Содержание

Глава 14

Сетевые аппаратные средства

Независимо от того, работают ваши системы в центре обработки данных, в облаке или пусковой ракетной шахте, у них есть нечто общее — необходимость обмена информацией по сети. Возможность быстрой и надежной передачи данных необходима в любой среде. Если есть область, в которой технология UNIX затронула человеческие жизни и повлияла на другие операционные системы, то она связана с практической реализацией крупномасштабного пакетированного транспорта данных.

Сети проходят такую же эволюцию, как и серверы, поскольку физические и логические представления сети все больше разделяются уровнем виртуализации, имеющим собственную конфигурацию. В облаке такие конфигурации являются стандартными, но даже физические центры обработки данных в настоящее время часто включают в себя слой программно конфигурируемых сетей (software-defined networking — SDN).

Администраторы взаимодействуют с сетевым оборудованием реального мира менее часто, чем когда-то, но знакомство с традиционными сетями остается решающим навыком. Виртуализированные сети тесно имитируют физические сети в своих функциях, терминологии, архитектуре и топологии.

Многие сетевые технологии продвигались в течение долгих лет, но в результате появился очевидный победитель — Ethernet. Сегодня технологию Ethernet можно встретить всюду: от игровых приставок до холодильников. Глубокое понимание принципов работы этой системы чрезвычайно важно для успешной работы системного администратора.

Совершенно очевидно, что быстродействие и надежность сетей непосредственно влияют на результаты деятельности компаний. Однако в настоящее время сетевые технологии настолько вездесущи, что состояние сети может повлиять на возможность вза-

имодействия между людьми, например возможность делать телефонные звонки. Плохая организация сети — это личная и профессиональная неудача, которая может иметь катастрофические социальные последствия. Кроме того, устранение этих недостатков порой обходится очень дорого.

Успешное создание сети зависит от по крайней мере четырех важнейших факторов:

- разработки разумной структуры сети;
- выбора высококачественного оборудования;
- правильной инсталляции и документирования;
- компетентной эксплуатации и сопровождения.

В этой главе рассматриваются принципы, инсталляция и функционирование сетей Ethernet. Мы также кратко опишем такие устаревшие технологии, как DSL (Digital Subscriber Line), которые обычно предстают перед конечными пользователями в облике — сюрприз! — технологии Ethernet.

14.1. Технология Ethernet: сетевая панацея

Захватив более 95% мирового рынка локальных сетей (Local Area Network — LAN), технология Ethernet в самых разных формах проявляется почти всюду. Разработку стандарта Ethernet начал Боб Меткалф (Bob Metcalfe) из Массачусетского технологического института в рамках своей кандидатской диссертации, но в настоящее время она описана во многих стандартах IEEE.

В первоначальной спецификации Ethernet была определена скорость передачи данных 3 Мбит/с (мега*бит* в секунду), но почти сразу же она выросла до 10 Мбит/с. Как только в 1994 году была закончена работа над стандартом, предусматривавшим скорость 100 Мбит/с, стало ясно, что технология Ethernet будет лишь эволюционировать, а не вытесняться новой технологией. Это вызвало гонку технологий, в ходе которой производители старались создать все более быстродействующую версию Ethernet, и это соревнование еще не закончено. Основные этапы эволюции различных стандартов Ethernet приведены в табл. 14.1[1].

Таблица 14.1. Эволюция Ethernet

Год	Скорость	Название стандарта	Номер IEEE	Расстояние	Средство передачи[a]
1973	3 Мбит/с	Xerox Ethernet	–	?	Коаксиальный кабель
1976	10 Мбит/с	Ethernet 1	–	500 м	Коаксиальный кабель RG-11
1989	10 Мбит/с	10BASE-T	802.3	100 м	Медный кабель НВП категории 3
1994	100 Мбит/с	100Base-TX	802.3u	100 м	Медный кабель НВП категории 5
1999	1 Гбит/с	1000BASE-T (“gigabit”)	802.3ab	100 м	Медный кабель НВП категорий 5e и 6
2006	10 Гбит/с	10GBASE-T (“10 Gig”)	802.3an	100 м	ВП категории 6a, 7, НВП категории 7a
2009	40 Гбит/с	40GBASE-CR4	P802.3ba	10 м	Медный кабель НВП
		40GBASE-SR4		100 м	ММ-оптоволокно

[1]Мы не упомянули несколько менее популярных стандартов.

Окончание табл. 14.1

Год	Скорость	Название стандарта	Номер IEEE	Расстояние	Средство передачи[а]
2009	100 Гбит/с	100GBASE-CR10	P802.3ba	10 м	Медный кабель НВП
		100GBASE-SR10		100 м	ММ-оптоволокно
2018[б]	200 Гбит/с	200GBASE-FR4	P802.3bs[в]	2 км	CWDM-оптоволокно
		200Gbase-LR4		10 км	CWDM-оптоволокно
2018[б]	400 Гбит/с	400GBASE-SR16	P802.3bs	100 м	ММ-оптоволокно (16 жил)
		400Gbase-DR4		500 м	ММ-оптоволокно (4 жилы)
		400GBASE-FR8		2 км	CWDM-оптоволокно
		400Gbase-LR8		10 км	CWDM-оптоволокно
2020[б]	1Тбит/с	TbE	TBD	TBD	TBD

[а] ММ — многомодовое, НВП — неэкранированная витая пара, ВП — витая пара, CWDM — разреженное спектральное мультиплексирование.

[б] Промышленный проект.

[в] Мы немного сомневаемся и предполагаем, что этот вариант кодировки был неудачным совпадением.

Как работает Ethernet

Технологию Ethernet можно представить в виде великосветского раута, на котором гости (компьютеры) не перебивают друг друга, а ждут паузы в разговоре (отсутствия трафика в сетевом кабеле), чтобы заговорить. Если два гостя начинают говорить одновременно (т.е. возникает конфликт), оба они останавливаются, извиняются друг перед другом, ждут немного, а затем один из них начинает говорить снова.

В технической терминологии такая схема называется CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов). Смысл этого названия заключается в следующем:

- контроль несущей (CS) — вы можете говорить одновременно с другими;
- множественный доступ (MA) — говорить могут все;
- обнаружение конфликтов (CD) — вы знаете, когда перебиваете кого-то.

Фактическая задержка при обнаружении конфликтов является случайной. Это позволяет избежать такого развития событий, при котором два компьютера одновременно передают сообщения в сеть, обнаруживают коллизию, ждут некоторое время, а затем синхронно возобновляют передачу, переполняя, таким образом, сеть конфликтами.

В настоящее время важность соглашений CSMA/CD осознали даже приверженцы коммутаторов, которые обычно ограничивают количество хостов в домене, в котором происходят коллизии, до двух. (Если продолжить аналогию с великосветским раутом, можно описать этот вариант как ситуацию, в которой два собеседника, как в старом кино, чопорно сидят на противоположных концах длинного обеденного стола.)

Топология Ethernet

С точки зрения топологии сеть Ethernet представляет собой разветвляющуюся шину, но без петель. У пакета есть только один путь следования между любыми двумя хостами, расположенными в одной сети. В сети Ethernet могут передаваться пакеты трех типов: однонаправленные (unicast), групповые (multicast) и широковещательные (broadcast). Пакеты первого типа адресованы одному хосту, второго — группе хостов, третьего — всем хостам сегмента.

