TPS
شماره ثبت: ۵۰۸۰۱

راهنمای کاربر نهایی

مبدل های سری S1021

شرکت طیف پردازان اسپادانا

ویرایش ۱,۰,۲۳

فهرست موضوعی مطالب

۱- الزامات قبل از راه اندازی مبدل

در این بخش به معرفی الزامات راه اندازی مبدل سری S1021 پرداخته می شود.

۱-۱ میزان ولتاژ

- ولتاژ صحیح ورودی دستگاه ۱۲-۲۴ ولت DC می باشد.
- دقت فرمایید که حداکثر ولتاژ کاری مبدل این سری ۲۴ ولت DC می باشد.
- لازم به ذکر است یک کابل برق در جعبه محصول قرار گرفته است(رنگ قرمز مثبت است).
- توجه فرمایید که قسمت مثبت در سمت چپ قرار گرفته است.

۱-۲ IP پیشفرض مبدل

- به زبان ساده آدرس IP Default Gateway همان آدرس IP صفحه پیکربندی تنظیمات مبدل است که در سمت شبکه LAN قرار دارد.

IP Default Gateway : 192.168.1.100

۱-۳ وسایل جانبی مورد نیاز

- کابل LAN متصل شده بین کامپیوتر و مبدل

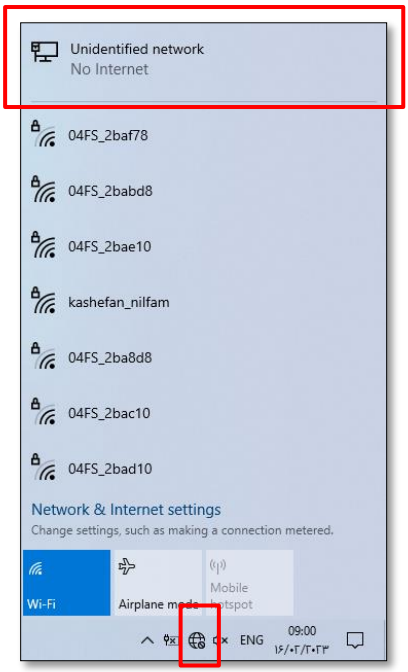
جهت توضیحات بیشتر پیرامون سایر مشخصات فنی مبدل به کاتالوگ محصول مراجعه کنید.

۲- پنجره ی پیکر بندی تنظیمات مبدل

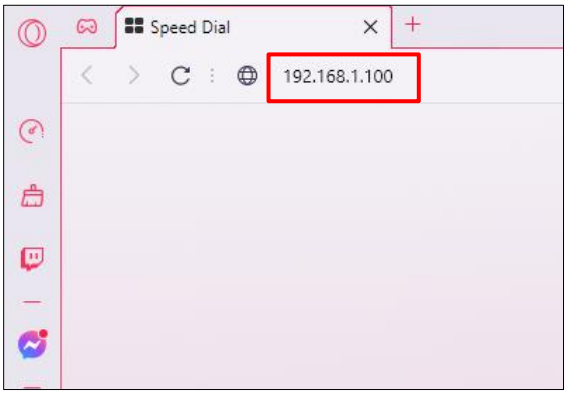
در این بخش به معرفی پنجره پیکربندی مبدل پرداخته می شود.

۲-۱ ورود به پنجره تنظیمات پیکربندی :

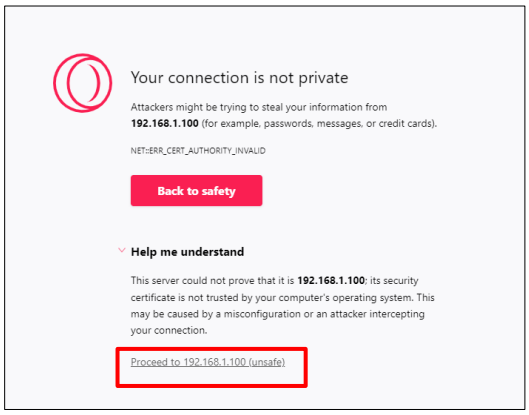
- می بایست الزامات گفته شده در فصل گذشته را فراهم کنید.
- از اتصال صحیح کابل برق اطمینال حاصل کنید.
- از اتصال کابل LAN بین کامپیوتر و مبدل اطمینال حاصل کنید.
- اگر به وای فای دیگری متصل هستید ، از آن شبکه خارج شوید.



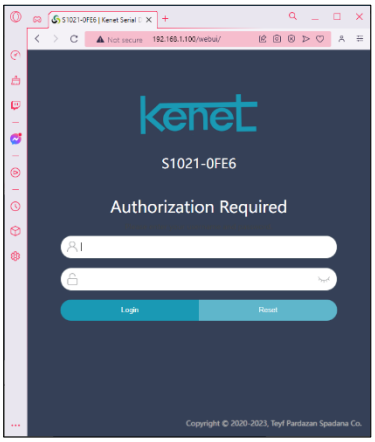
- ممکن است پس از اتصال به مودم، آیکن بخش اینترنت ویندوز شما عدم وجود اینترنت را نشان دهد.
- مطمئن شوید که کارت شبکه سیستم شما، مبدل را شناخته باشد.
- سپس مرورگر خور را باز کرده و در نوار آدرس مرورگر خود، IP Default Gateway مبدل را وارد کنید(۱۹۲.۱۶۸.۱.۱۰۰).



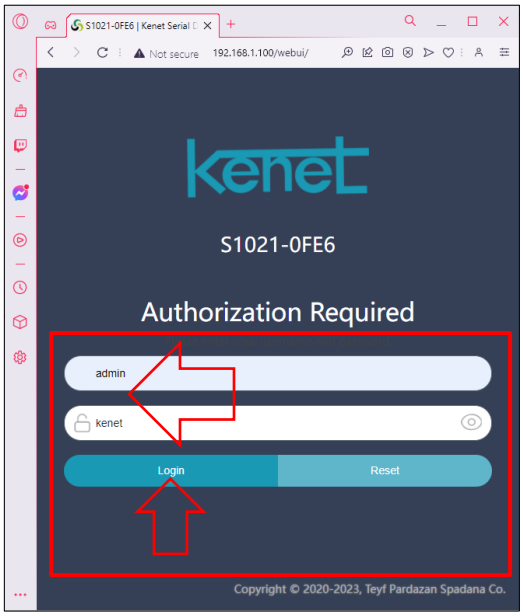
- ممکن است مرورگر، هشدار غیرایمن بودن صفحه را به شما بدهد؛ در این صورت شما، ادامه به صورت غیر ایمن را انتخاب کنید.



- در نهایت تب ورود به پیکربندی تنظیمات مبدل یا صفحه ی INTERFACE مبدل نمایش داده خواهد شد.



- برای ورود به صفحه ی پیکربندی لازم است نام کاربری و رمز عبور را وارد کنید .



- به صورت پیشفرض مقادیر زیر را وارد کنید :

  نام کاربری admin

  رمز عبور kenet

- رمز عبور به حروف بزرگ و کوچک حساس است.

- در نهایت در صورت وارد کردن مقادیر صحیح ، به صفحه پیکربندی تنظیمات مبدل وارد می شوید.

۲-۲ معرفی بخش های اصلی پنجره رابط کاربری

در این بخش به توضیح اجمالی و مختصر هر یک از بخش ها می پردازیم.

- بخش STATUS
- بخش SYSTEM
- بخش SERVICES
- بخش NETWORK

۲-۲-۱ بخش STATUS

- این بخش یک سری اطلاعات کلی پیرامون تنظیمات رابط به ما می دهد.
- هم چنین می توان فیلد های مبدل را بررسی اجمالی کرد.

۲-۲-۲ بخش SYSTEM

- کلیه کارهایی که به عنوان یک ادمین می توان روی مبدل پیاده کنیم.
- اطلاعات و تنظیمات پیرامون فریمورک ، پشتیبان گیری و راه اندازی مجدد در این قسمت قرار دارد.

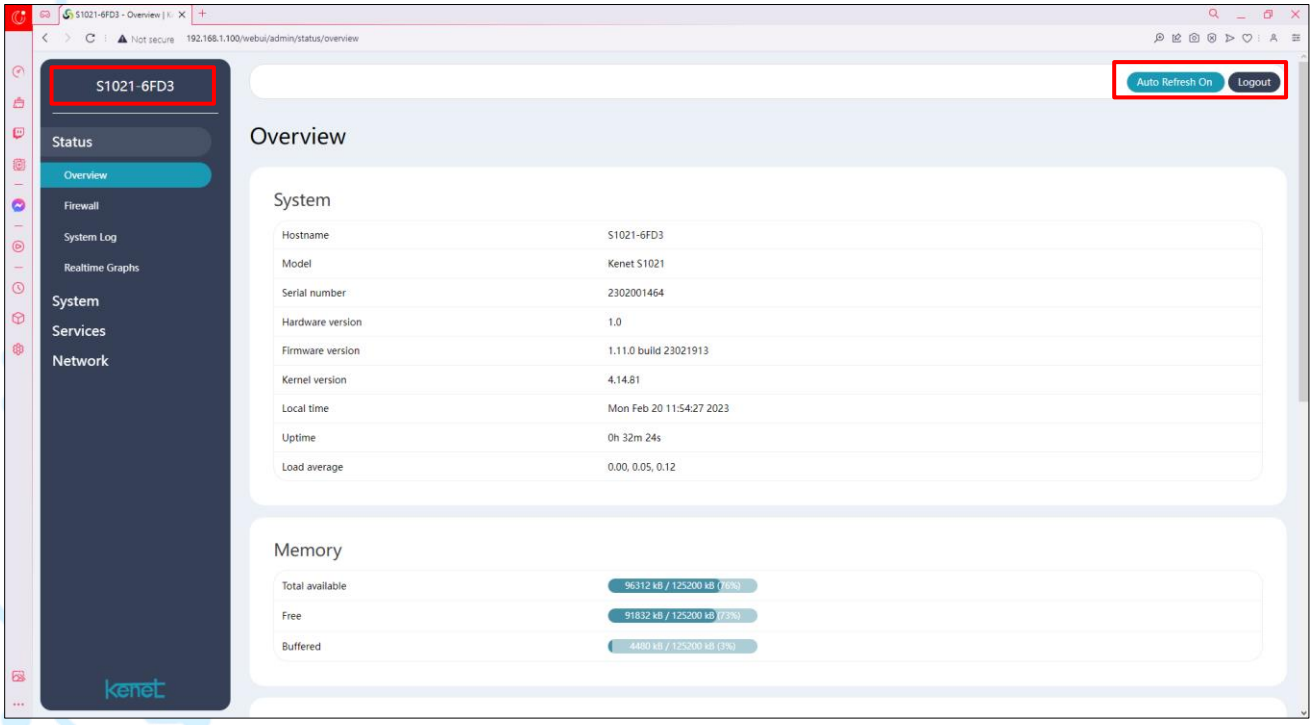
۲-۲-۳ بخش SERVICES

- کلیه سرویس هایی که این مبدل ارائه می دهد ، در این بخش قرار دارد.
- تنظیمات پیرامون پورت های RS232 وRS485 ، سرویس ها ، SNMP و VPN در این قسمت قرار دارد.

۲-۲-۴ بخش NETWORK

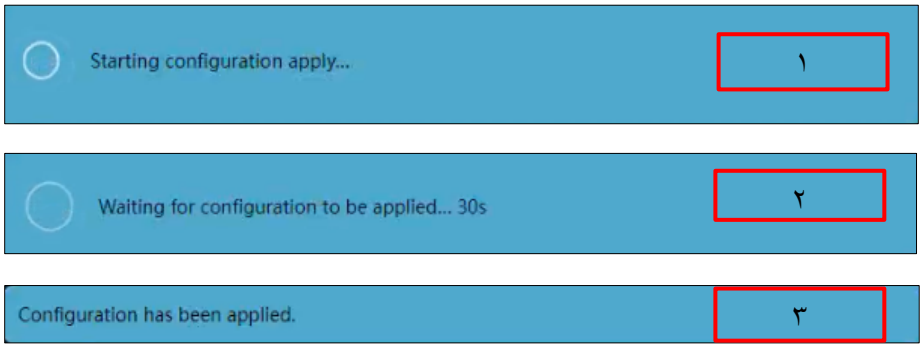
- تنظیمات پیرامون شبکه در این قسمت قرار دارد.
- تنظیماتی از جمله عوض کردن IP پیشفرض ، تعریف مد کاری مبدل ، IP های اختصاص داده شده توسط مبدل ، مسیر های تعریف شده توسط LAN ، PORT FORWARDS در این بخش قرار دارد.

۲-۳ توضیحات جانبی پنجره پیکربندی



- در بالای صفحه گزینه ای برای فعال و غیر فعال کردن به روزرسانی صفحه قرار گرفته است.
- Host Name مبدل در بالای صفحه سمت چپ قرار گرفته است ، که برای هر مبدل یکتاست.
-

- در هر قسمت ، ممکن است تغییراتی را لحاظ نمایید اگر قصد ایجاد چندین تغییر در یک صفحه را دارید ، صرفا کافی است پس از انجام هر تغییر گزینه Save را بزنید ؛ سپس در پایان گزینه Save & Apply را انتخاب نمایید.
- پس از زدن گزینه Save & Apply پیغامی به شما نمایش داده می شود که روند اعمال تغییرات را به شما نشان می دهد.

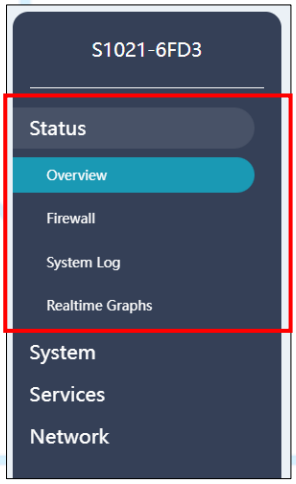


- در نظر داشته باشید درصورت انجام ندادن عملیات و تغییر خاصی پس از چند ثانیه ، صفحه پیکربندی تنظیمات بسته می شود و احتیاج به ورود مجدد دارید.

۳- بخش STATUS

در این بخش به معرفی بخش STATUS مبدل پرداخته می شود.

۳-۱ قسمت های بخش STATUS

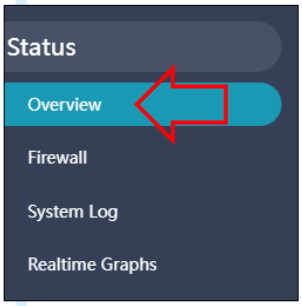


- قسمت Overview
- قسمت Firewall
- قسمت System Log
- قسمت Realtime Graphs

۳-۲ قسمت Overview

۳-۲-۱ معرفی

این بخش اطلاعات و توضیحاتی پیرامون دسته بندی های زیر ارائه می دهد :

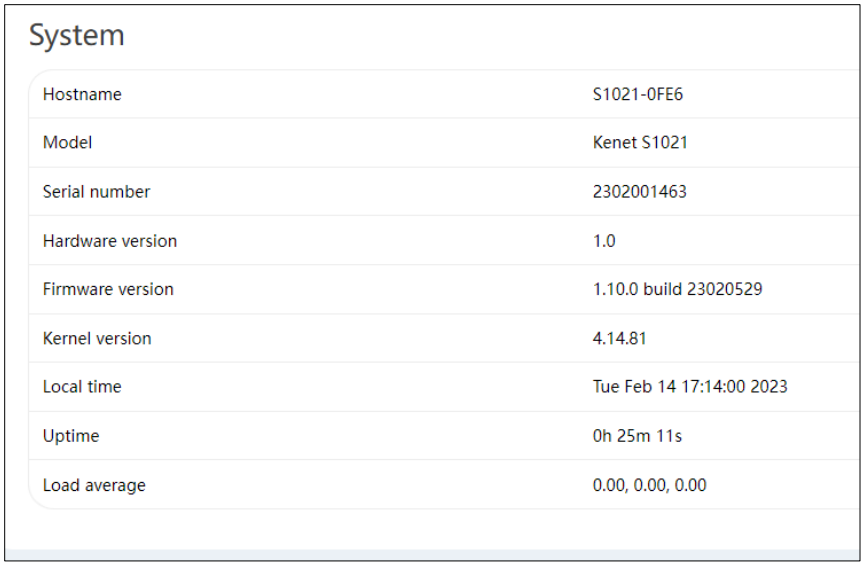


- زیر بخش System
- زیر بخش Memory
- زیر بخش Network
- زیر بخش Active DHCP Leases
- زیر بخش Active DHCPv6 Leases

۳-۲-۲ زیر بخش System

این زیر بخش اطلاعات مشخصه ای مبدل را نمایش می دهد؛ این اطلاعات شامل موارد ذیل هستند:

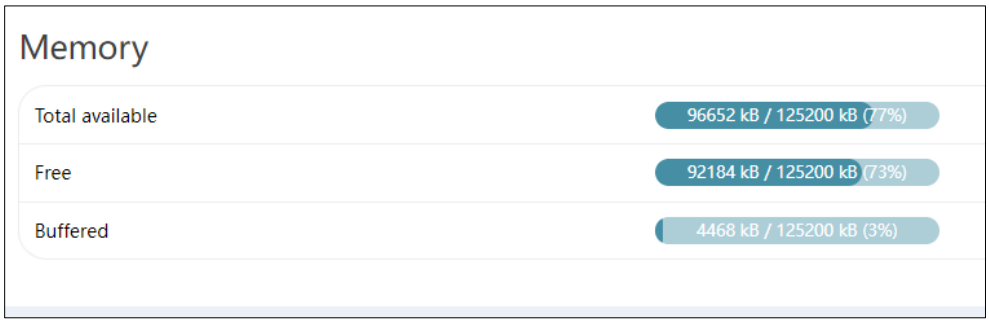
- Hostname : نام یکتای مبدل
- Model : مدل مبدل
- Serial number : سریال یکتا محصول
- Hardware version : نسخه سخت افزار مبدل
- Firmware version : نسخه برنامه مبدل
- Kernel version : نسخه پوسته لینوکس مبدل
- Local time : منطقه زمانی مبدل
- Uptime : زمان روشن بودن مبدل
- Load average : میانگین بار پردازنده



۳-۲-۳ زیر بخش Memory

اطلاعات حافظه دستگاه در قالب موارد ذیل، قابل مشاهده هستند :

- Total available : مجموع فضای موجود مبدل
- Free : میزان فضای ازاد حافظه مبدل
- Buffered : میزان فضای میانگیر استفاده شده

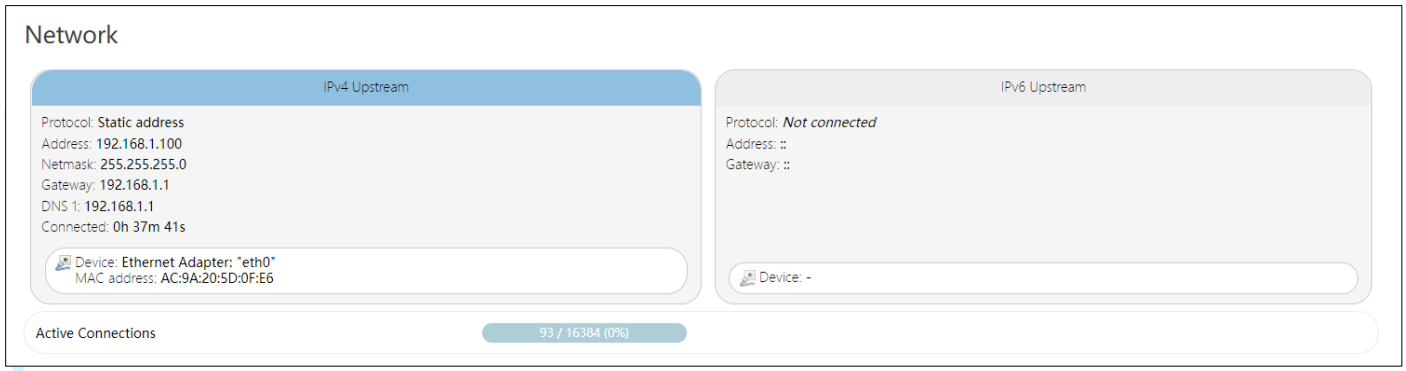


۳-۲-۴ زیر بخش Network

اطلاعات مشخصه ای شبکه مبدل، را به ۲ صورت IPv4 و IPv6 نشان می دهد ؛

- Protocol : پروتکل IP استفاده شده
- Address : ادرس IP مبدل
- Netmask : SUBNETMASK
- Gateway : ادرس GETEWAY
- DNS 1 : ادرس DNS

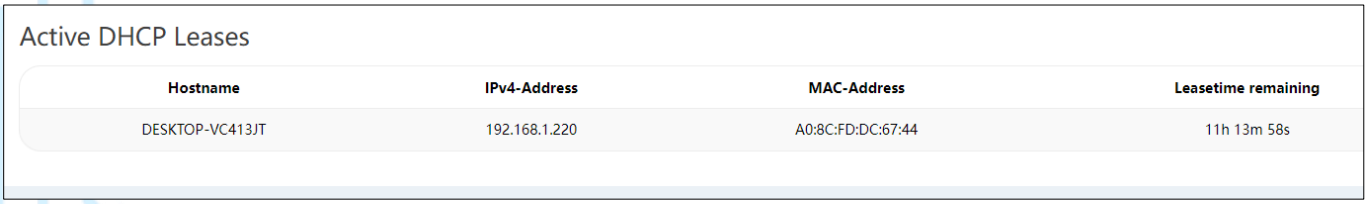
- Connected : زمان متصل شدن مبدل
- Device : نوع بستر ارتباطی مبدل با کامپیوتر
- MAC address : ادرس MAC مبدل
- Active Connections : تعداد اتصالات فعال



۳-۲-۵ زیر بخش Active DHCP Leases

به ازای هر دستگاه متصل به مبدل، ۴ مولفه زیر را نمایش می دهد:

- Hostname : نام یکتا هر دستگاه متصل به مبدل
- IPv4-Address : ادرس IP ویرایش ۴ دستگاه متصل
- MAC-Address : ادرس MAC دستگاه متصل
- Leasetime remaining : زمان باقی مانده از اختصاص ip



۳-۲-۶ زیر بخش Active DHCPv6 Leases

مشابه زیر بخش قبلی؛ به ازای هر دستگاه متصل به مبدل، ۴ مولفه زیر را نمایش می دهد:

- Host : نام یکتا هر دستگاه متصل به مبدل
- IPv6-Address : ادرس IP ویرایش ۶ دستگاه متصل
- DUID : شناسه اختصاصی dhcp
- Leasetime remaining : زمان باقی مانده از اختصاص ip

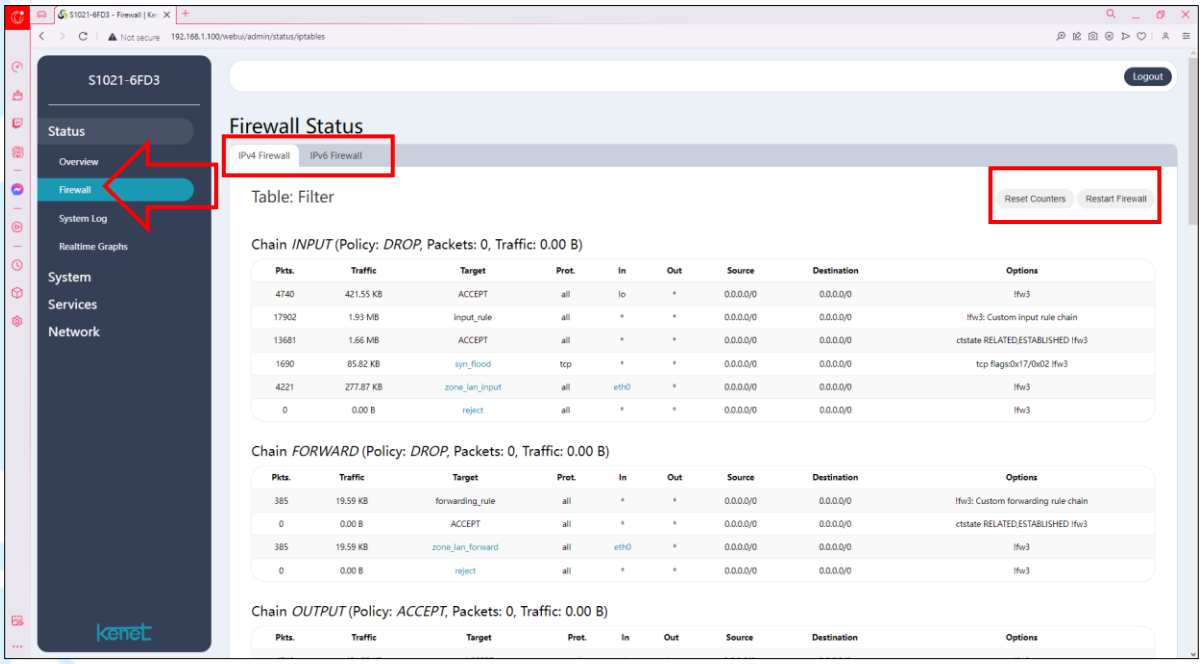
Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
DESKTOP-VC413JT	fd3d:e996:d82b::1c0/128	000100012a697b1fa08cfddc6744	11h 15m 30s

۳-۳ قسمتFirewall

۳-۳-۱ معرفی

- این بخش Firewall مبدل است .
- این بخش ترافیک رد و بدل شده در شبکه را کنترل می کند.
- به نوعی تضمین کننده امنیت دستگاه، با جداسازی داده امن از ناحیه ی نا امن و کنترل ارتباطات بین این دو است.
- در مبدل در ۲ قسمت مجزا برای IP های ویرایش ۴ و ۶ به صورت جدول تعبیه شده است.
- لازم به ذکر است که می توان Firewall را بازنشانی یا صفر نمود (از قسمت بالا، سمت راست).



۳-۳-۲ اجزای بخش IPV4 FIREWALL

- از ۴ جدول برای نمایش دیتا ها استفاده می کند:
- Filter : جدول پیشرفض مورد استفاده iptables است که برای فیلتر کردن پکت های ورودی و خروجی مورد استفاده قرار میگیرد.
- NAT : جدولی است که به منظور اعمال تنظیمات NAT مورد استفاده قرار میگیرد.

- Mangle : از طریق این جدول میتوان تغییراتی را در header پکت ها ایجاد نمود.
- Raw : این جدول این امکان را فراهم میکند تا با پکت ها قبل از این که کرنل بر اساس state آنها اقدامی انجام دهد کارکرد.
- هر جدول شامل تعدادی chain هستند که هر کدام گروهی از rule ها را در خود نگه میدارند. که میتوانند سیستمی باشند یا توسط کاربر ساخته شود.

