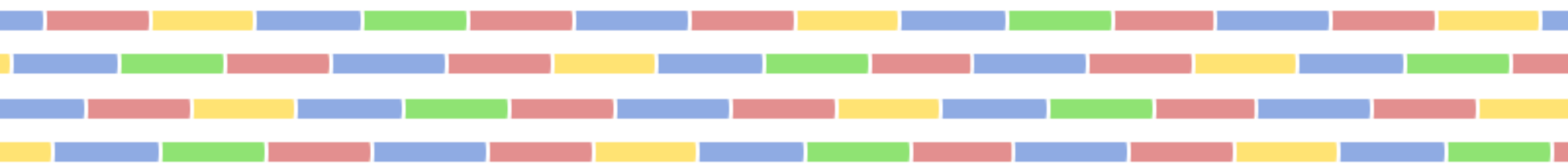
VPN

Виртуальная частная сеть



VPN

Virtual Private Network — виртуальная частная сеть

Обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети.

wikipedia.org

Под определение попадает очень много разных технологий на разных уровнях стека TCP/IP и/или сетевой модели OSI.

Термином “VPN” принято называть некий набор технологий (PPTP, L2TP,OpenVPN и т.д.)

Синонимом “тунель” принято называть другой набор (IP-IP, GRE и т.д.)

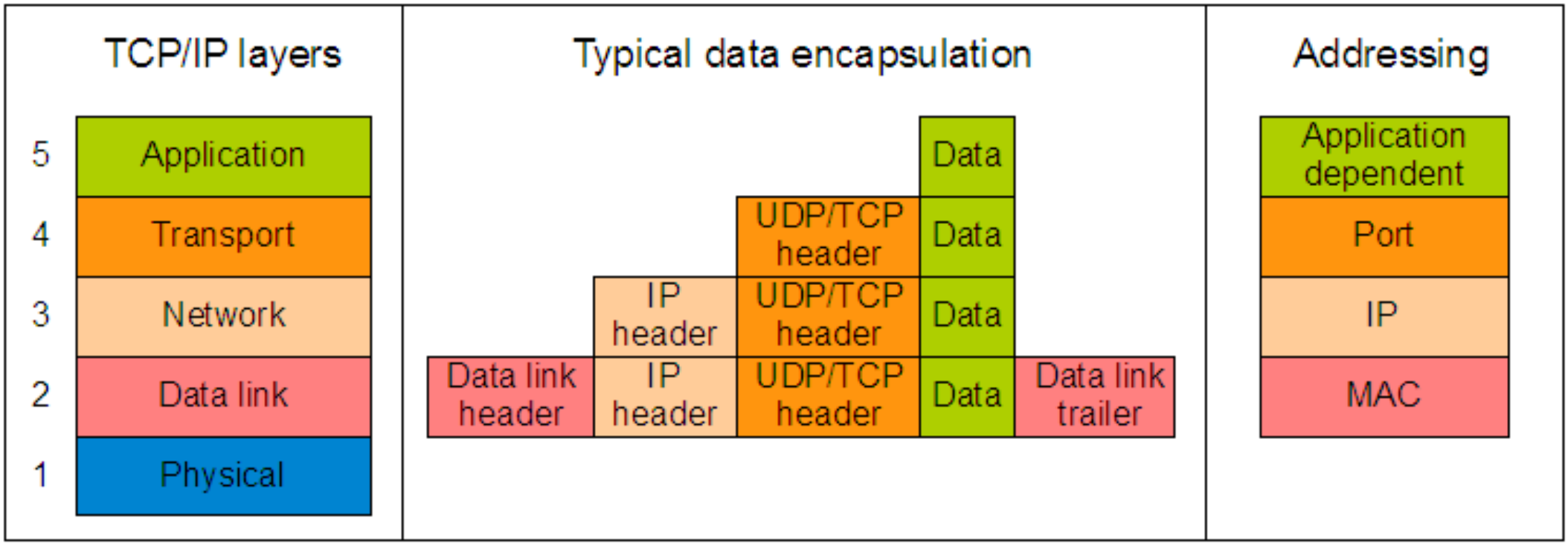
VPN

Классификация

VPN Классификация

- Область применения / защищеность
  - Внутри организации / доверительные сети
    VLAN, MPLS, VPLS и другие
  - Через открытые сети / защищенные
    PPTP, L2TP, OpenVPN и другие
- Открытые / проприетарные протоколы
- Способ реализации
  - VPN точка-точка (с PPP и без него)
  - VPN многоточка

TCP/IP



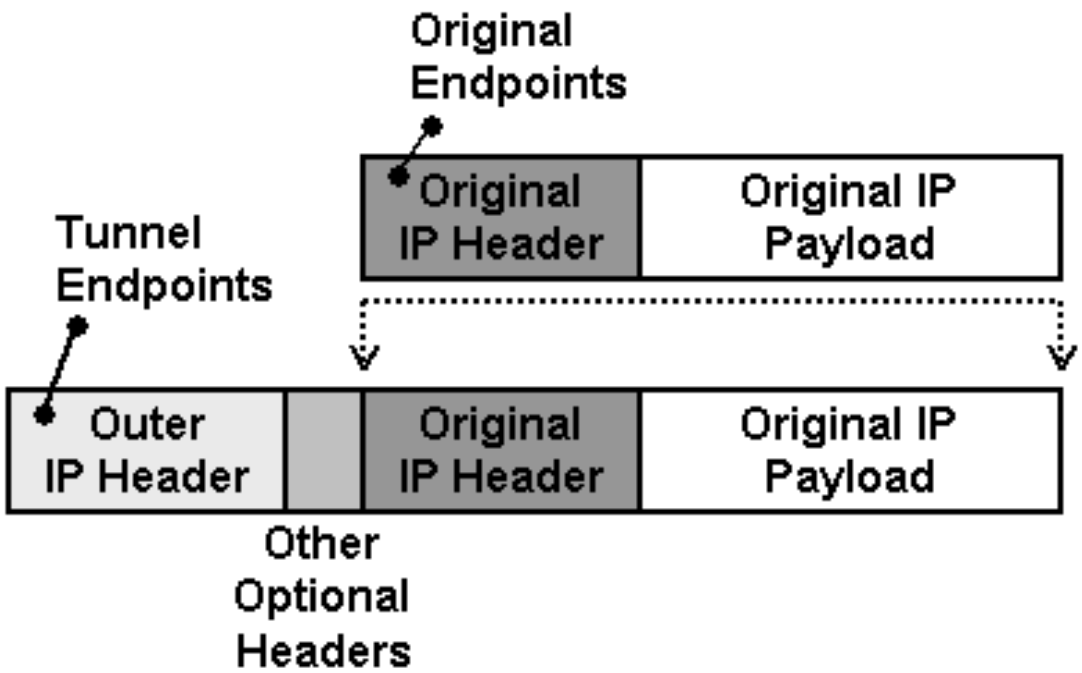
MTU 1500 байт (на Network уровне)

VPN точка-точка

Туннели IP-IP, GRE

IP-IP

Простая инкапсуляция

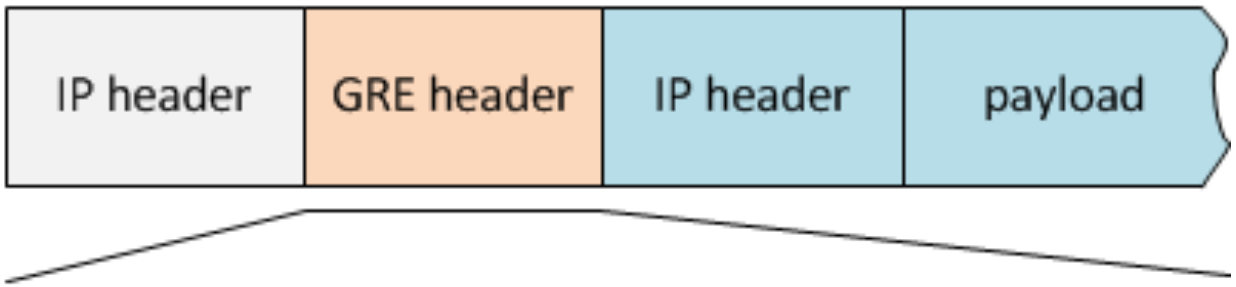


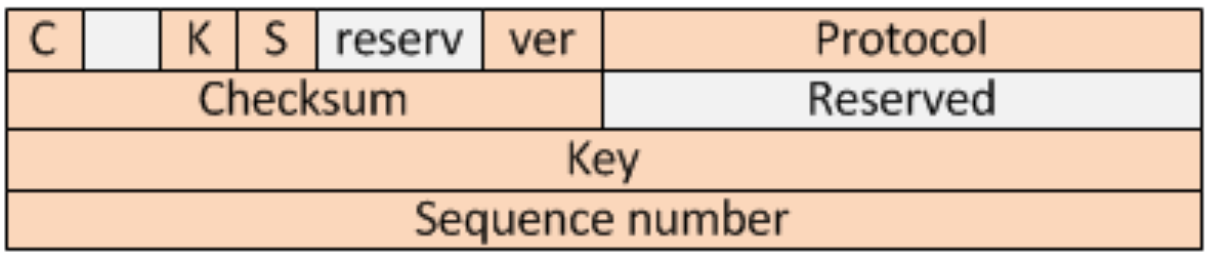
Защиты нет.
Аудентификации нет.

Каждый тунель должен настраиваться вручную.

Накладные расходы 20 байт
MTU в туннеле 1480.

GRE - Generic Routing Encapsulation





Разработка Cisco

RFC 2784

Аудентификации, защиты нет.

Возможны несколько тунелей с одинаковыми концами (различный key)

Накладные расходы 20 байт (IP) + 4 байта (GRE)

VPN точка-точка

PPP

PPP (Point-to-Point Protocol)

Layer 2 по стеку TCP/IP

PPP может работать на любой “трубе” способной передать байты/символы в обе стороны.

Разработан в 1989 г, RFC1661 - 1994 г.

PPP over SSH - одной командой

```
/usr/bin/pppd updetach noauth silent nodeflate pty \
     "/usr/bin/ssh root@remote-gw pppd nodetach notty noauth" \
     ipparam vpn 10.0.8.1:10.0.8.2
```

PPP (Point-to-Point Protocol)

Разрабатывался для канального уровня (по стеку TCP/IP)

Возможности

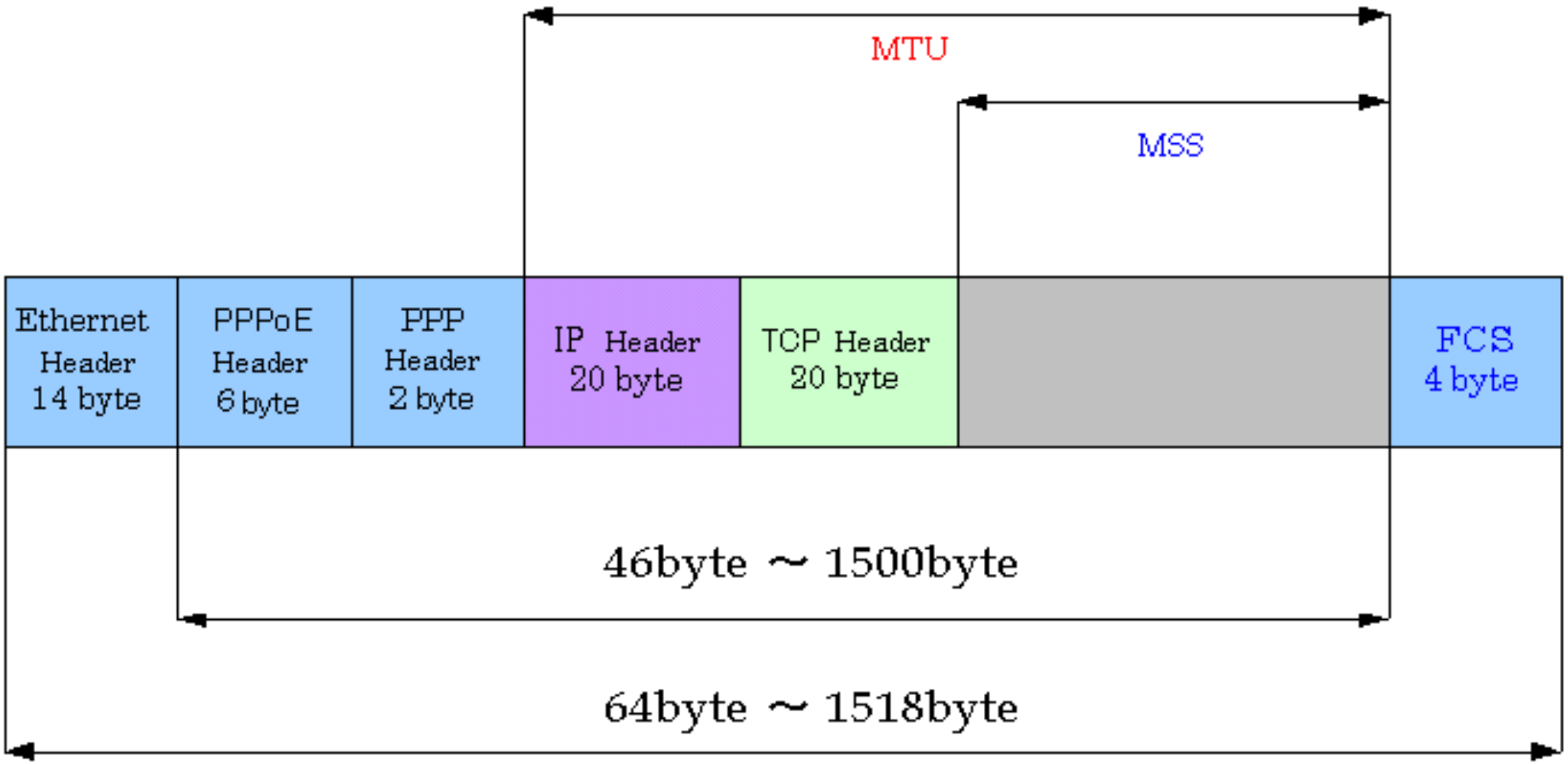
- Аутентификация (защита слабая)
- Поддержка многих сетевых протоколов (3-го уровня)
- Сжатие
- Шифрование (слабое)

На практике необходимо указать логин и пароль, остальные параметры могут быть согласованы автоматически.

