

**Модернизация активного сетевого оборудования в модулях «Корпоративной
сети передачи данных» с учетом внедрения двухсайтовой архитектуры.
Технические требования**

СОДЕРЖАНИЕ

| | | |
|-----|---|----|
| 1. | Введение | 3 |
| 2. | Технические требования | 4 |
| 2.1 | Общие требования | 4 |
| 2.2 | Требования к КСПД | 6 |
| 2.3 | Требования к надежности и доступности | 7 |
| 2.4 | Требования к модулям модернизируемой КСПД по производительности, размещению, портовой емкости, масштабируемости и отказоустойчивости | 7 |
| 2.5 | Требования к Поставщику | 10 |
| 2.6 | Требования к Службе технической поддержки | 10 |
| 2.7 | Требования к конфиденциальности и защите информации | 10 |
| 3. | Перечень сокращений | 11 |

1. ВВЕДЕНИЕ

Общей целью проведения работ по модернизации активного сетевого оборудования в модулях корпоративной сети передачи данных (далее КСПД) является замена устаревшего активного сетевого оборудования и построение, на базе нового оборудования, полнофункциональной, надежной и отказоустойчивой сетевой инфраструктуры с учетом 2-хсайтовой архитектуры.

КСПД выполняет роль опорной сети для ИТ-инфраструктуры и информационных систем. Она обеспечивает сетевое взаимодействие внутренних и внешних клиентов и прикладных сервисов с информационными системами.

КСПД обеспечивает связность географически разнесенных зданий через поставщиков телекоммуникационных услуг.

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

2.1 Общие требования

2.1.1 Модернизация активного сетевого оборудования в модулях КСПД должна выполняться с учетом создания двухсайтовой архитектуры. Структурная схема двухсайтовой архитектуры после модернизации представлена на рисунке 1.

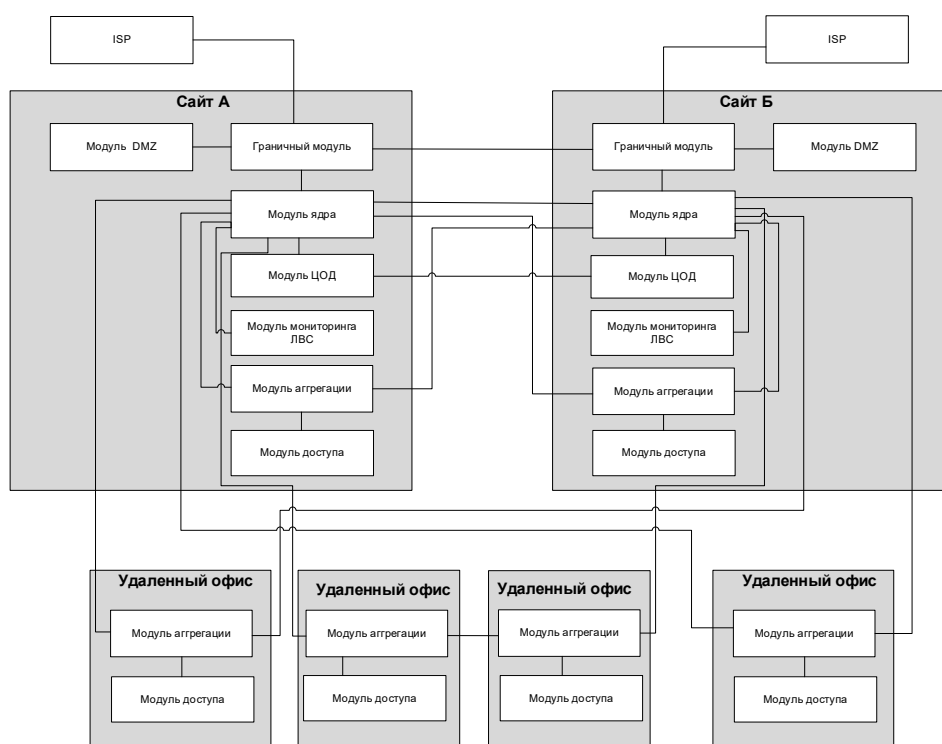


Рисунок 1. Структурная схема КСПД после модернизации с учетом двухсайтовой архитектуры.

