Основные сведения о IP-сетях для установщиков IP-АТС Panasonic серии TDA

Авторы: Сайед Ахмад, Марк Эванс
Kyushu Matsushita Electric Co., Ltd.
Ньюпорт, 2002

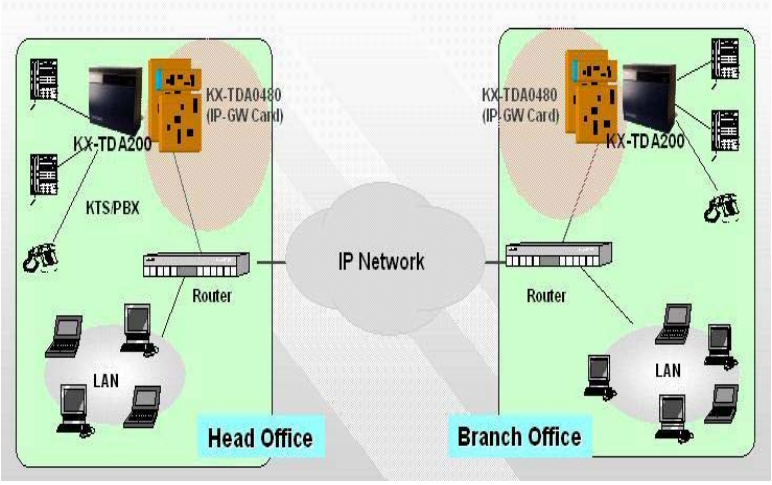
Содержание

Введение ***2***
Наши читатели 3
Цель 3
Локальные сети ***3***
Протоколы ***3***
Сети Ethernet ***4***
Кабели и монтаж ***5***
IP-адресация ***7***
Частные IP-сети ***9***
Маски подсети ***9***
Концентраторы, коммутаторы, маршрутизаторы ***10***
Концентраторы 10
Коммутаторы 11
Маршрутизаторы 11
Сетевые серверы ***12***
Сервер DHCP 12
DNS-сервер 12
Основные термины ***13***
Примечания ***14***

Введение

Сетевые технологии очень распространены в современном мире. Компьютеры, которые вы используете, наверняка подключены к какой-либо сети. Когда вы получаете электронную почту, общаетесь с кем-либо в чате или посещаете какой-то веб-сайт, вы подключаетесь к сети Интернет - самой большой сети в мире. Когда вы отправляете SMS-сообщение с вашего мобильного телефона, вы также используете сеть Интернет.

Система Panasonic KX-TDA100/200 является цифровой гибридной IP-АТС, которую можно подключать к корпоративным сетям передачи данных при помощи платы компьютерной телефонии (номер компонента: KX-TDA0410). Сетевой интерфейс придаёт системам TDA дополнительные функции и преимущества. Системные администраторы теперь смогут программировать и конфигурировать офисные АТС Panasonic со своего компьютера через локальную сеть, а также, используя Интернет, из любой точки мира.



Head Office – главный офис
Branch Office – филиал
IP Network – IP-сеть
IP-GW Card – плата IP-шлюза
Router – маршрутизатор
LAN – локальная сеть

Система TDA также имеет плату интерфейса VoIP (Voice over Internet Protocol – Протокол Передачи Речи по Интернет), которая может использоваться аналогично другим платам соединительных линий для соединения двух и более систем TDA через корпоративную сеть передачи данных для снижения затрат на телефонные переговоры.

Так как новая цифровая гибридная IP-АТС Panasonic KX-TDA100/200 рассчитана на работу в сетях передачи данных, мы решили составить небольшой справочный документ об основах построения сетей для сотрудников дилерских компаний по всему миру. Настоящий документ разработан в соответствии с нашими традициями предоставления максимального объема полезной информации с целью получения нашими дилерами знаний о важнейших понятиях сетевых технологий. Мы надеемся, что этот документ поможет дилерским компаниям обеспечить высочайшее качество услуг для наших клиентов.

Наши читатели

Настоящий документ предназначен для тех, кто уже знаком с оборудованием и программным обеспечением АТС, но не знаком с понятиями сетевых технологий или начинающих изучение построения IP-сетей.

