Пример настройки аутентификации 802.1X через Web-интерфейс

Стандарт **IEEE 802.1X** (IEEE Std 802.1X-2010) описывает использование протокола EAP (Extensible Authentication Protocol) для поддержки аутентификации с помощью сервера аутентификации. Стандарт IEEE 802.1X осуществляет контроль доступа и не позволяет неавторизованным устройствам подключаться к локальной сети через порты коммутатора.

Сервер аутентификации **Remote Authentication in Dial-In User Service** (**RADIUS**) проверяет права доступа каждого клиента, подключаемого к порту коммутатора, прежде чем разрешить доступ к любому из сервисов, предоставляемых коммутатором или локальной сетью.

В стандарте IEEE 802.1X определены три роли устройств в общей схеме аутентификации:

- Клиент (Client/Supplicant);
- Аутентификатор (Authenticator);
- Сервер аутентификации (Authentication Server).

Клиент (Client/Supplicant) — это рабочая станция, которая запрашивает доступ к локальной сети и отвечает на запросы коммутатора. На рабочей станции должно быть установлено клиентское ПО для 802.1X, например, то, которое встроено в ОС клиентского компьютера или установлено дополнительно.

Сервер аутентификации (Authentication Server) выполняет фактическую аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор о предоставлении или отказе клиенту в доступе к локальной сети. Служба RADIUS является клиент/серверным приложением, при работе которого информация об аутентификации передается между сервером RADIUS и клиентами RADIUS.

Аутентификатор (Authenticator) управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Эту роль выполняет коммутатор. Он работает как посредник (Proxy) между клиентом и сервером аутентификации: получает запрос на проверку подлинности от клиента, проверяет данную информацию при помощи сервера аутентификации и пересылает ответ клиенту. Коммутатор реализует функциональность клиента RADIUS, который отвечает за инкапсуляцию и деинкапсуляцию кадров EAP и взаимодействие с сервером аутентификации.

Коммутаторы D-Link поддерживают две реализации аутентификации 802.1X:

- Port-Based 802.1X (802.1X на основе портов);
- MAC-Based 802.1X (802.1X на основе MAC-адресов).

При аутентификации 802.1X на основе портов (Port-Based 802.1X), после того как порт был авторизован, любой компьютер, подключенный к нему, может получить доступ к сети.

В отличие от аутентификации 802.1X на основе портов, где один порт, авторизированный клиентом, остается открытым для всех клиентов, аутентификация 802.1X на основе MAC-адресов (MAC-Based 802.1X) — это аутентификация множества клиентов на одном физическом порте коммутатора. При аутентификации 802.1X на основе MAC-адресов проверяются не только имя пользователя/пароль, подключенных к порту коммутатора клиентов, но и их количество. Количество подключаемых клиентов ограничено максимальным количеством MAC-адресов, которое может изучить каждый порт коммутатора. Для функции MAC-Based 802.1X количество изучаемых MAC-адресов указывается в спецификации на устройство. Сервер аутентификации проверяет имя пользователя/пароль, и, если информация достоверна, аутентификатор (коммутатор) открывает логическое соединение на основе MAC-адреса клиента. При этом, если достигнут предел изученных портом коммутатора MAC-адресов, новый клиент будет заблокирован.

Функция **802.1X Guest VLAN** используется для создания гостевой VLAN с ограниченными правами для пользователей, не прошедших аутентификацию. Когда клиент подключается к порту коммутатора с активизированной аутентификацией 802.1X и функцией Guest VLAN, происходит процесс аутентификации (локально или удаленно с использованием сервера RADIUS). В случае успешной аутентификации клиент будет помещен в VLAN назначения (Target VLAN) в соответствии с предустановленным на сервере RADIUS параметром VLAN. Если этот параметр не определен, то клиент будет возвращен в первоначальную VLAN (в соответствии с настройками порта подключения).

В том случае, если клиент не прошел аутентификацию, он помещается в Guest VLAN с ограниченными правами доступа.

Примечание к настройке

Рассматриваемый пример настройки подходит для следующих серий коммутаторов: DGS-1100/ME, DGS-1210, DGS-1210/ME, DGS-1210/FL, DGS-3000.

Задача №1

В локальной сети необходимо обеспечить аутентификацию пользователей при подключении их к сети.

Задача решается настройкой Port-Based 802.1X на портах коммутатора.

Помимо коммутатора, необходимо настроить RADIUS-сервер и 802.1X-клиент на рабочей станции. В качестве RADIUS-сервера можно использовать пакет **freeradius** для ОС Linux.