- 2.1.2 Сайт А и Сайт Б должны функционировать в синхронном отказоустойчивом режиме (режим работы сайтов с точки зрения сервисов – «онлайн»), следовательно, КСПД должна обеспечить:
- “мобильность приложений”, т.е. возможность перемещения виртуальной машины (далее VM) с сервером приложений из одного сайта на другой с сохранением ее сетевой конфигурации без остановки приложения, обеспечивая при этом оптимальную маршрутизацию трафика в тот сайт, где в данный момент находится VM;
 - сетевую связность на уровне Layer3 модели OSI сайтов ОВЦ, РВЦ, внутренних и внешних потребителей услуг КСПД;
 - сетевой связности на уровне Layer2 модели OSI сайтов ОВЦ и РВЦ для некоторых сетевых сегментов в модулях ЦОД используя организацию Layer2 туннелей поверх стандартных маршрутизируемых (Layer3) IP-сетей (технология Overlay, проброс L2-сети поверх L3-сегмента);
 - непрерывность процедур резервного копирования и архивирования данных и обеспечения сетевой связности сайтов для гарантированного восстановления информационных систем, расположенных на любом из сайтов.
- 2.1.3 Каждый сайт в случае возникновения глобальных кризисных ситуаций (разрушение одного из двух сайтов) должен иметь возможность полной изоляции и обеспечения автономного функционирования сетевой инфраструктуры для обслуживания информационных систем, размещенных на этом сайте и клиентов КСПД, подключающихся к этому сайту.
- 2.1.4 Сетевая инфраструктура должна обеспечить связность потребителей услуг (вычислительные информационные ресурсы, системы хранения данных, системы мониторинга, системы управления инженерными системами, системы информационной безопасности, рабочие станции и т.д.) с заданным уровнем обслуживания в географически распределенной среде, а также учитывать и обеспечивать возможность масштабирования сетевой инфраструктуры и информационных систем.
- 2.1.5 Сетевая инфраструктура должна обеспечить сетевое взаимодействие с поставщиками телекоммуникационных услуг, внешними потребителями, внешними информационными системами с помощью технологий, обеспечивающих отказоустойчивые связи и автоматическое переключение на резервные маршруты прохождения трафика.
- 2.1.6 При выполнении модернизации, должно быть предусмотрено построение полноценных модулей DMZ, которые должны располагаться в граничных модулях. Поставщики телекоммуникационных услуг должны подключаться к граничному модулю на двух сайтах.
- 2.1.7 Используемые в проектом решения технологии сетевой связности и отказоустойчивости должны обеспечивать:
- поддержку статических и динамических протоколов маршрутизации (OSPF (Open Shortest Path First), BGP (Border Gateway Protocol) или аналоги) без ограничений по количеству сетей (vlan-ов), маршрутов, добавляемых в них;
 - поддержку протокола Equal Cost Multipath Routing (ECMP) — производит L3 балансировку трафика при наличии нескольких каналов передачи и обеспечивает передачу данных при выходе из строя одного из них;

