

**Dcrypt Smart SFP –
новый способ защиты на
канальном уровне**



Выходцева Елена
Коммерческий директор

О КОМПАНИИ



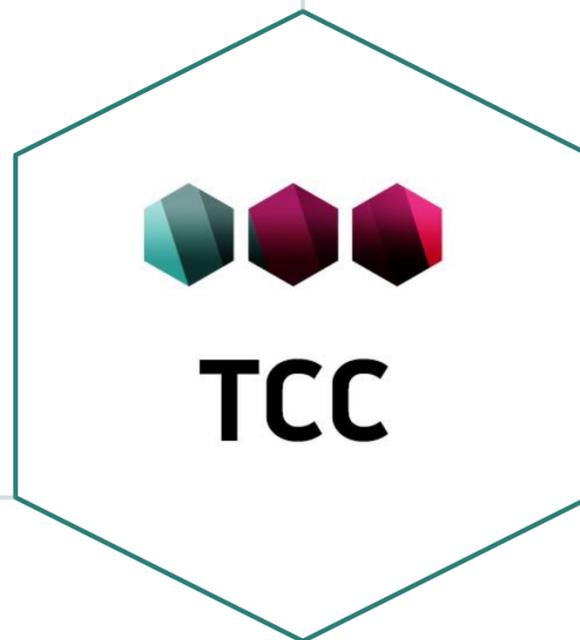
ТСС - РАЗРАБОТЧИК СОВРЕМЕННЫХ
ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ПРОГРАММНЫХ
И АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

- ✓ РАЗВЕТВЛЕННАЯ ПАРТНЕРСКАЯ СЕТЬ
- ✓ РЕЗЕДЕНТ СКОЛКОВО
- ✓ 13+ ЛЕТ НА РЫНКЕ ИБ

НАШИ ЗАКАЗЧИКИ



85% - ГОСУДАРСТВЕННЫЕ КОРПОРАЦИИ И ГОСОРГАНЫ
15% - КРУПНЫЕ И СРЕДНИЕ КОММЕРЧЕСКИЕ СТРУКТУРЫ



ЧТО МЫ ДЕЛАЕМ

ОСНОВНОЙ ПРОФИЛЬ – РАЗРАБОТКА
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ,
СХЕМОТЕХНИЧЕСКИХ И КОНСТРУКТОРСКИХ
РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ



НАШИ РАЗРАБОТКИ

с 2009 года развиваем технологию **Diamond**
с 2017 года развиваем технологию **Dcrypt**
с 2020 года разрабатываем **Diamond NCC**

КЛЮЧЕВЫЕ ЗАКАЗЧИКИ



РОСАТОМ



Банк России



РусГидро



РОСРЕЕСТР

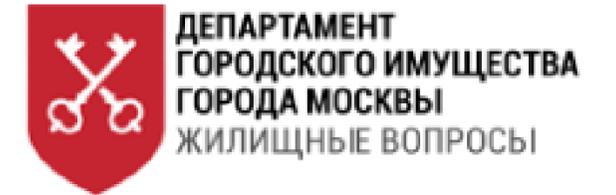
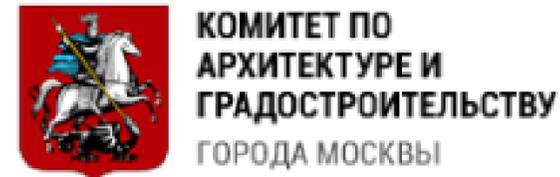
Федеральная служба
государственной регистрации,
кадастра и картографии



МРСК
СЕВЕРНОГО КАВКАЗА



China Construction Bank





ОСНОВНЫЕ ПРОДУКТЫ



№ п/п	Название продукта	Назначение	Целевые функции	Архитектуры процессоров и ОС
1	Система контроля и разграничения доступа в средствах вычислительной техники МКСЗ Diamond ACS	Защита от НСД	Средство вычислительной техники	Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) – Linux
2	Многофункциональный комплекс сетевой защиты Diamond VPN/FW с функциями МЭ, СОВ и СОА	Многофункциональный комплекс сетевой защиты	МЭ, СОВ, СОА	Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) – Linux
3	СКЗИ Dcrypt	Средство криптографической защиты информации	КриптоАРМ, АП VPN, Криптографические библиотеки	Intel – Windows/Linux RISC (ARM, MIPS, RISC-V) – Linux, аппаратные модули расширения

