Аппаратное и программное обеспечение ЭВМ и сетей

Раздел 5 Сети TCP/IP. Сетевой уровень. Транспортный уровень. Прикладной уровень

Тема № 21

Протоколы DHCP, ICMP

Протокол DHCP

- Для нормальной работы сети каждому сетевому интерфейсу компьютера и маршрутизатора должен быть назначен IP-адрес.
- Назначение IP-адресов может происходить вручную в результате выполнения процедуры конфигурирования интерфейса, для компьютера, маршрутизатора. При этом администратор должен помнить, какие адреса из имеющегося множества он уже использовал для других интерфейсов, а какие еще свободны. При конфигурировании администратор должен назначить клиенту не только IP-адрес, но и другие параметры стека TCP/IP, необходимые для его эффективной работы, например маску и IP-адрес маршрутизатора по умолчанию, IP-адрес сервера DNS, доменное имя компьютера и т. п. При большом размере сети эта работа представляет для администратора утомительную процедуру.
- Протокол динамического конфигурирования хостов (**Dynamic Host Configuration Protocol**, DHCP) автоматизирует процесс конфигурирования сетевых интерфейсов, гарантируя защиту от дублирования адресов за счет централизованного управления их распределением. Работа DHCP описана в RFC 2131 и 2132.

Протокол DHCP *Dynamic Host Configuration Protocol* Режимы DHCP

- Протокол DHCP работает в соответствии с моделью клиент-сервер. Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес и некоторые другие конфиг- параметры.
- При этом **сервер DHCP может работать в разных режимах**,:
  - **ручное назначение статических адресов;**
  - **автоматическое назначение статических адресов;**
  - **автоматическое распределение динамических адресов.**
- Во всех режимах работы администратор при конфигурировании DHCP-сервера сообщает ему один или несколько диапазонов IP-адресов, причем все эти адреса относятся к одной сети, то есть имеют одно и то же значение в поле номера сети.
- **В ручном режиме** администратор, помимо пула доступных адресов, снабжает DHCP-сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов. DHCP-сервер, пользуясь этой информацией, всегда выдает определенному DHCP-клиенту один и тот же назначенный ему администратором IP-адрес (а также набор других конфигурационных параметров.

Протокол DHCP Режимы DHCP (продолжение)

- **В режиме автоматического назначения статических адресов** DHCP-сервер самостоятельно без вмешательства администратора произвольным образом выбирает клиенту IP-адрес из пула наличных IP-адресов. Адрес дается клиенту из пула в постоянное пользование, то есть между идентифицирующей информацией клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первого назначения DHCP-сервером IP-адреса клиенту. При всех последующих запросах сервер возвращает клиенту тот же самый IP-адрес.
- **При динамическом распределении адресов** DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды. Когда компьютер, DHCP-клиент, удаляется из подсети, назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес.

Алгоритм динамического назначения адресов DHCP

- Администратор управляет процессом конфигурирования сети, определяя два основных параметра конфигурации DHCP-сервера: пул адресов, доступных распределению, и срок аренды. *Срок аренды диктует, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от DHCP-сервера. Срок аренды зависит от режима работы пользователей сети.* Если это небольшая сеть учебного заведения, куда со своими компьютерами приходят многочисленные студенты для выполнения лабораторных работ, то срок аренды может быть равен длительности лабораторной работы. Если же это корпоративная сеть, в которой сотрудники предприятия работают на регулярной основе, то срок аренды может быть достаточно длительным — несколько дней или даже недель.
- DHCP-сервер должен находиться в одной подсети с клиентами, учитывая, что клиенты посылают ему широковещательные запросы. Для снижения риска выхода сети из строя из-за отказа DHCP-сервера в сети иногда ставят резервный DHCP-сервер (такой вариант соответствует сети 1 на рис. 5-21.1).

