Пример настройки аутентификации 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:

- 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 коммутаторов с D-Link-like CLI.

Задача № 1

В локальной сети необходимо обеспечить аутентификацию пользователей при подключении их к сети. Задача решается настройкой Port-Based 802.1X на портах коммутатора. Кроме коммутатора, необходимо настроить RADIUS-сервер и 802.1X-клиент на рабочей станции. В качестве RADIUS-сервера можно использовать пакет **freeradius** для ОС Linux.

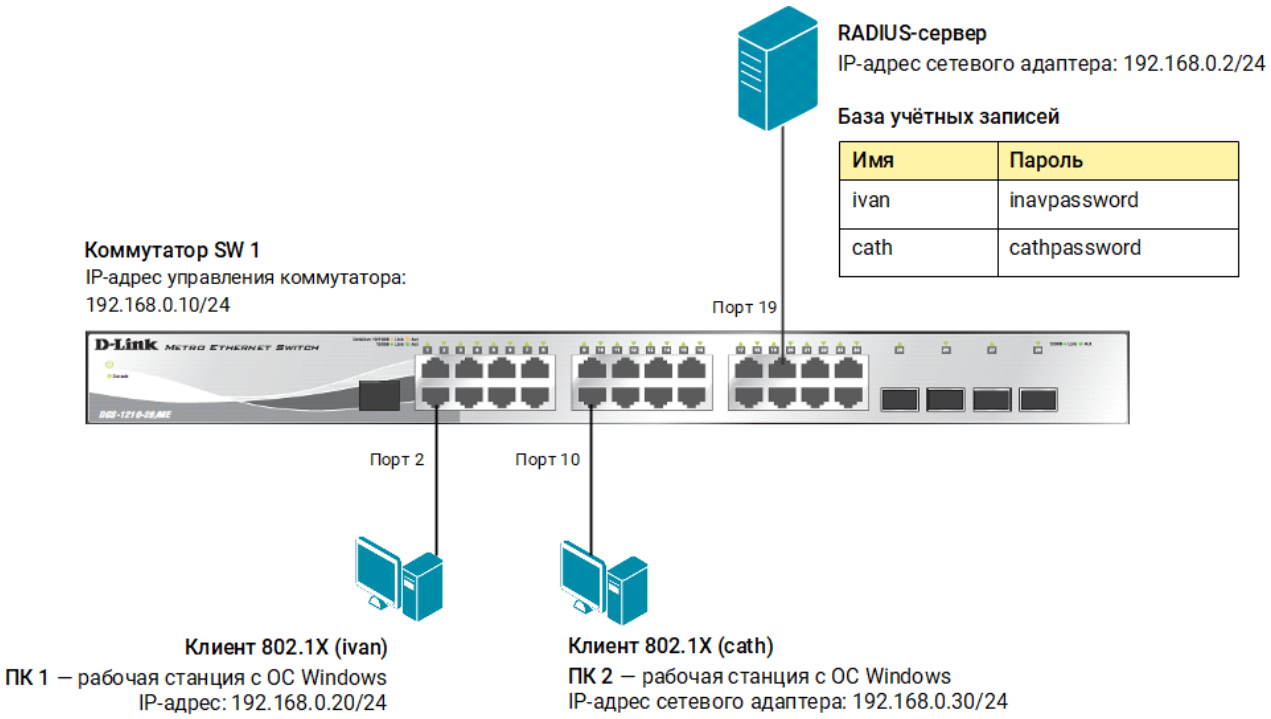

Рис. 1 Схема подключения

Настройка коммутатора SW 1

1. Измените IP-адрес интерфейса управления коммутатора:

```
config ipif System ipaddress 192.168.0.10/24
```

2. Активируйте функцию 802.1X:

```
enable 802.1x
```

3. Настройте проверку подлинности пользователей на RADIUS-сервере:

```
config 802.1x auth_protocol radius_eap
```

4. Настройте тип аутентификации 802.1X (port-based):

```
config 802.1x auth_mode port_based
```

5. Настройте порты в качестве аутентификатора:

```
config 802.1x capability ports 2,10 authenticator
```

6. Настройте параметры RADIUS-сервера:

```
config radius add 1 192.168.0.2 key dlinkpassword
```

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.

