SpringerBriefs in Computer Science

For further volumes:
http://www.springer.com/series/10028

Mohammed M. Alani

Guide to Cisco Routers Configuration

Becoming a Router Geek

Springer

Mohammed M. Alani
Department of Computing
Middle-East College of Info. Tech.
Al Rusayl
Muscat 124
Oman

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-1-4471-4245-4 ISBN 978-1-4471-4246-1 (eBook)
DOI 10.1007/978-1-4471-4246-1
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2012940963

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

When accessing your Facebook account, sending an email, or downloading a YouTube video, the network traffic that you just created will travel from your computer, smart phone, or tablet through the Internet to a server that might be thousands of kilometers away. The Internet is composed of many interconnected networks connected together through routers and switches. According to an ACG research report published in November 2011, when it comes to the routing and switching market, Cisco is by far the market leader with a market share of 54 % compared with 18 % to its closest competitor.

This book is a practical hands-on introduction to administering Cisco routers. This book is divided into seven stand-alone chapters. Chapter 1 of this book covers the basics of how to connect to a Cisco router to perform basic configurations. Then the book covers more advanced topics including routing protocols, WANs, router security, upgrades, and backups.

The book assumes basic understanding of network concepts. No prior knowledge or experience dealing with routers is assumed. Access to a Cisco router (physical or remote access) or a Cisco router emulator/simulator is needed to conduct the hands-on portion of the book. This book can be used as a text book to introduce student to the basics of routing using Cisco routers, or can be used with a theoretical book in an advanced undergraduate networking class. Professionals interested in the field of computer networking and its implementation using Cisco routers can use this book as a self-study, or use it as a reference to the most common tasks performed on a Cisco router.

What I really like about this book is its practical approach. It covers the most common tasks that a network administrator needs to do to manage a cisco network. The author not only gives you the commands necessary to perform a task, but also explains in detail what is being accomplished by these commands. Before presenting the task, the author gives an explanation why this task is important and what situation would require the user to perform this task.

I congratulate the author on a well-written book that provides the reader with an easy and fun way into the wonderful world of Cisco routers.

PA, USA — Assoc. Prof. Mahdi Nasereddin

Preface

It has become clear to all people involved in the field of computer networks that Cisco Systems has taken the lead in networking equipments market. This was not unexpected. Cisco's equipments have proved high quality from low-end to high-end sophisticated equipments.

You might be familiar with the title of this brief through the website holding the same name. This project started as a website a few years ago and kept piling up until it took the shape that is in your hands currently. The journey of this project from a website into a brief has been nothing less than joyful.

This brief provides a simplified step-by-step guide to configuring Cisco routers. This guide does not get the reader into the implications of theoretical aspects of networking. It simply shows the reader how to get things done in a clear, simple, and yet comprehensive way.

This guide starts from connecting the router through console port all the way up to complicated tasks, such as site-to-site VPNs and multiple-area OSPF.

Since this is a configuration guide, I assume that the reader is familiar with basic networking operation such as addressing, and routing protocols.

This guide covers basic and advanced configuration procedures as well. Basic procedures start from setting the hostname, passwords, and IP addresses of the router, configuring dynamic routing protocols, and password recovery procedures. The guide also includes advanced routing topics such as single- and multiple-area OSPF configuration, and integrated IS–IS configuration. The guide includes a chapter for domestic configurations that are currently considered essential duties of a router, such as DHCP, NAT, and inter-VLAN routing. The guide also includes a chapter dedicated to the configuration of different wide area network technologies ranging from ADSL to ISDN and frame-relay, along with PPP.

A chapter was dedicated to various security procedures to cope with the growing security requirements in modern networks. This chapter includes procedures to configure site-to-site VPN and SSH and Telnet access protection.

The largest chapter in this brief is concerned with maintaining the router configuration and operating system. This chapter includes multiple procedures to upgrade, backup, and restore the router IOS. It also provides simple steps to

backing up and restoring router configuration. The brief is finalized with a collection of hints and tips that can be useful to anyone configuring Cisco routers for learning or in real-life situations.

Inteded Audience of the Guide:

- field network engineers engaging Cisco routers;
- students working on Cisco routers in their labs;
- lab instructors;
- Cisco certification seekers;
- Cisco networking academy students;
- everyone working with or wanting to learn about Cisco routers configuration.

How to Use this Guide:

To make guide easier to use, different parts of the text were formatted differently. The meanings of these formats:

- `courier new font (small letters)` is used for output of the router;
- **`courier new bold font (small letters)`** is used for commands input to the router;
- **`courier new bold font (CAPITAL LETTERS)`** is used for commands parameters that the reader have to choose.

Finally, I would like to express my sincere thanks to my editors Wayne Wheeler and Simon Rees for making this project possible. I would also like to extend my thanks to all the website visitors who helped me with their queries and comments, all have participated in producing this guide in the form it is in today.

Muscat, Oman, 24 February 2012 Mohammed M. Alani

Contents

1 Starting Up 1
1.1 How to Connect the Router for Configuration. 1
1.2 Basic Configuration of a Cisco Router 2

2 Routing Protocols 5
2.1 How to Configure RIP in a Cisco Router 5
2.2 How to Configure EIGRP on a Cisco Router 7
2.3 How to Configure Single-Area OSPF on a Cisco Router 10
2.4 How to Configure Multiple-Area OSPF on a Cisco Router. 12
2.4.1 Configuration of Area 0 ABR. 13
2.4.2 Configuration of Area X ABR 14
2.4.3 Other Commands 15
2.5 More about Multiple-Area OSPF Configuration 15
2.6 How to Configure Integrated IS–IS on a Cisco Router. 17
2.7 How to Configure Load Balancing in a Cisco Router 20
2.7.1 Per-Packet and Per-Destination Load Balancing 20

3 Domestic Jobs 23
3.1 How to Configure a Cisco Router as a DHCP Server 23
3.2 How to Configure a Cisco Router as a DHCP Client. 26
3.3 How to Configure NAT and PAT on a Cisco Router. 26
3.3.1 Static NAT Configuration 27
3.3.2 Dynamic NAT Configuration 27
3.3.3 Troubleshooting Commands 29
3.3.4 Disabling NAT 29
3.4 How to Configure Inter-VLAN Routing on a Cisco Router 30

4 WAN Technologies. 33
4.1 How to Configure ADSL on a Cisco Router. 33
4.2 How to Configure PPP on a Cisco Router 35

4.3 How to Configure HDLC on a Cisco Router 37
4.4 How to Configure BRI ISDN in a Cisco Router 38
4.5 How to Configure ISDN Dialer Profiles in a Cisco Router 41
4.6 How to Configure a Cisco Router as a Frame-Relay Switch 43

5 Upgrades and Backups 45
5.1 Hints and Tips Before Upgrading the IOS of a Cisco Router . . . 45
5.2 Understanding the IOS File Name Convention 46
5.3 How to Backup and Restore the Configuration of a Cisco Router 48
5.4 How to Backup an IOS File from a Cisco Router 50
5.5 How to Upgrade IOS on a Cisco Router 52
5.5.1 Upgrade Procedure for Cisco Routers with Internal Flash 52
5.5.2 Upgrade Procedure for Cisco Routers with PCMCIA Flash 55
5.6 How to Upgrade IOS of a Cisco Router Using HyperTerminal 56
5.7 How to Upgrade or Install IOS on Cisco Router using ROMmon Mode 58
5.8 How to Copy IOS From One Cisco Router to Another 61
5.9 How to Partition Internal Flash Memory of a Cisco Router 61

6 Security 63
6.1 How to Secure Telnet Sessions Using Access-Lists on a Cisco Router 63
6.2 How to Configure SSH on a Cisco Router 64
6.3 How to Configure Site-to-Site VPN in Cisco Routers 66

7 Miscellaneous Hits and Tips 69
7.1 Top 10 Tips for Cisco Routers Configuration 69
7.2 Ten `show` Commands Everybody Needs to Know in Cisco Routers 72
7.3 How to Simulate Break Key Sequence in a Cisco Router 74
7.4 How to Recover Cisco 2600 Router's Password 75
7.5 How to Recover Cisco 2500 Router's Password 76

References 79

Chapter 1
Starting Up

Keywords Cisco · Router · Console · Hyper terminal · Terminal emulation · Basic configuration · Telnet · Interface

1.1 How to Connect the Router for Configuration

In order to configure the Cisco router to perform the network operation desired the first thing to do is to connect the router through console connection. This connection is used to configure the router and it does not carry user data.

Most routers come with console cable that has one DB-9 end and the other end is RJ-45 connecter. These connectors can be seen in Fig. 1.1. The cable is usually a slim ribbon that looks different from the regular LAN twisted pair cables.

Leave the router off and connect the RJ-45 end of the cable to the port of the router labeled console. The other end, the DB-9 one, should be connected to the computer serial port. Most of the modern laptops do not have the legacy DB-9 serial port. Instead of the DB-9 serial port, a USB port can be used. This would require the use of a USB-to-DB9 adapter.

Some older routers come with console cables that have RJ-45 connectors in both of their ends. These cables come with RJ-45-to-DB9 adapters.

After connecting the console cable to the computer, using the DB-9 connecter or the USB, software for terminal emulation is required.

The first choice is HyperTerminal® if you are using Windows XP®. If you are using Windows Vista® or Windows 7®, there are several free alternatives such as PuTTY or Tera Term. If you are using Linux, you can use MiniCom or CuteCom. For Mac®, you can use MiniCom and ZTerm.

The basic settings that need to be done in the terminal emulation software are the following:

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1_1, © Mohammed M. Alani 2012

Fig. 1.1 Console cable

1. Bits per sec: 9600
2. Data bits: 8
3. Parity: none
4. Stop bits: 1
5. Flow control: none

After connecting the cable and configuring the settings on the terminal emulation software, turn the router power on.

The screen should show the router boot-up process and information such as the IOS version, amount of memory available, types of interfaces, etc.

Eventually, you will end up at the user EXEC mode with the prompt "Router>". If the router was configured before and it has console password configured in it, you will be asked to input the password before getting to the user EXEC mode.

1.2 Basic Configuration of a Cisco Router

You should think of the basic router configuration as the greeting that should be said to a router coming out of the box or surviving a configuration erase.

The basic configuration steps are as follows:

1. Go to the global configuration mode and give the router a hostname:
   ```
   Router>enable
   Router#configure terminal
   Router(config)#hostname NEWROUTERNAME
   This would change the hostname of the router from ''Router''
   to NEWROUTERNAME. Keep in mind that this name follows the
   old file name rules (It should start with a letter, and should
   not contain spaces or symbols).
   ```
2. Set up enable/secret password:
   ```
   Router(config)#enable password
   YOURPASSWORD
   ```
   Or
   ```
   Router(config)#enable secret YOURPASSWORD
   ```

This password will be required when you type "enable" to go from user EXEC mode to privilege mode.
The first one saves the password in plain text, while the second one saves the password in encrypted format.
The first one is almost obsolete. It is more secure to use the second one. Remember that only one of them is required. If you set them both, the second one will prevail.

3. Set up console password:
   ```
   Router(config)#line console 0
   Router(config-line)#password YOURCONSOLEPASSWORD
   Router(config-line)#login
   ```
   This password will be required when a console connection is made. It is the first password that an administrator will be asked for before entering any mode.
4. To prevent the router messages from interrupting your writing, use the following command in the console line configuration mode:
   ```
   Router(config-line)#logging synchronous
   ```
5. If you plan to use Telnet set up the Telnet password. If you do not intend to use Telnet in the near future, do not set it up.
   ```
   Router(config)#line vty 0 4
   Router(config-line)#password YOURTELNETPASSWORD
   Router(config-line)#login
   ```
   In some routers, vty 0 15 is used instead of vty 0 4, depending on the number of simultaneous Telnet sessions you want to allow. If you need only one, just write vty 0.
6. Assign IP addresses to interfaces you plan to use:
   ```
   Router(config)#interface TYPE INTNUMBER
   Router(config-if)#ip address
   YOU.RIP.ADD.RES SUB.NET.MAS.K00
   ```
   Where,
   TYPE is the interface type such as ethernet, fastethernet, or serial.
   YOU.RIP.ADD.RES is the IP address you want to assign to this interface.
   SUB.NET.MAS.K00 is the subnet mask of the network this interface is connected to.
7. By default, all router interfaces are down. To turn on an interface use the following command in the interface configuration mode:
   ```
   Router(config-if)#no shutdown
   ```
8. Repeat steps 6 and 7 for each interface you need.
9. Save the configuration from the RAM to the NVRAM.
   ```
   Router#copy running-configuration startup-configuration
   ```

There are few other configurations that are useful but not necessary for the network to operate:

1. Setting a banner to be shown whenever someone tries to logon to the router configuration:
   ```
   Router(config)#banner motd #TYPE YOUR MESSAGE HERE#
   ```

2. Encrypt the passwords such that they become noncomprehendible to anyone viewing them in the running-configuration.
   Secret password is already encrypted. All other passwords (vty, console, and auxiliary) are not. The command to encrypt them is:
   `Router(config)#service password-encryption`
   There are two recommended methods to use this command. Because it is a service, it is not advised to keep it running all the time and consume processing power and memory. Thus, it can be used and turned off and the passwords will remain encrypted. One way to do this is to turn this command before setting up any passwords and turning it off after finishing the password setup commands using the following command:
   `Router(config)#no service password-encryption`
   The second way to do it is after finishing the setup of all passwords, turn on password encryption, issue a "`show running-config`" at the privilege mode, and then turn the password encryption off.
   The encryption used here is very weak. The only purpose of it is to prevent people looking at the configuration from knowing the password.
3. It is a very good practice to add interface descriptions. These descriptions are similar to remarks put into code of a program. It does not affect the operation of the interface in any way, but it gives information to the administrator viewing the configuration. This command should be written inside the interface configuration mode.
   `Router(config-if)#description WRITE YOUR OWN DESCRIPTION HERE`
   This description can be used in many useful ways such as writing the network name to which this interface is connected to, or writing the name of the other end of this link.

Chapter 2
Routing Protocols

Keywords Cisco · Router · RIP · Dynamic routing · EIGRP · Autonomous system · Metric · OSPF · Single-area OSPF · Multiple-Area OSPF · ABR · ASBR · Stub area · IS–IS · Integrated IS–IS · Load balancing · Per-packet load balancing

2.1 How to Configure RIP in a Cisco Router

When would you need this: When you need to implement a routing protocol for a small network and you need the configuration to be simple. Routing Information Protocol is the simplest that it can get.
Special Requirements: None.

1. The first thing to do is to enable the RIP protocol on the router.

   ```
   Router(config)#router rip
   ```

2. Identify the networks to be advertised using the 'network' command. Using this command, you need to identify only the networks that are directly connected to the router.

   ```
   Router(config-router)#network YOU.RNE.TWR.KID
   ```

   If the network is subnetted, you will need to write the main network address without the need to write the subnets. For example, if you have the following subnets connected to the router (172.16.0.0/24, 172.16.1.0/24, and 172.16.2.0/24), you can put them all in single 'network' command like this:

   ```
   Router(config-router)#network 172.16.0.0
   ```

   The router is intelligent enough to figure out which subnets are connected to the router.

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1_2,

3. If you need to adjust the timers (update, invalid, holddown, and flush timers) use the '`timers basic`' command. All the four parameters of this command, update, invalid, holddown, and flush timer consequently, are in seconds.

   ```
   Router(config-router)#timers basic 30 180 180 240
   ```

   The example above is set with the default values of the RIP timers. Remember to keep the relativity of the timer values. Always keep it as (n 6n 6n 8n). If, for example, you set the update timer to 40, you need to make the other timers 240 240 320 consequently. It is highly recommended that you keep the timers on their default values.

4. You will need to stop the updates from being broadcasted to the Internet, if one of the router interfaces is connected to the Internet. For this purpose, use the '`passive interface`' command. This command prevents the interface from forwarding any RIP broadcasts, but keeps the interface listening to what others are saying in RIP.

   ```
   Router(config-router)#passive-interface
   INTTYPE INTNUMBER
   ```

   where,
   INTTYPE is the type of the interface, such as Serial, Fastethernet, or Ethernet.
   INTNUMBER is the number of the interface such as 0/0 or 0/1/0.

5. RIP, by nature, sends updates as broadcast. If the router is connected through non-broadcast networks (like Frame Relay), you will need to tell RIP to send the updates on this network as unicast. This is achieved by the '`neighbor`' command.

