Руководство пользователя

HG100R-AK

Примечание

Благодарим Вас за покупку продукта HUMAX. Пожалуйста, внимательно прочтите данное руководство пользователя для обеспечения безопасной установки, эксплуатации продукта, а также поддержания его максимальной производительности. Храните данное руководство пользователя вместе с вашим продуктом для дальнейшего использования в качестве справочной информации. Содержащаяся в данном руководстве пользователя информация подлежит изменению без уведомления.

Авторское право (Авторское право © 2015 HUMAX Corporation)

Информация по технике безопасности и нормативная информация

Инструкции по технике безопасности

Пожалуйста, прочтите эти инструкции перед использованием вашего резидентного шлюза. Мы не хотим допустить получение травм или повреждения вашего резидентного шлюза.

- Не используйте резидентный шлюз вблизи воды. Берегите резидентный шлюз от сырости. Если вам нужно очистить его, не используйте влажное полотенце. Протрите резидентный шлюз чистой и сухой тканью. Никогда не используйте очищающую жидкость или аналогичные химические вещества. Не распыляйте чистящие средства непосредственно на резидентный шлюз и не используйте продувочный воздух для удаления пыли.
- Не помещайте резидентный шлюз вблизи источников тепла, таких как горячие приборы, в частности, обогревателей и радиаторов, другой электроники, такой как компьютеры и стереосистемы, или внутри вашего камина. Ваш резидентный шлюз находится в охлажденном состоянии и вы должны сохранять его в таком состоянии.
- Не закрывайте резидентный шлюз и не блокируйте поток воздуха к резидентному шлюзу с помощью каких-либо других объектов. Берегите резидентный шлюз от чрезмерного тепла и влаги, а также вибрации и пыли.
- Резидентный шлюз предназначен только для использования внутри помещений. Пожалуйста, не пытайтесь использовать его вне помещений.
- Не пытайтесь открывать, модифицировать или ремонтировать свой резидентный шлюз. Это может привести к поражению электрическим током или травмам. Любая пользовательская модификация, не утвержденная компанией HUMAX, приведет к аннулированию вашего права на использование оборудования, а также к аннулированию гарантии на резидентный шлюз.
- Подключайте только те кабели и вспомогательное оборудование, которые указаны компанией HUMAX и соответствуют требованием шлюза HUMAX.
- Защитите силовой кабель вашего резидентного шлюза путем его неплотного размещения между резидентным шлюзом и розеткой питания. Не растягивайте его или сжимайте его между различными объектами.
- Осторожно обращайтесь с резидентным шлюзом. Не роняйте и не встряхивайте ваш резидентный шлюз.
- Предполагается, что ваш резидентный шлюз будет нагреваться, однако для того, чтобы он продолжал функционировать надлежащим образом он должен вентилироваться. Не закрывайте вентиляционные отверстия. Важно, чтобы резидентный шлюз был размещен на не загроможденной, твердой поверхности. Не устанавливайте резидентный шлюз на мягкой поверхности, такой как ковровое покрытие, которое может блокировать поток воздуха.
- Этот резидентный шлюз прошел испытания на соответствие требованиям в условиях, которые включали использование поставляемых кабелей между компонентами систем. Для обеспечения соответствия требованиям техники безопасности и нормативным нормам используйте только предоставленные силовые и интерфейсные кабели и устанавливайте их надлежащим образом.
- Отложите установку оборудования до тех пор, пока не будет исключена вероятность грозовой активности в зоне эксплуатации.
- После завершения всех работ по техническому обслуживанию или ремонту данного резидентного шлюза, попросите сервисного специалиста провести проверку безопасности, чтобы убедиться, что резидентный шлюз находится в безопасном рабочем состоянии.

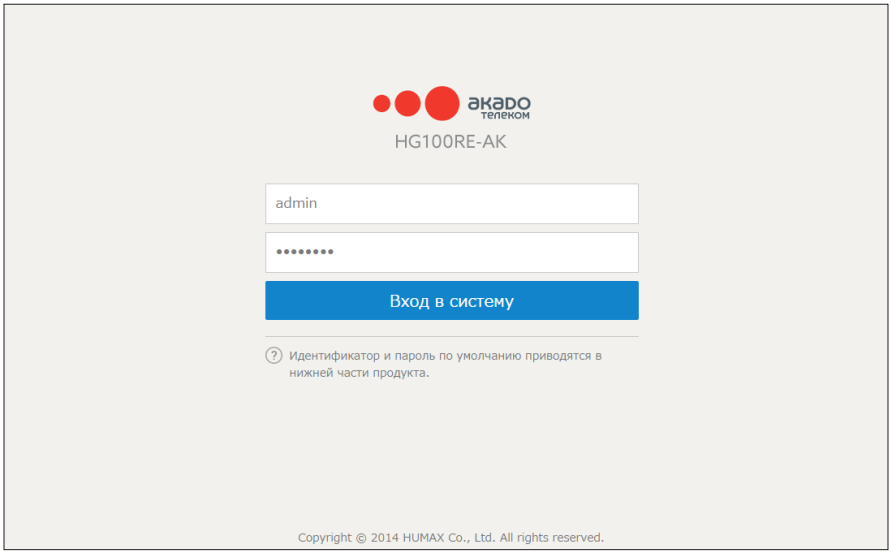
Опасности удушения

В комплект резидентного шлюза могут входить полиэтиленовые пакеты и хомуты-стяжки. Пожалуйста, утилизируйте их надлежащим образомм храните их в недоступном для детей месте, поскольку они могут представлять опасность удушения. Храните резидентный шлюз, его шнуры и вспомогательное оборудование в недоступном для маленьких детей месте.

Доступ к веб-странице

Чтобы настроить резидентный шлюз, вам необходимо получить доступ к веб-странице конфигурации. IP-адрес резидентного шлюза – 192.168.0.1 или 192.168.100.1 Чтобы настроить резидентный шлюз, выполните следующие действия:

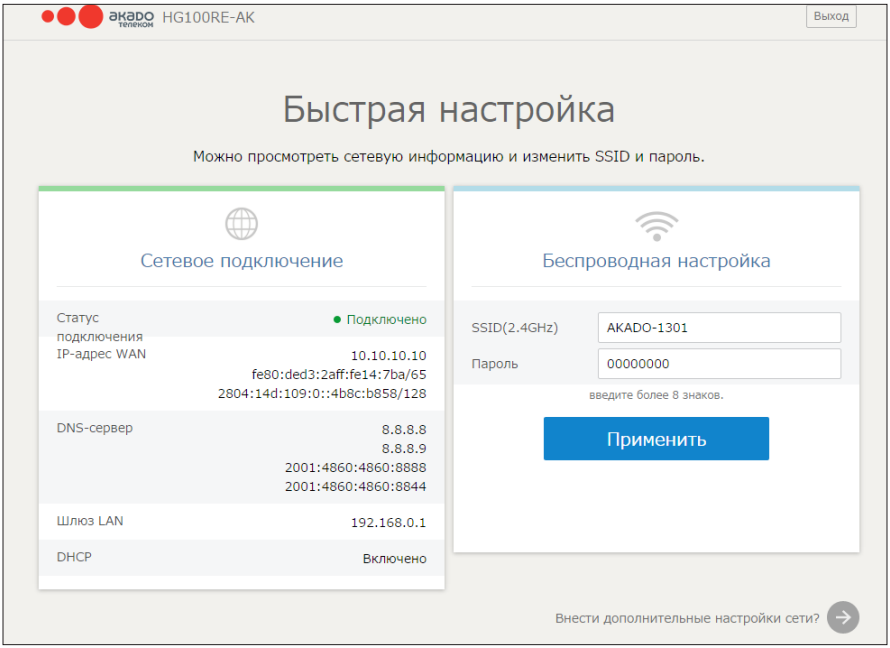
1. Получите IP-адрес от встроенного DHCP-сервера для вашего ПК, чтобы подключить ваш продукт.
2. Откройте веб-браузер (Internet Explorer, Chrome, Mozilla и т.д.) на вашем ПК.
3. Введите ***http://192.168.0.1 или http://192.168.100.1***, затем отобразится страница входа в систему. Идентификатором по умолчанию является слово **admin**, а паролем – **password**.



Быстрые настройки

На странице быстрой настройки можно просмотреть сетевую информацию и изменить SSID и пароль. Просто введите новый SSID и пароль, а затем нажмите **Применить**.

Чтобы настроить резидентный шлюз более детально, нажмите значок со стрелкой. После этого, вы сначала переходите к странице статуса соединения. Вы можете вернуться к странице быстрой настройки в любое время, нажав **Быстрая установка**.

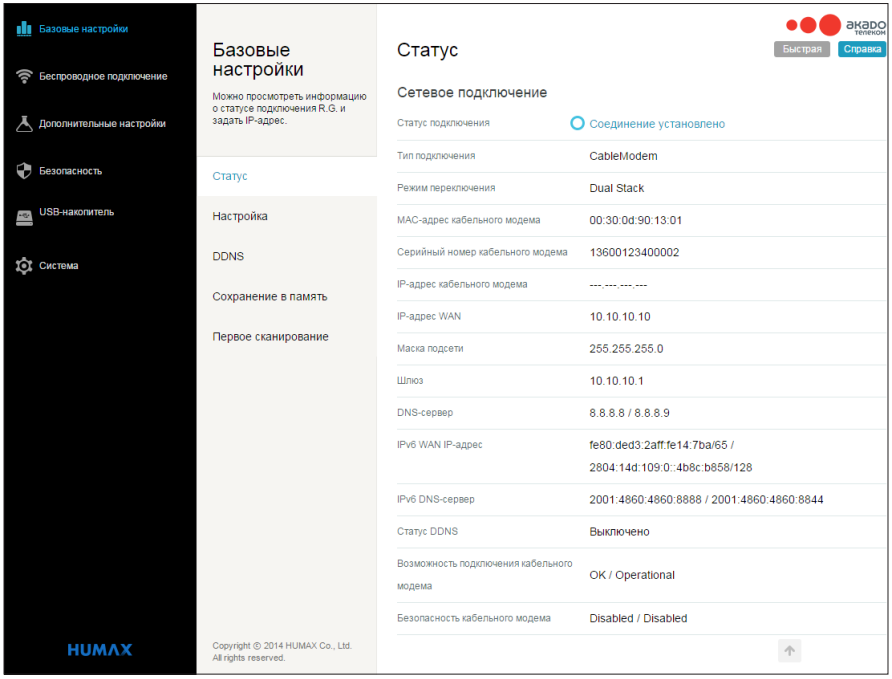


Информация о сети

Базовые настройки ➡ Статус

Вы можете проверить информацию о вашем продукте и сетевом подключении.

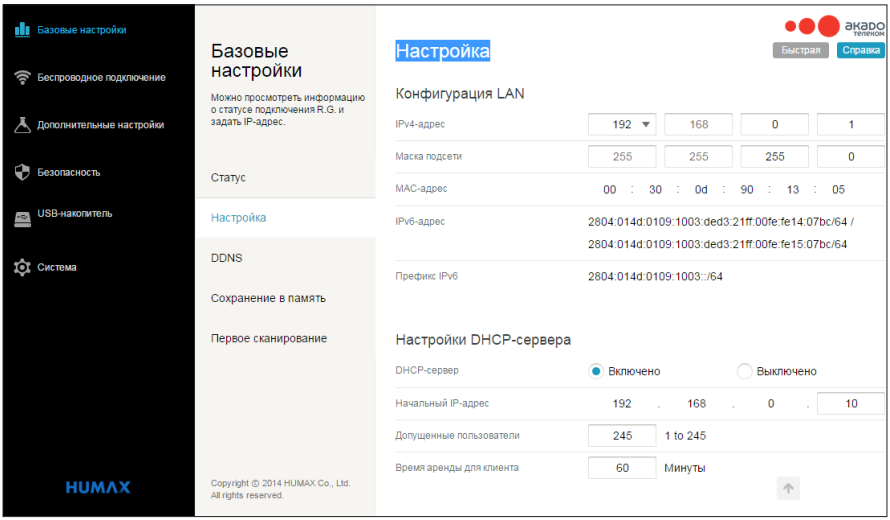
Примечание: Информация на этой странице может быть изменена в любое время при обновлении страницы веб-браузера.



Базовые настройки

Базовые настройки ➡ Настройка

Вы можете настроить основные функции резидентного шлюза и сетевого подключения. Введите необходимую информацию в поля, чтобы настроить резидентный шлюз.

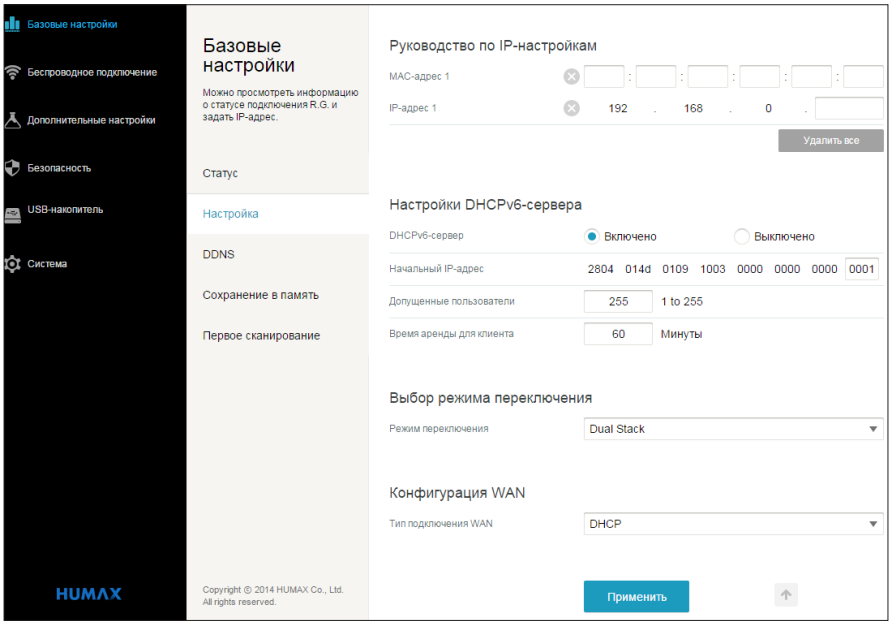


Конфигурация LAN

- **IPv4-адрес:** Введите IP-адрес резидентного шлюза вашей частной локальной сети.
- **Маска подсети:** Введите маску подсети для WAN-порта.
- **MAC-адрес:** Отображается адрес управления доступом к медиаданным.
- **IPv6-адрес:** Введите IPv6-адрес резидентного шлюза вашей частной локальной сети.
- **Префикс IPv6:** Формат адреса/длины префикса.