ПАК Diamond VPN/FW: функции



- ПАК Diamond VPN/FW модель 2XXX



- ПАК Diamond VPN/FW модель 3XXX



- ПАК Diamond VPN/FW модель 4XXX



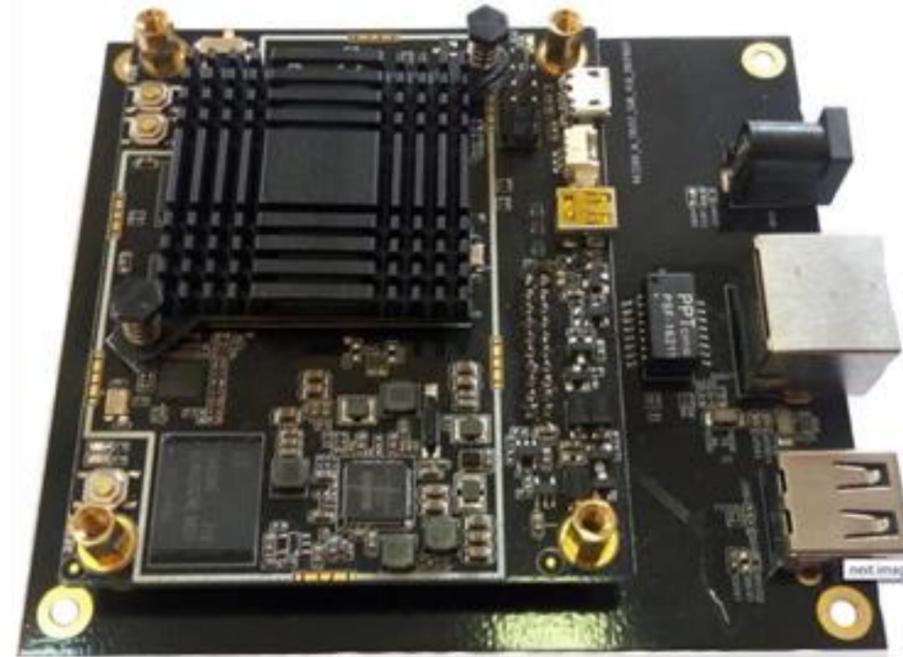
ПАК Diamond VPN/FW модель 5XXX



ПАК Diamond VPN/FW
модель 6XXX/7XXX



ПАК Diamond VPN/FW : для готовых платформ и систем с архитектурой процессора ARM





Dcrypt XG: варианты исполнения аппаратного шифратора



Шасси 3U, 4 модуля / 8 портов по 100 Гбит/с



Шасси 3U, 8 модулей / 16 портов по 100 Гбит/с



Шасси 1U, 1-2 модуля / 2-4 порта по 100 Гбит/с

Предпосылки появления решения SMART SFP

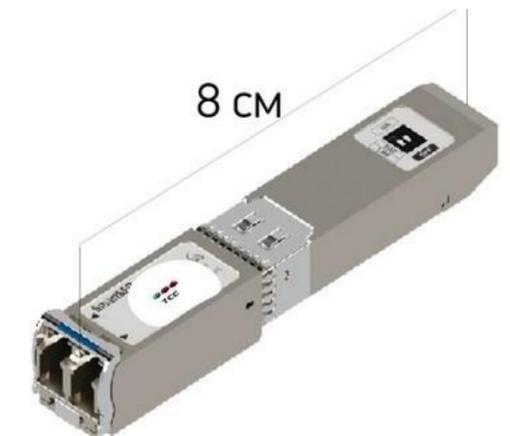
- Есть готовое решение с аппаратной реализацией СКЗИ (Dcrypt XG)
- Есть потребность в закрытии каналов с использованием отечественных алгоритмов
- Нет желания устанавливать дополнительное сетевое оборудование
- Соотношение цены и функционала

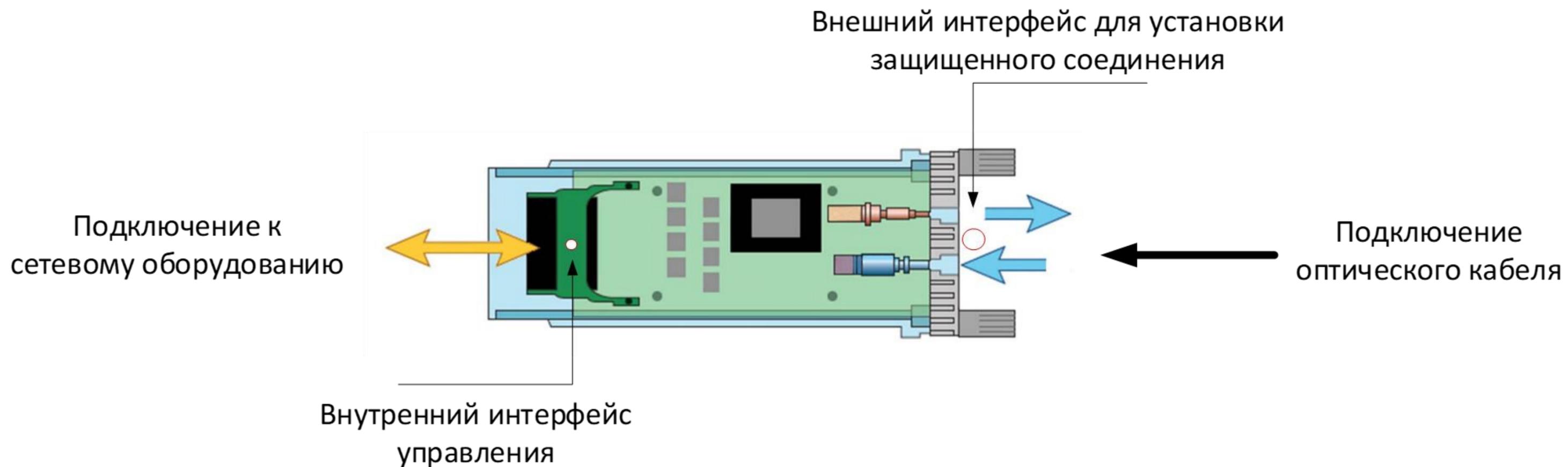


Что такое DCRYPT Smart SFP

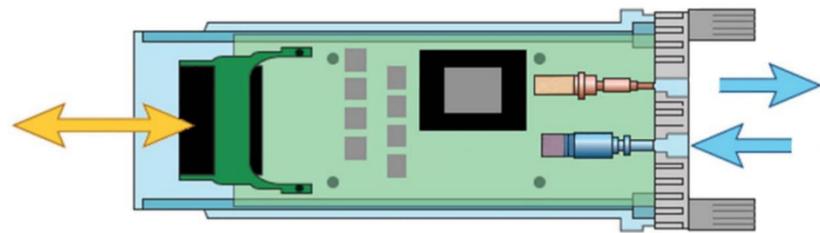


- Средство криптографической защиты информации
- Обеспечение защиты каналов связи на канальном уровне на скоростях до 800 Мбит/с
- СКЗИ класса КСЗ в миниатюрном корпусе
- Решение сертифицированное ФСБ России
- Обеспечение криптографической защиты информации в канале связи без использования дополнительного программного или аппаратного обеспечения. Защита поля MAC-адрес и Ethertype
- Совместимость с оборудованием всех ведущих производителей серверов, маршрутизаторов, коммутаторов и другого сетевого оборудования
- Удобство использования и простота инсталляции

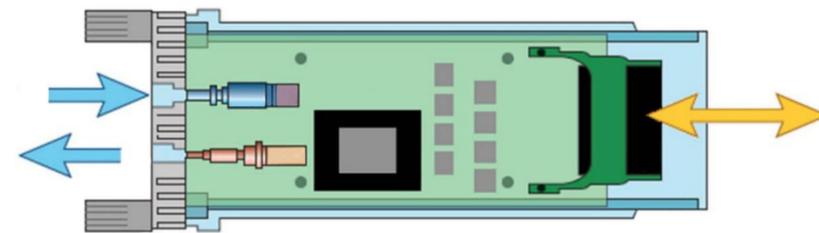




ТЕХНИЧЕСКИЕ ДЕТАЛИ



Темная оптика
L2 связность между трансиверами



Основные преимущества

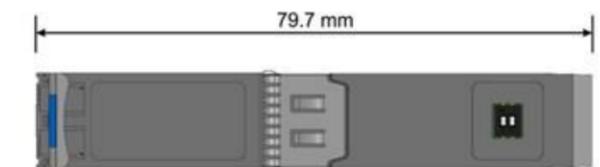
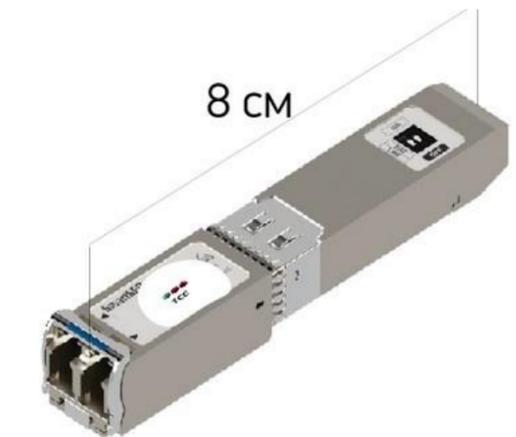


- Высокая производительность и низкие вносимые задержки за счёт аппаратной реализации криптографических алгоритмов. Скоростные характеристики лучше, чем у большинства программно-аппаратных шифровальных средств
- Не требуется дополнительного места в стойке и отдельного питания
- Не требуется дополнительная подготовка сетевой инфраструктуры для внедрения решения
- Позволяет использовать криптографическую защиту информации в канале связи с оборудованием, в составе которого невозможна реализация сертифицированных СКЗИ
- Низкая стоимость владения по сравнению с покупкой дополнительного устройства
- Может быть закуплен как модернизация к существующему оборудованию

