Network Working Group
Request for Comments: 2685
Category: Standards Track

B. Fox
Lucent Technologies
B. Gleeson
Nortel Networks

September 1999

Идентификатор виртуальной частной сети (VPN)

Virtual Private Networks Identifier

Статус документа

Данный документ содержит спецификацию протокола, предложенного сообществу Internet, и служит запросом к дискуссии в целях развития протокола. Информацию о статусе данного протокола можно найти в текущей редакции документа "Internet Official Protocol Standards" (STD 1). Документ может распространяться свободно.

Авторские права

Тезисы

Виртуальные частные сети IP могут покрывать множество автономных систем (AS) или сетей сервис-провайдеров (SP). Это порождает требование использования уникальных в глобальном масштабе идентификаторов VPN, которые позволят определить конкретные VPN (см. параграф 6.1.1 в документе [1]). В данном документе предложен формат уникального в глобальном масштабе идентификатора VPN.

1. Введение

По мере расширения публичной сети Internet и глобального расширения сетевой инфраструктуры существенно возрос интерес в виртуальным частным сетям (VPN[1]) на основе IP. VPN эмулирует частную сеть IP через публичные или разделяемые инфраструктуры. Сети VPN обеспечивают ряд преимуществ как для сервис-провайдеров, так и для их заказчиков. Для заказчиков VPN позволяет включить в единую сеть IP удаленные офисы и отдельных пользователей подключаемых к сети разными способами. Подключение к сети в каждом случае может осуществляться наиболее экономичным способом и это позволяет снизить расходы заказчика на оборудование, услуги и поддержку. Сервис-провайдеры могут повысить эффективность использования своей инфраструктуры, предлагая своим заказчикам подключение и/или услуги IP VPN.

Существует множество способов реализации услуг IP VPN. В базовом документе по таким сетям [1] выделены четыре типа поддерживаемых VPN: виртуальные выделенные линии (VLL[2]), виртуальные частные маршрутизируемые сети (VPRN[3]), виртуальные частные сети с коммутируемым доступом (VPDN[4]) и сегменты виртуальных частных ЛВС (VPLS[5]). В дополнение к упомянутому документу во множестве проектов спецификация описаны методы, которые могут использоваться сервис-провайдерами и/или их заказчиками для организации сервиса VPN. Решения могут выбираться для отдельных заказчиков или сети в целом. Сетевые решения могут обеспечивать подключение и услуги уровня 2 и/или 3. Устройствами, вовлеченными в реализацию решения могут быть оборудование заказчика (CPE[6]), оконечное оборудование сервис-провайдера (SPE[7]), и оборудование ядра сети сервис-провайдера, а также комбинации этих устройств.

Хотя различные методы реализации сервиса VPN еще будут обсуждаться, существуют два пункта, по которым имеется согласие:

- поскольку VPN является частной сетью, в ней могут использоваться блоки адресов, которые могут перекрываться с блоками других VPN или публичной сети Internet;
- VPN может простираться через множество автономных систем (AS) IP или сервис-провайдеров.

Первый пункт означает, что адреса IP имеют значение только в масштабе VPN, где эти адреса используются. По этой причине требуется идентифицировать VPN, в которой тот или иной адрес IP является значимым, или «область видимости» адреса IP.

Второй пункт означает, что в одной VPN может использоваться несколько типов доступа и способов предоставления услуг. Различные сервис-провайдеры могут реализовать разные стратегии с зависимости от своей инфраструктуры и имеющегося опыта. Желательно обеспечить возможность идентификации любой конкретной сети VPN на всех уровнях и в любом месте, где эта сеть может существовать, по одному идентификатору VPN.

---

[1] Virtual Private Network
[2] Virtual Leased Line
[3] Virtual Private Routed Network
[4] Virtual Private Dial Network
[5] Virtual Private LAN Segment
[6] Customer Premises Equipment
[7] Service Provider Edge

2. Глобальный идентификатор VPN

Задачей VPN-ID является идентификация VPN. Этот идентификатор может использоваться разными способами в зависимости от метода реализации сервиса VPN. Например, VPN-ID может быть включен:

- в базу MIB для конфигурирования атрибутов VPN или выделения физического или логического интерфейса доступа для конкретной VPN;
- в пакет данных управления для идентификации «зоны действия» приватного адреса IP и VPN, к которой относятся данные.

Необходимо обеспечить возможность идентификации VPN, с которой связан пакет данных. Идентификатор VPN-ID может использоваться для решения этой задачи явно (например, путем включения VPN-ID в заголовок инкапсуляции [2]) или неявно (например, путем включения VPN-ID в сигнальный обмен ATM [3]). Приемлемость использования VPN-ID в других вариантах контекста требует внимательного изучения.

