Network Working Group
Request for Comments: 950

J. Mogul (Stanford)
J. Postel (ISI)

August 1985

Стандартные процедуры организации подсетей IP

Internet Standard Subnetting Procedure

Статус документа

Этот документ описывает стандартный протокол для сообщества ARPA-Internet. При использовании подсетей настоятельно рекомендуется следовать описанным здесь процедурам.

Документ может распространяться свободно.

Обзор

В этом документе рассматривается разбиение сетей IP на подсети, являющиеся логическими фрагментами сетей IP. По административным и техническим соображениям многие организации предпочитают делить свои сети на несколько подсетей вместо приобретения нескольких блоков адресов IP (номеров сетей). В этом документе описываются процедуры организации подсетей и работы с ними. Описанные здесь процедуры применяются на хостах (например, рабочих станциях). Процедуры используемые для работы с подсетями на маршрутизаторах (шлюзах), описаны лишь частично. Основой для создания настоящего стандарта послужила работа RFC 940 [7].

Благодарности

Данный документ основан на результатах работы RFC 917 [1]. В разработке описываемого здесь стандарта участвовало много людей и особо хочется отметить значительный вклад J. Noel Chiappa, Chris Kent и Tim Mann. Важный вклад в разработку стандарта внесли также Zaw-Sing Su, Mike Karels и рабочая группа GADS[1].

1. Мотивация[2]

Исходное модель Internet представляла собой двухуровневую иерархию – на верхнем уровне находилась сеть Internet в целом, а на нижнем уровне располагались отдельные сети, каждая со своим номером. В Internet не используется иерархической топологии и двухуровневая иерархия связана лишь с интерпретацией адресов. В 2-уровневой модели каждый хост видит свою сеть, как единое целое, т. е., сеть можно трактовать как «черный ящик», к которому подключен набор хостов.

Хотя такое представление обеспечивает простоту и мощь, многие организации считают его неадекватным и добавляют третий уровень в иерархическую схему адресации Internet – в этом случае сеть IP рассматривается как набор подсетей.

Трехуровневая иерархия удобна для больших организаций (например, университетов или компаний, сети которых располагаются в нескольких зданиях), где множество ЛВС может входить в одну «локальную область». В таких случаях удобно трактовать каждую ЛВС как подсеть.

Существует несколько причин, по которым организация может использовать множество физических сетей:

- ***Различные топологии*** – зачастую (особенно в исследовательских организациях) в сети могут присутствовать ЛВС различных типов (например, Ethernet и сети с кольцевой топологией[3]).
- ***Технологические ограничения*** – большинству топологий ЛВС присущи те или иные ограничения (электрические параметры, число хостов в ЛВС, общая протяженность кабеля). Использование подсетей позволяет достаточно просто преодолеть эти ограничения (особенно ограничение протяженности кабеля).
- ***Насыщение сети*** – в локальных сетях могут возникать ситуации, когда небольшая группа хостов фактически монополизирует полосу пропускания сетевой среды. Общим решением таких проблем является сегментирование сети (разбиение на несколько фрагментов) с организацией раздельных кабельных систем.
- ***Использование каналов «точка-точка»*** - иногда «локальная сеть» (например, кампусная сеть университета) разделена на несколько фрагментов (например, ЛВС отдельных зданий), соединенных между собой скоростными каналами «точка-точка».

Организации, имеющие более одной ЛВС, могут выбрать один из трех вариантов распределения адресов IP:

1. Получить отдельный блок адресов для каждой локальной сети и не использовать подсетей.
2. Использовать для всей организации общий номер сети и распределять адреса независимо от расположения хостов (принадлежности хостов к ЛВС). Такой вариант получил название transparent subnets (прозрачные подсети).
3. Используя один номер сети, разделить адресное пространство на несколько подсетей в соответствии с имеющимися ЛВС. Такой вариант называется explicit subnets (явные подсети).

---

[1]Gateway Algorithms and Data Structures Task Force – группа по алгоритмам и структурам данных для шлюзов.

[2]Приведенные в этом разделе соображения отчасти утратили свою актуальность и сегодня разбиение на подсети диктуется зачастую совсем другими причинами. При переводе был полностью сохранен оригинальный текст. *Прим. перев.*

[3]FDDI, Token Ring. *Прим. перев.*

Каждый из вариантов имеет свои преимущества и недостатки. Первый вариант не требует добавления или изменения протоколов, но ведет к разрастанию таблиц маршрутизации Internet. Информация о внутренней структуре сети распространяется повсюду, хотя она мало кому нужна и в большинстве случаев не используется. В некоторых реализациях шлюзов может возникать проблема нехватки пространства в таблице маршрутов, поэтому такой вариант лучше не использовать[1].

