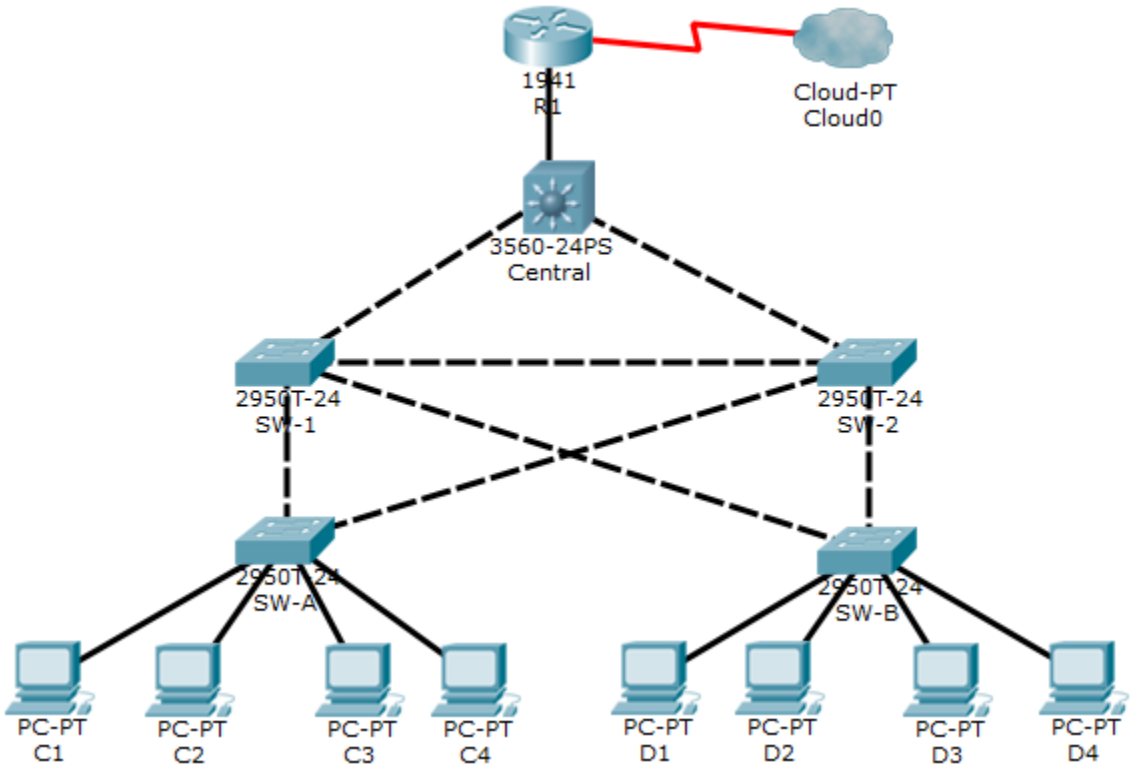
Packet Tracer. Обеспечение безопасности на 2-м уровне

Топология



Задачи

- Назначение коммутатора Central в качестве корневого моста.
- Защита параметров связующего дерева для предотвращения атак путем манипуляций STP.
- Включение защиты портов для предотвращения атак путем переполнения таблиц CAM.

Исходные данные/сценарий

Недавно сеть подверглась нескольким атакам. Поэтому сетевой администратор поручил вам настроить безопасность на 2-м уровне.

Для обеспечения оптимальной производительности и безопасности администратор хочет, чтобы в качестве корневого моста использовался коммутатор 3560 Central. Чтобы предотвратить атаки путем манипуляций с протоколом STP, администратору требуется гарантированная защита параметров STP. Чтобы предотвратить атаки путем переполнения таблиц CAM, сетевой администратор решил настроить защиту портов для ограничения количества MAC-адресов, которые может определить каждый порт коммутатора. Если число MAC-адресов превышает заданное ограничение, администратор должен выключить порт.

На всех коммутаторах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: **ciscoenpa55**
- Пароль консоли: **ciscoconpa55**
- Имя пользователя и пароль SSH: **SSHadmin/ciscosshpa55**

Часть 1: Настройка корневого моста

Шаг 1: Определите текущий корневой мост.

