МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т J.261

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(10/2009)

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

IPCablecom

Концепция внедрения преимущественной электросвязи в сетях IPCablecom и IPCablecom2

Рекомендация МСЭ-Т J.261

Рекомендация МСЭ-Т J.261

Концепция внедрения преимущественной электросвязи в сетях IPCablecom и IPCablecom2

Резюме

В настоящей Рекомендации предоставляется концепция внедрения возможностей преимущественной связи в сетях IPCablecom и IPCablecom2.

Подход настоящей Рекомендации состоит в определении концепции в отношении возможностей, которые могут быть использованы для удовлетворения требований, изложенных в Рекомендации МСЭ-Т J.260, и создает основу для разработки подробных Рекомендаций по вопросам IPCablecom и IPCablecom2 в целях обеспечения преимущественной электросвязи.

Источник

Рекомендация МСЭ-Т J.261 утверждена 30 октября 2009 года 9-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с Резолюцией 1 ВАСЭ.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). 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 осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное 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

Электросвязь в условиях чрезвычайных ситуаций/бедствий, предназначенная для правомочных пользователей, играет жизненно важную роль в обеспечении здоровья, безопасности и благополучия народов во всех странах. Обычно в целях содействия осуществлению операций в условиях чрезвычайных ситуаций/бедствий используются гарантированные возможности в отношении ориентированных на пользователя услуг преимущественной электросвязи, которые могут быть реализованы с помощью технических решений и/или административной политики. Возможности кабельных инфраструктур IPCablecom и IPCablecom2 являются важным ресурсом для обеспечения гарантированных услуг преимущественной электросвязи.

Ключевые аспекты преимущественной электросвязи в кабельных сетях, которые рассматриваются в настоящей концептуальной Рекомендации, подразделяются на две основные области – аутентификацию и приоритет. Эти две области являются существенными особенностями сетей, требуемыми для получения ресурсов кабельных сетей при необходимости преимущественного обслуживания. Другие области, такие как политика, управление трафиком, маршрутизация с обходными путями, обеспечение возможности восстановления и др., не входят в сферу применения настоящего варианта или не рассматриваются в нем.

Изменяющийся характер сетей электросвязи в общем и кабельных сетей в частности пригоден для поэтапного подхода к обеспечению преимущественного обслуживания. При поэтапном подходе необходимо рассматривать изменение Рекомендаций по вопросу IPCablecom: первоначальный набор Рекомендаций по IPCablecom, Рекомендации по IPCablecom, пересмотренные в 2005 году, и набор Рекомендаций по IPCablecom2.

Рекомендация МСЭ-Т J.261

Концепция внедрения преимущественной электросвязи в сетях IPCablecom и IPCablecom2

1 Сфера применения

Цель настоящей Рекомендации – предоставление концепции для внедрения услуг преимущественной электросвязи в кабельных сетях, описанных в [ITU-T J.160] и [ITU-T J.360]. Эта концепция составляет содержание одной Рекомендации из набора Рекомендаций, в которых рассматриваются эти услуги.

Ключевыми аспектами услуг преимущественной электросвязи, которые рассматриваются в рамках этой концепции, являются приоритет и аутентификация. Архитектурные различия этих двух ключевых аспектов рассматриваются в плане логических функциональных объектов, определенных в [ITU-T J.160] и [ITU-T J.360], соответственно.

Хотя в настоящем варианте концепции рассматривается два ключевых аспекта, а именно приоритет и аутентификация, необходимые для обеспечения преимущественного обслуживания при предоставлении услуг электросвязи, другие аспекты, такие как политика, управление трафиком, маршрутизация с обходными путями, обеспечение возможности восстановления, не входят в сферу применения или оставлены для дальнейшего исследования. Например, в будущих вариантах предполагается рассмотреть вопросы предоставления преимущественных услуг для конкретных пользователей и/или устройств (адаптеров медиатерминала) в конкретных местоположениях.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей Рекомендации на какой-либо документ не придает ему как отдельному документу статус рекомендации.