Широковещательный домен — это совокупность хостов, которые принимают пакеты, направляемые по аппаратному широковещательному адресу. В каждом логическом сегменте сети Ethernet существует только один широковещательный домен. В ранних стандартах Ethernet и средствах передачи (например, 10Base5) понятия физического и логического сегментов были тождественными, поскольку все пакеты передавались по одному большому кабелю, в который втыкались сетевые интерфейсы компьютеров[2].

С появлением современных коммутаторов логические сегменты стали включать в себя множество (десятки и даже сотни) физических сегментов, к которым подключено всего два устройства: порт коммутатора и компьютер. Коммутаторы отвечают за доставку групповых и однонаправленных пакетов в физический сегмент, где расположен нужный адресат (адресаты); широковещательные пакеты направляются во все сетевые порты логического сегмента.

С появлением коммутаторов сегодняшние логические сегменты обычно состоят из многих физических сегментов (возможно, десятков или сотен), к которым подключены только два устройства: порт коммутатора и хост.[3] Коммутаторы несут ответственность за сопровождение многоадресатных и одноадресатных пакетов к физическим (или беспроводным) сегментам, на которых находятся предполагаемые получатели. Широковещательный трафик пересылается всем портам в логическом сегменте.

Логический сегмент может состоять из физических сегментов, имеющих разную скорость передачи данных. Следовательно, коммутаторы должны иметь средства буферизации и синхронизации для предотвращения возможных конфликтов.

Неэкранированная витая пара

Неэкранированная витая пара (НВП) — самая популярная среда передачи данных в сетях Ethernet. Общая схема сети на основе НВП изображена на рис. 14.1.

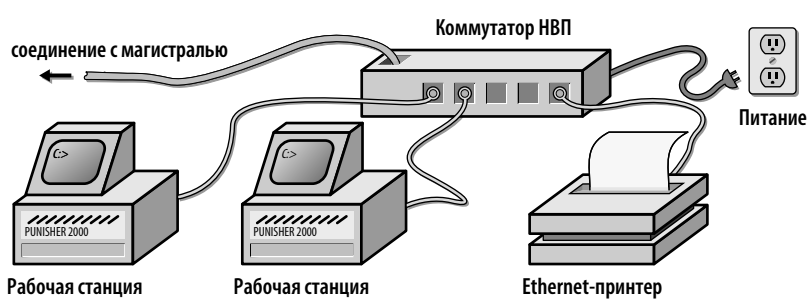

Рис. 14.1. Схема сети на основе НВП

[2]Мы не шутим! Подключение нового компьютера к сети предполагало прокалывание отверстия в изоляции кабеля с помощью специального соединителя, называемого «зуб вампира», который позволял добраться до центрального проводника. Этот соединитель затем зажимался винтами.

[3]Беспроводные сети — еще один распространенный тип логического сегмента Ethernet. Они ведут себя, скорее, как традиционные формы Ethernet, которые используют один кабель для соединения многих хостов сети (см. раздел 14.2).

Провода, используемые в современных локальных вычислительных сетях на основе неэкранированной витой пары, обычно подразделяют на восемь категорий. Эта система оценки параметров была впервые введена компанией Anixter, крупным поставщиком кабельной продукции, и впоследствии стандартизирована организацией TIA (Telecommunications Industry Association — ассоциация телекоммуникационной промышленности). Сегодня выделяются категории 1–7 и промежуточные категории 5e и 6a.

Организация ISO (International Organization for Standartization — Международная организация по стандартизации) тоже подключилась к процессу стандартизации кабелей и предложила собственную классификацию, которая почти в точности повторяет классификацию TIA. Например, кабель категории 5 в системе TIA эквивалентен кабелю класса D в системе ISO. Для наглядности в табл. 14.2 подытожены ключевые различия между основными современными стандартами кабелей. Эта таблица поможет вам произвести впечатление на своих друзей во время вечеринки.

Таблица 14.2. Характеристики кабелей НВП

Параметр[a]	Единица измерения	Категории						
		5 D[б]	5e	6 E	6a EA	7 F	7a FA	8 I
Ширина полосы	МГц	100	100	250	500	600	1000	2000
Затухание	дБ	24	24	21,7	18,4	20,8	60	50
NEXT	дБ	27,1	30,1	39,9	59	62,1	60,4	35,6
ELFEXT	дБ	17	17,4	23,2	43,1	46,0	35,1	–
Затухание отраженного сигнала (обратная потеря)	дБ	8	10	12	32	14,1	61,93	8
Задержка распространения сигнала	нс	548	548	548	548	504	534	548

[a]NEXT (Near-end crosstalk) — ослабление перекрестной наводки на ближнем конце. ELFEXT (Equal level far-end crosstalk) — ослабление равноуровневой перекрестной наводки на дальнем конце.

[б]Включая дополнительные спецификации TIA TSB 95 и ISO FDAM 2.

Кабель категории 5 поддерживает работу на скорости 100 Мбит/с. Кабели категорий 5e, 6 и 6a поддерживают скорость передачи 1 Гбит/с и в настоящее время используются в качестве стандарта. Кабель категории 6a лучше всего подходит для организации новых сетей, поскольку он особенно устойчив к помехам, возникающим из-за использования старых стандартов передачи сигналов (например, 10BASE-T). При прокладке кабелей категорий 5 и 5e были зафиксированы определенные проблемы. Кабели категорий 7 и 7a предназначены для передачи данных со скоростью 10 Гбит/с, а кабели категорий 8 — 40 Гбит/с.

Более быстродействующие стандарты требуют применения нескольких пар НВП. Это ускоряет передачу данных по линии связи по сравнению с использованием единственной пары. Для соединений 10BASE-T требуются две пары проводов категории 5. В соединениях 100BASE-TX предельная длина та же, но используются две пары проводов категории 5. Соединение 1000BASE-TX требует четырех пар проводов категорий 5e или 6/6a. Аналогично соединение 10GBASE-TX требует четырех пар проводов категорий 6a, 7 или 7a. Длина кабеля во всех стандартах ограничена 100 м.

Существуют провода с поливинилхлоридной и тефлоновой изоляцией. Выбор изоляции диктуется средой, в которой будут проложены кабели. В замкнутых помещениях, связанных с вентиляционной системой здания, обычно требуется тефлоновая изоляция[4]. Поливинилхлоридная изоляция дешевле и проще в эксплуатации.

[4]Конкретную информацию можно получить у пожарного инспектора или ответственного за пожарную безопасность.

Подключая четырехпарный НВП-кабель к коммутационным панелям и настенным розеткам RJ-45, придерживайтесь стандарта разводки TIA/EIA-568A. Этот стандарт, совместимый с другими вариантами RJ-45 (например, RS-232), позволяет избежать ошибок при разводке концов кабеля, независимо от того, есть ли свободный доступ к парам. Требования стандарта отражены в табл. 14.3.

Таблица 14.3. Стандарт TIA/EIA-568A для подключения четырехпарного НВП-кабеля к розетке RJ-45

Пара	Цвета	Контакты разъема
1	Белый/синий	5/4
2	Белый/оранжевый	3/6
3	Белый/зеленый	1/2
4	Белый/коричневый	7/8

Имеющаяся в здании проводка может не подходить для прокладки сетей, в зависимости от того, как и когда она прокладывалась.

