Пример настройки 802.1X

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:

- Multi-host;

- Multi-auth.

Если порт работает в режиме **multi-host** и аутентифицирован один из узлов, подключенных к порту, то всем другим узлам будет разрешен доступ к порту. Согласно аутентификации 802.1X, если повторная аутентификация завершается неудачно или аутентифицированный пользователь выходит из учетной записи, порт будет блокироваться на период молчания (quiet period). Порт восстановит обработку пакетов EAPOL после периода молчания.

Если порт работает в режиме **multi-auth**, каждый узел должен проходить аутентификацию индивидуально для доступа к порту. Узел представлен своим MAC-адресом. Доступ к сети будет только у авторизованных узлов.

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 активированной 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-1250, DGS-1510, DGS-1520, DGS-3130, DGS-3630, DXS-3610.

Задача 1

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

Задача решается настройкой аутентификации 802.1X в режиме multi-host на портах коммутаторах.

Кроме коммутатора, нужно настроить RADIUS-сервер и 802.1X-клиент на рабочей станции. В качестве RADIUS-сервера может использоваться различное ПО, например, freeradius для ОС Linux.

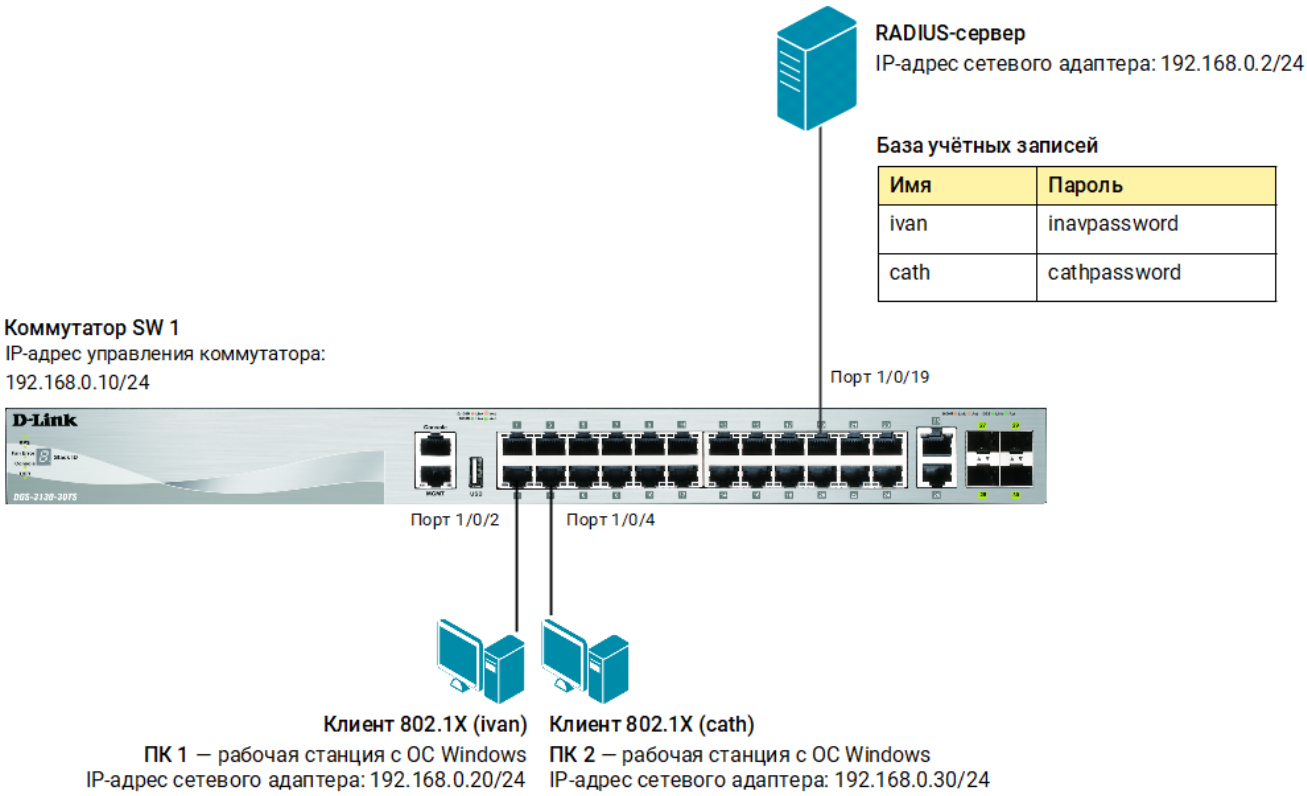

Рис. 1 Схема подключения

Настройка клиента 802.1X на рабочей станции с ОС Windows 10

1. Нажмите комбинацию клавиш **Win+R**, в текстовом поле введите команду **services.msc** и нажмите клавишу **Enter**.

2. Выберите в списке службу **Проводная автонастройка** и двойным щелчком мыши откройте окно настроек.

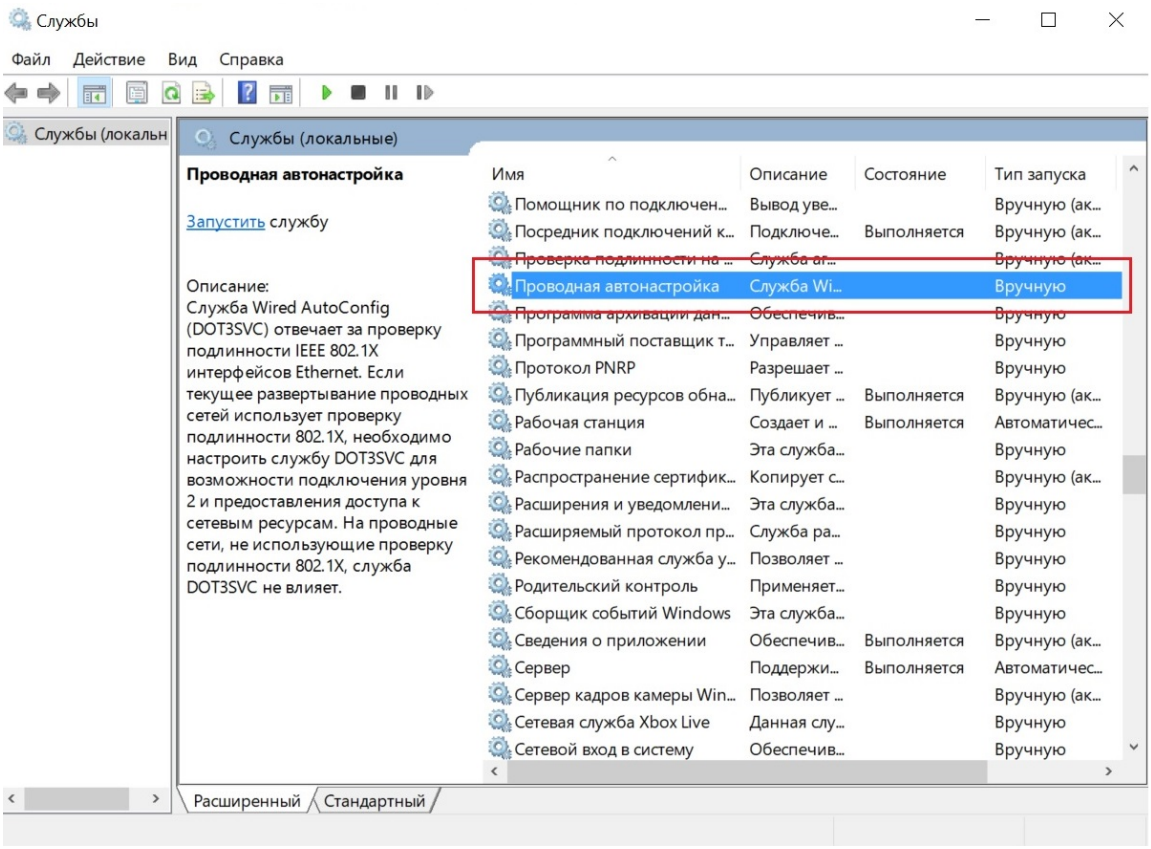

Рис. 2 Служба Проводная автонастройка

3. В открывшемся окне выберите тип запуска **Автоматически** и нажмите кнопку **Запустить**. Когда служба запустится, нажмите кнопку **ОК**.