Второй вариант требует использования неких соглашений или протоколов, позволяющих объединить множество ЛВС в одну сеть IP. Например, этот вариант можно реализовать в ЛВС, где каждый адрес IP транслируется в аппаратный адрес с использованием протокола ARP[2], имея мосты между ЛВС, которые будут перехватывать запросы ARP для нелокальных адресатов (см. RFC 925 [2]). Однако такое решение возможно не для всех технологий ЛВС, особенно в тех случаях, когда технология не использует протокол ARP или ЛВС не поддерживает широковещания. Более фундаментальная проблема заключается в том, что мосты должны узнавать к какой ЛВС принадлежит хост, возможно используя для этого широковещательные рассылки. По мере увеличения числа ЛВС расходы на поддержку такого широковещания будут быстро возрастать; расти будет и размер кэша трансляции в мостах, требуемого для преобразования адресов.

Третий вариант используется для явной поддержки подсетей. Он тоже имеет свои недостатки – в частности, требуется модификация протокола IP, которая влечет за собой необходимость изменения существующих реализаций IP (если планируется использовать их с подсетями). Однако требуемые изменения сравнительно невелики и после их внесения проблема будет эффективно решена[3]. Кроме того, этот вариант не требует каких-либо изменений, которые будут несовместимы с существующими хостами в сетях без разбиения на подсети.

После выбора одного из вариантов может оказаться, что хосты, которые предполагалось использовать в среде без подсетей, попадут в одну из подсетей (см. RFC 917 [1]). Такое решение может быть полезно в тех случаях, когда нет возможности явно поддерживать подсети или требуется постепенный переход.

2. Стандарты для подсетей

В этой главе сначала описаны предложения по интерпретации адресов IP для поддержки подсетей. После этого рассматриваются изменения программ на хостах, которые обеспечат поддержку подсетей. И, наконец, описаны процедуры определения способа интерпретации адресов, используемого в сети (т. е., значения маски).

2.1. Интерпретация адресов Internet

Предположим, что организация имеет сеть IP с зарегистрированным номером и планирует разделить свою сеть на несколько подсетей. Что в таких случаях нужно сделать?

Поскольку распределение битов локальной части адреса почти ничем не ограничено, для представления номеров подсетей может использоваться несколько вариантов:

1. **Поле переменной длины** - для нумерации подсетей используется произвольное число битов локальной части адреса. Размер поля номера подсети сохраняется в масштабах каждой подсети, но может различаться в разных подсетях. Если поле имеет нулевой размер, это говорит об отсутствии подсетей.
2. **Поле фиксированной длины** - для нумерации подсетей используется фиксированное число битов (например, 8).
3. **Поле переменной длины с автокодированием**. Классы сетей (размер поля номера сети) определяются значениями старших битов адреса IP – аналогично этому старшие биты локальной части адреса могут задавать размер поля номера подсети.
4. **Поле фиксированной длины с автокодированием**. Для нумерации подсетей используется заданное число битов.
5. **Маскирование битов.** Для идентификации битов номера сети используется битовая маска.

Какие критерии могут использоваться для выбора одной из 5 предложенных схем? Следует ли использовать схемы с автокодированием? Должна ли обеспечиваться возможность обнаружить наличие подсетей по адресу IP без использования дополнительной информации?

Отличительной особенностью автокодирования является то, что оно позволяет разделить пространство адресов на подсети различных размеров (обычно одна подсеть размером в половину адресного пространства и группа подсетей меньших размеров).

В качестве примера рассмотрим разбиение сети класса C с использованием схемы автокодирования. Старший бит показывает наличие (или отсутствие) большой подсети, а три следующих бита используются для идентификации подсетей меньших размеров. Если первый бит имеет нулевое значение, это указывает на большую подсеть (половина адресного пространства); 1 в старшем бите говорит о разбиении на более мелкие подсети. Поскольку для идентификации мелких подсетей используется 3 бита, такая схема позволяет создать 1 подсеть со 128 адресами и 8 подсетей по 16 адресов в каждой.

