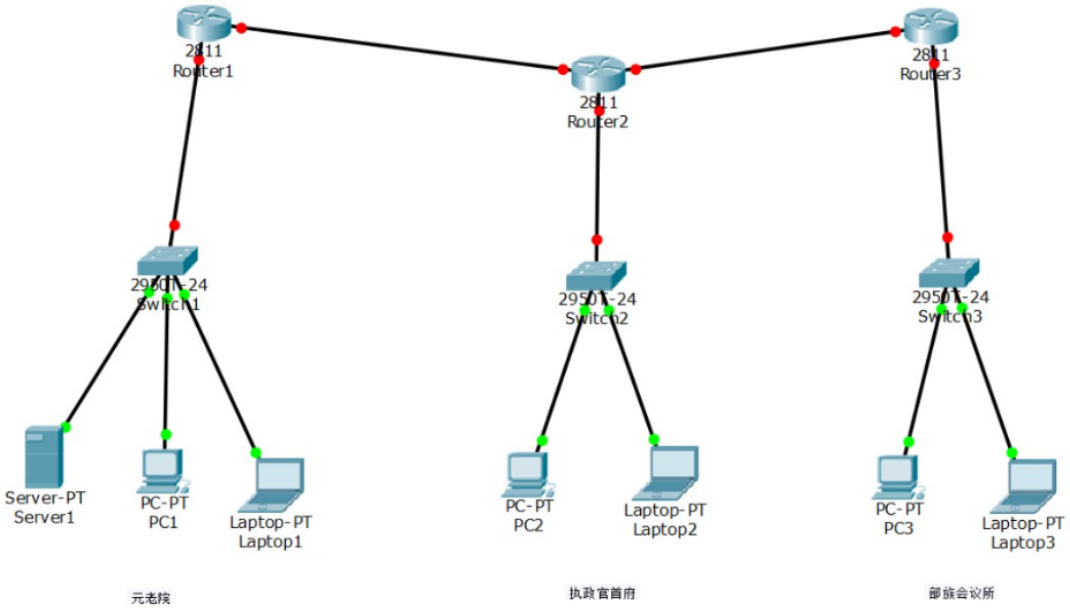
计算机网络安全技术 【实验1】 网络搭建及路由配置

计83 李天勤 2018080106

> At present, the "Republic" mainly contains three institutions of power, the Senate (元老院), the Capital of the Consul (执政官首府) and the Tribal Council (部族会议所). Because the three have different divisions of labor, they all use different subnets for management. Before leaving, Caesar left you with a sketch of the network topology and a papyrus with an IP address allocation plan.




```
元老院（192.168.1.0/24）：Router1, Switch1, Server1, PC1, Laptop1
执政官首府（192.168.2.0/24）：Router2, Switch2, PC2, Laptop2
部族会议所（192.168.3.0/24）：Router3, Switch3, PC3, Laptop3
```

IP 分支方案

Device	Port	IP	Mask	Gateway
Router1	端口1	192.168.1.1	/24	----------
	端口2	10.0.1.1	/24	----------
Router2	端口1	10.0.1.2	/24	----------
	端口2	（3）	/24	----------
	端口3	192.168.2.1	/24	----------
Router3	端口1	（1）	/24	----------
	端口2	192.168.3.1	/24	----------
PC1	端口1	192.168.1.2	/24	192.168.1.1
PC2	端口1	192.168.2.2	/24	192.168.2.1
PC3	端口1	192.168.3.2	/24	192.168.3.1
Server1	端口1	192.168.1.3	/24	（2）
Laptop1	端口1	192.168.1.4	/24	192.168.1.1
Laptop2	端口1	192.168.2.3	/24	192.168.2.1
Laptop3	端口1	192.168.3.3	/24	192.168.3.1

任务1: 破旧的莎草纸（3）

> You find that due to the age, the papyrus with the IP address allocation plan is damaged in two places. In addition, due to Caesar's lack of network knowledge, there is a flaw in his IP address allocation plan. Please complete the plan, and point out and correct the mistakes in the plan. To facilitate network management, please plan your IP address in a way that is easy to remember.

