

Начинающему СІО: архитектура сети (часть 1)



Евгения ШУМИЛОВА,
ведущий инженер компании
CompTek

В первой статье этой серии («Начинающему СІО: построение ЛВС центрального офиса», Connect! № 12/2007) были подробно рассмотрены четыре основные группы функциональных характеристик современных ЛВС – производительность, надежность, безопасность и управляемость, а также основные технологии и механизмы, способные обеспечить должный уровень этих характеристик. Сегодня начнем разговор непосредственно об архитектуре сети. Напомним, что в статьях серии «Начинающему СІО» рассматривается относительно небольшая корпоративная сеть, в которой находится до 500 рабочих мест.

К основным факторам, определяющим выбор архитектуры сети, следует отнести следующие:

- высокая доступность – всегда должен быть предусмотрен резервный путь для передачи тра-

фика в случае неполадки или отказа части сети;

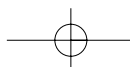
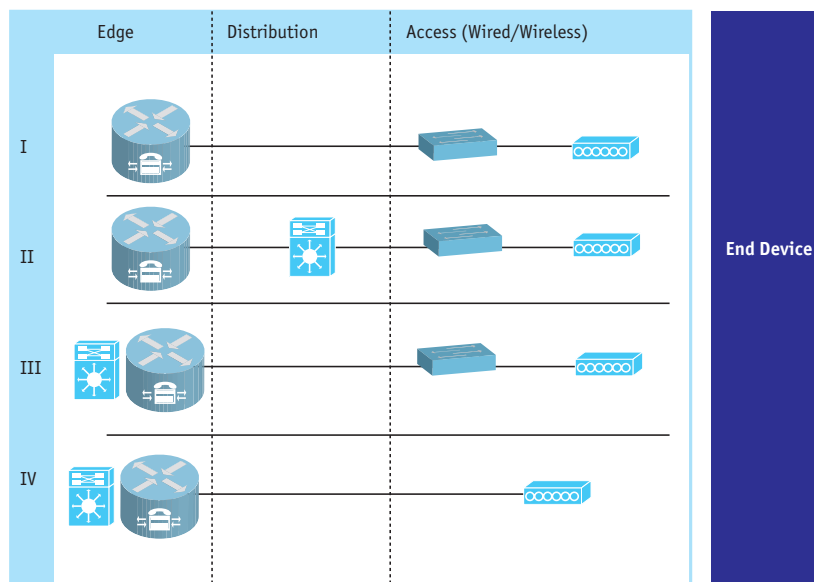
- масштабируемость – архитектура сети должна обеспечивать возможность адаптации к увеличению количества пользователей и сервисов без

серьезных изменений структуры;

- безопасность – сеть должна быть закрыта для доступа неавторизованных пользователей и защищена от сетевых атак;



Рис. 1. Уровни и варианты структуры ЛВС



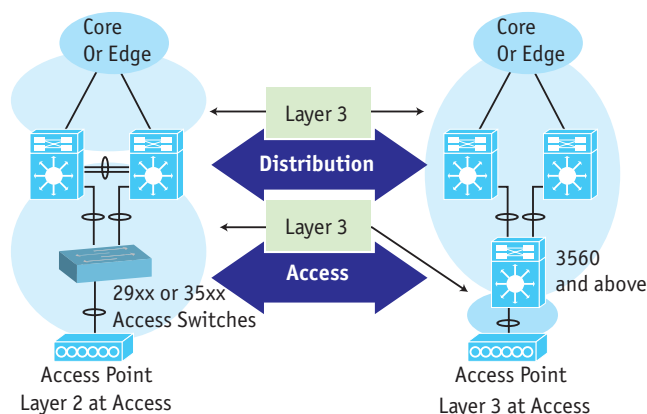
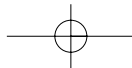


