

Министерство образования и науки Российской Федерации
Государственное образовательное учреждение
высшего профессионального образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

*КОМПЛЕКСНАЯ ЗАЩИТА
ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ*

КНИГА 21

А. А. ВОРОНИН

ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Учебное пособие



Владимир 2011

УДК 004.7
ББК 32.97
В75

Редактор серии – доктор технических наук,
профессор М. Ю. Монахов

Рецензенты:

Кандидат технических наук, профессор
зав. кафедрой информатики и вычислительной техники
Владимирского государственного гуманитарного университета
Ю. А. Медведев

Доктор технических наук, профессор
Владимирского государственного университета
О. В. Веселов

Печатается по решению редакционного совета
Владимирского государственного университета

Воронин, А. А.

В75 Вычислительные сети : учеб. пособие / А. А. Воронин ; Вла-
дим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2011. –
88 с. (Комплексная защита объектов информатизации. Кн. 21).
ISBN 978-5-9984-0179-4.

Представлен систематизированный материал о компьютерных сетях, принципах их проектирования, реализации и эксплуатации. Приводятся рекомендации к практическим и лабораторным занятиям, контрольные вопросы.

Предназначено для студентов специальности 090104 «Комплексная защита объектов информатизации» дневной формы обучения, а также может быть полезно студентам других специальностей, в том числе и дистанционной формы обучения, и широкому кругу читателей, самостоятельно осваивающих вычислительные сети.

Табл. 10. Ил. 32. Библиогр.: 8 назв.

УДК 004.7
ББК 32.97

ISBN 978-5-9984-0179-4

© Владимирский государственный
университет, 2011

ПРЕДИСЛОВИЕ

Многие организации используют большое количество компьютеров, зачастую значительно удаленных друг от друга. Поначалу эти компьютеры нередко работают изолированно друг от друга, однако в какой-то момент руководство организации может принять решение объединить их, чтобы иметь возможность быстрого и оперативного доступа к информации в пределах компании и удаленного доступа за ее пределами.

Если посмотреть на эту проблему с более общих позиций, то основным вопросом является совместное использование ресурсов, а целью – предоставление доступа к программам, оборудованию и данным любому пользователю сети, независимо от физического расположения ресурса и пользователя.

В наше время любая компания независимо от ее размеров просто немыслима без данных, представленных в электронном виде. Большинство фирм старается вести базу данных клиентов, товаров, счетов, финансовых операций, очень часто требуется налоговая информация и многое другое.

В маленьких компаниях все компьютеры обычно собраны в пределах одного офиса или, по крайней мере, одного здания. Если же речь идет о больших фирмах, то и вычислительная техника, и служащие могут быть разбросаны по десяткам представительств в разных странах.

Тот факт, что пользователь удален от физического хранилища данных на тысячи километров, никак не должен ограничивать его возможности доступа к этим данным.

Проще всего информационную систему компании представить как совокупность одной или более баз данных и некоторого количе-

ства работников, которым удаленно предоставляется информация. В этом случае данные хранятся на сервере. Довольно часто сервер располагается в отдельном помещении и обслуживается системным администратором.

Компьютеры работников идентифицируются в сети как клиенты и могут иметь удаленный доступ к информации и программам, хранящимся на сервере.

Работа компьютерной сети связана в большей степени с людьми, чем с информацией или вычислительными машинами. Ранние сети передачи данных были ограничены посимвольной передачей данных между соединенными компьютерными системами. Современные сети эволюционировали до сетей, обеспечивающих передачу голосовой, видеоинформации, текста и графики между множеством устройств различного типа, что позволяет людям взаимодействовать непосредственно друг с другом практически мгновенно.

Важным применением компьютерных сетей является возможность электронного делового общения с другими компаниями. Особенно это касается взаимоотношений типа «поставщик – клиент». С помощью компьютерных сетей процесс составления и отправки заказов можно автоматизировать. Более того, заказы могут формироваться строго в соответствии с производственными нуждами, что позволяет резко повысить эффективность.

Сети передачи данных, используемые ранее для обмена информацией в коммерческом секторе, сегодня переориентируются на улучшение качества жизни. Это электронная коммерция, банковские услуги, консультации экспертов, средства совместной работы.

Средства общения дают возможность студентам сотрудничать с преподавателем, другими студентами в классе или другими студентами по всему миру. Смешанные курсы позволяют объединить плюсы очного и дистанционного обучений. Доступ к высококвалифицированным преподавателям более не ограничен для студентов, которые не имеют возможности личного контакта.

Компьютерные сети получили широкое распространение в сфере развлечений и индустрии туризма. Способствовало этому появление и

развитие Интернета. Интернет дает возможность увидеть места, которые вы хотели бы посетить. Владея этой информацией, вы можете лучше спланировать свою поездку.

Интернет также используется в традиционных формах развлечений. Мы можем слушать музыку, смотреть фильмы, читать книги, скачивая их из компьютерной сети.

Сеть создала новую форму развлечений, такую как online-игры.

В предлагаемом пособии содержится описание методов и приемов проектирования и реализации вычислительных сетей, особое внимание уделяется грамотному планированию инфраструктуры и составлению документации.

При достаточно успешном освоении этих приемов возникает возможность дальнейшего продвижения вперед в изучении более специфических разделов вычислительных сетей.

Материал, представленный в пособии, может активно использоваться во время учебных занятий и самостоятельно в домашних условиях, даже при наличии только одного компьютера.

КОМПЬЮТЕРНЫЕ СЕТИ

Выделяют два основных способа организации компьютерных сетей: локальные и глобальные сети. Каждая состоит из программных, аппаратных компонентов и соединяющих кабелей.

Локальные сети (LAN – Local Area Network) предназначены для повышения эффективности использования ресурсов за счет их совместного применения большим количеством работников. LAN объединяет рабочие станции, периферийное оборудование, терминалы и другие устройства в пределах организации.

Характерными особенностями локальной сети являются:

- ограниченные географические размеры LAN;
- высокая пропускная способность (скорость передачи);
- постоянное подключение к ресурсам LAN;
- физическое соединение рядом стоящих устройств.

Глобальные сети (WAN – Wide Area Network) предназначены для объединения локальных сетей и обеспечивают связь между этими сетями (компьютерами, находящимися в локальных сетях).

Характерными особенностями глобальной сети являются:

- подключаемые устройства и сети обычно разделены большими расстояниями;
- обычно используются общедоступные среды передачи: сети телефонных компаний, кабельных (телевизионных) компаний, спутниковых систем и сети провайдеров (ISP – Internet Service Provider);
- применяется множество различных технологий доступа, чтобы обеспечить доступ большому количеству пользователей: коммутируемый и широкополосный доступ, беспроводной и т.д.

Процесс объединения сетей обычно называется организацией межсетевого взаимодействия.

Объединение и построение сетей осуществляется в соответствии с одной из принятых топологий организации сети. Под топологией сети понимается конфигурация графа, вершинам которого соответствуют

конечные узлы сети и коммуникационное оборудование, а ребрам – электрические и информационные связи между ними.

При объединении устройств в сеть могут применяться промежуточные устройства (транзитные), используемые для управления сетью и процессом передачи. В роли промежуточного устройства может выступать как компьютер, так и специализированное устройство типа маршрутизатора.

От выбора топологии во многом зависят характеристики будущей сети.

Среди множества возможных топологий различают следующие типы:

- *Полносвязные*. При использовании данной топологии каждый компьютер (устройство) непосредственно связан линиями связи со всеми остальными. Редко применяются в крупных сетях, так как при большом количестве соединяемых устройств возникают большие проблемы с управлением (сложность администрирования, большое количество элементов сети).

- *Неполносвязные*. При использовании данной топологии для организации обмена данными между двумя компьютерами (устройствами) может применяться промежуточная передача данных через другие устройства сети.

Основные используемые топологии:

- Топология "звезда". В данном случае каждый компьютер (устройство) подключается к коммутирующему устройству с помощью отдельного кабеля. Основная задача коммутирующего устройства – управление потоком данных.

- Ячеистые топологии (mesh). Получаются из полносвязной путем удаления некоторых связей. Данная топология характерна для крупных сетей.

- Кольцевые топологии (ring). Данные в сетях с такой топологией передаются по кольцу от одного компьютера (устройства) к другому.

- Топология «общая шина». В данной топологии все устройства подключаются к единой кабельной системе и разделяют общую

среду передачи. Примерами сетей, построенных на топологии «общая шина», являются сети кабельного телевидения и беспроводные сети. Передаваемая информация доступна одновременно всем подключенным к среде передачи устройствам.

Указанные топологии могут использоваться не только для объединения устройств в рамках одной сети, а также и для объединения сетей. В настоящее время топология «звезда» является самой распространенной топологией связи как в локальных, так и глобальных сетях.

В топологию могут вводиться дополнительные связи между устройствами в целях повышения надежности, защиты от сбоев, повышения пропускной способности, балансирования нагрузки.

ЭЛЕМЕНТЫ КОМПЬЮТЕРНОЙ СЕТИ

Основные элементы компьютерной сети: хост, коммутирующее устройство (маршрутизатор, коммутатор), среда передачи.

Компьютеры, которые используются в компьютерной сети, часто называют или хостами, или оконечными системами: хостами, потому что являются «основой» для программ, выполняемых на них; оконечными системами, потому что расположены на границе сети (в конечной точке). Обычно данные понятия равноправны.

Хосты разделяются на две категории: клиенты и серверы. Неформально, клиенты часто, как правило, это настольные ПК и рабочие станции, в то время как серверы – более мощные компьютеры. Серверы могут быть изготовлены для установки в серверные стойки (рис. 1) или выполнены в отдельном корпусе (рис. 2).

Некоторые из производителей серверов: IBM, Cisco Systems, Dell, HP.

Однако есть и более точный смысл клиента и сервера в области компьютерных сетей: в клиент-серверной модели клиентская программа, работающая на одной оконечной системе, запрашивает и по-

лучает информацию от сервера (программы) на другой оконечной системе.

Клиент-серверная модель является наиболее распространенной схемой взаимодействия для сетевых приложений. Службы Веб, электронной почты, передачи файлов, удаленного доступа и многие другие базируются на клиент-серверной модели.



Рис. 1. Сервер IBM System x3250 M3 для установки в стойку



Рис. 2. Сервер IBM System x3200 M2 в отдельном корпусе

Поскольку клиент обычно работает на одном компьютере, а сервер на другом, то подобные приложения по определению являются

распределенными приложениями. При этом клиент и сервер взаимодействуют друг с другом, передавая друг другу сообщения через компьютерную сеть.

На уровне хостов коммутирующие устройства, каналы связи и прочие «детали», из которых состоит компьютерная сеть, являются "черными ящиками", обеспечивающими передачу сообщений между клиентом и сервером.

Основные коммутирующие устройства, используемые в компьютерных сетях: маршрутизатор (router) и коммутатор (switch).

Коммутатор – сетевое устройство, которое может одновременно устанавливать соединения между несколькими парами портов и реализует виртуальные соединения между сегментами компьютерной сети. Также коммутаторы обеспечивают усиление сигнала. Коммутатор «изолирует» каждый сегмент сети от других сегментов, сужая область распространения ошибок до одного сегмента. При монтаже современных компьютерных сетей в каждом сегменте, подключенном к порту коммутатора, размещен только один хост. Это позволяет снизить до минимума количество ошибок при передаче и добиться максимальной скорости.

Маршрутизаторы используются для объединения отдельных сетей и доступа к глобальным сетям (в том числе сети Интернет). Они обеспечивают прохождение трафика между различными сетями на основании адресной информации и способны принимать решение о выборе оптимального маршрута движения данных от одной сети до другой. Обычно маршрутизаторы оснащены только двумя портами: для подключения к локальной сети организации и подключения к внешней сети.



а)

б)

Рис. 3. Типовое обозначение коммутатора (а) и маршрутизатора (б)

Коммутирующее оборудование аналогично хостам может быть выполнено в форме для установки в стойку (рис. 4, 5) или в отдельном корпусе (рис. 6). Первый вариант применяется в основном в крупных сетях с большим количеством оконечных устройств (и оснащается большим количеством портов), второй – в небольших организациях или дома при небольшом количестве хостов.



Рис. 4. Коммутатор Cisco WS-C2960-48TC-L



Рис. 5. Маршрутизатор Cisco серии 1900



Рис. 6. Маршрутизатор D-Link DI-824 (а) и коммутатор D-Link DES-1008F (б)

Маршрутизаторы и коммутаторы могут совмещаться с точками доступа (беспроводной сети) и модемами.

Некоторые из производителей коммутирующего оборудования: Cisco Systems, D-Link, ZyXEL, 3COM, ASUS.

В локальных сетях каждый хост подключается к сети с помощью некоторой передающей среды. Как правило, у каждого хоста имеется только один сетевой адаптер.

Для обозначения среды передачи применяются следующие символы:

-  - среда передачи в глобальной сети;
-  - среда передачи в локальной сети;
-  - беспроводная среда передачи.

Для локальных сетей обычно прокладывается специализированная кабельная система, называемая структурированной кабельной системой.

Кабели можно разделить на электрические (чаще всего медные – Copper cable) и оптоволоконные (Fiber-optic cable). Быстрое распространение также получают технологии беспроводного доступа к компьютерным сетям.

Стандарты, наиболее часто используемые при проектировании и реализации кабельной системы компьютерных сетей: TIA/EIA-568-A, TIA/EIA-568-B, TIA/EIA-569-A, TIA/EIA-570-A, TIA/EIA-606, TIA/EIA-607. В России с 2010 года действует ГОСТ Р 53246-2008. «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования».

МОДЕЛИ ВЗАИМОДЕЙСТВИЯ СИСТЕМ

По мере развития компьютерных сетей стали все более актуальными проблемы их объединения. Было сложно объединять сети, использующие различные спецификации аппаратного и программного обеспечения и реализованные по разным стандартам.

Для решения проблемы Международная Организация Стандарти-

зации (ISO) предложила модель OSI (базовая эталонная модель взаимодействия открытых систем, англ. Open Systems Interconnection Basic Reference Model, 1978 г.). Модель снабдила разработчиков аппаратного и программного обеспечения набором стандартов, обеспечивающих совместимость различных типов сетей, построенных при использовании сетевого оборудования, разработанного разными производителями.

Модель OSI базируется на семи относительно автономных уровнях, каждый из которых реализует четко определенное множество сетевых функций. По мере того как подлежащая отсылке информация проходит вниз через уровни модели, происходит ее преобразование от формы, «понятной человеку», до формы, «понятной компьютерам».

Модель OSI упрощает понимание сетевых функций благодаря: уменьшению сложности процесса передачи данных путем разделения процесса на более простые части; стандартизации интерфейсов; введению модульности элементов аппаратного и программного обеспечения. Введение модели также позволило ускорить процесс разработки новых более производительных и надежных сетевых устройств и сервисов.

При передаче, когда данные переходят с одного уровня модели на другой, происходит добавление к данным заголовка (или прицепа) на каждом уровне. Заголовки и контейнеры содержат управляющую информацию для сетевых устройств и получателя, которая гарантирует правильную доставку данных и их интерпретацию (такой процесс называется инкапсуляцией). При получении происходит обратная операция, т.е. управляющая информация из заголовка (и прицепа) считывается, выполняются необходимые операции и они удаляются.

Модель OSI исключает прямую связь между равными по положению уровнями, находящимися в разных системах. Задача каждого уровня – предоставление услуг вышележащему уровню, маскируя детали реализации этих услуг. При этом каждый уровень на одном компьютере работает так, будто он напрямую связан с таким же уровнем на другом компьютере.

Функции уровней модели OSI

Группа	PDU ¹	Уровень	Краткое описание
Уровни хоста	Данные	7 – Прикладной (Application)	Предоставление сетевых сервисов пользователю (передача файлов, электронная почта и т.д.) Не предоставляет услуги другим уровням. Управляет остальными шестью уровнями
		6 – Представительский (Presentation)	Преобразование данных для обработки на прикладном уровне, сжатие, шифрование/дешифрование и т.п.
		5 – Сеансовый (Session)	Управление взаимодействием в симплексном (simplex), полудуплексном (half-duplex) и полнодуплексном (full-duplex) режимах. Управление распределением данных между приложениями
	Сегмент	4 – Транспортный (Transport)	Установка, управление и разрыв соединения между двумя хостами. Контроль доступа, обеспечение выбранного уровня качества передачи
Уровни среды передачи	Пакет, Датаграмма	3 – Сетевой (Network)	Адресация пакетов, перевод логических имён в физические сетевые адреса (и обратно), выбор маршрута передачи пакета до сети назначения
	Фрейм	2 – Канальный (Data-link)	Формирование пакетов для передачи. Управление доступом к среде передачи, обнаружение ошибок передачи, повторная передача ошибочных пакетов
	Бит	1 – Физический (Physical)	Кодирование передаваемой информации в форму сигналов, принятых в среде передачи, обратное декодирование. Передача сигналов. Также здесь определяются требования к соединениям, разъёмам, заземлению, защите от помех и т.п.

¹ Protocol Data Unit – обобщённое название фрагмента данных на разных уровнях модели. Обычно в PDU помимо сообщения включаются имя отправителя, тип сообщения, а также другая служебная информация.

Уровни взаимодействуют в соответствии с правилами, описанными в сетевых протоколах. Сетевые протоколы – это наборы правил и стандартов, в соответствии с которыми работают сетевые сервисы.

Существует множество различных протоколов со своими функциями и задачами, соответствующих разным уровням модели OSI (рис.7).

Ниже приведено несколько распространённых протоколов:

- DNS (Domain Name System, система доменных имён). Чаще всего используется для получения IP-адреса по имени хоста.
- FTP (File Transfer Protocol, протокол передачи файлов). Предназначен для передачи файлов в компьютерных сетях.
- SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты). Предназначен для передачи электронной почты.
- TCP (Transmission Control Protocol, протокол управления передачей). Один из основных протоколов Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP.

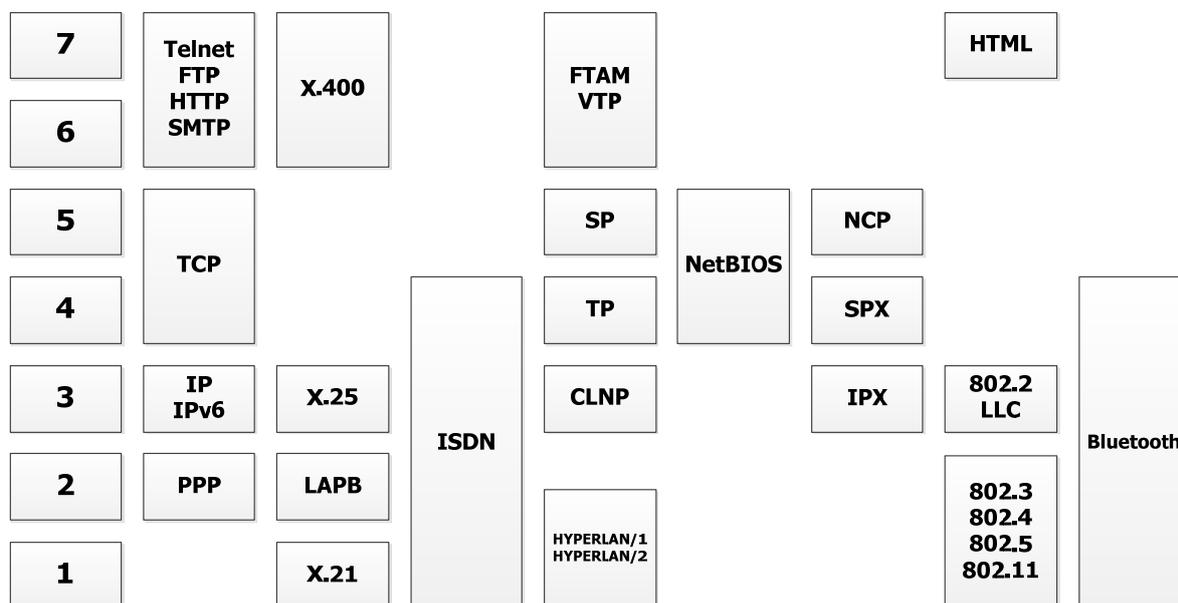


Рис. 7. Некоторые из наиболее распространенных стандартов и протоколов, распределенных по уровням модели OSI

Снабжение каждого уровня модели собственным протоколом наряду с достоинствами имеет и несколько недостатков. Первый связан с нередко встречающейся ситуацией дублирования одних и тех же

функций различными уровнями (например контроль ошибок). Другой потенциальный недостаток заключается в том, что функциям одного уровня может понадобиться информация, хранящаяся на другом уровне (например время).

Иерархически организованный набор сетевых протоколов, достаточный для организации взаимодействия хостов в сети, называется стеком протоколов.

