МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

H.235.9

(09/2005)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг – Системные аспекты

Безопасность H.323: Поддержка шлюзов безопасности для H.323

Рекомендация МСЭ-Т H.235.9

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ H

АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	H.100–H.199
ИНФРАСТРУКТУРА АУДИОВИЗУАЛЬНЫХ УСЛУГ	
Общие положения	H.200–H.219
Мультиплексирование и синхронизация при передаче	H.220–H.229
Системные аспекты	**H.230–H.239**
Процедуры связи	H.240–H.259
Кодирование движущихся видеоизображений	H.260–H.279
Сопутствующие системные аспекты	H.280–H.299
Системы и оконечное оборудование для аудиовизуальных услуг	H.300–H.349
Архитектура услуг справочника для аудиовизуальных и мультимедийных услуг	H.350–H.359
Качество архитектуры обслуживания для аудиовизуальных и мультимедийных услуг	H.360–H.369
Дополнительные услуги для мультимедиа	H.450–H.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	H.500–H.509
Мобильность для мультимедийных систем и услуг серии H	H.510–H.519
Приложения и услуги мобильной мультимедийной совместной работы	H.520–H.529
Защита мобильных мультимедийных систем и услуг	H.530–H.539
Защита приложений и услуг мобильной мультимедийной совместной работы	H.540–H.549
Процедуры мобильного взаимодействия	H.550–H.559
Процедуры взаимодействия мобильной мультимедийной совместной работы	H.560–H.569
ШИРОКОПОЛОСНЫЕ И МУЛЬТИМЕДИЙНЫЕ TRIPLE-PLAY УСЛУГИ	
Предоставление широкополосных мультимедийных услуг по VDSL	H.610–H.619

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т H.235.9

Безопасность H.323: Поддержка шлюзов безопасности для H.323

Резюме

В данной Рекомендации определяется метод для обнаружения шлюзов безопасности (SG) на трактах сигнализации между взаимодействующими объектами H.323, и для совместного использования информации безопасности между привратником и SG для сохранения целостности и конфиденциальности сигнализации.

Источник

Рекомендация МСЭ-Т H.235.9 утверждена 13 сентября 2005 года 16-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

Ключевые слова

Шлюз, безопасность, сигнализация.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Использование брандмауэров и/или устройств трансляции сетевых адресов (NAT) для обеспечения безопасности трафика между участками сети с различным административным управлением создает проблему для протоколов сигнализации телефонии, которые должны обмениваться сетевыми адресами для сигнализации и медиаобмена.

В Рекомендации МСЭ-Т H.235.5 описывается инфраструктура, в которой конечная точка и привратник или два привратника могут использовать первоначальные сообщения RAS для согласования набора сильных общих секретов для них, и использовать эти секреты для шифрования отдельных частей последующих сообщений сигнализации вызова и RAS и аутентификации этих сообщений. Данный метод применяется только к сигнализации, маршрутизируемой привратником. Аналогичные методы и профили безопасности определяются в Рекомендациях МСЭ-Т H.235.1, H.235.2 и H.235.3. Данная безопасность может вступать в конфликт с шлюзами уровня приложения (ALG), которые соединяют области сети и манипулируют адресами сигнализации и медиапередачи, передаваемыми в сообщениях RAS H.225.0 и/или сигнализации вызова. Такие изменения в сообщении вызовут ошибку проверки аутентификации в месте назначения.

В данной Рекомендации описываются простые средства, с помощью которых можно проинформировать привратника о наличии шлюзов ALG на тракте сигнализации, и совместно использовать согласуемый ключ аутентификации с этими ALG. Это позволит ALG манипулировать в сообщениях сигнализации неконфиденциальными данными, в особенности адресами передачи, а затем аутентифицировать результат до передачи модифицируемого сообщения далее. В тексте данной Рекомендации такие устройства называются шлюзами безопасности (SG). Данный метод сохраняет сквозную конфиденциальность любых зашифрованных элементов в сигнализации.

Рекомендация МСЭ-Т H.235.9

Безопасность H.323: Поддержка шлюзов безопасности для H.323

1 Сфера применения

Данная Рекомендация может использоваться для любого привратника и конечной точки, использующих протоколы RAS H.225.0, с одним или более промежуточными шлюзами безопасности с заданным режимом работы.

2 Справочные документы

2.1 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и другой справочной литературе содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации. На момент опубликования, действовали указанные редакции документов. Все Рекомендации и другая справочная литература, являются предметом корректировки, и стороны пришли к договоренности основываться на этой Рекомендации и стараться изыскивать возможность для использования самых последних изданий Рекомендации и справочной литературы, перечисленной ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему, как отдельному документу, статуса рекомендации.

– ITU-T Recommendation H.225.0 (2003 г.), *Протоколы сигнализации о соединении и пакетирование потоков носителей для мультимедийных систем связи на основе пакетов*.

– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

– ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.

– ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile*.

– ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile*.