Протокол DHCP

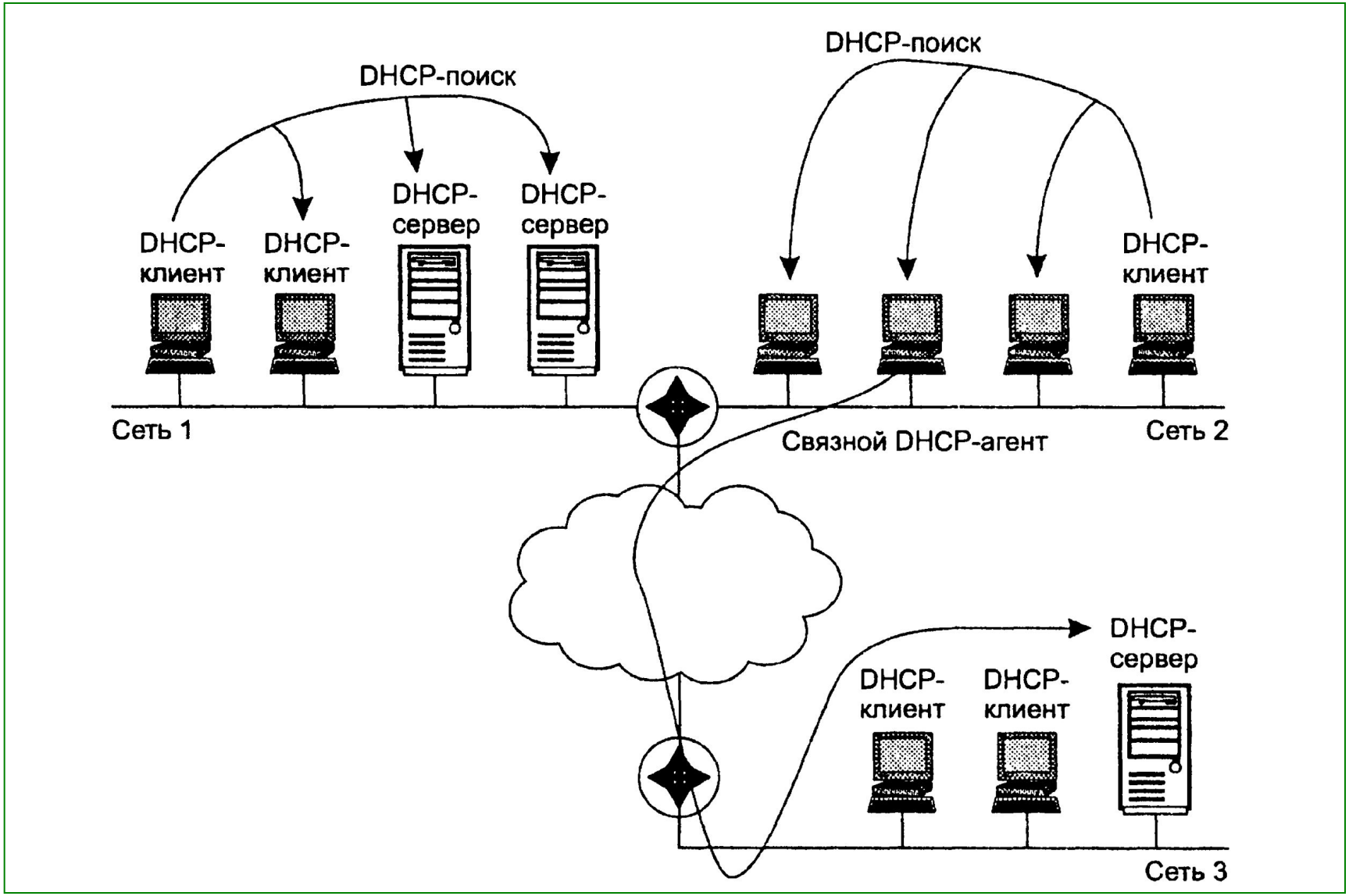


Рис. 5-21.1. Схемы взаимного расположение серверов и клиентов DHCP

Протокол DHCP

- Иногда наблюдается и обратная картина: в сети нет ни одного DHCP-сервера, его подменяет связной DHCP-агент — программное обеспечение, играющее роль посредника между DHCP-клиентами и DHCP-серверами (пример такого варианта — сеть 2 на рисунке). Связной агент переправляет запросы клиентов из сети 2 DHCP-серверу сети 3. Таким образом, один DHCP-сервер может обслуживать DHCP-клиентов нескольких разных сетей.
- Ниже дана упрощенная схема обмена сообщениями между клиентскими и серверными частями DHCP.
- 1. Когда компьютер включают, установленный на нем DHCP-клиент посылает ограниченное широковещательное сообщение DHCP-поиска (IP-пакет с адресом назначения, состоящим из одних единиц, который должен быть доставлен всем узлам данной IP-сети).
- 2. Находящиеся в сети DHCP-серверы получают это сообщение. Если в сети DHCP-серверы отсутствуют, то сообщение DHCP-поиска получает связной DHCP-агент. Он пересылает это сообщение в другую, возможно, значительно отстоящую от него сеть DHCP-серверу, IP-адрес которого ему заранее известен.

Упрощенная схема обмена протокол DHCP

- 3. Все DHCP-серверы, получившие сообщение DHCP-поиска, посылают DHCP-клиенту, обратившемуся с запросом, свои DHCP-предложения. Каждое предложение содержит IP-адрес и другую конфигурационную информацию. (DHCP-сервер, находящийся в другой сети, посылает ответ через агента.)
- 4. DHCP-клиент собирает конфигурационные DHCP-предложения ото всех DHCP-серверов. Как правило, он выбирает первое из поступивших предложений и отправляет в сеть широковещательный DHCP-запрос. В этом запросе содержатся идентификационная информация о DHCP-сервере, предложение которого принято, а также значения принятых конфигурационных параметров.
- 5. Все DHCP-серверы получают DHCP-запрос, и только один выбранный DHCP-сервер посылает положительную DHCP-квитанцию (подтверждение IP-адреса и параметров аренды), а остальные серверы аннулируют свои предложения, в частности возвращают в свои пулы предложенные адреса.
- 6. DHCP-клиент получает положительную DHCP-квитанцию и переходит в рабочее состояние.