Размеры и варианты исполнения



- Gigabit Ethernet, 1000BASE-LX, DDM, 850 нм, 550 м, два многомодовых волокна (2xMMF), LC
- Gigabit Ethernet, 1000BASE-LX, DDM, 1310 нм, 2 км, два многомодовых волокна (2xMMF), LC
- Gigabit Ethernet, 1000BASE-LX, DDM, 1310 нм, 20 км, два одномодовых волокна (2xSMF), LC
- Gigabit Ethernet, 1000BASE-LX, DDM, Tx: 1310 нм, Rx: 1550 нм, 20 км, одно одномодовое волокно (SMF)
- Gigabit Ethernet 1000BASE-LX, DDM, Tx: 1550 нм, Rx: 1310 нм, 20 км, одно одномодовое волокно (SMF)
- Gigabit Ethernet, 10/100/1000BASE-T, RJ-45



Размеры и варианты исполнения

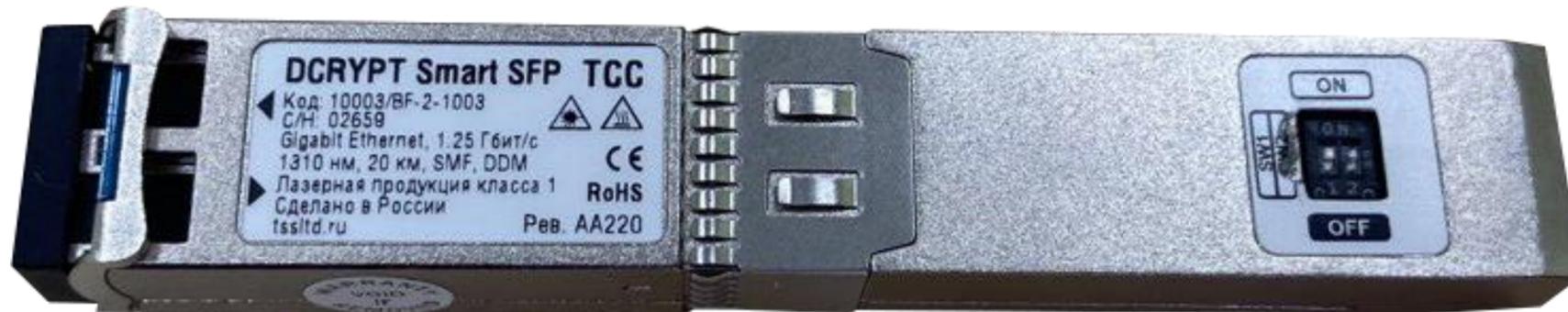


Схема построения защищенной сегмента сети с использованием устройства «DCRYPT Smart SFP». Тип соединения точка-точка.

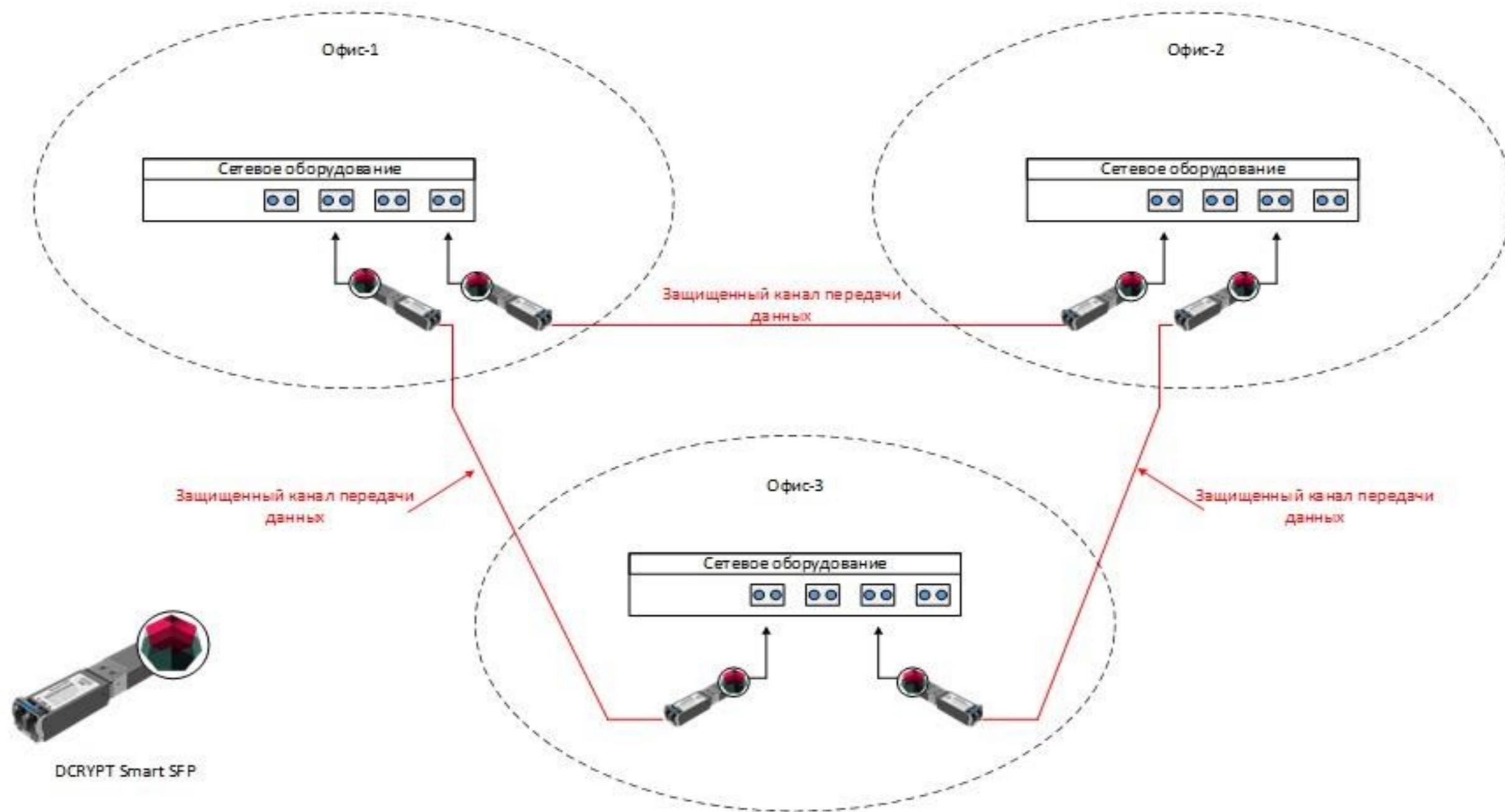
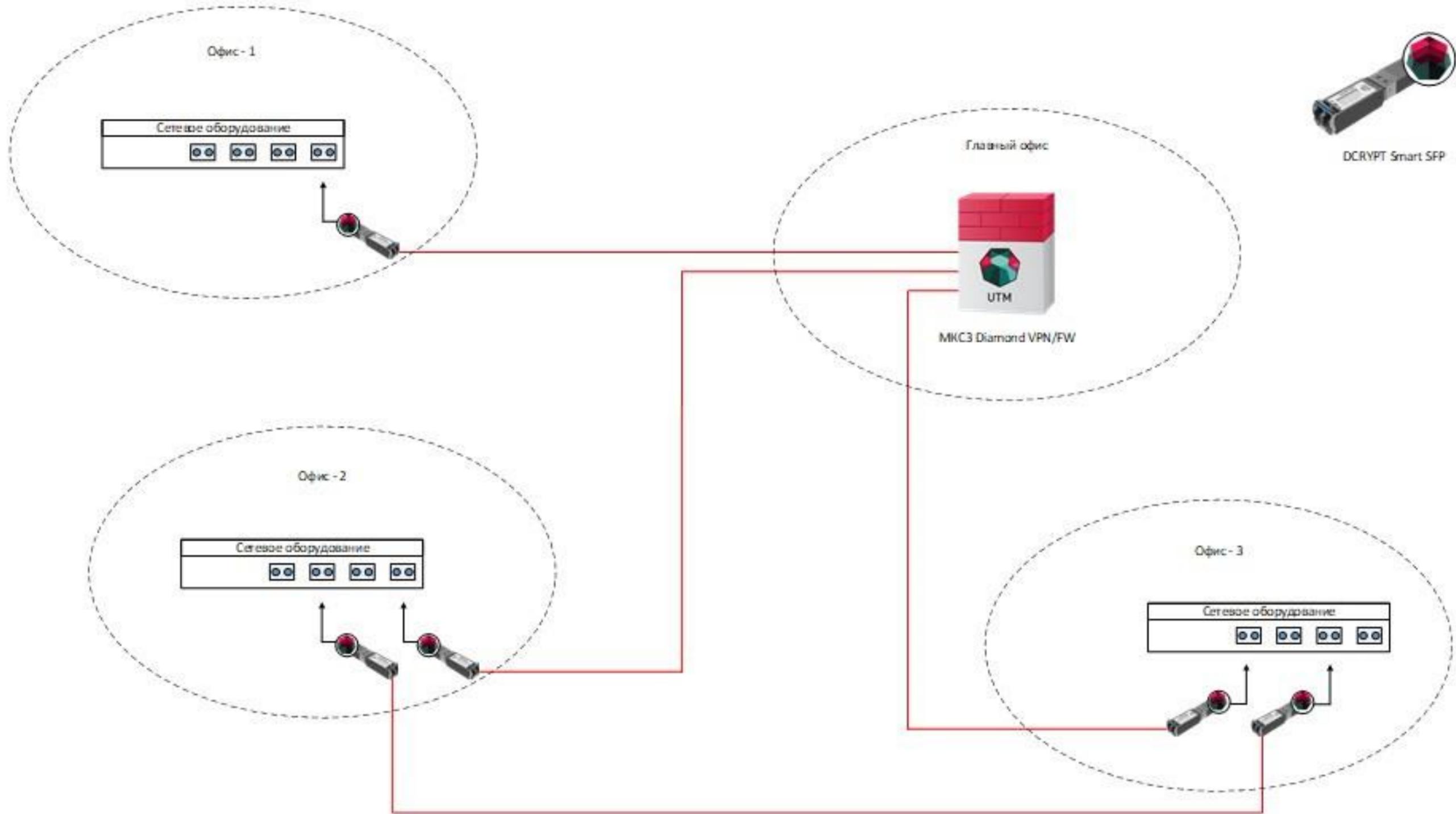


