Introduction to Cisco Hardware Lab

What you will learn from this lab:

- How to log into a Cisco router.
- Differences in available methods of access.
- Different levels of access permissions available on router
- How to identify router operating system and installed memory.
- Memory hierarchy, and how to best utilize it.
- How to identify interfaces.
- How to load and store configuration information.

Table of Contents

Supplementary Materials Attached:

- ✓ Refer to www.cisco.com

0.0 Preparation for this lab-

1. Read through this document, and familiarize yourself with the terms and concepts associated with Cisco's hardware and design philosophy.
2. Look at www.cisco.com or our supplementary materials to get to know the equipment you will be dealing with. Our lab is equipped with the following types of routers:
   - Cisco 7000 Series
   - Cisco 2500 Series
     - 2503
     - 2524

The 7000 Series is modular. Do not concern yourself with which modules are installed in the equipment. Rather, pay attention to the specifics of the router's architecture, especially the interaction of the Route Processor (RP) and Switch Processor (SP).

The 2XXX series, on the other hand, is (generally) not modular. Each model number corresponds to a specific set of interfaces. Using www.cisco.com or the supplements, make a list of interfaces that should be associated with each model. When we gain connectivity, we can check for correctness.

3. If you will be using your laptop for this lab, verify that you have a good TELNET program available for use. A program that is capable of logging the session will be extremely useful in this, and future labs.

1.0 Cisco's Three Tier Model

Over years of producing network equipment, Cisco Systems® has developed and embraced a three-tier model. They both build their equipment according to this philosophy, and also recommend that end-users construct their networks in the same mold. Generally, Cisco is careful to maintain that all of their equipment has the same general line of functionality (i.e. a 7000 can do what a 2501 can do, just much faster). However, if carefully engineered, responsibilities should be spread among the three layers. Let's look at the aforementioned layers to get an idea:

Core Layer-

- ✓ Generally consist of 7000 series and above
- ✓ Provide central internetwork for the business, and my include LAN and WAN backbones
- ✓ Primary function: to provide an optimized and reliable transport structure.

"Core routers provide services that optimize communication among routers at different sites or in different logical groupings. In addition, core routers provide maximum availability and reliability. Core routers should be able to maintain connectivity when LAN or WAN circuits fail at this layer. A fault tolerant network design ensures that failures do not have an impact on network connectivity" – Advanced Cisco Router Configuration, Chappel, Laura, p4.

Conclusion: the core is designed to provide fault tolerance, and to move packets through as fast as possible.

Distribution Layer-

- ✓ Consist of 3XXX – 4XXX series routers.
- ✓ Provides a "campus" backbone.
- ✓ Main aggregation point for costly functions like security.

"Distribution routers control access to resources that are available at the core layer and must, therefore, make efficient use of bandwidth. In addition, a distribution router must address the quality of service (QoS) needs for different protocols by implementing policy-based traffic control to isolate backbone and local environments. Policy-based traffic control enables you to prioritize traffic to ensure the best performance for the most time-critical and time-dependent applications" – Advanced Cisco Router Configuration, Chappel, Laura, p4.

Conclusion: the distribution layer polices access to the core, but also provides the main gateway of connectivity to different logical areas.

