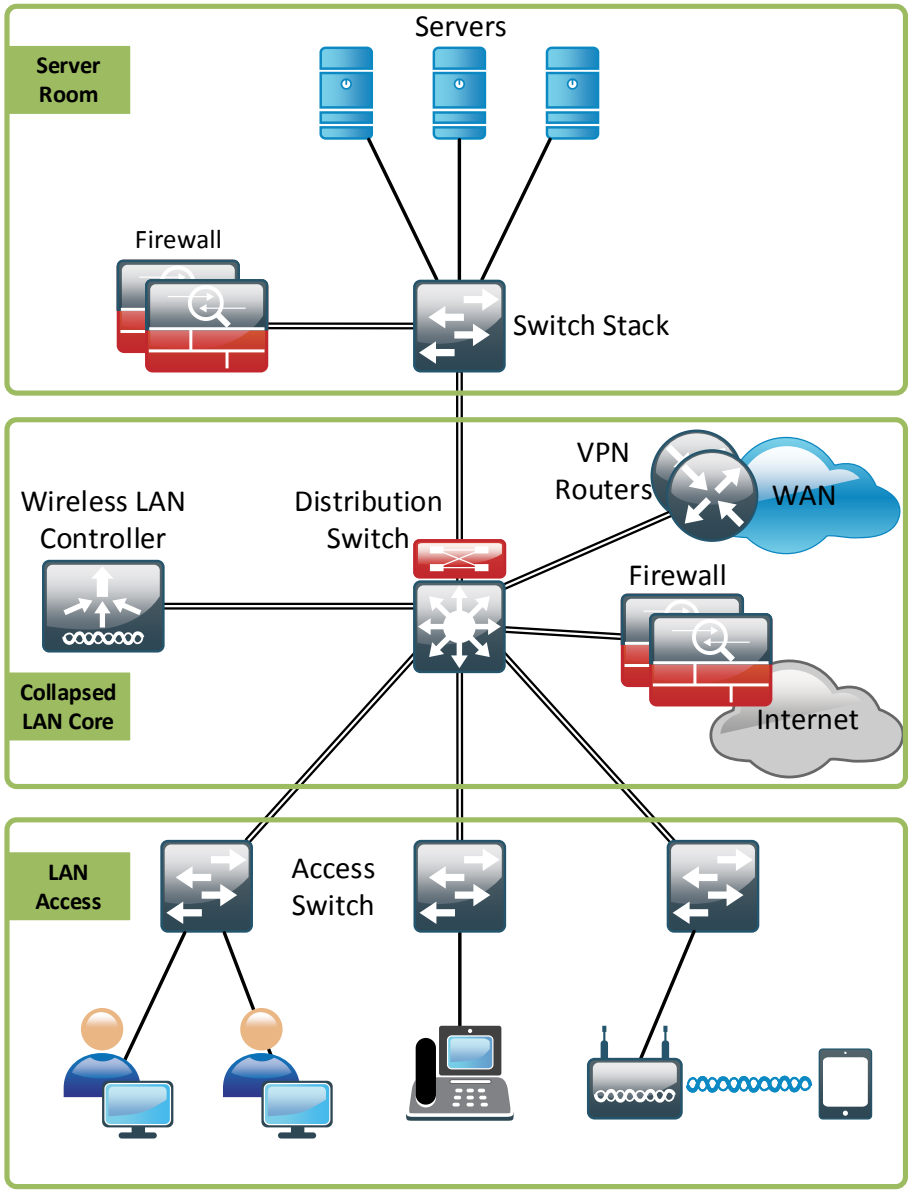
2014 Ver 1.0

John Cooper
NETSKILLS.RU
SKILL-ADMIN.BLOGSPOT.RU

Архитектура корпоративных сетей

Краткое руководство



NetSkills
online network school

ОГЛАВЛЕНИЕ

ЧИТАТЕЛЮ

Это небольшое руководство, которое каким-либо образом попало к вам в руки, создавалось долгие девять месяцев, длинными и дождливыми вечерами в попытке структурировать полученные знания и опыт. За это время книга дважды переписывалась и претерпела серьезные изменения в содержании для того, чтобы читатель получил максимум пользы от полученной информации. При этом автор старался сохранять доступный для понимания стиль изложения материала, рассчитанный на читателей разного уровня подготовки.

Единственная просьба к читателю это ценить труд и время автора - не нарушать авторское право и не публиковать данное руководство в открытый доступ в сети Интернет.

ВВЕДЕНИЕ

Данное руководство является результатом нескольких лет работы в области системной интеграции, а так же основано на анализе и переработке (с учетом российских реалий) архитектур Cisco SAFE и Cisco SBA Borderless Networks. Здесь будут рассмотрены Иерархическая модель и основные модули корпоративной сети, их расположение в сети, а так же основные методы защиты.

Будет описан процесс подключения удаленных филиалов к головному офису, подключение основных модулей корпоративной сети (серверный модуль, модуль Интернет (Internet Edge), модуль территориальных сетей WAN).

Рассмотрим возможные варианты оборудования для каждого из уровней иерархической модели и основных модулей. Определимся с методами реализации отказоустойчивости и повышения пропускной способности сети.

Руководство по дизайну корпоративных сетей предназначено для организаций с количеством пользователей до 10 000.

ДЛЯ КОГО ЭТО РУКОВОДСТВО

- Системные инженеры, которые нуждаются в стандартизации применяемых сетевых решений
- Преподаватели/тренера, которые ищут материалы для обучения сотрудников внутри организации

P.S. Документ в первую очередь предназначен для обучения сотрудников внутри организации и не является абсолютной истиной для всех.

ПРИМЕНЕНИЕ

Данный документ описывает основные аспекты проектирования крупных корпоративных сетей, однако может быть применен и для среднего и малого бизнеса. Естественно, что в рамках этого руководства невозможно рассмотреть все потребности всех организаций в части сетевой инфраструктуры. В настоящем документе представляется лишь некий “шаблон” которого стоит придерживаться при проектировании сетей, но он может быть изменен или модернизирован в соответствии с требованиями Заказчика.

Описанная ниже архитектура не гарантирует абсолютной безопасности вашей сети. Однако следуя этому руководству и используя рациональную политику безопасности, вы сможете существенно обезопасить сетевую инфраструктуру. Для построения более комплексной и надежной защиты необходимо разбираться в современных методах атак, вирусах и других вопросах безопасности, которые не будут рассматриваться в данном руководстве.

Все представленные решения основываются на оборудовании Cisco, однако я постараюсь описать некоторые альтернативы (дизайн для малого и среднего бизнеса) предназначенные для уменьшения стоимости сетевой архитектуры.

Так же предполагается, что читатель обладает необходимым уровнем знаний и способен отличить коммутатор от маршрутизатора.

1. ОСНОВЫ ДИЗАЙНА

Архитектура корпоративной сети включает в себя проводные и беспроводные соединения. В этом документе мы рассмотрим основные аспекты построения проводной сети.

Представленная архитектура не является каким-то открытием или новшеством в области сетевых технологий. Это просто комплекс, впитавший в себя все необходимое для обеспечения сетевой безопасности, а также устойчивости и масштабируемости.

Главные цели представленной архитектуры:

- Простота внедрения - развертывание решения в кратчайшие сроки.
- Гибкость и масштабируемость - модульная архитектура позволяет внедрять только те решения, которые необходимы в данный момент, с возможность последующего роста информационной инфраструктуры.
- Отказоустойчивость и безопасность - защита пользовательского трафика, отказоустойчивое исполнение гарантирующее стабильную работу сети даже во время атак.
- Простота управления - централизованное управление всей сетевой инфраструктурой.
- Готовность к новым технологиям - построенная архитектура позволяет легкое внедрение новых технологий и сервисов (например Cisco Collaboration).

