**Требования к общей топологии ЛВС**

При построении локальной вычислительной сети должна использоваться многоуровневая модель с использованием беспетлевой топологии, согласно которой ЛВС делится на следующие основные уровни:

* уровень ядра;
* уровень серверных ферм/ЦОД;
* уровень доступа.

В зависимости от особенностей реализации ЛВС возможно использование отдельных уровней управления (Management) и агрегации.

Также отдельно выделяется уровень диспетчерского сегмента ЛВС, который предназначен для обеспечения работы критически важных ИУС и рабочих станций диспетчеров в случае неработоспособности основной ЛВС.

***Уровень ядра.***

При построении уровня ядра необходимо использовать высокопроизводительные модульные коммутаторы уровня L3.

Данный уровень предназначен для решения следующих задач:

1. высокоскоростной коммутации и маршрутизации трафика;
2. агрегирования трафика от устройств нижнего уровня;
3. изоляции деталей сетевой топологии от устройств верхнего и нижнего уровней;
4. маршрутизации между виртуальными локальными сетями (VLAN);
5. разграничения доступа к внутренним ресурсам сети;
6. подключения к узлу МСС/СЗП на уровне L3/L2.

Не допускается использование ядра ЛВС в качестве сервера DHCP.

Состав оборудования определяется исходя из количества, подключаемого к уровню ядра сетевого и серверного оборудования, требований по надежности, производительности и возможности дальнейшего расширения.

Для организации обмена маршрутной информацией (L3) с узлом МСС/СЗП на уровне ядра должен быть использован протокол динамической маршрутизации OSPF.

***Уровень серверных ферм/ЦОД.***

Данный уровень предназначен для решения следующих задач:

1. подключения серверного оборудования (в том числе и серверов с виртуальными машинами) и других устройств, обеспечивающих обработку и хранение данных в ЦОД;
2. обработку трафика на уровнях L2 (коммутация) и L3 (маршрутизация) передаваемого в пределах ЦОД;
3. подключение серверного сегмента ЦОД к коммутаторам уровня ядра ЛВС.

Для ИА и филиалов ОДУ подключение коммутаторов уровня серверных ферм/ЦОД к коммутаторам уровня ядра ЛВС и ЯДС должно быть реализовано на уровне L3 с использованием протокола динамической маршрутизации OSPF. Для филиалов ОДУ допускается подключение коммутаторов уровня серверных ферм/ЦОД к ядру ЛВС и ЯДС на уровне L2 при условии реализации беспетлевой топологии подключения.

Для филиалов ОДУ допускается совмещение функционала уровня ядра ЛВС/ЯДС и уровня серверных ферм/ЦОД (подключение сетевых интерфейсов физических серверов непосредственно в коммутаторы уровня ядра ЛВС и ЯДС) в зависимости от размеров проектируемой или эксплуатируемой ЛВС.

Для филиала РДУ использование отдельного уровня серверных ферм/ЦОД не предусмотрено, подключение физических серверов должно производиться непосредственно в коммутаторы уровня ядра ЛВС (для серверов диспетчерского сегмента – в ЯДС). В случае реализации в филиале РДУ проекта виртуализации серверов (ЛВК) подключение должно осуществляться таким образом, что основной комплект (кластер серверов виртуализации) подключается в ядро ЛВС, а резервный комплект (кластер серверов виртуализации) подключается в ЯДС. Детализировано варианты подключения комплектов ЛВК к ЛВС описаны в документе «Типовые требования к архитектуре, настройке и организации эксплуатации ЛВК филиалов АО «СО ЕЭС» РДУ». По отдельному согласованию с СПАК ИА допускается использовать другие схемы подключения комплектов виртуализации серверов, если при этом не происходит ухудшение функциональных возможностей, а также не происходит ухудшения показателей производительности и надежности.

При реализации ЕТРК ЦОД/ОКВ в ОДУ, ЛВК в РДУ запрещается подключать данные сервера в сегмент ДМЗ.

***Уровень доступа.***

Для данного уровня подразумевается использование коммутаторов, которые обеспечивают подключение ПК и ноутбуков пользователей (рабочих станций), IP телефонов, IP видеокамер (внутри здания), сетевых принтеров, МФУ и др. к ЛВС. Данный уровень предназначен для решения следующих задач:

1. обеспечение подключения к сети рабочих станций и ноутбуков пользователей, IP телефонов, IP видеокамер, сетевых принтеров, МФУ и др.;
2. обеспечение подключения к сети «основных» рабочих станций диспетчеров;
3. предотвращение несанкционированного доступа в ЛВС со стороны неавторизованных источников;
4. классификации пользовательского трафика в соответствии с заданным уровнем обслуживания;
5. предоставление питания по технологии PoE подключаемым сетевым устройствам (внутренние IP видеокамеры и IP телефоны).

