



Troubleshooting and Advanced Customer Manual

Host Name:	Huawei
Model Number:	HG8245W5
Firmware Version:	HWTCA51910110
Serial Number:	48575443D150E29D (HWTCD150E29D)

Autor: Adam Husár, Ľuboš Lendáč

Date: 7.11.2019

Version: 2

1 Contents

2	Možné problémy so zariadením Huawei HG8245W5 a ich riešenie.....	3
2.1	Želaný stav	3
2.2	Popis LED kontroliek a možných problémov.....	3
2.3	Nastavenie Wi-Fi	4
2.4	Kontrola fyzického zapojenia	5
2.5	Kontrola pripojenia	7
3	Advanced Customer Manual.....	8
3.1	IPv4.....	8
3.1.1	Static LAN DHCP	8
3.1.2	Port forwarding a DMZ	9
3.2	IPv6.....	12
3.2.1	Port Mapping Configuration	12
3.2.2	IPv6 Firewall Configuration	14
3.2.3	Filter Configuration	14
3.2.4	PCP	16
3.2.5	Zmena prefixu	17
3.2.6	Prístup z WAN	20
3.3	IPv4 and IPv6.....	21
3.3.1	MAC Filter	21
3.3.2	Smart Wi-Fi.....	21
3.3.3	Parental Control	22
3.3.4	Guest Wi-Fi.....	23
3.3.5	Wi-Fi automatic shutdown.....	24
3.3.6	Firewall.....	25
3.3.7	Reštart zariadenia	26
3.3.8	Obnovenie továrenských nastavení.....	27
3.3.9	Zmena prihlasovacieho hesla.....	27
3.3.10	Firewall záznamy.....	28

2 Možné problémy so zariadením Huawei HG8245W5 a ich riešenie

2.1 Želaný stav

Zariadenie Huawei HG8245W5 je funkčné ak svietia LED kontrolky, ktoré sú zelené (POWER a PON). Kontrolky LAN 1-4, TEL1-2, USB, WLAN môžu svietiť alebo blikať v závislosti na tom či je pripojené nejaké zariadenie a či práve komunikuje.

Prvá kontrolka zľava (POWER) indikuje, že je zariadenie zapnuté. Druhá kontrolka (PON) indikuje, že zariadenie je pripojené do optickej siete a užívateľ by mal byť schopný pripojiť sa na internet.

Ak nesvieti (ani neblinká) žiadna kontrolka, užívateľ by mal skontrolovať napájanie a napájacie tlačidlo.



Obrázok 1 Želaný stav

2.2 Popis LED kontroliek a možných problémov

Tabuľka 1.

LED	Popis	Stav kontrolky	Popis stavu	Možné riešenie problému
POWER	Kontrolka zapnutia	Svieti	Zariadenie je zapnuté	
		Nesvieti	Zariadenie je vypnuté	Skontrolujte tlačidlo napájania a napájací kábel.
PON	Autentifikačná LED	Vid' tabuľka 2		
LOS	LED spojenia	Vid' tabuľka 2		
LAN1-4	Kontrolka portov	Stále svieti	Pripojenie je v norme	
		Bliká	Prebieha prenos dát	
		Nesvieti	Pripojenie nie je zostavené	Pripojte počítač k jednému zo štyroch LAN portov
TEL1-2	Kontrolka telefónneho spojenia	Svieti	Zariadenie je pripravené na telefónne spojenie	
		Bliká	Prebieha telefónne spojenie	
		Nesvieti	Pripojenie nie je zostavené	Pripojte telefón k jednému z TEL portov

USB	Kontrolka USB	Svieti	Je pripojené USB zariadenie ale neprebieha prenos dát	
		Bliká	Prebieha prenos dát	
		Nesvieti	Nie je pripojené zariadenie do USB portu	
WLAN	Kontrolka WLAN (Wi-Fi)	Svieti	Funkcia WLAN je zapnutá	
		Bliká	Prenášajú sa dáta	
		Nesvieti	Funkcia WLAN je vypnutá	Kapitola Nastavenie Wi-Fi
WPS	Kontrolka WPS	Svieti	Funkcia WPS je zapnutá	
		Bliká	Terminál Wi-Fi pristupuje k systému	
		Nesvieti	Funkcia WPS je vypnutá	

Tabuľka 2. Popis PON a LOD LED kontroliek

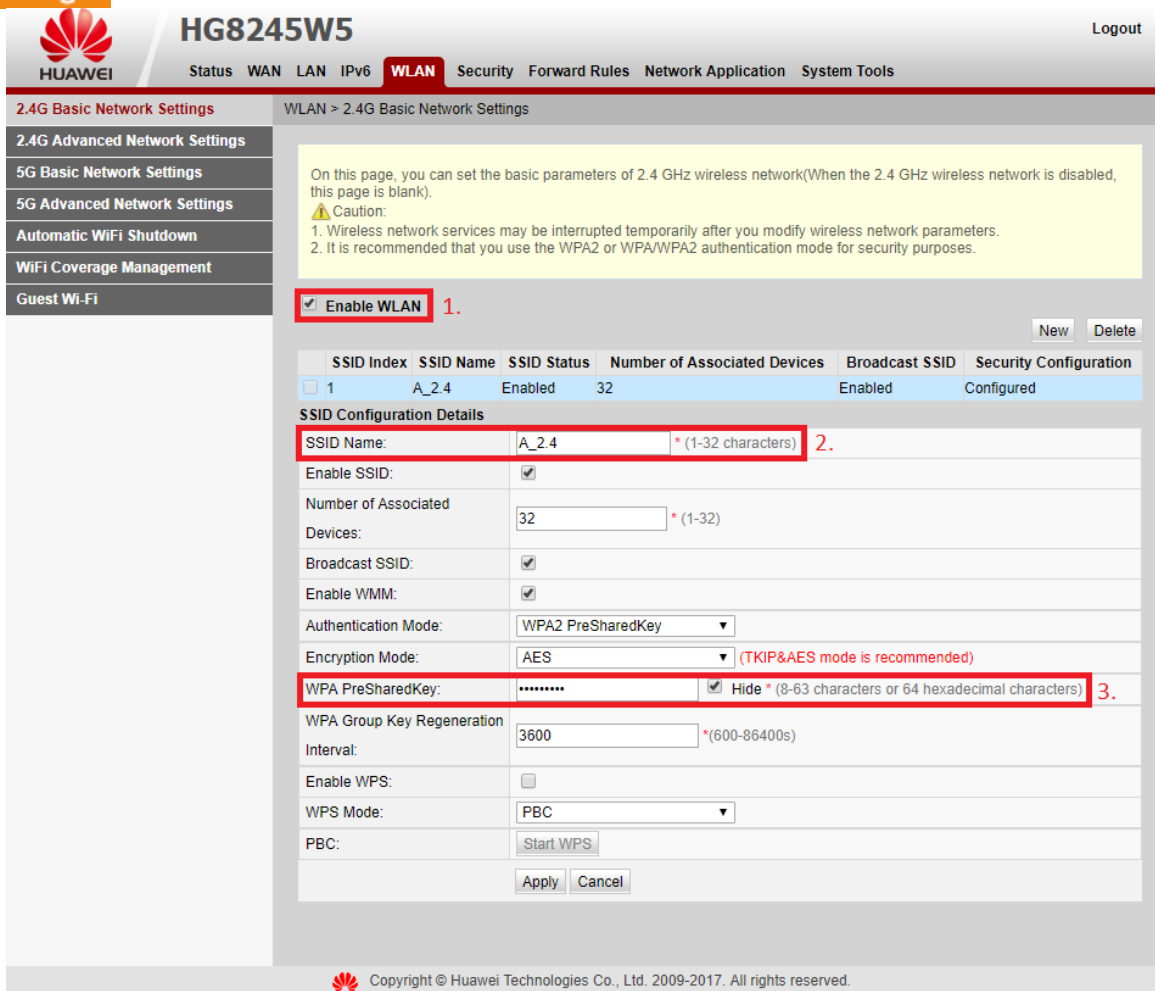
	Stav LED		Popis stavu
	PON	LOS	
1	Nesvieti	Nesvieti	OLT zamedzilo prístupu ONT
2	Bliká rýchlo (dvakrát za sekundu)	Nesvieti	ONT nadväzuje spojenie s OLT
3	Svieti	Nesvieti	Spojenie medzi ONT a OLT je nadviazané
4	Nesvieti	Bliká pomaly (jedenkrát za sekundu)	Nie je pripojené optické vlákno alebo nie je neprijímaný optický signál
5	Bliká rýchlo (dvakrát za sekundu)	Bliká rýchlo (dvakrát za sekundu)	OLT deteguje že zariadenie je neautorizované
6	Bliká rýchlo (dvakrát za sekundu)	Bliká pomaly (jedenkrát za sekundu)	Prijímaný signál je mimo rozsah citlivosti prijímača

2.3 Nastavenie Wi-Fi

Ak na zariadení nesvieti kontrolka WLAN pre bezdrôtovú sieť, užívateľ by mal skontrolovať nastavenie Wi-Fi siete vo webovom rozhraní zariadenia.

Po prihlásení do webového rozhrania na IP adrese zariadenia 192.168.100.1, pomocou mena „root“ a hesla, ktoré je napísané na zariadení (toto meno a heslo je pôvodné a malo by byť funkčné, pokiaľ ho užívateľ nezmenil), v hlavnom hornom menu kliknite na záložku WLAN. Po načítaní stránky v ľavom menu vyberte možnosť 2.4G/5G Basic Network Settings.

Pre zapnutie Wi-Fi treba zaškrtnúť možnosť *Enable WLAN* (Obr.2 , číslo 1). Užívateľ tu môže zmeniť aj názov siete Wi-Fi (Obr.2, číslo 2). Heslo k sieti Wi-Fi sa nachádza na štítku umiestnenom na spodku zariadenia. V prípade zmeny hesla je potrebné prejsť do kolónky *WPA PreSharedKey* (Obr.2, číslo 3) a tam vložiť nové heslo. Vedľa tejto kolónky je možnosť schovať/zobraziť heslo k Wi-fi