– ITU-T Recommendation H.235.5 (2005), *H.323 security: Framework for secure authentication in RAS using weak shared secrets*.

– ITU-T Recommendation H.245 (2005 г.), *Управляющий протокол для мультимедийной связи*.

– ITU-T Recommendation H.323 (2003 г.), *Мультимедийные системы связи на основе пакетов*.

2.2 Информативные справочные документы

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

3 Определения

В данной Рекомендации определяются следующие термины:

3.1 шлюз уровня приложения: Устройство, поддерживающее протоколы, которое соединяет два или более участка сети, и может интерпретировать и модифицировать протоколы уровня приложения для обеспечения трансляций адресов передачи и выполнения других функций. ALG может обеспечивать NAT транспортного уровня и функции брандмауэра изнутри или может контролировать их извне.

3.2 локальный адрес: Адрес передачи внутри локальной области адреса.

3.3 медиашлюз: Устройство, соединяющее две или более области сети, которое может контролироваться другим устройством (например, SG) для обеспечения контролируемых медиапотоков между областями. MG является эффективно программируемым NAT/брандмауэром при работе на транспортном уровне и ниже.

3.4 трансляция сетевых адресов: Операция установления соответствия между сетевыми адресами передачи в различных областях сети.

3.5 микроканал: Тракт, по которому пакетам и сообщениям разрешено проходить через SG (или контролируемый им медиашлюз) из одной области в другую. Обычно микроканал характеризуется четырьмя адресами передачи (адрес источника в области A, адрес SG в области A, адрес SG в области B, адрес назначения в области B). К другим характеристикам относятся транспортный протокол и направленность. Источник адреса может быть не указан, например, для порта listen ("слушающий" порт).

3.6 область: Участок сети, который совместно использует пространство общего сетевого адреса; предполагается, что различные области используют несовместимые, конфликтующие или конфиденциальные пространства адреса.

3.7 шлюз безопасности: Устройство, устанавливаемое между двумя или более участками IP сети для выполнения таких функций безопасности, как проверка достоверности или ограничение потоков пакетов и установление соответствий между транспортными адресами различных участков сети. В данной Рекомендации предполагается, что шлюз безопасности осведомлен о ALG протоколов сигнализации H.323.

4 Сокращения

В данной Рекомендации используются следующие сокращения:

ALG	Application Level Gateway	Шлюз уровня приложения
GCF	GatekeeperConfirm	Сообщение GatekeeperConfirm (подтверждение привратника)
GK	Gatekeeper	Привратник
GRJ	GatekeeperReject	Сообщение GatekeeperReject (отклонение привратника)
LCF	LocationConfirm	Сообщение LocationConfirm (подтверждение местонахождения)
LRQ	LocationRequest	Сообщение LocationRequest (запрос местонахождения)
MG	Media Gateway	Медиашлюз
NAT	Network Address Translation	Служба трансляции сетевых адресов
OID	Object Identifier	Идентификатор объекта
RAS	Registration, Admission and Status	Регистрация, допуск и статус
SG	Security Gateway	Шлюз безопасности
UDP	User Datagram Protocol	Протокол передачи дейтаграмм пользователя

5 Соглашения о терминах

В данной Рекомендации определяются различные идентификаторы объекта (OID) для сигнализации возможностей безопасности, процедур или алгоритмов безопасности. Эти OID относятся к иерархическому дереву заданных значений, которые могут происходить из внешних источников или являться частью дерева OID, утвержденных МСЭ-Т. Идентификаторы OID, относящиеся лишь к Рек. МСЭ-Т, имеют следующий вид:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V N**} где знак **V** символизирует одну десятичную цифру, обозначающую соответствующую версию Рек. МСЭ-Т H.235; например, 1, 2, 3 или 4. Знак **N** – символичное представление десятичной цифры, являющейся уникальным обозначением экземпляра OID и, таким образом, процедуры, алгоритма или возможности безопасности.

Таким образом, OID, зашифрованный в ASN.1 (Абстрактно-синтаксическая нотация, версия 1), состоит из последовательности чисел. Для удобства, текстовое мнемоническое обозначение строки краткой записи для каждого идентификатора объекта (OID) используется в тексте как "OID". Приводится (таблица) соответствий, в которой проводится соответствие между каждой строкой OID и последовательностью чисел в ASN.1. Разработки в соответствии с Рек. МСЭ-Т H.235, должны использовать только числа, зашифрованные в ASN.1.

Основные допущения

В данной Рекомендации рассматривается модель сети IP, в которой многочисленные участки сети, называемые областями, соединены между собой устройствами, называемыми шлюзами безопасности (SG), поддерживающими протокол H.323. Шлюзы безопасности созданы для контроля потоков информации между областями сети, которые они соединяют. Предполагается, что SG проверяют сообщения сигнализации, проходящие между областями, гарантируют их подлинность, извлекают информацию о транспортных адресах, которой обмениваются области, используют эту транспортную информацию для создания подходящих трактов прохождения между областями, делают адреса передачи подходящими для области, в которую пересылается сообщение. Конечно, шлюзы SG должны обеспечивать прохождение потока трактов сигнализации через себя, но они могут контролировать поддержку другим устройством любых создающихся медиапотоков. Протокол контроля между SG и "медиашлюзом" в данной Рекомендации не специфицируется.