Настройки DHCP-сервера

- **DHCP-сервер:** Выберите **Включено**, чтобы включить DHCP-сервер в вашей локальной сети.
- **Начальный IP-адрес:** Введите начальный адрес, присваиваемый клиентам DHCP-сервером.
- **Допущенные пользователи:** Введите число клиентов, чтобы DHCP-сервер присвоил им частные IP-адреса.
- **Время аренды для клиента:** Введите количество времени, которое будет дано пользователю в аренду. По истечении этого времени пользователю будет автоматически присваиваться новый динамический IP-адрес.



Руководство по IP-настройкам

- **MAC-адрес:** Введите MAC-адрес, чтобы вручную назначить статический IP-адрес.
- **IP-адрес:** Введите IP-адрес, чтобы вручную назначить статический IP-адрес.

Настройки DHCPv6-сервера

- **DHCPv6-сервер:** Выберите Включено, чтобы включить DHCPv6-сервер в вашей локальной сети.
- **Начальный IP-адрес:** Введите начальный адрес, присваиваемый клиентам DHCP-сервером.
- **Допущенные пользователи:** Введите число клиентов, чтобы DHCP-сервер присвоил им частные IP-адреса.
- **Время аренды для клиента:** Введите количество времени, по истечении которого пользователю будет автоматически присваиваться новый динамический IP-адрес.

Выбор режима переключения

- **Режим переключения:** Выберите параметр.

  IPv4: Работает в режиме NAT при использовании IPv4-адреса

  IPv6: Работает в режиме NAT при использовании IPv6-адреса

  Двойной стек: Работает в режиме NAT при использовании как IPv4-, так и IPv6-адреса

  Мост: Работает в режиме моста

Конфигурация WAN

- **Тип подключения WAN:** Выберите параметр.

  DHCP: Автоматически присваивает IP-адреса клиентским устройствам.

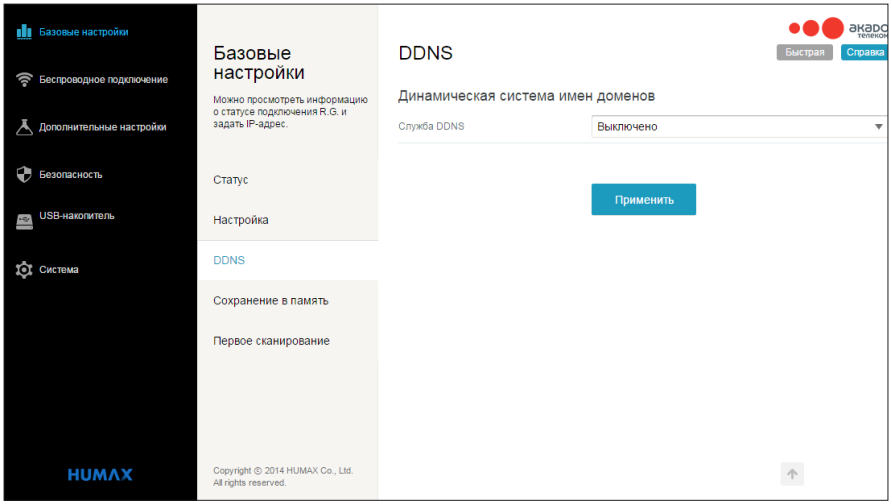
  Статический IP: Введите IP-адрес, маску подсети, шлюз и DNS.

Поддержка системы динамических доменов имен

Базовые настройки ➡ DDNS

Динамический DNS (DDNS) обеспечивает привязку динамического IP-адреса к статическому, предварительно заданному имени хоста, таким образом с этим хостом могут легко связаться другие хосты в Интернете, даже если его IP-адрес изменен.

Резидентный шлюз поддерживает динамический DNS-клиент, совместимый со службой динамического DNS или службой No-IP.



Динамическая система имен доменов

Как активировать DDNS-клиент

1. Перейдите на веб-сайт **http://www.dyndns.com** или **http://www.noip.com** и создайте учетную запись для службы динамического DNS.

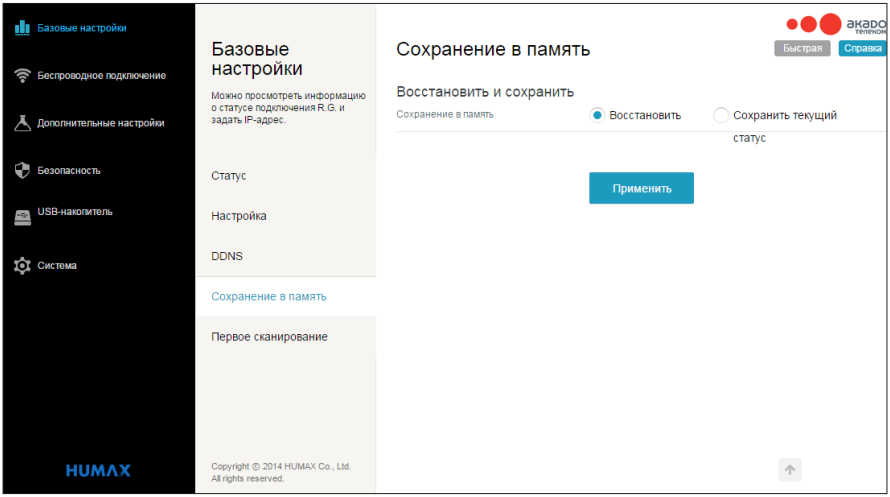
- Войдите в систему DynDNS или No-IP, используя имя пользователя и пароль.
- Перейдите в пункт My Account > My Services > Add Host Services.
- Введите имя хоста для сервера и выберите присваиваемый вашему хосту динамический DNS-домен.
- Проверьте интервал повторных попыток, в котором резидентный шлюз выполняет повторные попытки связаться с сервером доменных имен.
- Проверьте текущий IP-адрес вашего хоста. Это IP-адрес WAN, который был присвоен CMG во время подготовки. (См. IP-адрес WAN в меню Basic / Setup.)

2. На странице DDNS выберите **www.DynDNS.org** или **NoIP.com** из списка служб DDNS, чтобы включить данную службу, введите информацию вашей учетной записи, и нажмите **Применить**.
3. DDNS-клиент будет направлять уведомление в службу DDNS при каждом изменении IP-адреса WAN, таким образом, выбранное вами имя хоста будет обрабатываться надлежащим образом хостами, осуществляемыми запрос.

Резервная копия информации о конфигурации

Базовые настройки ➡ Сохранение в память

Вы можете сохранить текущие настройки конфигурации резидентного шлюза на локальном ПК. Вы можете восстановить эти настройки, если вам нужно восстановить определенную конфигурацию или отменить изменения, которые вы, возможно, внесли.



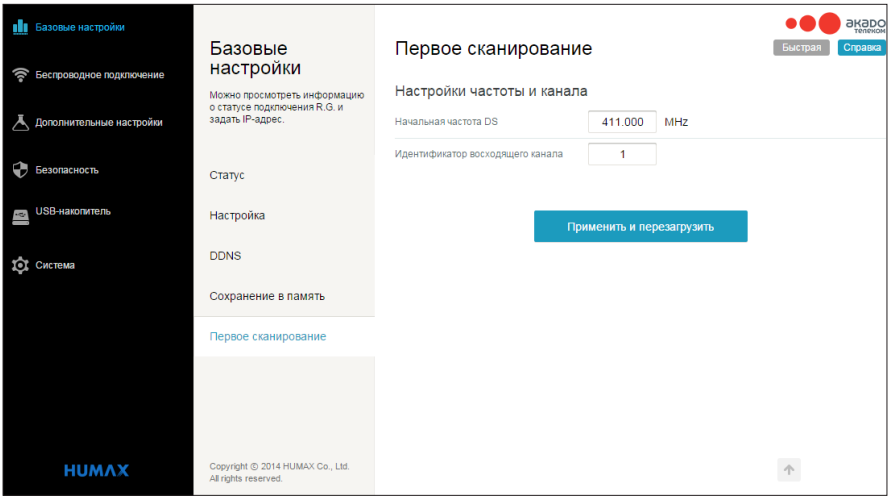
Для восстановления предыдущей конфигурации выберите **Восстановить** и выполните данную процедуру, чтобы восстановить предыдущие настройки.
Чтобы создать резервную копию текущей конфигурации, выберите **Сохранить текущий статус**.

Примечание: После восстановления настроек будет выполнен перезапуск вашего продукта.

Статус первоначального сканирования

Базовые настройки ➡ Первое сканирование

Вы можете настроить частоту запуска вашего продукта.



Настройки частоты и канала

- **Начальная частота DS:** Введите нисходящую частоту.
- **Идентификатор восходящего канала:** Введите идентификатор восходящего канала.

Нажмите **Применить и перезагрузить**, чтобы начать сканирование кабельной сети, начиная с вводимых значений.

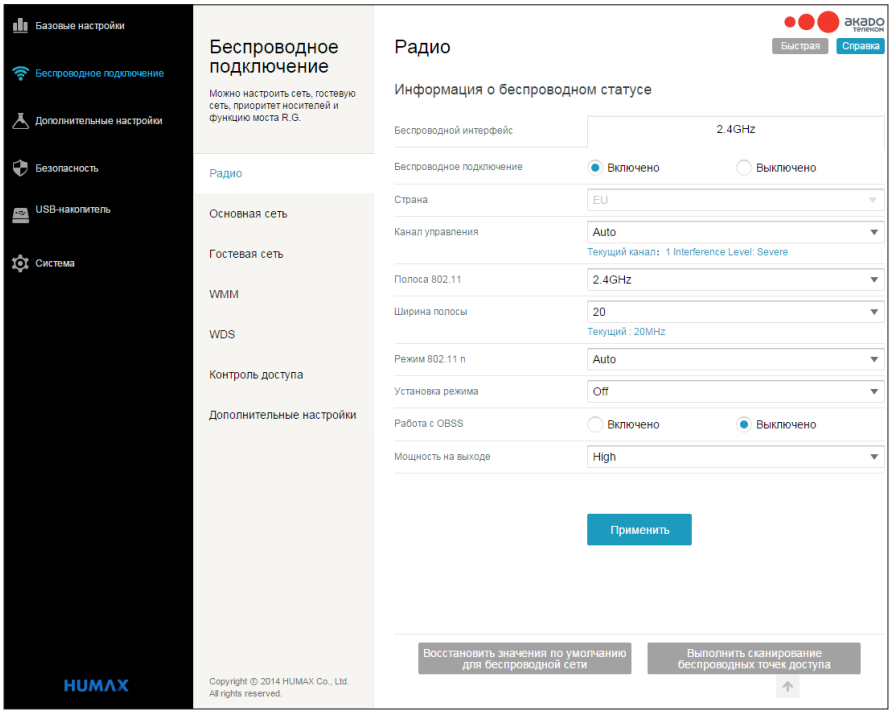
Примечание: Эта страница предназначена только для поставщика услуг. Не изменяйте вводимые значения, если вы не знаете, как выполнять данную операцию.

Ваш продукт также может быть использован в качестве беспроводной точки доступа IEEE 802.11 (ТД).
При установке платы беспроводной связи описанный ниже полный набор страниц конфигураций беспроводных подключений будет отображаться под меню Wireless.

Настройки радиосвязи

Беспроводное подключение ➡ Радио

Вы можете настроить физические параметры вашей беспроводной сети.



Информация о беспроводном статусе

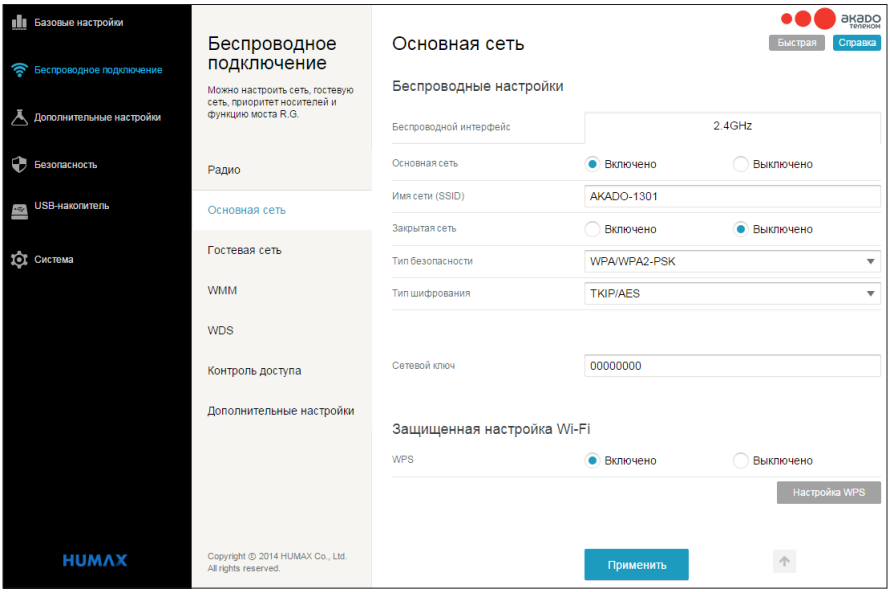
- **Беспроводное подключение:** Выберите **Включено**, чтобы включить беспроводной интерфейс.
- **Страна:** Ваша страна отображается с целью ограничения набора каналов на основе нормативных требований страны эксплуатации.
- **Канал управления:** Выберите канал для работы точки доступа. Список доступных каналов зависит от выбранной страны.
- **Полоса 802.11:** Выберите полосу 2,4 ГГц или 5 ГГц, в которой будет работать радиосвязь. При использовании полосы 5 ГГц существует вероятность меньшего количества помех от других беспроводных сетей и бытовых приборов, однако в этой полосе частот невозможно подключение устройств 802.11b/g.
- **Ширина полосы:** ширина полосы каналов 802.11b/g составляет всего 20 МГц. ширина полосы каналов 802.11n может составлять 40 МГц. При этом, существует некоторые проблемы обратной совместимости с каналами 40 МГц. Скорее всего, с подобными проблемами можно столкнуться при использовании полосы 2,4 ГГц, в котором унаследованные устройства (802.11b/g) могут функционировать, используя каналы 20 МГц.
- **Режим 802.11n:** Выберите **Auto**, чтобы использовать 802.11n-режим, позволяющий повышать скорость работы сети.
- **Режим регулирования:** Выберите опцию **Off,** протокол **802.11d** или **802.11h** для режима регулирования.
- **Сосуществование перекрывающихся базовых наборов служб (OBSS):** Выберите **Включено**, чтобы разрешить перекрытие совместимости служб спутникового вещания (BSS).
- **Мощность на выходе:** Выберите силу мощности на выходе.