Протокол DHCP

- Время от времени компьютер пытается обновить параметры аренды у DHCP-сервера. Первую попытку он делает задолго до истечения срока аренды, обращаясь к тому серверу, от которого он получил текущие параметры. Если ответа нет или ответ отрицательный, он через некоторое время снова посылает запрос. Так повторяется несколько раз, и, если все попытки получить параметры у того же сервера оказываются безуспешными, клиент обращается к другому серверу. Если и другой сервер отвечает отказом, то клиент теряет свои конфигурационные параметры и переходит в режим автономной работы.
- DHCP-клиент может и по своей инициативе досрочно отказаться от выделенных ему параметров.
- **Недостатки DHCP** В сети, где адреса назначаются динамически, нельзя быть уверенным в адресе, который в данный момент имеет тот или иной узел. И такое непостоянство IP-адресов влечет за собой некоторые проблемы.

Протокол DHCP- Недостатки

- **Во-первых**, ***возникают сложности при преобразовании символьного доменного имени в IP-адрес***. Действительно, представьте себе функционирование системы DNS, которая должна поддерживать таблицы соответствия символьных имен IP-адресам в условиях, когда последние меняются каждые два часа! Учитывая это обстоятельство, для серверов, к которым пользователи часто обращаются по символьному имени, назначают статические IP-адреса, оставляя динамические только для клиентских компьютеров. Однако в некоторых сетях количество серверов настолько велико, что их ручное конфигурирование становится слишком обременительным. Это привело к разработке усовершенствованной версии DNS (так называемой динамической системы DNS), в основе которой лежит согласование информационной адресной базы в службах DHCP и DNS.

Протокол DHCP

- **Во-вторых, *трудно осуществлять удаленное управление и автоматический мониторинг интерфейса* (например, сбор статистики), если в качестве его идентификатора выступает динамически изменяемый IP-адрес**.
- Наконец, для обеспечения безопасности сети многие сетевые устройства могут блокировать (фильтровать) пакеты, определенные поля которых имеют некоторые заранее заданные значения. Другими словами, при динамическом назначении адресов ***усложняется фильтрация пакетов по IP-адресам.***
- Последние две проблемы проще всего решаются отказом от динамического назначения адресов для интерфейсов, фигурирующих в системах мониторинга и безопасности.

Протокол ICMP

- **Протокол межсетевых управляющих сообщений (Internet Control Message Protocol, ICMP)** играет в сети вспомогательную роль, но тем не менее важную роль, он всегда востребован.
- Протокол ICMP не предназначен для исправления возникших при передаче пакета проблем: если пакет потерян, ICMP не может послать его заново. Задача ICMP другая — он является средством оповещения отправителя о «несчастных случаях», произошедших с его пакетами. Протокол ICMP «отслеживает» передвижение пакета по сети и при отбрасывании пакета маршрутизатором передает сообщение об этом узлу-источнику, обеспечивая таким образом обратную связь между посланным пакетом и отправителем.

Назначение протокола ICMP – констатация ошибок, проблем связанных с доставкой пакетов IP на том или ином участке сети. ICMP протокол применяется также для диагностики и мониторинга сети. Спецификация этого протокола содержится в RFC 792.

- Существует ряд ситуаций, когда протокол IP не может доставить пакет адресату, например, когда истекает время жизни пакета, когда в таблице маршрутизации отсутствует маршрут к заданному в пакете адресу назначения, когда пакет не проходит проверку по контрольной сумме, когда шлюз не имеет достаточно места в своем буфере для передачи какого-либо пакета и т. д. и т. п..
- Пусть, например, протокол IP, работающий на каком-либо маршрутизаторе, обнаружил, что пакет для дальнейшей передачи по маршруту необходимо фрагментировать, но в пакете установлен признак DF (не фрагментировать). Протокол IP, обнаруживший, что он не может передать IP-пакет далее по сети, должен отправить ***диагностическое*** ICMP-сообщение узлу-источнику и только потом отбросить пакет.

Протокол ICMP

- Помимо диагностики ICMP также используется для ***мониторинга*** сети. Так, в основе популярных утилит для мониторинга IP-сетей ping и tracert лежат ICMP-сообщения. С помощью ICMP-сообщений приложение может определить маршрут перемещения данных, оценить работоспособность сети, определить время прохождения данных до заданного узла, сделать запрос о значении маски определенного сетевого интерфейса и т. п.
- Заметим, что некоторые из пакетов могут исчезнуть в сети, не вызвав при этом никаких оповещений. В частности, протокол ICMP не предусматривает передачу сообщений о проблемах, возникающих при обработке IP-пакетов, несущих ICMP-сообщения об ошибках. (Это правило, однако, не действует для ICMP - запросов.) Такое решение было принято разработчиками протокола, чтобы не порождать «штормы» в сетях, когда количество сообщений об ошибках лавинообразно возрастает. По этой же причине ICMP-сообщения не передаются, если ошибка возникла при передаче какого-либо фрагмента, кроме первого, а также когда потерянный пакет имел широковещательный IP-адрес или был упакован в кадр с широковещательным адресом несущей технологии.