Схема построения защищенной сегмента сети с использованием устройства «DCRYPT Smart SFP». Тип соединения точка-многоточка.



Сроки поставки



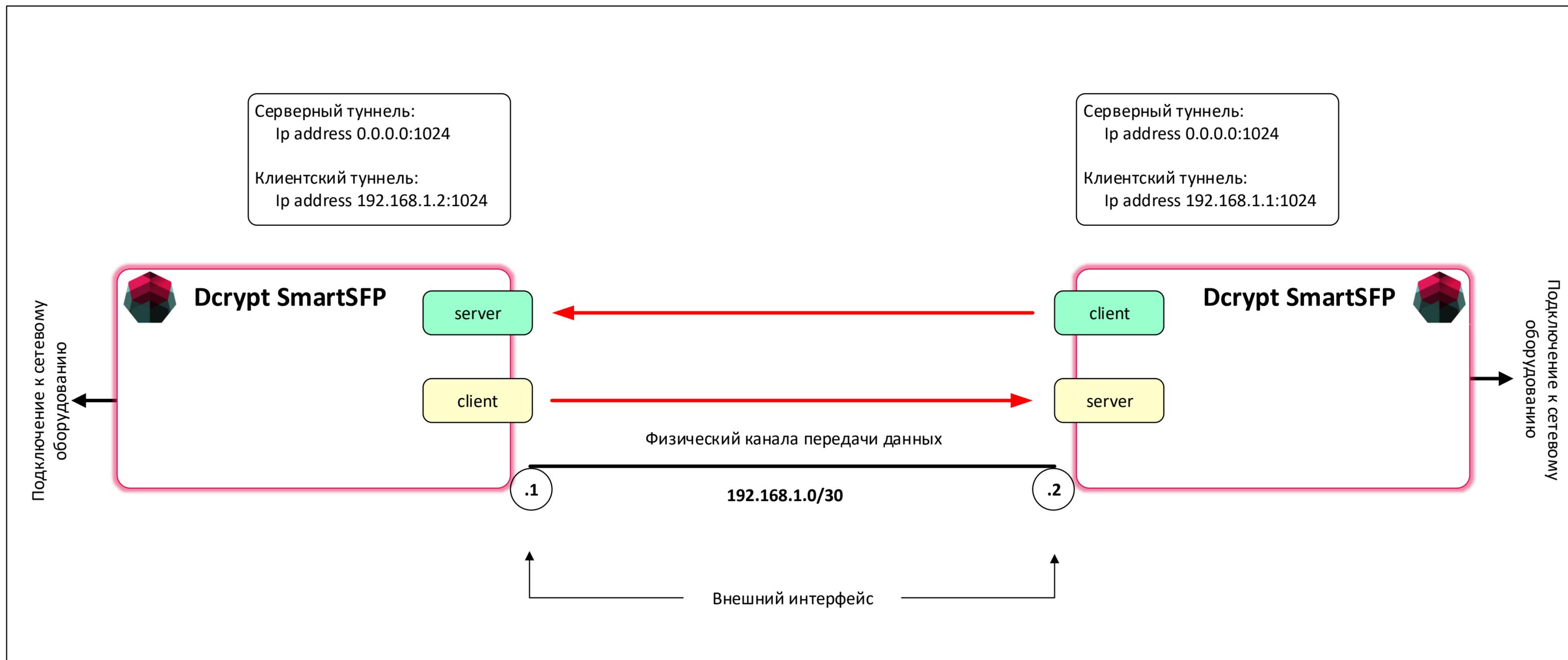
- Gigabit Ethernet, 1000BASE-LX, DDM, 850 нм, 550 м, два многомодовых волокна (2xMMF), LC
- Gigabit Ethernet, 1000BASE-LX, DDM, 1310 нм, 2 км, два многомодовых волокна (2xMMF), LC
- Gigabit Ethernet, 1000BASE-LX, DDM, 1310 нм, 20 км, два одномодовых волокна (2xSMF), LC
- Gigabit Ethernet, 1000BASE-LX, DDM, Tx: 1310 нм, Rx: 1550 нм, 20 км, одно одномодовое волокно (SMF)
- Gigabit Ethernet 1000BASE-LX, DDM, Tx: 1550 нм, Rx: 1310 нм, 20 км, одно одномодовое волокно (SMF)
- Gigabit Ethernet, 10/100/1000BASE-T, RJ-45

