РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 269 873** (13) **C2**

(51) МПК
H04L 12/28 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2003110438/09, 12.09.2001**

(24) Дата начала действия патента: **12.09.2001**

(30) Приоритет: **13.09.2000 US 09/660,709**

(43) Дата публикации заявки: **20.08.2004**

(45) Опубликовано: **10.02.2006 Бюл. № 4**

(56) Список документов, цитированных в отчете о поиске: **US 5745884, 24.04.1998. RU 2144282 C1, 10.01.2000. US 5960074, 28.09.1999. WO 0052575, 08.09.2000.**

(85) Дата перевода заявки PCT на национальную фазу: **14.04.2003**

(86) Заявка PCT:
US 01/28424 (12.09.2001)

(87) Публикация PCT:
WO 02/23825 (21.03.2002)

Адрес для переписки:
129010, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
СПИРМАН Энтони К.(US),
ТОМПКИНС Эндрю Э.(US)

(73) Патентообладатель(ли):
ВП МЕДИА ИНК (US)

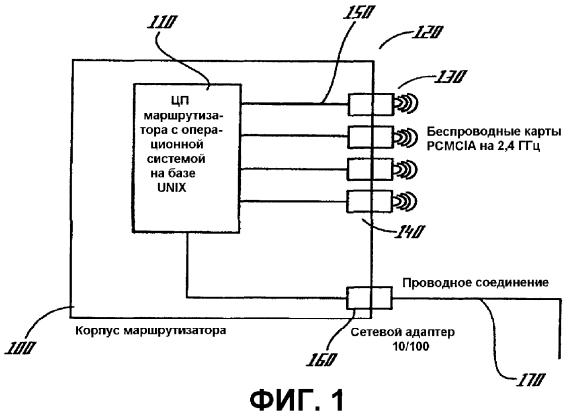
RU 2269873 C2

(54) БЕСПРОВОДНОЕ УСТРОЙСТВО ИНИЦИАЛИЗАЦИИ

(57) Реферат:

Изобретение относится к телекоммуникационному оборудованию. Беспроводное устройство инициализации (БУИ) представляет собой систему администрирования трафика компьютерных данных, способную маршрутизировать трафик TCP/IP с использованием 2.4 ГГц-ого оборудования. Это БУИ, стратегически, подлежит размещению в областях логических сегментов беспроводной сети для облегчения администрирования трафика. Это устройство действует таким образом, чтобы обеспечить возможность соединения между точками беспроводного доступа к магистрали. Устройство может также располагаться в абонентской локальной сети (ЛС), обеспечивая возможность подключения к глобальной сети (ГС). Беспроводное устройство имеет аутентификатор, поддерживающий оперативную связь с операционной системой. Беспроводное устройство способно фильтровать IP-адреса, управлять брандмауэром, и/или маршрутизатором, и/или мостом. Техническим результатом является повышение эффективного пропускания трафика TCP/IP по ГС или ЛС, в то же время обеспечение безопасного администрирования и повышенной связности. 2 н. и 26 з.п. ф-лы, 3 ил.

RU 2269873 C2



ФИГ. 1

RU 2269873 C2

RU 2269873 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 269 873** (13) **C2**

(51) Int. Cl.
H04L 12/28 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2003110438/09, 12.09.2001**

(24) Effective date for property rights: **12.09.2001**

(30) Priority: **13.09.2000 US 09/660,709**

(43) Application published: **20.08.2004**

(45) Date of publication: **10.02.2006 Bull. 4**

(85) Commencement of national phase: **14.04.2003**

(86) PCT application:
US 01/28424 (12.09.2001)

(87) PCT publication:
WO 02/23825 (21.03.2002)

Mail address:
129010, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
SPIRMAN Ehntoni K.(US),
TOMPKINS Ehndrju Eh.(US)

(73) Proprietor(s):
VP MEDIA INK (US)

RU 2269873 C2

(54) WIRELESS INITIALIZATION DEVICE

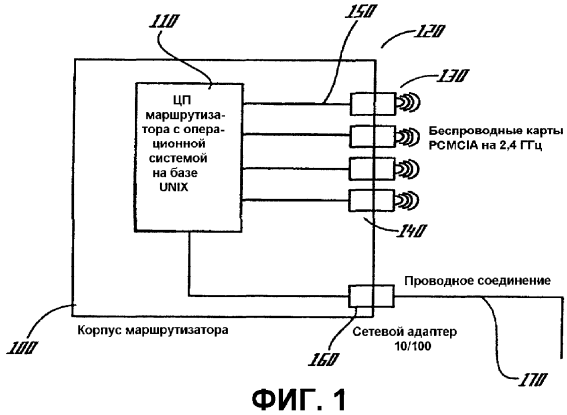
(57) Abstract:

FIELD: engineering of telecommunication equipment.

SUBSTANCE: wireless initialization device is a system for administrating computer data traffic, capable of routing TCP/IP traffic with utilization of 2,4 GHz equipment. Aforementioned wireless initialization device, strategically, is subject to positioning in areas of logical segments of wireless network for facilitation of traffic administration. This device operates to provide for possible connection between wireless access points and main line. Device also may be positioned in client local network, providing possibility of access to global network. Wireless device has authentication means, maintaining operative connection with operation system. Wireless device is capable of filtering IP-addresses, controlling a firewall and/or router and/or bridge.

EFFECT: increased effective TCP/IP traffic capacity for global network or local network, at the same time, realization of safe administration and improved integrity.

2 cl, 3 dwg



ФИГ. 1

RU 2269873 C2

Область техники, к которой относится изобретение

Настоящее изобретение относится к телекоммуникационному оборудованию и, в частности, в предпочтительной форме, к беспроводным устройствам инициализации, выполненным с возможностью маршрутизации трафика TCP/IP с использованием 2,4 ГГц-
5 овой аппаратуры.

Уровень техники

До недавнего времени возможность Интернет-соединения ограничивалась проводными соединениями с облаком Интернета. С появлением более мощных 2,4 ГГц-антенн, стало более практичным обеспечивать беспроводные подключения к компьютерам, которые, в
10 итоге, подключались бы обратно к облаку Интернета. С ростом скорости беспроводного оборудования беспроводные соединения с пользователем стали более экономичными, чем кабельные. В результате, были предприняты попытки заменить проводные глобальные сети (ГС, WAN) высокоскоростными беспроводными соединениями.

В настоящее время беспроводное оборудование представляет собой только мосты. Эти
15 беспроводные мосты содержат одну или две беспроводные карты, в зависимости от производителя, и одно проводное соединение. В некоторых случаях имеются две беспроводные карты и одно проводное соединение. Однако, в связи с быстрым развитием телекоммуникаций, может возникать необходимость в 3 или 4 беспроводных соединениях и 3 или 4 проводных соединениях. Хотя мост хорошо подходит для соединения друг с другом
20 двух или трех локальных сетей (ЛС, LAN), чрезмерное количество мостов не будет работать в протяженной ГС, поскольку современная маршрутизирующая логика имеет теоретический предел работоспособности от 3 до 5 мостов. Таким образом, современные 2,4 ГГц-овые беспроводные точки доступа обеспечивают мосты, которые значительно ограничивают способность пользователя размещать беспроводное оборудование в
25 глобальной сети. 2,4 ГГц-овая беспроводная аппаратура предназначена для создания ЛС с концентраторами и для соединения между собой двух или более небольших ЛС посредством мостов. Она не предназначена для работы в среде ГС общего пользования.

Кроме того, современные беспроводные соединения предназначены для внутреннего пользования, и безопасность связана только с сетевым именем. Альтернативно, систему
30 можно поддерживать закрытой, используя адресацию уровня управления доступом к среде (УДС, MAC). Несмотря на беспроводную функцию, такие решения ЛС предусматривали, что подключений обратно к точке беспроводного доступа сравнительно немного и что соединения являются до некоторой степени стационарными. В результате, для доступа к точке доступа постоянно используется фильтрация УДС. Для вступления в силу нового
35 списка контроля доступа обычно требуется перезагрузка точки доступа. Кроме того, в точке доступа можно разместить конечное количество УДС-адресов. Это существенно ограничивает количество пользователей роуминга, которых можно добавлять в систему. Всякий раз при добавлении нового члена, приходится обновлять и перезагружать каждую точку доступа в сети.

