VINES 5.5 ARL Overview LAN Services Tutorial #10

Contents

Introduction

An access rights list (ARL) is a means of securing VINES file services (network drives) so that access to files contained on them is limited to the appropriate people. In VINES 4.11, each directory and subdirectory on a network drive has an ARL that specifies users and designates access rights levels. As a system administrator, whenever you create a new file service or new directories on existing services you must execute the SETARL program and edit the default ARL to limit user access. Up to five StreetTalk names -- user IDs, lists, or StreetTalk patterns -- can be entered on a VINES 4.11 directory ARL.

With VINES 5.5 (and VINES 5.0), Banyan completely redesigned the ARL scheme. What was wrong with the VINES 4.11 ARL scheme? Absolutely nothing, but Banyan wanted to accomodate other file systems, such as the Mac and Unix, which already have their own file security methods. The result is an ARL scheme that is more flexible and extensive, and at the same time, more difficult to understand, particularly as one moves to VINES 5.5 from VINES 4.11.

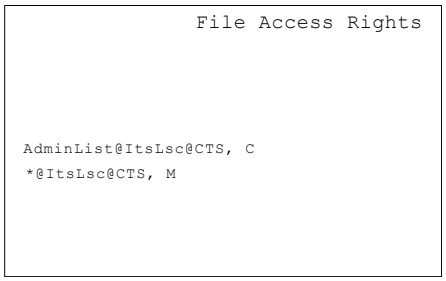
This tutorial provides an overview of the VINES 5.5 ARL scheme and how VINES 4.11 ARLs migrate to VINES 5.5 ARLs. In addition, you'll find suggestions for configuring VINES 5.5 ARLs after upgrading from VINES 4.11 and after creating a new VINES 5.5 file service. The Appendix includes a review of VINES 4.11 ARLs and a discussion of access rights under the Mac and Unix file systems.

VINES 5.5 ARLs Summary

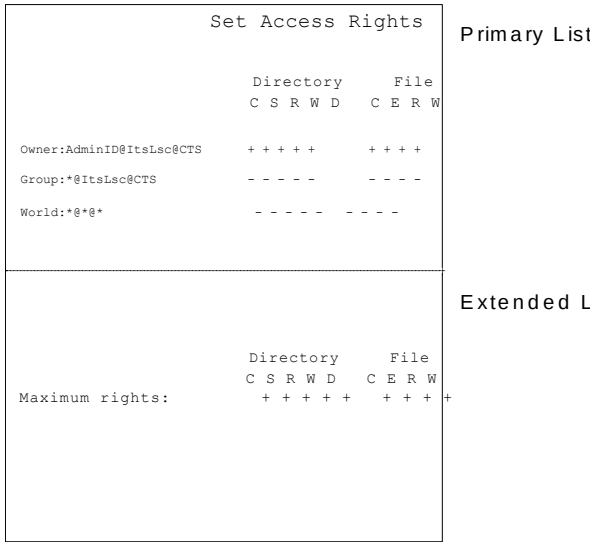
Just as in VINES 4.11, you can examine and change VINES 5.5 ARLs by executing the VINES SETARL command, which displays the access rights screen. There the similarity to VINES 4.11 ends, however. (See the Appendix for a review of VINES 4.11 ARLs.) Here are some of the key highlights of VINES 5.5 ARLs. The rest of this section will explore each of these points in greater detail.

- The access rights list is a two-part list consisting of a *primary list* and an *extended list*. The extended list is optional; the primary list is not.
- The primary list contains three different user categories for purposes of assigning access rights; these are the *Owner*, *Group*, and *World*. The extended list can hold up to five StreetTalk names, lists, or patterns.
- The primary and secondary list each contain two ARLs: the *directory ARL* specifies access rights for the directory itself and for new subdirectories created within the directory; the *new file ARL* specifies the rights for each new file created in that directory. After a file is created or copied to a subdirectory, its *file ARL* can be viewed and edited independently of the directory ARL, and likewise, editing the directory ARL will not affect the file ARLs of existing files.
- Each access right must be set explicitly; that is, the access rights are not cumulative as they were in VINES 4.11. For example, to achieve a setting comparable to the VINES 4.11 Control rights, you must select all the rights -- control, search, read, write, and delete -- for a directory, as well as control, execute, read, and write for new files.
- The default settings for an ARL depend upon whether the server was upgraded from VINES 4.11 or a new VINES 5.5 file service was created.
- Access rights settings can be viewed and saved according to the rules for VINES or Mac ARL schemes, although it's recommended that all users at PG&E follow VINES rules. See "VINES and Mac ARLs compared" later in this document for more information.