Оптическое волокно

Оптическое волокно используется в тех ситуациях, когда применение медного кабеля по тем или иным причинам неприемлемо. Оптическое волокно передает сигнал быстрее, чем медный провод. Кроме того, оно является более устойчивым к электрическим помехам, что в некоторых приложениях очень важно. Там, где оптическое волокно не является абсолютно необходимым, обычно выбирают медный кабель, поскольку он дешевле и с ним легче работать.

Оптическое волокно бывает “многомодовым” и “одномодовым”. Многомодовое оптическое волокно обычно используется в зданиях или комплексах зданий. Оно толще, чем одномодовое, и может проводить несколько лучей света; это свойство позволяет использовать менее дорогую электронику (например, в качестве источника света можно использовать светодиоды).

Одномодовое оптическое волокно часто используется в магистральных приложениях, например для прокладки линий связи между городами и регионами. Оно может проводить только один световой луч и требует дорогой прецизионной электроники в конечных точках.

Стандарт TIA-598C рекомендует цветовую кодировку оптического волокна, представленную в табл. 14.4. Следует помнить основное правило: все элементы должны соответствовать друг другу. Оптическое волокно, соединяющее конечные точки, оптические кабели перекрестной коммутации и электронные приборы, установленные в конечных точках, должны иметь один и тот же тип и размер. Обратите внимание на то, что кабели OM1 и OM2 не являются взаимозаменяемыми, хотя и окрашены в один и тот же оранжевый цвет — проверьте размеры, указанные на кабелях, чтобы убедиться, что они соответствуют друг другу. Если вы нарушите это правило, то вам будет сложно обеспечить изоляцию в конечных точках.

На концах оптических волокон используются разъемы более чем 30 типов, и нет ни четких правил, ни принципов, регламентирующих их выбор. В каждой конкретной ситуации на выбор того или иного типа разъема влияют поставщики оборудования или параметры оптического волокна, уже проложенного внутри здания.

Таблица 14.4. Атрибуты стандартных оптических волокон

Количество мод	Название ISO*	Диаметр сердечника, мкм	Диаметр оптической оболочки, мкм	Цвет
Много	OM1	62,5	125	Оранжевый
Много	OM2	50	125	Оранжевый
Много	OM3	50 *	125	Голубой
Одна	OS1	8–10	125	Желтый

[а] В соответсвии со стандартатом ISO 11801.

[б] OM3 оптимизирован под лазерный луч.

Соединение и расширение сетей Ethernet

Сети Ethernet можно соединять с помощью устройств нескольких типов. На выбор устройств, описанных ниже, влияет их стоимость, причем более дешевые устройства описаны в первую очередь. Чем сложнее логические правила, по которым устройства перемещают биты из одной сети в другую, тем больше аппаратного и встроенного программного обеспечения необходимо и тем более дорогой становится сеть.

Концентраторы

Концентраторы (hub) иногда еще называют *повторителями* (repeators). Это активные устройства, используемые для соединения сегментов сетей Ethernet на физическом уровне. Им требуется внешний источник питания.

Выступая в качестве повторителя, концентратор ретранслирует Ethernet-фреймы, но никак не интерпретирует их. Он “не имеет представления” ни о том, куда направляются пакеты, ни о том, какой протокол они используют. За исключением экзотических ситуаций, *концентраторы больше не должны использоваться в промышленных сетях*, и мы не советуем их использовать даже в домашних сетях. (Почему? Потому что коммутаторы (switches) значительно эффективнее используют полосу пропускания частот в сети и в настоящее время стоят недорого.)

Коммутаторы

Коммутатор соединяет сети Ethernet на канальном уровне. Его назначение — объединить две физические сети так, чтобы они выглядели как одна большая физическая сеть. В настоящее время коммутаторы являются промышленным стандартом для соединения устройств Ethernet.

Коммутаторы принимают, регенерируют и ретранслируют пакеты на аппаратном уровне. Они используют алгоритм динамического обучения. Коммутаторы запоминают, какие исходные адреса поступают с одного порта, а какие — с другого. Пакет переходит из одного порта в другой только при необходимости. Первоначально пересылаются все пакеты, но через несколько секунд, когда коммутатор изучит расположение большинства хостов сети, запускается механизм фильтрации.

Поскольку между сетями пересылаются не все пакеты, каждый сегмент кабеля менее загружен, чем в случае, когда все компьютеры подключены к одному кабелю. А если учесть, что основной трафик имеет тенденцию к локализации, то увеличение реальной пропускной способности может оказаться заметным. Кроме того, коммутатор не влияет на логическую модель сети, поэтому его установка требует лишь незначительного вмешательства со стороны администратора.

Если сеть имеет петли, коммутатор может безнадежно запутаться, потому что пакеты, посылаемые одним компьютером, окажутся сразу на двух (или более) портах коммутатора. В одной сети Ethernet петлей не бывает, но после объединения нескольких таких сетей с помощью маршрутизаторов и коммутаторов топология изменится, вследствие чего может образоваться несколько путей к одному хосту. Некоторые коммутаторы решают эту проблему путем резервирования альтернативных маршрутов на тот случай, если основной маршрут станет недоступным. Они упрощают топологию видимой ими сети, отсекая дублирующиеся пути до тех пор, пока в оставшихся сегментах не окажется только по одному маршруту к каждому хосту сети. Другие коммутаторы создают между сетями двойные каналы и переключают трафик по циклическому принципу.

Коммутаторы должны просматривать каждый пакет, определяя, нужно ли его пересылать в другой сегмент. Производительность этих устройств обычно измеряют как скоростью просмотра пакетов, так и скоростью их пересылки. Многие поставщики не указывают в диаграммах производительности коммутаторов размеры протестированных пакетов, поэтому реальная производительность может быть ниже объявленной.

Несмотря на то что быстродействие коммутаторов Ethernet все время растет, эффективно использовать их можно при объединении в один логический сегмент не более сотни компьютеров. В крупных коммутируемых сетях часто возникают проблемы наподобие "широковещательных штормов", поскольку широковещательный трафик должен проходить через все порты. Для решения этой проблемы нужно изолировать широковещательный трафик между коммутируемыми сегментами посредством маршрутизатора (создавая тем самым более одного логического Ethernet-сегмента).

Выбор коммутатора может представлять определенную трудность. В этом сегменте рынка очень высокая конкуренция, следствием которой являются многочисленные рекламные заявления, не всегда подтверждаемые на практике. Поэтому не стоит особо доверять данным, которые приводятся поставщиками; лучше прислушаться к советам независимых экспертов (просмотрите тесты, приводимые в журналах). В последние годы нередко случалось так, что чей-то продукт оказывался "лучшим" в течение нескольких месяцев, а затем, после попыток внесения улучшений, его производительность или надежность падала ниже критической отметки.

В любом случае убедитесь, что скорость объединительной панели коммутатора является достаточной. У хорошо спроектированного коммутатора эта скорость должна превышать сумму скоростей всех его портов.

