Содержание

Список рисунков 1
1. Введение 1
2. Сетевая этика 4
3. Из истории компьютерных сетей. Предпосылки возникновения сетей 12
4. Компьютерные сети на базе протокола UUCP 19
5. Протокол TCP/IP 30
6. Архитектура сети Ethernet 50
7. Коаксиальный кабель 53
8. Кабель витой пары 56
9. Стандарт 100Base-T(Fast Ethernet) 59
10. Расширение Ethernet-сети 60
11. HUB (Хаб или концентратор) 60
12. Правило 4-х хабов 61
13. Switch (или Bridge) 62
14. Router (маршрутизатор) 64
15. Правило построения смешанной сети 64
16. Оценка качества услуг 65
17. Построение региональных сетей 65
18. Принципы построения национальной сети 66
19. Глобальная оптоволоконная инициатива США 68
20. Принципы построения экономически эффективных региональных сетей 68
21. Топология региональной сети 71
22. Политика региональной сети 72
23. Схема региональной сети 73
24. Задачи, требующие разрешения в процессе построения и эксплуатирования региональной сети 74
25. ПК-роутер 81
26. Watchdog 83
27. Надежность сети 89
28. Организация центрального сервера (узла) региональной сети 92
29. Модемный пул 92
30. Внешние каналы 94
31. Механизмы управления трафиком 95
32. Этап создания и развития сети 104
33. Этап эксплуатации сети 106

34. Система сетевого администрирования Nadmin 107
35. Темы рефератов-I 112
36. Темы рефератов-II 113
37. Вопросы для самоконтроля 114
38. Терминологический словарь 117

Список рисунков

1 Перфокарта 13
2 Колода перфокарт 14
3 Перфоленты 14
4 Аппарат коррекции ошибок пробивки перфоленты 15
5 Магнитофон для записи данных фирмы IBM, плотность записи: 100 бит на дюйм, длина ленты на бобине: 1200 футов, 1953 год 16
6 Совтский магнитофон ЕС5017 17
7 Маршрутизация в UUCP-сети. Простейшая (a) и доменная (b) организация таблицы маршрутизации 22
8 Пример IP-подсети `83.149.205.0/25`, понятие адреса и маски подсети 35
9 Классы IP-сетей 37
10 Проверка принадлежности IP-адреса подсети 40
11 Прохождение DNS-запроса 45
12 Сеть топологии «звезда» 52
13 Коаксиальный кабель, подготовленный для соединения с разъемом 53
14 BNC-разъем 54
15 T-разъем 55
16 Схема подключения рабочего места пользователя в локальной сети 10Base-2 с коаксиальным кабелем 56
17 Кабель из 4-х неэкранированных витых пар 58
18 Разъем RJ-45 для витой пары со вставкой 59
19 Подключение рабочего места пользователя в локальной сети 10Base-T витой парой 60
20 Хаб (концентратор) 61

21 Структура национальной сети 66
22 Слева: антенна параболическая ГРАД 2497; справа: антенна штыревая ГРАД 2401 79
23 График удельной стоимости (за 1 метр) 80
24 Новое поколение ПК-роутеров 82
25 Аппаратный Watchdog (принципы работы) 85
26 Новая версия Watchdog (вид снизу) 89
27 Новая версия Watchdog (вид сверху) 90
28 Блок бесперебойного питания 91
29 Стратегия ограничения пользователей на входе в сеть 97
30 Стратегия разделения ресурса между пользователями 98
31 Сетка приоритетов на использование ресурса 99
32 Очередь с приоритетами 100
33 Алгоритм «дырявого ведра» 102
34 Иерархические очереди 103
35 Карта Переславской сети 105
36 Структура системы Nadmin 109
37 Внешний вид системы Nadmin 111

1. Введение

Вся история развития человечества связана с тем, что люди в процессе своей жизни оперируют с тремя сущностями: «вещество», «энергия» и «информация», используя различные методы (и развивая новые методы) добычи, переработки, хранения и транспортировки вещественных объектов, энергии и информации. По мере развития цивилизации приоритет интересов общества перемещается слева направо по шкале:

$$\text{«вещество»} \Longrightarrow \text{«энергия»} \Longrightarrow \text{«информация»}.$$

Начиная со второй половины двадцатого века, с возникновением и развитием вычислительной техники и компьютерных сетей начался стремительный процесс формирования нового общества, в котором основную ценность и движущую силу приобретает информация.

Это отличает эпоху информационного общества от эпох сельскохозяйственного, сырьевого и промышленного производства, в которых к основным приоритетам относились категории «вещество» и «энергия». Это не означает, что человечеству больше не требуются вещественные ценности (пища, орудия труда, жилища, корабли, самолеты и т. п.) и разные виды энергии. Речь идет о том, что из триады «вещество», «энергия» и «информация» именно информация, способы (технологии) ее добычи, переработки, хранения и транспортировки будут играть главенствующую роль в будущем обществе.

Любая держава, стремящаяся к передовым позициям в мире, должна обладать самой передовой технологией, самыми точными и обширными сведениями, на основе которых будут строиться экономика и вооруженные силы. Всем остальным странам будет уготована функция поставщиков сырья и полуфабрикатов. Из этого сырья руками рабочих из тех же слаборазвитых стран, но на производствах, принадлежащих более прогрессивным и технологически развитым странам, будут создаваться высокотехнологичные изделия. Затем готовые изделия будут продаваться (в том числе и в слаборазвитые страны) по цене, на порядки превышающей цену исходного сырья.

Элита общества, «золотой миллиард» населения планеты постепенно избавляется от наследия индустриализации и входит в информационное общество, основной движущей силой которого, очевидно, является информация, а главное средство ее производства — это образование и наука, вычислительная техника и средства коммуникаций. Такой переход от индустриального общества к информационному есть ни что иное, как метасистемный переход (по терминологии В. Ф. Турчина [?bib:VF-MST]), квант развития, скачок от одного состояния человеческого общества к другому.

Разумеется, что такой скачок затронет лишь малую часть населения планеты, но мы хотим быть в их числе. Вхождение в новое состояние общества потребует пересмотра всех привычных стереотипов поведения, управления, организации жизни, экономики, политики и прочих сфер, характеризующих жизнь людей. Одной из основ нового общества станет повсеместное развитие глобальных коммуникаций, которые окончательно сотрут пространственные, возрастные, половые различия участников сетевого общения. На смену централизованному, иерархическому принципу управления приходит распределенный, сетевой принцип, не подчиняющийся привычным законам, представляющий собой результат сложного взаимодействия

автономных агентов, который, несмотря на противоречивость интересов, в конечном итоге вырабатывает некие решения, позволяющие всей структуре вести себя целенаправленно, и быть похожей на единый организм. Механизмы сетевых взаимодействий и самоорганизацию агентов еще предстоит осмыслить, хотя произойдет это — по теории В. Ф. Турчина — лишь после того, как процесс перехода к новой общественной формации будет завершен.

Тем не менее, уже сейчас очевидно, что новая реальность, которая разворачивается у нас на глазах, заставляет воссоздать в новых условиях тот опыт человечества, который был накоплен за тысячелетия его истории. В новом виртуальном мире человек выступает в качестве творца, создающего новую личность[1] , наделяя ее по своему желанию теми или иными качествами. Однако человек несовершенен и сотворенная им личность будет, как кривое зеркало отражать его самого, обнажая все то, что он сам пытается скрыть в реальном мире. Достаточная анонимность и вследствие того кажущаяся безнаказанность освобождают нереализованные желания.

Реальный мир за свою историю выработал ряд механизмов, позволяющих сдерживать разрушительные инстинкты человека, к ним относятся мораль и право, причем мораль имеет более глубокое влияние на личность: даже преступая закон, человек в большинстве случаев продолжает руководствоваться моральными принципами. В виртуальном обществе моральные принципы еще не успели пройти долгой исторической шлифовки, знакомые по реальному миру понятия здесь трансформированы.

Рассмотрим пример: виртуальное убийство (например, в игре Counter-Strike, Quake и т. д.) своего соперника, когда удачливый игрок приставляет оружие к голове противника и наблюдает, как после выстрела кровавые ошметки разлетаются по округе, при этом зная, что роль убитого играет его друг. Кто-нибудь задумывался об этичности такого поступка? «Разумеется, нет, — скажете вы, — это ведь только

---

[1]Если в жизни кто-то — скучный толстый мужчина, то в сети его могут представлять как молодого веселого парня, гоняющего игроков по Counter Strike. Сеть стирает все физические ограничения, оставляя только ментальность, как в фильме «Матрица» [?bib:matrix-movie], фантазирующем на тему отделения физического от ментального. Учитывая, что уже сейчас есть люди, которые зарабатывают, тратят, учатся, знакомятся и проводят все свободное время в Интернете, пищевая трубка как единственная связь с реальным миром уже не кажется такой уж нелепостью.

игра». Действительно, это игра. Однако, чего стоит точно так же одним кликом мыши добиться сбоя или отказа компьютера, на котором работает ваш приятель, воспользовавшись уязвимостью его операционной системы? Или послать кому-то вирус, уничтожающий данные на диске и стирающий BIOS (Win95.CIH — «Чернобыль» вывел из строя тысячи компьютеров по всему миру). Это уже просто «шуткой» назвать нельзя, «игра» в виртуальном мире уже напрямую касается мира реального и затрагивает благосостояние, а возможно, здоровье и даже жизнь человека. Обратим внимание, что в «виртуале» границы добра и зла, плохого и хорошего сглажены, и подчас привычных представлений о морали недостаточно, чтобы оценить тот или иной поступок, тем более все усугубляется уже упомянутой ранее мнимой свободой, анонимностью и безнаказанностью.

Вследствие приведенных выше рассуждений необходимо, прежде чем переходить к рассмотрению технических особенностей сетей, обратить внимание на сам феномен сети как явления и норм поведения человека в сетевом сообществе.

2. Сетевая этика

Этикой называют учение о морали, ее развитии, принципах, нормах и роли в обществе, как, впрочем, под словом *этика* понимается и совокупность норм поведения. *Сетевой этикой* мы будем называть совокупность норм поведения в сети. Этические нормы удерживают общество от хаоса и разрушения, позволяют уживаться людям друг с другом. Эти задачи стоят и перед сетевой этикой, которая, как и сетевое сообщество, еще только формируется и ее нормы еще окончательно не выработаны. Тем не менее, существуют своды правил, принятых немалым количеством провайдеров[2] . Рассмотрим пример таких норм, закрепленных в Абонентском договоре системы телекоммуникаций (СТ) «Ботик», предоставляющей в городе Переславле-Залесском услуги высокоскоростного доступа к городской компьютерной сети и к сети Интернет.

> **4. Ответственность сторон**
>
> 4.5. Исполнитель имеет право отключить Абонента от СТ «Ботик» (в том числе — закрыть входы в арендуемые им на узлах СТ «Ботик» FTP/WWW-пространство) в случае злоупотребления услугами сети. К злоупотреблениям, в первую очередь, относятся:

[2]Здесь «провайдер» — организация, занимающаяся предоставлением услуг доступа в Интернет.

- деятельность в сети, нарушающая действующее законодательство Российской Федерации (в том числе — авторское право);*
- широковещательное распространение по электронной почте материалов рекламного или коммерческого характера;
- распространение порнографических материалов по сети;*
- незапланированная или необоснованная загрузка ресурсов сети в ущерб другим пользователям;
- попытка доступа к данным и программам лиц, не имеющих на это права; попытки несанкционированного доступа к иным сетевым ресурсам; попытки подобрать пароли других пользователей; уничтожение или фальсификация данных и программ (в том числе, вследствие заражения компьютерными вирусами); незаконное копирование данных, нелегальная модификация данных;*
- распространение по сети информации, оскорбительной для других пользователей сети;*
- другие виды компьютерной преступности и нарушения общепринятой сетевой этики.

Знаком «*» мы отметили пункты, имеющие отражение в действующем законодательстве Российской Федерации. Более полный перечень [?bib:ofips-site-norms] норм пользования сетью содержится в выработанном сетевым сообществом «Открытом форуме Провайдеров Интернет Услуг» (Open Forum of Internet Service Providers — OFISP).

Фундаментальный принцип, провозглашаемый в этих документах, таков: правила использования любых ресурсов сети Интернет определяют владельцы этих ресурсов, и только они (здесь и далее словом «ресурс» обозначается любая совокупность программных и аппаратных средств, составляющих в том или ином смысле единое целое. Ресурсом сети Интернет могут считаться, например, почтовый ящик, персональный компьютер, виртуальный или физический сервер, локальная вычислительная сеть, канал связи и т. д.).

В следующих разделах мы рассмотрим некоторые нормы, регулирующие сетевое взаимодействие пользователей.

2.1. Запрет на передачу незапрошенных (нежелательных) сообщений. В последнее время в Сети очень часты факты широковещательного распространения по электронной почте и другими

средствами персонального обмена информацией материалов рекламного или коммерческого характера. Данное явление называют *СПАМ*. Термин «спам» ведет свое происхождение от старого (1972) скетча английской комик-группы Monty Python Flying Circus, в котором посетители ресторанчика, пытающиеся сделать заказ, вынуждены слушать хор викингов, воспевающий мясные консервы (SPAM — SPiced hAM). В меню этого ресторана все блюда состоят из содержимого этих консервов.

Применительно к навязчивой сетевой рекламе термин «спам» стал употребляться, когда рекламные компании начали публиковать в новостных конференциях Usenet свои рекламные объявления. По оценкам компании «Яndex» в 2003 году, 60–70% писем электронной почты представляют собой спам. Получение спама приводит пользователей российского Интернета к убыткам, превышающим $200 млн. в год, считают в интернет-холдинге Rambler. Только частные интернет-пользователи России ежегодно платят совокупный «налог на спам» порядка $120 млн. В мировом масштабе объемы спама стремительно растут. Если в 2001 г. спам занимал лишь 8% всего трафика электронной почты, то уже в 2002 году доля спама в общем трафике сообщений превысила 40%. Спам засоряет каналы передачи данных, увеличивает нагрузки на узлы сети, вызывает рост трафика и оплаты пользователями лишних мегабайтов почты.

Для одних спам — источник неприятностей, а для других — выгодный и быстро растущий бизнес. По мнению компаний-разработчиков программ, занимающихся фильтрацией спама, общие заработки спамеров в российском сегменте Интернета составляют порядка $3–5 млн. в год, что сопоставимо с объемом всего легального рынка онлайновой рекламы в Рунете. По их данным, в день в Рунете рассылается от 15 млн. до 30 млн. спамерских писем. Беда в том, что спам действительно очень эффективен по сравнению с обычной рекламой. Анализ показывает, что после рассылки спама за $500 звонков заказавшей рассылку фирме больше, чем после рекламы в глянцевом журнале за $5000. А о вреде для репутации, наживании врагов и прочих косвенных неприятностях такие заказчики пока не задумываются.

Вообще говоря, норма сетевой этики связанная с рассмотренным явлением весьма широкая: недопустимо распространение по электронной почте и другими средствами персонального обмена информации, которая может оказаться нежелательной (незапрошенной, досадной неожидоннастью) для получателя. Обратим внимание, что норма покрывает случаи одно- (и мало-) адресных рассылок и случаи рассылки некомерческой информации. Единственный существенный признак нарушения этики: получатель не ожидал такого письма, на запрашивал полученную информацию, сообщение для него оказалось нежелательным. В своей сетевой практики надо помнить об этом широком толковании понятия «нежелательная почта», и критически относится к каждому своему посланию, особенно для незнакомых адресатов.

2.2. Соблюдение правил, установленных владельцами ресурсов. Владелец любого информационного или технического ресурса Сети может установить для этого ресурса собственные правила его использования. Правила использования ресурсов, либо ссылка на них, публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Правила должны быть легко доступными, написанными с учетом разного уровня подготовки пользователей. Правила использования ресурса, установленные владельцем, не должны нарушать права владельцев других ресурсов или приводить к злоупотреблениям в отношении других ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

2.3. Недопустимость фальсификации. Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его и используемые им средства доступа к Сети. При этом пользователь не должен:

(1) Использовать идентификационные данные (имена, адреса, телефоны и т. п.) третьих лиц, кроме случаев, когда эти лица явно уполномочили пользователя на такое использование.
(2) Фальсифицировать свой IP-адрес, а также адреса, используемые в других сетевых протоколах, при передаче данных в Сеть.

(3) Использовать несуществующие обратные адреса при отправке электронных писем и других сообщений.
(4) Небрежно относиться к конфиденциальности собственных идентификационных реквизитов (в частности, паролей, прочих кодов авторизованного доступа), что может привести к использованию тех или иных ресурсов третьими лицами от имени данного пользователя (с сокрытием, таким образом, истинного источника действий).

2.4. Настройка собственных ресурсов. При работе в сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами. В связи с этим пользователь должен принять надлежащие меры по такой настройке своих ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов третьими лицами, а при обнаружении случаев такого использования принимать оперативные меры по их прекращению. Примерами потенциально проблемной настройки сетевых ресурсов являются:

(1) открытые ретрансляторы электронной почты (open SMTP-relays);
(2) общедоступные для неавторизованной публикации серверы новостей (конференций, групп);
(3) средства, позволяющие третьим лицам неавторизованно сокрыть источник соединения (например, открытые прокси-серверы);
(4) общедоступные широковещательные адреса локальных сетей, позволяющие проводить с их помощью атаки;
(5) электронные списки рассылки с недостаточной надежностью механизма подтверждения подписки или без возможности ее отмены;
(6) www-сайты и другие подобные ресурсы, осуществляющие отправку корреспонденции третьим лицам по анонимному или недостаточно аутентифицированному запросу.

2.5. Запрет несанкционированного доступа и сетевых атак. Не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них, за исключением случаев, когда атака на сетевой

ресурс проводится с явного разрешения владельца или администратора этого ресурса. Проблема компьютерного взлома, в отличие от вышеперечисленных, лежит не только в плоскости этических норм и правил хорошего тона, но и рассматривается как правонарушение, которое может повлечь административную и уголовную ответственность. В следующем разделе мы рассмотрим выдержки из действующего законодательства, направленные на борьбу с компьютерными правонарушениями.

2.6. Российское законодательство, применимое для борьбы с компьютерными преступлениями. Непосредственно законодательство России в области информатизации начало формироваться с 1991 года и включает ряд законов, среди которых:

- закон «О средствах массовой информации»;
- закон «О правовой охране программ для электронных вычислительных машин и баз данных»;
- закон «Об авторском праве и смежных правах»;
- закон «О связи»;
- закон «Об информации, информатизации и защите информации»;
- некоторые виды компьютерных преступлений описаны в 28 главе Уголовного Кодекса, которая называется «Преступления в сфере компьютерной информации».

Глава 28 УК. Преступления в сфере компьютерной информации.

Статья 272 Неправомерный доступ к компьютерной информации. Статья 272 Уголовного Кодекса предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию или копирование информации, нарушение работы вычислительных систем. Статья состоит из двух частей. В первой части наиболее серьезное наказание злоумышленика состоит в лишении свободы до двух лет. Часть вторая ст. 272 предусматривает в качестве признаков, усиливающих уголовную ответственность, совершение преступления группой лиц либо с использованием служебного положения (например, использование доступа к информационной вычислительной системе) и допускает вынесение приговора с лишением свободы до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ. Статья предусматривает уголовную ответственность за создание компьютерных программ для ЭВМ или их модификацию, заведомо приводящее к несанкционированному уничтожению, блокированию и модификации, либо копированию информации, нарушению работы информационных систем, а равно использование таких программ или машинных носителей с такими программами. Уголовная ответственность по этой статье возникает уже в результате создания программы, независимо от того, использовалась эта программа или нет. По смыслу ст. 273 *наличие исходных текстов* вирусных программ *уже является основанием для привлечения к ответственности.* Максимально тяжелым наказанием для преступника в этом случае будет лишение свободы до трех лет.

Глава 17 УК. Преступления против свободы, чести и достоинства личности.

Статья 129. Клевета. Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. Наказывается штрафом в размере от пятидесяти до ста минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.

Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев.

Статья 130. Оскорбление. Оскорбление, то есть унижение чести и достоинства другого лица, выраженное в неприличной форме, — наказывается штрафом в размере до ста минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца, либо обязательными работами на срок до ста двадцати часов, либо исправительными работами на срок до шести месяцев.

Оскорбление, содержащееся в публичном выступлении, публично демонстрирующемся произведении или в средствах массовой информации, — наказывается штрафом в размере до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до двух месяцев, либо обязательными работами на срок до ста восьмидесяти часов, либо исправительными работами на срок до одного года.

Глава 19. Преступления против конституционных прав и свобод человека и гражданина.

Статья 146. Нарушение авторских и смежных прав. Незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб, — наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

Глава 25. Преступление против здоровья населения и общественной нравственности.

Статья 242. Незаконное распространение порнографических материалов или предметов. Незаконное изготовление в целях распространения или рекламирования порнографических материалов или предметов, а равно незаконная торговля печатными изданиями, кино- или видеоматериалами, изображениями или иными предметами порнографического характера — наказываются штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев либо лишением свободы на срок до двух лет.

Глава 29. Преступление против основ конституционного строя и безопасности государства.

Статья 282. Возбуждение национальной, расовой или религиозной вражды. Действия, направленные на возбуждение национальной, расовой или религиозной вражды, унижение национального достоинства, а равно пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, национальной или расовой принадлежности, если эти деяния совершены публично или с использованием средств массовой информации,

- наказываются штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо ограничением свободы на срок до трех лет, либо лишением свободы на срок от двух до четырех лет.

Те же деяния, совершенные:

(1) с применением насилия или с угрозой его применения;
(2) лицом с использованием своего служебного положения;
(3) организованной группой;

наказываются лишением свободы на срок от трех до пяти лет.

2.7. Контроль за соблюдением сетевой этики. В силу несовершенства законодательства и недостатка судебного опыта, контроль над выполнением этических и правовых норм, несет на себе, прежде всего, провайдер. Поэтому, в Абонентском договоре СТ «Ботик» есть упоминание о возможности расторжения договора с абонентом, что дает право отказать в предоставлении услуг связи пользователю, нарушающему нормы Сетевой этики. С учетом возможных «тяжелых случаев» (принципиальный отказ следовать нормам сетевой этики и т. п.) данный раздел сформулирован максимально гибко. Рассмотрим Пункт 7 Договора:

«7. ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА *7.1. Настоящий Договор может быть расторгнут по инициативе любой Стороны без объяснения причин. Сторона-инициатор расторжения Договора должна письменно предупредить другую Сторону о своем намерении не позднее, чем за один месяц до предполагаемой даты расторжения Договора.*»

3. Из истории компьютерных сетей. Предпосылки возникновения сетей

Вычислительная техника зародилась в 40х–50х годах прошлого века. Первоначально компьютеров было немного, а первыми их потребителями были ученые, решающие важнейшие задачи (частенько связанные с оборонными проблемами). По мере развития вычислительной техники и увеличения количества компьютеров появилась задача обмена информацией между компьютерами. Это послужило предпосылкой создания компьютерных сетей.

3.1. Способы хранения информации. Прежде чем описывать способы передачи информации, рассмотрим, какие существовали методы хранения данных. Эти сведения помогут нам лучше понять процесс развития, как компьютерных сетей, так и всей компьютерной индустрии в целом.

3.2. Перфокарты. Использование перфокарт для хранения данных началось в 40-х годах 20 века и просуществовало до середины 80-х годов.

Перфокарта — это размеченный кусок картона, сетка разметки содержит восемьдесят колонок и двенадцати рядов (см. Рис. 1). В каждой позиции сетки разметки (на пересечении колонок и рядов) может быть или отсутствовать прямоугольное отверстие (перфорация). Каждая позиция на перфокарте кодировала один бит: если в позиции была пробито отверстие, то соответствующий бит полагался равным единице, в противном случае — нулю. Двенадцать позиций в одной колонке, то есть двенадцать бит, кодировали один байт. Как известно в одном байте восемь, а не двенадцать, бит. В колонке перфокарты избыточные биты используются для контроля и коррекции ошибок, которые могут возникнуть при чтении перфокарты. Всего на одной перфокарте в восьмитесяти колонках кодировалось восемьтесят байт.

Заметим, что даже в настоящее время сохранились отголоски использования перфокарт: стандартный текстовый видеорежим IBM PC также содержит восемьтесят символов в строке.

Файл в терминах перфокарт — колода перфокарт (Рис. 2). Чтение файла происходило путем установки колоды в считывающее устройство, которое брало поочередно карту за картой и при помощи фотопар определяло, в каких местах есть отверстие (то есть, закодирована единичка), а в каких — нет отверстия (нолик), занося в память байт за байтом. Так поочередно считывались все перфокарты файла.

Помимо устройств ввода данных с перфокарт, существовали и устройства вывода данных на перфокарты — *перфораторы*, — которые пробивали отверстия в «чистых» перфокартах.

Данная технология, просуществовав достаточно долго, была сопряжена со многими сложностями. Процедуры ввода информации были крайне ненадежны. Кроме того, простое рассыпание колоды перфокарт приводило к потере последовательности перфокарт в колоде, восстановление которой было крайне хлопотным делом.