Поскольку IP-пакет содержит адрес отправителя, но не содержит никакой адресной информации о промежуточных маршрутизаторах, ICMP-сообщения направляются только конечным узлам. Здесь сообщения могут быть обработаны либо ядром операционной системы, либо протоколами транспортного и прикладного уровней, либо приложениями, либо просто проигнорированы. Важно, что обработка ICMP-сообщений не входит в обязанности протоколов IP и ICMP.

Протокол ICMP

Типы ICMP-сообщений

- Все типы ICMP-сообщений могут быть разделены на два класса:
  - диагностические сообщения об ошибках;
  - информационные сообщения типа запрос/ответ.
- ICMP-сообщение инкапсулируется в поле данных IP-

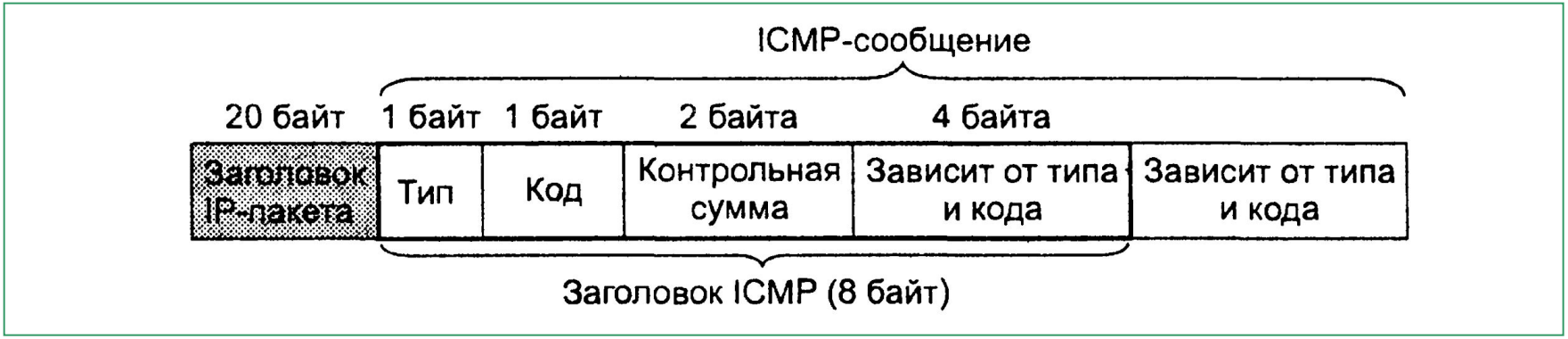


Рис. 5-21.6. Инкапсуляция и формат ICMP-сообщения

Протокол ICMP

- **Заголовок ICMP состоит из 8 байт; поля заголовка перечислены ниже**.
  - **Тип** (размером 1 байт) содержит код, определяющий тип сообщения. Основные типы сообщений перечислены в табл. 5-21.4.
  - **Код** (размером 1 байт) более тонко дифференцирует тип ошибки.
  - **Контрольная сумма,** подсчитанная для всего ICMP-сообщения, занимает 2 байта.
  - **Поле из 4 байт**:
    1. В сообщениях типа **запрос/ответ это поле содержит 2-байтовые подполя идентификатора** и **порядкового номера** (см. далее). Числа из этих подполей дублируются из сообщения-запроса в сообщение-ответ. **Идентификатор** позволяет узлу-получателю сообщения определить, какому приложению направлен этот ответ, а **порядковый номер** используется приложением, чтобы связать ответ с соответствующим запросом (учитывая, что одно приложение может выдать несколько

Протокол ICMP

Таблица 5-21.1. Возможные значения поля типа

Значение	**Тип сообщения**
0	Эхо-ответ
3	Узел назначения недостижим
4	Подавление источника
5	Перенаправление маршрута
8	Эхо-запрос
11	Истечение времени дейтаграммы
12	Проблема с параметром пакета
13	Запрос отметки времени
14	Ответ отметки времени
17	Запрос маски
18	Ответ маски

Протокол ICMP

- **Каждый тип ошибки** может быть более точно охарактеризован кодом ошибки. Например, в табл. 5-21.2 приведены коды для сообщения о недостижимости узла назначения (ошибка типа 3 из предыдущей таблицы). Эти коды, которые могут быть указаны в сообщении этого типа, позволяют выявить множество различных причин данной ситуации. Недостижимость узла назначения может, в частности, быть вызвана временной неработоспособностью аппаратуры, неверным адресом назначения, отсутствием протокола прикладного уровня или открытого порта UDP/TCP в узле назначения.

