id:
    <200209061757.g86HvWA28525@mindworkshop.com>
```

If you have all spam blocking removed from your account, then you will receive spam. It will not be blocked. Please do not forward spam to LAFN if you have selected this option.

In any case, do not respond to spam e-mails. Frequently they will include a statement to e-mail some address or go to some web page to remove yourself from future mailings. Unless this is a reputable corporation you are familiar with, its most likely a means to gather working e-mail addresses to sell to spammers. Responding to either of them will generally result in additional spam from more sources.

Spam Blocking with Individual Bypasses

If a user has a correspondent that uses an ISP that is being blocked, the user can request that the specific correspondent be permitted to bypass the block. This approach is appropriate for users who have a few correspondents who are being blocked. Please note, that this bypass is for individuals, not mail relays or entire sites. In order to request a bypass, go to User Services and select the link for Add Spam Bypasses. Fill out the form for the correspondent you want to get through the block. We would still like to resolve the real problem so that exceptions are not required. We don't know just how much work will be required to provide this option, but as long as it does not interfere with other activities it will be provided. If the workload gets too much this option may have to be discontinued.

Please note that bypasses are only available for individual e-mail addresses. The only way to have a domain not blocked is for that domain to resolve the spam issues first. In addition, many forwarding services, mail-list servers, and mail bounces generate a unique from address for each message they provide. Often that is done by inserting a unique serial number into the address or by including an invalid character into the address. In either case there is no way to bypass that address. If a unique serial number is used, then that address will never be used again. If an invalid character is used, then there is no way for the mail system to handle that address properly.

E-mail sent by LAFN users using the LAFN SMTP server will not be spam blocked. If you are sending mail via another SMTP server and using your LAFN e-mail address and that specific Mail Transfer Agent is blocked, then the recipient will be notified that an LAFN address has been blocked. There

is no way to bypass LAFN e-mail addresses. You need to use a from address in the message envelope that belongs to the ISP you are sending from. Then we can establish a bypass. There is also the situation where LAFN addresses will appear in the blocked message notifications. Spammers can use LAFN addresses in their spam. We see this quite frequently.

Please note that when you request a bypass it permits anyone using that address to send mail to all LAFN users. Keep in mind that both the real holder of the address and spammers can use it. We may have to terminate a bypass if spammers start using that address to spam other users. This doesn't happen very often but we have encountered it.

The list of addresses you have requested bypasses for is available in User Services. Its helpful to the mail server if you check it periodically and send an e-mail to ops@lafn.org for those that can be removed as the addresses have changed or are no longer required. Since only one LAFN user id is saved for each bypass, there are a few situations where multiple users have requested a bypass for the same address. When this happens, only one of those users will see the address in their bypass list.

Users can also elect to receive a daily e-mail notification of blocked e-mails. Every night LAFN scans the mail logs to identify blocked messages. If you enable blocked mail notification in LAFN User Services then you will receive a message listing the originating e-mail addresses of messages blocked. Please note that this listing is not guaranteed to be complete since it is generated from log file analysis. The analysis is run on the previous day's log file. Each address will only be reported once regardless of the number of messages actually received.

Mail Forwarding Services

If a user has a large number of correspondents being blocked, an e-mail forwarding services may be helpful. E-mail forwarding services in essence are a different e-mail address that just forwards mail received to your LAFN mailbox. Generally these are not blocked because their administrators manage them carefully. We believe that iname.com (mail.com), hotmail.com, juno.com, yahoo.com, netforward.com provide forwarding services. In addition, there is a listing of such services at http://www.internetemail-list.com/Forwarding/ that lists many others. Some of them are free. If you have a large number of correspondents who are routinely blocked, establishing a forwarding service to your account here may be a solution. Note however that forwarding services will forward everything including spam. LAFN will not be able to block spam received through your forwarding service. In addition, it does occasionally happen when the mail forwarding services get blocked because they have a spam problem that has not been resolved. Those forwarding services that use your address in the envelope

From address are the best approach since if their Mail Transport Agent is spam blocked, you only have to request one bypass to receive the mail. If the service leaves the originator's address in the envelope spam blocking bypasses will not be effective.

Spam Blocking Removal

This option is to have all spam blocking removed from your account. If you select this mode, you will receive any and all junk or spam mail addressed to your account. LAFN will not be able to prevent delivery of such mail. You will have to download it and delete it yourself. There will still be some messages which contain specific viruses that have caused problems for the LAFN servers that will always be blocked. To initiate or terminate this option, send an e-mail to ops@lafn.org requesting the change.