VPN точка-точка

С использованием PPP

PPPoE (PPP over Ethernet)



PPP Over Ethernet - RFC 2516, 1999г

PPPoE (PPP over Ethernet)

Для настройки клиента необходимо указать

- Параметры PPP (Обычно логин и пароль)
- MAC адрес сервера/концентратора (не обязательно)

MAC адреса доступных концентраторов находится через широковещательный запрос PADI (PPPoE Active Discovery Initiation).

Накладные расходы (байт)

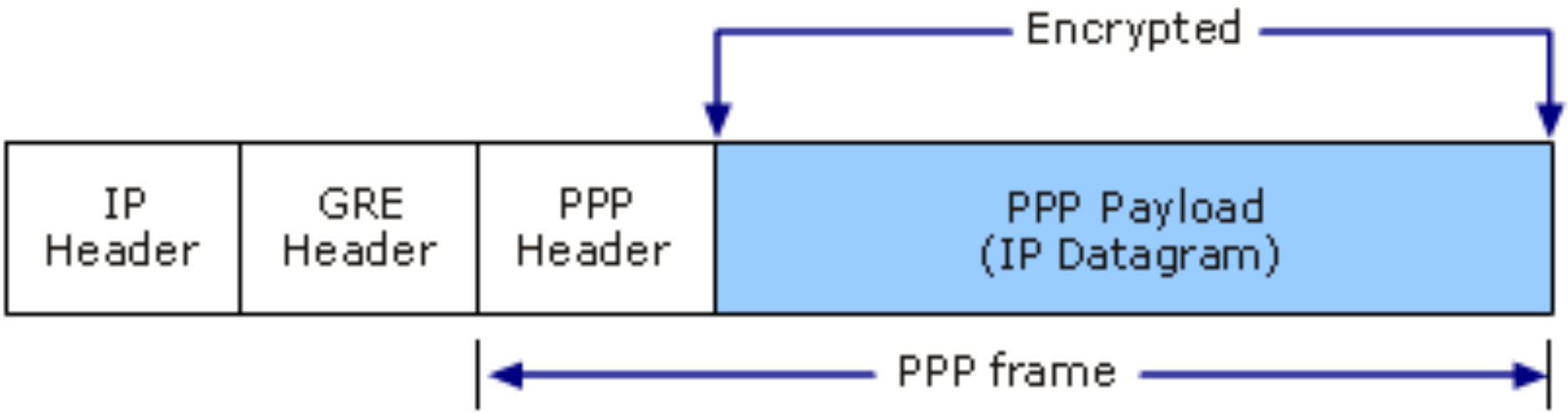
6 (PPPoE) + 2 (PPP) = **8 байт**

Защита

Аудентификация и шифрование - слабые

Поддерживается многими сетевыми устройствами.

PPTP (PPP over GRE)



Point-to-Point Tunneling Protocol - RFC 2637, 1999г

Использует

- Управляющее соединение TCP 1723
- Модифицированный GRE для инкапсуляции PPP

PPTP (PPP over GRE)

Для настройки клиента необходимо указать

- Адрес VPN сервер
- Параметры PPP (обычно логин и пароль)

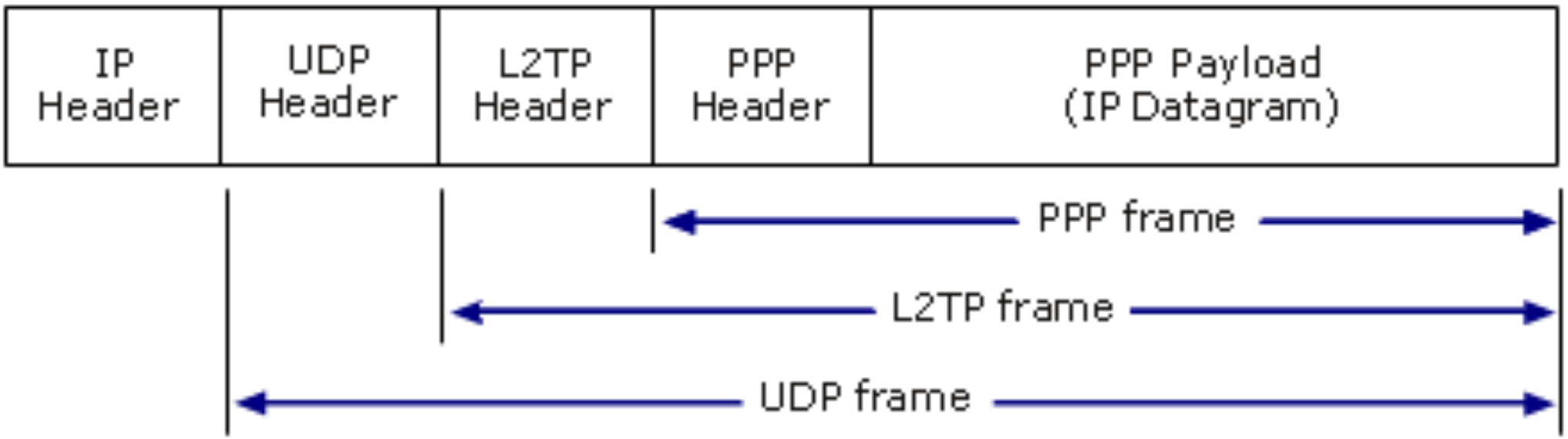
Накладные расходы (байт)
20 (IP) + 4 (GRE) + 2 (PPP) = **26 байт**

Защита
Аудентификация и шифрование - слабые

Поддерживается большинством сетевых устройств.

Может НЕ заработать через NAT

L2TP (PPP over UDP)



Layer 2 Tunneling Protocol - RFC 2661, 1999г

Протокол UDP порт 1701

L2TP (PPP over UDP)

Для настройки клиента необходимо указать

- Адрес VPN сервер
- Параметры PPP (обычно логин и пароль)

Накладные расходы (байт)

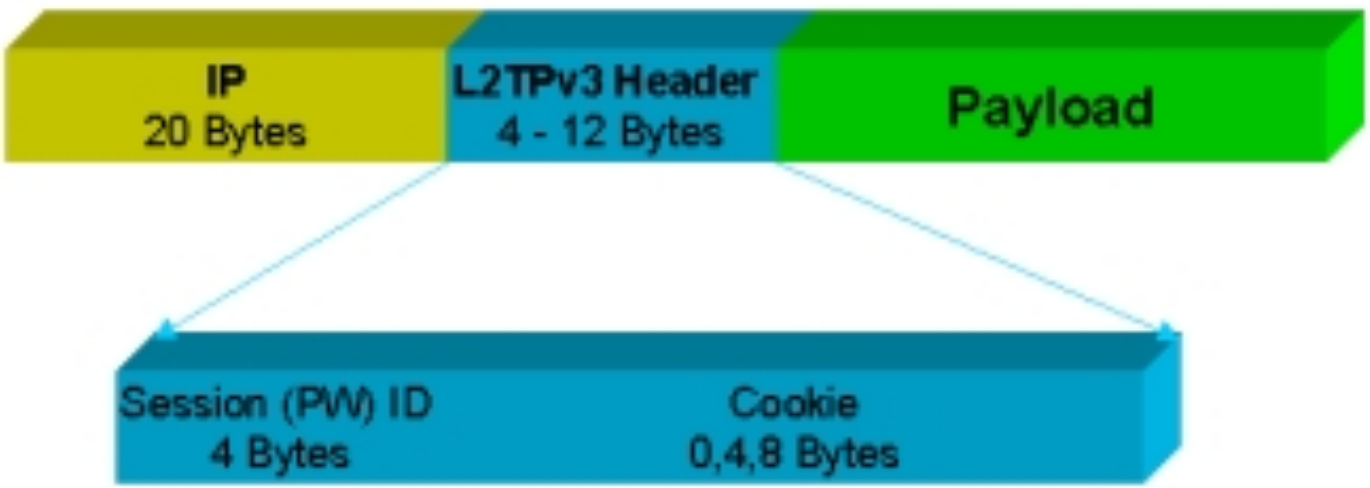
20 (IP) + 8 (UDP) + 4 (L2TP) + 2 (PPP) = **34 байт**

Защита

Аудентификация и шифрование - слабые

Поддерживается многими сетевыми устройствами.

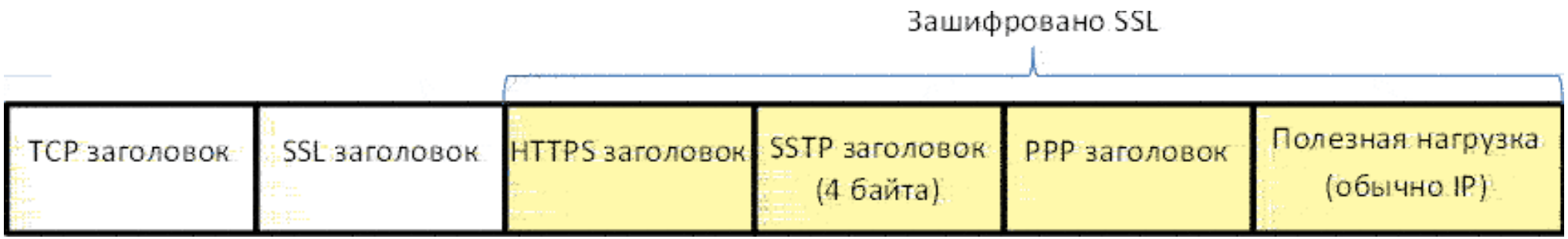
L2TPv3



Без PPP

В примерах часто встречается объединение Ethernet сегментов через IP сеть

SSTP (PPP over HTTPS)



Разработка Microsoft. RFC нет.

Протокол TCP порт 443 (https)

SSTP (PPP over HTTPS)

Для настройки клиента необходимо указать

- Адрес VPN сервер
- Сертификат с закрытым ключом клиента
- Параметры PPP (обычно логин и пароль)

Накладные расходы (байт)

20 (IP) + 20 (TCP) +

? (SSL) + ? (HTTP) + 4 (SSTP) + 2 (PPP) = ? байт

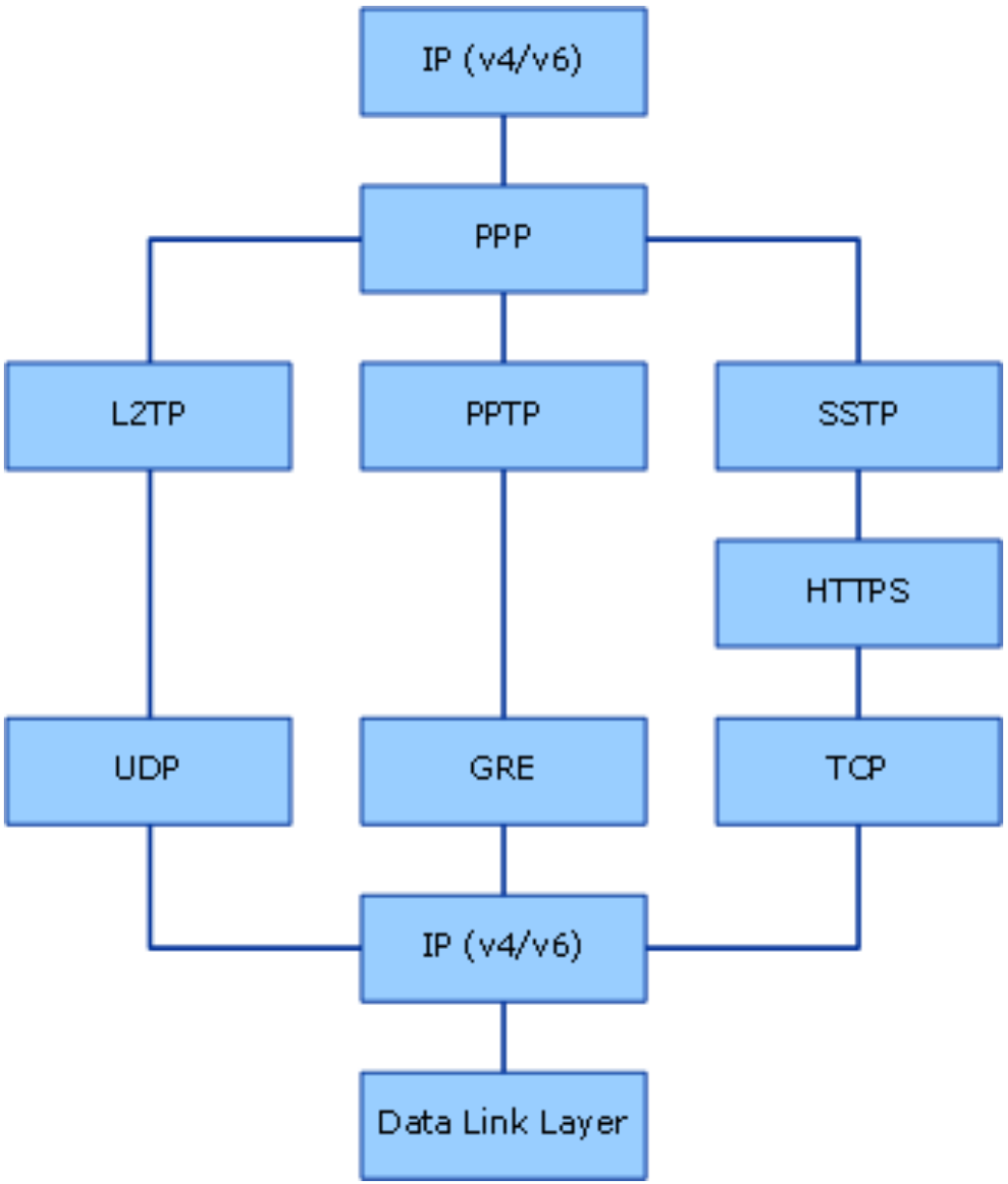
Защита

Аудентификация и шифрование - зависят от настроек SSL

Набирает популярность.

