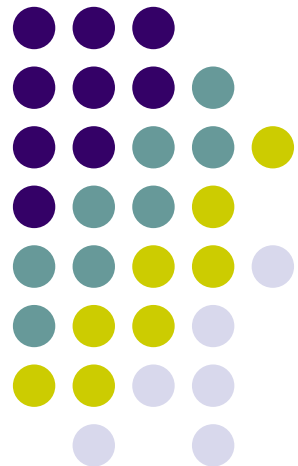
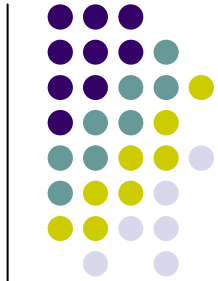
CCNA2 Final Exam Review

Chapters 1 - 11

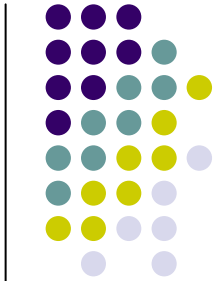


Overview



- Router functions
  - Selection of best path based on logical addressing
  - Segmentation of Local Area Networks
  - Packet switching

1.1.1 Introduction to WANs



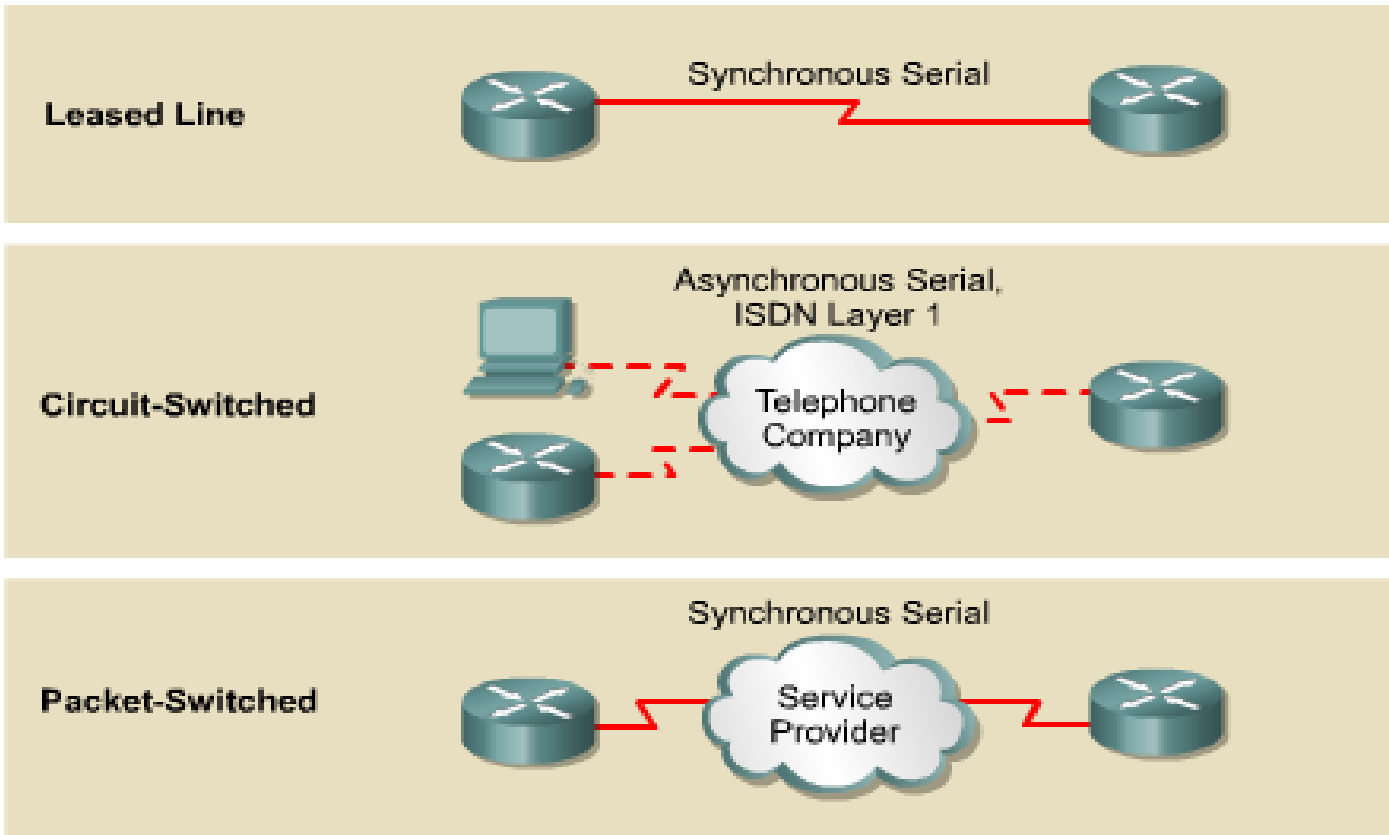
- These are the major characteristics of WANs:
- They connect devices that are separated by wide geographical areas.
- They use the services of carriers such as the Regional Bell Operating Companies (RBOCs), Sprint, MCI, VPM Internet Services, Inc., and Altantes.net.
- They use serial connections of various types to access bandwidth over large geographic areas.