Mail Client Bayesian Filtering

There is an additional approach to handling spam when you have spam blocking removed from your account. Bayesian filtering mail programs are available which use complex approaches to identify spam you have received and removing it from the inbox on your computer. This approach is very effective in separating spam from your inbox. You still have to wait for the spam to be downloaded and will have to periodically delete it. LAFN does not endorse any specific products providing this service. We are making you aware that this approach is very effective.

This approach is generally best with spam blocking removed from the account. This gives you the ability to receive e-mail from maillists that can not otherwise be bypassed.

Mail Server Bayesian Filtering (dspam)

LAFN provides an spam blocking option where the filtering is done on our mail server. This functions similar to the Mail Client Bayesian Filtering option above. However, the filtering is done on the server so you have to interact with the mail server to define spam messages. The advantage of this approach is you only download desired messages. Spam messages are retained on the server. However, that means you have to regularly access the spam messages and check for incorrectly identified spam and delete the real spam. You save a bit on download time, but acquire additional work that can only be done while connected to LAFN.

This option is only viable for users who are competent at working with a fairly complex user interface. Please note, that the web based user interface requires the proper implementation of CSS by your browser. Netscape and IE versions 4.x will not work properly. You have to use version 5.x or later.

We don't recommend this option for all users. The best option for most users we believe is the Mail Client Bayesian Filtering.

To use Mail Server Bayesian Filtering you must first train the server for it to be able to identify spam. At first all mail will be delivered to your mailbox. You download it and then for those messages that you consider spam, you forward them to a specific address to help the server learn about spam. Complete information on the operation of this option (also called dspam) is contained in the Frequently Asked Questions on our web page.

The Mail Server Bayesian Filtering option is still in a trial period. It is certainly not a finished product and the resources it requires my be too large for our systems. It is being offered on a trial basis.

Challenge-Response Spam Filtering (TMDA)

TMDA is a challenge response approach to controlling spam. Basically, anytime an e-mail is sent to you, it is placed in a quarantine and not delivered. A challenge is sent to the originator. If the originator responds, then the original message is delivered and that originator can send additional e-mails to you without further challenges. The messages in the quarantine are retained for a specific period (7 days at present).

You can go to TMDA management in User Services and access the e-mails in the quarantine. There you can have individual e-mails deleted or delivered. In addition you can create an update a whitelist (originators who can send without challenge), a blacklist (originators whose e-mail are discarded), and the confirmed list (originators who successfully responded to the challenge).

The advantage that TMDA has is that the whitelist can handle maillists reasonably well. It can also be used to admit e-mail from an entire domain. For example, the entry lafn.org is automatically included in each whitelist. That permits delivery of all mail from LAFN users.

Mail-lists and Mail Relays

Mail-lists and mail relays present difficult problems with spam blocking. Frequently a mail list server will include a unique serial number in their return address. As a result, bypasses are not possible. They never use the same address twice. Likewise mail relays often use the originator's address as the from address of the relayed message. As a result, there is no way to provide a simple bypass for all messages sent through the relay. If you are having to deal with these issues there are several approach available that can be used.

The simplest is to have all spam blocking removed from your account. You will then receive all messages from mail-lists or relays unless they contain a virus. However, you will also receive all spam addressed to you. Using Mail Client Bayesian

Filtering will greatly assist in this approach. Another approaches involves establishing a family account or a disposable e-mail address that you only use for the mail-list or relay. You leave spam blocking on your primary account and have it removed from the account used for the mail-list or relay. This will work as long as that address does not become visible to any spammers. The Mail Server Bayesian Filtering approach will also enable the receipt of these messages.

TMDA permits a fairly effective way of receiving mail from mail-lists and mail relays. Frequently the sender of mail-list e-mails will have the form of something on the order of: clio-bounces@ares.listmoms.net or lists.freeradius.org. Those can be placed in the whitelist and mail from the list will then be received. If the list has a more consistent approach to their from addresses (such as owner-freebsd-questions@freebsd.org), then that should be used to prevent spam from spoofed addresses similar to the mail-list from being delivered. You may have to monitor the quarantine closely at first to get the whitelist entries correct.

As with individual bypasses, there is a limit to the effective number of whitelist entries. We don't have a good feel for what that limit is as its difficult to test for that. However, the advantage is that when you exceed the limit, it only affects delivery of e-mail to you. With individual bypasses, it affects all LAFN users.

The rules for whitelist and blacklist entries are that the domain name must be specified. The user name is optional. With just a domain name (like lafn.org) than all e-mail from an address like xxx@lafn.org will be permitted or denied. E-mail from yyy@zzz.lafn.org will not be affected. When you include the user name (like bc979@lafn.org) then it only affects e-mail from that specific address.