Многие понятия, рассматриваемые в этом документе, могут показаться некоторым читателям слишком простыми, однако мы рекомендуем прочесть документ полностью. Мы полагаем, что после ознакомления с настоящим документом читатель получит достаточное количество информации, чтобы подключить к локальной сети цифровую гибридную IP-АТС Panasonic серии TDA.

Цель

Цель настоящего документа состоит в том, чтобы обеспечить базовый уровень знаний, необходимый для понимания различных методов построения IP-сетей и технологий, используемых в новых цифровых гибридных IP-АТС Panasonic серии TDA.

Локальные сети (LAN)

Сеть – это любая совокупность независимых компьютеров или сетевых устройств, которые взаимодействуют друг с другом посредством общедоступной сетевой среды. Локальные сети являются географически небольшими сетями, обычно ограниченными пределами одного здания или территорией предприятия. Локальные сети могут быть очень маленькими и объединять всего три компьютера, но чаще всего они связывают сотни компьютеров, используемых тысячами людей. Разработка стандартных сетевых протоколов и средств привела к быстрому росту количества локальных сетей среди коммерческих и образовательных организаций по всему миру.

Система Panasonic KX-TDA100/200 является цифровой гибридной IP-АТС, и может быть подключена к корпоративной локальной сети передачи данных при помощи платы компьютерной телефонии.

Протоколы

Сетевые протоколы - это стандарты, определяющие правила взаимодействия компьютеров между собой в сети. Протокол определяет процедуру идентификации компьютеров в сети, форму передачи данных и способ обработки данных после их получения. Протоколы также определяют процедуры обработки потерянных или поврежденных передач или "пакетов". На сегодняшний день существуют следующие основные типы сетевых протоколов: TCP/IP (Transfer Control Protocol / Internet Protocol – Протокол Управления Передачей / Интернет-Протокол – для ОС Unix, Windows NT, Windows 95 и других платформ),

IPX (для сетей под управлением Novell NetWare), стек протоколов AppleTalk (для компьютеров Macintosh) и протоколы NetBIOS/NetBEUI (для Windows LAN Manager и сетей Windows NT).

Телефонные системы серии TDA поддерживают наиболее известный и широко применяемый сетевой протокол TCP/IP. Используя локальную сеть на базе TCP/IP, системный администратор со своего рабочего места при помощи одного компьютера может программировать и конфигурировать несколько систем TDA. Компания, имеющая несколько филиалов, может оборудовать одно рабочее место для сетевого администратора, с которого тот сможет программировать, конфигурировать и администрировать все взаимосвязанные системы TDA.

Сети Ethernet

Если у вас уже имеется сеть, с 90-процентной вероятностью можно предположить, что это сеть Ethernet. При создании новой сети в соответствии с вашими требованиями вероятность того, что это будет сеть Ethernet, составит 95%, т.к. именно Ethernet является на сегодняшний день самым используемым сетевым стандартом.

В 1972 году д-р Роберт Меткалф перешел в ныне знаменитую Лабораторию вычислительной техники в Исследовательском центре Palo Alto (PARC) компании Зирокс (Xerox), чтобы принять участие в первых разработках персональных компьютеров. В 1973 году он изобрел Ethernet (читается "эзернет"), технологию локальных сетей, на которую он оформил четыре патента. В середине 1970-х д-р Меткалф совместно с компаниями Xerox®, DEC™ и Intel® разрабатывал Ethernet как сетевой протокол для передачи данных со скоростью 10 Мбит/с (что было по тем временам очень высокой скоростью) по толстому коаксиальному кабелю (стандартный Ethernet).

Несмотря на то, что в современном мире многие сети построены по технологии Fast Ethernet (до 100 Мбит/с) и даже Gigabit Ethernet (до 1000 Мбит/с), стандартный Ethernet со скоростью передачи 10 Мбит/с все еще популярен и составляет основу большинства сетей.