   ```
   Router(config-router)#neighbor NEI.GHB.ORA.DRS
   ```

   where NEI.GHB.ORA.DRS is the IP address of the neighbor.

6. Cisco's implementation of RIP Version 2 supports authentication, key management, route summarization, classless inter-domain routing (CIDR), and variable-length subnet masks (VLSMs). By default, the router receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the router to receive and send only Version 2 packets. To do so, use the '`version`' command.

   ```
   Router(config-router)#version 2
   ```

   If you like to stick to version one, just replace the 2 in the command above with 1. Furthermore, you can control the versions of the updates sent and received on each interface to have more flexibility in support of both versions. This is achieved by the '`ip rip send version`' and '`ip rip receive version`' commands.

```
Router(config-if)#ip rip send version 2
Router(config-if)#ip rip receive version 1
```

7. Check the RIP configuration using these commands:

```
Router#show ip route
Router#show ip protocols
Router#debug ip rip
```

2.2 How to Configure EIGRP on a Cisco Router

When would you need this: When you are implementing a routing protocol on a large Internetwork and all the networking devices involved are Cisco devices or devices supporting EIGRP.
Special Requirements: EIGRP is a Cisco proprietary protocol. So, either all the routers in the Internetwork must be Cisco routers, or the routers should be EIGRP capable.

Before we start, if you have not set the bandwidth of the interfaces, set them now. For correct routing decisions, you need to set the bandwidth for the serial interfaces depending on the WAN technologies that you are using. This is done using the following command on each serial interface:

```
Router(config-if)#bandwidth BW
```

where BW is the bandwidth of the WAN connection in *kilobits per second*.
Next, you can start configuring EIGRP as in the following steps:

1. Enable EIGRP on the router with the command,

   ```
   Router(config)#router eigrp AS
   ```

   where `AS` is the Autonomous System number. The same AS number must be used for all the routers that you want to exchange routing information.

2. Instruct the router to advertise the networks that are directly connected to it.

   ```
   Router(config-router)#network NET.WOR.KAD.DRS
   ```

   where NET.WOR.KAD.DRS is the network address of a network that is directly connected to the router. Repeat this step for each network that is directly connected to the specific router that you are configuring. For subnetted networks, remember that you need only to write the original network address of a group of subnets and the router will automatically identify the subnets.
   For example, if the router is connected to the networks, 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24, you will need to do one '`network`' command with the address 172.16.0.0.

3. Although it is not recommended, if you need to change the way the metrics of the routes are calculated, you can set them using the command:

   `Router(config-router)#`**`metric weights TOS K1 K2 K3 K4 K5`**

   where,
   `tos` is the type of service index and the values of k1–k5 are used to calculate the metric using the following equation:

$$metric = \left(k1 \times bandwidth + \frac{k2 \times bandwidth}{256 - load} + k3 \times delay\right) \times \frac{k5}{reliability + k4}$$

   the default values are k1 = k3 = 1 and k2 = k4 = k5 = 0
   if k5 = 0, the formula is reduces to,

$$metric = \left(k1 \times bandwidth + \frac{k2 \times bandwidth}{256 - load} + k3 \times delay\right)$$

   It is *highly recommended* that you leave the metric in the default values unless you are a highly experienced network designer.

4. By default, EIGRP packets consume a maximum of 50 % of the link bandwidth, as configured with the 'bandwidth' interface configuration command. You might want to change that value if a different level of link utilization is required or if the configured bandwidth does not match the actual link bandwidth (it may have been configured to influence route metric calculations). Use the following command to set the percentage of bandwidth to be used on each interface separately:

   `Router(config-if)#`**`ip bandwidth-percent eigrp BP`**

   where BP is the percentage of bandwidth to be used (ex: 70).

5. You can change the intervals of the hello packets and the holddown timer on each interface using command:

   `Router(config-if)#`**`ip hello-interval eigrp AS TIME`**

   where AS is the autonomous system number and TIME is the new hello packet interval time in seconds.

   `Router(config-if)#`**`ip hold-time eigrp AS TIME`**

   where AS is the autonomous system number and TIME is the new holddown time in seconds.

6. Check your configuration on the routers after configuring all the routers in the internetwork using the following commands:

   To display information about interfaces configured for EIGRP.

   `Router#`**`show ip eigrp interfaces INTYPE AS`**

Display the EIGRP discovered neighbors.

```
Router#show ip eigrp neighbors
```

To display the EIGRP topology table for a given process.

```
Router#show ip eigrp topology AS
```

Or

```
Router#show ip eigrp topology NET.WOR.KAD.DRS SUB.NET.MAS.K00
```

To display the number of packets sent and received for all or a specified EIGRP process.

```
Router#show ip eigrp traffic AS
```

where,
INTYPE is the interface type
AS autonomous system number
NET.WOR.KAD.DRS and SUB.NET.MAS.K00 are the network address and subnet mask.

Configuring EIGRP Route Authentication (Optional)

EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol. The MD5 keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources. Before you can enable EIGRP route authentication, you must enable EIGRP.

The steps for setting the EIGRP route authentication are:

1. Identify a keychain to be used in the authentication,

   ```
   Router(config)#key chain NAME
   ```

   where NAME is the name of the keychain that will be created

2. Identify the key number,

   ```
   Router(config-keychain)#key NO
   ```

   where NO is the number of the key

3. Identify the key string,

   ```
   Router(config-keychain)#key-string STRNG
   ```

   where STRNG is the key string

4. You can stop here or set up a period in which the key will be effective,

   ```
   Router(config-keychain)#accept-lifetime START-TIME {IN-
   FINITE| END-TIME | DURATION}
   ```

```
Router(config-keychain)#send-lifetime START-TIME {INF-
INITE |END-TIME | DURATION}
```

You can set a start time and either end time, or duration in seconds, or you can leave the operation infinite.

EIGRP Implementation notes:

1. If you are using discontiguous networks, which is mostly the case, you should turn off auto-summarization using the following command:

   ```
   Router(config)#no ip auto-summary
   ```

2. You can set manual summary addresses using the following command:

   ```
   Router(config-if)#ip summary-address AS MASK
   ```

   where AS is the autonomous system number and MASK is the address mask.

3. When you are using non-broadcast networking technologies such as Frame Relay and SMDS, you will need to turn off split-horizon to let EIGRP perform efficiently and effectively

   ```
   Router(config-if)#no ip split-horizon AS
   ```

   where AS is the autonomous system number.

4. To clear the neighbor table use the command,

   ```
   Router#clear ip eigrp neighbors
   ```

2.3 How to Configure Single-Area OSPF on a Cisco Router

When would you need this: When you need to set up dynamic routing.
Special Requirements: None.

OSPF is one of the most widely used dynamic routing protocols. Cisco's version of OSPF is compatible with non-Cisco routers. If your network is large, jump into Sect. 2.4. Single-area OSPF is suitable for small-to-medium internetworks. An *area* is a logical grouping of routers running OSPF. All routers in the same area share the same topology database. Multiple-Area OSPF is used for large networks to prevent their topology databases from becoming out of the capability of the router.

Single-area OSPF configuration is as follows:

1. Since OSPF best route calculations rely solely on bandwidth, you need to set up the bandwidth of the serial interface involved in the routing process using the following command on the interface:

   ```
   Router(config-if)#bandwidth BW
   ```

where BW is the bandwidth of the connection in *kilobits per second.*
Remember that this command does not change the actual bandwidth. It only changes the bandwidth being seen by the routing protocol for the purpose of best path calculation.

2. Instruct the router to activate the OSPF routing process:

   `Router(config)#`**`router ospf PN`**

   where PN is the process number of OSPF. This process number is of local significance. It does not have to be the same on all routers.

3. Instruct the router to advertise the directly connected networks:

   `Router(config-router)#`**`network NET.WOR.KAD.DRS WIL.DCA.RDM.ASK area 0`**
   where,
   NET.WOR.KAD.DRS is the network address of a directly connected network.
   WIL.DCA.RDM.ASK is the wildcard mask of the network address.
   Since we are setting a single-area OSPF, we will always use "`area 0`".

4. Repeat step 3 for every network that is directly connected to the router.

Note
If you are not familiar with the wildcard mask, just invert the subnet mask and you will get the wildcard mask (ex: S/N Mask of 255.255.255.0 becomes Wildcard Mask of 0.0.0.255, S/N Mask of 255.255.255.192 becomes 0.0.0.63)

If you finished the first fours steps on all the routers involved in the process, everything should work just fine. If you want to do more configurations, there are a few optional advanced steps to go through:

1. To change the selection process of the DR (Designated Router) and BDR (Backup Designated Router) use the following command to change the router's OSPF priority on a certain interface:

   `Router(config)#`**`ip ospf priority PP`**

   where PP is the priority (0–255). The router with the *highest* priority becomes the DR. A priority of 0 means that this router will never be elected as DR.

2. To restart the whole process of DR and BDR elections use the command:

   `Router#`**`clear ip ospf process *`**

3. To change the cost of a certain link in the OSPF process use the following command:

   `Router(config-if)#`**`ip ospf cost CC`**

   where CC is the suggested cost (0–65,535)

For troubleshooting, you can use the following commands:

1. To show the OSPF processes information:

   ```
   Router#show ip ospf
   ```

2. To show the OSPF database of the topology:

   ```
   Router#show ip ospf database
   ```

3. To show the OSPF operation on the interfaces:

   ```
   Router#show ip ospf interface
   ```

4. To show the OSPF neighbors table:

   ```
   Router#show ip ospf neighbor
   ```

5. To debug all the OSPF process events:

   ```
   Router#debug ip ospf events
   ```

2.4 How to Configure Multiple-Area OSPF on a Cisco Router

When would you need this: When you need to set up dynamic routing for a large network and not all your routers are Cisco routers.
Special Requirements: None.
OSPF is one of the most widely used dynamic routing protocols. Cisco's version of OSPF is compatible with non-Cisco routers. If your network is not too large, Sect. 2.3 describes the steps of configuring single-area OSPF.

As defined in the previous section, an *area* is a logical grouping of routers running OSPF. All routers in the same area share the same topology database. Multiple-Area OSPF is used for large networks to prevent their topology databases from becoming out of the capability of the router.

When you design the areas and assign them IP addresses, remember to assign IP addresses that can be summarized. Make sure that all IP addresses in an area can be summarized into a single address with a different subnet mask. This is very important in reducing the amount of routing information exchanged between routers. (This, basically, is the idea behind creating multiple areas instead of one).

Area 0, or sometimes referred to as *Backbone Area*, will act as the center of the universe for all the other areas. *All areas must be connected to Area 0*. On the edge of each area, the router connected to another area is called Area Border Router (*ABR*). If not all areas can be connected to Area 0, there is a solution called *Virtual Links* that is discussed later in Sect. 2.5.

Let us move on to the configuration. For the sake of clearness, the ABR router that you plan to put into area 0 will be called "Area 0 ABR". The ABR at the border of other areas will be called "Area X ABR"

2.4.1 Configuration of Area 0 ABR

1. OSPF best route calculations rely solely on bandwidth. Hence, you need to set up the bandwidth of the serial interface involved in the routing process using the following command on the interface:

   ```
   Router(config-if)#bandwidth BW
   ```

   where BW is the bandwidth of the connection in *kilobits per second.*
   Remember that this command does not change the actual bandwidth, it only changes the bandwidth being seen by the routing protocol for the purpose of best path calculation.

2. Instruct the router to activate the OSPF routing process:

   ```
   Router(config)#router ospf PN
   ```

   where PN is the process number of OSPF. This process number is of local significance. It does not have to be the same on all routers.

3. Instruct the router to advertise the directly connected networks of area 0

   ```
   Router(config-router)#network NET.WOR.KAD.DRS
   WIL.DCA.RDM.ASK area 0
   ```

   where,
   NET.WOR.KAD.DRS is the network address of a directly connected network.
   WIL.DCA.RDM.ASK is the wildcard mask of the network address.

   Note
   If you are not familiar with the wildcard mask, just invert the subnet mask and you will get the wildcard mask (ex: S/N Mask of 255.255.255.0 becomes Wildcard Mask of 0.0.0.255, S/N Mask of 255.255.255.192 becomes 0.0.0.63)

4. Repeat step 3 for every network that is directly connected to the router *and* is part of Area 0
5. Instruct the router to advertise the directly connected network of area X

   ```
   Router(config-router)#network
   NET.WOR.KAD.DRS WIL.
   DCA.RDM.ASK area X
   ```

   where,
   NET.WOR.KAD.DRS is the network address of the directly connected network that connects area 0 to area X.
   WIL.DCA.RDM.ASK is the wildcard mask of the network address.
   X is the area number.

6. Configure the range of IP addresses for the whole area (similar to a summary-address):

```
Router(config-router)#area 0 range NNN.NNN.NNN.NNN SUB.
NET.MAS.K00
```

where,

NNN.NNN.NNN.NNN is the network address that summarizes all the networks in the area 0
SUB.NET.MAS.K00 is the subnet mask for the summarized address
This command reduces the size of the topology database, which is important in the backbone area.

2.4.2 Configuration of Area X ABR

1. As mentioned earlier, OSPF best route calculations relies solely on Bandwidth. Hence, you need to set up the bandwidth of the serial interface involved in the routing process using the following command on the interface:

   ```
   Router(config-if)#bandwidth BW
   ```

   where BW is the bandwidth of the connection in *kilobits per second.*
   Remember that this command does not change the actual bandwidth. It only changes the bandwidth being seen by the routing protocol for the purpose of best path calculation.

2. Instruct the router to activate the OSPF routing process:

   ```
   Router(config)#router ospf PN
   ```

   where PN is the process number of OSPF. This process number is of local significance. It does not have to be the same on all routers.

3. Instruct the router to advertise the directly connected networks of area X

   ```
   Router(config-router)#network NET.WOR.KAD.DRS
   WIL.DCA.RDM.ASK area X
   ```

   where,
   NET.WOR.KAD.DRS is the network address of the directly connected network that is in Area X.
   WIL.DCA.RDM.ASK is the wildcard mask of the network address.
   X is the area number.

4. Repeat step 3 for every network that is directly connected to the router *and* is a part of Area X
5. Instruct the router to advertise the directly connected network of area 0

   ```
   Router(config-router)#network NET.WOR.KAD.DRS
   WIL.DCA.RDM.ASK area 0
   ```

where,
NET.WOR.KAD.DRS is the network address of a directly connected network that connects area 0 and area X.
WIL.DCA.RDM.ASK is the wildcard mask of the network address.
X is the area number.

6. Configure the range of IP addresses for all the networks in area X (similar to a summary-address):

```
Router(config-router)#area X range NNN.NNN.NNN.NNN
SUB.NET.MAS.K00
```

where,
NNN.NNN.NNN.NNN is the network address that summarizes all the networks in the area X.
SUB.NET.MAS.K00 is the subnet mask for the summarized address.

2.4.3 Other Commands

You can use the following commands in troubleshooting:

1. To show the OSPF processes information:

```
Router#show ip ospf
```

2. To show the OSPF database of the topology:

```
Router#show ip ospf database
```

3. To show the OSPF operation on the interfaces:

```
Router#show ip ospf interface
```

4. To show the OSPF neighbors table:

```
Router#show ip ospf neighbor
```

5. To debug all the OSPF process events:

```
Router#debug ip ospf events
```

If you want more OSPF to configure, jump on to the next Sect. 2.5.

2.5 More about Multiple-Area OSPF Configuration

This article is a continuation of the previous section on Configuration of Multiple-Area OSPF on Cisco Routers. Refer to the previous section for the essential configuration of Multiple-Area OSPF.

1. ASBR

   A router is called Autonomous System Boundary Router (*ASBR*) when it connects the OSPF area to a different autonomous system. This router should be configured with a summary-address to summarize routes received into OSPF via redistribution:

   ```
   Router(config-router)#summary-address SUM.MAR.RYA.DRS SUB.NET.MAS.K00
   ```

   where
   SUM.MAR.RYA.DRS is the summary-address for the summarized subnets
   SUB.NET.MAS.K00 is the subnet mask of the summarized address.
   This command is usually issued at the router connecting the internetwork to the Internet.