40 Простой протокол сетевого управления (SNMP), позволяющий управлять точкой беспроводного доступа, стал стандартным методом передачи данных. Чтобы модифицировать фильтр УДС, по сети передают административный пароль для доступа к точке доступа. Этот пароль передают в виде чистого текста. В отсутствие соединений защищенной оболочки, подключившись к ГС, можно легко перехватить это сообщение в
45 виде чистого текста. Взлом административного пароля ставит под удар всю систему. В более ранних системах, во избежание подобной ситуации, сетевое имя предоставляли только членам организации. Без сетевого имени беспроводные карты не могут подключиться к точке доступа. В среде общего пользования сетевое имя является общим для всех, кто пользуется услугой, что открывает сравнительно широкие возможности
50 несанкционированного доступа.

Требуется элемент беспроводного оборудования, позволяющий эффективно устанавливать соединения в большой ГС. Также требуется беспроводное устройство инициализации, которое обеспечивает сетевую маршрутизацию на узле-отправителе и

меры безопасности по сети. Кроме того, требуются 2,4 ГГц-овые точки беспроводного доступа, играющие роль мостов, чтобы пользователь имел возможность размещать беспроводное оборудование в глобальной сети. Также требуются беспроводные соединения, предусматривающие внешнее пользование и гибкую защиту. Кроме того, требуется система, способная обеспечивать многочисленные подключения обратно к точке беспроводного доступа без необходимости перезагрузки до добавления в систему новых пользователей роуминга.

Сущность изобретения

Настоящее изобретение предлагает беспроводное устройство инициализации, способное маршрутизировать трафик TCP/IP с использованием 2,4 ГГц-ового оборудования. Это устройство стратегически следует размещать в областях логических сегментов беспроводной сети, чтобы облегчать администрирование трафика данных. Это устройство призвано обеспечивать возможность соединения между беспроводными точками доступа к магистрали. Устройство может также располагаться в абонентских ЛС, обеспечивая возможность подключения к ГС. Согласно предпочтительному варианту осуществления беспроводное устройство имеет всего семь беспроводных сегментов. Беспроводное устройство способно фильтровать IP-адреса, контролировать потребности брандмауэра, и/или маршрутизатора, и/или моста и увеличивает эффективное пропускание трафика TCP/IP по ГС или ЛС, в то же время обеспечивая безопасное администрирование и повышенную связность.

Главной задачей настоящего изобретения является создание элемента беспроводного оборудования, позволяющего эффективно устанавливать соединения в большой ГС.

Другой задачей настоящего изобретения является создание беспроводного устройства инициализации, которое обеспечивает сетевую маршрутизацию на узле-отправителе и меры безопасности по сети. Для этого необходимо обеспечить защищенные соединения между точками беспроводного доступа и к точкам, которые требуют административных соединений.

Еще одной задачей настоящего изобретения является 2,4 ГГц-овые точки беспроводного доступа, играющие роль мостов, чтобы пользователь имел возможность размещать беспроводное оборудование в глобальной сети (ГС).

Еще одной задачей настоящего изобретения является создание беспроводных соединений, предусматривающих внешнее пользование и гибкую защиту. Можно предложить несколько вариантов осуществления настоящего изобретения, позволяющих решить вышеперечисленные задачи, в частности, с применением аутентификации по протоколу RADIUS (службы аутентификации удаленных пользователей по коммутируемым каналам связи). Протокол RADIUS представляет собой метод аутентификации, отличающийся повышенной универсальностью, гибкостью и безопасностью. Процесс аутентификации осуществляется посредством защищенных подключений к центральному серверу. В случае нарушения защиты по какой-либо причине на сервере можно сменить имя пользователя и пароль, внеся изменения в базу данных, а не в аппаратуру. Используя новую операционную систему совместно с современными беспроводными картами, беспроводные устройства можно конфигурировать для логического администрирования посредством защищенных соединений. Кроме того, аутентификацию по протоколу RADUS можно безопасно передавать через беспроводное устройство в защищенную сеть.

Дополнительной задачей настоящего изобретения является создание системы, выполненной с возможностью обеспечения многочисленных подключений обратно к точке беспроводного доступа без необходимости перезагрузки до добавления в систему новых пользователей роуминга.

Для решения этих и других задач один аспект настоящего изобретения предусматривает беспроводное устройство инициализации, способное выполнять в узле функции маршрутизатора, обеспечивая пониженную избыточную нагрузку сети и стабилизируя сеть в надежную ГС с резервированием.

Прочие задачи, признаки и преимущества изобретения станут очевидными из нижеследующего подробного описания, приведенного в сочетании с прилагаемыми чертежами.

Краткое описание чертежей

Фиг.1 - схема беспроводного устройства инициализации в соответствии с настоящим изобретением.

Фиг.2 - схема варианта осуществления беспроводного устройства с двумя разъемами в соответствии с настоящим изобретением.

Фиг.3 - схема беспроводной системы инициализации в соответствии с настоящим изобретением.

Подробное описание изобретения

Система инициализирующего маршрутизатора, согласно настоящему изобретению, содержит множество точек беспроводного доступа, беспроводное устройство инициализации для приема, передачи и направления данных по множеству сетей и выполнена с возможностью поддержания соединения между точками беспроводного доступа и беспроводным устройством инициализации, причем беспроводное устройство инициализации содержит шасси, по меньшей мере, одну сетевую карту, по меньшей мере, одну беспроводную карту, по меньшей мере, один процессор и, по меньшей мере, одну операционную систему, оперативно конфигурируемую в шасси и связанную, по меньшей мере, с одной из множества точек беспроводного доступа для передачи и приема данных между точкой беспроводного доступа и системой высокочастотной связи, и при этом беспроводное устройство инициализации выполнено с возможностью обеспечения многочисленных подключений обратно к точке беспроводного доступа, без необходимости перезагрузки до добавления в систему нового пользователя роуминга, систему высокочастотной связи, позиционированную для связи между беспроводным устройством инициализации и множеством точек беспроводного доступа для передачи и приема данных между беспроводным устройством инициализации и множеством точек беспроводного доступа посредством защищенного соединения, и протокол безопасной аутентификации с возможностью аутентификации трафика при прохождении его через систему высокочастотной связи.

В данной заявке используются следующие термины.

Точка доступа. Сетевое устройство, позволяющее компьютерам, не являющимся частью сети, подключаться к сети и поддерживать связь с ней. Главной функцией точки доступа является обеспечение точки доступа для этих неподключенных компьютеров.

Аутентификация. Система мер для поддержания в системе информации, защищенной от повреждения или любопытных глаз. В сетях, процедура, посредством которой компьютер подтверждает идентификацию пользователя. В наиболее общем виде предусматривает сравнение входного имени и пароля с сохраненным файлом утвержденных имен пользователя и паролей. При обнаружении какого-либо различия между ними доступ пользователя к информации перекрывается.

Мост. Связывает сети так, что данные могут проходить из одной сети в другую сеть через еще одну сеть.

Дейтаграмма. Единичный блок данных, который передается через сеть и содержит информацию о пункте назначения.

Элемент обслуживания каталогов. Система сетевого администрирования, размещенная на одном компьютере предприятия. Этот компьютер поддерживает каталог базы данных, в которой хранится вся информация от тарификации до привилегий аутентификации для пользователей сети. В частности, эта машина записывает УДС-адреса и профили тарификации для пользователей системы. Этот компьютер является центральным хранилищем, которое управляет пользовательским доступом, системными привилегиями и статусом оплаты.

Протокол динамической конфигурации хоста (DHCP). Интернет-протокол для автоматизации конфигурации компьютеров, которые используют TCP/IP. DHCP можно

использовать для автоматического присвоения IP-адресов, для доставки параметров базовой конфигурации TCP/IP и для предоставления другой информации, например адресов, вспомогательным серверам.