VINES 4.11



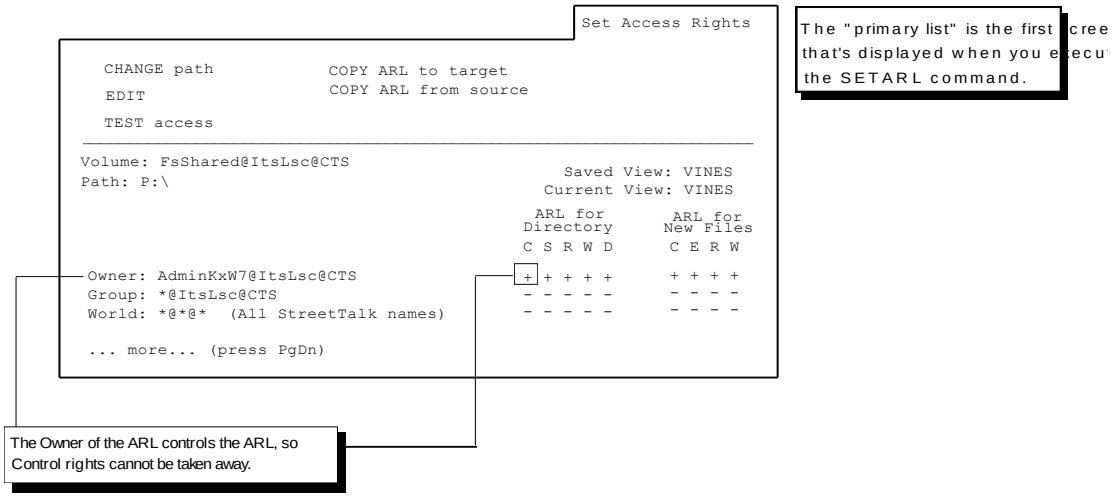
VINES 5.5



Access Rights Lists

The access rights list is a two-part list consisting of a *primary list* and an *extended list*. The primary list is the first screen that's displayed when you execute the SETARL command; the extended list is an optional list that can contain up to five StreetTalk names.

The primary list contains three categories of users to whom access rights can be assigned; these are the Owner, the Group, and the World.



The Owner controls the access rights list for the file service, directory, or file. Anyone on the AdminList can change the StreetTalk name of the owner, but there must be a single StreetTalk name listed as Owner -- not a list, not a pattern. In addition, the Owner field cannot be left blank, nor can the Control rights by taken away (by placing a "-" under the "C" column). However, all other rights can be taken away.

- When you create a new VINES 5.5 file service, your AdminID will be in the Owner field.
- When you upgrade from VINES 4.11, the Owner field will display the name of the file service itself.

Regardless of whether the file service is new or has just been upgraded from 4.11, the Owner field has all rights across the top line (more on the meaning of the rights later). However, anyone on the AdminList for the file service can change the name of the Owner and the access rights settings for the Owner, within the constraints mentioned above. (See *Setting Access Rights* later in this document for more information.)

The Group category represents the rights a specified group will have.

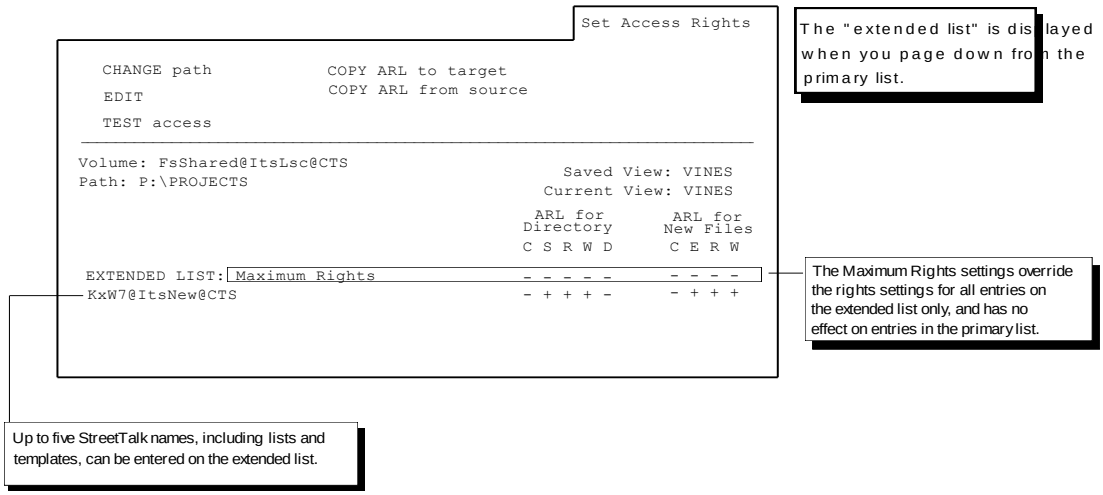
- When you create a new VINES 5.5 file service, the group name (pattern) that matches your AdminID's group@org will be displayed in this field.
- When you upgrade from VINES 4.11, the Group field will be displayed as -- literally -- <any group>.

