CCNA ASSIGNMENT 4

Q.1 List of IP services Types and Example of HSRP?

ANS. 1. The Client/Server Model

2. Telnet

3. File Transfer Protocol (FTP)

4. Trivial File Transfer Protocol (TFTP)

5. Simple Mail Transfer Protocol (SMTP)

6. Network File System (NFS)

7. Simple Network Management Protocol (SNMP)

8. Domain Name System (DNS)

HOT STANDBY ROUTING PROTOCOL (HSRP)

Active Gateway Election.

Preemption.

Authentication.

HSRP Timers.

HSRP Version 1 and 2.

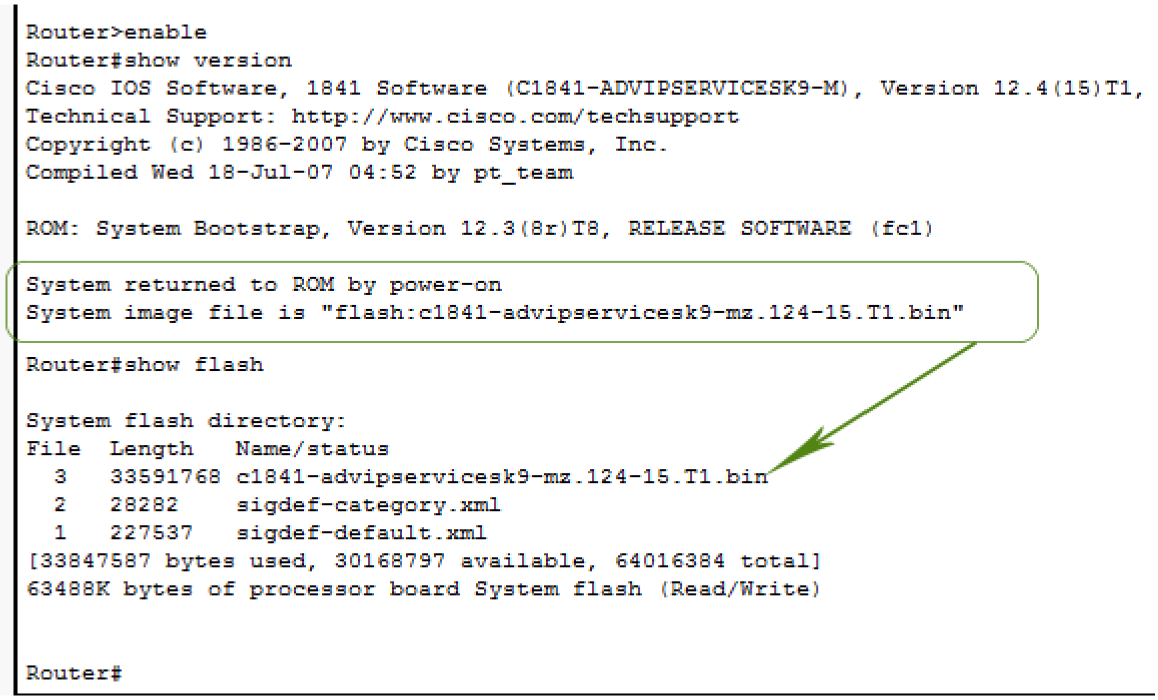
Object (Interface) Tracking.

The Hot Standby Router Protocol (HSRP) is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. HSRP provides high network availability, because it routes IP traffic from hosts on networks without relying on the availability of any single router.

Q.2 Example of Backup and restore Router managing IOS?

ANS. Access the privileged-exec mode of the router and run the 'show version' command. From the output, note down the name of the IOS file.