Протокол ICMP

- **Таблица 5-21.2.** Коды, детализирующие причину ошибки о недостижимости узла назначения, тип 3 таблица 5-21.1

Код	Причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
4	Требуется фрагментация, а бит DF установлен
5	Ошибка в маршруте, заданном источником
6	Сеть назначения неизвестна
7	Узел назначения неизвестен
8	Узел-источник изолирован
9	Взаимодействие с сетью назначения административно запрещено
10	Взаимодействие с узлом назначения административно запрещено
11	Сеть недостижима для заданного класса сервиса
12	Узел недостижим для заданного класса сервиса
13	Взаимодействие административно запрещено путем фильтрации

Протокол ICMP

- **Формат поля данных ICMP-сообщения также зависит от значений полей типа и кода**. Чтобы показать различия в форматах разных типов сообщений, рассмотрим два примера:
  - сообщения типа эхо-запрос и эхо-ответ;
  - сообщение о недостижимости узла назначения.
- **Формат эхо- запроса / эхо- ответа и утилита *ping***
- На рис. 5-21.2 показаны форматы эхо- запроса и эхо- ответа. Они отличаются друг от друга только значением поля типа (нули — для ответа, единицы — для запроса). В **поле данных запроса отправитель помещает информацию, которую затем получает в ответе от узла назначения.**

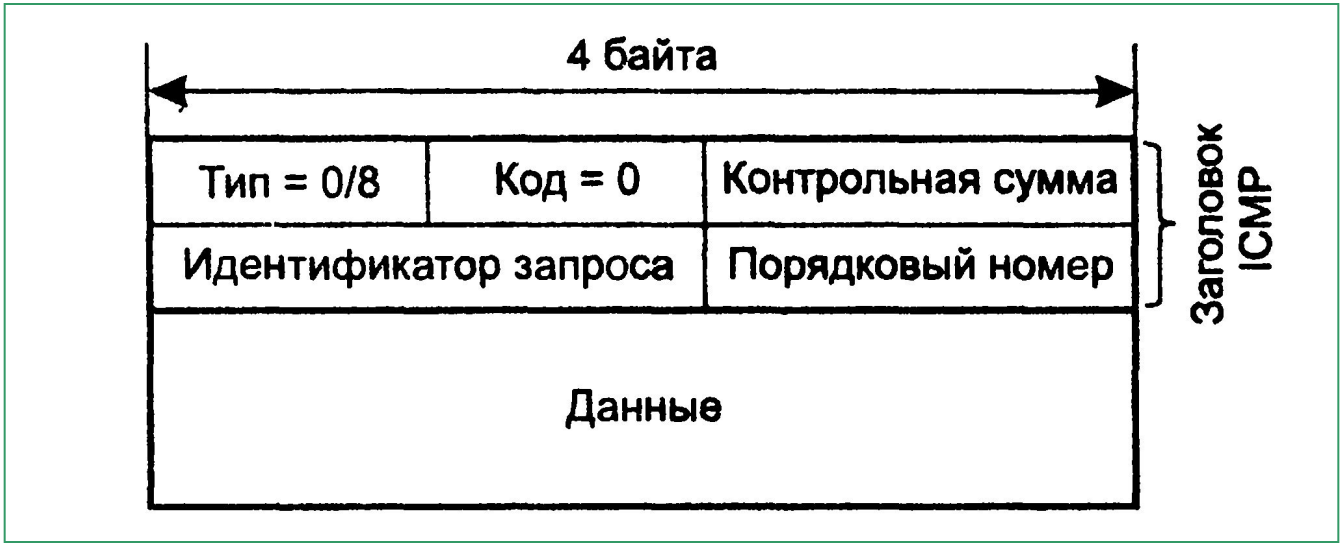


Рис. 5-21.2 Формат ICMP-сообщений типа эхо-запрос/эхо-ответ

Протокол ICMP

- Эхо-запрос и эхо-ответ, в совокупности называемые эхо- протоколом, представляют собой очень простое средство мониторинга сети. Компьютер или маршрутизатор посылает по составной сети эхо-запрос, указывая в нем IP-адрес узла, достижимость которого нужно проверить. Узел, получивший эхо-запрос, формирует и отправляет эхо-ответ отправителю запроса. Так как эхо-запрос и эхо-ответ передаются по сети внутри IP-пакетов, то их успешная доставка означает нормальное функционирование всей транспортной системы составной сети.
- Во многих операционных системах используется утилита ping, предназначенная для тестирования достижимости узлов. Эта утилита обычно посылает серию эхо- запросов к тестируемому узлу и предоставляет пользователю статистику об утерянных эхо- ответах и среднем времени реакции сети на запросы. Утилита ping выводит на экран сообщения следующего вида обо всех поступивших ответах:

ping **serverl.citmgu.ru**

Pinging **serverl.citmgu.ru** [193.107.2.200] with 64 bytes of data:

Reply from 193.107.2.200: bytes-64 time-256ms TTL- 123

Reply from 193.107.2.200: bytes=64 time-310ms TTL= 123

Reply from 193.107.2.200: bytes=64 time=260ms TTL- 123

Reply from 193.107.2.200: bytes=64 time=146ms TTL= 123

Протокол ICMP

- Из приведенной распечатки видно, что в ответ на тестирующие запросы, посланные узлу **server1.mgu.ru**, было получено 4 эхо- ответа. Длина каждого сообщения составляет 64 байта. В следующей колонке помещены значения времени оборота (RTT), то есть времени от момента отправки запроса до получения ответа на тот запрос. Как видим, сеть работает достаточно нестабильно — время в последней строке отличается от времени во второй более чем в два раза. На экран выведено также оставшееся время жизни поступивших пакетов.
- В зависимости от конкретной реализации утилиты ping, а также ее настроек (ключей) выводимые экранные формы могут отличаться. У утилиты ping обычно имеется несколько ключей, с помощью которых можно установить размер поля данных сообщения, начальное значение поля TTL, количество повторных передач пакетов, флаг DF.
- В том случае, когда за установленное время тайм-аута ответы не приходят или протокол ICMP сообщает об ошибках, утилита ping выводит на экран соответствующие диагностические сообщения.

