Network Working Group J. Klensin
Request for Comments: 4084 May 2005
BCP: 104
Category: Best Current Practice

Терминология для описания услуг по подключению к Internet

Terminology for Describing Internet Connectivity

Статус документа

В этом документе рассматривается позитивный опыт (Best Current Practices), который может быть полезен сообществу Internet. Документ служит приглашением к дискуссии в целях дальнейшего совершенствования и может распространяться свободно.

Аннотация

Когда сеть Internet развилась достаточно сильно, началась активная реклама и продажа «подключения к Internet[1]». В силу того, что предложения могут существенно различаться по своим возможностям, набору опций, а также по причине отсутствия стандартизованной терминологии, конечные пользователи зачастую не могут разобраться с предлагаемыми услугами. В этом документе приводится список терминов и определений, описывающих различные типы сервиса, которые могут предлагаться. Эти определения могут оказаться полезными для провайдеров, потребителей и (возможно) контролирующих органов.

Оглавление

1. Введение

1.1. Проблема и требования

Различные поставщики услуг доступа в Internet (ISP) и другие провайдеры предлагают широкий спектр продукции и услуг, обозначаемых как "Internet" или "доступ в Internet". Эта продукция характеризуется различным набором функций и, в результате, может оказаться подходящей для одних пользователей и совершенно неприемлемой для других. Например, сервис, который обеспечивает только доступ в Web (в контексте этого документа – часть Internet, доступная по протоколам HTTP и HTTPS), может устроить тех, кто интересуется исключительно Web-серверами и почтовыми системами на базе Web. Однако такой сервис не подойдет тем, кто хочет загружать из сети файлы или использовать электронную почту более интенсивно. Очевидно, что еще меньше такой сервис подойдет тем, кто предоставляет свои серверы для других пользователей или нуждается в каналах VPN (виртуальные частные сети) или иных системах организации защищенного доступа в удаленный офис, а так же тем, кому нужна синхронизация электронной почты для работы с ней без постоянного доступа в сеть (offline0.

Недавние и быстротекущие изменения в среде электронной почты Internet привели к дополнительным ограничениям на передачу и получение (retrieving) почты. Эти ограничения, большинство из которых разработаны как часть системы предотвращения незапрошенной почты[2], могут вводиться независимо от типа сервиса, описанного ниже, и рассматриваются отдельно в главе 3.

В данном документе описываются лишь функции, предлагаемые или разрешаемые сервис-провайдерами. В документе не описываются функции, которые могут поддерживаться различным пользовательским оборудованием.

Термины SHOULD (**следует**), MUST (**должно**), и MAY (**можно**) выделяются в этом документе, как описано в [1].

1.2. Адаптация терминов

Приведенные здесь определения будут иметь мало смысла, если сервис-провайдеры не примут их. Предложенные здесь термины не следует рассматривать как “уничижительные”, несмотря на то, что ряд членов сообщества IETF считает некоторые из описанных здесь типов сервиса “забытыми” (broken) или не относящимися к "Internet-сервису” (not really an Internet service). Упоминание того или иного типа сервиса или модели в данном документе не является подтверждением или признанием существования или возможности существования его на реальном рынке. Таким образом, опыт (Best Current Practice), описываемый в этом документе, относится к терминологии, а приведенная информация предназначена для пользователей и не задает типов сервиса, которые следует предлагать.

[1] В оригинале используется термин “Internet connectivity”. *Прим. перев.*
[2] Спама. *Прим. перев.*

2. Общая терминология

В этом параграфе перечислены основные типы сервиса IP. Есть надежда, что сервис-провайдеры примут эти определения для того, чтобы лучше определить услуги, предлагаемые потенциальным пользователям и заказчикам. Термины, относящиеся к провайдерам (ISP), выражены в технических параметрах или условиях обслуживания. Возможна работа над конкретной реализацией этих характерных типов подключения, но такая свобода обычно не имеет смысла для провайдеров и не факт, что она будет поддерживаться в случае прекращения работ в этом направлении.

Определения типов обслуживания приводятся в порядке возрастания возможностей вплоть до полнофункционального подключения к Internet[1].

- **Web connectivity (Web-подключение).**

  Этот тип сервиса обеспечивает подключение к Web, т. е., к службам, поддерживаемым с помощью Web-браузеров (таких, как Firefox, Internet Explorer, Mozilla, Netscape, Lynx или Opera), в частности, к службам, работающим по протоколам HTTP и HTTPS. Другие типы сервиса в общем случае не поддерживаются. В частности, такой тип сервиса может не предоставлять доступа к электронной почте по протоколам POP3 или IMAP4, не поддерживать шифрованные туннели и другие механизмы VPN.