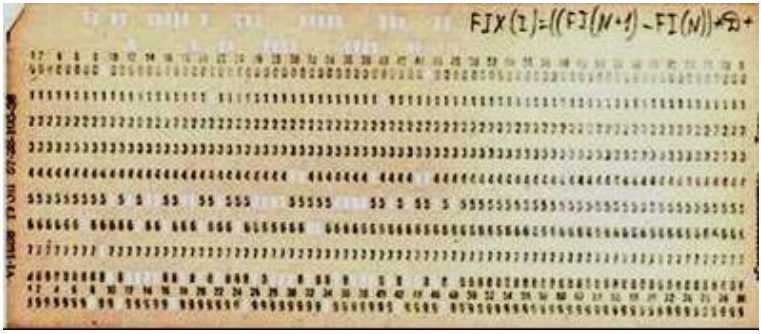

Рис. 1. Перфокарта

Рис. 2. Колода перфокарт

3.3. Перфоленты. Следующим шагом в хранении информации стали перфоленты, которые представляли собой ленты, в каждой колонке которой можно было (в виде последовательности отверстий

Рис. 3. Перфоленты

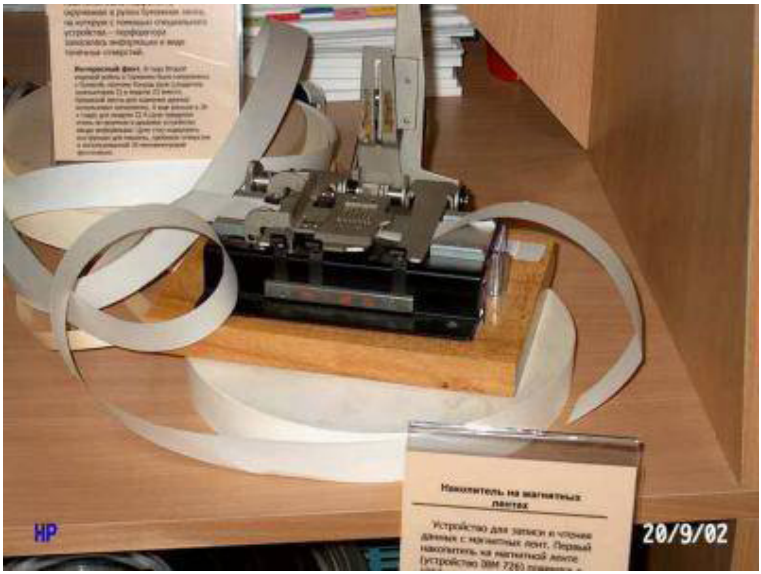

Рис. 4. Аппарат коррекции ошибок пробивки перфоленты

Рис. 5. Магнитофон для записи данных фирмы IBM, плотность записи: 100 бит на дюйм, длина ленты на бобине: 1200 футов, 1953 год

или их отсутствия) записать один байт. Это позволяло на одном метре ленты записать порядка половины килобайта. Кроме уплотнения записи информации, переход на перфоленту решал проблему нарушения порядка следования байтов по причине рассыпания колоды перфокарт. Однако, сохранялись другие возможные источники ненадежности хранения информации на таком носителе. Например, перфоленту легко было случайно порвать.

3.4. Магнитные ленты. Перфоленты сменили более прогрессивные технологии — магнитные ленты . Они позволяли записывать еще большие объемы информации, однако тоже были достаточно ненадежны, так как магнитный слой с пленки при высыхании осыпался, ленты могли рваться и размагничиваться. Для работы с магнитными лентами использовались сложные устройства чтения/записи (магнитофоны, Рис. 5 и 6), которые позволяли перемещать ленту с большой скоростью в рваном темпе (резкое начало движения и резкие остановки). При этом требовалось обеспечить сохранность ленты.

Рис. 6. Совтский магнитофон ЕС5017

3.5. Передача информации. Передача информации из одного места в другое может быть выполнена либо за счет физического перемещения носителя информации, либо за счет использования передачи данных по каналам связи. В обоих случаях можно говорить о следующих основных характеристиках передачи:

Задержка (latency) — измеряется в единицах времени (секунды). Определяется путем замера времени от момента *начала отправки* сообщения от источника до момента *начала получения* его в приемнике.

Скорость передачи (bandwidth), *пропускная способность* или *емкость канала* — отношение объема переданной информации к времени ее передачи (байт в секунду). Это максимальная пропускная способность, определяется измерением количества данных, полученных за некоторое время, начиная с момента получения первого байта сообщения.

Надежность канала (или способа передачи данных) — вероятность события «отправленная к получателю информация не будет потеряна, дойдет до него (возможно с искажениями)».

Достоверность передачи данных — вероятность события «если удалось передать информацию, то получено ровно то, что было отправлено, то есть передача информации произошла без искажения».

Основные требования к передаче данных (к каналу связи):

- низкая задержка;
- высокая пропускная способность канала;
- высокая надежность канала (или способа передачи данных);
- высокая достоверность передачи данных.

3.6. Физическая передача носителя информации. Самые первые передачи информации от одного компьютера к другому осуществлялись за счет физического перемещения колоды перфокарт, в дальнейшем — перфолент, бобин магнитных лент, носителей на жестких магнитных дисках и т.п. Этот способ передачи данных — физическая передача (перемещение) носителя информации, — до сих пор используется во многих учреждениях, да и просто владельцами персональных компьютеров — они часто передают друг-другу информацию на дискетах, CD ROM, Flash-накопителях и т. п.

Такой способ передачи данных может быть организован при минимальных капитальных затратах. При этом, такой способ полностью обеспечивает достоверность передачи информации, предварительно зафиксированной на носителе и проконтролированной непосредственно в пунктах ее регистрации (записи на носитель).

Для физического способа передачи информации задержка велика (если перевозка носителей производится автотранспортом, то это время в пути, минуты, а то и часы), однако пропускная способность канала (bandwidth) может быть огромной, так как весь объем данных на носителе достигает получателя практически одновременно[3], а перевезти (автомобилем) можно огромный объем информации.

Существенным недостатком такого способа обмена данными является сравнительно большая вероятность сбоя передачи информации, за счет физической порчи носителя: колода перфокарт может быть рассыпана, перфолента может порваться и т. п.

Таким образом, основные достоинства использования физического перемещения носителей данных для организации передачи информации:

---

[3]Более точно: пропускная способность в данном случае равна скорости ввода информации с перемещенного носителя и определяется используемым устройством ввода. Как правило, все подобные устройства характеризуются большими скоростеми чтения и передачи данных с носителя.

- минимальные капитальне затраты для организации передачи данных;
- высокая пропускная способность «канала»;
- высокая достоверность передачи данных;

основные недостатки:

- высокая задержка;
- низкая надежность передачи — возможность порчи носителя при физическом перемещении.

3.7. Передача по каналам связи. В 60-х–70-х годах появились первые устройства, позволяющие передавать информацию по каналам связи, а именно — по проводам. Так началась эра передачи данных без физического перемещения носителей информации. В качестве первых таких устройств были прародители современных модемов. В то время эти устройства позволяли передавать информацию между компьютерами по существующим системам связи: использовались обычные (коммутируемые) телефонные линии, сеансовое соединение, изначально исследователи не рассматривали возможность организации между компьютерами отдельного (выделенного) канала.

Для первых модемов скорость передачи информации была невелика: от нескольких сотен до тысячи бит в секунду. Это гораздо меньше, чем при физическом перемещении носителей информации. Однако задержка, которая при перемещении носителей составляла несколько минут, а то и часы, была существенно меньше:

- Доли секунд, если соединение между компьютерами уже было установлено. В этом случае весьма малое время поступления первого байта сообщения определяется высокой скоростью распространения сигнала по телефонному кабелю (скорости света) и небольшими аппаратными задержками в электронных схемах модемов.
- Несколько секунд — в противном случае. По большей части это то время, которое необходимо на «дозвонку» — набор телефонного номера и установления соединния между модемами.

После появления первых модемов, следующим шагом в развитии сетей было создание программной поддержки передачи данных. Зарождались первые протоколы передачи данных, програмные реализации этих протоколов и на их основе — первые компьютерные сети, в том числе и глобальные.

4. Компьютерные сети на базе протокола UUCP

4.1. Протокол UUCP. В данной работе мы будем использовать следующее значение термина «протокол»: *протокол передачи данных — это согласованный набор форматов сообщений, последовательностей сообщений и действий, позволяющий компьютерам обмениваться информацией.*

В данном разделе мы рассмотрим протокол UUCP, который послужил основой создания одних из первых глобальных компьютерных сетей. Этот протокол был впервые предложен лабораториями Bell в 1977 году. В названии протокола — UUCP: UNIX to UNIX Copy Protocol (Program) — нашел отражение тот факт, что UNIX в то время был наиболее распространеной операционной системой, по крайней мере, на тех ЭВМ, которые объединяли в компьютерные сети.

Проекты создания первых компьютерных сетей (в том числе на основе протокола UUCP) своей целью ставили обеспечение возможности пересылки файлов с одного (любого) компьютера в сети на любой другой[4]. При разработке проекта UUCP необходимо было учитывать следующие обстоятельства:

- неверно, что между любыми двумя компьютерами в UUCP-сети можно обеспечить прямой канал связи или иную возможность прямой (без посредников) передачи данных;
- как правило, компьютеры в то время соединялись между собой при помощи коммутируемых линий и использовался сеансовый режим связи.

4.2. Адресация в UUCP-сетях. Для того чтобы точно знать, куда надо передать тот или иной файл в сети, компьютеры должны были иметь свои собственные уникальные имена. В протоколе UUCP используется доменный принцип именования компьютеров. Например, имя одного из компьютера в переславской системе телекоммуникаций (СТ) «Ботик»:

[4]Интересно отметить, что коммуникации людей не рассматривались как цель в первых проектах компьютерных сетей.

```
pier.botik.ru
```

Здесь `pier` — имя машины (host name), `botik.ru` — имя домена (domain name), состоящий из поддоменов: `ru` — домен, принадлежащий России, `botik` — поддомен переславской системы телекоммуникаций «Ботик».

4.3. Графовое представление сети. При изучении сетей (в том числе UUCP-сетей) удобно сеть изображать в виде *графа*, в котором:

- узлы изображают компьютеры (или другие устройства), входящие в сеть;
- ребра изображают возможность прямой (без посредников) передачи данных между двумя компьютерами — это может быть выделенная линия связи или возможность установления сеанся связи по коммутируемым линиям.

Как правило данный граф *неориентированный* — ребра в нем ненаправленные, что отражает тот факт, что возможность передачи информации от компьютера **A** к компьютеру **B** как правило в сетях означает и возможность передачи информации в обратном направлении: от компьютера **B** к компьютеру **A**.

Как правило компьютерным сетям соответствуют (см. правую часть Рис. 7):

- *неполные графы*, то есть, неверно, что между каждыми двумя компьютерами существует прямой канал связи или иная возможность прямой (без посредников) передачи данных;
- *связанные графы*, то есть, верно, что из лююбого компьютера **A** к любому компьютеру **B** в сети найдется способ передачи данных, возможно через нескольких компьютеров-посредников.

4.4. Маршрутизация в сетях UUCP. Пусть некоторой компьютерной сети соответствует неполный связанный граф. Тогда при передаче сообщений в такой сети приводит к необходимости решения задачи маршрутизации: для передачи сообщения от компьютера **A** к компьютеру **C**, необходимо[5] построить путь (маршрут передачи сообщения) через ряд компьютеров-посредников:

$$\mathbf{A}, \mathbf{B}_1, \mathbf{B}_2, \ldots \mathbf{B}_n, \mathbf{C}$$

[5]Если между компьютерами **A** и **C** нет возможности непосредственной связи.

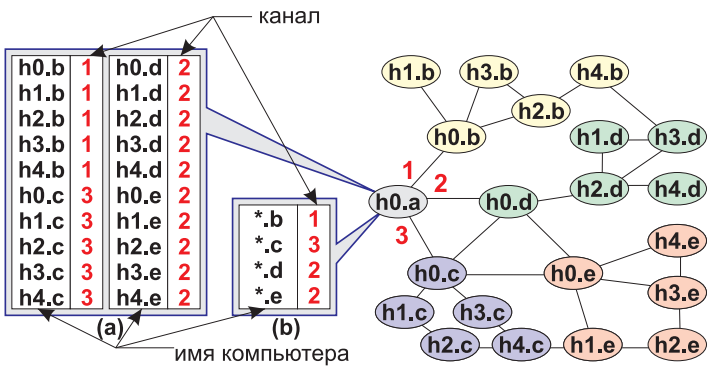

Рис. 7. Маршрутизация в UUCP-сети. Простейшая (a) и доменная (b) организация таблицы маршрутизации

где $\mathbf{B}_i$, $i \in \{1..n\}$, выбраны так, что между парами компьютеров

$$(\mathbf{A}, \mathbf{B}_1),\ (\mathbf{B}_n, \mathbf{C}) \text{ и } (\mathbf{B}_k, \mathbf{B}_{k+1}), \text{ где } k \in \{1..n-1\}$$

есть канал связи — есть возможность непосредственной передачи сообщений.

Так, в сети, граф которой показан на рисунке 7, для передачи сообщения от компьютера **h0.a** к компьютеру **h4.e** может быть использован такой путь:

$$\mathbf{h0.a} - \mathbf{h0.d} - \mathbf{h0.e} - \mathbf{h4.e}$$

В сетях UUCP задача маршрутизации при передачи сообщения от компьютера к компьютеру через несколько последовательных серверов (в случае отсутствия прямого канала между ними) решается при помощи построения и использовании *таблиц маршрутизации UUCP*. При этом, такая своя собственная таблица маршрутизации хранится в каждом компьютре, входящем в UUCP-сеть. Эта таблица для компьютера **A** в простейшем случае представляет собой набор упорядоченных пар:

$$host - channel$$

где *host* — имена всех компьютеров из UUCP-сети, *channel* — номер того самого канала, по которому требуется направить файл из компьютера **A**, чтобы он приблизился на один шаг к компьютеру с именем *host*.

На рисунке 7 показан (позиция (a)) пример такой таблицы маршрутизации, хранимой в компьютере **h0.a**. Видно, что при этом потребовалось в таблице маршрутизации компьютера **h0.a** перечислить все компьютеры сети и сопоставить каждому компьютеру один из трех каналов передачи данных, по которому сообщение будет «приближаться» к пункту назначения. Такой способ организации таблиц маршрутизации обладает рядом недостатков:

- Развитие сети приводит к росту размеров таблиц маршрутизации. Это влечет:
  - рост вероятности ошибок в заполнении таблиц маршрутизации;
  - повышении сложности работы с таблицами маршрутизации; существенные временные задержки при решении задачи маршрутизации.
- Изменение структуры сети в одной ее части (подключение новой машины, введение в строй нового канала и т. п.) влечет необходимость пересмотра всех таблиц маршрутизации во всех узлах сети.

Если учесть, что таблицы маршрутизации в UUCP чаще всего заполнялись вручную, то можно понять, что подобная простейшая форма организации таблиц маршрутизации была огромным тормозом на пути развития UUCP-сети.

Решение этой проблемы было найдено в использовании доменных имен компьютеров, в группировке компьютеров в таблицах маршрутизации в домены. В таком случае, зная название домена и имя компьютера-адресата, достаточно переслать сообщение серверу, отвечающему за данный домен, а он сам определит по своей локальной таблице маршрутизации путь, по которому должно проследовать сообщение далее до адресата.

При доменной организации таблиц маршрутизации в строках таблицы маршрутизации с каналами передачи данных уже могут связываться не только отдельные имена компьютеров, но и множества имен (домены и поддомены), задаваемые регулярными выражениями — см. рисунок 7, позицию (b), символ «*****» здесь обозначает «*произвольная подстрока*».

Данный способ доменной адресации и маршрутизации имеет следующие преимущества:

- способствует развитию сети за счет независимости таблиц маршрутизации от изменения сетевой инфраструктуры «внутри» доменов сети;
- уменьшает вероятность ошибок прои заполнении таблиц и ускоряет работу с таблицами маршрутизации — за счет большей компактности таблиц; доменов существенно меньше, чем компьютеров.

Вопросы и понятия, обсужденные выше — задача маршрутизация, таблицы маршрутизации, решение задачи маршрутизации только на один шаг, приближающий нас к адресату, — пожалуй впервые рассматривались именно при создании UUCP-сетей. И затем, те же самые вопросы и понятия рассматривались многократно в последующей истории развитии компьютерных сетей, но уже для других протоколов передачи данных. Мы увидем это при обсуждении технологии Switched Ethernet (раздел **??**) и маршрутизации в TCP/IP-сетях (раздел **??**).

Обсуждая вопросы маршрутизации в сетях необходимо отметить, что для нас важнее всего, чтобы сообщение было обязательно доставлено. Поэтому, в первую очередь важно, чтобы маршрут передачи сообщения был обязательно построен, а вопросы оптимальности маршрута (если путей доставки сообщения имеется несколько) могут уже рассматриваться во вторую очередь. Или не рассматриваться вовсе.

4.5. UUCP задания. Ключ к пониманию UUCP — понятие *задания* (*job*). Каждая передача между компьютерами **A** и **B**, которую пользователь инициализирует с помощью команд (uucp или uux) из набора программ UUCP, называется *заданием*. Задание состоит из программы, которая будет выполнена на удаленной системе **B**, и набора файлов, которые будут перемещены между системами **A** и **B**. Любая из этих частей может отсутствовать.

4.6. Сеансовая связь в протоколе UUCP. *Сеансность* связи означает, что линии коммуникаций между компьютерами **A** и **B** могут быть непостоянными. О времени сеансов связи договаривались заранее, и системный администратор каждого компьютера должен был вручную составить расписание сеансов.

4.6.1. *Установление сеанса связи.* При установлении между компьютерами **A** и **B** сеанса связи, компьютеры выполняют процедуру «*hand-shaking*» (*рукопожатие*), проверяя полномочия сторон на сеанс связи и готовность к приему/передаче данных — прежде чем начать передачу данных, инициатор обмена должен авторизоваться в ЭВМ, с которой планируется обмен, и активизировать ее систему UUCP.

4.6.2. *Передача информации.* После установления сеанса связи передача информации осуществляется в обе стороны: сначала сервер-инициатор сеанса связи **A** передавал всю информацию скопившуюся у него для передачи в **B**, после чего право передачи передавалось другой стороне и т. д. При этом:

- Во время передачи заданий с компьютера **A** в компьютер **B**, пересылаются не только те здания, которые адресованы непосредственно компьютеру **B**, но также и задания для таких компьютеров **C**, что между **A** и **C** нет непосредственной связи и путь из **A** в **C** проходит через посредника **B**.
- Все задания, передаваемые с компьютера **A** в компьютер **B**, сохраняются в специальном spool-буфере, а их обработка будет выполнена *после завершения сеанса* связи — одним абзацем ниже это обсуждается подробнее.

4.6.3. *Завершение сеанса связи.* Когда обе стороны выполняли все необходимые передачи данных — установленный сеанс связи завершался.

4.6.4. *Сохранение информации для последующей обработки (spooling).* UUCP не вызывает выполнения задания на удаленной системе немедленно сразу после перемещения на нее задания. Вместо этого описание задания временно сохраняется на удаленной системе в специальном хранилище (*spool*). Это называется *буферизацией заданий* (*spooling*).

Более точное описание этого процесса:

- Все полученные во время передачи от компьютера **A** к компьютеру **B** задания сохраняются в spool-буфере без какой либо обработки.
- Обработка всех сохраненных в spool-буфере заданий выполняется программой uuxqt, которая выполняется после разрыва соединения.
- Программа uuxqt просматривает все задания **job** в spool-буфере на компьютере **B** и для каждого из них:

– Программа uuxqt обеспечивает запуск задания **job** на исполнение, если задание **job** адресованно как раз компьютеру **B** — то есть задание уже достигло конечной точки назначения, где оно должно быть выполнено.
– Программа uuxqt обеспечивает планирование дальнейшей пересылки задания **job**, если задание **job** адресованно другому компьютеру **C** — то есть задание еще не достигло конечной точки назначения, компьютер **B** всего лишь посредник (перевалочный пункт) на пути к пункту назначения.

4.6.5. *Общая структура сеанса связи в UUCP.* Тем самым, сеанс связи состоит из следующих этапов: установление связи (открытие канала), последовательность выполнения запросов на пересылку файлов (в одну и другую сторону), сохранение информации для последующей обработки (spooling), закрытие канала и обработка заданий в spool-буфере.

4.7. Схема работы протокола UUCP. Резюмируя описание работы UUCP-сети, перечислим пошаговую последовательность выполнения операций компьютеров, взаимодействующих по протоколу UUCP.

(1) Формирование множества заданий на сервере-отправителе.
(2) Сортировка заданий по тому, в какие каналы они должны проследовать — определяется по адресу получателя при помощи таблицы маршрутизации.
(3) Установление связи (в соответсвии с расписанием сеансов связи) с удаленным сервером по одному из каналов, выполнение процедуры hand-shaking.
(4) Передача всех сообщений, назначенных для передачи по данному каналу. В процессе передачи осуществляется контроль надежности передачи данных: подсчет контрольных сумм и подтверждение удачной передачи — квитирование. С сервера-отправителя сообщение удаляется только после подтверждения удачной передачи. При приеме задания сервером-получателем оно сохраняется в spool-буфеере для последующей обработки.
(5) После передачи всех сообщений, назначенных для передачи по данному каналу, инициатива передачи отдается серверу-получателю и выполняется прием сообщений от него. Когда

он передаст все сообщения, он вернет инициативу передачи обратно и цикл повторится снова.

(6) Если ни у одной из сторон, участвующей в сеансе связи не окажется заданий, назначенных для передачи по установленному каналу, то стороны выполняют разрыв соединения.

(7) После разрыва соединения стороны выполняют образботку полученных и сохраненных в spool-буфеере заданий:
   - Обеспечивается запуск задания **job** на исполнение, если задание **job** адресованно как раз данному компьютеру — то есть задание уже достигло конечной точки назначения, где оно должно быть выполнено.
   - Обеспечивается планирование дальнейшей пересылки задания **job**, если задание **job** адресованно другому компьютеру — то есть задание еще не достигло конечной точки назначения.

4.8. Возможные ошибки маршрутизации и способы борьбы с ними в UUCP-сетях. Рассмотрим произвольную UUCP-сеть, в которой в каждом узле определена некоторым образом (правильно или с ошибками — не важно) таблица маршрутизации. Предположим, что все эти таблицы маршпрутизации зафиксированы — не меняются. Пусть из узла **A** данной сети послано сообщение в узел **B**. В данных предположениях несложно доказать, что возможны только три исхода данной посылки (вне зависимости от правильности заполнения таблиц маршрутизации):

- *Успешная доставка*: за конечное число передач сообщение будет доставлено в узел **B**.
- *Отсутствие маршрута*: за конечное число передач сообщение достигнет узла **C** в котором в таблице маршрутизации шаг очередной передачи будет неопредлен (либо в таблице не будет пары, отвечающей узлу **B**, либо эта пара будет указывать на несуществующий канал).
- *Петля в маршрутизации (routing loop)*: за конечное число шагов из узла **A** сообщение достигнет некоторого узла **C**:

  $$\mathbf{A} - \mathbf{A}_1 - \mathbf{A}_2 - \ldots - \mathbf{A}_n - \mathbf{C}$$

  затем через некоторое число шагов, пройдя по некоторой петле, сообщение сново попадет в узел **C**:

  $$\mathbf{C} - \mathbf{C}_1 - \mathbf{C}_2 - \ldots - \mathbf{C}_k - \mathbf{C}$$

и в дальнейшем сообщение будет совершать бесконечную цепочку передач по данной петле:

$$\begin{aligned}&\mathbf{C}-\mathbf{C}_1-\mathbf{C}_2-\ldots-\mathbf{C}_k-\mathbf{C}-\\&\quad\mathbf{C}_1-\mathbf{C}_2-\ldots-\mathbf{C}_k-\mathbf{C}-\\&\quad\mathbf{C}_1-\mathbf{C}_2-\ldots-\mathbf{C}_k-\mathbf{C}-\\&\ldots\end{aligned}$$

В общем случае, сбой в доставке сообщения связан либо с отсутствием маршрута (и этот случай распознается явно через конечное числов шагов), либо с бесконечной последовательностью передач сообщения (на практике при этом как правило обнаруживается петля в маршруте).

В UUCP применяются дледующие приемы для борьбы с ошибками маршрутизации, локализации места этих ошибок и поддержки их исправления.

- *Фиксация маршрута доставки.* При прохождении сообщения от отправителя к получателю, на каждом шаге в сообщении запоминается информация о том, через какие узлы сети сообщение прошло, вся цепочка прохождения сообщения фиксируется в служебных заголовках сообщения.

  Заметим, что при очередном шаге, анализируя эти служебные заголовки можно обнаружить петлю в маршруте на раннем этапе — при попытке передать сообщение в узел, в котором оно уже бывало.
- *Ограничение числа передач.* Для борьбы с возможными бесконечными блужданиями сообщения в сети из-за ошибок маршрутизации на узлах сети число уже выполненых шагов передачи сообщения сравнивали с некоторым предельным значением. Например, можно было задать ограничение: сообщение не может делать более 50 шагов. При достижении данного ограничения передача сообщение объявлялось неудачной.
- *Гарантированная передача сообщения о неудачной доставке сообщения.* Если исходное сообщение не удалось доставить адресату, то отправителю обратно отправлялось сообщение об ошибке, которое включало исходное сообщение, путь, которое оно прошло до обнаружения ошибки и описание ошибки: отсутствие маршрута, петля в маршруте или превышение ограничения числа передач.

Это сообщение об ошибке отправляется по маршруту, в точности повторющем (но в обратном направлении, конечно) уже пройденный путь. Такой подход (как «нить Ариадны» в известной легенде) гарантировал доставку сообщения об ошибке к отправителю.

Получив сообщение об ошибке в доставке системный администратор, отвечающий за UUCP-подсистему (постмастер) узла-отправителя, изучал путь прохождения письма, находил ошибку в маршрутизации и сообщал об этом постмастеру того сервера, на котором им была замечена ошибка в локальной таблице маршрутизации.

4.9. Первые приложения UUCP сетей. Создание протокола UUCP и глобальных стей на его основе стало огромным прогрессом в деле реализации новых возможностей обмена данными между компьютерами. Когда между многими компьютерами в мире были установлены расписания сеансов связи, и сложилась глобальная система UUCP передачи данных, тогда был завершен первый этап создания глобальных компьютерных телекоммуникаций.

Была реализована возможность передачи информации из любого компьютера в мире на любой другой компьютер в мире. Эта передача осуществлялась с приличной (по тем временам) скоростью и с весьма небольшой задержкой: сообщение из любой точки земного шара в любую другую точку приходило за одни–двое–трое суток.

С самого начала протокол UUCP создавался как способ обмена данными между программами, не между людьми. Однако в скором времени после создания глобальных UUCP-сетей их приспособили для обмена информацией между людьми. Именно тогда зародилось такое понятие как *электронная почта* (*e-mail*).