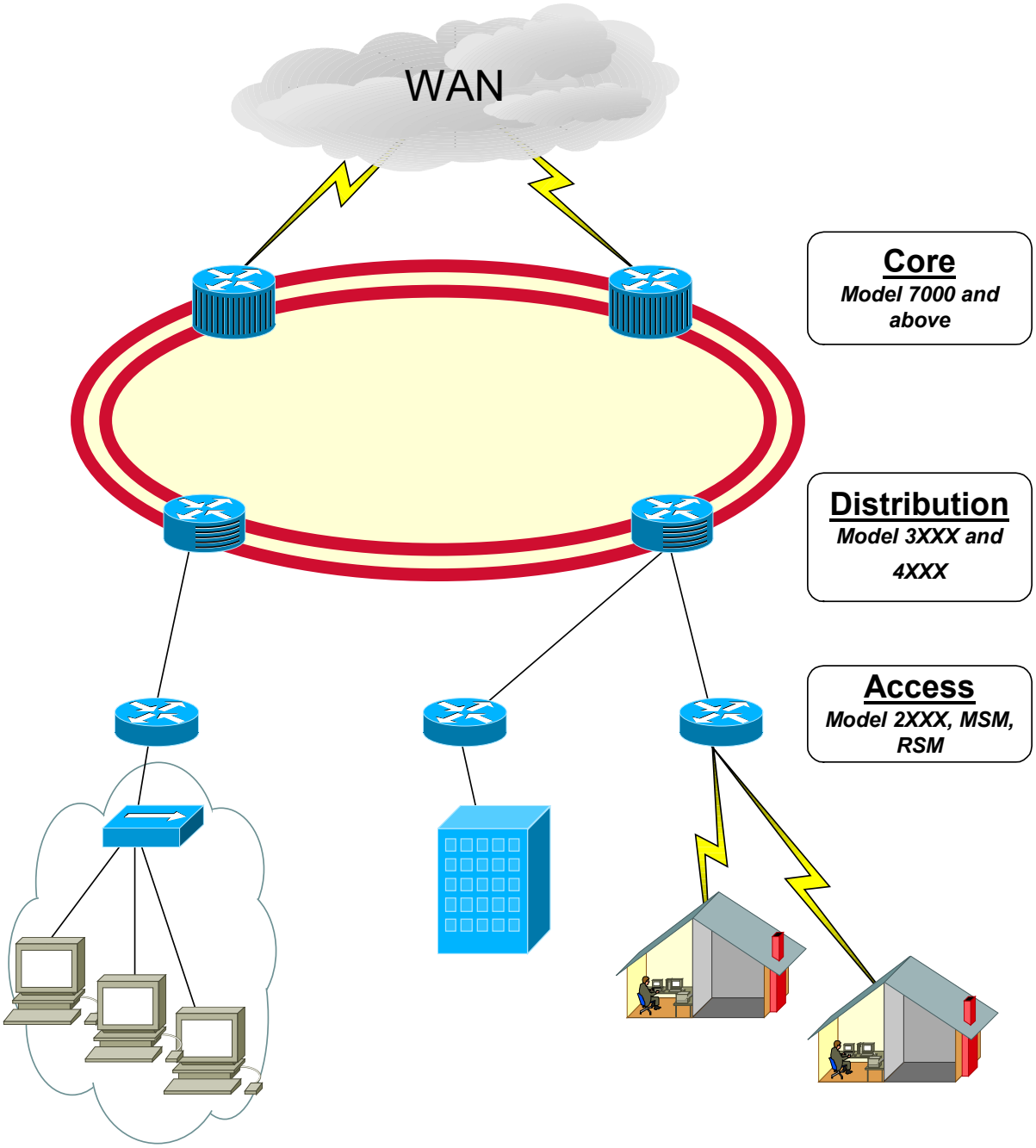
Access Layer-

- ✓ Provides access to corporate resources for a workgroup on a local segment**.**
- ✓ Last line of layer 3 hardware between network and user segment.

"Access routers control traffic by localizing broadcasts and service requests to the access media. Access routers must also provide connectivity without compromising network integrity. For example, the routers at the access point must be able to detect whether a telecommuter dialing in is legitimate, yet require minimal authentication steps required by the telecommuter"

Conclusion: the access layer is the first and last line of defense for the network. It represents the gateway between Layer 2 and Layer 3 connectivity for the entire structure.

Cisco's Three Tier Design - Overview



Why is this important?

Cisco designs their equipment specifically to meet this specification. Knowing the motivation helps us to understand why their equipment is constructed the way it is.