Нажмите **Восстановить значения по умолчанию для беспроводной сети**, чтобы очистить все настройки и выполнить их сброс к значениям по умолчанию.
Нажмите **Выполнить сканирование беспроводных точек доступа**, чтобы дать команду точке доступа модема сканировать другие точки доступа в пределах принимаемого диапазона.

Настройки основной сети

Беспроводное подключение ➡ Основная сеть

Вы можете настраивать основную беспроводную сеть и задать настройки безопасности для нее.



Беспроводные настройки

- **Основная сеть:** Выберите **Включено** или **Выключено**, чтобы установить режим работы основной сети.
- **Имя сети (SSID):** Введите свое имя сети для основной сети. Для всех устройств в беспроводной сети должно быть указано одно имя сети и оно дол жно состоять из более, чем 8 символов.
- **Закрытая сеть:** Выберите **Включено**, чтобы скрыть имя сети. Вы можете предотвратить обнаружение вашей сети другими пользователями, когда они будут пытаться просмотреть наличие доступных беспроводных сетей.
- **Тип безопасности:** Установить режим общего ключа.

  WPA-PSK: Режим общего ключа алгоритма WPA, который не требует использования сервера RADIUS. Он также известен как WPA Personal. WPA и WPA-PSK не могут быть использованы одновременно.

  WPA2-PSK: Режим общего ключа WPA2, также известный как WPA2 Personal. WPA2 и WPA2-PSK не могут быть использованы одновременно. WPA2-PSK и WPA-PSK могут быть использованы одновременно с целью обеспечения обратной совместимости с устройствами, которые не поддерживают WPA2.

  WPA/WPA2-PSK: Режим общего ключа алгоритма WPA, который не требует использования сервера RADIUS. Он также известен как WPA Personal. WPA и WPA-PSK не могут быть использованы одновременно.

  WPA2-Enterprise: Расширенная форма WPA, которая является более безопасной. Это режим Enterprise алгоритма WPA2, который требует использования сервера RADIUS. WPA2 и WPA могут

быть использованы одновременно с целью обеспечения обратной совместимости с устройствами, которые не поддерживают WPA2.

WPA/WPA2-Enterprise: AES обеспечивает наиболее криптостойкое шифрование, в то время как TKIP обеспечивает криптостойкое шифрование с улучшенной обратной совместимостью. Режим TKIP + AES позволяет осуществлять подключение клиентов с поддержкой TKIP и AES.

WEP/Auto: Шифрование данных WEP используется при настройке беспроводных устройств на работу в режиме аутентификации общего ключа. Метод 64-битного шифрования данных WEP позволяет осуществлять ввод пяти символов (40-бит). Метод 128-битного шифрования данных WEP состоит из 104 конфигурируемых пользователем бит. Режим общего ключа WPA2, также известный как WPA2 Personal.

WPA2 и WPA2-PSK не могут быть использованы одновременно.
WPA2-PSK и WPA-PSK могут быть использованы одновременно с целью обеспечения обратной совместимости с устройствами, которые не поддерживают WPA2.

- **Тип шифрования:** Установите режим шифрования при использовании любой из схем аутентификации WPA.

  AES обеспечивает наиболее криптостойкое шифрование.

  TKIP/AES обеспечивает криптостойкое шифрование с улучшенной обратной совместимостью.

Защищенная настройка Wi-Fi

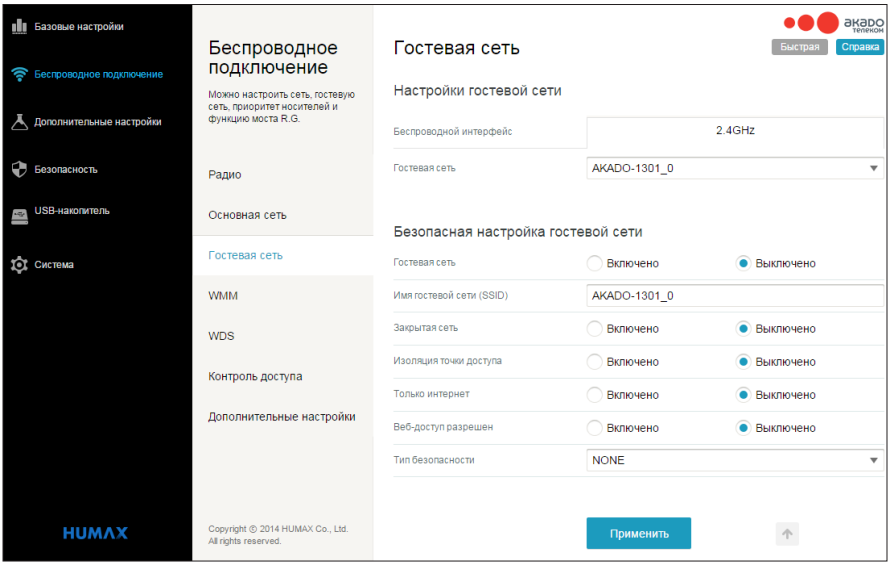
- **WPS:** Выберите **Включено**, чтобы создать безопасную беспроводную сеть и добавить беспроводные устройства к беспроводной сети.

  Нажмите кнопку **Настройка WPS**, чтобы создать беспроводное подключение WPS.

Настройки гостевой сети

Беспроводное подключение ➡ Гостевая сеть

Вы можете настроить гостевую сеть по беспроводному интерфейсу. Эта сеть изолирована от локальной сети. Все клиенты, которые связаны с SSID гостевой сети, будут изолированы от частной локальной сети и могут устанавливать связь исключительно через WAN-хосты только тогда, когда включена опция изоляции точки доступа.



Настройка гостевой сети

- **Гостевая сеть:** Выберите гостевую сеть, чтобы пользователи могли получить доступ к клиентам в вашей локальной сети.

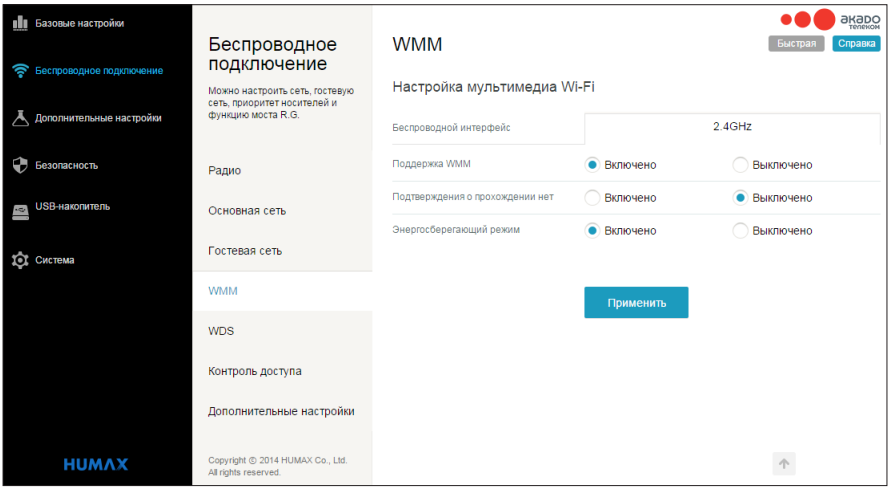
Безопасная настройка гостевой сети

- **Гостевая сеть:** Выберите **Включено** или **Выключено**, чтобы установить режим работы гостевой сети.
- **Имя гостевой сети (SSID):** Введите свое имя сети для гостевой сети.
- **Закрытая сеть:** Выберите **Включено**, чтобы скрыть имя сети. Вы можете предотвратить обнаружение вашей сети другими пользователями, когда они будут пытаться просмотреть наличие доступных беспроводных сетей.
- **Изоляция IP:** Выберите **Включено** или **Выключено**, чтобы установить изоляцию точки доступа. При выборе опции **Включено** каждое устройство изолируется от других. При выборе опции **Выключено** для общественной точки доступа любой пользователь может подключиться и начинать выполнять действия для просмотра или получения доступа к управлению другими устройствами в сети. Изоляция точки доступа предотвращает это и позволяет каждому пользователю сети быть уверенным в том, что обеспечена его полная безопасность.
- **Только интернет:** Выберите **Включено**, чтобы разрешить доступ в Интернет только для клиентских устройств в вашей гостевой сети. Клиентское устройство не может получить только доступ к пользовательскому веб-интерфейсу, но также устанавливать внутреннюю сеть.
- **Разрешен доступ к пользовательскому веб-интерфейсу:** Выберите **Включено**, чтобы разрешить доступ клиентского устройства к пользовательскому веб-интерфейсу.
- **Тип безопасности:** Установить режим общего ключа. Для ознакомления с опциями смотрите описания, приводимые в основной сети.

Настройки WMM

Беспроводное подключение ➡ WMM

Вы можете настроить протокол Wi-Fi Multimedia (WMM). WMM является воплощением качества обслуживания (QoS), которое определяется стандартом 802.11e.



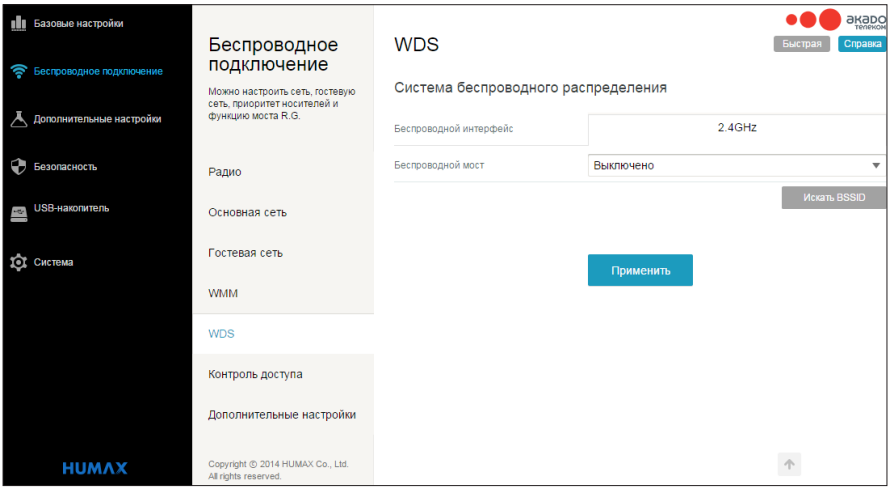
Настройка мультимедиа Wi-Fi

- **Поддержка WMM:** Выберите **Включено**, чтобы передавать или принимать мультимедийные данные по беспроводной сети.
- **Подтверждения о прохождении нет:** Выберите **Включено**, чтобы не принимать WMM ACK.
- **Энергосберегающий режим:** Выберите **Включено**, чтобы автоматически войти в режим ожидания, если устройство не будет работать в течение заданного времени.

Настройки WDS

Беспроводное подключение ➡ WDS

Вы можете настроить систему беспроводного распределения (WDS), которая также известна как беспроводной мост. WDS позволяет подключаться к нескольким беспроводным точкам доступа вместе от одной сети, используя беспроводную связь типа «точка-точка».



Система беспроводного распределения

- **Беспроводной мост:** Установите беспроводной мост с **WDSMaster** или **WDSSlave**.

  В режиме WDSMaster модем-маршрутизатор является главным устройством для группы беспроводной станции режима моста.
  Таким образом, весь трафик задается на это главное устройство, а не на другие точки доступа.

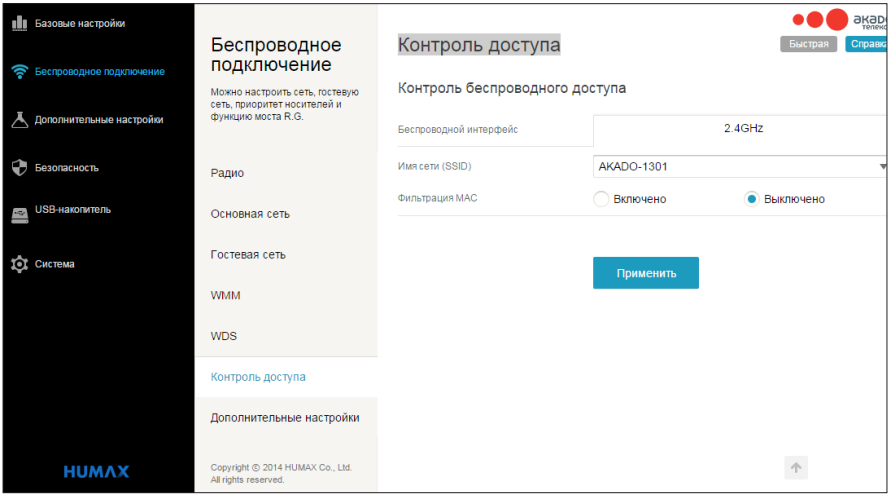
  В режиме WDSSlave модем-маршрутизатор связывается с другой беспроводной станцией режима моста.

- **Удаленные мосты:** Введите MAC-адреса удаленного моста, утвержденные для установки беспроводного моста. Могут быть подключены макс. 4 удаленных моста. Как правило, вы также необходимо будет ввести MAC-адрес вашей точки доступа на удаленном мосте.

Настройки доступа

Беспроводное подключение ➡ Контроль доступа

Вы можете выбирать, какие из беспроводных клиентов могут получить доступ к вашей беспроводной сети. Эта опция также предоставляет информацию о беспроводных клиентах, подключенных к вашей точке доступа.