Requesting an E-mail Bypass

These guidelines provide information on how best to get bypasses done right the first time. To request a bypass for an e-mail address, go to User Services and select the link to Add Spam Bypasses. There you will be able to add new addresses, edit address, and delete obsolete addresses. Please note that LAFN no longer accepts requests for bypasses via e-mail. They must be entered via User Services.

There have been a lot of problems lately with the address submitted to be bypassed. Frequently we receive an address which is obviously not right. Often the top level domain is missing. The User Services function for managing bypasses tries to check the requested address for correctness, but it is not always possible to detect errors. Frequently, the address has been "cut and pasted" from somewhere. Sometimes they are retyped and are not right. In these cases we usually get a complaint a few days later that the bypass doesn't work and would we please get it right this time. Sometimes they even send the right address the second time. Sometimes not and it takes a few more e-mails before we find out what the right address is.

Another common problem is that a user forwards a request to bypass the address that they are sending to. That works except when the desired user uses a different

address to send from. Bypasses only work for the listed address. Often people have multiple addresses. They may not be sending from the one you know. We can offer sympathy, but that's about it. Sometimes we can get real lucky digging through the logs and figure out the proper address to bypass. That will only work if the LAFN user only receives a couple e-mails daily. It takes a lot of work to walk through the logs. LAFN receives a lot of e-mail daily.

The best approach for using e-mail bypasses is to go to User Services and activate blocked mail notification. This will give you the real address that was used when the message was blocked.

Some other things to keep in mind: don't bother trying to have all addresses at spammer.com unblocked. Unblocking a domain requires that they or the ISP they use resolve the spam issue first. They are blocked because someone using one of their addresses is spamming LAFN users. Spammers don't identify themselves in their spam. They know that if they do, most ISPs will terminate their accounts. Thats not beneficial to them. Therefore they setup the messages to point to non-existent users or someone they don't care about. Addresses inside the message are never checked by the mail system. You can be listed as the originator of spam messages sent from anywhere in the internet. It happens daily. The KLEZ virus does this quite well. You may even be the recipient of a spam message showing you as the originator.

Replying to click here to remove you from our address list is usually only going to validate your e-mail address as one that is actually read. That way it can be sold for a higher rate to other spammers. Unless it's a well known corporation list, don't respond. You will become a popular spam recipient otherwise.

Frequently you may receive another blocked notification after you have requested that the bypass was established. This is normally not a problem with the bypass. It goes into effect as soon as ops enters it into the mail system. The mail system is generally updated at least daily. The problem is that the blocked mail notices are at least a day behind and sometimes two days behind.

Delays in Sending E-mail

The spam protection mechanisms require that our mail server contact several other mail systems to determine if the mail source is to be blocked. This is described previously. Since the mail system does not distinguish between LAFN users and other mail sources, this check is also done for e-mail originated by our users. The check requires several accesses across the internet. If there are internet problems, or some of those hosts are down, our mail server will have to wait for a timeout to detect the problem. As a result, it will appear to take considerably longer for your mail client to send e-mail than normal.

The normal time for the spam checks is considerably less than one second. However, when network problems occur, it can take up to 3 minutes. This is a

"normal" situation and you do not need to notify LAFN about a problem. It is not an issue we can resolve. We all just have to wait for whichever network is having a problem to get it resolved. Many mail clients time out around 45 seconds. When this occurs you need to tell the client to continue to wait. There are some clients for which you can change the timeout period. We recommend setting to at least 3 minutes.

Delays in E-mail Delivery

Occasionally you will encounter situations where e-mails make take several days to be received. This can occur with e-mail you are receiving or sending. This situation can occur for a large number of reasons, but basically the way e-mail is sent is that the originating mail server opens a connection to the receiving mail server. If that connection cannot be established, then it waits some time and tries again. Connections cannot be established if there is a link down between the two servers or if the receiving server is overloaded or down for maintenance. LAFN has no control over when mail servers send mail to us. There are some mail server that batch mail. They only send when they have a number of messages to the same receiving server.

Disposable E-mail Addresses

There are often situations where you need to give an e-mail address to an organization but have no assurance that your address will not be distributed to others without your consent. Some organizations have a policy of selling their address lists to other organizations. As a result you can end up receiving unsolicited e-mail (spam) that you just can't seem to get turned off.

Disposable e-mail addresses are a tool to help you with these situations. Disposable e-mail addresses are purchased from LAFN and really are an alias to your real e-mail address. The difference is that when you give out the disposable address and it becomes the recipient of unsolicited e-mail, you can have the disposable address deleted and you will no longer receive the spam sent to that address. The proper way to use disposable addresses is to reserve your real e-mail address for friends and organizations you trust. Then you use disposable addresses for others. While you can give one disposable address to multiple organizations, you do need to be careful about that as terminating the address will stop e-mail from all the organizations to whom you have given it.