Для разработки стандарта на параметры и реализации подсетей с автокодированием схема кодирования должна быть зафиксирована и сохраняться неизменной в масштабе Internet.

Можно предположить повсеместное использование подсетей – это позволяет интерпретировать адреса без использования дополнительной информации.

Возможность определения принадлежности двух хостов к одной сети без привлечения дополнительной информации является важным обстоятельством. Однако с таким решением связан и существенный недостаток – оно может порождать проблемы для существующих сетей, в которых при нумерации хостов используются произвольные биты локальной части адреса. Иными словами, полезно иметь возможность управления использованием подсетей, независимого от распределения адресов хостов.

---

[1]Современные маршрутизаторы и протоколы маршрутизации не порождают таких проблем, но этот вариант все равно остается нежелательным по причине общей нехватки адресов IP и снижения уровня защиты сетей. *Прим. перев.*

[2]Address Resolution Protocol - протокол преобразования адресов. *Прим. перев.*

[3]В настоящее время эта проблема успешно разрешена. *Прим. перев.*

Альтернативный вариант обеспечивает независимое (от битов адреса) хранение информации о наличии подсетей (флага). Если флаг использования подсетей установлен, предполагается использование схемы с автокодированием. В противном случае считается, что сеть представляет собой единое целое.

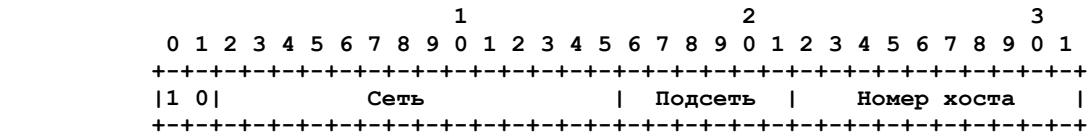
Если автокодирование не применяется, нет смысла использовать схему с полем фиксированной длины, поскольку это требует для каждой сети использовать тот или иной «флаг», говорящий об использовании подсетей и размере поля. А необходимость использования целого числа (размер поля номера подсети) взамен логического значения (факт использования подсетей) только осложняет задачу. Преимущество использования схемы с адресными масками состоит в том, что она позволяет каждой организации выбрать оптимальный вариант распределения хостов по подсетям и обеспечивает экономное использование адресного пространства. Следовательно, мы выбираем схему на основе масок как наиболее гибкую - издержки, связанные с реализацией этой схемы, не превышают издержек для других вариантов.

Например, адрес IP можно интерпретировать как:

<номер сети><номер подсети><номер хоста>

где поле <**номер сети**> определяется стандартом IP [3], поле <**номер хоста**> включает по крайней мере 1 бит, а поле <**номер подсети**> является постоянным для данной сети. Для полей **<номер подсети>** и **<номер хоста>** не требуется дополнительного структурирования. Если размер поля <**номер подсети**> равен 0, подсети не используются (адресация в соответствии с [3]).

Например, в сети класса B с 6-битовым номером подсети адрес будут интерпретироваться следующим образом:



Поскольку биты, идентифицирующие подсеть, указываются маской, эти биты не обязаны составлять непрерывный массив. Однако рекомендуется использовать для нумерации подсетей старшие биты локальной части адреса.

Специальные адреса

Из документа Assigned Numbers [9][1]:

«В некоторых случаях полезно зафиксировать некоторые адреса для выполнения специальных функций, а не для обозначения конкретных хостов. Обычно поле, состоящее из одних нулей интерпретируется, как «данная сеть», а поле адреса, состоящее только из единиц, интерпретируется, как «все хосты». Таким образом, запись 128.9.255.255 может интерпретироваться как «все хосты сети 128.9», а адрес 0.0.0.37 указывает на хост 37 в данной сети».

Полезно сохранить такую интерпретацию и для случаев использования подсетей. В соответствии с этим значения, состоящие только из нулей или единиц, не должны использоваться для нумерации реальных (физических) подсетей.

В приведенном выше примере 6-битовое поле номера подсети позволяет использовать номера от 1 до 62 (0 и 63 используются как служебные).

Отметим, что это не оказывает влияния и не создает новых ограничений для сетей без разбиения на подсети.

2.2. Изменение программ на хостах для поддержки подсетей

В большинстве реализаций IP имеется код, обслуживающий исходящие дейтаграммы и принимающий решение о передаче каждой дейтаграммы хосту локальной сети или пересылке ее на шлюз (маршрутизатор).