- поддержку технологии MPLS (все устройства, за исключением модуля DMZ, должны иметь функционал P/PE-устройств и обеспечивать построение сети с полноценной коммутацией по меткам);
- поддержку протокола Link Aggregation (802.3ad) — позволяет объединять до восьми физических соединений в одно логическое, для увеличения пропускной способности канала и распределения нагрузки;
- возможность создания изолированных, в том числе “перекрывающихся”, доменов маршрутизации для контролируемого подключения определенных потребителей к определенным ресурсам (поддержка сетевой виртуализации устройств (VRF, VR, VDOM или аналогов));
- поддержку отказоустойчивости «шлюза-по-умолчанию» (например, протоколов семейства FHRP (First Hop Redundancy Protocol), HSRP (Hot Standby Redundancy Protocol), VRRP (Virtual Router Redundancy Protocol) или аналогов);
- поддержку L2-L4 аппаратных ACL;
- поддержку разных типов аутентификации пользователей (mac-based, web-based, 802.1x);
- ограничение MAC адресов на порту;
- поддержку технологий IP source guard и ARP dynamic inspection;
- поддержку технологии DOS storm protection;
- поддержку не менее двух протоколов канального уровня, позволяющих сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения (LLDP, CDP, EDP);
- поддержку протокола QoS — качества обслуживания в точках, где происходит превышение реального трафика над физически возможной пропускной способностью канала / порта / устройства.

2.1.8 Поставляемое оборудование должно быть уровня Data Center.

2.1.9 Предлагаемое к реализации техническое решение должно обеспечивать сохранение и использование имеющегося теоретического и практического опыта, полученного администраторами при администрировании и обслуживании сетевой инфраструктуры и систем информационной безопасности.

2.1.10 Взаимодействие сайтов должно осуществляется через выделенные оптические каналы связи с использованием аппаратного шифрования по двум разнесенным маршрутам через поставщиков телекоммуникационных услуг.

2.2 Требования к КСПД

Характеристики оборудования в модулях сети КСПД должны соответствовать требованиям раздела 2.1, а также соответствовать следующим основным параметрам:

- модульность, стекирование оборудования;
- неблокируемая коммутация трафика;
- поддержка технологии приоритезации QoS;
- аппаратная отказоустойчивость и горячее резервирование управляющих модулей, интерфейсных модулей, модулей коммутации и модулей питания;

- возможность обновления ПО на сетевом оборудовании, без остановки функционирования каждого отдельного устройства (ISSU – in-service software update);
- поддержка агрегированных каналов на уровне L2/L3;
- поддержка протоколов SSH2, SNMP v3, семейство Flow, AAA (RADIUS, TACACS);
- поддержка протоколов мониторинга и анализа проходящего трафика (SPAN, RSPAN, ERSPAN или аналоги);
- поддержка access-list, prefix-list, distribution-list, policy base routing;
- резервирование по электропитанию;
- возможность оперативного наращивания емкости оборудования в модулях.

2.3 Требования к надежности и доступности

- 2.3.1 Режим функционирования – круглосуточно (в режиме 24часа/7дней в неделю/365дней в году).
- 2.3.2 Архитектура, оборудование, каналы связи, протоколы маршрутизации, виртуализации сети и прочие технологии, применяемые в модернизированных модулях КСПД, должны обладать отказоустойчивыми резервируемыми компонентами и функционалом, обеспечивающим «горячее» переключение на резерв без прерывания сетевой доступности. Контрольное значение проверки отказоустойчивости любого модуля – при выходе из строя единицы оборудования в тракте передачи данных, время сходимости сети – не более 1минуты, время автоматического переключения на резервные маршруты (OSFP, BGP) – не более 1 минуты.
- 2.3.3 Активное сетевое оборудование модернизируемых модулей КСПД должно обладать отказоустойчивыми резервируемыми компонентами и позволять проводить регламентные работы по обслуживанию единичных элементов без прерывания сетевой доступности. При необходимости полного отключения оборудования, полное восстановление работоспособности сетевой инфраструктуры двух сайтов должно занимать не более 45 минут с момента запуска сетевого оборудования.

2.4 Требования к модулям модернизируемой КСПД по производительности, размещению, портовой емкости, масштабируемости и отказоустойчивости

Поставляемое оборудование должно иметь возможность установки в существующие телекоммуникационные шкафы (42U 600x800).

По согласованию с Заказчиком, количество активного сетевого оборудования, портовой емкости, комплектации оборудования может быть изменено.

2.4.1 Модуль ядра.

