Описание технологии : 802.1X, Guest VLAN

D-Link, Октябрь 2014

Александр Зайцев, консультант по проектам
e-mail: azaitsev@dlink.ru

D-Link®
Building Networks for People

Функции обеспечения безопасности и ограничения доступа к сети

Аутентификация пользователей 802.1X

Аутентификация – процедура проверки подлинности субъекта, на основе предоставленных им данных.

- Стандарт IEEE 802.1X (IEEE Std 802.1X-2010) описывает использование протокола EAP (Extensible Authentication Protocol) для поддержки аутентификации с помощью сервера аутентификации и определяет процесс инкапсуляции данных EAP, передаваемых между клиентами и серверами аутентификации.
- Стандарт IEEE 802.1X осуществляет контроль доступа и не позволяет неавторизованным устройствам подключаться к локальной сети через порты коммутатора.

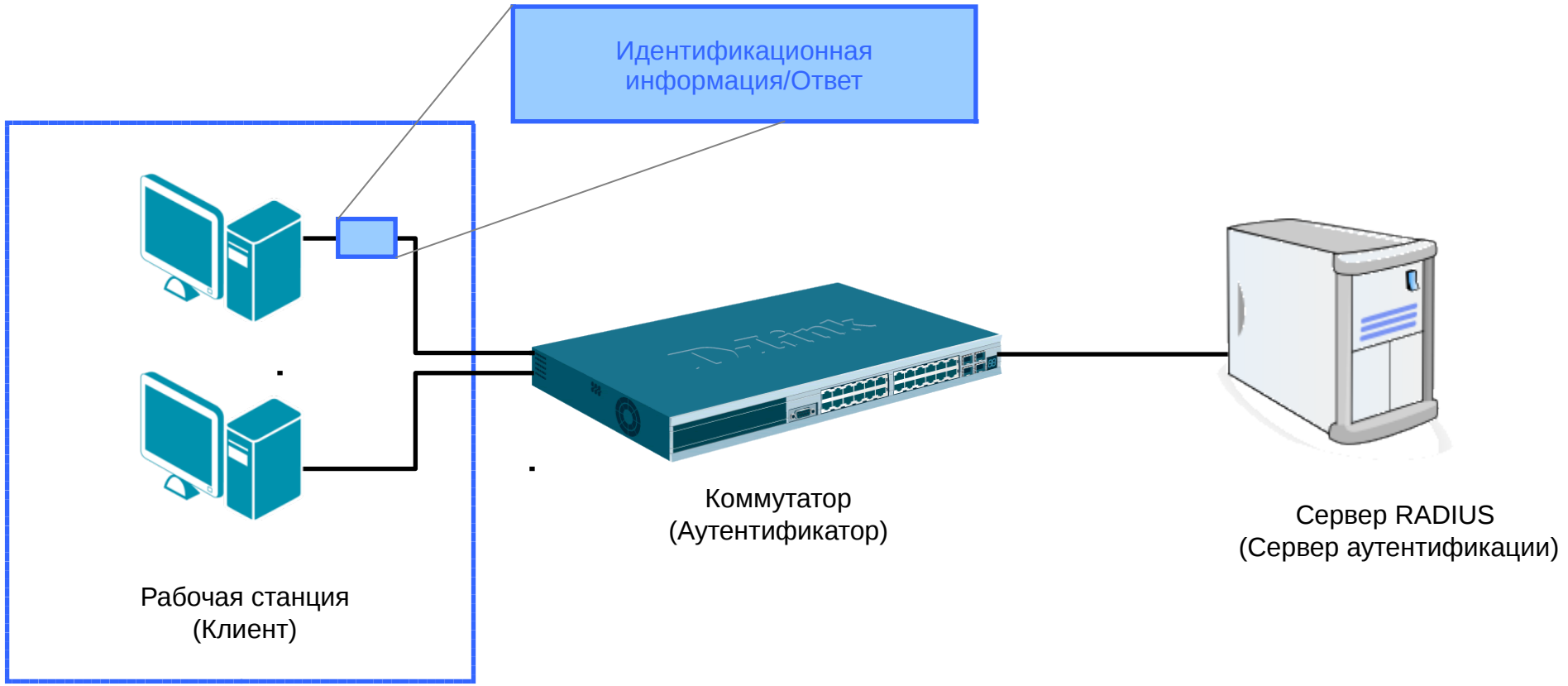
В стандарте IEEE 802.1X определены следующие три роли, которые могут выполнять устройства:

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

Функции обеспечения безопасности и ограничения доступа к сети

Роли устройств в стандарте 802.1X: клиент

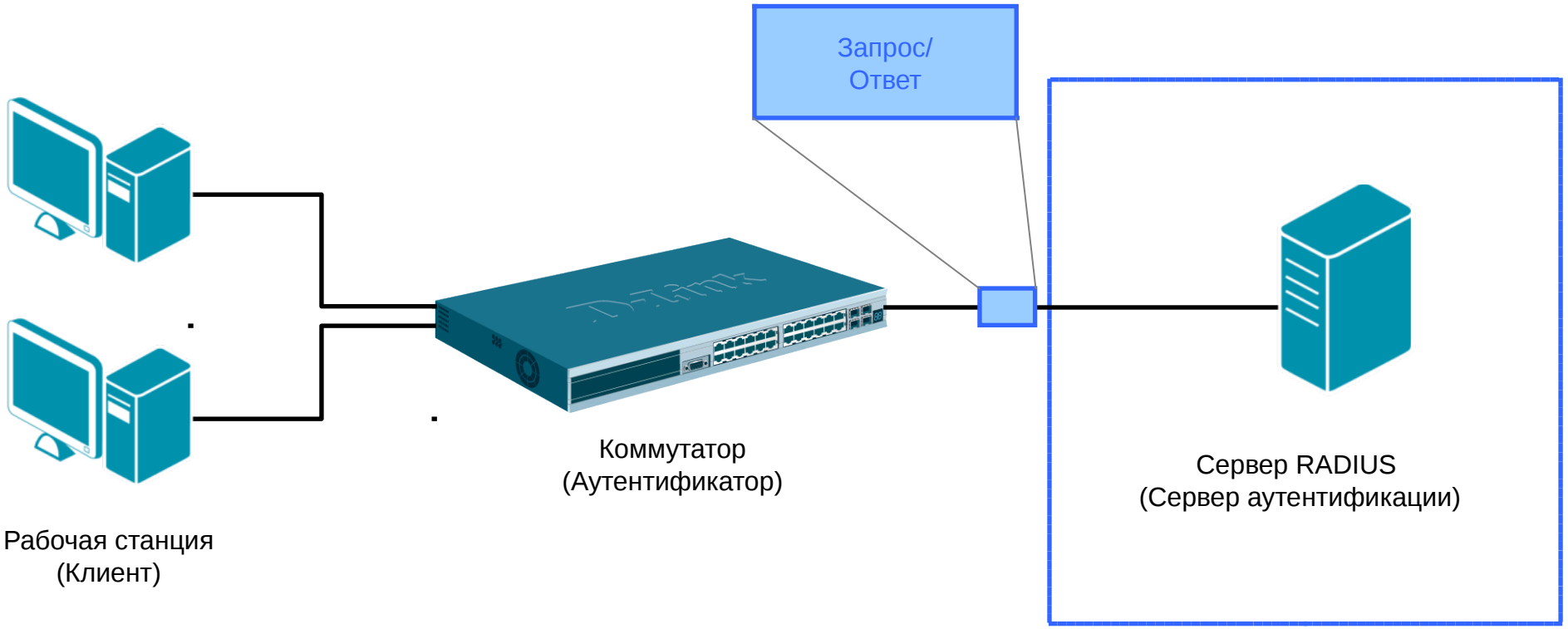
Клиент (Client/Supplicant) – это рабочая станция, которая запрашивает доступ к локальной сети и сервисам коммутатора и отвечает на запросы от коммутатора. На рабочей станции должно быть установлено клиентское ПО для 802.1X, например, то, которое встроено в ОС Microsoft Windows XP.