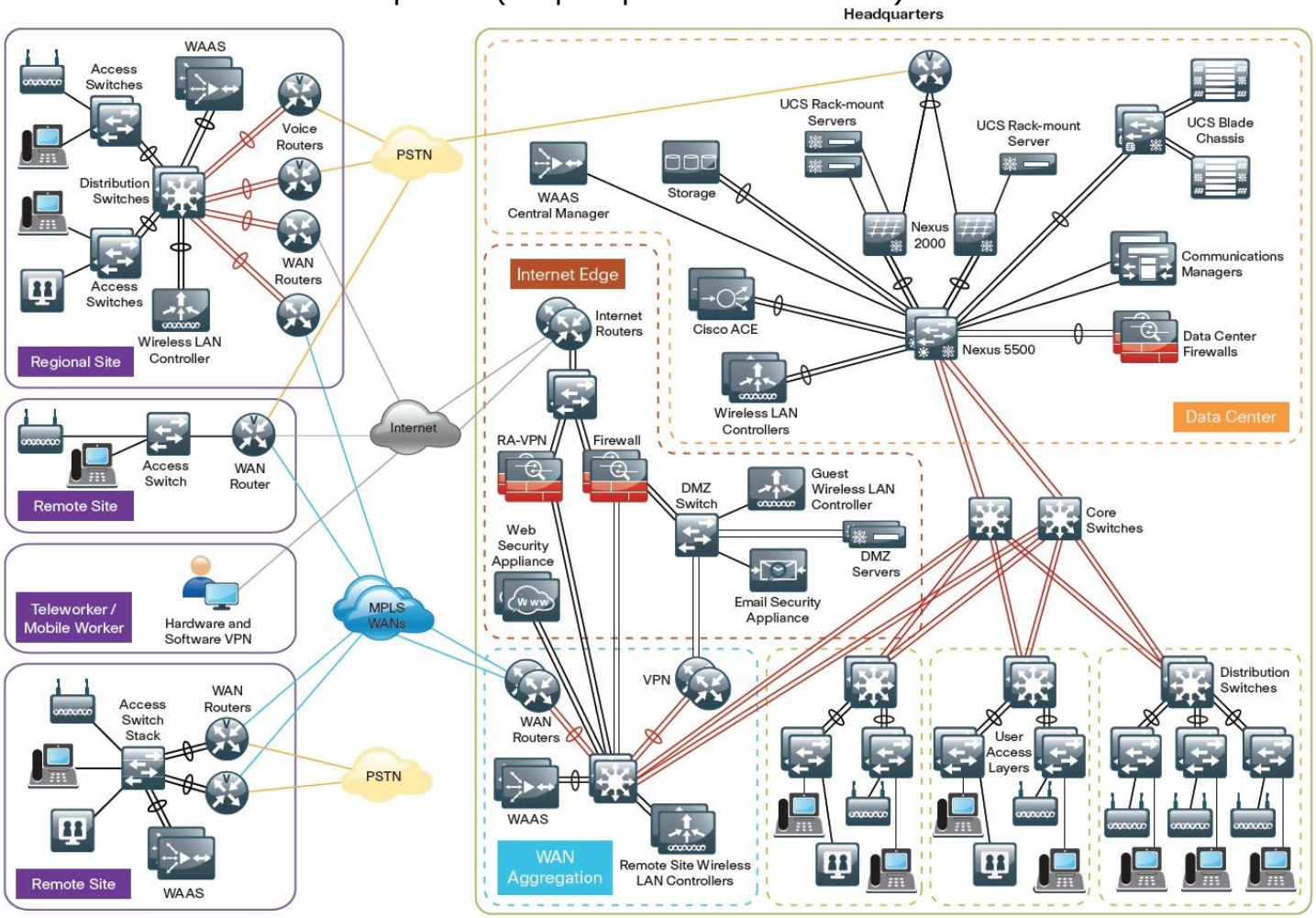


Рис.1.1. Архитектура корпоративной сети

1.1. ПРИНЦИП МОДУЛЬНОСТИ

Разбив архитектуру сети на модули можно сконцентрироваться на функционале каждого из них по отдельности, что существенно упрощает дизайн, внедрение и управление. Созданные модули, как детали конструктора из которых вы можете собрать сеть, соответствующую вашим требованиям. Эти же детали можно применять повторно (репликация), сильно сокращая время проектирования. Принцип репликации (повторения) элемента упрощает масштабируемость сети и ускоряет ее развертывание. На рис. 1.2 представлен процесс модернизации сети. Можно заметить, что масштабирование сводится к простому добавлению дополнительных модулей.

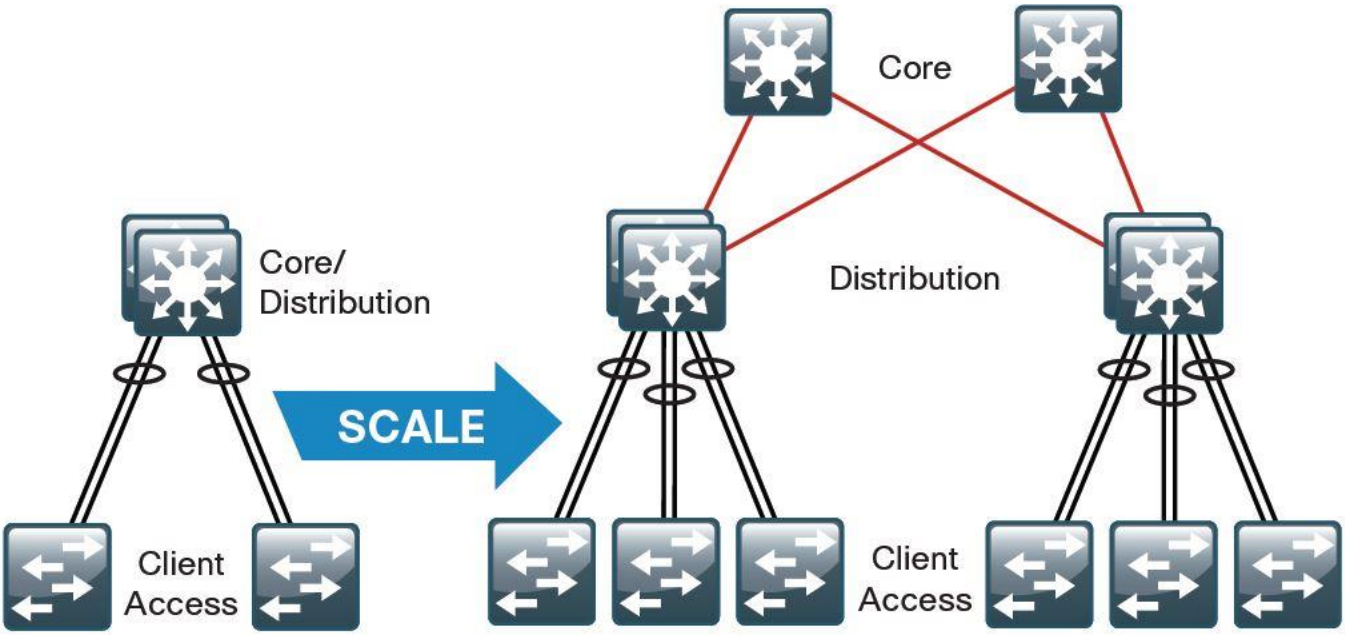


Рис. 1.2. Масштабируемость модульной сети

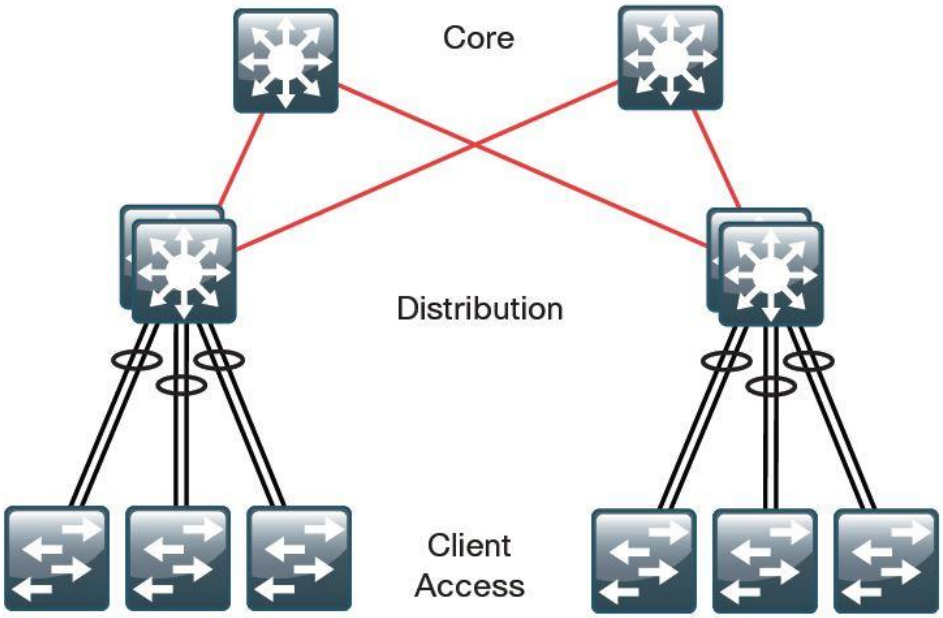


Рис. 1.3. Иерархическая модель сети

Разбиение большой сети на небольшие, простые для понимания, модули (уровни) способствует устойчивости сети за счет локализации возникающих проблем. Таким образом при возникновении какого-либо сбоя в сети необходимо определить на каком уровне возникла ошибка, затем приступать к ее решению, не затрагивая при этом другие модули сети.