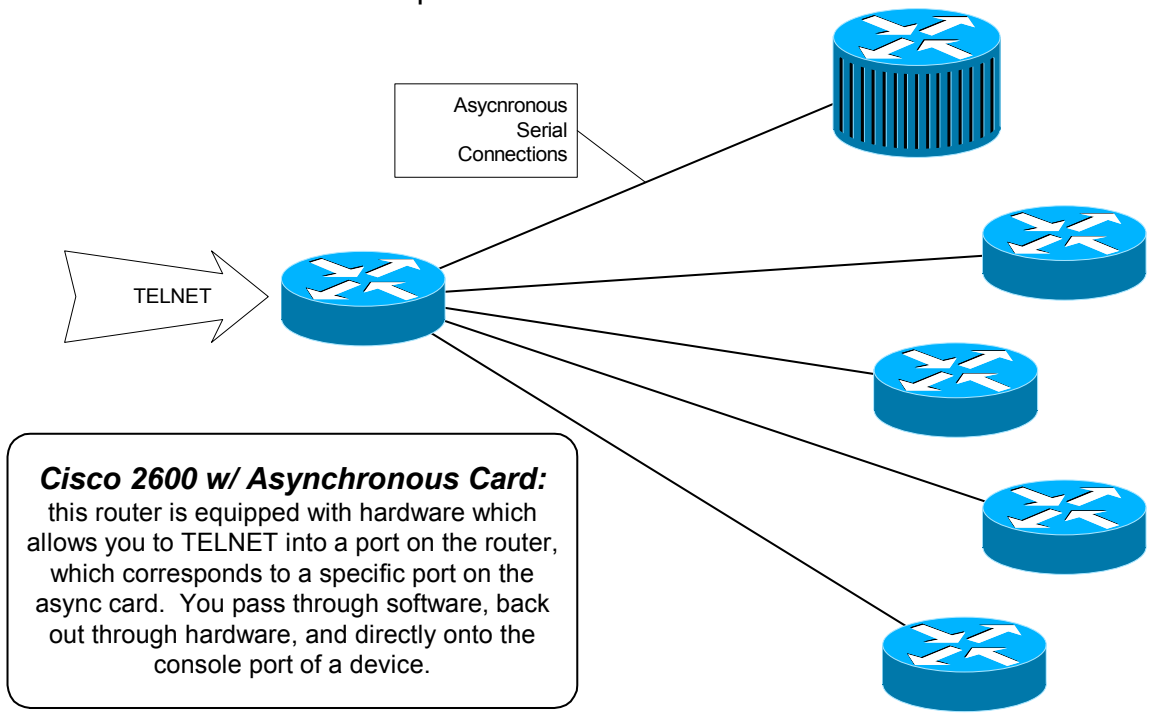
2.0 Accessing a Cisco Device

There are two primary methods for accessing a piece of Cisco equipment:

Console – the console is a physical port on the device that can only be accessed by manually plugging a cable into the RJ-45 slot. Though they can be modified, Cisco's default settings for this serial port are 9600 N-8-1. The console is the most powerful method of accessing a device, it can even be used to reset the password applied to it. Obviously, this necessitates impeccable security.

VTY (Virtual TTY's) – VTY's on a Cisco device are nothing more than TELNET access. (Note: the term TTY comes from the old "teletype" terminals that used to be associated with UNIX, anyone familiar with *NIX might have noticed this!). VTY's are software devices, therefore they are only available if the OS is up and running.

However, our lab uses an interesting hybrid of these two available access methods. You will be TELNETing into a device that will grant you access to individual router's console ports.



Cisco 2600 w/ Asynchronous Card: this router is equipped with hardware which allows you to TELNET into a port on the router, which corresponds to a specific port on the async card. You pass through software, back out through hardware, and directly onto the console port of a device.

This solution provides you with a single point of connection for all devices in the lab, without restricting your ability to perform configuration. You will be connected to each device as if you were sitting next to it with a serial cable attached!