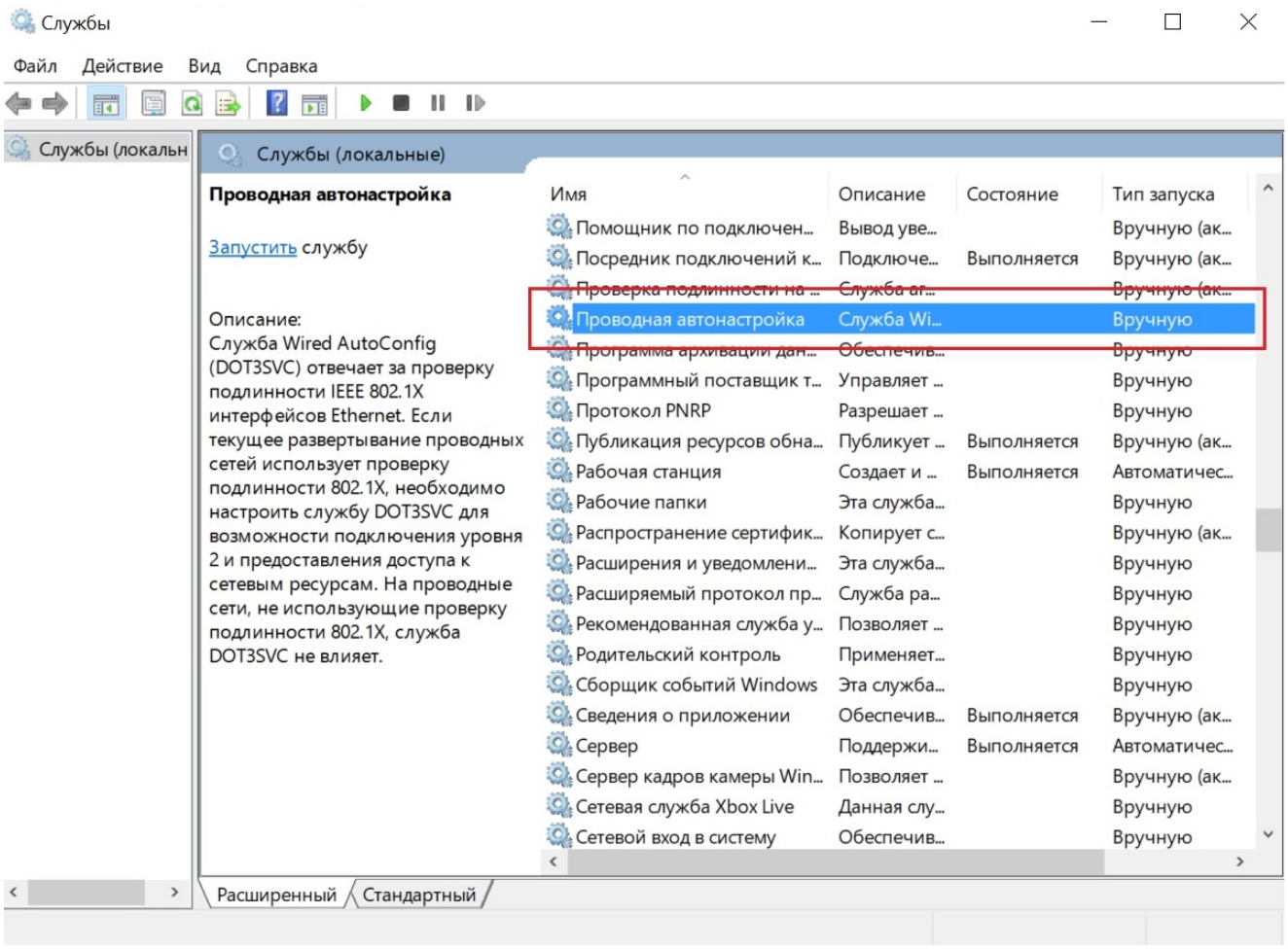

Рис. 2 Служба Проводная автонастройка

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