Протокол ICMP

Формат сообщения об ошибке и утилита traceroute

- На рис. 5-21.3 показан формат ICMP-сообщения об ошибке, в данном случае это сообщение о недостижимости узла назначения. Остальные ICMP-сообщения об ошибках имеют такой же формат и отличаются друг от друга только значениями полей типа и кода.

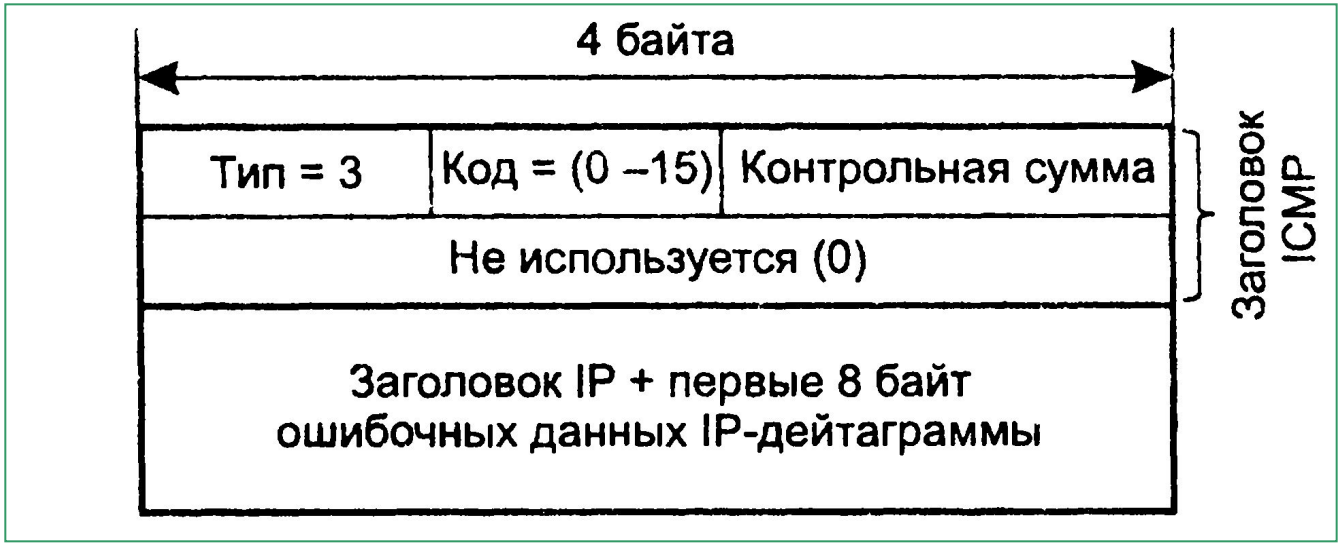


Рис. 5-21.3 Формат ICMP-сообщения об ошибке — недостижимости узла назначения

- Когда маршрутизатор не может передать или доставить IP-пакет, он отсылает узлу, отправившему этот пакет, сообщение о недостижимости узла назначения. В поле типа помещается значение 3, а в поле кода — значение из диапазона 0-15, уточняющее причину, по которой пакет не был доставлен. **Следующие за полем контрольной суммы 4 байт заголовка не используются и заполняются нулями.**

Протокол ICMP

- Помимо причины ошибки, указанной в заголовке, **в поле данных ICMP-сообщения всегда помещается заголовок IP и первые 8 байт данных того IP-пакета, который вызвал ошибку**. Эта информация позволяет узлу-отправителю точнее установить причину ошибки, так как все протоколы стека TCP/IP, использующие для передачи своих сообщений IP-пакеты, содержат наиболее важную для анализа информацию в первых 8 байт своих сообщений. В частности, ими вполне могут оказаться первые 8 байт заголовка TCP или UDP, в которых содержится информация, идентифицирующая приложение, пославшее потерянный пакет. Следовательно, при разработке приложения можно предусмотреть встроенные средства реакции на сообщения о не доставленных пакетах.
- Узел (или сеть) назначения может быть недостижим по причине временной неработоспособности аппаратуры из-за того, что отправитель указал неверный адрес назначения или маршрутизатор не имеет данных о пути к сети назначения. Недостижимость протокола и порта означает отсутствие реализации какого-либо протокола прикладного уровня в узле назначения или же отсутствие открытого порта протокола UDP или TCP в узле назначения.