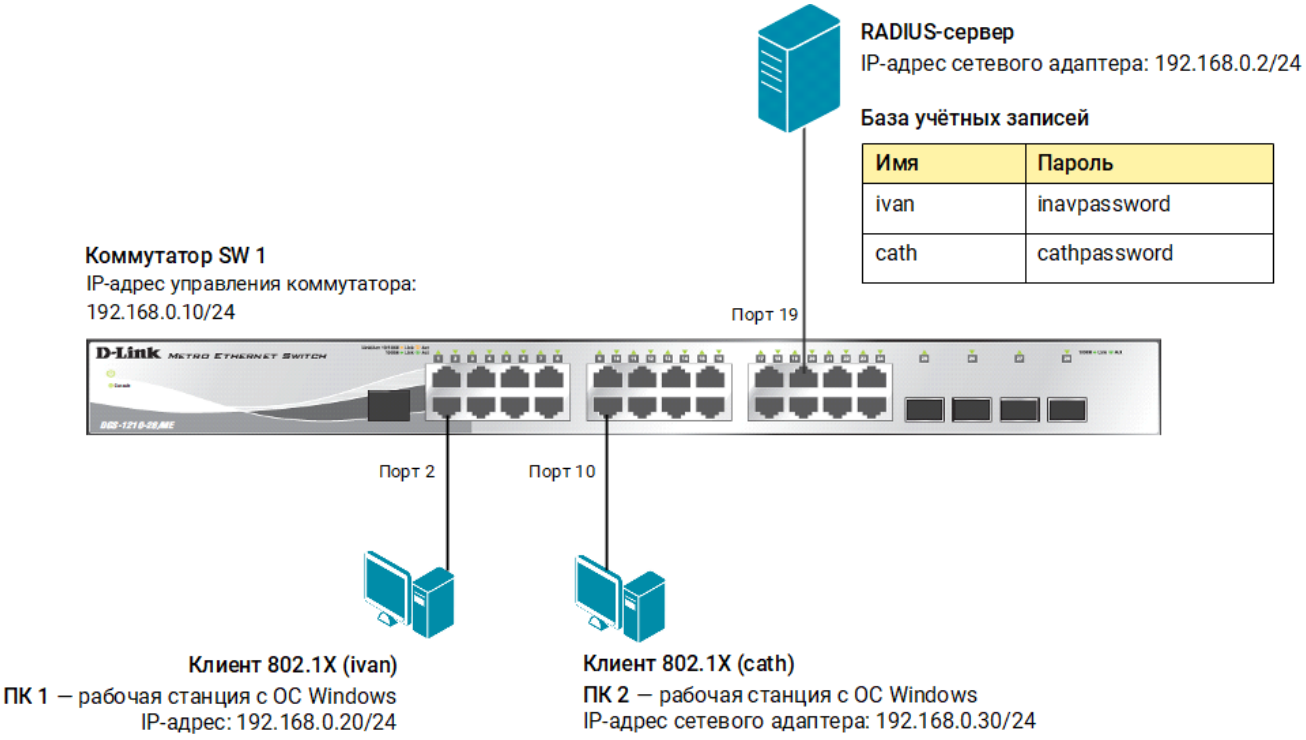
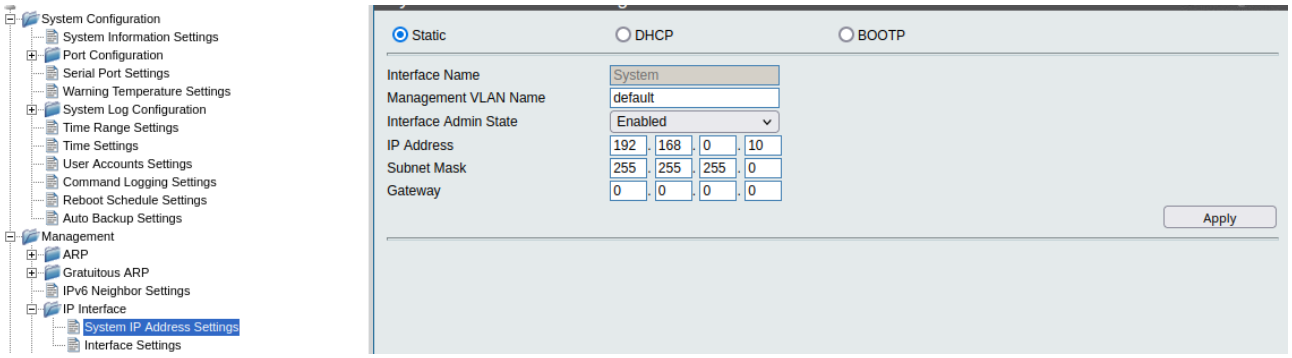


Рис. 1 Схема подключения

Настройка коммутатора SW 1

1. В меню слева выберите **Management** → **IP Interface** → **System IP Address Settings** и измените IP-адрес интерфейса управления коммутатора (в примере – 192.168.0.10/24).



