
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Меня хорошо видно && слышно?

Ставьте +, если все хорошо
Напишите в чат, если есть проблемы

VPN

Кулиничев Алексей

Администратор Сетей

Santchous42@yandex.ru

Правила вебинара

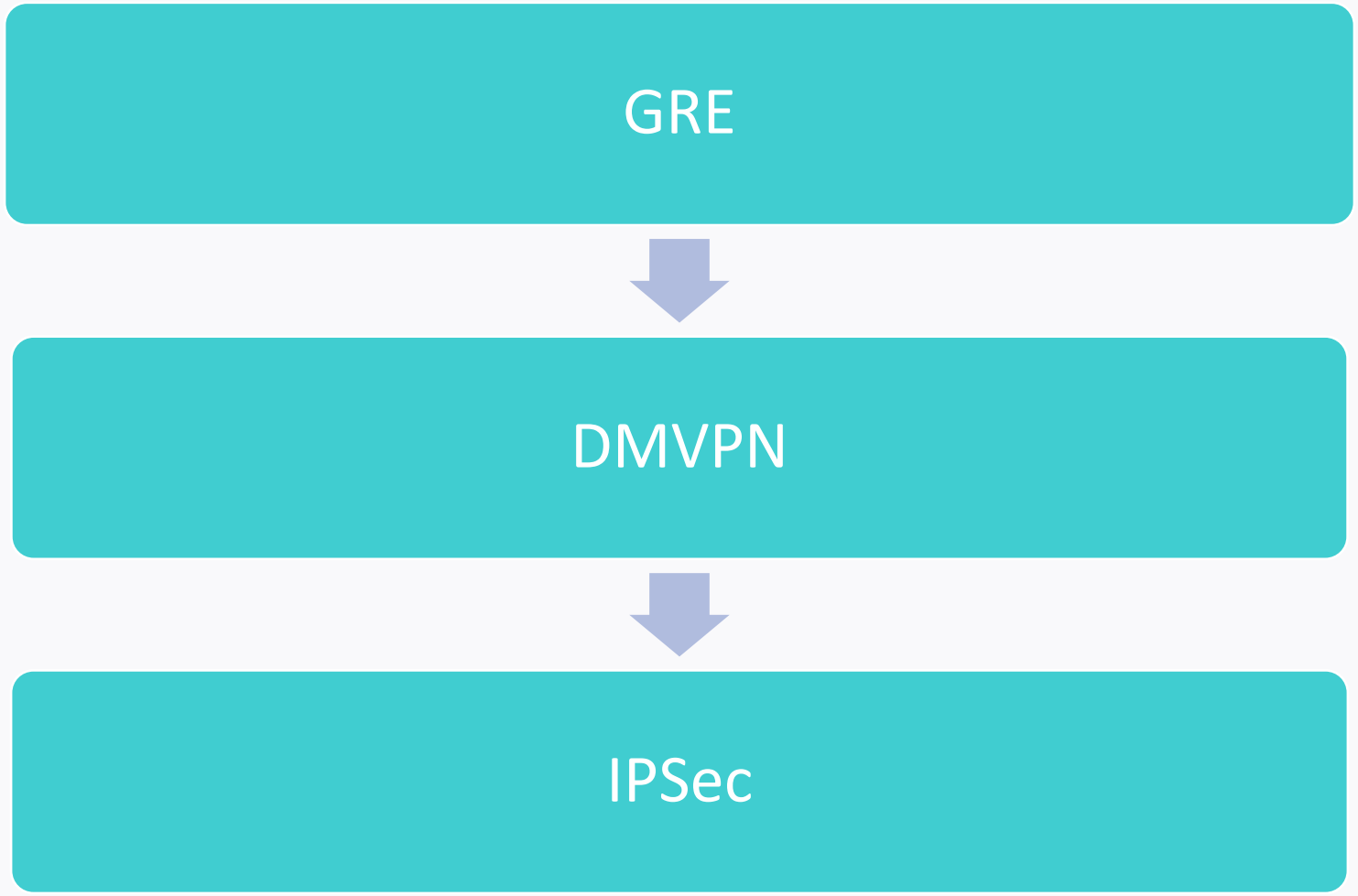
Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

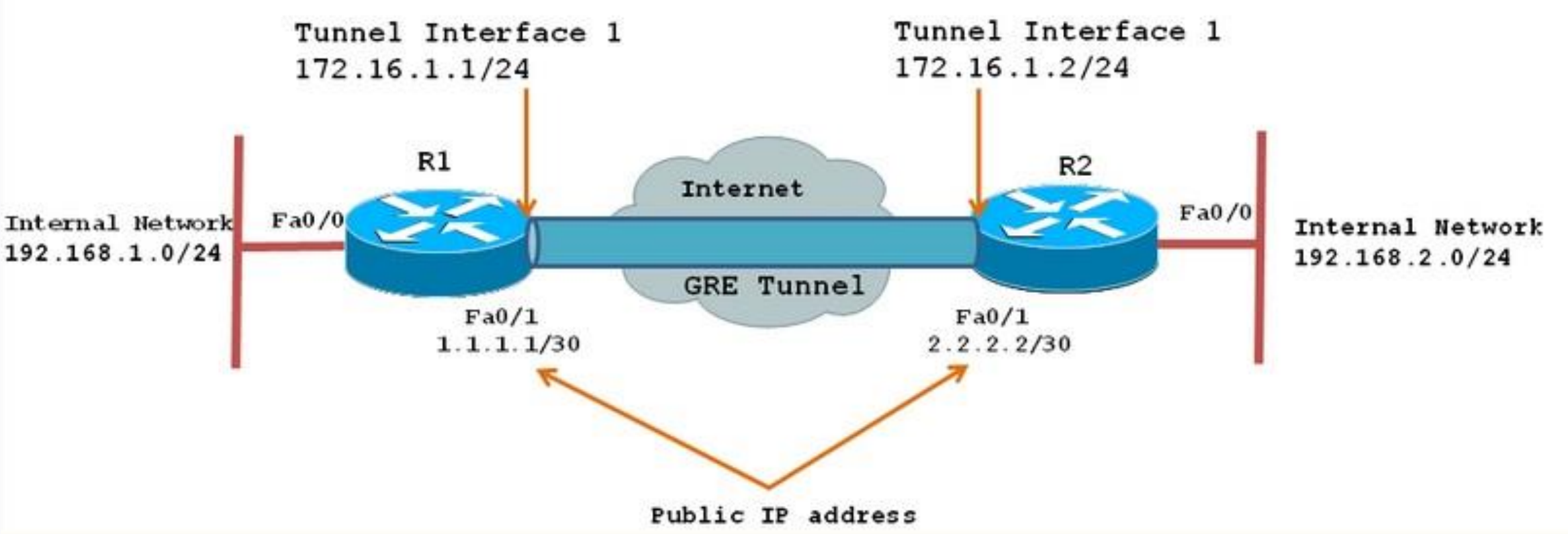
Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара




1
GRE

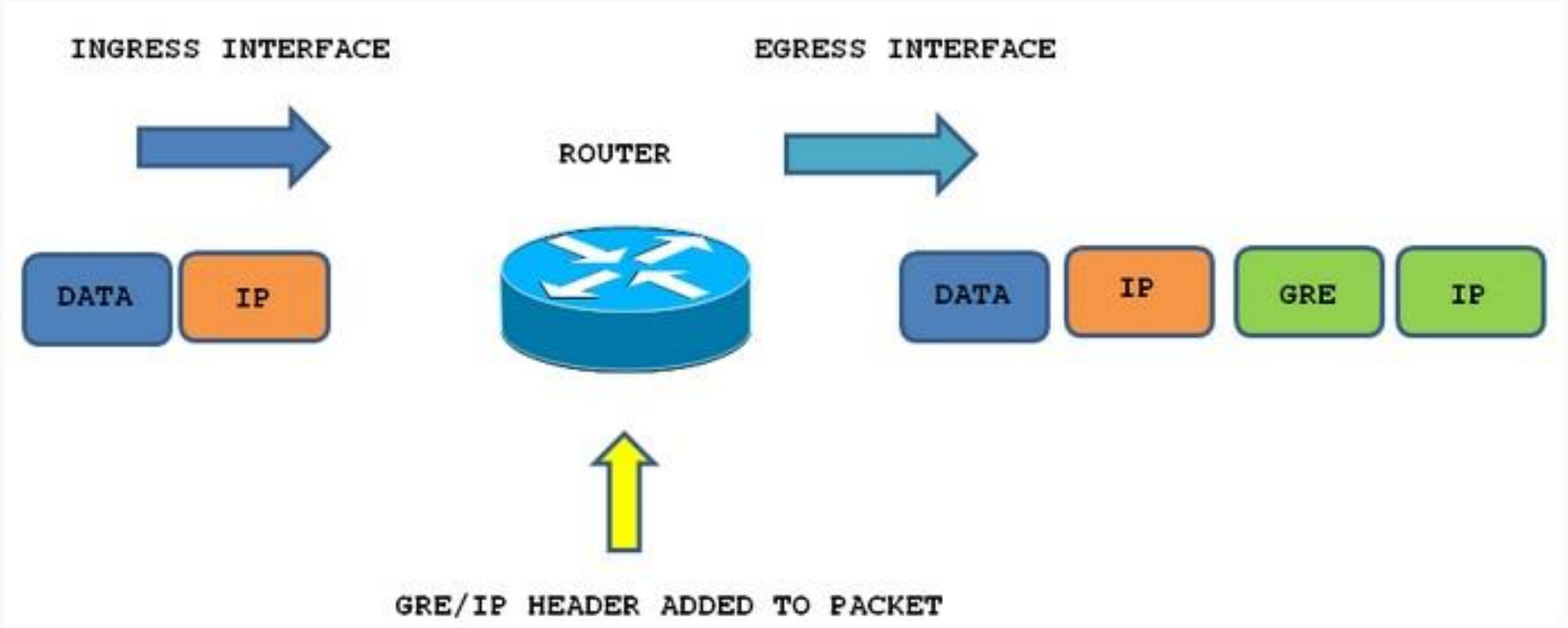
GRE


Tunnel Interface 1
172.16.1.1/24
Tunnel Interface 1
172.16.1.2/24
R1
R2
Internet
Internal Network
192.168.1.0/24
Fa0/0
Fa0/0
Internal Network
192.168.2.0/24
GRE Tunnel
Fa0/1
1.1.1.1/30
Fa0/1
2.2.2.2/30
Public IP address

GRE

R1(config)# interface Tunnel1	R2(config)# interface Tunnel1
R1(config-if)# ip address 172.16.1.1 255.255.255.0	R2(config-if)# ip address 172.16.1.2 255.255.255.0
R1(config-if)# ip mtu 1476(1440)	R2(config-if)# ip mtu 1476(1440)
R1(config-if)# ip tcp adjust-mss 1456(1400)	R2(config-if)# ip tcp adjust-mss 1456(1400)
R1(config-if)# tunnel source 1.1.1.1	R2(config-if)# tunnel source 2.2.2.2
R1(config-if)# tunnel destination 2.2.2.2	R2(config-if)# tunnel destination 1.1.1.1

GRE


INGRESS INTERFACE
EGRESS INTERFACE
ROUTER
DATA
IP
DATA
IP
GRE
IP
GRE/IP HEADER ADDED TO PACKET

2

DMVPN

DMVPN

DMVPN – проприетарная технология для построения динамических виртуальных сетей между маршрутизаторами Cisco

В каких областях может использоваться?

DMVPN

1. Для построения VPN между центральным офисом и большим количеством географически удаленных филиалов

2. Для построения VPN, между удаленному филиалами и центральным офисом

3. При подключении различных терминалов

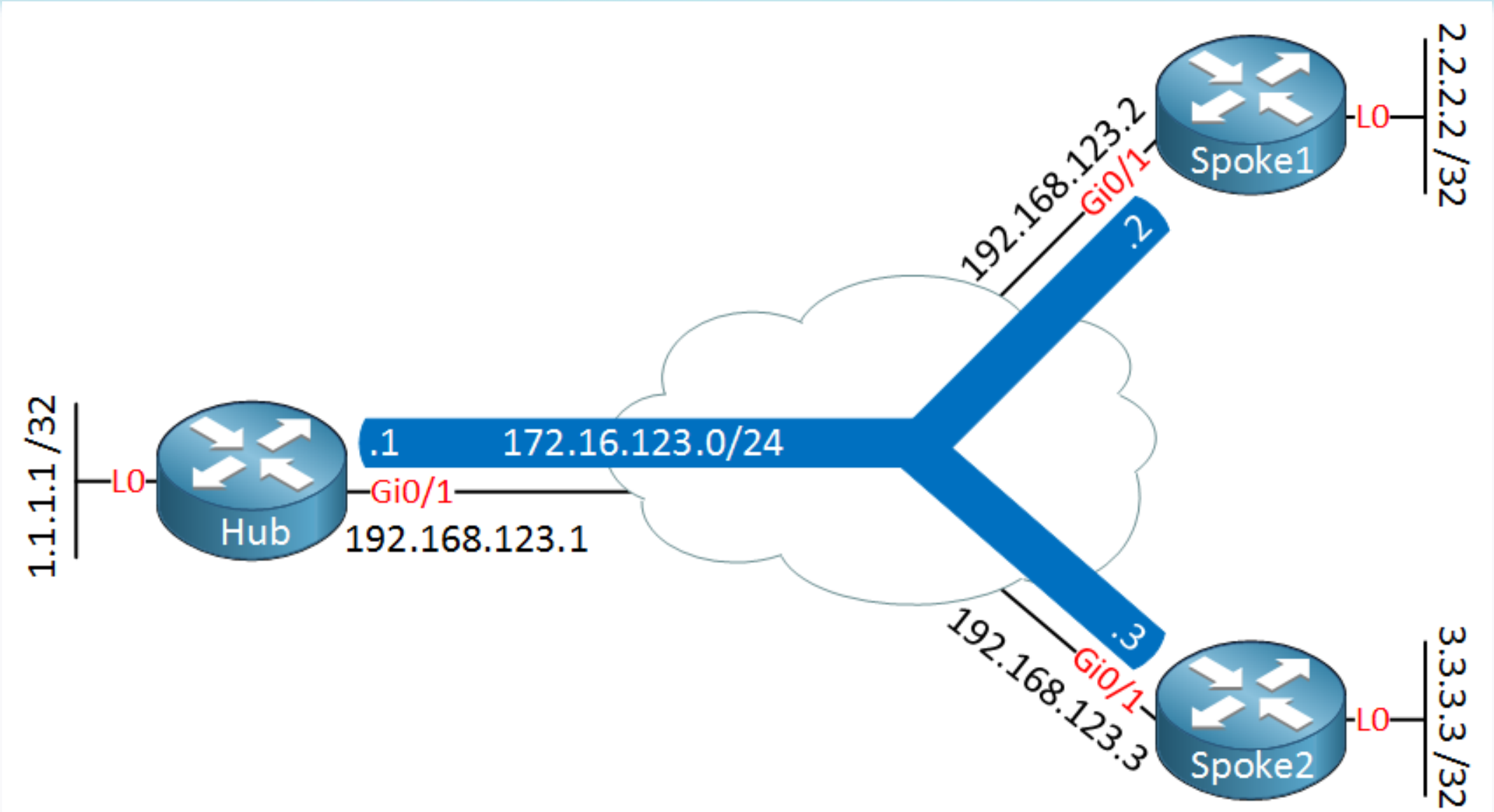
DMVPN

Позволяет решить две основные проблемы:

1. Динамическое построение Full-Mesh топологий
2. Уменьшает нагрузку на центральном маршрутизаторе, при построении большого количества VPN каналов при передаче трафика между филиалами

При этом остается возможность защищать трафик IPSec и есть возможность использовать протоколы маршрутизации

DMVPN


Spoke1
Lo
2.2.2.2 /32
192.168.123.2
Gi0/1
.2
1.1.1.1 /32
Lo
Hub
.1
172.16.123.0/24
Gi0/1
192.168.123.1
.3
192.168.123.3
Gi0/1
Spoke2
Lo
3.3.3.3 /32


2.1
NHRP

NHRP

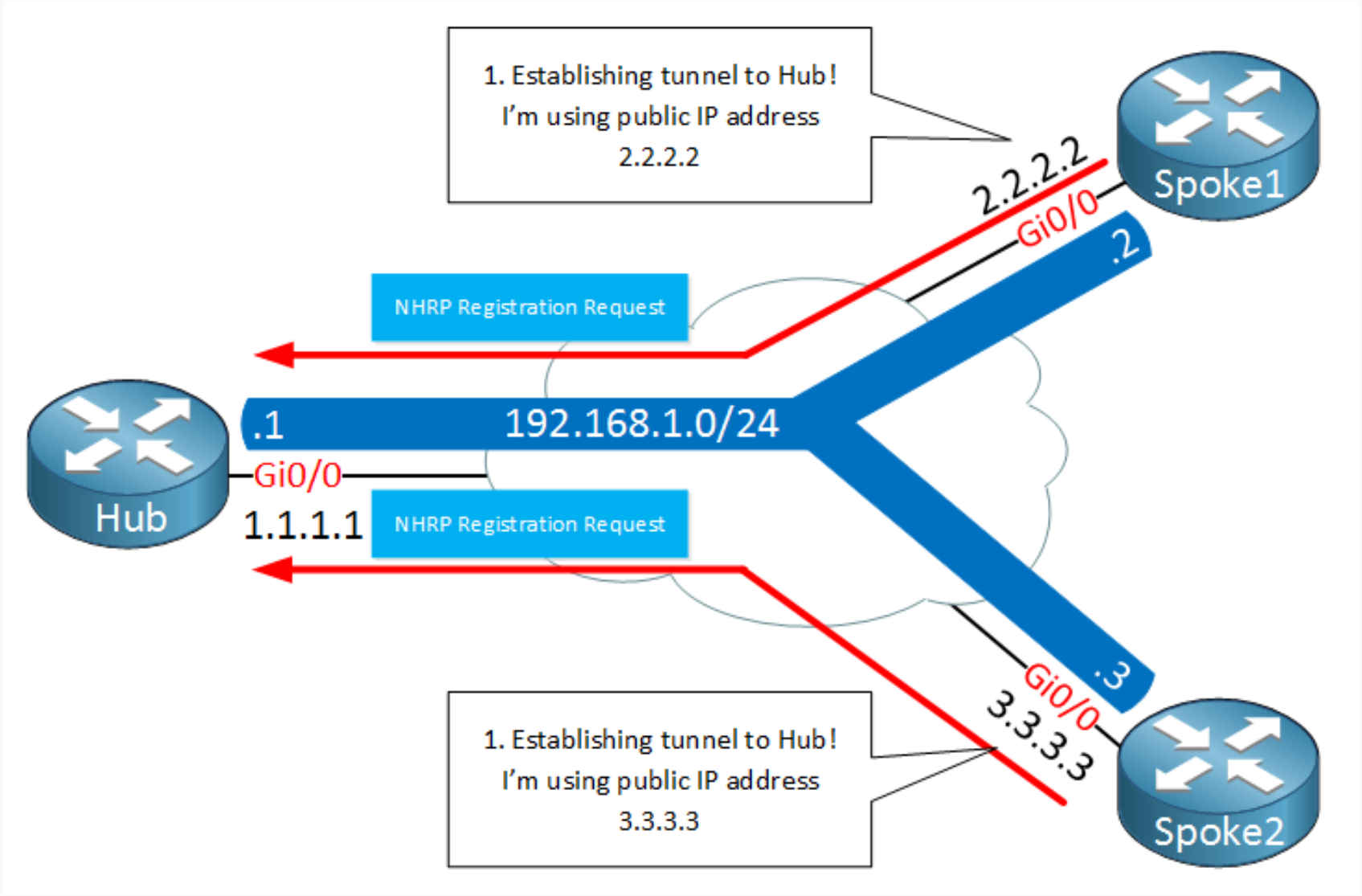
NHRP – Next-Hop Resolution Protocol.

Протокол формирует таблицу соответствия реальных адресов и виртуальных.

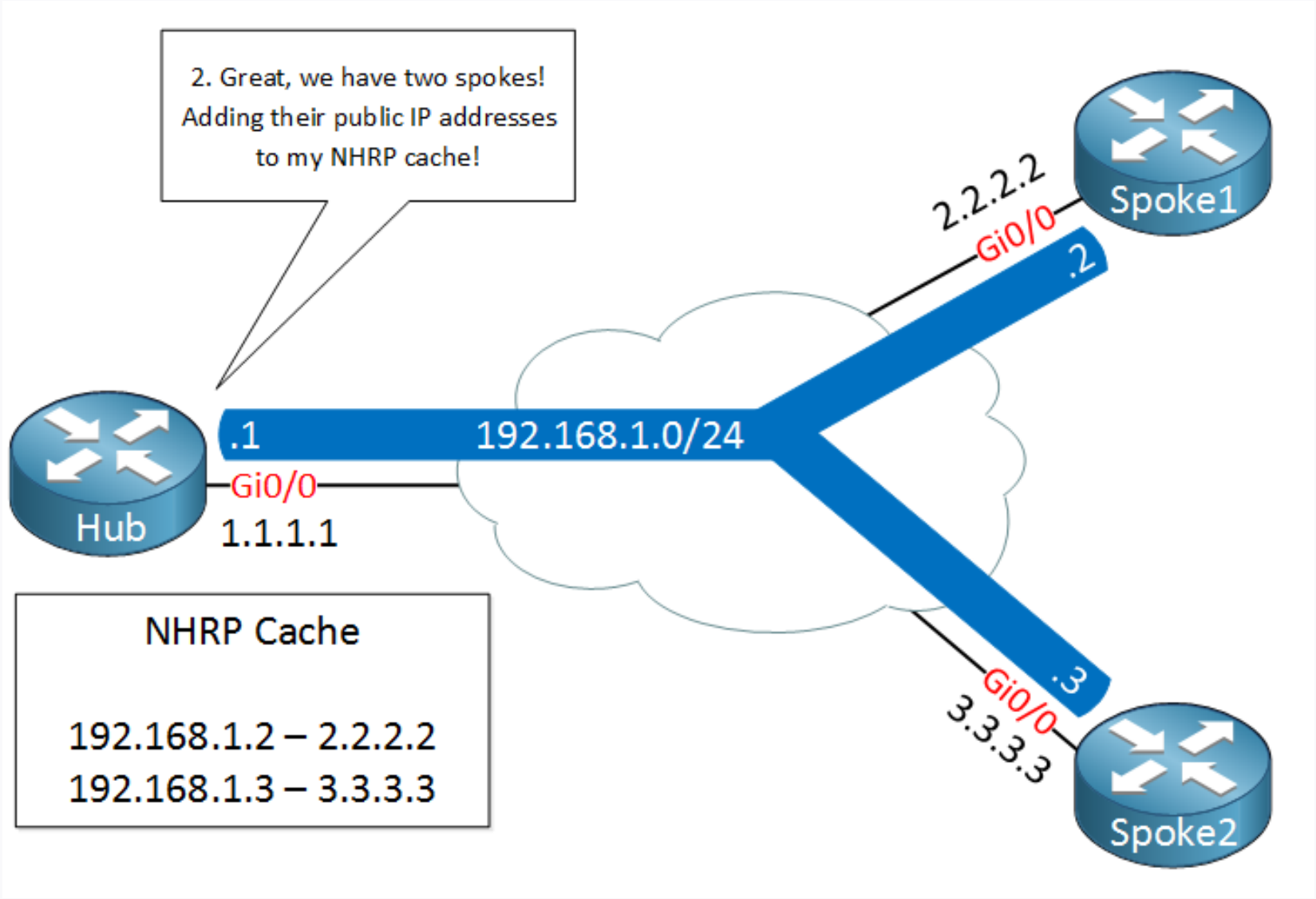
Таблица хранится на HUB маршрутизаторе

Как только Spoke регистрируется на HUB, его данные попадают в таблицу NHRP и могут анонсироваться другим Spoke.