2. ИЕРАРХИЧЕСКАЯ МОДЕЛЬ СЕТИ

Иерархическая модель представляет собой фундамент для сетевой инфраструктуры: подключение пользователей, принтеров, сканеров, WAN маршрутизаторов, устройств безопасности, серверов и т.д.

Иерархическая модель (Рис. 1.3) делит сеть на три основных уровня/модуля.

Уровни иерархической модели:

- Уровень доступа (Access Layer) - предоставляет пользователям или устройствам (принтер, сканер, ip-телефон) доступ к сети.
- Уровень распределения (Distribution Layer) - агрегирует/объединяет уровни доступа и предоставляет доступ к различным сервисам организации.
- Уровень ядра/базовый уровень (Core Layer) - агрегирует/объединяет уровни распределения в больших сетях.

Эти три уровня предоставляют различные функции и возможности. В зависимости от необходимости могут применяться один, два или все три уровня. Например для офиса с количеством пользователей менее 10 имеет смысл внедрять только уровень доступа. Для большой организации, занимающей несколько этажей или целое здание, будет разумным применение как уровня доступа, так и уровня распределения. Для огромных сетей, объединяющих несколько зданий необходимы все три уровня: уровень доступа, уровень распределения и уровень ядра.

2.1. УРОВЕНЬ ДОСТУПА (ACCESS LAYER)

Уровень доступа является точкой входа в сеть для пользователей и сетевых устройств (принтеры, сканеры, ip-телефоны и т.д.). Доступ как проводной, так и беспроводной. В более ранней литературе данный уровень называется “Модуль доступа”.

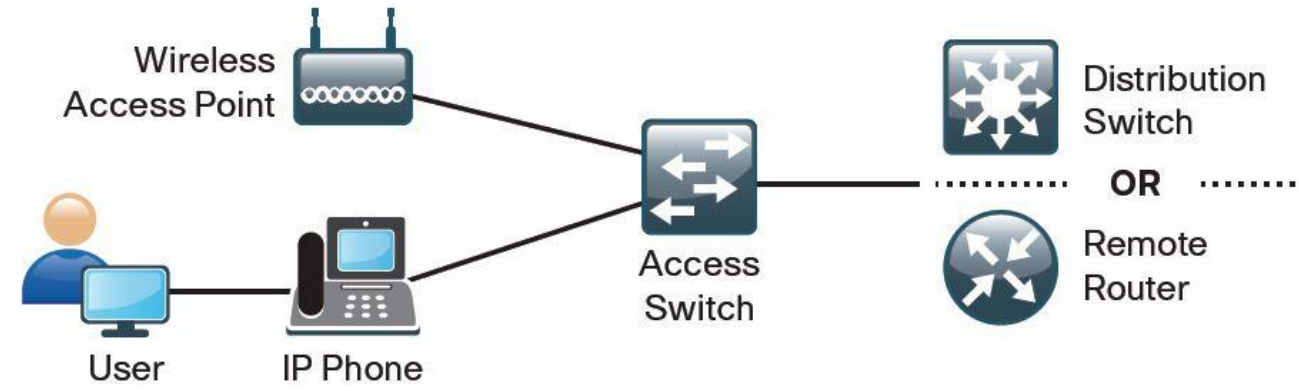


Рис. 2.1. Уровень доступа

2.1.1. УСТРОЙСТВА

Устройства уровня доступа это, как правило, коммутаторы второго уровня (L2) модели OSI, т.е. без функции маршрутизации. Коммутаторы осуществляют первичное сегментирование сети (технология VLAN). Однако в некоторых случаях могут применяться и устройства третьего

уровня (L3). Устройства уровня доступа должны предоставлять высокоскоростное проводное (Gigabit Ethernet) и беспроводное (802.11n) подключение к сети.

Оборудование которое может применяться в качестве уровня доступа:

Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot
Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E
Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports
Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports
Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports
Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports
Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports
Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports
Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports

2.1.2. УГРОЗЫ

Поскольку уровень доступа является входной точкой в сеть для клиентских устройств он в первую очередь должен обеспечивать защиту самих пользователей, корпоративных ресурсов и сеть от вредоносных атак со стороны подключаемых клиентов/устройств (в случае их заражения всевозможными вирусами) или хакеров, получивших доступ в локальную сеть.

Уровень доступа включает в себя следующие технологии защиты:

- DHCP-snooping - защищает пользователей от получения адреса от неизвестного DHCP-сервера, а так же не позволяет злоумышленнику захватить все ip-адреса.
- IP Source guard - защита от IP spoofing-а, т.е. от подмены IP-адреса источника.
- Port security - устанавливается ограничение на кол-во MAC адресов поступающих на порт коммутатора. Защищает от подмены MAC адреса и от атак, направленных на переполнение таблицы коммутации.
- Dynamic ARP inspection - защита от ARP spoofing-а, т.е. от перехвата трафика между компьютерами.

Более подробное рассмотрение технологий атак и защиты от них, выходит за рамки данного руководства.

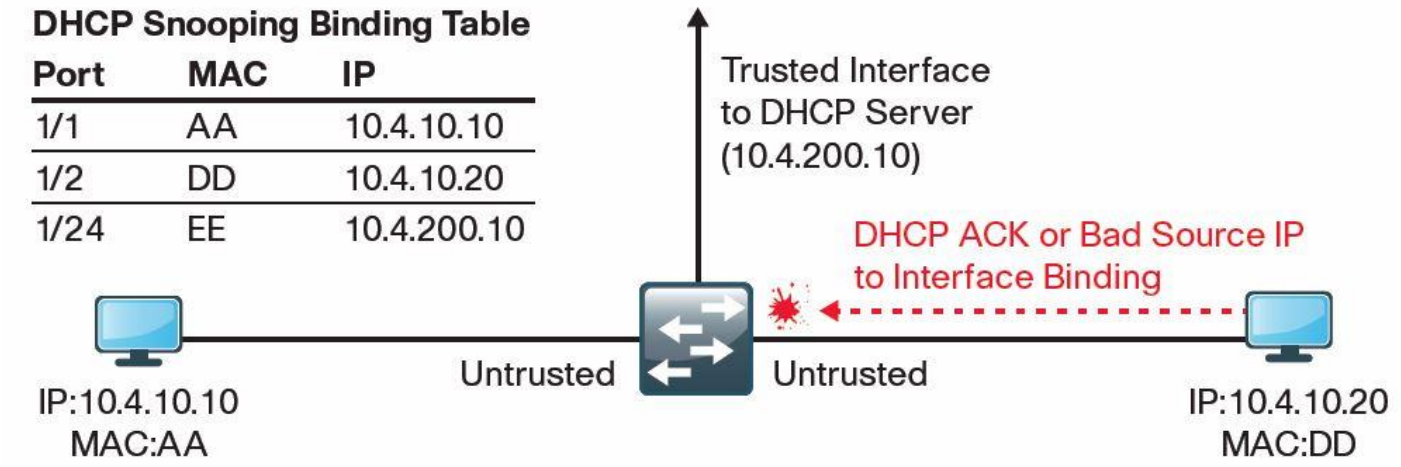


Рис. 2.2. DHCP-snooping и ARP Inspection

2.1.3. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

В случае если планируется подключение к сети таких устройств, как ip-телефоны, ip-видеокамеры или беспроводные точки доступа, будет разумным использовать коммутаторы с поддержкой технологии PoE (Power over Ethernet). Это существенно упростит и удешевит внедрение вышеуказанных устройств (исключается необходимость в дополнительном питании от электросети).