4.9.1. *Электронная почта.* Электронная почта явилась первым сетевым приложением, ориентированным для поддержки взаимодействия людей, а не компьютеров. И до сих пор в электронной почте используется стандарт записи электронных адресов людей, принятый именно в эпоху UUCP. E-mail-адреса пользователя *user* зарегистрированного на компьютере `host.domain` до сего дня записываются как

`user@host.domain`

Здесь символ «`@`» читается как «at коммерческое», таким образом, адрес следует читать как «*user* at *host*».

4.9.2. *Адресаты электронного письма.* В служебной части электронного письма, определяющей, куда надо письмо доставить, допускает наличие нескольких адресов, объединенных в три группы: «`To:`», «`Cc:`», «`Bcc:`».

- `To:` — список прямых адресатов, перечисленных через разделитель; как правило это адреса персон, от которых ожидается получить отклик;
- `Cc:` (*Carbon Copy*, «под копирку») — список адресатов, которые должны быть в курсе данного письма, причем основные получатели также видят, что копия отослана по указанным в поле `Cc:` адресам; как правило это адреса персон, от которых не обязателен отклик, но которых желательно держать информированными по обсуждаемому вопросу;
- `Bcc:` (*Blind Carbon Copy*, слепая (тайная) копия) — список адресатов, которых желательно держать информированными по обсуждаемому вопросу, причем в тайне от других получателей.

4.9.3. *Маршрутизация электронного письма с множеством получателей.* Так как в электронном письме имеется несколько адресатов, то маршрутизация их доставки имеет в UUCP-сетях ряд особенностей — если в адресной части письма указано более одного получателя, то:

- Для каждого из адресов решается задача маршрутизации.
- Если ряд адресов имеет одинаковый очередной шаг маршрута следования, для этих адресов письмо не дублируется, а выполняет очередной шаг как единое задание.
- Дублирование письма происходит только в том случае, если в некоторый момент маршруты достижения различных адресатов разветвляются.

Такой механизм позволяет уменьшить трафик при передаче писем.

4.9.4. *Информационные сервисы, основанные на электронной почте.* С возникновением электронной почты появилось большое количество сервисов (программ), которые имели почтовый интерфейс.

Пользователь такого сервиаа посылает на адрес программы письмо-запрос в специальном формате, описывающее заказ на выполнение тех или иных действий. Программа после получения письма выполняла запрошенные действия (например, производила поиск в базе данных, бронировала авиабилет и т. д.) и отправляла письмом с описанием результата своей работы пользователю.

Такой режим работы с информационным сервисом называют *off-line-режимом*.

4.9.5. *Новостные службы (news).* Помимо электронной почты и информационных сервисов, основанных на электронной почте, на базе протокола UUCP возникла служба новостей (*News*), позволяющая на отдельном сервере аккумулировать сообщения по некоторой *теме* и предоставлять пользователям возможность прочтения существующих сообщений, написание реплик на уже существующие сообщения и написание нового сообщения.

Тем самым уже во времена UUCP-сетей велись коллективные обсуждения различных тем, в news-архивах строились деревья сообщений наподобие того, как это сейчас обычно делается в Веб-форумах.

5. Протокол TCP/IP

5.1. Предпосылки возникновения протокола TCP/IP. С ростом количества компьютеров и расширением сетей стали всё более явно проявляться недостатки протокола UUCP. Основными из них являлись

- сеансность связи, что определяло высокие задержки передачи файлов (из практики: до трех суток);
- возможность монополизации канала;
- низкие скорости решения задачи маршрутизации, высокая вычислительная нагрузка на процессоры компьютеров-узлов UUCP-маршрутизации.

Перечисленные недостатки препятствовали увеличению скорости и качества передачи данных, что делало невозможным сетевое общение в реальном времени (on-line).

Рассмотрим подробнее два последних недостатка.

5.1.1. *Возможность монополизации канала.* Протокол UUCP обладал тем существенным недостатком, что позволял монополизировать канал передачи. В UUCP допускается передача файлов большого размера. Время передачи такого файла может быть весьма значительным и на все время передачи файла используемый для передачи канал будет монополизирован — через него будет невозможно передавать никакую иную информацию, ни в ту, ни в иную сторону[6]. Таким образом, если отправитель создает файл с UUCP-заданием огромных

[6]Более того, как правило UUCP-мапины обладали небольшим количеством модемов, часто — всего одним. И в этом случае монополизируестя не только канал, но и весь узел или даже пара узлов, задействованных в передаче.

размеров, то вся цепочка серверов на пути следования данного сообщения будет в течение достаточно длительного времени заниматься исключительно его «прокачкой», а остальные задания будут стоять в очереди.

Более того, монополизация пары узлов на длительное время возможна даже и в случае передачи небольших заданий — за счет того, что соединение не будет разрываться до тех пор, пока хотя бы одной стороне есть что передавать другой стороне, при этом, во время передачи работающими на узлах программами могу порождаться новые задания на передачу.

5.1.2. *Высокая сложность задачи маршрутизации.* Маршрутизация в UUCP основана на сравнении адреса-строки с шаблоном, представляющим собой регулярное выражение. Данная операция требует исполнения нескольких тысяч команд процессора. Поиск в таблице маршрутизации в UUCP решается исключительно линейно, поэтому для достаточно больших таблиц время существенно увеличивается. Обозначим через M среднее количество команд центрального процессора, которое необходимо выполнить для сравнения адреса с шаблоном, а через N — количество строк в таблице маршрутизации (количество сетей). Тогда среднее количество команд центрального процессора, которое необходимо для решения задачи маршрутизации равно $\frac{N \times M}{2}$.

С ростом количества сетей время передачи будет расти линейно. При весьма правдоподобных и скромных предположениях M=1000 и N=2000 получается, что задача маршрутизации решается примерно за один миллион команд (что занимало около 1 секунды в те времена).

5.1.3. *Протокол TCP/IP.* Перечисленные выше проблемы удалось успешно решить в протоколе *TCP/IP* — Transmission Control Protocol/Internet Protocol—Протокол управления передачей/Межсетевой

протокол[7]. В 1983 данный протокол был принят как стандарт и от всех узлов (хостов) в сети требовалось его использование.

5.1.4. *Решение в рамках протокола TCP/IP основных проблем протокола UUCP.* Обсудим, как в рамках протокола TCP/IP были решены проблемы монополизации канала и сложной маршрутизации.

Очевидно, что основным монополизирующим фактором является большой размер сообщения. Проблему монополизации удастся решить, запретив сообщениям быть произвольного размера.

Именно эта идея усовершенствования протокола была реализована в TCP/IP: было введено ограничение на максимальную длину *пакета* — атомарной единицы передаваемого сообщения. Обычно максимальная длина пакета (Maximum Transmission Unit, MTU[8]) в TCP/IP составляет 1500 байтов.

Наложенное ограничение решило еще одну проблему: были ослаблены требование к ресурсам маршрутизаторов — устройств, занимающихся маршрутизацией пакетов. Маршрутизаторам достаточно иметь оперативной памяти столько, чтобы одновременно хранить небольшое количество пакетов стандартного (обычно 1500 байт) размера.

Обсудим решение проблемы большой сложности задачи UUCP-маршритизации. Корни данной проблемы в следующем:

- очень сложное понятие «UUCP-адрес» — доменное имя, строка символов произвольной длины;
- очень сложное понятие «UUCP-подсеть» — задается регулярным выражением;
- как результат:
  - очень сложная проверка условия «UUCP-адрес входит в UUCP-подсеть?» — сравнение строки с регулярным выражением, может потребовать для своего вычисления исполнения около тысячи команд процессора;

---

[7]Идея открытой сетевой архитектуры была впервые высказана Робертом Каном в 1972 году, вскоре после того, как он начал работать в DARPA (Defense Advanced Research Projects Agency).

Деятельность, которой занимался Кан, первоначально была частью программы разработки пакетных радиосетей, но впоследствии она переросла в полноправный проект под названием «Internetting». Для работоспособности пакетных радиосистем ключевым элементом был надежный сквозной протокол, способный поддерживать эффективные коммуникации, несмотря на радиопомехи или временное непрохождение радиосигнала на том или ином участке.

[8]См. `http://en.wikipedia.org/wiki/MTU(networking)`

– приходится использовать линейный поиск в таблице UUCP-маршрутизации, трудно использовать стандартные подходы к ускорению процедуры поиска в таблице (например, использовать метод половинного деления, дихотомию).

Данный анализ дает очевидный подход к решению данной проблемы:

- надо использовать простое понятие «адреса» — например, натуральное число ограниченной длины (32 бита, например);
- надо использовать простое понятие «подсеть» — например, подсеть это интервал $[a..b]$ адресов;
- как результат получим:
  - очень простую проверку условия «адрес входит в подсеть?» — такая проверка потребует для своего вычисления исполнения около пяти команд процессора ($K = 5$);
  - в таблице маршрутизации можно все подсети отсортировать и, после этого, легко будет использовать стандартный подход к ускорению процедуры поиска в таблице — использовать алгоритм дихотомии.

Использование дихотомии в процедуре поиска в таблице маршрутизации позволяет радикально уменьшить порядок сложности алгоритма: если в таблице маршрутизации будет N записей о подсетях, то поиск в таблице потребует выполнения всего лишь $K \times \log_2 N$ команд процессора, где K — количество команд, требуемых для сравнения адреса с подсетью, ниже будет показано, что можно обеспечить $K = 5$.

Именно такие усовершенствования и были введены в протоколе TCP/IP:

- Для адресации участников сети используются так называемые *IP-адреса* — числовые адреса с длиной 4 байта (32 разряда).
- IP-сети (IP-подсети) по сути являются отрезками (подряд идущих) IP-адресов.

Все это позволило радикально улучшить (именно так, как обсуждено выше) алгоритмы маршрутизации в TCP/IP. Сравнение необходимого числа операций и времени для решения задачи маршрутизации в UUCP и TCP/IP приведено в Таблице 1. Время в таблице посчитано из предположения, что центральный процессор способен выполнить

Таблица 1. Сравнение сложности задачи маршрутизации в UUCP и TCP/IP

Протокол	N	M, K	Кол-во операций	Время (мсек)
UUCP	2 000	$M = 1\,000$	$\sim 1\,000\,000$	$\sim 1\,000$
TCP/IP	2 000	$K = 5$	~ 55	~ 0.055

один миллион команд в сегунду, что соответствует действительности на период перехода от UUCP к TCP/IP.

5.2. IP-адреса и IP-подсети. Как уже было сказано, в TCP/IP-сетях для адресации участников сети используются так называемые *IP-адреса* — числовые адреса с длиной 4 байта (32 разряда). Данные адреса принято записывать как четверку десятичных чисел, разделенных точкой. Каждое из этих чисел представляет значение соответсвующего байта и, соответсвенно, может быть от 0 до 255. Например, в сети телекоммуникаций «Ботик» центральный сервер `www.botik.ru` имеет IP-адрес `193.232.174.1`.

В UUCP был заложен удачный принцип разбиения сети на подсети. Этот принцип нашел свое отражение и в TCP/IP.

Подсетью в TCP/IP будем называть несколько подряд идущих IP-адресов $A_0, A_1, ..., A_N$, двоичная запись которых имеет одинаковое для них всех *начало* (*префикс*, некоторой длины L) и все возможные значения в *окончаниях* (в *суффиксах*, который имеет длину $32 - L$). Маской[9] данной подсети будем называть 32-разядное число M, двоичная запись которого имеет следующий вид: L единиц, за которыми следует $32 - L$ нулей.

В силу данного определения:

- первый (младший) адрес A_0 в подсети имеет вид «префикс, за которым записан суффикс из одних нулей»;
- последний (старший) адрес A_N в подсети имеет вид «префикс, за которым записан суффикс из одних единиц»;
- количество IP-адресов в IP-сети равно 2^{32-L}, где L длина префикса;
- подсеть однозначно определяется значением младшего адреса A_0 в подсети — его принято называть *адресом подсети* $A = A_0$, — и длиной префикса L;

[9]Маска подсети удобна для выполнения поразрядных операций с IP-адресами и с адресами IP-подсетей — будет обсуждено ниже.

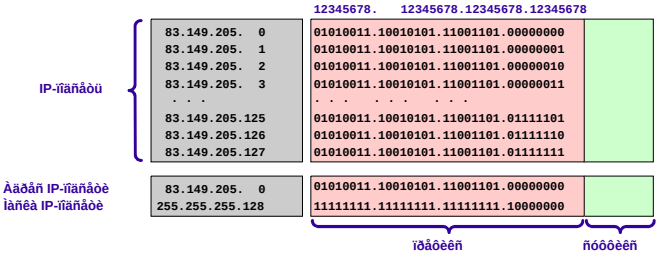

Рис. 8. Пример IP-подсети `83.149.205.0/25`, понятие адреса и маски подсети

- пара «адрес подсети и ее маска» — (A, M), — так же однозначно определяет подсеть.

На практике, для обозначения IP-подсетей используют либо указание адреса подсети A и ее маски M, либо такую нотацию: адрес подсети A, за которым размещают символ «/» и затем длину L префикса. На рисунке 8 проиллюстрированы все введеные выше понятия на примере IP-подсети `83.149.205.0/25`.

5.3. Классы IP-адресов и IP-подсетей. Хотя на практике используют IP-подсети с самой различной длиной префикса, в качестве наиболее широко применениимых было введено 5 предопределенных классов IP-адресов, отличающиеся количеством бит в сетевом номере — то есть, длиной префикса, — и количеством бит в номере хоста — то есть, длиной суффикса. При этом, класс адреса определяется значением его первых бит (см. Рис. 9).

Рис. 9. Классы IP-сетей

Адреса класса A содержат в старшем бите «0», предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов. Всего имеется $2^7 = 128$ подсетей класса A, в каждой подсети имеется $2^{24} = 16\,777\,216$ адресов, всего — $2^{31} = 2\,147\,483\,648$ адресов.

Адреса класса B содержат в двух старших битах «10», используются в сетях среднего размера, например, сетях крупных городов, крупных университетов или компаний. Всего имеется $2^{14} = 16\,384$ подсетей класса B, в каждой подсети имеется $2^{16} = 65\,536$ адресов, всего — $2^{30} = 1\,073\,741\,824$ адреса.

Адреса класса C содержат в трех старших битах «110» используются в сетях с небольшим числом компьютеров. Всего имеется $2^{21} = 2\,097\,152$ подсетей класса C, в каждой подсети имеется $2^8 = 256$ адресов, всего — $2^{29} = 536\,870\,912$ адресов.

Адреса класса D используются при обращениях к группам машин (multicast groups), а *адреса класса E* зарезервированы на будущее.

5.4. Специальные (выделенные) IP-адреса. Некоторые IP-адреса являются выделенными и трактуются по-особому:

- `0...00...0` — «данный узел», local host, получатель совпадает с отправителем;
- `0...0h...h` — узел `h..h` в той же подсети, что и отправитель;
- `1...11...1` — широковещание, получателями являются все узлы в подсети отправителя;
- `n...n0...0` — адрес подсети `n..n`;
- `n...n1...1` — широковещание, получателями являются все узлы в подсети `n...n`;
- `127.x.x.x` — посылка пакета к самому себе, «петля», loop back (используется для тестирования).

В выделенных IP-адресах все нули соответствуют либо данному узлу, либо данной IP-сети, а IP-адреса, состоящие из всех единиц, используются при широковещательных передачах в рамках подсети.

Для ссылок на всю IP-сеть в целом используется IP-адрес с нулевым номером узла.

Особый смысл имеет IP-адрес, первый октет которого равен 127 — «петля». Он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы «петля». Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые. Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127.

5.5. Реализация алгоритма маршрутизации методом дихотомии. В сетях TCP/IP важную роль играют *маршрутизаторы* (routers). Именно они обеспечивают доставку пакетов адресатам. Получая по некоторому *интерфейсу* пакет, адресованный узлу с IP-адресом x маршрутизатор должен определить, по какому интерфейсу (по какому направлению) надо послать данный пакет дальше, чтобы он продолжал приближаться к адресату x.

Для этого маршрутизатор использует находящуюся в его памяти *таблицу маршрутизации*. В разделах **??**, **??** и **??** будет изложено каким образом и в какое время выполняется заполнение таблицы маршрутизации. А здесь мы рассмотрим структуру данной таблицы и ее использование в процессе решания задачи маршрутизации.

Таблицу маршрутизации можно рассматривать как массив из троек величин:

$$(A_0, M_0) \to i_0\,,\ (A_1, M_1) \to i_1\,,\ \ldots (A_N, M_N) \to i_N$$

здесь (A_k, M_k) — адреса и маски подсетей, i_k — номер интерфейса маршрутизатора (то есть, направление) по которому надо посылать пакеты, чтобы они «приблежались» (двигались по направлению) к узлам подсети (A_k, M_k).

Задача маршрутизации в данном случае сводится к следующему: по заданному адресу x получателя пакета надо в таблице маршрутизации найти такую тройку $(A_k, M_k) \to i_k$, что адрес x принадлежит подсети (A_k, M_k). После чего надо пакет отправить по интерфейсу i_k.

Если таблицу маршрутизации отсортировать по возрастанию троек $(A_k, M_k) \to i_k$, то поиск в таблице маршрутизации можно выполнять с использованием метода деления пополам — алгоритма дихотомии. Основная суть алгоритма[10] в следующем:

(1) Введем термин *зона анализа*: первоначально рассматриваем таблицу целиком, в дальнейшем мы будем из зоны анализа убирать целые куски таблицы.
(2) Если зона анализа пустая, то есть в таблице маршрутизации не оказалось подсети, которой принадлежит адрес x, то считаем, что задача маршрутизации решена, пакет передается по специальному умолчательному интерфейсу i_{def} (default, обсуждается в разделе **??**) и на этом исполнение алгоритма маршрутизации завершается. Если зона анализа не пустая, то переходим к следующему пункту.
(3) Рассматриваем элемент $(A_k, M_k) \to i_k$, находящийся (примерно) в середине зоны анализа.
(4) Если адрес x принадлежит подсети (A_k, M_k), то задача маршрутизации решена, пакет передается по интерфейсу i_k и на этом алгоритм завершается.
(5) Если адрес x меньше всех адресов из подсети (A_k, M_k), то удаляем из зоны рассмотрения тройку $(A_k, M_k) \to i_k$ и все тройки правее ее. Возвращаемся к шагу 2.
(6) Если адрес x больше всех адресов из подсети (A_k, M_k), то удаляем из зоны рассмотрения тройку $(A_k, M_k) \to i_k$ и все тройки левее ее. Возвращаемся к шагу 2.

[10] Технические детали алгоритма очевидны и здесь рассматриваться не будут.

Видно, что на каждой итерации алгоритма зона амнализа сокращается не менее, чем вдвое. Поэтому, если на исполнение каждой итерации приходится K команд процессора маршрутизатора, то на решение всей задачи маршрутизации будет поитрачено (в худшем случае) $K \times \log_2 N$ команд процессора.

5.6. Алгоритмы проверки принадлежности IP-адреса какой-либо подсети. Рассмотрим более детально операции, производимые маршрутизатором для определения принадлежности адреса к некоторой подсети из таблицы маршрутизации. Пусть A — адрес подсети, M — маска, а x — IP-адрес для проверки на принадлежность к данной подсети.

Будем предполагать, что центральный процессор маршрутизатора поддерживает следующие команды над 32-разрядными целыми числами a и b без знака:

- a `>` b — обычное (арифметическое) сравнение 32-разрядных целых чисел a и b без знака;
- a `xor` b — побитовое сложение по модулю 2 («исключающее или»);
- a `and` b — побитовая операция «и»;
- a `or` b — побитовая операция «или»;
- `not` a — побитовая операция отрицания «не».

Для определения факта, что x принадлежит подсети (A, M) надо проверить, что адрес подсети A и проверяемый адрес x имеют одинаковый префикс. Это можно сделать за две операции центрального процессора: `(`x `xor` A`) and` M.

Действительно, после выполнения операции `xor` мы получаем результат побитового сравнения x и A: если некие биты x и A различны, то эти же биты (и только они) будут равны «1» у величины y `=` `(`x `xor` A`)`.

Второй операцией (y `and` M) у получившегося значения y «гасятся» (приравниваются нулю) все биты, кроме бит префикса.

То есть, если в результате вычисления (`(`x `xor` A`) and` M) получается ноль во всех разрядах, то значит IP-адрес x и A имеют *одинаковые префиксы* и значит x принадлежит подсети (A, M). Если хотя бы один бит в результате будет не нулевым, то значит IP-адрес x не принадлежит подсети (A, M).

Для алгоритма дихотомии необходимо уметь выполнять не только проверку вида «IP-адрес x принадлежит подсети (A, M)», но и

Пусть (A, M) — адрес и маска некоторой подсети, x — адрес для проверки на принадлежность подсети (A, M). Тогда, следующие вычисления позволяют выполнить следующие проверки:

Вычисление	**Реализуемая проверка**
`((`x `xor` A`) and` M`)==0`	x принадлежит подсети (A, M)
x `<` A	x меньше всех адресов из подсети (A, M)
x `>` `(`A `or (not` M`))`	x больше всех адресов из подсети (A, M)

Таблицы побитовых операций:

`xor`	0	1
0	0	1
1	1	0

`and`	0	1
0	0	0
1	0	1

`or`	0	1
0	0	1
1	1	1

`not`	
0	1
1	0

Рис. 10. Проверка принадлежности IP-адреса подсети

проверки «IP-адрес x меньше всех адресов подсети (A, M)», «IP-адрес x больше всех адресов подсети (A, M)». Для этого надо уметь вычислять первый (самый маленький) и последний (самый большой) IP-адрес в подсети (A, M).

Так как первый (самый маленький) IP-адрес в подсети (A, M) это A, то проверка условия «IP-адрес x меньше всех адресов подсети (A, M)» сводится к выполнению одной единственной команды процессора: выполнению сравнения x `<` A.

В принципе, умения выполнять две проверки («IP-адрес x принадлежит подсети (A, M)» и «IP-адрес x меньше всех адресов подсети (A, M)») достаточно, для реализации дихотомии — третье условие («IP-адрес x больше всех адресов подсети (A, M)») является отрицанием первых двух.

Однако, для полноты картины мы выпишем независмое вычисление условия «IP-адрес x больше всех адресов подсети (A, M)». Для этого заметим, что величина (`not` M) содержит «0» во всех разрядах префикса и «1» во всех разрядах суффикса. Значит, величина z `=` A `or (not` M`)` имеет правильный префикс подсети (A, M) и «1» во всех разрядах суффикса. То есть, z является самым большим IP-номером в подсети (A, M). Значит проверку условия «IP-адрес x больше всех

адресов подсети (A, M)» можно выполнить за счет вычисления выражения: x `>` `(`A `or (not` M`))`.

Выше приведен полный список вычислений, требуемый для реализации алгоритма дихотомии при решении задачи маршрутизации.

5.7. Умолчательный интерфейс. Необходимо отметить, что у маршрутизаторов таблицы маршрутизации редко бывают полными, то есть такими, что объединение всех подсетей, перечисленных в таблице покрывает весь диапазон всех возможных IP-номеров. То есть, в маршрутизаторах при решении задачи маршрутизации может возникнуть ситуация, что полученный адрес не принадлежит ни одной подсети из перечисленных в таблице маршрутизации.

Для такого случая в маршрутизаторе задается умолчательный (default) интерфейс, на который отправляются пакеты, адрес получателя которого не удалось разрешить в таблице маршрутизации. Умолчательный маршрут ведет к так называемому «умному маршрутизатору («smart host»), который обладает большей информацией о маршрутизации.

5.8. DNS-служба. Введение числовых IP-адресов позволило в TCP/IP-сетях эффективно решать задачи маршрутизации — ожидаемый результат, компьютерам (маршрутизаторам, в том числе) «удобно» обрабатывать числовые данны. Однако людям, многочисленным пользователям компьютерных сетей удобнее оперировать с символьными доменными именами: человеку значительно проще запомнить адрес `www.yandex.ru`, чем IP-номер этого сервера `213.180.204.11`.

В TCP/IP-сетях используется такое решение данной проблемы:

- Для передачи TCP/IP-пакетов используются только IP-адреса компьютеров, входящих в сеть.
- Пользователи при работе с сетевыми приложениями могут использовать текстовые доменные имена компьютеров.
- В сети реализована распределенная служба DNS — *Domain Name Service, служба доменных имен,* — позволяющая переводить числовые IP-адреса в текстовые доменные имена и обратно.

DNS — это иерархическая система, поддерживаемая серверами, которые обычно называются серверами имен (name servers). В их функции входит выборка соответствующей информации из распределённой базы данных и за счет этого реализация основного своего

назначения: перевод числовых IP-адресов в текстовые доменные имена и обратно.

Подробнее различные аспекты организации DNS-службы рассмотрены ниже.

5.8.1. *Доменные имена узлов сети.* Доменный принцип построения текстовых имен компьютеров в TCP/IP-сетях была заимствована из UUCP-сетей. Например, рассмотрим ипя компьютера `pier.botik.ru`. Здесь `ru` — домен первого уровня, `botik` — домен второго уровня (подддомен в домене `ru`), `pier` — имя хоста. При записи домены, поддомены и названия хоста разделяются точкой.

5.8.2. *Делегирование поддоменов и IP-сетей.* Кроме доменной структуры сети от UUCP протокол TCP/IP унаследовал систему *делегирования доменов*, то есть разделение ответственности за выдачу имен.

Так за домены верхнего (первого) уровня отвечает организация InterNIC (http://www.internic.net). Именно эта организация выдает (делегирует) другим организациям право управления тем или иным доменом первого уровня и заведения в нем поддоменов второго уровня.

Так, например, за домен `ru` отвечает организация РосНИИ РОС[11] — Российский НИИ развития общественных сетей,— и его представитель организация «RU-center»[12].

В свою очередь эти организации могут другим организациям делегировать поддомены второго уровня из домена `ru` — делегировать право распоряжаться поддоменом второго уровня из домена `ru` и ответсвенность за умелое управление им.

Так, поддомены `botik.ru` и `pereslavl.ru` второго уровня из домена `ru` делегированы организации Российский НИИ региональных проблем (РосНИИ РП), расположенной в Переславле-Залесском. В свою очередь, РосНИИ РП может делегировать поддомен третьего уровня какой-либо организации. Так поддомен `u.pereslavl.ru` был делегирован Университету города Переславля им. А. К. Айламазяна.

