МСЭ-Т

J.191

(07/2002)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Некоторые аспекты

Упаковка возможностей IP для усовершенствования кабельных модемов

Рекомендация МСЭ-Т J.191

(Ранее "Рекомендация МККТТ")

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ J

ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

Общие Рекомендации	J.1 – J.19
Общие спецификации для передачи аналоговых звуковых программ	J.10 – J.19
Характеристики показателей качества линий для аналоговых звуковых программ	J.20 – J.29
Оборудование и линии, используемые для линий аналоговых звуковых программ	J.30 – J.39
Цифровые кодеры для сигналов аналоговых звуковых программ	J.40 – J.49
Цифровая передача сигналов звуковых программ	J.50 – J.59
Линии передачи для аналоговых телевизионных программ	J.60 – J.69
Аналоговая телевизионная передача по металлическим линиям и взаимное соединение с радиорелейными звеньями	J.70 – J.79
Цифровая передача телевизионных сигналов	J.80 – J.89
Вспомогательные цифровые услуги для телевизионной передачи	J.90 – J.99
Эксплуатационные требования и методы для телевизионной передачи	J.100 – J.109
Диалоговые системы для распределения цифрового телевидения	J.110 – J.129
Транспортирование сигналов MPEG-2 по сетям с пакетной обработкой	J.130 – J.139
Измерение качества обслуживания	J.140 – J.149
Распределение цифрового телевидения по местным абонентским сетям	J.150 – J.159
IPCablecom	J.160 – J.179
Некоторые аспекты	**J.180 – J.199**
Приложение для диалогового цифрового телевидения	J.200 – J.209

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

Рекомендация МСЭ-Т J.191

Упаковка возможностей IP для усовершенствования кабельных модемов

Резюме

Эта Рекомендация предоставляет набор возможностей, основанных на IP, которые могут быть добавлены к кабельному модему, что даст возможность кабельным операторам предоставлять своим пользователям дополнительный набор усовершенствованных услуг, включая поддержку Качества обслуживания (*QoS, Quality of Service*) модели IPCablecom, усовершенствованную безопасность, дополнительные свойства по административному управлению и по обеспечению, а также улучшенную адресацию и обработку пакетов.

Источник

Рекомендация МСЭ-Т J.191 была подготовлена Исследовательской комиссией ИК 9 МСЭ-Т (2001-2004 гг.) и утверждена по процедуре Резолюции 1 ВАСЭ 29 июля 2002 года.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи (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.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, разрабатывают 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 данной Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация данной Рекомендации может включать в себя 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 извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации данной 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.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т J.191

Упаковка возможностей IP для усовершенствования кабельных модемов

1 Сфера применения

Эта Рекомендация предоставляет набор возможностей, основанных на IP, которые могут быть добавлены к кабельному модему, что даст возможность кабельным операторам предоставлять своим пользователям дополнительный набор усовершенствованных услуг, включая поддержку Качества обслуживания (*QoS, Quality of Service*) модели IPCablecom, усовершенствованную безопасность, дополнительные свойства по административному управлению и по обеспечению, а также улучшенную адресацию и обработку пакетов.

2 Ссылки

2.1 Нормативные ссылки

В ссылках по данному тексту, нижеследующие Рекомендации МСЭ-Т и другие ссылки содержат положения, которые поддерживают эту Рекомендацию. На момент публикации указанные издания были действующими. Все Рекомендации и другие ссылки являются предметом пересмотра; поэтому всем пользователям этой Рекомендации предлагается изучить возможность применения самого современного издания Рекомендаций и других ссылок, приведенных ниже. Перечень действующих в данный момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ внутри этой Рекомендации не дает ему, как отдельно взятому документу, статус Рекомендации.

[МСЭ-Т J.112] Дополнение B Рекомендации МСЭ-Т J.112 (2001), *Спецификации интерфейсов услуг передачи данных по кабелю: Спецификация радиочастотного интерфейса.*

[МСЭ-Т J.161] Рекомендация МСЭ-Т J.161 (2001), *Требования к кодеку аудио для обеспечения двунаправленной услуги аудио через сети кабельного телевидения, используя кабельные модемы.*

[МСЭ-Т J.163] Рекомендация МСЭ-Т J.163 (2001), *Динамическое качество обслуживания для обеспечения услуг реального времени через сети кабельного телевидения, используя кабельные модемы.*

[МСЭ-Т J.170] Рекомендация МСЭ-Т J.170 (2002), *Спецификация безопасности модели IPCablecom.*

[МСЭ-Т X.509] Рекомендация МСЭ-Т X.509 (2000) | ИСО/МЭК 9594-8:2001, *Информационные технологии – Взаимное соединение открытых систем – Справочник: Открытый ключ и структура сертификата атрибута.*

[МСЭ-Т X.690] Рекомендация МСЭ-Т X.690 (2002) | ИСО/МЭК 8825-1:2002, *Информационные технологии – Правила кодирования ASN.1: Спецификация основного кодирования (BER, Basic Encoding), Правил канонического кодирования (CER, Canonical Encoding Rules) и Правил выделенного кодирования (DER, Distinguished Encoding Rules).*

[FIPS 140-2] FIPS PVB 140-2 (2001), *Требования безопасности для криптографических модулей, Департамент торговли, NIST.*

[ИСО/МЭК 10038] ИСО/МЭК 10038 (Стандарт 802.1D ANSI/IEEE): 1993, *Информационные технологии – Связь и обмен информацией между системами – Местные сети – Мосты управления доступом к носителю информации (MAC, Media access control).*

[RFC 768] IETF RFC 768 (1980), *Датаграммный протокол пользователя.*

[RFC 792] IETF RFC 792 (1981), *Протокол сообщения для управления Интернет*

[RFC 868] IETF RFC 868 (1983), *Протокол времени.*

[RFC 1034] IETF RFC 1034 (1987), *Названия доменов – Концепции и возможности.*

[RFC 1035] IETF RFC 1035 (1987), *Названия доменов – Осуществление и спецификация.*

[RFC 1122] IETF RFC 1122 (1989), *Требования для ведущих узлов Интернет – Уровни связи.*

[RFC 1123] IETF RFC 1123 (1989), *Требования для ведущих узлов Интернет – Приложение и поддержка.*

[RFC 1157] IETF RFC 1157 (1990), *Простой протокол сетевого административного управления (SNMP, Simple Network Management Protocol).*

[RFC 1350] IETF RFC 1350 (1992), *Протокол TFTP (Пересмотр 2.)*

[RFC 1901] IETF RFC 1901 (1996), *Введение в протокол SNMPv2, основанный на сообществе*.

[RFC 1905] IETF RFC 1905 (1996), *Операции протоколов для версии 2 Простого протокола сетевого административного управления (SNMPv2).*

[RFC 1907] IETF RFC 1907 (1996), *Информационная база административного управления для версии 2 Простого протокола сетевого административного управления (SNMPv2).*

[RFC 2011] IETF RFC 2011 (1996), *Информационная база административного управления SNMPv2 для протокола Интернет, использующего SMIv2.*

[RFC 2013] IETF RFC 2013 (1996), *Информационная база административного управления SNMPv2 для Датаграммного протокола пользователя, использующего SMIv2.*

[RFC 2131] IETF RFC 2131 (1997), *Протокол динамической конфигурации ведущего узла.*

[RFC 2132] IETF RFC 2132 (1997), *Варианты выбора DHCP и расширения поставщика BOOTP.*

[RFC 2236] IETF RFC 2236 (1997), *Протокол административного управления группами Интернет, версия 2.*

[RFC 2349] IETF RFC 2349 (1998), *Интервал выдержки времени TFTP и варианты выбора размера для переноса.*

[RFC 2570] IETF RFC 2570 (1999), *Введение в версию 3 структуры сетевого административного управления по стандарту Интернет.*

[RFC 2571] IETF RFC 2571 (1999), *Архитектура для описания структур административного управления SNMP.*

[RFC 2572] IETF RFC 2572 (1999), *Обработка сообщения и координация для*

Простого протокола сетевого административного управления (SNMP).

[RFC 2573] IETF RFC 2573 (1999), *Приложения SNMP.*

[RFC 2574] IETF RFC 2574 (1999), *Модель безопасности, основанная на пользователе (USM, User-based Security Model), для версии 3 Простого протокола сетевого административного управления (SNMPv3).*

[RFC 2575] IETF RFC 2575 (1999), *Модель управления доступом, основанная на обзоре (VACM, View-based Access Control Model), для Простого протокола сетевого административного управления (SNMP).*

[RFC 2576] IETF RFC 2576 (2000), *Сосуществование между версией 1, версией 2 и версией 3 Структуры сетевого административного управления на основе стандарта Интернет.*

[RFC 2578] IETF RFC 2578 (1999), *Структура версии 2 Информации административного управления (SMIv2, Structure of Management Information).*

[RFC 2579] IETF RFC 2579 (1999), *Текстовые соглашения для SMIv2.*

[RFC 2580] IETF RFC 2580 (1999), *Заявления о соответствии для SMIv2.*

[RFC 2669] IETF RFC 2669 (1999), *Информационная база административного управления кабельным устройством MIB из кабельного устройства DOCSIS для кабельных модемов и систем завершения кабельных модемов, соответствующих спецификации DOCSIS.*

[RFC 2670] IETF RFC 2670 (1999), *Информационная база административного управления радиочастотным интерфейсом (RF, Radio Frequency) для интерфейсов RF, соответствующих MCNS/DOCSIS.*

[RFC 2786] IETF RFC 2786 (2000), *Информационная база административного управления ключом USM и тестовые соглашения.*

[RFC 2863] IETF RFC 2863 (2000), *База MIB Группы интерфейсов.*

[RFC 3022] IETF RFC 3022 (2001), *Традиционный транслятор сетевого адреса IP (Традиционный NAT).*

[RFC 3280] IETF RFC 3280 (2002), *Сертификат инфраструктуры открытого ключа X.509 Интернет и профиль перечня отмены сертификата (CRL, Certificate Revocation List).*

2.2 Информативные ссылки

[FIPS 186-2] FIPS PUB 186-2 (2000), *Стандарт цифровой подписи, Департамент торговли, NIST.*

[RFC 347] IETF RFC 347 (1972), *Процесс эха.*

[RFC 2663] IETF RFC 2663 (1999), *Терминология и соображения по транслятору сетевого адреса IP (NAT, Network Address Translator).*

[DOCSIS2] *Информационная база административного управления для Кабельных модемов и систем завершения кабельных модемов DOCSIS для положительной величины основной конфиденциальности,* draft-ietf-ipcdn-bpiplus-mib-01.txt (работа продолжается).

draft-ietf-ipcdn-bpiplus-mib-06 ПРОЕКТ ИНТЕРНЕТ – База MIB положительной величины основной конфиденциальности DOCSIS - *Информационная база*

административного управления для Кабельных модемов и систем завершения кабельных модемов DOCSIS для положительной величины основной конфиденциальности, ноябрь 2001 года.

[ID-IGMP] FENNER (W) и др. *Циркулярная переадресация на основе IGMP ("Посредничество IGMP")*, Проект Интернет IETF, http://ietf.org/internet-drafts/drafts-ietf-magma-igmp-proxy-oo.txt.

3 Термины и определения

Эта Рекомендация определяет следующие термины:

3.1. портал кабельной безопасности (*CSP, cable security portal*): Функциональный элемент, который обеспечивает функции трансляции и административного управления безопасностью между сетью HFC и домом.

3.2. сервер административного управления вызовом (*CMS, call management server*): [IPCablecom] Управляет соединениями аудио. В терминологии MGCP/SGCP также называется Агентом вызова.

3.3. динамическое Качество обслуживания (*DQoS, dynamic Quality of Service*): [IPCablecom] Значение, назначенное налету для каждой связи в зависимости от затребованного качества QoS.

3.4. встроенный адаптер терминала мультимедиа (*E-MTA, embedded multimedia terminal adapter*): [IPCablecom] Отдельный узел, который содержит как адаптер MTA, так и кабельный модем.

3.5. IP-усовершенствованный кабельный модем: Кабельный модем, который был усовершенствован путем добавления возможностей этой Рекомендации.

3.6. услуга портала (*PS, portal service*): Функциональный элемент, который обеспечивает функции административного управления и трансляции между сетью HFC и домом.

3.7. устройство IP сети LAN: Устройство IP местной компьютерной сети LAN (*LAN, Local Area Network*) является представителем типового устройства IP, которое должно находиться в доме, и которое содержит стек TCP/IP, а также клиента DHCP.

3.8. сквозной проход: Под-функция CAP, функция "Сквозной проход" перемыкает неизмененные пакеты на стороне WAN-Data портала CAP к стороне LAN-Pass.

3.9. автономный адаптер терминала мультимедиа (*S-MTA, stand-alone multimedia terminal adapter*): Отдельный узел, что содержит адаптер MTA и управление MAC, не принадлежащее к спецификации DOCSIS (например, Ethernet).

4 Сокращения, акронимы и соглашения

4.1 Сокращения и акронимы

Эта Рекомендация использует следующие сокращения и акронимы:

ASP Программа-посредник, характерная для приложения (*Application-Specific Proxy*)

CA Полномочия сертификата (*Certificate Authority*)

CAP Портал кабельного адреса (*Cable Address Portal*)

CAT Трансляция кабельного адреса (*Cable Address Translation*)

CDC Кабельный клиент DCHP (*Cable DHCP Client*)

CDP	Кабельный портал DCHP (*Cable DHCP Portal*)
CDS	Кабельный сервер DCHP (*Cable DHCP Server*)
CM	Кабельный модем (*Cable modem*)
CMP	Портал кабельного административного управления (*Cable Management Portal*)
CMS	Сервер административного управления вызовом (*Call Management Server*)
CMTS	Система завершения кабельного модема (*Cable Modem Termination System*)
C-NAPT	Трансляция адреса и порта кабельной сети (*Cable Network Address and Port Translation*)
C-NAT	Трансляция кабельного сетевого адреса (*Cable Network Address Translation*)
CNP	Портал кабельного присваивания имен (*Cable Naming Portal*)
CQoS	Кабельное качество обслуживания (*Cable Quality of Service*)
CQP	Портал кабельного качества обслуживания (*Cable Quality-of-Service Portal*)
CRL	Перечень отмены сертификатов (*Certificate Revocation List*)
CSP	Портал кабельной безопасности (*Cable Security Portal*)
CTP	Портал испытания CableHome (*CableHome Testing Portal*)
CVC	Сертификат проверки кода (*Code Verification Certificate*)
CVS	Подпись проверки кода (*Code Verification Signature*)
CxP	Подфункция кабельной услуги PS (*Cable PS Sub-function*)
DER	Правила выделенного кодирования (*Distinguished Encoding Rules*)
DHCP	Динамический протокол конфигурации ведущего узла (*Dynamic Host Configuration Protocol*)
DNS	Система названий доменов (*Domain Name System*)
DOCSIS	Спецификация интерфейса службы передачи данных по кабелю (*Data-Over-Cable Service Interface Specification*)
DQoS	Динамическое качество обслуживания (*Dynamic Quality of Service*) (IPCablecom)
E-MTA	Встроенный адаптер терминала мультимедиа (*Embedded Multimedia Terminal Adapter*)
FTP	Протокол переноса файлов (*File Transfer Protocol*)
FW	Средства межсетевой защиты (*Firewall*)
GMT	Время по Гринвичу (*Greenwich Mean Time*)
HA	Домашний доступ (*Home Access*)
HEX	16-ричный (*Hexadecimal*)
HFC	Гибридный волоконно-коаксиальный кабель (*Hybrid Fiber Coax*)
ICMP	Протокол сообщения для управления Интернет (*Internet Control Message*

	Protocol)
IGMP	Протокол административного управления группой Интернет (*Internet Group Management Protocol*)
IP	Протокол Интернет (*Internet Protocol*)
KDC	Центр распределения ключей (*Key Distribution Center*)
LAN-pass	Сквозной адрес сети LAN (*Pass-through LAN address*)
LAN-Trans	Транслируемый адрес сети LAN (*Translated LAN address*)
MAC	Управление доступом к носителю информации (*Media Access Control*)
MGCP	Протокол управления шлюзом носителя информации (*Media Gateway Control Protocol*)
MIB	Информационная база административного управления (*Management Information Base*)
MPLS	Многопротокольная коммутация на основе меток (*Multiprotocol Label Switching*)
MSO	Оператор множественных услуг (*Multiple Service Operator*)
MTA	Адаптер терминала мультимедиа (*Multimedia Terminal Adapter*)
NAPT	Трансляция сетевого адреса и портала (*Network Address and Portal Translation*)
NAT	Трансляция сетевого адреса (*Network Address Translation*)
NCS	Сигнализация вызова на основе сети (*Network-based Call Signalling*)
NMS	Система сетевого административного управления (*Network Management System*)
OID	Идентификатор объекта (*Object Identifier*)
OSI	Взаимосвязь открытых систем (*Open System Interconnection*)
OSS	Система поддержки операций (*Operations Support System*)
PDU	Блок данных протокола (*Protocol Data Unit*)
PING	Пакетный межсетевой группирователь (*Packet Inter-Network Grouper*)
PKI	Инфраструктура с открытым ключом (*Public Key Infrastructure*)
PKINIT	Криптография с открытым ключом для первоначального удостоверения подлинности (*Public-Key Cryptography for Initial Authentication*)
PS	Услуга портала (*Portal Service*)
PS WAN-Data	Интерфейс данных территориальной сети WAN элемента Услуги портала (*Portal Service element WAN data interface*)
PS WAN-Man	Интерфейс административного управления территориальной сети WAN элемента Услуги портала (*Portal Service element WAN management interface*)
QoS	Качество обслуживания
RFC	Запрос для замечаний (*Request for Comments*)
RSA	Ривест, Шамир, Адлеман (*Rivest, Shamir, Adleman*)
SHA-1	Безопасный алгоритм 1 случайных данных (*Secure Hash Algorithm 1*)

S-MTA	Автономный адаптер терминала мультимедиа (*Stand-alone Multimedia Terminal Adapter*)
SNMP	Простой протокол сетевого административного управления (*Simple Network Management Protocol*)
SOA	Начало полномочий (*Start of Authority*)
SPF	Фильтрование пакетов с изменением состояния в процессе исполнения (*Stateful Packet Filtering*)
SYSLOG	Системная регистрация (*System Log*)
TCP	Протокол управления передачей (*Transmission Control Protocol*)
TFTP	Очевидный протокол переноса файлов (*Trivial File Transfer Protocol*)
TLV	Тип –длина - значение (*Type-Length-Value*)
UDP	Датаграммный протокол пользователя (*User Datagram Protocol*)
USFS	Переключатель избирательной переадресации восходящего направления (*Upstream Selective Forwarding Switch*)
USM	Модель безопасности пользователя (*User Security Model*)
UTC	Скоординированное всемирное время (*Coordinated Universal Time*)
VACM	Модель управления доступом, основанная на обзоре (*View-based Access Control Model*)
VoIP	Передача голоса по протоколу Интернет (*Voice over Internet Protocol*)
WAN	Территориальная компьютерная сеть (*Wide Area Network*)
WAN-Data	Адресная область данных территориальной компьютерной сети (*Wide Area Network Data address realm*)
WAN-Man	Адресная область административного управления территориальной компьютерной сетью (*Wide Area Network Management address realm*)

4.2 Соглашения

При осуществлении этой Рекомендации ключевые слова "ОБЯЗАН" [*MUST*] и "ДОЛЖЕН" [*SHALL*], а также "ТРЕБУЕМЫЙ" [*REQUIRED*], должны истолковываться как указывающие обязательный аспект этой Рекомендации. Ключевые слова, указывающие определенный уровень значимости конкретного требования, которые используются по тексту этой Рекомендации, обобщены ниже.

"ОБЯЗАН" [*MUST*]	Это слово или прилагательное "ТРЕБУЕМЫЙ" [*REQUIRED*] означает, что аспект является абсолютным требованием этой Рекомендации
"НЕ ОБЯЗАН" [*MUST NOT*]	Эта фраза означает, что аспект является абсолютным запрещением этой Рекомендации.
"СЛЕДУЕТ" [*SHOULD*]	Это слово или прилагательное "РЕКОМЕНДУЕМЫЙ" [*RECOMMENDED*] означает, что в конкретных обстоятельствах могут существовать веские причины, чтобы игнорировать этот аспект, но следует понимать полные последствия, а случай следует тщательно взвешивать перед выбором другой линии поведения.
"НЕ СЛЕДУЕТ" [*SHOULD NOT*]	Эта фраза означает, что в конкретных обстоятельствах могут существовать веские причины, когда перечисленное поведение

является приемлемым или даже полезным, но следует понимать полные последствия, и случай следует тщательно взвешивать перед осуществлением любого поведения, описанного с помощью этой метки.

"МОЖЕТ" [*MAY*] Это слово или прилагательное "ДОПОЛНИТЕЛЬНОЕ" [*OPTIONAL*] означает, что этот аспект действительно является дополнительным (необязательным). Один поставщик может принять решение включить аспект, поскольку этого требует конкретный рынок, или потому что оно, например, улучшает продукт; другой поставщик может опустить тот же самый аспект.

5 Требования упаковки возможностей IP, архитектура и обзор

Эта Рекомендация предоставляет набор возможностей, основанных на IP, которые могут быть добавлены к Кабельному модему, который будет давать возможность кабельным операторам предоставлять их клиентам дополнительный набор усовершенствованных услуг. Эти возможности, основанные на IP, находятся внутри логического элемента, называемого Услугой портала (*PS, Portal Service* или просто Портал). Кабельный модем, который содержит эти усовершенствованные возможности, упоминается как IP-усовершенствованный Кабельный модем (*IPCM, IP-enhanced Cable Modem*), который является осуществлением класса устройства HA J.190. Как описано в Рекомендации МСЭ-Т J.190, класс устройства HA включает в себя как функциональные возможности Кабельного модема, так и функциональные возможности Услуг порталов.

Главными областями и возможностями являются следующие:

– *Административное управление и обеспечение*

- Дистанционное административное управление и конфигурация услуги PS;
- Простой посредник административного управления для домашних устройств, основанных на IP (например, персональный компьютер);
- Пассивное обеспечение для услуги PS.

– *Адресация и обработка пакетов*

- Индивидуальная трансляция адреса для домашних устройств;
- Трансляция из одного адреса во многие адреса для домашних устройств;
- Адресация без трансляции для домашних устройств;
- Простой сервер DNS в услуге PS.

– *Качество обслуживания*

- Функциональные возможности прозрачного перемыкания для обмена сообщениями QoS модели IPCablecom между приложениями, удовлетворяющими IPCablecom, и от них.

– *Безопасность*

- Удостоверение подлинности устройства PS;
- Сообщения безопасного административного управления;
- Безопасная загрузка из главной системы файлов конфигурации и программного обеспечения;
- Безопасное качество QoS на звене HFC;

- Дистанционное административное управление средствами межсетевой защиты услуги PS.

5.1 Архитектура

См. Рисунок 1.

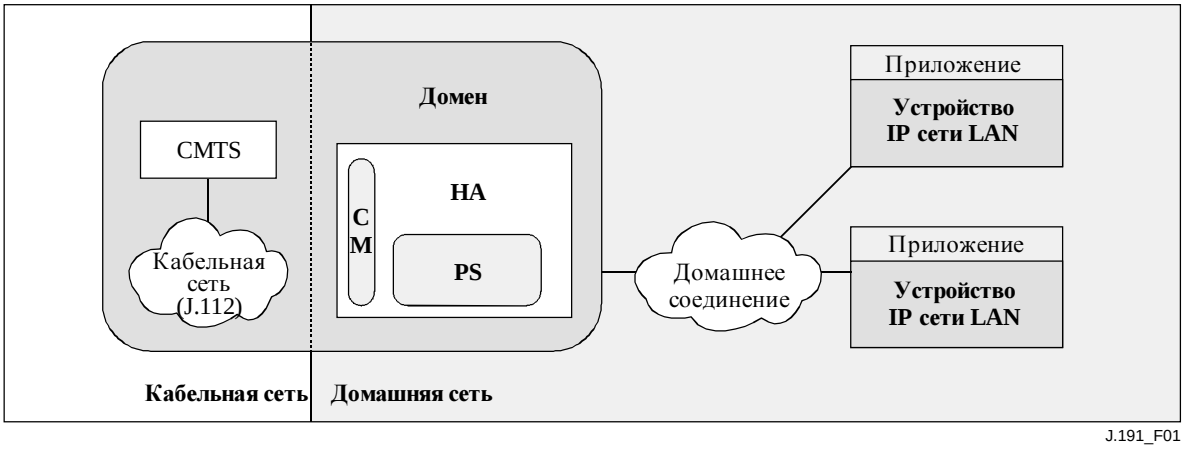


Рисунок 1/J.191 – Ключевые понятия

5.1.1 Услуга портала

Услуга портала является логическим элементом, который обеспечивает, в помещении и при общей безопасности, услуги административного управления, обеспечения и адресации. Определены три набора функций услуг порталов. Ими являются набор функций административного управления, набор функций Качества обслуживания (*QoS, Quality of Service*) и набор функций безопасности.

5.1.2 Адресные области

Адресная область определяется как "сетевой домен (область), в которой сетевые адреса назначаются объектам однозначным образом так, что к ним могут быть направлены датаграммы" [RFC 2663]. Внутри этой Рекомендации адресные области определяются категориями как адресные области сети WAN и адресные области сети LAN (см. Рисунок 2).

Адреса сети WAN находятся в одной из двух областей: в адресной области Административного управления сетью WAN (WAN-Man) или в адресной области Данных сети WAN (WAN-Data). Адреса сети LAN также находятся в одной из двух областей: в адресной области Сквозного прохода сети LAN (LAN-Pass) или в Транслируемой адресной области сети LAN (LAN-Trans). Свойства этих областей адресации являются следующими:

- Адресная область административного управления сетью WAN (WAN-Man) предназначена для переноса трафика сетевого административного управления на кабельной сети между системой сетевого административного управления и элементом PS. Обычно адреса в этой области будут находиться в частном адресном пространстве IP.
- Адресная область Данных сети WAN (WAN-Data) предназначена для переноса прикладного трафика абонента на кабельной сети и за ее пределами, например, трафика между Устройствами IP сети LAN и ведущими узлами Интернет. Обычно адреса в этой области будут находиться в адресном пространстве IP общего пользования.

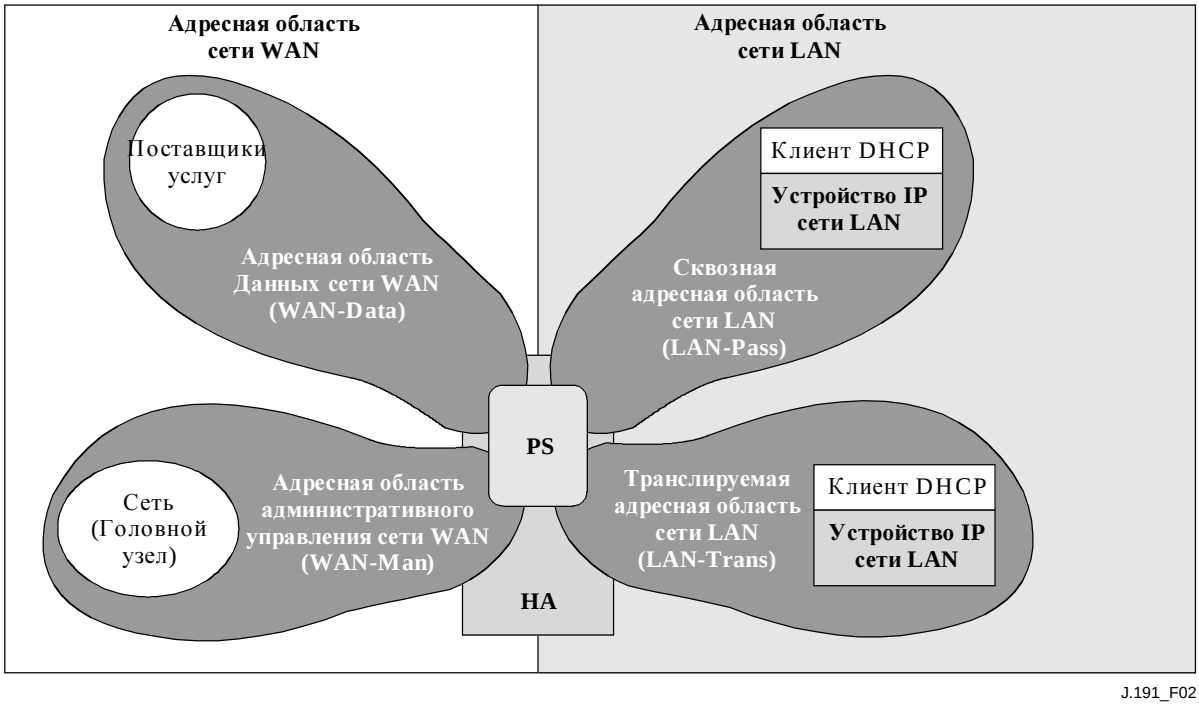


Рисунок 2/J.191 – Адресные области

- Транслируемая адресная область сети LAN (LAN-Trans) предназначена для переноса прикладного трафика абонента и трафика административного управления на домашней сети между Устройствами IP сети LAN и услугой PS. Обычно адреса в этой области будут находиться в частном адресном пространстве IP и обычно могут повторно использоваться между абонентами.
- Сквозная адресная область сети LAN (LAN-Pass) предназначена для переноса прикладного трафика абонента, например, трафика между Устройствами IP сети LAN и ведущими узлами Интернет, на домашнем звене, на кабельной сети и за ее пределами. Обычно адреса в этой области будут находиться в адресном пространстве IP общего пользования.

На стороне сети LAN адреса в Сквозной адресной области сети LAN (LAN-Pass) напрямую извлекаются из адресов в адресной области Данных сети WAN. Эти адреса используются Устройствами IP сети LAN и такими приложениями, как модель IPCablecom, которые нетерпимы к адресной трансляции и требуют глобально прокладываемого адреса IP. Кроме того, на стороне сети LAN, Устройства IP сети LAN могут использовать транслируемые адреса из Транслируемой адресной области сети LAN (LAN-Trans).

5.2 Функции административного управления

Для поддержки обеспечения и административного управления Устройствами IP сети LAN внутри дома определяются три класса Функций административного управления:

- Функции сервера административного управления;
- Функции клиента административного управления;
- Функции портала услуги административного управления.

Несколько Функций сервера административного управления находятся внутри головного узла (*HE, headend*). Функции клиента административного управления обычно находятся внутри Устройств IP сети LAN. Функции портала услуги административного управления располагаются внутри логического элемента PS Кабельного модема и могут включать в себя

функциональные возможности, похожие на возможности сервера, клиента и переприема, чтобы группировать и транслировать сообщения между головным узлом и Устройствами IP сети LAN. Примеры функций сервера административного управления, PS и клиента, введенные в Таблицах 1, 2 и 3, иллюстрируются на Рисунке 3.

Таблица 1/J.191 – Описание функции сервера административного управления

Функции сервера административного управления	**Описание**
Сервер DHCP головного узла	Сервер DHCP является составной частью головного узла, что предоставляет услуге PS адресную информацию для адресных областей WAN-Man и WAN-Data.
Сервер DNS головного узла	Сервер DNS головного узла является конторской составной частью, используемой для преобразования между названиями доменов ASCII и адресами IP.
Сервер обмена сообщениями административного управления головного узла	Обмен сообщениями административного управления головного узла, загрузка из главной системы, серверы уведомления о событиях, включая такие протоколы, как SNMP, SYSLOG, и TFTP.

Таблица 2/J.191 – Описание функции PS административного управления и обеспечения

Функции портала административного управления	**Описание**
Портал кабельного адреса (*CAP, Cable Address Portal*)	Внутри услуги PS портал CAP взаимно соединяет адресные области сетей WAN и LAN для трафика данных (см. CAT/Сквозной проход).
Трансляция кабельного адреса (*CAT, Cable Address Translation*)	Подфункция портала CAP, CAT транслирует адреса на стороне WAN-Data портала CAP в адреса внутри отдельной логической подсети на стороне LAN-Trans.
Сквозной проход	Подфункция портала CAP, функция "Сквозной проход" без изменения перемыкает пакеты на стороне WAN-Data портала CAP к стороне LAN-Pass.
Портал кабельного административного управления (*CMP, Cable Management Portal*)	Функция, которая обеспечивает интерфейс между головным узлом и базой данных PS.
Кабельный портал DCHP (*CDP, Cable DHCP Portal*)	Функции адресной информации (например, те, что передаются через протокол DHCP), включая сервер для области LAN и клиента для областей WAN.
Портал кабельного присваивания имен (*CNP, Cable Naming Portal*)	Портал CNP предоставляет простую услугу DNS для Устройств IP сети LAN, требующих услуги наименования.
Портал испытания CableHome (*CTP, CableHome Testing Portal*)	Портал предоставляет удаленные средства для инициации перебросок информации и обратных шлейфов внутри сети LAN.

Таблица 3/J.191 – Описание функции клиента административного управления

Функции клиента административного управления	Описание
Клиент DHCP Устройства IP сети LAN	Функция кабельного клиента DHCP является домовой составной частью, используемой во время процесса обеспечения Устройства IP сети LAN, чтобы динамически запрашивать адреса IP и другую информацию о конфигурации логического элемента.
Ответчик обратного шлейфа Устройства IP сети LAN	Внутри Устройства IP сети LAN, ответчик обратного шлейфа заворачивает данные, полученные от функции шлейфа CTP, обратно к функции шлейфа CTP.

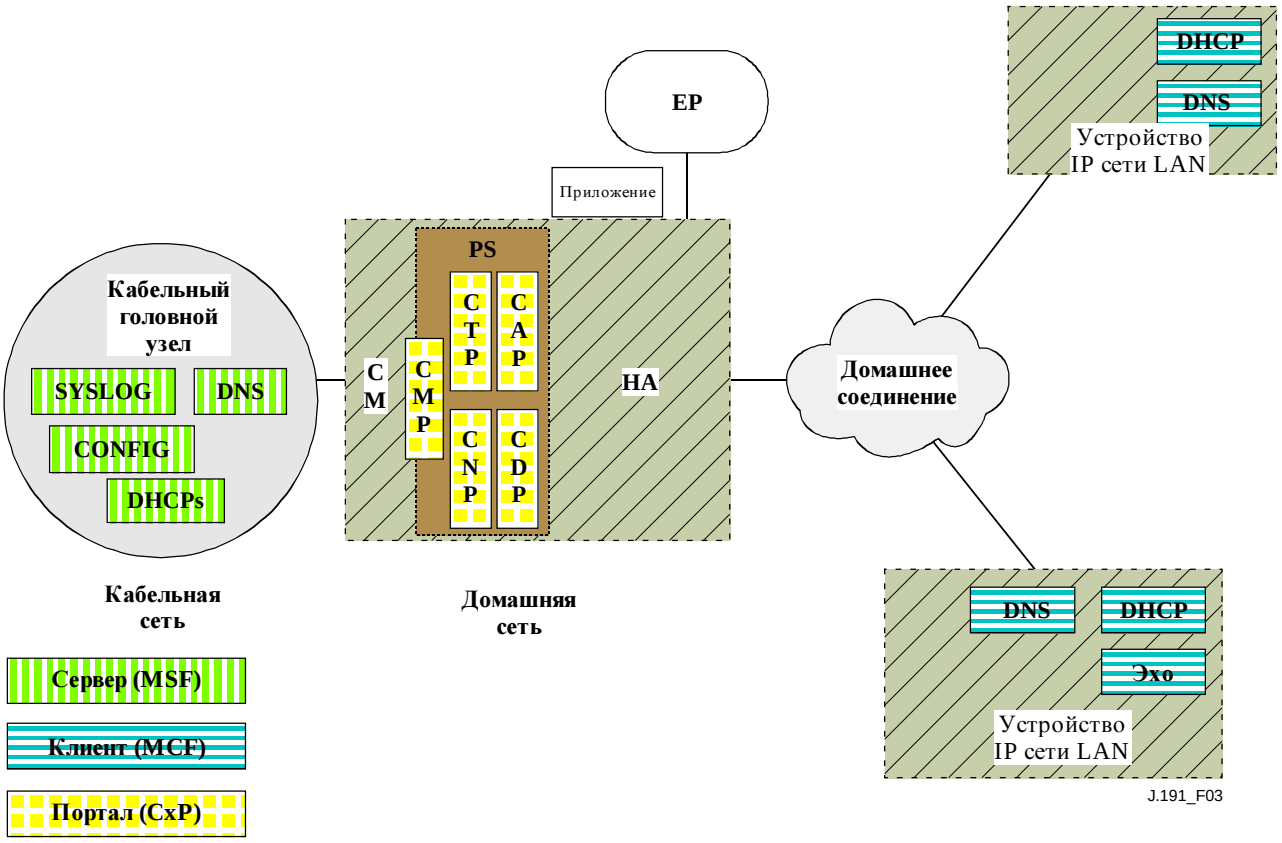


Рисунок 3/J.191 – Взаимоотношения "Клиент– сервер административного управления "

5.3 Функции безопасности

Функции безопасности разбиты на категории Функции портала безопасности или Функции сервера безопасности. Взаимоотношение между различными элементами безопасности и их классификация в качестве функций сервера и портала представляется на Рисунке 4 и описывается в Таблицах 4 и 5.

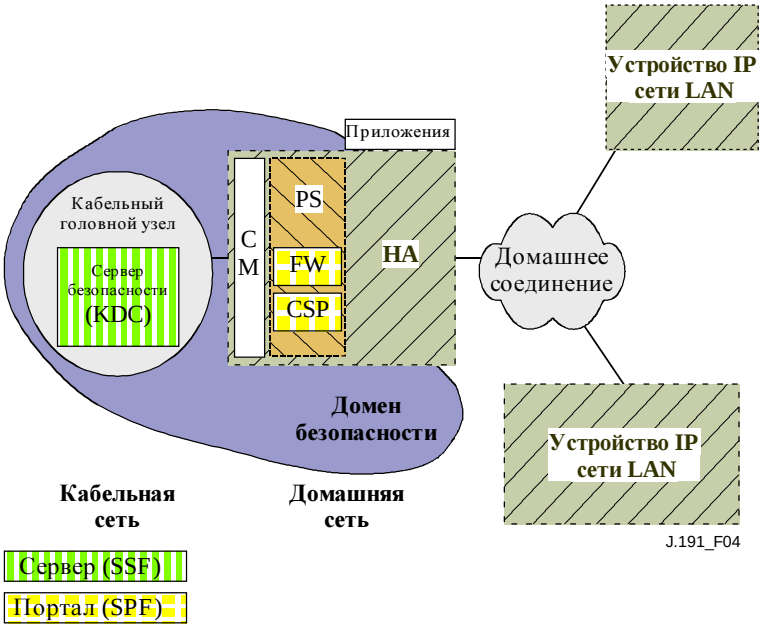


Рисунок 4/J.191 – Элементы безопасности

Таблица 4/J.191 – Описание функции портала безопасности

Функции портала безопасности	Описание
Портал кабельной безопасности (*CSP, Cable Security Portal*)	Портал CSP действует в качестве портала для материала защиты для всех других функций безопасности внутри PS. Портал CSP осуществляет связь на стороне сети WAN с Сервером безопасности (Центр распределения ключей) (*KDC, Key Distribution Center*).
Средства межсетевой защиты (*FW, Firewall*)	Средства межсетевой защиты обеспечивают защиту домашней окружающей среды IP от злонамеренной атаки.

Таблица 5/J.191 – Описание функции сервера безопасности

Функции сервера безопасности	Описание
KDC	Серверы KDC в головном узле обеспечивают услуги установления подлинности и распределение ключа для дома. Чтобы установить эти услуги, они осуществляют связь с функцией CSP.

5.4 Функции QoS

Архитектура QoS складывается из отдельного функционального объекта, основанного на услуге PS, который известен как Портал кабельного качества QoS (*CQP, Cable QoS Portal*). Портал CQP обеспечивает прозрачное перемыкание для обмена сообщениями QoS между приложениями IPCablecom и инфраструктурой QoS модели IPCablecom на кабельной сети.

5.5 Модель интерфейса обмена сообщениями

Связь между функциями в сетевых элементах и Устройствах IP сети LAN возникает на интерфейсах обмена сообщениями. Типы интерфейсов обмена сообщениями различаются элементами, что участвуют в осуществлении связи. Интерфейсы обмена сообщениями иллюстрируются на Рисунке 5.

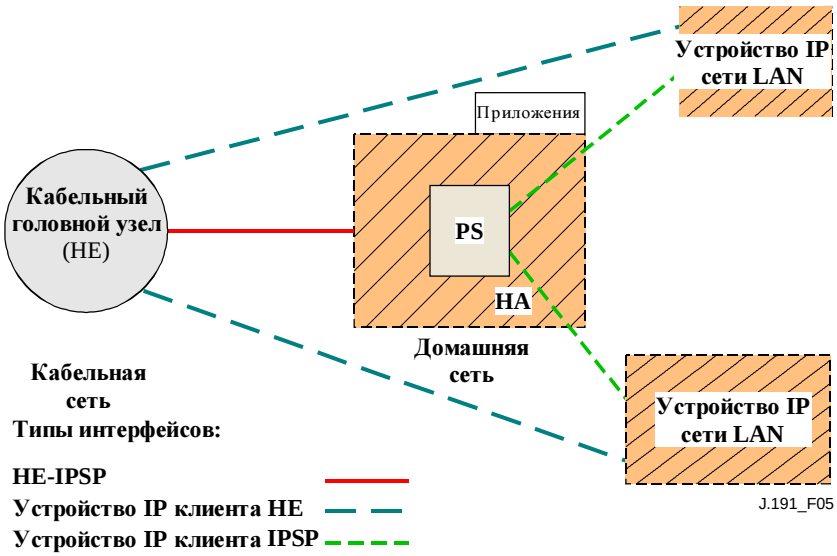


Рисунок 5/J.191 – Эталонные интерфейсы

Интерфейсы обмена сообщениями обобщены в Таблице 6.

Таблица 6/J.191 – Тракты действительных интерфейсов для каждой функциональной возможности

Функциональные возможности	Протокол	Интерфейс		
		HE-PS	Устройство IP сети LAN HE	Устройство IP сети LAN PS
Услуга названия	DNS	Не указано	Не указано	Не указано
Загрузка программного обеспечения из главной системы	TFTP	Эта Рекомендация	Не указано	Не указано
Приобретение адреса	DHCP	Эта Рекомендация	Не указано	Эта Рекомендация
Административное управление (отдельное) (оптом)	SNMP TFTP	Эта Рекомендация Эта Рекомендация	Не указано	Не указано
Уведомление о событии	SNMP SYSLOG	Эта Рекомендация Эта Рекомендация	Не указано	Не указано
QoS	Протоколы QoS IPCablecom	Не указано	IPCablecom	Не указано
Безопасность (распределение ключа)	Kerberos ("*Цербер*")	Эта Рекомендация	Не указано	Не указано
Безопасность (проверка подлинности)	Kerberos	Эта Рекомендация	Не указано	Не указано
Переброс информации	ICMP	Эта Рекомендация	Не указано	Эта Рекомендация
Шлейф/Эхо	UDP/TCP	Не указано	Не указано	Эта Рекомендация

5.6 Информационная эталонная модель

Действие модели административного управления основывается на запоминании информации, поддерживаемой в Портале с помощью функций различных порталов (CAP, CDP, CMP и пр.). Эти функции обязаны иметь средства взаимодействия посредством обмена информацией, а База данных портала является концептуальным объектом, который представляет запоминающее устройство для этой информации. База данных портала сама по себе является не фактической указанной базой данных, а, скорее всего, инструментом, чтобы помочь в понимании информации, которой обмениваются между различными элементами.

Рисунок 6 показывает взаимоотношение между функциями базы данных и портала, Таблица 7 описывает типовую информацию, связанную с каждой из этих функций. Рисунок 7 показывает подробный пример осуществления, указывая совокупность информации, функции, которые извлекают информацию, и отношения между функциями и информацией.

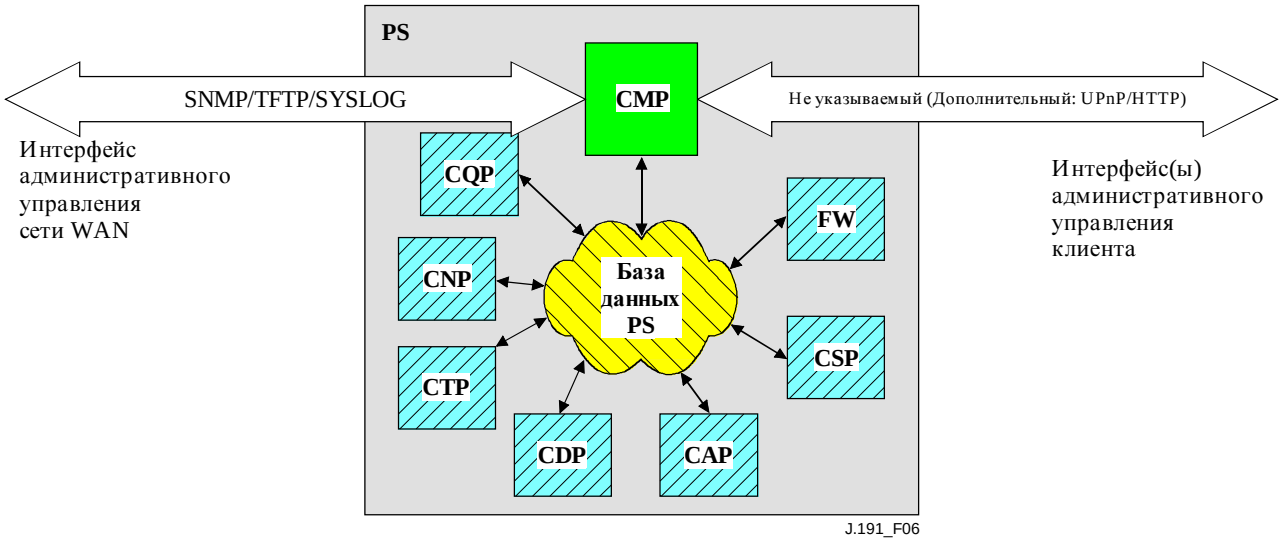


Рисунок 6/J.191 – Взаимоотношение функции портала и базы данных

Таблица 7/J.191 – Типовые примеры информации базы данных портала

Название	Использование (в общем виде)
Информация CDP	Информация, связанная с адресами, которые приобретаются и распределяются через протокол DHCP
Информация CAP	Информация, связанная с преобразованиями трансляции адресов
Информация CMP	Информация, связанная с состоянием функций управления
Информация CTP	Информация, связанная с результатами испытания сети LAN, выполненного с помощью портала CMP
Информация CNP	Информация, связанная с разрешением названия Устройства IP сети LAN
Информация USFS	Информация, связанная с функцией "Переключатель избирательной переадресации восходящего направления"
Информация CSP	Информация, связанная с установлением подлинности, обменом ключами и пр.
Информация средств межсетевой защиты	Информация, связанная с поведением средств межсетевой защиты (набор правил) и регистрацией средств межсетевой защиты
Информация о событии	Информация, связанная с местным журналом регистрации для всех общих событий, системных прерываний (захватов) и пр.

База данных портала хранит бесчисленное количество взаимосвязей данных. Портал CMP обеспечивает интерфейс административного управления сетью WAN (SNMP) к базе данных портала. Функции внутри портала вводят и пересматривают взаимосвязи данных в базе данных портала. Кроме того, функции внутри портала могут отыскивать и извлекать информацию из базы данных портала, что удерживается внутри портала другими функциями.

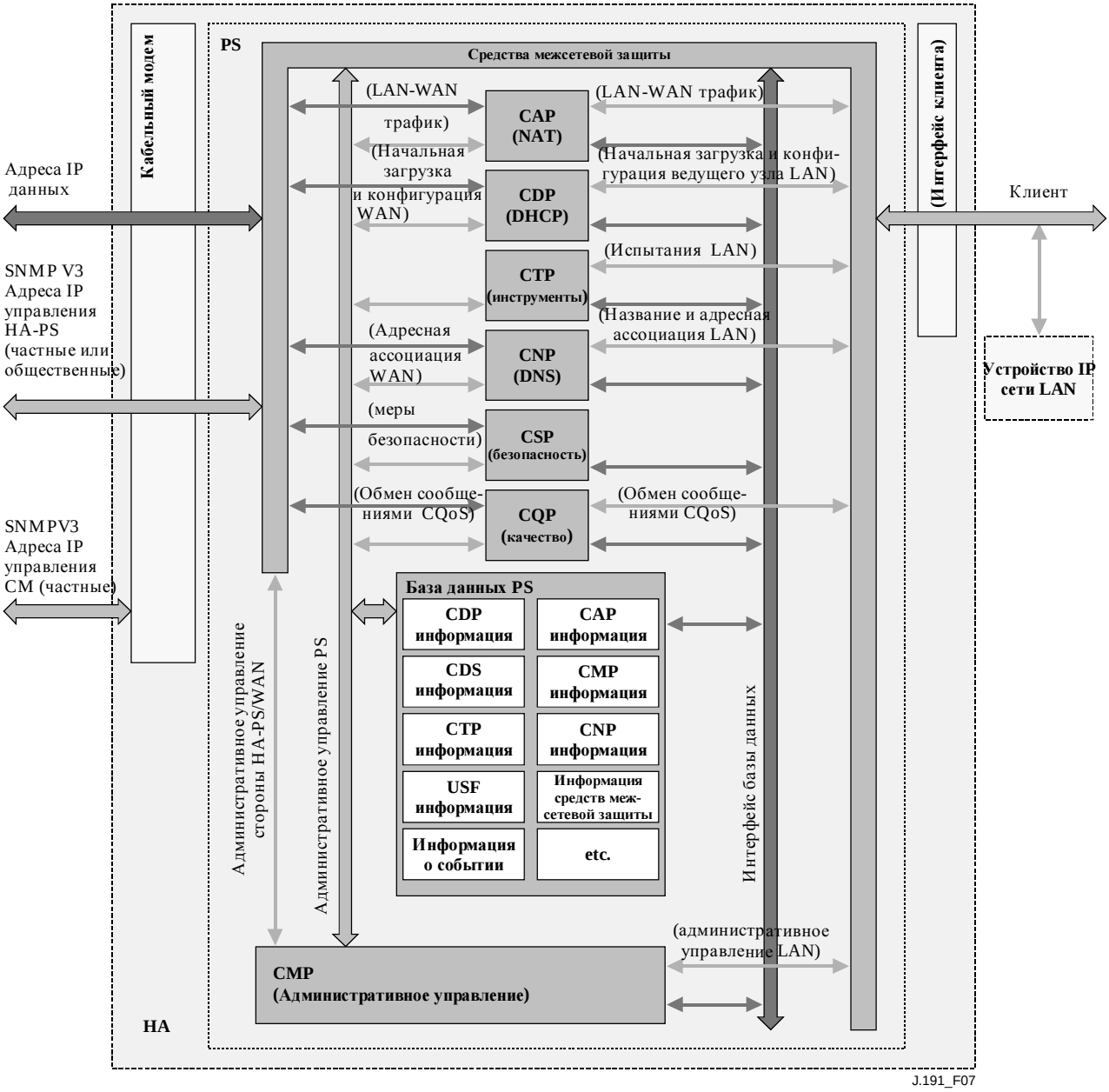


Рисунок 7/J.191 –Подробное примерное осуществление базы данных портала

Портал управляется из сети WAN через портал CMP, и в большей степени это включает в себя доступ к информации в базе данных портала. Административное управление используется для установления в начальное состояние и обеспечения сетевых элементов стороны WAN, а также для диагностики или статуса стороны LAN. Диагностика может полагаться на портал CTP для получения лучшей видимости в текущем состоянии сети LAN. Могут быть измерены связность и показатели качества элементарной сети.

Портал CNP является управляющей программой Системы названий доменов LAN (*DNS, Domain Name System*). Все Устройства IP сети LAN области LAN-Trans конфигурируются с помощью портала CDP для использования портала CNP в качестве первичного Сервера

названий. Портал CNP разрешает текстовые названия ведущего узла Устройств IP сети LAN, возвращая их соответствующие адреса IP, а в дополнение относит Устройства IP сети LAN к внешним серверам DNS для запросов, на которые не могут ответить на основе местной информации. Портал CNP откликается только на запросы к системе DNS на области LAN-Trans.

Портал CDP содержит адресные функции для поддержки сервера DHCP в области LAN-Trans и клиента DHCP в областях WAN.

Портал CAP создает отображения трансляции адресов между адресными областями WAN-Data и LAN-Trans. Портал CAP также является ответственным за решения Переключателя избирательной переадресации восходящего направления, чтобы оберегать полосу пропускания (WAN) восходящего канала HFC только от трафика местной сети LAN. Наконец, портал CAP содержит функцию сквозного прохода, которая перемыкает трафик между адресными областями LAN и WAN.

Портал CSP предоставляет возможности удостоверения подлинности ПОРТАЛА, а также действия по обмену ключами.

Портал CQP является частью системы, которая обеспечивает Качество обслуживания модели IPCablecom (*QoS, Quality of Service*) по всему порталу. Портал CQP, действующий в качестве прозрачного моста, направляет обмен сообщениями QoS, удовлетворяющими модели IPCablecom, между приложениями IPCablecom и инфраструктурой QoS модели IPCablecom.

Средства межсетевой защиты зависят от осуществления, и эта Рекомендация не указывает подробности осуществления средств межсетевой защиты.

5.7 Эксплуатационные модели

Эта усовершенствованная инфраструктура надстраивается над инфраструктурой кабельного модема для обеспечения дополнительных услуг, и включает в себя ряд возможностей, которые подобны тем, что существуют внутри системы обеспечения IPCablecom.

Для целей конфигурации портал может действовать в рамках одного из двух режимов обеспечения:

- Режим обеспечения DHCP;
- Режим обеспечения SNMP.

Когда услуга PS действует в рамках режима обеспечения DHCP, она может действовать в одном из двух подрежимов Сетевого административного управления:

- режим NmAccess;
- режим Сосуществования [*Coexistence*].

Рисунок 8 иллюстрирует различные эксплуатационные режимы PS вместе со связанными спусковыми устройствами для каждого режима.

Если информация Файла конфигурации портала (местоположение сервера и имя файла) обеспечивается Порталу в сообщении DHCP OFFER [*предложение*], выпущенном сервером DHCP кабельной сети, то Портал будет действовать в режиме обеспечения DHCP. При нахождении в режиме обеспечения DHCP Портал может действовать в одном из двух режимов сетевого административного управления (NmAccess и Сосуществование). В рамках режима обеспечения DHCP Портал будет действовать в режиме сетевого административного управления по умолчанию, но может быть конфигурирован системой NMS для действия в режиме Сосуществования.

Если информация Файла конфигурации портала не предоставляется Порталу в сообщении DHCP OFFER, выпускаемом сервером DHCP кабельной сети, то Портал будет действовать в режиме обеспечения SNMP. При работе в режиме обеспечения SNMP информация и

спусковые устройства для загрузки из главной системы Файла конфигурации портала предоставляются системой NMS через обмен сообщениями SNMP. В противоположность режиму обеспечения DHCP, поведение сетевого административного управления в рамках этого режима не меняется.

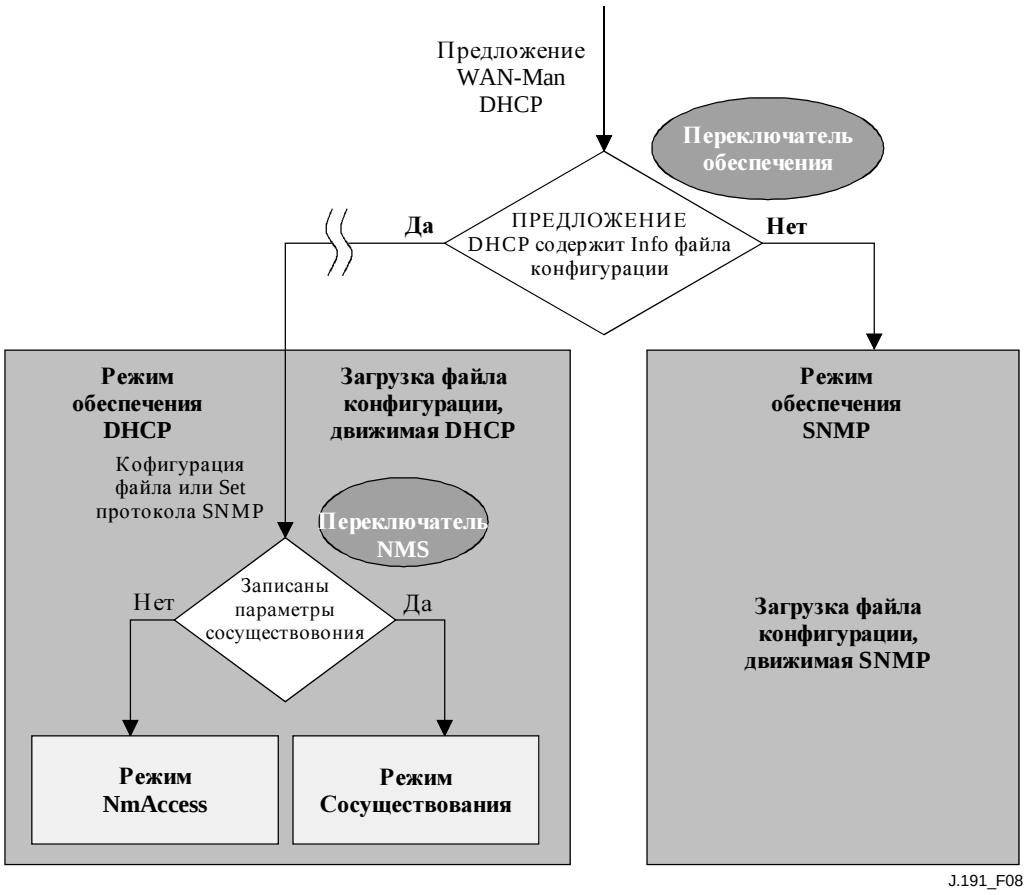


Рисунок 8/J.191 – Эксплуатационные режимы портала

Таблица 8 описывает возможности, которые вызываются каждым эксплуатационным режимом, описанным выше.

Таблица 8/J.191 – Инфраструктуры порталов

Режим	Непосредственно воздействующая возможность
Режим обеспечения SNMP	Загрузка файла конфигурации
Режим обеспечения DHCP	Загрузка файла конфигурации
Режим обеспечения DHCP: режим NmAccess	Версия SNMP, используемая между NMS и PS
Режим обеспечения DHCP: режим Сосуществования	Версия SNMP, используемая между NMS и PS

Эти различные эксплуатационные режимы предназначены для приспособления множества инфраструктур с точки зрения конторского сервера, включая различные версии SNMP и различные типы серверов безопасности. Больше подробностей можно найти в разделах с 13.1 по 13.3.

6 Инструменты административного управления

6.1 Введение/обзор

Инструменты административного управления обеспечивают кабельных операторов функциональными возможностями для наблюдения и конфигурирования Портала IPService, а также для выполнения дистанционной диагностики на Устройствах IP сети LAN. Этот раздел описывает и указывает требования для этих возможностей.

6.1.1 Цели

Цели для инструментов административного управления включают в себя:

- обеспечивать кабельных операторов обзором Устройств IP сети LAN;
- обеспечивать кабельных операторов минимальным набором дистанционных диагностических инструментов, которые позволят кабельному оператору проверять связность между элементом PS и любым Устройством IP сети LAN в адресной области LAN-Trans;
- обеспечивать кабельных операторов доступом, через базы MIB, к внутренним данным в элементе PS, и давать возможность кабельному оператору наблюдать за указанными параметрами и конфигурировать или повторно конфигурировать указанные возможности, как необходимо;
- предоставлять средства для информирования об исключениях и других событиях в форме системных прерываний (захватов) SNMP, сообщений к местному журналу регистрации, или сообщений к системному журналу регистрации (SYSLOG) в кабельной сети.

6.1.2 Предположения

Предположения для окружающей среды сетевого административного управления включают в себя:

- Подчиняющиеся устройства осуществляют набор протоколов в виде Протокола Интернет (IP).
- Для обмена сообщениями административного управления между системой NMS кабельной сети и Порталом IPService в кабельном модеме используется протокол SNMP. Протокол SNMP обеспечивает для системы NMS обзор интерфейсов на портале, с помощью доступа к внутренним данным Портала, через требуемые базы MIB.
- В качестве протокола административного управления между системой NMS и Услугой портала может быть использован любой из протоколов SNMPv1/v2c/v3.
- Устройства IP сети LAN осуществляют клиента DHCP.
- Информация, приобретаемая путем обмена сообщениями DHCP DISCOVER [*обнаруживать*], DHCP REQUEST [*запрашивать*] и DHCP OFFER [*предлагать*], которыми обмениваются между услугой PS и Устройствами IP сети LAN, и информация, имеющаяся от базы данных PS через базу MIB Группы интерфейсов, являются достаточными для обеспечения кабельного оператора желаемым знанием относительно Устройств IP сети LAN.
- Элемент PS и Устройства IP сети LAN поддерживают протокол ICMP.
- Обслуживающая программа PING поставляет функциональные возможности, достаточные для обеспечения кабельных операторов желаемой информацией относительно связности между элементом PS и Устройствами IP сети LAN.

6.2 Архитектура административного управления

6.2.1 Руководящие принципы разработки системы

Руководящие принципы разработки системы Инструментов административного управления перечисляются в Таблице 9. Этот перечень предоставляет руководящие принципы для развития спецификации инструментов административного управления.

Таблица 9/J.191 – Руководящие принципы разработки системы инструментов административного управления

Ссылка	Руководящие принципы разработки системы инструментов административного управления
Mgmt 1 [*управление*]	Услуга PS будет осуществлять протокол SNMPv1/v2c/v3 для обеспечения доступа к внутренним данным PS.
Mgmt 2	Услуга PS будет способна выпускать команду Переброса информации [*Ping*] ICMP к любому Устройству IP сети LAN в области LAN-Trans в направлении системы NMS кабельной сети и сохранять результаты в базе данных PS. Результаты дистанционных испытаний по Переброске информации доступны через объекты MIB CTP cabhCtpPingStatus, cabhCtpPingNumSent и cabhCtpPingNumRecv.
Mgmt 3	Услуга PS будет способна к выполнению Испытания скорости соединения с указанным Устройством IP сети LAN в области LAN-Trans в направлении системы NMS кабельной сети и к сохранению результатов в базе данных PS.
Mgmt 4	Элемент PS будет способен информировать о событиях.

6.2.2 Описание системы инструментов административного управления

Как показано на Рисунке 9, архитектура инструментов административного управления состоит из следующих составных частей:

1) Портал кабельного административного управления (*CMP, Cable Management Portal*);

2) Портал испытания CableHome (*CTP, CableHome Testing Portal*);

3) механизм информирования о событиях внутри портала CMP; и

4) Сервер сетевого административного управления SNMP (*NMS, Network Management Server*), который является частью кабельной сети.

Система NMS кабельной сети наблюдает за услугой PS и конфигурирует ее, осуществляя доступ к базе данных PS через базы MIB, указанные в 6.3.7. Система NMS может также непосредственно осуществлять связь с Устройствами IP сети LAN в области LAN-Pass.

Функциональные элементы CMP и CTP находятся внутри услуги PS.

Модем CM и услуга PS являются отдельными и независимыми объектами административного управления, и предполагается отсутствие совместного использования данных между CM и PS, за исключением случая загрузки из главной системы изображения программного обеспечения к услуге PS. К объектам docsDevSoftware кабельного модема получают доступ, чтобы установить, инициировать и наблюдать за загрузкой из главной системы отдельного составного изображения программного обеспечения. Из-за этой независимости административного управления модем CM и услуга PS ОБЯЗАНЫ откликаться на различные и независимые адреса IP административного управления. Объекты MIB модема CM видимы только тогда, когда управляющая программа дает им доступ через адрес IP административного управления CM, и они не являются видимыми через адрес IP административного управления PS (и наоборот). Права доступа SNMP к объектам PS и CM

ОБЯЗАНЫ быть установлены независимо. Это не препятствует использованию отдельного агента SNMP.

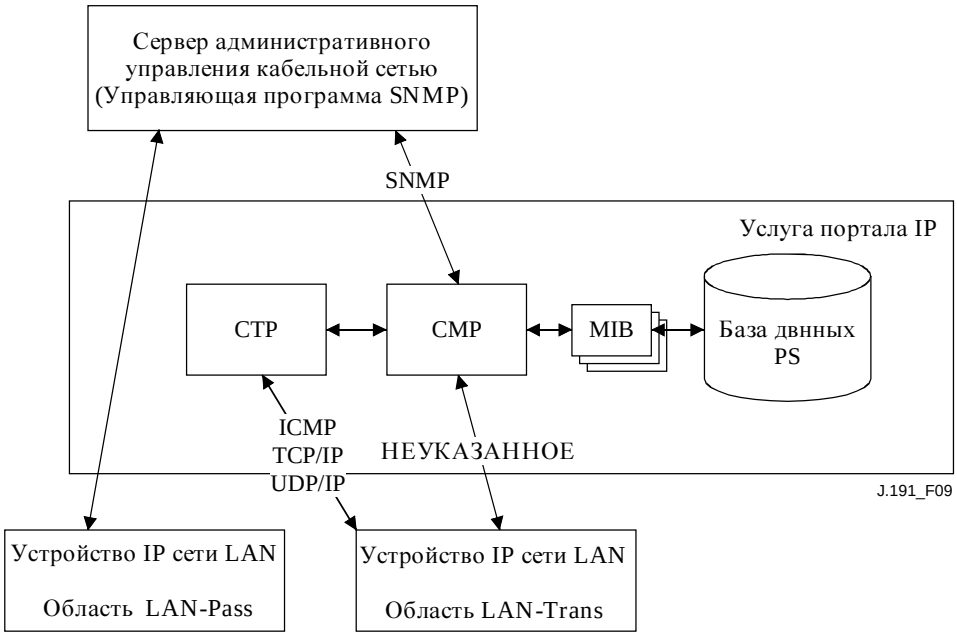


Рисунок 9/J.191 – Архитектура административного управления

Элемент PS поддерживает протоколы SNMPv1, SNMPv2c и SNMPv3. Раздел 5.7 ввел две модели обеспечения, поддерживаемые элементом PS, а раздел 7 предоставляет дополнительные подробности относительно этих режимов. Режим обеспечения, в котором услуга PS действует частично, определяет, которую из версий протокола SNMP использует услуга PS. Дополнительные подробности предоставляются в 6.3.3.

6.3 Портал кабельного административного управления (CMP)

Портал кабельного административного управления (*CMP, Cable Management Portal*) существует внутри услуги PS. Он служит в качестве концентратора директив Административного управления для доступов административного управления стороны WAN. Портал CMP группирует и взаимно соединяет информацию административного управления в областях WAN-Man и LAN-Trans, поскольку они непосредственно не имеют доступа друг к другу.

6.3.1 Цели CMP

Цели для Портала кабельного административного управления включают в себя:

- обеспечение и обновление информации конфигурации Портала кабельного адреса (*CAP, Cable Address Portal*);
- обеспечение обзора и обновления информации конфигурации средств межсетевой защиты;
- обеспечение Дистанционного переброса информации для Устройств IP сети LAN в области LAN-Trans, через Портал испытания CableHome (*CTP, CableHome Testing Portal*);
- обеспечение обзора информации Устройства IP сети LAN, полученной через Кабельный портал DHCP (*CDP, Cable DHCP Portal*);

- обеспечение обзора результатов наблюдения за показателями качества Устройства IP сети LAN, выполненного с помощью Портала испытания CableHome (*CTP, CableHome Testing Portal*);
- обеспечение доступа к другим параметрам конфигурации PS;
- обработку команд SNMP массива, пропущенных от системы NMS кабельной сети в Файле конфигурации PS;
- облегчение безопасности путем обеспечения доступа к параметрам безопасности и через использование протокола SNMPv1/v2c/v3 в соответствующем режиме сетевого административного управления;
- обеспечение возможности исключать из работы сегменты LAN.

6.3.2 Руководящие принципы разработки CMP

Руководящие принципы разработки CMP перечисляются в Таблице 10. Этот перечень предоставляет руководящие принципы для спецификации функциональных возможностей CMP.

Таблица 10/J.191 – Руководящие принципы разработки системы CMP

Ссылки	Руководящие принципы разработки системы CMP
CMP 1	Интерфейсы будут поддерживать характеристики административного управления и диагноза, а также функции, требуемые для поддержки услуг на основе кабеля, которые обеспечиваются в доме.
CMP 2	Потеря соединения между поставщиком (поставщиками) широкополосной услуги и усовершенствованным устройством IP не будет выключать из работы или ухудшать действие других внутренних домашних функций.
CMP 3	Услуга PS будет постепенно восстанавливаться после отказа питания, а устройства, подключенные к услуге PS, должны возвращаться в действующее состояние, в котором они были перед отказом питания.
CMP 4	Подобно домашнему прибору, устройства должны легко устанавливаться и конфигурироваться для работы.

6.3.3 Описание системы CMP

Как упоминалось ранее, портал CMP служит в качестве концентратора директив административного управления для доступов со стороны WAN, и он группирует информацию для административного управления Управлением сети WAN и сетевыми элементами LAN и соединяет их.

Портал CMP работает в любом из трех режимов сетевого административного управления.

Как описано в 5.7, при нахождении в режиме обеспечения SNMP, услуга PS:

1) действует, используя протокол SNMPv3;
2) поддерживает модели USM и VACM; и
3) использует систему Kerberos ["*Цербер*"] для распределения ключевого материала.

Как описывается в 5.7, при нахождении в режиме обеспечения DHCP, услуга PS может действовать в любом из других двух режимов сетевого административного управления, в режиме NmAccessTable и в режиме Сосуществования. В режиме NmAccessTable доступ административного управления контролируется с помощью NmAccessTable из документа [RFC 2669], и поддерживаются протоколы SNMPv1/v2c. В режиме Сосуществования доступ административного управления контролируется так, как описано в документе [RFC 2576], поддерживаются протоколы SNMPv1/v2c/v3, возможны модели USM и VACM, и ключевой

материал SNMPv3 распространяется, используя документ [RFC 2786] и значения TLV в Файле конфигурации PS.

Таблица 11 содержит определения для терминов, которые являются характерными для CMP.

Таблица 11/J.191 – Определение терминов

Контроль административного управления	Доступ для чтение или записи для установления параметров, которые управляют или наблюдают за поведением услуги PS.
База данных PS	Набор параметров, которые контролирует или наблюдает за поведением элемента PS, читаемого с помощью системы административного управления WAN. О нем можно думать как о хранилище информации, описывающей текущее состояние PS.
Пользователь	Как определяется в протоколе SNMP [RFC 2574, секция 2.1], Пользователь имеет имя, связанное с ним, связанную безопасность и доступ к Обзору.
Обзор	Обзор является набором объектов MIB и прав доступа к таким объектам. Каждый обзор имеет название, и оно связывается с Пользователем [RFC 2575, секция 2.4].
Окончательное удостоверение подлинности	Отдельные полномочия, что устанавливают, изменяют, или исключают идентификаторы ID Пользователя, ключи удостоверения подлинности, ключи шифрования и права доступа к базам данных PS. Окончательное удостоверение подлинности МОЖЕТ быть переключаемым между Пользователем в системе NMS кабельной сети и Пользователем в доме, но им НЕ СЛЕДУЕТ быть одновременно. Этому Пользователю доверяются операции административного управления безопасностью.
Пользователь технического обслуживания	Пользователь, который обычно выполняет операции "только чтения" на базе данных PS. Это обычно используется для наблюдения за показателями качества и ведения учета.
Пользователь администратора	Пользователь, который обычно выполняет как операции чтения, так и записи на базе данных PS. Эти операции используются для Административного управления конфигурацией и при неисправностях.

Примеры типов информации, которой манипулируют через директиву Кабельного административного управления, включают в себя установки алгоритмов средств межсетевой защиты, отображения NAT, конфигурированные с помощью системы NMS, инициацию дистанционных диагностических инструментов и доступ к результатам, статус PS и конфигурации диапазона адресов LAN. Как будет показано позднее, различные интерфейсы обмена сообщениями административного управления могут иметь права доступа к различным наборам параметров. Есть возможность получать доступ к базе данных PS как из сети WAN, так и из сети LAN; однако доступ сети LAN не указывается. Рисунок 10 указывает три возможные интерфейса обмена сообщениями административного управления:

- NMS – CMP: обмен сообщениями административного управления между системой NMS кабельной сети и порталом CMP;
- CMP – Устройство IP сети LAN: обмен сообщениями административного управления между порталом CMP и Устройством IP сети LAN в области LAN-Trans (не указывается);

- NMS – Устройство IP сети LAN: обмен сообщениями административного управления между системой NMS кабельной сети и Устройствами IP сети LAN в области LAN-Pass (не указывается);
- NMS – Устройство IP сети LAN: обмен сообщениями административного управления между системой NMS кабельной сети и Устройствами IP сети LAN в области LAN-Trans (обеспечивается конфигурацией портала CAP – см. 8.3.2). Этот обмен сообщениями не указывается.

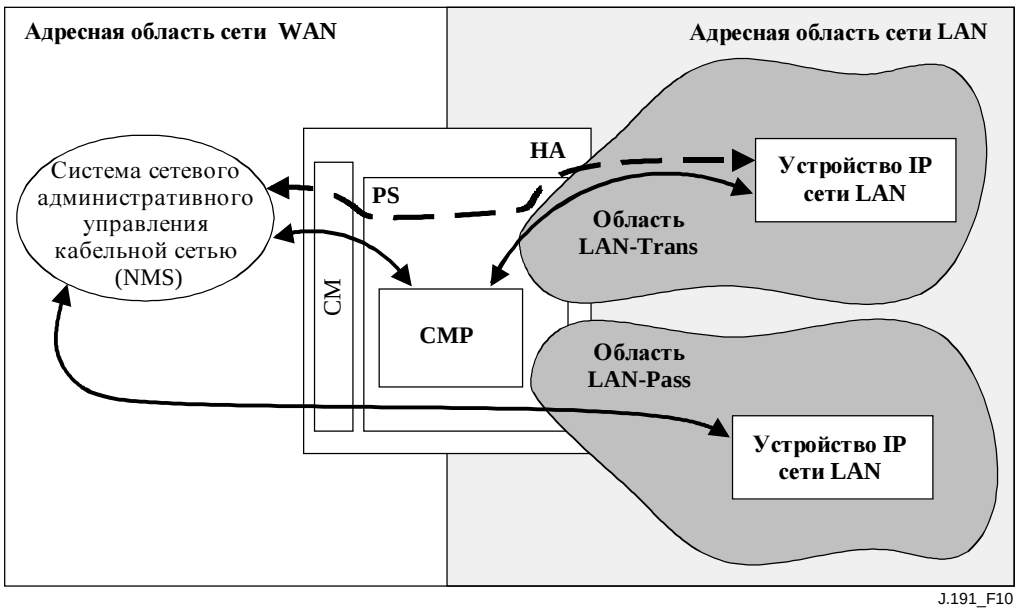


Рисунок 10/J.191 – Интерфейсы сообщений административного управления

Портал CMP главным образом является объектом, доступ к которому и управление которым обеспечивается сетью WAN (NMS). Дополнительно портал CMP может быть вызван для информирования системы NMS кабельной сети о событиях или файлах регистрации системы переноса, как требуется. Пример для осуществления портала CMP иллюстрируется на Рисунке 11, чтобы выразить понятия для функциональных возможностей CMP.

Инструменты административного управления NMS используют протокол SNMP для получения доступа и управления объектами в услуге PS. Протокол SNMPv3 обеспечивает установление подлинности Пользователя оператора NMS для услуги PS, доступ, основанный на обзоре, к объектам информационной базы (MIB) административного управления в услуге PS, а также шифрование сообщений административного управления, если требуется.

Агент протокола SNMP услуги PS имеет своей задачей преобразование идентификатора ID объекта (*OID, Object ID*) и экземпляра OID для всех листьев внутри функциональных блоков в PS, таких, как портал CAP или местное запоминающее устройство, например, база данных PS.

В дополнение к порталу CMP, оператор NMS может непосредственно осуществлять доступ или "управлять" Устройствами IP сети LAN, используя сквозную адресацию между головным узлом и устройством сети LAN, которым управляют. Однако нет требований по Устройствам IP сети LAN, чтобы откликаться на любые конкретные протоколы, административного управления или любые.

6.3.4 Общие требования CMP

Портал CMP ОБЯЗАН обеспечивать директиву Административного управления к сети WAN через протокол SNMP v3 [RFC 2571, RFC 2572].

Портал CMP ОБЯЗАН осуществлять протокол ICMP [RFC 792] и отвечать Запросам эха ICMP от системы NMS.

Если услуга PS работает в режиме обеспечения DHCP (указанном величиной '1' в объекте cabhPsDevProvMode), портал CMP ОБЯЗАН по умолчанию использовать протокол SNMPv1/v2c для обмена сообщениями административного управления с системой NMS и следовать правилам для режима NmAccess и режима Сосуществования, описанным в 6.3.6.1.

Если услуга PS действует в режиме обеспечения SNMP (указанном величиной '2' в объекте cabhPsDevProvMode), портал CMP ОБЯЗАН использовать протокол SNMPv3 для обмена сообщениями административного управления с системой NMS, следуя правилам, описанным в 6.3.6.2.

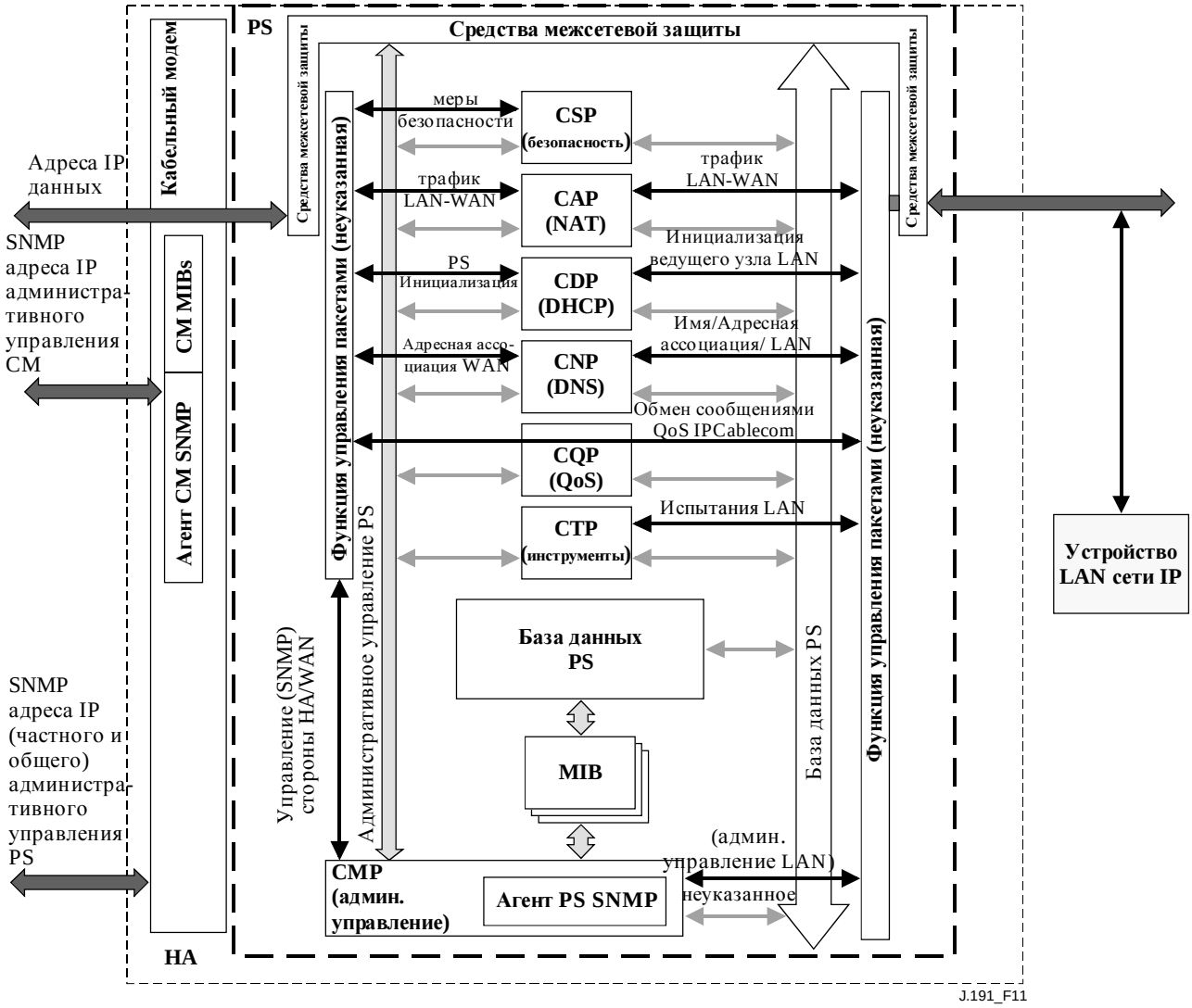


Рисунок 11/J.191 – Блок-диаграмма PS

Портал CMP ОБЯЗАН быть способен разрешать Окончательное удостоверение подлинности либо Администратору сети LAN, либо Администратору кабельной сети WAN (Администратору PS).

Установкой по умолчанию Окончательного удостоверения подлинности ОБЯЗАН быть Администратор сети WAN. Установка удостоверения подлинности МОЖЕТ быть отменена через доступ SNMP или файл конфигурации.

Корневым каталогом баз MIB (PSDev MIB, CAP MIB, CDP MIB, CTP MIB, и MIB безопасности) ОБЯЗАН быть (enterprises.[*предметная область*] 4491.2.4).

ОБЯЗАН быть осуществлен объект sysDescr из Системной группы MIB-2 (MIB-2 1) [RFC 1907] и он ОБЯЗАН сохраняться при переустановках устройств и циклах питания.

Значение sysDescr ОБЯЗАНО содержать пять полей в особом порядке следующим образом: HW_REV: hardware_version [*аппаратная версия*]; VENDOR [*поставщик*]: vendor_name; BOOTR: Boot_ROM_version; SW_REV: Software_version; Модель: Model_number.

Объект sysDesr складывается из перечня пяти пар "Тип/Значение". Разделение между Типом и Значением есть двоеточие и пробел. Разделение от одной пары "Тип/Значение" к следующей паре "Тип/Значение" есть точка с запятой и пробел. Требуемые пять пар SysDescr ОБЯЗАНЫ быть окружены двойными угловыми скобками. Например, объект sysDescr для услуги PS поставщика XYZ, аппаратная версия 5.2, версия 1.4 ROM начальной загрузки, программная версия 2.2 (*SW, software version*), и номер модели ABC ОБЯЗАНЫ показываться следующим образом:

> Любой текст «HW_REV: 5.2; VENDOR: XYZ; BOOTR: 1.4; SW_REV: 2.2; MODEL: ABC» любой текст

Услуга PS имеет необходимость сообщать, через поля sysDescr, обо всей информации, необходимой для определения, до какого обеспечения SW услуга PS способна обновляться. Если какие-либо требуемые поля sysDescr не применяются, то объект SysDescr ОБЯЗАН сообщить "NONE" [*никакое*] как о значении. Например, услуга PS без BOOTR будет сообщать BOOTR: NONE .

ОБЯЗАН быть осуществлен объект sysObjectID Системной группы MIB-2 [RFC 1907], и он ОБЯЗАН сохраняться при переустановках устройств и циклах питания.

ОБЯЗАН быть осуществлен объект sysUpTime Системной группы MIB-2 [RFC 1907]. Объект SysUpTime является количеством времени, которое истекает с момента переустановки системы.

ОБЯЗАН быть осуществлен объект sysContact Системной группы MIB-2 [RFC 1907], и он ОБЯЗАН сохраняться при переустановках устройств и циклах питания. Объект SysContact возвращает название пользователя или системного администратора, если они известны.

ОБЯЗАН быть осуществлен объект sysLocation Системной группы MIB-2 [RFC 1907], и он ОБЯЗАН сохраняться при переустановках устройств и циклах питания.

ОБЯЗАН быть осуществлен объект sysServices object Системной группы MIB-2 [RFC 1907], и он ОБЯЗАН сохраняться при переустановках устройств и циклах питания.

Объект SysServices ОБЯЗАН возвращать значение "3" (шлюз Интернет), когда запрашивается в элементе PS.

ОБЯЗАН быть осуществлен объект sysName object Системной группы MIB-2 [RFC 1907], и он ОБЯЗАН сохраняться при переустановках устройств и циклам питания. При опросе объект sysName возвращает название системы.

Объекты Системной группы MIB-2, отличающиеся от объектов sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation и sysServices, НЕ СЛЕДУЕТ осуществлять.

ОБЯЗАНА быть осуществлена база MIB группы интерфейсов [RFC 2863].

ОБЯЗАНА быть осуществлена группа SNMP MIB-2 [RFC 1907].

ОБЯЗАН быть осуществлен объект snmpSetSerialNo группы snmpSet [RFC 1907]. Объект SnmpSetSerialNo является консультативным замком, чтобы позволять нескольким кооперирующимся объектам SNMPv2, все из которых действуют в роли управляющей программы, координировать их использование операции установки SNMPv2.

Объекты группы SnmpSet, отличающиеся от snmpSetSerialNo, НЕ СЛЕДУЕТ осуществлять.