Regardless of whether the file service is new or has just been upgraded, by default the Group field has no rights at all, as noted by the series of "-" under the Directory and New File ARL column headings. However, the name of the group and the rights assigned to the

Group can be changed by anyone on the AdminList for the service. (See *Setting Access Rights* later in this document for more information.

The World category represents any other users; the designation for this field cannot be changed from *@*@*, but the rights that you give to this category can be loosened up if you like: By default, the World category has no privileges at all, as noted by the row of "-".

Paging down from the primary list will display the extended list, which can contain up to five StreetTalk entries. User names, lists, and patterns are all allowed on this list; Banyan recommends entering patterns for best performance.



- When you create a new VINES 5.5 file service, the extended list will be empty.
- When you upgrade from VINES 4.11, the extended list will contain the names of your ARLs as they were configured on 4.11.

The extended list always displays an entry labeled "Maximum Rights," which is a masking feature to temporarily override the rights for any and all entries on the extended list. For example, if you have five StreetTalk names or groups on the extended list with various levels of access, but you're moving files around on the service and you don't want people accessing documents while you're in the process (to prevent version control problems) you can lock everyone on the extended list out by simply changing the Maximum Rights line to all "-" across the line. When you're through moving files around, you can change the Maximum Rights line back to what it had been.

The Maximum Rights settings have no effect on the primary list entries, so if the extended list is empty, the maximum rights settings are meaningless.

Checking Order

When a user tries to access a network drive or change directories on a network drive, VINES checks the UserID against all entries in both the primary and extended lists, in this order:

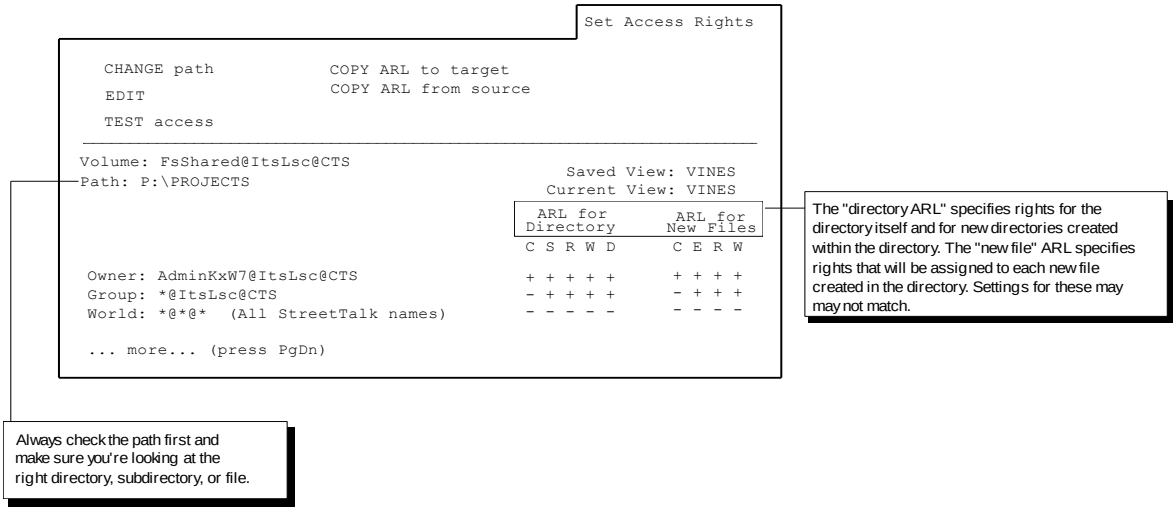
Primary List	Extended List
1. Owner	2. Individual StreetTalk name
3. Group list	4. Group pattern (*@group@org) or
	5. Organization pattern (*@*@org)
6. World	

If a user is a member of the Group or the World, but is also specifically listed by UserID or is a member of a group or list on the extended list, then that user will have the rights assigned on the extended list. For example, your AdminID may be listed on the extended list as AdminID@ItsLsc@CTS with complete access rights, while the group pattern *@ItsLsc@CTS is listed on the primary list as Group without any rights. Although you're a member of the group, VINES finds your name on the extended list before it sees it as part of the group on the primary list, and assigns you the rights listed on the extended list.

On the other hand, the Owner's rights on the primary list always take precedence over any rights that the owner may have as a member of a list or group on the extended list. For example, if your AdminID is listed on the primary list as the Owner with only "C" access rights -- you can only change the ARL -- and your group name is listed on the extended list as the group pattern *@ItsLsc@CTS, your rights when you login using your AdminID will be limited to the rights specified for the Owner.