Работает через NAT, прокси, и т.д.

PPP based VPN



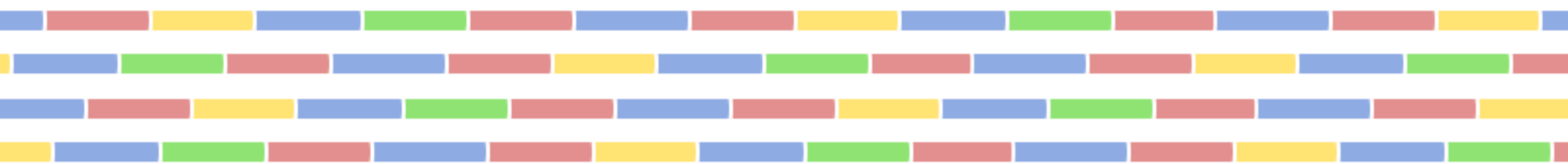
Источник technet.
microsoft.com

VPN точка-точка

Сами по себе протоколы

VPN

IPSec



IPSec (IP Security)

Протокол обмена ключами IKE (Internet Key Exchange)

- UDP порт 500 и 4500 (NAT-T)

Разделяют две фазы IKE

- Phase 1. Идентификация удаленного узла
- Phase 2. Согласование параметров шифрования

Дополнительные заголовки

- AH - Authentication Header. Обеспечивает целостность, но не шифрует
- ESP (Encapsulating Security Protocol). Шифрует

IPSec (IP Security)

Особенности

- Нет виртуального интерфейса. Трафик направляемый в тунель определяется ACL
- Любая сторона может инициировать соединение

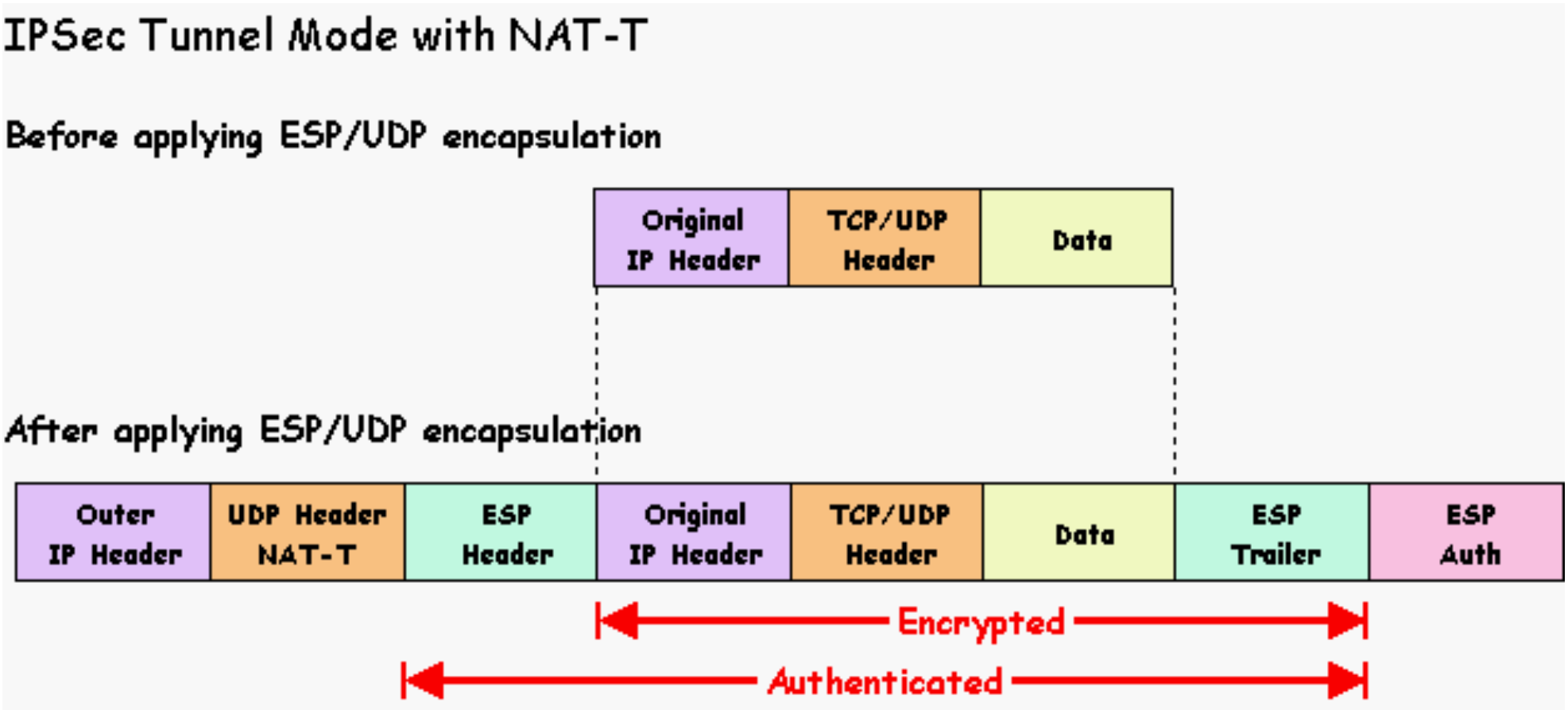
Множество разных реализаций IPSec

- Linux. IKE демоны - Racoon/Racoon2/strongSwan
- Microsoft Windows IPSec
- Cisco IPSec
- ...

Вполне могут быть совмещены между собой.

(в настоящее время)

IPSec (IP Security)



RFC2401 — RFC2412

IPSec IKEv1

Необходимо настроить/согласовать параметры

Peer IP address	**xx.xx.xx.xx**
PHASE I	
Key management	**Pre-shared | Certificates**
Encryption algorithm	**AES-128**
Hash algorithm	**SHA-1**
Diffie-Hellman group	**2**
Key lifetime in seconds	**86400**
PHASE II	
Encryption algorithm	**ESP-AES-128**
Authentication algorithm	**SHA-HMAC**
Perfect Forward Secrecy	**group2**
Security association lifetime in seconds	**28800**

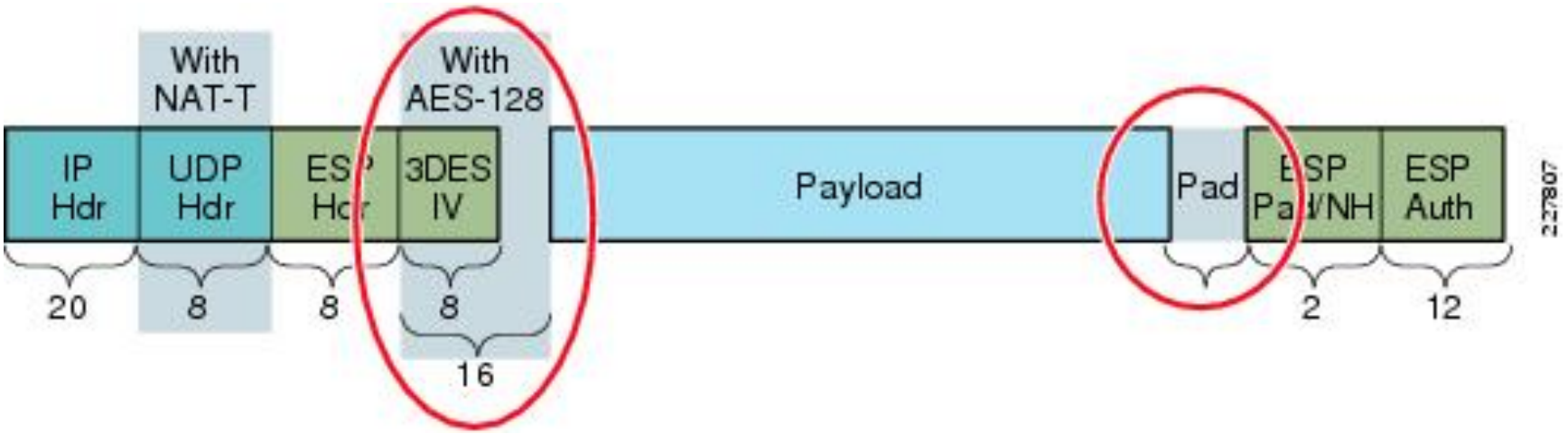
IPSec IKEv2

IKEv1 несовместим с IKEv2

Преимущества IKEv2

- Меньше работы человеку
- Меньше пакетов на установление соединения
- Гибкость аудентификации
- Другие улучшения

IPSec (IP Security)



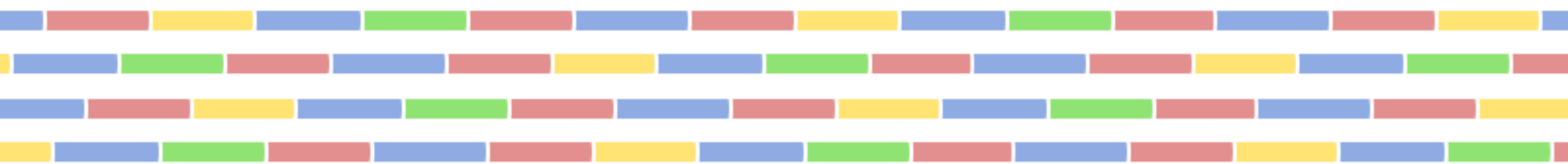
Шифруется блоки кратно 4-х байт.

Накладные расходы зависят от типа шифрования
Заголовки для ESP-AES-128 занимают до 41 байт

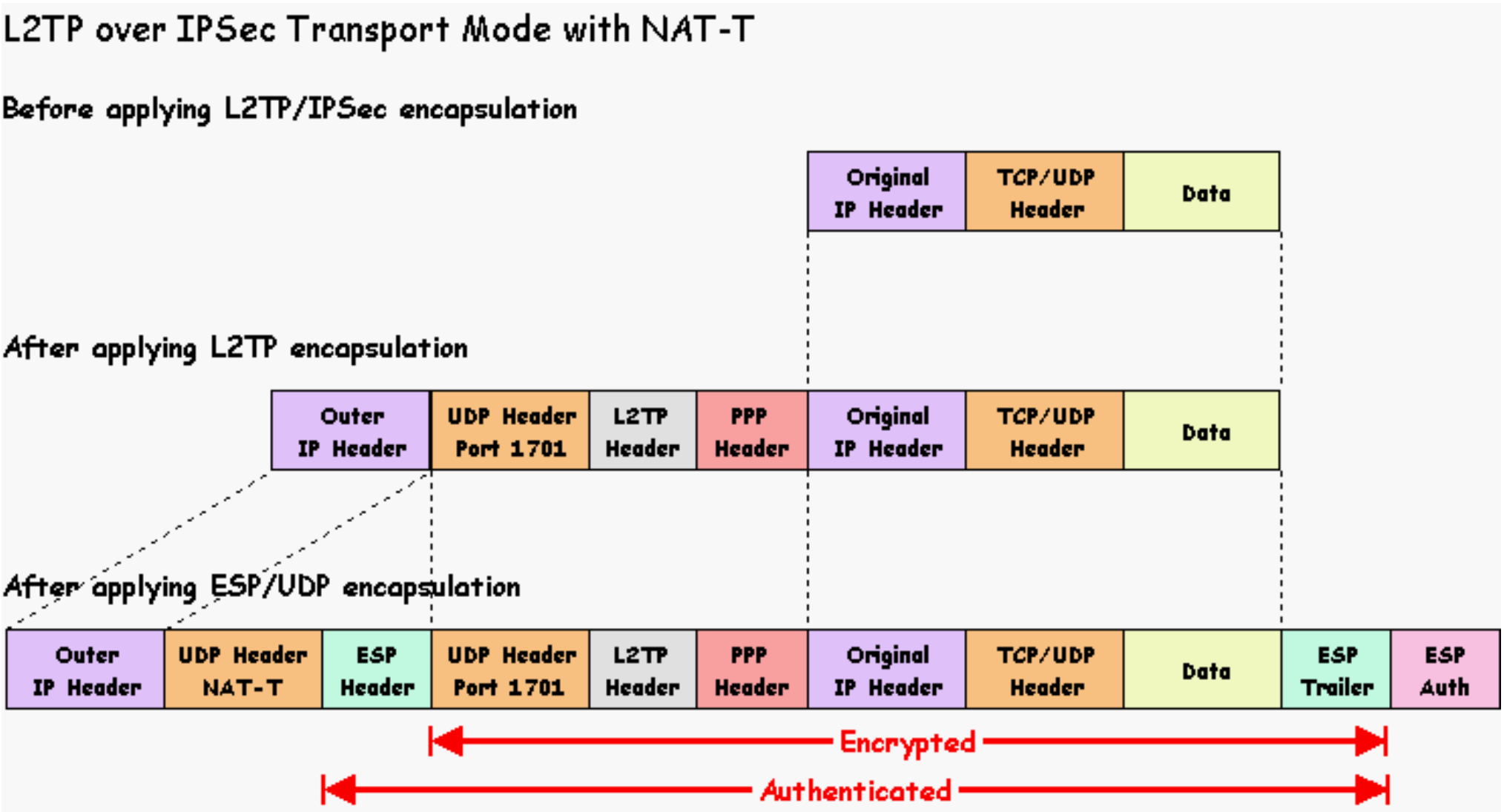
VPN/Tunnel Mode	**Overhead Elements**	**Maximum Bytes**
IP + ESP-AES-128	IP + ESP-AES-128	8 + 41 = **49**
IP + NAT-T + ESP-AES-128	IP + UDP + ESP-AES-128	20 + 8 + 41 = **69**
IP + NAT-T + ESP-AES-128 + SHA1	IP + UDP + ESP-AES-128 + SHA1	20 + 8 + 41 + 12 = **81**