Функции обеспечения безопасности и ограничения доступа к сети

Роли устройств в стандарте 802.1X: сервер аутентификации

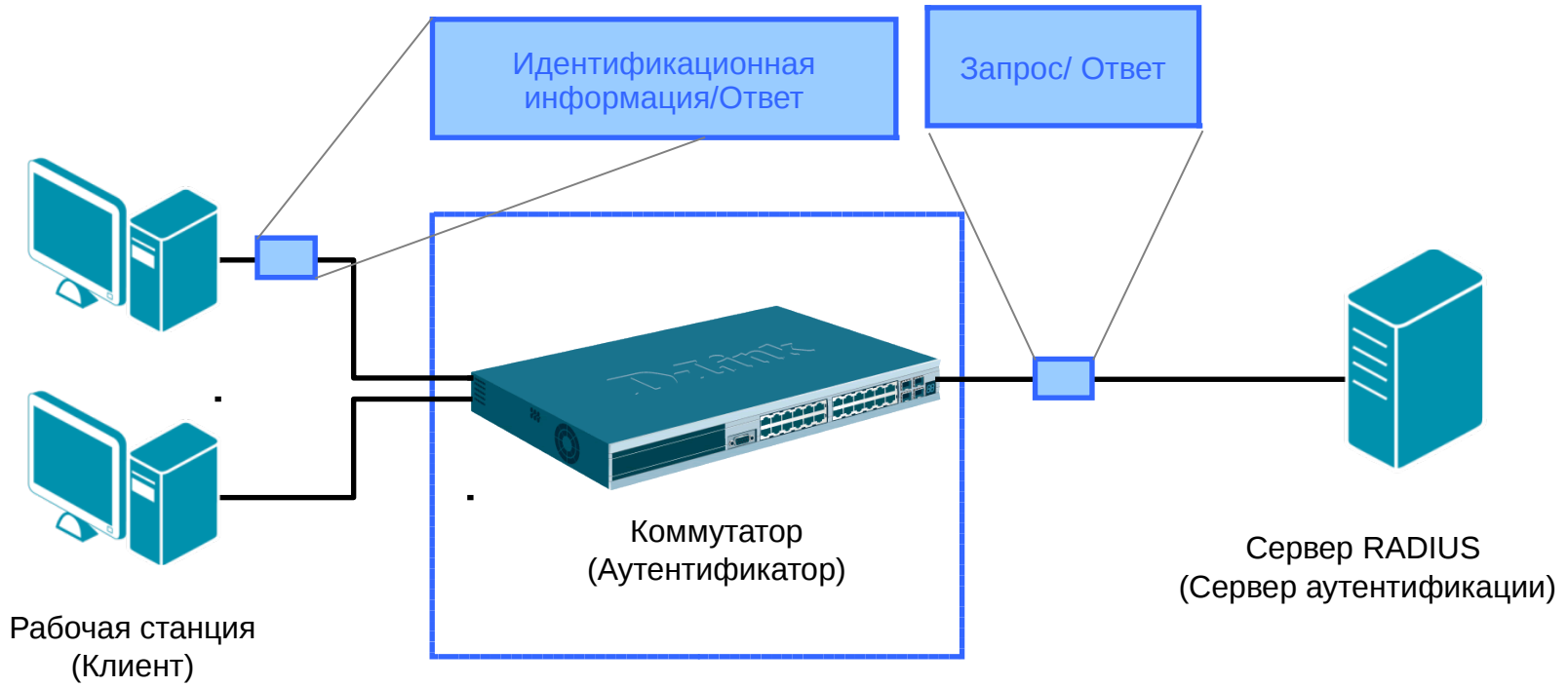
Сервер аутентификации (Authentication Server) выполняет фактическую аутентификацию клиента. Он проверяет подлинность клиента и информирует коммутатор предоставлять или нет клиенту доступ к локальной сети. RADIUS (Remote Authentication Dial-In User Service) работает в модели клиент/сервер, в которой информация об аутентификации передается между сервером RADIUS и клиентами RADIUS.



Функции обеспечения безопасности и ограничения доступа к сети

Роли устройств в стандарте 802.1X: аутентификатор (Authenticator)

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 поддерживает клиент RADIUS, который отвечает за инкапсуляцию и деинкапсуляцию кадров EAP, и взаимодействие с сервером аутентификации.



Функции обеспечения безопасности и ограничения доступа к сети

Реализации аутентификации 802.1X

В коммутаторах D-Link поддерживаются две реализации аутентификации 802.1X:

- Port-Based 802.1X (802.1X на основе портов):

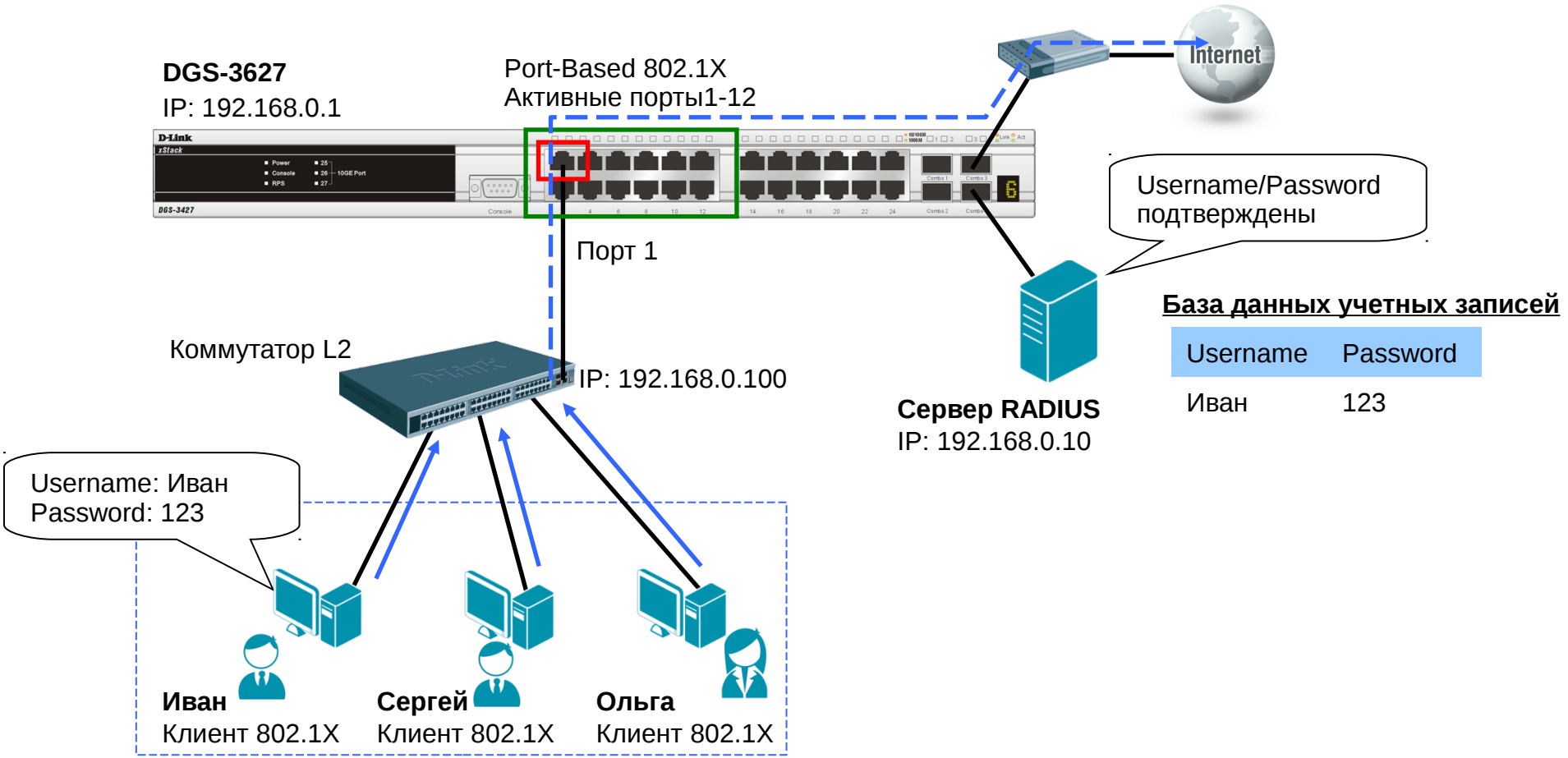
после того как порт был авторизован, любой пользователь, подключенный к нему, может получить доступ к сети.