1.2.7 Connecting WAN interfaces

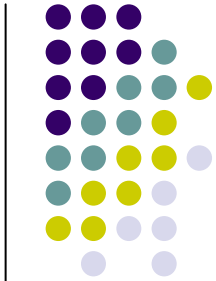
WAN Types

FIGURES

1
2
3
4

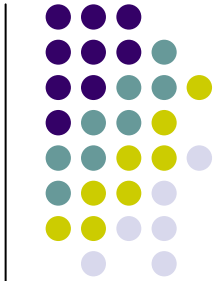


2.2.1 Initial startup of Cisco routers



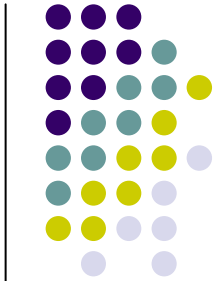
- When a Cisco router powers up, it performs a power-on self test (POST). During this self test, the router executes diagnostics from ROM on all hardware modules. These diagnostics verify the basic operation of the CPU, memory, and network interface ports. After verifying the hardware functions, the router proceeds with software initialization.
- After the POST, the following events occur as the router initializes:

2.2.1 Initial startup of Cisco routers



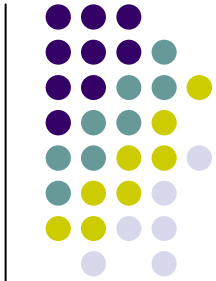
- **Step 1**The generic bootstrap loader in ROM executes.
- **Step 2**The IOS can be found in several places. The boot field of the configuration register determines the location to be used in loading the IOS.
- **Step 3**The operating system image is loaded.
- **Step 4**The configuration file saved in NVRAM is loaded into main memory and executed one line at a time.
- **Step 5**If no valid configuration file exists in NVRAM, the operating system searches for an available TFTP server. If no TFTP server is found, the setup dialog is initiated.

2.2.1 Initial startup of Cisco routers



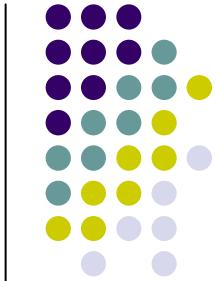
- During the setup process, **Ctrl-C** can be pressed at any time to terminate the process.
- If no valid configuration file exists in NVRAM, the operating system searches for an available TFTP server. If no TFTP server is found, the setup dialog is initiated.

2.2.3 Examining the initial router bootup



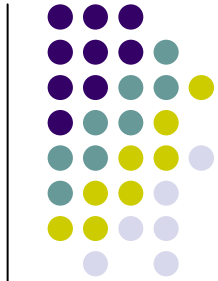
- The factory-default setting for the configuration register is 0x2102, which indicates that the router should attempt to load a Cisco IOS image from flash memory.