Another option for disposable addresses is to have spam blocking on your primary account. Then have spam blocking removed on a disposable address. Activate spam blocking notification via User Services. When a friend is blocked, send them the disposable address to use. That way if someone abuses the address you can always cancel it.

To request disposable e-mail addresses, go to LAFN User Services. There you will find all the specifics on purchasing them via credit card or check. The disposable addresses will be enabled and linked to your regular e-mail address when you receive them. To have a disposable address terminated, you need to send an e-mail to ops@lafn.org giving your LAFN user id and the specific disposable address you want terminated. To prevent abuse of these addresses, we require that you send the request using the LAFN outgoing mail server. SMTP-AUTH ensures that the sender knows the proper password for the account.

Web Access

LAFN provides web access directly to the Internet through our dial-in service. The connection to the Internet is direct from the dial-in service and does not go through LAFN servers. As a result you need to be sure that your computer is properly configured to prevent malicious attack from Internet hackers.

Personal Web Pages

LAFN provides personal web pages for individual accounts. These pages are limited to 20 MB and are not intended for business use. Misuse of Personal Web Pages or inappropriate material will result in appropriate administrative actions. The pages are limited to directly distributed material, e.g., html, gif, jpeg etc. CGI scripts and other active components are not supported. Additional personal web page space is available if needed. See the account features web page in User Services for full information.

Personal Web pages are established when your account is activated. There may be an hour delay before they are usable. Please note, if your account terminates for any reason, the personal web pages will be deleted. There is no way for us to recover them. So you need to create them on your computer and retain a copy.

Personal Web Pages are uploaded to the web server via ftp. ftp to www.lafn.org and use your user id (e.g., bc979) and password to connect. That will connect you to your web pages. You can then transfer the files to the server. Please note that ftp to your personal web page should only be used with connections directly dialed into LAFN. Ftp sends your user id and password unencrypted where they can be monitored traversing the internet. We are no longer prohibiting the use of ftp across the internet but you use it at your own risk. There are secure ftp protocols available, sftp and scp. However, the servers for those protocols do not properly restrict access to the web pages. Once that is resolved, LAFN will support secure ftp from Internet hosts.

The URL for your personal web page is http://www.lafn.org/~user_id/page where user_id is your user id and page is the name of the file you loaded as your top level page. Pages should have the appropriate extension (e.g., html, gif, pdf, jpg etc.) to ensure that the server and browsers transfer the pages properly. For example user

bc979 can create his top level page as index.html and his URL would then be http://www.lafn.org/~bc979/index.html. Personal Web Pages are not listed in the LAFN web pages.

If you try to upload a file to your Personal Web Page and it would cause your page size to exceed the personal web space limit, the upload will be terminated with an error.

The best way to upload web pages to your Personal Web Pages is with a ftp client such a Fetch for the Mac and CuteFTP for PCs. Both are available through shareware archives. In addition, Netscape and Internet Explorer are capable of ftp'ing the files. To use Netscape to upload a file to the LAFN server, enter the following URL:

```
ftp://userid:password@www.lafn.org/
```

That will give you a directory listing of your Personal Web Page. Note userid is your userid (e.g., bc979) and password is your password.

You can then upload a file using the Upload File... function which is in the File Menu. It will give you a dialog box to select the file to be uploaded and then it will update the directory listing when the transfer is complete. Please note that the ftp implementations in Netscape and Internet Explorer are subsets of the ftp commands. In particular, there is no way to delete a web page using them. The best you can do is create an empty page with the same name and upload it.

Likewise you can download a page from the server to your computer by double clicking on the entry in the directory listing.

To view the web page you use the URL:

```
http://www.lafn.org/~userid/page
```

where userid is your userid as before, and page is the file name of the specific page you want.

Please note, placing spaces (blanks) in file names will not generally work the way you would like. Browsers do not handle spaces consistently. LAFN strongly discourages the use of spaces or other special characters in page or directory names.

Restricting Access to Personal Web Pages

Generally PWP pages are open for anyone to view. LAFN provides its users the ability to control access to their personal web pages (PWP) by establishing a password. To establish/change/delete password controls for your personal web pages, go to LAFN User Services. There are two new functions to create and delete PWP passwords. If you decide to establish a password for your PWP, do not use the

same password you use for LAFN. You will have to provide anyone you want to access your PWP with your user id and the password.

Please note that the password should not contain spaces as they may not work properly with all browsers. Also note that the change in the password system can take up to 7 hours to be effective.

Nothing changes for you when updating the Personal Web Pages. However, you have to provide the PWP password to anyone you want to access your pages. They will use that with your LAFN user ID to gain authorization. If you need to change the PWP password, you go through the same steps that you used to create it.