В общем случае этот фрагмент кода работает так:

```
IF ip_net_number(dg. ip_dest) = ip_net_number(my_ip_addr)
       THEN
                send_dg_locally(dg, dg.ip_dest)
       ELSE
                send_dg_locally(dg, gateway_to(ip_net_number(dg.ip_dest)))
```

(при обслуживании множества соединений, код становится более сложным, но в контексте данного документа это не имеет значения).

Для поддержки подсетей требуется сохранять одно или несколько 32-битовых значений, называемых масками. Это битовая маска с установленными битами в полях, соответствующих номеру сети IP, и дополнительными битами, установленными в соответствии с номером подсети.

Соответствующий код будет иметь вид:

```
IF bitwise_and(dg.ip_dest, my_ip_mask) = bitwise_and(my_ip_addr, my_ip_mask)
       THEN
send_dg_locally(dg, dg.ip_dest)
       ELSE
send_dg_locally(dg, gateway_to(bitwise_and(dg.ip_dest, my_ip_mask)))
```

Часть выражений в условиях может быть вычислена заранее.

Может потребоваться изменение функции gateway_to так, чтобы она принимала во внимание биты номера подсети при выполнении операций сравнения.

Для поддержки хостов с множеством подключений код может быть изменен так, чтобы значения my_ip_addr и my_ip_mask сохранялись независимо для каждого интерфейса. Проверка условий должна выполняться для каждого интерфейса таких хостов.

[1] В последнем варианте документа Assigned Numbers (RFC 1700) приводится более развернутое описание с учетом сложившейся практики использования подсетей. В настоящее время серия документов Assigned Numbers утратила силу и все данные из них перенесены в базу, доступную по адресу www.iana.org/numbers.html. *Прим. перев.*

2.3. Определение адресной маски

Как хост может определить, что в подсети, к которой подключен хост, используется адресная маска? Эта проблема аналогична некоторым проблемам сетевой загрузки хостов Internet – как хосту определить собственный адрес и как узнать адрес шлюза в локальной сети? Для всех трех случаев существуют два варианта решения – «аппаратная» информация или использование протоколов на базе широковещания.

К аппаратной информации относятся сведения, доступные хосту без подключения к сети (изолированному) – эти сведения могут быть включены в программный код или (предпочтительно) сохранены в дисковом файле. Однако для случая бездисковых станций, загружаемых через ЛВС ни один из этих вариантов не подходит.

Поскольку большинство технологий ЛВС поддерживают широковещание, лучшим вариантом для «свежезагруженного» хоста является широковещательная передача запроса на получение требуемой информации. Например, для определения адреса IP хост может использовать протокол RARP[1] [4].

Поскольку хосту после загрузки нужно собрать достаточно много информации (свой IP-адрес, аппаратный адрес шлюза, IP-адрес сервера доменных имен, маску подсети), более эффективно будет запросить всю требуемую информацию разом, нежели делать множество широковещательных запросов. Механизм, разработанный для загрузки бездисковых станций через сеть, хост может использовать и для загрузки конфигурационного файла, содержащего всю требуемую информацию (см., например, RFC 951 [8]). Возможно (и желательно) получить все сведения, требуемые для работы хоста, в результате передачи одного широковещательного сообщения.

В тех случаях, когда хосту требуется определить адресную маску, используя для это отдельную операцию, применяется следующий механизм:

Для обеспечения сведений об адресных масках в протокол ICMP [5] добавлена пара новых типов сообщений ICMP - Address Mask Request (запрос маски) и Address Mask Reply (отклик на запрос маски), аналогичных сообщениям Information Request (запрос информации) и Information Reply (отклик на запрос информации. Эти типы сообщений описаны ниже (Приложение I. Сообщения ICMP Address Mask).

Новые сообщения ICMP используются следующим образом – хост при загрузке передает широковещательное сообщение Address Mask Request, а шлюз (или хост, действующий вместо шлюза), получив такое сообщение, будет передавать отклик Address Mask Reply. Если в запросе отправитель не был указан (поле IP Source Address имеет значение 0), отклик также передается в широковещательном сообщении. Запросивший информацию хост получит это сообщение и сможет определить адресную маску.

Поскольку для каждой конкретной ЛВС в сообщении Address Mask Reply может содержаться только одно значение, нет необходимости проверять соответствие отклика запросу. Даже при получении отклика от нескольких шлюзов, информация во всех сообщениях будет совпадать. Предполагается, что хосты перезагружаются достаточно редко, поэтому количество широковещательных сообщений для определения маски будет достаточно мало.

