

CCENT Study Guide

Chapter 7

Managing a Cisco Internetwork

Chapter 7 Objectives

- The CCENT Topics Covered in this chapter include:
 - **2.0 LAN Switching Technologies**
 - 2.6 Configure and verify Layer 2 protocols.
 - 2.6.a Cisco Discovery Protocol
 - 2.6.b LLDP
 - **4.0 Infrastructure Services**
 - 4.1 Describe DNS lookup operation.
 - 4.2 Troubleshoot client connectivity issues involving DNS.
 - 4.3 Configure and verify DHCP on a router (excluding static reservations).
 - 4.3.a Server
 - 4.3.b Relay
 - 4.3.c Client
 - 4.3.d TFTP, DNS, and gateway options
 - 4.4 Troubleshoot client- and router-based DHCP connectivity issues.
 - 4.5 Configure and verify NTP operating in client/server mode.
 - **5.0 Infrastructure Management**
 - 5.1 Configure and verify device-monitoring using syslog
 - 5.2 Configure and verify device management.
 - 5.2.a Backup and restore device configuration.
 - 5.2.b Using Cisco Discovery Protocol and LLDP for device Discovery
 - 5.2.d Logging
 - 5.2.e Timezone
 - 5.2.f Loopback

Table 7.1: Cisco router components

Bootstrap	Stored in the microcode of the ROM, the bootstrap is used to bring a router up during initialization. It boots the router up and then loads the IOS.	ROM (read-only memory)	Used to start and maintain the router. Holds the POST and the bootstrap program as well as the mini-IOS.
POST (power-on self-test)	Also stored in the microcode of the ROM, the POST is used to check the basic functionality of the router hardware and determines which interfaces are present.	Flash memory	Stores the Cisco IOS by default. Flash memory is not erased when the router is reloaded. It is EEPROM (electronically erasable programmable read-only memory) created by Intel.
ROM monitor	Again, stored in the microcode of the ROM, the ROM monitor is used for manufacturing, testing, and troubleshooting.	NVRAM (nonvolatile RAM)	Used to hold the router and switch configuration. NVRAM is not erased when the router or switch is reloaded. Does not store an IOS. The configuration register is stored in NVRAM.
Mini-IOS	Called the RXBOOT or bootloader by Cisco, the mini-IOS is a small IOS in ROM that can be used to bring up an interface and load a Cisco IOS into flash memory. The mini-IOS can also perform a few other maintenance operations.	Configuration register	Used to control how the router boots up. This value can be found as the last line of the show version command output and by default is set to 0x2102, which tells the router to load the IOS from flash memory as well as to load the configuration from NVRAM.
RAM (random access memory)	Used to hold packet buffers, ARP cache, routing tables, and also the software and data structures that allow the router to function. Running-config is stored in RAM, and most routers expand the IOS from flash into RAM upon boot.		

Verifying the Current Configuration

To verify the configuration in DRAM, use the show running-config command (sh run for short) like this:

```
Router#show running-config  
Building configuration...  
  
Current configuration : 855 bytes  
!  
version 15.0
```

The current configuration information indicates that the router is running version 15.0 of the IOS.

Copying the Current Configuration to NVRAM

By copying running-config to NVRAM as a backup, as shown in the following output, you ensure that your running-config will always be reloaded if the router gets rebooted. Starting in the 12.0 IOS, you'll be prompted for the filename you want to use:

```
Router#copy running-config startup-config  
Destination filename [startup-config]?[enter]  
Building configuration...  
[OK]
```

Copying the Configuration to a TFTP Server

Once the file is copied to NVRAM, you can make a second backup to a TFTP server by using the `copy running-config tftp` command, or `copy run tftp` for short. I'm going to set the hostname to Todd before I run this command:

```
Todd#copy running-config tftp
```

```
Address or name of remote host []? 10.10.10.254
```

```
Destination filename [todd-config]?
```

```
!!
```

```
776 bytes copied in 0.800 secs (970 bytes/sec)
```

If you have a hostname already configured, the command will automatically use the hostname plus the extension `-config` as the name of the file.

