Project Athena Technical Plan

The Athena Workstation

Win Treese
Bill Bryant
Bill Cattey
MIT Project Athena

Michael Johnson
Noah Mendelsohn
MIT Project Athena / International Business Machines Corp.

DRAFT of 26 November 1986 at 16:28
$Revision: 1.2 $

Table of Contents

1. Introduction

This document describes the Project Athena workstation and the services that it accesses through a network. It primarily addresses the workstation system itself, without specifying details of network services, though we assume that each service is available. For the most part, the system described here is a "public" workstation that is managed by Project Athena, though some consideration is given to changes necessary for private workstations. This is an evolving document developed by the Athena Workstation Design Team, and it will continue to change as the workstation design does.

There are several aspects of the workstation design discussed below. The first, "Classes of Workstations", discusses some of the major issues in workstation configuration and describes the basic properties of the standard Athena systems. Next, "User-Level Services" details the services (such as electronic mail) that are available to the user of a workstation. Third, "System-Level Services" describes the system and network services necessary to provide the Athena environment. Fourth, "Managing the System" discusses some of the issues involved in managing workstations in a distributed environment.

Note that this document currently describes a combination of the present workstation system, changes that are forthcoming in January of 1987, and changes that are further down the line. As the workstation design evolves, detailed descriptions of each system release will be made available.

Comments in *italics* indicate the firmness of a particular section or work that remains to be done.

1.1. What is an Athena Workstation?

An overview of the Athena workstation and its environment is described in the *Project Athena Technical Plan: Objectives and Requirements* (Section B), and *Project Athena's Model of Computation* (Section C). The software base assumed here is Berkeley UNIX[1] 4.3BSD. The UNIX kernel for each particular workstation is supplied by the vendor. Currently in use are Ultrix[2] for the VAXstation II and 4.2A for the IBM RT/PC[3]. Utilities that depend on the particular machine or kernel are drawn from the vendor systems as well; the rest of the software is drawn from 4.3BSD.

1.2. Design Criteria

There are several criteria for the design of a workstation for the Athena environment. One of the most important is that the workstation function well for students who are not especially interested in computers, since Project Athena is intended for educational applications. In addition, the workstation must also be:

- Reliable
- Similar to standard UNIX
- Maintainable
- Robust
- Reasonably secure
- Easy to install

---

[1] "UNIX" is a trademark of AT&T

[2] "Ultrix" and "VAXstation II" are trademarks of the Digital Equipment Corporation

[3] "RT/PC" is a trademark of International Business Machines Corporation

An important part of the workstation's robustness is its ability to ignore network service failures that occur when it is not in use. For example, if the library server crashes and is restarted when no one is using the workstation, the next user should not be affected by this. This implies that the workstation must be brought to a usable state when a user logs in. See the section on "Login/logout Service" below.

In addition, a workstation must require minimal system management. Traditionally, UNIX machines have had a "wizard" available to fix problems and assist users. This is unrealistic in a distributed workstation environment, so the workstation must not require "wizardry" to operate. Finally, the workstation is primarily designed for operation by a single user through the console.

2. Classes of workstations

Project Athena supports a small number of "standard" workstation configurations. These configurations have variations of two important characteristics: which users have access to them and what kind of network connection is available to them. There are also minor variations on these configurations. Such variations are generally part of exporting a service, such as printing, from a workstation.

2.1. Access

We define three categories of user access: public, semi-public, and private. Public workstations may be used by any registered Athena user who authenticates himself to the system and can be found in clusters scattered throughout the campus.

Semi-public workstations are generally used by a restricted set of people and are not open to the general Athena user. These are designed for use in living groups and development clusters.

Private workstations are those owned and managed by an individual, though he may allow access to his workstation certain other users.

2.2. Network Connection

We also define three categories of access to the campus network, based on the bandwidth of the connection: high-speed, medium/low-speed, and no connection at all. High-speed connections are usually available to workstations on the campus, while medium/low-speed connections are used by off-campus sites such as living groups. A workstation may also be operated without any network connection at all. Such workstations must not be configured to require access to any network services.