[ITU-T J.160] Рекомендация МСЭ-Т J.160 (2005 г.), *Архитектура структуры для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов.*

[ITU-T J.163] Recommendation ITU-T J.163 (2007), *Dynamic quality of service for the provision of real-time services over cable television networks using cable modems.*

[ITU-T J.170] Recommendation ITU-T J.170 (2005), *IPCablecom Security Specification.*

[ITU-T J.179] Рекомендация МСЭ-Т J.179 (2005 г.), *Обеспечение мультимедийной связи в IPCablecom.*

[ITU-T J.260] Рекомендация МСЭ-Т J.260 (2005 г.), *Требования к предпочтительному использованию средств электросвязи в сетях IPCablecom.*

[ITU-T J.360] Recommendation ITU-T J.360 (2006), *IPCablecom2 architecture framework.*

[ITU-T J.368] Recommendation ITU-T J.368 (2008), *IPCablecom2 quality of service specification.*

[IETF RFC 3261] IETF RFC 3261 (2002 г.), *SIP: Session Initiation Protocol*.

[IETF RFC 4412] IETF RFC 4412 (2006 г.) *Communications Resource Priority for the Session Initiation Protocol (SIP)*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 гарантированные возможности [ITU-T J.260]: Возможности, обеспечивающие высокую достоверность того, что критически важная связь доступна и надежно работает, или уверенность в этом.

3.1.2 аутентификация [ITU-T J.260]: Действие или метод, используемый для проверки заявляемой идентичности.

3.1.3 санкционирование [ITU-T J.260]: Действие для определения того, можно ли предоставить предъявителю конкретного полномочия конкретную привилегию, такую как доступ к ресурсам электросвязи.

3.1.4 кабельный модем [ITU-T J.160]: Кабельный модем представляет собой оконечное устройство второго уровня, которое завершает соединение DOCSIS со стороны клиента.

3.1.5 чрезвычайная ситуация [ITU-T J.260]: Опасная ситуация, которая наступает внезапно и неожиданно. Для восстановления нормального состояния, чтобы исключить дальнейший риск для людей или имущества, могут потребоваться масштабные неотложные значительные усилия, осуществлению которых содействует электросвязь. Если эта ситуация обостряется, то она может перерасти в кризис и/или бедствие.

3.1.6 международная чрезвычайная ситуация [ITU-T J.260]: Чрезвычайная ситуация, распространившаяся за пределы международных границ, которая затрагивает несколько стран.

3.1.7 IPCablecom [ITU-T J.160]: Проект МСЭ-Т, включающий архитектуру и серию Рекомендаций, делающих возможной поставку услуг в режиме реального времени по сетям кабельного телевидения с использованием кабельных модемов.

3.1.8 метка [ITU-T J.260]: Идентификатор, находящийся внутри элемента данных или прикрепленный к элементу данных. В рамках преимущественной электросвязи – это индикатор приоритетности. Такой идентификатор может использоваться как механизм преобразования различных уровней приоритетности в сети.

3.1.9 управляемая IP-сеть [ITU-T J.160]: IP-сеть, управляемая одним объектом для целей транспортирования сигнализации IPCablecom и медиапакетов.

3.1.10 преимущественная [ITU-T J.260]: Возможность, предоставляющая преимущества, по сравнению с обычными возможностями.

3.1.11 возможности приоритетного обслуживания [ITU-T J.260]: Возможности, которые обеспечивают первоочередный доступ к ресурсам сетей электросвязи и/или их использованию.

3.1.12 абонент [ITU-T J.360]: Объект (включающий одного или нескольких пользователей), который связан контрактом с поставщиком услуг.

3.1.13 агент пользователя (UA) [ITU-T J.360]: Агент SIP, определенный в [IETF RFC 3261].