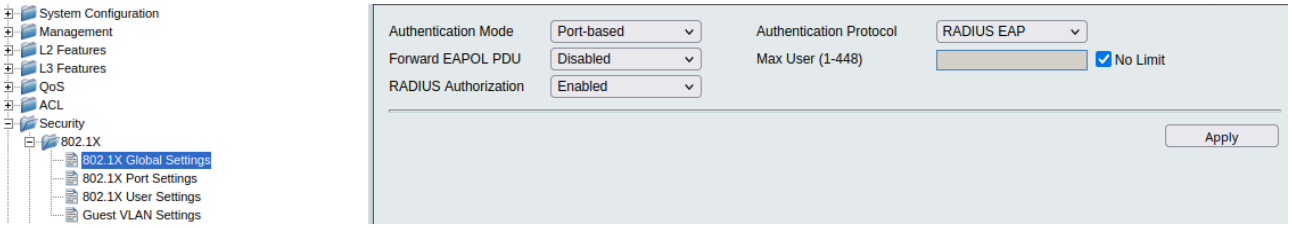
2. Выберите пункт меню **Security** → **802.1X** → **802.1X Global Settings** и активируйте функцию 802.1X, выполнив следующие настройки:

   – в поле **Authentication Mode** выберите **Port-based**;

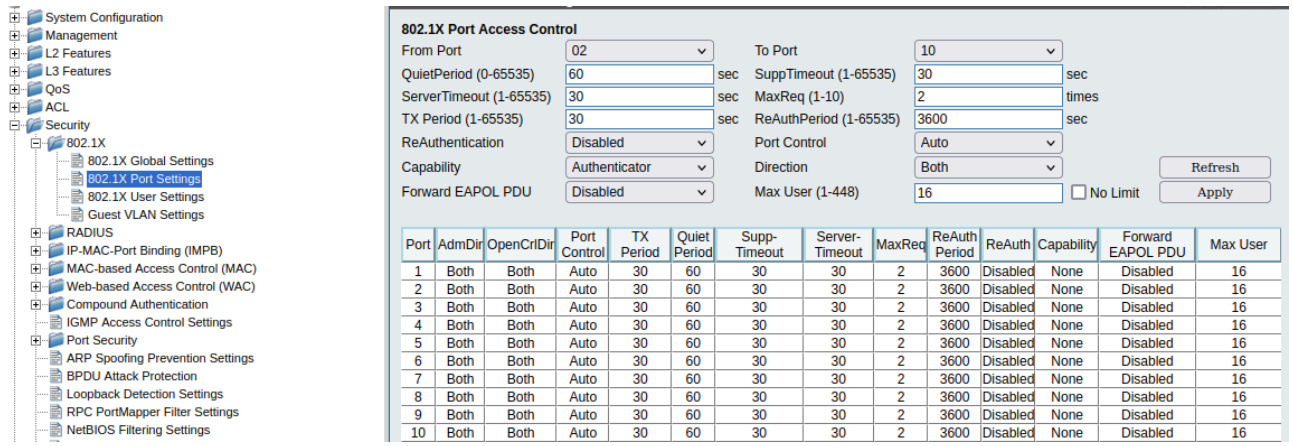
   – в поле **RADIUS Authorization** выберите **Enabled**;

   – в поле **Authentication Protocol** выберите **RADIUS EAP**.

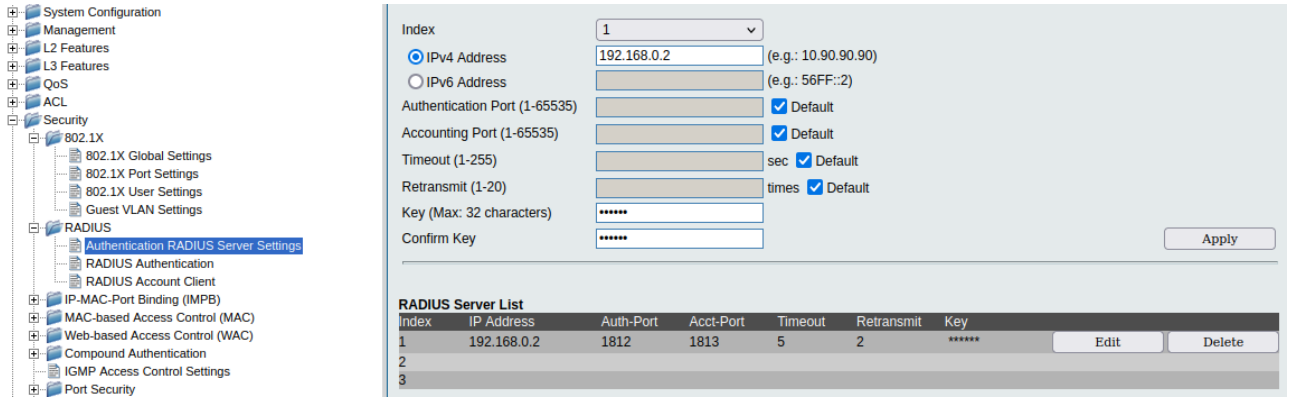
   Нажмите **Apply**.