Наиболее распространенный стек во всем мире – стек TCP/IP (рис. 8). Это определяется тем, что: схема адресации TCP/IP позволяет поддерживать очень большие сети; поддержка стека реализована фактически во всех операционных системах и платформах; разработано большое количество утилит и инструментов для данного стека протоколов; используется в сети Интернет.

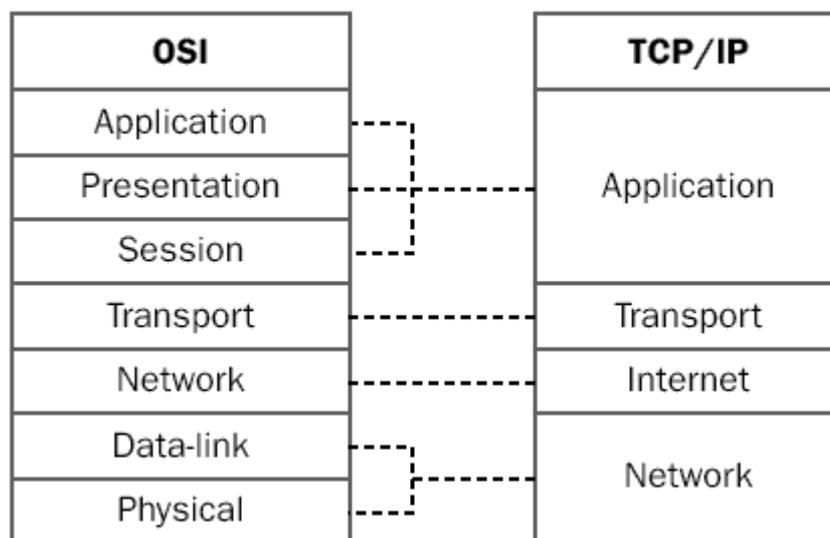


Рис. 8. Соответствие уровней моделей OSI и TCP/IP

Данный стек также может обозначаться как стек протоколов Интернета или стек DoD.

Модель взаимодействия TCP/IP базируется на четырех уровнях:
- Уровень процессов/приложений (Application Layer (process-to-process)). Протоколы данного уровня используются для предоставления сетевых сервисов пользователю, а также для управления сетью.

- Транспортный уровень (Transport Layer (host-to-host)). На данном уровне существуют два протокола: TCP – надежный протокол с установлением соединения и UDP (User Datagram Protocol) – протокол дейтаграмм пользователя, ориентированный на скоростную доставку без подтверждений.
- Уровень интернета (Internet Layer (internetworking)).
- Уровень доступа к сети (Link Layer).

ИСТОРИЯ РАЗВИТИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Историю развития компьютерных сетей можно разделить на пять периодов (табл. 2) и в каждом из которых выделить ряд ключевых технологий, сформировавших то, что мы сейчас называем компьютерной сетью.

Таблица 2

Ключевые моменты истории развития компьютерных сетей

Период	Ключевые элементы периода
1961 – 1972 гг.	<ul style="list-style-type: none"> - Разработка технологии коммутации пакетов Леонардом Клейнроком. - Разработка сети ARPAnet (Джозеф Карл Роберт Ликлайдер, Робертс (Lawrence G. Roberts)). В 1972 г. в сети насчитывалось 15 компьютеров. - Первый протокол управления сетью – NCP (Network-Control Protocol, RFC 001). - Первая программа электронной почты (1972), разработанная Рэем Томлинсоном
1972 – 1980 гг.	<ul style="list-style-type: none"> - Увеличение количества компьютерных сетей: Telenet (компания BBN), Cyclades (французская сеть), SNA (компания IBM), Tymnet, GE Information Services. - Беспроводная сеть ALOHAnet (Гавайские острова). - Разработка принципов технологии Ethernet Робертом Меткалфом (1973). - Попытки соединения разрозненных сетей, подключения периферийных устройств (принтера, дисков). - Разработка протоколов TCP, UDP, IP, ALOHA (с множественным доступом к среде передачи)

Период	Ключевые элементы периода
1980 – 1990 гг.	<ul style="list-style-type: none"> - 1980 г. – около 100 тыс. компьютеров, подключенных к компьютерным сетям. - Объединение локальных сетей в региональные сети: BITNET (файлы и почта), CSNET (исследование сетевых технологий), магистраль NSFNET (доступ к суперкомпьютеру). - 1 января 1983 г. – переход на стек TCP/IP. - Разработка DNS (Domain Name System). - Сеть Minitel (Франция) – 20 тыс. устройств (сетью пользовались около 20 % жителей Франции)
1990 – 2000 гг.	<ul style="list-style-type: none"> - Поглощение компьютерных сетей сетями коммерческих Интернет-провайдеров. - APRAnet прекратила существование. - Разработка технологии WWW, языка HTML, протокола HTTP, браузера и веб-сервера Тимом Бернерс-Ли. - Разработка браузера Mosaic (Марк Андрессен, 1993). - «Войны браузеров». - Развитие e-mail, icq, файловых архивов, расцвет электронных торгов
2000 – ...	<ul style="list-style-type: none"> - Увеличение количества ресурсоемких приложений. - Развитие широкополосного доступа (DSL). - Развитие технологий беспроводного доступа, подключение операторов мобильной связи к сети Интернет. - Децентрализованный доступ к ресурсам, сети P2P. - Распределённые вычисления. Проекты типа SETI@home (Search for Extra-Terrestrial Intelligence at Home, поиск внеземного разума на дому). Проекты на платформе BOINC. - Развитие индустрии развлечений в «сети»

ПРОЕКТИРОВАНИЕ КОМПЬЮТЕРНОЙ СЕТИ²

Правильная организация процесса проектирования позволяет построить эффективную и удовлетворяющую потребностям пользователей локальную сеть.

² Данный раздел написан совместно с инженером кафедры ИЗИ ГОУ ВПО ВлГУ А.А. Ворониной.

Основные характеристики, лежащие в основе сетевой архитектуры:

- Отказоустойчивость (надежность). Для технических устройств используются такие показатели надежности, как среднее время наработки на отказ, вероятность отказа, интенсивность отказов. Однако эти показатели пригодны для оценки надежности простых элементов и устройств, которые могут находиться только в двух состояниях – работоспособном или неработоспособном. Сложные системы, состоящие из многих элементов, кроме состояний работоспособности и неработоспособности могут иметь и другие промежуточные состояния. В связи с этим для оценки надежности сложных систем применяется другой набор характеристик:

1. *Готовность (availability)* означает долю времени, в течение которого система может быть использована. Её можно улучшить путем введения избыточности в структуру системы: ключевые элементы системы должны существовать в нескольких экземплярах, чтобы при отказе одного из них функционирование системы обеспечивали другие.

2. *Надежность*. Так как в основе работы сети лежит передача пакетов между хостами, то надежность можно выразить через *вероятность доставки пакета узлу назначения без искажений*. Наряду с этой характеристикой могут использоваться и другие: *вероятность потери пакета* (по любой из причин: переполнения буфера маршрутизатора; несовпадения контрольной суммы; отсутствия пути к узлу назначения и т.д.), *вероятность искажения отдельного бита передаваемых данных*.

3. *Отказоустойчивость (fault tolerance)*. В сетях под отказоустойчивостью понимается способность системы скрыть от пользователя отказ отдельных ее элементов. Отказ элементов в отказоустойчивых системах не приводит к ее остановке.

4. *Масштабируемость (расширяемость)*. Расширяемость (extensibility) означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, ком-

пьютеров, приложений, служб), наращивания длины сегментов сети и замены существующих элементов более производительными. При этом важно, чтобы процесс расширения не приводил к снижению производительности системы в целом. Масштабируемость (scalability) означает, что сеть позволяет наращивать количество хостов и протяженность сегментов в очень широких пределах, при этом производительность данной сети не ухудшается. В данном случае необходимо применять дополнительное коммуникационное оборудование и эффективно структурировать сеть. Оптимальной является иерархическая организация сети.

5. *Качество обслуживания.* Функции данного понятия заключаются в обеспечении гарантированного и дифференцированного обслуживания путем передачи контроля за использованием ресурсов и загруженностью сети ее оператору. *Дифференцированное обслуживание* предполагает разделение трафика на классы на основе требований к качеству обслуживания. При подобном обслуживании трафик распределяется по классам, каждый из которых имеет свой собственный приоритет. *Гарантированное обслуживание (guaranteed service)* предполагает резервирование сетевых ресурсов с целью удовлетворения специфических требований к обслуживанию со стороны потоков трафика по всей траектории его движения. Гарантированное обслуживание довольно часто называют еще жестким QoS (hard QoS) в связи с предъявлением строгих требований к ресурсам сети, а дифференцированное – мягким.

6. *Безопасность (security)* можно рассматривать как один из аспектов надежности. Это способность системы защитить данные от несанкционированного доступа. В сетях сообщения передаются по линиям связи, часто проходящим через общедоступные участки сети, в которых могут быть установлены средства прослушивания и перехвата, подключено дополнительное оборудование.

В общем случае процесс проектирования компьютерной сети включает в себя следующие этапы:

- обследование объекта, сбор требований, ожиданий и пожеланий пользователей;
- анализ собранной информации и подготовка коммерческого предложения (технического задания) по созданию локальной сети;
- проектирование структуры компьютерной сети на трех уровнях модели взаимодействия (с 1-го по 3-й): разработка структурных схем, схем адресации, схем размещения оборудования и т.д.;
- подготовка необходимой документации.

В дальнейшем осуществляются монтаж кабельной системы, установка необходимого сетевого оборудования, проведение пуско-наладочных работ. По завершению пуско-наладочных работ необходимо уточнить сведения в документации на компьютерную сеть.

Обследование объекта

Вначале следует собрать данные о структуре организации. Эта информация должна включать в себя данные об истории и текущем состоянии организации, планируемом росте, методах управления, офисных системах, а также мнение персонала, который будет работать в локальной сети.

Если в организации уже используется компьютерная сеть, целесообразно проанализировать ее работу, определить эффективность, попытаться выявить проблемные места.

Нужно зафиксировать существующее программное и аппаратное обеспечение и то, которое планируется использовать в будущем. Рекомендуется составить перечень вычислительных ресурсов в организации, определить уровень критичности для бизнеса выявленных ресурсов и требования к компьютерной сети, необходимые для использования ресурсов с учетом уровня квалификации персонала.

Возможно, в организации существуют ограничения на использование определенного вида сетевого оборудования (например в медицинских организациях) или определены жесткие требования к нему. Данные ограничения должны быть учтены.

На данном этапе желательно определиться с параметрами доступа к ресурсам (права доступа).

Основными источниками сведений являются:

- руководители различного уровня;
- сотрудники;
- документация на программные средства;
- конфигурационные файлы.

Подводя итог сказанному выше, на данном этапе необходимо провести инвентаризацию ИТ-ресурсов организации, опрос персонала и определить перечень нормативных и организационно-распорядительных документов, требования которых должны быть учтены в соответствии со спецификой деятельности организации.

Для проведения обследования целесообразно сформировать специальную рабочую группу. С целью оказания содействия и необходимой помощи рабочей группе выпускается соответствующее распоряжение по организации, в котором определяются полномочия группы, ее состав. В состав группы рекомендуется включать представителей подразделений, где планируется монтаж сети, и сотрудников, владеющих сведениями по вопросам обработки информации в данных подразделениях.

В процессе инвентаризации уточняется размещение рабочих мест пользователей, сетевого оборудования. Рекомендуется максимально полно документировать данный процесс. После инвентаризации аппаратного и программного обеспечения проводится инвентаризация протекающих в организации задач (бизнес-процессов).

При обследовании подсистем и задач выявляются все виды входящей, исходящей, хранимой и обрабатываемой информации. Данные сведения позволяют определить требования к пропускной способности каналов связи и промежуточному сетевому оборудованию.

На следующем этапе необходимо определиться с параметрами защиты информации, циркулирующей в сети (уровень защиты от сбоев, кражи, несанкционированные изменения и т.п.). В дальнейшем следует уточнить состав необходимых для каждой задачи ресурсов, определить параметры доступа по группам пользователей и указания по настройке применяемых средств защиты. Эти сведения будут использоваться в качестве эталона настроек средств защиты и для контроля правильности их установки.

Анализ собранных данных

Следующий этап – анализ собранных данных и оценка требований пользователей.

Полезность сети определяется ее доступностью. На доступность влияют многие факторы, включая следующие: пропускная способность; время отклика; доступ к ресурсам.

В правильно спроектированной компьютерной сети удастся добиться максимально возможной доступности при наименьших затратах. Для этого необходимо оценить потоки данных, генерируемые используемыми сетевыми приложениями. Нагрузка должна быть рассчитана для стандартного (типового) режима работы сети при максимальном количестве одновременно работающих пользователей и во время запуска всех сетевых служб.

Рекомендуется составить граф информационных потоков (рис. 9, 10).

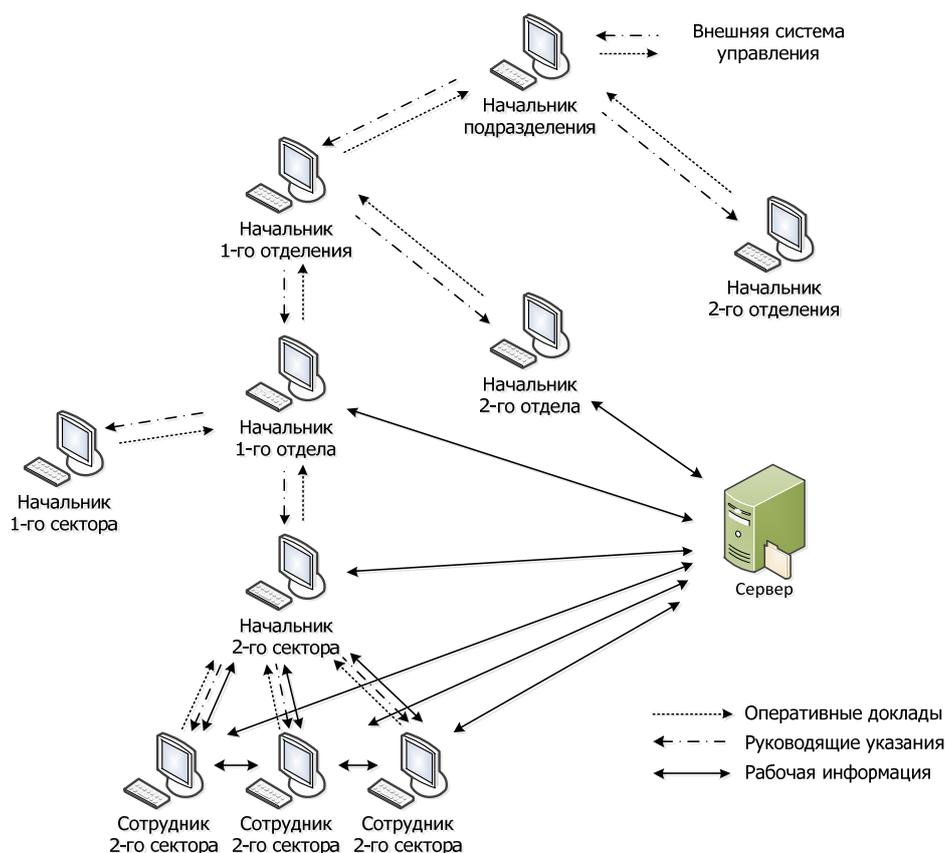


Рис. 9. Пример графа информационных потоков

Используя методы оптимального распределения ресурсов по уз-

лам графов (узлам сети), можно выявить узлы для размещения ресурсов, удовлетворяющие требованиям оптимальности (по производительности узлов сети, времени доступа).

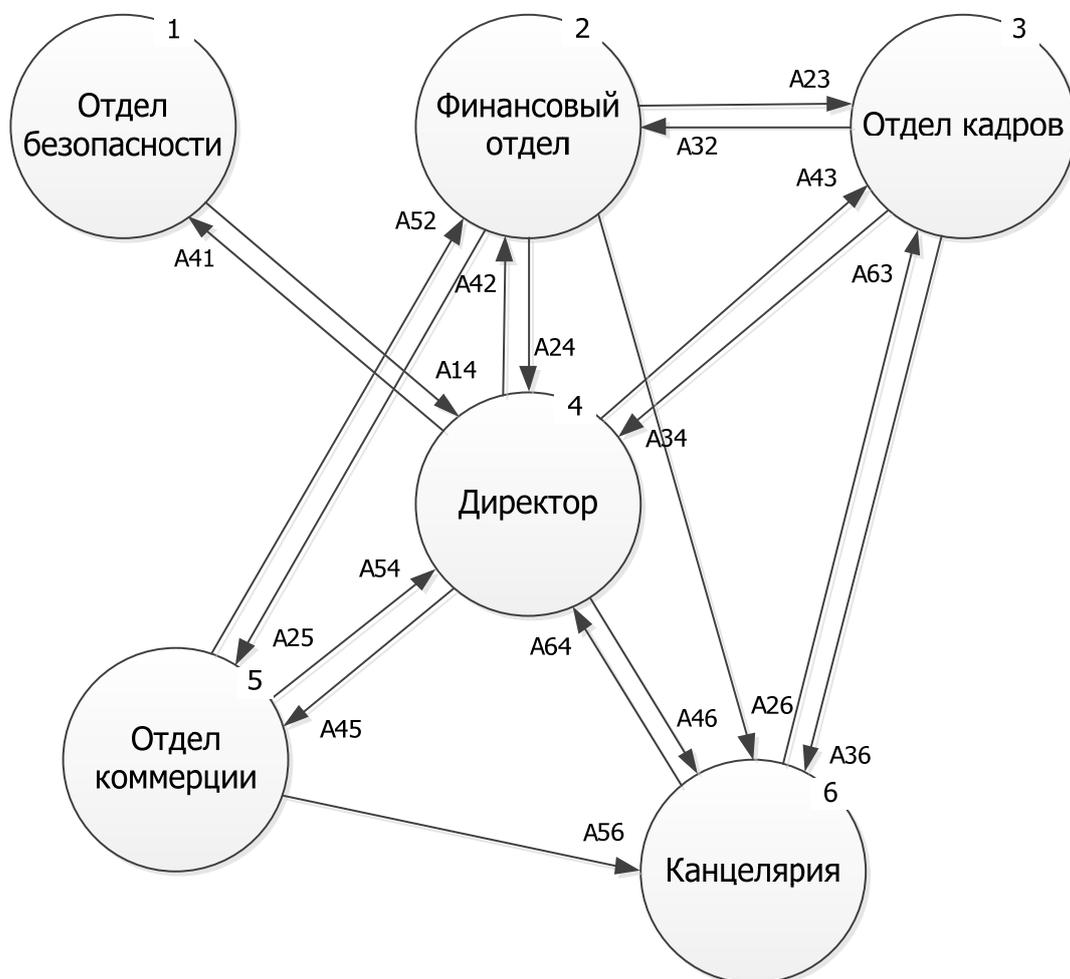


Рис. 10. Пример графа информационных потоков (A_{ij} – характеристики потоков данных)

Ситуация, когда группа пользователей работает с одной базой данных, приводит к тому, что в сети циркулирует большое количество одинаковой информации. В данном случае территориальное расположение фрагментов базы данных положительно влияет на средние задержки обслуживания пользователей. Возможными путями снижения задержек (кроме повышения быстродействия составляющих сеть элементов) могут быть:

- 1) оптимальное расположение баз данных на хостах (серверах)

компьютерной сети;

2) полное и (или) частичное дублирование баз данных на нескольких серверах;

3) дублирование баз данных и оптимальное распределение копий баз данных по серверам (комбинация первого и второго путей).

Первый вариант можно реализовать без использования дополнительных программных и аппаратных средств. Второй вариант предполагает наличие специальной службы синхронизации копий баз данных.

Рекомендуется создать таблицы необходимых сетевых ресурсов приложений (профили пользователей, приложений). В таблице отразить ориентировочный перечень приложений для каждой рабочей станции, определить средний объем трафика между рабочими станциями и серверами, перечень портов, служб и протоколов, параметры защиты. Необходимо также учесть служебный трафик, генерируемый рабочими станциями и серверами (обновления, резервное копирование и т.п.). Примерными формами таблиц могут быть следующие (табл. 3, 4, 5).

Таблица 3

Таблица профилей пользователей

№ п/п	Пользователь (группа пользователей)	Перечень задач	Приложения и службы, используемые для выполнения задач	Минимальные и рекомендуемые требования к аппаратному обеспечению хоста	Требования сети передачи данных (СПД) с учетом специфики задачи, используемых приложений и служб
1					
2					
3					

Перечень задач может быть определен дополнительной таблицей в соответствии с должностными инструкциями и бизнес-процессами

организации. Рекомендуется, чтобы на каждую задачу присутствовал формуляр задачи.

Следует учесть, что используемые приложения и службы должны быть зарегистрированы в фонде алгоритмов и программ.