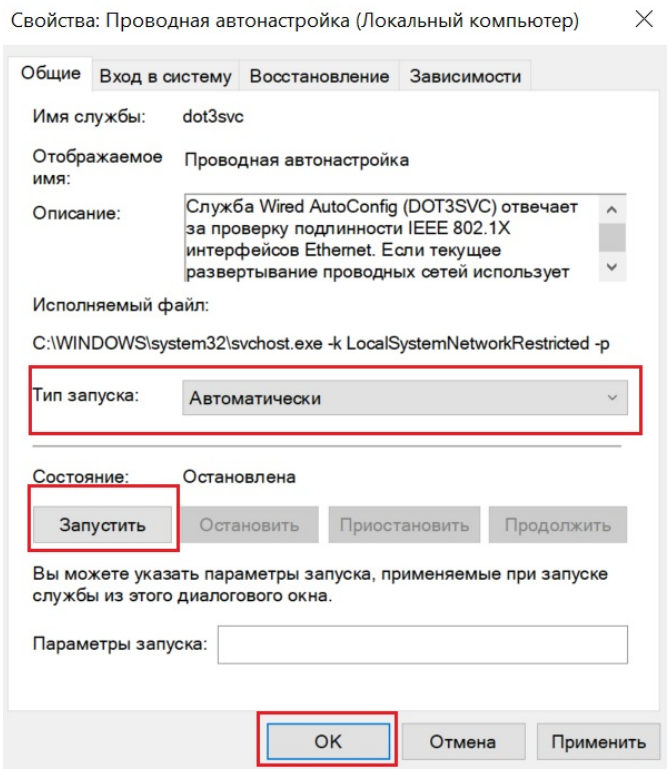

Рис. 3 Запуск службы Проводная автонастройка

4. Кликните правой кнопкой мыши **Пуск → Параметры → Сеть и Интернет→ Ethernet → Центр управления сетями и общим доступом → Изменение параметров адаптера**.

5. Выберите **Подключение по локальной сети**, кликните по нему правой кнопкой мыши и выберите **Свойства**.

6. Во вкладке **Проверка подлинности** установите галочку **Включить проверку подлинности IEEE 802.1X**. Нажмите кнопку **Параметры**.

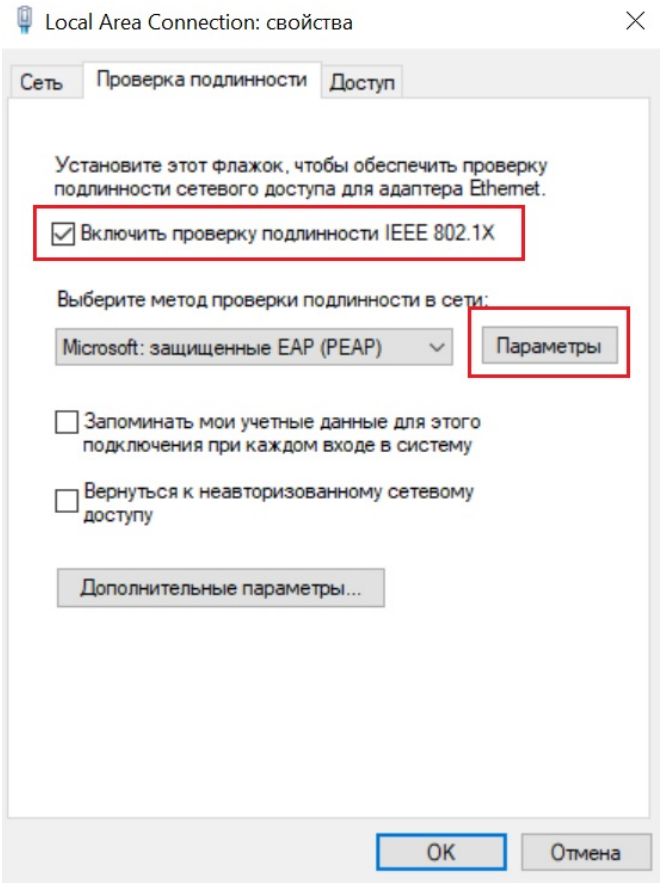

Рис. 4 Окно Проверка подлинности

7. В открывшемся окне снимите галочку **Подтверждать удостоверение сервера с помощью проверки сертификата** и нажмите кнопку **Настроить**.