Если хост подключен к нескольким ЛВС, он может определить маски для каждой подсети.

Возможны ситуации, когда хосту не удается определить маску даже после нескольких попыток. Это может происходить в трех ситуациях:

1. Локальная сеть постоянно изолирована от всех других сетей.
2. Подсети не используются и ни один из хостов не может сообщить адресную маску.
3. Все шлюзы локальной сети (временно) находятся в нерабочем состоянии (down).

В первых двух случаях адресная маска идентична маске сети, а в третьем случае не существует способа определить значение маски и самым безопасным вариантом будет использование адресной маски, совпадающей с маской сети. Хотя позднее может обнаружиться некорректность такой маски, ее использование не порождает проблем при передаче. После того, как восстановится нормальная работа шлюза, он будет передать широковещательное сообщение Address Mask Reply; когда хост получит это сообщение, он сможет изменить адресную маску в соответствии с полученным от шлюза значением. Хостам и шлюзам не следует передавать сообщений Address Mask Reply с «предполагаемой» маской.

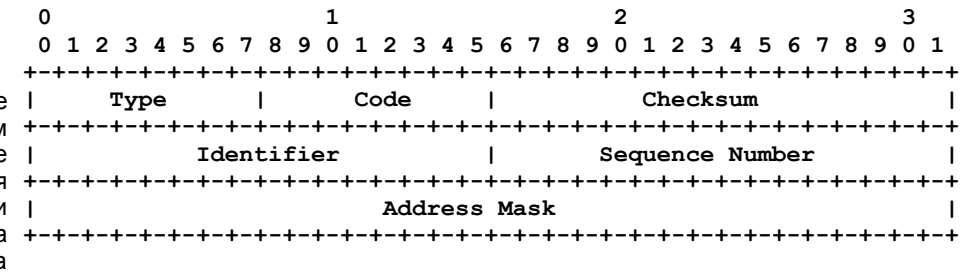
В заключение отметим, что хост не обязан использовать протокол ICMP для определения маски – параметры хоста могут сохраняться в энергонезависимой памяти.

[1] Reverse Address Resolution Protocol - протокол обратного преобразования адресов.

Приложение I. Сообщения ICMP Address Mask

Address Mask Request и Address Mask Reply

Поля IP



Адреса

Адрес отправителя в запросе адресной маски служит адресом получателя при передаче откликов. Для формирования отклика на запрос адресной маски адрес отправителя запроса помещается в поле адреса получателя, а адрес отправителя отклика помещается в поле отправителя, тип заменяется на AM2, адресная маска помещается в поле Address Mask и вычисляется контрольная сумма. Если же в запросе адрес отправителя имеет нулевое значение, в поле получателя отклика должен указываться широковещательный адрес.

Поля ICMP

Type (тип)

AM1 для запросов маски;
AM2 для откликов.

Code (код)

0 – для запросов;
0 – для откликов.

Checksum (контрольная сумма)

Контрольная сумма представляет собой 16-битовое поразрядное дополнение до единицы суммы дополнений до единицы полей сообщения ICMP, начиная с ICMP Type. При расчете контрольной суммы значение поля Checksum принимается равным 0. Алгоритм вычисления контрольной суммы в будущем может быть изменен.

Identifier (идентификатор)

Идентификаторы служат для сопоставления запросов и откликов. Это поле может иметь нулевое значение.

Sequence Number (порядковый номер)

Порядковый номер служит для сопоставления запросов и откликов. Поле может иметь нулевое значение.

Address Mask (адресная маска)

32-битовое значение маски.

Описание

Шлюзу, получившему запрос адресной маски, следует возвратить отклик, содержащий искомую маску, которая идентифицирует подсеть и сеть для подсети, из которой поступил запрос.

Если запрашивающий хост не знает своего адреса IP, он может указать 0 в поле адреса отправителя – отклик в таких случаях передается в широковещательном режиме. По возможности следует избегать широковещательной передачи откликов, поскольку она достаточно сильно загружает сеть. Даже при широковещательной передаче откликов не требуется проверять соответствие между запросом и откликом, поскольку для каждой подсети может использоваться только одна адресная маска. Следовательно, поля Identifier и Sequence Number можно игнорировать.

Пакеты типа AM1 могут приниматься от шлюзов и хостов, а пакеты типа AM2 – от шлюзов или хостов, действующих как шлюзы.