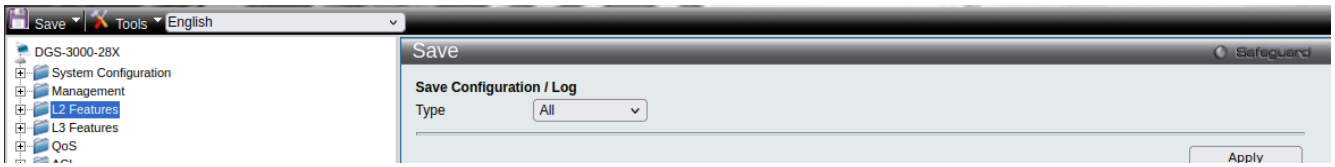
3. Выберите пункт меню **802.1X Port Settings** и укажите порт или диапазон портов, к которым будут подключены клиенты, выбрав соответствующие значения в полях **From Port** и **To Port** (в примере порты 2 – 10). В поле **Capability** выберите **Authenticator** и нажмите **Apply**.



4. Выберите пункт меню **RADIUS** → **Authentication RADIUS Server Settings**. В поле **IPv4 Address** укажите адрес своего сервера (в примере 192.168.0.2). Введите и подтвердите пароль в полях **Key/Confirm Key**. Нажмите **Apply**.



5. Чтобы сохранить выполненные настройки, в левом верхнем углу нажмите **Save**, выберите **Save Configuration** и нажмите **Apply**.



Задача № 2

В локальной сети необходимо обеспечить аутентификацию пользователей при их подключении к сети через неуправляемый коммутатор. Задача решается настройкой MAC-Based 802.1X на портах управляемого коммутатора.

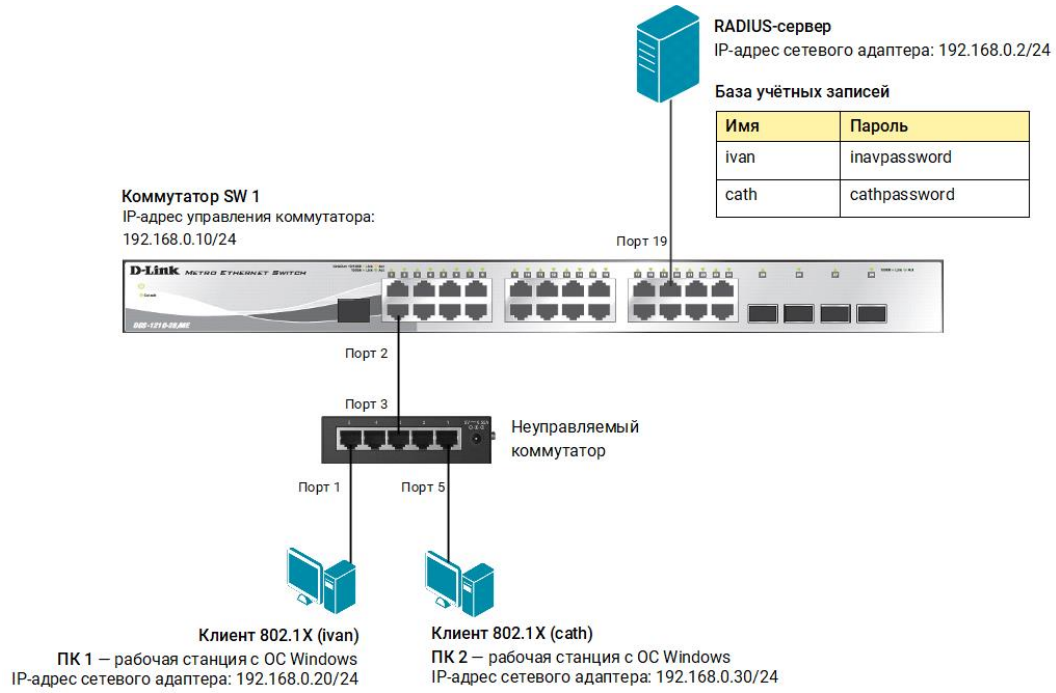


Рис. 2 Схема подключения

Настройка коммутатора SW 1

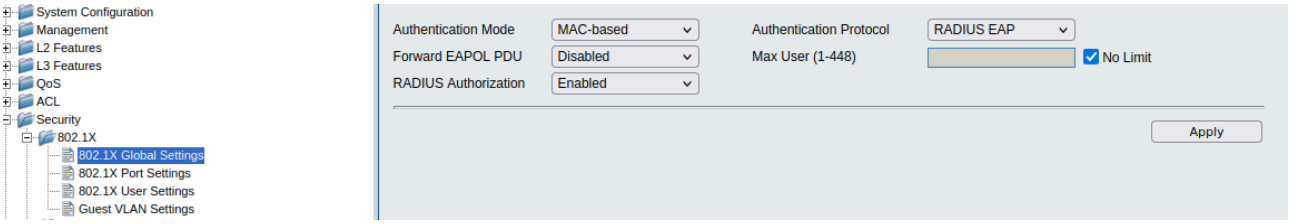
1. Выберите пункт меню **Security** → **802.1X** → **802.1X Global Settings** и выполните следующие настройки:

   –в поле **Authentication Mode** выберите **MAC-based**;