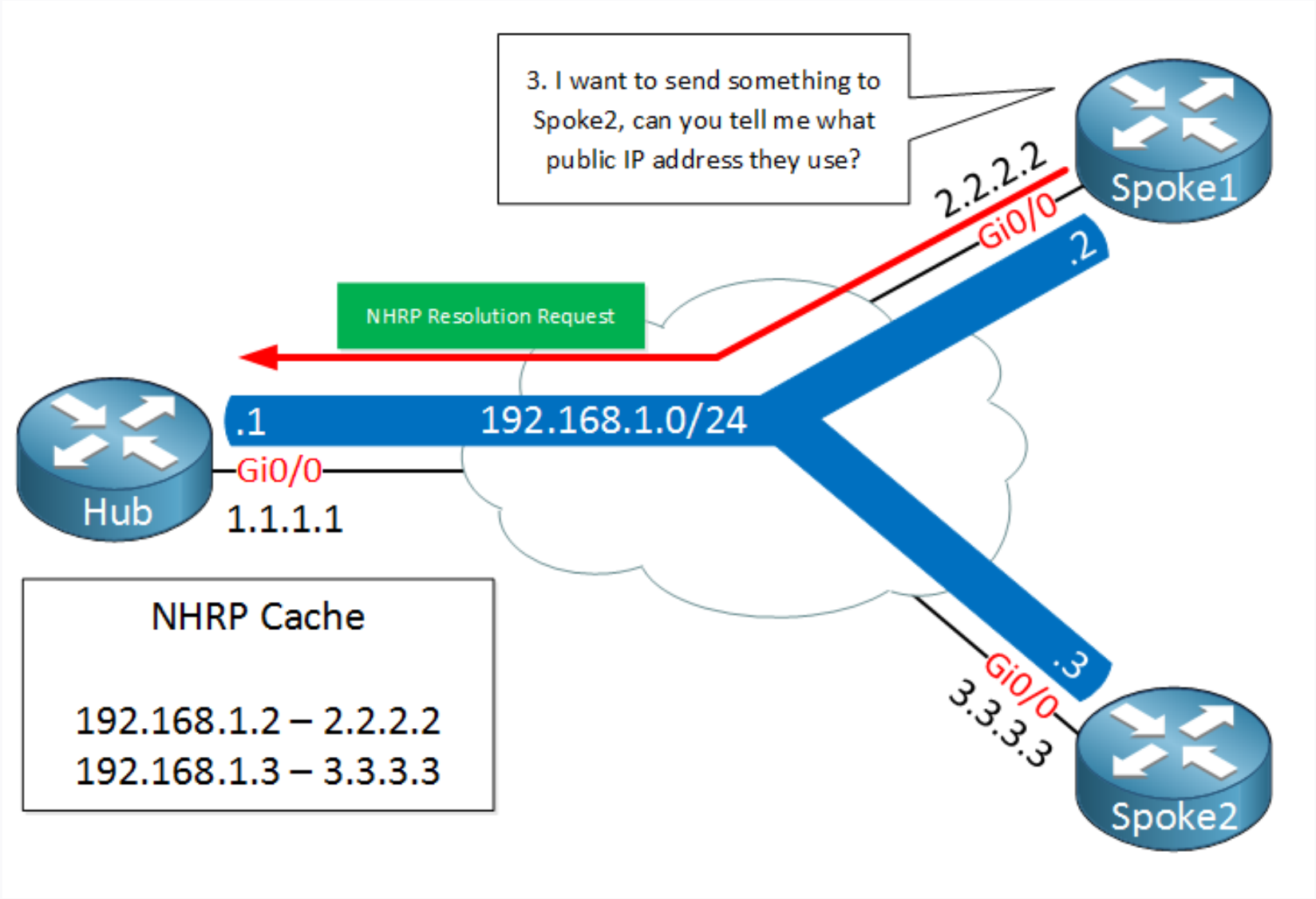
NHRP


1. Establishing tunnel to Hub!
I'm using public IP address
2.2.2.2
2.2.2.2
Gi0/0
Spoke1
.2
NHRP Registration Request
.1
192.168.1.0/24
Gi0/0
Hub
1.1.1.1
NHRP Registration Request
.3
Gi0/0
3.3.3.3
1. Establishing tunnel to Hub!
I'm using public IP address
3.3.3.3
Spoke2