Приложение II. Примеры

Приведенные здесь примеры показывают, как хост может определить адресную маску, используя сообщения ICMP Address Mask Request и Address Mask Reply. В примерах предполагается, что 255.255.255.255 означает широковещательный адрес для физической среды [6].

1. Сеть класса A

Предположим, что запрашивающий маску хост сети класса A 36.0.0.0 имеет адрес 36.40.0.123, адрес шлюза 36.40.0.62, а поле номера подсети имеет размер 8 битов, т.е., маска имеет значение 255.255.0.0.

Для хоста наиболее эффективно (рекомендуется поступать именно так) будет определить сначала свой адрес (например, с помощью RARP [4]) и только после этого передавать запрос ICMP по адресу 255.255.255.255:

Адрес отправителя:	36.40.0.123
Адрес получателя:	255.255.255.255
Протокол:	ICMP = 1
Тип:	Address Mask Request = AM1
Код:	0
Маска:	0

Шлюз может адресовать свой отклик непосредственно запрашивающему хосту.

Адрес отправителя:	36.40.0.62
Адрес получателя:	36.40.0.123
Протокол:	ICMP = 1
Тип:	Address Mask Reply = AM2

Код: 0
Маска: 255.255.0.0

Предположим, что хост 36.40.0.123 является бездисковой станцией и не знает своего номера. В таком случае хост может передать следующую дейтаграмму:

Адрес отправителя: 0.0.0.0
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Request = AM1
Код: 0
Маска: 0

Шлюз 36.40.0.62 получит эту дейтаграмму и передаст отклик:

Адрес отправителя: 36.40.0.62
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.0.0

Отметим, что шлюз использует минимальную из возможных областей широковещания для передачи отклика. Но даже в таком случае использование широковещания приводит к росту нагрузки на все хосты подсети, поэтому использования «анонимного» адреса отправителя (0.0.0.0) следует избегать.

Если широковещание не поддерживается, мы предполагаем, что хост имеет «аппаратную» возможность определения соседнего шлюза. В таких случаях хост 36.40.0.123 может передать дейтаграмму:

Адрес отправителя: 36.40.0.123
Адрес получателя: 36.40.0.62
Протокол: ICMP = 1
Тип: Address Mask Request = AM1
Код: 0
Маска: 0

Шлюз 36.40.0.62 будет отвечать точно так ж, как для предыдущего случая.

Адрес отправителя: 36.40.0.62
Адрес получателя: 36.40.0.123
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.0.0

2. Сеть класса B

Предположим, что запрашивающий маску хост сети класса B 128.99.0.0 имеет адрес 128.99.4.123, адрес шлюза 128.99.4.62, а для нумерации подсетей используется 6-битовое поле (маска 255.255.252.0).

Хост передает запрос ICMP по адресу 255.255.255.255:

Адрес отправителя: 128.99.4.123
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Request = AM1
Код: 0
Маска: 0

Шлюз может адресовать отклик непосредственно хосту.

Адрес отправителя: 128.99.4.62
Адрес получателя: 128.99.4.123
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.252.0

Бездисковый хост будет передавать запрос:

Адрес отправителя: 0.0.0.0
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Request = AM1
Код: 0
Маска: 0

Шлюз 128.99.4.62 получит эту дейтаграмму и должен передать отклик:

Адрес отправителя: 128.99.4.62
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.252.0

Если в сети не поддерживается широковещание, хост 128.99.4.123 будет передавать дейтаграмму:

Адрес отправителя: 128.99.4.123
Адрес получателя: 128.99.4.62
Протокол: ICMP = 1
Тип: Address Mask Request = AM1

Код: 0
Маска: 0

На которую шлюз 128.99.4.62 должен передать отклик, аналогичный предыдущему случаю.

Адрес отправителя: 128.99.4.62
Адрес получателя: 128.99.4.123
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.252.0

3. Сеть класса C (с разрывным массивом битов нумерации подсети)

Предположим, что запрашивающий хост сети класса C 192.1.127.0 имеет адрес 192.1.127.19, адрес шлюза 192.1.127.50, а для нумерации подсетей используется трехбитовое поле (01011000), т. е., маска равна 255.255.255.88.

Хост передает запрос ICMP по адресу 255.255.255.255:

Адрес отправителя: 192.1.127.19
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Request = AM1
Код: 0
Маска: 0

Шлюз может адресовать отклик непосредственно хосту.

