

NETSHe BR104 Configuration guide RU

[Original file](#)

цветной прямоугольник с графическим текстомРуководство



Маршрутизатор BR104
Руководство по настройке
Версия 3.0 февраль, 2020

Оглавление

Введение

Маршрутизатор BR104 с возможностью передачи данных через сотовые сети связи относится к типу полноценных маршрутизаторов с широким набором функций. Данное руководство охватывает только часть из них, а именно: некоторые аспекты сетевых протоколов, маршрутизацию и связности сетей на разных уровнях, включая беспроводные сети и сети операторов подвижной связи, и то, как эти функции реализованы во встроенном программном обеспечении (firmware) маршрутизатора.

Примеры, рассматриваемые по ходу документа, относятся к типовым случаям применения маршрутизаторов. Однако, если необходимо реализовать сложную или нетипичную схему с применением маршрутизаторов BR104, мы просим обращаться в службу поддержки ООО «Нетше лаб» на сайте <http://www.netshe-lab.ru>

Внимание!

*** Этот документ охватывает так же совместимые модели оборудования: BR104, BR104-IoT, AP145, AP147-2, MiROUTER. При чем этот список постоянно увеличивается за счет новых моделей. Также изложенное в этом руководстве относится к использованию операционной системы NETSHe версий 5.2 и 5.3. ***

Внимание!

*** IPsec описывается в отдельном руководстве 'BR104 IPsec Configuration and Troubleshooting guide'. ***

Доступ к устройству

При первом включении маршрутизатора пользователь может получить доступ к управлению маршрутизатором со следующими именами и паролями:

IP-адрес по умолчанию 192.168.1.1

URL веб-интерфейса <http://192.168.1.1>
<http://192.168.1.1:5556> (для NMMS совместимых версий)

Умалчиваемое имя superuser / abC123dEf_ (административные права)

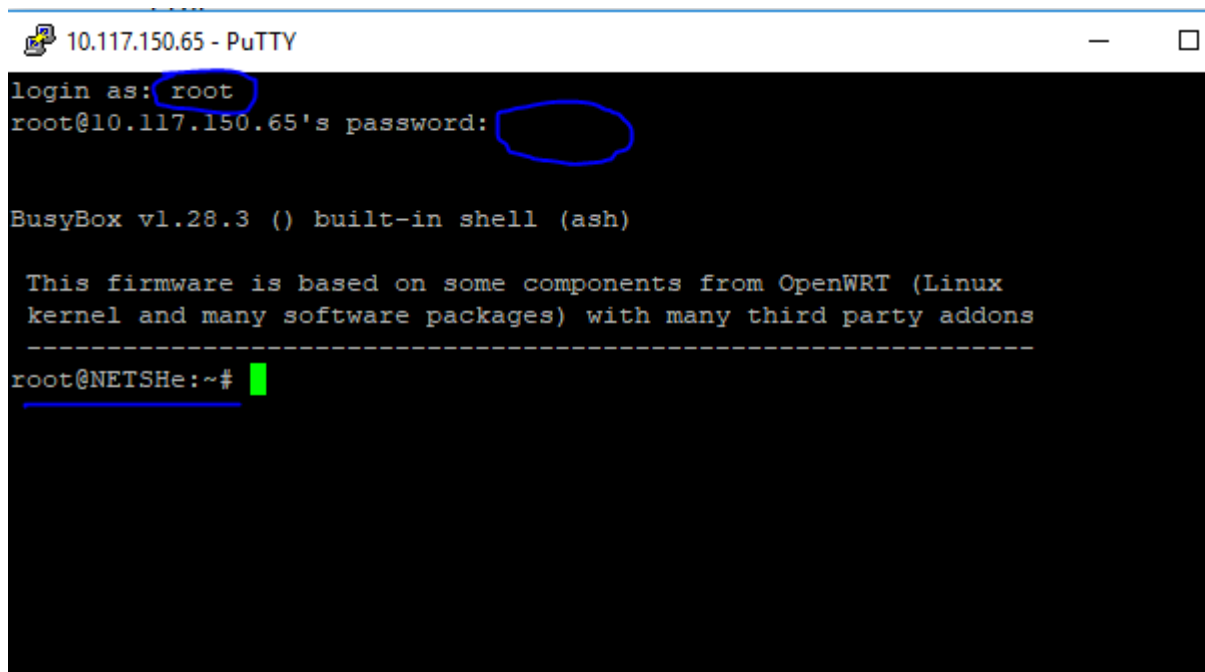
Пользователя и пароль root / root (системная учетная запись)

Большинство современных браузеров Firefox, Chrome, IE11 и т.д. поддерживают веб-доступ к управлению маршрутизатором.

Доступ из командной строки

CLI (доступ из командной строки) требуется для редко употребляемых команд, используется при решении проблем и получения информации о состоянии компонентов системы.

1. По умолчанию используется протокол SSH (TCP порт 22) для доступа к интерфейсу командной строки.
2. Telnet по умолчанию отключен. Пользователь может его включить, эта процедура будет описана в соответствующем пункте данного руководства.
3. Можно использовать стандартные приложения типа Putty или Secure SSH.
4. Доступ из командной строки требует аутентификации с системной учетной записью и паролем по умолчанию root / root.



```
10.117.150.65 - PuTTY
login as: root
root@10.117.150.65's password:
BusyBox v1.28.3 () built-in shell (ash)

This firmware is based on some components from OpenWRT (Linux
kernel and many software packages) with many third party addons
-----
root@NETSHe:~#
```

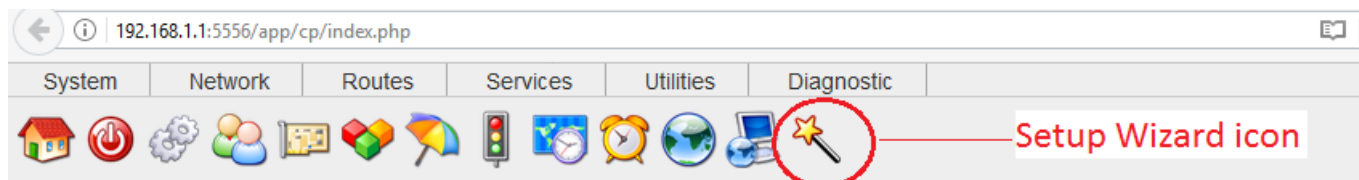
Мастер установки

Внимание!

*** Мастер установки помогает настроить WAN, LAN и прочие интерфейсы. Пользователь может настроить единственный WAN порт или два WAN (основной и резервный) по отказоустойчивому сценарию. Шаги мастера могут создаваться под конкретный проект и содержать настройки для разных компонентов. Мастер может автоматизировать настройки PPPoE, L2TP, PPTP, Cellular и Ethernet в качестве подключения первичного WAN и Cellular в качестве резервного WAN. Те же самые настройки можно произвести, отказавшись от мастера, и выполнить их вручную с помощью веб-интерфейса. Такой способ настройки требует больше внимания пользователя на разные детали, которые будут описаны по ходу этого документа. ***

При первоначальной загрузке маршрутизатора пользователю будет предложено пройти мастер настройки. Пользователь должен нажать 'Yes' и проследовать следующими шагами.

Если пользователь случайно пропустил предложение мастера, то он может вызвать мастер, нажав иконку с волшебной палочкой на панели инструментов.



Click on above icon to
start setup wizard

Attention!



The setup wizard will guide you through the initial (and minimal) configuration of device. Remember, that you should close browser window when process will done and reopen browser to start new session. Start the wizard?

Yes

No

Далее следует выбрать шаблон из выпадающего списка и нажать кнопку 'Next'.

Configuration template

Please, choose configuration template. This template will be used later

=> Default configuration template

Next

Конфигурация с единственным WAN интерфейсом

Шаг 1. Выберите 'CELLULAR CONNECTION' для настроек IPv4 соединения через сим-карту.

Welcome to simplest way to configure your device!

All changes will be applied when master will be completed

First step

Please choose type of your primary connection to Internet.

CELLULAR CONNECTION

WIRE CONNECTION WITH DHCPV4

WIRE CONNECTION WITH STATIC IPV4

WIRE CONNECTION WITH DHCPV6

WIRE CONNECTION WITH STATIC IPV6

PPPOE CONNECTION

WEBUI EXPERT MODE

Шаг 2. Введите настройки APN, как того требует ваш оператор сотовой связи, и нажмите 'NEXT'.

Please configure your connection.

Username:	
Password:	
Access point (APN): *	airtelgprs.com
PIN code:	
Authentication type:	auto
Use any possible cellular network or specified only:	auto
Switch device in IP passthrough mode?:	☐
I want to configure second connection (May be useful for VPN applications):	☐
Enable IP v6 over PPP link ?:	☐
IMEI:	869601014263557
Device information:	BroadMobi BM806U-E1 (M1.2.8_E1.0.5_A1.2.1)
RSSI:	-73dBm

* Filling of highlighted fields is mandatory!

NEXT ▶

BACK TO WIZARD START ▶

WEBUI EXPERT MODE ▶

Если IPv6 доступно для настройки в сети оператора, то выберите опцию 'Enable IPv6 over PPP link'.

Please configure your connection.

Username:	
Password:	
Access point (APN): *	airtelgprs.com
PIN code:	
Authentication type:	auto
Use any possible cellular network or specified only:	auto
Switch device in IP passthrough mode?:	☐
I want to configure second connection (May be useful for VPN applications):	☐
Enable IP v6 over PPP link ?:	☒
IMEI:	869715039423895
Device information:	MeiG SLM750-T (SLM750-T_2.0.4_EQ102)
RSSI:	-125dBm

* Filling of highlighted fields is mandatory!

NEXT ▶

BACK TO WIZARD START ▶

WEBUI EXPERT MODE ▶

Конфигурация с двумя подключениями WAN

Шаг 1. Выберите 'PPPOE CONNECTION'.

First step

Please choose type of your primary connection to Internet.

- CELLULAR CONNECTION ▶
- WIRE CONNECTION WITH DHCPV4 ▶
- WIRE CONNECTION WITH STATIC IPV4 ▶
- WIRE CONNECTION WITH DHCPV6 ▶
- WIRE CONNECTION WITH STATIC IPV6 ▶
- PPPOE CONNECTION ▶**

WEBUI EXPERT MODE ▶

Шаг 2. Пользователю следует заполнить параметры PPPoE в соответствии с требованиями провайдера. MAC-адрес является опциональным параметром и может учитываться, если пользователю уже сопоставлен какой-то MAC-адрес в сети провайдера, и он желает возобновить это соединение на новом маршрутизаторе.

First step

PPPoE connection

Please configure your connection.

Username: *	sushim
Password: *	
PPTP/L2TP Server/PPPOE Service Name:	joisterbb
Enable IP v6 over PPP link ?:	☐
MAC:	24:b6:fd:1c:e9:af MAC address required only in case of cloning for existing registered MAC with ISP.

* Filling of highlighted fields is mandatory!

NEXT ▶

BACK TO WIZARD START ▶

WEBUI EXPERT MODE ▶

Шаг 2.a. Щелкните на 'CONFIGURE BACKUP'.

First step

Backup primary WAN connection

May be you wish to configure cellular connection to backup primary Internet connection?

CONFIGURE BACKUP ▶

NEXT ▶

BACK TO WIZARD START ▶

WEBUI EXPERT MODE ▶

Шаг 2.b. Введите параметры APN и нажмите 'NEXT'.

Please configure your connection.

Username:	
Password:	
Access point (APN):*	airtelgprs.com
PIN code:	
Authentication type:	auto
Use any possible cellular network or specified only:	auto
Switch device in IP passthrough mode?:	☐
I want to configure second connection (May be useful for VPN applications):	☐
Enable IP v6 over PPP link ?:	☐
IMEI:	869601014263557
Device information:	BroadMobi BM806U-E1 (M1.2.8_E1.0.5_A1.2.1)
RSSI:	-73dBm

* Filling of highlighted fields is mandatory!

NEXT ▶

[BACK TO WIZARD START](#) ▶

[WEBUI EXPERT MODE](#) ▶

Шаг 3. На следующем шаге щелкните 'NEXT', ничего не меняя.

First step

WAN link state checking

You can configure method how to check WAN link state

Enable ping to public DNS servers as checking method : ☐

Or specify IP-address to ping (especially if device works in private network):

NEXT ▶

[BACK TO WIZARD START](#) ▶

[WEBUI EXPERT MODE](#) ▶

Шаг 4. Выберите 'NO', если нет необходимости менять настройки DNS, получаемые от провайдера.

First step

Nameserver's settings

Do you wish to specify own nameservers?

YES ▶

NO ▶

[BACK TO WIZARD START](#) ▶

[WEBUI EXPERT MODE](#) ▶

ИЛИ Шаг 4. Выберите 'YES' для того, чтобы задать настройки DNS вручную.

Внимание!

*** Задание параметров DNS обязательно в случае использования двух WAN интерфейсов, основного и резервного, на предыдущих шагах. В противном случае WAN интерфейс окажется поднятым, но пользователи не смогут получить доступ в Интернет из своих браузеров. Потому что при двух WAN соединениях системный DNS демон не сможет работать с двойными настройками, полученными от двух источников. Поэтому важно настроить DNS глобально на устройстве. ***

First step

Nameserver's settings

Please specify here Nameservers to use.

IP-Address of nameserver (clear up input box to remove row from settings): *

8.8.8.8

IP-Address of nameserver (clear up input box to remove row from settings):

59.21.6.92

* Filling of highlighted fields is mandatory!

NEXT ▶

BACK TO WIZARD START ▶

WEBUI EXPERT MODE ▶

Шаг 5. Введите широковещательное имя для беспроводного доступа (SSID) и пароль для аутентификации пользователей Wi-Fi, затем щелкните 'NEXT'.

Внимание!

*** Если пользователь желает отключить Wi-Fi в любом из диапазонов 5ГГц/2.4ГГц, то ему необходимо отметить данную опцию сверху страницы интерфейса 'wlan0'/'wlan1' соответственно. ***

First step

Wireless configuration

Please configure wireless parameters.

Tick checkbox to disable default wireless interface:

☐

Mode: *

Access Point / Mesh gateway ▼

Current frequency:

auto

ESSID: *

Airtel_CPE

Hide ESSID ?:

☐

Encryption:

WPA2 (Personal) ▼

Password, Encryption key or network passphrase:

MiAP101_1234

* Filling of highlighted fields is mandatory!

NEXT ▶

BACK TO WIZARD START ▶

WEBUI EXPERT MODE ▶

Шаг 6. Настройте адрес и подсеть для LAN интерфейса, по завершению щелкните 'NEXT'. Для того, чтоб отключить LAN DHCP-сервер, уберите галочку, показанную на следующей картинке.

Внимание!

*** В этом случае все пользователи должны настраивать адреса своих устройств**

вручную, задавая адреса из той же подсети, что и LAN интерфейс маршрутизатора. Либо в данной подсети должен быть другой рабочий DHCP-сервер. *

First step

IPv4 LAN

Please configure LAN address and using of DHCP. Please, keep in mind that widely used addresses such as 192.168.1.1 may cause issues in some configurations. Strongly recommend to change the address for another

IPv4 Address: *	192.168.2.1
IPv4 Netmask: *	255.255.255.0
Tick to enable DHCP Server :	☒
IP pool start and end addresses	192.168.2.30
	192.168.2.245

* Filling of highlighted fields is mandatory!

NEXT ▶

[BACK TO WIZARD START](#) ▶

[WEBUI EXPERT MODE](#) ▶

или Шаг 6.1. Если пользователь выбрал IPv6 на Шаг 2.1 выше, то следующий шаг появится для ввода адреса LAN IPv6 и DHCPv6 сервера.

First step

IPv6 LAN

Please configure LAN address and using of DHCP. Please, keep in mind that widely used addresses such as 192.168.1.1 may cause issues in some configurations. Strongly recommend to change the address for another

IPv6 Address: *	fd00::1	IP v6 Address for CPE LAN interface.
IPv6 Netmask: *	64	
Tick to enable DHCP Server :	☒ Enable DHCP by tiking check box.	IP v6 DHCP LAN Start and END ip range for LAN client.
IP pool start and end addresses	fd00::100	
	fd00::200	

* Filling of highlighted fields is mandatory!

NEXT ▶

[BACK TO WIZARD START](#) ▶

[WEBUI EXPERT MODE](#) ▶

Шаг 7. Щелкните 'Next' на предложение настроить DM VPN Spoke, чтоб пропустить эти настройки.

First step

Precision setup

May be you want to setup DMVPN Spoke now?

[YES. I WANT TO SETUP DMVPN SPOKE ▶](#)

[NEXT ▶](#)

[BACK TO WIZARD START ▶](#)

[WEBUI EXPERT MODE ▶](#)

Шаг 8. На этом шаге, если пользователь хочет настроить IPsec туннель, ему следует выбрать 'Yes, I want to ...'. В противном случае пользователь должен щелкнуть на 'Next', чтобы пропустить IPsec.

First step

Precision setup

May be you want to setup IPSEC connection now?

[YES. I WANT TO SETUP IPSEC CONNECTION ▶](#)

[NEXT ▶](#)

[BACK TO WIZARD START ▶](#)

[WEBUI EXPERT MODE ▶](#)

Если пользователь выбирает 'Yes, I Want to.....', следующий диалог будет показан. Параметры должны соответствовать другой стороне туннеля.

Внимание!

*** Пользователь должен проверить параметры IPsec средствами WebUI позднее, потому что параметры политики (интерфейса) гораздо шире, чем их предлагает мастер первоначальной настройки.** * Пользователь может найти подробную информацию про IPsec в руководстве 'BR104 IPsec Configuration and Troubleshooting guide'.

*

IPSEC connection

Please configure your connection.

Address of remote physical interface / address or hostname to establish tunnel: *	14.143.59.101
Local network to route through tunnel:	10.117.150.64/29, 10.117.150.80/32
Remote network to route through tunnel:	10.124.104.0/26, 10.118.74.232/29
Alias/DNS name for local node:	
Enable rekeying (non-zero value in seconds)? :	86400
Enable reauth (non-zero value in seconds)? :	28800
Enable aggressive mode :	☐
IKE version for tunnel:	ikev1
Cipher suite for phase1:	aes256-sha1-modp1536
Cipher suite for phase2:	aes256-sha1-modp1024
Preshared key (passphrase) for IPSEC or GRE tunnel: *	Tata@123

Fill correct parameters to match with peer.

* Filling of highlighted fields is mandatory!

NEXT ▶

[BACK TO WIZARD START](#) ▶

[WEBUI EXPERT MODE](#) ▶

Шаг 9. Пользователь может изменить имя маршрутизатора с умалчиваемого 'NETSHe' на что-нибудь ему удобное. Также пользователь может установить пароли для учетных записей 'root' и 'superuser', не забывая про требование сложности.

First step

Change password for user (root)

Device name. Please do not keep it default: *	NETSHe_1145295079
Password: *	root
Confirm password: *	root

Fill in 'Root' user password

Please change password for user (superuser) below

Password: *	admin@123
Confirm password: *	admin@123

Fill in Superuser password

* Filling of highlighted fields is mandatory!

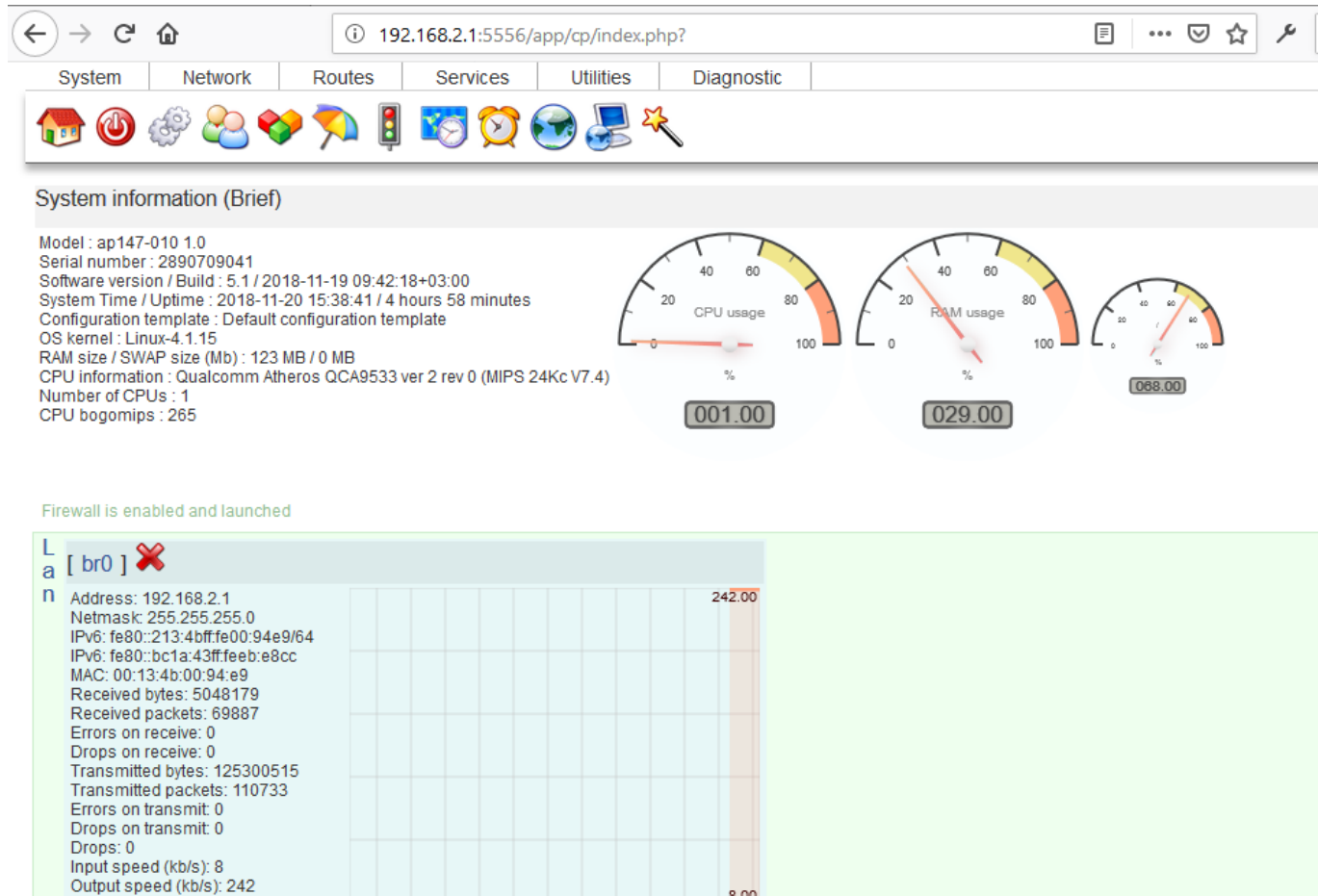
FINISH WIZARD, APPLY ALL CHANGES AND REBOOT THE DEVICE ▶

[BACK TO WIZARD START](#) ▶

[WEBUI EXPERT MODE](#) ▶

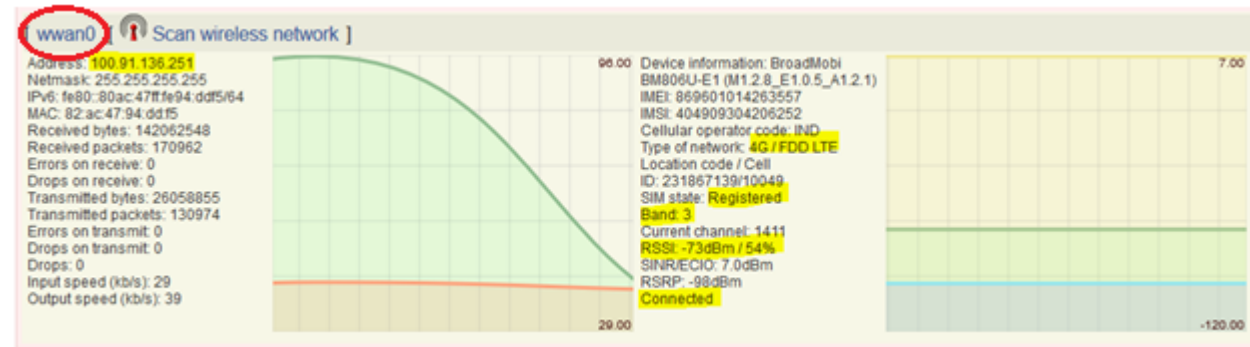
Полная перезагрузка маршрутизатора займет около двух с половиной минут. Пользователь должен подождать, пока страница автоматически перейдет на домашнюю страницу веб-интерфейса (WebUI). * Если автоматического перенаправления нет или страница не обновляется, следует проверить IP-адрес маршрутизатора и попробовать порт 5556 TCP.