Наиболее экономичным решением являются коммутаторы Catalyst серии 2960. Решение на основе этих коммутаторов предоставляет самую низкую стоимость за порт (подключенного пользователя, сервера или какого-либо другого устройства), при этом обеспечивает весь необходимый функционал для уровня доступа (сегментирование сети, QoS, PoE, и т.д.). Использование коммутаторов уровня доступа позволяет существенно снизить затраты на подключение пользователей и серверов. В настоящий момент в линейке появилась новая, более производительная и современная модель Cisco Catalyst 2960-X, стоимость которой сопоставима со стоимостью предыдущей модели. При проектировании сетей будет уместным использование новых коммутаторов. Коммутаторы серии 3560, 3750, 4500 и 4507 применяются гораздо реже и только в том случае, когда покупка отдельного коммутатора для уровня доступа является нецелесообразной (малое количество пользователей). Данные коммутаторы больше подходят для уровня распределения.

В случае установки нескольких коммутаторов уровня доступа, расположенных в непосредственной близости (в одном серверном шкафу) рекомендуется использовать технологию стекирования (Рис. 2.3).

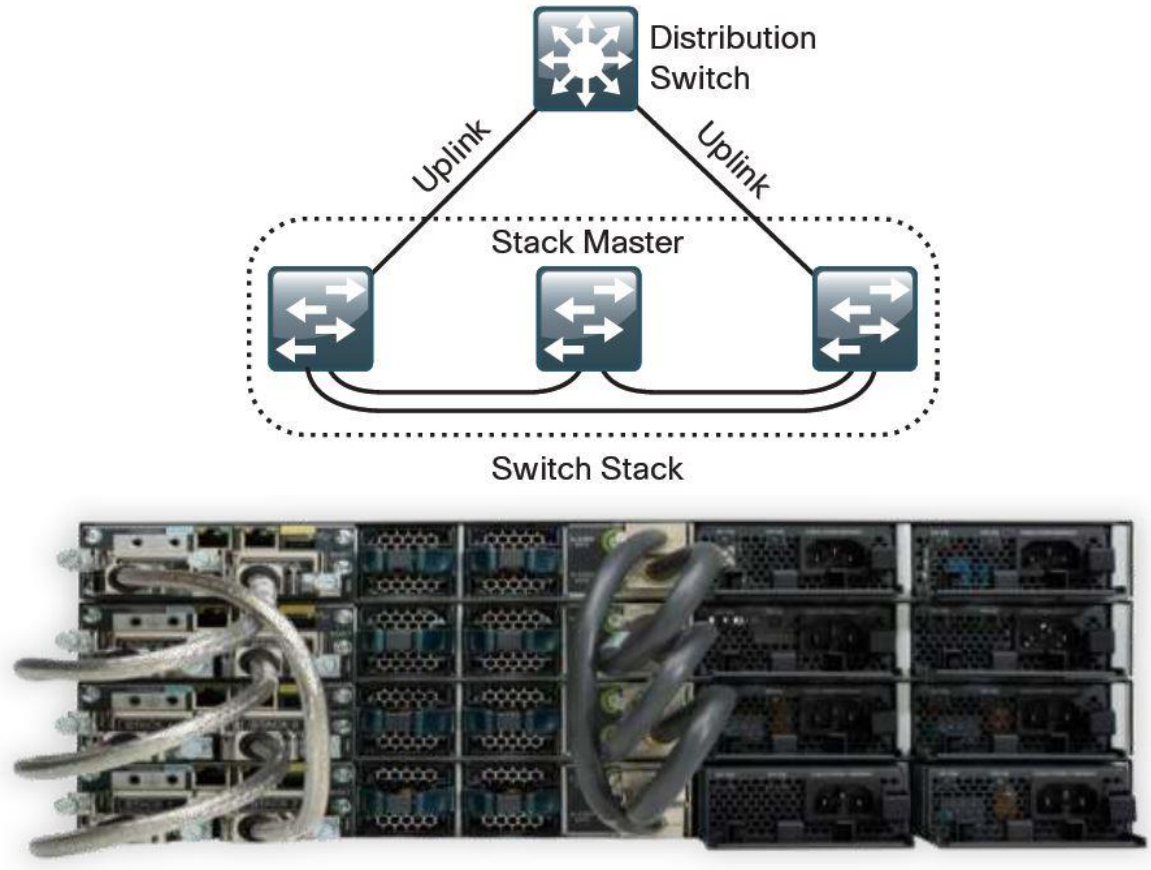


Рис. 2.3. Стек коммутаторов уровня доступа

Данная технология позволяет объединять оборудование в единое целое. Стек из трех 24-х портовых коммутаторов используется как одно устройство, имеющее 72 порта. Это существенно облегчает управление и конфигурирование, а так же реализует дополнительную отказоустойчивость. Однако следует отметить, что данное решение будет существенно дороже, т.к требует приобретения дополнительных модулей стекирования для коммутаторов серии 2960-S и 2960-X.

Каждый коммутатор уровня доступа должен подключаться к коммутаторам уровня распределения по агрегированному каналу (об этом чуть позже).

- Коммутаторы уровня доступа должны располагаться не более чем в 90 метрах от пользователей (коммутационный шкаф или серверная комната) для их подключения по витой паре.
- Если устройства уровня доступа находятся на расстоянии более чем 100 м от коммутаторов уровня распределения, то используется оптоволоконное соединение. Это стоит учитывать при проектировании и закладывать коммутаторы с поддержкой оптоволоконных подключений (технология SFP, SFP+).

2.1.4. АЛЬТЕРНАТИВЫ

Устройства уровня доступа являются самыми дешевыми в сетевой инфраструктуре, однако, их может быть большое кол-во, что ведет к большим затратам. Стоимость современного 24-х портового коммутатора компании Cisco (Catalyst 2960-X 24 GigE 4 x 1G SFP LAN Base) составляет около 2400$. При выборе других моделей стоит четко понимать какой функционал вам потребуется от устройств уровня доступа.

Коммутаторы второго уровня компаний D-link, Zyxel схожей конфигурации будут стоить дешевле в 2-3 раза. Такие коммутаторы подойдут для подключения серверов. Для подключения пользователей можно использовать более дешевые решения выше упомянутых компаний, но только в том случае, если требования к безопасности не слишком высоки. К примеру коммутаторы D-link и Zyxel очень распространены среди провайдеров интернет связи, ввиду своей дешевизны и достаточного для их задач функционала.

От себя хотелось бы добавить, что коммутаторы компании Cisco в крупном корпоративном сегменте стали практически стандартом.

2.2. УРОВЕНЬ РАСПРЕДЕЛЕНИЯ (DISTRIBUTION LAYER)

Уровень распределения обслуживает множество важных сервисов сети. Главной задачей уровня распределения является агрегация/объединение всех коммутаторов уровня доступа в единую сеть. Это позволяет существенно уменьшить количество соединений. Как правило, именно к коммутаторам распределения подключаются самые важные сервисы сети, другие модули сети: модуль сети Internet, модуль WAN сети, модуль дата-центра (Рис. 2.4).