Такой же механизм иерархического делегирования используется для распределения подсетей IP-адресов. Организации-участники сети Internet могут обратиться к вышестоящим (по сетевой иерархии) организациям с просьбой делегировать им подсеть IP-адресов того или иного размера. Если данная просьба хорошо обоснована и если будет найдена соответствующая техническая возможность, то

---

[11] См. `http://www.ripn.net`.

[12] См. `http://www.nic.ru`.

просителю может быть выделена и делегирована некоторая подсеть IP-адресов.

Получив права распоряжения некоторой IP-подсетью, организация может ее разбить на более мелкие подсети (с более длинным префиксом) и делегировать эти подсети участникам своей локальной TCP/IP-сети. И т.д.

Механизм делегирования обеспечивает следующее важное свойство сети Internet: получив полномочия на домены и IP-подсети участники сети Internet получают возможность автономно и бес дальнейших согласований развивать свои локальные участки сети Internet, конечно, в границах своих полномочий.

Именно механизм делегирования поддоменов и IP-подсетей:

- обеспечивает возможность развития сети независимо и одновременно в разных уголках земного шара;
- убирает необходимость наличия единого управляющего и согласующего центра в Сети, который мог бы быть «тормозом» на пути развития Сети;
- обеспечивает стремительное (экспоненциальное) развитие сети Internet.

5.8.3. *Обязательное DNS-обслуживание делегированных подсетей и доменов.* Организация, ответственная за тот или другой домен (или IP-подсеть) получает не только права, но и обязанности. В частности, она обязана поддерживать работоспособные name-серверы, на которых должна быть запущена служба DNS, обслуживающая этот домен (IP-подсеть).

Для надежости, обычно организуется несколько таких name-серверов, причем в разных местах Сети, как правило не меньше двух. Один из этих DNS-серверов называют основным, а остальные — вторичными. Если основной сервер выйдет из строя или станет недоступным, вторичные name-серверы зеркалируют (миррируют, создают зеркальную копию) содержимое основного сервера, копируя к себе с него информацию с некоторой периодичностью.

Наличие нескольких работоспособных name-серверов является непреложным условием, которое проверяется при рассмотрении заявок организаций о передаче (делегировании) им прав на поддомены и/или IP-подсети.

5.8.4. *Система DNS.* Иерархическая структура DNS-серверов напоминает дерево, вершина которого является Сетевой информационный центр сети Internet (*InterNIC — Internet Network Information*

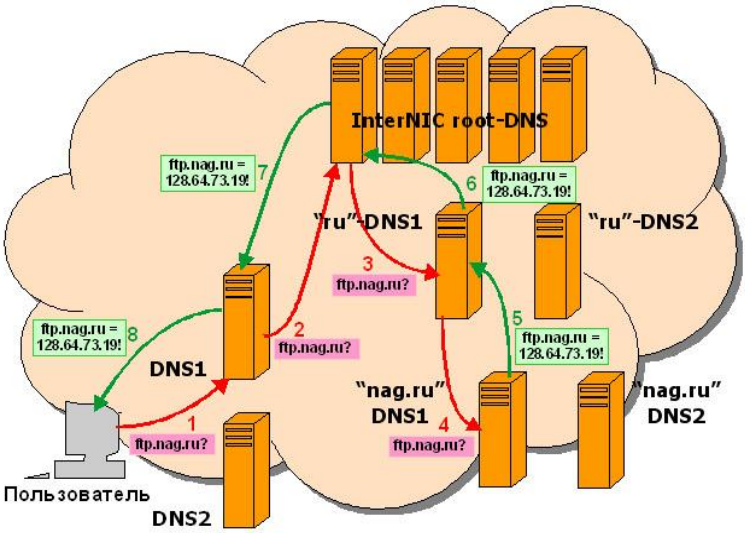

Рис. 11. Прохождение DNS-запроса

Center[13]), состоящий из нескольких развнозначных и равноправных *корневых DNS-серверов*. Дублирование корневых серверов сделано из соображений обеспечения надежности работы системы и для распределения нагрузки — по мере роста нагрузки может приниматься решение об увеличении числа корневых DNS-серверов.

Корневые DNS-серверы InterNIC поддерживают логические связи с несколько ближайшими узлами (DNS-серверами) в иерархическом дереве DNS, каждый из которых обслуживает соответсвующий домен верхнего (первого) уровня.

С доменами первого уровня, в свою очередь, может иметь связано несколько поддоменов второго уровня. И, соответсвенно, DNS-серверы, ответсвенные за обслуживание доменов первого уровня логически связаны с DNS-серверами, ответсвенными за обслуживание доменов второго уровня.

Рассмотрим механизм работы пользователя в сети. Прежде чем выполнить любой запрос пользователя по соединению с удаленным

[13]См. `http://www.internic.net/`.

хостом, заданным по имени (например, ftp.nag.ru), приложение преобразует имя в IP-адрес, сделав запрос к местному DNS-серверу[14], его адрес должен быть указан в настройках компьютера пользователя. В случае, если локальный DNS-сервер не находит соответствующей записи в локальной таблице, позволяющей преобразовать имя в IP-номер, то он посылает запрос («преобразовать указанное имя») к корневомуDNS-серверу сети Интернет (InterNIC root DNS), а от него запрос спускается к DNS-серверу, отвечающим за домены более низкого уровня, например «ru». Тот, в свою очередь, пытается выполнить преобразование при помощи своей локальной таблицы и, если не это не получается, то проверяет, кому принадлежит домен более низкого уровня (в данном примере nag.ru) и запрос направляется на сервер, отвечающий за этот домен. После разрешения преобразования имени, результат отсылается спрашивающему компьютеру, по пути, по которому пришел запрос. Кроме того, задействуе-ся механизм сохранения наиболее часто использованной информации в каждом DNS-сервере — *кэш*, — участвующем в обработке запроса: полученное соответствие «имя — IP-адрес» сохраняется и при повторном таком же запросе ответ возвращается из локального кэша и не происходит перенаправление запроса на другие DNS-сервера.

5.9. Распределение IP-номеров. Всего в текущей реализации протокола TCP/IP имеется 2^{32} или 4'294'967'296 номеров, которые (за вычетом особых интервалов) распределяются между всеми абонентами сети. В настоящее время количества IP-номеров катастрофически не хватает, поэтому разрабатывается проект увеличения длины IP-номера до 128 бит. Выделение IP-номеров происходит путем распределения адресов класса «A» между организациями, ответственными подсети уровня государств, те в свою очередь делегируют более мелкие подсети региональным представителям и так далее. На нижнем уровне происходит распределение IP-адресов конкретным хостам и занесение этих данных в локальную таблицу маршрутизации и в соответствующие DNS-серверы.

Поиск конкретного хоста по IP-номеру происходит аналогично тому, как работает доменный механизм поиска, то есть происходит запрос у локального маршрутизатора, тот ищет в своей локальной таблице маршрутизации и в кэше. Если не находит, то обращается к маршрутизатору, которому делегирована подсеть более высокого

[14]DNS1.

уровня, в которую входит данных IP-адрес. Он в свою очередь, если не находит в локальной таблице переправляет запрос серверу, ответственному за подсеть требуемого номера и т. д. Получить информацию об организации, которой делегирована подсеть можно при помощи сервиса Whois[15], который сообщает полную информацию об организации, отвечающую за указанную подсеть.

5.10. Заполнение таблиц маршрутизации. Далее мы рассмотрим реализованные в TCP/IP сетях решения двух проблем: как заполнять таблицы маршрутизации и как поддержать возможность именования компьютеров в сети не только IP-номерами (цифровые номера человеку запомнить существенно сложнее), но и легко запоминаемыми текстовыми (доменными) именами.

Обратимся к вопросу о заполнении таблиц маршрутизации. Легко понять, что полностью ручное построение таблиц неизбежно привело бы к возникновению массы ошибок и было бы серьезным бременем для программистов. Поэтому были разработаны автоматические и автоматизированные системы построения таблиц маршрутизации. Алгоритмы делятся на два основных класса: статические и динамические. Особенностью статической маршрутизации является то, таблицы не перестраиваются в режиме реального времени, динамические же способны перестраиваться в зависимости от ситуации в сети.

5.11. Статическая маршрутизация. В случае статической (фиксированной) маршрутизации администратор сети сам решает, на какие интерфейсы надо передавать пакеты с теми или иными адресами, и заносит соответствующие записи в таблицу маршрутизации вручную (например, с помощью утилиты route ОС UNIX или Windows). Таблица, как правило, создается в процессе загрузки и редактируется по мере необходимости. Такие исправления могут понадобиться, в частности, если в сети отказывает какой-либо сетевой узел, и его функции передаются другому. Таблицы делят на *одномаршрутные*, в которых для каждого адресата задан один путь, и *многомаршрутные*, когда предлагается несколько альтернативных путей. В случае многомаршрутных таблиц должно быть задано правило выбора одного из маршрутов. Чаще всего один путь является основным, а остальные резервными. Очевидно, что алгоритм фиксированной маршрутизации с его способом формирования таблиц маршрутизации вручную приемлем только в небольших сетях с простой топологией. Однако он

[15]Смотри, например, http://194.226.65.158:8080/nic/whois/

может быть эффективно использован и на магистралях крупных сетей с простой структурой и очевидными наилучшими путями следования пакетов в подсети. Явным недостатком такого типа построения таблиц маршрутизации является низкая отказоустойчивость сети: в случае выхода из строя некоторого узла, как правило, требуется вмешательство администратора для перенаправления путей следования пакетов.

5.12. Динамическая маршрутизация. Наибольшее распространение получили алгоритмы динамической (адаптивной) маршрутизации. Они обеспечивают автоматическое обновление таблиц маршрутизации после изменения конфигурации сети. Используя протоколы адаптивных алгоритмов, маршрутизаторы могут собирать информацию о топологии связей в сети и оперативно реагировать на все изменения конфигурации связей. В таблицы маршрутизации обычно заносится информация об интервале времени, в течение которого данный маршрут будет оставаться действительным. Это время называют временем жизни маршрута (Time To Live, TTL).

Адаптивные алгоритмы имеют распределенный характер, то есть в сети нет специально выделенных маршрутизаторов для сбора и обобщения всей топологической информации: эта работа распределена между всеми маршрутизаторами.

Адаптивные алгоритмы маршрутизации должны отвечать некоторым важным требованиям. Прежде всего, они обязаны обеспечивать выбор если не оптимального, то хотя бы рационального маршрута. Второе условие — простота алгоритмов, чтобы соответствующие реализации не потребляли значительных вычислительных и сетевых ресурсов: они не должны порождать слишком большой объем вычислений или интенсивный служебный трафик. И, наконец, алгоритмы маршрутизации должны обладать свойством сходимости, то есть всегда приводить к однозначному результату за приемлемое время.

Алгоритмы динамической маршрутизации основаны на специальных протоколах обмена информацией о маршрутах. Современные протоколы обмена информацией о маршрутах, в свою очередь, делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:

- дистанционно-векторные алгоритмы (Distance Vector Algorithm, DVA);
- алгоритмы состояния каналов (Link State Algorithm, LSA).

В алгоритмах дистанционно-векторного типа каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния от данного маршрутизатора до всех известных ему сетей. Под расстоянием обычно понимается число транзитных узлов. Метрика может быть и иной, учитывающей не только число промежуточных маршрутизаторов, но и время прохождения пакетов между соседними маршрутизаторами, пропускную способность или надежность путей.

Получив вектор от соседа, маршрутизатор увеличивает расстояние до указанных в нем сетей на длину пути от себя до данного соседа и добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно (если они подключены к его портам) или из аналогичных объявлений других маршрутизаторов, а затем рассылает новое значение вектора по сети.

Получая новые значения векторов с расстояниями каждый маршрутизатор будет «обновлять» свои знания о мире: если он узнал новый, более короткий маршрут к некоторой сети, то изменит соответствующую позицию в векторе; если новый маршрут не короче известного — обновления вектора не будет (как и рассылки — нет новой информации, которую можно разослать).

В конце концов, каждый маршрутизатор узнает информацию обо всех имеющихся в объединенной сети сетях и о расстоянии до них через соседние маршрутизаторы. Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях. В крупных сетях они загружают линии связи интенсивным широковещательным трафиком. Изменения конфигурации отрабатываются по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только обобщенной информацией — вектором расстояний, — к тому же полученной через посредников. Алгоритм обладает медленной сходимостью (slow convergence) то есть ему свойственно медленное перестроение таблиц маршрутизации на роутерах при изменении топологии сети. Примером такого типа протоколов является RIP (Routing Information Protocol).

В отличие от RIP, протоколы, основанные на алгоритмах состояния каналов не «рассказывает соседям о мире», наоборот «миру рассказывает о соседях», пересылая не всю таблицу маршрутизации, а лишь маленькие сообщения о состоянии близлежащих каналов (Link State Advertisement). Все маршрутизаторы работают на основании

одинаковых графов, в результате процесс маршрутизации оказывается более устойчивым к изменениям конфигурации. «Широковещательная» рассылка (то есть передача пакета всем ближайшим соседям маршрутизатора) производится здесь только при изменениях состояния связей, что в надежных сетях происходит не так часто. Также в сообщениях о состоянии каналов указывается время доставки пакета по тому иди иному пути, поэтому при построении таблицы маршрутизации выбирается наискорейшее направления, что обеспечивает оптимальную по времени работу сети.

Примерами протоколов на базе алгоритма состояния связей могут служить IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP и протокол NLSP стека Novell.

Примерами протоколов на базе алгоритма состояния связей могут служить IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP и протокол NLSP стека Novell.

6. Архитектура сети Ethernet

Ethernet — это сетевой стандарт, основанный на технологиях сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году. В 1980 году фирмы DEC, Intel, Xerox совместно разработали стандарт Ethernet II для сети, построенной на основе коаксиального кабеля. Поэтому стандарт Ethernet иногда называют стандартом DIX по заглавным буквам названий фирм. На основе стандарта Ethernet DIX был разработан стандарт IEEE 802.3. В зависимости от типа физической среды, используемой для передачи данных, стандарт IEEE 802.3 имеет различные модификации –10Base-5, 10Base-2, 10Base-T.

6.1. Принцип функционирования Ethernet. Хорошей аналогией взаимодействиям в среде Ethernet может служить разговор группы вежливых людей в небольшой темной комнате. При этом аналогией электрическим сигналам в кабеле служат звуковые волны в комнате. Каждый человек слышит речь других людей и пока кто-то говорит, все остальные в комнате молчат, ждут, когда закончит говорящий. Все люди в комнате имеют одинаковые возможности вести разговор (множественный доступ), но никто не говорит слишком долго, так как все вежливы и избегают монополизации на длительное

время права говорить. Если человек будет невежлив, то его попросят выйти (удалят из сети).

Если два человека начинают говорить одновременно, то они сразу обнаруживают это, поскольку слышат друг друга (обнаружение одновременной передачи, коллизии — *Collision domain*). В этом случае оба замолкают и ждут некоторое время, после чего один из них вновь начинает разговор. Длительность паузы каждый для себя определяет независимо, при помощи собственного датчика случайных чисел. Это делает маловероятной повторную коллизию.

Каждый человек имеет собственное уникальное имя (аналог уникального Ethernet-адреса). Каждый раз, когда кто-нибудь начинает говорить, он называет по имени того, к кому обращается, и свое имя, например: «Слушай Петя, это Андрей». Если кто-то хочет обратиться ко всем, то он говорит: «Слушайте все, это Андрей», (широковещательная передача).

Возвращаясь к передаче данных между компьютерами, имеем следующую модель взаимодействия: одна из станций посылает пакеты (кадры), которые распространяются по всей сети и воспринимаются всеми компьютерами (в том числе и ею самой). Такой режим совместного использования единой среды передачи информации называется *Shared Ethernet* или *режимом с разделением канал*а. Из-за того, что передаваемая информация получается всеми, требуется для каждого сообщения указывать адрес получателя и отправителя. В Ethernet таковым является *MAC-адрес*, принадлежащий непосредственно аппаратуре сетевого адаптера (сетевой карте) и присваивается в момент изготовления. Размер адреса в Ethernet — 6 байт. При записи 6-байтного Ethernet-адреса каждый байт указывается в 16-ричной системе и отделяется двоеточием. Чтобы избежать возможности монополизации общего канала, Ethernet разбивает данные на пакеты длиной от 64 до 1518 байтов.

Основная проблема Shared Ethernet состоит в том, что нет общего механизма распределения времени передачи, поэтому пара участников сети может одновременно начать передачу. Такая ситуация называется *коллизия*. При ее возникновении происходит наложение сигналов и искажение информации, поэтому, как только коллизия обнаруживается, передача всеми устройствами прекращается, затем передатчики выдерживают паузу случайной длительности (*случайная задержка*), затем, если никем не ведется передача, вновь перепосылают пакет. Для того чтобы можно было несколько раз высылать пакет

в случае коллизии, адаптер имеет буфер, в который может быть помещен один пакет. Различают два вида коллизии: *ранняя* и *поздняя*. *Ранней* называется коллизия, обнаруживаемая передающим устройством в самом начале передачи, еще до отправки данных. В этом случае передача прекращается и через случайный отрезок времени попытка передачи возобновляется. В случае *поздней* коллизии отправитель обнаруживает наложение сигналов уже после того, как данные отправлены и буфер очищен. Здесь пакет является потерянным и вопрос о его восстановлении выходит за рамки сетевого протокола и решается программным обеспечением.

Широковещательная передача или *broadcast* (*multicast*) — это передача сообщения всем абонентам сегмента сети. Для передачи такого сообщения в адресе получателя указывается адрес

FF:FF:FF:FF:FF:FF

(все 16-ричные цифры адреса имеют значения «F»). Пакеты с таким адресом воспринимаются всеми абонентами. Этот вид передачи широко используется для технических целей, когда абоненты обмениваются между собой короткими сообщениями, извещая тем самым о своем присутствии в сети и о своем состоянии.

6.2. Стандарты 10Base-2, 10Base-5. Первым стандартом Ethernet-сетей был 10Base-2 (Ethernet 10 Mbit, передаваемый по двухжильному коаксиальному кабелю). В качестве среды передачи здесь используется *коаксиальный кабель*, представляющий собой центральную медную жилу диаметром 0.89 м, окруженную полиэтиленовым изолятором и внешней оплеткой диаметром около 5 мм из медного провода. Максимальная длина сегмента без хабов[16] составляет 185 м. Максимальное количество станций, подключаемых к одному сегменту — 30. Используемый в 10Base-2 кабель еще называют «*тонкий коаксиал*».

Стандарт 10Base-5 обладает более высокими характеристиками: поддерживается до 100 узлов в сегменте и его длина ограничена 500 метрами. Иначе данный тип кабеля называют «*толстый коаксиал*». Он относительно жесткий, с диаметром около 1 см, существенно дороже «тонкого» коаксиала и более сложен в установке.

---

[16]Хаб [от англ. hub — центр, концентратор] — сетевой аппаратный узел, к которому подключаются все компьютеры в сети топологии «звезда»; активные концентраторы могут восстанавливать и ретранслировать сигналы; пассивные концентраторы просто выполняют коммутацию.

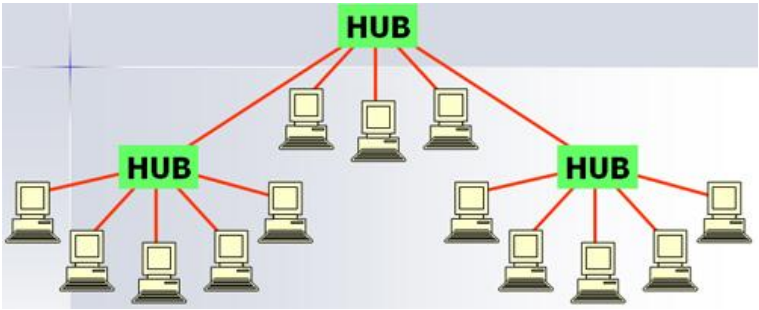

Рис. 12. Сеть топологии «звезда»

При помощи *Ethernet-адаптера* (сетевой карты с приемником/передатчиком Ethernet-пакетов, буфером, устройство имеет собственный MAC-адрес) к кабелю подключаются компьютеры. Соединения адаптеров производятся последовательно при помощи Т-образных сочленений (*T-connector*), на концах линии устанавливаются специальные заглушки — терминаторы, служащие для подавления сигнала и недопущения его экранирования. Такая архитектура последовательных соединений называется *«шина»*.

Общим недостатком стандартов 10Base-5 и 10Base-2 является низкая надежность: повреждение кабеля в одном месте канала выводит из строя весть Ethernet-сегмент. Поэтому данная архитектура весьма сложна в эксплуатации.

7. Коаксиальный кабель

Данный вид кабеля используется в прокладке сетей Ethernet стандарта 10Base-2. Кабель имеет два проводника и представляет собой центральную медную жилу, полиэтиленовый изолятор и проволочную оплетку, упакованные в пластиковую оболочку.

Соединение сегментов кабеля между собой и со станцией происходит при помощи специальных разъемов: BNC и Т-образного разъема.

Рис. 16 иллюстрирует схему подключения рабочего места пользователя в локальной сети 10Base-2 с коаксиальным кабелем. Здесь прямоугольниками на концах кабеля обозначены терминаторы (согласующие сопротивления) — устройства, необходимые для гашения сигналов и недопущения их отражения обратно в канал. Важным

Рис. 13. Коаксиальный кабель, подготовленный для соединения с разъемом

Рис. 14. BNC-разъем

требованием прокладки коаксиального сегмента сети является заземление одного (и только одного) из концов сегмента.

В настоящее время сети на коаксиальном кабеле уходят в прошлое, несмотря на свою дешевизну, относительно других кабельных систем, обусловленную низкой стоимостью самого изделия (RG-58,

Рис. 15. Т-разъем

$ 0.35/метр) и отсутствия необходимости приобретения активного сетевого оборудования (типа хаба). Это объясняется, прежде всего, низкой надежностью линейных сетей с топологией «шина», а также недостаточной скоростью передачи данных (это всего 10 Mbit/c). Сети на основе коаксиала постепенно вытесняются более надежными и перспективными сетями на основе кабеля витой пары.

7.1. Стандарт 10Base-T. Стандарт принят в 1991 году как дополнение к существующему набору стандартов Ethernet и имеет обозначение 802.3i. Использует в качестве среды двойную *неэкранированную витую пару* (Unshielded Twisted Pair, UTP — откуда и буква «T» — twisted в названии стандарта) с разъемами RJ-45. Вилки RJ-45 вставляются непосредственно в разъем сетевого адаптера на каждом компьютере. Сеть собирается по топологии «*звезда*», здесь второй конец каждого кабеля вставляется в разъем специального устройства, называемого *концентратором* или *хабом*. Хаб является общей

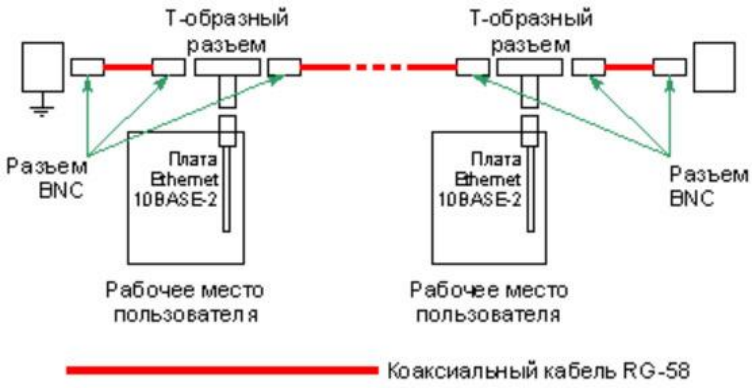

Рис. 16. Схема подключения рабочего места пользователя в локальной сети 10Base-2 с коаксиальным кабелем

точкой соединения узлов сети (центр звезды). Обычно хаб функционирует как повторитель. Хаб обнаруживает коллизию в сегменте в случае одновременной передачи сигналов по нескольким своим входам и посылает jam-последовательность на все свои выходы.

Стандарт определяет битовую скорость передачи данных 10 Мб/с и максимальное расстояние отрезка витой пары между двумя непосредственно связанными узлами (станциями и хабами) не более 100 м.

Сети, построенные на основе стандарта 10Base-T, обладают по сравнению с коаксиальными вариантами Ethernet'а (10Base-2) многими преимуществами. Эти преимущества связаны с разделением общего физического кабеля на отдельные кабельные отрезки, подключенные к центральному коммуникационному устройству. И хотя логически эти отрезки по-прежнему образуют общий домен коллизий, их физическое разделение позволяет индивидуально контролировать их состояние и индивидуально отключать в случае неисправности на каком-либо кабельном отрезке: обрыв, короткое замыкание или неисправность сетевого адаптера. Это обстоятельство существенно облегчает эксплуатацию больших сетей Ethernet.

8. Кабель витой пары

Особенность кабеля витой пары в том, что за счет перевитых между собой точно с определенным шагом пар проводов кабель начинает обладать волновыми свойствами (кроме функции проведения электрического тока). Этот факт позволяет ему стать средой для передачи высокочастотного сигнала. Кроме того, наличие навивки делает передаваемый сигнал достаточно устойчивым к внешнему электромагнитному излучению. Дело в том, что сигнал одновременно передается по обоим перевитым между собой проводам и в случае возникновения наводки с большой долей вероятности в обоих проводах произойдет примерно одинаковое[17] изменение потенциала. А в принимающем устройстве оценивается разность потенциалов между проводами, поэтому результат помехи будет для приемника практически незаметен.