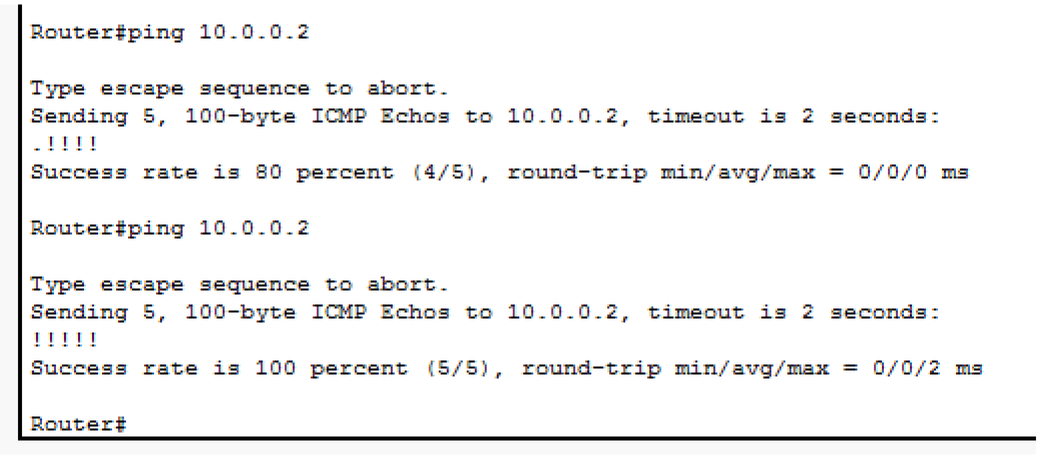
Run the 'show flash' command and note down the name of all available IOS image files.



```
Router>enable
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

Router#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1841-advipservicesk9-mz.124-15.T1.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)


Router#
```

To check and verify the connectivity between the router and the TFTP server, use the following command.

Router#ping 10.0.0.2



```
Router#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

Router#ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

Router#
```

To take the backup of the current or existing IOS image file, use the following command from the privileged-exec mode.

Router#copy flash tftp

This command needs three arguments.

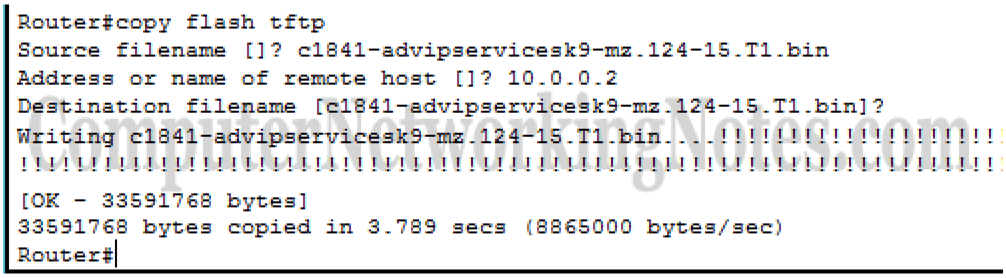
Source filename: - Specify the name of the IOS image file that you want to back up from the Flash memory to the TFTP server.

Address or name of remote host: - Type the IP address of the TFTP Server.

Destination filename: - If you want to store the IOS image file with a different name at the TFTP server, specify that name. To use the same name, press the Enter key.

TFTP protocol copies the specified IOS image file on the root directory of the TFTP server. It also prints the real-time progress of the copy operation.

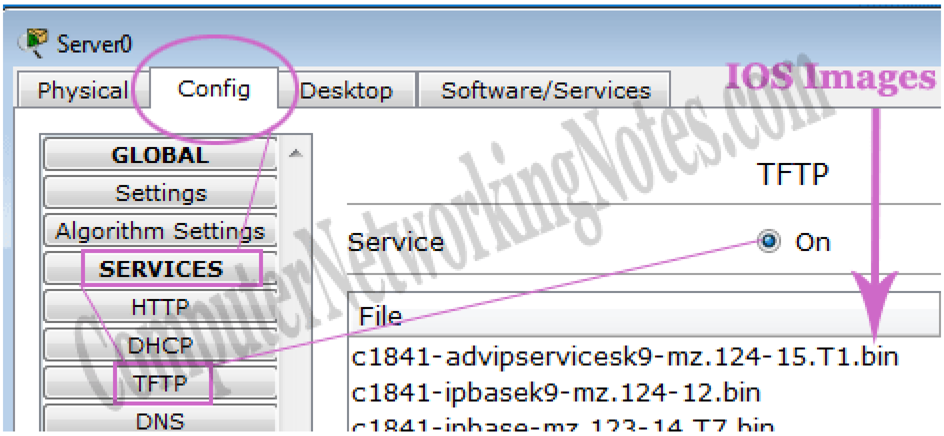
The following image shows the output of the above command with arguments.



```
Router#copy flash tftp
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 10.0.0.2
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Writing c1841-advipservicesk9-mz.124-15.T1.bin...!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 33591768 bytes]
33591768 bytes copied in 3.789 secs (8865000 bytes/sec)
Router#
```

To verify that the IOS image file has been successfully backed up, click the Server and click the config tab and expand the Services tab from the left menu. In the file section of the right pane, you can see the copied IOS image file.