6.3.5 Требования протокола SNMP

ОБЯЗАНЫ быть прикреплены или осуществлены, по обстоятельствам, следующие документы IETF RFC:

- Простой протокол сетевого административного управления [RFC 1157];
- Введение в протокол SNMPv2, основанный на Сообществе [RFC 1901];
- Протокольные операции для протокола SNMPv2 [RFC 1905];
- Транспортные преобразования для протокола SNMPv2 [RFC 1906];
- Информационная база административного управления для версии 2 Простого протокола административного управления (SNMPv2) [RFC 1907];
- Введение в протокол SNMPv3 [RFC 2570];
- База MIB FrameWork протокола SNMP [RFC 2571];
- Обработка и координация сообщений для протокола SNMP [RFC 2572];
- База MIB приложений SNMP [RFC 2573];
- Группа MIB SnmpUSM [RFC 2574];
- Группа MIB SnmpVACM [RFC 2575];
- База MIB Сообщества протокола SNMP [RFC 2576];
- SNMPv2-CONF.

В поддержку SMIv2 ОБЯЗАНЫ быть осуществлены следующие документы IETF RFC:

- Версия 2 Структуры управляемой информации (SMIv2) [RFC 2578];
- Текстовые соглашения для SMIv2 [RFC 2579];
- Заявления о соответствии для SMIv2 [RFC 2580].

6.3.6 Требования режима сетевого административного управления

Этот раздел описывает правила для режимов сетевого административного управления, которые требуются услуге PS для поддержки Раздела 6.3.6.1, а его подразделы описывают режимы сетевого административного управления для услуги PS, действующей в режиме обеспечения DHCP. Раздел 6.3.6.2 и его подразделы описывают режимы сетевого административного управления для услуги PS, действующей в режиме обеспечения SNMP.

6.3.6.1 Режим NmAccessTable и режим Сосуществования для услуги PS, действующей в режиме обеспечения DHCP

Услуга PS ОБЯЗАНА поддерживать протоколы SNMPv1, SNMPv2c и SNMPv3 и Сосуществование SNMP, как описано документами от [RFC 2571] до [RFC 2576]. Услуга PS ОБЯЗАНА также поддерживать режим NmAccessTable, как определено документом [RFC 2669]. Поддержка режимов сетевого административного управления для услуги PS, действующей в режиме обеспечения DHCP, является предметом следующих руководящих принципов:

6.3.6.1.1 Основная операция для услуги PS, действующей в режиме обеспечения DHCP

a) Следуя получению DHCP ACK, услуга PS, действующая в режиме обеспечения DHCP (указанном с помощью значения cabhPsDevProvMode в '1' (DHCPmode)) ОБЯЗАНА действовать следующим образом:

- Доступ только для чтения SNMPv1/v2c ко всем переменным величинам базы MIB, которые требуется обозревать в течение операции SNMPv1/v2c, разрешается из сети LAN. Не разрешается доступ из сети WAN, чтобы предотвратить несанкционированный доступ административного управления до того, как услуга PS конфигурирована через Файл конфигурации PS.
- Принимаются пакеты SNMPv1/v2c, которые содержат любую строчку сообщества.
- Все пакеты SNMPv3 опускаются.
- СЛЕДУЕТ запретить доступ к любой переменной величине MIB, что позволила бы определение адреса IP WAN-Man услуги PS, например, такой, как IpAddrTable базы MIB-2.
- Никакие из баз MIB протокола SNMPv3 (MIB сообщества, TARGET-MIB [*цель*], VACM-MIB, USM-MIB, NOTIFICATION-MIB [*уведомление*]) не являются доступными, за исключением того, что они могут быть установлены из Файла конфигурации PS.
- Никакие из элементов в SNMP-USM-DH-OBJECTS-MIB [*объекты*] не являются доступными, за исключением того, что они могут быть установлены из Файла конфигурации PS.
- Успешная обработка всех элементов MIB в Файле конфигурации PS ОБЯЗАНА быть завершена перед вычислением открытых значений в Таблице USMDHKickstart.

b) Если услуга PS действует в режиме обеспечения DHCP, то содержание Файла конфигурации PS определяет режим сетевого административного управления, как описано ниже:

- Услуга PS находится в режиме docsDevNmAccess протокола SNMPv1/v2c, если Файл конфигурации PS содержит ТОЛЬКО установку Таблицы docsDevNmAccess для управления доступом SNMP.
- Если Файл конфигурации PS не содержит аспекты управления доступом SNMP (docsDevNmAccessTable, или snmpCommunityTable, или TLV 34.1/34.2, или TLV38), то тогда услуга PS находится в режиме NmAccess.
- Если Файл конфигурации PS содержит установку snmpCommunityTable и/или тип 34.1 и 34.2 TLV и/или тип 38 TLV, то тогда услуга PS находится в режиме Сосуществования SNMP. В этом случае любые записи, сделанные к docsDevNmAccessTable, игнорируются.

c) После завершения процесса обеспечения, описанного в 13.2 (указанного значением 'pass' [*прохождение*] (1) в cabhPsDevProvState), услуга PS действует в одном из двух режимов сетевого административного управления. Режим сетевого административного управления определяется содержанием Файла конфигурации PS, описанного выше.

Режим NmAccess (использующий Таблицу docsDevNmAccess) с использованием протокола SNMPv1/v2c:

- Обрабатываются только пакеты SNMPv1/v2c.
- Пакеты SNMPv3 опускаются.
- Объект docsDevNmAccessTable управляет доступом и пунктами назначения захвата, как описано в документе [RFC 2669].
- Никакая из баз MIB протокола SNMPv3 (MIB сообщества, TARGET-MIB, VACM-MIB, USM-MIB, NOTIFICATION-MIB) не является доступной.

Режим Сосуществования, использующий протокол SNMPv1/v2c/v3.

Во время вычислений открытых значений USMDHKickstartTable:

- Услуга PS ОБЯЗАНА НЕ разрешать какой-либо доступ SNMP из сети WAN.
- Услуга PS МОЖЕТ продолжать разрешать доступ из сети LAN с ограниченным доступом, как конфигурировано с помощью MIB USM, базы MIB сообщества и VACM-MIB.

После вычисления открытых значений USMDHKickstartTable:

- Услуга PS ОБЯЗАНА послать системное прерывание (захват) холодного пуска или теплого пуска для указания того, что услуга PS сейчас является полностью управляемой по протоколу SNMPv3.
- Пакеты SNMPv1/v2c/v3 обрабатываются так, как описывается документами [RFC 2571] и [RFC 2576].
- Объект docsDevNmAccessTable не является доступным.
- Управление доступом и пункты назначения системных прерываний (захватов) определяются с помощью snmpCommunityTable, NOTIFICATION-MIB, TARGET-MIB, VACM-MIB, и USM-MIB.
- База MIB сообщества управляет трансляцией строки сообщества пакетов SNMPv1/v2c в безопасное название, которое выбирает записи в USM-MIB. Управление доступом обеспечивается с помощью VACM-MIB.
- USM-MIB и VACM-MIB управляют пакетами SNMPv3.
- Пункты назначения системных прерываний (захватов) указываются в TARGET-MIB и NOTIFICATION-MIB.

В случае неудачи завершения установки SNMPv3 в начальное состояние для Пользователя (т.е. система NMS не может получить доступ к услуге PS через блок PDU протокола SNMPv3), Таблица пользователя USM для такого пользователя ОБЯЗАНА быть исключена, услуга PS находится в режиме Сосуществования и услуга PS будет позволять доступ SNMPv1/v2c, если и только если, записи MIB сообщества (и связанные записи) являются конфигурированными.

6.3.6.1.2 Установление в начальное состояние протокола SNMPv3 режима сосуществования и изменения ключей

При нахождении в режиме Сосуществования услуга PS ОБЯЗАНА поддерживать требования "установления в начальное состояние протокола SNMPv3" и "Изменения ключей DH", указанные в следующих разделах.

6.3.6.1.2.1 Установление в начальное состояние протокола SNMPv3

Для каждого из 5 различных безопасных имен Администратор PS порождает пару номеров. Первоначально Администратор PS порождает случайное число Rm.

Затем Администратор IPCable2Home использует уравнение DH для трансляции числа Rm в открытое число "z". Уравнение является следующим:

$$z = g \wedge Rm \text{ MOD } p$$

где "g" берется из набора параметров Диффи-Хелдлмана [*Diffie-Hellman*], а "p" является простым числом.

Создается Файл конфигурации PS для включения пары (названия безопасности, открытого числа). Услуга PS ОБЯЗАНА поддерживать минимум 5 пар. Например:

тип 34.1 TLV (Название безопасности толчкового запуска [*Kickstart*] протокола SNMPv3) = Администратор PS;

тип 34.2 TLV (Открытое число толчкового запуска протокола SNMPv3) = z;

Услуга PS ОБЯЗАНА поддерживать записи VACM, определенные в 6.3.6.4. Будут (ОБЯЗАНЫ быть) активными только записи VACM, указанные с помощью соответствующего названия безопасности в Файле конфигурации PS.

Во время процесса первоначального запуска услуги PS вышеуказанные значения (название безопасности, открытое число) ОБЯЗАНЫ быть заполнены в объекте usmDHKickstartTable.

В этой точке:

usmDHKickstartMgrpublic.1 = "z" (строка октета);

usmDHKickstartSecurityName.1 = "Администратор PS ".

Когда объект usmDHKickstartMgrpublic.n во время регистрации устанавливается с действительным значением, создается соответствующий ряд в объекте usmUserTable со следующими значениями:

usmUserEngineID: localEngineID;

usmUserName: значение usmDHKickstartSecurityName.n;

usmuserSecurityName: значение usmDHKickstartSecurityName.n;

usmUserCloneFrom: ZeroDotZero;

usmUserAuthProtocol: usmHMACMD5AuthProtocol;

usmuserAuthKeyChange: (извлекается из значения набора);

usmUserOwnAuthKeyChange: (извлекается из значения набора);

usmUserPrivProtocol: usmDESPrivProtocol;

usmUserPrivKeyChange: (извлекается из значения набора);

usmUserOwnPrivKeyChange: (извлекается из значения набора);

usmUserPublic;

usmUserStorageType: постоянное;

usmUserStatus: активное.

ПРИМЕЧАНИЕ – Для записей dhKickstart (PS) в usmUserTable, "Постоянное" означает, что оно ОБЯЗАНО быть написано, но не исключается и не сохраняется во время повторных начальных загрузок.

После того как услуга PS завершила установление в начальное состояние (указанное значением '1' (прохождение) для cabhPsDevProvState):

1) Услуга PS порождает случайное число "xa" для каждого заполненного ряда в usmDHKickstartTable, которое имеет usmDHKickstartSecurityName и usmDHKickstartMgrPublic ненулевой длины.

2) Услуга PS использует уравнение DH для трансляции "xa" в открытое число "c" (для каждого ряда, определенного выше).

$$c = (g \wedge xa) \text{ MOD } p$$

где "g" берется из набора параметров Диффи-Хеллмана, а "p" есть простое число из таких параметров.

В этой точке:

usmDHKickstartMyPublic.1 = "c" (строка октета);

usmDHKickstartMgrPublic.1 = "z" (строка октета);

usmDHKickstartSecurityName.1 = "docsisManager".

3) Услуга PS вычисляет совместно используемое секретное "sk", где "sk" = z ^xa mod p.

4) Услуга PS использует "sk" для извлечения ключа секретности и ключа проверки подлинности для каждого ряда в объекте usmDHKickstartTable и устанавливает значения в объекте usmUserTable.

Как указано в документе [RFC 2786], ключ секретности и ключ проверки подлинности для связанного имени пользователя, "Администратор PS" в этом случае, извлекается из "sk" путем использования функции производной ключа PBKDF2, определенной в PKCS#5 v2.0.

ключ секретности ← PBKDF2(salt = 0xd1310ba6,

iterationCount = 500,

keyLength = 16,

prf = id-hmacWithSHA1)

ключ проверки подлинности ← PBKDF2(salt = 0x98dfb5ac,

iterationCount = 500,

keyLength = 16 (usmHMACMD5AuthProtocol),

prf = id-hmacWithSHA1)

В этой точке услуга PS (CMP) завершила свой процесс установление в начальное состояние протокола SNMPv3 и ОБЯЗАНА разрешить соответствующий уровень доступа к действительному объекту securityName с правильным ключом установления подлинности и/или ключом секретности.

Услуга PS ОБЯЗАНА должным образом заполнить ключи к соответствующим таблицам, как указано документами RFC, относящимися к протоколу SNMPv3, и документом [RFC 2786].

5) Следующий далее текст описывает процесс, который управляющая программа использует для извлечения уникального ключа установления подлинности и ключа секретности услуги PS.

Управляющая программа SNMP получает доступ к содержимому usmDHKickstartTable, используя название безопасности 'dhKickstart' без проверки подлинности.

Услуга PS ОБЯЗАНА обеспечить предварительно установленные записи в таблице USM и таблицах VACM для правильного создания пользовательского 'dhKickstart' уровня безопасности noAuthNoPriv, что имеет только доступ для чтения к системной группе и usmDHkickstartTable.

Если услуга PS находится в режиме Сосуществования и конфигурируется для использования протокола SNMPv3, спецификация Группы для Обзора dhKickstart ОБЯЗАНА быть осуществлена следующим образом:

Группа dhKickstart	
vacmGroupName	'dhKickstart'
vacmAccessContextPrefix	''
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	NoAuthNoPriv
vacmAccessContextMatch	точное

vacmAccessReadViewName	'dhKickstartView'
vacmAccessWriteViewName	''
vacmAccessNotifyViewName	''
vacmAccessStorageType	постоянное
vacmAccessStatus	активное

Обзор VACM для обзора dhKickstart ОБЯЗАН быть осуществлен следующим образом:

dhKickstartView под-дерево 1.3.6.1.2.1.1 (Системная группа) и 1.3.6.1.3.101.1.2.1 (usmDHkickstartTable).

Программа управления SNMP получает значение числа usmDHKickstartMypublic услуги PS, связанное с объектом securityName, для которого управляющая программа желает извлечь ключи проверки подлинности и секретности. Используя секретное случайное число, управляющая программа может вычислить совместно используемый секрет DH. Из такого совместно используемого секрета управляющая программа может извлечь ключи эксплуатационной проверки подлинности и конфиденциальности для объекта securityName, который управляющая программа собирается использовать для осуществления связи с услугой PS.

6.3.6.1.2.2 Изменения ключей Диффи-Хеллмана

Услуга PS ОБЯЗАНА поддерживать механизм изменения ключей, указанный в документе [RFC 2786].

6.3.6.2 Режим обеспечения протокола SNMP

Если услуга PS действует в режиме обеспечения SNMP, следуя АСК DHCP (как указывается значением '2' (SNMPmode) для cabhPsDevProvMode), она действует в режиме сетевого административного управления, используя протокол SNMPv3, USM VACM и систему установления подлинности Kerberos ["*Цербер*"] для обмена ключевым материалом (как описывается в 6.3.3), следуя правилам, описанным в этом разделе.

6.3.6.2.1 Обзоры административного управления

Директивы административного управления содержатся в элементе PS. Установки, основанные на режиме административного управления, определяют права доступа, которые предоставляются генератору команд для доступа к базе данных PS, через указанные базы MIB, через протокол SNMP из системы NMS кабельной сети. Генератор отдельной команды определяется спецификацией.

Рисунок 12 иллюстрирует несколько примеров Обзоров административного управления, используя протокол SNMPv3. Определяются обзор Администратора сети WAN (обзор Администратора PS) и Пользователя администратора сети WAN (пользователь

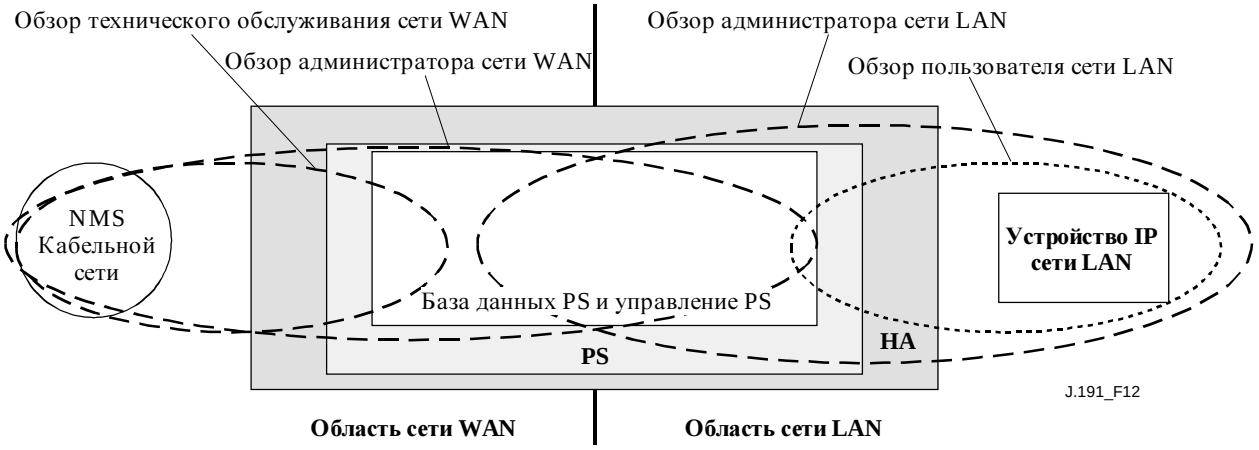


Рисунок 12/J.191 – Обзоры административного управления

Администратора PS). Другие такие Обзоры и Пользователи, как Обзор технического обслуживания сети WAN, Обзор администратора сети LAN, или Обзор пользователя сети LAN могут быть установлены с помощью Окончательного удостоверения подлинности (Администратор PS), следуя правилам, определенным в документах [RFC 2574] и [RFC 2575].

Управляемые параметры хранятся в базе данных PS. Как показано на Рисунке 12, имеется понятие Обзоров доступа в базу данных PS и Управления PS, которые позволяют одновременное административное управление как из сети LAN, так и из сети WAN путем определения Обзоров административного управления в базе данных PS и Управлении PS . Обзоры являются механизмами для обеспечения секретности и безопасности, а алгоритм может быть установлен отдельно Пользователем администратора PS.

Окончательное удостоверение подлинности (Пользователь администратора PS) имеет следующие ответственности:

- для установки всех Обзоров доступов как на интерфейсе административного управления сети LAN, так и сети WAN.
- для собственных идентификаторов ID пользователя и ключей.
- для создания и управления всеми профилями Пользователей, включая идентификаторы ID пользователей, ключи и привилегии доступа к базам данных PS .
- для установки алгоритма как для доступа стороны LAN, так и стороны WAN.

Полное осуществление VACM требует набора действий, которые привяжут "Пользователя" к "Группе", а "Группу" - к Обзору VACM, который определяет доступ. Раздел 6.3.6.4 описывает, как создавать эти взаимосвязи.

Объектом vacmSecurityName является "Пользователь". Это название безопасности привязано к объекту vacmGroupName. Таким образом, "Пользователь" привязывается к конкретной Группе. Группа затем определяется, чтобы указать, какой уровень безопасности используется, а также какие Обзоры чтения, записи и уведомления доступны для этой группы. Обзоры затем указываются, чтобы показать точно, какие объекты MIB являются доступными.

Модель управления доступом на основе Обзора определяет права доступа Группы, представляя нуль или более объектов securityNames, которые имеют те же самые права доступа. Для конкретного контекста, определяемого объектом contextName, к которому Группа, указанная объектом groupName, имеет доступ, используя конкретные объекты securityModel и securityLevel, права доступа такой Группы даются обзором чтения, обзором записи и обзором уведомления.

Обзор чтения представляет собой набор экземпляров объектов, санкционированных для Группы при чтении объектов. Объекты чтения возникают при обработке операции поиска и выборки информации (при обработке блоков PDU Класса чтения).

Обзор записи представляет собой набор экземпляров объектов, санкционированных для Группы при записи объектов. Объекты записи возникают при обработке операции поиска и выборки информации (при обработке блоков PDU Класса записи).

Обзор уведомления представляет собой набор экземпляров объектов для Группы при отправке объектов в уведомлении, например, при отправке уведомления (при отправке блоков PDU Класса уведомления).

Обзор Администратора PS предоставляет полный доступ для чтения и записи ко всем указанным базам MIB.

Требования Обзора административного управления указываются в 6.3.6.4.

6.3.6.2.2 Управление доступом сети WAN

Управление доступом SNMP, по документу [RFC 2575], будет использовано для Обзоров стороны WAN. Модель управления доступом на основе Обзора (*VACM, View-based Access Control Model*) [RFC 2575] определяет набор услуг, которые можно использовать для проверки прав доступа. Группы VACM определяют права для доступа к порталу CMP.

Как определено в документе [RFC 2575], секция 2.4, "Обзор базы MIB" является особым набором типов управляемых объектов, которые могут быть определены, и это понятие используется для поддержки Административного управления сети WAN услуги PS. Доступ Пользователя администратора PS и Обзор указываются в 11.3.3.2.2 и в 6.3.6.4. Примерная последовательность доступа базы данных PS от интерфейса WAN предоставляется в 12.3.1.

6.3.6.2.3 Безопасность

Безопасность сообщений административного управления обеспечивается протоколом SNMPv3. Можно сделать ссылку на раздел 11 для подробного описания того, как используется протокол SNMPv3. Портал CMP может использовать протокол SNMP v3 для подсчетов угроз, указанных в Дополнении C.

Для защиты против атак воспроизведения используется тактовый генератор реального времени, чтобы обеспечивать отметки времени для обмена сообщениями. Требования по безопасности обмена сообщениями административного управления указываются в 11.3.3.

6.3.6.3 Требования по безопасности

Требования по безопасности обмена сообщениями административного управления указываются в 11.3.3.

6.3.6.4 Требования модели управления доступом на основе обзора (*VACM, View-based Access Control Model*)

Для обеспечения контролируемого доступа к информации административного управления и создания четких областей административного управления ОБЯЗАНА использоваться Модель контроля доступа на основе Обзора (*VACM, View-based Access Control Model*), как определено документом [RFC 2575].

Обзор Администратора WAN ОБЯЗАН быть осуществлен в элементе PS. Обзоры по умолчанию, отличающиеся от Обзора администратора WAN, ОБЯЗАНЫ НЕ быть доступными на услуге PS. Другие обзоры МОГУТ быть созданы системой NMS кабельной сети путем конфигурации базы MIB VACM.

Спецификация Пользователя для Обзора администратора WAN ОБЯЗАНА быть осуществлена следующим образом:

vacmSecurityModel	3 (USM)
vacmSecurityName	'Администратор PS'
vacmGroupName	' Администратор PS'
vacmSecurityToGroupStorageType	постоянное
vacmSecurityToGroupStatus	активное

Спецификация Группы для Обзора администратора PS ОБЯЗАНА быть осуществлена следующим образом:

Группа администратора PS	
vacmGroupName	' Администратор PS'
vacmAccessContextPrefix	"
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	AuthPriv
vacmAccessContextMatch	точное
vacmAccessReadViewName	'PS AdministratorView'
vacmAccessWriteViewName	'PS AdministratorView'
vacmAccessNotifyViewName	'PS AdministratorView'
vacmAccessStorageType	постоянное
vacmAccessStatus	активное

Обзор VACM для обзора Администратора PS ОБЯЗАН быть осуществлен следующим образом:

Под-дерево Обзора администратора PS 1.3.6.1 (Полная база MIB).

6.3.7 Требования базы MIB

Объекты MIB, перечисленные в Дополнении A, ОБЯЗАНЫ быть осуществлены в элементе PS. Требуемыми объектами MIB являются объекты из следующих документов MIB:

База MIB группы интерфейсов [RFC 2863]

1) База MIB Кабельного устройства DOCSIS [RFC 2669];
2) Кабельная база MIB DEF CLAB [Дополнение E.4];
3) Кабельная база MIB PSDev [Дополнение E.1];
4) Кабельная база MIB CAP [Дополнение E.6];
5) Кабельная база MIB CDP [Дополнение E.5];
6) Кабельная база MIB CTP [Дополнение E.2];
7) Кабельная база MIB Безопасности [Дополнение E.3];
8) draft-ietf-ipcdn-bpiplus-mib-06.txt;
9) База MIB IP (SNMPv2) [RFC 2011];
10) База MIB UDP (SNMPv2) [RFC 2013];
11) Ключ USM Диффи-Хеллмана [RFC 2786];
12) Адресная база MIB INET [RFC 2851];
13) База MIB IF DOCS [RFC 2670];

14) База MIB ifType IANA.

За исключением группы SNMP из баз MIB 2, MIB USM и USM VACM, к которым имеется прямой доступ с помощью агента SNMP в услуге PS (CMP), И базы MIB кабельного устройства DOCSIS для случая загрузки программного обеспечения к услуге PS, услуга PS ОБЯЗАНА поддерживать отдельные экземпляры баз MIB, характерных для PS, из кабельного модема. Информация, к которой имеется доступ из базы данных PS через адрес WAN-Man услуги PS, ОБЯЗАНА быть отдельной и отличной от информации, к которой имеют доступ через адрес административного управления модема CM.

Общая иерархия базы MIB иллюстрируется на Рисунке 13. Конкретные идентификаторы OID, требуемые для индивидуальных баз MIB, перечисляются в Дополнении A.

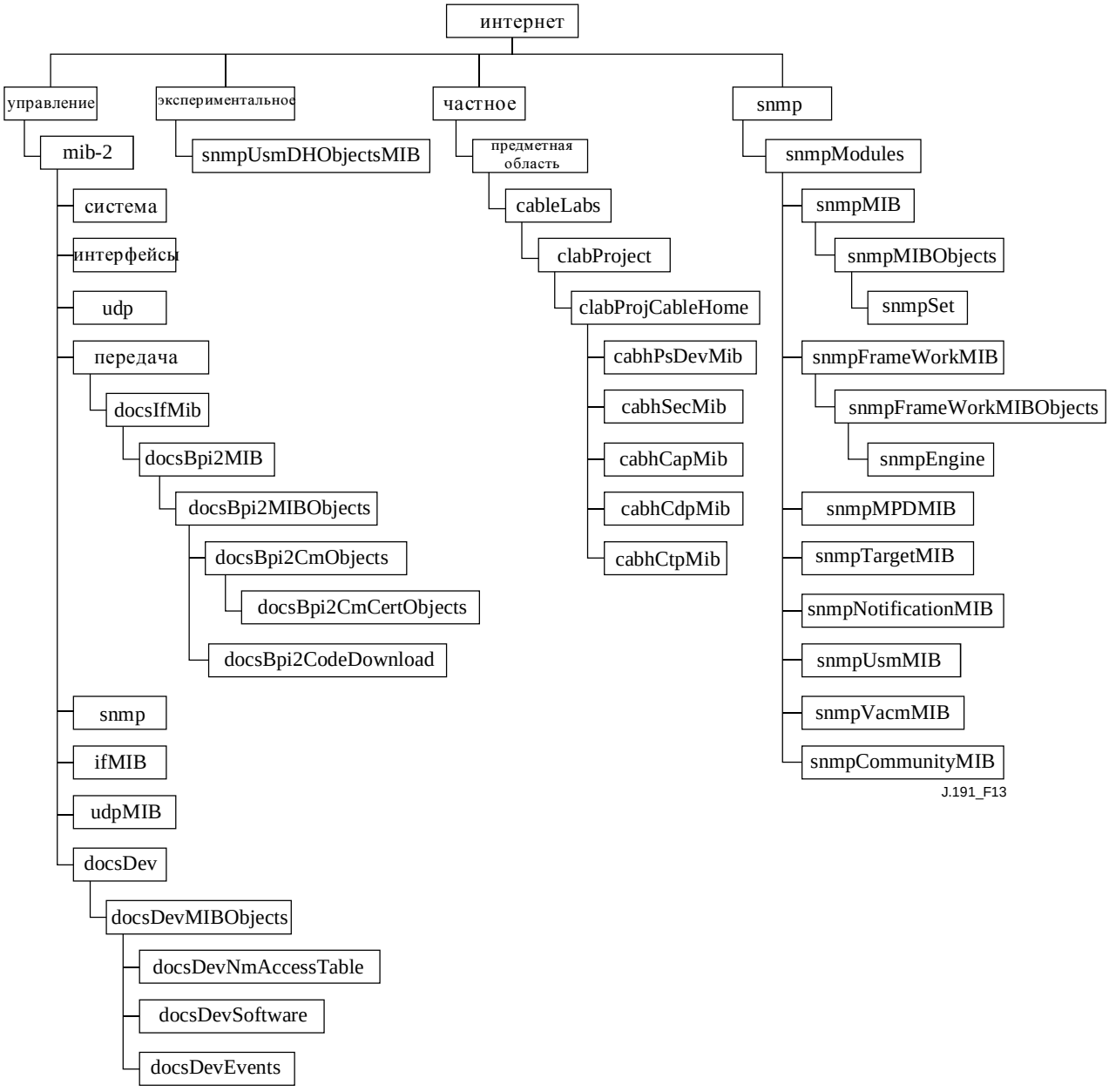


Рисунок 13/J.191 – Иерархия базы MIB

6.3.8 Требования базы MIB группы интерфейсов

База MIB Группы интерфейсов обеспечивает мощный инструмент, который позволяет кабельным операторам понимать состояние всех физических интерфейсов и видеть их статистику на элементе Услуги портала. Чтобы обеспечивать разумное использование этой

базы MIB, существенной является схема нумерации интерфейсов. Поэтому элементы PS нуждаются в соответствии следующим требованиям:

ОБЯЗАН существовать экземпляр IfEntry для интерфейса WAN из элемента PS, даже если такой интерфейс WAN является внутренним – как существует в случае встроенной услуги PS, использующей разработку интегральной микросхемы.

Экземпляр IfEntry ОБЯЗАН существовать для каждого физического интерфейса LAN элемента PS.

Интерфейсы ОБЯЗАНЫ быть перенумерованы так, как показано в Таблице 12.

Таблица 12/J.191 – Нумерация интерфейсов в объекте ifTable

Интерфейс	Описание
1	Интерфейс сети WAN
1 + n	Каждый интерфейс сети LAN

Если fAdminStatus заданного интерфейса = down [*не работает*], такой интерфейс ОБЯЗАН НЕ получать или перенаправлять какой-либо трафик.

6.3.9 Требования обработки файлов конфигурации CMP

Портал CMP является функциональным объектом в услуге PS, отвечающим за обработку параметров, передаваемых в Файлах конфигурации PS. Файлы конфигурации PS используются для повторной конфигурации услуги PS путем предоставления значений для управляемых параметров в базе данных PS.

Полученный Файл конфигурации PS сначала проверяется на целостность и проходит проверку подлинности, как описано в 11.3.7. Затем, кортежи (наборы взаимосвязанных величин) TLV в Файлах конфигурации PS анализируются и извлекаются идентификаторы объектов SNMP и их параметры. Портал CMP ОБЯЗАН использовать параметры, извлеченные из Файла конфигурации PS, чтобы установить управляемые объекты в базе данных PS. Этот процесс функционально эквивалентен операции SET [*установить*] протокола SNMP, но он не полагается на разрешения пользователя или доступа на основе обзора. Портал CMP ОБЯЗАН безоговорочно обновить объекты, соответствующие опознанным идентификаторам OID.

Установки конфигурации ОБЯЗАНЫ быть обработаны в том же самом порядке, в каком они появляются в Файле конфигурации PS. Портал CMP ОБЯЗАН быть способен к получению ряда параметров TLV, содержащихся в Файле конфигурации PS. Нет предубежденного состояния PS, когда принимается Файл конфигурации PS. Процесс загрузки и выполнения Файла конфигурации PS может прерывать обработку данных в услуге PS. Портал CMP ОБЯЗАН проигнорировать любую установку конфигурации, для которой не существует действительного параметра базы данных.

Для установок SNMP в Файле конфигурации PS услуга PS ОБЯЗАНА обрабатывать все переменные связывания SNMP (Varibinds) в Файле конфигурации услуги PS так, как будто они были получены в единственном блоке PDU протокола SNMP. Если в Файле конфигурации PS принимаются удвоенные переменные Varibinds, то тогда услуга PS ОБЯЗАНА остановить процесс обеспечения.

Объекты, определенные с помощью значений TLV, что проследовали в Файле конфигурации PS и не поддерживаются или не могут быть прочитаны в конкретном осуществлении PS, ОБЯЗАНЫ быть проигнорированы. Портал CMP ОБЯЗАН проигнорировать любое неизвестное значение TLV.

Размер Файла конфигурации PS, количество обрабатываемых значений TLV и количество проигнорированных значений TLV ОБЯЗАНО быть обновлено в объектах MIB: соответственно cabhPsDevProvConfigFileSize, cabhPsDevProvConfigTLVProcessed и cabhPsDevProvConfigTLVRejected.

Требования Файла конфигурации PS указываются в 7.3.

6.4 Испытательный портал CableHome (CTP)

6.4.1 Цели портала CTP

Цели для испытательного портала CableHome включают в себя:

- Обеспечивать диагностику неисправностей Устройства IP сети LAN;
- Обеспечивать обозримость для Устройств IP сети LAN, а также доступ к ряду и типам Устройств IP сети LAN;
- Обеспечивать наблюдение за показателями качества Устройства IP сети LAN.

6.4.2 Руководящие принципы разработки CTP

Руководящие принципы разработки системы Инструментов административного управления перечисляются в Таблице 13. Ряд из этих руководящих принципов является общим с руководящими принципами разработки CMP. Этот перечень предоставлял руководство для спецификации функциональных возможностей CTP.

Таблица 13/J.191 – Руководящие принципы разработки системы CMP

Ссылка	Руководящие принципы разработки системы CMP
CTP 1	Для интерфейсов существует потребность поддерживать свойства административного управления и диагностики, а также функции, требуемые для поддержки услуг на основе кабеля, обеспечиваемых в доме.
CTP 2	Нужны возможности местного и дистанционного наблюдения, которые могут наблюдать за домашней операцией и помогать клиенту и кабельному оператору определять проблемные области.
CTP 3	Система NMS кабельной сети требует метод, чтобы накапливать информацию идентификации относительно каждого устройства IP, подсоединенного в доме.
CTP 4	Система NMS кабельной сети требует метод для обнаружения, находится ли подключенное устройство в рабочем состоянии.

6.4.3 Описание системы CTP

Портал CTP (Испытательный портал CableHome) содержит "удаленные инструменты", с помощью которых административное управление NMS может собирать дальнейшую информацию об устройстве сети LAN. Испытания должны выполняться дистанционно, поскольку прохождение через функцию трансляции сетевого адреса (*NAT, network address translation*) в маршрутизаторе может быть сложной проблемой. Например, перебрасывание информации из сети WAN в сеть LAN не будет проходить через услугу PS, если портал CAP не был предварительно конфигурирован для пропускания этого трафика. Портал CTP является местным посредником, используемым для истолкования и выполнения дистанционного класса неисправности/диагностики из сообщений SNMP, которые он принимает от оператора NMS. Эти испытания Устройств IP сети LAN определяются на основе проблем, которые, похоже, должны встретиться: диагностика связности и производительности.

Эти функции называются Инструментом скорости соединения CTP и Инструментом дистанционного переброса информации CTP. Инструменты Скорости соединения и

Дистанционного переброса информации обеспечивают центр поддержки клиента кабельного оператора и центр сетевых операций возможностью узнавать больше подробностей относительно соединения между элементом PS и устройствами IP сети LAN IP в доме.

6.4.3.1 Инструмент скорости соединения CTP

Эта функция используется для получения грубой меры показателей качества через звено между услугой PS и Устройством IP сети LAN. Она посылает пачку пакетов между услугой PS и испытуемым Устройством IP сети LAN, и для пачки измеряется время задержки передачи по шлейфу. Вообще говоря, оператор NMS заполняет несколько параметров и запускает функцию, а результат хранится в базе данных PS для последующего поиска и извлечения через базу MIB портала CTP.

Функция Скорости соединения полагается на то, что Устройства IP сети LAN должны иметь встроенную "функцию обратного шлейфа" или "услугу эха". Полномочный орган по назначению адресов Интернет (*IANA, Internet Assigned Numbers Authority*) назначил порт 7 услуги эха как для протокола TCP, так и для протокола UDP [RFC 347]. Исходный IP адрес всегда является таким, как шлюз по умолчанию сети LAN услуги PS (cabhCdpServerRouter). Это испытательная особенность работает только на Устройствах IP сети LAN в адресной области LAN Trans.

Раздел по Испытуемым требованиям, приводимый ниже, перечисляет параметры и отклики для Инструмента скорости соединения. Раздел 12.2.1.1 приводит подробности операции для Инструмента скорости соединения.

6.4.3.2 Инструмент переброса информации CTP

Эту функцию вызывают, чтобы проверить возможность соединения между услугой PS и индивидуальным Устройством IP сети LAN. Результаты многократного выполнения испытания Инструмента переброса информации могут быть собраны системой NMS, чтобы создать сетевой просмотр Устройств IP сети LAN. Таблица DHCP портала CDP имеет список хронологических устройств, но только тех устройств, которые используют протокол DHCP. Переброс информации может захватить текущее состояние, включая клиентов, не являющихся клиентами протокола DHCP. Чтобы сохранять услугу PS простой, ожидается, что система NMS увеличивает адрес и хранит результаты в инструменте NMS, чтобы выполнить просмотр подсети LAN.

Инструмент переброса информации инициируется рядом сообщений Set Request " [*установить запрос*] протокола SNMP, выпускаемых консолью системы NMS кабельной сети к адресу административного управления услуги PS.

Инструмент Переброса информации ОБЯЗАН быть осуществлен с использованием возможностей "Эха" Протокола сообщения для управления Интернет (*ICMP, Internet Control Message Protocol*)". Портал CTP будет выпускать сообщение Echo Request [*Запрос эха*] протокола ICMP, а от Устройства IP сети LAN ожидается возврат сообщения Echo Reply [*Ответ эха*] протокола ICMP.

Раздел 6.4.4 перечисляет параметры и отклики для Инструмента переброса информации. Отметим, что время для ответа на запрос не сохраняется, поскольку время распространения типового кадра в доме может быть быстрее, чем могут точно измерить стандартные временные единицы (мс). Для измерения показателей качества следует использовать Инструмент скорости соединения.

Раздел 12.2.1.2 дает подробности Инструмента переброса информации.

6.4.4 Требования портала CTP

Портал CTP ОБЯЗАН осуществлять Инструмент скорости соединения с параметрами, перечисленными ниже, где угловые скобки указывают объект базы MIB портала CTP. Числа в

квадратных скобках являются вариантами выбора, или нижней и верхней границами диапазона параметров, а число в круглых скобках является значением по умолчанию:

– <cabhCtpConnSrcIp> (равно значению cabhCdpServerRouter) – адрес IP сети LAN, используемый в качестве источника Инструмента скорости соединения;

– <cabhCtpConnDestIp> – адрес IP сети LAN, используемый в качестве пункта назначения Инструмента скорости соединения;

ПРИМЕЧАНИЕ 1 – Может быть установлен в любой действительный адрес IPv4, чтобы находить Устройства IP сети LAN в адресной области LAN-Trans.

– <cabhCtpConnProto> [UDP (1), TCP (2)] (UDP) – протокол, используемый для Инструмента скорости соединения;

– <cabhCtpConnPort> [1 to 65535] (7) – порт, используемый для Инструмента скорости соединения.

ПРИМЕЧАНИЕ 2 – Орган IANA для этого использования резервирует порт 7. Могут быть полезны и другие порты.

– <cabhCtpConnNumPkts> [от 1 до 255] (1) – количество пакетов, подлежащих передаче для Инструмента скорости соединения;

– <cabhCtpConnPktSize> [–64 to 1518] (64) – размер испытательных кадров для Инструмента скорости соединения в байтах;

– <cabhCtpConnTimeOut> [от 0 до 600000] (600000) – значение выдержки времени, в миллисекундах, для отклика к Инструменту скорости соединения.

ПРИМЕЧАНИЕ 3 – Значение "нуль" указывает отсутствие выдержки времени и может быть использовано только для протокола TCP.

– <cabhCtpConnControl> [notRun (1), запуск (2), прекращение (3)] – управление для испытания Скорости соединения;

– <cabhCtpConnStatus> [прогон (1), завершение (2), прекращено (3)] – статус испытания Скорости соединения;

– <cabhCtpConnPktsSent> [от 1 до 255] – число пакетов, посланных в течение испытания Скорости соединения;

– <cabhCtpConnPktsRecv> [от 0 до 255] – число пакетов, полученных во время испытания Скорости соединения.

ПРИМЕЧАНИЕ 4 – Это значение позволяет оператору определять, была ли достигнута выдержка времени (PktsSent > PktsRecv) из-за пропадания пакетов, предполагая, что выдержка времени была правильно вычислена. Эта пара параметров была включена для поддержки обнаружения пропадания пакетов UDP. При нормальной работе PktsRecv равно PktsSent.

– <cabhCtpConnAvgRTT> [от 0 до 600000] – результат усреднения времени передачи по шлейфу для признанных пакетов в миллисекундах;

– <cabhCtpConnMaxRTT> [от 0 до 600000] – результирующий максимум значений времени передачи по шлейфу для признанных пакетов в миллисекундах;

– <cabhCtpConnMinRTT> [от 0 до 600000] – результирующий минимум значений времени передачи по шлейфу для признанных пакетов в миллисекундах;

– <cabhCtpConnNumIcmpError> [от 0 до 255] – число ошибок ICMP.

ПРИМЕЧАНИЕ 5 – Значение может включать в себя сеть или ведущий узел "запрещенный" [*prohibited*] или "недостигаемый" [*unreachable*]. Этот параметр является пустым по умолчанию, или когда не возникают ошибки.

– <cabhCtpConnIcmpError> [от 0 до 255] – последняя ошибка ICMP.

Портал CTP ОБЯЗАН осуществлять Инструмент переброса информации CTP с параметрами, перечисленными ниже, где угловые скобки указывают объект MIB портала CTP, числа в скобках являются нижними и верхними границами диапазона параметров, а число в круглых скобках является значением по умолчанию:

– <cabhCtpPingSrcIp> (равно значению cabhCdpServerRouter) – адрес IP сети LAN, используемый в качестве источника инструмента Удаленного переброса информации;

– <cabhCtpPingDestIp> – адрес IP сети LAN, используемый в качестве пункта назначения инструмента Удаленного переброса информации;

– <cabhCtpPingProto> [icmp (1)] (icmp) – протокол, использованный для инструмента Удаленного переброса информации;

– <cabhCtpPingNumPkts> [от 1 до 4] (1) –число пакетов, которые нужно отправить каждому ведущему узлу для испытания Удаленного переброса информации;

– <cabhCtpPingPktSize> [от –64 до 1518] (64) – размер испытательных кадров для испытания Удаленного переброса информации в байтах;

– <cabhCtpPingTimeBetween> [от 0 до 600000] (1000) – время между отправкой одного пакета и следующего пакета во время испытания Удаленного переброса информации в миллисекундах;

– <cabhCtpPingTimeOut> [от 0 до 600000] (5000) –выдержка времени для отклика отправки отдельного переброса информации во время испытания Удаленного переброса информации в миллисекундах;

– <cabhCtpPingControl> [notRun(1), запуск (2), прекращение (3)] – управление для испытания Удаленного переброса информации;

– <cabhCtpPingStatus> [прогон (1), завершение (2), прекращено (3)] – статус испытания Удаленного переброса информации;

– <cabhCtpPingNumSent> [от 0 до 254] – число перебросов информации, посланных во время испытания Удаленного переброса информации;

– <cabhCtpPingNumRecv> [от 0 до 254] – число перебросов информации, полученных во время испытания Удаленного переброса информации.

6.5 Информирование о событии

Информирование о событии и используемые механизмы управления находятся в документе RFC 2669, который определяет стандартный формат для того, чтобы сообщать об информации события, независимо от типа сообщения, включая таблицу регистрации местного события, в котором некоторые записи будут сохраняться во время повторного начального запуска услуги PS. Отметим, что события могут быть порождены любой частью услуги PS, но протокол CMP регистрирует и/или сообщает о событии или местным образом, или к серверу Syslog или Trap [*захват*].

6.5.1 Уведомление о событии

Услуга PS ОБЯЗАНА порождать асинхронные события, которые указывают важные события и ситуации, как указано в Дополнении B. События могут быть сохранены в ЖУРНАЛЕ [*LOG*] внутреннего события, хранимого в энергонезависимом запоминающем устройстве, сообщены другим объектам SNMP (в качестве сообщений протокола SNMP TRAP или INFORM), или посланы в качестве сообщения события SYSLOG к предварительно определенному серверу SYSLOG.

Услуга PS ОБЯЗАНА поддерживать следующие механизмы уведомления о событиях:

- регистрация местного события, где определенные записи в местном журнале могут быть определены с сохранением при повторном начальном запуске услуги PS;
- TRAP и INFORM протокола SNMP;
- SYSLOG.

Уведомление о событии услугой PS является полностью конфигурируемым. Услуга PS ОБЯЗАНА осуществить объект docsDevEvControlTable из документа [RFC 2669], чтобы управлять информированием о событиях. Услугой PS ОБЯЗАНЫ быть поддержаны следующие значения BIT для [RFC 2669] объекта object docsDevEvReporting:

- 1: местное-энергонезависимое(0);
- 2: 2: traps(1)
- 3: syslog(2);
- 4: местное-энергозависимое (3);
- 5: информировать(4).

Сообщения запроса SET [*установить*] протокола SNMP к объекту [RFC 2669] docsDevEvReporting, используя следующие значения, ОБЯЗАНЫ иметь своим результатом ошибку 'Неправильное значение' [*Wrong Value*] для блоков PDU протокола SNMP:

- 0x20 = только syslog;
- 0x40 = только системное прерывание (захват);
- 0x60 = только (захват + syslog).

Событие, сообщаемое с помощью Trap, Syslog или Inform, ОБЯЗАНО также порождать местную энергонезависимую запись в журнале, как описано в 6.5.1.1.

6.5.1.1 Регистрация местного события

Услуга PS ОБЯЗАНА сохранять отдельную таблицу событий местной регистрации, которая содержит события, хранимые как местные энергозависимые (разрушающиеся) события, так и местные энергонезависимые (не разрушающиеся) события. События, хранимые как местные энергонезависимые события, ОБЯЗАНЫ продолжать существовать во время повторной начальной загрузки услуги PS. Таблица событий местной регистрации ОБЯЗАНА быть организована как циклический буфер с минимум десятью записями. Отдельная таблица событий местной регистрации ОБЯЗАНА быть доступной через объект docsDevEventTable, как определено в документе [RFC 2669].

Описания событий ОБЯЗАНЫ появляться на английском языке. Описания событий ОБЯЗАНО НЕ быть длиннее, чем 255 байтов, что является максимумом, определенным объектом SnmpAdminString.

Объект EventId представляет собой незнаковое целое число из 32 битов. Объекты EventId, простирающиеся от 0 до $(2^{31} – 1)$, резервируются. Объект EventId ОБЯЗАН быть преобразован из кодов ошибок, определенных в Дополнении B. Объекты EventId, простирающиеся от 2^{31} до $(2^{32} – 1)$ ОБЯЗАНЫ быть использованы в качестве объектов EventId, характерных для поставщика, с использованием следующего формата:

- Бит 31 установлен для указания события, характерного для поставщика;
- Биты 30-16 содержат нижние 15 битов номера предприятия поставщика SNMP;
- Биты 15-0 использованы поставщиком для нумерации своих событий.

Объект [RFC 2669] docsDevEvIndex обеспечивает относительный порядок событий в журнале регистрации. Разметка ярлыками событий местной регистрации в качестве местных энергозависимых и местных энергонезависимых делает необходимым метод для синхронизации значений docsDevEvIndex между двумя типами событий после повторной начальной загрузки услуги PS. После повторной начальной загрузки услуги PS, чтобы синхронизовать значения docsDevEvIndex для энергозависимых и энергонезависимых событий, ОБЯЗАНА использоваться следующая процедура:

- Значения docsDevEvIndex для событий местной регистрации, маркированных в качестве местных энергонезависимых, ОБЯЗАНЫ быть перенумерованы, начиная с 1;
- Местная регистрация ОБЯЗАНА быть затем установлена в начальное состояние с событиями, маркированными как местные энергонезависимые, в том же самом

  порядке, как они были сразу же перед повторной начальной загрузкой;
- Последовательные события, записанные в местном журнале регистрации, будь ли они маркированы как местные энергозависимые, или местные энергонезависимые, ОБЯЗАНЫ использовать увеличивающиеся значения docsDevEvIndex.

Переустановка местного журнала регистрации, инициированная через сообщение SET протокола SNMP из объекта [RFC 2669] docsDevEvControl ОБЯЗАНА очистить все события из местного журнала регистрации, включая события регистрации, маркированные как местные энергозависимые, так и местные энергонезависимые.

6.5.1.2 TRAP и INFORM протокола SNMP

Услуга PS ОБЯЗАНА поддерживать блок PDU TRAP протокола SNMP, как описано в документе [RFC 2571]. Услуга PS ОБЯЗАНА поддерживать блок PDU INFORM протокола SNMP, как описано в документе [RFC 2571]. INFORM есть вариация системного прерывания (захвата) и требует от приемного ведущего узла подтверждать прибытие блока InformRequest-PDU с помощью InformResponse-PDU.

Когда в услуге PS обеспечивается стандартный захват SNMP, то она ОБЯЗАНА посылать уведомления для любого события в той категории, приоритет которой является либо "ошибка", либо "извещение".

Услуга PS МОЖЕТ поддерживать события, характерные для поставщика. Если они поддерживаются, то события PS, характерные для поставщика, о которых можно сообщить через TRAP протокола SNMP, ОБЯЗАНЫ быть описаны в частной базе MIB, которая распределяется с услугой PS. При определении захвата SNMP, характерного для поставщика, заявлению OBJECTS [*объекты*] из определения частного захвата СЛЕДУЕТ содержать объекты, которые объясняются ниже:

- EvLevel;
- EvIdText;
- Порог события (если такой имеется для захвата);
- IfPhysAddress (физический адрес, связанный с адресом IP WAN-Man услуги PS).

В заявлении OBJECTS может содержаться больше объектов, если этого желают.

6.5.1.3 Syslog

Сообщения SYSLOG, выпущенные услугой PS, ОБЯЗАНЫ быть в следующем формате:

< level>PortalServicesElement[vendor]: <eventId> текст

где:

level [*уровень*] – Представление в коде ASCII приоритета события, заключенного в угловых скобках, которое составляется как поразрядное ИЛИ [OR] Средства по умолчанию (128) и приоритета события (0-7). Результирующий уровень имеет диапазон между 128 и 135.

vendor [*поставщик*] – Название поставщика для сообщений SYSLOG, характерных для поставщика, или " CABLE" [кабель] для стандартных кабельных сообщений.

eventId [*идентификатор события*] – Представление в коде ASCII ЦЕЛОГО ЧИСЛА в десятичном формате, заключенного в угловых скобках, что однозначным образом определяет тип события. Этот объект EventID ОБЯЗАН быть тем же самым номером, что хранится в объекте docsDevEvId в docsDevEventTable. Для стандартных кабельных событий это число преобразуется из кода ошибки, используя следующие правила:

- Число является десятичным номером из восьми цифр;
- Первые две цифры (самые левые) являются кодом ASCII (десятичным) для буквы в коде Ошибки;
- Следующие четыре цифры заполняются 2 или 3 цифрами между буквой и точкой в коде Ошибки с нулевым заполнением в команде стирания в левой стороне;
- Последние две цифры заполняются числом после точки в коде Ошибки с нулевым заполнением в команде стирания слева.

Например, событие D04.2 преобразуется в 68000402, а событие I114.1 преобразуется в 73011401.

Пожалуйста, отметьте, что это представление использует только малую часть имеющегося номерного пространства, зарезервированного для Кабеля (от 0 до $2^{31} – 1$). Первая буква кода ошибки всегда находится на верхнем регистре.

текст – для стандартных кабельных сообщений эта строка ОБЯЗАНА иметь текстовое описание, как определено в Дополнении B.

Пример события syslog для события D04.2: "Время дня, полученное в недействительном формате":

<132>PS Element[CABLE]: <68000402> Time of the day received in invalid format.

Число 68000402 в данном примере является числом, назначенным этому конкретному событию.

6.5.2 Формат событий

Сообщения событий административного управления МОГУТ содержать любую из следующей информации:

- Счетчик событий – индикатор последовательности событий;
- Время события – время возникновения;
- Приоритет события – серьезность состояния. Документ [RFC 2669] определяет восемь уровней серьезности. Серьезность события по умолчанию может быть изменена на различное значение для каждого заданного события через интерфейс SNMP;
- Номер предметной области события – Этот номер определяет событие либо как стандартное событие, либо как событие, определенное поставщиком;
- Идентификатор ID события – определяет точное событие, когда оно сложено с номером предметной области события. Поставщики определяют свои собственные идентификаторы ID событий. Стандартные события административного управления определяются в Дополнении B. Каждому событию административного управления, описанному в дополнении, назначается идентификатор ID События;

- Текст события – описывает событие в человеческой читаемой форме;
- Адрес MAC – описывает адрес MAC устройства.

Точный формат этой информации для системных прерываний (захватов) и информирования определяется в Дополнении B. Формат для сообщения SYSLOG определяется в части требований в этом подразделе.

6.5.2.1 Приоритеты событий

Документ [RFC 2669] определяет 8 различных уровней приоритета и соответствующий механизм информирования для каждого уровня. Стандартные события, указанные в этом документе, используют эти уровни приоритетов.

1) Событие критического положения (приоритет 1)

   Зарезервировано для 'фатальных' аппаратных или программных ошибок, характерных для поставщика, которые препятствуют нормальному действию системы и заставляют информирующую систему осуществлять повторный начальный запуск. Каждый поставщик может определять свой собственный набор событий критического положения. Примерами таких событий могло бы быть 'буферы памяти недоступны', 'неудача испытания памяти' и пр.

2) Событие тревоги (приоритет 2)

   Серьезный отказ, который заставляет информирующую систему осуществить повторный начальный запуск, но повторный начальный запуск не вызывается неисправной работой аппаратной или программной частей. После восстановления из этого события система ОБЯЗАНА послать уведомление холодного/теплого запуска.

3) Критическое событие (приоритет 3)

   Серьезная неисправность, которая препятствует устройству передавать данные, но устройство может быть восстановлено без повторного начального запуска системы. После восстановления из критического события услуга PS ОБЯЗАНА послать уведомление Link Up [*звено работает*]. Примерами таких событий могли бы быть проблемы Файла конфигурации PS или неспособность получить адрес IP через протокол DHCP.

4) Событие ошибки (приоритет 4)

   Неисправность, которая могла бы прервать нормальный поток данных, но не заставляет устройство осуществлять повторную начальную загрузку. О событиях ошибок может быть сообщено в реальном времени, используя механизмы либо TRAP, либо SYSLOG.

5) Событие предупреждения (приоритет 5)

   Неисправность, которая могла бы прервать нормальный поток данных. Для этого уровня информирование Syslog и Trap отключено по умолчанию.

6) Событие извещения (приоритет 6)

   Важное событие, которое не является неисправностью, и о нем можно сообщить в реальном масштабе времени, используя механизмы либо TRAP, либо SYSLOG. Примерами событий NOTICE [*извещение*] являются 'Холодный запуск', 'Теплый запуск', 'Соединить' и 'успешное обновление программного обеспечения SW'.

7) Информационное событие (приоритет 7)

   Важное событие, которое не является неисправностью, но могло бы быть полезным для отслеживания нормального действия устройства.

8) Событие отладки (приоритет 8)

Зарезервировано для некритических событий, характерных для поставщика.

Приоритеты, связанные со стандартными событиями, ОБЯЗАНЫ НЕ изменяться.

Таблица 14 показывает типы уведомления по умолчанию для приоритетов различных событий. Услуга PS ОБЯЗАНА осуществлять типы уведомлений по умолчанию для восьми приоритетов событий. Например, тип уведомления по умолчанию для событий критического положения и тревоги необходимо поместить в местный журнал регистрации в качестве энергонезависимых записей.

Таблица 15 показывает минимальный уровень поддержки, требуемый для типов уведомлений для приоритетов различных событий. Например, услуга PS должна минимальным образом поддерживать энергонезависимые записи в местном журнале регистрации для приоритетов событий критического положения, тревоги и критического события. Услуга PS ОБЯЗАНА поддерживать минимальные требования для осуществления приоритетов событий для каждого типа информирования о событиях. Услуга PS МОЖЕТ выбирать информирование о приоритетах событий с большим количеством типов уведомлений, чем требуется в Таблице 15.

Таблица 14/J.191 – Типы уведомлений по умолчанию для приоритетов событий для PS

Приоритет события	**Местное энерго-независимое (бит-0)**	**Захват SNMP (бит-1)**	**SYSLOG (бит-2)**	**Местное энергозави-симое (бит-3)**	**Примечание**
1) Критическое положение	Да	Нет	Нет	Нет	Характерное для поставщика
2) Тревога	Да	Нет	Нет	Нет	Стандартное
3) Критическое событие	Да	Нет	Нет	Нет	Стандартное
4) Ошибка	Нет	Да	Да	Да	Стандартное
5) Предупреж-дение	Нет	Нет	Нет	Да	Стандартное
6) Извещение	Нет	Да	Да	Да	Стандартное
7) Информаци-онное событие	Нет	Нет	Нет	Нет	Стандартное и характерное для поставщика
8) Отладка	Нет	Нет	Нет	Нет	Характерное для поставщика

Таблица 15/J.191 – Минимальный уровень поддержки типа уведомления с помощью приоритета события в PS

Приоритет события	**Местное энергонезависмое (бит-0)**	**Захват SNMP (бит-1)**	**SYSLOG (бит-2)**	**Местное энергозави-симое (бит-3)**	**Примечание**
1) Критическое положение	Да	Да	Да	Да	Характерное для поставщика
2) Тревога	Да	Да	Да	Да	Стандартное
3) Критическое событие	Да	Да	Да	Да	Стандартное
4) Ошибка		Да	Да	Да	Стандартное

5) Предупреждение		Да	Да	Да	Стандартное
6) Извещение		Да	Да	Да	Стандарт
7) Информационное событие		Да	Да	Да	Стандарт и характерное для поставщика
8) Отладка		Да	Да	Да	Характерное для поставщика

6.5.2.2 Стандартные события

Услуга PS ОБЯЗАНА послать следующие общие захваты SNMP, как определено в документах [RFC 1907] и [RFC 2863]:

- coldStart [RFC 1907];
- linkUp [RFC 2863];
- linkDown [RFC 2863];
- Неудача установления подлинности SNMP [RFC 1907].

Услуга PS ОБЯЗАНА быть способна к порождению уведомлений о событиях на основе стандартных событий, перечисленных в Дополнении B.

6.5.3 Дросселирование и ограничение событий

Услуга PS ОБЯЗАНА поддерживать дросселирование и ограничение TRAP/INFORM и SYSLOG протокола SNMP, как описывается в документе [RFC 2669].

Услуга PS ОБЯЗАНА рассматривать события идентичными, если их идентификаторы EventId являются идентичными.

Документ [RFC 2669] указывает четыре состояния дросселирования:

- неограниченное(1) является причиной сообщений захватов (системных прерываний) и syslog, которые должны быть переданы безотносительно установок порогов;
- maintainBelowThreshold(2) является причиной сообщений передачи захватов и syslog, которые должны быть подавлены, если число захватов в противном случае превысило бы порог;
- stopAtThreshold(3) заставляет прекратить передачу захватов на пороге, и эта передача не возобновляется до тех пор, пока не будет получено указание сделать это;
- запрещенный(4) заставляет подавлять все сообщения передачи захвата и syslog.

Отдельное событие ОБЯЗАНО обрабатываться как отдельное событие для порогового подсчета, то есть, событие, заставляющее сообщение как захвата, так и syslog все еще обрабатываться как отдельные события.

7 Инструменты обеспечения

7.1 Введение/обзор

Элемент PS и Устройства IP сети LAN должны быть должным образом установлены в начальное состояние и конфигурированы, чтобы обмениваться значащей информацией друг с другом и с элементами, связанными с кабельной сетью и Интернетом. Инструменты обеспечения предоставляют средства для этого бесшовного установления в начальное состояние и конфигурации, и с минимальным вмешательством пользователя. Они также позволяют кабельным операторам добавлять ценность абонентам службы высокоскоростной передачи данных путем определения процессов, через которые кабельный оператор может

облегчить и настроить установление в начальное состояние и конфигурацию услуги PS и Устройства IP сети LAN. Определены три инструмента обеспечения, чтобы выполнить эту задачу, которые упомянуты ниже:

- Функция Кабельного портала DHCP (*CDP, Cable DHCP Portal*) в элементе PS;
- Инструмент оптовой конфигурации PS (*BPSC, Bulk PS Configuration*);
- Клиент Времени дня в элементе PS.

7.1.1 Режимы обеспечения

Поддерживаются два режима обеспечения. Они упоминаются как режим обеспечения DHCP (Режим DHCP) и режим обеспечения SNMP (Режим SNMP). Два режима обеспечения сравниваются в Таблице 16.

Таблица 16/J.191 – Режимы обеспечения

	Режим DHCP	**Режим SNMP**
Спусковое устройство Файла конфигурации PS	Запускается присутствием информации сервера TFTP в сообщении DHCP	Запускается системой NMS через сообщение SNMP
Требование Файла конфигурации PS	Требуется загрузка Файла конфигурации PS	Не требуется загрузка Файла конфигурации PS

Указанное поведение инструментов обеспечения зависит от режима обеспечения, в котором действует услуга PS.

Раздел 13 "Процессы обеспечения" описывает последовательность событий для каждого из двух режимов обеспечения.

7.1.2 Архиттектура обеспечения

Архитектура обеспечения иллюстрируется на Рисунке 14. Элементы PS будут взаимодействовать с функциями сервера в кабельной сети через интерфейс HFC, или с Устройствами IP сети LAN для удовлетворения руководящих принципов разработки системы, перечисленных в 7.2.1.

7.1.3 Цели

Цели Кабельного портала DHCP включают в себя:

- Назначать, через протокол DHCP, адреса IP Устройствам IP сети LAN согласно правилам, указанным в этом разделе;

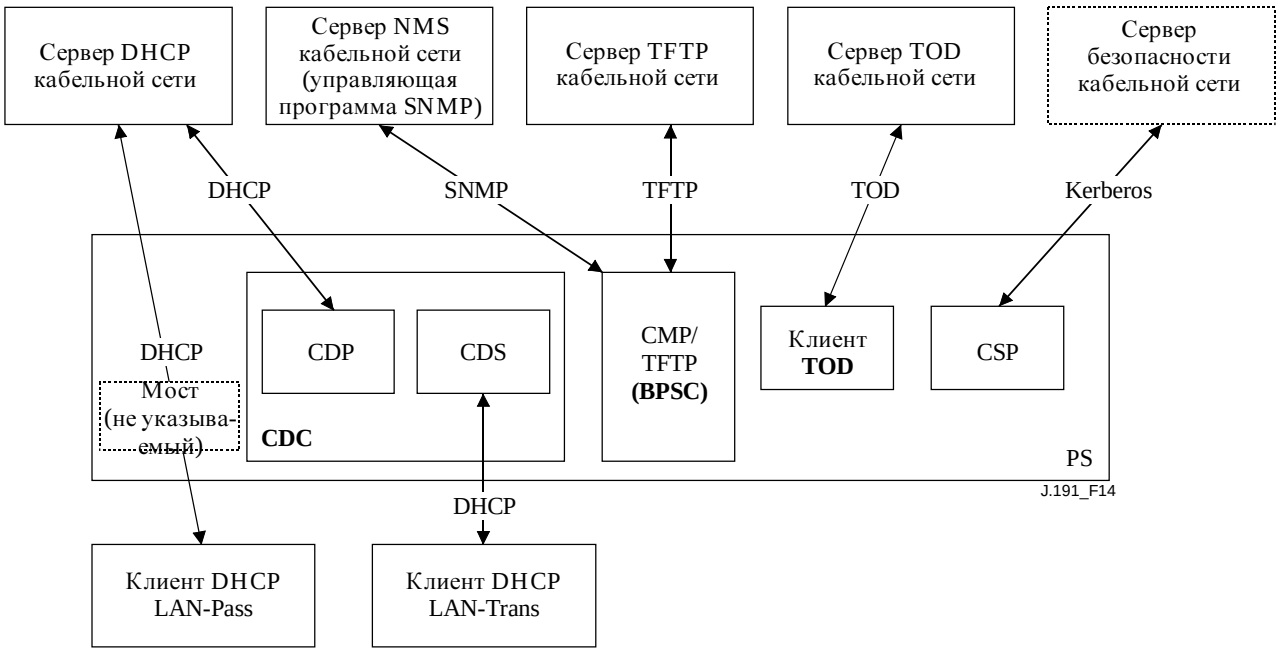


Рисунок 14/J.191 – Архитектура обеспечения

- Приобретать, через протокол DHCP, адреса IP для Интерфейсов WAN элемента PS согласно правилам, указанным в этом разделе.

Цели инструмента оптовой конфигурации услуг PS включают в себя:

- Загрузить из главной системы и обработать Файлы конфигурации.

Цели клиента Времени дня включают в себя:

- Синхронизировать тактовый генератор "Время дня" в элементе PS с таким генератором в сети Головного узла.

7.1.4 Предположения

Действующие предположения кабельного портала DHCP включают в себя:

1) Устройства IP сети LAN осуществляют клиента DHCP так, как определено документом [RFC 2131];

2) Система обеспечения кабельной сети осуществляет сервер DHCP так, как определено документом [RFC 2131];

3) Если сервер DHCP системы обеспечения кабельной сети поддерживает вариант выбора 61 протокола DHCP (вариант выбора идентификатора клиента), то интерфейсы IP WAN-Man и все интерфейсы IP WAN-Data IP могут совместно использовать общий адрес MAC;

4) Устройства IP сети LAN могут поддерживать различные варианты выбора DHCP и Расширения поставщика BOOTP, разрешенные документом [RFC 2132].

Действующие предположения инструмента Оптовой конфигурации услуги PS включают в себя:

– Оптовая конфигурация PS будет достигнута через загрузку из главной системы Файла конфигурации PS, содержащего один или более параметров.

Действующие предположения клиента "Время дня" включают в себя:

– Сервер головного узла DHCP будет предоставлять вариант выбора DHCP интерфейсу административного управления WAN, который указывает на сервер "Время дня", действующий внутри сети головного узла.

7.2 Архитектура кабельного портала DHCP

Кабельный портал (*CDP, Cable DHCP Portal*) является одним из трех инструментов обеспечения, введенных в 7.1. Этот раздел описывает руководящие принципы разработки системы, описание системы и требования, принадлежащие протоколу CDP.

7.2.1 Руководящие принципы разработки системы кабельного портала DHCP

Следующие руководящие принципы разработки в Таблице 17 управляют возможностями, определенными для портала CDP:

Таблица 17/J.191 – Руководящие принципы разработки системы CDP

Номер	Руководящие принципы разработки системы CDP
CDP 1	Механизмы адресации будут управляться оператором и будут предоставлять знание кабельного оператора об **Услуге портала** и Устройствах IP сети LAN и о возможности доступа к ним.
CDP 2	Процессы приобретения адреса и административного управления не будут требовать человеческого вмешательства (предполагая, что счет пользователя/семейства был уже установлен).
CDP 3	Процессы приобретения адреса и административного управления будут масштабируемыми для поддержки ожидаемого увеличения количества Устройств IP сети LAN.
CDP 4	Для адресов Устройств IP сети LAN предпочтительно оставаться теми же самыми после таких событий, как цикл питания или переключение поставщика услуги Интернет.
CDP 5	Будет обеспечен механизм, с помощью которого за Устройствами IP сети LAN в области LAN-Trans можно будет наблюдать, и ими можно будет управлять.
CDP 6	В доме связь будет продолжать работать, как обеспечено во время периодов выхода из строя адресного сервера Головного узла. Поддержка адресации будет обеспечена для вновь добавленных Устройств IP сети LAN и истечения адресов во время выходов из строя удаленных адресных серверов.
CDP 7	Адреса IP будут сохранены, когда это возможно (как глобально маршрутизируемые адреса, так и частные адреса административного управления кабельной сетью).

7.2.2 Описание системы кабельного портала DHCP

Кабельный портал DHCP (*CDP, Cable DHCP Portal*) является логическим объектом, который отвечает за деятельность адресации. Ответственности за запрос адреса и распределение адреса CDP включаю в себя:

- назначение адреса IP, техническое обслуживание адреса IP и доставку параметров конфигурации (через протокол DHCP) к Устройствам IP сети LAN в адресной области LAN-Trans;
- приобретение адресов IP WAN-Man и нуля или более адресов IP WAN-Data и параметров связанной конфигурации DHCP для элемента PS;

- обеспечение информации для Кабельного портала наименования (*CNP, Cable Naming Portal*) в поддержке услуг названия ведущего узла Устройства IP сети LAN.

Для своей роли в качестве маршрутизатора трафика в доме элемент PS требует Адрес IP (см. раздел 8, "Пакетная обработка и трансляция адреса"), сервера DHCP (CDS) и сервера DNS (см. раздел 9, Разрешающая способность имени). Для каждого из этих трех функций сервера и маршрутизатора Элементов услуги портала, адрес IP сети LAN сохраняется в базе данных PS. К каждому из них можно получить доступ через различные объекты MIB, которые перечисляются ниже и в Таблице 17.

– Адрес маршрутизатора (шлюз по умолчанию) cabhCdpServerRouter

– Адрес системы названий доменов (*DNS, Domain Name System*) cabhCdpServerDnsAddress

– Адрес Сервера динамической конфигурации ведущего узла (DHCP) (CDS) cabhCdpServerDhcpAddress

Значение по умолчанию объекта cabhCdpServerRouter есть 192.168.0.1. Значения по умолчанию объектов cabhCdpServerDnsAddress и cabhCdpServerDhcpAddress равны значению cabhCdpServerRouter.

Как показано на Рисунке 15, возможности портала CDP воплощены с помощью двух функциональных элементов, находящихся внутри портала CDP: Кабельный сервер DHCP *(CDS, Cable DHCP Server*) и Кабельный клиент DHCP (*CDC, Cable DHCP Client*).

Рисунок 15 также иллюстрирует взаимодействие между составными частями CDP и адресными областями, введенными в разделе 5. Клиент CDC обменивается сообщениями DHCP с сервером DHCP в кабельной сети (адресная область Административного управления сети WAN) для приобретения адреса IP и вариантов выбора DHCP для услуги PS, для целей технического обслуживания. Клиент CDC мог бы также обмениваться сообщениями DHCP с сервером DHCP в кабельной сети (адресная область Данных сети WAN) для приобретения нуля или более адресов IP по поручению Устройств IP сети LAN в области LAN-Trans. Сервер CDS обменивается сообщениями DHCP с Устройствами IP в сети LAN в области LAN-Trans и назначает частные адреса IP, разрешает аренду (владение адресом) и мог бы предоставлять варианты выбора DHCP клиентам протокола DHCP внутри таких Устройств IP сети LAN. Устройства IP сети LAN в области LAN-Pass получают свои адреса IP, аренду и варианты выбора DHCP непосредственно от сервера DHCP в кабельной сети. Портал CDP просто перемыкает сообщения DHCP между сервером DHCP в кабельной сети и Устройствами IP сети LAN в области LAN-Pass.

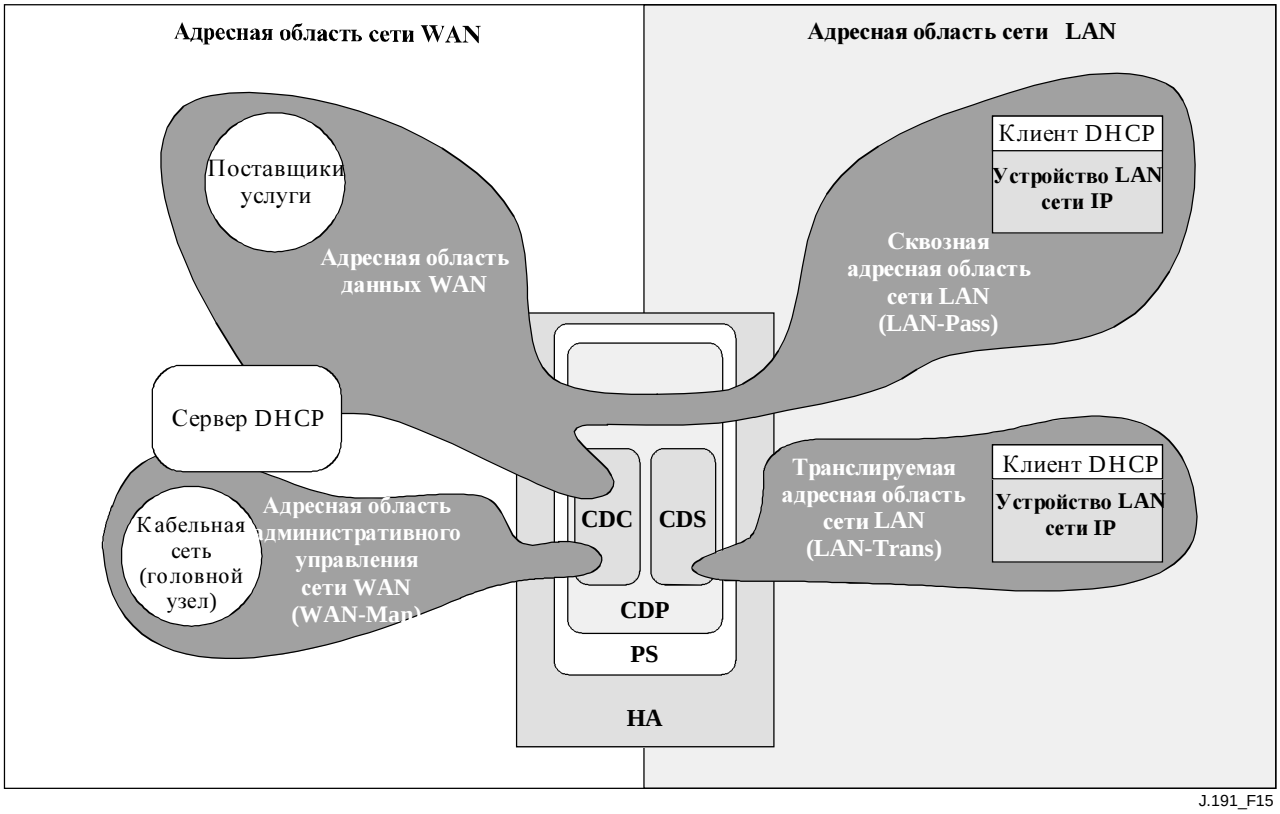


Рисунок 15/J.191 – Функции портала CDP

7.2.2.1 Описание системы CDS

Сервер CDS является стандартным сервером DHCP, как определено в документе [RFC 2131], и его ответственности включают в себя:

- Сервер CDS назначает адреса и доставляет параметры конфигурации DHCP Устройствам IP сети LAN, получающим адрес в адресной области LAN-Trans. Сервер CDS узнает варианты выбора DHCP от системы NMS и предоставляет эти варианты выбора DHCP Устройствам IP сети LAN. Если варианты выбора DHCP не были предоставлены системой NMS (например, когда услуга PS осуществляет начальный запуск из-за выхода кабеля из строя), сервер CDS для требуемых вариантов выбора полагается на встроенные значения по умолчанию (DefVals).
- Сервер CDS способен предоставлять услуги адресации DHCP Устройствам IP сети LAN независимо от состояния связности сети WAN.
- Количество адресов, поставляемых сервером CDS Устройствам IP сети LAN, контролируется с помощью системы NMS. Поведение сервера CDS, когда превышается предел, устанавливаемый кабельным оператором, также является конфигурируемым через систему NMS. Возможные действия сервера CDS, когда предел превышается, включают в себя:
  1) назначить адрес IP LAN-Trans и обрабатывать взаимное соединение CAT между сетями WAN и LAN, как это обычно имело бы место, если бы предел не был превышен; и
  2) не назначать адрес для запрашивающих устройств IP сети LAN.
- В отсутствие информации о времени дня от сервера "Время дня" (*TOD, Time of Day*), сервер CDS использует начальное время по умолчанию услуги PS в виде 0 (1 января 1900 года), обновляет Время истечения для любой активной аренды в области LAN-Trans для повторной синхронизации с клиентами DHCP в Устройствах IP сети LAN и

поддерживает аренды, основанные на такой начальной точке до тех пор, пока услуга PS синхронизируется с сервером "Время дня" в кабельной сети.

- При повторной начальной загрузке или переустановке PS сервер CDS остается пассивным до тех пор, пока не активирован услугой PS после успешной загрузки Файла конфигурации PS или через 5 неудачных попыток услугой PS осуществить загрузку Файла конфигурации PS, в зависимости от того, что случается первым. Сервер CDS тем самым предохраняется от предоставления аренды DHCP в области LAN-Trans, пока имелась разумная возможность для кабельного оператора обновлять такие параметры аренды LAN-Trans, как cabhCdpServerLeaseTime, cabhCdpLanPoolStart и cabhCdpLanPoolEnd.
- Если режим Первичной пакетной обработки PS (cabhCapPrimaryMode) был установлен в положение "Сквозной проход" [*Pass-through*], то тогда сервер CDS выключается.

Устройства IP сети LAN могут получать адреса, которые размещаются в области LAN-Pass. Как показано на Рисунке 15, запросы адресов LAN-Pass обслуживаются инфраструктурой адресации WAN, а не услугой PS. Процессы адресации LAN-Pass будут иметь место, когда услуга PS конфигурируется для работы в Сквозном режиме или Смешанном режиме Перемыкания/Маршрутизации (см. 8.2.2.2 для больших подробностей). В этих случаях взаимодействия DHCP будет иметь место непосредственно между Устройствами IP сети LAN и серверами Головных узлов, но эта Рекомендация не указывает процесс.

По тексту этой Рекомендации используются термины "Автоматическое распределение", "Динамическое распределение" и "Ручное распределение", как определено в документе [RFC 2131]. Автоматическое распределение адресов IP внутри адресной области LAN-Trans будет постоянным, и сервер CDS может повторно использовать Автоматические адреса, если все имеющиеся адреса были распределены. **Варианты выбора обеспеченного протокола DHCP сервера CDS**, объекты cabhCdpServer в базе MIB CDP используются сервером CDS для указания вариантов выбора DHCP, предлагаемых для устройств IP сети LAN, которым назначен адрес LAN-Trans. Варианты выбора обеспеченного протокола DHCP сервера CDS, объекты cabhCdpServer, сохраняются после цикла питания услуги PS, а система NMS может устанавливать, читать, записывать и исключать эти объекты. Варианты выбора обеспеченного протокола DHCP сервера CDS, объекты cabhCdpServer, сохраняются во время периодов выхода кабеля из строя, и эти объекты предлагаются устройствам IP сети LAN, которые назначили адрес LAN-Trans во время периодов выхода кабеля из строя. Постоянное хранение клиентом CDC вариантов выбора DHCP совместимо с документом [RFC 2131], секция 2.1. Определяются значения по умолчанию Вариантов выбора обеспеченного протокола DHCP сервера CDS, объекты cabhCdpServer (Таблица 17), и система NMS может переустанавливать Варианты выбора обеспеченного протокола DHCP сервера CDS, объекты cabhCdpServer, в их значения по умолчанию, путем записи в объект базы MIB cabhCdpSetToFactory.

Объекты **Адресного порога сервера CDS** (cabhCdpLanTrans) содержат параметры управления событиями, которые используются сервером CDS для того, чтобы сообщать порталу CMP о необходимости порождения уведомления к системе административного управления Головного узла, когда количество адресов LAN-Trans, назначенных сервером CDS, превышает предварительно установленный порог.

Объект "Подсчет адресов" (cabhCdpLanTransCurCount) является значением, указывающим количество адресов LAN-Trans, назначенных сервером CDS, что имеют активные аренды DHCP.

Объект "Адресный порог" (cabhCdpLanTransThreshold) является значением, указывающим, когда порождается уведомление к системе административного управления Головного узла. Уведомление порождается тогда, когда сервер CDS назначает адрес Устройству IP сети LAN,

что заставляет объект "Подсчет адресов" (cabhCdpLanTransCurCount) превышать объект "Адресный порог" (cabhCdpLanTransThreshold).

Объект "Действие превышенного порога" (cabhCdpLanTransAction) является действием, которое предпринимается сервером CDS в то время, когда объект "Подсчет адресов" (cabhCdpLanTransCurCount) превышает объект "Адресный порог" (cabhCdpLanTransThreshold). Если объект "Действие превышенного порога" (cabhCdpLanTransAction) разрешает адресные назначения после того, как подсчет превышается, то каждый раз, когда назначается адрес, порождается уведомление. Определенными акциями являются:

a) назначить адрес LAN-Trans как нормальный; и

b) не назначать адрес следующему запрашивающему Устройству IP сети LAN.

Подсчет адресов (cabhCdpLanTransCurCount) продолжается, чтобы обновиться во время периодов выхода кабеля из строя.

База MIB сервера CDS также содержит параметры "Начало адресного объединения ресурсов" (cabhCdpLanPoolStart) и "Окончание адресного объединения ресурсов" (cabhCdpLanPoolEnd). Эти параметры указывают диапазон адресов в области LAN-Trans, который может быть назначен сервером CDS для Устройств IP сети LAN.

Адресная таблица сети LAN портала CDP (cabhCdpLanAddrTable) содержит перечень параметров, связанных с адресами, которые распределены Устройствам IP сети LAN с адресами LAN-Trans. Эти параметры включают в себя:

1) Идентификаторы клиентов документа [RFC 2132], секция 9.14 (cabhCdpLanAddrClientID);

2) адрес IP сети LAN, назначенный клиенту (cabhCdpLanAddrIp);

3) индикацию, что адрес был распределен либо вручную (через портал CMP), либо автоматически (через портал CDP) (cabhCdpLanAddrConfig).

Сервер CDS использует адрес MAC для определения Устройств IP сети LAN.

Сервер CDS создает запись Таблицы CDP (cabhCdpLanAddrTable), когда он распределяет адрес IP Устройству IP сети LAN. Сервер CDS может создавать записи Таблицы CDP (cabhCdpLanAddrTable) во время периодов выходов кабеля из строя.

Таблица CDP (cabhCdpLanAddrTable) содержит время аренды DHCP для каждого Устройства IP сети LAN.

Записи Таблицы CDP, обеспеченные системой NMS (cabhCdpLanAddrTable), сохраняются во время периодов выхода кабеля из строя и сохраняются по циклам питания услуги PS.

7.2.2.2 Описание системы CDC

Клиент CDC является стандартным клиентом DHCP, как определено в документе [RFC 2131], а его ответственности включают в себя:

- Клиент CDC осуществляет запросы к серверам DHCP Головных узлов для приобретения адресов в WAN-Man и может осуществлять запросы к серверам DHCP Головных узлов для приобретения адресов в адресных областях WAN-Data. Клиент CDC также понимает ряд параметров Кабельной конфигурации DHCP и действует согласно им.
- Клиент CDC поддерживает приобретение одного адреса IP WAN-Man и нуля или более адресов IP WAN-Data.
- Клиент CDC поддерживает вариант выбора идентификатора класса поставщика (вариант 60 протокола DHCP), вариант выбора информации, характерной для

поставщика (вариант выбора 43 протокола DHCP), и вариант выбора идентификатора клиента (вариант 61 протокола DHCP).

- В случае по умолчанию клиент CDC будет приобретать отдельный адрес IP для одновременного использования интерфейсами IP WAN-Man и WAN-Data. Чтобы минимизировать изменения, необходимые для существующих серверов протокола DHCP Головных узлов, использование Идентификатора клиента (вариант выбора 61 протокола DHCP) клиентом CDC не требуется в этом случае по умолчанию.

Клиент CDP поддерживает различные варианты выбора DHCP и Расширения поставщика BOOTP, разрешенные документом [RFC 2132], как описывается в 7.2.2.2.1. "Варианты выбора Кабельных клиентов DHCP 60 и 43".

Вариант выбора идентификатора класса поставщика (вариант выбора 60 протокола DHCP) определяет особый класс устройства. Вариант выбора идентификатора класса поставщика будет содержать особую строку для определения логического элемента PS, всякий раз, когда клиент CDC запрашивает адрес WAN-Man или WAN-Data.

Вариант выбора информации, характерной для поставщика, (вариант выбора 43 протокола DHCP) далее определяет тип устройства и его возможности. Он описывает тип составной части, что осуществляет запрос, составные части, что содержатся в устройстве (модем CM, MTA, PS, etc.), порядковый номер устройства, а также позволяет конкретные параметры устройства.

Подробности требований для поддержки вариантов выбора 60 и 43 протокола DHCP находятся в Таблицах 19 и 20.

7.2.2.2.1 Вариант выбора 61 кабельного клиента DHCP

Элемент PS может иметь один или более адресов IP сети WAN, связанных с одним или более интерфейсами уровней звеньев (например, MAC). Поэтому клиент CDC не может полагаться только на адрес MAC как на уникальное значение идентификатора клиента.

Эта Рекомендация позволяет использование варианта выбора идентификатора клиента (вариант выбора 61 протокола DHCP), документ [RFC 2132], секция 9.14, чтобы единственным образом определять логический интерфейс WAN, связанный с конкретным адресом IP.

Для обеспечения совместимости с как можно большим количеством систем обеспечения кабельных операторов, клиент CDC будет поддерживать следующие конфигурируемые адресные режимы WAN:

Адресный режим 1 сети WAN: Элемент PS осуществляет использование единственного адреса IP сети WAN. Элемент PS имеет один Интерфейс WAN-Man и один Интерфейс IP WAN-Data, которые совместно используют общий Адрес MAC. Эти два Интерфейса совместно используют единственный, общий адрес IP. Это является фабричной конфигурацией элемента PS по умолчанию. Сервер DHCP головного узла кабельного оператора обычно не нуждается в изменениях программного обеспечения для поддержки этого режима обеспечения.