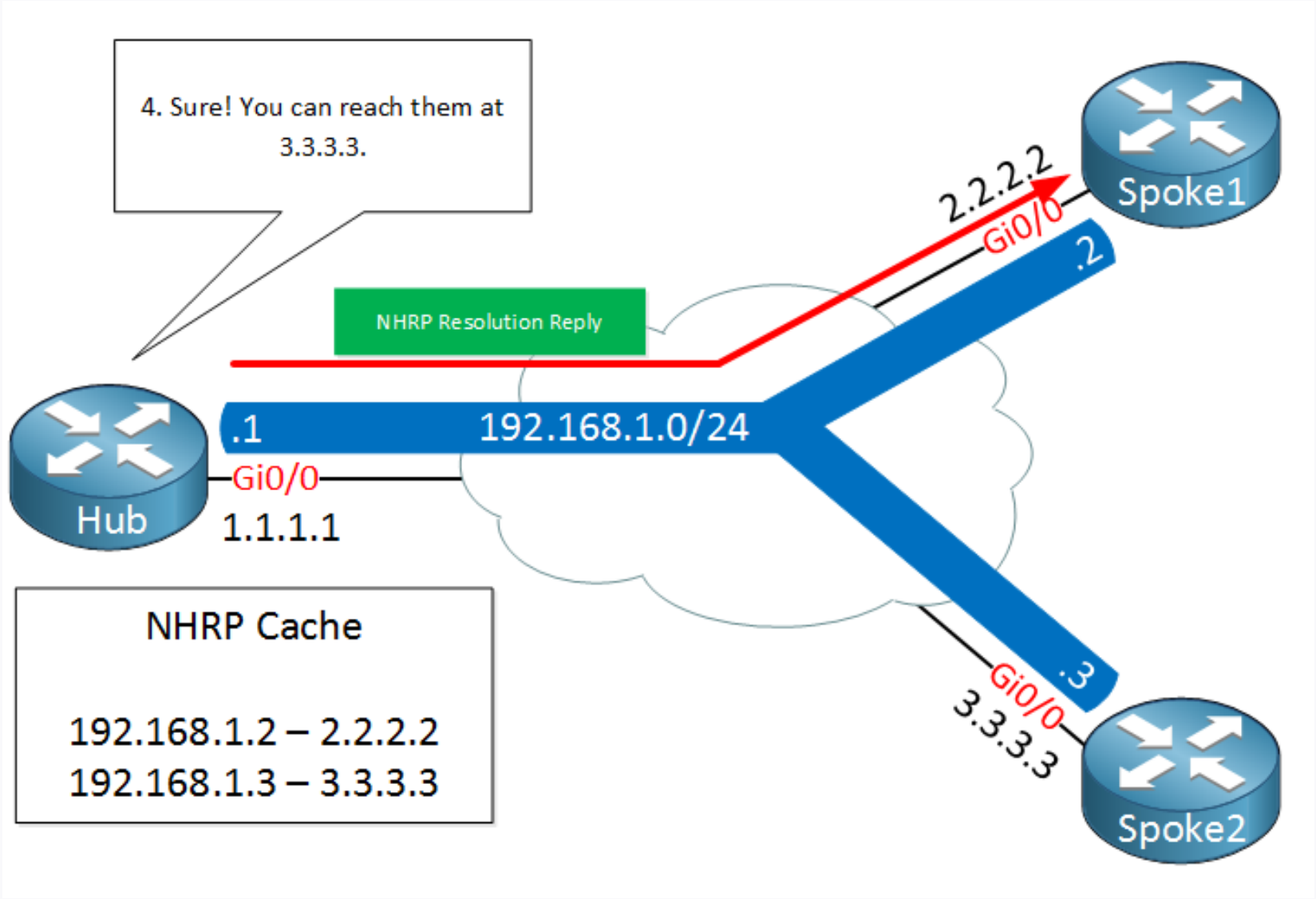
NHRP


2. Great, we have two spokes! Adding their public IP addresses to my NHRP cache!
Hub
.1
Gi0/0
1.1.1.1
192.168.1.0/24
2.2.2.2
Gi0/0
.2
Spoke1
.3
Gi0/0
3.3.3.3
Spoke2
NHRP Cache
192.168.1.2 – 2.2.2.2
192.168.1.3 – 3.3.3.3

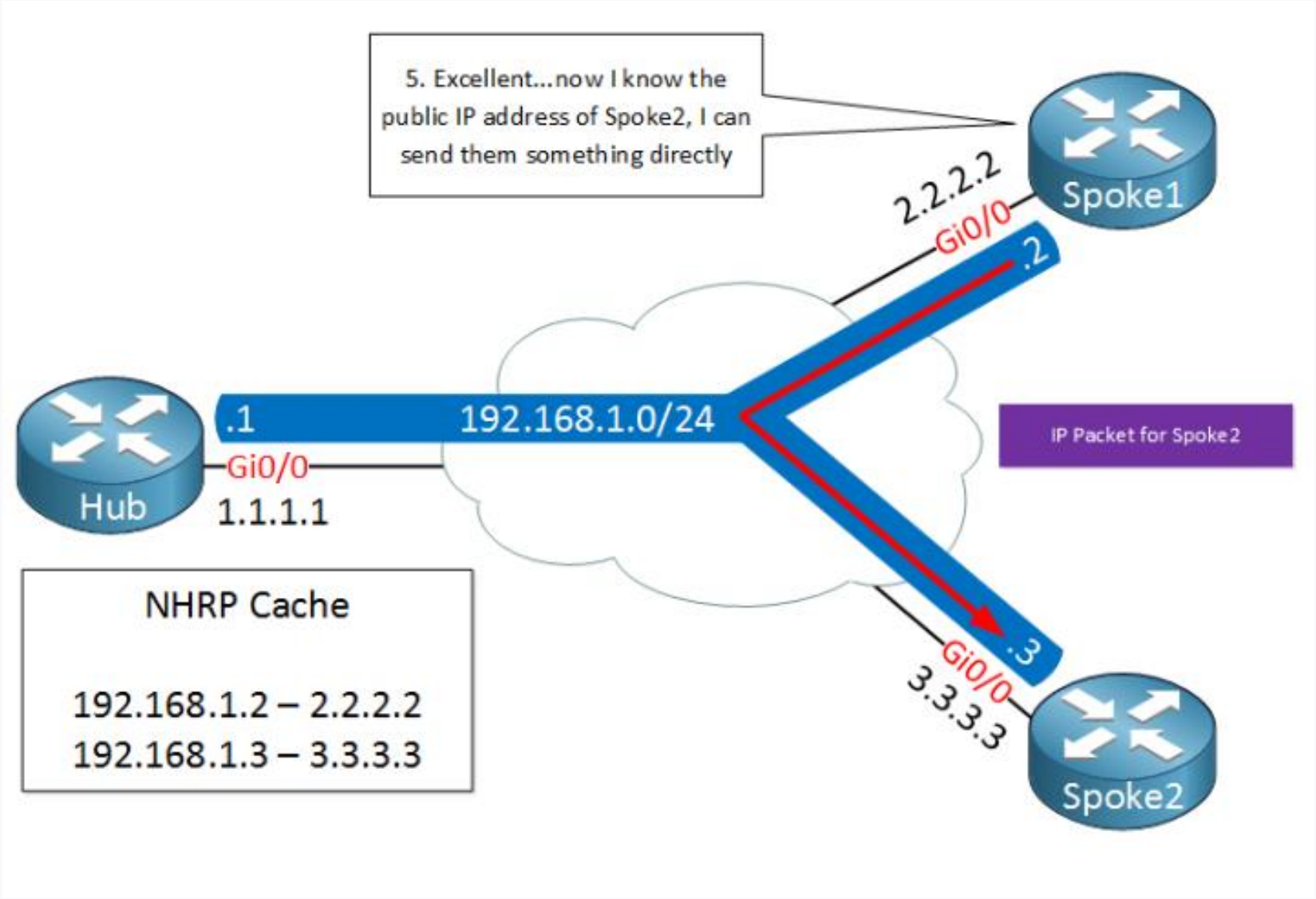
NHRP


3. I want to send something to Spoke2, can you tell me what public IP address they use?
Spoke1
2.2.2.2
Gi0/0
.2
NHRP Resolution Request
.1
192.168.1.0/24
Gi0/0
Hub
1.1.1.1
.3
Gi0/0
3.3.3.3
Spoke2
NHRP Cache
192.168.1.2 – 2.2.2.2
192.168.1.3 – 3.3.3.3

NHRP


4. Sure! You can reach them at 3.3.3.3.
NHRP Resolution Reply
2.2.2.2
Gi0/0
Spoke1
.2
.1
192.168.1.0/24
Gi0/0
1.1.1.1
Hub
.3
Gi0/0
3.3.3.3
Spoke2
NHRP Cache
192.168.1.2 – 2.2.2.2
192.168.1.3 – 3.3.3.3

NHRP


5. Excellent...now I know the public IP address of Spoke2, I can send them something directly
Spoke1
2.2.2.2
Gi0/0
.2
.1
192.168.1.0/24
Hub
Gi0/0
1.1.1.1
IP Packet for Spoke2
NHRP Cache
192.168.1.2 – 2.2.2.2
192.168.1.3 – 3.3.3.3
.3
Gi0/0
3.3.3.3
Spoke2

NHRP

Немного терминологии:

- DMVPN – Dynamic Multipoint VPN
- mGRE – multipoint GRE
- NHS – next-hop server
- NHC – next-hop client
- NHRP – Next-Hop Resolution Protocol


2.2
Phase 1

Phase 1

Реализуется соединение только между Hub и Spoke маршрутизаторами

Соединения между Spoke нет и весь трафик идет только через hub

Протоколы маршрутизации заменяют NHC адрес на адрес NHS

Phase 1

HUB#sh ip nhrp
10.1.1.2/32 via 10.1.1.2, Tunnel0 created 15:17:10, expire 01:22:43
Type: ***dynamic***, Flags: ***unique registered***
NBMA address: 172.16.2.1
10.1.1.3/32 via 10.1.1.3, Tunnel0 created 15:17:10, expire 01:22:43
Type: ***dynamic***, Flags: ***unique registered***
NBMA address: 172.16.3.1

SPOKE1#sh ip nhrp
10.1.1.1/32 via 10.1.1.1, Tunnel0 created 15:17:45, never expire
Type: ***static***, Flags: ***used***
NBMA address: 172.16.1.1

Phase 1

- Static — запись, для которой на интерфейсе явно прописано соответствие туннельного адреса и реального (ip nhrp map ...)
- Dynamic — запись, полученная по NHRP
- Incomplete — знаем туннельный адрес spoke, но еще не получили ответ на NHRP Resolution request.