۱-۲-۳-۳ جدول Filter

بخش FILTER از جدول های زیر تشکیل شده است :

- Chain INPUT :

مربوط به دسته هایی که مقصد ان ها خود Firewall است.

Chain *INPUT* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
841	74.01 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	!fw3
2354	228.24 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom input rule chain
1677	174.95 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED !fw3
206	10.46 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 !fw3
677	53.29 KB	zone_lan_input	all	eth0	*	0.0.0.0/0	0.0.0.0/0	!fw3
0	0.00 B	reject	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3

- Chain FORWARD :

مربوط به دسته هایی که از Firewall عبور می کنند.

Chain *FORWARD* (Policy: *DROP*, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
48	2.44 KB	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom forwarding rule chain
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED !fw3
48	2.44 KB	zone_lan_forward	all	eth0	*	0.0.0.0/0	0.0.0.0/0	!fw3
0	0.00 B	reject	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3

- Chain OUTPUT :

مربوط به دسته هایی که مبدا ان ها Firewall هستند.

Chain *OUTPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
841	74.01 KB	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	!fw3
2928	1.05 MB	output_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom output rule chain
2151	1020.40 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED !fw3
777	52.16 KB	zone_lan_output	all	*	eth0	0.0.0.0/0	0.0.0.0/0	!fw3

Chain reject -

Chain *reject* (References: 2)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	!fw3 reject-with tcp-reset
0	0.00 B	REJECT	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3 reject-with icmp-port-unreachable

Chain syn_flood -

Chain *syn_flood* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
206	10.46 KB	RETURN	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 limit: avg 25/sec burst 50 !fw3
0	0.00 B	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3

Chain zone_lan_dest_ACCEPT -

Chain *zone_lan_dest_ACCEPT* (References: 2)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
825	54.59 KB	ACCEPT	all	*	eth0	0.0.0.0/0	0.0.0.0/0	!fw3

Chain zone_lan_forward -

Chain *zone_lan_forward* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
48	2.44 KB	forwarding_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom lan forwarding rule chain
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT !fw3: Accept port forwards
48	2.44 KB	zone_lan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3

Chain zone_lan_input -

Chain *zone_lan_input* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
677	53.29 KB	input_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom lan input rule chain
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate DNAT !fw3: Accept port redirections
677	53.29 KB	zone_lan_src_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3

Chain zone_lan_output -

Chain *zone_lan_output* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
777	52.16 KB	output_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom lan output rule chain
777	52.16 KB	zone_lan_dest_ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3

Chain zone_lan_src_ACCEPT -

Chain *zone_lan_src_ACCEPT* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
677	53.29 KB	ACCEPT	all	eth0	*	0.0.0.0/0	0.0.0.0/0	ctstate NEW,UNTRACKED !fw3

۲-۲-۳-۳ جدول NAT

بخش NAT از جدول های زیر تشکیل شده است :

Chain PREROUTING -

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 1565, Traffic: 125.70 KB)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
1565	125.70 KB	prerouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom prerouting rule chain
1565	125.70 KB	zone_lan_prerouting	all	eth0	*	0.0.0.0/0	0.0.0.0/0	!fw3

Chain POSTROUTING -

Chain *POSTROUTING* (Policy: *ACCEPT*, Packets: 2168, Traffic: 144.99 KB)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
2168	144.99 KB	postrouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom postrouting rule chain
2076	139.55 KB	zone_lan_postrouting	all	*	eth0	0.0.0.0/0	0.0.0.0/0	!fw3

Chain zone_lan_postrouting -

Chain *zone_lan_postrouting* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
2076	139.55 KB	postrouting_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom lan postrouting rule chain

Chain zone_lan_prerouting -

Chain *zone_lan_prerouting* (References: 1)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
1565	125.70 KB	prerouting_lan_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	!fw3: Custom lan prerouting rule chain

۳-۳-۲-۳ جدول های Mangle و Raw :

این جدول ها هم مشابه جدول های قبلی، درصورت وجود رکورد قابل مشاهده هستند.

Table: Mangle

No chains in this table

Table: Raw

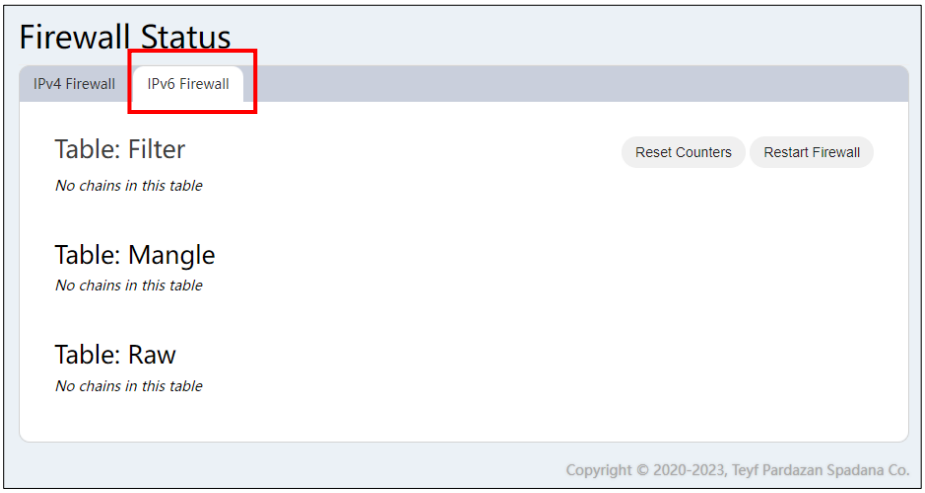
No chains in this table

۳-۳-۳ اجزای بخش IPV6 FIREWALL

- از ۳ جدول برای نمایش دیتا ها استفاده می کند:
- Filter : جدول پیشرفض مورد استفاده iptables است که برای فیلتر کردن پکت های ورودی و خروجی مورد استفاده قرار میگیرد.
- Mangle : از طریق این جدول میتوان تغییراتی را در header پکت ها ایجاد نمود.

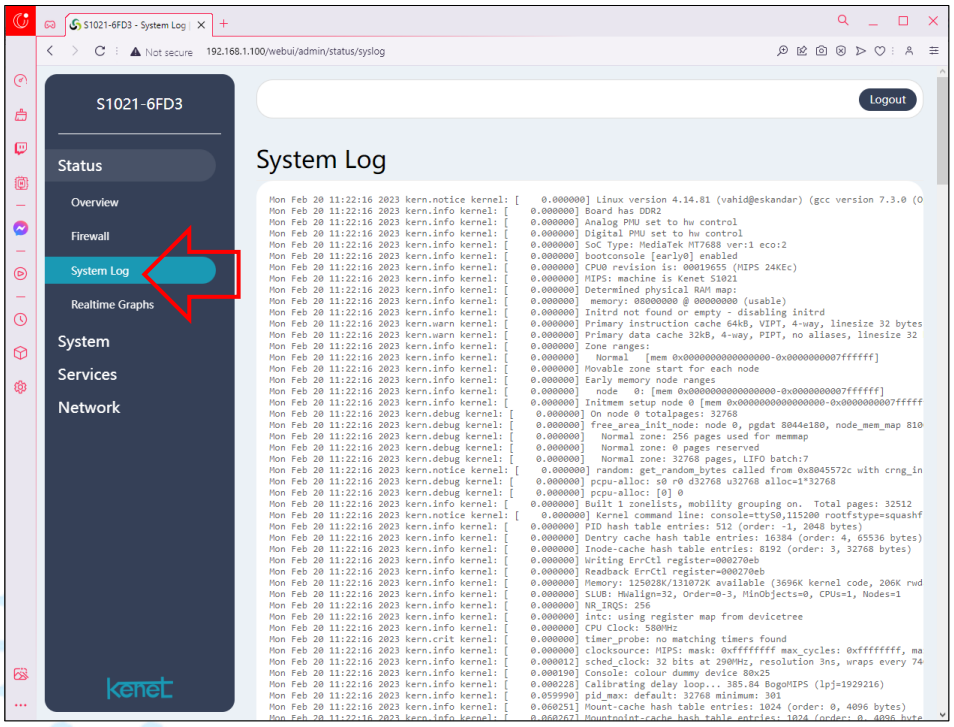
- Raw : این جدول این امکان را فراهم میکند تا با پکت ها قبل از این که کرنل بر اساس state آنها اقدامی انجام دهد کارکرد.

مشابه قسمت قبلی ، درصورت وجود رکورد ، این جدول ها قابل نمایش خواهند بود.



۳-۴ قسمت System Log

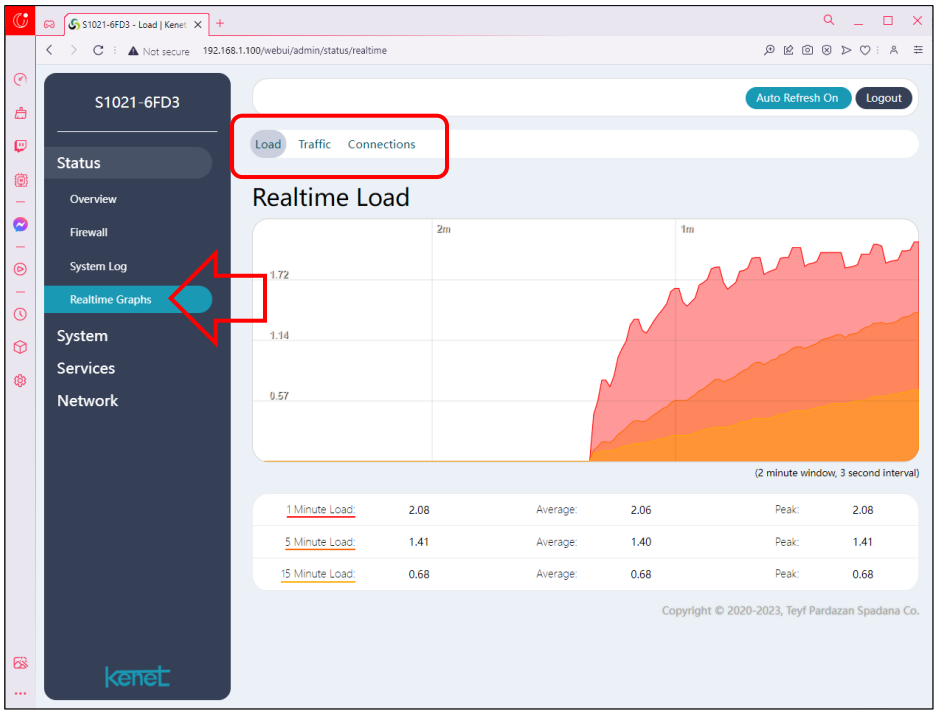
- تاریخچه فعالیت های اتفاق افتاده در مبدل را نمایش می دهد.



۳-۵ قسمت Realtime Graphs

۳-۵-۱ معرفی Realtime Graphs

- به صورت توصیفی اطلاعاتی از دیتا رد و بدل شده در مبدل را نمایش می دهد.



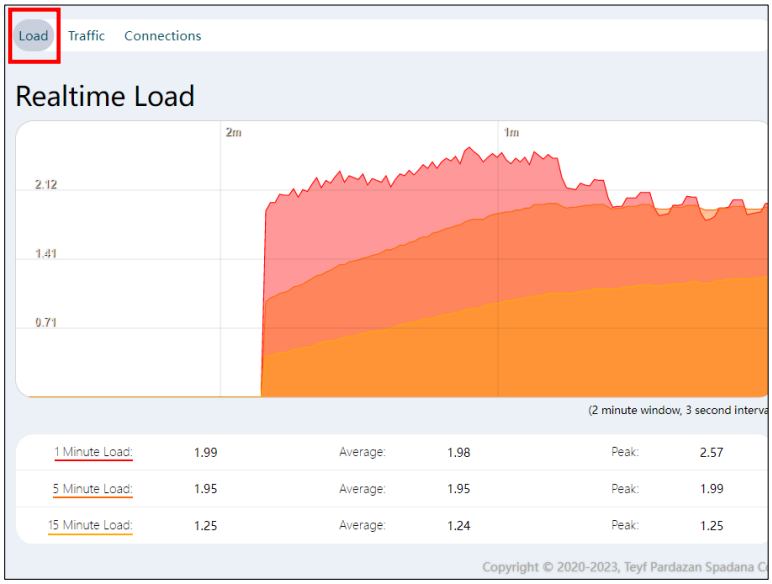
۳-۵-۲ اجزای قسمت Realtime Graphs

از ۳ قسمت تشکیل شده :

- Load : نمودار مقدار بارگزاری مبدل فاصله ۲ دقیقه ای اخیر
- Traffic : نمودار میزان ترافیک لحظه ای مبدل در فاصله ۲ دقیقه اخیر
- Connection : نمودار میزان اتصال TCP و UDP مبدل

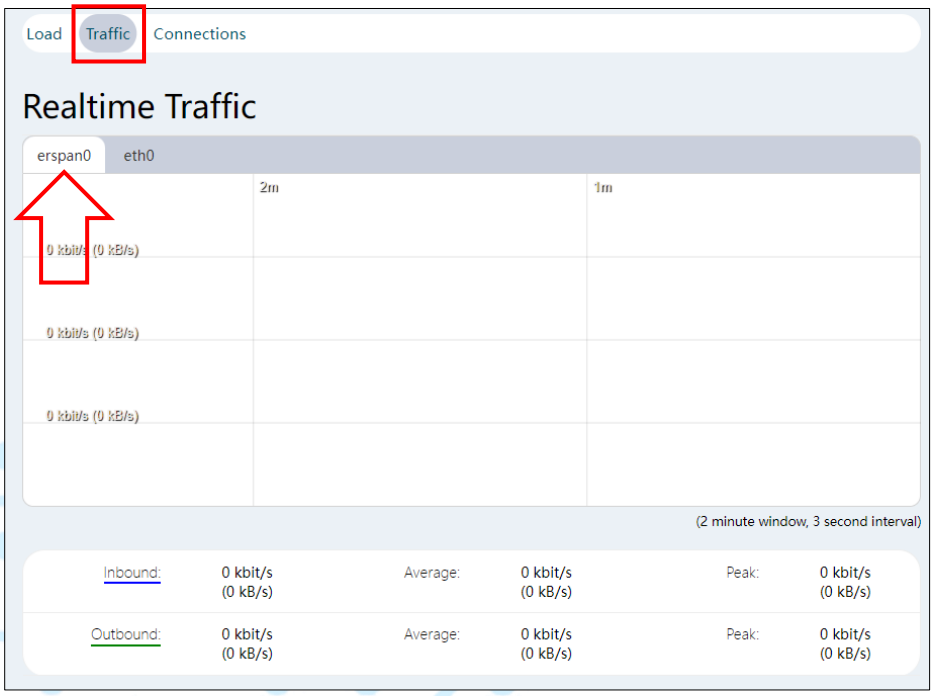
۳-۵-۳ نمودار Load

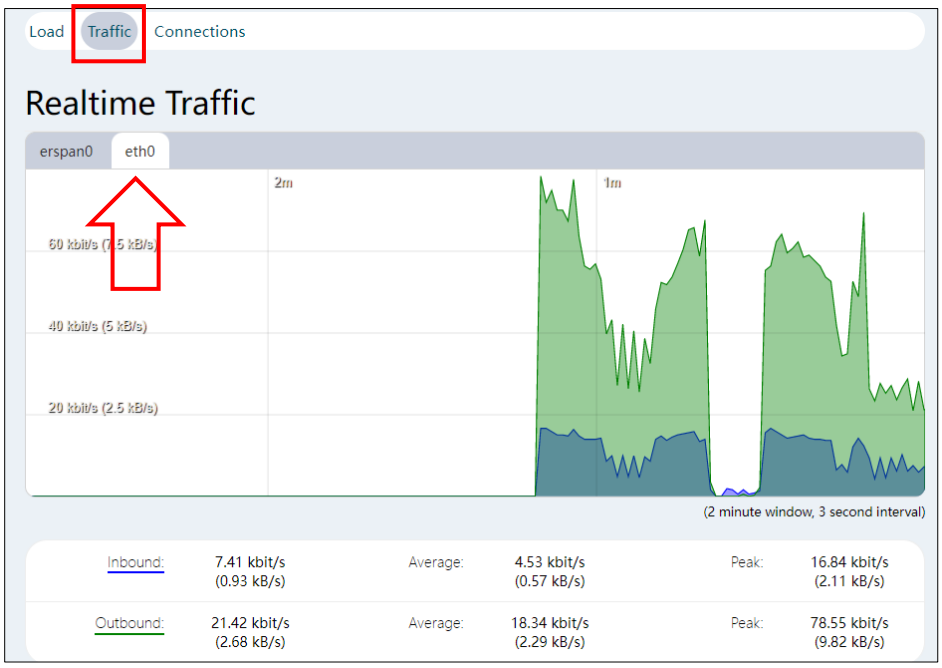
- نمودار مقدار بارگزاری مبدل فاصله ۲ دقیقه ای اخیر



۳-۵-۴ نمودار Traffic

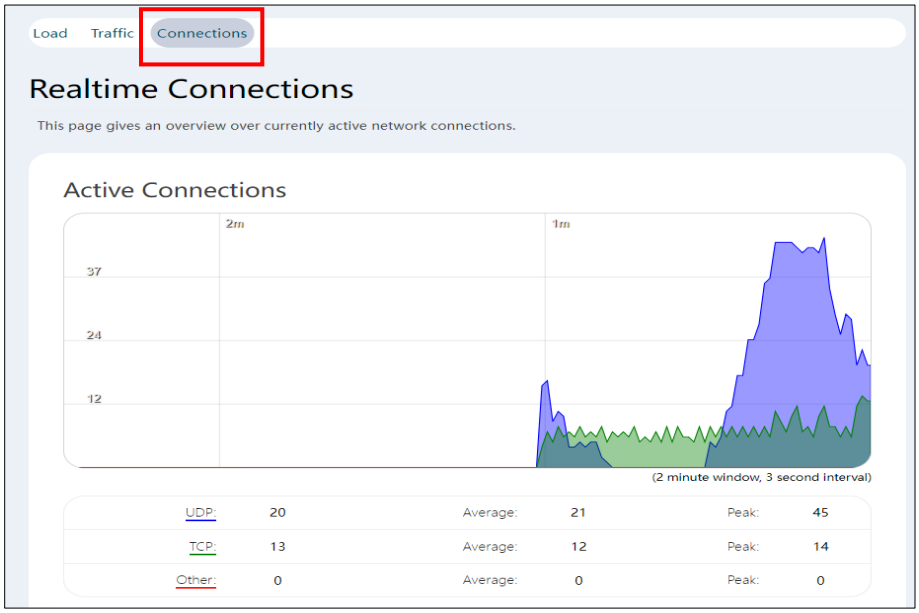
- نمودار میزان ترافیک لحظه ای مبدل در فاصله ۲ دقیقه اخیر
- به ۲ صورت erspan0 و eth0 قابل مشاهده است.



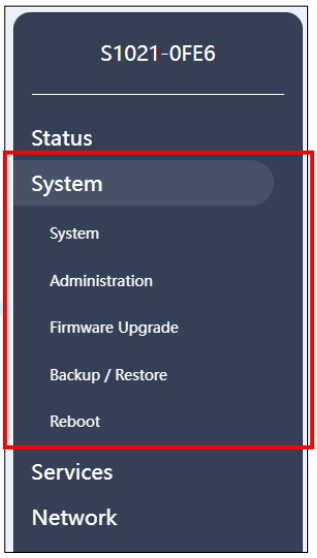


۵-۵-۳ نمودار Connection

- نمودار میزان اتصال TCP و UDP مبدل
- هم چنین این اطلاعات به صورت جدول نیز نمایش داده می شود.



Network	Protocol	Source	Destination	Transfer
IPV4	TCP	DESKTOP-VC413JT.lan:4915	S1021-0FE6.lan:443	14.78 KB (32 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4919	S1021-0FE6.lan:443	13.31 KB (31 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4917	S1021-0FE6.lan:443	4.02 KB (19 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4925	S1021-0FE6.lan:443	4.00 KB (19 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4921	S1021-0FE6.lan:443	3.99 KB (19 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4927	S1021-0FE6.lan:443	3.17 KB (12 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4926	S1021-0FE6.lan:443	2.58 KB (16 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4916	S1021-0FE6.lan:443	2.58 KB (16 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4924	S1021-0FE6.lan:443	2.55 KB (15 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4918	S1021-0FE6.lan:443	2.55 KB (15 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4914	S1021-0FE6.lan:443	2.55 KB (15 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4922	S1021-0FE6.lan:443	2.55 KB (15 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4920	S1021-0FE6.lan:443	2.55 KB (15 Pkts.)
IPV4	UDP	DESKTOP-VC413JT.lan:137	192.168.1.255:137	390 B (5 Pkts.)
IPV4	UDP	S1021-0FE6.lan:33167	192.168.1.1:53	284 B (4 Pkts.)
IPV4	UDP	S1021-0FE6.lan:54662	192.168.1.1:53	284 B (4 Pkts.)
IPV4	UDP	S1021-0FE6.lan:50602	192.168.1.1:53	213 B (3 Pkts.)

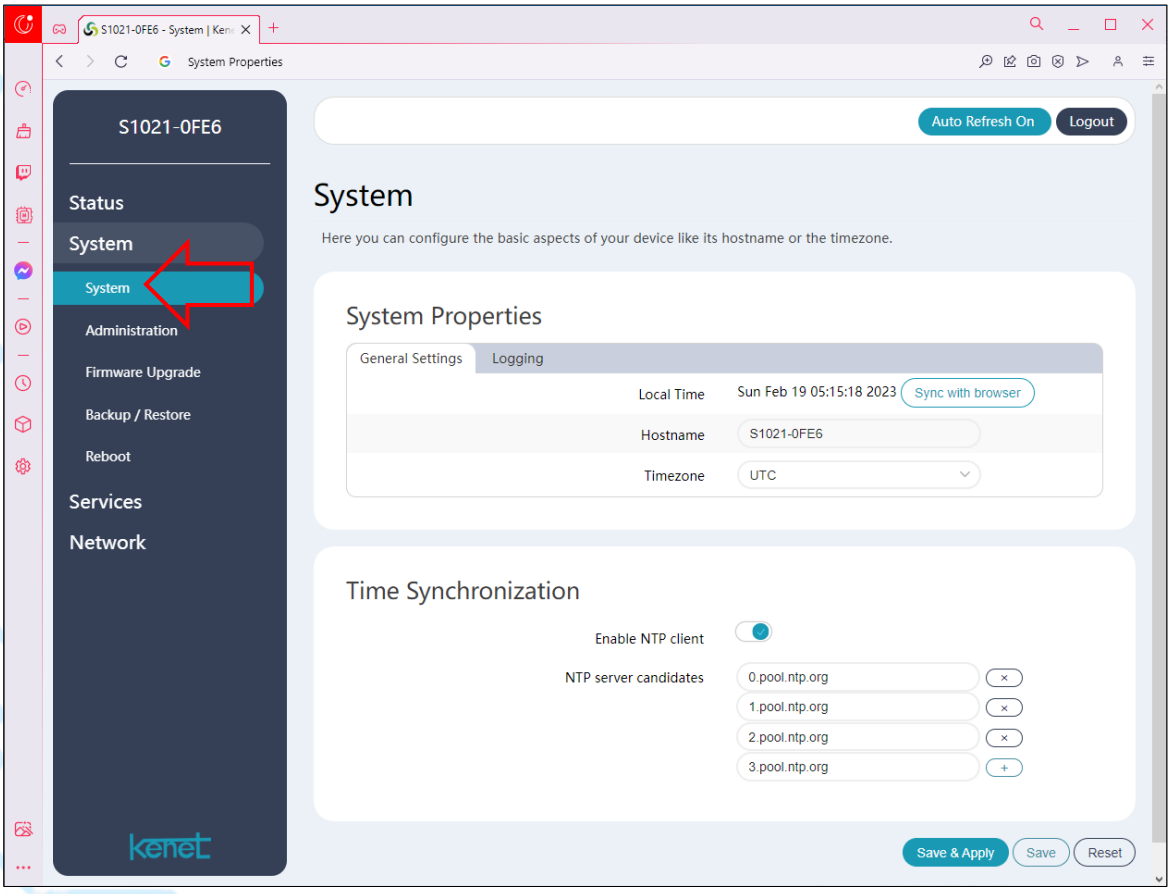


۴- بخش System

در این بخش به معرفی بخش System مبدل پرداخته می شود.

۴-۱ قسمت های بخش System

- قسمت System
- قسمت Adminstration
- قسمت Fireware Upgrade
- قسمت Backup / Restor
- قسمت Reboot



۴-۲ قسمت System

۴-۲-۱ معرفی System

- در این قسمت اطلاعات پایه ای دستگاه مانند منطقه زمانی ، نام میزبان را پیکربندی می کنید.
- این بخش از ۲ بخش تشکیل شده است.