Рис. 2. Варианты построения уровня доступа

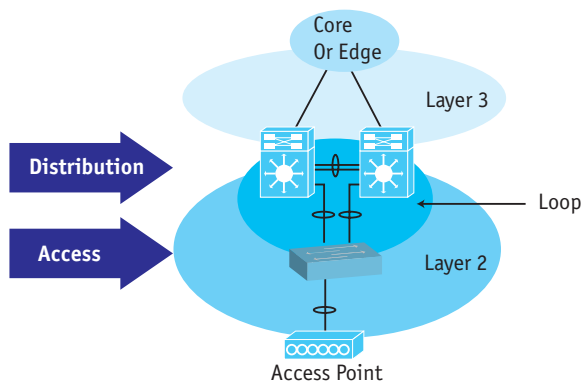


Рис. 3. Традиционная архитектура сети

• управляемость – архитектура сети должна обеспечивать простоту ее развертывания и поиска неисправностей, а возможности управления сетью не должны снижать общий уровень безопасности и надежности.

Мы рекомендуем многоуровневую архитектуру сети, которая имеет множество плюсов. Каждое сетевое устройство на своем уровне выполняет нужные функции, что упрощает конфигурирование сети и управление ею. Многоуровневая архитектура упрощает процессы поиска неисправностей в сети и ее отладки. Она позволяет разделить трафик между уровнями и снизить загрузку процессоров маршрутизаторов. Когда требуется, такая архитектура дает возможность интегрировать различные технологии без изменения структуры сети. Наконец, она обеспечивает простое масштабирование сети.

С точки зрения архитектуры локальная сеть может быть разделена на следующие уровни:

- уровень доступа, который обеспечивает подключение конечных пользователей через проводную либо беспроводную инфраструктуру. На этом уровне обеспечиваются такие сервисы, как безопасность (на канальном уровне L2) и аутентификация;
- уровень распределения, на котором могут задаваться пользовательские настройки (в частности, через DHCP), осуществ-

ляться маршрутизация трафика (на сетевом уровне L3) и сегментация сети. Этот уровень может использоваться для дополнительных сервисов. Например, на нем может работать беспроводной контроллер точек доступа или межсетевой экран;

- пограничный уровень, защищающий от вторжений и атак (межсетевой экран, системы обнаружения и предотвращения вторжений), обеспечивающий голосовые сервисы и выход в WAN-сеть.

Различные уровни и варианты структуры сети показаны на рис. 1.

Уровень доступа

На этом уровне пользователь подключается к сети, используя проводное или беспроводное соединение. На нем обычно функционируют следующие сервисы:

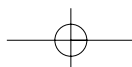
- разделение трафика по двум виртуальным ЛВС – голосовой VLAN и VLAN данных;
- защита от атак на канальном уровне (L2);
- приоритизация трафика и обеспечение качества обслуживания (QoS), в частности, для предотвращения атак типа отказ в обслуживании (DoS) и др.;
- аутентификация с использованием механизмов 802.1x и IBNS;
- гостевой доступ или гостевой VLAN;
- контроль доступа к сети (NAC), в частности, для защиты от вирусов.

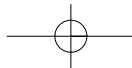
Существует два основных варианта построения уровня доступа: можно либо использовать в плоской сети коммутаторы L2, либо включить маршрутизацию (L3) и задействовать технологию VLAN для распределения пользователей по группам. Эти варианты показаны на рис. 2.

Уровень доступа с использованием устройств L2

Обычно коммутаторы работают на канальном уровне (L2), что может привести к проблемам с протоколом остоного дерева (Spanning Tree Protocol – STP): во-первых, усложняется поиск неисправностей, во-вторых, в сложной сети время сходимости увеличивается в случае изменения топологии. Эти трудности характерны для традиционной архитектуры сети, в которой два коммутатора уровня распределения и коммутатор уровня доступа оказываются вовлечены в петлю L2, как показано на рис. 3.

Коммутатор доступа (L2) соединен с обоими коммутаторами уровня распределения, которые соединены между собой посредством технологии EtherChannel. Обычно топология сети L2 организуется таким образом, что протокол STP блокирует избыточные соединения, и трафик может без проблем передаваться не только в





CONNECT!

