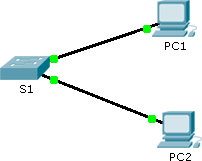


Packet Tracer. Отработка комплексных практических навыков

**Топология**



**Таблица адресации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** |
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |

**Сценарий**

Сетевой администратор попросил вас настроить новый коммутатор. В рамках этого упражнения, используя список требований, вам предстоит выполнить базовую настройку коммутатора, конфигурацию протокола SSH и параметры безопасности портов.

**Требования**

* Установите следующие начальные значения параметров коммутатора **S1**:
  + Имя узла
  + Баннер, который содержит слово **предупреждение (warning)**
  + Включить проверку пароля на консоль и пароль **cisco**
  + Зашифрованный пароль привилегированного режима — **class**
  + Зашифруйте все незашифрованные пароли
  + Адресация административного интерфейса
* Установите следующие параметры протокола SSH для безопасного удаленного доступа:
  + Имя домена **cisco.com**
  + Параметры пары ключей RSA для поддержки протокола SSH версии 2
  + Настройте протокол SSH версии 2
  + пользователь **admin** c секретным паролем **ccna**
  + линии VTY настроены на подключение только по протоколу SSH, а для проверки подлинности используются учетные данные из локальной базы данных

**Packet Tracer. Отработка комплексных практических навыков**

* Настройте функцию безопасности портов для ограничения сетевого доступа.
  + Отключите все неиспользуемые порты.
  + Настройте режим интерфейса в режим доступа (access).
  + Активируйте защиту порта, позволяющую подключаться только двум узлам к одному порту.
  + Запишите MAC-адрес в текущей конфигурации.
    - 0001.647c.697e – PC2
    - 00e0.b027.2245 – PC1
  + Убедитесь, что в случае нарушения порт будет отключен.