*** ===== Домашняя страница ===== После успешной перезагрузки устройства, пользователь может подключиться к WebUI, используя логин и пароль, введенные во время мастера настройки. После успешной аутентификации откроется домашняя страница, которая содержит: - Информацию о системе и время с последнего включения, - Счетчики потребления памяти, процессора, дисков, - Все настроенные и недонастроенные интерфейсы.**

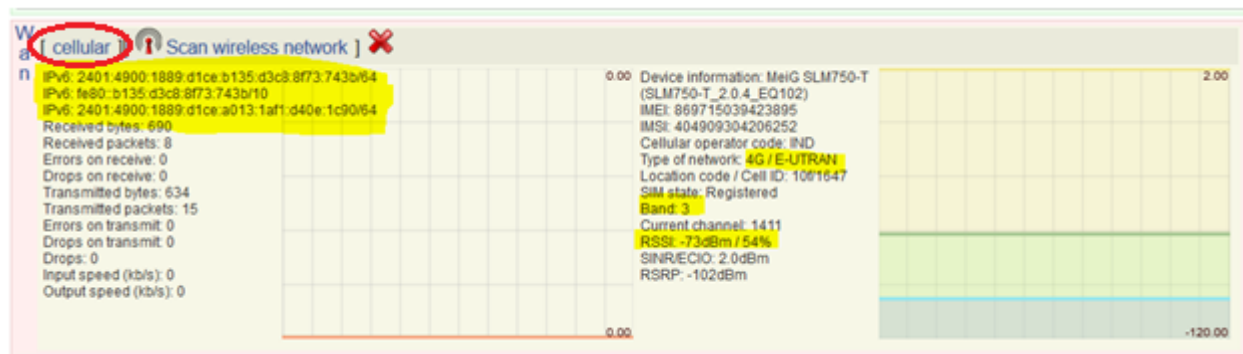


* В зависимости от установленного в маршрутизатор модема тип интерфейса сотового подключения может быть 'wwan0' или 'cellular', в данном руководстве для примера интерфейс 'wwan0' соответствует IPv4 сотовому соединению, а интерфейс 'cellular' предназначен для Ipv6.

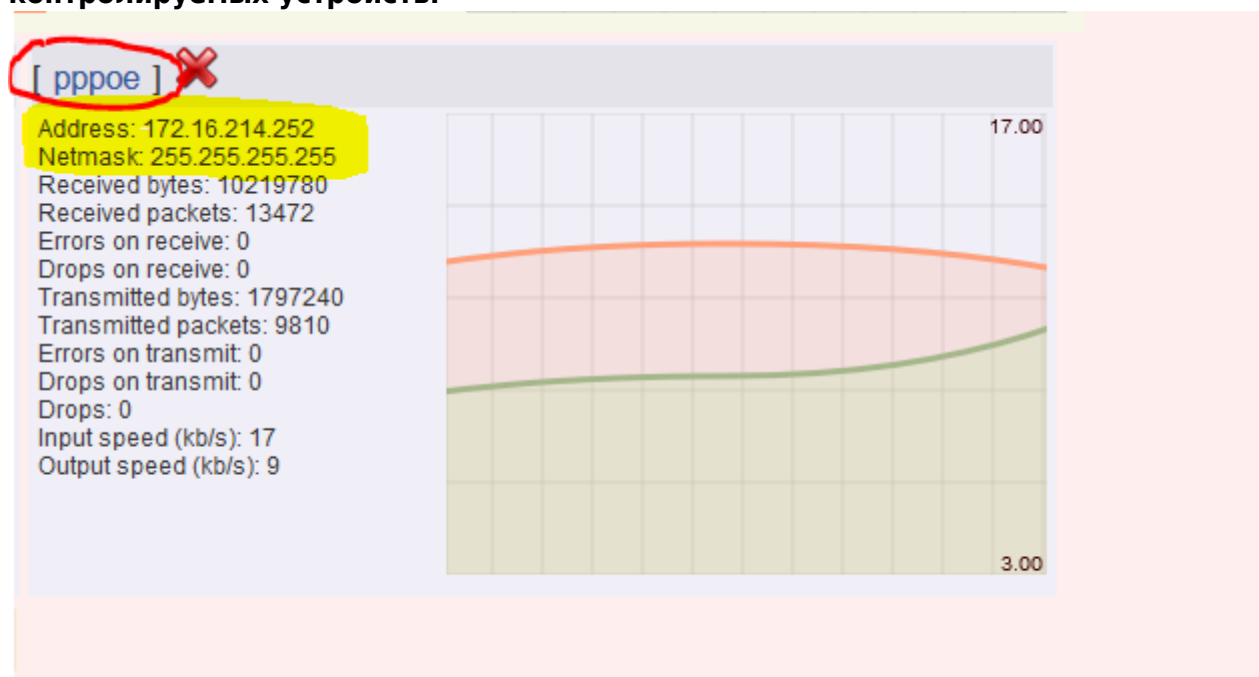
*** ===== Проверьте статус сотового подключения IPv4 ===== На домашней странице нужно найти интерфейс 'wwan0', это будет IPv4 сотовое соединение. Пользователю нужно проверить у этого интерфейса: - IPv4 адрес, назначенный оператором сотовой связи, - Статус регистрации сим-карты, - Привязку к текущей сети (2G/3G/4G), - Силу сигнала базовой станции.**



===== Проверьте статус сотового подключения IPv6 ===== Интерфейс с именем 'cellular' в данном примере является интерфейсом IPv6 для сотовых соединений. На следующей картинке выделены детали подключения:



Проверьте соединение PPPoE. Интерфейс 'pppoe' на домашней странице может означать туннель к агенту сервера NMMS (Network Management and Monitoring server). Данный агент применяется как вспомогательное устройство для связи NMMS и контролируемых устройств.



==== Проверьте статус IPsec туннелей ==== Если IPsec туннель поднят, статус интерфейса будет показан с внешними адресами обеих сторон туннеля и протоколом ESP. Если соединение не поднято, не сконфигурировано или сконфигурировано ошибочно, статус туннеля будет показан как 'Unknown'. В этом случае пользователю следует обратиться к руководству 'BR104 IPsec Configuration and Troubleshooting guide' для решения проблемы. ==== Проверьте маршрут по умолчанию ==== Откройте меню 'Diagnostic' и выберите опцию 'Routes' для того, чтобы увидеть таблицу маршрутизации. Маршрут с назначением '0.0.0.0' называется 'default route', т.е. маршрут по умолчанию.

The screenshot shows the OpenWRT web interface. The top navigation bar includes System, Network, Routes, Services, Utilities, and Diagnostic. The Diagnostic menu is open, showing options like Processes, Connections, Routes, ARP table, Logs, Create report for developers, Firewall rules, IPv6 filtering state, DHCP leases, Bridge filtering state, QOS state, and Current nameservers. The Routes page is displayed, showing a table of routes with columns for Destination, Gateway, Metric, and Interface. The interface also shows various system statistics and graphs.

Внимание! * 'Backup route', т.е. резервный маршрут не показывается в графическом интерфейсе. Его можно увидеть в выводе команды CLI:

Root@NETSHe# ip route show table default

*

The screenshot shows a PuTTY terminal window titled '10.117.150.65 - PuTTY'. The terminal displays the output of the command 'ip route show table default'. The output shows the default route table with the destination '0.0.0.0/0' and the gateway '120.138.115.72'. The interface 'pppoe' is listed as the outgoing interface. The command is highlighted with a red circle.

Настройка интерфейсов Внимание! *Пользователь должен проверить или заполнить все вкладки свойств интерфейса, затем сохранить настройки и перезагрузить маршрутизатор. Однако, если предполагается внести изменения нескольким интерфейсам и/или сервисам, то

следует все изменения выполнить (без нажатий опции 'restart the service'), а затем перезагрузить маршрутизатор для применения всех изменений в конфигурации.

*** Вид диалога параметров интерфейсов выглядит по-разному в зависимости от типа интерфейса. Обычно диалог для полноценного интерфейса имеет три вкладки: 1) 'Base Settings' вкладка, где предусмотрены общие параметры:**

- Опция включения/отключения интерфейса. - Опция для установки интерфейса как резервный к другому WAN интерфейсу. - Включение/отключение использования DNS от провайдера. (Опция отключения нужна в случае основного и резервного WAN. Поскольку разные провайдеры используют разные адреса DNS, а системный демон DNS не может оперировать с двумя наборами адресов одновременно, то рекомендуется отключить использование DNS обоих провайдеров и задать ручную свои настройки DNS.) - Опция включения IP passthrough mode на интерфейсе. Нужна в случае, когда надо пробросить адрес от провайдера на внутреннее устройство в своей сети. - Список методов аутентификации (PAP/CHAP/AUTO). - Варианты для ограничения стандартов сотового соединения AUTO/2G/3D/4G. 2) 'Additional' вкладка предназначена для привязывания интерфейса к зонам. Если интерфейс не привязан к зоне, часть сервисов на нем будет недоступна. 3) Вкладка 'Routes through interface' это наиболее короткий способ создать новый статический маршрут в таблице маршрутизации устройства. Вопросы маршрутизации рассматриваются подробнее в другом разделе данного руководства. Когда все настройки интерфейса заданы, следует нажать кнопку 'Save' и перезагрузить маршрутизатор, для того чтоб измененная конфигурация применилась. Для этого надо открыть меню 'Utilities' и выбрать 'Reboot System', далее выбрать 'Yes' на запрос перезагрузки устройства.

Внимание! * Все интерфейсы должны именоваться в соответствии с правилами, чтобы пользователям было понятно назначение интерфейса по его имени. Например, ethX соответствует физическому Ethernet порту, а имена pppoe/l2tp/pptp – соответствующим сервисам. Интерфейсы с '.auto' в имени создаются системой для сервисных нужд и не могут быть изменены пользователями.

Transmitted bytes: 21025056	
Transmitted packets: 44711	
Errors on transmit: 0	
Drops on transmit: 0	
Drops: 0	
Input speed (kb/s): 0	
Output speed (kb/s): 0	
wwan0]	
Address: 10.16.167.71	
Netmask: 255.255.255.240	
IPv6: fe80::f054:58ff:fed9:f9a8/64	
MAC: f2:54:58:d9:f9:a8	
Received bytes: 7820221	
Received packets: 15621	
Errors on receive: 0	
Drops on receive: 0	
Transmitted bytes: 1933982	
Transmitted packets: 17787	
Errors on transmit: 0	
Drops on transmit: 0	
Drops: 0	
Input speed (kb/s): 0	
Output speed (kb/s): 0	

*** ===== Сим-карта IPv4, интерфейс wwan0 =====**

Выберите интерфейс 'wwan0' на домашней странице, как это показано на картинке выше, откроются параметры интерфейса. На вкладке 'Base Settings' можно изменить

параметры сим-карты, а так же включить/отключить сам интерфейс.

[Configure interface wwan0]

Enable interface : ☒

Base settings | Additional | Helpful information | Routes through interface

Type of connection: * QMI

Username:

Password:

Access point (APN): airtelgprs.com

PIN code:

Authentication type: auto

Use any possible cellular network or specified only: auto

Disable roaming: ☐

Use interface as backup?: ☒

Do not replace existing default route?: ☐

Do not use peer DNS?: ☒

Enable IP v6 over PPP link?: ☐

Switch device in IP passthrough mode?: ☐

MTU: 0

Static IP address for interface. Usually ISP assigns address in automatic manner. Leave blank if you are unsure:

Tick to restart service(s) after saving: ☐ Save

На вкладке 'Additional' можно назначить интерфейс в 'WAN' зону.

[Configure interface wwan0]

Enable interface ? : ☒

Base settings | Additional | Band settings | Helpful information | Routes through interface

Interface is a member of zone: Wan

===== Сим-карта IPv6, интерфейс CELLULAR ===== **Внимание** * Конфигурирование IPv6 интерфейса вручную потребует дополнительной настройки DHCPv6 и определения правил NAT на сетевом экране IPv6.

* Для того, чтобы создать IPv6 интерфейс вручную, пользователю следует внизу домашней страницы найти поле 'Input name of interface to add' и ввести туда имя 'cellular' (без кавычек), щелкнуть кнопку 'New'.

Transmitted packets: 0
Errors on transmit: 0
Drops on transmit: 0
Drops: 0
Input speed (kb/s): 0
Output speed (kb/s): 0

[eth0]

IPv6: fe80::26b6:fdff:fe1c:f94e
MAC: 24:b6:fd:1c:f9:4e
Received bytes: 65549694
Received packets: 146285
Errors on receive: 0
Drops on receive: 0
Transmitted bytes: 12640066
Transmitted packets: 75029
Errors on transmit: 0
Drops on transmit: 0
Drops: 0
Input speed (kb/s): 10
Output speed (kb/s): 11

Transmitted packets: 0
Errors on transmit: 0
Drops on transmit: 0
Drops: 0
Input speed (kb/s): 0
Output speed (kb/s): 0

[tunipsec0] ❌

Configured

(You can use names like ethX.Y for VLANs, names like br* for bridges, pppX for PPP interfaces)

Input name of interface to add: cellular

New

После того, как откроются настройки интерфейса, на вкладке 'Base settings' ввести требуемые настройки.

System Network Routes Services Utilities Diagnostic

[Configure interface cellular]

Enable interface : ☒

Base settings Additional Helpful information Routes through interface

Type of connection: * CELLULAR

Cellular Service Subtype: UMTS/EDGE/GPRS

Username:

Password:

Device or interface used to establish connection: /dev/ttyUSB2

Access point (APN): airtelgprs.com

PIN code:

Authentication type: auto

Use any possible cellular network or specified only: auto

Disable roaming: ☐

Use interface as backup?: ☒

Do not replace existing default route?: ☒

Do not use peer DNS?: ☒

Enable IP v6 over PPP link?: ☒

Use synchronous PPP?: ☐

Disable buffering for PPP link?: ☐

Switch device in IP passthrough mode?: ☐

MTU: 0

Затем на вкладке 'Additional' назначить интерфейс в зону WAN, после чего нажать кнопку 'Save'.

System Network Routes Services Utilities Diagnostic

[Configure interface cellular]

Enable interface : ☒

Base settings Additional Helpful information Routes through interface

Interface is a member of zone: Wan

Tick to restart service(s) after saving : ☐ Save

Save changes and then click this link to configure QoS for this interface

* Filling of highlighted fields is mandatory!

===== PPPoE IPv4 интерфейс =====

Для того, чтобы вручную создать интерфейс PPPoE, пользователь должен заполнить поле 'Input name of interface to add' в конце домашней страницы именем 'pppoe' (без кавычек) и нажать 'New'.

[eth0]

IPv6: fe80::26b6:fdff:fe1c:f94e
MAC: 24:b8:fd:1c:f9:4e
Received bytes: 68987882
Received packets: 157503
Errors on receive: 0
Drops on receive: 0
Transmitted bytes: 14214085
Transmitted packets: 82653
Errors on transmit: 0
Drops on transmit: 0
Drops: 0
Input speed (kb/s): 9
Output speed (kb/s): 12

[tunipsec0] ❌

Configured

(You can use names like ethX.Y for VLANs, names like br* for bridges, pppX for PPP interfaces)

Input name of interface to add pppoe New

Далее на открывшейся вкладке 'Base settings' следует заполнить параметры подключения, как того требует провайдер.

System	Network	Routes	Services	Utilities	Diagnostic
--------	---------	--------	----------	-----------	------------

[Configure interface pppoe]

Enable interface : ☒

Base settings | Additional | Helpful information | Routes through interface

Type of connection: *
Username:
Password:
Device or interface used to establish connection:
PPTP/L2TP Server/PPPOE Service Name:

PPPoE
sushim

eth0.2
joisterbb

Use interface as backup?:
Do not replace existing default route ?:
Do not use peer DNS ?:
Enable IP v6 over PPP link ?:
Use synchronous PPP?:
Disable buffering for PPP link?:
Switch device in IP passthrough mode?:
MTU:

☐
☐
☐
☐
☐
☐
☐
0

Static IP address for interface. Usually ISP assigns address in automatic manner. Leave blank if you are unsure:

Tick to restart service(s) after saving : ☐

Save

Далее на вкладке 'Additional' пользователь должен добавить интерфейс в 'WAN' зону и нажать кнопку 'Save', чтоб сохранить настройки.

System	Network	Routes	Services	Utilities	Diagnostic
--------	---------	--------	----------	-----------	------------

[Configure interface pppoe]

Enable interface : ☒

Base settings | Additional | Helpful information | Routes through interface

Interface is a member of zone:

Wan

Do relaying for PPPoE connections?:

☐

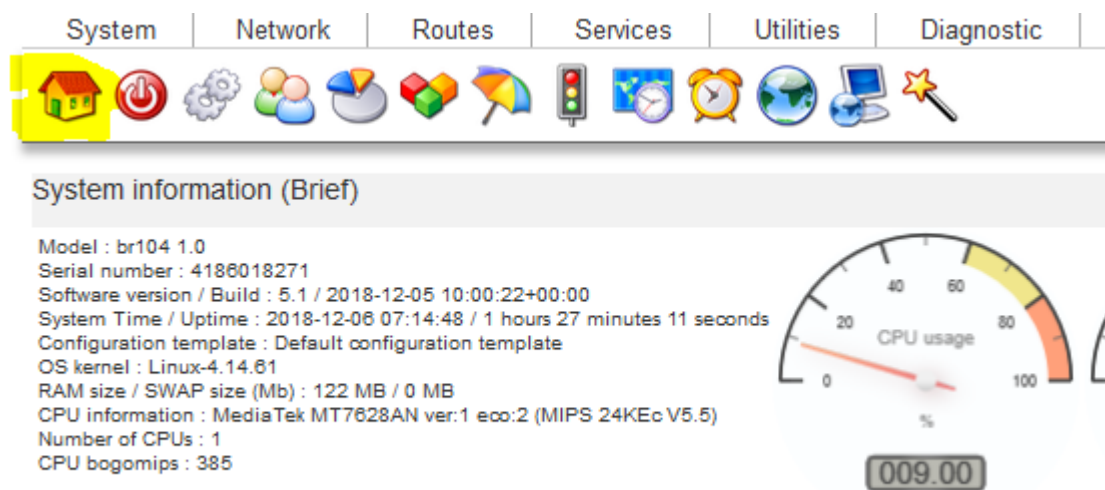
Tick to restart service(s) after saving : ☐

Save

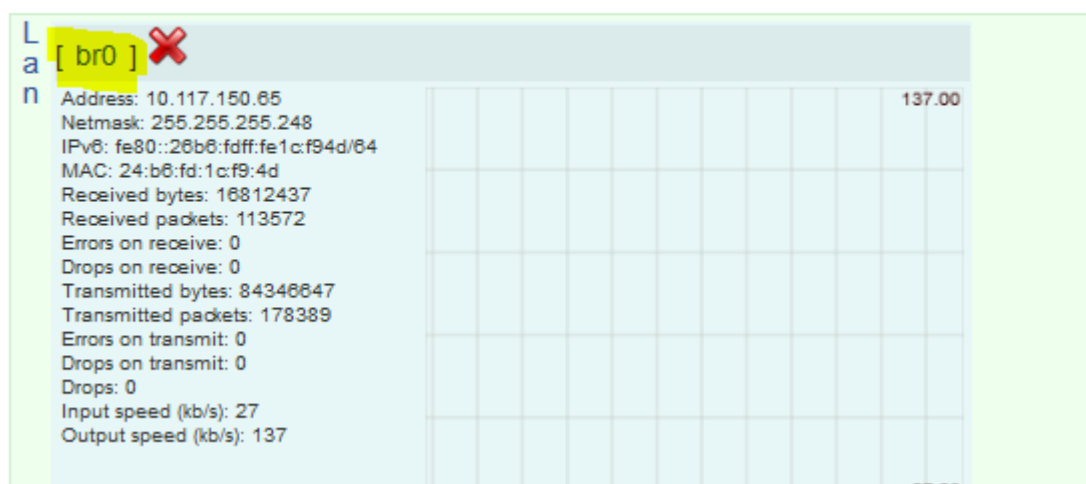
Save changes and then click this link to configure QoS for this interface

* Filling of highlighted fields is mandatory!

===== Интерфейс локальной сети br0 ===== Пользователь должен найти интерфейс 'br0' на домашней странице или в пункте меню 'Network→Interfaces'.