Таблица 4

Таблица профилей приложений и служб

№ п/п	Приложение, служба	Минимальные требования к СПД	Дополнительные характеристики
1			
2			
3			

В дополнительных характеристиках приложения можно перечислить используемые протоколы, порты.

Таблица 5

Таблица ресурсов, подлежащих защите

№ п/п	Ресурс	Степень конфиденциальности, (высокая, средняя, низкая)	Степень целостности (высокая, средняя, низкая)	Размещение ресурса в компьютерной сети (хост)	Используемые средства защиты	Ответственный
1						
2						
3						

Степень конфиденциальности и целостности определяется в соответствии с регламентированными нормативными и организационно-распорядительными документами, а также может быть определена методом экспертной оценки.

Основной результат данного этапа – логическая схема организации компьютерной сети. Необходимо оценить сильные и слабые стороны различных топологий, так как это может оказать сильное влия-

ние на производительность и эффективность сети. Сейчас наиболее используемой топологией является «звезда».

Проектирование структуры компьютерной сети

Следующий этап проектирования – переложить логическую структуру, разработанную с учетом особенностей организации, ее потребностей и информационных потоков на реальное оборудование (рис. 11).

Логическую структуру компьютерной сети нужно распределить по трем уровнями модели OSI: сетевому, канальному и физическому. В точках объединения информационных потоков обычно устанавливаются коммутирующие сетевые устройства.

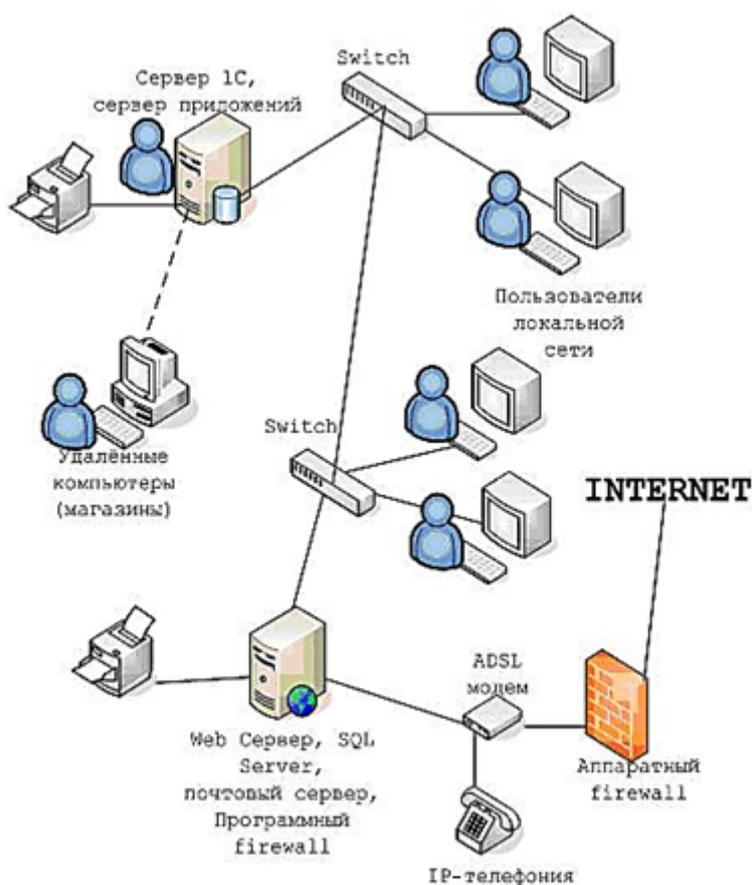


Рис. 11. Логическая структура компьютерной сети предприятия (пример представления)

Проектирование топологии на физическом и канальном уровнях

предполагает решение вопросов, связанных с реальным сетевым оборудованием и кабельной системой. Решение включает в себя выбор типа кабеля (обычно медный, оптоволоконный), определение структуры кабельной системы. При проектировании и прокладке кабелей следует руководствоваться стандартами организации структурированных кабельных систем (в России – ГОСТ Р 53246-2008).

Так как большинство проблем функционирования компьютерной сети – это проблемы на физическом уровне, работы, связанные с реальным оборудованием, рекомендуется проводить особенно аккуратно. На данном этапе следует составить планы физического размещения компонентов сети, схемы прокладки кабелей (рис. 12, 13, 14), а также выполнить проверку на наличие возможных источников помех (близкое расположение электрических щитков, скрытой проводки и т.д.). При решении поставленных задач можно воспользоваться схемами и планами, имеющимися в организации (планы этажей, коммуникаций), а также проконсультироваться с обслуживающим персоналом. В процессе монтажа возможно использование специального тестирующего оборудования для документальной проверки характеристик смонтированного оборудования и кабельной системы.

Типичным сетевым устройством 2-го уровня является коммутатор (switch). Коммутаторы задают границы коллизионных и широковещательных доменов (процесс разделения называется процессом сегментирования сетей). Большие размеры коллизионных и широковещательных доменов приводят к снижению производительности сети и увеличивают вероятность распространения вирусов. При использовании концентратора полоса пропускания разделяется между всеми подключенными к нему хостами. Следует отметить, что концентраторы в настоящее время практически не используются. Их функции перешли на коммутаторы.

При учете особенностей физической реализации сети в организации вполне вероятна ситуация, когда потребуется установка дополнительного сетевого оборудования.

При построении схемы размещения оборудования, планов прокладки кабелей, монтажа розеток руководствуются рекомендациями

стандартов, а также особенностями процесса администрирования, наличия служебных помещений, вспомогательных сетей и т.п.

Часть оборудования рекомендуется размещать в специально оборудованных помещениях, в которых поддерживается оптимальный «климат» для работы сетевого оборудования. Кроме того, это позволяет решить некоторые вопросы безопасности и в ряде случаев сделать процесс администрирования более оперативным.

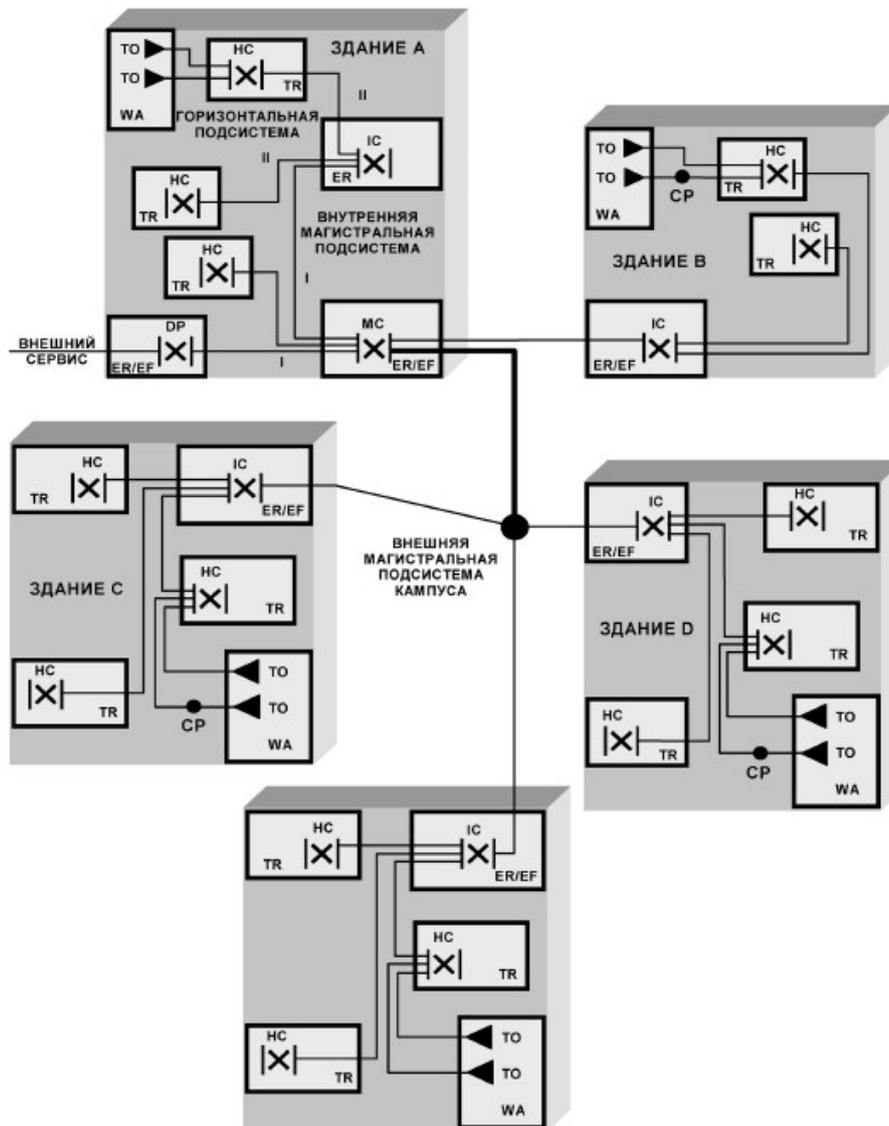


Рис. 12. Пример организации кабельных сетей кампуса в соответствии со стандартом ГОСТ Р 53246-2008

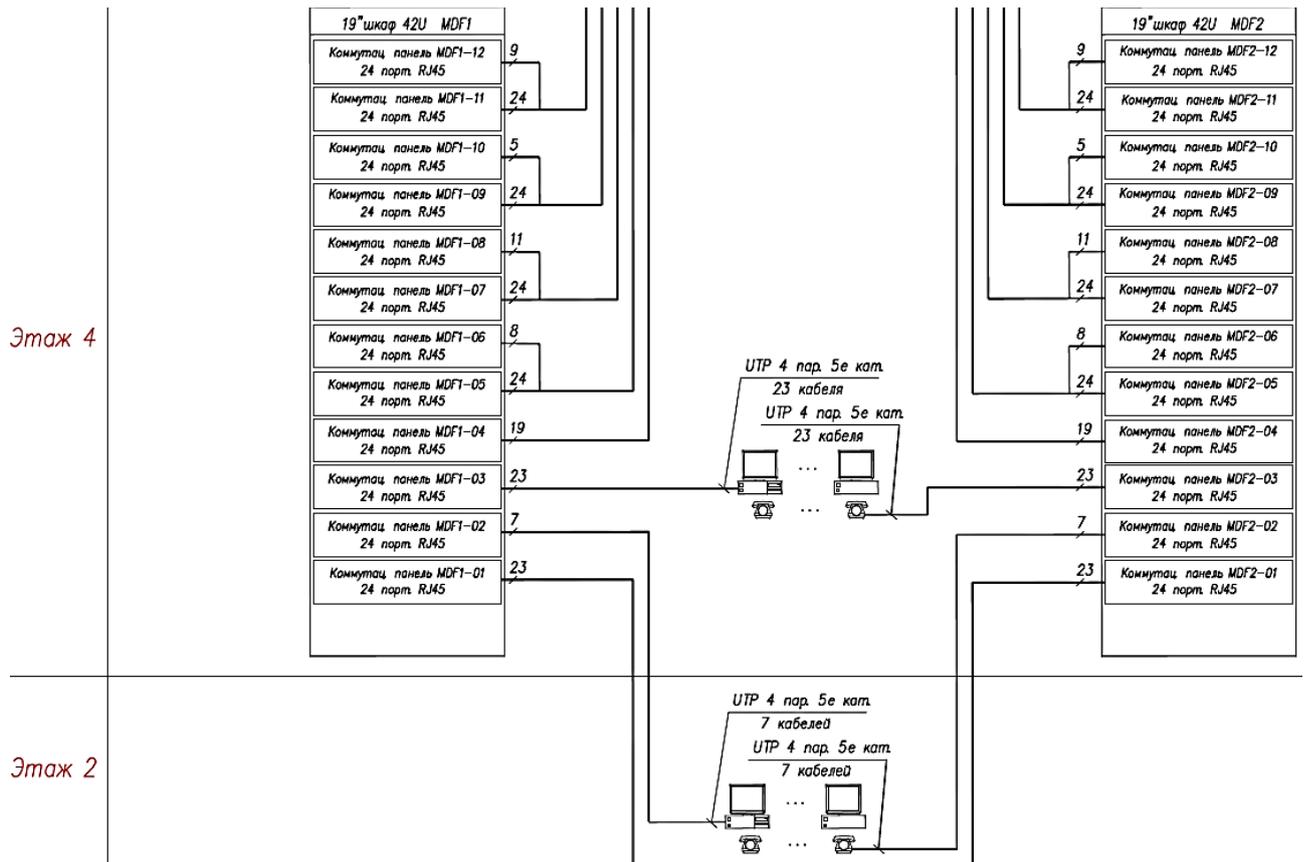


Рис. 13. Фрагмент структурной схемы СКС

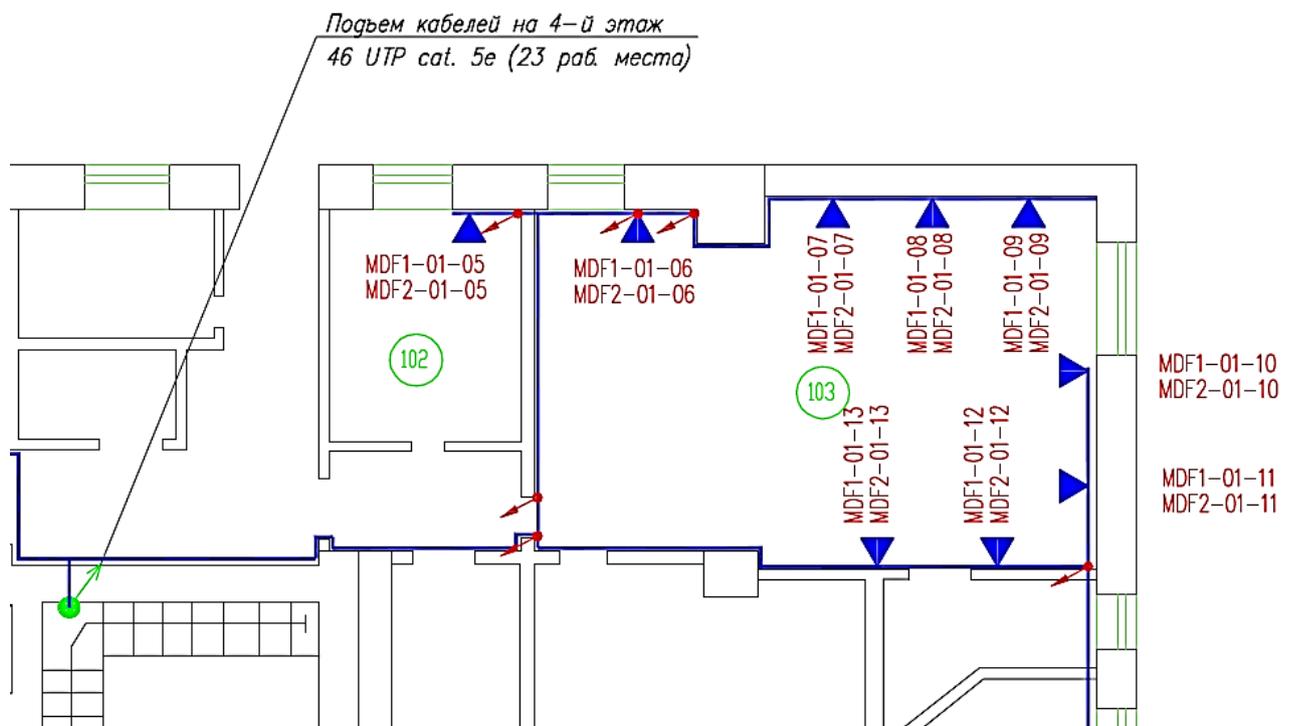


Рис. 14. Фрагмент плана этажа с отмеченными элементами СКС

Следует учитывать, что перестройка физической структуры компьютерной сети производится довольно редко (обычно раз в 5 – 10 лет) и, следовательно, она должна быть тщательно спланирована и предполагать возможность дальнейшего расширения сети в будущем. Вопрос детального документирования протекающих процессов также важен, так как сильно упрощает процесс дальнейшего сопровождения сети.

На 3-м уровне модели взаимодействия работают маршрутизаторы, которые сегментируют сеть на обособленные физические и логические сети, управляют качеством передачи, а также обеспечивают передачу данных между сегментами локальных и глобальных сетей. Широкие возможности при сегментировании позволяют добиться эффективного использования адресного пространства и обеспечить расширяемость сети в будущем. Маршрутизаторы также ограничивают широковещательные домены (рис. 15).

Применение технологии виртуальных сетей повышает уровень безопасности сети за счет изоляции трафика групп пользователей, подключенных к различным виртуальным сетям.

На данном уровне проводится распределение адресов, именование оборудования, определение параметров взаимодействия сетевого оборудования.

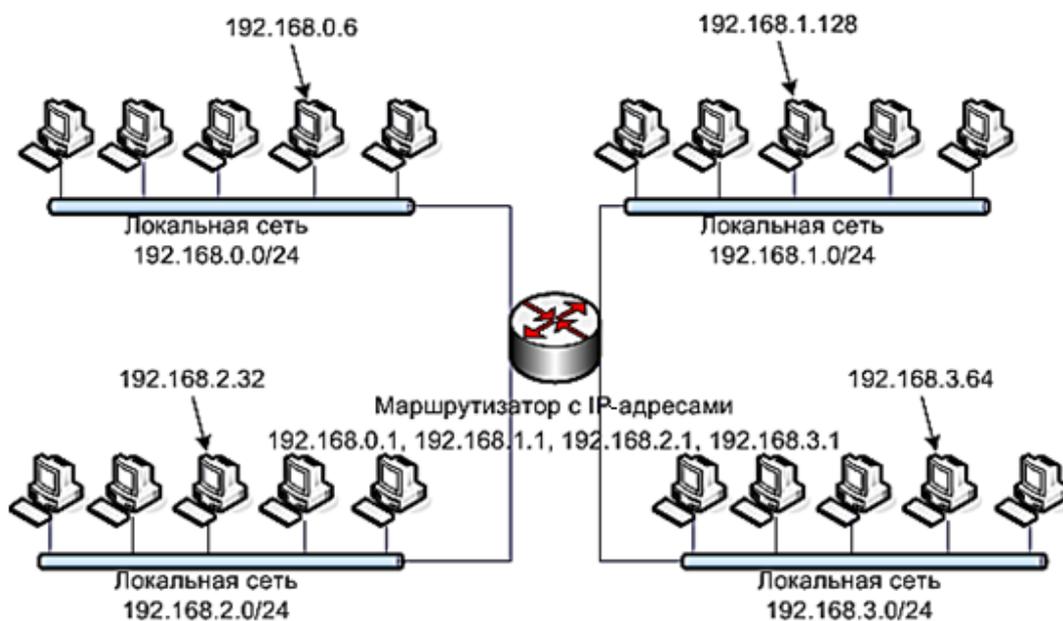


Рис. 15. Пример разделения сети на четыре сегмента при использовании маршрутизатора

В компьютерной сети каждое устройство обладает набором адресов. Адреса используются для организации взаимодействия на прикладном, транспортном, сетевом и канальном уровнях (табл. 6). Рассмотрим назначение каждого из адресов и общие принципы их использования.

Таблица 6

Схема адресации в компьютерной сети
(для стека TCP/IP, модель OSI)

Уровень	Адрес	Назначение
7 – Прикладной	DNS-имя хоста	Идентификация хостов на основе легко запоминаемых имен. Обычно пользователь знает доменное имя хоста, к которому собирается обращаться. Буквенное представление IP-адреса. Назначается администратором, например www.yandex.ru
4 – Транспортный	Порт	На хосте может одновременно работать несколько приложений. Для разделения приложений используется адресация транспортного уровня – порты. Определяется автоматически приложением из диапазона свободных портов или в соответствии со стандартами, например, порт 25 используется для отправки почты
3 – Сетевой	IP-адрес	Для идентификации интерфейса хоста в локальной и глобальной сети. Цифровой адрес, назначаемый администратором в соответствии с принятой схемой распределения адресного пространства. Хост может быть подключен к нескольким сетям. В этом случае хост должен иметь несколько IP-адресов. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение, например 192.168.0.1
2 – Канальный	MAC-адрес	При физической передаче пакетов необходимо знать адрес сетевого интерфейса устройства, которому осуществляется передача. Адрес канального уровня определяется технологией, с помощью которой построена сеть. Эти адреса назначаются производителями оборудования или администраторами, например 00-05-9A-3C-78-00

Адреса прикладного уровня – DNS

С точки зрения пользователя каждый хост или ресурс идентифицируется уникальным доменным именем. С точки зрения сетевого оборудования уникальный ресурс идентифицируется IP-адресом.

Для трансляции доменных имен в IP-адреса и обратно используется служба DNS (Domain Name System). Функция перевода доменных имен в IP-адреса называется функцией разрешения имени (name resolution). В данном случае используется DNS-протокол.