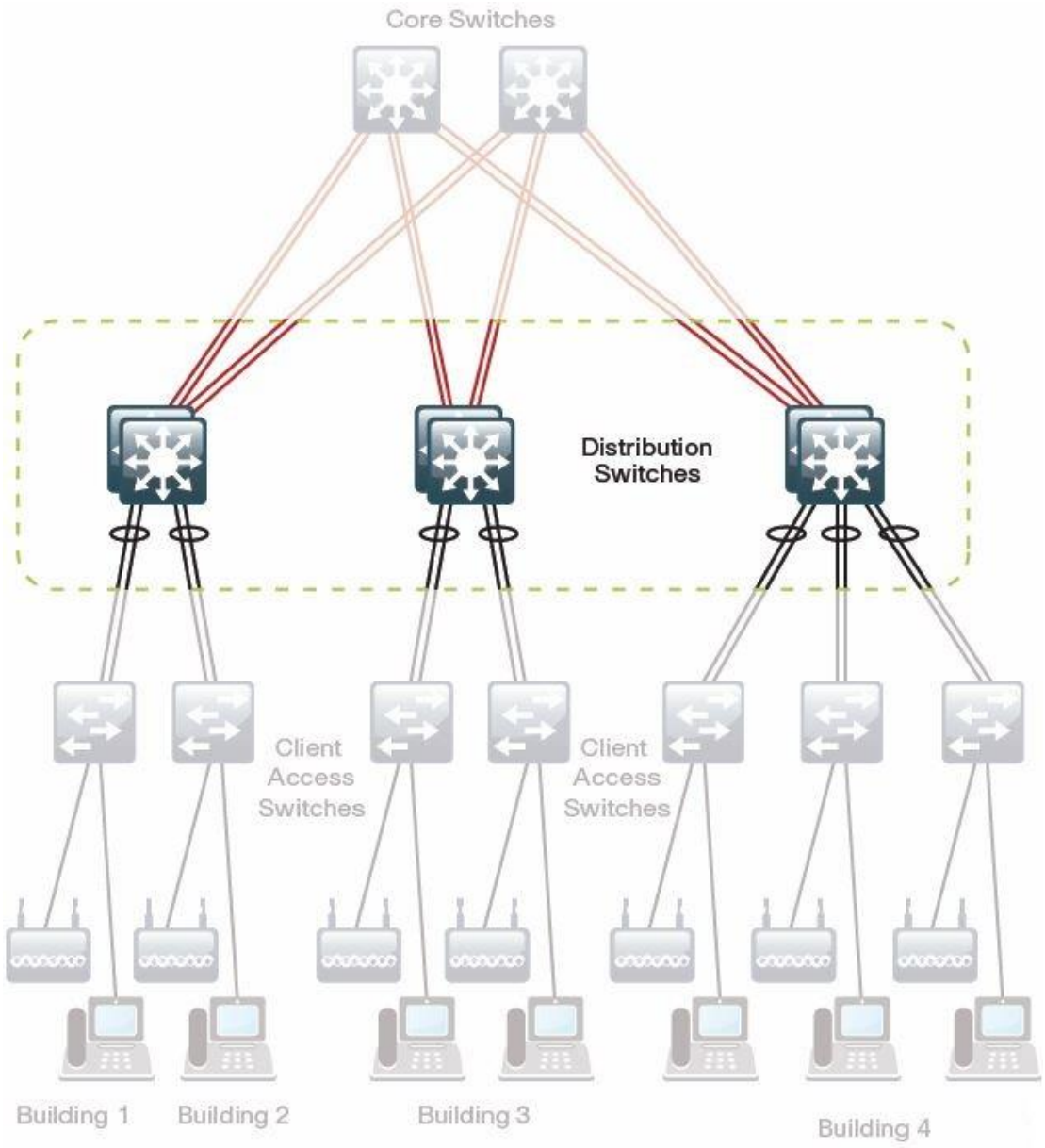


Рис. 2.4. Уровень распределения

2.2.1. УСТРОЙСТВА

Устройства уровня распределения это, как правило, коммутаторы третьего уровня (L3) модели OSI. Коммутаторы осуществляют маршрутизацию трафика между сегментами сети (между различными VLAN), а так же реализуют систему безопасности и сетевые политики (контроль доступа).

Оборудование которое может применяться в качестве уровня распределения:

Cisco Catalyst 6500 E-Series 6-Slot Chassis
Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4
Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4
Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4
Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4
Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module

Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot
Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps
Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module
Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module
Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports
Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module
Cisco Catalyst 3750-X Series Four GbE SFP ports network module

Так же можно использовать эти модели:
Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000
Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000

Однако, следует учитывать, что это Stand-Alone коммутаторы, т.е. не поддерживают технологию стекирования (в отличии от 3750-X), а значит высокопроизводительная и отказоустойчивая конфигурация не доступна при использовании коммутаторов этой модели.

2.2.2. УГРОЗЫ

Уровень распределения включает в себя следующие технологии защиты:

- Контроль доступа - атаки на корпоративные ресурсы ограничиваются политиками безопасности (списки доступа)
- Защита от IP spoofing-а

Как можно заметить, защита от угроз является второстепенной функцией уровня распределения. Основные функции описаны выше.

2.2.3. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Уровень распределения является очень важным звеном в работе всей сетевой инфраструктуры и требует высокопроизводительного, отказоустойчивого исполнения.

Модель Cisco SBA LAN предполагает использование технологии стекирования и агрегированных соединений межу сетевыми устройствами, в то время как традиционная модель использует принцип избыточности (redundant).

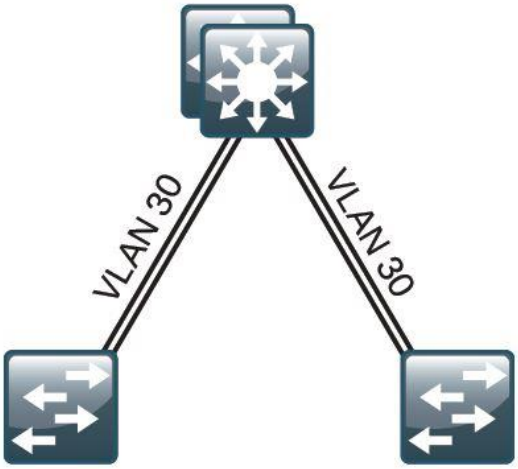


Рис. 2.5. Новая модель SBA LAN

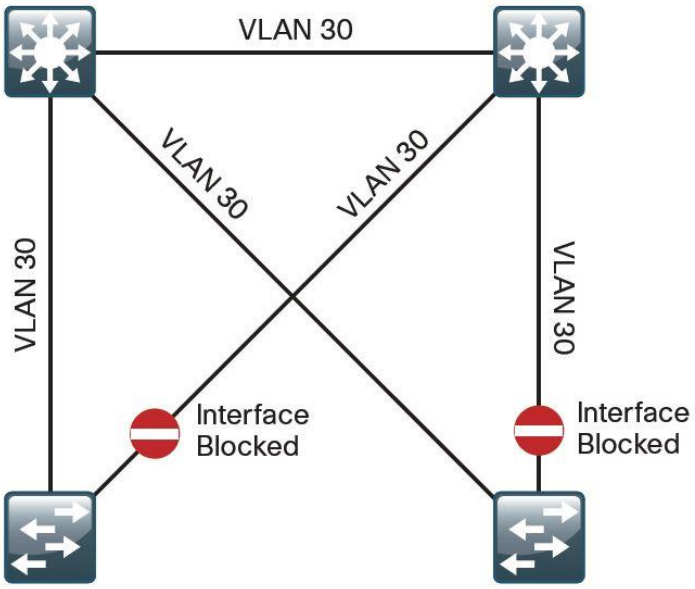


Рис. 2.6. Традиционная Избыточная модель

Новая модель SBA использует агрегированные каналы между устройствами уровня доступа и уровня распределения (с использование таких протоколов как EtherChannel) одновременно обеспечивая отказоустойчивость и более высокую производительность. Агрегированный канал является объединением 2-х, 3-х или более физических (проводных) соединений в одно логическое. При этом все соединения передают информацию, что существенно увеличивает пропускную способность канала (Рис. 2.5). В случае отказа одного из соединений, входящего в агрегированный канал, информация по прежнему передается по другим исправным соединениям без каких-либо перерывов в работе сети. Это выгодное отличие от традиционной Избыточной модели в которой блокируются дополнительные соединения (протокол STP, RSTP) для предотвращения петель (Рис. 2.6). Таким образом при использовании традиционной модели производительность не увеличивается, реализуется только отказоустойчивость.

Коммутаторы уровня распределения объединяются в стек (с использованием таких технологий как StackWise Plus). Агрегированный канал образуется при объединении портов разных коммутаторов стека (Рис. 2.7). Другими словами, логический интерфейс образуется объединением двух (или более) портов, при этом один порт принадлежит первому коммутатору стэка, а второй порт - второму. Оба порта участвуют в передаче трафика. Таким образом оказываются задействованными все устройства, обеспечивая высокую производительность и отказоустойчивость.