Коммутаторы, позволяющие создавать виртуальные локальные сети

В крупных организациях можно использовать коммутаторы, позволяющие разбивать их порты (программным путем) на группы, называемые виртуальными локальными сетями (Virtual Local Area Network — VLAN). Виртуальная локальная сеть — это группа портов, принадлежащая к одному логическому сегменту, как если бы порты были соединены со своим собственным выделенным коммутатором. Подобное секционирование позволяет повысить степень изоляции трафика, что полезно с точки зрения как безопасности, так и производительности.

Трафиком между виртуальными локальными сетями управляет маршрутизатор или, в некоторых случаях, модуль маршрутизации или уровень программной маршрутизации самого коммутатора. Расширение этой системы, называемое *транкингом виртуальной локальной сети* (один из примеров реализации — протокол IEEE 802.1Q), позволяет разным коммутаторам обслуживать порты одной логической виртуальной локальной сети.

Важно помнить, что сами сети VLAN почти не обеспечивают дополнительной защиты. Для того чтобы обеспечить защиту, необходимо фильтровать трафик VLAN.

Маршрутизаторы

Маршрутизаторы (известные также как "коммутаторы третьего уровня") направляют трафик на третьем сетевом уровне модели OSI. Маршрутизаторы доставляют пакеты адресатам на основании информации, хранящейся в TCP/IP-заголовках. Помимо простого перемещения пакетов, маршрутизаторы могут также выполнять ряд особых функций, например фильтрацию пакетов (в соответствии с правилами безопасности), разделение трафика по приоритетам (в соответствии с заданным качеством обслуживания) и обнаружение общей сетевой топологии.

Конфигурация маршрутизаторов бывает фиксированной или модульной.

- Устройства первого типа содержат сетевые интерфейсы, установленные в заводских условиях. Они обычно подходят для специализированных применений. Например, маршрутизатор с интерфейсами T1 и Ethernet может оказаться удобным, когда нужно подключить небольшую компанию к Интернету.
- Модульные маршрутизаторы имеют слотовую или шинную архитектуру, а интерфейсы к ним добавляются пользователями. Как правило, это более дорогие устройства, но зато они гибче в эксплуатации.

В зависимости от необходимой надежности и ожидаемого трафика, специализированный маршрутизатор может оказаться как дороже, так и дешевле системы UNIX или Linux, сконфигурированной в качестве маршрутизатора. Однако специализированное устройство, как правило, демонстрирует более высокую производительность и надежность. Это та область сетевого проектирования, где лучше заранее вложить чуть больше денег, чем потом иметь головную боль.

Автосогласование

С появлением разных стандартов Ethernet возникла необходимость, чтобы устройства могли идентифицировать конфигурацию своих соседей и согласовывать с ними свои настройки. Например, сеть не будет работать, если на одной стороне соединения она работает со скоростью 1 Гбит/с, а на другой — со скоростью 10 Гбит/с. Для выявления и решения этой проблемы организацией IEEE был разработан стандарт автосогласования Ethernet. В одних случаях он работает, а в других применяется неправильно и лишь усугубляет проблему.

Следует запомнить два золотых правила автосогласования.

- Вы *обязаны* использовать автосогласование всех интерфейсов, работающих на скорости 1 Гбит/с и выше. Этого требует стандарт.
- Если интерфейсы ограничены скоростями 100 Мбит/с и ниже, необходимо либо конфигурировать *оба конца* соединения, либо вручную настроить скорость и дуплекс (половинный или полный) *обеих* сторон. Если в режиме автосогласования настроить только одну сторону соединения, то в большинстве случаев она не сможет выяснить, какую конфигурацию имеет другая сторона. В результате конфигурация станет несогласованной и производительность упадет.

Для того чтобы выяснить, как задать стратегию автосогласования интерфейсов, прочитайте специальный раздел 13.10.

Передача электропитания по сетям Ethernet

Технология передачи питания по сетям Ethernet (Power on Ethernet — PoE) основана на передаче электропитания по той же неэкранированной витой паре (UTP Ethernet), по которой передается сигнал Ethernet. Данная технология регламентируется стандартом IEEE 802.3af. Это особенно удобно для систем связи, обеспечивающих передачу речевого сигнала по сети Интернет (Voice over IP — VoIP), или пунктов доступа к системе беспроводной связи (мы указали только два примера, но список можно продолжить), в которых требуется как маломощный источник питания, так и сетевое соединение.

По мощности питания системы PoE разделяются на четыре класса в диапазоне от 3,84 до 25,5 Вт. Промышленность, которая никогда не останавливается на достигнутом, уже работает над новым стандартом (802.3bt), предусматривающим более высокую мощность (более 60 Вт). Будет ли этого достаточно, чтобы подключить духовку Easy-Bake к сетевому порту в конференц-зале?[5]

Технология PoE порождает два обстоятельства, о которых должен знать системный администратор.

- Вы должны знать о существовании устройств PoE в вашей инфраструктуре, чтобы правильно спланировать доступ к портам коммутаторов, поддерживающих технологию PoE. Эти порты дороже, чем порты, не поддерживающие технологию PoE.
- Вычисляя расход электроэнергии на обслуживание коммуникационных шкафов, содержащих коммутаторы PoE, следует учитывать мощность устройств PoE. Обратите внимание на то, что вы не должны учитывать дополнительный расход электроэнергии на охлаждение коммуникационных шкафов, поскольку бо́льшая часть тепла, выделяемого из-за потребления мощности PoE, рассеивается за пределами шкафа (обычно по офису).

Гигантские пакеты

Технология Ethernet стандартизована для типичного пакета размером 1 500 байт (вместе с фреймом — 1 518 байт). Это значение было выбрано давно, когда сети были медленными и память для буферов была дефицитной. В настоящее время пакеты размером 1 500 байт выглядят крохотными в контексте гигабитных сетей Ethernet. Поскольку с каждым пакетом связаны накладные расходы и определенное время задержки, производительность сети можно повысить, если допустить более крупные размеры пакетов.

К сожалению, стандарты IEEE для разных типов сетей Ethernet запрещают использование крупных пакетов по соображениям совместимости сетей. Однако, поскольку скорость магистрального трафика часто во много раз превышает установленный предел, нестандартные большие пакеты Ethernet в современных сетях перестали быть редкостью. Подстрекаемые нетерпеливыми потребителями, производители сетевого оборудования негласно бойкотируют стандарт IEEE и обеспечивают поддержку крупных фреймов в своей гигабитной продукции.

Для использования так называемых *гигантских пакетов* (jumbo frames) необходимо лишь повысить максимально возможный размер пакета (maximal transmission unit — MTU) в интерфейсах сети. Повышение производительности зависит от вида трафика, но наибольший выигрыш достигается для крупномасштабных перемещений по протоколу TCP (например, в файловых службах NFSv4 или CIFS). Ожидается, что умеренное, но заметное повышение производительности должно составить примерно 10%.

---

[5]Для интересующихся этим вопросом: да, существует возможность загрузить небольшую систему Linux через порт сети PoE. Возможно, проще всего это сделать с помощью Raspberry Pi и коммутатора Pi PoE Switch HAT.

Тем не менее следует отметить следующее.