Сети Ethernet являются недорогими и высокоскоростными локальными сетями. В стандартизации IEEE стандарт Ethernet имеет официальное название IEEE 802.3 CSMA/CD[1]. Для построения локальной сети Ethernet на персональные компьютеры устанавливаются специальные адаптеры – сетевые платы Ethernet. Эти платы также называются интерфейсными платами для локальных сетей или просто платами LAN. На задней панели этих плат расположен разъем RJ-45, обеспечивающий подключение компьютера к корпоративной локальной сети при помощи соответствующего кабеля. Следует отметить, что в сети Ethernet можно объединять не только компьютеры, но и многие другие типы устройств, например, сетевые принтеры, широкополосные модемы и телефонные станции. АТС Panasonic серии TDA также можно подключать к корпоративной сети передачи данных. Для подключения системы TDA к сети Ethernet необходима плата компьютерной телефонии (см. рисунок), которая работает со скоростью 10 Мбит/с.

Сетевые платы Ethernet, в зависимости от своего типа, позволяют передавать и принимать данные со скоростью 10 или 100 миллионов бит в секунду (Мбит/с). Чтобы было легче представить такую скорость, приведем следующий пример: по сети Ethernet со скоростью 10 Мбит/с можно передать содержимое стандартной дискеты 1,44 Мбайт всего лишь за 1,2 секунды!

Сигналы в сети Ethernet передаются последовательно, побитно, на каждый компьютер в сети. Каждый компьютер может послать по сети сообщение в любое время, не дожидаясь отдельного разрешения. Посылаемый сигнал направляется на каждый компьютер в сети. Каждый компьютер получает сообщение, но распознает его только тот компьютер, для которого оно предназначено. Компьютер адресата распознает сообщение, так как оно содержит его адрес. Сообщение также содержит адрес компьютера отправителя, что обеспечивает возможность подтверждения сообщения.

От:	Компьютер отправителя
Адрес:	192.168.0.1
Куда:	Компьютер адресата
Адрес:	192.168.0.100
Примечание: прилагается сообщение Ethernet	

Рис. 1 - Логический пакет данных в сети Ethernet

Если два компьютера посылают сообщения одновременно, происходит конфликт ("коллизия"), перемешивание сигналов. Компьютер "понимает", что произошел сетевой конфликт, когда он перестаёт получать свои собственные сообщения в течение определенного промежутка времени. При возникновении конфликта каждый из участвующих в нем компьютеров выжидает в течение случайно выбираемого интервала времени, после чего повторно отправляет сообщение.

В большинстве случаев процесс разрешения конфликта занимает всего лишь доли секунд. Конфликты являются нормальными и ожидаемыми событиями в сети Ethernet. В целях уменьшения числа конфликтов используются коммутаторы Ethernet, которые разбивают сеть на отдельные участки (см. ниже).

Кабели и монтаж

Когда сети Ethernet ещё только появились, в них использовался толстый коаксиальный кабель, похожий на кабель телевизионной антенны. Такие сети были прозваны ThickNet, т.е. "толстые сети". Толстые коаксиальные кабели имели два недостатка: негибкость и высокую стоимость, поэтому на смену им быстро пришли более гибкие и дешевые кабели меньшего

сечения. Их назвали ThinNet, т.е. "тощие сети", или, что более точно, CheaperNet – "дешевые сети". Еще более экономичное решение связано с применением в сети Ethernet неэкранированной витой пары. С появлением кабелей "витая пара" пятой категории (Cat.5), большинство сетей Ethernet перешло на эти кабели. В сетях Ethernet также используются волоконно-оптические кабели, обеспечивающие повышенную помехоустойчивость и передачу на очень большие расстояния. Для каждого типа кабеля стандарт Ethernet имеет свое название:

- 10BASE-5 (ThickNet)
- 10BASE-2 (ThinNet)
- 10BASE-T (Витая пара)
- 10BASE-FL (Волоконно-оптический кабель)

Примечания:

а) «10» в начале обозначает скорость передачи в сети 10 Мбит/с

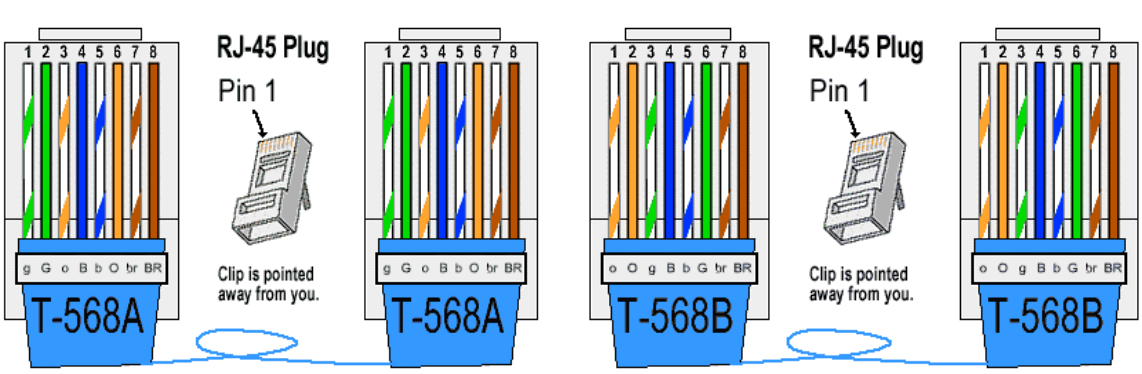
б) «BASE» означает, что используется узкополосная передача

в) «5» или «2» на конце обозначают максимальную длину кабеля - 500 или 200 метров

г) «T» на конце обозначает кабель типа «витая пара»

д) «FL» на конце обозначает волоконно-оптический кабель. Максимальная длина кабеля при использовании волоконно-оптического кабеля - 2 километра.

Наиболее часто в корпоративных сетях Ethernet применяется кабель 10Base-T или 100Base-T. На обоих концах кабеля монтируются разъёмы типа RJ-45. Разъём RJ-45 имеет 8 контактов, но в стандартной сети Ethernet используются только контакты 1, 2, 3 и 6, причем контакты 1 и 2 – это передающая пара, а контакты 3 и 6 - принимающая пара. Также кабели имеют цветную маркировку проводов для удобства в работе. Для подключения платы компьютерной телефонии к концентратору или коммутатору Ethernet, т.е. для подключения системы TDA к локальной сети, используется т.н. "прямой" кабель (также называемый "проходным" (straight through)).



Вилка RJ-45
Контакт 1
Зажим сзади

Новый стандарт T-568A для прямого кабеля **Действующий стандарт T-568B для прямого кабеля**

Примечание: стандарты T-568A и T-568B не имеют функциональных различий

Рис. 2 – кабель RJ-45 для Ethernet (витая пара)

IP-адресация

IP-адрес – это 32-разрядное число[2], представленное в виде четырех 8-разрядных десятичных чисел, разделенных точками. Типичный IP-адрес выглядит примерно так: 127.169.190.1 Компьютер преобразует этот адрес из десятичного в двоичный формат, что для нашего примера соответствует следующему числу: 01111111.10101001.10111110.00000001

Каждое из четырех чисел называется октетом. Октет может быть представлен любым числом от 0 до 255 включительно. Поскольку IP-адрес содержит четыре октета, то всего может существовать 4 294 967 296 уникальных IP-адресов.

IP-адрес уникален для каждого компьютера или любого другого сетевого устройства (например, TDA) и отличает его от других устройств в сети. Это важно при работе в сети Интернет или в любой другой сети, так как устройствам необходим уникальный идентификатор, чтобы они могли передавать и принимать сообщения в виде пакетов данных.

Следует отметить, что прежде чем подключать систему TDA к корпоративной сети Ethernet при помощи платы компьютерной телефонии, необходимо выполнить простое программирование при помощи программного обеспечения, прилагаемого к системе TDA. Сетевое устройство может получить IP-адрес одним из двух стандартных способов: либо автоматически, от специального DHCP-сервера (см. ниже), либо фиксированный (уникальный) IP-адрес будет присвоен устройству администратором сети. Плате компьютерной телефонии системы TDA требуется фиксированный IP-адрес, который необходимо ввести в память системы в процессе программирования.

Чтобы лучше понять принципы работы с IP-адресами, познакомимся с тем, как происходит проверка IP-адреса вашего собственного компьютера (если он подключен к какой-нибудь сети).

