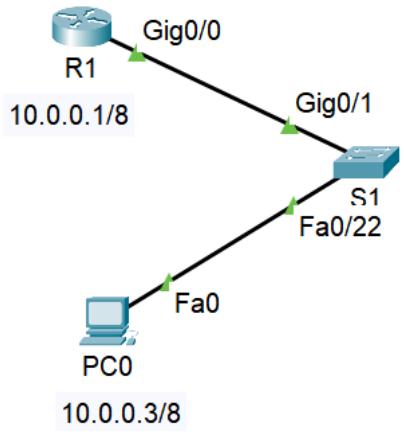
Application Protocols

Telnet and SSH



Use one router, one switch and one end device.

Configure the router:

- hostname is R1, domain name is cisco.com
- set logging synchronization on the console line
- create one user: username admin, password (secret) cisco
- configure SSH settings, SSH version 2, key length 1024
- IP address for the connected interface is 10.0.0.1/8
- set VTY access to the both telnet and ssh

PC:

- IP address 10.0.0.3/8
- geteway 10.0.0.1

Connect R1 from PC using telnet. Is it possible? If yes, go to the privileged exec mode. Is it possible? If no, fix it. Use the telnet command:

```
telnet 10.0.0.1
```

Connect R1 from PC using SSH. Use the ssh command:

```
ssh -l admin 10.0.0.1
```

There exists one application intended for the given purpose, find this application.

DNS Resolution

If we want to manually resolve between a name and an IP address or otherwise communicate with a DNS server, we have the `nslookup` command in Windows, and the `host`, `nslookup` and `dig` commands in UNIX-like systems.

Task:

Compare the output of these commands:

```
host iana.org
nslookup iana.org

dig iana.org
dig iana.org +short
dig iana.org aaaa +short
dig iana.org mx +short
dig iana.org ns +short
dig @1.1.1.1 iana.org
dig google.com txt +short
```

Start Wireshark and capture the traffic for the following command:

```
dig google.com
```

Compare the output of the given command and the captured traffic.

Reverse Resolution: PTR Records

In DNS, there are several types of resource records (RR): A for IPv4, AAAA for IPv6, CNAME for aliases, TXT for various purposes including security, PTR for reverse resolution.

Task:

Find out the IPv4 address of google.com (with `dig`) and then use the discovered address in the following command:

```
dig –x address ptr
```

Network statistics

The `netstat` command is used to display network statistics. It exists on different platforms, but the same option can have different meanings on different systems. On UNIX systems, we can use the `ss` command as well, it is intended for investigating sockets.

Windows:

All usable options can be listed by

```
netstat -?
```

The following variants are used quite a lot:

```
netstat –ano   ; full statistics for all protocols, including PIDs of communicating processes
netstat –sp icmp    ; statistics of the ICMPv4 protocol
netstat –sp icmpv6  ; for the ICMPv6 protocol
netstat –sp tcp     ; statistics of the TCP protocol
```

Linux, MacOS, Solaris and other UNIX and UNIX-like systems:

All usable options can be listed by

```
netstat -?
man netstat
```

The following variants are used quite a lot:

```
netstat –anp        ; full statistics for all protocols, including PIDs
netstat –ant        ; statistics of TCP
netstat –anu        ; statistics of UDP
netstat –tpc        ; TCP, including processes, continous monitoring
                      (use some web browser to capture any http traffic)
netstat –l          ; all ports on which a process is listening

ss –l         ; displays all listening sockets, including related information
ss –e         ; detailed information about sockets
ss –le        ; detailed info about listening sockets
sudo ss –ulp        ; processes listening on UDP ports
```