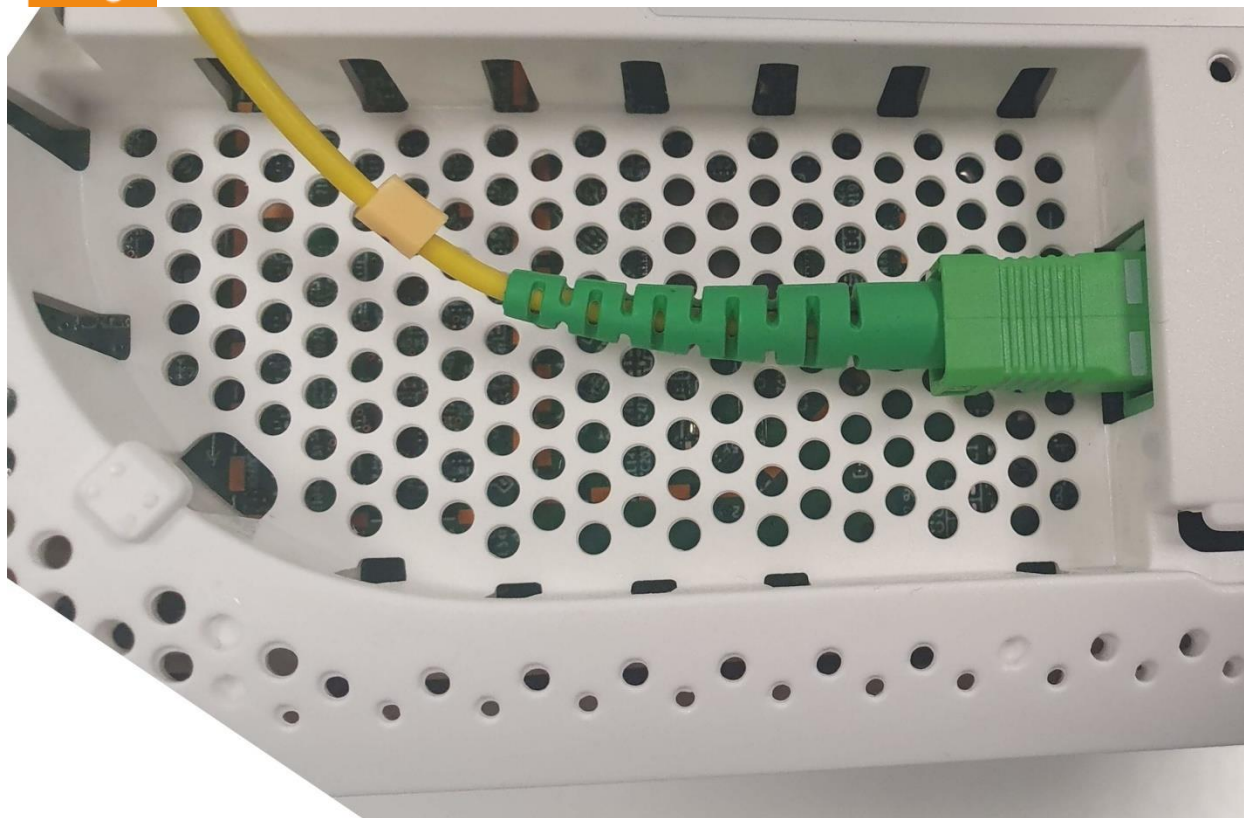


Obrázok 2 Nastavenie Wi-Fi

2.4 Kontrola fyzického zapojenia

Pri kontrole fyzického zapojenia musí byť optické vlákno zapojené do zariadenia tak ako na Obr. 3. Pokiaľ je takto zapojený nie je potrebné ho vyberať. Kábel RJ-45, ktorým sa prepojí počítač s HG8245W5, musí byť zapojený do jedného zo štyroch LAN portov, na zariadení sú žltej farby (Obr. 5, číslo 1). Kábel RJ-11, ktorým sa prepojí telefónny prístroj a HG8245W5 sa pripája do jedného z dvoch TEL portov, na zariadení sú šedej farby (Obr. 5, číslo 2). Vľavo sa potom nachádza vstup pre pripojenie adaptéra (Obr. 5, číslo 3) a tlačidlo napájania (Obr. 5, číslo 4).

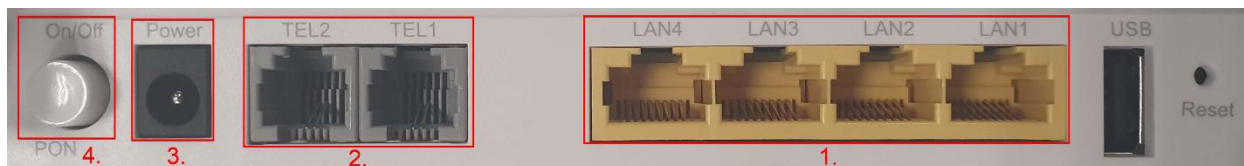
Na pravej strane sa tiež nachádza tlačidlo pre resetovanie zariadenia do výrobných nastavení (Obr. 6, číslo 1).



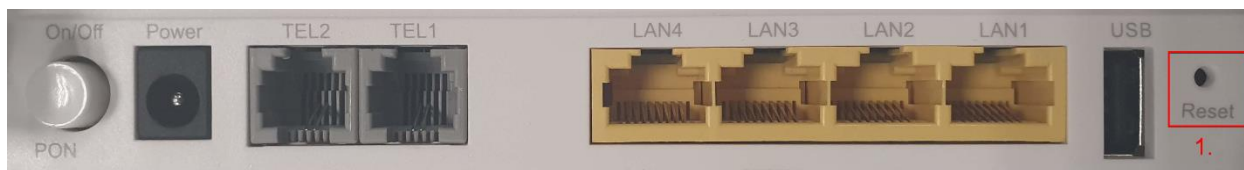
Obrázok 3 Pripojenie optického vlákna do HG8245W5



Obrázok 4 Káble RJ-45 a RJ-11



Obrázok 5 Rozhrania HG8245W5


Obrázok 6 Umiestnenie tlačidla Reset

2.5 Kontrola pripojenia

Funkčnosť fyzického pripojenia a linkovej vrstvy môžete skontrolovať vo webovom rozhraní zariadenia. Po prihlásení kliknite na možnosť *Status* v hornej časti obrazovky a potom v menu na ľavej časti obrazovky kliknite na WAN Information. Na *Obr. 7* v označenej časti vidieť stav pripojenia, Connected znamená že pripojenie bolo úspešné a užívateľ má prístup na internet. Po kliknutí na pripojenie sú vidieť aj ďalšie informácie o pripojení ako napr. IP adresy. *Obr. 7* zobrazuje IPv6 pripojenie. *Obr. 7a* zobrazuje IPv4 pripojenie.

HG8245W5 Logout

Status WAN LAN IPv6 WLAN Security Forward Rules Network Application System Tools

WAN Information Status > WAN Information

On this page, you can query the connection and line status of the WAN port.

IPv4 Information (Click any table cell for details)

WAN Name	Status	IP Address	VLAN/Priority	Connect
5_TR069_R_VID_851	Connected	10.34.0.179	851/6	Always On

WAN Information

MAC Address: F0:63:F9:86:6D:F8

VLAN: 851

Policy: Use the specified value

Priority: 6

NAT: Disable

IP Acquisition Mode: DHCP

IP Address/Subnet Mask: 10.34.0.179/255.255.255.192

Gateway: 10.34.0.129

DNS Servers: 213.151.208.161,213.151.208.162

Lease Time: 151200 s

Remain Lease: 127368 s

NTP Servers: 10.14.127.149,10.14.127.150

Time Zone Info:

SIP Servers:

Static Route: 213.151.223.0/25>10.34.0.129 85.237.225.0/25>10.34.0.129
85.237.225.230/32>10.34.0.129

Vendor Info: dsiforum.org

Online Duration (dd:hh:mm:ss): 04:15:40:12

IPv6 Information (Click any table cell for details)

WAN Name	Status	Prefix	IP Address	VLAN/Priority	Connect
1_IPTV_INTERNET_R_VID_837	Connected	2a01:c846:f40:300::/56	fe80::f263:f9ff:fe86:6df4	837/0	Always On

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Obrázok 7 Webové rozhranie zariadenia

WAN Information Status > WAN Information

On this page, you can query the connection and line status of the WAN port.

IPv4 Information (Click any table cell for details)

WAN Name	Status	IP Address	VLAN/Priority	Connect
1_INTERNET_R_VID_836	Connected	213.151.242.12	836/0	Always On
5_TR069_R_VID_851	Connected	10.34.0.177	851/6	Always On

WAN Information

MAC Address:	44:00:4D:31:E4:89
VLAN:	836
Policy:	DSCP to Pbit mapping
Default Priority:	0
NAT:	Enable
IP Acquisition Mode:	DHCP
IP Address/Subnet Mask:	213.151.242.12/255.255.255.240
Gateway:	213.151.242.1
DNS Servers:	213.151.233.250,213.151.233.251
Lease Time:	111600 s
Remain Lease:	110724 s
NTP Servers:	
Time Zone Info:	
SIP Servers:	
Static Route:	
Vendor Info:	
Online Duration (dd:hh:mm:ss):	00:00:14:36

Obrázok 7a Webové rozhranie zariadenia

3 Advanced Customer Manual

3.1 IPv4

3.1.1 Static LAN DHCP

V hlavnom menu klikneme na záložku LAN. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „DHCP Static IP Configuration“. Pre vytvorenie nového záznamu klikneme na „New“. Do políčka „MAC Address“ napíšeme fyzickú (MAC) adresu zariadenia, a do políčka „IP Address“ napíšeme IP adresu ktorú bude router pridelovať tomuto zariadeniu. Po vyplnení políčok klikneme na „Apply“ pre uloženie záznamu. Pre vymazanie konkrétneho záznamu označíme záznam zaškrtnutím kolónky pri zázname a klikneme na „Delete“. Druhou možnosťou pre nastavenie statickej IP adresy je vybraním možnosti „Satus“ na hlavnej lište, následne „User Device information“. Pri vybranom zariadení vyberte možnosť „Network application“ a po načítaní stránky vyberte „Configure Reversed DHCP IP Adresses“.

LAN > DHCP Static IP Configuration

On this page, you can configure the reserved IP address that is assigned using DHCP for the specified MAC address.

New Delete

MAC Address	IP Address
MAC Address: <input type="text" value="(AA:BB:CC:DD:EE:FF)"/>	IP Address: <input type="text"/>

Apply Cancel

Obrázok 8 Pridelenie statickej DHCP adresy

3.1.2 Port forwarding a DMZ

Port forwarding je aplikácia (NAT), ktorá presmeruje komunikáciu z internetu na daný port zariadenia ONT na port Vami definovaného zariadenia v LAN (PC). Výhodou Port forwarding je možnosť pripojiť sa na PC v LAN z internetu. Oproti DMZ má bezpečnostnú výhodu v tom, že si môžeme zvoliť rozsah portov zariadenia v LAN, ktorý chceme sprístupniť do internetu a taktiež si môžeme vybrať verejné IP adresy, ktoré sa budú môcť pripojiť.

Demilitarizovaná zóna (DMZ) pracuje podobne ako port forwarding s tým rozdielom, že sú zo strany internetu prístupné všetky porty vybraného zariadenia (PC) a prístup má akékoľvek zariadenie z internetu.

3.1.2.1 Port forwarding

V hlavnom hornom menu kliknite na záložku „Forward Rules“. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „Port Mapping Configuration“. Na tejto stránke môžete vytvárať pravidlá, ktoré budú uplatnené vo Firewall. Pre vytvorenie nového pravidla kliknite na tlačidlo „New“. Ako môžete vidieť na Obr.9.

Logout

HG8245W5

Status WAN LAN **IPv6** WLAN Security Forward Rules Network Application System Tools

LAN Address Configuration
DHCPv6 Static IP Configuration
Firewall Configuration
Port Mapping Configuration
IP Filter Configuration

IPv6 > Port Mapping Configuration

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to access the Internet.
Note: 1) The well-known ports for voice services cannot be in the range of the mapping ports.
2) The configured port mapping rule takes effect only after the IPv6 firewall control on packet forwarding is enabled.

New Delete

Mapping Name	WAN Name	Internal Host	External Host	Enable
---	---	---	---	---

Type: User-defined Application

Application: Web Server (HTTP) ▾

Enable Port Mapping:

Mapping Name: HTTP_name

WAN Name: 1_IPTV_INTERNET_R_ ▾

Internal Host: 2a01:c846:f40:300:fc43:5101:715d:a346 LuboThinkpad ▾

External Source IP Address: --

Protocol: TCP ▾ Port number: 80 --80

Delete

Add

Apply Cancel

Obrázok 9 Vytvorenie nového pravidla.