Firewall is enabled and launched



Далее

пользователь должен сделать следующее: - Щелкнуть по имени интерфейса 'br0', чтоб изменить настройки. - Убедиться, что интерфейс включен, проверив соответствующую опцию. - Отредактировать IP4 или IPv6 адрес и маску сети. - Сохранить настройки кнопкой 'Save'. - Перезагрузить маршрутизатор, чтоб настройки вступили в силу. ===== Настройка Wi-Fi ===== Пользователь может настроить Wi-Fi посредством настройки интерфейсов 'wlan0' и 'wlan1'. В зависимости от firmware устройство может иметь двух диапазонный Wi-Fi и 'wlan1' интерфейс соответственно. Рассмотрим настройки 5ГГц Wi-Fi для примера.

Enable interface : ☒

Wireless Wireless Security Wireless Multimedia (QoS) Settings Fast roaming, Interworking and Hotspot 2.0 Additional IP settings

Interface is a member of bridge:
 Mode: *
 ESSID: *
 Country Code:
 Modulation:
 Channel width:
 Current frequency:
 Transmitter power in dBm:

br0
 Access Point / Mesh gateway
 YourWiFi
 NN
 802.11ac
 80MHz
 5180
 0

Save

Save changes and then click this link to configure QoS for this interface

Enable interface : ☒

Wireless Wireless Security Wireless Multimedia (QoS) Settings Fast roaming, Interworking and Hotspot 2.0 Additional IP settings

Hide ESSID ? :
 Isolate clients ? :
 Limit number of connections ('0' for unlimited):
 Encryption:
 Disable TKIP:
 Username:
 Password, Encryption key or network passphrase:
 Allow connections to next MAC-addresses (comma separated list):
 Deny connections from next MAC-addresses (comma separated list):
 Certificate of Authority for Wireless network : Not installed
 Client Certificate : Not installed
 Private key : Not installed

☐
☐
 0
 WPA2 (Personal)
☐

 yourWiFipassword

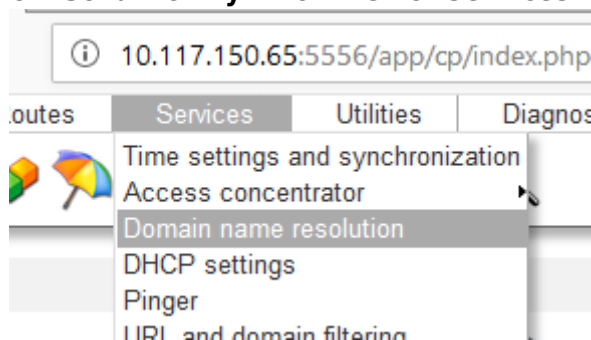
 Browse... No file selected.
 Browse... No file selected.
 Browse... No file selected.

Save

Save changes and then click this link to configure QoS for this interface

* Filling of highlighted fields is mandatory!

Пользователь опцией 'enable interface' может включить Wi-Fi и задать имя беспроводной сети (SSID), а так же WPA2 пароль для защиты. ===== Настройки DNS ===== Пользователю следует воспользоваться пунктом меню 'Services→Domain



'name resolution' как показано ниже.

выбрать вкладку 'DNS Resolver settings', ввести IP адрес DNS сервера в поле 'IP-Address of' и сохранить настройки кнопкой 'Save'.

Нужно

10.117.150.65:5556/app/cp/index.php?q=cp.dns.config

System Network Routes Services Utilities Diagnostic

Set up nameservers, static (local) host/address resolution, DNS forwarder and dynamic DNS client (if needed)

DNS Resolver settings Static DNS settings DNS forwarder Dynamic DNS service settings

Please, specify one or more nameservers to be used by the system

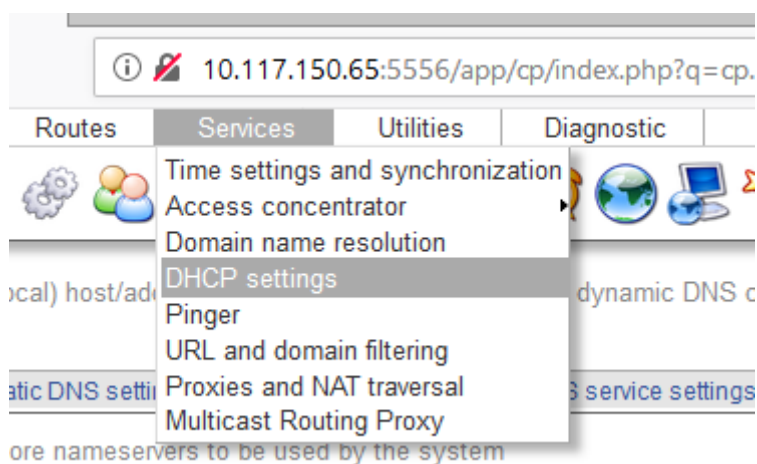
Our domain: * localdomain

IP-Address of nameserver (clear up input box to remove row from settings) * 8.8.8.8

Save

* Filling of highlighted fields is mandatory!

===== Настройка DHCP сервера IPv4 / IPv6 ===== Внимание! * Изменения в настройках DHCP следует производить, принимая во внимание IP-адрес интерфейса. Следует убедиться, что адрес интерфейса 'br0' из того же самого диапазона, что и DHCP пул для выдачи адресов клиентам. В противном случае эта нестыковка может не дать желаемого от DHCP результата.

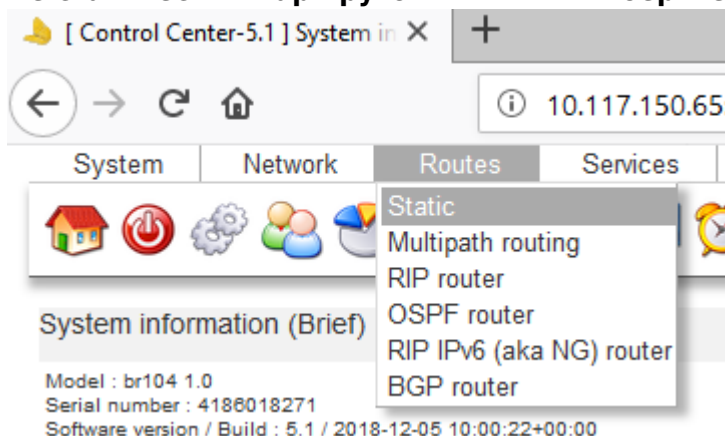


*** Выберите 'Services→DHCP Settings'**

Картинка ниже показывает параметры, которые можно задать: - DHCP пул адресов IPv4 / IPv6, - Опция включения/отключения DHCP сервера, - Время аренды адресов, - Привязки MAC адресов или резервирования IP.

System	Network	Routes	Services	Utilities	Diagnostic
DHCP Server settings (Interfaces where server works, IP pools, pairs of static MAC-address/IP-address to assign, etc)					
Tick to enable DHCP Server : ☒					
Choose interfaces to bind on and set up IP-pool to assign to clients * br0: ☒ IP range: 10.117.150.66 - 10.117.150.70 IPv6 range:					
Address of nameserver. The system offers own address if this field is blank: Address of WINS-server. The system offers own address if this field is blank: Default lease time: 7200 Maximum lease time: 86400					
Static IP-address assignment rules. Assign this IP-address to this MAC. Input order: MAC, IP-ADDRESS, description Use '+'-button to add a new rule. Clear up input boxes to remove rule from ruleset *					
Ignore requests to obtain IP-address from those MAC-addresses. Use '+'-button to add a new rule. Clear up input box to remove rule from ruleset *					
Static routes for clients (in notation AAA.BBB.CCC.DDD/netmask) and gateway (may be blank) *					
Tick to restart service(s) after saving : ☐ Save					

===== Добавление статических маршрутов ===== Выберите меню 'Routes', а в



нем пункт 'Static'.
 '+', чтоб добавить статический маршрут.

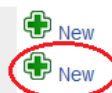
Щелкните на второй

Here you can setup static routes, routes for two or more uplinks, routing and nameservers for each uplink
 Enable multi-WAN support? ☐

Static routes: **wwan0** **eth1** **pppoe** **pptp** **l2tp** **cellular**

You can setup routes that will be removed from or installed to system routing table on boot

Routes that will be removed before other static routes will be installed *	Routes that will be installed when the system will booted *



Click this icon to add a new static route

Tick to restart service(s) after saving : ☐ **Save**

Add static route

Protocol: * IPv4

Address / Netmask: * 123.64.96.230 / 32

Interface: eth0.2

or

Gateway: 125.21.54.1

Metric: 1

Description: * APP server Route via Ethernet

Save

* Filling of highlighted fields is mandatory!

После нажатия 'Save' новый маршрут отразится в списке маршрутов, как показано ниже. Далее нажмите кнопку

http://10.229.47.14:5556/app/cp/index.php?q=core.route.config

System Network Routes Services Utilities Diagnostic

Here you can setup static routes, routes for two or more uplinks, routing and nameservers for each uplink

Enable multi-WAN support? ☐

Static routes wwan0 eth1 pppoe pptp l2tp cellular

You can setup routes that will be removed from or installed to system routing table on boot

Routes that will be removed before other static routes will be installed *

Routes that will be installed when the system will be booted *

Protocol	Address	Netmask	Interface	Gateway	Metric	Description	Options
IPv4	172.24.176.0	24	br0	10.229.47.13	1	Route to Customer LAN	

Total: 1

Tick to restart service(s) after saving: ☐ Save

'Save'.

Перезагрузите маршрутизатор, чтоб применить маршрут. Перезагрузку можно выполнить через пункт меню 'Utilities→Reboot system'.

192.168.1.1:5556/app/cp/index.php?q=core.route.config

System Network Routes Services Utilities Diagnostic

Here you can setup static routes, routes for two or more uplinks, routing and nameservers

Enable multi-WAN support? ☐

Static routes wwan0 eth1 pppoe pptp l2tp cellular

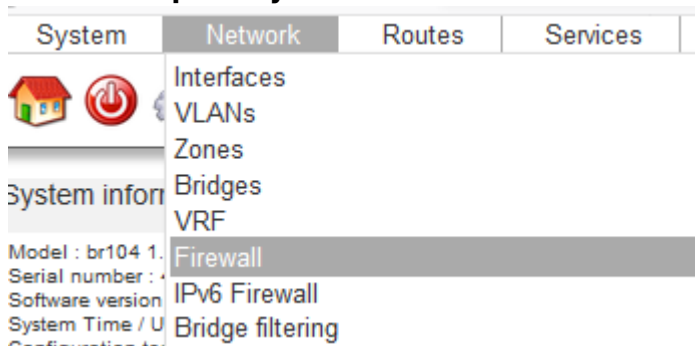
Utilities

- Ping host
- Traceroute
- Execute a command
- Reboot system
- Halt system
- Warm restart
- Backup/Restore
- Upgrade firmware

BR104

маршрутизатор поддерживает широкий набор функций маршрутизации, включая

протоколы динамической маршрутизации: RIP, OSPF, BGP, а так же механизмы типа маршрутизации от источника (source routing) или маршрутизации на основе политик (policy base routing). Функции маршрутизации собраны в пункте меню 'Routes'. Данный документ не сфокусирован на сетевых технологиях и их теории. В случае сложных применений или больших распределенных сетей пользователям следует проконсультироваться с техподдержкой ООО «Нетше лаб». ===== Сетевой экран и настройки NAT ===== Выберите пункт меню 'Network' и в нем строку 'Firewall'(IPv4)



или 'IPv6 Firewall'. Если маршрутизатор расположен на периметре сети, сетевой экран должен быть обязательно включен. Сетевой экран можно выключить на устройствах, используемых исключительно внутри безопасной сети. Если сетевой экран включен, то все интерфейсы маршрутизатора должны принадлежать какой-нибудь зоне. В противном случае трафик таких интерфейсов будет отбрасываться.

Device operates with zone-based firewall. [Configure zones](#)
Please, specify default policy for zone, set of advanced rules, NAT and port-forwarding if

Base settings Lan Wan Dmz

Tick to enable firewall :



Настройки сетевого

экрана любой зоны имеют три секции с правилами: - Первая секция описывает поведение экрана для входящего трафика зоны. Эти правила разрешают или запрещают трафик в зависимости от заданных TCP/UDP портов и/или IP адресов/подсетей приемника или источника. - Вторая секция включает правила проброса портов (Port forwarding) для входящего трафика на IP адреса внутри сети. - Третья секция реализует правила NAT(на базе источника). NAT (Network address translation) нужен для передачи IP-пакетов локального источника по сети Интернет, заменяя локальный адрес на публичный IP, маршрутизируемый в сети Интернет.

Base settings Lan Wan Dmz

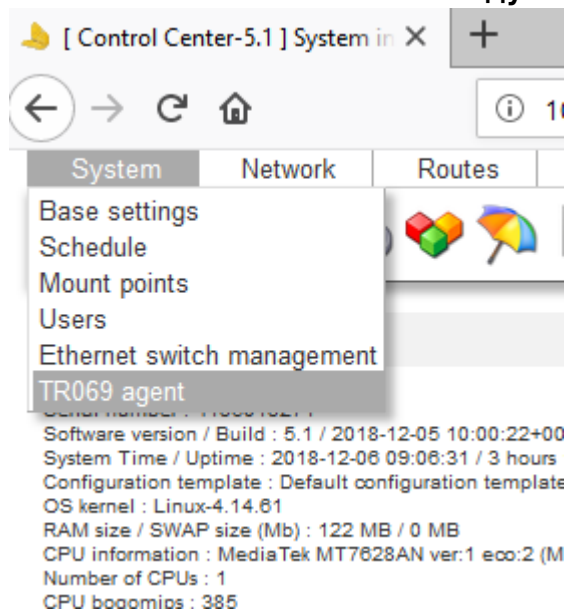
Default policy :		
Incoming traffic:	Accept	Tick to log mached packets: ☐
Outgoing traffic:	Accept	Tick to log mached packets: ☐
Forwarding traffic:	Accept	Tick to log mached packets: ☐
What is to be done with forwarding to other zones traffic :		
Zone	Tick to do NAT	Tick to fix MSS for transit packets (Enabling this option can decrease performance)
Wan	☒	☒
Dmz	☐	☐

===== Настройка Port Forwarding ===== В обратном направлении действует Port Forwarding или PAT (Port Address Translation), который используется для доступа к локальным IP-адресам из Интернет. Наши устройства реализуют PAT тем же системным механизмом, что реализует и сетевой экран. В случае port forwarding настройки правил имеют следующий вид: - Протокол может быть TCP или UDP. - 'External IP' это адрес, запрашиваемый из Интернет. Пользователь может его не

указывать, тогда запрос на любой адрес будет попадать под это правило. - 'External Port' это порт, запрашиваемый из Интернет. В общем случае он может быть случайным, тогда надо это поле в правиле не заполнять. - 'Internal address' это IP адрес из локальной сети, который привязан правилом к внешнему адресу WAN в целях доступности из Интернет. - 'Internal port' это порт приложения локального сервера, на который внешний запрос и будет отправлен. Чаще всего это популярные порты TCP типа 443 для SSL. - 'Description' любое понятное описание правила, объясняющее его суть и отличающее его от других правил.

Save the settings after Done.

===== Настройка агента TR069 ===== Пользователю следует из меню 'System'



выбрать строку 'TR069 agent'. В открывшемся диалоге пользователь должен задать параметры TR069 ACS сервера, как того требует администратор этого сервера.

System	Network	Routes	Services	Utilities	Diagnostic
					
Please, set up ACS url, credentials and device-specific data. You should be registered in ACS and have login/password to access Automatic configuration server (ACS) helps you to management of your device					
Enable TR-069 client? :					☒
Full specified URI for ACS server : *					http://demo.friendly-tech.com:8080/ftacs-basic/ACS
Login : *					tata
Password : *					*****
Device manufacturer : *					NETSHe
Hardware version : *					1.0
Specify organization unique identifier (OUI) : *					1314af
Serial number					4186018271
Specify the interface to listen by agent : *					pppoe
Login to deal with local agent :					
Password to deal with local agent :					
Specify local port to listen by agent					
Interval to send informs to server in seconds. (0) means configured by server					3000
You can specify external IP address if device is behind NAT and port forwarding is configured					
Disable 'Expect: 100-continue' in request to deal with some servers :					☐
Send INFORM messages only :					☐
Tick to restart service(s) after saving : ☐ Save					

После сохранения настроек маршрутизатор нужно перезагрузить. Для этого пользователь может воспользоваться меню 'Utilities' и пунктом 'Reboot system'.
 ===== Балансировка нагрузки для двух Ethernet WAN портов ===== Первый Ethernet порт на маршрутизаторе это WAN порт по умолчанию. Чтоб создать дополнительный Ethernet WAN порт, пользователю нужно сделать небольшие изменения, а именно, сделать таговый порт с новым VLAN таким образом, чтобы устройство могло оперировать портами, логически разделенными на VLAN-ы. Другими словами пользователь должен изолировать любой из LAN портов в новом VLAN-е, чтобы тот стал WAN портом. ===== Настройка VLAN метки ===== Картинка ниже показывает умалчиваемые настройки встроенного коммутатора. Пользователь может найти их в меню 'System→Ethernet Switch Management'.

政治密室軍事「郭德亮換職」? | Google 翻譯 | 政治 - Yahoo 奇摩新聞 | [Control Center-5.1] Ethernet | Index of /share/strix

← → ↻ 🔒 不安全 | 192.168.1.1/app/cp/index.php?q=core.ethsw.config 🔍 ☆ 已暫停

StrixSYSTEMS
Networks Without Wires®

System Network Routes Services Utilities Diagnostic

Please, configure switch here. You can specify VLAN ID for each port. Put '0' in input field to remove port from settings

Attention! Please, be very careful.
Wrong data may brick your device!
Some switches allows to use VLAN IDs in range 1-15 only (Please refer to your support).
You should reboot device when switch configuration has been changed

Switch setup :

Ports	VLAN ID for port
Port 0	2
Port 1	1
Port 2	1
Port 3	1
Port 4	1
Port 5	0

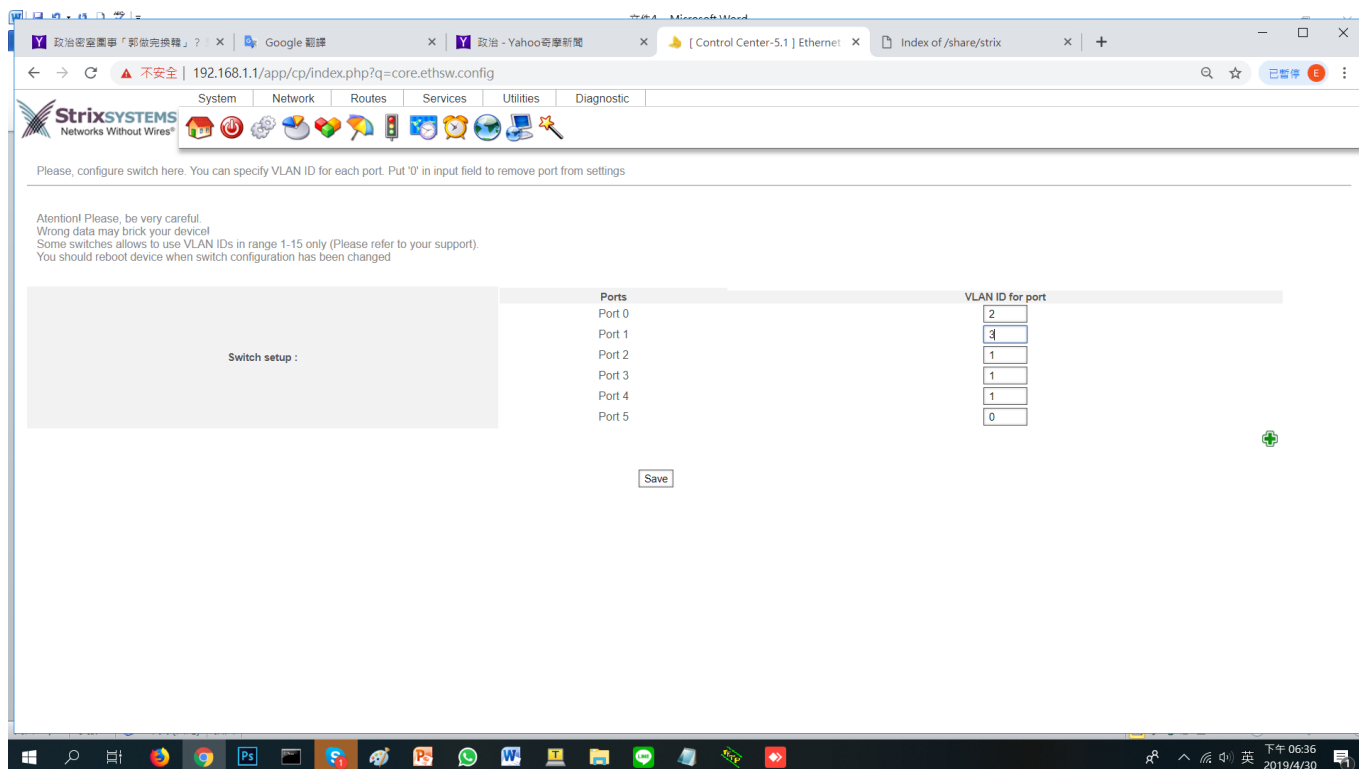
Save

下午 06:35 2019/4/30

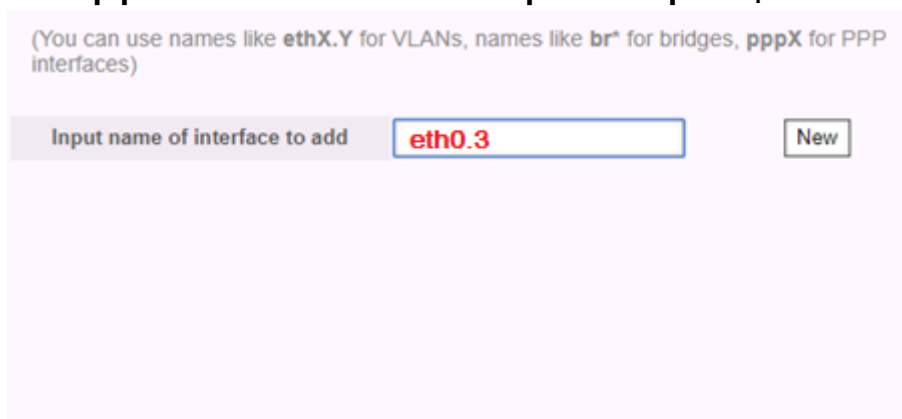
Чтоб создать новый Ethernet WAN интерфейс, пользователь вносит изменения,

которые показаны ниже. Номер “3” в поле VLAN ID для Port 1 (Физически это второй порт на маршрутизаторе слева направо). Внимание! * VLAN здесь означают так называемые VLAN на основе портов. Чтоб оперировать VLAN 802.11q, пользователь должен создать интерфейсы следующего уровня, например, eth0.3.20 для dot11.q VLAN20.