Не допускается совмещать функции уровня доступа с функциями уровня ядра сети в одном коммутаторе или стеке коммутаторов.

В случае если на рабочем месте пользователя используется корпоративный IP телефон Cisco, то подключение рабочей станции пользователя должно осуществляться через встроенный в этот IP телефон сетевой коммутатор.

В случае если к портам коммутаторов доступа предполагается подключение устройств с поддержкой питания PoE (внутренние IP видеокамеры и IP телефоны), то рекомендуется предусмотреть использование коммутаторов уровня доступа с поддержкой PoE, в зависимости от требуемого кол-ва PoE портов это может быть, как коммутатор с поддержкой PoE на всех портах, так и с поддержкой PoE только на части портов.

***Уровень управления (Management).***

Для ИА, филиалов ОДУ и РДУ возможно использование уровня управления, реализованного на отдельных сетевых коммутаторах, которые обеспечивают подключение к ЛВС интерфейсов управления различных устройств: сетевое оборудование, сервера, СХД, ленточные библиотеки, SAN коммутаторы и т.д. Коммутаторы уровня управления должны подключаться непосредственно в ядро ЛВС или ЯДС.

***Уровень агрегации.***

Для ИА, филиалов ОДУ и РДУ допускается использование отдельных коммутаторов, агрегирующих линки на уровне L2, для подключения физических серверов, серверов виртуализации, коммутаторов доступа или управления в случае если технически затруднительно осуществить такое подключение непосредственно в ядро ЛВС или ЯДС (территориальная удаленность мест расположения подключаемого оборудования от ядра ЛВС/ЯДС, необходимость прокладки большого кол-ва дополнительных кабелей, и т.д.). При этом сетевые интерфейсы оборудования должны подключаться непосредственно к портам агрегирующих коммутаторов, а агрегирующие коммутаторы в свою очередь должны подключаться в ядро ЛВС или ЯДС соединениями на основе технологии 10 Gigabit Ethernet с объединением нескольких (два для РДУ и не менее двух для ОДУ) физических интерфейсов в один логический канал – PortChannel с использованием протокола LACP (если данный протокол поддерживается оборудованием).

**Оборудование, применяемое на разных уровнях ЛВС**

***Уровень ядра ЛВС***

Для филиала РДУ в качестве коммутаторов уровня ядра сети должны использоваться два шассийных коммутатора типа Cisco Catalyst 45XX с объединением в один логический коммутатор по технологии VSS. Кол-во модулей Supervisor (управляющий модуль) в каждом шасси – 1 или 2, версия лицензии ПО IOS не ниже Enterprise Services. Также для филиала РДУ в качестве коммутаторов уровня ядра сети допускается использовать стек коммутаторов типа Cisco 3750X или 3850, версия лицензии ПО IOS не ниже IP Services.

***Уровень агрегации.***

В качестве агрегирующих коммутаторов рекомендуется использовать стек коммутаторов Cisco 2960XR, Cisco 3750X или 3850, версия лицензии ПО IOS не ниже Lan Base.

***Уровень доступа.***

В качестве коммутаторов уровня доступа рекомендуется использовать модели коммутаторов типа Cisco 2960X (некритичные АРМ или сетевые устройства) или Cisco 2960XR (критичные АРМ или сетевые устройства, АРМ диспетчеров/дежурных) с версией лицензии ПО IOS Lan Base.

***Уровень управления (Management).***

В качестве коммутаторов уровня управления рекомендуется использовать модели коммутаторов типа Cisco 2960X (интерфейсы управления некритичного оборудования) или Cisco 2960XR (интерфейсы управления критичного оборудования) с версией лицензии ПО IOS Lan Base.

***Диспетчерский сегмент.***

В филиалах РДУ в качестве коммутаторов ЯДС должны использоваться коммутаторы моделей типа Cisco 2960XR. В зависимости от необходимой портовой емкости это может быть стек из двух и более коммутаторов.

Для филиалов ОДУ и РДУ по отдельному согласованию с СПАК ИА допускается в качестве коммутаторов на всех уровнях и в диспетчерском сегменте использовать иные модели коммутаторов Cisco – функциональные возможности, показатели производительности и надежности которых не хуже, чем у рекомендуемых моделей коммутаторов. Не допускается использовать модели коммутаторов или модули супервизоров (в случае шассийных коммутаторов), которые имеют встроенный функционал контроллера Wi-Fi, если нет возможности полного отключения данного функционала.