



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

**МСЭ-Т**

СЕКТОР СТАНДАРТИЗАЦИИ  
ЭЛЕКТРОСВЯЗИ МСЭ

**J.167**

(11/2005)

СЕРИЯ J: Кабельные сети и передача сигналов  
телевизионных и звуковых программ и других  
мультимедийных сигналов

Проект IPCablecom

---

**Требования к подготовке к работе блока  
адаптера медиатерминала (МТА) для  
поставки услуг в режиме реального времени  
по сетям кабельного телевидения с  
использованием кабельных модемов**

Рекомендация МСЭ-Т J.167

---



## **Рекомендация МСЭ-Т J.167**

### **Требования к подготовке к работе блока адаптера медиатерминала (МТА) для поставки услуг в режиме реального времени по сетям кабельного телевидения с использованием кабельных модемов**

#### **Резюме**

В данной Рекомендации описывается процесс инициализации и подготовки к работе устройства блока адаптера медиатерминала (МТА) проекта IPcablecom. Сфера применения данной Рекомендации ограничена подготовкой к работе встроенного блока МТА IPcablecom единственным поставщиком услуг подготовки к работе и управления сетью.

#### **Источник**

Рекомендация МСЭ-Т J.167 утверждена 29 ноября 2005 года 9-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т А.8.

## 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/>.

© ITU 2007

Все права сохранены. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо средств без письменного разрешения МСЭ.

## СОДЕРЖАНИЕ

	Стр.
1	Сфера применения ..... 1
2	Справочные документы ..... 1
3	Термины и определения ..... 2
4	Сокращения и соглашения ..... 2
4.1	Сокращения ..... 2
4.2	Соглашения о терминах ..... 3
5	Введение ..... 3
5.1	Цели предоставления услуги ..... 3
5.2	Цели спецификации ..... 4
5.3	Справочная архитектура IP-Cablecom ..... 5
5.4	Компоненты и интерфейсы ..... 5
6	Обзор подготовки к работе ..... 9
6.1	Подготовка к работе устройства ..... 9
6.2	Подготовка к работе конечной точки ..... 9
6.3	Смена состояний при подготовке к работе ..... 9
6.4	Смена состояний при подготовке к работе с использованием базового и гибридного процессов ..... 10
7	Процессы подготовки к работе ..... 10
7.1	Возвраты, повторы и периоды ожидания ..... 11
7.2	Процессы инициализации встроенного МТА в момент включения ..... 12
7.3	Процесс инициализации встроенного МТА в момент включения (базовый процесс) ..... 20
7.4	Процесс инициализации встроенного МТА в момент включения (гибридный процесс) ..... 22
7.5	Уведомление о завершении подготовки к работе конечных точек ..... 25
7.6	Пошаговая подготовка к работе отдельных конечных точек по завершении подготовки к работе МТА ..... 26
7.7	Отражение состояния интерфейса конечной точки в таблице ifTable ..... 29
7.8	Подготовка к работе коммуникационного канала сигнализации между МТА и CMS ..... 29
7.9	Замена МТА ..... 29
7.10	Временная потеря сигнала ..... 30
7.11	Сценарии полной перезагрузки и частичного сброса МТА ..... 30
8	Опции DHCP ..... 30
8.1	Опция DHCP 122: Опция конфигурации клиента ..... 30
8.2	Опция DHCP 60: Идентификатор производителя клиента ..... 35
8.3	Опции DHCP 12 и 15 ..... 35
8.4	Опция DHCP 6 ..... 35
8.5	Опция DHCP 43 ..... 35
8.6	Опция DHCP 1 ..... 38
8.7	Опция DHCP 3 ..... 38

	<b>Стр.</b>
9	Подготавливаемые к работе атрибуты МТА ..... 38
9.1	Файл конфигурации МТА..... 38
10	Технические возможности устройства МТА..... 53
10.1	Версия IPCablecom ..... 54
10.2	Количество конечных точек телефонии ..... 54
10.3	Поддержка TGT ..... 54
10.4	Поддержка метода доступа HTTP для загрузки файлов ..... 54
10.5	Поддержка уведомления SYSLOG о событии МТА24 ..... 54
10.6	Поддержка процесса обслуживания NCS..... 54
10.7	Поддержка первичной линии ..... 55
10.8	Тип(ы) TLV, определяемые производителем..... 55
10.9	Поддержка хранения мандатов/информации о мандатах в энергонезависимой памяти NVRAM ..... 55
10.10	Поддержка отправки отчета о подготовке к работе ..... 55
10.11	Поддерживаемые кодеки (CODEC(s)) ..... 55
10.12	Поддержка подавления тишины..... 56
10.13	Поддержка устранения эффекта "эхо" ..... 56
10.14	Поддержка RSVP (Resource Reservation Protocol, протокол резервирования ресурсов)..... 56
10.15	Поддержка UGS-AD (Unsolicited Grant Service with Activity Detection) (Услуга предоставления канала с обнаружением активности) ..... 56
10.16	Начальный номер "ifIndex" МТА в таблице "ifTable" ..... 56
10.17	Поддержка ведения журнала событий процесса подготовки к работе..... 56
10.18	Поддерживаемые процессы подготовки к работе ..... 57
10.19	Поддержка версии T38 ..... 57
10.20	Поддержка коррекции ошибок T38..... 57
10.21	Поддержка RFC 2833 DTMF..... 58
10.22	Поддержка голосовых параметров..... 58
10.23	Поддержка MIB устройства..... 58
10.24	Поддержка множественного предоставления канала в течение одного интервала (MGPI) ..... 60
11	Спецификация TLV-38 приемника уведомлений SNMP..... 60
11.1	Вложенные TLV TLV-38..... 60
11.2	Соответствие полей TLV таблицам SNMP ..... 62
11.3	Пример конфигурации TLV-38 и TLV-11 ..... 68
12	Требования к управлению SNMPv2c ..... 72
12.1	Содержимое таблиц, созданное МТА после шага МТА4 в ходе выполнения гибридного и базового процессов в режиме сосуществования SNMPv2c ..... 73
12.2	Значения SNMP по умолчанию для доступа SNMPv2..... 74
13	Поддержка отправки отчетов о влиянии перебоев в оказании услуг и прочих расширенных возможностей..... 76
13.1	Поддержка требований eDOCSIS..... 76
13.2	Расширение MIB IPCablecom ..... 76

	<b>Стр.</b>
13.3 MIB резервного питания .....	77
13.4 MIB SYSLOG .....	77
13.5 Обнаружение чужеродного потенциала .....	77
Дополнение I – Пример конфигурации для случая сосуществования SNMPv2c – Шаблон для поставщиков услуг .....	78



## Рекомендация МСЭ-Т J.167

### Требования к подготовке к работе блока адаптера медиатерминала (МТА) для поставки услуг в режиме реального времени по сетям кабельного телевидения с использованием кабельных модемов

#### 1 Сфера применения

В данной Рекомендации описывается подготовка к работе и инициализация блока адаптера медиатерминала (МТА) проекта IPCom. Сфера применения данной Рекомендации ограничена подготовкой к работе встроенного блока МТА IPCom единственным поставщиком услуг подготовки к работе и управления сетью.

#### 2 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 даёт ему, как отдельному документу, статуса рекомендации.

- ITU-T Recommendation J.83 (1997), *Digital multi-programme systems for television, sound and data services for cable distribution.*
- ITU-T Recommendation J.112 Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification.*
- ITU-T Recommendation J.162 (2005), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems.*
- ITU-T Recommendation J.166 (2005)\*, *IPCom Management Information Base (MIB) framework.*
- ITU-T Recommendation J.170 (2005), *IPCom security specification.*
- IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol.*
- IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions.*
- IETF RFC 2475 (1998), *An Architecture for Differentiated Services.*
- IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1.*
- IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals.*
- IETF RFC 2863 (2000), *The Interfaces Group MIB.*
- IETF RFC 3396 (2002), *Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4).*
- IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework.*
- IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.*
- IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).*

---

\* Заменяет Рек. МСЭ-Т J.166 (2001 г.), J.168 (2001 г.), J.169 (2001 г.) и J.176 (2002 г.).

- IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.
- IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.
- IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.
- IETF RFC 3495 (2003), *Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration*.
- IETF RFC 3584 (2003), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.
- IETF RFC 3594 (2003), *PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option*.
- IETF RFC 3617 (2003), *Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP)*.

### 3 Термины и определения

В данной Рекомендации определены следующие термины:

**3.1 кабельный модем:** Кабельный модем представляет собой оконечное устройство второго уровня, которое завершает соединение со стороны заказчика в соответствии с Рекомендацией J.112

**3.2 IPCablecom:** Проект МСЭ-Т, в который включены архитектура и серия Рекомендаций, делающие возможным поставку услуг в режиме реального времени (таких как телефонная связь) по сети кабельного телевидения с использованием кабельных модемов.

### 4 Сокращения и соглашения

#### 4.1 Сокращения

В данной Рекомендации используются следующие сокращения:

CM	Cable Modem	Кабельный модем	
CMS	Call Management Server	Сервер управления вызовами	
CPE	Customer Premises Equipment	Оборудование в помещении клиента	
DHCP	Dynamic Host Configuration Protocol	Протокол динамического конфигурирования узла	
DNS	Domain Name System	Доменная система имен	
FQDN	Fully Qualified Domain Name	Полное доменное имя узла	
HTTP	HyperText Transfer Protocol	Протокол передачи гипертекста	
IP	Internet Protocol	Протокол Интернет	
IPSec	Internet Protocol Security	Протокол безопасности Интернет	
MAC	Media Access Control	Управление доступом к среде	
MTA	Media Terminal Adapter	Адаптер медиатерминала	
PSTN	Public Switched Telephone Network	Коммутируемая телефонная сеть общего пользования	КТСОП
SNMP	Simple Network Management Protocol	Простой протокол управления сетью	
TFTP	Trivial File Transfer Protocol	Тривиальный протокол передачи файлов	
TGS	Ticket Granting Server	Сервер предоставления мандата	

## 4.2 Соглашения о терминах

Применение данной Рекомендации не является обязательным. В случаях ее применения, такие ключевые слова как "ДОЛЖЕН", "СЛЕДУЕТ" и "ТРЕБУЕТСЯ" следует понимать как указывающее на обязательную сторону настоящей Рекомендации. Используемые в тексте данной Рекомендации ключевые слова, которые указывают на определенный уровень значимости специфических требований, приведены ниже:

- "ДОЛЖЕН" Данное слово, наречие "НЕОБХОДИМО" или глагол "ТРЕБУЕТСЯ" означает, что данное условие является абсолютным требованием этой Рекомендации.
- "НЕ ДОЛЖЕН" Данное словосочетание означает, что на данное условие этой Рекомендацией налагается абсолютный запрет.
- "СЛЕДУЕТ" Данное слово или глагол "РЕКОМЕНДУЕТСЯ" означает, что могут существовать веские условия при определенных обстоятельствах, в которых данное условие можно игнорировать, но перед тем, как выбрать другой вариант, необходимо получить полное понимание последствий и тщательно взвесить ситуацию.
- "НЕ СЛЕДУЕТ" Данное словосочетание означает, что могут существовать веские условия при определенных обстоятельствах, в которых описанный образ действий приемлем или даже полезен, но перед тем, как выполнить действия, отмеченные этим обозначением, необходимо получить полное понимание последствий и тщательно взвесить ситуацию.
- "МОЖЕТ" Данное слово или наречия "МОЖНО", "НЕОБЯЗАТЕЛЬНО" означает, что данное условие является необязательным. Один поставщик вправе использовать его, потому что этого будет требовать рыночная ситуация или, например, это приведет к улучшению продукта, а другой поставщик может опустить это условие.

## 5 Введение

### 5.1 Цели предоставления услуги

Операторы кабельного телевидения заинтересованы в развертывании высокоскоростных информационных систем связи с использованием кабельных телевизионных сетей. Предполагаемая услуга делает возможными телефонную связь, видео и информационные услуги, основанные на двунаправленной передаче IP-трафика, между головным узлом кабельной системы и местоположением клиента, по коаксиальной или оптоволоконно-коаксиальной (HFC) кабельной сети, как определено в Рек. МСЭ-Т J.83 и J.112. В упрощенной форме этот процесс представлен на рисунке 1.

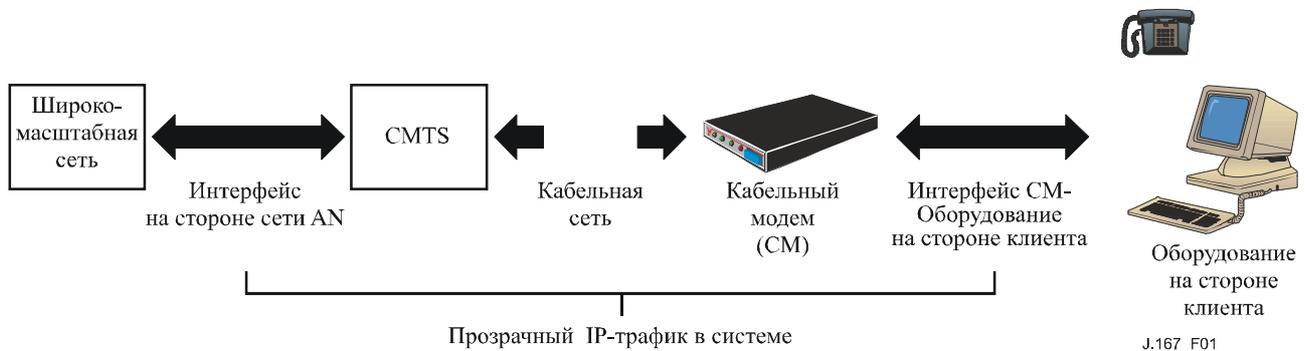


Рисунок 1/J.167 – Прозрачный IP-трафик в системе передачи данных по кабельным сетям

Канал передачи по кабельной системе реализуется системой завершения (CMTS) кабельного модема в головном узле и кабельным модемом (CM) в местоположении каждого клиента. Основной целью здесь является обеспечение возможности операторам прозрачно передавать IP-трафик между данными интерфейсами.

## 5.2 Цели спецификации

Ниже представлены требования, важные для подготовки к работе устройства:

- Полная подготовка к работе и управление одним физическим устройством (например, встроенным МТА) должны производиться одной коммерческой структурой. Этот поставщик может дополнительно устанавливать деловые отношения с другими поставщиками для оказания таких услуг, как обмен данными, телефонная связь, а также других услуг.
- Встроенный МТА представляет собой МТА IPcablecom, объединенный с CM. Для подготовки к работе встроенного МТА ДОЛЖНЫ быть выполнены шаги как по подготовке к работе CM, так и по подготовке к работе устройства IPcablecom. Встроенный МТА ДОЛЖЕН иметь два IP-адреса: IP-адрес CM, и отличный от него IP-адрес МТА. Встроенный МТА ДОЛЖЕН иметь два MAC-адреса: MAC-адрес CM и отличный от него MAC-адрес МТА. Более того, МТА ДОЛЖЕН работать вне зависимости от того, в одной или разных подсетях он находится с CM.
- Требованием проекта IPcablecom является наличие уникального FQDN для МТА-компонента во встроенном МТА. Это FQDN ДОЛЖНО включаться в сообщения DHCP OFFER и DHCP ACK для МТА-компонента. В рамках проекта IPcablecom не предъявляется дополнительных требований к FQDN для CM во встроенном МТА, кроме описанных в Рек. МСЭ-Т J.112. Преобразование FQDN в IP-адрес ДОЛЖНО осуществляться на сетевом сервере DNS и быть доступным для остальной сети.
- При подготовке к работе встроенного МТА IPcablecom ДОЛЖНЫ быть использованы Опции 12 и 15 DHCP для передачи FQDN МТА к E-МТА.
- Подготовка к работе встроенного МТА IPcablecom ДОЛЖНА поддерживать два отдельных файла конфигурации: файл конфигурации, описанный в Рек. МСЭ-Т J.112 для CM-компонента, и файл конфигурации, соответствующий стандартам IPcablecom для МТА.
- Встроенный МТА находится вне сетевой "границы доверия" IPcablecom, как определено в Рек. J.160 по архитектуре IPcablecom.
- IPcablecom ДОЛЖЕН поддерживать загрузку программного обеспечения DOCSIS 1.1 (Рек. МСЭ-Т J.112) или DOCSIS 2.0 (Рек. МСЭ-Т J.122), что определено Рек. МСЭ-Т J.112. Процесс загрузки программного обеспечения DOCSIS 1.1 или DOCSIS 2.0 поддерживает загрузку одного файла для кабельного модема или встроенного МТА. Одна и та же загрузка программного обеспечения DOCSIS 1.1 или DOCSIS 2.0 ДОЛЖНА использоваться для модернизации кода как программного обеспечения DOCSIS, так и IPcablecom.
- В рамках проекта IPcablecom при использовании протокола SNMPv2c (простой протокол управления сетью) в операциях управления сетью ДОЛЖНО поддерживаться сосуществование устройств, работающих в соответствии с базовым процессом подготовки к работе и гибридным процессом подготовки к работе, а при использовании протокола SNMPv3/v2 – сосуществование устройств, работающих в соответствии с защищенным процессом подготовки к работе.
- Подготовка к работе встроенного МТА IPcablecom сводит к минимуму влияние на сетевые устройства, описанные в Рек. МСЭ-Т J.112/J.122 (CM и CMTS (Завершающая система кабельных модемов)).  
Предпочтительными являются стандартные серверные решения (TFTP, SNMP, DNS и т. д.). При этом следует понимать, что для координации обеспечения работы встроенного МТА IPcablecom с использованием этих протоколов могут потребоваться определенные действия на уровне приложений.
- Где необходимо, поддерживаются протоколы управления, описанные в Рек. J.112/J.122 (SNMP, DHCP, TFTP).

### 5.3 Справочная архитектура IPCablecom

На рисунке 2 представлена справочная архитектура сети IPCablecom. Более подробная информация о справочной архитектуре сети IPCablecom содержится в Рекомендации МСЭ-Т J.160.

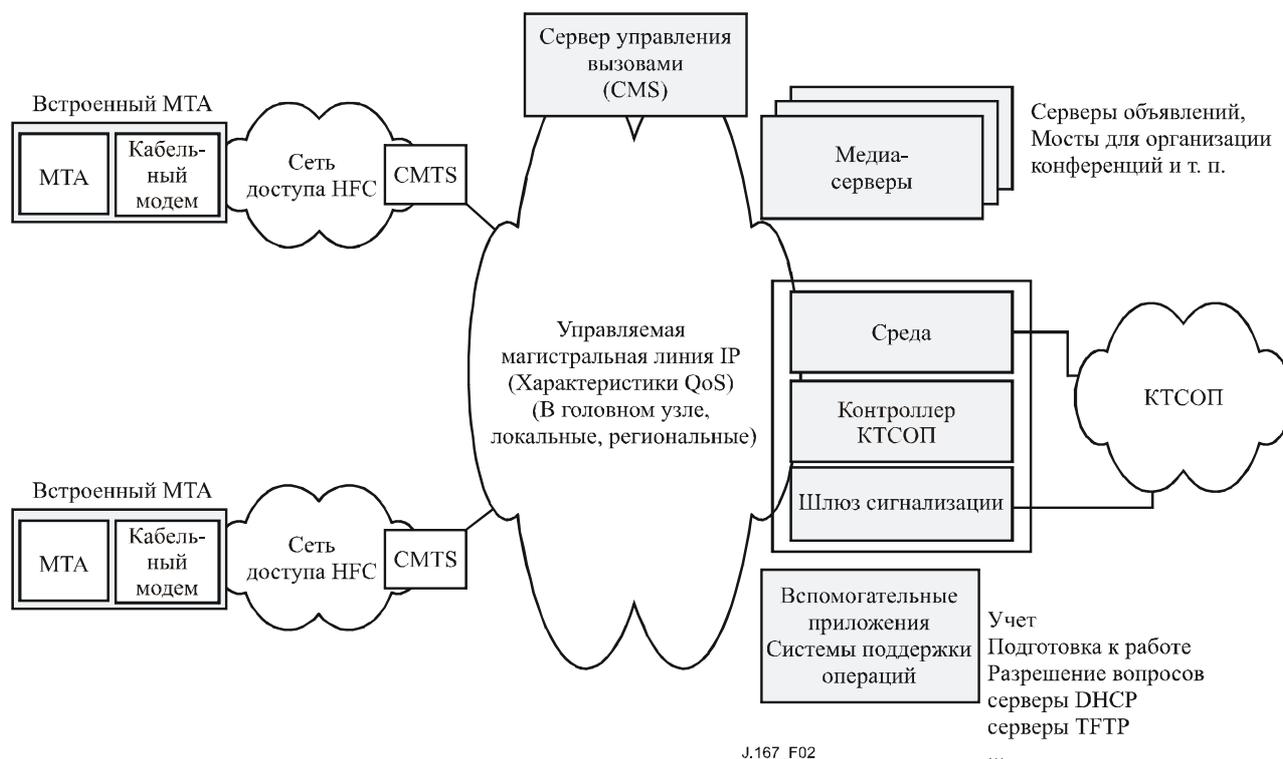


Рисунок 2/J.167 – Справочная модель сетевых компонентов IPCablecom (частичная)

### 5.4 Компоненты и интерфейсы.

Базовая справочная архитектура подготовки к работе встроенного МТА IPCablecom показана на рисунке 3. На данном рисунке представлены основные компоненты и интерфейсы, обсуждаемые в рамках настоящей Рекомендации.

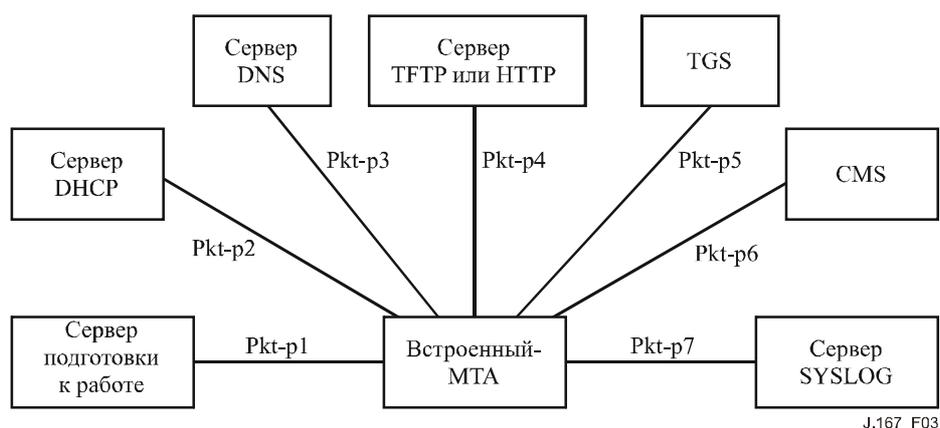


Рисунок 3/J.167 – Интерфейсы подготовки к работе IPCablecom

#### 5.4.1 МТА

При подготовке к работе МТА ДОЛЖНЫ выполняться требования, приведенные ниже.

##### 5.4.1.1 Требования к защите МТА

При подготовке к работе МТА ДОЛЖНЫ выполняться следующие требования:

- Структура MIB (информационная база управления) устройства MTA приспособлена для представления соответствий между конечными точками MTA и CMS. Более подробная информация о защищенном соединении между MTA и CMS содержится в Рек. МСЭ-Т J.170.
- Основное наименование Kerberos CMS не содержится в явном виде в конечных точках MTA. MTA ДОЛЖЕН иметь возможность определять основное наименование Kerberos CMS, базируясь на FQDN CMS, как указано в Рек. МСЭ-Т J.170.
- Для каждой установленной для конечной точки уникальной пары "Основное наименование Kerberos CMS/Область Kerberos", MTA ДОЛЖЕН получить единый мандат Kerberos согласно Рек. МСЭ-Т J.170.
- Если MTA уже содержит действительный мандат Kerberos для данного CMS, то MTA НЕ ДОЛЖЕН запрашивать дополнительный мандат Kerberos для данного CMS. (До тех пор, пока окончание срока действия текущего мандата Kerberos  $\leq$  текущее время + "льготный период" (Grace Period) PKINIT). По наступлении этого момента MTA ДОЛЖЕН получить новый мандат для данного CMS.
- В том случае, если происходит преобразование FQDN CMS в несколько IP-адресов, MTA первоначально ДОЛЖЕН установить защищенное соединение по протоколу IPSec с одним из IP-адресов, возвращенных сервером DNS. MTA МОЖЕТ также первоначально установить защищенные соединения по протоколу IPSec с дополнительными IP-адресами CMS. Более подробная информация содержится в Рек. МСЭ-Т J.170.
- Если MTA уже установлено защищенное соединение (входящее или исходящее) с определенным IP-адресом CMS, MTA НЕ ДОЛЖЕН пытаться установить дополнительные защищенные соединения с тем же IP-адресом.

В процессе подготовки к работе не предъявляется особых требований по защите для базового (Basic Flow) или гибридного процессов (Hybrid Flow).

#### 5.4.1.2 Требования SNMP к MTA

В процессе подготовки к работе в соответствии с защищенным процессом (Secure Flow) MTA ДОЛЖЕН соответствовать приведенным ниже требованиям протокола SNMPv3:

- Обеспечение защиты MTA в SNMPv3 осуществляется отдельно от обеспечения защиты CM в SNMPv3. Информация безопасности USM (модель защиты, определенная пользователем) (аутентификация и ключи секретности, а также другие позиции таблицы USM) настраивается отдельно.
- Инициализация SNMPv3 ДОЛЖНА быть завершена перед информированием о регистрации подготовки к работе.
- Во время работы в соответствии с защищенным процессом, MTA ДОЛЖЕН поддерживать управление устройствами, основанное на SNMPv3 и SNMPv2, как определено в RFC 3414 и RFC 3584.

В процессе подготовки к работе в соответствии с базовым или гибридным процессами MTA ДОЛЖЕН соответствовать приведенным ниже требованиям протокола SNMPv2:

- Инициализация SNMPv2с должна быть завершена немедленно после фазы DHCP.

Управление устройствами, основанное на SNMPv2с, описано в RFC 3584.

#### 5.4.2 Сервер подготовки к работе

Сервер подготовки к работе состоит из следующих компонентов:

- Приложение подготовки к работе – С помощью приложения подготовки к работе обеспечивается координация процесса подготовки к работе встроенного MTA. У этого приложения имеется связанный модуль SNMP.
- Модуль подготовки к работе SNMP – Модуль подготовки к работе SNMP ДОЛЖЕН включать обработчик прерываний/информационных сообщений для регистрации подготовки к работе и статуса подготовки к работе, а также механизм SNMP для получения информации о возможностях устройства и установки имени файла данных конфигурации и метода

доступа. Для получения информации об атрибутах МТА, доступных MIB, см. Рек. МСЭ-Т J.160 (MIB МТА).

Интерфейс между приложением подготовки к работе и связанным модулем SNMP не задан в рамках IP-Cablecom и реализуется поставщиком. Интерфейс между сервером подготовки к работе и сервером TFTP не задан в рамках IP-Cablecom и реализуется поставщиком.

#### **5.4.3 Интерфейс МТА – Сервер Syslog**

В устройствах МТА IP-Cablecom ДОЛЖЕН быть реализован механизм управления событиями (MEM), как описано в Рек. МСЭ-Т J.172. Кроме этого, устройство МТА должно включать MEM MIB, как определено Рек. МСЭ-Т J.166, предусматривающую поддержку сервера Syslog.

В устройствах МТА IP-Cablecom также ДОЛЖНЫ быть реализованы все события управления подготовкой к работе (Provisioning Management Events) IP-Cablecom, описанные в Приложении A/J.172.

#### **5.4.4 Интерфейс МТА – Сервер DHCP**

Использование данного интерфейса предъявляет особые требования к серверу DHCP и клиенту при присвоении IP-адресов в ходе процесса инициализации МТА:

- И сервер DHCP и встроенный МТА ДОЛЖНЫ поддерживать коды опций 6, 7, 12, 15, 43, 60 DHCP и код опции 122 DHCP (что определено в RFC 2132). Коды опций 12 (Имя Хоста) и 15 (Доменное имя) ДОЛЖНЫ образовывать Полное доменное имя узла и ДОЛЖНЫ быть доступны для получения сервером DNS.
- Сервер DHCP ДОЛЖЕН принимать ширококвотельные и одноадресные сообщения от клиента DHCP МТА согласно RFC 3396.
- Сервер DHCP ДОЛЖЕН включать заданный FQDN МТА в сообщения DHCP OFFER и DHCP ACK, передаваемые компоненту МТА встроенного МТА. Более подробная информация о сообщении DHCP OFFER содержится в RFC 2131.

#### **5.4.5 Интерфейс МТА – Приложение подготовки к работе**

Этот интерфейс служит для распознавания особых требований для приложения подготовки к работе, что необходимо для инициализации и регистрации МТА. Требования к приложению подготовки к работе приведены ниже:

- МТА ДОЛЖЕН формировать коррелирующий идентификационный номер – произвольное значение, являющееся частью информации о функциональных возможностях устройства, которая будет использоваться для обмена с приложением подготовки к работе. Это значение используется как идентификатор для сопоставления связанных событий при подготовке к работе МТА.
- Приложение подготовки к работе ДОЛЖНО предоставлять МТА файл данных конфигурации МТА. Файл данных конфигурации МТА создается специально для МТА-компонента встроенного МТА и не зависит от файла данных конфигурации CM-компонента.
- Файл данных конфигурации МТА создается в двоичном TLV-формате (Type-Length-Value), приспособленном для передачи при помощи заданного TFTP или HTTP метода доступа.
- Приложение подготовки к работе ДОЛЖНО иметь возможность конфигурирования МТА для работы с различными поставщиками услуг передачи данных и голосовой связи.
- Приложение подготовки к работе ДОЛЖНО использовать только SNMPv3 при подготовке к работе устройств с применением защищенного процесса. Поддержка базового и гибридного процессов является необязательной для приложения подготовки к работе. Если базовый и гибридный процессы поддерживаются, приложение подготовки к работе ДОЛЖНО использовать только SNMPv2c для подготовки к работе устройств с применением базового или гибридного процессов.
- В приложении подготовки к работе ДОЛЖНЫ использоваться SNMPv3 и SNMPv2 для управления устройствами.
- Приложение подготовки к работе ДОЛЖНО поддерживать онлайн-пошаговую подготовку к работе устройства/абонента с использованием SNMP.