В двух модулях ядра, для подключения к ним других модулей, должно быть по 2 устройства, объединенных в один общий стек или по схеме N+1, общее количество устройств 4. Каждое устройство должно соответствовать следующим техническим характеристикам (не менее):

- 4 порта 40Gb QSFP+ Ethernet;
- 8 портов 10Gb QSFP+ Ethernet;
- 1 х консольный порт;

- оборудование должно иметь гарантию не менее 5-ти лет и лицензию позволяющую использовать максимальный функционал;
- 2 оптических модуля QSFP+ 40Gb 20км;
- 2 оптических модуля QSFP+ 40Gb 300м и оптические пачкорды MM/LC-LC (full duplex) 1м 4шт или кабели для стекирования;
- 8 оптических модулей SFP+ 10Gb 20км;
- 4 оптических пачкорда SM/LC-LC (full duplex) 3м;
- Тип разъема шнура питания IEC C13/C14;
- Наличие консольного кабеля.

2.4.2 В граничных модулях EDGE (Сайт А, Сайт Б) для подключения к ядру сети и другим устройствам должно быть по 2 коммутатора L2/L3 с поддержкой протоколов маршрутизации (OSPF, BGP), которые объединяются в стек, в каждом из которых обеспечена портовая емкость не менее:

- 4 порта 10Gb (Uplink) SFP+;
- 12 портов Ethernet 1Gb;
- 1 х консольный порт;
- оборудование должно иметь гарантию не менее 5-ти лет и лицензию позволяющую использовать максимальный функционал;
- в комплекте должны быть 4 оптических трансивера 10G SFP+ 850nm 300м;
- 12 оптических пачкордов MM/LC-LC (full duplex) 3м;
- Кабель для стекирования или кабель прямого подключения DAC;
- Тип разъема шнура питания IEC C13/C14;
- Наличие консольного кабеля.

2.4.3 Для построения зон DMZ и подключения поставщиков телекоммуникационных услуг, необходимо по 4 стекируемых L2 коммутатора на каждом центре (Сайт А, Сайт Б), на каждом из устройств:

- 2 порта 10Gb (Uplink) SFP+;
- 20 портов 1/10Gb с поддержкой модулей SFP, SFP RJ-45, SFP+;
- 1 х консольный порт;
- оборудование должно иметь гарантию не менее 5-ти;
- в комплекте должны быть 12 оптических трансиверов 10G SFP+ 850nm 300м, 5 оптических трансиверов 10G SFP+ 850nm 300м 5 модулей 1G Ethernet (SFP RJ-45);
- 1 оптический пачкорд SM/LC-LC (full duplex) 3м;
- 6 оптических пачкордов MM/LC-LC (full duplex) 1,5м;
- 12 оптических пачкордов MM/LC-LC (full duplex) 3м;
- 6 оптических пачкордов MM/LC-LC (full duplex) 10м;
- Кабель для стекирования или кабель прямого подключения DAC;
- Тип разъема шнура питания IEC C13/C14;
- Наличие консольного кабеля.