Стандартом определена следующая конфигурация кабеля витой пары 5 категории (использующейся для построения сетей передачи данных): 4 пары перевитых между собой проводов (обвитых еще и между собой с определенным шагом), помещенных в пластиковую оболочку. Для каждого из 8-ми проводов стандартом закреплен свой цвет, причем один провод из витой пары окрашен сплошным цветом, а второй — пунктирным. Цвета проводников следующие: оранжевый, белый с оранжевым, голубой, белый с голубым, зеленый, белый с зеленым, коричневый, белый с коричневым. Такой тип кабеля называется UTP (*Unshielded Twisted Pair*) — неэкранированная витая пара. Для уменьшения воздействия внешних электромагнитных воздействий выпускаются защищенные варианты кабеля витой пары. FTP (*Foiled Twisted Pair*) — фольгированная витая пара, изделие, в основе имеющее UTP, но дополнительно перевитый провод обернут алюминиевой фольгой, экранирующей внешние волновые помехи. Более надежен и удобен в использовании вариант STP (*Shielded Twisted Pair*) — экранированная витая пара, кабель, имеющий вместо фольги оплетку из проводов, что повышает его надежность (фольга более подвержена повреждениям при сгибе) и облегчает обработку

[17] Из соображений симметрии, «равноправности» каждого провода в перевитой паре проводов.

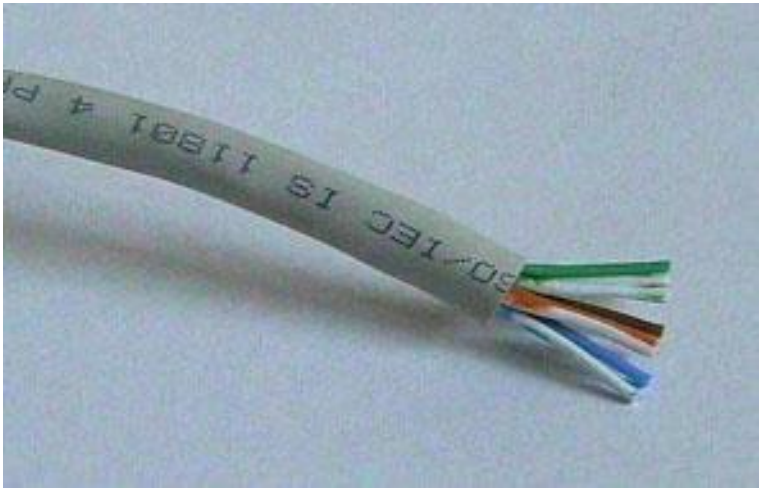

Рис. 17. Кабель из 4-х неэкранированных витых пар

(проволока легче паяется, чем фольга). В случае, если кабель предстоит прокладывать в сильно зашумленном электромагнитными помехами помещении, применяют вариант SFTP — дважды экранированный кабель, представляющий комбинацию двух экранов в виде фольги и оплетки.

Для передачи данных используются только две витые пары из четырех, поэтому существуют варианты кабелей, в которых присутствуют только две витые пары, что удешевляет изделие. Кабель витой пары соединяется с различными устройствами (сетевой адаптер, хаб) с использованием разъема стандарта RJ-45.

Как уже отмечалось ранее, витопарный кабель используется для построения сетей стандарта Ethernet 10BASE-T, а также FastEthernet 100BASE-T — стандарта, допускающего передачу данных со скоростью 100 Mbit/c. Данные типы сетей строятся на основе хабов и топологии типа «звезда». Для удобства эксплуатации провод от хаба к рабочему месту не делают единым, а делят на две части: магистраль и патчкорд. Магистральная линия соединяется с хабом и крепится вдоль помещения, на конце имеет розетку для подключения пользовательского окончания — патчкорда. Такое устройство сетевых

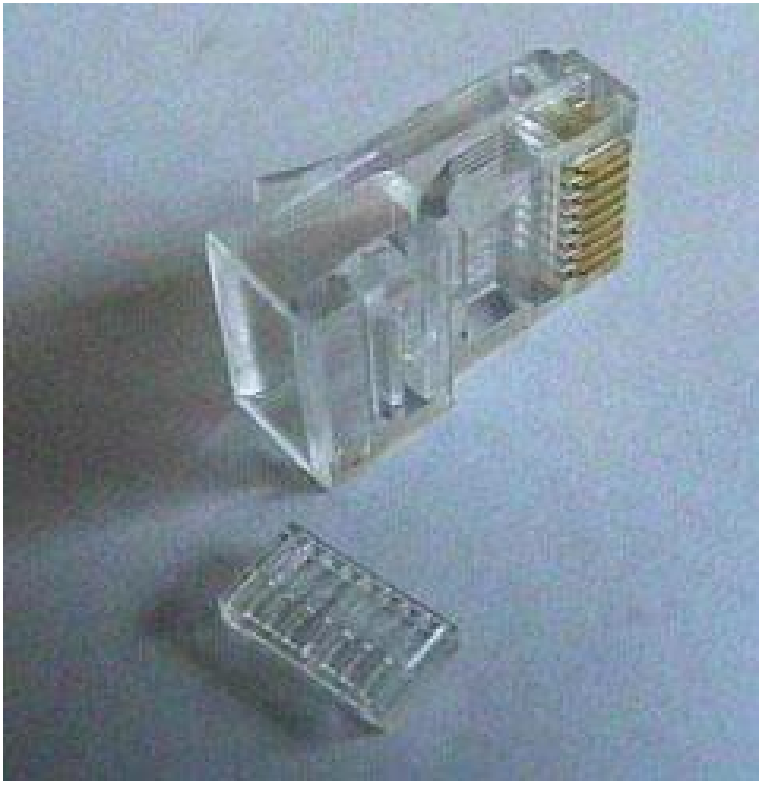

Рис. 18. Разъем RJ-45 для витой пары со вставкой

подключений позволяет сделать рабочее место более мобильным, не нарушая проложенной конфигурации сети.

Указанные особенности построения сети нашли свое отражение и в оборудовании: для магистральных кабелей витой пары используются провода, представляющие собой единую медную жилу, по которой лучше распространяется сигнал, но эти провода более чувствительны к деформациям. Для патчкордов используют провода, состоящие из

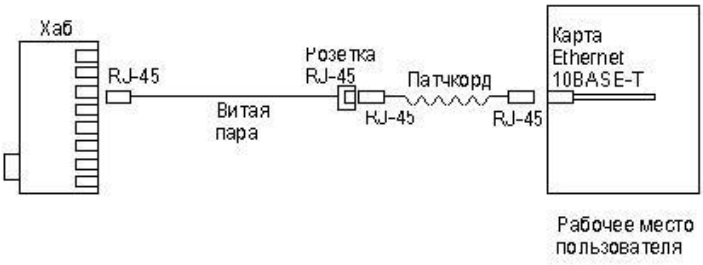

Рис. 19. Подключение рабочего места пользователя в локальной сети 10Base-T витой парой

множества более тонких жил, которые легче приспособлены к изгибам, присущим пользовательским окончаниям. Для соединения витопарных кабелей обоих типов есть соответствующие RJ-45 разъемы, учитывающие указанные особенности.

9. Стандарт 100Base-T(Fast Ethernet)

9.1. Радио-Ethernet.

10. Расширение Ethernet-сети

Возникает вопрос: можно ли «растить» Ethernet, т. е. увеличивать длину сегмента кабеля и количество машин больше, чем позволяют описанные стандарты? Да, есть оборудование, которое позволяет расширить возможности Ethernet, не нарушая ее основных принципов.

11. HUB (Хаб или концентратор)

Хаб (*повторитель, концентратор, репитер*) уже упомянут в описании сети стандарта 10Base-T, он соединяет отрезки кабеля, усиливает сигнал и ретранслирует его в дополнительные сегменты. Хабы передают из сегмента в сегмент каждый бит данных, даже если данные состоят из искаженных пакетов или пакетов, не предназначенных для этого сегмента. В результате, проблемы одного сегмента могут

Рис. 20. Хаб (концентратор)

повредить всем остальным сегментам. Хабы не могут служить фильтром, который бы ограничивал поток некорректных пакетов. Кроме того, хабы передают из сегмента в сегмент и лавину широковещательных пакетов, распространяя их по всей сети. Когда количество широковещательных пакетов приблизится к ширине полосы пропускания сети, ее производительность резко снижается. Производительность сети также падает, когда устройство отвечает на пакеты, непрерывно циркулирующие по сети, или пакеты постоянно пытаются достичь устройства, которое никогда не отзывается. Итак, повторитель способен лишь на ретрансляцию и усиление сигнала и борется только с его затуханием, не решая проблему коллизий.

Хабы бывают нескольких стандартных конфигураций, различающихся по типу и количеству портов, а также поддерживаемому стандарту (10/100 Mbit Ethernet). При этом, в виду своей простоты Hub не способен иметь несколько интерфейсов, к которым были бы подключены Ethernet-сегменты, работа в которых ведется на разных скоростях (10/100 Mbit). Отчасти решают эти проблемы устройства, называемые Switching hub, некоторая информация о которых будет дана ниже.

12. Правило 4-х хабов

Стандарты физического уровня Ethernet допускают использование до 4-х хабов, соединяющих до 5 сегментов, каждый длиной до 100 метров, если используемые хабы удовлетворяют ограничениям на допустимые величины задержек сигналов. При этом максимальная длина сети (расстояние между любыми двумя абонентами сети) не будет превышать 500 м, и такая конфигурация гарантирует правильное обнаружение коллизии крайними станциями сети.

Правила 4-х хабов и максимальной длины каждого из сегментов легко использовать на практике для определения корректности конфигурации сети. Однако эти правила применимы только тогда, когда все соединяемые сегменты представляют собой одну физическую среду. Но для смешанных случаев, когда в одной сети Ethernet присутствуют сегменты различных физических стандартов, правила, основанные только на количестве хабов и максимально длинных сегментов, становятся более запутанными.

Наличие данного правила, как и ограничений на длину сегментов, объясняется конечностью скорости распространения сигнала в среде. При большей длине кабеля крайние компьютеры могут не успевать распознать коллизию на ранней стадии, и пакеты будут теряться.

Данное правило не позволяет избежать другой проблемы, которая проявляется при построении сложной конфигурации Ethernet-сегмента с большим количеством подключенных абонентов — это рост вероятности коллизий при росте количества пользователей. Решать данную проблему призваны устройства, рассматриваемые далее.

13. Switch (или Bridge)

Следующее устройство для расширения Ethernet — *Bridge* (мост) или современное его название *Switch* (коммутатор). Как и повторитель, Switch может соединять сегменты или локальные сети. Однако, в отличие от Hub, Switch позволяет разбить сеть на несколько сегментов, изолировав за счет этого часть трафика. Например, если трафик компьютеров какого-то отдела «наводняет» сеть пакетами, уменьшая ее производительность в целом, то с помощью Switch можно выделить эти компьютеры в отдельный сегмент и изолировать его от сети. Устройства типа Switch решают следующие задачи:

- увеличивают размер сети;

- увеличивают максимальное количество компьютеров в сети;
- устраняют узкие места, появляющиеся в результате подключения избыточного числа компьютеров, и как следствие, возрастания трафика; Switch'и разбивают перегруженную сеть на отдельные сегменты с уменьшенным трафиком. В итоге каждая подсеть будет работать эффективно.
- соединяют разнородные физические носители, такие как витая пара и коаксиальный кабель;
- соединяют разнородные сегменты сети и переносят между ними пакеты.

Работа коммутатора основана на принципе, согласно которому каждый узел сети имеет уникальный адрес, Switch передает пакеты, исходя из адреса узла назначения. Можно сказать, что Switch'и обладают некоторым «интеллектом», поскольку изучают, куда следует направить данные. Когда пакеты передаются через Switch, данные об адресах компьютеров сохраняются в его оперативной памяти, на их основе выполняется построение таблицы маршрутизации. В начале работы таблица маршрутизации Switch'а пуста. При появлении пакета от компьютера с определенным MAC-адресом X на некотором порту I, в таблицу маршрутизации вносится информация, что компьютер с адресом X находится на порту I. При появлении следующего пакета, прежде чем разослать его по всем портам (как это делает Hub), у Switch'а происходит проверка, нет ли адреса получателя в таблице маршрутизации. Если есть, то пакет посылается только на соответствующий порт, не засоряя остальные каналы, если же нет, то устройство поступает как обычный Hub, то есть рассылает пакет во все порты, кроме того, через который он был доставлен.

В силу того, что Switch не распространяет пакеты напрямую, а сохраняет их в буфере, и лишь потом перенаправляет по нужному адресу, возможно одновременное подключение к Switch сегментов Ethernet, в которых сигнал передается с разной скоростью (т. е. могут быть несколько портов, работающих на скорости 10 Mbit/c и несколько на 100Mbit/c). В силу различных пропускных способностей каналов, Switch может иметь механизм очередей на портах, длина которых зависит от сложности (а соответственно и стоимости) Switch. В самых простых вариантах очередь может состоять всего из одной ячейки. При превышении объема очереди вновь пришедшим пакетам отказывается в обслуживании (они выбрасываются).

Сеть, построенная не на Hub, а на Switch, называется switched Ethernet. В такой конфигурации правило четырех хабов может нарушаться.

Из приведенного краткого описания Switch видно, что его устройство существенно сложнее, чем у Hub, соответственно его стоимость выше. В качестве некоторого «среднего» решения используется т. н. «свичующий хаб» (Switching hub). Данное устройство является гибридом Switch и Hub. Возможны два варианта таких устройств:

- вариант, при котором в одном корпусе помещаются два Hub, между которыми установлен Switch. Такая конфигурация позволяет разделить сеть на два сегмента, а в дополнение каждый Hub может работать на разных скоростях, а Switch конвертировать пакеты между ними;
- второй вариант представляет собой упрощенный Switch, для которого канал взаимодействия между портами может быть только один, поэтому в каждый момент времени передача осуществляется только между двумя направлениями, а остальные ожидают очереди.

14. Router (маршрутизатор)

В Ethernet-сетях роутеры (Router) выполняют ту же функцию, что и в сетях стандарта TCP/IP. Получая пакет с MAC-адресом получателя, роутер преобразует адрес по локальной таблице соответствия в его IP-адрес и, согласно своей таблице маршрутизации, отсылает пакет в подсеть, которой данный адрес принадлежит. При получении же пакета извне происходит обратное преобразование IP-адреса в MAC-адрес и посылка пакета в разделяемый сегмент Ethernet. Таким образом, использование роутеров позволяет связать друг с другом сегменты Ethernet, не нарушая принципов функционирования Ethernet-сети.

15. Правило построения смешанной сети

Если в проектируемой Ethernet-сети планируется использовать Hub, Switch и Router, то алгоритм расчета ее работоспособности следующий:

(1) нарисовать граф сети, пометив на нем перечисленное сетевое оборудование;

(2) удалить все вершины, в которых помещен Switch вместе со смежными ребрами, граф распадется на компоненты связности;
(3) удалить все вершины, помеченные роутерами, а на концах, подходивших к этим вершинам ребер, поместить абонентов;
(4) в полученном многосвязном графе останутся одни хабы, и для каждой их компонент связности должно выполняться правило четырех хабов.

Дополнительно накладывается ограничение: в Ethernet-сетях не должно быть циклов, в которых используются только Switch и Hub. В случае возникновения такого цикла возникает циклическое распространение пакетов и появление конфликтов MAC-адресов. Для предотвращения этого в каждом цикле должен находиться роутер.

16. Оценка качества услуг

В процессе развития сетей появилось понятие качества услуг — *QoS* (*Quality of Service*), т. е. ставится вопрос об устойчивости значений таких базовых параметров сети как пропускная способность и задержка. Возникает также понятие гарантированного QoS, где гарантируется, что пропускная способность будет не менее, а задержка — не более некоторой величины. Достигается это путем расставления приоритетов в обслуживании очередей для привилегированных пакетов.

Для реализации возможности гарантированного качества услуг сети существует специальный протокол ATM. В нем специфицируется сеть, построенная на ATM-switch. Для исключения возможности монополизации канала используются пакеты размером всего в 53 байта, что дает возможность гарантировать, сколько времени один пакет занимает канал. Сам протокол ориентирован на «соединение», то есть каждый абонент, прежде чем начать передачу данных, резервирует канал связи до получателя с указанием требуемых характеристик. Передача начинается только после того, как гарантированный канал построен. Такие технологии требуются, прежде всего, для гарантированной передачи потокового аудио и видео сигнала, для которых слишком большая задержка или потеря пакета оборачиваются искажением передачи и перепосылка данных бесполезна, так как потребление информации идет в реальном времени.

17. Построение региональных сетей

В теме построения региональной сети одним из ключевых моментов будет ее *малобюджетность* или *самоокупаемость*, поэтому достаточное внимание будет уделяться финансовой составляющей этой задачи. Другие аспекты, которые также будут изучаться - это организационная составляющая, а также техническая и технологическая база. Все рассматриваемые вопросы будут привязаны к российской действительности, а примеры браться из опыта построения малобюджетной сети города Переславля-Залесского.

18. Принципы построения национальной сети

Россия обладает рядом особенностей, одна из которых — это огромные территории с относительно низкой плотностью населения, поэтому вопрос дорог и коммуникаций стоит перед Россией наиболее остро, возможно, даже острее, чем для других стран. Национальная телекоммуникационная компьютерная сеть для России — это один из основных факторов развития экономики, социальной и других областей. Общие принципы построения сети национального масштаба, если подходить к этому вопросу рационально, можно изложить следующим образом: для покрытия всей территории единой сетью, необходимо создать национальную магистральную сеть, которая бы соединяла бы между собой все крупные города (например, областные центры). То есть требуется поставить роутеры во всех крупных городах и соединить их скоростными и надежными каналами связи. От базовых узлов должна отходить региональная сеть, объединяющая более мелкие города (например, районные центры), от которых строится более мелкая сеть муниципального уровня, соединяющая непосредственно конечных абонентов — частных лиц и организации

Оценим количество требуемых затрат на создание такого типа сети. Ограничим количество узлов магистрального уровня сотней (примерное количество областей), среднее количество районных центров в каждой области порядка 10. Таким образом, магистральная часть включает в себя порядка 1000 узлов и каналов, которые стоят вполне разумных денег. Переходя на самый низкий уровень райцентров, получаем порядок от 10000 до 100000 абонентов (в перспективе) для одного районного центра. Легко видеть, что количество структурных единиц сети на уровне магистрали и на конечном уровне разнится в сотни и тысячи раз. Отсюда несложно сделать вывод, что федеральному бюджету скорей всего не удастся профинансировать

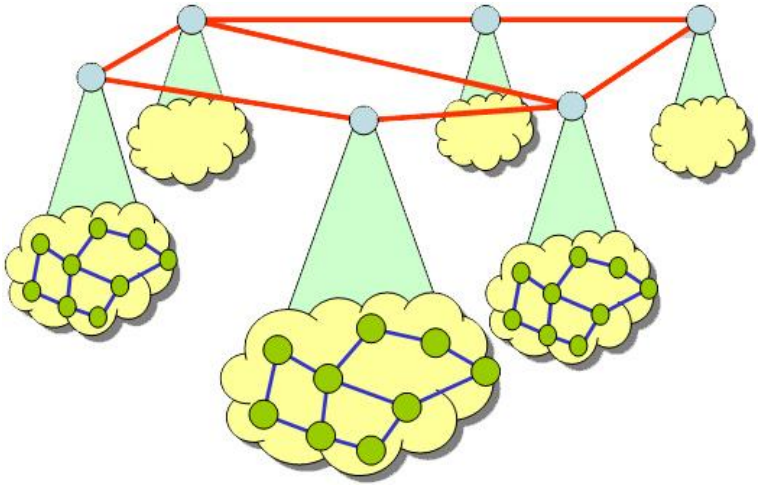

Рис. 21. Структура национальной сети

построение линий телекоммуникаций непосредственно до конечного пользователя, однако вполне может (и должен) быть построен магистральный уровень сети. В итоге получаем, что проблема создания сети регионального уровня на сегодняшний день в конкретной стране Россия может быть решена только самостоятельно жителями конкретной местности на свои собственные средства.

Обратимся к вопросу о том, как идет построение государством телекоммуникационной сети магистрального уровня. Обзор выполненных в этом направлении работ приводит к выводу о нерациональном планировании и вложении средств. Вместо того чтобы сконцентрировать ресурсы на решение задачи построения единой национальной магистральной сети, происходит создание множества дублирующих друг друга ведомственных и специализированных сетей, таких как Научнообразовательная сеть, сеть Российских университетов, сеть Центробанка РФ, Сбербанка, Сеть для проведения выборов, сеть Газпрома, военные сети и т. д. Кроме *ведомственных сетей с политикой* (то есть сетей, подключиться к которым может только определенный круг абонентов — закрытые сети) существуют сети без политики,

коммерческие сети, такие как Ростелеком (компания, унаследовавшая телекоммуникационные сети, существовавшие еще при Советском Союзе), Трансгелеком (дочерняя компания Министерства путей сообщения, которое прокладывает оптоволоконный кабель вдоль принадлежащих им железнодорожных путей) и т. д. Налицо крайняя неэффективность решения задачи при недостаточном финансировании. Для сравнения обратимся к опыту других стран и рассмотрим, как им удалось решить ту же самую проблему создания магистральной сети национального уровня.

19. Глобальная оптоволоконная инициатива США

Обратимся к не самой бедной стране — Соединенным штатам Америки. Рассмотрим сеть Министерства обороны США (иначе Пентагон) и ключевую фразу «*глобальная оптоволоконная инициатива*», под которой понимается, что, во-первых, оборонное ведомство США в качестве среды передачи данных рассматривает оптоволокно по причинам высокой пропускной способности и защиты от прослушивания (сигнал не выходит за оптоволокно в отличие от медного кабеля, в котором распространяется электромагнитная волна, которая существует и вне него, и существует возможность снимать сигнал за счет внешних наводок), во-вторых, предполагается повсеместное использование каналов передачи данных, вплоть до использования оптоволокна на поле боя. Однако возникает вопрос, как передавать данные на большие расстояния, есть ли собственная военная магистраль? Оказывается, военное ведомство США использует для передачи данных обычные гражданские каналы связи, арендуя их у коммерческих компаний. Вопрос о соблюдении секретности данных находится в компетенции специалистов по криптографии. Современные методы шифрования гарантируют необходимые условия секретности. Рассмотренный пример еще раз демонстрирует, что создание множества специализированных сетей крайне неэффективно.

20. Принципы построения экономически эффективных региональных сетей

Предварительные рассуждения показывают, что при построении региональных сетей ждать помощи от государства не приходится, а задача, которая стоит перед нами — на порядки сложнее, чем те, которыми занимается государство. Учитывая, что вся финансовая

нагрузка при построении региональной сети ложится на жителей региона, покупательная способность которых невысока, делаем вывод, что использовать затратные технологии не представляется возможным. Требуется разработать и реализовать экономически эффективные сетевые технологии. Данная постановка задачи накладывает серьезные ограничения на используемое оборудование и программное обеспечение, в числе которых отметим:

(1) **Отказ от законченных сетевых решений для провайдеров** (в силу крайней дороговизны последних). Существуют так называемые «законченные сетевые решения» — профессиональные изделия, полностью готовые для выполнения требуемых функций. При этом, при ближайшем рассмотрении такое профессиональное оборудование практически ничем не отличается от пользовательского в плане функциональности, в нем лишь уделено дополнительное внимание надежности, однако стоимость этих изделий во много раз перекрывает стоимость аналогичной техники, поставляемой на рынок домашних устройств даже с учетом дополнительных затрат на обеспечение большей надежности. Примером таких решений может служить Web-сервер, поставляемый в виде системного блока с полностью установленным настроенным программно-аппаратным обеспечением, который требуется только подсоединить к сети и по FTP поместить странички. Такой подход, разумеется, очень удобен и не требует наличия специалистов, которые бы занимались установкой и настройкой этого сервера, однако за такое удобство необходимо заплатить в 2-3-4-5 раз дороже, чем за аналогичный компьютер с тем же софтвером. Другой пример — это IP-маршрутизаторы, где лидером на рынке является фирма *CISCO*. Поставляемые ею маршутизаторы при ближайшем рассмотрении являются всё теми же компьютерами, однако, со специализированным аппаратным обеспечением, ускоряющим решение задачи маршрутизации и управления IP-пакетов. Стоимость этих изделий крайне высокая: от 2000–3000 до десятков тысяч долларов. Плюс к этому оборудование комплектуется специфическим программным обеспечением.

(2) **Отказ от коммерческого программного обеспечения.** Данный тезис не подразумевает пиратское использование

ПО, так как создается общедоступный ресурс, который оказывается под пристальным надзором соответствующих государственных служб. Таким образом, складывается ситуация, при которой воровать мы не можем, а покупать — нет денег, тогда нам не остается ничего другого, как пользоваться некоммерческим, свободно распространяемым софтвером.

(3) **Отказ от аренды каналов (линий связи)**. При построении серьезных сетей с большим бюджетом проще всего решать проблему каналов связи их арендой. У организаций-владельцев телекоммуникационных каналов запрашивается либо физический набор проводов (например, 2 или 4 медных кабеля), либо канал, т. е. некоторая полоса пропускания в их цифровых потоках. Такой подход очень удобен, но на сегодняшний день слишком дорог.

Отказавшись практически от всех базовых элементов построения сети, требуется найти им соответствующую замену. Перечислим аналогичные малобюджетные решения:

(1) **Широкое использование аппаратуры массового производства: класса IBM PC, технологий и изделий семейства Ethernet (и др.), а также собственных аппаратных разработок.** Дешевизна данной аппаратуры обусловлена, прежде всего, ее массовым производством, поэтому основной задачей при комплектации сети будет приспособление различного оборудования, предназначенного для конечного пользователя к нуждам провайдера, с вытекающими отсюда требованиями к функциональности надежности. Чаще всего возможностей массовой аппаратуры будет достаточно для построения сети, но чего-то может не хватать, поэтому потребуется использовать собственные аппаратные разработки для доведения ее до требуемого уровня надежности и функциональности. Возможность доработки промышленной аппаратуры во многом объясняется тем, что для массового оборудования существует подробная документация в свободном доступе, что выгодно отличает этот класс аппаратуры от изделий дорогих брендов.

(2) **Широкое использование свободного программного обеспечения с исходными текстами + собственные**

программные модификации и разработки. Под свободным ПО мы будем понимать, что «свободное» обозначает не только бесплатное, но и поставляемое с исходными кодами (open source). Важность открытости исходных кодов состоит в том, чтобы работать вне зависимости от первоначальных разработчиков используемого ПО. Зачастую может не хватать какой-то специфической функциональности, или что-то может работать не так, поэтому всегда нужно иметь возможность внести необходимые изменения и дополнения. Кроме того, наличие открытого кода дает возможность контролировать информационную безопасность продукта, в том числе отслеживать наличие так называемых «закладок» — дополнительной, не анонсируемой функциональности, которая срабатывает без ведома пользователя (типа «троянский конь»).