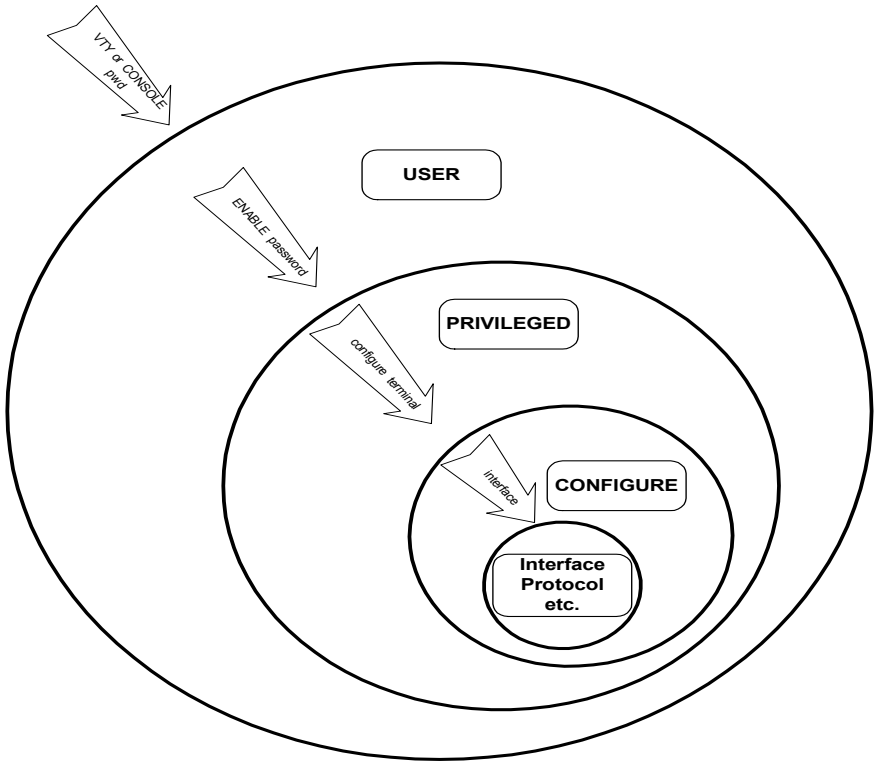
3.0 Levels of Access

Access levels on a router can vary wildly, as the IOS (Internetwork Operating System) allows for 16 user-defined levels. Generally, however, there are two default levels: **user** and **privileged**. Gaining access to a device via the console or VTY port grants **user** rights. Issuing the **enable** command enters privileged mode.

Initial access to the device is limited on a method by method basis. That is, you may place a password on the *console* port, and then place a different password on the *VTY* ports. Generally, these passwords are not encrypted when stored in the router, since they grant such a low level of administration. However, the enable password is global. Regardless of the method of connection, the enable password is consistent. It is stored as an MD5 hash, which is much more difficult to crack.

Once privileged, a user is granted access to the final mode of Cisco's IOS, which is **configuration mode**. Once in configuration mode, there are numerous available modes, corresponding to each interface, routing protocol, process, etc. For instance, to configure serial 0/0, in configuration mode, simply enter `int s0/0` .The "exit" command allows you to get out of a specific mode, and CTRL-Z exits configuration mode altogether.

Level of Access	***Command to Obtain***	***Required Permissions***
user	*None, login via console or VTY*	Correct password on method of login
privileged	*enable*	Correct enable password
Configuration mode	*Configure terminal*	Privileged mode



4.0 Command Line Semantics-

Inline help - Cisco's command line features an inline help function. For instance, at the privileged command line, typing "?" will bring up a list of all available functions. More importantly, typing a piece of the command, followed by a "?" will list all functions that begin with the typed term. For instance: issuing "`ac?`" at the command line results in:

```
access-enable  access-template
```

The IOS has gone and found all commands available that begin with "ac".

This is also applicable to command parameters. Issuing "show ip ?" will return a list of all objects that may be viewed with "show ip".

Tab/Incomplete Commands – when typing a command, the entire string does not have to be entered if it is unique. Example: the "show version" command. Typing "show ver" and hitting the return key will return the output of "show version". Also, the TAB key can be used to complete a word. Again, typing "show ver", but instead of pressing the ENTER key, pressing TAB, the IOS will finish the word "version". This will work on any "piece" of an issued command.