- Поддерживать и использовать гигантские пакеты должно все сетевое оборудование в подсетях, включая коммутаторы и маршрутизаторы. Их нельзя смешивать и подгонять.
- Поскольку гигантские пакеты являются нестандартными, обычно их необходимо разрешать явным образом. Устройства могут принимать гигантские пакеты по умолчанию, но, вероятнее всего, они не будут их генерировать.
- Поскольку гигантские пакеты представляют собой незаконное явление, не существует соглашения, насколько большими они могут или должны быть. Типичной величиной является 9000 байт или 9018 вместе с фреймом. Необходимо проверить, какой максимальный размер пакета может принять ваше устройство. Пакеты размером больше 9 Кбайт иногда называют сверхгигантскими, но это экзотическое название вас пугать не должно. Чем больше размер, тем лучше, по крайней мере в диапазоне до 64 Кбайт.

Мы одобряем использование гигантских пакетов в гигабитных сетях Ethernet, но будьте готовы к дополнительной отладке, если что-то пойдет не так, как надо. Лучше всего развернуть новую сеть, задав максимально возможный размер пакета по умолчанию, а позднее, когда надежность сети будет проверена, изменить эти настройки и разрешить гигантские пакеты.

14.2. Беспроводные сети: локальная сеть для кочевников

Беспроводные сети состоят из беспроводных точек доступа (Wireless Access Points — WAP) и клиентов беспроводной сети. Точки WAP могут соединяться традиционными проводными сетями (обычная конфигурация) или с другими точками WAP без использования проводов (конфигурация известна под названием “беспроводная сеть”).

Стандарты беспроводных сетей

Распространенными стандартами беспроводных сетей в настоящее время являются IEEE 802.11g, 802.11n и .802.11ac Стандарт 802.11g работает на частоте 2,4 ГГц и обеспечивает доступ к локальной сети со скоростью, достигающей 54 Мбит/с. Радиус действия одной точки доступа колеблется от 100 м до 40 км, в зависимости от оборудования и физических особенностей местности.

Стандарт 802.11n обеспечивает скорость до 600 Мбит/с [6] и может использовать частоты как 5 ГГц, так и 2,4 ГГц (при этом рекомендуется использовать диапазон 5 ГГц). Радиус действия точки доступа в стандарте IEEE 802.11n в два раза больше, чем в стандарте IEEE 802.11g. Преемником стандарта IEEE 802.11n является стандарт IEEE 802.11ac, поддерживающий производительность многостанционной сети на уровне до 1 Гбит/с.

Все эти стандарты обозначаются одним общим термином Wi-Fi. Формально говоря, метка Wi-Fi ограничена семейством стандартов IEEE 802.11. Однако это лишь один из многих видов аппаратного обеспечения Ethernet, доступных на рынке, поэтому все беспроводные сети Ethernet называются Wi-Fi.

[6] Скорость 600 Мбит/с в стандарте 802.11n является, скорее, теоретической. На практике полоса пропускания в окрестности точки WAP при оптимальной конфигурации может обеспечить скорость передачи данных не более 400 Мбит/с. Это объясняется различием между теоретическими и практическими возможностями оборудования и среды. В беспроводных сетях всякое бывает!

В настоящее время стандарты 802.11g и 802.11n стали общепринятыми. Трансиверы недороги и встроены в большинство ноутбуков. Кроме того, платы расширения также стоят недорого и доступны для любых персональных компьютеров.

Доступ клиентов к беспроводной сети

Вы можете настроить системы UNIX или Linux для подключения к беспроводной сети в качестве клиента, если у вас есть правильное оборудование и драйвер. Поскольку большинство беспроводных плат на базе персональных компьютеров все еще предназначены для системы Microsoft Windows, они могут не поставляться с завода с драйверами FreeBSD или Linux.

При попытке добавить беспроводное подключение к системе FreeBSD или Linux вам, скорее всего, понадобятся следующие команды:

- **`ifconfig`** — для конфигурирования интерфейса беспроводной сети;
- **`iwlist`** — для получения списка доступных точек доступа к беспроводной сети;
- **`iwconfig`** — для настройки параметров беспроводного соединения;
- **`wpa_supplicant`** — для аутентификации в беспроводной сети (или проводной сети 802.1x).

К сожалению, гонка продаж дешевого оборудования часто означает, что для настройки правильной работы беспроводного адаптера в системе UNIX или Linux может потребоваться много часов проб и ошибок. Планируйте все заранее или выясните в Интернете, какой адаптер лучше всего подходит для вашей операционной системы.

Беспроводные коммутаторы и точки беспроводного доступа

Все хотят иметь доступ к беспроводной сети в любом месте, и для обеспечения этой услуги доступно множество продуктов. Но, как и во многих других областях, вы получаете то, за что платите. Недорогие устройства часто удовлетворяют потребности домашних пользователей, но не могут хорошо масштабироваться в корпоративной среде.

Топология беспроводных сетей

Точки беспроводного доступа (Wireless Access Point — WAP) обычно представляют собой специализированные устройства, состоящие из одной или нескольких радиостанций и некоторой формы встроенной сетевой операционной системы, часто урезанной версии Linux. Одна точка WAP может обеспечить подключение нескольких клиентов, но их число ограничено. Хорошее эмпирическое правило состоит в том, чтобы одновременно обслуживать не более сорока клиентов с помощью одной корпоративной точки WAP. В качестве клиента может действовать любое устройство, которое обменивается данными по беспроводному стандарту, поддерживаемому вашими точками WAP.

Точки WAP имеют один или несколько "служебных идентификаторов сети", а также идентификатор SSID, который служит именем беспроводной локальной сети и должен быть уникальным в определенной окрестности. Когда клиент хочет подключиться к беспроводной локальной сети, он выясняет, какие идентификаторы SSID доступны, и выбирает одну из этих сетей.

Вы можете сделать имя своего идентификатора SSID осмысленным и легко запоминающимся, например `Third Floor Public` (Третий этаж, открытый доступ), или изобрести что-нибудь необычное. Некоторые из наших любимых имен SSID:

- `FBI Surveillance Van` (Служба наблюдения ФБР);
- `The Promised LAN` (Обещанная локальная сеть);
- `IP Freely` (Свободный IP);
- `Get Off My LAN` (Убирайся из моей локальной сети);
- `Virus Distribution Center` (Центр распространения вирусов);
- `Access Denied` (Доступ запрещен).

Нет ничего лучше, чем изобретательные чудаки... В простейших сценариях точка WAP объявляет единственный SSID, ваш клиент подключается к этому SSID и всё — вы в сети!

Тем не менее несколько аспектов беспроводной сети действительно просты. Что делать, если ваш дом или здание слишком большие, чтобы обслуживаться одной точкой WAP? Или что если вам нужно предоставлять разные сети различным группам пользователей (например, сотрудникам или гостям)? Для этих случаев вам необходимо стратегически структурировать свою беспроводную сеть.

Вы можете использовать несколько SSID для разбивки групп пользователей или функций. Как правило, вы сопоставляете их с отдельными виртуальными локальными сетями, которые затем можно маршрутизировать или фильтровать по желанию, как и проводные сети.

Частотный спектр, выделенный для беспроводной сети 802.11, разбивается на полосы, обычно называемые *каналами*. Точка WAP самостоятельно выбирает свободный радиоканал для объявления SSID. Клиенты и точка WAP используют этот канал для связи, формируя единый широковещательный домен. Ближайшие точки WAP, скорее всего, будут выбирать другие каналы, чтобы максимизировать доступную полосу пропускания и минимизировать помехи.