2. Stub Areas

   Stub areas in OSPF are areas where only one ABR is there, or where co-located ABRs exist. For this kind of areas, the following configuration can be made to reduce the routing traffic between the ABRs:

   ```
   Router(config-router)#area X stub
   ```

   where X is the area number.
   This command should be issued on both ABR; the stub area ABR and the Area 0 ABR that is connected to the stub area. If more than one router exists in the stub area, the previous command needs to be issued on *all* routers of the stub area.
   Usually, if there is only one router in the stub area, instead of defining all directly connected networks, the following command is used:

   ```
   Router(config-router)#network 0.0.0.0 255.255.255.255 area X
   ```

   where X is the area number.

3. Virtual-Links

   By design, all OSPF areas must be connected to Area 0. If there is an area that cannot be directly connected to Area 0, you will have to use a Virtual-Link. Remember that despite the fact that configuration of the virtual-link is simple, many things can go wrong in a virtual-link, and it is *not* a recommended solution.
   To implement a virtual-link between Area 0 ABR and Area X ABR (where Area X is not directly connected to Area 0), we need to create logical loopback interfaces on both routers and link them together:
   On Area 0 ABR:

```
Router(config)#int loopback 0

Router(config-if)#ip address ARE.A0L.OOP.BCK SUB.NET.
MAS.K00
Router(config-if)#exit

Router(config)#router ospf PP

Router(config)#area X virtual-link ARE.AXL.OOP.BCK
```

where,
ARE.A0L.OOP.BCK is an IP address that you assign to the logical interface of Area 0 ABR. This address will be used by the Area X ABR to connect virtually.
SUB.NET.MAS.K00 is the subnet mask that you assign to the logical interface.
PP is the process-id of OSPF on the Area 0 ABR.
ARE.AXL.OOP.BCK is the IP address that you assign to the logical interface of the Area X ABR.
On Area X ABR:

```
Router(config)#int loopback 0

Router(config-if)#ip address ARE.AXL.OOP.BCK SUB.NET.
MAS.K00

Router(config-if)#exit

Router(config)#router ospf PP

Router(config)#area X virtual-link ARE.A0L.OOP.BCK
```

where,
ARE.AXL.OOP.BCK is an IP address that you assign to the logical interface of Area X ABR. This address will be used by the Area 0 ABR to connect virtually.
SUB.NET.MAS.K00 is the subnet mask that you assign to the logical interface.
PP is the process-id of OSPF on the Area X ABR.
ARE.A0L.OOP.BCK is the IP address that you assigned to the logical interface of the Area 0 ABR.

4. Some additional show commands to show the virtual-links currently configured the ABRs information, respectively:

```
Router#show ip ospf virtual-links

Router#show ip ospf border-routers
```

2.6 How to Configure Integrated IS–IS on a Cisco Router

When would you need this: When you need to set up dynamic routing for a large network and not all your routers are Cisco routers. It is being currently used to support MPLS routing and IPv6 routing.

Special Requirements: None.
IS–IS is an old interior gateway protocol. It is a routing protocol that was aimed to replace TCP/IP, but failed to. Anyway, why are we discussing this old protocol? Because new interest in it has appeared over the past few years. This interest is caused by the fact that IS–IS protocol is independent, ToS-supporting, and really scalable.

The cornerstone of IS–IS operation is having a properly addressed internetwork for IS–IS. This means that your subnets must be addressed in a summarizable way such that you can express the LANs connected to the router as a summarized address.
Let us move on to the configuration:

1. Create an LoopBack interface (logical interface) on the router and give it an IP address of your choice. Remember that this IP address will be part of the *Network Entity Title* (NET) address.

   ```
   Router(config)#int loopback 0
   ```

   ```
   Router(config-if)#ip address IPA.DDR.ESS.LO0 SUB.NET.MAS.K00
   ```

   where,
   IPA.DDR.ESS.LO0 is the IP address you want to assign to the loopback interface.
   SUB.NET.MAS.K00 is the subnet mask that you want to assign to the loopback interface.

2. Write down the NET address that you will assign to the router. There are many ways of creating NET address. We will not discuss them now. We will use the router's loopback address as the system ID as follows:

   AA.BBBB.CCCC.DDDD.EEEE.FF
   where,
   AA is the AFI. We will use "49" here as the AFI. This "49" means that we are making up our own NET address.
   BBBB is the area number (ex: 0001, or 0002). Remember that no more than 3 routers can operate in a single IS–IS area. You should start from 1.
   CCCC.DDDD.EEEE is the loopback IP address of the router. Previously defined as IPA.DDR.ESS.LO0, here it should be rewritten as IPAD.DRES.SLO0 (ex: 172.16.0.254 becomes 172.016.000.254 which becomes 1720.1600.0254)
   FF is the SEL. We will use "00" here. This "00" value means that this whole identifier is the NET of the device.
   A quick example: For a router with loopback address of 192.168.0.1, and the area is 1, the NET can be written as 49.0001.1921.6800.0001.00

3. Enable the IS–IS routing process on the router:

   ```
   Router(config)#router isis
   ```

4. Configure the NET that you have written down earlier:

   ```
   Router(config-router)#net AA.BBBB.CCCC.DDDD.EEEE.FF
   ```
   where AA.BBBB.CCCC.DDDD.EEEE.FF is the NET you have assigned to the router.

5. Configure route summarization *only* on the routers connected to other areas:

   ```
   Router(config-router)#summary-address SUM.MAR.YAD.RES SUB.NET.MAS.K01
   ```

   where,
   SUM.MAR.YAD.RES is the address summarizing all the networks of the area.
   SUB.NET.MAS.K01 is the subnetmask used for the summarization.

6. Enable IS–IS for IP on the serial interfaces that will be involved in the routing process:

   ```
   Router(config-if)#ip router isis
   ```

7. Repeat this configuration on all the routers that you want to involve in the IS–IS routing process. Remember that each router must have its own NET address and a maximum of *three* routers in each area.

What we have introduced here is a very simplified introduction to the configuration of IS–IS. There are many other configuration scenarios that need to be tackled in order to use IS–IS in a large network such as configure IS–IS for NBMA networks, or configuring different IS–IS levels.
For troubleshooting, you can use the following commands:

```
Router#show clns neighbor
Router#show clns interface
Router#show isis database
Router#show isis database detail
```

Note

If you are wondering why this protocol is called “Intermediate-System-to-Intermediate-System”, it was because a PC is thought of as an End-System, and the router as an Intermediate-System. Since this protocol is aimed to provide routing information exchange between routers, it was named “IS–IS” protocol.

2.7 How to Configure Load Balancing in a Cisco Router

When would you need this: When you are using a dynamic routing protocol, and have more than one path to destination networks.
Special Requirements: None
The first fact to be set is that *all* router platforms support load balancing. In a short description, load balancing is the operation in which the router forwards packets in different routes to the same destination. This happens when there is more than one path available for the same destination network.

There are two types of load balancing:

1. Multiple entries to the same destination with equal metrics.

   In this situation, protocols such as RIP, RIPv2, IGRP, EIGRP, and OSPF automatically does the operation and no configuration is needed.

2. Multiple entries to the same destination with different metrics.

   With a complex metric calculation method, like the ones used in IGRP and EIGRP, it is rare to get equal metrics for different paths to the same destination. In this case, configuration is needed.
   You can configure something called *variance*. The variance value determines the percentage that you are willing tolerate in choosing a secondary path. If the value of the variance is chosen to be 1, this means that only the paths with equal best metric will be used. And a value of 1.2, for example, means that the best path as well as the paths with a metric up to 1.2 of best path's metric will be used.
   A numerical example is,
   For a variance of 1.3, if the best path's metric is 1000, paths of metric in the range of 1,000–1,300 will also be used. Keep in mind that we are talking about multiple paths to the same destination.
   One more important note is that we are talking about paths derived from the same routing protocol, i.e., paths with the same *administrative distance*.
   The configuration of unequal path load balancing for IGRP and EIGRP is done with a single command:

   ```
   Router(config-router)#variance X
   ```

   where X represents the value of the variance that you want to use.

2.7.1 Per-Packet and Per-Destination Load Balancing

There are two types of load balancing; Per-Packet and Per-Destination. In *Per-Packet load balancing*, packets going to the same destination are sent over different paths. This way you will guarantee that all paths to the destination network

are being used. But using this method causes increased load on the routers' resources and low-end routers may crash. Also, the packets may arrive out of order because of different network latencies in different paths.

Using the *Per-Destination load balancing*, packets going to one destination pass through one path. This way you will lower the load on the router. But the different paths will not be utilized to the best.

To activate Per-Destination load balancing issue the following command on the interface that you want to use this method of load balancing,

```
Router(config-if)#ip route-cache
```

And to activate Per-Packet load balancing use,

```
Router(config-if)#no ip route-cache
```

Newer switching schemes such as Cisco Express Forwarding (*CEF*) allow you to do per-packet and per-destination load balancing more quickly. However, this method requires some extra resources to deal with maintaining CEF entries and adjacencies.

Chapter 3
Domestic Jobs

Keywords Cisco · Router · DHCP · DHCP server · DHCP client · Relay agent · DHCP pool · NAT · Network address translation · PAT · Port address translation · Static NAT · Dynamic NAT · NAT pool · Inter-VLAN routing · VLAN

3.1 How to Configure a Cisco Router as a DHCP Server

When would you need this: When using the router as a DHCP server to provide IP addresses and related information to DHCP clients.

Specials Requirements: DHCP server software is supported for these series; 800, 1000, 1400, 1600, 1700 series (support for the Cisco 1700 series was added in Cisco IOS Release 12.0[2]T), 2500, 2600, 3600, 3800, MC3810, 4000, AS5100, AS5200, AS5300, 7000, 7100, 7200, MGX 8800 with an installed Route Processor Module, 12000, uBR900, uBR7200, Catalyst 5000 family switches with an installed Route Switch Module, Catalyst 6000 family switches with an installed MultiLayer Switch Feature Card, and Catalyst 8500.

The configuration steps are:

1. Define the DHCP address pool,

   ```
   Router(config)#ip dhcp pool POOLNAME
   ```

   ```
   Router(dhcp-config)#network NET.OWR.KAD.DRS SUB.NET.MAS.K00
   ```

   where,
   POOLNAME is the DHCP pool name,
   NET.OWR.KAD.DRS is the network address to be used by the DHCP pool,
   SUB.NET.MAS.K00 is the subnet mask for the network.
   You can replace the subnet mask by a (/PREFIX) to provide the subnet mask.

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1_3, © Mohammed M. Alani 2012

2. Configure the parameters to be sent to the client,

   `Router(dhcp-config)#`**`dns-server DNS.IPA.DDR.ESS`**
   To provide the DNS server IP address

   `Router(dhcp-config)#`**`default-router DEF.LTG.ATE.WAY`**

   To provide the IP address of the default gateway, which is usually the IP address of the router interface connected to the network.

   `Router(dhcp-config)#`**`domain-name NAME`**

   To provide the name of the domain of the network (if in a domain environment)

   `Router(dhcp-config)#`**`netbios-name-server NET.BIO.SAD.DRS`**

   To provide the IP address of the NetBIOS name server

   `Router(dhcp-config)#`**`lease DAYS HOURS MINUTES`**

   To define the lease time of the addresses given to the client. You can make it infinite by using this command instead

   `Router(dhcp-config)#`**`lease infinite`**

   There is a large group of settings that you can configure to be sent to the clients, and I have only mentioned the most frequently used.

3. Configure the IP addresses to be excluded from the pool. This is usually done to avoid the conflicts caused by the DHCP with servers and printers. Remember to give *all* servers and network printers static IP addresses in the same range of the DHCP pool. Afterwards, exclude these addresses from the pool to avoid conflicts.

   `Router(config)#`**`ip dhcp excluded-address EXC.LDI.PAD.DRS`**

   Use the command in the previous form to exclude a single address. You can repeat it as much as you see fit for the IP addresses you want to exclude.
   You can also use the same command to exclude a range of IP addresses all in a single command:

   `Router(config)#`**`ip dhcp excluded-address STA.RTI.PAD.DRS END.IPA.DDR.ESS`**

   where,

   STA.RTI.PAD.DRS is the start of the range to be excluded from the pool
   END.IPA.DDR.ESS is the end of the range

4. Enable the DHCP service in the router

   `Router(config)#`**`service dhcp`**

   To disable it use

```
Router(config)#no service dhcp
```

Usually the DHCP service is enabled by default on your router.

5. Use the following commands to check the DHCP operation on the router:

```
Router#show ip dhcp binding
```

This command shows the current bindings of addresses given to clients

```
Router#show ip dhcp server statistics
```

This command shows the DHCP server statistics.

```
Router#debug ip dhcp server
```

This debug command is used to troubleshoot DHCP issues.

Implementation notes:

1. If you have a DHCP server other than the router and you would like the router to pass the DHCP requests to this DHCP server laying outside the LAN, go to the Ethernet interface that does not have the DHCP server and type the following command:

```
Router(config-if)#ip helper-address DHC.PSR.VRA.DRS
```

where DHC.PSR.VRA.DRS is the IP address of the DHCP server located outside this LAN.

2. You can create a DHCP database agent that stores the DHCP binding database. A DHCP database agent is any host, for example, an FTP, TFTP, or RCP server that stores the DHCP bindings database. You can configure multiple DHCP database agents and you can configure the interval between database updates and transfers for each agent. To configure a database agent and database agent parameters use the following command in global configuration mode:

```
Router(config)#ip dhcp database URL [timeout seconds |
write-delay seconds]
```

An example URL is this

```
ftp://user:password@192.168.0.3/router-dhcp
```

If you choose not to configure a DHCP database agent, disable the recording of DHCP address conflicts on the DHCP server. To disable DHCP address conflict logging, use the following command in global configuration mode:

```
Router(config)#no ip dhcp conflict logging
```

3. DHCP service uses port **67** and **68**. So, if you are using a firewall, remember to open these ports.
4. To clear DHCP server variables, use the following commands as needed:
   `Router#clear ip dhcp server statistics`

```
Router#clear ip dhcp binding *
```

If you want to clear a certain binding not all of them, replace the * in the previous command with the IP address to be cleared.

3.2 How to Configure a Cisco Router as a DHCP Client

When would you need this: When your ISP gives you a dynamic IP address upon each connection or you need to configure the router to obtain its interface IP address automatically.
Special Requirements: None.

This is done using a single command,

```
Router(config-if)#ip address dhcp
```

Some service providers might ask you to use a client-id and/or a hostname of their own choice. This can be done by adding the following parameters to the command above,

```
Router(config-if)#ip address dhcp client-id INTNAME hostname HOST
```

where,

INTNAME is the interface name that will be used for the client-id

HOST is the hostname that will be used for the DHCP binding.

This hostname can be different from the one that was set for the router in the global configuration. You can use both of these parameters, one of them, or none of them.

If you need, use the '`ip nat outside`' command at the interface and set up the rest of the NAT configuration as mentioned in the NAT and PAT configuration procedure in Sect. 3.3.

3.3 How to Configure NAT and PAT on a Cisco Router

When would you need this: When you want to connect a local network to the Internet and the available global IP addresses are less than the local IP addresses. This can also be used as an additional security feature.
Special Requirements: None.

There are two types of NAT that can be configured on a Cisco router; static, and dynamic.

3.3.1 Static NAT Configuration

This type is used when you want to do one-to-one assignment of global IP addresses to local IP addresses.

1. Establish static translation between an inside local address and an inside global address,

   `Router(config)#` **`ip nat inside source static LOC.ALI.PAD.DRS GLO.ABL.IPA.DRS`**
   where,

   LOC.ALI.PAD.DRS is the (inside) local address
   GLO.ABL.IPA.DRS is the (inside) global address

2. Specify the local interface. This is done by going to the interface configuration mode and issuing,

   `Router(config-if)#` **`ip nat inside`**

3. Specify the global interface. This is done by going to the interface configuration mode and issuing,

   `Router(config-if)#` **`ip nat outside`**

3.3.2 Dynamic NAT Configuration

This type is used when you want the router to do the mapping dynamically. This method is useful when you have too many global and local addresses and you do not want to do the mapping manually, or when the number of global addresses available is less than the local addresses.