- Все Характеристики МТА ДОЛЖНЫ быть указаны в Опции-60 DHCP в соответствии с пунктом 10.
- Приложением подготовки к работе НЕ ДОЛЖНЫ предусматриваться какие-либо Характеристики, не имеющие значений по умолчанию. В случае, если характеристики, предоставляемые МТА не согласуются в формате и/или числе и/или значениях, приложение подготовки к работе ДОЛЖНО использовать другие средства для идентификации характеристик МТА (например, SNMPv3 если возможно).

#### 5.4.6 Интерфейс МТА–СМS

Сигнализация является основным интерфейсом между МТА и СМS. Для получения более подробного описания данного интерфейса см. Рек. МСЭ-Т J.162 по сигнализации IPcablecom.

- СМS ДОЛЖЕН принимать сигнализацию и запросы канала-носителя от МТА с которым установлено активное защищенное соединение.
- СМS НЕ ДОЛЖЕН принимать сигнализацию и запросы канала-носителя от МТА, с которым не установлено активное защищенное соединение за исключением случаев, когда это предписывается информацией, содержащейся в объекте "pktsMtaDevCmslPsecCtrl" МIВ.

#### 5.4.7 Интерфейс МТА – Сервер защиты (KDC)

Интерфейс между МТА и Центром распределения ключей (KDC) ДОЛЖЕН соответствовать требованиям спецификации защиты IPcablecom, приведенным в Рек. МСЭ-Т J.170.

Механизм возврата и повторного запуска обмена AP-REQ/REP передачи ключа SNMPv3 с использованием Kerberos, определенный в Рек. МСЭ-Т J.170 управляется значениями, приводимыми в опции DHCP 122, подопции 5 (см. п. 8.14).

Механизм возврата и повторного запуска обмена AS-REQ/REP передачи ключа SNMPv3 с использованием Kerberos, определенный в Рек. МСЭ-Т J.170 управляется значениями, приводимыми в опции DHCP 122, подопции 4 (см. п. 8.13) или значениями по умолчанию соответствующих объектов МIВ из таблицы области в случае, если подопция 4 отсутствует в опции DHCP 122.

#### 5.4.8 МТА и доступ к файлу данных конфигурации

Данная Рекомендация предусматривает несколько методов доступа для загрузки файла данных конфигурации в МТА:

- МТА ДОЛЖЕН поддерживать метод доступа TFTP для загрузки файла данных конфигурации МТА.
- МТА МОЖЕТ поддерживать метод доступа HTTP для загрузки файла данных конфигурации МТА.
- Сервер подготовки к работе ДОЛЖЕН предоставить МТА адрес сервера TFTP/HTTP в формате URL и имя файла конфигурации при помощи команды SET SNMPv3 в случае использования защищенного процесса. Сервер подготовки к работе ДОЛЖЕН предоставить МТА адрес сервера TFTP/HTTP в формате URL и имя файла конфигурации при помощи команды SET SNMPv2 в случае, если он поддерживает гибридный процесс. При использовании базового процесса применения команды SET SNMPv2 не требуется; сервер подготовки к работе ДОЛЖЕН предоставить МТА адрес сервера TFTP/HTTP в полях "file" и "siaddr" DHCP в случае, если он поддерживает режим подготовки к работе с использованием базового процесса. Для получения дополнительной информации см. п. 7.3.

#### 5.4.9 Расширения DOCSIS для подготовки к работе МТА

Данная Рекомендация содержит требования по поддержке следующих дополнений к процессам DOCSIS для автоматической подготовки к работе МТА:

- Новый код опции 122 DHCP и связанные процедуры ДОЛЖНЫ быть реализованы в DOCSIS.

## **6 Обзор подготовки к работе**

Подготовка к работе является частью процесса управления конфигурацией. Подготовка к работе включает, помимо прочего, определение конфигурируемых атрибутов данных, управление заданными значениями атрибутов, инициализацию и регистрацию ресурсов, управление программным обеспечением ресурсов и выдачу отчетов о данных конфигурации. Термин ресурс (или управляемый ресурс) всегда употребляется применительно к устройству МТА. Далее соответствующий абонент также будет обозначаться как "управляемый ресурс".

### **6.1 Подготовка к работе устройства**

Подготовкой к работе устройства называется процесс, в ходе которого встроенный МТА конфигурируется для поддержки услуг голосовой связи.

Подготовка к работе устройства включает получение МТА его IP-конфигурации, необходимой работы в сети, регистрацию его в сети и загрузку данных конфигурации с сервера подготовки к работе.

В случае, если подготовка к работе устройства происходит с использованием "защищенного процесса", МТА ДОЛЖЕН иметь возможность проверить подлинность файла конфигурации, загружаемого с сервера. Файл конфигурации, сформированный с использованием "защищенного процесса" является "подписанным" и может быть "запечатан". Более подробная информация содержится в Рек. МСЭ-Т J.170.

Информация о правилах подготовки к работе, связанных с защищенными соединениями, приведена в п. 5.4.1.

В случае, если подготовка к работе устройства происходит с использованием базового или гибридного процессов, МТА ДОЛЖЕН осуществлять проверку целостности содержимого файла конфигурации. Более подробная информация содержится в п. 9.1.

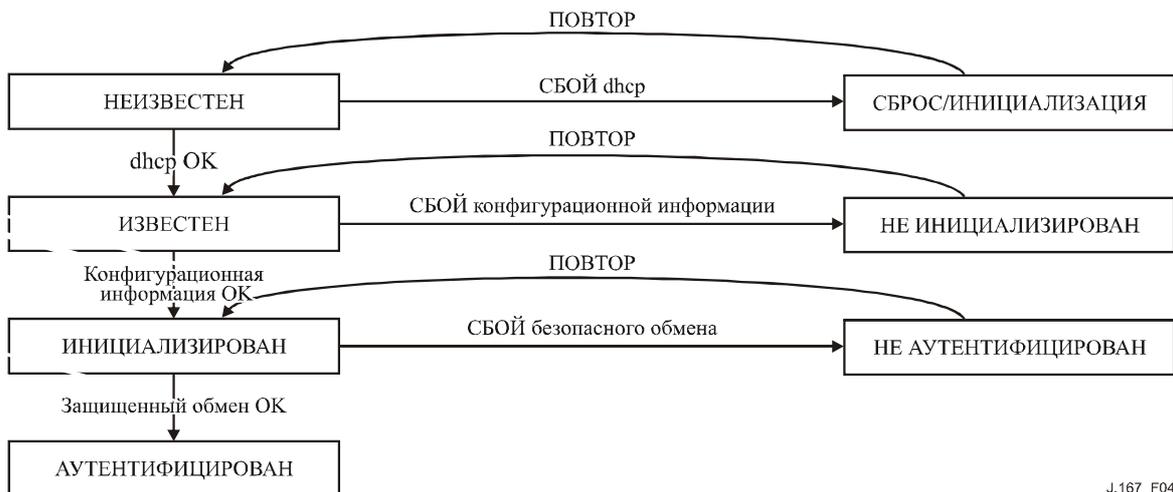
### **6.2 Подготовка к работе конечной точки**

Подготовка к работе конечной точки представляет собой процесс, в ходе которого подготавливаемый к работе МТА аутентифицируется на CMS и устанавливает защищенное соединение с этим сервером. Таким образом, последующая сигнализация вызова защищена посредством установленного защищенного соединения.

МТА ДОЛЖЕН следовать требованиям спецификации безопасности IP-Cablecom (Рек. МСЭ-Т J.170), вне зависимости от типа процесса, в соответствии с которым происходила подготовка к работе МТА (защищенный, гибридный или базовый).

### **6.3 Смена состояний при подготовке к работе**

На рисунке 4 представлены логические состояния устройства и возможные переходы между этими логическими состояниями. Данное представление приведено только в демонстративных целях и не отражает реальной реализации данного процесса. Приведенные ниже переходы между состояниями МТА не показывают реального количества повторных попыток или реальных значений периодов ожидания перед повторами:

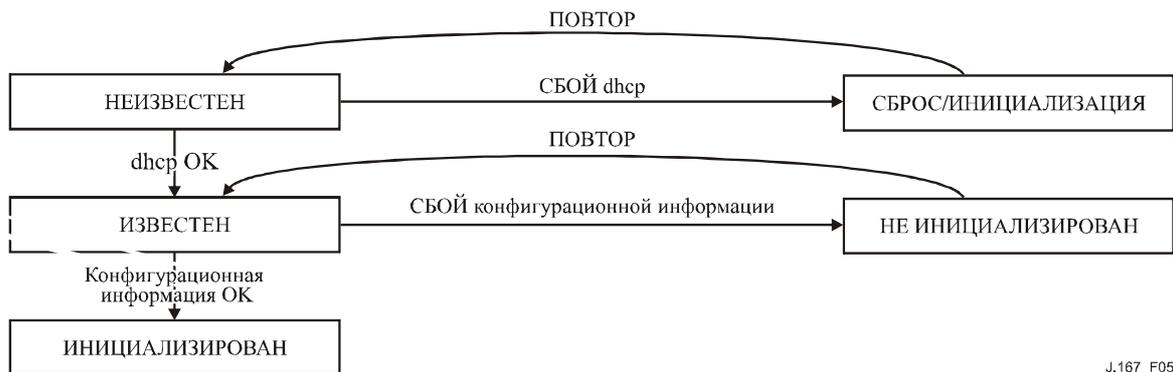


J.167\_F04

**Рисунок 4/J.167 – Состояния устройства и их смена при подготовке к работе с использованием защищенного процесса**

#### 6.4 Смена состояний при подготовке к работе с использованием базового и гибридного процессов

На рисунке 5 представлены логические состояния устройства и возможные переходы между этими логическими состояниями. Данное представление приведено только в демонстративных целях и не отражает реальной реализации данного процесса. Приведенные ниже переходы между состояниями МТА не показывают реального количества повторных попыток или реальных значений периодов ожидания перед повторами:



J.167\_F05

**Рисунок 5/J.167 – Состояния устройства и их смена в процессе подготовки к работе с использованием базового или гибридного процессов**

### 7 Процессы подготовки к работе

Подготовка к работе МТА IPCablecom происходит с использованием одного из 3 процессов подготовки к работе:

- Защищенный процесс поддерживает взаимную аутентификацию Kerberos между МТА и системой подготовки к работе, а также обмен SNMPv3-сообщениями с использованием Kerberos. Устройства МТА IPCablecom и приложения подготовки к работе ДОЛЖНЫ поддерживать использование защищенного процесса.
- Базовый процесс представляет собой упрощенный процесс подготовки к работе образца DOCSIS без использования систем безопасности Kerberos или SNMPv3, а также без регистрации SNMP при помощи SNMP INFORM. Устройствам МТА IPCablecom и приложениям подготовки к работе СЛЕДУЕТ поддерживать использование базового процесса.
- Гибридный процесс в целом представляет собой защищенный процесс с отключенной службой обмена сообщениями Kerberos и SNMPv3 вместо SNMPv2c. Устройствам МТА IPCablecom и приложениям подготовки к работе СЛЕДУЕТ поддерживать использование гибридного процесса.

Любое упоминание SNMP в данной Рекомендации без специальной ссылки на версию протокола SNMP нужно трактовать следующим образом:

- При использовании защищенного процесса, МТА ДОЛЖЕН поддерживать 'только SNMPv3' для процесса подготовки к работе и сосуществование протоколов SNMPv3/v2c для управления сетью и/или отслеживания состояния сети. Сосуществование протоколов SNMPv3/v2c ДОЛЖНО поддерживаться и конфигурироваться с использованием значений TLV-38 или TLV-11 и TLV-64 в файле конфигурации МТА.
- При использовании гибридного или базового процессов, МТА ДОЛЖЕН поддерживать SNMPv2c для подготовки к работе, управления сетью и/или отслеживания состояния сети. Поддержка уровня доступа SNMPv2c ДОЛЖНА осуществляться согласно значениям TLV-38 или TLV-11 и TLV-64 в файле конфигурации МТА.

МТА также может быть сконфигурирован для работы с другими целевыми объектами SNMPv2c при помощи использования значений TLV-38 или TLV-11 и TLV-64 в файле конфигурации МТА.

Команда МТА на запуск определенного процесса инициализации передается при помощи опции DHCP 122 подопции 6, как описано в п. 8.1.5. Каждый из этих процессов начинается с общего для всех типов процессов набора стандартных шагов.

### 7.1 Возвраты, повторы и периоды ожидания

Механизмы возврата делают возможным прерывание регистрации устройства в сети в условиях обычной или общей регистрации, когда запросы клиента МТА не обрабатываются в течение заданного протоколом периода ожидания. Детальное описание подготовки к работе в условиях общей регистрации выходит за рамки IPsec; тем не менее, в данном пункте представлены следующие рекомендации и требования:

- Прерывание регистрации МОЖЕТ базироваться на регистрации CM DOCSIS.
- МТА ДОЛЖЕН использовать механизмы периодов ожидания и повторов, указанные в спецификации DHCP (RFC 2131) и HTTP. Рекомендуется следовать указаниям IETF RFC 3413 для механизмов периодов ожидания и повторного запуска SNMP.
- МТА ДОЛЖЕН использовать адаптивные периоды ожидания для TFTP, как указано в DOCSIS (Рек. МСЭ-Т J.112/J.122).
- МТА ДОЛЖЕН соответствовать рекомендациям по применению возвратов и повторов, описанным в спецификации безопасности (Рек. МСЭ-Т J.170) для защищенных процессов.
- Все процессы подготовки к работе (защищенный, базовый и гибридный) описаны в пунктах 7.2, 7.3 и 7.4.
  - Датчик времени подготовки к работе ДОЛЖЕН начинать работу сразу после получения DHCP ACK и ДОЛЖЕН заканчивать работу в момент завершения ответа файла конфигурации TFTP/HTTP.
  - В случае, если датчик времени подготовки к работе закончит работу до завершения ответа файла конфигурации TFTP/HTTP, МТА ДОЛЖЕН вернуться к шагу МТА1.
  - МТА НЕ ДОЛЖЕН ждать, пока датчик времени подготовки к работе завершит работу в случае, если необходимо предпринять какие-либо действия в связи с возникновением сбоя на каком-либо шаге. Например, для защищенного процесса, если происходит сбой на шаге МТА19, МТА не должен ждать, пока датчик времени подготовки к работе завершит работу, а в момент обнаружения сбоя сразу должен вернуться к шагу МТА1.
- В случае использования защищенного процесса подготовки к работе – если сбой происходит на любом из шагов, связанных с PROV\_SNMP\_ENTITY (модуль инициализации SNMP) (МТА13, МТА14, МТА15, МТА19) до того, как МТА получит файл конфигурации устройства – и МТА получил несколько IP-адресов для PROV\_SNMP\_ENTITY (модуль инициализации SNMP) (FQDN, полученный в подопции 3 Опции 122), тогда перед возвратом к шагу МТА1 он ДОЛЖЕН повторить шаги со всеми полученными IP-адресами, если иное не предписывается Рек. МСЭ-Т J.170. Тем не менее, следует отметить, что тот полученный IP-адрес, который выберет МТА для использования в шаге МТА13, он ДОЛЖЕН использовать и в шагах МТА15 и МТА25.
- В случае использования гибридного процесса подготовки к работе – если сбой происходит на любом из шагов, связанных с PROV\_SNMP\_ENTITY (H-МТА15, H-МТА19), до того, как МТА получит файл конфигурации устройства – и МТА получил несколько IP-адресов для PROV\_SNMP\_ENTITY (FQDN, полученный в подопции 3 Опции 122), тогда перед

возвратом к шагу МТА1 он ДОЛЖЕН повторить шаги со всеми полученными IP-адресами. Тем не менее, следует отметить, что тот полученный IP-адрес, который выберет МТА для шага Н-МТА15, он ДОЛЖЕН использовать и в шаге Н-МТА25.

## 7.2 Процессы инициализации встроенного МТА в момент включения

В таблице 1 представлен обязательный процесс сообщений, которому ДОЛЖЕН следовать встроенный МТА в процессе инициализации в момент включения (если иное не предписано в явном виде). Следует понимать, что эти процессы не предполагают точного выполнения и не ограничивают функциональные возможности.

Хотя в данных процессах представлен процесс загрузки файла конфигурации МТА с сервера TFTP, текстовые описания уточняют требования для поддержки загрузки файла конфигурации МТА с сервера HTTP.

Следует отметить, что на приведенной ниже подробной схеме процесса некоторые шаги могут вызвать появление цикла в случае возникновения сбоя. Другими словами, если на данном шаге произойдет сбой, данный шаг необходимо повторить. Тем не менее, в случае, если желаемое число попыток возврата и повторного запуска не позволяет успешно завершить выполнение шага, рекомендуется, чтобы устройством, обнаружившим сбой, было сформировано предупреждение о сбое.

Следует отметить, что в приведенной ниже подробной схеме процесса (см. рисунок 6 и таблицу 1) вычисление хеша и шифрование/дешифрование файла конфигурации МТА ДОЛЖНЫ производиться в соответствии с требованиями Рек. МСЭ J.170.

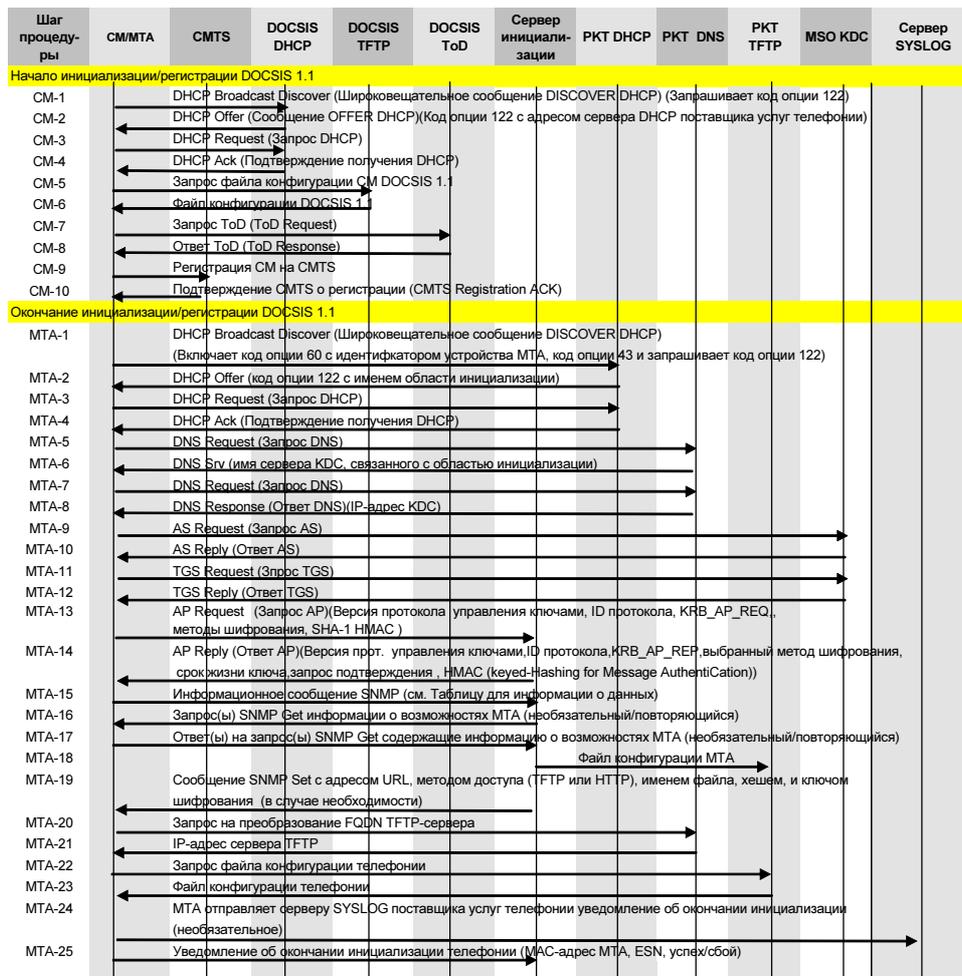


Рисунок 6/J.167 – Защищенный процесс инициализации встроенного МТА при включении

Таблица 1/J.167 – Описание процесса инициализации встроенного МТА при включении

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
СМ1	<p>Устройство-клиент начинает регистрацию путем отправки СМ-компонентом широковещательного сообщения DHCP DISCOVER.</p> <p>В данное сообщение включается код опции 60 (Опция, задаваемая поставщиком) в формате "docsis1.1:xxxxxxx". Данное сообщение ДОЛЖНО запрашивать Опцию 122 в Опции 55, списке запрашиваемых параметров. Оставшаяся часть данного сообщения ДОЛЖНА формироваться в соответствии с Рек. МСЭ-Т J.112.</p>	<p>Начальный</p> <p>Далее процесс ДОЛЖЕН продолжаться по порядку</p>	<p>В соответствии с DOCSIS</p>
СМ2	<p>Сервер DHCP DOCSIS, в случае, если он сконфигурирован для поддержки устройств МТА, ДОЛЖЕН включать опцию 122 с подписью 1 и, возможно, подписей 2, как указано в п.8.1. Если сервер сконфигурирован таким образом, чтобы не допускать подготовки к работе компонента МТА, подпись 1 кода опции 122 ДОЛЖНА содержать значение адреса сервера DHCP "0.0.0.0".</p> <p>Серверы DHCP DOCSIS, не предназначенные для работы с МТА, МОГУТ отвечать на запрос сообщением DHCP OFFER без включения опции 122</p>	<p>СМ2 ДОЛЖЕН выполняться по завершении шага СМ1</p>	<p>В соответствии с DOCSIS</p>
СМ3	<p>При получении сообщения DHCP OFFER СМ ДОЛЖЕН проверить наличие в ответе запрошенной опции 122. Если данная опция отсутствует, СМ ДОЛЖЕН предпринять 3 попытки повторного осуществления DHCP DISCOVER (СМ1) с экспоненциально возрастающим интервалом ожидания между попытками (например, через 2, 4 и 8 секунд). В случае, если после использования механизма экспоненциального повтора не было получено ни одного ответа DHCP OFFER, содержащего код опции 122, СМ ДОЛЖЕН рассмотреть сообщения DHCP OFFER без кода опции 122 и принять одно из них в соответствии со спецификацией DHCP (RFC 2131). В этом случае устройство-клиент (СМ) ДОЛЖНО отправить широковещательное сообщение DHCP REQUEST серверу DHCP, сообщение OFFER которого было принято, как указано в спецификации DHCP (RFC 2131).</p>	<p>СМ3 ДОЛЖЕН выполняться по завершении шага СМ2</p>	<p>В соответствии с DOCSIS</p>
СМ4	<p>Сервер DHCP отправляет СМ-компоненту устройства-клиента сообщение DHCP ACK в подтверждение приема предложенной информации. При получении DHCP ACK СМ ДОЛЖЕН еще раз проверить наличие опции 122. Отсутствие опции 122 в сообщении DHCP ACK предполагает, что он НЕ ДОЛЖЕН инициализировать встроенный МТА. Наличие опции 122 в сообщении DHCP ACK предполагает, что он ДОЛЖЕН инициализировать встроенный МТА и отправлять подпись 1 и, возможно, подпись 2.</p> <p>В случае, если содержание опций данного сообщения DHCP ACK отличается от ранее полученного DHCP OFFER, содержание сообщения DHCP ACK признается приоритетным (в соответствии с RFC 2131).</p>	<p>СМ4 ДОЛЖЕН выполняться по завершении шага СМ3</p>	<p>В соответствии с DOCSIS</p>
СМ5–СМ10	<p>СМ-компонент устройства-клиента заканчивает оставшуюся часть процесса регистрации СМ. Это включает загрузку файла конфигурации СМ, запрос времени дня регистрации и регистрацию на СМТS.</p>	<p>СМ5-СМ10 ДОЛЖНЫ выполняться по завершении шага СМ4</p>	<p>В соответствии с DOCSIS</p>

Таблица 1/J.167 – Описание процесса инициализации встроенного МТА при включении

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
МТА1	<p>Широковещательный поиск DHCP DISCOVER. МТА ДОЛЖЕН отправить широковещательное сообщение DHCP DISCOVER. В данное сообщение включается код опции 60 (Опция, задаваемая поставщиком) в формате "pktc1.0:xxxxxxx". МТА ДОЛЖЕН включать код опции 43 в сообщении DHCP DISCOVER, как указано в п.8.5. В опции DHCP 55 МТА ДОЛЖЕН запросить следующие опции: 1, 3, 6, 7, 12, 15 и 122. В случае, если в опции DHCP 122 подопции 1 (переданной СМ МТА) содержится значение адреса сервера DHCP "0.0.0.0", МТА НЕ ДОЛЖЕН пытаться начинать подготовку к работе и ДОЛЖЕН оставаться в неактивном (dormant) до тех пор, пока не будет реинициализирован СМ.</p>	<p>МТА1 НЕ ДОЛЖЕН выполняться до завершения шага СМ4</p>	<p>В случае сбоя в протоколе DHCP, происходит возврат к шагу МТА1</p>
МТА2	<p>Сообщение DHCP OFFER</p> <p>МТА может получить несколько сообщений DHCP OFFER (в течение периода ожидания, как указано в RFC 2131).</p> <p>К МТА и/или приложению подготовки к работе и предъявляются следующие требования:</p> <ol style="list-style-type: none"> <li>1) МТА ДОЛЖЕН принимать только действительные сообщения DHCP OFFER. Действительные сообщения DHCP OFFER ДОЛЖНЫ быть отправлены первичным или вторичным сервером DHCP, информация о которых была получена в коде опции 122 подопциях 1 и 2 встроенным МТА в ходе подготовки к работе СМ на шаге СМ4. Действительное сообщение DHCP OFFER также ДОЛЖНО включать следующие опции: 1, 3, 6, 7, 12, 15 и 122 (122 – с подопциями 3 и 6). Опция 122 МОЖЕТ дополнительно содержать подопции 4, 5, 7 и 9.</li> <li>2) В случае, если в опции 122 подопции 6, полученной от действительного сервера DHCP указывается, что должен быть использован базовый или гибридный процесс подготовки к работе, МТА ДОЛЖЕН проигнорировать подопции 4, 5, 7 и 9 опции 122, если они присутствуют.</li> <li>3) В случае, если в опции 122 подопции 6, полученной от действительного сервера DHCP указывается, что должен быть использован базовый процесс подготовки к работе, сервер подготовки к работе ДОЛЖЕН включить размещение файла конфигурации в поля "siaddr" и "file" ответов DHCP.</li> <li>4) В случае, если в опции 122 подопции 6, полученной от действительного сервера DHCP указывается, что должен быть использован защищенный процесс подготовки к работе, МТА ДОЛЖЕН обрабатывать подопции 4, 5, 7 и 9 опции 122.</li> </ol> <p>Далее МТА обрабатывает действительные сообщения DHCP OFFER в соответствии с правилами, приводимыми ниже:</p> <ol style="list-style-type: none"> <li>а) МТА ДОЛЖЕН проверить значение опции DHCP 122, подопции 3. В случае, если действительные сообщения OFFER содержат значение "0.0.0.0" в опции DHCP 122, подопции 3, МТА НЕ ДОЛЖЕН продолжать процесс работы с DHCP, а ДОЛЖЕН отключиться до тех пор, пока он не будет реинициализирован. В противном случае МТА ДОЛЖЕН ограничить набор действительных сообщений OFFER теми, у которых в опции DHCP 122, подопции 3 содержится ненулевое значение.</li> </ol>	<p>МТА2 ДОЛЖЕН выполняться по завершении шага МТА1</p>	<p>В случае сбоя в протоколе DHCP, происходит возврат к шагу МТА1</p>

Таблица 1/J.167 – Описание процесса инициализации встроенного МТА при включении

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
МТА2	<p>б) МТА ДОЛЖЕН проверить значение опции DHCP 122, подопции 6 на предмет указания об использовании защищенного процесса инициализации. В случае, если ни одно из полученных действительных сообщений OFFER не предписывает использование защищенного процесса, МТА ДОЛЖЕН предпринять 3 повторные попытки DHCP DISCOVER (МТА1) с экспоненциальным возрастанием периода ожидания между попытками (например, с интервалами в 2, 4, и 8 секунд). В случае, если сообщения, предписывающего использование защищенного процесса, не было получено, МТА ДОЛЖЕН выбрать действительное сообщение OFFER, предписывающее использование гибридного процесса или действительное сообщение OFFER, предписывающее использование базового процесса в указанном порядке.</p> <p>В случае, если не было получено ни одного действительного сообщения OFFER МТА ДОЛЖЕН зафиксировать сбой на соответствующем шаге процесса подготовки к работе.</p> <p>ПРИМЕЧАНИЕ. – В случае использования защищенного процесса, если МТА поддерживает TGT (Ticket Granting Ticket) и получает сообщение, где в опции 122 подопции 7 установлено значение FALSE, данный МТА НЕ ДОЛЖЕН запрашивать TGT. Если МТА поддерживает TGT и получает сообщение, где в опции 122 подопции 7 установлено значение TRUE, данный МТА ДОЛЖЕН запрашивать TGT. Если МТА не поддерживает TGT, он ДОЛЖЕН проигнорировать значение опции 122 подопции 7.</p>		
МТА3	<p>Широковещательное сообщение DHCP REQUEST</p> <p>Когда МТА выбрал действительное сообщение DHCP OFFER, МТА ДОЛЖЕН отправить широковещательное сообщение DHCP REQUEST для того, чтобы принять DHCP OFFER в соответствии с RFC 2131.</p>	МТА3 ДОЛЖЕН выполняться по завершении шага МТА2	В случае сбоя в протоколе DHCP, происходит возврат к шагу МТА1
МТА4	<p>Сообщение DHCP ACK</p> <p>Сервер DHCP отправляет сообщение DHCP ACK МТА. Сообщение DHCP ACK ДОЛЖНО включать все опции и подопции, которые были переданы в сообщении DHCP OFFER (МТА2). В случае, если значения опций и подопций данного сообщения DHCP ACK отличаются от значений ранее полученного сообщения DHCP OFFER (МТА2), значения опций и подопций DHCP ACK являются приоритетными (в соответствии с RFC 2131).</p>	МТА4 ДОЛЖЕН выполняться по завершении шага МТА3	В случае сбоя в протоколе DHCP, происходит возврат к шагу МТА1
МТА4	<p>В случае, если сообщение DHCP ACK недействительно согласно критериям, установленным на шаге МТА2, МТА ДОЛЖЕН зафиксировать сбой на данном шаге.</p> <p>ПРИМЕЧАНИЕ. – Процесс подготовки к работе разветвляется на три направления, указанных ниже:</p> <p>В случае, если сообщение DHCP ACK на шаге МТА4 указывает на необходимость использования базового процесса, МТА ДОЛЖЕН продолжить выполнение процесса с шага В-МТА-22, описанного в п.7.3.</p> <p>В случае, если сообщение DHCP ACK на шаге МТА4 указывает на необходимость использования гибридного процесса, МТА ДОЛЖЕН продолжить выполнение процесса с шага Н-МТА-15, описанного в п.7.4.</p> <p>Если все предшествующее неверно, МТА ДОЛЖЕН продолжить выполнение процесса с шага МТА5.</p>		