2.3. Athena Standard Configurations

Of the possible variations of systems listed above, Athena defines certain ones as "standard" and "supported". They are:

1. Public Workstation -- available in clusters on campus; accessible by any Athena user. The workstation is reset between sessions such that nothing of a previous user remains. These workstations are managed by Project Athena.

2. Living Group Workstation -- available in small clusters in a living group, usually with a high-speed local area network and a medium/low-speed connection to the campus network. Management of these is shared between the living group and Project Athena.

3. Private Workstation -- owned by a particular individual. At this time, this kind is most commonly found in the offices of Athena staff members. It has a high-speed

connection to the campus network. The owner is responsible for managing it, though Athena provides software and system support. A private workstation may also have a non-standard hardware configuration, though Athena may not support differences from the standard systems.

4. Standalone Workstation -- This workstation is configured to work without a network connection at all. It has sufficient local software and services to be useful with the network. Standalone workstations are managed by their owners, which may include Project Athena.

Some workstations, as well as larger machines, are configured to act as servers for various network services. These systems are described in the document *Athena Server Configuration*.

2.4. For More Information

Separate documents describe the following aspects of the workstation system:

- The User Viewpoint
- Living Group Configuration
- Athena Server Configuration

None of these documents have been written at this time.

3. User-Level Services

This section discusses the software and services available to users of Athena workstations. Access to services is generally limited to users who can authenticate themselves (see the section on "Authentication" below).

3.1. User Interface (Shell)

The standard user interface to a workstation is the C shell, supplied by 4.3BSD. Standard environments and command scripts, such as those executed at login time or used by a course, are designed with this interface in mind. There may be other shells available for use, but Athena may not support standard environments for them.

3.2. File Management

Users can store their files in a variety of ways. They may be stored on central disks operated by Athena, or on removable media, such as floppy disks or magnetic tapes. These issues are dealt with more fully by Bill Cattey in the document "Athena Storage Model"; this document presents the plan for managing user files.

3.2.1. Disk Storage

Central disk storage is provided using the Remote Virtual Disk (RVD) system. Each user is allocated a "locker", or RVD filesystem. He can then attach the locker to the workstation filesystem and use it for working or temporary storage. The locker behaves as an integral part of the workstation filesystem. Servers for user lockers are managed by Athena, but the filesystems on them are not.

To attach a locker to the filesystem, a user executes the "up" command. This program requests necessary information from the nameserver (discussed below), spins up the RVD pack, and mounts the filesystem. When the user is finished, he may explicitly detach it. If he does not, the system will detach it when he logs out.

Lockers may eventually be replaced by a network-based filesystem, if a suitable one becomes available. Users will need tools to manage their lockers. SMS will need to handle allocation and location of lockers.

3.2.2. Removable Media

There are two types of removable media available for workstations: streaming tape and floppy disk. Both may be accessed from all workstations, though it may be necessary to use a network service to do so.

Streaming tapes hold large quantities of data and are best used for backups or for transferring many files at a time. The tapes currently available can contain 70 to 100 megabytes. Two incompatible tapes are available, the TK50 for DEC machines and the QIC02 tape for the RTPC. The *tar* command is used for reading and writing tape archives. The commands *dump* and *restore* may be used for backing up entire filesystems, such as an RVD locker or a filesystem on a semi-private or private machine.

Floppy disks may be used for storage between login sessions. They can contain 1.2 megabtyes of data (some older Athena workstations have floppy disks that contain only 360 kilobytes). The floppy disks use a filesystem based on that of MS-DOS. Commands for accessing the floppy, such as *dosread*, *doswrite*, *dosdel*, and *dosdir*, is available.

The software for this already exists on the RTPC. Licensing issues for the VSII will need to be resolved. A filesystem check utility for DOS filesystems needs to be developed. Other solutions to this are also possbile; they are discussed by J. H. Saltzer in The File Interchange Problem.

