

Пример настройки аутентификации 802.1Х

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 802.1Х, 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 МАС-адресов).

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

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

Функция 802.1X Guest VLAN используется для создания гостевой VLAN с ограниченными правами для пользователей, не прошедших аутентификацию. подключается Когда клиент К порту коммутатора С активизированной аутентификацией 802.1X функцией Guest VLAN, И 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 OC 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 802.1Х:

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 802.1Х 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.

| 🗳 Службы — 🗆 🗙 | | | | | | | | |
|---------------------------|---|---|---|----------------------------|---|---|--|--|
| Файл Действие Вид Справка | | | | | | | | |
| 🗢 🔿 🔲 🗔 | i 🔒 🛿 🧊 🕨 🔳 🕪 | | | | | | | |
| 🎑 Службы (локальн | 🔍 Службы (локальные) | | | | | | | |
| | Проводная автонастройка | Лмя | Описание | Состояние | Тип запуска | ^ | | |
| | <u>Запустить</u> службу | Помощник по подключен Посредник подключений к Проверка подлинности на | Вывод уве Подключе Служба аг | Выполняется | Вручную (ак Вручную (ак Вручную (ак | _ | | |
| | Описание: Служба Wired AutoConfig (DOT3SVC) отвечает за проверку подлинности IEEE 802.1X интерфейсов Ethernet. Если текущее развертывание проводных сетей использует проверку подлинности 802.1X, необходимо настроить службу DOT3SVC для возможности подключения уровня 2 и предоставления доступа к сетевым ресурсам. На проводные сети, не использующие проверку подлинности 802.1X, служба DOT3SVC не влияет. | 🙀 Проводная автонастройка | Служба Wi | | Вручную | | | |
| | | Программа архивации дан Программный поставщик т Протокол PNRP Публикация ресурсов обна Рабочая станция Рабочие папки Рабочие папки Распространение сертифик Расширения и уведомлени Расширяемый протокол пр Расширяемый протокол пр Рекомендованная служба у Родительский контроль Сборщик событий Windows | Управляет Разрешает Публикует Создает и Эта служба Копирует с Эта служба ра Позволяет Применяет Эта служба | Выполняется Выполняется | Вручную Вручную Вручную (ак Автоматичес Вручную Вручную Вручную Вручную Вручную Вручную Вручную | | | |
| < >> | Расширенный / Стандартный / | Сведения о приложении Сервер Сервер кадров камеры Win Сетевая служба Xbox Live Сетевой вход в систему | Обеспечив Поддержи Позволяет Данная слу Обеспечив | Выполняется Выполняется | Вручную (ак Автоматичес Вручную (ак Вручную Вручную | ~ | | |

Рис. 2 Служба Проводная автонастройка

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

| Общие | Вход в с | жистему Восстановление Зависимости | | | | |
|---|-------------------------|--|-----------------------------------|----------------------------|--|--|
| Имя сл | Имя службы: | | dot3svc | | | |
| Отображаемое имя: | | Проводная автонастройка | | | | |
| Описание: | | Служба Wired AutoConfig (DOT3SVC) отвечает за проверку подлинности IEEE 802.1X интерфейсов Ethemet. Если текущее развертывание проводных сетей использует | | | | |
| Исполн | няемый ф | айл: | | | | |
| C:\WIN | DOWS\sys | stem32\s | vchost.exe -k LocalS | SystemNetworkRestricted -p | | |
| Тип запуска: Автоматически 🗸 | | | | | | |
| Состояние: Остановлена Запустить Остановить Приостановить Продолжить | | | | | | |
| Вы мо службы | жете указ ы из этого | ать пара диалого | аметры запуска, пр ового окна. | рименяемые при запуске | | |
| Параметры запуска: | | | | | | |
| | | | | | | |
| | | | ОК | Отмена Применить | | |

Свойства: Проводная автонастройка (Локальный компьютер) 🛛 🛛 🗙

Рис. 3 Запуск службы Проводная автонастройка

- 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**.