V otvorenom menu na vytvorenie nového pravidla *Obr. 9: Vytvorenie nového pravidla*, si najskôr vyberte typ nastavenia:

User-Defined – manuálne vyplnenie položiek v menu „Add“

Application – menu doplní porty danej aplikácie na základe vybraného protokolu (pozrite aj *Obr. 10. Vopred definované aplikácie*).

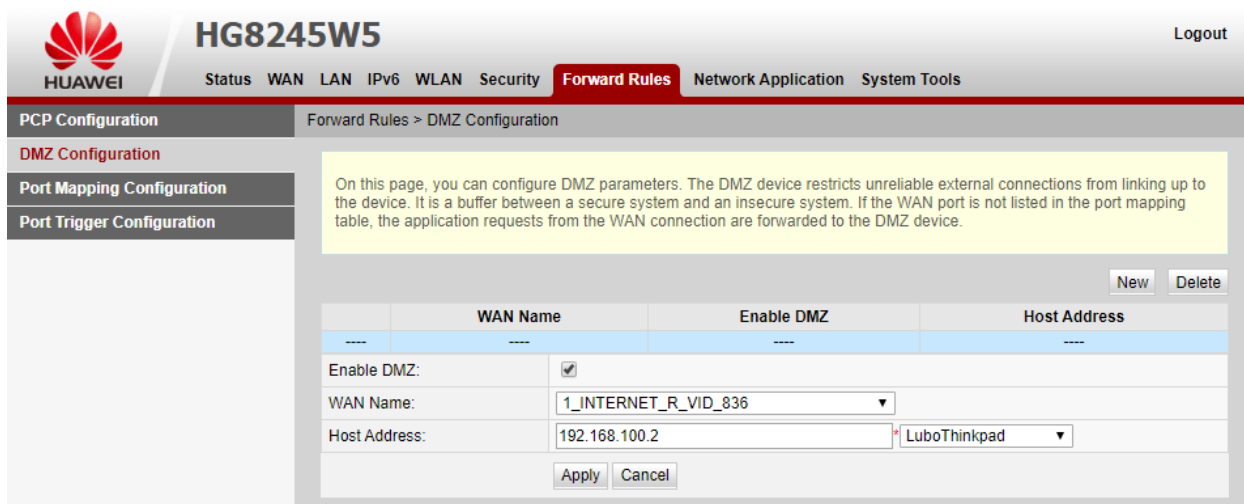
Pri voľbe „User-Defined“ pokračujeme doplnením „Internal Host“ a „External Source IP Address“ do poľa „Internal Host“ zadáme verejnú adresu zariadenia, ktoré chceme aby bolo dostupné z internetu. A do poľa „External Source IP Address“ zadáme verejnú adresu zariadenia z ktorého sa budeme pripájať na zariadenie uložené v LAN sieti.



Obrázok 10 Vopred definované aplikácie

3.1.2.2 DMZ

V hlavnom hornom menu kliknite na záložku Forward Rules. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „DMZ Configuration“. Pre vytvorenie nového pravidla kliknite na tlačidlo „New“.



Obrázok 11 Vytvorenie novej DMZ

Enable DMZ – zapnutie/vypnutie DMZ pravidla

WAN Name – Meno pripojenia

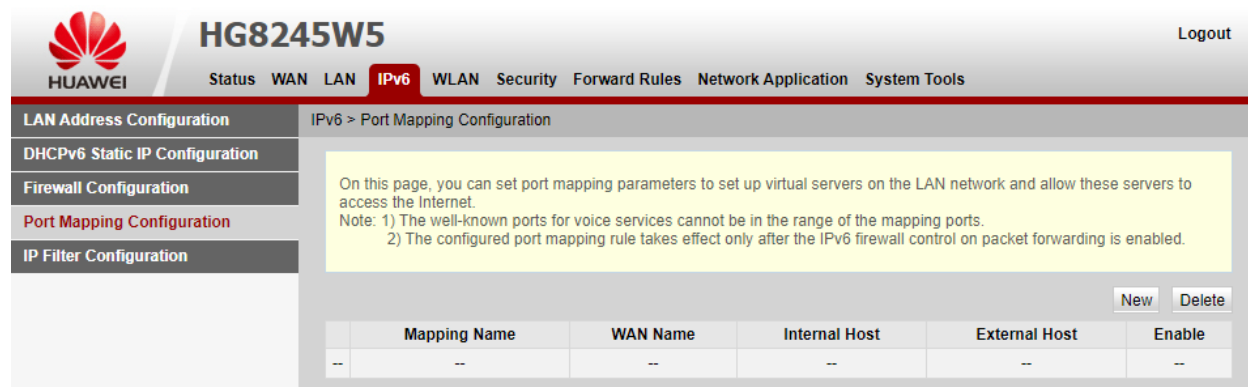
Host Address – IP adresa zariadenia ktoré má byť umiestnené v DMZ, je odporúčané zariadeniu určiť statickú adresu

Pozn. Pokiaľ je FTP server umiestnený v DMZ, tak pre jeho správne fungovanie v tejto konfigurácii je dôležité nastaviť číslo portu na ktorom počúva na iné ako 21. Porty 21, 80 a 443 sú použité na interné účely v ONT takže servery v LAN ktoré poskytujú služby FTP, HTTP alebo HTTPS musia pre účely DMZ bežať na iných portoch.

3.2 IPv6

3.2.1 Port Mapping Configuration

Pre IPv6 konfiguráciu v hlavnom hornom menu kliknite na IPv6 záložku. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „Port Mapping Configuration“. Na tejto stránke môžete vytvárať pravidlá, ktoré budú uplatnené v IPv6 Firewall. Pre vytvorenie nového pravidla kliknite na tlačidlo „New“. Ako môžete vidieť na *Obr. 12.*



The screenshot shows the Huawei HG8245W5 web interface. The top navigation bar includes 'Status', 'WAN', 'LAN', 'IPv6', 'WLAN', 'Security', 'Forward Rules', 'Network Application', and 'System Tools'. The left sidebar menu is expanded to show 'Port Mapping Configuration'. The main content area contains a yellow informational box with the following text:

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to access the Internet.
 Note: 1) The well-known ports for voice services cannot be in the range of the mapping ports.
 2) The configured port mapping rule takes effect only after the IPv6 firewall control on packet forwarding is enabled.

Below the note is a table with the following structure:

Mapping Name	WAN Name	Internal Host	External Host	Enable
--	--	--	--	--

Buttons for 'New' and 'Delete' are located above the table.

Obrázok 12 Nastavenie port mapping pravidla pre IPv6

V otvorenom menu na vytvorenie nového pravidla *Obr. 13* si najskôr vyberte typ nastavenia:

User-Defined – manuálne vyplnenie položiek v menu „Add“

Application – menu doplní porty danej aplikácie na základe vybraného protokolu (pozrite aj *Obr. 14: Vopred definovane aplikácie.*).

Ďalej doplníme „Internal Host“ a „External Source IP Address“ do poľa „Internal Host“ zadáme verejnú IPv6 adresu zariadenia. V našom prípade tam je IPv6 adresa zariadenia na ktorom je HTTP server Do poľa „External Source IP Address“ zadáme verejnú adresu zariadenia s ktorého sa budeme pripájať na zariadenie uložené v LAN sieti. Ak „External Source IP Address“ nevyplníte zariadenie bude dostupné z celého internetu. Na *Obr.13.* Môžeme vidieť vytvorenie pravidla pre HTTP komunikáciu pomocou Type – Application z ktorej sme si vybrali HTTP. Stránka nám automaticky doplní ďalšie potrebné nastavenia pre konkrétny HTTP protokol.

HUAWEI **HG8245W5** Logout

Status WAN LAN **IPv6** WLAN Security Forward Rules Network Application System Tools

LAN Address Configuration DHCPv6 Static IP Configuration Firewall Configuration **Port Mapping Configuration** IP Filter Configuration

IPv6 > Port Mapping Configuration

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to access the Internet.
 Note: 1) The well-known ports for voice services cannot be in the range of the mapping ports.
 2) The configured port mapping rule takes effect only after the IPv6 firewall control on packet forwarding is enabled.

New Delete

Mapping Name	WAN Name	Internal Host	External Host	Enable
---	---	---	---	---

Type: User-defined Application

Application: Web Server (HTTP) ▾

Enable Port Mapping:

Mapping Name: HTTP_name

WAN Name: 1_IPTV_INTERNET_R_ ▾

Internal Host: 2a01:c846:f40:300:fc43:5101:715d:a346 LoboThinkpad ▾

External Source IP Address: --

Protocol: TCP ▾ Port number: 80 --80 *

Delete Add

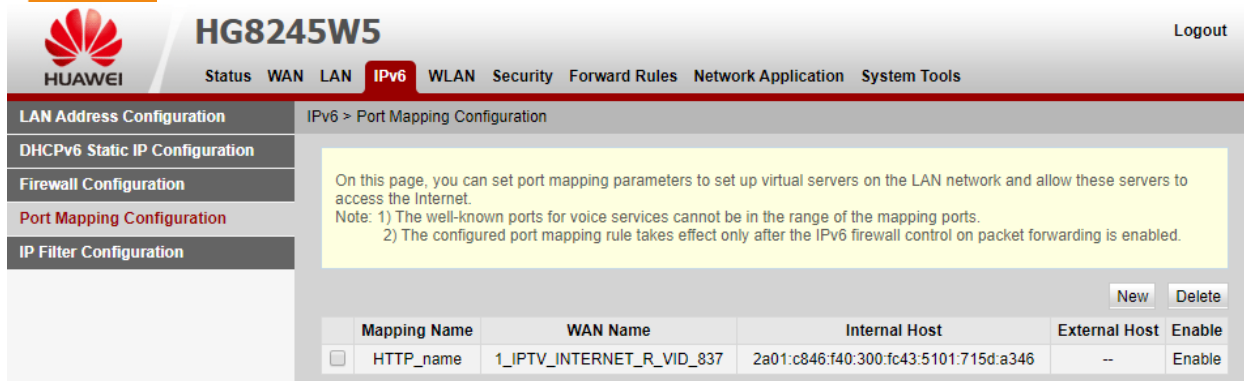
Apply Cancel

Obrázok 13 Vytvorenie nového pravidla.

- Select...
- Domain Name Server (DNS)
- FTP Server
- IPSEC
- Mail (POP3)
- Mail (SMTP)
- PPTP
- Real Player 8 Plus
- Secure Shell Server (SSH)
- Secure Web Server (HTTPS)
- SNMP
- SNMP Trap
- Telnet Server
- TFTP Server
- TFTP
- Web Server (HTTP)

Obrázok 14 Vopred definovane aplikácie

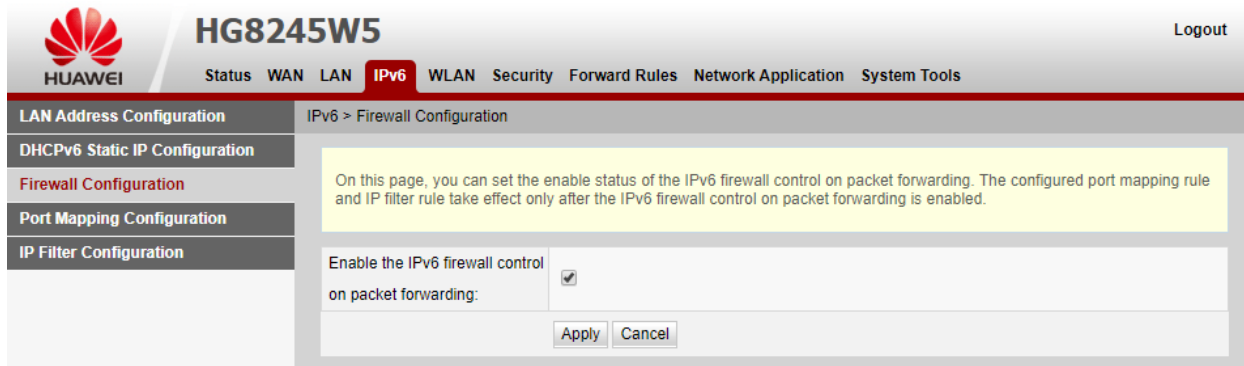
Na poslednom obrázku môžete vidieť vytvorené pravidlo, ktoré povoľuje HTTP komunikáciu na zariadenie umiestnené v LAN sieti.