- 2.4.4 Для связи двух модулей EDGE (Сайт А, Сайт Б), требуется поставка 4 оптических модулей SFP+ 10Gb 20км и 4 оптических пачкордов SM/LC-LC (full duplex) 3м.
- 2.4.5 Для построения модулей агрегации (6 модулей) в каждом из которых по 2 стекируемых коммутатора L2/L3 с поддержкой протоколов маршрутизации (OSPF, BGP) с портовой емкостью каждого устройства не менее:
- 12 портов 10Gb SFP+;
 - 1 х консольный порт;
 - оборудование должно иметь гарантию не менее 5-ти лет и лицензию позволяющую использовать максимальный функционал;
 - 2 оптических трансивера SFP+ 10Gb 20км;
 - 8 оптических трансиверов 10G SFP+ 850nm 300m;
 - 4 оптических пачкорда MM/LC-LC (full duplex) 1,5м;
 - 2 оптических пачкорда SM/LC-LC (full duplex) 3м;
 - Кабель для стекирования или кабель прямого подключения DAC;
 - Тип разъема шнура питания IEC C13/C14;
 - Наличие консольного кабеля.
- 2.4.6 Проектное решение должно предусматривать необходимое количество и пропускную способность каналов связи на межмодульных соединениях (uplink) внутри Сайт А, Сайт Б, чтобы исключить появление “узких мест”. Должны выполняться требования к соотношениям пропускных способностей (уровням переподписки) uplink и портов подключения оконечных устройств (downlink):
- в модуле ЦОД в направлении модуля ядра – не более 1:3;
 - в модуле распределения (доступа пользователей) в направлении модуля ядра – не более 1:2;
 - в модуле агрегации (периферии) в направлении модуля ядра - не более 1:2 в периферийных модулях (удаленного доступа, граничном модуле Edge) – не более 1:5.
- 2.4.7 Для организации каналов связи между сайтами должна обеспечиваться возможность перехода с технологий 40Гбит/с на технологии 40/100Гбит/с без необходимости замены сетевого оборудования (допускается замена коммутирующих модулей в сетевом оборудовании).
- 2.4.8 Архитектура решения должна предусматривать возможность добавления новых вычислительных центров, без необходимости изменения архитектуры и структуры решения.

2.5 Требования к Поставщику

- 2.5.1 Поставляемое оборудование должно иметь соответствующие сертификаты и разрешения для применения в сетях связи Республики Беларусь, поддерживать стандарты RFC, опубликованные IETF.
- 2.5.2 Поставщик решения должен предоставить подтверждение производителя о возможности получения технической поддержки поставляемого оборудования сроком не менее 5 лет.
- 2.5.3 Поставщик должен иметь официальный статус от производителей оборудования и ПО, предлагаемого к использованию в рамках проекта модернизации активного сетевого оборудования в модулях КСПД.
- 3.5.4 Поставщик должен произвести поставку технической документации на оборудование и его настройку, оказать помощь в настройке поставляемого оборудования и при необходимости оказать техническую консультацию.

2.6 Требования к Службе технической поддержки

- 2.6.1 Служба технической поддержки должна быть доступна для обращения Заказчика круглосуточно (в режиме 24часа/7дней в неделю/365дней в году).
- 2.6.2 Срок обработки обращений заказчика – не более 1 часа.
- 2.6.3 При поставке оборудования Поставщик должен обеспечить Заказчику доступ к службе технической поддержки поставляемого оборудования и возможность самостоятельно регистрировать кейсы.
- 2.6.4 Срок предоставления исправлений программного обеспечения – не более 24 часов с момента обращения Заказчика. Срок предоставления оборудования для гарантийной замены – не более 30 рабочих дней с момента обращения заказчика.

2.7 Требования к конфиденциальности и защите информации

- 2.7.1 Поставщик обязан соблюдать требования по защите информации, действующие у Заказчика.
- 2.7.2 Поставщик обязан заключить с Заказчиком Соглашение о конфиденциальности и неразглашении технической, коммерческой либо любой иной информации Заказчика, ставшей ему доступной при выполнении обследования объектов.
- 2.7.3 Поставщик обязан принять все организационные, технические и иные меры для предотвращения утечки данных.

3. Перечень сокращений

| | |
|------|--|
| ВОЛС | – Волоконно-Оптическая Линия Связи |
| КСПД | – Корпоративная Сеть Передачи Данных |
| ТТ | – Технические Требования |
| ПО | – Программное Обеспечение |
| ЦОД | – Центр Обработки Данных |
| ACL | – Access Control List |
| BGP | – Border Gateway Protocol |
| FC | – FibreChannel |
| GE | – Gigabit Ethernet |
| IP | – Internet Protocol |
| LAN | – Local Area Network |
| MAC | – Media Access Control |
| OSI | – Open Systems Interconnection Basic Reference Model |
| OSPF | – Open ShortestPath First protocol |
| STP | – Spanning Tree Protocol |
| VRF | – Virtual Routing and Forwarding |