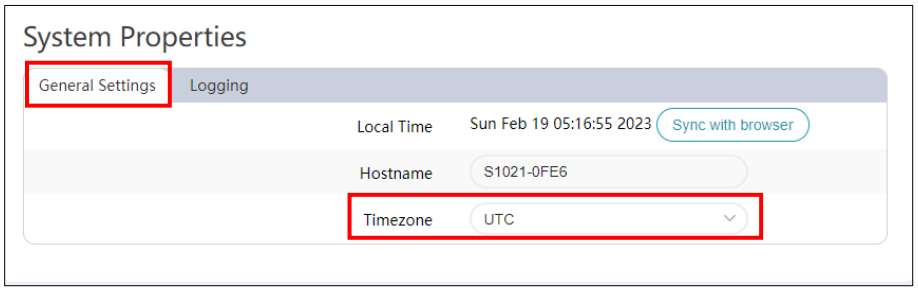
- System Properties : ویژگی های سیستم
- Time Synchronization: همگام سازی زمانی

۴-۲-۲ زیر بخش System Properties

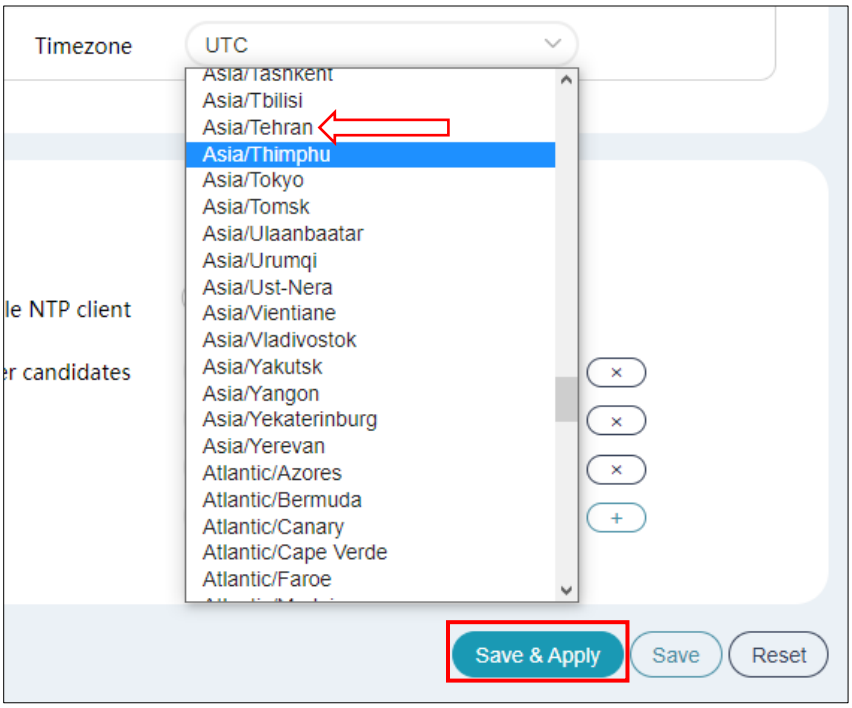
- این بخش از ۲ قسمت زیر تشکیل شده است.
- General Settings : تنظیمات کلی
- Logging : گزارشات سیستم

۴-۲-۲-۱ بخش General Settings

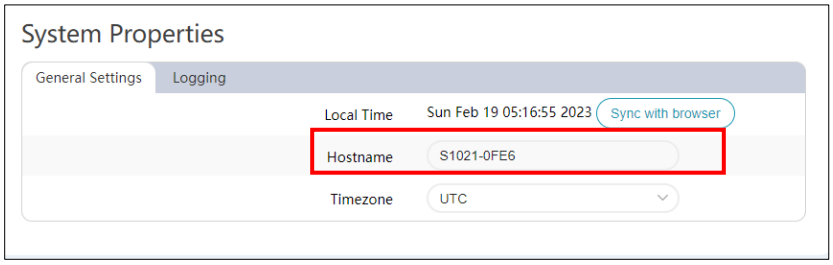
- از فیلد های زیر تشکیل شده است:
- Local Time : زمان محلی
- Hostname : نام مبدل(قابل تغییر)
- Timezone : منطقه زمانی (قابل تنظیم)



- می توانید منطقه زمانی خود را، با بازکردن منوی کشویی تنظیم نمایید.



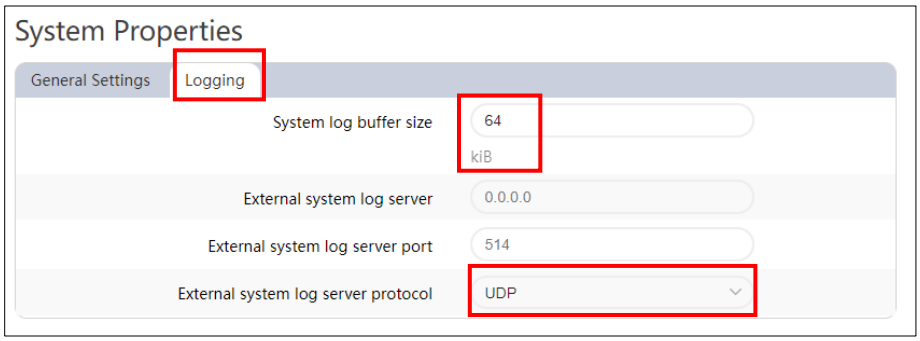
- ترجیحا منطقه زمانی تهران را انتخاب نمایید.
- هم چنین می توانید نام مبدل خود را نیز تغییر دهید.



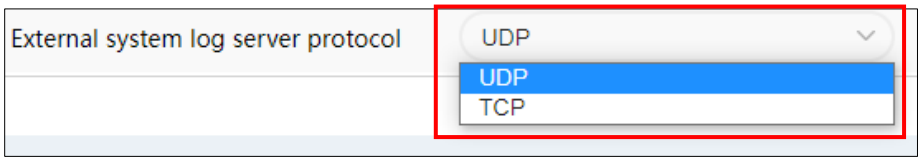
- بعد از اعمال تغییرات، گزینه Save & Apply را انتخاب نمایید.

۲-۲-۲-۴ بخش Logging

- از فیلد های زیر تشکیل شده است:
- System log buffer size : اندازه لاگ بافر بر حسب kiB
- External system log server : لاگ سرور خارجی
- External system log server port : پورت لاگ سرور خارجی
- External system log server protocol :پروتکل لاگ سرور خارجی

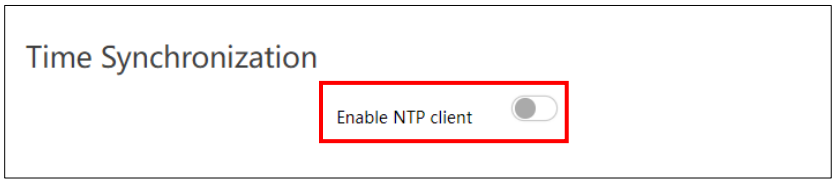


- اندازه لاگ بافر برحسب kiB قابل تغییر است.
- پروتکل هم بین ۲ حالت TCP و UDP قابل تغییر است.

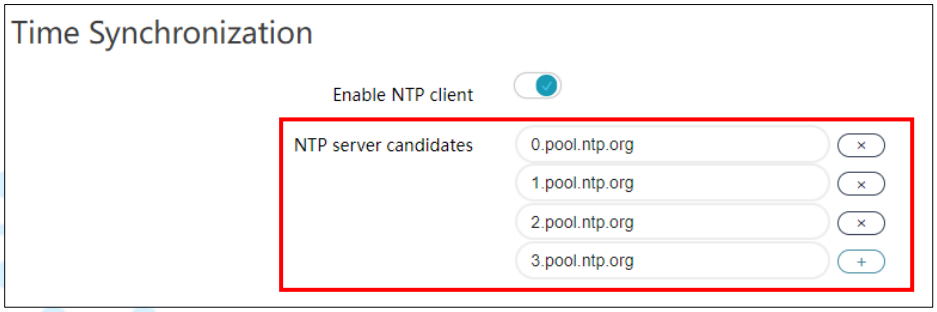


۳-۲-۴ زیر بخش Time Synchronization

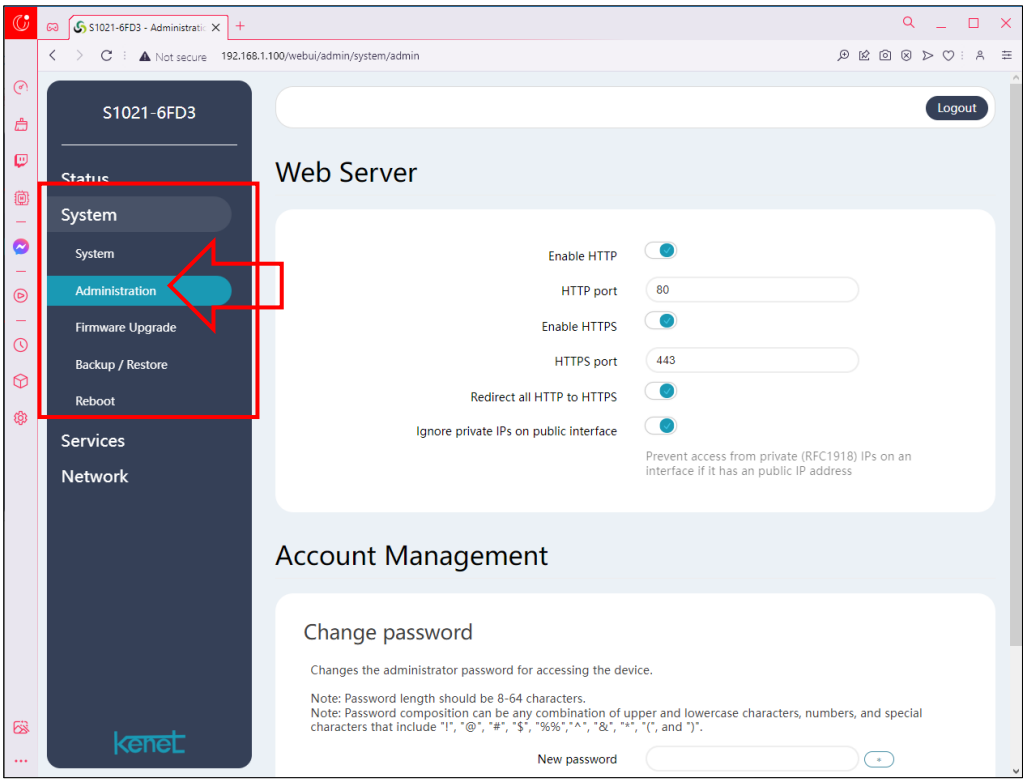
- این بخش از ۲ قسمت زیر تشکیل شده است.
- Enable NTP client : فعال یا غیرفعال کردن NTP client
- NTP server candidates : کاندید های NTP server



- در صورت فعال کردن این بخش ، فیلد های زیر برای شما نمایش داده می شود.



۴-۳ قسمت Adminstration

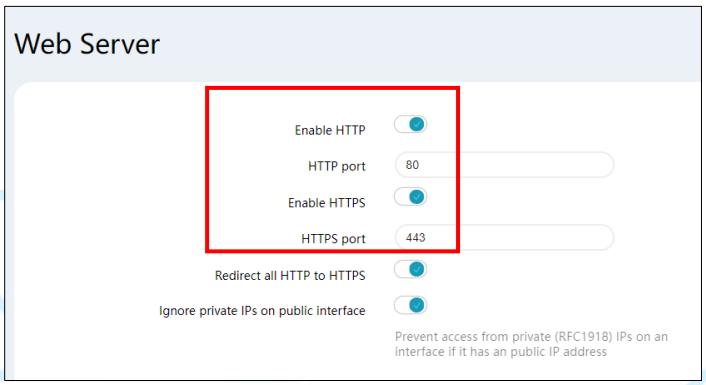


۴-۳-۱ معرفی Adminstration

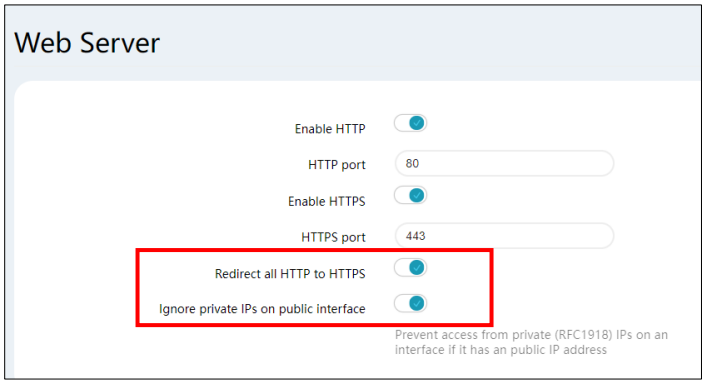
- این بخش از ۲ قسمت مهم تشکیل شده است :
- Web Server : بخش فعال سازی یا غیرفعال سازی http وhttps
- Account Management: بخش تغییر رمز

۴-۳-۲ بخش Web Server

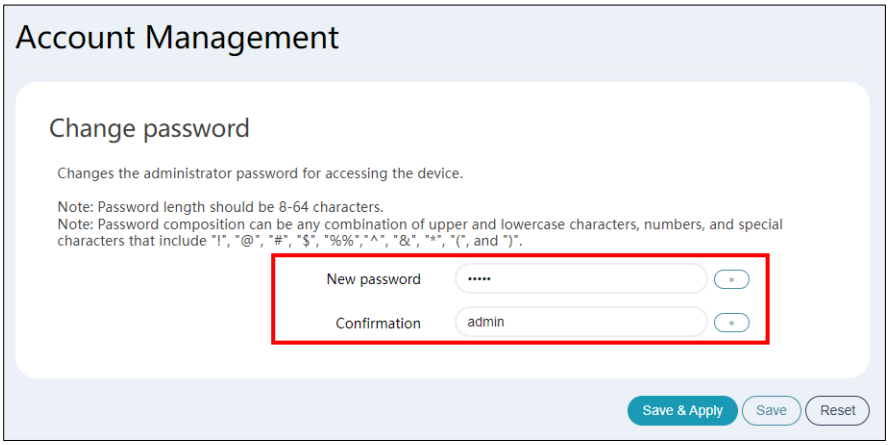
- در این بخش می توانید پروتکل های HTTP و HTTPS را فعال یا غیر فعال نمایید.



- هم چنین می توانید درخواست های HTTP را به HTTPS هدایت کنید.
- در صورت استفاده از http و https باید پورت مورد نظر را باز کنید(بخش ؟).
- هم چنین می توانید فعال بودن یا نبودن ERROR RFC 1918 را مدیریت کنید.

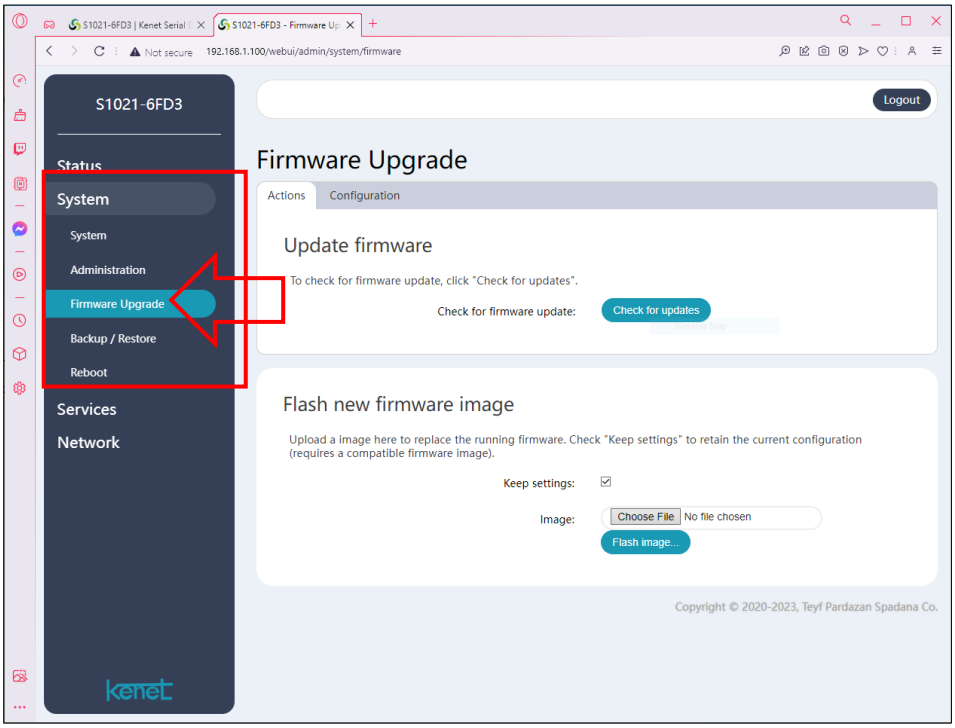


۴-۳-۳ بخش Account Management



- در این بخش می توان پسورد خود را تغییر دهید.
- پس از وارد کردن پسورد جدید ، یکبار دیگر ان را جهت تایید ، دوباره وارد نمایید.
- گزینه ای برای نمایش پسورد تایپ شده در سمت راست با علامت ستاره فراهم گردیده است.
- پس از اعمال تنظیمات مورد نظر خود، تنظیمات را ذخیره و اعمال نمایید.
- بهتر است از کاراکتر های خاص برای افزایش امنیت پسورد خود استفاده کنید.
- کاراکتر های خاص قابل استفاده :
  - "!" ,"@" ,"#" ,"$" ,"%" ,"^" ,"&" ,"*" ,")" ,"("

۴-۴ قسمت Firmware Upgrade



۴-۴-۱ معرفی Fireware Upgrade

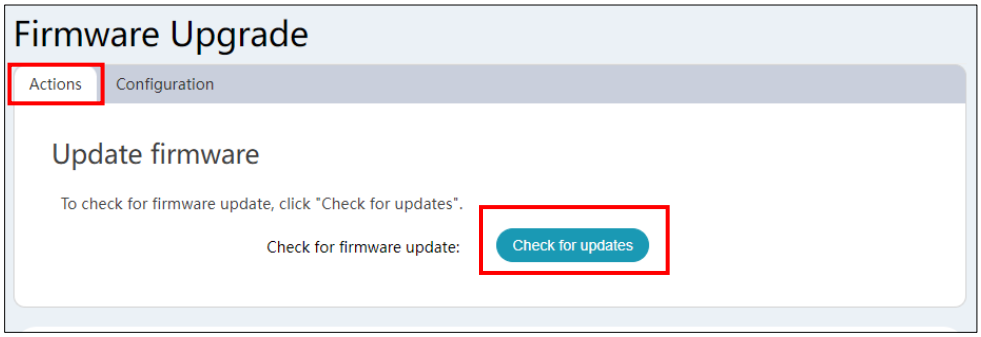
- با کمک این بخش می توانید برنامه مبدل را به روز رسانی نمایید.
- این بخش از ۲ قسمت زیر تشکیل شده است :
  - Actions : بررسی به روز رسانی
  - Configuration : تنظیمات به روز رسانی

۴-۴-۲ بخش Actions

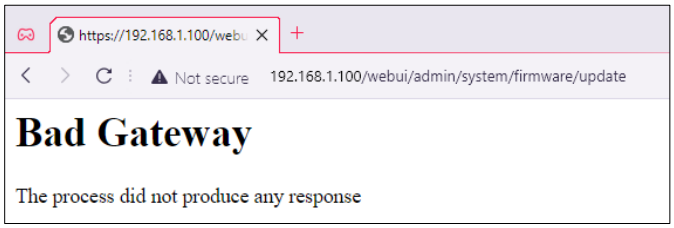
- این بخش از ۲ زیر بخش زیر تشکیل شده است :
  - Update firmware : بررسی به روزرسانی موجود
  - Flash new firmware image : بروزرسانی توسط فایل با پسوند .img

۴-۴-۲-۱ بخش Update firmware

- در صورت وجود به روز رسانی ، ان را دانلود کرده و سپس مبدل را به روز می کند.
- برای بررسی به روز رسانی ، از اتصال مبدل به اینترنت اطمینال حاصل فرمایید.

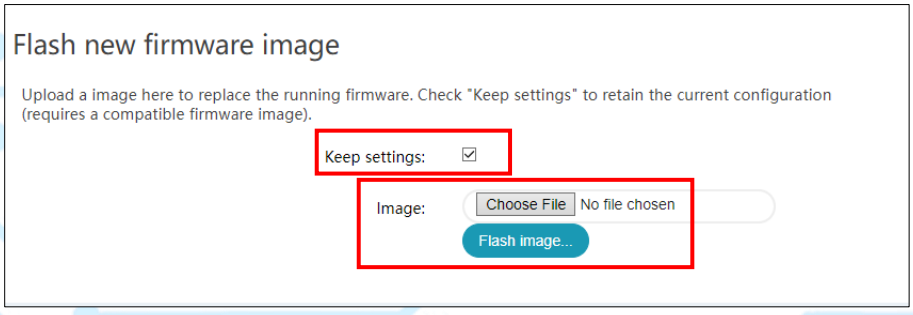


- در صورت عدم دسترسی مبدل به اینترنت صفحه زیر به شما نشان داده خواهد شد.



۲-۲-۴-۴ بخش Flash new firmware image

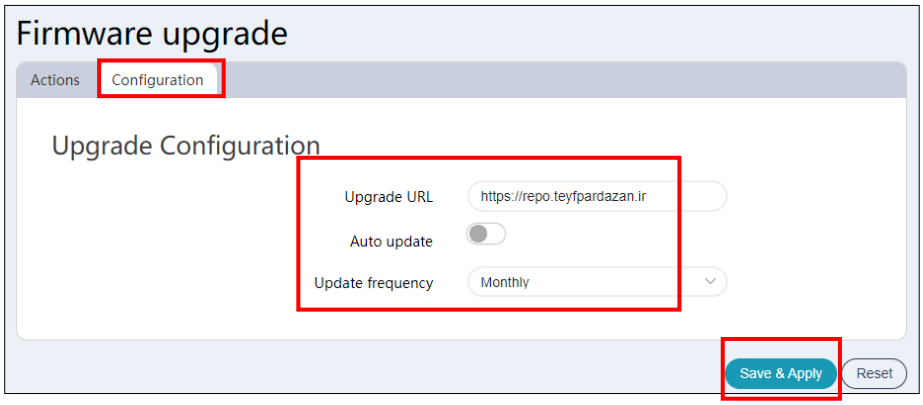
- اگر فایل با پسوند img. به روزسانی را در اختیار داشته باشید، می توانید از طریق این بخش ، مبدل را به روز رسانی کنید.
- فایل با پسوند img. را از پشتیبانی شرکت دریافت نمایید(بخش؟).
- در نظر داشته باشید که فایل با پسوند img. شما صحیح و اخرین نسخه باشد.
- هم چنین برای حفظ تنظیمات خود قبل از به روز رسانی توسط این روش ، می توانید تیک حفظ تنظیمات را هم فعال نمایید .



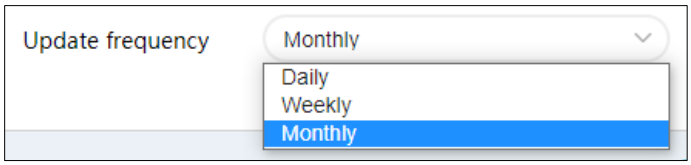
۳-۴-۴ بخش Configuration

- تنظیمات مربوط به به روز رسانی را در این مرحله می توانید تنظیم کنید.
- از ۳ قسمت تشکیل شده است :

- Upgrade URL : ادرس سایتی که بروز رسانی خودکار از ان دریافت می شود.
- Auto update : فعال یا غیر فعال کردن ابدیت خودکار مبدل
- Update frequency : تعیین بازه ابدیت خودکار

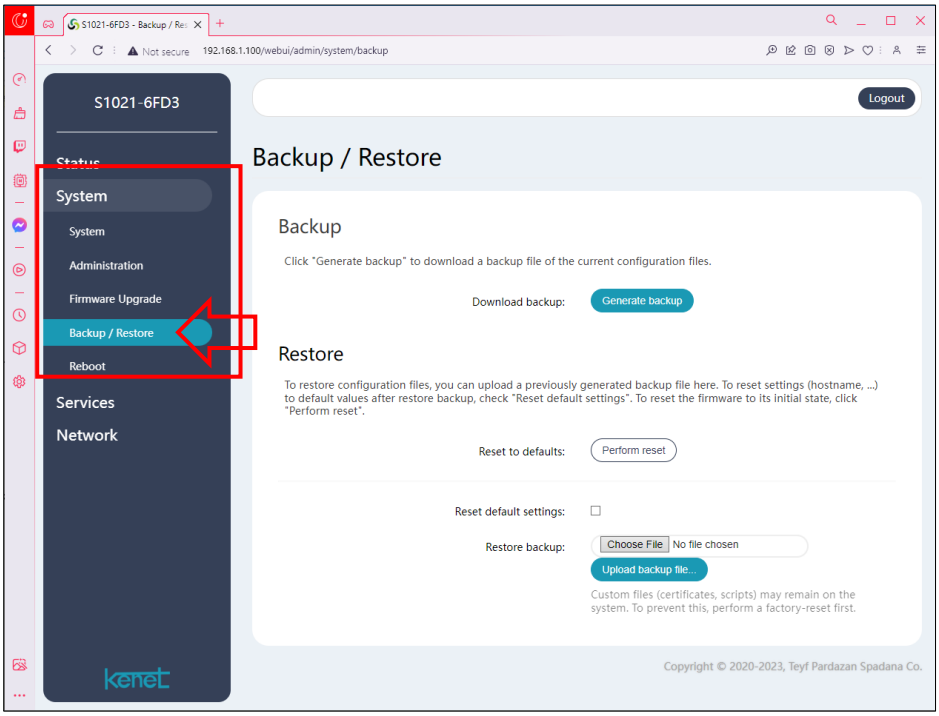


- که بازه بررسی ابدیت خودکار می تواند روزانه ، هفتگی و یا ماهانه تنظیم شود.



- دقت فرمایید که پس از انجام تغییرات مورد نظر، حتما گزینه ذخیره و اعمال تغییرات را انتخاب نمایید.

۴-۵ قسمت Backup / Restor

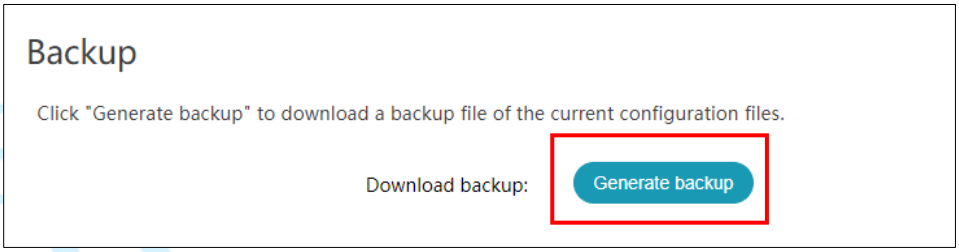


۴-۵-۱ معرفی Backup / Restor

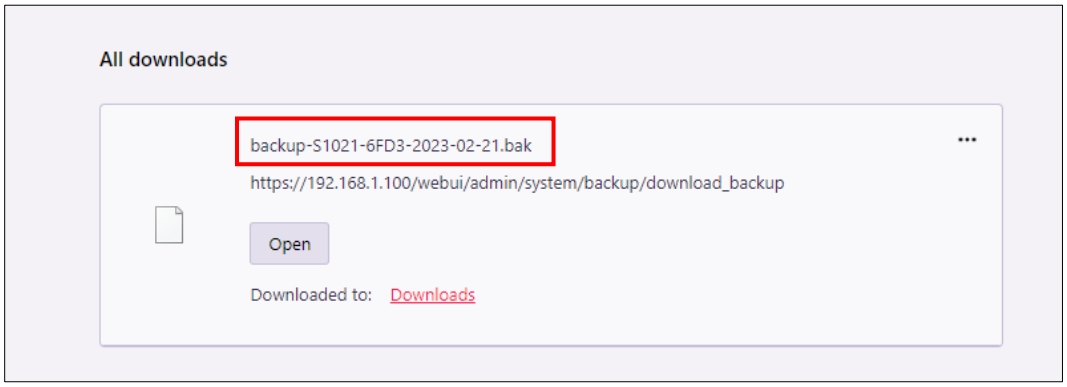
- با کمک این بخش می توانید از تنظیمات نسخه پشتیبان تهیه نمایید.
- این بخش از ۲ قسمت زیر تشکیل شده است :
  - Backup : ایجاد فایل پشتیبان از تنظیمات
  - Restore : بازگردانی تنظیمات پشتیبانی گرفته شده

۴-۵-۲ بخش Backup

- به کمک این بخش می توانید از تنظیمات ، پشتیبان گیری کنید.