If a particular workstation does not have the desired device, it is possible to access a device remotely. To do this, a user must first "grab" the remote device for exclusive access. Network-based versions of the standard commands for accessing tapes or floppy disks may then be used to read or write data. When done, a user should release the device so others can use it. If he does not, the exclusive access expires after a certain period of time (currently five minutes).

These utilities and procedures for using them need to be worked out.

3.2.3. Backup

It is the responsibility of the user to backup any important data stored in RVD lockers, removable media, or the workstation disk. The standard commands for accessing removable media and RVD lockers may be used for this. In particular, it may be useful in some cases to use *dump* and *restore* to backup filesystems such as an RVD locker.

3.2.4. Transferring Files Between Systems

Files may be transferred to or from other hosts using the commands *ftp*, *tftp*, and *rcp*. Files may not be transferred to another public workstation unless the current user of that workstation has authorized it (see "Remote Access to Other Workstations" below). Such authorizations expire when the user logs out. Files may not be transferred to an unused public workstation.

The authorization needs to be implemented. The method of access may change with a network-based filesystem.

3.3. Access to Course Material

Materials used by particular MIT courses are available as RVD packs. When a user requests that a course filesystem be attached, the RVD system locates, spins up, and mounts the desired pack.

In order to allow automatic modification of a user's environment for course work, the root of an "attached" filesystem can contain a file called *.attachrc*. A standard alias in the default *.cshrc* can be used to attach a filesystem and execute *.attachrc* using the csh built-in *source* command. The attach command provides as output the mount point of the filesystem so that the *source* command can find it. A user may execute the unaliased version of the command if he does not wish to modify his environment.

Corresponding to *attach* is a *detach* command, which can be used to remove attached filesystems. Part of the detach procedure is to undo as many changes to the user's environment as possible. An instructor has two options for accomplishing this: one is to perform all of the course work in a subshell, which exits when the filesystem is detached; the other is to preserve the user's environment in a file and restore it later. Preserving and restoring the environment is the standard method.

Course RVD lockers are updated by creating a new version and then performing an RVD packname exchange, under the control of authorized managers for that course's lockers. When a name exchange has been done, the manager may notify all continuing users of the old pack through the notification service (see below).

3.4. Printing

A user may send files to a printer using the *lpr* command. The printer system does no queueing on the workstation; if *lpr* cannot connect to the appropriate printer server it simply notifies the user of this fact. The user may request that he be notified through mail or the notification service when the printing has completed.

A possible upgrade to the printing system is being explored by the Hardcopy Task Force.

Changes to alter the queuing behavior of lpr need to be implemented.

3.5. Mail

3.5.1. Receiving Mail

Each user receives mail at a "post office", a server maintained on a separate machine. He may read his mail by first transferring it to his current workstation and then reading it locally, using the MH mail handling system. Several other methods for reading mail are available, such as *gnuemacs* RMAIL and Berkeley *Mail*. The Post Office Protocol (POP) is used for transferring mail. A user may save his mail in a variety of ways, as described in the file storage section of this plan.

3.5.2. Sending Mail

Mail sent by a user is processed by the ***sendmail*** system available with 4.3BSD. A workstation forwards all mail to an outgoing mail server, which then routes it appropriately. The standard interface to ***sendmail*** uses MH, though others (*e.g.*, Gnuemacs RMAIL and Berkeley ***Mail***) are available.

3.6. Real-time Communication with Other Users

The primary channels for this are the standard ***talk*** and ***write*** programs, modified to use the notification service (discussed below).

3.7. Notification

Users may be notified of events by the notification service, which talks to the workstation window system. Notifications may come from other users or from services. A user may "subscribe" to certain classes of messages that he wishes to see. See the document *Project Athena Technical Plan: Notify Service* (Section E.4.1) for more information.

The notification service is still under design.

3.8. Documentation

A user may browse through documentation available on the Athena system. At this time, on-line documentation consists of the UNIX manual pages and the standard UNIX documents contained in */usr/doc*.

A subgroup of the Human Interface group is examining documentation browsers.

3.9. On-line Consulting

A user may communicate with Athena consultants or other knowledgeable users through the On-Line Consulting (OLC) system.