- MAC-Based 802.1X (802.1X на основе MAC-адресов):

аутентификация множества клиентов на одном физическом порте коммутатора. Проверяются не только имя пользователя/пароль, подключенных к порту коммутатора клиентов, но и их количество.

Функции обеспечения безопасности и ограничения доступа к сети

Настройка функции Port-Based 802.1X



Функции обеспечения безопасности и ограничения доступа к сети

Настройка коммутатора DGS-3627

- Настроить проверку подлинности пользователей на сервере RADIUS.

```
config 802.1x auth_protocol radius_eap
```

- Настроить тип аутентификации 802.1X: port-based.

```
config 802.1x auth_mode port_based
```

- Настроить порты, к которым подключаются клиенты в качестве аутентификатора (на Uplink-портах к вышестоящим коммутаторам не следует настраивать режим «authenticator»).

```
config 802.1x capability ports 1-12 authenticator
```

- Активизировать функцию 802.1X.

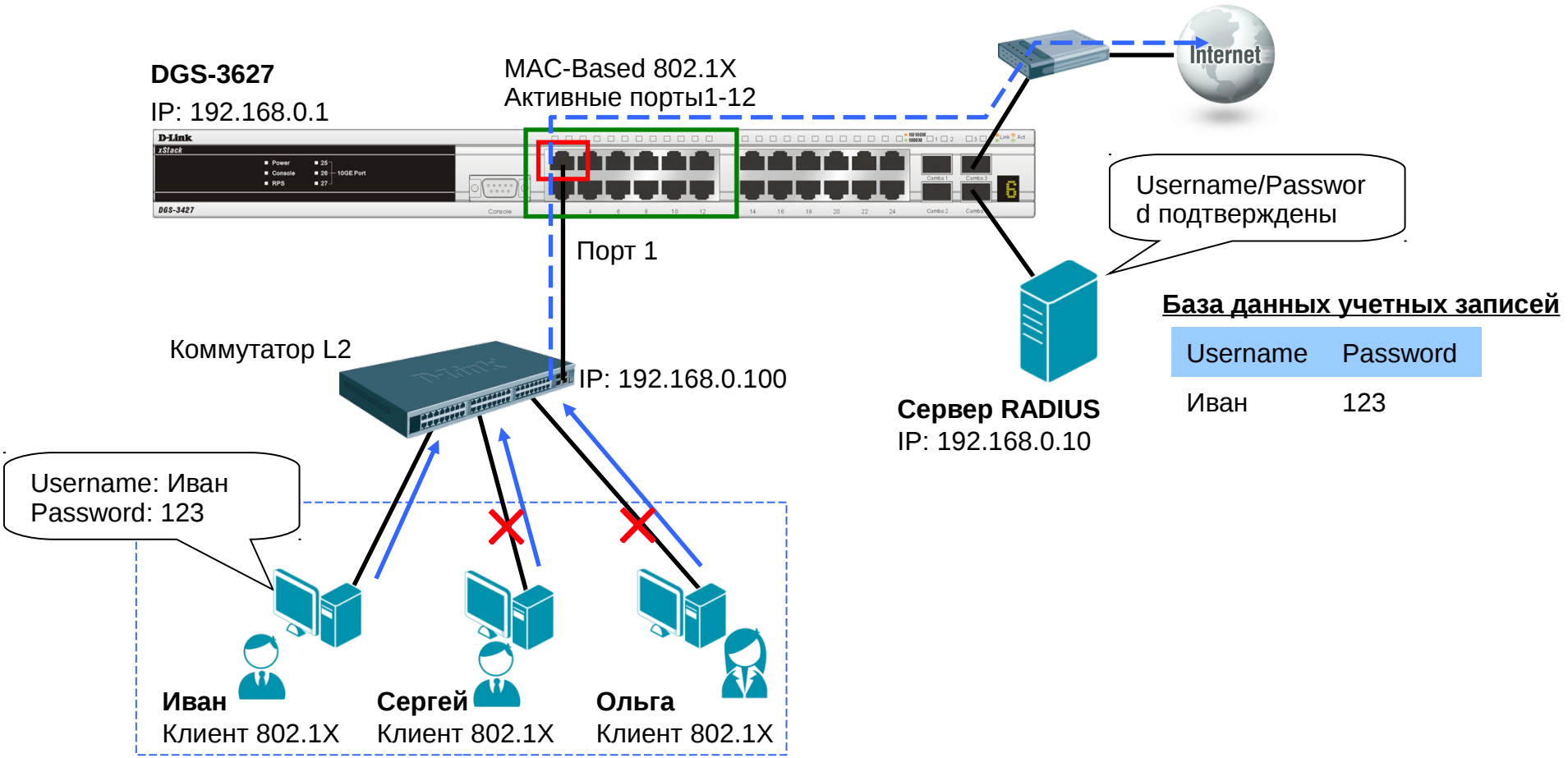
```
enable 802.1x
```

- Настроить параметры сервера RADIUS.

```
config radius add 1 192.168.0.10 key 123456 default
```

Функции обеспечения безопасности и ограничения доступа к сети

Настройка функции MAC-Based 802.1X



Функции обеспечения безопасности и ограничения доступа к сети

Настройка коммутатора DGS-3627

- Настроить проверку подлинности пользователей на сервере RADIUS.

```
config 802.1x auth_protocol radius_eap
```

- Настроить тип аутентификации 802.1X: MAC-based.

```
config 802.1x auth_mode mac_based
```

- Настроить порты, к которым подключаются клиенты в качестве аутентификатора.

```
config 802.1x capability ports 1-12 authenticator
```

- Активизировать функцию 802.1X.

```
enable 802.1x
```

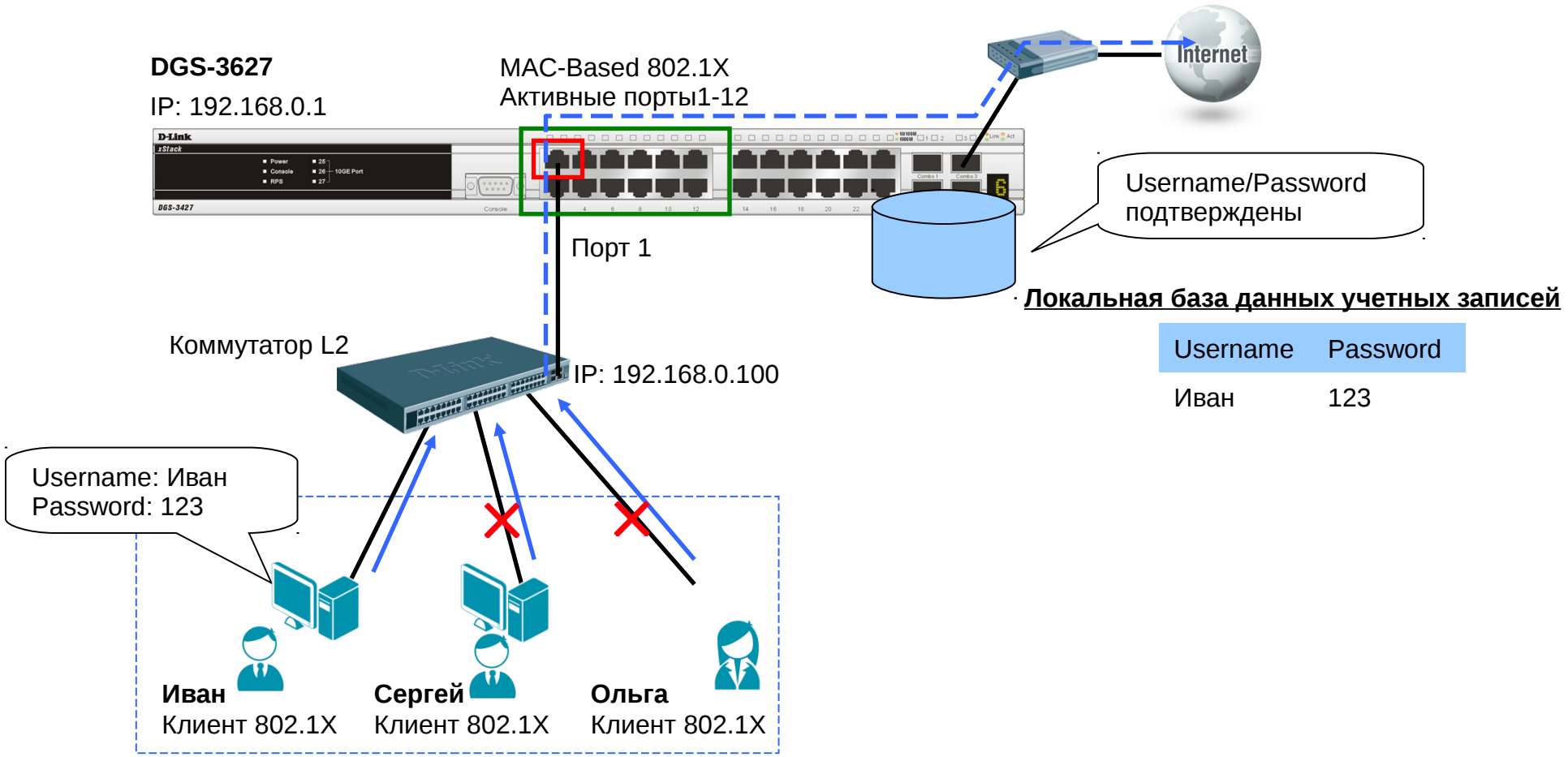
- Настроить параметры сервера RADIUS.

```
config radius add 1 192.168.0.10 key 123456 default
```