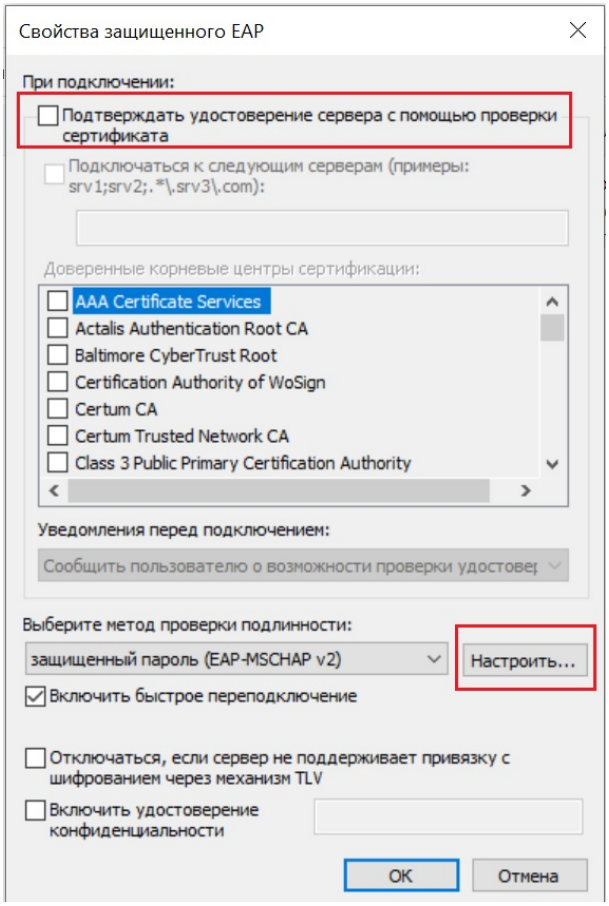

Рис. 5 Настройка свойств защищённого EAP

8. В открывшемся окне снимите галочку **Использовать автоматически имя и пароль из Windows** и нажмите кнопку **OK**. В окне **Свойства защищенного EAP** нажмите кнопку **OK**.