3.1.3 Configuring router passwords



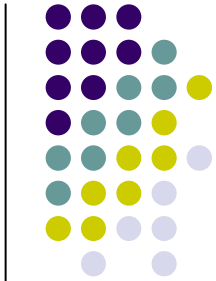
- A password must be set on one or more of the virtual terminal (VTY) lines for users to gain remote access to the router using Telnet.
- Typically Cisco routers support five VTY lines numbered 0 through 4, although different hardware platforms support different numbers on VTY connections.
- Often the same password is used for all lines but sometimes one line is set uniquely to provide a fall-back entry to the router if the other four connections are in use.

3.1.5 Configuring a serial interface



- A serial interface can be configured from the console or through a virtual terminal line. To configure a serial interface follow these steps:
  - Enter global configuration mode
  - Enter interface mode
  - Specify the interface address and subnet mask
  - Set clock rate if a DCE cable is connected. Skip this step if a DTE cable is connected.
  - Turn on the interface

3.2.2 Interface descriptions



- An interface description should be used to identify important information such as a distant router, a circuit number, or a specific network segment. A description of an interface can help a network user remember specific information about the interface, such as what network the interface services.

3.2.4 Login banners

- Message of the Day banners will appear when:
  - Telnetting into the router
  - Configuring the router for the first time
  - Using the console port to check current configurations

3.2.6 Host name resolution

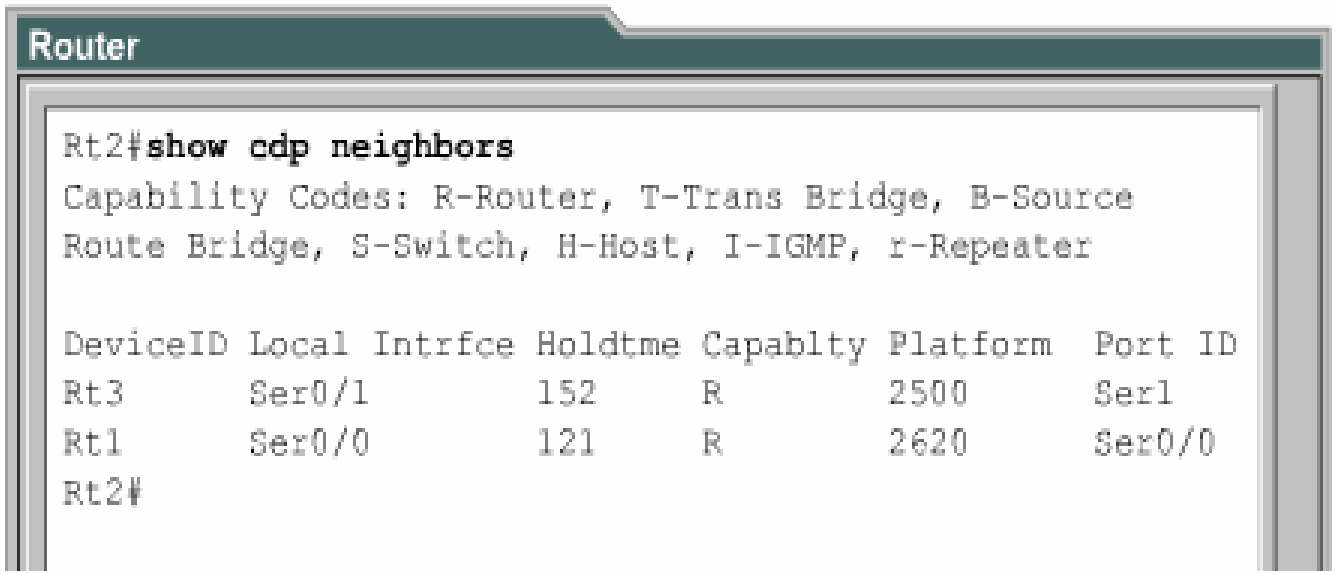
The following is an example of the configuration of a host table on a router:

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

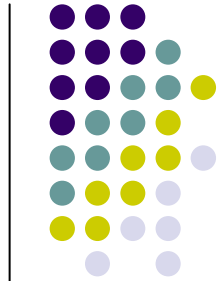
4.1.1 Introduction to CDP

- Cisco Discovery Protocol (CDP) is a Layer 2 protocol that connects lower physical media and upper network layer protocols.
- CDP is used to obtain information about neighboring devices.
- CDP is media and protocol independent, and runs on all Cisco equipment over the Subnetwork Access Protocol (SNAP).
- Each device configured for CDP sends periodic messages, known as advertisements, to multiple routers.

4.1.3 Implementation, monitoring, and maintenance of CDP

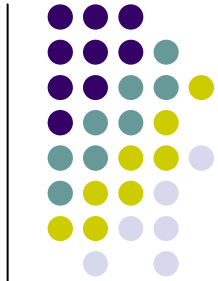


4.2.1 Telnet



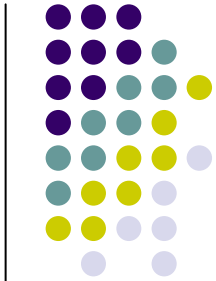
- Telnet is a virtual terminal protocol that is part of the TCP/IP protocol suite.
- It allows connections to be made to remote hosts.
- Telnet provides a network terminal or remote login capability.
- Telnet is an IOS EXEC command used to verify the application layer software between source and destination.
- This is the most complete test mechanism available.

4.2.1 Telnet



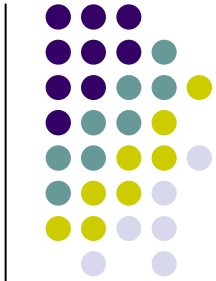
- A router can have multiple simultaneous incoming Telnet sessions.
- The range zero through four is used to specify five VTY or Telnet lines.
- These five incoming Telnet sessions could take place at one time.

4.2.2 Establishing and verifying a Telnet connection



- To initiate a Telnet session any of the following alternatives can be used:
- Denver>**connect paris**
  Denver>**paris**
  Denver>**131.108.100.152**
  Denver>**telnet paris**
- A hostname table or access to DNS for Telnet must be present for a name to work.

5.1.3 Using the boot system command



- **ROM** – If flash memory is corrupted and the network server fails to load the image, booting from ROM is the final bootstrap option in software. However, the system image in ROM will likely be a subset of the Cisco IOS that lacks the protocols, features and configurations of the full Cisco IOS. Also, if the software has been updated since the router was purchased, the router may have an older version stored in ROM.

5.1.3 Using the boot system command

Boot IOS from TFTP Server

FIGURES

1

2

3

```
Router#configure terminal
Router(config)#boot system tftp IOS_image 172.16.13.111
 [Ctrl-Z]
Router#copy running-config startup-config
```

5.1.3 Using the boot system command

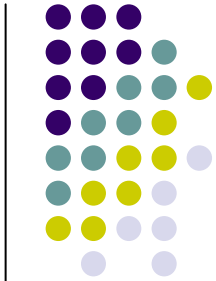
- **show-running config** will indicate if a boot system statement is configured on a router.

5.1.4 Configuration register

- To configure the system to use the boot system commands in NVRAM, set the configuration register to any value from 0x*nnn*2 to 0x*nnn*F, where *nnn* represents the previous value of the non-boot field digits. These values set the boot field bits to a value between 0010 and 1111 binary. Using boot system commands in NVRAM is the default.

Value	Description
0xnnn0	Use ROM monitor mode (manually boot using the **b** command)
0xnnn1	Automatically boot from ROM (default if router has no Flash)
0xnnn2 to 0xnnnF	Examine NVRAM for boot system commands (0xnnn2 is the default if the router has Flash)

5.1.4 Configuration register



- To enter the ROM monitor mode, set the configuration register value to 0x*nnn*0, where *nnn* represents the previous value of the non-boot field digits. This value sets the boot field bits to 0000 binary. From ROM monitor, boot the operating system manually by using the **b** command at the ROM monitor prompt.