Функции обеспечения безопасности и ограничения доступа к сети

Аутентификация 802.1X на основе MAC-адресов с использованием локальной базы данных учетных записей пользователей

Коммутатор может выполнять роль сервера аутентификации. В этом случае база данных учетных записей пользователей будет храниться локально на самом коммутаторе.



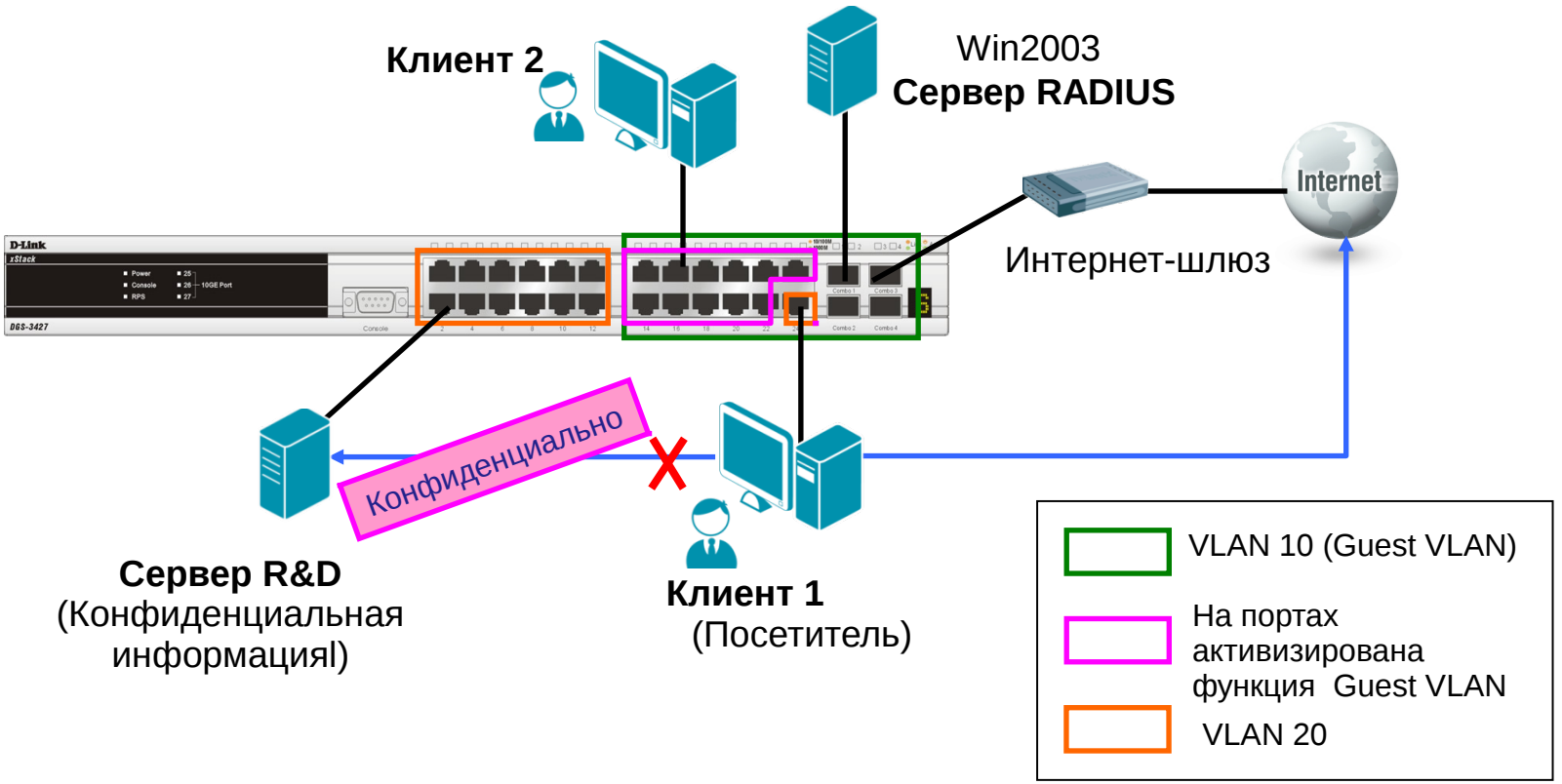
Функции обеспечения безопасности и ограничения доступа к сети