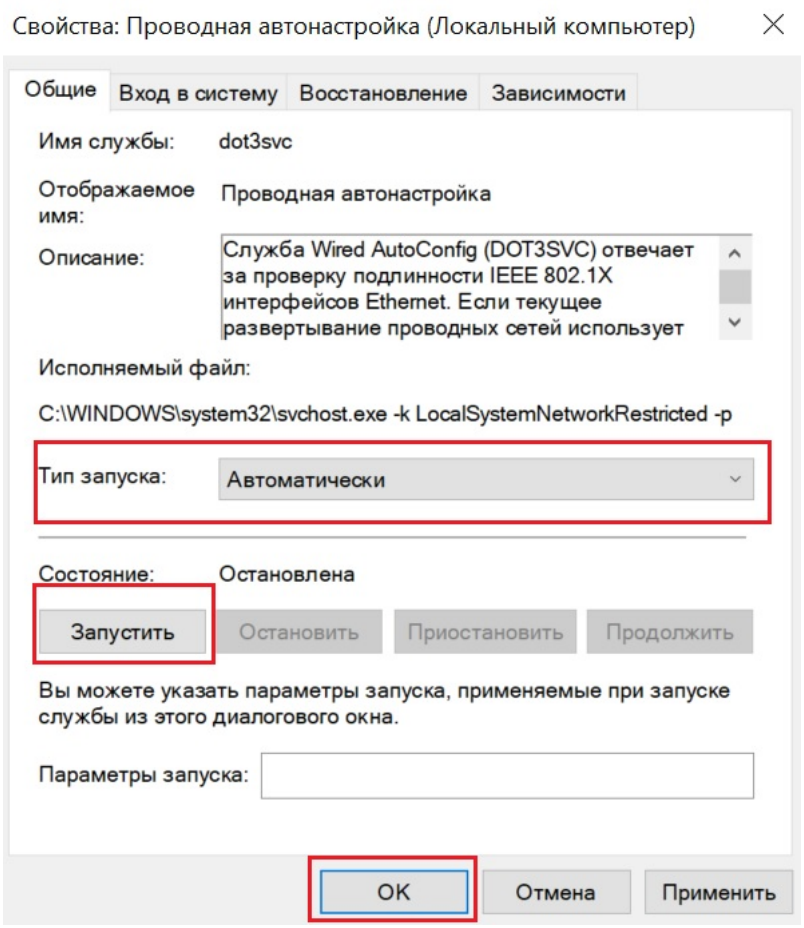

Рис. 3 Запуск службы Проводная автонастройка

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**.