Адресный режим 2 сети WAN: Элемент PS осуществляет использование двух или более различных Адресов IP сети WAN. Элемент PS мог бы иметь один Интерфейс IP WAN-Man и один или более Интерфейсов IP WAN-Data, которые совместно используют общий Адрес MAC. Эти два или более Интерфейсов имели бы каждый свой собственный неразделенный адрес IP. Сервер DHCP Головного узла кабельного оператора может нуждаться в изменении программного обеспечения для поддержки назначения множественных Адресов IP единственному Адресу MAC. В этом режиме сервер DHCP Головного узла будет нуждаться в поддержке назначения IP, основанного на идентификаторе ID клиента (вариант выбора 61), а также Адреса MAC.

Адресный режим 2 сети WAN запускается путем записи уникальной строки идентификатора ID Клиента в записи cabhCdpWanDataAddrClientId из cabhCdpWanDataAddrTable баз MIB портала CDP, для каждого интерфейса WAN-Data, подлежащего использованию. Чтобы поддерживать этот режим обеспечения, кабельный оператор будет нуждаться в обеспечении (через систему NMS, файл конфигурации или ручную запись клиента через собственный интерфейс) элемента PS с уникальной строкой идентификатора ID Клиента для каждого Интерфейса IP WAN-Data.

7.2.3 Требования кабельного портала DHCP

7.2.3.1 Требования портала CDP

Ручное распределение адреса ОБЯЗАНО быть поддержано с использованием записей Таблицы CDP (cabhCdpLanAddrTable), созданных через систему NMS или файл конфигурации.

Записи Таблицы административного управления сети LAN для обеспечиваемого портала CDP (cabhCdpLanAddrTable) ОБЯЗАНЫ быть сохранены во время выхода кабеля из строя и ОБЯЗАНЫ сохраняться после цикла питания PS. Сервер CDS ОБЯЗАН быть способен обеспечивать услуги адресации DHCP для Устройств IP сети LAN вне зависимости от состояния связности сети WAN.

7.2.3.2 Требования сервера CDS

Поведение сервера CDS ОБЯЗАНО быть в соответствии с требованиями Сервера из документа [RFC 2131], секция 4.3.

Сервер CDS ОБЯЗАН поддерживать Автоматическое, Динамическое и Ручное распределение адресов в соответствии с документом [RFC 2131], секция 1.

При переустановке или начальном перезапуске услуги PS сервер CDS ОБЯЗАН НЕ обмениваться сообщениями DHCP с Устройствами IP сети LAN, пока сервер CDS не активируется услугой PS, следуя успешной загрузке Файла конфигурации PS, или следуя 5 последовательным неуспешным попыткам загрузки Файла конфигурации PS, в зависимости оттого, что является первым.

Сервер CDS ОБЯЗАН назначать адреса и доставлять параметры конфигурации DHCP только к Устройствам IP сети LAN, получающим адрес в адресной области LAN-Trans.

Автоматическое распределение адресов внутри адресной области LAN-Trans ОБЯЗАНО быть постоянным, а сервер CDS МОЖЕТ повторно использовать Автоматические адреса, если все имеющиеся адреса были распределены.

Сервер CDS ОБЯЗАН использовать аппаратный адрес (MAC) Устройств IP сети LAN в качестве значения идентификатора клиента.

Сервер CDS ОБЯЗАН поддерживать базу MIB портала CDP, включая все объекты в cabhCdpLanAddrTable, объекты cabhCdpLanPool, объекты cabhCdpServer и объекты cabhCdpLanTrans.

Сервер CDS ОБЯЗАН поддерживать варианты выбора DHCP, указанные как обязательные в колонке "Поддержка протокола CDS" из Таблицы 18.

Таблица 18/J.191 – Варианты выбора DHCP сервера CDS

Номер варианта выбора	Функция варианта выбора	Поддержка протокола CDS обязательная (M) или дополнительная (O)	Поддержка управления CDS обязательная (M) или дополнительная (O)	Фабричные значения по умолчанию CDS	Сохранение при выходе кабеля из строя CDS, Обязательное (M)	CDS, устойчивый к пропаданию питания, Обязательный (M)	Название объекта MIB
0	Заполнение	M	–	N/A[недоступное]	N/A	N/A	N/A
255	Конец	M	M	N/A	N/A	N/A	N/A
1	Маска подсети	M	M	255.255.255.0	M	M	cabhCdpServer SubnetMask
2	Смещение времени	M	O	O	N/A	N/A	cabhCdpServer TimeOffset
3	Вариант маршрутизатора	M	M	192.168.0.1	M	M	cabhCdpServer Router
6	Север названия домена	M	M	192.168.0.1	M	M	cabhCdpServer DnsAddress
7	Сервер регистрации	M	M	0.0.0.0	M	M	cabhCdpServer SyslogAddress
12	Название главного узла	M	O	N/A	N/A	N/A	N/A
15	Название домена	M	M	Нулевая строчка	M	M	cabhCdpServer DomainName
23	Время существования по умолчанию	M	M	255	M	M	cabhCdpServer TTL
26	Интерфейс MTU	M	M	1520	M	M	cabhCdpServer InterfaceMTU
43	Информация, характерная для поставщика	M	M	Выбирается поставщиком	M	M	cabhCdpServer VendorSpecific
50	Затребованный адрес IP	M	N/A	N/A	N/A	N/A	N/A
51	Время аренды адреса IP	M	M	60	M	M	cabhCdpServer LeaseTime
54	Идентификатор сервера	M	M	192.168.0.1	M	M	cabhCdpServer DhcpAddress
55	Перечень запроса параметров	M	N/A	N/A	N/A	N/A	N/A
60	Идентификатор класса поставщика	M	N/A	N/A	N/A	N/A	N/A
61	Идентификатор клиента	M	N/A	N/A	N/A	N/A	N/A

Сервер CDS ОБЯЗАН поддерживать обеспечение вариантов выбора NMS, указанных как Обязательные в колонке "Поддержка управления CDS" Таблицы 18.

Варианты выбора DHCP сервера CDS, указанные как Обязательные в колонке "Сохранение при выходе кабеля из строя CDS" Таблицы 18, ОБЯЗАНЫ быть сохранены в течение выхода из строя кабельной услуги.

Варианты выбора DHCP сервера CDS, указанные как Обязательные в колонке "CDS, устойчивый к пропаданию питания" Таблицы 18, ОБЯЗАНЫ сохраняться после цикла питания CDP.

Сервер CDS ОБЯЗАН поддерживать значения по умолчанию, указанные в колонке "Фабричные значения по умолчанию CDS" Таблицы 18, если вариант выбора DHCP не был обеспечен.

Если режим Первичной пакетной обработки PS (cabhCapPrimaryMode) был установлен в "Сквозной", то тогда сервер CDS ОБЯЗАН быть выключен.

В поддержке Автоматического распределения адресов сервер CDS ОБЯЗАН быть способен к созданию, изменению и исключению записей таблицы CDP для устройств, которым распределен адрес LAN-Trans.

Сервер CDS ОБЯЗАН поддерживать параметр "Подсчет адресов" (cabhCdpLanTransCurCount), указывая количество адресов LAN-Trans, назначенных устройствам IP сети LAN.

"Подсчет адресов" ОБЯЗАН увеличивать каждый раз аренду для предоставляемого адреса LAN-Trans Устройству IP сети LAN, и ОБЯЗАН снижать каждый раз, когда адрес LAN-Trans освобождается, или когда аренда адреса LAN-Trans истекает.

Сервер CDS ОБЯЗАН сравнивать параметр "Подсчет адресов" (cabhCdpLanTransCurCount) с параметром "Адресный порог" (cabhCdpLanTransThreshold) после назначения адреса LAN-Trans. Если параметр "Подсчет адресов" (cabhCdpLanTransCurCount) превышает параметр "Адресный порог" (cabhCdpLanTransThreshold), то ОБЯЗАНО быть порождено уведомление, как в случае соответствия механизму информирования о событии, определенному в 6.5. В то время как параметр "Подсчет адресов" (cabhCdpLanTransCurCount) превышает параметр "Адресный порог" (cabhCdpLanTransThreshold), сервер CDS ОБЯЗАН быть способен к следующим действиям при превышении порога для следующего сообщения DISCOVER [*обнаружить*] протокола DHCP из сети LAN: назначать адреса LAN-Trans как нормальные или не назначать адрес.

Особое действие, предпринимаемое сервером CDS, ОБЯЗАНО быть указано, как указывается обеспечиваемым параметром "Действие при превышении порога" (cabhCdpLanTransAction).

7.2.3.3 Требования клиента CDC

Поведение клиента CDC ОБЯЗАНО быть в соответствии требованиями Клиента из документа [RFC 2131].

Элемент PS ОБЯЗАН иметь аппаратный адрес интерфейса WAN, что отличен от кабельного модема.

Если портал CDC получает, в отклике DHCP [RFC 2131] от сервера DHCP в кабельной сети, действительный адрес IP в поле 'siaddr', И название действительного файла в поле 'file' [*файл*], И не получает под-вариант выбора 51 из варианта выбора 177 DHCP, услуга PS ОБЯЗАНА установить объект cabhPsDevProvMode в '1' (Режим DHCP).

Если портал CDC получает, от сервера DHCP в кабельной сети, действительный адрес IP для под-варианта выбора 51 из варианта выбора 177 DHCP, И не получает действительный адрес IP в поле 'siaddr', И не получает название действительного файла в поле 'file', то услуга PS ОБЯЗАНА установить объект cabhPsDevProvMode в '2' (Режим SNMP).

Если клиент CDC получает, в сообщении DHCP [RFC 2131] от сервера DHCP в кабельной сети, под-вариант выбора 51 из варианта выбора 177 DHCP, И действительный адрес IP в

поле 'siaddr', ИЛИ, если клиент CDC получает под-вариант выбора 51 из варианта выбора 177 DHCP, И название действительного файла в поле 'file', то услуга PS ОБЯЗАНА зарегистрировать ошибку в местном журнале регистрации и повторно передать циркулярным образом сообщение DISCOVER [*обнаружить*] протокола DHCP (т.е. повторно запустить последовательность обеспечения в случае этого недействительного состояния).

Если клиент CDC не получает под-вариант выбора 51 из варианта выбора 177 DHCP, И не получает действительный адрес IP в поле 'siaddr', И не получает название действительного файла в поле 'file', то услуга PS ОБЯЗАНА зарегистрировать ошибку в местном журнале регистрации и повторно передать циркулярным образом сообщение DISCOVER протокола DHCP (т.е. повторно запустить последовательность обеспечения в случае этого недействительного состояния).

Под-вариант выбора 11 варианта выбора 43 DHCP является параметром, зависящим от устройства. Он указывает, запрашивается ли адрес в Административном управлении сети WAN услуги PS, или в области WAN Data услуги PS. Таблица 19 указывает, как значения для под-варианта выбора 11 из варианта выбора 43 DHCP ОБЯЗАНЫ быть установлены для этих интерфейсов.

Таблица 19/J.191 – Значения под-варианта выбора 11 из варианта выбора 43 DHCP

Идентификатор Id элемента	Описание и комментарии
PS WAN-Man = 0x01	Определяет запрос для адреса области WAN-Man
PS WAN-Data = 0x02	Определяет запрос для адреса области WAN-Data

Клиент CDC ОБЯЗАН осуществлять Вариант выбора идентификатора класса поставщика (вариант выбора 60 DHCP), как указано в Таблице 20.

Кабельный модем и элемент PS каждый посылают отдельные запросы DHCP. Таблица 20 описывает, как клиент CDC ОБЯЗАН устанавливать содержание вариантов выбора 60 и 43 для услуги PS, когда запрашиваются отдельные адреса Административного управления сети WAN услуги PS и Данные сети WAN услуги PS.

Клиент CDC ОБЯЗАН поддерживать варианты выбора DHCP, указанные как обязательные в колонке "Поддержка протокола CDC" в Таблице 21.

Таблица 21 представляет варианты выбора DHCP, которые являются обязательными и дополнительными для клиента CDC, чтобы поддерживать их. Варианты выбора DHCP, перечисленные как обязательные в Таблице 21, ОБЯЗАНЫ быть включены в сообщения DISCOVER протокола DHCP и REQUEST [*запросить*] протокола DHCP, посланные клиентом CDC к серверу DHCP кабельной сети.

Услуга PS ОБЯЗАНА поддерживать Адрес объекта SNMP поставщика услуги (под-вариант выбора 3 варианта выбора 177 DHCP), конфигурированный в качестве адреса IPv4.

Всякий раз, когда первый интерфейс WAN-Data услуги PS не имеет текущей аренды DHCP, такой первый интерфейс WAN-Data услуги PS ОБЯЗАН устанавливать по умолчанию следующие параметры IP:

(Этот адрес IP используется для отображения сети WAN для Динамической трансляции NAPT кортежа. Этот адрес не может быть использован для отображения NAT, поскольку сторона WAN отображения NAT является устойчивой. Он также не может быть использован для Сквозных адресов, которые назначаются из адресного объединения ресурсов IP поставщика услуги.)

Таблица 20/J.191 – Варианты выбора DHCP для встроенных запросов адресов WAN-Man и WAN-Data услуги PS

Варианты выбора запросов DHCP	Значения	Описание
Запрос DHCP услуги PS для адреса административного управления сети WAN		
Вариант выбора 60 CPE	"PS"	
Под-вариант 1 из варианта выбора 43 CPE	вектор под-варианта выбора запроса	Перечень под-вариантов выбора (внутри варианта выбора 43), подлежащих возвращению сервером. Никакой не определен
Под-вариант12 из варианта выбора 43 CPE	"EPS"	Встроенная услуга PS
Под-вариант 3 из варианта выбора 43 CPE	"ECM:EPS"	Перечень встроенных устройств (Встроенный модем CM и встроенная услуга PS)
Под-вариант 4 из варианта выбора 43 CPE	например, "123456"	Порядковый номер устройства
Под-вариант 11 из варианта выбора 43 CPE	PS WAN-Man (0x01)	Определяет, что запрашивается адрес в области Административного управления сети WAN услуги PS
Запрос DHCP услуги PS для адреса WAN-Data		
Вариант выбора 60 CPE	"PS"	
Под-вариант 1 из варианта выбора 43 CPE	вектор под-варианта выбора запроса	Перечень под-вариантов выбора (внутри варианта выбора 43), подлежащих возвращению сервером. Никакой не определен
Под-вариант 2 из варианта выбора 43 CPE	"EPS"	Встроенная услуга PS
Под-вариант 3 из варианта выбора 43 CPE	"ECM:EPS"	Перечень встроенных устройств (Встроенный модем CM и встроенная услуга PS)
Под-вариант 4 из варианта выбора 43 CPE	например, "123456"	Порядковый номер устройства
Под-вариант 11 из варианта выбора 43 CPE	PS WAN-Data (0x02)	Определяет, что запрашивается адрес в области WAN-Data услуги PS

Адрес IP Административного управления: 192.168.100.5

Сетевая маска: 255.255.255.0

Шлюз по умолчанию: 192.168.100.1

Даже при использовании адреса IP WAN-Data по умолчанию 192.168.100.5, клиент CDC ОБЯЗАН продолжать производить сообщение DISCOVER протокола DHCP каждые 10 секунд, пока не предоставляется действительная аренда DHCP для такого интерфейса WAN-Data услуги PS (или интерфейса WAN-Man, если WAN-Man и WAN-data совместно используют один адрес IP).

Когда услуга PS для своего интерфейса WAN-Man приобретает адрес IP WAN-Man, клиент CDC ОБЯЗАН всегда вставлять свой аппаратный адрес сети WAN в поле идентификатора ID Клиента (вариант выбора 61 DHCP) в сообщении Discover протокола DHCP.

Таблица 21/J.191 – Варианты выбора DHCP клиента CDC

Номер варианта выбора	Функция варианта выбора	Поддержка протокола CDC, обязательная (M)
0	Заполнение	M
255	Окончание	M
1	Маска подсети	M
2	Вариант выбора смещения времени	M
3	Вариант выбора маршрутизатора	M
4	Вариант выбора сервера времени	M
6	Сервер названия домена	M
7	Сервер регистрации (syslog)	M
12	Название главного узла	M
15	Название домена	M
23	Время существования по умолчанию	M
26	Интерфейс MTU	M
43	Информация, характерная для поставщика	M
50	Запрашиваемый адрес IP	M
51	Время аренды адреса IP	M
54	Идентификатор сервера	M
55	Перечень запроса параметров	M
60	Идентификатор класса поставщика	M
61	Идентификатор клиента	M
177	Под-вариант выбора 3 – Адрес объекта SNMP поставщика услуги	M
177	Под-вариант выбора 51 – Адрес IP сервера Kerberos	M

Когда услуга PS, действующая в Адресном режиме 2 сети WAN (как описано в 7.2.2.2), приобретает адрес IP WAN-Data для интерфейса WAN-Data, который будет использовать адрес IP отличающимся способом от интерфейса WAN-Man, клиент CDC ОБЯЗАН включать вариант выбора Идентификатора клиента (cabhCdpWanDataAddrClientId) в сообщение Discover протокола DHCP. Чтобы обеспечивать эти уникальные идентификаторы ID Клиента Wan-Data, клиент CDC ОБЯЗАН дать возможность системе NMS создавать записи cabhCdpWanDataAddrClientId в объекте cabhCdpWanDataAddrTable.

Если услуга PS действует в Адресном режиме 2 сети WAN (как описывается в 7.2.2.2), клиент CDC ОБЯЗАН попытаться получить адрес IP, через протокол DHCP, для каждого уникального идентификатора ID клиента (cabhCdpWanDataAddrClientId) в объекте cabhCdpWanDataAddrTable.

Клиент CDC ОБЯЗАН продолжать осуществлять вещательную передачу своего сообщения DISCOVER протокола DHCP (в соответствии с документом [RFC 2131]), пока он не получит адрес и ACK [*подтверждение*] протокола DHCP. Конкретная выдержка времени для доступа сервера DHCP является зависимой от осуществления. Однако клиент CDC ОБЯЗАН НЕ осуществлять вещательную передачу сообщения DISCOVER протокола DHCP более 3 раз в любом 30-секундном периоде. Как минимум, клиент CDC ОБЯЗАН осуществлять вещательную передачу сообщения DISCOVER протокола DHCP, по меньшей мере, один раз на 30-секундный интервал, пока он успешно не приобретет адрес.

Если клиент CDC не получает сообщение OFFER [*предложение*] протокола DHCP после 5 попыток осуществить вещательную передачу сообщения DISCOVER протокола DHCP, услуга PS ОБЯЗАНА инициировать операцию сервера CDS таким образом, чтобы Устройства IP сети LAN в области LAN-Trans можно было обслуживать с помощью адресов IP.

7.3 Архитектура оптовой конфигурации PS

7.3.1 Руководящие принципы разработки системы оптовой конфигурации PS

Следующие руководящие принципы разработки системы в Таблице 22 продвигают возможности, определенные для инструмента Оптовой конфигурации PS:

Таблица 22/J.191 – Руководящие принципы разработки системы оптовой конфигурации PS

Номер	Руководящие принципы разработки системы оптовой конфигурации PS (BPSC)
BPSC 1	Необходимо предоставить механизм, с помощью которого услуга PS может загружать и обрабатывать Файлы конфигурации.

7.3.2 Описание системы оптовой конфигурации PS

Оптовая конфигурация услуги PS обычно выполняется во время обеспечения элемента PS, путем обработки установок конфигурации, содержащихся внутри Файла конфигурации. Однако эта обработка может быть инициирована в любое время. Инструмент оптовой конфигурации услуги PS состоит из следующих составных частей:

Формат Файла конфигурации:

1) режимы запуска процесса загрузки;
2) средства установления подлинности файла;
3) средства для информирования в обратном направлении о статусе загрузки Файла конфигурации PS и другие соображения.

Оптовая конфигурация услуги PS (*BPSC, Bulk PS Configuration*) является инструментом, который операторы могут использовать для изменения установок конфигурации PS оптом, через Файл конфигурации. Обычно Файл конфигурации будет содержать множество установок, поскольку первоначальная полезность, предоставляемая использованием Файлов конфигурации, является способностью изменять ряд установок конфигурации при минимальном вмешательстве кабельного оператора.

Процесс оптовой конфигурации услуги PS может вести себя точно так же, как последовательные установки SNMP, выполняемые оператором вручную. Файл конфигурации является инструментом, предназначенным для того, чтобы сделать операторов более производительными и осуществлять большие изменения конфигурации при меньшей зависимости от ошибок.

Важно отметить, что услуга PS не нуждается в том, чтобы Файл конфигурации был нагружен раньше, чем она может действовать. Ожидается, что услуга PS будет устанавливать себя в известное состояние, и услуга PS могла бы выполняться во время существования, не имея загруженного Файла конфигурации. Однако услуга PS будет получать и обрабатывать Файл конфигурации, когда он предоставляется.

Загрузка Файла конфигурации средств межсетевой защиты использует аналогичную процедуру, как загрузка параметра "Оптовая конфигурация услуги PS". Для описания процедуры "Загрузка файла конфигурации средств межсетевой защиты" можно сослаться на 11.3.5.2.

7.3.3 Требования оптовой конфигурации PS

7.3.3.1 Требования формата Файла конфигурации

Данные конфигурации услуги PS ОБЯЗАНЫ содержаться в файле, который загружается из главной системы через протокол TFTP. Файл конфигурации PS ОБЯЗАН состоять из ряда

установок конфигурации (1 на каждый параметр), каждая из формы "Тип-Длина-Значение" (*TLV, Type-Length-Value*). Определения этих терминов предоставляются в Таблице 23.

Таблица 23/J.191 – Определения TLV

Тип	Идентификатор из единственного октета, который определяет параметр
Длина	Один или более октетов, указывающих длину поля "Значение" (не включая поля "Тип" и "Длина")
Значение	Набор октетов "Длина" в течение долгого времени, содержащий конкретное значение для параметра

Установки конфигурации ОБЯЗАНЫ следовать одна за другой непосредственно в файле, который является потоком октетов (без маркеров записи). Длина файла ОБЯЗАНА быть заполнена до целого числа 32-разрядных слов. См. 7.3.3.1.1 для определения заполнения. Установки конфигурации разделяются на три типа:

- стандартные установки Конфигурации, которые должны присутствовать;
- дополнительные или необязательные установки конфигурации, которые МОГУТ присутствовать;
- установки конфигурации, характерные для поставщика.

Файл конфигурации PS МОЖЕТ содержать множество различных параметров, но единственным параметром, который ОБЯЗАН быть включен в любой Файл конфигурации PS, является "Маркер окончания данных" (Тип 255).

Чтобы позволить единообразное административное управление IP-усовершенствованных Кабельных модемов, соответствующих этой Рекомендации, соответствующие Устройства ОБЯЗАНЫ поддерживать Файл конфигурации, который имеет длину до 64 кбайт.

Каждый элемент PS ОБЯЗАН поддерживать, а Файл конфигурации PS МОЖЕТ включать в себя Типы 0, 4, 9, 17, 21, 28, 32, 33 и 255 параметра конфигурации, которые описываются в этом разделе.

Размер значения поля "Длина" для любого параметра конфигурации, включенного в Файл конфигурации PS, ОБЯЗАН быть 2 октета.

Значение "Длина" для каждого Типа, описанного в пунктах с 7.3.3.1.1 по 7.3.3.1.10, является фактической длиной в октетах поля "Значение".

7.3.3.1.1 Установка конфигурации заполнения

Это не имеет полей "Длина" или "Значение" и используется только после маркера окончания данных, чтобы заполнить файл до целого числа 32-разрядных слов.

Тип	Длина	Значение
0	–	–

7.3.3.1.2 Открытый ключ RSA

Этот Атрибут является атрибутом строки, содержащим DER-кодированный RSAPublicKey ASN.1 тип, как определено в Стандарте шифрования RSA PKCS #1 v2.0 [RSA1].

PKCS #1 v2.0 указывает, что открытый ключ RSA состоит как из открытого модуля RSA, так и открытого представителя RSA; тип RSAPublicKey включает оба из этих объектов в качестве DER-кодированных типов ЦЕЛЫХ ЧИСЕЛ.

PKCS #1 v2.0 устанавливает, что открытый представитель RSA может быть стандартизован в особых спецификациях, и документ предлагает значения 3 или 65537 (F4). Эта Рекомендация требует F4 для открытого представителя и использует 2048-разрядный модуль.

Тип	Длина	Значение
4	106, 140 или 270[a)]	DER-кодированный RSAPublicKey ASN.1 Тип
[a)] Длина DER-кодирования, используя соответственно F4 в качестве открытого представителя и 2048-разрядный открытый модуль.		

7.3.3.1.3 Имя файла обновления программного обеспечения

Имя файла обновления программного обеспечения для услуги PS. Имя файла полностью определяется названием "директория-тракт". Ожидается, что файл должен находиться на сервере TFTP, указанном в варианте выбора установки конфигурации.

Тип	Длина	Значение
9	Переменная [a)]	имя файла
[a)] Длина ОБЯЗАНА НЕ быть причиной превышения сообщением административного управления MAC максимально разрешенного размера.		

7.3.3.1.4 Управление доступом для записи SNMP

Этот объект делает возможным выключение доступа "Set" [*установить*] протокола SNMP к индивидуальным объектам MIB. Каждый экземпляр этого объекта управляет доступом ко всем способным для записи объектам MIB, чьи префиксы "Идентификатор объекта" (*OID, Object Identifier*) совпадают. Этот объект может быть повторен для выключения доступа к любому количеству объектов MIB.

Тип	Длина	Значение
10	n	Префикс OID плюс флаг управления

Где "n" есть размер кодирования префикса OID Рекомендации МСЭ-Т X.690 по Основным правилам кодирования ASN.1 плюс один байт для флага управления.

Флаг управления может принимать следующие значения:

– 0 Разрешить доступ для записи;

– 1 Отключить доступ для записи.

Может быть использован любой префикс OID. Может быть использован Нулевой идентификатор OID 0.0 для управления доступом ко всем объектам MIB (Идентификатор OID 1.3.6.1 будет иметь то же самое воздействие.)

Когда присутствуют и перекрываются повторяющиеся экземпляры этого объекта, имеет превосходство самый длинный (наиболее конкретный) префикс.

Таким образом, одним примером могло бы быть:

– someTable не разрешает доступ для записи;

– someTable.1.3 разрешает доступ для записи.

Этот пример не разрешает доступ ко всем объектам в someTable, кроме someTable.1.3.

7.3.3.1.5 CA-Сертификат

Этот Атрибут является атрибутом строки, содержащим Сертификат CA X.509, как определено в Рекомендации МСЭ-Т X.509.

Тип	Длина	Значение
17	Переменная величина [a)]	Сертификат CA X.509 (DER-кодированный ASN.1)
[a)] Длина ОБЯЗАНА НЕ быть причиной для превышения сообщением административного управления MAC максимально разрешенного размера.		

7.3.3.1.6 Сервер TFTP обновления программного обеспечения

Адрес IP сервера TFTP, на котором располагается файл обновления программного обеспечения для услуги PS.

Тип	Длина	Значение
21	4	ip1, ip2, ip3, ip4

7.3.3.1.7 Объект MIB протокола SNMP с расширенной длиной

Этот объект разрешает произвольным объектам MIB протокола SNMP устанавливаться через процесс TFTP-Регистрация, где значение есть связывание переменной величины SNMP (VarBind), как определено в документе [RFC 1157]. VarBind кодируется согласно Основным правилам кодирования ASN.1 так же, как если бы она была частью запроса Set протокола SNMP.

Тип	Длина	Значение
28	Переменная [a)]	связывание переменной
[a)] Длина ОБЯЗАНА НЕ быть причиной для превышения сообщением административного управления MAC максимально разрешенного размера.		

Услуга PS ОБЯЗАНА обрабатывать связывание переменной, в Типе 28 TLV, как если бы оно было частью запроса Set протокола SNMP со следующими предостережениями:

- Она ОБЯЗАНА обрабатывать запрос как полностью санкционированный (она не может отклонить запрос из-за недостатка преимущества);
- Положения "Управление записью" SNMP не применяются (см. предыдущее предложение);
- Услугой PS не порождается отклик SNMP;
- Этот объект МОЖЕТ повторяться с различными VarBinds, чтобы "Установить" ряд объектов MIB. Все Установки SNMP в Файле конфигурации ОБЯЗАНЫ обрабатываться как одновременные. Каждое VarBind ОБЯЗАНО быть ограничено до 65535 байтов.

7.3.3.1.8 Сертификат проверки кода производителя

Сертификат проверки кода производителя (*M-CVC, Manufacturer's Code Verification Certificate*) для Безопасной загрузки программного обеспечения. Файл конфигурации PS ОБЯЗАН содержать сертификат M-CVC и/или C-CVC, чтобы разрешить устройству загрузить файл кода из сервера TFTP.

Тип	Длина	Значение
32	Переменная	Сертификат CVC производителя (DER-кодированный ASN.1)

Если длина кода M-CVC превышает 65 535 байтов, то M-CVC ОБЯЗАНО быть разбито на два или более последовательных элементов Типа 32. Каждый фрагмент, кроме последнего, ОБЯЗАН быть длиной в 65 535 байтов. Услуга PS перестраивает M-CVC путем сцепки содержимого (Значение TLV) последовательных элементов Типа 32 в порядке, в котором они появляются в Файле конфигурации. Например, первый байт, сопровождающий поле длины второго элемента Типа 32, обрабатывается так, как если бы он сразу же сопровождал последний байт первого элемента Типа 32.

7.3.3.1.9 Сертификат проверки кода совместно подписавшейся стороны

Сертификат проверки кода совместно подписавшейся стороны (*C-CVC, Co-signer's Code Verification Certificate*) для Безопасной загрузки программного обеспечения. Файл конфигурации PS ОБЯЗАН содержать сертификат C-CVC и/или M-CVC, чтобы разрешать устройству загружать файл кода из сервера TFTP.

Тип	Длина	Значение
33	Переменная	Сертификат CVC совместно подписавшейся стороны (DER-кодирован ASN.1)

Если длина сертификата C-CVC превышает 65 535 байтов, то C-CVC ОБЯЗАН быть разбит на два или более последовательных элементов Типа 33. Каждый фрагмент, кроме последнего, ОБЯЗАН быть длиной 65 535 байтов. Услуга PS перестраивает C-CVC путем сцепки содержимого (Значение TLV) последовательных элементов Типа 33 в порядке, в котором они появляются в Файле конфигурации. Например, первый байт, сопровождающий поле длины второго элемента Типа 33, обрабатывается так, как если бы он сразу же сопровождал последний байт первого элемента Типа 33.

7.3.3.1.10 Значение толчкового запуска SNMPv3

Подчиняющиеся элементы PS ОБЯЗАНЫ понимать следующее значение TLV и его под-элементы, а также должны быть способны осуществлять толчковый запуск доступа SNMPv3 к услуге PS вне зависимости от того, действует ли услуга PS в режиме NmAccess или в режиме Сосуществования (см. 6.3.3 и 6.3.6).

Тип	Длина	Значение
34	n	Составное

В Файл конфигурации могут быть включены до 5 этих объектов. Каждые результаты в дополнительном ряду добавляется к объектам usmDHKickstartTable и usmUserTable, а результаты для этих рядов порождаются в открытом номере агента.

7.3.3.1.10.1 Название безопасности толчкового запуска SNMPv3

Тип	Длина	Значение
34.1	2-16	Название безопасности, кодированное согласно UTF8

Для набора знаков ASCII, кодирования UTF8 и ASCII являются идентичными. Обычно это будет указано как один из встроенных пользователей USM спецификации DOCSIS, например, "docsisManager," "docsisOperator," "docsisMonitor," "docsisUser."

Название безопасности НЕ завершается нулем. Об этом сообщается в объекте usmDHKickStartTable как usmDHKickStartSecurityName и в объекте usmUserTable как usmUserName и usmUserSecurityName.

7.3.3.1.10.2 Открытый номер управляющей программы толчкового запуска SNMPv3

Тип	Длина	Значение
34.2	n	Открытое число Диффи-Хеллмана управляющей программы, выраженное как строка октета.

Это число является открытым числом Диффи-Хеллмана, извлеченным из случайного числа, порожденного секретным образом (управляющей программой или оператором), и преобразованного согласно документу [RFC 2786]. О нем сообщается в объекте usmDHKickStartTable как usmKickstartMgrPublic. Будучи сложенным с объектом, о котором сообщают в том же самом ряду как о usmKickstartMyPublic, оно может быть использовано для извлечения ключей в связанном ряду в usmUserTable.

7.3.3.1.11 Элемент файла конфигурации – Приемник docsisV3Notification

Тип	Длина	Значение
38	Переменная величина	(См. ниже.)

Этот элемент Файла конфигурации PS указывает Станцию сетевого административного управления, которая будет получать уведомления от услуги PS, когда она находится в режиме сетевого административного управления "Сосуществование". В Файл конфигурации PS могут быть включены до 10 этих элементов.

Вот формат этого элемента:

Определение поля элемента docsisV3NotificationReceiver;

Все поля из множества байтов имеют байты наибольшего значения первыми в этом поле.

Это значение TLV (38) состоит из нескольких под-значений TLV внутри элемента Файла конфигурации TLV:

Под-значение TLV 38.1 – Адрес IP приемника захвата, в двоичной форме

Адрес IP из 4 байтов Адреса IP для приемника захвата, в двоичной форме.

Под-значение TLV 38.2 – Номер порта UDP приемника захвата, в двоичной форме

Номер Порта UDP байтов Порта 2 приемника захвата, в двоичной форме.

(Если отсутствует, то используется значение по умолчанию 162)

Под-значение TLV 38.3 – Тип захвата, посланный услугой PS (Примечание 2)

2 байта типа захвата

1 = захват SNMP v1 в пакете SNMP v1;

2 = захват SNMP v2c в пакете SNMP v2c;

3 = информирование SNMP в пакете SNMP v2c;

4 = захват SNMP v2c в пакете SNMP v3;

5 = информирование SNMP в пакете SNMP v3.

Под-значение TLV 38.4 – Выдержка времени, в миллисекундах, используемая для отправки информирования

2 байта выдержки времени 0-65535.

Под-значение TLV 38.5 – Количество повторных попыток при отправке информирования, после отправки информирования первый раз.

2 байта повторных попыток 0-65535.

Под-значение TLV 38.6 – Параметры фильтрации уведомления

Если это под-значение TLV отсутствует, то приемник уведомления будет получать все уведомления, порождаемые агентом SNMP.

Отфильтровать Идентификатор объекта, форматированный согласно ASN.1 OID, из значения snmpTrapOID, что указывает об уведомлениях, подлежащих отправке к приемнику уведомления. Будут посланы это уведомление и все уведомления ниже его. Объект <z> есть длина, в байтах, кодирования ASN.1. Это поле начинается с байта Универсального типа 6 ASN.1 (Идентификатор объекта), затем следует поле длины ASN.1, затем составные части идентификатора кодированного объекта ASN.1.

Под-значение TLV 38.7 – Название безопасности для использования при отправке Уведомления SNMP V3

Это под-значение TLV не требуется для типа "Захват" = 1, 2 или 3 выше. Если оно не поставляется для типа "Захват" 4 или 5, тогда будет послано уведомление V3 в уровне безопасности noAuthNoPriv, используя название безопасности "@config" (Примечание 2).

SecurityName

Название безопасности V3 для использования при отправке Уведомления V3. Используется только в том случае, если тип "Захват" установлен в 4 или 5. Это название должно быть названием, указанным в Типе 34 TLV Файла конфигурации в качестве процедуры Толчкового запуска DH. Будет послано уведомление, используя Ключи установления подлинности и секретности, вычисленные услугой PS во время процедуры Толчкового запуска DH.

ПРИМЕЧАНИЕ 1 – При получении одного из этих элементов TLV, услуга PS ОБЯЗАНА осуществить записи к следующим таблицам, чтобы вызвать передачу желаемого захвата: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable и vacmViewTreeFamilyTable.

ПРИМЕЧАНИЕ 2 – Тип захвата: Строка сообщества для захватов в пакетах V1 и V2 протокола SNMP ОБЯЗАНА быть "public" [*открытая*]. Название безопасности в захватах и информированиях в пакетах V3 протокола SNMP, где безопасное название не было указано, ДОЛЖНО быть "@config", и в таком случае уровень безопасности ДОЛЖЕН быть be noAuthNoPriv.

ПРИМЕЧАНИЕ 3 – Фильтр OID: V3 протокола SNMP разрешает спецификацию, какие из идентификаторов OID Захвата должны быть посланы к приемнику захвата. Фильтр OID в элементе config указывает идентификатор OID корня под-дерева фильтра захвата. Все Захваты с идентификатором OID Захвата, содержащиеся в этом под-дереве фильтра захвата, ДОЛЖНЫ быть посланы приемнику захвата.

ПРИМЕЧАНИЕ 4 – Номер TLV файла config: Поле типа этого TLV ДОЛЖНО быть (38).

ПРИМЕЧАНИЕ 5 – Файл конфигурации PS МОЖЕТ также содержать элементы MIB TLV, которые осуществляют записи к любой из 10 таблиц, перечисленных в Примечании 1. Эти элементы MIB TLV НЕ ДОЛЖНЫ использовать колонки индексов, что начинаются знаками "@config".

ПРИМЕЧАНИЕ 6 – Этот элемент TLV ДОЛЖЕН быть обработан только в том случае, если услуга PS ввела режим Сосуществования V3 протокола SNMP во время обработки Файла конфигурации PS.

7.3.3.1.12 Маркер "Окончание данных"

Это специальный маркер для окончания данных. Он не имеет полей "Длина" или "Значение".

Тип	Длина	Значение
255	–	–

7.3.3.2 Режим запуска

Перенос файла конфигурации, от сервера TFTP в сети Головного узла к элементу PS, инициируется событием, упоминаемым как спусковое устройство. Требования для запуска переноса Файла конфигурации PS от сервера TFTP к услуге PS являются следующими.

Режим запуска загрузки Файла конфигурации PS зависит от Режима обеспечения, в котором действует услуга PS. Портал The CMP ОБЯЗАН читать значение cabhPsDevProvMode (см. 7.2.3.3) перед инициацией любой загрузки Файла конфигурации PS.

Спусковое устройство загрузки Файла конфигурации PS для Режима обеспечения DHCP:

Если услуга PS получает адрес сервера TFTP в поле 'siaddr' и название Файла конфигурации PS в поле 'file' из сообщения OFFER протокола DHCP, услуга PS ОБЯЗАНА объединить адрес сервера TFTP и название Файла конфигурации P, чтобы сформировать URL-кодированное значение и записать такое значение в объекте cabhPsDevProvConfigFile. Случайные данные Конфигурации PS, прибавленные к названию Файла конфигурации PS НЕ ОБЯЗАНЫ быть включены в URL-кодированное значение.

Загрузка Файла конфигурации PS услугой PS, действующей в режиме обеспечения DHCP, запускается путем присутствия местоположения Файла конфигурации PS (адрес IP сервера TFTP) и названия в сообщении DHCP, выпущенного к услуге PS (CDC) с помощью сервера DHCP в кабельной сети. Можно сослаться на 7.2.3.3.

Если услуга PS действует в режиме обеспечения DHCP (как указано значением cabhPsDevProvMode), после того, как услуга PS (CDC) получает DHCPACK от сервера DHCP в кабельной сети, услуга PS ОБЯЗАНА выпустить запрос Get [*получить*] протокола TFTP к серверу, указанному в поле 'siaddr' сообщения DHCP для загрузки файла, указанного в поле 'file' сообщения DHCP.

Спусковое устройство для загрузки из главной системы Файла конфигурации PS для Режима обеспечения SNMP:

Если услуга PS действует в режиме обеспечения SNMP (как указывается значением cabhPsDevProvMode), загрузка Файла конфигурации PS ОБЯЗАНА НЕ происходить до завершения процесса удостоверения подлинности SNMP v3 (ссылка на раздел 11 "Безопасность" для подробностей относительно процесса удостоверения подлинности SNMP).

Если услуга PS действует в режиме обеспечения SNMP (как указывается значением cabhPsDevProvMode), элемент PS ОБЯЗАН НЕ инициировать загрузку Файла конфигурации PS, если действительное значение для объекта cabhPsDevProvConfigHash (PSDev MIB) не было обеспечено системой NMS.

Если услуга PS действует в Режиме обеспечения SNMP (как указывается значением cabhPsDevProvMode), И объект cabhPsDevProvConfigHash из базы MIB PSDev имеет действительное значение, загрузка Файла конфигурации PS ОБЯЗАНА быть запущена тогда, когда сообщение Set-Request протокола SNMP, адресованное интерфейсу WAN-Man услуги PS, содержит действительное значение для объекта MIB PSDev cabhPsDevProvConfigFile. Формат cabhPsDevProvConfigFile ОБЯЗАН быть URL-кодированным адресом IP сервера TFTP и названием файла конфигурации.

Операция после запуска:

Будучи запущенной, услуга PS ОБЯЗАНА использовать клиента TFTP, соответствующего документу [RFC 1350], чтобы загружать Файлы конфигурации PS.

Если Файл конфигурации PS должным образом заверен, когда загрузка TFTP Файла конфигурации PS завершена, услуга PS ОБЯЗАНА обработать значения TLV, содержащиеся внутри файла. Можно сослаться на 6.3.9 для описания того, как портал CMP обрабатывает Файл конфигурации.

7.3.3.3 Средства проверки подлинности Файла конфигурации PS

Этот раздел определяет процедуру для проверки подлинности Файла конфигурации PS.

Для проверки подлинности Файла конфигурации PS используется вычисление случайных данных. Система NMS вычисляет случайные данные Файла конфигурации PS и затем посылает результирующее значение случайных данных к элементу PS. Подлинность системы NMS, что породила Файл конфигурации PS, удостоверяется путем сравнения случайных данных Файла конфигурации PS, что был порожден системой NMS и транспортирован к элементу PS, в сравнении со случайными данными (вычисленными услугой PS) на Файле конфигурации PS, загруженном из сервера TFTP. Подлинность элемента PS, запрашивающего файл, не требуется.

Алгоритм безопасности, используемый для проверки подлинности Файла конфигурации PS, зависит от режима обеспечения элемента PS (см. 5.7). Имеются два типа режимов обеспечения: режим обеспечения DHCP и режим обеспечения SNMP. Следующие далее подразделы описывают алгоритмы секретности и требования, необходимые для подтверждения Файла конфигурации PS, которые основаны на режиме обеспечения элемента PS. Элемент PS ОБЯЗАН поддерживать оба алгоритма секретности, указанные в 7.3.3.3.1 и 7.3.3.3.2.

7.3.3.3.1 Алгоритм удостоверения подлинности Файла конфигурации PS для режима обеспечения DHCP

Процедура удостоверения подлинности для Файла конфигурации PS элементом PS в режиме обеспечения DHCP является следующей:

1) Когда система NMS создает новый Файл конфигурации PS или изменяет существующий файл, система NMS будет создавать случайные данные SHA-1 всего содержимого Файла конфигурации PS, которое берется как строка байта.

2) Система NMS добавляет значение случайных данных к названию Файла конфигурации PS, что посылается к элементу PS в сообщении Offer протокола DHCP (см. 7.2.3.3 и 13.2). Разграничитель, используемый между названием Файла конфигурации PS и значением случайных данных, представляет собой знак '@' (например, "configfile1.txt@23423487987345"). Элемент PS обновляет объект MIB cabhPsDevProvConfigHash с помощью полученного значения случайных данных.

3) Элемент PS загружает именованный файл из конфигурированного сервера TFTP.

4) Элемент PS ОБЯЗАН вычислить случайные данные SHA-1 по всему содержимому Файла конфигурации PS и сравнить вычисленные случайные данные со случайными данными в объекте MIB cabhPsDevProvConfigHash. Если вычисленные и конфигурированные значения случайных данных являются теми же самыми, то Файл конфигурации PS удостоверяется; в противном случае, файл ОБЯЗАН быть отвергнут.

5) Когда удостоверение подлинности является успешным, элемент PS ОБЯЗАН использовать содержимое Файла конфигурации PS для своей конфигурации.

7.3.3.3.2 Алгоритм удостоверения подлинности Файла конфигурации для режима обеспечения SNMP

Процедура для удостоверения подлинности Файла конфигурации PS элементом PS в режиме обеспечения SNMP является следующей:

1) Когда система NMS создает новый Файл конфигурации PS или изменяет существующий файл, система NMS будет создавать случайные данные SHA-1 всего содержимого Файла конфигурации PS, взятого в качестве строки байта.
2) Система NMS посылает значение случайных данных, вычисленное в шаге 1, к элементу PS через сообщение SET [*установить*] протокола SNMP и обновляет объект MIB cabhPsDevProvConfigHash.
3) Система NMS посылает имя и местонахождение Файла конфигурации PS через сообщение SET протокола SNMP и обновляет объект MIB cabhPsDevProvConfigFile (это запускает загрузку TFTP, см. 7.3.3.2).
4) Элемент PS загружает именованный файл из конфигурированного сервера TFTP.
5) Элемент PS ОБЯЗАН вычислить случайные данные SHA-1 по всему содержимому Файла конфигурации PS и сравнить вычисленные случайные данные со случайными данными в объекте MIB cabhPsDevProvConfigHash. Если вычисленные и конфигурированные значения случайных данных являются теми же самыми, Файл конфигурации PS удостоверяется; в противном случае, файл ОБЯЗАН быть отвергнут.
6) Когда удостоверение подлинности является успешным, элемент PS ОБЯЗАН использовать содержимое Файла конфигурации PS для своей конфигурации.

Успешная загрузка Файла конфигурации PS определяется как завершенная, и с правильным приемом элементом PS содержимого Файла конфигурации PS внутри периода выдержки времени TFTP, И вычислением услугой PS значений случайных данных для Файла конфигурации PS без ошибок, являющихся результатом вычисления.

7.3.3.4 Средства для информирования о статусе

Услуга PS ОБЯЗАНА сообщить о статусе загрузки Файла конфигурации и об ошибочных состояниях, используя процесс "Информирование о событии", описанный в 6.5.

Таблица 24 определяет режимы обработки, которые ОБЯЗАНЫ быть выполнены, и действие, которое ОБЯЗАНО быть предпринято, когда обнаруживаются эти режимы обработки.

Можно сослаться на Дополнение B для перечня событий, включая те, что перечислены в Таблице 24, и информацию о том, как сообщают о событиях.

Если обрабатываются любые установки конфигурации, то событие ОБЯЗАНО быть порождено тогда, когда обнаруживается окончание файла, и это событие ОБЯЗАНО включать в себя число успешно обработанных значений TLV и число опущенных значений TLV.

Запустив загрузку Файла конфигурации PS, элемент PS ОБЯЗАН продолжать пытаться загрузить указанный Файл конфигурации PS из указанного местоположения, пока Файл конфигурации не будет успешно загружен, а случайные данные не будут успешно вычислены, как описано в 7.3.3.3. Конкретная выдержка времени для доступа сервера TFTP зависит от осуществления. Однако услуга PS ОБЯЗАНА НЕ пытаться получить доступ к серверу TFTP более чем 3 раза в любом 5-минутном периоде. Как минимум, услуга PS ОБЯЗАНА сделать попытку один раз на каждый 5-минутный интервал для загрузки Файла конфигурации PS, пока Файл конфигурации PS не будет успешно загружен.

Услуга PS ОБЯЗАНА порождать соответствующе событие, которое определено в Дополнении B, указывая неудачную загрузку Файла конфигурации PS каждый раз, когда услуга PS терпит неудачу в загрузке Файла конфигурации PS.

Если услуга PS успешно загружает Файл конфигурации PS, услуга PS ОБЯЗАНА переустановить счетчик загрузки Файла конфигурации PS в нуль и породить соответствующее событие, определяемое в Дополнении B, для указания успешной загрузки Файла конфигурации PS.

Если услуга PS действует в режиме DHCP (как указывается значением cabhPsDevProvMode) И прекращает процесс загрузки Файла конфигурации PS, услуга PS ОБЯЗАНА породить событие, определенное в Дополнении B, для указания неудачи процесса загрузки Файла конфигурации PS, И освободить свой адрес IP WAN-Man услуги PS в соответствии с документом [RFC 2131], И повторно выпустить сообщение DISCOVER протокола DHCP в соответствии с документом [RFC 2131], т.е. услуга PS должна повторно запустить процесс установления в начальное состояние.

Таблица 24/J.191 – Режимы обработки Файла конфигурации PS

Режим неудачи	Действие
Поле типа не является действительным	Игнорировать субъект TLV и сообщить о событии. Продолжать обрабатывать файл.
Файл терпит неудачу проверки целостности (целостность файла все еще нуждается в определении)	Сообщить о событии. Не пытаться обрабатывать файл.
Файл слишком большой	Сообщить о событии. Не пытаться обрабатывать файл.
Файл конфигурации не найден	Сообщить о событии. Не пытаться обрабатывать файл.
Файл не заполнен должен образом	Сообщить о событии. Не пытаться обрабатывать файл.
Отсутствует маркер "Окончание файла"	Сообщить о событии. Не пытаться обрабатывать файл.
Не способен установить значение	Сообщить о событии и отклонить Файл конфигурации, а также осуществить переустановку. Установить обратно (в значение перед сообщением Set протокола SNMP) любые значения, что были сохранены в энергонезависимой памяти.
Встречается значение, где идентификатор OID протокола SNMP не является распознаваемым	Игнорировать субъект TLV и сообщить о событии. Продолжать обрабатывать файл.

Услуга PS ОБЯЗАНА использовать адаптивную выдержку времени для TFTP, основанную на бинарной показательной функции возврата к прежнему состоянию, как описано в документах [RFC 1123] и [RFC 2349].

7.4 Архитектура Клиента времени дня

7.4.1 Руководящие принципы разработки системы Клиента времени дня

Следующие руководящие принципы разработки системы в Таблице 25 продвигают возможности, определенные для Клиента времени дня PS:

Таблица 25/J.191 – Руководящие принципы разработки системы

Номер	Руководящие принципы разработки системы Клиента времени дня
TOD 1	Необходимо предоставить механизм, с помощью которого услуга PS может достичь синхронизации времени с сетью Головного узла.

7.4.2 Описание системы Клиента времени дня

Элемент PS использует клиента Времени дня, удовлетворяющего документу [RFC 868], чтобы достигнуть синхронизации по времени с таймером времени на сети головного узла. Синхронизация по времени является существенной для функций безопасности PS, а также для обмена сообщениями о событиях.

Когда клиент DHCP CDC запрашивает Адрес IP – от сервера DHCP Головного узла – для интерфейса WAN-Man, клиент DHCP будет получать адрес IP сервера TOD Головного узла внутри варианта выбора 4 протокола DHCP. Клиент DHCP будет также получать Смещение времени (по отношению к UTC), внутри варианта выбора 2 протокола DHCP.

Как только стек IP WAN-Man начинает использование адреса IP, который он получил от протокола DHCP, ему следует послать запрос времени к серверу TOD согласно документу [RFC 868]. Если сервер TOD откликается действительным откликом, то услуга PS начнет использование этого Времени дня для функций безопасности и обмена сообщениями о событиях.

Требования клиента Времени дня

Элемент PS ОБЯЗАН осуществлять клиента Времени дня.

Клиент Времени дня услуги PS ОБЯЗАН соответствовать протоколу Времени дня документа [RFC 868] и использовать только протокол UDP.

При переустановке элемент PS ОБЯЗАН установить свое начальное время в 0 (0:0.0 январь 1, 1900 год) в соответствии с документом [RFC 868].

Элемент PS ОБЯЗАН стремиться к синхронизации Времени дня с сервером TOD, указанным вариантом выбора 4 протокола DHCP, что принимается в сообщении Offer протокола DHCP, направленном к интерфейсу WAN-Man.

Услуга PS ОБЯЗАНА сложить время, найденное и выбранное от сервера TOD, со смещением времени, предоставляемым вариантом 2 протокола DHCP, чтобы создать текущее местное время.

Элемент PS ОБЯЗАН использовать текущее местное время, вычисленное из времени, найденного и выбранного из сервера TOD, и смещения времени, полученного вариантом выбора 2 протокола DHCP, для обмена сообщениями о событиях и функций безопасности, и нуждается только в том, чтобы быть точным по отношению к ближайшей секунде.

Элемент PS ОБЯЗАН продолжать стремиться осуществлять связь с сервером Времени дня до тех пор, пока не устанавливается местное время. Конкретная выдержка времени для запросов Времени дня зависит от осуществления. Однако клиент Времени дня услуги PS ОБЯЗАН НЕ превышать более 3 запросов TOD в любом 5-минутном периоде. Как минимум, клиент Времени дня услуги PS ОБЯЗАН выпустить, по меньшей мере, 1 запрос TOD на каждый 5-минутный период, пока не установится местное время.

Если сервер TOD не откликается с помощью действительного отклика, услуга PS ОБЯЗАНА осуществить следующее, необязательно в перечисленном порядке:

- Установить значение cabhPsDevTodSyncStatus в '2' (доступ к TOD неудачен).
- Если в области LAN-Trans имеются активные аренды, как указано ненулевым значением для cabhCdpLanTransCurCount, установить cabhCdpLanAddrCreateTime в текущее время и установить объект cabhCdpLanAddrExpireTime в значение cabhCdpLanAddrCreateTime плюс значение cabhCdpServerLeaseTime для каждой активной аренды (Время истечения = CreateTime + LeaseTime);
  - зарегистрировать неудачу и породить стандартное событие, определенное в Дополнении B; и

– продолжать повторно осуществлять связь с сервером TOD, пока не устанавливается местное время.

Если услуга PS успешно синхронизирует свой эталон времени с сервером TOD в кабельной сети, услуга PS ОБЯЗАНА установить значение cabhPsDevTodSyncStatus в '1' (синхронизация TOD успешна).

Если значение cabhPsDevTodSyncStatus есть '1', т.е., если местное время уже было установлено, то нет необходимости для клиента Времени дня выпускать запрос TOD.

8 Пакетная обработка и трансляция адреса

8.1 Введение/обзор

8.1.1 Цели

Ключевые цели, которые продвигают возможности пакетной обработки, включают в себя:

- обеспечение кабельных функциональных возможностей дружественной трансляции адреса, дающих возможность обзора кабельного оператора и административной управляемости домашних устройств при сохранении архитектуры маршрутизации, основанной на источнике кабельной сети;
- предотвращение ненужного трафика на кабельной и домашних сетях;
- сбережение глобально прокладываемых открытых адресов IP, а также частных адресов административного управления кабельной сетью;
- облегчение внутридомовой маршрутизации трафика IP путем назначения сетевых адресов Устройствам IP сети LAN так, что они находятся в той же самой логической подсети.

8.1.2 Предположения

- Предполагается, что когда серверы обеспечения кабельного оператора, обеспечивают многократные глобально маршрутизируемые адреса IP к устройствам клиента в доме, эти адреса не обязательно будут находиться в той же самой подсети.
- Предполагается, что изменение поставщиков услуг Интернет должно иметь место сравнительно нечасто, возникая на скорости, подобной скорости изменения семейством своего первичного оператора дальней связи.
- Функция обработки пакетов PS может направлять вещательный трафик ко всем интерфейсам LAN и WAN-Data прозрачным образом. Дросселирование вещательного трафика не требуется. Предполагается, что кабельный модем DOCSIS обладает возможностью фильтровать вещательный трафик IP.

8.2 Архитектура

Этот раздел описывает ключевые понятия, лежащие в основе функциональных возможностей пакетной обработки и трансляции адреса.

8.2.1 Руководящие указания по разработке системы

См. Таблицу 26.

8.2.2 Описание системы обработки пакетов

Этот раздел предоставляет обзор ключевых понятий обработки пакетов и трансляции адресов.

Функциональные возможности трансляции адресов и обработки пакетов обеспечиваются функциональным объектом, известным как Портал кабельного адреса (*CAP, Cable Address*

Portal). Портал CAP осуществляет следующие элементы трансляции адресов и переадресации пакетов:

- Трансляция кабельного адреса (*CAT, Cable Address Translation*);
- Сквозная функция;
- Переключатель избирательной переадресации восходящего направления (*USFS, Upstream Selective Forwarding Switch*).

Таблица 26/J.191 – Руководящие принципы разработки системы обработки пакетов и трансляции адресов

Номер	Руководящие принципы разработки системы
Обработка пакетов 1	Механизмы адресации будут управляться оператором и будут предоставлять оператору знание относительно возможности доступа к услуге PS.
Обработка пакетов 2	Адресация не будет осуществлять ничего, что будет компрометировать архитектуры маршрутизации текущих кабельных сетей (например, маршрутизацию на основе источника, MPLS).
Обработка пакетов 3	Механизмы административного управления трафиком будут изолировать кабельную сеть от трафика, порожденного путем осуществления связи между равноправными объектами внутри дома, если такое имеется.
Обработка пакетов 4	Адреса IP будут сохранены, когда это возможно (как глобально маршрутизируемые адреса, так и частные адреса административного управления кабельной сетью).

8.2.2.1 Функциональное обозрение пакетной обработки

Как показано на Рисунке 16, функция CAT предоставляет механизм для взаимного соединения адресной области WAN-Data и адресной области LAN-Trans (через трансляцию адресов), в то время как Сквозная функция предоставляет механизм для взаимного соединения адресной области WAN-Data и адресной области LAN-Pass (через перемыкание). Функция CAT удовлетворяет секции 2 документа [RFC 3022] по традиционной трансляции сетевых адресов (*NAT, Traditional Network Address Translation*). Как в случае традиционной NAT, имеются две разновидности CAT, упоминаемые как прозрачная маршрутизация трансляции адресов кабельной сети (*C-NAT, Cable Network Address Translation*) и прозрачная маршрутизация адресов кабельной сети и трансляции портов (*C-NAPT, Cable Network Address and Port Translation*). Прозрачная маршрутизация C-NAT является версией секции 2.1 документа [RFC 3022], соответствующей кабелю, а прозрачная маршрутизация C-NAPT является версией NAPT секции 2.2 документа [RFC 3022], соответствующей кабелю.

Согласно документу [RFC 3022], прозрачная маршрутизация C-NAT есть "метод, с помощью которого адреса IP из одной группы отображаются в другой группе, прозрачной для конечных пользователей", а прозрачная маршрутизация C-NAPT "есть метод, с помощью которого множество сетевых адресов и их порты TCP/UDP (Протокол управления передачей /Датаграммный протокол пользователя) [*TCP/UDP, Transmission Control Protocol/User Datagram Protocol*] транслируются в единственный сетевой адрес и его порты TCP/UDP". Кроме того, согласно документу [RFC 3022], целью функциональных возможностей C-NAT и C-NAPT является "обеспечение механизма для подсоединения области с частными адресами к внешней области с глобально уникальными зарегистрированными адресами ".

Сквозная функция (*CPT, CableHome Pass-through*) является указанным процессом перемыкания, который соединяет между собой адресную область WAN-Data и адресную область LAN-Pass без трансляции адресов.

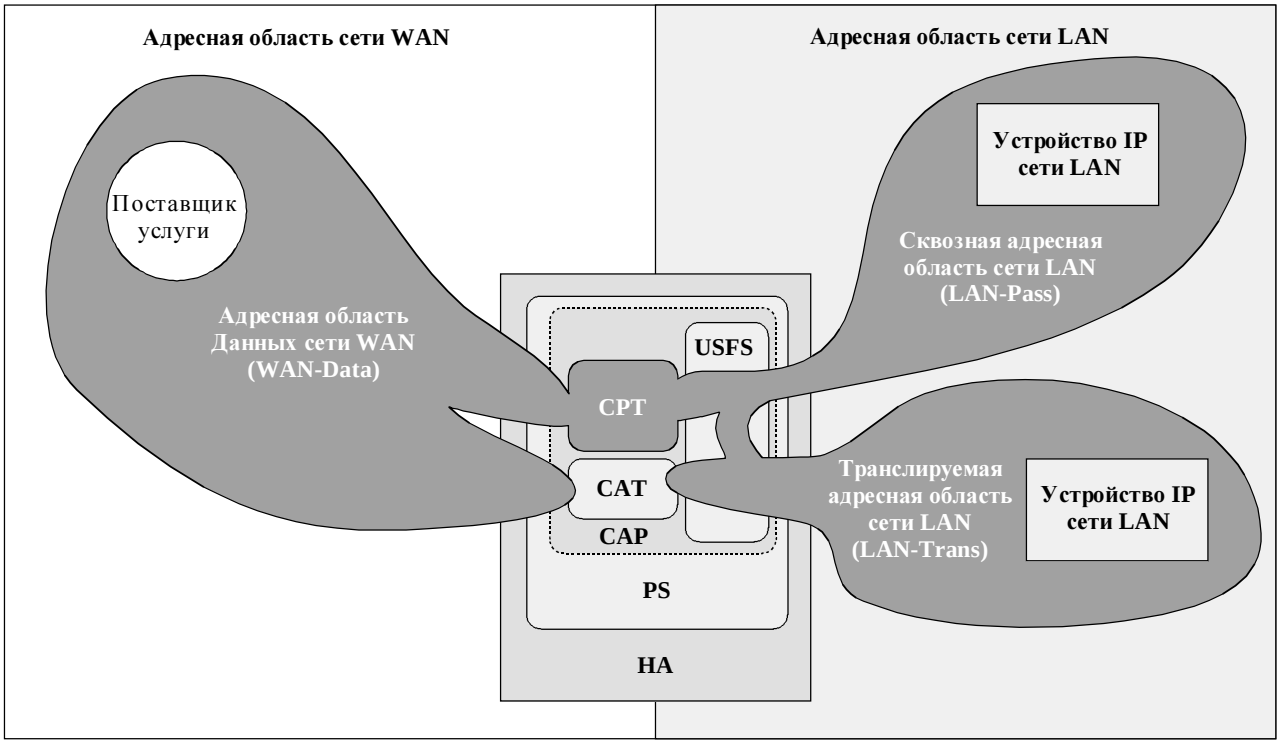


Рисунок 16/J.191 – Функции Кабельного адресного портала (CAP)

Переключатель избирательной переадресации восходящего направления (*USFS, Upstream Selective Forwarding Switch*) определяет функцию внутри портала CAP с возможностью ограничения в домашнем трафике к дому, даже когда внутридомовые устройства, порождающие этот трафик, находятся на различных логических подсетях IP. Конкретно, эта функция направляет трафик, берущий начало от одного адреса IP в одной из адресных областей сети LAN, который предназначен адресам IP в одной из адресных областей сети LAN, непосредственно к своему пункту назначения. Эти функциональные возможности непосредственной переадресации предохраняют трафик от пересечения границы сети HFC, и взаимно соединяет адресные области LAN-Trans и LAN-Pass.

По всему тексту этой Рекомендации термины "Связывание адресов", "Развязывание адресов", "Трансляция адресов" и "Сеанс" используются так, как определено в документе [RFC 2663]. Кроме того, термин "Отображение" [Mapping] определяется как информация, требуемая для выполнения Прозрачной маршрутизации C-NAT и Прозрачной маршрутизации C-NAPT.

В частности, Отображение C-NAT определяется как кортеж (набор взаимосвязанных величин) формы (адрес IP WAN-Data, адрес IP LAN-Trans), обеспечивающей непосредственное отображение между адресами WAN-Data и адресами LAN-Trans. Подобным образом, Отображение C-NAPT определяется как кортеж формы (адрес IP WAN-Data и порт TCP/UDP, адрес IP LAN-Trans и порт TCP/UDP), обеспечивающей отображение из одного во множество между единственным адресом WAN-Data и многократными адресами LAN-Trans. Для трафика ICMP (такого, как переброс информации), номер последовательности ICMP используется вместо номера порта TCP/UDP.

Трафик из сети LAN к сети WAN определяется как пакеты, производимые Устройствами IP сети LAN, которые предназначены для устройств на стороне сети WAN услуги PS. Трафик из сети WAN к сети LAN определяется пакетами, производимыми главными узлами сети WAN, которые предназначены для устройств IP сети LAN. Трафик между сетями LAN определяется как пакеты, производимые Устройствами IP сети LAN, которые предназначены Устройствам IP сети LAN на той же самой или другой подсети.

8.2.2.2 Режимы пакетной обработки

Элемент PS является конфигурируемым, через объект MIB cabhCapPrimaryMode, чтобы действовать в одном из трех Режимов первичной обработки пакетов при обработке трафика из сети LAN к сети WAN и из сети WAN к сети LAN:

1) Сквозной режим;

2) Режим Прозрачной маршрутизации C-NAT; и

3) Режим Прозрачной маршрутизации C-NAPT.

Более того, первичные режимы C-NAT или C-NAPT могут также действовать в смешанном режиме, описываемом ниже.

В Сквозном режиме портал CAP действует в качестве прозрачного моста [Мосты ISO DIS 10038 MAC] между областью WAN-Data и областью LAN-Pass. В Сквозном режиме решения по переадресации принимаются первоначально на Уровне 2 BOC [*OSI Layer 2*] (уровень звена данных). В этом режиме портал CAP не осуществляет какие-либо функции Прозрачной маршрутизации C-NAT или C-NAPT.

Портал CAP поддерживает Уровень 3 BOC (сетевой уровень), осуществляя переадресацию как в режиме Прозрачной маршрутизации C-NAT, так и в режиме Прозрачной маршрутизации C-NAPT, которые описаны ниже.

В режиме C-NAT элемент PS (CDC) приобретает один или более адресов IP, используемых для трафика WAN-Data во время процесса начального запуска услуги PS. После приобретения, через протокол DHCP, эти адреса IP используются в качестве части адреса IP WAN-Data Динамически создаваемых кортежей отображения C-NAT. Эти адреса IP сети WAN составляют объединение ресурсов адресов, доступных для Динамически создаваемых отображений C-NAT. Если имеющийся адрес IP существует в объединении ресурсов адресов IP WAN-Data, то портал CAP создает Динамическое отображение C-NAT, когда он впервые видит трафик IP от сети LAN к сети WAN, что не имеет существующего отображения. Если имеющийся адрес IP не существует в объединении ресурсов адресов IP WAN-Data, то Динамическое отображение C-NAT не может быть создано, этот трафик опускается и порождается событие (см. Дополнение B).

Динамические отображения C-NAT для трафика UDP разрушаются, когда истекает период выдержки времени отсутствия активности, cabhCapUdpTimeWait. Динамические отображения C-NAT для трафика TCP уничтожаются, когда истекает период выдержки времени отсутствия активности, cabhCapTcpTimeWait, или когда заканчивается сеанс TCP. Динамические отображения C-NAT для трафика ICMP уничтожаются, когда истекает период выдержки времени отсутствия активности, cabhCapIcmpTimeWait. Кроме того, могут быть созданы или уничтожены Статические отображения C-NAT, когда система NMS записывает в таблицу MIB объект cabhCapMappingTable или исключает этот объект из нее.

В режиме C-NAPT (фабричный режим по умолчанию для системы) элемент PS (CDC) приобретает один адрес IP, используемый для трафика WAN-Data. После приобретения, через протокол DHCP, этот адрес IP используется в качестве части адреса IP WAN-Data для Динамически создаваемых кортежей отображений C-NAPT. Если адрес IP WAN-Data был приобретен, то Динамические отображения C-NAPT создаются тогда, когда портал CAP впервые видит трафик IP из сети LAN к сети WAN, который не имеет существующего отображения. Если адрес IP WAN-Data не был приобретен (т.е. не имеет активной аренды DHCP), то Динамическое отображение C-NAPT не может быть создано, этот трафик опускается и порождается стандартное событие (см. Дополнение B).

Динамические отображения C-NAPT для трафика UDP разрушаются, когда истекает период выдержки времени отсутствия активности, cabhCapUdpTimeWait. Динамические отображения C-NAPT для трафика TCP разрушаются, когда истекает период выдержки времени отсутствия

активности, cabhCapTcpTimeWait, или заканчивается сеанс TCP. Динамические отображения C-NAPT для трафика ICMP разрушаются, когда истекает период выдержки времени отсутствия активности, cabhCapIcmpTimeWait. Кроме того, могут быть созданы или разрушены Статические отображения C-NAPT, когда система NMS записывает в таблицу MIB объект cabhCapMappingTable или исключает его из таблицы.

Рисунок 17 показывает типичный процесс Динамического отображения C-NAPT с пакетом TCP. В этом примере услуга PS конфигурируется для действия в режиме NAPT, и уже получила адрес IP сети WAN, а Устройство IP сети LAN уже получило адрес IP в области LAN-Trans.

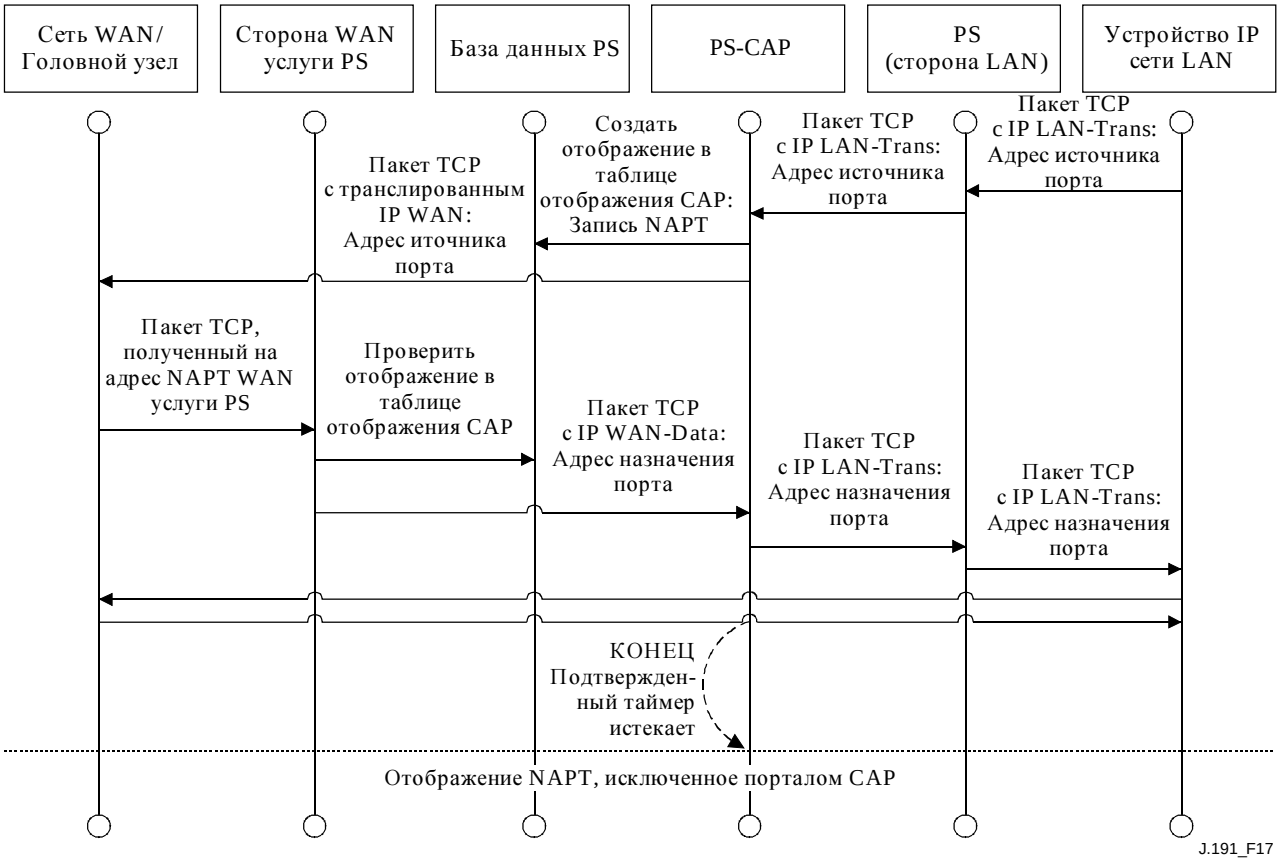


Рисунок 17/J.191 – Диаграмма последовательности конфигурации PS (Таблица отображения CAP – NAPT)

Для услуги PS оказывается возможным также действовать в Смешанном режиме "Перемыкание/Маршрутизация". В этом случае система NMS устанавливает первичный режим к Прозрачной маршрутизации C-NAT или C-NAPT, и система NMS записывает один или более адресов MAC, принадлежащих Устройствам IP сети LAN, чей трафик должен быть перемкнут, в Сквозную таблицу (cabhCapPassthroughTable). В этом Смешанном режиме услуга PS проверяет адреса MAC принятых кадров для определения, осуществлять ли прозрачное перемыкание кадра, или выполнять какие-либо функции Прозрачной маршрутизации C-NAT или C-NAPT в уровне IP. В случае трафика из сети LAN к сети WAN услуга PS проверяет адрес MAC источника, и если такой адрес MAC существует в объекте cabhCapPassthroughTable, то кадр прозрачным образом перемыкается к интерфейсу WAN-Data. В случае трафика из сети WAN к сети LAN услуга PS проверяет адрес MAC пункта назначения, и если такой адрес MAC существует в объекте cabhCapPassthroughTable, то кадр прозрачным образом перемыкается к соответствующему интерфейсу LAN. Если адрес MAC

не существует в объекте cabhCapPassthroughTable, то пакет обрабатывается функциями верхнего уровня, включая функцию Прозрачной маршрутизации C-NAT/C-NAPT.

Следует отметить, что функциональные возможности USFS (см. 8.2.2.3) применяются в каждом из трех Первичных обработок пакетов, и вне зависимости от того, используется ли Смешанный режим, или нет. Решения по продвижению USFS будут обладать преимуществом над другими решениями по продвижению, что могли бы потенциально направлять трафик из сети LAN к сети WAN.

8.2.2.3 Обзор переключателя избирательной переадресации восходящего направления

В некоторых случаях Устройство IP сети LAN в адресной области LAN-Pass будет находиться в другой логической подсети IP по сравнению с другими Устройствами IP сети LAN, подсоединенными к тому же самому элементу PS. Важно предотвратить трафик между этими Устройствами IP сети LAN от пересечения границы сети HFC. Предотвращение этого нежелательного трафика HFC является функцией, которая обеспечена Переключателем избирательной переадресации восходящего направления (*USFS, the Upstream Selective Forwarding Switch*).

Конкретно, переключатель USFS прокладывает трафик (который подается из дома и направляется к дому) непосредственно к его пункту назначения. Поставляемый трафик Устройства IP сети LAN, чей адрес IP пункта назначения находится вне адресной области LAN, пропускается неизмененным к функциональным возможностям перемыкания/маршрутизации CAP.

Функциональные возможности переключателя USFS используют Таблицу трансляции адресов IP (как определено в документе [RFC 2011]) внутри элемента PS. Эта таблица, ipNetToMediaTable [RFC 2011], содержит перечень Адресов MAC, их соответствующие Адреса IP и номера "Индексы интерфейсов" услуги PS из физических интерфейсов, с которыми связаны эти адреса. Переключатель USFS будет ссылаться на эту таблицу, чтобы принять решение относительно направления потока трафика из сети LAN к сети WAN. Чтобы населить объект ipNetToMediaTable, услуга PS узнает адреса IP и MAC и их ассоциации. Для каждого связанного физического интерфейса услуга PS узнает все адреса IP LAN-Trans и LAN-Pass вместе с их соединенными привязками MAC, и это узнавание может происходить через множество методов. Методы узнавания адресов IP/MAC, характерные для поставщика, могут включать в себя: отслеживание ARP, наблюдение за трафиком и принятие во внимание записей CDP. Записи очищаются от объекта ipNetToMediaTable после того, как обоснованный период выдержки времени отсутствия активности истек.

Переключатель USFS изучает весь трафик IP, полученный на интерфейсах LAN услуги PS. Если обнаруживается, что адрес IP пункта назначения (через ipNetToMediaTable) находится на интерфейсе LAN услуги PS, то первоначальный адрес пункта назначения звена данных кадра изменяется от такого адреса шлюза по умолчанию на такой адрес Устройства IP сети LAN пункта назначения, а трафик направляется к соответствующему интерфейсу LAN услуги PS. Если соответствие к адресу IP пункта назначения не найдено в объекте ipNetToMediaTable, то пакет пропускается, в первоначальной форме, к функции Прозрачной маршрутизации C-NAT/C-NAPT или к функции Сквозного перемыкания (в зависимости от активного режима обработки пакетов).

8.2.2.4 Широковещание

Портал CAP поддерживает трафик Широковещания путем прозрачного перемыкания обмена сообщениями IGMP [RFC 2236] и пакетов Широковещания IP. Портал CAP направляет трафик IGMP, порожденный на сети WAN, к сети LAN, чтобы разрешить объявлениям достичь Устройств IP сети LAN. Устройство IP сети LAN будет определять, к какому широковещанию оно желает присоединиться, и будет посылать сообщение широковещания "join" [*присоединиться*]. Источник широковещания затем будет способен пропускать далее

данные к Устройству IP сети LAN. Когда услуга широковещания больше не является желательной, Устройство IP сети LAN может либо игнорировать услугу, и поток будет прекращен, или Устройство IP сети LAN может послать сообщение "leave" [*покинуть*] протокола IGMP к цепи, чтобы сорвать потоковый трафик. Рисунок 18 предоставляет подробный пример процессов IGMP и Широковещания, проходящих через услугу PS.

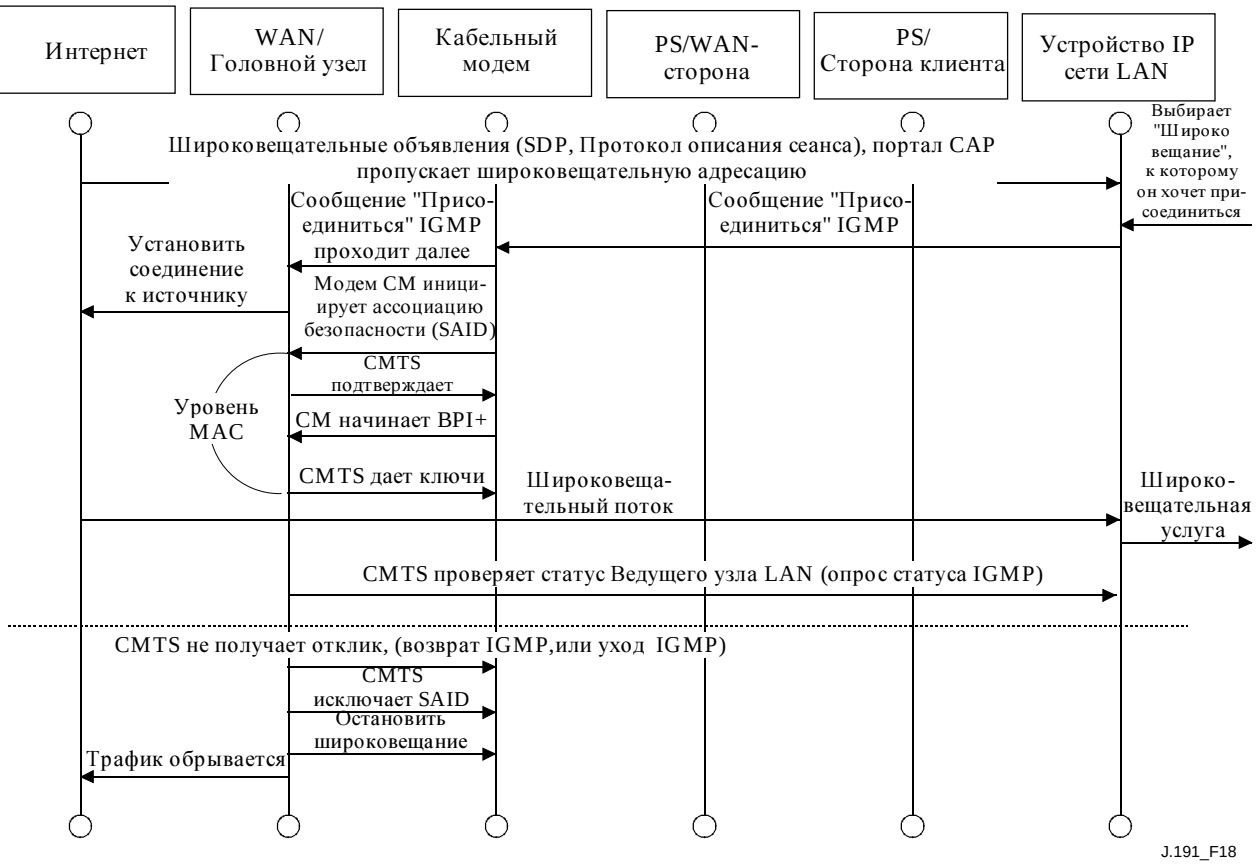


Рисунок 18/J.191 – Широковещание через последовательность IGMP

8.2.2.5 Примеры обработки пакетов

Этот раздел предоставляет информативный обзор по обработке, касающейся обработки пакетов. Рисунок 19 показывает пример возможных шагов по обработке пакетов для однонаправленного трафика из сети LAN к сети WAN, а Рисунок 20 показывает пример возможных шагов обработки пакетов для однонаправленного трафика из сети WAN к сети LAN. Эти примеры являются только информативными и не предполагают какие-либо требования по осуществлению.

8.3 Требования CAP

8.3.1 Общие требования

Все логические интерфейсы IP на элементе PS ОБЯЗАНЫ удовлетворять документу [RFC 1122], секции 3 и 4, чтобы обеспечивать стандартную связь с Главными узлами Интернет.

Портал CAP ОБЯЗАН поддерживать Широковещательный трафик путем прозрачного перемыкания обмена сообщениями IGMP и Широковещательных пакетов IP, как определено в документе [RFC 2236].