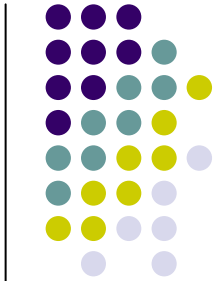
6.1.3 Configuring static routes

- Use the following steps to configure static routes:
  - Determine all desired destination networks, their subnet masks, and their gateways. A gateway can be either a local interface or a next hop address that leads to the desired destination.
  - Enter global configuration mode.
  - Type the **ip route** command with a destination address and subnet mask followed by their corresponding gateway from Step one. Including an administrative distance is optional.
  - Repeat Step three for as many destination networks as were defined in Step one.
  - Exit global configuration mode.
  - Save the active configuration to NVRAM by using the **copy running-config startup-config** command.

6.1.4 Configuring default route forwarding

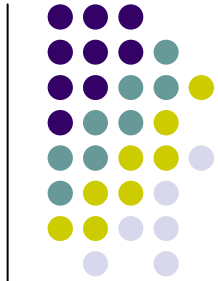
- Use the following steps to configure default routes:
- Enter global configuration mode.
- Type the **ip route** command with 0.0.0.0 for the destination network address and 0.0.0.0 for the subnet mask. The gateway for the default route can be either the local router interface that connects to the outside networks or the IP address of the next-hop router. In most cases, it is preferred that the IP address of the next hop router is specified.
- Exit global configuration mode.
- Save the active configuration to NVRAM by using the **copy running-config startup-config** command.

6.2.6 Link-state routing protocol features



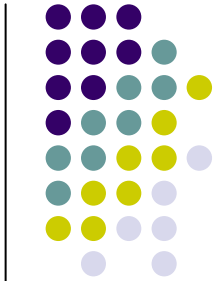
- OSPF
  - Functions as a link-state routing protocol
  - Floods updates as topology changes occur
  - Created as a proprietary routing protocol

7.2.1 RIP routing process



- When a router receives a routing update that contains a new or changed entry, the TTL value is increased by 1 to account for itself as a hop in the path. If this causes the TTL to be incremented beyond 15, it is considered to be infinity and the network destination is considered unreachable.