Попробуйте узнать ваш IP-адрес, выполняя следующие простые действия:

- В ОС Windows нажмите кнопку «Пуск» (Start) и выберите «Выполнить…» (Run…). Появится небольшое окно.
- Введите в поле 'Cmd' (Windows NT, 2000, XP) или 'Command' (Windows 95, 98, ME) в зависимости от версии Windows, установленной на компьютере.
- После этого появится диалоговая оболочка, иногда ошибочно называемая окном DOS.
- В командной строке (например, **C:/>**) наберите **Winipcfg** (Wndows 95, 98, ME) или **ipconfig** (Windows NT, 2000, XP) и нажмите клавишу ENTER.
- В результате на экран будет выведен IP-адрес компьютера, а также маска подсети и шлюз, используемый по умолчанию.

На экране должна появиться подобная информация (IP-адрес компьютера):

IP-адрес	**192.170.40.154**
Маска подсети	**255.255.255.0**
Шлюз, используемый по умолчанию	**192.170.40.1**

Если вам известен IP-адрес какого-нибудь другого устройства, подключенного к той же сети, например, IP-адрес системы TDA, можно легко проверить, может ли компьютер корректно взаимодействовать с TDA или нет. Предположим, что IP-адрес TDA - 192.170.40.199. Теперь выполните следующие действия на компьютере:

- В ОС Windows нажмите кнопку «Пуск» (Start) и выберите «Выполнить…» (Run…). Появится небольшое окно.
- Введите в поле 'Cmd' (Windows NT, 2000, XP) или 'Command' (Windows 95, 98, ME) в зависимости от версии Windows, установленной на компьютере.
- После этого появится диалоговая оболочка, иногда ошибочно называемая окном DOS.
- В командной строке (например, **C:/>**) наберите **ping 192.170.40.199** и нажмите клавишу ENTER.

Если все сделано правильно и компьютер может корректно взаимодействовать с платой компьютерной телефонии системы TDA, на экране компьютера появится примерно следующий результат выполнения команды Ping:

Pinging 192.170.40.199 with 32 bytes of data:

Reply from 192.170.40.199: bytes=32 time<10ms TTL=255
Reply from 192.170.40.199: bytes=32 time<10ms TTL=255
Reply from 192.170.40.199: bytes=32 time<10ms TTL=255
Reply from 192.170.40.199: bytes=32 time<10ms TTL=255

Ping statistics for 192.170.40.199:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

ПРИМЕЧАНИЕ: Обратите внимание, что не стоит пытаться изменить IP-адрес компьютера без разрешения сетевого администратора. Несанкционированное изменение IP-адреса может привести к тому, что компьютер будет неспособен взаимодействовать с сетью, и в результате важные данные могут быть потеряны.

Частные IP-сети

Частный IP-адрес – это локальный IP-адрес в частной сети, которая не связана с какой-либо сетью общего пользования, например, сетью Интернет. Так, при необходимости подключить несколько систем TDA к локальной сети с целью демонстрации их функциональности потенциальному покупателю, нужно будет выделить частный IP-адрес каждой из систем.

Даже если сетевые устройства не будут иметь доступ к сети Интернет, то всё равно при назначении их частных IP-адресов лучше воспользоваться рекомендациями IANA – Internet Assigned Numbers Authority (Агентство по выделению имен и уникальных параметров протоколов Интернет). Технически в частной сети можно использовать любые допустимые IP-адреса, но если существует вероятность, что существующие требования к сети в будущем изменятся, сеть разрастется, и потребуется соединить ее с корпоративной сетью передачи данных или даже с сетью Интернет, то в этом случае необходимо следовать рекомендациям IANA.

Для частных сетей IANA выделило следующие диапазоны IP-адресов:

- **от 10.0.0.0 до 10.255.255.255**
- **от 172.16.0.0 до 172.31.255.255**
- **от 192.168.0.0 до 192.168.255.255**

Эти адреса не разглашаются и не трассируются (т.е. если рабочий компьютер имеет IP-адрес 192.168.0.1, никто, кроме сотрудников компании не сможет получить доступ к этому компьютеру, так как с точки зрения внешнего компьютера этот адрес является недоступным).