802.1X Guest VLAN

- 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.
  - 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).
  - Если клиент не прошел аутентификацию, он помещается в Guest VLAN с ограниченными правами и доступом.

Функции обеспечения безопасности и ограничения доступа к сети

802.1X Guest VLAN – аутентификация не пройдена

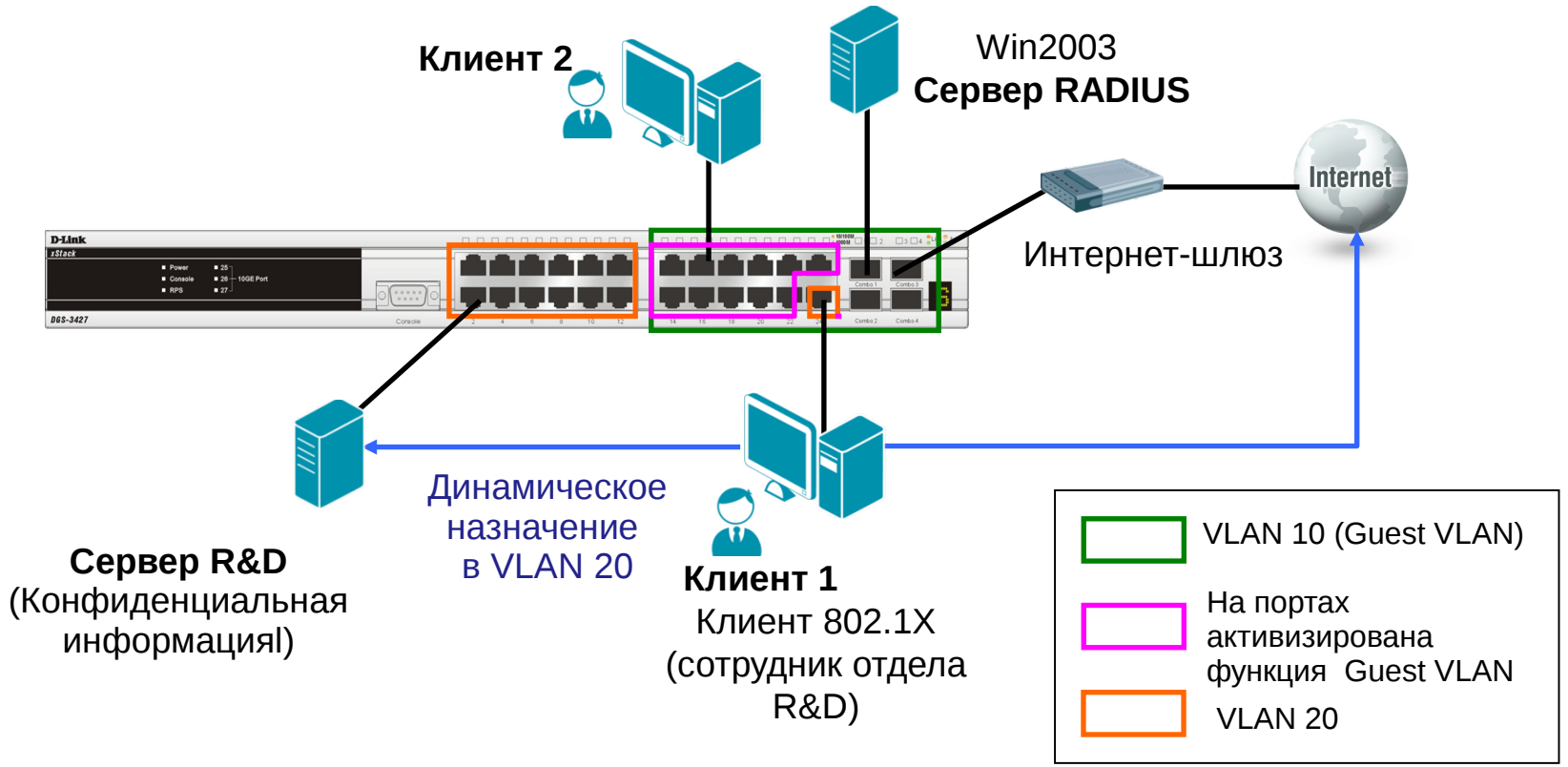


Аутентификация не пройдена

- Если посетитель (клиент1) не сможет пройти аутентификацию 802.1X, он останется в Guest VLAN (VLAN 10) с ограниченными правами и доступом.
- В этом примере посетитель получает доступ в Интернет, но сервер R&D для него не доступен.