Obrázok 15 Vytvorené pravidlo

3.2.2 IPv6 Firewall Configuration

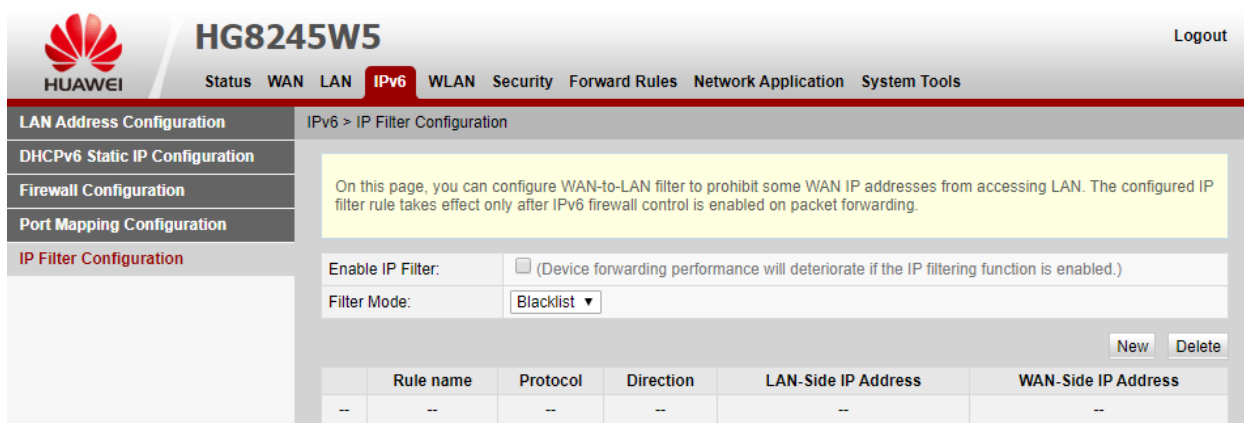
V hlavnom hornom menu kliknite na IPv6 záložku. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti, z ktorých vyberieme „Firewall Configuration“. Na tejto stránke môžete kliknutím alebo odkliknutím vypnúť a zapnúť Ipv6 firewall, ako môžete vidieť na *Obr.16*. Nastavenie firewalu potvrdíte stlačením tlačidla Apply. Firewall je v defaultnom nastavení zapnutý.



Obrázok 16 Nastavenie IPv6 firewallu.

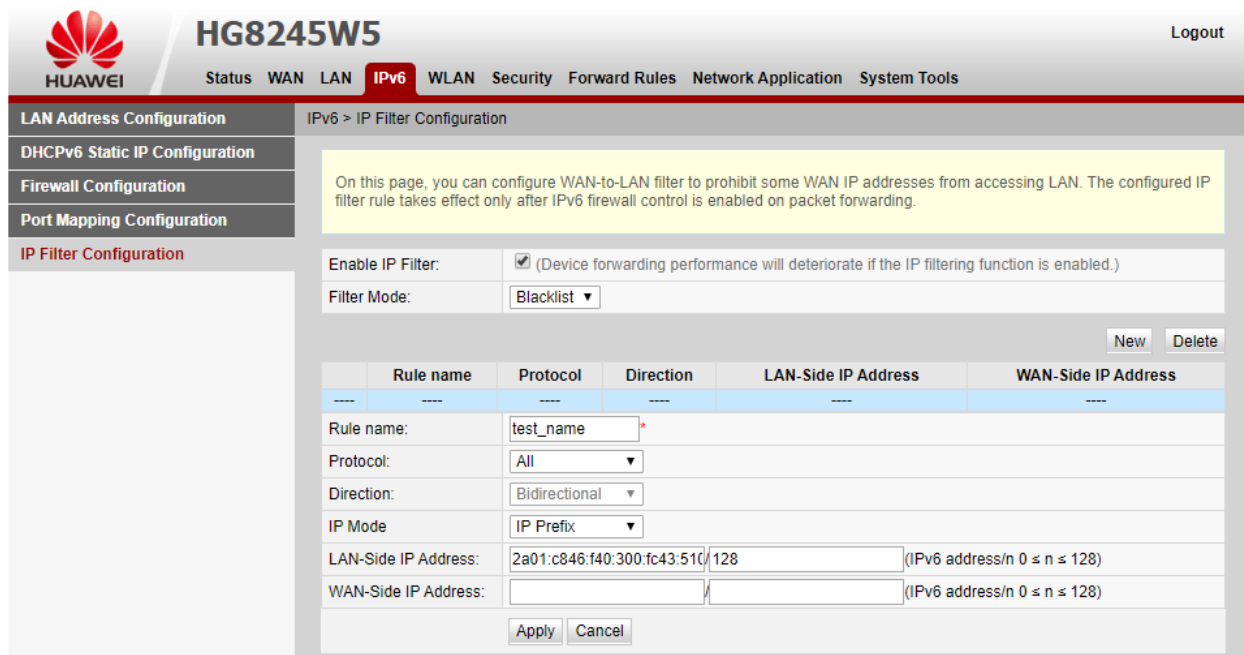
3.2.3 Filter Configuration

V hlavnom hornom menu kliknite na IPv6 záložku. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti z ktorých vyberieme „IP Filter Configuration“. Na tejto stránke môžete vytvárať filtrovacie pravidlá, ktoré budú uplatnené v Ipv6 Firewall. Na stránke zakliknite „Enable IP Filter“ pre zapnutie IP filtra. Položka Filter Mode označuje akým spôsobom budú uplatňované pravidlá, Blacklist zakáže prístup zadanej adrese a Whitelist povolí prístup len zadanej adrese. Ďalej na vytvorenie nového pravidla kliknite na tlačidlo „New“. Ako môžete vidieť na *Obr. 17*



Obrázok 17 Vytvorenie filtrovacieho pravidla

Zadáme názov Filtrovacieho pravidla do poľa „Rule name“. Toto pole je povinné. Ďalej zadáme do poľa „LAN-side IP Address“ adresu alebo rozsah adries, ktoré chceme v LAN sieti blokovať. A do poľa „WAN-side IP Address“ zadáme adresu alebo rozsah adries, ktoré budú blokované pre zariadenia v LAN. Nastavenie filtra potvrdíte stlačením tlačidla „Apply“.

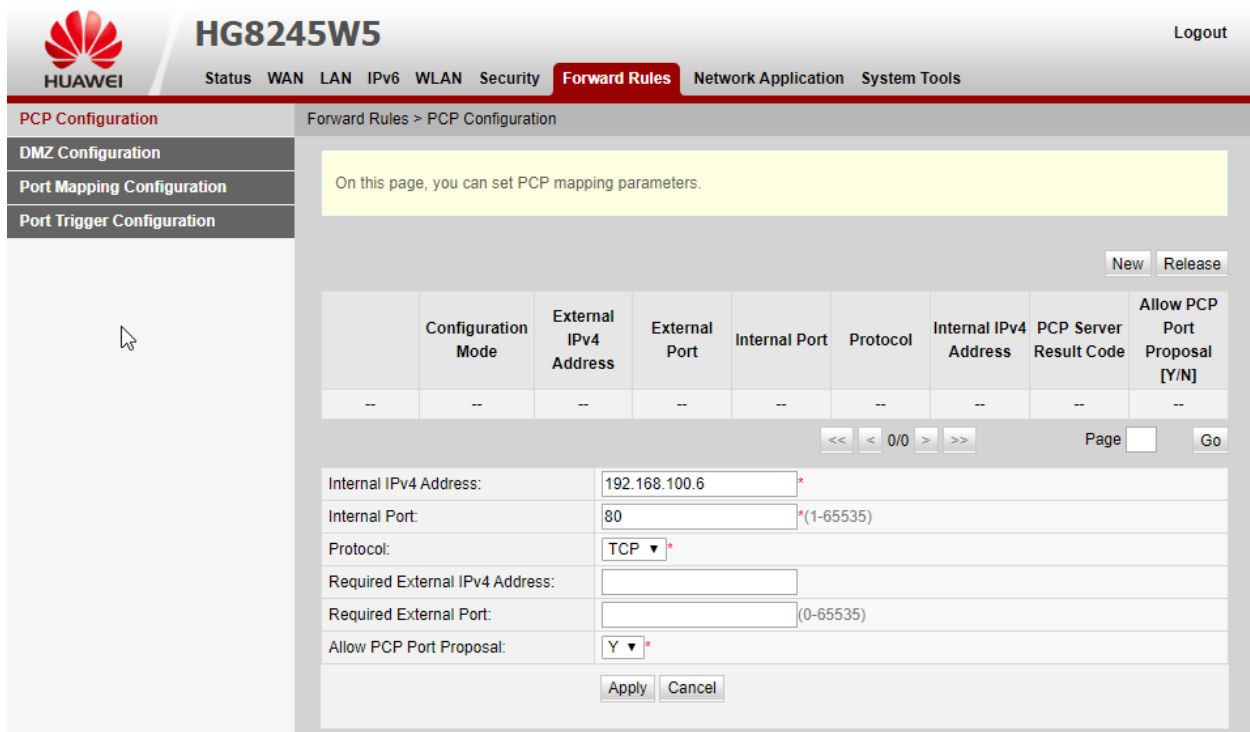


Obrázok 18 Vytvorenie filtrovacieho pravidla

3.2.4 PCP

V hlavnom hornom menu kliknite na záložku „Forward Rules“. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „PCP“.

Po kliknutí na „New“ vytvoríme nové pravidlo. V našom príklade je vytvorené pravidlo pre HTTP komunikáciu port 80. Počítač, pre ktorý je pravidlo vytvorené má pridelenú IPv4 adresu 192.168.100.6. Preto do poľa „Internal IPv4 Address“ zadáme 192.168.100.6. Do poľa „Required External IPv4 Address“ môžete zadať adresu CGN, cez ktorú chcete na ONT zariadenie pristupovať. Ďalšie pole je „Required External Port“ cez ktorého chcete pristupovať na ONT zariadenie. Tieto polia nie sú povinné. Nevyplnené polia znamenajú, že prístup na nastavený port bude z celého internetu.



PCP Configuration

Forward Rules > PCP Configuration

On this page, you can set PCP mapping parameters.