Управление беспроводным доступом

- **Имя сети (SSID):** Выберите свою сеть, чтобы установить в ней беспроводной доступ.
- **Фильтрация MAC-адресов:** Выберите **Включено** или **Выключено**, чтобы разрешить или запретить беспроводной доступ беспроводной клиент с указанным MAC-адресом. Чтобы разрешить доступ всем клиентам, выберите **Выключено**.
- **Правило фильтрации:** Выберите **Разрешить** или **Отказать**, чтобы установить доступ для клиентского устройства.

MAC-адрес клиента

Эта настройка отображается при выборе опции **Включено** для фильтрации MAC-адресов в управлении беспроводным доступом.

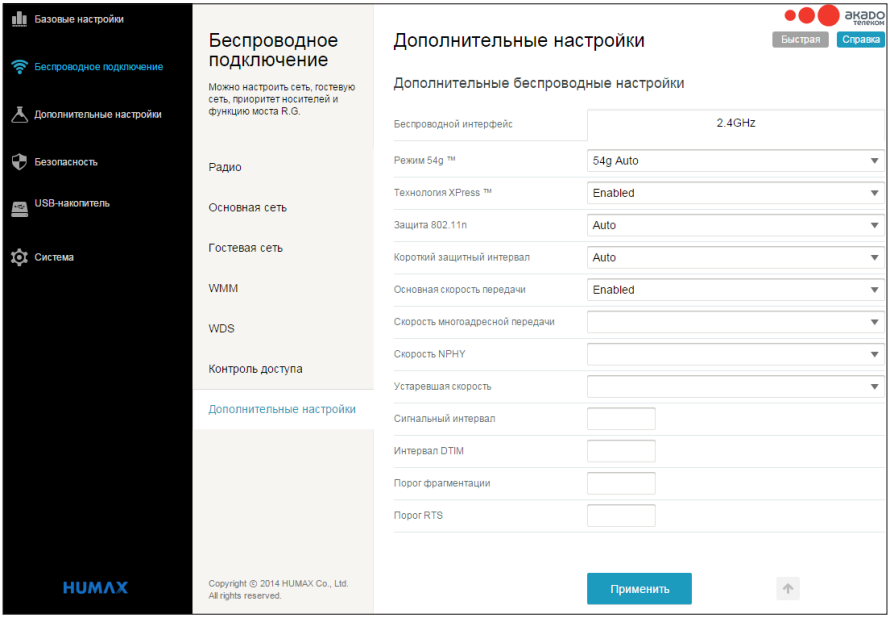
- **MAC 1/2/3:** Введите MAC-адрес беспроводного клиента, чтобы разрешить или запретить с использованием правила фильтрации.

Чтобы отобразить подключенных беспроводных клиентов, нажмите **Беспроводные клиенты**. Вы можете проверить информацию о клиенте, такую как идентификатор клиента, его MAC-адрес, сила сигнала и так далее.

Беспроводное подключение

Беспроводное подключение ➡ Дополнительные настройки

Вы можете конфигурировать дополнительные настройки беспроводного подключения. Большинство пользователей не имеют необходимости изменять эти настройки.



Дополнительная беспроводная настройка

- **Режим 54g™:** В качестве сетевого режима выбран режим **54g Auto**.

  Режим 54g Auto принимает клиентов с протоколами 54g, 802.11g и 802.11b, однако оптимизирует производительность на основе типа подключенных клиентов.
- **Технология XPress™:** Вы можете включить фирменный метод HUMAX подтверждения прохождения блока данных через протокол 802.11g. Эта функция может улучшить пропускную способность, но может привести к возникновению проблем.
- **Защита 802.11n:** Эта опция аналогична защите 54g, за исключением того, что она применяется к устройствам 802.11n.
- **Короткий защитный интервал:** Вы можете установить защитный интервал, чтобы избежать потери данных под воздействием помех или в результате задержек из-за многолучевого распространения.
- **Основная скорость передачи:** Вы можете проверить, какие скорости указываются как базовые, и можете установить все доступные скорости в качестве базовых. По умолчанию используются стандартные настройки драйвера.
- **Скорость многоадресной передачи:** Вы можете установить скорость многоадресной передачи, при которой многоадресные пакеты передаются в станции.
  Многоадресные пакеты не принимаются.
- **Скорость NPHY:** Вы можете выбрать скорость 802.11n, применяемую ко всем одноадресным пакетам.

- **Устаревшая скорость:** Вы можете принудительно задать скорость, при которой будет работать точка доступа. Данная опция активируется при **отключении** режима 802.11n.
- **Сигнальный интервал:** Вы можете установить сигнальный интервал в миллисекундах для точки доступа. Значение по умолчанию – 100, которое отлично подходит почти для всех приложений.
- **Интервал DTIM:** Вы можете установить интервал пробуждения для клиентов в энергосберегающем режиме. Если клиент работает в энергосберегающем режиме, то использование более низких значений обеспечивают более высокую производительность, но приводит к снижению времени работы клиента от батареи, в то время как использование более высоких значений обеспечивают меньшую производительность, но приводит к увеличению времени работы клиента от батареи.
- **Порог фрагментации:** Вы можете установить порог фрагментации. Пакеты, превышающие этот порог, фрагментируются в пакеты с размером, не превышающим текущее значение порога до момента передачи пакетов.
- **Порог RTS:** Вы можете установить порог RTS. Пакеты, превышающие этот порог, подают команду точке доступа на выполнение процедуры обмена RTS/CTS с целью сохранения среды беспроводного подключения перед передачей пакетов.

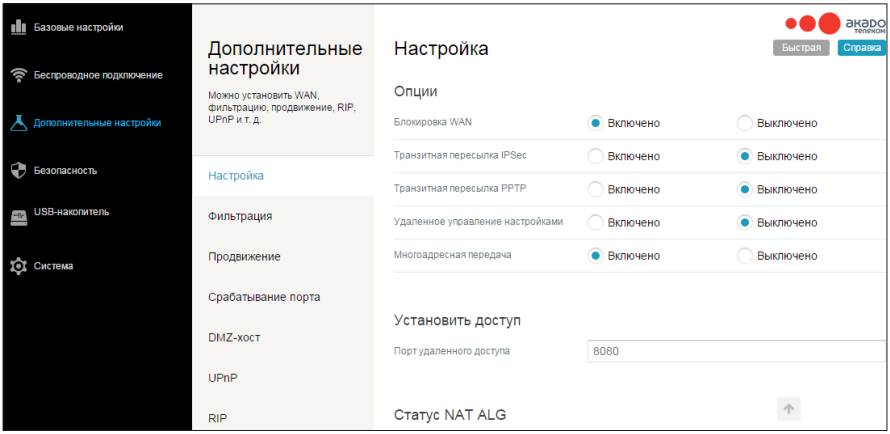
Ваш продукт поддерживает следующие дополнительные функции:

- Поддержка дополнительной блокировки WAN, передачи IPSec, передачи PPTP, удаленного управления, многоадресного режима и режима включения UPnP
- Фильтрация IP-адреса локальной сети, MAC-адреса и номера порта
- Переадресация и переключение с WAN на LAN
- Поддержка DMZ-хостинга (или отображаемого хоста)
- Включение Universal Plug and Play RIP-маршрутизатора

Расширенные настройки

Дополнительные настройки ➡ Настройка

Вы можете управлять вашим продуктом в нескольких режимах, которые регулируют методы маршрутизации IP-трафика устройством.

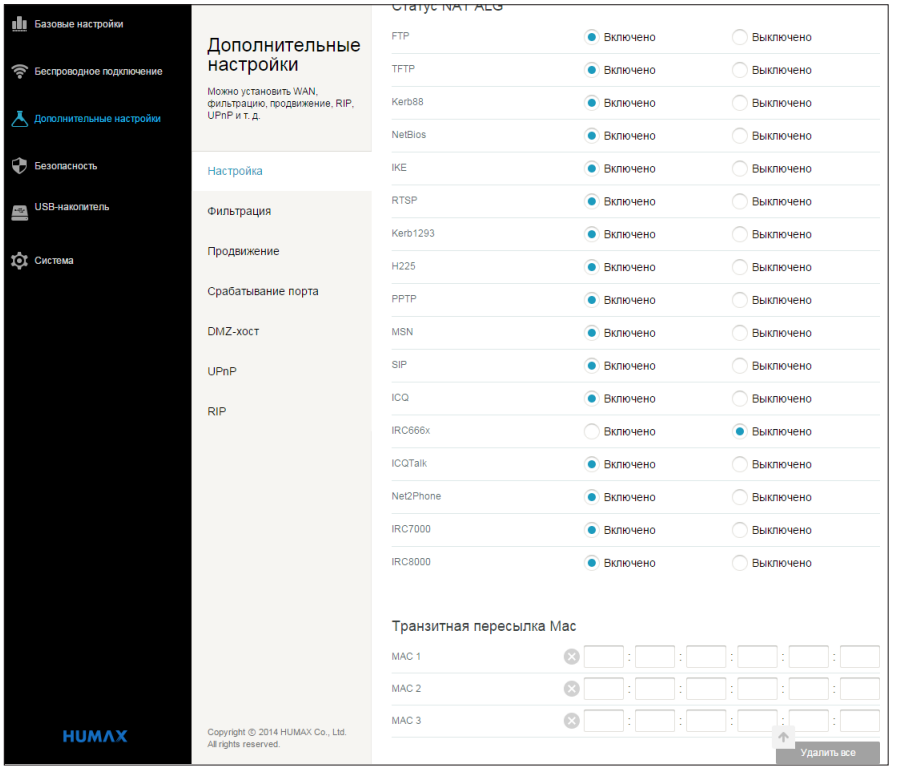


Опции

- **Блокировка WAN** скрывает резидентный шлюз или эксплуатируемый ПК от сети WAN. Например, к WAN IP-адресу резидентного шлюза или эксплуатируемому ПК, не возвращаются пакеты проверки связи. Таким образом, хакерам будет значительно труднее обнаружить ваш WAN IP-адрес, чтобы начать атаку на вашу частную локальную сеть.
- **Прохождение IPSec** и **прохождение PPTP** позволяет использовать эти протоколы через резидентный шлюз, в результате чего VPN-устройство или программное обеспечение может подключаться должным образом к сети WAN.
- **Удаленное управление конфигурацией** позволяет управлять (конфигурировать) резидентным шлюзом из глобальной сети WAN с помощью серфинга к WAN IP-адресу через порт 8080 резидентного шлюза из любой точки в Интернете (например, в окне URL браузера введите http://WanIPAddress:8080/, чтобы удаленно получить доступ к резидентному шлюзу).
- **Многоадресная передача** обеспечивает прохождение определенного трафика многоадресных пакетов (обозначаются конкретным адресом многоадресной передачи) в и из ПК по частной сети за резидентным шлюзом.

Установить доступ

- **Порт удаленного доступа:** Введите номер порта сервера для удаленного доступа. Для повышения безопасности введите порт (1~65535), за исключением 80.



Статус NAT ALG

NAT ALG – это шлюз прикладного уровня, который осуществляет преобразование сетевых адресов. Вы можете включать или выключать эти компоненты брандмауэра.

Чтобы включить функцию, выберите опцию, а затем **Применить**. Эти опции могут быть изменены без перезагрузки системы.

Примечание: Использование дополнительных настроек рекомендуется только для опытных пользователей. Если вы не знаете как выполнять данную операцию, не изменяйте настройки на этой странице.

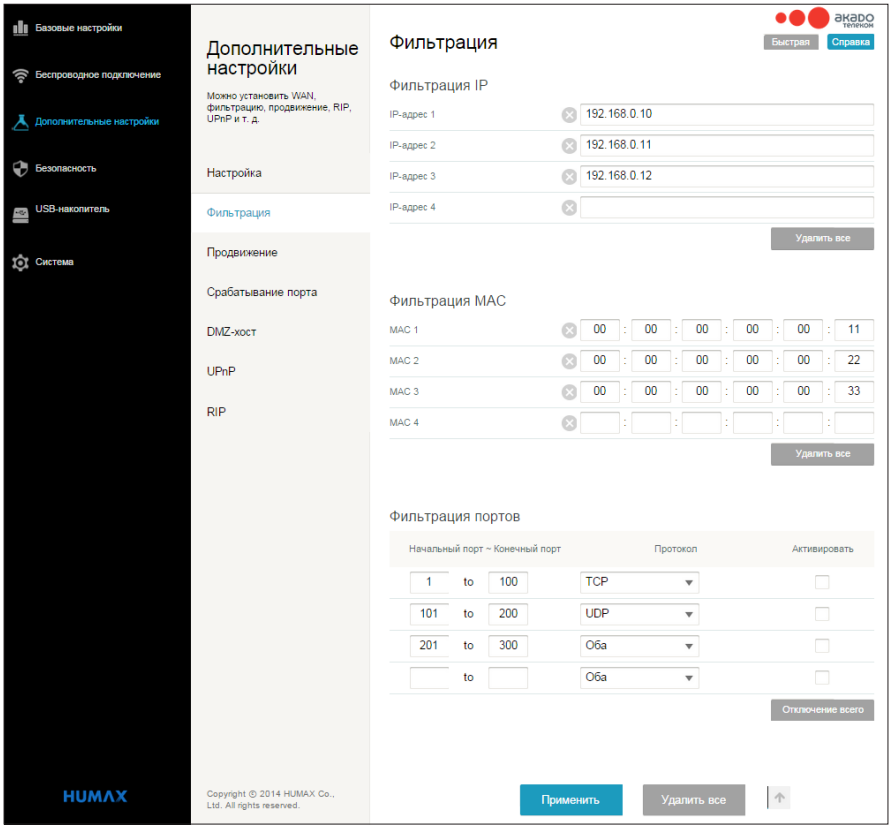
Прохождение пакетов через Mac-адрес

Введите MAC-адрес, чтобы назначить внешний IP-адрес.

Фильтрация

Дополнительные настройки ➡ Фильтрация

Вы можете настроить брандмауэр на осуществление фильтрации пакетов, следовательно, разрешить или запретить трафик данных для обеспечения безопасности данных.



Фильтрация IP

Вы можете настроить резидентный шлюз таким образом, чтобы локальные ПК не получали доступ к глобальной сети WAN, указав IP-адреса, которые должны фильтроваться.
Введите IP-адреса тех локальных ПК, которые будут лишены доступа к глобальной сети WAN.