Для того чтобы сделать услуги привратника в одной области доступными для конечных точек или привратников в другой области, SG может предоставить адрес обнаружения привратника в каждой обслуживаемой им области, где нет известного привратника. Затем SG направит любое сообщение обнаружения, полученное на один из этих адресов, на действительный привратник, после проведения любой необходимой обработки сообщения H.323. Пример конфигурации изображен на рисунке 1, где привратник обслуживает конечные точки в многочисленных областях сети.

В действительности шлюзы безопасности должны представлять привратник в каждой обслуживаемой ими области (разумеется, кроме той области, где находится привратник, например, область A для привратника A на схеме). На рисунке B SG предоставляет адреса обнаружения для обоих привратников, таким образом обеспечивая тракт привратник–привратник для сигнализации LRQ/LCF. Заметьте также, что шлюзу SG не нужно обеспечивать доступ к каждому привратнику в каждой области. Например, на рисунке 1 шлюзу A SG можно задать такую конфигурацию, что он будет поддерживать адрес обнаружения в области B только для привратника A.

Предполагается, что каждый привратник знает уникальное имя для каждого SG в системе, и что привратник и каждый SG также совместно используют криптографически сильные секреты, которые могут быть использованы для установления между ними безопасного соединения. То, как происходит согласование и обмен идентификационной информацией и соответствующими ключами, обсуждается ниже, однако не является главным предметом данной Рекомендации. Общий секрет для пары SG/привратник должен быть уникальным. Предполагается, что SG будут вносить изменения в адреса RAS и сигнализации вызова, для обеспечения прохождения через них трафика RAS и сигнализации вызова.