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин:

3.2.1 оборудование пользователя: Любое устройство, непосредственно используемое конечным пользователем для осуществления связи.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

AKA	Authentication and Key Agreement	Соглашение об аутентификации и ключе
ATM	Automatic Teller Machine	Автоответчик
AVP	Attribute Value Pair	Пара значений атрибута

CM	Cable Modem		Кабельный модем
CMS	Call Management Server		Сервер управления вызовами
CMTS	Cable Modem Termination System		Система окончания кабельного модема
DQoS	Dynamic Quality of Service		Динамическое качество обслуживания
E-DVA	Embedded Digital Voice Adapter		Встроенная цифровая телефонная приставка
E-MTA	Embedded Media Terminal Adapter		Встроенный адаптер медиатерминала
IPSec	Internet Protocol Security		Протокол IPSec
KDC	Key Distribution Centre		Центр распределения ключей
MGC	Media Gateway Controller		Контроллер медиашлюза
MTA	Media Terminal Adapter		Адаптер медиатерминала
P-CSCF	Proxy Call Session Control Function		Посредническая функция управления вызовами и сеансами
PIN	Personal Identification Number		Персональный идентификационный номер
PKI	Public Key Infrastructure		Инфраструктура открытого ключа
PKINIT	Public Key Cryptography for Initial Authentication		Шифрование с открытым ключом для первоначальной аутентификации
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
QoS	Quality of Service		Качество обслуживания
RTP	Real-time Transport Protocol		Транспортный протокол реального времени
SIP	Session Initiation Protocol		Протокол инициирования сеанса
TGT	Ticket Granting Ticket		"Пропуск на выдачу билета"
TLS	Transport Layer Security		Безопасность транспортного уровня
UE	User Equipment	ПО	Пользовательское оборудование

5 Условные обозначения

Нет.

6 Общая концепция приоритета

В [ITU-T J.260] перечисляется ряд требований для обеспечения приоритетного обслуживания в сетях IPCablecom и IPCablecom2. Несмотря на существующие различия в архитектуре между сетью IPCablecom, описанной в [ITU-T J.160], и сетью IPCablecom2, описанной в [ITU-T J.360], в настоящем пункте рассматривается концепция, применимая к обеим сетям. При рассмотрении приоритетного обслуживания в отношении услуг преимущественной электросвязи учитывают три аспекта – классификацию или маркировку сеанса или вызова как требующих приоритетного обслуживания, сигнализацию, относящуюся к приоритету, и механизмы обеспечения требуемого приоритета. Выбор механизмов и правил, а также их соответствующих реализаций не входят в сферу применения настоящей Рекомендации.

В таблице 1 приведено распределение требований по категориям в соответствии с этими тремя аспектами – классификацией, сигнализацией и механизмами. Некоторые требования отнесены к категориям, имеющим более одного аспекта, поскольку следует соблюдать классификацию приоритета вызова, а существующие механизмы сохранения классификации могут изменяться.

Таблица 1 – Отображение требований в виде аспектов приоритета

Требование [ITU-T J.260]	Категория
Приоритетный доступ к сетям IPCablecom и IPCablecom2 (1a)	Классификация
Активирование вызова и особенности вызова (1b)	Сигнализация
Распределение ресурсов сети (1c)	Механизмы
Приоритет, предоставленный маркированным вызовам на шлюзах (1d)	Сигнализация и механизмы
Присвоение меток исходящим вызовам (2)	Классификация
Приоритет, предоставленный маркированным вызовам в сетях IPCablecom и IPCablecom2 (3)	Механизмы
Преобразование меток, используемых на направлении от кабельной сети к шлюзовому устройству соединения с сетью и на направлении от шлюзового устройства соединения с сетью к кабельной сети (4 и 5)	Механизмы
Сохранение метки приоритета в пределах кабельной сети (6)	Сигнализация и механизмы
Приоритетный вызов при транзите через кабельную сеть обслуживается в соответствии с возможностями кабельной сети (7)	Классификация и механизмы
Количество уровней приоритета: минимально 1 уровень и дополнительные уровни исходя из национальных возможностей (8)	Классификация
Приоритетное обслуживание, предоставляемое кабельной сетью, в отношении вызовов с меткой приоритета, поступающих из защищенной сети (9)	Механизмы

Установление приоритета означает получение большей вероятности завершения вызова/сеанса. Другими словами, после определения того, что трафик относится к услуге преимущественной электросвязи, на основе принципов должна быть обеспечена большая вероятность успеха, касающегося принятия вызова, маршрутизации и доставки трафика. Эта возможность должна существовать на линии доступа и распространяться на все соответствующие объекты сети, такие как серверы управления вызовами (CMS) и контроллеры медиашлюза (MGC) или объекты, входящие в инфраструктуру протокола инициирования сеанса (SIP).