*

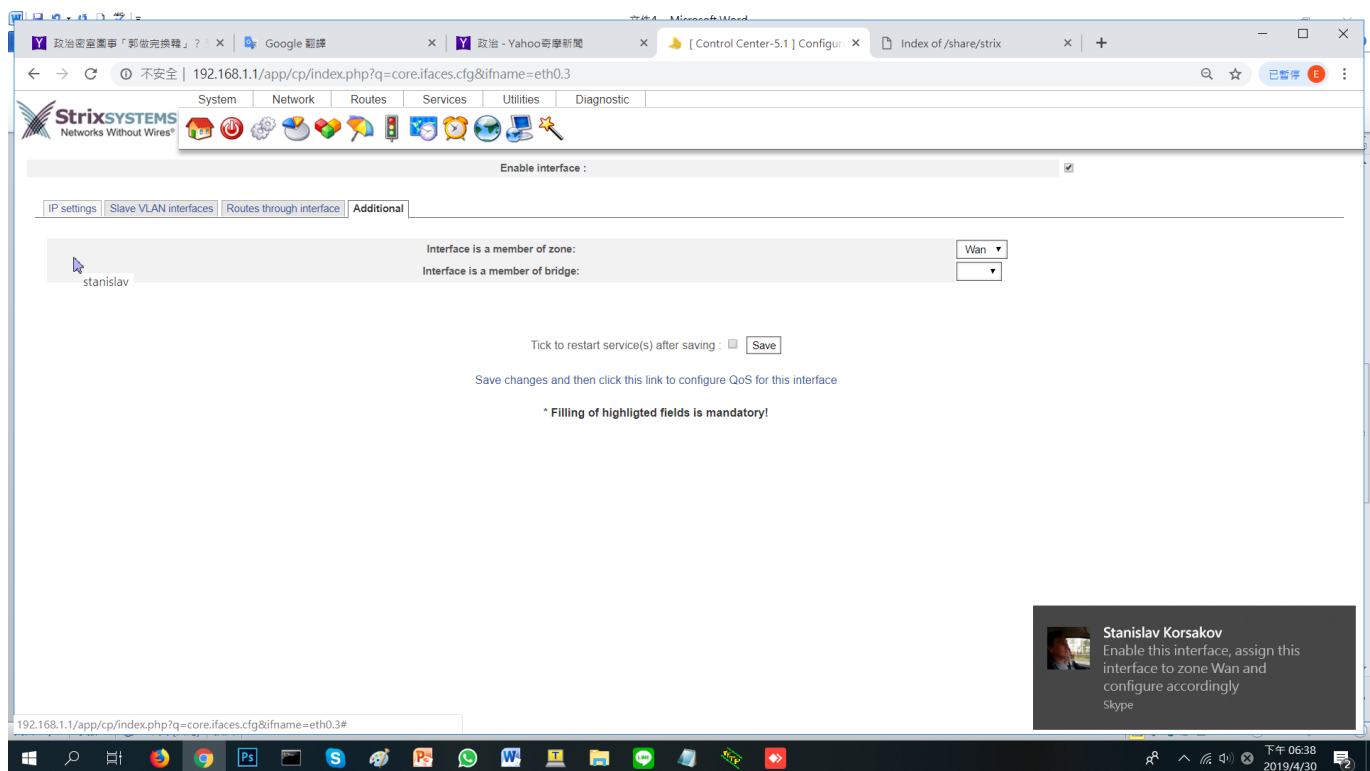


Для этого надо открыть ‘Network→Interfaces’, промотать до конца списка, найти поле для нового интерфейса, как показано на следующей картинке. Ввести ‘eth0.3’ в поле имени создаваемого интерфейса и нажать ‘New’. Откроется страница со свойствами

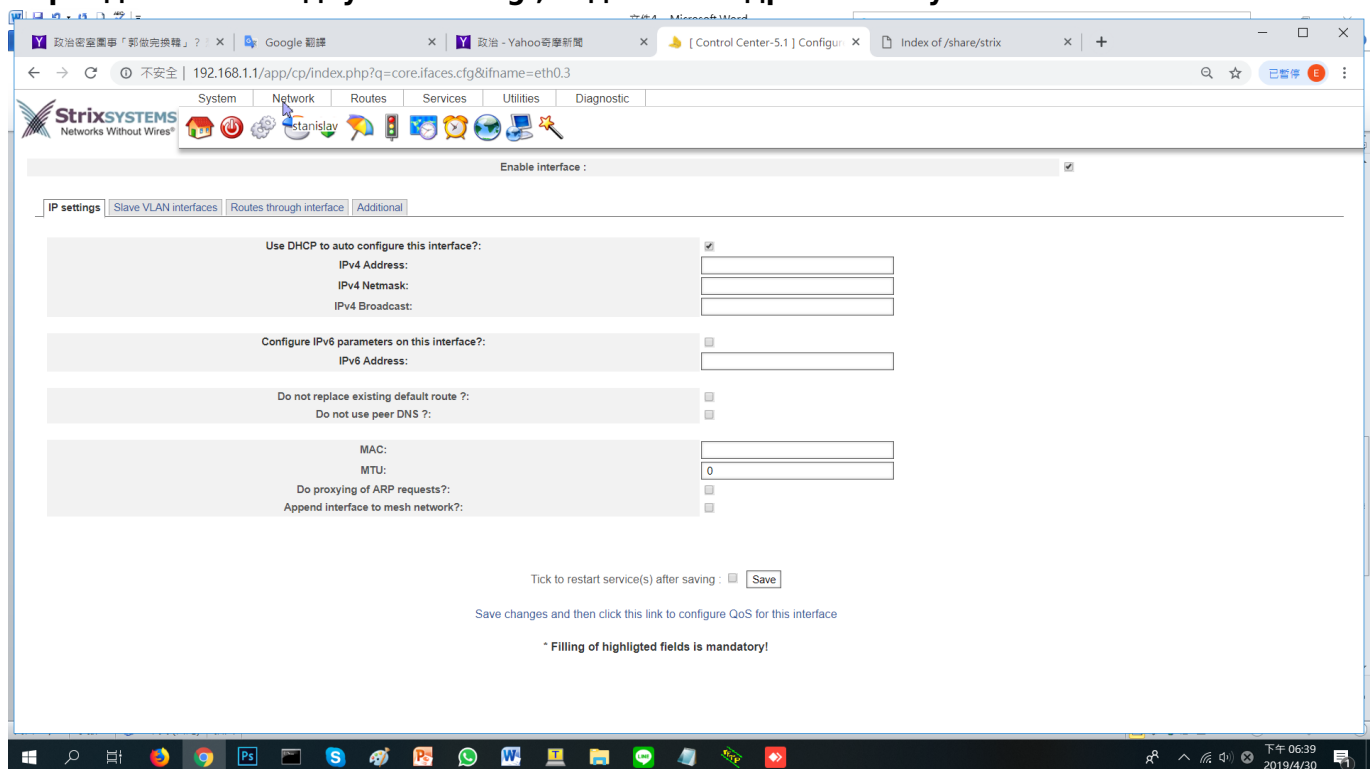


интерфейса eth0.3.

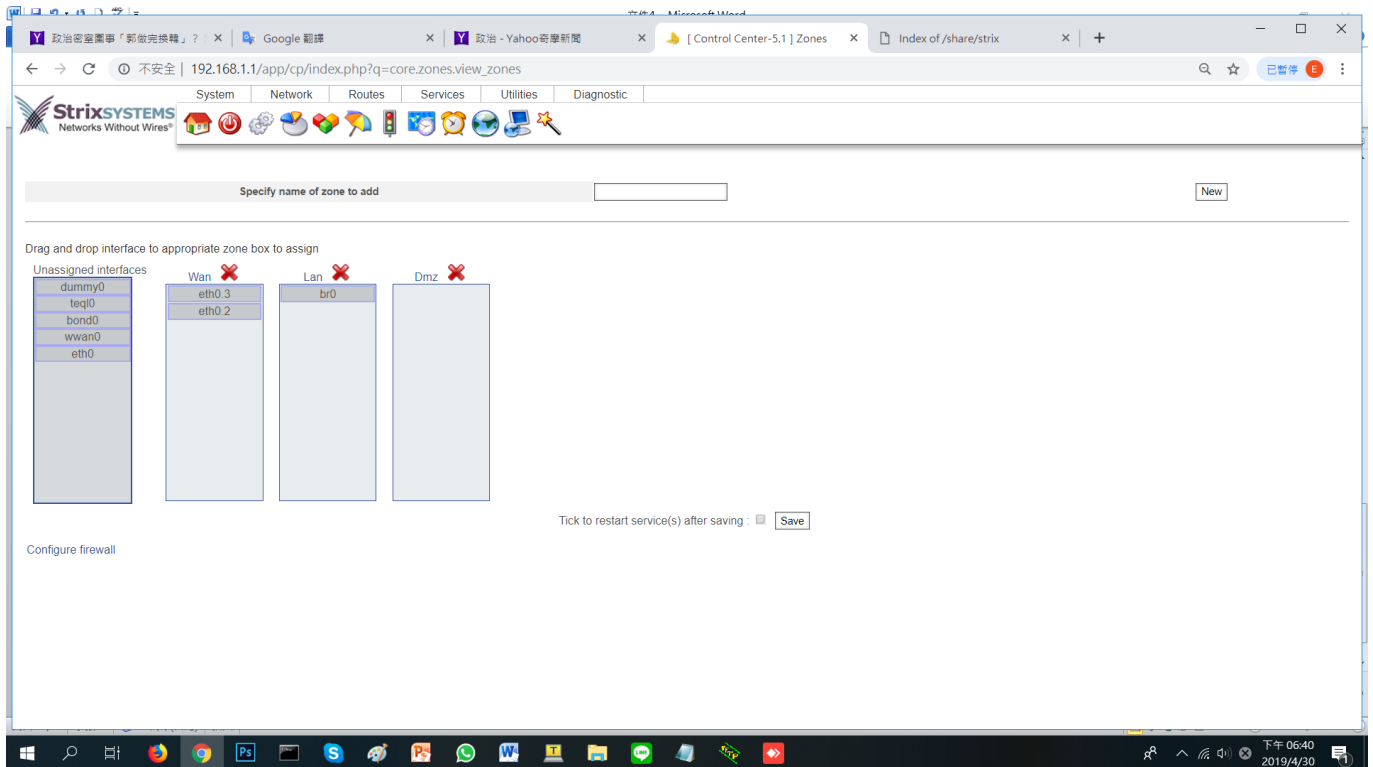
Отметьте опцию ‘Enable’ в верхнем правом углу. Так же убедитесь на вкладке ‘Additional’, что интерфейс eth0.3 добавлен в зону ‘WAN’.



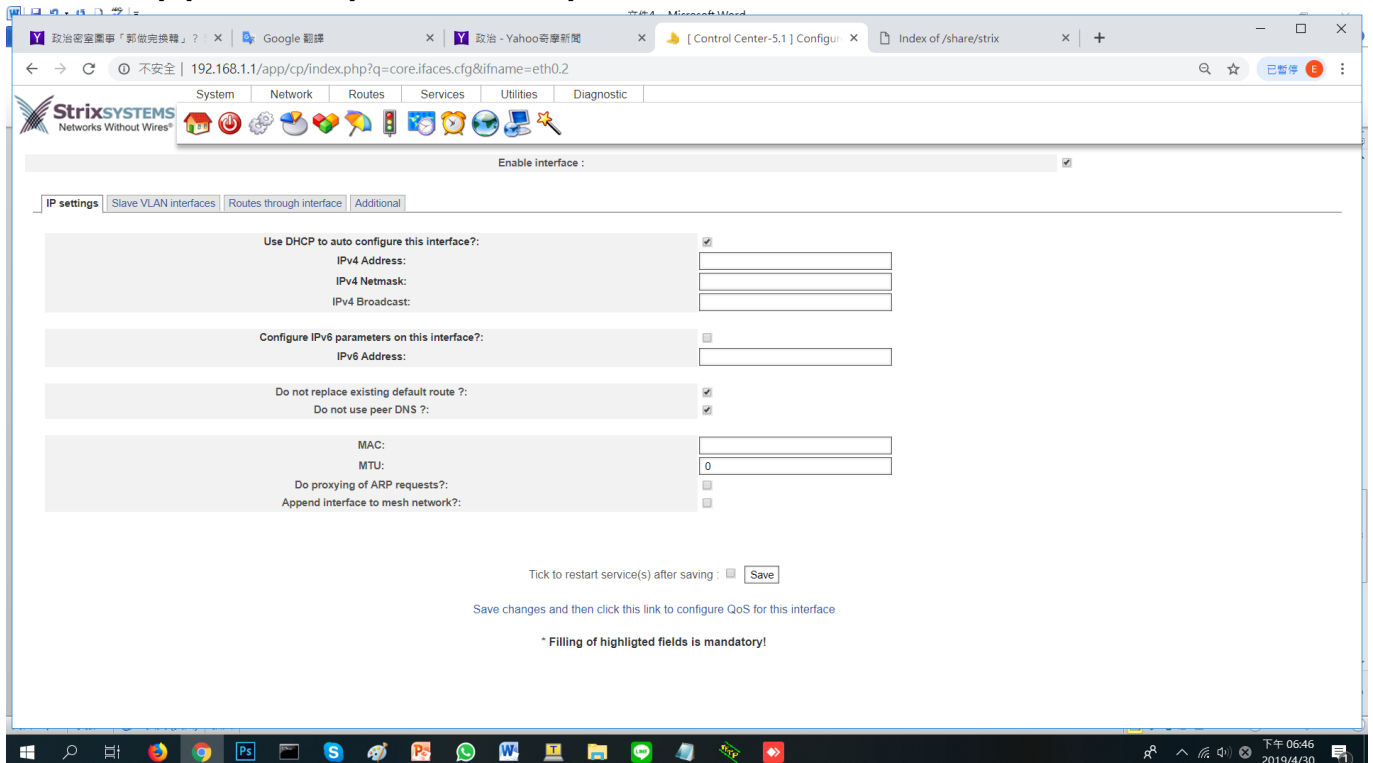
Перейдите на вкладку 'IP Setting', задайте IP адрес и маску сети.



==== Настройки зон ==== В пункте 'Network→Zones' пользователь увидит следующее (имена интерфейсов могут быть другими).



В данном примере пользователю следует проверить вновь созданный eth0.3, входит ли он в зону WAN. Если нет, то пользователь должен перетащить eth0.3 в WAN, а затем нажать 'Save'. ===== Балансировка нагрузки ===== В случае двух WAN портов необходимо настраивать общий DNS, для этого на каждом из WAN интерфейсов нужно отметить опцию 'Do not use peer DNS'. Как уже объяснялось, системный DNS демон может работать только с одним набором настроек DNS, поэтому настройки DNS должны быть определены глобально на маршрутизаторе и выключены на каждом из WAN интерфейсов. Картинка для первого WAN eth0.2:



Картинка для второго WAN eth0.3:

Enable interface: ☒

IP settings | Save VLAN interfaces | Routes through interface | Additional

Use DHCP to auto-configure this interface?: ☒

IPv4 Address:

IPv4 Netmask:

IPv4 Broadcast:

Configure IPv6 parameters on this interface?: ☐

IPv6 Address:

Do not replace existing default route?: ☒

Do not use peer DNS?: ☒

MAC:

MTU:

Do proxying of ARP requests?: ☐

Append interface to mesh network?: ☐

Tick to restart service(s) after saving: ☐ Save

===== Настройка общего DNS ===== Выберите пункт меню 'Services→Domain name resolution' и далее вкладку 'DNS resolver settings'. Введите адрес доступного DNS сервера.

DNS Resolver settings | Static DNS settings | DNS forwarder | Dynamic DNS service settings

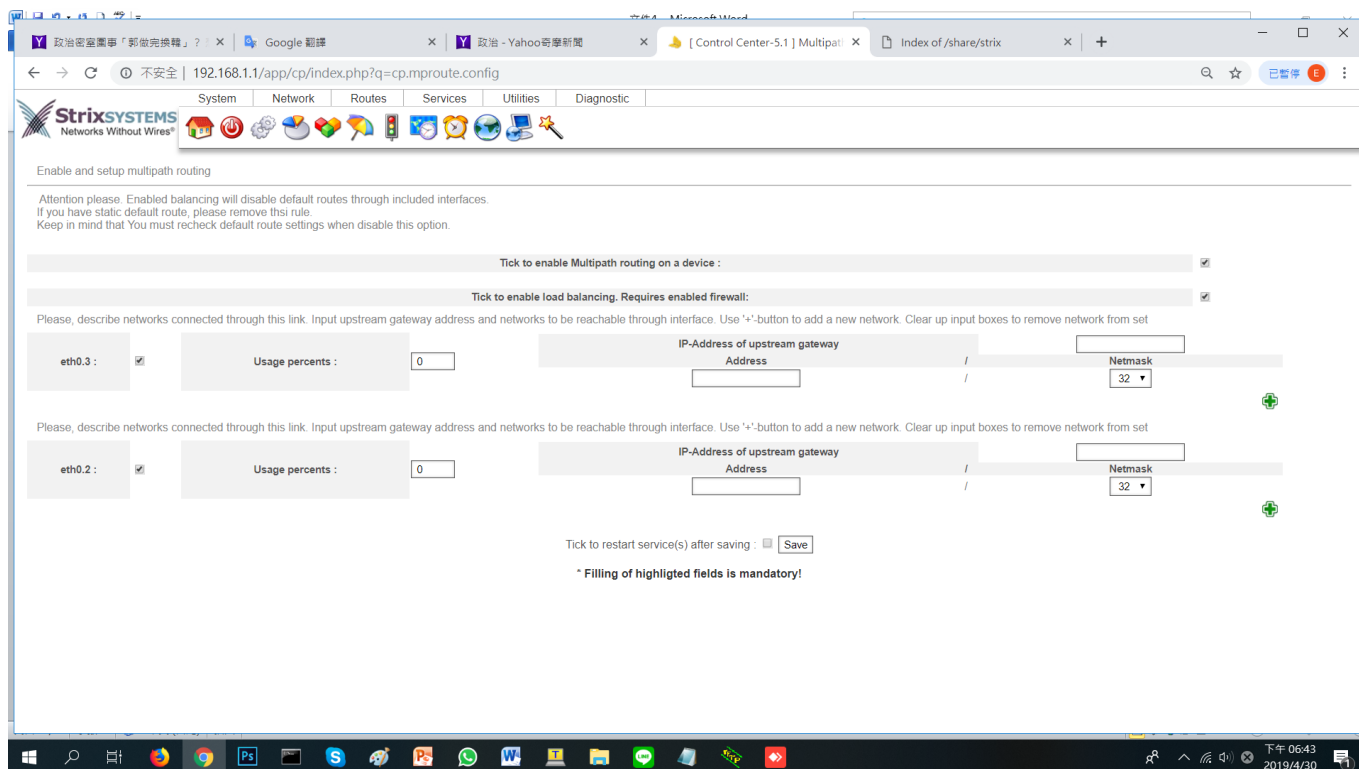
Please, specify one or more nameservers to be used by the system

Our domain: * localdomain

IP-Address of nameserver (clear up input box to remove row from settings) * 8.8.8.8

Save

Балансировка нагрузки в терминах NETSHe называется 'Multipath Routing'. Найдите одноименный пункт меню в меню 'Routes' и сделайте следующее: - Включите 'Multipath Routing', для этого выберите одноименную опцию и 'Load balance' под ней. - Слева на странице выберите eth0.2 и eth0.3 для включения балансировки между ними. - Умалчиваемое значение 0 означает балансировку 50/50. Эту величину можно изменить по усмотрению пользователя. - Сохраните изменения.

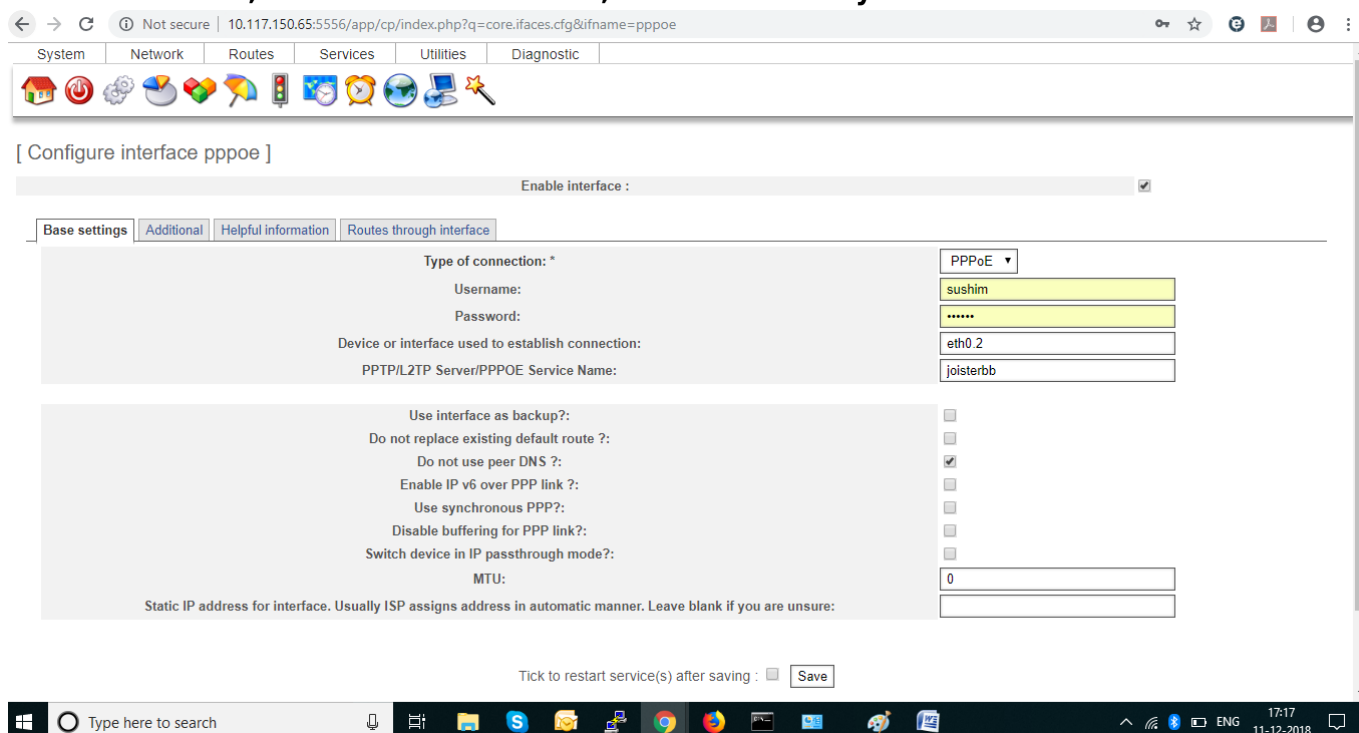


===== Отказоустойчивость при двух WAN (основной - резервный) =====

Предположим, у пользователя имеется: - PPPoE WAN соединение на местного провайдера Интернет, которое получает частный IP на PPPoE интерфейсе. - Сим-карта с Интернет подключением в качестве резервного WAN. Конфигурация с основным и резервным подключением может быть настроена и проверена следующими шагами:

===== Настройки PPPoE интерфейса =====

У PPPoE WAN интерфейса откройте вкладку 'Base Settings', проверьте опцию 'Do not use Peer DNS' и, если что-то изменили, нажмите кнопку 'Save'.