Таблица 1/J.167 – Описание процесса инициализации встроенного MTA при включении

Шаг процесса	Описание процесса инициализации встроенного MTA при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
MTA5	Запрос DNS Srv MTA запрашивает имя сервера KDC MSO (Multiple Service Operator, Оператор множественных услуг) для данной области Kerberos.	MTA5 ДОЛЖЕН выполняться по завершении шага MTA4	MTA1
MTA6	Ответ DNS Srv Возвращает имя сервера KDC MSO, связанного с областью подготовки к работе.	MTA6 ДОЛЖЕН выполняться по завершении шага MTA5	MTA1
MTA7	Запрос DNS Теперь MTA запрашивает IP-адрес MSO KDC.	MTA7 ДОЛЖЕН выполняться по завершении шага MTA6	MTA1
MTA8	DNS Reply Сервер DNS возвращает IP-адрес MSO KDC.	MTA8 ДОЛЖЕН выполняться по завершении шага MTA7	MTA1
MTA9	Запрос AS Сообщение AS Request отправляется MSO KDC для запроса мандата на доступ Kerberos.	Если MTA9 имеет место, он ДОЛЖЕН выполняться по завершении шага MTA8	MTA1 Условия возникновения сбоев описаны в спецификации безопасности J.170
MTA10	Ответ AS Сообщение AS Reply, содержащее мандат на доступ Kerberos, поступает от MSO KDC. ПРИМЕЧАНИЕ 1. – KDC ДОЛЖЕН установить соответствие MAC-адреса MTA и FQDN перед отправкой сообщения AS Reply. ПРИМЕЧАНИЕ 2. – Шаги MTA11 – MTA12 в некоторых случаях являются необязательными, см. спецификацию безопасности (J.170). ПРИМЕЧАНИЕ 3. – Модуль SNMPv3 (FQDN) ДОЛЖЕН быть преобразован в IP-адрес в промежутке от MTA5 до MTA12 (включая оба указанных шага). ПРИМЕЧАНИЕ 4. – В случае, если IP-адрес указан в поле Дополнительная информация ответа DNS-SRV (MTA6), MTA МОЖЕТ использовать тот же самый и пропустить шаги MTA7 и MTA8. ПРИМЕЧАНИЕ 5. – В случае, если у MTA имеется действующий мандат на доступ к серверу приложения подготовки к работе, сохраненный в энергонезависимой памяти NVRAM, MTA ДОЛЖЕН пропустить шаги от MTA5 до MTA12 при последующих перезагрузках MTA (шаги MTA1 – MTA25).	MTA10 ДОЛЖЕН выполняться по завершении шага MTA9	MTA1
MTA11	Запрос TGS (сервер выдачи мандатов) В случае, если MTA получил TGT на шаге MTA10, запрос TGS отправляется MSO KDC.	Если MTA11 имеет место, он ДОЛЖЕН выполняться по завершении шага MTA10	MTA1

Таблица 1/J.167 – Описание процесса инициализации встроенного МТА при включении

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
МТА12	<p>Ответ TGS</p> <p>Сообщение TGS Reply поступает от MSO KDC.</p>	<p>МТА12 ДОЛЖЕН выполняться по завершении шага МТА11</p>	<p>МТА1</p>
МТА13	<p>Запрос AP</p> <p>Сообщение AP Request отправляется серверу подготовки к работе для запроса информации о ключах для SNMPv3.</p>	<p>МТА13 ДОЛЖЕН выполняться по завершении шага МТА12</p>	<p>МТА1</p> <p>Условия возникновения сбоев описаны в спецификации безопасности J.170</p>
МТА14	<p>AP Reply</p> <p>Сообщение AP Reply, содержащее информацию о ключах для SNMPv3, поступает от сервера подготовки к работе.</p> <p>ПРИМЕЧАНИЕ – Ключи SNMPv3 должны быть заданы до перехода к следующему шагу на основе информации, полученной в сообщении AP Reply.</p>	<p>МТА14 ДОЛЖЕН выполняться по завершении шага МТА13</p>	<p>МТА1</p>
МТА15	<p>Информационное сообщение о регистрации SNMP (SNMP Enrollment INFORM)</p> <p>МТА ДОЛЖЕН отправлять SNMP Enrollment INFORM в адрес PROV_SNMP_ENTITY (указанного в опции Опции DHCP 122 подопции 3) Данное информационное сообщение SNMP ДОЛЖНО содержать объект "PktcMtaDevProvisioningEnrolment", определенный в Рек. МСЭ-Т J.166</p> <p>PROV_SNMP_ENTITY уведомляет приложение подготовки к работе о том, что МТА вошел в управляемый домен.</p> <p>ПРИМЕЧАНИЕ. – На данном этапе процесса сервер подготовки к работе может перезагрузить МТА. МТА является частью домена безопасности и ДОЛЖЕН отвечать на управляющие запросы, сообщение SNMP INFORM шага МТА15 является указателем, см. 5.4.1.2.</p>	<p>МТА15 ДОЛЖЕН выполняться по завершении шага МТА14</p>	<p>В случае сбоя в протоколе SNMP, происходит возврат к шагу МТА1. Сервер SNMP ДОЛЖЕН отправить ответ на сообщение SNMP-INFORM.</p>
МТА16	<p>Запрос GET SNMPv3 (необязательный). Если приложению инициализации (PROV_APP) требуются какие-либо дополнительные технические возможности МТА, приложение инициализации запрашивает МТА о наличии этих возможностей посредством запросов GET SMNPv3. В этом случае приложение инициализации отправляет PROV_SNMP_ENTITY многократный "запрос GET", PROV_SNMP_ENTITY отправляет МТА один или несколько запросов GET SNMPv3 для получения требуемой информации о возможностях МТА. Приложение подготовки к работе может использовать запрос GETBulk для получения нескольких частей пакета информации в одном сообщении.</p>	<p>Шаг МТА16 является необязательным, может выполняться по завершении шага МТА15</p>	<p>Недоступно</p>
МТА17	<p>Ответ SNMPv3 GET (SNMPv3 GET Response)</p> <p>Многократно:</p> <p>МТА отправляет PROV_SNMP_ENTITY ответ на каждый запрос GET. После того, как все запросы GET и GETBulk завершены, PROV_SNMP_ENTITY отправляет запрошенную информацию приложению инициализации.</p>	<p>МТА17 ДОЛЖЕН выполняться по завершении шага МТА16</p>	<p>Недоступно</p>

Таблица 1/J.167 – Описание процесса инициализации встроенного МТА при включении

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
MTA18	<p>Данный протокол не определен в рамках IP-Cablecom. Приложение инициализации МОЖЕТ использовать информацию, полученную на шаге MTA16 и MTA17 для определения содержимого файла данных конфигурации МТА. Механизмы отправки, хранения и, возможно, создания файла конфигурации описаны в шаге MTA19.</p>	<p>MTA18 СЛЕДУЕТ выполнять по завершении шага MTA15, в случае, если не выполнялся шаг MTA16. Если выполнялся шаг MTA16, данный шаг СЛЕДУЕТ выполнять по завершении шага MTA17.</p>	<p>Недоступно</p>
MTA19	<p>Сообщение SNMPv3 SET</p> <p>На данном этапе приложение инициализации МОЖЕТ создавать файл конфигурации или использовать заранее заданный файл. Содержимое файла конфигурации ДОЛЖНО быть хешировано. Файл конфигурации МОЖЕТ быть зашифрован. Хеш и ключ шифрования (если файл зашифрован) ДОЛЖНЫ быть отправлены МТА. Приложение инициализации ДОЛЖНО сохранить файл конфигурации на соответствующем сервере TFTP.</p> <p>Далее приложение инициализации предписывает Объекту инициализации SNMP (PROV_SNMP_ENTITY) отправить МТА сообщение SNMP SET, содержащее следующие переменные:</p> <p>pktcMtaDevConfigFile pktcMtaDevProvConfigHash и pktcMtaDevProvConfigKey (Данная переменная НЕ ДОЛЖНА включаться, если файл конфигурации не зашифрован).</p> <p>ПРИМЕЧАНИЯ:</p> <ol style="list-style-type: none"> <li>1) В случае, если загрузка файла происходит по методу доступа HTTP, имя файла должно быть закодировано в формате URL в соответствии с RFC 2616 за исключением случаев, указанных ниже в Примечании 3.</li> <li>2) В случае, если загрузка файла происходит по методу доступа TFTP, имя файла должно быть закодировано в формате URL в соответствии с RFC 3617 за исключением случаев, указанных ниже в Примечании 3.</li> <li>3) МТА ДОЛЖЕН принимать адреса IPv4 встроенные в URL-кодированный формат с квадратными скобками или без них.</li> </ol>	<p>MTA19 ДОЛЖЕН выполняться по завершении шага MTA18</p>	<p>В случае сбоя в протоколе SNMP, происходит возврат к шагу MTA1</p>
MTA20	<p>Запрос DNS (DNS Request)</p> <p>В случае, если в URL-кодированном запросе содержится FQDN вместо адреса IPv4, МТА ДОЛЖЕН использовать DNS сети поставщика услуг для преобразования данного FQDN в IPv4-адрес сервера TFTP или HTTP.</p>	<p>MTA20 ДОЛЖЕН выполняться по завершении шага MTA19 если используется FQDN</p>	<p>В случае сбоя в протоколе DNS, происходит возврат к шагу MTA1</p>
MTA21	<p>Ответ DNS (DNS Reply)</p> <p>Ответ DNS: сервер DNS возвращает IP-адрес в ответ на запрос DNS MTA20.</p>	<p>MTA21 ДОЛЖЕН выполняться по завершении шага MTA20 если используется FQDN</p>	<p>В случае сбоя в протоколе DNS, происходит возврат к шагу MTA1</p>

Таблица 1/J.167 – Описание процесса инициализации встроенного МТА при включении

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
МТА22	<p>ТFTP/HTTP-запрос файла конфигурации (ТFTP/HTTP Configuration file Request)</p> <p>МТА ДОЛЖЕН осуществить обмен данными либо по протоколу ТFTP, либо по протоколу HTTP, как указано в шаге S-МТА-19, для загрузки своего файла конфигурации. Для получения подробной информации по каждому из протоколов см. RFC 3415, RFC 3412.</p>	<p>МТА22 ДОЛЖЕН выполняться по завершении МТА19 в случае, если использование DNS не требуется.</p> <p>ДОЛЖЕН выполняться по завершении МТА21 в случае, если требуется использование DNS.</p>	<p>В случае сбоя в протоколе HTTP или ТFTP, происходит возврат к шагу МТА1</p>
МТА23	<p>ТFTP/HTTP-запрос файла конфигурации (ТFTP/HTTP Configuration file Response)</p> <p>Сервер ТFTP/HTTP ДОЛЖЕН отправить запрошенный файл конфигурации МТА. Для получения подробной информации по каждому из протоколов см. RFC 3415, RFC 3412. МТА вычисляет хеш полученного файла конфигурации и сравнивает его со значением, полученным на шаге МТА19. В случае, если хеши не совпадают, МТА ДОЛЖЕН зафиксировать сбой на данном шаге. В случае, если файл конфигурации зашифрован, он ДОЛЖЕН быть расшифрован.</p> <p>Для получения информации о содержимом файла конфигурации МТА см. п.9.1.</p>	<p>МТА23 ДОЛЖЕН выполняться по завершении шага МТА22</p>	<p>В случае, если загрузка файла конфигурации по протоколам HTTP или ТFTP дает сбой, происходит возврат к шагу МТА1. В иных случаях происходит переход к шагу МТА24 или МТА25, а в случае, если файл конфигурации содержит ошибку, отправляется ответ с уведомлением о сбое.</p>
МТА24	<p>Уведомление сервера SYSLOG (SYSLOG Notification)</p> <p>В случае, если сервер SYSLOG сконфигурирован и включен в процесс подготовки к работе (см. шаг МТА2 для информации об опциях DHCP и Рек. МСЭ-Т J.172 и J.166 для информации о конфигурировании с использованием MEM-MIB), МТА ДОЛЖЕН отправить серверу SYSLOG поставщика услуг голосовой связи сообщение о событии "подготовка к работе завершена" (provisioning complete) указывающее на статус операции подготовки к работе. В данное уведомление должно быть включено сообщение о результате выполнения процесса подготовки к работе. В общем виде формат данного уведомления приведен в п. 5.4.3.</p>	<p>МТА24 ДОЛЖЕН выполняться по завершении шага МТА23 в случае, если SYSLOG сконфигурирован.</p>	<p>МТА МОЖЕТ предпринять повторные попытки выполнения данного шага, прежде чем перейти к шагу МТА25.</p>

Таблица 1/J.167 – Описание процесса инициализации встроенного МТА при включении

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
MTA25	<p>Информационное сообщение SNMP (SNMP INFORM) МТА ДОЛЖЕН отправлять PROV_SNMP_ENTITY (указан в Опции DHCP 122 подопции 3) информационное сообщение SNMP, содержащее уведомление об окончании подготовки к работе ("provisioning complete"). Получение информационного сообщения подтверждается ответным сообщением, как определено RFC 3414.</p> <p>Информационное сообщение SNMP ДОЛЖНО содержать объект "PktcMtaDevProvisioningStatus", как определено в Рек. МСЭ-Т J.166.</p> <p>ПРИМЕЧАНИЯ:</p> <ol style="list-style-type: none"> <li>1) На данном этапе информации подготовки к работе МТА достаточно для предоставления минимального набора услуг, определенного поставщиком (например, 611).</li> <li>2) В зависимости от конфигурации TLV-38 станциям управления SNMP может быть отправлено несколько информационных сообщений SNMP.</li> </ol>	<p>MTA25 ДОЛЖЕН выполняться по завершении шага MTA24 в случае, если использовался SYSLOG. В противном случае MTA25 ДОЛЖЕН выполняться по завершении шага MTA23.</p>	<p>MTA МОЖЕТ создать уведомление о событии "Сбой подготовки к работе" для сервера управления сбоями поставщика услуг. Процесс подготовки к работе останавливается, требуется вмешательство. Сервер SNMP ДОЛЖЕН отправить ответ на информационное сообщение SNMP.</p>

### 7.3 Процесс инициализации встроенного МТА в момент включения (базовый процесс)

Базовый процесс подготовки к работе МТА очень похож на процесс подготовки к работе CM DOCSIS. См. рисунок 7 и таблицу 2.

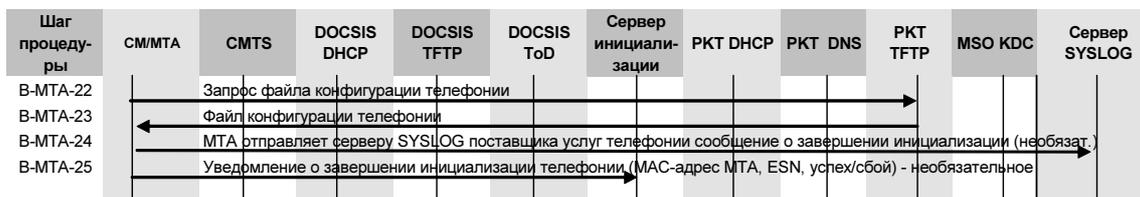


Рисунок 7/J.167 – Базовый процесс инициализации встроенного МТА в момент включения

Таблица 2/J.167 – Описание базового процесса инициализации встроенного МТА в момент включения

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
	<p>ПРИМЕЧАНИЕ. – FQDN, указанное в Опции DHCP 122 подопции 3 сообщения DHCP ACK (адрес объекта подготовки к работе) ДОЛЖЕН быть преобразован в IP-адрес до выполнения шага V-MTA-22.</p>		
V-MTA-22	<p>Запрос файла конфигурации по протоколу TFTP (TFTP Configuration File Request)</p> <p>MTA ДОЛЖЕН выполнить обмен данными по протоколу TFTP для загрузки своего файла конфигурации. Поля "siaddr" и "file" сообщения DHCP ACK используются для указания местонахождения файла конфигурации. Подробная информация по протоколу TFTP находится в RFC 3415.</p>	<p>V-MTA-22 ДОЛЖЕН выполняться по завершении шага MTA4</p>	<p>В случае сбоя в протоколе TFTP, происходит возврат к шагу MTA1</p>

**Таблица 2/J.167 – Описание базового процесса инициализации встроенного МТА в момент включения**

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
В-МТА-23	<p>Ответ на запрос файла конфигурации по протоколу TFTP (TFTP Configuration File Response)</p> <p>Сервер TFTP ДОЛЖЕН отправить запрошенный файл конфигурации МТА. Подробная информация по протоколу TFTP находится в RFC 3415.</p> <p>Загруженный файл конфигурации ДОЛЖЕН содержать объект MIB 'pktcMtaDevConfigHash'. МТА ДОЛЖЕН вычислить хеш загруженного файла конфигурации в соответствии с указаниями, приведенными в п.9.1, и сравнить полученное значение со значением, содержащимся в объекте 'pktcMtaDevConfigHash'. В случае, если эти значения различаются, МТА ДОЛЖЕН зафиксировать сбой на данном шаге.</p> <p>Для получения информации о содержимом файла конфигурации см. п.9.1.</p>	В-МТА-23 ДОЛЖЕН выполняться по завершении шага В-МТА-22	<p>В случае, если загрузка файла конфигурации по протоколу TFTP заканчивается сбоем, происходит возврат к шагу МТА1.</p> <p>В иных случаях происходит переход к шагу В-МТА-24, а в случае, если файл конфигурации содержит ошибку, отправляется ответ с уведомлением о сбое.</p>
В-МТА-24	<p>Уведомление сервера SYSLOG (SYSLOG Notification)</p> <p>В случае, если сервер SYSLOG сконфигурирован и включен в процесс подготовки к работе (см. шаг МТА2 для информации об опциях DHCP и Рек. МСЭ-Т J.172 и J.166 для информации о конфигурировании с использованием MEM-MIB), МТА ДОЛЖЕН отправить серверу SYSLOG поставщика услуг голосовой связи сообщение о событии "подготовка к работе завершена" (provisioning complete) указывающее на статус операции подготовки к работе. В общем виде формат данного уведомления приведен в п. 5.4.3.</p>	В-МТА-24 ДОЛЖЕН выполняться по завершении шага В-МТА-23 в случае, если сервер SYSLOG сконфигурирован	МТА МОЖЕТ предпринять повторные попытки выполнения данного шага, прежде чем перейти к шагу В-МТА-25.
В-МТА-25	<p>Информационное сообщение SNMPv2c о статусе подготовки к работе (необязательное) (SNMPv2c Provisioning Status INFORM)</p> <p>МТА ДОЛЖЕН отправлять PROV_SNMP_ENTITY (указан в Опции DHCP 122 подопции 3) информационное сообщение SNMP, содержащее уведомление об окончании подготовки к работе ("provisioning complete"), если это предписано опцией DHCP 122 подопцией 6. Получение информационного сообщения подтверждается ответным сообщением.</p> <p>Информационное сообщение SNMP ДОЛЖНО содержать объект "PktcMtaDevProvisioningStatus", как определено в Рек. МСЭ-Т J.166.</p> <p>Имя сообщества SNMPv2c, используемое в информационном сообщении о статусе SNMP ДОЛЖНО иметь значение "public" (без кавычек).</p> <p><b>ПРИМЕЧАНИЯ:</b></p> <ol style="list-style-type: none"> <li>1) На данном этапе информации подготовки к работе МТА достаточно для предоставления минимального набора услуг, определенного поставщиком (например, 611).</li> <li>2) В зависимости от значений пар конфигурации TLV-38 станциям управления SNMP может быть отправлено несколько информационных сообщений SNMP.</li> </ol>	В-МТА-25 является необязательным, МОЖЕТ выполняться по завершении выполнения шага В-МТА-24 в случае, если использовался SYSLOG, в противном случае МОЖЕТ выполняться по завершении шага В-МТА-23.	Процесс подготовки к работе останавливается, требуется вмешательство. Сервер SNMP ДОЛЖЕН отправить ответ на информационное сообщение SNMP.

#### 7.4 Процесс инициализации встроенного МТА в момент включения (гибридный процесс)

Гибридный процесс подготовки к работе (гибридный процесс, Hybrid Flow) по большинству параметров идентичен защищенному процессу, отличие заключается в том, что в гибридном процессе отсутствует обмен ключами Kerberos и протокол SNMPv2c заменен на SNMPv3. Имя сообщества SNMPv2c, используемое в информационных сообщениях SNMP, отправляемых МТА при выполнении шагов Н-МТА-15 и Н-МТА-25, должно принимать значение "public" (без кавычек). См. рисунок 8 и таблицу 3.

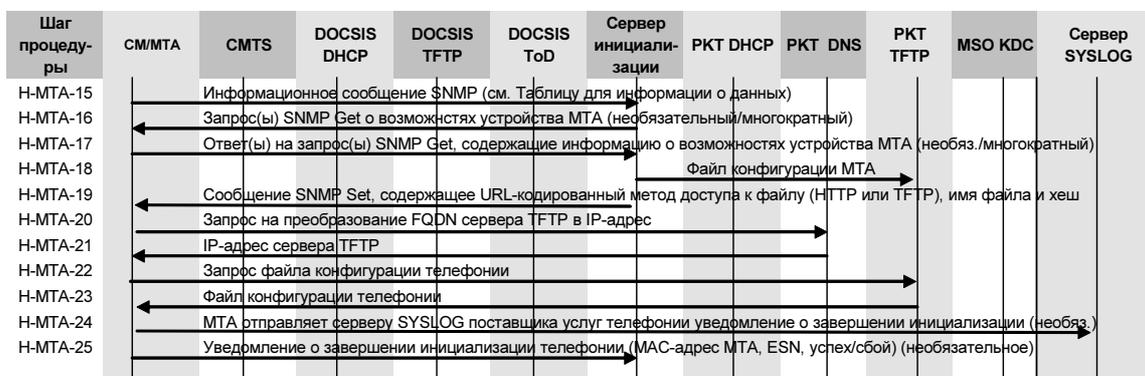


Рисунок 8/J.167 – Гибридный процесс инициализации встроенного МТА в момент включения

Таблица 3/J.167 – Описание гибридного процесса инициализации встроенного МТА в момент включения

Шаг процесса	Описание процесса инициализации встроенного МТА при включении	Нормальный порядок шагов процесса	Сюда ДОЛЖЕН осуществляться переход в случае сбоя
	ПРИМЕЧАНИЕ! – FQDN, указанное в Опции DHCP 122 подопции 3 сообщения DHCP ACK (адрес модуля подготовки к работе) ДОЛЖЕН быть преобразован в IP-адрес до выполнения шага Н-МТА-15.		
Н-МТА-15	Информационное сообщение о регистрации SNMP (SNMP Enrollment INFORM) МТА ДОЛЖЕН отправлять SNMP Enrollment INFORM в адрес PROV_SNMP_ENTITY (указанного в Опции DHCP 122 подопции 3). Данное информационное сообщение SNMP ДОЛЖНО содержать объект "PktcMtaDevProvisioningEnrolment", определенный в Рек. МСЭ-Т J.166 PROV_SNMP_ENTITY уведомляет приложение инициализации о том, что МТА вошел в управляемый домен.	Н-МТА-15 ДОЛЖЕН выполняться по завершении шага МТА4	В случае сбоя в протоколе SNMP, происходит возврат к шагу МТА1. Сервер SNMP ДОЛЖЕН отправить ответ на информационное сообщение SNMP.
Н-МТА-16	Запрос GET SNMPv2 (необязательный). Приложение подготовки к работе (PROV_APP) может запросить дополнительную информацию о технических возможностях МТА посредством запросов GET SMNPv2. В этом случае приложение подготовки к работе отправляет PROV_SNMP_ENTITY "запрос GET". Множественно: PROV_SNMP_ENTITY отправляет МТА один или несколько запросов GET SNMPv2 для получения требуемой информации о возможностях МТА. Приложение подготовки к работе может использовать запрос GETBulk для получения нескольких частей пакета информации в одном сообщении.	Н-МТА-16 является необязательным, МОЖЕТ выполняться по завершении шага Н-МТА-15	Недоступно

**Таблица 3/J.167 – Описание гибридного процесса инициализации  
встроенного МТА в момент включения**

<b>Шаг процесса</b>	<b>Описание процесса инициализации встроенного МТА при включении</b>	<b>Нормальный порядок шагов процесса</b>	<b>Сюда ДОЛЖЕН осуществляться переход в случае сбоя</b>
Н-МТА-17	<p>Ответ SNMPv2 GET (SNMPv3 GET Response)</p> <p>Множественно:</p> <p>МТА отправляет PROV_SNMP_ENTITY ответ на каждый запрос GET. После того, как все запросы GET и GETBulk завершены, PROV_SNMP_ENTITY отправляет запрошенную информацию приложению подготовки к работе.</p>	<p>Н-МТА-17 ДОЛЖЕН выполняться по завершении шага Н-МТА-16, если Н-МТА-16 выполнялся</p>	Недоступно
Н-МТА-18	<p>Данный протокол не определен в рамках PCablecom.</p> <p>Приложение подготовки к работе МОЖЕТ использовать информацию, полученную на шаге Н-МТА-15, -16 и -17 для определения содержимого файла данных конфигурации МТА. Механизмы отправки, хранения и, возможно, создания файла конфигурации описаны в шаге Н-МТА-19.</p>	<p>Н-МТА-18 СЛЕДУЕТ выполнять по завершении шага Н-МТА-15, если не выполнялся шаг Н-МТА-16. В противном случае Н-МТА-18 СЛЕДУЕТ выполнять по завершении шага Н-МТА-17.</p>	Недоступно
Н-МТА-19	<p>Установка файла конфигурации SNMPv2 (SET)</p> <p>На данном этапе приложение подготовки к работе МОЖЕТ создавать файл конфигурации или использовать заранее заданный файл. Приложение подготовки к работе ДОЛЖНО вычислить SHA-1 хеш содержимого файла конфигурации. Приложение подготовки к работе ДОЛЖНО сохранить файл конфигурации на соответствующем сервере TFTP.</p> <p>Далее приложение подготовки к работе предписывает Объекту инициализации SNMP (PROV_SNMP_ENTITY) отправить МТА сообщение SNMPv2c SET, содержащее следующие переменные:</p> <p>pkcMtaDevConfigFile pkcMtaDevProvConfigHash.</p> <p>В отличие от защищенного процесса, объект MIB pkcMtaDevProvConfigKey НЕ ДОЛЖЕН включаться. В случае, если объект pkcMtaDevProvConfigKey включен, МТА ДОЛЖЕН вернуть сообщение об ошибке "несовместимое значение" (inconsistent value) (для получения более подробной информации об ответах SNMP SET см. RFC 3413).</p> <p><b>ПРИМЕЧАНИЯ:</b></p> <ol style="list-style-type: none"> <li>1) В случае, если загрузка файла происходит по методу доступа HTTP, имя файла должно быть закодировано в формате URL в соответствии с RFC 2616 за исключением случаев, указанных ниже в Примечании 3.</li> <li>2) В случае, если загрузка файла происходит по методу доступа TFTP, имя файла должно быть закодировано в формате URL в соответствии с RFC 3617 за исключением случаев, указанных ниже в Примечании 3.</li> <li>3) МТА ДОЛЖЕН принимать адреса IPv4 встроенные в URL-кодированный формат с квадратными скобками или без них.</li> </ol>	<p>Н-МТА-19 ДОЛЖЕН выполняться по завершении шага Н-МТА-18</p>	<p>В случае сбоя в протоколе SNMP, происходит возврат к шагу МТА1</p>

**Таблица 3/J.167 – Описание гибридного процесса инициализации  
встроенного MTA в момент включения**

<b>Шаг процесса</b>	<b>Описание процесса инициализации встроенного MTA при включении</b>	<b>Нормальный порядок шагов процесса</b>	<b>Сюда ДОЛЖЕН осуществляться переход в случае сбоя</b>
H-MTA-20	Запрос DNS (необязательный) В случае, если в URL-кодированном запросе содержится FQDN вместо адреса IPv4, MTA ДОЛЖЕН использовать DNS сети поставщика услуг для преобразования данного FQDN в IPv4-адрес сервера TFTP или HTTP.	H-MTA-20 ДОЛЖЕН выполняться по завершении шага H-MTA-19, если используется FQDN	В случае сбоя в протоколе DNS, происходит возврат к шагу MTA1
H-MTA-21	Ответ DNS (необязательный) Ответ DNS: сервер DNS возвращает IP-адрес в ответ на запрос DNS H-MTA-20.	H-MTA-21 ДОЛЖЕН выполняться по завершении шага H-MTA-20, если используется FQDN	В случае сбоя в протоколе DNS, происходит возврат к шагу MTA1
H-MTA-22	TFTP/HTTP-запрос файла конфигурации (TFTP/HTTP Configuration file Request) MTA ДОЛЖЕН осуществить обмен данными либо по протоколу TFTP, либо по протоколу HTTP, как указано в шаге S-MTA-19, для загрузки своего файла конфигурации. Для получения подробной информации по каждому из протоколов см. RFC 3415, RFC 3412.	H-MTA-22 ДОЛЖЕН выполняться по завершении шага H-MTA-19, если не указан FQDN. Если FQDN указан, H-MTA-22 ДОЛЖЕН выполняться по завершении шага H-MTA-21	В случае сбоя в протоколе TFTP или HTTP, происходит возврат к шагу MTA1
H-MTA-23	Ответ на TFTP/HTTP-запрос файла конфигурации (TFTP/HTTP Configuration file Response) Сервер TFTP/HTTP ДОЛЖЕН отправить запрошенный файл конфигурации MTA. Для получения подробной информации по каждому из протоколов см. RFC 3415, RFC 3412. MTA вычисляет хеш полученного файла конфигурации и сравнивает его со значением, полученным на шаге H-MTA-19. В случае, если хеши не совпадают, MTA ДОЛЖЕН зафиксировать сбой на данном шаге. Для получения информации о содержимом файла конфигурации MTA см. п.9.1.	H-MTA-23 ДОЛЖЕН выполняться по завершении шага H-MTA-22	В случае, если загрузка файла конфигурации по протоколам HTTP или TFTP дает сбой, происходит возврат к шагу MTA1. В иных случаях происходит переход к шагу MTA24 или MTA25, а в случае, если файл конфигурации содержит ошибку, отправляется ответ с уведомлением о сбое.