Инфраструктура DNS географически распределена по всему миру и организована иерархически (рис. 16). На верхнем уровне (в корне дерева) расположен единственный корневой домен (root domain). Обозначается точкой (данный символ обычно опускается при записи имени хоста). Ниже по иерархии расположено множество доменов верхнего (первого) уровня (top-level domain, TLD). Каждый TLD называется дочерним от корневого домена и может иметь множество собственных дочерних доменов – доменов второго уровня (second-level domain, или enterprise-level domain). При дальнейшем делении доменов появляются домены третьего, четвертого и так далее уровней.

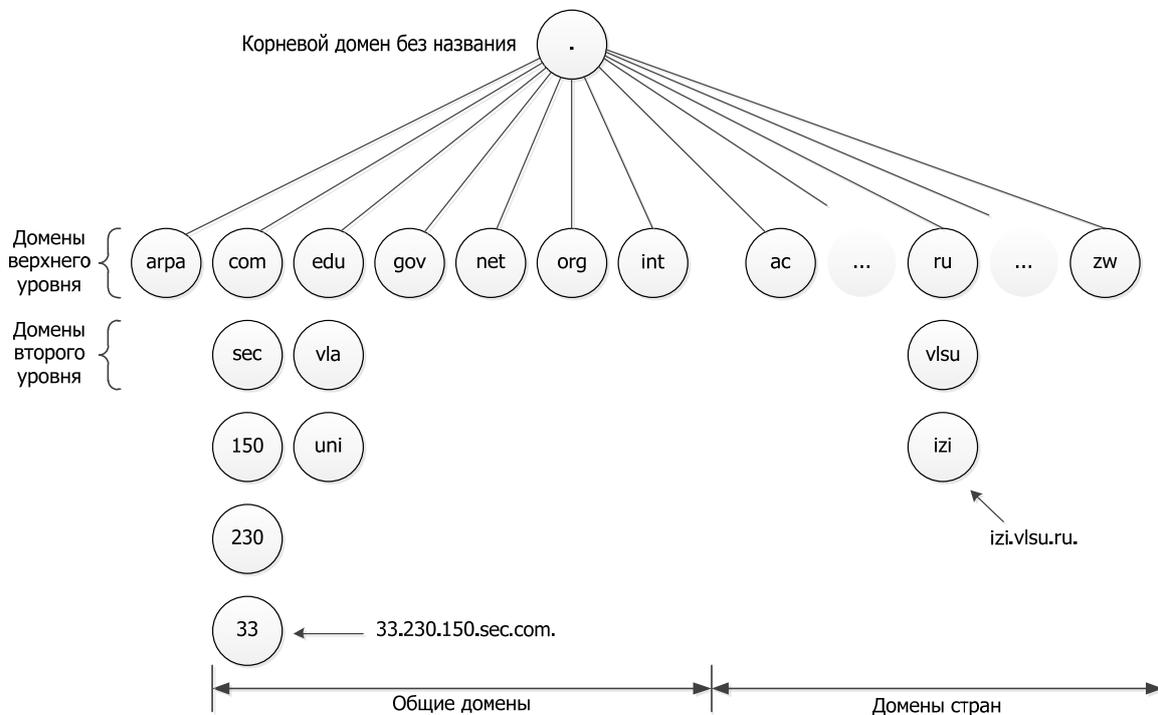


Рис. 16. Инфраструктура DNS

Доменное имя определяет порядок прохождения доменов, например, имя market.example.ru относится к домену третьего уровня – "market", который определен в домене второго уровня – "example", который в свою очередь определен в домене первого уровня (TLD) – "ru".

Каждая часть имени, отделенная от других частей точкой, называется доменом. При соединении всех частей получаем «полностью определенное доменное имя» (или просто – доменное имя) – Fully Qualified Domain Name – FQDN.

Имеется несколько миллионов доменов второго уровня. Например, (по сведениям Википедии) численность доменов на 8 октября 2010 г.:

- доменов .com, .net, .org, .info, .biz соответственно: 92 711 640; 13 738 150; 9 325 078; 7 799 731; 2 207 631;
- российских доменов .рф, .ru и союзных .su: 778 298; 3 223 195; 92 775.

В инфраструктуре DNS насчитывается большое количество name-серверов, которые управляют базой данных доменных имен и предоставляют сервис DNS. Домены второго уровня обычно регистрируются за организацией на определенный срок (в среднем на один год).

Адреса транспортного уровня – Порты TCP/UDP

Для идентификации программ протоколы транспортного уровня (обычно это TCP и UDP) используют уникальные числовые значения – номера портов. Номера портов назначаются программам в соответствии с выполняемыми ими функциями на основе определенных стандартов.

Порты могут принимать значение от 0 до 65535 (два байта – 2^{16}) и разделены на три группы:

1. Общеизвестные порты (0 – 1023). Не должны использоваться без регистрации IANA (Internet Assigned Numbers Authority, Администрация адресного пространства Интернет). В большинстве случаев выделяются системным процессам или приложениям, запущенным привилегированными пользователями.

2. Зарегистрированные порты (1024 – 49151). Не должны использоваться без регистрации IANA. Выделяются процессам и приложениям, запущенным обычными пользователями.

3. Динамически выделяемые порты и/или порты, используемые внутри закрытых (private) сетей (49152 – 65535). Не могут быть зарегистрированы.

Первоначально список общеизвестных и зарезервированных портов был описан в RFC 1700. В настоящее время RFC 1700 «отменен» (в соответствии с RFC 3232). Перечень и назначение портов теперь приведен в on-line базе данных организации IANA, которая постоянно поддерживается в актуальном состоянии.

Список портов можно посмотреть на сайте: [http://www.iana.org / assignments/port-numbers](http://www.iana.org/assignments/port-numbers).

Локальная копия списка входит в установочный пакет сетевых операционных систем. Файл локальной копии списка обычно называется services. В системах Windows расположен в «C:\Windows\system32\drivers\etc», в UNIX-подобные ОС – в «/etc».

Пакеты TCP или UDP всегда содержат два поля номера порта: отправителя и получателя.

Список некоторых портов:

- 20, 21: FTP – Протокол передачи файлов (незащищенный).
- 22: SSH (Secure SHell). Применяется для безопасного входа в систему, безопасной пересылки файлов, безопасного удаленного доступа.
- 23: (telnet) – Применяется для передачи текстовых сообщений в незашифрованном виде, консоль терминала.
- 25: SMTP (Simple Mail Transfer Protocol). Используется для пересылки почтовых сообщений между серверами и от клиента серверу.
- 53: DNS. Служба доменных имен.
- 67, 68: (DHCP). Используется службой Dynamic Host Configuration Protocol для автоматического управления адресами, а также для удаленной загрузки бездисковых станций.

- 69: Trivial File Transfer Protocol (TFTP) – тривиальный FTP.
- 80, 8080: HTTP (Hypertext Transfer Protocol). Используется веб-браузерами.
- 110: POP3 (Post Office Protocol 3). Используется для передачи почты от сервера клиенту.
- 143: IMAP (Internet Message Access Protocol). Используется для передачи почты от сервера клиенту.
- 443: HTTP поверх TLS/SSL (HTTPS). Безопасный HTTP (шифрованный).
- 465: SMTP поверх SSL (SMTPS). Безопасный SMTP (шифрованный).
- 546, 547: DHCPv6. Служба DHCP для следующей версии протокола IP (IP версии 6).
- 666: Doom, шутер от первого лица.

Приложения взаимодействуют через сокеты.

Термин "сокет" (socket) означает одновременно библиотеку сетевых интерфейсов и оконечное устройство канала связи (точку связи), через которое процесс может передавать или получать данные. При создании сокета обычно указываются адрес хоста, номер порта и используемое семейство протоколов.

Адреса сетевого уровня – IPv4, IPv6

Адреса сетевого уровня сейчас нужно разделять на две группы: адрес по протоколу IP версии 4 (IPv4 или просто IP) и адрес по протоколу IP версии 6 (IPv6). IPv4 описан в RFC 791, IPv6 – в RFC 2460.

Каждый хост в сети на базе стека TCP/IP идентифицируется по уникальному цифровому IP-адресу (как минимум в рамках своей подсети).

IP-адрес представляет собой 32-разрядное двоичное число, записанное в виде четырех октетов (8 бит). Обычно IP-адрес представляется в виде четырёх десятичных чисел (от 0 до 255), разделённых точками. Это называется представлением в десятичной форме с разделением точками. Адрес также может быть представлен в шестнадцатеричной форме с разделением точками.

ричной или восьмеричной форме с точками. И иногда используют формы без точки, в которых адрес представлен в виде одного числа.

Адрес условно разделен на две части: адрес сети (подсети) и адрес (номер) хоста. Место деления частей обозначается числом через дробь. Например, адрес 192.168.1.10/24 расшифровывается: 24 бита выделено для адреса сети, остальное для адреса хоста в пределах подсети. Адрес сети обычно представляется первым доступным адресом в данной сети (192.168.1.0).

В случае изолированной сети IP-адрес хоста может быть выбран администратором произвольно. Однако обычно администраторы придерживаются общепринятых принципов адресации в соответствии со стандартами, размерами сети и ее сегментов.

Рассмотрим схему адресации для протокола IP (наиболее распространенного).

Адресное пространство (в соответствии с RFC 791) разделено на четыре класса IP-адресов. Четвертый класс был разделен еще на два: D, E (рис. 17). Класс адреса определяет, какие биты относятся к адресу сети, а какие – к адресу хоста. Также он определяет максимально возможное количество узлов в сети.

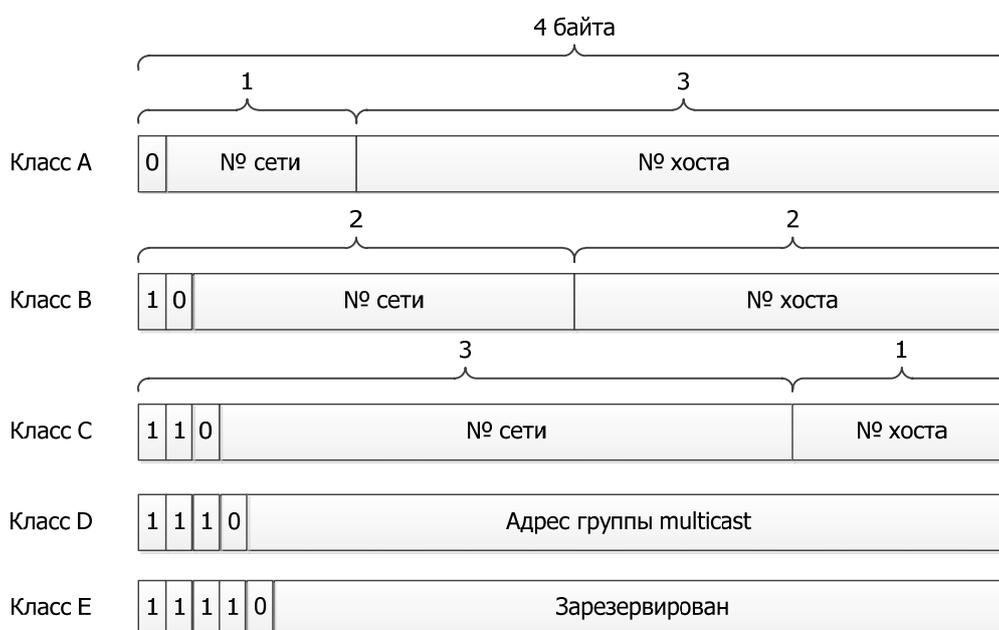


Рис. 17. Классы IP-адресов

Диапазон адресов, соответствующих каждому классу сетей, представлен в табл. 7.

Таблица 7

Классовое разделение адресного пространства

Класс	Количество сетей	Количество хостов в сети	Наименьший адрес	Наибольший адрес	Маска подсети
A	126 (2^7-2)	16,777,214 ($2^{24}-2$)	01.0.0.0	126.0.0.0	255.0.0.0
B	16,382 ($2^{14}-2$)	65,534 ($2^{16}-2$)	128.0.0.0	191.255.0.0	255.255.0.0
C	2,097,150 ($2^{21}-2$)	254 (2^8-2)	192.0.1.0	223.255.255.0	255.255.255.0
D	Не делится	-	224.0.0.0	239.255.255.255	-
E	Не делится	-	240.0.0.0	247.255.255.255	-

Первый адрес используется для обозначения, что это адрес сети. Последний адрес – широковещательная передача.

Изначально использовалась классовая адресация (INET, приведенная выше), но со второй половины 90-х гг. XX века она была вытеснена бесклассовой адресацией (CIDR), при которой количество адресов в сети определяется маской подсети и классы как таковые не учитываются. Однако на практике в основном используется классовая адресация. Бесклассовая адресация применяется на маршрутизаторах, так как позволяет существенно сократить размеры маршрутных таблиц.

Основные причины разделения сетей на подсети:

- Упрощение процесса администрирования. Каждая подсеть может администрироваться независимо (разными администраторами). Все подсети могут быть построены по одним принципам.
- Возможность использования различных технологий построения сетей (Ethernet, FDDI, Token Ring и т.д.) как проводных, так и беспроводных.
- Уменьшение общего количества адресов, так как в разных подсетях могут использоваться одинаковые адреса.
- Уменьшение перегрузки сети. Уменьшая количество хостов в сети, уменьшается объем трафика, циркулирующего в сети. Уменьшается объем широковещательной рассылки.

- Уменьшение количества глобальных сбоев. Сбои будут происходить в рамках подсетей, а в целом сеть будет продолжать функционирование.
- Усиление безопасности, так как возможно выделение подсетей и ограничение доступа к ним.
- Разделение трафика и управление качеством обслуживания. Выделение специального трафика (ip-телефония, видеоконференции и т.д.) в отдельные подсети позволяет повысить качество обслуживания.

Для вычисления параметров адреса в соответствии с INET можно воспользоваться калькулятором подсетей – <http://www.subnet-calculator.com/> или <http://opennet.ru/ipcalc.shtml>. Для вычисления параметров адреса в соответствии с CIDR можно воспользоваться калькулятором подсетей – <http://www.subnet-calculator.com/cidr.php>.

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов (RFC 3330). Некоторые из них представлены ниже:

- Если IP-адрес состоит только из нулей, то он обозначает адрес того хоста, который сгенерировал этот пакет.
- Если в поле адреса сети стоят нули, то по умолчанию считается, что этот хост принадлежит той же самой сети, что и хост, который отправил пакет.
- Если IP-адрес состоит только из единиц, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast).
- Если поле адреса хоста состоит из единиц, то пакет рассылается всем хостам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast). Ограниченный широковещательный IP-адрес и широковещательный IP-адрес ограничены либо сетью, к которой принадлежит хост – источник пакета, либо сетью, адрес которой указан в адресе назначения.
- Адреса 127.0.0.1/8 зарезервированы для организации обратной

связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

- 169.254.0.0/16. Link-Local Address – адреса сети, которые предназначены только для коммуникаций в пределах одного сегмента местной сети. Адреса link-local часто используются для автоматического конфигурирования сетевого адреса, в случаях, когда внешние источники информации об адресах сети недоступны.

- 192.0.2.0/24. Test-Net. Адреса выделены для использования в литературе.

- 198.18.0.0/15. Адреса выделены для тестирования производительности сетевых устройств.

- 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Адреса трех указанных диапазонов выделены для использования в частных сетях.

Стабильность работы сети Интернет базируется на уникальности IP-адресов. Следовательно, в глобальной сети не должно быть хостов с одинаковыми IP-адресами. Выделение адресов контролируется глобально. Такие адреса называются публичными. Количество IP-адресов ограничено и очень быстро истощается.

В 1994 г. IETF предложил выделить блок IP-адресов для частных сетей. Частные (private) сети, которые нуждались в IP, не требуя обеспечения связи с Интернетом, могли использовать адреса из выделенных блоков IP-адресов (по одному в каждом классе сети). Адреса в этом диапазоне не должны использоваться в качестве публичных адресов в сети Интернет.

Однако со временем потребовался доступ из частных сетей в публичные. Это достигается за счет механизма трансляции адресов (NAT). Network Address Translation (преобразование сетевых адресов) – механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

IP-адрес может быть:

- Статическим (постоянным), если он определен пользователем в настройках устройства и не может быть присвоен другому устройству. Также может назначаться автоматически при под-

ключении устройства к сети (при этом выставляется неограниченный интервал аренды).

- Динамическим (непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети (при этом он арендуется на ограниченный промежуток времени). Как правило, адрес выделяется устройству до завершения сеанса подключения.

- Виртуальным. Адрес устройства при использовании механизма NAT. NAT осуществляет трансляцию виртуального адреса в динамический или статический и обратно.

Не виртуальные IP-адреса называют реальными (прямыми, внешними, общественными, публичными, «белыми»). Обычно все статические IP-адреса являются таковыми.

Протокол IP использует дейтаграммный метод передачи, фрагментацию пакетов, разрешает отправителю задавать максимальное число маршрутизаторов (хопов), которые может пройти пакет.

Группа IETF (Internet Engineering Task Force, открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, которое занимается развитием протоколов и архитектуры Интернета) представила предложение по модернизации протокола IP. Протокол IPv6 оставляет основные принципы IPv4 неизменными, устраняя некоторые назревшие проблемы протокола IPv4.

Основные отличия протокола IPv6 от IPv4:

- Использование более длинных адресов. Версия 6 использует 128-битные адреса.

- Гибкий формат заголовка. Заголовок фиксированного размера с определенными полями в IPv4 заменен на базовый заголовок фиксированного формата плюс набор необязательных заголовков различного формата.

- Поддержка резервирования полосы пропускания. В IPv6 механизм резервирования пропускной способности заменяет механизм классов сервиса (QoS) версии IPv4.

- Поддержка расширяемости протокола. В протоколе разрешается поддержка дополнительных функций.

- Маршрутизаторы больше не разбивают пакет на части. Возможна передача пакетов до 4Гб.

- Обязательная поддержка протокола IPSec. IPSec (сокращение от IP Security) – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. В IPv4 она не обязательна.

Используемые в настоящее время протоколы и сервисы прикладного уровня перерабатываются под IPv6.

При распределении адресов в настоящее время рекомендуется использовать технологию VLSM (Variable Length Subnet Mask, переменной длины маски подсети).

Бесклассовая адресация (Classless InterDomain Routing, CIDR) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Бесклассовая адресация основана на переменной длине маски подсети (VLSM). Документ RFC 1009 от 1987 г. сформулировал, каким образом в сетях, состоящих из нескольких подсетей, можно использовать больше одной маски подсети.

При использовании метода VLSM вводится ряд новых правил распределения адресов, которые позволяют значительно уменьшить их расход. В данном случае разрешено применять к разным частям сети различные маски. Это позволяет в случае необходимости разделять сеть на меньшие части. Единственное требование заключается в том, чтобы диапазоны адресов в подсетях не перекрывали друг друга.

Общий алгоритм использования VLSM:

1. Сортировка подсетей по убыванию количества хостов в них.
2. Выбирается подсеть с максимальным количеством хостов (первая в списке). Определяется маска подсети, которая позволяет организовать подсеть с необходимым количеством адресов хостов (+2 адреса: адрес подсети и широковещательный).
3. Исходный диапазон адресов разбивается пропорционально на несколько частей в соответствии с вычисленной маской подсети.
4. Первый диапазон используется для выбранной подсети (первой в списке).

5. Выбирается следующая по списку подсеть. Если она занимает более половины следующего диапазона адресов, то ей выделяется данный диапазон, если менее половины, тогда для выбранного диапазона снова вычисляется минимально необходимая маска подсети.

6. Повтор п. 5, пока не будут израсходованы все диапазоны адресов для данной маски подсети.

7. Если распределены не все адреса, тогда переходим к следующему диапазону адресов и повторяем п. 5 – 7.

Обычно, чтобы избежать перекрытия адресов, операции выполняются в двоичной системе счисления.

Для вычисления параметров подсетей можно воспользоваться VLSM Calculator – <http://www.vlsm-calc.net> (рис. 18).

Исходная сеть	192.168.0.0/24	
Подсети	Название	Размер
	A	100
	B	25
	C	46
	Количество подсетей:	3 <input type="button" value="Изменить"/>
	Упорядочить результаты:	по размеру <input type="button" value="v"/>
<input type="button" value="Отправить"/>		

Разбиение выполнено успешно

Исходная сеть: 192.168.0.0/24
 Доступно адресов в исходной сети: 254
 Количество необходимых IP-адресов: 171
 Available IP addresses in allocated subnets: 218
 Около 88% доступного адресного пространства исходной сети использовано
 Около 78% адресного пространства разбитой сети использовано

Название подсети	Размер	Выделенный размер	Адрес	Маска	Десятичная маска	Диапазон доступных адресов	Широковещание
A	100	126	192.168.0.0	/25	255.255.255.128	192.168.0.1 - 192.168.0.126	192.168.0.127
C	46	62	192.168.0.128	/26	255.255.255.192	192.168.0.129 - 192.168.0.190	192.168.0.191
B	25	30	192.168.0.192	/27	255.255.255.224	192.168.0.193 - 192.168.0.222	192.168.0.223

Рис. 18. Расчет адресов при использовании VLSM Calculator

Адреса канального уровня – MAC-адреса

Прежде чем данные смогут быть отправлены на какой-нибудь компьютер, отправитель должен знать аппаратный адрес хоста получателя.