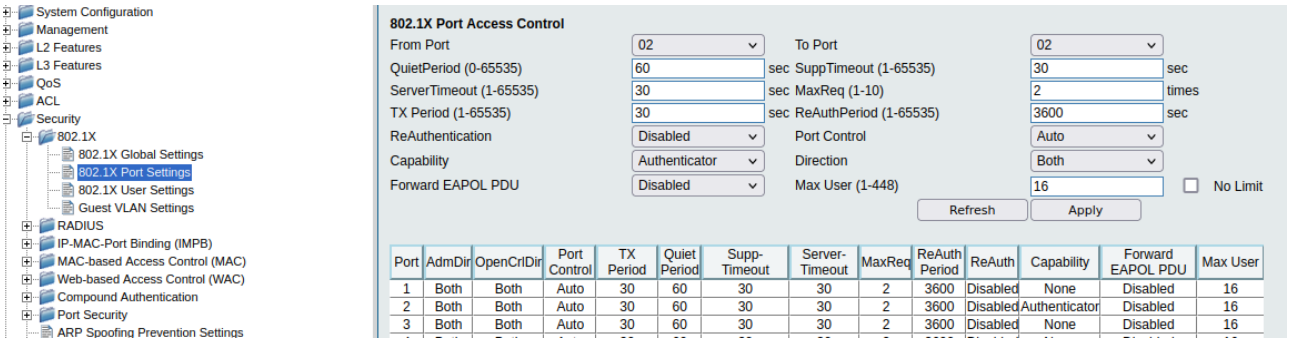
   –в поле **RADIUS Authorization** выберите **Enabled**;

   –в поле **Authentication Protocol** выберите **RADIUS EAP**.

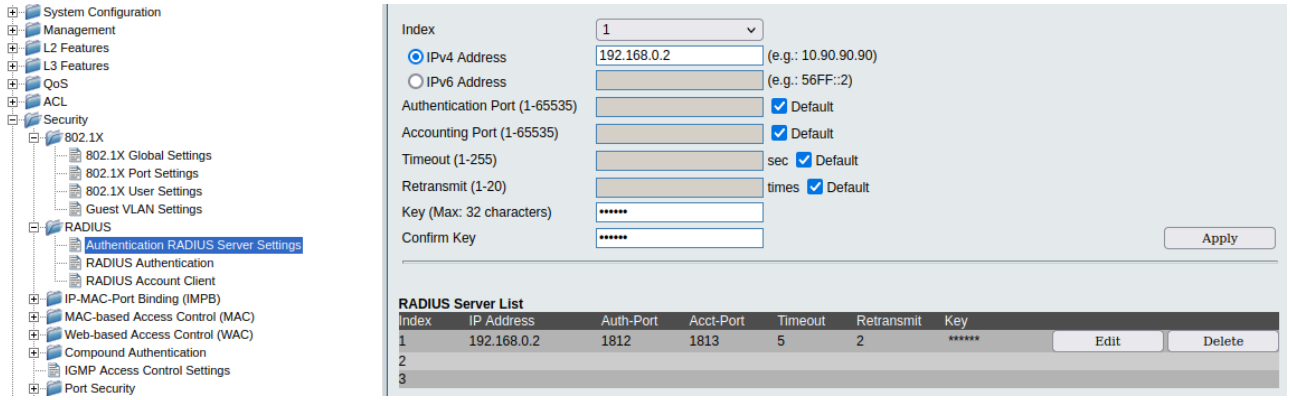
   Нажмите **Apply**.



2. Выберите пункт меню **802.1X Port Settings** и укажите порт, к которому будет подключен неуправляемый коммутатор, выбрав соответствующее значение в полях **From Port** и **To Port** (в примере – порт 2). В поле **Capability** выберите **Authenticator** и нажмите **Apply**.



3. Выберите пункт меню **RADIUS** → **Authentication RADIUS Server Settings**. В поле **IPv4 Address** укажите адрес своего сервера (в примере 192.168.0.2). Введите и подтвердите пароль в полях **Key/Confirm Key**. Нажмите **Apply**.



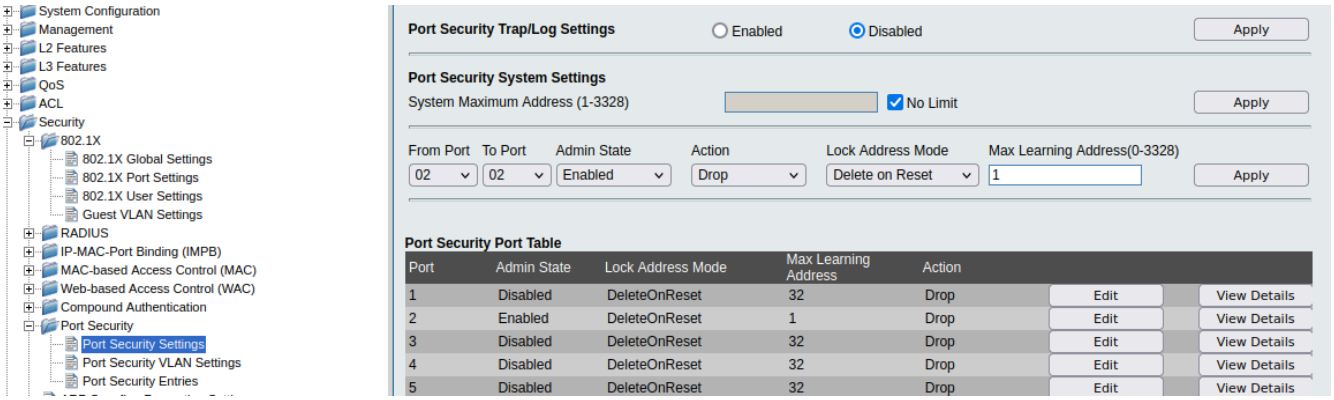
4. Установите максимальное количество изучаемых MAC-адресов равным 1. Для этого в меню слева выберите **Port Security** → **Port Security Settings** и задайте следующие настройки:

   – выберите порт, к которому подключен неуправляемый коммутатор (в примере – порт 2);

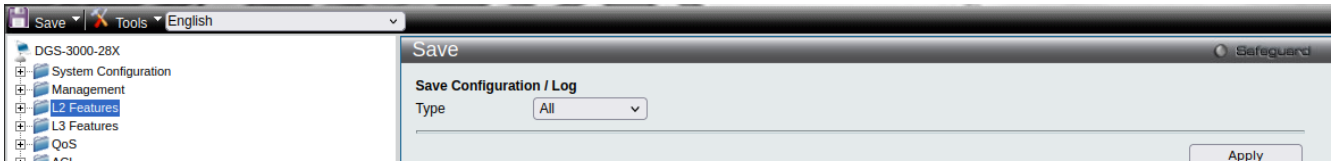
   - в поле **Admin State** выберите **Enabled**;

   - в поле **Action** выберите **Drop**;

   - в поле **Max Learning Address(0-3328)** укажите **1** и нажмите **Apply**.



5. Чтобы сохранить выполненные настройки, в левом верхнем углу нажмите **Save**, выберите **Save Configuration** и нажмите **Apply**.



Задача № 3

В локальной сети необходимо обеспечить аутентификацию пользователей при их подключении к сети. До прохождения успешной аутентификации, или в случае её неуспеха, пользователь должен получать доступ в «гостевую» VLAN.

Задача решается настройкой 802.1X Guest VLAN на коммутаторе. Неаутентифицированным пользователям, находящимся в VLAN 10, разрешен доступ в Интернет. После успешной аутентификации пользователей, порты к которым они подключены, будут добавлены в VLAN 20.