Теория состоит в том, что по мере того, как клиенты перемещаются по окружающей среде, они будут отделяться от одной точки WAP, когда ее сигнал становится слабым, и соединяться с ближней точкой WAP с более сильным сигналом. Однако теория и реальность часто не согласуются друг с другом. Многие клиенты поддерживают связь с точкой WAP, излучающей слабый сигнал, и игнорируют лучшие варианты.

В большинстве ситуаций вы должны разрешить WAP автоматически выбирать свои предпочтительные каналы. Если вы должны вручную вмешаться в этот процесс, используя стандарты 802.11b/g/n, рассмотрите выбор между каналами 1, 6 или 11. Спектр, выделенный этим каналам, не перекрывается, поэтому комбинации этих каналов обеспечивают наибольшую вероятность широкого распространения — открытую беспроводную магистраль. Каналы по умолчанию для 802.11a/ac не перекрываются вообще, поэтому просто выберите свой любимый номер.

Некоторые точки WAP имеют несколько антенн и используют технологию множественного ввода и множественного вывода (multiple-input, multiple-output — MIMO). Эта практика может увеличить доступную полосу пропускания, используя несколько передатчиков и приемников, чтобы использовать преимущества смещения сигнала в результате задержки распространения. В некоторых ситуациях эта технология может обеспечить небольшое улучшение производительности, хотя, вероятно, не такое значительное улучшение, как широкая сеть антенн.

Если вам нужна физически большая зона покрытия, разверните несколько точек WAP. Если область полностью открыта, вы можете развернуть их в структуре решетки. Если существуют физические препятствия вроде стен, проведите исследование для определения наилучших вариантов размещения точек WAP с учетом физических атрибутов вашего пространства.

Дешевая беспроводная связь

Нам нравятся продукты Ubiquiti (`ubnt.com`) для недорогих, высокопроизводительных домашних сетей. Google Wifi — замечательное облачное решение, если вы поддерживаете связь с удаленными членами семьи. Другим вариантом является запуск урезанной версии Linux (например, OpenWrt или LEDE) на коммерческой точке WAP (см. сайт `Openwrt.org` для получения дополнительной информации и списка совместимого оборудования).

Буквально десятки продавцов сейчас поставляют оборудование для точек беспроводного доступа. Вы можете купить их в Home Depot и даже в продуктовом магазине. Дешевые точки доступа (в диапазоне 30 долл.), вероятно, будут плохо работать при обработке больших файлов или наличии нескольких активных клиентов.

Дорогая беспроводная связь

Большая беспроводная связь означает большие деньги. Предоставление надежной беспроводной сети высокой плотности (в крупных больницах, спортивных учреждениях, школах, городах) представляет собой сложную задачу, связанную с ограничениями физических установок, плотностью пользователей и законами физики. В таких ситуациях вам нужны беспроводные устройства корпоративного класса, которые знают местоположение и состояние каждой точки WAP и активно настраивают каналы WAP, силу сигналов и группы клиентов, чтобы обеспечить наилучшие результаты. Эти системы обычно поддерживают прозрачный роуминг, который позволяет группе клиентов с определенной виртуальной локальной сетью и сессией беспрепятственно перемещаться между точками WAP.

Наши любимые крупные беспроводные платформы — это Aerohive и Meraki (последняя принадлежит компании Cisco). Эти платформы следующего поколения управляются из облака, что позволяет вам пить мартини на пляже, контролируя свою сеть через браузер. Вы даже можете выбросить отдельных пользователей из беспроводной сети, не вставая с шезлонга. Уйди, противный!

Если вы развертываете беспроводную сеть в больших масштабах, вам, вероятно, придется приобрести анализатор беспроводной сети. Мы настоятельно рекомендуем аналитические продукты, разработанные компанией AirMagnet.

Безопасность беспроводных сетей

Традиционно безопасность беспроводных сетей очень низкая. Существует протокол WEP (Wired Equivalent Privacy), применяемый в сетях 802.11b и для шифрования пакетов, передаваемых с помощью радиоволн. К сожалению, в современной версии стандарта была обнаружена фатальная проектная недоработка, которая делает его практически бесполезным. Посторонний человек, находящийся за пределами здания, может получить прямой доступ к сети и остаться незамеченным.

Тем не менее недавно появившиеся стандарты Wi-Fi Protected Access (WPA) возродили доверие к безопасности беспроводных сетей. В настоящее время во всех новых инсталляциях должны использоваться стандарты WPA (в частности, стандарт WPA2), а не WEP. Без применения стандарта WPA2 беспроводные сети должны считаться полностью незащищенными и не должны использоваться за пределами предприятия. Даже дома не используйте стандарт WEP!

Для того чтобы запомнить, что стандарт WEP является незащищенным, а стандарт WPA — безопасным, просто расшифруйте аббревиатуру WAP (Wired Equivalent Privacy — конфиденциальность на уровне проводных сетей). Это название точно отражает суть дела; протокол WEP обеспечивает такую защиту, как проводная сеть, допускающая

непосредственное подключение посторонних лиц. (Иначе говоря, никакой защиты — по крайне мере на уровне IP.)

14.3. SDN: программно-коммутируемые сети

Как и при виртуализации серверов, разделение физического сетевого оборудования с функциональной архитектурой сети может значительно повысить гибкость и управляемость. Лучшим средством для достижения этих целей являются программно-коммутируемые сети (software-defined networking — SDN).

Основная идея SDN заключается в том, что компоненты, управляющие сетью (плоскость управления), физически отделены от компонентов, которые пересылают пакеты (плоскость данных). Плоскость данных программируется через плоскость управления, поэтому вы можете настраивать или динамически изменять маршруты передачи данных для достижения целей производительности, безопасности и доступности.

Как и многое в нашей отрасли, SDN для корпоративных сетей превратилась в маркетинговый трюк. Первоначальная цель состояла в том, чтобы стандартизировать независимые от поставщика способы перенастройки сетевых компонентов. Несмотря на то что некоторые из этих планов были реализованы, многие поставщики теперь предлагают собственные продукты SDN для предприятий, которые в какой-то мере степени противоречат первоначальной цели SDN. Если вы изучаете пространство предприятия SDN, выбирайте продукты, соответствующие открытым стандартам и совместимые с продуктами других поставщиков.

Для крупных поставщиков облачных вычислений SDN добавляет уровень гибкости, который уменьшает вашу потребность знать (или заботиться) о том, где определенный ресурс находится физически. Хотя эти решения могут быть коммерческими, они тесно интегрированы в платформы облачных провайдеров и могут упростить настройку вашей виртуальной инфраструктуры.

Сеть SDN и ее система управления, основанная на интерфейсах API, предлагают системным администраторам соблазнительную возможность интегрировать управление топологией сети с другими инструментами стиля DevOps для непрерывной интеграции и развертывания. Возможно, в каком-то идеальном мире у вас всегда есть производственная среда, поставленная и готовая к активации одним щелчком мыши. По мере того как новая среда продвигается к производству, сетевая инфраструктура магическим образом преобразуется, устраняя простои, заметные для пользователя, и необходимость планировать окна обслуживания.