The following image shows the above steps with the sample output.



TFTP

Service ● On

File
c1841-advipservicesk9-mz.124-15.T1.bin
c1841-ipbasek9-mz.124-12.bin
c1841-ipbase-mz.123-14.T7.bin

Suppose that the IOS image file stored in the flash memory is accidentally or intentionally deleted. If a functional IOS image file is not available, the router does not start. To simulate this situation, you can delete the IOS image file from the flash memory.

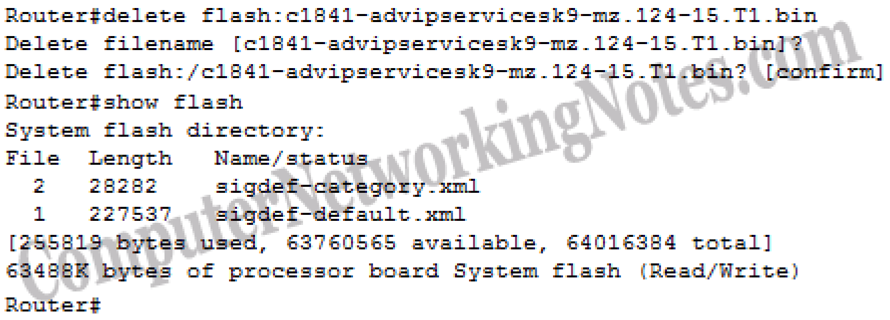
To delete the IOS image file from the flash memory, use the following command from the privileged-exec mode.

Router#delete:[IOS File Name]

To confirm the delete operation, press the 'Enter' key when it prompts.

To verify that the file has been successfully deleted, you can use the 'show flash' command again.

The following image shows the output of this command.



```
Router#delete flash:c1841-advipservicesk9-mz.124-15.T1.bin
Delete filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Delete flash:/c1841-advipservicesk9-mz.124-15.T1.bin? [confirm]
Router#show flash
System flash directory:
File  Length   Name/status
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[255819 bytes used, 63760565 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
Router#
```

As mentioned above, when we power-up a router, the router copies the IOS image file from the flash memory into the RAM and uses the IOS image file from the RAM as long as it stays on. Because of this, the router will keep functioning till the next boot.

But, at the next boot time when the router fails to find a valid IOS image file in the flash memory, the router will not start. By default, if a router does not find a valid IOS image file on startup, it starts a special emergency mode. This mode is known as the ROMMON mode. The ROMMON mode allows us to install a new IOS image or restore the IOS image file from a file server.

To restart the router, run the 'reload' command from the privileged-exec mode.

RESTORING IOS IMAGE FILE

To download a new IOS image file from the TFTP server, the 'tftdnld' command is used. Before we use this command, we must have to set a few essential variables. These variables are the following.

IP_ADDRESS:- Temporary IP address of the router.

IP_SUBNET_MASK:- Subnet mask of the assigned IP address.

DEFAULT_GATEWAY:- IP address of the TFTP Server.

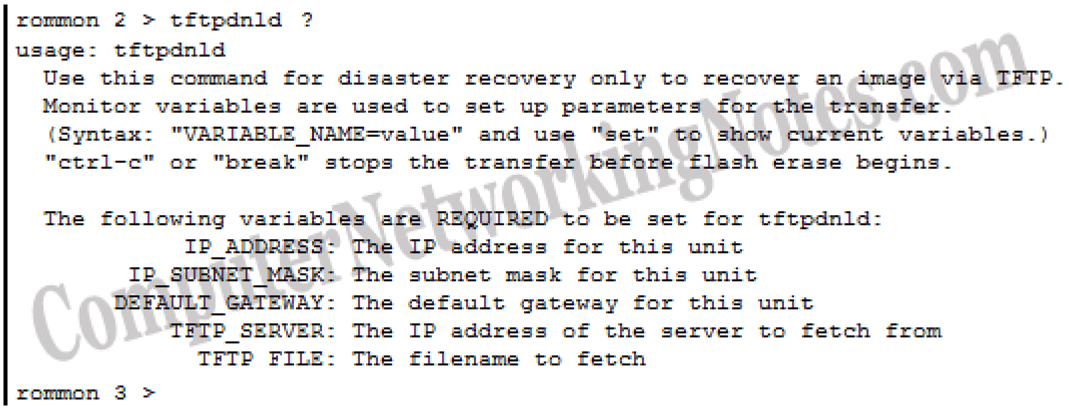
TFTP_SERVER:- IP address of the TFTP Server.