New Release

	Configuration Mode	External IPv4 Address	External Port	Internal Port	Protocol	Internal IPv4 Address	PCP Server Result Code	Allow PCP Port Proposal [Y/N]
--	--	--	--	--	--	--	--	--

Internal IPv4 Address: 192.168.100.6 *

Internal Port: 80 *(1-65535)

Protocol: TCP *

Required External IPv4 Address:

Required External Port: (0-65535)

Allow PCP Port Proposal: Y *

Apply Cancel

Obrázok 19 Vytvorenie nového PCP pravidla

Internal IPv4 Address – IPv4 adresa cieľa v LAN sieti

Internal port – port na ktorý je posielaná komunikácia

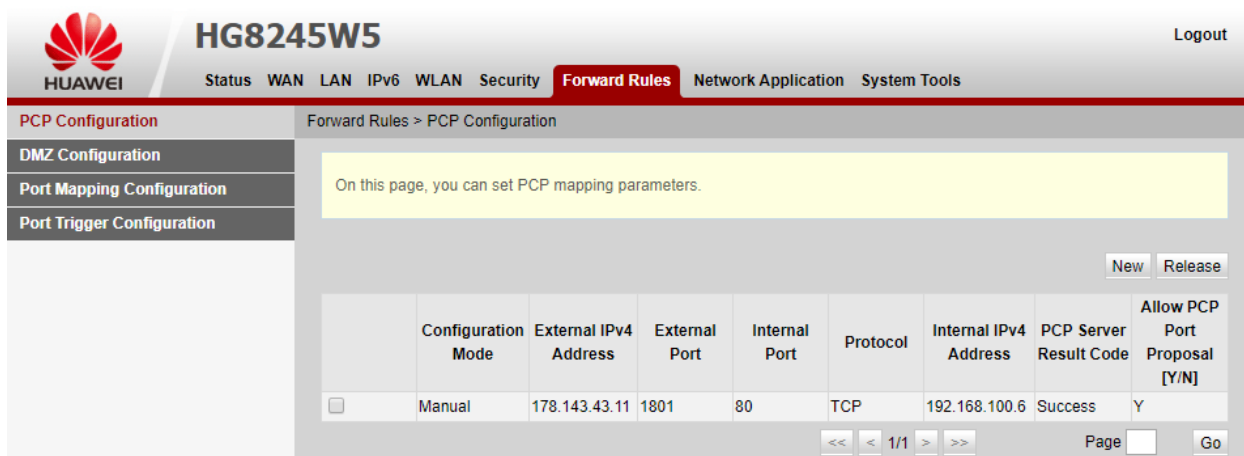
Protocol – komunikačný protokol TCP/UDP

Required External IPv4 Address – žiadaná externá IPv4 adresa

Required External Port - žiadaný externý port

Allow PCP Port Proposal – Y / N -> Yes/No

Po úspešnom vyjednaní parametrov ich uvidíme v kolónkach „External IPv4 Address“ a „External Port“ blikať načerveno.

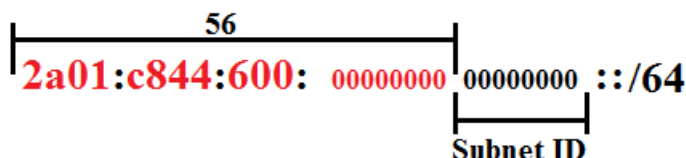


Obrázok 20 Vytvorenie nového PCP pravidla

3.2.5 Zmena prefixu

Orange Slovensko prideliť zákazníkovi prefix /56 (prvých 56 bitov z ľavej strany). Rozlišujeme Statický a Dynamický prefix pre zákazníka. V Statickom sa prefix /56 nemení ani po reštarte zariadenia ale pre Dynamický sa po každom reštarte, vyp./zap. zariadenia zmení delegovaný prefix /56.

Defaultné nastavenie je, že k delegovanému prefixu /56, zariadenie automaticky doplní + 8 núl (Subnet ID - 0). Vid' na Obr. 21. Tento prefix /64 je pridelený pre zariadenia v LAN sieti.



Obrázok 21 Prefix

Zákazník si môže zmeniť svoj prefix /64 v LAN tým, že zmení Subnet ID. Alebo aktuálna verzia firmware umožňuje zmenu prefixu od /56 do /64.

3.2.5.1 Zmena Subnet ID

V záložkách kliknite na záložku IPv6 a v ľavom menu vyberte „LAN Address Configuration“. Na tejto stránke Obr.22. v sekcii „Interface Address Information“ zmeníme „Method of obtaining prefixes“ z „WAN Agent“ na „Static configuration“. Objaví sa pridelený prefix od Orange Slovensko, ktorý budete meniť. V prefixe meníte posledné dve hexadecimálne číslice pred ::/64 v poli prefix (POZOR ! Môžete zadávať len od 0 po 255 čo je v hexadecimálnej sústave 00 až FF). Na Obr. 23. môžete vidieť zmenu Subnet ID na hodnotu 50.

LAN Address Configuration IPv6 > LAN Address Configuration

On this page, you can set IPv6-related feature parameters.

Interface Address Information

IPv6 Address:	fe80::1 *
Method of Obtaining Prefixes:	WAN agent ▼
Parent Prefix:	▼
Child Prefix Mask:	::/64 *(IPv6 address/64)
MTU:	1472 *(1280-1500)

DNS Information

DNS Source on the LAN Side:	DNS agent ▼
-----------------------------	-------------

Resource Allocation Information

Enable Route Advertisement:	<input checked="" type="checkbox"/>
Enable DHCPv6 Server:	<input checked="" type="checkbox"/>
Resource Allocation Mode:	Manual ▼
Address/Prefix Assignment Mode:	<input type="radio"/> DHCPv6 <input checked="" type="radio"/> SLAAC
Other Information Assignment Mode:	<input checked="" type="radio"/> DHCPv6 <input type="radio"/> SLAAC

ULA information

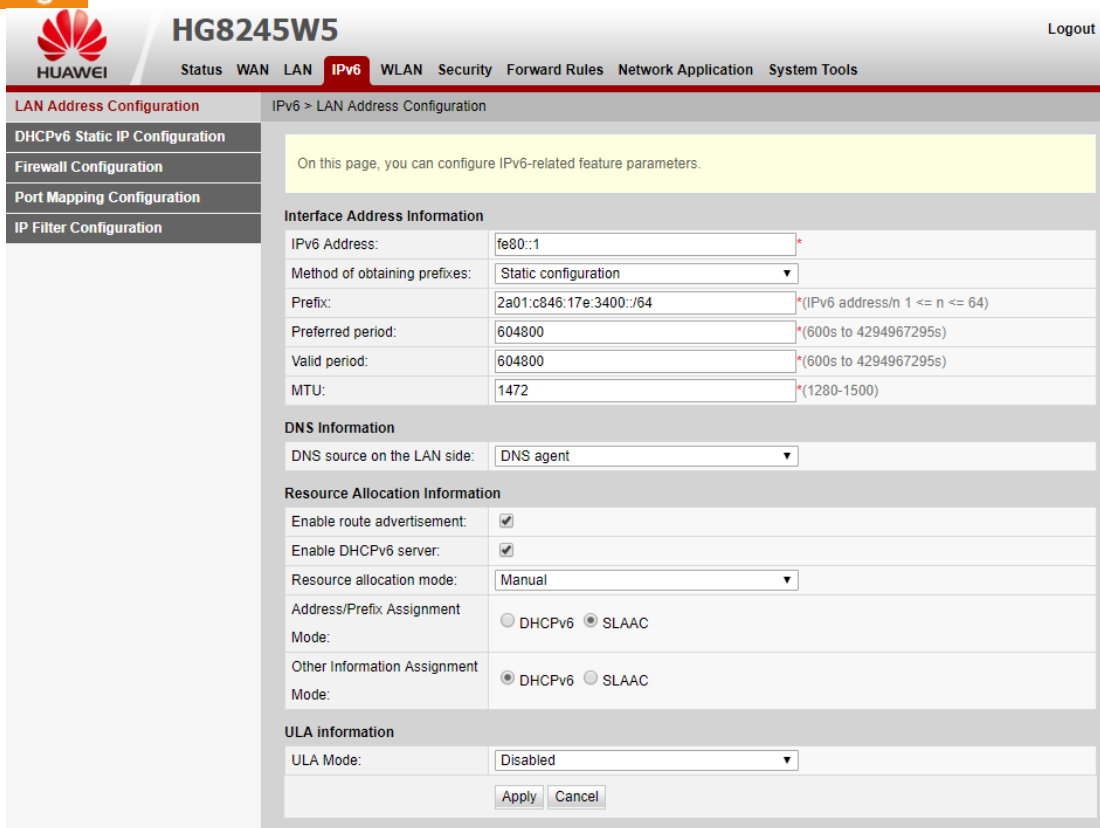
ULA Mode:	Disabled ▼
-----------	------------

Apply Cancel

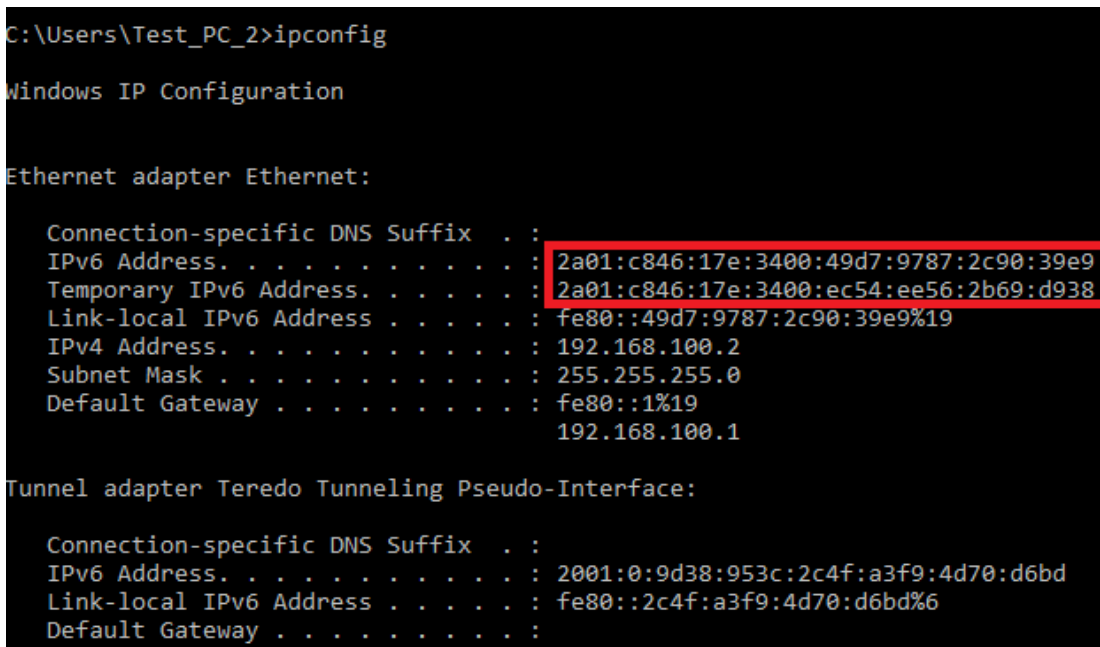
Obrázok 22 Pôvodné nastavenia

Nastavenia vykonané v LAN sieti si môžete skontrolovať na pripojenom PC. Otvorenie príkazovom riadku (win + r), zadáte *cmd* a následne v príkazovom riadku *ipconfig*. Výsledok a zmenu nastavení nájdete v informáciách o interface, ktorým ste pripojený do LAN siete Obr. 24.. Adresy budú obsahovať vami zvolený prefix. Tento prefix bude pridelený všetkým zariadeniam v LAN sieti.

Zmena SubnetID je perzistentná a zostane platná aj po reštarte zariadenia resp. v prípade Dynamického prefixu aj po pridelení nového /56 subnetu.