Для преобразования IP-адресов в адреса канального уровня используются протоколы ARP и RARP:

- Протокол ARP (Address Resolution Protocol – Протокол определения адреса, RFC 826) предназначен для определения аппаратного (MAC) адреса компьютера в сети по его IP-адресу. Перед поиском аппаратного адреса в сети сначала проверяется наличие адреса в локальном КЭШе. Если уже были обращения по данному IP-адресу, то информация о MAC-адресе должна сохраниться в кэше. Если ничего не найдено, то в сеть посылается широковещательный запрос, который получают все компьютеры сети. Тот, кому принадлежит искомый IP, ответит на запрос, указав свой MAC-адрес.

- Протокол RARP (Reverse Address Resolution Protocol – Обратный протокол преобразования адресов) – определяет IP-адрес по известному MAC-адресу.

MAC-адрес (Media Access Control – управление доступом к среде) – это уникальный идентификатор, присваиваемый каждой единице сетевого оборудования. Большинство сетевых протоколов канального уровня используют одно из трёх пространств MAC-адресов, управляемых IEEE. Наиболее распространённым является MAC-48 (рис. 19). Адреса типа MAC-48 используются в таких технологиях, как Ethernet, Token ring, FDDI, WiMAX и других и состоят из 48 бит.



Рис. 19. Структура MAC-48

На рис. 19:

- Поле I/G – флаг индивидуального или группового адреса: 0 – адрес является индивидуальным адресом; 1 – адрес мультикастинговый.

- Поле UL – флаг универсального или местного управления (определяет механизм присвоения адреса сетевому интерфейсу): 0 – адреса присваиваются изготовителем; 1 – адреса присваиваются локально администратором.

- Поле OUI (organizationally unique identifier) – идентификатор производителя сетевого интерфейса. Каждому производителю присваивается один или несколько OUI.

- Поле OUA (organizationally unique address) – уникальный адрес интерфейса. Производитель несет ответственность за уникальность адреса. Двух интерфейсов одного и того же производителя с идентичными номерами не должно существовать. Размер поля позволяет произвести примерно 16 миллионов интерфейсов.

Комбинация OUI и OUA составляет UAA (universally administrated address = IEEE-адрес).

Узнать производителя по MAC-адресу можно здесь – http://www.coffer.com/mac_find/?string=/.

На http://www.coffer.com/mac_info/ размещена подробная информация о том, как узнать MAC-адрес для различных операционных систем.

MAC-адрес может быть легко изменен практически в любой современной операционной системе. Обычно адрес, заданный драйвером устройства (в операционной системе), имеет приоритет над адресом, заданным производителем. Подробнее о смене адреса можно узнать из <http://www.tech-faq.com/how-to-change-a-mac-address.html>.

При смене MAC-адреса следует учитывать следующее: многие промежуточные сетевые устройства (маршрутизаторы, точки доступа, коммутаторы и т.д.) запоминают hosts по MAC-адресам, предоставляя или ограничивая доступ к определенным ресурсам и сервисам.

Информацию об используемых адресах хоста можно получить с помощью утилит ipconfig (для ОС Windows) и ifconfig (для Unix-подобных ОС). Утилиты могут выдавать краткую и развернутую информацию о сетевых подключениях и их настройках.

Документирование вычислительной сети

Документирование сети обеспечивает ускорение процесса поиска неисправностей, ускорение процесса модернизации (расширения) сети, упрощение процесса администрирования.

Физическая топология описывается диаграммой, которая представляет собой модель сетевой топологии без точного указания всех деталей прокладки кабельной системы (схемы прокладки кабелей рекомендуется отражать на планах этажей, планах электрических сетей).

Элементы логической диаграммы:

- точное расположение монтажных шкафов (наименование кабинетов, ответственные лица);
- тип и количество кабелей, включая запасные кабели для увеличения полосы пропускания между монтажными шкафами;
- подробную документацию на все кабельные трассы, идентификационные номера и порты на вертикальных и горизонтальных соединениях.

Следующим шагом является документирование схемы IP-адресации. Рекомендуется составить описание для каждого участка сети. Нужно придерживаться однотипного распределения адресного пространства, зарезервировать определенный диапазон адресов для служебных целей.

Обычно начальные адреса подсети используются для управления промежуточными сетевыми устройствами (маршрутизаторы, шлюзы, точки доступа и т.д.). Также в данном диапазоне адресов выделяются адреса для серверов. Адреса в конце диапазона адресов подсети обычно выделяют для общих сетевых ресурсов, в качестве которых обычно выступают сетевые принтеры. Пример распределения адресов представлен в табл. 8.

Таблица 8

Распределение диапазонов адресов (подсеть с маской /24)

Логический адрес	Устройство
х.х.х.1 - х.х.х.10	Маршрутизаторы
х.х.х.11 - х.х.х.20	Управляемые коммутаторы
х.х.х.21 - х.х.х.30	Серверы организации
х.х.х.31 - х.х.х.40	Серверы рабочих групп организации
х.х.х.41 - х.х.х.254	Хосты (рабочие места)

Схема распределения адресов должна быть масштабируемой (учитывать возможное дальнейшее расширение сети) и не должна содержать противоречий внутри всей сети. Рекомендуется построить таблицы разделения адресов для каждой подсети и сети в целом.

Следующий шаг – создание физической карты. На карте отражаются специфические характеристики соединения промежуточного и окончного оборудования. Физическая карта является основой для поиска неисправностей на физическом уровне. Также целесообразно составить кабельные журналы.

Документация по одному этапу может частично пересекаться с документацией по другому. Указанный перечень документов может быть дополнен.

Общий принцип подготовки документации – ее должно быть достаточно для точного воссоздания сети в случае ее разрушения или поломки.

ПРИНЦИПЫ КОММУТАЦИИ И МАРШРУТИЗАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Коммутация реализована аппаратно на втором уровне модели OSI, таким образом, в процессе коммутации используются MAC-адреса адаптеров хостов.

Коммутаторы работают очень быстро, поскольку не пользуются информацией из заголовков сетевого уровня, а анализируют аппаратные адреса при принятии решения о перенаправлении на другой порт или об отбросе пакета (уничтожении).

Особенности коммутации: аппаратная реализация элементов коммутатора; высокая скорость обработки пакетов; низкая стоимость устройства.

Высокая скорость и эффективность коммутации определяется тем, что не производится изменений в пакетах данных, так как все модификации связаны с фреймами и, следовательно, процесс коммутации выполняется быстрее и менее подвержен ошибкам, чем при маршрутизации.

Коммутация используется в связях между рабочими группами, при сегментации сети, разделении доменов конфликтов.

Применение коммутации позволяет выделить каждому пользователю максимальную полосу пропускания, поскольку каждая связь интерфейса хоста пользователя и коммутатора образует собственный домен конфликтов. Основным недостатком коммутации заключается в том, что коммутаторы не способны контролировать широковещательные рассылки.

Коммутатор выполняет три основные функции при обработке пакетов:

- **Изучение адресов.** Коммутаторы запоминают MAC-адрес источника каждого полученного интерфейсом кадра и сохраняют эту информацию в своей базе данных MAC-адресов (каждый адрес связан с определенным портом коммутатора). После выключения питания коммутатора таблица MAC-адресов очищается. Коммутатор не может принять самостоятельного решения о перенаправлении кадров, пока не получит информацию о местонахождении хоста назначения. Это возможно только после получения пакета от хоста назначения (коммутатор извлечет адрес источника из полученного кадра и поместит его в таблицу MAC-адреса, связав с необходимым интерфейсом). Если в таблице MAC-адресов присутствует адрес хоста назначения, то возможно установление соединения типа "точка – точка" и автоматическое перенаправление кадра с порта-источника на порт назначения и обратно (так как адрес источника уже известен). Если соединение еще не установлено, то кадры рассылаются на все интерфейсы, кроме того, с которого он пришел. Если в течение определенного интервала времени при передаче хосты не откликаются, то соответствующие записи в таблице MAC-адресов удаляются (таким образом, поддерживается корректность таблицы адресов).
- **Решение о пересылке.** Когда интерфейс коммутатора получает кадр, проводится поиск MAC-адреса хоста назначения и соответствующего ему порта (интерфейс) коммутатора. Если порт определен, то кадр передается далее, при этом остальные порты ком-

мутатора свободны и могут осуществлять прием и передачу других кадров. Этот процесс называется фильтрацией кадров (frame filtering). Если MAC-адрес не известен, то кадр отсылается широковещательной рассылкой на все активные интерфейсы коммутатора (за исключением того, на который пришел). Если один из хостов или одно из сетевых устройств откликается (коммутаторы могут каскадироваться) на широковещательную рассылку, происходит обновление базы данных MAC-адресов.

- **Исключение зацикливания.** Если между коммутаторами в целях избыточности проложено несколько путей, то возможно зацикливание при передаче информации. Протокол STP (Spanning Tree Protocol – протокол покрывающего дерева) позволяет исключить зацикливание пакетов в сети при сохранении избыточности. Избыточность может быть полезной в некоторых случаях, например, наличие дополнительных линий связи помогает предотвратить отказ сети при выходе из строя одной из них. Зацикливание также возможно при использовании неправильно построенной топологии компьютерной сети.

Наиболее серьезные последствия зацикливания:

1. Переполнение коммутатора бесконечными широковещательными рассылками (шторм широковещательных рассылок, broadcast storm).
2. Хост может получить несколько копий одного кадра, поскольку кадры одновременно поступают из разных сегментов.
3. Таблица MAC-адресов не может быть заполнена корректно, поскольку коммутатор может получить ответы от одного хоста по нескольким линиям связям. Коммутатор будет постоянно обновлять таблицу MAC-адресов на основе меняющихся сведений о местоположении адреса источника (этот процесс называется "хлопаньем" (thrashing) MAC-таблицы).
4. Появление нескольких зацикленных путей в компьютерной сети. Зацикливание одного пути порождает зацикливание в других путях, при этом шторм широковещательных рассылок будет усиливаться до такой степени, что произойдет полная остановка работы в сети.

Типы коммутаторов

Задержка при коммутации пакетов зависит от выбранного режима работы коммутатора. Существуют три режима работы коммутатора:

1. Store and forward (сохранить и передать). В буфер коммутатора записывается весь кадр данных, проверяется CRC, а затем в таблице MAC-адресов осуществляется поиск адреса хоста назначения. В таком режиме коммутатор полностью копирует кадр в собственный встроенный буфер, следовательно, задержка коммутации зависит от длины кадра. При ошибке CRC кадр отбрасывается. Также отбрасываются слишком короткие (менее 64 байтов) или слишком длинные (более 1518 байтов) кадры.

2. Cut-through (сквозной). Сразу после получения адреса хоста назначения (еще до завершения приема всего кадра) коммутатор осуществляет его поиск в таблице MAC-адресов. В этом режиме в собственный встроенный буфер копируется только адрес хоста назначения (первые шесть байтов после преамбулы). Сквозные коммутаторы обеспечивают низкую задержку, поскольку начинают пересылку кадра сразу после чтения адреса хоста назначения и определения выходного интерфейса.

3. Fragment Free (без фрагментации). Иногда называют модифицированным сквозным режимом (modified cut-through). Производится проверка первых 64 байтов кадра (из-за возможных конфликтов в сегменте). Если обнаруживается ошибка в принятом пакете, то она всегда проявляется в первых 64 байтах. Безфрагментный режим обеспечивает лучшую проверку на ошибки по сравнению со сквозным режимом (в частности, за счет того, что не происходит увеличения задержки на длинных кадрах).

Маршрутизация

Маршрутизация служит для приема пакета от одного хоста или сетевого устройства и передачи его по компьютерной сети другому устройству через другие сети. Если в сети нет маршрутизаторов, то не поддерживается и маршрутизация.

Для маршрутизации пакетов необходима следующая информация:

- адрес хоста назначения;
- информация о соседних маршрутизаторах, от которых он может узнать информацию об удаленных сетях;
- доступные пути ко всем удаленным сетям;
- наилучший путь до каждой удаленной сети;
- методы обслуживания и проверки информации о маршрутизации.

Маршрутизатор узнает об удаленных сетях от соседних маршрутизаторов (автоматически) или от сетевого администратора (задается вручную). Данная информация используется для построения маршрутных таблиц, в которых описываются маршруты (порядок прохождения маршрутизаторов) до удаленных сетей.

Если сегмент сети подключен непосредственно к маршрутизатору, он уже знает, как направить пакет в эту подсеть. Если же сеть не подключена напрямую, маршрутизатор должен узнать (изучить) пути доступа к удаленной сети с помощью статической маршрутизации (вводится администратором) или с помощью динамической маршрутизации. Динамическая маршрутизация – это процесс протокола маршрутизации, определяющий взаимодействие маршрутизатора с соседними маршрутизаторами.

При динамической маршрутизации сведения о каждой изученной сети автоматически обновляются, если происходит изменение в процедуре доступа к данной сети. При статической маршрутизации ответственность за поддержание сведений о маршрутах (их актуальности) ложится на администратора.

Статическая маршрутизация – это процесс ввода администратором сети путей в таблицы маршрутизации всех маршрутизаторов.

Преимущества статической маршрутизации:

- минимальная нагрузка на процессор маршрутизатора;
- служебная информация (маршрутная) не передается по компьютерной сети, следовательно, снижается загрузка сети и повышается уровень защиты.

Недостатки статической маршрутизации:

- администратор должен хорошо понимать особенности сети и правильно настроить каждый маршрутизатор;
- при добавлении (или удалении) маршрутизатора в сети, администратору необходимо добавить новые пути (или обновить старые) во все маршрутизаторы.

Статическая маршрутизация неприменима в крупных сетях, поскольку требует большого объема работы.

Утилита route (MS Windows) выводит на экран и изменяет записи в локальной таблице IP-маршрутизации хоста.

Маршрутизация по умолчанию используется для пересылки пакетов в удаленную сеть назначения, которая не отмечена в таблице маршрутизации через маршрутизатор следующего участка.

Можно использовать маршрутизацию по умолчанию в тупиковых сетях (stub network), т.е. сетях, имеющих только один выходной порт. Для настройки пути по умолчанию в сетевом адресе и маске статического пути используются символы-заменители (wildcards – «инверсная маска сети»). Маршрутизация по умолчанию в некоторых случаях необходима, так как когда маршрутизатор получает пакет для подсети назначения, которой нет в таблице маршрутизации, он будет его отбрасывать (удалять).

Динамическая маршрутизация – это процесс использования протокола для поиска и обновления таблиц маршрутизации. Для работы протоколов динамической маршрутизации требуются ресурсы процессора маршрутизатора и полосы пропускания линий связи. Наиболее распространённым протоколом является протокол RIP – Routing Information Protocol (протокол информации о маршрутизации).

Во время настройки протокола маршрутизации следует учитывать административные расстояния (AD, administrative distance). Значение данного параметра определяет степень доверия к информации о маршрутизации, полученной маршрутизатором.

Значение AD представляется целым числом в диапазоне от 0 до 255, где 0 означает наибольшее доверие, а 255 – запрет передачи трафика по данному маршруту.

В табл. 9 представлены некоторые значения административных

расстояний (по умолчанию), которые используются маршрутизаторами Cisco в процессе время выбора маршрута (пути) до удаленной сети.

Таблица 9

Административные расстояния (по умолчанию)

Источник пути	Расстояние
Подключенный интерфейс	0
Статический маршрут	1
Протокол BGP	20
Внутренний протокол EIGRP	90
Протокол IGRP	100
Протокол OSPF	110
Протокол IS-IS	115
Протокол RIP	120
Внешний BGRP	170
Внешний протокол EIGRP	190
Неизвестный	255

Если подсеть подключена непосредственно к маршрутизатору, то всегда используется интерфейс подключения. Если администратор установит статический путь, маршрутизатор будет предпочитать его всем другим путям к той же сети.

Существуют три класса протоколов маршрутизации: вектора расстояния (Distance vector); состояния связи (Link state) и гибридный (Hybrid).

Протоколы маршрутизации по вектору расстояния используют для поиска наилучшего пути до удаленной сети. Каждое перенаправление пакета маршрутизатором называется участком (hop). Счетчик участков увеличивается при прохождении пакета через маршрутизатор. Наилучшим считается путь к удаленной сети с наименьшим количеством участков. Примерами протоколов маршрутизации по вектору расстояния являются RIP и IGRP.

Алгоритм маршрутизации по вектору расстояния предполагает пересылку всей таблицы маршрутизации соседним устройствам. После этого маршрутизатор объединяет полученную таблицу с соб-

ственной таблицей маршрутизации для построения полной карты сети. В сети может существовать несколько путей к одной удаленной сети. В данном случае маршруты сравниваются по административным расстояниям и другим метрикам (значениям, характеризующим канал связи). Некоторые протоколы могут использовать одновременно несколько путей с целью балансирования нагрузки (протокол RIP способен сбалансировать нагрузку по шести каналам связи).

Протокол "маршрутизация по вектору расстояния" отслеживает все изменения в объединенной сети за счет периодической широковещательной рассылки обновлений во все активные интерфейсы маршрутизатора. Так как на рассылку таблиц всеми маршрутизаторами необходимо время, то до завершения процесса возможны ошибки при маршрутизации и возникновение петель (routing loop).

Частично решить проблему возникновения петель и ускорить процесс обмена маршрутной информацией позволяет ограничение на максимальное значение счетчика участков. Например, протокол RIP определяет максимум 15 участков (любой путь с количеством участков 16 считается недостоверным и недостижимым).

Также в протоколе может применяться метод деления горизонта (split horizon). При данном методе информация о маршрутизации не может передаваться в обратном направлении. Таким образом, деление горизонта не позволит маршрутизатору В послать обновление обратно в маршрутизатор А, если оно было получено от маршрутизатора А.

Протоколы класса состояния связи (Link state) обычно используют три таблицы в процессе маршрутизации. Одна из таблиц отражает состояние непосредственно подключенных соседних маршрутизаторов, вторая предназначена для хранения сведений о топологии всей сети, а третья является таблицей маршрутизации. Для выполнения маршрутизации используются специальные сообщения «объявления о состоянии канала» (link-state advertisements, LSA).

Устройство, действующее по протоколу состояния связи, имеет больше сведений о сети, чем любой протокол вектора расстояния. Пример протокола состояния связи – протокол OSPF (Open Shortest Path First, открой кратчайший путь первым).

- В режиме исследования сети выполняются следующие операции:
- маршрутизаторы обмениваются друг с другом LSA-сообщениями (в первую очередь с соседями);
 - маршрутизаторы параллельно друг с другом создают топологическую базу данных, содержащую все LSA-сообщения;
 - маршрутизатор на основе SPF-алгоритма вычисляет достижимость сетей, определяя кратчайший путь до каждой сети, где применяется протокол маршрутизации с учетом состояния канала связи;
 - маршрутизатор создает логическую топологию кратчайших путей в виде SPF-дерева, помещая себя в корень (SPF-дерево содержит пути от маршрутизатора до всех пунктов назначения);
 - наилучшие пути (в SPF-дереве) переносятся в таблицу маршрутизации.

Для использования протоколов маршрутизации данного класса необходим большой объем ресурсов, доступных на маршрутизаторе.

При больших размерах сети возможны ситуации, когда в одних частях сети маршрутные таблицы будут строиться быстрее, чем в других, и могут возникнуть проблемы с маршрутизацией.

Гибридный (Hybrid) протокол маршрутизации использует отдельные характеристики протоколов состояния связи и вектора расстояния (например EIGRP). Для определения наилучших путей до сетей назначения в протоколе сбалансированной гибридной маршрутизации применяются векторы расстояния с более точной метрикой. Отличается от большинства протоколов маршрутизации по вектору расстояния тем, что обновление маршрутной информации инициируется фактом изменения топологии.

Протоколы, относящиеся к типу сбалансированной гибридной маршрутизации, сходятся быстрее, приближаясь по этому показателю к протоколам маршрутизации с учетом состояния канала связи. Однако они отличаются от них меньшим потреблением таких ресурсов, как ширина полосы пропускания, объем памяти и меньшими накладными расходами процессора маршрутизатора.

Не существует единого способа конфигурации протоколов марш-

рутизации. Эта задача всегда решается с учетом особенностей конкретной сети.

Виртуальные локальные сети (Virtual LAN)

При использовании коммутации появилась возможность проектировать большие по размеру сети за счет уменьшения размера домена конфликтов и увеличения длины кабелей. В то же время увеличение количества пользователей (устройств) привело к увеличению количества широковещательных пакетов. Любой широковещательный пакет пересылается всем устройствам, вне зависимости от того, нужно ли устройству принимать эти данные. На его обработку тратятся ресурсы и время. Исключить широковещательную рассылку невозможно, так как она лежит в основе многих используемых протоколов.