Directory, New File, and File ARLs

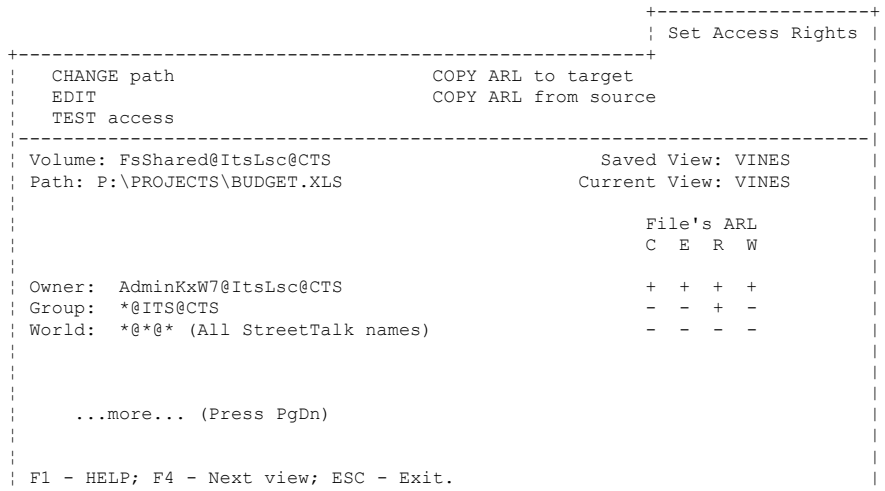
The primary and secondary list each contain two ARLs: the *directory* ARL specifies access rights for the directory itself and for new subdirectories created within the directory; the *new file* ARL specifies the rights for each new file created in that directory.



You can execute SETARL from the directory whose ARL you want to view, or you change paths within the SETARL program to display the ARLs for directories, subdirectories, and files that are nested below the root -- presuming you have access rights to do so. As system administrator, you should create subdirectories for users or groups as needed, and set the ARLs for the subdirectories so that users can access the files they need (see *Setting Access Rights* for recommendations).

After a file is created in a subdirectory, its ARL can be viewed and changed independently of the directory ARL. In addition, editing the directory ARL or the new file ARL will have no effect on the file ARLs of existing files.

For example, you may give a group complete access to a directory and new files, but you could single out selected files within the directory and set the file ARL for Read only access:



Access Rights

Each access right in VINES 5.5 must be explicitly set. An access right level is granted by placing a "+" under the column heading for the right, and not granted by placing a "-" under the column heading. Here are the five different access rights levels that can be applied to a directory, and what they'll let a user who has them do:

C	Control	Change the directory ARL, including changing the Owner and the Group. This right cannot be taken away from the Owner.
S	Search	Search for all the file and directory names in a directory. Access the attributes of the directory and the files and subdirectories in it.
R	Read	Read subdirectory and file names in a directory.
W	Write	Create, rename, and change the attributes of subdirectories and files within a directory.
D	Delete	Delete subdirectories and files from the the directory.

Here are the four different access rights levels that can be applied to a file, and what they'll let a user who has them do:

C	Control	Change the file ARL, including changing the Owner and the Group. This right cannot be taken away from the Owner.
E	Execute	Enables executable file to run its program.
R	Read	Open a file for reading only. Requires Write access to the file and Read access to the parent directory in order to save, delete, or make changes to the file.
W	Write	Open a file for writing. Requires file Read access to open the file. File can be saved with or without changes.

The Search and Read directory rights are needed for virtually all other levels of access. For example, in order to open a file with Read rights, all parent directories must have Search and Read rights. If a directory has Read rights but not Search rights, you'll be able to look at a directory listing of the directory, but you won't be able to change to any subdirectories. If a directory has Search rights but not Read rights, you won't be able to see a directory, but you will be able to change directories (as long as you know the name of the subdirectory that you want to change to).

See *Default ARLs and Recommended Settings* for more details about how to configure file services, directories, and files.

Default ARLs and Recommended Settings

The default settings for an ARL depend upon whether the server was upgraded from VINES 4.11 or is a newly created VINES 5.5 file service; in either case you may want to change the default settings. Here are some general guidelines for creating file services at PG&E:

- Create a different file service for each network drive that you want to establish for your users, rather than creating a single file service with multiple subdirectories branching off the root. Multiple file services are preferable for many reasons, including easier restoration of files.

- Set the ARL in the root directory for Read and Search access so that users will have access to their subdirectories.

- Create subdirectories as needed for different users and groups, and provide access accordingly.

When a new file or directory is created, the names and access rights will be copied from the root directory ARL to the ARL of the new file or directory, according to VINES inheritance rules. VINES inheritance rules also dictate that new subdirectories inherit both the directory and new file ARLs of the parent directory, and that new files inherit access rights according to the parent directory's new file ARL.

Mac inheritance rules are different, and are discussed in *VINES and Mac ARLs Compared*. Nonetheless, the recommended setting for all file services, even those storing Mac files, is to follow VINES rights and inheritance rules for ease of administration.