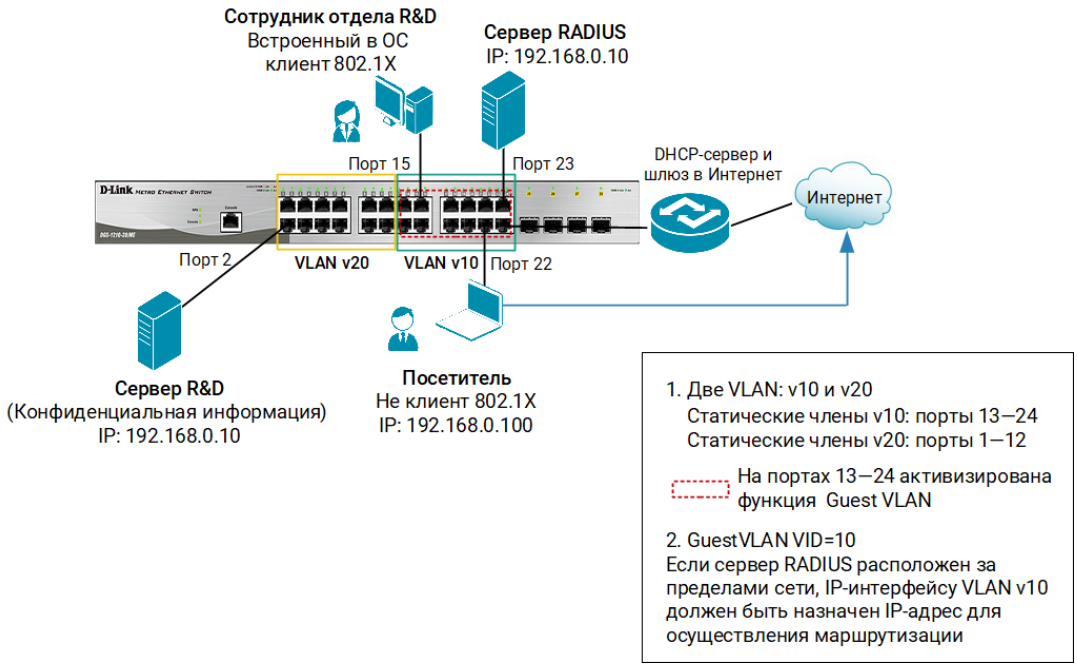
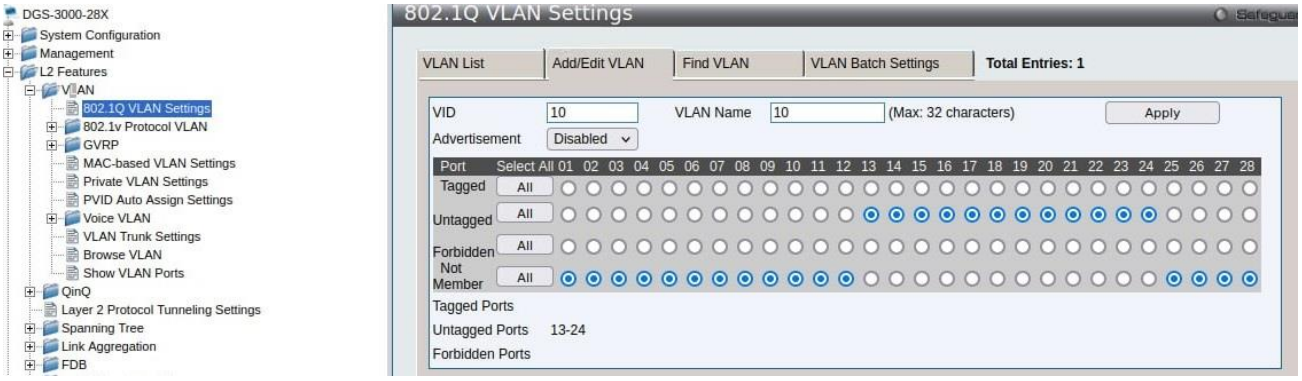
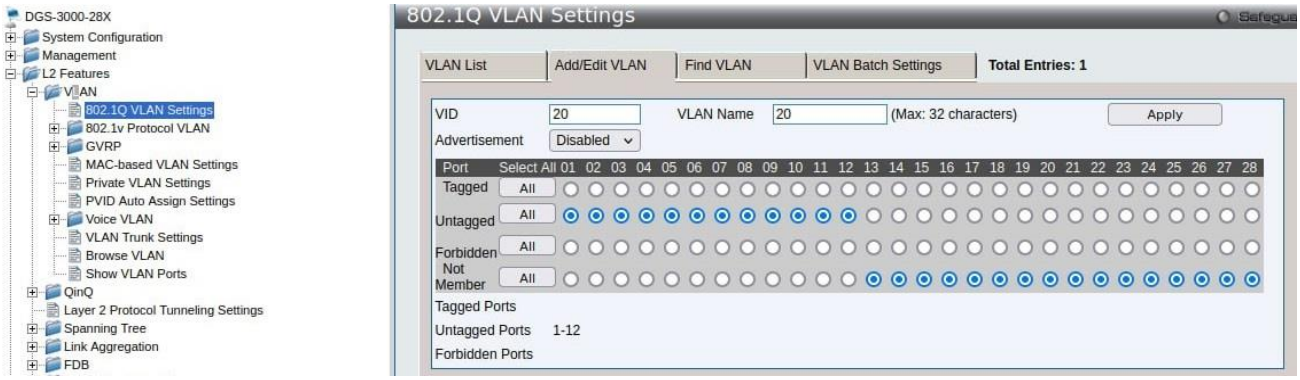


Рис. 3 Схема подключения

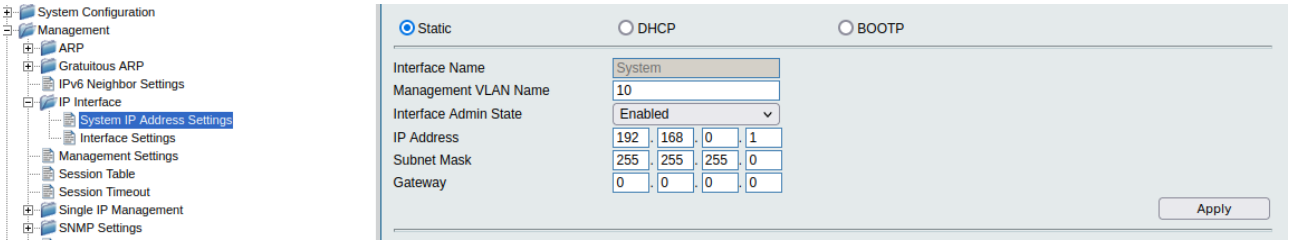
Настройка коммутатора SW 1

1. Выберите пункт меню **L2 Features** → **VLAN** → **802.1Q VLAN Settings**, откройте вкладку **Add/Edit VLAN** и создайте необходимые VLAN (в примере VLAN v10 и v20):
   - в поле **VID** укажите номер VLAN;
   - в поле **VLAN Name** введите название VLAN;
   - отметьте порты, которые будут являться немаркированными членами VLAN, как **Untagged** (в примере: порты 13 – 24 для VLAN v10 и 1 – 12 для VLAN v20)
   - нажмите **Apply**.





2. Создайте IP-интерфейс для VLAN 10. Для этого в меню слева выберите **Management → IP Interface → System IP Address Settings**. В поле **Management VLAN Name** укажите название соответствующей VLAN и нажмите **Apply**.