Создание виртуальной локальной сети VLAN помогает решить многие проблемы «плоской» коммутации. VLAN может быть развернута на базе коммутаторов при относительно небольших затратах по сравнению с подходом деления на подсети при использовании маршрутизаторов. Все устройства сети VLAN являются членами одного широковещательного домена и получают все широковещательные рассылки. По умолчанию широковещательные рассылки блокируются на всех портах коммутатора, которые не являются членами выбранной сети VLAN. Когда сеть VLAN становится очень большой, можно сформировать новые сети VLAN, не позволив широковещательным рассылкам занимать полосу пропускания. Чем меньше пользователей в сети VLAN, тем на меньшее количество пользователей действуют широковещательные рассылки.

Применение VLAN позволяет повысить уровень защиты в сети за счет изоляции VLAN сетей друг от друга (в обычном случае это реализуется маршрутизаторами). При использовании VLAN можно накладывать ограничения на подключаемые к коммутатору хосты по аппаратным адресам, протоколам и сетевым приложениям.

Хосты в каждой сети VLAN могут взаимодействовать только друг с другом. Взаимодействие между сетями VLAN происходит через устройство 3-го уровня модели OSI (маршрутизатор).

Статические сети VLAN являются типичным способом формирования подобных сетей и отличаются высокой безопасностью. Присвоенные сети VLAN порты коммутатора всегда сохраняют свое состояние, пока администратор не выполнит новое присваивание портов. Этот тип VLAN легко конфигурировать и отслеживать.

Динамические сети VLAN автоматически осуществляют присваивание хостов. В данном случае возможно формирование динамических VLAN на основе MAC-адресов MAC, используемых протоколов и сетевых приложений. Это упрощает администрирование. Например, если пользователь перемещается в другое место сети, порт коммутатора будет автоматически присвоен в нужную сеть VLAN.

Так как сеть VLAN может распространяться на несколько соединенных коммутаторов, то для определения принадлежности кадра к некоторой сети VLAN используется маркирование кадров (frame tagging). Маркирование предполагает присваивание кадрам уникального идентификатора, определенного пользователем, который часто называют присваиванием VLAN ID или присваиванием цвета.

Существует несколько протоколов отслеживания кадров VLAN:

- Протокол ISL (Inter-Switch Link – протокол связи между коммутаторами) лицензирован для коммутаторов Cisco и используется только в сетях FastEthernet и Gigabit Ethernet. Предназначен для передачи информации о принадлежности трафика к VLAN. ISL предполагает инкапсуляцию исходного кадра в кадр собственного формата с добавлением заголовка, в котором содержится информация о принадлежности трафика к определенной VLAN. Может использоваться только на оборудовании, в котором реализована поддержка протокола ISL.
- Протокол IEEE 802.1q. Создан институтом IEEE в качестве стандартного метода маркирования кадров VLAN. Предполагает вставку в кадр дополнительного поля для идентификации VLAN.
- Протокол LANE. Протокол эмуляции локальной сети LANE (LAN emulation) служит для взаимодействия нескольких VLAN поверх ATM.

- Протокол IEEE 802.10. Позволяет пересылать информацию VLAN поверх FDDI.

Хосты в сети VLAN находятся в собственном ширококвещательном домене и свободно взаимодействуют друг с другом. Для взаимодействия хостов или любых других устройств из разных сетей VLAN необходимы устройства 3-го уровня модели OSI. Можно использовать маршрутизатор, имеющий физические интерфейсы в каждой сети VLAN, либо маршрутизатор с поддержкой маршрутизации по протоколу отслеживания кадров VLAN.

СТРУКТУРИРОВАННЫЕ КАБЕЛЬНЫЕ СИСТЕМЫ

Топология современных локальных сетей стала практически независимой от применяемых технологий физической передачи данных, что обусловило появление концепции СКС (структурированных кабельных систем, Structured Cabling System).

Концепция является основой создания коммуникационной инфраструктуры зданий, насыщенных компьютерной техникой. В структурированную кабельную систему могут входить системы пожарной, охранной сигнализации, телевизионного вещания и пр.

В России разработка СКС должна осуществляться в соответствии с ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования», введенным в действие с 01.01.2010.

Согласно концепции СКС по всей площади здания, на которой потенциально могут располагаться рабочие места (Work area), устанавливаются телекоммуникационные розетки. Каждое рабочее место рекомендуется оборудовать минимум парой розеток. От каждой абонентской розетки прокладываются кабели к телекоммуникационной или аппаратной (коммуникационные центры), где подключаются к горизонтальному кроссу. Кабели от рабочих мест в таком случае называют горизонтальными, хотя фактически они могут иметь и вертикальные участки.

Горизонтальные кабели не должны по длине превышать 90 м.

Оставшаяся длина кабеля (10 метров) используется для кроссировки и подключения рабочих мест к розеткам. Эти шнуры называют патч-кордами (Patch cords).

Коммуникационные центры связываются между собой магистральными линиями, которые называют вертикальными.

В общем виде коммутация должна обеспечивать возможность относительно произвольного подключения абонентских розеток к портам коммуникационного оборудования. При этом все переключения не должны механически затрагивать стационарные кабели горизонтальной кабельной системы.

Категория (Category) витой пары определяет частотный диапазон, в котором ее применение эффективно.

Витая пара может быть:

- STP, Shielded Twisted Pair – экранированная витая пара;
- UTP (Unshielded Twisted Pair) – неэкранированная витая пара;
- ScTP (Screened Twisted Pair) – кабель, в котором каждая пара заключена в отдельный экран;
- FTP (Foilled Twisted Pair) – кабель, в котором витые пары заключены в общий экран из фольги;
- PiMF (Pair in Metal Foil) – кабель, в котором каждая пара завернута в полосу металлической фольги, а все пары еще в общем экране.

Экранированный кабель дороже неэкранированного, но при корректном заземлении экрана обеспечивает лучшую защиту, в случае некорректного заземления возможен обратный результат. Кабели могут иметь различные номиналы сопротивления, которые должны соответствовать сопротивлению соединяемого ими оборудования. Кабели различаются по диаметру (калибру). Наиболее распространенный калибр – 24 AWG.

На концах кабеля монтируются коннекторы. Коннектор обеспечивает механическую фиксацию и электрический контакт. Как и кабели, они классифицируются по категориям, определяющим диапазон рабочих частот. Для витой пары широко применяют модульные разъемы (Modular Jack), известные под названием RJ-45: розетки (Outlet,

Jack) и вилки (Plug). Для экранированной проводки розетки и вилки должны также иметь экраны.

Схемы раскладки контактов в коннекторах и розетках, а также цветовая маркировка проводов стандартизованы. Каждая пара представляется двумя проводами, обозначаемыми Tip (TD) и Ring (RD) (условно – прямой и обратный провода), для которых определены цвет изоляции и номер контакта разъема.

Существует несколько стандартов, в основном различающиеся шириной, количеством используемых контактов и раскладкой пар проводов (рис. 20, табл. 10).

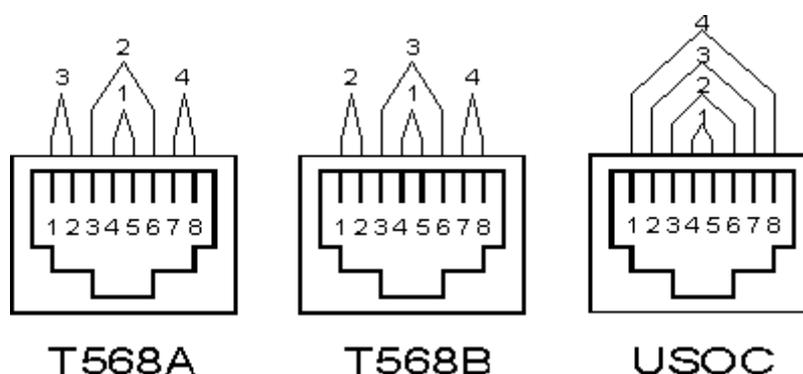


Рис. 20. Раскладка проводов (вид на розетку), снизу подписаны используемые стандарты

Таблица 10

Раскладка пар проводов по цвету

T568A			T568B		
№ п/п	Цвет	Пара	№ п/п	Цвет	Пара
1	Бело-зеленый	3	1	Оранжевый	2
2	Зеленый	3	2	Бело-оранжевый	2
3	Бело-оранжевый	2	3	Бело-зеленый	3
4	Синий	1	4	Синий	1
5	Бело-синий	1	5	Бело-синий	1
6	Оранжевый	2	6	Зеленый	3
7	Бело-коричневый	4	7	Бело-коричневый	4
8	Коричневый	4	8	Коричневый	4

При монтаже СКС рекомендуется использовать раскладку EIA/TIA-568A (сокращенно T568A) или EIA/TIA-568B (сокращенно T568B).

Для соединения оборудования используется один из двух типов кабелей: прямой (straight-through) или перекрестный (crossover).

Прямой кабель предполагает одинаковую раскладку проводов на обоих концах кабеля. На рис. 21 показано распределение по контактам для такого кабеля.

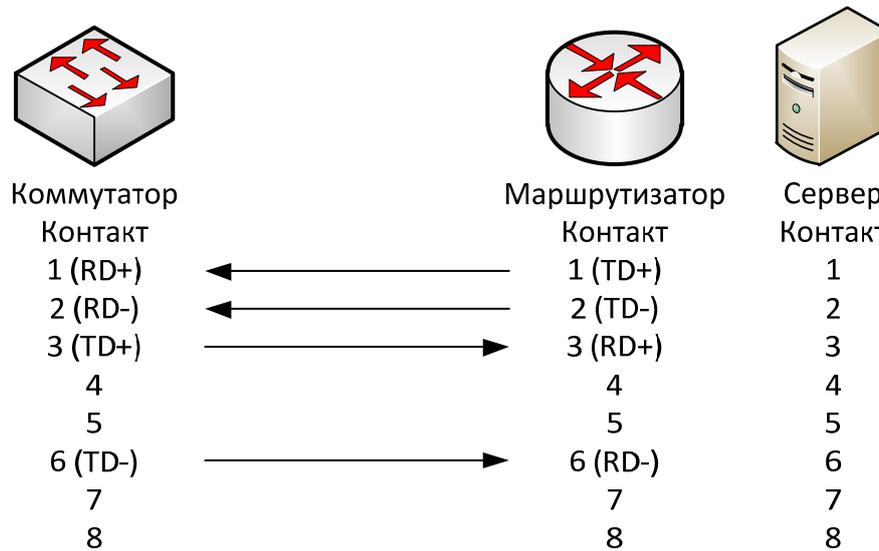


Рис. 21. Схема раскладки проводов кабеля straight-through

Прямой кабель используется в следующих случаях:

- для подключения маршрутизатора к коммутатору (концентратору);
- подключения сервера к коммутатору (концентратору);
- подключения рабочей станции к коммутатору (концентратору).

В общем случае прямой кабель используется для соединения оборудования различного типа.

В перекрестном кабеле провода "перехлестнуты" на концах кабеля. На рис. 22 показана схема раскладки проводов перекрестного кабеля. В данном случае 1-й контакт на одной стороне кабеля соединен с 3-м контактом на другой стороне, а 2-й контакт соединен с 6-м.

Перекрестный кабель используется в следующих случаях:

- для подключения по исходящим (каскадным) связям (uplink) между коммутаторами;
- подключения концентратора к коммутатору, концентратора к другому концентратору;

- подключения маршрутизатора к другому маршрутизатору;
- соединения двух ПК без использования концентратора или коммутатора.

В общем случае перекрестный кабель используется для соединения оборудования одного типа.

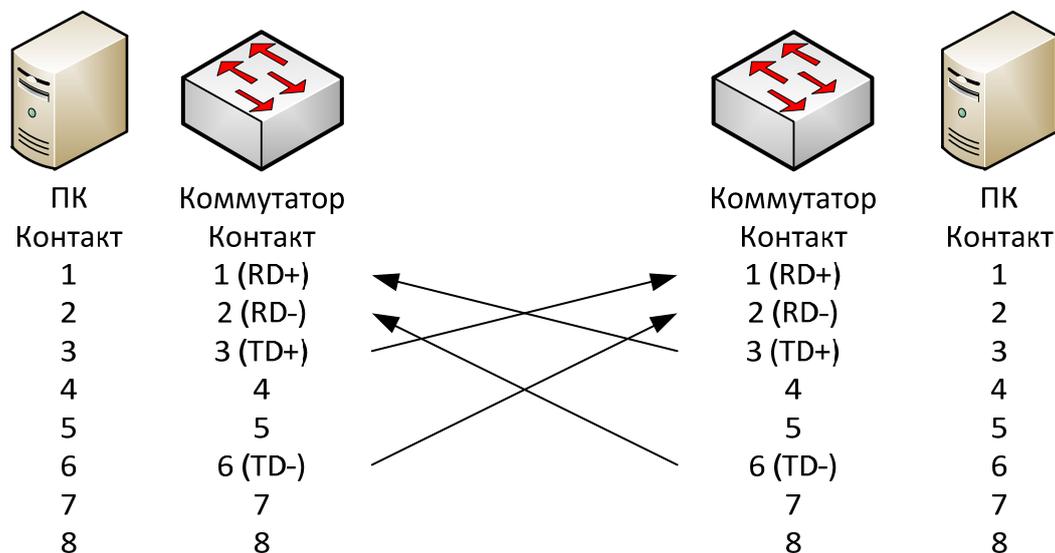


Рис. 22. Схема раскладки проводов кабеля crossover

Следует отметить, что для обеспечения скорости передачи в 1 Гб/с (и выше) необходимо использовать все четыре пары кабеля, для 100 Мб/с достаточно двух пар (таким образом, возможно подключение по одному кабелю сразу двух розеток).

Сейчас существует достаточно большое количество оборудования различных производителей, которое может самостоятельно определять используемую схему раскладки. Поэтому соблюдение схемы раскладки становится фактически рекомендацией, нежели стандартом.

Некоторые дополнительные правила построения горизонтальной системы СКС:

- к каждой розетке рекомендуется подводить свой кабель (для независимости сетевых приложений);
- при разделке концов кабеля не допускается расплетение пары больше чем на 1 см;

- по внешнему виду (цвету шнуров или колпачков) прямые кабели должны отличаться от перекрестных;
- шнуры должны быть подписаны на обоих концах (как и порты коммутационного оборудования).

Монтаж разъемов RJ-45

Монтаж коннектора осуществляется по следующей схеме (рис. 23).

Резаком, встроенным в обжимной инструмент, аккуратно обрежьте конец кабеля. Снимите изоляцию с кабеля примерно 2 – 3 см от обрезанного конца.

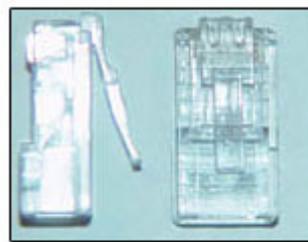


Рис. 23. Коннектор RJ-45

Снимите изолирующее покрытие и расплетите жилы (рис. 24, а). Отсортируйте пары по цвету в соответствии с рекомендациями стандартов. Выровняйте жилы в одну линию (рис. 24, б), отрежьте лишнюю длину проводов, оставив примерно сантиметр-полтора до изоляции.

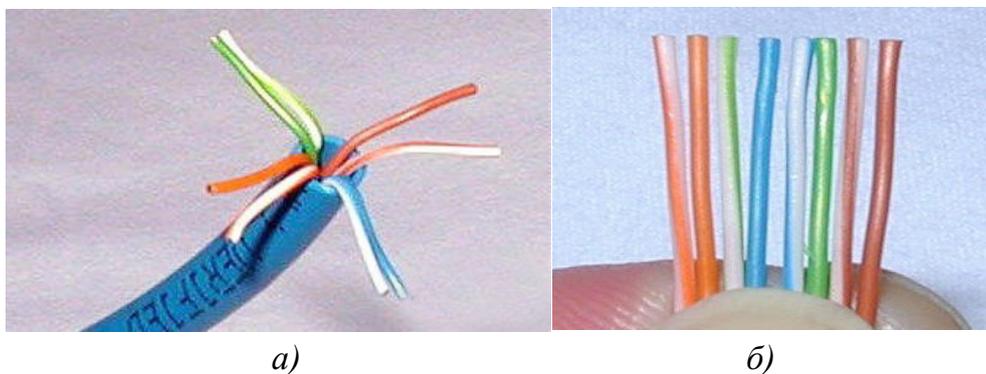


Рис. 24. Раскладка жил кабеля по цвету
 а – расплетение жил кабеля;
 б – раскладка жил и обрезка

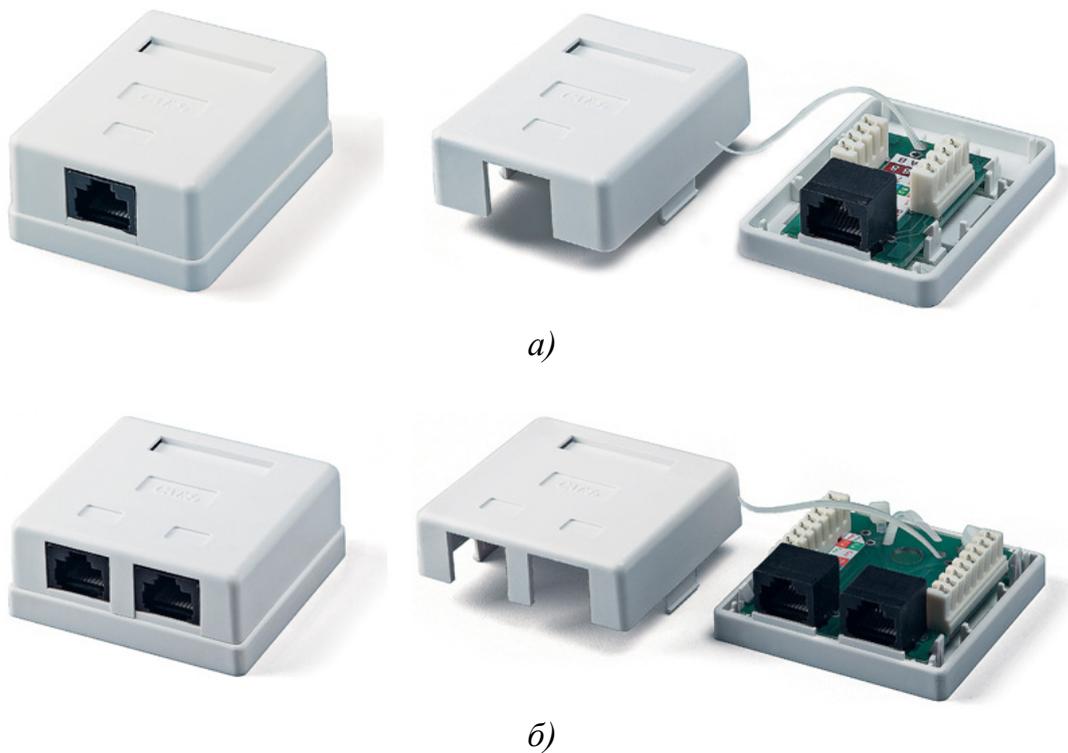
Возьмите коннектор так, чтобы пластиковый фиксатор смотрел в сторону от Вас и вниз. Аккуратно вставьте отсортированные и выровненные жилы в коннектор по направляющим до упора. Можно использовать специальные вставки, которые не позволяют жилам перемешиваться в данном случае.

Убедитесь, что конец изоляции находится внутри коннектора RJ-45 и все жилы упираются в переднюю стенку коннектора. Затем вставьте коннектор в соответствующее гнездо обжимного инструмента и плавно сомкните ручки инструмента (рис. 25).



*Рис. 25. Инструмент для обжимки витой пары:
а – для одного типа коннекторов; б – для двух типов коннекторов*

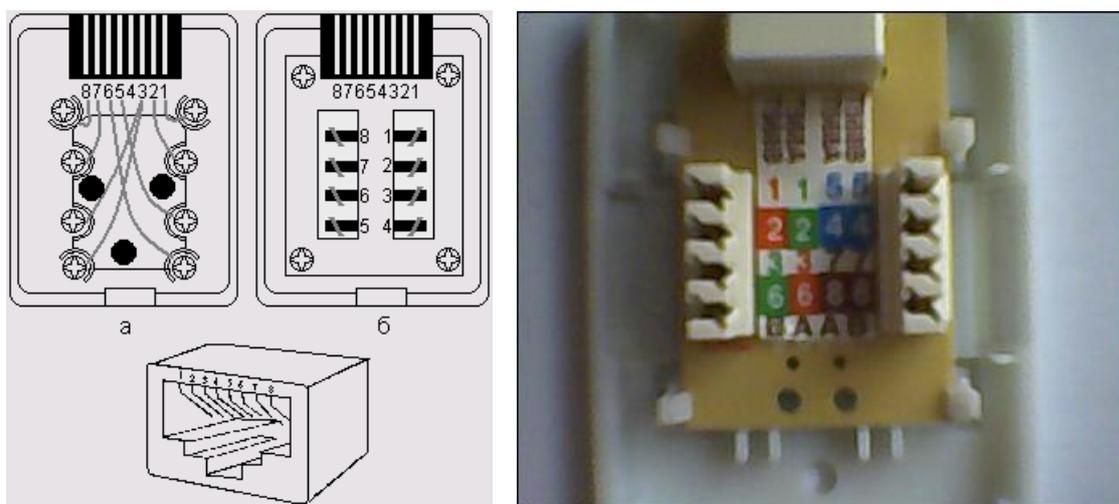
Повторите процедуру с другим концом кабеля.
Монтируются розетки по следующей схеме (рис. 26).