File Transfers (FTP)

File transfer is supported by LAFN through its dial-in service to other Internet servers. File transfer to LAFN Personal Web Pages is now supported from other ISPs. You must be aware, however, that with standard ftp clients your user id and password are transmitted across the internet and can be intercepted. This is a risk that you have to decide whether or not to accept. LAFN now provides a ftp server that handles the ftp-ssl and ftp-tls protocols (RFC-2228). These protocols will encrypt the user id and password and can also be configured to encrypt the file contents if desired. The standard ftp port, 21, is used for both encrypted and non-encrypted ftp sessions. The older sftp, scp, and implicit ftp-ssl protocols are not supported. Obviously transfer times are longer if encryption is used. There are several Windows and Unix clients that support these protocols. The following clients are believed to work properly:

```
CuteFTP Pro 2.0             Windows
FileZilla 2.0.0 beta 5      Windows (GPL)
SmartFTP 1.0 build 969      Windows
WinSSLWrap 1.17             Windows
WS_FTP Pro 7.5              Windows
FTP Voyager Secure 9.1.0.1  Windows
Lftp 2.5.2                  Unix
```

In addition there is a client available at http://bsdftpd-ssl.sc.ru that will work with Windows 9x, NT, 2000, and some Linux distributions. There are now several known clients for Macintosh. One is available in the LAFN FAQ. It only works with OS-X and is the command line client from the fstftpd-ssl distribution. In addition fetch (not free) and cyberduck (free) now support ftps although cyberduck calls it FTP-SSL. Other clients may also be available.

If you configure a ftp client to use ssl or tls, then you will see additional messages from the ftp server indicating that the SSL or TLS protocols are being used along with information on the actual encryption algorithm that was negotiated. If you don't see those messages, then encryption is not being used. Here is an example of how the connection message might appear:

```
220 www.lafn.org FTP server (Version 6.00LS+TLS)
    ready.
Name (www.lafn.org): bc979
234 AUTH TLS OK.
[TLSv1/SSLv3, cipher DES-CBC3-SHA, 168 bits]
331 Password required for bc979.
Password:
230 User bc979 logged in, access restrictions apply.
200 PBSZ command successful (PBSZ=0)
200 PROT set to P.
TLS/SSL protection of data connections on.
Remote system type is UNIX.
Using binary mode to transfer files.
```

For graphical ftp clients you would need to check for a log file that would show the actual ftp commands to determine if encryption was used.

FileZilla (version 2.2.17) requires some unusual settings. The Servertype must be set to FTP over TLS (explicit encryption). Logontype must be set to Normal. In the Advanced settings, Use passive mode must be set. Other versions are likely to require those settings also.

News Access

LAFN provides a limited News server. The disk space required for full news service is too extensive for LAFN. Therefore, we have tried to limit the news groups to those most frequently accessed by LAFN members. In addition, our server only retains news entries for 5 days. To setup a news reader for Regular or SlipStream Dial-in, you only need to configure the server to news.lafn.org. For Extended Dial-in you also have to configure Authentication using your user id and password. Users connecting via another ISP (such as DSL or Cable) can also access news by configuring their reader to provide authentication using their user id and password.

The LAFN news server appears to support the use of TLS (SSL) to encrypt user ids and passwords using port 119. The default nntp protocol does do some munging of passwords, but the algorithm used is extremely simple and trivially easy to reverse. Thus the use of TLS (SSL) is necessary to protect them. Unfortunately, we have not found any news clients that support TLS or SSL to be able to test this feature. We know there is at least one as we have seen some TLS error messages in the server logs.

Posting articles to a news group requires that you provide an e-mail address with the post. LAFN policy prohibits the use of false addresses. However, since the harvesting of news posting addresses is so common by spammers, we have provided the following approach that may be used. You can wrap your user id with no.spam as in the following example:

```
no.bc979.spam@lafn.org
```

This approach will prevent the harvesting of your address while retaining your real user id if it is necessary for us to contact you.

LAFN also provides local news groups that are moderated on community interests. These groups can be found from the LAFN news server as their names all start with lafn. In addition there is an index of these news groups available on the LAFN web pages.

Full news access is available from a number of web servers on the internet such as http://groups.google.com/.

User Computer Protection

Malicious attacks on user's computers has become a significant problem. As a result you need to insure it is properly configured so that it is protected from malicious attack. There are a number of products available for personal computers that are designed to prevent attacks when the computer is connected to the internet. These products, typically described as firewalls, are one approach to providing this protection. All current user computer operating systems provide the tools for this protection. However, it may require more understanding and knowledge of the system to configure those properly.