| Loc | al Area Connection: свойс | тва | × |
|-----------|---|--|------------------|
| Сеть | Проверка подлинности | Доступ | |
| yc no, | тановите этот флажок, что длинности сетевого доступ Включить проверку подлин | бы обеспечить про на для адаптера Eth нности IEEE 802.1> | рверку hemet. |
| Вь | оберите метод проверки по | длинности в сети: | |
| М | icrosoft: защищенные EAP (| (PEAP) ~ | Параметры |
| | Запоминать мои учетные , подключения при каждом Вернуться к неавторизова доступу | данные для этого входе в систему анному сетевому | |
| | Дополнительные парамет | ры | |
| | | | |
| | | | |
| | | | |
| | | ОК | Отмена |

Рис. 4 Окно Проверка подлинности

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

| Свойства защищенного ЕАР | \times |
|---|----------|
| При подключении: | |
| Подтверждать удостоверение сервера с помощью проверки сертификата | |
| Подключаться к следующим серверам (примеры: srv1;srv2;.*\.srv3\.com): | |
| Доверенные корневые центры сертификации: | |
| AAA Certificate Services | |
| Actalis Authentication Root CA | 11 |
| Baltimore CyberTrust Root | |
| | |
| | |
| Class 3 Public Primary Certification Authority | |
| < > > | |
| | - |
| уведопления перед подключением. | . 1 |
| Сообщить пользователю о возможности проверки удостове: 💛 | 1.1 |
| Выберите метод проверки подлинности: | |
| защищенный пароль (EAP-MSCHAP v2) У Настроить. | |
| Включить быстрое переподключение | |
| | |
| Отключаться, если сервер не поддерживает привязку с шифрованием через механизм TLV | |
| Включить удостоверение конфиденциальности | |
| ОК Отмена | |

Рис. 5 Настройка свойств защищённого ЕАР

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

| Свойства защищенного ЕАР | > |
|---|------------|
| Свойства ЕАР МSCHAPv2 Х | |
| | о проверки |
| При подключении: | |
| Использовать автоматически имя входа и пароль из Windows (и имя домена, если существует). | |
| ОК Отмена | ^ |
| Certum CA | |
| Certum Trusted Network CA | |
| Class 3 Public Primary Certification Authority | |
| COMODO RSA Certification Authority | 1.628 |
| DigiCert Assured ID Root CA | × 1 |
| • | / |
| Уведомления перед подключением: | |
| Сообщить пользователю о возможности проверки у | достовер 🗸 |
| | |
| Выберите метод проверки подлинности: | |
| защищенный пароль (EAP-MSCHAP v2) 🛛 🗸 | Настроить |
| Включить быстрое переподключение | |
| | |
| Отключаться, если сервер не поддерживает привя шифрованием через механизм TLV | вку с |
| Включить удостоверение конфиденциальности | |
| ОК | Отмена |

Рис. 6 Настройка свойств защищённого ЕАР

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.

| Дополнительные параметры | × | Безопасность Windows | × |
|--|--|--------------------------|-------------------------------------|
| Параметры 802.1Х | | Сохранить учетные | е данные |
| 🗹 Указать режим проверки по, | длинности | Сохранение учетных данн | ых позволяет персональному |
| Проверка подлинності \vee | Сохранить учетные данные | компьютеру подключитьс | я к сети, когда ваша личная учетная |
| Удалить учетные данны | е для всех пользователей | запись не подключена (на | пример, для загрузки обновлении). |
| Включить единую регистра | цию для сети | ivan | × |
| Выполнять непосредстве пользователя | енно перед входом | ••••• | |
| Выполнять сразу после в | хода пользователя | L | |
| Максимальная задержка (се | кунды): 10 📫 | | |
| Разрешить отображение диалоговых окон при еди | дополнительных ином входе | ОК | Отмена |
| В этой сети используютс виртуальные локальные подлинности компьютера | я отдельные сети для проверки а и пользователя | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | ОК Отмена | | |

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 802.1Х:

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 МАС-адресов равным 1:

config port security 2 admin state enable max learning addr 1

Задача № З

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 802.1Х 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 802.1Х:

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