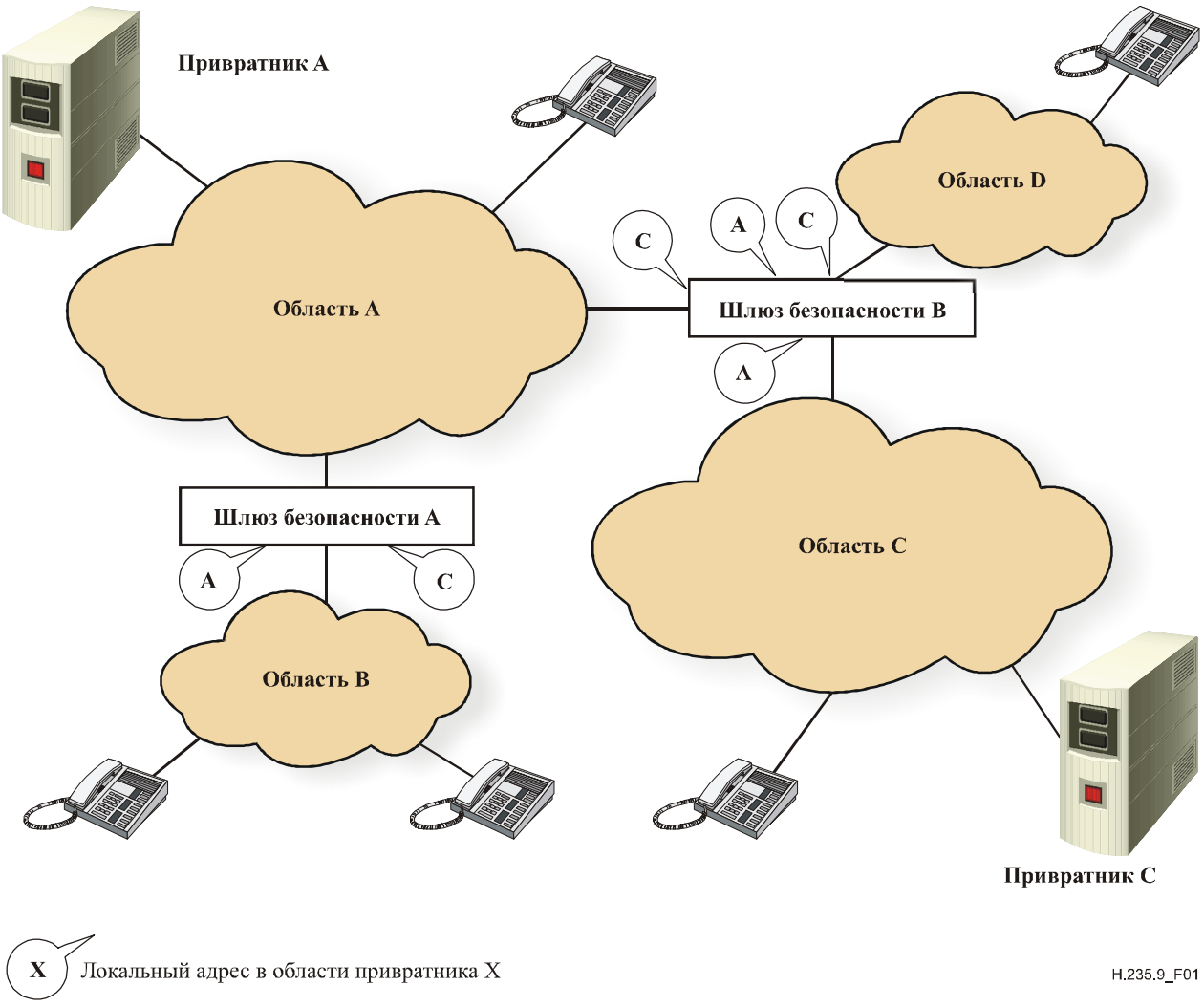


Рисунок 1/H.235.9 – Конфигурация шлюза безопасности

Кроме того, средства установления трансляции маршрутизации и/или адреса для первоначального процесса обнаружения не являются главным предметом данной Рекомендации, но обсуждаются ниже. Предполагается, что последующее создание адреса, наряду с требуемыми трансляциями, выполняется как часть функционирования SG.

6 Основы функционирования

В следующем описании предполагается, что каждый присутствующий в системе SG зарегистрирован на каждом привратнике, который он намеревается обслуживать. Подробности того, как это можно сделать, описываются далее. Предполагается, что для основной работы SG идентифицирует себя на каждом привратнике, совместно используя уникальный, сильный секрет с каждым привратником и предоставляет каждому привратнику один или более "локальных" адресов обнаружения привратника. Подробности регистрации SG будут обсуждены в одном из последующих пунктов. Далее описывается, как SG участвуют в регистрации конечной точки для получения доступа к ключу сквозной аутентификации, согласуемому между GK и конечной точкой.

6.1 Обнаружение привратника конечной точкой

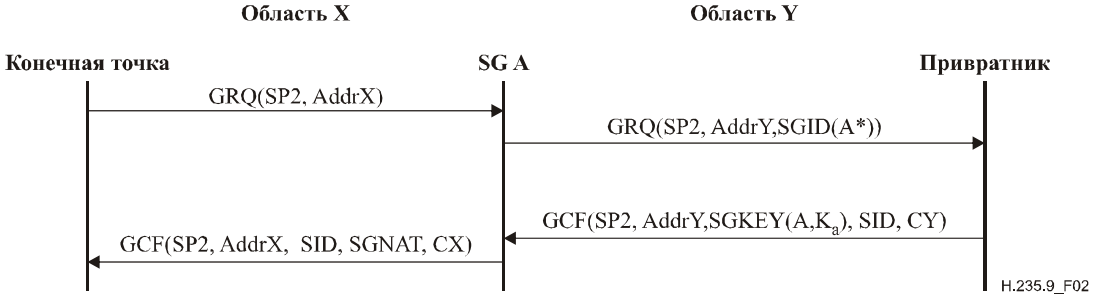
Когда конечная точка посылает GRQ на адрес обнаружения привратника, и GRQ проходит через SG на тракте к одному или более привратников, SG может добавить поле **ClearToken** к элементу GRQ.**token**, поскольку оно управляет адресами внутри GRQ. Это **ClearToken** будет идентифицироваться как маркер SG-id (идентифицируемый при помощи его **tokenOID**) и будет содержать строку идентификации, которая уникально идентифицирует SG. SG должен удалить из

профиля **authenticationCapability**, любой определенный **AuthenticationMechanism** (например, TLS в RFC 2246 и RFC 3546 или IPsec в RFC 2401), процедуру аутентификации сообщения которого он не может поддерживать. Это гарантирует, что привратник выберет профиль, совместимый с SG. SG, который первым получает сообщение GRQ должен включать элемент, идентифицирующий адрес обнаружения, на который он (шлюз) получил GRQ от конечной точки. Подразумевается, что каждый SG будет манипулировать с любыми полями адреса сигнализации внутри GRQ и последующих сообщений RAS для обеспечения прохождения всех сообщений сигнализации через SG для обработки адреса.

6.2 Распределение ключа аутентификации конечной точки

Когда сообщение GRQ достигает привратника (GK), он будет обрабатывать GRQ, включая маркер SG-id. Если GK будет выступать в качестве привратника конечной точки, он приготовится послать сообщение GCF обратно конечной точке. Затем GK включит в сообщение GCF выбранный **AuthenticationMechanism**, а также ключ SG **ClearToken** (идентифицируемый при помощи его **tokenOID**) для SG, идентифицируемого полученным маркером SG-id. Этот маркер ключа будет включать в себя идентификацию SG, идентификацию GK, вектор инициализации и ключ аутентификации сеанса, зашифрованный с использованием IV, а также секрет, общий для SG и привратника. Алгоритм шифрования должен быть согласован во время регистрации SG, или предоставлен заранее.