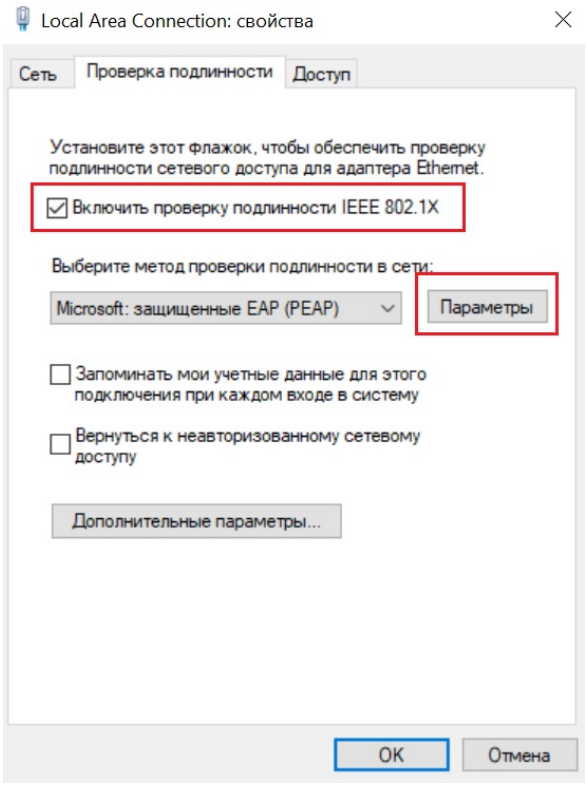

Рис. 4 Окно Проверка подлинности

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

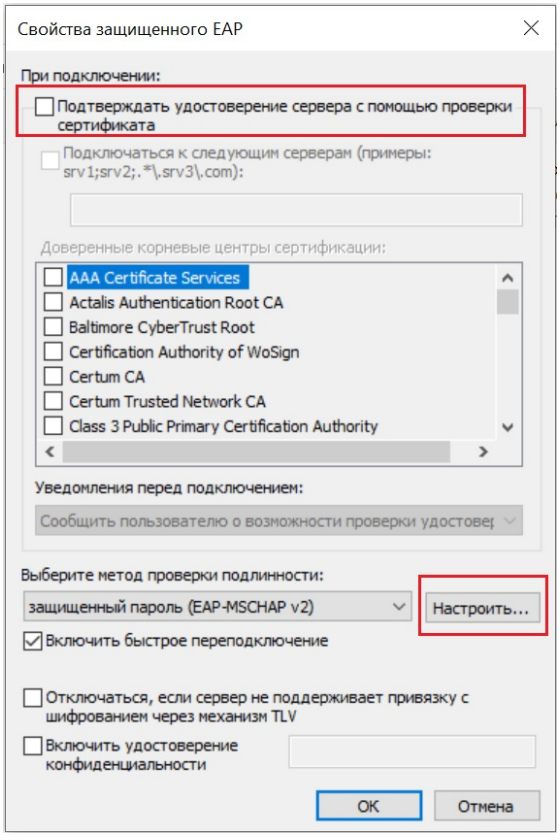

Рис. 5 Настройка свойств защищённого EAP

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