Restoring the Cisco Configuration

If you did copy the configuration to a TFTP server as a second backup, you can restore the configuration using the copy tftp running-config command (copy tftp run for short), or the copy tftp startup-config command (copy tftp start for short), as shown in the output below. Just so you know, the old command we used to use for this is config net:

```
Todd#copy tftp running-config
Address or name of remote host []?10.10.10.254
Source filename []?todd-config
Destination filename[running-config]?[enter]
Accessing tftp://10.10.10.254/todd-config...
Loading todd-config from 10.10.10.254 (via FastEthernet0/0):
!!
[OK - 776 bytes]
776 bytes copied in 9.212 secs (84 bytes/sec)
Todd#
*Mar  7 17:53:34.071: %SYS-5-CONFIG_I: Configured from
tftp://10.10.10.254/todd-config by console
```

Okay, here we can see that the configuration file is an ASCII text file, meaning that before you copy the configuration stored on a TFTP server back to a router, you can make changes to the file with any text editor.

Erasing the Configuration

To delete the startup-config file on a Cisco router or switch, use the command `erase startup-config`, like this:

```
Todd#erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files!
```

```
Continue? [confirm][enter]
```

```
[OK]
```

```
Erase of nvram: complete
```

```
*Mar 7 17:56:20.407: %SYS-7-NV_BLOCK_INIT: Initialized the  
geometry of nvram
```

```
Todd#reload
```

```
System configuration has been modified. Save? [yes/no]:n
```

```
Proceed with reload? [confirm][enter]
```

```
*Mar 7 17:56:31.059: %SYS-5-RELOAD: Reload requested by console.  
Reload Reason: Reload Command.
```

This command deletes the contents of NVRAM on the switch and router. If you type **reload** while in privileged mode and say no to saving changes, the switch or router will reload and come up into setup mode.

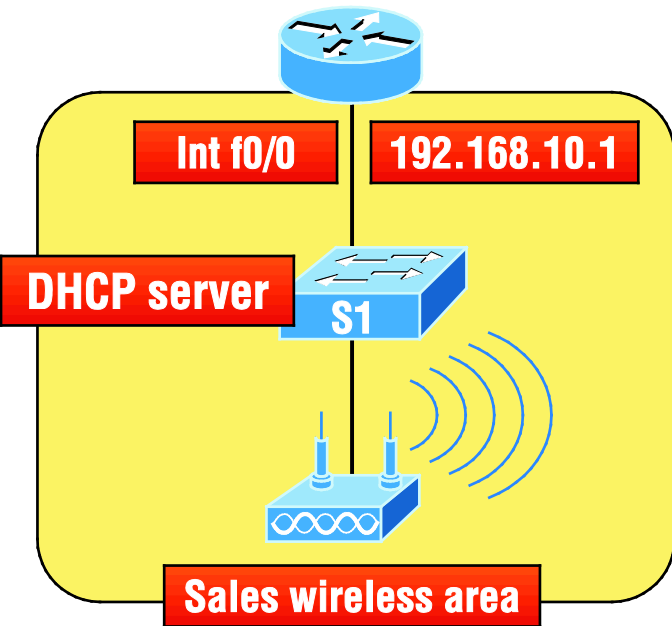
Configuring DHCP

Here are your configuration steps:

1. Exclude the addresses you want to reserve. The reason you do this step first is because as soon as you set a network ID, the DHCP service will start responding to client requests.
2. Create your pool for each LAN using a unique name.
3. Choose the network ID and subnet mask for the DHCP pool that the server will use to provide addresses to hosts.
4. Add the address used for the default gateway of the subnet.
5. Provide the DNS server address(es).
6. If you don't want to use the default lease time of 24 hours, you need to set the lease time in days, hours, and minutes.

Figure 7.1: DHCP Configuration example on a switch

Here's how we'll configure DHCP using the 192.168.10.0/24 network ID:

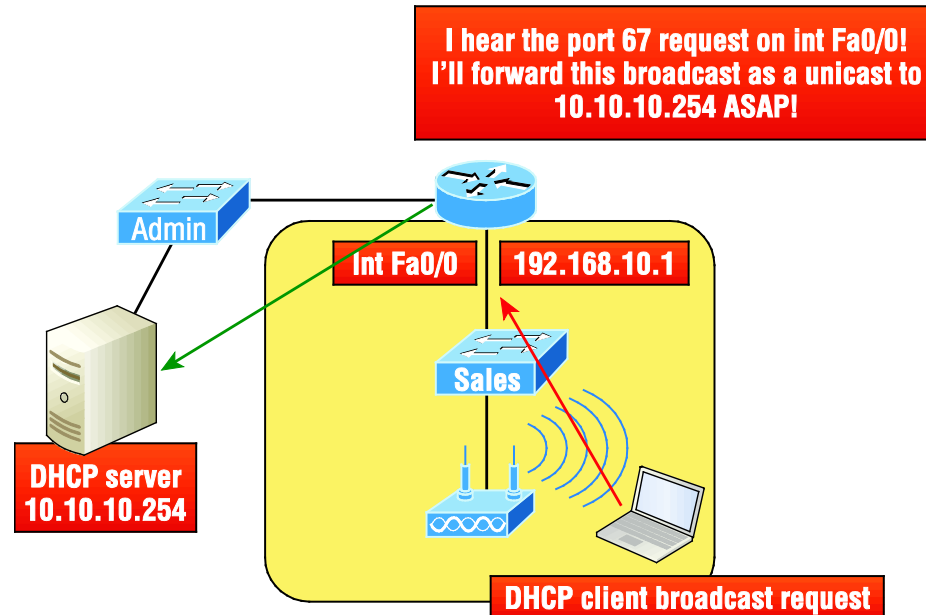


```
Switch(config)#ip dhcp excluded-address
192.168.10.1 192.168.10.10
Switch(config)#ip dhcp pool Sales_Wireless
Switch(dhcp-config)#network 192.168.10.0
255.255.255.0
Switch(dhcp-config)#default-router 192.168.10.1
Switch(dhcp-config)#dns-server 4.4.4.4
Switch(dhcp-config)#lease 3 12 15
```

First, you can see that I reserved 10 addresses in the range for the router, servers, and printers, etc. I then created the pool named Sales Wireless, added the default gateway and DNS server, and set the lease to 3 days, 12 hours, and 15 minutes (which isn't really significant because I just set it that way for demonstration purposes).

DHCP Relay

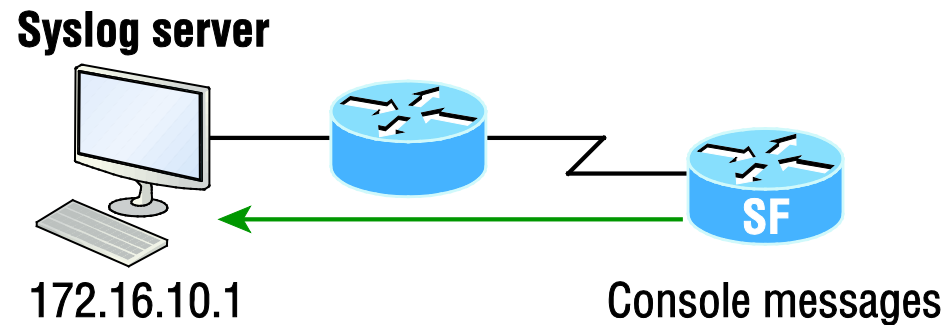
But what happens if we need to provide an IP address from a DHCP server to a host that's not in our broadcast domain, or if we want to receive a DHCP address for a client from a remote server?



So we know that because the hosts off the router don't have access to a DHCP server, the router will simply drop their client request broadcast messages by default. To solve this problem, we can configure the F0/0 interface of the router to accept the DHCP client requests and forward them to the DHCP server like this:

```
Router#config t  
Router(config)#interface fa0/0  
Router(config-if)#ip helper-address 10.10.10.254
```

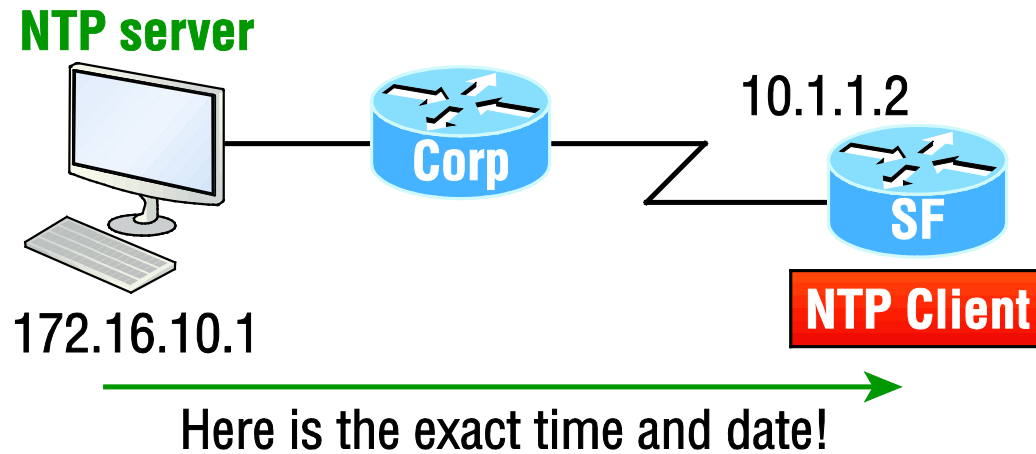
Figure 7.3: Sending console messages to a syslog server