Когда сообщение GCF проходит обратно к конечной точке, оно проходит через SG, который предоставил маркер SG-id. SG должен проанализировать сообщение и найти идентификатор сеанса и маркер своего собственного ключа. Затем шлюз должен расшифровать ключ аутентификации сеанса и использовать его для аутентификации полученного сообщения. Если сообщение аутентично, SG будет манипулировать с любыми транспортными адресами как с приемлемыми. Затем SG перестроит сообщение без собственного маркера ключа SG (SG-key), вставит маркер SG-NAT, если его еще нет, аутентифицирует перестроенное сообщение и отошлет его далее. Необходимо сохранить идентификатор сеанса и ключ аутентификации для использования с последующими сообщениями RAS и сигнализации вызова в данном сеансе. Базовый цикл прохождения сообщений через одиночный SG изображен на рисунке 2. Заметьте также, что SG должен подготовить любые микроканалы, как выведенные из GCF (например, микроканал RAS и дополнительные микроканалы адреса GK.)



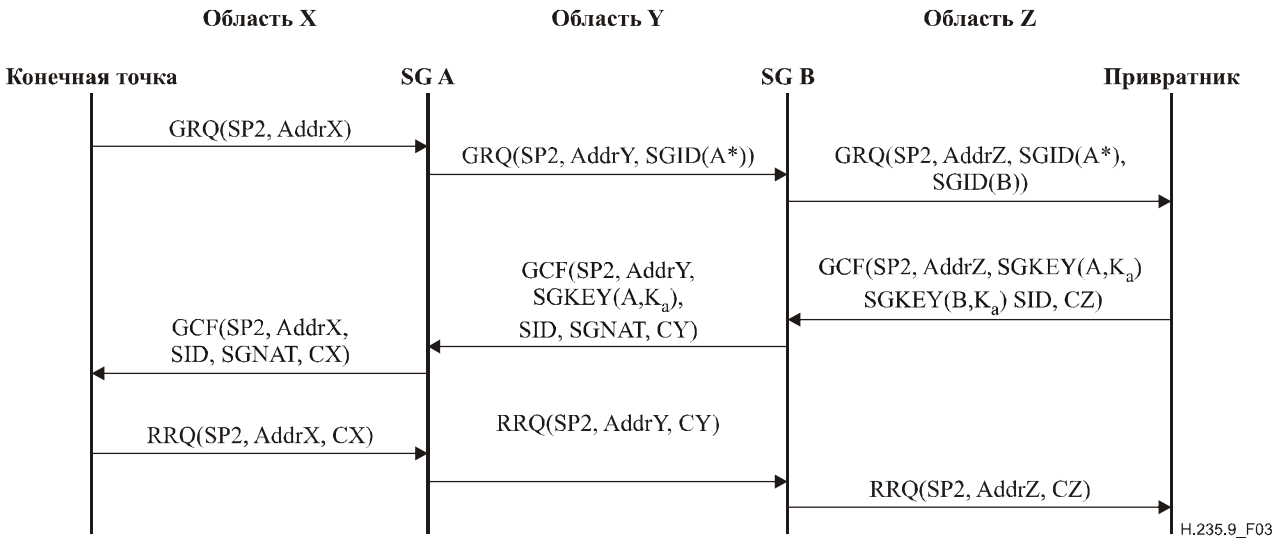
SP2 = профиль безопасности H.235.5
Addrx = адреса в области x
SGID(A*) = SG-id ClearToken, идентифицирующий наличие SG A
(* указывает, что SGID включает адрес обнаружения, использованный GRQ.)
SID = идентификатор сессии (присваиваемый привратником)
K_a= ключ аутентификации сообщения для SID
SGKEY(A, K_a) = SG-key ClearToken с K_a, зашифрованным секретным ключом шлюза A.
SGNAT = ClearToken SG-NAT
Cx = контрольная сумма сообщения (вычисляется с использованием согласованного K_a) в области x

Рисунок 2/H.235.9 – Основной обмен сообщениями через SG

В данную схему можно легко включить ряд SG между конечной точкой и привратником. Каждый SG добавляет свой собственный ClearToken при прохождении сообщения GRQ, и очищает свой собственный ответ ClearToken из GCF, при прохождении сообщения обратно от привратника к конечной точке. Первый SG на тракте сообщения GCF к конечной точке должен вставить в него

маркер SG-NAT. Данная операция изображена на рисунке 3. Обработка последующих сообщений RAS показана в виде трансформации транспортных адресов в сообщении RRQ и повторного вычисления контрольной суммы.

Аналогичный цикл можно выполнять в обмене LRQ/LCF, используя те же элементы сообщения, а результаты можно использовать для обработки и аутентификации последующих сообщений сигнализации в этом сеансе.