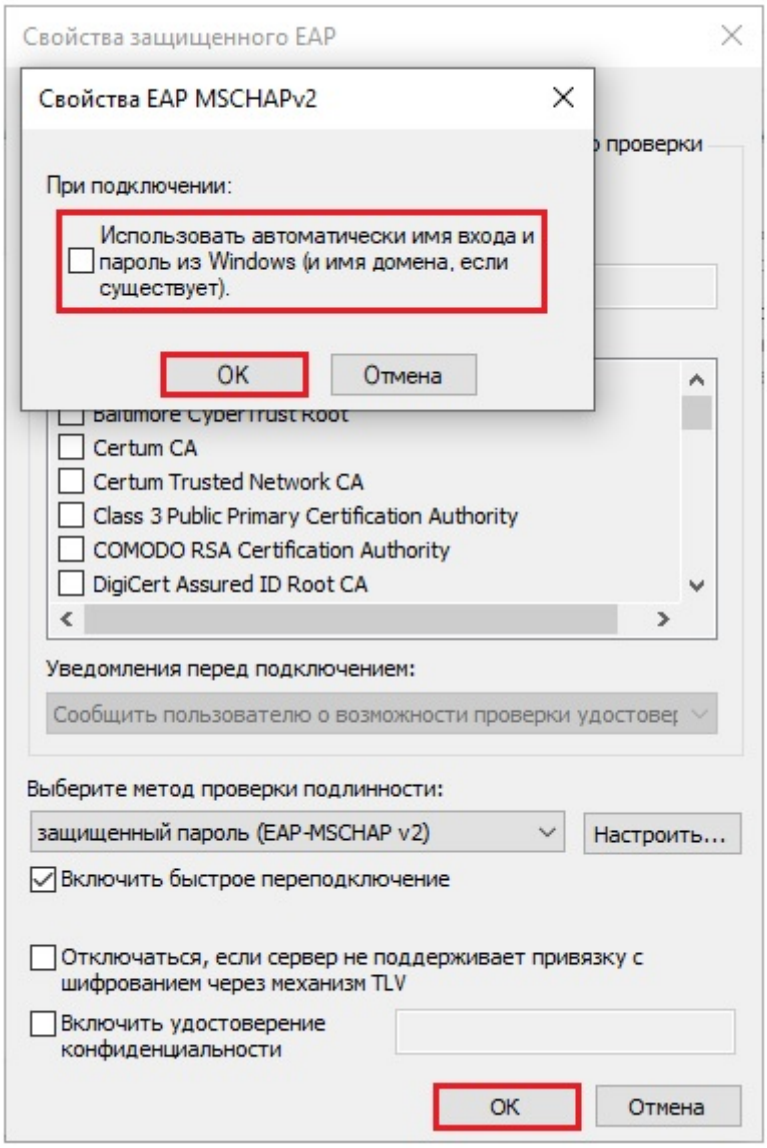

Рис. 6 Настройка свойств защищённого EAP

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 **ОК**.

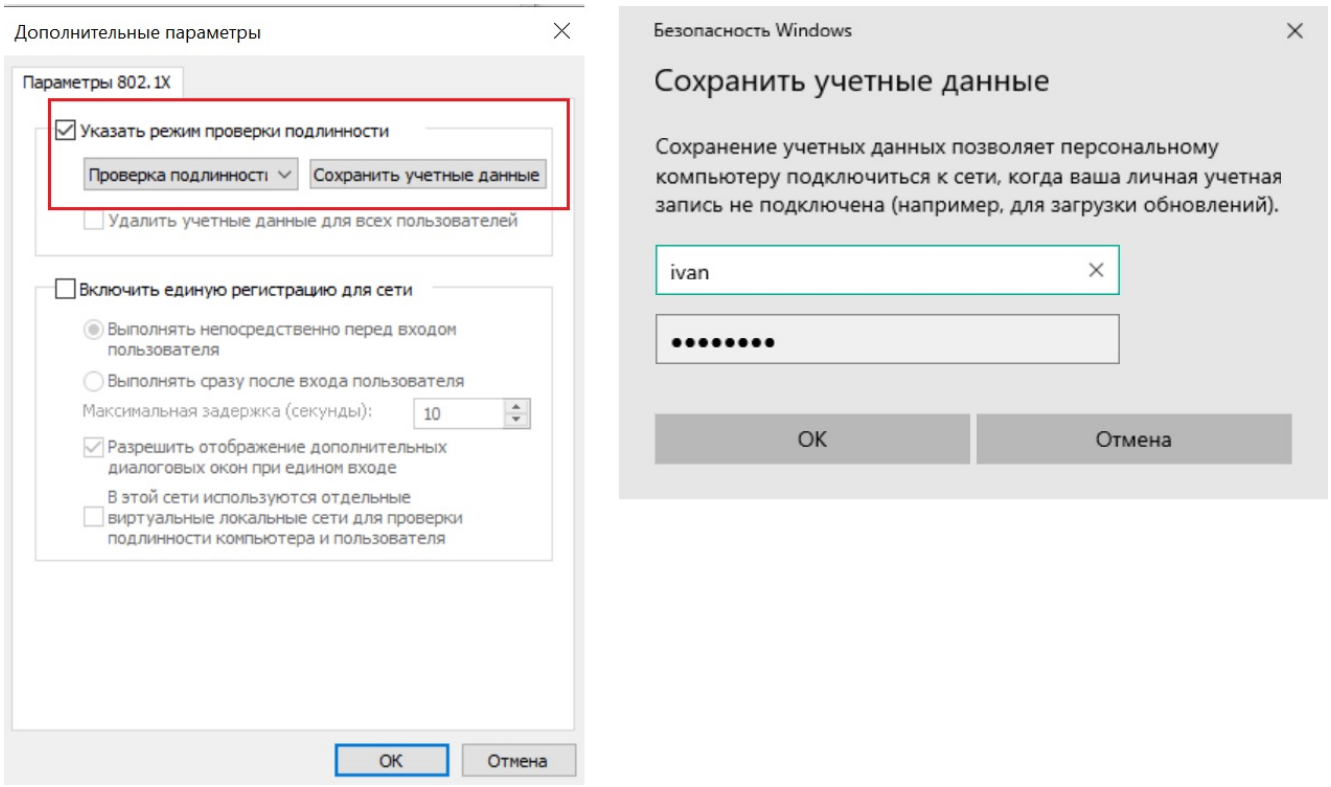

Рис. 7 Настройка проверки подлинности пользователя

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.