**Таблица 3/J.167 – Описание гибридного процесса инициализации  
встроенного МТА в момент включения**

<b>Шаг процесса</b>	<b>Описание процесса инициализации встроенного МТА при включении</b>	<b>Нормальный порядок шагов процесса</b>	<b>Сюда ДОЛЖЕН осуществляться переход в случае сбоя</b>
Н-МТА-24	<p>Уведомление сервера SYSLOG (SYSLOG Notification)</p> <p>В случае, если сервер SYSLOG сконфигурирован и включен в процесс подготовки к работе (см. шаг МТА2 для информации об опциях DHCP и Рек. МСЭ-Т J.172 и J.166 для информации о конфигурировании с использованием MEM-MIB), МТА ДОЛЖЕН отправить сервера SYSLOG поставщика услуг голосовой связи сообщение о событии "подготовка к работе завершена" (provisioning complete) указывающее на статус операции подготовки к работе. В данное уведомление должно быть включено сообщение о результате выполнения процесса подготовки к работе. В общем виде формат данного уведомления приведен в п. 5.4.3.</p>	Н-МТА-24 ДОЛЖЕН выполняться по завершении шага Н-МТА-23 в случае, если SYSLOG сконфигурирован.	МТА МОЖЕТ предпринять повторные попытки выполнения данного шага, прежде чем перейти к шагу Н-МТА-25.
Н-МТА-25	<p>Информационное сообщение SNMPv2c о статусе подготовки к работе (необязательное) (SNMPv2c Provisioning Status INFORM)</p> <p>МТА ДОЛЖЕН отправлять PROV_SNMP_ENTITY (указан в Опции DHCP 122 подопции 3) информационное сообщение SNMP, содержащее уведомление об окончании подготовки к работе ("provisioning complete"). Получение информационного сообщения подтверждается ответным сообщением.</p> <p>Информационное сообщение SNMP ДОЛЖНО содержать объект "PktcMtaDevProvisioningStatus", как определено в Рек. МСЭ-Т J.166.</p> <p><b>ПРИМЕЧАНИЯ:</b></p> <p>1) На данном этапе информации подготовки к работе МТА достаточно для предоставления минимального набора услуг, определенного поставщиком (например, 611).</p> <p>2) В зависимости от значений пар конфигурации TLV-38 станциям управления SNMP может быть отправлено несколько информационных сообщений SNMP.</p>	Н-МТА-25 является необязательным, МОЖЕТ выполняться по завершении выполнения шага Н-МТА-24 в случае, если использовался SYSLOG, в противном случае МОЖЕТ выполняться по завершении шага Н-МТА-23.	Процесс подготовки к работе останавливается, требуется вмешательство. Сервер SNMP ДОЛЖЕН отправить ответ на информационное сообщение SNMP.

### 7.5 Уведомление о завершении подготовки к работе конечных точек

После успешной подготовки к работе МТА, вне зависимости от выбранного процесса подготовки к работе, МТА должен устанавливать необходимые защищенные соединения со связанными сконфигурированными областями CMS (KDC). Программное обеспечение сигнализации NCS (Network Call Signalling, сигнализация вызовов сети) МТА должно инициировать установление защищенных соединений по протоколу IPSec со сконфигурированными кластерами CMS. Уведомления о событиях создаются в случае, если защищенные соединения не могут быть установлены (как предписано Рек. МСЭ-Т J.170).

По завершении процесса подготовки к работе (базового, гибридного или защищенного) и после установления всех необходимых защищенных соединений программное обеспечение сигнализации NCS МТА определяет, может ли канал сигнализации быть установлен при помощи сообщения RSIP и соответствующего сообщения ACK. Начиная работу в ситуации отсутствия связи, МТА должен отправлять прерывание установления связи SNMP (SNMP Link Up Trap) когда в ответ на сообщение RSIP поступает соответствующее подтверждение. Это указывает на то, что конечная точка подготовлена к работе. В случае, если один и тот же CMS используется для нескольких конечных точек, сообщение SNMP об установлении связи должно отправляться каждой из этих конечных

точек. В случае, если не все конечные точки используют один и тот же CMS, данный процесс должен быть повторен для каждой конечной точки, требующей другого сконфигурированного CMS.

## **7.6 Пошаговая подготовка к работе отдельных конечных точек по завершении подготовки к работе МТА**

В данном пункте описываются процессы, позволяющие приложению подготовки к работе производить пошаговую подготовку к работе отдельных конечных точек голосовой связи после завершения подготовки к работе МТА. Пошаговая подготовка к работе конечной точки по окончании подготовки к работе МТА МОЖЕТ предусматривать общение с представителем службы работы с потребителями.

### **7.6.1 Синхронизация атрибутов подготовки к работе с файлом конфигурации**

Пошаговая подготовка к работе включает добавление, удаление или изменение одной или более абонентских услуг на одной или более конечных точках встроенного МТА. Услуги на встроенном МТА ДОЛЖНЫ изменяться при помощи SNMP с использованием MIB МТА (см. Рек. МСЭ-Т J.166). Вспомогательные приложения ДОЛЖНЫ поддерживать "проточный (flow-through)" механизм подготовки к работе, синхронизирующий всю информацию подготовки к работе устройства с соответствующими вспомогательными серверами и базами данных. Синхронизация необходима для тех случаев, когда требуется восстановление информации подготовки к работе для реинициализации устройства. Хотя детальное обсуждение синхронизации со вспомогательными приложениями выходит за рамки данной Рекомендации, предполагается, что, как минимум, будет обновляться следующая информация: записи по абонентам и файл конфигурации МТА на сервере TFTP или HTTP.

### **7.6.2 Добавление/подключение телефонных услуг на конечной точке МТА**

Услуги телефонии могут быть добавлены и/или подключены на конечной точке МТА. Услуги телефонии могут быть добавлены на конечных точках МТА, которые ранее не были подготовлены к работе.

Когда добавляются/подключаются услуги на такой конечной точке МТА:

- МТА ДОЖЕН быть подготовлен к работе информацией о конфигурации "уровня устройства" при помощи файла конфигурации (как описано в п. 9.1.1).
- Уполномоченная станция управления SNMP ДОЛЖНА подготавливать к работе все необходимые атрибуты конфигурации как описано в п.9.1.3, 9.1.4 и 9.1.5 при помощи операций SNMP SET для того, чтобы обновить атрибуты подготовки к работе на устройстве для подключения какого-либо конкретного порта телефонных услуг.

Услуги телефонии, подготовленные к работе на конечных точках МТА, но отключенные, могут быть подключены (см. п.7.6.3 и 9.1.1 для получения более подробной информации). Для подключения ранее отключенных услуг телефонии на конечной точке МТА уполномоченная станция управления SNMP ДОЛЖНА использовать соответствующие операции SNMP SET для того, чтобы выполнить нижеследующее:

- Убедиться, что в объекте статуса ряда MIB (pktnCsEndPntConfigStatus) для ряда, соответствующего данной конечной точке установлено значение "active (1)" (или изменить его соответствующим образом, если установлено какое-либо другое значение).
- Убедиться, что для объекта "ifAdminStatus", соответствующего данной конечной точке, установлено значение "up (2)" (или изменить его соответствующим образом, если установлено какое-либо другое значение).

Когда конечная точка подготовлена к работе или подключена, МТА ДОЛЖЕН выполнить следующие действия (порядок не критичен):

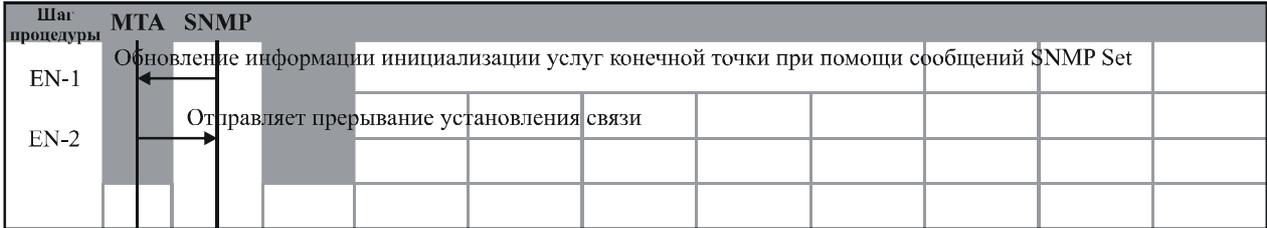
- Следовать процедурам, описанным в п. 7.1.1.2.5 спецификации безопасности (J.170).
- Изменить значение объекта MIB "ifOperStatus" согласно п. 7.7.

В случае, если для объекта MIB "pktnMtaDevEnabled" установлено значение "true (1)" МТА ДОЛЖЕН выполнить приведенные выше действия для всех сконфигурированных конечных точек.

Следует отметить, что поскольку Подготовка к работе конечных точек по природе своей является объектом MIB, контролирующим наличие/отсутствие защищенных соединений с сервером управления вызовами по протоколу IPSec, она не может использоваться для изменения статуса IPSec (см. Приложение A/J.166 для получения более подробной информации). Таким образом, подключение новых услуг с помощью сервера управления вызовами, статус которого не был указан ранее (при помощи файла конфигурации), приведет к включению IPSec при подключении к конечной точке.

В качестве примера подключения услуги телефонии на конечной точке рассмотрим случай, когда абонент запрашивает услугу на конечной точке, которая ранее не была подготовлена к работе.

ПРИМЕЧАНИЕ. – Данный пример предусматривает, что создание лицевого счета у поставщика услуг закончено, и показывает только ключевые для процесса компоненты. Например, предполагается, что создание лицевых счетов и учетных баз данных доступно и интегрировано в систему вспомогательных приложений.



J.167\_F09

Рисунок 9/J.167 – Подключение услуг на конечной точке MTA

Таблица 4/J.167 – Описание процесса подключения услуг на конечной точке MTA

Шаг процесса	Описание шага процесса подключения услуг на конечной точке MTA	Нормальный порядок выполнения процесса
EN-1	Уполномоченная станция управления SNMP выполняет необходимые для добавления услуг на конечную точку MTA операции SNMP SET.	Если требуется выполнить конфигурацию конечной точки, шаг EN-1 ДОЛЖЕН выполняться после успешного завершения выполнения процесса инициализации при включении.
EN-2	MTA ДОЛЖЕН отправить прерывание установления связи сконфигурированным станциям управления SNMP. См. п. 7.7 и IF-MIB (RFC 2863) для получения дополнительной информации.	EN-2 ДОЛЖЕН выполняться по завершении шага EN-1.

### 7.6.3 Удаление/отключение услуг телефонии на конечной точке MTA

Подготовленные к работе и подключенные услуги могут быть отключены (обслуживание приостановлено) или удалены в случае необходимости при помощи SNMP с использованием MTA MIB (Рек. МСЭ-Т J.166) и сигнализации MIB (Рек. МСЭ-Т J.166) для каждой отдельно взятой конечной точки.

Когда возникает необходимость удалить услугу на конечной точке, уполномоченная станция управления SNMP ДОЛЖНА удалить соответствующие атрибуты конфигурации, описанные в п.9.1.3, 9.1.4 и 9.1.5 с соответствующей конечной точки при помощи операций SNMP SET.

В случае необходимости отключения услуг на конечной точке MTA, уполномоченная станция управления SNMP ДОЛЖНА выполнить одно или несколько из приведенных ниже условий при помощи операций SNMP SET:

- Для конкретной конечной точки присвоить объекту статуса ряда в "pktnCsEndPntConfigTable" значение, отличное от "active (1)".
- Для конкретной конечной точки изменить значение объекта "ifAdminStatus" на "down (2)".

В случае, если конечная точка удаляется или отключается в тот момент, когда имеется активный вызов, MTA ДОЛЖЕН:

- Завершить все сеансы передачи медиаинформации, если таковые имеются;

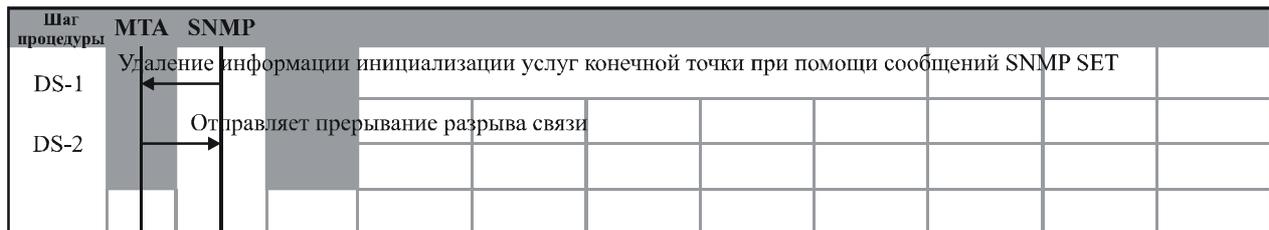
- Завершить сигнализацию NCS следуя процедурам Restart in Progress описанным в спецификации NCS IPCablecom (Рек. МСЭ-Т J.162).
- Перевести объект MIB pktcNcsEndPntStatusError для конкретной конечной точки в состояние "disconnected (3)".

В случае, если для объекта MIB "pktcMtaDevEnabled" установлено значение "false (2)", МТА ДОЛЖЕН выполнить указанные выше действия для всех сконфигурированных конечных точек.

В качестве примера отключения услуги телефонии на конечной точке рассмотрим случай, когда абонент запрашивает отключение услуги на конечной точке, которая ранее была инициализирована.

ПРИМЕЧАНИЕ 1. – Предполагается, что обновление лицевого счета у поставщика услуг закончено, и иллюстрирует только ключевые для работы МТА этапы.

ПРИМЕЧАНИЕ 2. Данный пример предусматривает, что обновление лицевого счета у поставщика услуг закончено, и иллюстрирует только ключевые для работы МТА этапы.



J.167\_F10

Рисунок 10/J.167 – Отключение услуг на конечной точке МТА

Таблица 5/J.167 – Описание процесса отключения услуг на конечной точке МТА

Шаг потока	Описание шага процесса подключения услуг на конечной точке МТА	Нормальный порядок выполнения процесса
DS-1	Уполномоченная станция управления SNMP выполняет необходимые для отключения услуг на конечной точке МТА операции SNMP SET.	DS-1 ДОЛЖЕН выполняться после того, как конечная точка приведена во включенное состояние: или сразу по завершении первоначальной подготовки к работе или после пошаговой подготовки к работе отдельно взятой конечной точки.
DS-2	МТА ДОЛЖЕН отправить прерывание разрыва связи сконфигурированным станциям управления SNMP. См. п. 7.7 и IF-MIB (RFC 2863) для получения дополнительной информации.	DS-2 ДОЛЖЕН выполняться по завершении шага DS-1

#### 7.6.4 Изменение услуг телефонии на конечной точке МТА

Услуги телефонии могут быть изменены на подготовленной к работе в данный момент конечной точке МТА. Это производится при помощи SNMP с использованием MIB МТА (см. Рек. МСЭ-Т J.166) и сигнализации MIB (см. Рек. МСЭ-Т J.166) для каждой конкретной конечной точки. В случае, если в ходе данных изменений меняется связанный CMS (pktcNcsEndPntConfigCallAgentId) и/или порт (pktcNcsEndPntConfigCallAgentUdpPort), обслуживанием конечной точки временно прекращается (в соответствии с п.7.6.3), а затем возобновляется (в соответствии с п.7.6.2).

МТА ДОЛЖЕН следовать процедурам, описанным в спецификации безопасности (J.170).

Следует отметить, что:

- Изменения, касающиеся характеристик услуг, производятся на CMS, а не на МТА.
- Изменения параметров уровня услуг, касающиеся СМ-компонента встроенного МТА, могут потребовать перезагрузки встроенного МТА.

## 7.7 Отражение состояния интерфейса конечной точки в таблице ifTable

Операционное состояние каждой конечной точки отражается в объекте "ifOperStatus" MIB МТА. На данный процесс оказывают влияние следующие факторы:

Соответствующий административный статус конечной точки, отраженный в таблице "ifAdminStatus".

- Состояние предоставления услуг телефонии соответствующей конечной точке.
- Наличие/отсутствие на соответствующей конечной точке защищенных соединений по протоколу IPSec, при условии, что IPSec включен (т.е. для объекта MIB "pktcMtaDevCmsIpsecCtrl" установлено значение "true (1)" для данной конечной точки).

В случае реинициализации МТА (после перезагрузки или сброса) он ДОЛЖЕН немедленно установить для пунктов таблицы "ifAdminStatus", соответствующих всем физическим конечным точкам, значения "up (1)". Однако этот статус может быть изменен соответствующими параметрами файла конфигурации или управляющей станцией SNMP. В дальнейшем МТА отражает результаты влияния указанных выше факторов в операционном статусе каждой конечной точки, как объяснено ниже.

Для каждого пункта таблицы "ifTable" MIB, соответствующего конечной точке, МТА ДОЛЖЕН установить следующие значения "ifOperStatus":

- "down (2)" в случае, если конечная точка удаляется или отключается, или соответствующее значение "ifAdminStatus" – "down (2)".
- "up (1)" в случае, если соответствующее значение "ifAdminStatus" – "up (1)", услуги телефонии были добавлены или подключены для данной конечной точки и IPSec отключен соответствующим сервером управления вызовами.
- "up (1)" в случае, если соответствующее значение "ifAdminStatus" – "up (1)", услуги телефонии были добавлены или подключены для данной конечной точки и IPSec включен соответствующим сервером управления вызовами и защищенные соединения по протоколу IPSec были установлены.
- "dormant (3)"(неактивен) в случае, если соответствующее значение "ifAdminStatus" – "up (1)", услуги телефонии были добавлены или подключены для данной конечной точки и IPSec включен соответствующим сервером управления вызовами, но защищенные соединения по протоколу IPSec не были установлены.

В дальнейшем МТА НЕ ДОЛЖЕН устанавливать для 'ifOperStatus' значение "dormant (3)" для конечных точек, на которых отключен IPSec. Для получения дополнительной информации по включению/отключению IPSec см. Рек. МСЭ-Т J.166, по добавлению/подключению конечных точек см. п.7.6.2, по отключению/удалению конечных точек см. п.7.6.3.

МТА ДОЛЖЕН иметь возможность включать и отключать прерывание установления связи и прерывание разрыва связи (Link Up Trap/Link Down Trap) при помощи объекта MIB "ifLinkUpDownTrapEnable" (см. IP-MIB для получения дополнительной информации).

## 7.8 Подготовка к работе коммуникационного канала сигнализации между МТА и CMS

Предполагается, что все вопросы, касающиеся создания и поддержки процессов обслуживания NCS, будут разрешаться средствами DOCSIS. Обсуждение данных вопросов, таким образом, выходит за рамки настоящей Рекомендации.

## 7.9 Замена МТА

В рамках IP-Cablecom не предъявляется никаких специальных требований к процедурам замены МТА. Однако описанные в настоящей Рекомендации процессы последовательности подготовки к работе предоставляют достаточные возможности и являются достаточно гибкими для поддержки замены МТА. В действительности последовательность инициализации замененного МТА может быть идентична последовательности первой инициализации первоначально установленного МТА. Процедуры вспомогательных приложений, связанные с переходом абонента с одного МТА на другой, зависят от сетевых операций конкретного поставщика услуг. В связи с тем, что данные

процедуры могут быть чрезвычайно разнообразными, их обсуждение выходит за рамки данной Рекомендации.

### **7.10 Временная потеря сигнала**

В случае, если в связи с какими-либо факторами, касающимися уровня сигнала (например, временная потеря сигнала) СМ-компонент встроенного МТА выполняет сброс, связанный с ним встроенный МТА IP-Cablecom также ДОЛЖЕН выполнить сброс.

ПРИМЕЧАНИЕ. – Это действие повлияет на активные в данный момент вызовы.

### **7.11 Сценарии полной перезагрузки и частичного сброса МТА**

Под "полной перезагрузкой" понимается процедура включения и последующего включения питания всего устройства встроенного МТА. "Частичным сбросом" называется "сброс SNMP" МТА-компонента встроенного МТА, сброс SNMP СМ-компонента встроенного МТА, что влечет за собой сброс связанного встроенного МТА, или какой-либо фактор, касающийся уровня сигнала, в результате которого происходит сброс СМ, что также влечет за собой сброс связанного МТА.

МТА-компонент встроенного МТА НЕ ДОЛЖЕН использовать разные схемы действий в случае выполнения полной перезагрузки и частичного сброса. В частности это означает, что МТА ДОЛЖЕН использовать одни и те же параметры инициализации (например, таблицы SNMP) и выполнять те же требования, касающиеся долговременного хранения информации (например, хранение мандатов доступа в энергонезависимой памяти NVRAM) как в случае полной перезагрузки, так и в случае частичного сброса.

## **8 Опции DHCP**

DHCP используется для получения IPv4-адресов как для СМ, так и для МТА. Требования СМ и МТА для кодов опций 122 и 60 DHCP подробно описаны в пунктах 8.1 и 8.2. В случае, если общее число октетов(байт) в любой опции DHCP превышает 255(байт) октетов, МТА ДОЛЖЕН разделить сообщение DHCP на несколько вложенных сообщений как описано в RFC 3396.

### **8.1 Опция DHCP 122: Опция конфигурации клиента**

Код Опции DHCP 122 заменяет ранее использовавшуюся опцию 177 согласно RFC (данная опция была предназначена для временного использования). СМ и МТА НЕ ДОЛЖНЫ запрашивать опцию 177 в сообщениях DISCOVER или REQUEST в Опции DHCP 55 (список запрашиваемых параметров). В случае, если СМ и МТА запрашивают и опцию 122, и опцию 177:

- Сервер подготовки к работе ДОЛЖЕН ответить опцией 122 DHCP.
- Сервер подготовки к работе НЕ ДОЛЖЕН отвечать опцией 177 DHCP.
- СМ и МТА ДОЛЖНЫ рассматривать опцию 122 DHCP как приоритетную.

Код Опции DHCP 122 используется в сообщениях OFFER/ACK DHCP СМ и МТА для доставки адресов действующих серверов сети IP-Cablecom и различных данных конфигурации устройств.

Полная информация о кодировании Опции DHCP 122 содержится в RFC 3495 и RFC 3594.

В следующих пунктах содержится дополнительная информация о каждой подопции Опции DHCP 122.

**Таблица 6/J.167 – Опции сервера**

<b>Опция</b>	<b>Под-опция</b>	<b>Описание и комментарии</b>	<b>Обязательная (О) или необязательная (Н) подопция</b>	<b>Значение по умолчанию</b>
122	1	Адрес первичного сервера DHCP поставщика услуг. Требуется только СМ.	О	Нет
	2	Адрес вторичного сервера DHCP поставщика услуг. Необязательное требование СМ.	Н	Пустая строка
	3	Адрес модуля подготовки к работе поставщика услуг	О	Нет
	4	Возврат и повтор AS-REQ/REP-обмена для управления ключами SNMPv3	Н	Согласно объектам MIB: "pktcMtaDevRealmUnsolicitedKeyNomTimeout", "pktcMtaDevRealmUnsolicitedKeyMaxTimeout", "pktcMtaDevRealmUnsolicitedKeyMaxRetries"
	5	Возврат и повтор AP-REQ/REP подготовки к работе с использованием Kerberos	Н	Согласно объектам MIB: "pktcMtaDevProvUnsolicitedKeyNomTimeout" "pktcMtaDevProvUnsolicitedKeyMaxTimeout" "pktcMtaDevProvUnsolicitedKeyMaxRetries"
	6	Область Kerberos модуля SNMP	О	Нет
	7	Использование сервера выдачи мандатов	Н	Нет, если МТА не применяет TGT. В противном случае – 0.
	8	Датчик времени подготовки к работе	Н	Согласно объекту MIB "pktcMtaDevProvisioningTimer" (10 минут)
	9	Признание недействительными мандатов безопасности	Н	0 – применяются обычные правила признания мандатов безопасности недействительными (J.170)

МТА ДОЛЖЕН иметь возможность получать и обрабатывать информацию из всех подопций, приведенных в таблице выше. Сервер подготовки к работе ДОЛЖЕН предоставлять МТА все "обязательные" подопции и МОЖЕТ предоставлять все "необязательные".

В случае, если "необязательная" подопция не предоставлена сервером подготовки к работе, МТА ДОЛЖЕН использовать значение по умолчанию для данной подопции.

В случае, если сервером подготовки к работе не предоставлена "обязательная" подопция, МТА ДОЛЖЕН отвергнуть соответствующие сообщения DHCP OFFER/ACK.

В случае, если подопция содержит неверное (недопустимое) значение, МТА ДОЛЖЕН:

- отвергнуть соответствующие сообщения DHCP OFFER/ACK, если подопция является "обязательной";
- использовать значение по умолчанию, если подопция является "необязательной". В случае, если подопция включает несколько параметров (например опция 122 подопция 4 или опция 122 подопция 5), МТА должен использовать значение по умолчанию только для того параметра или параметров, которые содержат недопустимые значения.

### 8.1.1 Адрес сервера DHCP поставщика услуг (подопция 2)

Адрес сервера DHCP поставщика услуг указывает серверы DHCP, с которых будут приниматься сообщения DHCP OFFER для получения уникального IP-адреса МТА для данного сетевого административного домена поставщика услуг.

Кодирование данных подопций определено в RFC 3495.

Подопция 1 ДОЛЖНА быть включена в сообщения DHCP OFFER/ACK, отправляемые в адрес CM, а также она указывает IP-адрес первичного сервера DHCP. Значением Подопции 1 ДОЛЖЕН быть действительный IP-адрес, значение 255.255.255.255 или значение 0.0.0.0. Значение, которое содержится в подопции 2, ДОЛЖНО представлять собой действительный IP-адрес.

МТА ДОЛЖЕН следовать логике таблицы 7 при определении стратегии DHCP вне зависимости от используемого процесса подготовки к работе.

**Таблица 7/J.167 – Адрес сервера DHCP поставщика услуг (подопция 2)**

Значение подопции 1	Значение подопции 2	
	Действительный IP – сервер DHCP отвечает	Действительный IP – сервер DHCP не отвечает
Действительный IP – сервер DHCP отвечает	МТА ДОЛЖЕН принимать сообщения DHCP OFFER поступающие только с IP-адреса, указанного в подопции 1.	МТА ДОЛЖЕН принимать сообщения DHCP OFFER поступающие только с IP-адреса, указанного в подопции 1.
Действительный IP – сервер DHCP НЕ отвечает	МТА ДОЛЖЕН предпринять как минимум 3 повторные попытки с экспоненциальным увеличением времени ожидания между попытками перед тем, как принять сообщение DHCP OFFER от сервера DHCP, указанного в подопции 2.	МТА ДОЛЖЕН вернуться к шагу МТА1.
255.255.255.255	МТА ДОЛЖЕН выбирать сообщения OFFER согласно логике RFC 2131. Значение подопции 2 ДОЛЖНО быть проигнорировано.	МТА ДОЛЖЕН выбирать сообщения OFFER согласно логике RFC 2131. Значение подопции 2 ДОЛЖНО быть проигнорировано.
0.0.0.0	МТА ДОЛЖЕН прекратить попытки подготовки к работе, а также все остальные действия.	МТА ДОЛЖЕН прекратить попытки подготовки к работе, а также все остальные действия.

### 8.1.2 Адрес модуля подготовки к работе поставщика услуг (подопция 3)

Адрес модуля подготовки к работе поставщика услуг является сетевым адресом сервера подготовки к работе для данного сетевого административного домена поставщика голосовых услуг.

Кодирование данной подопции определено в RFC 3495. Данный адрес ДОЛЖЕН быть сконфигурирован только в качестве FQDN.

Значение FQDN 0.0.0.0 в подопции 3 действительного DHCP OFFER/ACK МТА определяет, что МТА ДОЛЖЕН завершить работу и не пытаться подготавливаться к работе до тех пор, пока он не будет реинициализирован CM. Это объясняется в шаге МТА2 процесса подготовки к работе в п. 7.2.

Компонент "адрес модуля подготовки к работе поставщика услуг" ДОЛЖЕН иметь возможность принимать прерывания SNMP.

Подопция 3 ДОЛЖНА быть включена в сообщение DHCP OFFER, отправляемое в адрес МТА.