SP2 = профиль безопасности H.235.5
Addrx = адреса в области x
SGID(A*) = SG-id ClearToken, идентифицирующий наличие SG A
(* показывает присутствие адреса обнаружения, использованного конечной точкой)
SID = идентификатор сессии (присваиваемый привратником)
K_a = ключ аутентификации сообщения для SID
SGKEY(A, K_a) = SG-key ClearToken с K_a, зашифрованным секретным ключом шлюза A.
SGNAT = ClearToken SG-NAT
Cx = контрольная сумма сообщения в области x

Рисунок 3/H.235.9 – Двухуровневый обмен сообщениями через SG

6.3 Операции с адресами

Когда каждое сообщение сигнализации H.225.0 или H.245 проходит через шлюз SG, он должен проверить и заменить любые содержащиеся в них транспортные адреса так, чтобы они были действительными в следующей области, через которую будет проходить сообщение. Для этого может потребоваться, чтобы SG создал новые микроканалы потока для поддержки связанных потоков сигнализации и/или медиа, для создания которых предназначены данные адреса. Заметьте, что некоторые адреса представляют порты listen, которые должны быть открыты "на всякий случай"; когда/если пакет прибывает на порт listen, будет создан полностью специфицированный микроканал.

Каждый SG может анализировать каждый полученный транспортный адрес места назначения для выяснения, действительно ли он отображает адрес назначения на данном SG. Обратите внимание на пример конфигурации области и медиатрактов на рисунке 4. Медиапоток от конечной точки в области B к конечной точке в области C должен проходить через B SG и C, данный поток обозначен цифрой "1". Без специальной обработки шлюзом B SG медиапоток между двумя конечными точками в области B будет проходить эквивалентный тракт до области A и обратно в область B, данный поток обозначен цифрой "2". Теперь, если B SG обнаруживает, что адреса источника и места назначения, предоставленные для потока в области A, в действительности являются адресами на B SG, он может сократить поток любым из двух способов. Он может направить поток внутри области, как изображено потоком "3" (показанным на C SG для ясности), или, если он обнаруживает, что обе конечные точки находятся в области B, он может заменить адреса конечных точек в области B, для того чтобы маршрутизировать поток непосредственно между конечными точками, как представлено в потоке "4". Заметьте, что адреса "конечной точки", которые рассматривает B SG, могут в

действительности представлять собой адреса в SG (назовем его D), соединяющимся с другой областью. После того, как B SG модифицирует адреса для проведения "прямой" маршрутизации между адресами на D SG, D SG может затем таким же образом укоротить тракт потоков.