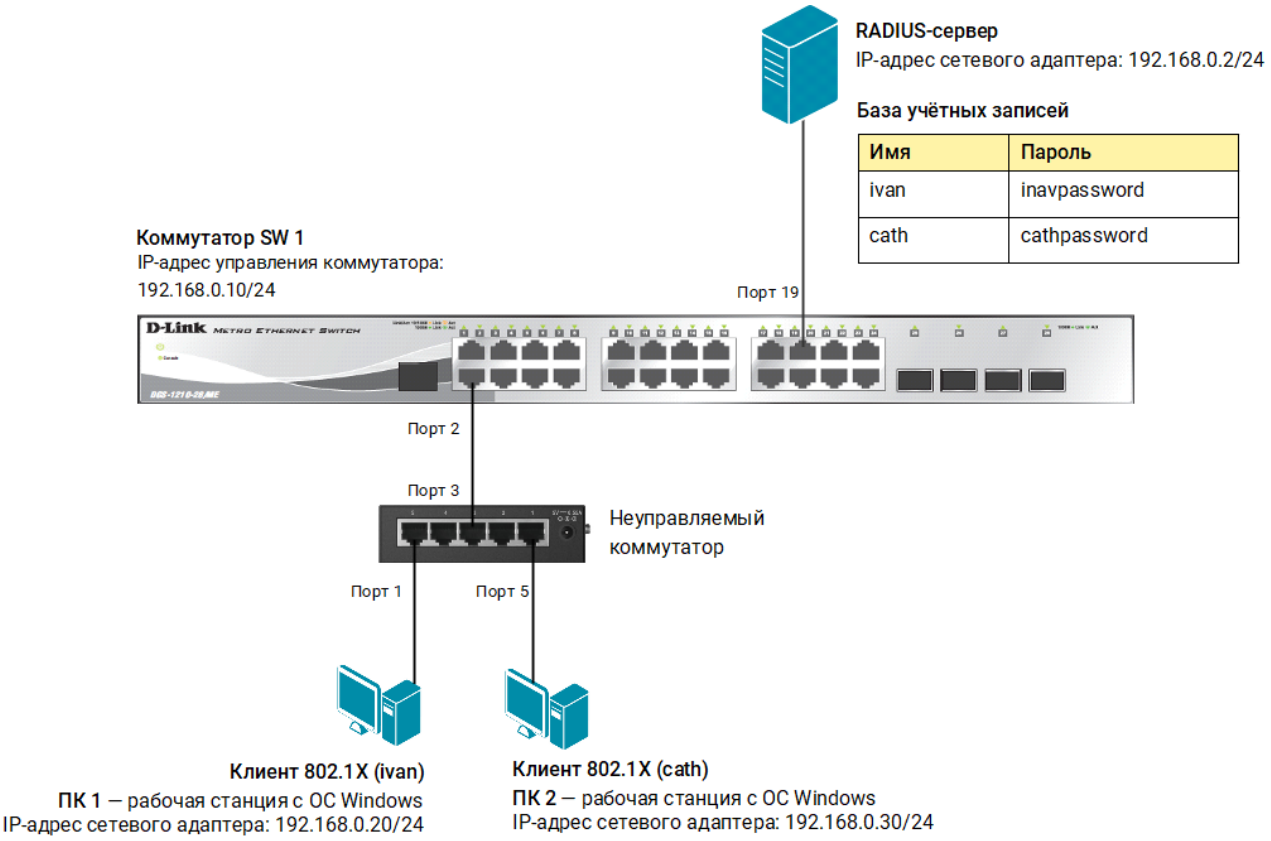

Рис. 8 Схема подключения

Настройка коммутатора SW 1

1. Активируйте функцию 802.1X:

```
enable 802.1x
```

2. Настройте проверку подлинности пользователей на RADIUS-сервере:

```
config 802.1x auth_protocol radius_eap
```

3. Настройте тип аутентификации 802.1X (MAC-based):

```
config 802.1x auth_mode mac_based
```

4. Настройте порт в качестве аутентификатора:

```
config 802.1x capability ports 2 authenticator
```

5. Настройте параметры RADIUS-сервера:

```
config radius add 1 192.168.0.2 key dlinkpassword
```

6. Установите максимальное количество изучаемых MAC-адресов равным 1:

```
config port_security 2 admin_state enable max_learning_addr 1
```

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.