### 8.1.3 Возврат и повтор AS-REQ/REP-обмена для управления ключами SNMPv3 (подопция 4)

МТА ДОЛЖЕН использовать опцию DHCP 122 подопцию 4, если она включена, только в случае применения защищенного процесса. Механизм возврата и повторного запуска обмена AS-REQ/REP передачи ключа SNMPv3 с использованием Kerberos, определенный в Рек. МСЭ-Т J.170, управляется

значениями, содержащимися в данной подопции, или значениями по умолчанию соответствующих объектов MIB из таблицы области в случае, если данная подопция не включена в Опцию DHCP 122.

Кодирование данной подопции определено в RFC 3495.

Номинальное значение периода ожидания (timeout) данной подопции соответствует объекту MIB `pkcMtaDevRealmUnsolicitedKeyNomTimeout` в таблице `pkcMtaDevRealmTable`.

Максимальное значение периода ожидания (timeout) данной подопции соответствует объекту MIB `pkcMtaDevRealmUnsolicitedKeyMaxTimeout` в таблице `pkcMtaDevRealmTable`.

Максимальное количество повторных попыток данной подопции соответствует объекту MIB `pkcMtaDevRealmUnsolicitedKeyMaxRetries` в таблице `pkcMtaDevRealmTable`.

МТА также ДОЛЖЕН иметь возможность извлекать указанные выше параметры из данной подопции, если они переданы ему сервером подготовки к работе.

Сервер подготовки к работе МОЖЕТ передать МТА указанные выше параметры в данной подопции.

В случае, если какое-либо из значений, определенных в данной подопции, равно "FFFFFFFF" (шестнадцатеричный формат), ДОЛЖНО быть использовано значение по умолчанию соответствующего столбца таблицы `Realm`.

#### **8.1.4 Возврат и повтор AP-REQ/REP подготовки к работе с использованием Kerberos (подопция 5)**

МТА ДОЛЖЕН использовать Опцию DHCP 122 подопцию 5, если она включена, только в случае применения защищенного процесса. Механизм возврата и повторного запуска обмена AP-REQ/REP передачи ключа SNMPv3 с использованием Kerberos, определенный в Рек. МСЭ-Т J.170, управляется значениями, содержащимися в данной подопции.

Кодирование данной подопции определено в RFC 3495.

Номинальное значение периода ожидания (timeout) данной подопции соответствует объекту MIB `pkcMtaDevProvUnsolicitedKeyNomTimeout`.

Максимальное значение периода ожидания (timeout) данной подопции соответствует объекту MIB `pkcMtaDevProvUnsolicitedKeyMaxTimeout`.

Максимальное количество повторных попыток данной подопции соответствует объекту MIB `pkcMtaDevProvUnsolicitedKeyMaxRetries`.

МТА также ДОЛЖЕН иметь возможность извлекать указанные выше параметры из данной подопции, если они переданы ему сервером подготовки к работе.

Сервер подготовки к работе МОЖЕТ передать МТА указанные выше параметры в данной подопции.

В случае, если какое-либо из значений, определенных в данной подопции, равно "FFFFFFFF" (шестнадцатеричный формат), ДОЛЖНО быть использовано значение по умолчанию соответствующего объекта MIB.

#### **8.1.5 Область Kerberos модуля SNMP (подопция 6)**

Вместе с адресом модуля подготовки к работе область Kerberos используется как средство связи с модулем SNMP в области подготовки к работе. Имя области используется для выполнения сервером DNS поиска для KDC области.

Опция DHCP 122 подопция 6 ДОЛЖНА включаться в сообщение DHCP OFFER, отправляемое в адрес МТА. В случае использования защищенного процесса Опция DHCP 122 подопция 6 ДОЛЖНА содержать только имя области в формате FQDN (тип=0 согласно RFC 3495).

МТА ДОЛЖЕН выбирать соответствующий процесс подготовки к работе согласно таблице 8 (сравнение содержимого Опции DHCP 122 подопции 6 производится с учетом регистра, все буквы значений ДОЛЖНЫ быть заглавными).

**Таблица 8/J.167 – Выбор процесса подготовки к работе МТА**

Содержимое Опции DHCP 122 подопции 6	Выбор процесса подготовки к работе МТА
BASIC.1	В случае, если значение Опции DHCP 122 подопции 6 "BASIC.1" (без кавычек), МТА ДОЛЖЕН выполнить базовый процесс без отправки информационного сообщения о завершении подготовки к работе (SNMP INFORM)
BASIC.2	В случае, если значение Опции DHCP 122 подопции 6 "BASIC.2" (без кавычек), МТА ДОЛЖЕН выполнить базовый процесс с отправкой информационного сообщения о завершении подготовки к работе (SNMP INFORM)
HYBRID.1	В случае, если значение Опции DHCP 122 подопции 6 "HYBRID.1" (без кавычек), МТА ДОЛЖЕН выполнить гибридный процесс без отправки информационного сообщения о завершении подготовки к работе (SNMP INFORM)
HYBRID.2	В случае, если значение Опции DHCP 122 подопции 6 "HYBRID.2" (без кавычек), МТА ДОЛЖЕН выполнить гибридный процесс с отправкой информационного сообщения о завершении подготовки к работе (SNMP INFORM)

В случае, если в Опции DHCP 122 подопции 6 указано какое-либо другое значение, МТА ДОЛЖЕН выполнить защищенный процесс. Кодирование Опции DHCP 122 подопции 6 для защищенного процесса определено в RFC 3495.

#### **8.1.5.1 Установка ключа SNMPv3**

Установка ключа SNMPv3 применяется только при использовании защищенного процесса. В начальной фазе подготовки к работе МТА использует AP Request/AP Reply, описанные на рисунке 6, сопутствующее описание процесса, а также спецификацию безопасности для установки ключей безопасности вида "МТА-Prov-xx:xx:xx:xx:xx:xx", где xx:xx:xx:xx:xx:xx представляет собой MAC-адрес МТА (все буквы заглавные), с пользователем USM (модель безопасности, определённая пользователем, User-based Security Model) SNMPv3. МТА ДОЛЖЕН присвоить данному пользователю значение в USM MIB, описанной в RFC 3414, предусмотрев возможность использования ключа с применением метода управления ключами Kerberos IPCablecom, описанного в спецификации безопасности. Аутентификация SNMPv3 является обязательной, обеспечение конфиденциальности необязательно. Перечень допустимых алгоритмов аутентификации и конфиденциальности SNMPv3 приведен в Рек. МСЭ-Т J.170.

Дополнительно, для параметра usmUserSecurityName ДОЛЖНО быть установлено значение "МТА-Prov-xx:xx:xx:xx:xx:xx" (без кавычек) где xx:xx:xx:xx:xx:xx представляет собой MAC-адрес МТА (все буквы заглавные). Таким образом гарантируется, что для каждого МТА будет создан уникальный usmUserSecurityName.

В первую очередь МТА ДОЛЖЕН получить мандат на обслуживание для области подготовки к работе, как описано в шаге МТА9. Управление ключами USM осуществляется по протоколу UDP, как указано в Рек. МСЭ-Т J.170. Ключи SNMPv3 устанавливаются прежде, чем происходит какой-либо обмен информацией по протоколу SNMPv3, таким образом сообщения SNMPv3 всегда ДОЛЖНЫ быть аутентифицированы, при этом конфиденциальность является необязательной.

МТА ДОЛЖЕН использовать созданного как описано выше пользователя USM в первоначальном информационном сообщении (initial INFORM).

#### **8.1.6 Использование сервера выдачи мандатов (подопция 7)**

МТА ДОЛЖЕН использовать Опцию DHCP 122 подопцию 7, если она включена, для управления ключами с использованием Kerberos при подготовке к работе только в случае применения защищенного процесса. Значение данной подопции содержит переменную булевского типа, значение которой "истина" указывает, что МТА СЛЕДУЕТ получить TGT (Ticket Granting Ticket).

Подопция 7 МОЖЕТ включаться в сообщения DHCP OFFER/ACK, отправляемые в адрес МТА.

Кодирование данной подопции определено в RFC 3495.

### **8.1.7 Датчик времени подготовки к работе (подопция 8)**

Подопция 8 определяет значение, которое должно будет использоваться для датчика времени подготовки к работе. Подопция 8 МОЖЕТ включаться в сообщения DHCP OFFER/ACK, отправляемые в адрес МТА.

Кодирование данной подопции определено в RFC 3495.

### **8.1.8 Признание недействительными мандатов безопасности (подопция 9)**

Подопция 9 содержит битовую маску, которая предписывает МТА признавать недействительными определенные мандаты безопасности сервера приложений. Подопция 8 МОЖЕТ включаться в сообщения DHCP OFFER/ACK, отправляемые в адрес МТА.

Кодирование данной подопции определено в RFC 3594.

## **8.2 Опция DHCP 60: Идентификатор производителя клиента**

Опция 60 содержит строку, показывающую технические возможности МТА. МТА ДОЛЖЕН отправлять в Опции DHCP 60 следующую строку кода ASCII: "pktcl.0:xxxxxx", где xxxxxx ДОЛЖНО представлять собой ASCII-представление шестнадцатеричного кода закодированной способом TLV информации о возможностях МТА, как определено в п.10.

## **8.3 Опции DHCP 12 и 15**

В опциях 12 и 15 в адрес встроенного МТА ДОЛЖНО быть отправлено FQDN МТА. В опции 12 ДОЛЖНА содержаться часть FQDN "Имя узла", а в опции 15 – часть FQDN "Имя домена".

Например, если FQDN МТА – "mta1.pclab.com", то в опции 12 должно содержаться "mta1", а в опции 15 – "pclab.com".

## **8.4 Опция DHCP 6**

С помощью Опции DHCP 6 МТА получает список адресов своих серверов DNS. В опции 6 ДОЛЖЕН содержаться по крайней мере один адрес сервера DNS. Опция 6 может содержать адрес вторичного сервера DNS. В случае, если опция содержит более чем два адреса, МТА ДОЛЖЕН использовать первые два.

## **8.5 Опция DHCP 43**

МТА ДОЛЖЕН включать Опцию DHCP 43 в сообщения DHCP DISCOVER и DHCP REQUEST при использовании защищенного, гибридного и базового процессов.

В опции 43 содержится количество подопций, определенных для передачи вспомогательным системам специфической информации об устройстве МТА. В опции 43 подопции 1–10, 31 и 32 определены в рамках IPCablecom, подопции 11–30 зарезервированы для использования в Рекомендациях IPCable2Home (серии J.19x), подопции 33–50 зарезервированы для IPCablecom, подопции 51–127 зарезервированы для стандартизации использования в будущем, а подопции 128 и далее – для использования производителем. Подопции Опции DHCP 43 ДОЛЖНЫ использоваться в формате "Закапсулированные расширения производителя" ("Encapsulated vendor-specific extensions" (RFC 2132).

В таблице 9 приведены подопции Опции DHCP 43, которые ДОЛЖНЫ использоваться МТА. МТА ДОЛЖЕН отправлять все перечисленные в приведенной ниже таблице подопции за исключением случаев, когда иное предписывается в явном виде. В случае, если количество октетов (байт) всех подопций Опции DHCP 43 вместе взятых превышает 255, МТА ДОЛЖЕН воспользоваться указаниями RFC 3396 для того, чтобы разделить опцию на несколько опций меньшего размера.

Таблица 9/J.167 – Синтаксис Опции DHCP 43

Подопция Опции DHCP 43 MTA	Обязательная (О)/ не используется в Опции DHCP 43 (Н)	Значение	Описание
Подопция 1	Н		Вектор данной подопции в запросе представляет собой перечень подопций (входящих в опцию 43), которые сервер должен вернуть клиенту в ответе на запрос. Никакие подопции не определены. MTA НЕ ДОЛЖЕН использовать подопцию 1 Опции DHCP 43, а сервер подготовки к работе ДОЛЖЕН проигнорировать ее в случае обнаружения.
Подопция 2	О	<DevType> (тип устройства)	Подопция 2 содержит тип устройства компонента, выполняющего запрос DHCP. MTA ДОЛЖЕН отправлять подопцию 2 Опции DHCP 43. Допустимые типы устройств для MTA IPCablecom: – "EMTA" – для встроенных MTA – "SMTA" – для S-MTA (Standalone MTA, автономный MTA)
Подопция 3	Н		В подопции 3 содержится разделенный двоеточиями перечень всех компонентов устройства eDOCSIS (встроенный DOCSIS). Данный перечень используется встроенным CM (CM-компонент встроенного MTA) eDOCSIS. MTA НЕ ДОЛЖЕН отправлять подопцию 3 Опции DHCP 43, а сервер подготовки к работе ДОЛЖЕН проигнорировать ее в случае обнаружения.
Подопция 4	О	<device serial number> (серийный номер устройства)	Подопция 4 содержит серийный номер устройства, представленный в виде строки ASCII. MTA ДОЛЖЕН отправлять подопцию 4 Опции DHCP 43. Значение подопции 4 Опции DHCP 43 ДОЛЖНО совпадать со значением объекта MIB pktcMtaDevSerialNumber
Подопция 5	О	<Hardware version> (версия аппаратного обеспечения)	Подопция 5 содержит номер версии аппаратного обеспечения устройства, представленный в виде строки ASCII. MTA ДОЛЖЕН отправлять подопцию 5 Опции DHCP 43. Значение подопции 5 Опции DHCP 43 ДОЛЖНО совпадать со значением версии аппаратного обеспечения (Hardware Version), указанным в поле <Hardware Version> объекта MIB II sysDescr.
Подопция 6	О	<Software version> (версия программного обеспечения)	Подопция 6 содержит номер версии программного обеспечения устройства, представленный в виде строки ASCII. MTA ДОЛЖЕН отправлять подопцию 6 Опции DHCP 43. Значение подопции 6 Опции DHCP 43 ДОЛЖНО совпадать со значением объекта MIB pktcMtaDevSwCurrentVers.

**Таблица 9/J.167 – Синтаксис Опции DHCP 43**

Подопция Опции DHCP 43 МТА	Обязательная (О)/ не используется в Опции DHCP 43 (Н)	Значение	Описание
Подопция 7	О	<Boot ROM Version> (Версия загрузочного ROM)	Подопция 7 содержит номер версии Boot ROM, представленный в виде строки ASCII. МТА ДОЛЖЕН отправлять подопцию 7 Опции DHCP 43. Значение подопции 7 Опции DHCP 43 ДОЛЖНО совпадать с содержимым поля <Boot ROM Version> объекта MIB II sysDescr.
Подопция 8	О	<OUI> (Уникальный организационный идентификатор)	В подопции 8 содержится OUI (Organizational Unique Identifier, Уникальный организационный идентификатор), в виде шестнадцатеричного представления строки, состоящей из 3 восьмиразрядных байтов. Он МОЖЕТ совпадать с OUI, содержащимся в MAC-адресе МТА. МТА ДОЛЖЕН отправлять подопцию 8 Опции DHCP 43. В случае, если данная подопция опущена, сервер подготовки к работе ДОЛЖЕН использовать MAC-адрес МТА в качестве OUI МТА.
Подопция 9	О	<Model Number> (номер модели)	Подопция 9 содержит номер модели устройства МТА, представленный в виде строки ASCII. МТА ДОЛЖЕН отправлять подопцию 9 Опции DHCP 43. Значение подопции 9 Опции DHCP 43 ДОЛЖНО совпадать с содержимым поля <Model Number> объекта MIB II sysDescr.
Подопция 10	О	<Vendor Name> (Наименование производителя)	Подопция 10 содержит Наименование производителя, представленное в виде строки ASCII. МТА ДОЛЖЕН отправлять подопцию 10 Опции DHCP 43. Значение подопции 10 Опции DHCP 43 ДОЛЖНО совпадать с содержимым поля <Vendor Name> объекта MIB II sysDescr.
Подопции 11–30			Зарезервировано для использования в рамках проекта IPCableHome
Подопция 31	О	<MTA MAC Address> (MAC-адрес МТА)	Подопция 31 содержит MAC-адрес МТА, представленный в виде строки, состоящей из 6 восьмиразрядных байтов. МТА ДОЛЖЕН отправлять подопцию 31 Опции DHCP 43. Значение подопции 31 Опции DHCP 43 ДОЛЖНО совпадать со значением объекта MIB pkteMtaDevMacAddress.

**Таблица 9/J.167 – Синтаксис Опции DHCP 43**

<b>Подопция Опции DHCP 43 MTA</b>	<b>Обязательная (О)/ не используется в Опции DHCP 43 (Н)</b>	<b>Значение</b>	<b>Описание</b>
Подопция 32	О	<Correlation ID> (идентификатор взаимосвязи)	Подопция 32 содержит номер Correlation ID, представленный в виде 4-байтового целого, порядок байтов сетевой. MTA ДОЛЖЕН отправлять подопцию 32 Опции DHCP 43. Значение подопции 31 Опции DHCP 43 ДОЛЖНО совпадать со значением объекта MIB pkcMtaDevCorrelationId.
Подопции 33–50			Зарезервировано для использования в рамках проекта IPCablecom.
Подопции 51–127			Зарезервировано для использования CableLabs.
Подопции 128–254			Зарезервировано для использования производителями.

### **8.6 Опция DHCP 1**

Опция DHCP 1 определена в RFC 2132.

### **8.7 Опция DHCP 3**

Опция DHCP 3 определена в RFC 2132.

## **9 Подготавливаемые к работе атрибуты MTA**

В данном пункте приводится перечень атрибутов и их свойств, используемых в ходе подготовки к работе устройства. Все подготавливаемые к работе атрибуты, приведенные в данном пункте, МОГУТ быть изменены при помощи файла данных конфигурации или с использованием SNMP для каждого конкретного атрибута.

Требованием IPCablecom является обеспечение всех встроенных MTA файлом данных конфигурации MTA в течение процесса регистрации. Во время инициализации устройства нет необходимости в активации голосовых услуг на конечных точках. Информация о конфигурации MTA уровня устройства ДОЛЖНА быть предоставлена в процессе инициализации. Сведения по данным вопросам содержатся в п. 9.1.1.

Длина URL информации о конфигурации MTA, сформированного приложением подготовки к работе, НЕ ДОЛЖНА превышать 255 байт и не должна быть нулевой. Так как данное имя файла предоставляется MTA приложением подготовки к работе в процессе регистрации, нет необходимости устанавливать соглашения об именовании файлов.

### **9.1 Файл конфигурации MTA**

В данном пункте описываются формат и содержание файла конфигурации MTA. В этом файле содержится серия параметров типа "type length value" (TLV). Каждый TLV-параметр в файле конфигурации описывает атрибут MTA или конечной точки. Этот файл данных конфигурации состоит из TLV-параметров с доступом "чтение-запись", "только чтение" или недоступных MIB. Все доступные MIB параметры файла конфигурации, за исключением конкретно указанных, ДОЛЖНЫ быть определены с использованием TLV-типа 11 DOCSIS, TLV-типа 64 IPCablecom или TLV-типа 38 IPCablecom. Тип TLV 64 определен в рамках IPCablecom и отличается от типа TLV 11 DOCSIS тем, что значение длины (length) занимает 2 байта, в то время как в TLV 11 DOCSIS – 1 байт. Тип TLV 64 ДОЛЖЕН применяться в случае, если длина превышает 254 байта. В случае необходимости информация производителя может быть добавлена к файлу конфигурации при помощи формата TLV-43, предназначенного для производителей. Данный формат TLV описан в спецификации DOCSIS (Рек. МСЭ-Т J.112). Производители НЕ ДОЛЖНЫ использовать форматы TLV 11 или TLV 64 для предоставления

специфической информации производителя. Формат TLV-38 определен в рамках IPcablecom и является аналогом формата TLV-38, используемого в DOCSIS и IPcable2Home. MTA ДОЛЖЕН иметь возможность обрабатывать форматы TLV, приведенные в таблице 10:

**Таблица 10/J.167 – Файл конфигурации MTA**

Тип	Длина	Значение
11	n, где n равен 1 байту	связка переменных (variable binding)
64	m, где m равен 2 байтам	связка переменных (variable binding)
38	n, где n равен 1 байту	Составное (Содержит вложенные TLV)
254	1 байт	0xFE для начала файла и 0xFF для конца файла
ПРИМЕЧАНИЕ. – где это возможно, использование TLV 11 является предпочтительным по сравнению с использованием TLV 64		

Новые форматы TLV, вводимые в действие в рамках IPcablecom в будущем, должны иметь размер "поля длины" равный 2 байтам.

Тип данных VarBind кодируется в базовых правилах кодирования ASN.1 точно так же, как если бы он был частью запрос SNMP Set.

Файл конфигурации MTA ДОЛЖЕН начинаться с управляющего кода "начало файла конфигурации телефонии ("telephony configuration file start")" и заканчиваться управляющим кодом "конец файла конфигурации телефонии ("telephony configuration file end")". Данные управляющие коды позволяют отличить параметры MTA TLV от параметров DOCSIS TLV. Также данные управляющие коды служат определяющими указателями на начало и конец файла конфигурации MTA.

Файл конфигурации MTA ДОЛЖЕН содержать атрибуты, обозначенные как "обязательные" в таблице данных конфигурации уровня устройства, приведенной в п.9.1.1; в противном случае MTA ДОЛЖЕН отвергнуть файл конфигурации и предпринять необходимые шаги, описанные в п.7.2 (Сбой на шаге 23 в связи с "Ошибкой в файле конфигурации"). Файл конфигурации MTA МОЖЕТ содержать любые атрибуты из числа обозначенных как "необязательные" в таблице данных конфигурации уровня устройства. В случае, если файл конфигурации не содержит обязательных атрибутов, он должен быть отвергнут. Файл конфигурации MTA ДОЛЖЕН отправляться встроенному MTA каждый раз, когда происходит включение питания этого устройства.

Данные уровня устройства по услугам МОГУТ быть переданы MTA как часть файла конфигурации или отправлены посредством SNMP. В случае, если данные включаются в файл конфигурации, он ДОЛЖЕН содержать все атрибуты, обозначенные как "обязательные" в таблице данных конфигурации уровня устройства, если таковые имеются. Файл конфигурации MTA МОЖЕТ дополнительно содержать любые атрибуты из числа обозначенных как "необязательные" в таблице данных конфигурации уровня устройства.

В случае, если требуется предоставление голосовых услуг на MTA на любой конечной точке, ДОЛЖНЫ быть выполнены следующие действия:

- 1) Для pktcMtaDevEnabled ДОЛЖНО быть установлено значение TRUE (истина);
- 2) Информация о конфигурации для конкретной конечной точки ДОЛЖНА быть предоставлена либо посредством файла конфигурации MTA (в течение подготовки к работе), либо путем подготовки к работе конечных точек с использованием SNMP по завершении подготовки к работе MTA.

Детальная информация по конечной точке, если таковая предоставляется, ДОЛЖНА содержать все атрибуты, обозначенные как "обязательные" в таблице данных конфигурации для конкретной конечной точки, приведенной в п.9.1.3. Файл конфигурации MTA МОЖЕТ дополнительно содержать любые атрибуты из числа обозначенных как "необязательные" в таблице данных конфигурации для

конкретной конечной точки, приведенной в п.9.1.3. Информация о конфигурации для конкретной конечной точки ДОЛЖНА отправляться МТА, когда активируется услуга голосовой связи.

Следует отметить, что Данные уровня устройства по услугам и данные конфигурации для конкретной конечной точки могут быть отправлены МТА посредством пошаговой подготовки к работе с использованием SNMP. МТА ДОЛЖЕН поддерживать пошаговую подготовку к работе.

МТА ДОЛЖЕН иметь возможность обрабатывать все значения TLV-11 и TLV-64 со связками переменных, содержащие все объекты MIB, определенные в Рек. МСЭ-Т J.166, если иное не предписано.

Для получения информации о синхронизации атрибутов подготовки к работе со вспомогательными системами см. п. 7.6.1.

При использовании защищенного или гибридного процессов подготовки к работе МТА ДОЛЖЕН аутентифицировать файл конфигурации в соответствии со спецификацией безопасности IPCablecom J.170; МТА ДОЛЖЕН отвергнуть файл конфигурации в случае, если аутентификация не проходит и предпринять соответствующие шаги, указанные в п. 7.2 для защищенного и в п.7.4. для гибридного процесса. В случае, если файл конфигурации содержит объект MIB 'pkcMtaDevProvConfigHash' при использовании защищенного или гибридного процессов МТА ДОЛЖЕН проигнорировать значение данного объекта MIB, продолжить обработку файла конфигурации, отправить отчет passWithWarnings (успешно с предупреждениями) и заполнить таблицу Error OID (Идентификаторы ошибок в объектах)(pkcMtaDevErrorOidsTable).

В случае использования базового процесса, сервер подготовки к работе и МТА ДОЛЖНЫ поддерживать процедуру проверки файла конфигурации, описанную ниже:

- 1) Когда сервер подготовки к работе создает новый файл конфигурации МТА или изменяет существующий, предназначенный для передачи МТА с использованием базового процесса, он ДОЛЖЕН вычислить SHA-1 хеш содержимого всего файла конфигурации МТА, включая маркеры начала и конца, взятого как строка байтов.
- 2) Сервер подготовки к работе ДОЛЖЕН добавить полученное на шаге 1 значение хеша к файлу конфигурации МТА в форме триплета TLV-11, соответствующего объекту MIB 'pkcMtaDevProvConfigHash'. Сервер подготовки к работе ДОЛЖЕН поместить данный триплет TLV-11 перед маркером конца файла конфигурации. Сервер подготовки к работе НЕ ДОЛЖЕН изменять порядок элементов TLV файла конфигурации после того, как был вычислен хеш. Далее файл конфигурации делается доступным для МТА на соответствующем сервере TFTP/HTTP.
- 3) По получении файла конфигурации МТА ДОЛЖЕН выполнить следующее: в случае, если объект 'pkcMtaDevProvConfigHash' отсутствует, МТА ДОЛЖЕН отвергнуть данный файл конфигурации и отправить отчет 'failOtherReason' (Сбой по прочим причинам).

В случае, если объект MIB 'pkcMtaDevProvConfigHash' присутствует, МТА ДОЛЖЕН:

- a) Вычислить SHA-1 хеш содержимого полученного файла конфигурации без учета триплета TLV-11, содержащего 'pkcMtaDevProvConfigHash' и записать вычисленное значение в объект MIB pkcMtaDevProvConfigHash. МТА ДОЛЖЕН сохранять порядок элементов TLV для обеспечения корректности расчета.
- b) Если вычисленное значение хеша и значение объекта MIB 'pkcMtaDevProvConfigHash' совпадают, проверка целостности файла завершена успешно и МТА ДОЛЖЕН принять файл конфигурации на дальнейшую обработку; в противном случае МТА ДОЛЖЕН отвергнуть данный файл конфигурации и отправить отчет 'failOtherReason' (Сбой по прочим причинам).

МТА также должен проверить файл конфигурации на наличие ошибок. Как описано выше, ошибки в обязательных параметрах ДОЛЖНЫ рассматриваться как ошибки в файле конфигурации и соответствующие шаги ДОЛЖНЫ предприниматься (Сбой на шаге МТА23 в связи с "Ошибкой в файле конфигурации").

В случае наличия ошибок в необязательных параметрах МТА ДОЛЖЕН принять данный файл конфигурации, но отправить тот же отчет о статусе (на шаге МТА25).

В случае, если файл конфигурации содержит данные для конкретного CMS или параметры для конкретных конечных точек, относящиеся к CMS, еще не связанному с конечными точками, МТА НЕ ДОЛЖЕН устанавливать защищенные соединения до тех пор, пока конечные точки не получат привязку к этому конкретному CMS (при помощи SNMP или перенаправления NCS).

МТА ДОЛЖЕН отправить отчет о состоянии полученного файла конфигурации в информационном сообщении об окончании подготовки к работе (шаг МТА25 в процессе подготовки к работе), как описано ниже:

- Если файл конфигурации удалось проанализировать успешно и МТА способен отразить соответствующие значения параметров в МІВ, он должен вернуть 'pass' (успех).
- Если в файле конфигурации была обнаружена ошибка (некорректное значение обязательных параметров) МТА ДОЛЖЕН отвергнуть данный файл и вернуть 'failConfigFileError' (Сбой из-за ошибки в файле конфигурации).
- МТА также ДОЛЖЕН записать в таблицу 'pktcMtaDevErrorOidsTable' параметр, содержащий некорректное значение. Он также МОЖЕТ записать в таблицу 'pktcMtaDevErrorOidsTable' другие ошибки/предупреждения, если файл удалось проанализировать до конца.
- Если значения обязательных параметров в файле конфигурации верны, но есть ошибки в необязательных параметрах (сюда включаются любые определяемые производителем параметры, значение которых некорректно или неизвестно МТА), МТА ДОЛЖЕН вернуть 'passWithWarnings' (успешно с предупреждениями).
- Он также ДОЛЖЕН записать в таблицу populate 'pktcMtaDevErrorOidsTable' список всех отвергнутых параметров с указанием причин. МТА также ДОЛЖЕН использовать для всех таких параметров значения по умолчанию, если они не были заменены какими-либо другими способами (например с помощью DHCP). В таких случаях МТА ДОЛЖЕН использовать те значения, на которые были заменены некорректные значения.
- Если файл конфигурации не содержит ошибок, но МТА не способен отразить соответствующие значения параметров в МІВ (например, если имеется слишком большое число параметров, что ведет к переполнению памяти), он ДОЛЖЕН принять информацию, касающуюся CMS, связанных с конечными точками и вернуть 'passWithIncompleteParsing' (успех с неоконченным анализом).
- МТА также ДОЛЖЕН записать в таблицу 'pktcMtaDevErrorOidsTable' список всех параметров, значения которых не удалось отразить в МІВ.
- Если файл конфигурации не может быть проанализирован из-за внутренней ошибки, МТА ДОЛЖЕН вернуть 'failureInternalError' (сбой из-за внутренней ошибки). Ему также СЛЕДУЕТ попытаться записать в таблицу 'pktcMtaDevErrorOidsTable' параметры, приведшие к ошибке.
- Если МТА не может принять файл конфигурации по каким-либо причинам, отличным от перечисленных выше, он ДОЛЖЕ вернуть 'failureOtherReason' (сбой по прочим причинам). Ему также СЛЕДУЕТ попытаться записать в таблицу 'pktcMtaDevErrorOidsTable' параметры, приведшие к ошибке.