There should be documentation on this elsewhere.

3.10. Remote Access to Other Workstations

By default, it is not possible to remotely login to a workstation. This restriction is intended to protect the user of a workstation from malicious activities. The user of a workstation can specify which other users may remotely access his workstation.

The authorization mechanism for this needs to be designed and implemented. There is also

a problem of allowing operators to login remotely to fix problems.

3.11. Standard Applications

Several standard applications, some from 4.3BSD, some from third-party vendors, are available on Athena workstations. These are normally accessed through the system library service described below.

3.12. Programming Interface

The programming interface, for users writing their own programs, for a workstation is the standard Athena interface defined in the *Project Athena Technical Plan.*

3.13. Integrity Check

A user may, at any time, validate the integrity of his workstation. A check is also performed when a user logs out. There are three kinds of validations that may be run:

- Fast, but not entirely thorough.
- Thorough, but slower.
- System update.

The fast version operates by simply checking the modification dates and sizes of each file on the workstation root filesystem and comparing them with those of files on an RVD pack containing a copy of the currently distributed system. The RVD pack contains a file listing the necessary information in order to speed the process.

The more thorough version makes the same checks as the fast one, but also computes checksums on the files and attempts to verify that system configuration files are at least reasonable, since they vary somewhat from workstation to workstation.

The update version brings the workstation in line with the RVD pack, except for local configuration. This case is discussed under "System Update" below.

This system needs to be designed and implemented; it is not fully specified here.

4. System-Level Services

In addition to the services available to the user, the workstation system requires that certain low-level services be available to support the users and the environment. This section describes those services and some details of their interactions with the rest of the world.

4.1. Access to Software Libraries

The standard Athena workstation provides access to a large set of software. Because of the hardware configuration of these workstations, this set is divided into two parts: software stored on the workstation and software accessed through the network. As a general rule, the software that resides locally on the workstations consists of the minimal set necessary to get the workstation up and running, as well as that necessary to fix software problems on a workstation. In practice, the local software is a relatively standard UNIX root filesystem; that is, it consists of the root directory and the subdirectories ***/etc***, ***/bin***, and ***/lib***.

Other standard software, normally part of the ***/usr*** filesystem, is accessed through the network using the Remote Virtual Disk (RVD) system.

Software libraries such as those for courses or user-contributed software are available through the RVD system as well.

4.2. System Update

In order to provide new software and upgrades to existing software, some method of updating the software must be available. For remote software libraries, updating is performed by creating a new version of an RVD pack and copying it to all library servers. This procedure is described in the *RVD Operations Guide*.

Updates to the workstation's local software are initiated by the workstation at periodic intervals or when requested by the user. A copy of the currently distributed system is available on an RVD pack, which the workstation compares to its own system, making any changes that are necessary. Such changes are managed by the *track* update system, which also handles differences in configuration files. Updates of public workstations are logged to a central location so they can be monitored.

The track system is currently being evaluated for this use.

4.3. Name Translation

Name translation is the key to a useful network environment. A request to use a network service must be able to find the host providing the service and must know how to connect to it. For example, a request to print a file on a nearby printer must determine which of the many available printers is "nearby," find the name of the server with the printer, and look up its network address in order to open a connection to it. Details of the name resolution system can be found in *Project Athena Technical Plan: Name Service* (Section E.2.2).

Resolution of machine names to network addresses is handled by a name service provided by MIT Telecommunications.

Workstation services that require name translation other than machine names include:

- RVD packs
- authentication
- printer names
- mail
- software libraries
- login

- network port lookup (replacement for */etc/services*)
- on-line consulting

Part of the installation procedure is to initialize the workstation's nameserver cache with important information about itself. Each time it boots, the workstation will check with the nameserver to see if information about it has become available. If so, the workstation discard the cache information. This procedure also allows customization of the nameserver cache for private workstations.

Details of this modification need to be worked out.