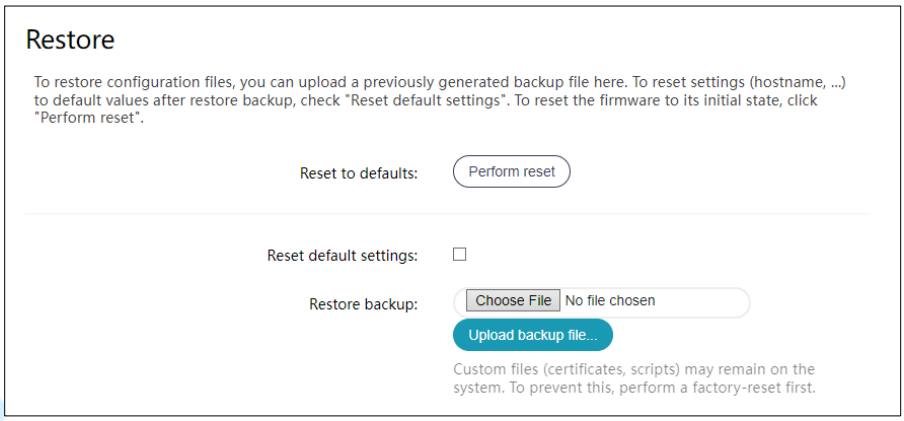


- در صورت انتخاب گزینه ایجاد فایل پشتیبان فایلی با پسوند .bak در قسمت دانلود مرورگر ایجاد می شود.



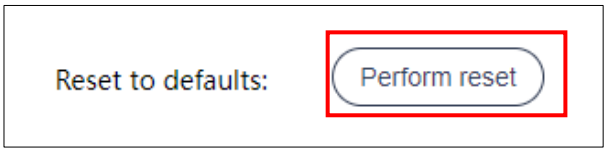
۴-۵-۳ بخش Restore

- به کمک این بخش می توانید فایل پشتیبان تنظیمات مورد نظر خود را، در سیستم بارگزاری و اعمال نمایید.
- از ۳ بخش مهم تشکیل شده است :
  - Reset to defaults : بازیابی به تنظیمات کارخانه
  - Reset default settings : برگشت تنظیمات به مقدار پیشفرض
  - Restore backup : انتخاب فایل پشتیبان



۴-۵-۳-۱ بخش Reset to defaults

- برای بازگردانی تنظیمات به مقادیر پیشفرض گزینه Perform reset را انتخاب نمایید.
- در واقع این گزینه نقش بازگردانی به تنظیمات کارخانه را دارد.

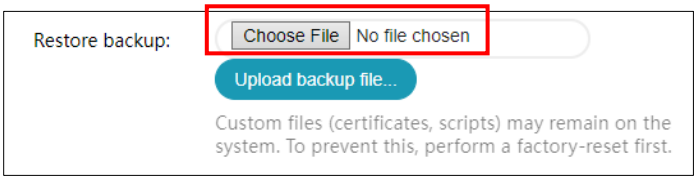


۴-۵-۳-۲ بخش Reset default settings

- با فعال کردن تیک این بخش تنظیمات پیشفرض بر روی مبدل ، بعد از بازیابی از فایل پشتیبانی به تنظیمات کارخانه اعمال می شود.

۴-۵-۳-۳ بخش Restore backup

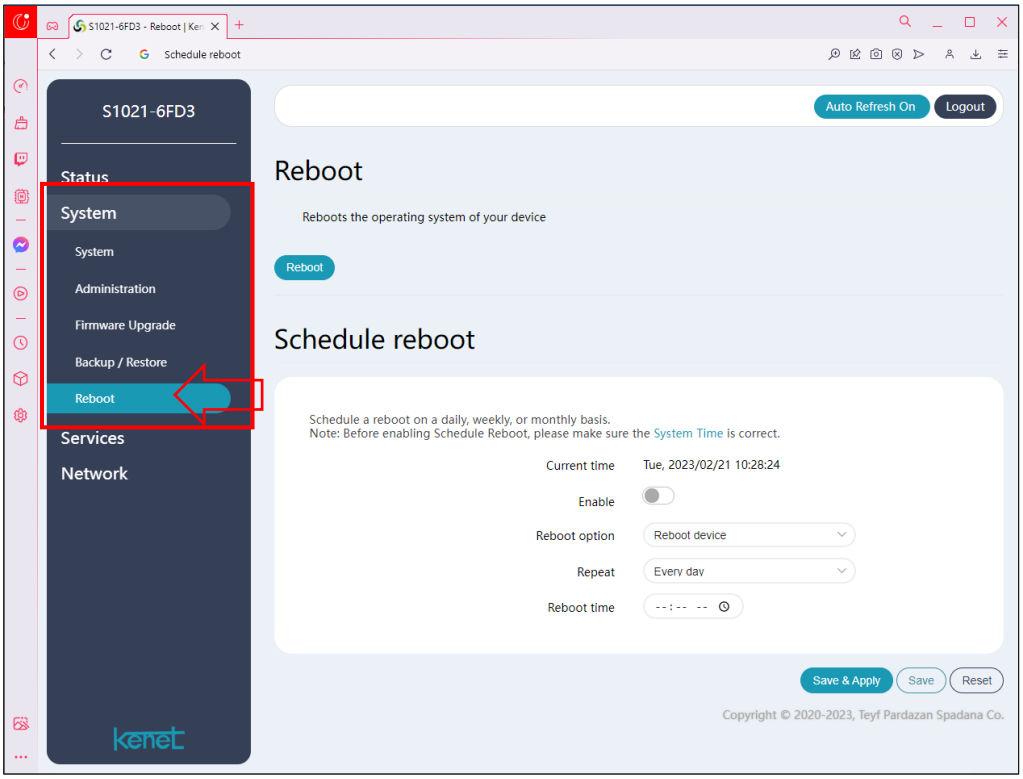
- از طریق این بخش می توانید فایل تنظیمات پشتیبان گرفته شده خود را انتخاب و بازیابی را شروع نمایید.



- در نظر داشته باشید فایل های سفارشی ممکن است در سیستم باقی بمانند، برای جلوگیری از این امر ابتدا یک بار بازیابی به تنظیمات کارخانه را انجام دهید.

- در صورتی که می خواهید یک بار تنظیمات را انجام دهید و بر روی چند مبدل فایل بکاپ تنظیمات را بازگردانی کنید ؛ در نظر داشته باشید که نام مبدل دستگاهی که در حال بازگردانی هستید ، به نام مبدل فایل پشتیبانی تغییر نام می دهد ؛ شما باید نام مبدل را تغییر دهید ؛ و یا تیک قسمت Reset default settings را فعال نمایید.؟

۴-۶ قسمت Reboot

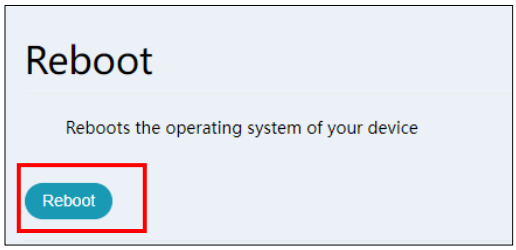


۴-۶-۱ معرفی

- به کمک این بخش می توانید مبدل خود را راه اندازی مجدد کنید.
- این بخش از ۲ قسمت تشکیل شده است :
  - Reboot : راه اندازی مجدد
  - Schedule reboot : راه اندازی مجدد زمان دار

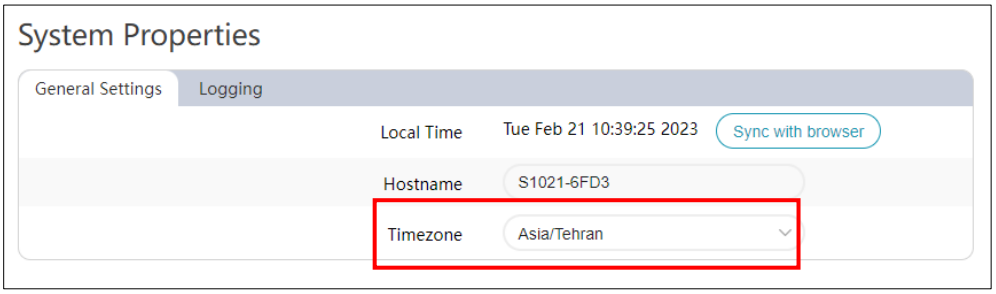
۴-۶-۲ بخش Reboot

- با انتخاب گزینه Reboot می توانید مبدل خود را راه اندازی مجدد کنید.

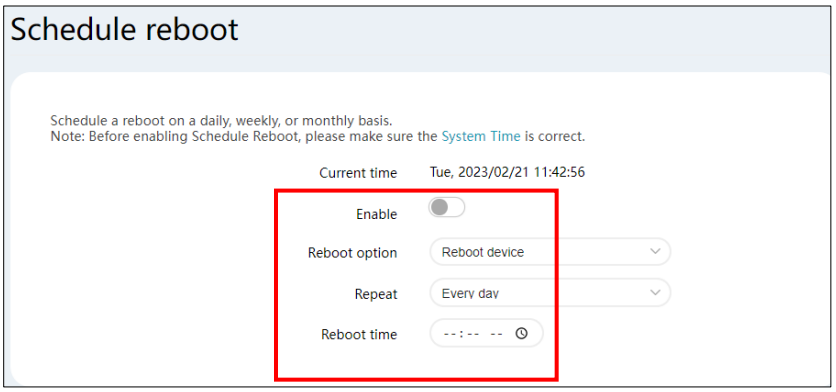


۳-۶-۴ بخش Schedule reboot

- در بخش می توانید زمان مشخصی را برای راه اندازی مجدد مبدل تنظیم کنید.
- لازم است قبل از انجام تنظیمات این بخش، منطقه زمانی خود را تنظیم کنید.
- برای تنظیم منطقه زمانی مراحل زیر را انجام دهید:
  - صفحه رابط کاربری مبدل را باز کنید.
  - از ۴ منوی سمت راست ، منوی دوم یعنی System را انتخاب کنید.
  - از زیر منو های باز شده System ، اولین زیر منو یعنی System را انتخاب کنید.
  - سپس از قسمت System Properties ، بخش General Settings را انتخاب کنید.
  - Timezone را روی منطقه زمانی مورد نظر، ترجیحا Asia/Tehran قرار دهید.
  - سپس در نهایت ، ذخیره و اعمال تنظیمات را انتخاب نمایید.
  - برای توضیحات دقیق تر می توانید به فصل System ، بخش System مراجعه کنید.

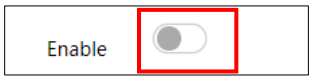


- این بخش از ۵ قسمت تشکیل شده است:
  - Current time : زمان و تاریخ جاری را نشان می دهد.
  - Enable : فعال یا غیر فعال سازی قابلیت راه اندازی زمان دار
  - Reboot option : نوع عملیات راه اندازی مجدد
  - Repeat : میزان دفعات تکرار راه اندازی مجدد
  - Reboot time : زمان هر راه اندازی مجدد

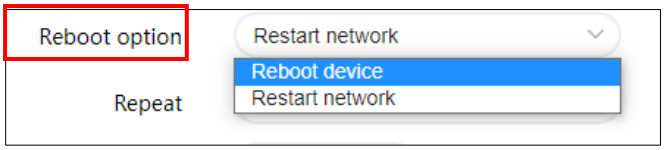


۴-۶-۴ مراحل راه اندازی مجدد زمان دار

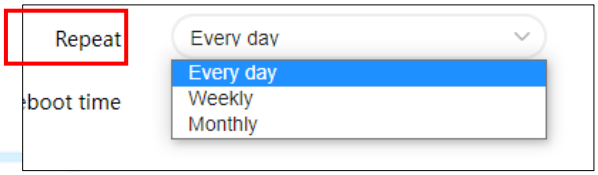
- منطقه زمانی خود را بر روی تهران (طبق بخش قبلی) تنظیم کنید.
- به وسیله گزینه دوم این بخش را فعال نمایید.



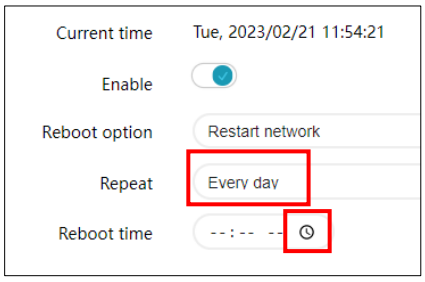
- نوع راه اندازی خود را مشخص کنید ، ۲ نوع راه اندازی تعریف شده است:
  - Reboot device : راه اندازی مجدد مبدل
  - Restart network : بازگردانی مجدد تنظیمات شبکه به حالت پیشفرض

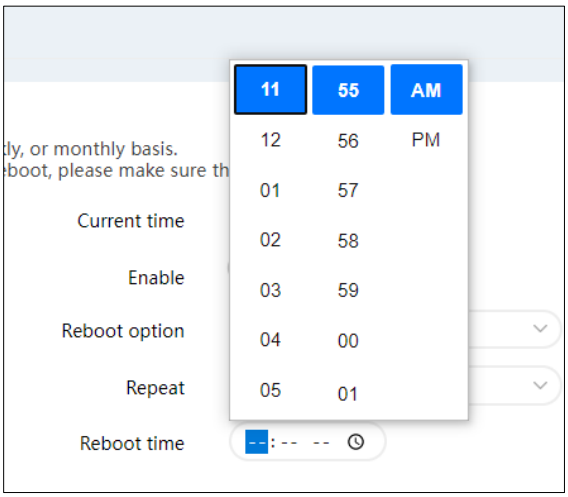


- در قسمت بعدی بازه میزان دفعات تکرار را مشخص کنید.
  - روزانه
  - ماهانه
  - هفتگی

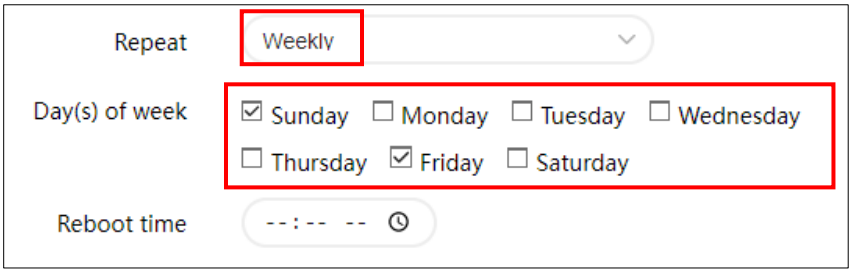


- در صورت انتخاب به صورت روزانه، در مرحله بعدی فقط احتیاج به ساعت روزانه خواهید داشت.
- برای انتخاب زمان ، کافی است روی ایکن ساعت انتخاب، و زمان مورد نظر را وارد نمایید.

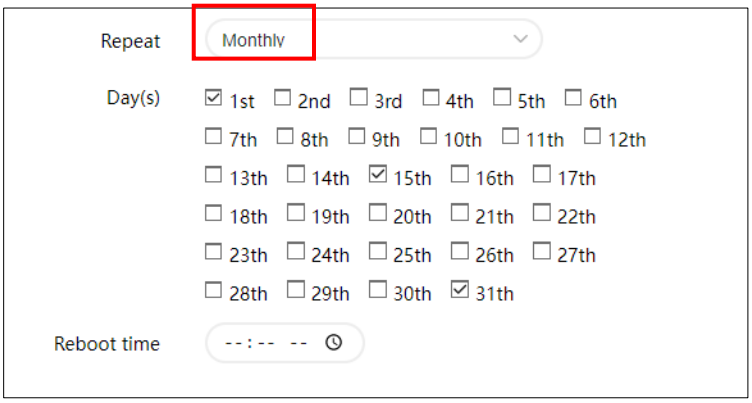




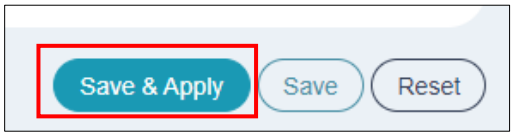
- دقت کنید که فرمت زمانی که وارد می کنید، ۱۲ ساعته است.
- اگر دفعات تکرار را ، هفتگی قرار دهید؛ می توانید روز های هفته مد نظر خود را انتخاب نمایید.
- سپس مانند مرحله قبل، زمان مورد نظر خود را تنظیم کنید.



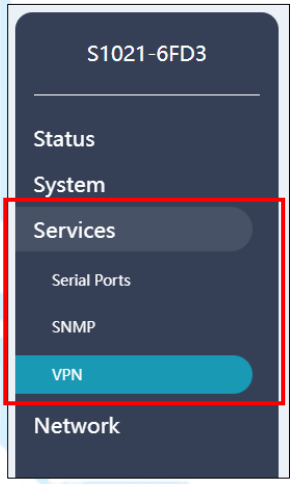
- در صورت انتخاب به صورت ماهانه هم، مشابه روش هفتگی می توانید روز های هفته مورد نظر خود را انتخاب کرده ؛ سپس زمان را تنظیم کنید.



- لازم به ذکر است که در پایان ، باید تغییرات را ذخیره و اعمال کنید.



۵- بخش SERVICES

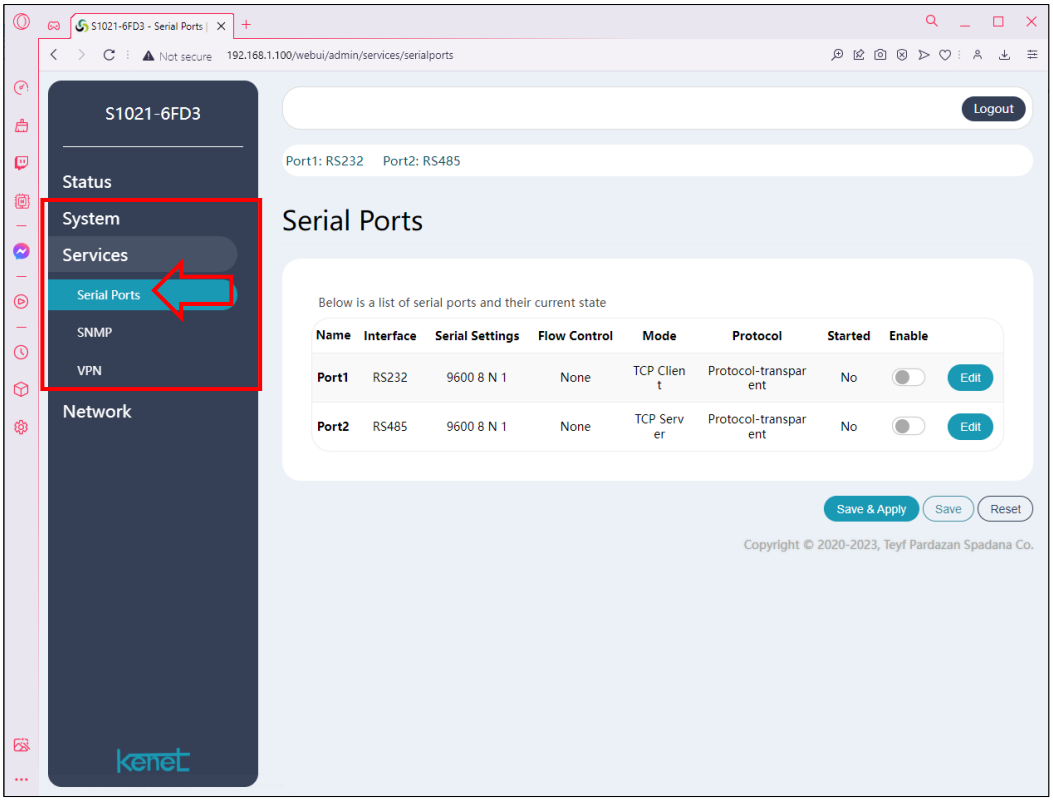


در این بخش به معرفی بخش SERVICES مبدل پرداخته می شود.

۵-۱ قسمت های بخش SERVICES

- قسمت Serial Ports
- قسمت SNMP
- قسمت OpenVPN

۵-۲ قسمت Serial Ports

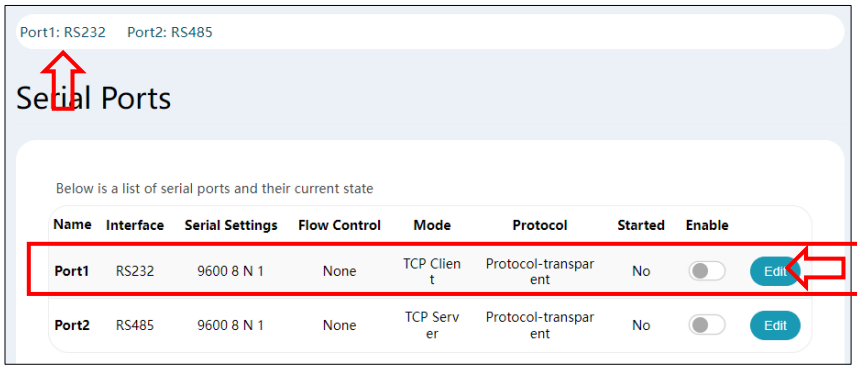


۵-۲-۱ معرفی

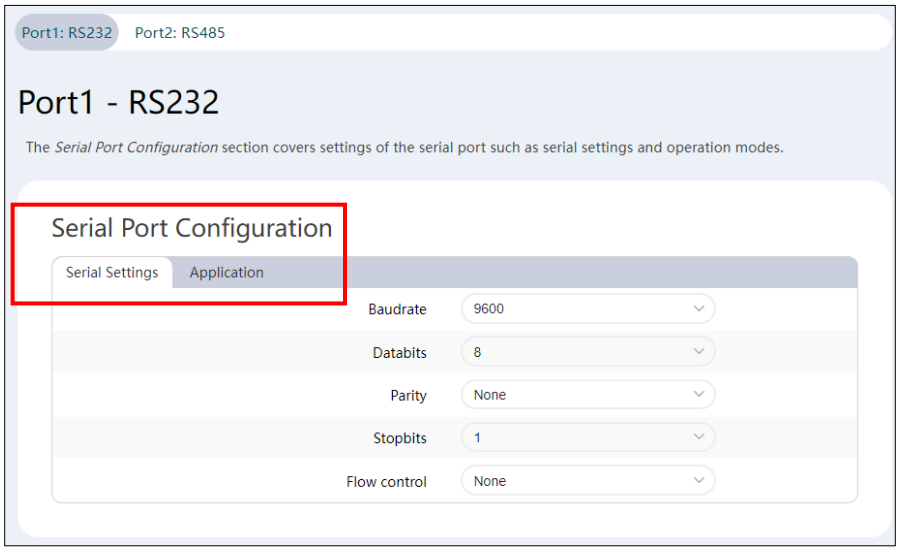
- این بخش اطلاعاتی پیرامون پورت های RS485 و RS232 ارائه می دهد.
- از ۲ بخش زیر تشکیل شده است:
  - RS232 : تنظیمات پیکربندی RS232
  - RS485 : تنظیمات پیکربندی RS485

۵-۲-۲ تنظیمات پورت RS232

- برای ورود به بخش تنظیمات این بخش ، کافی است از سمت راست پنجره ، بر روی EDIT قسمت RS232 انتخاب نمایید.

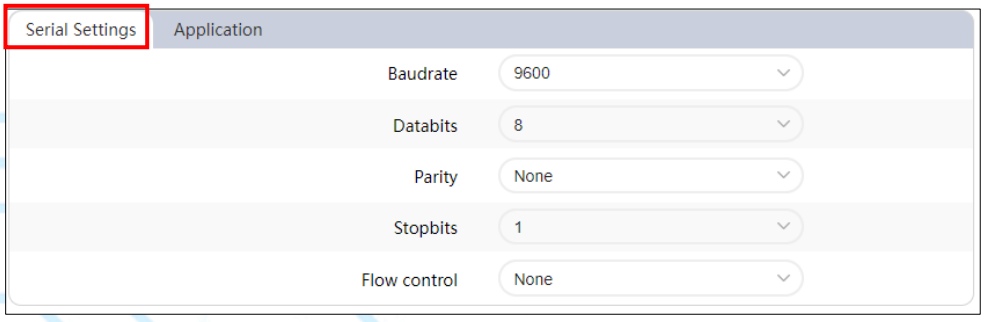


- هم چنین شما می توانید از بالای صفحه ، بر روی PORT1:RS232 انتخاب نمایید.
- پس از باز شدن بخش پیکربندی RS232 ، پنجره ی زیر برای شما نمایش داده می شود.



- تنظیمات پیکربندی پورت RS232 به ۲ بخش زیر تقسیم می شود:
- Serial Settings : تنظیمات کلی بخش پورت RS232
- Application : پیکربندی تنظیمات تخصصی RS232

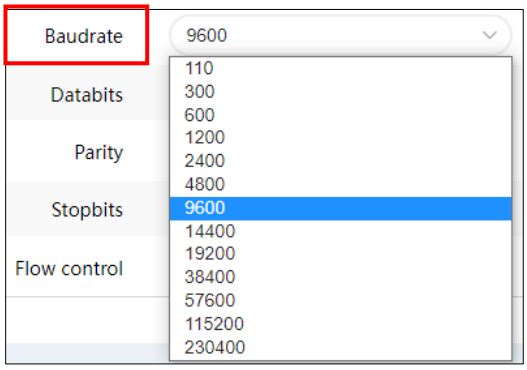
۵-۲-۲-۱ بخش Serial Settings



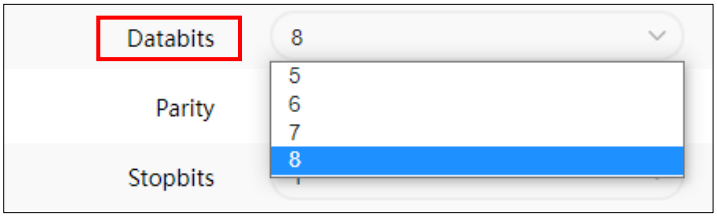
- این بخش از ۵ پارامتر تشکیل شده است:

- Baudrate : نرخ تبادل اطلاعات
- Databits : طول(بیت) دیتا ارسالی
- Parity : بیت تصحیح ارسال دیتا
- Stopbits : بیت مشخص کننده پایان دیتا
- Flow control : کنترل جریان دیتا

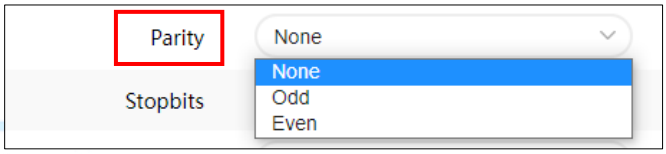
- در قسمت Baudrate مقادیر زیر قابل انتخاب هستند.
- بازه مقادیر از ۱۱۰ الی ۲۳۰۴۰۰ می باشد.
- ۱۳ مقدار قابل انتخاب در این بخش موجود است.