  Используемые для такого сервиса адреса могут быть приватными и/или недоступными в глобальном масштабе. Адреса обычно выделяются динамически (см. обсуждение в параграфе 3) и срок их использования достаточно мал (часы или дни). Такие адреса часто анонсируются как динамические (dynamic) для тех, кто поддерживает списки динамических адресов, используемых для коммутируемого доступа. Провайдер может использовать фильтрацию с помощью Web-прокси для соединений; прокси-сервер может изменять или перенаправлять URL на другие сайты взамен тех, которые указаны пользователем или приведены в ссылке.

- **Client connectivity only, without a public address (подключение в качестве клиента без предоставления публичного адреса).**

  Этот тип сервиса обеспечивает доступ в Internet без поддержки возможности организации серверов и реализации большинства функций peer-to-peer. Выделяемый пользователю адрес IP является динамическим и обычно относится к приватным блокам. Серверы и функции peer-to-peer обычно не поддерживаются системами трансляции адресов (NAT), которые требуются при использовании приватных адресов. Более точное описание категорий NAT в документе [2] в некоторых случаях отличается от трактовки в данном документа. Такие функции могут рассматриваться как отдельные типы сервиса, описанные в главе 4.

  Для этого типа сервиса обычно используются фильтрующие Web-прокси, и провайдерам **следует** указывать наличие или отсутствие такого сервера.

- **Client only, public address (подключение в качестве клиента с предоставлением публичного адреса).**

  Этот тип сервиса обеспечивает доступ в Internet без поддержки возможности организации серверов и реализации большинства функций peer-to-peer. Пользователю предоставляется публичный[2] адрес IP. Адрес обычно выделяется динамически или может быть изменен в любое время, но работа с одним адресом может продолжаться в течение месяцев. С этим типом обслуживания работает большинство систем VPN[3] и подобных им соединений. Провайдер может запретить пользователю организацию серверов на уровне контракта или путем фильтрации попыток входящих (к пользователю) соединений.

  Фильтрующие Web-прокси нехарактерны для этого типа сервиса и провайдерам **следует** сообщать о наличии таких серверов.

- **Firewalled Internet Connectivity (подключение с использованием межсетевого экрана).**

  Этот тип сервиса обеспечивает доступ в Internet и поддерживает возможность организации серверов и использования большинства функций peer-to-peer functions с предоставлением клиенту одного публичного адреса IP или блока таких адресов (обычная практика). Этот тип сервиса похож на полнофункциональное подключение, описанное ниже, и к нему применимы все описанные для этого сервиса классификации и ограничения. Однако для данного типа сервиса используется подключение через поддерживаемый провайдером межсетевой экран[4], который находится между пользователем и публичной частью Internet. Поддержка межсетевого экрана обычно включается по запросу заказчика и повышает стоимость обслуживания. Условия фильтрации пользовательского трафика на межсетевом экране оговариваются в контракте и могут обеспечивать блокирование некоторых услуг.

  Отдельные типы сервиса могут перехватываться прокси-серверами, системами фильтрации содержимого и шлюзами приложений. Провайдерам **следует** указывать какие типы сервиса они блокируют, перехватывают или меняют тем или иным способом.

  В большинстве случаев услуги межсетевого экранирования предлагаются в качестве платного дополнения к сервису Full Internet Connectivity, который отличается от описанной выше модели тем, что любая фильтрация или блокирование трафика выполняются по запросу заказчика, а не как ограничение возможностей пользователей.

- **Full Internet Connectivity (полнофункциональное подключение).**

  Этот тип сервиса обеспечивает пользователям полнофункциональное подключение к Internet с предоставлением одного публичного адреса или блока таких адресов. Клиентам могут предоставляться динамические адреса с большим сроком жизни, которые не будут требовать частой замены записей DNS для серверов и будут представляться удаленным хостам как статические.

  Фильтрующие Web-прокси, перехватывающие прокси-серверы, NAT и иные вносимые провайдером ограничения для входящего или исходящего трафика или портов несовместимы с этим типом сервиса. Серверы в локальной

[1] В оригинале - "full Internet connectivity". *Прим. перев.*
[2] Маршрутизируемый через Internet. *Прим. перев.*
[3] Virtual Private network – виртуальная частная сеть. *Прим. перев.*
[4] Firewall. В русском языке часто используется термин брандмауэр или транслитерация “фаервол”. *Прим. перев.*

сети пользователя обычно рассматриваются как нормальное явление. Допустимыми для такого сервиса ограничениями являются полоса канала и запрет на недопустимое использование ресурсов и противоправные действия.