Obrázok 23 Zmena subnet ID



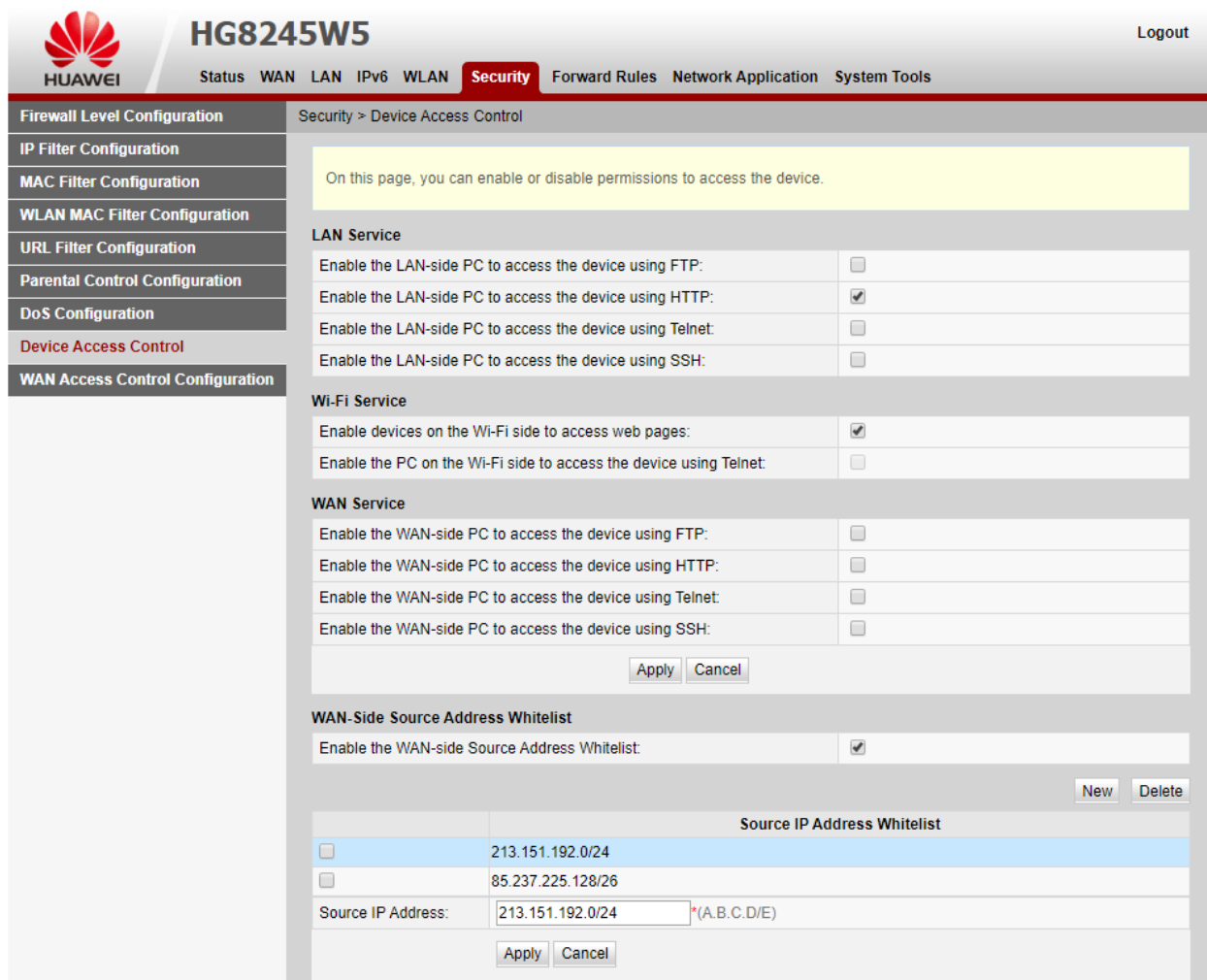
Obrázok 24 Kontrola subnet ID

3.2.6 Prístup z WAN

Pokiaľ v sekcii “Security” v ľavom menu klikneme na “Device Access Control” a v časti WAN zaškrtneme checkbox pre daný druh pripojenia, umožníme tým pripojenie daného typu na zariadenie HGW-U z WAN pre všetky IP.

Ak chceme umožniť prístup len pre daný rozsah IP adries, tak pod “Wan-side Source Address Whitelist” klikneme na “new” a zadáme rozsah adries, ktorým chceme umožniť pripojenie. Pre aktivovanie nového Whitelist-u je potrebné mať zaškrtnutý checkbox “Enable the WAN-side Source Address Whitelist” a po nastavení rozsahu kliknúť na “Apply”.

Defaultne je prístup z Wan umožnený len pre HTTP v sekcii “WAN Access Control Configuration” pre rozsah OSK 2a01:c840:0110:8003::/64. Tu môžeme pridať vlastný rozsah IP adries, ktoré sa môžu pripojiť a taktiež môžeme zvoliť spôsob pripojenia zaškrtnutím príslušného checkboxu a stlačením “Apply”.



The screenshot shows the configuration page for 'Security > Device Access Control' on a Huawei HG8245W5 device. The interface includes a navigation menu on the left with options like 'Firewall Level Configuration', 'IP Filter Configuration', and 'Device Access Control'. The main content area is divided into several sections:

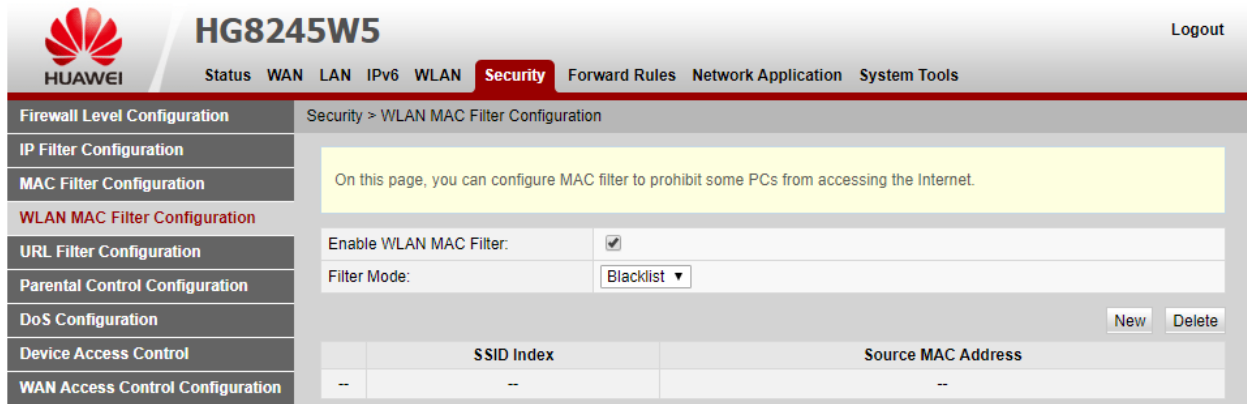
- LAN Service:** Contains four rows with checkboxes for enabling LAN-side PC access via FTP, HTTP (checked), Telnet, and SSH.
- Wi-Fi Service:** Contains two rows with checkboxes for enabling Wi-Fi side access via web pages (checked) and Telnet.
- WAN Service:** Contains four rows with checkboxes for enabling WAN-side PC access via FTP, HTTP, Telnet, and SSH.
- WAN-Side Source Address Whitelist:** Features a checkbox 'Enable the WAN-side Source Address Whitelist' which is checked. Below it are 'New' and 'Delete' buttons. A table titled 'Source IP Address Whitelist' shows two entries: '213.151.192.0/24' and '85.237.225.128/26'. Below the table is a form for adding a new entry with a text field containing '213.151.192.0/24' and a label '(A.B.C.D/E)'. 'Apply' and 'Cancel' buttons are at the bottom.

Obrázok 25 Nastavenie prístupu z WAN

3.3 IPv4 and IPv6

3.3.1 MAC Filter

V hlavnom hornom menu kliknite na záložku „Security“. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti z ktorých vyberieme „WLAN MAC Filter Configuration“ pre Wi-Fi a „MAC Filter Configuration“ pre Ethernet.



Obrázok 26 Vytvorenie nového filtrovacieho pravidla

Enable WLAN MAC Filter - zapíname alebo vypíname filter.

Filter Mode – Druh filtrovania

Whitelist – povoľuje prístup iba adresám v zozname

Blacklist – zakazuje prístup adresám zo zoznamu

Pre vytvorenie nového záznamu klikneme na „New“

SSID Index – Názov siete pre ktorú chceme pravidlo vytvoriť (len pre Wi-Fi)

Source MAC Address – MAC adresa zariadenia na ktoré chceme aplikovať pravidlo

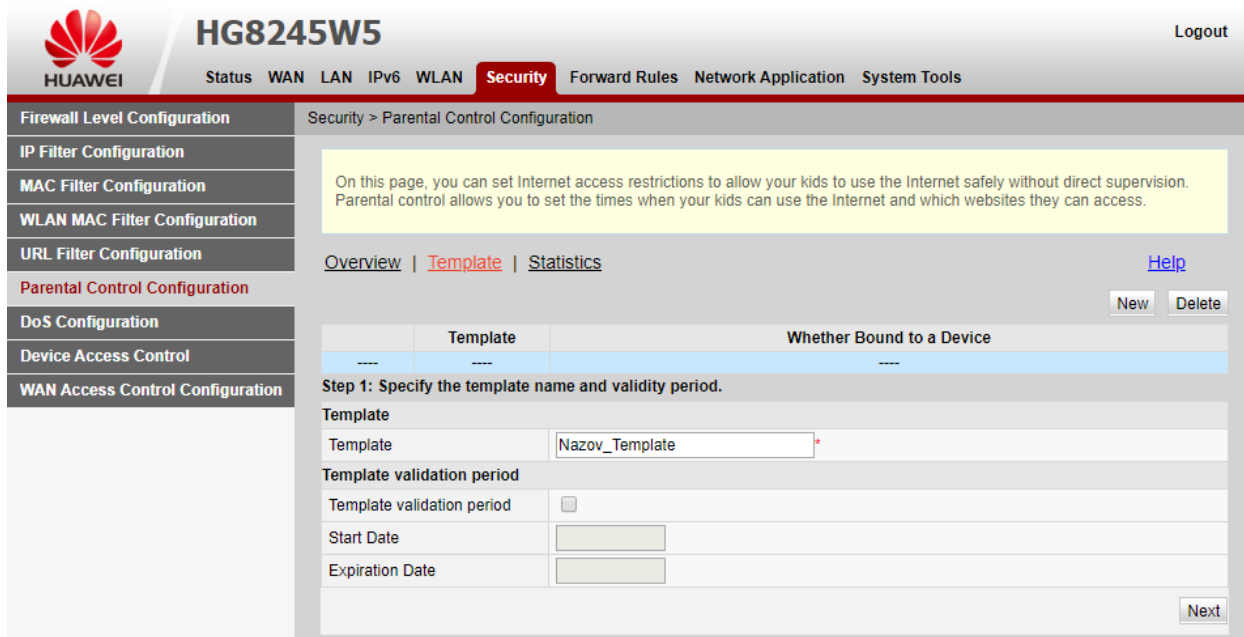
3.3.2 Smart Wi-Fi

Smart wifi je aplikácia, ktorá umožňuje pripojiť do LAN ONT viac ako jeden bezdrôtový prístupný bod (Access point) a následne prepínať medzi nimi tak, aby sa PC alebo telefón vždy pripojil na Access point so silnejším signálom respektíve podľa definovaných nastavení.