- در قسمت Databits مقادیر زیر قابل انتخاب هستند.
- ۴ مقدار ۵ و۶ و۷ و۸ بیت ، برای طول دیتا قابل انتخاب می باشند.

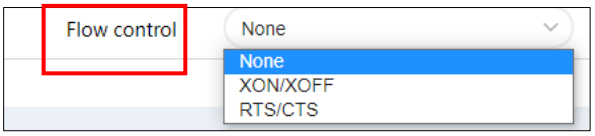


- در قسمت Parity مقادیر زیر قابل انتخاب هستند.
- ۳ مقدار ، زوج – فرد – بدون مقدار ،برای تصحیح خطای ارسال قابل انتخاب می باشد.



- در قسمت Stopbits مقادیر زیر قابل انتخاب هستند.
- ۲ مقدار ، ۱و۲ بیت ،برای پایان دیتا قابل انتخاب می باشند.

- در قسمت Flow control نیز مقادیر زیر قابل انتخاب هستند.
- ۳ مقدار، بدون مقدار-XON/XOFF – RTS/CTS برای کنترل جریان قابل انتخاب هستند.
- RTS/CTS : نرم افزاری
- XON/XOFF : سخت افزاری

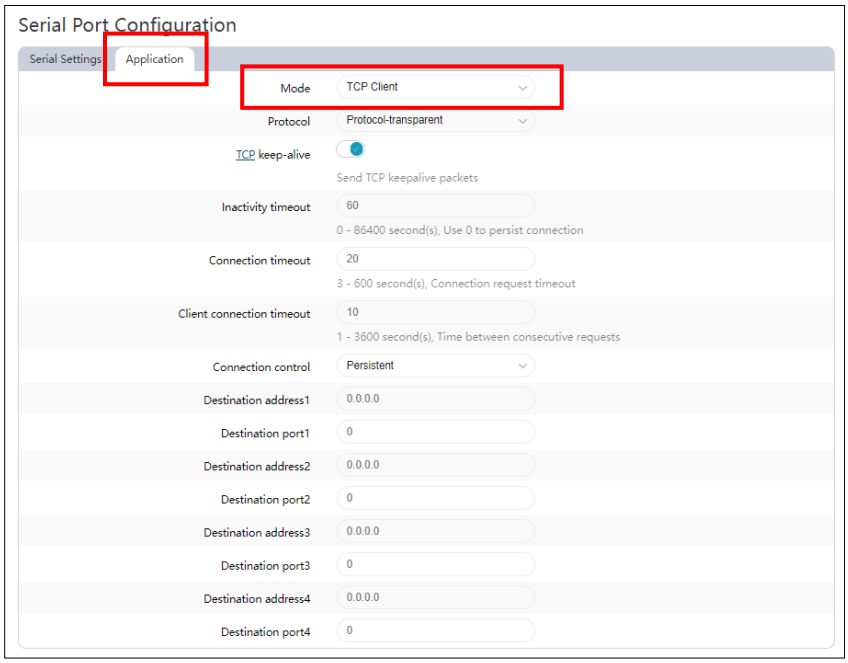


- پس از پیکربندی تنظیمات مورد نظر، ذخیره و اعمال را انتخاب نمایید.

۵-۲-۲-۲ بخش Application

- این بخش با توجه به فیلد MODE بخش های متفاوتی دارد.
- MODE می تواند مقدار های زیر را دریافت کند.
  - TCP CLIENT
  - TCP SERVER

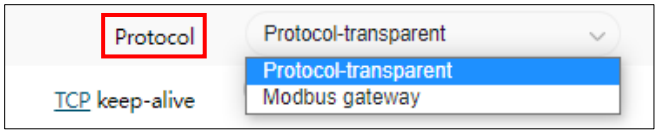
۵-۲-۲-۲-۱ حالت TCP CLIENT



- در این بخش فیلد های زیر مقدار می گیرند:
  - Protocol
  - TCP keep-alive
  - Inactivity timeout
  - Connection timeout
  - Client connection timeout
  - Connection control
  - Destination address1
  - Destination port1
  - Destination address2
  - Destination port2
  - Destination address3
  - Destination port3
  - Destination address4
  - Destination port4

- در قسمت Protocol مقادیر زیر قابل انتخاب هستند.
- protocol transparent : توانایی کار مستقل از پروتکل
- modbus gateway :

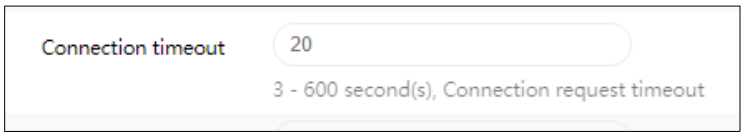
تبدیل modbus rtu به Modbus tcp ip



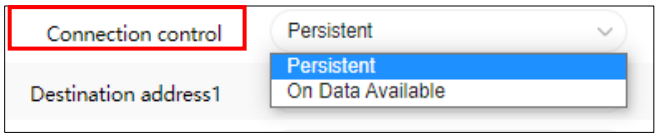
- قسمت TCP keep-alive قابل فعال سازی می باشد.
- ارسال دوره ای بسته tcp برای زنده نگه داشتن جلسه tcp

- در قسمت Inactivity timeout ، زمان عدم فعالیت را تعیین نمایید .
- از بازه ۰ الی ۸۶۴۰۰ ثانیه قابل انتخاب است.
- از ۰ برای تداوم اتصال استفاده کنید.

- در قسمت Connection timeout ، مهلت درخواست اتصال را تعیین نمایید.
- از بازه ۳ الی ۶۰۰ ثانیه قابل انتخاب است.

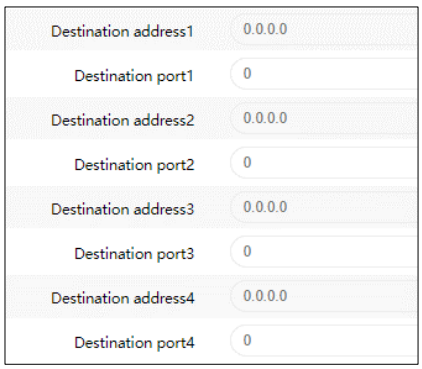


- در قسمت Connection control مقادیر زیر قابل دریافت هستند.
- Persistent : مداوم
- no data available : بدون داده موجود

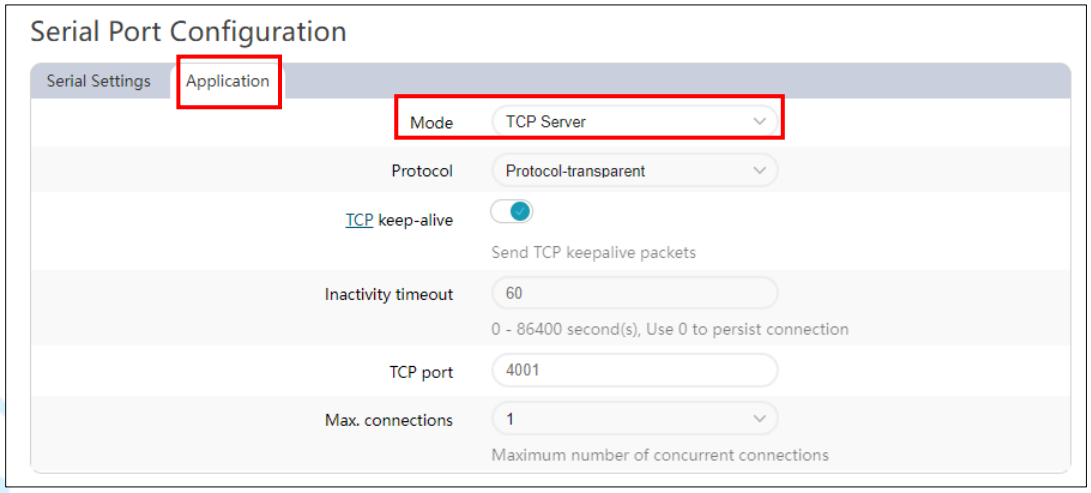


- در قسمت انتهایی این بخش هم به ازای ۴ ادرس می توان مقادیر زیر را تنظیم کرد.

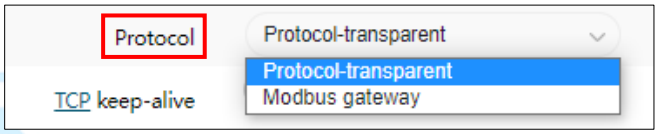
- Destination address : ادرس مقصد
- Destination port : پورت مقصد



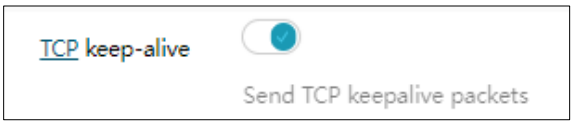
۲-۲-۲-۵ حالت TCP SERVER



- در قسمت Protocol مقادیر زیر قابل انتخاب هستند.



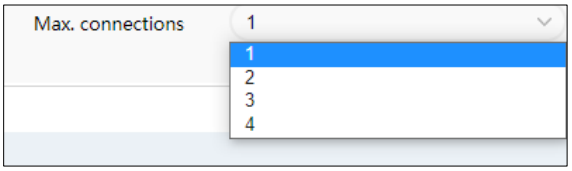
- قسمت TCP keep-alive قابل فعال سازی می باشد.
- ارسال دوره ای بسته tcp برای زنده نگه داشتن جلسه tcp



- در قسمت Inactivity timeout ، زمان عدم فعالیت را تعیین نمایید .

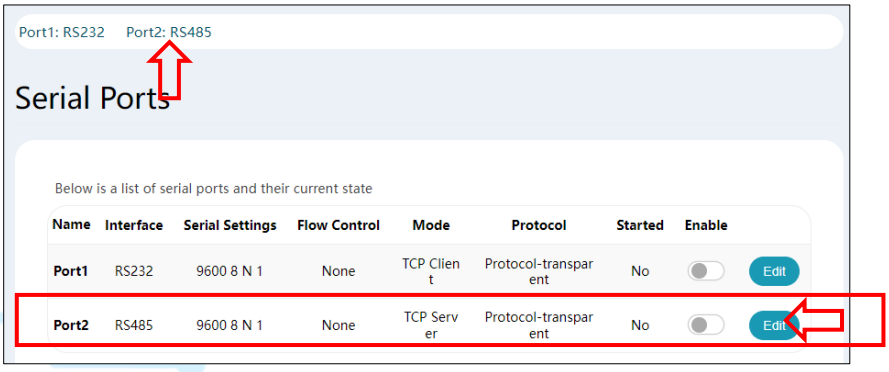
- در قسمت TCP port باید یک پورت را وارد کنید.

- در قسمت Max connections ، بیشترین تعداد کلاینت متصل را تعیین نمایید.
  - تعداد ۱ الی ۴ کلاینت قابل انتخاب است.

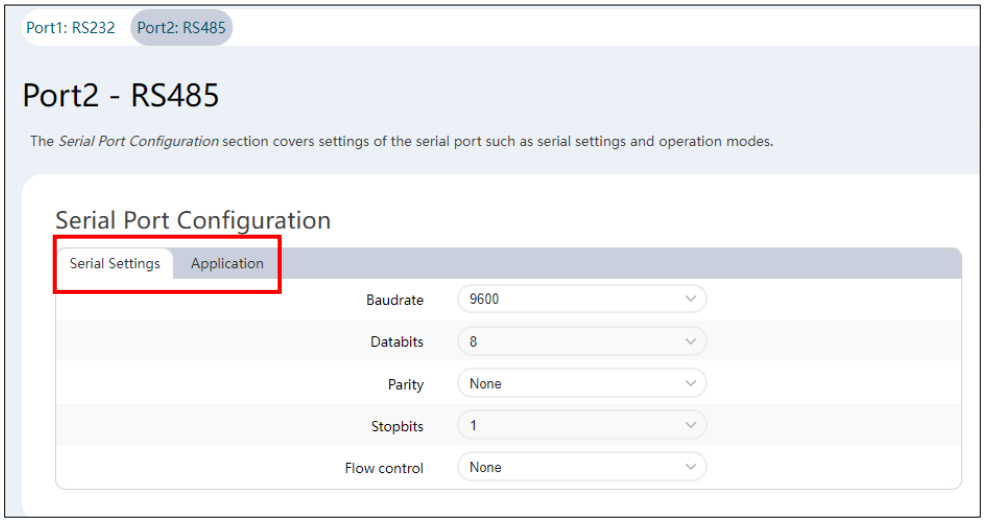


۳-۲-۵ تنظیمات پورت RS485

- برای ورود به بخش تنظیمات این بخش ، کافی است از سمت راست پنجره ، بر روی EDIT قسمت RS485 انتخاب نمایید.

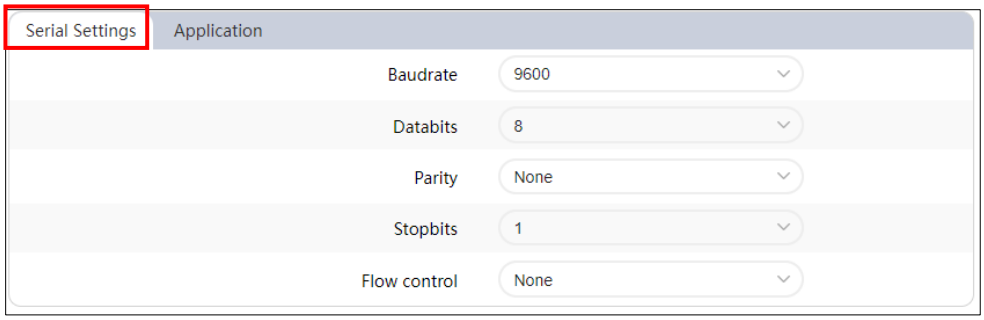


- هم چنین شما می توانید از بالای صفحه ، بر روی PORT2:RS485 انتخاب نمایید.
- پس از باز شدن بخش پیکربندی RS485 ، پنجره ی زیر برای شما نمایش داده می شود.



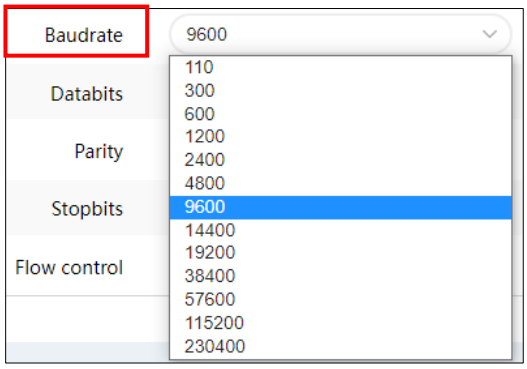
- تنظیمات پیکربندی پورت RS485 به ۲ بخش زیر تقسیم می شود:
- Serial Settings : تنظیمات کلی بخش پورت RS485
- Application : پیکربندی تنظیمات تخصصی RS485

۵-۲-۳-۱ بخش Serial Settings

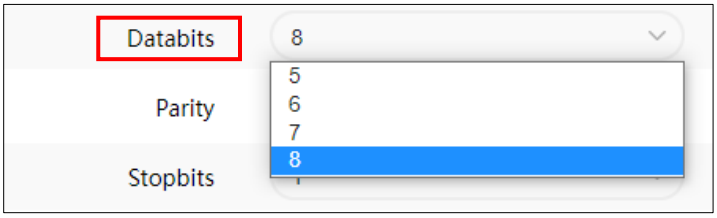


- این بخش از ۵ پارامتر تشکیل شده است:
- Baudrate : نرخ تبادل اطلاعات
- Databits : طول(بیت) دیتا ارسالی
- Parity : بیت تصحیح ارسال دیتا
- Stopbits : بیت مشخص کننده پایان دیتا
- Flow control : کنترل جریان دیتا
- در قسمت Baudrate مقادیر زیر قابل انتخاب هستند.
- بازه مقادیر از ۱۱۰ الی ۲۳۰۴۰۰ می باشد.

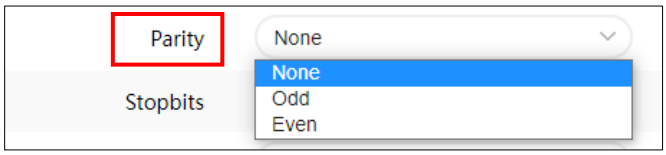
- ۱۳ مقدار قابل انتخاب در این بخش موجود است.



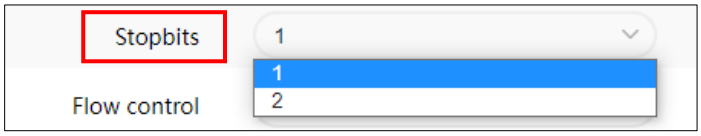
- در قسمت Databits مقادیر زیر قابل انتخاب هستند.
- ۴ مقدار ۵ و۶ و۷ و۸ بیت ، برای طول دیتا قابل انتخاب می باشند.



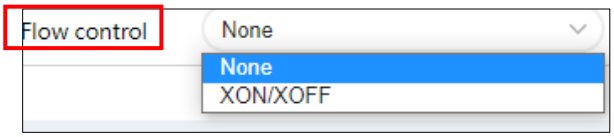
- در قسمت Parity مقادیر زیر قابل انتخاب هستند.
- ۳ مقدار ، زوج – فرد – بدون مقدار ،برای تصحیح خطای ارسال قابل انتخاب می باشد.



- در قسمت Stopbits مقادیر زیر قابل انتخاب هستند.
- ۲ مقدار ، ۱و۲ بیت ،برای پایان دیتا قابل انتخاب می باشند.



- در قسمت Flow control نیز مقادیر زیر قابل انتخاب هستند.
- ۳ مقدار، بدون مقدار-XON/XOFF ، برای کنترل جریان قابل انتخاب هستند.
- XON/XOFF : سخت افزاری

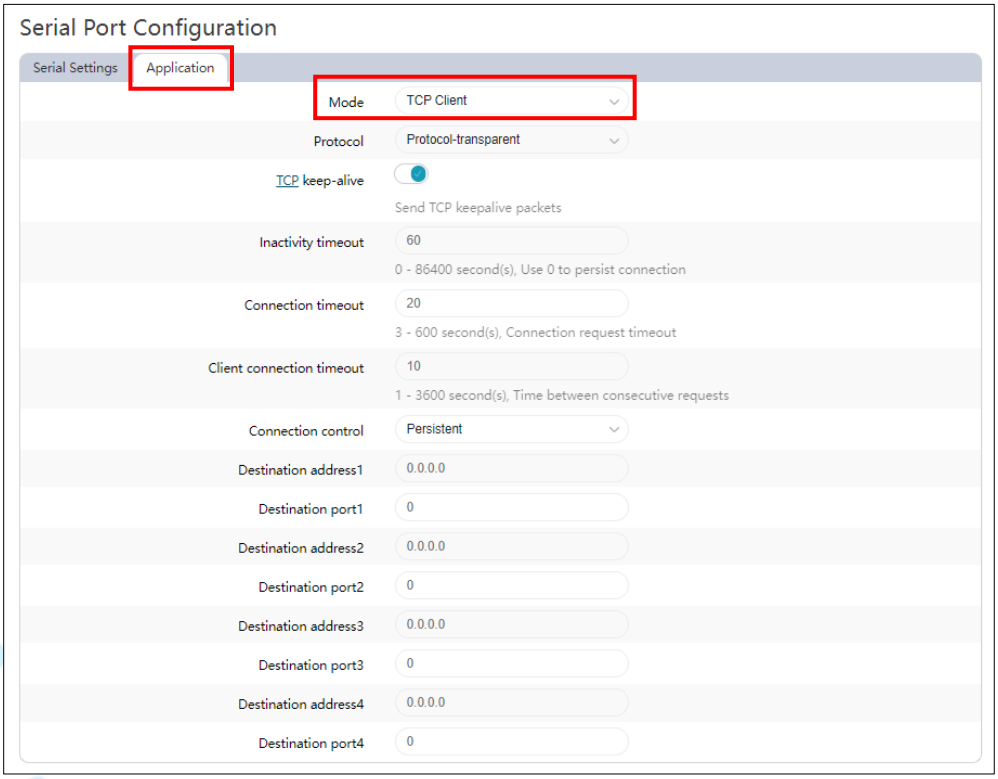


- پس از پیکربندی تنظیمات مورد نظر، ذخیره و اعمال را انتخاب نمایید.

۵-۲-۳-۲ بخش Application

- این بخش با توجه به فیلد MODE بخش های متفاوتی دارد.
- MODE می تواند مقدار های زیر را دریافت کند.
  - TCP CLIENT
  - TCP SERVER

۵-۲-۳-۲-۱ حالت TCP CLIENT

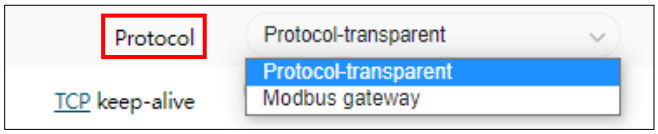


- در این بخش فیلد های زیر مقدار می گیرند:
  - Protocol
  - TCP keep-alive
  - Inactivity timeout
  - Connection timeout
  - Client connection timeout

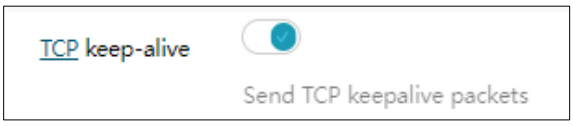
- Connection control
- Destination address1
- Destination port1
- Destination address2
- Destination port2
- Destination address3
- Destination port3
- Destination address4
- Destination port4

- در قسمت Protocol مقادیر زیر قابل انتخاب هستند.
- protocol transparent : توانایی کار مستقل از پروتکل
- modbus gateway :

تبدیل modbus rtu به tcp ip modbus



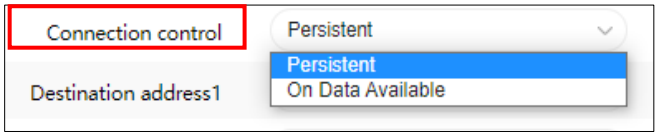
- قسمت TCP keep-alive قابل فعال سازی می باشد.
- ارسال دوره ای بسته tcp برای زنده نگه داشتن جلسه tcp



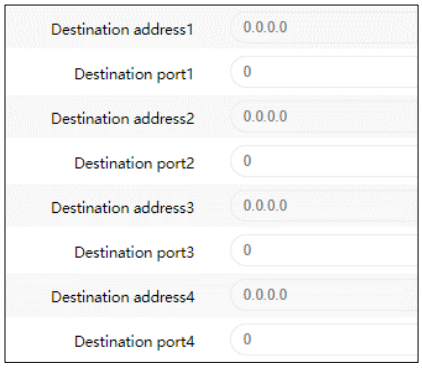
- در قسمت Inactivity timeout ، زمان عدم فعالیت را تعیین نمایید .
- از بازه ۰ الی ۸۶۴۰۰ ثانیه قابل انتخاب است.
- از ۰ برای تداوم اتصال استفاده کنید.

- در قسمت Connection timeout ، مهلت درخواست اتصال را تعیین نمایید.
- از بازه ۳ الی ۶۰۰ ثانیه قابل انتخاب است.

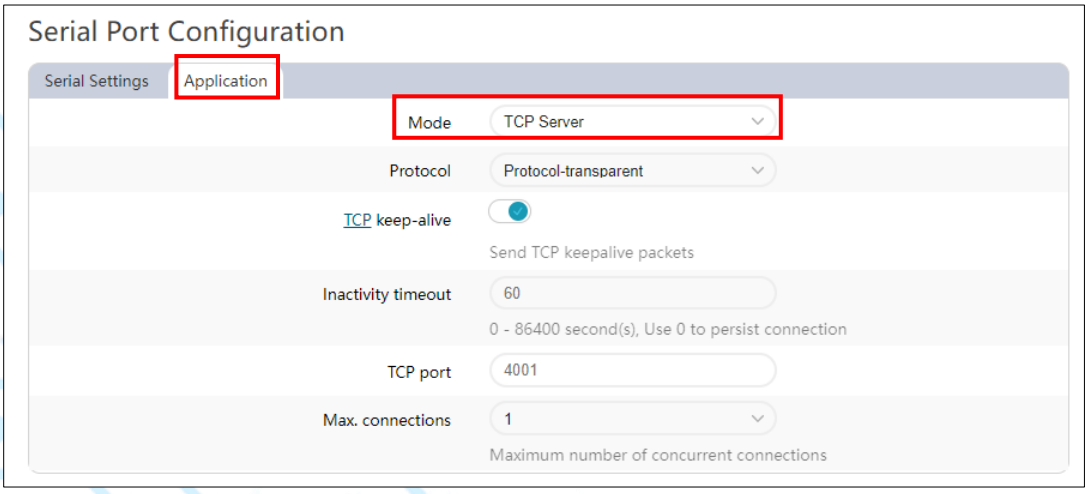
- در قسمت Connection control مقادیر زیر قابل دریافت هستند.
- Persistent : مداوم
- no data available : بدون داده موجود



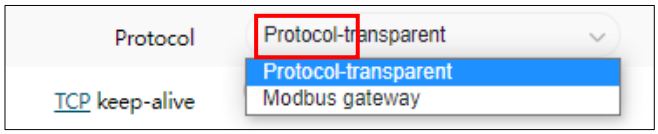
- در قسمت انتهایی این بخش هم به ازای ۴ ادرس می توان مقادیر زیر را تنظیم کرد.
- Destination address : ادرس مقصد
- Destination port : پورت مقصد



۲-۲-۳-۲-۵ حالت TCP SERVER



- در قسمت Protocol مقادیر زیر قابل انتخاب هستند.