VPN

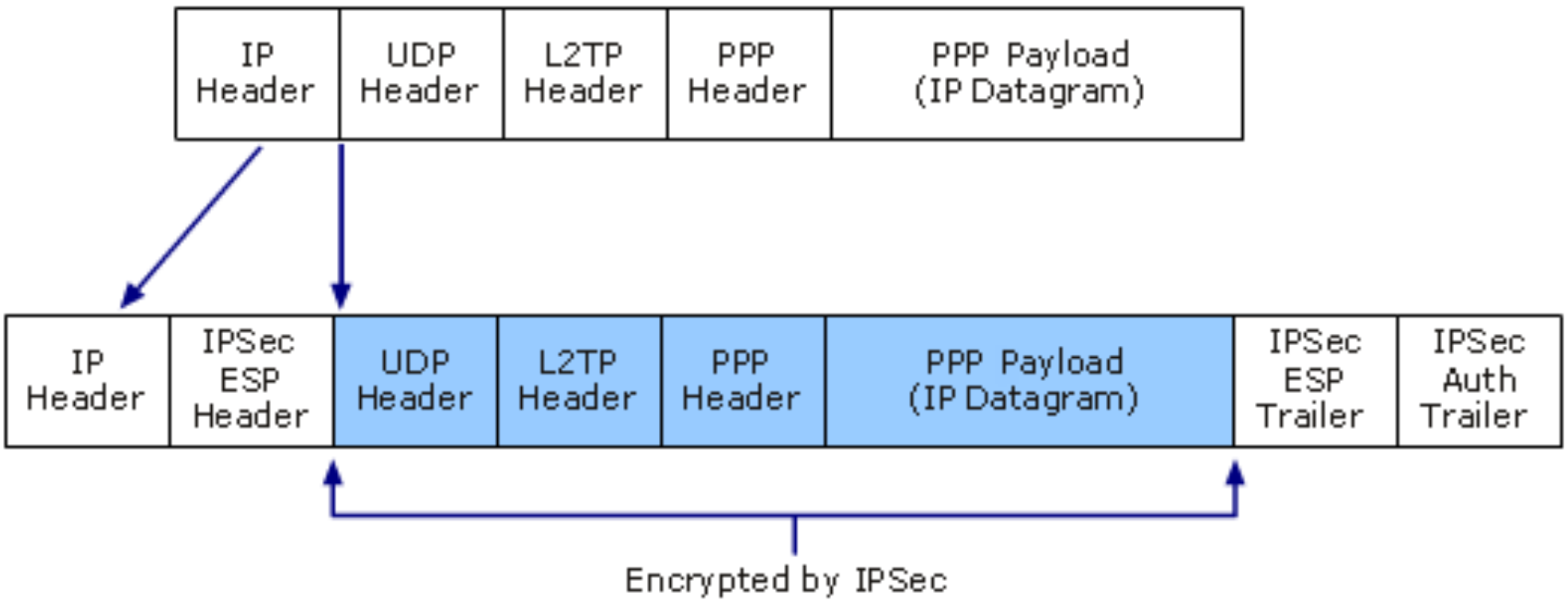
L2TP over IPSec



L2TP over IPSec



L2TP over IPSec



Накладные расходы (байт)

20 (IP) + (8) UDP + 4(L2TP) + 2 (PPP) = 34

8 (ESP Header) + до 45 (ESP Trailer) + 8 (NAT-T) = 61

Итого до 95 байт при AES128+SHA1

VPN точка-точка

OpenVPN

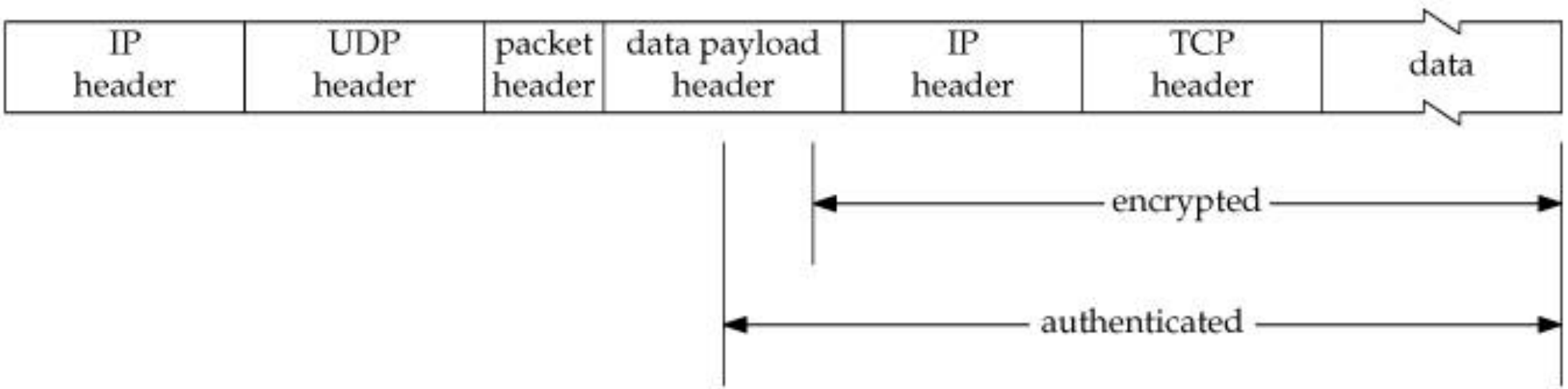
OpenVPN

OpenVPN Version 1 - 2001г
Лицензия GNU GPL
RFC нет

Использует

- TCP и/или UDP порт 1194
- SSL/TLS via OpenSSL
- TAP/TUN интерфейсы - Ethernet / IP пакеты соответственно

OpenVPN



(A) TCP Packet Header (3 bytes)

(B) UDP Packet Header (1 byte)

OpenVPN

Настройки клиента

- Адрес сервера
- Тип интерфейса
- Аудентификация
  - Certificates
  - Pre-shared key
  - Login / Password

Накладные расходы (байт)

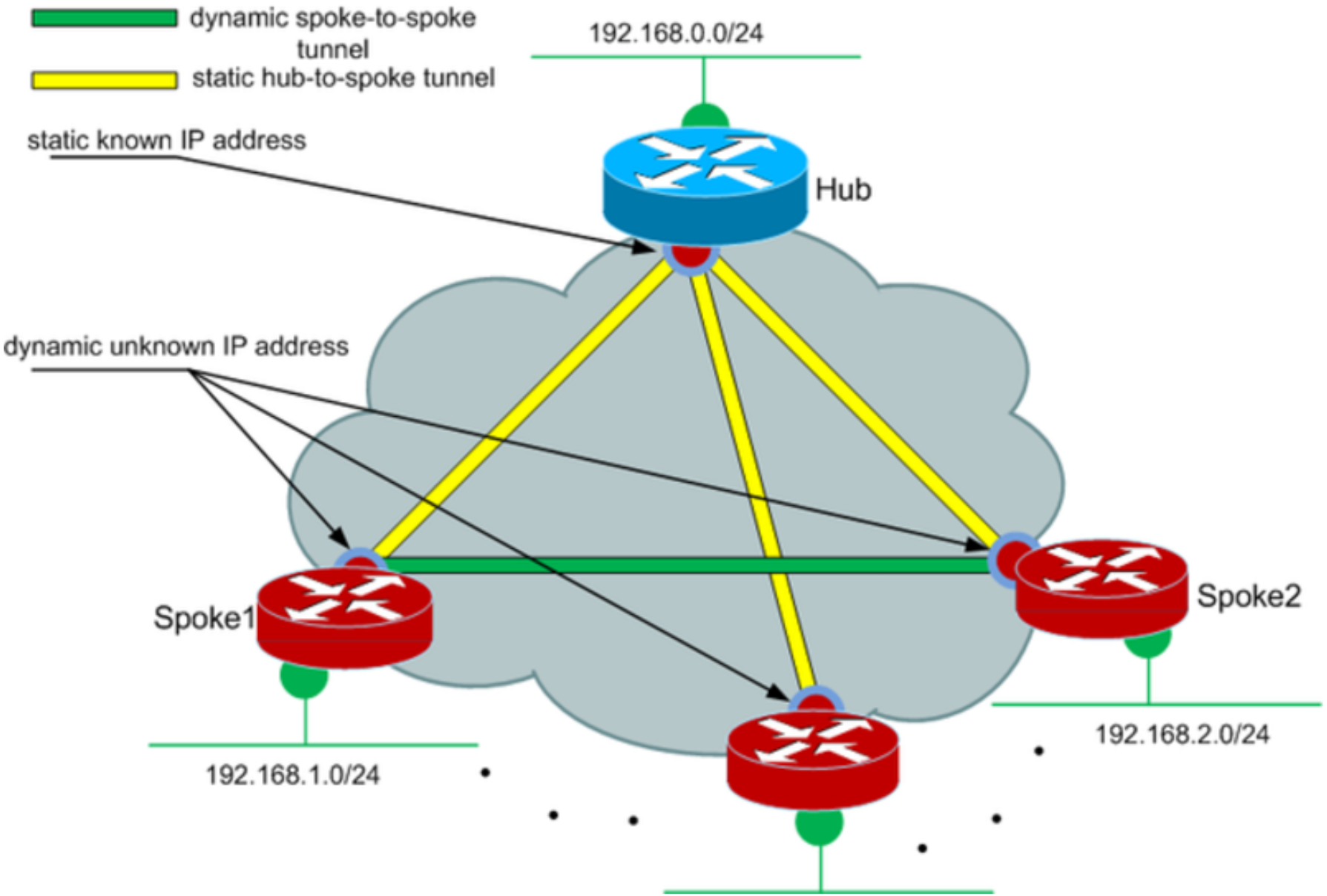
20(IP) + 8(UDP) + 1(OpenVPN) = 29 байт

20(IP) + 20(TCP) + 3(OpenVPN)= 43 байт

VPN многоточка

DMVPN

DMVPN Dynamic Multipoint Virtual Private Network



DMVPN

Использует

- IPSec, IKEv1
- mGRE - Multipoint GRE
- NHRP - Next Hop Resolution Protocol

Связь инициирует всегда Spoke

DMVPN mGRE

Multipoint GRE

Такой tunnel интерфейс в котором не указывается peer

```
interface Tunnel1
    ip address 10.10.10.1 255.255.255.0
    tunnel source FastEthernet0/0
    tunnel mode gre multipoint
```

Как же узнать адрес peer-а ?

DMVPN NHRP

Next Hop Resolution Protocol — клиент-серверный протокол преобразования адресов, позволяющий всем хостам, которые находятся в NBMA (Non Broadcast Multiple Access) - сети, динамически выучить NBMA-адреса (физические адреса) друг друга обращаясь к next-hop-серверу (NHS).

Hub

```
interface Tunnel1
  ip address 172.16.1.1 255.255.255.0
  tunnel source FastEthernet0/0
  tunnel mode gre multipoint
  ip nhrp map multicast dynamic
```

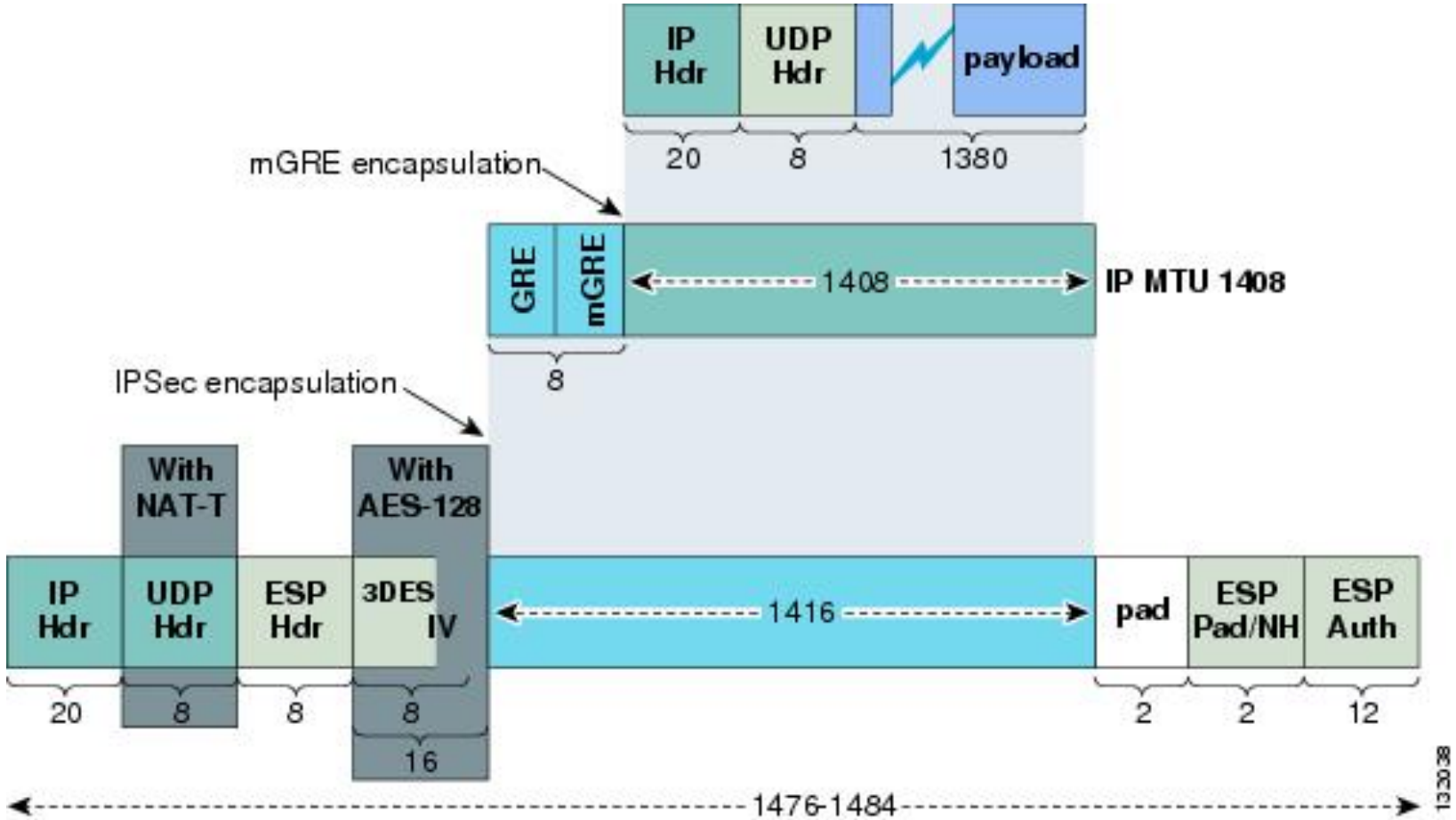
Spoke

```
interface Tunnel1
  ip address 172.16.1.101 255.255.255.0
  tunnel source FastEthernet0/0
  tunnel mode gre multipoint
  ip nhrp map multicast 1.1.1.1
  ip nhrp map 172.16.1.1 1.1.1.1
```

Достаточно знать IP адрес HUB-а, чтобы попасть в сеть!