3. Терминология, относящаяся к фильтрации и безопасности

Как было отмечено во введении, усилия по контролю или ограничению нежелательного трафика могут приводить к дополнительным ограничениям сервиса Internet. К нежелательному трафику может относиться незапрошенная электронная почта различных видов (включая спам), программные черви, вирусы и (в некоторых случаях) определенные типы информации (контента).

В общем случае максимальные ограничения очевидно будут связаны с такими типами сервиса, как Web-подключение и подключение без предоставления публичного адреса, но некоторые рекомендации предлагают применять ограничения ко всем уровням сервиса. Некоторые ограничения для электронной почты не позволяют клиента передавать почту напрямую (однако можно передавать почту через сервер провайдера), запрещают пользователю устанавливать произвольный обратный адрес в письмах и могут даже закрывать доступ к серверам электронной почты (за исключением предоставленных провайдером) по протоколам типа POP3 или IMAP4. Поскольку пользователям может требоваться доступ к файловым серверам и удаленным почтовым серверам (хотя бы для того, чтобы можно было пользоваться своим электронным адресом из разных мест), важно, чтобы провайдеры указывали доступные при подключении службы и вводимые ограничения.

Некоторые вопросы фильтрации электронной почты имеют особую важность и рассмотрены ниже.

- **Динамические адреса.**

  Множество систем, включая некоторые “черные списки” (blacklist), работают на основе допущения, что значительная часть незапрошенной почты поступает от хостов с динамическими адресами, особенно от компьютеров с коммутируемым доступом по телефонным линиям или домашних систем, подключенных по широкополосным каналам. Следовательно, предпринимаются попытки предотвратить передачу почты с таких адресов (за исключением передачи сообщений через серверы провайдера).

  Для идентификации систем с динамическими адресами используются различные методы, включая анонсирование провайдерами динамически распределяемых блоков держателям “черных списков”, эвристические методы, преобразование адресов в доменные имена и проверка наличия в полученном имени подстрок типа "dsl" или "dial". В некоторых случаях отсутствие реверсной записи DNS трактуется как принадлежность адреса к числу динамических. Отметим, что метод запрета соединений FTP с адресов, для которых отсутствует возможность обратного преобразования DNS, был разработан несколько лет назад и показал свою несостоятельность (множество ложных срабатываний и частый пропуск действительно динамических адресов). Провайдерам **следует** описывать свои требования (действия) в данном направлении как для входящего, так и для исходящего трафика. Пользователей следует предупреждать о том, что анонсирование провайдером динамических адресов может делать невозможной прямую передачу электронной почты даже для сервиса типа Full Internet Connectivity.

- **Приватные адреса и трансляция NAT.**

  Системы NAT, используемые для преобразования приватных адресов в публичные (и обратно) позволяют подключаться к удаленным почтовым службам и передавать почтовый трафик в обоих направлениях, но соглашения с провайдерами зачастую запрещают использование серверов, не относящихся к сети провайдера, а также использование клиентских станций в качестве почтовых серверов (обычно это требование не определено достаточно четко).

- **Фильтрация провайдером исходящего трафика по портам.**

  Другим распространенным способом блокирования соединений с серверами за пределами сети провайдера является фильтрация соединений с портами TCP. Разные провайдеры имеют различные “теории” на сей счет. Некоторые запрещают своим клиентам использовать внешние серверы SMTP для отправки сообщений, но позволяют использовать такие функции при наличии аутентификации отправителя [3]. Другие провайдеры пытаются блокировать все связанны с отправкой почты соединения (такой подход реже используется для клиентов с публичными адресами, нежели для клиентов с приватными адресами и NAT). При использовании такой фильтрации, особенно для сервиса типа "Client only, public address" или "Full Internet Connectivity", провайдер **должен** сообщать об этом клиентам (см. также главу 4).

  Некоторые провайдеры могут перенаправлять исходящий почтовый трафик на свои серверы и теоретически это избавляет от необходимости изменять конфигурацию мобильных хостов, которые могут подключаться к разным провайдерам. О таком перенаправлении почтового трафика провайдеры **должны** оповещать своих пользователей (особенно в тех случаях, когда это оказывает существенное влияние на безопасность и конфиденциальность).

  Фильтры, которые блокируют передачу (или получение) почты полностью или частично, а также пытаются перенаправлять почтовый трафик на серверы провайдера, становятся все более распространенными и о них **следует** оповещать пользователей.

4. Дополнительные термины

Эти дополнительные термины хоть и не играют столь важную роль в описании типов сервиса, как рассмотренные выше термины, приведены здесь для того, чтобы сервис-провайдеры могли выбрать и описать дополнительные услуги, предлагаемые заказчикам. Потенциальные заказчики могут использовать эти термины для оценки услуг того или иного провайдера.