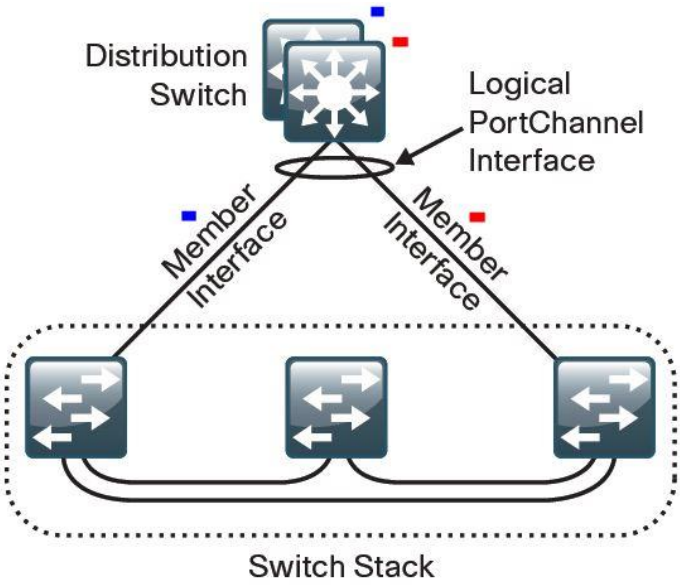


Рис. 2.7. Объединение портов стека коммутаторов в один PortChannel

В традиционной Избыточной (Redundant) модели сетевой трафик передает только одно устройство. Второе устройство становится активным только при падении первого, либо при отказе одного из активных соединений (сработает технология STP).

2.2.4. АЛЬТЕРНАТИВЫ

Для снижения затрат и общего числа устанавливаемых устройств можно объединить уровень распределения с уровнем ядра, если это позволяют размеры сети и требования к пропускной способности. Это довольно частая практика. Уровень распределения выступающий в качестве уровня ядра называется Collapsed core (Рис. 2.8).

В качестве альтернативного оборудования можно выбрать решения компании Juniper или HP. Данные компании является основными конкурентами компании Cisco в корпоративном сегменте. Коммутаторы Juniper и HP немного дешевле, однако если в сетевой инфраструктуре преобладают коммутаторы (а так же межсетевые экраны, IPS) компании Cisco, то не стоит "разводить зоопарк" из оборудования ради небольшой экономии. Гораздо проще управлять сетями, построенными на оборудовании одного вендора (особенно если это касается оборудования компании Cisco). Так же стоит учесть важность поддержки технологии стекирования.

Одним из самых дешевых решений являются коммутаторы компании D-Link. К примеру модель DGS-3120-24PC/B1ARI - L3 коммутатор, поддерживающий технологию стекирования.

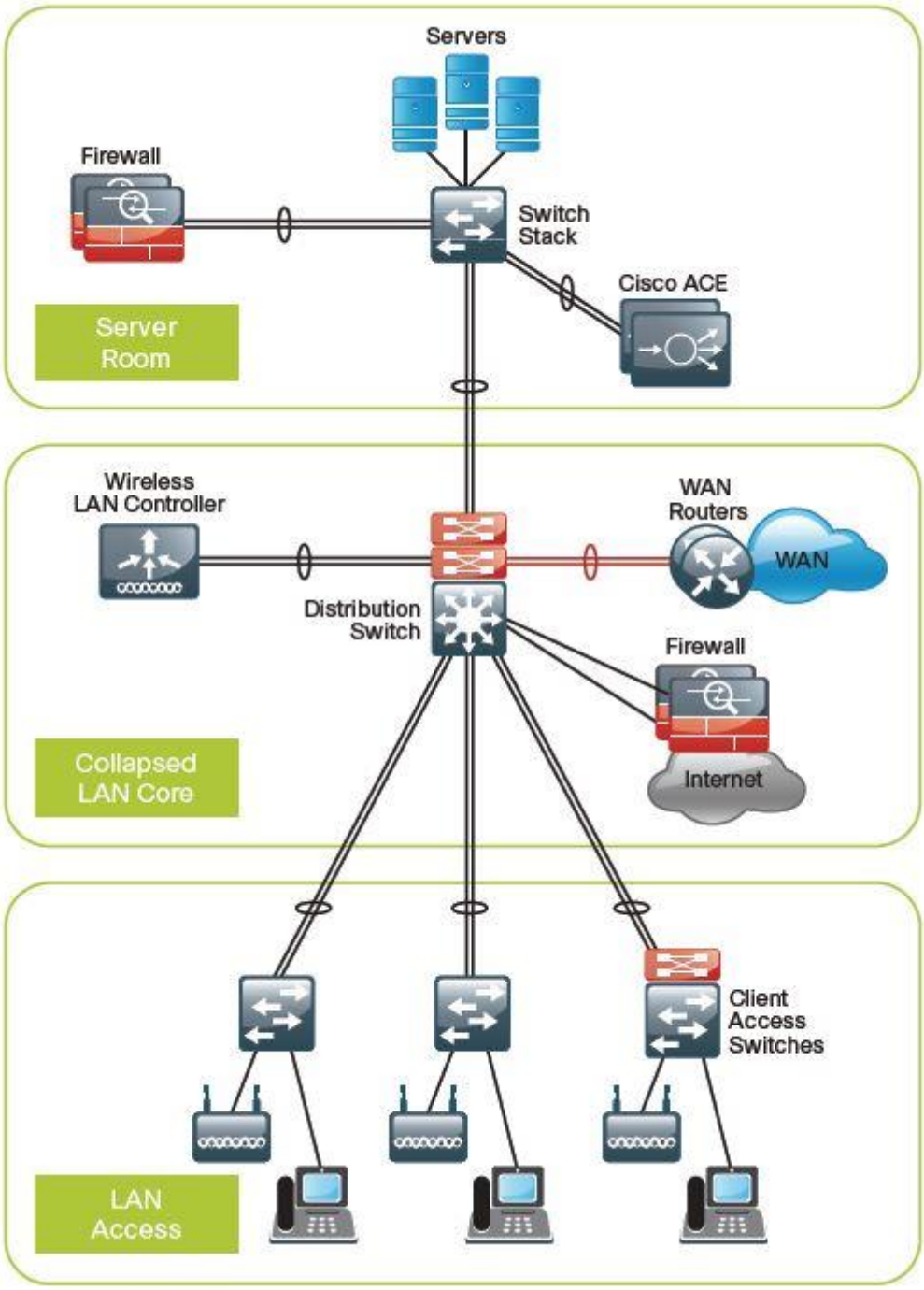


Рис. 2.8. Уровень распределения в качестве уровня ядра (Collapsed core)

2.3. УРОВЕНЬ ЯДРА (CORE LAYER)

Дизайн больших корпоративных сетей, охватывающих два и более зданий, обязывает использование Уровня Ядра. Главной задачей уровня ядра является агрегация/объединение всех коммутаторов уровня распределения в единую сеть. Это позволяет существенно уменьшить количество соединений. На Рис. 2.9 и 2.10 представлены дизайн сети, без и с уровнем ядра соответственно. Как видим, без использования уровня ядра количество соединений значительно больше.