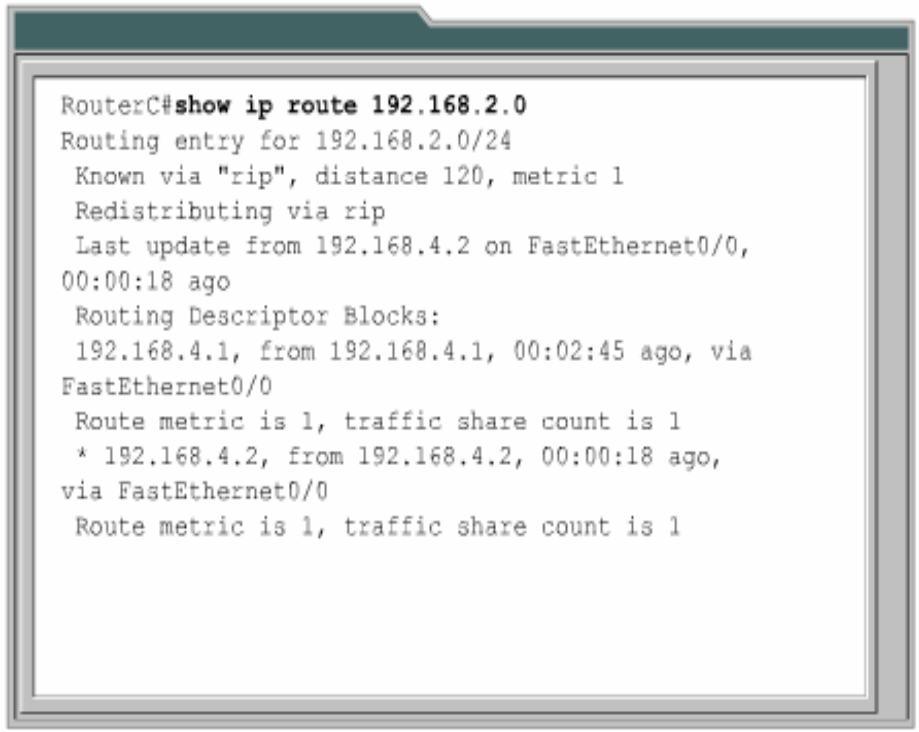
7.2.4 Common RIP configuration issues



- To control the set of interfaces that will exchange routing updates, the network administrator can disable the sending of routing updates on specified interfaces by configuring the **passive-interface** command.

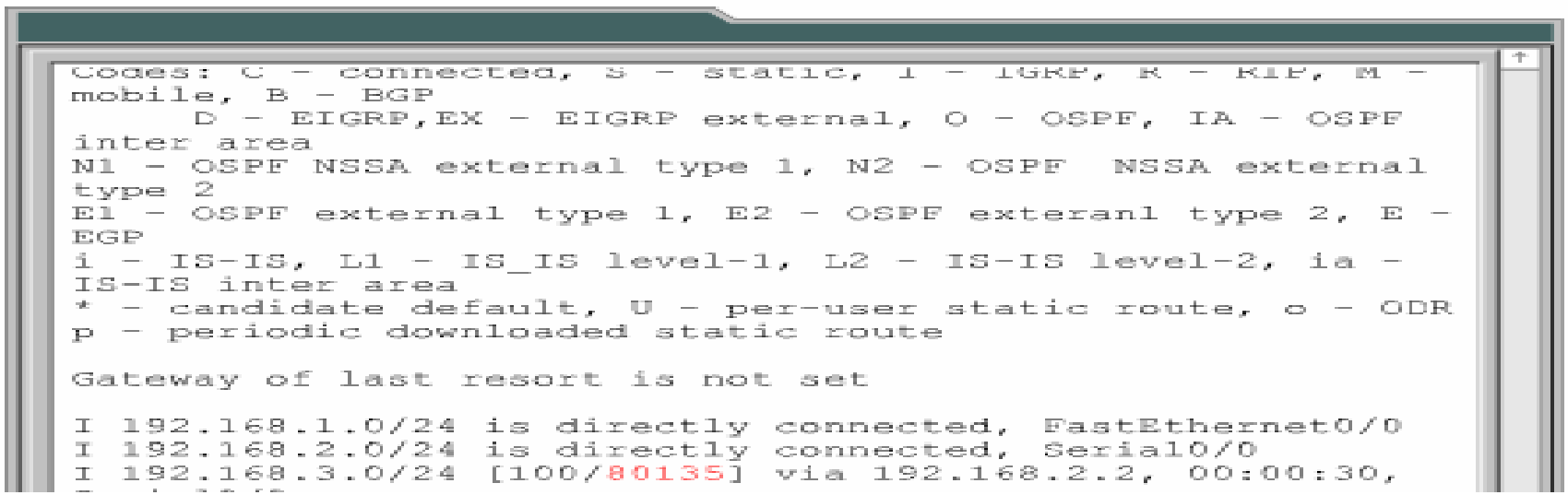
7.2.8 Load balancing with RIP

- Because the metric for RIP is hop count, no regard is given to the speed of the links.
- Equal cost routes can be found by using the **show ip route** command.
- Notice there are two routing descriptor blocks. Each block is one route. There is also an asterisk (*) next to one of the block entries. This corresponds to the active route that is used for new traffic.



7.3.2 IGRP metrics

- IGRP uses a **composite metric**. This metric is calculated as a function of bandwidth, delay, load, and reliability. By default, only bandwidth and delay are considered.