Несмотря на то что в IPCablecom механизмы обеспечения приоритета и присвоение QoS не являются одинаковыми, классы сеансов DQoS могут быть использованы для назначения тому или иному сеансу приоритетного обслуживания. Одним из требований распределения ресурсов, которое может быть обеспечено в сетях IPCablecom, является принцип мультимедийных вентилей, описанный в [ITU-T J.163] и [ITU-T J.179]. Рекомендация [ITU-T J.163] относится к IPCablecom и рассматривается ниже. Вентили используются для управления доступом IP-потока с повышенным QoS, поступающим из сети DOCSIS. Вентили устанавливают в системе окончания кабельного модема (CMTS), с тем чтобы обеспечить создание служебных потоков с гарантированным качеством обслуживания путем резервирования требуемых ресурсов. Управление доступом в системе CMTS используется для обеспечения большего объема ресурсов, чем объем выделенных и зарезервированных ресурсов. В случае IPCablecom при использовании [ITU-T J.163] клиент, такой как встроенный адаптер медиатерминала (E-MTA), инициирует резервирование и активирование ресурсов, в то время как [ITU-T J.179] поддерживающий мультимедийный вентиль обеспечивает выполнение этих шагов сервером-посредником от имени конечного клиента.

Приоритетная сигнализация для IPCablecom и IPCablecom2 рассматривается по отдельности из-за различных подходов, используемых E-MTA или UE для соединения с сетью доступа.

В сетях IPCablecom и IPCablecom2 в качестве транспортного протокола среды передачи для аудио- и видеопакетов используется транспортный протокол реального времени (RTP). Как указано в [b-IETF RFC 4190], RTP не включает маркировки для указания приоритета пакета с меткой. Рассматриваются различные методы, включающие описание нового поведения преимущественного трафика по участкам сети, нового протокола промежуточного уровня поверх IP или маркировку пакета прикладного уровня.

7 Общая концепция аутентификации

Для осуществления аутентификации в сетях IPCablecom и IPCablecom2 требуются предоставляемые в некоторой форме полномочия, которые используются системой для проверки целостности идентификатора, представляемого предполагаемым пользователем системы. Управление этими полномочиями имеет большое значение при рассмотрении типа механизма(ов) аутентификации, используемого(ых) в любой кабельной сети. Необходимо также учитывать существующие применяемые механизмы аутентификации (например, для абонентов), а также приемлемость и практичность существующих применяемых механизмов аутентификации при использовании в целях преимущественной электросвязи в других сетях. Существуют две формы аутентификации:

- на основе полномочий пользователя, когда преимущественный пользователь должен ввести в устройство (например, E-MTA) информацию или предоставить ее; и
- на основе оборудования, когда аутентификация базируется на распознавании системой кабельной сети оборудования преимущественного пользователя.

7.1 Аутентификация на основе полномочий пользователя

При аутентификации на основе полномочий пользователя используется встроенная в устройство или сеть функциональная возможность, которая принимает представленную в некоторой форме вводную информацию, с помощью которой преимущественный пользователь может аутентифицировать свой идентификатор. Устройство взаимодействует с сервером аутентификации, входящим в инфраструктуру, для проверки идентификатора с целью обеспечения возможности предоставления преимущественной услуги. Пользователь может выполнить аутентификацию на основе полномочий пользователя путем вызова специального номера и ввода персонального идентификационного номера (PIN). Этот метод позволяет использовать любое пользовательское оборудование систем IPCablecom и IPCablecom2 со стандартной 12-клавишной цифровой клавиатурой. Метод с PIN является полезным ввиду его простоты и обратной совместимости с возможностями преимущественного обслуживания в развернутых сетях.