Функции обеспечения безопасности и ограничения доступа к сети

802.1X Guest VLAN – аутентификация не пройдена

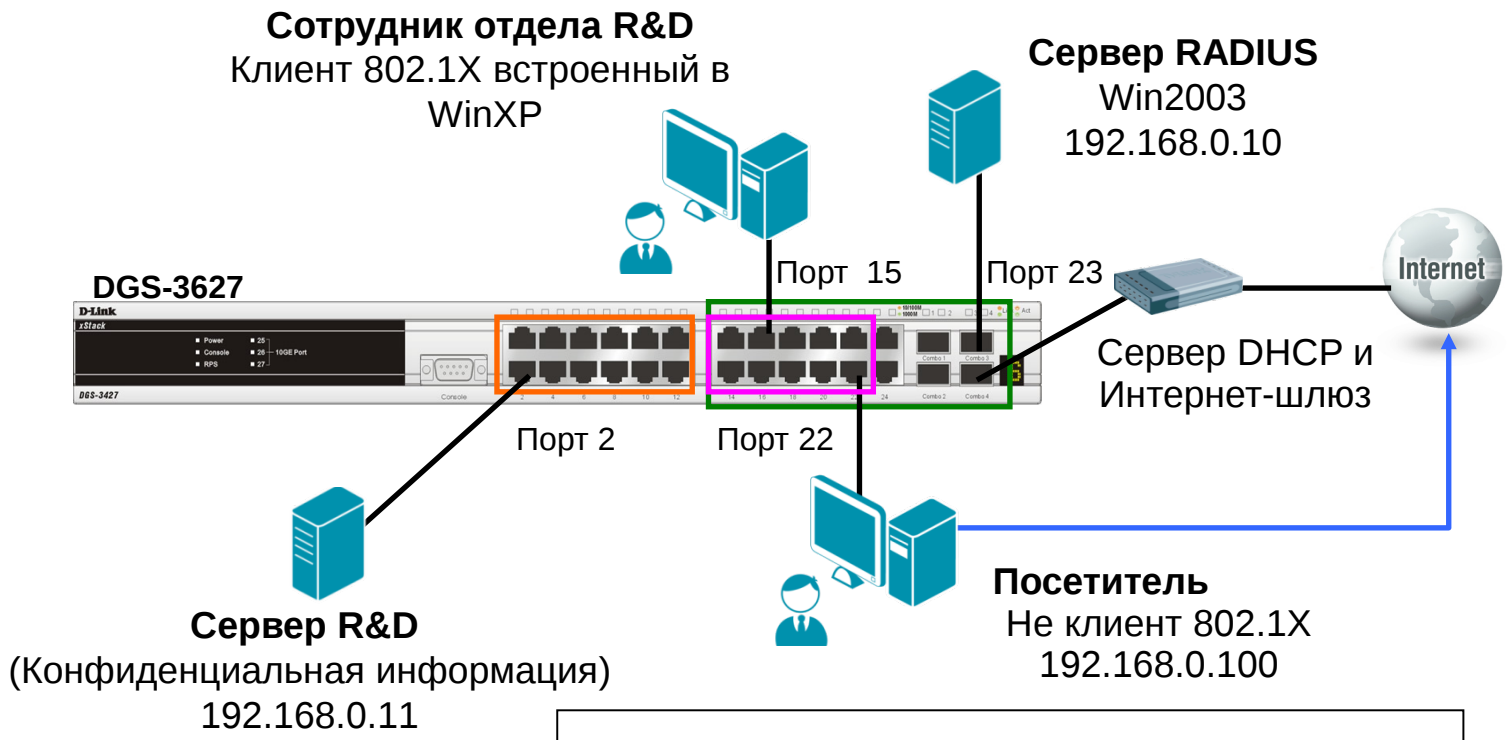


Аутентификация пройдена

- Если аутентификация успешно пройдена, клиент 1 динамически помещается в VLAN 20. Клиент 1 получит доступ к конфиденциальной информации на сервере R&D.

Функции обеспечения безопасности и ограничения доступа к сети

Пример настройки 802.1X Guest VLAN



1. Две VLAN : v10 и v20
   - Статические члены v10 - порты 13-24
   - Статические члены v20 - порты 1-12
   - На портах 13-22 активизирована функция Guest VLAN
2. Guest VLAN VID=10

Если сервер RADIUS расположен за пределами сети, IP-интерфейсу VLAN v10 должен быть назначен IP-адрес для осуществления маршрутизации

Функции обеспечения безопасности и ограничения доступа к сети

Настройка коммутатора DGS-3627

- Создать 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
```

- Активизировать функции 802.1X и Guest VLAN.

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

- Настроить коммутатор в качестве аутентификатора и задать параметры сервера RADIUS.

```
config 802.1x capability ports 13-24 authenticator
config radius add 1 192.168.0.10 key 123456 default
```