Фильтрация MAC

Вы можете запретить ПК отправку исходящего TCP-/UDP-трафика в сеть WAN через их MAC-адреса.

Эта опция полезна с точки зрения того, что MAC-адрес конкретного сетевого адаптера (NIC) никогда не изменяется, в отличие от его IP-адреса, который может быть назначен через DHCP-сервер или может жестко кодироваться по различным адресам в течение долгого времени.

Фильтрация портов

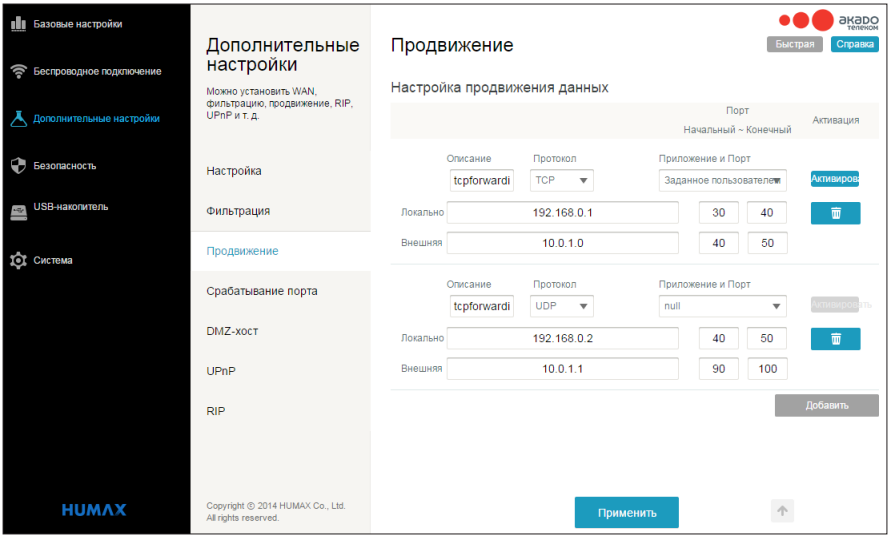
Вы можете запретить ПК отправку исходящего TCP-/UDP-трафика в сеть WAN по конкретным номерам IP-портов. Введите начальный и конечный диапазон портов, чтобы определить, какой TCP-/UDP-трафик будет отправляться в сеть WAN на попортовой основе.

Примечание: Указанные диапазоны портов блокируется для ВСЕХ ПК и этот параметр не относится к IP-или MAC-адресу.

Переадресация портов

Дополнительные настройки ➡ Продвижение

Вы можете запустить общедоступный сервер в локальной сети, установив отображение TCP-/UDP-портов для локального ПК.



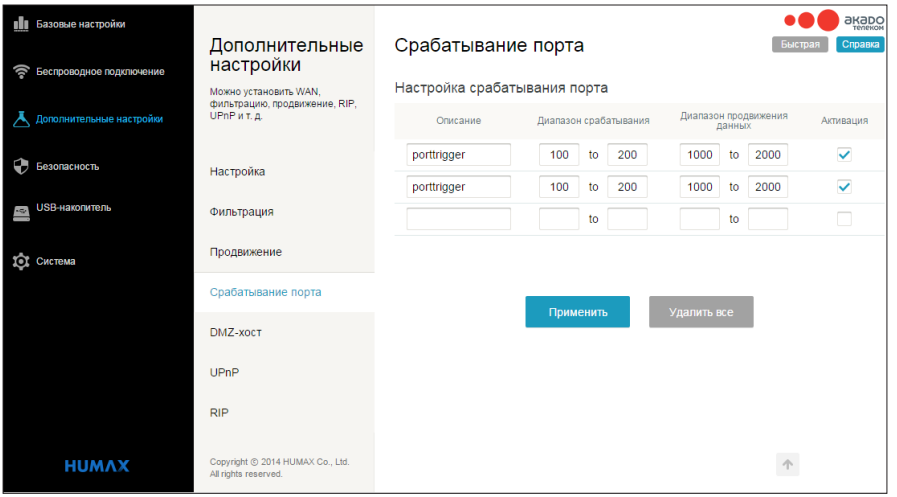
Чтобы установить отображение портов, введите диапазон номеров портов, переадресация которых будет осуществляться локально, а также IP-адрес, по которому на эти порты будет отправляться трафик.

Примечание: Если вы хотите установить отображение только одного порта, введите один и тот же номер порта в начальном и конечном портах для этого IP-адреса.

Срабатывание портов

Дополнительные настройки ➡ Срабатывание порта

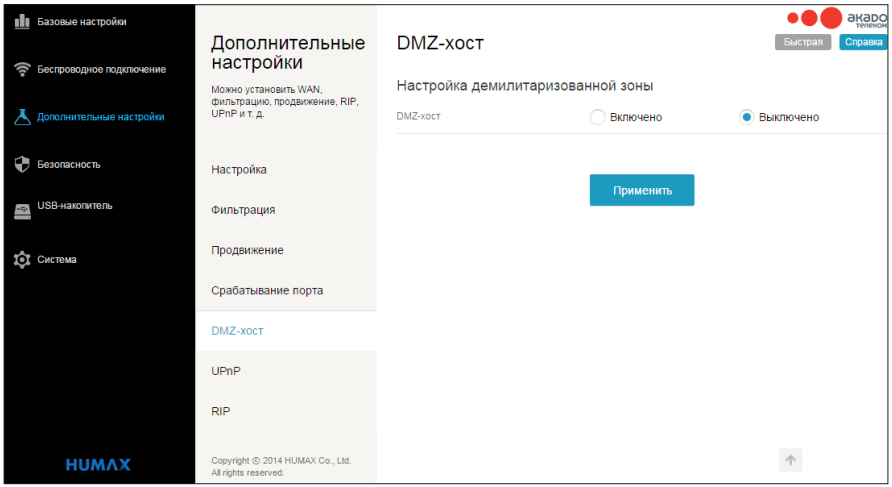
Опция срабатывание портов аналогична опции переадресации порта, за исключением того, что используемые порты не являются статическими портами, открытыми на постоянной основе. Когда резидентный шлюз обнаруживает исходящие данные по определенному номеру IP-порта, установленному в срабатываемом диапазоне, то порты, установленные в переадресованном диапазоне открываются для приема входящих (или иногда называются двунаправленными портами) данных. Если исходящий трафик не обнаружен по портам в срабатываемом диапазоне в течение 10 минут, то переадресованный диапазон портов закрывается. Это более безопасный метод для открытия определенных портов для специальных приложений (например, программ видеоконференц-связи, интерактивных игр, передачи файлов в чат-программах и т.д.), поскольку они динамически срабатывает и не остаются постоянно открытыми или ошибочно оставленными открытыми с помощью администратора маршрутизатора и подвержены обнаружению потенциальными хакерами.



DMZ-хостинг

Дополнительные настройки ➡ DMZ-хост

DMZ-хостинг (демилитаризованная зона) (также известен как «Отображаемый хост» (Exposed Host)) позволяет указать получателя по умолчанию WAN-трафика, который NAT не в состоянии преобразовать в известный локальный ПК. Этот хост также можно рассматривать как компьютер или небольшую подсеть, которая находится между защищенной внутренней частной сетью и незащищенным общественным Интернетом.

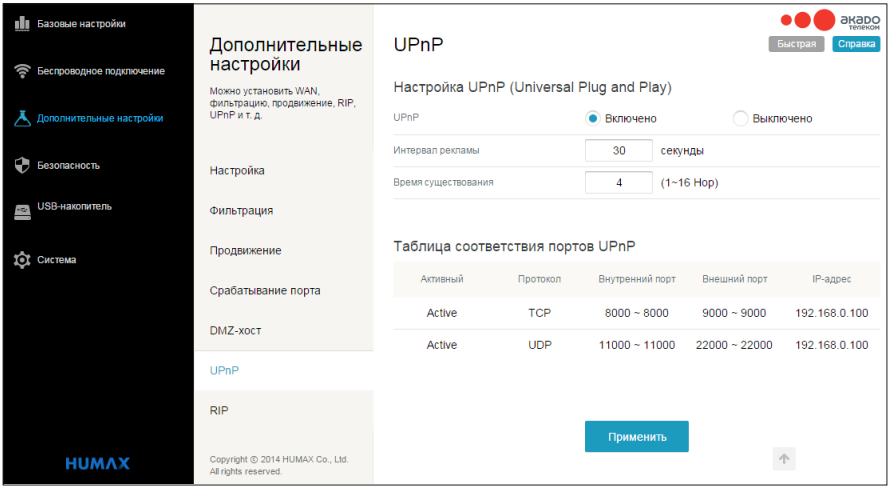


Вы можете настроить один компьютер в качестве DMZ-хоста. Как правило, этот параметр используется для проблемных приложений используемых на ПК, которые используют случайные номера портов и не функционируют надлежащим образом с конкретными опциями настроек срабатывания или переадресации портов, которые были упомянуты ранее. Если конкретный ПК настроен в качестве DMZ-хоста, не забудьте установить обратно значение 0 после завершения работы с требуемым приложением, поскольку этот ПК будет существенно подвергаться угрозам общественного Интернета, не смотря на то, что он по-прежнему будет защищен от атак отказа в обслуживании (DoS) через брандмауэр.

Настройка UPnP

Дополнительные настройки ➡ UPnP

Universal Plug and Play (UPnP) помогает таким устройствам, как интернет-устройства и компьютеры, получать доступ к сети и подключаться к другим устройствам. Устройства UPnP могут автоматически обнаруживать службы других зарегистрированных устройств UPnP в сети.



Настройка UPnP (Universal Plug and Play)

- **UPnP:** включает UPnP-агент в резидентном шлюзе. Если вы работаете в CPE-приложение, которое требует использования UPnP, выберите **Включено**.
- **Интервал извещения:** Введите время передачи UPnP-информации в каждый заданный период времени.
- **Время существования:** Введите число раз, чтобы ограничить срок службы UPnP.

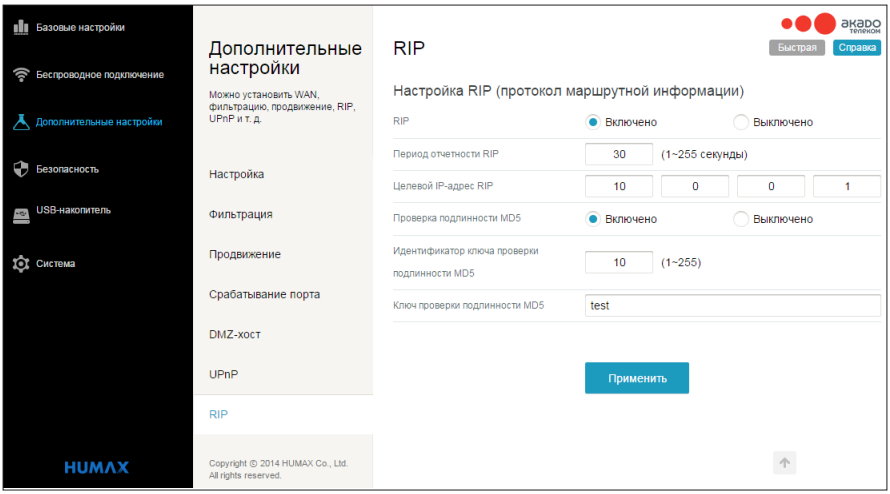
Таблица сопоставления портов UPnP

Вы можете видеть рабочее состояние по набору переадресации портов UPnP.

Настройка RIP

Дополнительные настройки ➡ RIP

Протокол маршрутизации (RIP) является одним из старейших протоколов дистанционно-векторной маршрутизации, который использует число прыжков в качестве метрика маршрутизации. RIP предотвращает образование петель маршрутизации путем установки ограничение на количество прыжков, допустимых по маршруту от источника к месту назначения.



Протокол маршрутизации

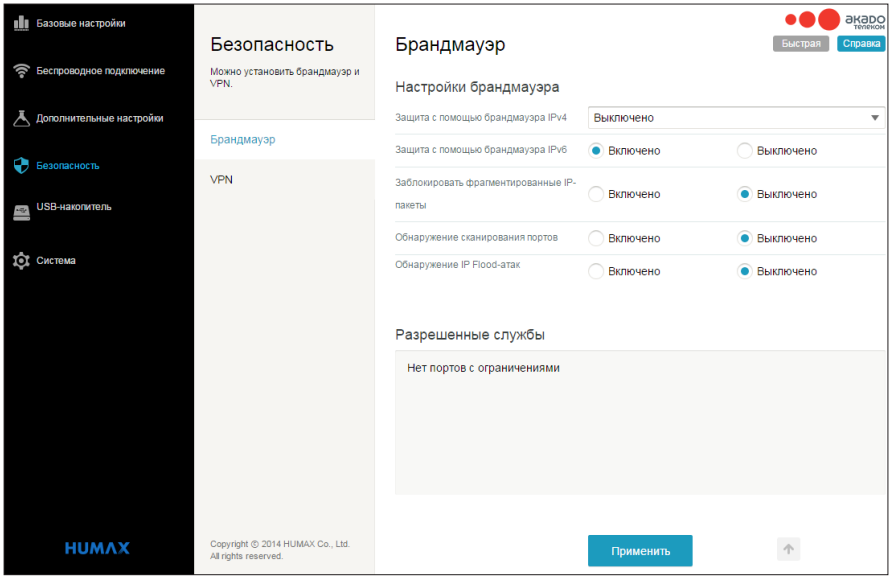
- **RIP:** Выберите **Включено**, чтобы активировать протокол маршрутизации (RIP).
- **Интервал отчетности RIP:** Введите время обновления маршрута в каждый заданный период времени.
- **Целевой IP-адрес RIP:** Введите целевой адрес хоста или сети.
- **Проверка подлинности MD5:** Выберите **Включено**, чтобы принять проверку подлинности MD5.
- **Ключ проверки подлинности MD5:** Введите пароль проверки подлинности MD5.
- **Идентификатор ключа проверки подлинности MD5:** Введите индекс ключа проверки подлинности MD5.

Резидентный шлюз содержит встроенное приложение брандмауэра для защиты частной локальной сети от вредоносных атак из WAN-интерфейса.