New File Services

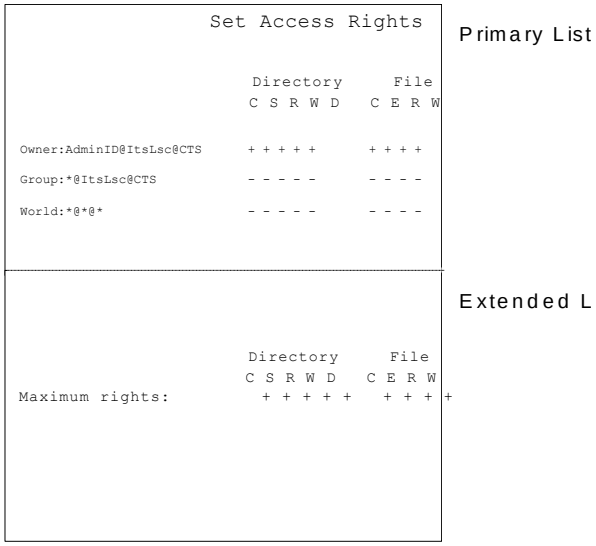
When you login using your AdminID and create a VINES 5.5 file service, the root directory's default ARL will show:

- Your AdminID as the Owner, with all rights on both the directory and new file ARLs;

- Your AdminID's group will be specified as the Group and have no rights;

- The World (*@*@*) will have no rights.

- The extended list will be empty:



After creating a new file service in VINES 5.5, you can go immediately to the VINES File Utility menu and set the ARLs by selecting MANAGE Files. In order for users to see any subdirectories you create for them on this file service, they'll at least need Search and Read rights, so you should give them those rights.

If more than one group will be accessing this file service, you'll also need to add the other group names to the extended list. If groups in an entire organization will need access, you can change the Group on the primary list to include all groups in an organization (*@*@org).

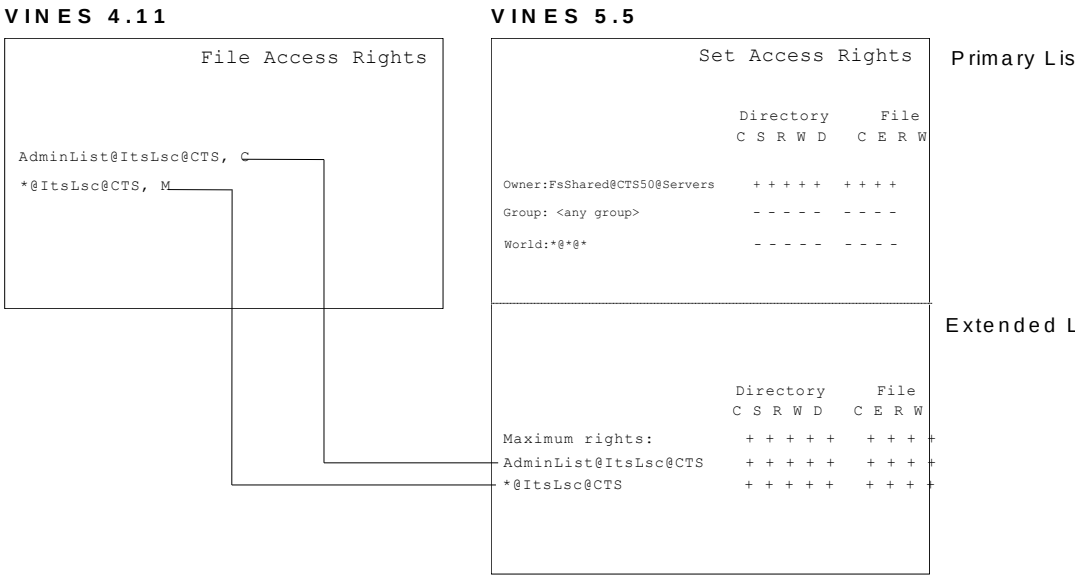
When editing the field names on the ARL screens, note that you can only use a wildcard character (*) as a placeholder for the entire item field or for both the item and group field. For example:

*@group@org
@@org

ARLs After Upgrading from VINES 4.11

When you upgrade a server from VINES 4.11 to VINES 5.5, the root directory's default ARL will show:

- The StreetTalk name of the file service as the Owner, with all rights on both the directory and new file ARLs;
- The file service's group will be specified as the Group and have no rights;
- The World (*@*@*) will have no rights.
- The extended list will contain will contain all your 4.11 ARLs with the comparable rights specified under the VINES 5.5 settings. For example, if your AdminID was on the VINES 4.11 ARL with Control rights, your AdminID will be listed on the extended list with all rights selected.



Because of the way the primary and extended lists are checked, the net result of the migration is that you'll still have the same rights as you did before, as will users. Nonetheless, you might consider changing the ARL in this manner:

- Put your AdminID on the ARL as Owner.
- Change the Group to the name of the group that actually mostly uses the service or directory. (This name will probably be on the extended list.)
- Leave rights to the World alone, or set the access that you would like everyone in the company to have.
- Delete your AdminID from the extended list once you're established as the Owner.
- Delete the group from the extended list after moving to the primary list as Group.

