Пароль на enable в Router:

1. Conf t
2. Enable secret <pass>

Пароль на консоль:

1. Conf t
2. Line console 0
3. Password cisco
4. Login
5. Login

Пароль на telnet (Router - маршрутизатор)

1. Conf t
2. Line vty 0 15
3. Password telnet1
4. Login
5. Transport input telnet
6. end

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проверка захода 2х компов через telnet:

1. в c:/ - telnet <address> интерфейса, который работает с компом, например g0/1

Проверка работы SSH:

1. В С:/> ssh –l admin <address> ||address – установили где vlan interface 0 1

В роутер прописать описание интерфейсов:

1. Conf
2. Int g0/0
3. Desc “To P\_1”
4. End

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Для SHH на коммутаторе (S\_1)

Первоначальная настройка интерфейса, к которому будет подключаться SSH:

1. Enable - > configure terminal
2. Interface vlan 0 1
3. Ip address <ip> <subnet> (ПО ЗАДАНИЮ)
4. No shutdown

SSH:

1. Conf t
2. Hostname S\_1
3. Ip domain name cisco.com
4. Crypto key generate rsa general-keys modulus 2048
5. Username admin secret <pass> - создали пользователя в локальной БД
6. Line vty 0 14 – выделяем порты для SSH
7. Login local – для проверки подлинности строки vty в локальной базе данных
8. Transport input ssh