7.2 Аутентификация на основе оборудования

Аутентификация на основе оборудования базируется на распознавании системой PCablecom или IPCablecom2 пользовательского оборудования преимущественной связи. В данном методе идентичность оборудования (например, цифровой сертификат устройства) используется в качестве полной или частичной идентификации пользователя преимущественной электросвязи. Данная аутентификация будет производиться на конкретных частях оборудования (например, телефонах, приставках E-MTA) и может потребовать использования дополнительных механизмов (например, смарт-карт, меток и/или PIN) помимо базовой физической защиты оборудования.

7.3 Базовые механизмы аутентификации

Несмотря на то что механизмы с использованием PIN являются самыми простыми и наиболее доступными возможными методами в существующих сетях IPCablecom, в будущем для некоторых приложений могут потребоваться более безопасные методы. Эти методы рассматриваются в настоящем пункте.

Аутентификация может быть выполнена пользователем путем набора специального номера и ввода PIN. Данный метод позволяет использовать любое пользовательское оборудование IPCablecom со стандартной 12-клавишной цифровой клавиатурой. Метод PIN является полезным ввиду его простоты и обратной совместимости с возможностями преимущественного обслуживания в развернутых сетях. Однако полагаться на PIN означает основываться на единственном факторе (что-то, что известно отдельному лицу), а не на сочетании факторов (таких, как "что-то, чем обладает отдельное лицо" или "что-то присущее только отдельному лицу"). В условиях растущей зависимости от пакетной связи за основу, как правило, принимается использование двух факторов, таких как:

- знание PIN в сочетании с владением картой с магнитной кодовой полоской (например, подобно используемой для доступа в банкомат);
- знание пароля в сочетании с владением устройством предоставления ограниченных по времени полномочий (например, как используемое для онлайновой банковской и финансовой деятельности).

Однако большая часть этих различных методов являются применимыми, только если устройство имеет более широкие возможности ввода/вывода чем стандартная 12-клавишная клавиатура.

Помимо функциональных средств PIN существует несколько механизмов аутентификации (или сочетаний механизмов), которые можно использовать в кабельных сетях. Например, в качестве варианта можно было бы использовать пароли-фразы (предполагая, что возможности распознавания голоса обладают достаточно низкими "ложноположительными" и "ложноотрицательными" показателями). Тогда как существуют многочисленные другие механизмы аутентификации (например, пароли, смарт-карты, биометрические считыватели и др.), их непросто реализовать, принимая во внимание архитектуры кабельных сетей (например, приставки E-MTA не имеют считывающих устройств для смарт-карт).

Для мультимедийных услуг, требующих QoS, в IPCablecom определены интерфейсы, в которых используется аутентификация на основе протоколов RADIUS и Diameter: RADIUS – между сервером управления вызовами и diameter – между функцией P-CSCF и функцией данных начисления платы. Ниже перечислены возможные механизмы, которые не определены в Рекомендациях по IPCablecom и которые можно было бы рассмотреть для осуществления аутентификации пользователя услуг преимущественной связи:

- пароли в сочетании с инфраструктурой аутентификации на основе протокола RADIUS;
- пароли в сочетании с инфраструктурой аутентификации на основе протокола Diameter;
- пароли в сочетании с центром распределения ключей (KDC), таким как Kerberos;
- пароли в сочетании со смарт-картами; и
- пароли в сочетании со смарт-картами и инфраструктурой открытого ключа (PKI).

Механизмы каждого типа различаются между собой в отношении обеспечиваемой каждым из них степени гарантирования того, что идентичность действительна и представлена действительным пользователем системы. Эти механизмы отличаются также по масштабу развертывания, рабочим возможностям и сложности. Перечисленные выше методы следует дополнительно рассмотреть на предмет их соответствующих возможностей аутентификации, степени масштабируемости, качества, междоменной функциональной совместимости и функциональной совместимости с унаследованными/существующими механизмами аутентификации.