Phase 1

- **Unique** – Означает, что данный mapping — уникальный и в случае смены NBMA адреса обновление этой записи проводиться не будет.
- **Registered** — получена из NHRP Registration, обычно бывает на хабе.
- **Learned** — получена из NHRP Registration, наоборот, обычно на spoke.
- **Authoritative** – Может использоваться для ответов на NHRP resolution request.
- **Used** – Запись использовалась в предшествующие 60 секунд.
- **Router** – Записи для удаленного роутера или для сетей за ним маркируются таким флагом.
- **Implicit** – Запись получена из информации об источнике в NHRP пакете.
- **NAT** – (появилась в 12.4(6)T версии IOS, не показывается после 12.4(15)T. Показывает, что удаленный пир поддерживает работу через NAT. После 12.4(15) T просто показывается в записи еще и claimed NBMA адрес.

Phase 1

- **no socket** – Запись, для которой роутер не имеет необходимости или не хочет устанавливать IPSec туннель, потому что нет трафика, которому этот туннель нужен. Если в дальнейшем такой трафик появится, то запись будет преобразована в “socket” и туннель IPsec будет поднят. Записи типа Local и implicit всегда сначала маркируются как “no socket”

- **Negative** – Означает, что запрошенный mapping еще не получен. Когда NHRP шлет NHRP resolution request, он ставит этот (negative) флаг на запись типа incomplete, что избавляет роутер от многократных отправок этих запросов в ожидании ответа или установления IPSec соединения.

Phase 1

При обмене маршрутной информацией Hub ставит себя в качестве next-hop для каждого маршрута.

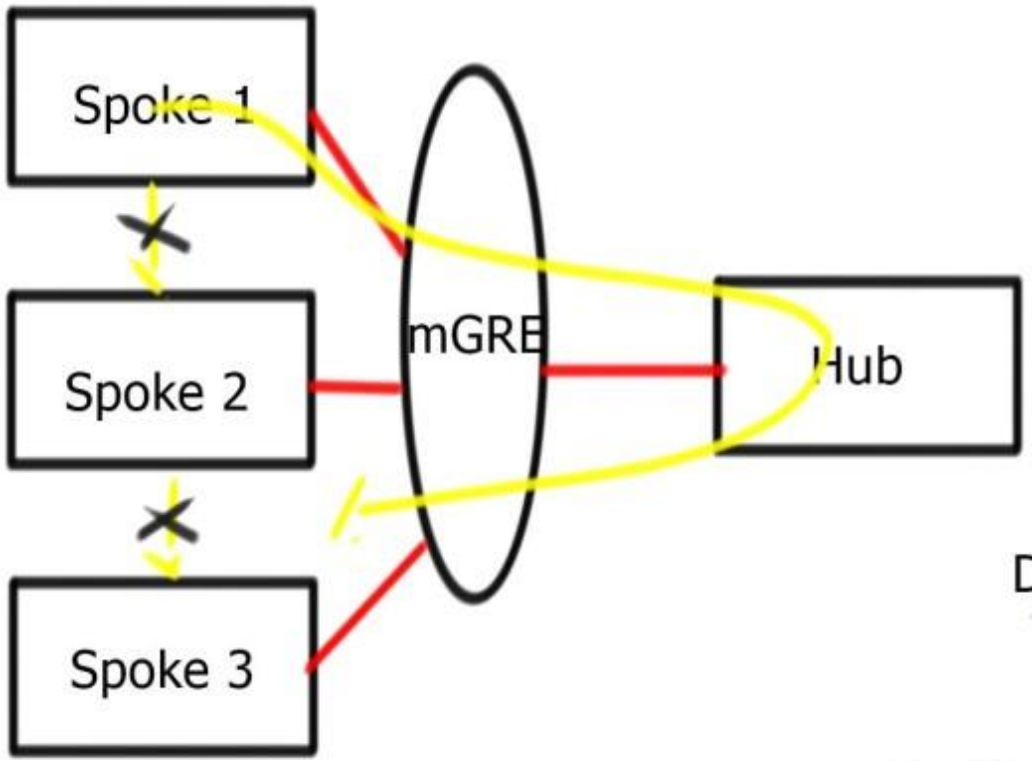
Преимущества:

- Один туннель до всех клиентов
- Оптимизация конфига и работы маршрутизаторов

Недостатки:

- Маршрутизация только через HUB
- Увеличивается задержка

Phase 1



P2P GRE on spoke routers

mGRE on hub router

Default routing on spokes

Dynamic Spoke registration

Data traffic flows through the Hub

No Multicast between Spoke and Spoke


2.3
Phase 2

Phase 2

Реализуется соединение spoke-to-spoke
Все маршрутизаторы получают маршруты без измененного next-hop

В остальном работает аналогично Phase 1

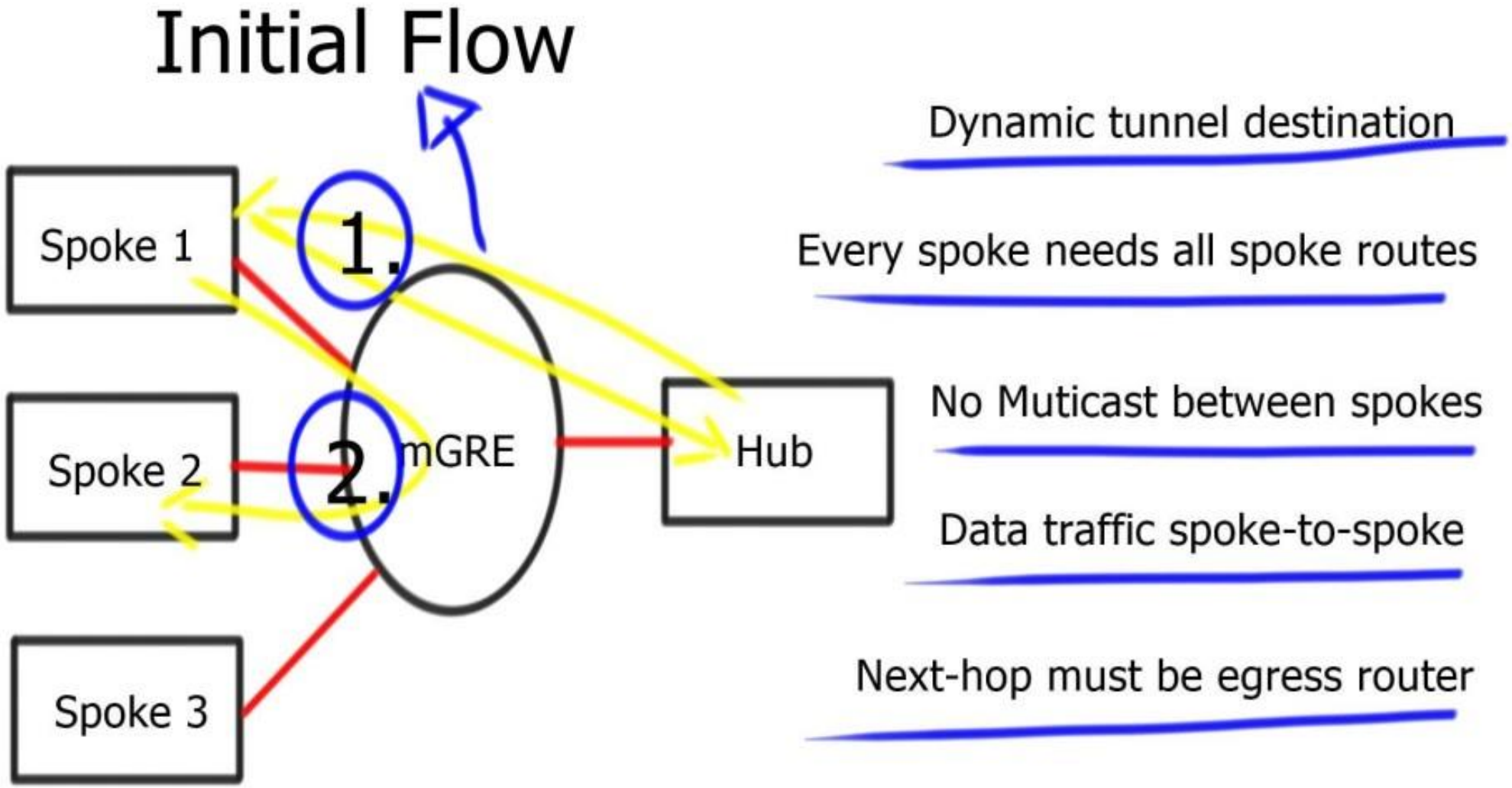
Phase 2

Логика работы:

1. Первый пакет отправляется через NHS.
2. NHC пошлет NHS NHRP request
3. NHS ответит адресом второго spoke
4. Данные передаются напрямую между spoke через GRE

В целом же работа Phase 1 и 2 не сильно отличается друг от друга.

Phase 2


Initial Flow
Spoke 1
Spoke 2
Spoke 3
1.
2.
mGRE
Hub
Dynamic tunnel destination
Every spoke needs all spoke routes
No Muticast between spokes
Data traffic spoke-to-spoke
Next-hop must be egress router


2.4
Phase 3

Phase 3

Основное и главное отличие от Phase 1 и 2 – NHC клиент может отвечать на NHRP requests игнорируя NHS

Регистрации на NHS остается. Это позволяет установить соседство по протоколу маршрутизации и обменяться маршрутной информацией.

У маршрутов может меняться next-hop. Так же возможно(желательно) отправлять суммарную маршрутную информацию, чтобы NHC было проще все обработать.

Phase 3

Когда NHS получает по mGRE туннелю пакет - вынужден отправить его обратно по этому же интерфейсу (но уже другому NHC), NHS шлет NHC источнику — NHRP redirect message.

Это сообщение говорит NHC, можно использовать другой путь до другого NHC.

И указывает использовать NHRP resolution для уточнения пути у NHC.

Первый пакет в любом случае отправляется NHS по адресу.

Phase 3

NHC, пославший первый пакет, получает сообщение redirect, содержащее адрес назначения того самого первого пакета. Этот NHC шлет NHRP resolution request об этом же IP, но не к NHS, а опять по этому же адресу
То есть NHC спрашивает другого NHC о его реальном адресе.

Адрес назначения в NHRP resolution request не NHS, а именно тот NHC, которым интересуется источник, при этом запрос в любом случае будет добираться через NHS.

NHS отправит его тем же самым путем по назначению

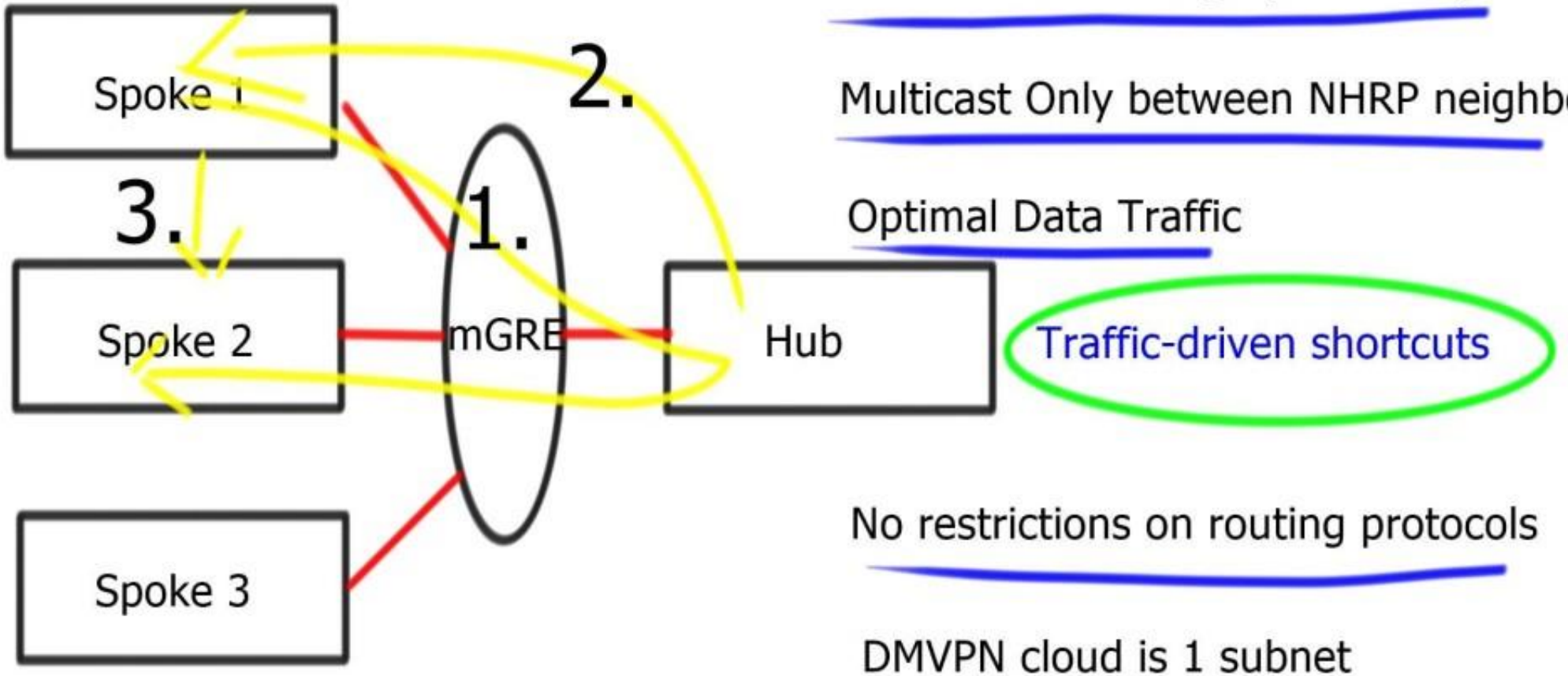
Phase 3

NHC назначения (не NHS) отвечает на resolution request. Используя реальный адрес, приложенный к запросу, этот NHC ответит отправителю напрямую, минуя NHS.

При этом, ответ будет содержать всю сеть (маршрут, префикс), найденный в RIB, а не только запрошенный адрес.