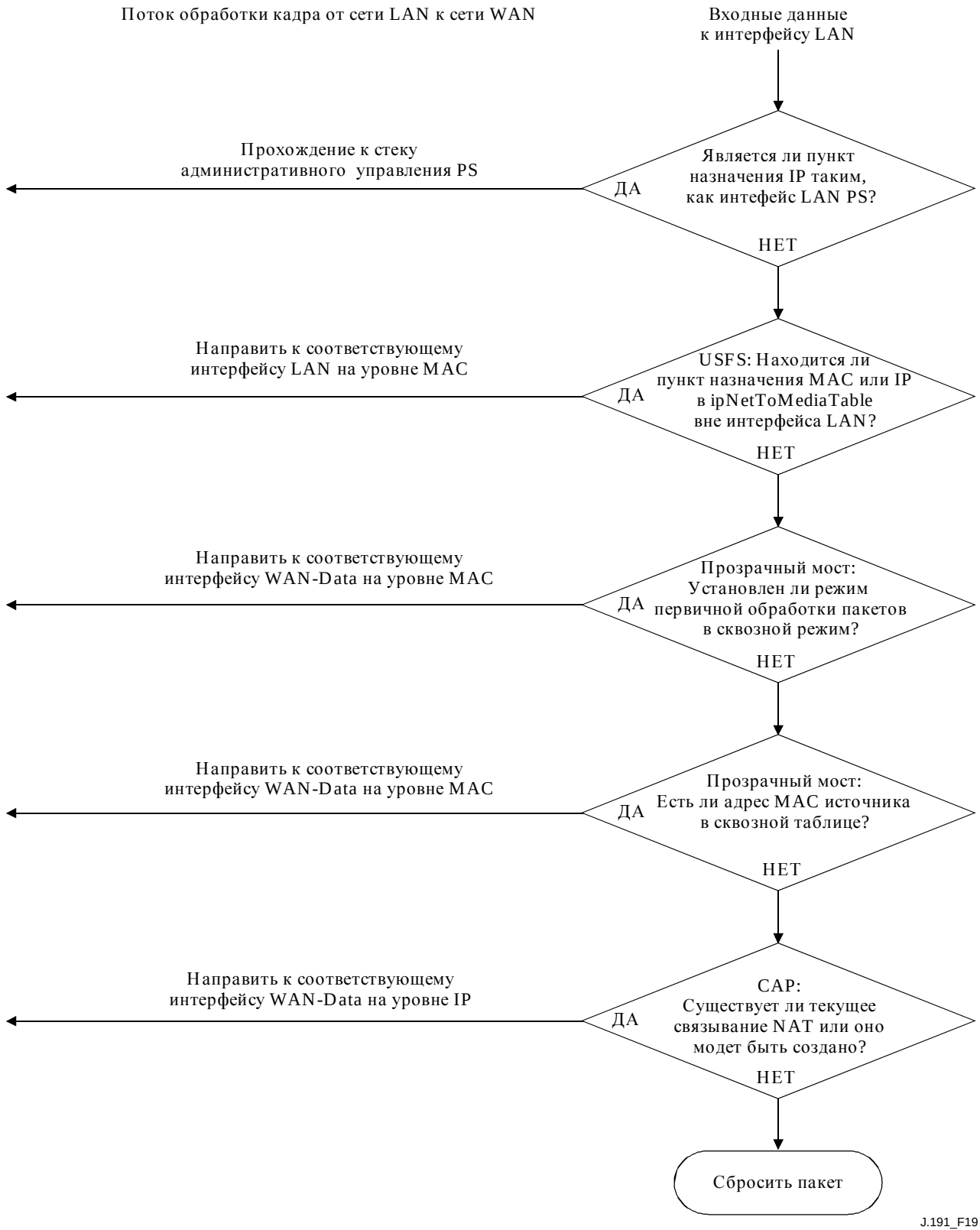


Рисунок 19/J.191 – Пример обработки пакетов из сети LAN к сети WAN

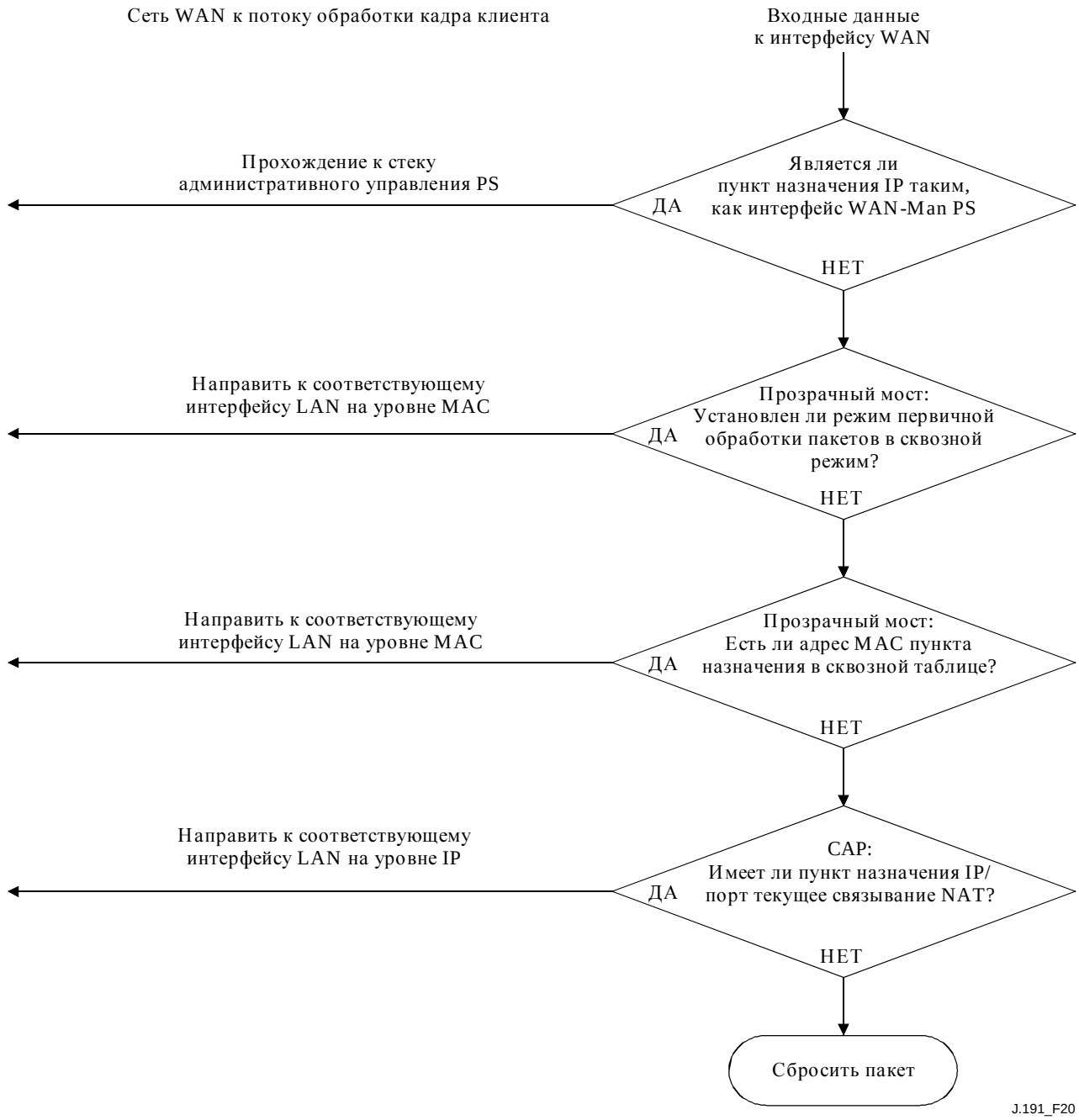


Рисунок 20/J.191 – Пример обработки пакетов из сети WAN к сети LAN

8.3.2 Требования по обработке пакетов

Портал CAP ОБЯЗАН поддерживать Сквозной режим, режим Прозрачной маршрутизации C-NAT и режим Прозрачной маршрутизации C-NAPT, кроме того, портал CAP ОБЯЗАН поддерживать выбор этого режима Первичной обработки пакетов, через объект MIB cabhCapPrimaryMode.

Если режим Первичной обработки пакетов, cabhCapPrimaryMode, установлен в C-NAT, портал CAP ОБЯЗАН убедиться, что существует доступный адрес IP, поставляемый Головным узлом, в Объединении ресурсов адресов IP WAN-Data (с текущей арендой DHCP) перед тем, как попытаться использовать этот адрес IP в качестве части отображения C-NAT. Если портал CAP неспособен создать отображение C-NAT, из-за истощения Объединения ресурсов адресов IP WAN-Data, он должен породить стандартное событие (как определено в Дополнении B).

Если режим Первичной обработки пакетов, cabhCapPrimaryMode, устанавливается в C-NAPT, портал ОБЯЗАН убедиться, что существует текущий адрес IP сети WAN (с текущей арендой DHCP из обеспечения Головного узла), перед тем, как попытаться использовать этот адрес IP в качестве части отображения C-NAPT. Если портал CAP не способен создать отображение C-NAPT, по причине отсутствия текущего адреса IP сети WAN, или из-за истощения номеров портов, то он обязан породить стандартное событие (как определено в Дополнении B).

Трафик между сетями LAN никогда НЕ ОБЯЗАН прокладываться или перемыкаться за пределом интерфейса сети WAN.

8.3.2.1 Сквозные требования

Когда Режим первичной обработки пакетов портала CAP, cabhCapPrimaryMode, устанавливается в Сквозной режим, портал CAP ОБЯЗАН действовать в качестве прозрачного моста, как определено в документе [ИСО/МЭК 10038], между областью WAN-Data и областью LAN-Pass, и ОБЯЗАН НЕ осуществлять какие-либо функции Прозрачной маршрутизации C-NAT или C-NAPT. Даже тогда, когда режим Первичной обработки пакетов устанавливается в Сквозной режим, обработка USFS ОБЯЗАНА обладать преимуществом перед решениями перемыкания сетей LAN-WAN.

8.3.2.2 Требования прозрачной маршрутизации C-NAT и C-NAPT

Когда режим Первичной обработки пакетов (cabhCapPrimaryMode) устанавливается в C-NAT, портал CAP ОБЯЗАН поддерживать процессы трансляции адресов C-NAT в соответствии с основными требованиями NAT, как определено в документе [RFC 3022].

Когда режим Первичной обработки пакетов (cabhCapPrimaryMode) устанавливается в C-NAPT, портал CAP ОБЯЗАН поддерживать процессы трансляции адресов C-NAPT в соответствии с основными требованиями NAPT, определенными в документе [RFC 3022].

Несмотря на режим Первичной обработки пакетов, портал CAP ОБЯЗАН поддерживать создание и исключение Статических отображений C-NAT и C-NAPT, путем предоставления системе NMS возможности читать, создавать и исключать (через портал CMP) записи Статических отображений CAP (cabhCapMappingTable).

Созданные с помощью системы NMS Статические отображения C-NAT и C-NAPT ОБЯЗАНЫ сохраняться при повторных начальных загрузках услуги PS.

Портал CAP ОБЯЗАН поддерживать создание Динамических отображений C-NAT и C-NAPT, инициированных трафиком TCP, UDP или ICMP от сети LAN к сети WAN. Портал CAP ОБЯЗАН давать возможность системе NMS читать (через портал CMP) записи Динамического отображения CAP (cabhCapMappingTable) .

Портал CAP ОБЯЗАН поддерживать исключение Динамических отображений C-NAT и C-NAPT, если заданное отображение связано с сеансом TCP, И если сеанс TCP завершается, ИЛИ выдержка времени для отсутствия активности TCP, объект cabhCapTcpTimeWait, для такого отображения истекает.

Портал CAP ОБЯЗАН поддерживать исключение Динамических отображений C-NAT и C-NAPT, если заданное отображение связывается с сеансом UDP, И выдержка времени для отсутствия активности UDP, объект cabhCapUdpTimeWait, для такого отображения истекает.

Портал CAP ОБЯЗАН поддерживать исключение Динамических отображений C-NAT и C-NAPT, если заданное отображение связывается с сеансом ICMP, И выдержка времени для отсутствия активности ICMP, объект cabhCapIcmpTimeWait, для такого отображения истекает.

Динамические отображения C-NAT и C-NAPT ОБЯЗАНЫ НЕ сохраняться при повторных начальных загрузках услуги PS.

8.3.2.3 Требования смешанного режима "Перемыкание/маршрутизация"

Портал CAP ОБЯЗАН поддерживать Смешанный режим "Перемыкание/Маршрутизация", как описано в 8.2.2, где режим Первичной обработки пакетов, cabhCapPrimaryMode, устанавливается в Прозрачную маршрутизацию C-NAT или C-NAPT, и где портал CAP будет также прозрачным образом перемыкать трафик для конкретных адресов MAC. Если режим Первичной обработки пакетов CAP, cabhCapPrimaryMode, устанавливается в Прозрачную маршрутизацию C-NAT или C-NAPT, И система NMS записала адрес MAC, принадлежащий Устройству IP сети LAN, в объект cabhCapPassthroughTable, портал CAP ОБЯЗАН прозрачным образом перемыкать трафик из сети LAN к сети WAN, питаемый этим адресом MAC, и трафик из сети WAN к сети LAN, предназначенный для этого адреса MAC.

При нахождении в Смешанном режиме "Перемыкание/Маршрутизация", как описано в 8.2.2, функция USFS ОБЯЗАНА применяться ко всему принятому трафику, берущему начало в сети LAN.

8.3.3 Требования USFS

Функциональные возможности Переключателя избирательной переадресации восходящего направления (*USFS, Upstream Selective Forwarding Switch*) ОБЯЗАНЫ быть применены к пакетной обработке, вне зависимости от режима обработки пакетов портала CAP (Сквозной, C-NAT, C-NAPT, или смешанный типа "Перемыкание/Маршрутизация").

Элемент PS ОБЯЗАН узнавать все адреса IP и MAC LAN-Trans IP, LAN-Pass Устройств IP сети LAN, связанные с каждым из своих активных физических сетевых интерфейсов. Адреса IP и адреса MAC, которые узнаны элементом PS, и номера индексов физических интерфейсов PS ОБЯЗАНЫ быть доступными для системы NMS (через портал CMP) с помощью объекта ipNetToMediaTable документа [RFC 2011]. Элемент PS ОБЯЗАН исключать записи от объекта ipNetToMediaTable, когда истекает выдержка времени для отсутствия активности.

Функция USFS ОБЯЗАНА рассматривать весь трафик IP, берущий начало на интерфейсах LAN услуги PS, чтобы определять, является ли адрес IP пункта назначения из пакета таким, как адрес устройства, находящегося на интерфейсе LAN услуги PS. Если адрес IP пункта назначения в пакете, рассмотренном переключателем USFS, является таким же, как у Устройства IP сети LAN, находящегося вне интерфейса LAN услуги PS, то функция USFS ОБЯЗАНА заменить адрес пункта Назначения уровня MAC, внутри заголовка Уровня 2 пакета, адресом MAC Устройства IP сети LAN такого пункта назначения и направить кадр за пределы соответствующего физического интерфейса LAN.

9 Разрешающая способность имени

9.1 Введение/Обзор

9.1.1 Цели

Цели разрешающей способности имени включают в себя:

- Обеспечивать Систему названий доменов (*DNS, Domain Name System*) от сервера в услуге PS клиентам DNS внутри Устройств IP сети LAN, даже во время выходов из строя кабельных соединений.
- Давать возможность абонентам ссылаться на местные устройства через интуитивные имена устройств вместо того, чтобы осуществлять это с помощью адреса IP.
- Отсылать клиентов DNS сети LAN к серверам DNS Головных узлов, для разрешающей способности имен, не принадлежащих местным главным узлам.
- Обеспечивать легкое восстановление услуги DNS при повторном установлении связности кабеля после выхода из строя.

9.1.2 Предположения

Действующие предположения для услуг именования включают в себя:

- Сервер DNS в элементе PS является единственным сервером DNS, уполномоченным для Устройств IP сети LAN в области LAN-Trans.
- Элемент PS не будет обеспечивать услугу DNS Устройствам IP сети LAN в области LAN-Pass.
- Если элемент PS использует многократные адреса WAN-Data, то будет использована информация сервера DNS сети WAN, полученная во время самого последнего процесса приобретения адреса WAN-Data (DHCP).

9.2 Архитектура

9.2.1 Руководящие принципы разработки системы

См. Таблицу 27.

Таблица 27/J.191 – Руководящие принципы разработки системы разрешающей способности имени

Ссылка	Руководящие принципы разработки системы
Разрешающая способность имени 1	Обеспечивать услугу имени домена от сервера в услуге PS к клиентам DNS внутри Устройств IP сети LAN, для разрешающей способности имени Устройств IP сети LAN (независимо от состояния соединения WAN)
Разрешающая способность имени 2	Обеспечивать направление DNS к серверам DNS Головных узлов, для клиентов DNS внутри Устройств IP сети LAN, для разрешающей способности имен неместных ведущих узлов

9.2.2 Описание системы

Этот раздел предоставляет обзор услуг разрешающей способности имени внутри элемента PS.

9.2.2.1 Функциональный обзор разрешающей способности имени

Портал кабельного присваивания имен (*CNP, Cable Naming Portal*) является услугой, выполняющейся в PS, что обеспечивает простой сервер DNS для Устройств IP сети LAN в адресной области LAN-Trans. Портал CNP не используется Устройствами IP сети LAN в адресной области LAN-Pass, поскольку они будут непосредственно обслуживаться серверами DNS, которые являются внешними по отношению к дому.

Все Устройства IP сети LAN в области LAN-Trans конфигурируются порталом CDP для использования портала CNP в качестве своего Сервера имени домена. Услуга CNP в области LAN-Trans не зависит от состояния соединения сети WAN. Портал CNP выполняет следующие задачи:

- Решает проблему имен ведущих узлов для Устройств IP сети LAN, возвращая их соответствующие адреса IP.
- Отсылает Устройства IP сети LAN к внешним серверам DNS для вопросов, которые не могут быть решены через местную информацию PS. Это действие имеет место только тогда, когда информация сервера DNS сети WAN имеется в услуге PS. Иначе портал CNP возвращает ошибку, указывающую, что имя не может быть разрешено в это время.

Создавая портал CNP, первичный сервер DNS в помещении клиента избегает потребности повторно формировать Устройства IP сети LAN, когда состояние соединения WAN изменяется. Это также разрешает изменять назначение внешнего сервера DNS без повторного формирования Устройств IP сети LAN.

9.2.2.2 Операция разрешающей способности имени

Когда запрашивается разрешение имени ведущего узла, портал CNP выполняет процесс поиска, показанный на Рисунке 21. Портал CNP откликается на первоначальные стандартные вопросы DNS [RFC 1035], направленные к объекту cabhCdpServerDnsAddress, для всех поисков имен. Если портал CNP откликается с помощью направления к внешним серверам DNS, то предполагается, что ответственностью Устройства IP сети LAN является посылка вопроса непосредственно к упоминаемому серверу.

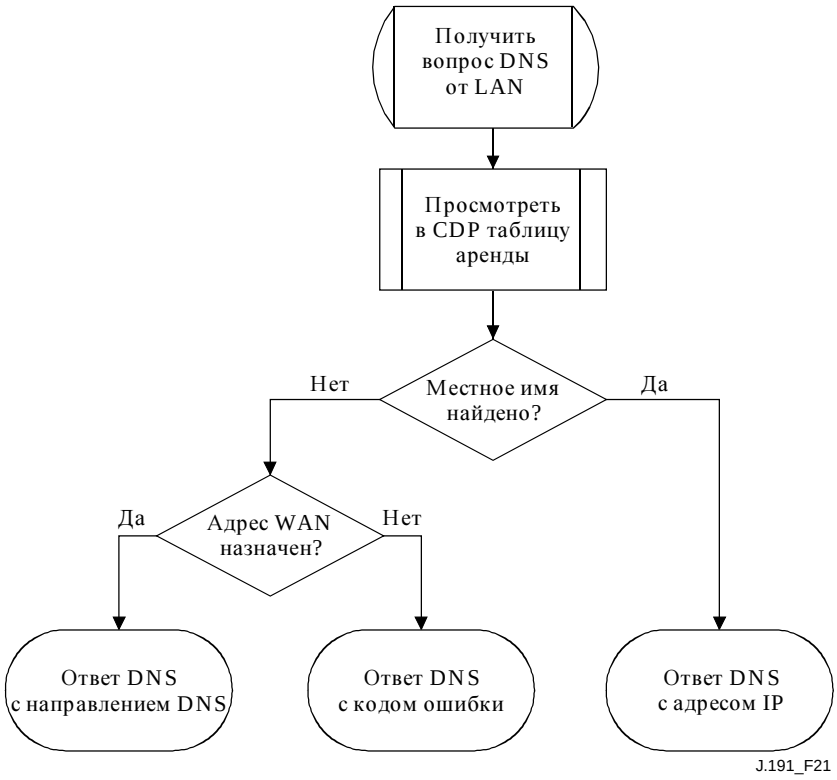


Рисунок 21/J.191 – Обработка пакета CNP

Портал CNP полагается на объект cabhCdpLanAddrTable портала CDP, чтобы узнавать имена ведущих узлов, связанные с текущими адресами IP активных Устройств IP сети LAN. Пока Устройство IP сети LAN сохраняет активную аренду DHCP с порталом DCP, и уже обеспечило имя ведущего узла к порталу CDP (в качестве части его процесса приобретения адреса IP), его имя может быть решено порталом CNP. Если имя ведущего узла, затребованное для разрешающей способности, не может быть найдено в объекте cabhCdpLanAddrTable, то портал CNP возвращает DNS направление, которое указывает на внешний сервер DNS (который узнан клиентом CDC через варианты выбора DHCP). Адрес IP внешнего сервера DNS является последней записью объекта cabhCdpWanDataAddrDnsIp в объекте cabhCdpWanDataAddrServerTable портала CDP.

Стандартный вопрос DNS указывает название целевого домена (QNAME), тип вопроса (QTYPE) и класс вопроса (QCLASS) и запрашивает Записи ресурсов, которые совпадают. Портал CNP будет откликаться на вопросы DNS с помощью QCLASS = IN и QTYPE = A, NS, SOA или PTR, как определено в документе [RFC 1035]. Поддержка переносов зон и системы DNS через протокол TCP не требуется.

Поскольку портал CNP является официальным сервером DNS внутри области LAN-Trans, он будет обеспечивать записи "Начало полномочий" (*SOA, Start of Authority*) и "Официальный сервер имени" (*NS, Nameserver*) по запросу. Таблица 28 является примером полей записей SOA (см. секцию 3.3.13 документа [RFC 1035]).

Таблица 28/J.191 – Поля записей SOA

Поле RFC 1035 RDATA	Объект MIB портала CDP
MNAME	cabhCdpServerDomainName
RNAME	Не указывается
SERIAL[*порядковый*]	Не указывается
REFRESH [*обновить*]	Не указывается
RETRY [*повторная попытка*]	Не указывается
EXPIRE [*истечение*]	Не указывается
MINIMUM [*минимум*]	Не указывается

Поле MNAME является именем домена адресной области LAN-Trans. Портал CNP использует значение, хранимое в объекте cabhCdpServerDomainName, как имя домена адресной области LAN-Trans.

Поле RNAME является почтовым ящиком ответственной личности для домена. Если услуга PS поддерживает адрес электронной почты для администратора, то эта информация могла быть указана в этом поле.

Поле SERIAL является незнаковым 32-разрядным числом, используемым для определения информации зоны. Но поскольку переносы зон не указываются, значение этого поля не указывается.

9.3 Требования разрешающей способности имени

Портал CNP ОБЯЗАН соответствовать стандартному формату сообщения DNS и поддерживать стандартные вопросы DNS , как описано в документах [RFC 1034, RFC 1035].

Портал CNP является сервером, не имеющим состояния, который ОБЯЗАН быть способен получать вопросы и посылать ответы в пакетах UDP [RFC 768].

Портал CNP ОБЯЗАН действовать, по крайней мере, в не рекурсивном режиме, как определено в документе [RFC 1034].

Портал CNP отвечает на вопросы имен, используя только местную информацию внутри услуги PS, и его ответные сообщения ОБЯЗАНЫ содержать ошибку, ответ или направление к внешнему серверу DNS.

Портал CNP ОБЯЗАН откликаться на вопросы системы DNS, адресованные к объекту cabhCdpServerDnsAddress.

Портал CNP ОБЯЗАН НЕ откликаться на любые вопросы системы DNS, обращенные к адресам IP WAN-Man и WAN-Data услуги PS.

При получении вопроса по разрешающей способности начального имени ведущего узла от Устройства IP сети LAN, портал CNP ОБЯЗАН осуществить доступ к объекту cabhCdpLanAddrTable портала CDP, чтобы отыскать имена ведущих узлов, связанные с адресами IP, которые арендованы для Устройств IP сети LAN.

Независимо от состояния записи объекта cabhCdpWanDataAddrDnsIp в объекте cabhCdpWanDataAddrServerTable портала CDP, если имя ведущего узла может быть разрешено с помощью портала CNP из местных данных, портал CNP ОБЯЗАН откликнуться на вопрос разрешающей способности имени ведущего узла с помощью адреса IP именованного Устройства IP сети LAN.

При функционировании в качестве не рекурсивного сервера DNS: если имя ведущего узла не может быть разрешено порталом CNP из местных данных, И последняя запись

cabhCdpWanDataAddrDnsIP в объекте cabhCdpWanDataAddrServerTable портала CDP заполнена, портал CNP ОБЯЗАН откликнуться на вопрос разрешающей способности имени ведущего узла с помощью направления к внешнему серверу DNS, представленному адресом IP, который содержится в объекте cabhCdpWanDataAddrDnsIp.

Если имя ведущего узла не может быть решено порталом CNP из местных данных, И объект cabhCdpWanDataAddrDnsIp не заполнен, портал CNP ОБЯЗАН откликнуться на вопрос разрешающей способности имени ведущего узла с помощью соответствующей ошибки, указанной документом [RFC 1035].

Когда истекает последняя аренда DHCP WAN-Data, клиент CDC ОБЯЗАН очистить все записи cabhCdpWanDataAddrDnsIp из объекта cabhCdpWanDataAddrServerTable.

Портал CNP ОБЯЗАН откликаться на вопросы DNS типа QCLASS = IN и QTYPE = A, NS, SOA или PTR.

Отклики портала CNP на вопросы DNS ОБЯЗАНЫ соответствовать секции 3.3 документа [RFC 1035], с битом "Официальный ответ", установленным в '1' в Секции заголовка (см. секцию 4.1.1 документа [RFC 1035]).

Поскольку портал CNP является официальным сервером DNS внутри области LAN-Trans, он ОБЯЗАН обеспечивать по запросу записи "Начало полномочий (*SOA, Start of Authority*) и "Официальный сервер имен" (*NS, Nameserver*). Поля записей SOA (см. секцию 3.3.13 документа [RFC 1035]) ОБЯЗАНЫ содержать запись для поля MNAME, которое равно значению объекта MIB cabhCdpServerDomainName портала CDP.

Если объект cabhCdpServerDomainName не установлен, то портал CNP ОБЯЗАН по-прежнему предоставлять услугу направления DNS к Устройствам IP сети LAN.

10 Качество обслуживания

10.1 Введение

Этот раздел описывает роль усовершенствованного Кабельного модема IP в осуществлении домашних приложений, чтобы использовать ресурсы качества QoS модели IPCablecom и спецификации DOCSIS. Эти ресурсы обеспечивают механизм административного управления, который оказывает предпочтение потокам сеансов данных для поддержки такого прикладного трафика реального времени, как VoIP, потоковая передача данных A/V и деловые игры видео, путем уменьшения задержки пакетов и задержек фазовых дрожаний. Механизмы QoS модели IPCablecom и спецификации DOCSIS также позволяют более эффективное административное управление трафиком через сеть HFC.

Качество QoS определяет необходимые требования элементов PS, которые обеспечивают возможность приложениям IPCablecom устанавливать различные уровни качества QoS по сети HFC.

10.1.1 Цели

Цели для качества QoS включают в себя:

- Давать возможность домашним приложениям устанавливать предпочитаемые сеансы передачи данных между системой CMTS и устройством PS, используя обмен сообщениями, соответствующий модели IPCablecom.
- Облегчать разработку и полевые испытания для производства и возможности взаимодействия удовлетворяющих аппаратных и программных средств многими поставщиками.

10.1.2 Предположения

Для качества QoS были сделаны следующие предположения:

- Качество QoS предполагает, что в кабельной сети существуют системы IPCablecom.
- Чтобы избежать проблем с функциями NAT в элементе CAP, приложения, согласующиеся с моделью IPCablecom, будут использовать адресацию LAN-Pass, как определено в разделах 7 и 8.

10.2 Архитектура QoS

Архитектура качества обслуживания (*CQoS, quality-of-service*) складывается из функциональных элементов и класса устройства HA. Разработчики оборудования для создания сетей (например, аппаратного и программного) осуществляют один или более из этих элементов, в зависимости от желаемого набора свойств этих продуктов. Указанные минимальные наборы возможностей требуются для участия в Домене CQoS. Основные элементы CQoS представляются в 10.2.2.

10.2.1 Руководящие принципы разработки системы

Руководящие принципы разработки системы QoS перечисляются в Таблице 29.

Таблица 29/J.191 – Руководящие принципы разработки системы QoS

Номер	Руководящие принципы разработки системы QoS
QoS 1	Будет существовать стандартный механизм сигнализации QoS, который позволяет усовершенствованным Кабельным модемам IP поддерживать установление предпочтительных сеансов услуг через сеть DOCSIS для мультимедийных приложений.
QoS 2	Мультимедийные приложения могут быть встроены в устройство HA или во внешнее устройство, подключенное к устройству HA.
QoS 4	Мультимедийные приложения могут включать в себя услуги IPCablecom (E-MTA/S-MTA).

10.2.2 Описание системы QoS

Архитектура CQoS складывается из следующих объектов:

- Домен CQoS;
- Функция услуг портала (PS);
- Функция "Портал кабельного качества обслуживания" (*CQP, Cable Quality-of-Service Portal*);
- Устройство HA;
- Система CMTS.

Домен CQoS определяет сферу непосредственного влияния функциональных возможностей CQoS, которые расширяются на устройство HA от головного узла кабельной сети. Элементы PS и CQP полностью находятся и указываются внутри Домена CQoS. Домен CQoS существует для обеспечения услуг приложениям, удовлетворяющим модели IPCablecom.

Эталонная архитектура также описывает устройство HA. См. раздел 5.

Система завершения кабельного модема (*CMTS, cable modem termination system*) размещается в головном узле кабельной сети и управляет функциями QoS спецификации DOCSIS.

10.2.2.1 Элемент – Услуги портала

Элемент "Услуги портала" (*PS, Portal Services*) является логическим элементом, который содержит сетевую адресацию, административное управление, безопасность и составные части портала QoS, которые обеспечивают трансляцию функций между сетью HFC и домом. Услуга PS размещается только в устройствах HA (см. раздел 5). Составная часть QoS упоминается как "Портал кабельного качества обслуживания (*CQP, Cable Quality-of-Service Portal*). Портал CQP действует в качестве портала CQoS для приложений, подчиняющихся модели IPCablecom. Его первичная функция состоит в том, чтобы направлять обмен сообщениями QoS между системой CMTS и приложениями IPCablecom.

10.2.2.2 Домен CQoS

Домен CQoS существует на основе каждого дома. Индивидуальные дома являются отдельными и обладают независимыми Доменами CQoS. Элемент CQP ограничивает Домен CQoS внутри заданного дома.

10.2.2.3 Классы физических устройств и функциональные элементы CQoS

Устройства HA содержат логический элемент PS и функциональный элемент CQP. Портал CQP действует в качестве прозрачного моста для обмена сообщениями QoS приложений (*APP, applications*) IPCablecom. Пример взаимоотношения между функциональными элементами CQoS и классом устройства HA представляется на Рисунке 22.

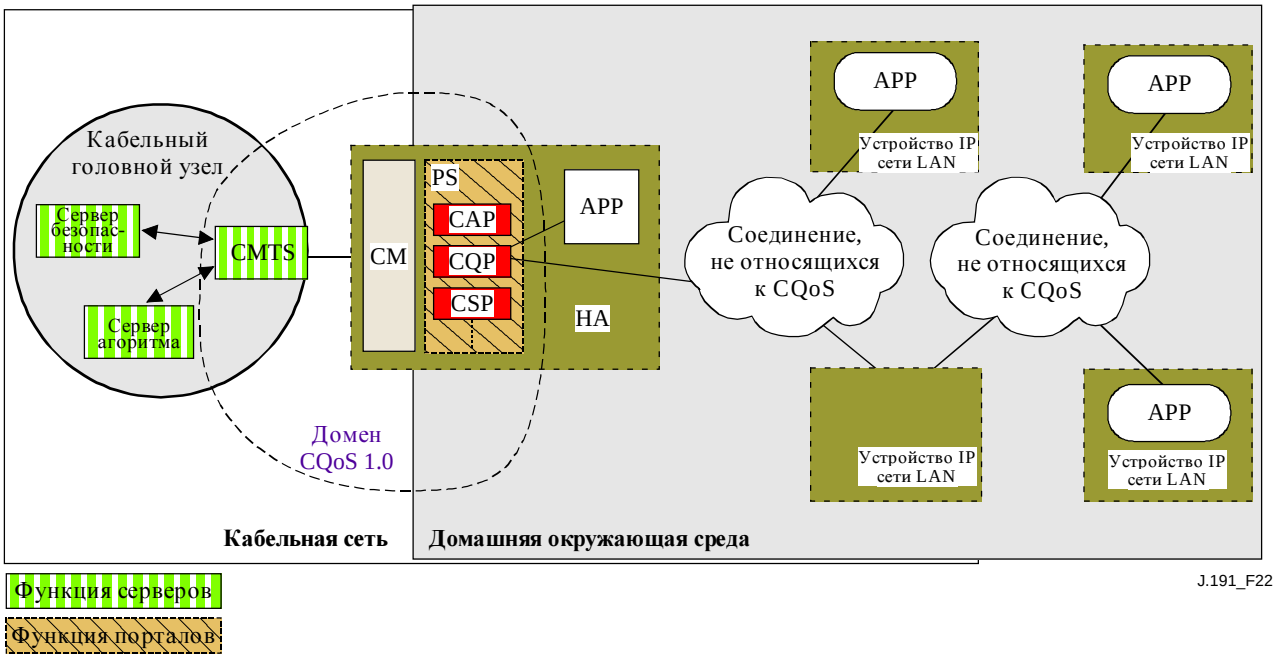


Рисунок 22/J.191 – Пример функциональных элементов CQoS

10.3 Требования по обмену сообщениями кабельного QOS

Архитектура QoS (CQoS) состоит из функционального элемента CQP в домене CQoS. Портал CQP существует в услуге PS и поддерживает доставку при обмене сообщениями QoS через сеть HFC для приложений IPCablecom. Обмен сообщениями, удовлетворяющими модели IPCablecom, включает в себя обмен сообщениями QoS и другими сообщениями, относящимися к аспектам конкретной услуги, например, алгоритмические решения и использование моделей двухфазного резервирования.

Функциональные требования для портала CQP и других элементов CQoS определяются в следующих подразделах.

10.3.1 Требования CQP

Портал CQP ОБЯЗАН действовать в качестве прозрачного моста и направлять обмен сообщениями QoS IPCablecom (Рекомендации МСЭ-Т J.161 и J.163) между системой CMTS и приложениями IPCablecom. Прикладные данные связываются с потоком услуги DOCSIS согласно классификатору, который создается в интерфейсе CM на основе информации, включенной в сообщения IPCablecom (такие, как RSVP PATH [*тракт*]).

Так как требование портала CQP состоит в том, чтобы только направлять обмен сообщениями QoS модели IPCablecom, то нет никакой зависимости от системы NMS для поддержания этой функции. Поэтому эта функция CQP остается той же самой и для режима обеспечения DHCP, и для режима обеспечения SNMP (см. 5.7).

10.3.2 Административное управление алгоритмом QoS и управление доступом

Обмен сообщениями QoS определяется Рекомендациями по модели IPCablecom (Рекомендации МСЭ-Т J.161 и J.163). По существу, административное управление алгоритмом QoS и функции управления доступом также определяются такими Рекомендациями модели IPCablecom.

11 Безопасность

11.1 Введение/Обзор

Этот раздел определяет интерфейсы безопасности, протоколы и функциональные требования, необходимые для того, чтобы надежно доставлять основанные на кабеле услуги IP к услуге PS в безопасной окружающей среде.

Поддержка поставки надежных мультимедийных услуг IP к устройствам клиентов в доме требует безопасного механизма, который защищает эти услуги от незаконного доступа, наблюдения и разрушения. Цель любой технологии безопасности состоит в том, чтобы защитить ценность, либо потока дохода, либо информационный актив некоторого типа, который может быть куплен. Угрозы этому потоку дохода существуют тогда, когда пользователь сети чувствует ценность, расходует усилие и деньги, и изобретает технику, чтобы обойти создание необходимых платежей (См. Дополнение C). Некоторые пользователи сети пойдут далеко, чтобы украсть, когда они чувствуют чрезвычайную ценность. Дополнение технологии безопасности, чтобы защитить ценность, имеет связанную стоимость; чем больше израсходовано денег, тем больше безопасность (эффективность безопасности, таким образом, является основной экономикой).

11.1.1 Цели

Цели для модели безопасности будут включать в себя:

- Использовать эффективную по стоимости технологию безопасности, чтобы вынудить любого пользователя, намеревающего украсть или разрушить услуги сети, потратить неблагоразумную сумму денег или времени.
- Защитить домашние соединения, используемые для предложения высокоценных услуг на основе кабеля так, чтобы это было, по крайней мере, столь же безопасным, как технологии DOCSIS и IPCablecom на гибридной волоконно-коаксиальной сети (*HFC, hybrid fiber-coax*).
- обеспечить гибкие механизмы безопасности, чтобы быть совместимым с механизмами безопасности DOCSIS и IPCablecom, используемыми на сети HFC.

11.1.2 Предположения

Предположения по безопасной окружающей среде включают в себя:

- Функциональные возможности PS и CM находятся в единственном физическом устройстве.
- В доме могут существовать более низкие уровни безопасности, когда считается, что предоставляемые услуги обладают низкой ценностью.

11.2 Архитектура безопасности

Архитектура безопасности основана на общей архитектуре, как определено в разделе 5. Архитектура определяет элемент Портала IPService (*PS, Service Portal*), который включает в себя функции Административного управления/Обеспечения, Безопасности и качества QoS.

Архитектура также включает в себя набор элементов головных узлов. Эти элементы включают в себя Систему завершения кабельного модема (*CMTS, Cable Modem Termination System*), сервер Протокола динамической конфигурации ведущего узла (*DHCP, Dynamic Host Configuration Protocol*), сервер Сетевого административного управления, сервер Безопасности и пр.

Спецификация безопасности сосредотачивается на определении, функциональных возможностях и интерфейсах функций безопасности и на серверах головных узлов, относящихся к безопасности.

11.2.1 Руководящие принципы разработки системы

Требования по разработке безопасности перечисляются в Таблице 30. Этот перечень предоставил руководящие принципы для развития спецификации безопасности.

Этот раздел ограничивает свою сферу применения до этих первичных требований безопасности системы, но признает, что в некоторых случаях может быть желательной дополнительная безопасность. Озабоченности индивидуальных операторов или изготовителей могут привести к дополнительным средствам по защите безопасности. Эта Рекомендация не ограничивает использование дальнейших средств защиты, пока они не находятся в противоречии с намерением и руководящими принципами этой Рекомендации.

Таблица 30/J.191 – Руководящие принципы разработки системы безопасности

Ссылка	Руководящие принципы разработки системы безопасности
SEC1	Оператор будет обладать способностью дистанционно управлять подчиняющимися продуктами межсетевой защиты.
SEC2	В разработку системы безопасности будет включен интерфейс регистрации события межсетевой защиты /обмена сообщениями, который позволяет оператору наблюдать и пересматривать активность средств межсетевой защиты.
SEC3	Будут удостоверены и на дополнительной основе зашифрованы, чтобы защитить от несанкционированного наблюдения и управления, сообщения административного управления средствами межсетевой защиты между кабельным головным узлом и услугой PS.
SEC4	В разработку системы безопасности будет включено взаимное удостоверение подлинности элементов.
SEC5	Уровень домашней безопасности будет таким, что среднему абоненту будет нелегко получать несанкционированный доступ к сети HFC и услугам на основе кабеля.
SEC6	При установлении счета абонента будет автоматическим удостоверение подлинности услуги PS с системой обеспечения оператора.
SEC7	Оператор будет обладать возможностью безопасно загружать из главной системы к

Таблица 30/J.191 – Руководящие принципы разработки системы безопасности

Ссылка	Руководящие принципы разработки системы безопасности
	элементу PS изображения программного обеспечения, файлы конфигурации и наборы правил межсетевой защиты.
SEC8	Безопасность будет обеспечивать необходимую поддержку для качества DQoS, гарантированного моделью IPCablecom через средства межсетевой защиты.
SEC9	Для защиты от несанкционированного наблюдения и управления будут удостоверены и на дополнительной основе зашифрованы сообщения сетевого административного управления между кабельным головным узлом и услугой PS.

11.2.2 Описание системы

Следующие подразделы обеспечивают обзор всех элементов, которые являются частями архитектуры безопасности.

Архитектура безопасности включает в себя следующие элементы безопасности:

- Домен безопасности;
- Функцию портала IPService (*PS, Service Portal*);
- Функцию "Портал кабельной безопасности" (*CSP, Cable Security Portal*);
- Средства межсетевой защиты (*FW, Firewall*);
- Сервер безопасности.

Домен безопасности определяет границу сферы прямого влияния, где функциональные возможности безопасности расширены на услугу PS от головного узла кабельной сети. Элементы PS, CSP и FW полностью находятся в пределах Домена безопасности. Элемент PS содержит адресацию сети, административное управление и функции портала безопасности. Портал CSP действует как граничный элемент между Доменом безопасности и небезопасным доменом. Домен безопасности существует, чтобы обеспечивать услуги безопасности подчиняющимся устройствам.

Эти элементы содержат конкретные функциональные возможности клиента, сервера или портала и могут существовать в различных типах физических устройств. Архитектура определяет класс устройства HA. Пример взаимоотношения между различными элементами безопасности и классами устройств HA представляется на Рисунке 23. На рисунке, внутридомовые приложения представлены как APP, а сервер OSS является сервером системы NMS.

11.2.2.1 Домен безопасности

Домен безопасности определяется на Рисунке 23 и осуществляет элемент PS в HA и иллюстрированные серверы головных узлов.

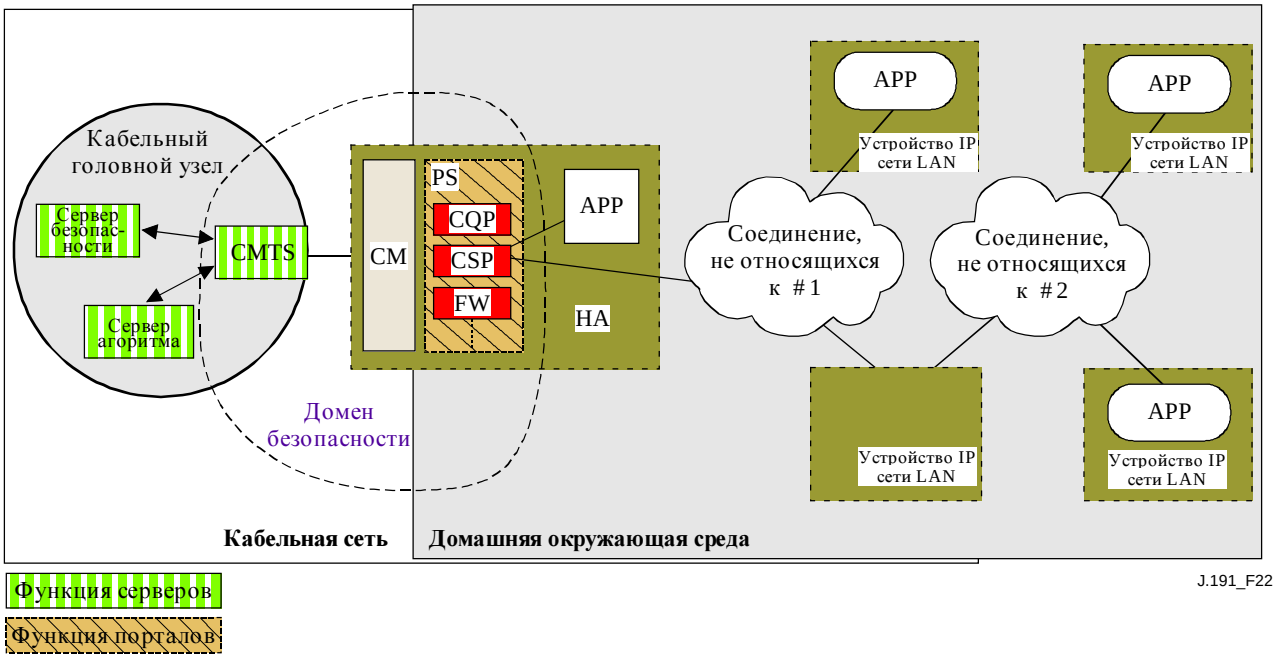


Рисунок 23/J.191 – Элементы безопасности

11.2.2.2 Функция услуги PS

Услуга портала (*PS, Portal Service*) является логическим элементом, который содержит сетевую адресацию, административное управление и функции портала безопасности. Она размещается только в устройствах HA. Услуга PS включает в себя следующие элементы:

- Портал кабельной безопасности (*CSP, Cable Security Portal*);
- Средства межсетевой защиты (*FW, Firewall*).

Портал CSP действует как портал безопасности для других элементов PS. Одна из его первичных функций состоит в том, чтобы направлять обмен сообщениями безопасности между серверами OSS главных узлов (включая сервер безопасности) и приложениями IPCablecom. Для элемента PS портал CSP также обеспечивает такие услуги безопасности, как удостоверение подлинности и административное управление ключом.

Услуга PS также включает в себя функциональные возможности средств межсетевой защиты. Средства межсетевой защиты обеспечивают защиту пользователю, а также сети HFC, от нежелательного трафика, прибывающего от доменов сетей WAN или LAN. Такой трафик может включать предумышленные атаки на внутридомовую сеть, а также на ограничение трафика для родительских приложений управления.

Спецификация безопасности не определяет подробную спецификацию для осуществления средств межсетевой защиты, но будет взамен этого определять набор требований для обеспечения дистанционного административного управления с помощью оператора.

Как правило, средства межсетевой защиты построены, используя комбинацию двух различных компонентов: сервер посредника и фильтрование пакетов. Модуль фильтрования пакетов является, вероятно, самым обычным компонентом средств межсетевой защиты, потому что он определяет, какие потоки пакетов блокируются, а каким разрешено пересечь средства межсетевой защиты. Каждое индивидуальное решение, сбрасывающее пакет, основывается на статической информации конфигурации, которая дает полномочия на осмотр полей заголовка пакета, включая: адреса IP источника и пункта назначения, номера портов протокола источника и пункта назначения, тип протокола и т.д. В зависимости от

желательного уровня безопасности, вероятно, придется формировать большое число фильтров на средствах межсетевой защиты, которые могут быть очень трудными, требуя хорошего понимания типа услуг (протоколов), подлежащих фильтрованию.

Посредник, характерный для приложения (*ASP, application-specific proxy*), другая типичная составная средств межсетевой защиты, создает конечную точку и переприем протокола путем осуществления необходимого клиента и частей серверов определенного протокола "клиент-сервер". Есть выгоды безопасности в использовании посредников ASP. Например, возможно добавлять перечни управления доступом к протоколам, требуя от пользователей или систем обеспечивать некоторый уровень удостоверения подлинности прежде, чем предоставляется доступ. Кроме того, будучи определенным протоколом, посредник ASP понимает протокол и может формироваться так, чтобы блокировать только подразделы протокола. Например, посредник ASP протокола FTP может формироваться так, чтобы блокировать трафик от несанкционированных пользователей, предоставляя в то же время санкционированным пользователям избирательный доступ к командам "put" [*поместить*] и "get" [*получить*], скажем, в зависимости от того, на каком направлении эти команды выпускаются.

Конкретная комбинация средств навигации по файловой системе пакетов и посредников ASP на заданном изделии межсетевой защиты составляет компромисс между показателями качества и уровнем безопасности, который дарят средства межсетевой защиты. Обычно, будучи механизмом сетевого уровня, фильтры пакетов имеют тенденцию приводить к лучшим показателям качества, чем посредники ASP, которые являются механизмами прикладного уровня. Компромиссное решение, становящееся все более и более популярным, состоит в использовании фильтрования пакетов с изменением состояния в процессе исполнения (*SPF, stateful packet filtering*), где информация состояния накапливается из пакетов, которые принадлежат тому же самому соединению, и используется в создании решения, опускающего пакет.

Статическое фильтрование или фильтрование SPF и посредники ASP в средствах межсетевой защиты являются, в конечном счете, ручками управления, которые алгоритм безопасности использует для того, чтобы осуществлять желательный уровень безопасности для сайта. Однако в то время как алгоритм безопасности определяет разрешенные услуги и путь, которым они используются через средства межсетевой защиты, алгоритм безопасности не влечет за собой конкретную конфигурацию для средств межсетевой защиты. Он является набором правил, полученным из алгоритма безопасности, который определяет собрание правил управления доступом (правила действия фильтра и посредника), который затем определяет, какие пакеты средства межсетевой защиты направляют, а какие они отклоняют. Большая проблема состоит в получении набора правил от заявлений в алгоритме безопасности, который обычно выражается на человеческом языке высокого уровня.

Поскольку средство межсетевой защиты нуждается только в наборе правил, чтобы формировать свои компоненты SPF и ASP, определение алгоритма безопасности и извлечение соответствующих наборов правил рассматриваются вне сферы применения средств межсетевой защиты. Соответствующий набор правил должен формироваться в средствах межсетевой защиты через санкционированную загрузку файла конфигурации средств межсетевой защиты. Фактический формат для файла, содержащего набор правил, применимых к конкретному продукту средств межсетевой защиты, и как такой файл используется в средствах межсетевой защиты, чтобы формировать компоненты SPF и ASP, является зависящим от осуществления. Эта Рекомендация обращается только к механизму удостоверения подлинности, используемому в загрузке набора правил межсетевой защиты к элементу PS.

Рисунок 24 иллюстрирует взаимоотношение среди составных частей межсетевой защиты. В частности, рисунок предлагает, что должен использоваться набор правил (*RS, rule set*) для внутренней конфигурации всех составных частей межсетевой защиты. Эти составные части

состоят из функций фильтра прибывающего пакета (*IPF, inbound packet filter*), фильтра убывающего пакета (*OPF, outbound packet filter*) и посредника конкретных приложений (*ASP, applications specific proxy*) или фильтра пакетов с изменением состояния в процессе исполнения (*SPF, stateful packet filter*). Рисунок 24 также предоставляет более подробный обзор услуги PS, и ее отношение к функциям межсетевой защиты и другим составным частям в устройстве HA. В частности, рисунок предлагает, чтобы функция Посредника, характерного для приложения/Фильтрования пакетов с изменением состояния в процессе исполнения (*ASP/SPF, Application-Specific Proxy/Stateful Packet Filtering*), была глубоко связана с функцией "Трансляция сетевого адреса" (NAT, *Network Address Translation*) портала CAP. Поскольку функция NAT ломает некоторые приложения, требуется обработка, характерная для приложения, как часть осуществления NAT и, поэтому, осуществление услуги PS МОЖЕТ объединять функции ASP/SPF и NAT.

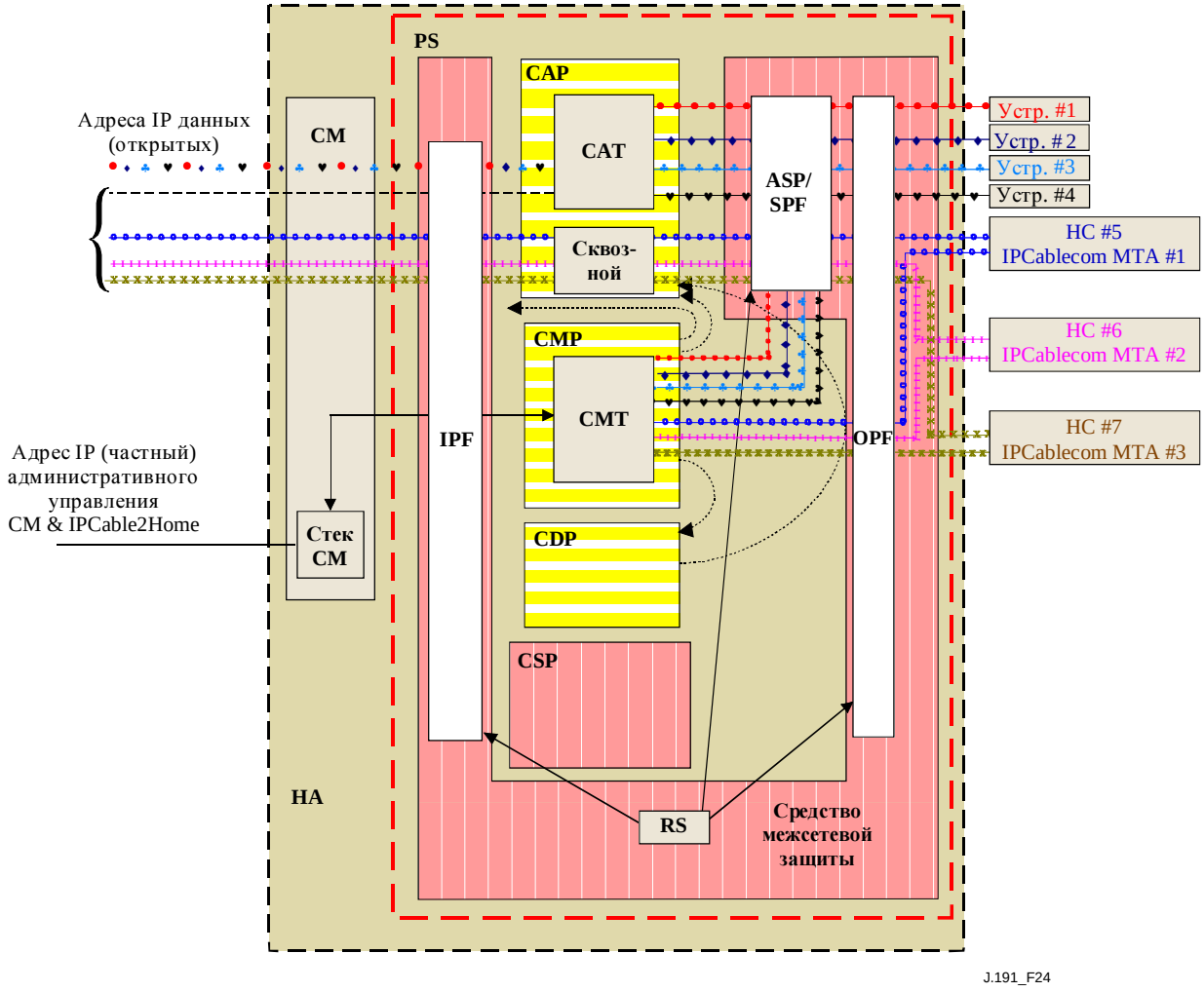


Рисунок 24/J.191 – Пример элемента PS в устройстве HA

11.2.3 Сервер центра распределения ключей (KDC)

Поддерживаемый сервер Безопасности является сервером "Центр распределения ключей" (*KDC, Key Distribution Center*). Если сервер KDC, который поддерживает, имеется в головном узле, то он будет использован для обеспечения услуг установления подлинности и распределения ключей с использованием протокола Kerberos [*система "Цербер"*]. Если он имеется, то центр KDC будет осуществлять связь с функцией CSP для установления этих услуг.

11.2.4 Другие связанные элементы и функции

Следующие далее элементы не рассматриваются в качестве элементов безопасности, но должны использоваться или принимать участие в административном управлении этими услугами безопасности.

- OSS;
- CMP.

Система OSS представляет набор серверов головных узлов, которые обеспечивают административное управление элементами в доме. Серверы OSS осуществляют связь с порталом CMP, чтобы управлять функциями безопасности и услугами. Звено между системой OSS и порталом CMP гарантируется с использованием услуг удостоверения подлинности и секретности, определенных в этой Рекомендации.

Портал CMP является функцией административного управления внутри услуги PS. Архитектура безопасности обеспечивает установление подлинности и другие услуги безопасности для своей связи с серверами OSS в головном узле. Портал CMP обеспечивает административное управление функциями PS, включая административное управление услугами безопасности.

Дальнейшие подробности этих элементов и их функций можно найти в разделах 12 и 13, а также в разделе 10 (QoS).

11.3 Требования

Для всех ссылок на безопасность модели IPCablecom, пожалуйста, обращайтесь к Рекомендации МСЭ-Т J.170.

11.3.1 Удостоверение подлинности элемента

Для целей безопасности, до обмена любой значащей информацией, важно знать, с кем вы осуществляете связь. Удостоверение подлинности обеспечивает средства для надежной идентификации неизвестных сторон, которые желают осуществлять связь. Имеются три части по удостоверению подлинности: мандат именования, проверка мандата именования для законности и обычные средства для передачи информации именования. Эта Рекомендация определяет мандат идентификации стандарта промышленности, использование сертификатов X.509 в соединении с документом [RFC 2459]. Сертификат элемента PS обеспечивает именование связанного элемента PS путем шифрованного связывания адреса MAC элемента PS с сертификатом открытого ключа, выпущенного для такого элемента PS. Кроме того, сертификаты открытых ключей обеспечивают безопасный способ сообщать информацию именования.

Когда центр KDC, который поддерживает это приложение, доступен в головном узле, удостоверение подлинности поддерживается. Если центр KDC доступен, то рекомендуется чтобы обеспечение кабельным оператором элемента PS в режиме обеспечения SNMP (как описано в 5.1) использовало в своих интересах указанный взаимный опознавательный протокол с применением системы Kerberos ("*Цербер*"), применяя расширение PKINIT. Система Kerberos обеспечивает протокол для безопасного взаимного удостоверения подлинности, чтобы обеспечивать манипуляцию материалом и учреждение связи только между заверенными сторонами. Поскольку эта модель установления подлинности была уже определена моделью IPCablecom, эта Рекомендация ссылается на модель IPCablecom, когда это соответствует.

11.3.1.1 Kerberos/PKINIT

Когда элемент PS обеспечивается в режиме обеспечения SNMP, эта Рекомендация определяет использование системы Kerberos с расширением открытого ключа PKINIT для удостоверения подлинности и для поддержки требований по административному управлению ключами.

Элементы (клиенты) подтверждают свою подлинность центру KDC с помощью протокола PKINIT. После удостоверения подлинности центру KDC клиенты могут получить билет Kerberos для того, чтобы подтвердить свою подлинность конкретному серверу.

Обеспеченное удостоверение подлинности центра KDC ОБЯЗАНО следовать спецификации для системы Kerberos/PKINIT как определено в Рекомендации МСЭ-Т J.170. Центр KDC эквивалентен или является тем же самым, что и центр KDC оператора IPCablecom (IPCablecom определяет использование нескольких центров KDC). Элемент PS ОБЯЗАН действовать как клиент по отношению к центру KDC. В Рекомендации по безопасности IPCablecom адаптер MTA является клиентом. Ожидается, что реализации будут использовать функциональные возможности клиента, указанные для адаптера MTA для элемента PS. Элемент PS использует систему Kerberos для протокола SNMP. Сертификаты, используемые в PKINIT, определены в 11.3.2. Там, где модель IPCablecom указывает сертификат устройства MTA, эта Рекомендация обеспечивает сертификат для элемента PS (Сертификат элемента PS), а осуществления элементов PS ОБЯЗАНЫ включать в себя Сертификат элемента PS.

Безопасность модели IPCablecom не применяется к этой Рекомендации для следующих функциональных возможностей системы Kerberos:

1) Управление версиями ключа услуги (см. 6.4.10/J.170);

2) Действие системы Kerberos через область (см. 6.4.11/J.170);

3) Сообщения ретрансляции (см. 6.5.4/J.170);

4) IPsec, охваченное системой Kerberos (см. 6.5.6/J.170);

5) Местоположения серверов системы Kerberos и соглашения по присваиванию имен (см. 6.4.6.3, CMS).

11.3.1.2 Особые переменные величины удостоверения подлинности

Модель IPCablecom указывает некоторые особые имена переменных величин для системы Kerberos в Сетевой архитектуре IPCablecom. Для того чтобы для этой Рекомендации использовать модель IPCablecom, нужно изменить следующие имена переменных величин:

- Заменить pktcKdcToMtaMaxClockSkew, как определено в Спецификации безопасности IPCablecom, с помощью KdcToClientMaxClockSkew.
- Заменить pktcSrvrToMtaMaxClockSkew, как определено в Спецификации безопасности IPCablecom, с помощью SrvrToClientMaxClockSkew.
- Заменить MTAProvSrvr, как определено в Спецификации безопасности IPCablecom, с помощью ProvSrvr.
- Заменить MTA-FQDN-Map, как определено в Спецификации безопасности IPCablecom, с помощью FQDN-Map.

Реализации Kerberos ОБЯЗАНЫ игнорировать часть поля Идентификатора объекта (*OID, Object Identifier*), которая читается как clabProjPacketCable (2) внутри объекта AppSpecificTypedData в составе сообщений KRB-ERROR [*ошибка*].

11.3.2 Инфраструктура открытого ключа (PKI)

Эта Рекомендация использует сертификаты открытых ключей, которые соответствуют спецификации Рекомендации МСЭ-Т X.509 и документа IETF [RFC 3280].

11.3.2.1 Общая структура

11.3.2.1.1 Версия

Версия сертификатов ОБЯЗАНА быть согласно X.509 v3, как отмечено в качестве v2 в фактическом сертификате (потому что v1 не имела никакого связанной версии нумерации). Все сертификаты ОБЯЗАНЫ удовлетворять документу [RFC 3280], за исключением случаев,

где несоблюдение документа RFC явно заявлено в этом разделе. Любой запрос несоблюдения в соответствии с этой Рекомендацией для содержимого не подразумевает несоблюдение для формата. Любой определенный запрос несоблюдения для формата будет явно описан.

11.3.2.1.2 Тип открытого ключа

По всем иерархиям сертификатов, описанным в 11.3.2.2, используются Открытые ключи RSA. Используемый идентификатор OID subjectPublicKeyInfo.algorithm ОБЯЗАН быть 1.2.840.113549.1.1.1 (rsaEncryption).

Открытым представителем для всех ключей RSA ОБЯЗАНО быть F4 – 65537.

11.3.2.1.3 Расширения

Расширения (subjectKeyIdentifier, authorityKeyIdentifier, KeyUsage, BasicConstraints, Алгоритм подписи, SubjectName and IssuerName) ОБЯЗАНЫ следовать документу [RFC 3280]. Любые другие расширения сертификатов МОГУТ быть также включены как некритические. Этикетками кодирования являются ["c":критическое, "n":некритическое; "m":обязательное, "o":дополнительное] и эти этикетки определяются в таблице для каждого сертификата.

11.3.2.1.3.1 subjectKeyIdentifier

Расширение subjectKeyIdentifier, включенное во все сертификаты, как это требуется документом [RFC 3280] (например, все сертификаты, кроме сертификатов устройств и вспомогательных сертификатов), ОБЯЗАНО включать в себя значение keyIdentifier, сложенное из 160-разрядных случайных данных SHA-1 от значения subjectPublicKey СТРОКА БИТОВ (исключая этикетку, длину и число неиспользуемых битов из кодирования ASN.1) (см. документ [RFC 3280]).

11.3.2.1.3.2 authorityKeyIdentifier

Расширение authorityKeyIdentifie, включенное во все сертификаты, как это требуется документом [RFC 3280], ОБЯЗАНО включать в себя subjectKeyIdentifier из сертификата запрашивающей стороны (см. документ [RFC 3280]).

11.3.2.1.3.3 KeyUsage

Расширение keyUsage ОБЯЗАНО быть использовано для всех сертификатов класса "Полномочия сертификатов" (*CA, Certification Authority*) и Сертификатов проверки кода (*CVC, Code Verification Certificates*). Для сертификатов CA расширение keyUsage ОБЯЗАНО быть маркировано как критическое, со значением keyCertSign и cRLSign. Для сертификатов CVC расширение keyUsage ОБЯЗАНО быть маркировано как критическое, со значением digitalSignature и keyEncipherment. Сертификаты конечного объекта могут использовать расширение keyUsage, как перечислено в документе [RFC 3280].

11.3.2.1.3.4 Основные ограничения

Расширение basicConstraints ОБЯЗАНО быть использовано для всех сертификатов CA и CVC и ОБЯЗАНО быть маркировано как критическое. Значения для каждого сертификата для объекта basicConstraints ОБЯЗАНО быть маркировано так, как указано в описании сертификата (Таблицы с 31 по 42).

11.3.2.1.4 Алгоритм подписи

Используемым алгоритмом подписи ОБЯЗАНО быть SHA-1 с Шифрованием RSA. Особый идентификатор OID составляет 1.2.840.113549.1.1.5.

11.3.2.1.5 SubjectName и IssuerName

Если строка не может быть закодирована как PrintableString, она ОБЯЗАНА быть закодирована как UTF8String (этикетка [UNIVERSAL 12] [*универсальная*]).

При кодировании Имени X.500:

- каждый объект RelativeDistinguishedName (RDN) ОБЯЗАН содержать только единственный элемент в наборе атрибутов X.500;
- порядок названий RDN в имени X.500 ОБЯЗАН быть таким же, как порядок, в котором они представляются в этой Рекомендации.

11.3.2.2 Иерархии сертификатов

Есть три отдельные используемые иерархии сертификатов. Цепь изготовителя используется, чтобы идентифицировать санкционированных изготовителей; Цепь проверки кода используется, чтобы идентифицировать подчиняющиеся изображения программного обеспечения; Цепь поставщика услуги используется, чтобы идентифицировать устройства на сети поставщика услуги для взаимного удостоверения подлинности к устройствам абонента.

Иерархии сертификатов являются родовыми по характеру и применимыми ко всем приложениям, нуждающимся в сертификатах. Это означает, что основная инфраструктура может многократно использоваться для каждого приложения (DOCSIS, IPCablecom, PS). Могут быть различия в сертификатах конечного объекта, требуемых для каждого проекта, но в случаях, где сертификаты конечных объектов перекрываются, мог бы использоваться один сертификат конечного объекта, чтобы поддерживать перекрывание. Например, модель IPCablecom требует центр KDC для поставщика услуги, и эта Рекомендация может использовать в своих интересах центр KDC, который поддерживает модель IPCablecom, чтобы обеспечивать взаимное удостоверение подлинности. Если поставщик услуги на своих системах управляет обеими сетевыми архитектурами, они могут использовать тот же самый центр KDC и тот же самый сертификат KDC для связи на обеих системах, т. е., модель IPCablecom и это приложение. В этом случае этот прикладной центр KDC эквивалентен или является тем же самым, как центр KDC оператора IPCablecom (модель IPCablecom указывает использование нескольких центров KDC).

На Рисунке 25 термин "Полномочия сертификата "сокращен как CA, "Сертификат проверки кода " сокращен как CVC.

11.3.2.2.1 Иерархия сертификатов производителей

Иерархия сертификатов Производителя, или цепь Производителя, внедрена в CA Корня производителя, что используется для выпуска сертификатов "Полномочия сертификатов производителя" (*CA, Certificate Authority*) для набора санкционированных производителей. Производители используют свои CA, чтобы выпускать индивидуальные Сертификаты элемента PS. Эта цепь используется для удостоверения подлинности устройств в доме.

Информация, содержавшаяся в следующих таблицах, представляет собой определенные значения для требуемых полей согласно документу [RFC 3280]. Эти определенные значения для иерархии Сертификатов производителя ОБЯЗАНЫ следовать согласно Таблицам с 31 по 33. Если требуемое поле конкретно не внесено в список в таблицах, то ОБЯЗАНЫ следовать руководящим принципам, изложенным в документе [RFC 3280]. Родовые расширения также ОБЯЗАНЫ быть включены, как определено в 11.3.2 (PKI).

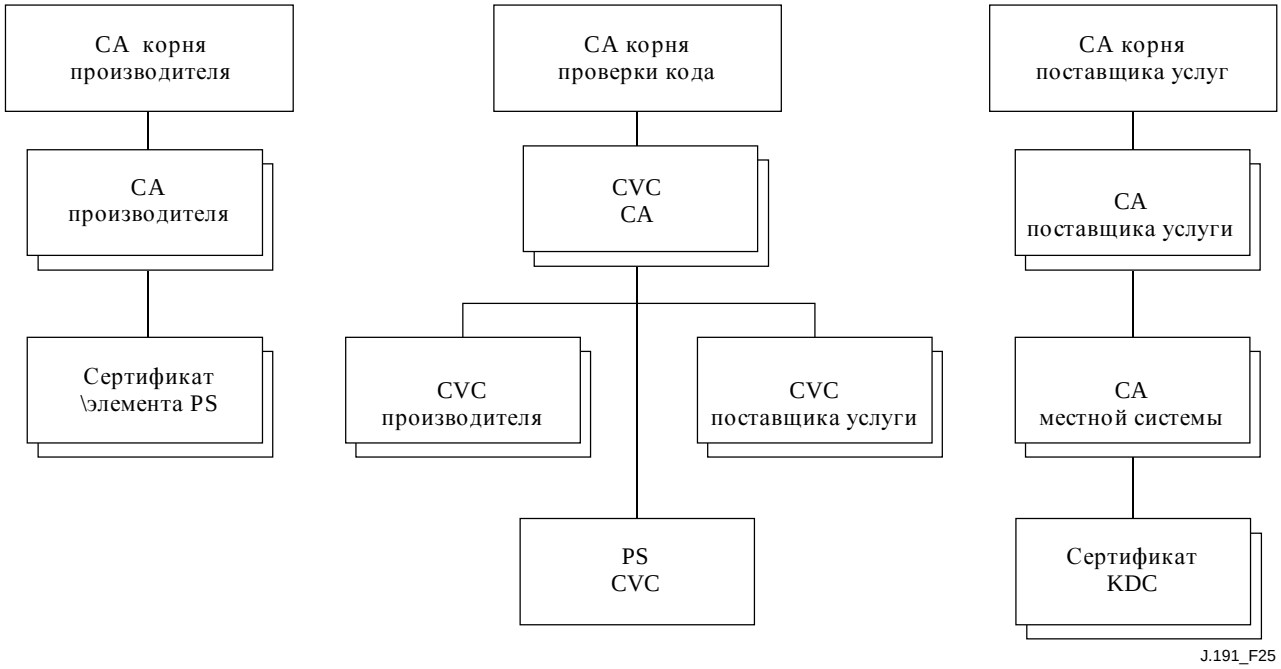


Рисунок 25/J.191 – Иерархия сертификатов

11.3.2.2.1.1 Сертификат CA корня производителя

Сертификат CA корня производителя (см. Таблицу 31) ОБЯЗАН быть проверен как часть цепи сертификатов, содержащей Сертификат CA корня производителя, Сертификат CA производителя и Сертификат элемента PS.

Таблица 31/J.191 – Сертификат CA корня производителя

Форма имени субъекта	C = <страна>, O = , CN = CA корня производителя
Предназначенное использование	Этот сертификат используется для выпуска Сертификатов CA производителя.
Подписано	Самоподписанный
Период действительности	20+ лет. Планируется, что период действительности достаточно длинен, чтобы этот сертификат никогда не переиздавался.
Длина модуля	2048
Расширения	keyusage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true) [*истинно*]

11.3.2.2.1.2 Сертификат CA производителя

Сертификат CA производителя (см. Таблицу 32) ОБЯЗАН быть проверен как часть цепи сертификатов, содержащей Сертификат CA корня производителя, Сертификат CA производителя и Сертификат элемента PS.

Государство/провинция, город и свойство производителя являются дополнительными атрибутами. Производитель может иметь более одного сертификата CA производителя. Если производитель использует более одного сертификата CA производителя, то элемент PS ОБЯЗАН иметь доступ к соответствующему сертификату, как проверено путем соответствия имени выпускающей стороны в Сертификате элемента PS с именем субъекта в Сертификате

CA производителя. Если присутствует, объект authorityKeyIdentifier Сертификата элемента PS ОБЯЗАН быть согласован с объектом subjectKeyIdentifier сертификата производителя, как описано в документе [RFC 3280].

Таблица 32/J.191 – Сертификат CA производителя

Форма имени субъекта	C = <страна>, O = <Название компании>, [S = <государство/провинция>,] [L = <город>,] OU = , [OU = <Свойство производителя>,] CN = <Название компании> Mfg CA
Предназначенное использование	Этот сертификат выпускается каждому Производителю с помощью CA Корня производителя и может быть предоставлен каждому элементу PS либо во время производства, либо во время обновления кода поля. Этот сертификат появляется как параметр "только для чтения" в базе MIB элемента PS. Этот сертификат выпускает Сертификаты элемента PS. Этот сертификат, наряду с Сертификатом CA корня производителя и Сертификатом элемента PS, используется для удостоверения подлинности именования элемента PS.
Подписано	CA Корня производителя
Период действительности	20 лет
Длина модуля	2048
Расширения	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier basicConstraints[c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.1.3 Сертификат элемента PS

Сертификат элемента PS ОБЯЗАН быть проверен как часть цепи сертификатов, содержащей Сертификат CA корня производителя, Сертификат CA производителя и Сертификат элемента PS.

Государство/провинция, город и свойство производителя являются дополнительными атрибутами.

Адрес MAC элемента PS ОБЯЗАН быть выражен как шесть пар 16-ричных чисел, разделенных двоеточиями, например, "00:60:21:A5:0A:23". Знаки HEX альфа (A-F) ОБЯЗАНЫ быть выражены буквами верхнего регистра.

Сертификат элемента PS постоянно установлен и не является обновляемым или заменяемым. Поэтому Сертификат элемента PS ОБЯЗАН иметь период действительности больше, чем эксплуатационная продолжительность времени конкретного устройства (см. Таблицу 33).

11.3.2.2.2 Иерархия сертификата проверки кода

Иерархия Сертификата проверки кода (*CVC Code Verification Certificate*), или цепь проверки кода внедрена в CA Корня проверки кода, который выпускает сертификат CA Проверки кода. CA проверки кода используется для выпуска сертификатов CVC к набору санкционированных производителей и поставщиков услуг. CA проверки кода также выпускает сертификат CVC. Эта цепь специально используется для удостоверения загрузок программного обеспечения. Инфраструктура PKI учитывает сертификаты CVC производителя, сертификат CVC и сертификаты CVC Поставщика услуги.

Таблица 33/J.191 – Сертификат устройства

Форма имени субъекта	C = <страна>, O = <Название компании>, [S = <государство/провинция>,] [L = <город>], OU = [OU = <Название продукта>,] [OU = <Свойство производителя>,] CN = <Адрес MAC>
Предназначенное использование	Этот сертификат выпускается с помощью CA Производителя и устанавливается на фабрике. Сервер NMS не может обновлять этот сертификат. Этот сертификат проявляется как параметр "только для чтения" в базе MIB элемента PS. Этот сертификат используется для удостоверения подлинности именования элемента PS .
Подписано	CA Производителя
Период действительности	20 лет
Длина модуля	2048
Расширения	keyUsage[n, o](digitalSignature, keyEncipherment), authorityKeyIdentifier, Расширение keyUsage является дополнительным. Когда расширение keyUsage используется, его СЛЕДУЕТ маркировать как некритическое.

Информация, содержавшаяся в следующих таблицах, представляет собой определенные значения для требуемых полей согласно документу [RFC 3280]. Эти определенные значения для иерархии Сертификата проверки кода ОБЯЗАНЫ следовать согласно Таблицам с 34 по 38. Если требуемое поле определенно не внесено в список в таблицах, тогда ОБЯЗАНЫ следовать руководящим принципам документа [RFC 3280]. Родовые расширения ОБЯЗАНЫ быть также включены, как определено в 11.3.2 (PKI).

11.3.2.2.2.1 Сертификат CA корня проверки кода

Этот сертификат (см. Таблицу 34) ОБЯЗАН быть проверен как часть цепи сертификатов, содержащей Сертификат CA корня проверки кода, CA Проверки кода и Сертификаты проверки кода.

11.3.2.2.2.2 Сертификат CA проверки кода

Сертификат CA проверки кода (см. Таблицу 35) ОБЯЗАН быть проверен как часть цепи сертификатов, содержащей Сертификат CA корня проверки кода, Сертификат CA проверки кода и Сертификат проверки кода. МОЖЕТ иметься более одного CA Проверки кода.

11.3.2.2.2.3 Сертификат проверки кода производителя

Этот сертификат (см. Таблицу 36) ОБЯЗАН быть проверен как часть цепи сертификатов, содержащей Сертификат CA корня проверки, Сертификат CA проверки кода и Сертификаты проверки кодов.

Таблица 34/J.191 – Сертификат CA корня проверки кода

Форма имени субъекта	C = <страна>, O =, CN = CA корня CVC
Предназначенное использование	Этот сертификат используется для подписи Сертификатов CA проверки кода.
Подписано	Самоподписанный
Период действительности	20+ лет. Планируется, что период действительности достаточно длинен, чтобы этот сертификат никогда не переиздавался.
Длина модуля	2048
Расширения	keyUsage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true, pathLenConstraint = 0)

Таблица 35/J.191 – Сертификат CA Проверки кода

Форма имени субъекта	C = <страна>, O =, CN = CVC CA
Предназначенное использование	Этот сертификат выпускается с помощью CA Корня проверки кода. Этот сертификат выпускает Сертификаты проверки кодов.
Подписано	CA Корня проверки кода
Период действительности	20 лет
Длина модуля	2048
Расширения	keyUsage [c, m] (keyCertSign, cRL Sign), subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints [c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.2.4 Сертификат проверки кода

Сертификат проверки кода (см. таблицу 37) ОБЯЗАН проверяться как часть цепи сертификатов, содержащей Сертификат CA корня проверки кода, Сертификат CA проверки кода и Сертификат проверки кода

11.3.2.2.2.5 Сертификат проверки кода поставщика услуги

Сертификат проверки кода поставщика услуги (см. Таблицу 38) ОБЯЗАН проверяться как часть цепи сертификата, содержащей Сертификат CA корня проверки кода, Сертификат CA проверки кода и Сертификат проверки кода поставщика услуги.

11.3.2.2.3 Иерархия сертификатов поставщиков услуг

Иерархия сертификатов Поставщиков услуг, или цепь Поставщика услуг, внедряется в CA Корня поставщика услуг, что используется, чтобы выпускать сертификаты для набора санкционированных Поставщиков услуг. CA Поставщика услуг может использоваться, чтобы выпускать дополнительные Сертификаты CA Местной системы или вспомогательные сертификаты. Если CA Поставщика услуги не выпускает вспомогательные сертификаты, то тогда это будет делать CA Местной системы. Вспомогательные сертификаты являются сертификатами конечных объектов на сети кабельного оператора.

Таблица 36/J.191 – Сертификат проверки кода производителя

Форма имени субъекта	C = <страна>, O = <Название компании>, [S = <государство/провинция>], [L = <город>], CN = <Название компании> Mfg CVC
Предназначенное использование	CA проверки кода выпускает этот сертификат каждому санкционированному Производителю. Это используется в алгоритме, устанавливаемом кабельным оператором для безопасной загрузки программного обеспечения.
Подписано	CA Проверки кода
Период действительности	2 года
Длина модуля	2048
Расширения	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

Таблица 37/J.191 – Сертификат проверки кода

Форма имени субъекта	C = <страна>, O =, CN = CVC
Предназначенное использование	CA Проверки кода выпускает этот сертификат. Он выпускается для удостоверения подлинности проверяемого кода. Он используется в алгоритме, устанавливаемом кабельным оператором для безопасной загрузки программного обеспечения.
Подписано	CA Корня проверки кода
Период действительности	2 года
Длина модуля	2048
Расширения	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

Таблица 38/J.191 – Сертификат проверки кода поставщика услуги

Форма имени субъекта	C = <страна>, O = <Название компании>, [S = <государство/провинция>,][L=<город>], CN = <Название компании> CVC Поставщика услуги
Предназначенное использование	CA проверки кода выпускает этот сертификат для каждого санкционированного Поставщика услуг. Он используется в алгоритме, устанавливаемом кабельным оператором, для безопасной загрузки программного обеспечения.
Подписано	CA Корня проверки кода
Период действительности	2 года
Длина модуля	2048
Расширения	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

Информация, содержащаяся в следующих таблицах, представляет собой особые значения для требуемых полей согласно документу [RFC 3280]. Эти особые значения для иерархии "Сертификат поставщика услуги" должны следовать согласно Таблицам с 39 по 42. Если требуемое поле конкретно не перечислено в таблицах, то тогда ОБЯЗАНЫ соблюдаться руководящие принципы в документе [RFC 3280]. Родовые расширения ОБЯЗАНЫ быть также включены, как указано в 11.3.2 (PKI).

11.3.2.2.3.1 Сертификат CA Корня поставщика услуг

Этот сертификат (см. Таблицу 39) ОБЯЗАН быть проверен как часть цепи сертификатов, содержащей Сертификат CA корня поставщика услуг, Сертификат CA поставщика услуг, дополнительный Сертификат CA местной системы и вспомогательные Сертификаты.

Таблица 39/J.191 – Сертификат CA корня поставщика услуг

Форма имени субъекта	C = <страна>, O =, CN = CA корня поставщика услуги
Предназначенное использование	Этот сертификат используется для выпуска Сертификатов CA поставщиков услуг.
Подписано	Самоподписанный
Период действительности	20+ лет. Планируется, что период действительности достаточно длинен, чтобы этот сертификат никогда не переиздавался.
Длина модуля	2048
Расширения	keyUsage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true)

11.3.2.2.3.2 Сертификат CA поставщика услуг

Сертификат CA поставщика услуг (см. Таблицу 40) ОБЯЗАН проверяться как часть цепи сертификатов, содержащей Сертификат CA корня поставщика услуги, Сертификат CA поставщика услуги, Сертификат CA местной системы и вспомогательные Сертификаты.

11.3.2.2.3.3 Сертификат CA местной системы

Этот сертификат (см. Таблицу 41) является дополнительным для поставщика услуги. Если этот сертификат существует, то он ОБЯЗАН проверяться как часть цепи сертификатов, содержащей Сертификат CA корня поставщика услуги, Сертификат CA поставщика услуги, дополнительный Сертификат местной системы и вспомогательные Сертификаты.

11.3.2.2.3.4 Сертификат KDC

Этот сертификат (см. Таблицу 42) ОБЯЗАН проверяться как часть цепи сертификатов, содержащей Сертификат CA корня поставщика услуги, Сертификат CA поставщика услуги, Сертификат CA местной системы и дополнительные Сертификаты (например, сертификаты KDC).

Сертификат KDC ОБЯЗАН включать в себя subjectAltName PKINIT Kerberos, как указано в спецификации безопасности IPCablecom, под названием "Сертификат центра распределения ключей".

Таблица 40/J.191 – Сертификат CA поставщика услуг

Форма имени субъекта	C = <страна>, O = <Название компании>, CN = < Название компании > CA Поставщика услуг
Предназначенное использование	CA Поставщика услуги выпускает этот сертификат для каждого поставщика услуги. Чтобы сделать легким обновление этого сертификата, каждый сетевой элемент формируется с помощью атрибута OrganizationName из SubjectName Сертификата CA поставщика услуги. Это единственный атрибут в сертификате, который должен оставаться постоянным. Этот сертификат появляется как параметр "чтение-запись" в объекте MIB, что указывает атрибут OrganizationName для области Kerberos. Элемент не воспринимает сертификаты поставщика услуги, что не соответствуют этому значению атрибута OrganizationName в SubjectName. Если головной узел содержит центр KDC, что поддерживает это приложение, то тогда элементу PS нужно выполнить первый обмен PKINIT с центром KDC сразу же после повторной начальной загрузки, во время которой его таблицы MIB еще не сформированы. В такое время клиент Kerberos ОБЯЗАН воспринять любой атрибут OrganizationalName Поставщика услуг, но он должен позже проверить, что такое значение, добавленное в базу MIB для этой области, является тем же самым, что и значение в первоначальном ответе PKINIT. Этот CA выпускает сертификаты CA Местной системы или вспомогательные сертификаты.
Подписано	CA Корня поставщика услуг
Период действительности	20 лет
Длина модуля	2048
Расширения	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints[c, m](cA = true, pathLenConstraint = 1)

11.3.2.3 Подтверждение сертификата

Подтверждение сертификата вовлекает подтверждение связанной цепи сертификатов от сертификатов конечного объекта до действительного Корня. Например, подпись на Сертификате элемента PS проверяется с помощью Сертификата CA производителя, а затем подпись на Сертификате CA производителя проверяется с помощью Сертификата CA корня производителя. Сертификат CA корня производителя является самоподписанным, и этот сертификат безопасным способом принимается от источника, которому доверяют. Открытый ключ, присутствующий в Сертификате CA корня производителя, используется, чтобы утвердить подпись на этом же самом сертификате.

Точные правила для подтверждения цепи сертификатов ОБЯЗАНЫ полностью соответствовать документу [RFC 3280], где они упоминаются как "Подтверждение тракта сертификата". Вообще, сертификаты X.509 поддерживают либеральный набор правил для того, чтобы определить, соответствует ли название сертификата выпускающей стороны названию субъекта другой стороны. Правила таковы, что поля двух названий могут быть объявлены соответствующими, даже притом, что двоичное сравнение полей двух названий не указывает совпадение. Документ [RFC 3280] рекомендует, чтобы полномочия сертификатов

ограничивали шифрование полей названий так, чтобы осуществление могло объявлять о соответствии или несоответствии, используя простое двоичное сравнение. Эта безопасность следует этой Рекомендации. Соответственно, DER-кодируемое поле tbsCertificate.issuer сертификата ОБЯЗАНО быть точным соответствием относительно DER-кодируемому полю tbsCertificate.subject своего сертификата выпускающей стороны. Осуществление МОЖЕТ сравнивать название выпускающей стороны по отношению к названию субъекта путем осуществления двоичного сравнения DER-кодируемых полей tbsCertificate.issuer и tbsCertificate.subject.

Таблица 41/J.191 – Сертификат CA местной системы

Форма имени субъекта	C = <страна>, O = <Название компании>, CN = < Название компании > CA местной системы
Предназначенное использование	Этот сертификат является дополнительным, и если он существует, то он выпускается с помощью CA Поставщика услуги. Этот CA выпускает дополнительные сертификаты. Сетевым серверам позволено свободно передвигаться между региональными CA того же самого поставщика услуги.
Подписано	CA Поставщика услуги
Период действительности	20 лет
Длина модуля	2048
Расширения	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints[c, m](cA = true, pathLenConstraint = 0)

Таблица 42/J.191 – Сертификат KDC

Форма имени субъекта	C = <страна>, O = <Название компании>, [OU = <Имя местной системы >], OU = <KDC>, CN = <Адрес IP сервера KDC>
Предназначенное использование	Этот сертификат выпускается либо с помощью CA Поставщика услуги, либо CA местной системы. Он используется для установления подлинности центра KDC по отношению к клиентам Kerberos во время обменов PKINIT. Этот сертификат пропускается к элементу PS внутри ответа PKINIT.
Подписано	CA Поставщика услуги или CA местной системы
Период действительности	20 лет
Длина модуля	2048
Расширения	keyUsage[n, o](digitalSignature, keyEncipherment), authorityKeyIdentifier. Расширение keyUsage является дополнительным. Когда оно используется, его СЛЕДУЕТ маркировать как некритическое. subjectAltName [n, m] (см. спецификацию безопасности IPCablecom).

Подтверждение периодов достоверности для вложения не проверяется и преднамеренно не предписывается, что подчиняется текущим стандартам. Во время выпуска, дата начала достоверности любого сертификата конечного объекта ОБЯЗАНА быть той же самой или

более поздней, чем дата начала выпуска периода достоверности сертификата CA. После того, как сертификат CA обновляется, даты начала сертификатов конечных объектов МОГУТ быть более ранними, чем дата начала издания сертификата CA. Для выпуска CA дата конца достоверности для объектов может быть более ранней, той же самой, как дата конца достоверности, или после нее, как определено в таблицах Сертификатов.

11.3.2.3.1 Подтверждение для цепи производителя и проверка корня

Центр KDC ОБЯЗАН утвердить связанную цепь сертификатов производителей. Обычно первый сертификат в цепи явно не включается в цепь сертификатов, что посылают по проводу. В случаях, где Сертификат CA корня производителя явно включен по проводу, это ОБЯЗАНО уже быть известно проверяющей стороне раньше времени проверки этого сертификата. Сертификат CA корня производителя, посланный по проводу, ОБЯЗАН НЕ содержать никаких изменений к сертификату, кроме возможного исключения для порядкового номера сертификата, периода достоверности и значения подписи. Если в сертификате CA корня производителя существуют изменения, кроме порядкового номера сертификата, периода достоверности и значения подписи, по сравнению с известным Сертификатом CA корня производителя (что было передано по проводу), то центр KDC, осуществляющий сравнение, ОБЯЗАН потерпеть неудачу в проверке сертификата.