Аутентификация преимущественного обслуживания определенных вызовов/сеансов в сетях IPCablecom обязательно требует наличия высокого уровня безопасности. Однако получение аутентификации пользователем должно быть очень простым, в том числе, потому что в некоторых случаях пользователь будет находиться в условиях чрезвычайной ситуации. Поэтому, по возможности, следует выбирать сочетание механизмов, которые обеспечат простоту использования и высокий уровень безопасности.

7.4 Механизмы управления полномочиями

Управление полномочиями имеет важное значение, для того чтобы обеспечить использование системой обновленных и точно определенных полномочий для аутентификации пользователя. Управление полномочиями включает в себя следующее: обновления полномочий, аннулирование полномочий и обмен информацией о полномочиях между доменами поставщиков услуг.

Управление полномочиями зависит от самих полномочий, таких как базы данных паролей, серверы RADIUS/Diameter, серверы KDC, смарт-карты, корневой сервер PKI и др. Механизмы каждого из этих типов отличаются по степени целостности данных и защиты конфиденциальности, обеспечиваемых полномочиями. Эти механизмы различаются также масштабом развертывания, рабочими возможностями и сложностью.

8 Аутентификация и приоритет в сетях IPCablecom

8.1 Аутентификация в сетях IPCablecom

В [ITU-T J.160] и [ITU-T J.170] описаны механизмы, используемые для аутентификации клиента, запрашивающего услугу. Для аутентификации клиента используется расширение протокола Kerberos с шифрованием с открытым ключом для первоначальной аутентификации (PKINIT). Протокол безопасной передачи данных по протоколу Интернет (IPSec) на основе Kerberos используется для создания ассоциации между CMS и MTA (клиентом). Описаны три этапа. На первом этапе клиент взаимодействует с центром распределения ключей (KDC) путем предоставления сертификата своего устройства для получения "пропуска на выдачу билета" (TGT) с целью получения от KDC пропуска в конкретный сервер, такой как CMS. Клиент может пропустить первый этап и предоставить KDC сертификат устройства для непосредственного получения пропуска в конкретный сервер. На третьем этапе совместно с прикладным сервером устанавливается пара параметров безопасности для направления и получения защищенных данных по протоколу IPSec.

8.2 Приоритет в сетях IPCablecom

Преимущественные пользователи будут получать приоритетное обслуживание. Это приоритетное обслуживание обеспечивается с использованием метода, описанного в [ITU-T J.163].

Резервирование ресурсов в IPCablecom осуществляется с использованием двух компонентов. Первый компонент – уровень линии данных, на котором обеспечивается более оперативная доступность потоков услуги DOCSIS для вентилей определенного класса сеансов. Второй компонент – сеансовый уровень, на котором описывается статус приоритета вызова, так чтобы информация могла распространяться ко всем соответствующим объектам в сети.

Установление приоритета на кабельной линии доступа может быть обеспечено, прежде всего, путем взаимоувязывания вентилей динамического качества обслуживания (DQoS) с конкретным классом обслуживания, зарезервированным специально с этой целью, а затем, как следствие, требования, чтобы система CMTS осуществила конкретное действие. В зависимости от важности класса сеанса к конечному запросу ресурса применяется различное управление доступом. Например, можно было бы определить класс сеанса для нормальной телефонной связи и класс перекрывающего сеанса для вызовов преимущественной электросвязи, с тем чтобы обеспечить распределение вплоть до 50% и 70% от общего объема ресурсов на восходящем направлении, соответственно, и оставить оставшиеся 30–50% от общей ширины на восходящем направлении для других услуг, возможно имеющих более низкий приоритет.

В [b-ITU-T J.162] описана основанная на сети сигнализация для вызовов, используемая в IPCablecom между E-MTA и агентом вызовов для создания или удаления соединений. Тогда как при установлении вызова агент вызовов предоставляет идентификатор GateID адаптеру MTA, в отношении сеанса должен использоваться отсутствующий в настоящее время механизм для сообщения адаптеру MTA о желаемом приоритете трафика DOCSIS. Приоритет трафика DOCSIS используется системой CMTS для назначения приоритета трафика в течение периодов перегрузки. В этой области необходимо провести дальнейшие исследования в контексте преимущественной электросвязи.