Маски подсети (Subnet mask)

Маска подсети позволяет преобразовать одну большую IP-сеть в несколько подсетей. Предположим, требуется подключить восемь АТС TDA и ещё пару компьютеров к частной сети с использованием IP-адресов из диапазона

192.168.0.1 ~ 192.168.0.10

В этом случае лучше всего было бы использовать такую маску подсети: 255.255.255.0. Это позволит всем вашим сетевым устройствам взаимодействовать друг с другом. Однако если вы по ошибке используете вот такую маску подсети: 255.255.0.255, то ни одно из сетевых устройств не будет способно взаимодействовать с другими устройствами.

Чтобы лучше понять смысл маски подсети, преобразуем октеты маски подсети в двоичную форму:

маска подсети 255.255.255.0 = 11111111.11111111.11111111.00000000,

тогда как маска подсети 255.255.0.255 = 11111111.11111111.00000000.11111111

(Примечание: запись 0 = 00000000 использована только в целях иллюстрации)

Метод назначения маски подсети заключается в следующем: при необходимости блокировать (не распознавать) какой-либо из октетов IP-адресов в сети, вы должны в маске подсети установить для этого октета значение 1, а при необходимости разрешить октет - значение 0. Таким образом, в нашем примере, если используется маска подсети **255.255.255.0** для IP-адресов с 192.168.0.1 по 192.168.0.10, то первые три октета IP-адресов (192.168.0) блокируются (не распознаются), и доступ к сети разрешён IP-адресам вида x.x.x.1~10. Однако если используется маска подсети **255.255.0.255**, то блокируются первый, второй и четвёртый октеты (192.168.x.0~10), и так как все устройства в нашем примере имеют "0" в третьем октете, то они не смогут корректно работать в нашей подсети, т.к. их адреса будут неотличимы друг от друга.

Концентраторы, коммутаторы, маршрутизаторы

Концентраторы (Hub)

Концентраторы используются для соединения двух и более сегментов сети Ethernet любого типа друг с другом. В больших сетях Ethernet, где используются достаточно длинные кабели, сигнал может значительно ослабляться при передаче. Концентраторы обеспечивают усиление сигнала, что позволяет существенно удлинять кабельные участки. Концентратор принимает входящий сигнал и ретранслирует его.

Концентраторы Ethernet необходимы в сетях с топологией «звезда», как, например, сети 10BASE-T. Важно отметить, что только концентраторы позволяют пользователям совместно использовать сеть Ethernet. Сеть с концентраторами называется «shared Ethernet», т.е. сеть Ethernet коллективного доступа, что означает, что все устройства в сети (например, компьютеры или АТС TDA) соревнуются за право передачи своих данных по сети. Таким образом, отдельные элементы сети коллективного доступа получают в свое распоряжение лишь какую-то часть от доступной пропускной способности сети. Обычно в коллективной сети Ethernet эффективно передается только 35-40% пакетов данных, тогда как передача остальных 60-65% связана с возникновением так называемых "коллизий" ("столкновений" пакетов данных).

Это означает, что в сети Ethernet со скоростью 10 Мбит/с средняя пропускная способность составляет всего лишь около 3-4 Мбит/с.

Коммутаторы (Switch)

Коммутаторы фиксируют адреса устройств, подключенных к сети Ethernet на каждом ее участке, и пропускают только необходимый трафик. Когда коммутатор получает пакет, он определяет, в каких участках сети находятся адресат и отправитель. Если участок один и тот же, пакет отбрасывается (фильтруется); если участки разные, то коммутатор перенаправляет его на нужный участок. Коммутаторы фильтруют пакеты данных и перенаправляют их на сетевой участок адресата, тем самым предотвращая сетевые конфликты (коллизии) и обеспечивая эффективное использование пропускной способности сети.

