MAE 2.0: AppleTalk Access Privileges (3/95)

Article Created: 16 March 1995

TOPIC -----

This article describes AppleTalk access privileges and UNIX permissions when sharing files (directories) under Macintosh Application Environment (MAE) 2.0.

DISCUSSION -----

When you share a folder or a disk, by default anyone on the network can open it, read it, or change it. However, you can set access privileges to files and folders you own (that is, those that you have created or whose ownership has been transferred to you) to specify who can use your shared items. You can also allow access to guest users; see "Naming Specific Users," later in this section.

There are three types of FileShare access privileges:

• See Folders: You can open the folder.

• See Files: You can open any file within the folder.

• Make Changes: You can change the contents of any file within the folder.

IMPORTANT: When MAE users export part of a UNIX file system via file sharing, they can grant FileShare access only to the extent that the UNIX permissions allow them that access. For example, if an MAE user does not have write access to a file, the user cannot export that file with FileShare write access. Thus, the privileges another user has when accessing files are the most restrictive combination of the UNIX permissions and the file sharing privileges.

Differences between UNIX and Macintosh access permissions

The differences between UNIX permissions and Macintosh file-sharing privileges can be summarized as follows:

• Macintosh file-sharing privileges affect file sharing over AppleTalk. UNIX permissions affect permissions across all UNIX networks.

• All files and folders (directories) created within UNIX are assigned default UNIX permissions automatically. Folders and their contents are assigned Macintosh file-sharing permissions only if the owner of the folder has made the

folder available to others.

• UNIX permits the owner to assign different permissions to every item within a directory; Macintosh file sharing allows the owner to set privileges for the folder. These privileges are transferred to all the contents of the folder collectively.

• In most cases, a user should not share the root directory without careful configuration of access privileges. For example, sharing the root directory with read-only permission allows remote users to view files such as /etc/passwd. Users should be especially cautious when sharing folders on NFS volumes via file sharing.

The following table shows UNIX permissions compared with file sharing privileges:

If UNIX permissions are			Then file sharing privileges are	
Read	Write	Execute	See Folders and See Files	Make Changes
----	-----	-------	-------------	-------
No	No	No	No	No
No	No	Yes	No	No
No	Yes	No	No	Yes
No	Yes	Yes	No	Yes
Yes	No	No	No	No
Yes	No	Yes	Yes	No
Yes	Yes	No	No	Yes
Yes	Yes	Yes	Yes	Yes

Support Information Services

Keywords: supt,knts

==========

19960215 11:05:19.00
Tech Info Library Article Number: 17375