7.3.2 IGRP metrics

- The metrics that IGRP uses are:
- **Bandwidth** – The lowest bandwidth value in the path
- **Delay** – The cumulative interface delay along the path
- **Reliability** – The reliability on the link towards the destination as determined by the exchange of keepalives
- **Load** – The load on a link towards the destination based on bits per second
- **MTU** – The Maximum Transmission Unit value of the path.

9.3.1 Troubleshooting Layer 1 using show interfaces

- The first parameter refers to the hardware layer and essentially reflects whether the interface is receiving the Carrier Detect (CD) signal from the other end of the connection. If the line is down, a problem may exist with the cabling, equipment somewhere in the circuit may be powered off or malfunctioning, or one end may be administratively down. If the interface is administratively down it has been manually disabled in the configuration.

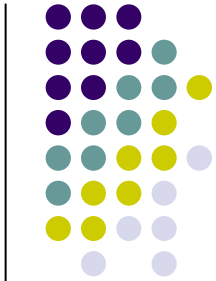
```
Router#show interface serial 0/0

Serial 0/0 is up, line protocol is up

Hardware is cxBus serial
Description: 56Kb Line San Jose - MP
```

Carrier Detect (Line Status) Layer 1

Keepalives Layer 2

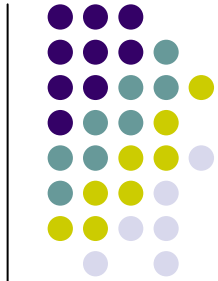
```
Serial 0/0 is up, line protocol is up                    Operational.
Serial 0/0 is up, line protocol is down                  Connection Problem
Serial 0/0 is down, line protocol is down                Interface Problem
Serial 0/0 is administratively down, line protocol is down   Disabled
```

9.3.7 Introduction to debug



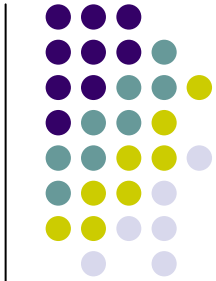
- If a telnet session is being used to examine the router, then the **debug** output and system messages can be redirected to the remote terminal.
- This is done through the telnet session by issuing the **terminal monitor** command.

11.1.2 How ACLs work



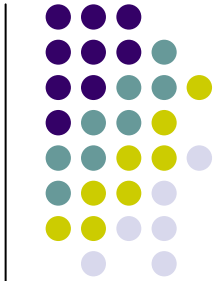
- As a review, ACL statements operate in sequential, logical order.
  - If a condition match is true, the packet is permitted or denied and the rest of the ACL statements are not checked.
  - If all the ACL statements are unmatched, an implicit "deny any" statement is placed at the end of the list by default and any packets will be dropped.
  - Even though the "deny any" is not visible as the last line of an ACL, it is there and it will not allow any packets not matched in the ACL to be accepted.

11.1.3 Creating ACLs



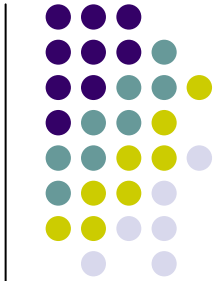
- These basic rules should be followed when creating and applying access lists:
  - One access list per protocol per direction.
  - Standard access lists should be applied closest to the destination.
  - Extended access lists should be applied closest to the source.
  - Use the inbound or outbound interface reference as if looking at the port from inside the router.
  - Statements are processed sequentially from the top of list to the bottom until a match is found, if no match is found then the packet is denied.
  - There is an implicit deny at the end of all access lists. This will not appear in the configuration listing.

11.1.3 Creating ACLs



- Access list entries should filter in the order from specific to general. Specific hosts should be denied first, and groups or general filters should come last.
- The match condition is examined first. The permit or deny is examined ONLY if the match is true.
- Never work with an access list that is actively applied.
- Use a text editor to create comments outlining the logic, then, fill in the statements that perform the logic.

11.2.2 Extended ACLs



- The **ip access-group** command links an existing extended ACL to an interface. Remember that only one ACL per interface, per direction, per protocol is allowed. The format of the command is:
- Router(config-if)#**ip access-group** *access-list-number* {in | out}