The IP address for Router3 that is missing at (1) should be set to have the same network segment as Router(2) to be able to communicate, such as 10.0.2.1

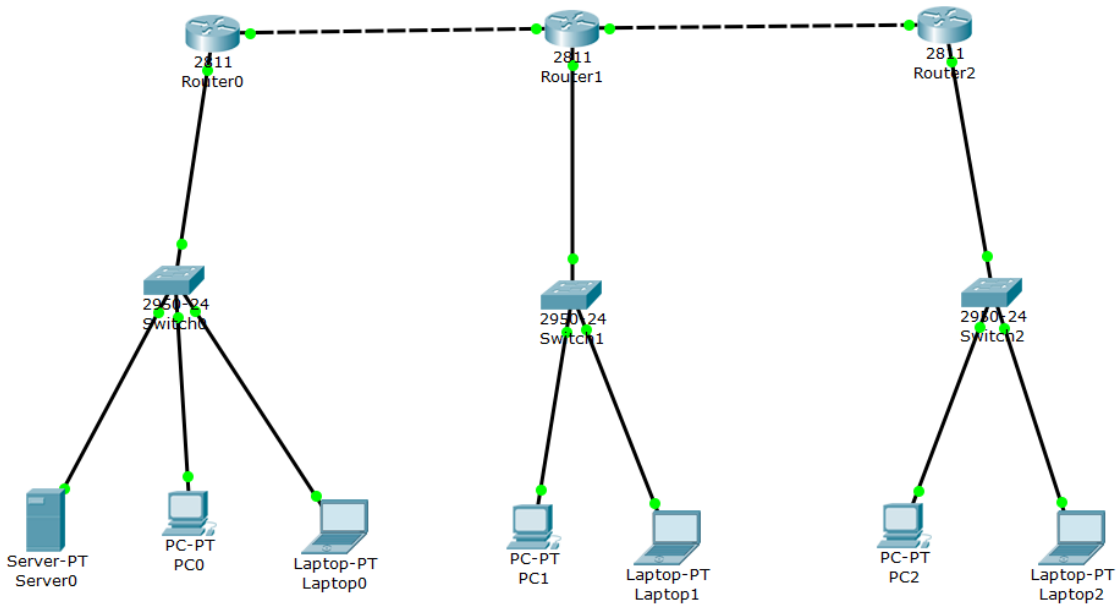
The gateway that is missing at (2) should be 192.168.1.1. This is because the upper level router for Server 1 has IP address of 192.168.1.1, and any destination address sent outside this subnet will be handed over to that gateway for processing.

There is IP Address error for Router2 at (3). Originally 20.0.2, this IP segment is not considered a private IP segment. Thus should not be used as private. We need to correct this to a private IP address, such as 10.0.2.2.

任务2: "一天建起的罗马城" （2）

> After completing the network construction plan, please select the appropriate equipment and connections to build the network, and configure the corresponding IP and other attributes for each interface. Please provide necessary screenshots to prove to Caesars that you personally participated in the network construction work

This is the finished network after setting up the proper IP address, gateways, and routes.



The communication capabilities can be tested using ping. The tests are shown in task 4.

任务3: 要点防卫 （7）

> The access point of the public network and the "Republic" intranet is located on Router1 of the Senate. In order to prevent malicious intrusion by others, Caesars requires you to set a login password for Router1 at least. You need to set three kinds of passwords for it: the password password1 for entering the user mode through the console port, the password password2 for entering the privileged mode through the user mode, and the password password3 for logging in to the router through telnet.
>
> If the router configuration file may be leaked, have your settings changed? Try to analyze, when you configure the passwords with the following four levels of complexity, the attacker's time requirements for brute force cracking, assuming that the time for a brute force attempt is 1: (1) a total length of six-digit pure digital password (2) Passwords with a total length of six digits mixed with numbers and lowercase letters (3) Passwords with a total length of six digits mixed with numbers, uppercase letters, and lowercase letters (4) Passwords with a total length of eight digits mixed with numbers, uppercase letters, and lowercase letters