This would lead us to two different scenarios,

A. The number of global IP addresses is more than one and it is equal or less than the local addresses.

1. Define a pool of global addresses that would be employed in the translation,

   `Router(config)#` **`ip nat pool NAME STA.RTG.LOB.AL0 END.GLO.BAL.IP0 netmask GLO.BAL.SUB.NET`**
   where,
   NAME is the name of the pool
   STA.RTG.LOB.AL0 is the starting IP address of the pool
   END.GLO.BAL.IP0 is the end IP address of the pool
   GLO.BAL.SUB.NET is the subnet mask of the network that the pool is part of (the global network)

2. Define the range of local addresses permitted to participate in the translation using an access-list.

   `Router(config)#`**`access-list ACLNO permit LOC.ALN.ETW.ORK WIL.DCA.RDM.ASK`**
   where,
   ACLNO is the number of the access-list, which is usually a standard access-list, thus the number can be any number from 1 to 99.
   LOC.ALN.ETW.ORK is the network address of the local network or the starting IP address of the range.
   WIL.DCA.RDM.ASK is the wildcard mask used to define the range
   You can issue more than one access-list sentence in the same access-list to define the specific IP address range(s). If you are not familiar with wildcard masks, refer to the note in Sect. 2.3.

3. Associate the pool and the local range in a dynamic NAT translation command,

   `Router(config)#`**`ip nat inside source list ACLNO pool NAME [overload]`**
   where,
   ACLNO is the number of the access-list
   NAME is the name of the global pool
   `overload` This parameter *must* be used when you have global IP addresses less than local IP addresses (this type of NAT is also known as Port Address Translation, *PAT*).

4. Specify the local interface. This is done by going to the interface configuration mode and issuing,

   `Router(config-if)#`**`ip nat inside`**

5. Specify the global interface. This is done by going to the interface configuration mode and issuing,

   `Router(config-if)#`**`ip nat outside`**

B. The other scenario is when there is only one global IP address and a group of local IP addresses.
In this case, the only global IP address is assigned to the interface connected to the global network.

1. Define the range of local addresses permitted to participate in the translation using an access-list.

   `Router(config)#`**`access-list ACLNO permit LOC.ALN.ETW.ORK WIL.DCA.RDM.ASK`**
   where,
   ACLNO is the number of the access-list, which is usually a standard access-list, thus the number can be any number from 1 to 99.

LOC.ALN.ETW.ORK is the network address of the local network or the starting IP address of the range.
WIL.DCA.RDM.ASK is the wildcard mask used to define the range
You can issue more than one access-list sentence in the same access-list to define the specific IP address range(s). If you are not familiar with wildcard masks, refer to the note in Sect. 2.3.

2. Associate the pool and the local range in a dynamic NAT translation command,

   `Router(config)#ip nat inside source list ACLNO interface TYPE INTNO overload`
   where,
   ACLNO is the number of the access-list
   TYPE is the type of the interface that has the global IP address (e.g., serial or Ethernet)
   INTNO the number of the interface
   An example of the interface type and number is serial 0, or Ethernet 0.

3. Specify the local interface. This is done by going to the interface configuration mode and issuing,

   `Router(config-if)#ip nat inside`

4. Specify the global interface. This is done by going to the interface configuration mode and issuing,

   `Router(config-if)#ip nat outside`

3.3.3 Troubleshooting Commands

1. To show the current translations preformed by NAT

   `Router#show ip nat translation`

2. To show the static translations of NAT

   `Router#show ip nat static`

3. To watch the instantaneous interactions of NAT

   `Router#debug ip nat`

3.3.4 Disabling NAT

To disable NAT, you need to do the following steps:

1. Disable NAT on the local and global interfaces

   `Router(config-if)#no ip nat inside` on the local, and
   `Router(config-if)#no ip nat outside` on the global interface.

2. Clear the contents of the translation table,

   `Router#clear ip nat translations`

3. Remove the NAT assignment command by preceding it with a '**no**'
4. Remove the access-list, if any.

3.4 How to Configure Inter-VLAN Routing on a Cisco Router

When would you need this: When you want to perform routing between different VLANs.
Special Requirements: You have to make sure that your router supports the frame tagging technology used between the switches.

Before jumping into the router configuration, you have to configure a port in the switch that will be connected to the router to be a trunk port. Your choice of VLAN tagging method configured on the switch (ISL or 802.1Q, 802.10, or LANE) will be the same that you will have to configure the router to operate by.

What will be done in this procedure is creating logical interfaces inside the single physical interface (on the router) that will be linking the switch to the router. These logical interfaces will be treated as separate interfaces in the routing decisions.

1. Remove the IP address from the physical interface, and turn it on,

   `Router(config-if)#no ip address`
   `Router(config-if)#no shutdown`

2. Create a logical interface to be assigned to one of the VLANs

   `Router(config-if)#int fastethernet 0/0.X`
   You can change the '`fastethernet`' to the type you have and the '`0/0`' with the interface number that you are using.
   X represents the logical interface number (not number of logical interfaces). You can use any number here, but it is a good practice to use the same number of the VLAN that you will assign to this logical interface. For example, for the logical interface that you will use for VLAN 5 use '`int fastethernet 0/0.5`'. This way, you will easily know which interface refers to which VLAN.

3. Assign the logical interface to a VLAN number

   `Router(config-subif)#encapsulation ENC VLANNO`

where,
ENC is the encapsulation type you are using for the VLANs (e.g., isl or dot1q which is 802.1Q)
VLANNO is the VLAN number that this logical interface will be assigned to.

4. Assign an IP address to the logical interface

   ```
   Router(config-subif)#ip address INT.IPA.DDR.ESS SUB.NET.MAS.K00
   ```

   where INT.IPA.DDR.ESS and SUB.NET.MAS.K00 are the IP address and the subnet mask, respectively, you want to use. Remember to give the logical interface an IP address that is laying in the range of the available IP addresses in the VLAN you assigned it to. This logical interface will be the gateway to the hosts connected to this VLAN.
   Repeat the steps 2–4 for each VLAN that you want.

5. Configure static or dynamic routing in the way you need it. Treat the logical interfaces the exact same way you treat the physical interfaces when doing the routing.

   If you want some VLANs (i.e, networks) not to participate in the routing, you can either not include them in the routing protocol or not assign a logical interface for them.

6. Configure access-lists in the way you find appropriate to filter the traffic going from one VLAN to another and apply them to the logical interfaces the same way you apply them to physical interfaces.

Implementation notes:

1. If you plan to let routing updates go through the router from one VLAN to another, it is necessary to turn off split-horizon. Split-horizon technology forbids the update coming from one interface to go out the same interface. Split-horizon can be turned off using the following command issued in the *physical* interface:

   ```
   Router(config-if)#no ip split-horizon
   ```

2. Most switches support trunks on FastEthernet or faster interfaces, and do not support the old Ethernet with 10 Mbps.

Chapter 4
WAN Technologies

Keywords Cisco · Router · ADSL · DSL · Internet · ATM · PPPoE · PPP · Chap PAP · Authentication · HDLC · BRI · PRI · ISDN · Dialer profile · SPID · Dialer-list · Dialer string · Dialer map · Frame-relay · DLCI

4.1 How to Configure ADSL on a Cisco Router

When would you need this: When you need to configure your router to operate on ADSL line provided by an ISP.
Special Requirements: ADSL WAN interface on the router.

Before starting, make a list of the information you will need from your service provider. This list includes:

Your account's username and password, MTU size (usually 1492), and PVC value (usually 0/35 or 8/35). You will also need to know if the IP address assigned to you by the ISP is a static public IP address, or your address is going to be dynamically assigned.

The configuration described here, moves the PPPoE operation to the router itself, so you will not have to setup PPPoE on the PC in order to dial in the Internet connection. The router will do that for you.

Now, let us jump into the configuration:

1. Enable the PPPoE operation in the global configuration as follows:

```
Router(config)#vpdn enable
Router(config)#no vpdn-logging
Router(config)#vpdn-group pppoe
Router(config-vpdn)#request dialin
Router(config-vpdn-req-in)#protocol pppoe
```

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1_4, © Mohammed M. Alani 2012

2. Setup the Fast Ethernet interface that will be connected to the local network, or any other type of interface you want to have:

```
Router(config)# int fa X/Y
Router(config-if)#ip address YOUR.LOCA.LIPA.DDRS
YOUR.SUBN.ETMA.SK00
Router(config-if)#ip tcp adjust-mss 1452
```

where,
X/Y is the number of your fast ethernet interface.
YOUR.LOCA.LIPA.DDRS is the local IP address of your fast ethernet interface
YOUR.SUBN.ETMA.SK00 is the subnet mask of the local interface
If '`ip tcp adjust-mss`' does not work, try out '`ip adjust-mss`' instead. If both do not work, you will need to upgrade the IOS of the router.

3. Setup the physical ADSL interface:

```
Router(config)#int atm 0
Router(config-if)#no ip address
Router(config-if)#pvc PVCNUMBER
Router(config-if-atm-vc)#pppoe-client dial-pool-number
1
Router(config-if-atm-vc)#no shut
```

where,
PVCNUMBER is the values of PVC you took from the ISP. (Usually 0/35 or 8/35).

4. Setup the dialer interface:

```
Router(config)#int dialer 1
```

If the IP address the ISP is giving you is as static public IP address, use this command:

```
Router(config-if)#ip address ISPG.IVEN.IPAD.DRSS
ISPG.IVEN.SBNE.TMSK
```

where,
ISPG.IVEN.IPAD.DRSS and ISPG.IVEN.SBNE.TMSK are the IP address and subnet mask given to you by the ISP
If the IP address is being assigned by the ISP dynamically, use this command instead:

```
Router(config-if)#ip address negotiated
```

After setting the IP address, continue the rest of the dialer configuration:

```
Router(config-if)#mtu MTUSIZE
Router(config-if)#no ip directed-broadcast
Router(config-if)#encapsulation ppp
Router(config-if)#dialer pool 1
Router(config-if)#ppp authentication chap pap callin
Router(config-if)#ppp chap hostname USERNAME
Router(config-if)#ppp chap password PASSWORD
```

```
Router(config-if)#ppp pap sent-username USERNAME pass-
word PASSWORD
```

where,
MTUSIZE is the size of the MTU given to you by the ISP (usually 1492)
USERNAME is the username of your account given by the ISP
PASSWORD is the password of your account given by the ISP.

5. The last step is to configure a default route to forward the traffic to the Internet through the dialer interface:

```
Router(config)#ip classless
Router(config)#ip route 0.0.0.0 0.0.0.0 interface dialer 1
```

It is a common practice to use NAT with the ADSL connection to facilitate the use of the ADSL connection by more than one host. Use the procedure outlined in Sect. 3.3 to configure NAT. In the aforementioned procedure, use the `dialer 1` interface instead of the outside interface. For example, the `ip nat outside` command must be given in the `dialer 1` interface with the group of commands displayed here in step 4. Another example is in the case of the use of a single public IP address, the NAT command must become `ip nat inside source list LL interface dialer 1 overload`.

4.2 How to Configure PPP on a Cisco Router

When would you need this: When you are creating a WAN link. This procedure might also be required when the other end of a WAN link is *not* a Cisco router. Point-to-Point Protocol can be used in synchronous, asynchronous, HSSI, and ISDN links.
Special Requirements: None.

1. Get to the interface configuration mode of the router's serial interface and issue the following command,

```
Router(config-if)#encapsulation ppp
```

2. If you want to configure authentication (which is almost always the case), go through the following steps:

   a. Choose the authentication type; Password Authentication Protocol (PAP), or Challenge Handshake Authentication Protocol (CHAP)

```
Router(config-if)#ppp authentication ENC
```

where ENC is the authentication type which can be: PAP, CHAP, PAP CHAP, or CHAP PAP. The last two choices are to use the second authentication type when the first one fails.
CHAP is strongly recommended over PAP for two reasons. First, PAP sends the username and password in plaintext, while CHAP sends hashed challenges only. Second is that CHAP does an operation similar to periodic re-authentication in the middle of the communication session, such that it provides more security than PAP.

b. Set a username and a password that the remote router would use to connect to your local router. You can define many username/password pairs for many PPP connections to the same router.

```
Router(config)#username USER password PASS
```

where USER is the host name of the remote router, and PASS is its password. Issue this command once for each PPP connection. For example, if you are connecting RouterA to RouterB and RouterC, on RouterA issue this command once for each remote router.

c. Now, you can set the username and password that your local router would use to access the remote router. For PAP authentication, you can specify the username and password that the local router will send to the remote router for authentication using the following command,

```
Router(config-if)#ppp pap sent-username USER password PASS
```

For CHAP, two commands are used,

```
Router(config-if)#ppp chap hostname USER
Router(config-if)#ppp chap password PASS
```

The usernames and passwords are case sensitive, so be careful when writing them. This way, you will have to write the username and password of the remote router in your local router and write the username and password of your local router into your remote using the '`username`' command.
If you do not set the username and password that will be sent from the local router to the remote router for authentication, the router will use its hostname and secret password instead.

3. You can monitor the quality of the serial link that is using PPP with the following command,

```
Router(config-if)#ppp quality PERCENT
```

where PERCENT is the minimum accepted link quality. If the link quality drops below PERCENT, the link will be shutdown and considered bad.

4. If the available bandwidth is small, you might consider compressing the data being transmitted using the following command,

```
Router(config-if)#ppp compress
COMP
```

where COMP is the compression type which can be `predictor` or `stacker`.

5. To troubleshoot PPP, you can use the following commands,

```
Router#debug ppp negotioations
Router#debug ppp packets
Router#debug ppp errors
Router#debug ppp authentication
```

Note

The compression might affect the system performance because it increases the CPU load. Check the CPU load with '`show process cpu`' and disable the compression if the CPU load is over 65 %.

4.3 How to Configure HDLC on a Cisco Router

When would you need this: When you connect two Cisco routers through a WAN connection, or in a back-to-back router setup.
Special Requirements: Both routers need to be Cisco routers.

Cisco HDLC is not compatible with other vendors' HDLC, so you need to make sure that routers on both ends of the communication are Cisco routers.

There is no long procedure to do this. The configuration is actually a single command:

```
Router(config-if)#encapsulation hdlc
```

Usually, the default encapsulation on the out-of-the-box Cisco routers is HDLC.

For troubleshooting, you can use the following commands to check that it has been configured properly:

```
Router#show interface serial X/X
```

where X/X is the number of the interface to check.

You can also check the status and IP address of the interfaces using the following command:

```
Router#show ip interface brief
```

4.4 How to Configure BRI ISDN in a Cisco Router

When would you need this: When you have ISDN WAN link and you want the router to use it.
Special Requirements: The router should have BRI interface(s).

There are two ways to configure ISDN in a Cisco router. The first one is to setup the ISDN connection to be always on. This method will be costly because most ISDN service providers charge not only by monthly subscription, but by the amount of data that you transfer. Having the connection always alive will cause extra expenses, because all kinds of traffic will pass through the ISDN link.

The second method is Dial on Demand Routing (DDR). DDR employs a mechanism that filters the traffic into *interesting* (worth connecting for) and *non-interesting* (not worth it). Using the DDR, the call scenario will be that the router does not setup the connection until interesting traffic needs to be routed to the other side. Once the connection is setup, all kinds of traffic (interesting and non-interesting) will pass unless you filter the passing traffic with an access list. Then, the router sets a down counter (idle-timer), and if no interesting traffic comes in and the timer goes to zero, the connection is terminated. If interesting traffic comes in before the idle timer is finished, the traffic is passed and the idle timer is reset. What made this function possible is the very small call setup time in ISDN.

If you are connecting two nodes using ISDN, keep reading. However, if you are connecting more than two nodes, you will need to go to Sect. 4.5 about configuring DDR Dialer Profiles.

To configure DDR on the router's BRI interface, perform the following steps:

1. The first thing to do is to setup routing. Static routing is usually preferred with DDR. Setting dynamic routing protocol, will cause the link to be on all (or most) of the time. Thus, static routing is a better solution. You can setup dynamic routing and tune it a bit for the DDR. This tuning might include changing the timers of routing updates.
   The following is an example of static routing;
   ```
   Router(config)#ip route 192.168.1.0 255.255.255.0
   192.168.2.1
   ```
   ```
   Router(config)#ip route 192.168.2.1 255.255.255.255 bri0
   ```
   Or, a default route,
   ```
   Router(config)#ip route 0.0.0.0 0.0.0.0 bri0
   ```
   Keep in mind that you will need to setup routing on both ends of the WAN link.

2. Specify the type of the ISDN switch. This piece of information should be provided to you by the ISDN service provider. You can issue this command,
   ```
   Router(config)#isdn switch-type SWTCH
   ```
   where SWTCH is the ISDN switch type.