ТЕХНОЛОГИИ

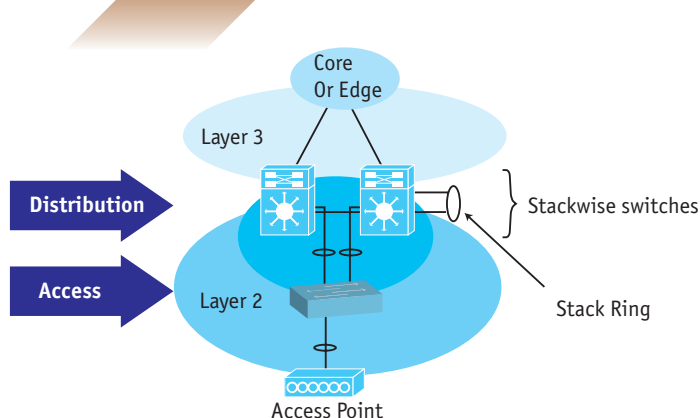


Рис. 4. Альтернативный способ построения уровня доступа

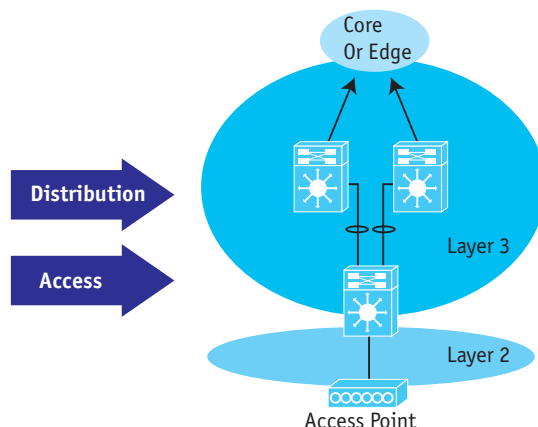


Рис. 5. Пример построения уровня доступа с использованием устройств L3

режиме нормальной работы, но и при возникновении неисправности в сети. Проблема большого времени сходимости решается за счет использования протокола RSTP (Rapid Spanning Tree Protocol), который перестраивает топологию в течение нескольких секунд после отказа канала или устройства. Ошибки в конфигурации могут усложнить устранение неисправностей, но при наличии документации не должны стать серьезной проблемой для обученного инженера.

На рис. 4 показан иной способ построения уровня доступа с применением устройств L2.

посредством технологии Ether-Channel. В этой топологии нет петель L2, но протокол STP все равно должен быть включен на случай их возникновения.

Уровень доступа с использованием устройств L3

Использование функциональности L3 на уровне доступа открывает новые возможности. В таком решении маршрутизация включена, но пользователи по-прежнему распределяются по VLAN. Необходимо, чтобы

менее секунды, например, при использовании протокола EIGRP.

Однако в общем случае не рекомендуется разворачивать данную архитектуру в небольших сетях. Основная причина – высокая стоимость такого решения. Кроме того, решения L2 на уровне доступа предоставляют возможность «беспшовной» интеграции различных сервисов.

Включение маршрутизации на уровне доступа максимально уменьшает размер домена L2, в котором пользователи распределяются по VLAN-сетям. В таком случае исключены петли L2, и можно даже отключить протокол STP для ускорения процесса отладки. В части домена L2 данное решение не требует значительной поддержки и характеризуется быстрым временем сходимости. Поэтому если более высокая стоимость, характерная для устройств L3, не является для вас существенным фактором, вы вполне можете выбрать данный вариант.

Итак, мы проанализировали особенности построения уровня доступа локальной вычислительной сети с использованием как традиционных коммутаторов (L2), так и маршрутизирующих коммутаторов с функциональностью L3. В следующей статье будут рассмотрены технологии VLAN и QoS, а также специфика построения уровня распределения. ■

Многоуровневая архитектура упрощает процессы поиска неисправностей в сети и ее отладки.

В такой топологии на уровне распределения используются стековые коммутаторы с протоколом HSRP. Эта топология более устойчива и масштабируема. Здесь коммутаторы, обеспечивающие возможность резервирования на сетевом уровне (L3), объединены в стек. Высокий уровень доступности между уровнем доступа и уровнем распределения обеспечен

платформа, устанавливаемая на уровне доступа, поддерживала и маршрутизацию, и коммутацию (рис. 5). Коммутатор доступа имеет несколько каналов, равнозначных по стоимости (с точки зрения маршрутизации трафика), в сторону магистрального или пограничного устройства. В случае отказа сервиса время сходимости составит