- **Поддержка версий протокола.**

  Версии протокола IP, поддерживаемые провайдером – только IPv4, IPv4 и IPv6 или только IPv6.

- **Поддержка аутентификации.**

Технические механизмы, используемые провайдером для организации и аутентификации соединений. Примерами могут служить DHCP, PPP, RADIUS, перехват (interception) HTTP.

- **VPN и туннели.**

  Поддерживается ли использование IPSec? Поддерживаются ли другие механизмы организации туннелей на уровне IP или ниже (например, L2TP)? Предпринимаются ли попытки блокирования туннельных механизмов прикладного уровня (например, SSH)?

- **Поддержка групповой адресации.**

  Может ли пользовательская станция принимать пакеты с групповой адресацией?

- **Поддержка DNS.**

  Требуется ли от клиента использование DNS-серверов провайдера или запросы DNS могут отправляться на произвольные серверы?

- **ICMP и traceroute.**

  Пропускаются ли сообщения ICMP в направлении пользователя и от него? Блокируется ли использование таких инструментов, как ping и traceroute (если да, то в какой точке сети)?

- **Роуминг.**

  Поддерживает ли провайдер IP-роуминг? Поддерживается ли для широкополосных соединений возможность организации коммутируемого соединения в качестве резервного или при отъезде в другое место? Как в случае работы с роумингом осуществляется доступ к электронной почте и т. п.?

- **Электронная почта и хостинг.**

  Предоставляется ли электронная почта и/или Web-хостинг в составе сервиса? Для почтовых служб следует определить тип доступа к почтовым ящикам (POP3, IMAP4 или Web, а также средства аутентификации для каждого из вариантов доступа.

- **Блокировка исходящих соединений с серверами.**

  Блокирует ли провайдер использование чужих серверов SMTP или перехватывает их и перенаправляет их на свой сервер? Ограничивается ли на почтовых серверах использование “чужих” доменов в исходящих почтовых сообщениях (см. также главу 3)? Поддерживается ли команда FTP PASV? Блокируются (перехватываются) ли обращения в файлообменные сети или использование других механизмов передачи файлов, а также серверы конференций и приватных приложений?

  Провайдерам следует указывать все свои ограничения на использование чужих серверов приложений (т. е., серверов, не поддерживаемых за пределами сети данного провайдера).

- **Блокирование входящих соединений с серверами.**

  Использует ли провайдер какие-либо ограничения для соединений, которые может организовывать пользовательское оборудование, в дополнение к ограничениям, связанным с динамическими и приватными адресами? В частности, следует выяснить блокируются ли входящие соединения SMTP, HTTP, HTTPS, FTP, peer-to-peer и др.?

- **Фильтрация содержимого.**

  Провайдерам следует сообщать своим пользователям о средствах фильтрации, используемых для предотвращения червей, вирусов и спама, атак на службы или ограничения доступа к Web (в частности, для детей).

- **“Прослушивание” и перехват.**

  В описание сервиса **следует** включать сведения о возможности законного перехвата проходящего через сеть провайдера трафика. Провайдеру следует также оповещать пользователей будут ли они получать от провайдера предупреждение об активизации такого перехвата. Аналогичные вопросы следует задать и по поводу хранящейся у провайдера данных о трафике пользователей.

5. Вопросы безопасности

Данный документ посвящён терминологии, а не протоколам, следовательно, он не оказывает какого-либо влияния на вопросы безопасности. Однако при широком распространении предложенной здесь терминологии она может упростить идентификацию связанных с безопасностью ожиданий для отдельных хостов, ЛВС и типов подключения.

6. Благодарности

Толчком к созданию этого документа послужила переписка по электронной почте с Верноном Шрайнером (Vernon Schryver), Паулем Викси (Paul Vixie0 и Натаниэлем Борнстейном (Nathaniel Bornstein). Разговоры о необходимости разработки таких определений велись уже много лет, упомянутая переписка убедила автора в том, что настало время перейти от слов к делу. Harald Alvestrand, Brian Carpenter, George Michaelson, Vernon Schryver и другие внесли в черновой вариант документа предложения, которые позволили подготовить новый черновой вариант. Stephane Bortzmeyer, Brian Carpenter, Tony Finch, Susan Harris, David Kessens, Pekka Savola и Vernon Schryver внесли много полезных предложений в последующие версии документа. Сьюзан Харрис (Susan Harris) внимательно прочла предпоследнюю версию документа и внесла поправки как редактор (RFC Editor).

7. Литература

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[3] Gellens, R. and J. Klensin, "Message Submission", RFC 2476, December 1998.

Адрес автора

John C Klensin

1770 Massachusetts Ave, #322

Cambridge, MA 02140

USA

Phone: +1 617 491 5735

EMail: john-ietf@jck.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.