A syslog server saves copies of console messages and can timestamp them so you can view them at a later time. This is actually rather easy to do. Here would be your configuration on the SF router:

```
SF(config)#logging host 172.16.10.1  
SF(config)#service timestamps log datetime msec
```

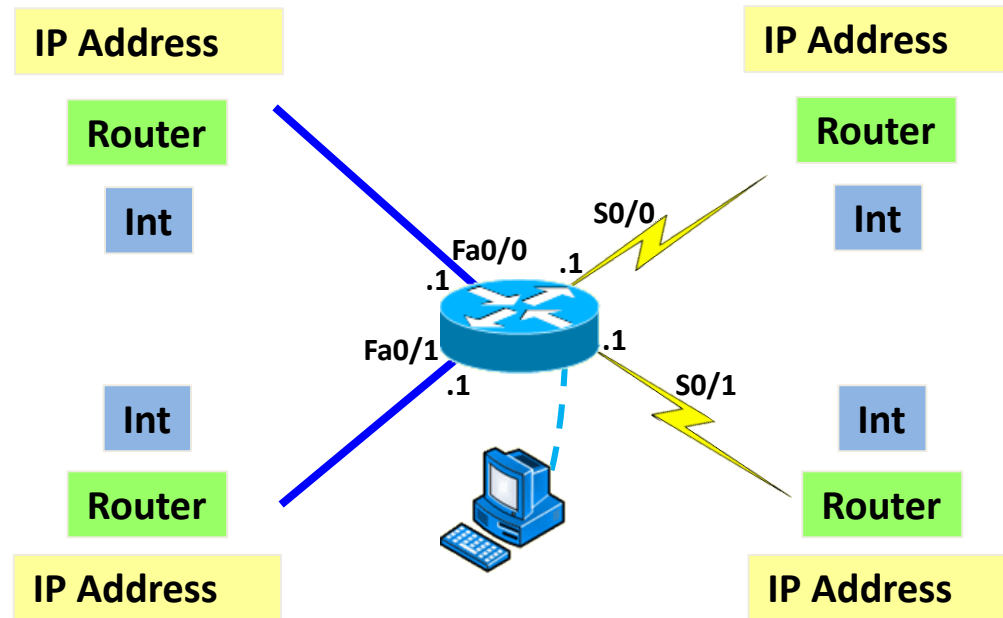
Network Time Protocol (NTP)



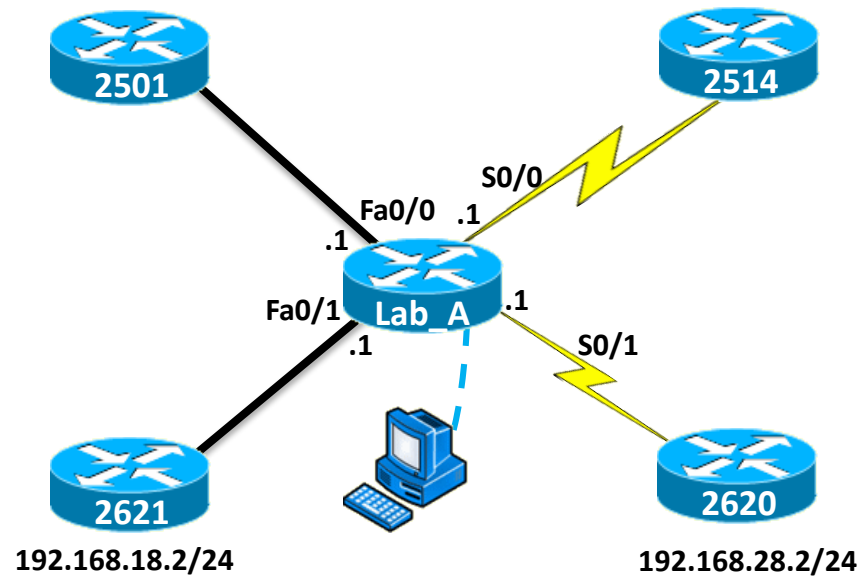
To make sure all devices are synchronized with the same time information, we'll configure our devices to receive the accurate time information from a centralized server

```
SF(config)#ntp server 172.16.10.1 version 4
```

Documenting a network topology using CDP



Network topology documented



Written Labs and Review Questions

- Read through the Exam Essentials section together in class.
- Open your books and go through all the written labs and the review questions.
- Review the answers in class.