9 Аутентификация и приоритет в сетях IPCablecom2

9.1 Аутентификация в сетях IPCablecom2

Система IPCablecom2 поддерживает как встроенное, так и отдельное пользовательское оборудование (ПО), которое основано на программном обеспечении и может подключаться к защищенному аппаратному инструменту, такому как смарт-карта. Предполагается, что механизмы аутентификации, существующие в сетях IPCablecom2, будут более разнообразными, а достижение соответствующей аутентификации в сетях IPCablecom2 будет более доступным.

В Дополнении III к [ITU-T J.360] описаны три механизма аутентификации, обеспечиваемые архитектурой IPCablecom2: соглашение об аутентификации и ключе (AKA) IMS, сжатая аутентификация SIP и аутентификация на основе сертификата. Требования к различным компонентам

сетей IPCablecom2 определяются в зависимости от механизма, используемого для аутентификации. Например, для обеспечения сжатой аутентификации необходимо надежно хранить имена пользователей и пароли.

Защита сигнализации между ПО и P-CSCF обеспечивается путем применения IPSec или TLS. В [ITU-T J.360] требуется, чтобы ПО поддерживало согласование для использования протокола TLS. Определены две модели обеспечения защиты по протоколу TLS. Пользовательское оборудование (ПО) и сервер (например, P-CSCF), которые взаимно аутентифицируются с помощью этого протокола, проверяют сертификаты друг друга и аутентификацию со стороны сервера, причем для установления безопасности сигнализации сертификат предоставляется только на стороне сервера. Первая предоставляет более высокий уровень безопасности; в сети IPCablecom2 требуется обеспечение аутентификации на стороне сервера. Может быть желательно рассмотреть взаимную аутентификацию пользовательского оборудования, которое используется для инициирования услуг преимущественной электросвязи.

В сети IPcablecom2 требуется, чтобы установление идентичности абонента выполнялось с помощью функции P-CSCF для обеспечения доставки информации о подлинности пользователя в другие сетевые элементы защищенной сети и удаления идентичности при осуществлении связи с сетевыми элементами незащищенных сетей. Установление и удаление идентичности обеспечивает инициирование услуг преимущественной связи правомочным пользователем.

Требования определены в [b-ITU-T J.262].

9.2 Приоритет в сетях IPCablecom2

Архитектура IPCablecom2, описанная в [ITU-T J.360], основана на инфраструктуре IMS 3GPP. Приоритет возникает в трех местах: при сигнализации IMS, в механизме осуществления и при использовании маркировки пакетов.

9.2.1 Сигнализация приоритета

На уровне сигнализации IMS используются новые заголовки SIP "приоритета ресурса" (Resource-Priority, R-P) и "принятия приоритета ресурса" (Accept-Resource-Priority), определенные в [IETF RFC 4412]. Добавление этих заголовков в сообщениях запроса и ответа, соответственно, позволяет серверам-посредникам SIP и ПО предоставлять запросам приоритетное обслуживание.

В [IETF RFC 4412] определены новые заголовки, называемые приоритетом ресурса (R-P) в сообщениях запроса SIP для запроса приоритетного доступа к ресурсам. Заголовок Accept-Resource-Priority включен в ответ, указывающий значения R-P, которые агент пользователя SIP готов поддерживать. Значения R-P регистрируются в Ассоциации IANA, а заголовок является факультативным полем. Пять пространств имен зарегистрированы Ассоциацией IANA и включены в RFC. В настоящей Рекомендации не предлагается конкретное пространство имен для использования, а дополнительные пространства имен, требуемые для услуг преимущественной электросвязи, могут быть зарегистрированы в соответствии с процедурами, определенными в [IETF RFC 4412]. Применение заголовка R-P обеспечивает сигнализацию приоритета.