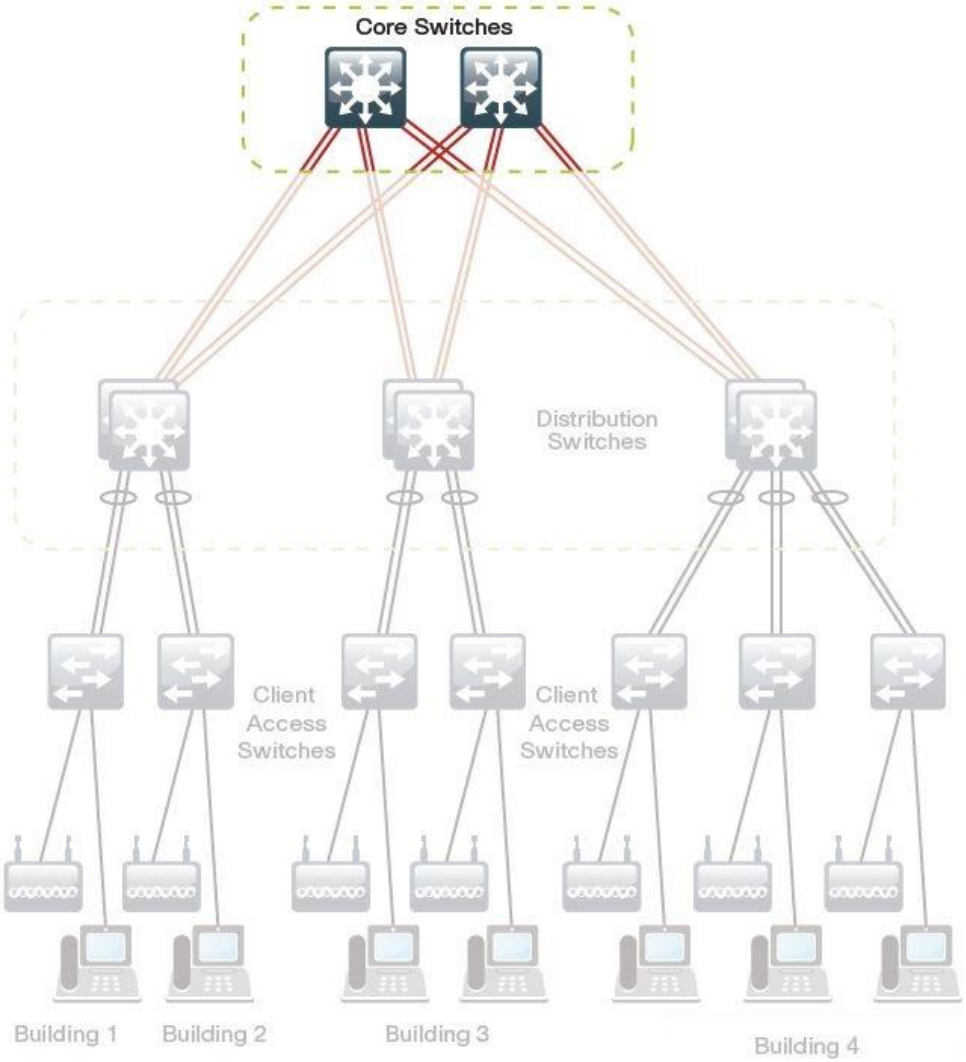


Рис. 2.9. Уровень Ядра (Core Layer)

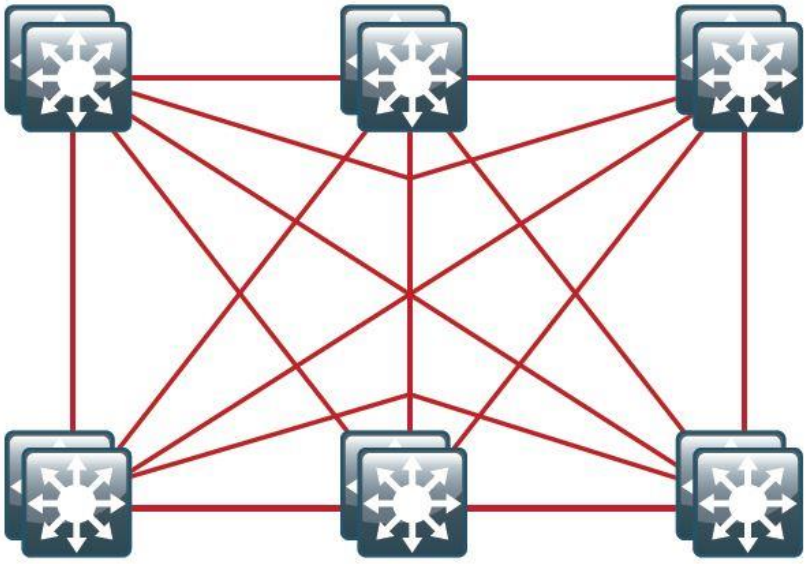


Рис. 2.10. Дизайн сети без уровня ядра

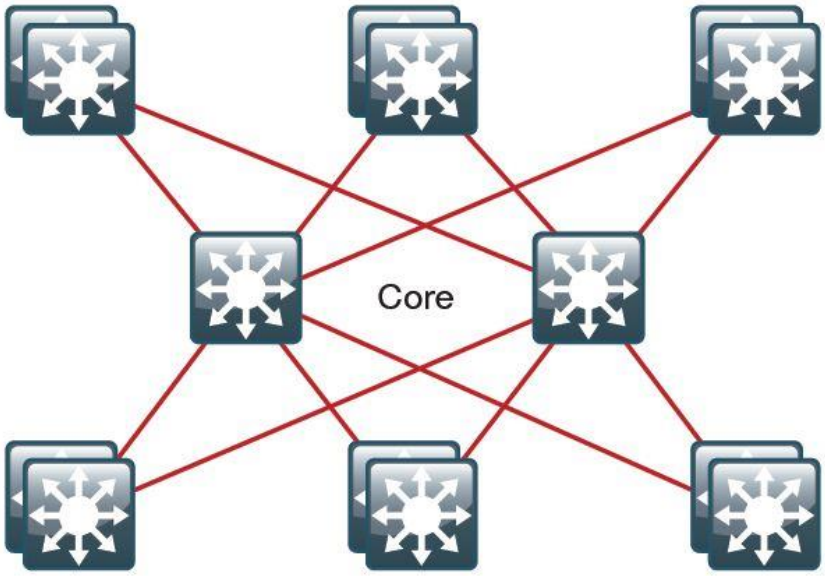


Рис. 2.11. Дизайн сети с уровнем ядра

2.3.1. УСТРОЙСТВА

Коммутаторы уровня ядра не должны выполнять каких-либо сложных действий. Их основная функция это маршрутизация трафика между модулями сети. Уровень ядра это, как правило, два коммутатора, подключение к которым осуществляется только на третьем уровне модели OSI, т.к. время сходимости на L3 уровне гораздо меньше чем на L2.

В качестве устройств уровня ядра применяются коммутаторы третьего уровня модели OSI (L3).

Оборудование которое может применяться в качестве уровня распределения:
Cisco Catalyst 6500 E-Series 6-Slot Chassis
Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4
Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4
Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4
Cisco Catalyst 6500 8-port 10GbE Fiber Module w/ DFC4

2.3.2. УГРОЗЫ

Что касается угроз, то обеспечение безопасности не входит в основные задачи уровня Ядра. Основная и главная функция уровня Ядра это маршрутизация трафика. Нагружать оборудование дополнительными задачами (списки доступа, port security, и т.д.) не рекомендуется, чтобы не снижать производительность сети.

2.3.3. РЕКОМЕНДАЦИИ ПО ДИЗАЙНУ

Важно понимать, что объединение в единую сеть нескольких зданий возможно только с использованием контролируемой зоны. Под контролируемой зоной понимается собственный

канал передачи данных (оптический канал, медный и т.д.). Т.е. если между двух зданий соединение осуществляется по специальному выделенному каналу (который находится в контролируемой зоне) то в этом случае можно организовывать Уровень ядра. Если же два здание соединены по средствам Интернет канала, то в этом случае стоит применять специальный для этого модуль - либо модуль Интернет (Internet Edge) либо модуль сети WAN (WAN area), о которых мы поговорим позже.

К уровню ядра подключаются все модули сети (все коммутаторы уровня распределения). В общем виде схема подключения представлена на рисунке 2.12.

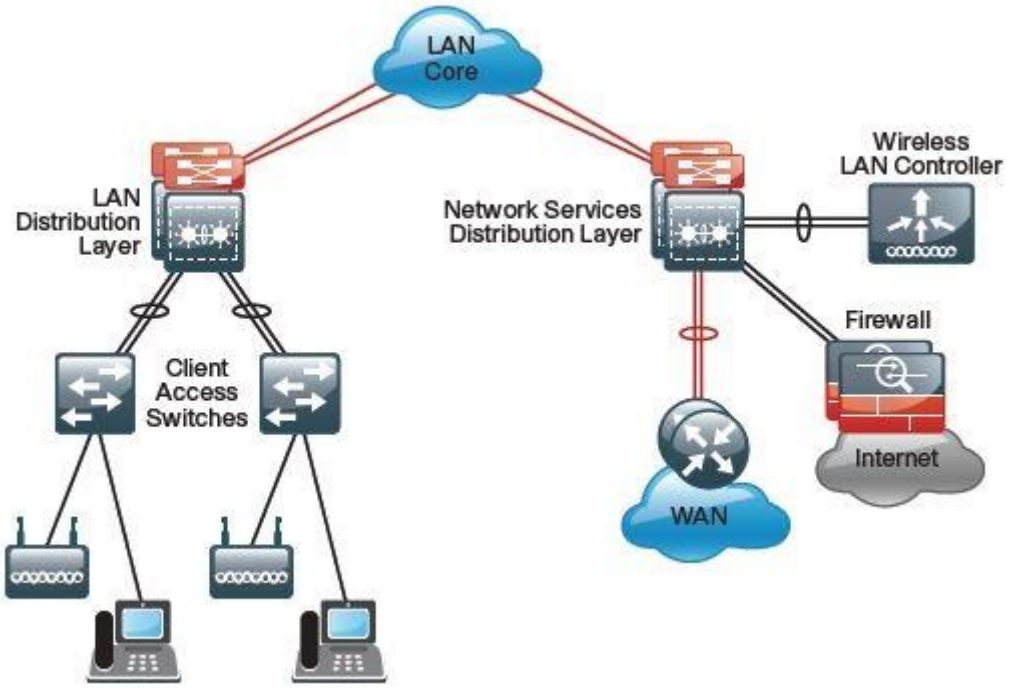


Рис. 2.12. Подключение модулей сети к уровню ядра

Коммутаторы уровня ядра должны обладать самой высокой пропускной способностью среди всех коммутаторов вашей сети (от 40 Гбит/с). Все коммутаторы уровня распределения и любые другие модули должны подключаться к обоим коммутаторам уровня яда, таким образом обеспечивая отказоустойчивость. Подключение осуществляется с использованием технологий EtherChannel, что позволяет балансировать поток трафика. На рисунке 2.13 представлен пример использования уровня Ядра.