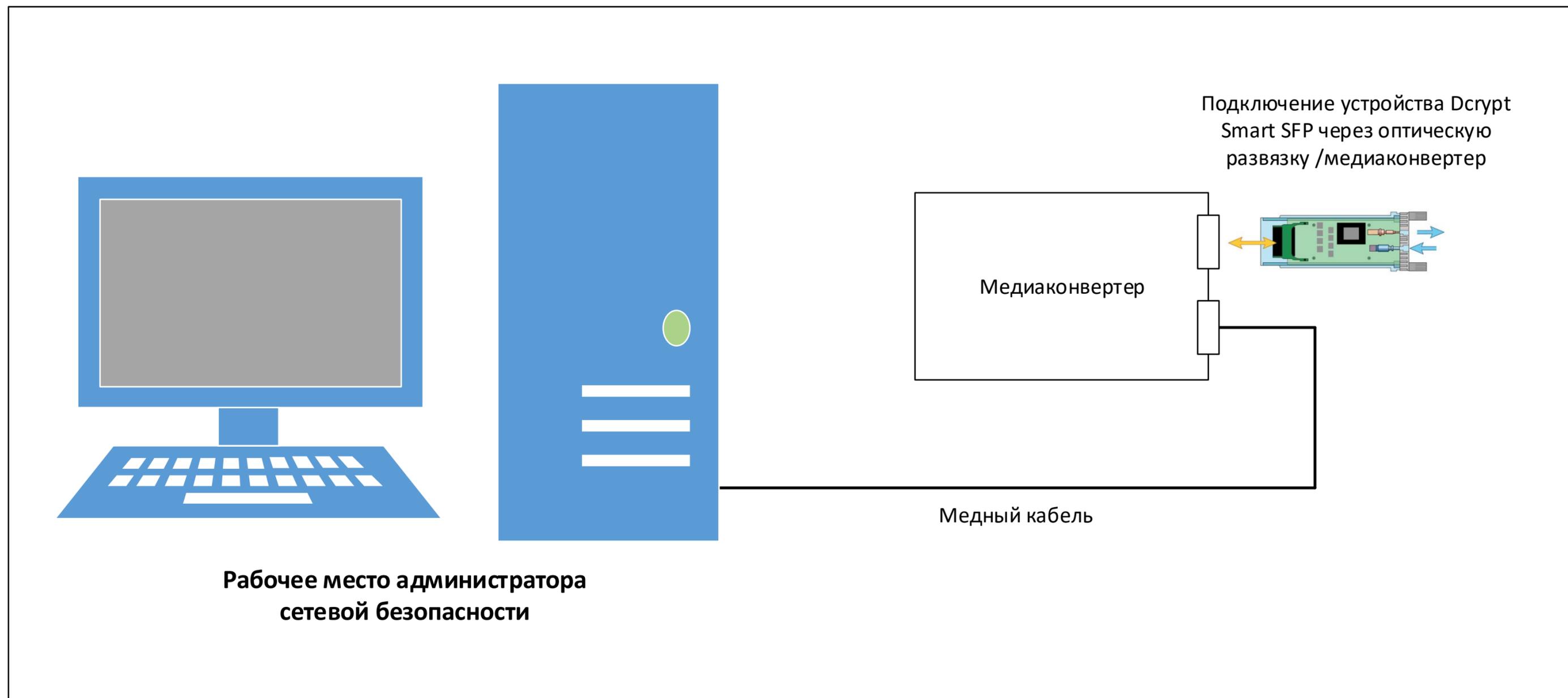
2-3 недели

- Gigabit Ethernet, CWDM, 80 км

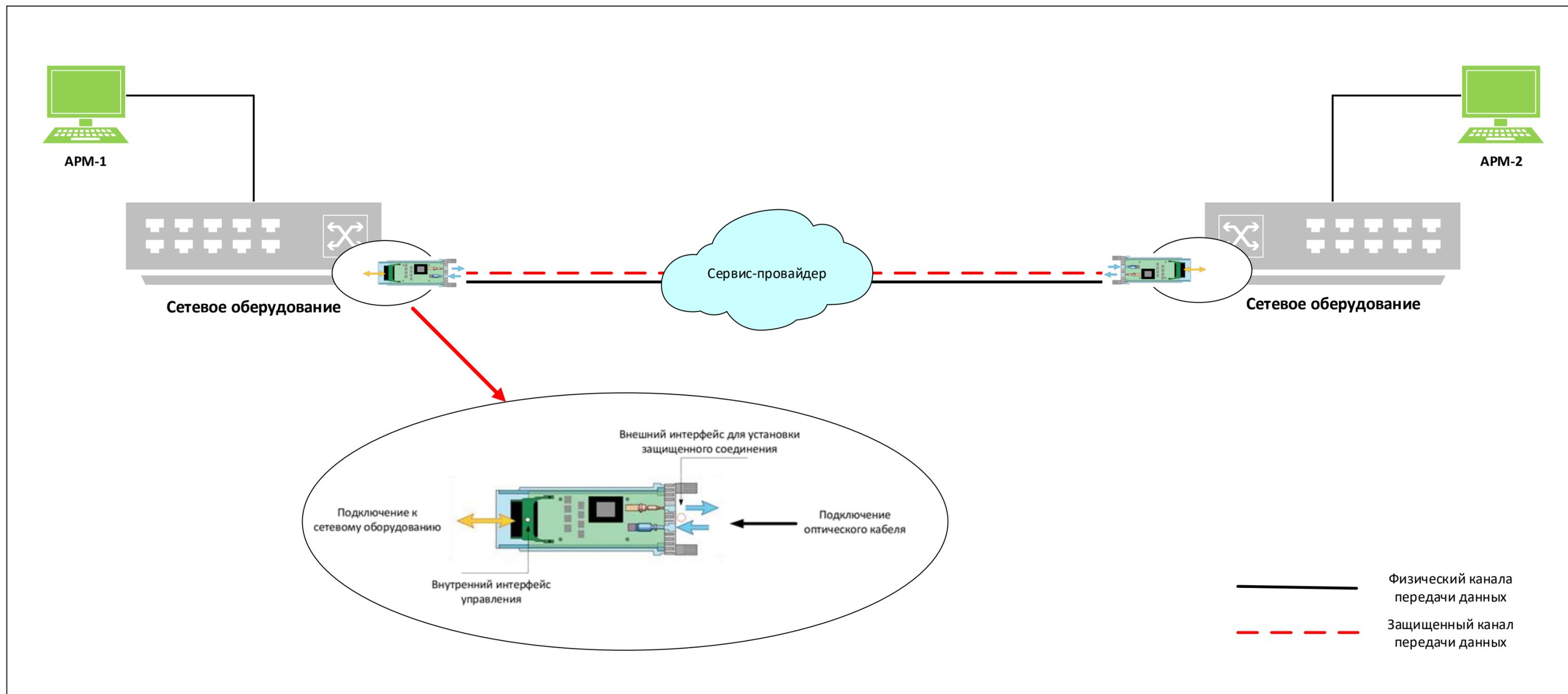
24 недели

УСТАНОВКА ЗАЩИЩЕННОГО СОЕДИНЕНИЯ

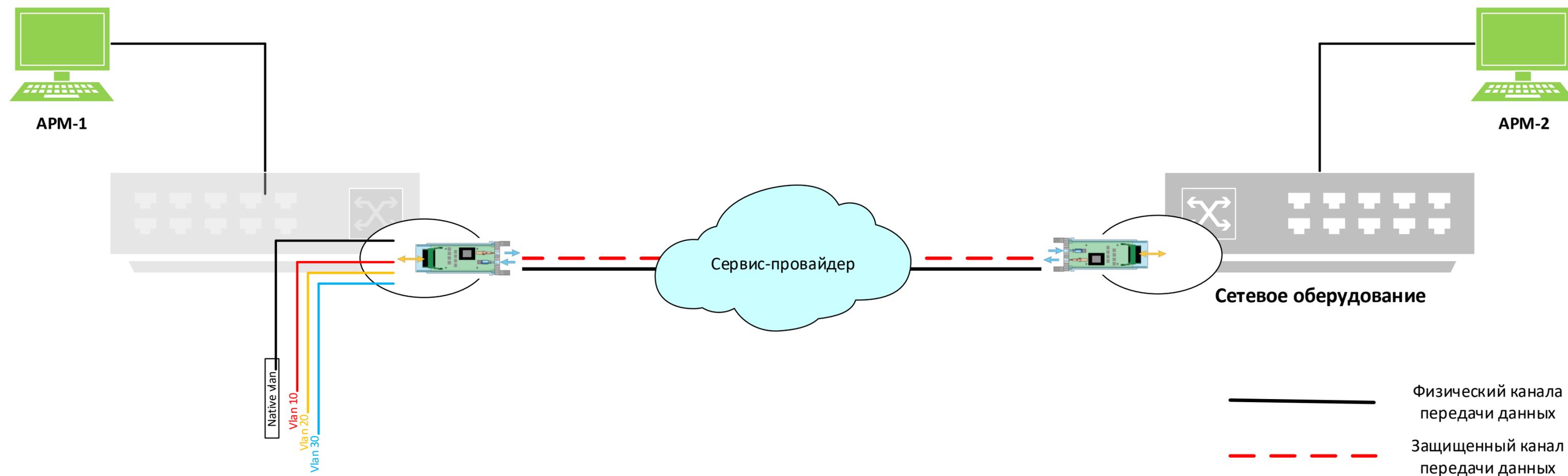


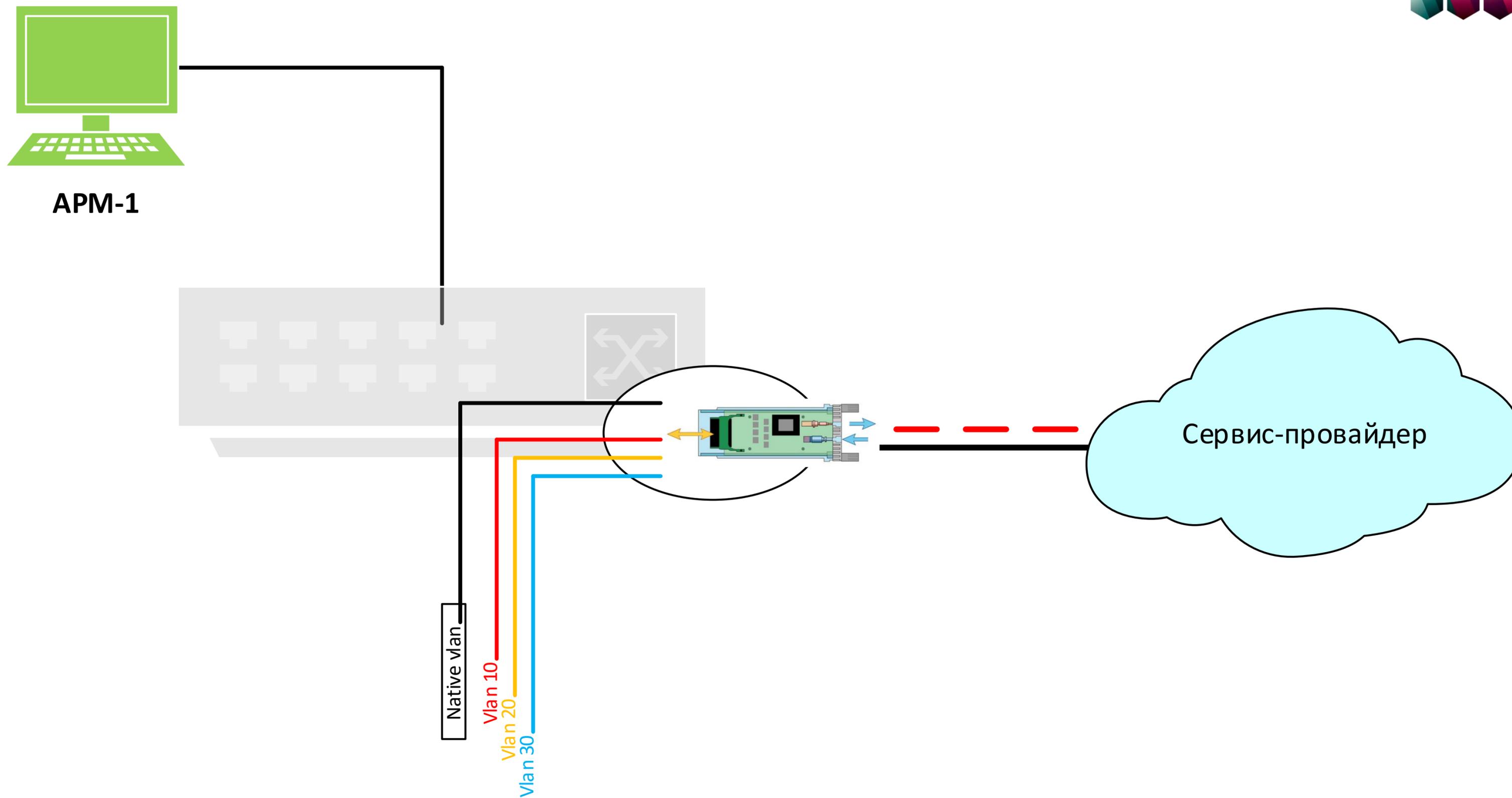