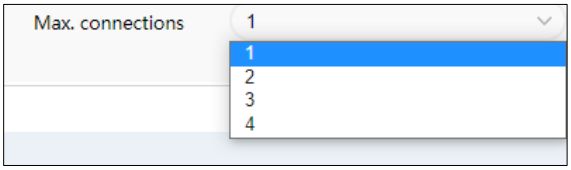


- قسمت TCP keep-alive قابل فعال سازی می باشد.
- ارسال دوره ای بسته tcp برای زنده نگه داشتن جلسه tcp

- در قسمت Inactivity timeout ، زمان عدم فعالیت را تعیین نمایید .

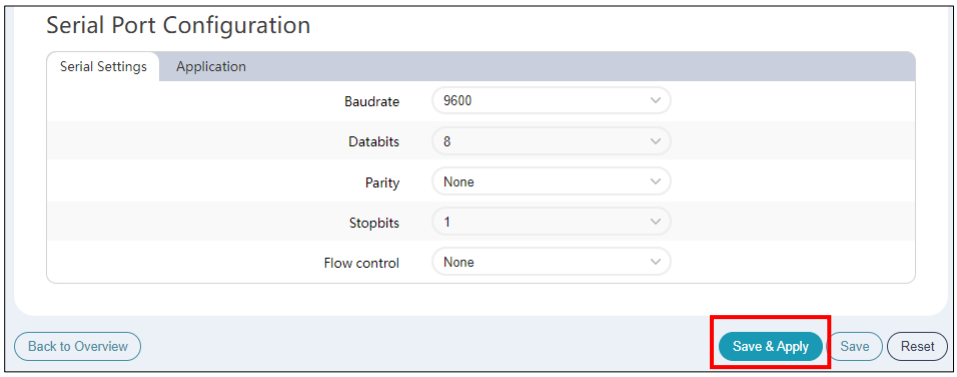
- در قسمت TCP port باید یک پورت را وارد کنید.

- در قسمت Max connections ، بیشترین تعداد کلاینت متصل را تعیین نمایید.
- تعداد ۱ الی ۴ کلاینت قابل انتخاب است.

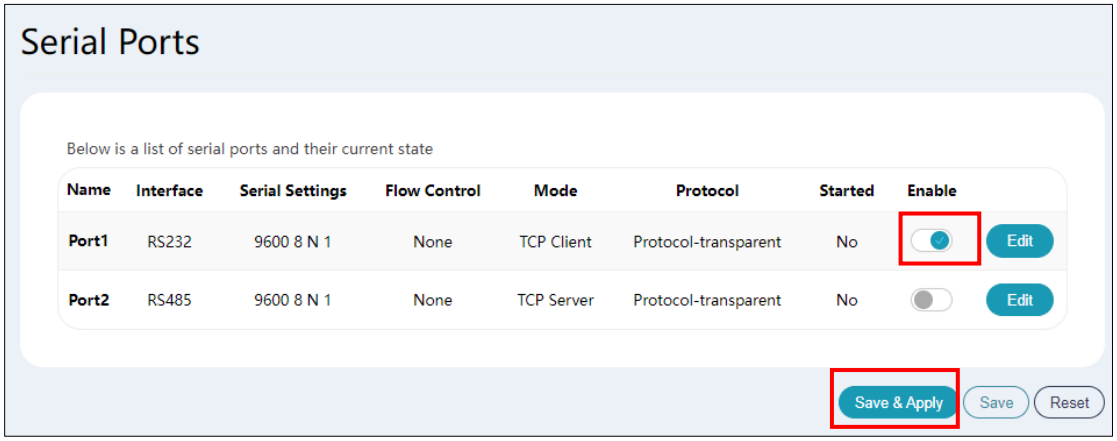


۴-۲-۵ نکات بخش Serial Ports

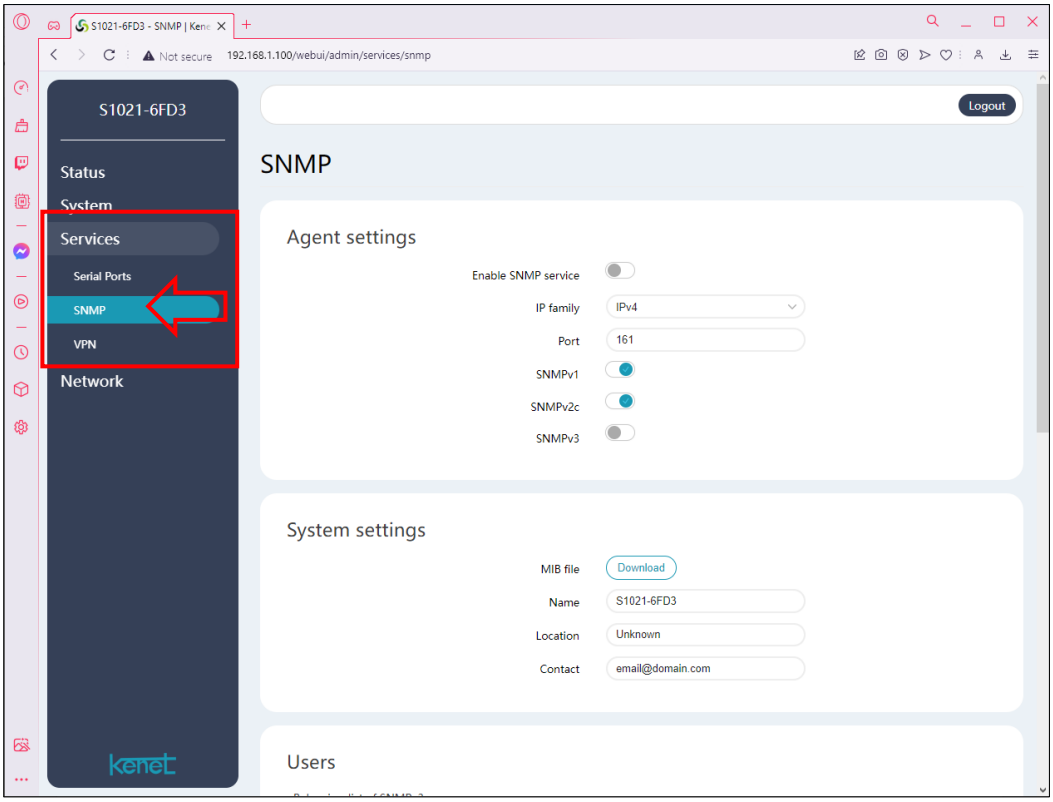
- بعد از انجام تنظیمات هریک از بخش های RS232 و RS485 یک بار ذخیره و اعمال را بزنید.



- سپس بعد از فعال کردن پورت مورد نیز بار دیگر ذخیره و اعمال را دوباره انتخاب نمایید.



۵-۳ قسمت SNMP



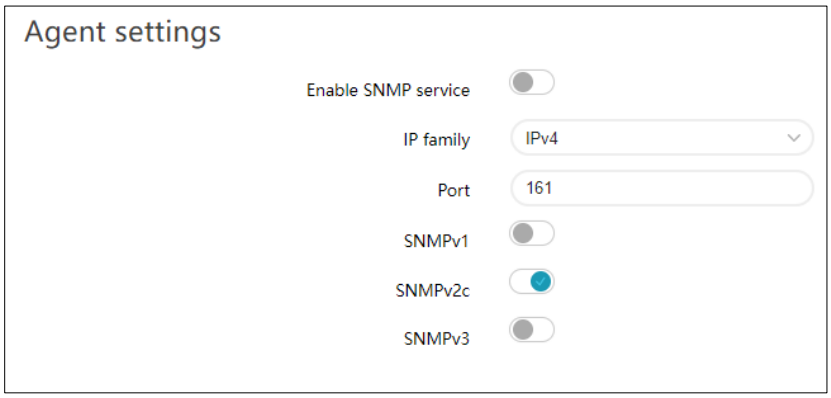
۵-۳-۱ معرفی SNMP

- مخفف عبارت Simple Network Management Protocol می باشد.
- پروتکل SNMP یکی از پروتکل های لایه Application است که امکان نقل و انتقال اطلاعات مدیریتی را بین عناصر شبکه ایجاد می کند و در واقع قسمتی از پروتکل TCP/IP می باشد. این پروتکل به طور وسیعی برای مانیتورینگ و مدیریت اجزاء شبکه استفاده می شود. بسیاری از وندورها، تجهیزات تولیدی خود را به پروتکل SNMP مجهز می کنند تا امکان نظارت بر عملکرد آنها به کمک نرم افزارهای مانیتورینگ فراهم شود؛ در حال حاضر سه نسخه از پروتکل SNMP وجود دارد، SNMPv1، SNMPv2 و SNMPv3.
- از این بخش بیشتر برای مانیتور کردن استفاده می شود.
- یک خروجی mib. از این بخش گرفته شده و به نرم دیگر جهت مانتیور کردن ارجاع داده می شود.
- از ۵ بخش زیر تشکیل شده است:
  - Agent settings : تنظیمات نماینده
  - System settings : تنظیمات سیستم

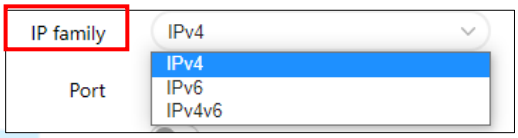
- Users : کاربران
- SNMP community : جامعه SNMP
- SNMP IPv6 community : جامعه SNMP IPv6

۵-۳-۲ بخش Agent settings

- این بخش از ۶ بخش زیر تشکیل شده است:
- Enable SNMP service : فعال کردن سرویس SNMP
- IP family : نوع ادرس IP
- Port : پورت مد نظر
- SNMPv1 : این اولین نسخه SNMP است که در RFC های شماره ۱۱۵۵ و ۱۱۵۷ تعریف شده است.
- SNMPv2c : این نسخه تجدید نظر شده SNMPv1 است که بهینه سازی های فراوانی روی آن صورت گرفته، از نوع پکت ها، روش تبادل و حتی ساختار MIB این نسخه بسیار بهینه تر شده است.
- SNMPv3 : این نسخه ایمن ترین و آخرین نسخه SNMP است.



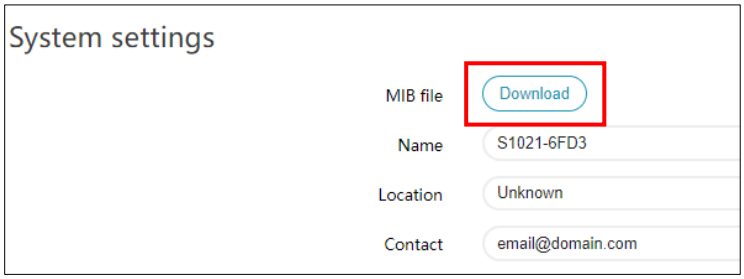
- در بخش IP می توان ۳ نوع انتخاب زیر را داشت :



۵-۳-۳ بخش System settings

- این بخش از ۴ بخش زیر تشکیل شده است:
- MIB file : برای دانلود .mib فایل استفاده می شود.

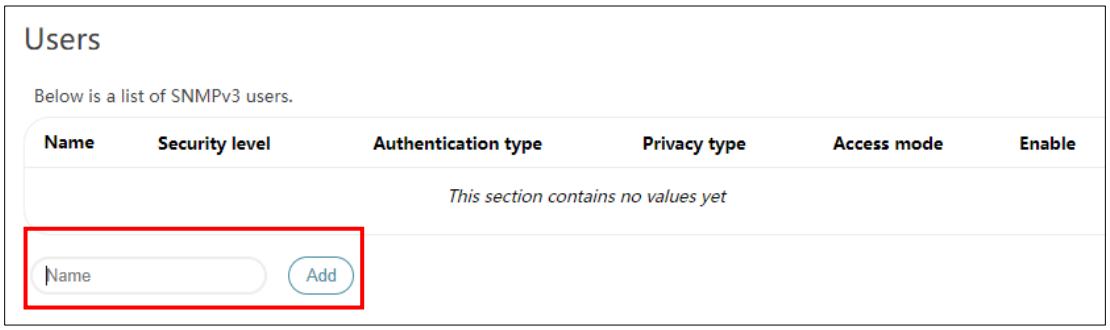
- Name : نام دستگاه
- Location : مکان نصب دستگاه
- Contact : راه ارتباطی با ناظر دستگاه



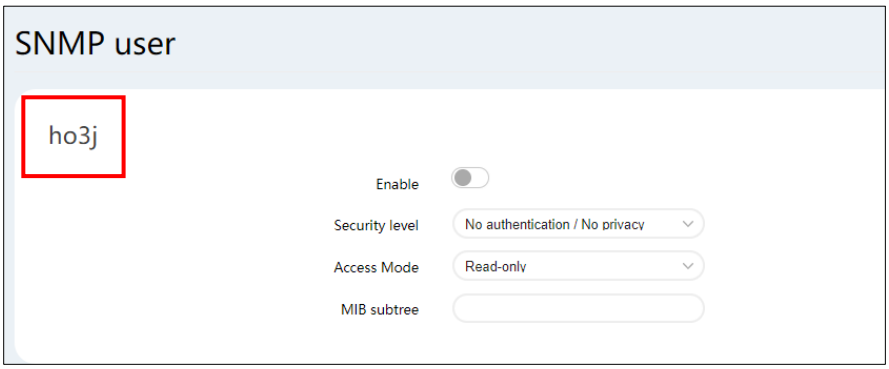
- فایل دانلود شده ، در قسمت دانلود های شما در مرورگر موجود است.

۴-۳-۵ بخش Users

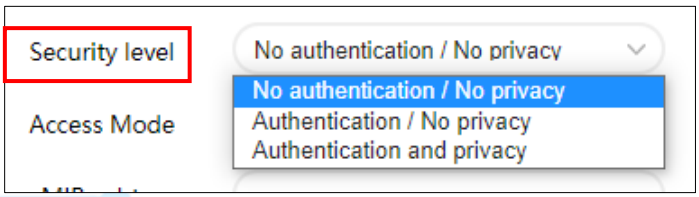
- در این بخش می توان کاربر تعریف نمود و هم چنین بقیه ی کاربران موجود را مدیریت نمود.
- اطلاعات جدول کاربران به ردیف های زیر خلاصه می شود:
  - Name : نام کاربر
  - Security level : سطح امنیتی کاربر
  - Authentication type : نوع احراز هویت
  - Privacy type : نوع حریم خصوصی
  - Access mode : حالت دسترسی
  - Enable : فعال یا غیر فعال بودن کاربر
- برای تعریف کاربر جدید ، در قسمت مشخص شده نام کاربر جدید را وارد کرده، سپس بر روی گزینه add انتخاب کنید.



- پس از نوشتن نام کاربر مورد نظر، وارد صفحه ی زیر می شوید.



- همان طور که مشاهده می کنید ، نام کاربری که می خواهید اضافه کنید در قسمت بالای صفحه نمایش داده شده است.
- ۴ بخش برای کاربر جدید باید تعریف شود:
  - Enable : فعال سازی کاربر
  - Security level : سطح دسترسی کاربر
  - Access Mode : حالت دسترسی
  - MIB subtree : زیرشاخه mib که این کاربر دسترسی دارد.
- در بخش Security level ، ۳ سطح امنیتی تعریف شده است:



- No authentication / no authentication :

بدون احراز هویت و بدون حریم خصوصی

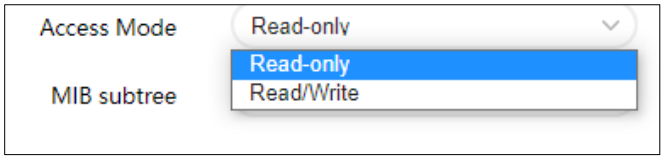
- Authentication / no privacy :

با احراز هویت و بدون خریم خصوصی

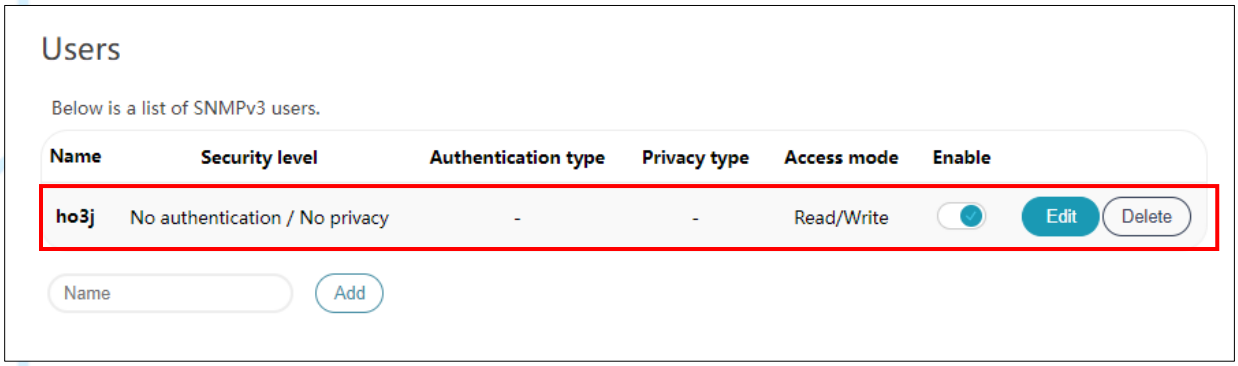
- Authentication and privacy :

با احراز هویت و با حریم خصوصی

- در بخش Access Mode ، ۲ مورد سطح دسترسی به اطلاعات تعریف شده است.
- Read-only : فقط خواندن
- Read/Write : خواندن و نوشتن



- پس از انتخاب موارد مورد نظر، بر روی ذخیره و اعمال انتخاب کنید.

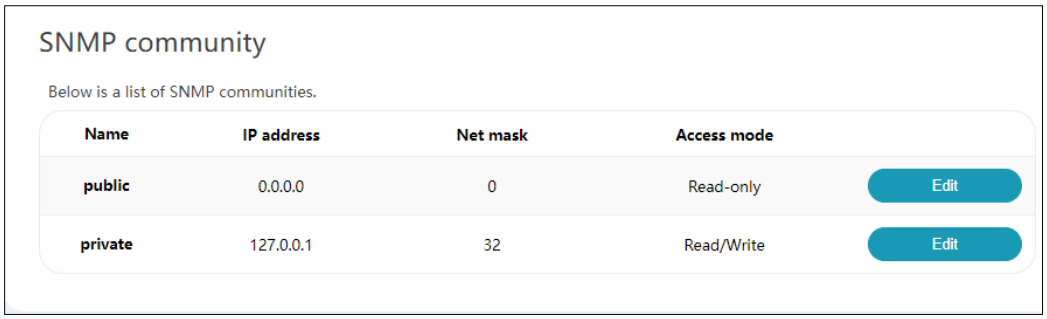


- هم چنین می توانید ، کاربران فعلی را غیر فعال کنید و یا اطلاعات انان را ویرایش کنید.

۵-۳-۵ بخش SNMP community

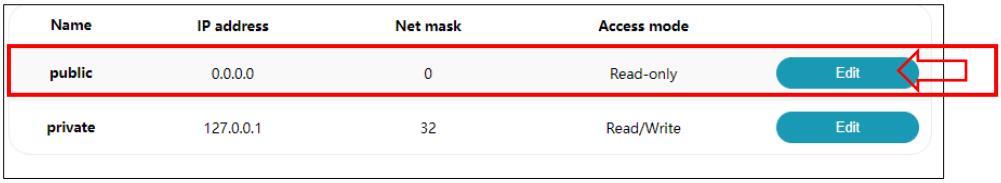
- در این قسمت راه های ارتباطی IPV4 قرار دارد.
- جدولی با ۲ ردیف با عنوان های خصوصی و عمومی در این بخش قرار گرفته است.
- جدول این بخش از ستون های زیر تشکیل شده است:
- Community name : نام
- IP address : ادرس IP
- Net mask : تفکیک ۲ قسمت هاست و شبکه
- Access mode : حالت دسترسی

- هم چنین گزینه ای برای ویرایش تنظیمات بخش عمومی و بخش تخصصی به صورت جداگانه تعبیه شده است.



۱-۵-۳-۵ ویرایش بخش عمومی

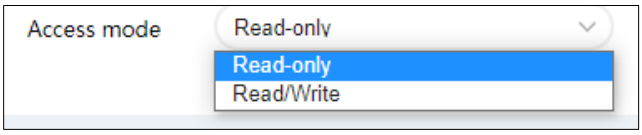
- برای ویرایش کافی است روی گزینه edit در ردیف اول که مربوط به بخش عمومی جدول هست ، را انتخاب نمایید.



- سپس پنجره زیر برای شما نمایش داده خواهد شد:

- شما می توانید فیلد های زیر را ویرایش نمایید:
  - Community name : نام
  - IP address : ادرس IP
  - Net mask : تفکیک ۲ قسمت هاست و شبکه
  - Access mode : حالت دسترسی

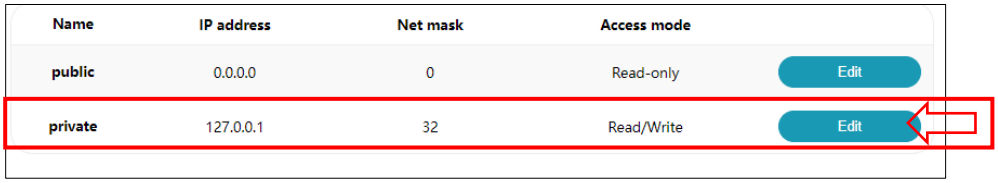
- حالت Access mode ۲ حالت زیر را دارا می باشد:



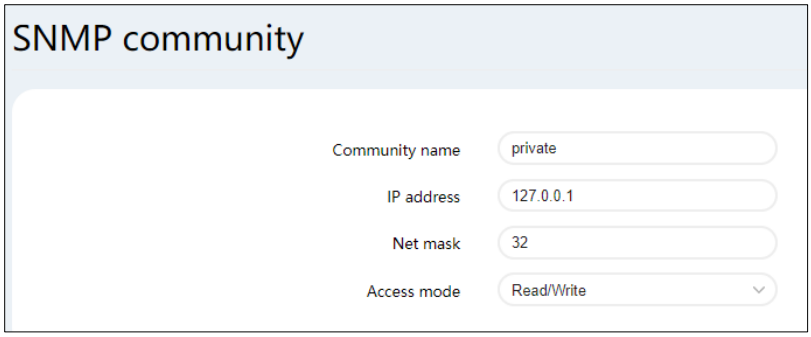
- در پایان حتما گزینه ذخیره و اعمال را انتخاب کنید.

۲-۵-۳-۵ ویرایش بخش خصوصی

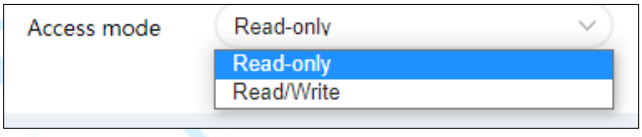
- برای ویرایش کافی است روی گزینه edit در ردیف اول که مربوط به بخش خصوصی جدول هست ، را انتخاب نمایید.



- سپس پنجره زیر برای شما نمایش داده خواهد شد:



- شما می توانید فیلد های زیر را ویرایش نمایید:
  - Community name : نام
  - IP address : ادرس IP
  - Net mask : تفکیک ۲ قسمت هاست و شبکه
  - Access mode : حالت دسترسی
- حالت Access mode ۲ حالت زیر را دارا می باشد:



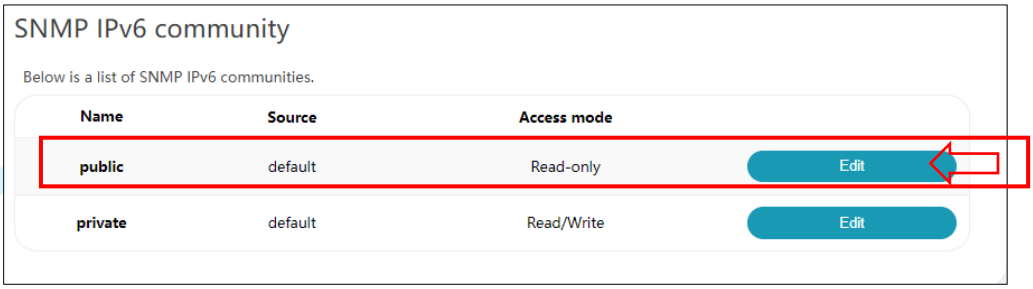
- در پایان حتما گزینه ذخیره و اعمال را انتخاب کنید.

۵-۳-۶ بخش SNMP IPv6 community

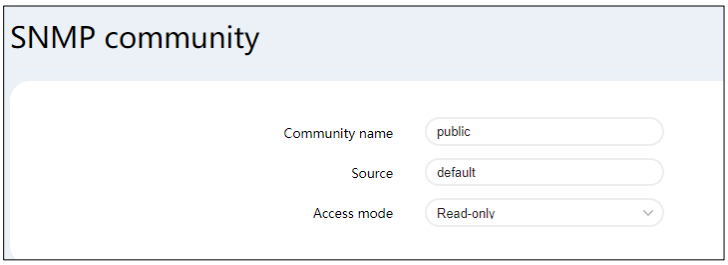
- در این قسمت راه های ارتباطی IPV6 قرار دارد.
- جدولی با ۲ ردیف با عنوان های خصوصی و عمومی در این بخش قرار گرفته است.
- جدول این بخش از ستون های زیر تشکیل شده است:
  - Name : نام
  - Source : منبع
  - Access mode : حالت دسترسی
- هم چنین گزینه ای برای ویرایش تنظیمات بخش عمومی و بخش تخصصی به صورت جداگانه تعبیه شده است.

۵-۳-۶-۱ ویرایش بخش عمومی

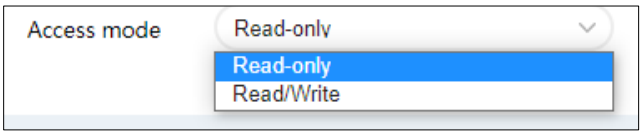
- برای ویرایش کافی است روی گزینه edit در ردیف اول که مربوط به بخش عمومی جدول هست ، را انتخاب نمایید.