===== Настройка WWAN0 (сим-карты) ===== Откройте параметры интерфейса 'wwan0' на вкладке 'Base Settings', выделите опции 'Use this interface as Backup' и 'Do not use peer DNS', сохраните настройки.

← → ↻ ⓘ Not secure | 10.117.150.65:5556/app/cp/index.php?q=core.ifaces.cfg&iface=wwan0

System Network Routes Services Utilities Diagnostic

[Configure interface wwan0]

Enable interface : ☒

Base settings Additional Helpful information Routes through interface

Type of connection: * QMI

Username: sushim

Password: *****

Access point (APN): airtelgprs.com

PIN code:

Authentication type: auto

Use any possible cellular network or specified only: auto

Disable roaming: ☐

Use interface as backup?: ☒

Do not replace existing default route?: ☐

Do not use peer DNS?: ☒

Enable IP v6 over PPP link?: ☐

Switch device in IP passthrough mode?: ☐

MTU: 0

Static IP address for interface. Usually ISP assigns address in automatic manner. Leave blank if you are unsure:



==== Настройка общего DNS для двух WAN ==== Откройте меню 'Services→Domain name resolution' на вкладке 'DNS resolving settings' или с иконки на панели инструментов, как это показано на картинке ниже. Задайте адрес DNS сервера, сохраните настройки.

← → ↻ ⓘ Not secure | 10.117.150.65:5556/app/cp/index.php?q=cp.dns.config

System Network Routes Services Utilities Diagnostic

Set up nameservers, static (local) host/address resolution, DNS forwarder and dynamic DNS client (if needed)

DNS Resolver settings Static DNS settings DNS forwarder Dynamic DNS service settings

Please, specify one or more nameservers to be used by the system

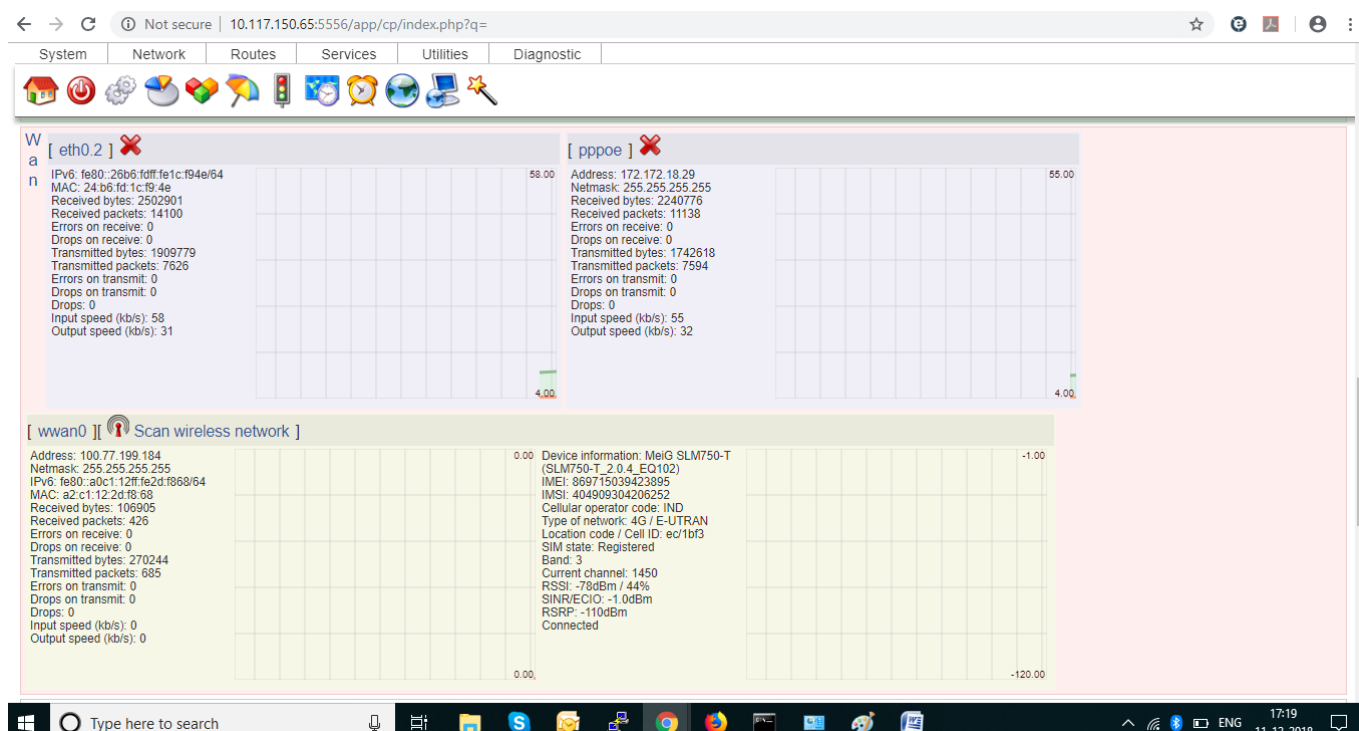
Our domain: * localdomain

IP-Address of nameserver (clear up input box to remove row from settings) * 8.8.8.8

Save

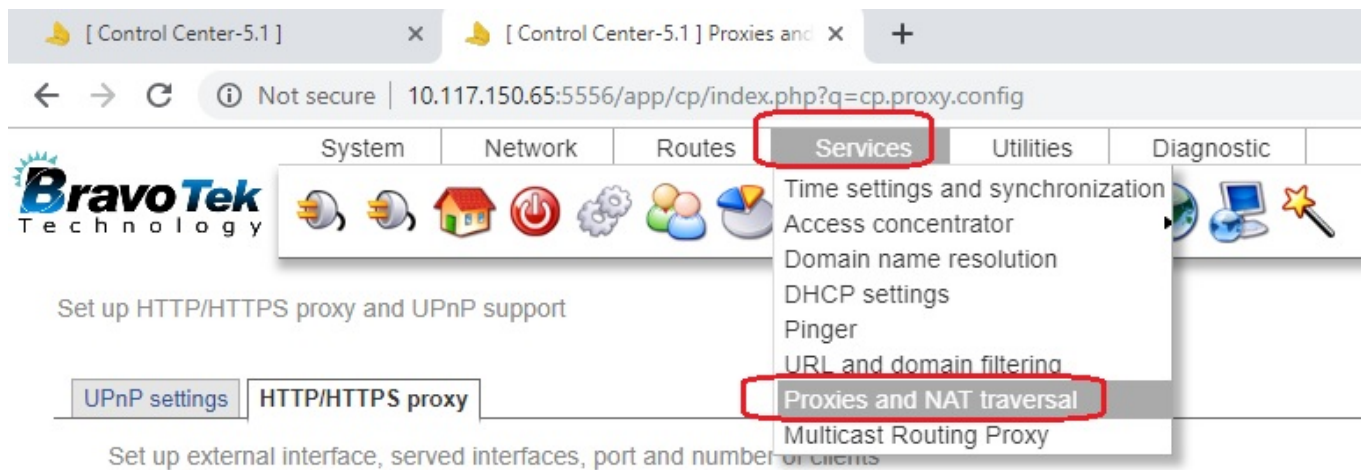
* Filling of highlighted fields is mandatory!

Проверьте, оба ли WAN соединения подняты, как показано на картинке:



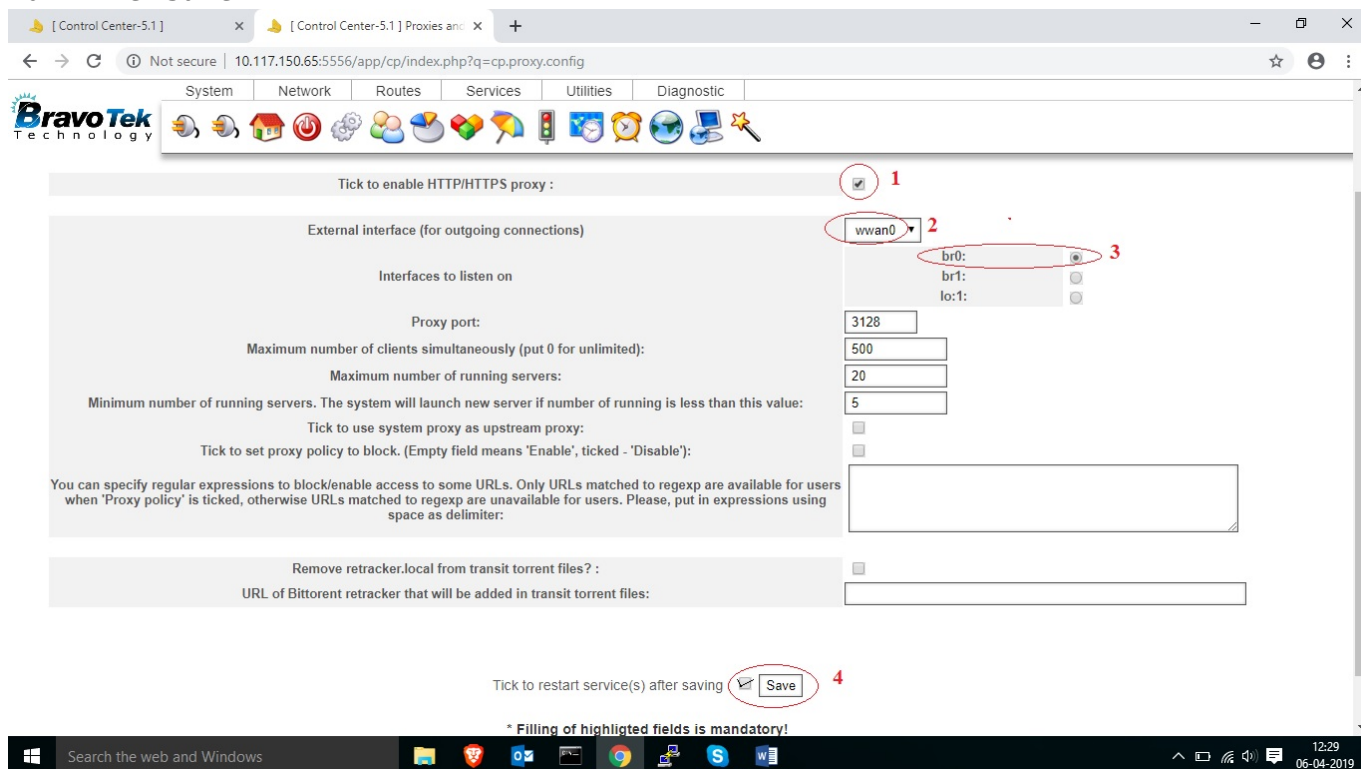
Когда оба интерфейса WAN имеют назначенные IP адреса, проверьте соединение с Интернет серфингом или откройте почту. Отключите основное соединение, подождите, пока соединение перестроится на резервный WAN. Время переключения зависит от типа порта и используемого типа соединения (обычно около полутора минут). **Внимание!** * Если интерфейсы не настроены как основной и резервный, и оба работают, то в случае падения одного из них, второй продолжает работать, но с большой задержкой в 4-5 секунд в зависимости от скорости соединения.

* ===== URL фильтрация ===== Механизм URL фильтрации в устройствах с ОС NETSHe работает согласно следующим принципам: - На странице URL фильтрации пользователь увидит две секции. Верхняя секция предназначена для HTTPS трафика (Blacklist), нижняя секция - для HTTP (Blacklist или Whitelist). - HTTPS трафик может только блокироваться по «черному» списку. Поскольку HTTPS передает зашифрованные данные, он не может быть досмотрен напрямую. Это требует высокопроизводительное оборудование для выполнения расшифровки, и только после этого пакеты могут блокироваться. Однако маршрутизатор может блокировать (blacklist) трафик по URL. Что бы пользователь ни указал в данной секции, это будет блокироваться, а остальной трафик пропускаться. - HTTP трафик пропускается по «белому» списку, если не выбрана опция 'URL filtering policy' и заполнен список URL. Все упомянутое в этом списке будет пропускаться, а остальной трафик будет блокироваться. - HTTP трафик будет фильтроваться по «черному» списку, если опция 'URL filtering policy' выбрана и список URL определен. Все, что там указано, будет заблокировано. Все поисковые системы и прокси не могут быть заблокированы полностью, какие-то из них будут заблокированы, а какие-то успешно проходить. По той же самой причине. Этот тип сайтов нужно тщательно inspectировать, применяя базы данных сигнатур, а для этого требуется производительное оборудование. Настройка URL фильтрации включает в себя несколько шагов: - Нужно включить HTTP Proxy, - Нужно включить фильтрацию URL, - Задать URL списки. Включить HTTP Proxy В процессе фильтрации используются функции встроенного в маршрутизатор сервиса прокси. Пользователям не нужно указывать настройки этого прокси на своих устройствах.



Tick to enable HTTP/HTTPS proxy :

Включите опцию 'Enable service' сверху и выберите подходящий WAN интерфейс (для сотовых подключений имя интерфейса 'wwan0'), выберите 'br0' для прослушивания и нажмите 'Save'.



==== Параметры URL фильтров ==== Выберите пункт 'Services' и в нем строку 'URL and domain filtering'.

[Control Center-5.1] System info x +

← → ↺ ⓘ Not secure | 192.168.168.1:5556/app/cp/index.php

System Network Routes **Services** Utilities Diagnostic

BravoTek Technology

System information (Brief)

Model : ap147-2 1.0
 Serial number : 3831834136
 Software version / Build : 5.1 / 2019-04-04 14:15:59+00:00
 System Time / Uptime : 2019-04-06 13:22:12 / 6 minutes 21 seconds
 Configuration template : Default configuration template
 OS kernel : Linux-4.14.61
 RAM size / SWAP size (Mb) : 122 MB / 0 MB
 CPU information : MediaTek MT7628AN ver:1 eco:2 (MIPS 24KFc V5.5)

Time settings and synchronization
 Access concentrator
 Domain name resolution
 DHCP settings
 Pinger
URL and domain filtering
 Proxies and NAT traversal
 Multicast Routing Proxy

==== HTTPS «черный» или «белый» списки =====

===== HTTPS «черный» или «белый» списки =====

You can configure blocking for HTTP sites by matching in URLs and DNS resolution for specified domains. DNS blocking prevent accessing HTTPS sites by domain names.

Enable filtering :

☒

Block DNS resolution for next domains (space separated list). It prevents any connection (e.g. HTTPS) to this names :

in.yahoo.com mail.gmail.com google.co.in

Tick to set URL filtering policy to block. (Empty field means 'Allow all except matched', ticked - 'Allow only matched'):

☒

Space delimited list of words to block (or enable if policy is 'block') HTTP requests which has matched words in URL:

pmtv.in ndtv.com bing.com

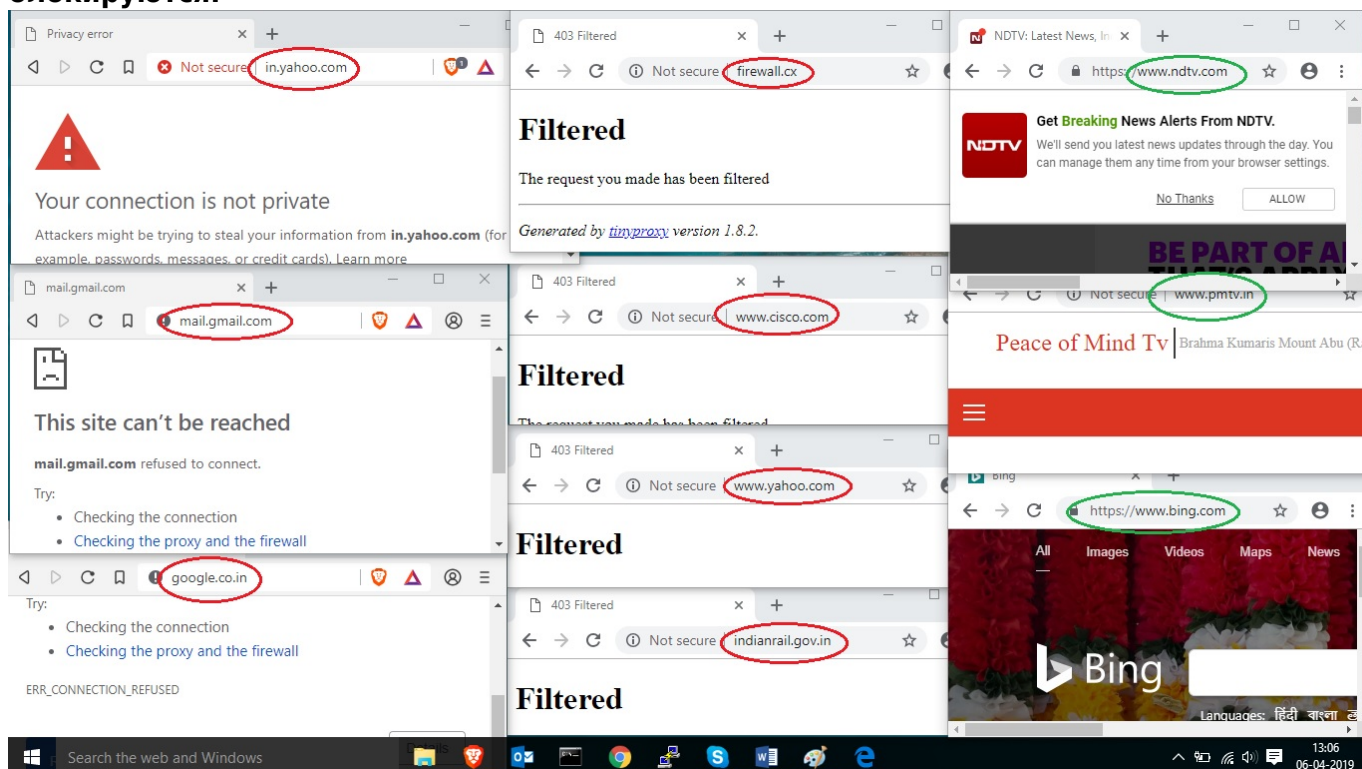
Save

List of Sites to Allow

Only these sites allowed , all other http sites blocked.

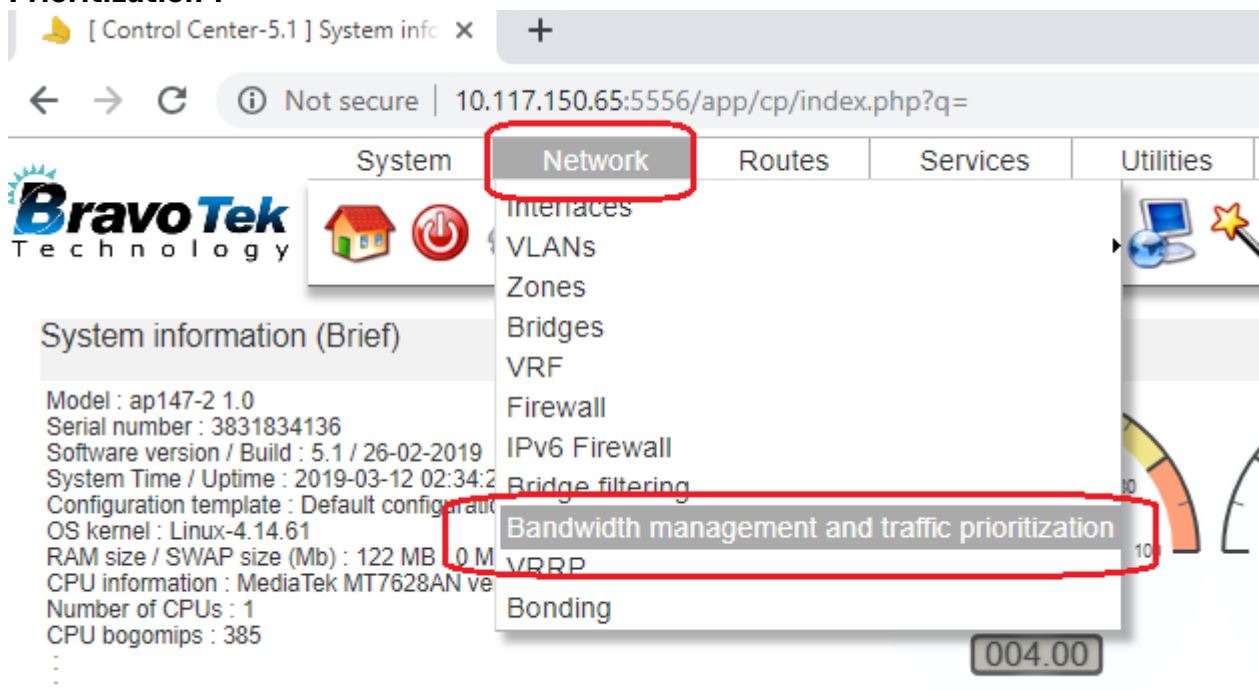
* Filling of highlighted fields is mandatory!

Результат показан ниже: сайты по «белому» списку открываются, а остальные блокируются.