Checking Your Protection

While you are dialed into the LAFN dial-in service, go to http://www.grc.com. Wait for a few seconds while it goes past its splash screen to the full page. Then scroll down till you find the image for "Shields Up". Click on that and it takes you to the check page. Scroll part way down till you come to the Test My Shields button. Select that and wait while it runs the test. It will provide a resulting page that check two key protection components: Preliminary Internet Access and NetBIOS access. Both of these must return a result of closed or your protection is not working correctly.

Then scroll down to the button for Probe My Ports and select it. Wait while it runs that test and returns the results page. There are a number of ports listed. All of them must show as closed or your protection is not working correctly.

Please note that this test will not work properly if you are using the old LAFN dial-in numbers. Check the IP address that is shown early in the test process. If it shows 206.117.18.6 then you are not testing your computer, but you are testing our proxy server. The results of that test are not valid for your computer.

There is another protection check service available at

http://www.norton.com/securitycheck/

Windows 95/98/NT

Windows has the ability to be configured such that your computer is protected from malicious attack. The instructions for this configuration can be found at http://www.grc.com/su-bondage.htm. Please note that these instructions are quite involved, although not difficult. You must follow them exactly correctly or there will be no protection. In particular, where it says all, it really means all. For example, when setting the bindings for all transports, they must all be set correctly, not just the ones you plan on using. Failure to follow the instructions completely will mean that your computer is still open to attack.

There are also firewall products available that will provide similar protection without having to deal with the Windows internal configurations. Many users find the firewall products easier to setup. In addition, they will log access attempts so that you can see what was attempted.

Newer Windows Versions

Check at http://www.grc.com/su-bondage.htm for information on the latest Windows versions. Please note that it takes awhile for the information to appear after a new release.

Macintosh Systems (Non OS-X)

Macintosh system are basically setup in secure mode provided you have not added any servers. Please note, servers are very rarely added to user computers so this is highly unlikely to be an issue. There are several firewall products available for Macintosh systems. Generally the primary feature they provide is the logging of attempts to access the system. As for PCs, these products are simple to setup correctly.

Macintosh OS-X and Unix/Linux

Most all Unix and it variants have a number of servers that are listening on various port. There are a variety of different ways to protect these systems, but they are frequently dependent on the specific system in use. Consult the system documentation for appropriate techniques for protecting these systems.

Available Firewalls

There are a number of firewalls available for PCs and Macs. LAFN does not evaluate or recommend specific products. The following are brought to your attention because we know they exist. Some of them must be purchased and some are free for personal use.

Black Ice Defender
http://www.networkice.com/products/soho_solutions.html

Norton Personal Firewall
http://www.symantec.com/sabu/nis/npf/

Zone Alarm Pro
http://www.zonelabs.com/download/index.html
Sygate Personal Firewall
http://www.sygate.com/products/shield_ov.htm

McAfee Personal Firewall
http://www.mcafee.com/myapps/firewall/ov_mail-list

Additional firewall products are listed at
http://www.dslreports.com/information/rated/security

Time Service

Time service enables your computer to synchronize its clock to the LAFN server's clock. This is not required but some users find it useful. LAFN provides time service using a complete implementation of the Network Time Protocol (NTP) version 3 standard, as defined by RFC 1305, that also retains compatibility with version 1 and 2 servers as defined by RFC 1059 and RFC 1119, respectively. Time servers are available using port 123 on zoon (206.117.18.9), zoom (206.117.18.8), and zook (206.117.18.5).

User Domains

LAFN supports User domains. A user domain permits a user to have their e-mail and web addresses use a personal domain such as joe@joe.com. There is a cost for establishing a user domain. See LAFN User Services for the current cost of this service.

To establish a user domain you must first register your domain using one of the registries. See http://www.internic.net/regist.html for the current list of registries. When you register your domain you must notify the registry of the DNS servers for your domain. You have two options: have the registry provide DNS for you or have LAFN provide DNS for you. LAFN does not charge extra for providing DNS. Costs for registering a domain change occasionally so check with the registry for that information.

If you elect to have the registry (or some other DNS server) provide DNS then you must arrange with them to setup DNS entries for mail pointing to mail.lafn.org (currently 206.117.18.9). You also have to have them setup a DNS entry for www

pointing to www.lafn.org (currently 206.117.18.8). Please note, if we have to change those assignments you will also need to make corresponding changes to your DNS service.

If you elect to have LAFN provide DNS, then you will need to register the domain name with DNS servers selected from the following list:

dns1.lafn.org
dns2.lafn.org
dns3.lafn.org
dns4.lafn.org
dns.rexx.com
ns3.rexx.com

Including one of the rexx.com servers is probably a good idea as it ensures that DNS is not dependent on our internet connection. Then you need to send a request to ops@lafn.org with the new domain name.