(i.e) issuing a "show ip interfaces brief"
type: "show ip int<TAB>"
returns "show ip interfaces"
type: "brie<TAB>"
returns "show ip interfaces brief"

Cisco Hot-Keys:

Command	Issued At	Effect
Delete	Anywhere	Removes one char to the right of cursor
Backspace	Anywhere	Removes one char to the left of cursor
TAB	Anywhere	Finishes a partial command.
Ctrl-A	Anywhere	Moves the cursor to beginning of current line.
Ctrl-E	Anywhere	Moves cursor to end of current line.
Ctrl-R	Anywhere	Redisplays a line.
Ctrl-U	Anywhere	Erases a line.
Ctrl-W	Anywhere	Erases previous word.
Ctrl-Z	Configuration Mode	Ends configuration mode and returns to EXEC
Up Arrow	Anywhere	Scroll forward through former commands.
Down Arrow	Anywhere	Scroll backward through former commands.

5.0 Getting Access on Real Hardware

1. Obtain connectivity to your router. (TELNET: litec-wti.ecse.rpi.edu <portnum>). If prompted to enter a configuration dialog, answer "no".
2. You should receive a prompt that looks something like the following:

   ```
   Router>
   ```

   This is the initial state of the router upon boot. It currently has no configuration, as if you just removed it from the box and turned it on.
   Currently, you are in **user** state. It is a restricted form of access that allows you to view a limited set of router conditions.
3. Issue the "enable" command. The ">" symbol at the end of our prompt is now replaced with the octothorpe. ***(Note: when a router is unconfigured, the only way to obtain the initial privileged access is via the console. Until the enable password is set up, no access to privileged mode is allowed via VTY).***
4. You have now been granted privileged access. Use some of the hot-keys and inline help functions now, and get used to the interface.
5. Issue a "`config term`" which is short for "`configure terminal`"
   The router should respond with a prompt that looks like : `Router(config)#` indicating that you are in configure mode.
6. The first thing we want to do is set an enable password on this device. Try issuing an "en?" to see if there is a command available.
   The router should respond with: `enable end`
7. Since there are two commands that begin with "en" we will have to narrow it down for the IOS. `Type "ena<TAB>"`.
   The router should complete the command for you and respond with: `enable`
8. Now issue a "?" to see what parameters are available for the command. The router gives back:

   ```
   last-resort  Define enable action if no TACACS servers respond
    password     Assign the privileged level password
    secret       Assign the privileged level secret
    use-tacacs   Use TACACS to check enable passwords
   ```

9. We want to issue a secret, so type "secret ?", which will bring up the inline help for the now complete "enable secret" command. ***(Note: a point of confusion arises here, why not issue password? Cisco's "enable password" command does not encrypt the password in memory by default. Though encryption can be turned on, the method is very weak. "enable secret", however, mandates the router encrypt the password using the MD5 hash. By default, if both are specified, the router will look for the secret password only)***
   The router will respond with:

   ```
   0      Specifies an UNENCRYPTED password will follow
   5      Specifies an ENCRYPTED secret will follow
   LINE   The UNENCRYPTED (cleartext) 'enable' secret
   level  Set exec level password
   ```

10. Rather than using the more convoluted 0, 5 parameters, we will simply issue the cleartext password as specified by "LINE". Issue "`enable secret cisco`"
11. The enable password is set, and this router will now be accessible via VTY.

Exercise – Setting the Hostname:

- ✓ Now that the password is set, we would like to set the hostname. Try to do this. *Hint: you don't need a specific mode for this, use the inline help from the main configuration mode prompt.*
- ✓ ***Note: when in configuration mode, a change can be un-done by issuing "no <command>" (i.e. no hostname LONDON_WAN, erases the hostname).***

6.0 Cisco Router Memory Organizaton

Cisco devices generally maintain three types of storage:

Flash: erasable NVRAM. Most often the residence of the IOS.

NVRAM: also erasable NVRAM, however, it is usually much smaller than the flash used for IOS (32K as opposed to 8-64MB). Configuration scripts are stored here.