Настройки брандмауэра

Безопасность ➡ Брандмауэр

На странице веб-фильтра имеются различные настройки, связанные с блокированием или исключительным разрешением на передачу различных типов данных через резидентный шлюз из глобальной сети WAN в локальную сеть LAN.



Настройка брандмауэра

- **Защита с помощью брандмауэра IPv4:** Выберите опцию защиты брандмауэра.

  При выборе опции **Выключено** активируется передача всего трафика.

  Опция **Low** не блокирует какие-либо службы/порты, однако она действительно защищает от недопустимых пакетов и хорошо известных атак.

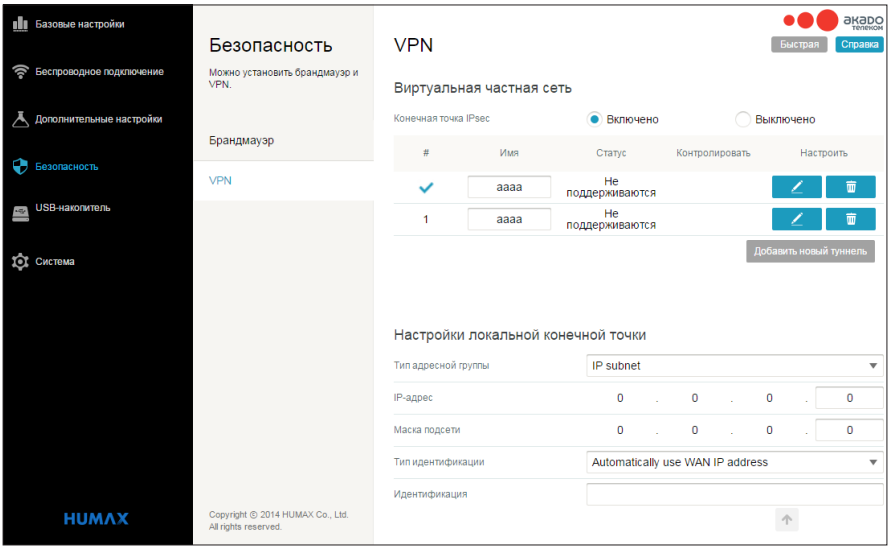
  Выбор опции **Medium** может привести к отбрасыванию брандмауэром пакета, если только он не передается по определенному порту разрешенных служб. Разрешенные службы перечислены на той же странице.

  Опция **High** аналогична опции Medium, но позволяет получить доступ к еще меньшему количеству служб.
- **Защита с помощью брандмауэра IPv6:** Выберите **Включено**, чтобы установить защиту с помощью брандмауэра IPv6.
- **Заблокировать фрагментированные IP-пакеты:** Выберите **Включено**, чтобы заблокировать прохождение фрагментированных IP-пакетов через брандмауэр.
- **Обнаружение сканирования портов:** Выберите **Включено**, чтобы обнаружить и заблокировать процесс сканирования порта, происходящий как в локальной LAN, так и в глобальной сети WAN.
- **Обнаружение IP Flood-атак:** Выберите **Включено**, чтобы включить обнаружение брандмауэром IP flood-атак.

Конфигурация VPN

Безопасность ➡ VPN

Вы можете настроить несколько VPN-туннелей на различных клиентских ПК. Различные туннели могут быть сконфигурированы и сохранены, но не включены для обеспечения простоты использования вместе с подключениями и (или) клиентскими ПК, которые не используются на постоянной основе. Уникальные IPsec-параметры каждой конфигурации туннеля сохраняются через меню IPsec Settings в нижней части страницы.



Виртуальная частная сеть

- **Конечная точка IPsec:** Выберите **Включено** или **Выключено** для вкл./выкл. режима конечной точки IPsec.
- **Имя (Name):** отображение пользовательского имени туннеля
- **Статус (Status):** отображение текущего состояния подключения
- **Управление (Control):** Выберите опцию на основании текущего состояния туннельного подключения.

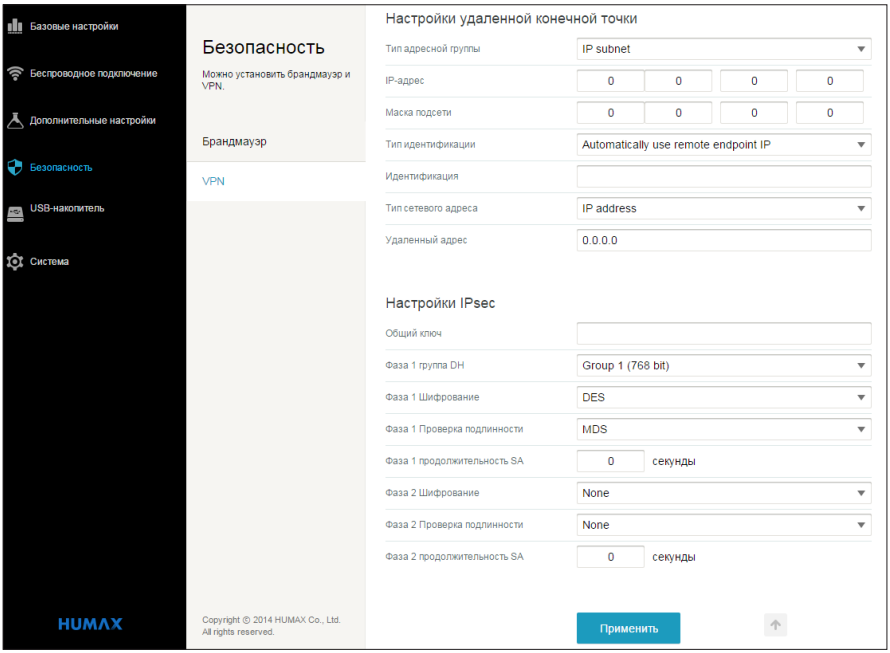
  Выберите **Включено**, чтобы активировать VPN-сервер.

  Выберите **Выключено**, чтобы деактивировать VPN-сервер.

  Выберите **Подключить**, чтобы подключиться к VPN-серверу.

  Выберите **Отключить**, чтобы отключиться от VPN-сервера.
- **Настроить:** Нажмите **Редактировать** или **Удалить**, чтобы настроить VPN-туннель.

Нажмите кнопку **Добавить новый туннель**, чтобы создать конфигурацию нового туннеля.



Настройки локальной конечной точки

- **Тип адресной группы:** Локальная группа доступа VPN может быть настроена здесь в качестве конкретного одинарного IP-адреса одного компьютера, диапазона IP-адресов, покрывающего небольшую группу компьютеров, или в качестве целой подсети/сети.

  Выберите **IP Subnet**, чтобы ввести информацию подсети и маски.

  Выберите **Single IP address**, чтобы ввести только конкретный IP-адрес.

  Выберите **IP address range**, чтобы ввести начальный и конечный IP-адреса для создания пула последовательных IP-адресов, которые будут иметь доступ к VPN-туннелю.
- **IP-адрес:** Введите конечный IP-адрес в вашей локальной сети, чтобы задать VPN.
- **Маска подсети:** Введите маску подсети.
- **Тип идентификации:** Вы можете установить тип идентификации локальной конечной точки, чтобы автоматически использовать WAN IP-адрес маршрутизатора или в качестве пользовательского IP-адреса, полного доменного имени (FQDN), или адреса электронной почты.
- **Идентификация:** После выбора из вышеуказанных позиций типа идентификации здесь необходимо заполнить строку идентификации. Для режима IP адреса необходимо просто ввести x.x.x.x. В строке доменного имени будет введено «yourdomain.com», а в строк идентификации адреса электронной почты – «yourname@yourdomain.com». Удаленная конечная точка VPN на другой стороне туннеля должна соответствовать указанным здесь параметрам для настройки ее удаленной конечной точки.

Настройки удаленной конечной точки

Вы можете задать параметры удаленной конечной точки таким же образом, как и в меню «Настройки локальной конечной точки» (Local Endpoint Setting) и, таким образом осуществить подключение к удаленной сети, как при подключении к локальной сети напрямую.

- **Тип сетевого адреса:** Выберите IP-адрес или полное доменное имя (FQDN) для типа WAN-адреса удаленной конечной точки.
- **Удаленный адрес:** Введите либо IP-адрес удаленной конечной точки или его полное доменное имя, в зависимости от того, какой тип сетевого адреса выбран из вышеперечисленных.

Настройка IPsec

У VPN-туннелей существует две фазы сопоставления безопасности (SA). Фаза 1 используется для создания IKE SA. После завершения фазы 1 используется фаза 2 для создания одного или более сопоставлений безопасности IPSEC SA, которые в дальнейшем используются для ключевых сессий IPSec.

- **Общий ключ:** Если одна сторона VPN-туннеля использует уникальный идентификатор брандмауэра (или общий ключ), то его необходимо вводить в поле «Pre-shared Key».
- **Фаза 1 группа DH:** Выберите группу Диффи-Хелмана. Диффи-Хелман – это криптографическая технология, которая использует общие и частные ключи для шифрования и дешифрования. Чем больше число битов выбрано, тем более высокая степень безопасности.
- **Фаза 1 Шифрование:** Шифрование используется для защиты VPN-подключения между конечными точками. Доступны пять различных типов шифрования. Может быть выбрана любая форма шифрования, которая может быть совместима с дальней конечной точкой. Одной из наиболее распространенных здесь настроек является 3DES; при этом, AES также является очень эффективным методом шифрования.
- **Фаза 1 Проверка подлинности:** Проверка подлинности представляет собой еще один уровень безопасности. Рекомендуется использовать надежный алгоритм хэширования (SHA), поскольку он является более безопасным. Может быть использован любой тип проверки подлинности при условии, что другая конечная точка VPN-туннеля использует тот же метод.
- **Фаза 1 продолжительность SA:** В этом поле задается срок службы отдельных вращающихся ключей. Введите время срока действия ключа до выполнения повторного согласования ключей между каждой конечной точкой. Как правило, меньший срок действия является более безопасным, так как в таком случае хакеру предоставляется меньшее количество времени для взлома ключа, однако процесс согласования ключей нагружает полосу пропускания, что приводит к уменьшению пропускной способности сети при применении небольших сроков действия ключей. Как правило, сюда вводятся значения в тысячах или десятках тысяч секунд.
- **Фаза 2 Шифрование:** Шифрование используется для защиты VPN-подключения между конечными точками. Доступны пять различных типов шифрования: Может быть выбрана любая форма шифрования, которая может быть совместима с дальней конечной точкой. Одной из наиболее распространенных здесь настроек является 3DES; при этом, AES также является очень эффективным методом шифрования и рекомендуемым решением, так как является очень стойким ко взлому.
- **Фаза 2 Проверка подлинности:** Проверка подлинности представляет собой еще один уровень безопасности. Доступны три типа проверки подлинности: Рекомендуется использовать надежный алгоритм хэширования (SHA), поскольку он является более безопасным. Может быть использован любой тип проверки подлинности при условии, что другая конечная точка VPN-туннеля использует тот же метод.
- **Фаза 2 продолжительность SA:** В этом поле задается срок службы отдельных вращающихся ключей. Введите время срока действия ключа до выполнения повторного согласования ключей между каждой конечной точкой. Как правило, меньший срок действия является более безопасным, так как в таком случае хакеру предоставляется меньшее количество времени для взлома ключа, однако процесс согласования ключей нагружает полосу пропускания, что приводит к уменьшению пропускной способности сети при применении небольших сроков действия ключей. Как правило, сюда вводятся значения в тысячах секунд.

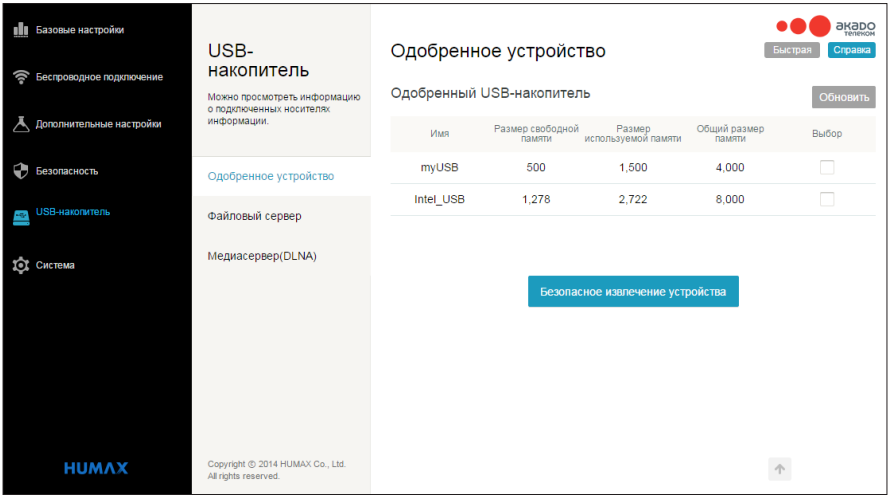
Ваш продукт имеет USB-порт для подключения внешнего жесткого диска, который позволяет обмениваться файлами и папками с другими пользователями посредством беспроводной связи.

Настройка USB-накопителя

USB-накопитель ➡ Одобренное устройство

Вы можете видеть информацию о подключенном внешнем устройстве хранения данных.

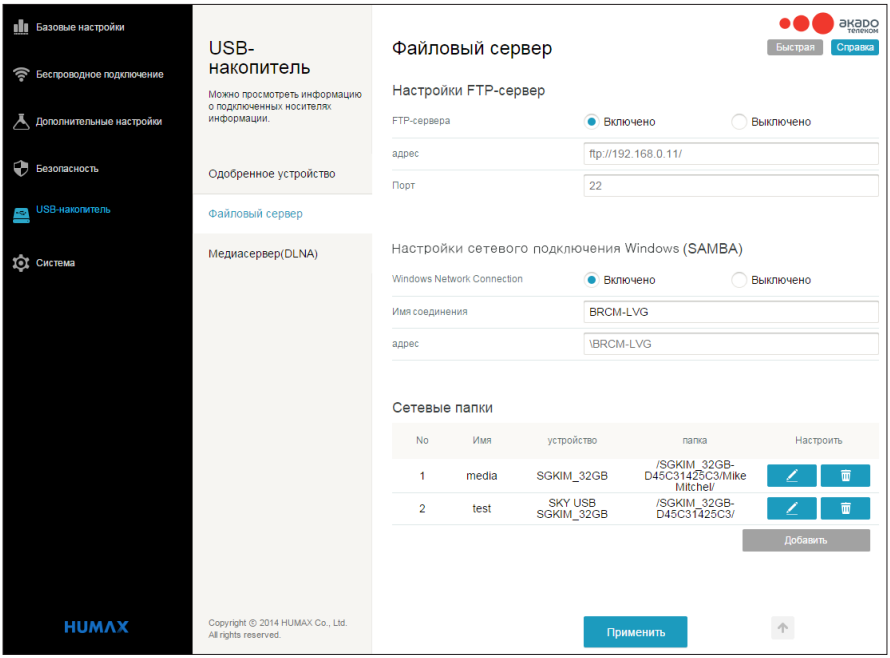
Чтобы отключить USB-накопитель от продукта, выберите USB-накопитель, а затем нажмите **Безопасное извлечение устройства**.