Адрес отправителя: 192.1.127.50
Адрес получателя: 192.1.127.19
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.255.88

Бездисковый хост будет передавать запрос:

Адрес отправителя: 0.0.0.0
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Request = AM1
Код: 0
Маска: 0

Шлюз 192.1.127.50 будет принимать запрос и должен ответить на него дейтаграммой:

Адрес отправителя: 192.1.127.50
Адрес получателя: 255.255.255.255
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.255.88

Если широковещание не поддерживается, хост 192.1.127.19 будет передавать дейтаграмму:

Адрес отправителя: 192.1.127.19
Адрес получателя: 192.1.127.50
Протокол: ICMP = 1
Тип: Address Mask Request = AM1
Код: 0
Маска: 0

на которую шлюз 192.1.127.50 должен отвечать, как в предыдущем случае, дейтаграммой:

Адрес отправителя: 192.1.127.50
Адрес получателя: 192.1.127.19
Протокол: ICMP = 1
Тип: Address Mask Reply = AM2
Код: 0
Маска: 255.255.255.88

Приложение III. Глоссарий

Bridge - мост

Узел, соединяющий две или более сети, не различаемые административно, но относящиеся к разным физическим подсетям, и автоматически пересылающий дейтаграммы между подсетями, когда это требуется. Другие хосты о существовании моста просто не знают. Иногда для обозначения мостов используют термин software repeater[1] (программный повторитель).

Gateway – шлюз (маршрутизатор)

Узел, соединяющий две или более административно различающихся сети и/или подсети и пересылающий дейтаграммы между ними.

Host Field – поле хоста

Битовое поле в адресе IP, используемое для идентификации конкретного хоста.

Internet

Множество связанных между собой сетей IP.

Local Address – локальный адрес

Биты адреса IP, не используемые для задания номера сети (в соответствии с определением в работе [3]).

[1]В настоящее время этот термин устарел и практически не используется. *Прим. перев.*

Network - сеть
Одна сеть IP, которая может представлять единое целое или состоять из множества подсетей.

Network Number - номер сети
Поле идентификации сети в адресе IP.

Subnet - подсеть
Одна или несколько физических сетей, формирующие подмножество сети IP. Подсеть явно задается в адресе IP.

Subnet Field – поле подсети
Битовое поле в адресе IP, содержащее номер подсети. Биты этого поля не обязаны быть непрерывными в адресе.

Subnet Number – номер подсети
Номер, идентифицирующий подсеть внутри сети.

Приложение IV. Выделенные номера

В качестве параметров протоколов, используемых для поддержки подсетей, были выделены специальные значения. Эти значения используются только протоколом ICMP [5].

ICMP Message Type (типы сообщений)

AM1 = 17
AM2 = 18

Литература

[1] Mogul, J., "Internet Subnets", RFC 917, Stanford University, October 1984.

[2] Postel, J., "Multi-LAN Address Resolution", RFC 925, USC/Information Sciences Institute, October 1984.

[3] Postel, J., "Internet Protocol", RFC 791, USC/Information Sciences Institute, September 1981.

[4] Finlayson, R., T. Mann, J. Mogul, M. Theimer, "A Reverse Address Resolution Protocol", RFC 903, Stanford University, June 1984.

[5] Postel, J., "Internet Control Message Protocol", RFC 792, USC/Information Sciences Institute, September 1981.

[6] Mogul, J., "Broadcasting Internet Datagrams", RFC 919, Stanford University, October 1984.

[7] GADS, "Towards an Internet Standard Scheme for Subnetting", RFC 940, Network Information Center, SRI International, April 1985.

[8] Croft, B., and J. Gilmore, "BOOTP -- UDP Bootstrap Protocol", RFC 951[1], Stanford University, August 1985.

[9] Reynolds, J., and J. Postel, "Assigned Numbers", RFC 943[2], USC/Information Sciences Institute, April 1985.

Перевод на русский язык
Николай Малых
nmalykh@gmail.com

[1]Этот документ частично пересмотрен в более поздних RFC 1395, RFC 1497, RFC 1532, RFC 1542. *Прим. перев.*
[2]Этот документ время от времени обновлялся. Последний вариант можно найти в RFC 1700. В настоящее время серия документов Assigned Numbers утратила силу и все данные из них перенесены в базу, доступную по адресу www.iana.org/numbers.html. *Прим. перев.*