4.4. Authentication

In a distributed workstation environment, it is much more difficult to verify the identity of a user, since anyone may reboot a workstation and claim to be any Athena user on that workstation. The Athena authentication system is discussed in *Project Athena Technical Plan: Kerberos Authentication Service* (Section E.2.1). Workstation services that require authentication include:

- tftp
- rlogin, rsh, rcp
- User information
- RVD
- mail reading (from the post office)

4.5. Login/logout Service (Toehold)

4.5.1. Logging In

Because a public workstation contains no information about users when not in use, the workstation environment requires several modifications to the standard UNIX login and logout procedures. A user must be authenticated using a central service, and the workstation must be brought into a usable state.

When not in use, a workstation displays the message "Hit any key to begin" on the console. The window system is not running, since the workstation has no RVD packs spunup. When someone presses a key, the workstation firsts spins up its default RVD packs and starts the window system. The RVD packs used are specified by the nameserver. The window system displays a single window, with a prompt for the user to login. The workstation also requests the time from a time server.

At this point, the user types his username and password. Authentication of the user is handled by Kerberos. If the user is who he claims to be, the *login* program discards his password and adds a standard password entry, provided by the nameserver, for the user into */etc/password*. On private workstations, a user may already be listed in the password file. If so, he is assumed to have a permanent account there.

Next, the workstation attempts to find an RVD locker for the user. The nameserver provides information about lockers, including their locations and mount points. If the mount point for the locker is his home directory (~), it is spunup and mounted there. If it is another directory (assumed to be relative to his home directory) or if a locker cannot be spunup, a home directory is created for the user. The locker is mounted on the appropriate directory if it is available. The workstation also copies standard initialization files, such as *.login* into a home directory that it creates.

Finally, the login process completes by starting a shell. As usual, the shell finds its

initialization files in the user's home directory, whether it is on the local disk or an RVD pack.

The workstation also collects system messages for the user and displays them appropriately.

It is also possible, using CTRL-~, to get a login prompt on a workstation without spinning up the standard RVD packs and starting the window system. This is intended for use by operations personnel when repairing problems with a workstation.

The toehold system needs to be reworked to fit into this model. The nameserver must know about password files entries and RVD lockers. Eventually, the system messages will be provided by the notification service. X version 11 will make it possible to run the window system while the RVD packs are not spunup. The contents of the initialization files remain to be worked out.

4.5.2. Logging Out

For the most part, the logout procedure reverses what was done at login. First, all processes owned by the user are killed. The user's locker is spundown if it is mounted. If a home directory for the user was created, its contents are deleted and it is removed. The user's Kerberos authenticator is also deleted, and his entry is removed from */etc/passwd*. The authorization list for remote access is cleared. Next, the workstation kills the window system and runs an integrity check. If this check fails, it attempts a system update. If the update fails, this information is logged to a central location for Operations. Finally, all RVD packs are spundown.

Again, toehold needs to be modified to fit this model.

4.6. Time Service

Workstations must have the same date and time in order to synchronize events, particularly the timestamps on Kerberos authenticators. To do this, each system requests the time from a central service when it boots and when it deactivates.

The time service will probably be supplied by the Kerberos server machine.

4.7. Messages of the Day

Many services, as well as the Athena staff, will want to provide messages to users when they login or first access these services. All system messages are collected by the workstation when a user logs in and displayed in an appropriate window.

Initially, messages will be displayed in the login window. Eventually, they will be handled by the notification service.

4.8. Internet Address Assignment

As workstations become more prevalent and are moved from place to place, it will become necessary to automatically assign network addresses to machines at boot time.

Jeff Schiller is working on a method for managing this.

4.9. Boot

There are a number of actions necessary at system boot time. These are described separately, in the document "Boot Procedures for Athena Systems" by Win Treese (not yet written). In particular, a workstation that has filesystem errors which ***fsck*** cannot handle will halt until a knowledgeable person can repair the filesystem.

