Router and Switch File Maintenance

TEXT

Router File Systems

If you are thinking that you cannot possibly remember how you configured every device in your network, you are not alone. In a large network, it would not be possible to keep track of every configuration change. Particularly when you are using a tool(s) to update your configurations, we have simply pushed them to. To do this, you will need to know how to view and manage your file systems.

The Cisco IOS file system (IFS) allows the administrator to navigate to different directories and list the files in a directory. The administrator can also create subdirectories in flash memory or on a disk. The directories available depend on the device.

The example displays the output of the **show file systems** command, which lists all of the available file systems on a Cisco 4221 router.

```
Router# show file systems
File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
       -           -        opaque   rw   system:
       -           -        opaque   rw   tftp:
 7516192768  7509491251     disk   rw   flash:  flash:0
 2684354560  2167197696     disk   rw   usb0:
 2684354560  2167196672     disk   rw   usb1:
       -           -        opaque   rw   null:
       -           -        opaque   rw   tar:
       -           -        network  rw   rcp:
       -           -        network  rw   http:
       -           -        network  rw   scp:
       -           -        network  rw   https:
       -           -        network  rw   ftp:
       -           -        network  rw   sftp:
       -           -        network  rw   ftpi:
       -           -        network  rw   sftpi:
       -           -        opaque   rw   ram:
Router#
```

The command provides useful information such as the amount of total and free memory, the type of file system, and its permissions. Permissions include read only (ro), write only (wo), and read and write (rw). The prefixes are the keywords that are used to specify a file system.

Although there are several file systems listed, all of interest to us will be the flash, usb0 and usb1 file systems.

Notice that the flash file system also has an asterisk preceding it. This indicates that flash is the current default file system. The bootable IOS is located in flash. Therefore, the secure version (IS) is expected to be flash listing, indicating that it is bootable disk.

The Flash File System

The command displays the output from the **dir** command (extended command).

```
Router# dir
Directory of flash:/  doorflash:
  1  drwx   16384  Jan 1 2037 00:00:00 +00:00  lost+found
 11  drwx    4096  Jan 1 2037 00:00:00 +00:00  dmi
 12  drwx    4096  Jan 1 2037 00:00:00 +00:00  crash
 13  drwx    4096  Aug 2 2023 00:12:00 +00:00  core
 14  drwx    4096  Jan 1 2037 00:00:00 +00:00  boot
 489  drwx   4096  Aug 2 2023 00:12:00 +00:00  _custom_conf
 490  drwx   4096  Aug 2 2023 00:12:00 +00:00  _iox_conf
 491  drwx   4096  Aug 2 2023 00:12:00 +00:00  gs_script
 492  drwx   4096  Aug 2 2023 00:12:00 +00:00  vdisk_conf
 493  drwx   4096  Aug 2 2023 00:12:00 +00:00  vnfd_conf
 494  drwx   4096  Aug 2 2023 00:12:00 +00:00  iox_partition_conf
 495  drwx   4096  Aug 2 2023 00:12:00 +00:00  throughput_monitor_params
 496  drwx   4096  Jan 1 2037 00:00:00 +00:00  tftpboot
 497  drwx   4096  Jan 1 2037 00:00:00 +00:00  ldap_cacert_dir
 11038976  drwx   4096  Aug 30 2023 17:48:31 +00:00  ucmscripts
 11039488  drwx   4096  Jan 1 2037 00:00:00 +00:00  trustpool
 11039744  drwx   4096  Jan 1 2037 00:00:00 +00:00  trustpool_backup
 11040000  drwx   4096  Jan 1 2037 00:00:00 +00:00  ssa_comm
 11040256  drwx   4096  Aug 30 2023 17:48:31 +00:00  dhcp
 11040512  drwx   4096  Aug 30 2023 17:48:31 +00:00  activelog
 11040768  drwx   4096  Aug 30 2023 17:48:31 +00:00  netdump
 11041024  drwx   4096  Aug 30 2023 17:48:31 +00:00  cdr_char
 11041280  drwx   4096  Aug 30 2023 17:48:31 +00:00  cdr_repository
 11041536  drwx   4096  Aug 30 2023 17:48:31 +00:00  cm/bin
 11041792  drwx   4096  Aug 30 2023 17:48:31 +00:00  cfg
 11042304  drwx   4096  Aug 30 2023 17:48:31 +00:00  images
 11042560  drwx   4096  Aug 30 2023 17:48:31 +00:00  install
 11042816  drwx   4096  Aug 30 2023 17:48:31 +00:00  huronfw
 11043328  drwx   4096  Aug 30 2023 17:48:31 +00:00  drf
 11043584  drwx   4096  Aug 30 2023 17:48:31 +00:00  osl
 11043840  drwx   4096  Aug 30 2023 17:48:31 +00:00  setup
 11044352  drwx   4096  Aug 30 2023 17:48:31 +00:00  cdp
 11044608  drwx   4096  Aug 30 2023 17:48:31 +00:00  snmp
 11044864  drwx   4096  Aug 30 2023 17:48:31 +00:00  cores
 11045120  drwx   4096  Aug 30 2023 17:48:31 +00:00  spool
 11045376  drwx   4096  Aug 30 2023 17:48:31 +00:00  db
 11045632  drwx   4096  Aug 30 2023 17:48:31 +00:00  solr
 11045888  drwx   4096  Aug 30 2023 17:48:31 +00:00  tomcat
 11046144  drwx   4096  Aug 30 2023 17:48:31 +00:00  sdl
 11046400  drwx   4096  Aug 30 2023 17:48:31 +00:00  sdr
 11046656  drwx   4096  Aug 30 2023 17:48:31 +00:00  characters
 11046912  drwx   4096  Aug 30 2023 17:48:31 +00:00  commprov
 11047168  drwx   4096  Aug 30 2023 17:48:31 +00:00  root
 11047424  drwx   4096  Aug 30 2023 17:48:31 +00:00  cdm
 11047680  drwx   4096  Aug 30 2023 17:48:31 +00:00  tftp
 11047936  drwx   4096  Aug 30 2023 17:48:31 +00:00  RTMTReports
 11048192  drwx   4096  Aug 30 2023 17:48:31 +00:00  ipsec
 11048448  drwx   4096  Aug 30 2023 17:48:31 +00:00  platform
Router#
```