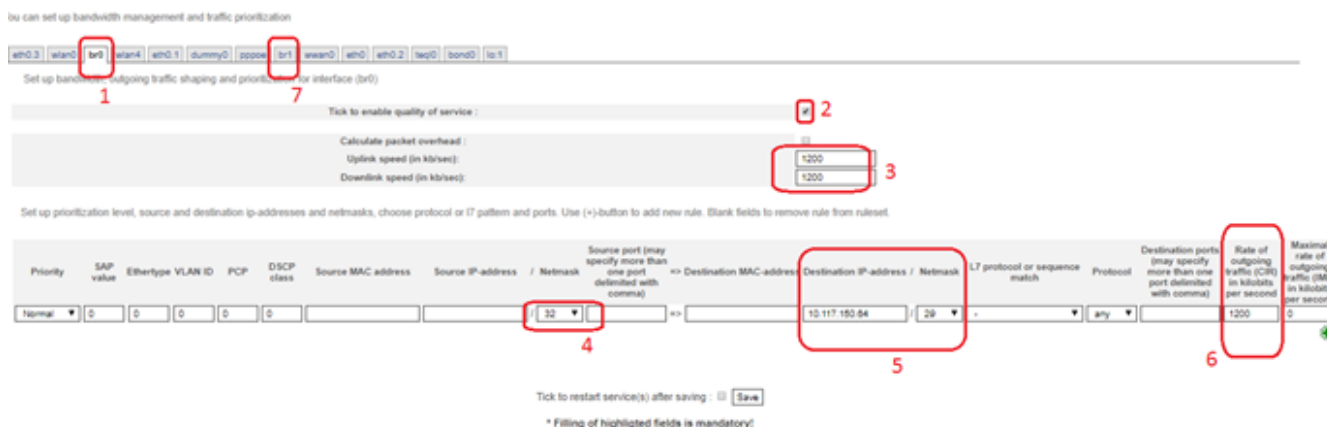
===== QoS и Bandwidth политики ===== Следующий пример демонстрирует ограничение полосы пропускания для пользователей. В нем будет ограничена подсеть LAN или отдельные адреса LAN в использовании Интернет. ===== Создание политики QoS ===== Выберите пункт меню 'Network→Bandwidth Management and Traffic

Prioritization'.



Затем выберите вкладку с интерфейсом 'br0', соответствующую LAN подсети, и сделайте следующие действия: - включите QoS, - (в данном случае) настройте значения upload/download равными 1200 Kbps, - Назначьте destination subnet адрес и маску, соответствующие для 'br0', в правиле QoS, - Задайте CIR как максимально разрешенный для интерфейса. Внимание! * Правила QoS применимы только для исходящего трафика. Правила QoS третьего уровня (L3) оперируют IP-адресами источника и назначения. Правила QoS второго уровня (L2) оперируют номерами IP протоколов, номерами VLAN и MAC адресами.

*



Перейдите на вкладку 'br1' (в данном примере это вторая подсеть LAN). Повторите действия как для 'br0' и выставьте CIR равным 800 Kbps. Установите IP адрес интерфейса 'br1' как адрес назначения.

Control Center-5.1 | Bandwidth: x +

Not secure | 10.117.150.65:5556/app/cp/index.php?q=core.qos.config

System Network Routes Services Utilities Diagnostic

you can set up bandwidth management and traffic prioritization

eth0.3 wlan0 br0 wlan4 eth0.1 dummy0 **pppoe** br1 wwan0 eth0 eth0.2 teg0 bond0 lo.1

Set up bandwidth, outgoing traffic shaping and prioritization for interface (br1)

Tick to enable quality of service : ☒ 8

Calculate packet overhead : ☐

Uplink speed (in kb/sec): 800 9

Downlink speed (in kb/sec): 800

Set up prioritization level, source and destination ip-addresses and netmasks, choose protocol or I7 pattern and ports. Use (+)-button to add new rule. Blank fields to remove rule from ruleset.

Priority	SAP value	Ethertype	VLAN ID	PCP	DSCP class	Source MAC address	Source IP-address / Netmask	Source port (may specify more than one port delimited with comma)	=> Destination MAC-address	Destination IP-address / Netmask	L7 protocol or sequence match	Protocol	Destination ports (may specify more than one port delimited with comma)	Rate of outgoing traffic (CIR) in kilobits per second	Maximal rate of outgoing traffic (IMR) in kilobits per second
Normal	0	0	0	0	0		32			192.168.0	24	-	any	800	0

Затем перейдите на вкладку 'PPPoE' (WAN). Включите QoS на интерфейсе PPPoE и создайте два потока для двух LAN сетей как показано на картинке ниже:

you can set up bandwidth management and traffic prioritization

eth0.3 wlan0 br0 wlan4 eth0.1 dummy0 **pppoe** br1 wwan0 eth0 eth0.2 teg0 bond0 lo.1

Set up bandwidth, outgoing traffic shaping and prioritization for interface (pppoe)

Tick to enable quality of service : ☒ 14

Calculate packet overhead : ☐

Uplink speed (in kb/sec): 2000 15

Downlink speed (in kb/sec): 2000

Set up prioritization level, source and destination ip-addresses and netmasks, choose protocol or I7 pattern and ports. Use (+)-button to add new rule. Blank fields to remove rule from ruleset.

Priority	SAP value	Ethertype	VLAN ID	PCP	DSCP class	Source MAC address	Source IP-address / Netmask	Source port (may specify more than one port delimited with comma)	=> Destination MAC-address	Destination IP-address / Netmask	L7 protocol or sequence match	Protocol	Destination ports (may specify more than one port delimited with comma)	Rate of outgoing traffic (CIR) in kilobits per second	Maximal rate of outgoing traffic (IMR) in kilobits per second
Normal	0	0	0	0	0		10.117.150.64	29			-	any		1200	1200
Normal	0	0	0	0	0		192.168.168.0	24			-	any		800	800

Tick to restart service(s) after saving : ☒ Save 20

* Filling of highlighted fields is mandatory!

===== Правила сетевого экрана для изолирования трафика двух LAN ===== Сетевой экран нужен, чтобы изолировать трафик одной LAN подсети от другой. Настройте их в пункте 'Network→Firewall' на вкладке LAN.

Base settings **Lan** Wan Dmz lan2

Default policy : Incoming traffic: Accept Outgoing traffic: Accept Forwarding traffic: Accept

What is to be done with forwarding to other zones traffic : Tick to fix MSS for transit packets (Enabling this option can decrease performance)

Zone	Tick to do NAT
Wan	☒
Dmz	☐
lan2	☐

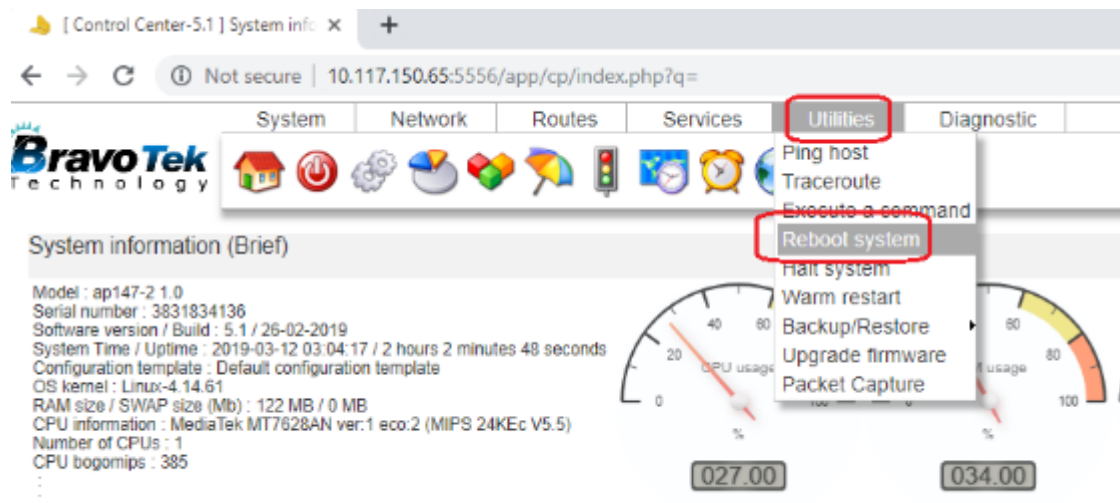
Advanced ruleset for zone. Clear up fields SOURCE, DESTINATION and PORT to remove rule from ruleset. Use '+'-button to add a new rule. :

Select a match to application or content (L7)	Select a match to the type of peer-to-peer traffic	Protocol	Source MAC	Source network or host / Netmask	=> Destination network or host / Netmask	Destination port	Traffic target	#	Description for rule
-	-	any		10.117.150.64 / 29	=> 192.168.168.0 / 24		Drop		
-	-	any		192.168.168.0 / 24	=> 10.117.150.64 / 29		Drop		

Rules to redirect incoming traffic to do port-forwarding. Clear up input boxes to remove row from ruleset. Use '+'-button to add a new row. :

Protocol	External IP-address (may be blank)	External port or portrange delimited by '-' (port1-port2)	=> Internal address	Internal port or portrange delimited by '-' (port1-port2)	#	Description for rule

Перезагрузите маршрутизатор через пункт 'Utilities→Reboot system'. После перезагрузки проверьте скорость скачивания/загрузки для обеих LAN сетей.



=====

Настройка нескольких беспроводных интерфейсов (SSID) ===== Внимание! *

Маршрутизатор поддерживает до 4х физических радиомодулей. 'wlan0' соответствует первому физическому радио, 'wlan1' – второму и т.д.

Каждый радиомодуль поддерживает до 4х интерфейсов. Учитывая четыре радиомодуля, нумерация интерфейсов одного модуля должна быть через 4, т.е.

'wlan0', 'wlan4', 'wlan8', 'wlan12' для первого модуля, 'wlan1', 'wlan5', 'wlan9', 'wlan13' для второго и т.д.

*** Физическое радио имеет ряд ограничений: - Одно устройство не может быть WDS точкой доступа и WDS клиентом. - На маршрутизаторе не может быть более одного AD-Нос. - Все интерфейсы одного радиомодуля должны работать на одной частоте (канале). Если пользователь имеет разнородный и сложный Wi-Fi проект, то крайне рекомендовано узнать полный список подобных ограничений от службы поддержки ООО «Нетше лаб». 'wlan0' беспроводной LAN интерфейс по умолчанию. Ему соответствует первый SSID по умолчанию. Помня правила нумерации, следующий новый интерфейс будет 'wlan4'. Номера каналов, их ширина и т.д. должны быть одинаковыми для всех SSID одного модуля. Но можно таким интерфейсам задавать разные типы шифрования и разные пароли для каждого SSID. ===== Создание нового беспроводного интерфейса ===== На домашней странице найдите пункт 'Network→Interface', прокрутите страницу вниз. Введите имя 'wlan4' и нажмите рядом кнопку 'New'.**

The screenshot displays the configuration interface of the NETSHe BR104. At the top, there is a navigation bar with tabs: System, Network, Routes, Services, Utilities, and Diagnostic. Below the tabs is a row of icons representing various system functions. The main content area is divided into two sections. The left section shows network statistics for a specific interface, including IPv6 address, MAC address, received and transmitted bytes and packets, errors, drops, and input/output speeds. The right section shows a graph of network traffic over time. Below the statistics, there is a form to add a new interface. The form has a label 'Input name of interface to add' and a text input field containing 'wlan4'. A 'New' button is next to the input field. The form is highlighted with a pink background. The number '1' is placed above the input field, and the number '2' is placed below the 'New' button.

IPv6: fe80::213:4bff:fe70:1d9
MAC: 00:13:4b:70:01:d9
Received bytes: 16024732
Received packets: 19421
Errors on receive: 0
Drops on receive: 6
Transmitted bytes: 1855157
Transmitted packets: 10240
Errors on transmit: 0
Drops on transmit: 0
Drops: 0
Input speed (kb/s): 29
Output speed (kb/s): 60

(You can use names like ethX.Y for VLANs, names like br* for bridges, pppX for PPP interfaces)

Input name of interface to add

=====

Задание нового SSID ===== Откроется диалог параметров беспроводного интерфейса. Перейдите на вкладку 'Wireless' и задайте режим, SSID, выберите модуляцию и канал в соответствующих полях, как показано на картинке ниже:

← → ↻ ⓘ Not secure | 10.117.150.65:5556/app/cp/index.php?q=core.radio.cfg&ifname=wlan4

System Network Routes Services Utilities Diagnostic

Enable interface : ☒

Wireless Wireless Security Wireless Multimedia (QoS) Settings Fast roaming, Interworking and Hotspot 2.0 Additional IP settings

Interface is a member of bridge: **br1** Assign this SSID to appropriate Bridge group

Mode: * Access Point / Mesh gateway

ESSID: * **Sub24** New SSID name

Country Code: IN

Modulation: 802.11n

Channel width: 20MHz

Current frequency: 2412

Transmitter power in dBm: 0

These settings must be same as they are under WLAN0 interface

Save

Перейдите на вкладку 'Wireless security' и назначьте тип шифрования и пароль, нажмите на кнопку 'Save', по окончании всех настроек перезагрузите маршрутизатор.

Wireless **Wireless Security** Wireless Multimedia (QoS) Settings Fast roaming, Interworking and Hotspot 2.0 Additional IP settings

Hide ESSID ? : ☐

Isolate clients ? : ☐

Limit number of connections ('0' for unlimited): 0

Encryption: **WPA2 (Personal)**

Disable TKIP: ☐

Username:

Password, Encryption key or network passphrase: **1234567890**

Allow connections to next MAC-addresses (comma separated list):

Deny connections from next MAC-addresses (comma separated list):

Certificate of Authority for Wireless network : Not installed

Client Certificate : Not installed

Private key : Not installed

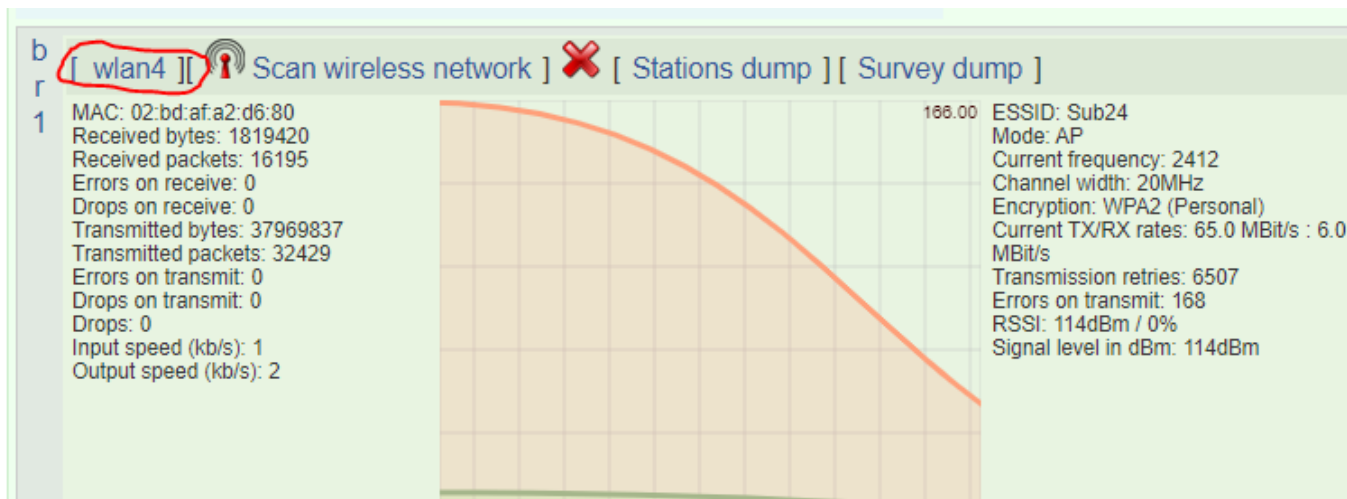
Choose file No file chosen

Choose file No file chosen

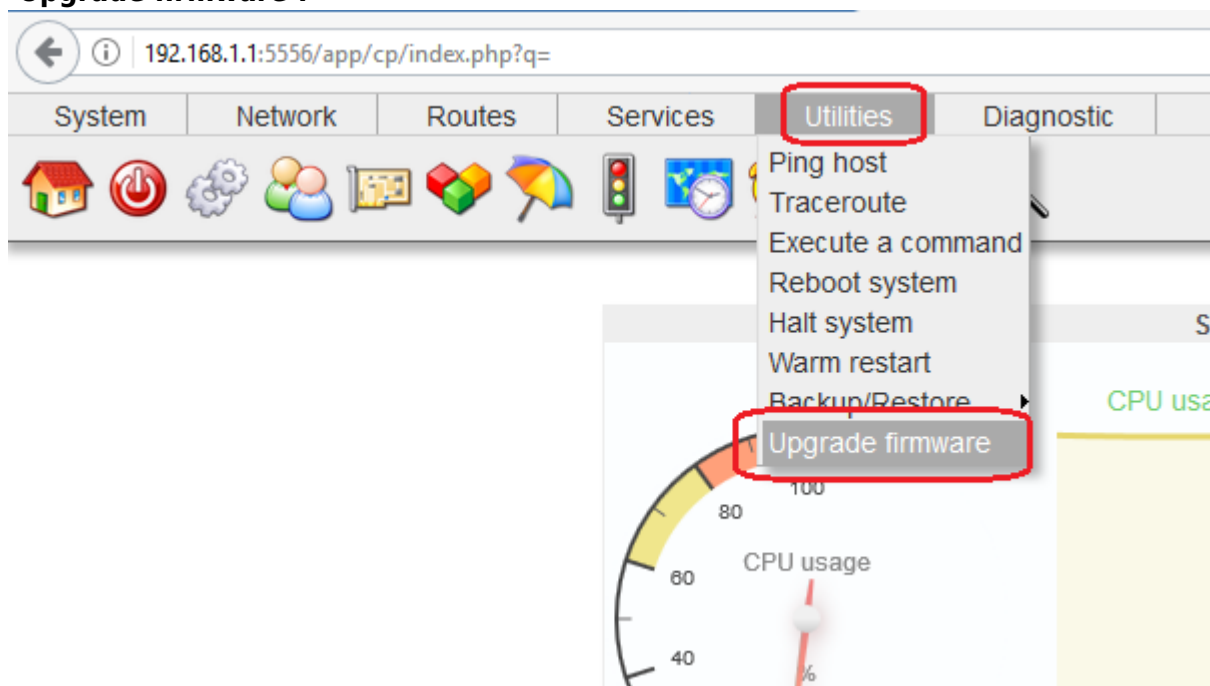
Choose file No file chosen

Save

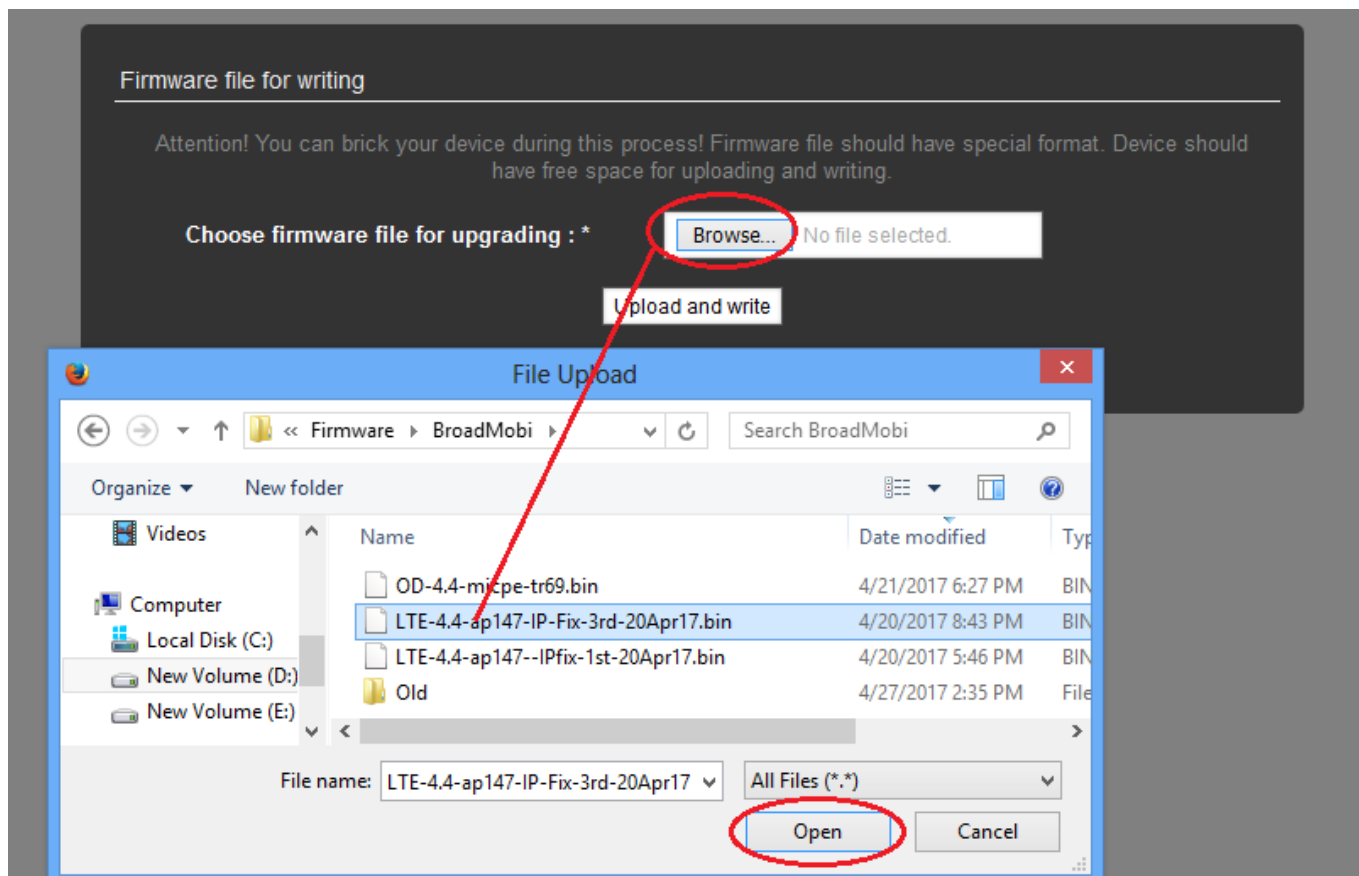
Когда маршрутизатор перезагрузится, пользователь сможет увидеть новый интерфейс в списке интерфейсов на домашней странице.