Протокол ICMP

- Как было показано на примере утилиты ping, ICMP-сообщения эффективно используются для мониторинга сети. В частности, сообщения об ошибке истечения тайм-аута лежат в основе работы другой популярной утилиты traceroute для Unix, имеющей в Windows 2000 название tracert. Эта утилита позволяет проследить маршрут до удаленного хоста, определить RTT, IP-адрес и доменное имя для каждого промежуточного маршрутизатора (если это имя зарегистрировано в обратной зоне службы DNS). Такая информация полезна для локализации маршрутизатора, на котором обрывается путь пакета к удаленному хосту.
- Утилита traceroute осуществляет трассировку маршрута путем посылки обычных IP-пакетов с адресом назначения, являющимся конечной точкой изучаемого маршрута. Суть метода трассировки состоит в том, что значение TTL первого отправляемого пакета установлено равным 1. Когда протокол IP первого маршрутизатора принимает этот пакет, то он в соответствии со своим алгоритмом уменьшает значение TTL на 1 и получает 0. Маршрутизатор отбрасывает пакет с нулевым временем жизни и возвращает узлу-источнику ICMP-сообщение об ошибке истечения тайм-аута вместе с заголовком IP и первыми 8 байтами потерянного пакета.

Протокол ICMP

- Получив ICMP-сообщение о причине недоставки пакета, утилита traceroute запоминает адрес первого маршрутизатора (который извлекает из заголовка IP-пакета, несущего ICMP-сообщение) и вычисляет для него RTT. Затем traceroute посылает следующий IP-пакет, но теперь со значением TTL, равным 2. Этот пакет благополучно проходит первый маршрутизатор, но «умирает» на втором, о чем немедленно отправляется аналогичное ICMP-сообщение об ошибке истечения тайм-аута. Утилита traceroute запоминает адрес и время для второго маршрутизатора и т. д. Такие действия выполняются с каждым маршрутизатором вдоль маршрута вплоть до узла назначения.
- Мы рассмотрели работу утилиты traceroute весьма схематично, но и этого достаточно, чтобы оценить изящество идеи, лежащей в основе ее работы.

Протокол ICMP

- Ниже приведена копия экранной формы, выведенной утилитой tracert (Windows) при трассировке хоста **ds.internjc**.net [198.49.45.29]:

1 311 ms 290 ms 261 ms 144.206.192.100

2 281 ms 300 ms 271 ms 194.85.73.5

3 2023 ms 290 ms 311 ms **moscow-m9-2-S5.relcom.eu.net** [193.124.254.37]

4 290 ms 261 ms 280 ms MSK-M9-13 **Relcom.EU.net** [193.125.15.13]

5 270 ms 281 ms 290 ms **MSK.RAIL-l-ATM0-155Mb.Relcom.EU.net** [193 124.254.82]

6 300 ms 311 ms 290 ms **SPB-RASC0M-l-E3-l-34Mb.Relcom.EU.net** [193.124.254.78]

7 311 ms 300 ms 300 ms **Hssill-0.GW1.STK2.ALTER.NET** [146.188.33.125]