2.3.4. АЛЬТЕРНАТИВЫ

Коммутаторы уровня Ядра являются самыми дорогими устройствами в иерархической модели сети (если рассматривать только коммутаторы и не брать в расчет устройства безопасности). Далеко не каждая организация может себе позволить данные устройства. Однако при необходимости использования уровня Ядра, в первую очередь нужно определиться с пропускной способностью, которая требуется от оборудования. Возможно, что для ваших целей подойдут устройства из более дешевого сегмента (например коммутаторы уровня распределения). Так же необходимо понимать, что одним из важнейших параметров уровня Ядра является отказоустойчивость, т.к. от устройства данного уровня зависит работа огромной

сети (в маленьких сетях уровень ядра обычно отсутствует или же интегрирован с уровнем распределения). Поэтому при выборе оборудования стоит обращать внимание на технологии организации отказоустойчивости, резервирования питания. Лидерами среди коммутаторов уровня ядра являются компании: Cisco, Juniper, HP, Brocade, Extreme Networks. Однако есть и более дешевые решения уровня ядра от компании D-Link.

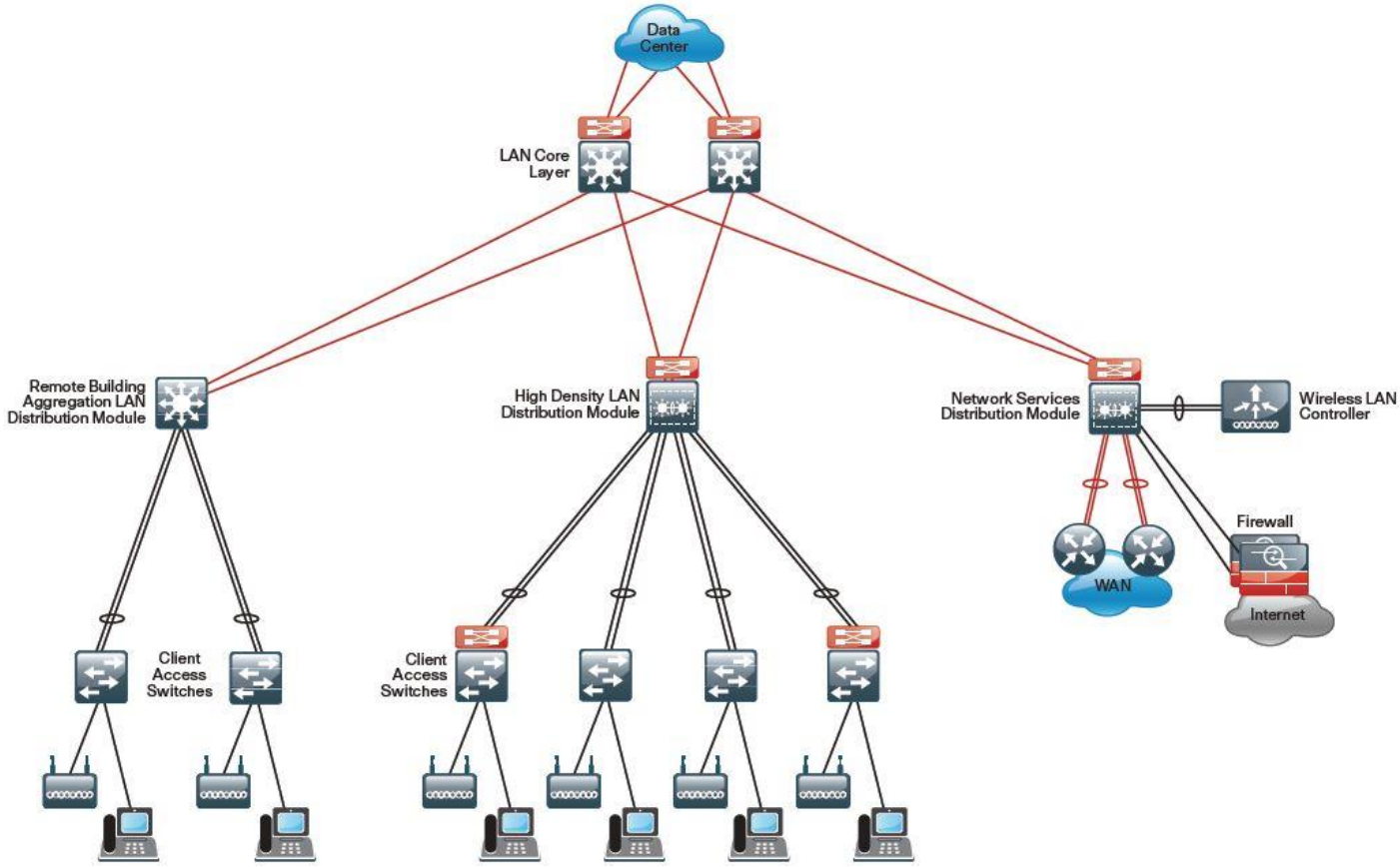


Рис. 2.13. Пример использования Уровня Ядра (LAN Core Layer)

3. МОДУЛИ КОРПОРАТИВНОЙ СЕТИ

Освоив иерархическую модель и построив “скелет” сети можно переходить к внедрению остальных корпоративных модулей. В этом и заключается одно из главных преимуществ модульной архитектуры - построение сети осуществляется небольшими, простыми для понимания, частями.

4. МОДУЛЬ СЕТИ ИНТЕРНЕТ

Трудно представить современную компанию без наличия доступа к сети Internet. Огромное количество бизнес процессов завязаны на использование интернет ресурсов (web-сайты, электронная почта и т.д.). Соответственно доступ в Internet должен быть стабильным и безопасным. Именно для этого используется Модуль сети Интернет (или, как еще его называют - Internet Edge).

Модуль сети Интернет в свою очередь разбивается на несколько функциональных блоков, обеспечивающих работу определенных сервисов. Таким образом организация может внедрять данные блоки исходя из бизнес потребностей.

Современный Модуль сети Интернет должен включать в себя следующие функциональные блоки:

- Межсетевой экран (МЭ) - осуществляет контроль доступа между различными сегментами сети (сегмент серверов, сегмент пользователей и т.д.), а также предоставляет другие сетевые сервисы, такие как NAT и организация DMZ.
- Система предотвращения вторжений (IPS) - проверяет (инспектирует) трафик на предмет подозрительной и аномальной активности.
- Удаленный доступ (Remote access или RA VPN) - предоставление безопасного удаленного доступа к локальным корпоративным ресурсам, не зависимо от местонахождения пользователя.
- Защита электронной почты - защита от спама и писем, содержащих вредоносный код.
- Веб-защита - контроль использования интернет ресурсов и обеспечение безопасности пользователя в сети Интернет.

Ключевое отличие модульной архитектуры - масштабируемость, эффективность и устойчивость. Каждый блок Модуля сети Интернет независим от остальных. Таким образом вы можете использовать только необходимые вашему бизнесу блоки, создавая свой собственный дизайн сети.

На рисунке 4.1 представлен пример реализации Модуля сети Интернет (Internet Edge).

Рис. 4.1. Пример дизайна Модуля сети Интернет