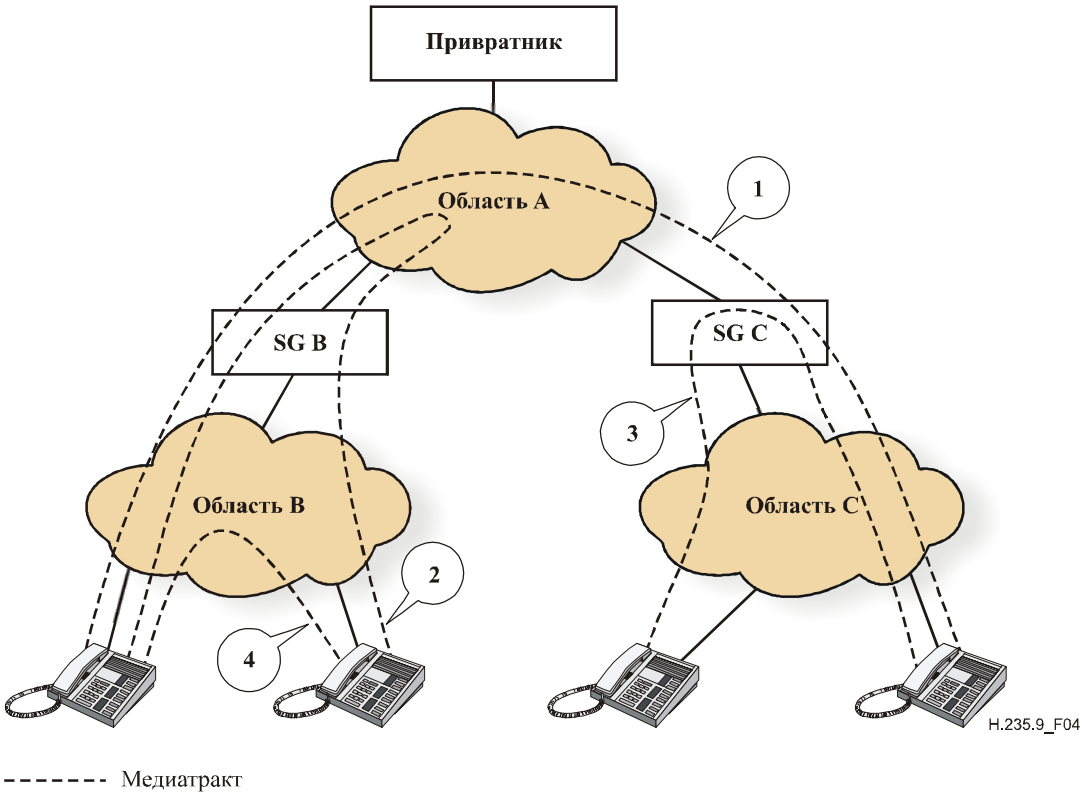


Рисунок 4/H.235.9 – Медиатракты

Единственным видом конфигурации, которая не работает по этой схеме, является случай, когда один участок получает доступ к другому участку более чем через один SG. Если регистрация и сигнализирование конечной точки проходит через один SG, а сигнализация другой конечной точки на том же участке происходит через другой SG, любому из этих SG будет трудно определить, что обе конечные точки находятся в одной области, или то, какие адреса использовать для конечной точки, сигнализация которой проходит через другой SG. Для предотвращения данной проблемы, необходимо использовать один SG, способный обрабатывать ожидаемый уровень сигнализации; нагрузку обработки медиапотока можно передать отдельным медиашлюзам, контролируемым SG.

7 Подробное описание сигнализации

Наиболее эффективно идентифицировать поддержку данной возможности можно по стандартному идентификатору объекта (OID) в соответствующих явных маркерах. Далее эти маркеры будут называться маркерами SG. Это позволяет любому получающему привратнику (или промежуточному шлюзу или другому неучаствующему устройству) игнорировать данную функцию. Заданные OID будут использоваться для идентификации полей **ClearToken**, содержащих следующие элементы:

- **tokenOID** – со значением OID, заданного для данной функции, назовем его "SG1", см. пункт 11;
- **generalID** – если присутствует, указывается имя SG, которому направляется данный **ClearToken** (использованный в маркере SG-key);
- **sendersID** – содержащий имя SG, создающего данный **ClearToken** (использованный в маркере ключа SG (SG-key);
- **profileInfo** – содержит особую информацию, передаваемую данным **ClearToken**, как определено в таблице 1.

Таблица 1/H.235.9 – Элементы профиля для обнаружения SG

Имя элемента	Значение ElementID	Тип элемента (длина)	Описание элемента
Token Type	1	целое число	0 = маркер SG-id 1 = маркер SG-key 2 = маркер SG-NAT 3 = маркер SG-register
Encrypted Key	2	октеты (16 для SP2)	Ключ аутентификации сеанса из указанного профиля безопасности, зашифрованный общим секретом для определенных SG и GK. Посылается в маркер ключа SG. Необходимый IV для расшифровывания специфицируется в ProfileElement.paramS.
ServedRealm	3	имя	Имя области, для которой SG может/должен предоставить адрес обнаружения привратника

8 Анализ конфигурации SG

Процедуры, описанные в данной Рекомендации, зависят от некоторых средств, которыми пользуются SG в сети для обнаружения трактов к привратнику(ам), услуги которых необходимо сделать доступными для пользователей в различных областях сети. Каждый SG должен быть способен связаться со своим(и) привратником(ами) в одной области, и обеспечить конечным точкам (или другим привратникам) в другой области доступ к этим привратникам. Например, на рисунке 3, B SG получает доступ к привратнику в области Z. Он может обеспечить доступ к привратнику для элементов в области Y. Таким образом, A SG может получить доступ к привратнику через B SG. Получив доступ к привратнику, B SG может обеспечить доступ для абонентов в области X. Это наводит на мысль использования самими SG протоколов обнаружения, таких, как RAS. Данную процедуру также можно использовать для идентификации каждого SG на каждом доступном привратнике и для согласования (набора) ключей для защиты обмена сообщениями сигнализации пользователя.

8.1 Регистрация SG

SG одной области может служить представителем привратника в другой области, доступной для SG. Например, на рисунке 1, A SG может обеспечивать представление (адрес обнаружения) для привратника в области A для области B, если ему известен адрес обнаружения привратника в области A. Эту схему можно расширить до нескольких уровней шлюзов SG; так как каждый SG обнаруживает привратника (или представителя), он может предоставить адрес обнаружения для данного привратника в одной или более новых областях, в которых точка SG, подключенная к данной области, может обнаружить эти новые адреса.

Шлюзы SG должны использовать процедуры RAS H.225.0 для обнаружения и регистрации привратников в любой области, которую они хотят обслуживать в качестве шлюза безопасности. SG должен идентифицироваться как тип конечной точки **gateway**. SG может определять поддержку протокола для H.323, если он хочет задать поддерживаемые коды зон и/или ограничения пропускной способности, но это не является необходимым. Для аутентификации SG на привратнике и согласования защищенных общих секретов для использования в описанных ниже процедурах необходимо использовать стандартные процедуры безопасности, например, описанные в Рекомендациях МСЭ-Т H.235.1, H.235.2, H.235.3 и H.235.5. Процедуры H.235.1, H.235.2, H.235.3 и H.235.5 могут проходить через другие шлюзы безопасности, поддерживающие данную Рекомендацию. В сообщение RRQ, посылаемое привратнику, SG должен также включить SG-register ClearToken. Данный маркер служит для идентификации шлюза как SG, он должен содержать элемент **ServedRealm** для каждой новой области, обслуживаемой SG. Каждый элемент отображает потенциально новый адрес обнаружения привратника в соответствующей области. Конфигурацию каждого SG можно настроить таким образом, чтобы ограничить области, которым предоставляется адрес обнаружения для привратника. Например, на рисунке 1, конфигурацию B SG можно изменить таким образом, чтобы не предоставлять адрес обнаружения для привратника C в области D, таким