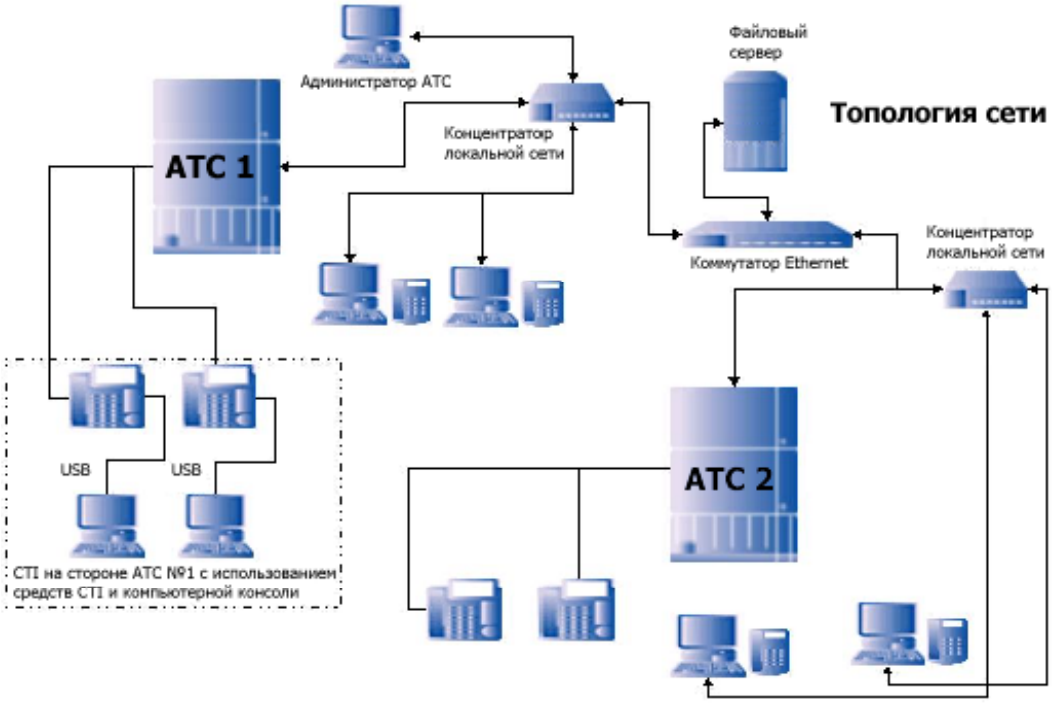


Рис. 3 - Топология сети, обеспечивающей передачу данных между телефонными системами.

По архитектуре коммутаторы подразделяются на коммутаторы типа «получил-передал» (cut-through) и коммутаторы с промежуточным хранением (store and forward). Коммутатор типа «получил-передал» проверяет адрес получателя пакета данных только перед отправкой этого пакета в сетевой участок адресата, а коммутатор с промежуточным хранением принимает и анализирует весь пакет перед тем, как перенаправить его к адресату.

Маршрутизаторы (Router)

Маршрутизаторы сортируют сетевой трафик не по адресам пакетов, а, скорее, по видам протоколов. Маршрутизаторы обеспечивают логическое разделение, а не физическое. IP-

маршрутизатор может разделять сеть на различные подсети так, чтобы между отдельными частями сети доставлялись только пакеты, посылаемые на определенные IP-адреса.

Сетевые серверы (backend servers)

Сервер DHCP

Для того чтобы подключить компьютер к локальной IP-сети, ему надо назначить IP-адрес. Для этого сетевой администратор должен отредактировать настройки сети на этом компьютере. Однако для больших сетей, состоящих из сотен или даже тысяч компьютеров, это невозможно, поэтому в таких сетях IP-адреса назначаются автоматически при помощи специального сервера, называемого DHCP-сервером[3].

Когда компьютер подключается к сети с DHCP-сервером, он запрашивает свой IP-адрес и другие необходимые сетевые параметры у DHCP-сервера. Сервер проверяет права компьютера на доступ к сети и затем назначает ему параметры из имеющейся базы параметров.

Например, когда вы подключаетесь к сети Интернет, сервер вашего интернет-провайдера после регистрации отправляет вашему компьютеру все необходимые сетевые параметры, включая IP-адрес. При отключении компьютера от сети, его IP-адрес освобождается и может быть выделен кому-то другому, кто подключится к тому же провайдеру.