Once that is complete, you need to go to LAFN User Services and activate the user domain. User domains can be paid for via check or credit card. Once the payment has been processed, the domain will be activated. Please note, that domain activations only occur after 11 PM and take about 2 hours to complete. If everything is in place by 11 PM then your domain will be active by 1 AM.

All mail sent to any user at your new domain will be directed to your LAFN mailbox. Please note, this is required by RFC since all domains are required to have several mailboxes that are monitored by a user - particularly abuse, postmaster etc.

LAFN does require that you notify ops@lafn.org if for any reason your domain registration is allowed to lapse or is terminated. We need to ensure that we are not advertising unregistered domains.

Please note that your user domain will only work with browsers that send HTTP 1.1 requests. The older HTTP 1.0 browsers do not include the information to identify which domain is being requested. There will be some people who get the LAFN home page when trying to access your personal web page. They will need to use the old form of URL to access your personal web pages.

User Services

LAFN User Services provide a way for users to access their account information and make changes to some of the LAFN services. User Services is access through the LAFN web page at http://www.lafn.org and select the LAFN User Services link. User Services requires SSL encryption to protect the information from being monitored as it traverses the Internet.

When you login to User Services you must enter your user id and password. Do not enter your mail address, e.g., bc979@lafn.org. Just enter your user id, e.g., bc979 and your password. The dialog box will usually say User Name, but that is misleading. It will only work with your user id. If you try to login with the local login button and your are not dialed into LAFN, you will get a password error return.

Establishing a SSL Certificate

The first time you use a particular computer to access the User Services web pages you will be presented with a new certificate to accept. While the process is different between Netscape and Internet Explorer, the concepts are the same and the same general approach is used. Here is the Netscape approach:

First window: New Site Certificate
Press the "Next" button

Second Window: Here is the Certificate being presented...
There is a "more info" button you can press that will take you through the contents of the certificate. That is not required but might be interesting.
It will return you eventually back to this window.
Press the "Next" button.

Third Window: Are you willing to accept this certificate...
Select the radio button for Accept this certificate forever
Press the "Next" button.

Fourth Window: By accepting this certificate you are ensuring that all information you exchange with this site will be encrypted...
Press the "Next" button.

Fifth Window: You have finished examining the certificate presented by zoon.lafn.org...
Press the "Finish" button.

At this point you should be at the LAFN Management Functions page and the browser should show that the page is encrypted. Netscape has the lock closed.

Once this procedure is completed successfully, you will not be asked about the certificate again - at least until it expires.

The User Services web pages will function the same as when you are dialed in, however, they will be slower. It takes time to both encrypt and decrypt the information. Please remember that the browser will retain your user id and password which you have to enter to access the functions. You will need to quit the browser when you are done to clear them from the system.

E-mail Forwarding

E-mail forwarding is established through the LAFN User Services web page. The "Forward your e-mail outside LAFN" function will permit you to enter a forwarding e-mail address. When you submit that form, your e-mail will be forwarded to the new address. Please note, any e-mail in your mailbox at the time you submit the form will not be forwarded. You still have to retrieve it via the LAFN POP server.

If you want to change your e-mail forwarding, the same function will make the change. To remove e-mail forwarding so that your e-mail is once again delivered to the LAFN POP server, use the remove e-mail forwarding function.

Changing your Password

The LAFN User Services web page includes a "Change your password" function. This function provides you the ability to enter a new password. Please note, the password appears on your screen in the clear. Protect it. Once you have submitted the form with the new password, it can take up to 2 hours for the new password to become effective. Please note, LAFN cannot read your password, It is encrypted after you enter it. If you forget it, you will have to call the LAFN answering machine described below to have a new one created.

Changing your User ID

Your user id is used to identify you to anyone you have communicated with. This includes e-mail, news, mail lists etc. When you make this change, those people (and lists) will not be able to communicate with you unless you properly notify them of the change. For some people this may be very difficult because some lists and people do not send to you very often and may be easily overlooked. Once the change is made it can be difficult to recover those connections.

The user id can be changed for either a primary account or a family account. The procedure is basically the same in either case. If you are converting a primary account that has family accounts (or affiliate accounts) with the id style of userid-n where n is a single digit, then those will be converted also to the new user id. If you have previously changed the id of any family accounts, those will not be changed but retained as they are.

For example, if you are changing the primary account xxx to yyy and have 3 family accounts: xxx-1, zzz (previously changed from xxx-2), and xxx-3 then after you do the conversion to yyy you will have the primary account of yyy and the family accounts of yyy-1, zzz, and yyy-3.