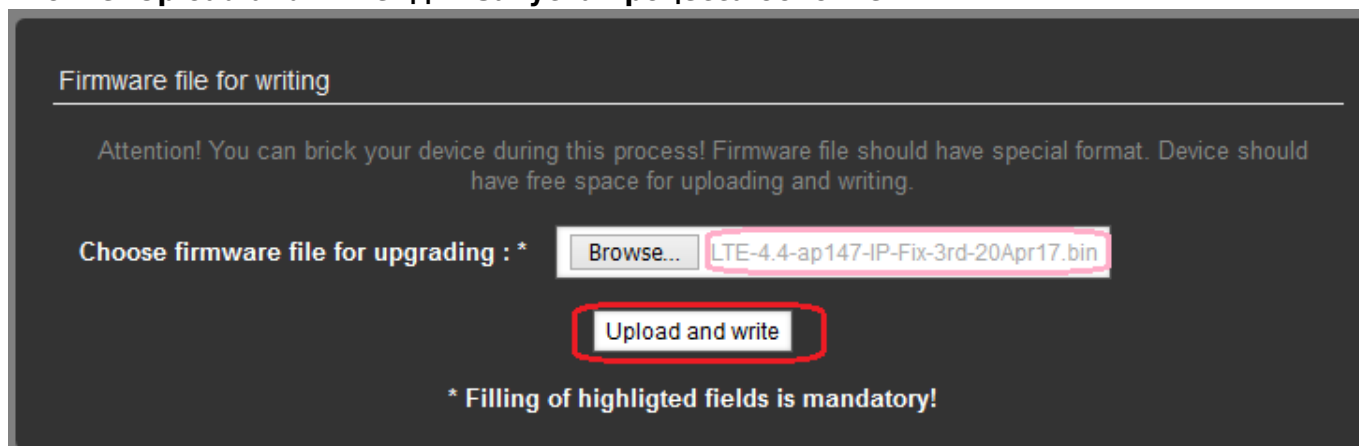
===== Как обновить встроенное ПО ===== Выберите меню 'Utilities' и строку 'Upgrade firmware'.



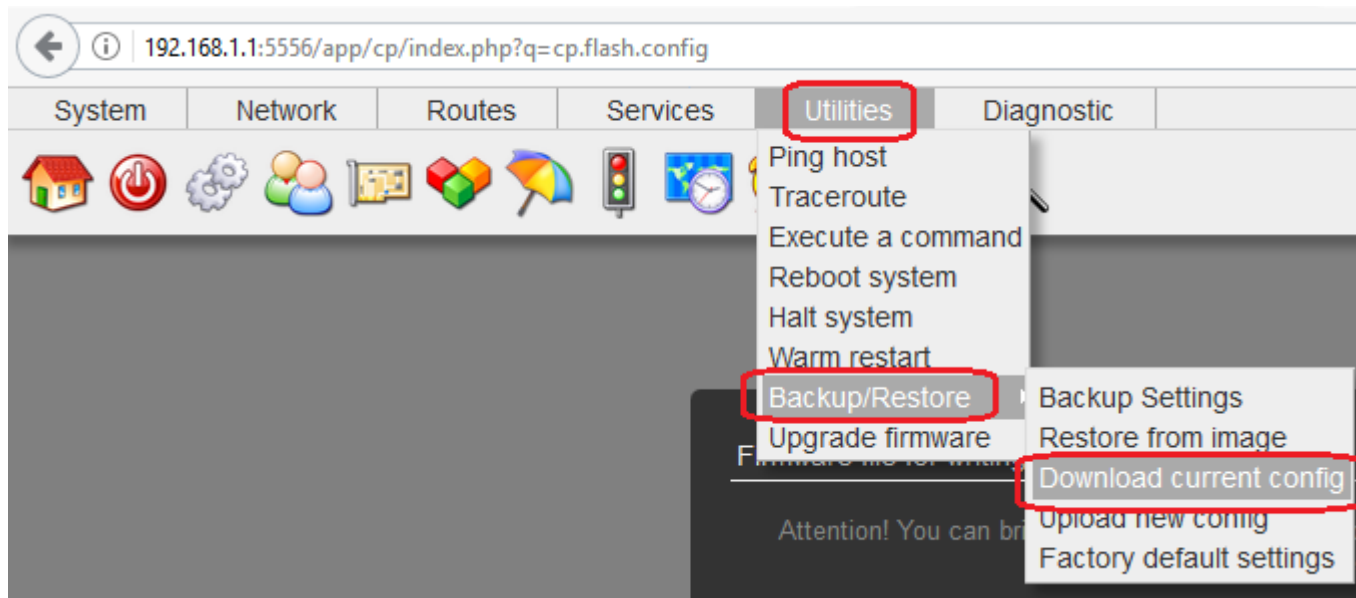
На следующем диалоге щелкните на кнопке 'Browse' и в диалоге открытия файла выберите *.bin файл с локального компьютера или из папки в сетевом окружении.



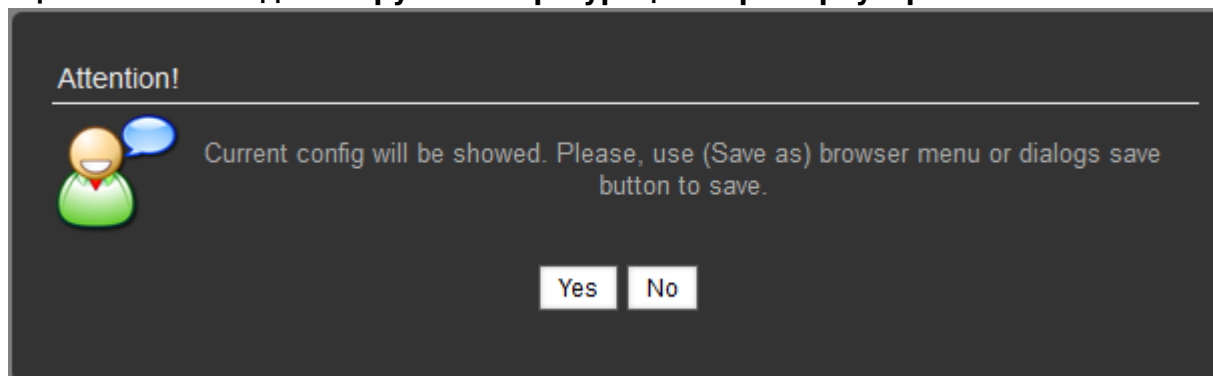
Как только подходящий файл выбран, он будет показан в диалоге. Щелкните на кнопке 'Upload and write' для запуска процесса обновления.



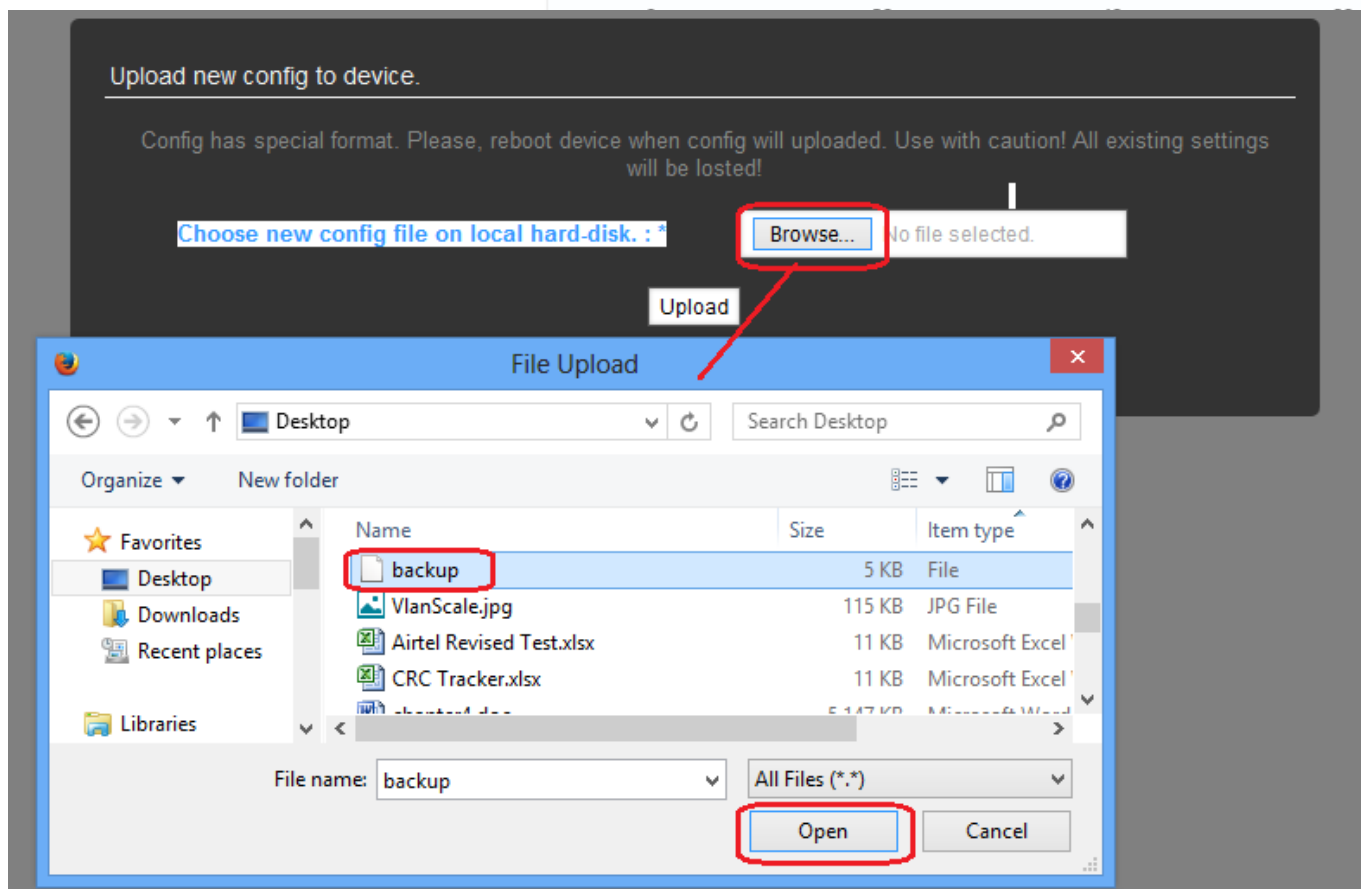
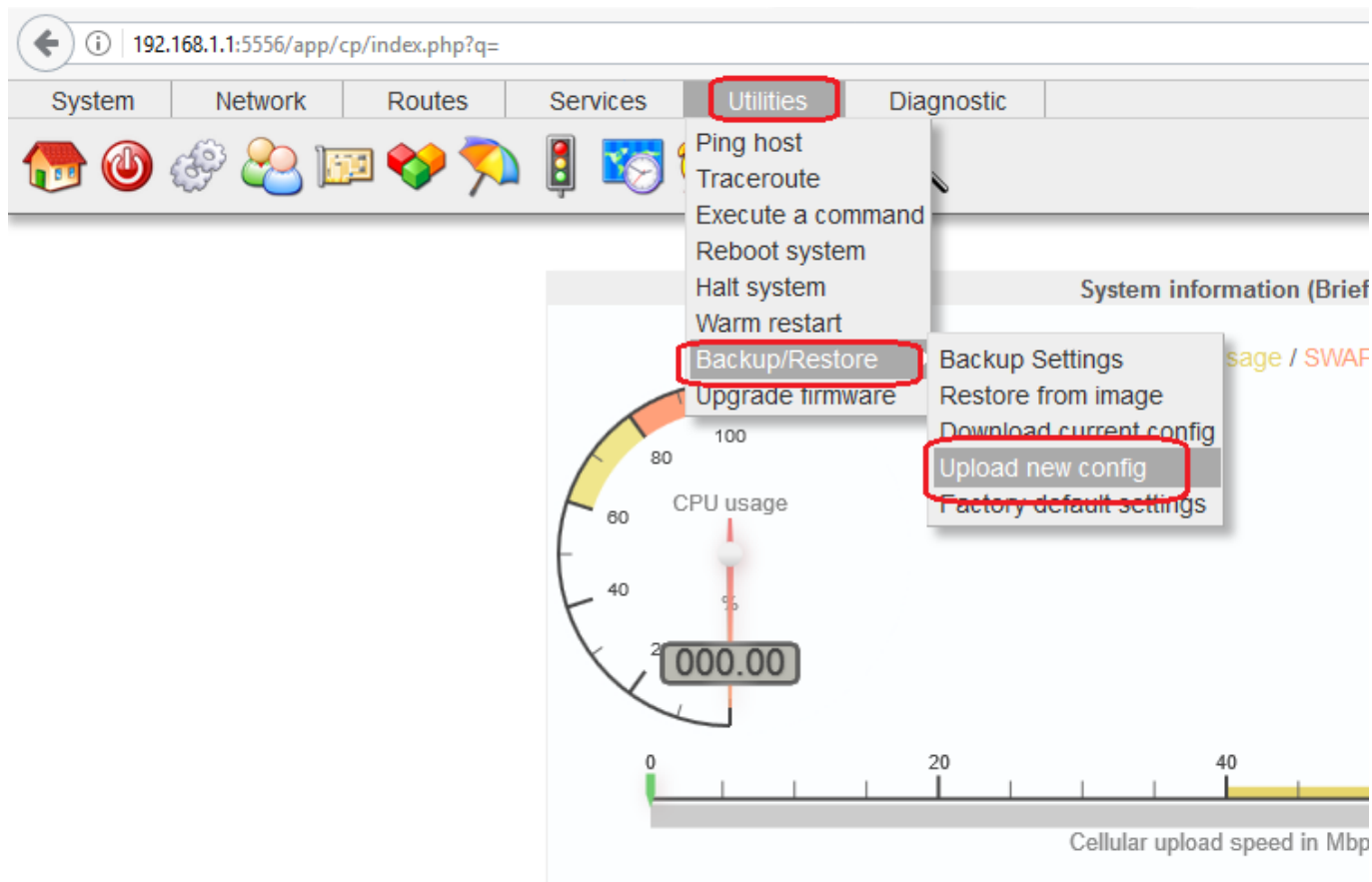
Файл *.bin будет загружен на флэш-карту маршрутизатора. Система проверит MD5 хэш файла и сравнит существующую и новую версии/билды. Если версия/билд нового программного обеспечения старше существующих, и программное обеспечение соответствует модели устройства, то процесс обновления будет запущен, после него маршрутизатор перезапустится. - Обновление и перезагрузка займут около 5 минут. Не нужно выключать питание маршрутизатора и не нужно форсировать соединение до истечения этого времени. - Процесс обновления встроенного ПО не стирает конфигурацию устройства. После перезагрузки пользователь сможет присоединиться к маршрутизатору со старыми учетными данными на прежний IP-адрес. =====
Сохранение и восстановление конфигурации ===== Выберите пункт меню 'Utilities→Backup/Restore→Download current config'



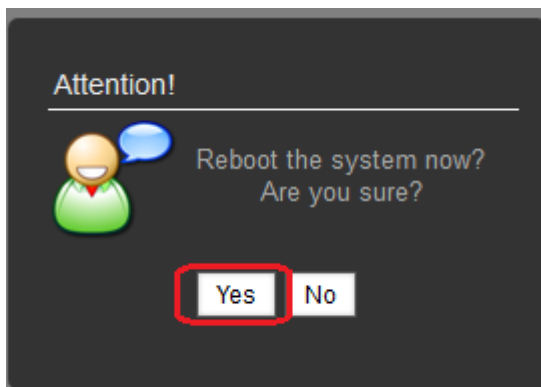
Щелкните 'Yes' для загрузки конфигурации через браузер.



Index.php файл будет загружен в папку для загрузок, заданную в браузере. Потом пользователь может переименовать файл конфигурации, дав понятное имя с указанием даты, чтоб потом можно было этот файл распознать среди многих таких же в процессе эксплуатации. После того, как файл получен, можно нажать 'No' для возврата на домашнюю страницу. Аналогично восстановить сохраненную ранее конфигурацию можно через пункт меню 'Utilities→Backup/Restore→Upload new config'.

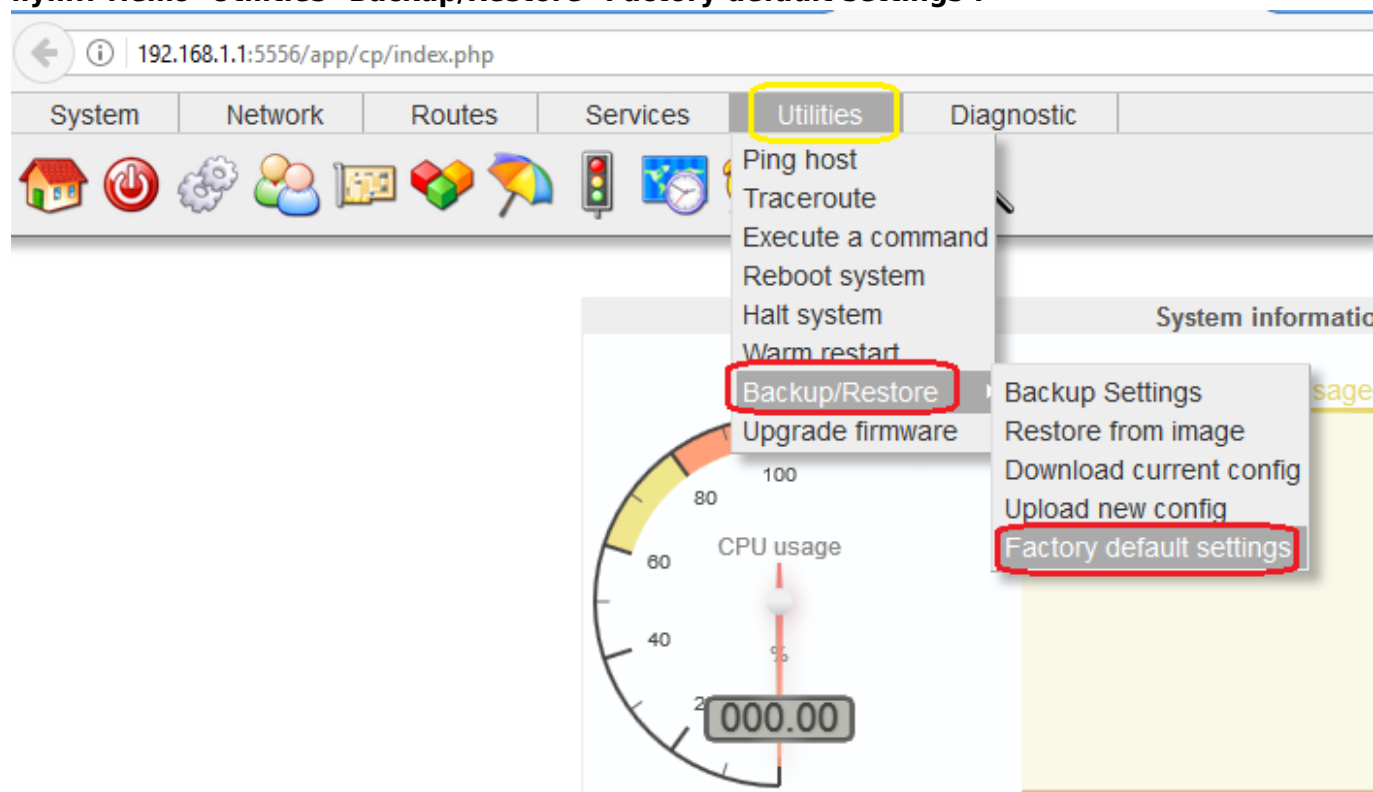


После выбора файла следует нажать 'Upload', а затем 'Yes' на предложение

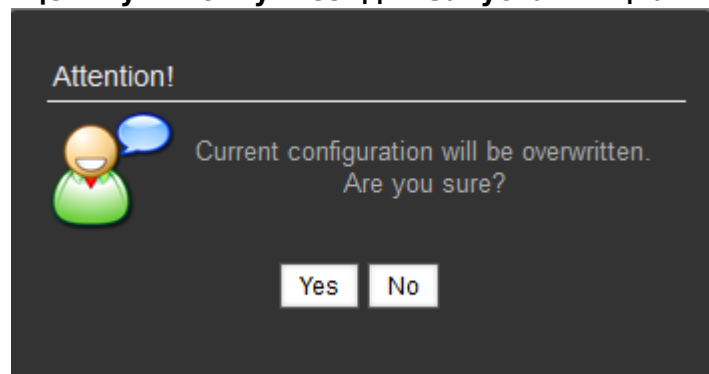


перезагрузить маршрутизатор.

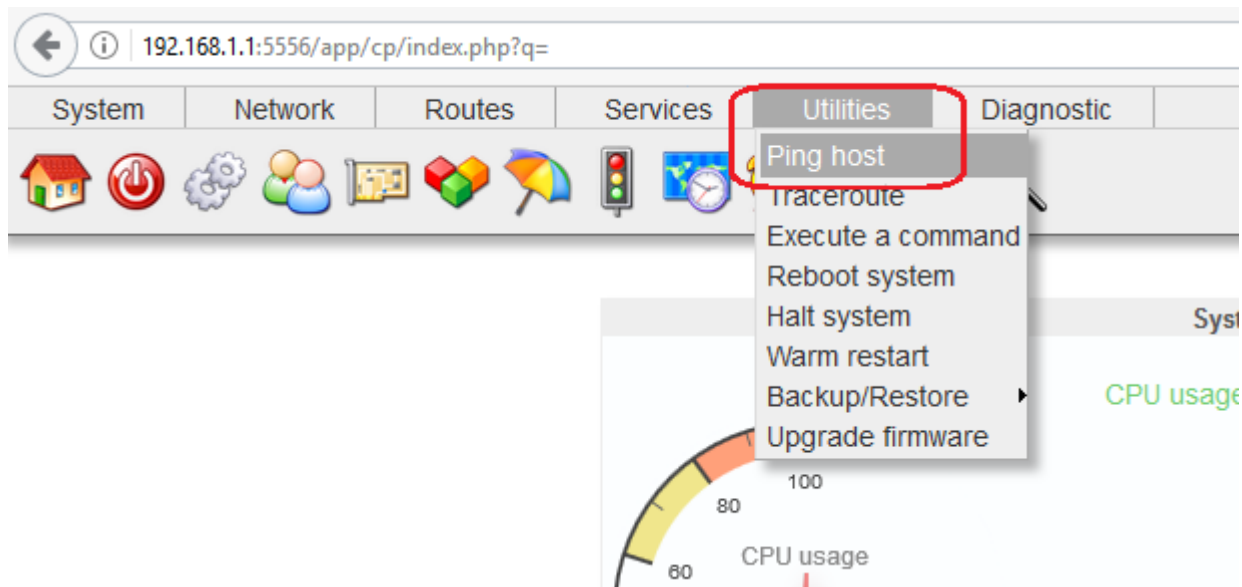
==== Сброс к заводским настройкам ==== Пользователь может вернуть заводские настройки маршрутизатору, нажав кнопку 'RST' на корпусе и отпустив ее после мигания индикаторов. Возможно, для нажатия потребуется острый предмет типа иголки. Так же пользователь может сбросить настройки маршрутизатору через Web GUI, выбрав пункт меню 'Utilities→Backup/Restore→Factory default settings'.