А где безопасность?

DMVPN



Cisco рекомендует MTU = 1408 байт для DMVP

Накладные расходы ~ 80 байт

FlexVPN как развитие DMVPN

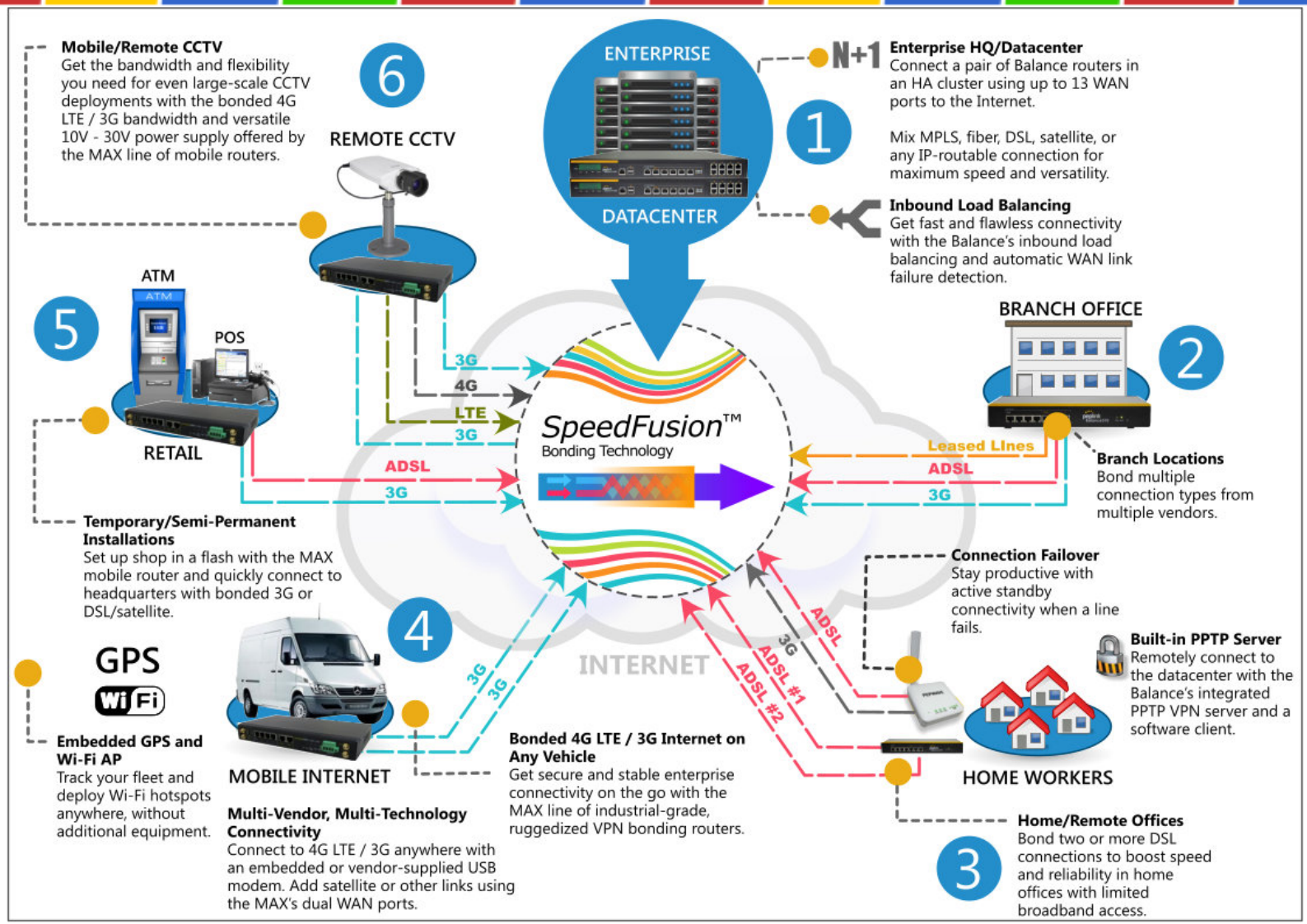
VPN	Interop	Dynamic Routing	IPsec Routing	Spoke-spoke direct (shortcut)	Remote Access	Simple Failover	Source Failover	Config push	Per-peer config	Per-Peer QoS	Full AAA Management
Easy VPN	No	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
DMVPN	No	Yes	No	Yes	No	partial	No	No	No	group	No
Crypto Map	Yes	No	Yes	No	Yes	poor	No	No	No	No	No
Flex VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

FlexVPN - реализация IKEv2 и не только

VPN

Свободные мысли

Load Balancing / Aggregation



Peplink / Baracuda / Mushroom и другие

VPN с коррекцией ошибок

Проблема - имеем из точки А в точку Б несколько каналов с некой надежностью и некоторой вероятностью потерь

Желаю надежный VPN с максимальной надежностью и практически без потерь

Предполагаемые решения

- Дублирование пакетов по всем каналам
- Forward Error Correction (как на спутниковых каналах). FEC 3/4 - посылаем 3 полезных пакета + 1 контрольный

FEC over IP запатентован =(
Номер патентной публикации WO2013098810A1

VPN что ещё ?

Проприетарные решения

- VipNet
- CheckPoint VPN
- Hamachi

Новые opensource решения

- SoftEther - все в одном “флаконе”

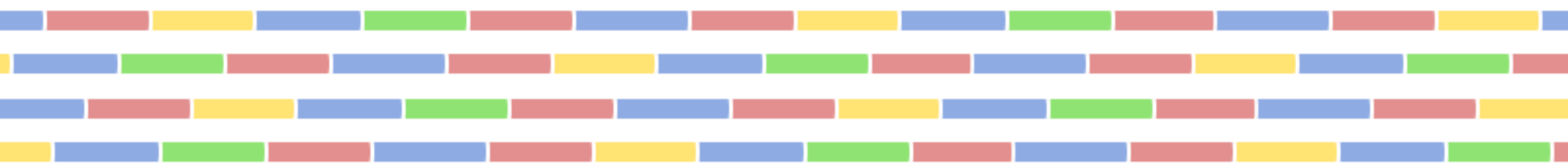
Малоизвестные opensource проекты

peervpn, tinc, campagnol, GVPE, Neorouter, Cloudvpn, N2N

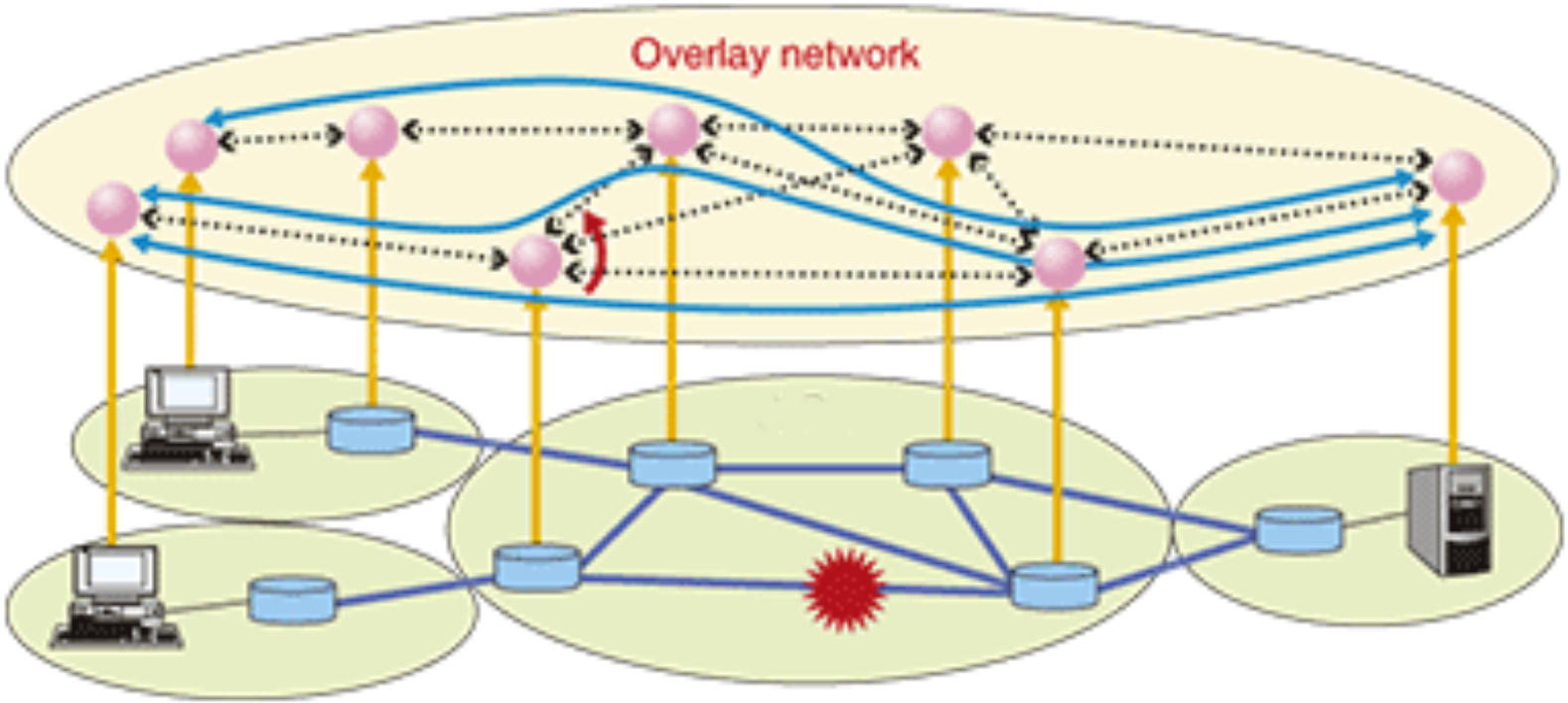
Экзотика

Туннель over ICMP, туннель over DNS

Overlay Networks



Overlay Networks



Overlay Network — общий случай логической сети, создаваемой поверх другой сети

Узлы сети связаны “логическими” соединенями

Сети на виртуалках

Сетевые желания ЦОД

- Настраивать сети / vlan-ы для вируалок так же легко как и создание самих виртуалок
- Убрать vlan-ы виртуалок с реального оборудования

Решение

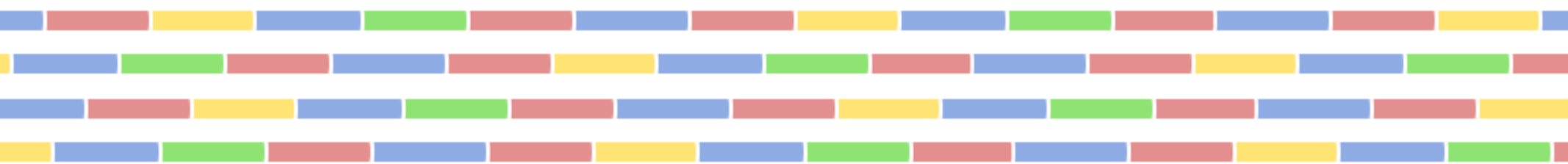
Оверлейная сеть!

