8.11.3 Special Permission Facts

This lesson covers the following topics:

- About special permissions
- Managing special permissions

About Special Permissions

Be aware of the following special permissions:

Permission	Letter Abbreviation	Example	Octal Value	Description
SUID (Set User ID)	**s** in the execute permission position of the user permissions	rw**s**rw-rw-	4	If the SUID bit is set, the program will run with the permissions of the file owner, not with the permissions of the user who runs the program. • The most common use of SUID is to allow users to run a command as the root user. • Users do not become the root user, but rather the command or program runs as if executed by the root user. • Some programs require the SUID bit set for proper functionality. • Be careful in setting the SUID bit as it could give a program too many permissions.
SGID (Set Group ID)	**s** in the execute permission position of the group permissions	rwxrw**s**rw-	2	If the SGID bit is set: • On a file, the program will run with the group permissions of the group owner. • On a directory, a newly created file will receive/inherit the same group owner as assigned to the parent directory.

Sticky bit	**t** in the execute permission position of the other permissions	rwxrw-rw**t**	1	This marks the file in such a way as to prevent the file's deletion from the system by anyone except the file owner. Setting the sticky bit works particularly well with shared files. Sticky bits can also be set on directories.

Managing Special Permissions

Use the following commands when managing special permissions:

Command	Description	Example
ls -l	Displays a long file listing. A long file listing shows the permissions for the files (among other information).	**drwsr-xr-x** 22 root root 4096 Jun 19 15:01 sales (This is a script with 4755 as its mode and has the SUID set.)

chmod	Assigns a special permission. Be aware of the following syntax options:
	• ***[decimal_value]*** sets the permissions for the file according to the numbers represented for each mode category.
	  ◦ The special permission *precedes* the standard octal representation of a set of permissions.
	  ◦ Only the *first* number changes to identify the special permission group settings.
	• ***[category]+[permission]*** adds a special permission for a user, group, or other (category) to a file.
	• ***[category]-[permission]*** removes a special permission for a user, group, or other from a file.
		chmod 4*xxx* sets the SUID.
		chmod u+s sets the SUID.
		chmod u-s removes the SUID.
		chmod 2*xxx* sets the SGID.
		chmod g+s sets the SGID.
		chmod 1*xxx* sets the sticky bit.
		chmod u+t sets the sticky bit.
		chmod u-t removes the sticky bit.
		chmod 6*xxx* sets both the SUID and SGID.
		chmod 7*xxx* sets the SUID, GUID, and sticky bit.