14.4. Тестирование и отладка сетей

Ключ к отладке сети — ее разбивка на сегменты и тестирование каждого из них до тех пор, пока не будет обнаружена неисправность. Загадочные лампочки на коммутаторах и концентраторах (обозначающие, к примеру, состояние канала и наличие трафика пакетов) помогают быстро выявить источник проблемы. Для того чтобы эти индикаторы работали так, как вы хотите, следует руководствоваться первоклассной документацией.

Как всегда, важно иметь под рукой нужные инструменты, чтобы выполнить работу правильно и без проволочек. На рынке предлагаются средства сетевой отладки двух типов (правда, наблюдается тенденция к их объединению).

Устройство первого типа — ручной кабельный тестер. Он измеряет электрические характеристики кабеля, включая его длину (для этого применяется особая технология,

называемая рефлектометрией во временной области). Такие устройства способны выявлять простейшие проблемы, например разрыв или неправильную разводку кабеля.

Нашим любимым инструментом тестирования локальных сетей является устройство Fluke LanMeter. Это универсальный анализатор, способный даже посылать эхо-пакеты протокола ICMP. Профессиональные варианты этого оборудования описаны на специальном веб-сайте. Для телекоммуникационных сетей WAN лучше всего подходит тестер T-BERD, выпускаемый компанией Viavi (`viavisolutions.com`).

Средства отладки второго типа — это анализаторы сетевых пакетов. Они просматривают сетевые пакеты на предмет наличия ошибок протоколов, неправильной конфигурации и прочего беспорядка. Эти анализаторы работают на уровне каналов, а не на электрическом уровне, поэтому они не могут распознавать проблемы, связанные с физическими повреждениями кабелей или электропитанием.

Существуют профессиональные анализаторы сетевых пакетов, но мы нашли свободно распространяемую программу Wireshark[7] (`wireshark.org`), которая может выполняться на полнофункциональном ноутбуке. Именно ее можно считать наилучшим выбором. Более подробная информация об анализаторах сетевых пакетов приведена в разделе 13.12.

14.5. Прокладка кабелей

Если вы занялись прокладкой кабелей в здании, то самый ценный совет, который мы можем вам дать, звучит так: “Делайте все правильно с первого раза”. Это не та область, в которой можно скупиться или халтурить. Покупая качественные материалы, выбирая компетентного подрядчика для прокладки кабелей и устанавливая дополнительные разъемы (отводы), вы тем самым избежите многолетних мучений.

Неэкранированная витая пара

Кабель категории 6a имеет наилучшее соотношение цены и производительности на современном рынке. Его стандартный вариант — четыре пары проводов под одной оболочкой, что подходит для большинства соединений, включая RS-232 и гигабитные линии.

Спецификации кабеля категории 6a требуют, чтобы скрутка провода заканчивалась в точке контакта. Для того чтобы обеспечить это требование, необходимы специальное обучение и оконечное оборудование. При этом необходимо использовать настенные розетки и коммутационные панели категории 6a. Самые хорошие отзывы заслужила продукция компании Siemon.

Офисные точки подключения

Многие годы идут споры, сколько точек подключения требуется для офиса. Одной точки подключения на офис явно недостаточно. Сколько же нужно — две или четыре? Мы рекомендуем четыре, обосновывая это следующими причинами.

- Их можно использовать просто для подключения телефонов и других специализированных устройств.
- Большинство пользователей предпочитают подключаться с помощью беспроводных сетей, а не проводов.
- Гораздо дешевле проложить весь кабель сразу, чем делать это поэтапно.

[7] Как и многие популярные программы, программа Wireshark часто подвергается атакам хакеров. Убедитесь, что вы используете самую последнюю ее версию.

- Средства, выделенные на приобретение проводов, лучше потратить на основную инфраструктуру, а не на оборудование отдельных офисов.

При прокладке кабеля в здании можно установить дополнительные розетки в коридорах, конференц-залах, столовых, туалетных комнатах и на потолках (для точек беспроводного доступа). Однако не забывайте о безопасности и размещайте открыто предоставляемые порты на "гостевой" виртуальной локальной сети, не допуская посторонних к своим внутренним сетевым ресурсам. Публикуя защищенные публичные порты, используйте стандарт аутентификации 802.1x.

Стандарты кабельных систем

Необходимость обеспечения всех видов деятельности внутри современных зданий обусловливает потребность в крупной и сложной кабельной инфраструктуре. Заглянув в обычный коммутационный шкаф, вы будете потрясены, увидев его стенки, сплошь покрытые непомеченными проводами одного цвета.

С целью улучшения оперативного контроля и стандартизации кабельных систем зданий в феврале 1993 г. организация TIA опубликовала административный стандарт на телекоммуникационную инфраструктуру коммерческих зданий (TIA/EIA-606). В 2012 г. появилась его обновленная версия TIA/EIA-606-B.

Этот стандарт устанавливает требования и принципы идентификации и документирования телекоммуникационной инфраструктуры. Он касается следующих аспектов:

- оконечной аппаратуры;
- кабелей;
- прокладки кабелей;
- расстояний между элементами оборудования;
- цветовой маркировки;
- символических обозначений стандартных компонентов.

В частности, определены стандартные цвета маркировки проводов (табл. 14.5).

Таблица 14.5. Таблица цветовой маркировки по стандарту TIA/EIA-606

Тип оконечного устройства	Цвет	Код[а]	Комментарии
Граничное	Оранжевый	150C	Центральная телефонная станция
Сетевые соединения	Зеленый	353C	Также применяется для вспомогательных электросетей
Общее оборудование[б]	Фиолетовый	264C	Основное оборудование коммутации и передачи данных
Магистраль первого уровня	Белый	—	Кабели
Магистраль второго уровня	Серый	422C	Кабели
Станция	Синий	291C	Горизонтальные кабели
Магистраль между зданиями	Коричневый	465C	Кампусные кабели
Разное	Желтый	101C	Служебные и сигнальные линии
Ключевые телефонные системы	Красный	184C	—

[а] В соответствии с цветовой моделью Pantone.

[б] Офисные АТС, компьютеры, локальные сети, мультиплексоры и т.д.

14.6. Проектирование сетей

В этом разделе рассматриваются вопросы, связанные с логическим и физическим проектированием сетей среднего размера. Представленные здесь идеи подходят для нескольких сотен хостов, но неприменимы ни для трех, ни для нескольких тысяч компьютеров, включенных в одну сеть. Также предполагается, что работа будет начата с нуля.

Основной объем работ по проектированию сети состоит из определения:

- типов сред передачи;
- топологии и способов прокладки кабелей;
- системы концентраторов, коммутаторов и маршрутизаторов.

Еще один ключевой вопрос проектирования сети связан с управлением перегрузкой. Например, файловые протоколы NFS и SMB очень сильно загружают сеть, поэтому такие файловые системы нежелательно подключать по магистральному кабелю.

Ниже анализируются аспекты, которые необходимо учитывать при проектировании сети.

Структура сети и архитектура здания

Структуру сети проще изменить, чем архитектуру здания, но обе они должны нормально сосуществовать. Если вам крупно повезло, т.е. представилась возможность проектировать сеть до постройки здания, будьте щедрым. К сожалению, в большинстве случаев здание и отдел технического обслуживания компании на момент проектирования сети уже существуют и налагают жесткие ограничения на структуру сети.