Interoperability between VINES 4.11 and VINES 5.5 ARLs

If you're managing both VINES 4.11 and VINES 5.5 file services, here are some things to keep in mind.

- Be sure to login from a VINES 5.5 workstation to set the ARLs on a VINES 5.5 file service. You won't be able to set ARLs on a VINES 5.5 file service from a VINES 4.11 workstation; instead, you'll get `***Error code 14***`.

- If you're logged in from a VINES 5.5 workstation and try to set ARLs on a VINES 4.11 file service, you'll get the 4.11 SETARL menu. If you test your access, you'll see the message `No access entries apply -- user has no access`. Despite this message, you can change the ARLs if you're on the AdminList for the file service.

Recommended Settings for ARLs

In VINES 5.5, each access right must be set explicitly; that is, the access rights are not cumulative as they were in VINES 4.11. For example, VINES 4.11 Control access provides complete access to the ARL and the directory, including the ability to read and write files contained there as well as change the ARL, but the VINES 5.5 Control right only provides the ability to change the ARL itself.

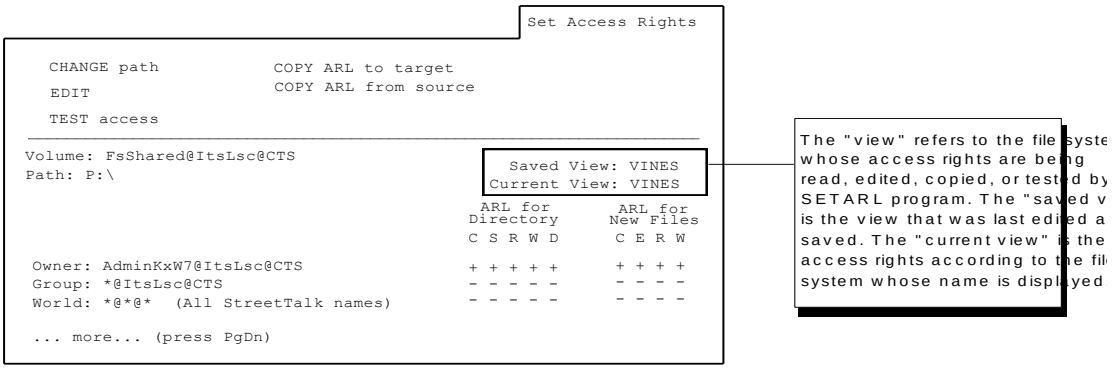
To achieve rights comparable to VINES 4.11 Control rights, you must select all the rights under the directory column heading -- control, search, read, write, and delete -- and all the rights under the new file ARL -- control, execute, read, and write. Other recommended settings for standard levels of file and directory security are summarized in the chart below:

	Directory					File			
	C	S	R	W	D	C	E	R	W
Read only	-	+	+	-	-	-	-	+	-
Read only, but can save as new file	-	+	+	+	-	-	-	+	+
Can open and modify files	-	+	+	+	+	-	-	+	+
Execute only	-	+	+	-	-	-	+	-	-
Equivalent to VINES 4.11 "modify"	-	+	+	+	+	-	+	+	+
Equivalent to VINES 4.11 "control"	+	+	+	+	+	+	+	+	+

VINES and Mac ARLs Compared

Access rights settings can adhere to either VINES or Mac rules. The *view* refers to the name of the file system whose access rights are being read, edited, copied, or tested by the SETARL program. The *saved view* is the view that was last edited and saved, while the current view is what is displayed on the screen.

ARLs must be restored from the same view in which they were set so that they'll be interpreted in the same way -- another reason that the last saved view is important.



Although you can save ARLs for Mac files under the Mac's own filing system, it's recommended that the VINES view be used exclusively at PG&E for consistency. If you choose not to follow this guideline, remember that user access to files and directories will be different for Mac users than for DOS workstation users: the Mac user's access rights will follow the guidelines used by AppleShare rights.

User access to directories and files is determined by the rights granted in the saved view. Because the VINES file system and the Mac file system check the ARLs in a different order, it's important to pay attention to the saved view.

When verifying access, AppleShare compares the user name against the Owner, Group, and World fields. If the user name matches two or three fields, then the user has a combination of the access rights granted to those named in the fields.

In order to follow the Mac rules, change the *view* on the Set Access Rights screen to "Mac" (by default, the views are always VINES).

Saved Views Determine Checking Order

If you save under the VINES view, the user will be granted access based on the first match found between a user name and the ARL.

If you save under the Mac view, the user will be granted access based on the combined access rights of whatever the user name matches.