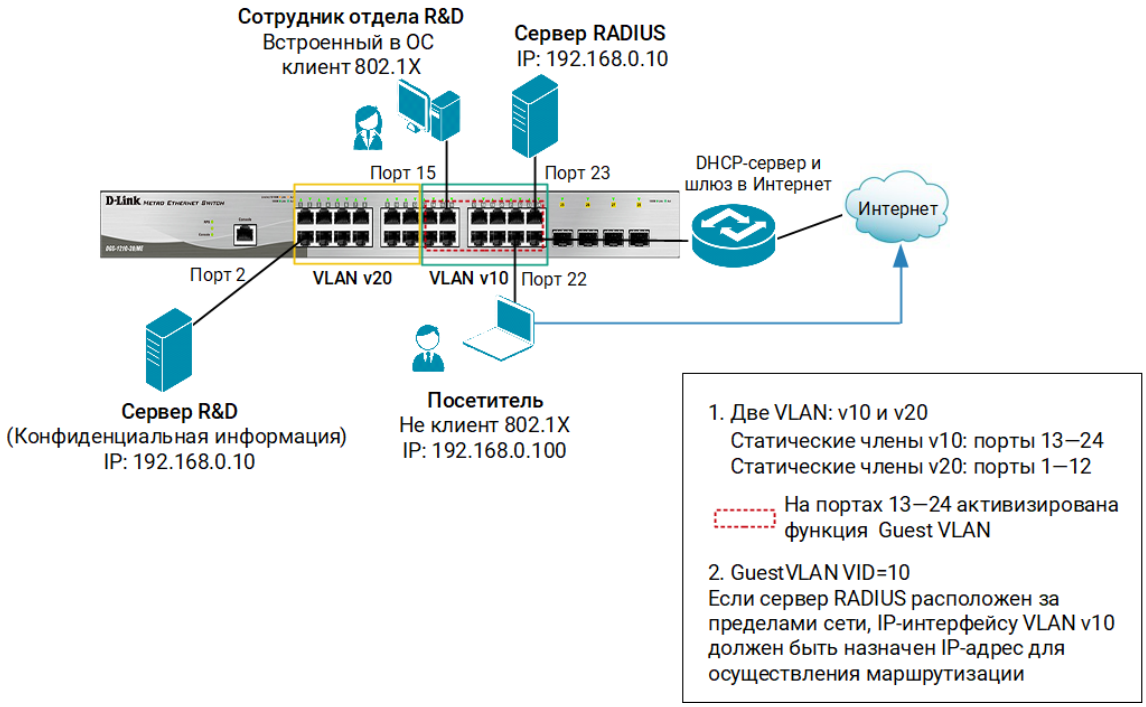

Рис. 9 Схема подключения

Настройка коммутатора SW 1

1. Создайте на коммутаторе VLAN v10 и v20:

```
config vlan default delete 1-24

create vlan v10 tag 10
config vlan v10 add untagged 13-24

create vlan v20 tag 20
config vlan v20 add untagged 1-12

config ipif System ipaddress 192.168.0.1/24 vlan v10
```

2. Активируйте функцию 802.1X:

```
enable 802.1x
```

3. Настройте проверку подлинности пользователей на RADIUS-сервере:

```
config 802.1x auth_protocol radius_eap
```

4. Настройте VLAN v10 в качестве гостевой VLAN:

```
create 802.1x guest_vlan v10
config 802.1x guest_vlan ports 13-24 state enable
```

5. Настройте порты в качестве аутентификатора:

```
config 802.1x capability ports 13-24 authenticator
```

6. Настройте параметры RADIUS-сервера:

```
config radius add 1 192.168.0.10 key dlinkpassword auth_port 23
```