TFTP_FILE:- Exact name of the IOS image file. The name is case sensitive.

TFTP_CHECKSUM:- Prevent checksum errors.

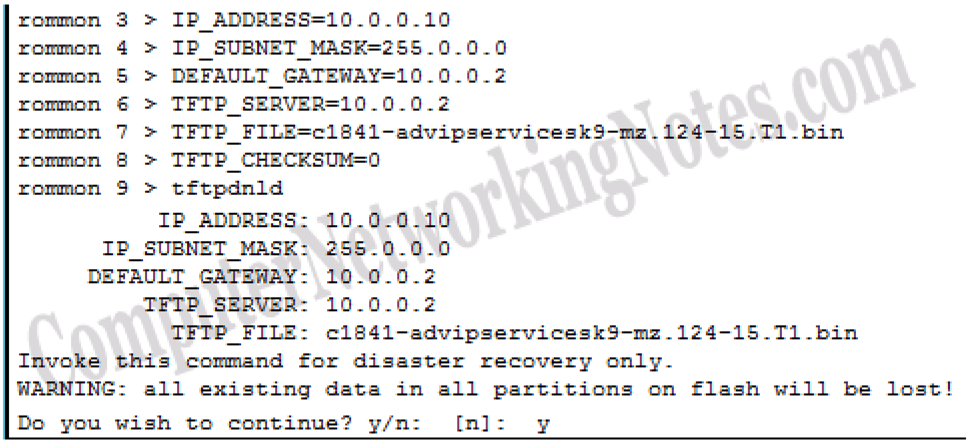
There is no need to memorize these variables. To view these variables along with a short description explaining how to use this command, type a question mark after this command and press the Enter key.

rommon > tftpdnld ?



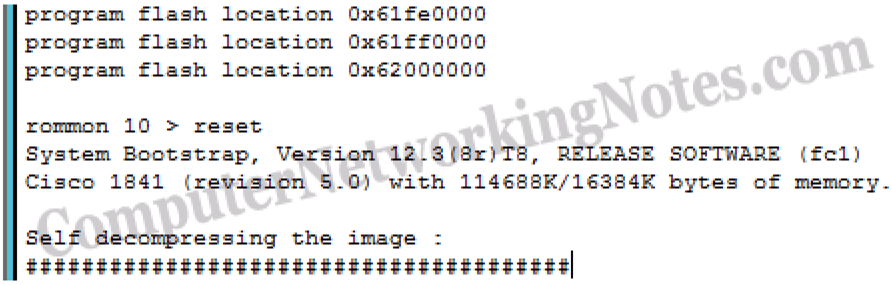
```
rommon 2 > tftpdnld ?
usage: tftpdnld
  Use this command for disaster recovery only to recover an image via TFTP.
  Monitor variables are used to set up parameters for the transfer.
  (Syntax: "VARIABLE_NAME=value" and use "set" to show current variables.)
  "ctrl-c" or "break" stops the transfer before flash erase begins.

  The following variables are REQUIRED to be set for tftpdnld:
            IP_ADDRESS: The IP address for this unit
        IP_SUBNET_MASK: The subnet mask for this unit
       DEFAULT_GATEWAY: The default gateway for this unit
           TFTP_SERVER: The IP address of the server to fetch from
             TFTP FILE: The filename to fetch
rommon 3 >
```

Set the required variables and run the 'tftpdnld' command. This command lists all variables and their values. If a variable is incorrect, type 'N' and correct that variable and execute this command again. If all the variables are true, type 'Y' to confirm the download operation.



```
rommon 3 > IP_ADDRESS=10.0.0.10
rommon 4 > IP_SUBNET_MASK=255.0.0.0
rommon 5 > DEFAULT_GATEWAY=10.0.0.2
rommon 6 > TFTP_SERVER=10.0.0.2
rommon 7 > TFTP_FILE=c1841-advipservicesk9-mz.124-15.T1.bin
rommon 8 > TFTP_CHECKSUM=0
rommon 9 > tftpdnld
          IP_ADDRESS: 10.0.0.10
      IP_SUBNET_MASK: 255.0.0.0
     DEFAULT_GATEWAY: 10.0.0.2
         TFTP_SERVER: 10.0.0.2
           TFTP_FILE: c1841-advipservicesk9-mz.124-15.T1.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:  y
```