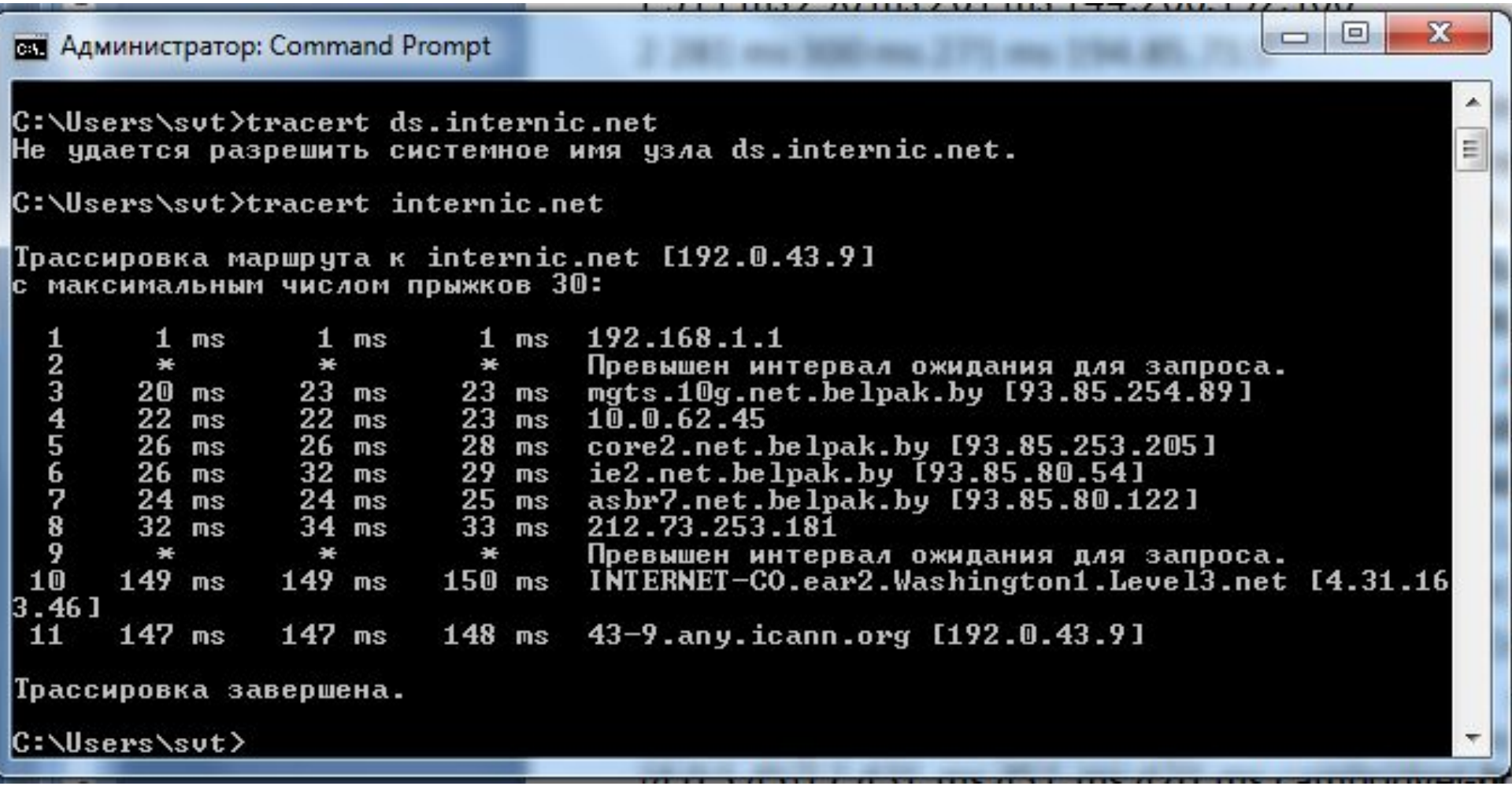
8 311 ms 330 ms 291 ms 421.ATM6-0-0.CR2.STK2.Alter.Net [146.188.5.73]

9 360 ms 331 ms 330 ms 219 **Hssi4-0.CR2.LND1.Alter.Ne**t [146.188.2.213]

10 351 ms 330 ms 331 ms **412.Atm5-0.BRl.LNDl.Alter.net** [146.188.3.205]

11 420 ms 461 ms 420 ms 167.ATM8-0-0.CR1.ATL1.Alter.Net [137.39.69.182]12 461 ms 441 ms 440 ms 311.ATM12-0-0.BR1.ATL1.Alter.Net [137.39.21 73]13 451 ms 410 ms 431 ms **atlantal-brl.bbnplanet.net** [4.0.2.141]14 420 ms 411 ms 410 ms **viennal-br2.bbnplanet.net** [4.0.3.154]15 411 ms 430 ms 2514 ms viennal-**nbr3.bbnplanet.net** [4.0.3.150]16 430 ms 421 ms 441 ms viennal-**nbr2.bbnplanet.net** [4.0.5.45]17 431 ms 451 ms 420 ms cambridgel-**brl.bbnplanet.net** [4.0.5.42]18 450 ms 461 ms 441 мс cambridgel-**crl4.bbnplanet.net** [4.0.3.94Ц9 451 мс 461 мс 460 мс **attbcstoll.bbnplanet.net** [206.34.99.38120 501 мс 460 мс 481 мс **shutdown.ds.internic.net** [198.49.45.29]

Протокол ICMP



Протокол ICMP

- Последовательность строк соответствует последовательности маршрутизаторов, образующих маршрут к заданному узлу. Первое число в строке — число хопов до соответствующего маршрутизатора. Утилита traceroute тестирует каждый маршрутизатор трижды, поэтому следующие три числа в строке — это значения RTT, вычисленные путем посылки трех пакетов, время жизни которых истекло на этом маршрутизаторе. Если ответ от какого-либо маршрутизатора не приходит за заданное время, то вместо времени на экране печатается звездочка (*).
- Далее идут IP-адрес и доменное имя (если оно имеется) маршрутизатора. Видно, что почти все интерфейсы маршрутизаторов поставщиков услуг Интернета зарегистрированы в службе DNS, а первые два, относящиеся к локальным маршрутизатором, — нет.
- Еще раз подчеркнем, что время, указанное в каждой строке, это не время прохождения пакетов между двумя соседними маршрутизаторами, а время, за которое пакет проделывает путь от источника до соответствующего маршрутизатора и обратно. Так как ситуация в Интернете с загрузкой маршрутизаторов постоянно меняется, то время достижимости маршрутизаторов не всегда нарастает

Тема 5 - 25. Протоколы DHCP и ICMP

Список использованных источников:

Литература:

1) **Олифер В. Г. Олифер. Н. А. Компьютерные сети.** Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 е.: ил. для данной темы см. 257-264;
2) **Э. Таненбаум** . Компьютерные сети. 4-е изд. /. — СПб.: Питер, 2003. — 992 с
3) **В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г.**