- سپس پنجره زیر برای شما نمایش داده خواهد شد:



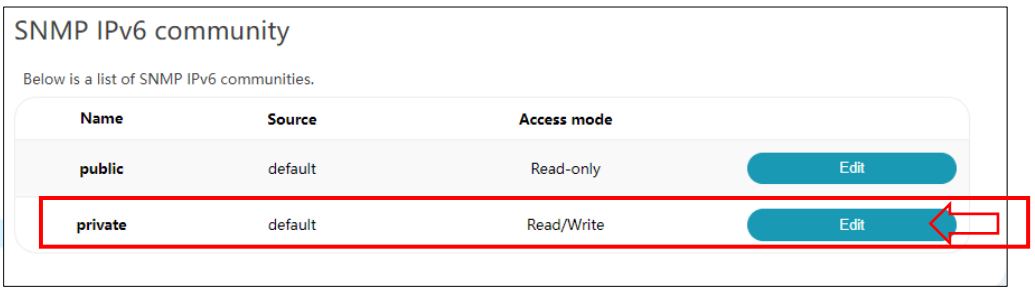
- شما می توانید فیلد های زیر را ویرایش نمایید:
  - Community name : نام ارتباط
  - IP address : ادرس IP
  - Access mode : حالت دسترسی
- حالت Access mode ۲ حالت زیر را دارا می باشد:



- در پایان حتما گزینه ذخیره و اعمال را انتخاب کنید.

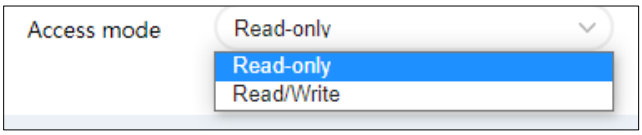
۲-۶-۳-۵ ویرایش بخش خصوصی

- برای ویرایش کافی است روی گزینه edit در ردیف اول که مربوط به بخش خصوصی جدول هست ، را انتخاب نمایید.



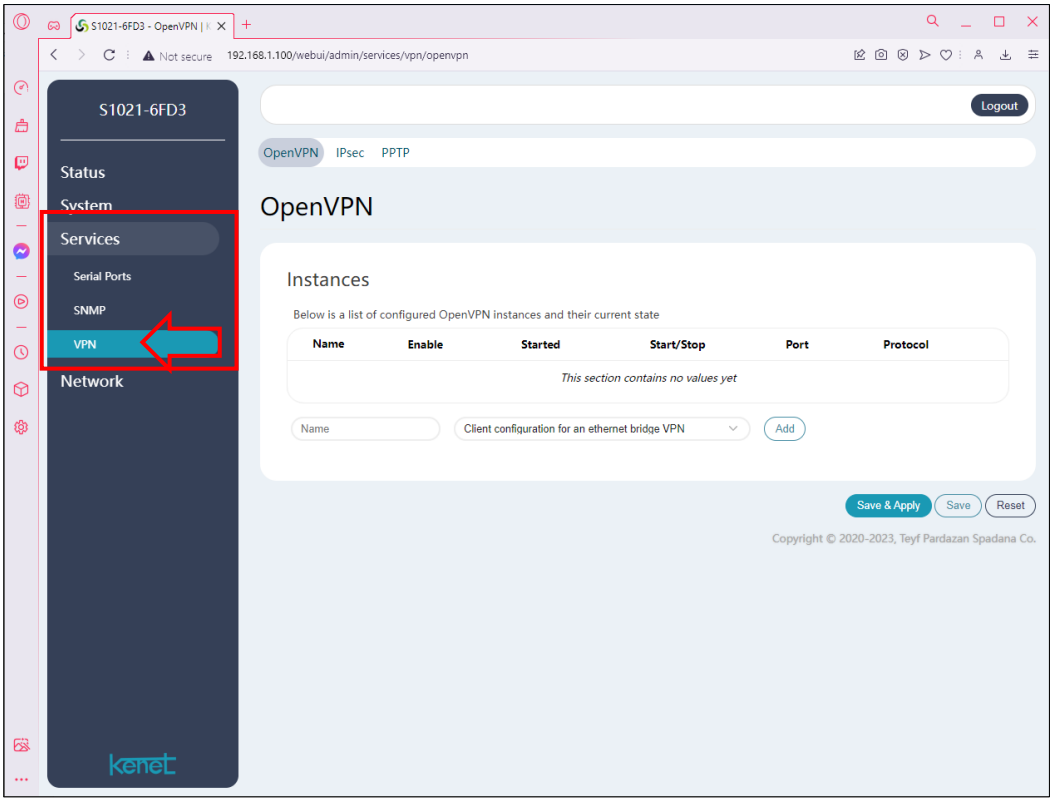
- سپس پنجره زیر برای شما نمایش داده خواهد شد:

- شما می توانید فیلد های زیر را ویرایش نمایید:
  - Community name : نام ارتباط
  - IP address : ادرس IP
  - Access mode : حالت دسترسی
- حالت Access mode ۲ حالت زیر را دارا می باشد:



- در پایان حتما گزینه ذخیره و اعمال را انتخاب کنید.

۵-۴ قسمت VPN



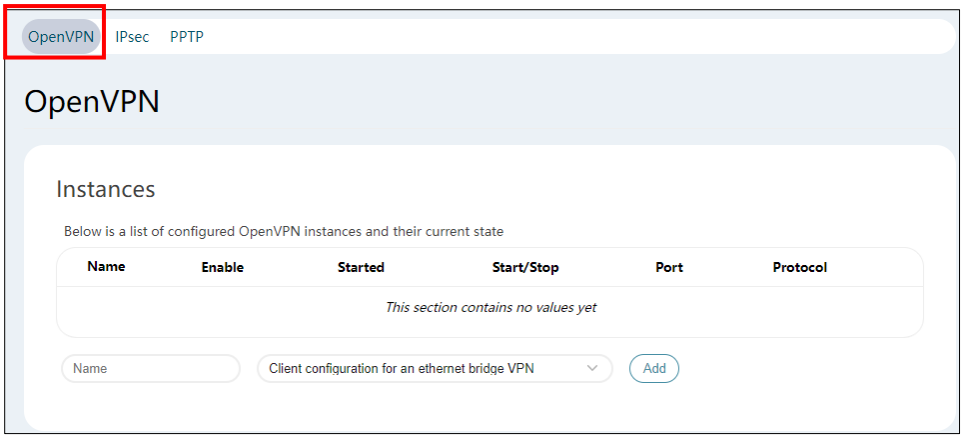
۵-۳-۱ معرفی VPN

- Virtual private network به جای اینکه شما را به یک فضای نا امن و شلوغ در اینترنت متصل کند شما را به یک شبکه خصوصی از اینترنت انتقال میدهد که تنها به خودتان اختصاص دارد.
- از ۳ بخش زیر تشکیل شده است:
  - OpenVPN : Open Source
  - IPsec : IP Security
  - PPTP : Point-to-Point Tunneling Protocol

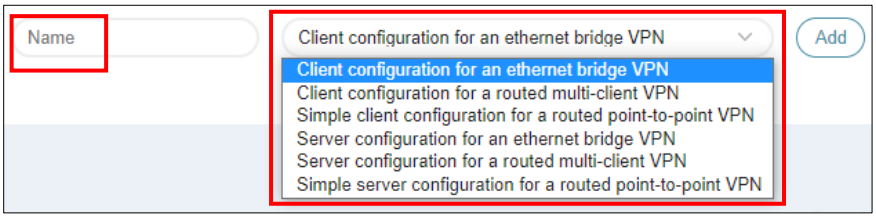
۵-۳-۱-۱ پروتکل OpenVPN

- از تکنولوژی‌های منبع باز (Open Source) استفاده می‌کند و در اغلب سیستم‌عامل‌ها و موبایل‌ها می‌توان از آن استفاده کرد.

- در لیست سرویس‌های تمام ارائه دهندگان وجود دارد و به دلیل منبع باز بودن آن، هر کدام تغییراتی در این پروتکل اعمال کرده و به کاربر ارائه می دهند.



- جدول این بخش از ۶ قسمت زیر تشکیل شده است:
  - Name : نام
  - Enable : فعال بودن
  - Started : وضعیت فعال یا فعال بودن vpn مورد نظر
  - Start/Stop : توقف و شروع دستی
  - Port : پورت
  - Protocol : نوع پروتکل انتخابی
- برای اضافه کردن vpn به این بخش هم در قسمت اضافه کردن در پایین همین بخش، پس از درج نام مورد نظر نوع مورد نظر را انتخاب کرده و سپس گزینه اضافه کردن را انتخاب نمایید.

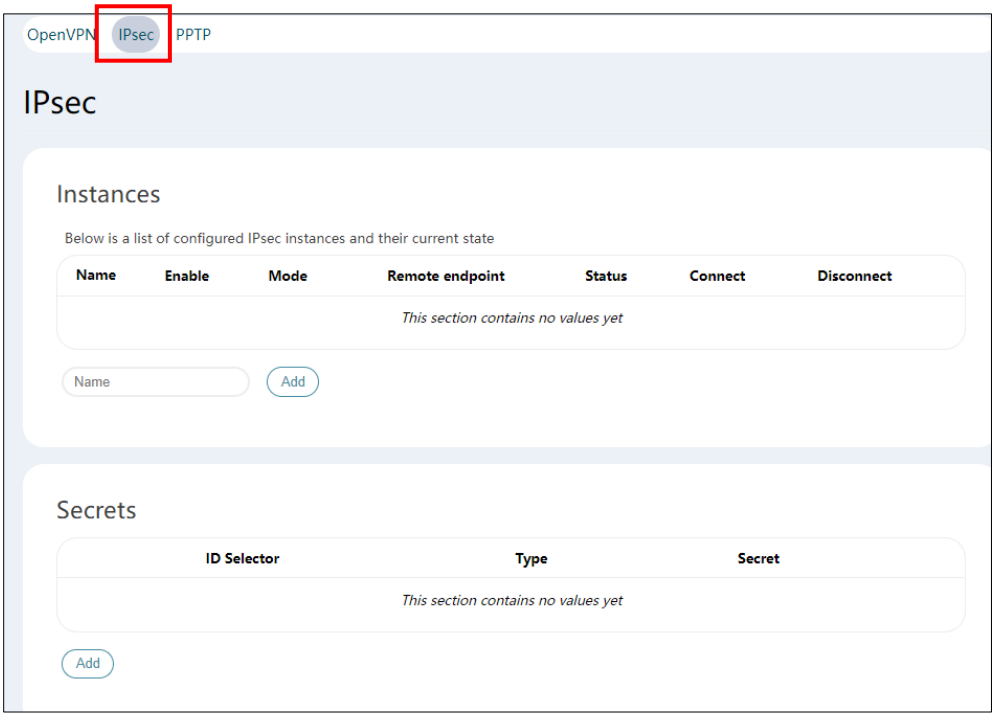


- ۶ حالت به صورت نمونه قابل انتخاب است:
  - Client configuration for an ethernet bridge VPN
  - Client configuration for a routed multi-client VPN
  - Simple client configuration for a routed point-to-point VPN
  - Server configuration for an ethernet bridge VPN

- Server configuration for a routed multi-client VPN
- Simple server configuration for a routed point-to-point VPN

۲-۱-۳-۵ پروتکل IPsec

- IPSec مخفف و کوتاه شده عبارت IP Security است که به مجموعه ای از پروتکل ها اشاره کرده و تبادل امن بسته ها در لایه IP را پشتیبانی میکند.
- IPSec بطور گسترده در تکنولوژی VPN جهت احراز هویت، محرمانگی، یکپارچگی و مدیریت کلید در شبکه های مبتنی بر IP، مورد استفاده قرار میگیرد.

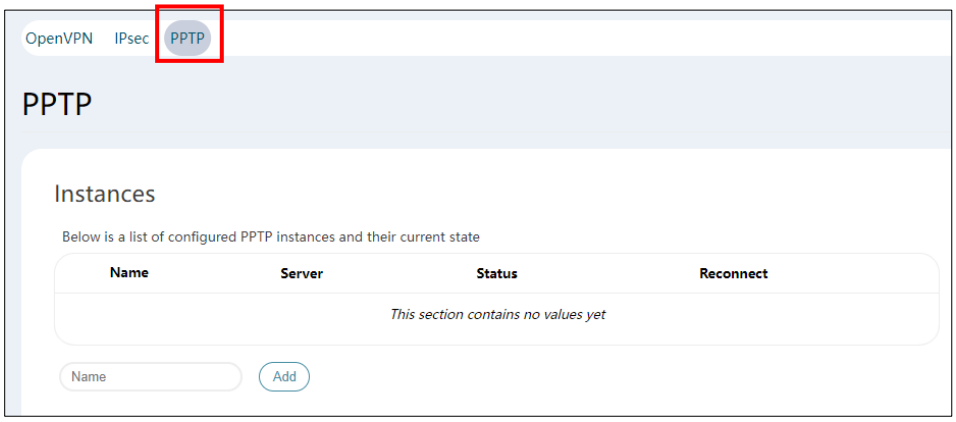


- از ۲ بخش اصلی تشکیل شده است:
  - Instances
  - Secrets
- جدول قسمت Instances از ۷ عنوان زیر تشکیل شده است:
  - Name : نام
  - Enable : وضعیت فعال بودن
  - Mode : حالت
  - Remote endpoint : نقطه پایانی از راه دور
  - Status : وضعیت

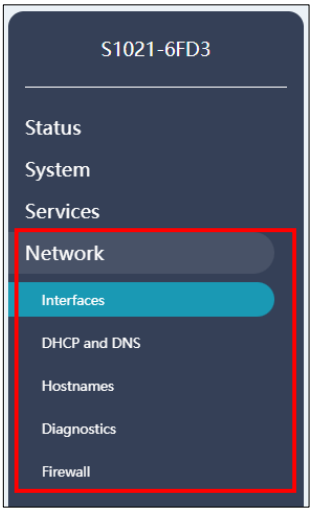
- Connect : وضعیت اتصال
- Disconnect : وضعیت عدم اتصال
- جدول قسمت Secrets از ۳ عنوان زیر تشکیل شده است:
  - ID Selector : شناسه انتخابگر
  - Type : نوع
  - Secret : رمز

۳-۱-۳-۵ پروتکل PPTP

- PPTP یکی از رایج ترین و البته ضعیف ترین پروتکل‌هایی است که در ارتباطات VPN استفاده می‌شود.
- PPTP مخفف Point-to-Point Tunneling Protocol است توسط شرکت مایکروسافت ایجاد شده است که برای تونلینگ استفاده شده و با پروتکل MPPE رمزگذاری می‌شود.



- جدول این بخش از ۳ عنوان زیر تشکیل شده است :
  - NAME : نام
  - Server : ادرس سرور
  - Status : وضعیت
  - Reconnect : فرمان وضعیت اتصال مجدد به صورت دستی



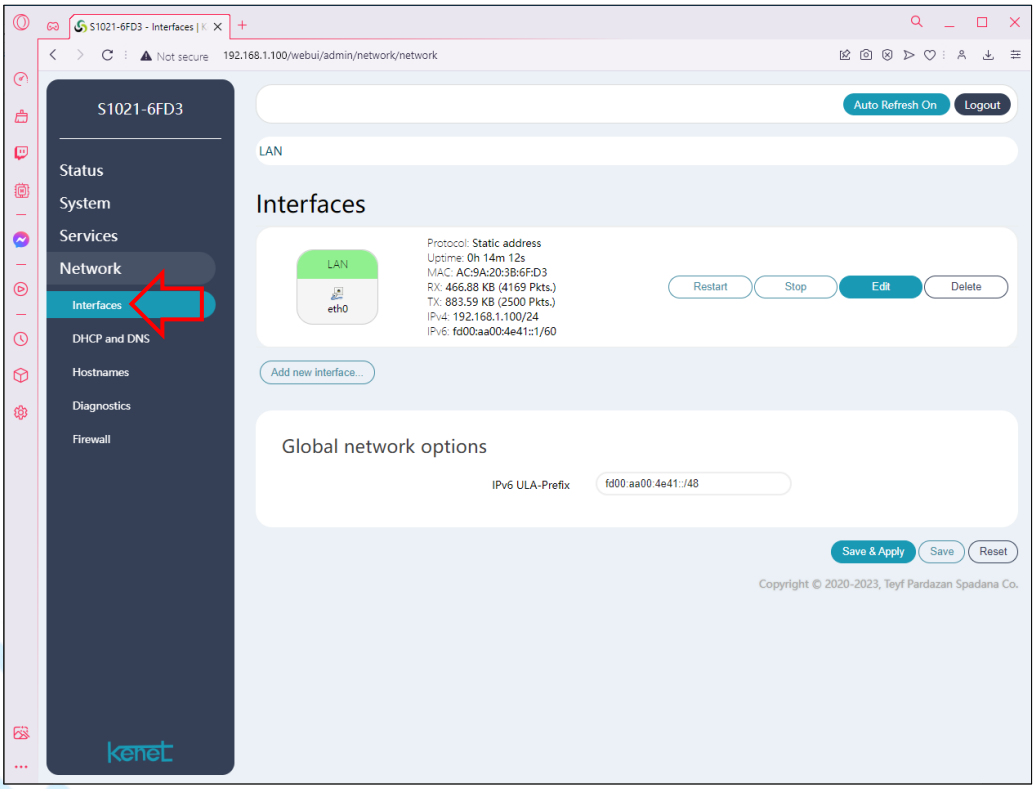
۶- بخش network

در این بخش به معرفی بخش network مبدل پرداخته می شود.

۶-۱ قسمت های بخش network

- قسمت Interfaces
- قسمت DHCP and DNS
- قسمت Hostnames
- قسمت Diagnostics
- قسمت Firewall

۶-۲ قسمت Interfaces



۶-۲-۱ معرفی Interfaces

- در این بخش ، اطلاعات پورت LAN مبدل قابل دسترسی و پیکربندی است.
- این بخش از ۳ قسمت زیر تشکیل شده است :
  - LAN
  - Global network options

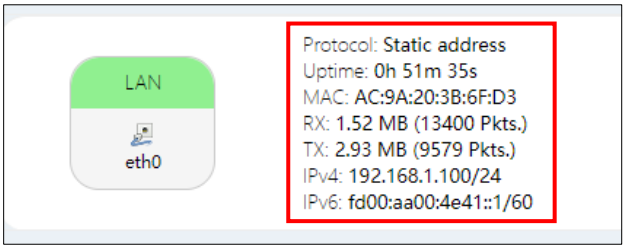
- ADD NEW INTERFACE

۶-۲-۲ بخش LAN

- از ۲ قسمت تشکیل شده است:
- اطلاعات مشخصاتی LAN
- دکمه های کنترلی LAN سمت راست

۶-۲-۲-۱ اطلاعات مشخصاتی LAN

- Protocol : پروتکل فعلی LAN
- Uptime : زمان فعال بودن
- MAC : ادرس MAC پورت LAN
- RX : میزان PKs های دریافتی
- TX : میزان PKs های ارسالی
- IPv4 : ادرس IP ویرایش ۴
- IPv6 : ادرس IP ویرایش ۶

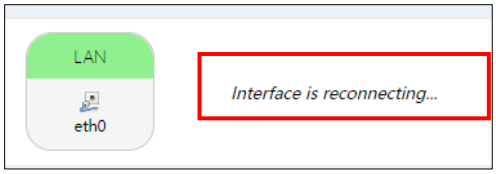


۶-۲-۲-۲ دکمه های کنترلی LAN

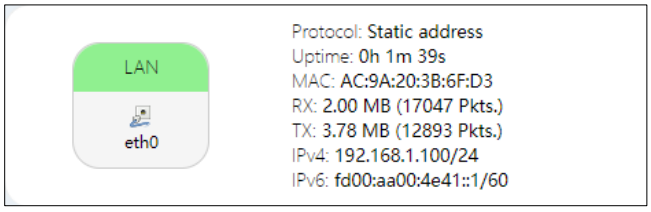
- RESTART : راه اندازی مجدد LAN
- STOP : توقف فعالیت LAN
- EDIT : ویرایش LAN
- DELET : حذف LAN

۶-۲-۲-۱ بخش RESTART

- این بخش باعث اتصال مجدد پورت LAN می شود.

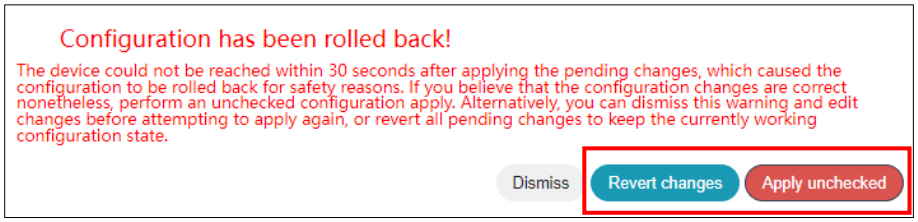


- در نهایت ، LAN مجددا راه اندازی می شود.



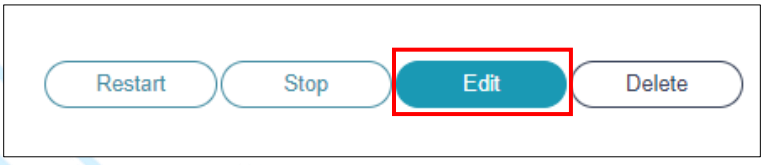
۶-۲-۲-۲-۲ بخش STOP

- این بخش باعث توقف فعالیت LAN می گردد.
- در صورت انتخاب این گزینه پیام هشدار زیر نمایش داده می شود.

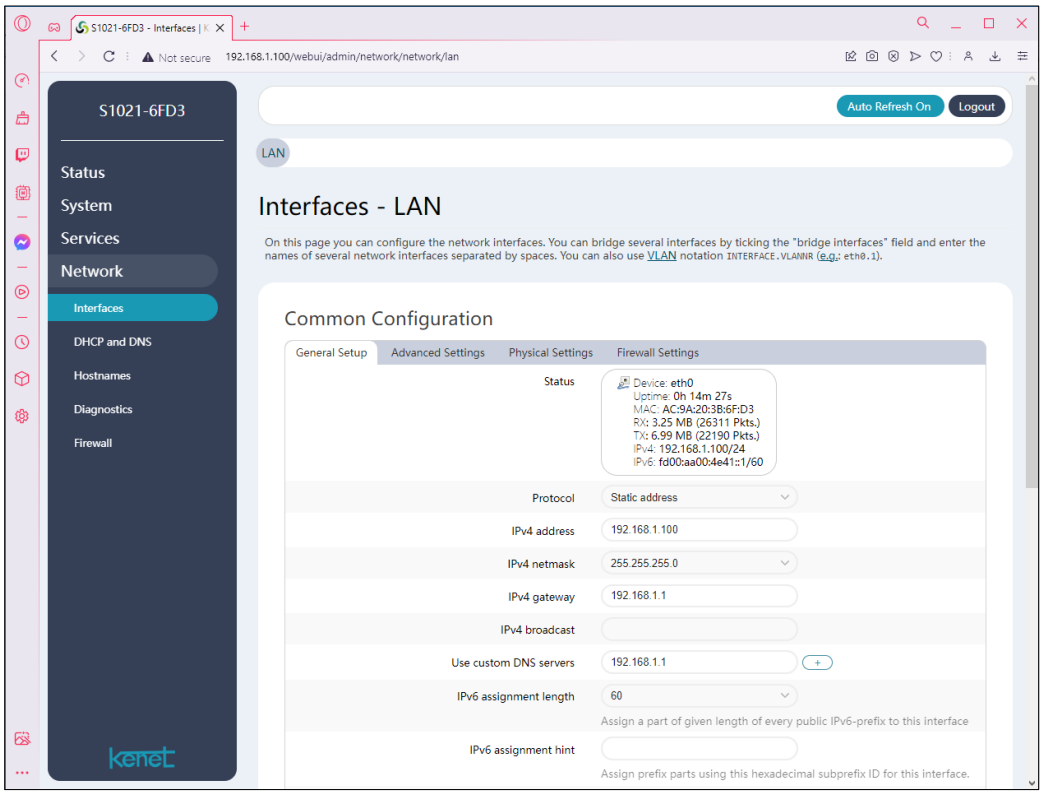


- در صورتی که قصد توقف LAN را دارید گزینه APPLY UNCHECKED را انتخاب نمایید؛ در غیر این صورت برای بازگرداندن این عمل ، گزینه REVERT CHANGES را انتخاب نمایید.
- در نظر داشته باشید در صورتی که گزینه APPLY را انتخاب کنید ارتباط شما با مبدل قطع می شود.

۶-۲-۲-۲-۳ بخش EDIT



- در صورا انتخاب این گزینه به بخش تنظیمات LAN وارد می شوید.



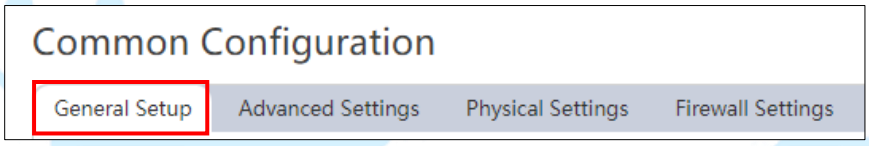
- این بخش از ۲ زیر بخش زیر تشکیل شده است.
  - Common Configuration
  - DHCP Server

۱-۳-۲-۲-۶ زیر بخش Common Configuration

- این قسمت از ۴ قسمت تشکیل شده است:
  - General Setup : تنظیمات کلی
  - Advanced Settings : تنظیمات تخصصی
  - Physical Settings : تنظیمات لایه فیزیکی
  - Firewall Settings : تنظیمات بخش FIREWALL

۱-۱-۳-۲-۲-۶ بخش General Setup

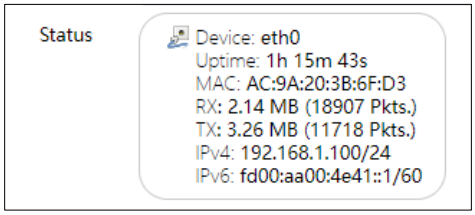
- تنظیمات کلی در این بخش قرار دارد.



- این بخش از قسمت های زیر تشکیل شده است:

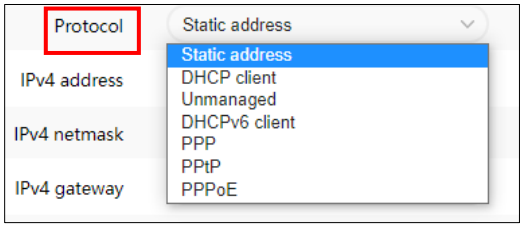
- Status

که بیانگر وضعیت کلی LAN می باشد.



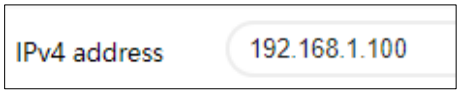
- Protocol

در این بخش می توانید پروتکل مد نظر خود را انتخاب کنید.



