### Конфигурирование функции Port Security

Port-security – функция коммутатора, позволяющая указать MAC-адреса узлов, которым разрешено передавать свои данные через определенный порт. После этого порт устройства не передает кадры, если MAC-адрес отправителя в них не относится к разре- шенным.

Просмотр состояния функции port-security осуществляется с помощью команд:

**Switch#show port-security** – отображает общую ин- формацию о функции port-security на интерфейсах коммутатора;

**Switch#show port-security interface fa0/1** – отображает подробную информацию о функции port-security на указанном интерфейсе;

**Switch#show port-security address** – отображает информацию о записях таблицы разрешенных MAC-адресов функ- ции port-security.

Для поддержки функции port-security на определенном ин- терфейсе коммутатора вначале необходимо явно перевести его в режим доступа (**Switch(config-if)#switchport mode access**), а затем использовать следующие команды:

**Switch(config-if)#switchport port-security** – включение защиты порта (соответственно, с префиксом **no** – вы- ключение данной функции);

**Switch(config-if)#switchport port-security maximum <N>** – установка максимального числа адресов, одно- временно используемых на порту, где N – число поддерживаемых на порту адресов (зависит от модели коммутатора), по умолчанию (если не использовать команду) устанавливается в 1;

**Switch(config-if)#switchport port-security violation <action>** – определяет действия в случае наруше- ния функции port-security. Параметр action может принимать сле- дующие значения:

* **protect** – когда количество разрешенных MAC-адресов до- стигает максимального числа, настроенного на интерфейсе, кадры с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока администратором не будет удалено достаточное количе- ство имеющихся MAC-адресов, чтобы их количество стало меньше максимального значения, или увеличено максимальное количество разрешенных адресов. Оповещений о нарушении безопасности в этом случае нет;
* **restrict** – аналогично предыдущему значению параметра, но в этом режиме при нарушении безопасности отправляются опове- щение SNMP-trap, сообщение syslog и увеличивается счетчик нарушений (violation counter);
* **shutdown** – используется по умолчанию, нарушение без- опасности приводит к тому, что интерфейс немедленно переводит- ся в состояние error-disabled, отправляется SNMP-trap, сообщение syslog и увеличивается счетчик нарушений. Интерфейс коммутато- ра из состояния error-disabled можно вывести, введя последователь- но команды **shutdown** и **no shutdown**;

# Switch(config-if)#switchport port-sec mac-addr

**<MAC-адрес>** – позволяет создать статическую запись для ука- занного MAC-адреса (параметр MAC-адрес указывается в нотации Cisco, например 1111.2222.3333). Если вместо адреса указать клю- чевое слово **sticky**, то коммутатор автоматически занесет адрес узла в конфигурацию при первом его появлении на интерфейсе и сделает эту запись статической. Если команду не использовать, то формируются динамические записи, которые при нарушении без- опасности интерфейса будут удалены из таблицы функции port- security.

## ВЫПОЛНИТЬ!

1. Справа от имеющейся схемы создать сеть, изображенную на рис. 2.2. Интерфейсы коммутатора FastEthernet c номерами с 1 по 5 назначить в VLAN10, с 6 по 10 – в VLAN20 и подключить Hub0 к Fa0/1, Server0 – к Fa0/2, Server1 – к Fa0/6.

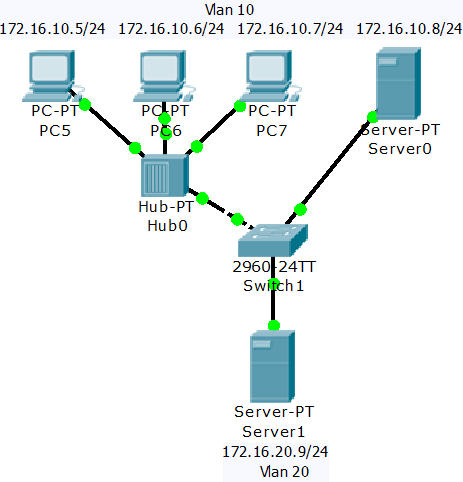


Рис. 2.2. Расширение имеющейся сети

## ВЫПОЛНИТЬ!

1. Включить функцию port-security на интерфейсе

FastEthernet0/1.

1. Задать на интерфейсе FastEthernet0/1 максимальное число

MAC-адресов для функции port-security, равное трем.

1. Выполнить на PC5 команду **ping** в адрес узла Server0.
2. Проанализировать содержимое таблицы MAC-адресов port- security и таблицы коммутации.
3. Создать статическую запись port-security для узла PC6.
4. Выполнить команду создания статической записи port- security с параметром **sticky**.
5. Выполнить на PC7 команду **ping** в адрес узла Server0.
6. Проанализировать содержимое таблицы MAC-адресов и таблицы коммутации.
7. Отобразить общую информацию о конфигурации port- security и состоянии функции на интерфейсе FastEthernet0/1.
8. Сменить MAC-адрес сетевого адаптера на узле PC5. Если интерфейс FastEthernet0/1 коммутатора Switch1 не отключился (операция функции port-security по умолчанию), выполнить на PC5 команду **ping** в адрес узла Server0.
9. Проанализировать содержимое таблицы MAC-адресов port- security и таблицы коммутации.
10. Вывести информацию о состоянии интерфейса

FastEthernet0/1 и вернуть его в рабочее состояние.

1. Выполнить на PC5 команду **ping** в адрес узла Server0.
2. Проанализировать содержимое таблицы MAC-адресов port- security и таблицы коммутации.
3. Убедиться в том, что Server0 доступен для узлов PC5, PC6, PC7.