11.3.2.3.2 Подтверждение для цепи проверки кода и проверки корня

Сервер вспомогательного офиса может проверить достоверность Цепи проверки кода до начала процесса загрузки программного обеспечения. Для подробностей, см. 11.3.7, "Безопасная загрузка программного обеспечения".

11.3.2.3.3 Подтверждение для цепи поставщика услуги и проверки корня

Элемент PS ОБЯЗАН проверить достоверность связанной цепи сертификатов Поставщика услуги. Обычно первый сертификат в цепи явно не включается в цепь сертификатов, что посылают по проводу. В случаях, где Сертификат CA корня поставщика услуги явно включается по проводу, это ОБЯЗАНО уже быть известно проверяющей стороне раньше времени проверки этого сертификата. Сертификат CA корня поставщика услуги ОБЯЗАН НЕ содержать никаких изменений к сертификату, кроме возможного исключения порядкового номера сертификата, периода достоверности и значения подписи. Если в Сертификате CA корня поставщика услуги существуют изменения, кроме серийного номера сертификата, период достоверности и значения подписи, по сравнению с известным Сертификатом CA корня поставщика услуги (что было переслано по проводу), то элемент PS, осуществляющий сравнение, ОБЯЗАН считать неудачной проверку сертификата.

11.3.2.4 Аннулирование сертификата

Аннулирование сертификата выходит за рамки этой Рекомендации.

11.3.3 Безопасный обмен сообщениями административного управления

Алгоритм безопасности, используемый для установления в начальное состояние обмена сообщениями SNMP, зависит от режима обеспечения элемента PS (см. 5.7). Имеются два типа режимов обеспечения: режим обеспечения DHCP и режим обеспечения SNMP. Режим обеспечения DHCP имеет дополнительные под-режимы, которые определяют, формируется ли это для режима NmAccess, или для режима Сосуществования. Для административного управления обменом сообщениями режим обеспечения SNMP требует протокол SNMPv3.

Следующий подраздел описывает алгоритмы безопасности и требования, необходимые для установления обмена сообщениями административного управления SNMP в начальное состояние на основе режима обеспечения элемента PS. Элемент PS ОБЯЗАН поддерживать алгоритмы безопасности SNMPv3, указанные в 11.3.3.1.2 и 11.3.3.2.

11.3.3.1 Алгоритмы безопасности для SNMP в режиме обеспечения DHCP

В режиме обеспечения DHCP элемент PS может быть сформирован для режима NmAccess или режима Сосуществования. В режиме Сосуществования элемент PS может быть сформирован для обмена сообщениями административного управления SNMPv1, SNMPv2 и/или SNMPv3.

11.3.3.1.1 Режим NmAccess

Если элемент PS обеспечивается в режиме обеспечения DHCP с режимом NmAccess, сетевое административное управление на основе SNMP внутри элемента PS не использует SNMPv3 и поэтому не нуждается в установлении в начальное состояние функций безопасности SNMPv3. Установление в начальное состояние звена административного управления SNMPv1/v2 определяется в 6.3.6.1.

11.3.3.1.2 Режим сосуществования

Если элемент PS обеспечивается в режиме обеспечения DHCP с режимом Сосуществования, и определяется, что протокол обмена сообщениями административного управления должен быть протоколом SNMPv3 (см. 6.3.6.1), то тогда элемент PS ОБЯЗАН использовать безопасность SNMPv3, указанную документом [RFC 2574]. Удостоверение подлинности SNMPv3 ОБЯЗАНО быть включено на все времена, и МОЖЕТ быть также использована секретность SNMPv3.

Чтобы установить ключи SNMPv3, модем CM, подчиняющийся услуге PS, ОБЯЗАН поддерживать "установление в начальное состояние протокола SNMPv3", описанное ниже.

ПРИМЕЧАНИЕ – Кабельный модем обозначается как имеющий "очень безопасное" положение защиты в контексте Приложения A документа RFC-2574 и Приложения A документа RFC-2575. Это означает, что записи по умолчанию usmUser и vacmAccess, определенные в Приложении A документа RFC-2574 и Приложения A документа RFC-2575, ОБЯЗАНЫ НЕ присутствовать.

1) Для каждых из 5 различных имен безопасности управляющая программа порождает пару чисел:
   a) Управляющая программа порождает случайное число Rm;
   b) Управляющая программа использует уравнение DH для трансляции Rm в открытое число "z":

      $$z = g \wedge Rm \text{ MOD } p$$

      где "g" берется из набора параметров Диффи-Хеллмана, "p" есть простое число из этих параметров.
2) Создается файл конфигурации модема CM для включения пары (имя безопасности, открытое число), и модем CM ОБЯЗАН поддерживать минимум 5 пар. Например:

   тип 34.1 TLV (Имя безопасности толчкового запуска SnmpV3) = docsisManager

   тип 34.2 TLV (Открытое число толчкового запуска SnmpV3) = z

Во время процесса включения начального запуска модема CM вышеуказанные значения (имя безопасности, открытое число) будет (ОБЯЗАНО) заполнено в объекте usmDHKickstartTable.

В этой точке:

```
usmDHKickstartMgrpublic.1 = "z"  (строка октета)
usmDHKickstartSecurityName.1 = "docsisManager"
```

Когда объект usmDHKickstartMgrpublic.n устанавливается с действительным значением во время регистрации, в объекте usmUserTable создается соответствующий ряд со следующими значениями:

```
usmUserEngineID: localEngineID
```

```
usmUserName: usmDHKickstartSecurityName.n value
usmuserSecurityName: usmDHKickstartSecurityName.n value
usmUserCloneForm: ZeroDotZero
usmUserAuthProtocol: usmHMACMD5AuthProtocol
usmuserAuthKeyChange: извлечено из установленного значения
usmUserOwnAuthKeyChange: извлечено из установленного значения
usmUserPrivProtocol: usmDESPrivProtocol
usmUserPrivKeyChange: извлечено из установленного значения
usmUserOwnPrivKeyChange: извлечено из установленного значения
usmUserPublic: ""
usmUserStorageType: постоянный
usmUserStatus: активный
```

ПРИМЕЧАНИЕ – Для записей dhKickstart (CM) в usmUserTable, "Постоянный" означает, что оно ОБЯЗАНО быть записано, но не исключено, и не сохраняется при повторных начальных загрузках.

После того, как модем CM зарегистрировался с помощью AN:

– Модем CM порождает случайное число "xa" для каждого ряда, заполненного в объекте usmDHKickstartTable, который имеет объекты usmDHKickstartSecurityName и usmDHKickstartMgrPublic ненулевой длины.

– Модем CM использует уравнение DH для трансляции "xa" в открытое число "c" (для каждого ряда, определенного выше):

$$c = g \wedge xa \text{ MOD } p$$

где "g" берется из набора параметров Диффи-Хеллмана, "p" есть простое число из таких параметров.

В этой точке:

```
usmDHKickstartMyPublic.1 = "c" (строка октета)
usmDHKickstartMgrPublic.1 = "z" (строка октета)
usmDHKickstartSecurityName.1 = "docsisManager"
```

3) модем CM вычисляет совместно используемый секрет "sk", где sk = z ^xa mod p;

4) модем CM использует "sk" для извлечения ключа секретности и ключа удостоверения подлинности для каждого ряда в объекте usmDHKickstartTable и устанавливает значения в объекте usmUserTable.

Как указано в документе RFC 2786, ключ секретности и ключ удостоверения подлинности для связанного имени пользователя, "docsisManager" в этом случае, извлекается из sk путем применения функции извлечения ключа PBKDF2, определенной в PKCS#5v2.0.

```
privacy key [ключ секретности]<---      PBKDF2( salt = 0xd1310ba6,
            iterationCount = 500,
            keyLength = 16,
            prf = id-hmacWithSHA1)
authentication key [ключ удостоверения подлинности]<---- PBKDF2( salt =
0x98dfb5ac,
                  iterationCount = 500,
                  keyLength = 16 (usmHMACMD5AuthProtocol),
                  prf = id-hmacWithSHA1)
```

В этой точке модем CM завершил свой процесс установления в начальное состояние протокола SNMPv3 и ОБЯЗАН разрешить соответствующий уровень доступа к действительному объекту securityName с правильным ключом удостоверения подлинности и /или ключом секретности.

Подчиняющийся модем CM ОБЯЗАН правильно заполнить ключи к соответствующим таблицам, как указано документами RFC, относящимися к SNMPv3, и документом RFC 2786.

5) Следующий материал описывает процесс, который управляющая программа использует для извлечения уникального ключа удостоверения подлинности и ключа секретности модема CM.

Управляющая программа SNMP осуществляет доступ к содержанию объекта usmDHKickstartTable, используя имя безопасности из объекта 'dhKickstart' без удостоверения подлинности.

Подчиняющийся модем CM ОБЯЗАН обеспечивать предварительно установленные записи в таблице USM и в таблицах VACM, чтобы правильно создавать объект 'dhKickstart' пользователя из уровня безопасности объекта noAuthnoPriv, что имеет доступ только для чтения к системной группе и к объекту usmDHkickstartTable.

Управляющая программа SNMP получает значение числа usmDHKickstartMypublic модема CM, связанного с именем безопасности, для которого администратор хочет извлечь ключи удостоверения подлинности и секретности. Со знанием управляющей программы о закрытом случайном числе, управляющая программа может вычислить совместно используемый секрет DH. Из такого совместно используемого секрета управляющая программа может извлечь эксплуатационные ключи удостоверения подлинности и конфиденциальности для имени безопасности, которое управляющая программа собирается использовать для осуществления связи с модемом CM.

Чтобы поддерживать установление в начальное состояние протокола SNMPv3 и изменения ключей, элемент PS ОБЯЗАН также обладать способностью получения значений TLV типов 34, 34.1, и 34.2, как определено в B.C.1.2.8/J.112, спецификация "Радиочастотный интерфейс DOCSIS", и осуществлять механизм изменения ключа, указанный в документе [RFC 2786], который включает в себя объект MIB usmDHKickstartTable.

11.3.3.2 Алгоритмы безопасности для протокола SNMPv3 в режиме обеспечения SNMP

Если элемент PS обеспечивается в режиме обеспечения SNMP, то сетевое административное управление на основе SNMP внутри элемента PS ОБЯЗАНО пробежать SNMPv3 с безопасностью, указанной документом [RFC 2574]. Удостоверение подлинности SNMPv3 ОБЯЗАНО быть включено на все времена, а также МОЖЕТ быть использована секретность SNMPv3. Чтобы установить ключи SNMPv3, все интерфейсы SNMP ОБЯЗАНЫ использовать административное управление ключом SNMPv3, охваченное системой Kerberos [*Kerberized*], как указано в 11.3.3.2.3.

11.3.3.2.1 Алгоритмы шифрования SNMPv3

Идентификаторы преобразования шифрования, подлежащие использованию административным управлением ключа, охваченного системой Kerberos [*Kerberized*], чтобы обсуждать алгоритм шифрования для использования протоколом SNMPv3, являются теми же самыми идентификаторами, которые определены в 6.3.1/J.170.

11.3.3.2.2 Алгоритмы удостоверения подлинности SNMPv3

Идентификаторы преобразования удостоверения подлинности, подлежащие использованию административным управлением ключа, охваченного системой Kerberos, чтобы обсуждать алгоритм удостоверения подлинности сообщения для использования протоколом SNMPv3, является теми же самыми идентификаторами, которые определены в 6.3.2/J.170.

11.3.3.2.3 Протокол SNMPv3, охваченный системой Kerberos

Профиль административного управления ключа, охваченного системой Kerberos [*Kerberized*], характерного для протокола SNMPv3, является тем же самым профилем, определенным в 6.5.7/J.170.

11.3.3.2.4 Идентификаторы ID движущих механизмов SNMPv3

Поскольку Управляющая программа и Клиент протокола SNMP ОБЯЗАНЫ проверить, что идентификатор ID движущего механизма SNMPv3 в сообщениях Request [*запрос*] AP и Reply [*ответ*] AP основаны на соответствующем главном имени системы Kerberos в билете [Рекомендация МСЭ-Т J.170], следующий далее материал определяет правило, подлежащее использованию при порождении идентификаторов ID движущих механизмов SNMPv3 для использования в этом приложении:

- Идентификатор ID движущего механизма SNMPv3 следует формату, определенному в документе [RFC 2571], т.е. первый бит установлен в 1 (единицу), и используется соответствующее значение для первых четырех байтов [RFC 2571];
- Пятый байт несет значение 4 (четыре) для указания того, что следующие байты до 27-го, должны рассматриваться как текст. Эти байты до 27-го байта определяются следующим образом:
  - Для байтов ID движущего механизма используются первые 25 знаков главного имени системы Kerberos, начиная с 6-го байта.
  - Вышеуказанная последовательность байтов, которая указывает главное имя системы Kerberos, сопровождается байтом, который нужно рассматривать как 8-разрядное значение HEX. Каждое различное значение определяет конкретный движущий механизм SNMP в устройстве (элемент или сервер NMS). Значение 0 (нуль) ОБЯЗАНО НЕ использоваться.
  - Строка текста, что начинается на 6-м байте, заканчивается с помощью знака "Пусто" [*null*].

Отметим, что возможны другие форматы, следуя подходам в документе [RFC 2571]. Вышеупомянутый выбор, тем не менее, предназначен для уменьшения сложности осуществления, которая потребовалась бы, если бы позволялись все подходы в документе [RFC 2571].

11.3.3.2.5 Заполнение usmUserTable

Объект msgSecurityParameters в сообщениях SNMPv3 несет поле msgUserName, которое указывает пользователя, по поручению которого осуществляется обмен сообщениями, и с информацией безопасности которого производятся поля msgAuthenticationParameters и msgPrivacyParameters. Для движущего механизма SNMP элемента, чтобы обработать эти сообщения, необходимая пользовательская информация ОБЯЗАНА быть введена в объект usmUserTable [RFC 2574] для движущего механизма элемента. Объект usmUserTable ОБЯЗАН быть заполнен в элементе PS сразу же после получения сообщения Reply AP со следующей информацией:

- usmUserEngineID: местный идентификатор ID движущего механизма SNMP, как определено в 11.3.3.2.4;
- usmUserName: администратор PS -XXXXXX;
- usmUserSecurityName: администратор PS-XXXXXX;
- usmUserCloneFrom: 0.0;
- usmUserAuthProtocol: указывает протокол удостоверения подлинности, выбранный пользователем, из сообщения Replay AP;
- usmUserAuthKeyChange: значение по умолчанию "";
- usmUserOwnAuthKeyChange: значение по умолчанию "";
- usmUserPrivProtocol: указывает протокол шифрования, выбранный пользователем из сообщения Reply AP;
- usmUserPrivKeyChange: значение по умолчанию "";

- usmUserOwnPrivKeyChange: значение по умолчанию "";
- usmUserPublic: значение по умолчанию "";
- usmUserStorageType: постоянное;
- usmUserStatus: активное.

Значение XXXXXX будет адресом "Элемент MAC" для такого элемента PS.

Новые пользователи SNMPv3 МОГУТ быть созданы с помощью стандартного клонирования SNMPv3, как определено в документе [RFC 2475]. Для дополнительной информации можно обратиться к 7.1.1.3.1/J.170.

11.3.4 Безопасное качество CQoS

Кабельное качество CQoS обеспечивает качество QoS к приложениям IPCablecom, которые требуют сквозного адреса. Сообщения DQoS модели IPCablecom между MTA и CMTS, CMS или CM защищены спецификацией безопасности PCablecom. Для безопасности необходимо гарантировать, что эти сообщения IPCablecom, уже защищенные с помощью IPCablecom, могут пройти средства межсетевой защиты в услуге PS. В сферу действия 'njq Рекомендации не входит добавление безопасности для сообщений IPCablecom. Поскольку требование безопасности качества CQoS элемента PS состоит в том, чтобы только направлять обмен сообщениями IPCablecom, то нет никакой зависимости от системы NMS в поддержке этой функции. Поэтому, функция безопасности CQoS остается той же самой как для режима обеспечения DHCP, так и для режима обеспечения SNMP (см. 5.7).

Требование для организации защиты CQoS состоит в том, чтобы обеспечить безопасность, которая не является чрезмерно обременительной на системе. Ключевой пункт к организации защиты QoS заключается в том, чтобы гарантировать, что кража услуги и разрушение сети уменьшаются до незначащей потери. Является также критическим для понимания то, что кабельное качество CQoS есть шлюз QoS в дом, и поэтому будет, вероятно, или управлять всеми приложениями и приборами в доме, или поддерживать их, требуя качество QoS на кабельной сети к услуге PS и через нее. Поэтому особенно критическим является гарантирование этой точки входа, которая не должна быть слабым звеном в системе QoS.

11.3.4.1 Архитектура CQoS

Архитектура CQoS состоит из функционального элемента CQP, который облегчает установление потоков QoS через кабель HFC для приложений IP. Элемент CQP существует в услуге PS. См. раздел 10. Элемент CQP действует в качестве прозрачного моста для обмена сообщениями CQoS между приложениями, подчиняющимися модели IPCablecom, и системой CMTS. От средств межсетевой защиты требуется быть способными пропускать далее обмен сообщениями, подчиняющимися безопасности IPCablecom и QoS.

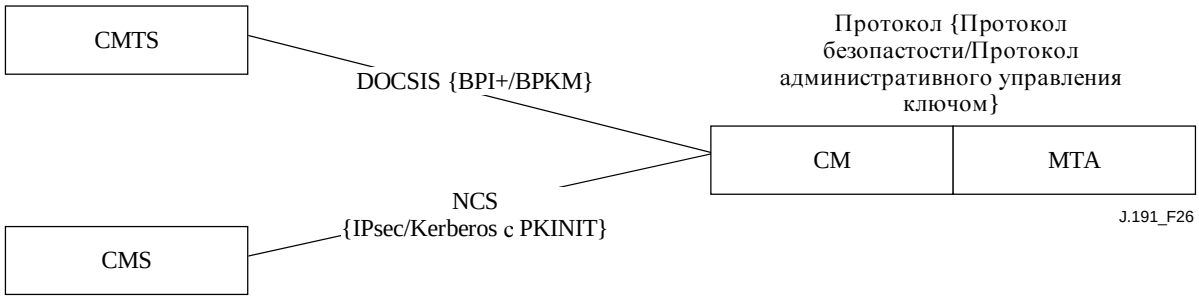
См. раздел 10 для более полных подробностей по качеству CQoS.

11.3.4.2 Безопасная архитектура DQoS модели IPCablecom

Этот раздел описывает безопасную архитектуру DQoS модели IPCablecom, чтобы обсуждать, как эти сообщения взаимодействуют со средствами межсетевой защиты в услуге PS. В пределах DQoS, Адаптер терминала мультимедиа (*MTA, Multimedia Terminal Adapter*) осуществляет связь с системой CMTS и Сервером административного управления вызовом (*CMS, Call Management Server*), чтобы установить необходимое качество QoS для его услуг IPCablecom. Адаптер MTA встроен с помощью модема CM спецификации DOCSIS. Ниже находятся таблица (Таблица 43) и диаграмма (Рисунок 26) устройств, протокола связи и протокола безопасности для DQoS.

Таблица 43/J.191 – Безопасная архитектура DQoS

E-MTA		
Звено к адаптеру MTA в доме	**Протокол**	**Протокол безопасности**
E-MTA/CM – CMS	NCS	IPsec
E-MTA/CM – CMTS	DOCSIS	BPI+

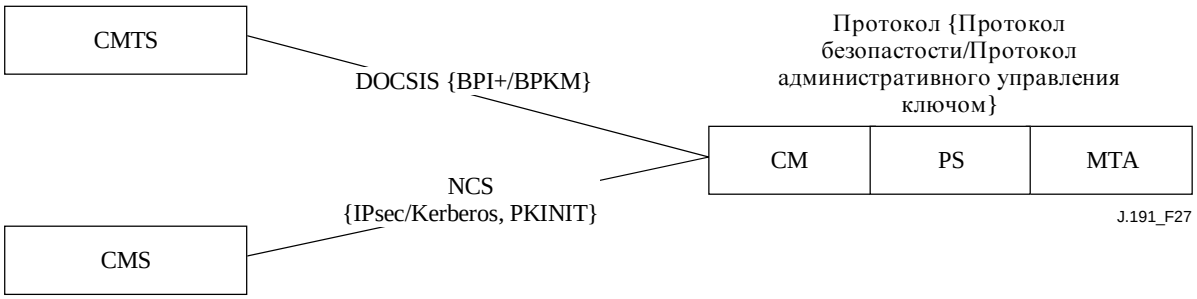


E-MTA DQoS связи

Рисунок 26/J.191 – Безопасная архитектура DQoS к адаптеру MTA

11.3.4.3 Архитектура безопасности CQoS

Качество CQoS требует обмена сообщениями DQoS модели IPCablecom [Рекомендация МСЭ-Т J.163]. Все обмены сообщениями CQoS ОБЯЗАНЫ быть застрахованы, как описано в спецификации безопасности IPCablecom. Рисунок 27 показывает протоколы, необходимые для поддержки E-MTA для DQoS. Единственное различие в застрахованной архитектуре CQoS и застрахованной архитектуре DQoS модели IPCablecom заключается в том, что услуга PS логически находится между модемом CM и адаптером MTA. Однако, поскольку услуга PS действует в качестве прозрачного моста, в протоколах и звеньях связи нет изменений.



E-CM-IPSP-MTA CQoS связи

Рисунок 27/J.191 – Безопасная архитектура CQoS к адаптеру MTA

11.3.4.4 Роль портала CSP в CQoS

Портал кабельной безопасности (*CSP, Cable Security Portal*) является единственной точкой управления безопасностью внутри функции PS в архитектуре; поэтому портал CSP обеспечивает безопасность в архитектуре CQoS. Портал CQP действует в качестве

прозрачного моста для сообщений DQoS, которые он поддерживает; поэтому портал CSP не обеспечивает какие-либо услуги для CQoS.

11.3.5 Административное управление средствами межсетевой защиты

В то время как проблемы безопасности долгое время были главной заботой для сетевых корпораций, увеличивающаяся повсеместность связности всегда включенной Интернет через Кабельный модем (*CM, Cable Modem*) приводит заботы о безопасности к дому. Поскольку средний абонент испытывает недостаток в технических знаниях, понимание проблем безопасности и времени (чтобы держать свои домашние компьютеры в первоклассной безопасной работе), а также средства межсетевой защиты становятся необходимой первой линией обороны в защите небезопасных компьютеров в доме.

Для средств межсетевой защиты имеются много определений, включая:

– "Средства межсетевой защиты являются подходом к безопасности, они помогают осуществлять алгоритм большей безопасности, который определяет услуги и доступ, что должны быть позволены ".

– "Средства межсетевой защиты являются агентом, что некоторым образом экранирует сетевой трафик, блокируя трафик, который он считает несоответствующим, опасным, или то и другое ".

Следовательно, средства межсетевой защиты осуществляют алгоритм безопасности путем использования некоторого механизма для блокирования трафика, который алгоритм безопасности оговаривает как нежелательный.

Требования обработки трафика средств межсетевой защиты включает в себя:

• Модель IPCablecom (см. Таблицу 44) и протоколы, определенные в этой Рекомендации, ОБЯЗАНЫ НЕ разбиваться средствами межсетевой защиты. Например, средствам межсетевой защиты следует иметь поддержку соответствующего посредника, характерного для приложения, или фильтрования пакетов с изменением состояния в процессе исполнения, чтобы открывать порты UDP, которые определяются как результат сигнализации IPCablecom.

Таблица 44/J.191 – Уместные Рекомендации модели IPCablecom для средств межсетевой защиты

Описание	Рекомендация
Спецификация кодеков аудио/видео	J.161
Спецификация Динамического качества обслуживания	J.163
Спецификация протокола сигнализации вызова на основе сети	J.162
Спецификация обеспечения устройства MTA	J.167
Спецификация безопасности	J.170
Спецификация механизма события административного управления	J.172
Спецификация протокола сервера аудио	J.175
Спецификация сигнализации сервера административного управления вызовом	J.cmss

Протоколы, определяемые моделью IPCablecom, включают в себя следующее:

• Обеспечение SNMPv3, DHCP, DNS, TFTP, SYSLOG;

• Поток носителя информации RTP, RTCP;

• QoS RSVP;

- Сигнализация сетевого вызова MGCP, SDP;
- Безопасность Обмен сообщениями Kerberos, IPsec.

Протоколы, определяемые этим приложением, включают в себя следующее:

- Обеспечение SNMPv3, DHCP, DNS, TFTP, SYSLOG;
- Административное управление ICMP;
- Безопасность Kerberos.

Средствам межсетевой защиты СЛЕДУЕТ защищать от просмотра (сканирования) порта или сети, который запускается изнутри или извне дома. Им также СЛЕДУЕТ защищать от следующих атак по опровержению обслуживания: "Ping of Death" [*Звон смерти*], "Teardrop" [*Слезинка*], "Bonk"[*Подзатыльник*], "Nestea", "SYN Flood", "LAND Attack", "Spoofing IP" [*Имитация*], "Smurf Attack" и "WinNuke".

Средства межсетевой защиты ОБЯЗАНЫ быть способны позволять доступ тех же самых популярных прикладных протоколов Интернет, как определено в Дополнении D. Для наших целей простая трансляция NAT или фильтр пакетов не являются достаточными. Чтобы обеспечивать гибкое и безопасное решение, средства межсетевой защиты ОБЯЗАНЫ осуществлять либо Посредника, характерного для приложения (*ASP, Application-Specific Proxy*), либо межсетевую защиту в виде Фильтрования пакетов с изменением состояния в процессе исполнения (*SPF, Stateful Packet Filtering*).

11.3.5.1 Дистанционная загрузка набора правил межсетевой защиты

Будут разрешены свойства в элементе PS, которые позволят оператору дистанционно управлять функциями межсетевой защиты. Большая часть этого управления достигается через загрузку файла конфигурации. Файл конфигурации межсетевой защиты содержит набор правил для конкретного алгоритма безопасности. Административное управление средствами межсетевой защиты достигается путем доступа к объектам административного управления для базы NIB Безопасности.

Алгоритм безопасности определяет желательный уровень безопасности/функциональных возможностей для средств межсетевой защиты абонента. Может существовать более одного алгоритма, чтобы можно было выбрать подходящий алгоритм. Файлы, содержащие соответствующий набор правил для этих алгоритмов безопасности, сохраняются на сервере файла оператора. Услуга PS ОБЯЗАНА использовать клиента TFTP, подчиняющего документу [RFC 1350], чтобы загружать файл конфигурации набора правил межсетевой защиты. Чтобы удостоверить подлинность загрузки файла набора правил, алгоритм удостоверения подлинности, определенный в 7.3.3.3.2, ОБЯЗАН использоваться с соответствующими параметрами случайных данных и административного управления имени файла, определенными в 11.3.5.2 ниже.

Используя интерфейс административного управления базой MIB Безопасности, оператор формирует параметры файла в наборе правил алгоритма безопасности, перечисленные в 11.3.5.2, а затем следует процедуре, определенной в 7.3.3.3.2, чтобы загрузить и подтвердить подлинность файла. Если загрузка имеет успех, то файл набора правил алгоритма безопасности ОБЯЗАН быть "активирован" на средствах межсетевой защиты. Если удостоверение подлинности терпит неудачу, то набор правил алгоритма ОБЯЗАН быть сброшен.

11.3.5.2 Параметры административного управления набором правил межсетевой защиты

Следующие параметры административного управления ОБЯЗАНЫ быть осуществлены в услуге PS, как определено базой MIB Безопасности для поддержки файла набора правил межсетевой защиты:

- **cabhSecFwPolicyFileURL** – Содержит имя файла набора правил алгоритма и адрес IP сервера TFTP, содержащего файл набора правил алгоритма, в формате URL протокола TFTP. Как только объект cabhSecFwPolicyFileURL был обновлен, он ОБЯЗАН запустить загрузку файла. Услуга PS ОБЯЗАНА использовать клиента TFTP, подчиняющегося документу [RFC 1350], для загрузки файла конфигурации межсетевой защиты.
- **cabhSecFwPolicyFileHash** – Определяет каталог SHA-1 для соответствующего файла набора правил.
- **cabhSecFwPolicyFileOperStatus** – Объект InProgress(1) указывает, что производится загрузка файла набора правил, либо как результат несоответствия версии в обеспечении, либо как результат запроса upgradeFromMgt. Объект CompleteFromProvisioning(2) указывает, что последнее обновление файла набора правил было результатом несоответствия версии в обеспечении. Объект CompleteFromMgt(3) указывает, что последнее обновление файла набора правил было результатом установки объекта FirewallPolicyFileAdminStatus в upgradeFromMgt. Объект Failed(4) указывает, что последняя попытка загрузки потерпела неудачу, обычно из-за выдержки времени TFTP.
- **cabhSecFwPolicyFileCurrentVersion** – Версия файла набора правил, действующая в настоящее время в элементе PS. Этому объекту следует быть в синтаксисе, используемом индивидуальным поставщиком, чтобы определить версии файлов набора правил. Если это не применяется, то этот объект ОБЯЗАН содержать пустую строку.
- **cabhSecFwPolicyFileEnable** – Разрешает активацию и деактивацию алгоритма безопасности средств межсетевой защиты.

11.3.5.3 Регистрация события межсетевой защиты

Средства межсетевой защиты ОБЯЗАНЫ быть способны к регистрации следующих типов событий:

- ТИП 1: попытки как от частных, так и от общественных клиентов пересечь межсетевую защиту, что нарушает Алгоритм безопасности.
- ТИП 2: определенные попытки атак Опровержения обслуживания.
- ТИП 3: сделаны изменения к активному алгоритму межсетевой защиты или к параметрам конфигурации межсетевой защиты.

Выбор, какой из типов событий межсетевой защиты фактически становится зарегистрированным, формируется через интерфейс базы MIB Безопасности, как описано в 11.3.5.2.

Операторы могут наблюдать за событиями межсетевой защиты, используя механизм обмена сообщениями о событии, определенный в 6.5. К параметрам административного управления регистрацией события получают доступ через базу MIB Безопасности MIB, что определяется в 6.5

Регистрация сообщения о событии межсетевой защиты позволяет оператору оценивать уровень деятельности хакера через сеть оператора, и наблюдать за изменениями к алгоритму безопасности средств межсетевой защиты. Когда типы сообщений о событиях случая были обеспечены через параметры административного управления базы MIB Безопасности, эти события межсетевой защиты ОБЯЗАНЫ быть зарегистрированы с помощью записи сообщения о событии, используя механизм регистрации события, определенный в 6.5

Запись сообщения о событии межсетевой защиты будет содержать следующую информацию:

- Приоритет события;

- Дату и время – когда событие имело место;
- Протокол – указанный полем заголовка IP (TCP, UDP, ICMP);
- Адрес IP источника;
- Адрес IP пункта назначения;
- Порт назначения (TCP и UDP) или Тип сообщения (ICMP);
- Правило уместного алгоритма;
- Описание события (дополнительное).

Раздел 6.5.2.1 определяет поле "Приоритет события", которое описывает различные уровни приоритета для зарегистрированных событий. Это поле "Приоритет события" ОБЯЗАНО быть установлено в приоритет 6 для событий межсетевой защиты Типов 1, 2 и 3. Если поле не применяется, оно должно быть оставлено пустым. Элемент PS ОБЯЗАН форматировать сообщения о событиях межсетевой защиты, как определено в Дополнении B.

Чтобы помочь в наблюдении за деятельностью хакера на межсетевой защите абонента, объекты административного управления тревоги хакера были определены в базе MIB Безопасности. Это свойство приводит в готовность оператора, когда число событий межсетевой защиты Типов 1 и 2 превышает аварийный порог в течение данного аварийного периода (в днях). Аварийный порог и аварийный период формируются оператором. Элемент PS накапливает количество событий межсетевой защиты Типов 1 и 2, которые произошли за прошлое количество дней, определенных аварийным периодом. Если это количество превышает аварийный порог, сообщение о событии тревоги хакера регистрируется, чтобы сообщить оператору.

11.3.5.4 Параметры административного управления для регистрации событий

Следующие параметры административного управления ОБЯЗАНЫ быть осуществлены в элементе PS, как определено базой MIB Безопасности, чтобы наблюдать/формировать регистрацию событий межсетевой защиты:

- **cabhSecFwEventType1Enable** – Обеспечивает или выключает регистрацию сообщений о событиях межсетевой защиты типа 1.
- **cabhSecFwEventType2Enable** – Обеспечивает или выключает регистрацию сообщений о событиях межсетевой защиты типа 2.
- **cabhSecFwEventType3Enable** – Обеспечивает или выключает регистрацию сообщений о событиях межсетевой защиты типа 3.
- **cabhSecFwEventAttackAlertThreshold** – Если количество атак хакеров типа 1 или 2 превышает этот порог в период, определенный объектом cabhSecFwEventAttackAlertPeriod, то сообщение о событии межсетевой защиты ОБЯЗАНО быть зарегистрировано с уровнем приоритета 4.
- **cabhSecFwEventAttackAlertPeriod** – Указывает период, подлежащий использованию в последние дни для объекта cabhSecFwEventAttackAlertThreshold.

11.3.6 Базы MIB

Услуга PS ОБЯЗАНА поддерживать следующие базы MIB поддержки загрузки программного обеспечения, определенные в документе [RFC 2669]:

- **docsDevSwAdminStatus** – Если установлено в upgradeFromMgt(1), устройство будет инициировать загрузку программного изображения TFTP, используя docsDevSwFilename.
- **docsDevSwFilename** – Имя файла изображения программного обеспечения, подлежащего загрузке в устройство.

- **docsDevSwCurrentVers** – Версия программного обеспечения, действующая в устройстве в настоящее время.
- **docsDevSwServer** – Адрес сервера TFTP, используемого для обновлений программного обеспечения.
- **docsDevSwOperStatus** – Статус загрузки программного обеспечения.

Услуга PS ОБЯЗАНА поддерживать базы MIB загрузки программного обеспечения, определенные в Рекомендации МСЭ-Т J.112, Дополнение B.O]:

- **docsBpi2CodeDownloadGroup** – Совокупность объектов, что обеспечивают удостоверенную надлежащим образом поддержку загрузки программного обеспечения. Объект docsBpi2CodeDownloadGroup включает в себя:
  - **docsBpi2CodeDownloadStatusCode** – Указывает результат проверки CVC файла последней конфигурации, проверки CVC протокола SNMP или проверки файла кода.
  - **docsBpi2CodeDownloadStatusString** – Дополнительная информация к коду статуса.
  - **docsBpi2CodeMfgOrgName** – Название организации производителя устройства [*organizationName*].
- **docsBpi2CodeMfgCodeAccessStart** – Текущее значение codeAccessStart производителя устройства, отнесенное ко времени по Гринвичу (*GMT, Greenwich Mean Time*).
- **docsBpi2CodeMfgCvcAccessStart** – Текущее значение cvcAccessStart производителя устройства, отнесенное ко времени по Гринвичу (GMT).
  - **docsBpi2CodeCoSignerOrgName** – Название совместно подписавшей организации [*organizationName*].
- **docsBpi2CodeCoSignerCodeAccessStart** – Текущее значение codeAccessStart совместно подписавшей организации, отнесенное ко времени по Гринвичу (GMT).
- **docsBpi2CodeCoSignerCvcAccessStart** – Текущее значение cvcAccessStart совместно подписавшей организации, отнесенное ко времени по Гринвичу (GMT).
  - **docsBpi2CodeCvcUpdate** – Запускает устройство для проверки сертификата CVC и обновляет значение cvcAccessStart.
  - **docsBpi2CmPublicKey** – DER-кодированная строка типа ASN.1 RSAPublicKey, как определено в Стандарте кодирования RSA [RSA1].
  - **docsBpi2CmDeviceCmCert** – DER-кодированный сертификат устройства по X.509.
  - **docsBpi2CmDeviceManufCert** – DER-кодированный сертификат CA производителя по X.509, который подписал сертификат устройства.

Услуга PS ОБЯЗАНА поддерживать следующую базу MIB поддержки загрузки конфигурации:

- **cabhPsDevProvConfigHash** – Случайные данные SHA-1 всего содержимого из файла конфигурации, взятого в качестве строки байта.

11.3.7 Безопасная загрузка программного обеспечения

Элемент PS в устройстве ОБЯЗАН быть способен к дистанционной загрузке изображения программного обеспечения по сети. Новое изображение программного обеспечения позволило бы оператору улучшать показатели качества, приспосабливать новые функции и особенности, исправлять недостатки разработки и позволять создавать тракт перемещения для устройств, поскольку эта Рекомендация развивается. Возможность загрузки

программного обеспечения ОБЯЗАНА позволить изменение функциональных возможностей элемента PS, не требуя, чтобы персонал кабельной системы физически посещал и повторно формировал каждый блок. Безопасный процесс загрузки программного обеспечения обращается к следующим первичным требованиям системы:

- Механизм, используемый для загрузки программного обеспечения, ОБЯЗАН быть переносом файла TFTP.
- Загрузка программного обеспечения ОБЯЗАНА быть инициирована одним из двух способов:
  1) запросом SET [*установить*] протокола SNMP, выпущенным системой NMS к объекту docsDevSwAdminStatus;
  2) через файл конфигурации элемента PS.

  Если Имя файла обновления программного обеспечения в файле конфигурации не соответствует текущему изображению программного обеспечения устройства, элемент PS ОБЯЗАН запросить указанный файл через протокол TFTP от сервера программного обеспечения.
- Элемент PS ОБЯЗАН проверить, что загруженное изображение программного обеспечения является для него соответствующим. Если загруженное изображение программного обеспечения является соответствующим, то элемент PS ОБЯЗАН записать новое изображение программного обеспечения в энергонезависимое запоминающее устройство. Как только перенос файла успешно закончен, устройство ОБЯЗАНО перезапустить себя с новым кодовым изображением.

  – Если элемент PS неспособен закончить перенос файла по любой причине, элемент PS ОБЯЗАН оставаться способным к принятию новых загрузок программного обеспечения (без взаимодействия с оператором или пользователем), даже если питание или связность между попытками нарушается.
  - Элемент PS ОБЯЗАН зарегистрировать неудачи загрузки программного обеспечения и МОЖЕТ асинхронно сообщать о неудачах сетевому администратору.
  - Там, где программное обеспечение было обновлено, чтобы соответствовать новой версии этой Рекомендации, в таком случае является критическим то, что программное обеспечение ОБЯЗАНО работать с предыдущей версией, чтобы позволить постепенный переход блоков на сети.
  - Элемент PS ОБЯЗАН удостоверять подлинность инициатора загрузки программного обеспечения.
  - Элемент PS ОБЯЗАН проверить, что загруженный код не был изменен по сравнению с первоначальной формой, в которой он был предоставлен источником, которому доверяют.
  - Процесс загрузки программного обеспечения ОБЯЗАН обеспечивать оператора механизмами, чтобы обновлять или понижать кодовую версию элементов.
  - Процесс загрузки программного обеспечения ОБЯЗАН обеспечивать варианты выбора для оператора, чтобы диктовать свои собственные алгоритмы загрузки
  - Производитель файла кода ОБЯЗАН применять Подпись проверки кода (*CVS, Code Verification Signature*) по кодовому изображению и по любым другим удостоверенным атрибутам, как определено в этой Рекомендации для цифровой подписи структуры PKCS*7 к файлу кода; закрытый ключ, используемый для применения подписи, ОБЯЗАН быть ограничен сертификатом открытого ключа, что прикрепляется к корню CVC. Подпись производителя подтверждает подлинность источника и целостности файла кода.

- В дополнение к подписи производителя одобрить файл кода МОЖЕТ совместно подписывающая сторона (оператор или услуга PS).
- Элемент PS ОБЯЗАН быть способен обрабатывать цифровую подпись PKCS#7 и сертификат X.509, как соответственно определено в 11.3.7.2.1.1 и 11.3.7.3.
- (Дополнительное): Элементу PS СЛЕДУЕТ быть способным обновлять Открытый ключ CA корня CVC, хранимый в устройстве.
- (Дополнительное): Элементу PS СЛЕДУЕТ быть способным заменять Сертификат (сертификаты) CA производителя, хранимый в устройстве.
- (Дополнительное): Элементу PS СЛЕДУЕТ быть способным обновлять сертификат CA CVC, хранимый в устройстве.

Дополнительная загрузка Открытого ключа CA корня CVC, Сертификата CA CVC, и/или Сертификата CA производителя как часть файла кода позволяет ясно отличать кодовое изображение от других параметров в файле кода загрузки. Она также делает возможной изменять Открытый ключ CVC корня, Сертификат CA CVC, Сертификаты CA производителя или параметры SignedData в файле кода загрузки, не прерывая или не изменяя кодовое изображение, которое элемент PS будет получать. Это разрешает элементу PS проверять, что кодовое изображение не было изменено даже притом, что файл кода загрузки изменился из-за изменений в Открытом ключе CA корня CVC, в Сертификате CA CVC, в Сертификатах CA производителей или в параметрах SignedData.

11.3.7.1 Загрузка программного обеспечения в элементы PS

Так как элемент PS является встроенным в кабельный модем, то изображение PS/CM ОБЯЗАНО быть единственным изображением, а загрузка программного обеспечения ОБЯЗАНА выполняться только кабельным модемом.

11.3.7.2 Требования файла кода

11.3.7.2.1 Структура файла загрузки кода для безопасной загрузки программного обеспечения

Для безопасной загрузки программного обеспечения, файл кода разгрузки является файлом, построенным с использованием структуры, подчиняющейся PKCS*7, которая была определена в конкретном формате для использования с элементами PS. Файл кода ОБЯЗАН соответствовать документу [PKCS*7] и ОБЯЗАН быть кодируемым согласно правилам DER. Файл кода ОБЯЗАН соответствовать структуре, показанной в Таблице 45.

При загрузке Открытого ключа CA корня CVC и/или Сертификатов CA (например, Сертификат CA CVC и/или Сертификат CA производителя) как части файла кода, сертификаты МОГУТ соответственно содержаться в объекте RootCAPublicKey и/или в полях CACerts, как определено в Таблице 45, и отделены от фактического кодового изображения, содержавшегося в поле CodeImage.

11.3.7.2.1.1 Подписанные данные

Файл загрузки кода будет содержать информацию в типе содержимого Подписанных данных PKCS*7, как показано в Таблице 46. Хотя при поддержании согласия с документом [PKCS*7] используемая структура была ограничена в формате, чтобы облегчить обработку, выполняемую услугой PS, чтобы утвердить подпись. PKCS*7 Подписанные данные ОБЯЗАНЫ быть кодируемым по правилам DER и точно соответствовать структуре, показанной ниже, за исключением любого изменения в порядке, требуемом для кодирования DER (например, приведение в порядок атрибутов SET OF). Элементу PS СЛЕДУЕТ отклонить подпись PKCS*7, если Подписанные данные PKCS*7 не соответствуют структуре, кодированной согласно правилам DER.

Таблица 45/J.191 – Структура файла кода

Файл кода	Описание
Цифровая подпись PKCS#7 {	
ContentInfo	
ContentType	SignedData
SignedData ()	ТОЧНОЕ подписанное значение содержимого данных: включает в себя сертификат CVS и сертификаты CVC, подчиняющиеся X.509
} *конец цифровой подписи PKCS#7*	
SignedContent {	
DownloadParameters {	Обязательный формат TLV (Тип 28). (Длина равна нулю, если нет под-значений TLV.)
RootCAPublicKey ()	Дополнительное значение TLV для Открытого ключа CA корня CVC CL, форматированного согласно формату Открытого ключа RSA (Тип 4).
CACerts ()	Дополнительное значение TLV для одного или более DER-кодированного сертификата (сертификатов), каждый из которых кодирован согласно формату TLV CA-сертификата (Тип 17).
}	
CodeImage ()	Обновить кодовое изображение
} *конец SignedContent*	

Таблица 46/J.191 – Подписанные данные PKCS#7

Поле PKCS#7	Описание
Подписанные данные {	
версия	версия = 1
DigestAlgorithmIdentifiers	SHA-1
ContentInfo	
ContentType	данные (объект SignedContent сцеплен в конце структуры PKCS#7)
сертификаты {	(Сертификат проверки кода CableLabs (*CVC, Code Verification Certificate*))
mfgCVC	(ТРЕБУЕТСЯ для всех файлов кодов)
co-signerCVC	(ДОПОЛНИТЕЛЬНЫЙ; требуется для совместных подписей)
} *конец сертификатов*	
SignerInfo {	
MfgSignerInfo {	(ТРЕБУЕТСЯ для всех файлов кодов)
версия	версия = 1
issuerAndSerialNumber	
issuerName	
CountryName	US
organizationName	CableLabs

Таблица 46/J.191 – Подписанные данные PKCS#7

CommonName	CA корень CableLabs CVC
certificateSerialNumber	<порядковый номер CVC Mfg >
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	данные (contentType из signedContent)
Время подписания	UTCTime(GMT),YYMMDDhhmmssZ
messageDigest	(каталог содержимого, как определено в [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *конец info подписавшейся стороны mfg*	
CoSignerInfo {	(ДОПОЛНИТЕЛЬНЫЙ; требуется для совместных подписей)
версия	версия = 1
issuerandserialnumber	
issuername	
CountryName	US
organizationName	CableLabs
CommonName	CableLabs CVC Root CA
certificateSerialNumber	<порядковый серийный номер CVC coSigner >
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	данные (contentType из signedContent)
signing Time	UTCTime (GMT),YYMMDDhhmmssZ
messageDigest	(каталог содержимого, как определено в [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *конец info подписавшей стороны mso*	
} *конец инфо подписавшей стороны*	
} *конец подписанных данных*	

11.3.7.2.1.2 Подписанное содержимое

Поле подписанного содержимого для файла кода содержит кодовое изображение и поле параметров загрузки, которое, возможно, содержит дополнительные пункты – Открытый ключ CA корня CVC и CA Сертификатов (например, Сертификат CA CVC и/или Сертификат CA производителя).

Заключительное кодовое изображение находится в формате, совместимом с элементом PS пункта назначения. В поддержку требований подписи PKCS*7, кодовое содержание печатается как данные; т.е. простая строка октета. Формат заключительного кодового изображения здесь не определяется, и будет определяться каждым производителем согласно их требованиям.

Каждому производителю СЛЕДУЕТ строить свой код с дополнительными механизмами, которые проверяют, что обновленное кодовое изображение совместимо с элементом PS пункта назначения.

Если он включен в поле подписанного содержимого, Открытый ключ CA корня CVC предназначен для замены Открытого ключа CA корня CVC, хранимого в настоящее время в элементе PS. Если загрузка кода и установка являются успешными, то элемент PS ОБЯЗАН заменить свой Открытый ключ CA корня CVC, хранимый в настоящее время, Открытым ключом CA корня CVC, полученным в поле подписанного содержимого. Этот новый Открытый ключ CA корня CVC будет затем использоваться для последующей проверки сертификата CVC.

Если он включен в поле подписанного содержимого, Сертификат (сертификаты) CA предназначен для замены Сертификата (сертификатов) CA, который в настоящее время хранится в элементе PS. Например, если загрузка кода и установка были успешными, а объект CACert, содержал Сертификат CA производителя, то элемент PS ОБЯЗАН заменить свой хранимый в настоящее время Сертификат (сертификаты) производителя Сертификатом (сертификатами) производителя, полученным в поле подписанного содержимого.

11.3.7.2.1.3 Ключи подписания кода

Цифровая подпись PKCS*7 использует Алгоритм шифрования RSA с помощью SHA-1 [FIPS 186]. Модуль ключа RSA для подписания кода составляет в длине 2048 битов. Элемент PS ОБЯЗАН быть способен проверять подписи файлов кодов, которые подписаны, используя этот размер модуля. Открытый есть F4 (десятичное число 65537).

11.3.7.3 Формат "Сертификат проверки кода " (CVC)

11.3.7.3.1 Формат CVC для безопасной загрузки программного обеспечения

Для безопасной загрузки программного обеспечения, формат, используемый для сертификата CVC, подчиняется документу X.509. Однако структура X.509 была ограничена, чтобы облегчить обработку, которую элемент PS делает, чтобы утвердить сертификат и извлечь открытый ключ, используемый для проверки подписи CVC. Подпись CVC ОБЯЗАНА быть кодируемой согласно правилам DER и точно соответствовать структуре, показанной в Таблице 47, за исключением любых изменений, в порядке, требуемом для кодирования DER (например, приведение в порядок атрибутов SET OF). Элементу PS СЛЕДУЕТ отклонить сертификат CVC, если он не соответствует кодируемой структуре по правилам DER, представленной в Таблице 47.

11.3.7.3.2 Отмена сертификата

Эта Рекомендация не требует или не определяет использование перечней отмены сертификатов (*CRL, certificate revocation lists*). От элемента PS не требуется поддерживать перечни CRL. Операторы могут желать определять и использовать перечни CRL вне сети HFC, чтобы помогать управлять файлами кода, которые предоставлены им производителями. Однако есть метод для отмены сертификатов, основанный на дате начала достоверности сертификата. Этот метод требует, чтобы обновленный сертификат CVC был доставлен элементу PS с обновленным временем начала достоверности. Как только сертификат CVC успешно удостоверяется, время начала достоверности документа X.509 будет обновлять текущее значение элемента PS из объекта cvcAccessStart.

Таблица 47/J.191 – Сертификат проверки кода, подчиняющегося документу X.509

Сертификат X.509	Описание
Сертификат {	
версия	2 (т.е., версия 3 документа X.509)
SerialNumber	целое число, из 8 октетов (т.е., уникальное число, назначенное с помощью CA корня)
Подпись	SHA-1 RSA, нулевые параметры
выпускающая сторона	
countryName	US
organizationName	CableLabs
commonName	CA корня CVC CableLabs
достоверность	
notBefore	utcTime (GMT), YYMMDDhhmmssZ (т.е., время выпуска)
notAfter	utcTime (GMT), YYMMDDhhmmssZ
субъект	
countryName	<Название страны>
organizationName	<Название организации>
commonName	<Общее название>
subjectPublicKeyInfo	
Алгоритм	шифрование RSA, нулевые параметры
SubjectPublicKey	модуль в 2048 битов
расширение	
KeyUsage	<Использование ключа>
authorityKeyIdentifier	<Идентификатор ключа полномочий>
signatureAlgorithm	SHA-1 RSA, нулевые параметры
Значение подписи	<Значение подписи>
} *конец сертификата*	

11.3.7.4 Директивы доступа файла кода

Для безопасной загрузки программного обеспечения специальные значения управления включаются в файл кода для элемента PS, чтобы проверять перед тем, как он удостоверит изображение кода. Условия, налагаемые на значения этих параметров управления, ОБЯЗАНЫ быть удовлетворены прежде, чем элемент PS удостоверит сертификат CVC или подпись CVS, и примет изображение кода.

11.3.7.4.1 Названия организаций субъектов

Элемент PS будет опознавать до двух названий, в любой момент времени, что он рассматривает как доверенных агентов, подписывающих код, в поле субъекта CVC файла кода. Эти названия включают:

- производитель устройства: название производителя в поле субъекта CVC ОБЯЗАНО точно соответствовать названию производителя, сохраненному в энергонезависимой памяти элемента PS производителем. Сертификат CVC производителя всегда ОБЯЗАН включаться в файл кода.
- агент совместно подписывающей стороны: Разрешено, чтобы другая доверенная организация совместно подписывала файлы кодов, предназначенные устройству. В большинстве случаев это есть оператор, управляющий текущим эксплуатационным доменом устройства. Название организации совместно подписывающей стороны

сообщается элементу PS через сертификат CVC совместно подписывающей стороны в файле конфигурации при установке в начальное положение процесса проверки кода элемента PS. Название совместно подписывающей организации в поле субъекта CVC совместно подписывающей стороны ОБЯЗАНО точно соответствовать названию совместно подписывающей организации, предварительно полученному в сертификате CVC установки в начальное положение совместно подписывающей стороны и сохраненному элементом PS.

Элемент PS МОЖЕТ сравнивать названия организаций, используя двоичное сравнение.

11.3.7.4.2 Директивы, меняющиеся со временем

Чтобы уменьшить возможность получения элементом PS предыдущего файла кода через атаку воспроизведения, файлы кодов включают в себя значение времени подписания в структуре PKCS*7, что может использоваться для указания времени, когда кодовое изображение было подписано. Элемент PS ОБЯЗАН хранить два значения времени UTC, связанные с каждым подписывающим код агентом. Один набор ОБЯЗАН всегда храниться и поддерживаться для производителя устройства. Кроме того, если файл кода совместно подписан другой стороной, элемент PS ОБЯЗАН также хранить и поддерживать отдельный набор значений времени для совместно подписывающей стороны.

Эти значения используются, чтобы управлять доступом файла кода к элементу PS, индивидуально управляя достоверностью подписи CVS и сертификатом CVC. Этими значениями являются:

- codeAccessStart: значение времени UTC из 12 байтов, отнесенное ко времени по Гринвичу (*GMT, Greenwich Mean Time*).
- cvcAccessStart: значение времени UTC из 12 байтов, отнесенное ко времени по Гринвичу.

Значения UTCTime в сертификате CVC ОБЯЗАНЫ быть выражены как время по Гринвичу (GMT) и должно включать секунды. То есть, они ОБЯЗАНЫ быть выражены в следующей форме: YYMMDDhhmmssZ. Поле года (YY) ОБЯЗАНО истолковываться следующим образом:

- Там, где YY больше или равно 50, год должен истолковываться как 19YY.
- Там, где YY меньше, чем 50, год должен истолковываться как 20YY.

Эти значения всегда будут относиться ко времени по Гринвичу, поэтому заключительный знак (Z) кода ASCII может быть удален, когда хранится элементом PS в качестве codeAccessStart и cvcAccessStart.

Элемент PS ОБЯЗАН поддерживать каждое из этих значений времени в формате, который содержит эквивалентную информацию времени и точность к формату UTV с 12 знаками (т.е., YYMMDDhhmmss). Элемент PS ОБЯЗАН точно сравнивать эти хранимые значения со значениями времени UTC, доставленными элементу PS в сертификате CVC. Эти требования обсуждаются позже в этой Рекомендации.

Значения объектов codeAccessStart и cvcAccessStart, соответствующие производителю элемента PS, ОБЯЗАНЫ НЕ уменьшаться. Значения объектов codeAccessStart и cvcAccessStart, соответствующие совместно подписывающей стороне, ОБЯЗАНЫ НЕ уменьшаться, пока не изменяет совместно подписавшая сторона, а элемент PS поддерживает такие меняющиеся со временем значения директив совместно подписавшей стороны.

11.3.7.5 Установление в начальное положение обновления кода

11.3.7.5.1 Установление производителя в начальное положение

Ответственностью производителя является правильно установить начальную версию кода в элементе PS.

Для поддержки безопасной загрузки программного обеспечения, значения для изменяющихся во времени директив производителя ОБЯЗАНЫ быть загружены в энергонезависимую память элемента PS:

- Название организации производителя элемента PS
- Значения директив производителя, меняющихся во времени:
  a) значение установления в начальное положение codeAccessStart;
  b) значение установления в начальное положение cvcAccessStart.

Название организации производителя элемента PS ОБЯЗАНО всегда присутствовать в устройстве. Название организации производителя элемента PS МОЖЕТ быть сохранено в изображении кода устройства. Название производителя, используемое для обновления кода, не обязательно является тем же самым названием, используемым в Сертификате CA производителя.

Значения директив, меняющихся во времени, codeAccessStart и cvcAccessStart, ОБЯЗАНЫ быть установлены в начальное положение по отношению ко времени UTC, совместимому со временем начала достоверности последнего сертификата CVC производителя. Эти значения, меняющиеся во времени, будут периодически обновляться при нормальной эксплуатации через сертификаты CVC производителя, которые принимаются и проверяются элементом PS.

11.3.7.5.2 Установление сети в начальное положение

В поддержке проверки кода Файл конфигурации PS используется как заверенное средство, чтобы устанавливать в начальное положение процесс проверки кода. В файле конфигурации элемента PS, элемент PS получает установки конфигурации, уместные для проверки обновления кода.

Файлу конфигурации СЛЕДУЕТ всегда включать самый современный сертификат CVC, применимый для элемента PS пункта назначения; но когда файл конфигурации используется, чтобы инициировать обновление кода, он ОБЯЗАН включать в себя Сертификат проверки кода (*CVC, Code Verification Certificate*), чтобы задавать начальные условия элементу PS для получения файлов кода согласно этой Рекомендации. Независимо от того, требуется ли обновление кода или нет, сертификат CVC в файле конфигурации ОБЯЗАН быть обработан элементом PS. Файл конфигурации МОЖЕТ содержать:

- Отсутствие сертификата CVC – Элемент PS ОБЯЗАН НЕ признавать файл кода.
- Только сертификат CVC производителя - Перед признанием файла кода элемент PS ОБЯЗАН проверить что сертификат CVC производителя тянется цепью до корня CVC. Когда файл конфигурации элемента PS содержит только сертификат CVC действительного производителя, только тогда устройство будет требовать подпись производителя на файлах кода. В этом случае, элемент PS ОБЯЗАН НЕ признавать файлы кода, которые были подписаны совместно.
- Только сертификат CVC совместно подписавшей стороны - Перед приемкой файла кода элемент PS ОБЯЗАН проверить, что сертификат CVC совместно подписавшей стороны тянется цепью до Корня CVC. Когда файл конфигурации элемента PS содержит действительный сертификат CVC совместно подписавшей стороны, он используется, чтобы задать начальные условия устройству с помощью совместно подписавшей стороны. Будучи удостоверенным, название субъекта CVC organizationName станет совместно подписавшей стороной кода, назначенной

элементу PS. Чтобы элемент PS мог впоследствии принять кодовое изображение, совместно подписывающая сторона, в дополнение к производителю устройства, ОБЯЗАНА была подписать файл кода.

- И сертификат CVC производителя, и сертификат CVC совместно подписывающей стороны. Перед приемкой файла кода элемент PS ОБЯЗАН проверить, что оба сертификата CVC тянутся цепью до Корня CVC.

Прежде, чем элемент PS запустит свои способности обновлять файлы кода на сети, он ОБЯЗАН получить действительный сертификат CVC в файле конфигурации. Кроме того, когда файл конфигурации элемента PS не содержит действительный сертификат CVC, а его способность обновлять файлы кода была повреждена, элемент PS ОБЯЗАН отклонить любую информацию в сертификате CVC, впоследствии поставленном через протокол SNMP.

Название организации производителя элемента PS и значения директив, изменяющихся во времени, ОБЯЗАНЫ всегда присутствовать в элементе PS. Если элемент PS устанавливается в начальное положение, чтобы принять код, совместно подписанный дополнительной совместно подписавшей стороной, название организации, и их соответствующие значения директив, изменяющиеся во времени, ОБЯЗАНЫ быть сохранены и поддержаны, пока они эксплуатируются. В памяти элемента PS ОБЯЗАНО быть распределено место для следующих значений директив совместно подписавшей стороны:

1) название организации агента совместного подписания;
2) изменяющиеся во времени значения директив совместно подписавшей стороны:
   a) cvcAccessStart;
   b) codeAccessStart.

Набор этих значений производителя ОБЯЗАН быть сохранен в энергонезависимой памяти элемента PS и не утерян, когда источник питания устройства удаляется, или в течение начальной перезагрузки.

Когда элементу PS назначена совместно подписывающая сторона, набор значений CVC совместно подписывающей стороны ОБЯЗАН быть сохранен в памяти элемента PS. Элемент PS МОЖЕТ сохранить эти значения в энергонезависимой памяти, которая не будет потеряна, когда источник питания устройства удаляется, или в течение начальной перезагрузки. Однако при назначении совместно подписывающей стороны элементу PS, сертификат CVC всегда находится в файле конфигурации. Поэтому элемент PS будет всегда получать значения директив совместно подписывающей стороны в течение стадии установления в начальное положение, и не требуется хранить значения директив совместно подписывающей стороны, когда основное питание потеряно, или в течение процесса начальной перезагрузки.

11.3.7.6 Обработка сертификата CVC

Чтобы ускорить поставку обновленного сертификата CVC, не требуя от услуги PS обрабатывать обновление кода, сертификат CVC МОЖЕТ быть доставлен либо в файле конфигурации, либо в базе MIB протокола SNMP. Формат CVC является тем же самым, находится ли он в файле кода, в файле конфигурации или в базе MIB протокола SNMP.

11.3.7.6.1 Обработка сертификата CVC файла конфигурации

Когда сертификат CVC включается в файл конфигурации, элемент PS ОБЯЗАН проверить, сертификат CVC перед принятием любой из установок обновления кода, которые он содержит. При получении сертификата CVC в файле конфигурации, элемент PS ОБЯЗАН выполнить следующие шаги подтверждения и процедуры. Если любая из следующих проверок подтверждения терпит неудачу, элемент PS ОБЯЗАН сразу же остановить процесс проверки CVC и зарегистрировать ошибку, если применяется. Если файл конфигурации элемента PS не включает в себя сертификат CVC, который подтверждается должным образом,

элемент PS ОБЯЗАН НЕ загружать файлы обновления кода, вне зависимости от того, запущены ли они файлом конфигурации элемента PS, или через базу MIB протокола SNMP. Кроме того, если файлы конфигурации элемента PS не включают в себя сертификат CVC, который удостоверяется должным образом, от элемента PS не требуется обрабатывать сертификаты CVC, впоследствии поставленные через базу MIB протокола SNMP, и он ОБЯЗАН НЕ принимать информацию от сертификата CVC, впоследствии поставленного через базу MIB протокола SNMP.

При получении сертификата CVC в файле конфигурации, элемент PS ОБЯЗАН:

1) проверить, что расширение использования продленного ключа находится в сертификате CVC, как определено в 11.3.2.2.2.;

2) проверить название организации субъекта CVC.

   a) Если сертификат CVC является сертификатом CVC производителя (Тип 32), тогда:

      i) Если название организации идентично названию производителя устройства, ТО ТОГДА это есть сертификат CVC производителя. В этом случае элемент PS ОБЯЗАН проверить, что время начала достоверности сертификата CVC производителя больше или равно значению cvcAccessStart производителя, которое в настоящий момент удерживается в элементе PS.

      ii) Если название организации не идентично названию производителя устройства, ТО ТОГДА этот сертификат CVC ОБЯЗАН быть отклонен, и должна быть зарегистрирована ошибка.

   b) Если сертификат CVC является сертификатом CVC совместно подписавшей стороны (Тип 33), то тогда:

      i) Если название организации является идентичным текущей стороне, совместно подписывающей код элемента PS, ТО ТОГДА это есть текущий сертификат CVC совместно подписавшей стороны, и элемент PS ОБЯЗАН проверить, что время начала достоверности больше или равно значению cvcAccessStart совместно подписавшей стороны, удерживаемому в элементе PS.

      ii) Если название организации не является идентичным текущему названию стороны, совместно подписывающей код, ТО ТОГДА после того, как сертификат CVC был проверен на достоверность (и регистрация завершена), это название организации субъекта станет новой стороной, совместно подписывающей код элемента PS. Элемент PS ОБЯЗАН НЕ признавать файл кода, пока он не был подписан производителем и не подписан этой совместно подписывающей стороной.

3) проверить достоверность подписи выпускающей стороны CVC, используя Открытый ключ CA сертификата CVC, удерживаемый элементом PS.

4) проверить достоверность подписи CA сертификата CVC, используя Открытый ключ CA корня CVC, удерживаемый элементом PS. Проверка подписи будет подтверждать подлинность источника и утвердит доверие к параметрам CVC

5) обновить текущее значение элемента PS из объекта cvcAccessStart, соответствующего названию организации субъекта CVC (т.е. производителю или совместно подписывающей стороне) со значением времени начала достоверности от утвержденного сертификата CVC. Если значение времени начала достоверности больше, чем текущее значение codeAccessStart элемента PS, то обновить значение codeAccessStart элемента PSD с помощью значения времени начала достоверности. Элементу PS СЛЕДУЕТ сбросить любые остатки сертификата CVC.

11.3.7.6.2 Обработка сертификата CVC протокола SNMP

Элемент PS ОБЯЗАН обрабатывать доставленные сертификаты CVC протокола SNMP, когда позволяется обновление файлов кода; иначе, все сертификаты CVC, поставленные через протокол SNMP, ОБЯЗАНЫ быть отклонены. При подтверждении сертификата CVC, поставленного через протокол SNMP, элемент PS ОБЯЗАН выполнить следующее подтверждение и процедурные шаги. Если любая из следующих проверок подтверждения терпит неудачу, элемент PS ОБЯЗАН сразу же остановить процесс проверки CVC, зарегистрировать ошибку, если применяется, и удалить все остатки процесса к такому шагу.

Элемент PS ОБЯЗАН:

1) проверить, что расширение использования продленного ключа находится в сертификате CVC, как определено в 11.3.2.2.2.

2) проверить название организации субъекта CVC.

   a) Если название организации идентично названию производителя устройства, ТО ТОГДА это есть сертификат CVC производителя. В этом случае элемент PS ОБЯЗАН проверить, что время начала достоверности сертификата CVC производителя больше или равно значению cvcAccessStart производителя, которое в настоящий момент удерживается в элементе PS.

   b) Если название организации идентично текущей стороне, совместно подписывающей код элемента PS, ТО ТОГДА это есть сертификат CVC текущей совместно подписывающей стороны, и время начала достоверности ОБЯЗАНО быть больше, чем значение cvcAccessStart совместно подписывающей стороны, которое в настоящий момент удерживается в элементе PS.

   c) Если название организации не идентично названию производителя устройства или текущему названию совместно подписывающей стороны, ТО ТОГДА элемент PS ОБЯЗАН сразу же отклонить этот сертификат CVC.

3) проверить достоверность подписи выпускающей стороны сертификата CVC, используя Открытый ключ CA сертификата CVC, удерживаемый элементом PS.

4) проверить достоверность подписи CA сертификата CVC, используя Открытый ключ CA корня CVC, удерживаемый элементом PS. Проверка подписи будет санкционировать сертификат и подтверждать доверие во время начала достоверности CVC.

5) обновить текущее значение для значений cvcAccessStart с подтвержденным значением времени начала достоверности сертификата CVC. Если значение времени начала достоверности больше, чем текущее значение codeAccessStart элемента PS, то обновить значение codeAccessStart элемента PS с помощью значения времени начала достоверности. Все параметры сертификатов, КРОМЕ времени начала достоверности, больше не нужны и их СЛЕДУЕТ сбросить.

11.3.7.7 Требования подписания кода

11.3.7.7.1 Требования полномочий сертификата (CA)

Сертификаты проверки кода (*CVC, Code Verification Certificates*) подписываются и выпускаются с помощью полномочий CA сертификата CVC. Сертификат CVC ОБЯЗАН быть точно таким, как определено в 11.3.7.3. CA сертификата CVC ОБЯЗАНО НЕ подписывать какой-либо сертификат CVC, пока он не идентичен формату, указанному в таком разделе. Перед подписанием сертификата CVC, CA сертификата CVC ОБЯЗАН проверить, что запрос сертификата является подлинным.

Полномочия CA сертификата CVC будут нести ответственность за регистрацию названий санкционированных абонентов CVC. Абоненты CVC включают в себя производителей и оператора элемента PS, которые будут совместно подписывать кодовые изображения. Ответственностью CA сертификата CVC будет гарантирование того, что название организации каждого абонента CVC является отличающимся. При назначении названий организаций для сторон, совместно подписывающих файлы кода, ОБЯЗАНЫ быть предписаны следующие руководящие принципы:

- Название организации, используемое для своей идентификации в качестве агента стороны, совместно подписывающей код в сертификате CVC, ОБЯЗАНО быть назначено организацией, которая выпустила сертификат корня.
- Название ОБЯЗАНО быть строкой, пригодной для печати, из восьми 16-ричных цифр, которая уникальным образом отличает агента, подписывающего код, от всех других.
- Каждая 16-ричная цифра в названии ОБЯЗАНА быть выбрана из набора знаков 0-9 (0x30-0x39) или A-F (0x41-0x46).
- Строка, состоящая из восьми цифр 0, не разрешается и ОБЯЗАНА НЕ использоваться в сертификате CVC.

Чтобы сохранять пространство запоминающего устройства, элемент PS МОЖЕТ внутренне представить название стороны, совместно подписывающей код, в дополнительном формате, пока вся информация обслуживается, а первоначальный формат может быть воспроизведен; например, как целое 32-разрядное число, отличное от нуля, со значением целого числа 0, представляющего отсутствие стороны, подписывающей код.

11.3.7.7.1.1 Требования сертификата CVC производителя

Чтобы подписывать свои файлы кодов, производитель ОБЯЗАН получить действительный сертификат CVC от CA сертификата CVC. Все кодовые изображения производителя, предоставленные оператору для дистанционного обновления устройства, ОБЯЗАНЫ быть подписаны согласно требованиям, определенным в этой Рекомендации. При подписании файла кода, производитель МОЖЕТ выбрать вариант, чтобы не обновлять значение signingTime PKCS*7 в информации подписания производителя. Эта Рекомендация требует, чтобы значение signingTime PKCS*7 было равно или больше, чем время начала достоверности CVC. Если производитель использует значение signingTime, равное времени начала достоверности CVC при подписании ряда файлов кодов, то такие файлы кодов могут использоваться и повторно использоваться. Это позволяет оператору использовать файл кода, чтобы или обновлять или понижать версию кода для устройств такого производителя. Эти файлы кодов будут действительны до тех пор, пока новый сертификат CVC не будет произведен и получен элементом PS.

11.3.7.7.1.2 Требования оператора

Когда оператор получает файлы кодов обновления программного обеспечения от производителя, оператору СЛЕДУЕТ утвердить кодовое изображение, используя Открытый ключ CA сертификата CVC. Это позволит оператору проверять, что кодовое изображение является таким, как построено производителем, которому доверяют. Оператор может перепроверить файл кода в любое время, повторяя процесс.

Если оператор хочет осуществить вариант выбора совместного подписания кодового изображения, предназначенного для устройства на своей сети, оператор ОБЯЗАН получить действительный сертификат CVC от CA сертификата CVC.

При подписании файла кода оператор ОБЯЗАН совместно подписывать содержимое кода файла согласно стандарту подписи PKCS*7, и включать свой сертификат CVC оператора, как определено в 11.3.7.2.1.1. Это приложение не требует от оператора совместно подписывать

файлы кодов; но когда оператор следует всем правилам, определенными в этой Рекомендации для того, чтобы готовить файл кода, элемент PS ОБЯЗАН это принять.

11.3.7.8 Процесс запуска

Загрузки кодов, независимо от режима обеспечения, могут быть начаты в течение процесса обеспечения и регистрации через загрузку, инициированную конфигурацией файла; или в течение нормального действия, используя команду загрузки, инициированную протоколом SNMP. Элемент PS ОБЯЗАН поддерживать оба метода.

ПРИМЕЧАНИЕ - До запуска безопасной загрузки программного обеспечения, соответствующая информация CVC ОБЯЗАНА быть включена в файл конфигурации. Если в качестве метода запуска безопасной загрузки программного обеспечения оператор решает использовать загрузку, инициированную протоколом SNMP, то рекомендуется, чтобы информация CVC всегда присутствовала в файле конфигурации так, что элемент PS всегда будет иметь информацию CVC, установленную в начальное положение, когда необходимо. Если оператор в качестве метода запуска безопасной загрузки программного обеспечения решает использовать загрузку, инициированную конфигурацией файла, то нужно, чтобы информация CVC присутствовала в файле конфигурации в то время, когда устройство осуществляет начальный перезапуск, чтобы получить файл конфигурации, который запустит обновление.

11.3.7.8.1 Загрузка программного обеспечения, инициированная протоколом SNMP

От станции сетевого административного управления:

- установить объект docsDevSwServer к адресу сервера TFTP для обновлений программного обеспечения;
- установить объект docsDevSwFilename к имени тракта файла изображения обновления программного обеспечения;
- установить объект docsDevSwAdminStatus к объекту Upgrade-from-mgt [*обновить из*]. Объект docsDevSwAdminStatus ОБЯЗАН оставаться постоянным при переустановке/начальных перезагрузках до тех пор, пока не будет перезаписан заново от управляющей программы SNMP или через файл конфигурации элемента PS.

Состояние по умолчанию объекта docsDevSwAdminStatus ОБЯЗАНО быть allowProvisioningUpgrade {2}, пока это не переписано с помощью объекта ignoreProvisioningUpgrade {3} после успешного обновления программного обеспечения, инициированного протоколом SNMP, или в противном случае изменено станцией управления. Объект docsDevSwOperStatus ОБЯЗАН сохраняться во время переустановок, чтобы сообщать о результате последней попытки обновления программного обеспечения

Если в течение обновления, инициированного протоколом SNMP, в элементе PS имеет место пропадание питания или переустановка, то элемент PS ОБЯЗАН возобновить обновление, не требуя ручного вмешательства, и когда элемент PS возобновляет процесс обновления:

- объект docsDevSwAdminStatus ОБЯЗАН быть Upgrade-from-mgt{1};
- объект docsDevSwFilename ОБЯЗАН быть именем файла изображения программного обеспечения, подлежащего обновлению;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего изображение программного обеспечения, подлежащее обновлению;
- объект docsDevSwOperStatus ОБЯЗАН быть inProgress{1};
- объект docsDevSwCurrentVers ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

В случае, где элемент PS достигает максимального числа повторений (максимум повторений = 3), являющихся результатом многократных пропаданий питания или переустановок в течение обновления, инициированного протоколом SNMP, статус элемента PS ОБЯЗАН придерживаться следующих требований после того, как он зарегистрирован:

- объект docsDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};
- объект docsDevSwFilename ОБЯЗАН быть именем файла программного обеспечения, которое потерпело неудачу процесса обновления;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего программное обеспечение, что потерпело неудачу процесса обновления;
- объект docsDevSwOperStatus ОБЯЗАН быть другим {5};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

Если элемент PS исчерпывает требуемое число повторений TFTP, выпуская в сумме 16 следующих друг за другом повторений, элемент PS ОБЯЗАН вернуться назад к последнему известному рабочему изображению, перейти к действующему состоянию и придерживаться следующих требований:

- объект docDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};
- объект docDevSwFilename ОБЯЗАН быть именем файла программного обеспечения, что потерпело неудачу процесса обновления;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего программное обеспечение, что потерпело неудачу процесса обновления;
- объект docsDevSwOperStatus ОБЯЗАН быть потерпевшим неудачу{4};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

После того, как элемент PS закончил безопасное обновление программного обеспечения, инициированное протоколом SNMP, элемент PS ОБЯЗАН осуществить начальную перезагрузку и стать действующим с правильным изображением программного обеспечения, а после того, как устройство становится действующим, он ОБЯЗАН придерживаться следующих требований:

- установить свой объект docsDevSwAdminStatus в ignoreProvisioningUpgrade{3};
- установить свой объект docsDevOperStatus в completeFromMgt{3};
- осуществить начальную перезагрузку.

Элемент PS ОБЯЗАН соответствующим образом использовать статус ignoreProvisioningUpgrade, чтобы проигнорировать значение обновления программного обеспечения, которое может быть включено в файл конфигурации элемента PS, и стать действующим с правильным изображением программного обеспечения, а после того, как устройство стало действующим, он ОБЯЗАН придерживаться следующих требований:

- объект docsDevSwAdminStatus ОБЯЗАН быть ignoreProvisioningUpgrade{3};
- объект docsDevSwFilename МОЖЕТ быть именем файла программного обеспечения, действующего в настоящее время в элементе PS;
- объект docsDevSwServer МОЖЕТ быть адресом сервера TFTP, содержащего программное обеспечение, которое в настоящее время действует в элементе PS;
- объект docsDevSwOperStatus ОБЯЗАН быть completeFromMgt{3};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в элементе PS.

В случае, где элемент PS успешно загружает (или обнаруживает в течение загрузки) изображение, которое не предназначено для устройства:

- объект docsDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};

- объект docsDevSwFilename ОБЯЗАН быть именем файла программного обеспечения, которое потерпело неудачу в обновлении;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего программное обеспечение, которое потерпело неудачу процесса обновления;
- объект docsDevSwOperStatus ОБЯЗАН быть другим{5};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

В случае, где элемент PS определяет, что изображение загрузки повреждено или искажено, элемент PS ОБЯЗАН отклонить заново загруженное изображение. Элемент PS МОЖЕТ осуществить повторную попытку загрузки, если число MAX повторений последовательности TFTP не было достигнуто. Если элемент PS не хочет осуществлять повторение, а число MAX повторений последовательности TFTP не было достигнуто, то элемент PS ОБЯЗАН вернуться к последнему известному рабочему изображению и перейти к действующему состоянию, породить уведомление о соответствующем событии, как определено в 11.3.7.10, и придерживаться следующих требований:

- объект docsDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};
- объект docsDevSwFilename ОБЯЗАН быть именем файла программного обеспечения, которое потерпело неудачу в обновлении;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего программное обеспечение, которое потерпело неудачу процесса обновления;
- объект docsDevSwOperStatus ОБЯЗАН быть другим {5};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

В случае, где элемент PS определяет, что изображение повреждено или искажено, элемент PS ОБЯЗАН отклонить заново загруженное изображение. Элемент PS МОЖЕТ осуществить повторную попытку загрузить новое изображение, если число MAX повторений последовательности TFTP не было достигнуто. На 16-ой последовательной неудавшейся попытке загрузки программного обеспечения, элемент PS ОБЯЗАН вернуться к последнему известному рабочему изображению и перейти к действующему состоянию. В этом случае, элемент PS обязан послать два уведомления, одно, чтобы уведомить, что предел повторения TFTP MAX был достигнут, и другое, чтобы уведомить, что изображение повреждено. Сразу же после того, как элемент PS достигает действующего состояния, элемент PS ОБЯЗАН придерживаться следующих требований:

- объект docsDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};
- объект docsDevSwFilename ОБЯЗАН быть именем файла программного обеспечения, которое потерпело неудачу в обновлении;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего программное обеспечение, что потерпело неудачу процесса обновления;
- объект docsDevSwOperStatus ОБЯЗАН быть другим {5};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

11.3.7.8.2 Загрузка программного обеспечения, инициированная файлом конфигурации

Загрузка программного обеспечения, начинаемая файлом конфигурации, инициируется отправкой Имени файла обновления программного обеспечения в файле конфигурации элемента PS. Если Имя файла обновления программного обеспечения в файле конфигурации элемента PS не соответствует текущему изображению программного обеспечения устройства,

то элемент PS ОБЯЗАН запросить указанный файл через протокол TFTP от Сервера программного обеспечения.

ПРИМЕЧАНИЕ - Адрес IP Сервера программного обеспечения является отдельным параметром. Если он присутствует, то элемент PS пытается загружать указанный файл от этого сервера. Если он не присутствует, то элемент PS пытается загружать указанный файл от сервера файла конфигурации.

В случае, где элемент PS достигает максимального числа повторений (максимум повторений = 3), являющихся результатом многократных пропаданий питания или переустановок в течение обновления, начатого файлом конфигурации, статус элемента PS ОБЯЗАН придерживаться следующих требований после того, как он зарегистрирован:

- объект docsDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};
- объект docsDevSwFilename ОБЯЗАН быть именем файла программного обеспечения, которое потерпело неудачу процесса обновления;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего программное обеспечение, которое потерпело неудачу процесса обновления;
- объект docsDevSwOperStatus ОБЯЗАН быть другим {5};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

Если элемент PS исчерпывает требуемое число повторений TFTP, издавая в сумме 16 следующих друг за другом повторений, то элемент PS ОБЯЗАН вернуться к последнему известному рабочему изображению, перейти к действующему состоянию и придерживаться следующих требований:

- объект docDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};
- объект docDevSwFilename ОБЯЗАН быть именем файла программного обеспечения, которое потерпело неудачу процесса обновления;
- объект docsDevSwServer ОБЯЗАН быть адресом сервера TFTP, содержащего программное обеспечение, которое потерпело неудачу процесса обновления;
- объект docsDevSwOperStatus ОБЯЗАН быть неудачным{4};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

После того, как элемент PS закончил безопасное обновление программного обеспечения, начатое файлом конфигурации, элемент PS ОБЯЗАН осуществить начальную перезагрузку с помощью правильного изображения программного обеспечения. После того, как элемент PS регистрируется:

- объект docsDevSwAdminStatus ОБЯЗАН быть allowProvisioningUpgrade{2};
- объект docsDevSwFilename МОЖЕТ быть именем файла программного обеспечения, которое в настоящее время действует в устройстве;
- объект docsDevSwServer МОЖЕТ быть адресом сервера TFTP, содержащего программное обеспечение, которое в настоящее время действует в устройстве;
- объект docsDevSwOperStatus ОБЯЗАН быть completeFromProvisioning{2};
- объект docsDevSwCurrentVer ОБЯЗАН быть текущей версией программного обеспечения, которое действует в устройстве.

11.3.7.9 Проверка кода

Для безопасной загрузки программного обеспечения, элемент PS ОБЯЗАН выполнить контрольные проверки, представленные в этом разделе. Если любая контрольная проверка терпит неудачу, или если любая часть файла кода отклоняется из-за недействительного форматирования, то элемент PS ОБЯЗАН сразу же остановить процесс загрузки,

зарегистрировать ошибку, если это применяется, удалить все остатки процесса до такого шага, и продолжать работать с его существующим кодом. Контрольные проверки могут быть сделаны в любом порядке, пока делаются все применимые контрольные проверки, представленные в этом разделе.

1) Элемент PS ОБЯЗАН утвердить информацию подписи производителя путем проверки того, что значение signingTime PKCS#7 есть:
   a) равно или более, чем значение codeAccessStart производителя, которое в настоящее время удерживается элементом PS;
   b) равно или более, чем время начала достоверности сертификата CVC производителя;
   c) меньше или равно времени окончания достоверности сертификата CVC производителя.
2) Элемент PS ОБЯЗАН утвердить сертификат CVC производителя путем проверки того, что:
   a) название организации субъекта CVC является идентичным названию производителя, которое в настоящее время хранится в памяти элемента PS;
   b) время начала достоверности сертификата CVC равно или более, чем значение cvcAccessStart производителя, которое в настоящее время удерживается в элементе PS;
   c) расширение использования продленного ключа находится в сертификате CVC, как определено в 11.3.2.2.2.
3) Элемент PS ОБЯЗАН утвердить подпись сертификата, используя Открытый ключ CA сертификата CVC, удерживаемый элементом PS. В свою очередь, подпись сертификата CA CVC утверждается Открытым ключом CA корня CVC, удерживаемым элементом PS. Проверка подписи подтвердит подлинность источника открытого ключа проверки кода (*CVK, code verification key*) и подтвердит доверие к ключу. Как только в CVK производителя было установлено доверие, остающиеся параметры сертификата, КРОМЕ времени начала достоверности, больше не являются необходимыми, и их СЛЕДУЕТ сбросить.
4) Элемент PS ОБЯЗАН проверить подпись файла кода производителя.
   a) Элемент PS ОБЯЗАН выполнить новые случайные данные SHA-1 по объекту SignedContent. Если значение messageDigest не соответствует новым случайным данным, элемент PS ОБЯЗАН считать, что подпись на файле кода является недействительной;
   b) Если подпись не удостоверяет подлинность, то все компоненты файла кода (включая изображение кода) и любые значения, полученные из процесса проверки, ОБЯЗАНЫ быть отклонены и их СЛЕДУЕТ немедленно сбросить.
5) Если подпись производителя удостоверяет подлинность, и требуется подпись совместно подписывающего агента:
   a) Элемент PS ОБЯЗАН утвердить информацию подписи совместно подписывающей стороны, проверяя, что:
      i) информация подписи совместно подписывающей стороны включена в файл кода;
      ii) значение signingTime PKCS#7 равно или более, чем соответствующее значение codeAccessStart, которое в настоящий момент удерживается в элементе PS;
      iii) значение signingTime PKCS#7 равно или более, чем соответствующее время начала достоверности CVC;

iv) значение signingTime PKCS#7 меньше или равно соответствующему времени окончания достоверности CVC.

b) Элемент PS ОБЯЗАН утвердить сертификат CVC совместно подписавшей стороны путем проверки того, что:

i) название организации субъекта CVC является идентичным названию организации совместно подписавшей стороны, которое в настоящий момент хранится в памяти элемента PS;

ii) время начала достоверности CVC равно или более, чем значение cvcAccessStart, которое в настоящий момент удерживается элементом PS для соответствующего названия организации субъекта;

iii) расширенное использование удлиненного ключа находится в сертификате CVC, как определено в 11.3.2.2.2.

c) Элемент PS ОБЯЗАН утвердить подпись сертификата, используя Открытый ключ CA сертификата CVC, удерживаемый элементом PS. В свою очередь, подпись сертификата CA CVC утверждается Открытым ключом CA корня CVC, удерживаемого элементом PS. Проверка подписи подтвердит подлинность источника открытого ключа проверки кода совместно подписывающей стороны (*CVK, code verification key*) и подтвердит доверие к ключу. Как только доверие было установлено в ключе CVK совместно подписавшей стороны, остающиеся параметры сертификата, КРОМЕ времени начала достоверности, больше не являются необходимыми, и их СЛЕДУЕТ сбросить.

d) Элемент PS ОБЯЗАН проверить подпись кода совместно подписавшей стороны.

e) Элемент PS ОБЯЗАН произвести новые случайные данные SHA-1 на объекте SignedContent. Если значение messageDigest не соответствует новым случайным данным, то элемент PS ОБЯЗАН считать подпись на файле кода недействительной.

f) Если подпись не удостоверяет подлинность, то все компоненты файла кода (включая изображение кода), и любые значения, полученные из процесса проверки, ОБЯЗАНЫ быть отклонены, и их СЛЕДУЕТ немедленно сбросить.