Следует отметить, что эти заголовки непосредственно не влияют на поведение IP-маршрутизаторов, связанное с переадресацией. Проводится исследование такой функциональной возможности на сетевом уровне или уровне 3. В [IETF RFC 3690] определены общие требования к системе для предоставления преимущественных услуг в общей области IP-телефонии как сквозного обслуживания. Полезно рассмотреть эти требования в рамках IPCablecom2 для обеспечения преимущественного обслуживания.

9.2.2 Механизм осуществления

На уровне сети доступа при запросе ресурсов сети доступа может использоваться пара значений атрибута (AVP) "приоритета резервирования" (Reservation-Priority). В целях определения характеристик вентиля для резервирования ресурсов функция P-CSCF взаимодействует с администратором приложений IPCablecom2 с использованием интерфейса Rx, определенного в IMS 3GPP. В этом интерфейсе используется протокол Diameter с рядом новых AVP, определенных в спецификации QoS, приведенной в [ITU-T J.368].

Сообщения GateSpec, используемые для запроса и активирования ресурсов сети доступа, включают идентификатор класса сеанса, который определяет уровень приоритета запроса. Тогда как при установлении вызова агент вызовов предоставляет идентификатор GateID адаптеру встроенной цифровой телефонной приставки (E-DVA), в отношении сеанса должен использоваться отсутствующий в настоящее время механизм для сообщения адаптеру E-DVA о желаемом приоритете трафика DOCSIS. Приоритет трафика DOCSIS используется системой CMTS для назначения приоритета трафика в течение периодов перегрузки. В этой области необходимо провести дальнейшие исследования.

В рамках сети доступа может быть назначен приоритет трафика DOCSIS для предоставления приоритетного обслуживания среди различных типов служебных потоков.

Определение конкретных значений, используемых для указания уровней приоритета услуги преимущественной электросвязи, не входит в сферу применения настоящей Рекомендации.

Существуют механизмы для обеспечения приоритетной маршрутизации IP-пакетов в базовой сети, включая сигнализацию SIP и пакетов канала-носителя RTP, однако их определения не включены в настоящую Рекомендацию.

9.2.3 Маркировка

В настоящее время протокол RTP, который является протоколом передачи медиатрафика, используемым в IPCablecom2, не обеспечивает маркировку приоритета.

Подробные требования установлены в [b-ITU-T J.263].

Библиография

[b-ITU-T E.106] Рекомендация МСЭ-Т E.106 (2003 г.), *Международная схема аварийных приоритетов (IEPS) для операций по ликвидации последствий чрезвычайных ситуаций*.

[b-ITU-T J.162] Recommendation ITU-T J.162 (2007), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*.

[b-ITU-T J.262] Recommendation ITU-T J.262 (2009), *Specifications for authentication in preferential telecommunications over IPCablecom2 networks***.**

[b-ITU-T J.263] Recommendation ITU-T J.263 (2009), *Specification for priority in preferential telecommunications over IPCablecom2 networks*.

[b-ITU-T Q-Sup.57] ITU-T Q-series Recommendation Supplement 57 (2008), *Signalling requirements to support the emergency telecommunications service (ETS) in IP networks*.

[b-ITU-T Y.1271] Рекомендация МСЭ-Т Y.1271 (2004 г.), *Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов*.

[b-ITU-T Y.2205] Рекомендация МСЭ-Т Y.2205 (2008 г.), *Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения*.

[b-ITU-T Y.2702] Рекомендация МСЭ-Т Y.2702 (2008 г.), *Требования к аутентификации и авторизации для СПП варианта 1*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3689] IETF RFC 3689 (2004), *General Requirements for Emergency Telecommunication Service (ETS)*.

[b-IETF RFC 3690] IETF RFC 3690 (2004), *IP Telephony Requirements for Emergency Telecommunication Service (ETS)*.

[b-IETF RFC 4190] IETF RFC 4190 (2005), *Framework for Supporting Emergency Telecommunication Services (ETS) in IP Telephony*.

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 протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2010 г.