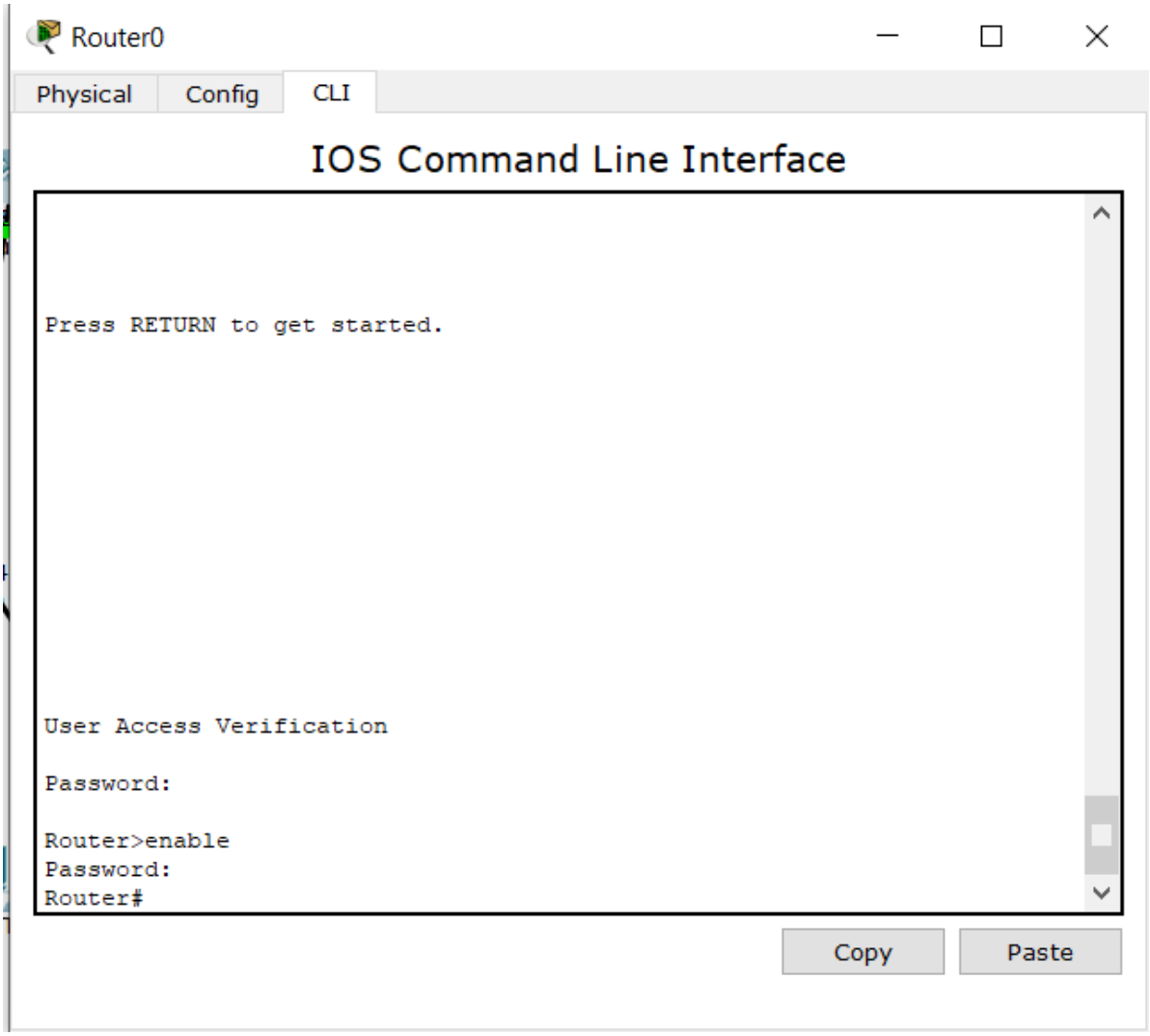
Password Setting

User Mode Password: veni

Privileged Mode Password: vidi

Telnet Password: vici

After setting the passwords, lets confirm by logging in.



Brute-Force Hacking Time Requirements

1. $10^6 = 1,000,000$
2. $36^6 = 2,176,782,336$
3. $62^6 = 56,800,235,584$
4. $62^8 = 218,340,105,584,896$

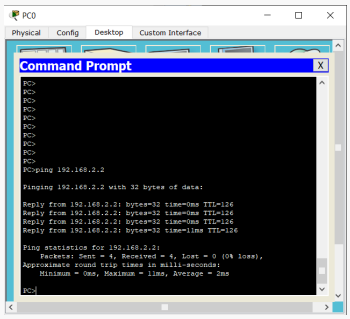
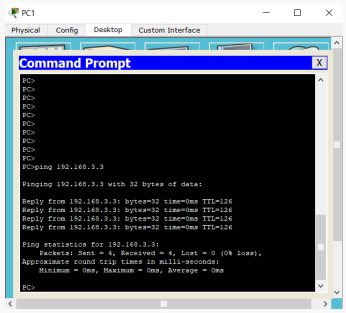
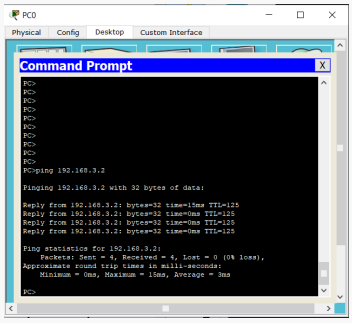
任务4: "三权"间的初步通信 （4）

> After setting up the network, you want to test whether the networks of the various authorities of the "Republic" are connected. The ICMP protocol provides you with appropriate network control information for detection. Due to the relatively simple network structure of the "Republic", you decide to use static routing to ensure normal communication within the intranet. However, improper use of static routes can easily bring inconvenience to network maintenance. For example, when the network is expanded, redundant static routes may also affect the new network. Therefore, please allow the three power departments to communicate with each other without using redundant static routing.