DNS-сервер

В отличие от людей компьютеры хорошо понимают и запоминают числа. Когда вы подключаете восемь систем TDA к IP-сети, чрезвычайно сложно запомнить IP-адрес каждой системы. Поэтому существует специальный сетевой сервер, называемый DNS-сервер – сервер доменных имен. Именно служба доменных имен (DNS) позволяет вам, набрав адрес www.google.co.uk, попасть на знаменитый поисковый веб-сайт Google. Не будь службы DNS, то каждый раз, чтобы попасть на сайт Google, приходилось бы вводить некоторое загадочное число, например, что-нибудь вроде 213.171.95.43. Администратор локальной сети может назначить каждой системе TDA определенное имя в соответствии с ее IP-адресом. После этого, чтобы связаться с системой, нужно будет всего лишь ввести удобное для запоминания имя, например, АТС1, АТС2, АТС3 и т.д.

Основные термины

№	Термин	Объяснение
1	SMTP	Simple Mail Transfer Protocol. Используется для отправки электронной почты.
2	POP	Post Office Protocol. Протокол используется для получения электронной почты со стандартного сервера электронной почты. Протоколы SMTP и POP являются стандартными протоколами электронной почты и составляют основу всех почтовых программ электронной почты (Outlook, Eudora, Netscape и т.д.).
3	FTP	File Transfer Protocol. Протокол обеспечивает передачу файлов по сети на большие расстояния.
4	HTTP	Hypertext Transfer Protocol. Протокол используется для передачи гипертекстовых (HTML) документов (веб-страниц) в сетях TCP/IP и является основой всемирной сети WWW.
5	Proxy server	Прокси-сервер - компьютерное приложение, которое располагается между пользователем и внешней сетью (например, сетью Интернет). Оно принимает запросы от пользователя, посылает эти запросы во внешнюю сеть от лица пользователя, получает ответы на имя пользователя и в конечном итоге передает ответы пользователю.
6	Firewall	Брандмауэр – это механизм, разработанный для защиты сети передачи данных от проникновения извне. Брандмауэры могут быть реализованы как программно, так и аппаратно. По соображениям безопасности (и в первую очередь для защиты от хакеров) все сети передачи данных защищены теми или иными брандмауэрами.
7	NAT	Network Address Translation. Трансляция сетевых адресов – процедура преобразования IP-адреса одной сети в IP-адрес другой сети. Одна сеть обозначается как *внутренняя* сеть и другая – как *внешняя*. Как правило, в исходящих пакетах данных локальные сетевые адреса, используемые в пределах корпоративной сети, преобразуются в один или несколько глобальных внешних IP-адресов и наоборот –

		во входящих пакетах глобальные IP-адреса преобразуются в локальные IP-адреса. Это полезно для целей обеспечения безопасности, так как каждый исходящий или входящий запрос должен пройти процесс преобразования, что дает возможность проверять разрешение на передачу такого запроса или сравнивать его с предыдущим запросом. Транслятор сетевых адресов также экономит число необходимых компании глобальных IP-адресов, что позволяет компании использовать один IP-адрес для связи с миром. Транслятор является частью **маршрутизатора** и часто включается в состав корпоративного **брандмауэра**.

Примечания

[1] CSMA/CD (Carrier Sense Multiple Access / Collision Detect) - Множественный доступ с контролем несущей / Обнаружение конфликтов.

[2] В протоколе IP-V4 используется 32-разрядная адресация, тогда как в следующем поколении протокола IP-V6 адреса состоят из 48 битов, что позволяет объединять в сеть гораздо больше устройств и снимает проблему нехватки IP-адресов.

[3] DHCP (Dynamic Host Control Protocol) – Протокол динамической конфигурации хоста. Это механизм, обеспечивающий выделение различным устройствам IP-адресов из базы доступных адресов.

Настоящий документ защищён авторским правом и не может быть воспроизведен любым способом, полностью или частично, без предварительного письменного разрешения компании Panasonic (CIS) Oy.

Все сторонние торговые знаки, упоминаемые в настоящем документе, принадлежат их соответствующим владельцам.