Шлюз. Сложное устройство межсетевого взаимодействия, которое преобразует информацию от одного протокола к другому. Шлюзы переносят информацию между сетями, использующими разные протоколы связи. В действительности, шлюзы ликвидируют информацию от одной службы и восстанавливают ее в формате протокола другой сети. Шлюзы включают в себя все аппаратные и программные средства, используемые для связывания разнородных сетевых операционных систем (СОС, NOS) или для связывания локальных сетей (ЛС) с головными вычислительными машинами или глобальными сетями (ГС). Шлюзы также используются в электронной почте (E-mail) для преобразования сообщений между службами, использующими разные протоколы электронной почты.

Графический интерфейс пользователя (ГИП, GUI). Для выполнения команд ГИП использует графические символы, т.н. иконки, и меню.

Локальная сеть (ЛС). Группа компьютеров, обычно в одном здании или учреждении, физически соединенных таким образом, чтобы они могли связываться и взаимодействовать друг с другом. Чтобы сеть работала, нужен сервер, т.е. компьютер, который поддерживает данные, используемые разными компьютерами в сети. Некоторые преимущества сетевого соединения включают в себя возможность совместного использования документальных файлов и дорогостоящего оборудования. Для осуществления сетевых соединений можно использовать различные комбинации топологии, протоколы, программные и аппаратные средства. Сеть, в которой для соединения компьютеров вместо кабелей используется радиосвязь, можно называть локальной беспроводной сетью.

Управление доступом к среде (УДС, MAC). Протокол, который определяет передачу информации в сети.

Узел. Любое устройство, которое может связываться с другими компьютерами в группе соединенных между собой компьютеров. Обычно под узлом понимают компьютерную систему (КС) или терминал, которая(ый) является частью сети.

Пакет. Блок данных, передаваемых от одного компьютера к другому по сети или по Интернету. Пакет содержит три части: данные, подлежащие передаче, данные, необходимые для проводки пакета к месту назначения, и данные, которые исправляют ошибки, возникающие по пути следования. Обычная передача состоит из нескольких пакетов. Компьютер производит разбивку передачи в точке передачи и повторно собирает ее в точке назначения.

Протокол. Набор правил и процедур для обмена данными между компьютерами в сети или через Интернет. Протоколы обычно включают в себя проверку информации или ошибок, сжатие данных и отправку и прием сообщений.

Маршрутизатор. Элемент сети связи, который принимает передачи и пересылает их по назначению с использованием кратчайшего из доступных маршрутов. По пути к месту назначения данные могут проходить через несколько маршрутизаторов.

Простой протокол сетевого управления (SNMP). Он осуществляет обмен сетевой информацией посредством сообщений, известных в данной области техники как протокольные блоки данных (ПБД, PDU).

Сетевой теледоступ. Эмуляция терминала, в которой пользователь подключается к удаленному хосту с использованием учетной записи Интернета, как в случае непосредственного подключения пользователя к хосту, так что сеанс связи продолжается, как если бы пользователь находился на терминале, подключенном к хосту, хотя пользователь, в действительности, подключается к другому сайту, используя Интернет для подключения к хосту.

Топология. Физическая конфигурация сети, которая определяет, как соединены между собой компьютеры сети.

Протокол управления передачей/Интернет-протокол (TCP/IP) Язык, управляющий

связью между всеми компьютерами в Интернете. TCP/IP представляет собой два отдельных протокола, TCP и IP, которые используются совместно. Раздел стандарта, отвечающий Интернет-протоколу, указывает, как передавать пакеты информации по сетям. IP располагает методом адресации пакетов, который позволяет любому компьютеру в Интернете пересылать пакет другому компьютеру, который находится на расстоянии шага или еще ближе к получателю пакета. Протокол управления передачей гарантирует надежность передачи данных по сетям, подключенным к Интернету. TCP проверяет пакеты на предмет наличия ошибок и выдает запросы на повторную передачу в случае обнаружения ошибок, он также восстанавливает многочисленные пакеты сообщения в правильную, исходную последовательность, когда сообщение достигает пункта назначения.

Глобальная сеть (ГС). Совокупность компьютеров, соединенных друг с другом или объединенных в сеть в географической области. ГС обычно требуют особых соглашений с телефонными компаниями, поскольку передача данных между микрорайонами (т.н. сайтами) осуществляется по телефонным линиям.

Компьютерная сеть является просто совокупностью автономных компьютеров, соединенных друг с другом для обеспечения совместного использования аппаратных и программных ресурсов и для повышения общей надежности. Отличительный термин «локальная» обычно применяется к компьютерным сетям, в которых компьютеры находятся в одном здании или близлежащих зданиях, например, в университетском городке или на едином корпоративном сайте. Когда компьютеры удалены в большей степени, используется термин «глобальная сеть», но разница между ними чисто количественная и определения иногда перекрываются.

Мост это устройство, которое подключается, по меньшей мере, к двум ЛС и серверам, чтобы передавать кадры или пакеты сообщений между ЛС, что позволяет станции-отправителю в одной ЛС передавать данные на станцию-получатель в другой ЛС вне зависимости от местоположения получателя. Мосты, в принципе, являются полезными сетевыми компонентами, потому что полное количество станций в одной ЛС ограничено. Мосты можно реализовать так, чтобы они работали на выбранном уровне сетевого протокола.

В основе любой компьютерной сети лежит протокол связи. Протокол - это набор соглашений или правил, которые управляют переносом данных между компьютерными устройствами. Простейшие протоколы задают только аппаратную конфигурацию, тогда как более сложные протоколы задают хронирование, форматы данных, обнаружение и методы исправления ошибок и программные структуры.

Компьютерные сети почти всегда используют несколько уровней протоколов. Протокол самого низкого, физического уровня обеспечивает передачу и прием потока данных между двумя устройствами. Построение пакетов данных осуществляется на канальном уровне. Протоколы сетевого и транспортного уровней, располагающиеся над физическим уровнем, управляют передачей данных по сети, тем самым гарантируя надежную доставку данных.

Была предложена и получила широкое распространение модель сетевой архитектуры. Она известна как эталонная модель взаимодействия открытых систем (OSI), утвержденная Международной организацией по стандартизации (ISO). Сама по себе эталонная модель OSI не является сетевой архитектурой. Она лишь задает иерархию протокольных уровней и определяет функции каждого уровня в сети. Каждый уровень на одном компьютере сети общается с соответствующим уровнем на другом компьютере, с которым осуществляется связь в соответствии с протоколом, задающим правила осуществления этой связи. В действительности, на одном компьютере происходит перенос информации вниз от уровня к уровню, затем через канальную среду и снова вверх по последовательным уровням на другом компьютере. Однако в целях рассмотрения конструкции различных уровней и их функций проще считать, что компьютеры связываются между собой на каждом из уровней в «горизонтальном» направлении.

Низший уровень, предусмотренный в модели OSI, называется физическим уровнем и относится к передаче «сырых» битов данных по каналу связи. Конструкция физического

уровня опирается на такие области техники, как электричество, механика или оптика, в зависимости от среды, используемой для канала связи. Уровень, следующий после физического уровня, называется канальным уровнем. Основная задача канального уровня заключается в преобразовании физического уровня, который непосредственно связан с канальной средой, в линию связи, которую сетевой уровень, следующий в порядке повышения уровня, воспринимает как свободную от ошибок. Канальный уровень осуществляет такие функции, как структурирование данных в пакеты и присоединение управляющей информации к пакетам.

Хотя канальный уровень, в основном, не зависит от природы физической среды передачи, в некоторых аспектах работа канального уровня в большей степени зависит от среды передачи. По этой причине канальный уровень в некоторых сетевых архитектурах делится на два подуровня: подуровень управления логическим каналом, который осуществляет все функции канального уровня, не зависящие от среды, и подуровень УДС. Этот подуровень определяет, какая станция должна получить доступ к каналу связи при наличии конфликтующих запросов доступа. Функции уровня УДС обычно зависят от природы носителя передачи.