*Рис. 26. Розетки RJ-45 для настенного монтажа:
а – розетка с одним портом; б – розетка с двумя портами*

В большинстве случаев сетевые розетки представляют собой пластмассовый короб со съёмной крышкой, в верхней части которого смонтирована ответная часть разъёма RJ-45, оснащённая восемью подпружиненными контактами. Также существуют внутренние розетки, монтируемые в стены или специальные короба.

Если развернуть розетку разъемом к себе таким образом, чтобы контакты оказались внизу, то номера контактов отсчитываются с 1-го по 8-й справа налево (рис. 27).



а)

б)

Рис. 27. Раскладка жил кабеля в розетке RJ-45:
а – схема раскладки; б – внешний вид розетки

Общая последовательность монтажа сетевых розеток RJ-45:

1. Снимите крышку розетки.
2. Закрепите розетку на стене вблизи рабочего места. Внутренние розетки необходимо монтировать уже после присоединения жил кабеля к контактам розетки.
3. Освободите от наружной изоляции кабель на требуемую глубину (3 – 5 см, впоследствии выступающие жилы можно подрезать) и аккуратно расплетите жилы.
4. Присоедините жилы к контактам розетки согласно выбранной вами схеме заделки кабеля. Схема указана на розетке по цвету и номерам жил в кабеле.

5. Зафиксируйте кабель в розетке с помощью хомута.
6. Закройте крышку розетки.
7. Проложите кабель до коммутационной панели, фиксируя его через равные промежутки или в коробах.
8. На противоположном от розетки конце кабеля смонтируйте разъем RJ-45, соблюдая выбранную вами схему заделки для подключения к порту промежуточного сетевого оборудования (коммутатора, маршрутизатора и т.д.). Можно проверить правильность и корректность монтажа с помощью специальных тестеров (LAN-тестеров).
9. Подключите разъем RJ-45 в соответствующий порт.

ЭМУЛЯЦИЯ И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СЕТИ

По завершении процесса проектирования целесообразно провести проверку проектных решений. Для этих целей можно использовать эмулятор Cisco Packet Tracer (рис. 28). Эмулятор позволяет воспроизвести практически все проектные решения, настроить виртуальное оборудование согласно разработанным спецификациям, проверить работоспособность сети на тестовых пакетах.

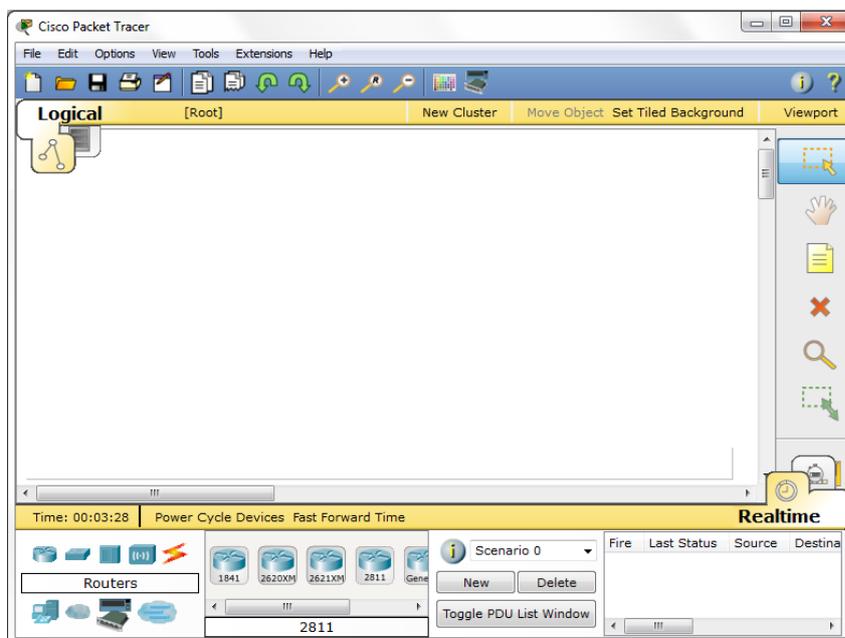


Рис. 28. Основное окно Cisco Packet Tracer
(логическая схема сети)

Packet Tracer (PT) – эмулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями (через облако). Включает в себя серии маршрутизаторов Cisco 1800, 2600, 2800 и коммутаторов 2950, 2960, 3650. Кроме того, есть серверы DNS, HTTP, TFTP, FTP, рабочие станции, различные модули к компьютерам и маршрутизаторам, устройства WiFi, различные типы кабелей. PT позволяет эмулировать даже сложные сети, проверять на работоспособность топологии. Доступен бесплатно для участников Программы Сетевой Академии Cisco.

Благодаря режиму визуализации Cisco Packet Tracer пользователь может отследить процесс перемещения данных по сети, изменения параметров IP-пакетов при прохождении данных через сетевые устройства и другие параметры. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности.

Приложение Cisco Packet Tracer доступно для платформ Windows и Linux.

Также можно воспользоваться GNS3 – графическим эмулятором локальной сети предприятия, построенной на основе маршрутизаторов, межсетевых экранов компании Cisco.

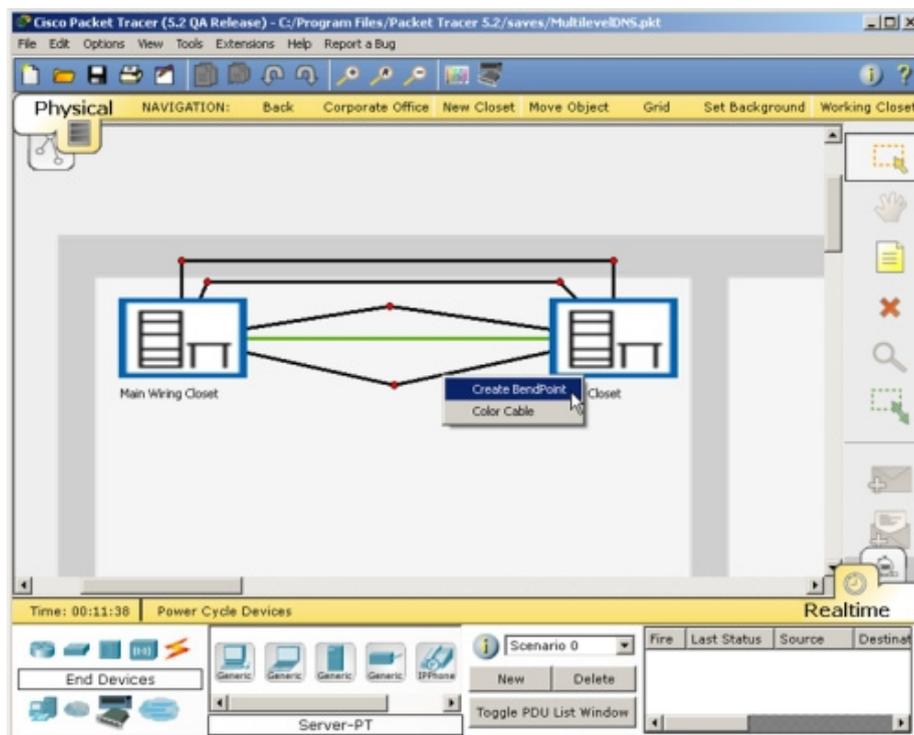
Эмуляторы могут использоваться для подготовки и проверки конфигурационных файлов сетевого оборудования с последующим переносом настроек на реальное оборудование.

Дальнейшее описание дается относительно Cisco Packet Tracer.

Интерфейс программы состоит:

- из панели инструментов с типовым набором элементов;
- панели Logical/Physical (рис. 28, 29), которая расположена под панелью инструментов. Панель позволяет переключаться между логической и физической топологиями сети. Физическая топология позволяет посмотреть размещение оборудования в «городе», «офисе», «стойке»;

- рабочей области, в которой размещаются устройства и устанавливаются связи между ними;



*Рис. 29. Основное окно Cisco Packet Tracer
(физическая схема сети)*

- окно конфигурации устройств (рис. 30), которое конфигурирует устройство (вызывается двойным щелчком по левой кнопке мыши). Возможно конфигурирование в следующих режимах: физическом (physical), графического интерфейса (config), командной строки (CLI).

В физическом режиме показан внешний вид устройства и предоставляется возможность добавлять либо убирать модули. В режиме графического интерфейса можно конфигурировать оборудование без применения командной строки. При этом отображаются соответствующие команды для CLI. В режиме командной строки пользователь получает доступ к командной строке операционной системы конфигурируемого устройства. Это имитация доступа через терминальную программу (типа telnet).

- блока выбора устройств и связей, расположенного под рабочей областью слева и по центру;
- панели эмуляции. Работа сети возможна в двух режимах: Real

Time и Simulator. Во втором режиме можно получать детальную информацию о циркулирующих в сети пакетах.

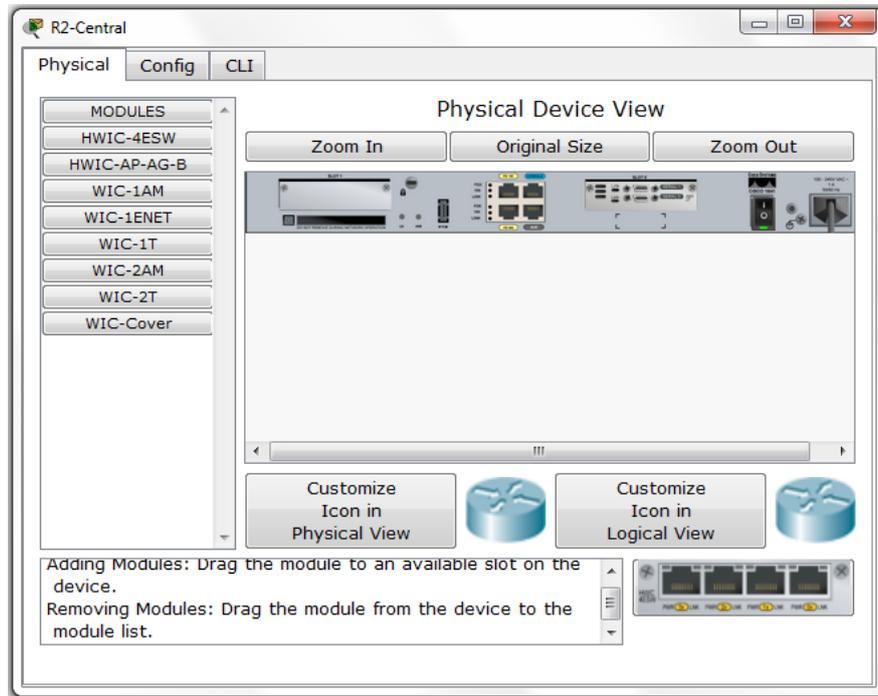


Рис. 30. Окно конфигурации устройства

Также в приложении можно выполнять задания (предоставляются в рамках изучаемых в Сетевой академии курсов). В данном случае эмулятор контролирует правильность выполнения заданий (рис. 31).

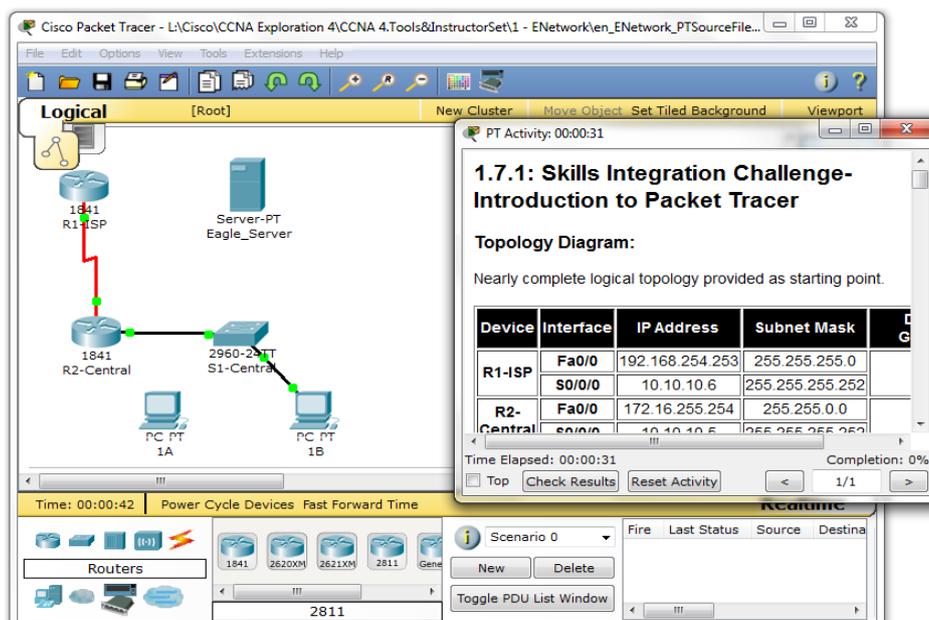


Рис. 31. Выполнение задания в Cisco Packet Tracer

Более полную информацию о работе с эмулятором можно получить из справочной системы, которая помимо текстового описания, содержит и видеоматериалы.

ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Ниже приведен обзор некоторых наиболее часто встречающихся проблем на первых трех уровнях модели OSI.

На 1-м уровне:

- 1) обрыв или неподсоединение кабеля;
- 2) подключение кабеля к другому порту (который может быть отключен политикой безопасности);
- 3) нестабильный контакт в месте подсоединения кабеля;
- 4) неправильная заделка кабеля в разъем;
- 5) применение неправильных типов кабелей;
- 6) отсутствие питания в сетевом устройстве.

На 2-м уровне:

- 1) неправильное конфигурирование интерфейсов;
- 2) неработающая плата сетевого интерфейса.

На 3-м уровне:

- 1) используется неправильный протокол маршрутизации;
- 2) неправильное конфигурирование протоколов маршрутизации;
- 3) некорректный IP-адрес;
- 4) некорректная маска подсети;
- 5) неправильно задан интерфейс.

Полезно иметь общую методику, которую можно использовать для поиска и устранения неисправностей. Она должна содержать следующие этапы:

- определение проблемы, симптомов и потенциальных причин;
- сбор фактов и изолирование причин;
- рассмотрение возможностей, уменьшение области поиска, определение границ проблемы;
- составление плана действий по решению одной из проблем;
- воплощение плана действий;

- наблюдение за результатами. Определяется, решена проблема или нет. Если проблема решена, то процесс на этом завершается;
- повторение процесса. Если проблема не решена, необходимо перейти к следующей наиболее вероятной причине.

Рекомендуется документировать возникающие проблемы в целях ускорения решения подобных ситуаций в будущем. Для поиска и устранения неисправностей можно использовать аппаратное и программное обеспечение.

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Далее приведены основные темы практических занятий:

1. Разработать методику проведения обследования компьютерной сети. Подготовить необходимые документы и распоряжения.
2. Провести обследование компьютерной сети организации в соответствии с разработанной методикой:
 - 1) используя имеющуюся в организации документацию;
 - 2) провести физическое обследование компьютерной сети.
3. Разработать проект компьютерной сети (считается, что к этому моменту компьютерная сеть в организации отсутствует):
 - 1) разработать необходимые схемы, определить параметры сети (в том числе описать параметры конфигурации оборудования);
 - 2) рассчитать стоимость сети (оборудования сетевого, строительного и монтажного, работ, расходных материалов, программного обеспечения) с привязкой к ценам в регионе;
 - 3) разработать концепцию защиты периметра сети;
 - 4) составить план-график работ по реализации сети в организации.
4. Разработать проект модернизации компьютерной сети (основываясь на текущей ситуации):
 - 1) определить элементы компьютерной сети, требующие модернизации;
 - 2) предложить пути модернизации инфраструктуры и устране-

ния уязвимостей и проблемных мест;

3) рассчитать стоимость работ, оборудования и программного обеспечения;

4) оценить пути повышения защищенности сети.

Рекомендуемый состав компьютерной сети при проведении исследований:

- наличие пограничного маршрутизатора, через который осуществляется подключение компьютерной сети организации к компьютерным сетям ISP (интернет-сервис провайдера);

- наличие промежуточного маршрутизатора, используемого для разделения компьютерной сети организации на сегменты, принадлежащие отдельным подразделениям организации и организации VLAN;

- наличие точки доступа беспроводных устройств, работающей в скрытом режиме, для подключения мобильных пользователей в пределах компьютерной сети организации;

- наличие аппаратного межсетевого экрана (его функции могут быть реализованы в маршрутизаторе списками ACL);

- кабельная система организации проложена через помещения, не принадлежащие организации (необходимо учесть возможность несанкционированного доступа и помех, снижающих качество передаваемых сигналов);

- количество используемых серверов – 2: один доступен из внешней сети (http, ftp, telnet/SSH); второй – контроллер домена, осуществляет управление пользователями, резервирование и т.д.

- в организации работает несколько групп пользователей.

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Ниже приведен перечень основных лабораторных работ с краткими рекомендациями по их выполнению. Некоторые проектные решения могут быть приняты в ходе выполнения заданий на практических занятиях.

Лабораторная работа № 1 **Конфигурирование интерфейсов**

Цель работы. Изучить методику конфигурирования сетевых интерфейсов различных операционных систем.

Задание:

- Выбрать, установить и настроить систему управления виртуальными машинами (СУВМ): VMWare Player, VirtualBox.
- Подготовить образы операционных систем MS Windows XP, Windows 7, Windows Server, Ubuntu. Рекомендуется использовать актуальные на момент выполнения работ версии операционных систем.
- Определить последовательность операций по настройке сетевых интерфейсов для работы с DHCP-сервером и при ручной настройке параметров соединений (получить схему распределения адресов компьютерной сети от преподавателя).
- Провести настройку сетевых компонентов СУВМ и ручную настройку сетевых интерфейсов образов двух виртуальных машин. Экспериментально подтвердить обмен пакетами между образами (воспользоваться утилитой ping).

Отчет о проделанной работе оформляют по писчей бумаге формата А4:

Содержание отчета:

- Использованный дистрибутив СУВМ.
- Работоспособные образы виртуальных машин.

Лабораторная работа № 2 **Эмулятор СРТ**

Цель работы. Изучить интерфейс и возможности эмулятора Cisco Packet Tracer.

Задание:

- Установить эмулятор Cisco Packet Tracer. Рекомендуется использовать актуальную на момент выполнения работы версию

эмулятора. Также можно использовать эмулятор GNS3.

- Изучить интерфейс эмулятора.
- Создать простую сеть, состоящую из следующих устройств: сервера, коммутатора, маршрутизатора, нескольких рабочих станций. Получить схему адресации и логическую топологию сети. Соединить перечисленные устройства и настроить схему адресации.
- Описать последовательность операций по настройке сетевых интерфейсов.

Рекомендации по выполнению:

- Для соединения устройств рекомендуется использовать элемент auto-connect (группа connections).

Содержание отчета:

- Описание проделанной работы.
- Файл *.rpa с результатами выполненной работы.

Лабораторная работа № 3 **Построение простой сети**

Цель работы. Получить навык построения простой сети, использования специализированного инструмента.

Задание:

- Провести настройку сетевых интерфейсов двух рабочих станций (PC). Подсеть содержит только две PC.
- Обжать кабель для соединения двух PC без использования промежуточных сетевых устройств. Промаркировать кабель. Экспериментально подтвердить обмен пакетами между PC.
- Обжать кабель для соединения двух PC при использовании промежуточных сетевых устройств (коммутатора). Промаркировать кабель. Экспериментально подтвердить обмен пакетами между PC.

Рекомендации по выполнению:

- Рекомендуется использовать описание, подготовленное в лабораторной работе № 1.
- Для проверки наличия соединения следует использовать утилиту ping.

Содержание отчета:

- Описание проделанной работы.

Лабораторная работа № 4

Построение сложной сети

Цель работы. Получить навыки построения «сложной» сети организации, распределенной по нескольким зданиям, и использования систем эмуляции.