5. Managing the System

Managing a system of several hundred workstations with associated services is not easy. It is necessary to provide many tools for this purpose, as well as to restrict to a great extent the differences that must be handled. One important requirement is that much of the management should be automatic, with only occasional manual intervention. A current example is the generation of password files for Athena timesharing machines, which is entirely automatic, except when problems arise. The Service Management System, described in *Project Athena Technical Plan: Service Management System* (not yet written), handles most of these problems. It is assumed that workstations owned by Athena are managed centrally, except when the management is delegated to a local cluster, as in a living group or development group. The general approach is that the local workstation filesystem is standard, with necessary configuration files generated "on the fly."

5.1. Installation Kits

Installation kits and procedures for workstations are designed to allow complete installation (both hardware and software) in approximately two hours: 40 minutes for hardware setup and diagnostics, 60 minutes for software installation and configuration, 20 minutes for ironing out the bugs. The general approach is to boot a workstation from floppy disk or tape, spinup an RVD pack, and dump its contents onto the workstation hard disk. After completing the dump, the system asks the installer for configuration information. Some of this information is permanent, such as the hostname. Other information is be used to provide name service information until the standard Athena nameservers know of the newly installed workstation. This method also allows installation of private workstations that fit the Athena model.

Permanent configuration information includes:

- What is the machine's name?
- What class is it in?
- Is the machine a printer server?
- Is the machine an RVD server?
- Is the machine an RVD client?
- Is the machine a post office?
- Does the machine run a sendmail daemon to receive mail?
- Does the machine use disk quotas?
- What filesystems does the machine have?

Initial name service information includes information on defaults for:

- Printer servers
- RVD server
- Kerberos server
- OLC server
- Password entry server

Current installation kits need to be reworked to this model.

5.2. Configuration Differences

One of the most difficult problems to handle on a large scale is configuration differences between workstations. To simplify this problem, we first define a small number of supported classes of workstations, described above. Each class defines certain standard characteristics for that kind of workstation.

Some differences are handled at boot time. The ***/etc/rc.local*** file defines several "configuration variables". These variables then affect the exact actions performed later, but they allow several differences to be restricted to a single file.

Many configuration differences are handled by the name resolution system. For example, the name system knows which printers are normally associated with a given workstation. This decreases the number of files that differ from workstation to workstation, since the nameserver can subsume the functions of, for example, *clustertab* and */etc/services*.

Private workstations present additional problems, since their owners may wish to modify many parts of the system. This problem is handled by a defined a standard private workstation configuration, which includes guidelines describing which parts a user can modify while retaining compatibility with the Athena system. Private workstations may also use a non-standard update description file, making it possible for the owner to track changes to the standard Athena system and add appropriate changes to his workstation. Tools for managing accounts on private workstations are be available as well.

The private workstation configuration document needs to be written. Tools for account management need to be implemented. Update description files will work with the track system described above.

5.3. Remote Error Handling

There are two sides to handling errors remotely: logging of errors that occur on workstations and servers, and repairing problems from a remote machine. The first problem, error logging, can be solved using the 4.3 *syslog* system. Normally, remote error logging is disabled, though operators may enable it for a particular workstation if it is having problems that are difficult to trace. Some services, such as RVD, log critical errors remotely so that operators may respond quickly. System updates and integrity-check failures are also logged.

Repairing problems remotely is difficult in some cases, easy in others. A workstation that encounters fileystem errors that an unattended *fsck* cannot handle would not be available for access through the network. Other problems, such as a full filesystem, may be fixed easily if an operator logs in from another machine. Privileged operators can remotely login to a workstation if it is in a reasonable state.

It is not clear that the operators can login given the restrictions on network access given above. This problem will require some thought.

5.4. Exporting Services

As Athena evolves, users will wish to export services from public workstations during a session or from private workstations that they own. To fit in with the Athena model, those services will want to take advantage of some of the standard services used by system software, particularly name resolution and authentication.

The issues of how users can use them still need to be worked out.

I. Changes to this document

```
$Source: /u1/projects/workstations/RCS/draft.mss,v $
$Log:   draft.mss,v $
Revision 1.2  86/11/26  16:28:06  treese
Extensive reworking.

Revision 1.1  86/11/07  10:49:59  treese
Initial revision
```