Когда NHC-отправитель запроса получит такой ответ, он узнает реальный next-hop такого адреса, заполнит NHRP-таблицу

Phase 3



No limits on routing Spoke-to-Spoke

Multicast Only between NHRP neighbors

Optimal Data Traffic

Traffic-driven shortcuts

No restrictions on routing protocols

DMVPN cloud is 1 subnet

2.5

Setting

Setting (HUB Phase 1-2)

R1(config)#int tunnel0
(config-if)# ip address 10.1.1.1 255.255.255.0
(config-if)# tunnel source FastEthernet0/0
(config-if)# tunnel mode gre multipoint

Идентификатор сети:
(config-if)#ip nhrp network-id 10

Опционально аутентификацию
R1(config-if)#ip nhrp authentication otus

Маппинг мультикаст рассылок в динамически узнаваемые адреса:
R1(config-if)#ip nhrp map multicast dynamic

Setting (Spoke Phase 1)

```
R1(config)#int tunnel0
(config-if)# ip address 10.1.1.1 255.255.255.0
(config-if)# tunnel source FastEthernet0/0
(config-if)# tunnel destination 10.0.0.1
```

Идентификатор сети:

```
(config-if)#ip nhrp network-id 10
```

Опционально аутентификацию

```
R1(config-if)#ip nhrp authentication otus
```

Setting (Spoke Phase 1)

Маппинг мультикаст рассылок в адрес хаба. Указывается реальный адрес:
R1(config-if)#ip nhrp map multicast 10.0.0.1

Указываем туннельный адрес NHS:
(config-if)# ip nhrp nhs 100.0.0.1

И создаем маппинг для этого туннельного адреса в реальный:
(config-if)# ip nhrp map 100.0.0.1 10.0.0.1

Setting (Spoke Phase 2)

Для второй фазы меняется только тип интерфейса у Spoke:

```
Spoke1(config)# interface Tunnel0
Spoke1(config-if)# ip address 100.0.0.4 255.255.255.0
Spoke1(config-if)# tunnel source FastEthernet0/0
Spoke1(config-if)# tunnel mode gre multipoint
```

Setting (Phase 3)

Для 3 фазы на HUB маршрутизаторе добавляются команды:
(config-if)# ip nhrp redirect

На Spoke маршрутизаторах добавляются:
(config-if)# ip nhrp shortcut
(config-if)# ip nhrp redirect


3
IPSec

IPSec

При работе с DMVPN IPsec с аутентификацией через сертификаты самое удобное и безопасное решение.

1. Настройка CA сервера
2. Выпуск сертификатов
3. Настройка 1 и 2 фазы
4. Привязка к интерфейсу

IPSec

Настройка центра сертификации.
Задать имя домена:
ip domain-name otus.ru

Включить http-сервер:
ip http server

Создать пару корневых ключей:
crypto key generate rsa general-keys label CA exportable modulus 2048

Включаем CA-сервер:
crypto pki server CA
 no shut

IPSec

Настройка клиентов CA-сервера
Создать пару ключей:
crypto key generate rsa label VPN modulus 2048

Настроить trustpoint:
crypto pki trustpoint VPN
 enrollment url http://10.0.0.1
 subject-name CN=R4,OU=VPN,O=Otus,C=RU
 rsakeypair VPN
 revocation-check none

IPSec

Запросить сертификат CA
(config)#crypto pki authenticate VPN

Запросить сертификат для маршрутизатора
(config)#crypto pki enroll VPN

Выдать сертификат на маршрутизаторе CA:
crypto pki server CA grant

IPSec

Выдать сертификат маршрутизатору, который работает как CA-сервер:

Сгенерировать еще один trustpoint
```
crypto pki trustpoint I_CA
 enrollment url http://10.0.1.1
 subject-name CN=R1,OU=VPN,O=OTUS,C=RU
 revocation-check none
 rsakeypair I_CA
```

И аналогично запросить оба сертификата:
```
crypto pki authenticate I_CA
crypto pki enroll I_CA
```

IPSec

Настройка IPSec через сертификаты:
crypto isakmp policy 10
 authentication rsa-sig

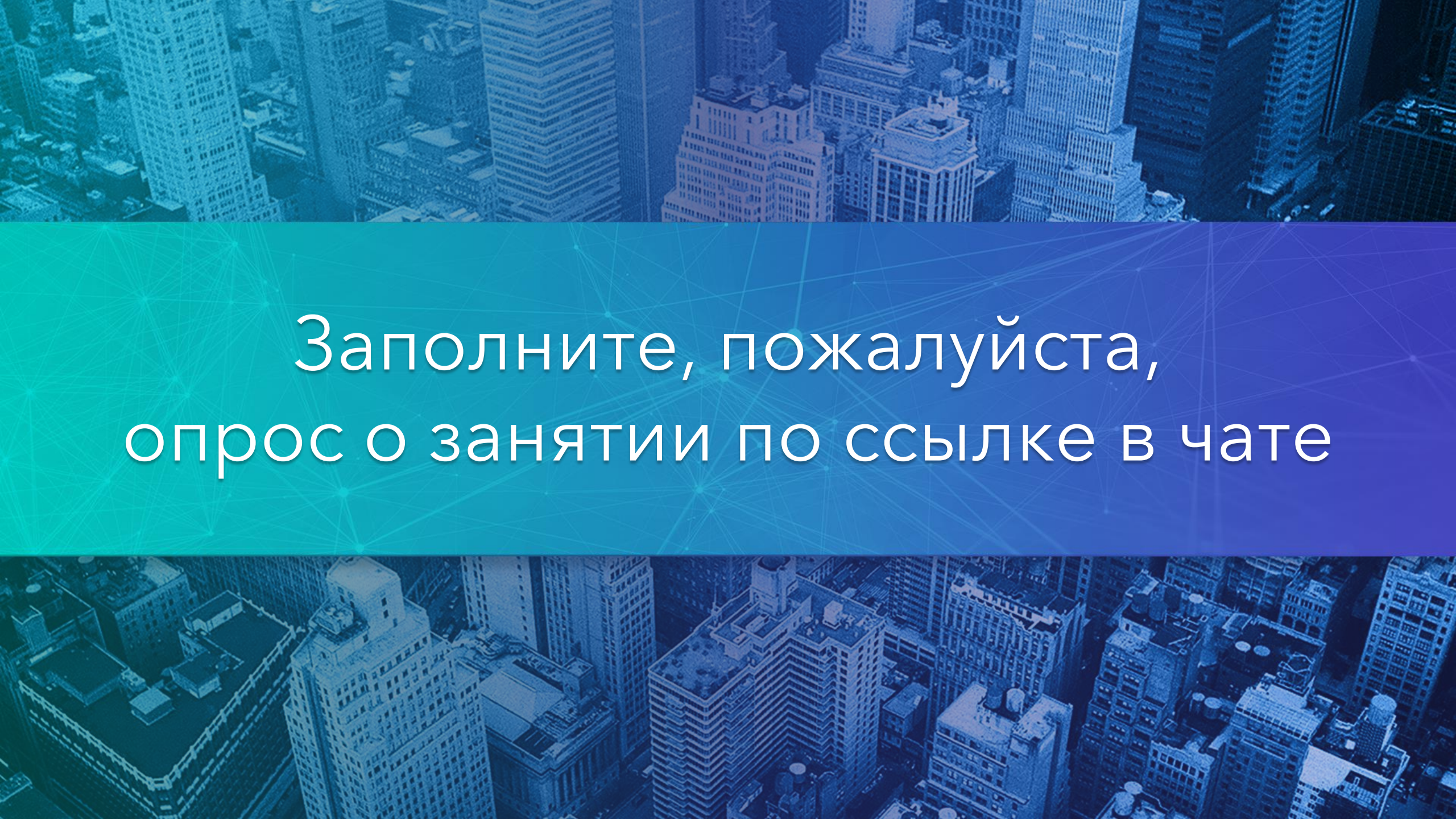
Настроить политику защиты данных
crypto ipsec transform-set SET esp-aes esp-sha-hmac

crypto ipsec profile VTI_prof
 set transform-set SET

Привязать к виртуальному интерфейсу
 interface Tunnel0
 tunnel protection ipsec profile VTI_prof

IPSec

ISAKMP: sh crypto isakmp sa sh crypto isakmp sa detail sh crypto isakmp peers IPSec: sh crypto ipsec sa sh crypto ipsec sa detail sh crypto ipsec profile sh crypto session { brief | detaill}	Проверить работу CA-сервера sh crypto pki server Посмотреть сертификаты на маршрутизаторе sh crypto pki certificates Посмотреть запросы на сертификат sh crypto pki server CA requests


Заполните, пожалуйста,
опрос о занятии по ссылке в чате

До новых встреч!
Приходите на следующие занятия

Кулиничев Алексей
Администратор Сетей
Santchous42@yandex.ru