TBD (Táto časť manuálu bude doplnená)

3.3.3 Parental Control

V hlavnom menu kliknite na záložku „Security“. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti z ktorých vyberieme „Parental Control Configuration“. V strede stránky sa zobrazia tri možnosti: „Overview“, „Template“ a „Statistics“. Kliknite na možnosť „Template“, potom na „New“.



Obrázok 27 Smart Wi-Fi Template

Do kolónky Template zadajte názov nového Template. Pokiaľ chcete aby pravidlo platilo len po určitéj dobe zaškrtnite checkbox „Template validation period“ a do políčka „Start Date“ zadajte odkedy a do políčka „Expiration Date“ dokedy má dané pravidlo platiť. Kliknite na „Next“ a následne na „new“. Tu si môžete vybrať, či bude pravidlo platiť celý deň alebo iba vo vybrané hodiny a taktiež dni, počas ktorých sa pravidlo bude pravidelne aplikovať. Kliknite na „next“ a následne na „new“. Ak chcete zakázať nejakú internetovú stránku (napr. www.facebook.com), zaškrtnite checkbox „Enable website filter“ a do políčka „URL Address“ zadajte Vami vybranú stránku, na ktorú nechcete umožniť prístup. Kliknite na „Finish“ a následne na možnosť „Overview“. Po kliknutí na „new“ sa zobrazí nasledovná stránka.

The screenshot shows the Huawei HG8245W5 web interface. The top navigation bar includes 'Status', 'WAN', 'LAN', 'IPv6', 'WLAN', 'Security' (highlighted), 'Forward Rules', 'Network Application', and 'System Tools'. The left sidebar lists various configuration options, with 'Parental Control Configuration' selected. The main content area is titled 'Security > Parental Control Configuration' and contains a yellow informational box, navigation links ('Overview', 'Template', 'Statistics', 'Help'), radio buttons for 'Apply on all devices' and 'Apply on specified devices', and a table for device configuration. The table has columns for 'Device', 'Description', and 'Binding Templates'. Below the table are input fields for 'Specified Device', 'Device Description', and 'Binding Templates', along with 'Apply' and 'Cancel' buttons.

Obrázok 28 Smart Wi-Fi Overview

Pokiaľ sa má pravidlo vzťahovať na všetky PC v LAN zaškrtnite „Apply on all devices“. V opačnom prípade do kolónky „Specified Device“ kliknite na šípku (Popup) a podľa mena PC alebo podľa MAC adresy vyberte počítač, na ktorý sa má pravidlo vzťahovať. Do kolónky „Device Description“ môžete dať počítaču prezývku (napr. Michalov_PC). V kolónke „Template“ vyberte Vami vytvorený Template a kliknite na „Apply“.

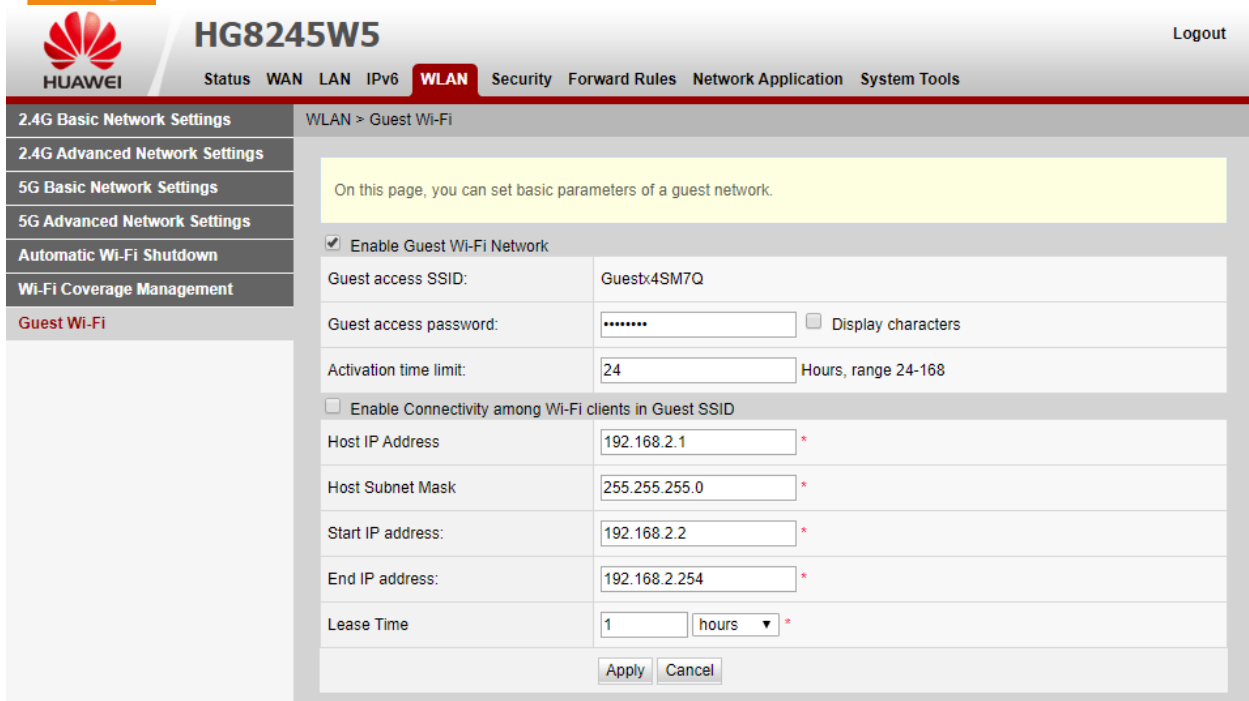
Ak chcete vidieť koľkokrát sa PC snažil pripojiť na Vami zakázanú IP alebo vo Vami zakázanej dobe, kliknite na „Statistics“.

Po kliknutí na možnosť „Overview“ sa zobrazí zoznam zariadení pre ktoré bol nastavený parental control a ku každému vybraný Template.

3.3.4 Guest Wi-Fi

Guest wifi je bezdrôtový prístup do LAN zariadenia pre neautentifikovaných užívateľov, akými sú napríklad hostia. Takýto užívatelia po zadaní hesla budú mať prístup na internet, avšak s obmedzeniami vyplývajúcimi podľa Vášho nastavenia. Napríklad nebudú mať prístup k zmene nastavení zariadenia, alebo k iným užívateľom.

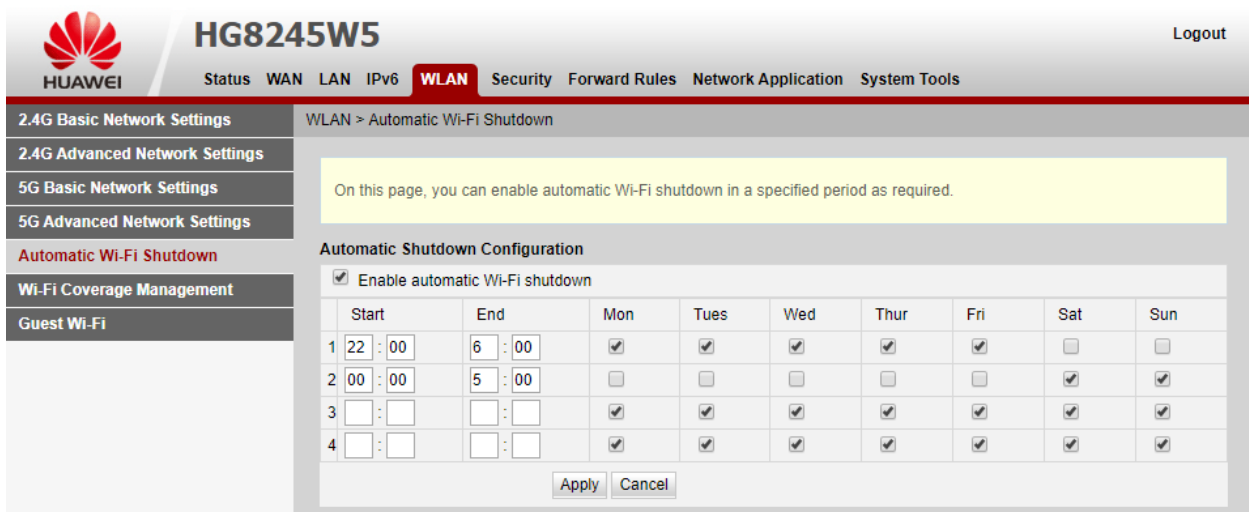
V hlavnom hornom menu kliknite na záložku WLAN. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti, z ktorých vyberieme „Guest Wi-Fi“. Po zaškrtnutí Checkboxu „Enable Guest WiFi Network“ sa zobrazia nové kolónky. Do kolónky s názvom „Guest access Password“ zadajte heslo, ktorým chcete, aby sa hostia autentifikovali pri pripojení na Guest Wi-Fi. Dobu pripojenia môžeme obmedziť v „Activation time limit“, kde môžeme vybrať ľubovoľný čas v rozsahu 24 až 168 hodín.



Obrázok 29 Nastavenie Guest Wi-Fi

3.3.5 Wi-Fi automatic shutdown

V hlavnom hornom menu kliknite na záložku WLAN. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti, z ktorých vyberieme „Automatic WiFi Shutdown“. Checkbox „Enable automatic WiFi shutdown“ musí byť zaškrtnutý. V kolónke „Start“ zadáme hodinu a minútu, v ktorej sa má WiFi vypnúť a v kolónke „End“ zase hodinu a minútu, kedy sa WiFi znovu zapne. Napravo od času si vyberieme dni, v ktorých má príslušné pravidlo platiť a potvrdíme tlačidlom „Apply“.

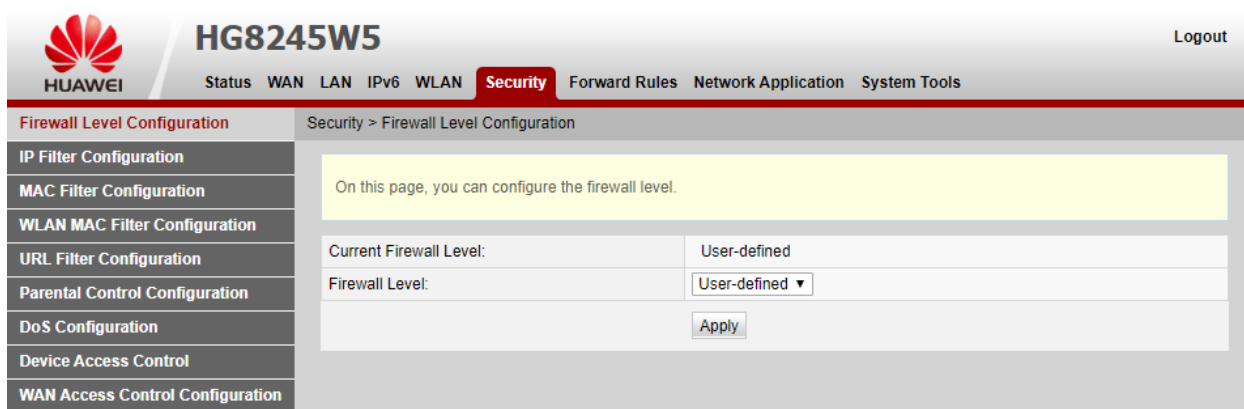


Obrázok 30 Nastavenie automatic Wi-Fi shutdown

3.3.6 Firewall

Defaultne nastavená úroveň firewall-u je User-defined. Pokiaľ chcete jeho úroveň zmeniť, v hlavnom hornom menu kliknite na záložku Security. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „Firewall Level Configuration“. V časti Firewall Level si môžeme z lišty vybrať niekoľko úrovní firewallu. Výber je treba potvrdiť tlačidlom Apply.. V nižšie uvedených tabuľkách sú uvedené všetky stupne firewall-u a k nim sprístupnené protokoly, pričom krížik znamená, že

protokol pri danej úrovni firewall-u nie je povolený.



