

## Настройка защищенного VPN-туннеля (ГОСТ) на уровне L2 (VLAN)

Для создания защищенного канала связи в режиме шифрования/дешифрования в Dionis-NX должны быть предварительно созданы ключи доступа и загружены ключи абонентов Disec. Это описано в разделе «Инициализация криптографических компонентов в Dionis DPS»

### Пример организации L2 туннелей с шифрованием трафика между двумя криптомаршрутизаторами Dionis DPS

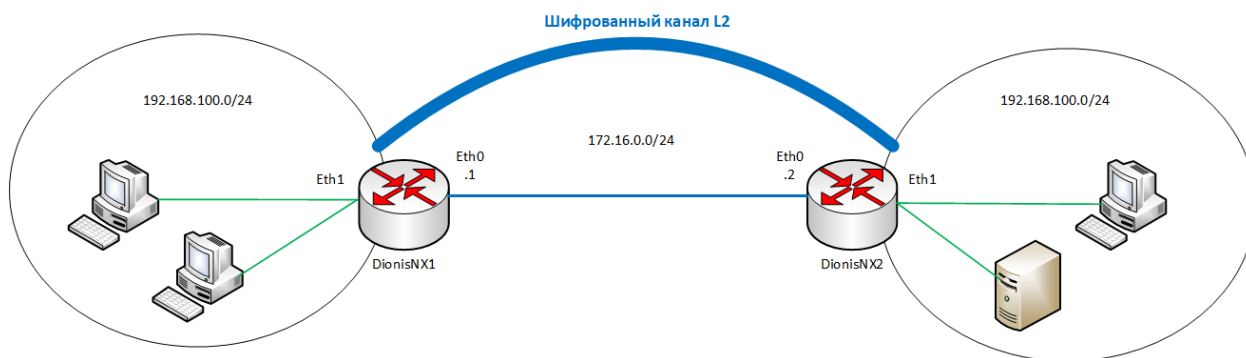


Рис.1

### Настройка Dionis NX1

Будем считать, что на устройствах была произведена инициализация криптографических компонентов.

Предварительная настройка интерфейсов на устройстве Dionis NX1:

WAN интерфейсы

```
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.1/24
(config-if-ethernet0)# enable
```

VLAN интерфейс

```
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# enable
```

```
(config-if-ethernet1)# interface ethernet 1.10
(config-if-ethernet1)# enable
```

Создание интерфейса ditap:

```
(config)# interface ditap 0
```

*В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0). Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:*

```
(config-if-ditap0)# id 1
```

*id: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.*

```
(config-if-ditap0)# alg encrypt
```

*alg: алгоритм трансформации данных в туннеле; возможные значения:*

- *compression: только сжатие данных;*
- *encryption: только шифрование данных;*
- *both: и сжатие, и шифрование данных;*
- *none: никакой трансформации данных не производится.*

**(config-if-ditap0)# serial 222**

*serial: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.*

**(config-if-ditap0)# local-cn 1**

*local-cn: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.*

**(config-if-ditap0)# remote-cn 1**

*remote-cn: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.*

**(config-if-ditap0)# local 172.16.0.1**

*local: задает IP-адрес локального конца туннеля.*

**(config-if-ditap0)# remote 172.16.0.2**

*remote: задает IP-адрес удаленного конца туннеля.*

**(config-if-ditap0)# enable**

*Делает интерфейс активным.*

Для реализации отбора трафика в интерфейс ditap необходимо объединить физический интерфейс ethernet и интерфейс ditap при помощи интерфейса bridge:

**(config-if-ditap0)# interface bridge 0**

**(config-if-bridge0)# port ethernet 1.10**

**(config-if-bridge0)# port ditap 0**

**(config-if-bridge0)# enable**

Далее необходимо произвести симметричные настройки на другом криптомаршрутизаторе.

## **Настройка DionisNX2**

Предварительная настройка интерфейсов на устройстве DionisNX2

**(config)# interface ethernet 0**

**(config-if-ethernet0)# ip address 172.16.0.2/24**

**(config-if-ethernet0)# enable**

**(config-if-ethernet0)# interface ethernet 1**

**(config-if-ethernet1)# enable**

**(config-if-ethernet0)# interface ethernet 1.10**

**(config-if-ethernet1)# enable**

Создание и настройка туннельного L2 интерфейса ditap:

**(config)# interface ditap 0**

**(config-if-ditap0)# id 1**

**(config-if-ditap0)# alg encrypt**

**(config-if-ditap0)# serial 222**

**(config-if-ditap0)# local-cn 1**

**(config-if-ditap0)# remote-cn 1**

**(config-if-ditap0)# local 172.16.0.2**

**(config-if-ditap0)# remote 172.16.0.1**

**(config-if-ditap0)# enable**

Объединение физического и туннельного интерфейса:

**(config-if-ditap0)# interface bridge 0**

**(config-if-bridge0)# port ethernet 1.10**

**(config-if-bridge0)# port ditap 0**

**(config-if-bridge0)# enable**