Задание:

- Разработать общую схему компьютерной сети в соответствии с требованиями, далее определить необходимое сетевое оборудование и точки его размещения по территории здания и этажам в соответствии с рекомендациями стандартов. Обозначить на схеме зданий точки размещения оборудования и основные кабельные каналы.
- Провести обзор доступного в розничной продаже сетевого оборудования. Рассчитать стоимость необходимого сетевого оборудования, а также «расходных материалов» (розеток, кабеля, коннекторов и т.п.).
- Предложить схему разделения адресного пространства (IP-адресов) в двух вариантах: при использовании VLSM и без.
- Используя эмулятор, проверить правильность заполнения конфигурационных файлов.

Общие требования к разрабатываемой компьютерной сети:

- Общая сеть должна быть разделена минимум на две подсети (по зданиям). Широковещательный трафик между подсетями блокируется. В сети присутствуют два DHCP-сервера (в каждом здании) и один FTP-сервер (в здании 1). Имеется общая точка доступа в Internet (в здании 1). Общее количество рабочих мест – 440 (290 в первом здании).
- Объекты для проектирования и монтажа СКС: за основу взять обобщенную схему двух 6-этажных зданий. Компьютеры равномерно распределены по всем этажам и в пределах этажа. Здания

прямоугольной формы – размеры (20×40 м). Минимальное расстояние между зданиями – 80 м. Общая схема первого этажа приведена на рис. 32.

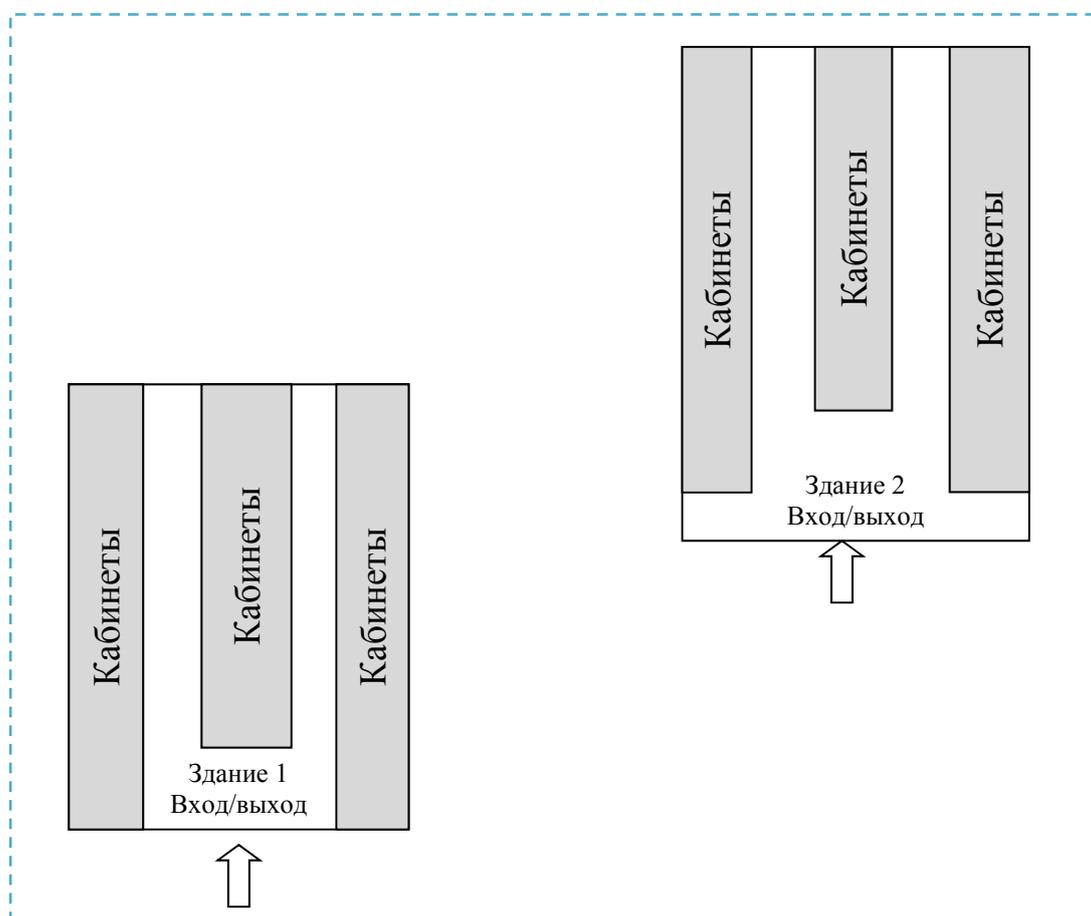


Рис. 32. Схема зданий организации

- Каждое рабочее место СКС должно быть обеспечено не менее чем двумя информационными розетками RJ-45.
- Большая часть оборудования устанавливается в монтажных шкафах (стойках) и соединяется кабелями с информационными розетками на рабочих местах.
- Горизонтальная подсистема СКС в зданиях должна быть построена на основе неэкранированного кабеля типа «витая пара» (UTP) категории 5е. Предусмотреть использование неэкранированной витой пары категории 6.

Все активное сетевое оборудование должно удовлетворять следующим требованиям:

- активное сетевое оборудование должно основываться на технологии коммутируемых сетей Ethernet, Fast Ethernet, Gigabit Ethernet;
- активное сетевое оборудование должно обеспечить подключение рабочих станций со скоростью не менее 100 Мбит/с;
- активное сетевое оборудование должно обеспечить подключение серверов со скоростью не менее 100 Мбит/с с возможностью перехода на 1000 Мбит/с;
- пропускная способность магистральных каналов связи между активным сетевым оборудованием должна быть не менее 1000 Мбит/с;
- активное оборудование должно комплектоваться источниками бесперебойного питания (ИБП) мощностью не менее 1 кВА;
- для обеспечения установки серверов, ИБП, активного и пассивного сетевого оборудования соответствующего исполнения должны быть предусмотрены монтажные шкафы (стойки) со следующими характеристиками: ширина – 19 дюймов, высота – 42 юнита. Все вмонтированные в шкаф устройства должны быть подключены к ИБП.
- В качестве активного сетевого оборудования компьютерной сети для подключения серверов и персональных компьютеров пользователей необходимо использовать управляемые сетевые коммутаторы с характеристиками: 24 (48) порта(ов) 10/100 Мбит/с, 2 порта 10/100/1000 Мбит/с.
- В здании 1 установлен ADSL-модем – точка доступа в Internet.

Содержание отчета:

- Описание проделанной работы.
- Файл *.pka с результатами выполненной работы (фрагментами реализованной компьютерной сети).

Лабораторная работа № 5

Маршрутные таблицы

Цель работы. Получить навык анализа маршрутных таблиц маршрутизаторов Cisco.

Задание:

- Восстановить топологию сети и ее основные характеристики (протоколы, схемы адресации, распределение адресов и т.д.) путем анализа информации из маршрутных таблиц.

Содержимое маршрутных таблиц маршрутизаторов:

Маршрутизатор 1:

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E – EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o – ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/30 is subnetted, 1 subnets

C 10.10.10.252 is directly connected, Serial0/0/0

172.16.0.0/30 is subnetted, 1 subnets

C 172.16.100.0 is directly connected, Serial0/0/1

R 192.168.1.0/24 [120/1] via 10.10.10.254, 00:00:03, Serial0/0/0

R 192.168.2.0/24 [120/1] via 10.10.10.254, 00:00:03, Serial0/0/0

R 192.168.3.0/24 [120/1] via 10.10.10.254, 00:00:03, Serial0/0/0

C 192.168.4.0/24 is directly connected, Loopback0

C 192.168.5.0/24 is directly connected, Loopback1

C 192.168.6.0/24 is directly connected, Loopback2

R 192.168.7.0/24 [120/1] via 172.16.100.2, 00:00:04, Serial0/0/1

R 192.168.8.0/24 [120/1] via 172.16.100.2, 00:00:04, Serial0/0/1

R 192.168.9.0/24 [120/1] via 172.16.100.2, 00:00:04, Serial0/0/1

Маршрутизатор 2:

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E – EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o – ODR
 P - periodic downloaded static route
 Gateway of last resort is not set
 10.0.0.0/30 is subnetted, 1 subnets
 C 10.10.10.252 is directly connected, Serial0/0/0
 R 172.16.0.0/16 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
 C 192.168.1.0/24 is directly connected, Loopback0
 C 192.168.2.0/24 is directly connected, Loopback1
 C 192.168.3.0/24 is directly connected, Loopback2
 R 192.168.4.0/24 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
 R 192.168.5.0/24 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
 R 192.168.6.0/24 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
 R 192.168.7.0/24 [120/2] via 10.10.10.253, 00:00:04, Serial0/0/0
 R 192.168.8.0/24 [120/2] via 10.10.10.253, 00:00:04, Serial0/0/0
 R 192.168.9.0/24 [120/2] via 10.10.10.253, 00:00:04, Serial0/0/0

Маршрутизатор 3:

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E – EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o – ODR
 P - periodic downloaded static route
 Gateway of last resort is not set
 R 10.0.0.0/8 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
 172.16.0.0/30 is subnetted, 1 subnets
 C 172.16.100.0 is directly connected, Serial0/0/1
 R 192.168.1.0/24 [120/2] via 172.16.100.1, 00:00:19, Serial0/0/1
 R 192.168.2.0/24 [120/2] via 172.16.100.1, 00:00:19, Serial0/0/1
 R 192.168.3.0/24 [120/2] via 172.16.100.1, 00:00:19, Serial0/0/1

R 192.168.4.0/24 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
R 192.168.5.0/24 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
R 192.168.6.0/24 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
C 192.168.7.0/24 is directly connected, Loopback0
C 192.168.8.0/24 is directly connected, Loopback1
C 192.168.9.0/24 is directly connected, Loopback2

Содержание отчета:

- Описание проделанной работы.
- Файл *.pka с результатами выполненной работы.

Лабораторная работа № 6

Инвентаризация и администрирование компьютерных сетей

Цель работы. Получить навык работы с инструментальными средствами инвентаризации и администрирования корпоративных сетей.

Задание:

- Изучить возможности программного обеспечения по инвентаризации сетей.
- Заполнить БД сведениями о структуре и компонентах компьютерной сети организации (сегмента сети, не менее пяти компьютеров).
- Используя утилиту nmap (предназначена для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов и определения состояния объектов сканируемой сети), провести сканирование 2 – 3 компьютеров в сети (один из них сервер) и определить перечень открытых портов и запущенных на них служб.
- Составить перечень доступных в сети ресурсов и прокомментировать назначение запущенных сетевых служб.

В качестве программного обеспечения инвентаризации можно использовать утилиту Friendly Pinger – это мощное и удобное приложение для администрирования, мониторинга и инвентаризации компьютерных сетей (URL: <http://www.kilievich.com/rus/fpinger/>).

Содержание отчета:

- Описание проделанной работы.
- Файл *.map с результатами выполненной работы и файлы с экспортированными данными по конфигурации и комплектности устройств.

Лабораторная работа № 7
Перехват и анализ трафика

Цель работы. Изучить методы перехвата и анализа трафика с помощью сетевых анализаторов.

Задание:

- Установить на компьютер программу-анализатор трафика сетей Ethernet Wireshark. Изучить интерфейс программы-анализатора.
- Включить протоколирование интерфейса подключения к локальной сети.
- Используя различные клиенты сетевых приложений (веб, FTP, электронной почты и т.д.), запросить ресурсы с других хостов в локальной сети и сети Интернет.
- Проанализировать перехваченный трафик:
 - 1) определить перечень используемых протоколов;
 - 2) прокомментировать назначение протоколов, а также определить выделенные порты;
 - 3) статистику их использования.
- Проверить наличие соединения с удаленным хостом (используя утилиту ping):
 - 1) проанализировать перехваченные пакеты;
 - 2) прокомментировать значения полей пакетов.
- Осуществить трассировку маршрута до удаленного хоста (желательно с количеством хопов (прыжков) более 5):
 - 1) проанализировать перехваченные пакеты;
 - 2) прокомментировать значения полей пакетов;
 - 3) построить алгоритм, использованный при трассировке.
- Подключиться к FTP-серверу и скачать файл. Проанализировать перехваченный трафик:

- 1) последовательность команд при установлении соединения;
 - 2) использованные имя пользователя и пароль.
- Предложить методы (средства) защиты трафика от перехвата.

Содержание отчета:

- Описание проделанной работы.
- Файл с результатами работы программы-анализатора.

Лабораторная работа № 8 **Диагностика уязвимостей**

Цель работы. Изучение способов идентификации уязвимостей в программном обеспечении.

Задание:

- Использую статистику NIST (<http://web.nvd.nist.gov/view/vuln/statistics>, <http://web.nvd.nist.gov/view/vuln/search>) и базу данных US-CERT (<http://www.kb.cert.org/vuls/html/search>):

1. Проанализировать динамику выявления уязвимостей протокола HTTP и веб-сервера apache. Определить средний уровень критичности и группы уязвимостей для данного сервера за последние три года.
2. Проанализировать динамику выявления уязвимостей протокола HTTP и веб-сервера IIS. Определить средний уровень критичности и группы уязвимостей для данного сервера за последние три года. Сравнить с другим HTTP-сервером.
3. Проверить наличие уязвимостей для используемого веб-браузера и определить пути их устранения (если имеются).

Содержание отчета:

- Описание проделанной работы.

Лабораторная работа № 9 **Защита периметра сети**

Цель работы. Получить навык установки и настройки системы обнаружения вторжений.

Задание:

- В работе используется IDS Snort. Установить IDS и произвести начальную настройку.

- Исследовать режимы работы IDS (снифер, обнаружения вторжений, сигнализации).

Содержание отчета:

- Описание проделанной работы.

- Конфигурационные файлы IDS.

КОНТРОЛЬНЫЕ ВОПРОСЫ

По разделу «Компьютерные сети»

1. Какие существуют способы организации компьютерных сетей?
2. Какими особенностями обладают локальные сети?
3. Какие существуют топологии организации компьютерных сетей?
4. Какая топология организации компьютерных сетей является самой распространённой?

По разделу «Элементы компьютерной сети»

1. Какие устройства (элементы) используются для построения компьютерной сети?
2. На какие категории разделяются хосты? Чем характеризуется каждая из категорий?
3. Какие основные коммутирующие устройства используются в компьютерных сетях? С какой целью используются эти устройства?
4. Какие графические символы используются для обозначения на схемах: коммутирующих устройств, линий связи, оконечного оборудования?
5. Какие стандарты используются при построении компьютерной сети?

По разделу «Модели взаимодействия систем»

1. Каковы предпосылки разработки моделей взаимодействия систем?

2. Какое количество уровней взаимодействия определено в модели взаимодействия OSI?
3. Какое количество уровней взаимодействия определено в модели взаимодействия TCP/IP? Какие базовые функции реализует каждый из уровней?
4. Что такое PDU? Какое обозначение имеет PDU на каждом из уровней моделей взаимодействия OSI и TCP/IP?
5. Что такое протокол? Перечислите несколько наиболее распространенных.
6. В чем заключаются различия между моделями взаимодействия OSI и TCP/IP?

По разделу «История развития компьютерных сетей»

1. Каковы основные периоды развития компьютерных сетей?
2. Когда были разработаны принципы Ethernet?
3. В какой период начались работы над технологией беспроводной передачи данных в компьютерных сетях?
4. Когда был введен стек протоколов TCP/IP?
5. В какой период была разработана технология WWW? Какие основные элементы входят в данную технологию?

По разделу «Проектирование компьютерной сети»

1. Какие основные характеристики лежат в основе любой сетевой архитектуры?
2. Какие данные необходимо собрать на этапе обследования объекта при проектировании компьютерной сети?
3. Какие документы необходимо подготовить в результате проведения анализа собранных данных об организации? Что является основным результатом этапа анализа?
4. На каких уровнях модели OSI осуществляется проектирование компьютерной сети? Перечислите основные правила проектирования компьютерной сети на каждом из уровней.
5. Какие виды адресации используются в компьютерных сетях? Укажите назначение каждого вида адреса.
6. Какова схема адресации на прикладном уровне модели взаимодействия OSI?

7. На какие группы разделяются адреса транспортного уровня? Приведите примеры наиболее часто используемых адресов (портов) транспортного уровня.
8. Что такое IP-адрес? Приведите структуру IP-адреса и соглашения об особой интерпретации IP-адресов.
9. Что такое классовая и бесклассовая адресации? Укажите основные причины деления на подсети.
10. В чем заключаются основные отличия версий протоколов IP?
11. Какие протоколы используются на канальном уровне?
12. Какой основной принцип подготовки документации на компьютерную сеть?

По разделу «Принципы коммутации и маршрутизации в компьютерных сетях»

1. Какие причины применения коммутации и маршрутизации в компьютерных сетях?
2. Какие функции выполняет коммутатор?
3. В каких режимах может работать коммутатор?
4. Какие виды маршрутизации используются в компьютерных сетях? Перечислите преимущества и недостатки каждого из видов.
5. Какие существуют классы протоколов маршрутизации? Приведите примеры протоколов в каждом из классов.
6. Какие причины применения VLAN?
7. Какие основные протоколы используются для отслеживания кадров VLAN?

По разделу «Структурированные кабельные системы»

1. Что такое СКС?
2. В соответствии с какими стандартами должна осуществляться разработка СКС? Какие группы требований определены в стандартах?
3. Какие схемы раскладки проводов кабеля используются в компьютерных сетях? Укажите порядок раскладки проводов.
4. В каком порядке осуществляется монтаж разъемов RJ-45?

По разделу «Эмуляция и экспериментальное исследование сети»

1. Какие причины использования эмуляторов при проектировании компьютерных сетей?
2. Какие эмуляторы можно использовать? Перечислите основные возможности выбранных систем.

По разделу «Поиск и устранение неисправностей»

1. Какие основные неисправности встречаются на 1-м уровне модели взаимодействия OSI? Прокомментируйте каждую из них.
2. Какие основные неисправности встречаются на 2-м уровне модели взаимодействия OSI? Прокомментируйте каждую из них.
3. Какие основные неисправности встречаются на 3-м уровне модели взаимодействия OSI? Прокомментируйте каждую из них.

Технологии передачи данных постоянно развиваются. Данная книга затрагивает только несколько небольших разделов проектирования сетей. Однако пособие может стать основой для дальнейшего изучения сетевых технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Амато, В. Основы организации сетей Cisco. В 2 т. Т. 1 / В. Амато. – М. : Вильямс, 2002. – 512 с. – ISBN 5-8459-0258-4.
2. Амато, В. Основы организации сетей Cisco. В 2 т. Т. 2 / В. Амато. – М. : Вильямс, 2004. – 464 с. – ISBN 5-8459-0561-3.
3. Куроуз, Дж. Компьютерные сети. – 2-е изд., стер. / Дж. Куроуз, К. Росс. – СПб. : Питер, 2004. – 768 с. – ISBN 5-8046-0093-1.
4. Лэммл, Тодд. CCNA. Cisco Certified Network Associate. Экзамен 640-507 : учеб. рук. / Тодд Леммл ; пер. с англ. М. Кузьмина ; под науч. ред. А. Головки. – 2-е изд., стер. – М. : ЛОРИ, 2002. – 620 с. – ISBN 5-85582-180-3.
5. Программа сетевой академии Cisco CCNA 1 и 2 : вспом. рук. : пер. с англ. – 3-е изд., испр. – М. : Вильямс, 2007. – 1168 с. – ISBN 5-8459-0842-6, 1-58713-150-1.
6. Программа сетевой академии Cisco CCNA 3 и 4 : вспом. рук. :

пер. с англ. – 3-е изд., испр. – М. : Вильямс, 2007. – 944 с. – ISBN 5-8459-1120-6, 1-58-713113-7.

7. Таненбаум, Э. Компьютерные сети. / Э. Таненбаум. – 4-е изд., стер. – СПб. : Питер, 2011. – 991 с. – ISBN 978-5-318-00492-6.

8. ГОСТ Р 53246-2008. Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы : Общие требования. – Введ. с 2010-01-01. – Калуга : Изд-во стандартов, 2009. – 77 с.

ОГЛАВЛЕНИЕ

Предисловие	3
Компьютерные сети	6
Элементы компьютерной сети	8
Модели взаимодействия систем	12
История развития компьютерных сетей	17
Проектирование компьютерной сети	18
Принципы коммутации и маршрутизации в компьютерных сетях	47
Структурированные кабельные системы	58
Эмуляция и экспериментальное исследование сети	66
Поиск и устранение неисправностей	70
Рекомендации по проведению практических занятий	71
Рекомендации по проведению лабораторных работ	72
Контрольные вопросы	83
Библиографический список	86

Учебное издание

Комплексная защита объектов информатизации. Книга 21.

ВОРОНИН Алексей Александрович

ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Учебное пособие

Редактор Е. А. Амирсейидова

Подписано в печать 14.09.11.
Формат 60x84/16. Усл. печ. л. 5,11. Тираж 80 экз.

Заказ

Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
600000, Владимир, ул. Горького, 87.