Inheritance Rules

The VINES and Mac file systems have different rules regarding how access rights are applied to new files and folders. VINES rules dictate that:

- new files inherit access rights according to the parent directory's new file ARL
- new subdirectories inherit both the directory and new file ARLs of the parent
- when a new file or directory is created, the names and access rights in both the primary and extended lists are copied to the ARL of the new file or directory

Mac rules, on the other hand, dictate that new folders belong to the creator, so if the creator is not the owner of the parent folder, the new folder will inherit the access privileges of the parent. In other words, the owner of the new folder is the creator of the folder under Mac rules, while under VINES rules, the owner of the new folder is always the owner of the parent folder.

Only in the Mac view are you given the option of selecting Mac or VINES inheritance rules. (By default folders and files created from a Mac inherit by Mac rules.)

You can change the inheritance rules independently from the view in which you save an ARL. To do so,

- Display the Mac view
- Change the inheritance rules
- Return to the VINES view
- Press <F10> to save the ARL

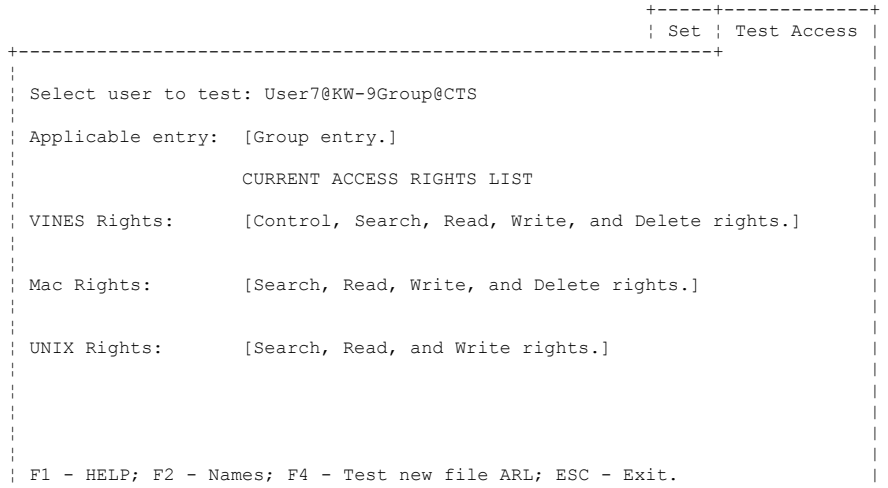
Recommendations

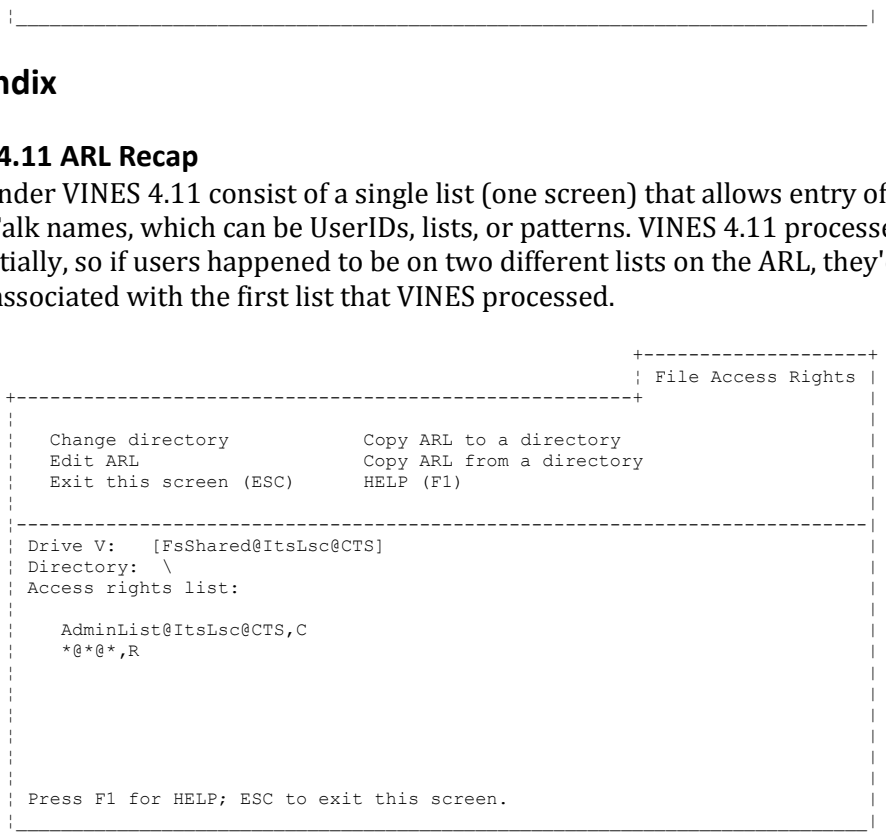
- Keep VINES inheritance rules to maintain control over files and subdirectories, regardless of the file type.

- Add the line VIEWS = V to the profiles of Mac users so that their file access will be governed by VINES rules; if the Mac user tries to change to the Mac view, he or she will get an error message.

