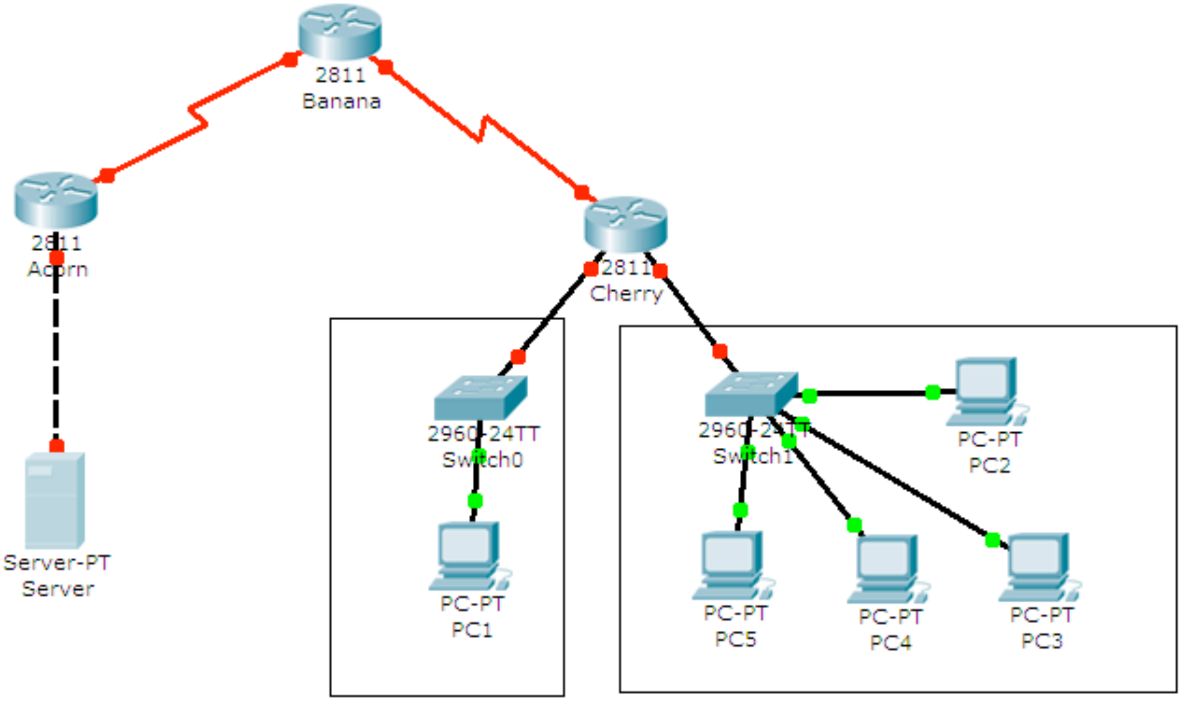
ACLs & AAA



Device	Interface	IP Address	Subnet Mask
Acorn	FA0/0	80.11.69.1	255.255.255.0
Acorn	S0/2/0	10.1.1.1	255.255.255.252
Banana	S0/2/0	10.1.1.2	255.255.255.252
Banana	S0/3/0	10.2.2.2	255.255.255.252
Cherry	S0/3/0	10.2.2.1	255.255.255.252
Cherry	FA0/0	192.168.1.1	255.255.255.0
Cherry	FA0/1	192.168.2.1	255.255.255.0

Tasks

Open the `Labweek4-Topology.pkt` file. To solve the following tasks, DO NOT configure anything on the switches

The hosts' and server's IP addresses have already been configured for you. DO NOT change them.

1. Important! „?" and „tab":

- Remember to type „`?`" in all configuration modes to list the commands available to you. The „`?`" can be used to list all the forms of a certain command, too. Simply type „`?`" after the first word in the command and you will get a list of parameters that you can use to continue the command. For example, typing `configure ?` will return a list in which you will find `terminal` as an option.
- The „tab" key autocompletes the words that make up commands, as long as there is no confusion. For example, pressing „tab" after typing `c` will not give you `configure`, but pressing „tab" after `conf` will.

2. Important! Writing answers:

- Whenever you are asked to answer a question that doesn't require configuration, type the answer in a notepad window and keep it until the lab assistant checks that task.

3. Important! Telnet.

- You can telnet from any device to any router in this scenario as long as you have properly configured the IP addressing scheme. Don't forget that a router will not allow you to telnet to it if you don't configure a password on its vty lines first.

1. Configure the hostnames and the IP addressing scheme as shown in the topology. Make sure that all devices have full connectivity with their neighbors.

   Hint: Don't forget about the clock rate on the serial interfaces.

2. Create the required static routes on the three routers in order to ensure connectivity between all five networks.

3. The user on PC2 is not trustworthy so it has been decided that PC2 will not have access to the server anymore. Create a standard numerical access list that denies all traffic coming from PC2 and going to the server.

   Hint: Pay attention to the location of the ACL.

4. The user on PC2 seems to be causing troubles to his colleagues, too. Make sure that he will not be able to communicate with any host in PC1's network, while still being able to communicate with other networks and hosts.

5. Use one or more named ACLs to block router Cherry from contacting the other two routers via Telnet.

6. Test the web server on the server using any PC. Block all HTTP and HTTPS packets sent from PC1 to the server.

7. Create an ACL to ensure that PC1 will not be able to receive TCP sessions initiated from outside its network, but still be able to access eveything else from the inside.

8. Create an ACL on the VTY lines so that only the hosts with odd IP address numbers (look at the last byte) will be able to Telnet into router Acorn.

9. Create an ACL to explicitely block the two types messages involved in a „ping" (and only those two), so that Acorn will not be able to ping Banana.

   Hint: Remember that Banana has two active interfaces, and so does Acorn.

10. Create a AAA authentication list called MY_AUTH that will try several authentication methods, in the following order: the local user database, the RADIUS servers, the TACACS+ servers and finally, if everything else fails, authentication will be permitted unconditionally.