Основная функция моста состоит в том, чтобы прослушивать в беспорядочном режиме, т.е. весь трафик сообщений на всех ЛС, к которым он подключен, и пересылать каждое сообщение, которое он слышит, на ЛС, отличные от той, откуда получено сообщение. Мосты также поддерживают базу данных местоположений станций, извлеченных из содержимого пересылаемых сообщений. Мосты подключены к ЛС посредством путей, именуемых «каналами». Проработав некоторое время, мост может связать практически каждую станцию с тем или иным каналом, соединяющим мост с ЛС, и затем, пересылать сообщения более эффективным образом, передавая только по надлежащему каналу. Мост также может распознать сообщение, не нуждающееся в пересылке, когда отправитель и получатель связаны одним и тем же каналом. Помимо «изучения» местоположений станций или хотя бы направлений станций, мост, в основном, действует как ретранслятор сообщений.

По мере усложнения сетевых топологий при большом количестве ЛС и многочисленных мостах, соединяющих их, могут возникать проблемы в работе, если разрешены все возможные мостовые соединения ЛС. В частности, если несколько ЛС соединены мостами с образованием замкнутого контура, сообщение может циркулировать обратно в ЛС, откуда оно первоначально было передано, в результате чего генерируются множественные копии одного и того же сообщения. В худшем случае, сообщения дублируются до такой степени, что сети, по существу, забиваются этими сообщениями и оказываются неспособны обработать их все.

Интернет - это совокупность сетей, включая ARPANET, NSFnet, региональные сети, локальные сети в различных учебных и научных учреждениях и различные военные сети. Протоколы, обычно именуемые TCP/IP, первоначально были разработаны для использования только в сети ARPANET и затем получили широкое распространение в области связи. Протоколы обеспечивают набор услуг, которые позволяют пользователям связываться друг с другом по всему Интернету. Конкретные услуги, которые представляют эти протоколы, включают в себя передачу файлов, удаленную регистрацию, удаленное выполнение, удаленную печать, компьютерную почту и доступ к сетевым файловым системам.

Основная функция протокола управления передачей (TCP) состоит в том, чтобы гарантировать, что команды и сообщения из протокола уровня приложений, например, компьютерная почта, доставляются по назначению. TCP отслеживает отправления и повторно передает все, что не было правильно доставлено адресату. Если какое-либо сообщение настолько длинно, что его нельзя доставить в одной дейтаграмме, TCP разбивает его на несколько дейтаграмм и гарантирует, что все они будут правильно доставлены и повторно собраны для прикладной программы в пункте приема. Поскольку эти функции необходимы для многих приложений, они собраны в отдельный протокол

(TCP), а не включены в качестве составной части в каждое приложение. TCP реализован на транспортном уровне эталонной модели OSI.

Интернет-протокол (IP) реализован на сетевом уровне эталонной модели OSI и предоставляет TCP основную услугу, а именно, доставку дейтаграмм по назначению. TCP просто передает IP дейтаграмму с указанным местом назначения; IP не располагает информацией о взаимосвязи между последовательными дейтаграммами, и просто маршрутизирует каждую дейтаграмму по ее адресу назначения. Если местом назначения является станция, подключенная к другой ЛС, то IP использует маршрутизаторы для пересылки сообщения. TCP/IP часто использует небольшое отклонение от семиуровневой модели OSI, заключающееся в уменьшении количества уровней. Перечислим эти семь уровней:

Уровень 7 - уровень приложений. Идентифицирует параметры связи, безопасность пользователя и аутентификацию, а также конкретные детали синтаксиса передачи. Примерами протоколов уровня 7 являются протокол передачи файлов (FTP), простой протокол пересылки электронной почты (SMTP) и сетевой теледоступ.

Уровень 6 - представительский уровень. Отвечает за преобразование передачи из данных в текст в зависимости от используемой прикладной программы. Управление, в общем случае, передается операционной системе, которая работает с конкретными аспектами данных посредством таких протоколов, как Экспертная группа по вопросам движущегося изображения (MPEG) и Объединенная группа экспертов в области фотографии.

Уровень 5 - уровень сеанса связи. Устанавливает соединение между сторонами в обоих направлениях, прекращает его по завершении передачи, посредством таких протоколов, как AppleTalk и протокол управления сеансом связи (SCP).

Уровень 4 - транспортный уровень. На этом уровне протокол управления передачей (TCP), протокол дейтаграмм пользователя (UDP) и протокол связи имен (NBP) добавляют транспортные данные в пакет и передают его на уровень 3.

Уровень 3 - межсетевой уровень. Когда локальный хост (или хост-отправитель) инициирует действие, которое должен выполнить или на которое должен ответить удаленный хост (или хост-получатель), этот уровень берет пакет с уровня 4 и добавляет в него информацию IP, после чего передает его на уровень 2. Посредством таких протоколов, как пограничный межсетевой протокол (протокол пограничной маршрутизации) (BGP) или протокол обмена информацией о маршрутизации (RIP), уровень 2 идентифицирует получателя передачи на основании конкретных сетевых протоколов и управляет маршрутом каждого пакета данных, во всей передаче, на всем его пути.

Уровень 2 - уровень сетевого интерфейса. Это то, что "видит" сетевое устройство, например хост или локальный компьютер, и та среда, через которую данные поступают на уровень 1. Добавляет, посредством таких протоколов как управление логическим соединением (УЛС, LLC) или управление доступом к среде (УДС), конкретный код, необходимый, чтобы брать пакеты данных на их пути с использованием информации с уровня 3. Например, если сетевой стандарт требует, чтобы каждый пакет данных начинался со строки из конкретных двоичных цифр, их можно добавлять на уровне 2.

Уровень 1 - физический уровень. Это буквально Эфирнет (Ethernet) или сам межсетевой протокол для последовательного канала (SLIP). Задает физический интерфейс, необходимый для доставки информации из точки А в точку В, и включает в себя различные технические условия ЛС и ГС.

На приемном хосте уровни срываются по очереди, и их информация передается следующему, более высокому уровню, пока опять не достигнет уровня приложений. При наличии шлюза между хостом-отправителем и хостом-получателем шлюз берет пакет с физического уровня, передает его через канал передачи данных на физический уровень IP для продолжения. При передаче сообщения от первого хоста на второй шлюзы передают пакет, срывая нижележащие уровни, переадресуя нижележащий уровень, а затем передают пакет по конечному назначению.

Маршрутизатор, как и мост, представляет собой устройство, подключенное к двум или более сетям. Однако, в отличие от моста, маршрутизатор действует на сетевом уровне, а не на канальном уровне. При адресации на сетевом уровне используется 32-битовое поле адреса для каждого хоста, и поле адреса включает в себя идентификатор сети и идентификатор хоста внутри сети. Маршрутизаторы используют идентификатор сети назначения в сообщении для определения оптимального пути от сети-отправителя к сети-адресату. Для определения оптимальных путей маршрутизаторы могут использовать различные алгоритмы маршрутизации. Обычно маршрутизаторы обмениваются информацией об идентичности сетей, к которым они подключены.

Когда сообщение достигает сети назначения для завершения пересылки на хост назначения требуется адрес канального уровня. Адреса канального уровня имеют размер 48 бит, и никакие два хоста, где бы они не располагались, не имеют одинаковых адресов канального уровня. Имеется протокол, именуемый ARP (протокол разрешения конфликта IP-адреса сетевого уровня с физическим адресом уровня установления соединения (протокол переопределения адреса)), который получает адрес канального уровня из соответствующего адреса сетевого уровня (адреса, который использует IP). Обычно каждый маршрутизатор поддерживает таблицу базы данных, в которой можно искать адрес канального уровня, но если хост назначения отсутствует в этой базе данных ARP, маршрутизатор может передать ARP-запрос. Отвечает только адресованный хост назначения, и тогда маршрутизатор способен вставлять в пересылаемое сообщение правильный адрес канального уровня и передавать сообщение по конечному назначению.

IP-маршрутизация задает, что IP-дейтаграммы распространяются через объединенные сети шаг за шагом на основании адреса назначения в IP-заголовке. Весь маршрут не известен на начальном этапе распространения. Напротив, в каждом промежуточном пункте вычисляется следующий пункт назначения путем сопоставления адреса назначения с IP-заголовком дейтаграммы с элементом таблицы маршрутизации текущего узла.