Obrázok 31 Nastavenie úrovni firewallu

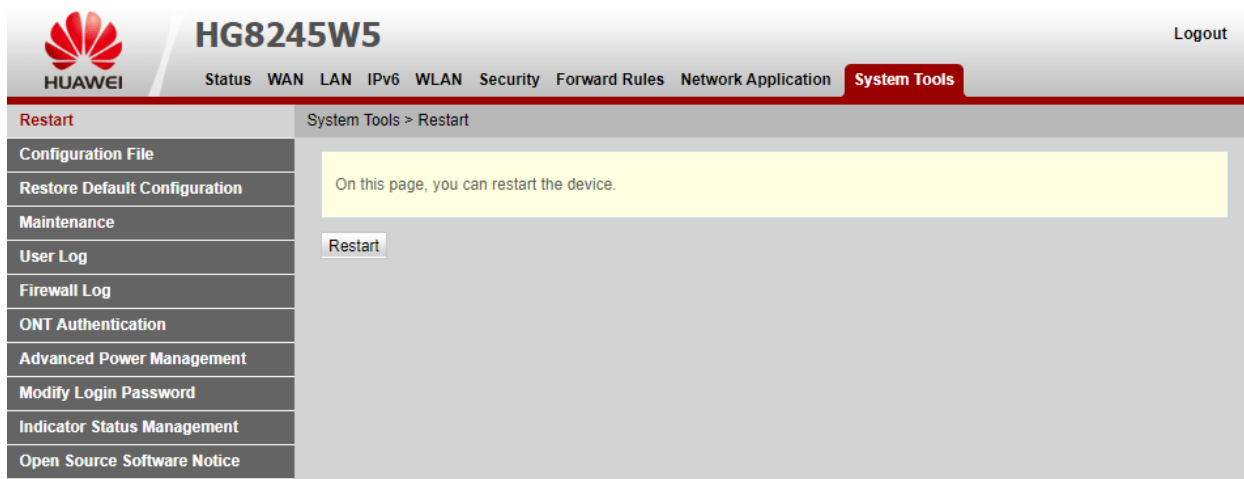
Firewall level	WAN->ONT						
	Stateful Firewall	PING	ACS	HTTP	FTP	Telnet	Other
High	✓	✗	✓	✗	✗	✗	✗
Medium	✓	✗	✓	✗	✗	✗	✗
Low	✓	✗	✓	✗	✓	✗	✗
User-define	✓	✗	✓	✗	✗	✗	✗
Disable	✓	✓	✓	✗	✓	✓	✓

Firewall level	LAN->ONT				
	HTTP	Telnet&PING	FTP	DNS&DHCP	Other
High	✓	✗	✗	✓	✗
Medium	✓	✓	✗	✓	✗
Low	✓	✓	✗	✓	✗
User-defined	✓	✓	✗	✓	✓
Disable	✓	✓	✓	✓	✓

Firewall level	LAN->WAN	
	FTP&HTTP(S)&DNS	Other
High	✓	✗
Medium	✓	✓
Low	✓	✓
User-define	✓	✓
Disable	✓	✓

3.3.7 Reštart zariadenia

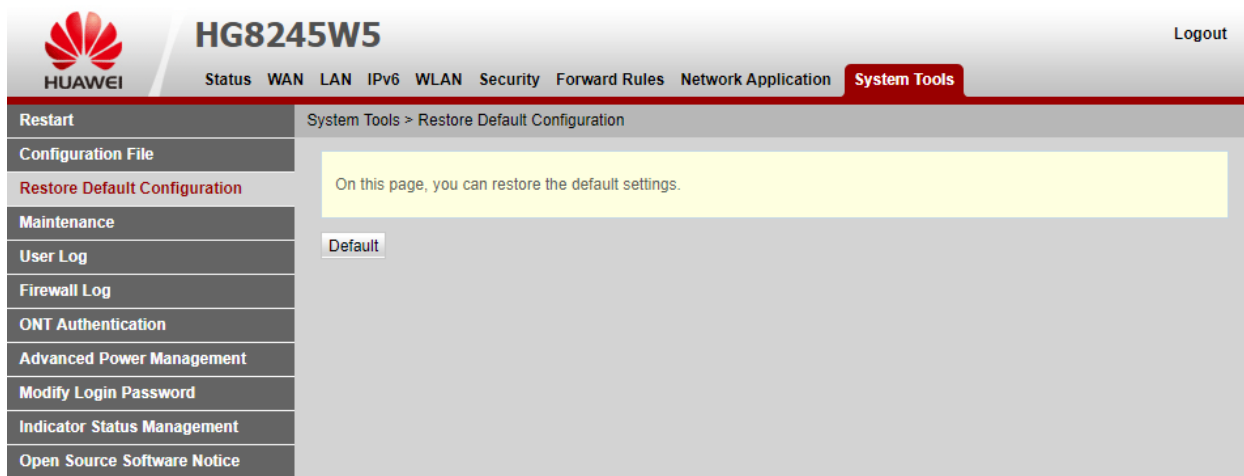
V hlavnom hornom menu kliknite na záložku System Tools. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „Reboot“. Po kliknutí na tlačidlo Restart sa zariadenie reštartuje.



Obrázok 32 Stránka na reštart zariadenia

3.3.8 Obnovenie továrenských nastavení

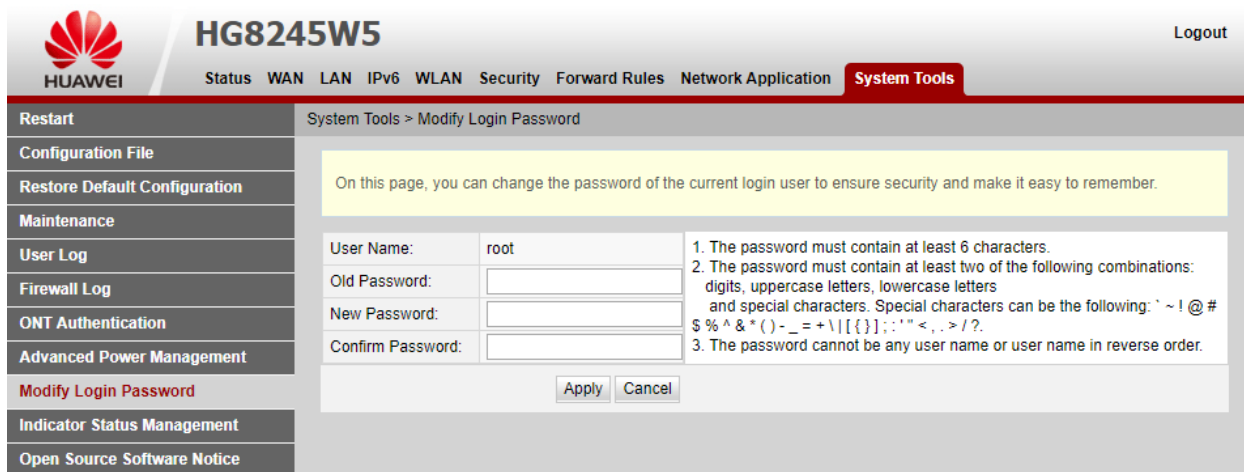
V hlavnom hornom menu kliknite na záložku System Tools. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „Restore Default Configuration“. Po kliknutí na tlačidlo Default sa na zariadení obnovia továrenské nastavenia.



Obrázok 33 Stránka na uvedenie zariadenia do továrenských nastavení

3.3.9 Zmena prihlasovacieho hesla

V hlavnom hornom menu kliknite na záložku „System Tools“. Po načítaní stránky sa nám v ľavom menu zobrazia možnosti s ktorých vyberieme „Modify Login Password“. Na stránke v časti „Change Password“ nastavíme nové heslo.



Obrázok 34 Stránka na zmenu prihlasovacieho hesla



New Password – nové heslo

Confirm Password – potvrdenie hesla

Nové heslo musí mať minimálne 6 znakov, musí obsahovať minimálne dve

1. z nasledujúcich: číslo
2. veľké písmeno, malé písmeno
3. špeciálny znak: ` ~ ! @ # \$ % ^ & * () - _ = + \ | [{ }] ; : ' " < , . > / ?

3.3.10 Firewall záznamy

FireWall záznam sa rovnako ako systémový záznam nachádza v menu *System Tools*. Zaznamenáva sa 100 výpisov, ktoré sa radia systémom FIFO. V jednoduchosti sa dá tvrdiť, že sa ukladá 100 najaktuálnejších výpisov. Pri zvýšenom zaťažení zariadenia môže zachytávanie výpisov Firewall záznamu znižovať rýchlosť posielania dát.

Je možné súčasne aplikovať štyri smery *Firewall-u*: *From Internet to LAN*, *From Internet to local*, *From LAN to Internet* a *From LAN to local*. Pri každom smere je na výber uplatniť tzv. *Log Rule Action*, či sa jedná o povolený (*Accept*) alebo zamietnutý (*Reject*) typ akcie samotným Firewall-om zariadenia. Z toho vyplýva, že maximálny počet kombinácií smerov a typov akcie Firewall záznamov je limitovaný na 8. Pri vytváraní väčšieho počtu je užívateľ touto skutočnosťou oboznámený vyskočením príslušného okna.

Pri systémových hláseniach sa zaznamenávajú všetky druhy hlásenia a je na užívateľovi, aký druh hlásenia chce zobraziť, prípadne uložiť si do počítača. Pri *Firewall Log*-och však treba vytvoriť príslušný druh záznamu, ktorý sa bude následne zaznamenávať. Je možné súčasne aplikovať všetkých spomínaných 8 druhov.

Restart System Tools > Firewall Log

Configuration File

Restore Default Configuration

Maintenance

User Log

Firewall Log New Delete

ONT Authentication

Advanced Power Management

Modify Login Password

Indicator Status Management

Open Source Software Notice

On this page, you can configure, download, and query a firewall log.

Enable Firewall Log (If enabled, device forwarding performance will be deteriorated.)

	Log Rule Status	Log Access Direction	Log Rule Action
<input type="checkbox"/>	Enabled	From Internet to LAN	Accept

Enable Log Rule:

Log Access Direction: From Internet to LAN ▼*

Log Rule Action: Accept ▼*

Apply Cancel

Download and View Logs

Download Log File

Manufacturer: Huawei Technologies Co., Ltd;
 ProductClass: HG8245W5;
 SerialNumber: 4857544341F8AC9F;
 IP: 10.34.0.177;
 HWVer: HWTCA163DA;
 SWVer: HWTCA51910110;

Obrázok 35: Voľba smerov a typ akcie Firewall záznamu

Pri zobrazenom *Firewall* zázname v GUI zariadenia sa nezobrazujú údaje v reálnom čase. Pre zobrazenie aktuálne doposiaľ zachyteného záznamu je nutné opätovne načítať stránku pre Firewall záznam. Pri stiahnutí do počítača sa vždy uloží najaktuálnejší záznam nehľadiac na zobrazovanú skutočnosť v GUI zariadenia.