(3) **Строительство собственных линий передачи данных.** Для реализации такой постановки потребуется найти и реализовать способы построения дешевых и надежных каналов на региональном уровне. Данный тезис выглядит спорным, особенно после заявлений о нерациональности построения ведомствами своих особых подсетей. Дело в том, что общинная сеть, строящаяся за счет средств абонентов и сеть государственного ведомства — суть вещи разные. Нерациональным является двойное, тройное и т. д. расходование средств из общего государственного бюджета, т. е. из кармана налогоплательщика только потому, что ведомственные чиновники не смогли или не захотели договориться о более рациональном расходовании средств. В случае самостоятельной оплаты сети приходится выбирать наиболее дешевое решение и, если в какой-то момент стоимость аренды канала будет стоить вполне приемлемую сумму, которую абонент будет готов платить коммерческой организации, то необходимость в построении и обслуживании собственных линий связи отпадет.

21. Топология региональной сети

Первоначально высокобюджетные сети создавались следующим образом: закупалась и устанавливалась дорогая аппаратура, затем

арендовался канал с внешним подключением. После чего объявлялось о начале подключения абонентов, которые могли либо по коммутируемым линиям подсоединяться через модем, либо арендовать постоянный канал, соединенный с аппаратурой. В итоге получается архитектура типа звезды, где каждый канал заканчивается в общей точке, на которую с ростом сети нагрузка будет неуклонно возрастать. К тому же зачастую каналы будут создаваться нерационально: для двух абонентов, находящихся по соседству, придется прокладывать или арендовать отдельные линии до точки подключения, которая может находиться на приличном расстоянии, и соответственно, сигнал между ними должен будет пройти через центральную точку. Описанная архитектура характерна для телефонных линий связи, которая повторяет административное деление, существующее в России, а при создании сетей такое деление просто повторялось. Так, например, телефонный сигнал из Переславля в Москву первоначально идет в Ярославль, где коммутируется и идет в Москву через канал, который физически проходит через Переславль, при этом путь, проделанный сигналом, возрастает в три раза. Описанная высоко централизованная система имеет и свой плюс: простоту в контроле над сетью. Основным же недостатком является возможность перегрузить систему.

Вместо того чтобы строить систему, повторяющую искусственно сложившуюся иерархию, мы будем стараться строить сеть, которая повторяет географическое расположение объектов. Естественные потребности в коммуникации людей в некомпьютерной среде в большой степени состоят из локального обмена информацией и существенно меньшего обмена информацией с уделенными абонентами, в то же время с развитием телекоммуникаций, вопрос о территориальной привязке агента становится неактуальным. Тем не менее, в нынешних условиях мы вынуждены искусственно ставить барьер между локальными и глобальными коммуникациями, причем прежде всего по причине высокой стоимости внешнего трафика. Локальный же трафик имеет ограничение только в виде пропускной способности канала и мощностей оборудования. Учитывая описанные условия, получаем, что региональная сеть должна максимально способствовать развитию локальных коммуникаций, чтобы отчасти возместить недостаточную доступность внешней коннективности. В силу этого локальные каналы по своей пропускной способности должны существенно

превышать внешние, так как именно на них ложится основная нагрузка.

22. Политика региональной сети

Определимся, какая категория пользователей должна иметь возможность подключения к региональной сети. Несложно понять, что для того, чтобы выжить и успешно развиваться региональная сеть не должна содержать политики, то есть ее абонентом может стать любой желающий, будь то частное лицо или организация. Конкретно же причины такого решения следующие:

(1) *экономическая:*
при низком финансировании вводить ограничения на подключение неразумно, так как каждый новый абонент приносит с собой деньги;

(2) *технологическая:*
из вышеизложенного ясно, что основной архитектурой для региональной сети является Ethernet, который имеет серьезное ограничение на расстояние (200–700 метров) между оборудованием. Таким образом, узлы сети должны располагаться на таком же расстоянии друг от друга в черте города, при этом было бы неплохо, поставив оборудование в некоторой точке, собрать вокруг него клиентов. В городской черте с ее достаточно плотной застройкой на указанном расстоянии с большой вероятностью найдется клиент для подключения к сети.

23. Схема региональной сети

Теперь можно схематически изобразить архитектуру региональной сети. Здесь в качестве оборудования будут использоваться изделия семейства Ethernet: hub, switch, IP-router. Узлы между собой будут связаны линиями передачи данных, причем для повышения надежности сети, она будет избыточна (содержать кольца). IP-маршрутизаторы должны использовать динамическую маршрутизацию, чтобы в случае нарушения линии автоматически задействовать резервные каналы. К узлам размещения оборудования будут подключены абоненты. В некоторые точки системы должны подходить каналы внешнего доступа. Наконец, в некоторой точке системы должен быть установлен центральный сервер, который бы предоставлял услуги клиентам (почтовый сервер, web-сервер, ftp-сервер), так и содержал

бы инструменты для управления сетью техническим персоналом, в том числе DNS, маршрутизация, служба мониторинга и сообщения об отказах, наконец, служба расчета с клиентами.

24. Задачи, требующие разрешения в процессе построения и эксплуатирования региональной сети

Рассмотрим те технические решения, которые требуется найти для следующих компонент:

(1) построение сети
  (a) центральный узел, обеспечивающий услуги:
    (i) DNS
    (ii) Mail (POP3, SMTP)
    (iii) WWW
    (iv) FTP
    (v) News
    (vi) Proxy Cash и др.
  (b) магистральная сеть
    (i) каналы
    (ii) активное оборудование
      (A) хабы
      (B) коммутаторы
      (C) роутеры
  (c) лицензирование
(2) эксплуатация сети
  (a) обеспечение надежности
    (i) мониторинг работоспособности
    (ii) самовосстановление после сбоя
    (iii) оповещение об отказах
  (b) биллинг (учет услуг и взимание оплаты) и конфигурирование системы — Nadmin
  (c) предотвращение перегрузки
  (d) автоматизация управления сетью — Nadmin

24.1. Организация каналов в региональных сетях. Перечислим те материалы, которые доступны на сегодняшний день для прокладки магистральных каналов в региональных сетях.

$^{(I)}$ **Среда передачи. SFTP 5 cat.** Указанный кабель является собственной разработкой СТ «Ботик». Заняться собственными разработками заставил тот факт, что производители кабеля чаще всего

Среда передачи	Дистанция, м	Скорость, Мбит/с	Технология передачи	Стоимость интерфейсов	Стоимость кабеля кабеля
SFTP 5 cat.$^{(I)}$	150–170$^{(II)}$	100	Ethernet	\$ 30$^{(III)}$	\$ 0.25/1 м
SFTP 5 cat.	250–300	10	Ethernet	\$ 30	\$ 0.25/1 м
Коаксиал. кабель РК75 4.9312$^{(IV)}$	600–1200	10	Ethernet	\$ 30	\$ 0.18/1 м
Многомод. оптовол.$^{(V)}$	2000	10	Ethernet	\$ 230	\$ 4/1 м
Многомод. оптовол.	4000	100	Ethernet	\$ 500	\$ 4/1 м$^{(VI)}$
Радио $^{(VII)}$	до 12000 (в зоне прямой видимости)	11	Radio-Ethenet	\$ 1100 \$ 1100	Оформл. лиценз. (\$ 4000)

Таблица 2. Стоимость прокладки кабелей разного типа

ориентируются на его прокладку внутри зданий и не рассчитывают на то, что он будет использоваться вне зданий. Это ведет к тому, что внешняя оболочка кабеля выполняется из неустойчивого к солнечной радиации пластика, который через некоторое время пребывания на улице растрескивается и кабель разрушается. СТ «Ботик» для прокладки магистральных каналов использует кабель, который производится в два этапа: на первом московском заводе делается кабель неэкранированной витой пары (UTP), который перевозится на доработку на другой московский завод, где на него наносится две оплетки: фольга и экран, после чего все заливается светостабилизированным полиэтиленом.

$^{(II)}$ **Дистанция передачи. SFTP 5 cat. 150-170 м.** Обратим внимание, что в графе «Дистанция» указаны цифры, превышающие значения, которые по стандарту варьируются в районе 100 метров. Всё дело в том, что со времени написания стандартов технологии создания кабелей и сетевых карт ушли вперед и на настоящий момент получены изделия с более качественными характеристиками:

боле мощным приемником, более чувствительным передатчиком, более низким коэффициентом затухания сигнала, что дает возможность корректировать расстояния гарантированной передачи в большую сторону. В указанных интервалах длин меньшая — это гарантированная длина на любом оборудовании, большая — возможная длина при соответствующем подборе изделий.

(*III*) Стоимость интерфейсов. SFTP 5 cat. $ 30. В графу «стоимость интерфейсов» заложена стоимость двух сетевых плат примерно по $ 10, плюс розетки, патчкорд, вилки, крепеж и т. д.

(*IV*) **Среда передачи. Коаксиальный кабель РК75 4.9 312.** В данном случае коаксиальный кабель используется в режиме «точка–точка» (то есть используется «шина» с двумя абонентами на концах). Известно, что стандарт 10BASE-2, в котором используется коаксиальный кабель, предназначен для использования на дистанциях в 300 метров. Удалось добиться работы этого типа кабеля на дистанциях в 600–1200 метров за счет использования нестандартного кабеля, который не предназначен для прокладки компьютерных сетей, и был подобран специально для увеличения длины сегмента. Дистанция передачи сигнала зависит от множества параметров, например, от затухания и времени передачи сигнала. Расстояние, пройденное сигналом, равняется времени передачи, умноженной на скорость распространения электромагнитного сигнала в среде передачи (проводе), которая для каждого материала разная. В кабеле сигнал передается по поверхности проводника, то есть физически он располагается в изоляции кабеля, находящемся между несущей жилой и оплеткой, поэтому скорость передачи зависит от проводящих характеристик наполнителя. Так в используемом кабеле вместо обычного полиэтилена в качестве наполнителя использован вспененный полиэтилен, обладающий лучшей проводимостью. Плюс к этому взят кабель, отличающийся от стандартного кабеля по волновому сопротивлению (по стандарту оно равно 50 Ом), здесь использован кабель с сопротивлением в 75 Ом. В дополнение, сам кабель толще, что позволяет снизить обычное сопротивление. Интересно, что в итоге данный кабель получился дешевле своего стандартного аналога.

(*V*) **Среда передачи. Многомодовое оптоволокно.** Сам канал представляет собой светопроводящую среду, на концах которой расположена фотопара: излучатель — фотодиод и приемник — фоторезистор. Выбирается способ кодирования сигналов (например, изменение амплитуды). Чтобы передавать сигнал с частотой в 10/100

Мбит/с требуются высокочастотные приемники и передатчики, способные генерировать и принимать высокочастотный сигнал. В качестве среды передачи используется стекло, которое становится гибким, если его сделать достаточно тонким, таким, что его можно даже сгибать. Толщина волокна сопоставима с толщиной человеческого волоса, и это очень сложное инженерное сооружение. Сама жила оптоволокна делается двухслойной: внутри идет ядро — стекло с низким коэффициентом преломления, а внешний слой — с высоким. За счет этого при малых углах наблюдается эффект полного отражении, и свет, проходя по изогнутому оптоволоконному кабелю, отражается практически без потерь от его стенок и при этом находится всё время внутри ядра оптоволокна.

Многомодовое волокно, в отличие от одномодового волокна, рассчитанного на передачу сигналов с конкретной частотой излучения (за счет чего передача возможна на большие дистанции, но при этом конечные устройства достаточно дорогие), рассчитано на передачу сигналов для широкого спектра частот, что делает его использование дешевле. В силу того, что само волокно очень ранимо, оно заключено в защитную трубочку, заполненную гелем. Данная конструкция называется жила. Из набора таких жил строится кабель. СТ «Ботик» в настоящее время использует два типа кабеля. Первый тип кабеля называется «кабель оптический подвесной», который состоит из оболочки, изготовленной из светостабилизированного полиэтилена, с несущим тросиком и полостью для различного количества оптоволоконных жил (по заказу). В региональной сети Переславля используются 4-х и 8-ми жильные кабели.

Второй типа кабеля — кабель для закопки в землю. Данный тип кабеля стоит дороже за счет того, что на нем имеется хорошая гидроизоляция, есть защита от сдавливания и даже слой защиты от грызунов.

Оконцовку оптоволоконного кабеля должен осуществлять только специалист и только специальными инструментами. Рассмотрим это более детально.

Для присоединения конца кабеля к приемнику/получателю требуется идеально точно направить излучатель на ядро оптического волокна. Для этого на конец каждого волокна надевается керамическая вилка, в которой есть канал размером с жилу, которую нужно, освободив от внешних оплеток, туда поместить, предварительно

сделав перпендикулярно скол стеклянной жилы с точностью до полградуса. (Для справки: инструмент для скола оптоволокна с нужной точностью стоит $ 500.) После вставки обрубленного волокна в вилку, последняя помещается в точно подогнанную муфту, где фиксируется при помощи специального клея, стоящего порядка $ 10–$ 50 за 2 грамма. После этого стык полируется специальными средствами с особым контролем. Оконцованный провод вставляется в плату на компьютере, имеющую оптический разъем.

После прокладки оптоволоконного канала встает вопрос о передаче данных по нему. Для этого существуют соответствующие платы Ethernet с оптическим разъемом, хабы Ethernet-сигнала в оптический и наоборот. Для передачи данных используются две оптические жилы: для передачи и приема в одном и в другом направлении. В таком случае невозможны коллизии, так как для каждого передатчика существует собственный канал передачи, в силу этого снимается ограничение на длину пакетов данных и достигаются большие расстояния передачи.

$^{(VI)}$ **Стоимость кабеля. Многомодовое оптоволокно.** $ 4/1 м. В стоимости отражен «подвешенный» кабель, то есть включены затраты на его монтаж.

$^{(VII)}$ **Среда передачи. Радио.** В технологии RadioEthenet эмулируются те же процессы, что и при передаче данных в технологии витой пары со всеми понятиями, знакомыми по 10BASE-T: коллизия, разрешение коллизии и т. д. Ключевым изделием на сегодняшний день для данной технологии передачи является карта PCMCIA (Personal Computer Memory Card International Association), на которой смонтирован передатчик, приемник и выход для подключения антенны. Антенна может комплектоваться антенным усилителем для увеличения дальности передачи сигнала, это позволяет получить расстояние не 12 км, а существенно больше, вплоть до 100 км. Кроме того, существуют соответствующие switch и router, в которых есть порты для витопарного Ethernet 10/100 Mbit/c и слоты для карт PCMCIA. В зависимости от задачи могут использоваться разные конфигурации антенн: круговые антенны (штыревые) и узконаправленные (параболические). В случае использования круговой антенны, в зоне ее покрытия располагаются абоненты, оснащенные оборудованием приема/передачи сигнала. Такая конфигурация является одним сегментом shared-Ethernet, ее называют «сота», в ней также как и в

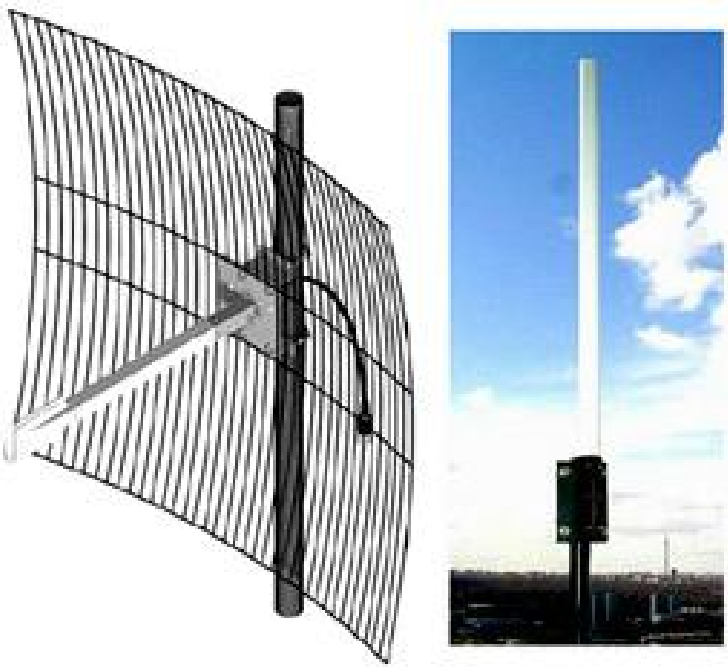

Рис. 22. Слева: антенна параболическая ГРАД 2497; справа: антенна штыревая ГРАД 2401

уже рассмотренных сегментах проводного Ethernet возникают коллизии. Вторая конфигурация — «*ad hoc*» [лат. *специально для данного случая*] представляет собой две параболические антенны, т. е. передача происходит в режиме «точка–точка».

Отметим, что затраты на оборудование и лицензирование достаточно велики, поэтому массовое использование этой технологии для подключения абонентов в малобюджетных сетях затруднительно. Более перспективным выглядит использование этой технологии для объединения достаточно удаленных сегментов сети, включающих некоторую группу пользователей. Однако необходимо отметить и плюсы в использовании такого вида каналов, такие как быстрота

развертывания, мобильность (возможность легко перенести оборудование при исчезновении необходимости в данном канале) и высокая надежность.

Обратимся к вопросу лицензирования радио-канала. В соответствии со стандартом IEEE 802.11 — RadioEthernet в диапазоне частот 2,4 ГГц, мощность сигнала без усилителя составляет 32 мВт, а сигнал кодируется таким образом, чтобы он был похож для других приемников на белый шум. На данную частоту необходимо получить лицензию, хотя ее излучение практически совпадает с излучением, которое производит в процессе работы микроволновая печь. Лицензированию подлежит тот факт, что организация имеет право на определенной местности (указывается радиус зоны покрытия) излучать сигнал определенной частоты (указывается частота) некоторой мощности (указывается мощность), плюс указывается тип модуляции сигнала.

Обратим также внимание на тот факт, что для успешной радиопередачи с указанной частотой требуется прямая видимость, так как сигнал такой частоты практически не огибает препятствий. Эта задача довольно серьезна, так как при малейших помехах на пути сигнала его мощность падает очень сильно. Кроме того, при больших расстояниях уже требуется учитывать кривизну Земли и проектировать вышки в соответствии с этой поправкой.

Рис. 23 иллюстрирует экономическую эффективность использования тех или иных технологий при прокладке каналов на различные расстояния.

24.2. Узлы региональной сети. В качестве узлов региональной сети выступают три категории оборудования:

(1) хабы;
(2) коммутаторы (switch);
(3) роутеры.

Хабы для построения сети проще всего взять готовыми, так как это достаточно распространенные изделия и цена на них приемлема (порядка \$ 20–25 за 8×10BaseT — 8-портовый хаб для 10 Mbit/c соединения по витой паре). Аналогичная ситуация и с коммутаторами, которые при качественном исполнении стоят порядка \$ 50–60 за 8×100BaseTX — 8-портовый switch для 100 Mbit/c Ethernet. В качестве IP-маршрутизаторов можно использовать законченные сетевые

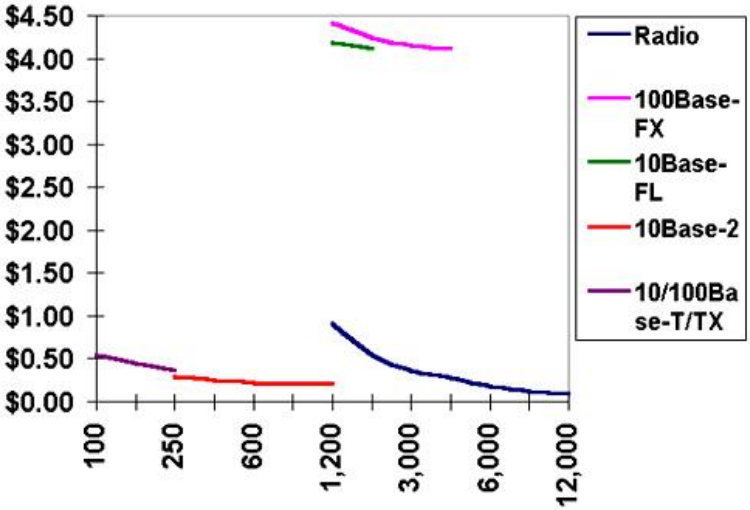

Рис. 23. График удельной стоимости (за 1 метр)

решения от известных фирм, но их стоимость составляет тысячи долларов, что в нашем случае не годится. В качестве маршрутизаторов нами будут использоваться изделия под названием PC-роутер.

Ранее уже обсуждалось, что любой IP-марштуризатор, поставляемый в виде законченного решения, является специализированным компьютером (но все же компьютером), с установленной на нем операционной системой и выполняющий задачу маршрутизации пакетов. При этом есть доступ к нему через telnet, иногда через web-интерфейс для его конфигурации, фильтрации пакетов и т. д.

25. ПК-роутер

Вместо того чтобы воспользоваться законченным изделием, можно собрать его самостоятельно. Для этого требуется взять обычный IBM PC, из которого за ненадобностью исключены устройства типа монитор, видеокарта, клавиатура, дисковод. Нам потребуется только материнская плата (побольше слотов расширения), процессор (x386, x486 порядка 100MGz), оперативная память (16 Mb), жесткий диск

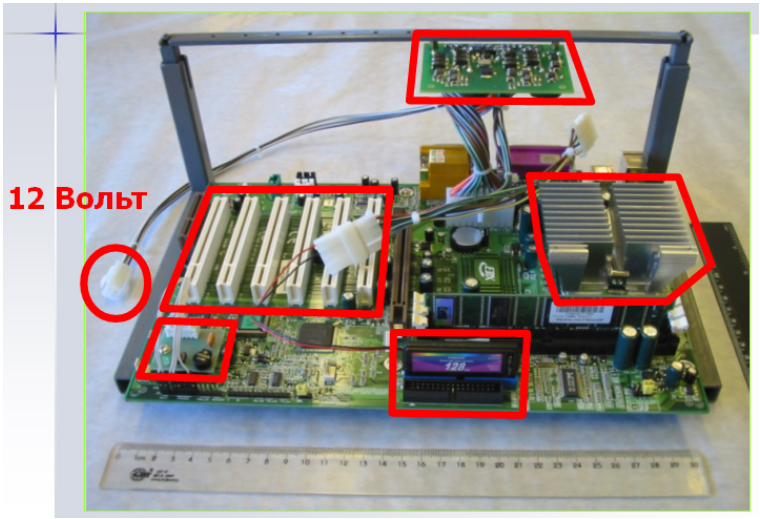

Рис. 24. Новое поколение ПК-роутеров

(170 Mb), которые назовем базовой конфигурацией, плюс интерфейсные карты: сетевые платы, поддерживающие обычный Ethernet, оптоволоконный интерфейс, RadioEthernet и т. д.

Затем требуется оснастить данное оборудование соответствующим программным обеспечением, позволяющим решать задачу маршрутизации. В качестве базы используется свободно распространяемая ОС Linux с функциями, присущими роутеру.

С точки зрения денег получается следующая картина: в 2000 году базовый комплект можно было купить за $ 95, плюс стоимость сетевых интерфейсов. По большей части используется витопарный Ethernet, для которого сетевые карты стоят порядка $ 12. В итоге получаем разницу по стоимости изделия в десятки раз, но не все так просто дается. Профессиональное оборудование все же отличается от достаточно устаревшей аппаратуры, предназначенной для домашнего пользования, прежде всего, повышенной надежностью. С компьютерами, собранными по описанной схеме, нередки случаи самопроизвольного «зависания», и вывести его из такого состояния возможно лишь при помощи аппаратной перезагрузки (reset). Решать данную

проблему придется путем собственных дополнительных разработок. Прежде чем перейти к рассмотрению устройства оборудования, гарантирующего работоспособность роутера, убедимся, что использование аппаратной перезагрузки будет действительно полезно и не выведет роутер из строя.

25.1. Особенности хранения данных на ПК-роутерах. Устойчивость роутера к внезапным перезагрузкам — есть обязательное требование к данному изделию (мы должны помнить о нестабильном электропитании в малом городе). Утверждается, что PC-роутер МОЖНО остановить в любой момент времени без вреда для его будущей работоспособности. Почему это верно? Все современные операционные системы для ускорения времени работы с диском не занимаются записью на винчестер сразу после получения соответствующей команды, а кэшируют ее, чтобы впоследствии произвести запись большим объемом и затратить меньше времени, либо более быстро выдать данные при их запросе. Поэтому, если в произвольный момент отключить питание от компьютера, то структура файловой системы на диске может быть с некоторой вероятностью нарушена. Для решения указанной проблемы была применена следующая разработка: на ПК-роутерах используется три класса хранения данных:

(1) **корневой раздел** — / монтируется только для чтения, используется для хранения неизменяемой информации, физически размещается на локальном диске;
(2) /**volatile** монтируется на отдельном разделе диска, открыт на чтение/запись, предназначен для хранения временных, служебных, лог-файлов. Данный раздел не будет подлежать восстановлению, а при каждом старте системы он будет создаваться заново (форматироваться);
(3) /**remote** для надежного хранения данных используется удаленный диск, открытый для чтения/записи (на центральном узле, для которого обеспечивается бесперебойная работа).

Таким образом, при перезагрузке целостность всех важных для работоспособности данных гарантируется, раздел с временной информацией восстанавливается при загрузке, а данные, которые необходимо надежно хранить, содержатся на удаленном сервере с гарантированным электропитанием. Очевидно, что описанная архитектура файловой системы позволяет не опасаться перезагрузок.