6) Если подпись производителя, и дополнительно, совместно подписывающей стороны, была проверена, то изображению кода можно доверять, а установка может осуществляться дальше. Перед установкой изображения кода все другие компоненты файла кода и любые значения, извлеченные из процесса проверки, кроме значения signingTime PKCS*7 и значений начала достоверности CVC, СЛЕДУЕТ немедленно сбросить.

7) Если установка кода не является успешной, то элемент PS ОБЯЗАН отклонить значения signingTime PKCS#7 и значения начала достоверности CVC, которые он только что получил в файле кода.

8) Когда установка кода является успешной, элемент PS ОБЯЗАН обновить директивы производителя, меняющиеся во времени, с помощью значений из информации подписи производителя и сертификата CVC:

a) Обновить текущее значение codeAccessStart с помощью значения signingTime PKCS#7;

b) Обновить текущее значение cvcAccessStart с помощью значения начала достоверности сертификата CVC.

9) Когда установка кода является успешной, ЕСЛИ файл кода был совместно подписан, элемент PS ОБЯЗАН обновить директивы совместно подписавшей стороны,

изменяющиеся во времени, с помощью значений из информации подписи совместно подписавшей стороны и сертификата CVC:

a) Обновить текущее значение codeAccessStart с помощью значения signingTime PKCS#7;

b) Обновить текущее значение cvcAccessStart с помощью значения начала достоверности сертификата CVC.

11.3.7.10 Коды ошибок

Коды ошибки определяются, чтобы отразить состояния неудач, возможные в течение процесса проверки кода для безопасной загрузки программного обеспечения.

1) Несоответствующие директивы файлов кодов:

   a) Название организации субъекта CVC для производителя не соответствует названию производителя элемента PS.

   b) Название организации субъекта CVC для совместно подписавшегося агента кода не соответствует текущему совместно подписавшему агенту кода элемента PS.

   c) Значение signingTime PKCS#7 производителя меньше, чем значение codeAccessStart, которое в настоящий момент удерживается в элементе PS.

   d) Значение времени начала достоверности PKCS#7 производителя меньше, чем значение cvcAccessStart, которое в настоящий момент удерживается в элементе PS.

   e) Время начала достоверности сертификата CVC производителя меньше, чем значение cvcAccessStart, которое в настоящий момент удерживается в элементе PS.

   f) Значение signingTime PKCS#7 производителя меньше, чем время начала достоверности сертификата CVC.

   g) Пропавшее или несоответственное расширение использования удлиненного ключа в сертификате CVC производителя.

   h) Значение signingTime PKCS#7 совместно подписавшей стороны меньше, чем значение codeAccessStart, которое в настоящий момент удерживается в элементе PS.

   i) Значение времени начала достоверности PKCS#7 совместно подписавшей стороны меньше, чем значение cvcAccessStart, которое в настоящий момент удерживается в элементе PS.

   j) Значение времени начала достоверности CVC совместно подписавшей стороны меньше, чем значение cvcAccessStart, которое в настоящий момент удерживается в элементе PS.

   k) Значение signingTime PKCS#7 совместно подписавшей стороны меньше, чем время начала достоверности сертификата CVC.

   l) Пропавшее или несоответственное расширение использования удлиненного ключа в сертификате CVC совместно подписавшей стороны.

2) Неудача подтверждения сертификата CVC производителя файла кода.

3) Неудача подтверждения подписи CVS производителя файла кода.

4) Неудача подтверждения сертификата CVC совместно подписавшей стороны для файла кода.

5) Неудача подтверждения подписи CVS совместно подписавшей стороны для файла кода.

6) Несоответствующий формат CVC файла конфигурации (например, пропавший или несоответствующий атрибут использования ключа).

7) Неудача подтверждения сертификата CVC файла конфигурации.

8) Несоответствующий формат сертификата CVC протокола SNMP:

   a) Название организации субъекта CVC для производителя не соответствует названию производителя устройства.

   b) Название организации субъекта CVC для совместно подписавшего агента кода не соответствует текущему совместно подписавшему агенту кода элемента PS.

   c) время начала достоверности сертификата CVC меньше или равно соответствующему значению cvcAccessStart субъекта, которое в настоящий момент удерживается в элементе PS.

   d) Пропавший или несоответствующий атрибут использования ключа.

9) Неудача подтверждения сертификата CVC протокола SNMP.

11.3.7.11 Понижение версии программного обеспечения

Понижение версии программного обеспечения определяет процесс удаления обновленной версии загрузки изображения программного обеспечения, тем самым, возвращая устройство к точному предыдущему состоянию.

Когда элемент PS получает файл кода со временем подписания, которое позднее, чем время подписания, которое он имеет в своей памяти, устройство будет обновлять свою внутреннюю память с помощью полученного значения.

Поскольку элемент PS не будет принимать файлы кода с более ранним временем подписания, чем это внутренне хранимое значение, чтобы обновлять устройство с помощью нового файла кода, не отрицая доступа к прошлым файлам кода, подписывающая сторона может не пожелать обновлять время подписания. В этой манере, многократные файлы кода с тем же самым временем подписания кода позволяют оператору свободно понижать версию изображения кода устройства до прошлой версии (то есть, пока сертификат CVC не был обновлен). Это имеет множество преимуществ для оператора, но эти преимущества следует взвесить в сравнении с возможностями атаки воспроизведения файла кода.

Другой подход состоял бы в том, чтобы подписать предыдущий файл кода со временем подписания, которое является равным или больше, чем время подписания последнего обновления.

11.3.8 Физическая безопасность

Это приложение требует от услуги PS поддержания, в его памяти, ключей и других переменных величин шифрования, связанных с безопасностью сети. Все элементы и устройства ОБЯЗАНЫ сдерживать несанкционированный физический доступ к этому шифровальному материалу.

Уровень физической защиты ключевого материала, который требуется для сетевых элементов и устройств, указывается в понятиях уровней безопасности, определенных в документе FIPS PUBS 140-2, "Требования безопасности для шифровальных модулей", стандарт [FIPS 140-2]. В частности, элементы ОБЯЗАНЫ удовлетворять требования Уровня 1 безопасности FIPS PUBS 140-2.

Уровень 1 безопасности FIPS PUBS 140-2 требует минимальной физической защиты через использование разграничения ступеней производства и рекомендованных методов программного обеспечения.

12 Процессы административного управления

12.1 Введение/Обзор

Этот раздел предоставляет примеры процессов, связанных с использованием инструментов, описанных в разделе 6 ("Инструменты административного управления"), и дополнительных процессов, которые облегчают другие требуемые функции административного управления, определенные в этой Рекомендации. Доступ базы данных PS и другие действия PS Портала кабельного административного управления (*CMP, Cable Management Portal*) описаны в разделе 6. Типичные правила доступа MIB предоставляются в 6.3.6.

Процессы, относящиеся к административному управлению, и другие описательные процессы предоставляются для следующих сценариев:

- Процессы инструментов административного управления;
- Операция портала CTP:
  - Дистанционное испытание скорости соединения;
  - Дистанционное испытание по переброске информации.
- Операция PS;
- Доступ к базе данных PS;
- Реконфигурация:
  - Загрузка программного обеспечения PS;
  - Загрузка файла конфигурации PS.
- Доступ MIB;
- Конфигурация VACM;
- Конфигурация обмена сообщениями о событии административного управления:
  - Операция уведомления о событии CMP;
  - Операция дросселирования и ограничения событий CMP.

12.1.1 Цели

Этот раздел главным образом составлен из информативного текста, предназначенного помочь пониманию читателя, и не содержит требования. Примеры описывают, как используются инструменты административного управления для достижения типичных функций административного управления. Также представлены диаграммы последовательности дополнительных процессов, связанных с управлением, (т.е. те, что не определяются в разделе 6), включая процессы административного управления или шаги процессов, связанные с использованием требуемых инструментов административного управления. Все показанные процессы вовлекают взаимодействие элемента PS с системами головных узлов.

12.2 Инструментальные процессы административного управления

Инструментальными процессами административного управления являются те, что связаны с требуемыми инструментами административного управления, определенными в разделе 6.

12.2.1 Операция портала CTP

Испытательный портал CableHome (*CTP, CableHome Testing Portal*) обеспечивает возможности "Дистанционное испытание скорости соединения" и "Дистанционное испытание по переброске информации", соответственно описанные в 6.4.3.1 и 6.4.3.2.

12.2.1.1 Дистанционное испытание скорости соединения

Дистанционное испытание скорости соединения может быть полезным в утверждении уровней показателей качества, указывая возможные ошибки конфигурации и определяя другие характеристики, ориентированные на показатели качества (см. Рисунок 28).

- Система сетевого административного управления (*NMS, Network Management System*) запускает испытание путем установления в начальное положение параметров испытаний и устанавливая флаг "Начать испытание" [*Begin Test*], через запрос SET [*установить*] протокола SNMP.
- Агент протокола SNMP портала CMP обновляет базу данных услуги PS с помощью параметров испытаний и сообщает порталу CTP начать испытание.
- Портал CTP консультируется с базой данных PS относительно параметров испытаний.
- Портал CTP выпускает пачку пакетов UDP к порту 7 указанного Устройства IP сети LAN. Порт 7 резервируется для услуги эха.
- Целевое Устройство IP сети LAN просто возвращает полезную нагрузку пакета UDP обратно к порталу CTP.
- Как только все из пакетов были получены, или период выдержки времени испытания истек, портал CTP обновляет базу данных PS с помощью результатов испытания и устанавливает флаг "Испытание завершено" [*Test Complete*].
- Система NMS проверяет, что команда завершена, путем проверки Status=complete [*Статус = завершен*].
- Система NMS запрашивает результаты испытания через запрос GET [*получить*] протокола SNMP.
- Агент протокола SNMP портала CMP консультируется с базой данных PS относительно результатов испытаний и сообщает их в отклике GET протокола SNMP. Если испытание не было завершено, то данные испытаний будут указывать, что испытание все еще продолжается. Система NMS должна повторять запрос GET протокола SNMP до тех пор, пока результаты испытаний не покажут, что испытание было завершено.

12.2.1.2 Дистанционное испытание по переброске информации

Дистанционное испытание по переброске информации может быть полезным в подтверждении состояния связности, уровней показателей качества и в определении возможных ошибок конфигурации (см. Рисунок 29).

- Система сетевого административного управления (*NMS, Network Management System*) запускает испытание путем установления в начальное положение параметров испытаний и устанавливая флаг "Начать испытание" [*Begin Test*] через запрос SET протокола SNMP.
- Агент протокола SNMP портала CMP обновляет базу данных услуги PS с помощью параметров испытаний и сообщает порталу CTP начать испытание.
- Портал CTP консультируется с базой данных PS относительно параметров испытаний.
- Портал CTP выпускает пакет запроса "Эхо" ICMP к указанному Устройству IP сети LAN.
- Целевое Устройство IP сети LAN откликается с помощью отклика "Эхо" ICMP.
- Портал CTP обновляет базу данных PS с помощью результатов испытания и устанавливает флаг "Испытание завершено"[*Test Complete*].
- Система NMS проверяет, что команда завершена, путем проверки Status=complete [*Статус = завершен*].

- Система NMS запрашивает результаты испытания через запрос GET протокола SNMP.
- Агент протокола SNMP портала CMP консультируется с базой данных PS относительно результатов испытаний и сообщает их в отклике GET протокола SNMP. Если испытание не было завершено, то данные испытаний будут указывать, что испытание все еще продолжается. Система NMS должна повторять запрос GET протокола SNMP до тех пор, пока результаты испытаний не покажут, что испытание было завершено.

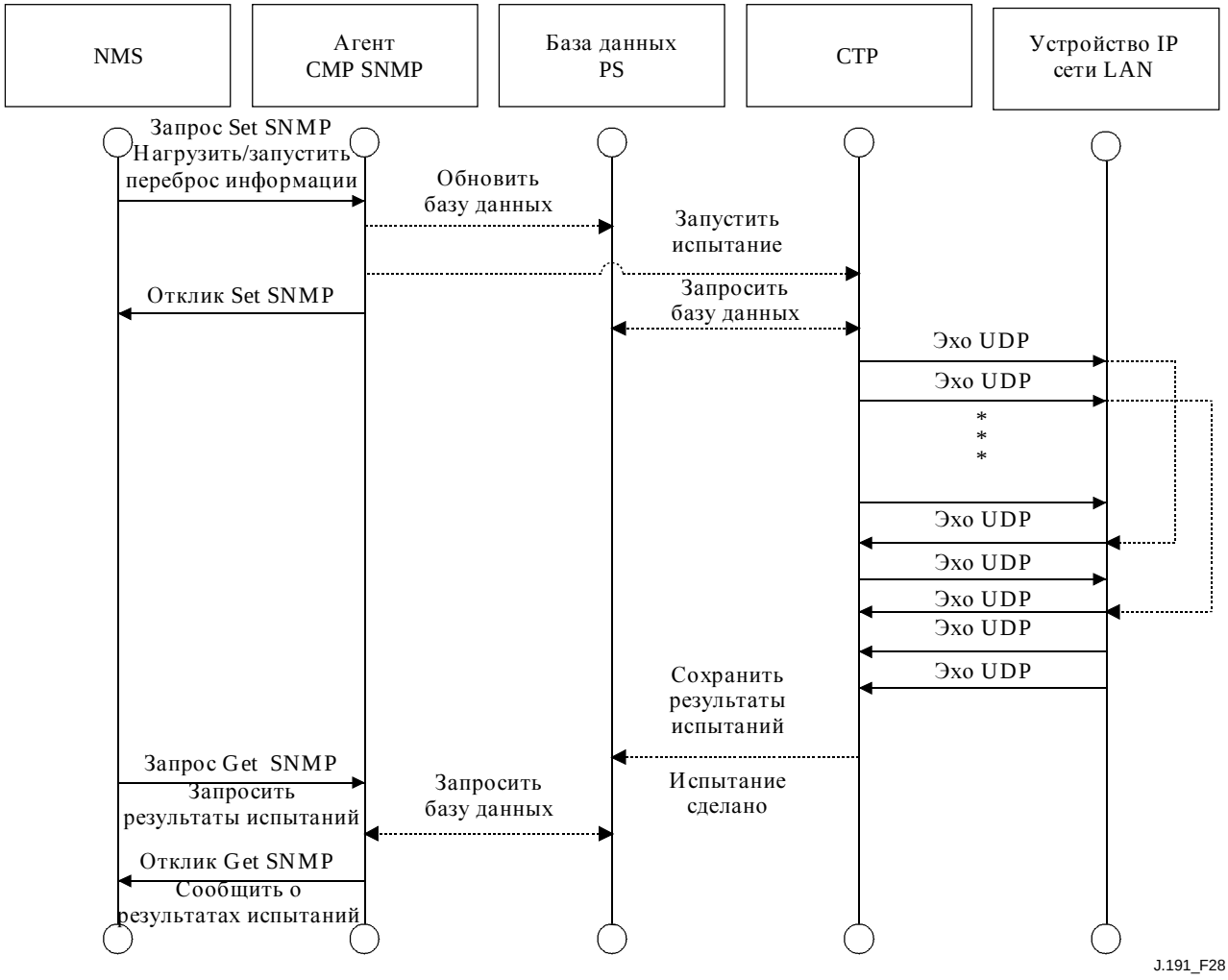


Рисунок 28/J.191 – Диаграмма последовательности испытания скорости соединения

12.3 Операция услуги PS

Портал кабельного административного управления (*CMP, Cable Management Portal*) предоставляет доступ к базе данных PS через интерфейс WAN-Man услуги PS, как описано в разделе 6. Последовательность сообщений для типичной операции доступа к базе данных PS из интерфейса WAN-Man услуги PS описывается ниже.

12.3.1 Доступ к базе данных PS

К конфигурации и параметрам управления, хранимым в базе данных PS, получают доступ с помощью системы NMS через базы MIB протокола SNMP. Параметры ищутся и выбираются, используя сообщения Get request [*Запрос получить*], Get Next Request [*Получить следующий запрос*], Get Bulk [*Получить оптом*] протокола SNMP, выпускаемого системой NMS с помощью адреса WAN-Man услуги PS в качестве адрес пункта назначения. Могут быть

изменены параметры и выполнены действия (такие, как испытания Скорости соединения и Удаленного переброса информации) с помощью системы NMS, выпуская сообщения Set request [*установить запрос*] протокола SNMP с соответствующими параметрами к адресу WAN-Man услуги PS.

Рисунок 30 описывает последовательности сообщений административного управления для типичного доступа к базе данных PS из интерфейса WAN-Man услуги PS. Последовательность сообщений предполагает, что установлено безопасное звено SNMPv3.

- Система NMS читает данные из базы данных PS, используя запрос Get протокола SNMP. Запрос перечисляет конкретные объекты, которые NMS хочет получить из базы данных.
- Агент протокола CMP портала CMP консультируется с базой данных PS для конкретных параметров.

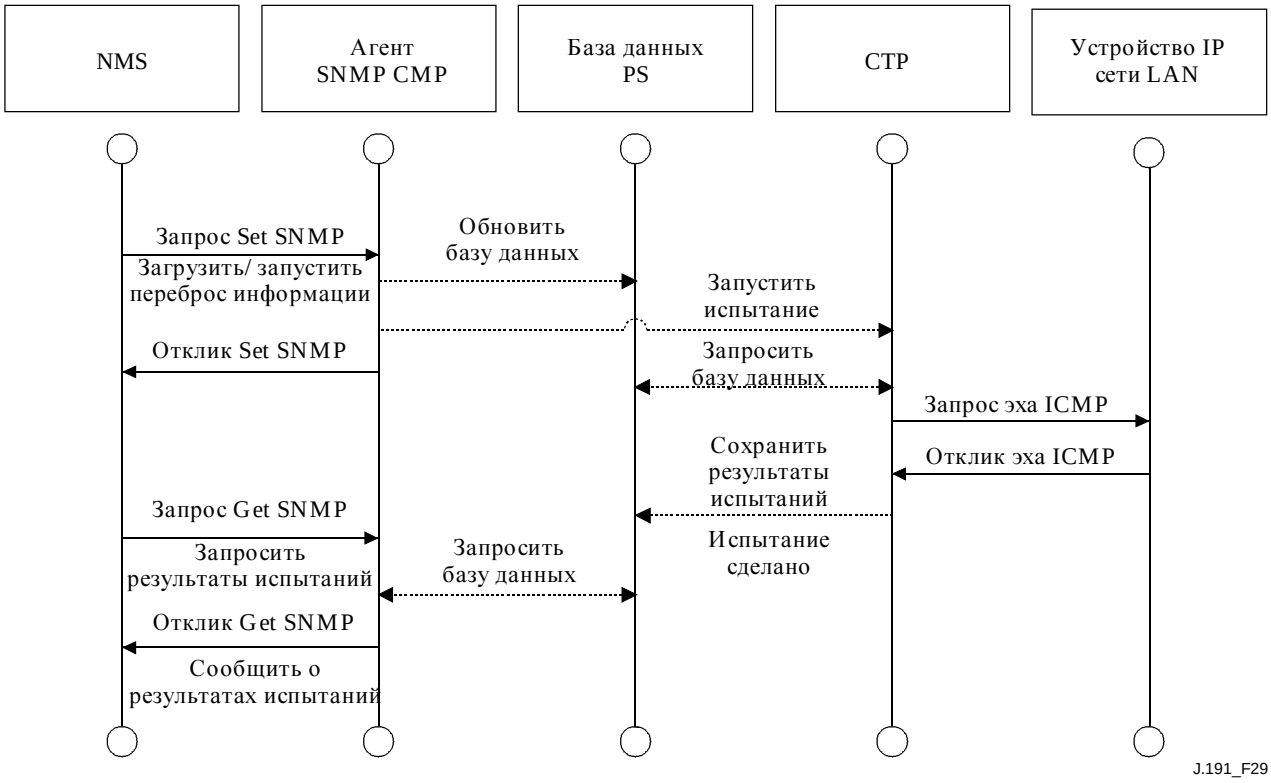


Рисунок 29/J.191 – Диаграмма последовательности дистанционного испытания по переброске информации

Er WAN/ **annot be created from e** PS **les.**
Головной узел Агент SNMP (Внутренняя DB)

Рисунок 30/J.191 – Диаграмма последовательности доступа к базе данных PS из интерфейса WAN-Man услуги PS

- Протокол SNMP пор Запрос Get SNMP цает данные системе NMS с помощью отклика Get протокола SNMP. Запросить Базу данных

12.3.2 Реконфигурация

Отклик Get SNMP

12.3.2.1 Загрузка программного ооеспечения PS

Следующий пример на Рисунке 31 иллюстрирует процесс загрузки программного обеспечения/фирменного обеспечения для услуги PS в режиме обеспечения SNMP. Этот процесс запускается системой NMS. Услуге PS говорят, где получить новый файл кода программного обеспечения. Как только загрузка файла кода будет завершена, услуга PS испытает изображение на любое искажение, которое, возможно, произошло в течение

загрузки. Выполняется удостоверение подлинности, чтобы проверить, что файлу кода можно доверять. После этого шага выполняется начальная перезагрузка системы.

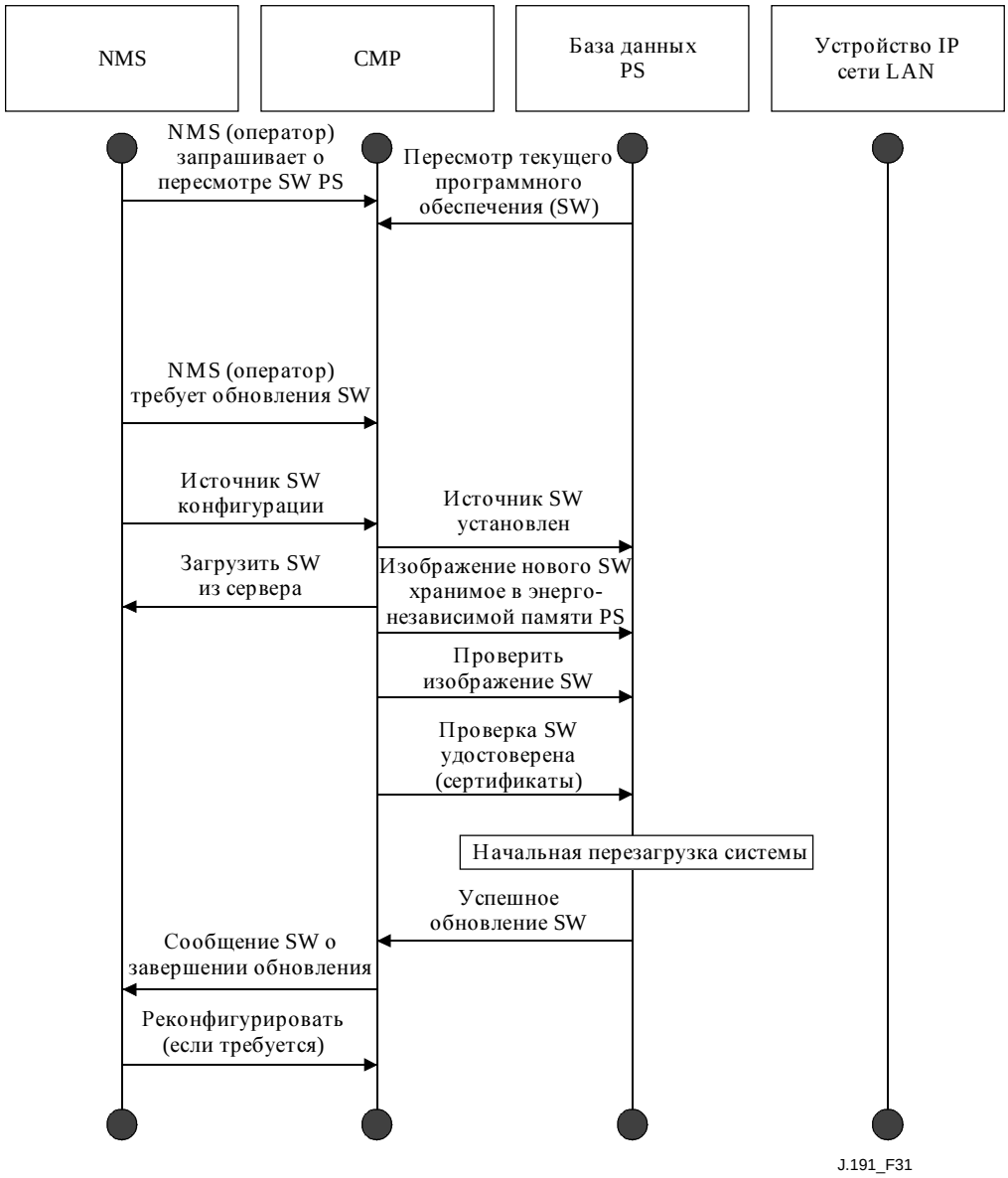


Рисунок 31/J.191 – Диаграмма последовательности загрузки программного обеспечения услуги PS

После начальной перезагрузки услуга PS возобновляет действие на новом изображении программного обеспечения. Услуга PS, возможно, будет нуждаться в реконфигурации после

обновления программного обеспечения, и интерфейсы сети WAN, возможно, снова будут нуждаться в обеспечении (не показано). Если услуга PS не соглашается с новым изображением программного обеспечения, она возвратится назад к предшествующей (резервной) версии программного обеспечения и сообщит системе NMS о том, что случилось.

12.3.2.2 Загрузка файла конфигурации PS

Следующий пример на Рисунке 32 иллюстрирует реконфигурацию услуги PS в режиме обеспечения SNMP, через загрузку файла конфигурации. Этот процесс запускается системой NMS. Файл конфигурации дается услуге PS путем записи сервера файла и имени файла в услуге PS, и запуская услугу PS для загрузки файла. Как только файл конфигурации будет загружен, команды в пределах него истолковываются. Если любая из команд не понята или не

является соответствующей, они опускаются, и порождается событие. Когда услуга PS закончила обработку файла конфигурации, она запишет число кортежей TLV, обработанных и опущенных в соответствующих объектах MIB.

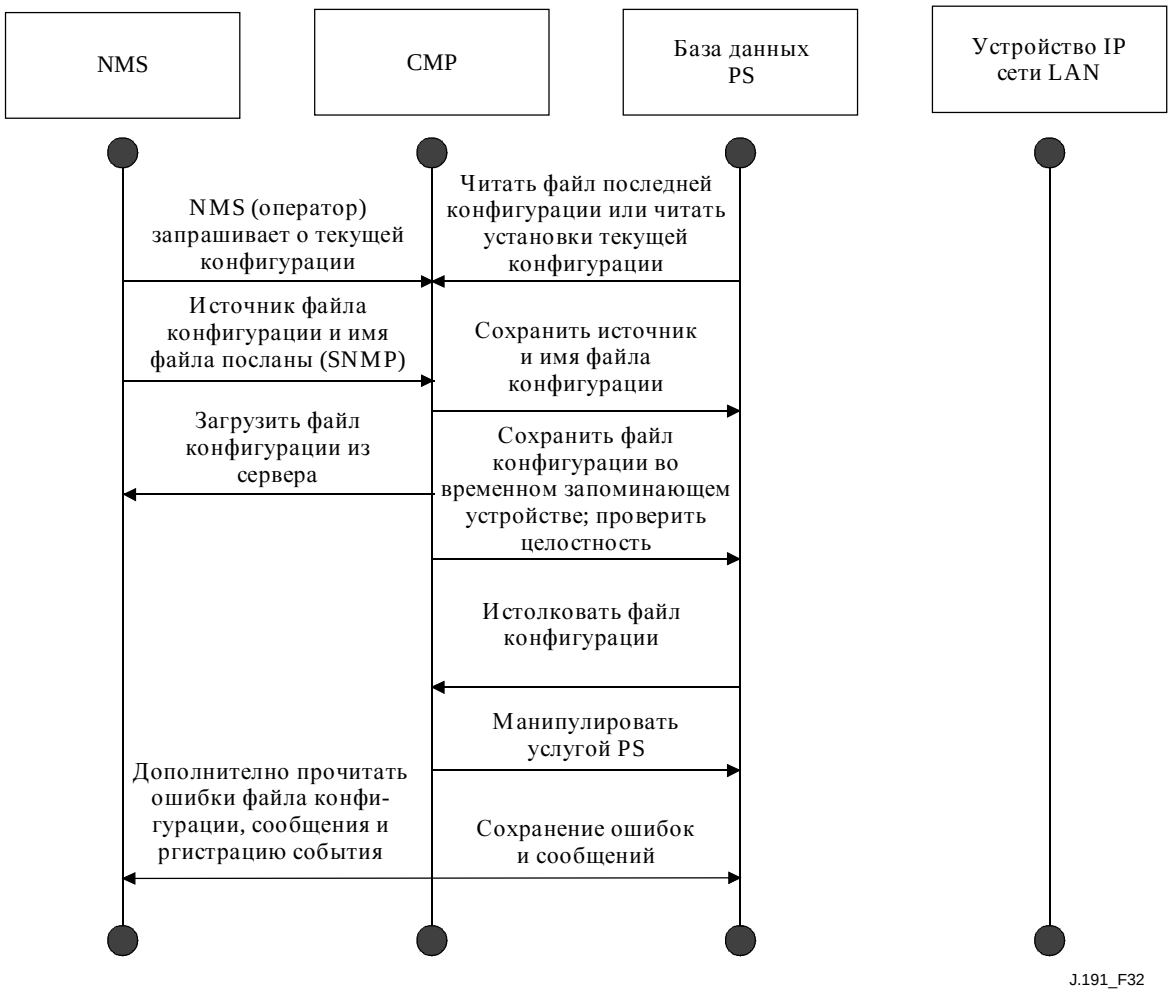


Рисунок 32/J.191 – Диаграмма последовательности повторной конфигурации услуги PS (Загрузка файла конфигурации)

12.4 Доступ MIB

12.4.1 Конфигурация VACM

Кабельный оператор обладает управлением области административного управления. Пример конфигурации параметров VACM показан на Рисунке 33.

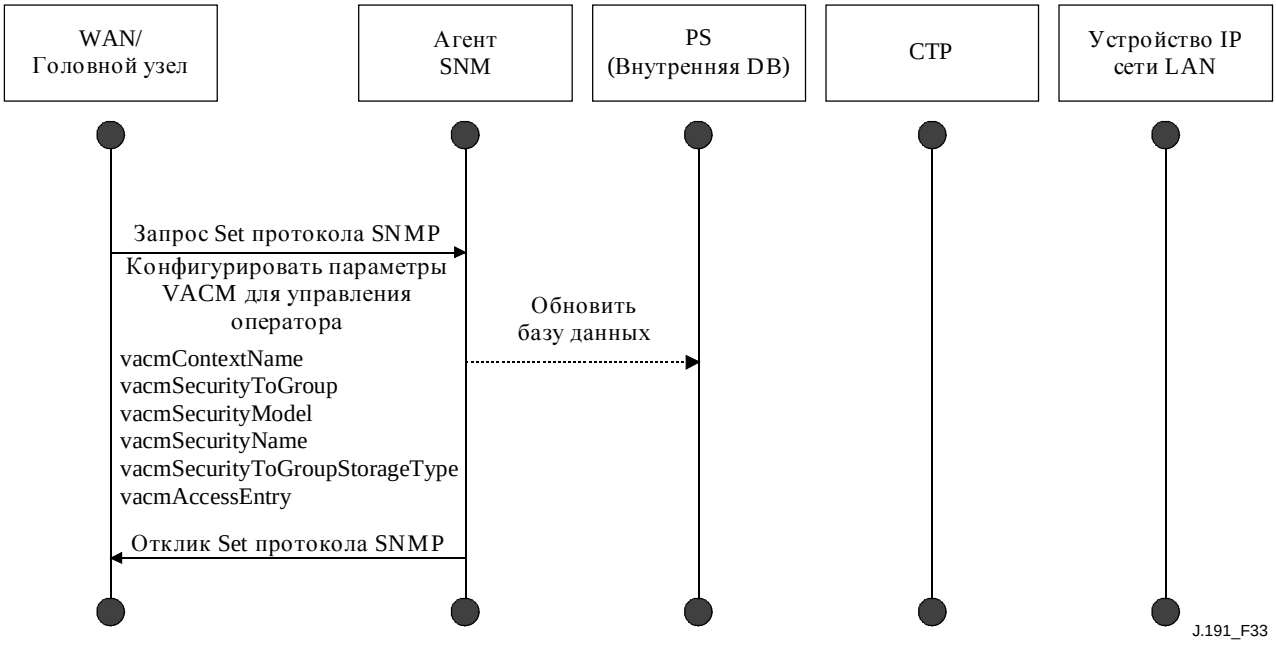


Рисунок 33/J.191 – Последовательность конфигурации PS (параметры VACM)

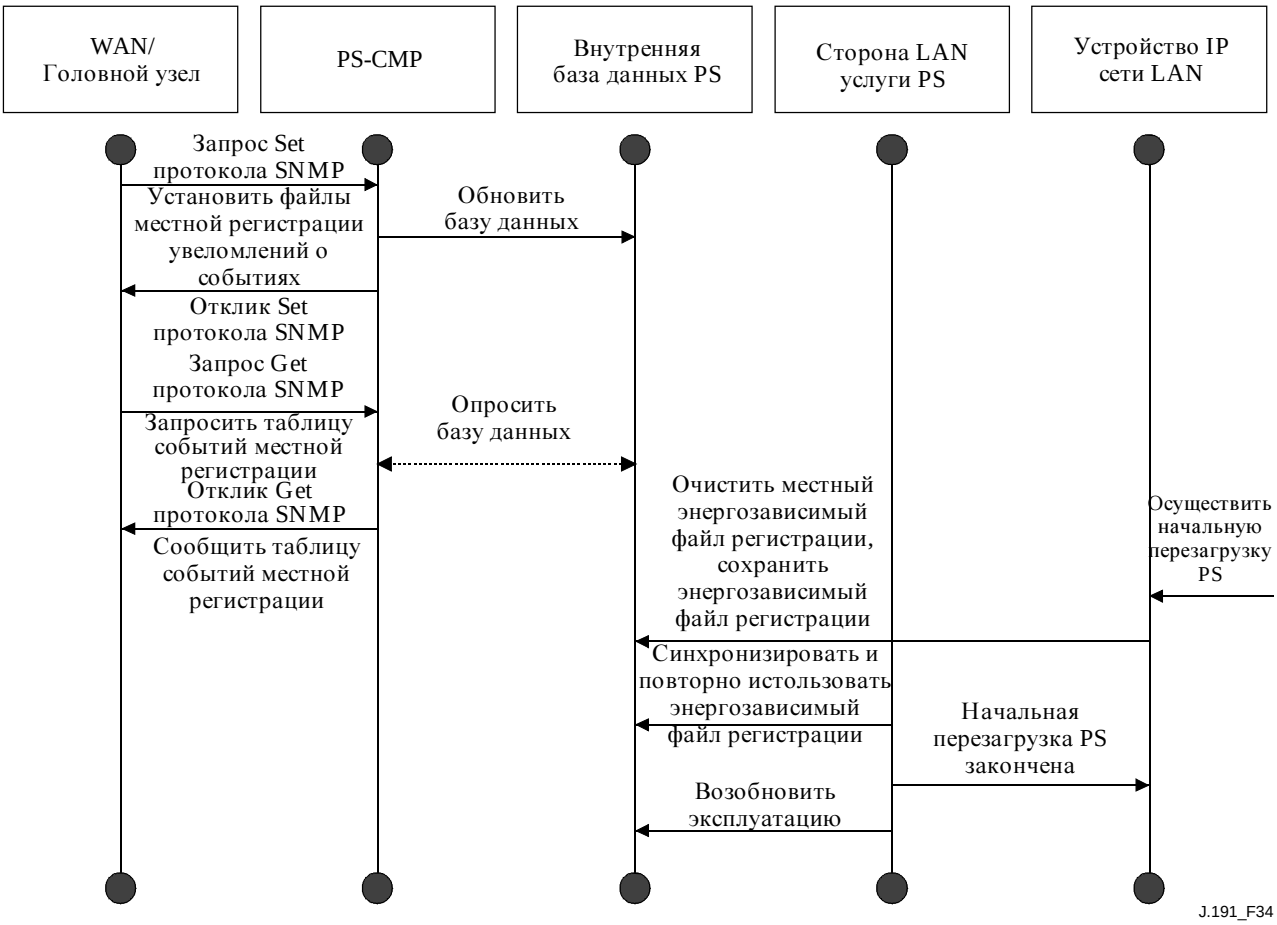


Рисунок 34/J.191 – Последовательность конфигурации PS (управление событием)

12.4.2 Конфигурация обмена сообщениями о событии административного управления

12.4.2.1 Операция уведомления о событии CMP

О событиях сообщают через регистрацию местного события, сообщения TRAP [*системное прерывание*, *захват*] протокола SNMP, INFORM [*информировать*] протокола SNMP, и SYSLOG. Механизм уведомления о событиях может быть установлен или изменен системой NMS, путем использования сообщения запроса Set протокола SNMP к адресу WAN-Man услуги PS.

Следующие примеры на Рисунке 34 иллюстрируют конфигурирование базы данных PS, чтобы хранить события в файлах местной регистрации. События местной регистрации имеются двух типов: местные энергонезависимые и местные энергозависимые. Система NMS будет читать содержимое местного журнала и записывать такое содержимое для системы регистрации событий головных узлов. Начальный перезапуск услуги PS вызывает очистку из базы данных PS только энергозависимых событий. Энергонезависимые события сохраняются при начальных перезагрузках.

Следующий сценарий (Рисунок 35) иллюстрирует загрузку файла конфигурации для услуги PS в режиме обеспечения SNMP. Этот процесс запускается через запрос Set протокола SNMP. Услуга PS должна проверить этот файл перед принятием его. В примере существует ошибка TLV, и о ней сообщают. Так как уведомление события установлено в режим TRAP [*системное прерывание*, *захват*] протокола SNMP, адрес сервера TRAP ищется и выбирается из базы данных PS, а такому серверу TRAP посылают событие.

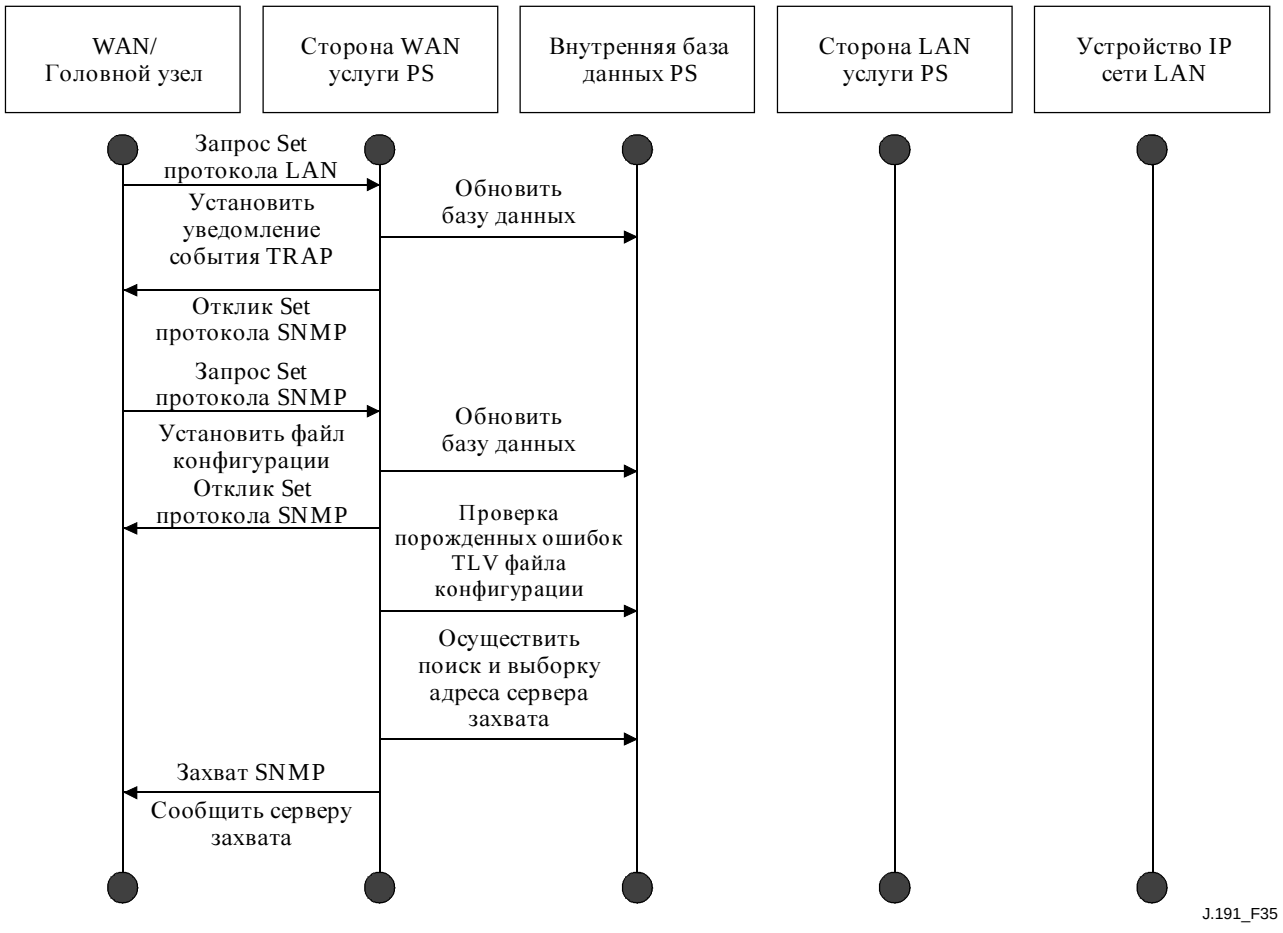


Рисунок 35/J.191 – Последовательность загрузки файла конфигурации PS (с недействительными значениями TLV)

Следующий пример (Рисунок 36) иллюстрирует процесс Устройства IP сети LAN, пытающегося получить адрес IP от местного сервера DHCP (CDS). Функция CDS проверяет базу данных PS для доступного адреса IP. В этом случае сервер CDS обнаруживают, что никакой IP адрес не доступен из объединения адресов, и он порождает событие к SYSLOG.

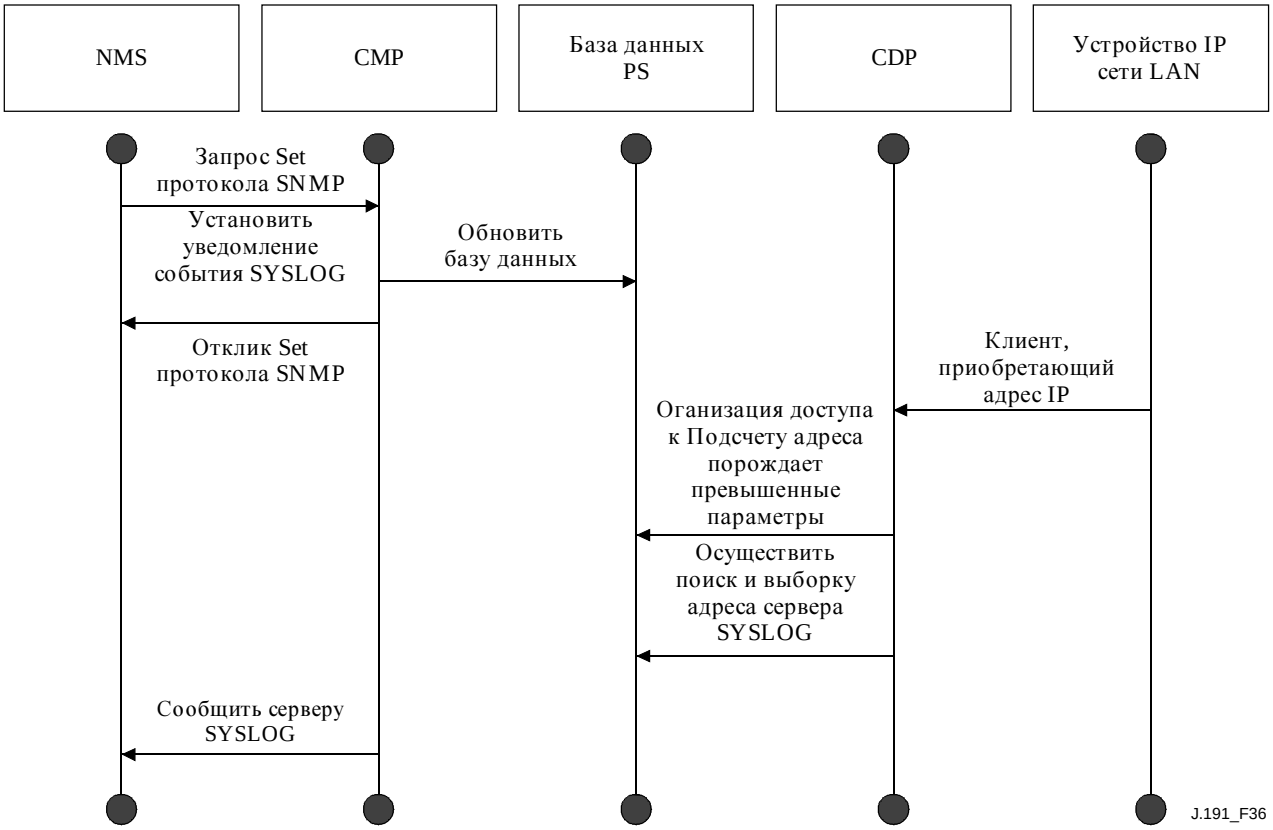


Рисунок 36/J.191 – Последовательность приобретения адреса устройства IP сети LAN (запрос превышает обеспеченный подсчет)

12.4.2.2 Пример дросселирования события CMP и ограничение действия

Механизм дросселирования события обеспечивается через функциональные возможности CMP услуги PS. Дросселирование и ограничение события являются очень гибкими и могут включить случаи, в которых системе NMS сообщают обо всех событиях, и случаи, в которых ни о каких событиях не сообщают. Дается ссылка на Рисунок 37 для описания механизма дросселирования и ограничения события CMP.

Пример, показанный на Рисунке 37, иллюстрирует конфигурирование базы данных PS, чтобы возвращать события через метод INFORM [*информировать*] протокола SNMP. Первоначально, несколько сообщений INFORM записываются в файл местной регистрации и доставляются системе NMS. Механизм дросселирования событий устанавливает предел числа событий, которые можно послать системе NMS в пределах заданного кадра времени. Когда такой предел достигнут, услуга PS прекратит посылать сообщения INFORM системе NMS. Чтобы повторно запустить уведомление о событии, системе NMS следует повторно обеспечить информирование о событии.

13 Процессы обеспечения

Этот раздел описывает участвующие процессы, когда используются Инструменты обеспечения, описанные в разделе 7, для первоначального обеспечения Устройства IP сети LAN и элемента PS. Обеспечение имеет три следующие задачи:

1) Приобретение сетевого адреса;

2) Приобретение информации сервера;

3) Безопасная загрузка и обработка файла конфигурации PS.

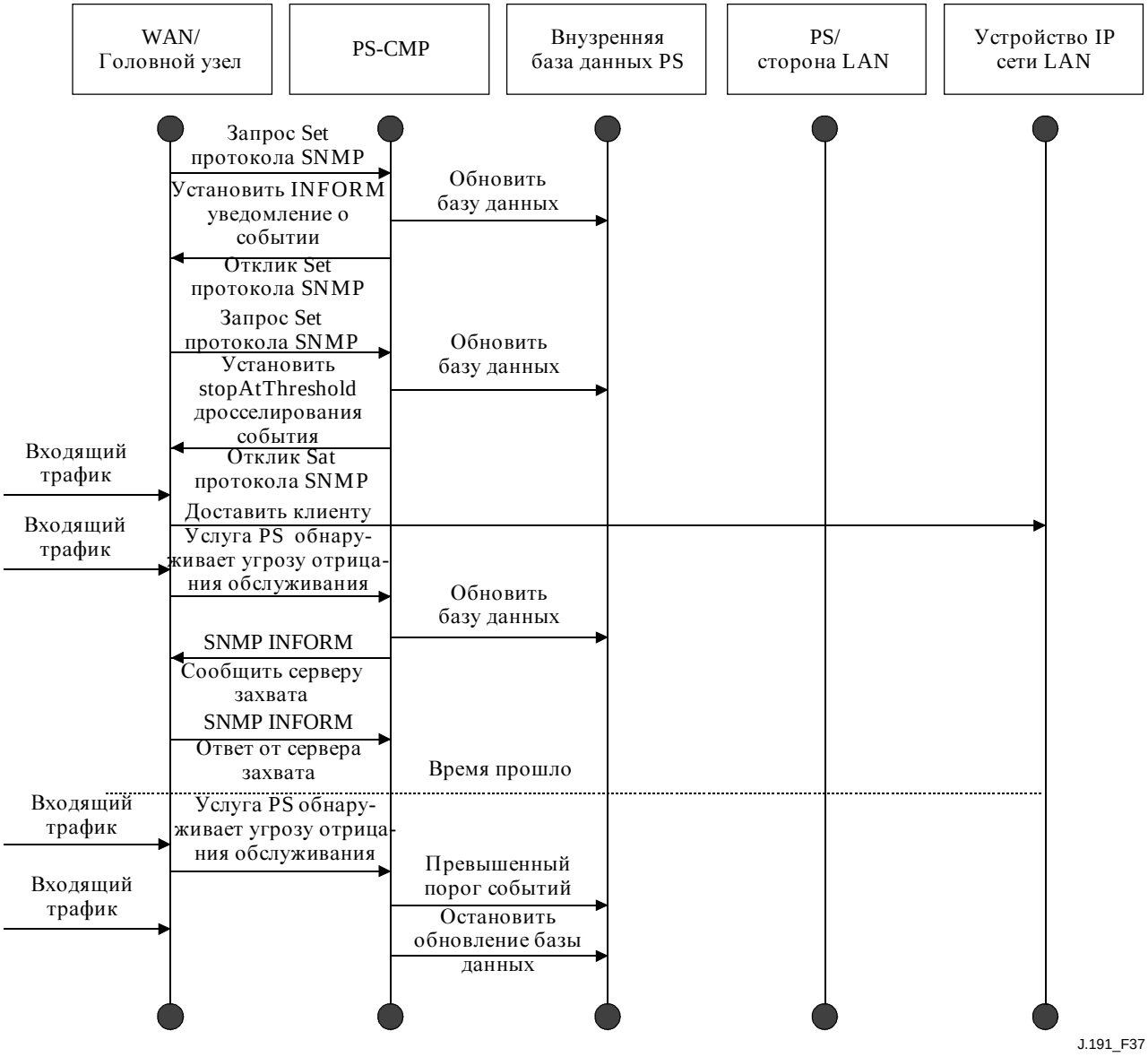


Рисунок 37/J.191 – Дросселирование события и ограничение действия CMP

Процессы обеспечения описываются в этом разделе для каждого из следующих уместных случаев:

- WAN-Man услуги PS – Обеспечение функциональных возможностей административного управления на основе сети WAN услуги PS;
- Данные сети WAN услуги PS – Обеспечение адресов IP WAN-Data услуги PS, подлежащих использованию для создания отображений CAT к Устройствам IP сети LAN в адресной области LAN-Trans;
- Устройство IP сети LAN в области LAN-Trans – Обеспечение Устройства IP сети LAN с транслированным адресом IP;
- Устройство IP сети LAN в области LAN-Pass – Обеспечение Устройства IP сети LAN с адресом IP, который пропускают через сеть WAN.

Обеспечение функциональных возможностей кабельного модема является отдельным аспектом и отличающимся от обеспечения услуги PS, и выходит за рамки этой Рекомендации. Читателя можно отослать к спецификации DOCSIS для описаний обеспечения кабельного модема.

Функциональные элементы, с которыми взаимодействует элемент PS в течение процессов обеспечения, перечисленных выше, определяются на Рисунке 38. Функциональный элемент Центра распределения ключей (*KDC, Key Distribution Center*) показан с помощью пунктирного контура, поскольку он используется в режиме обеспечения SNMP, а не в режиме обеспечения DHCP. Другие функциональные элементы используются в обоих режимах обеспечения.

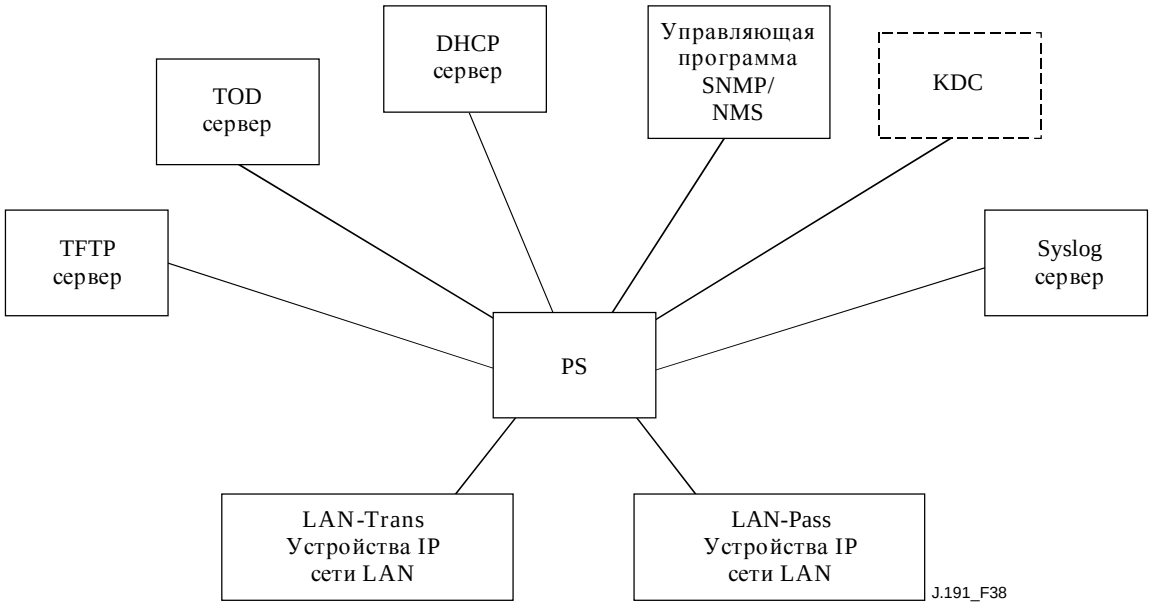


Рисунок 38/J.191 – Функциональные элементы обеспечения

Сервер Тривиального протокола переноса файлов (*TFTP, Trivial File Transfer Protocol*) обеспечивает доступ к файлу конфигурации PS для услуги PS и следует правилам, описанным в документе [RFC 1350]. Сервер Времени дня (*TOD, Time of Day*) обеспечивает средства для услуги PS, чтобы приобрести текущее время в формате UTC, как описано в документе [RFC 868]. Сервер Динамического протокола конфигурации ведущего узла (*DHCP, Dynamic Host Configuration Protocol*) обеспечивает услугу PS частными и/или глобальными адресами IP, следуя документу [RFC 2131], а также обеспечивая другую информацию через варианты выбора DHCP в соответствии с документом [RFC 2132]. Управляющая программа Простого протокола административного управления сетью (*SNMP, Simple Network Management Protocol*) из Системы сетевого административного управления (*NMS, Network Management System*) соответствует документу [RFC 1157] и, возможно, более современным версиям протокола SNMP, например, [RFC 2571], [RFC 2572], [RFC 2574] и [RFC 2575]. Центр распределения ключей (*KDC, Key Distribution Center*) управляет проверкой полномочий и ключами шифрования для того, чтобы установить доверие между сетевыми элементами, и осуществляет правила, определенные в документе [RFC 1949]. Сервер регистрация системы (SYSLOG) обрабатывает сообщения о событиях, порожденные услугой PS и Устройствами IP сети LAN в доме. Услуга PS осуществляет клиентов для этих серверов головного узла, и использует эти функции клиента в течение процессов обеспечения, описанных в этом разделе, чтобы выполнить задачи, перечисленные в начале этого раздела.

13.1 Режимы обеспечения

Разделы 5.7 и 7.1.1 вводят два режима обеспечения, поддерживаемые элементом Услуги портала: режим обеспечения DHCP и режим обеспечения SNMP. В этом разделе каждый из этих двух режимов представлен более подробно. Рисунок 39 иллюстрирует возможный поток события для двух режимов обеспечения. Ключевым пунктом Рисунка 39 является переключатель, используемый услугой PS для определения режима обеспечения, в котором она должна работать.

Услуга PS работает в режиме обеспечения DHCP (Режим DHCP), если сервер DHCP в кабельной сети обеспечивает действительный адрес IP для сервера TFTP в поле 'siaddr' сообщения DHCP, обеспечивает действительное имя файла для Файла конфигурации услуги PS в поле 'file' [*файл*] протокола DHCP, и НЕ обеспечивает под-вариант 51 из варианта выбора 177 протокола DHCP к клиенту CDC услуги PS, в течение фазы DHCPOFFER процесса установления в начальное состояние. Режим обеспечения DHCP предназначен для того, чтобы позволить услуге PS действовать на инфраструктуре, которая не включает в себя усовершенствованные особенности модели IPCablecom.

Режим обеспечения SNMP в услуге PS запускается тогда, когда сервер DHCP в кабельной сети не обеспечивает значения для 'siaddr' и "file', и когда сервер DHCP кабельной сети ДЕЙСТВИТЕЛЬНО посылает под-вариант 51 из варианта выбора 177 протокола DHCP. Режим обеспечения SNMP предназначен для того, чтобы позволить услуге PS использовать в своих интересах усовершенствованные особенности инфраструктуры IPCablecom.

13.2 Процесс для обеспечения услуги PS для административного управления: Режим обеспечения DCHP

Услуга PS запрашивает от системы обеспечения головного узла адрес IP, подлежащий использованию для обмена сообщениями административного управления между системой NMS и услугой PS. Услуга PS производит структурный анализ сообщения DHCP, возвращенного в сообщении OFFER [*предложение*] протокола DHCP и делает определение относительно режима обеспечения, в котором она должна работать (см. 7.2.3.3). Раздел 7.2.2.2.1 описывает два адресных режима сети WAN, поддерживаемых услугой PS для приобретения адресов IP от сервера DHCP в кабельной сети.

Если услуга PS делает определение, что она должна действовать в режиме обеспечения DHCP, она будет использовать информацию файла конфигурации услуги PS, которая прошла в сообщении DHCP, в качестве спускового механизм, чтобы загрузить Файл конфигурации услуги PS, как описано в 7.2. Загрузка Файла конфигурации услуги PS является требованием для услуги PS, действующей в режиме обеспечения DHCP, но является дополнительной для услуги PS, действующей в режиме обеспечения SNMP. После начальной загрузки Файла конфигурации услуги PS, запущенной полями сообщений DHCP, система NMS может инициировать конфигурацию последующего обеспечения, выпуская запрос Set [*установить*] протокола SNMP к объектам базы MIB cabhPsDevProvConfigHash и cabhPsDevProvConfigFile, как описано в 7.3.

В режиме обеспечения DHCP услуга PS (CMP) устанавливается по умолчанию в использование режима NmAccess для обмена сообщениями административного управления с системой NMS, но система NMS может дополнительно формировать портал CMP для режима Coexistence [*сосуществование*]. Эти режимы административного управления обменом сообщениями описаны в 6.3.3.

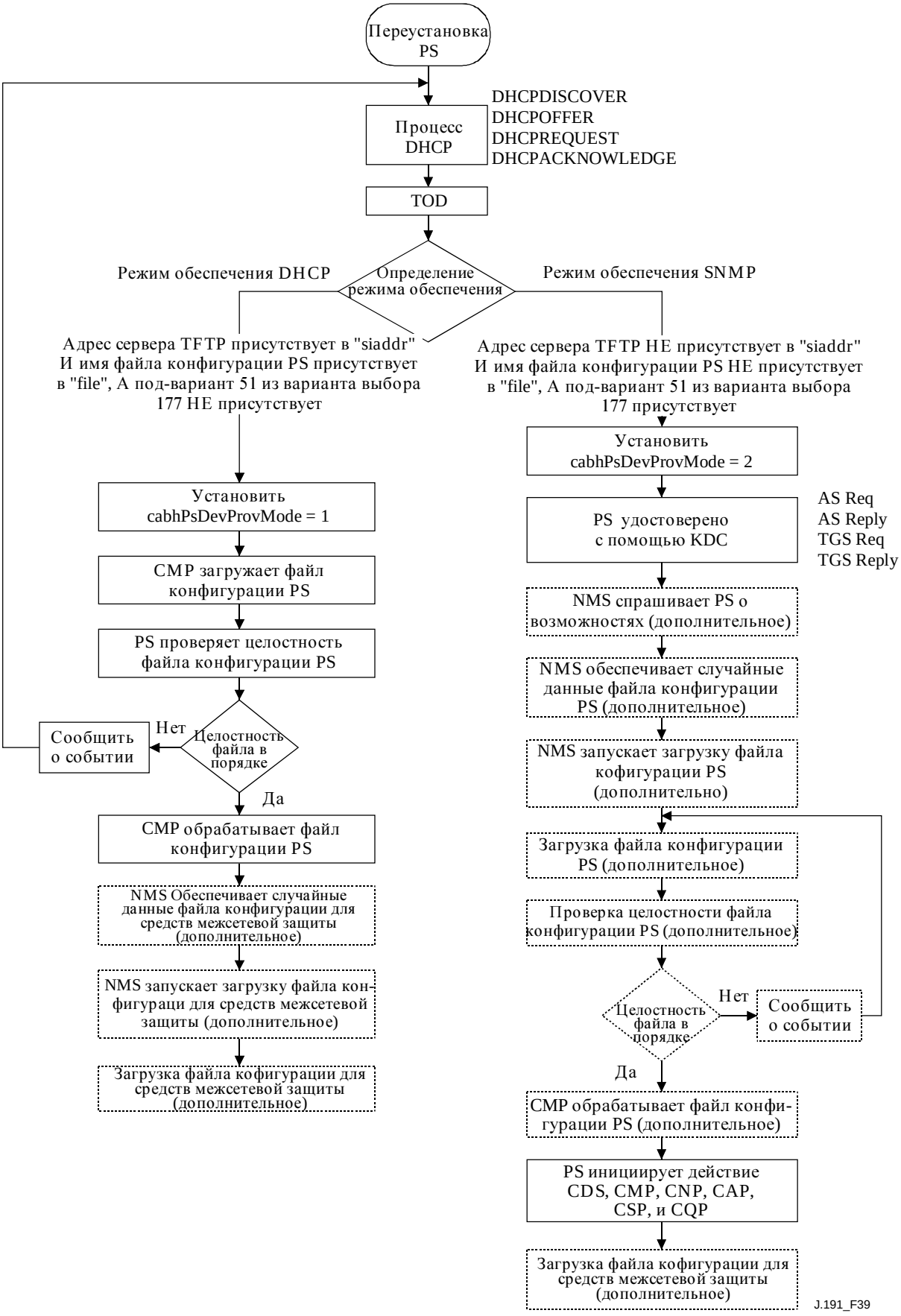


Рисунок 39/J.191 – Режимы обеспечения

Рисунок 40 и Таблица 48 описывают последовательность сообщений, необходимых для установления в начальное положение услуги PS, действующей в режиме обеспечения DHCP.

Обеспечение для услуги PS ОБЯЗАНО НЕ произойти перед процессом обеспечения кабельного модема.

Дополнительный процесс загрузки Файла конфигурации средств межсетевой защиты показан на Рисунке 40 с помощью штриховки.

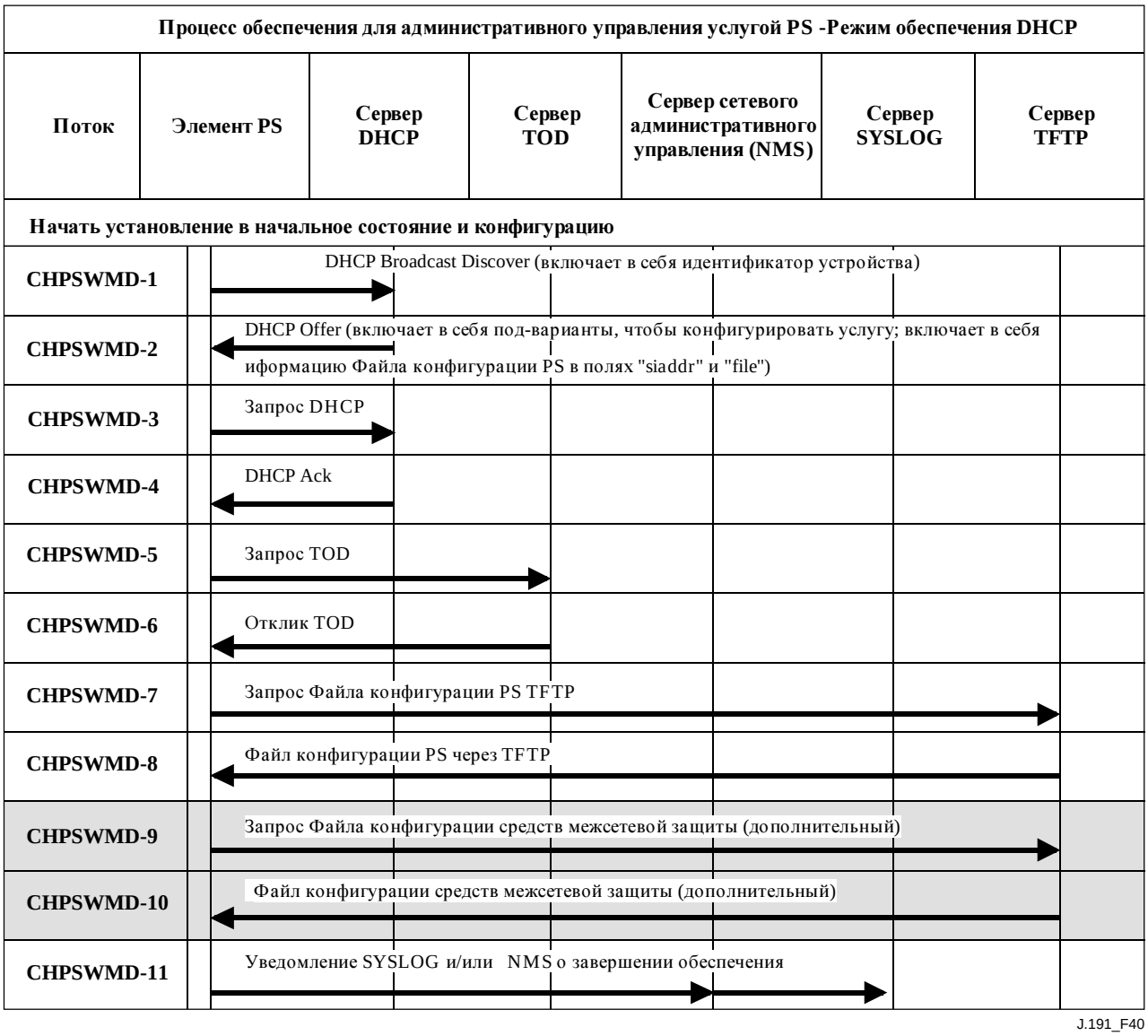


Рисунок 40/J.191 – Процесс обеспечения для административного управления услугой PS – Режим обеспечения DHCP

Таблица 48 описывает индивидуальные сообщения от CHPSWMD-1 до CHPSWMD-11, показанные на Рисунке 40.

Таблица 48/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения DHCP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения DHCP	Нормальная последовательность	Последовательность неудачи
CHPSWMD-1	*DHCP Broadcast Discover* Портал CDP (CDC) ОБЯЗАН послать широковещательное сообщение DISCOVER [*обнаружить*] протокола DHCP. Широковещание DISCOVER DHCP с помощью CDP (CDC) ОБЯЗАНО включать в себя обязательные варианты, перечисленные в Таблице 21. Услуга PS ОБЯЗАНА запустить Таймер обеспечения, используя начальное значение, которое доступно через cabhPsDevProvTimer, И установить объект cabhPsDevProvState в статус 'inProgress' (2), когда клиент CDC посылает широковещательное сообщение DISCOVER протокола DHCP.	Начать последовательность обеспечения.	Если не является успешным по протоколу DHCP, сообщить об ошибке и продолжать повторно пытаться послать Broadcast Discover DHCP, пока не достигнут успеха (возвратиться к шагу CHPSWMD-1). После 5 повторных попыток услуга PS инициирует действие CDS, как указано в 7.2.3.3
CHPSWMD-2	*DHCP OFFER* Ожидается, что OFFER [*предложение*] протокола DHCP, выпущенное сервером DHCP в кабельной сети, не будет включать в себя вариант кода 177 с под-вариантом 51, И ожидается, что оно будет включать в себя информацию Файла конфигурации PS в полях 'siaddr' и 'file' из сообщения DHCP. Услуга PS изменяет объект cabhPsDevProvMode, основанный на информации, полученной в OFFER протокола DHCP (см. 7.2.3.3).	CHPSWMD-2 ОБЯЗАН возникать после завершения CHPSWMD-1.	Если неудача по протоколу DHCP, возвратиться к CHPSWMD-1 и сообщить об ошибке.
CHPSWMD-3	*DHCP REQUEST* Портал CDP ОБЯЗАН послать соответствующему серверу DHCP сообщение DHCP REQUEST [*запрос*] для принятия DHCP OFFER.	CHPSWMD-3 ОБЯЗАН возникать после завершения CHPSWMD-2.	Если неудача по протоколу DHCP, возвратиться к CHPSWMD-1 и сообщить об ошибке.
CHPSWMD-4	*DHCP ACK* Сервер DHCP посылает порталу CDP сообщение DHCP ACK, которое содержит адрес IPv4 услуги PS. Услуга PS ОБЯЗАНА хранить адрес сервера Времени дня в cabhPsDevTimeServerAddr.	CHPSWMD-4 ОБЯЗАН возникать после завершения CHPSWMD-3.	Если неудача по протоколу DHCP, возвратиться к CHPSWMD-1 и сообщить об ошибке.

Таблица 48/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения DHCP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения DHCP	Нормальная последовательность	Последовательность неудачи
CHPSWMD-5	*Запрос Времени дня (TOD) согласно документу [RFC 868]* Услуга PS ОБЯЗАНА выпустить Запрос TOD к серверу TOD, определенный в DHCP OFFER.	CHPSWMD-5 ОБЯЗАН возникать после завершения CHPSWMD-4.	Продолжать с помощью CHPSWMD-6.
CHPSWMD-6	*Отклик TOD* Ожидается, что сервер TOD должен ответить текущим временем в формате UTC.	CHPSWMD-6 ОБЯЗАН возникать после завершения CHPSWMD-5.	Продолжать с помощью CHPSWMD-7,сообщить об ошибке и возвратиться к CHPSWMD-5 (продолжать делать попытки TOD, пока не будет успех).
CHPSWMD-7	*Запрос TFTP* Услуга PS, действующая в режиме обеспечения DHCP, ОБЯЗАНА послать серверу TFTP Запрос Get протокола TFTP, чтобы запросить файл данных указанной конфигурации, как описано в 7.3.3.	CHPSWMD-7 ОБЯЗАН произойти после завершения CHPSWMD-5. CHPSWMD-7 МОЖЕТ произойти перед завершением CHPSWMD-6.	Продолжать к CHPSWMD-8.

Таблица 48/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения DHCP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения DHCP	Нормальная последовательность	Последовательность неудачи
CHPSWMD-8	*Сервер TFTP посылает Файл конфигурации PS* После получения Файла конфигурации PS, вычисляются случайные данные Файла конфигурации и сравниваются со значением, добавленным к имени Файла конфигурации PS (см. 7.3.3.3). Файл конфигурации затем обрабатывается. Можно сослаться на 7.3.3 для содержимого Файла конфигурации PS. На дополнительной основе, адрес IP/FQDN сервера TFTP Файла конфигурации средств межсетевой защиты, имя файла для файла конфигурации средств межсетевой защиты, случайные данные Файла конфигурации средств межсетевой защиты и ключ шифрования (если Файл конфигурации средств межсетевой защиты шифруется) включаются в Файл конфигурации услуги PS, если Файл конфигурации средств межсетевой защиты должен быть загружен, и это есть метод, выбранный для указания этого.	CHPSWMD-8 ОБЯЗАН возникать после завершения CHPSWMD-7.	Если загрузка TFTP терпит неудачу, сообщить об ошибке, возвратиться к шагу CHPSWMD-7 (продолжать пытаться загрузить Файл конфигурации PS). Если обработка Файла конфигурации PS производит ошибку, продолжать с помощью шага CHPSWMD-9 и сообщить об ошибке как о событии. Если Таймер обеспечения истекает перед тем, как Файл конфигурации PS был успешно загружен, услуга PS ОБЯЗАНА сообщить об ошибке и вернуться к CHPSWMD-1.
CHPSWMD-9	*Запрос TFTP – Файл конфигурации средств межсетевой защиты (Дополнительный)* Если услуга PS получает в Файле конфигурации PS информацию Файла конфигурации средств межсетевой защиты (сервер межсетевой защиты TFTP и имя Файла конфигурации межсетевой защиты), услуга PS посылает серверу TFTP конфигурации межсетевой защиты запрос Get протокола TFTP, чтобы запросить Файл конфигурации средств межсетевой защиты (см. 11.3.5.1). Если услуга PS не получает информацию Файла конфигурации средств межсетевой защиты в Файле конфигурации PS, процесс обеспечения PS (Режим обеспечения DHCP) ОБЯЗАН опустить шаги CHPSWMD-9 и CHPSMWD-10 и продолжать с помощью шага CHPSWMD-11.	Если возникает шаг CHPSWMD-9, то он ОБЯЗАН возникать после завершения шага CHPSWMD-8.	Если TFTP терпит неудачу, продолжать с помощью операции PS, но сообщить об ошибке и продолжать пытаться осуществить шаг CHPSWMD-9.

Таблица 48/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения DHCP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения DHCP	Нормальная последовательность	Последовательность неудачи
CHPSWMD-10	*Сервер TFTP посылает Файл конфигурации средств межсетевой защиты (Дополнительный)* Если возникает шаг CHPSWMD-9, сервер TFTP посылает услуге PS Отклик TFTP, содержащий запрашиваемый файл. После получения Файла конфигурации средств межсетевой защиты вычисляются случайные данные Файла конфигурации и сравниваются со значением, полученным в Файле конфигурации PS. Если файл зашифрован, то он дешифруется. Затем файл обрабатывается. Можно сослаться на 11.3.5.	CHPSWMD-10 ОБЯЗАН возникать после завершения CHPSWMD-9.	Если TFTP терпит неудачу, продолжать с операцией PS, но сообщить об ошибке и пытаться перейти к шагу CHPSWMD-9. Если обработка файла конфигурации межсетевой защиты дает ошибку, продолжать и сообщить об ошибке как о событии.
CHPSWMD-11	*Обеспечение завершено* Если это запрашивается системой обеспечения, от услуги PS требуется информировать систему обеспечения о статусе обеспечения PS. Система обеспечения могла бы запросить от услуги PS посылку сообщения SYSLOG или захвата SNMP, или то и другое. Если услуга PS успешно завершила все требуемые шаги от CHPSWMD-1 до CHPSWMD-10, И услуга PS получила адрес сервера SYSLOG в DHCP OFFER, услуга PS ОБЯЗАНА послать сообщение о завершении обеспечения к серверу SYSLOG с состоянием обеспечения, установленным в PASS [*пропустить далее*]. Если услуга PS успешно завершила все требуемые шаги обеспечения от CHPSWMD-1 до CHPSWMD-10, И услуга PS получила действительные параметры для docsDevNmAccessGroup, указывающие "Приемник захвата" (docsDevNmAccessIP) и конфигурирующие завершенный захват обеспечения (cabhPsDevInitTrap) для значения 'читать только с захватами' (установив управление docsDevNmAccess в '4'. Ссылка на документ [RFC 2669]), услуга PS ОБЯЗАНА послать завершенный захват обеспечения (cabhPsDevInitTrap) с соответствующим параметром к "Приемнику захвата".	CHPSWMD-11 ОБЯЗАН возникать после завершения CHPSWMD-109.	Если захват SNMP терпит неудачу, сервер обеспечения может не знать, что процесс обеспечения завершился, пока он не опросит объект cabhPsProvState.

Таблица 48/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения DHCP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения DHCP	Нормальная последовательность	Последовательность неудачи
CHPSWMD-11	Если таймер обеспечения PS заканчивает работу перед тем, как были завершены все требуемые шаги от CHPSWMD-1 до CHPSWMD-10, И услуга PS получила адрес сервера SYSLOG в DHCP OFFER, услуга PS ОБЯЗАНА послать сообщение завершения обеспечения к серверу SYSLOG с состоянием обеспечения, установленным в FAIL [*неудача*]. Если таймер обеспечения PS заканчивает работу перед тем, как были завершены все требуемые шаги от CHPSWMD-1 до CHPSWMD-10, И услуга PS получила действительные параметры для объекта docsDevNmAccessGroup, определяющего Приемник захвата (docsDevNmAccessIP), и формирующего завершенный захват (cabhPsDevInitTrap) для положения 'считывать только с Захватами' (управление docsDevNmAccess установлено в '4'. Ссылка на документ [RFC 2669].), услуга PS ОБЯЗАНА послать неудавшийся захват обеспечения (cabhPsDevInitRetryTrap) к "Приемнику захвата". Услуга PS ОБЯЗАНА обновить значение cabhPsDevProvState со статусом 'pass' [*пропустить далее*] (1), когда шаги потоков обеспечения от CHPSWMD-1 до CHPSWMD-11 успешно завершились. Услуга PS ОБЯЗАНА обновить значение cabhPsDevProvState со статусом 'fail' [*неудача*] (3) И сообщить о событии, указывая неудачу процесса обеспечения, если Таймер обеспечения PS заканчивает работу до того, как значение cabhPsDevProvState обновляется со статусом 'pass'.		

Таймер обеспечения PS ОБЯЗАН НЕ переустанавливаться в начальное значение из объекта cabhPsDevProvTimer до тех пор, пока не закончит работу Таймер обеспечения PS, И значение cabhPsDevProvState все еще равно inProgress (2), ИЛИ услуга PS переустанавливается.

13.3 Процесс для обеспечения PS для административного управления: Режим обеспечения SNMP

Услуга PS запрашивает сетевой адрес WAN-Man из сервера DHCP головного узла, подлежащий использованию для обмена сообщениями административного управления между функциями административного управления PS и системой NMS кабельной сети. Если услуга PS определяет на основе процедуры, описанной в 7.2.3.3, что она действует в режиме обеспечения SNMP, услуга PS обезопасит свои сообщения административного управления, используя протокол SNMPv3, следуя процедуре удостоверения подлинности, описанной в 11.3.3.

Система NMS кабельной сети может дополнительно проинструктировать услугу PS (CMP), действующую в режиме обеспечения SNMP, загрузить Файл конфигурации PS из сервера TFTP. Уведомление о завершении процесса обеспечения предоставляется через процесс "Информирование о событии", описанный в 6.5.

Рисунок 41 иллюстрирует потоки сообщений, которые подлежат использованию для достижения обеспечения услуги PS, когда она действует в режиме обеспечения SNMP.

Процесс обеспечения для интерфейса WAN-Man услуги PS, действующей в режиме обеспечения SNMP, ОБЯЗАН иметь место через последовательность, которая изображается на Рисунке 41 и в подробностях описывается в Таблице 49. Дополнительные шаги показаны заштрихованным фоном на Рисунке 41. Эти дополнительные шаги могут быть выполнены немедленно, следуя шагу CHPSWMS-15, в более позднее время, или не выполнены вовсе.

Таблица 49 описывает индивидуальные шаги процесса обеспечения, отраженные на Рисунке 41.

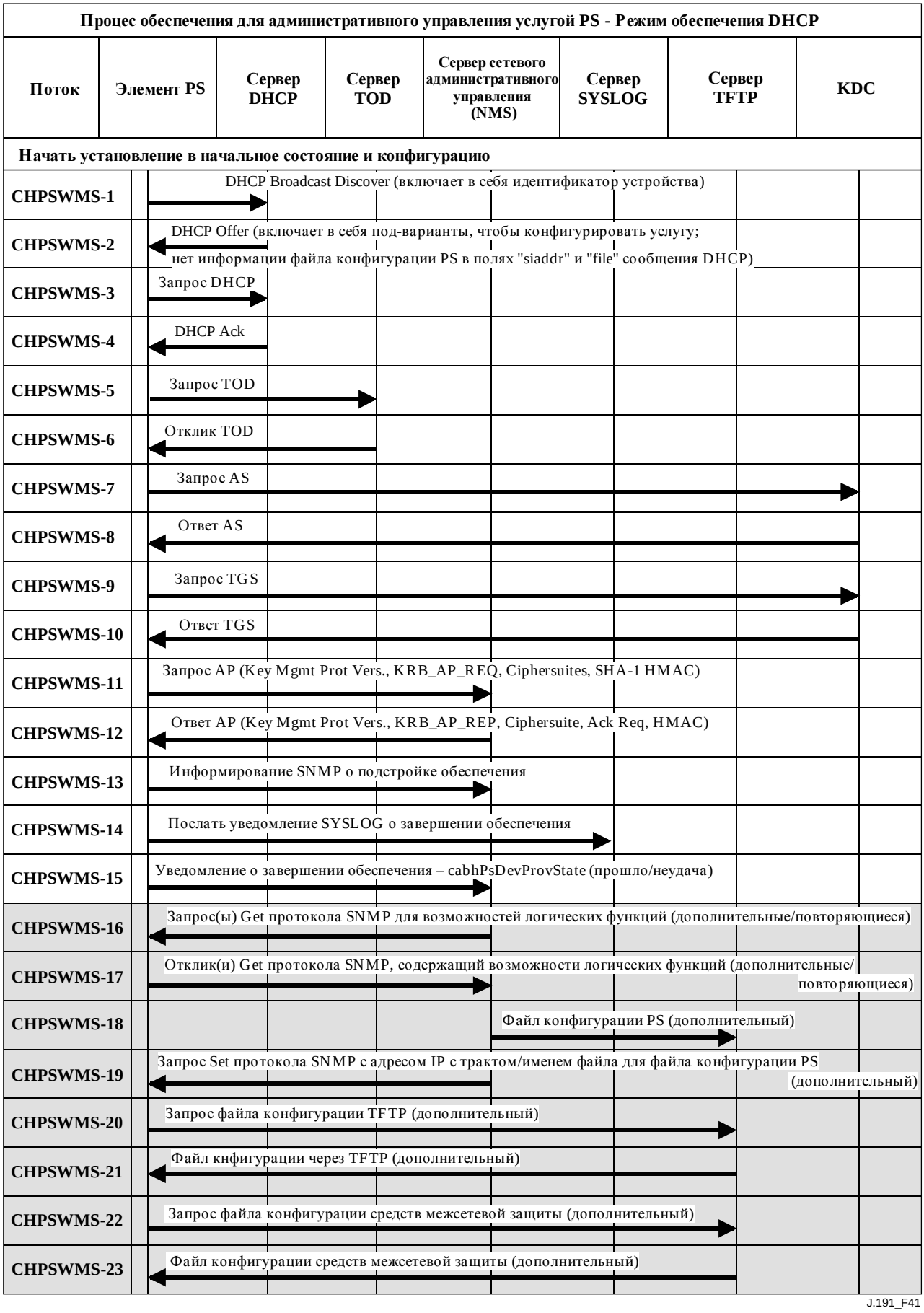


Figure 41/J.191 – Процесс обеспечения для административного управления услугой PS – Режим обеспечения SNMP

Таблица 49/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения SNMP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения SNMP	Нормальная последовательность	Последовательность неудачи
CHPSWMS-1	*DHCP Broadcast Discover* Портал CDP (CDC) ОБЯЗАН послать широковещательное сообщение DHCP DISCOVER. Широковещание DHCP DISCOVER с помощью портала CDP (CDC) ОБЯЗАНО включать в себя обязательные варианты, перечисленные в Таблице 21. Услуга PS ОБЯЗАНА запустить Таймер обеспечения, используя значение, доступное через cabhPsDevProvTimer, И установить cabhPsDevProvState в статус 'inProgress' (2), когда клиент CDC посылает широковещательное сообщение DHCP DISCOVER.	Начать последовательность обеспечения.	Если неудача по протоколу DHCP, сообщить об ошибке и продолжать пытаться передавать DHCP Broadcast Discover, пока не достигнут успеха (возврат к CHPSWMS-1). После 5 повторных попыток услуга PS инициирует операцию CDS, как указано в 7.2.3.3.
CHPSWMS-2	*DHCP OFFER* Ожидается, что DHCP OFFER, выпущенное сервером DHCP в кабельной сети, должно включать в себя вариант выбора кода 177 с под-вариантом И отсутствие информации Файла конфигурации PS в полях 'siaddr' и 'file' сообщения DHCP. Услуга PS изменяет объект cabhPsDevProvMode на основе информации, полученной в DHCP OFFER (см. 7.2.3.3).	CHPSWMS-2 ОБЯЗАН возникать после завершения CHPSWMS-1.	Если неудача по протоколу DHCP, возвратиться к шагу CHPSWMS-1 и сообщить об ошибке.
CHPSWMS-3	*DHCP REQUEST* Портал CDP ОБЯЗАН послать соответствующему серверу DHCP сообщение DHCP REQUEST для принятия сообщения DHCP OFFER.	CHPSWMS-3 ОБЯЗАН возникать после завершения CHPSWMS-2.	Если неудача по протоколу DHCP, возвратиться к шагу CHPSWMS-1.
CHPSWMS-4	*DHCP ACK* Сервер DHCP посылает порталу CDP сообщение DHCP ACK, которое содержит адрес IPv4 услуги PS. Услуга PS ОБЯЗАНА сохранить адрес сервера Времени дня в объекте cabhPsDevTimeServerAddr.	CHPSWMS-4 ОБЯЗАН возникать после завершения CHPSWMS-3.	Если неудача по протоколу DHCP, возвратиться к шагу CHPSWMS-1 и сообщить об ошибке.