ПЕРЕДАЧА ТРАФИКА ЧЕРЕЗ ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ

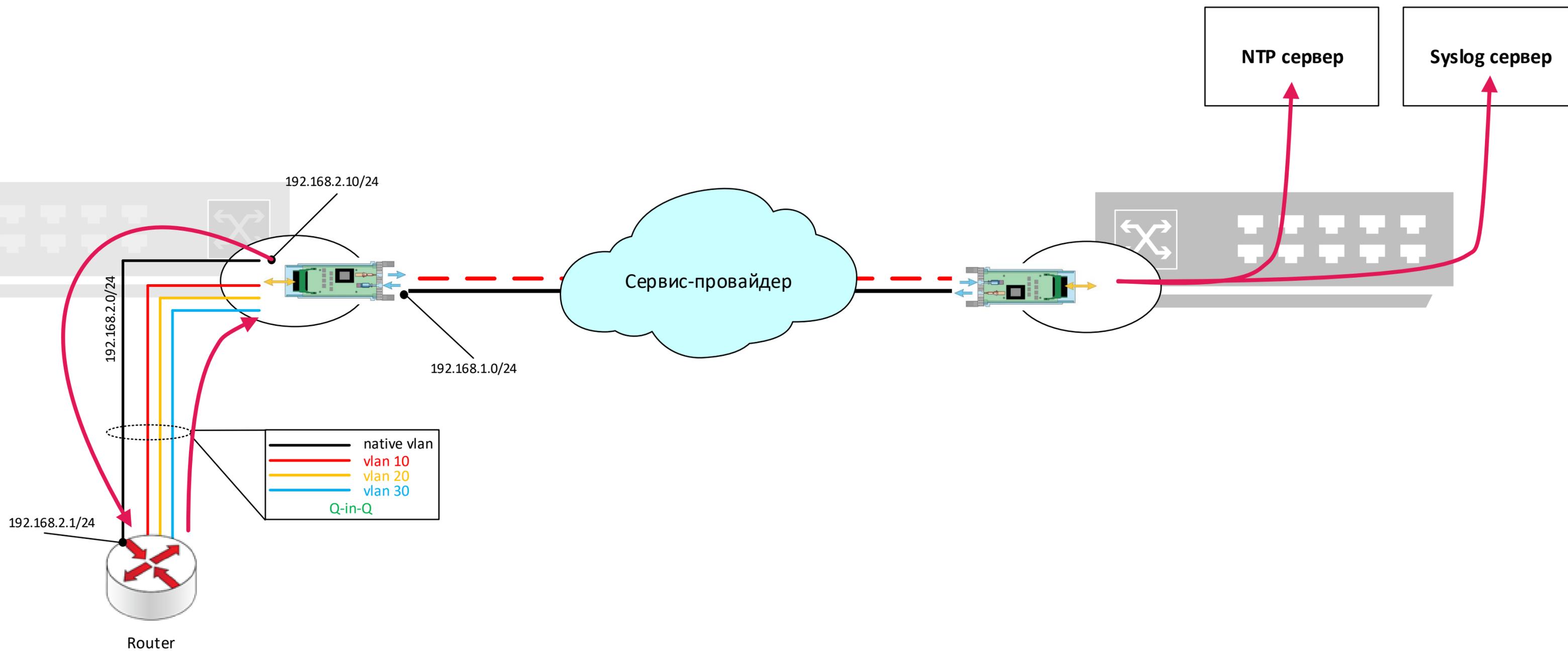


ПЕРЕДАЧА СЕТЕВОГО ТРАФИКА ЧЕРЕЗ ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ

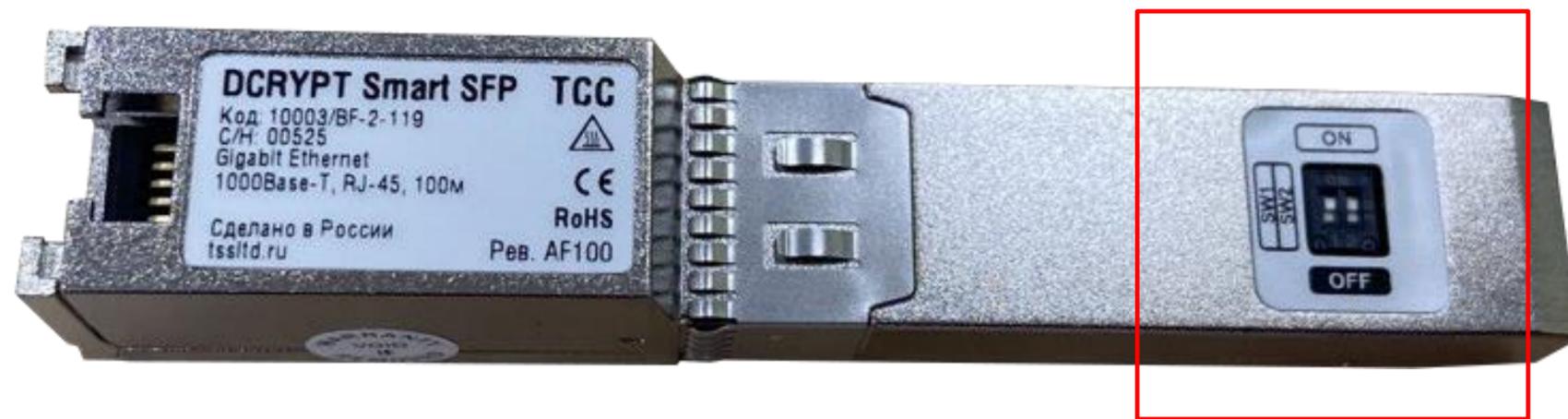




ДОСТУПНОСТЬ РЕСУРСОВ НА УРОВНЕ L3



ВОССТАНОВЛЕНИЕ ОБРАЗА

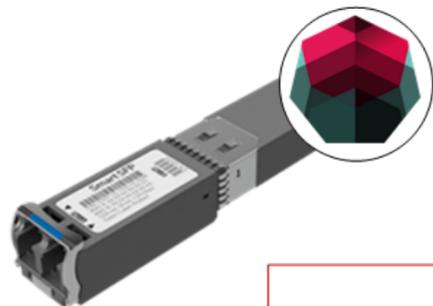


Специальные тумблеры для восстановления ПО

Процесс восстановления ПО:

- 1) Переключить тумблеры.
- 2) Подключить Smart SFP к сетевому устройству.
- 3) Дождаться восстановления образа.
- 4) Вернуть тумблеры в исходное положение.
- 5) Подключить Smart SFP для настройки.