Issuing this command in the global configuration mode will cause *all* the router's ISDN interfaces to be set to use this type of switch. You can set different types of switches for different interfaces if you issue the same command in the interface configuration mode like the following example:

```
Router(config)#int bri0
Router(config-if)#isdn switch-type SWTCH1
Router(config-if)#int bri1
Router(config-if)#isdn switch-type SWTCH2
```

After defining the switch type, identify the SPIDs in the BRI interface configuration mode,

```
Router(config-if)#isdn spid1 FRSTSPD YYY
Router(config-if)#isdn spid2 SCNDSPD YYY
```

The numbers used here should be provided to you by the ISDN service provider. Most providers in Europe *do not* use SPIDs in their ISDN networks. So, unless you are supplied with SPID numbers from the provider, just neglect all the commands of setting SPIDs in this procedure.

3. Specify interesting traffic to the router. This traffic is defined as the traffic permitted by a command named '`dialer-list`' which is similar to '`access-list`.'
   This can be done in two ways; the first is to use the following command,

```
Router(config)#dialer-list DLNO protocol PR permit
```

   where DLNO is the dialer-list number and PR is the protocol you want to permit. In addition, you can use '`deny`' instead of the '`permit`' part to prevent a certain protocol from becoming categorized as interesting. However, this is not a very powerful way of defining the interesting traffic.
   The second way is more recommended. The second way is to do a complete access list permitting the traffic that you want the router to consider interesting, and then attach it to a dialer list.
   Create the access list the exact same way you create any other access list, but do not apply it to an interface. Instead, associate it with a dialer list. All the traffic permitted by this access list, will be considered interesting. An example is the following:

```
Router(config)#access-list 110 deny tcp any any telnet
Router(config)#access-list 110 deny icmp any any
Router(config)#access-list 110 permit ip any any
```

   And the step that will associate the access list to the dialer list is:

```
Router(config)#dialer-list 5 protocol ip list 110
```

   where 5 is the dialer-list number and 110 is the access-list number. These two numbers do not need to be the same.
   Keep in mind that these dialer list and access list *do not* filter the traffic outgoing through the ISDN interface, it just chooses which traffic is entitled to initiate a

call. Once the call is setup, all traffic willing to pass through the ISDN link will pass. If you want to filter the traffic that is passing through the ISDN interface, create another access list for that with the filters that you find appropriate and apply it to the BRI interface as you do to any other type of interface.

4. Setup the encapsulation protocol, PPP. Using PAP authentication does not provide that much of security, so it is suggested that you use CHAP for authentication.
   The first thing to do to configure PPP to use CHAP is to set a username and a password.

   `Router(config)#username USER password PASS`
   where USER is the username and PASS is the password. The username should be the hostname of the other end and the password is the secret password of the other end. If you like to use different usernames and passwords, please refer to the PPP configuration procedure in Sect. 4.2.

   Then, move into the interface configuration mode of the ISDN interface,
   `Router(config)#int bri A/B`
   Now, set an IP address and a subnet mask for the interface,

   `Router(config-if)#ip address INT.IPA.DDR.ESS SUB.NET.MAS.K00`
   Set the encapsulation and authentication types;

   ```
   Router(config-if)#encapsulation ppp
   Router(config-if)#ppp authentication chap
   ```

5. Apply the dialer list to the interface,

   `Router(config-if)#dialer-group DLNO`
   where DLNO is the dialer list that was setup in step 3.

6. Define the idle timeout that you find appropriate for each call,

   `Router(config-if)#dialer idle-timeout IDLETO`
   where IDLETO is the duration of the call in seconds (the default is usually 120 s). The idle timeout is the period of time in which the call will remain alive waiting for more interesting traffic. If more interesting traffic comes in before the timer is over, the timers will be reset. If no interesting traffic comes in, the call will be terminated even if there was noninteresting traffic being transferred.

7. If you are using this link between two points only and your router will be dialing only for one destination using the ISDN network, use the following command to set the dialer string:

   `Router(config-if)#dialer string DSTRING`
   where DSTRING is the dialer string that is provided to you by the service provider. This dialer string is similar to the phone number that you dial in the

regular PSTN. So, you command the router to dial the string of the other side. For further security, you can use a different command that associates the dialing to a destination IP address with a username and a dialer string,

```
Router(config-if)#dialer map ip DES.TIP.ADD.RES name USER DSTRING
```

Where,
DES.TIP.ADD.RES is the IP address of the other end of the ISDN link
USER is the same username that you have setup to use with PPP
DSTRING is the dialer string of the other end of the ISDN link.

8. You can optionally use the following command to setup a threshold of load on which the second channel (in a BRI link) becomes active.

```
Router(config-if)#dialer load-threshold THR either
```

where THR is a number between 1 and 255, 1 being the minimum load and 255 being 100 % load on the first channel. This means that this command tells the router to activate the second channel once the first one is THR/255 loaded.

9. You can check the operation of the ISDN using the following commands;

```
Router#show isdn active
Router#show isdn status
Router#show dialer
```

and

```
Router#debug isdn q921
Router#debug isdn q931
Router#debug dialer
```

4.5 How to Configure ISDN Dialer Profiles in a Cisco Router

When would you need this: When you are using ISDN links among more than two nodes.
Special Requirements: The router should have ISDN interface(s).

If you are implementing ISDN between two nodes only, you can refer to the BRI ISDN configuration procedure in Sect. 4.4.

What the dialer profiles do is the mapping of a dial string along with username to a certain destination. This way, the router knows what number to dial for different ISDN destinations using the same link. The main problem you may face without the use of dialer profiles is that the configuration is applied directly to the physical interface. Thus, different logical links will need to use the same IP address and other configuration settings. The dialer profile applies the settings to the interface on on-call basis.

Multiple dialer interfaces may be configured on a router. Each dialer interface is the complete configuration for a destination. The '`interface dialer`' command creates a dialer interface and enters interface configuration mode.

I will assume that you already set the switch type and SPIDs. If you have not done that yet, refer to Sect. 4.4. Let us start the configuration as the following:

1. Create a dialer interface that contains the configuration of the interface to be used with a certain destination.

   `Router(config)#`**`interface dialer INTNO`**
   where INTNO is the dialer interface number that you may choose.

2. Configure the dialer interface as if you are configuring the regular DDR in Sect. 4.4. This configuration can be IP address, encapsulation and authentication types, idle timer, and dialer group for interesting traffic. You can configure the encapsulation and authentication types on the physical interface later, if all of your connections use the same encapsulation and authentication types.

3. Configure a dialer string to this interface, along with a '`dialer remote-name`,'

   `Router(config-if)#`**`dialer string DSTRING`**
   `Router(config-if)#`**`dialer remote-name DESTNAME`**
   where DSTRING is the dial string for the destination and DESTNAME is the name of the destination. Usually, you are supplied with two dial strings for each ISDN end. Just repeat the 'dial string' command once for each dial string.

4. Associate the dialer interface to a dialer pool. This pool will be associated to one or a group of physical interfaces such that the physical interfaces use these dialer settings on on-call basis.

   `Router(config-if)#`**`dialer pool N`**
   where N is the dialer pool number.
   Now, repeat steps 1–4 for as many destinations as you have that can be contacted by this router (using the ISDN network). For the destinations you want to use the same physical interface, give the same dialer pool number (N).

5. After you finish setting the dialer interfaces, one step is left; associating the physical interfaces to the dialer pool. This is done using the following command:

   `Router(config-if)#`**`dialer pool-member N`**
   where N is the dialer pool number that you want this physical interface to be associated with.
   Please note that this command must be issued on the physical interface *not* the dialer interface. You can make the same physical interface a member of more than one dialer pool.

As an optional parameter, you can set priority of the physical interface in the dialer pool if the pool contains more than one physical member. An example is the following,

```
Router(config-if)#dialer pool-member 1 priority 100
```

where 100 is the priority you chose for this physical interface.
If multiple calls need to be placed and only one interface is available, then the dialer pool with the highest priority is the one that dials out.
In general, the dialer pool can be used with any combination of synchronous, asynchronous, BRI, and PRI interfaces.

4.6 How to Configure a Cisco Router as a Frame-Relay Switch

When would you need this: When you are setting up your own Frame-Relay network. This setup is frequently used for lab setup.
Special Requirements: A Cisco router with at least two serial interfaces.

This setup is mainly done for lab experiments because operating a Cisco router as an actual Frame-Relay Switch requires a high number of Serial interfaces.

As a start, you need to keep in mind that when a Cisco router operates as a frame-relay switch, it will stop operating as an IP router. No IP routing processes will occur during the Frame-Relay operation. The router will become exclusively a Frame-Relay Switch.

Before you start the configuration, draw the network topology and mark on it the numbers of DLCIs that will be used. What the frame-relay switch does is receiving a frame with a certain DLCI number from one interface and forwarding it to a different interface after assigning it a different DLCI number. With that said, now we move on to the configuration:

1. Enable Frame-Relay Switching operation on the router's global configuration:

```
Router(config)#frame-relay switching
```

2. Configure the two (or more) serial interfaces that will participate in the frame-relay switching process

```
Router(config-if)#no ip address
Router(config-if)#encapsulation frame-relay
Router(config-if)#logging event subif-link-status
Router(config-if)#logging event dlci-status-change
Router(config-if)#clock rate CLKRT
Router(config-if)#no frame-relay inverse-arp
Router(config-if)#frame-realy inft-type dce
```

where CLKRT is the clock rate of your choice (64,000 is a good choice)
Now compare the frame-relay routing configuration on the same interface,

```
Router(config-if)# frame-relay route INDLCI interface
serial INTNO OUTDLCI
```

where,

INDLCI is the DLCI number of the incoming frame
OUTDLCI is the DLCI number that will be assigned to the outgoing frame
INTNO is the serial interface number to which the frame will be forwarded to be sent out of the router.
Repeat the frame-relay routing command for as much DLCIs as you plan to be passing through this interface. Keep in mind that this command is given at the interface that is receiving the frame-relay frames.

3. After completing the steps of configuration for one of the interfaces in step 2, repeat step 2 on each serial interface you want to be part of the frame-relay switching process.
4. For verification and troubleshooting use the following command to find out the status of each route you have configured on the frame-relay switch:

```
Router#show frame-realy route
```

Chapter 5
Upgrades and Backups

Keywords Cisco · Router · IOS · IOS upgrade · Router upgrade · IOS file name · Show flash · TFTP · TFTP server · Configuration backup · Configuration restore · IOS backup · IOS restore · FTP · FTP server · Copy flash TFTP · Internal flash · Slot0 · Router update · Hyperterminal · Rommon mode · Copy IOS · Partition flash

5.1 Hints and Tips Before Upgrading the IOS of a Cisco Router

Upgrading your router's IOS is a critical operation. You need to be careful and cautious with every command you write. Take a look on these hints and tips before you start upgrading.

1. Before considering upgrading, evaluate the real need to a new IOS. If the router's current IOS covers all the jobs that you need the router to do, no upgrade is needed. Upgrade is usually necessary when you are adding new hardware, the router is not capable of handling what you want, or there is a problem with the old IOS. Sometimes there appear to be some security glitches in the IOS so you might need to upgrade even if the router is performing smoothly.
2. To see the contents of the flash and check for the available space use the following command,

   ```
   Router#show flash
   ```
   if your router has PCMCIA flash, use this command instead,

   ```
   Router#show slot0:
   ```
   and

   ```
   Router#show slot1:
   ```

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1_5, © Mohammed M. Alani 2012

3. If the space is not enough for the old and new copies of IOS together, you will have to erase the old one. *Do not* do that manually using '`delete flash:IOSFILE.bin`'. Once you start copying the new IOS, you will be asked to erase or keep the old contents of the flash. If you have enough space for both copies, do not erase the flash.
4. If the flash of your router is Class B and have more than one bank, you can partition the flash. Partitioning the flash is useful in any copying operations because the router would be able to hold and maintain two different copies of IOS files. Partitioning protects you from the risk of erasing the old copy of IOS accidentally while upgrading. A procedure for flash partitioning is in Sect. 5.9.
5. *Do not* change the IOS file name; neither the old one nor the new one. You must have full understanding of the IOS file name conventions. You can find a brief description of the meanings of the IOS file name in Sect. 5.2.
6. It is always safer to do the upgrade through TFTP server and not through Xmodem. TFTP server's software is easy to master and many distributions of TFTP server are available for free.
7. When upgrading through HyperTerminal (Xmodem), *do not* reload the router before the whole copying process is complete.
8. If you have more than one IOS file on the flash and you do not know which one is currently loaded, use the '`show version`' command to find the name of the loaded IOS file.

5.2 Understanding the IOS File Name Convention

Before planning an upgrade or install of an IOS file, you will need to understand the meaning of the name of each IOS file.

The old IOS file name is usually similar to this form:

```
xxxx-yyy-ww.aaa-bb.bin
```

1. The `xxxx` is the platform. For example:

`c1005` – For 1005 platform
`c1600` – For 1600 platform
`c1700` – For 1700, 1720, and 1750 platforms
`c2500` – For 25xx, 3xxx, 5100, and AO (11.2 and later only) platforms
`c2600` – For 2600 platform
`c2800` – For Catalyst 2800 platform
`c2900` – For 2910 and 2950 platforms
`c3620` – For 3620 platform
`c3640` – For 3640 platform
`c4000` – For 4000 platform (11.2 and later only)
`c4500` – For 4500 and 4700 platforms

2. The yyy is the feature set. For example,

   b For Apple talk support
   boot For boot image
   c For CommServer lite (CiscoPro)
   drag For IOS based diagnostic image
   g For ISDN subset (SNMP, IP, Bridging, ISDN, PPP, IPX, and AppleTalk)
   i For IP sebset (SNMP, IP, Bridging, WAN, Remote Node, and Terminal Services)
   n For IPX support
   q For asynchronous support
   t For Telco return (12.0)
   y For reduced IP (SNMP, IP RIP/IGRP/EIGRP, Bridging, ISDN, and PPP) (c1003 or c1004)
   z For managed modems
   40 For 40 bit encryption
   50 For 50 bit encryption

3. The ww is for the format (where the IOS file runs in the router)

   f For flash
   m For RAM
   r For ROM
   l For the image will be relocated at run time
   The file might also be compressed. The following letters denote the compression type,
   z For zip compression
   x For mzip compression
   w For "STAC" compression
   aaa-bb represent the version of the IOS. It is usually read like this "Version aa.a(bb)". The last part of the IOS file name might contain letters like T (new feature release identifier), S (individual release number), or XR (modular packages).

Cisco follows a packaging model that provides a wide selection of feature sets for the new IOS files. These feature sets are:

a. ipbase—for basic IP features
b. ipvoice—VoIP support
c. advsecurity—advanced security feature.
d. spservices—service provider services
e. entbase—basic enterprise services
f. advipservices—advanced IP services
g. entservices—enterprise services
h. adventerprise—advanced enterprise services

These feature sets have an inheritance structure such that each feature set contains all the features of previous sets with additions. For example, advsecurity feature set contains all features from ipvoice and ipbase and adds more security features to them.

5.3 How to Backup and Restore the Configuration of a Cisco Router

When would you need this: When you plan to implement something new in the configuration, or when you need to copy the configuration from one router to the other, or for regular backups.
Special Requirements: None.

Before starting the procedure of configuration backup or restore, you will need to install TFTP server software on a PC connected to the router Ethernet interface. There are many free downloadable TFTP servers' software on the Internet, however, our recommendation is TFTPd or Free TFTP Server.

Afterwards, you make sure to direct the TFTP server software to the folder that you want to contain the backups, and that the TFTP server has enough free space to contain the backups.

1. Create a console connection with the default settings (9600 baud, 8 databits, 0 parity bits, 1 stop bit, no flow control).
2. Check the connectivity between the router and the TFTP server with the 'ping' command in the privileged mode.
3. Start copying the configuration to the TFTP server:

```
Router#copy run tftp
```

Or

```
Router#copy start tftp
```

Then you will be asked for the IP address of the TFTP server

```
Address or name of remote host []? TFT.PSR.VIP.ADR
```

Afterwards, you will be asked for a destination file name to be saved on the TFTP server

```
Destination filename [Router-confg]? backup_cfg_for__routerX
```

It is better to choose a descriptive name so you would not mix the different configuration files. Now you will see the progress of the operation
!!

```
nnn bytes copied in t.tt secs (rr bytes/sec)
```

The configuration file is usually copied quickly because it is not more than few kilobytes.