Таблица 49/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения SNMP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения SNMP	Нормальная последовательность	Последовательность неудачи
CHPSWMS-5	*Запрос Времени дня (TOD, Time of Day) по [RFC 868]* Услуга PS посылает запрос TOD к адресу, хранимому в объекте cabhPsDevServerTime, как требуется в 7.4.2	CHPSWMS-5 ОБЯЗАН возникать после завершения CHPSWMS-4.	Продолжать с помощью шага CHPSWMS-6.
CHPSWMS-6	*Отклик TOD* Ожидается, что сервер TOD должен ответить с помощью текущего времени в формате UTC.	CHPSWMS-6 ОБЯЗАН возникать после завершения CHPSWMS-5.	Продолжать с помощью шага CHPSWMS-7, сообщить об ошибке и возвратиться к шагу CHPSWMS-5 (продолжать пытаться осуществить TOD, пока не будет успех).
CHPSWMS-7	*Запрос AS*[a)] Услуга PS ОБЯЗАНА послать сообщение "Запрос AS" к оператору KDC, чтобы запросить билет Kerberos.	CHPSWMS-7 ОБЯЗАН возникать после завершения CHPSWMS-5. CHPSWMS-7 МОЖЕТ возникать до завершения CHPSWMS-6.	Возвратиться к шагу CHPSWMS-1.
CHPSWMS-8	*Ответ AS* От оператора KDC принимается сообщение "Ответ AS", содержащее билет Kerberos.	CHPSWMS-8 ОБЯЗАН возникать после завершения CHPSWMS-7.	Возвратиться к шагу CHPSWMS-1.
CHPSWMS-9	*Запрос TGS* Если услуга PS получила Билет предоставления билета (*TGT, Ticket Granting Ticket*) в шаге CHPSWMS-10 процесса обеспечения Интерфейса WAN-Man услуги PS, то оператору KDC ОБЯЗАНО быть послано сообщение "Запрос TGS".	CHPSWMS-9 ОБЯЗАН возникать после завершения CHPSWMS-8.	Возвратиться к шагу CHPSWMS-1.
CHPSWMS-10	*Ответ TGS* От оператора KDC принимается сообщение "Ответ TGS", содержащее билет.	CHPSWMS-10 ОБЯЗАН возникать после завершения CHPSWMS-9.	Возвратиться к шагу CHPSWMS-1.

Таблица 49/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения SNMP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения SNMP	Нормальная последовательность	Последовательность неудачи
CHPSWMS-11	*Запрос AP* К Серверу обеспечения ОБЯЗАНО быть послано сообщение "Запрос AP", чтобы запросить ключевую информацию для протокола SNMPv3.	CHPSWMS-11 ОБЯЗАН возникать после завершения CHPSWMS-10.	Возвратиться к шагу CHPSWMS-1.
CHPSWMS-12	*Ответ AP* От сервера обеспечения принимается сообщение "Ответ AP", содержащего ключевую информацию для протокола SNMPv3. ПРИМЕЧАНИЕ – Перед следующим шагом ключи протокола SNMPv3 ОБЯЗАНЫ быть установлены, а связанные таблицы SNMPv3 заполнены. Ключи и таблицы устанавливаются с использованием информации в Ответе AP.	CHPSWMS-12 ОБЯЗАН возникать после завершения CHPSWMS-11.	Возвратиться к шагу CHPSWMS-1.
CHPSWMS-13	*Информация SNMP* Услуга PS ОБЯЗАНА послать системе NMS INFORM протокола SNMPv3 (cabhPsDevProvEnrollTrap), запрашивая регистрацию. Адрес IP этого ОБЪЕКТА SNMP ОБЕСПЕЧЕНИЯ содержится в сообщении DHCP OFFER.	CHPSWMS-13 ОБЯЗАН возникать после завершения CHPSWMS-12.	Возвратиться к шагу CHPSWMS-1.
CHPSWMS-14	*Уведомление SYSLOG* Если услуга PS приняла адрес сервера SYSLOG в DHCP OFFER, услуга PS ОБЯЗАНА послать к SYSLOG уведомление "обеспечение завершено". Это уведомление будет включать в себя результат неудачи прохождения для операции обеспечения. Общий формат этого уведомления является таким, как определено в 6.5.1.	CHPSWMS-14 ОБЯЗАН возникать после завершения CHPSWMS-13.	

Таблица 49/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения SNMP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения SNMP	Нормальная последовательность	Последовательность неудачи
CHPSWMS-15	*SNMP Inform* Услуга PS ОБЯЗАНА послать системе NMS сообщение SNMP INFORM (cabhPsDevInitTrap), содержащее уведомление "обеспечение завершено". FAIL [*неудача*] возникает тогда, когда обработка файла конфигурации терпит неудачу. В противном случае состояние обеспечения есть PASS [*прохождение*]. Услуга PS ОБЯЗАНА обновить значение cabhPsDevProvState со статусом 'pass' (1), когда шаги потока обеспечения с CHPSWMS-1 по CHPSWMS-23 завершаются успешно. Услуга PS ОБЯЗАНА обновить значение cabhPsDevProvState со статусом 'fail' (3) И сообщить о событии, указывая неудачу процесса обеспечения, если Таймер обеспечения услуги PS заканчивает работу до того, как значение cabhPsDevProvState обновляется со статусом 'pass'.	CHPSWMS-15 ОБЯЗАН возникать после завершения CHPSWMS-14.	Если SNMP Inform терпит неудачу, сервер обеспечения может не знать, что процесс обеспечения был завершен, пока он не опросит объект cabhPsProvisioningState.
Дополнительные шаги			
CHPSWMS-16	*SNMP Get*[b)] Если система обеспечения нуждается в дополнительных возможностях устройств, то система обеспечения запрашивает эти возможности от услуги PS через Запросы Get протокола SNMPv3. (повторяющееся:) Система NMS посылает услуге PS один или более запросов Get протокола SNMPv3 для получения любой необходимой информации о возможностях PS. Приложение обеспечения может использовать запрос GETBulk для получения нескольких образцов информации в единственном сообщении.	Не ожидается, что шаг CHPSWMS-16 возникнет до завершения шага CHPSWMS-15.	Возвратиться к шагу CHPSWMS-1.

Таблица 49/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения SNMP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения SNMP	Нормальная последовательность	Последовательность неудачи
CHPSWMS-17	*Отклик Get протокола SNMP* (Повторяющийся:) Услуга PS ОБЯЗАНА ответить на сообщения запроса Get или Get Bulk [*Получить оптом*] системы NMS с помощью отклика Get для каждого запроса Get. После всех запросов Get или Get Bulk система NMS посылает запрошенные данные к обеспечивающему приложению.	CHPSWMS-17 ОБЯЗАН возникать после завершения CHPSWMS-16.	Не имеется (N/A)
CHPSWMS-18	*Создание файла конфигурации* (Дополнительный:) Система обеспечения использует информацию от шагов CHPSWMS-14 и CHPSWMS-15 обеспечения услуги PS, чтобы создать Файл конфигурации PS. Система обеспечения выполняет случайные данные на содержимом файла конфигурации. Случайные данные посылаются к услуге PS в следующем шаге.	CHPSWMS-18 ОБЯЗАН возникать после завершения CHPSWMS-17.	N/A
CHPSWMS-19	*SNMP Set* Система обеспечения могла бы приказать системе NMS послать сообщение Set [*установить*] протокола SNMP к услуге PS, содержащее Адрес IP сервера TFTP, имя файла для Файла конфигурации PS и случайные данные файла конфигурации, как описано в 7.3.3.2 (режим обеспечения SNMP). Дополнительно, Адрес IP сервера TFTP Файла конфигурации средств межсетевой защиты, имя файла для Файла конфигурации средств межсетевой защиты, случайные данные Файла конфигурации средств межсетевой защиты и ключ шифрования (если Файл конфигурации межсетевой защиты шифрован) включаются в Set протокола SNMP, если должен быть загружен Файл конфигурации межсетевой защиты, и этот метод выбирается для указания его.	CHPSWMS-19 ОБЯЗАН возникать после завершения CHPSWMS-18.	Возвратиться к шагу CHPSWMS-1, если было получено Set, но была ошибка обработки.

Таблица 49/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения SNMP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения SNMP	Нормальная последовательность	Последовательность неудачи
CHPSWMS-20	*Запрос TFTP* Если NMS запускает услугу PS, чтобы загрузить Файл конфигурации PS, как описано в 7.3.3.2, услуга PS ОБЯЗАНА послать серверу TFTP запрос Get протокола TFTP, чтобы запросить указанный Файл конфигурации PS.	CHPSWMS-20 ОБЯЗАН возникать после завершения CHPSWMS-19.	Продолжать с помощью шага CHPSWMS-21.
CHPSWMS-21	*Сервер TFTP посылает Файл конфигурации* После того, как услуга PS получает Файл конфигурации PS, услуга PS вычисляет случайные данные Файла конфигурации PS и сравнивает их со значением, полученным в шаге CHPSWMS-19. Затем услуга PS обрабатывает Файл конфигурации PS. Можно сослаться на 7.3.3 для содержимого Файла конфигурации PS. Дополнительно, адрес IP /FQDN сервера TFTP Файла конфигурации средств межсетевой защиты, имя файла для Файла конфигурации средств межсетевой защиты, случайные данные Файла конфигурации средств межсетевой защиты и ключ шифрования (если Файл конфигурации средств межсетевой защиты зашифрован) включаются в Файл конфигурации PS, если имеется Файл конфигурации средств межсетевой защиты, подлежащий загрузке, и это является методом, выбранным для указания его.	CHPSWMS-21 ОБЯЗАН возникать после завершения CHPSWMS-20.	Если загрузка TFTP терпит неудачу, сообщить об ошибке, перейти к CHPSWMS-23 и продолжать повторно попытаться осуществить CHPSWMS-20 (продолжать повторно пытаться загрузить Файл конфигурации PS). Если обработка Файла конфигурации порождает ошибку, продолжать и сообщить об ошибке, как о событии.
CHPSWMS-22	*Запрос TFTP – Файл конфигурации средств межсетевой защиты* (Дополнительный) Услуга PS посылает серверу TFTP конфигурации средств межсетевой защиты запрос Get TFTP, чтобы запросить файл конфигурации указанных средств межсетевой защиты.	Если возникает шаг CHPSWMS-22, он ОБЯЗАН возникать после завершения шага CHPSWMS-21.	Возвратиться к шагу CHPSWMS-1.

Таблица 49/J.191 – Описания потоков для процесса обеспечения WAN-Man услуги PS для режима обеспечения SNMP

Шаг потока	Обеспечение WAN-Man услуги PS: Режим обеспечения SNMP	Нормальная последовательность	Последовательность неудачи
CHPSWMS-23	*Сервер TFTP посылает Файл конфигурации средств межсетевой защиты* Сервер TFTP посылает услуге PS отклик TFTP, содержащий запрашиваемый файл. После того, как услуга PS получает Файл конфигурации средств межсетевой защиты, услуга PS вычисляет случайные данные Файла конфигурации средств межсетевой защиты и сравнивает их со значением, полученным в шаге CHPSWMS-21. Если файл зашифрован, то он дешифруется. Затем файл обрабатывается. Можно сделать ссылку на 7.3.3 для описания содержимого Файла конфигурации.	CHPSWMS-23 ОБЯЗАН возникать после завершения CHPSWMS-22.	Если загрузка TFTP терпит неудачу, продолжать операцию с услугой PS, но сообщить об ошибке и продолжать повторно осуществлять шаг CHPSWMS-22. Если обработка файла конфигурации средств межсетевой защиты порождает ошибку, продолжать и сообщить об ошибке, как о событии.

a) В некоторых случаях шаги CHPSWMS-7-CHPSWMS-10 являются дополнительными. Для подробностей можно сослаться на раздел 11.

b) Операции Get протокола SNMP и следующего отклика Get протокола SNMP являются дополнительными, в зависимости от того, требуется ли дополнительная информация для формирования Файла конфигурации PS, а также в зависимости от того, нужен ли Файл конфигурации PS.

13.3.1 Загрузка файла конфигурации WAN-Man услуги PS

Услуга PS, действующая в режиме обеспечения SNMP МОЖЕТ содержать достаточную фабричную информацию, заданную по умолчанию, чтобы обеспечивать действие либо обеих сторон сетей WAN и LAN, либо одной стороны без загружаемого Файла конфигурации PS. Если услуга PS действует в режиме обеспечения SNMP, то Файл конфигурации PS МОЖЕТ быть загружен для начального обеспечения, чтобы заменить фабричные значения по умолчанию или обеспечить дополнительную информацию.

Файл конфигурации средств межсетевой защиты содержит информацию для обеспечения функции межсетевой защиты. Индикация о загрузке Файла конфигурации средств межсетевой защиты войдет или в Файл конфигурации PS или через сообщение SET протокола SNMP во время установления в начальное состояние.

13.3.2 Таймер обеспечения PS

Таймер обеспечения предоставляется для того, чтобы гарантировать, что услуга PS будет продолжать циклически действовать через процесс обеспечения, если какая-либо из операций не завершена. Объект таймера, cabhPsDevProvTimer, имеет установление в начальное состояние по умолчанию около 5 минут.

Режим обеспечения DHCP

Таймер обеспечения ОБЯЗАН начинать обратный отсчет, когда начинается шаг CHPSWMD-1. Если Таймер обеспечения PS заканчивает работу перед тем, как выполняется шаг CHPSWMD-12, клиент CDC ОБЯЗАН установить объект cabhPsDevProvState в статус '3' (неудача), процесс обеспечения ОБЯЗАН возвратиться к шагу CHPSWMD-1, И услуга PS должна породить соответствующее событие и переустановить Таймер обеспечения PS в значение cabhPsDevProvTimer.

Режим обеспечения SNMP

Таймер обеспечения ОБЯЗАН начать обратный отсчет, когда начинается шаг CHPSWMS-1. Если Таймер обеспечения PS заканчивает работу перед тем, как выполняется шаг CHPSWMS-23, клиент CDC ОБЯЗАН установить объект cabhPsDevProvState в статус '3' (неудача), процесс обеспечения ОБЯЗАН вернуться к шагу CHPSWMS-1, услуга PS ОБЯЗАНА сообщить о соответствующем событии, И услуга PS ОБЯЗАНА переустановить Таймер обеспечения PS в значение of cabhPsDevProvTimer.

13.3.3 Информация о регистрации обеспечения/о завершении обеспечения

Для услуги PS, действующей только в режиме обеспечения SNMP, информация регистрации обеспечения, определенная в Дополнении B, дает возможность Серверу обеспечения определять, что услуга PS готова для Файла конфигурации PS.

В Режимах обеспечения как DHCP, так и SNMP захват завершения обеспечения (cabhPsDevInitTrap), определяемый в Дополнении B, указывает, была ли последовательность обеспечения завершена успешно, или нет.

13.4 Обеспечение SYSLOG

Адрес IP сервера syslog ОБЯЗАН быть обеспечен через процесс DHCP. Событие syslog не будет посылаться, если адрес IP сервера syslog не конфигурирован.

13.4.1 Состояние обеспечения и информирование об ошибке

Как указано в Таблицах 48 и 49, неудача шагов в процессе обеспечения обычно имеет своим результатом перезапуск процесса на первом шаге, CHPSWMD-1 или CHPSWMS-1.

13.5 Процесс обеспечения WAN-Data услуги PS

Услуга PS запрашивает нуль или более сетевых адресов WAN-Data от сервера DHCP в кабельной сети, подлежащих использованию для обмена данными между элементами, подключенными к Интернет и Устройствам IP сети LAN.

Нет различий в действии WAN-Data услуги PS между режимами обеспечения DHCP и SNMP.

Следующие диаграммы иллюстрируют потоки сообщений, которые должны использоваться для завершения обеспечения адресов WAN-Data услуги PS.

Если возникает режим обеспечения для адреса (адресов) WAN-Data услуги PS, то он ОБЯЗАН следовать последовательности, отображенной на Рисунке 42 и подробно описанной в Таблице 50.

Рисунок 42/J.191 – Процесс обеспечения WAN-data услуги PS

Таблица 50/J.191 – Описания потоков для процесса обеспечения WAN-data услуги PS

Шаг потока	Обеспечение адреса WAN-Data услуги PS	Нормальная последова-тельность	Последова-тельность неудачи
CHPSWD-1	*DHCP Broadcast Discover* Услуга PS ОБЯЗАНА послать широковещательное сообщение DHCP DISCOVER, включив обязательные варианты, перечисленные в Таблице 21.	Перейти к CHPSWD-2.	Если неудача по протоколу DHCP, повторить шаг CHPSWD-1.
CHPSWD-2	*DHCP OFFER* Сервер DHCP в головном узле получает пакет DHCP DISCOVER, назначает адрес IP из объединения ресурсов WAN-Data, выстраивает пакет DHCP OFFER и передает DHCP OFFER к Агенту переприема DHCP в системе CMTS.	Перейти к CHPSWD-3.	Если неудача, клиент запустит выдержку времени по протоколу DHCP, и шаг CHPSWD-1 будет повторен.
CHPSWD-3	*DHCP REQUEST* Портал CDP ОБЯЗАН послать к	CHPSWD-3 ОБЯЗАН	Если неудача по протоколу

Таблица 50/J.191 – Описания потоков для процесса обеспечения WAN-data услуги PS

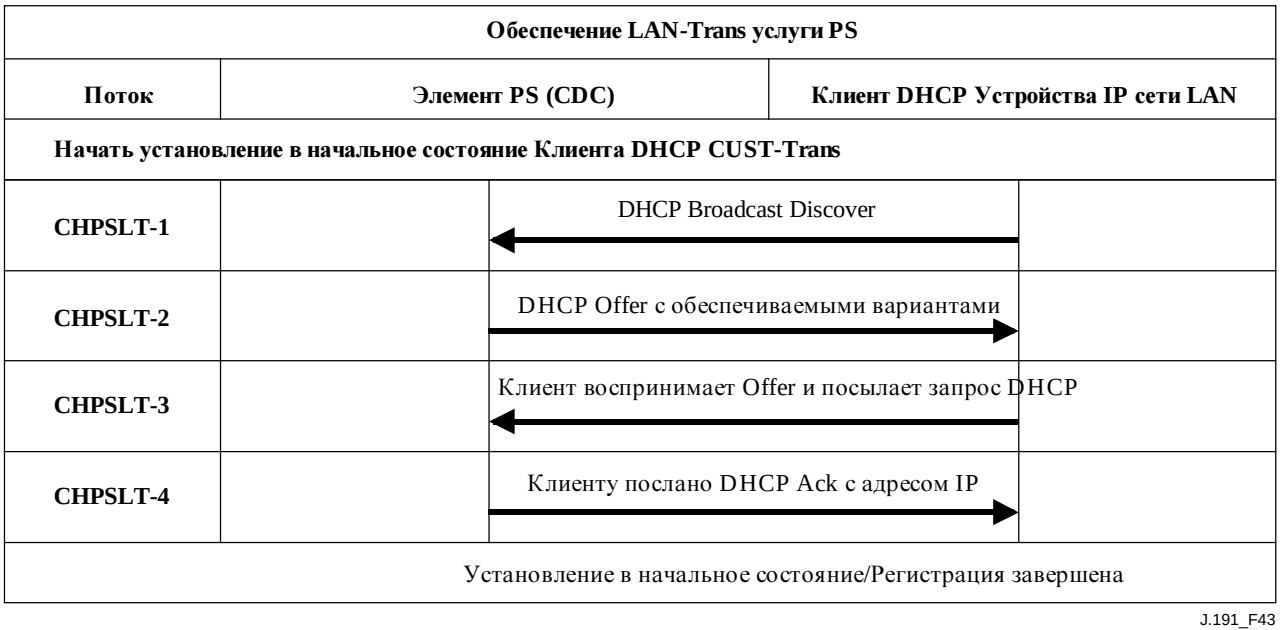
Шаг потока	Обеспечение адреса WAN-Data услуги PS	Нормальная последова-тельность	Последова-тельность неудачи
	соответствующему серверу DHCP сообщение DHCP REQUEST, чтобы принять DHCP OFFER.	возникать после завершения CHPSWD-2.	DHCP, вернуться к CHPSWD-1.
CHPSWD-4	*DHCP ACK* Сервер DHCP посылает порталу CDP сообщение DHCP ACK, которое содержит адрес IPv4 для интерфейса WAN-Data услуги PS.	CHPSWD-4 ОБЯЗАН возникать после завершения CHPSWD-3. Обеспечение завершается с завершением CHPSWD-4.	Если неудача по протоколу DHCP, вернуться к шагу CHPSWD-1.

13.6 Процесс обеспечения: Клиент DHCP в области LAN-Trans

Устройства IP сети LAN запрашивают адреса IP через процессы DHCP. Элемент PS обрабатывает эти сообщения согласно параметрам обеспечения, назначенным системой NMS кабельной сети (см. 7.2.3.2).

Этот раздел описывает процесс обеспечения для случая, где система NMS обеспечила услугу для действий в режиме "Первичная пакетная обработка" C-NAT или C-NAPT (см. раздел 8). Нет различия в процессе обеспечения Устройства IP области LAN-Trans между режимами обеспечения DHCP и SNMP.

Потоки сообщений процесса обеспечения для Устройства IP сети LAN в адресной области LAN-Trans описываются на Рисунке 43. Дополнительные подробности относительно процесса предоставлены в Таблице 51.



J.191_F43

Рисунок 43/J.191 – Процесс обеспечения для Устройства IP сети LAN IP в области LAN-Trans

Процесс обеспечения для Устройства IP сети LAN в области LAN-Trans ОБЯЗАН происходить через последовательность, отображенную на Рисунке 43 и подробно описанную в Таблице 51.

Таблица 51/J.191 – Описания потоков для процесса обеспечения LAN-Trans услуги PS

Шаг потока	Обеспечение адреса Клиента LAN-Trans	Нормальная последова-тельность	Последовате-льность неудачи
CHPSLT-1	*DHCP Broadcast Discover* Клиент[a)] посылает широковещательное сообщение DHCP DISCOVER на свою местную сеть LAN[b)].	Перейти к шагу CHPSLT-2.	Если неудача по протоколу DHCP, повторить шаг CHPSLT-1.
CHPSLT-2	*DHCP OFFER* Услуга PS на своем интерфейсе LAN получает сообщение DHCP DISCOVER и проверяет поле chaddr. Если: – имеется доступный адрес LAN-Trans; и – нет административных соображений, которые мотивируют отрицание адреса LAN-Trans для клиента, то тогда услуга PS ОБЯЗАНА послать сообщение DHCP OFFER к клиенту, чтобы предложить ему адрес LAN-Trans либо в качестве односторонней передачи, либо в качестве широковещательной передачи, характерной для звена (согласно биту BROADCAST поля флагов из DHCP DISCOVER).	Перейти к шагу CHPSLT-3.	Если неудача, клиент будет осуществлять выдержку времени по протоколу DHCP, и шаг CHPSLT-1 будет повторен.
CHPSLT-3	*DHCP REQUEST* Клиент DHCP Устройства IP сети LAN получает сообщение DHCP OFFER. Когда клиент DHCP Устройства IP сети LAN желает принять сообщение DCHP OFFER, ожидается, что он будет форматировать и посылать пакет DHCP REQUEST, используя широковещание, характерное для звена[c)].	Перейти к шагу CHPSLT-4.	Если неудача, клиент будет осуществлять выдержку времени по протоколу DHCP и шаг CHPSLT-1 будет повторен.
CHPSLT-4	*DHCP ACK* Услуга PS на своем интерфейсе LAN получает сообщение DHCP REQUEST. Если указанный адрес LAN-Trans все еще пригоден для назначения, услуга PS ОБЯЗАНА затем послать сообщение DHCP ACK к клиенту либо в качестве односторонней передачи, либо в качестве широковещательной передачи, характерной для звена (согласно биту BROADCAST поля флагов из DHCP REQUEST).	Обеспечение завершено.	Если неудача, клиент будет осуществлять выдержку времени по протоколу DHCP и шаг CHPSLT-1 будет повторен.

a) Если клиент осведомлен о своем предыдущем адресе IP (например, следуя начальной перезагрузке), он может опустить сообщение DHCP DISCOVER и перейти к шагу 3.

b) Если клиент располагается в сети без широковещания, то ожидается осуществление однонаправленной передачи сообщения к Серверу DHCP.

c) Если клиент располагается в сети без широковещания, то ожидается, что он осуществит однонаправленную передачу сообщения к услуге PS.

13.6.1 Выбор адреса LAN-Trans и варианты выбора DCHP

Услуга PS ОБЯЗАНА выбрать адрес LAN-Trans, что предлагается из диапазона, указанного переменными величинами MIB cabhCdpLanPoolStart и cabhCdpLanPoolEnd.

Система CDS услуги PS ОБЯЗАНА включать в сообщение DHCP OFFER обязательные варианты, перечисленные в Таблице 18.

13.7 Процесс обеспечения: Клиент DCHP в области LAN-Pass

Некоторые приложения клиентов не будут функционировать должным образом с транслированным сетевым адресом. Чтобы приспособить эти приложения, услуге PS разрешается действовать в Сквозном режиме (прозрачное перемыкание). Как описано в 8.2.2.2, перемыкание происходит тогда, когда система NMS кабельной сети устанавливает режим "Первичная обработка пакетов" (cabhCapPrimaryMode) в сквозной режим, или путем чтения индивидуальных адресов MAC Устройства IP сети LAN – в Сквозную таблицу (cabhCapPassthroughTable). Рисунок 44 описывает процесс для запроса и назначения сетевого адреса Устройствам IP сети LAN, для которых услуга PS предварительно была обеспечена так, чтобы перемыкать трафик. Когда услуга PS была конфигурирована для перемыкания трафика для Устройства IP сети LAN, сообщения DHCP DISCOVER и DHCP REQUEST, выпущенные таким Устройством IP сети LAN, будут обслуживаться сервером DHCP кабельной сети, а не системой CDS.

Процесс обеспечения для Устройства IP сети LAN в области LAN-Pass ОБЯЗАН иметь место через последовательность, отображенную на Рисунке 44 и подробно описанную в Таблице 52.

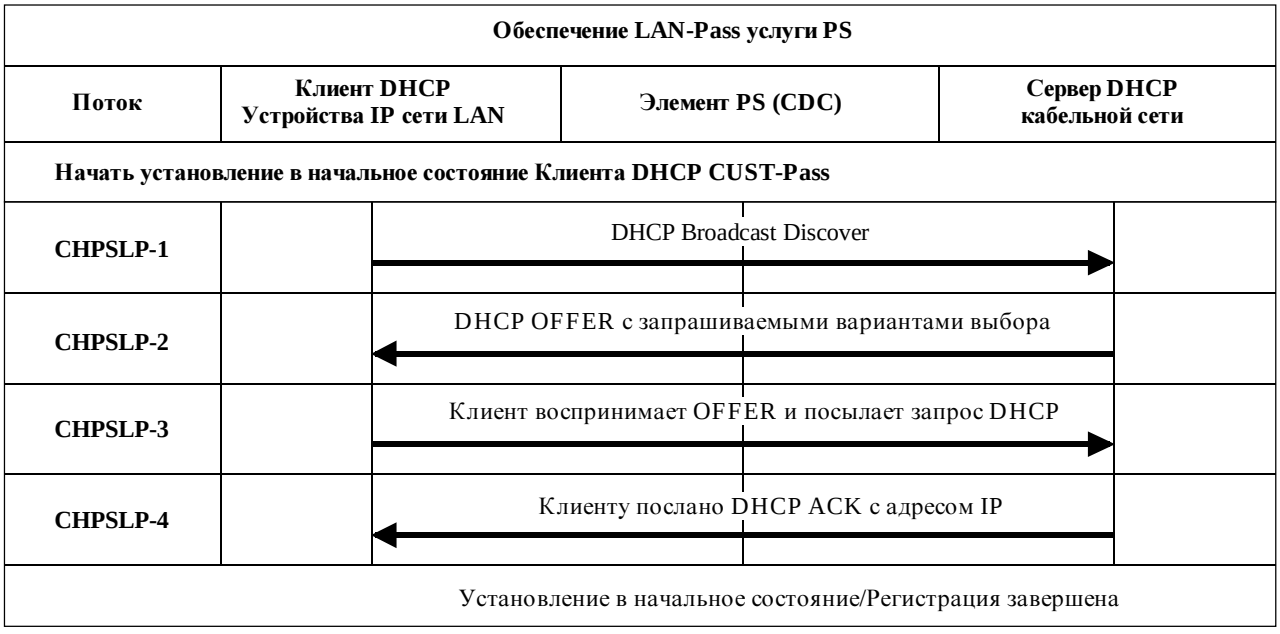


Рисунок 44/J.191 – Процесс обеспечения для Устройства IP сети LAN в области LAN-Pass

Таблица 52/J.191 – Описания потоков для процесса обеспечения LAN-Pass

Шаг потока	**Обеспечение проходного адреса клиента**	**Нормальная последова-тельность**	**Последовате-льность неудачи**
CHPSLP-1	*DHCP Broadcast Discover* Устройство IP сети LAN осуществляет широковещание сообщения DHCP DISCOVER на своей местной сети LAN[a)]. Услуга PS на своем интерфейсе LAN получает широковещательный пакет DHCP DISCOVER и ОБЯЗАНА прозрачно перемкнуть пакет на интерфейс сети WAN без изменения содержимого пакета.	Перейти к шагу CHPSLP-2.	Если неудача по протоколу DHCP, повторить шаг CHPSLP-1.
CHPSLP-2	*DHCP OFFER* Сервер DHCP в головном узле получает пакет DHCP DISCOVER и назначает адрес IP, к которому можно обратиться внешним образом, и другие варианты выбора, выстраивает пакет DHCP OFFER и передает DHCP OFFER к Устройству IP сети LAN. Услуга PS ОБЯЗАНА прозрачным образом перемкнуть сообщение DHCP OFFER с интерфейса сети WAN на свой интерфейс сети LAN без изменения содержимого пакета IP.	Перейти к шагу CHPSLP-3.	Если неудача, то Устройство IP сети LAN осуществит выдержку времени по протоколу DHCP, и будет повторен шаг CHPSLP-1.
CHPSLP-3	*DHCP REQUEST* Устройство IP сети LAN получает сообщение DHCP OFFER и выпускает сообщение DHCP REQUEST. Услуга PS ОБЯЗАНА прозрачным образом перемкнуть сообщение DHCP REQUEST из своего интерфейса сети LAN к своему интерфейсу сети WAN без изменения содержимого пакета IP.	Перейти к шагу CHPSLP-4.	Если неудача по протоколу DHCP, повторить шаг CHPSLP-1.
CHPSLP-4	*DHCP ACK* Сервер DHCP головного узла получает сообщение DHCP REQUEST и посылает сообщение DHCP ACK к Устройству IP сети LAN с адресом IPv4 Устройства IP сети LAN. Услуга PS ОБЯЗАНА прозрачным образом перемкнуть сообщение DHCP ACK из своего интерфейса сети WAN к своему интерфейсу LAN без изменения содержимого пакета IP.	Обеспечение завершено.	Если неудача, то Устройство IP сети LAN осуществит выдержку времени по протоколу DHCP, и шаг CHPSLP-1 будет повторен.

[a)] Если клиент располагается в сети без широковещания, то он должен осуществить однонаправленную передачу сообщения к Серверу DHCP или к Агенту переприема DHCP в кабельной сети.

Дополнение A

Объекты MIB

Это дополнение перечисляет все требуемые объекты MIB, как указано в 6.3.7.

ИМЯ MIB/Параметр	**Max-Access**	**Постоянный**
mib-2		
система		
sysDescr	только для чтения	Да
sysObjectID	только для чтения	Да
sysUpTime	только для чтения	Нет
sysContact	только для чтения	Да
sysName	только для чтения	Да
sysLocation	только для чтения	Да
sysServices	только для чтения	Да
интерфейс [RFC 2863]		
ifNumber	только для чтения	Нет
ifTable/ifEntry		
ifIndex	только для чтения	Нет
ifDescr	только для чтения	Нет
ifType	только для чтения	Нет
ifMtu	только для чтения	Нет
ifSpeed	только для чтения	Нет
ifPhysAddress	только для чтения	Нет
ifAdminStatus	для чтения и записи	Нет
ifOperStatus	только для чтения	Нет
ifLastChange	только для чтения	Нет
ifInOctets	только для чтения	Нет
ifInUcastPkts	только для чтения	Нет
ifInNUcastPkts	только для чтения	Нет
ifInDiscards	только для чтения	Нет
ifInErrors	только для чтения	Нет
ifInUnknownProtos	только для чтения	Нет
ifOutOctets	только для чтения	Нет
ifOutUcastPkts	только для чтения	Нет
ifOutNUcastPkts	только для чтения	Нет
ifOutDiscards	только для чтения	Нет
ifOutErrors	только для чтения	Нет
ifOutQLen	только для чтения	Нет
ifSpecifc	только для чтения	Нет
ip [RFC 2011]		
ipForwarding	для чтения и записи	Нет

ipDefaultTTL	для чтения и записи	Нет
ipInReceives	только для чтения	Нет
ipInHdrErrors	только для чтения	Нет
ipInAddrErrors	только для чтения	Нет
ipForwDatagrams	только для чтения	Нет
ipInUnknownProtos	только для чтения	Нет
ipInDiscards	только для чтения	Нет
ipInDelivers	только для чтения	Нет
ipOutRequests	только для чтения	Нет
ipOutDiscards	только для чтения	Нет
ipOutNoRoutes	только для чтения	Нет
ipReasmTimeout	только для чтения	Нет
ipReasmReqds	только для чтения	Нет
ipReasmOKs	только для чтения	Нет
ipReasmFails	только для чтения	Нет
ipFragOKs	только для чтения	Нет
ipFragFails	только для чтения	Нет
ipFragCreates	только для чтения	Нет
ipNetToMediaTable/ipNetToMediaEntry		
ipNetToMediaIfIndex	для чтения и создания	Нет
ipNetToMediaPhyAddress	для чтения и создания	Нет
ipNetToMediaNetAddress	для чтения и создания	Нет
ipNetToMediaType	для чтения и создания	Нет
icmp		
icmpInMsgs	только для чтения	Нет
icmpInErrors	только для чтения	Нет
icmpInDestUnreachs	только для чтения	Нет
icmpInTimeExcds	только для чтения	Нет
icmpInParmProbs	только для чтения	Нет
icmpInSrcQuenchs	только для чтения	Нет
icmpInRedirects	только для чтения	Нет
icmpInEchos	только для чтения	Нет
icmpInEchosReps	только для чтения	Нет
icmpInTimestamps	только для чтения	Нет
icmpInTimestampsReps	только для чтения	Нет
icmpInAddrMasks	только для чтения	Нет
icmpInAddrMaskReps	только для чтения	Нет
icmpOutMsgs	только для чтения	Нет
icmpOutErrors	только для чтения	Нет
icmpOutDestUnreachs	только для чтения	Нет
icmpOutTimeExcds	только для чтения	Нет
icmpOutParmProbs	только для чтения	Нет
icmpOutSrcQuenchs	только для чтения	Нет
icmpOutRedirects	только для чтения	Нет

icmpOutEchos	только для чтения	Нет
icmpOutEchosReps	только для чтения	Нет
icmpOutTimestamps	только для чтения	Нет
icmpOutTimestampReps	только для чтения	Нет
icmpOutAddrMasks	только для чтения	Нет
icmpOutAddrMaskReps	только для чтения	Нет
udp [RFC 2013]		
udpInDatagrams	только для чтения	Нет
udpNoPorts	только для чтения	Нет
udpInErrors	только для чтения	Нет
udpOutDatagrams	только для чтения	Нет
udpTable/udpEntry		
udpLocalAddress	только для чтения	Нет
udpLocalPort	только для чтения	Нет
передача [RFC draft-ietf-ipcdn-bpiplus-mib-06.txt]		
docsIfMib		
docsBpi2MIB		
docsBpi2MIBObjects		
docsBpi2CmObjects		
docsBpi2CmCertObjects		
docsBpi2CmDeviceCertTable/docsBpi2CmDeviceCertEntry		
docsBpi2CmDeviceCmCert	для чтения и записи	Да
docsBpi2CmDeviceManufCert	только для чтения	Да
docsBpi2CodeDownloadControl		
docsBpi2CodeDownloadStatusCode	только для чтения	Да
docsBpi2CodeDownloadStatusString	только для чтения	Да
docsBpi2CodeMfgOrgName	только для чтения	Да
docsBpi2CodeMfgCodeAccessStart	только для чтения	Да
docsBpi2CodeMfgCvcAccessStart	только для чтения	Да
docsBpi2CodeCoSignerOrgName	только для чтения	Да
docsBpi2CodeCoSignerCodeAccessStart	только для чтения	Да
docsBpi2CodeCoSignerCvcAccessStart	только для чтения	Да
docsBpi2CodeCvcUpdate	для чтения и записи	Да
snmp [RFC 1907]		
snmpInPkts	только для чтения	Нет
snmpOutPkts	только для чтения	Нет
snmpInBadVersions	только для чтения	Нет
snmpInBadCommunityNames	только для чтения	Нет
snmpInBadCommunityUses	только для чтения	Нет
snmpInASNParseErrs	только для чтения	Нет
snmpInTooBigs	только для чтения	Нет
snmpInNoSuchNames	только для чтения	Нет
snmpInBadValues	только для чтения	Нет
snmpInReadOnlys	только для чтения	Нет

snmpInGenErrs	только для чтения	Нет
snmpInTotalReqVars	только для чтения	Нет
snmpInTotalSetVars	только для чтения	Нет
snmpInGetRequests	только для чтения	Нет
snmpInGetNexts	только для чтения	Нет
snmpInSetRequests	только для чтения	Нет
snmpInGetResponses	только для чтения	Нет
snmpInTraps	только для чтения	Нет
snmpOutTooBigs	только для чтения	Нет
snmpOutNoSuchNames	только для чтения	Нет
snmpOutBadValues	только для чтения	Нет
snmpOutGenErrs	только для чтения	Нет
snmpOutGetRequests	только для чтения	Нет
snmpOutGetNexts	только для чтения	Нет
snmpOutSetRequests	только для чтения	Нет
snmpOutGetResponses	только для чтения	Нет
snmpOutTraps	только для чтения	Нет
snmpEnableAuthenTraps	для чтения и записи	Нет
snmpSilentDrops	только для чтения	Нет
snmpProxyDrops	только для чтения	Нет
ifMIB [RFC 2863]		
ifMIBOjects		
ifXTable/ifXEntry		
ifName	только для чтения	Нет
ifInMulticastPkts	только для чтения	Нет
ifInBroadcastPkts	только для чтения	Нет
ifOutMulticastPkts	только для чтения	Нет
ifOutBroadcastPkts	только для чтения	Нет
ifHCInOctets	только для чтения	Нет
ifHCInUcastPkts	только для чтения	Нет
ifHCInMulticastPkts	только для чтения	Нет
ifHCInBroadcastPkts	только для чтения	Нет
ifHCOutOctets	только для чтения	Нет
ifHCOutUcastPkts	только для чтения	Нет
ifHCOutMulticastPkts	только для чтения	Нет
ifHCOutBroadcastPkts	только для чтения	Нет
ifLinkUpDownTrapEnable	для чтения и записи	Нет
ifHighSpeed	только для чтения	Нет
ifPromiscuousMode	для чтения и записи	Нет
ifConnectorPresent	только для чтения	Нет
ifAlias	для чтения и записи	Нет
ifCounterDiscontinuitityTime	только для чтения	Нет
docsDev [RFC 2669]		
docsDevMIBObjects		

docsDevNmAccessTable/docsDevNmAccessEntry		
docsDevNmAccessIndex	Не является доступным	Нет
docsDevNmAccessIp	для чтения и создания	Нет
docsDevNmAccessIpMask	для чтения и создания	Нет
docsDevNmAccessCommunity	для чтения и создания	Нет
docsDevNmAccessControl	для чтения и создания	Нет
docsDevNmAccessInterfaces	для чтения и создания	Нет
docsDevNmAccessStatus	для чтения и создания	Нет
docsDevSoftware		
docsDevSwServer	для чтения и записи	Да
docsDevSwFilename	для чтения и записи	Да
docsDevSwAdminStatus	для чтения и записи	Да
docsDevSwOperStatus	только для чтения	Да
docsDevSwCurrentVers	только для чтения	Да
docsDevEvent		
docsDevEvControl	для чтения и записи	Нет
docsDevEvSyslog	для чтения и записи	Нет
docsDevEvThrottleAdminStatus	для чтения и записи	Нет
docsDevEvThrottleInhibited	только для чтения	Нет
docsDevEvThrottleThreshold	для чтения и записи	Нет
docsDevEvThrottleInterval	для чтения и записи	Нет
docsDevEvControlTable/docsDevEvControlEntry		
docsDevEvPriority	не является доступным	Нет
docsDevEvReporting	для чтения и записи	Нет
docsDevEventTable/docsDevEventEntry		
docsDevEvIndex	не является доступным	Да
docsDevEvFirstTime	только для чтения	Да
docsDevEvLastTime	только для чтения	Да
docsDevEvCounts	только для чтения	Да
docsDevEvLevel	только для чтения	Да
docsDevEvId	только для чтения	Да
docsDevEvText	только для чтения	Да
закрытые		
предметные области		
cableLabs		
clabProject		
clabProjCableHome		
cabhPsDevMib		
cabhPsDevBase		
cabhPsDevDateTime	для чтения и записи	Нет
cabhPsDevResetNow	для чтения и записи	Нет

cabhPsDevSerialNumber	только для чтения	Да
cabhPsDevHardwareVersion	только для чтения	Да
cabhPsdevMacAddress	только для чтения	Да
cabhPsDevTypeIdentifier	только для чтения	Да
cabhPsDevResetDefaults	для чтения и записи	Нет
cabhPsDevWanManClientId	для чтения и записи	Да
cabhPsDevTodSyncStatus	только для чтения	Нет
cabhPsDevProvMode	только для чтения	Нет
cabhPsDevDwnldMode	только для чтения	Нет
cabhPsDevProv		
cabhPsDevProvisioningTimer	для чтения и записи	Да
cabhPsDevProvConfigFile	для чтения и записи	Нет
cabhPsDevProvConfigHash	для чтения и записи	Нет
cabhPsDevProvConfigFileSize	только для чтения	Нет
cabhPsDevProvConfigTLVProcessed	только для чтения	Нет
cabhPsDevProvConfigTLVRejected	только для чтения	Нет
cabhPsDevProvSolicitedKeyTimeout	для чтения и записи	Да
cabhPsDevProvState	только для чтения	Нет
cabhPsDevProvAuthState	только для чтения	Нет
cabhPsDevProvCorrelationId	только для чтения	Нет
cabhPsDevServerType	только для чтения	Нет
cabhPsDevServerTime	только для чтения	Нет
cabhSecMib		
cabhSecFwObjects		
cabhSecFwBase		
cabhSecFwPolicyFileEnable	для чтения и записи	Да
cabhSecFwPolicyFileURL	для чтения и записи	Нет
cabhSecFwPolicyFileHash	для чтения и записи	Нет
cabhSecFwPolicyFileOperStatus	только для чтения	Нет
cabhSecFwPolicyFileCurrentVersion	для чтения и записи	Да
cabhSecFwLogCtl		
cabhSecFwEventType1Enable	для чтения и записи	Да
cabhSecFwEventType2Enable	для чтения и записи	Да
cabhSecFwEventType3Enable	для чтения и записи	Да
cabhSecFwEventAttachAlertThreshold	для чтения и записи	Да
cabhSecFwEventAttackAlertPeriod	для чтения и записи	Да
cabhCapMib		
cabhCapObjects		
cabhCapBase		
cabhCapTcpTimeWait	для чтения и записи	Да
cabhCapUdpTimeWait	для чтения и записи	Да
cabhCapIcmpTimeWait	для чтения и записи	Да
cabhCapPrimaryMode	для чтения и записи	Да
cabhCapSetToFactory	для чтения и записи	Нет

cabhCapMap		
cabhCapMappingTable/cabhCapMappingEntry		
cabhCapMappingWanAddrType	не является доступным	Да[1]
cabhCapMappingWanAddrType	не является доступным	Да[1]
cabhCapMappingWanPort	не является доступным	Да[1]
cabhCapMappingLanAddrType	не является доступным	Да[1]
cabhCapMappingLanAddrType	не является доступным	Да[1]
cabhCapMappingLanPort	не является доступным	Да[1]
cabhCapMappingMode	только для чтения	Да[1]
cabhCapMappingMethod	только для чтения	Да[1]
cabhCapMappingProtocol	только для чтения	Да[1]
cabhCapPassthroughTable/cabhCapPassthroughEntry		
cabhCapPassthroughMACAddr	не является доступным	Да
cabhCapPassthroughRowStatus	для чтения и создания	Нет
cabhCdpMib		
cabhCdpObjects		
cabhCdpBase		
cabhCdpSetToFactory	для чтения и записи	Нет
cabhCdpLanTransCurCount	только для чтения	Да
cabhCdpLanTransThreshold	для чтения и записи	Да
cabhCdpLanTransAction	для чтения и записи	Да
cabhCdpAddr		
cabhCdpLanAddrTable/cabhCdpLanAddrEntry		
cabhCdpLanAddrIpType	не является доступным	Да
cabhCdpLanAddrIp	не является доступным	Да
cabhCdpLanAddrClientID	только для чтения	Да
cabhCdpLanAddrCreateTime	только для чтения	Да
cabhCdpLanAddrExpireTime	только для чтения	Да
cabhCdpLanAddrMethod	только для чтения	Да
cabhCdpLanAddrHostName	только для чтения	Да
cabhCdpLanAddrRowStatus	для чтения и создания	Нет
cabhCdpWanDataAddrTable/cabhCdpWanDataAddrEntry		
cabhCdpWanDataAddrIndex	не является доступным	Да

---

[1] Объекты cabhCapMappingEntry являются постоянными, если они обеспечены с помощью NMS, и непостоянными, если созданы динамически на основе исходящего трафика. Ссылка на 8.3.2.2.

cabhCdpWanDataAddrClientId	для чтения и создания	Да
cabhCdpWanDataAddrIpType	для чтения и создания	Нет
cabhCdpWanDataAddrIp	для чтения и создания	Нет
cabhCdpWanDataAddrAddrRenewalTime	для чтения и создания	Нет
cabhCdpWanDataAddrRowStatus	для чтения и создания	Нет
cabhCdpWanDataAddrServerTable/cabhCdpWanDataAddrServerEntry		
cabhCdpWanDataAddrDnsIpType	не является доступным	Нет
cabhCdpWanDataAddrDnsIp	не является доступным	Нет
cabhCdpWanDataAddrDnsRowStatus	для чтения и создания	Нет
cabhCdpServer		
cabhCdpLanPoolStartType	для чтения и записи	Да
cabhCdpLanPoolStart	для чтения и записи	Да
cabhCdpLanPoolEndType	для чтения и записи	Да
cabhCdpLanPoolEnd	для чтения и записи	Да
cabhCdpServerSubnetMaskType	для чтения и записи	Да
cabhCdpServerSubnetMask	для чтения и записи	Да
cabhCdpServerTimeOffset	для чтения и записи	Да
cabhCdpServerRouterType	для чтения и записи	Да
cabhCdpServerRouter	для чтения и записи	Да
cabhCdpServerDnsAddressType	для чтения и записи	Да
cabhCdpServerDnsAddress	для чтения и записи	Да
cabhCdpServerSyslogAddressType	для чтения и записи	Да
cabhCdpServerSyslogAddress	для чтения и записи	Да
cabhCdpServerDomainName	для чтения и записи	Да
cabhCdpServerTTL	для чтения и записи	Да
cabhCdpServerInterfaceMTU	для чтения и записи	Да
cabhCdpServerVendorSpecific	для чтения и записи	Да
cabhCdpServerLeaseTime	для чтения и записи	Да
cabhCdpServerDhcpAddressType	для чтения и записи	Да
cabhCdpServerDhcpAddress	для чтения и записи	Да
cabhCtpMib		
cabhCtpObjects		
cabhCtpBase		
cabhCtpReset	для чтения и записи	Нет
cabpCtpConnSpeed		
cabhCtpConnSrcIpType	для чтения и записи	Нет
cabhCtpConnSrcIp	для чтения и записи	Нет
cabhCtpConnDestIpType	для чтения и записи	Нет
cabhCtpConnDestIp	для чтения и записи	Нет
cabhCtpConnProto	для чтения и записи	Нет
cabhCtpConnPort	для чтения и записи	Нет
cabhCtpConnNumPkts	для чтения и записи	Нет

cabhCtpConnPktSize	для чтения и записи	Нет
cabhCtpConnTimeOut	для чтения и записи	Нет
cabhCtpConnControl	для чтения и записи	Нет
cabhCtpConnStatus	только для чтения	Нет
cabhCtpConnPktsSent	только для чтения	Нет
cabhCtpConnPktsRecv	только для чтения	Нет
cabhCtpConnAvgRTT	только для чтения	Нет
cabhCtpConnMaxRTT	только для чтения	Нет
cabhCtpConnMinRTT	только для чтения	Нет
cabhCtpConnNumIcmpError	только для чтения	Нет
cabhCtpConnIcmpError	только для чтения	Нет
cabhCtpPing		
cabhCtpPingSrcIpType	для чтения и записи	Нет
cabhCtpPingSrcIp	для чтения и записи	Нет
cabhCtpPingDestIpType	для чтения и записи	Нет
cabhCtpPingDestIp	для чтения и записи	Нет
cabhCtpPingProto	для чтения и записи	Нет
cabhCtpPingNumPkts	для чтения и записи	Нет
cabhCtpPingPktSize	для чтения и записи	Нет
cabhCtpPingTimeBetween	для чтения и записи	Нет
cabhCtpPingTimeOut	для чтения и записи	Нет
cabhCtpPingControl	для чтения и записи	Нет
cabhCtpPingStatus	только для чтения	Нет
cabhCtpPingNumSent	только для чтения	Нет
cabhCtpPingNumRecv	только для чтения	Нет
экспериментальное		
snmpUSMDHObjectsMIB [RFC 2786]		
usmDHKeyObjects		
usmDHPublicObjects		
usmDHPParameters	для чтения и записи	Нет
usmDHUserKeyTable/usmDHUserKeyEntry		
usmDHUserAuthKeyChange	для чтения и создания	Нет
usmDHUserOwnAuthKeyChange	для чтения и создания	Нет
usmDHUserPrivKeyChange	для чтения и создания	Нет
usmDHUserOwnPrivKeyChange	для чтения и создания	Нет
usmDHKickstartGroup		
usmDHKickstartTable/usmDHKickstartEntry		
usmDHKickstartIndex	не является доступным	Нет
usmDHKickstartMyPublic	только для чтения	Нет
usmDHKickstartMgrPublic	только для чтения	Нет
usmDHKickstartSecurityName	только для чтения	Нет
snmpV2		
snmpModules		

snmpMIB		
snmpMIBObjects		
snmpSet		
snmpSetSerialNo	для чтения и записи	Нет
snmpFrameworkMIB [RFC 2571]		
snmpEngine		
snmpEngineID	только для чтения	Да
snmpEngineBoots	только для чтения	Да
snmpEngineTime	только для чтения	Нет
snmpEngineMaxMessageSize	только для чтения	Да
snmpMPDMIB [RFC 2572]		
snmpMPDObjects		
snmpMPDStats		
snmpUnknownSecurityModels	только для чтения	Нет
snmpInvalidMsgs	только для чтения	Нет
snmpUnknownPDUHandlers	только для чтения	Нет
snmpTargetMIB [RFC 2573]		
snmpTargetObjects		
snmpTargetSpinLock	для чтения и записи	Нет
snmpTargetAddrTable/snmpTargetAddrEntry		
snmpTargetAddrName	не является доступным	Нет
snmpTargetAddrTDomain	для чтения и создания	Нет
snmpTargetAddrTAddress	для чтения и создания	Нет
snmpTargetAddrTimeout	для чтения и создания	Нет
snmpTargetAddrRetryCount	для чтения и создания	Нет
snmpTargetAddrTagList	для чтения и создания	Нет
snmpTargetAddrParams	для чтения и создания	Нет
snmpTargetAddrStorageType	для чтения и создания	Нет
snmpTargetAddrRowStatus	для чтения и создания	Нет
snmpTargetParamsTable/snmpTargetParamsEntry		
snmpTargetParamsName	не является доступным	Нет
snmpTargetParamsMPModel	для чтения и создания	Нет
snmpTargetParamsSecurityModel	для чтения и создания	Нет
snmpTargetParamsSecurityName	для чтения и создания	Нет
snmpTargetParamsSecurityLevel	для чтения и создания	Нет
snmpTargetParamsStorageType	для чтения и создания	Нет
snmpTargetParamsRowStatus	для чтения и создания	Нет
snmpUnavailableContexts	только для чтения	Нет
snmpUnknownContexts	только для чтения	Нет
snmpNotificationMIB [RFC 2573]		
snmpNotifyObjects		
snmpNotifyTable/snmpNotifyEntry		

snmpNotifyName	не является доступным	Нет
snmpNotifyTag	для чтения и создания	Нет
snmpNotifyType	для чтения и создания	Нет
snmpNotifyStorageType	для чтения и создания	Нет
snmpNotifyRowStatus	для чтения и создания	Нет
snmpNotifyFilterProfileTable/snmpNotifyFilterProfileEntry		
snmpNotifyFilterProfileName	для чтения и создания	Нет
snmpNotifyFilterProfileStorType	для чтения и создания	Нет
snmpNotifyFilterProfileRowStatus	для чтения и создания	Нет
snmpNotifyFilterTable/snmpNotifyFilterEntry		
snmpNotifyFilterSubtree	не является доступным	Нет
snmpNotifyFilterMask	для чтения и создания	Нет
snmpNotifyFilterType	для чтения и создания	Нет
snmpNotifyFilterStorageType	для чтения и создания	Нет
snmpNotifyFilterRowStatus	для чтения и создания	Нет
snmpUsmMIB [RFC 2574]		
usmStats		
usmStatsUnsupportedSecLevels	только для чтения	Нет
usmStatsNotInTimeWindows	только для чтения	Нет
usmStatsUnknownUserNames	только для чтения	Нет
usmStatsUnknownEngineIDs	только для чтения	Нет
usmStatsWrongDigests	только для чтения	Нет
usmStatsDecryptionErrors	только для чтения	Нет
usmUser		
usmUserSpinLock	для чтения и записи	Нет
usmUserTable/usmUserEntry		
usmUserEngineID	не является доступным	Нет
usmUserName	не является доступным	Нет
usmUserSecurityName	только для чтения	Нет
usmUserCloneFrom	для чтения и создания	Нет
usmUserAuthProtocol	для чтения и создания	Нет
usmUserAuthKeyChange	для чтения и создания	Нет
usmUserOwnAuthKeyChange	для чтения и создания	Нет
usmUserPrivProtocol	для чтения и создания	Нет
usmUserPrivKeyChange	для чтения и создания	Нет
usmUserOwnPrivKeyChange	для чтения и создания	Нет
usmUserPublic	для чтения и создания	Нет
usmUserStorageType	для чтения и создания	Нет
usmUserStatus	для чтения и создания	Нет
SNMP-VIEW-BASED-ACM-MIB [RFC 2575]		

snmpVacmMIB		
vacmMIBObjects		
vacmContextTable/vacmContextEntry		
vacmContextName	только для чтения	Нет
vacmSecurityToGroupTable/vacmSecurityToGroupEntry		
vacmSecurityModel	не является доступным	Нет
vacmSecurityName	не является доступным	Нет
vacmGroupName	для чтения и создания	Нет
vacmSecurityToGroupStorageType	для чтения и создания	Нет
vacmSecurityToGroupStatus	для чтения и создания	Нет
vacmAccessTable/vacmAccessEntry		
vacmAccessContextPrefix	не является доступным	Нет
vacmAccessSecurityModel	не является доступным	Нет
vacmAccessSecurityLevel	не является доступным	Нет
vacmAccessContextMatch	для чтения и создания	Нет
vacmAccessReadViewName	для чтения и создания	Нет
vacmAccessWriteViewName	для чтения и создания	Нет
vacmAccessNotifyViewName	для чтения и создания	Нет
vacmAccessStorageType	для чтения и создания	Нет
vacmAccessStatus	для чтения и создания	Нет
vacmMIBViews		
vacmViewSpinLock	для чтения и записи	Нет
vacmViewTreeFamilyTable/vacmViewTreeFamilyEntry		
vacmViewTreeFamilyViewName	не является доступным	Нет
vacmViewTreeFamilySubtree	не является доступным	Нет
vacmViewTreeFamilyMask	для чтения и создания	Нет
vacmViewTreeFamilyType	для чтения и создания	Нет
vacmViewTreeFamilyStorageType	для чтения и создания	Нет
vacmViewTreeFamilyStatus	для чтения и создания	Нет
snmpCommunityMIB [RFC 2576]		
snmpCommunityMIBObjects		
snmpCommunityTable/snmpCommunityEntry		
snmpCommunityIndex	не является доступным	Нет
snmpCommunityName	для чтения и создания	Нет
snmpCommunitySecurityName	для чтения и создания	Нет
snmpCommunityContextEngineID	для чтения и создания	Нет
snmpCommunityContextName	для чтения и создания	Нет

snmpCommunityTransportTag	для чтения и создания	Нет
snmpCommunityStorageType	для чтения и создания	Нет
snmpCommunityStatus	для чтения и создания	Нет
snmpTargetAddrExtTable/snmpTargetAddrExtEntry		
snmpTargetAddrTMask	для чтения и создания	Нет
snmpTargetAddrMMS	для чтения и создания	Нет
snmpTrapAddress	доступен для уведомления	Нет
snmpTrapCommunity	доступен для уведомления	Нет

Дополнение B

Дополнение B – Формат и содержание для события, SYSLOG и захватов SNMP

Таблица B.1 обобщает формат и содержание для записи событий местной регистрации, сообщений syslog и захватов SNMP.

Каждый ряд в Таблице B.1 указывает событие, которое услуга PS должна быть способна порождать. Об этих событиях сообщают с помощью услуги PS одним или всеми из трех средств: регистрация местного события, как осуществляется с помощью таблицы местного события в документе [RFC 2669], SYSLOG и захват SNMP. Формат SYSLOG указывается в 6.5.1.3, а формат захвата SNMP определяется в этом дополнении, следуя Таблице B.1.

Первая и вторая колонки указывают, в какой стадии случается событие. Третья колонка указывает приоритет, назначенный событию. Эти приоритеты являются теми же самыми, как сообщается в объекте docsDevEvLevel в документе [RFC 2669] и в поле LEVEL [*уровень*] сообщения syslog.

Четвертая колонка указывает текст события, о котором сообщается в объекте docsDevEvText документа [RFC 2669], и текст поля сообщения syslog. Пятая колонка предоставляет дополнительную информацию о тексте события 4-й колонки. Например, некоторые поля текстов событий являются постоянными величинами (константами), а некоторые поля текстов событий включают в себя информацию переменной величины. Некоторые из переменных величин требуются только в SYSLOG, как описывается в пятой колонке. Шестая колонка указывает набор кода ошибки.

Седьмая колонка указывает уникальный номер идентификации для события, которое назначено объекту docsDevEvId и полю <eventId> сообщения syslog. Восьмая колонка указывает захват SNMP, который уведомляет об этом событии приемник события SNMP.

Правила для порождения уникальным образом идентификатора ID события из кода ошибки описываются в 6.5.1.3. Идентификаторы ID событий в Таблице B.1 даются в десятичном формате.

Чтобы лучше проиллюстрировать Таблицу B.1, далее дается пример, используя первый ряд в секции событий "Обновление программного обеспечения".

Первая и вторая колонки представляют собой "SW Upgrade" [*Обновление программного обеспечения*] (SW)" и "SOFTWARE UPGRADE INIT" [*модуль обновления программного обеспечения*]. Приоритет события есть "Notice" [*извещение*]. Текст события есть "Software Download INIT – Via NMS" [*начать загрузку программного обеспечения – через NMS*]. Пятая

колонка читается "For SYSLOG only, append: MAC addr [*Только для SYSLOG, добавить*]: <P1> P1 = PS Mac Address" [*адрес MAC PS*]. Это замечание относительно SYSLOG. То есть, основной материал текста syslog будет иметь вид "Software Download INIT – Via NMS – MAC addr: x1 x2 x3 x4 x5 x6".

Последняя колонка "Имя захвата" есть cabhPsDevSwUpgradeInitTrap, формат для которой дается в конце этого дополнения.

Таблица B.1/J.191 – Определенные события

Процесс	Под-процесс	Приоритет PS	Текст события	Примечания и детали сообщения	Набор кода ошибки	ID события	Имя захвата
Ошибки DHCP перед завершением обеспечения							
Начать	DHCP	Критичес-кий	Неудача DHCP – Послано сообщение Discover, но предложение не получено		D01.0	68000100	
Начать	DHCP	Критичес-кий	Неудача DHCP – Послан запрос, Нет отклика		D02.0	68000200	
Начать	DHCP	Критичес-кий	Неудача DHCP – Запрошенное Info не поддержано.		D03.0	68000300	
Начать	DHCP	Критичес-кий	Неудача DHCP – Отклик не содержит ВСЕ действительные поля, как описано в этой Рекомендации		D03.1	68000301	
Ошибки TOD перед завершением обеспечения							
Начать	TOD	Предупреж-дение	Послан запрос TOD – Отклик не получен		D04.1	68000401	
Начать	TOD	Предупреж-дение	Отклик TOD получен – Недействительный формат данных		D04.2	68000402	
Ошибки TFTP перед завершением обеспечения							

Таблица B.1/J.191 – Определенные события

Процесс	Под-процесс	Приоритет PS	Текст события	Примечания и детали сообщения	Набор кода ошибки	ID события	Имя захвата
Начать	TFTP	Критический	Неудача TFTP – Послан запрос – Нет отклика		D05.0	68000500	
Начать	TFTP	Критический	Неудача TFTP – Файл конфигурации НЕ НАЙДЕН	Только для SYSLOG, добавить: Имя файла = <P1> P1 = имя запрашиваемого файла	D06.0	68000600	
Начать	TFTP	Критический	Неудача TFTP – Пакеты В НЕИСПРАВНОСТИ		D07.0	68000700	
Начать	TFTP	Критический	Файл TFTP завершен – но потерпела неудачу MIC проверка Целостности сообщения	Только для SYSLOG, добавить: Имя файла = <P1> P1 = имя файла для файла TFTP	D08.0	68000800	
Начать	TFTP	Критический	Неудача TFTP – Превышено максимальное число повторных попыток	Только для SYSLOG, добавить: Предел повторных попыток = <P1> P1 = максимальное число повторных попыток	D09.0	68000900	
Успех TFTP							
Начать	TFTP	Извещение	Успех TFTP		D10.0	68001000	
Структурный анализ TLV							
Начать	Структурный анализ TLV	Извещение	TLV-28 – Неопознанный OID		I401.0	73040100	cabhPsDevInitTLVUnknownTrap
Начать	Структурный анализ TLV	Извещение	Неизвестное TLV <P1>	Только для SYSLOG: <P1> = завершение TLV в 16-ричном формате	I401.1	73040101	cabhPsDevInitTLVUnknownTrap
Начать	Структурный анализ TLV	Извещение	Недействительный формат/содержимое TLV <P1>	Только для SYSLOG: <P1> = завершение TLV в 16-ричном формате	I401.2	73040102	
Обеспечение							
Начать	SNMP Inform	Извещение	Послано SNMP, сигнализирующее, что обеспечение завершено (проходит/неудача)	Только для SYSLOG, добавить: MAC Addr: <P1>. P1 = адрес MAC PS	I11.0	73001100	cabhPsDevInitTrap
Начать	Переприем SNMP Inform	Критическое	Послано Inform SNMP, сигнализирующее, что обеспечение завершено (проходит/неудача), но нет отклика. Послано повторно Inform SNMP	Только для SYSLOG, добавить: MAC Addr: <P1>. P1 = адрес MAC PS	I11.1	73001101	cabhPsDevInitRetryTrap
Начать обновление программного обеспечения (SW)							

Таблица B.1/J.191 – Определенные события

Процесс	Под-процесс	Приоритет PS	Текст события	Примечания и детали сообщения	Набор кода ошибки	ID события	Имя захвата
Обновление программного обеспечения (SW)	Начало обновления программного обеспечения (SW)	Извещение	Начало загрузки (INIT) программного обеспечения (SW) – Через NMS	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 =адрес IP сервера TFTP	E101.0	69010100	cabhPsDev SwUpgrade InitTrap
Обновление программного обеспечения (SW)	Обновление программного обеспечения (SW)	Извещение	Начало загрузки (INIT) программного обеспечения (SW) – Через файл Config <P1>	P1 = имя файла config CM только для SYSLOG, добавить: файл SW: <P2> – сервер SW: < P3>. P2 = имя файла SW и P3 = адрес IP сервера TFTP	E102.0	69010200	cabhPsDev SwUpgrade InitTrap
Общая неудача обновления программного обеспечения (SW)							
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Обновление SW потерпело неудачу во время загрузки – Максимум повторных попыток превышен (3)	Только для SYSLOG, добавить: файл SW <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E103.0	69010300	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Обновление программного обеспечения (SW) потерпело неудачу перед загрузкой – Сервер не присутствует	Только для SYSLOG, добавить: файл SW <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E104.0	69010400	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Обновление SW потерпело неудачу перед загрузкой – Файл не присутствует	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E105.0	69010500	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Обновление SW потерпело неудачу перед загрузкой – Превышено число повторных попыток TFTP	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E106.0	69010600	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Обновление SW потерпело неудачу перед загрузкой – Несовместимый файл SW	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E107.0	69010700	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Обновление SW потерпело неудачу после загрузки – Искажение файла SW	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E108.0	69010800	cabhPsDev SwUpgrade FailTrap

Таблица B.1/J.191 – Определенные события

Процесс	Под-процесс	Приоритет PS	Текст события	Примечания и детали сообщения	Набор кода ошибки	ID события	Имя захвата
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Прерывание во время загрузки SW – Отказ питания	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E109.0	69010900	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Прерывание во время загрузки SW – RF удалено	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E110.0	69011000	cabhPsDev SwUpgrade FailTrap
Успех обновления SW							
Обновление программного обеспечения (SW)	Успех обновления SW	Извещение	Загрузка SW успешна – Через NMS	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW и P2 = адрес IP сервера TFTP	E111.0	69011100	cabhPsDev SwUpgrade SuccessTrap
Обновление программного обеспечения (SW)	Успех обновления SW	Извещение	Загрузка SW успешна – Через файл Config	Только для SYSLOG, добавить: файл SW: <P1> – сервер SW: <P2>. P1 = имя файла SW иP2 = адрес IP сервера TFTP	E112.0	69011200	cabhPsDev SwUpgrade SuccessTrap
Неудача DHCP после завершения обеспечения					D100.0	68010000	
DHCP		Ошибка	Послано DHCP RENEW – Нет отклика		D101.0	68010100	cabhPsDev DHCPFailTrap
DHCP		Ошибка	Послано DHCP REBIND – Нет отклика		D102.0	68010200	cabhPsDev DHCPFailTrap
DHCP		Ошибка	Послано DHCP RENEW – Недействительный вариант DHCP		D103.0	68010300	cabhPsDev DHCPFailTrap
DHCP		Ошибка	Послано DHCP REBIND – недействительный вариант DHCP		D104.0	68010400	cabhPsDev DHCPFailTrap
Неудача TOD после завершения обеспечения							
TOD	TOD	Предупреж-дение	Послан запрос TOD – Отклик не получен		D04.3	68000403	cabhPsDev TODFailTrap
TOD	TOD	Предупреж-дение	Отклик TOD получен – Недействительный формат данных		D04.4	68000404	cabhPsDev TODFailTrap

Таблица B.1/J.191 – Определенные события

Процесс	Под-процесс	Приоритет PS	Текст события	Примечания и детали сообщения	Набор кода ошибки	ID события	Имя захвата
Проверка файла кода					E200		
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Несоответствующие директивы файла кода	Только для SYSLOG , добавить: Файл кода: <P1> – Сервер файла кода : <P2>. P1 = Имя файла кода, P2 = адрес IP сервера файла кода	E201.0	69020100	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Неудача проверки достоверности CVC производителя файла кода	Только для SYSLOG , добавить: Файл кода : <P1> – Сервер файла кода : <P2>. P1 = Имя файла кода, P2 = адрес IP сервера файла кода	E202.0	69020200	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Неудача проверки достоверности CVS производителя файла кода	Только для SYSLOG , добавить: Файл кода : <P1> – Сервер файла кода : <P2>. P1 = Имя файла кода, P2 = адрес IP сервера файла кода	E203.0	69020300	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Неудача проверки CVC стороны, совместно подписавшей файл кода	Только для SYSLOG , добавить: Файл кода : <P1> – Сервер файла кода : <P2>. P1 = Имя файла кода, P2 = адрес IP сервера файла кода	E204.0	69020400	cabhPsDev SwUpgrade FailTrap
Обновление программного обеспечения (SW)	Общая неудача обновления программного обеспечения (SW)	Ошибка	Неудача проверки CVS стороны, совместно подписавшей файл кода	Только для SYSLOG , добавить: Файл кода : <P1> – Сервер файла кода : <P2>. P1 = Имя файла кода, P2 = адрес IP сервера файла кода	E205.0	69020500	cabhPsDev SwUpgrade FailTrap
Проверка CVC							
Обновление программного обеспечения (SW)	Проверка CVC	Ошибка	Несоответствующий формат CVC файла конфигурации – Сервер TFTP: <P1> – Файл Config: <P2>	P1 = P2 адреса IP сервера TFTP = Имя файла Config	E206.0	69020600	cabhPsDev SwUpgrade CVCFailTrap
Обновление программного обеспечения (SW)	Проверка CVC	Ошибка	Неудача проверки достоверности CVC файла конфигурации – Сервер TFTP: <P1> – Файл Config: <P2>	P1 = P2 адреса IP сервера TFTP = Имя файла Config	E207.0	69020700	cabhPsDev SwUpgrade CVCFailTrap
Обновление программного обеспечения (SW)	Проверка CVC	Ошибка	Несоответствующий формат CVC SNMP – Управляющая программа SNMP: <P1>	P1 = Адрес IP управляющей программы SNMP	E208.0	69020800	cabhPsDev SwUpgrade CVCFailTrap

Таблица B.1/J.191 – Определенные события

Процесс	Под-процесс	Приоритет PS	Текст события	Примечания и детали сообщения	Набор кода ошибки	ID события	Имя захвата
Обновление програм-много обеспечения (SW)	Проверка CVC	Ошибка	Неудача проверки достоверности CVC SNMP – Управляю-щая программа SNMP: <P1>	P1 = Адрес IP управляющей программы SNMP	E209.0	69020900	cabhPsDev SwUpgrade CVCFailTrap
События CDP					P		
CDP	CDS	Извещение	Попытка распределить больше адресов IP, LAN TRANS, чем разрешено		P01.0	80000100	cabhPsDev CDPTrap
События CSP							
CSP	Средства межсетевой защиты (FW)	Извещение	Порог Типа 1 и Типа 2 межсетевой защиты и порог хакера Типа 2 превышены		P101.0	80010100	cabhPsDev CSPTrap
CSP	Средства межсетевой защиты (FW)	Извещение	Обнаружено событие Типа 1 средств межсетевой защиты (FW)	P1 = Адрес IP источника, P2 = адрес IP пункта назначения , P3 = тип протокола , P4 = имя файла набора активных правил, P5 = описание события	P102.0	80010200	cabhPsDev CSPTrap
CSP	Средства межсетевой защиты (FW)	Извещение	Обнаружено событие Типа 2 средств межсетевой защиты (FW)	P1 = Адрес IP источника, P2 = адрес IP пункта назначения , P3 = тип протокола , P4 = имя файла набора активных правил, P5 = описание события	P103.0	80010300	cabhPsDev CSPTrap
CSP	Средства межсетевой защиты (FW)	Извещение	Конфигурация средств межсетевой защиты изменилась	P1 = описание изменения в параметрах конфигурации средств межсетевой защиты	P120.0	80012000	cabhPsDev CSPTrap
События CAP							
CAP	C-NAT	Извещение	Портал CAP не способен осуществить преобразование C-NAT. Нет адреса IP WAN-data		P201.0	800201.00	cabhPsDev CAPTrap
CAP	C-NAPT	Извещение	Портал CAP не способен осуществить преобразование C-NAPT. Нет адреса IP WAN-data		P250.0	800250.00	cabhPsDev CAPTrap

B.1 Описания захватов

```
cabhPsDevInitTLVUnknownTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      СТАТУС текущий
      ОПИСАНИЕ
            "Событие из-за обнаружения неизвестного значения TLV во время
            процесса структурного анализа TLV. Значения docsDevEvLevel, docsDevId
            и DocsDevEvText взяты из записи, которая регистрирует это событие в
            объекте docsDevEventTable. Значение ifPhysAddress является адресом
            MAC услуги PS. Эта часть информации сделана однообразной по всем
            захватам PS."
      := { cabhPsDevTraps 1 }

cabhPsDevInitTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevServerConfigFile,
                  количество значений TLV,
                  количество опущенных значений TLV }
      СТАТУС текущий
      ОПИСАНИЕ
            "События, чтобы сообщить, что процесс установления в начальное
            состояние завершен, как обнаружено в услуге PS. Значения
            docsDevEvLevel, docsDevId и docsDevEvText берутся из записи, которая
            регистрирует это событие в объекте docsDevEventTable. Значение
            ifPhysAddress указывает адрес MAC услуги PS.
            DocsDevServerConfigFile является именем используемого файла
            конфигурации. Также как число значений TLV в файле config и число
            опущенных значений TLV. Если файл конфигурации не был использован,
            установить все три значения в 'никакое'.
            Эта часть информации сделана однообразной по всем захватам PS."
      ::= { cabhPsDevTraps 2 }

cabhPsDevInitRetryTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      СТАТУС текущий
      ОПИСАНИЕ
            "Во время процесса установления в начальное состояние случилось и
            обнаружено в услуге PS событие, о котором надо сообщить. Значения
            docsDevEvLevel, docsDevId и docsDevEvText берутся из записи, которая
            регистрирует это событие в объекте docsDevEventTable. Значение
            ifPhysAddress указывает адрес MAC услуги PS.
            Эта часть информации сделана однообразной по всем захватам PS."
      ::= { cabhPsDevTraps 3 }
cabhPsDevDHCPFailTrap ТИП УВЕДОМЛЕНИЯ

      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevServerDhcp }
      СТАТУС текущий
      ОПИСАНИЕ
            "Событие, чтобы сообщить о неудаче сервера DHCP. Значение
            docsDevServerDhcp есть адрес IP сервера DHCP."
```

```
      ::= { cabhPsDevTraps 4 }

cabhPsDevSwUpgradeInitTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      СТАТУС текущий
      ОПИСАНИЕ
            "Событие, чтобы сообщить о событии, инициированном обновлением
            программного обеспечения. Значения docsDevSwFilename и
            docsDevSwServer указывают название изображения программного
            обеспечения и адрес IP сервера, из которого взято изображение."
      ::= { cabhPsDevTraps 5 }

cabhPsDevSwUpgradeFailTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      СТАТУС текущий
      ОПИСАНИЕ
            "Событие, чтобы сообщить о неудаче попытки обновления программного
            обеспечения. Значения docsDevSwFilename и docsDevSwServer указывают
            название изображения программного обеспечения и адрес IP сервера, из
            которого взято изображение."
      ::= { cabhPsDevTraps 6 }

cabhPsDevSwUpgradeSuccessTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      СТАТУС текущий
      ОПИСАНИЕ
            "Событие, чтобы сообщить о событии обновления программного
            обеспечения. Значения docsDevSwFilename и docsDevSwServer указывают
            название изображения программного обеспечения и адрес IP сервера, из
            которого взято изображение."
      ::= { cabhPsDevTraps 7 }

cabhPsDevSwUpgradeCVCFailTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      СТАТУС текущий
      ОПИСАНИЕ
            "Событие, чтобы сообщить о неудаче проверки файла кода, которая
            случилась во время попытки безопасного обновления программного
            обеспечения."
      ::= { cabhPsDevTraps 8 }

cabhPsDevTODFailTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
```

```
                  docsDevServerTime }
      СТАТУС текущий
      ОПИСАНИЕ
            "Событие, чтобы сообщить о неудаче сервера Времени дня. Значение
            docsDevServerTime указывает адрес IP сервера."
      ::= { cabhPsDevTraps 9 }

cabhPsDevCDPTrap ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  addressThreshold }
      СТАТУС текущий
      ОПИСАНИЕ
            "Сообщить о событии с помощью Портала DHCP."
      ::= { cabhPsDevTraps 10 }

cabhPsDevCSPTrap   ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      СТАТУС текущий
      ОПИСАНИЕ
            "Сообщить о событии с помощью портала безопасности."
      ::= { cabhPsDevTraps 11 }

cabhPsDevCAPTrap   ТИП УВЕДОМЛЕНИЯ
      ОБЪЕКТЫ { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      СТАТУС текущий
      ОПИСАНИЕ
            "Сообщить о событии с помощью портала безопасности."
      ::= { cabhPsDevTraps 12 }
```

Дополнение C

Угрозы безопасности и предупредительные меры

При развитии технологии безопасности важно понимать, какими являются первичные угрозы для данного приложения или окружающей среды. Эта информация затем может быть использована для выбора наиболее эффективных инструментов безопасности и технологий для защиты и предотвращения злонамеренных атак.

Были определены следующие первичные угрозы безопасности абонентам и операторам:

– **Кража услуги**: Кража услуги происходит в двух формах: несанкционированный доступ к кабельным услугам и несанкционированное копирование содержимого услуги.

  Несанкционированный доступ включает в себя абонента или 3-ю сторону (такую, как сосед), имеющих доступ к кабельным услугам, за которые они не заплатили. Устройства могли быть "клонированы" или изменены, чтобы появиться в качестве пригодного устройства в доме абонента. Это могло бы также ухудшить показатели качества доставки услуги, поскольку эти устройства потребляют дополнительные транспортные ресурсы на звеньях HFC и домов.

Несанкционированное копирование обычно включает в себя абонента или 3-ю сторону (такую, как сосед), которые снимают незаконные копии содержимого услуги. В некоторых случаях эти копии распространяются другим потребителям без одобрения оператора или поставщика содержимого (контента).

– **Атаки по отрицанию обслуживания (*DOS, Denial of Service*)**: Атаки по отрицанию обслуживания могут иметь место, когда объект 3-й стороны (атакующий объект, раздраженный клиент и пр.) нарушает нормальную связь и доставку услуг между оператором и его абонентами. Эти негодные передачи данных, приходящие от устройства/источника, который появляется как действительный, могли бы быть введены в домашнее звено и существенно ухудшить его нормальные функции. Эти негодные передачи данных могли бы также простираться до сети HFC оператора, вызывая там проблемы показателей качества.

– **Конфиденциальность обслуживания**: Конфиденциальность обслуживания включает в себя 3-ю сторону (соседи, атакующие объекты и пр.), наблюдающую/принимающую информацию относительно абонентов и услуг, которые она использует. Это могло бы приводить к осуществлению кражи информации паролей или конфигурации устройств, разрешая атакующим объектам получать в дальнейшем доступ к сетевым ресурсам абонентов и конфиденциальным файлам /данным.

Имеется ряд различных методов, которые могут быть использованы для предотвращения угроз безопасности, упомянутых выше. К сожалению, один метод не может предотвратить все угрозы, но сочетание их могло бы быть лучшей линией обороны. Можно использовать следующие предупредительные меры:

– **Удостоверение подлинности**: Удостоверение подлинности включает в себя проверку того, что отправляющий и посылающий объекты являются теми, какие требуются. Это включает в себя источник услуги, приемное устройство и абонента.

  Удостоверение подлинности помогает предотвратить кражу услуги путем проверки достоверности конечных устройств и пользователей, но оно не предотвращает от незаконного копирования содержимого, или не препятствует несанкционированному доступу 3-ми сторонами, которые наблюдают за звеном. Оно действительно делает хорошую работу в предотвращении атак DOS, поскольку трафик может быть отклонен, если он не приходит из действительного источника. Само по себе удостоверение подлинности не обеспечивает никакой поддержки конфиденциальности, для этого должно использоваться шифрование.

– **Защита от копирования**: Методы защиты от копирования ограничивают способность приемного устройства делать несанкционированные копии содержимого услуги.

  Защита от копирования предотвращает кражу услуги путем ограничения, сколько копий можно сделать, но она не предотвращает несанкционированный доступ к услугам. Она также не предотвращает DOS или защиту конфиденциальности обслуживания. В общем случае, эта предохранительная мера осуществляется на верхних прикладных уровнях.

– **Шифрование данных**: Шифрование данных предотвращает несанкционированное раскрытие данных/доступ данных.

  Шифрование данных делает превосходную работу в обеспечении конфиденциальности и защиты от кражи услуги. Шифрование осуществляет защиту, делая невозможным прочтение данных без правильного ключа дешифровки; однако оно не подтверждает правильность объектов источника/приема и не обеспечивает защиту от копирования после того, как данные были дешифрованы. Оно также не предотвращает атаки DOS.

– **Средства межсетевой защиты**: Применения средств межсетевой защиты предохраняют сетевой трафик от прохождения из одной области к другой области, пока он не удовлетворяет определенным критериям, установленным абонентом или оператором. В домашних приложениях средства межсетевой защиты обычно располагаются на жилых шлюзовых устройствах, которые подключают сеть HFC к дому.

  Применение межсетевой защиты помогает предотвращать атаки DOS и атаки конфиденциальности со стороны территориальной сети (*WAN, wide-area network*) средств межсетевой защиты, но не предохраняет от этих видов атак, приходящих с домовой стороны средств межсетевой защиты. Оно также не обеспечивает защиту от кражи услуги.

– **Безопасность сообщения административного управления**: Этот метод предотвращения включает в себя удостоверение подлинности и шифрование только сообщений административного управления. Сообщения сетевого административного управления используются для конфигурации устройства, наблюдения за сетью/управления сетью, обеспечения услуги и сохранения качества обслуживания (*QoS, Quality of Service*).

  Безопасность сообщений административного управления обеспечивает хороший механизм для предотвращения атак DOS путем удостоверения подлинности и шифрования сообщений административного управления. Личная информация абонента и информации сетевой конфигурации также защищаются от атак на конфиденциальность, но содержимое услуги не защищается. Кроме того, безопасность сообщений административного управления не предотвращает кражу содержимого услуги несанкционированными объектами.

Дополнение D

Приложения через CAT и средства межсетевой защиты

Известно существование функциональных возможностей NAT и средств межсетевой защиты, чтобы раздробить ряд протоколов и приложений. Следующий перечень протоколов и приложений ОБЯЗАН работать через реализации CAT и Средств межсетевой защиты. Этот перечень НЕ расположен в соответствии с приоритетами.

1) FTP;
2) Приложение между равными объектами (т.е. Gnutella, LimeWire, BearShare, Morpheus и пр.);
3) IPsec;
4) IGMP и Вещательное IP;
5) H.323 (Использованная в Windows® для различных приложений);
6) Приложения по Безотлагательному обмену сообщениями (т.е. AOL, Microsoft, Yahoo и пр.);
7) Электронная почта [*E-mail*] (протоколы SMTP и POP);
8) Приложения Направленных носителей информации (т.е. Real, MediaPlayer и пр.).

Кроме того, поставщикам СЛЕДУЕТ осуществлять любую попытку в поддержке игровых приложений реального времени через реализации CAT и средств межсетевой защиты.