В уже построенных зданиях сеть должна адаптироваться к архитектуре, а не противостоять ей. В современных зданиях, помимо высоковольтной электропроводки, водо- и газопроводов, иногда имеются каналы для прокладки кабелей. Часто монтируются подвесные потолки — настоящий подарок для тех, кто прокладывает сеть. Во многих университетских городках существуют туннели, которые облегчают создание сетей.

Необходимо следить за целостностью брандмауэров.[8] При прокладке кабеля через брандмауэр отверстие должно соответствовать диаметру кабеля и заполняться негорючим веществом. Выбирая кабель, учитывайте наличие приточной вентиляции. Если узнают, что вы нарушили правила пожарной безопасности, вас могут оштрафовать и заставить устранить недостатки, даже если для этого придется проложить заново всю сеть.

Логическая структура сети должна соответствовать физическим ограничениям зданий, в которых она будет функционировать. Приступая к проектированию, помните, что можно найти логически красивое решение, а затем вдруг обнаружить, что реализовать его физически сложно или вообще невозможно.

Расширение сетей

Прогнозировать потребности на десять лет вперед очень сложно, особенно в области вычислительной техники и сетей. Поэтому, проектируя сеть, всегда следует учитывать перспективы ее расширения и увеличения пропускной способности. Прокладывая кабель, особенно в труднодоступных местах, протягивайте в три-четыре раза больше пар,

[8] Речь идет о брандмауэрах в виде бетонных, кирпичных или огнеупорных стен, которые препятствуют распространению огня по всему зданию. Значительно отличаясь от сетевых брандмауэров, они не менее важны.

чем нужно. Помните: основная часть стоимости прокладки сети приходится на оплату труда, а не на материалы.

Даже если волоконно-оптические линии не планируется использовать немедленно, разумно будет все же проложить немного оптического волокна, особенно если известно, что впоследствии протянуть его будет гораздо труднее. Прокладывайте и многомодовый, и одномодовый кабели. Как правило, нужным оказывается как раз тот кабель, который не проложен.

Перегрузка

Сеть — как цепь: ее качество определяется самым слабым или самым медленным звеном. Производительность Ethernet, как и многих других сетевых технологий, при увеличении нагрузки падает.

Активно эксплуатируемые коммутаторы, нестыкующиеся интерфейсы, низкоскоростные каналы связи — все это может привести к перегрузке. Эффективный способ борьбы с ней заключается в локализации трафика путем создания подсетей и установки маршрутизаторов. Подсети можно использовать и для изоляции компьютеров, задействованных в отдельных экспериментах. Трудно проводить эксперимент на нескольких компьютерах, если нет надежного способа изолировать их физически и логически от остальной части сети.

Обслуживание и документирование

Опыт показывает, что удобство обслуживания сети напрямую зависит от качества документации на нее. Точная, полная, своевременно корректируемая документация абсолютно необходима.

Кабели следует маркировать во всех точках подключения. Рекомендуем вкладывать копии местных монтажных схем в коммутационные шкафы, чтобы при всех изменениях эти экземпляры можно было скорректировать на месте. Каждые несколько недель необходимо переносить все корректировки в электронную базу данных.

Стыки между крупными системами в виде коммутаторов или маршрутизаторов могут упростить отладку, поскольку позволяют изолировать части сети и отлаживать их по отдельности. Полезно также разграничивать административные области.

14.7. Управление сетью

Если необходимо обеспечить нормальную работу сети, одни функции управления следует централизовать, другие — распределить, а третьи — оставить на локальном уровне. Требуется сформулировать и согласовать обоснованные “правила поведения добропорядочных граждан”.

Типичная крупномасштабная среда включает в себя:

- магистральную сеть, соединяющую здания;
- сети подразделений, подключенные к магистрали;
- подсети рабочих групп в рамках подразделения;
- соединения с внешним миром (например, с Интернетом или периферийными филиалами).

При проектировании и реализации сетей следует предусматривать централизованные контроль, ответственность, сопровождение и финансирование. Поскольку подразделения, как правило, стремятся свести к минимуму собственные расходы, быстро растет число сетей с централизованной оплатой каждого соединения. Вот основные объекты централизованного управления:

- структура сети, в том числе принципы использования подсетей, маршрутизаторов, коммутаторов и т.д.;
- магистральный кабель, в том числе подключения к нему;
- IP-адреса и имена компьютеров, доменные имена;
- используемые протоколы (требуется обеспечить их взаимодействие);
- правила доступа в Интернет.

Имена доменов, IP-адреса и сетевые имена компьютеров в определенном смысле уже находятся под централизованным контролем таких организаций, как ARIN (American Registry for Internet Numbers) и ICANN, но координация использования этих элементов на локальном уровне также необходима.

Центральный орган управления имеет общее представление о сети, ее структуре, производительности и перспективах роста. Он может позволить себе иметь собственное контрольное оборудование (и обслуживающий его персонал) и следить за нормальной работой магистральной сети. Центральный орган может настоять на правильном выборе структуры сети, даже если для этого придется заставить подразделение купить маршрутизатор и создать подсеть для подключения к магистрали. Такое решение иногда необходимо для того, чтобы новое соединение не навредило работе существующей сети.

Если в сети работают разнородные компьютеры, операционные системы и протоколы, обязательно нужно иметь "высокоинтеллектуальный" маршрутизатор (например, компании Cisco), который будет служить шлюзом между сетями.

14.8. Рекомендуемые поставщики

Занимаясь более 30 лет инсталляцией сетей по всему миру, мы не раз обжигались на продуктах, которые не соответствовали спецификациям, имели завышенную цену, неправильно указанные характеристики или как-то иначе не оправдывали ожидания. Ниже приведен список поставщиков, которым мы доверяем и услугами которых рекомендуем пользоваться.

Кабели и разъемные соединения

AMP (подразделение Tyco) (800) 522-6752 amp.com	Anixter (800) 264-9837 anixter.com	Black Box Corporation (724)746-5500 blackbox.com
Belden Cable (800) 235-3361 (765) 983-5200 belden.com	Siemon Company (860) 945-4395 siemon.com	Newark Electronics (800) 463-9275 newark.com

Тестовые приборы

Fluke	Siemon	Viavi
(800) 443-5853	(800) 945-4395	(844) 468-4284
fluke.com	siemon.com	vivasolutions.com

Маршрутизаторы/коммутаторы

Cisco Systems	Juniper Network
(415) 326-1941	(408) 745-2000
www.cisco.com	juniper.com

14.9. Литература

- ANSI/TIA/EIA-568-A. *Commercial Building Telecommunications Cabling Standard* и ANSI/TIA/EIA-606, *Administration Standard for the Telecommunications Infrastructure of Commercial Buildings*. Это стандарты телекоммуникационной промышленности для построения кабельных систем зданий. К сожалению, они не бесплатны. Посетите веб-сайт www.tiaonline.org.
- Barnett David, Groth David and Jim McBee. *Cabling: The Complete Guide to Network Wiring (3rd* edition). San Francisco: Sybex, 2004.
- Goransson, Paul, and Chuck Black. *Software Defined Networks, A Comprehensive Approach* (2nd Edition). Burlington, MA: Morgan Kaufman, 2016.
- Spurgeon, Charles, and Joann Zimmerman. *Ethernet*: *The Definitive Guide: Designing and Managing Local Area Networks (2nd Edition)*. Sebastopol, CA: O'Reilly, 2014.