The static routes are set as shown

Router0	Router1	Router2
Network Address 192.168.2.0/24 via 10.0.1.2 192.168.3.0/24 via 10.0.2.1	Network Address 192.168.1.0/24 via 10.0.1.1 192.168.3.0/24 via 10.0.2.1	Network Address 192.168.2.0/24 via 10.0.2.2 192.168.1.0/24 via 10.0.1.1

Test to show connections

PC0 to PC1	PC1 to PC2	PC0 to PC2
Subnet 1 and 2 Test	Subnet 2 and 3 Test	Subnet 1 and 3 Test
		

任务5: "三权"间的高效通信 （4）

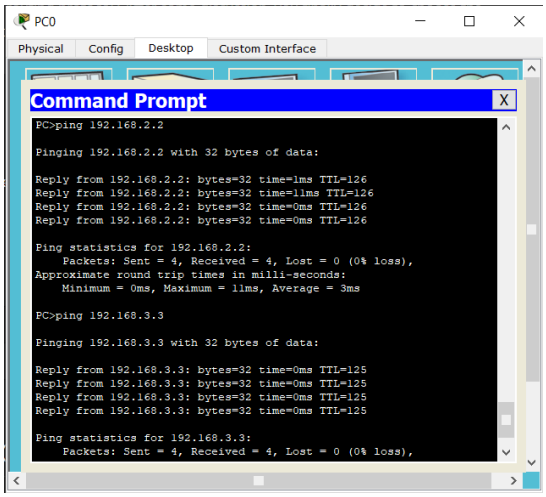
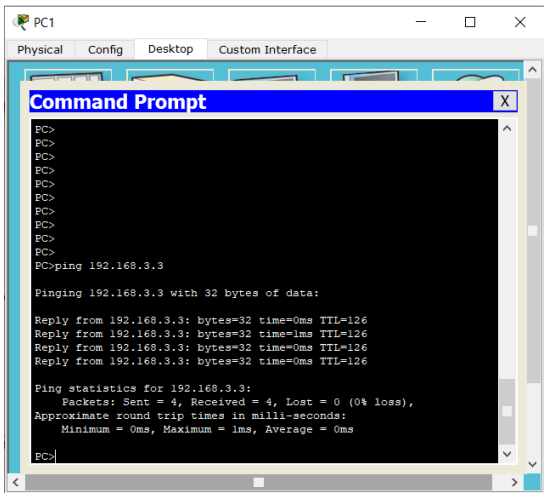
> In order to reduce the maintenance cost of the network and improve the efficiency of communication, you suggest to Caesars to use the routing protocol to dynamically manage and maintain routing. When discussing which routing protocol to use, Caesars pointed out that "Because the current network scale of the 'Republic' is small, the total number of PCs, notebooks and servers connected to the network is less than 16, which can be managed by the routing protocol RIP suitable for small networks. "(Apparently he took advantage of this time to learn some network knowledge). Do you think there is a problem with Caesar's view? why? Is it currently possible to use RIP as a routing protocol? After some discussion, you finally decide to choose the __ routing protocol to maintain the current LAN of the "Republic". Please complete the configuration of the protocol and verify whether it can meet the requirements.

Caesar believes that the RIP routing protocol can be applied since the total number of hosts does not exceed 16. This is incorrect, it should be that the number of hops is less than 16, not the number of hosts. In a network of 16 hosts, there is no possibility of any two hosts having 16 hops between them.

Thus, after much debate, we decide to choose the RIP protocol, and remove the static routing table. The process and configurations are as shown:

PC0	PC1	PC2
RIP Network Network Address 10.0.0.0 192.168.1.0	RIP Network etwork Addre 10.0.0.0 192.168.2.0	RIP Network etwork Addre 10.0.0.0 192.168.3.0

Similar Tests as Task 4 are Applied

PC0 to PC1 and PC2	PC1 to PC2
	

Bonus 任务：凯撒的赏赐 （2）

1. In recent days, Caesar suddenly became interested in the password security of the "Republic" intranet. He requested that the privileged mode password of the "Republic" intranet should be stored encrypted to a certain extent in the configuration file using the secret command. Try to find out how to encrypt the password stored using this command.

   The router saves the password in MD5 has mode, and performs authentication by checking whether or no the hash value of the text of the password is consistent during each authentication during each login.

2. In task 4, after the static route is configured, packet loss will occur when the ping test is initiated for the first time. Please use your network knowledge to explain this situation.

   During the Ping process, a host machine such as a laptop sends a packet to the target IP address. When we send a packet in the link layer, we need to know the MAC address of the next device, known as the Destination MAC or MAC address of the target host. Only when the source host knows the Destination Mac, can it construct a packet to send it out. But during the first ping, the local machine searches the MAC address of the host whose target IP is not found in the ARP cache (or the host whose IP is the next hop obtained by searching the routing table), and then sends an ARP broadcast for query instead, so there is no Ping out.