Вклад каждого узла в процесс маршрутизации состоит только в пересылке пакетов на основании внутренней информации, присутствующей в маршрутизаторе, вне зависимости от того, достигают ли пакеты конечного назначения. В порядке продвижения этого объяснения на шаг вперед IP-маршрутизация не изменяет исходной дейтаграммы. В частности, адрес отправителя и получателя дейтаграммы остаются неизменными. IP-заголовок всегда задает IP-адрес исходного отправителя и IP-адрес конечного получателя.

Когда IP выполняет алгоритм маршрутизации, он вычисляет новый адрес, IP-адрес устройства, на которое затем следует послать дейтаграмму. Этот алгоритм использует информацию из элементов таблицы маршрутизации, а также любую кэшированную информацию, локальную по отношению к маршрутизатору. Этот новый адрес, скорее всего, является адресом другого маршрутизатора/шлюза. Если дейтаграмму можно доставить непосредственно, то новый адрес будет таким же, как адрес назначения в IP-заголовке.

Следующий адрес, заданный вышеуказанным методом, не хранится в IP-дейтаграмме. Нет резервного места, где его держать, и он вообще не «хранится». После выполнения алгоритма маршрутизации для задания адреса следующего шага к конечному пункту назначения. Программное обеспечение IP-протокола передает дейтаграмму и адрес следующего этапа программному обеспечению сетевого интерфейса, отвечающего за физическую сеть, по которой теперь нужно передать дейтаграмму.

Программное обеспечение сетевого интерфейса связывает адрес следующего шага с физическим адресом, формирует пакет с использованием физического адреса, помещает дейтаграмму в область данных пакета и передает результат по физическому сетевому интерфейсу, через который достигается шлюз следующего шага. Следующий шаг принимает дейтаграмму, и вышеописанный процесс повторяется. Кроме того, IP не обеспечивает сообщение об ошибке обратно отправителю, когда имеют место аномалии маршрутизации. Эта задача остается другому Интернет-протоколу, а именно протоколу управляющих сообщений в Интернете (ICMP).

Маршрутизатор осуществляет преобразование протокола. Один пример присутствует на

уровнях 1 и 2. Если дейтаграмма поступает через интерфейс Эфирнета и подлежит выводу на последовательный канал, например, маршрутизатор срывает заголовочную и хвостовую части сообщения Эфирнета и заменяет их соответствующими заголовочной и хвостовой частями для конкретных сетевых сред, например, SMDS (Switched Multimegabit Data Service) (служба высокоскоростной передачи данных с коммутацией каналов).

Для извлечения адреса следующего шага, вместо элементов таблицы маршрутизации можно использовать стратегию маршрутизации. В системе и методологии, отвечающих настоящему изобретению, тестируют адрес отправителя, чтобы видеть, в каком диапазоне адресов поставщика услуг Интернета (ISP) он находится. Определив диапазон адресов поставщика услуг Интернета, пакет маршрутизируют по адресу следующего шага, связанному с конкретным поставщиком услуг Интернета.

Следует заметить, однако, что маршрутизация беспроводных сетей на узлах доступа является наиболее эффективным средством передачи данных в Интернете. Один аспект настоящего беспроводного устройства инициализации состоит в обеспечении маршрутизации на каждой точке доступа узлов. Это обеспечивает более сильную сеть и обеспечивает гибкость в конструкции сети. Эта гибкость позволяет лучше администрировать сетевой график и расширяет общую полосу пропускания за счет снижения сетевой задержки посредством оптимизации маршрутов и администрирования пакетов данных. Хотя беспроводное устройство инициализации может выступать в качестве моста, решение об использовании беспроводного инициализирующего маршрутизатора в качестве моста к сети или маршрутизатора на сеть должен принимать сетевой инженер. Эта особенность дает сетевому инженеру дополнительную гибкость при определении конструкции сети. Кроме того, гибкий характер оборудования позволяет пользователю менять краевой узел, который служит мостом к узлу базовой сети, который осуществляет маршрутизацию с использованием модификации кода без необходимости перезагрузки.

Затем по мере роста узла сетевой инженер может обновлять этот узел, чтобы удовлетворять потребности сети без ущерба для существующих клиентов. Вставив карты в разъемы шасси, которое в качестве операционной системы (ОС) содержит открытый исходный код, предпочтительно, LINUX, беспроводное устройство инициализации можно конфигурировать как маршрутизатор или мост. Модуль маршрутизации системы LINUX не является частью главного операционного ядра. Будучи подкомпонентом ОС, модуль маршрутизации допускает обновление и модификацию без перезагрузки системы. Перезагрузка усовершенствованного блока LINUX может занимать до 30 минут. Обновление модуля маршрутизации в LINUX может занимать менее 2 секунд для повторной инициализации. Эта повторная инициализация прозрачна для абонентов, присоединенных к этому блоку. Модуль маршрутизации допускает замену модулем моста, если узлу доступа не требуется маршрутизация. Маршрутизация в точке доступа позволяет фильтровать IP-адреса либо для всех абонентов, присоединенных к этому узлу, либо для отдельного IP-адреса, присоединенного к этому узлу. Кроме того, модуль маршрутизации содержит маршрутизирующую логику, способную повышать пропускную способность. Только этот процесс позволяет передавать определенные объемы данных по определенному IP-адресу абонента и/или с него.

Настоящее изобретение развивает уровень техники за счет дополнительных точек доступа. Благодаря гибкой конфигурации, предусматривающей, предпочтительно, восемь портов, беспроводное устройство инициализации может содержать до семи беспроводных соединений и одно проводное соединение или семь проводных соединений и одно беспроводное соединение, или любую комбинацию, подходящую для сети. Это снижает общие затраты и снижает потребности в свободном месте. Благодаря замене этой системы более быстрым набором микросхем, оборудование эффективно обрабатывает больше данных из одной и той же точки. Кроме того, эта особенность позволяет расширять систему, для развития от внешнего краевого узла с малой нагрузкой к узлу базовой сети с многократным резервированием, не затрагивая существующих абонентов. Пользователь

также может увеличивать количество потенциальных абонентов к точке доступа в сети, добавляя карты и антенны без необходимости изменять шасси. Поскольку физическая конфигурация системы размещается в шасси персонального компьютера, содержащем, предпочтительно, восемь возможных сетевых разъемов, беспроводное устройство инициализации можно конфигурировать разными количествами беспроводных карт и сетевых карт. Шасси может содержать до двух процессоров. Работа операционной системы LINUX в одно- или двухпроцессорной конфигурации обеспечивает мощное администрирование данных. Благодаря такой конфигурации процессоров и значительному объему оперативной памяти, операционная система может манипулировать значительно большими объемами информации, чем традиционные беспроводные точки доступа.

Устройство инициализации, согласно настоящему изобретению, также решает вопросы защиты беспроводного оборудования. Благодаря подключению сетевого теледоступа защищенной оболочки к беспроводному устройству инициализации, другие пользователи в сети не могут перехватывать трафик сообщений и административную информацию. Благодаря этой особенности, беспроводное оборудование общего пользования может получить широкое распространение. Эта особенность использует более универсальную схему администрирования сетевого теледоступа. Таким образом, администратор может написать графические интерфейсы пользователя (ГИП) или может управлять узлом, используя экран командной строки открытого текста. Подключение к этим узлам может быть ограничено авторизованными IP-адресами и именами доменов, что снижает вероятность неавторизованных входов в сеть. В настоящее время беспроводное оборудование использует простой протокол сетевого управления, версия 1 (SNMPV-1) для администрирования устройства доступа. SNMPV-1 ограничен трафиком текстовых сообщений. Любое соединение с этой точкой доступа находится в том же логическом сегменте, что и те, которые производят административную работу к устройству доступа. В каждом сетевом решении логические сегменты содержат всю информацию, которая передается внутри сегмента. Перехват трафика на этом логическом сегменте является давней проблемой циклических сетей. Протокол SNMPV-6 является типичным решением этой проблемы при использовании протокола SNMP. Однако SNMPV-6 является протоколом, требующим интенсивной работы процессора, обеспечивающим значительную избыточную нагрузку разветвленной сети. Благодаря использованию защищенного соединения сетевого теледоступа, избыточная нагрузка сети снижается, а защищенность системы повышается. Только защищенное соединение сетевого теледоступа позволяет определенным IP подключаться к определенным портам данных. Эта структура ограниченного соединения, по существу, создает различные логические сегменты в одном и том же физическом сегменте сети. Вновь созданный логический сегмент не дает обычному пользователю перехватывать административный трафик.