Существует другая очень важная функция, для выполнения которой может использоваться идентификатор VPN, - определение «агентство VPN» (VPN authority), - которая отвечает за координацию подключения и услуг, предоставляемых данной VPN. Агентством VPN может быть администратор частной сети или основной сервис-провайдер. Этот орган будет служить главной точкой контактов для данной VPN. Агентство может передавать на аутсорсинг некоторые функции и подключения путем заключения контрактных соглашений с другим сервис-провайдером и координировать конфигурацию, производительность и восстановление при отказах.

Эти функции требуют глобальной зоны действия идентификатора VPN и возможности его использования в разных решениях. Для того, чтобы идентификатор VPN был уникальным в глобальном масштабе, формат идентификатора не должен основываться на каких-либо допущениях о разделяемой сети (сетях). И наоборот, формат не следует определять таким образом, чтобы возникали ограничения на использование возможностей разделяемой сети (сетей). Необходимо отметить, что одна и та же VPN может идентифицироваться на разных уровнях одной разделяемой сети (например, на уровнях ATM и IP). Для обоих уровнях следует в таких случаях использовать общее значение и формат VPN-ID.

Методы использования VPN-ID выходят за пределы данного документа.

3. Требования к формату глобального идентификатора VPN

К формату идентификатора VPN следует предъявлять перечисленные здесь требования:

- значение идентификатора VPN должно быть уникальным и используемым в сетях разных сервис-провайдеров;
- должны поддерживаться не связанные с IP идентификаторы VPN-ID для использования в VPN канального уровня.
- VPN-ID должен идентифицировать VPN Authority.

4. Формат глобального идентификатора VPN

Глобальный идентификатор VPN включает

3-октетный идентификатор агентства VPN (VPN OUI[1]) [4]

за которым следует

4-октетный индекс VPN (VPN Index), идентифицирующий VPN в рамках OUI

```
 0 1 2 3 4 5 6 7 8
+-+-+-+-+-+-+-+-+
| VPN OUI (MSB) |
+-+-+-+-+-+-+-+-+
|    VPN OUI    |
+-+-+-+-+-+-+-+-+
| VPN OUI (LSB) |
+-+-+-+-+-+-+-+-+
|VPN Index (MSB)|
+-+-+-+-+-+-+-+-+
|   VPN Index   |
+-+-+-+-+-+-+-+-+
|   VPN Index   |
+-+-+-+-+-+-+-+-+
|VPN Index (LSB)|
+-+-+-+-+-+-+-+-+
```

VPN OUI (IEEE 802-1990 Organizationally Unique Identifier) [4] идентифицирует Агентство VPN. Этот орган будет являться основным администратором VPN. Агентством может быть компания/организация, к которой относится VPN, или сервис-провайдер, обеспечивающий инфраструктуру VPN с использованием своей (или других сервис-провайдеров) разделяемой сети. 4-октетный индекс VPN идентифицирует отдельную VPN, обслуживаемую агентством VPN.

5. Вопросы безопасности

В этом документе определен формат глобального идентификатора VPN без спецификации его использования. Однако связывание частных характеристик и возможностей с идентификатором VPN требует использования стандартных процедур защиты при любом применении идентификаторов. Некорректная настройка или непреднамеренная утрата идентификатора VPN могут приводить к различным нарушениям защиты, включая возникновение связи между разными VPN.

6. Литература

[1] Gleeson, Heinanen, Lin, Armitage, Malis, "A Framework for IP Based Virtual Private Networks", Work in Progress[2].

[2] Grossman, D. and J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 2684, September 1999.

[3] "MPOA v1.1 Addendum on VPN Support", ATM Forum, af-mpoa-0129.000, August, 1999, Bernhard Petri, editor, final ballot document.

[4] http://standards.ieee.org/regauth/oui/index.html

7. Адреса авторов

Barbara A. Fox

[1]Organizationally Unique Identifier - уникальный идентификатор организации.
[2]Работа завершена и опубликована в RFC 2764. *Прим. перев.*

Lucent Technologies

300 Baker Ave, Suite 100

Concord, MA 01742-2168

Phone: +1-978-287-2843

EMail: barbarafox@lucent.com

Bryan Gleeson

Nortel Networks

4500 Great America Parkway,

Santa Clara, CA 95054

Phone: +1-408-855-3711

EMail: bgleeson@shastanets.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

8. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.