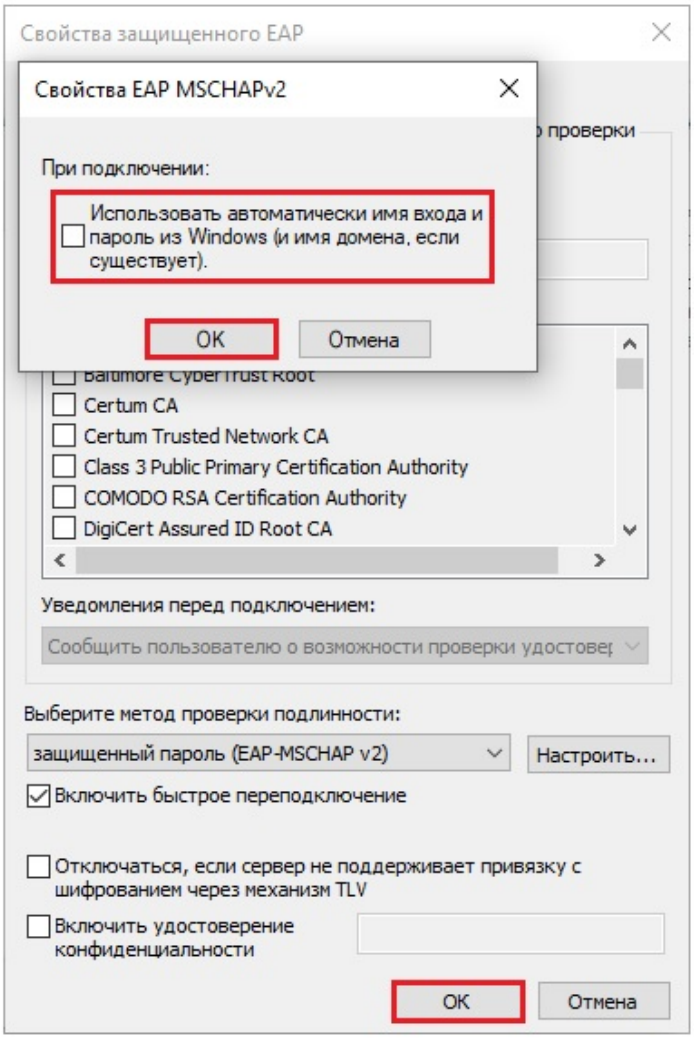

Рис. 6 Настройка свойств защищённого EAP

9. Во вкладке **Проверка подлинности** нажмите кнопку **Дополнительные параметры**. В открывшемся окне установите галочку **Указать режим проверки пользователя**, в выпадающем списке **Проверка подлинности** выберите параметр **Проверка подлинности пользователя** и нажмите кнопку **Сохранить учётные данные**. В открывшемся окне введите имя пользователя **ivan**, пароль — **ivanpassword**. Нажмите кнопку **OK**.