Согласно предпочтительному варианту осуществления настоящего беспроводного устройства инициализации, ограниченная статическая УДС-адресация заменяется аутентификацией RADIUS или объединяется с ней. Аутентификацию RADIUS можно присоединить к УДС-адресации совместно с именем пользователя и паролем. Этот метод аутентификации значительно снижает вероятность хищения услуг и обеспечивает пользователю мобильное решение между сотовыми ячейками. Кроме того, эта особенность подходит к методу обслуживания каталогов, который обеспечивает пользователю более специализированный интерфейс. Благодаря использованию IP-фильтрации, уровней авторизации и администрирования пользователей в рамках предприятия, беспроводной инициализирующий маршрутизатор совместно со службой каталогов управляет потреблением полосы частот и предоставляет пользователю более специализированное обслуживание. В отсутствие аутентификации RADIUS пользователи подключаются к сети без какого-либо управления со стороны центрального сервера. Благодаря обеспечению аутентификации RADIUS, один сервер управляет возможностью пользователя входить в те или иные части сети.

Различные варианты осуществления настоящего изобретения предусматривают

брандмауэр и посредническую услугу. Посредническая услуга - это комбинация позиционной фильтрации пакетов с инспекцией содержимого. По существу, Firebox перехватывает трафик, предназначенный для другого места назначения (например, веб-сервера или почтового сервера) и применяет строгие правила доступа и маршрутизации, предусматривающие защиту внутренних сетей и серверов. Опасный трафик отбрасывается, а нормальный график пропускается в предусмотренный пункт назначения. Другими словами, приложение переключения сетевого трафика, которое представляет доверенных, обычно локальных клиентов, когда они обращаются к ресурсам неизвестной сети, часто используется для защиты локальной корпоративной ЛС от потенциально враждебных внешних хостов. Беспроводное устройство инициализации может обеспечивать обе эти услуги на пользовательском терминале. Эти услуги обеспечивают пользователю дополнительный уровень защиты без необходимости в администрировании безопасности. Кроме того, посредник будет обеспечивать преобразование IP-адресов и позволять пользователям поддерживать сети за пределами точки входа в сеть.

Беспроводные устройства инициализации, отвечающие настоящему изобретению, обеспечивают соединения как от карт персональных компьютеров, так и от других беспроводных устройств инициализации. Поэтому одна и та же беспроводная ГС может содержать единичных пользователей и большие ЛС. В традиционных конфигурациях беспроводного оборудования, пользователь должен по выбору предоставлять услугу либо персональному компьютеру, содержащему карты, либо беспроводному мосту доступа. Коммерческие пользователи выбирают использование моста доступа, тогда как резидентный пользователь выбирает использование персонального компьютера. В отсутствие беспроводного устройства инициализации, пришлось бы создавать две отдельные беспроводные инфраструктуры, чтобы удовлетворить все типы абонентов. Беспроводное устройство инициализации позволяет пользователю подключаться к беспроводной инфраструктуре с использованием либо отдельного персонального компьютера, либо другого беспроводного устройства инициализации. В результате, можно создавать одну беспроводную инфраструктуру, удовлетворяющую все возможные типы абонентов.

Очевидно, что компоненты настоящего изобретения, описанные в целом и проиллюстрированные здесь на фигурах, можно скомпоновать и построить в широком ряду различных конфигураций. Таким образом, следующее более подробное описание вариантов осуществления системы и способа настоящего изобретения, представленных на фиг.1-3, не призваны ограничивать заявленный объем изобретения, но лишь представляют предпочтительные в настоящее время варианты осуществления изобретения.

Для обеспечения наилучшего понимания предпочтительных в настоящее время вариантов осуществления изобретения дана ссылка на чертежи фиг.1-3, где аналогичные детали обозначены подобными позициями.

В целом, на фиг.1-3 показана автономная беспроводная система. На фиг.3 показано, что к беспроводному облаку 300 подключен граничный маршрутизатор 310 в каждой точке доступа. Согласно предпочтительному варианту осуществления настоящего изобретения, граничный маршрутизатор 310 является обычным проводным маршрутизатором. К одному уровню облака 300 подключен элемент 320 обслуживания каталогов. Это устройство можно сконфигурировать для управления объектами, аутентификацию которых проводят все компьютеры клиентской стороны. Облако 300, подключенное к мачте 330, проходит через беспроводной маршрутизатор 340. Этот маршрутизатор 340 служит как маршрутизатором, так и сервером протокола динамической конфигурации хоста (DHCP). Все другие подключения на мачте также используют беспроводные маршрутизаторы для подключения центрального беспроводного маршрутизатора.

Каждый раз, когда беспроводной маршрутизатор 340 располагается на мачте 330, этот маршрутизатор действует как ее собственный сервер DHCP. Мачте 330 присвоен заданный набор IP-адресов. Вся аутентификация DHCP возвращает элементу 320 обслуживания каталогов правильную учетную запись. В микрорайонах с большой нагрузкой, например, на

заводах 350, беспроводной маршрутизатор 340 размещен в выходной точке доступа 360. Этот беспроводной маршрутизатор 340 выступает в качестве внутреннего маршрутизатора для всего оборудования на предприятии и граничного маршрутизатора для микрорайона. Беспроводной маршрутизатор 340 необходим только тем клиентам, которые имеют большое количество компьютеров, подключенных к беспроводной сети. Домашние пользователи и малые предприятия 370, которые имеют один или два ПК 380, могут непосредственно подключаться обратно к беспроводному маршрутизатору 340 на мачте 330. Кроме того, пользователи малых компьютеров могут иметь мостовое соединение обратно к мачте 330 и затем не получать маршрутизацию, пока не достигнут граничного маршрутизатора 310 на выходе облака 300 Интернета.

В частности, согласно фиг.1, иллюстративный вариант осуществления беспроводного устройства инициализации, согласно настоящему изобретению, может содержать шасси 100, соответствующим образом сконфигурированное с операционной системой 110 на базе UNIX, например, операционной системой LINUX, работающей на ЦП 120 на базе Intel. 2,4 ГГц-ые беспроводные карты 130 снабжены обычными разъемами PCMCIA 140. Этот разъем приспособлен к структуре 150 шины ПК посредством адаптера от PCMCIA к PCI. Шинный интерфейс ПК всегда является PCI. Информация поступает на беспроводные карты и выводится из них через шину PCI в стек TCP (не показан) ОС LINUX 110. Стек TCP на ОС LINUX сконфигурирован таким образом, чтобы либо перенаправлять, либо передавать данные через соответствующий интерфейс. Во многих случаях данные поступают в беспроводное устройство инициализации через карту сетевого интерфейса 10/100 (NIC) 160 посредством стандартных методов проводной связи IP 170. Когда информация поступает через проводное соединение 170, конфигурация стека TCP в модуле стека LINUX направляет трафик от соответствующего соединения. Конфигурация стека TCP LINUX оптимизирует поток трафика сетевых данных.

На фиг.2, где в общем виде изображена обычная конфигурация для 2,4 ГГц-ового моста 200, показаны 1 и 2 беспроводные карты 210 с разъемами PCMCIA 220. Эти карты 210 подключены к шине моста через соединения PCMCIA 230. Выход из беспроводного моста 200 представляет собой либо эфирнет 10/100, либо другую беспроводную карту 210. Беспроводные карты 210 имеют адаптер 240 для повышенного коэффициента усиления антенны. Эти разъемы ведут к разрядному устройству 250 для предотвращения повреждения от электрических разрядов. Эти разрядники 250 подключены к особым антенным кабелям 260 с низкими потерями. Антенные кабели 260 с низкими потерями подключены к антеннам с повышенным коэффициентом усиления переменных глобальных диаграмм направленности и интенсивности. В некоторых случаях эти антенны требуют разветвителей 270 и усилителей 280 для оптимизации глобальных диаграмм направленности для области.