Файл конфигурации МТА ДОЛЖЕН содержать информацию о конфигурации по конкретной области. В случае использования защищенного процесса подготовки к работе данные о конфигурации по конкретной области ДОЛЖНЫ содержать как минимум данные, касающиеся области подготовки к работе, указанной в Опции DHCP 122 подопции 6.

В случае использования защищенного процесса подготовки к работе по получении файла конфигурации МТА ДОЛЖЕН проверить следующее:

- Значение объекта МІВ "pktcMtaDevRealmName" в таблице области (Realm Table) ДОЛЖНО совпадать с именем области (Realm Name), переданным в адрес МТА в Опции DHCP 122 подопции 6.
- Значение объекта МІВ "pktcMtaDevRealmOrgName" таблице области ДОЛЖНО совпадать со значением атрибута "Наименование организации" ("Organization Name") в Сертификате поставщика услуг.
- Шифрование и аутентификацию файла конфигурации МТА согласно Рек. МСЭ-Т J.170.

МТА ДОЛЖЕН рассматривать возникновение сбоя на любом из приведенных выше этапов проверки как сбой на шаге МТА23 процесса подготовки к работе и ДОЛЖЕН отвергнуть файл конфигурации.

Если МТА встречает определяемый производителем элемент TLV-43 с идентификатором производителя, который не опознается МТА как его собственный, МТА ДОЛЖЕН проигнорировать данный элемент TLV-43 и продолжить обработку файла конфигурации. Если МТА фиксирует присутствие элемента TLV неизвестного формата (отличного от TLV-11, TLV-43, TLV-64, TLV-38, и TLV-254), МТА ДОЛЖЕН проигнорировать данный элемент TLV предположив, что размер "поля длины" неустановленного формата TLV составляет 2 байта и продолжить обработку. МТА ДОЛЖЕН отправить отчет о статусе инициализации `passWithWarnings` и заполнить таблицу `pktcMtaDevErrorOidsTable`, если фиксирует присутствие неустановленного формата TLV. Если МТА встречает нераспознаваемую связку переменных в элементах формата TLV-11 или TLV-64, он ДОЛЖЕН проигнорировать данную связку, отправить отчет о статусе инициализации `passWithWarnings` и заполнить таблицу `pktcMtaDevErrorOidsTable`. Производителям настоятельно рекомендуется уделять большое внимание обратной совместимости с предыдущими версиями при изменении существующих или вводе новых вложенных TLV для TLV-43.

МТА ДОЛЖЕН принимать файл конфигурации, содержащий допустимый набор информации о конфигурации для конкретного CMS или конкретной области, описанной в п.9.1.4 и 9.1.5, даже в том случае, если конечные точки МТА не связаны с CMS, указанным в информации о конфигурации для конкретного CMS.

Объекты MIB `IPcablecom` в МТА-MIB (Рек. МСЭ-Т J.166), `Signaling-MIB` (Рек. МСЭ-Т J.166) и `Event-MIB` (Рек. МСЭ-Т J.166) типа `RowStatus` НЕ ДОЛЖНЫ включаться в файл конфигурации МТА. В случае, если какой-либо объект MIB (`MIB` МТА, `Signaling MIB` или `Event MIB`) типа `RowStatus` включается в файл конфигурации, МТА ДОЛЖЕН проигнорировать значение любого объекта типа `RowStatus`, отправить отчет о статусе инициализации `passWithWarnings` и соответствующим образом заполнить таблицу `pktcMtaDevErrorOidsTable`. Вне зависимости от шагов, предпринятых МТА, он ДОЛЖЕН правильно записать в таблицу Идентификаторов ошибок в объектах идентификатор объекта `RowStatus`. В файле конфигурации МТА могут присутствовать или отсутствовать не-`IPcablecom` объекты MIB типа `RowStatus` и МТА ДОЛЖЕН обработать данные объекты согласно соответствующим RFC для конкретных объектов MIB (например, таблице `SMNPv2c`).

Если в файл конфигурации МТА включен объект MIB `pktcEnMtaDevMtplGrantsPerInterval`, он присутствует для того, чтобы активировать функцию "множественного предоставления канала в течение одного интервала" (`Multiple Grants per Interval (MGPI)`), и если МТА не поддерживает данную функцию, он ДОЛЖЕН проигнорировать данный объект и отправить отчет 'PassWithWarnings' и соответствующим образом заполнить таблицу Идентификаторов ошибок в объектах.

### 9.1.1 Информация о конфигурации уровня устройства

Для получения более подробной информации относительно данных атрибутов и их значений по умолчанию см. МТА MIB (МСЭ-Т Рек. J.166) (см. таблицу 11).

- Сертификат производителя МТА подтверждает Сертификат устройства МТА.

**Таблица 11/J.167 – Конфигурации уровня устройства**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
Telephony Config File Start (Начало файла конфигурации телефонии)	Целое число	3, обязательное	Нет	Недоступно	Недоступно	Тип Длина Значение (Type) (Length) (Value) 254 1 1 Файл конфигурации MTA ДОЛЖЕН начинаться с этого атрибута
Telephony Config File End (Конец файла конфигурации телефонии)	Целое число	3, обязательное	Нет	Недоступно	Недоступно	Тип Длина Значение (Type) (Length) (Value) 254 1 255 Этот атрибут ДОЛЖЕН быть последним в файле конфигурации MTA
Telephony MTA Admin State (Административный статус телефонии MTA)	Перечень	3, обязательное	Ч/З	MIB устройства MTA	pktcMtaDev Enabled	Используется для подключения/отключения всех портов телефонии на MTA. Применяется к MTA-компоненту встроенного MTA или автономному MTA целиком. Позволяет осуществлять общее управление всеми портами телефонии (внешними интерфейсами) на устройстве. Статус MTA контролируется данным объектом MIB. Для получения более подробной информации об этом объекте см. MIB MTA (J.166).
Realm Organization Name (Наименование организации области)	Строка	3, обязательное (защищенный процесс подготовки к работе.) 3, необязательное (базовый и гибридный процессы)	Ч/З	MIB устройства MTA	pktcMtaDev RealmOrg Name	Значение атрибута "Наименование организации" в имени X.500 в имени субъекта Сертификата поставщика услуг.
Solicited Key Timeout (Обязательное время действия ключа)	Целое число	3, необязательное	Ч/З	Недоступно	pktcMtaDev ProvSolicitedKey Timeout	Данное время действия ключа применяется только в случае, если сервер подготовки к работе инициировал действия по управлению ключами для SNMPv3 (при помощи сообщения Wake Up). Это период, в течение которого MTA должен сохранить временное значение (в поле "порядковый номер") из отправленного AP-запроса и будет ждать получения соответствующего AP-ответа от сервера подготовки к работе. Данный параметр является необязательным, поскольку существует значение по умолчанию.
Reset Kerberos ticket information (Сброс информации мандатах Kerberos)	Целое число 32	3, необязательное	Ч/З	MIB устройства MTA	pktcMtaDev ResetKrb Tickets	Спецификация безопасности (J.170) позволяет хранить мандаты на доступ, связанные с каким-либо сервером (сервером подготовки к работе или CMS), в энергонезависимой памяти NVRAM до окончания срока их действия. Данный атрибут MIB используется для передачи MTA информации о действиях, которые необходимо предпринять, в связи с отслеживанием периодов действия мандатов, хранящихся в NVRAM. По получении данного атрибута в составе файла конфигурации MTA ДОЛЖЕН предпринять указанные действия. Для получения дополнительной информации см. J.166.

### 9.1.2 Информация по услугам уровня устройства

Для получения более подробной информации относительно данных атрибутов и их значений по умолчанию (см. таблицу 13) см. MTA MIB (Рек. МСЭ-Т J.166), спецификации сигнализации вызова NCS (Рек. МСЭ-Т J.162), NCS MIB (Рек. МСЭ-Т J.166), а также RFC 2475.

**Таблица 12/J.167 – Услуги уровня устройства**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
NCS Default Call Signalling TOS (Тип услуги сигнализации вызова NCS по умолчанию)	Целое число	3, необяз.	Ч/3	MIB сигнализации MTA	pktcSigDefCallSigTos	Значение по умолчанию используется в заголовке IP для установки типа услуги для сигнализации вызова NCS
NCS Default Media Stream TOS (Тип услуги медиапотока NCS по умолчанию)	Целое число	3, необяз.	Ч/3	MIB сигнализации MTA	pktcSigDefMediaStreamTos	Значение по умолчанию используется в заголовке IP для установки типа услуги для пакетов медиапотоков NCS
MTA UDP receive port used for NCS (принимающий UDP-порт MTA для NCS)	Целое число (1025..65535)	3, необяз.	Только чтение	MIB сигнализации MTA	pktcSigDefNcsReceiveUdpPort	Данный объект содержит номер порта UDP (User Datagram Protocol, Пользовательский протокол дейтаграмм), используемого для сигнализации NCS. Значение данного объекта следует изменять только помощи файла конфигурации.
NCS TOS Format Selector (Селектор формата типа услуги NCS)	Перечень	3, необяз.	Ч/3	MIB сигнализации MTA	pktcSigTosFormatSelector	Формат значений типа услуг по умолчанию для сигнализации NCS и медиапотока NCS. Допустимые значения: "IPv4 TOS octet" или "DSCP codepoint". См. RFC 2475.
тактовый сигнал R0	Битовое поле	3, необяз.	Ч/3	MIB сигнализации MTA	pktcSigDevR0Cadence	Определяемое пользователем поле, где каждый бит представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина. Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).
тактовый сигнал R6	Битовое поле	3, необяз.	Ч/3	MIB сигнализации MTA	pktcSigDevR6Cadence	Определяемое пользователем поле, где каждый бит представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина. Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).
тактовый сигнал R7	Битовое поле	3, необяз.	Ч/3	MIB сигнализации MTA	pktcSigDevR7Cadence	Определяемое пользователем поле, где каждый бит представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина. Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).

**Таблица 12/J.167 – Услуги уровня устройства**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
тактовый сигнал R1	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev R1Cadence	<p>Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина.</p> <p>Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).</p>
тактовый сигнал R2	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev R2Cadence	<p>Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина.</p> <p>Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).</p>
тактовый сигнал R3	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev R3Cadence	<p>Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина.</p> <p>Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).</p>
тактовый сигнал R4	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev R4Cadence	<p>Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина.</p> <p>Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).</p>
тактовый сигнал R5	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev R5Cadence	<p>Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина.</p> <p>Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).</p>

**Таблица 12/J.167 – Услуги уровня устройства**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
тактовый сигнал Rg	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev RgCadence	Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина. Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).
тактовый сигнал Rt	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev RtCadence	Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина. Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).
тактовый сигнал Rs	Битовое поле	3, необяз.	Ч/З	MIB сигнализации MTA	pktcSigDev RsCadence	Определяемое пользователем поле, где каждый бит (самый младший бит) представляет длительность в 100мс (всего 6). 1 – активный сигнал, 0 – тишина. Для представления используются 64 бита; 60 бит от самого старшего бита – для тактового сигнала. Бит 61 используется для указания на повторяемость (значение НОЛЬ) или отсутствие повторяемости (значение ЕДИНИЦА). Оставшиеся 3 бита зарезервированы для использования в будущем и в настоящий момент заполняются нулями (000).

### 9.1.3 Информация о конфигурации для конкретной конечной точки

Для получения более подробной информации относительно данных атрибутов и их значений по умолчанию (см. таблицу 13) см. NCS MIB (Рек. МСЭ-Т J.166), спецификации NCS (Рек. МСЭ-Т J.162), спецификации безопасности (Рек. МСЭ-Т J.170) и MIB MTA (Рек. МСЭ-Т J.166).

- MTA отправляет KDC сертификат MTA/CMS, FQDN MTA, CMS-ID. KDC возвращает MTA "Мандат Kerberos", указывающий, что "этот MTA связан с данным CMS".
- Сертификат поставщика услуг телефонии подтверждает Сертификат телефонии MTA.
- В случае, если две различные конечные точки совместно используют одну Область Kerberos и один FQDN CMS, следующие четыре атрибута ДОЛЖНЫ быть идентичными: "льготный период" (grace period) PKINIT, список имен KDC, сертификат телефонии MTA, сертификат поставщика услуг телефонии.

**Таблица 13/J.167 – Конфигурация конкретной конечной точки**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
Port Admin State (Административный статус порта)	Перечень	3, необяз.	Ч/З	IF-MIB (RFC 2863)	ifAdminStatus	Административный статус порта, который оператор может использовать для включения/отключения услуг на этом порту. Административный статус может быть использован для прекращения доступа к пользовательскому порту без деинициализации абонента. Допустимые значения: up(1) или down(2). В случае доступ по протоколу SNMP объект ifAdminStatus находится в таблице ifTable MIB-II.
Call Management Server Name (Имя сервера управления вызовами)	Строка	3, обязательное	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigCallAgentId	Данный атрибут представляет собой строку, где указано имя CMS, с которым связана данная конечная точка. Имя вызывающего агента, следующее за символом "@", ДОЛЖНО представлять собой FQDN и ДОЛЖНО иметь соответствующую ему концептуальную строку в таблице pkcMtaDevCmsTable. Предполагается, что DNS поддерживает несколько CMS, как описано в спецификации NCS.
Call Management Server UDP Port UDP-порт сервера управления вызовами	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigCallAgentUdpPort	UDP-порт для CMS
Partial dial time-out (Период ожидания при неполном наборе номера)	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigPartialDialTO	Период ожидания окончания набора при неполном наборе номера в секундах.
Critical dial time-out (Период ожидания при экстренном наборе номера)	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigCriticalDialTO	Период ожидания при экстренном наборе номера в секундах.
Busy tone time-out (Период ожидания при передаче сигнала "занято")	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigBusyToneTO	Период ожидания при передаче сигнала "занято" в секундах.
Dial tone time-out (Период ожидания при передаче тонального сигнала "линия свободна")	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigDialToneTO	Период ожидания при передаче тонального сигнала "линия свободна" в секундах.

**Таблица 13/J.167 – Конфигурация конкретной конечной точки**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
Message waiting time-out (Период ожидания при передаче сигнала "ожидает сообщение")	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigMessageWaitingTO	Период ожидания при передаче сигнала "ожидает сообщение" в секундах.
Off-hook warning time-out (Период ожидания при предупреждении о том, что линия занята)	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigOffHookWarningTO	Период ожидания при предупреждении о том, что линия занята в секундах
Ringing time-out (Период ожидания при передаче сигнала о вызове)	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigRingingTO	Период ожидания при передаче сигнала о вызове в секундах.
Ringback time-out (Период ожидания при предоставлении услуги "ответный вызов")	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigRingBackTO	Период ожидания при предоставлении услуги "ответный вызов" в секундах
Reorder tone time-out (Период ожидания при предоставлении услуги "повторный заказ")	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigReorderToneTO	Период ожидания при предоставлении услуги "повторный заказ" в секундах.
Stutter dial time-out (Период ожидания при передаче прерывистого сигнала)	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigStutterDialToneTO	Период ожидания при передаче прерывистого сигнала в секундах.
TS Max	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigTSMax	Содержит максимальное время с момента передачи первоначальной дейтаграммы.
Max1	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigMax1	Порог подозрения на ошибку при повторной передаче для каждой конечной точки.
Max2	Целое число	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigMax2	Порог отсоединения при повторной передаче для каждой конечной точки.
Max1 Queue Enable (Включение очереди Max1)	Перечень	3	Ч/3	MIB сигнализации MTA	pkcNcsEndPntConfigMax1QueueEnable	Включает/отключает запрос DNS Max1, когда время работы Max1 истекает.

**Таблица 13/J.167 – Конфигурация конкретной конечной точки**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
Max2 Queue Enable (Включение очереди Max2)	Перечень	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigMax2QEnable	Включает/отключает запрос DNS Max2, когда время работы Max2 истекает.
MWD	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigMWD	Время ожидания перед выполнением перезапуска после того, как получена команда на перезапуск в секундах.
Tdinit	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigTdinit	Время ожидания после отсоединения в секундах
TdMin	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigTDMIN	Минимальное время ожидания после отсоединения в секундах
TdMax	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigTDMAX	Максимальное время ожидания после отсоединения в секундах
RTO Max	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigRtoMax	Максимальное время ожидания при повторной передаче в секундах.
RTO Init	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigRtoInit	Первоначальное значение времени ожидания при повторной передаче в секундах.
Long Duration Keepalive (Поддержание длительного вызова)	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigLongDurationKeepAlive	Период ожидания в минутах при отправке уведомлений о наличии длительного вызова.
Thist	Целое число	3	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigThist	Время ожидания после которого определяется, что ответа нет, в секундах.
Call Waiting Max Reps (Максимальное количество повторений сигнала об ожидающем вызове)	Целое число	3, необяз.	Ч/З	MIB сигнализации MTA	pkcNcsEndPntConfigCallWaitingMaxRep	Данный объект содержит максимальное количество повторений сигнала об ожидающем вызове, который MTA будет воспроизводить для одного запроса SMS. В случае, если SMS запускает повтор воспроизведения, будет использовано значение (0).
Call Waiting Delay (Задержка между повторами передачи сигнала об ожидающем вызове)	Целое число	3, необяз.	Ч/З	IF-MIB (RFC 2863)	pkcNcsEndPntConfigCallWaitingDelay	Данный объект содержит задержку между повторами сигнала об ожидающем сообщении, который будет воспроизводиться MTA для одного запроса SMS.

#### 9.1.4 Информация о конфигурации для конкретной области

Для получения более подробной информации относительно данных атрибутов и их значений по умолчанию см. MIB MTA (J.166). Для получения более подробной информации по использованию областей Kerberos см. Рекомендацию безопасности (J.170). В таблице pkcMtaDevRealmTable ДОЛЖНА быть по крайней мере одна концептуальная строка для начала обслуживания по окончании конфигурирования. Данные параметры конфигурации являются необязательными в файле конфигурации, но если они включены, файл конфигурации ДОЛЖЕН содержать по крайней мере одно Имя области для корректной установки данной таблицы. В случае, если поддерживается несколько областей, в таблице может присутствовать более чем один набор значений.

**Таблица 14/J.167 – Информация о конфигурации для конкретной области**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
Pkinit Grace Period ("льготный период" PKINIT)	Целое число	3, необязат.	Ч/3	MIB устройства MTA	pktcMtaDevRealmPkinitGracePeriod	Для целей безопасного обмена ключами с CMS по протоколу IPSec, MTA ДОЛЖЕН получить новый мандат Kerberos (при помощи обмена PKINIT) за много минут до истечения срока действия старого. Минимально допустимое значение – 15 минут. Значение по умолчанию – 30 минут. Этот параметр может также использоваться другими приложениями, применяющими Kerberos.
TGS Grace Period ("льготный период" сервера выдачи мандатов)	Целое число	3, необязат.	Ч/3	MIB устройства MTA	pktcMtaDevRealmTgsGracePeriod	В случае, если данная реализация MTA использует сообщения Kerberos TGS Request/TGS Reply для организации безопасного обмена ключами с CMS по протоколу IPSec, MTA ДОЛЖЕН получить новый мандат на обслуживание (при помощи запроса TGS) за много минут до истечения срока действия старого. Минимально допустимое значение – 1 минута. Значение по умолчанию – 10 минут. Этот параметр может также использоваться другими приложениями, применяющими Kerberos.
Realm Org Name Наименование организации области	Целое число	3, обязат.	Ч/3	MIB устройства MTA	pktcMtaDevRealmOrgName	Значение атрибута "Наименование организации" в каталоге X.500 в имени субъекта Сертификата поставщика услуг.
Unsolicited Keying max Timeout (Максимальный период ожидания в ходе обмена ключами по инициативе MTA)	Целое число	3, необязат.	Ч/3	MIB устройства MTA	pktcMtaDevRealmUnsolicitedKeyMaxTimeout	Данный период ожидания применяется только в том случае, если обмен ключами был инициирован MTA. Максимальное значение периода ожидания – значение, которое не должно превышать в ходе выполнения экспоненциального алгоритма возврата.
Unsolicited Keying Nominal Timeout (Номинальный период ожидания в ходе обмена ключами по инициативе MTA)	Целое число	3, необязат.	Ч/3	MIB устройства MTA	pktcMtaDevRealmUnsolicitedKeyNomTimeout	Данный период ожидания применяется только в том случае, если обмен ключами был инициирован MTA. Как правило это среднее время прохождения пакета туда и обратно между MTA и KDC.
Unsolicited Keying Max Retries (Максимальное количество повторных попыток при обмене ключами по инициативе MTA)	Целое число	3, необязат.	Ч/3	MIB устройства MTA	pktcMtaDevRealmUnsolicitedKeyMaxRetries	Значение – максимальное количество повторов, после которого MTA прекращает попытки установить защищенные соединения.

### **9.1.5 Информация о конфигурации для конкретного CMS**

Для получения более подробной информации относительно данных атрибутов и их значений по умолчанию см. MIB MTA (J.166). В таблице pkcDevCmsTable ДОЛЖНА быть по крайней мере одна концептуальная строка для начала обслуживания по окончании конфигурирования. Данные параметры конфигурации являются необязательными в файле конфигурации, но если они включены, в файл конфигурации ДОЛЖЕН быть указан по крайней мере один CMS и соответствующее ему Имя области Kerberos. В случае, если поддерживается несколько областей, в таблице может присутствовать более чем один набор значений.

Согласно Рек. J.170 МСЭ-Т, управление безопасностью сигнализации IPSec должно осуществляться Оператором в зависимости от технического оснащения и условий работы. После того, как защищенное соединение по протоколу IPSec установлено между MTA и CMS, контроль над включением/отключением IPSec также следует осуществлять для конкретного CMS. Включение/отключение безопасности сигнализации IPSec ДОЛЖНО определяться только информацией в файле конфигурации MTA, когда файл загружается, а смена состояний Включение/отключение ДОЛЖНА иметь место только в результате сброса MTA.

Для получения более подробной информации об Объекте MIB, контролирующем включение/отключение IPSec см. MIB MTA (J.166).

**Таблица 15/J.167 – Информация о конфигурации для конкретного CMS**

Атрибут	Синтаксис	Доступ конфигурации	Доступ SNMP	Файл MIB	Объект	Комментарии
Kerberos Realm Name (Имя области Kerberos)	Строка	3, обязат. (Прим.)	Ч/3	MIB устройства MTA	pktcMtaDevCmsKerbRealmName	Имя связанной области Kerberos. Это соответствующее Имя области Kerberos из Информации о конфигурации для конкретной области.
CMS Maximum Clock Skew (Максимальное отклонение часов CMS)	Целое число	3, необяз.	Ч/3	MIB устройства MTA	pktcMtaDevCmsMaxClockSkew	Максимально возможное расхождение в значениях часов MTA и CMS.
CMS Solicited Key Timeout (Период ожидания при обмене ключами по инициативе CMS)	Целое число	3, необяз.	Ч/3	MIB устройства MTA	pktcMtaDevCmsSolicitedKeyTimeout	Данный период ожидания применяется только в случае, если обмен ключами был инициирован CMS (посредством сообщения Wake Up или Rekey). Это период, в течение которого MTA должен сохранить временное значение(в поле "порядковый номер"), взятое из отправленного запроса AP Request, и ожидает получения соответствующего ответа AP Response от CMS.
Unsolicited Key Max Timeout (Максимальный период ожидания при обмене ключами по инициативе MTA)	Целое число	3, необяз.	Ч/3	MIB устройства MTA	pktcMtaDevCmsUnsolicitedKeyMaxTimeout	Данный период ожидания применяется только в случае, если обмен ключами был инициирован MTA. Максимальное значение периода ожидания – значение, которое не должно превышать в ходе выполнения экспоненциального алгоритма возврата.
Unsolicited Key Nominal Timeout (Номинальный период ожидания при обмене ключами по инициативе MTA)	Целое число	3, необяз.	Ч/3	MIB устройства MTA	pktcMtaDevCmsUnsolicitedKeyNomTimeout	Данный период ожидания применяется только в том случае, если обмен ключами был инициирован MTA. Как правило это среднее время прохождения пакета туда и обратно между MTA и KDC.
Unsolicited Key Max Retries (Максимальное количество повторов при обмене ключами по инициативе MTA)	Целое число	3, необяз.	Ч/3	MIB устройства MTA	pktcMtaDevCmsUnsolicitedKeyMaxRetries	Значение – максимальное количество повторов, после которого MTA прекращает попытки установить защищенные соединения.
IPSec Control (управление IPSec)	Целое число	3, необяз.	Только чтение	MIB устройства MTA	pktcMtaDevCmsIpsSecCtrl	Управление IPSec для каждого CMS: контролируется установка IPSec и связанные с IPSec процедуры управления ключами.
ПРИМЕЧАНИЕ. – Если в файл конфигурации включается какая-либо информация из таблицы Информации о конфигурации для конкретного CMS, данное значение ДОЛЖНО быть включено.						

### 9.1.6 Исключение объектов MIB из файла конфигурации

Приведенные ниже объекты MIB НЕ ДОЛЖНЫ отправляться в файле конфигурации, поскольку значения этих объектов могут быть установлены только МТА или сервером DHCP при подготовке к работе. В случае, если МТА получает файл конфигурации, содержащий данные объекты MIB, он ДОЛЖЕН проигнорировать эти объекты, отправить отчет passWithWarnings (успешно с предупреждениями) и заполнить таблицу Error OID.

- PktcMtaDevSnmpEntity
- PktcMtaDevProvKerbRealmName
- PktcMtaDevFqdn
- PktcMtaDevSerialNumber
- PktcMtaDevMacAddress
- PktcMtaDevEndPntCount
- PktcMtaDevTypeIdentifier
- PktcEnNcsEndPntQuarantineState
- PktcEnNcsEndPntHookState
- pktcEnEndPntInfoTable
- pktcDevEventDescrEnterprise
- pktcDevEventDescrFacility
- pktcDevEventDescrText
- pktcDevEvLogIndex
- pktcDevEvLogTime
- pktcDevEvLogLevel
- pktcDevEvLogId
- pktcDevEvLogText
- pktcDevEvLogEndpointName
- pktcDevEvLogType
- pktcDevEvLogTargetInfo
- pktcDevEvLogCorrelationId
- pktcMtaDevProvConfigKey

ПРИМЕЧАНИЕ. – для значений SYSLOG, конкретно для объектов MIB "pktcDevEvSyslogAddressType" и "pktcDevEvSyslogAddress" МТА ДОЛЖЕН проверить предоставленное (или сохраненное) значение 'type' и предоставленное (или сохраненное) значение 'Syslog Address'. В случае, если их целостность нарушена, МТА ДОЛЖЕН проигнорировать все такие значения в файле конфигурации, отправить отчет passWithWarnings (успешно с предупреждениями) и заполнить таблицу Error OID.

## 10 Технические возможности устройства МТА

Строка с информацией о технических возможностях устройства МТА отправляется серверу подготовки к работе в коде опции 60 (Идентификатор класса производителя) – для того, чтобы дать возможность вспомогательным приложениям различать МТА в процессе подготовки к работе. Использование информации о технических возможностях приложением подготовки к работе является необязательным.

Строка с информацией о возможностях представляет собой строку ASCII-символов, содержащую информацию о технических возможностях МТА в формате TLV.

Например, первые два триплета TLV (Версия IPCablecom 1.0 и Количество конечных точек телефонии = 2) в виде ASCII будет выглядеть как 05nn0101020102. Следует отметить, что МТА IPCablecom требуется гораздо больше TLV и поле nn, таким образом, будет содержать длину всех TLV. В данном примере показаны только два TLV для простоты представления.

Поле "значение" (value) описывает возможности конкретного модема, то есть ограничения содержания или количества характеристик, поддерживаемых модемом, зависящие от конкретной реализации устройства. Данное поле составлено из ряда закапсулированных полей TLV. Следует отметить, что определенные поля подтипов действительны только в рамках закапсулированной строки установки конфигурации возможностей.

Тип (Тип)	Length (Длина)	Value (Значение)
5	n	

Возможные закапсулированные поля описаны ниже.

МТА ДОЛЖЕН отправлять строку с информацией о технических возможностях в опции 60 запроса DHCP DISCOVER.

### 10.1 Версия IPCablecom

Данный TLV ДОЛЖЕН быть включен в строку с информацией о возможностях.

Тип	Length	Value	Комментарий	Значение по умолчанию
5.1	1	0	PacketCable 1.0	Нет
		1	PacketCable 1.5	

### 10.2 Количество конечных точек телефонии

Данный TLV подтипа 5.2 (Количество конечных точек телефонии) ДОЛЖЕН быть включен в строку с информацией о возможностях.

Тип	Length	Value	Комментарий	Значение по умолчанию
5.2	1	n	Количество конечных точек телефонии	Нет

### 10.3 Поддержка TGT

Тип	Length	Value	Комментарий	Значение по умолчанию
5.3	1	0	0: Нет	0
		1	1: Да	

### 10.4 Поддержка метода доступа HTTP для загрузки файлов

Тип	Length	Value	Комментарий	Значение по умолчанию
5.4	1	0	0: Нет	0
		1	1: Да	

### 10.5 Поддержка уведомления SYSLOG о событии MTA24

Тип	Length	Value	Комментарий	Значение по умолчанию
5.5	1	0	0: Нет	1
		1	1: Да	

### 10.6 Поддержка процесса обслуживания NCS

Тип	Length	Value	Комментарий	Значение по умолчанию
5.6	1	Не определено	Зарезервировано	Не определено

Подтип 5.6, ранее использовавшийся для указания на поддержку процесса обслуживания NCS в настоящее время не определен и зарезервирован для использования в будущем.