Реальное оборудование - транспорт для оверлейной сети

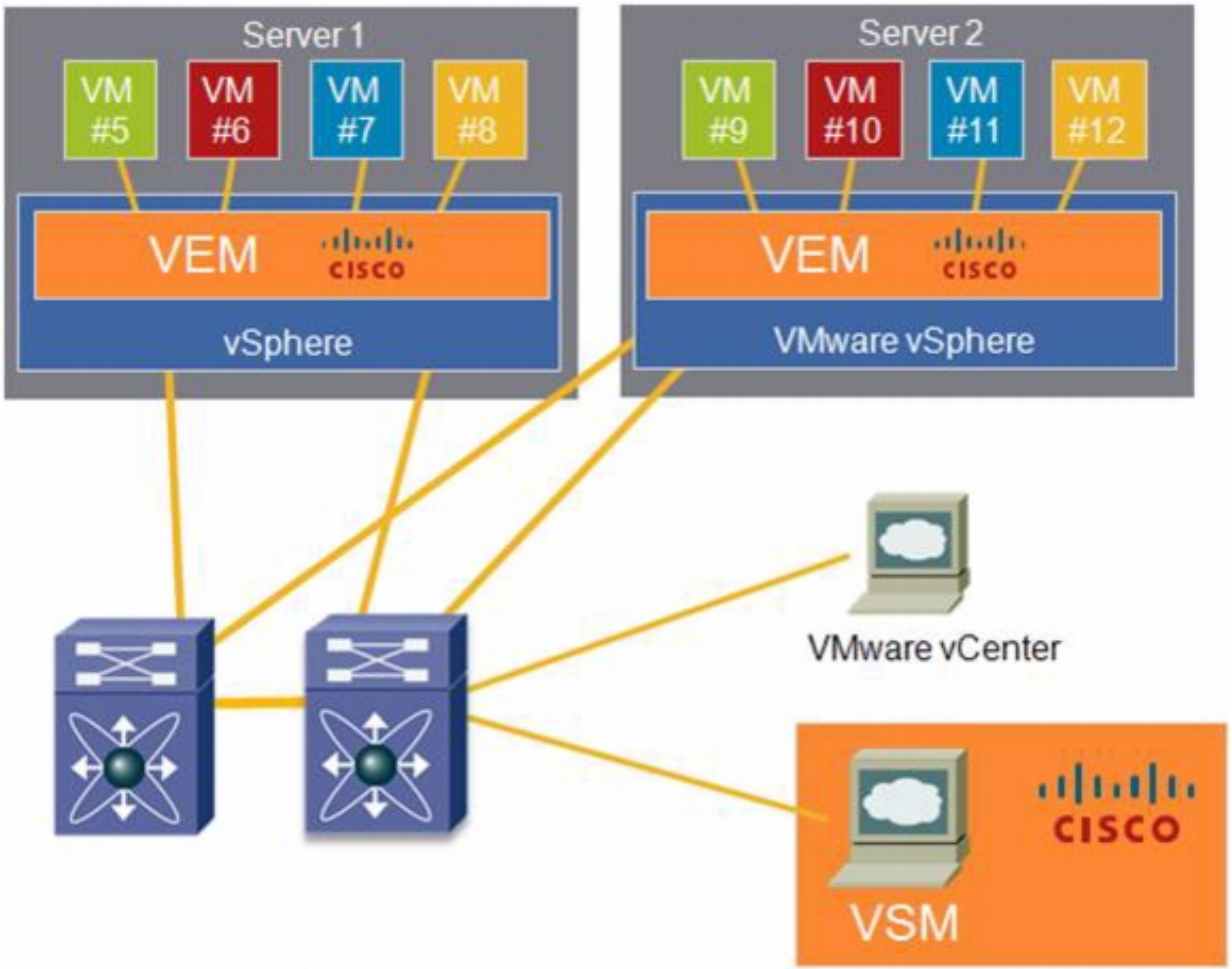
Общее название - distributed virtual switch

Overlay Networks

Cisco Nexus 1000v



Cisco Nexus 1000v

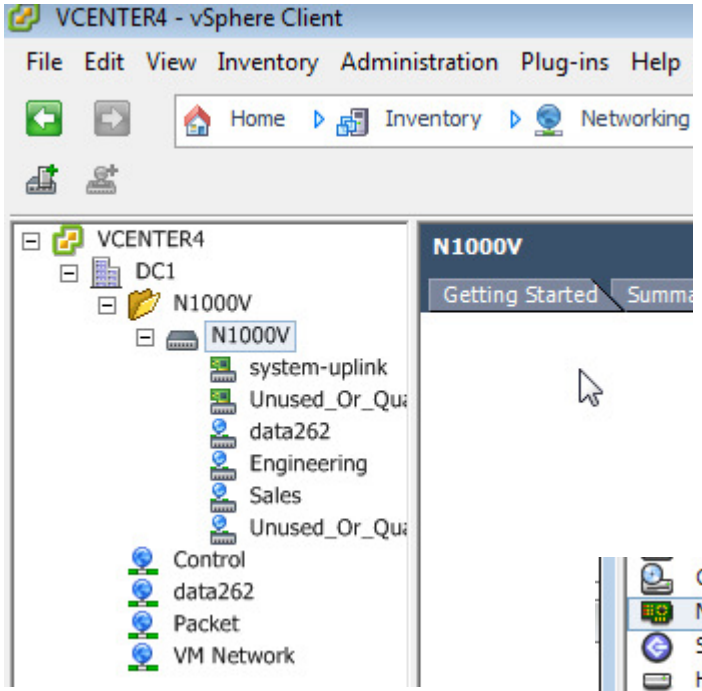


VEM
Virtual Ethernet Module (компонент/модуль для ОС хоста)

VSM
Virtual Supervisor Module (виртуальная машина - оркестратор/контроллен для VEM. до 64 шт)

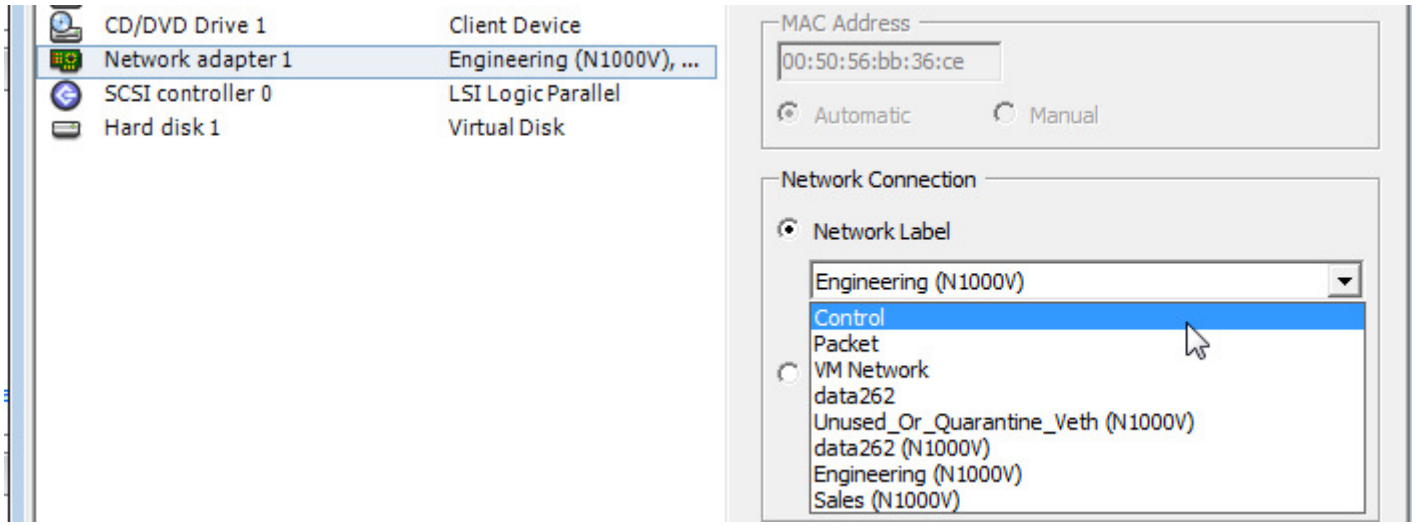
Cisco Nexus 1000v - набор программного обеспечения для VMware vSphere

Cisco Nexus 1000v



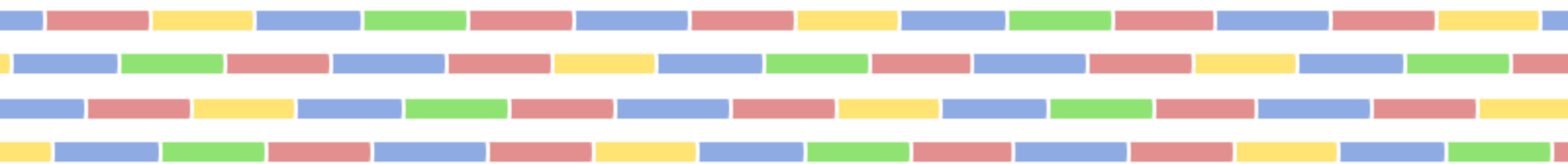
В закладке сеть появляется виртуальный коммутатор (один на весь кластер vSphere)

В настройках виртуалки можно выбрать сети с виртуального коммутатора



Overlay Networks

VXLAN



VXLAN

VXLAN — логическая L2 сеть поверх существующей L3

Разработка Cisco + VMware.

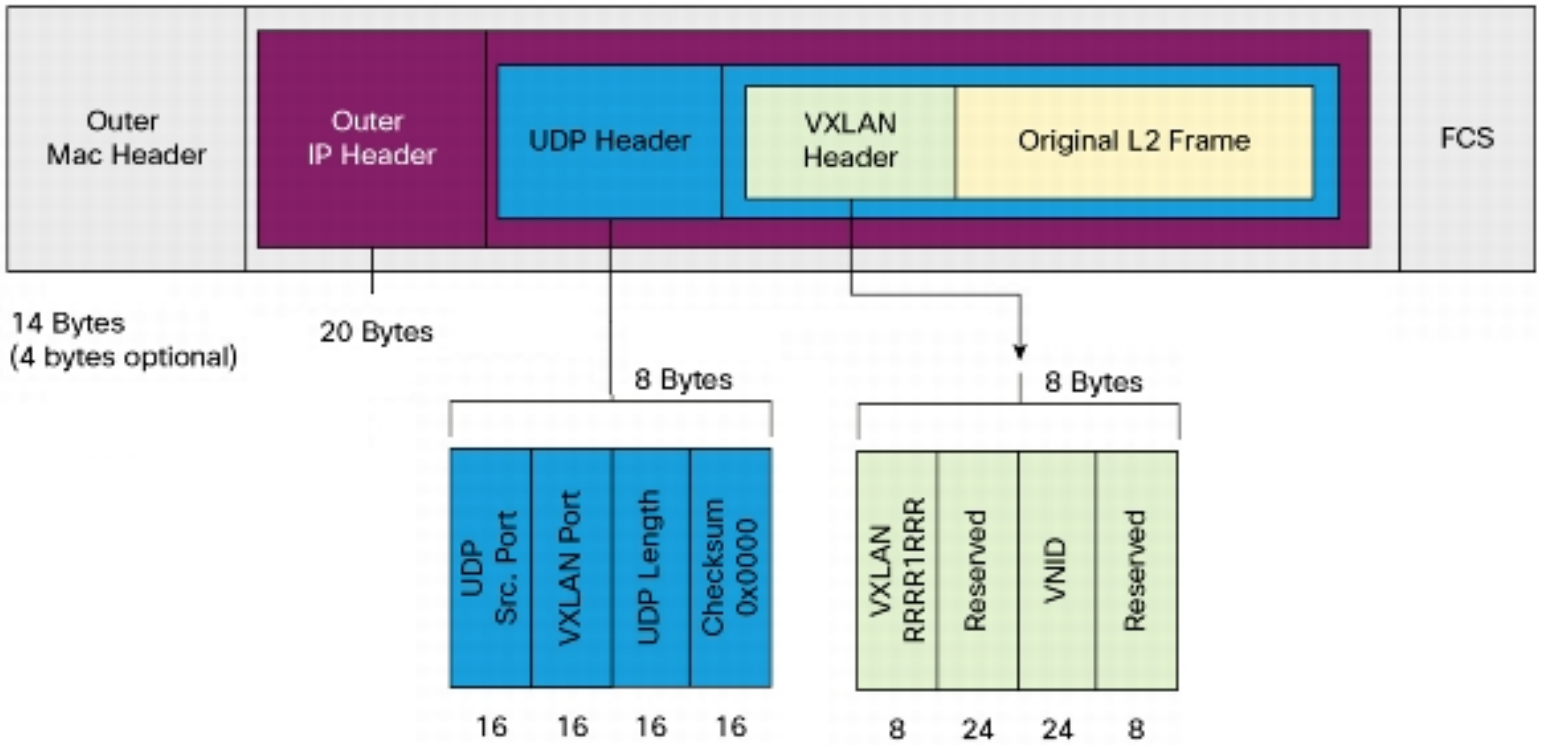
Инфраструктура VXLAN:

- Multicast, IGMP и PIM
- Идентификатор VNI внутри IP-пакета
- Компонент VXLAN Tunnel End Point (VTEP) на стороне сервера виртуализации

Идентификатор интерфейса виртуалки - VNI + MAC.