To make the change in user ids you need to go to the new user registration web page and register as if you were creating a new account with the new user id. Enter all the information that is required accurately as this will become your user record. Your last name and date of birth must match those in the current record.

Once the data is correct, submit for a new account. You will receive a page telling you how to pay for the account etc. Ignore that page. You do not need to send any money for this change.

Instead, go back to LAFN User Services and select the "Convert an old user id to a new one" link and fill out the form. When you submit the form, the moving of the accounts will be attempted automatically. The new account should be ready to use the following day. If there is an error in processing the request you will be provided an error message. Send it to ops@lafn.org.

After the move is complete, the old account will be expired and will be deleted 30 days later. During that time you will be able to use it to check for e-mail from people you forgot to notify. However, at the end of the 30 days, any e-mail remaining in that account will be deleted and anyone sending to it will be told the account does not exist.

Updating your Account Information

Your LAFN Account record includes the information that you entered when the account was registered. This includes name, address, and phone number. This information needs to be kept current. If you call LAFN with a problem and provide your user id, we use that to obtain address and phone number in order for a mentor to contact you to help you resolve the problem. If you have moved and not kept the account information up to date, the mentors have no way to contact you and will close the trouble ticket.

You can view your account information through the web and update it as appropriate. From the www.lafn.org select the entry for LAFN User Services and then select the entry for Update your LAFN User Record. You will be asked for your user id and password to insure that only you can update your account information. Review the information in the form. Correct as appropriate and select the Update button to update it if necessary.

Mentors

Volunteer mentors provide the technical support to LAFN users to assist them with problems in using LAFN services. Since many problems prevent the receipt of e-mail, mentors frequently have to call the users. Because LAFN covers a very large area, we need mentors in all areas we serve. There is always a need for more mentors who are willing to volunteer their time and expertise in assisting other users. If you are interested, please e-mail jay@lafn.org for more information.

Trouble Tickets

LAFN has established a Trouble Ticket System to track the issues raised by our users and ensure timely responses are provided. Trouble tickets are initiated for calls received on

the LAFN answering machine or from e-mail received by LAFN staff that needs to be referred to the mentors. The LAFN home web page has a link to the Trouble Ticket Entry form for you to use to enter problem information. Please note, while there is nothing preventing you from calling the phone number, sending e-mail, and creating a ticket that will result in 3 tickets being generated for you. Since all of our mentors are volunteers, that will not endear you to them. The fastest approach is to generate the ticket yourself since it eliminates at least one manual step.

User Training

LAFN provides user training sessions via the web. Because the area of coverage for LAFN is too large to make hands-on training impractical we are in process of developing Quicktime presentations to provide information on using and configuring the various clients commonly used on the internet. To access User Training you go to User Services and select the link for user training. You will need to be sure you have Quicktime installed on your computer. There are complete details on obtaining Quicktime in the User Training web pages.

Contacting LAFN

Account Issues

Account issues should be e-mailed to gladys@lafn.org if you have the ability to send e-mail. If not, then you can call the LAFN answering machine at (323) 906-7219 and leave a message. Please note, that number is an answering machine and will be checked daily and forwarded to our mentors.

Technical Issues

The fastest method is to create a Trouble Ticket as described above. Technical issues can also be e-mailed to ops@lafn.org if you have the ability to send e-mail, or called in to the LAFN answering machine at (323) 906-7219. The answering machine is checked frequently and the messages will become trouble tickets for the mentors.

Problems with LAFN Services not functioning properly

Problems with LAFN services failing should be sent via e-mail to ops@lafn.org. While they can be called in to the LAFN answering machine, that will delay our response to the problem. Non-functioning services will affect many users and we need to get them repaired as quickly as possible. Please note, we may not be able to respond to your e-mail since the volume of messages may be quite high. When we have information on the problem or its correction we will issue a System Bulletin.

Status information on LAFN system problems is also available at the news group news:lafn.admin.questions. You may want to check with this news group if you are

encountering problems before making changes to your system. If there is a known LAFN problem it will be posted there. That group is monitored frequently while problems exist.

Status information is also available from the web page:

```
http://lafn.blogspot.com/
```

Please note that access to this site will generally be available even when the LAFN servers or internet connection is down.

When reporting problems with dial-in connections, we will need at a minimum the number you are calling from, the number you are calling, what you get when you call that number on a phone, and your local telephone company (e.g., Verizon or Pac Bell). Please note, we need the full numbers including area code. We may also need the type modem you are using. For other issues, please keep in mind that we cannot see your computer. You have to tell us the specific details of what you are trying to do and what happens in result. The specific wording of error messages is very important. Sometimes the needed information is buried in what appears to be insignificant in the message.