26. Watchdog

Теперь обратимся к проблеме автоматического контроля за работоспособностью роутера и его самовосстановлению после сбоев. Специалистами СТ «Ботик» разработана система автоматического слежения за работоспособностью роутера и восстановления в случае сбоя или отказа — Watchdog. Заметим, что существуют промышленные аналоги, поставляемые с соответствующим программным обеспечением, однако, как водится в мире законченных решений, стоят они дорого (до $ 100, что сопоставимо со стоимостью всего ПК-роутера), стоимость же домашней разработки укладывается в $ 3. Данное программно-аппаратное изделие перегружает роутер в случае отказа по любой причине, будь то программный или аппаратный сбой, здесь важен тот факт, что роутер можно многократно аппаратно перегружать без нарушения его работоспособности. Схематически Watchdog выглядит следующим образом:

Устройство данного изделия очень просто: на программном уровне существуют программы — проверяльщики (*сенсоры*), которые делают оценку состояния различных функций роутера. Например, для гарантии нормальной работоспособности узла требуется убедиться, что функции маршрутизации и DNS работают нормально, все ли интерфейсы функционируют и т. д. Конфигурация проверок выглядит как некий скрипт (набор команд), для соответствующего ПО, формирующего на выходе результат: «все в порядке» или «есть проблемы». Такой набор команд формируется индивидуально для каждого роутера, в виду того, что они различаются друг от друга качеством и количеством интерфейсов. Если сбоев не обнаружено, то драйвер Watchdog'а на специальную плату с некоторой частотой посылает сигнал «все в порядке». На самом деле, все происходит еще проще: драйвер Watchdog'а с определенной частотой все время посылает сигнал «все в порядке» на плату, программы проверки же в своем режиме тестируют систему и как только обнаруживается сбой, происходит завершение работы драйвера, что ведет к последующей перезагрузке. Аппаратная часть устройства (собственно плата) включает в себя прежде всего таймер, установленный на некоторый интервал времени (например, 3 минуты), при этом частота сигналов, поступающая от драйвера выше, чем время таймера. Получение сигнала «все в порядке» от драйвера «сбрасывает» таймер, и отсчет начинается сначала. В случае если сигнал о нормальном функционировании не поступает и таймер доходит до нуля, то происходит reset компьютера.

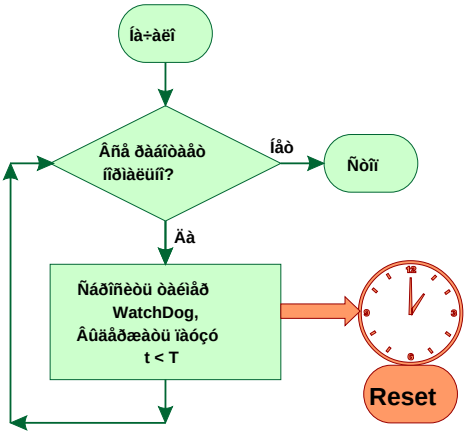

Рис. 25. Аппаратный Watchdog (принципы работы)

Рассмотрим более детально реализацию аппаратной части устройства. Очевидно, что у него должен быть разъем, установленный на reset, также требуется, чтобы была возможность программному обеспечению подавать сигнал на устройство о том, что все в порядке. Вопрос о его подключении не так прост. Дело в том, что разместить Watchdog можно в один из стандартных слотов (PCI, USB, COM, ...), но, во-первых, у роутера «потерять» любой стандартный порт жалко, так как он может быть использован для подключения дополнительного сетевого интерфейса, во-вторых, изготовление платы для стандартного слота — дело хлопотное и недешевое. В данном случае для подключения был использован разъем спикера. Тогда драйвер посылает сигнал «все в порядке,» в виде стандартной команды спикеру. В итоге плата Watchdog имеет четыре контакта, один на reset, второй на спикер, третий на светодиод TURBO и, наконец, четвертый на кнопку TURBO. Электропитание для платы получается также с разъема спикера. Светодиод используется для визуального контроля за тем, что система работает, а кнопка TURBO — для отключения Watchdog в случае, если требуется проводить работу с роутером.

Время таймера Watchdog'а определяется временем загрузки Linux, компьютер должен иметь возможность полностью загрузить ядро, и аппаратная часть могла Watchdog начать работу. Иначе будет происходить постоянный reset, и система не сможет загрузиться.

На настоящее время реализована новая версия Watchdog, использующая микроконтроллер. На нем реализована более сложная логика: Watchdog в первый раз делает большую паузу (чтобы система успела загрузиться), а потом пауза становится меньше, чтобы минимизировать простой роутера при обнаружении сбоя. Кроме того реализована возможность автоматически распознавать разъемы, к которым подключены контакты, поэтому можно соединять контакты не задумываясь, где спикер, где reset и т. д.

26.1. Функциональность ПК-роутера. Рассмотрим более детально программное обеспечение и ПК-роутера, и выполняемую им функциональность. Отметим, что здесь, как и в остальных случаях, используется только свободное программное обеспечение плюс свои собственные разработки. Основные функции роутера:

(1) **IP-маршрутизация.**
Обеспечивается ядром Linux;
(2) **Динамическая маршрутизация (DSPF2, BGP4).**
Происходит переход на ПО Zebra;

(3) **Фильтрация IP-пакетов.**
Отказ в маршрутизации пакетов по определенным причинам, Основные области применимости данной функции — обеспечение безопасности и отключение неплательщиков. Реализуется при помощи средств, содержащихся в ядре Linux, плюс утилита ipfwadmin (IP FireWall Admin);

(4) **IP-маскарадинг.**
Механизм, меняющий IP-адрес отправителя пакета. При получении пакета IP-адрес, предназначенного для отправления на адрес получателя, адрес отправителя заменяется на IP-адрес роутера, и обратно, при получении ответа снова подменяется адрес теперь уже получателя на истинный IP-адрес реального отправителя. Эта функция требуется для того, чтобы скрыть истинный IP-номер отправителя, либо предоставить возможность использовать приватные IP-номера;

(5) **Ethernet-bridge.**
Роутер может работать как switch, то есть обрабатывать MAC-адреса. Такой подход может быть полезен, так как switch в трассе прохождения IP-пакета «не виден», то есть прохождение через него не добавляет дополнительный шаг (хоп) в счетчике пакета. Напомним, что у каждого пакета есть счетчик времени жизни TTL (Time To Live), который уменьшается после прохождения каждого из роутеров, при достижении нуля пакет выбрасывается. Это делается для того, чтобы пакет не жил в сети бесконечно долго (в случае ошибки маршрутизации) и не занимал каналов, он должен когда-то прекратить свое существование. По этой причине, если TTL пакета невелико, то он может просто не доходить до адресата по причине большого количества роутеров между ними. Объединение функциональности роутера и switch может быть полезно, когда в узле часть интерфейсов соединена по правилам коммутации, а часть маршрутизируется. Реализуется при помощи доработанного ядра Linux и утилитой brcfg;

(6) **Удаленное управление.**
Чтобы удаленно менять конфигурацию роутера используются протоколы Telnet, RSH, SSH, SNMP. Реализуется ядром Linux;

(7) **Сбор статистики.**
Требуется для учета платного трафика, позволяет наблюдать за сетью и разбирать спорные и конфликтные ситуации. Используется ядро Linux, ipfwadmin, TCPdump — утилита, сохраняющая проходящие IP-пакеты;

(8) **Доставка статистики.**
Результаты сохраняются в разделе /remote роутера, находящемся на удаленном сервере. Реализуется ядром Linux;

(9) **Обслуживание модемов.**
Используются утилиты: mgetty, Xchat, uucord;

(10) **Назначение псевдостатических IP-номеров.**
Необходимо для модемных использования подключений, которые должны получать DNS-разрешимые имена и псевдостатические номера. В момент подключения модемного пользователя производится выделение ему номера из некоторого множества IP-номеров и внесение в DNS соответствующей правки, что данный номер принадлежит абоненту с некоторым именем. Разумеется, было бы правильнее минимизировать количество правок в DNS, поэтому при выделении номера проверяется, свободен ли IP-номер, использовавшийся данным пользователем в прошлый сеанс связи. Если это так, то номер выделяется и правки таблицы DNS не происходит. Используется программа migrator собственной разработки СТ «Ботик»;

(11) **Контроль использования IP-номеров.**
Такая функциональность требуется для того, чтобы не происходил подмен IP-номеров пользователями, как по ошибке, так и с целью кражи трафика.

(12) **Вторичный (кэширующий) сервер DNS.**
Для уменьшения нагрузки на каналы при разрешении задачи преобразования IP-номера в имя и обратно (услуга DNS) разумно использовать на каждом роутере вторичный DNS-сервер. Это позволит решать задачу преобразования имен в большинстве случаев без обращения к центральному узлу. DNS на роутере занимается только кэшированием данных таблиц преобразования имен на центральном сервере. Кроме разгрузки сети такая организация позволяет увеличить скорость работы DNS-службы;

(13) **Диагностика.**

Роутер должен диагностировать свою работоспособность и работу окрестных узлов. Используются утилиты TCPDump, Ping, TTCP, NetCard, программная часть Watchdog;

(14) **Каскадирование IP-роутеров.**
В случае если количество интерфейсов роутера становится меньше, чем количество подходящих к нему каналов, требуется поставить еще один роутер, но таким образом, чтобы минимизировать затраты. Это делается путем установки компьютера в базовой комплектации, но без винчестера (ведомый роутер), соединенного Fast Ethernet сетью точка–точка с основным (ведущим) роутером. Файловая система ведомого роутера монтируется с ведущего, загрузка его также происходит по сети.

27. Надежность сети

Как уже обсуждалось выше, в условиях города удобно строить сеть небольшими участками. Если предположить, что сеть действительно будет сроиться участками по 100–200 метров, то чтобы покрыть расстояние в 5–10 километров (примерное расстояние внутри небольшого города) придется использовать порядка 50 сегментов. Зададимся вопросом надежности такой сети. Предположим, что надежность одного сегмента равна $p<1$, тогда надежность системы в целом равно $p50$, а это число существенно меньшее единицы. Вероятность отказа такой системы существенно понижается, поэтому лучше для опорной магистрали использовать более длинные пролеты. Кроме того, очевидно, что на опорную магистраль (back bone) ложится основная нагрузка и необходимо увеличить ее пропускную способность, поэтому в СТ «Ботик» используется оптоволокно со скоростью передачи 100 Mbit/c.

В качестве узлов back bone можно использовать IP-роутеры, однако у такого решения ряд основных недостатков: во-первых, каждый роутер добавляет один хоп (*hop* — прыжок, шаг) и убавляет TTL на единицу, тем самым приближая «границу мира» абонента, во-вторых, на каждом роутере решается задача маршрутизации и тем самым время прохождения пакета увеличивается на программную задержку на каждом роутере, в-третьих, при перебоях или некачественном электропитании (ниже или выше нормального), а это достаточно распространенное в небольших городах явление, роутер на время перестает работать и магистраль «разваливается». Установка источника

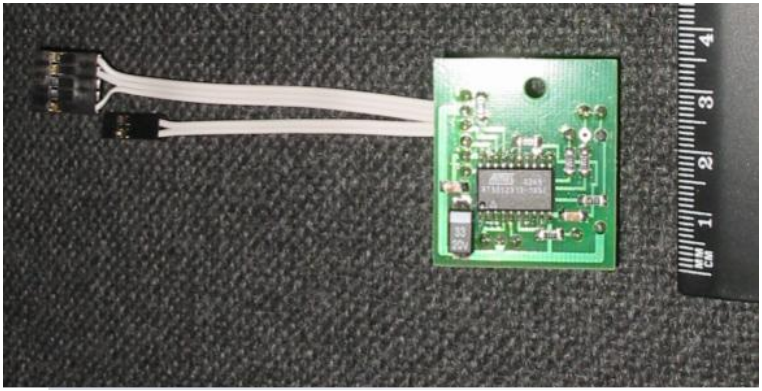

Рис. 26. Новая версия Watchdog (вид снизу)

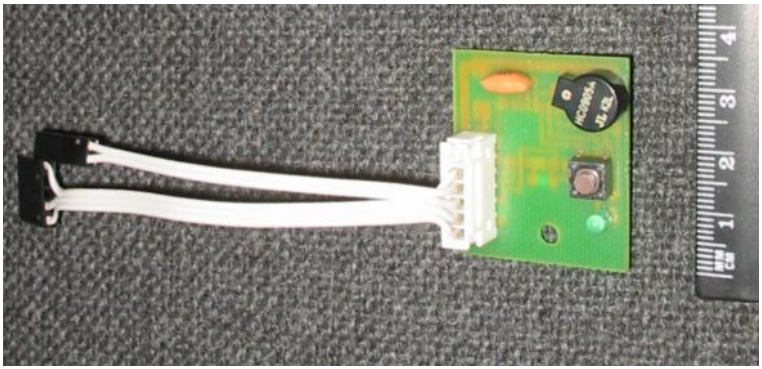

Рис. 27. Новая версия Watchdog (вид сверху)

бесперебойного питания (UPS) данную проблему в нашем случае не решит, так как перерывы в подаче электроэнергии могут составлять до 8 часов, а соответствующий UPS кроме того, что будет крайне дорог, еще и имеет большие габариты, что усложняет его установку. В СТ «Ботик» было найдено решение, позволяющее решить проблему гарантированного электропитания магистрального оборудования.

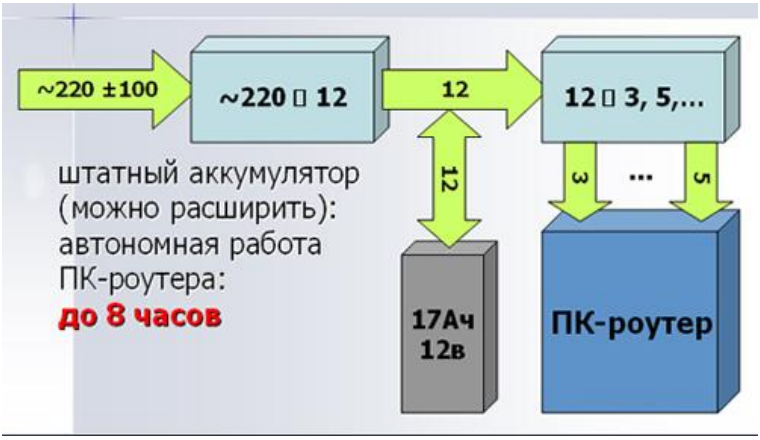

Рис. 28. Блок бесперебойного питания

Прежде всего, вместо роутеров на магистральном уровне были установлены Ethernet switch и необходимое количество трансиверов для преобразования оптоволоконного Ethernet в витопарный, при этом роутеры остались физически на месте, обеспечивая подключение районной подсети к back bone. Очевидно, что устройства типа switch и трансивер гораздо менее энергоемки, чем компьютер (ПК-роутер), и можно было бы использовать стандартный UPS, однако рассмотрим устройство блока бесперебойного питания (Рис. 28).

Видно, что прежде чем питание дойдет до потребителя, оно пройдет через два трансформатора (220 AC * 12 DC; 12 DC * 220 AC), а, учитывая тот факт, что как switch, так и трансиверы потребляют 12 AC, то имеет место третий трансформатор 220 AC * 12 DC. При КПД трансформатора в 80% имеем, что в случае работы от сети до потребителя доходит только порядка 50% мощности (что нестрашно), в случае работы от батареи - порядка 60% (что неприятно, так как энергию хотелось бы использовать более рационально). Из схемы легко понять, что два трансформатора, идущие от батареи к нагрузке являются в данном случае лишними, что и было учтено в изделии, выполненном специалистами СТ «Ботик» и получившем название «*Коммутаторный блок с гарантированным электропитанием*».

Данное устройство представляет собой небольшую коробку, включающее в себя блок питания, switch и 6 слотов для подключения трансиверов. Была достигнута такая характеристика устойчивости, при которой, если в течение 8ми часов в сутки подается электричество, то остальные 16 часов оборудование может работать автономно. Кроме устойчивости с введением описанной технологии удалось достичь: 1) уменьшения количества хопов при прохождении пакета, 2) существенного уменьшения задержки (программная заменена на аппаратную).

28. Организация центрального сервера (узла) региональной сети

Вопрос об организации центрального узла не является надуманным, а есть необходимость для предоставления некоторого набора услуг, которые уже были упомянуты выше. Отметим их еще раз:

В коммерческой сети распространенным решением является покупка серьезного сервера с установленным программным обеспечением, решающим все поставленные задачи, однако такое оборудование и лицензионное ПО достаточно дорого. В нашем случае мы воспользуемся недорогой аппаратурой и свободным программным обеспечением. В качестве сервера разумно взять компьютер, немного превышающий «средний уровень» на текущий момент. Такой средний уровень всегда разный: когда-то это был Pentium100 или Pentium II 400, но всегда выдерживается ценовая граница, «хорошая» машина в каждый момент времени стоит в районе $ 1500.

В качестве особенностей компьютера, выполняющего функции центрального узла, можно отметить высокие требования к оперативной и дисковой памяти и скорости обмена. Необходимы существенные вычислительные возможности процессора, при этом достаточно наличие одного сетевого интерфейса и минимальных графических возможностей. По мере развития региональной сети приходится заниматься модернизацией центрального узла. Возможны два подхода, первый — плановое наращивание, связанное с увеличением объема памяти, количества и вместимости винчестеров, частоты процессора и т. д. Возможна также кардинальная перестройка всего узла, когда обновляется сразу все оборудование. В плане экономии выгоднее идти по первому пути, добавляя к первоначальной стоимости сервера некоторую сумму, тратить снова $ 1500. Также разумным является

DNS	Первичный DNS-сервер, отвечающий за подсеть. Как уже отмечалось, на роутерах полезно иметь вторичные или кэширующие DNS-сервера.
MAIL	Базовый принимающий (POP3) и отправляющий (SMTP) почту серверы.
WWW	HTTP-сервер для предоставления в мир информации о себе
FTP	Сервер хранения пользовательской и общесетевой информации
NEWS	Группы новостей
Proxy Cash	Механизм кэширования web-запросов. Механизм работы следующий: пользователь региональной сети вместо того чтобы напрямую запрашивать внешние ресурсы на свой компьютер, производит запрос Proxy-сервера, который, прежде всего, «смотрит» в свое локальное хранилище запросов, если находит нужную информацию, то проверяет ее актуальность, обращаясь к ори-оригиналу, и если она актуальна, то выдает ее, не обращаясь «наружу», иначе по указанному адресу скачивает требуемую web-страничку, выдает ее пользователю и сохраняет в локальном хранилище. Данный механизм позволяет уменьшить нагрузку на внешний канал, уменьшить задержку при получении часто требующейся информации и снизить стоимость внешнего трафика. В СТ «Ботик» на 2003 год использует Proxy-cash объемом 9Гб.
Мониторинг сети	Проверка работоспособности самого сервера (различных сервисов) и роутеров в сети, нагрузка каналов, занятость модемного пула и т. д.

Таблица 3. Услуги центрального сервера

использование нескольких машин для организации центрального узла, поделив между ними исполняемые сервисы.

29. Модемный пул

Зачастую требуется использование не только постоянного подключения, но и модемного соединения. Вопрос о модемных подключениях уже частично обсуждался, но остановимся на нем еще раз. Как обычно, создание модемного пула возможно за счет использования законченных решений, которые достаточно дороги или при помощи широко распространенного оборудования, приспособленного для решения требуемых задач. Используется ПК-роутер, к которому по COM-портам подключаются модемы, однако в стандартной поставке количество таких портов невелико: от 2-х до 4-х. Существуют мультипортовые платы, добавляющие 8 или 16 COM-портов, однако их стоимость достаточна велика: порядка $ 500 за 16-портовую плату во время становления СТ «Ботик». Были проведены разработки по созданию собственной мультипортовой платы на 16 COM-портов, весь цикл разработки и производства оказался дешевле, чем покупка готового оборудования.

После комплектации ПК-роутера описанной платой расширения, к нему подключается требуемое количество модемов. На АТС также полезно получить поддержку в виде группового номера (т. е. одного номера на несколько линий). Смысл такого решения в следующем: каждый модем имеет свой собственных телефонный номер, однако можно выделить некоторый общий номер, звоня по которому, оборудование АТС последовательно пытается соединить абонента с одним из свободных модемов. Отказ (короткие гудки) происходит только в случае, если все линии заняты. Таким образом, абоненту нужно запомнить только один номер, а оборудование автоматически обнаружит для него свободную линию.

30. Внешние каналы

Внешние каналы, как правило, покупаются у провайдеров, расположенных на данной территории. Физически каналы можно разделить на наземные и спутниковые (двусторонний и односторонний каналы). Наземные каналы покупаются в виде телефонной или цифровой линии, связанной с провайдером, и неважно, как приходит канал к точке подключения. Спутниковый двусторонний канал состоит из спутника, антенны и спутникового модема.

Спутник работает в данной системе как ретранслятор, покрывающий большую территорию, принцип работы этого способа передачи поход на Ethernet. Чтобы не происходило коллизий, для каждого абонента выделяют свою полосу в частоте вещания, и каждый абонент настроен на свою частоту. Спутник получает все сигналы от всех абонентов, усиливает их и ретранслирует на большую территорию. Подобная схема позволяет быстро развертывать систему связи на большой территории. Как правило, используются стационарные спутники. Такие спутники делают оборот вокруг Земли за одни сутки, и получается, что для наблюдателя с Земли они «висят» над одной точкой. Плюс к тому, спутник должен находиться точно в экваториальной плоскости и иметь круговую орбиту, чтобы на наблюдателя не было колебаний, и оборудование не приходилось подстраивать. Средний радиус орбиты спутника порядка 36–40 тысяч километров. Недостаток такой связи очевиден: большое расстояние (порядка 70–80 тыс. километров в обе стороны), что составляет примерно 0,25 секунды для сигнала, плюс аппаратные задержки, поэтому среднее время прохождения «космического» хопа — это 0.5–0.6 секунды. Второй недостаток - очень дорогое оборудование и его сложная настройка.

31. Механизмы управления трафиком

При рассмотрении тех или иных аспектов построения и эксплуатации региональной сети мы уже обращали внимание на проблемы, связанные с эффективным использованием ресурсов и возможностями их расширения в случае необходимости. Отметим, что ресурсы можно подразделить на два больших типа:

(1) легко расширяемые, некритичные ресурсы (вроде дискового пространства на сервере или пропускной способности внутренних каналов, которые хоть и не так просто, но поддаются расширению за разумные деньги);
(2) лимитирующие ресурсы, то есть их расширение связано с большими сложностями, зачастую упирающиеся в серьезные финансовые затраты (пропускная способность внешнего канала).

Прежде мы рассматривали лишь некритичные ресурсы и обозначали способы их использования и расширения, теперь обратим внимание на такой ресурс как внешний канал и перечислим ряд способов решения задач его эффективного использования. Как в юбом

другом вопросе, тут есть два принципиальных подхода к его решению: высокозатратный и малобюджетный. В первом случае можно сделать многократный запас коннективности внешнего канала и расширять его при возникновении такой необходимости. Подобный экстенсиональный подход избавляет от изобретения сложных схем, но экономически неприемлем. Второй вариант — иметь небольшой запас ресурса внешнего канала, но добиваться его эффективного использования, вводя некоторые ограничения на работу пользователей в часы пиковой нагрузки, предохраняя тем самым сеть от перегрузки и выхода из строя. Такой способ скорей всего является наиболее отвечающим требованиям региональной сети, содержащейся за счет общины. Однако здесь придется решать немало задач, связанных со справедливым распределением ресурсов. Какие же пути решения поставленной задачи можно выделить?

31.1. Ограничение пользователей на входе в сеть. Идея данного подхода состоит в том, что естественным[18] или искусственным[19] путем ограничивается доступ пользователей к ресурсу (здесь и далее в качестве разделяемого ресурса будем иметь в виду пропускную способность внешнего канала).

Данный способ имеет тот недостаток, что не в полной мере используются ресурсы сети в том случае, когда ресурса достаточно, но в силу ограничений пользователь не имеет возможности эффективно его использовать.

31.2. Разделение ресурса. Возможно такое решение проблемы, в котором каждому пользователю (в случае их небольшого количества) предоставляется некоторый объем ресурса, который он самостоятельно использует и оплачивает. Данную политику ведет провайдер Runnet, выделяя своим клиентам персональный канал.

Минусами такого подхода, как и в предыдущем случае, является недоиспользование имеющихся ресурсов. Не исключено возникновение ситуации, когда кто-то канал не использует, а сосед задыхается от недостатка пропускной способности. Но вместе с тем при данном способе более или менее справедливо распределяется оплата за ресурс.

---

[18] Например, предел пропускной способности телефонной сети.

[19] Установка фильтров на роутере.

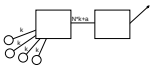

Рис. 29. Стратегия ограничения пользователей на входе в сеть

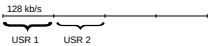

Рис. 30. Стратегия разделения ресурса между пользователями

+	- Высокий
0	- Общий
-	- Низкий

Рис. 31. Сетка приоритетов на использование ресурса

31.3. Разделение времени. Подход отличается от предыдущего тем, что каждому пользователю предоставляется весь ресурс и ограничением является лишь работа другого пользователя, конкурирующего за ресурс. При таком подходе естественно возникают следующие подзадачи:

(1) справедливое разделение ресурса между внутренними пользователями;
(2) разделение ресурса между внутренними и внешними пользователями;
(3) построение системы приоритетного обслуживания для удовлетворения запросов клиента;
(4) учет использования ресурса и оплата трафика.

Перечисленные задачи технически во многом решаются на уровне управления очередью запросов на обработку сервером. Очевидно, чтобы создать более или менее гибкую систему, обычной FIFO-очереди будет недостаточно, так как придется решать задачу расстановки приоритетов. Предположим, мы устанавливаем следующую сетку приоритетов:

Исходя из предложенной структуры, каждый пользователь может, оценив свои задачи, решаемые в сети, и финансовые ресурсы, в каждый момент времени определять свое место в данной таблице. От его выбора буде зависеть скорость его работы и соответственно оплата за трафик. Причем игра с приоритетами является исключительно игрой между пользователями за трафик, а не способом наживы для провайдера, так как в случае выбора всеми пользователями какой-либо одной стратегии, их права и оплата соответственно выравниваются и в сумме равняются стоимости канала. Такая схема позволяет дать изначальный приоритет внутреннему пользователю (который платит) перед внешним (который не платит), поместив внешнего пользователя на самый низкий приоритет.