VNI - 24 бита или 16 000 000 штук

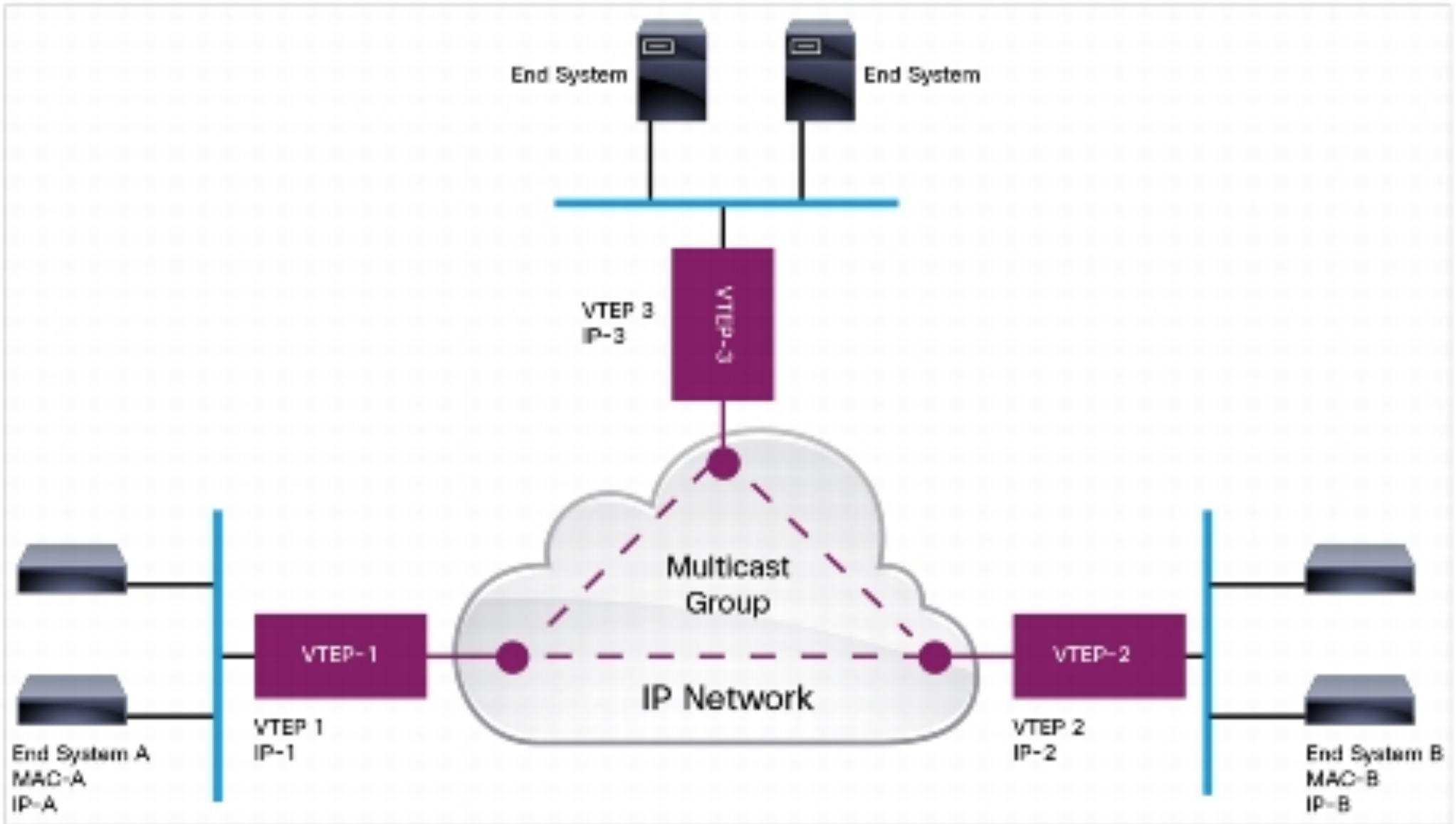
VXLAN



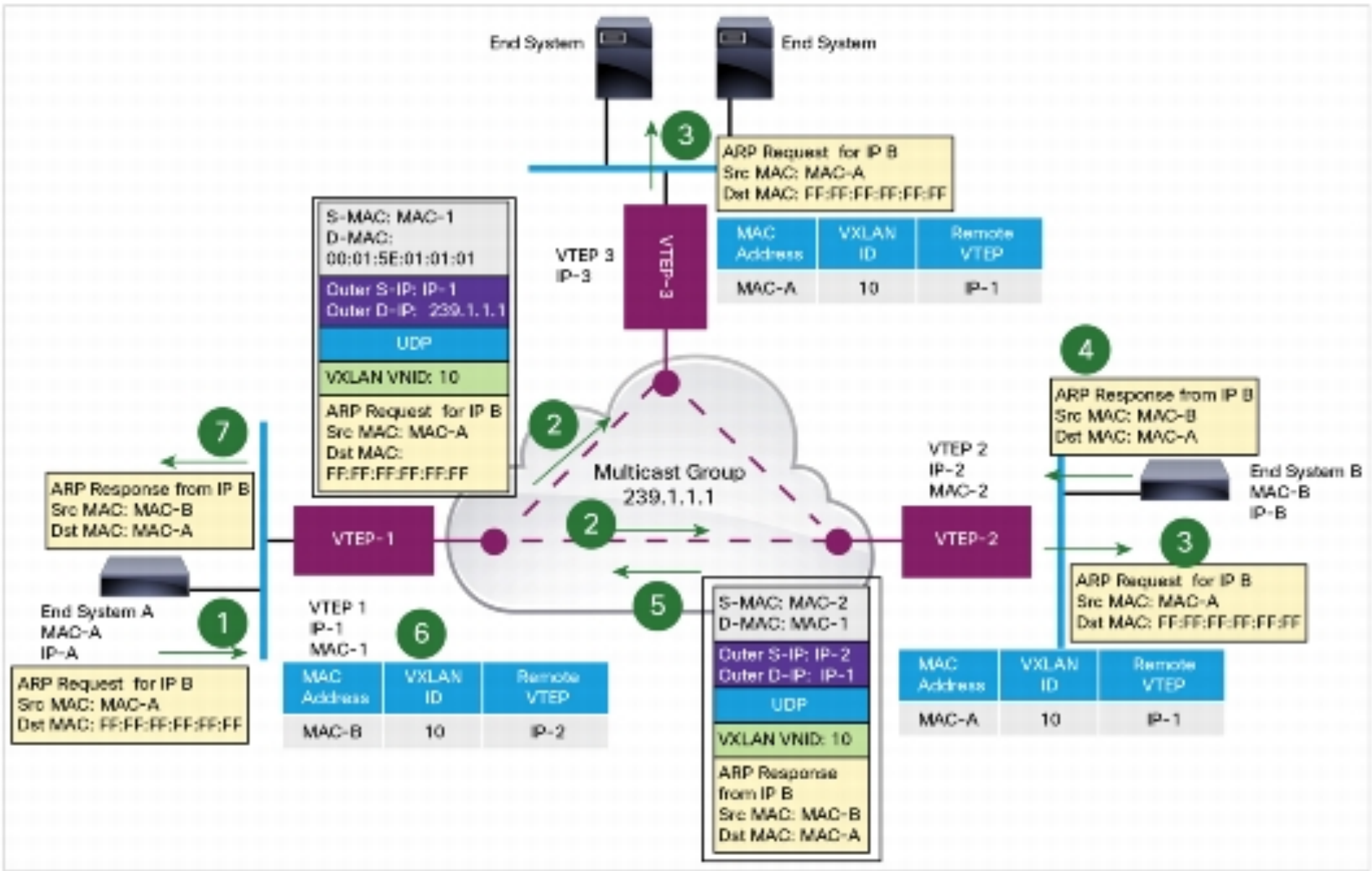
К оригинальному Ethernet фрейму добавляется
14 (Ethernet) + 20 (IP) + 8 (UDP) + 8 (VXLAN) = 50 байт

Для работы VXLAN

VXLAN

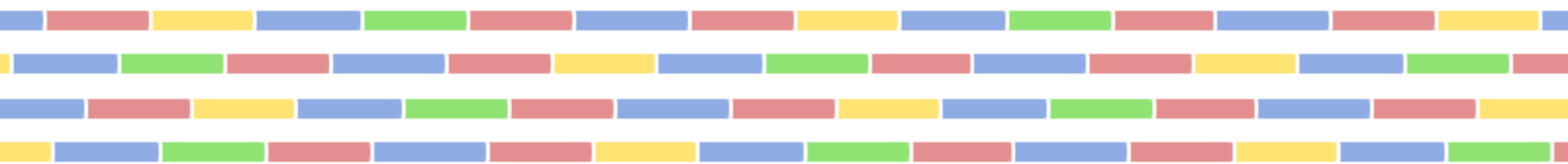

End System
End System
VTEP 3
IP-3
VTEP-3
Multicast
Group
IP Network
VTEP-1
VTEP-2
VTEP 1
IP-1
VTEP 2
IP-2
End System A
MAC-A
IP-A
End System B
MAC-B
IP-B

VXLAN

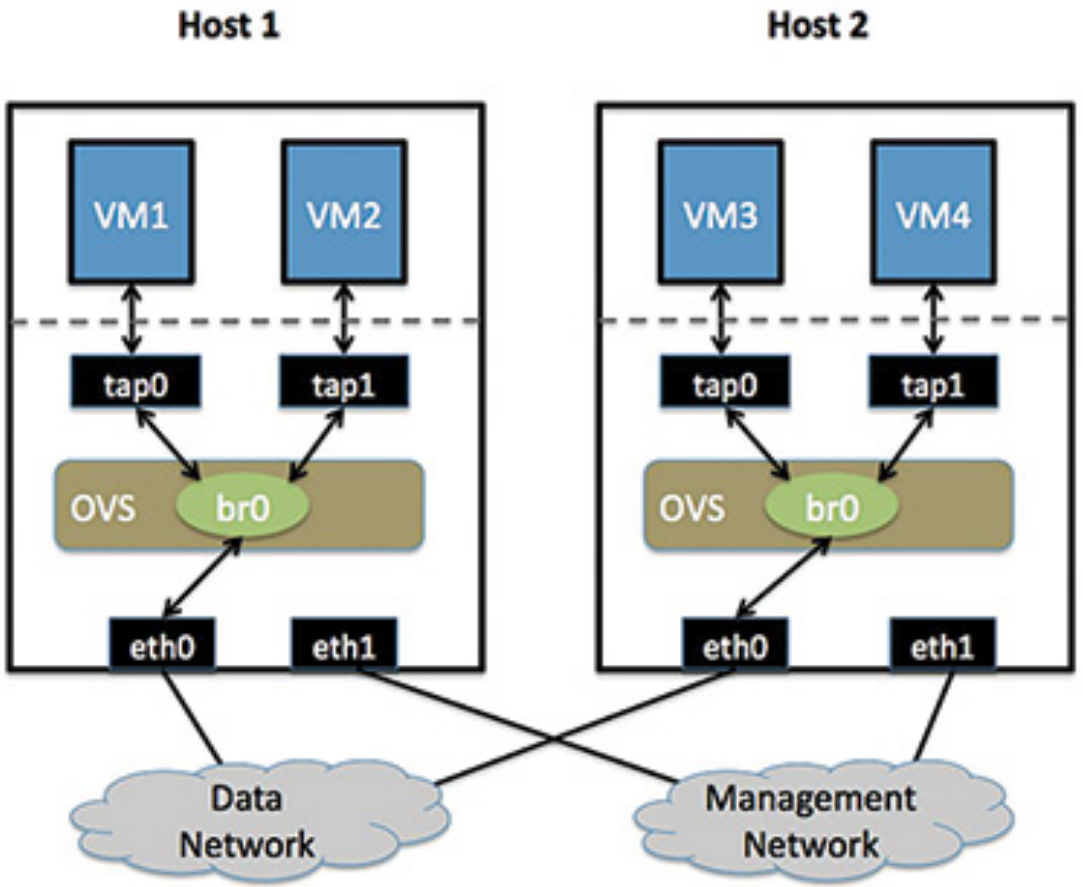

End System
End System
3
ARP Request for IP B
Src MAC: MAC-A
Dst MAC: FF:FF:FF:FF:FF:FF
MAC Address
VXLAN ID
Remote VTEP
MAC-A
10
IP-1
S-MAC: MAC-1
D-MAC: 00:01:5E:01:01:01
Outer S-IP: IP-1
Outer D-IP: 239.1.1.1
UDP
VXLAN VNID: 10
ARP Request for IP B
Src MAC: MAC-A
Dst MAC: FF:FF:FF:FF:FF:FF
VTEP 3
IP-3
VTEP-3
4
ARP Response from IP B
Src MAC: MAC-B
Dst MAC: MAC-A
End System B
MAC-B
IP-B
VTEP 2
IP-2
MAC-2
2
Multicast Group
239.1.1.1
2
7
ARP Response from IP B
Src MAC: MAC-B
Dst MAC: MAC-A
VTEP-1
VTEP-2
3
ARP Request for IP B
Src MAC: MAC-A
Dst MAC: FF:FF:FF:FF:FF:FF
End System A
MAC-A
IP-A
1
5
S-MAC: MAC-2
D-MAC: MAC-1
Outer S-IP: IP-2
Outer D-IP: IP-1
UDP
VXLAN VNID: 10
ARP Response from IP B
Src MAC: MAC-B
Dst MAC: MAC-A
VTEP 1
IP-1
MAC-1
6
MAC Address
VXLAN ID
Remote VTEP
MAC-B
10
IP-2
MAC Address
VXLAN ID
Remote VTEP
MAC-A
10
IP-1
ARP Request for IP B
Src MAC: MAC-A
Dst MAC: FF:FF:FF:FF:FF:FF

Overlay Networks

Open vSwitch



Open vSwitch



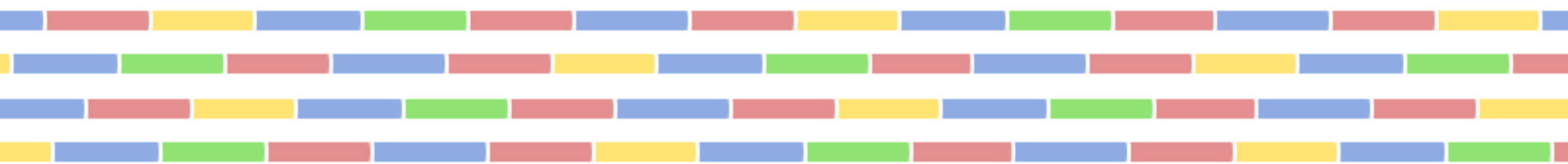
Overlay networks over

- GRE
- VXLAN
- IPsec

Open vSwitch (OVS) - открытое ПО для автоматизации сети виртуалок.