Устройство и система, отвечающие настоящему изобретению, хорошо работают во многих случаях и не блокируют и не влияют на будущие усовершенствования сетевых протоколов и операционных систем. Чтобы убедиться, что операциям на прикладном и транспортном уровнях быстро становятся известны изменения адреса, устройство и система могут исключить сцену единичной точки провала, исключить или снизить подоптимальную маршрутизацию для всех приложений, обеспечивают повышенную безопасность для защиты связи по беспроводным средам и позволяют пользователям переключать карты сетевых адаптеров, в то же время сохраняя все соединения, например прикладные программы и сетевую администрацию, прозрачно для пользователя.

Настоящее изобретение можно воплощать в других конкретных формах, не отклоняясь от его сущности или важнейших характеристик. Описанные варианты осуществления следует рассматривать во всех отношениях только как иллюстрацию, а не как ограничение. Объем изобретения, поэтому, обозначен в прилагаемой формуле изобретения, а не в вышеприведенном описании. Все изменения, которые отвечают смыслу и диапазону эквивалентности формулы изобретения, подлежат включению в ее объем.

Формула изобретения

1. Беспроводное устройство инициализации для использования в сетях общего пользования, доступное пользователю мобильного вычислительного устройства, отличающееся тем, что содержит шасси, по меньшей мере, одну сетевую карту, по меньшей мере, одну беспроводную карту, по меньшей мере, один процессор, операционную систему, оперативно конфигурируемую на шасси для управления, по меньшей мере, одной сетевой картой, по меньшей мере, одной беспроводной картой и, по меньшей мере, одним процессором, которые оперативно связаны с шасси, пакетно-коммутируемый интерфейс, выполненный с возможностью приема совокупности входящих кадрированных пакетных данных для обеспечения входящих пакетов и передачи совокупности исходящих кадрированных пакетных данных, включая исходящие пакеты, контроллер каналообразования, подключенный к пакетно-коммутируемому интерфейсу, который канализирует входящие пакеты на основании входящей адресной информации и который строит исходящие пакеты и канализирует исходящие пакеты с помощью исходящей адресной информации, причем контроллер каналообразования содержит программные средства сетевого интерфейса, выполненные с возможностью приема входящих пакетов от пакетно-коммутируемого интерфейса, формирования исходящих пакетов с использованием физического адреса пакета и с возможностью эффективного подключения, по меньшей мере, к одной сети посредством операционной системы для разрешения программным средствам сетевого интерфейса передавать исходящие пакеты в упомянутую сеть, и аутентификатор, оперативно поддерживающий связь с операционной системой, для обеспечения аутентификации на беспроводном устройстве инициализации, благодаря чему пользователь мобильного вычислительного устройства подключается к беспроводному устройству инициализации без необходимости первоначального доступа в Интернет.

2. Беспроводное устройство инициализации по п.1, отличающееся тем, что контроллер каналообразования служит маршрутизатором для входящих пакетов.

3. Беспроводное устройство инициализации по п.2, отличающееся тем, что контроллер каналообразования служит маршрутизатором для исходящих пакетов.

4. Беспроводное устройство инициализации по п.1, отличающееся тем, что контроллер каналообразования служит мостом для входящих пакетов.

5. Беспроводное устройство инициализации по п.4, отличающееся тем, что контроллер каналообразования служит мостом для исходящих пакетов.

6. Беспроводное устройство инициализации по п.1, отличающееся тем, что операционная система беспроводного устройства инициализации является системой на базе UNIX с открытым исходным текстом.

7. Беспроводное устройство инициализации по п.1, отличающееся тем, что система на базе UNIX с открытым исходным текстом представляет собой LINUX.

8. Беспроводное устройство инициализации по п.1, отличающееся тем, что дополнительно содержит второй процессор, управляемый операционной системой и соединенный с шасси.

9. Беспроводное устройство инициализации по п.1, отличающееся тем, что дополнительно содержит устройство памяти и устройство хранения.

10. Беспроводное устройство инициализации по п.1, отличающееся тем, что сетевая карта, беспроводная карта, процессор, операционная система, пакетно-коммутируемый интерфейс и контроллер каналообразования оперативно расположены в шасси беспроводного устройства инициализации.

11. Беспроводное устройство инициализации по п.10, отличающееся тем, что аутентификатор оперативно расположен в шасси беспроводного устройства инициализации.

12. Беспроводное устройство инициализации по п.1, отличающееся тем, что операционная система беспроводного устройства инициализации выполнена с

возможностью управления пропускной способностью для отдельного пользователя.

13. Беспроводное устройство инициализации по п.1, отличающееся тем, что операционная система беспроводного устройства инициализации выполнена с возможностью управления типом протокола отдельного пользователя.

14. Система, обеспечивающая пользователям безопасный доступ к сетям общего пользования посредством мобильных вычислительных устройств, отличающаяся тем, что содержит множество точек беспроводного доступа; по меньшей мере, одно беспроводное устройство инициализации для приема, аутентификации, передачи и направления данных по множеству сетей, выполненное с возможностью поддержания соединения между точками беспроводного доступа и беспроводным устройством инициализации, причем беспроводное устройство инициализации содержит шасси, по меньшей мере, одну сетевую карту, по меньшей мере, одну беспроводную карту, по меньшей мере, один процессор и, по меньшей мере, одну операционную систему, оперативно конфигурируемую в шасси и находящуюся в оперативной связи с, по меньшей мере, одной сетевой картой, с, по меньшей мере, одной беспроводной картой, с, по меньшей мере, одним процессором и выполненную с возможностью управления, по меньшей мере, одной сетевой картой, по меньшей мере, одной беспроводной картой, по меньшей мере, одним процессором, причем операционная система связана, по меньшей мере, с одной из множества точек беспроводного доступа для передачи и приема данных между точкой беспроводного доступа и высокочастотным конструктивным элементом и при этом беспроводное устройство инициализации выполнено с возможностью обеспечения многочисленных подключений обратно к точке беспроводного доступа без необходимости перезагрузки до добавления в систему нового пользователя роуминга; высокочастотный конструктивный элемент, позиционированный для связи между беспроводным устройством инициализации и множеством точек беспроводного доступа, для передачи и приема данных между беспроводным устройством инициализации и множеством точек беспроводного доступа посредством защищенного соединения; протокол безопасной аутентификации, инициируемый беспроводным устройством инициализации, с возможностью аутентификации трафика при прохождении его через высокочастотный конструктивный элемент.

15. Система по п.14, отличающаяся тем, что высокочастотный конструктивный элемент представляет собой соответствующую антенну, выполненную с возможностью обеспечения мостовых решений, которые предоставляют пользователю возможность размещать беспроводное оборудование в глобальной сети.

16. Система по п.15, отличающаяся тем, что протокол безопасной аутентификации представляет собой протокол аутентификации RADIUS.

17. Система по п.15, отличающаяся тем, что беспроводное устройство инициализации обеспечивает посредническую услугу.

18. Система по п.15, отличающаяся тем, что беспроводное устройство инициализации обеспечивает услугу брандмауэра.

19. Система по п.14, отличающаяся тем, что протокол безопасной аутентификации представляет собой протокол аутентификации RADIUS.

20. Система по п.14, отличающаяся тем, что беспроводное устройство инициализации обеспечивает посредническую услугу.

21. Система по п.14, отличающаяся тем, что беспроводное устройство инициализации обеспечивает услугу брандмауэра.

22. Система по п.14, отличающаяся тем, что защищенное соединение высокочастотного конструктивного элемента представляет собой соединение защищенной оболочки сетевого теледоступа.

23. Система по п.14, отличающаяся тем, что дополнительно содержит, по меньшей мере, одну антенну.