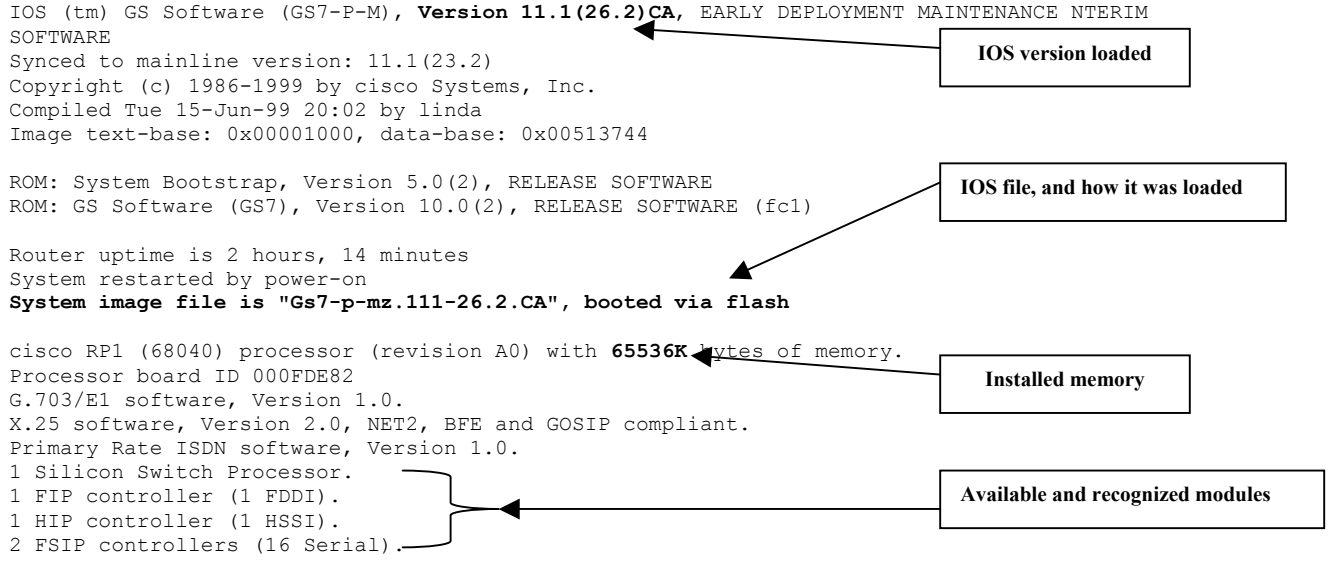
RAM: regular non-static Random Access Memory. Used upon power up for storage of dynamic data like routing tables and as processing space for the protocols.

6.1 Determining Available Resources

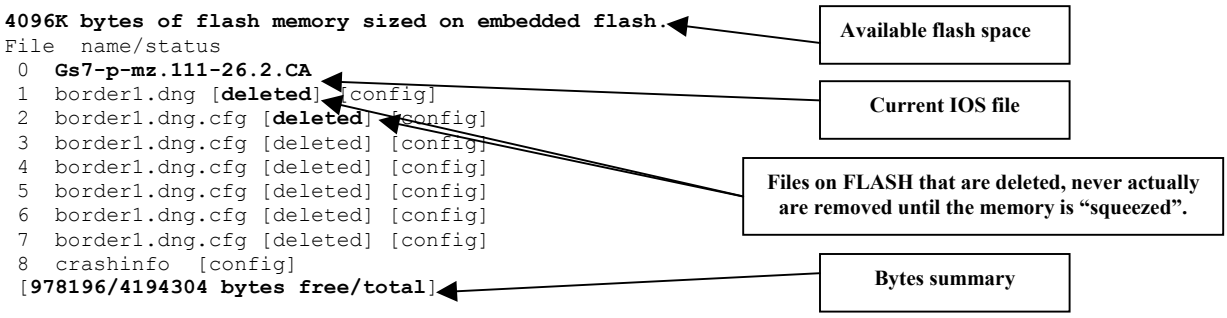
When a device is started, a bootstrap program is loaded from ROM, and begins searching for the IOS. (For simplification, we will assume that it looks only in FLASH, though it can be configured to load via other sources like TFTP). IOS is loaded from the FLASH memory, and then the configuration NVRAM is read. The script is parsed line by line and the commands are applied accordingly. Meanwhile, RAM is being used as space for the processes loaded by commands, and as storage for those processes' data.