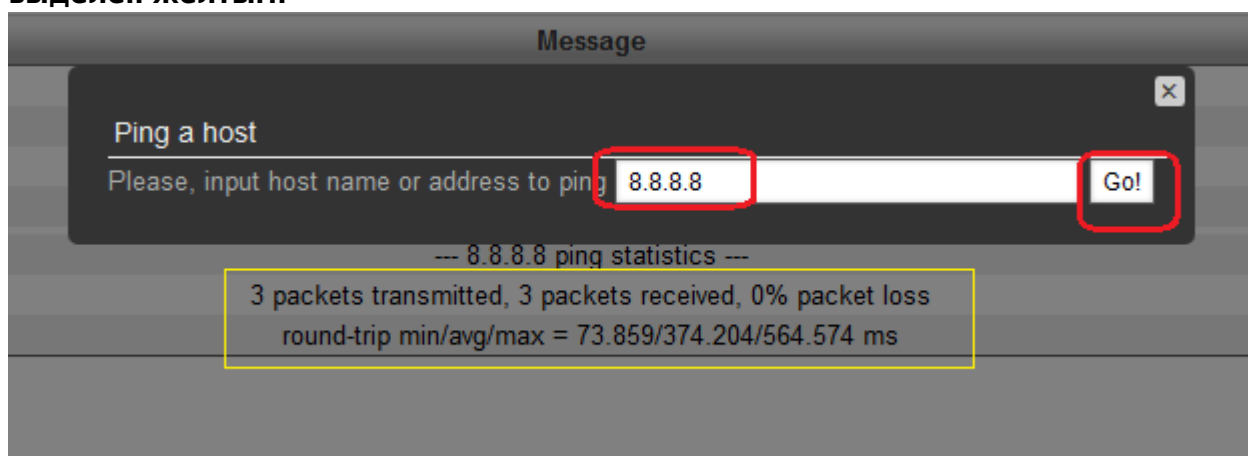
Щелкнув кнопку 'Yes' для запуска инициализации.



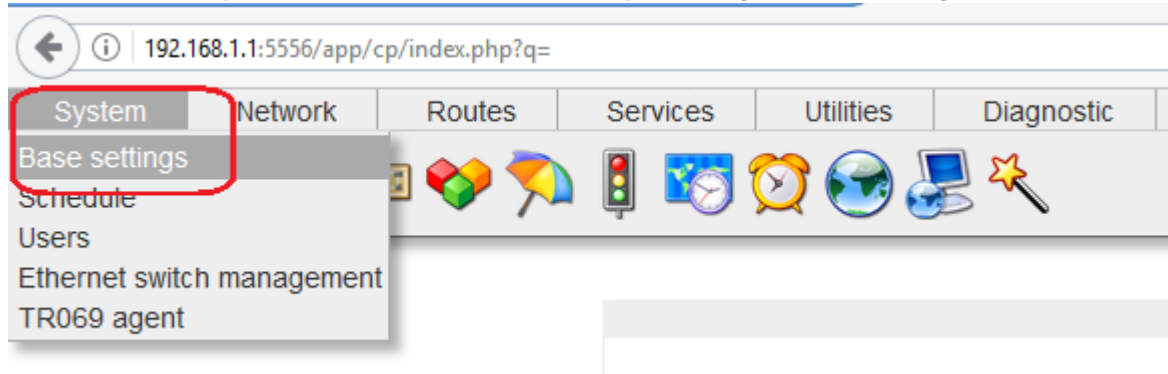
Около трех минут займет сброс и перезагрузка. После успешной загрузки маршрутизатора пользователь сможет зайти уже на IP адрес, с именем и паролем по умолчанию. ==== Использование ping из веб-интерфейса ==== Выберите пункт 'Utilities→Ping host'.



Введите IP-адрес или имя хоста назначения ICMP пакетов и щелкните кнопку 'Go!'. Результат ping будет отображаться под диалогом, как на картинке снизу, результат выделен желтым.



===== Настройки Telnet ===== Откройте пункт меню 'System→Base setting'.



Пользователю нужно перейти на вкладку 'Remote access', разрешить telnet в соответствующей секции и задать порт 23 или любой желаемый. Telnet и SSH доступ принимают root/root в качестве логина и пароля по умолчанию.

Basic settings | RADIUS client setup | Upstream proxy | **Remote access**

Web-interface settings

Interfaces to listen on :

All interfaces:

- br0: ☒
- wwan0: ☐
- eth1: ☐
- dummy0: ☐
- pppoe: ☐
- eth0: ☐
- tunipsec0: ☐
- pptp: ☐
- l2tp: ☐
- cellular: ☐

Port : 5556

Telnet access settings

Tick to enable telnet access (very insecure. Avoid using) : ☒

Port : 23

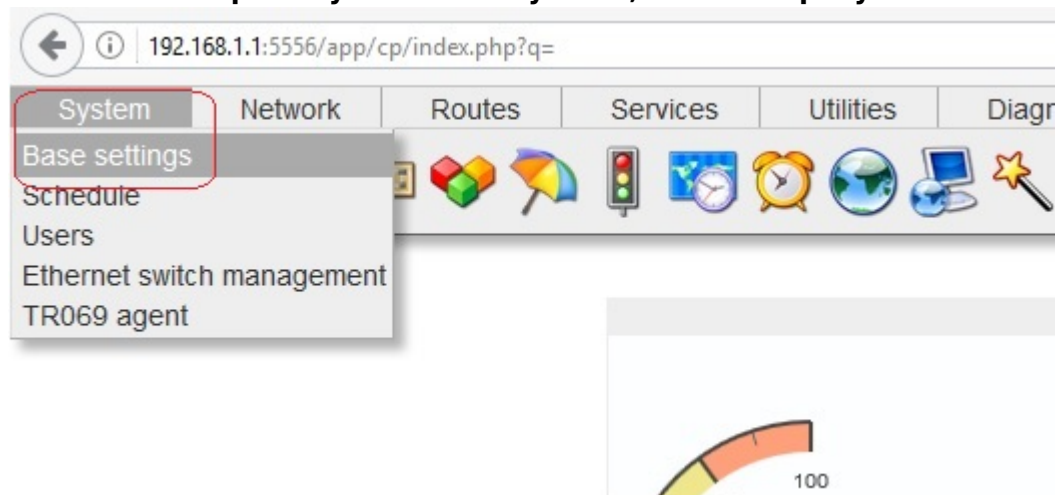
Secure shell (SSH) access settings

Tick to enable SSH access : ☒

Port : 22

Tick to restart service(s) after saving : ☐ **Save**

===== Удаленный доступ со стороны WAN интерфейса
 ===== Выберите пункт меню 'System', а в нем строку 'Base settings'.



Когда откроется страница 'Base setting', пользователю следует выбрать вкладку 'Remote Setting'. На вкладке выбрать опцию 'All interfaces' и щелкнуть кнопку 'Save' внизу.

Web-interface settings

Upstream proxy Remote access

To access device from WAN or Outside use the following setting.

Interfaces to listen on :

All interfaces: ☒ eth0: ☐ eth1: ☐ br0: ☐ tunipsec0: ☐ pppoe: ☐ pptp: ☐ l2tp: ☐ wwan0: ☐ ppp102: ☐ dummy0: ☐

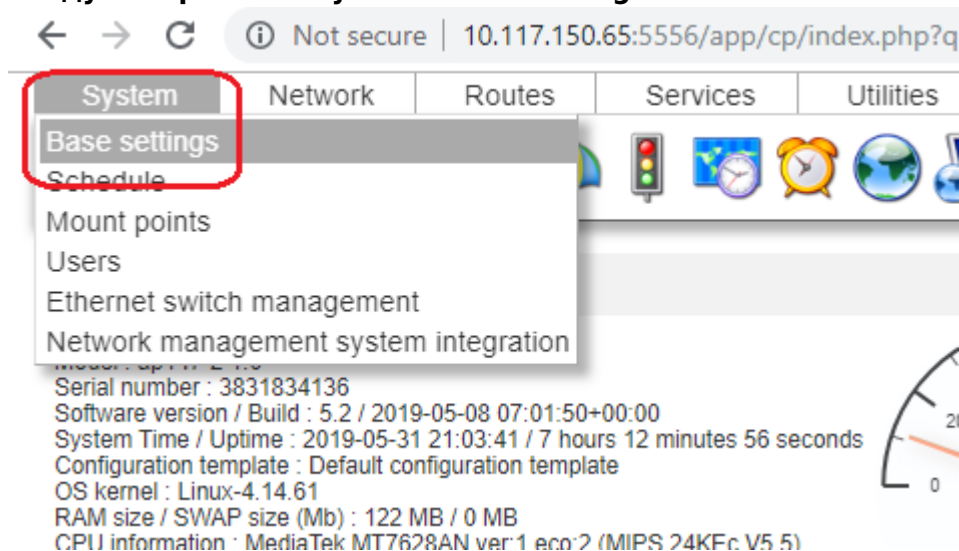
Port : 5556

Tick to restart service(s) after saving: ☐ Save

Внимание! * Из соображений безопасности удаленный доступ закрыт по умолчанию со стороны WAN маршрутизатора. С настройками, показанными выше, устройство будет доступно с любой стороны. Рекомендовано это делать с осторожностью.

Не следует забывать о настройках сетевого экрана для приема соединений удаленного доступа на все нужные интерфейсы.

* ===== Настройки Syslog ===== По умолчанию журнал syslog хранится локально в @/var/log/messages. Для того, чтобы настроить хранение на удаленном сервере, следует перейти в 'System→Base settings'.



Выбрать вкладку 'Basic settings' и заменить путь для хранения путем с IP-адресом внешнего сервера, как показано ниже.

Basic settings
RADIUS client setup
Upstream proxy
Remote access

Hostname: *
netshe

Disable ip routing on the device (Enable L2/bridging mode only) :
☐

Syslog settings: logging program, destination, etc.

Syslog server or filename: *
10.117.150.67

Port of remote syslog server (usually 514): *
514

Logging level: *
6

Log buffer size: *
100

Tick to restart service(s) after saving: ☒ Save

Содержимое журналов можно посмотреть в пунктах меню 'Diagnostic→Log→System' или 'Hardware'. Оно выглядит примерно, как показано на этом рисунке.

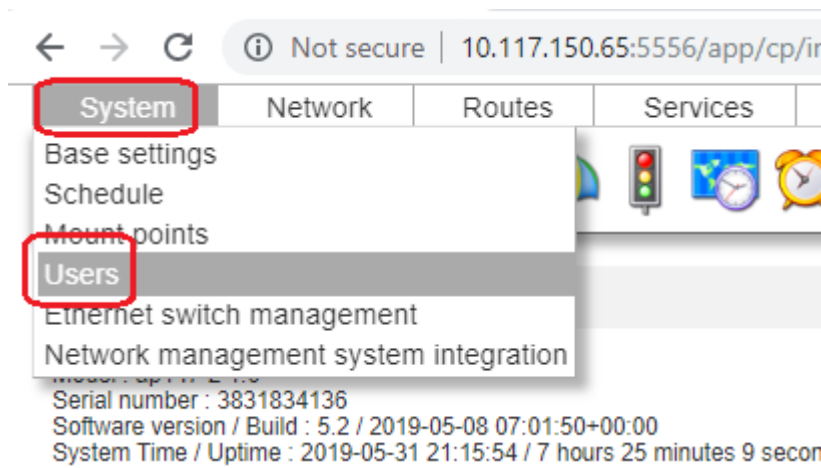
```

May 31 15:25:41 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:25:44 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:25:45 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:25:46 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:25:47 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:30:21 (none) user.notice event: /opt/stasoft/bin/.events/link/010restart_wan.sh down
May 31 15:30:21 (none) user.notice event: /opt/stasoft/bin/.events/link/down/md_wrapper.sh
May 31 15:30:21 (none) user.notice event: /opt/stasoft/bin/.events/link/010restart_wan.sh down
May 31 15:30:21 (none) user.notice event: /opt/stasoft/bin/.events/link/down/md_wrapper.sh
May 31 15:35:11 (none) user.notice event: /opt/stasoft/bin/.events/link/010restart_wan.sh down
May 31 15:35:11 (none) user.notice event: /opt/stasoft/bin/.events/link/down/md_wrapper.sh
May 31 15:36:11 (none) user.notice event: /opt/stasoft/bin/.events/link/010restart_wan.sh down
May 31 15:36:11 (none) user.notice event: /opt/stasoft/bin/.events/link/down/md_wrapper.sh
May 31 15:40:11 (none) user.notice event: /opt/stasoft/bin/.events/link/010restart_wan.sh down
May 31 15:40:11 (none) user.notice event: /opt/stasoft/bin/.events/link/down/md_wrapper.sh
May 31 15:42:12 (none) user.notice event: /opt/stasoft/bin/.events/link/010restart_wan.sh down
May 31 15:42:12 (none) user.notice event: /opt/stasoft/bin/.events/link/down/md_wrapper.sh
May 31 15:43:23 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:43:24 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:43:25 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:43:26 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:43:47 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:43:48 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:43:49 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:43:50 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:44:07 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:44:08 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:44:09 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba
May 31 15:44:10 (none) user.notice HOSTAPD: Event AP-STA-POSSIBLE-PSK-MISMATCH for wlan0 with param 58:db:15:db:17:ba

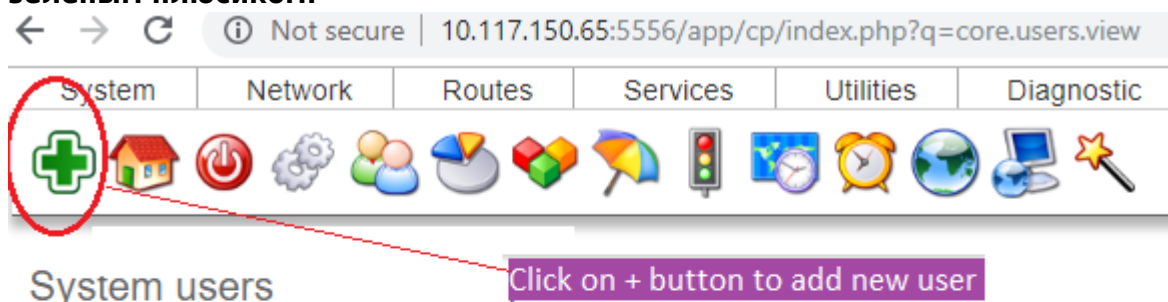
```

===== Локальные пользователи =====

Эти учетные записи пользователей применяются для аутентификации в процессе управления устройством или мониторинга. Чтоб найти список пользователей, нужно пройти в пункт меню 'System→Users'.



Откроется список учетных записей пользователей. Чтоб создать новую запись, нужно нажать на иконку с зеленым плюсиком.



You can manage system users here. Add, edit change password or delete.

Username	Password
root	\$1\$J34F3oJP\$O6U/Mp6w6xj0FIkfVrYtS
daemon	
ftp	
network	
nobody	
superuser	\$1\$P7RZZw7\$ueyzJmvGYyQUTvj2Tmfz

Что создать пользователя с ограниченными правами, достаточно указать только имя и пароль.

Add new user

Empty shells (/bin/false, /bin/nologin) permit readonly web-access. Leave [password] field blank, if you do not want to change it. Fill in [home] and [group] fields only if you are sure what you are doing

Username:	support
Password:	
Confirm password:	
Group:	
Home dir:	
Shell:	/bin/false

Save

* Filling of highlighted fields is mandatory!

For read only user only provide username and password only.

Список пользователей по умолчанию показан ниже:

System users

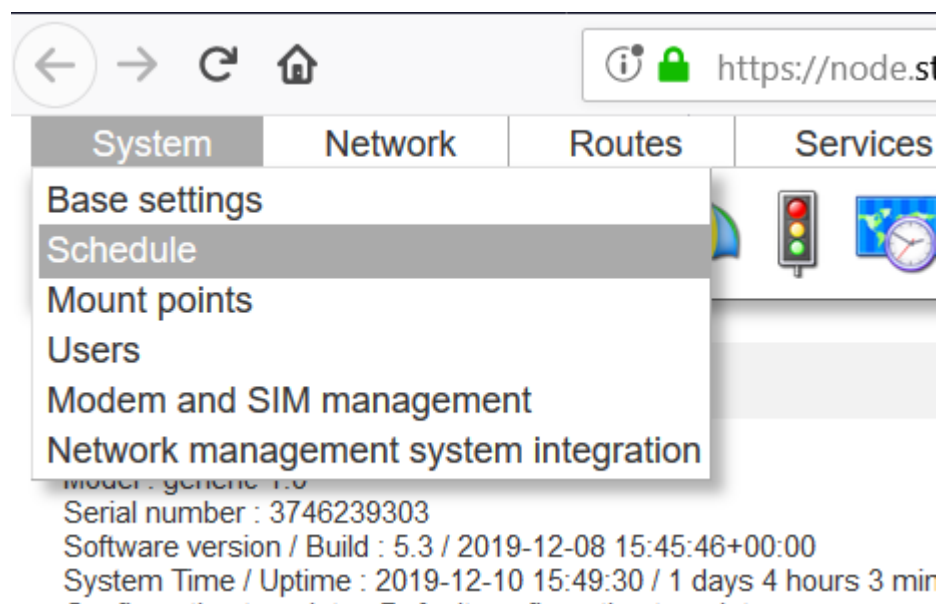
You can manage system users here. Add, edit change password or delete.

Username	Password	Group	Home dir	Shell	Options
root	\$1\$J34F3oJP\$O6U/Mp6w6xj0FIkVrYTS/	root	/root	/bin/ash	
daemon		daemon	/var		
ftp		ftp	/home/ftp		
network		network	/var		
nobody		nogroup	/var		
superuser	\$1\$pf7RZZw7\$ueyzJmvGYyQUTvj2TmfzQ/	root	/var		
test	\$1\$Qrt1fKJ4\$hPzmP3sDL5Or29.RYpZbb.	test	/home/test		

Для того, чтобы изменить пароль пользователя, нужно щелкнуть на иконку в виде пера справа от имени пользователя, заменить пароль и сохранить изменения. Чтоб удалить учетную запись пользователя, необходимо щелкнуть по красному крестику справа от имени пользователя. **Внимание!** * Никогда не пытайтесь удалить системные учетные записи 'superuser' и 'root'. Да система и не позволит этого сделать.

Расписание задач устройства

Устройство может выполнять определенные запланированные действия. Расписание этих действий можно найти в пункте меню 'System→Schedule'.



Обычное расписание выглядит как список на следующей картинке:

System
Network
Routes
Services
Utilities
Diagnostic

Please, specify actual set of schedules or clear up input boxes to remove schedule from settings. Use '+'-button to add a new schedule.
Put data with the following format: minutes, hours, days, months, years, command and comments.
'5' in a 'minute' field means that scheduled task is will executed at 5 minutes past every hour. '*/5' means that sheduled task is to be executed every 5 minutes. At least one 'time' field should not contain "" sign.

To be run correctly, schedule for application must be configured properly, for example: 2 4 * * * /opt/stasoft/bin/backup.php
*/5 * * * * /opt/stasoft/usr/bin/rad_maint_5min.sh, 10 1 * * * /opt/stasoft/usr/bin/rad_maint_daily.sh

	Minutes (0-59)	Hour (0-23)	Day (1-31)	Month (1-12)	Day of week (0 or 7 - Sunday, 1-6)	Command to execute	Description
Schedules :	*/5	*	*	*	*	/app/suite/tmp/spool/rm/169.254.0.6/?/opt/sl	
	15	*/4	*	*	*	/app/suite/tmp/spool/rm/169.254.0.6/?/opt/sl	
	*/30	*	*	*	*	/app/suite/tmp/spool/rm/169.254.0.6/?/opt/sl	
	40	3	*	*	*	/app/suite/tmp/spool/rm/169.254.0.6/?/opt/sl	
	*/5	*	*	*	*	/app/suite/tmp/spool/rm/169.254.0.6/?/opt/sl	

+

Save

Формат строк расписания описан тут же на странице настройки расписания. Любая задача может быть выполнена либо с интервалом, либо по часам/минутам.

Регистрация на NMMS

Находится в меню 'System→Network management system integration'.

Index of /share/in/tr069
[Control Center-5.1] System info

← → ↻ ⓘ Not secure | 10.117.150.65:5556/app/cp/index.php?q=

System
Network
Routes
Services
Utilities

Base settings
Schedule
Mount points
Ethernet switch management
Network management system integration

Model : br104 1.0
Serial number : 4186018271
Software version / Build : 5.1 / 2018-12-11 15:21:34+00:00
System Time / Uptime : 2018-12-11 22:19:54 / 24 minutes 12 seconds
Configuration template : Default configuration template
OS kernel : Linux-4.14.61
RAM size / SWAP size (Mb) : 122 MB / 0 MB
CPU information : MediaTek MT7628AN ver:1 eco:2 (MIPS 24KEc V5.5)
Number of CPUs : 1
CPU bogomips : 385

'Network management system' меню включает настройки подключения к NMMS, чтобы устройство было доступно для централизованного контроля и мониторинга. Регистрация на NMMS требует указать имя и пароль. Пользователь может прочитать руководство 'Quick Administration Guide NMMS' для понимания работы в среде NMMS.


https://node.net/app/suite/tmp/spool/rm/169.254.0.6/?/af
90%

System
Network
Routes
Services
Utilities
Diagnostic








Please, setup NMS credentials and device-specific data. You should be registered in NMS and have credentials to access NMS
Network management system helps you to do configuring, monitoring and management of your device

Full specified URI for NMS server : *	https://hc.stasoft.net
Login	xxxxxxxxx
Device/Host name (Serial number 1226942692 will be added automatically) : *	tank_1226942692
Device coordinate: Latitude :	
Device coordinate: Longitude :	
Device description / System location :	
Contact person :	
Contact email :	admin@127.0.0.1

Save data and Register device

* Filling of highlighted fields is mandatory!

Заключение

Маршрутизатор BR104 содержит довольно большой набор свойств, которые в процессе комбинирования превращаются в огромное число вариантов использования маршрутизатора. Все эти варианты сложно описать в одном руководстве, а еще сложнее будет такое руководство читать широкому кругу пользователей.

Поэтому специалисты ООО «Нетше лаб» всегда готовы предложить решение, максимально соответствующее вашей текущей задаче. Наши координаты вы можете найти на сайте <http://www.netshe-lab.ru>

From: <http://docs.netshe-lab.ru/> - Документация по NETShe

Permanent link:

<http://docs.netshe-lab.ru/doku.php?id=%D0%BD%D0%80%D1%81%D1%82%D1%80%D0%BE%D0%89%D0%8A%D0%80%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80%D0%B0> br10

Last update: 2020/07/16 04:52