The backup procedure is now over. You can open the file copied to the TFTP server with the text editor and view or modify it.
The restore procedure is done by replacing step 3 of the previous procedure with the following:

```
Router#copy tftp run
```
Or

```
Router#copy tftp start
```
Now you will be asked to provide the TFTP server IP address

```
Address or name of remote host []? TFT.PSR.VIP.ADR
```
Then you will be asked for the source file name

```
Source filename []?backup_cfg_for__routerX
Destination filename [running-config]? <<< or [startup-config]
Accessing tftp://TFT.PSR.VIP.ADR/backup_cfg_for_routerX...
Loading backup_cfg_for_router from TFT.PSR.VIP.ADR (via FastEthernet0/0): !
[OK - bbbb bytes]
nnnn bytes copied in t.tt secs (rrr bytes/sec)
```
It is advised that you remove any configuration lines containing 'AAA' commands from the backup file before restoring so you would not have any security problems accessing the router. You can do that with any text editor.

There are two other ways to backup and restore the configuration; FTP and the HyperTerminal.
You can use FTP to backup and restore the configuration by doing the following:

1. Give the router username and password to use for FTP access:

```
Router(config)#ip ftp username YOURUSERNAME
Router(config)#ip ftp password YOURPASSWORD
```

2. Use the following commands for copying the configuration to and from the FTP server:

```
Router#copy run ftp
```
or **copy start ftp**
And

```
Router#copy ftp run
```
or **copy ftp start**
And you will have to give the same info given in step 3 of the previous procedure to complete the transfers.

If you do not have TFTP or FTP servers around, you can use the good old HyperTerminal to backup and restore the configuration by doing the following steps:

1. Create a console connection with the default settings (9600 baud, 8 databits, 0 parity bits, 1 stop bit, no flow control).
2. Issue the following command:

   `Router#terminal length 0`
   This command will cause the show commands results to be displayed continuously without pagination.

3. On the HyperTerminal menu, select "Transfer" and from the transfer menu, select "Capture Text". The Capture Text window will appear.
4. Choose a name for the configuration file to be saved (ex: configuration.txt) and click Start.
5. On the router, issue the command:

   `Router#show run`
   or **`show start`** depending on the configuration you want to backup

6. After you see the whole configuration displayed, on the HyperTerminal menu, go to the "Transfer" menu and select the "Capture Text" submenu and select "Stop" to end the screen capture.
   This concludes the backup. You may also edit the file that you have saved to erase the lines containing '`AAA`' commands to avoid access and security problems that may be caused by the restore operation.

   The restore procedure goes as the following:

1. Open the configuration backup file with a text editor and select all the text by pressing Ctrl-A key combination. Now choose 'Copy' from the Edit menu or simply press Ctrl-C.
2. Go to the HyperTerminal window that is connecting you to the router you want to perform the restore on. Afterwards, go to the privileged mode.
3. From the HyperTerminal menu, open the "Edit" menu and select "Paste to Host"
4. Check the configuration by '**`show run`**' command. If everything sounds fine, use the '`copy run start`' command to save the restored configuration.

5.4 How to Backup an IOS File from a Cisco Router

When would you need this: When you are planning to upgrade the IOS file or you need to copy it to another router.
Special Requirements: None.

Before starting the procedure of IOS file backup, you will need to install TFTP server software on a PC connected to the router Ethernet interface. There are many free downloadable TFTP servers' software on the Internet, however, our recommendation is TFTPd or Free TFTP Server.

Afterwards, you make sure to direct the TFTP server to the folder that you want to contain the backups, and that the TFTP server has enough free space to contain the backups.

1. Create a console connection with the default settings (9600 baud, 8 databits, 0 parity bits, 1 stop bit, no flow control).
2. Check the connectivity between the router and the TFTP server with the '`ping`' command.
3. Start copying the IOS file with one of the following commands:

   `Router#`**`copy flash tftp`**
   Use this command if your router has internal flash memory (ex: 2600). If your router uses PCMCIA flash cards (ex: 3600), use the following command:

   `Router#`**`copy slot1: tftp`**
   or `Slot0`: depending on the file you want to copy

4. Now you will be asked for the IP address of the TFTP server:

   `Address or name of remote host []?` **`TFT.PSR.VIP.ADR`**

5. Afterwards, you will be asked for a destination file name to be saved on the TFTP server

   `Destination filename [cNNNN-N-NN.NNN-NN.bin]?`
   It is better to leave the IOS file name as it is and press 'enter' to avoid any possible confusion at the time of restore.
   Now you will see the progress of the files transfer
   !!
   !!
   !!!
   !!
   !!
   !!

   `[OK - nnnnn bytes]`
   `nnnnnn bytes copied in yy.yyy secs (zzz bytes/sec)`
   For the restore procedure, you can refer to the IOS file upgrade procedure in Sect. 5.5.

5.5 How to Upgrade IOS on a Cisco Router

When would you need this: The upgrade is required when you plan to add more duties to the router or a new hardware module. The installation is also required when the IOS image you have on the router is corrupted.
Special Requirements: The router's flash size should be enough for the new IOS image.

Before starting the procedure of IOS upgrade, you will need to install TFTP server software on a PC connected to the router Ethernet interface. There are many free downloadable TFTP servers' software on the Internet, however, our recommendation is TFTPd or Free TFTP Server.

Afterwards, you should make sure to direct the TFTP server to the folder containing the new IOS image that you have.

We will put down two procedures for two different type of routers; a procedure for routers having Internal Flash (ex: 2600), and a slightly different procedure for routers with PCMCIA flash cards (ex: 3600).

5.5.1 Upgrade Procedure for Cisco Routers with Internal Flash

1. Create a console connection with the default settings (9600 baud, 8 databits, 0 parity bits, 1 stop bit, no flow control).
2. Verify the connectivity between the router and the TFTP server using '`ping`'. Make sure that the router interface and the TFTP server IP addresses are in the same range and the ping is responding well.
3. Although the upgrade will be happening in the flash and the configuration is saved in the NVRAM, make a backup of the configuration. This is recommended in case something goes wrong in the upgrade. Also, make a backup copy of the IOS you already have on the router. In case the new IOS image is corrupted, you will be on the safe side. For the backup process, please refer to the IOS backup procedure in Sect. 5.4 and configuration backup procedure in Sect. 5.3
4. Start the upgrade by the command:

   `Router#`**`copy tftp flash`**
   Now you will be prompted for the IP address of the TFTP server:

   `Address or name of remote host []?` **`TFT.PSR.VIP.ADR`**
   Afterwards, you will be asked for the name of the new IOS file being copied from the TFTP server:

   `Source filename []?` **`cNNNN-N-NN.NNN-NN.bin`**
   The IOS file name is case sensitive.
   Now you will be asked for the destination file name on your router,

`Destination filename []?`**`cNNNN-N-NN.NNN-NN.bin`**

It is preferred to keep it as the source file name, to be able to easily identify the files on the TFTP servers as compared to the ones on the routers. Also, keeping the name means identifying the features of this IOS easily.

Now you will be asked whether to erase the existing file(s) in the flash or not. If you have enough free space on the flash, don't erase the old IOS image, you might need it.

`Erase flash: before copying? [confirm]`

Afterwards, the router starts copying the new IOS file to the router, or start erasing the flash and then copying. If you wish to keep the contents of the flash, just write 'n' and hit enter.

```
Erasing the flash filesystem will remove all files! Continue?
[confirm]y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeee
eeeeeeeeee ...erased
Erase of flash: complete
Loading cNNNN-N-NN.NNN-NN.bin from TFT.PSR.VIP.ADR (via
Ethernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - nnnnnn/mmmmmm bytes]
Verifying checksum... OK (0xAC8A)
nnnnnn bytes copied in tt.tt secs (yyyyy bytes/sec)
```

The copying process takes several minutes; the time differs from network to network. During the copy process, messages are displayed to indicate which file has been accessed.

The exclamation point "!" indicates that the copy process is taking place. Each exclamation point indicates that ten packets have been transferred successfully. A checksum verification of the image occurs after the image is written to flash memory.

5. Before reloading the router, you need to make sure of two things. The first is that the configuration register value is 0x2102. You can check that wit the '`show version`' command. If the configuration register's value is not 0x2102, you will need to set it to that value with the following command:

`Router(config)#`**`config-register 0x2102`**

If you did not erase the contents of the flash, you will need to setup the router to boot from the new IOS file with the following commands:

```
Router(config)#no boot system
Router(config)#boot system flash cNNNN-N-NN.NNN-NN.bin
```

6. If you type the reload command, the router asks you if you want to save the configuration. You need to pay attention to this situation. If the router is in boot mode for instance, it is a subset of the full Cisco IOS software which is running and there is no routing functionality. Therefore, all the routing configuration is automatically erased from the running configuration. Thus, if you save the configuration at this time, you will erase the complete startup-configuration that is already there in the NVRAM and replace it by the incomplete running-configuration. Save the configuration only if you are sure that you have the full configuration in the output of show run. It is *not* necessary to save the configuration to take into account the new config-register if this one has been changed previously. That is done automatically.

```
Router#reload
System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]
Proceed with reload? [confirm]y
```

7. To verify that the new image is loaded after the 'reload', use 'show version' command.

```
00:22:25: %SYS-5-CONFIG_I: Configured from console by
console
Cisco Internetwork Operating System Software
IOS ™ CNNNN Software (CNNNN-N-N), Version NN.N(NN),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 25-Mar-02 20:33 by xxxxx
Image text-base: 0×80008088, data-base: 0×80828788
ROM: System Bootstrap, Version nn.n(n)XA4, RELEASE SOFT-
WARE (fc1)
XXXX uptime is 22 minutes
System returned to ROM by reload
System image file is ''flash: cNNNN-N-NN.NNN-NN.bin '' ←
Check it here
```

In step 1 or after the upgrade, if the router boots into rommon mode or boot mode and you have one of the following cases:

```
rommon 1 > dir flash:
device does not contain a valid magic number
dir: cannot open device ''flash:''
rommon 2 >
```

or

```
router(boot)>
```

```
device does not contain a valid magic number
boot: cannot open ''flash:''
boot: cannot determine first file name on device ''flash:''
```

This means that the flash is empty or the file system is corrupted. In this case, you have to consider using the procedure of Upgrading or Installing the IOS from ROMmon mode in Sect. 5.7.

5.5.2 *Upgrade Procedure for Cisco Routers with PCMCIA Flash*

1. Create a console connection with the default settings (9600 baud, 8 databits, 0 parity bits, 1 stop bit, no flow control). If your router does not boot regularly, refer to Sect. 5.6.
2. Check if you have enough space in the flash card for the new IOS file:

   ```
   Router#dir slot1:
   ```

   If you find that there is not enough space, you can delete one or more files from the flash:

   ```
   Router#delete slot1: FILENAME.bin
   ```

   If you delete on or more files from the flash *do not* reload or powercycle the router until you finish this procedure. The operating system the router using now is loaded to the router's RAM. Thus, if you power-cycle the router before flashing the new IOS, the router will malfunction.

3. Verify the connectivity between the router and the TFTP sever with the 'ping' command. Make sure that the TFTP server software is running and the working directory of the TFTP server contains the new IOS file. It is also advised that you backup the configuration and old IOS file before proceeding. For this purpose, you can refer to IOS backup procedure in Sect. 5.4 and configuration backup procedure in Sect. 5.3.
4. Copy the new IOS file from the TFTP server to the router:

   ```
   Router#copy tftp slot1:
   Address or name of remote host []? TFT.PSR.VIP.ADR
   Source filename []? cNNNN-N-NN.NNN-NN.bin
   Destination filename [cNNNN-N-NN.NNN-NN.bin]?
   Accessing        tftp://TFT.PSR.VIP.ADR/cNNNN-N-NN.NNN-
   NN.bin...
   Erase slot1: before copying? [confirm]n
   ```

   You can say 'no' here because you have already emptied space for the new IOS file

   ```
   Loading cNNNN-N-NN.NNN-NN.bin from TFT.PSR.VIP.ADR (via
   Ethernet1/0):
   ```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - nnnnnnn/mmmmmmmm bytes]
Verifying checksum... OK (0x13F0)
nnnnnnnn bytes copied in tt.ttt secs (rrrrr bytes/sec)
Router#
```

5. Verify the new IOS file in the flash card:

```
Router#dir slot1:
```

6. Direct the router to load the new IOS file in the next boot:

```
Router(config)#no boot system
Router(config)#boot system flash slot1:cNNNNN-N-NN.NNN-NN.bin
```

7. Make sure that the configuration register has the value of 0x2102. This is verified by the '`show version`' command. If the configuration register has a value other than 0x2102, use the following command to change it:

```
Router(config)#config-register 0x2102
```

8. Save the configuration with one of the two following commands:

```
Router#write memory
```

Or

```
Router#copy run start
```

9. Reload the router with '`reload`' command and verify the new IOS version with the '`show version`' command after the reload. This command will also show you the name of the IOS file that has been loaded.

5.6 How to Upgrade IOS of a Cisco Router Using HyperTerminal

When would you need this: When you want to upgrade the IOS file and you do not have TFTP of FTP servers around, or you have a corrupt IOS in the router and the router is not booting up.

Special Requirements: The router flash size should be adequate for the new IOS image, and you should have enough RAM in the router for the operation and temporary storage of the new IOS file.

It is recommended that you backup the old IOS file before the upgrade using the IOS backup procedure in Sect. 5.4, and backup the configuration too using the procedure in Sect. 5.3 if you still have access to the router. Keep in mind that this procedure is not recommended. It is recommended that you upgrade using a TFTP or FTP server from Sect. 5.5. This is because it takes much more time and you do not see an error when it occurs until the copying is finished. To upgrade or install a IOS using HyperTerminal or any other terminal emulation software, do the following steps:

1. Create a console connection with the default settings (9600 baud, 8 databits, 0 parity bits, 1 stop bit, no flow control).
2. Change the baud rate of the console port to its maximum 115,200

```
Router#set baud = 115200
```

3. Reset the console port

```
Router#reset
```
Now you will not get anymore output on the screen until you finish step 4.

4. Change the connection speed of the HyperTerminal by disconnecting and reconnecting with the baud rate of 115200 with all the rest of the settings mentioned in step 1 left the same.
5. Prepare the router for the reception of the new IOS file

```
Router#upload xmodem
```
Now you will have the following message,

```
Ready for X/Modem upload...
[note: no status bar for xmodem transfers, abort with
Control-X or break]
```

6. Send the file from your terminal emulation software. This is done by selecting "Transfer" from the upper menu of HyperTerminal and then "Send File". In the Send File dialog box, choose the new IOS file using the "Browse" button, choose "Xmodem" as the protocol, and then press "Send".
   The sending operation may take a long time, and there is no progress indicator in the router, but you will have a progress indicator in the HyperTerminal. After the copying is finished, you will receive a message,

   ```
   upload: succeeded (ttt seconds)
   ```
   Now the new IOS file is in the router's RAM.

7. If you don't have enough space in the router's flash for the old and new files, delete the old IOS file (this is not recommended though),

```
Router#delete flash:OLD_IOS_FILE.bin
```

8. Save the new IOS file to the flash,

```
Router#save file = NEW_IOS_FILE.bin
```

the NEW_IOS_FILE.bin is a name of your choice for the new IOS file. It is better to use the same name of the original file that was stored on your computer.

9. Direct the router to load the new IOS file at the next startup,

```
Router(config)#no boot system
Router(config)#boot system flash NEW_IOS_FILE.bin
```

10. You can reload the router now, but remember to change back the settings of the HyperTerminal to the 9600 baud to get output on your screen after the reload. If you type the reload command, the router might ask you if you want to save the configuration. If the router is in boot mode for instance, it is a subset of the full Cisco IOS software which is running and there is no routing functionality. Therefore, all the routing configuration is gone in the running configuration and if you save the configuration at this time, then you erase the good startup-configuration in NVRAM and replace it by the incomplete running-configuration. Save the configuration only if you are sure that you have the full configuration in the output of show run. It is *NOT* necessary to save the configuration.

Note

Instead of reloading, you can issue 'boot' command that will boot the new software image. For example:

```
boot flash:NEW_IOS_IMAGE.bin
```

5.7 How to Upgrade or Install IOS on Cisco Router using ROMmon Mode

When would you need this: If your router flash, or IOS file is corrupted, you can use this procedure to install a new IOS file. Although it is not recommended, this procedure can also be used to upgrade the router IOS.
Special Requirements: The router flash size should be enough for the new IOS file.

Before starting the procedure of IOS upgrade or installation, you will need to install TFTP server software on a PC connected to the router Ethernet interface. There are many free downloadable TFTP servers' software on the Internet, however, our recommendation is TFTPd and Free TFTP Server.

After installing the TFTP server software on your computer, make sure to direct the TFTP server to the folder containing the new IOS image that you have.

If you are using this procedure to upgrade the IOS file and router is operating properly, it is preferred to backup the old IOS file before starting the upgrade procedure. For this purpose, refer to the IOS backup procedure in Sect. 5.4.

1. Create a console connection with the default settings (9600 baud, 8 databits, 0 parity bits, 1 stop bit, no flow control).
2. If your flash or IOS file is corrupted and your router goes directly to router boot mode (`Router(boot)#`), go to step 4. If your router has some problems and boots into the ROMmon mode directly(`rommon 1 >` or `>`), go to step 3. If your router boots normally, interrupt the router boot sequence by pressing Ctrl-Break once the router is powered on. This will take you to ROMmon mode with the prompt:

   ```
   rommon 1>
   ```
   Or
   ```
   >
   ```
3. Change the value of the configuration register to 0x2101 to instruct the router to boot into router boot mode. Afterwards, reload the router.
   If you have the '`rommon 1>`' prompt use the commands:

   ```
   rommon 1> confreg 0x2101
   rommon 2> reset
   ```
   While if you have the '>' prompt, use:

   ```
   > o/r 0x2101
   > i
   ```
4. Now you are in the router boot mode with the prompt (`Router(boot)#`), you will need to give a valid IP address and default-gateway address to the router so it can communicate with the TFTP server. This IP address will be assigned to the router interface ethrnet 0/0 or fastethernet 0/0. Make sure that this interface is where you connect the TFTP server to the router.

   ```
   Router(boot)>enable
   Router(boot)#configure terminal
   Router(boot)(config)#interface ethernet 0
   Router(boot)(config-if)#ip address ROU.TER.INT.IPA
   255.255.255.0
   Router(boot)(config-if)#no shutdown
   Router(boot) (config-if)#exit
   Router(boot)(config)#ip default-gateway DEF.AUL.TGW.IPA
   ```
   You can replace Ethernet with fastethernet if this is the type of the interface your router has. The default gateway IP address does not matter if you have the TFTP server in the same network where the router interface is. You can easily set it up to be the IP address of the TFTP server.

5. Check the connectivity between the router and the TFTP server with the 'ping' command.
6. Start the copying of the new IOS file from the TFTP server to the flash.

Router(boot)#**copy tftp flash**
Now you will be asked for the IP address of the TFTP server

Address or name of remote host [255.255.255.255]? **TFT.PSR.VIP.ADR**
Then, the source file name,

Source file name? **cNNNN-N-N.NNN-NNN.bin**
Please note that the file name is case sensitive and make sure that the TFTP server's working directory is the one containing the new IOS file.
Afterwards, you will be asked for a destination file name,

Destination file name [cNNNN-N-N.NNN-NNN.bin]?
It is advised that you keep the file name unchanged for future reference.

```
Accessing file 'cNNNN-N-N.NNN-NNN.bin' on TFT.PSR.VIP.ADR...
Loading cXXXX-X-X.XXX-XXX.bin from TFT.PSR.VIP.ADR (via Ethernet0):
! [OK] Device needs erasure before copying new file
Erase flash device before writing? [confirm]y
Copy 'cNNNN-N-N.NNN-NNN.bin' from server as 'cNNNN-N-N.NNN-NNN.bin'into Flash
WITH erase? [yes/no]yes
Erasing device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading cNNNN-N-N.NNN-NNN.bin from TFT.PSR.VIP.ADR (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!

OK – nnnnnn/yyyyyy bytes]Verifying checksum... OK (0×6526)
Flash device copy took 00:yy:yy [hh:mm:ss]
Router(boot)#
```

7. Change back the configuration register value to 0x2102.

Router(boot)#**configure terminal**
Router(boot)(config)#**config-register 0x2102**

```
Router(boot)(config)#exit
Router(boot)#
```

8. Reload the router

```
Router(boot)#reload
System configuration has been modified. Save? [yes/no]: no
Building configuration...
[OK]
Proceed with reload? [confirm]
```

9. Everything should look fine now, and you should be getting the regular (`Router >`) prompt. To check the version and file name of the new IOS, use the '`show version`' command.

5.8 How to Copy IOS From One Cisco Router to Another

When would you need this: When you want to copy IOS file from one router to another for the purposes of upgrade or install. This is usually required when you do not have a TFTP server around.
Special Requirements: The flash size of the destination router should be adequate for the new IOS file size. The models of both routers must be the same.

On the source router that contains the IOS file that you want to copy, issue the following command:

```
Router(config)#tftp-server flash:/SOURCE-IOS-FILE.bin
```

Where `SOURCE-IOS-FILE.bin` is the name of the IOS file that you want to copy. If you are using a router that has PCMCIA flash car, replace the '`flash:`' with '`slot0:`' or '`slot1:`' in the previous command, depending on the slot that contains the file that you want to copy.

This command will make the router act as a TFTP server. And the rest of the procedure is done on the target router and can be found in Sect. 5.5.

After you complete the copy operation, issue the command to disable the TFTP server on the router:

```
Router(config)#no tftp-server flash:/SOURCE-IOS-FILE.bin
```

5.9 How to Partition Internal Flash Memory of a Cisco Router

When would you need this: When you have enough space in the router's flash and you intend to have two IOS images to load alternatively.

Special Requirements: To partition Flash memory, you must have at least two banks of Flash memory. A bank is a set of four chips. This requirement includes systems that support a single SIMM that has two banks of Flash memory. The minimum partition size is the size of a bank.

On most class B Flash file systems, you can partition banks of Flash memory into separate, logical devices so that the router can hold and maintain two or more different software images.

This partitioning allows you to write software into Flash memory while running software in another bank of Flash memory.

This command is an example of how to partition Flash memory:

```
Router(config)#partition flash partitions SIZE1 SIZE2
```

This following command is for Cisco 1600 and 3600 series routers:

```
Router(config)#partition flash-filesystem: NUMBER-OF-PAR-
TITIONS PARTITION-SIZE
```

All sizes mentioned here are in Megabytes. This task succeeds only if the system has at least two banks of Flash, *and* the partitioning does not cause an existing file in Flash memory to be split across the partitions.

For all platforms except the Cisco 1600 series and 3600 series routers, Flash memory can only be partitioned into two partitions.

For the Cisco 1600 and 3600 series routers, the number of partitions that you can create in a Flash memory device equals the number of banks in the device. Issue the `show flash-filesystem: all` command to view the number of banks on the Flash memory device. The number of partition size entries you set must be equal to the number of specified partitions. For example, the `partition slot0: 2 8 8` command configures two partitions to be 8 MB in size each. The first 8 corresponds to the first partition; the second 8 corresponds to the second partition.

Chapter 6
Security

Keywords Cisco · Router · Telnet · Security · Access-list · SSH · Secure shell · Transport input · VPN · Virtual private network · Site-to-site VPN · VPN configuration

6.1 How to Secure Telnet Sessions Using Access-Lists on a Cisco Router

When would you need this: When you need to set up Telnet on a Cisco Router to facilitate remote configuration.

Special Requirements: None.
The steps to secure a Telnet session with an access-list are very simple. However, we will start by creating a password for the Telnet access on the router as a first step of security:

1. If you expect to use no more than one Telnet session simultaneously, enable only one using the following command in the global configuration mode:

   ```
   Router(config)#line vty 0
   ```
   If you need to initiate more than one Telnet session at the same time, which is highly unlikely, you can write '`line vty 0 4`' or '`line vty 0 15`' depending on the type of the router you are using.

2. Setup a password for the Telnet session:

   ```
   Router(config-line)#password P@ssw0rd
   ```
   where `P@ssw0rd` is a password of your choice.

3. Activate the Telnet password:

   ```
   Router(config-line)#login
   ```

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1_6, © Mohammed M. Alani 2012

4. Configure the Access-List to allow the IP address of your network admin computer that will be allowed to Telnet the router:

```
Router(config)#access-list ACLNO permit host
ADM.INI.PAD.DRS
```

where,
ACLNO is the access-list number of your choice. Since we are creating a standard access-list, the number has to be between 1 and 99.
ADM.INI.PAD.DRS is the IP address of the network admin that will be allowed to Telnet the router.

Note
Remember that Telnet traffic is not encrypted. If you plan to Telnet your router from outside of your network, use SSH instead. SSH configuration can be found in Sect. 6.2.

5. If you want to Telnet the router from more than one computer, repeat step 4 for each IP address that you want to allow the Telnet from. Remember to keep the same access-list number for all the different IP addresses.
6. Apply the access-list to the Telnet line:

```
Router(config)#line vty 0
Router(config-line)#access-class ACLNO in
```

where ACLNO is the number of the access-list that you have configured earlier. This command applies the access-list to the Telnet line on the incoming traffic.

6.2 How to Configure SSH on a Cisco Router

When would you need this: When you need to configure your router remotely through an insecure environment.
Special Requirements: IOS version over 12.1.3.T (with a "k9" in its feature set).

Using Telnet over the Internet is not a smart choice. This is due to the fact that Telnet transports everything in plain text without any kind of encryption. The alternative for that is the use of secure shell host (SSH). SSH encrypts the traffic between the router and the terminal to ensure protection of the content. Let us jump into the configuration now:

1. You need to set up a hostname and domain name because they will be used in generating the security keys used in encryption:

```
Router#config t
Router(config)#hostname ROUTERNAME
ROUTERNAME(config)#ip domain-name
SOMEDOMAIN.COM
```

where,
ROUTERNAME is the hostname of your choice

SOMEDOMAIN.COM is the domain name of your network. If you are not using a domain name, just give any name for the sake of SSH.

2. Generate the keys to be used for the RSA encryption:

   ROUTERNAME(config)#**crypto key generate rsa**

3. Setup the two important parameters of SSH; the connection time-out and the number of authentication retries:

   ROUTERNAME(config)#**ip ssh time-out TOT**
   where TOT is the connection time-out in seconds (ex: for two minutes put 120)
   ROUTERNAME(config)#**ip ssh authenticationretries N**
   where N is the maximum number of authentication retries allowed.
   The settings of these two parameters, or one of them, along with the `crypto key generate rsa` enable SSH

4. Disable Telnet sessions, and setup the router to accept only SSH. Before doing that, it is advised to tryout SSH and make sure it is working properly.

   ROUTERNAME(config)#**line vty 0 15** (or 0 4, depending on the router type)
   ROUTERNAME(config-line)#**transport input ssh**

5. For troubleshooting use the following command:

   ROUTERNAME#**sh ip ssh**

6. As an additional security measure, you can change the port number that SSH uses. By default, SSH uses port number 22. You can change that through the following command:

   ROUTERNAME(config)#**ip ssh port PORTNUMBER**
   where PORTNUMBER is a port number of your choice. Remember to set up your SSH client to contact the new port, not the old 22.

7. To disable SSH, you can use the command:

   ROUTERNAME(config)#**crypto key zeroize rsa**
   This command deletes the RSA key. Hence, SSH will be disabled. If you want to go back to Telnet afterwards, use these commands:
   ROUTERNAME(config)#**line vty 0 15** (or 0 4, depending on the router type)
   ROUTERNAME(config-line)#**transport input telnet**

8. For further security, it is advised that you configure an Access- List to limit the IP addresses that are allowed to initiate SSH sessions with the router. This can be done using the procedure of securing Telnet sessions with an Access-List shown in Sect. 6.1.

6.3 How to Configure Site-to-Site VPN in Cisco Routers

When would you need this: When you want to create a secure tunnel to transfer data between two sites without the use of Virtual Private Network (VPN) concentrator or other security devices.
Special Requirements: The routers used must support IPSec. Most of Cisco routers do. Another need is that both sides use a static public IP address to connect to the Internet.

We will go through the steps to be done on one side and the same steps must be repeated on the other side too. The encryption of data will depend on a shared key. This way we will not need specialized CAs or RSA methodologies. If you have a hub-and-spoke topology refer to the note at the end of this procedure.

1. Create internet key exchange (IKE) key policy. The policy used for our case is policy number 9, because this policy requires a pre-shared key.

```
Router(config)#crypto isakmp policy 9
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
```

2. Setup the shared key that would be used in the VPN,

```
Router(config)#crypto isakmp key VPNKEY address
OTH.ERE.NDI.PAD
```

where,
VPNKEY is the shared key that you will use for the VPN, and remember to set the same key on the other end.
OTH.ERE.NDI.PAD the static public IP address of the other end.

3. Now we set lifetime for the IPSec security associations,

```
Router(config)#crypto ipsec securityassociation lifetime
seconds YYYYY
```

where YYYYY is the associations lifetime in seconds. It is usually used as 86,400, which is one day.

4. Configure an extended access-list to define the traffic that is allowed to be directed through the VPN-link.

```
Router(config)#access-list AAA permit ip
SSS.SSS.SSS.SSS WIL.DCA.RDM.ASK
DDD.DDD.DDD.DDD WIL.DCA.RDM.ASK
```

where,
AAA is the access-list number
SSS.SSS.SSS.SSS WIL.DCA.RDM.ASK is the source of the data allowed to use the VPN-link.
DDD.DDD.DDD.DDD WIL.DCA.RDM.ASK is the destination of the data that need to pass though the VPN-link.

5. Define the transformations set that will be used for this VPN connection,

```
Router(config)#crypto ipsec transform-set
SETNAME TRASET1 TRASET2
```

where,
SETNAME is the name of the transformations set. You can choose any name you like.
TRASET1 and TRASET2 is the transformation set. I recommend the use of "`esp-3des esp-md5-hmac`". You can also use "`esp-3des esp-sha-hmac`". Any one of these two will do the job.

6. After defining all the previous things, you need to create a cyptomap that associates the access-list to the other site and the transform set.

```
Router(config)#crypto map MAPNAME PRIORITY ipsec-
isakmp
Router(config-crypto-map)#set peer
OTH.ERE.NDI.PAD
Router(config-crypto-map)#set transform-set
SETNAME
Router(config-crypto-map)#match address AAA
```

where,
MAPNAME is a name of your choice to the crypto map
PRIORITY is the priority of this map over other maps to the same destination. If this is your only crypto map give it any number, for example 10.
OTH.ERE.NDI.PAD the static public IP address of the other end
SETNAME is the name of the transformations set that we configured in step 5
AAA is the number of the access-list that we created to define the traffic in step 4

7. The last step is to bind the crypto map to the interface that connects the router to the other end.