## 10.7 Поддержка первичной линии

Type	Length	Value	Комментарий	Значение по умолчанию
5.7	1	0	0: Нет	0
		1	1: Да	

## 10.8 Тип(ы) TLV, определяемые производителем

Данный TLV может включаться в состав строки с информацией о возможностях в случае, если МТА требуется специальная обработка определяемых производителем TLV.

Type	Length	Value	Комментарий	Значение по умолчанию
5.8	n	{последовательность байтов}	Один тип на байт	43

Подтип 5.8, ранее использовавшийся для указания на поддержку МТА определяемых производителем форматов TLV, в настоящее время устарел и зарезервирован для использования в будущем. Данный подтип НЕ ДОЛЖЕН использоваться МТА.

## 10.9 Поддержка хранения мандатов/информации о мандатах в энергонезависимой памяти NVRAM

Type	Length	Value	Комментарий	Значение по умолчанию
5.9	1	0	0: Нет	1
		1	1: Да	

## 10.10 Поддержка отправки отчета о подготовке к работе

Type	Length	Value	Комментарий	Значение по умолчанию
5.10	1	0	0: Нет	1
		1	1: Да	

## 10.11 Поддерживаемые кодеки (CODEC(s))

Данный TLV ДОЛЖЕН быть включен в строку с информацией о возможностях.

Type	Length	Value	Комментарий	Значение по умолчанию
5.11	n	{последовательность байтов}	Один идентификатор на байт	Нет

CODEC ID (идентификатор кодека) – значение, представленной типом "перечень" в объекте "PktcCodecType" TEXTUAL CONVENTION в MIB МТА:

- 1: другой;
- 2: неизвестный;
- 3: G.729;
- 4: зарезервировано;
- 5: G.729E;
- 6: PCMU;
- 7: G.726-32;
- 8: G.728;
- 9: PCMA;
- 10: G.726-16;
- 11: G.726-24;

- 12: G.726-40;
- 13: iLBC;
- 14: BV16;
- 15: Событие телефонии (telephone-event).

Событие телефонии (telephone-event) обозначает события DTMF RFC 2833. Для получения дополнительной информации см. Рек. МСЭ-Т J.161.

#### 10.12 Поддержка подавления тишины

Type	Length	Value	Комментарий	Значение по умолчанию
5.12	1	0	0: Нет	0
		1	1: Да	

#### 10.13 Поддержка устранения эффекта "эхо"

Type	Length	Value	Комментарий	Значение по умолчанию
5.13	1	0	0: Нет	0
		1	1: Да	

#### 10.14 Поддержка RSVP (Resource Reservation Protocol, протокол резервирования ресурсов)

Type	Length	Value	Комментарий	Значение по умолчанию
5.14	1	Undefined	Зарезервировано	Не определено

Подтип 5.14, ранее использовавшийся для указания на поддержку RSVP в настоящее время не определен и зарезервирован для использования в будущем.

#### 10.15 Поддержка UGS-AD (Unsolicited Grant Service with Activity Detection) (Услуга предоставления канала с обнаружением активности)

Type	Length	Value	Комментарий	Значение по умолчанию
5.15	1	0	0: Нет	0
		1	1: Да	

#### 10.16 Начальный номер "ifIndex" МТА в таблице "ifTable"

Данный TLV содержит значение "ifIndex" для первого интерфейса телефонии МТА в таблице "ifTable" MIB. Данный TLV ДОЛЖЕН включаться в строку информации о возможностях.

Type	Length	Value	Комментарий	Значение по умолчанию
5.16	1	n	Первый интерфейс МТА	9

#### 10.17 Поддержка ведения журнала событий процесса подготовки к работе

Для данной возможности устанавливается соответствующее значение в зависимости от технических характеристик процесса подготовки к работе (согласно 5.4.3).

Type	Length	Value	Комментарий	Значение по умолчанию
5.17	1	0	0: Нет	0
		1	1: Да	

## 10.18 Поддерживаемые процессы подготовки к работе

МТА ДОЛЖЕН включать данный TLV подтипа 5.18 (Поддерживаемые процессы подготовки к работе) в строку с информацией о возможностях. Данный TLV указывает, какие процессы подготовки к работе поддерживаются МТА (базовый, гибридный и защищенный). Он содержит битовую маску, указывающую все поддерживаемые МТА типы процессов подготовки к работе.

Type	Length	Value	Комментарий	Значение по умолчанию
5.18	2	{битовая маска}	См. ниже	Нет

Поле "значение" представляет собой 16-битное целое число без знака с сетевым порядком байтов. Каждый бит представляет отдельный тип процесса подготовки к работе. Если для бита установлено значение 1, МТА поддерживает соответствующую процесс. Если для бита установлено значение 0, МТА не поддерживает такой процесс.

Назначения битов:

Бит 0 – защищенный процесс (полный защищенный процесс подготовки к работе)

Бит 1 – гибридный процесс

Бит 2 – базовый процесс

МТА ДОЛЖЕН установить для всех неиспользуемых битов в битовой маске значение 0. МТА ДОЛЖЕН установить для Бита 0 в TLV значение 1, чтобы указать, что он поддерживает защищенный процесс. МТА также ДОЛЖЕН установить значения для Битов 1 и 2, чтобы указать, поддерживает ли он гибридный и базовый процессы. Пример: если МТА поддерживает защищенный и базовый процессы, целочисленное значение битовой маски будет 0x0005 и данная возможность будет закодирована в опции 60 следующей последовательностью октетов (в нотации HEX): 12 02 00 05.

Для обеспечения совместимости с версиями, существовавшими до ввода базового и гибридного процессов, отсутствие данного TLV говорит о том, что МТА поддерживает только защищенный процесс.

## 10.19 Поддержка версии T38

МТА ДОЛЖЕН включать данный TLV подтипа 5.19 (Поддержка версии T38) в строку информации о возможностях. Данный TLV указывает на номер версии T.38, поддерживаемой МТА. Для получения более подробной информации см. Рек. МСЭ-Т J.161.

Type	Length	Value	Комментарий	Значение по умолчанию
5.19	1	0	0: не поддерживается	1
		1	1: Версия Ноль	
		2	2: Версия Один	
		3	3: Версия Два	
		4	4: Версия Три	

## 10.20 Поддержка коррекции ошибок T38

МТА ДОЛЖЕН включать данный TLV подтипа 5.20 (Поддержка коррекции ошибок T38) в строку информации о возможностях. Данный TLV указывает на тип коррекции ошибок T.38, поддерживаемый МТА. Для получения более подробной информации см. Рек. МСЭ-Т J.161.

Type	Length	Value	Комментарий	Значение по умолчанию
5.20	1	0	0: Нет	1
		1	1: Redundancy	
		2	2: FEC	

Поддержка FEC подразумевает, что также поддерживается Redundancy. Для получения более подробной информации см. Рек. МСЭ-Т J.161.

### 10.21 Поддержка RFC 2833 DTMF

МТА ДОЛЖЕН включать данный TLV подтипа 5.21 (Поддержка RFC 2833 DTMF) в строку информации о возможностях. Данный TLV указывает поддержку ретрансляции RFC 2833 DTMF, поддерживаемый МТА. Для получения более подробной информации см. Рек. МСЭ-Т J.161.

Type	Length	Value	Комментарий	Значение по умолчанию
5.21	1	0	0: Нет	1
		1	1: Да	

### 10.22 Поддержка голосовых параметров

МТА ДОЛЖЕН включать данный TLV подтипа 5.22 (Поддержка голосовых параметров) в строку информации о возможностях. Данный TLV указывает на поддержку голосовых параметров, как указано в RFC 3611.

Type	Length	Value	Комментарий	Значение по умолчанию
5.22	1	0	0: Нет	1
		1	1: Да	

### 10.23 Поддержка MIB устройства

МТА ДОЛЖЕН включать данный TLV подтипа 5.23 (Поддержка MIB устройства) в строку информации о возможностях. Данный TLV указывает, какие типы MIB поддерживаются МТА.

Type	Length	Value	Комментарий	Значение по умолчанию
5.23	n	{последовательность байтов}	Поддерживаемые типы MIB, кодированные в форме пар 'length-value' (длина-значение)	Нет

Пары 'length-value' определены следующим образом:

[L1] [ОСТЕТ-1] [ОСТЕТ-2][ОСТЕТ-3] ...[ОСТЕТ-L1],

[L2] [ОСТЕТ-1] [ОСТЕТ-2][ОСТЕТ-3] ...[ОСТЕТ-L2]

(И другие пары 'length-value', расположенные соответствующим образом),

где:

L1 и L2 означают длины.

Первый октет (ОСТЕТ-1) всегда представляет организацию, выпускающую MIB (например, CableLabs, IETF и т. п.).

Остальные октеты всегда располагаются в сетевом порядке и формируют строку битов, где каждый бит представляет отдельный MIB. Установление для бита значения "1" указывает на поддержку соответствующего MIB, а установление для бита значения "0" указывает на отсутствие поддержки данного типа MIB.

МТА НЕ ДОЛЖЕН использовать какие-либо "зарезервированные обозначения", если они не определены в рамках IP-Cablecom или не определены производителем.

### 10.23.1 Обозначение организации, выпускающей MIB

ОСТЕТ-1 пары 'length-value' указывает на организацию, выпустившую данный MIB и имеет следующие условные обозначения:

Обозначение	Указатель организации
0	CableLabs
1	IETF
2–9	*зарезервировано*
10–63	*определяется производителем*

ПРИМЕЧАНИЕ. – Два старших бита октета-1 (ОСТЕТ-1) зарезервированы, что дает возможность сформировать 64 варианта.

### 10.23.2 MIB, выпущенные CableLabs

Для MIB, выпущенных CableLabs (ОСТЕТ-1 = 0), битовая маска определена следующим образом:

Бит 0	PacketCable 1.5 MIB MTA.
Бит 1	PacketCable 1.5 MIB сигнализации.
Бит 2	PacketCable 1.5 MIB управляющих событий.
Бит 3	PacketCable 1.5 MIB расширений MTA.
Бит 4	PacketCable 1.5 MIB расширений сигнализации.
Бит 5	PacketCable 1.5 MIB расширений MEM.
Бит 6	*Зарезервировано*
Бит 7	*Зарезервировано*

При этом биты расположены в следующем порядке:

7	6	5	4	3	2	1	0
---	---	---	---	---	---	---	---

Поскольку в настоящее время для битовой маски используется только один октет, длина данной пары length-value ДОЛЖНА равняться двум (один на указатель организации и один на битовую маску соответственно).

### 10.23.3 MIB, выпущенные IETF

Для MIB, выпущенных IETF (ОСТЕТ-1 = 1), битовая маска определена следующим образом:

Бит 0	MIB MTA.
Бит 1	MIB сигнализации
Бит 2	MIB управляющих событий
Бит 3	*Зарезервировано*
Бит 4	*Зарезервировано*
Бит 5	*Зарезервировано*
Бит 6	*Зарезервировано*
Бит 7	*Зарезервировано*

Поскольку в настоящее время для битовой маски используется только один октет, длина данной пары length-value ДОЛЖНА равняться двум (один на указатель организации и один на битовую маску соответственно).

### Пример

Для MTA, поддерживающего все определенные MIB IETF (MTA, сигнализации и MEM) и все определенные MIB расширений IPCom 1.5 (расширений MTA, расширений сигнализации и

расширений MEM), данная подопция в нотации HEX будет выглядеть следующим образом (взято в качестве снимка с опции 60):

...	...	17	06	02	00	38	02	00	07	...	...
-----	-----	----	----	----	----	----	----	----	----	-----	-----

ПРИМЕЧАНИЕ. – На момент написания данного документа никакие из предложенных IETF проектов не приобрели статуса RFC и все приведенные здесь ссылки даны только в качестве примера.

## 10.24 Поддержка множественного предоставления канала в течение одного интервала (MGPI)

МТА ДОЛЖЕН включать данный TLV подтипа 5.24 (Поддержка множественного предоставления канала в течение одного интервала) в строку информации о возможностях. Данный TLV указывает поддержку МТА множественного предоставления канала в течение одного интервала (MGPI). Для получения более подробной информации см. Рек. МСЭ-Т J.163

Type	Length	Value	Комментарий	Значение по умолчанию
5.24	1	0	0: Нет	0
		1	1: Да	

## 11 Спецификация TLV-38 приемника уведомлений SNMP

Данный TLV-38 IPCablecom указывает одну или несколько Станций управления сетью, которые должны получать уведомления от МТА (на шаге MTA25 или H-MTA-25 или B-MTA-25 или по завершении подготовки к работе, если необходимо). В случае, если данный TLV-38 или его вложенные TLV, определенные в данном пункте, содержат некорректное значение в поле "Length", МТА ДОЛЖЕН отвергнуть файл конфигурации и отправить отчет об ошибке "failConfigFile" (сбой в файле конфигурации). В случае, если TLV-38 содержит подтипы с некорректными значениями, МТА ДОЛЖЕН действовать в соответствии с требованиями, приводимыми ниже для каждого конкретного вложенного TLV.

Дополнительно, в случае, если МТА встречает неизвестные вложенные TLV внутри TLV-38, он ДОЛЖЕН:

- Основываться на предположении, что размер поля "Length" данного вложенного TLV составляет 1 байт;
- Проигнорировать данный вложенный TLV и продолжить обработку файла;
- отправить отчет о статусе подготовки к работе passWithWarnings и заполнить таблицу Error Oid.

Type	Length	Value
38	N	Составное (содержит вложенные TLV)

Если не указано или сконфигурировано иное, МТА ДОЛЖЕН отправлять уведомления системе подготовки к работе по умолчанию (описанной в подопции 3 опции 122 DHCP).

### 11.1 Вложенные TLV TLV-38

#### 11.1.1 IP-адрес приемника уведомлений SNMP

В данном вложенном TLV указывается IP-адрес приемника уведомлений.

Type	Length	Value
38.1	4	4 байта адреса в формате IPv4 с сетевым порядком байтов

В случае, если TLV-38 присутствует в файле конфигурации, а вложенный TLV-38.1 отсутствует, МТА ДОЛЖЕН проигнорировать TLV-38 и продолжить обработку файла конфигурации и ДОЛЖЕН отправить отчет о статусе подготовки к работе passWithWarnings и заполнить таблицу Error Oid (pkcMtaDevErrorOidsTable).

### 11.1.2 Номер UDP-порта приемника уведомлений SNMP

В данном вложенном TLV указывается UDP-порт приемника уведомлений, предназначенный для приема уведомлений.

Type	Length	Value
38.2	2	Номер порта UDP

В случае, если TLV-38 присутствует, а вложенный TLV-38.2 отсутствует, ДОЛЖНО быть использовано значение по умолчанию 162.

### 11.1.3 Тип приемника уведомлений SNMP

В данном вложенном TLV указывается тип приемника уведомлений SNMP; это тип уведомлений SNMP, которые МТА ДОЛЖЕН отправлять связанному с ним серверу уведомлений SNMP.

Type	Length	Value
38.3	2	1: SNMPv1-прерывание в пакете SNMPv1 2: SNMPv2c-прерывание в пакете SNMPv2c packet 3: Информационное сообщение SNMP в пакете SNMPv2c 4: Прерывание SNMP в пакете SNMPv3 5: Информационное сообщение SNMP в пакете SNMPv3

В случае, если TLV-38 присутствует, а вложенный TLV-38.3 отсутствует, МТА ДОЛЖЕН проигнорировать TLV-38 целиком и продолжить обработку файла конфигурации, а также отправить отчет о статусе подготовки к работе `passWithWarnings` и заполнить таблицу `Error OID (pkcMtaDevErrorOidsTable)`. МТА и сервер инициализации ДОЛЖНЫ поддерживать типы уведомлений 2 и 3 и МОГУТ поддерживать типы уведомлений 1, 4 и 5, указанные в таблице выше. В случае, если получено уведомление неподдерживаемого или некорректного типа, МТА ДОЛЖЕН проигнорировать содержимое всего TLV-38, а также отправить отчет о статусе инициализации `passWithWarnings` и заполнить таблицу `Error OID (pkcMtaDevErrorOidsTable)`. В случае, если уведомления типов 4 или 5 применяются при использовании базового или гибридного процессов, предполагается, что будет использован протокол SNMPv3 согласно рекомендациям по протоколу SNMPv3, обсуждение чего выходит за рамки настоящей Рекомендации.

### 11.1.4 Период ожидания приемника уведомлений SNMP

В данном вложенном TLV содержится время, по истечении которого отправитель информационного сообщения SNMP должен предпринять повторную попытку, если ему не удалось получить от адресата подтверждение получения этого сообщения. Следует отметить, что количество повторов определено во вложенном TLV 38.5.

Type	Length	Value
38.4	2	Время в мс

В случае, если TLV-38 присутствует, а вложенный TLV-38.4 отсутствует, ДОЛЖНО быть использовано значение по умолчанию 15000 мс. Это соответствует значению по умолчанию в 15 тысяч миллисекунд установленному для объекта MIB `snmpTargetAddrTimeout` (см. RFC 3413).

### 11.1.5 Повторы приемника уведомлений SNMP

В данном вложенном TLV содержится максимальное количество повторов отправки информационного сообщения SNMP, которое МТА ДОЛЖЕН предпринять в случае, если не удастся получить от адресата подтверждение получения сообщения. Следует отметить, что время ожидания перед каждым повтором определено вложенным TLV 38.4.

Type	Length	Value
38.5	2	Количество повторов

В случае отсутствия данного вложенного TLV ДОЛЖНО быть использовано значение по умолчанию 3. Максимально допустимое количество повторов – 255.

### 11.1.6 Параметры фильтрации приемника уведомлений SNMP

В данном вложенном TLV определяется схема фильтрации уведомлений и содержится корневой OID поддерева MIB, определяющего, какие уведомления должны отправляться на приемник уведомлений. МТА ДОЛЖЕН фильтровать уведомления, отправляемые менеджеру SNMP, указанному во вложенном TLV 38.1. Если данный вложенный TLV отсутствует, МТА ДОЛЖЕН использовать значение OID по умолчанию для корня 'iso'.

Type	Length	Value
38.6	n	Фильтр OID (Идентификатор объекта в формате ASN.1)

В закодированной форме значение данного поля TLV представляет собой Универсальный тип 6 ASN.1 (Идентификатор объекта), за которым следует поле длины в формате ASN.1. Завершает его компонент-идентификатор объекта в формате ASN.1.

### 11.1.7 Безопасное имя приемника уведомлений SNMPv3

В данном вложенном TLV определяется безопасное имя SNMPv3, которое используется при отправке SNMPv3-уведомлений. Данным вложенный TLV используется только в случае, если МТА поддерживает типы приемника уведомлений 4 и 5, как указано во вложенном TLV 38.3. МТА ДОЛЖЕН проигнорировать вложенный TLV 38.7, если в файле конфигурации (вложенный TLV 38.3) обозначены значения типа приемника, отличные от 4 или 5.

К МТА, поддерживающим типы приемников уведомлений 4 или 5 (согласно вложенному TLV 38.3), предъявляются следующие требования:

- В случае, если данный вложенный TLV 38.7 опущен, SNMPv3-уведомления ДОЛЖНЫ отправляться на уровне безопасности noAuthNoPriv с использованием безопасного имени "@mtaconfig".
- Если данный вложенный TLV присутствует, МТА проверяет, существует ли данное Безопасное имя на локальной системе авторизации МТА SNMP и создает значение для последующей связи с системой авторизации приемника уведомлений (используя уровни безопасности и ключи существующего Безопасного имени). В случае, если указанное в данном вложенном TLV Безопасное имя не существует на локальной системе авторизации, TLV-38 целиком ДОЛЖЕН быть проигнорирован и МТА ДОЛЖЕН отправить отчет о статусе инициализации passWithWarnings и заполнить таблицу Error OID (pktcMtaDevErrorOidsTable) для всего TLV-38 и связанных вложенных TLV, которые были проигнорированы.

Type	Length	Value
38.7	2–26	Безопасное имя

## 11.2 Соответствие полей TLV таблицам SNMP

В следующих пунктах подробно описывается соответствие TLV-38 файла конфигурации МТА "Приемник уведомлений SNMP PacketCable" функциональным таблицам SNMP.

По получении каждого значения TLV-38, для того, чтобы была осуществлена передача необходимого прерывания (SNMP TRAP) или информационного сообщения (SNMP INFORM), МТА ДОЛЖЕН записать значения в следующие таблицы: snmpNotifyTable, snmpTargetAddrTable, snmpTargetAddrExtTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable, and vacmViewTreeFamilyTable. МТА ДОЛЖЕН поддерживать как минимум 10 элементов TLV-38 в файле конфигурации.

### 11.2.1 Запись значений полей TLV в соответствующие созданные строки таблиц SNMP

Таблицы в данном пункте показывают, как поля TLV файла конфигурации МТА (управляющие коды в скобках вида <>) помещаются в таблицы SNMP.

Ниже приводится соответствие между управляющими кодами и собственно вложенными TLV:

<IP Address>(IP-адрес)	TLV 38.1
<Port> (Порт)	TLV 38.2
<Trap type>(Тип прерывания)	TLV 38.3
<Timeout> (Период ожидания)	TLV 38.4
<Retries>(Повторы)	TLV 38.5
<Filter OID>(OID фильтра)	TLV 38.6
<Security Name> (Безопасное имя)	TLV 38.7

Создание строк со значениями в столбцах или индексами с суффиксом "n" в приведенных ниже таблицах означает, что данные значения были созданы на основе n-1-го TLV-38 из файла конфигурации MTA.

### 11.2.1.1 snmpNotifyTable

Если элементы TLV-38 присутствуют и вне зависимости от количества элементов MTA ДОЛЖЕН создать две строки с фиксированными значениями, как показано в таблице 16.

**Таблица 16/J.167 – snmpNotifyTable**

<b>snmpNotifyTable (RFC 3413, SNMP- NOTIFICATION-MIB)</b>	<b>Первая строка</b>	<b>Вторая строка</b>
Имя столбца (* = часть Индекса)	Значение в столбце	Значение в столбце
* snmpNotifyName	"@mtaconfig_inform"	"@mtaconfig_trap"
snmpNotifyTag	"@mtaconfig_inform"	"@mtaconfig_trap"
snmpNotifyType	inform (2)	trap (1)
snmpNotifyStorageType	переменное	Переменное
snmpNotifyRowStatus	активен (1)	активен (1)

### 11.2.1.2 snmpTargetAddrTable

Для каждого элемента TLV-38 из файла конфигурации MTA ДОЛЖЕН создать одну строку согласно таблице 17.

**Таблица 17/J.167 – snmpTargetAddrTable**

<b>snmpTargetAddrTable (RFC 3413, SNMP-TARGET-MIB)</b>	<b>Новая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpTargetAddrName	"@mtaconfig_n" где n находится в диапазоне от 0 до m – 1, где m – количество TLV-элементов приемника уведомлений в файле конфигурации
snmpTargetAddrTDomain	snmpUDPDomain = snmpDomains.1
snmpTargetAddrTAddress (IP-адрес и UDP-порт приемника уведомлений)	Строка октетов (6) Оклеты 1–4: <IP Address> Оклеты 5–6: <Port>
snmpTargetAddrTimeout	<Timeout> из TLV
snmpTargetAddrRetryCount	<Retries> из TLV
snmpTargetAddrTagList	If <Trap type> = 2 "@mtaconfig_trap" Else If <Trap type> = 3 "@mtaconfig_inform"

**Таблица 17/J.167 – snmpTargetAddrTable**

<b>snmpTargetAddrTable (RFC 3413, SNMP-TARGET-MIB)</b>	<b>Новая строка</b>
snmpTargetAddrParams	"@mtaconfig_n" (То же значение, что и snmpTargetAddrName)
snmpTargetAddrStorageType	Переменное
snmpTargetAddrRowStatus	активен (1)

### 11.2.1.3 snmpTargetAddrExtTable

Для каждого элемента TLV-38 из файла конфигурации МТА ДОЛЖЕН создать одну строку согласно таблице 18.

**Таблица 18/J.167 – snmpTargetAddrExtTable**

<b>snmpTargetAddrExtTable (RFC 3584, SNMP-COMMUNITY-MIB)</b>	<b>Новая строка</b>
Имя столбца (* = Part of Index)	Значение в столбце
* snmpTargetAddrName	"@mtaconfig_n" где n находится в диапазоне от 0 до m – 1, где m – количество TLV-элементов приемника уведомлений в файле конфигурации
snmpTargetAddrTMask	<Zero length octet string> (строка октетов нулевой длины)
snmpTargetAddrMMS	0

### 11.2.1.4 snmpTargetParamsTable

Для каждого элемента TLV-38 из файла конфигурации МТА ДОЛЖЕН создать одну строку согласно таблице 19.

**Таблица 19/J.167 – snmpTargetParamsTable**

<b>snmpTargetParamsTable (RFC 3413, SNMP-TARGET-MIB)</b>	<b>Новая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpTargetParamsName	"@mtaconfig_n" где n находится в диапазоне от 0 до m – 1, где m – количество TLV-элементов приемника уведомлений в файле конфигурации
snmpTargetParamsMPModel SYNTAX: snmpMessageProcessingModel	SNMPv2c (1)
snmpTargetParamsSecurityModel SYNTAX: snmpSecurityModel	SNMPv2c (2) ПРИМЕЧАНИЕ – соответствие типов протоколов SNMP приводимым тут значениям отличается от snmpTargetParamsMPModel
snmpTargetParamsSecurityName	"@mtaconfig"
snmpTargetParamsSecurityLevel	NoAuthNoPriv
snmpTargetParamsStorageType	переменное
snmpTargetParamsRowStatus	активен (1)

### 11.2.1.5 snmpNotifyFilterProfileTable

Для каждого элемента TLV-38 из файла конфигурации с ненулевым значением подтипа 6 МТА ДОЛЖЕН создать одну строку согласно таблице 20.

Таблица 20/J.167 – snmpNotifyFilterProfileTable

snmpNotifyFilterProfileTable (RFC 3413, SNMP-NOTIFICATION-MIB)	New row
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpTargetParamsName	"@mtaconfig_n" где n находится в диапазоне от 0 до m – 1, где m – количество TLV-элементов приемника уведомлений в файле конфигурации
snmpNotifyFilterProfileName	"@mtaconfig_n" где n находится в диапазоне от 0 до m – 1, где m – количество TLV-элементов приемника уведомлений в файле конфигурации
snmpNotifyFilterProfileStorageType	переменное
snmpNotifyFilterProfileRowStatus	активен (1)

### 11.2.1.6 snmpNotifyFilterTable

Для каждого элемента TLV-38 из файла конфигурации с ненулевым значением подтипа 6 МТА ДОЛЖЕН создать одну строку согласно таблице 21.

Таблица 21/J.167 – snmpNotifyFilterTable

snmpNotifyFilterTable (RFC 3413, SNMP-NOTIFICATION-MIB)	Новая строка
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpNotifyFilterProfileName	"@mtaconfig_n" где n находится в диапазоне от 0 до m – 1, где m – количество TLV-элементов приемника уведомлений в файле конфигурации
* snmpNotifyFilterSubtree	<Filter OID> из TLV
snmpNotifyFilterMask	<Zero Length Octet String>
snmpNotifyFilterType	включенный (1)
snmpNotifyFilterStorageType	переменное
snmpNotifyFilterRowStatus	активен (1)

### 11.2.1.7 snmpCommunityTable

Если элементы TLV-38 присутствуют и вне зависимости от количества элементов МТА ДОЛЖЕН создать одну строку с фиксированными значениями, как показано в таблице 22.

**Таблица 22/J.167 – snmpCommunityTable**

<b>snmpCommunityTable (RFC 3584, SNMP-COMMUNITY-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpCommunityIndex	"@mtaconfig"
snmpCommunityName	"public"
snmpCommunitySecurityName	"@mtaconfig"
snmpCommunityContextEngineID	<The engineID of the MTA> (Идентификатор системы MTA)
snmpCommunityContextName	<Zero length octet string>
snmpCommunityTransportTag	<Zero length octet string>
snmpCommunityStorageType	Переменное
snmpCommunityStatus	активен (1)

**11.2.1.8 usmUserTable**

Таблица usmUserTable определена в RFC 3414. Значения в данной таблице определяют имя пользователя на удаленном приемнике уведомлений, в адрес которого направляется уведомление. Строки в данной таблице создаются двумя разными способами когда типы приемника уведомлений <Notification Receiver Type> 4 и 5 (согласно вложенному TLV 38.3) поддерживаются и включены в TLV-38.

- если Безопасное имя <Security Name> (TLV-38.7) не включено, вне зависимости от количества элементов в файле конфигурации MTA ДОЛЖЕН создать одну строку с фиксированными значениями, как показано в таблице 23.
- если Безопасное имя <Security Name> (TLV-38.7) включено, MTA ДОЛЖЕН создать дополнительные строки значений как описано вторым столбцом (Другие строки) в таблице 23. В таком случае создание дополнительных строк в таблице usmUserTable происходит каждый раз, когда возникает необходимость выяснить идентификатор системы (engine ID) приемника уведомлений. (см. RFC 3414 для получения более полной информации).