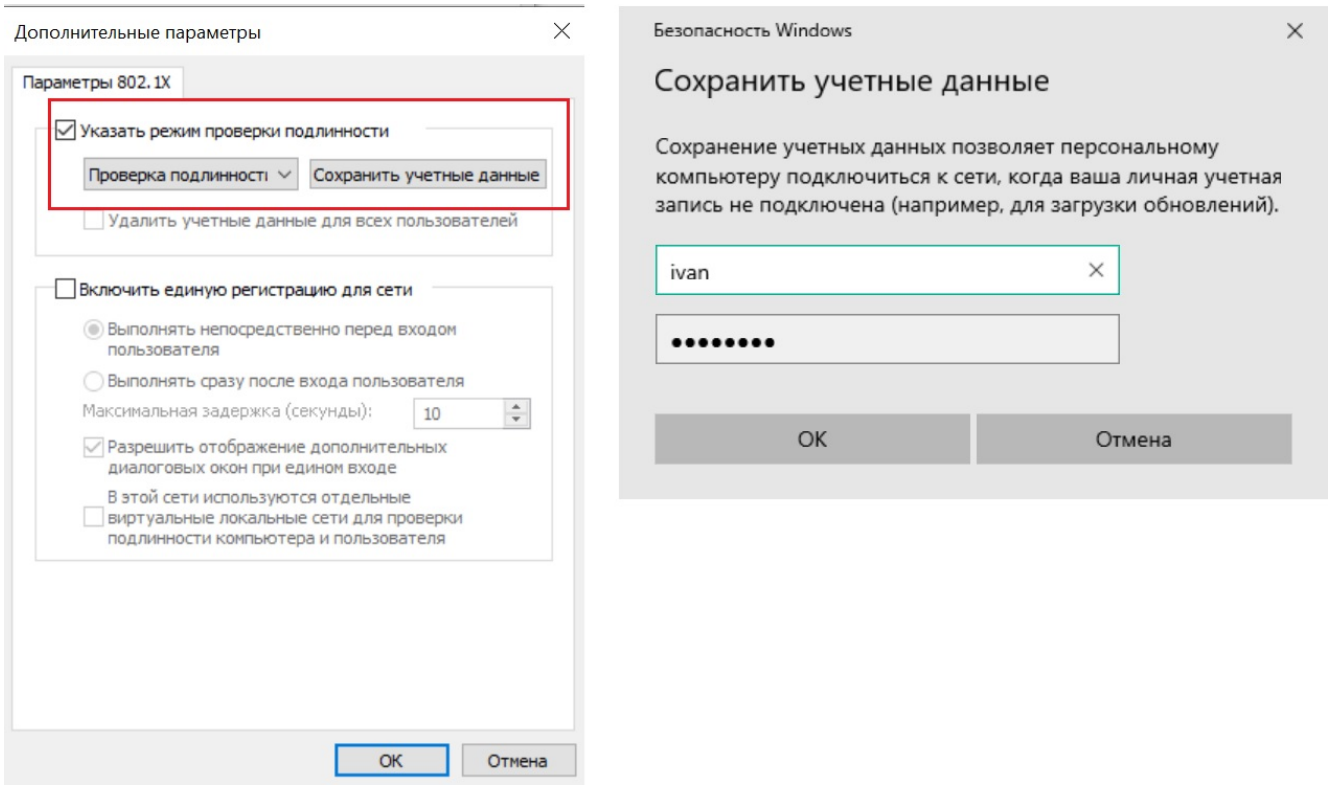

Рис. 7 Настройка проверки подлинности пользователя

Настройка коммутатора SW1

1. Настройте IP-адрес интерфейса VLAN 1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.0.10 255.255.255.0
Switch(config-if)# exit
```

> **Примечание**
>
> VLAN 1 существует на коммутаторе по умолчанию. Если в вашей сети используется другая VLAN, то настройте её интерфейс.

2. Активируйте функцию 802.1X:

```
Switch(config)# aaa new-model
Switch(config)# dot1x system-auth-control
```

3. Настройте параметры RADIUS-сервера:

```
Switch(config)# radius-server host 192.168.0.2 key dlinkpassword
```

4. Настройте порты 1/0/2 и 1/0/4 в качестве аутентификатора и укажите режим работы портов **multi-host**:

```
Switch(config)# interface range ethernet 1/0/2,1/0/4
Switch(config-if-range)# dot1x pae authenticator