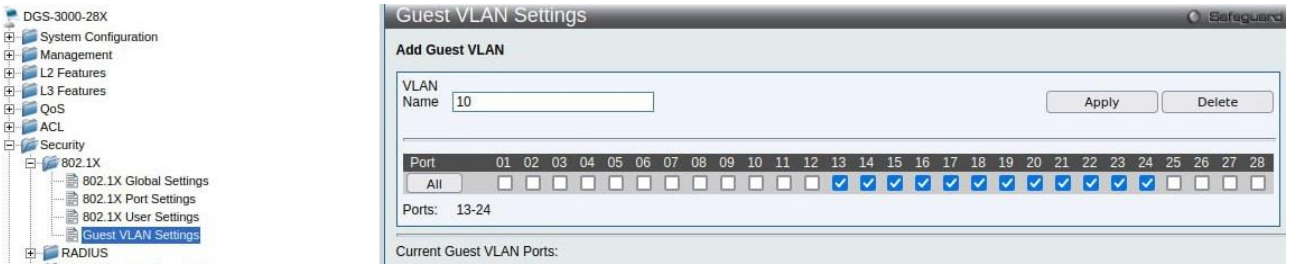


3. Выберите пункт меню **Security → 802.1X → 802.1X Global Settings** и активируйте функцию 802.1X, выполнив следующие настройки:

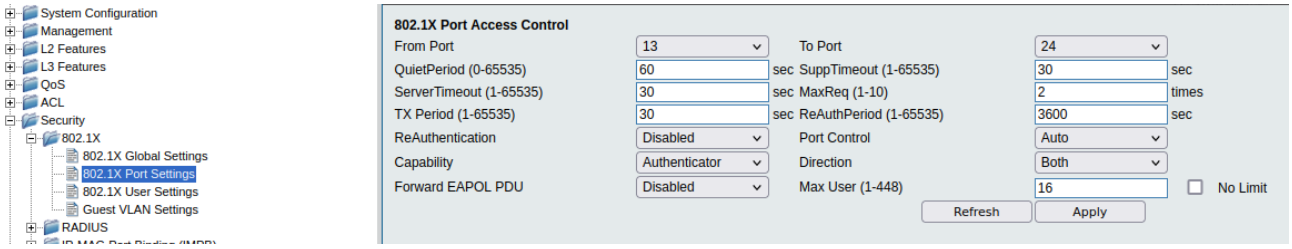
- в поле **RADIUS Authorization** выберите **Enabled**;
- в поле **Authentication Protocol** выберите **RADIUS EAP**.

Нажмите **Apply**.

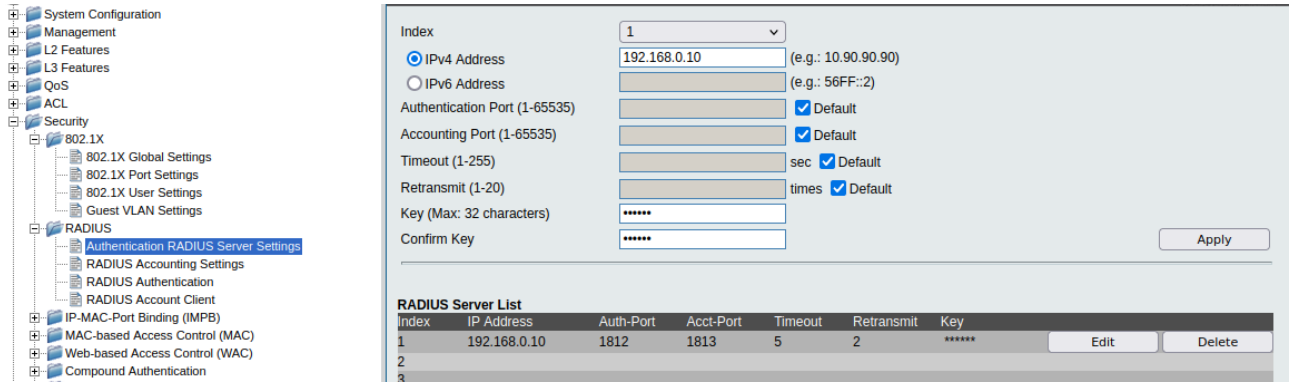
4. В разделе **Guest VLAN Settings** настройте VLAN v10 в качестве гостевой VLAN. Для этого в поле **VLAN Name** укажите **10**, отметьте порты, принадлежащие данной VLAN, и нажмите **Apply**.



5. Выберите пункт меню **802.1X Port Settings** и настройте порты, принадлежащие гостевой VLAN, в качестве аутентификатора. Для этого в полях **From Port** и **To Port** укажите порты **13 – 24**, в поле **Capability** выберите **Authenticator** и нажмите **Apply**.



6. Выберите пункт меню **RADIUS** → **Authentication RADIUS Server Settings**. В поле **IPv4 Address** укажите адрес своего сервера (в примере 192.168.0.10). Введите и подтвердите пароль в полях **Key/Confirm Key**. Нажмите **Apply**.



7. Чтобы сохранить выполненные настройки, в левом верхнем углу нажмите **Save**, выберите **Save Configuration** и нажмите **Apply**.