- Mac users should set "Inherit Using VINES Rules" option to Yes

By default, this option is set to No. Set to Yes to simplify using ARLs for Mac clients and to save disk space. With this setting, subdirectories will be automatically assigned the same ARL as the parent directory -- under Mac rules, the directory would be assigned the user's default ARL and the user would be forced to change the ARL.





Appendix

VINES 4.11 ARL Recap

ARLs under VINES 4.11 consist of a single list (one screen) that allows entry of up to five StreetTalk names, which can be UserIDs, lists, or patterns. VINES 4.11 processes the ARL sequentially, so if users happened to be on two different lists on the ARL, they'd have the rights associated with the first list that VINES processed.

The access rights themselves provide four different levels of access to the directory or subdirectory, from no access at all to a level that includes the ability to change the setting. Note that each level includes the rights of the level before it, so these rights are said to be cumulative:

Null	User has no access
Read	User can read, copy, and execute files in the directory
Modify	User can read, copy, and execute files in the directory; plus can add, modify, or delete files, and create subdirectories
Control	User can read, copy, execute, add, modify, delete files; create subdirectories; plus can change the ARL

Each created subdirectory inherits the access rights of its parent subdirectory. Modifying the parent ARL does not affect the subdirectory's ARL. The default ARL for the root directory of a newly created VINES 4.11 file service provides:

- Control rights to the AdminList@Group@Org of the file service, (presuming you had logged in using your AdminID from the AdminList for the file service); and
- Modify rights to all members of the Group@Org of the same name as the AdminList.

The following recommendations are for file services and ARLs under VINES 4.11 at PG&E:

- Don't let users write in the root directory of any file service; create directories and subdirectories for groups and users.
- Set the ARL in the root directory for Read access so that users will have access to their subdirectories.

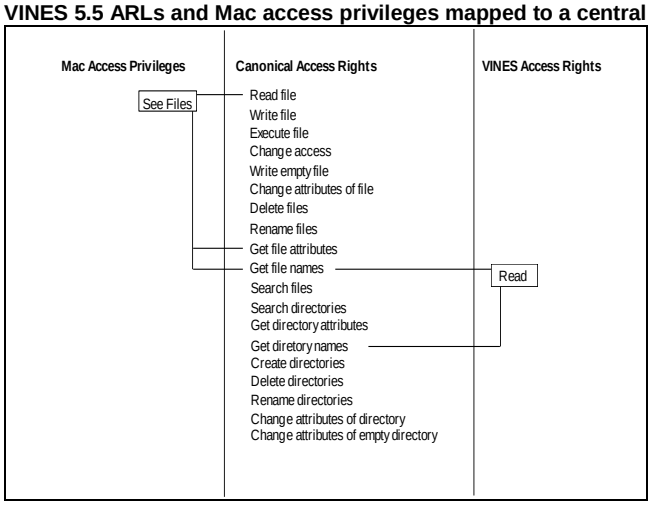
- Leave the ARL for the VINES Files subdirectory set to the default *@*@*, R, to prevent users from deleting files from the subdirectory or copying files to the subdirectory. Such a setting also prevents viruses from corrupting your VINES files.

How VINES 5.5 ARLs Work

The VINES ARL scheme that originated in VINES 386[?] was developed by Banyan to provide a security scheme for DOS, and later for OS/2 files, because those file systems do not have their own security system for storing files on network drives. On the other hand, the Mac and Unix operating systems do have their own security systems for network files. In order for Banyan to accomodate the VINES ARL scheme and these other access rights schemes in a shared, cross-platform network environment, the file system and the ARL scheme had to be completely redesigned in VINES 5.5.

Here's basically how it works: When access rights are set through one client interface, behind the scenes VFS stores the corresponding set of *canonical* rights. Something in its canonical form is said to be in its simplest form; Banyan's canonical rights scheme reduces all the sets of different native rights into a number of more specific rights.

VINES 5.5 ARLs and Mac access privileges mapped to a central "database" of canonical access rights



Mac Access Rights

Mac access rights -- called Access Privileges -- can be assigned to three classes of file users: the *Owner* of the file; the *Group* of users to which the owner belongs; and *Everyone* else. The three access privileges that can be set for each of these classes are:

See Files	User can see files (but not folders) within a folder Read the files contents Read the files attributes
See Folders	User can see folders (but not individual files)
Make Changes	User can add a file to a folder but cannot see the file

Make Changes and See Files together enable the user to create, delete, write, and rename files.

Unix Access Rights

Unix access rights can be assigned to three classes of file users: the *Owner* of the file; a specified *Group* of users; and the rest of the *World.* The three file permissions that can be set on either directories or files are:

Read	User can read a file or directory
Write	User can write a file or modify a directory by adding or removing files
Execute	User can execute a file or use a directory in a pathname