Switch(config-if-range)# authentication host-mode multi-host
Switch(config-if-range)# exit
```

5. Создайте группу серверов RADIUS с именем **dot1x**:

```
Switch(config)# aaa group server radius dot1x
Switch(config-sg-radius)# server 192.168.0.2
Switch(config-sg-radius)# exit
```

6. Укажите, что группа серверов **dot1x** будет использоваться для аутентификации:

```
Switch(config)# aaa authentication dot1x default group dot1x
```

Задача 2

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

Задача решается настройкой аутентификации 802.1X в режиме multi-auth на портах управляемого коммутатора.

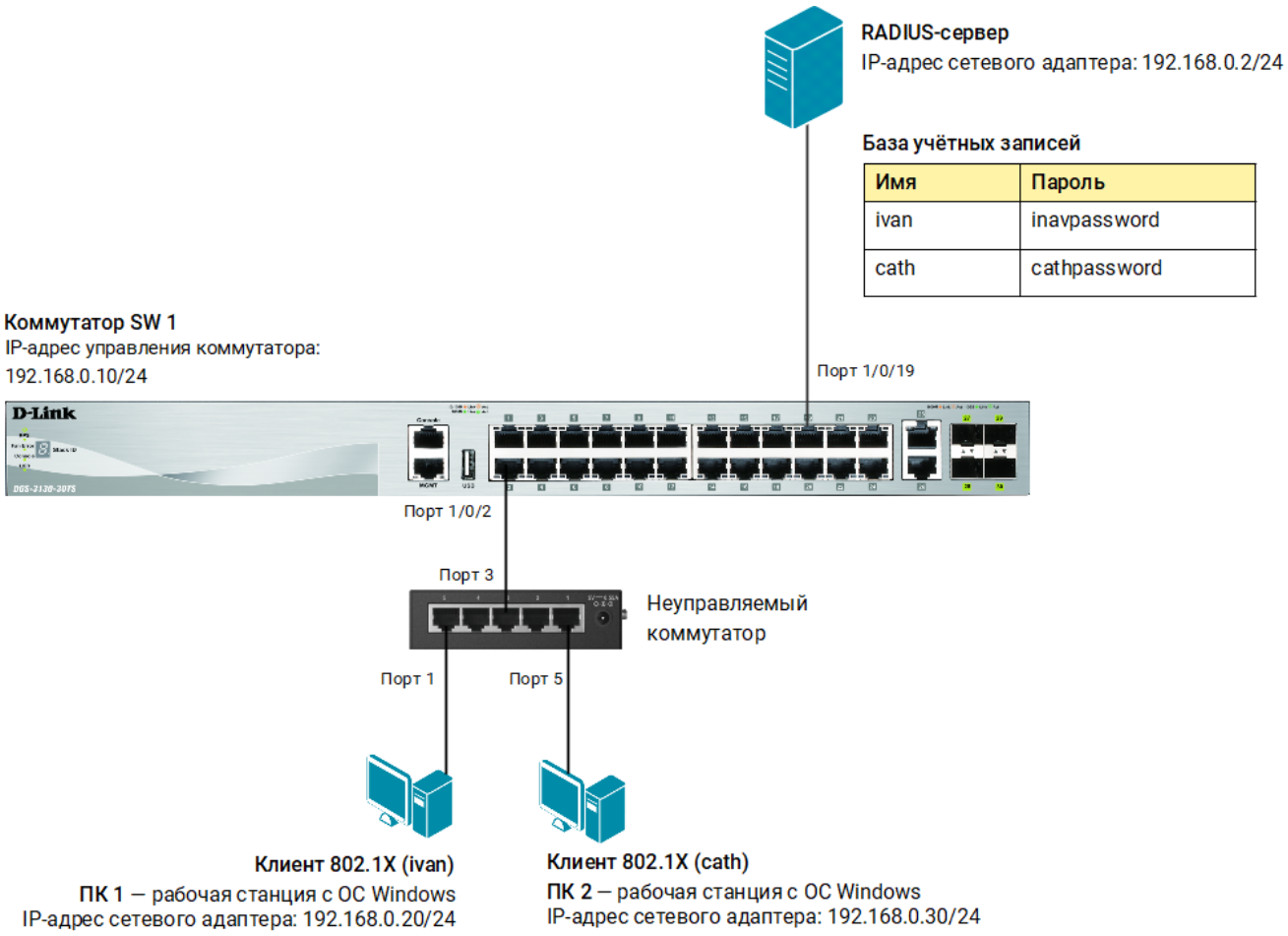

Рис. 8 Схема подключения

Настройка коммутатора SW1

1. Настройте IP-адрес интерфейса VLAN 1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.0.10 255.255.255.0
Switch(config-if)# exit
```