SDN

Software-defined Network



SDN

SDN - программно-определяемая сеть

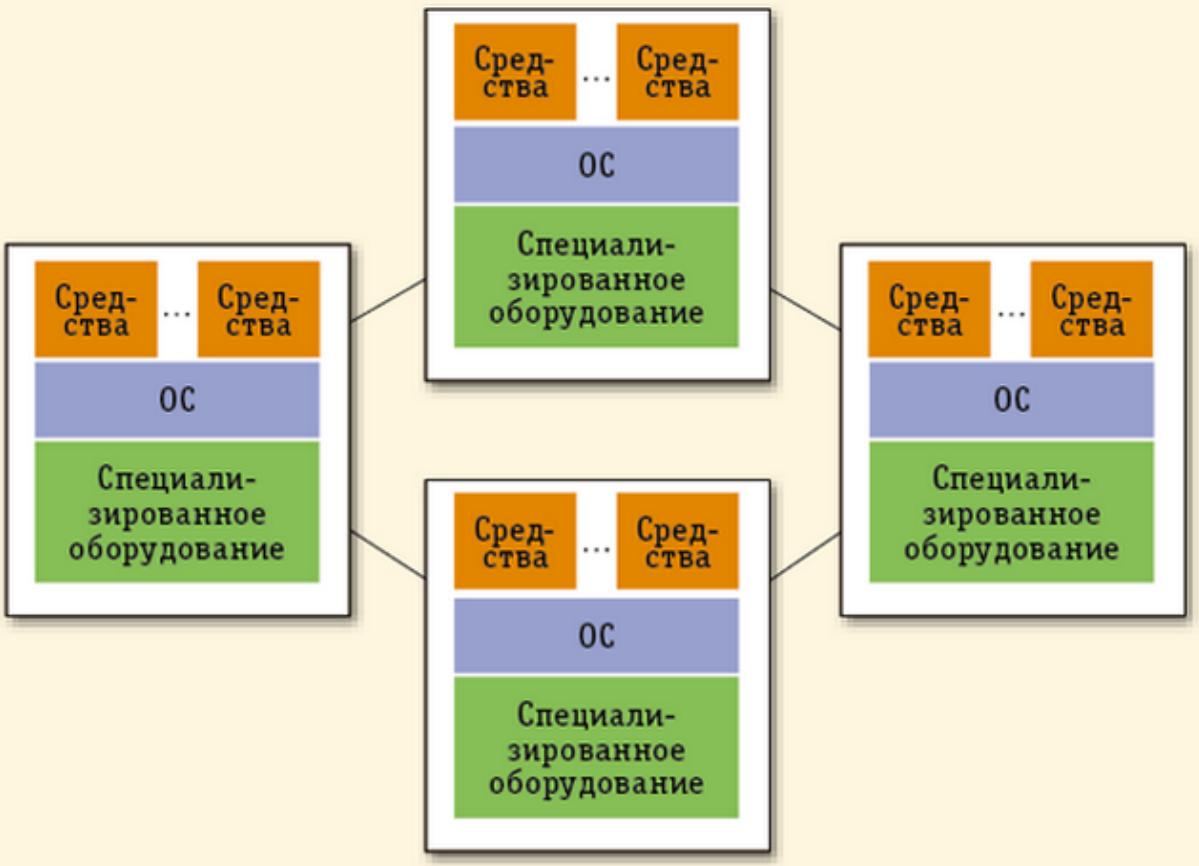
Идеи / принципы SDN

- разделение процессов передачи и управления данными
- перейти от настройки экземпляров сетевого оборудования к управлению сетью
- забыть про ACL, STP, SNMP, OSPF и т.д., просто управлять потоками трафика

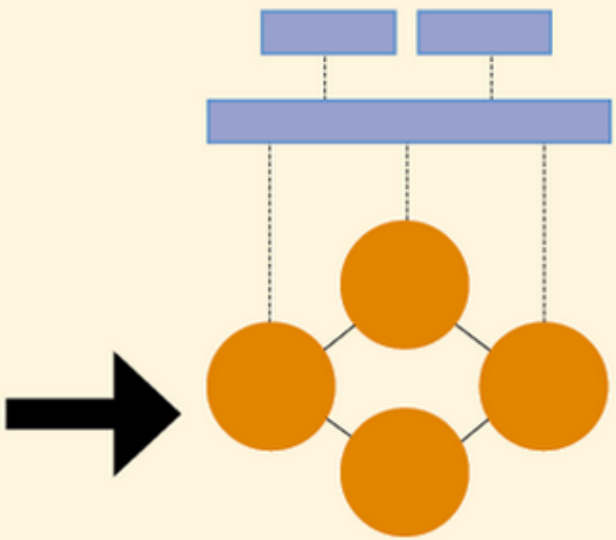
Состоит

- Коммутаторы OpenFlow
- Контроллер SDN

SDN



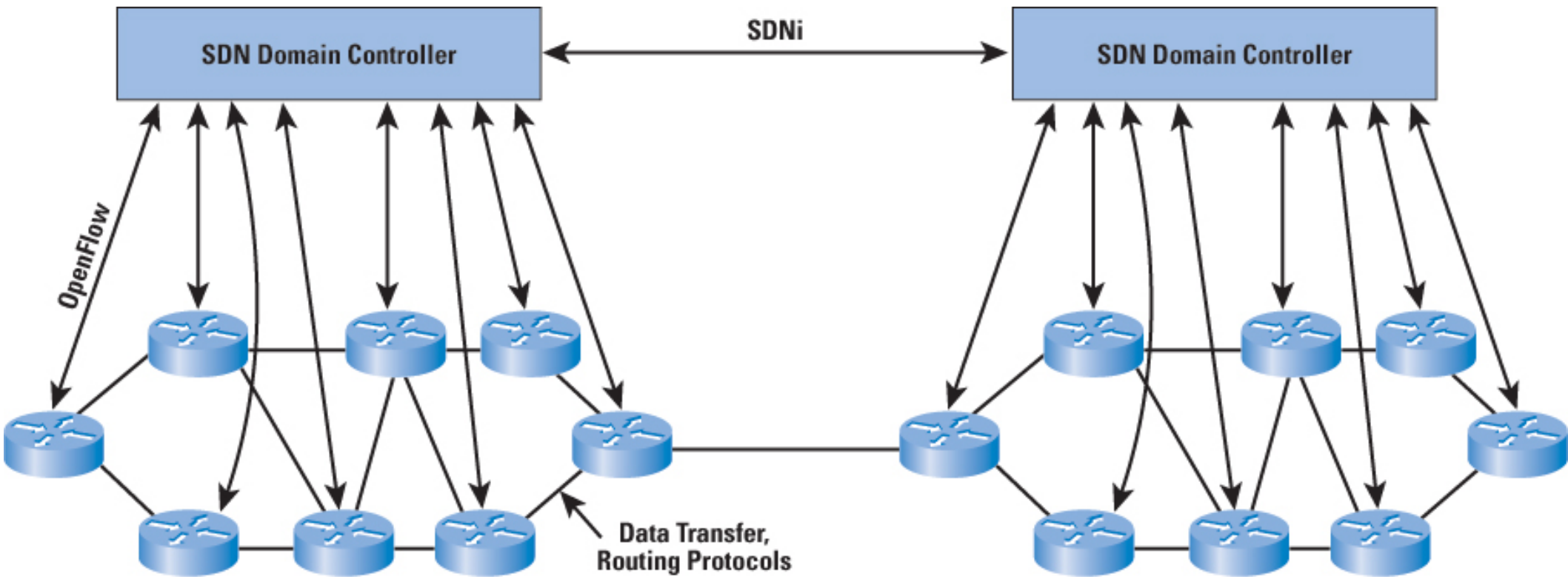
Сеть вертикально интегрированных, закрытых, проприетарных коммутаторов



OpenFlow/SDN:

- разделение процессов передачи и управления данными;
- единый, унифицированный, независящий от поставщика интерфейс между уровнем управления и уровнем передачи данных;
- логически централизованное управление сетью, осуществляемое с помощью контроллера с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями;
- виртуализация физических ресурсов сети.

SDN


SDN Domain Controller
SDNi
SDN Domain Controller
OpenFlow
Data Transfer,
Routing Protocols

SDN. Алгоритм работы коммутатора OpenFlow

Коммутатор связан с контроллером SDN (протокол OpenFlow)

Коммутатор имеет таблицу потоков (flow tables)

Приходящий поток пакетов/фреймов коммутатор проверяет по flow tables и применяет действие

Не опознанный пакет/фрейм отправляется на контроллер для принятия решения. Контроллер возвращает новое правило, которое запоминается во flow table.

SDN. Flow Tables

MAC SRC	MAC DST	SRC IP	IP DST	TCP Dport	TCP SPort	Action	Count
*	00:02:.	*	*	*		Port1	250
*	*	*	10.2.2.1	80	*	Port 3	320
*	*	192.*	*	*	*	drop	890
*	*	192.*	*	*	*	local	100
*	*	*	*	*	*	Controller	11

SDN. Flow Tables. L3 Routing

- **Flows has destination IP subnets only**

MAC SRC	MAC DST	SRC IP	IP DST	TCP Dport	TCP SPort	Action	Count
*	*	*	10.1.1.0/24	*	*	Port1	250
*	*	*	10.1.2.0/24	*	*	Port 2	320
*	*	*	*	*	*	Port 3	890

Destination Routing

Routing Port 2

Default Route

SDN. Flow Tables. L2 Switching

- **Gather MAC addresses in network**
- **Set flows with wildcards but for destination MAC address.**

MAC SRC	MAC DST	SRC IP	IP DST	TCP Dport	TCP SPort	Action	Count
*	0000.dead.beef	*	*	*	*	Port1	250
*	0000.cafe.beda	*	*	*	*	Port 2	320
*	*	*	*	*	*	Controller	320

SDN контроллер

Например Floodlight - Open source SDN Controller

Compatible Virtual Switches

- Open vSwitch (OVS)

Compatible Hardware Switches

- Arista 7050
- Brocade MLXe, Brocade CER, Brocade CES
- Dell S4810, Dell Z9000
- Extreme Summit x440, x460, x670
- HP 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl (the old-style L3)
- HP V2 line cards in the 5400zl and 8200zl (the newer L2 hardware match platform)
- Huawei openflow-capable router platforms
- IBM 8264
- Juniper (MX, EX)
- NEC IP8800,NEC PF5240

Ссылки

ERROR CORRECTION (FEC)
https://www.silver-peak.com/sites/default/files/infoctr/silver-peak_wp_fec.pdf
FEC патент
https://www.google.com/patents/WO2013098810A1
FEC патент картинка
http://patentscope.wipo.int/search/docservice_fpimage/WOIL2012000402@@@false@@@en
Transparent Error Correction for Lambda Networks
http://www.cs.cornell.edu/~mahesh/publications/docs/maelstromnsdi.pdf
VPN
http://ru.wikipedia.org/wiki/VPN
Коротко и ясно: Flex VPN
http://habrahabr.ru/post/160555/
Программная маршрутизация: история переезда с hub-n-spoke (vyatta+openvpn) на fullmesh (mikrotik+tincvpn)
http://habrahabr.ru/post/185624/
RFC 1661. The Point-to-Point Protocol (PPP)
http://tools.ietf.org/html/rfc1661
VPN over SSH
https://wiki.archlinux.org/index.php/VPN_over_SSH
PPTP
http://en.wikipedia.org/wiki/PPTP
Point-to-Point Tunneling Protocol (PPTP)
http://tools.ietf.org/html/rfc2637
SoftEther
http://habrahabr.ru/post/208782/
SoftEther
http://www.softether.org/
Картинка с GRE
http://twistedminds.ru/2012/08/tunnels/
Картинка с PPTP, L2TP
http://technet.microsoft.com/en-us/library/cc771298(v=ws.10).asp

IPSec ESP Header size
http://www.tcpipguide.com/free/t_IPSecEncapsulatingSecurityPayloadESP-4.htm
IPSec ESP Overhead
https://www.hamwan.org/t/tiki-index.php?page=IPsec
Картинка с PPPoE
http://www.infraexpert.com/info/5adsl.htm
Как устроен VPN через SSTP
http://habrahabr.ru/post/196134/
IPSec
http://www.isadocs.ru/articles/How-to-pass-IPSec-traffic-through-ISA-Server.html
IKEv2 FlexVPN
http://habrahabr.ru/post/186126/
OpenVPN Protocol Packet Format
http://openvpn.net/index.php/open-source/documentation/security-overview.html
OPenVPN Wireshark
http://wiki.wireshark.org/OpenVPN
OPenVPN
http://www.itrefers.com/OpenVPN/packetformat.php
DMVPN
http://www.anticisco.ru/blogs/2011/07/dmvpn-dynamic-multipoint-vpn-%D1%87%D0%B0%D1%81%D1%82%D1%8C-1/
IPsec Накладые расходы картинка
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/TNS_x_BB_whitepaper.html
DMVPN
http://xgu.ru/wiki/%D0%9D%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_DMVPN_%D0%BD%D0%B0_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80%D0%B0%D1%85_Cisco
Картинка DMVPN
http://certcollection.org/forum/topic/157871-advanced-concepts-of-dmvpn-cisco-live-2009/

Ссылки

Картинка Overlay Network
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200905sf4.html
Темная сторона интернета. Оверлейные сети
http://lex.io/security/temnaya-storona-interneta-overlejnye-seti.html
Distributed Hash Table
http://ru.wikipedia.org/wiki/DHT
Установка Nexus 1000V
http://habrahabr.ru/post/175663/
Картинка Nexus 1000V
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/license/configuration/guide/n1000v_license/license_1overview.html
Floodlight Is an Open SDN Controller
http://www.projectfloodlight.org/floodlight/
Open vSwitch
http://openvswitch.org/
Сколько стоит SDN?
http://habrahabr.ru/post/148745/
SDN
http://www.osp.ru/os/2012/09/13032491/
OpenFlow
http://demo.ipspace.net/get/OpenFlow%20Functions.pdf
OpenFlow Specifications
https://www.opennetworking.org/sdn-resources/onf-specifications/openflow
List of OpenFlow Software Projects (that I know of)
http://yuba.stanford.edu/~casado/of-sw.html

Questions?