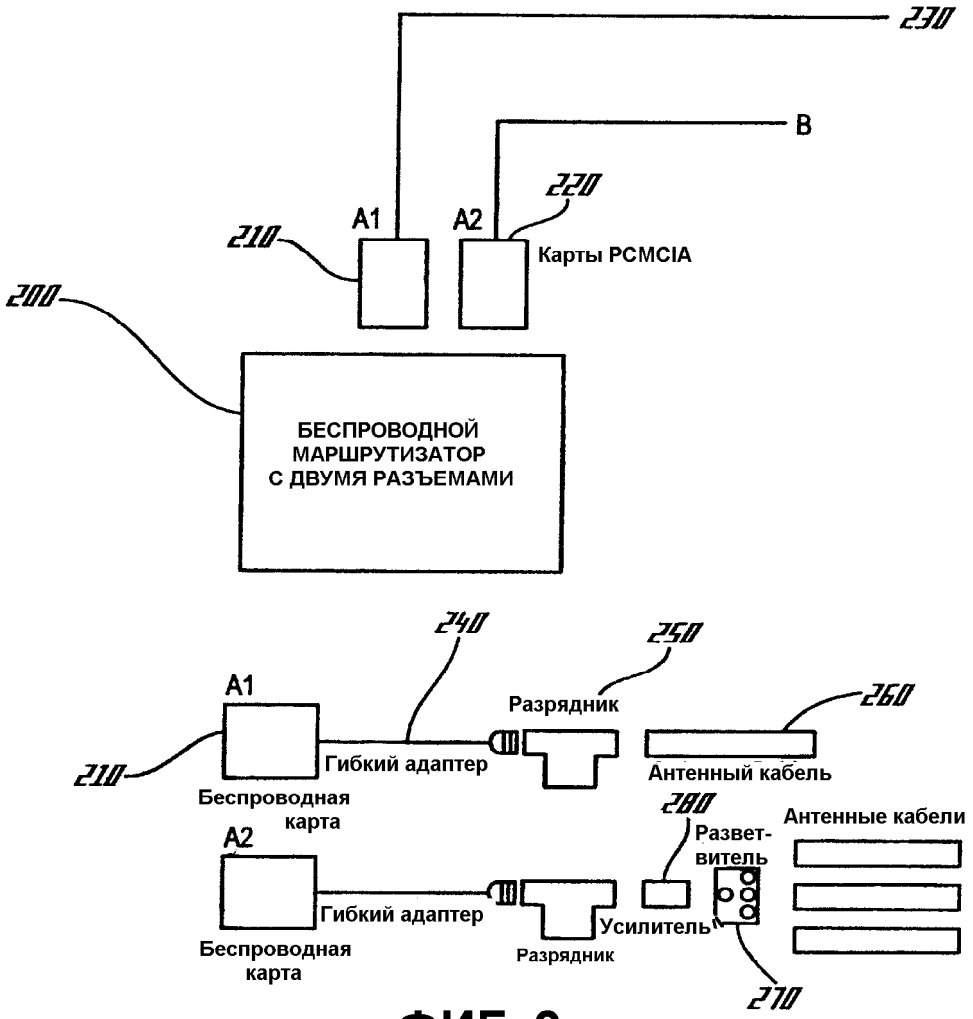
24. Система по п.14, отличающаяся тем, что, по меньшей мере, одна антенна является 2,4 ГГц-й антенной.

25. Система по п.14, отличающаяся тем, что операционная система беспроводного устройства инициализации является системой на базе UNIX с открытым исходным текстом.

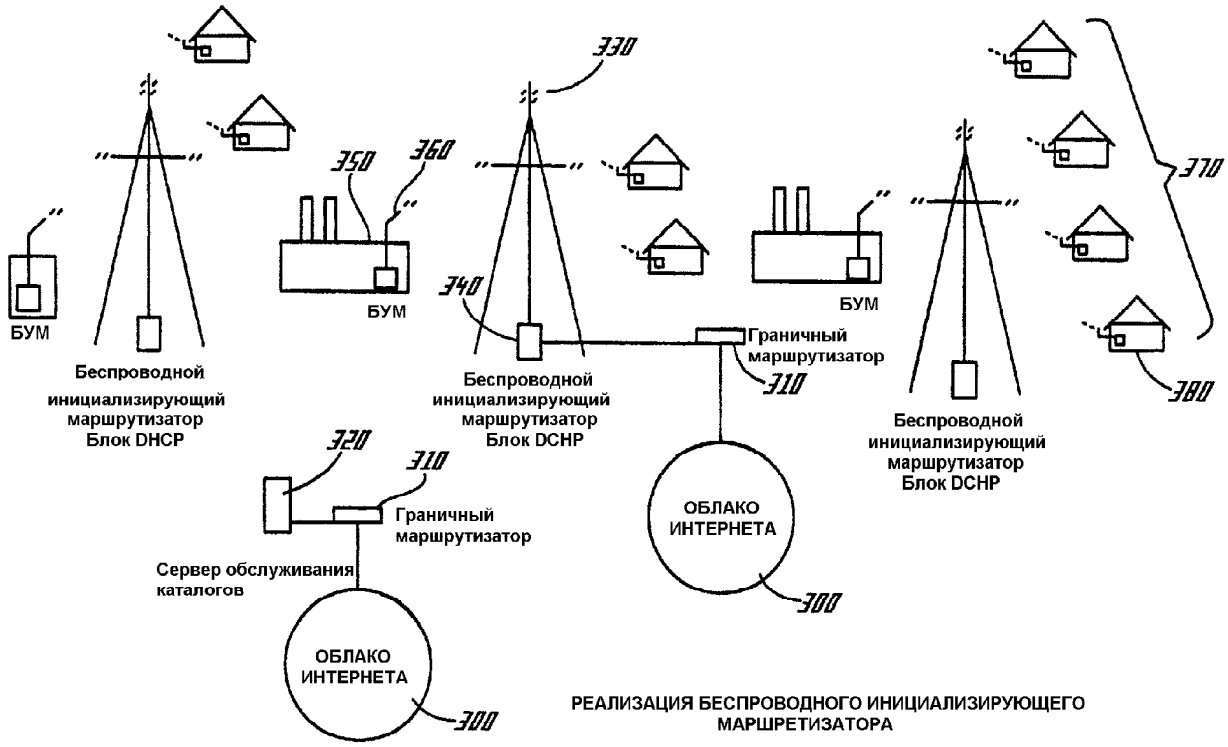
26. Система по п.14, отличающаяся тем, что система на базе UNIX с открытым исходным текстом представляет собой LINUX.

27. Система по п.23, отличающаяся тем, что содержит более одной антенны и пользователю предоставлена возможность регистрации в системе и поддержания соединения с системой при переходе от одной антенны к другой.

28. Система по п.23, отличающаяся тем, что пользователю предоставлена возможность регистрации в системе и поддержания соединения с системой при переходе от одной точки доступа к другой.


230
B
220
A1
A2
210
Карты PCMCIA
200
БЕСПРОВОДНОЙ
МАРШРУТИЗАТОР
С ДВУМЯ РАЗЪЕМАМИ
240
250
A1
Разрядник
260
210
Гибкий адаптер
Антенный кабель
Беспроводная
карта
280
Антенные кабели
A2
Развет-
витель
Гибкий адаптер
Усилитель
Беспроводная
карта
Разрядник
270

ФИГ. 2


330
350
360
370
БУМ
БУМ
340
Граничный
маршрутизатор
310
Беспроводной
инициализирующий
маршрутизатор
Блок DHCP
Беспроводной
инициализирующий
маршрутизатор
Блок DCHP
Беспроводной
инициализирующий
маршрутизатор
Блок DCHP
380
320
310
Граничный
маршрутизатор
ОБЛАКО
ИНТЕРНЕТА
Сервер обслуживания
каталогов
ОБЛАКО
ИНТЕРНЕТА
300
300
РЕАЛИЗАЦИЯ БЕСПРОВОДНОГО ИНИЦИАЛИЗИРУЮЩЕГО
МАРШРЕТИЗАТОРА

ФИГ. 3