> **Примечание**
>
> VLAN 1 существует на коммутаторе по умолчанию. Если в вашей сети используется другая VLAN, то настройте её интерфейс.

2. Активируйте функцию 802.1X:

```
Switch(config)# aaa new-model
Switch(config)# dot1x system-auth-control
```

3. Настройте параметры RADIUS-сервера:

```
Switch(config)# radius-server host 192.168.0.2 key dlinkpassword
```

4. Настройте порт 1/0/2 в качестве аутентификатора и укажите его режим работы **multi-host**:

```
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# authentication host-mode multi-auth
Switch(config-if)# exit
```

5. Создайте группу серверов RADIUS с именем **dot1x**:

```
Switch(config)# aaa group server radius dot1x
Switch(config-sg-radius)# server 192.168.0.2
Switch(config-sg-radius)# exit
```

6. Укажите, что группа серверов **dot1x** будет использоваться для аутентификации:

```
Switch(config)# aaa authentication dot1x default group dot1x
```

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.

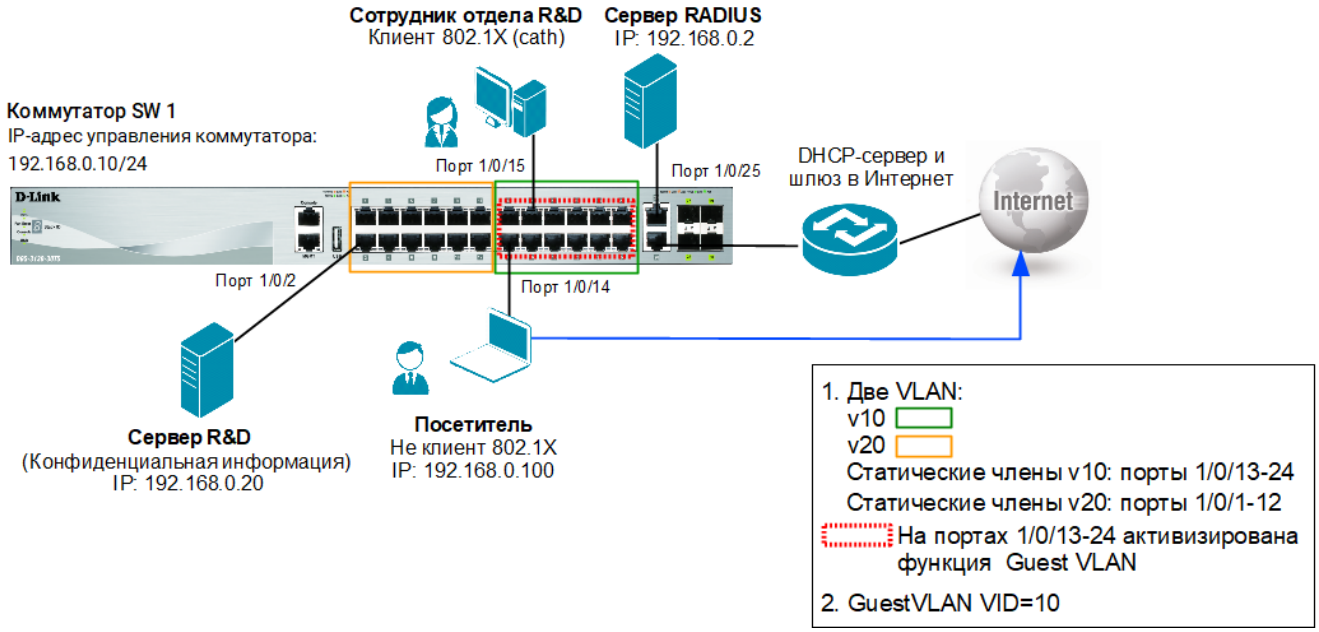

Рис. 9 Схема подключения

Настройка коммутатора SW1

1. Настройте IP-адрес интерфейса VLAN 1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.0.10 255.255.255.0
Switch(config-if)# exit
```

> **Примечание**
>
> VLAN 1 существует на коммутаторе по умолчанию. Если в вашей сети используется другая VLAN, то настройте её интерфейс.

2. Создайте на коммутаторе VLAN v10 и v20:

```
Switch(config)#vlan 10
Switch(config-vlan)#name v10
Switch(config-vlan)#exit
Switch(config)#interface range ethernet 1/0/13-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name v20
```

```
Switch(config-vlan)#exit
Switch(config)#interface range ethernet 1/0/1-12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

3. Настройте VLAN v10 в качестве гостевой VLAN:

```
Switch(config)#interface range ethernet 1/0/13-24
Switch(config-if-range)# authentication guest-vlan 10
Switch(config-if-range)#exit
```

4. Активируйте функцию 802.1X:

```
Switch(config)# aaa new-model
Switch(config)# dot1x system-auth-control
```

5. Настройте параметры RADIUS-сервера:

```
Switch(config)# radius-server host 192.168.0.2 key dlinkpassword
```

6. Настройте порты 1/0/13-24, к которым подключаются гости, в качестве аутентификатора и укажите режим работы портов **multi-host**:

```
Switch(config)# interface range ethernet 1/0/13-24
Switch(config-if-range)#dot1x pae authenticator
Switch(config-if-range)#authentication host-mode multi-host
Switch(config-if-range)#exit
```

> **Примечание**
>
> Функция Guest VLAN поддерживается только для аутентификации Multi-host 802.1X.

7. Создайте группу серверов RADIUS с именем **dot1x**:

```
Switch(config)# aaa group server radius dot1x
Switch(config-sg-radius)# server 192.168.0.2
```

```
Switch(config-sg-radius)# exit
```

8. Укажите, что группа серверов **dot1x** будет использоваться для аутентификации:

```
Switch(config)# aaa authentication dot1x default group dot1x
```

> **Примечание**
>
> Настройка параметров на сервере RADIUS включает установку следующих пользовательских атрибутов:
>
> Tunnel-Medium-Type (65) = 802
>
> Tunnel-Pvt-Group-ID (81) = 20 ← VID
>
> Tunnel-Type (64) = VLAN