If all variables are correct, this command downloads the IOS image file from the TFTP server to the flash memory. Once the downloading is done, use the 'reset' command to restart the router.



```
program flash location 0x61fe0000
program flash location 0x61ff0000
program flash location 0x62000000

rommon 10 > reset
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
#######################################
```

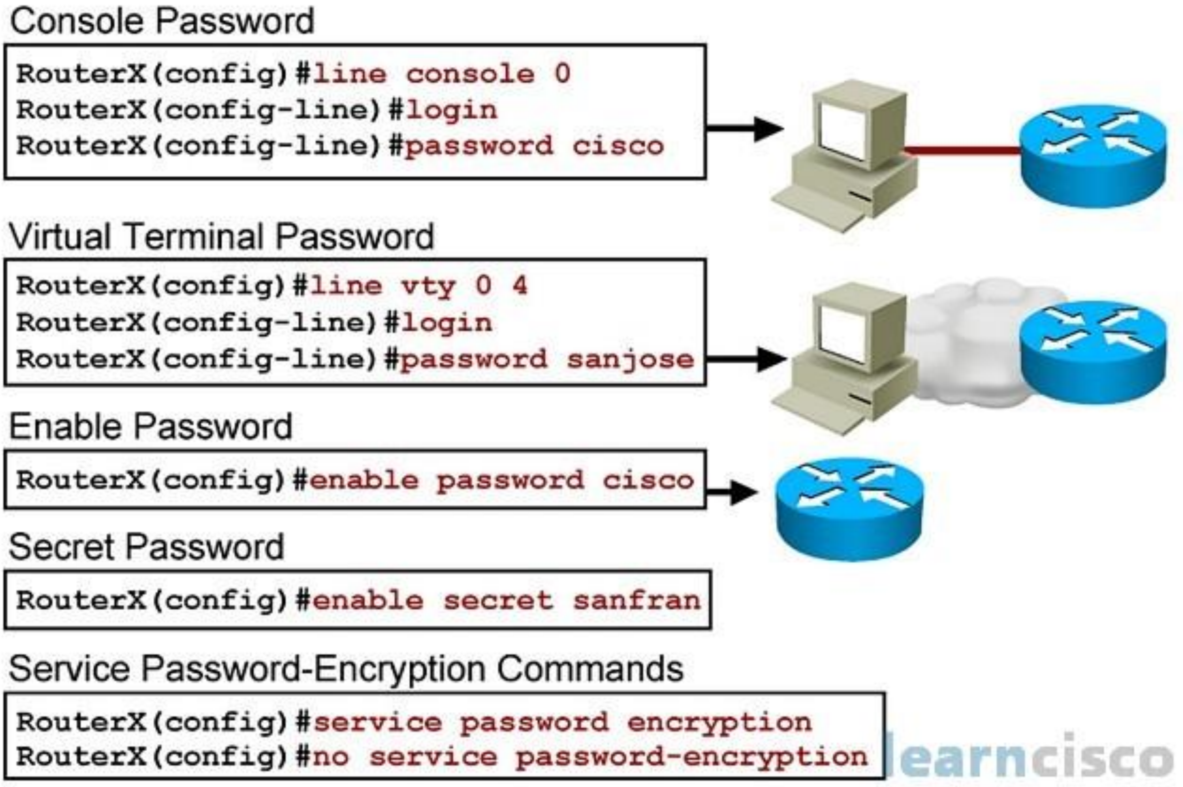
After the restart, if the router starts normally using the new IOS image file, it verifies that we have successfully restored the IOS image file.

Q.3 Explain Security Threat?

ANS. A security threat is a malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization. A security event refers to an occurrence during which company data or its network may have been exposed.

Q.4 List of Basic security of Password – Example with apply password in Router.

ANS.



Console Password

```
RouterX(config)#line console 0
RouterX(config-line)#login
RouterX(config-line)#password cisco
```

Virtual Terminal Password

```
RouterX(config)#line vty 0 4
RouterX(config-line)#login
RouterX(config-line)#password sanjose
```

Enable Password

```
RouterX(config)#enable password cisco
```

Secret Password

```
RouterX(config)#enable secret sanfran
```

Service Password-Encryption Commands

```
RouterX(config)#service password encryption
RouterX(config)#no service password-encryption
```

Q.5 Describe threat defense technologies.

ANS. Mobile Threat Defense tools are security tools specifically designed to detect and protect mobile devices against cyber threats. They analyze application characteristics and respond to threats in real-time while providing visibility of the risk level of all devices connected to the network.