Итак, каков же механизм реализации такой задачи? В последних пакетах ОС Linux уже существует встроенная возможность подобного регулирования трафика — Linux Traffic Control. Рассмотрим несколько подходов решения данной задачи.

31.4. Очередь с приоритетами. Такой тип очереди является расширением FIFO и содержит несколько очередей, по одной для каждого типа пользователей из приоритетной сетки. Схематически очередь с приоритетами можно изобразить следующим образом:

Механизм работы такой конструкции следующий: запросы от каждой группы пользователей устанавливаются в соответствующую очередь, причем, чем выше приоритет, тем выше эта очередь на картинке. Далее обработка происходит сверху вниз, то есть сначала обрабатываются все запросы, стоящие в верхней очереди, если она пуста, то берутся запросы из нижних очередей и так далее. Видно, что в данном случае соблюдается система приоритетов пользователя, и он получает больше ресурса. Однако в таком чистом виде эту схему использовать не очень удобно, так как у нижних очередей слишком мало шансов вообще дождаться обработки, при этом деньги ими заплачены, и «товар должен быть отгружен». Здесь нам нужно дать каждой очереди право на использование лишь какой-то части ресурса, не захватывая его целиком. Так, для приоритетной очереди, например, можно задать использование лишь максимум 60% канала, а остальные ресурсы распределить между остальными пользователями.

Итак, предположим, нам удалось установить нужную систему приоритетов, но наш канал слишком «узок» и не позволяет пропускать всего трафика, либо нам надо разделить канал между пользователями (как в предыдущем случае). Тогда можно воспользоваться алгоритмом ограничения скорости передачи информации, получившего название алгоритм «дырявого ведра». Суть его в следующем: внешний поток запросов помещается в некоторую ограниченную очередь, обработка запросов, в которой происходит не полностью, а с некоторой заданной интенсивностью. Смысл процесса хорошо иллюстрируется на Рис. 33.

31.5. Иерархические очереди. На основе принципа деления трафика между пользователями строится следующий тип очереди CBQ (Class Based Queueing). Выстраивается иерархия деления канала между пользователями, плюс к тому каждый пользователь имеет

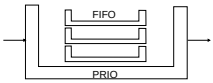

Рис. 32. Очередь с приоритетами

Рис. 33. Алгоритм «дырявого ведра»

возможность внутри своей «части» канала выставлять приоритетность тех или иных сетевых задач, как то: www, telnet, mail и т. д. в зависимости от их важности для пользователя. Схематически данный подход может выглядеть так:

Таким образом, мы пришли к возможности пропорционального деления ресурса не только между пользователями, но и между классами трафика. Это позволяет предоставить пользователю большую гибкость в работе с сетью и ее оплате.

31.6. Поддержка финансовой деятельности региональной системы телекоммуникаций. Мы уже обсуждали, что при построении сетей государственная поддержка, скорей всего, будет оказана для построения уровня национальной магистрали, а не для создания региональных подсетей. В силу этого не остается ничего иного, как использовать те финансовые ресурсы, которые есть у жителей и предприятий региона, которые весьма невелики. Отсюда мы приходим к выводу, что используемые при построении сети решения должны быть, прежде всего, экономически эффективными и далее необходимым требованием является наличие механизмов, обеспечивающих как минимум самоокупаемость данного предприятия. Мы будем различать две стороны этого вопроса: 1) самоокупаемость на этапе создания и развития сети, 2) покрытие эксплуатационных расходов.

32. Этап создания и развития сети

При создании рассмотренная система способна развиваться инкрементно: если через некоторый дом проходит сеть, а в соседнем доме появился клиент, желающий подключиться, то требуется «дотянуть» магистраль до указанной точки и подключить абонента. Несмотря на то, что узлы сети бывают разные (хабы, свичи, роутеры) и используются разные каналы (коаксиал, витая пара, оптоволокно), которые, естественно, имеют различную стоимость, средняя стоимость подключения остается примерно одинаковой за счет большого количества абонентов. В среднем стоимость «прохода» от одного дома до следующего равняется $ 108 (данные получены в результате акции «Ботик 2000», когда было подключено 50 новых домов).

Стоимость абонентского окончания от уже установленного оборудования до компьютера внутри дома в среднем равняется $ 42. Итого, в среднем себестоимость одного подключения составляет порядка

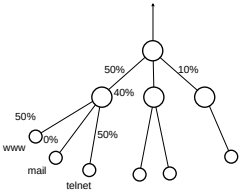

Рис. 34. Иерархические очереди

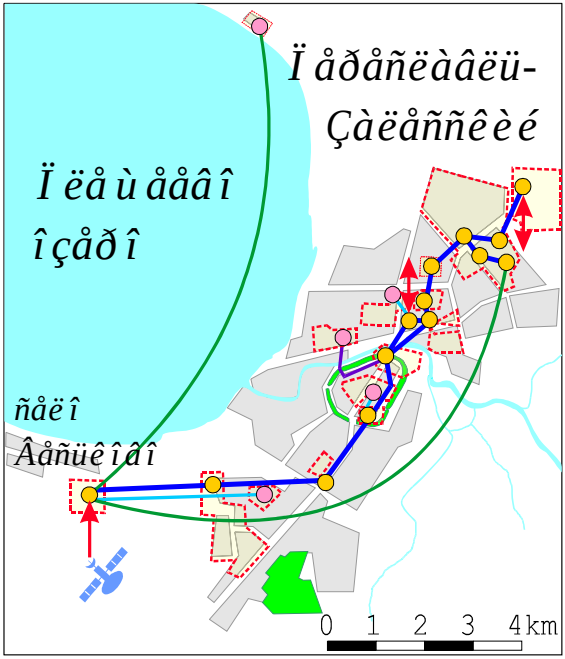

Рис. 35. Карта Переславской сети

$ 150 с учетом того, что в одном доме может быть несколько подключений, а в другом не будет ни одного, но оборудование туда должно быть поставлено. Для прокладки и эксплуатации оптоволоконной магистрали СТ «Ботик» сотрудничает со сторонними организациями, по договору с которыми с каждого нового подключения делается отчисление в $ 40. Итоговая стоимость подключения равняется $ 190. Если магистраль уже есть в доме, то новый абонент не освобождается от оплаты $ 108 за отрезок магистрали, но имеет право на рассрочку в платеже. Предложенные выкладки являются основой самоокупаемости на этапе создания и развития сети и зафиксированы в регламентирующих документах.

33. Этап эксплуатации сети

В процессе эксплуатации сети можно выделить две части расходов:

(1) *содержание внутренней сети:*
- выполнение ремонта оборудования;
- содержание системы;
- заработная плата персоналу, поддерживающему ее работоспособность. В настоящее время переславскую региональную сеть обслуживают 1 системный программист, 1 электронщик-разработчик, 2 электронщика, 2 монтажника и 1 инженер по металлу, кроме того, персонал, работающий с клиентами (4 человека), 1 бухгалтер и 1 руководитель;

(2) *содержание внешних подключений:*
- оплата услуг провайдеров (стоимость внешних каналов);
- оплата внешней коннективности, возникающая за счет того, что существуют выходы сети во внешний мир: отчисления Госсвязьнадзору, оплата доменных имен, оплата стоимости телефонных подключений и т. д.

Определим принципы взаиморасчетов с абонентами. Будем считать, что за работу во внутренней сети абонент платит фиксированную плату без учета времени и трафика — абонентскую плату, которая рассчитывается с учетом того, чтобы она покрывала расходы на содержание внутренней сети. Кроме того взимается оплата трафика для покрытия затрат на внешнюю коннективность. Нередко провайдер определяет стоимость мегабайта внешнего трафика некоторой

суммой, однако в случае, если сеть не коммерческая, когда канал покупается вскладчину всеми абонентами, более приемлем иной принцип. Оцениваются расходы на внешние каналы за месяц и делятся на общий внешний трафик всех абонентов, получается средняя стоимость мегабайта за расчетный период. Абонент платит за этот период сумму, равную произведению средней стоимости мегабайта и объема своего внешнего пользовательского трафика. Отметим, что кроме пользовательского существует системный трафик, связанный с обеспечением жизнедеятельности сети в целом (работа Proxy, DNS, и др.).

Такой механизм взимания оплаты соответствует принципу бесприбыльности построенной в Переславле региональной сети. Региональная сеть в таком виде представляет собой общину, которая сообща оптом покупает внешний канал, что выходит существенно дешевле, чем если бы каждый выходил на провайдера самостоятельно, так как начинают действовать оптовые цены. Кроме того, описанный помегабайтный принцип оплаты позволяет (в отличие от фиксированной платы) сдерживать аппетиты пользователей и укладываться в существующих емкостях внешних каналов. Такая экономическая обратная связь сдерживает систему от перегрузок.

34. Система сетевого администрирования Nadmin

Для обслуживания финансовых потоков, расчета услуг абонентам, ведения договоров и т. д. требуется соответствующее ПО. В СТ «Ботик» указанную (и немало другой) функциональность обеспечивает **система Nadmin** (*Network Administration*).

34.1. Структура Nadmin:

(1) **Датчики, являющиеся источниками статистики:**
a) IP-трафик. Собирается IP-статистика на пограничных роутерах (тех, через которые происходит связь с внешним миром) в виде TCP-dump, т. е. всех проходящих через него пакетов, обрабатываются (отрезаются только заголовки пакетов и выбрасывается содержимое) и сжимаются;
b) MAIL-трафик. Берется из лог-файлов mail-сервера;
c) Proxy-трафик. Берется из лог-файлов proxy-сервера;
d) WWW-аренда. Считается сумма размеров каталогов. Все данные содержатся в архивированном виде в хранилище в

течение некоторого времени для возможности разбора спорных вопросов, после его истечения происходит удаление наиболее старых архивов;

(2) **База данных системы:** *a) Абоненты.* Абонентом является физическое или юридическое лицо, заключившее договор на обслуживание. В базе хранится контактная информация о клиенте, а также его лицевой счет, т. е. остаток денежных средств после внесения авансового платежа. Абонент ассоциируется с его учетным именем;
b) Услуги. Перечень услуг, которые могут быть предоставлены абоненту в рамках договора;
c) Подсети. Рассматриваются IP-подсети, с ними ассоциируются атрибуты подсети, такие как шлюз, маска, номер подсети;
d) Цены. Объект позволяет рассчитать стоимость услуги для абонента, так как вычисление ее стоимости зависит от категории пользователя (специальной метки, ассоциируемой с абонентом). В базе данных используется принцип историчности хранения информации, то есть сохраняются все состояния базы на любой момент времени и можно узнать значения любых показателей в любой момент. Обсчет стоимости услуг абонентов за период происходит путем поочередного перевода состояния базы на некоторый день, обсчет этого дня, затем база переводится на следующий день и т. д.;

(3) **Функциональные блоки системы:**
a) Обработка статистики;
b) Генерация отчетов;
c) Хранение и чистка сгенерированных отчетов;
d) Расчет стоимости услуг;

(4) **Web-интерфейсы к системе:**
a) Интерфейс администратора:
— Печать договоров из счетов;
— Изменение в абонентах и услугах;
— Прочие модификации системы;
b) Интерфейс пользователя:
— Просмотр истории расчетов с абонентом;
— Просмотр текущей статистики абонента;
— Просмотр сводной статистики по всем абонентам.

Вся указанная система написана «с нуля», ее объем приблизительно равен 10000 строк на языке *Perl*. Несмотря на то, что она писалась под собственные нужды, система была неоднократно установлена в других регионах, характеризующихся своими принципами ценовой политики, отчетов, договоров и т. д. Отметим некоторые из использованных программистских решений при создании разных модулей Nadmin.

34.2. База данных. В качестве базы данных используется система плоских файлов, управляемая VCS (*Version Control System*) — системой управления версиями. Для получения вида файлов на определенную дату происходит средствами VCS приведение версий файлов на указанную дату и затем производится обсчет. Такое решение позволяет «бесплатно» получить требуемую функциональность и повысить устойчивость системы от взлома и некорректного ввода данных, так как VCS ведет аудит (лог-файлы) выполняемых операций.

34.3. Вычисление стоимости. В механизме расчета стоимости услуг в качестве цены за мегабайт используется не конечное значение, а формула, которая в зависимости от политики провайдера может иметь тот или иной вид. Так в СТ «Ботик» — это процедура типа «получить полную стоимость каналов и разделить на объем абонентского трафика», а в другом случае может стоять просто фиксированная величина. Кроме этого, по-разному может вычисляться величина абонентской платы, например, использование кроме категории пользователя тарифного плана и т. д.

34.4. Печать отчетов. В случае если отчет требуется выдать в виде HTML-страницы, то это несложно, однако требуется иметь и строгие печатные формы, причем управление печатью должно происходить из WEB-формы. В системе Nadmin для этих целей используется полиграфическая система LaTeX. На основании информации из базы данных формируется LaTeX-документ, который компилируется, и созданный PostScript-файл отправляется на принтер.

34.5. Управление сетью. Для эффективного взаимодействия с пользователями требуются частые небольшие модификации системы. Например, если абонент задолжал и имеет отрицательный платежный баланс, то его следует отключить от сети, чтобы он еще более не усугубил свое положение. В случае, если данный абонент имеет не одно, а несколько подключений, которые идут к разным роутерам,

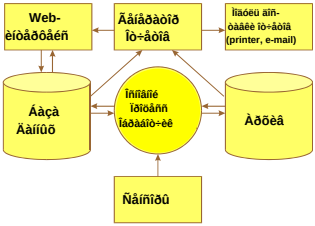

Рис. 36. Структура системы Nadmin

то придется поставить фильтрацию пакетов абонента на каждом из узлов его подключения к сети.

Все это требует времени системного администратора, труд которого оплачивается дорого, и если бы все подобные действия выполнялись вручную, то пришлось бы держать приличный штат администраторов, что увеличило бы эксплуатационные расходы. Было бы разумно автоматизировать возможно большее количество понятных и рутинных операций, возложив их выполнение на систему. В приведенном примере по отключению пользователя все перечисленные действия по изменению конфигурации роутеров производятся программно после получения сигнала по включению/отключению пользователя от сети.

Другой пример модификации состояния сети — подключение нового пользователя. Это достаточно сложное событие, которое связано с выделением IP-номера, маски подсети, шлюза, соответствующего физическому местоположению вновь подключаемого компьютера. Если договор подразумевает выделение почтового ящика, то требуется создать соответствующий почтовый account и сгенерировать пароль и т. д. В Nadmin эти действия автоматизированы, и их выполняет неподготовленный персонал, указав желаемое имя абонента и выбирая из списка нужную подсеть.

35. Темы рефератов-I

(1) Предпосылка зарождения компьютерных сетей. Сравнение 2-х способов передачи информации от компьютера к компьютеру:
   (a) физическое перемещение машинного носителя;
   (b) передача по каналам связи.
(2) Общая характеристика UUCP.
(3) Адресация и маршрутизация в UUCP-сетях.
(4) Сетевые приложения, основанные на UUCP, и их характеристики.
(5) Служебные строки электронного письма и их предназначение.
(6) Организация пересылки сообщений сразу многим адресатам в сети UUCP.
(7) Качественное сравнение UUCP-сетей и TCP/IP-сетей, основные идеи и технические решения при переходе от UUCP к TCP/IP.

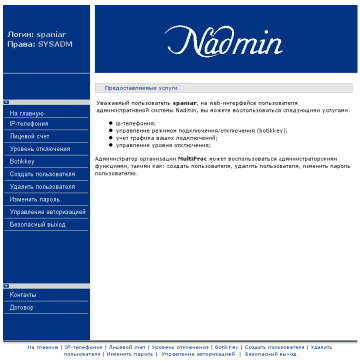

Рис. 37. Внешний вид системы Nadmin

(8) IP-адреса; IP-подсети, алгоритмы проверки вхождения IP-номера в подсеть, алгоритм IP-маршрутизации (при заданной таблице маршрутизации).
(9) DNS. Организация преобразования IP-номера в доменное имя машины и обратно.
(10) Делегирование блоков IP-номеров. Делегирование доменов. Проблемы, решаемые такими делегированиями. Использование сервиса WhoIs (назначение, примеры использования).
(11) Алгоритмы маршрутизации (алгоритмы построения таблиц маршрутизации).
(12) Сети Etherner. Общие принципы передачи данных в разделяемых сегментах Etherner. Mac-адреса.
(13) Ограничение на размеры разделяемого Etherner-сегмента. Причины возникновения ограничений на число абонентов и на физические размеры.
(14) Архитектура Etherner-сегментов: 10Base-2, 10Base-T. Правило 4-х хабов.

36. Темы рефератов-II

(1) Кабель витой пары, устойчивость витой пары к помехам, типы кабелей витой пары.
(2) Объединение сегментов сети Ethernet при помощи роутеров и при помощи коммутаторов.
(3) Устройство и принципы работы коммутатора Ethernet.
(4) Организация каналов в региональных сетях: использование кабелей витой пары и коаксиальных кабелей.
(5) Организация каналов в региональных сетях использование: оптоволоконных кабелей.
(6) Организация каналов в региональных сетях: использование устройств RadioEthernet.
(7) Организация каналов в региональных сетях: сравнение различных технологий и области применимости.
(8) Узлы региональной сети (хабы, коммутаторы, роутеры), их сравненоие между собой (сильные и слабые стороны), области применения. Стоимость изделий.
(9) Устойчивость PC-роутера к внезапной перезагрузке: зачем это надо и как это обеспечивается.

(10) Самоконтроль за работоспособностью и самовосстановление PC-роутера после сбоя или после отказа: зачем это надо и как это обеспечивается. Watchdog.
(11) Основные функции PC-роутеров: что и зачем реализовано.
(12) Центральный сервер для городской компьютерной сети. Аппаратура, функции и их реализация.
(13) Внешние каналы городской компьютерной сети — различные решения и их сравнение.
(14) Модернизация городской оптоволоконной сети в г. Переславле-Залесском в 2001 г.; какие проблемы и как были решены.
(15) Общие принципы обеспечения самоокупаемости городской сети телекоммуникации и их поддержка в системе Nadmin.
(16) Функции сетевого администрирования в системе Nadmin.
(17) Общая архитектура системы Nadmin. Использование свободного ПО в реализации системы Nadmin.

37. Вопросы для самоконтроля

(1) Дайте определение характеристики передачи информации: задержка — это ...
(2) В чем состоит доменный принцип именования компьютеров — разберите на примере какого-нибудь имени.
(3) Дайте определение IP-адреса и сравните его с UUCP-адресом.
(4) Напишите маску для подсети 83.149.128.128/25 (в двоичной и в десятеричной моде).
(5) Динамическая маршрутизация неэффективно борется с отказами оборудования при следующей топологии сети: ...
(6) Активный хаб делает следующее: ...
(7) Для 10Base-T достаточно ... пар в кабеле TP.
(8) Напишите маску для подсети 83.149.128.0/21 (в двоичной и в десятеричной моде).
(9) Поздняя коллизия — это: ...
(10) Ранняя коллизия — это: ...
(11) Элементы региональной сети. В качестве линии связи применяются: ...
(12) В UUCP «spool» — это: ...; «spooling» — это: ...
(13) Напишите маску для подсети 83.149.206.0/27 (в двоичной и в десятеричной моде).
(14) HUB — это ... (объяснить назначение слова и устройства).

(15) Switch отличается от hub'а следующим: ...
(16) Элементы региональной сети. В качестве узлов применяются: ..., ... и ...
(17) В UUCP «hand-shaking» — это: ...
(18) Напишите маску для подсети 83.149.128.128/26 (в двоичной и в десятеричной моде).
(19) Пусть X — IP-адрес, A — адрес подсети, M — маска подсети. Условие: «X находится в подсети (A, M)» вычисляет следующее выражение: ...
(20) Буквами SFTP обозначают следующее изделие: ...
(21) Буквы сокращения TTL означают: ...
(22) Switch похож на hub тем, что: ...
(23) Для организации передачи Ethernet по волоконно-оптическим линиям связи часто используется следующее изделие: ...
(24) Основные функции центрального узла региональной сети.
(25) Недостатки статической маршрутизации.
(26) Коллизии в Ethernet-сети — это: ...
(27) Буквами FTP обозначают следующее изделие: ...
(28) В каких случаях надо применять экранированный, а в каких — неэкранированный кабель витой пары?
(29) Почему России нужна компьютерная сеть, объединяющая всех жителей и все организации?
(30) Региональную сеть надо строить без сетевой политики — «сеть для всех», — и на это есть экономические причины: ...
(31) Дайте определение IP-подсети, сравните ее с UUCP-подсетью.
(32) Напишите маску для подсети 83.149.205.64/28 (в двоичной и в десятеричной моде).
(33) Динамическая маршрутизация обычно применяется в следующих случаях: ...
(34) В Ethernet-сети возможны коллизии по следующей причине: ...
(35) Буквами STP обозначают следующее изделие: ...
(36) Для чего перевивают между собой провода в витой паре? (Два эффекта)
(37) В оптоволокне световой сигнал не покидает волокно и при этом почти не затухает за счет того, что ...

(38) Дайте определение: задача маршрутизации — это ...
(39) Дайте определение IP-адреса и сравните его с UUCP-адресом.
(40) Напишите маску для подсети 83.149.205.0/30 (в двоичной и в десятеричной моде):
(41) Статическая маршрутизация обычно применяется в следующих случаях: ...
(42) Буквами UTP обозначают следующее изделие: ...
(43) Предназначение системы Nadmin.
(44) В чем состоит доменный принцип именования компьютеров — разберите на примере какого-нибудь имени.
(45) Напишите маску для подсети 83.149.205.128/29 (в двоичной и в десятеричной моде).
(46) У MAC-адреса следующий формат: ...
(47) В обозначении 10Base-T буква «T» означает: ...
(48) Можно ли в сети связать кольцом (для повышения надежности передачи) два хаба? (Да/нет? Почему?)
(49) Что содержит forwarding table коммутатора после включения питания?
(50) Расходы на содержание внешней коннективности включают в себя: ... + ...
(51) Буквы в сокращении TCP/IP означают: ...
(52) Напишите маску для подсети 83.149.205.64/28 (в двоичной и в десятеричной моде.
(53) Сколько (примерно) существует различных IP-номеров? На сколько лет хватит этого «запаса» номеров? Для справки: на Земле 6 млрд. жителей.
(54) Правило 4-х хабов состоит в следующем: ...
(55) Каким образом заполняется forwarding table коммутатора?
(56) Расходы на содержание внутренней сети: (описать две группы расходов).
(57) В сокращении UUCP буквы означают: ...
(58) Напишите маску для подсети 83.149.205.128/27 (в двоичной и в десятеричной моде.
(59) DNS-кэширование решает следующие проблемы: ...
(60) Вместо коммерческого программного обеспечения в региональных сетях широко используется ... и ...
(61) В ПК-роутере динамическая маршрутизация используется для обеспечения ...

(62) Дайте определение характеристики передачи информации: пропускная способность канала — это ...
(63) Дайте определение характеристики передачи информации: надежность передачи — это ...
(64) Дайте определение понятия: протокол передачи данных — это ...
(65) Что означает в электронном письме поле «Cc»?
(66) Что означает в электронном письме поле «Bcc»?
(67) Почему России нужна компьютерная сеть, объединяющая всех жителей и все организации?
(68) Почему в региональных сетях следует отказаться от коммерческого программного обеспечения? (Указать причины.)
(69) По-английски HUB, а по-русски — ...
(70) По-английски switch, а по-русски — ...
(71) Буквы в сокращении «DNS» означают: ...
(72) При помощи службы WhoIs можно получить следующую информацию: ...
(73) Как устроен магистральный кабель и как устроен кабель patchcord?
(74) Геостационарный спутник — укажите параметры орбиты: плоскость, тип орбиты, физические размеры.
(75) База данных Nadmin является ретроспективной, что означает ...
(76) Генерация печатных отчетов в системе Nadmin и их непосредственная печать осуществляется при помощи программы ...
(77) UUCP-сеть часто изображают в виде неполного графа. В нем: узлы — это ..., ребра — это ...

38. Терминологический словарь

Back bone (скелет, остов): опорная магистраль.

BCC (Blind Carbon Copy — слепая копия): список получателей без уведомления других получателей о существовании данных получателей.

CC (Carbon Copy — машинописная копия): список адресатов, которые должны быть в курсе данного письма, причем основные получатели также видят, что копия отослана по указанным в CC адресам.

Collision domain: обнаружение одновременной передачи, коллизии

Ethernet:

MAC-адрес:

Offline-режим:

Online-режим:

Smurf:

Switch (или Bridge): устройство для соединения сегментов сети или локальных сетей между собою

Switching hub:

Shared Ethernet: режим с разделением канала

TO: список прямых адресатов, перечисленных через разделитель — адреса персон, от которых ожидается получить отклик.

UNIX:

UUCP: первый протокол передачи данных (UNIX to UNIX Copy Protocol (Program))

Watchdog: сторожевое устройство, спомощью которого осуществляется аварийная перезагрузка PC-Роутера.

Буферизация задачи (spooling) в UUCP:

Домен:

Задержка (latency):

Кабель UTP (Unshielded Twisted Pair): неэкранированная витая пара

Кабель FTP (Foiled Twisted Pair): фольгированная витая пара

Кабель STP (Shielded Twisted Pair): экранированная витая пара

Кабель SFTP: дважды экранированный кабель.

Концентратор: то же, что и хаб.

Локальная сеть:

Патчкорд: пользовательское окончание сети.

Провайдер: организация, занимающаяся предоставлением услуг доступа в Интернет.

Протокол передачи данных: это согласованный набор сообщений и форматов сообщений, позволяющий компьютерам обмениваться информацией.

Сетевая атака: несанкционированный доступ к ресурсам Сети, компьютерный взлом с подбором пароля, уничтожение или порча ресурса Сети.

Сеанс связи:

Скорость передачи (bandwidth): , пропускная способность или ёмкость канала

Служба новостей (News):

Спам: несанкционированная массовая рассылка по электронной почте рекламы членам сетевого сообщества.

Таблица маршрутизации UUCP:

Хаб (от англ. hub — центр, концентратор): сетевой аппаратный узел, к которому подключаются все компьютеры в сети топологии «звезда», также называется повторитель, репитер.

Электронная почта:

. *Networks* .

().