Настройка файлового сервера

USB-накопитель ➡ Файловый сервер

Вы можете настроить FTP-сервер или сетевой сервер для обмена файлами или папками с внешним устройством хранения данных через Интернет.



Настройки файлового сервера

- **FTP-сервер:** Выберите **Включено**, чтобы активировать FTP-сервер.
- **Адрес:** Отображает IP-адрес, необходимый для получения доступа к USB-накопителю.
- **Порт:** Введите номер порта, чтобы получить доступ к USB-накопителю.

Настройки сетевого подключения Windows (SAMBA)

- **Windows Network Connection:** Выберите **Включено**, чтобы активировать сетевое подключение Windows (SAMBA) для получения доступа к USB-накопителю.
- **Имя подключения:** Введите имя сетевого подключения Windows, чтобы получить доступ к USB-накопителю.
- **Адрес:** Вы можете получить доступ к USB-накопителю, используя введенный вами адрес.

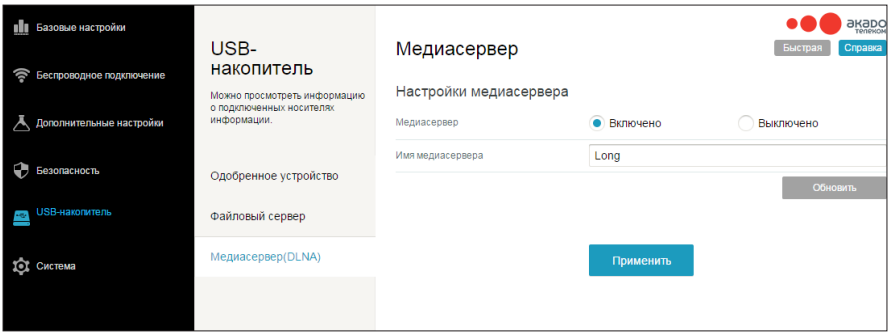
Сетевые папки

Вы можете добавлять или редактировать сетевые папки.

Настройки медиасервера

USB-накопитель ➡ Медиасервер (DLNA)

Вы можете настроить совместимые устройства домашней сети. Вы можете обмениваться файлами с другими пользователями, которые находятся в той же сети, что и ваш продукт.

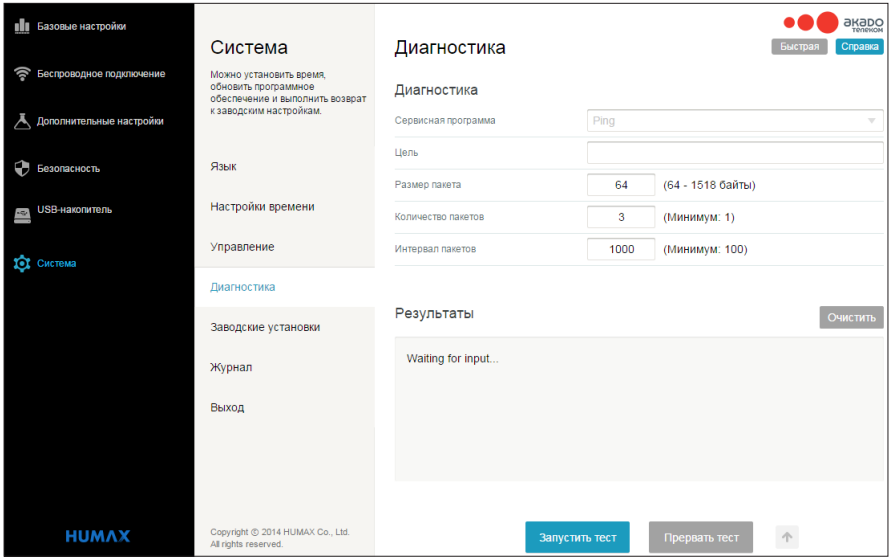


- **Медиа-сервер:** Выберите **Включено**, чтобы активировать медиа-сервер, отсканированных на подключенном USB-накопителе.
- **Имя медиа-сервера:** Введите имя медиа-сервера.

  Нажмите **Обновить**, чтобы обновить медиа-сервер, а затем нажмите **Применить**.

Системные настройки

Вы можете проверить текущее время в системе, изменить пароль или восстановить продукт к заводским настройкам.



Язык

Вы можете установить язык системы.

Настройка часового пояса

Вы можете видеть текущее время, установленное на устройстве Несколько устройств синхронизируются одновременно.

Управление

Вы можете изменить свой пароль. Дважды введите новый пароль. Нажмите **Применить**, чтобы сохранить изменения.

Диагностика

Вы можете видеть средства устранение неисправностей подключения. Для устранение неисправностей сетевого подключения предназначены две утилиты.

- **Утилита:** Выберите значение пакета проверки связи для диагностического испытания
- **Цель:** Введите IP-адрес конечного назначения.
- **Размер пакета:** Введите размер пакета проверки связи в диапазоне от 64 до 1 518 байт для отправки по адресу конечного назначения.
- **Количество пакетов:** Введите число пакетов проверки связи, чтобы отправить их по адресу конечного назначения.
- **Интервал пакетов:** Введите временной интервал периодической отправки пакета проверки связи. Значение колеблется в диапазоне 100–3 600 000 миллисекунд, а значение по умолчанию составляет 1 000 миллисекунд.

Примечание: Для запуска каждой утилиты внесите какие-либо изменения в параметры по умолчанию и нажмите Запустить тест, чтобы начать. Окно автоматически обновится после отображения результатов в таблице Результаты.

Сброс к заводским настройкам

Вы можете восстановить свой продукт к заводским настройкам по умолчанию. Чтобы восстановить заводские настройки по умолчанию, выберите **Да** и нажмите **Применить**.

Предупреждение: После восстановления заводских настроек по умолчанию будет осуществлен сброс всех сконфигурированных пользователем данных.

Журнал

Вы можете ознакомится с информацией о события, происходящих на вашем устройстве.

Выход

Будет выполнен автоматический выход вашей учетной записи из системы.

Specification

Размер (Ш x Г x В)	225 x 155 x 44 (мм)
Вес	440 г
Напряжение на входе	12В ⎓ 1,5А
Потребляемая мощность	17 Вт
Рабочая температура	0° – 40°C

Примечание: Технические характеристики подлежат изменению без уведомления.

Примечание о программном обеспечении с открытым исходным кодом

Этот продукт включает в себя программный код, разработанный третьей стороной, который, включая программный код, подпадающий под действие стандартной общественной лицензии (GPL) GNU или стандартной общественной лицензии ограниченного применения (LGPL) GNU. При необходимости с условиями лицензий GPL и LGPL, а также информацией о получении доступа к коду GPL и LGPL, используемого в этом продукте, можно ознакомится, перейдя по ссылке http://192.168.0.1/GPL/ (включая веб-интерфейс RG).

Коды GPL и LGPL, используемые в этом продукте распространяются БЕЗ ПРЕДОСТАВЛЕНИЯ КАКИХ-ЛИБО ГАРАНТИЙ, и является предметом авторских прав одного или нескольких авторов. Для получения подробной информации смотрите пункты GPL Code и LGPL Code для этого продукта и условий лицензий GPL и LGPL.

Глоссарий

точка доступа Устройство, обеспечивающее подключение WLAN к беспроводным клиентам (станций).

адаптер Устройство или плата, которая подключает компьютер, принтер или другое периферийное устройство к сети или какому-то другому устройству. Беспроводной адаптер подключает компьютер к беспроводной локальной сети WLAN.

ASCII Американский стандартный код для обмена информацией относится к алфавитно-цифровым данным для обработки и совместимости связи между различными устройствами; как правило, используется для асинхронной передачи.

проверка подлинности Процесс, при котором CMTS проверяет разрешение доступа, используя пароль, защищенный IP-адрес или серийный номер.

авторизация Часть процесса, выполняемого между CMTS и кабельным модемом или шлюзом, для обеспечения «базовой приватности» (Baseline Privacy).

полоса пропускания Пропускная способность среды с точки зрения диапазона частот. Большая полоса пропускания обеспечивает возможность передачи большего количества данных в течение заданного периода времени.

мост Сетевое устройство OSI layer 2, которое соединяет две локальные сети с использованием аналогичных протоколов. Оно фильтрует блоки данных на основе MAC-адреса с целью уменьшения объема трафика. Мост может быть помещен между двумя группами хостов, которые обмениваются большим объемом данных, но гораздо меньшим объемом данных с хостами в другой группе. Мост анализирует пункты назначения каждого пакета, чтобы определить, следует ли передавать его на другую сторону.

многоканальная передача Одновременная передача данных нескольким сетевым устройствам; механизм протокола поддерживает групповую и универсальную адресацию.

кабельный модем Устройство, устанавливаемое на месте абонента, для обеспечения передачи данных по сети HFC. Если не указано иное, любое упоминание фразы «кабельный модем» в этой документации относятся только к кабельным модемам DOCSIS или Euro-DOCSIS.

клиент В клиентской/серверной архитектуре клиентом является компьютер, который посылает запросы на получение файлов или услуг, таких как передача файлов, удаленный вход в систему или осуществление печати с сервера. Также известен как CPE. В сети WLAN клиентом является любой хост, который может подключаться к точке доступа. Беспроводной клиент также известен как «станция».

CMTS Система окончания кабельного модема представляет собой устройство в головном узле кабельной системы, который сопрягает сеть HFC с локальными или удаленными IP-сетями для подключения IP-хостов, кабельных модемов или шлюзов, а также абонентов. Оно управляет всей пропускной способностью кабельного модема. Оно также называется граничным маршрутизатором.

коаксиальный кабель Тип кабеля, состоящего из центрального провода, обернутого в изоляцию и заземленного экрана оплетенного (коаксиального) провода. Этот экран минимизирует воздействие электрических и радиочастотных помех. Коаксиальный кабель имеет высокую пропускную способность и может поддерживать передачу данных на большие расстояния.

CPE Абонентское оборудование, как правило, компьютеры, принтеры и т.д., подключенные к кабельному модему или шлюзу на месте абонента. CPE может быть предоставлено абоненту или поставщику Интернет-услуг. Также называется клиентом.

DHCP Протокол динамической конфигурации хост-сервера (DHCP) динамически назначает IP-адреса хост-клиентам в IP-сети. DHCP исключает необходимость назначать вручную статические IP-адреса, «предоставляя во временное пользование» каждому клиенту IP-адреса и маски подсети. Он обеспечивает автоматизированное многократное применение неиспользованных IP-адресов. DHCP-сервер в головном узле кабельной системы назначает общий IP-адрес резидентному шлюзу и, выборочно, клиентам в локальной сети резидентного шлюза. Резидентный шлюз содержит встроенный DHCP-сервер, который назначает частные IP-адреса клиентам.

DMZ «Демилитаризованная зона» представляет собой один или более хост-компьютеров, логически расположенных между частной локальной сетью и Интернетом. DMZ запрещает внешним пользователям прямой доступ к личным данным. (Этот термин походит от названия географических буферных зон, расположенных между какими-либо конфликтующими странами, например, Северной и Южной Кореей). В стандартной небольшой DMZ-конфигурации DMZ-хост получает запросы от частных пользователей локальной сети для доступа ко внешним веб-сайтам и инициирует сессии для этих запросов. DMZ-хост не может инициировать сессию обратно в частной локальной сети. Интернет-пользователи, находящиеся за пределами частной сети могут получать доступ только к DMZ-хосту. Вы можете использовать DMZ для настройки веб-сервера или для игр, сохраняя конфиденциальность данных.

DNS Система доменных имен является Интернет-системой для преобразования доменных имен в IP-адреса. DNS-сервер содержит соответствующие таблице доменные имена, такие как Internetname.com, IP-адреса, такие как 192.169.9.1. При получении доступа к всемирной сети DNS-сервер преобразовывает отображаемый в браузере URL в IP-адрес веб-сайта назначения. Справочная таблица DNS является распределенной базой данных в Интернете; нет один DNS-сервер не хранит все доменные имена по совпадающим IP-адресам.

DOCSIS Стандарт передачи данных по коаксиальному кабелю (Data-Over-Cable Service Interface Specification) определяет стандарты интерфейса для кабельных модемов, шлюзов и вспомогательного оборудования для передачи данных между сетью HFC и компьютерными системами или телевизорами. Чтобы подчеркнуть его использование в качестве стандарта для кабельного модема, DOCSIS теперь называется «Сертифицированные кабельные модемы CableLabs» (CableLabs Certified Cable Modems). Euro-DOCSIS является DOCSIS-стандартом, адаптированным для использования в Европе.

нисходящее направление В кабельной сети передачи данных это – направление данных, получаемых компьютером из Интернета.

динамический IP-адрес IP-адрес, что временно предоставляется в пользование хосту DHCP-сервером. Является полной противоположностью статического IP-адреса.

шифровать Кодировать данные.

конечная точка Конечная точка VPN удаляет VPN в маршрутизаторе, чтобы компьютерам в локальной сети резидентного шлюза не нужно было использовать программное обеспечение VPN-клиента для туннелирования данных через Интернет в VPN-сервер.

Ethernet Это наиболее широко используемый тип локальной сети, также известный как IEEE 802.3. Наиболее распространенными Ethernet-сетями являются сети 10Base-T, которые обеспечивают скорость передачи данных до 10 Мбит, как правило, через неэкранированный кабель

с витой парой, оконеченный разъемами RJ-45. Fast Ethernet (100Base-T) обеспечивает скорость до 100 Мбит «Base» означает «технология основной полосы частот», а «T» означает ««кабель с витой парой». Каждый Ethernet-порт имеет физический адрес, который называется MAC-адресом.