Determining Available Memory- the "`show version`" command outputs low-level information about the router. For example, on LONDON_WAN:

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GS7-P-M), Version 11.1(26.2)CA, EARLY DEPLOYMENT MAINTENANCE NTERIM
SOFTWARE
Synced to mainline version: 11.1(23.2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 15-Jun-99 20:02 by linda
Image text-base: 0x00001000, data-base: 0x00513744

ROM: System Bootstrap, Version 5.0(2), RELEASE SOFTWARE
ROM: GS Software (GS7), Version 10.0(2), RELEASE SOFTWARE (fc1)

Router uptime is 2 hours, 14 minutes
System restarted by power-on
System image file is "Gs7-p-mz.111-26.2.CA", booted via flash

cisco RP1 (68040) processor (revision A0) with 65536K bytes of memory.
Processor board ID 000FDE82
G.703/E1 software, Version 1.0.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Primary Rate ISDN software, Version 1.0.
1 Silicon Switch Processor.
1 FIP controller (1 FDDI).
1 HIP controller (1 HSSI).
2 FSIP controllers (16 Serial).
```



Determining Available Flash- the "show flash" command outputs any and all files that are resident in flash memory. It also provides a quick tabulation of used versus available space.



6.2 Loading and Storing Device Configuration

Being able to ascertain and monitor device resources is an essential step in planning for and implementing changes on network hardware. However, the most frequently used commands relate to manipulating user-defined configuration of the device.

Once a router has completed the initial boot phase, and loaded the available configuration script from memory, NVRAM is not accessed again unless specifically requested by the user. In fact, upon boot, the configuration is copied from NVRAM into RAM. When a user makes changes on a router, those changes are reflected in the RAM copy, and the NVRAM config is only overwritten when user directs so.

Command	***Description***
show running-config	Accesses the configuration script that is now resident in RAM, and displays it on the screen.
show start-config	Accesses the configuration stored in NVRAM, and displays it line by line on the screen.
copy running-config startup-config	IOS versions 11.0 and later use this command to copy the configuration script in RAM, along with any changes made to it by the user, to NVRAM.
copy startup-config running-config	Inverse of above. It is worth noting however, that this command merely re-runs the configuration script stored in NVRAM. Therefore, it will not always "refresh" the router configuration, since certain processes must be turned off manually with "no <process_name". It is usually best to avoid this command, and to restart the router if a fresh config is necessary
write terminal	IOS versions 10.X and before use this command instead of "show running-config". Write commands are always referring to RAM copy of configuration, so "write terminal" can be expanded to "write RAM_config to terminal". IOS versions after 10 also include this command for backward compatibility.
write memory	Same parameters as "write terminal", except that RAM configuration is now written to NVRAM.
write erase	Only command available to totally purge configuration NVRAM. Any config stored there will be erased.

Note: in our labs, it will be rare that we will store the configuration at the end of the session since the lab must be reinitialized for another group. However, the term project may require multiple sessions of work for completion, and these commands will be very necessary.

Exercise – Comprehensive:

- ✓ Returning to the router, verify the following information:
  - *IOS Version Loaded*
  - *IOS Storage Location*
  - *Available RAM*
  - *Available Flash*
  - *Current script stored in NVRAM*
  - *System Uptime*
  - *Installed modules*

Advanced Exercise:

- ✓ Using all the commands discussed in this lab, do the following:
  - Assign an ip address to any interface, and bring the interface up *(hint: to enable an interface issue "*`no shutdown`*"*
  - Obtain a log of the entire router configuration.
  - Obtain a log of interface status and counters *(hint: use* `show` *commands)*
  - Re-enter the device and remove all configuration by using "no".
  - Obtain a log of the final router configuration and compare it to initial values.