Дополнение E

Базы MIB

E.1 База MIB услуги портала (*PS, Portal Service*)

База MIB услуги PS ОБЯЗАНА быть осуществлена так, как определено ниже.

```
CABH-PS-DEV-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     OBJECT-TYPE,
     Integer32,
     NOTIFICATION-TYPE
                                        FROM SNMPv2-SMI
     TruthValue,
     DisplayString,
     PhysAddress,
     DateAndTime,
     TEXTUAL-CONVENTION
                                        FROM SNMPv2-TC
     OBJECT-GROUP,
     MODULE-COMPLIANCE,
     NOTIFICATION-GROUP
                                        FROM SNMPv2-CONF

     InetAddressType,
     InetAddress,
     InetAddressIPv4,
     InetAddressIPv6
                                        FROM INET-ADDRESS-MIB

     docsDevSwCurrentVers,
     docsDevEvLevel,
     docsDevEvId,
     docsDevEvText,
     docsDevSwFilename,
     docsDevSwServer,
                FROM DOCS-CABLE-DEVICE-MIB -- RFC 2669

     cabhCdpServerDhcpAddress,
     cabhCdpWanDataAddrClientId
                         FROM CABH-CDP-MIB

     clabProjCableHome
                                        FROM CLAB-DEF-MIB;

--============================================================================
--
--   Хронология:
--============================================================================

cabhPsDevMib MODULE-IDENTITY
     ПОСЛЕДНИЙ РАЗ ОБНОВЛЕНО "0112190000Z" -- Декабрь 19, 2001
     ORGANIZATION [ОРГАНИЗАЦИЯ]    Cable     NMP Group"
     CONTACT-INFO
     "Kevin Luehrs
     Почтовый адрес: Cable Television Laboratories, Inc.
                400 Centennial Parkway
                Louisville, Colorado 80027-1266
       U.S.A
       Телефон: +1 303-661-9100
       Факс: +1 303-661-9199
       E-mail: k.luehrs@cablelabs.com"
```

```
     ОПИСАНИЕ
       "Этот модуль MIB поддерживает основные объекты административного
       управления для устройства услуги PS. Параметры устройства PS описывают
       общие атрибуты устройства PS и характеристики поведения. Больше всего база
       MIB устройства PS необходима для загрузки конфигурации".

-- Текстовые соглашения
     X509Certificate ::= ТЕКСТОВЫЕ СОГЛАШЕНИЯ
       СТАТУС текущий
       ОПИСАНИЕ
          "Цифровой сертификат X.509, кодированный как объект DER ASN.1."
       СТРОКА ОКТЕТА СИНТАКСИСА (РАЗМЕР (0..4096))

--
-- предполагает административное управление загрузкой SNMPv3
-- только по DOCSIS 1.1
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhPsDevMibObjects ::= { cabhPsDevMib 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhPsDevBase ::= { cabhPsDevMibObjects 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhPsDevProv ::= { cabhPsDevMibObjects 2 }

--
-- Следующая группа описывает основные объекты в услуге PS.
-- Это параметры, основанные на устройстве.
--

ТИП ОБЪЕКТА cabhPsDevDateTime
     СИНТАКСИС     DateAndTime
     MAX-ACCESS [максимальный доступ]    для чтения и записи
     СТАТУС        текущий
     ОПИСАНИЕ
       "Дата и время, с дополнительной информацией зоны времени."
     ::= { cabhPsDevBase 1 }

ТИП ОБЪЕКТА cabhPsDevResetNow
     СИНТАКСИС          TruthValue
     MAX-ACCESS         для чтения и записи
     СТАТУС             текущий
     ОПИСАНИЕ
          "Установка этого объекта в "истинно" (1) вызывает переустановку
          устройства. Чтение этого объекта всегда возвращает "ложно" (2). Когда
          cabhPsDevResetNow устанавливается в "истинно", происходят следующие
          действия:
       1) Очистить всю статистику в услуге PS.
       2) Очистить журналы регистрации трасс.
       3) Очистить все ассоциации безопасности.
       4) Установить в начальное состояние все параметры конфигурации
       5) Исключить все трансляции адресов
       6) Исключить все FQDN к преобразованиям IP
       7) Исключить все хранимые трансляции ARP
       8) Поток обеспечения начинается на шаге PS - 1."
     ::= { cabhPsDevBase 2 }

ТИП ОБЪЕКТА cabhPsDevSerialNumber
     СИНТАКСИС     DisplayString (РАЗМЕР (0..128))
     MAX-ACCESS    только для чтения
     СТАТУС        текущий
     ОПИСАНИЕ
       "Порядковый номер производителя для этой услуги PS. Этот параметр
       обеспечивается производителем и хранится в энергонезависимой памяти."
     ::= { cabhPsDevBase 3 }

ТИП ОБЪЕКТА cabhPsDevHardwareVersion
```

```
      СИНТАКСИС      DisplayString (РАЗМЕР (0..48))
      MAX-ACCESS     только для чтения
      СТАТУС         текущий
      ОПИСАНИЕ
        "Аппаратная версия производителя для этой услуги PS. Этот параметр
        обеспечивается производителем и хранится в энергонезависимой памяти."
      ::= { cabhPsDevBase 4 }

ТИП ОБЪЕКТА cabhPsDevMacAddress
      СИНТАКСИС      PhysAddress
      MAX-ACCESS     только для чтения
      СТАТУС         текущий
      ОПИСАНИЕ
        "Адрес MAC из WAN-MAN услуги PS. Обычно адреса WAN-MAN услуги PS и
        WAN-DATA услуги PS будут идентичными. Идентификаторы клиентов
        не будут теми же самыми, так что каждому может быть назначен разный
        адрес IP."
      ::= { cabhPsDevBase 5 }

ТИП ОБЪЕКТА cabhPsDevTypeIdentifier
      СИНТАКСИС      DisplayString
      MAX-ACCESS     только для чтения
      СТАТУС         текущий
      ОПИСАНИЕ
       "Это является копией идентификатора типа устройства, используемого в
       варианте выбора DHCP 60, которым обмениваются между услугой PS
        и сервером DHCP."
      ::= { cabhPsDevBase 6 }

ТИП ОБЪЕКТА cabhPsDevResetDefaults
      СИНТАКСИС      TruthValue
      MAX-ACCESS     для чтения и записи
      СТАТУС         текущий
      ОПИСАНИЕ
      "Установка этого объекта в Истинно" устанавливает все параметры PS в
      фабричные значения по умолчанию".
      ::= { cabhPsDevBase 7 }

ТИП ОБЪЕКТА cabhPsDevWanManClientId
      СИНТАКСИС      СТРОКА ОКТЕТА (РАЗМЕР (1..80))
      MAX-ACCESS     для чтения и записи
      СТАТУС         текущий
      ОПИСАНИЕ
      "Это представляет собой идентификатор ID клиента, используемый для запросов
      DHCP WAN-MAN.
        Значение по умолчанию является 6-байтным адресом MAC."
      ::= { cabhPsDevBase 8 }

ТИП ОБЪЕКТА cabhPsDevTodSyncStatus
      СИНТАКСИС      TruthValue
      MAX-ACCESS     только для чтения
      СТАТУС         текущий
      ОПИСАНИЕ
      "Этот объект указывает, была ли способна услуга PS успешно
      синхронизироваться с сервером Времени дня (TOD Time of Day)в кабельной сети.
      Услуга PS устанавливает этот объект в "истинно" (1), если услуга PS успешно
      синхронизирует свое время с сервером TOD. Услуга PS устанавливает этот
      объект в "ложно" (2), если услуга PS не осуществляет успешно синхронизацию с
      сервером TOD."
      ССЫЛКА
        " "
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ [DEFVAL] { false }[ложно]
      ::= { cabhPsDevBase 9 }
```

```
ТИП ОБЪЕКТА cabhPsDevProvMode
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО
     {
          dhcpmode (1),
          snmpmode (2)
     }
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
     "Этот объект указывает режим обеспечения, в котором действует услуга PS.
     Если услуга PS получает информацию Файла конфигурации PS (адрес сервера и
     имя файла) в сообщении DHCP, выпущенном сервером DHCP в кабельной сети, то
     услуга PS затем устанавливает этот объект в DHCPmode(1). Если услуга PS
     получает под-вариант 51 из варианта выбора 177 DHCP И не получает информацию
     Файла конфигурации PS в сообщении DHCP, которую услуга PS получает от
     сервера DHCP в кабельной сети, услуга PS устанавливает этот объект в
     SNMPmode(2)."
     ::= { cabhPsDevBase 10 }

ТИП ОБЪЕКТА cabhPsDevDwnldMode
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО
     {
       standard     (1),
       enhanced     (2)
     }
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Это есть режим загрузки, который услуга PS будет использовать."
       ::= { cabhPsDevBase 11 }

--
--   Следующая группа определяет параметры, характерные для обеспечения
--

ТИП ОБЪЕКТА cabhPsDevProvisioningTimer
     СИНТАКСИС      ЦЕЛОЕ ЧИСЛО (0..16383)
     ЕДИНИЦЫ        "минуты"
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
     "Этот объект дает возможность пользователю устанавливать длительность
     таймера выдержки времени обеспечения. Значение устанавливается в минутах.
     Установка таймера в 0 выключает его. Значение по умолчанию для таймера
     составляет 5."
     ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {5}
     ::= {cabhPsDevProv 1}

ТИП ОБЪЕКТА cabhPsDevProvConfigFile
     СИНТАКСИС      DisplayString(РАЗМЕР(1..128))
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "URL главного узла TFTP для загрузки параметров обеспечения и конфигурации
       к этому устройству. Возвращает ПУСТОЕ [null], если адрес сервера
       неизвестен."
     ::= { cabhPsDevProv 2 }

ТИП ОБЪЕКТА cabhPsDevProvConfigHash
     СИНТАКСИС      СТРОКА ОКТЕТА (РАЗМЕР(20))
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
```

```
      "Случайные данные содержимого файла config, вычисленные и посланные к
      услуге PS перед отправкой файла конфигурации. Для алгоритма удостоверения
      подлинности SHA-1 длина случайных данных составляет 160 битов."
     ::= { cabhPsDevProv 3 }

ТИП ОБЪЕКТА cabhPsDevProvConfigFileSize
     СИНТАКСИС      Integer32
     ЕДИНИЦЫ        "байты"
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Размер файла конфигурации."
     ::={ cabhPsDevProv 4 }

ТИП ОБЪЕКТА cabhPsDevProvConfigTLVProcessed
     СИНТАКСИС      ЦЕЛОЕ ЧИСЛО (0..16383)
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Число значений TLV, обработанных в файле config."
     ::={ cabhPsDevProv 5 }

ТИП ОБЪЕКТА cabhPsDevProvConfigTLVRejected
     СИНТАКСИС      ЦЕЛОЕ ЧИСЛО (0..16383)
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Число значений TLV, отклоненных в файле config."
     ::={ cabhPsDevProv 6 }

ТИП ОБЪЕКТА cabhPsDevProvSolicitedKeyTimeout
     СИНТАКСИС      Integer32 (15..600)
     ЕДИНИЦЫ        "секунды"
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Эта временная выдержка применяется только тогда, когда сервер обеспечения
       инициировал административное управление ключом (с помощью сообщения Wake Up
       [запустить]) для протокола SNMPv3. Это период, во время которого услуга PS
       будет сохранять число (внутри поля номера последовательности) от
       отосланного запроса AP и ожидать ответа AP преобразования от Сервера
       обеспечения."
     ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 120 }
     ::= { cabhPsDevProv 7 }

ТИП ОБЪЕКТА cabhPsDevProvState
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО
     {
          pass          (1),
          inProgress    (2),
          fail          (3)
     }
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Этот объект указывает состояние завершения процесса установления в
       начальное состояние. После установления потока в начальное состояние имеют
       место состояния "Прохождение" или "Неудача". Состояние InProgress возникает
       из начала установления в начальное состояние услуги PS к окончанию
       установления в начальное состояние услуги PS."
       ::= { cabhPsDevProv 8 }

ТИП ОБЪЕКТА cabhPsDevProvAuthState
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО
```

```
    {
        accepted      (1),
        rejected      (2)
    }
    MAX-ACCESS    только для чтения
    СТАТУС        текущий
    ОПИСАНИЕ
      "Этот объект указывает состояние удостоверения подлинности для файла
      конфигурации."
    ::= { cabhPsDevProv 9 }

ТИП ОБЪЕКТА cabhPsDevProvCorrelationId
    СИНТАКСИС     Integer32
    MAX-ACCESS    только для чтения
    СТАТУС        текущий
    ОПИСАНИЕ
      "Случайное значение, порождаемое услугой PS для использования в
      санкционировании регистрации. Это только для использования в сообщениях
      установления в начальное состояние услуги PS и для загрузки файла
      конфигурации PS . Это значение появляется в обоих информационных
      сообщениях cabhPsDevProvisioningStatus и
      cabhPsDevProvisioningEnrollmentReport, чтобы проверить экземпляр загрузки
      файла конфигурации."
    ::= { cabhPsDevProv 10 }

ТИП ОБЪЕКТА cabhPsDevTimeServerAddrType
    СИНТАКСИС     InetAddressType
    MAX-ACCESS    только для чтения
    СТАТУС        текущий
    ОПИСАНИЕ
      "Тип адреса IP сервера Времени (RFC 868). Обычно используется версия 4 IP."
    ::= { cabhPsDevProv 11 }

ТИП ОБЪЕКТА cabhPsDevTimeServerAddr
    СИНТАКСИС     InetAddress
    MAX-ACCESS    только для чтения
    СТАТУС        текущий
    ОПИСАНИЕ
      "Адрес IP сервера Времени (RFC 868). Возвращает 0.0.0.0, если адрес IP
      сервера времени неизвестен."
    ::= { cabhPsDevProv 12 }

--
--   группа уведомления оставлена для будущего расширения.
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhPsNotification    ::= { cabhPsDevMib 2 0 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhPsConformance ::= { cabhPsDevMib 3 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhPsCompliances ::= { cabhPsConformance 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhPsGroups ::= { cabhPsConformance 2 }

--
--   Группа уведомления
--

ТИП УВЕДОМЛЕНИЯ cabhPsDevInitTLVUnknownTrap
    ОБЪЕКТЫ  {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress
    }
    СТАТУС текущий
    ОПИСАНИЕ
```

```
      "Событие благодаря обнаружению неизвестного значения TLV во время процесса
      структурного анализа TLV. Значения docsDevEvLevel, docsDevId и
      docsDevEvText берутся из записи, которая регистрирует это событие в
      объекте docsDevEventTable. Значение cabhPsDevMacAddress указывает адрес
      MAC услуги PS. Эта часть информации является однообразной по всем захватам
      PS."
    ::= { cabhPsNotification 1 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevInitTrap
    ОБЪЕКТЫ {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress,
      cabhPsDevProvConfigFile,
      cabhPsDevProvConfigTLVProcessed,
      cabhPsDevProvConfigTLVRejected
    }
    СТАТУС    текущий
    ОПИСАНИЕ
     "Это информационное сообщение выпускается для подтверждения успешного
     завершения процесса обеспечения."
    ::= { cabhPsNotification 2 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevInitRetryTrap
    ОБЪЕКТЫ  {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
    cabhPsDevMacAddress
    }
    СТАТУС    текущий
    ОПИСАНИЕ
     "Событие, чтобы сообщить о неудаче, которая случилась во время процесса
     установления в начальное состояние и была обнаружена в услуге."
    ::= { cabhPsNotification 3 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevDHCPFailTrap
    ОБЪЕКТЫ {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress,
      cabhCdpServerDhcpAddress
    }
    СТАТУС   текущий
    ОПИСАНИЕ
      "Событие, чтобы сообщить о неисправности сервера DHCP. Значение
      cabhCdpServerDhcpAddress является адресом IP сервера DHCP."
    ::= { cabhPsNotification 4 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevSwUpgradeInitTrap
    ОБЪЕКТЫ {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress,
      docsDevSwFilename,
      docsDevSwServer
    }
    СТАТУС текущий
    ОПИСАНИЕ
      "Событие, чтобы сообщить о событии, инициированном обновлением
      программного обеспечения. Значения docsDevSwFilename и docsDevSwServer
```

```
      указывают название изображения программного обеспечения и адрес IP
      сервера, откуда взято изображение."
    ::= { cabhPsNotification 5 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevSwUpgradeFailTrap
    ОБЪЕКТЫ {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress,
      docsDevSwFilename,
      docsDevSwServer
    }
    СТАТУС текущий
    ОПИСАНИЕ
      "Событие, чтобы сообщить о неудаче попытки обновления программного
      обеспечения. Значения docsDevSwFilename и docsDevSwServer указывают
      название изображения программного обеспечения и адрес IP сервера, откуда
      взято изображение."
    ::= { cabhPsNotification 6 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevSwUpgradeSuccessTrap
    ОБЪЕКТЫ {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress,
      docsDevSwFilename,
      docsDevSwServer
    }
    СТАТУС  текущий
    ОПИСАНИЕ
      "Событие, чтобы сообщить о событии успеха обновления программного
      обеспечения. Значения docsDevSwFilename и docsDevSwServer указывают
      название изображения программного обеспечения и адрес IP сервера, откуда
      взято изображение."
    ::= { cabhPsNotification 7 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevSwUpgradeCVCFailTrap
    ОБЪЕКТЫ {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress
    }
    СТАТУС   текущий
    ОПИСАНИЕ
      "Событие, чтобы сообщить о неудаче проверки файла кода, которая случилась
      во время попытки безопасного обновления программного обеспечения."
    ::= { cabhPsNotification 8 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevTODFailTrap
    ОБЪЕКТЫ {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevTimeServerAddr
    }
    СТАТУС   текущий
    ОПИСАНИЕ
      " Событие, чтобы сообщить о неудаче сервера Времени дня. Значение
      cabhPsDevTimeServerAddr указывает адрес IP сервера."
    ::= { cabhPsNotification 9 }
```

```
ТИП УВЕДОМЛЕНИЯ cabhPsDevCdpWanDataIpTrap
     ОБЪЕКТЫ {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhCdpWanDataAddrClientId
     }
     СТАТУС    текущий
     ОПИСАНИЕ
       "Событие, чтобы сообщить о неудаче услуги PS получить все необходимые
       адреса IP WAN-Data. Объект cabhCdpWanDataAddrClientId указывает ClientId,
       для которого имела место неудача."
     ::= { cabhPsNotification 10 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevCdpThresholdTrap
     ОБЪЕКТЫ {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress,
       cabhCdpLanTransThreshold
     }
     СТАТУС    текущий
     ОПИСАНИЕ
       "Событие, чтобы сообщить о том, что был превышен порог LAN-Trans."
     ::= { cabhPsNotification 11 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevCspTrap
     ОБЪЕКТЫ {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress
     }
     СТАТУС    текущий
     ОПИСАНИЕ
       "Сообщить о событии с помощью Портала кабельной безопасности."
     ::= { cabhPsNotification 12 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevCapTrap
     ОБЪЕКТЫ {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress
     }
     СТАТУС    текущий
     ОПИСАНИЕ
       "Сообщить о событии с помощью Портала кабельного адреса."
     ::= { cabhPsNotification 13 }

ТИП УВЕДОМЛЕНИЯ cabhPsDevProvEnrollTrap
     ОБЪЕКТЫ {
       cabhPsDevHardwareVersion,
       docsDevSwCurrentVers,
       cabhPsDevTypeIdentifier,
       cabhPsDevMacAddress,
       cabhPsDevProvCorrelationId
     }
     СТАТУС    текущий
     ОПИСАНИЕ
       "Это информационное сообщение выпускается, чтобы инициировать обеспечение
       процесса."
     ССЫЛКА
```

```
       "Информационное сообщение, как определено в документе RFC 1902."
     ::= { cabhPsNotification 14 }

-- заявления о соответствии

СООТВЕТСТВИЕ МОДУЛЯ cabhPsBasicCompliance
     СТАТУС    текущий
     ОПИСАНИЕ
       "Заявление о соответствии для устройств, которые осуществляют свойство PS."
     МОДУЛЬ   --cabhPsMib

-- безоговорочно обязательные группы

     ОБЯЗАТЕЛЬНЫЕ ГРУППЫ {
       cabhPsGroup
     }

::= { cabhPsCompliances 3 }

ГРУППА ОБЪЕКТА cabhPsGroup
     ОБЪЕКТЫ {
       cabhPsDevDateTime,
       cabhPsDevResetNow,
       cabhPsDevSerialNumber,
       cabhPsDevHardwareVersion,
       cabhPsDevMacAddress,
       cabhPsDevTypeIdentifier,
          cabhPsDevResetDefaults,
          cabhPsDevWanManClientId,
          cabhPsDevTodSyncStatus,
       cabhPsDevProvMode,
       cabhPsDevDwnldMode,

       cabhPsDevProvisioningTimer,
          cabhPsDevProvConfigFile,
          cabhPsDevProvConfigHash,
          cabhPsDevProvConfigFileSize,
          cabhPsDevProvConfigTLVProcessed,
          cabhPsDevProvConfigTLVRejected,
          cabhPsDevProvSolicitedKeyTimeout,
          cabhPsDevProvState,
          cabhPsDevProvAuthState,
       cabhPsDevProvCorrelationId,
       cabhPsDevTimeServerAddrType,
       cabhPsDevTimeServerAddr

     }
     СТАТУС    текущий
     ОПИСАНИЕ
       "Группа объектов для базы MIB услуги PS."
     ::= { cabhPsGroups 1 }

ГРУППА УВЕДОМЛЕНИЯ cabhPsNotificationGroup
     УВЕДОМЛЕНИЯ { cabhPsDevInitTLVUnknownTrap, cabhPsDevInitTrap,
cabhPsDevInitRetryTrap,
          cabhPsDevDHCPFailTrap, cabhPsDevSwUpgradeInitTrap,
cabhPsDevSwUpgradeFailTrap,
          cabhPsDevSwUpgradeSuccessTrap, cabhPsDevSwUpgradeCVCFailTrap,
cabhPsDevTODFailTrap,
          cabhPsDevCdpWanDataIpTrap, cabhPsDevCdpThresholdTrap, cabhPsDevCspTrap,
          cabhPsDevCapTrap, cabhPsDevProvEnrollTrap }
     СТАТУС   текущий
     ОПИСАНИЕ
          "Эти уведомления имеют дело с изменением в статусе Устройства PS."
```

```
     ::= { cabhPsGroups 2 }

КОНЕЦ
```

E.2 База MIB портала испытания CableHome

База MIB портала CTP ОБЯЗАНА быть осуществлена так, как определено ниже.

```
CABH-CTP-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     OBJECT-TYPE
               FROM SNMPv2-SMI
     TruthValue,
     TEXTUAL-CONVENTION
               FROM SNMPv2-TC
     OBJECT-GROUP,
     MODULE-COMPLIANCE
               FROM SNMPv2-CONF
     InetAddressType,
     InetAddress,
     InetAddressIPv4,
     InetAddressIPv6
               FROM INET-ADDRESS-MIB
     clabProjCableHome
               FROM CLAB-DEF-MIB;

--============================================================================
--
--   Хронология:
--
--============================================================================

ИМЕНОВАНИЕ МОДУЛЯ cabhCtpMib
     ПОСЛЕДНЕЕ ОБНОВЛЕНИЕ    "0112190000Z" -- Декабрь 19, 2001
     ORGANIZATION       "Cable NMP Group"
       CONTACT-INFO
       "Kevin Luehrs
       Почтовый адрес: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
          U.S.A.
          Телефон: +1 303-661-9100
          Факс: +1 303-661-9199
          E-mail: k.luehrs@cablelabs.com"
     ОПИСАНИЕ
       "Этот модуль MIB определяет директивы диагностики, предлагаемые Порталом
       испытания (CTP, CableHome Testing Portal).
        Подтверждения:
        "
     ::= { clabProjCableHome 5 }

-- Текстовые соглашения

--
-- предполагает, что административное управление загрузкой программного
-- обеспечения (SW)протокола SNMPv3 осуществляется только по DOCSIS 1.1
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpObjects ::= { cabhCtpMib 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpBase ::= { cabhCtpObjects 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpConnSpeed ::= { cabhCtpObjects 2 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpPing ::= { cabhCtpObjects 3 }
```

```
--
-- Следующая группа описывает основные объекты в Портале кабельного
-- административного управления.
--

ТИП ОБЪЕКТА cabhCtpReset
       СИНТАКСИС    TruthValue
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Установка этого объекта в значение "истинно" (1) вызывает завершение всех
       испытаний. Чтение этого объекта всегда возвращает значение "ложно" (2).
       Когда cabhCtpReset устанавливается в значение "истинно", происходят
       следующие действия:
        1) Завершить все выполняемые диагностические испытания.
        2) Очистить всю диагностическую статистику."
     ::= { cabhCtpBase 1 }

--
--   Параметры и результаты из Команды скорости соединения
--

ТИП ОБЪЕКТА cabhCtpConnSrcIpType
       синтаксис    InetAddressType
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса IP, используемого в качестве адреса источника для Испытания
       скорости соединения."
     ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
     ::= { cabhCtpConnSpeed 1 }

ТИП ОБЪЕКТА cabhCtpConnSrcIp
       СИНТАКСИС    InetAddress
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адрес IP, используемый в качестве адреса источника для Испытания скорости
       соединения. Обычно адрес будет значением в объекте cabhCdpServerRouter.
       Адрес по умолчанию есть 192.168.0.1."
       ССЫЛКА
          "Секция спецификации 6.4.3.2"
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 'c0a80001'h }    -- 192.168.0.1
       ::= { cabhCtpConnSpeed 2 }

ТИП ОБЪЕКТА cabhCtpConnDestIpType
       СИНТАКСИС    InetAddressType
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адрес IP, используемый в качестве адреса пункта назначения для Испытания
       скорости соединения."
        ::= { cabhCtpConnSpeed 3 }

ТИП ОБЪЕКТА cabhCtpConnDestIp
       СИНТАКСИС    InetAddress
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адрес IP, используемый в качестве адреса пункта назначения для испытания
       скорости соединения."
        ::= { cabhCtpConnSpeed 4 }
```

```
ТИП ОБЪЕКТА cabhCtpConnProto
      СИНТАКСИС             ЦЕЛОЕ ЧИСЛО {
                udp         (1),
                tcp         (2)
                }
      MAX-ACCESS  для чтения и записи
     СТАТУС       текущий
     ОПИСАНИЕ
      "Протокол, используемый в Испытании скорости соединения. Испытание TCP
      является дополнительным."
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { udp }
      ::= { cabhCtpConnSpeed 5 }

ТИП ОБЪЕКТА cabhCtpConnPort
      СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (1..65535)
      MAX-ACCESS  для чтения и записи
     СТАТУС       текущий
     ОПИСАНИЕ
      "Порт, используемый для Испытания скорости соединения."
     ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {7}
     ::= { cabhCtpConnSpeed 6 }

ТИП ОБЪЕКТА cabhCtpConnNumPkts
     СИНТАКСИС     ЦЕЛОЕ ЧИСЛО (1..255)
     MAX-ACCESS    для чтения и записи
     СТАТУС        текущий
     ОПИСАНИЕ
      "Количество пакетов, подлежащих отправке."
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {1}
      ::= { cabhCtpConnSpeed 7 }

ТИП ОБЪЕКТА cabhCtpConnPktSize
      СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (64..1518)
      MAX-ACCESS  для чтения и записи
     СТАТУС       текущий
     ОПИСАНИЕ
      "Размер испытательных кадров."
      ССЫЛКИ
      ""
      ::= { cabhCtpConnSpeed 8 }

ТИП ОБЪЕКТА cabhCtpConnTimeOut
      СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (0..600000)
     -- Максимум 10 минут
      ЕДИНИЦЫ     "миллисекунды"
      MAX-ACCESS  для чтения и записи
     СТАТУС       текущий
     ОПИСАНИЕ
      "Значение выдержки времени для отклика. Значение нуля указывает отсутствие
      выдержки времени и может быть использовано только для TCP."
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {600000}
     ::= { cabhCtpConnSpeed 9 }

ТИП ОБЪЕКТА cabhCtpConnControl
         СИНТАКСИС     ЦЕЛОЕ ЧИСЛО {
                       notRun        (1),
                       start         (2),
                       abort         (3)
                       }
      MAX-ACCESS  для чтения и записи
     СТАТУС       текущий
     ОПИСАНИЕ
```

```
      "Управление для Испытания скорости соединения. Значение notRun используется
      для указания того, что никогда не выполняется. Этому параметру следует
      устанавливаться только через протокол SNMP."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { notRun(1) }
     ::= { cabhCtpConnSpeed 10 }

ТИП ОБЪЕКТА cabhCtpConnStatus
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО {
                        running       (1),
                        complete      (2),
                        aborted       (3)
                    }
       MAX-ACCESS   только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
      "Статус испытания, выполняемого в настоящее время/последнего выполненного
      испытания."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { complete(2) }
       ::= { cabhCtpConnSpeed 11 }

ТИП ОБЪЕКТА cabhCtpConnPktsSent
       СИНТАКСИС    ЦЕЛОЕ ЧИСЛО (0..255)
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Количество отосланных пакетов."
       ::= { cabhCtpConnSpeed 12 }

ТИП ОБЪЕКТА cabhCtpConnPktsRecv
       СИНТАКСИС    ЦЕЛОЕ ЧИСЛО (0..255)
       MAX-ACCESS   только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Количество полученных пакетов."
     ::= { cabhCtpConnSpeed 13 }

ТИП ОБЪЕКТА cabhCtpConnAvgRTT
     СИНТАКСИС      ЦЕЛОЕ ЧИСЛО (0..600000)
     ЕДИНИЦЫ        "миллисекунды"
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
      "Результирующее усреднение значений времени передачи по шлейфу для
      подтверждаемых пакетов."
       ::= { cabhCtpConnSpeed 14 }

ТИП ОБЪЕКТА cabhCtpConnMaxRTT
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО (0..600000)
       ЕДИНИЦЫ          "миллисекунды"
       MAX-ACCESS       только для чтения
     СТАТУС             текущий
     ОПИСАНИЕ
      "Результирующий максимум значений времени передачи по шлейфу для
      подтвержденных пакетов."
       ::= { cabhCtpConnSpeed 15 }

ТИП ОБЪЕКТА cabhCtpConnMinRTT
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО (0..600000)
       ЕДИНИЦЫ          "миллисекунды"
       MAX-ACCESS   только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
      "Результирующий минимум для значений времени передачи по шлейфу для
      подтвержденных пакетов."
```

```
       ::= { cabhCtpConnSpeed 16 }

ТИП ОБЪЕКТА cabhCtpConnNumIcmpError
       СИНТАКСИС    ЦЕЛОЕ ЧИСЛО (0..255)
       MAX-ACCESS   только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Количество ошибок ICMP."
       ::= { cabhCtpConnSpeed 17 }

ТИП ОБЪЕКТА cabhCtpConnIcmpError
       СИНТАКСИС    ЦЕЛОЕ ЧИСЛО (0..255)
       MAX-ACCESS   только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Последняя ошибка ICMP."
     ::= { cabhCtpConnSpeed 18 }

--
--   Параметры и результаты для Команды по переброске
--

ТИП ОБЪЕКТА cabhCtpPingSrcIpType
       СИНТАКСИС    InetAddressType
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса IP, используемый в качестве адреса источника для Испытания по
       переброске информации."
       ::= { cabhCtpPing 1 }

ТИП ОБЪЕКТА cabhCtpPingSrcIp
       СИНТАКСИС    InetAddress
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адрес IP, используемый в качестве адреса источника для Испытания по
       переброске информации. Обычно адрес будет значением адреса IP WanMan услуги
       PS. Используется адрес 192.168.0.x."
       ::= { cabhCtpPing 2 }

PS cabhCtpPingDestIpType
       СИНТАКСИС    InetAddressType
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса IP пункта назначения для Испытания по переброске информации."
       ::= { cabhCtpPing 3 }

ТИП ОБЪЕКТА cabhCtpPingDestIp
       СИНТАКСИС        InetAddress
       MAX-ACCESS       для чтения и записи
     СТАТУС             текущий
     ОПИСАНИЕ
       "Адрес IP пункта назначения, используемый в качестве адреса для Испытания
       по переброске информации."
     ::= { cabhCtpPing 4 }

ТИП ОБЪЕКТА cabhCtpPingProto
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО {
                        icmp (1),
                        }
       MAX-ACCESS   для чтения и записи
     СТАТУС         текущий
```

```
     ОПИСАНИЕ
       "Протокол, используемый для накопления информационных сообщений топологии."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { icmp }
     ::= { cabhCtpPing 5 }

ТИП ОБЪЕКТА cabhCtpPingNumPkts
       СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (1..4)
       MAX-ACCESS  для чтения и записи
     СТАТУС        текущий
     ОПИСАНИЕ
       "Количество пакетов, подлежащих отправке каждому главному узлу."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {1}
       ::= { cabhCtpPing 6 }

ТИП ОБЪЕКТА cabhCtpPingPktSize
       СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (64..1518)
       MAX-ACCESS  для чтения и записи
     СТАТУС        текущий
     ОПИСАНИЕ
       "Размер испытательных кадров."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {64}
       ::= { cabhCtpPing 7 }

ТИП ОБЪЕКТА cabhCtpPingTimeBetween
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО (0..600000)
       ЕДИНИЦЫ          "миллисекунды"
       MAX-ACCESS       для чтения и записи
     СТАТУС             текущий
     ОПИСАНИЕ
       "Время между одной переброской информации и следующей."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 1000 }
       ::= { cabhCtpPing 8 }


ТИП ОБЪЕКТА cabhCtpPingTimeOut
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО (0..600000)
       ЕДИНИЦЫ          "миллисекунды"
       MAX-ACCESS       для чтения и записи
       СТАТУС           текущий
     ОПИСАНИЕ
       "Выдержка времени для отклика в переброске информации для отправки
       отдельной переброски."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 5000 } -- 5 seconds
       ::= { cabhCtpPing 9 }
ТИП ОБЪЕКТА cabhCtpPingControl
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО {
                        notRun        (1),
                        start         (2),
                        abort         (3)
                        }
       MAX-ACCESS  для чтения и записи
     СТАТУС        текущий
     ОПИСАНИЕ
       "Управление для Испытания по переброске информации. Значение notRun
       используется для указания того, что никогда не выполняется."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { notRun(1) }
       ::= { cabhCtpPing 10 }

ТИП ОБЪЕКТА cabhCtpPingStatus OBJECT-TYPE
       СИНТАКСИС        ЦЕЛОЕ ЧИСЛО {
                        running       (1),
                        complete      (2),
                        aborted       (3)
                        }
```

```
      MAX-ACCESS  только для чтения
     СТАТУС       текущий
     ОПИСАНИЕ
      "Статус испытания, выполняемого в настоящее время/последнего выполненного
      испытания."
       ::= { cabhCtpPing 11 }

ТИП ОБЪЕКТА cabhCtpPingNumSent
      СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (0..255)
      MAX-ACCESS  только для чтения
     СТАТУС       текущий
     ОПИСАНИЕ
      "Количество посланных перебросок информации."
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { complete(2) }
      ::= { cabhCtpPing 12 }

ТИП ОБЪЕКТА cabhCtpPingNumRecv
      СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (0..255)
      MAX-ACCESS  только для чтения
     СТАТУС       текущий
     ОПИСАНИЕ
      "Количество полученных перебросок информации."
      ::= { cabhCtpPing 13 }

--============================================================================

--
-- группа уведомления оставлена для будущего расширения.
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpNotification ::= { cabhCtpMib 2 0 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpConformance ::= { cabhCtpMib 3 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpCompliances ::= { cabhCtpConformance 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCtpGroups ::= { cabhCtpConformance 2 }

--
--   Группа уведомления
--

-- заявления о соответствии

СООТВЕТСТВИЕ МОДУЛЯ cabhCtpBasicCompliance
     СТАТУС   текущий
     ОПИСАНИЕ
      "Заявление о соответствии для устройства, которое осуществляет свойство
      Услуги портала."
     МОДУЛЬ   -- cabhCtpMib

-- безоговорочно обязательные группы

     ОБЯЗАТЕЛЬНЫЕ ГРУППЫ {
       cabhCtpGroup
     }

::= { cabhCtpCompliances 3 }

ГРУППА ОБЪЕКТА cabhCtpGroup
     ОБЪЕКТЫ {
       cabhCtpReset,
          cabhCtpConnSrcIpType,
          cabhCtpConnSrcIp,
          cabhCtpConnDestIpType,
          cabhCtpConnDestIp,
          cabhCtpConnProto,
```

```
          cabhCtpConnPort,
          cabhCtpConnNumPkts,
          cabhCtpConnPktSize,
          cabhCtpConnTimeOut,
          cabhCtpConnControl,
          cabhCtpConnStatus,
          cabhCtpConnPktsSent,
          cabhCtpConnPktsRecv,
          cabhCtpConnAvgRTT,
          cabhCtpConnMinRTT,
          cabhCtpConnMaxRTT,
          cabhCtpConnNumIcmpError,
          cabhCtpConnIcmpError,

          cabhCtpPingSrcIpType,
          cabhCtpPingSrcIp,
          cabhCtpPingDestIpType,
          cabhCtpPingDestIp,
          cabhCtpPingProto,
          cabhCtpPingNumPkts,
          cabhCtpPingPktSize,
          cabhCtpPingTimeBetween,
          cabhCtpPingTimeOut,
          cabhCtpPingControl,
          cabhCtpPingStatus,
          cabhCtpPingNumSent,
          cabhCtpPingNumRecv
        }
    СТАТУС    текущий
    ОПИСАНИЕ
      "Группа объектов для базы MIB кабельного портала CTP."
      ::= { cabhCtpGroups 1 }

КОНЕЦ
```

E.3 База MIB безопасности

База MIB безопасности ОБЯЗАНА быть осуществлена так, как определено ниже.

```
CABH-SEC-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
      Unsigned32,
      BITS,
      OBJECT-TYPE
                            FROM SNMPv2-SMI
      TruthValue,
      DisplayString,
      TimeStamp
                            FROM SNMPv2-TC
      OBJECT-GROUP,
      MODULE-COMPLIANCE     FROM SNMPv2-CONF
      InetAddressIPv4       FROM INET-ADDRESS-MIB
      SnmpAdminString       FROM SNMP-FRAMEWORK-MIB -- RFC 2571
      X509Certificate       FROM DOCS-BPI2MIB
      clabProjCableHome     FROM CLAB-DEF-MIB;

--=============================================================================
--
--   Хронология:
--
--
--
--=============================================================================
```

```
cabhSecMib MODULE-IDENTITY
     ПОСЛЕДНЕЕ ОБНОВЛЕНИЕ    "0112200000Z" -- декабрь 20, 2001
     ORGANIZATION       "Cable NMP Group"
     CONTACT-INFO
       "Kevin Luehrs
       Почтовый адрес: Cable Television Laboratories, Inc.
              400 Centennial Parkway
              Louisville, Colorado 80027-1266
       U.S.A.
       Телефон: +1 303-661-9100
       Факс: +1 303-661-9199
       E-mail: k.luehrs@cablelabs.com"
     ОПИСАНИЕ
      "Этот модуль MIB поставляет основные объекты административного управления
      для Услуг портала безопасности.

       Подтверждения:
       "
     ::= { clabProjCableHome 2 }

-- Текстовые соглашения

--
-- предполагает, что административное управление загрузкой программного
-- обеспечения (SW) протокола SNMPv3 осуществляется только по DOCSIS 1.1.


ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecFwObjects ::= { cabhSecMib 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecFwBase ::= { cabhSecFwObjects 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecFwLogCtl ::= { cabhSecFwObjects 2 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecCertObjects ::= { cabhSecMib 2 }
--
--   Следующая группа описывает основные объекты в Кабельных средствах межсетевой
--   зашиты.


ТИП ОБЪЕКТА cabhSecFwPolicyFileEnable
     СИНТАКСИС     ЦЕЛОЕ ЧИСЛО {
                        enable        (1),
                        disable       (2)
                        }
     MAX-ACCESS    для чтения и записи
     СТАТУС        текущий
     ОПИСАНИЕ
      "Этот параметр указывает, обеспечиваются или нет функциональные возможности
      средств межсетевой защиты."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {enable}
     ::= { cabhSecFwBase 1 }

ТИП ОБЪЕКТА cabhSecFwPolicyFileURL
     СИНТАКСИС     DisplayString
     MAX-ACCESS    для чтения и записи
     СТАТУС        текущий
     ОПИСАНИЕ
      "Содержит название и адрес IP файла набора правил для алгоритмов в формате
          URL TFTP. После того, как этот объект был обновлен, он будет запускать
      загрузку файла."
     ::= { cabhSecFwBase 2 }

ТИП ОБЪЕКТА cabhSecFwPolicyFileHash
     СТРОКА ОКТЕТА СИНТАКСИСА    (РАЗМЕР(20))
     MAX-ACCESS    для чтения и записи
     СТАТУС        текущий
```

```
      ОПИСАНИЕ
        "Случайные данные содержимого из файла набора правил, вычисленные и
        отправленные к услуге PS перед отправкой файла набора правил.
        Для алгоритма удостоверения подлинности SHA-1 длина случайных данных
        составляет 160 битов."
      ::= { cabhSecFwBase 3 }

ТИП ОБЪЕКТА cabhSecFwPolicyFileOperStatus
      СИНТАКСИС   ЦЕЛОЕ ЧИСЛО {
      inProgress(1),
      completeFromProvisioning(2),
      completeFromMgt(3),
      failed(4)
      }
      MAX-ACCESS     только для чтения
      СТАТУС         текущий
      ОПИСАНИЕ
        "Объект InProgress(1) указывает, что осуществляется загрузка TFTP,
        либо как результат несоответствия версии в обеспечении,
        или как результат запроса объекта upgradeFromMgt.
        CompleteFromProvisioning(2) указывает, что последнее обновление
        программного обеспечения было результатом несоответствия версии в
        обеспечении. CompleteFromMgt(3) указывает, что последнее обновление
        программного обеспечения было результатом установки
        объекта docsDevSwAdminStatus в upgradeFromMgt.
        Неудавшееся(4) указывает, что последняя предпринятая загрузка
        потерпела неудачу из-за выдержки времени TFTP."

      ::= { cabhSecFwBase 4 }

ТИП ОБЪЕКТА cabhSecFwPolicyFileCurrentVersion
      СИНТАКСИС           SnmpAdminString
      -- MAX-ACCESS только для чтения
      -- Добавляется доступ для записи, чтобы позволить фабричную конфигурацию
      MAX-ACCESS     для чтения и записи
      СТАТУС         текущий
      ОПИСАНИЕ
        "Версия набора правил, в настоящее время действующая в устройстве PS.
        Этому объекту следует быть в синтаксисе, используемом для индивидуального
        поставщика, чтобы указывать  версии программного обеспечения. Любой
        элемент PS ОБЯЗАН возвращать описательную строку текущей загрузки набора
       правил.
        Если это не применяется, то этот объект ОБЯЗАН содержать пустую строку."
        ::= { cabhSecFwBase 5 }

--
--   Параметры регистрации средств межсетевой защиты
--

ТИП ОБЪЕКТА cabhSecFwEventType1Enable
      СИНТАКСИС ЦЕЛОЕ ЧИСЛО         {
        enable                 (1), -- регистрировать событие
        disable                (2), -- не регистрировать событие
        }
      MAX-ACCESS  для чтения и записи
      СТАТУС      текущий
      ОПИСАНИЕ
        "Обеспечивает или исключает регистрацию сообщений о событиях межсетевой
       защиты типа 1."
      ::= { cabhSecFwLogCtl 1 }
```

```
ТИП ОБЪЕКТА cabhSecFwEventType2Enable
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО      {
       enable                (1), -- регистрировать событие
       disable               (2), -- не регистрировать событие
       }
     MAX-ACCESS  для чтения и записи
     СТАТУС      текущий
     ОПИСАНИЕ
      "Обеспечивает или исключает регистрацию сообщений о событиях межсетевой
      защиты типа 2."
     ::= { cabhSecFwLogCtl 2 }

ТИП ОБЪЕКТА cabhSecFwEventType3Enable
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО      {
       enable                (1), -- регистрировать событие
       disable               (2), -- не регистрировать событие
       }
     MAX-ACCESS  для чтения и записи
     СТАТУС      текущий
     ОПИСАНИЕ
       " Обеспечивает или исключает регистрацию сообщений о событиях межсетевой
       защиты типа 3."
     ::= { cabhSecFwLogCtl 3 }

ТИП ОБЪЕКТА cabhSecFwEventAttackAlertThreshold
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО      (0..65535)
     MAX-ACCESS  для чтения и записи
     СТАТУС      текущий
     ОПИСАНИЕ
       "Если число атак хакеров типа 1 или 2 превышает этот порог
      в периоде, определенном с помощью cabhSecFwEventAttackAlertPeriod, событие
      сообщения межсетевой защиты ОБЯЗАНО быть зарегистрировано с уровнем
      приоритета 4."
     ::= { cabhSecFwLogCtl 4 }

ТИП ОБЪЕКТА cabhSecFwEventAttackAlertPeriod
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО               (0..65535)
     MAX-ACCESS  для чтения и записи
     СТАТУС текущий
     ОПИСАНИЕ
       "Указывает период, подлежащий использованию (в днях) для
       объекта cabhSecFwEventAttackAlertThreshold."
     ::= { cabhSecFwLogCtl 5 }
ТИП ОБЪЕКТА cabhSecCertPsCert
     СИНТАКСИС     X509Certificate
     MAX-ACCESS    только для чтения
     СТАТУС        текущий
     ОПИСАНИЕ
       "Сертификат PS, DER-кодированный согласно X.509."
     ССЫЛКА
       "Секция 11.3.2.2 спецификации безопасности "
     ::= { cabhSecCertObjects 1 }

--
-- группа уведомления оставлена для дальнейшего расширения.
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecNotification ::= { cabhSecMib 3 0 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecConformance  ::= { cabhSecMib 4 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecCompliances  ::= { cabhSecConformance 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhSecGroups   ::= { cabhSecConformance 2 }

--
--   Группа уведомления
```

```
--

-- заявления о соответствии

МОДУЛЬ СООТВЕТСТВИЯ cabhSecBasicCompliance
     СТАТУС  текущий
     ОПИСАНИЕ
       "Заявление о соответствии для свойства Кабельной межсетевой защиты."
     МОДУЛЬ  --cabhSecMib

-- безоговорочно обязательные группы

     ОБЯЗАТЕЛЬНЫЕ ГРУППЫ {
       cabhSecFwGroup
     }

::= { cabhSecCompliances 3 }

ГРУППА ОБЪЕКТА cabhSecGroup
     ОБЪЕКТЫ {
       cabhSecFwPolicyFileEnable,
       cabhSecFwPolicyFileURL,
       cabhSecFwPolicyFileHash,
       cabhSecFwPolicyFileOperStatus,
       cabhSecFwPolicyFileCurrentVersion,

       cabhSecFwEventType1Enable,
       cabhSecFwEventType2Enable,
       cabhSecFwEventType3Enable,
       cabhSecFwEventAttackAlertThreshold,
       cabhSecFwEventAttackAlertPeriod,
       cabhSecCertPsCert
     }
     СТАТУС  текущий
     ОПИСАНИЕ
       "Группа объектов в базе MIB Кабельных средств межсетевой защиты"
     ::= { cabhSecGroups 1 }

КОНЕЦ
```

E.4 Definition MIB

База MIB определения ОБЯЗАНА быть осуществлена так, как определено ниже.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     enterprises
                                   FROM SNMPv2-SMI;

cableLabs MODULE-IDENTITY
     ПОСЛЕДНЕЕ ОБНОВЛЕНИЕ    "0201310000Z" -- Январь 31, 2002
     ORGANIZATION       "CableLabs"
     CONTACT -INFO
       "Ralph Brown
       Почтовый адрес: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
       U.S.A.
       Телефон: +1 303-661-9100
       Факс: +1 303-661-9199
       E-mail: r.brown@cablelabs.com"
```

```
     ОПИСАНИЕ
       "Этот модуль MIB поставляет основные категории объектов административного
       управления для Кабельных лабораторий.

     ::= { enterprises 4491 }

ИДЕНТИФИКАТОР ОБЪЕКТА clabFunction ::= { cableLabs 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА clabFuncMib2    ::= { clabFunction 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА clabFuncProprietary  ::= { clabFunction 2 }
ИДЕНТИФИКАТОР ОБЪЕКТА clabProject::= { cableLabs 2 }
ИДЕНТИФИКАТОР ОБЪЕКТА clabProjDocsis ::= { clabProject 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА clabProjPacketCable  ::= { clabProject 2 }
ИДЕНТИФИКАТОР ОБЪЕКТА clabProjOpenCable ::= { clabProject 3 }
ИДЕНТИФИКАТОР ОБЪЕКТА clabProjCableHome::= { clabProject 4 }

КОНЕЦ
```

E.5 База MIB Кабельного портала (CDP) протокола DHCP

База MIB портала CDP ОБЯЗАНА быть осуществлена так, как определяется ниже.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     OBJECT-TYPE,
       Integer32,
       Unsigned32
                                FROM SNMPv2-SMI
     TruthValue,
       TimeStamp,
       DisplayString,
     RowStatus,
     TEXTUAL-CONVENTION
                                FROM SNMPv2-TC
     OBJECT-GROUP,
     MODULE-COMPLIANCE
                                FROM SNMPv2-CONF
     InetAddressType,
     InetAddress,
     InetAddressIPv4,
     InetAddressIPv6
                                FROM INET-ADDRESS-MIB
     clabProjCableHome
                                FROM CLAB-DEF-MIB;

--=============================================================================
--
--   Хронология:
--
--
--
--=============================================================================

ИМЕНОВАНИЕ МОДУЛЯ cabhCdpMib
     ПОСЛЕДНЕЕ ОБНОВЛЕНИЕ    "0112190000Z" -- Декабрь 19, 2001 года
     ORGANIZATION  "Cable NMP Group"
     CONTACT-INFO
       "Kevin Luehrs
       Почтовый адрес: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
       U.S.A.
       Телефон: +1 303-661-9100
```

```
      Факс: +1 303-661-9199
      E-mail: k.luehrs@cablelabs.com"
    ОПИСАНИЕ
      "Этот модуль MIB поставляет основные объекты административного управления
      для портала CDP и частей CAP из базы данных PS.

      Подтверждения:
      "
    ::= { clabProjCableHome 4 }

-- Текстовые соглашения
CabhCdpLanTransDhcpClientId ::= ТЕКСТОВОЕ СОГЛАШЕНИЕ
    СТАТУС  текущий
    ОПИСАНИЕ
      "Информация варианта 61 DHCP LAN-Trans."
    СТРОКА ОКТЕТА СИНТАКСИСА (РАЗМЕР (1..80))

--
-- предполагает, что административное управление загрузкой программного
-- обеспечения (SW)протокола SNMPv3 осуществляется только по DOCSIS 1.1
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpObjects   ::= { cabhCdpMib 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpBase ::= { cabhCdpObjects 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpAddr ::= { cabhCdpObjects 2 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpServer ::= { cabhCdpObjects 3 }
--
--   Следующая группа описывает основные объекты в Кабельном портале
--   DHCP. Остальная часть этой группы имеет дело с адресами, определенными
--   на стороне LAN.
--

ТИП ОБЪЕКТА cabhCdpSetToFactory
    СИНТАКСИС     TruthValue
    MAX-ACCESS    для чтения и записи
    СТАТУС        текущий
    DESCRIPTION
      "Установка этого объекта в значение" истинно"(1) вызывает варианты DHCP по
      умолчанию, подлежащие возврату обратно к фабричным значениям по
      умолчанию, а все текущие преобразования должны использовать фабричные
      установки по умолчанию в следующее время обновления. Чтение этого объекта
      всегда возвращает значение "ложно"(2). Когда объект cabhCdpDhcpReset
     установлен в значение "истинно", происходит следующее:
      1) Установить все варианты DHCP CDS по умолчанию в фабричные значения по
         умолчанию.
      2) CDS будет предлагать фабричные варианты выбора DHCP по умолчанию
      в следующее время обновления аренды.
         Объектами, установленными в фабричные значения по умолчанию, являются:
         cabhCdpLanTransThreshold,
         cabhCdpLanTransAction,

         cabhCdpLanPoolStart,
         cabhCdpLanPoolEnd,
         cabhCdpServerSubnetMask,
         cabhCdpServerTimeOffset,
         cabhCdpServerRouter,
         cabhCdpServerDnsAddress,
         cabhCdpServerSyslogAddress,
         cabhCdpServerDomainName,
         cabhCdpServerTTL,
         cabhCdpServerInterfaceMTU,
         cabhCdpServerVendorSpecific,
         cabhCdpServerLeaseTime,
         cabhCdpServerDhcpAddress"
```

```
     ССЫЛКА
       ""
     ::= { cabhCdpBase 1 }

ТИП ОБЪЕКТА cabhCdpLanTransCurCount
     СИНТАКСИС     Unsigned32
     MAX-ACCESS  только для чтения
     СТАТУС      текущий
     ОПИСАНИЕ
       "Текущее число адресов IP LAN-Trans IP для транслируемых
       адресов (Взаимных соединений NAT и NAPT).
       Это подсчет адресов стороны сети WAN."
       ССЫЛКИ
          ""
     ::= { cabhCdpBase 2 }

ТИП ОБЪЕКТА cabhCdpLanTransThreshold
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО (1..65533)
     MAX-ACCESS    для чтения и записи
     СТАТУС    текущий
     ОПИСАНИЕ
       "Пороговое число адресов IP LAN-Trans, распределенных или назначенных,
       выше числа, при котором ОБЯЗАНО быть порождено состояние тревоги.
       Всякий раз, когда попытка распределить адрес IP LAN-Trans, когда
       объект cabhCdpLanTransCurCount более или равен
       объекту cabhCdpLanTransThreshold, событие порождается.
       Для адресов класса C в качестве значения по умолчанию используется 253.
       Для адресов класса B в качестве значения по умолчанию используется 65533.
       В любом случае эта установка выключает свойство."
       ССЫЛКА
          ""
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 65533 }
     ::= { cabhCdpBase 3 }

ТИП ОБЪЕКТА cabhCdpLanTransAction
     СИНТАКСИС     ЦЕЛОЕ ЧИСЛО {
                         normal              (1),
                         noAssignment             (2)
                              }
     MAX-ACCESS  для чтения и записи
     СТАТУС      текущий
     ОПИСАНИЕ
       "Предпринимаемое действие, когда CDS назначает адрес LAN-Trans
       и число назначенных адресов LAN-Trans, (cabhCdpLanTransCurCount),
       больше, чем порог cabhCdpLanTransThreshold).Действия являются следующими:

          нормальное -       назначить адрес LAN-Trans и обработать
                             взаимное соединение между сетями LAN и WAN, как это
                             бы  нормально происходило, если бы порог не был
                             превышен.

          noAssignment -     не назначать адрес IP LAN-Trans и не создавать
                             взаимное соединение."
     ССЫЛКА
       ""
     ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { нормальное }
     ::= { cabhCdpBase 4 }

--
--   Таблицы административного управления адресом CDP
--
--=================================================================
--
--   cabhCdpLanAddrTable (Таблица адресов LAN CDP)
```

```
--
--   Объект cabhCdpLanAddrTable содержит параметры DHCP для каждого адреса
--   IP, обслуживаемого для области LAN-Trans.
--
--   Эта таблица содержит перечень записей для параметров CDP стороны LAN.
--
--================================================================================

ТИП ОБЪЕКТА cabhCdpLanAddrTable
     СИНТАКСИС   ПОСЛЕДОВАТЕЛЬНОСТЬ ИЗ CabhCdpLanAddrEntry
     MAX-ACCESS  не является доступным
     СТАТУС    текущий
     ОПИСАНИЕ
       "Эта таблица является перечнем параметров области LAN-Trans. Этот перечень
       имеет одну запись для каждого распределенного адреса IP LAN-Trans."
     ::= { cabhCdpAddr 1 }

ТИП ОБЪЕКТА cabhCdpLanAddrEntry
     СИНТАКСИС      CabhCdpLanAddrEntry
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Перечень общих параметров для преобразований CDP."
     ИНДЕКС { cabhCdpLanAddrIpType, cabhCdpLanAddrIp }
     ::= { cabhCdpLanAddrTable 1 }

CabhCdpLanAddrEntry ::= ПОСЛЕДОВАТЕЛЬНОСЬБ {
     cabhCdpLanAddrIpType         InetAddressType,
       cabhCdpLanAddrIp               InetAddress,
       cabhCdpLanAddrClientId              CabhCdpLanTransDhcpClientId,
       cabhCdpLanAddrCreateTime   TimeStamp,
       cabhCdpLanAddrExpireTime   TimeStamp,
       cabhCdpLanAddrMethod           ЦЕЛОЕ ЧИСЛО,
       cabhCdpLanAddrHostName         DisplayString,
       cabhCdpLanAddrRowStatus        RowStatus
     }

ТИП ОБЪЕКТА cabhCdpLanAddrIpType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса, назначенный на стороне LAN для Таблицы адресов CDP."
     ::= { cabhCdpLanAddrEntry 1 }

ТИП ОБЪЕКТА cabhCdpLanAddrIp
     СИНТАКСИС      InetAddress
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адрес, назначенный на стороне LAN для таблицы адресов CDP."
     ::= { cabhCdpLanAddrEntry 2 }

ТИП ОБЪЕКТА cabhCdpLanAddrClientID
     СИНТАКСИС      CabhCdpLanTransDhcpClientId
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Идентификатор ID клиента, как указано в Варианте 61 DHCP Discover.
       Имеется однозначное соответствие между идентификатором ID клиента и
       назначенным адресом."
     ::= { cabhCdpLanAddrEntry 3 }

ТИП ОБЪЕКТА cabhCdpLanAddrCreateTime
```

```
     СИНТАКСИС      TimeStamp
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Время, когда была создана сторона LAN Таблицы LAN CDP. Эта запись
       устанавливается только тогда, когда создается запись cabhCdpLanAddrTable
       и запись еще не существует. Другими словами, это значение
       не переписывается во время обновления аренды."
     ::= { cabhCdpLanAddrEntry 4 }

ТИП ОБЪЕКТА cabhCdpLanAddrExpireTime
     СИНТАКСИС      TimeStamp
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Это время, когда истекает аренда стороны LAN. Когда аренда истекает,
       эта запись будет исключена из таблицы."
     ::= { cabhCdpLanAddrEntry 5 }

ТИП ОБЪЕКТА cabhCdpLanAddrMethod
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛОR {
                    cmp           (1),
                    cdp           (2)
                    }
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
       "Метод, который создал эту Адресную запись. Значение cmp
       указывает, что этот ряд (запись) установила конфигурация через CMP.
     Значение cdp указывает, что этот ряд (запись) установило обнаружение DHCP."
     ::= { cabhCdpLanAddrEntry 6 }

ТИП ОБЪЕКТА cabhCdpLanAddrHostName
     СИНТАКСИС      DisplayString(SIZE(0..80))
     MAX-ACCESS     только для чтения
     СТАТУС         текущий
     ОПИСАНИЕ
      "Это название главного узла адреса IP сети LAN, основанное на варианте
      выбора 12 протокола DCHP."
     ::= { cabhCdpLanAddrEntry 7 }

ТИП ОБЪЕКТА cabhCdpLanAddrRowStatus
     СИНТАКСИС      RowStatus
     MAX-ACCESS     для чтения и создания
     СТАТУС         текущий
     ОПИСАНИЕ
       "Взаимная блокировка RowStatus для создания и исключения."
     ::= { cabhCdpLanAddrEntry 8 }
--=========================================================================
--
--   cabhCdpWanDataAddrTable (Адресная таблица WAN-Data CDP)
--
--   Объект cabhCdpWanDataAddrTable содержит параметры конфигурации или DHCP
--   для каждого преобразования адреса IP по каждому адресу IP WAN-Data.
--
--=========================================================================

ТИП ОБЪЕКТА cabhCdpWanDataAddrTable
     СИНТАКСИС      ПОСЛЕДОВАТЕЛЬНОСТЬ ИЗ CabhCdpWanDataAddrEntry
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Эта таблица содержит информацию адресной области WAN-Data."
     ::= { cabhCdpAddr 2 }
```

```
ТИП ОБЪЕКТА cabhCdpWanDataAddrEntry
     СИНТАКСИС      CabhCdpWanDataAddrEntry
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Перечень общих параметров для адресной области WAN-Data CDP."
     ИНДЕКС { cabhCdpWanDataAddrIndex }
     ::= { cabhCdpWanDataAddrTable 1 }

CabhCdpWanDataAddrEntry ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
       cabhCdpWanDataAddrIndex                  ЦЕЛОЕ ЧИСЛО,
       cabhCdpWanDataAddrClientId               СТРОКА ОКТЕТА,
       cabhCdpWanDataAddrIpType                 InetAddressType,
       cabhCdpWanDataAddrIp                     InetAddress,
       cabhCdpWanDataAddrRenewalTime            Integer32,
       cabhCdpWanDataAddrRowStatus              RowStatus
     }

ТИП ОБЪЕКТА cabhCdpWanDataAddrIndex
     СИНТАКСИС      ЦЕЛОЕ ЧИСЛО (1..65535)
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Индекс в таблице."
     ::= { cabhCdpWanDataAddrEntry 1 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrClientId
     СТРОКА ОКТЕТА СИНТАКСИСА (РАЗМЕР (1..80))
     MAX-ACCESS     для чтения и создания
     СТАТУС         текущий
     ОПИСАНИЕ
       "Уникальный идентификатор ID клиента WAN-Data, используемый тогда, когда
       запрашивается Адрес IP WAN-Data через DHCP."
     ::= { cabhCdpWanDataAddrEntry 2 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrIpType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     для чтения и создания
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса, назначенный на стороне WAN-Data."
     ::= { cabhCdpWanDataAddrEntry 3 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrIp
     СИНТАКСИС      InetAddress
     MAX-ACCESS     для чтения и создания
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адрес, назначенный на стороне WAN-Data."
     ::= { cabhCdpWanDataAddrEntry 4 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrRenewalTime
     СИНТАКСИС      Integer32
     MAX-ACCESS     для чтения и создания
     СТАТУС         текущий
     ОПИСАНИЕ
       "Это время, остающееся перед тем, как истекает аренда.
       Это основывается на Варианте выбора 51 протокола DHCP."
     ::= { cabhCdpWanDataAddrEntry 5 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrRowStatus
     СИНТАКСИС      RowStatus
     MAX-ACCESS     для чтения и создания
```

```
     СТАТУС        текущий
     ОПИСАНИЕ
       "Взаимная блокировка RowStatus для создания и исключения."
     ::= { cabhCdpWanDataAddrEntry 6 }

--============================================================================
--
--   cabhCdpWanDataAddrServerTable (Таблица сервера DNS WAN-Data CDP)
--
--   Объект cabhCdpWanDataAddrServerTable содержит таблицу направления серверов
--   DNS.              .

--============================================================================

ТИП ОБЪЕКТА cabhCdpWanDataAddrServerTable
     СИНТАКСИС     ПОСЛЕДОВАТЕЛЬНОСТЬ ИЗ CabhCdpWanDataAddrServerEntry
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
       "Это содержит адреса IP, используемые для ведущих узлов DNS WAN-Data,
       полученные через вариант выбора 6 протокола DHCP во время процесса WAN-
       Data."
     ::= { cabhCdpAddr 3 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrServerEntry
     СИНТАКСИС     CabhCdpWanDataAddrServerEntry
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
       "Перечень ведущих узлов DNS WAN-Data."
     ИНДЕКС { cabhCdpWanDataAddrDnsIpType, cabhCdpWanDataAddrDnsIp }
     ::= { cabhCdpWanDataAddrServerTable 1 }

CabhCdpWanDataAddrServerEntry ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
     cabhCdpWanDataAddrDnsIpType      InetAddressType,
     cabhCdpWanDataAddrDnsIp               InetAddress,
     cabhCdpWanDataAddrDnsRowStatus             RowStatus
     }

ТИП ОБЪЕКТА cabhCdpWanDataAddrDnsIpType
     СИНТАКСИС     InetAddressType
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
       "Этот параметр указывает тип адреса IP сервера DNS."
       ::= { cabhCdpWanDataAddrServerEntry 1 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrDnsIp
     СИНТАКСИС     InetAddress
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
       "Этот параметр указывает адрес IP сервера DNS."
       ::= { cabhCdpWanDataAddrServerEntry 2 }

ТИП ОБЪЕКТА cabhCdpWanDataAddrDnsRowStatus
     СИНТАКСИС     RowStatus
     MAX-ACCESS    для чтения и создания
     СТАТУС        текущий
     ОПИСАНИЕ
       "Взаимная блокировка RowStatus для создания и исключения."
          ::= { cabhCdpWanDataAddrServerEntry 3 }

--
```

```
  -- Значения вариантов выбора стороны сервера DHCP (CDS, DHCP Server Side) для
       области LAN-Trans
--
ТИП ОБЪЕКТА cabhCdpLanPoolStartType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса начала диапазона Адресов IP LAN-Trans."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
     ::= { cabhCdpServer 1 }

ТИП ОБЪЕКТА cabhCdpLanPoolStart
     СИНТАКСИС      InetAddress
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Начало диапазона адресов IP LAN-Trans."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 'c0a8000a'h } -- 192.168.0.10
              -- 192.168.0.0 есть сетевое число
                                        -- 192.168.0.255 есть адрес широковещания
                                        -- и 192.168.0.1 резервируется для
                                        -- маршрутизатора
     ::= { cabhCdpServer 2 }

ТИП ОБЪЕКТА cabhCdpLanPoolEndType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса конца диапазона Адресов IP LAN-Trans."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
     ::= { cabhCdpServer 3 }

ТИП ОБЪЕКТА cabhCdpLanPoolEnd
     СИНТАКСИС      InetAddress
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Конец диапазона для адресов IP LAN-Trans."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 'c0a800fe'h } -- 192.168.0.254
     ::= { cabhCdpServer 4 }

ТИП ОБЪЕКТА cabhCdpServerSubnetMaskType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип маски подсети LAN-Trans."
     ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
     ::= { cabhCdpServer 5 }

ТИП ОБЪЕКТА cabhCdpServerSubnetMask
     СИНТАКСИС      InetAddress
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Значение 1 варианта выбора – Значение маски подсети LAN-Trans."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 'ffffff00'h }    -- 255.255.255.0
     ::= { cabhCdpServer 6 }

ТИП ОБЪЕКТА cabhCdpServerTimeOffset
      СИНТАКСИС             Integer32 (-86400..86400) -- от 0 до 24 часов (в
      секундах)
```

```
     ЕДИНИЦЫ        "секунды"
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Значение 2 варианта выбора - Значение смещения времени LAN-Trans от
       скоординированного мирового времени (UTC, Coordinated Universal Time)."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 0 }          -- UTC
     ::= { cabhCdpServer 7 }

ТИП ОБЪЕКТА cabhCdpServerRouterType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса, Маршрутизатор для адресной области LAN-Trans."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
     ::= { cabhCdpServer 8 }

ТИП ОБЪЕКТА cabhCdpServerRouter
     СИНТАКСИС      InetAddress
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
      "Значение 3 варианта выбора – Маршрутизатор для адресной области LAN-
      Trans."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 'c0a80001'h } -- 192.168.0.1
     ::= { cabhCdpServer 9 }

ТИП ОБЪЕКТА cabhCdpServerDnsAddressType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адресов IP серверов DNS адресной области LAN-Trans."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
     ::= { cabhCdpServer 10 }

ТИП ОБЪЕКТА cabhCdpServerDnsAddress
     СИНТАКСИС      InetAddress
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адреса IP серверов DNS адресной области LAN-Trans. По умолчанию
      имеется только один сервер DNS, и это есть адрес, указанный в значении 3
      варианта выбора - cabhCdpServerRouter. Указывается только один адрес."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 'c0a80001'h } -- 192.168.0.1
     ::= { cabhCdpServer 11 }

ТИП ОБЪЕКТА cabhCdpServerSyslogAddressType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса IP серверов SYSLOG LAN-Trans."
          ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
     ::= { cabhCdpServer 12 }

ТИП ОБЪЕКТА cabhCdpServerSyslogAddress
     СИНТАКСИС      InetAddress
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адреса IP серверов SYSLOG LAN-Trans.
       По умолчанию серверы SYSLOG отсутствуют.
```

```
      Фабричные значения по умолчанию содержат индикацию
      отсутствия значения сервера Syslog, которое равняется (0.0.0.0)."
         ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { '00000000'h } -- 0.0.0.0
    ::= { cabhCdpServer 13 }

ТИП ОБЪЕКТА cabhCdpServerDomainName
     СИНТАКСИС      DisplayString(РАЗМЕР(0..128))
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
       "Значение 15 варианта выбора – Название домена адресной области LAN-
       Trans."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ {""}
       ::= { cabhCdpServer 14 }

ТИП ОБЪЕКТА cabhCdpServerTTL
       СИНТАКСИС         ЦЕЛОЕ ЧИСЛО (0..255)
       MAX-ACCESS        для чтения и записи
       СТАТУС            текущий
       ОПИСАНИЕ
       "Значение 23 варианта выбора – Время существования LAN-Trans."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 64 }
       ::= { cabhCdpServer 15 }

ТИП ОБЪЕКТА cabhCdpServerInterfaceMTU
       СИНТАКСИС              ЦЕЛОЕ ЧИСЛО (68..4096)
       MAX-ACCESS             для чтения и записи
       СТАТУС                 текущий
       ОПИСАНИЕ
       "Значение 26 варианта выбора – MTU интерфейс LAN-Trans."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 1500 }
       ::= { cabhCdpServer 16 }

ТИП ОБЪЕКТА cabhCdpServerVendorSpecific
       СИНТАКСИС              СТРОКА ОКТЕТА (РАЗМЕР(0..255))
       MAX-ACCESS             для чтения и записи
       СТАТУС                 текущий
       ОПИСАНИЕ
       " Значение 43 варианта выбора – Варианты выбора, зависящие от поставщика."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ''h }
       ::= { cabhCdpServer 17 }

ТИП ОБЪЕКТА cabhCdpServerLeaseTime
       СИНТАКСИС         Unsigned32
       UNITS             "seconds"
       MAX-ACCESS        для чтения и записи
     СТАТУС   текущий
     ОПИСАНИЕ
       "Значение 51 варианта выбора – Время аренды по умолчанию LAN-Trans
       (секунды)."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 60 }
       ::= { cabhCdpServer 18 }

ТИП ОБЪЕКТА cabhCdpServerDhcpAddressType
       СИНТАКСИС         InetAddressType
       MAX-ACCESS        для чтения и записи
     СТАТУС              текущий
     ОПИСАНИЕ
       "Значение 54 варианта выбора – Тип адреса IP сервера DHCP LAN-Trans."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { ipv4 }
       ::= { cabhCdpServer 19 }

ТИП ОБЪЕКТА cabhCdpServerDhcpAddress
       СИНТАКСИС              InetAddress
```

```
      MAX-ACCESS       для чтения и записи
    СТАТУС             текущий
    ОПИСАНИЕ
      "Значение 54 варианта выбора – Адрес IP сервера DHCP LAN-Trans. Он
      устанавливается по умолчанию в адрес маршрутизатора, как указано в
       в cabhCdpServerRouter. На альтернативной основе поставщик может иметь
       желание отделить адрес CDS от адреса маршрутизатора."
       ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 'c0a80001'h }     --    192.168.0.1
       ::= { cabhCdpServer 20 }

--
-- группа уведомления оставлена для дальнейшего расширения.
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpNotification ::= { cabhCdpMib 2 0 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpConformance   ::= { cabhCdpMib 3 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpCompliances   ::= { cabhCdpConformance 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCdpGroups        ::= { cabhCdpConformance 2 }

--
--   Группа уведомления
--

-- заявления о соответствии

СООТВЕТСТВИЕ МОДУЛЯ cabhCdpBasicCompliance
    СТАТУС  текущий
    ОПИСАНИЕ
      "Заявление о соответствии для устройств, которые осуществляют свойство
      свойство MTA."
    МОДУЛЬ -- cabhCdpMib

-- безоговорочно обязательные группы

    ОБЯЗАТЕЛЬНЫЕ ГРУППЫ {
      cabhCdpGroup
    }

::= { cabhCdpCompliances 3 }

ГРУППА ОБЪЕКТА cabhCdpGroup
    ОБЪЕКТЫ {
      cabhCdpSetToFactory,
         cabhCdpLanTransCurCount,
      cabhCdpLanTransThreshold,
      cabhCdpLanTransAction,

         cabhCdpLanAddrIpType,
         cabhCdpLanAddrIp,
         cabhCdpLanAddrClientID,
         cabhCdpLanAddrCreateTime,
         cabhCdpLanAddrExpireTime,
         cabhCdpLanAddrMethod,
         cabhCdpLanAddrHostName,
         cabhCdpLanAddrRowStatus,

         cabhCdpWanDataAddrIndex,
         cabhCdpWanDataAddrClientId,
         cabhCdpLanAddrIpType,
         cabhCdpWanDataAddrIp,
         cabhCdpWanDataAddrRenewalTime,
         cabhCdpWanDataAddrRowStatus,

         cabhCdpWanDataAddrDnsIpType,
```

```
        cabhCdpWanDataAddrDnsIp,
        cabhCdpWanDataAddrDnsRowStatus,

        cabhCdpLanPoolStartType,
        cabhCdpLanPoolStart,
        cabhCdpLanPoolEndType,
        cabhCdpLanPoolEnd,
        cabhCdpServerSubnetMaskType,
        cabhCdpServerSubnetMask,
        cabhCdpServerTimeOffset,
        cabhCdpServerRouterType,
        cabhCdpServerRouterType,
        cabhCdpServerRouter,
        cabhCdpServerDnsAddressType,
        cabhCdpServerDnsAddress,
        cabhCdpServerSyslogAddressType,
        cabhCdpServerSyslogAddress,
        cabhCdpServerDomainName,
        cabhCdpServerTTL,
        cabhCdpServerInterfaceMTU,
        cabhCdpServerVendorSpecific,
        cabhCdpServerLeaseTime,
        cabhCdpServerDhcpAddressType,
        cabhCdpServerDhcpAddress
            }
    СТАТУС  текущий
    ОПИСАНИЕ
      "Группа объектов для базы MIB Кабельного CDB."
    ::= { cabhCdpGroups 1 }

КОНЕЦ
```

E.6 Портал кабельного адреса

База MIB портала CAP ОБЯЗАНА быть осуществлена так, как определено ниже.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
      Unsigned32
                            FROM SNMPv2-SMI
      TimeStamp,
      TruthValue,
      RowStatus,
      PhysAddress
                            FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE
                            FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetAddressIPv4,
    InetAddressIPv6
                            FROM INET-ADDRESS-MIB

    clabProjCableHome
                            FROM CLAB-DEF-MIB;
```

```
--=============================================================================
--
--   Хронология:
--
--
--=============================================================================

ИМЕНОВАНИЕ МОДУЛЯ cabhCapMib
     ПОСЛЕДНЕЕ ОБНОВЛЕНИЕ    "0112190000Z" – 19 декабря, 2001 года
     ORGANIZATION  "Cable NMP Group"
     CONTACT-INFO
       "Kevin Luehrs
       Почтовый адрес: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
       U.S.A.
       телефон: +1 303-661-9100
       Факс: +1 303-661-9199
       E-mail: k.luehrs@cablelabs.com"
     ОПИСАНИЕ
       "Этот модуль MIB поставляет основные объекты административного управления
       для портала CDP и частей портала CAP в базе данных PS.

       Подтверждения:
       "
     ::= { clabProjCableHome 3 }

-- Текстовые соглашения

CabhCapPacketMode ::= ТЕКСТОВОЕ СОГЛАШЕНИЕ
     СТАТУС   текущий
     ОПИСАНИЕ
       "Тип данных, установленный тогда, когда
       устанавливается связывание/преобразование."
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО {
                    napt           (1), -- NAT с трансляцией порта
                    nat            (2), -- Основная трансляция NAT
                    passthrough    (3), -- Сквозной внешний адрес
                    }

--
-- предполагает, что административное управление загрузкой программного
-- обеспечения SW протокола SNMPv3 осуществляется только по DOCSIS 1.1
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhCapObjects ::= { cabhCapMib 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCapBase::= { cabhCapObjects 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCapMap ::= { cabhCapObjects 2 }
--=============================================================================
--
-- Общие параметры CAP
--
--=============================================================================

ТИП ОБЪЕКТА cabhCapTcpTimeWait
     СИНТАКСИС      Unsigned32
       ЕДИНИЦЫ      "секунды"
     MAX-ACCESS     для чтения и записи
     СТАТУС         текущий
     ОПИСАНИЕ
      "Максимальное время ожидания перед тем, как предположить, что сеанс TCP
      завершен."
```

```
      ССЫЛКА
         ""
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 240 }       -- 4 минуты
    ::= { cabhCapBase 1 }

ТИП ОБЪЕКТА cabhCapUdpTimeWait
    СИНТАКСИС     Unsigned32
      ЕДИНИЦЫ     "секунды"
    MAX-ACCESS    для чтения и записи
    СТАТУС        текущий
    ОПИСАНИЕ
     "Максимальное время ожидания перед тем, как предположить, что сеанс UDP
     завершен."
      ССЫЛКА
         ""
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 86400 }-- 1 день
    ::= { cabhCapBase 2 }

ТИП ОБЪЕКТА cabhCapIcmpTimeWait
    СИНТАКСИС     Unsigned32
      ЕДИНИЦЫ     "секунды"
    MAX-ACCESS    для чтения и записи
    СТАТУС        текущий
    ОПИСАНИЕ
     " Максимальное время ожидания перед тем, как предположить, что сеанс Icmp
     завершен."
      ССЫЛКА
         ""
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { 86400 }-- 1 день
    ::= { cabhCapBase 3 }

ТИП ОБЪЕКТА cabhCapPrimaryMode
    СИНТАКСИС          CabhCapPacketMode
    MAX-ACCESS         для чтения и записи
    СТАТУС             текущий
    ОПИСАНИЕ
      "Режим первичной обработки пакетов, подлежащий использованию."
      ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ { napt }
    ::= { cabhCapBase 4 }
ТИП ОБЪЕКТА cabhCapSetToFactory
    СИНТАКСИС          TruthValue
    MAX-ACCESS         для чтения и записи
    СТАТУС             текущий
    ОПИСАНИЕ
      "Установка этого объекта в значение "истинно" (1) заставляет очистить все
      таблицы в CAP, а все объекты CAP со значениями по умолчанию должны быть
      переустановлены  обратно в их значения по умолчанию."
    ::= { cabhCapBase 5 }
--=========================================================================
--
--   cabhCapMappingTable (Таблица преобразования CAP)
--
-- Объект cabhCapMappingTable содержит преобразования для всех преобразований
-- CAP.
--
--=========================================================================

ТИП ОБЪЕКТА cabhCapMappingTable
      СИНТАКСИС            ПОСЛЕДОВАТЕЛЬНОСТЬ ИЗ CabhCapMappingEntry
    MAX-ACCESS  не является доступным
    СТАТУС      текущий
    ОПИСАНИЕ
     "Эта таблица содержит преобразования адресов IP для всех преобразований
     CAP."
```

```
     ::= { cabhCapMap 1 }

ТИП ОБЪЕКТА cabhCapMappingEntry
     СИНТАКСИС      CabhCapMappingEntry
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Перечень преобразований IP CAP."
     ИНДЕКС { cabhCapMappingWanAddrType, cabhCapMappingWanAddr,
     cabhCapMappingWanPort,
       cabhCapMappingLanAddrType, cabhCapMappingLanAddr, cabhCapMappingLanPort}
     ::= { cabhCapMappingTable 1 }

CabhCapMappingEntry ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
     cabhCapMappingWanAddrType        InetAddressType,
       cabhCapMappingWanAddr          InetAddress,
       cabhCapMappingWanPort          ЦЕЛОЕ ЧИСЛО,
       cabhCapMappingLanAddrType      InetAddressType,
       cabhCapMappingLanAddr          InetAddress,
       cabhCapMappingLanPort          ЦЕЛОЕ ЧИСЛО,
       cabhCapMappingMode             CabhCapPacketMode,
       cabhCapMappingMethod           ЦЕЛОЕ ЧИСЛО,
       cabhCapMappingProtocol         ЦЕЛОЕ ЧИСЛО
       }

ТИП ОБЪЕКТА cabhCapMappingWanAddrType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса IP, назначенный на стороне WAN. Обычно используется версия 4
       IP."
     ::= { cabhCapMappingEntry 1 }

ТИП ОБЪЕКТА cabhCapMappingWanAddr
     СИНТАКСИС      InetAddress
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Адрес IP, назначенный на стороне WAN. Обычно используется версия 4
       IP."
     ::= { cabhCapMappingEntry 2 }

ТИП ОБЪЕКТА cabhCapMappingWanPort
     СИНТАКСИС      ЦЕЛОЕ ЧИСЛО (1..65535)
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Номер порта TCP/UDP на стороне WAN."
     ::= { cabhCapMappingEntry 3 }

ТИП ОБЪЕКТА cabhCapMappingLanAddrType
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
     ОПИСАНИЕ
       "Тип адреса IP, назначенный на стороне LAN. Обычно используется
       версия 4 IP."
     ::= { cabhCapMappingEntry 4 }

ТИП ОБЪЕКТА cabhCapMappingLanAddr
     СИНТАКСИС      InetAddressType
     MAX-ACCESS     не является доступным
     СТАТУС         текущий
```

```
     ОПИСАНИЕ
       "Тип адреса IP, назначенный на стороне LAN. Обычно используется
       версия 4 IP."
     ::= { cabhCapMappingEntry 5 }

ТИП ОБЪЕКТА cabhCapMappingLanPort
     СИНТАКСИС     ЦЕЛОЕ ЧИСЛО (1..65535)
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
       "Номер порта TCP/UDP на стороне LAN."
     ::= { cabhCapMappingEntry 6 }

ТИП ОБЪЕКТА cabhCapMappingMode
     СИНТАКСИС   CabhCapPacketMode
     MAX-ACCESS    только для чтения
     СТАТУС        текущий
     ОПИСАНИЕ
       "Тип режима обработки пакетов для этого преобразования. Отметим, что эта
       информация могла быть подобрана из адреса IP и информации порта для
       этого преобразования."
     ::= { cabhCapMappingEntry 7 }

ТИП ОБЪЕКТА cabhCapMappingMethod
     СИНТАКСИС          ЦЕЛОЕ ЧИСЛО {
                              статическое   (1),
                              динамическое  (2),
                              }
     MAX-ACCESS    только для чтения
     СТАТУС        текущий
     ОПИСАНИЕ
       "Указывает, как это преобразование было создано. Статическое означает,
     что оно было обеспечено, а динамическое означает, что оно было обработано
     самой услугой PS."
     ::= { cabhCapMappingEntry 8 }

ТИП ОБЪЕКТА cabhCapMappingProtocol
     СИНТАКСИС   ЦЕЛОЕ ЧИСЛО {
                              другое    (1), -- не указывается
                              icmp      (2),
                              udp       (3),
                              tcp       (4)
                              }
     MAX-ACCESS    только для чтения
     СТАТУС        текущий
     ОПИСАНИЕ
       "Протокол для этого преобразования."
     ::= { cabhCapMappingEntry 9 }

--============================================================================
--
--   cabhCapPassthroughTable (Сквозная таблица CAP)
--
--   Объект cabhCapPassthroughTable содержит адреса MAC для всех Устройств
     IP сети LAN, которые будут конфигурированы как сквозные.
--
--============================================================================

ТИП ОБЪЕКТА cabhCapPassthroughTable
     СИНТАКСИС     ПОСЛЕДОВАТЕЛЬНОСТЬ ИЗ CabhCapPassthroughEntry
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
```

```
      "Эта таблица содержит адреса MAC для Устройств IP сети LAN, которые
      конфигурируются как работающие в сквозном режиме."
     ::= { cabhCapMap 2 }

ТИП ОБЪЕКТА cabhCapPassthroughEntry
     СИНТАКСИС     CabhCapPassthroughEntry
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
      "Перечень адресов MAC для Устройств IP сети LAN, которые конфигурируются
      как работающие в сквозном режиме. "
     ИНДЕКС {cabhCapPassthroughMACAddr }
     ::= { cabhCapPassthroughTable 1 }

CabhCapPassthroughEntry ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
     cabhCapPassthroughMACAddr        PhysAddress,
     cabhCapPassthroughRowStatus           RowStatus
     }

ТИП ОБЪЕКТА cabhCapPassthroughMACAddr
     СИНТАКСИС     PhysAddress
     MAX-ACCESS    не является доступным
     СТАТУС        текущий
     ОПИСАНИЕ
      "Перечень адресов MAC для Устройств IP сети LAN, которые конфигурируются
      как работающие в сквозном режиме. "
     ::= {cabhCapPassthroughEntry 1 }

ТИП ОБЪЕКТА cabhCapPassthroughRowStatus
     СИНТАКСИС     RowStatus
     MAX-ACCESS    только для чтения
     СТАТУС        текущий
     ОПИСАНИЕ
       "Взаимная блокировка RowStatus для создания и исключения
       записи cabhCapPassthroughTable."
     ::= { cabhCapPassthroughEntry 2 }

--
-- группа уведомления оставлена для дальнейшего расширения.
--

ИДЕНТИФИКАТОР ОБЪЕКТА cabhCapNotification ::= { cabhCapMib 2 0 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCapConformance ::= { cabhCapMib 3 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCapCompliances ::= { cabhCapConformance 1 }
ИДЕНТИФИКАТОР ОБЪЕКТА cabhCapGroups ::= { cabhCapConformance 2 }

--
-- Группа уведомления
--

-- заявления о соответствии

СООТВЕТСТВИЕ МОДУЛЯ cabhCapBasicCompliance
     СТАТУС   текущий
     ОПИСАНИЕ
       "Заявление о соответствии для устройств, которые осуществляют
       свойство MTA."
     МОДУЛЬ -- cabhCapMib

-- безоговорочно обязательные группы

     ОБЯЗАТЕЛЬНЫЕ ГРУППЫ {
       cabhCapGroup
     }
```

```
::= { cabhCapCompliances 3 }

ГРУППА ОБЪЕКТА cabhCapGroup
     ОБЪЕКТЫ {
       cabhCapTcpTimeWait,
       cabhCapUdpTimeWait,
       cabhCapIcmpTimeWait,
       cabhCapPrimaryMode,

--     cabhCapMappingWanAddrType,
--     cabhCapMappingWanAddr,
--     cabhCapMappingWanPort,
--     cabhCapMappingLanAddrType,
--     cabhCapMappingLanAddr,
--     cabhCapMappingLanPort,
       cabhCapMappingMode,
       cabhCapMappingMethod,
       cabhCapMappingProtocol,

--     cabhCapPassthroughMacAddr
       cabhCapPassthroughRowStatus
       }
     СТАТУС    текущий
     ОПИСАНИЕ
       "Группа объектов для базы MIB CDB."
     ::= { cabhCapGroups 1 }

КОНЕЦ
```

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
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 средства передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	**Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов**
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническая эксплуатация сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническая эксплуатация: 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 и взаимосвязь открытых систем
Серия Y	Глобальная информационная инфраструктура и аспекты межсетевого протокола (IP)
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2004 г.