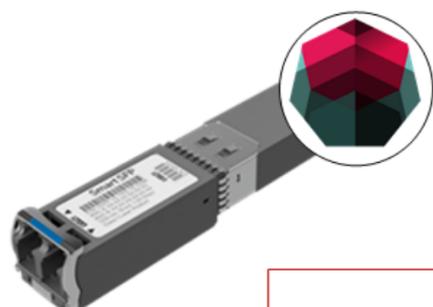
ТЕХНИЧЕСКИЕ ДЕТАЛИ



AM «Diamond VPN/FW 10321»

MAC заголовок

Данные



AM «Diamond VPN/FW 10321»

Произвольный заголовок
длиной 64 байта

Данные

ФОРМАТ ФРЕЙМА



CC-EB-18-fe-00-00 : CC-EB-18-ff-ff-ff

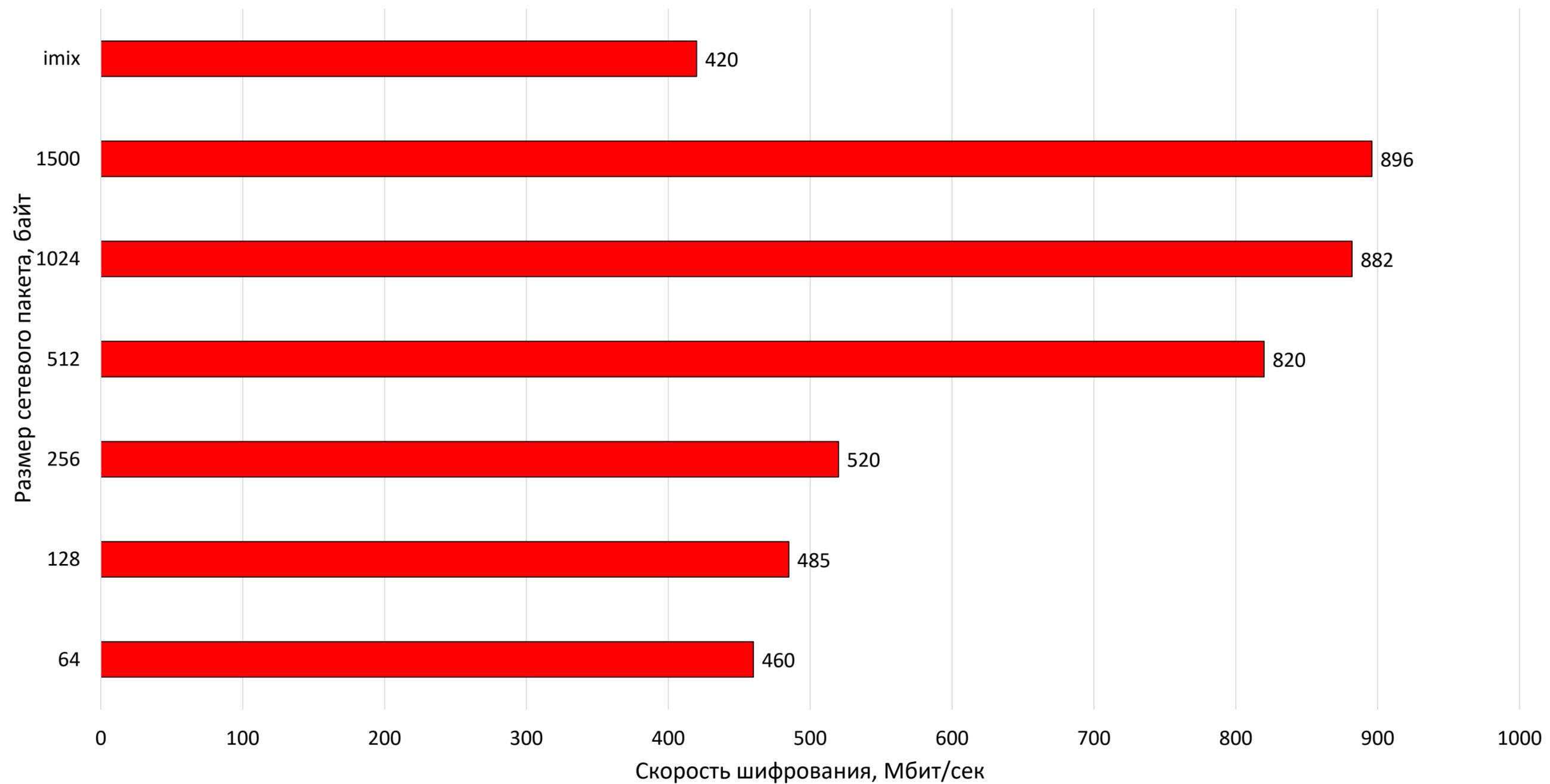
Заголовок

Полезные данные

22 байта

No.	Time	Source	Destination	Protocol	Length	Info
16	3.807586	192.168.1.101	192.168.1.102	UDP	60	34687 → 1024 Len=18
17	3.836961	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	ARP	60	Who has 192.168.1.102? Tell 192.168.1.101
18	3.839372	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	ARP	60	192.168.1.102 is at cc:eb:18:ff:00:08
19	3.842344	192.168.1.101	192.168.1.102	UDP	60	34687 → 1024 Len=18
20	3.845105	192.168.1.102	192.168.1.101	UDP	60	1024 → 34687 Len=18
21	3.845620	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	ARP	60	Who has 192.168.1.101? Tell 192.168.1.102
22	3.847816	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	ARP	60	192.168.1.101 is at cc:eb:18:ff:00:07
23	4.095927	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	0xffff	120	Ethernet II
24	4.096058	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	0xffff	120	Ethernet II
25	5.119905	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	0xffff	120	Ethernet II
26	5.120039	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	0xffff	120	Ethernet II
27	5.297618	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	0xffff	82	Ethernet II
28	5.297764	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	0xffff	82	Ethernet II
29	5.988429	192.168.1.102	192.168.1.101	UDP	60	45189 → 1024 Len=18
30	5.991373	192.168.1.101	192.168.1.102	UDP	60	1024 → 45189 Len=18
31	5.991581	192.168.1.101	192.168.1.102	UDP	60	1024 → 45189 Len=18
32	5.994256	192.168.1.102	192.168.1.101	UDP	60	45189 → 1024 Len=18
33	6.143907	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	0xffff	120	Ethernet II
34	6.144034	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	0xffff	120	Ethernet II
35	7.167905	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	0xffff	120	Ethernet II
36	7.168039	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	0xffff	120	Ethernet II
37	8.191884	cc:eb:18:ff:00:08	cc:eb:18:ff:00:07	0xffff	120	Ethernet II
38	8.192035	cc:eb:18:ff:00:07	cc:eb:18:ff:00:08	0xffff	120	Ethernet II
39	8.813151	192.168.1.102	192.168.1.101	UDP	60	1024 → 34687 Len=18
40	8.816219	192.168.1.101	192.168.1.102	UDP	60	34687 → 1024 Len=18
41	8.851167	192.168.1.101	192.168.1.102	UDP	60	34687 → 1024 Len=18
42	8.854017	192.168.1.102	192.168.1.101	UDP	60	1024 → 34687 Len=18

График зависимости скорости шифрования от размера сетевого пакета





Спасибо за внимание!