С коммутатора **Central** введите команду **show spanning-tree,** чтобы определить текущий корневой мост, используемые порты и их состояние.

Какой коммутатор является текущим корневым мостом?

_____

В зависимости от текущего корневого моста определите итоговое связующее дерево. (Нарисуйте топологию связующего дерева.)

Шаг 2: Назначьте коммутатор Central главным корневым мостом.

Используя команду **spanning-tree vlan 1 root primary**, назначьте коммутатор **Central** корневым мостом.

Шаг 3: Назначьте коммутатор SW-1 вторичным корневым мостом.

Назначьте коммутатор **SW-1** вторичным корневым мостом с помощью команды **spanning-tree vlan 1 root secondary**.

Шаг 4: Проверьте конфигурацию связующего дерева.

С помощью команды **show spanning-tree** убедитесь, что коммутатор **Central** является корневым мостом.

```
Central# show spanning-tree
VLAN0001
   Spanning tree enabled protocol ieee
   Root ID  Priority      24577
            Address       00D0.D31C.634C
            This bridge is the root
            Hello Time  2 sec  Max Age  20 sec   Forward Delay  15 sec
```

Какой коммутатор является текущим корневым мостом?

_____

В зависимости от нового корневого моста определите итоговое связующее дерево. (Нарисуйте топологию связующего дерева.)

Часть 2: Защита от атак на STP

Обеспечьте защиту параметров STP для предотвращения атак для манипулирования STP.

Шаг 1: Включите функцию PortFast на всех портах доступа.

Функция PortFast настроена на портах доступа, подключенных к компьютеру или серверу, что позволяет им намного быстрее становиться активными. На подключенных портах доступа коммутаторов **SW-A** и **SW-B** введите команду **spanning-tree portfast**.

Шаг 2: Включите функцию BPDU Guard на всех портах доступа.

BPDU Guard – это функция, позволяющая предотвращать появление мошеннических коммутаторов и спуфинг на портах доступа. Включите функцию BPDU Guard на портах доступа коммутаторов **SW-A** и **SW-B**.

Примечание. Функцию BPDU Guard для защиты связующего дерева можно включить на каждом отдельном порте с помощью команды **spanning-tree bpduguard enable** в режиме интерфейсной настройки или команды **spanning-tree portfast bpduguard default** в режиме глобальной настройки. Для целей оценки в этом задании используйте команду **spanning-tree bpduguard enable**.

Шаг 3: Включите Root Guard.

BPDU Guard можно включить на всех портах коммутатора, которые не являются корневыми. Лучше всего эту функцию развернуть на тех портах, которые подключены к другим некорневым коммутаторам. С помощью команды **show spanning-tree** определите расположение корневого порта на каждом коммутаторе.

На коммутаторе **SW-1** включите функцию Root Guard на портах F0/23 и F0/24. На коммутаторе **SW-2** включите Root Guard на портах F0/23 и F0/24.

Часть 3: Настройка безопасности портов и отключение неиспользуемых портов

Шаг 1: Настройте базовый уровень безопасности всех портов, подключенных к хостам.

Данную процедуру следует выполнить на всех портах доступа коммутаторов **SW-A** и **SW-B**. Задайте максимальное число полученных MAC-адресов равным **2**, разрешите динамическое изучение MAC-адресов и задайте для нарушения (параметр violation) значение **shutdown**.

Примечание. Порт коммутатора должен быть настроен как порт доступа для включения безопасности портов.

Почему безопасность портов не включена на портах, подключенных к другим коммутаторам?

_____

_____

_____

_____

_____

Шаг 2: Проверьте безопасность портов.

a. На коммутаторе **SW-A** введите команду **show port-security interface f0/1** и убедитесь, что безопасность портов настроена.

```
SW-A# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

b. Отправьте эхо-запрос с компьютера **C1** на компьютер **C2** и снова введите команду **show port-security interface f0/1**, чтобы убедиться, что коммутатор получил MAC-адрес для компьютера **C1**.

Шаг 3: Отключите неиспользуемые порты.

Отключите все порты, которые в настоящий момент не используются.

Шаг 4: Проверьте результаты.

Вы полностью выполнили задание. Нажмите **Check Results (Проверить результаты)** для просмотра отзыва и проверки завершенных обязательных компонентов.