Because flash is the default file system, the **dir** command lists the contents of flash. Several files are located in flash, but of specific interest is the last listing. This is the name of the current Cisco IOS file image that is running in RAM.

The NVRAM File System

To view the contents of NVRAM, you must change the current default file system by using the **cd** (change directory) command, as shown in the example.

```
Router#
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/  startup-config
  542  -rw-   3253                    startup-config
  543  ---    5684                    private-config
  544  -rw-     74                    underlying-config
  545  -rw-   2035                    private-config.1
  546  ---    5684                    private-config.2
  547  -rw-     81                    persistent-data
  548  -rw-    127                    ecfm_ma_db_v1_0_0
  549  -rw-     17                    ecfm_lock_info
  550  -rw-    128                    persistent-data.1
  551  -rw-     17                    ecfm_lock_info.1
  552  -rw-    128                    IOS-Self-Config-age
  553  -rw-   3253                    IOS-Self-Config-age.1
[262144 bytes total (233488896 bytes free)]
Router#
```

Any persistent startup directory contents is **-rw-**. The command confirms that we are viewing the NVRAM directory. Finally, the **dir** command lists the contents of NVRAM. Although there are several configuration files listed, of specific interest is the startup-configuration file.

TEXT

Switch File Systems

With the Cisco 2960 switch flash file system, you can copy configuration files, and archive (upload and download) software images.

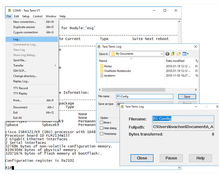
The command to view the file systems on a Catalyst switch is the same as on a Cisco router, **show file systems**, as displayed in the example.

```
Switch# show file systems
File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
  - 63963136    62881792     flash   rw   flash:  flash:0
       -           -        opaque   rw   system:
       -           -        opaque   rw   tftp:
       -           -        opaque   rw   flash:
       -           -        opaque   rw   mdisk:
    65536       65027       opaque   rw   vfat:
       -           -        opaque   rw   nvram:
       -           -        opaque   rw   cns:
       -           -        opaque   rw   null:
       -           -        opaque   rw   system:
       -           -        network  rw   rcp:
       -           -        network  rw   http:
       -           -        network  rw   scp:
       -           -        network  rw   https:
       -           -        network  rw   ftp:
       -           -        network  rw   sftp:
       -           -        network  rw   ftpi:
       -           -        network  rw   sftpi:
       -           -        opaque   rw   ram:
Switch#
```

TEXT

Use a Text File to Back Up a Configuration

Configuration files can be saved to a text file by using Tera Term, as shown in the figure.



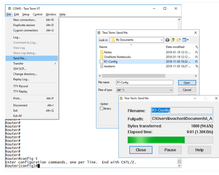
Step 1: On the File menu, click **Log**.
Step 2: Browse the folder location and filename to save the file and click **Save**. Tera Term will open **Tera Term: Log** window and will now capture all command and output from the switch console.
Step 3: To capture the current configuration, enter the **show running-config** command (privilege level 15 required). The text displayed in the terminal window will be saved to the specified log file.
Step 4: When the capture is complete, select **Close** in the Tera Term: Log window.
Step 5: Open the file to verify that the configuration was captured properly and not corrupt.

TEXT

Use a Text File to Restore a Configuration

A configuration can be copied from a file and then directly pasted to a device. The IOS executes each line of the configuration text as a command. This means that the file will require editing to ensure that encrypted passwords are in plaintext, and that non-command text such as **--More--** and IOS messages are removed. In addition, it may be necessary to add the **no shutdown** command to the beginning of the file or enter global configuration mode before pasting the configuration. This process is discussed in the last slide in this topic.

Instead of copying and pasting, a configuration can be restored from a text file by using Tera Term, as shown in the figure.



When using Tera Term, the steps are as follows:

Step 1: On the File menu, click **Send file**.
Step 2: Locate the file to be copied into the device and click **Open**.
Step 3: Tera Term will paste the file into the device.

The text in the file will be applied as commands in the CLI and become the running configuration on the device.

TEXT

Use TFTP to Back Up and Restore a Configuration

Use TFTP to Back Up a Configuration

Copies of configuration files should be stored as backup files in the event of a problem. Configuration files can be stored on a Trivial File Transfer Protocol (TFTP) server, or a USB drive. A configuration file should also be included in the network documentation.

To back the running configuration or the startup configuration to a TFTP server, use either the **copy running-config tftp** or **copy startup-config tftp** command, as shown in the example.

```
Router#copy running-config tftp
Address or name of remote host [255.255.255.255]?
Name of the configuration file to write on tftp host? rtr-new-2023
Write file rtr-new-2023 on host 255.255.255.255?[confirm]
!!!
```