```
Router(config-if)#crypto map MAPNAME
```

where MAPNAME is the name of the crypto map that we defined in step 6.

Note
If you want to implement multiple VPN connections to multiple sites (i.e., Hub-and-Spoke topology), you can do this by repeating the steps 2–7 (except step 3) for each VPN connection. The different crypto maps and their assignments differentiate between the different VPN connections.

8. Now repeat these VPN configuration steps on the other end, and remember to use the same key along with the same authentication and transform set.
9. For troubleshooting purposes you can use the following commands,

```
ROUTERNAME(config)#show crypto isakmp sa
ROUTERNAME(config)#show crypto ipsec sa
ROUTERNAME(config)#show crypto engine connections active
ROUTERNAME(config)#show crypto map
```

Chapter 7
Miscellaneous Hits and Tips

Keywords Cisco · Router · Configuration tips · Routers tips · Show · Show run · Break key · Simulate break key · Break key not working · Password recovery · Cisco router password · Lost password recovery · Cisco 2600 · Cisco 2500 · Config register · Confreg

7.1 Top 10 Tips for Cisco Routers Configuration

There are few simple things that might help administrators in utilizing their time working with Cisco routers. I gathered the most important 10 things in my point of view:

1. The best sequence of configuring a Cisco router, as I see it, is the following:
   a Set up the hostname with the '`hostname HOSTNAME`' command.
   b Set up the secret password (or enable password) with the '`enable secret PASSWORD`' command.
   c Set up console and Telnet passwords (use the '`logging synchronous`' command at the console) with the '`password PASSWORD`' and '`login`' commands.
   d Encrypt the unencrypted passwords with '`service password-encryption`' command and do not forget to turn it off after you '`show run`'.
   e Set up the interfaces (IP addresses, description, bandwidth, etc.) with '`ip address`', '`bandwidth`', and '`description`' commands
   f Set up the Routing protocols (or static routes)
   g Test the connectivity with '`ping`' and '`traceroute`'
   h Set up the access-lists
   i Test the connectivity (again)

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1_7,

2. Be as descriptive as possible.

   Use the '`description`' command on *all* interfaces. Give useful description in it. Describe the network to which this interface is connected, the bandwidth of the link, the duplex settings, and any other information that you might think useful. Use '`remark`' in writing the access-lists so you would identify the access-list according to its function. And if you find it necessary, use banners.
   Examples:

```
RouterA(config-if)#description This link is connected to
the Accounting LAN
RouterA(config)#access-list 101 remark This list stops the
Telnet to the Marketing net
RouterA(config)#banner motd #This router is connected to
the marketing and accounting LANS#
```

3. Use hotkeys.

   There are many useful hotkeys in the configuration command line environment. Few of the most important are:
   Ctrl-P Recalls the previous command in the history buffer
   Ctrl-N Recalls the next command in the history buffer
   Ctrl-E Goes to the end of the line
   Ctrl-A Goes to the beginning of the line

4. Prevent the router from looking up DNS server for wrong commands.

   When you misspell a command and hit the 'Enter' key, the router does not recognize the command and thinks that it might be a host name. The router, then, tries to contact the DNS server to resolve the name to an IP address so it would Telnet it. This would waste some time, especially when you have not set up a valid DNS server (because the router will broadcast the request and waits for a DNS server to reply). To turn this off, use the '`transport preferred none`' command in the console and vty lines.
   Example:

```
RouterA(config)#line con 0
RouterA(config-line)#transport preferred none
```

5. Set up the Bandwidth of serial interfaces.

   Use the '`bandwidth`' command for setting the bandwidth of *all* serial interfaces to guarantee the correct calculation of routing table. The bandwidth of a serial link is dependent on the type of WAN connection you are using. Unlike Ethernet or FastEthernet, serial interfaces cannot automatically detect the bandwidth of the link. And the bandwidth of the actual link might be different from the small link between the serial interface and the modem or CSU/DSU device you are using. Also remember to write the bandwidth after the '`bandwidth`' command in Kilobits per second.
   Example:

```
RouterA(config)#int serial 0
RouterA(config-if)#bandwidth 1024
```
This means the link bandwidth is 1 Mbit/second

6. Turn off Auto-summarization of routing updates when using subnetted addresses.

   If you are using subnetting, remember use the '`no autosummary`' command to turn off auto-summarization when using routing protocols that support it, like OSPF.
   Example:
   ```
   RouterA(config)#no auto-summary
   ```

7. Turn off split-horizon in two cases.

   The first is when you are doing inter-VLAN routing. This is because updates from one VLAN cannot pass to other VLANs. The second case is when you are using Frame Relay to connect one site to multiple sites.
   Example:
   ```
   RouterA(config-if)#no ip split-horizon
   ```

8. The '`show`' command is your best friend.

   Whenever you are in trouble, or even if you are not in trouble, yet your best friend comes up; the 'show' command. The most widely used '`show`' commands are the following:
   `show version`—Shows a large amount of information such as the IOS version, the configuration register value, and the interfaces available.
   `show ip route`—Shows the routing table
   `show ip interface`—Shows the access-lists applied to interfaces
   `show access-list`—Shows the contents of access-lists
   `show ip protocols`—Shows information about the routing protocols currently running.
   `show cdp neighbor detail`—Shows detailed information about neighboring devices.
   `show interface`—Shows status information about interfaces.
   `show run`—Shows the running configuration, i.e., all the commands now in action.

9. Keep the IP addresses of servers and printers out of the DHCP pool.

   When using the router as a DHCP server, *do not* forget to exclude the addresses of servers, router interfaces, and printers off the DHCP pool.
   Example:
   ```
   RouterA(config)#ip dhcp excluded-address 192.168.0.1
   RouterA(config)#ip dhcp excluded-address 192.168.0.1
   192.168.0.10
   ```
   You can use a single IP address in this command or a start-IP and end-IP to define a range of exclusions.

10. Keep a scheduled '`reload`' when configuring a router remotely.

    When you are configuring a router remotely, you might do something wrong and lose the connectivity with the router. In this case, you will need to restart the router physically. There are chances that no one is around the router to restart it for you. You can solve this by yourself by using the '`reload in MM`' command. This command schedules a reload after `MM` minutes. So, before you start nosing around the router remotely, issue this command and schedule a reload. If something goes wrong and you loose the connectivity with the router, the router will reload and you get back in business. If things go smooth and you do not need to reload after all, you can issue a '`reload cancel`' command to stop the scheduled restart from happening.

7.2 Ten `show` Commands Everybody Needs to Know in Cisco Routers

Some commands in the Cisco router configuration are just irreplaceable. The '`show`' commands are the most widely used in Cisco routers. Here is a list of the 10 mostly used of these '`show`' commands.

1. **`show running-config`**

   This command shows the complete configuration that is running currently. Using it you can troubleshoot almost all issues regarding routing, filtering, secure access, and many other issues. Using it before you start configuring the router would give you a clear idea of what services and protocols are operating by default and which are turned off by default.

2. **`show startup-config`**

   This command shows the configuration that is saved on the NVRAM. It is helpful in knowing the configuration that will be applied the next time the router is reloaded. This command also comes handy if you need to know the configuration that was loaded at the startup of the router before you made changes to it.

3. **`show interface`**

   This command shows status and statistics of interfaces. This command is almost always needed in troubleshooting routing and link issues. Information shown using this command includes interface IP address and subnet mask, interface status, encapsulation type, bandwidth, and many other important indicators about the interface operation.

4. **show ip route**

   This command shows the routing table. This table helps you in finding out the next hop for each and every routable packet. It is the first indicator to point a problem in routing.

5. **show ip protocols**

   This command shows the active routing protocols on the router and what networks are these protocols advertising. It also shows the sources of routing updates received at this router. It is very useful in troubleshooting routing issues.

6. **show access-list**

   This command shows the contents of each access-list. It is very useful in troubleshooting filtering issues. Note that this command does not show you where each access-list is applied.

7. **show ip interface**

   This command displays information about IP protocol and the interface. This command shows which access-lists are applied at the interfaces and in which direction. This kind of information is not shown by the 'show access-list' command. However, you can find out which access-list is applied where by using 'show run' also.

8. **show cdp neighbor detail**

   This command displays detailed information about the neighboring devices such as IP addresses, platforms, and host names. This command can be useful in troubleshooting connectivity issues, and can also be used in finding out how devices are connected to each other when you have no cleary-drawn network map.

9. **show version**

   This command shows detailed information about the IOS. It shows the file name of the IOS along with the version of the IOS and value of the configuration register. The configuration register is a set of bits that controls the boot sequence of the router. This command is the only command used to show this register's value.

10. **show flash** or **show slot0**

    This command is used to view the contents of the flash, the size of the IOS file(s), and the size of the flash and how much of it is free. It is necessary in upgrading or installing IOS files.

7.3 How to Simulate Break Key Sequence in a Cisco Router

When would you need this: When you are recovering a lost password and the required 'Ctrl-Break' key combination is not working.
Special Requirements: None.

First of all, you have to make sure that you are pressing the correct key sequence. There are few, slightly different, keys to press to break the router boot sequence in different routers and different terminal emulation software. Table 7.1 shows a list of different keystrokes to interrupt the router boot sequence.

The auxiliary (AUX) port is not active during the boot sequence of a router. Therefore, it is of no use to send a break through the AUX port. You need to have connection to the console port, and have these default settings:

Baud rate: 9600
Parity: None
Data bits: 8
Stop bits: 1
Flow control: None

Until here, things are supposed to be going smooth. If you have everything set right, and you press the correct key strokes during router initialization (within the first 60 s of router startup), you will be transferred to the ROM Monitor mode.

If the above is not working, you might consider the following notes:

- If you are using the HyperTerminal of Windows NT, you might consider upgrading the HyperTerminal. Some versions of Windows NT have hyperterminal software that cannot send the correct break key signal.
- If you are using a DB9-to-USB converter to connect to the console port, you might need to connect to a DB9 port directly. Not all converters of this type can convey the correct break sequence.
- If you still do not know the exact reason why this is not working, you should consider simulating the break key sequence.

To simulate the break key sequence, go through the following steps carefully:

1. Connect to the router with these terminal settings:

   Baud rate: 1200
   Parity: None
   Data bits: 8
   Stop bits: 1
   Flow control: None
   You will no longer see any output on your screen, and this is normal.

2. Power cycle (switch off and then on) the router and press the SPACEBAR for 10–15 s in order to generate a signal similar to the break sequence.
3. Disconnect your terminal, and reconnect with a 9,600 baud rate. You enter the ROM Monitor mode.

Table 7.1 Boot sequence interruption key combinations

Terminal emulation software	Operating system	Key combination
Hyperterminal	Windows 7, Vista, XP, and Server	Ctrl-Break
Kermit	Unix	Ctrl-\I or Ctrl-\B
Minicom	Linux	Ctr-A F
SecureCRT	Windows	Ctrl-Break
Telnet	–	Ctrl-] then type `send break`
Z-Terminal	Mac	Command-B

If all of this fails, you should consider trying a different PC or emulation software.

7.4 How to Recover Cisco 2600 Router's Password

When would you need this: When you forget the secret, enable, or console password of a 2600-series Cisco Router.

Special Requirements: None.

1. Interrupt the router booting operation. This is done by pressing (Ctrl + Break) key simultaneously as soon as you turn on the router. This step will get you to the ROM monitor mode (`rommon`).

   You will see something similar (not necessarily identical) to the following:

   ```
   System Bootstrap, Version 11.3(2)×A4, RELEASE SOFTWARE
   (fc1)
   Copyright (c) 1999 by cisco Systems, Inc.
   TAC:Home:SW:IOS:Specials for info
   PC = 0×fff0a530, Vector = 0×500, SP = 0×680127b0
   C2600 platform with 32768 Kbytes of main memory
   PC = 0×fff0a530, Vector = 0×500, SP = 0×80004374 monitor:
   command ''boot'' aborted due to user interrupt
   rommon 1 >
   ```

   The (`rommon 1 >`) prompt is for the ROM monitor mode. If you are having a problem interrupting the boot sequence of the router, you might be interested in the previous procedure to simulate break key sequence in Sect. 7.3.

2. Now you should change the value of the configuration register in order to make the router neglect the contents of the NVRAM in the next boot up. This is achieved using the following command:

   `rommon 1 >` **`confreg 0x2142`**

   This command will change the sixth bit (originally the configuration register is 0x2102) to one. By doing so, the router will act as new in the next boot despite the fact that the Startup configuration is not erased.

3. Perform a restart to the router using the following command:

```
rommon 1 > reset
```

4. The router will now restart and ask you if you want to use the setup mode; choose no. Now, in order not to lose the configuration that you already have in the router, you should go to the privileged mode and perform:

```
Router#copy start run
```

This will get you back your old configuration but with one exception, you already are in the privileged mode without having to know the password.
Now you choose a new password or passwords if you may:

```
Router(config) #enable secret YOURPASSWORD
```

You can also put new console and Telnet passwords if necessary.

5. To get things going back to normal, change the value of the configuration register to its original form (0x2102) using the following global configuration command:

```
Router(config)#config-register 0x2102
```

6. Save the configuration including the new passwords that you know:

```
Router#copy run start
```

7. Reload and you are good to go:

```
Router#reload
```

7.5 How to Recover Cisco 2500 Router's Password

When would you need this: When you loose the secret, enable, or console password of a 2500 Cisco Router.
Special Requirements: None.

1. Interrupt the router booting operation. This is done by pressing (Ctrl + Break) keys simultaneously as soon as you turn on the router. This step will get you to the ROM monitor mode (rommon).

You will see output similar (but not necessarily identical) to the following:

```
System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986–1996 by cisco Systems
2500 processor with 14336 Kbytes of main memory
Abort at 0×1098FEC (PC)
>
```

The (>) prompt is for the ROM monitor mode. If you are having a problem interrupting the boot sequence of the router, take a look into the procedure to simulate break key sequence in Sect. 7.3.

2. Change the value of the configuration register in order to make the router neglect the contents of the NVRAM in the next boot up. This is achieved using the following command:

   > **o/r 0x2142**

   This command will change the sixth bit (originally the configuration register is `0x2102`) to one. By doing so, the router will act as new in the next boot, i.e., the router will not look for the startup config in the NVRAM. The startup configuration will not be erased.

3. Perform a restart to the router using the following command:

   > **i**

   The (**i**) stands for (initialize).

4. The router now will restart and ask you if you want to use the setup mode; choose no. Now, in order not to lose the configuration that you already have in the router, you should go to the privileged mode and perform:

   `Router#`**copy start run**

   This will get you back your old configuration but with one exception, you already are in the privileged mode without having to know the password.
   Now you put a new password:
   `Router(config) #`**enable secret YOURPASSWORD**
   You can also put new console and Telnet passwords.

5. To get things back to normal, change the value of the configuration register to its original form (`0x2102`) using the following global configuration command:

   `Router(config) #`**config-register 0x2102**

6. Now you should save the configuration including the new passwords that you know:

   `Router#`**copy run start**

7. Now reload and you are good to go:

   `Router#`**reload**

References

Configuring RIP. http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1crip.html

Configuring EIGRP. http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1ceigrp.html

Configuring OSPF. http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1cospf.html

Configuring Integrated IS-IS. http://www.cisco.com/en/US/docs/ios/11_3/np1/configuration/guide/1cisis.html

Per-Packet Load Balancing. http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/pplb.html

Cisco IOS DHCP Server. http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/Easyip2.html

Configurable DHCP Client. http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtdhcpcf.html

Configuring Network Address Translation: Getting Started. http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml

Configuring InterVLAN Routing and ISL/802.1Q Trunking on a Catalyst 2900XL/3500XL/2950 Switch Using an External Router. http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a00800949fd.shtml

Cisco DSL Router Configuration and Troubleshooting Guide. http://www.cisco.com/en/US/tech/tk175/tk15/technologies_configuration_example09186a008015407f.shtml

Understanding and Configuring PPP CHAP Authentication. http://www.cisco.com/en/US/tech/tk713/tk507/technologies_tech_note09186a00800b4131.shtml

HDLC Back-to-Back Connections. http://www.cisco.com/en/US/tech/tk713/tk317/technologies_configuration_example09186a00800944ff.shtml

Configuring ISDN BRI. http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_cfg_sdn_bri_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Configuring ISDN DDR with Dialer Profiles. http://www.cisco.com/en/US/tech/tk801/tk133/technologies_configuration_example09186a0080093c2e.shtml

Cisco – Configuring Frame-Relay Switching. http://www.cisco.com/warp/public/125/fr_switching.pdf

White Paper: Cisco IOS and NX-OS Software Reference Guide. http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Backup and Restore of Configuration Files. http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a008020260d.shtml

Software Upgrade Procedure. http://www.cisco.com/en/US/products/ps5855/products_tech_note09186a00801fc986.shtml

How To Copy a System Image from One Device to Another. http://www.cisco.com/en/US/products/hw/routers/ps233/products_tech_note09186a00800a6744.shtml

M. M. Alani, *Guide to Cisco Routers Configuration*, SpringerBriefs in Computer Science,
DOI: 10.1007/978-1-4471-4246-1, © Mohammed M. Alani 2012

How to Upgrade from ROMmon Using the Boot Image. http://www.cisco.com/en/US/products/hw/routers/ps214/products_tech_note09186a0080110ed1.shtml
How to Partition Internal Flash Memeory. https://supportforums.cisco.com/docs/DOC-4062
Configuring IP Access Lists. http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml
Configuring Secure Shell on Routers and Switches Running Cisco IOS. http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml
Cisco IOS VPN Configuration Guide: Site-to-Site and Extranet VPN Business Scenarios. http://www.cisco.com/en/US/docs/security/vpn_modules/6342/configuration/guide/6342site3.html
Standard Break Key Sequence Combinations During Password Recovery. http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080174a34.shtml
Password Recovery Procedure for the Cisco 2600 and 2800 Series Routers. http://www.cisco.com/en/US/products/hw/routers/ps259/products_password_recovery09186a0080094675.shtml
Password Recovery Procedure for the Cisco 2000, 2500, 3000, 4000, AccessPro, 7000 (RP), AGS, IGS, and STS-10x. http://www.cisco.com/en/US/products/hw/routers/ps233/products_password_recovery09186a0080094795.shtml