образом принудив конечную точку в области D зарегистрироваться на привратнике A. До тех пор, пока SG сам не делает или принимает вызовы, ему не нужно предоставлять адрес сигнализации вызова во время регистрации; в сообщении RRQ он может ввести пустое SEQUENCE для **callSignalAddress**. Привратник должен ответить таким же образом в **callSignalAddress** сообщения RCF.

Область(и), которые может обслуживать SG, должны быть указаны привратником путем возвращения в сообщении RCF маркера SG-register, содержащего один или более элементов **ServedRealm** из сообщения RRQ шлюза SG. По окончании регистрации, SG должен открыть "слушающий" сокет (listen socket) для адреса обнаружения привратника в каждой обозначенной области. Для объявления данного адреса обнаружения внутри области могут быть использованы алгоритмы, не рассматриваемые в данной Рекомендации. Привратник может предпочесть использовать адреса обнаружения, предоставляемые SG в списке изменяющихся адресов.

Можно использовать любой профиль безопасности RAS при условии, что шлюзам SG разрешено считывать и преобразовывать адреса сигнализации и медиапередачи, и они могут заново аутентифицировать сообщение.

Для проведения соответствий между участками сети и возможностями соединения и для аутентификации SG привратник может воспользоваться информацией области SG. Привратник должен возвратить информацию SG:

- Мандат привратника.
- Адрес(а) регистрации, которые может использовать SG для ретрансляции запросов RAS от конечных точек на обслуживаемом(ых) участке(ах), (т. е. GK может отказаться поддерживать конечные точки на одном или более участках, обслуживаемых SG.).

Важным результатом успешной регистрации SG является сильный ключ с общим секретом для SG и привратника. Из этого ключа могут быть образованы ключи шифрования и/или аутентификации. Ключ аутентификации может использоваться для аутентификации схемы регистрации SG, а ключ шифрования следует использовать во время регистраций конечной точки для шифрования ключа аутентификации сеанса конечной точки для распределения SG, как описано выше.

8.2 Мандат аутентификации

В отличие от количества конечных точек, ожидается, что количество SG в сети с многочисленными участками относительно невелико. В большинстве случаев, ожидается, что обслуживание будет производиться по подписке или другому официальному соглашению. Поэтому у привратника будет некоторая идентифицирующая информация о шлюзах SG, которые могут на нем зарегистрироваться. В самом простом случае, SG могут представлять собой присвоенные пароли, и могут применяться H.235.1, H.235.2, H.235.3, H.235.5 или процедуры аутентификации запрос/вызов. Использование предварительных общих секретов, конечно, требует защищенного внеполосного механизма для их распределения.

Альтернативный механизм может основываться на сертификатах открытого ключа. Копии сертификата привратника (или сертификат, принадлежащий службе, подписавшей сертификат привратника) могут быть установлены на шлюзы SG в ходе доверенного процесса. Использование методов сертификата является предметом дальнейших исследований.

9 Анализ безопасности

Протоколы данного типа, в котором можно изменять сообщения при пересылке, подвержены атакам типа downgrade (понижение версии). Например, если конечная точка предоставляет зашифрованные и незашифрованные возможности медиапередачи, SG – недоброжелатель может удалить предложения шифрования и просто предоставить незашифрованные предложения, таким образом гарантировав то, что медиапотоки будут незашифрованными. Предотвратить данный тип атак можно, если конечные точки (и привратник) будут предлагать только те возможности, которые приемлемы для их собственной политики безопасности. Конечно, обеспечение создания и поддержания подходящего уровня безопасности является обязанностью конечных точек и их пользователей. То же утверждение относится к выбору профилей безопасности во время регистрации: если конечная точка требует сильной аутентификации, она должна уточнить это в GRQ, и не должна принимать более слабое предложение от привратника.

10 Применимость

Данная схема будет применима к другим профилям безопасности H.235.1, H.235.2 и H.235.3 в добавление к профилям, описанным в Рек. МСЭ-Т H.235.5. Может поддерживаться любой профиль безопасности, который обеспечивает образование подходящих ключей аутентификации. SG должны изучить элементы сообщений GRQ/GCF (например, **authenticationCapability** и/или **authenticationMode**) и проверить, могут ли они поддерживать согласуемую схему аутентификации сообщения или безопасности.

11 Идентификатор объекта

OID	Значение идентификатора объекта	Описание
"SG1"	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 65 }	ClearToken, передающий элементы профиля для обнаружения SG.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	**Аудиовизуальные и мультимедийные системы**
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.