Euro-DOCSIS Стандарт ComLabs, который является аналогом DOCSIS, адаптированным для использования в Европе.

событие Сообщение, генерируемое устройством для информирования оператора или системы сетевого управления о происшествии какого-либо события.

брандмауэр Программное обеспечение системы безопасности в резидентном шлюзе, которое определяет политику управления доступом между Интернетом и локальной сетью резидентного шлюза.

блок данных Набор данных, передаваемых между узлами сети, которые содержат данные по адресации и управлению протоколами. Некоторые блоки данных управления не содержат данных.

частота Количество повторений идентичного цикла электромагнитным сигналом в единицу времени, как правило, за одну секунду, измеряется в Гц, кГц, МГц или ГГц.

шлюз Устройство, которое обеспечивает связь между сетями, используя различные протоколы. См. также маршрутизатор.

шестнадцатеричный код исчисления Шестнадцатеричная система исчисления, которая использует шестнадцать последовательных числа (от 0 до 9, а также буквы от A до F) в качестве основных единиц, перед добавлением новой позиции. На компьютерах шестнадцатеричная система исчисления является удобным способом представления двоичных чисел.

хост В IP хостом является любой компьютер, поддерживающий приложения и услуги для конечных пользователей, предоставляемый полной двухсторонний сетевой доступ. Каждый хост имеет уникальный номер, который в сочетании с сетевым

номером образует его IP-адрес.

Под словом «Хост» также может подразумеваться:

- Компьютер, управляющий веб-сервером, который хранит страницы для одного или нескольких веб-сайтов, принадлежащих организации (ям) или физическим лицам,
- Компания, которая предоставляет эту услугу,
- В IBM-среде, главная ЭВМ в сети HFC, центр, который является уменьшенным головным узлом, выполняющим некоторые или все функции головного узла для части системы.

Гц Герц – один цикл в секунду. Единица измерения частоты, за которую выполняется переменный цикл электромагнитного сигнала в диапазоне высших и низших состояний. Используется для определения полос электромагнитного спектра, используемых в передаче голосовых сообщений и данных, или для определения пропускной способности среды передачи данных.

ICMP Протокол управления сообщениями в сети Интернет (Internet Control Message Protocol) – это протокол, используемый для создания сообщений об ошибках, неисправностях и информационных сообщений, передаваемых между IP-хостами и шлюзами. ICMP-сообщения обрабатываются с помощью программного обеспечения IP и, как правило, не отображаются для конечного пользователя.

IEEE Институт инженеров по электротехнике и электронике (The Institute of Electrical and Electronics Engineers, Inc.) (http://www.ieee.org) является организацией, которая разрабатывает стандарты, технические документы и симпозиумы для электрических и электронных отраслей промышленности и аккредитуется ANSI.

IEEE 802.11b Стандарты беспроводной сети

IEEE 802.11g

IEEE 802.3 См. Ethernet.

IP Интернет-протокол (Internet Protocol) представляет собой набор стандартов, которые позволяют различным типам компьютеров связываться друг с другом и обмениваться данными через Интернет. IP-обеспечивает создание единой целостной системы связи и превращает Интернет в виртуальную сеть.

IP-адрес Уникальное 32-разрядное значение, которое идентифицирует каждый хост в TCP-/IP-сети. TCP-/IP-сети маршрутизируют сообщения на основании пункта назначения IP-адреса.

IP-адрес состоит из двух частей:

- Сетевого адреса, присваиваемого IANA
- Сетевой администратор резидентного шлюза присваивает хост-адрес каждому хосту, подключенному к резидентному шлюзу, автоматически используя его DHCP-сервер в качестве статического IP-адреса. В сети класса C первые 24 бита являются сетевым адресом и последние 8 бит – хост-адресом; в точечно-десятичном формате IP-адрес отображается как «network.network.network.host.» При включении DHCP-клиента резидентного шлюза на основной DHCP-странице интернет-провайдер автоматически назначает сетевой адрес, маску подсети, имя домена, а также DNS-сервер для обеспечения непрерывного подключения к Интернету.

IPSec Протоколами безопасности интернет-протокола (Internet Protocol Security) являются IETF-стандарты проверки подлинности и шифрования для безопасного обмена пакетами через Интернет. IPSec работает на программной платформе OSI layer 3 и обеспечивает общую защиту в сети.

IKE Протокол обмена ключами.

ISP Интернет-провайдер.

LAN Локальная сеть обеспечивает постоянное, широкополосное соединение на ограниченной территории, например, в здании или кампусе. Ethernet является наиболее широко используемым стандартом локальной сети.

MAC-адрес Адрес управления доступом к медиаданным является уникальным 48-битным значением, постоянно сохраняющимся в ПЗУ заводской системы для идентификации каждого сетевого Ethernet-устройства.

МГц Мегагерц– один миллион циклов в секунду. Единица измерения радиочастоты

Многоадресная передача Передача данных от одного отправителя нескольким получателям.

NAT Преобразование сетевых адресов (Network Address Translation) – это Интернет-стандарт локальной сети, использующий один набор IP-адресов для внутреннего трафика и второй набор IP-адресов для внешнего трафика.

сеть Два или более компьютеров, подключенных друг к другу для обмена данными. Как правило, подключение сетей осуществляется с использованием различных кабелей.

NIC Плата сетевого интерфейса (network interface card) преобразовывает компьютерные данные в последовательные данные в пакетном формате, отправляемом по локальной сети. NIC устанавливается в слот расширения или может быть встроена. Каждая Ethernet NIC имеет MAC-адрес, постоянно сохраняющейся в ПЗУ.

пакет Блок данных, который направляется между отправителем и пунктом назначения по Интернету или по другой сети с пакетной коммутацией. При отправке данных, таких как сообщения электронной почты, через Интернет, IP-отправителя распределяет данные в однозначно-пронумерованные пакеты. Заголовок пакета содержит IP-адреса отправителя и пункта назначения. Отдельные пакеты могут передаваться по разным маршрутам. Когда все пакеты прибывают в пункт назначения, IP конечного получателя собирает пакеты.

клиент-получатель передаваемых данных Клиент-получатель передаваемых данных (pass-through) в локальной сети резидентного шлюза получает свой внешний IP-адрес от DHCP-сервера интернет-провайдера.

ПАКЕТ ПРОВЕРКИ СВЯЗИ (PING) Сетевая программная утилита, которая проверяет достижимость хоста, отправляя небольшой пакет хосту и ожидая ответа. При отправке такого пакета на IP-адрес компьютера и получении ответ, вы определите доступность этого компьютера в сети. Этот утилиту также называют Packet Internet Groper (отправитель интернет-пакетов).

порт На компьютере или другом электронном устройстве порт является разъемом или вилкой, используемыми для его физического подключения к сети или к другим устройствам. В TCP-/IP-сети порт представляет собой число от 0 до 65536, логически используемое клиентской программой для указания программы сервера. Порты 0 до 1024 являются зарезервированными.

срабатывание портов Механизм, который обеспечивает входящее соединение с указанными приложениями. В основном используется для игровых приложений.

PPTP Протокол туннелирования точка-точка (Point-to-Point Tunneling Protocol) формирует другие протоколы. Это новая технология создания VPN, совместно разработанная несколькими поставщиками услуг.

протокол Формальный набор правил и соглашений для обмена данными. Компьютеры различных типов (например, ПК, UNIX или большая ЭВМ) могут обмениваться данными, если они поддерживают общие протоколы.

подготовка Процесс автоматического открытия или ручной настройки кабельного модема в системе CMTS.

QoS Качество обслуживания (Quality of service) описывает приоритет, задержку, пропускную способность и полосу пропускания соединения.

RF Радио частота – сигналы, используемые в передатчике и приемнике CMTS для передачи данных по HFC-сети. Канал передачи информации модулируется с целью кодирования цифрового потока данных для передачи по кабельной сети.

маршрутизатор В IP-сетях это – устройство, подключающееся, как минимум, к двум сетям, которые могут быть аналогичными или отличающимися. Как правило, маршрутизатор расположен в шлюзе между сетями. Маршрутизатор работает на сетевом уровне OSI 3. Он фильтрует пакеты, исходя из IP-адреса, проверяя IP-адрес источника и пункта назначения, чтобы определить оптимальный маршрут, по которому будут направляться пакеты. Маршрутизатор часто входит в комплект в качестве части сетевого коммутатора. Маршрутизатор также может быть установлен в виде программного обеспечения на компьютере.

таблица маршрутизации Таблица с перечнем доступных маршрутов, которые используются маршрутизатором с целью определения наилучшего маршрута для передачи пакета.

RTS запрос на отправку данных сервера. В архитектуре клиента/сервера это– специализированный компьютер, который предоставляет файлы или службы, такие как передача файлов, удаленный вход в систему или печать в клиенты.

Поставщик услуг Компания, предоставляющая данные или телефонные услуги абонентам

SMTP Простой протокол электронной почты (Simple Mail Transfer Protocol) является стандартным интернет-протоколом для передачи сообщений электронной почты.

распределитель Устройство, которое распределяет сигнал из входного кабеля между двумя или более кабелями.

SSID Идентификатор набора служб (Service Set Identifier) или имя сети – это уникальный идентификатор, который используют беспроводные клиенты для связи с точкой доступа с целью различения нескольких беспроводных сетей в одной и той же зоне. Все клиенты в беспроводной локальной сети должны иметь одинаковый SSID в качестве точки доступа.

статический IP-адрес IP-адрес, который присваивается хост-компьютеру на постоянной основе. Как правило, статический IP-адрес назначается вручную. Он является полной противоположностью динамического IP-адреса.

станция Термин стандарта IEEE 802.11b для обозначения беспроводного клиента

абонент Домашний или офисный пользователь, которому интернет-провайдер предоставляет доступ к телевизионным, информационным или другим услугам.

маска подсети Битовая маска, к которой применяется операция поразрядной конъюнкции (логическое И), зная IP-адреса пакета, для определения сетевого адреса. Маршрутизатор направляет пакеты, используя сетевой адрес.

SYSLOG Фактически, это UNIX-стандарт для записи системных событий.

TCP Протокол управления передачей (Transmission Control Protocol) на 4 транспортном уровне OSI обеспечивает надежную передачу данных по сети с использованием IP (3 сетевого уровня). Это протокол межконцевого обмена, определяющий правила и процедуры для обмена данными между хостами по IP без организации соединения. TCP использует таймер для отслеживания необработанных пакетов, проверяет ошибки во входящих пакетах и повторно передает пакеты, если это необходимо.

TCP/IP Набор TCP/IP-протоколов. Он устанавливает стандарты и правила для передачи данных между сетями в Интернете. Это всемирный межсетевой стандарт и основной протокол интернет-связи.

TFTP Упрощенный протокол передачи файлов (Trivial File Transfer Protocol) – это простейший протокол, используемый для передачи файлов.

TKIP Протокол ограниченной во времени целостности ключа (Temporal Key Integrity Protocol)

туннель Размещает пакеты внутри других пакетов для их отправки по сети. Протокол вложенного пакета анализируется каждой конечной точкой или туннельным интерфейсом, через который пакет входит и выходит из сети. Работа VPN-сетей основывается на туннелировании для создания безопасной сети.

Для выполнения туннелирования требуются следующие типы протоколов:

- Протокол канала передачи информации, такой как TCP, используемый сетью, по которой передаются данные
- Протокол инкапсуляции, такой как IPSec, L2TP L2F, или PPTP, который охватывает исходные данные
- Пассажирский протокол, такой как IP, для одноадресной передачи

исходных данных Передача данных позиционирования, отправляемых от одного отправителя к одному получателю. Это стандартный способ получения доступа к веб-сайтам.

восходящее направление В кабельной сети передачи данных восходящим направлением является направление данных, отправляемых компьютером абонента через кабельный модем в систему CMTS и сеть Интернет.

VoIP Голосовая связь по интернет-протоколу (Voice over Internet Protocol) – это способ обмена голосовыми сообщениями, факсовыми сообщениями и другой информацией через Интернет. Передача голосовых и факсовых сообщений традиционно осуществлялась по телефонным линиям PSTN (телефонной сети общего пользования) с использованием специализированного канала для каждой линии. VoIP обеспечивает передачу звонков в виде пакетов дискретных данных по общим линиям. VoIP является важной частью конвергенции компьютеров, телефонов и телевидения в единую интегрированную информационную сеть.

VPN Виртуальная частная сеть (virtual private network) представляет собой частную сеть, которая использует «виртуальные» соединения (туннели), направляемые по общественным сетям (как правило, через Интернет) для обеспечения безопасной и быстрой связи, как правило, для пользователей,

работающих удаленно дома или в небольших офисах-филиалах. VPN-подключение обеспечивает безопасность и производительность, аналогичную производительности специализированной линии связи (например, выделенной линии), но при значительно более низкой стоимости.

WAN Сеть широкого охвата обеспечивает соединение в пределах большой географической области, например, страны или всего мира. Полоса пропускания данной сети зависит от потребностей и стоимости, но, как правило, является значительно меньшей, чем полоса локальной сети.

WEP Метод шифрования конфиденциальности на уровне проводных сетей (Wired Equivalent Privacy) обеспечивает защиту конфиденциальности данных, передаваемых по беспроводной сети. WEP использует ключи для шифрования и дешифрования передаваемых данных. Точка доступа должна аутентифицировать клиента, прежде чем она будет передавать данные другому клиенту. WEP является частью стандарта IEEE 802.11b. Поскольку WEP трудно использовать и он не обеспечивает сверх надежное шифрование.

WiFi Беспроводная достоверность (Wireless fidelity) (произносится как «вай-фай») – торговая марка, применяемая к продуктам, поддерживающим IEEE 802.11b.

WLAN Беспроводная локальная сеть

WPA Защищенный доступ WiFi (Wi-Fi Protected Access или WPA) – это метод шифрования, описанный на веб-станице объединения крупнейших производителей беспроводных устройств Wi-Fi: http://www. wifialliance.org. Он является гораздо более надежным видом шифрования, нежели WEP.