**Таблица 23/J.167 – usmUserTable**

<b>usmUserTable (RFC 3414, SNMP-USER-BASED-SM-MIB)</b>	<b>Постоянная строка Случай 1</b>	<b>Другие строки Случай 2</b>
Имя столбца (* = Часть индекса)	Значение в столбце	Значение в столбце
* usmUserEngineID	0x00, новая строка создается каждый раз, когда возникает необходимость выяснить идентификатор системы (engine ID) приемника уведомлений.	0x00, новая строка создается каждый раз, когда возникает необходимость выяснить идентификатор системы (engine ID) приемника уведомлений.
usmUserName	"@mtaconfig".	Когда другие строки созданы, данное значение заменяется на поле <Security Name> из TLV-элемента.
usmUserSecurityName	"@mtaconfig"	Когда другие строки созданы, данное значение заменяется на поле <Security Name> из TLV-элемента.
usmUserCloneFrom	<ignore> (zerodotZero) Данная строка не создается при помощи механизма клонирования	<ignore> (zerodotZero) Данная строка не создается при помощи механизма клонирования
usmUserAuthProtocol	Пустое значение (usmNoAuthProtocol)	Когда другие строки созданы, данное значение заменяется пустое значение (usmNoAuthProtocol) или

**Таблица 23/J.167 – usmUserTable**

<b>usmUserTable (RFC 3414, SNMP-USER-BASED-SM-MIB)</b>	<b>Постоянная строка Случай 1</b>	<b>Другие строки Случай 2</b>
		MD5 (usmHMACMD5AuthProtocol) или SHA (usmHMACSHAAuthProtocol) в зависимости от уровня безопасности пользователя SNMPv3.
usmUserAuthKeyChange	Пусто	Пусто
usmUserOwnAuthKeyChange	Пусто	Пусто
usmUserPrivProtocol	Случай 1: Пустое значение (usmNoPrivProtocol)	Когда другие строки созданы, данное значение заменяется пустое значение (usmNoPrivProtocol) или DES (usmDESPrivProtocol) в зависимости от уровня безопасности пользователя SNMPv3.
usmUserPrivKeyChange	Пусто	Пусто
usmUserOwnPrivKeyChange	Пусто	Пусто
usmUserPublic	Пусто	Пусто
usmUserStorageType	переменное (2)	переменное (2)
usmUserStatus	активен (1)	активен (1)

#### 11.2.1.9 vacmSecurityToGroupTable

В случае, если элементы TLV-38 присутствуют и вне зависимости от их количества МТА ДОЛЖЕН создать столбец "Вторая строка" и МОЖЕТ создать столбцы "Первая строка" и "Третья строка" с фиксированными значениями, как описано в таблице 24. МТА ДОЛЖЕН заполнять столбцы "Вторая строка" и "Третья строка" только в случае использования защищенного процесса.

**Таблица 24/J.167 – vacmSecurityToGroupTable**

<b>vacmSecurityToGroupTable (RFC 3415, SNMP-VIEW-BASED-ACM-MIB)</b>	<b>Первая строка</b>	<b>Вторая строка</b>	<b>Третья строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце	Значение в столбце	Значение в столбце
* vacmSecurityModel	SNMPV1 (1)	SNMPV2c (2)	SNMPUSM (3)
* vacmSecurityName	"@mtaconfig"	"@mtaconfig"	"@mtaconfig"
vacmGroupName	"@mtaconfigV1"	"@mtaconfigV2"	"@mtaconfigUSM"
vacmSecurityToGroupStorageType	переменное (2)	переменное (2)	переменное (2)
vacmSecurityToGroupStatus	активен (1)	активен (1)	активен (1)

#### 11.2.1.10 VacmAccessTable

В случае, если элементы TLV-38 присутствуют и вне зависимости от их количества МТА ДОЛЖЕН создать столбец "Вторая строка" и МОЖЕТ создать столбцы "Первая строка" и "Третья строка" с фиксированными значениями, как описано в таблице 25. МТА ДОЛЖЕН заполнять столбцы "Вторая строка" и "Третья строка" только в случае использования защищенного процесса.

**Таблица 25/J.167 – vacmAccessTable**

<b>vacmAccessTable (RFC 3415, SNMP-VIEW-BASED-ACM-MIB)</b>	<b>Первая строка</b>	<b>Вторая строка</b>	<b>Третья строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце	Значение в столбце	Значение в столбце
* vacmGroupName	"@mtaconfigV1"	"@mtaconfigV2"	"@mtaconfigUSM"
* vacmAccessContextPrefix	Пусто	Пусто	Пусто
* vacmAccessSecurityModel	SNMPv1 (1)	SNMPv2c (2)	USM (3)
* vacmAccessSecurityLevel	noAuthNoPriv (1)	noAuthNoPriv (1)	noAuthNoPriv (1)
vacmAccessContextMatch	точно (1)	точно (1)	точно (1)
vacmAccessReadViewName	Пусто	Пусто	Пусто
vacmAccessWriteViewName	Пусто	Пусто	Пусто
vacmAccessNotifyViewName	"@mtaconfig"	"@mtaconfig"	"@mtaconfig"
vacmAccessStorageType	переменное (2)	переменное (2)	переменное (2)
vacmAccessStatus	активен (1)	активен (1)	активен (1)

### 11.2.1.11 vacmViewTreeFamilyTable

В случае, если элементы TLV-38 присутствуют и вне зависимости от их количества приведенные ниже значение ДОЛЖНЫ быть созданы как показано в таблице 26. Следует отметить, что эти значения уже созданы при инициализации МТА.

**Таблица 26/J.167 – vacmViewTreeFamilyTable**

<b>vacmViewTreeFamilyTable (RFC 3415, SNMP-VIEW-BASED-ACM-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* vacmViewTreeFamilyViewName	"@mtaconfig"
* vacmViewTreeFamilySubtree	1.3
vacmViewTreeFamilyMask	<Default from MIB> (Значение по умолчанию из MIB)
vacmViewTreeFamilyType	включенный (1)
vacmViewTreeFamilyStorageType	переменное
vacmViewTreeFamilyStatus	активен (1)

## 11.3 Пример конфигурации TLV-38 и TLV-11

В данном пункте приводятся примеры создания TLV-38 и TLV-11 для конфигурации структуры SNMP, основанной на структурной модели обработке сообщений, определенной в RFC 3410, RFC 3411 и RFC 3412.

### 11.3.1 Пример TLV-38

Данный пункт является информационным. Приведенный ниже пример показывает удобство применения TLV-38. Одной из целей данного пункта является иллюстрация использования @mtaConfig\_n. Были сделаны следующие допущения:

- МТА игнорирует значения с <trap type> 1 и поддерживает <trap type> 2, 3, 4 и 5.
- В ходе процесса конфигурации МТА уже получил значения usmUserName и usmUserSecurityName ('mtaUser' и еще одно значением – 'superUser'). Для простоты, с данным профилем не связаны никакие значения VACM.

В таблице 27 показаны элементы Файла конфигурации. Пустые ячейки означают использование значений по умолчанию в случае необходимости.

**Таблица 27/J.167 – Пример элементов файла конфигурации**

<b>Вложенный TLV</b>					
<b>Порядок TLV-38 в файле конфигурации</b>	<b>TLV-38 Номер 1</b>	<b>TLV-38 Номер 2</b>	<b>TLV-38 Номер 3</b>	<b>TLV-38 Номер 4</b>	<b>TLV-38 Номер 5</b>
SNMP Notification Receiver IP Address (IP-адрес приемника уведомлений SNMP)	10.0.5.9	10.0.5.9	10.0.4.9	10.0.4.9	10.0.8.9
SNMPv2c Notification Receiver UDP Port Number (Номер UDP-порта приемника уведомлений SNMPv2c)		162		57000	
SNMPv2c Notification Receiver Trap Type (Тип прерывания приемника уведомлений SNMPv2c)	2	3	1	4	5
SNMPv2c Notification Receiver Timeout (Период ожидания приемника уведомлений SNMPv2c)	1500		2000		
SNMPv2c Notification Receiver Retries (Повторы приемника уведомлений SNMPv2c)	3	1	2		
Notification Receiver Filtering Parameters (Параметры фильтрации приемника уведомлений)	org	pktcMtaDevProvisioningStatus	mib-2	pktcMtaMib	pktcMtaDevProvisioningStatus
Notification Receiver Security Name (Безопасное имя приемника уведомлений)		не используется		SuperUser	mtaUser
<hr/>					
@mta@config n	0	1	2	3	4

### 11.3.2 Содержимое структурных таблиц SNMP после обработки приведенного выше примера TLV-38

На основе сделанных допущений и приведенного выше примера TLV-38 в данном пункте приводятся таблицы, которые следовало создать МТА. МТА игнорирует TLV-38 номер 1 (тип уведомления = 1), таким образом, значения @mtaconfig\_2 не существуют, Безопасное имя при TLV n=2 также игнорируется.

**Таблица 28/J.167 – snmpCommunityTable**

Наименование	[@mtaconfig]
Name	"public"
SecurityName	@mtaconfig
ContextEngineID	<MTA_ENGINEID>
ContextName	""
TransportTag	""
StorageType	переменный
Status	активен

**Таблица 29/J.167 – snmpTargetAddrExtTable**

Наименование	[@mtaconfig_0]	[@mtaconfig_1]	[@mtaconfig_2]	[@mtaconfig_3]	[@mtaconfig_4]	[@mtaconfig_5]
TMask	""	""	""	""	""	""
MMS	0	0	0	0	0	0

**Таблица 30/J.167 – usmUserTable**

Наименование	[0x00][@mtaconfig]	[<local-EngineID>][mtaUser]	[<local-EngineID>][superUser]	[0x00/<Notif-recv-EngineID>][mtaUser]	[0x00/<Notif-recv-EngineID>][superUser]
SecurityName	@mtaconfig	MtaUser	superUser	mtaUser	superUser
CloneFrom	ZeroDotZero	ZeroDotZero	zeroDotZero	zeroDotZero	zeroDotZero
AuthProtocol	usmNoAuthProtocol	usmNoAuthProtocol	usmHMACMD5AuthProtocol	usmNoAuthProtocol	usmHMACMD5AuthProtocol
AuthKeyChange	""	""	""	""	""
OwnAuthKeyChange	""	""	""	""	""
PrivProtocol	usmNoPrivProtocol	usmNoPrivProtocol	usmDESPrivProtocol	usmNoPrivProtocol	usmDESPrivProtocol
PrivKeyChange	""	""	""	""	""
OwnPrivKeyChange	""	""	""	""	""
Public	""	""	""	""	""
StorageType	Переменный	Переменный	Переменный	Переменный	Переменный
Status	Активен	Активен	Активен	Активен	Активен

**Таблица 31/J.167 – vacmContextTable**

Наименование
VacmContextName

**Таблица 32/J.167 – vacmSecurityToGroupTable**

Наименование	[1][@mtaconfig]	[2][@mtaconfig]	[3][@mtaconfig]
GroupName	@mtaconfigV1	@mtaconfigV2	@mtaconfigUSM
SecurityToGroupStorageType	Переменный	Переменный	Переменный
SecurityToGroupStatus	Активен	Активен	Активен

**Таблица 33/J.167 – vacmAccessTable**

Наименование	[@mtaconfigV1][1][noAuthNoPriv]	[@mtaconfigV2][2][noAuthNoPriv]	[@mtaconfigUSM][3][noAuthNoPriv]
ContextMatch	exact	exact	exact
ReadViewName	""	""	""
WriteViewName	""	""	""
NotifyViewName	@mtaconfig	@mtaconfig	@mtaconfig
StorageType	Переменный	Переменный	Переменный
Status	Активен	Активен	Активен

**Таблица 34/J.167 – vacmViewTreeFamilyTable**

Наименование	[@mtaconfig][org]
Mask	""
Type	Included
StorageType	Переменный
Status	Активен

**Таблица 35/J.167 – snmpNotifyTable**

Наименование	[@mtaconfig_inform]	[@mtaconfig_trap]
Tag	@mtaconfig_inform	@mtaconfig_trap
Type	Inform	Прерывание
StorageType	Volatile	Переменный
RowStatus	Active	Активен

**Таблица 36/J.167 – snmpTargetAddrTable**

Наименование	[@mtaconfig_0]	[@mtaconfig_1]	[@mtaconfig_3]	[@mtaconfig_4]
TDomain	snmpUDPDomain	snmpUDPDomain	snmpUDPDomain	snmpUDPDomain
TAddress	"0A 00 05 09 00 82"	"0A 00 05 09 00 82"	"0A 00 04 09 DE A8"	"0A 00 08 09 00 82"
Timeout	1500	1500	1500	1500
RetryCount	3	1	3	3
TagList	@mtaconfig_trap	@mtaconfig_inform	@mtaconfig_trap	@mtaconfig_inform
Params	@mtaconfig_0	@mtaconfig_1	@mtaconfig_3	@mtaconfig_4
StorageType	Переменный	Переменный	Переменный	Переменный
RowStatus	Активен	Активен	Активен	Активен

**Таблица 37/J.167 – snmpTargetParamsTable**

Наименование	[@mtaconfig_0]	[@mtaconfig_1]	[@mtaconfig_3]	[@mtaconfig_4]
MPModel	1	1	3	3
SecurityModel	2	2	3	3
SecurityName	@mtaconfig	@mtaconfig	@mtaconfig	@mtaconfig
SecurityLevel	noAuthNoPriv	noAuthNoPriv	noAuthNoPriv	NoAuthNoPriv
StorageType	Переменный	Переменный	Переменный	Переменный
RowStatus	Активен	Активен	Активен	Активен

**Таблица 38/J.167 – snmpNotifyFilterProfileTable**

Наименование	[@mtaconfig_0]	[@mtaconfig_1]	[@mtaconfig_3]	[@mtaconfig_4]
Name	[@mtaconfig_0]	[@mtaconfig_1]	[@mtaconfig_3]	[@mtaconfig_4]
StorType	Переменный	Переменный	Переменный	Переменный
RowStatus	Активен	Активен	Активен	Активен

**Таблица 39/J.167 – snmpNotifyFilterTable**

Наименование	[@mtaconfig_0] [org]	[@mtaconfig_1] [pktcMtaProvision- ingStatus]	[@mtaconfig_3] [PktcMtaMib]	[@mtaconfig_4] [pktcMtaProvision- ingStatus]
Mask	""	""	""	""
Type	Включенный	Включенный	Включенный	Включенный
StorageType	Переменный	Переменный	Переменный	Переменный
RowStatus	Активен	Активен	Активен	Активен

## 12 Требования к управлению SNMPv2c

Управление устройством МТА при помощи протокола SNMPv2c может быть сконфигурировано оператором, в случае необходимости, путем установления соответствующих таблиц сосуществования (используя TLV-11) в файле конфигурации МТА или посредством управления по завершении подготовки к работе.

- При использовании базового и гибридного процессов МТА ДОЛЖЕН сконфигурировать таблицы, описанные в п.п. 12.1 и 12.2 для того, чтобы предоставить SNMPv2c доступ к системе управления по умолчанию (модуль подготовки к работе, указанный в Опции DHCP 122 подопции 3) с правами на чтение/запись.
- При использовании защищенного процесса МТА ДОЛЖЕН сконфигурировать таблицы, приведенные в п. 12.2 в случае, если файл конфигурации содержит связки переменных TLV-11 с данными таблицы snmpCommunityTable. Для того, чтобы закрыть SNMP входящий доступ к МТА файл конфигурации может дополнительно содержать связки переменных TLV-11 для таблиц snmpTargetAddrTable и snmpTargetAddrExtTab.

В Дополнении I приведен примерный шаблон включения управления через SNMPv2c для операторов.

**12.1 Содержимое таблиц, созданное МТА после шага МТА4 в ходе выполнения гибридного и базового процессов в режиме сосуществования SNMPV2c**

См. таблицы 40–42.

**Таблица 40/J.167 – snmpCommunityTable Content**

<b>snmpCommunityTable (RFC 3584, SNMP-COMMUNITY-MIB)</b>	<b>Доступ на чтение/запись</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpCommunityIndex	"@mtaprov"
snmpCommunityName	"private"
snmpCommunitySecurityName	"@mtaprov"
snmpCommunityContextEngineID	<The engineID of the MTA>
snmpCommunityContextName	Пусто
snmpCommunityTransportTag	"@mtaprovTag"
snmpCommunityStorageType	Переменный (2)
snmpCommunityStatus	активен (1)

**Таблица 41/J.167 – snmpTargetAddrTable Content**

<b>snmpTargetAddrTable (RFC 3413, SNMP-TARGET-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpTargetAddrName	"@mtaprov"
snmpTargetAddrTDomain	snmpUDPDomain = snmpDomains.1
snmpTargetAddrTAddress (IP-адрес неофициального модуля SNMP)	ОСТЕТ STRING (6) (строка октетов) Оклеты 1–4: <IP address of SNMP Entity derived from 122.3> (IP-адрес модуля SNMP, взятый из 122.3) Оклеты 5–6: любое 2-байтовое значение порта
snmpTargetAddrTimeout	Ignore, <use default>
snmpTargetAddrRetryCount	ignore, <use default>
snmpTargetAddrTagList	"@mtaprovTag"
snmpTargetAddrParams	"@mtaprov"
snmpTargetAddrStorageType	Переменный (2)
snmpTargetAddrRowStatus	Активен(1)

**Таблица 42/J.167 – snmpTargetAddrExtTable Content**

<b>snmpTargetAddrExtTable (RFC 3584, SNMP-COMMUNITY-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Part of Index)	Значение в столбце
* snmpTargetAddrName	"@mtaprov"
snmpTargetAddrTMask	FFFFFFFF:0000
snmpTargetAddrMMS	0

## 12.2 Значения SNMP по умолчанию для доступа SNMPv2

Таблицы 43–49 ДОЛЖНЫ быть созданы МТА при инициализации агента SNMP для конфигурации доступа SNMPv2с.

**Таблица 43/J.167 – vacmSecurityToGroupTable default entries**

<b>vacmSecurityToGroupTable (RFC 3415, SNMP-VIEW-BASED- ACM-MIB)</b>	<b>Первая строка</b>	<b>Вторая строка</b>	<b>Третья строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце	Значение в столбце	Значение в столбце
* vacmSecurityModel	SNMPv2c (2)	SNMPv2c (2)	SNMPv2c (2)
* vacmSecurityName	"@mtaprov"	"admin"	"operator"
vacmGroupName	"@mtaprov"	"admin"	"operator"
vacmSecurityToGroupStorageType	постоянное (4)	постоянное (4)	постоянное (4)
vacmSecurityToGroupStatus	Активен (1)	Активен (1)	Активен (1)

**Таблица 44/J.167 – vacmAccessTable default entries**

<b>vacmAccessTable (RFC 3415, SNMP-VIEW- BASED-ACM-MIB)</b>	<b>Первая строка</b>	<b>Вторая строка</b>	<b>Третья строка</b>
Column Name (* = Part of Index)	Значение в столбце	Значение в столбце	Значение в столбце
* vacmGroupName	"@mtaprov"	"admin"	"operator"
* vacmAccessContextPrefix	Empty	Empty	Empty
* vacmAccessSecurityModel	SNMPv2 (2)	SNMPv2 (2)	SNMPv2 (2)
* vacmAccessSecurityLevel	noAuthNoPriv (1)	noAuthNoPriv (1)	noAuthNoPriv (1)
vacmAccessContextMatch	exact (1)	exact (1)	exact (1)
vacmAccessReadViewName	"@mtaconfig"	"@mtaconfig"	"@mtaconfig"
vacmAccessWriteViewName	"@mtaconfig"	"@mtaconfig"	Empty
vacmAccessNotifyViewName	"@mtaconfig"	Empty	Empty
vacmAccessStorageType	постоянное (4)	постоянное (4)	постоянное (4)
vacmAccessStatus	Активен (1)	Активен (1)	Активен (1)

**Таблица 45/J.167 – vacmViewTreeFamilyTable default entry**

<b>vacmViewTreeFamilyTable (RFC 3415, SNMP-VIEW-BASED-ACM-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Часть индекса)	Column Value
* vacmViewTreeFamilyViewName	@mtaconfig
vacmViewTreeFamilySubtree	1.3
vacmViewTreeFamilyMask	Пусто <значение по умолчанию из MIB>
vacmViewTreeFamilyType	включенный (1)
vacmViewTreeFamilyStorageType	переменный (2)
vacmViewTreeFamilyStatus	активен (1)

Следует отметить, что эти значения также создаются по умолчанию для обеспечения обработки TLV-38. Это означает, что для определения конфигурации управления SNMPv2c и TLV-38 требуется только один элемент, существующий по умолчанию.

**Таблица 46/J.167 – snmpTargetParamsTable default entry**

<b>snmpTargetParamsTable (RFC 3413, SNMP-TARGET-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpTargetParamsName	"@mtaprov"
snmpTargetParamsMPModel	1
snmpTargetParamsSecurityModel	2
snmpTargetParamsSecurityName	"@mtaprov"
snmpTargetParamsSecurityLevel	noAuthNoPriv
snmpTargetParamsStorageType	постоянное (4)
snmpTargetParamsRowStatus	активен (1)

**Таблица 47/J.167 – snmpNotifyTable default entry**

<b>snmpNotifyTable (RFC 3413, SNMP-NOTIFICATION-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpNotifyName	"@mtaprov"
snmpNotifyTag	"@mtaprovTag"
snmpNotifyType	информационное сообщение (2)
snmpNotifyStorageType	постоянный (4)
snmpNotifyRowStatus	активен (1)

**Таблица 48/J.167 – snmpNotifyFilterProfileTable default entry**

<b>snmpNotifyFilterProfileTable (RFC 3413, SNMP-NOTIFICATION-MIB)</b>	<b>Первая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце
* snmpTargetParamsName	"@mtaprov"
snmpNotifyFilterProfileName	"@mtaprov"
snmpNotifyFilterProfileStorageType	постоянный (4)
snmpNotifyFilterProfileRowStatus	активен (1)

**Таблица 49/J.167 – snmpNotifyFilterTable default entry**

<b>snmpNotifyFilterTable (RFC 3413, SNMP-NOTIFICATION-MIB)</b>	<b>Первая строка</b>	<b>Вторая строка</b>
Column Name (* = Part of Index)	Column Value	Значение в столбце
* snmpNotifyFilterProfileName	"@mtaprov"	"@mtaprov"
* snmpNotifyFilterSubtree	pktcMtaNotification	snmpTraps
snmpNotifyFilterMask	Пусто	Пусто
snmpNotifyFilterType	включенный (1)	включенный (1)
snmpNotifyFilterStorageType	постоянный (4)	постоянный (4)
snmpNotifyFilterRowStatus	активен (1)	активен (1)

## **13 Поддержка отправки отчетов о влиянии перебоев в оказании услуг и прочих расширенных возможностей**

### **13.1 Поддержка требований eDOCSIS**

Встроенный МТА IPCablecom относится к классу устройств eSAFE в рамках eDOCSIS функционировать в согласно соответствующим пунктам спецификации eDOCSIS, приведенной в Рек. МСЭ-Т J.126. В дополнение к обычным требованиям, в спецификации содержатся требования, которые, вероятно, будут определены в соответствующей спецификации eSAFE. Данный пункт рассматривает эти дополнительные требования, которые полагаются необходимыми к реализации спецификацией IPCablecom.

Требования возможно подразделить на:

- Требования к анализу влияния и составлению отчетов.
- Директивы перезагрузки eSAFE.

#### **13.1.1 Требования к анализу влияния и составлению отчетов**

В Рек. МСЭ-Т J.126 указано, что встроенный СМ имеет возможность отправки отчета о "Влиянии перебоев в оказании услуг" (Service Interruption Impact) для каждого устройства eSAFE в случае, если обслуживание, связанное с передачей данных действительно было прервано в момент выполнения запроса. В данном пункте обсуждаются уровень влияния и механизмы предоставления отчетов. Следует отметить, что встроенный МТА IPCablecom как правило связан с несколькими услугами (передача голоса, факсимильной информации) и с несколькими экземплярами каждой услуги (на каждой сконфигурированной конечной точке) и поэтому встроенный МТА ДОЛЖЕН отчитываться о максимально возможном влиянии на услуги/конечные точки.

##### **13.1.1.1 Анализ влияния**

Признается, что услуга или конечная точка подверглись влиянию, если конечная точка была "активна" и обслуживание, связанное с передачей данных, было прервано. "Активное" состояние определяется как состояние "снятой трубки" (offHook(3)) или "лежащей трубки при наличии активности NCS" (onHookPlusNCSActivity(3)) как определено в pktcNcsEndPntHookState. Для получения более подробной информации см. Рек. МСЭ-Т J.126.

##### **13.1.1.2 Поддерживаемые уровни влияния и способы предоставления отчета**

В рамках IPCablecom любое влияние на "активную"(даже потенциально) услугу, ДОЛЖНО признаваться Сильным влиянием, а все остальное – Слабым влиянием.

Таким образом, МТА ДОЛЖЕН отчитываться о влиянии в следующем порядке:

- Сильное влияние – если какие-либо конечные точки, связанные с данным МТА "активны", МТА ДОЛЖЕН отчитаться о наличии Сильного влияния.
- Слабое влияние – если все конечные точки, способные предоставлять услуги, связанные с данным МТА неактивны, МТА ДОЛЖЕН отчитаться о наличии Слабого влияния.

### **13.2 Расширение MIB IPCablecom**

Расширение MIB IPCablecom определено для всех новых MIB, входящих в состав IPCablecom 1.5. Для получения дополнительной информации см. Рек. МСЭ-Т J.166. Расширения касаются MIB МТА и MIB сигнализации.

#### **13.2.1 Расширение MIB МТА**

Расширение MIB МТА определено в Рек. МСЭ-Т J.166. Оно предоставляет новые средства для управления новыми функциями, такими, как множественное предоставление канала в течение одного временного интервала (MGPI) на конечной точке.

### **13.2.2 Расширение MIB сигнализации**

Расширение MIB сигнализации IPCablecom определено в Рек. МСЭ-Т J.166. Оно предоставляет дополнительные возможности в области контроля и отправки отчетов конечных точек в том, что касается DTMF-ретрансляции, работы с карантинном, состояния абонентского терминала и т. п.

### **13.3 MIB резервного питания**

Встроенный МТА представляет собой встроенное устройство, снабженное кабельным модемом. Поскольку телефония является высоковольтостребованной услугой, резервное питание очень важно. В черновом варианте Рек. МСЭ-Т J.bb определен набор MIB, предназначенных для технического обслуживания и поддержания в рабочем состоянии модулей батарей. Встроенные МТА, имеющие функциональную возможность резервного питания, ДОЛЖНЫ поддерживать MIB, описанные в черновом варианте Рек. МСЭ-Т J.bb.

### **13.4 MIB SYSLOG**

В Рек. МСЭ-Т J.166 разработан ряд MIB, предназначенных для поддержания уровня модульности услуги SYSLOG. Данные MIB помогают оператору решать возникающие при работе с SYSLOG проблемы и обеспечивают более высокий уровень контроля над сообщениями SYSLOG.

### **13.5 Обнаружение чужеродного потенциала**

Обнаружение чужеродного потенциала чрезвычайно важно для предоставления услуг телефонии. MIB "pktcEnEndPntInfoTable" была определена в Рек. МСЭ-Т J.166 с целью предоставления возможности своевременного отчета обо всех обнаружениях такого рода. Встроенные МТА ДОЛЖНЫ реализовывать такую возможность.

## Дополнение I

### Пример конфигурации для случая сосуществования SNMPv2c – Шаблон для поставщиков услуг

Операторы могут воспользоваться приведенным в данном Дополнении шаблоном для того, чтобы включить управление на основе SNMPv2c (в данном примере используются значения по умолчанию, определенные в п. 12.2). Следует отметить, что поставщики услуг не должны использовать данный пример в обязательном порядке. См. таблицы I.1–I.3.

**Таблица I.1/J.167 – snmpCommunityTable шаблон для файла конфигурации базового и гибридного процессов**

snmpCommunityTable (RFC 3584, SNMP-COMMUNITY-MIB)	Доступ чтение/запись	Доступ только чтение
Имя столбца (* = Часть индекса)	Значение в столбце	Значение в столбце
* snmpCommunityIndex	"admin"	"operator" or <any>
snmpCommunityName	<SNMP Community Name>	<SNMP Community Name>
snmpCommunitySecurityName	"admin"	"operator"
snmpCommunityContextEngineID	<The engineID of the MTA>	<The engineID of the MTA>
snmpCommunityContextName	Пусто	Пусто
snmpCommunityTransportTag	"adminTag"	"operatorTag"
snmpCommunityStorageType	переменное (2)	переменное (2)
snmpCommunityStatus	createAndGo (4)	createAndGo (4)

**Таблица I.2/J.167 – snmpTargetAddrTable шаблон для файла конфигурации базового и гибридного процессов**

snmpTargetAddrTable (RFC 3413 – SNMP-TARGET-MIB)	Первая строка	Вторая строка
Column Name (* = Part of Index)	Значение в столбце	Значение в столбце
* snmpTargetAddrName	"admin"	"operator"
snmpTargetAddrTDomain	snmpUDPDomain = snmpDomains.1	snmpUDPDomain = snmpDomains.1
snmpTargetAddrTAddress (IP Address non-Authoritative SNMP entity)	ОCTET STRING (6) Октеты 1–4: <SNMP Mgmt Station IPv4 Address> Октеты 5–6: <0x0000>	ОCTET STRING (6) Октеты 1–4: <SNMP Mgmt Station IPv4 Address> Октеты 5–6: <0x0000>
snmpTargetAddrTimeout	Ignore, <use default>	Ignore, <use default>
snmpTargetAddrRetryCount	Ignore, <use default>	Ignore, <use default>
snmpTargetAddrTagList	"adminTag"	"operatorTag"
snmpTargetAddrParams	Пусто	Пусто
snmpTargetAddrStorageType	переменное (2)	переменное (2)
snmpTargetAddrRowStatus	createAndGo (4)	createAndGo (4)

**Таблица I.3/J.167 – snmpTargetAddrExtTable шаблон для файла конфигурации базового и гибридного процессов**

<b>snmpTargetAddrExtTable (RFC 3584, SNMP-COMMUNITY-MIB)</b>	<b>Первая строка</b>	<b>Вторая строка</b>
Имя столбца (* = Часть индекса)	Значение в столбце	Значение в столбце
* snmpTargetAddrName	"admin"	"operator"
snmpTargetAddrTMask	СТРОКА ОКТЕТОВ (6) Октеты 1–4: <SNMP Mgmt Station Sub Net Mask> (Маска подсети станции управления SNMP) Октеты 5–6: <0x0000>	СТРОКА ОКТЕТОВ (6) Октеты 1–4: <SNMP Mgmt Station Sub Net Mask> (Маска подсети станции управления SNMP) Октеты 5–6: <0x0000>
snmpTargetAddrMMS	0	0





## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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
<b>Серия J</b>	<b>Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов</b>
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