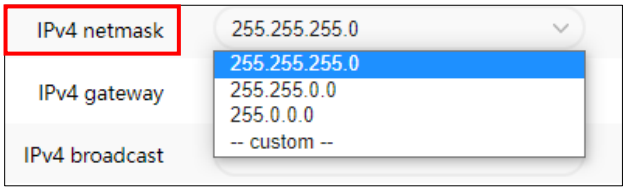
- IPv4 address

ادرس IP ویرایش ۴ مبدل را می توانید ویرایش کنید.



- IPv4 netmask

NETMASK را می توانید انتخاب کنید.



- IPv4 gateway

IP GATEWAY خود را می توانید ویرایش کنید.

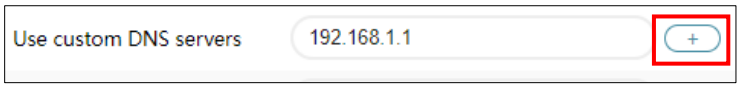
- IPv4 broadcast

می توانید ادرس IP برای BROADCAST خود را وارد کنید.

- Use custom DNS servers

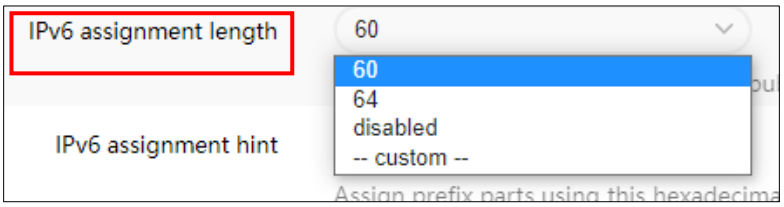
اگر DNS خود را می خواهید سفارشی سازی کنید از این قسمت استفاده کنید.

با زدن روی گزینه علامت + می توانید DNS خود را اضافه کنید.



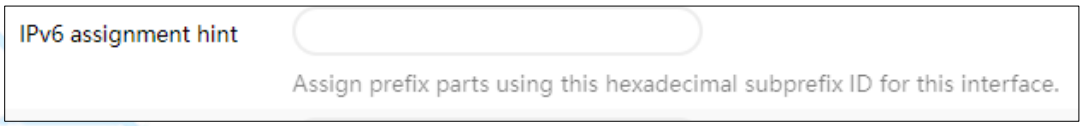
- IPv6 assignment length

بخشی از طول هر پیشوند عمومی IPv6 را به این رابط اختصاص دهید.



- IPv6 assignment hint

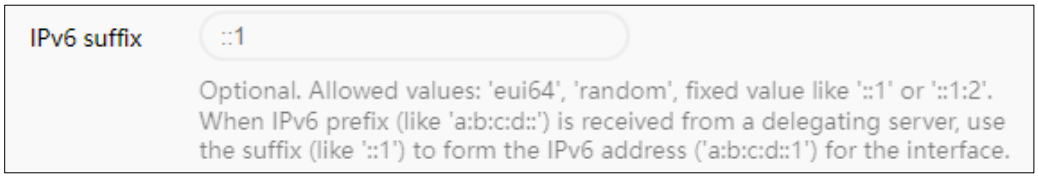
قسمت پیشوند را با استفاده از این شناسه ، زیر پیشوند هگزادسیمال برای این رابط اختصاص دهید.



- IPv6 suffix

بخش اختیاری؛ مقادیر مجاز: 'eui64'، 'تصادفی'، مقدار ثابت مانند '::۱' یا '::۲:۱'.

هنگامی که پیشوند IPv6 (مانند 'a:b:c:d::') از یک سرور واگذار کننده دریافت می شود، از پسوند (مانند '::۱') برای تشکیل آدرس IPv6 (‘a:b:c:d:1’) استفاده کنید.

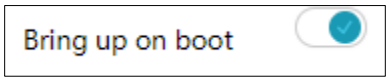


۲-۱-۳-۲-۲-۲-۶ بخش Advanced Settings

- تنظیمات تخصصی در این بخش قرار دارد.

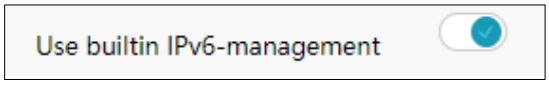
- این بخش از قسمت های زیر تشکیل شده است:
- Bring up on boot

فعال کردن در بوت



- Use builtin IPv6-management

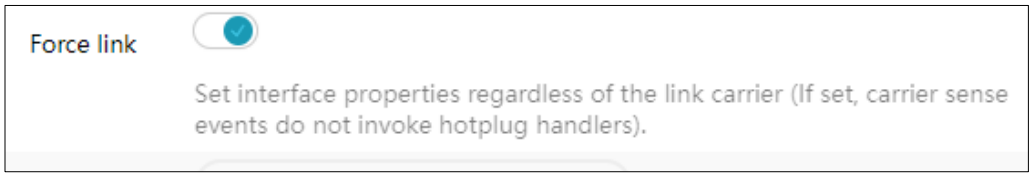
استفاده از مدیریت داخلی ipv6



- Force link

فعال کردن لینک فارغ از اتصال

ویژگی های رابط را بدون توجه به حامل پیوند تنظیم کنید (اگر تنظیم شود، رویدادهای حس حامل، کنترل کننده های هات پلاگ را احضار نمی کنند).؟



- Override MAC address

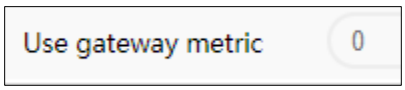
باز نویسی ادرس MAC

- Override MTU

باز نویسی mtu

- Use gateway metric

استفاده متریک دروازه

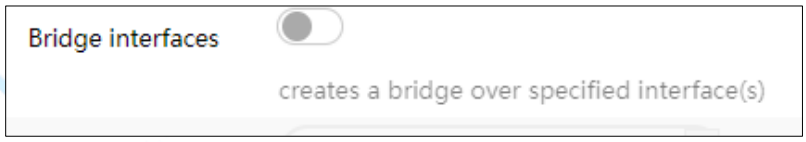


۳-۱-۳-۲-۲-۲-۶ بخش Physical Settings

- تنظمیات لایه فیزیکی شبکه در این بخش قرار دارد.

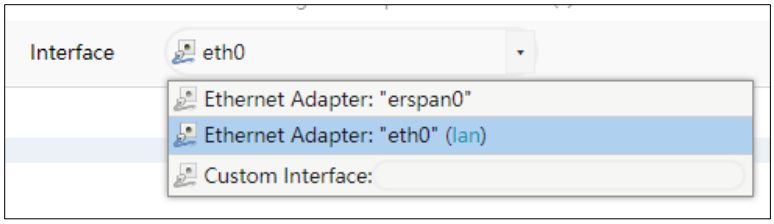
- این بخش از قسمت های زیر تشکیل شده است:
- Bridge interfaces

ایجاد یک brifge بین چند اینترفیس



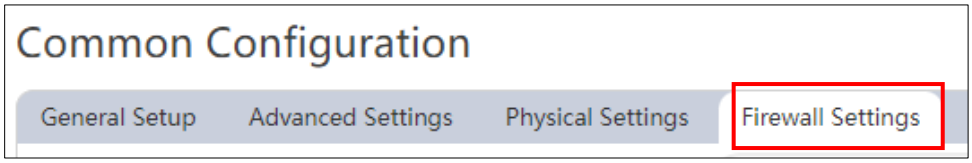
- Interface

اینترفیس

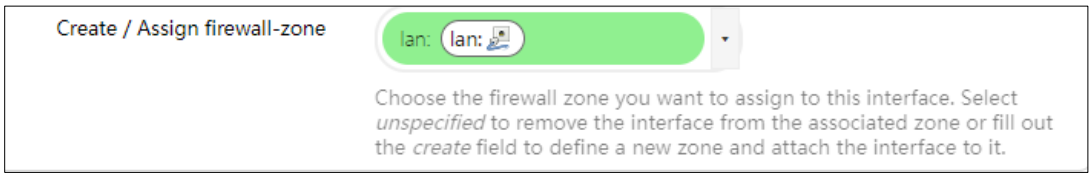


۴-۱-۳-۲-۲-۶-۲ بخش Firewall Settings

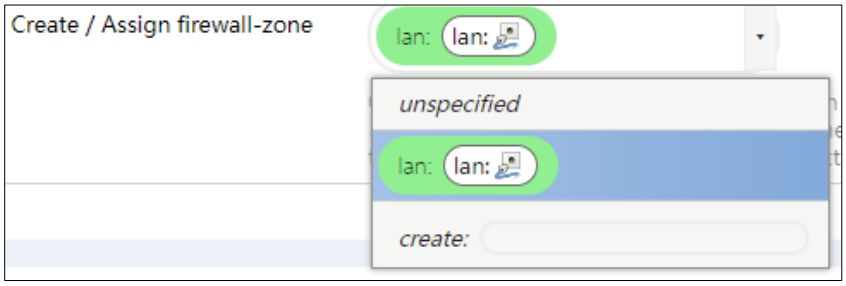
- تنظیمات Firewall شبکه در این بخش قرار دارد.



- تخصیص ناحیه فایروال



- هم چنین با بازکردن منو می توانید یک firewall zone ایجاد کنید و یا تخصیص دهید.

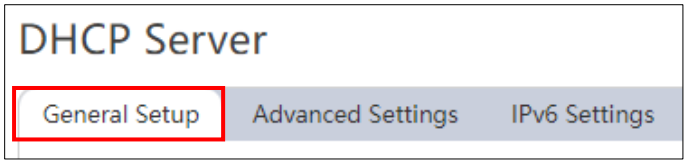


۲-۳-۲-۲-۲-۶-۲ زیر بخشDHCP Server

- این قسمت از ۳ قسمت تشکیل شده است:
- General Setup : تنظیمات کلی
- Advanced Settings : تنظیمات تخصصی
- IPv6 Settings: تنظیمات IPV6

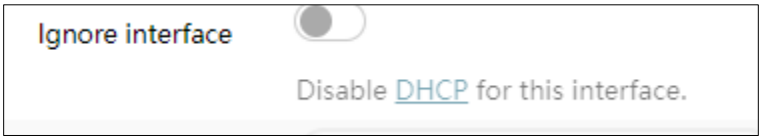
۱-۲-۳-۲-۲-۶ بخش General Setup

- تنظیمات کلی در این بخش قرار دارد.



- این بخش از قسمت های زیر تشکیل شده است:
- Ignore interface

نادیده گرفتن اینترفیس

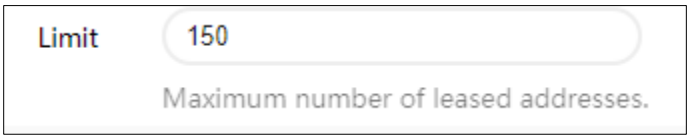


- Start

شروع

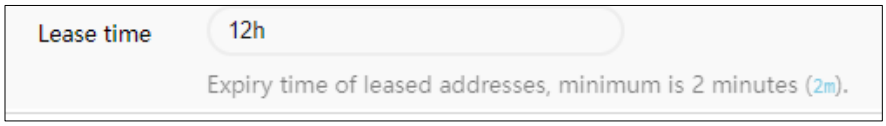
- Limit

محدود کردن



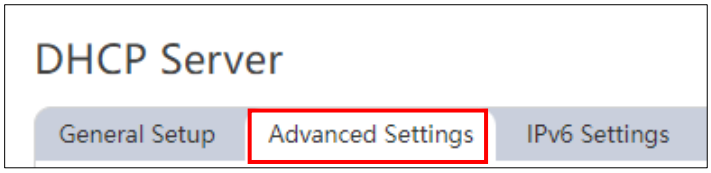
- Lease time

مدت زمان اختصاص ip توسط سرور dhcp



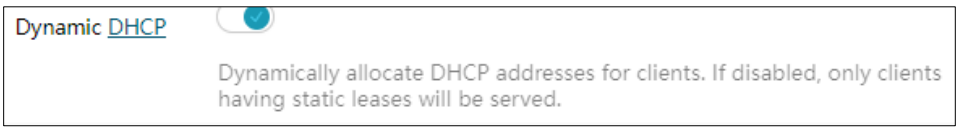
۲-۲-۳-۲-۲-۲-۶ بخش Advanced Settings

- تنظمیات تخصصی در این بخش قرار دارد.



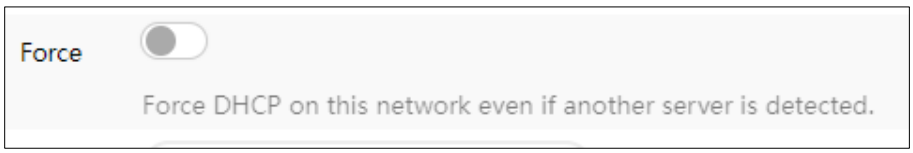
- این بخش از قسمت های زیر تشکیل شده است:
- Dynamic DHCP

فعال کردن سرویس تخصیص ip خودکار



- Force

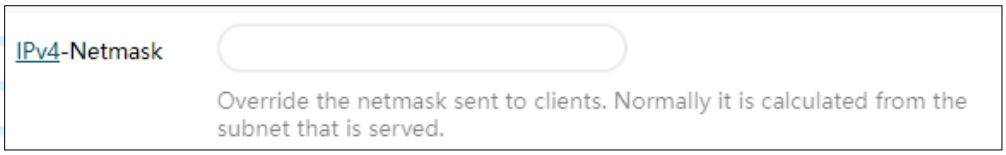
حتی اگر سرور دیگری شناسایی شود، DHCP را در این شبکه اجباری کنید.



- IPv4-Netmask

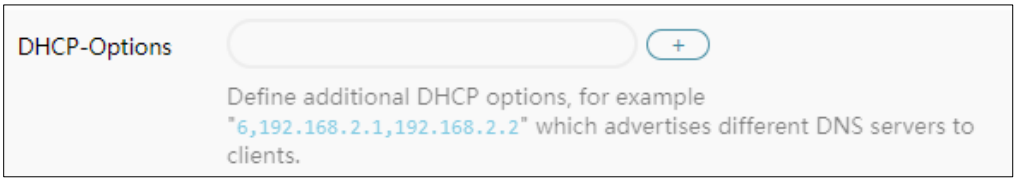
Netmask ارسال شده به مشتریان را بازنویسی کنید.

معمولاً از زیر شبکه ای که ارائه می شود محاسبه می شود.



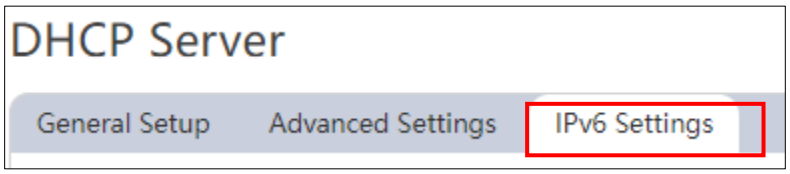
- DHCP-Options

گزینه های اضافی DHCP را تعریف کنید، برای مثال ۶,۱۹۲.۱۶۸.۲.۱,۱۹۲.۱۶۸.۲.۲" که سرورهای DNS مختلف را برای مشتریان تبلیغ می کند.



۳-۲-۳-۲-۲-۶ بخش IPv6 Settings

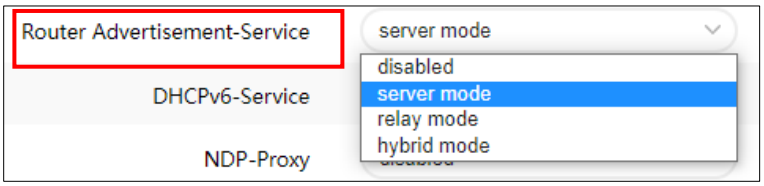
- تنظیمات IPV6 در این بخش قرار دارد.



- این بخش از قسمت های زیر تشکیل شده است:

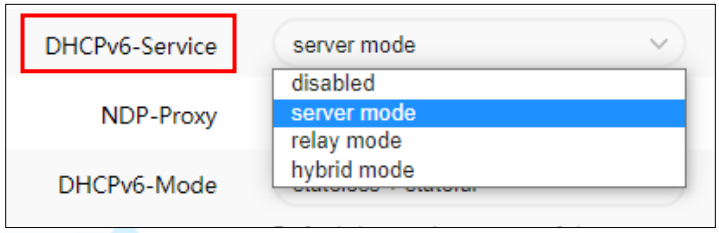
- Router Advertisement-Service

برای پیکربندی و مسیریابی خودکار IPv6 استفاده می شود.



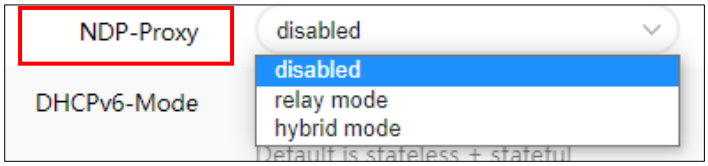
- DHCPv6-Service

سرویس تخصیص ip خودکار توسط ipv6



- NDP-Proxy

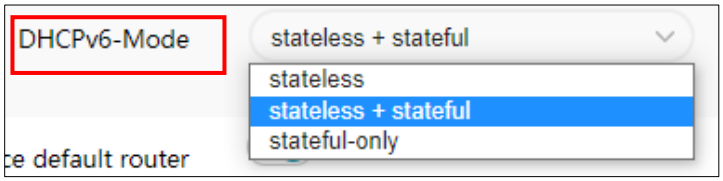
پروتکل Neighbor Discovery Protocol به ارتباط بین میزبان های همسایه در شبکه های محلی کمک می کند و مسیریاب دروازه را تعیین می کند.



- DHCPv6-Mode

تعیین حالت کاری dhcpv6

حالت پیشفرض stateless + stateful است.

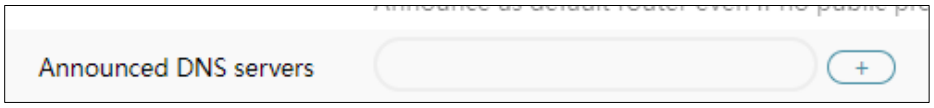


- Always announce default router

به عنوان روتر پیش فرض اعلام کنید حتی اگر هیچ پیشوند عمومی در دسترس نباشد.

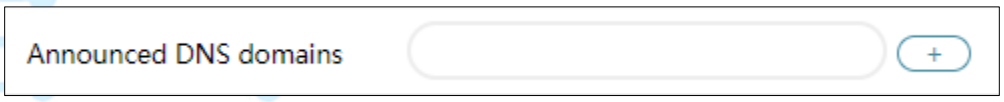
- Announced DNS servers

تنظیم DNS servers



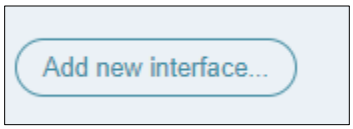
- Announced DNS domains

تنظیم DNS domains

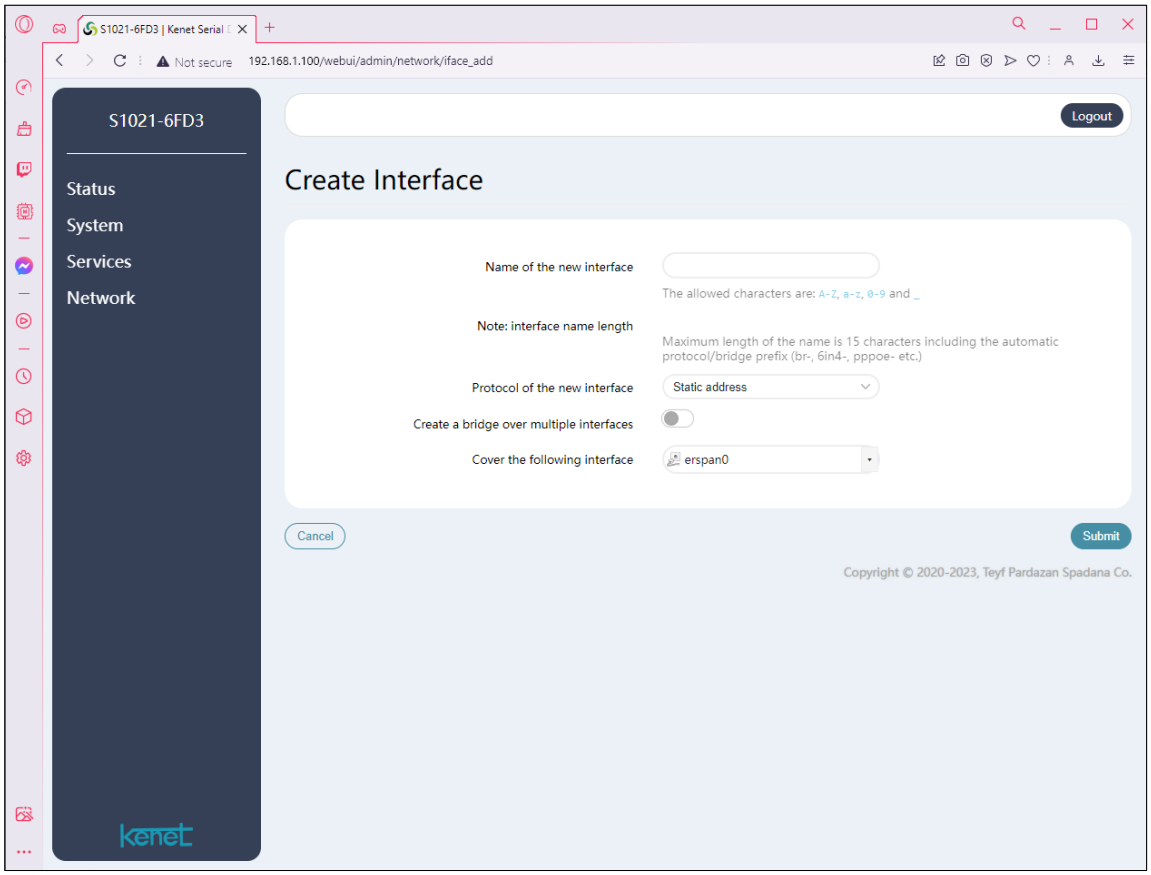


۳-۲-۶ بخش ADD NEW INTERFACE

- برای اضافه کردن INTERFACE جدید از این قسمت استفاده می کنیم.



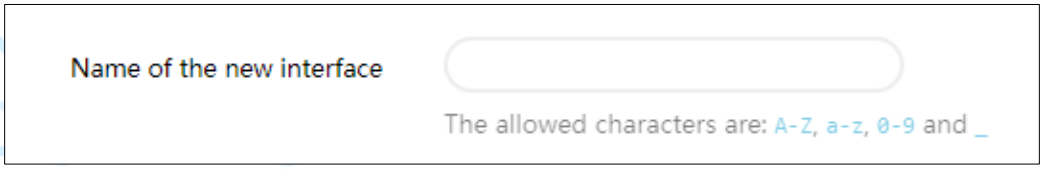
- پس از انتخاب این گزینه به صفحه زیر می رویم.

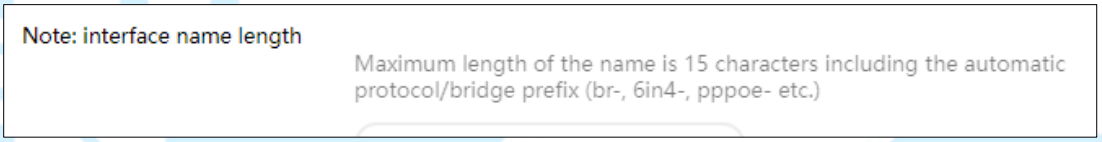


- از ۴ قسمت زیر تشکیل شده است:

- Name of the new interface

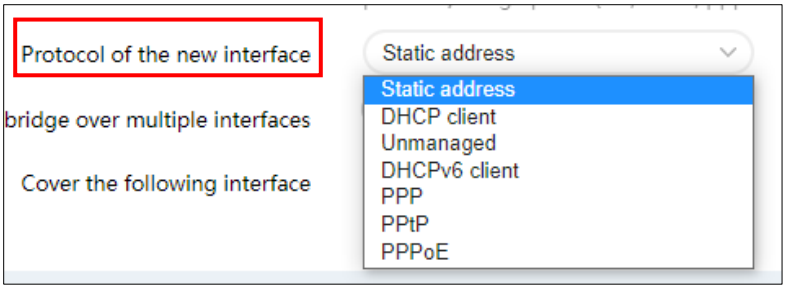
انتخاب نام برای اینترفیس جدید





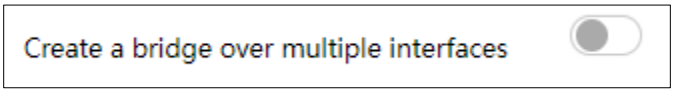
- Protocol of the new interface

تخصیص پروتکل برای اینترفیس جدید



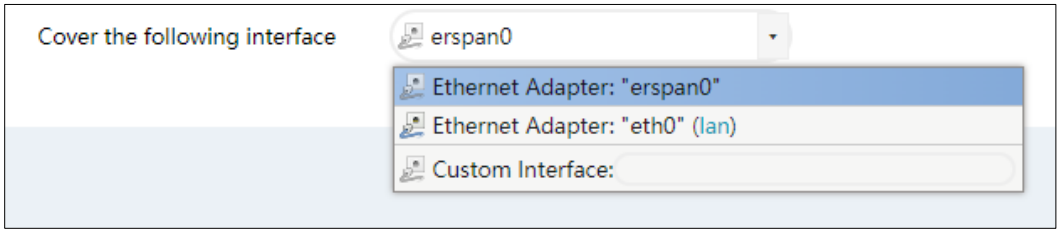
- Create a bridge over multiple interfaces

ایجاد یک bridge برای چندین رابط



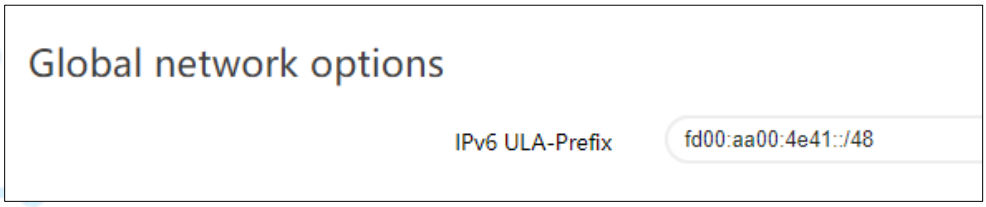
- Cover the following interface

این اینترفیس شامل چه دستگاهی شبکه ای هست.

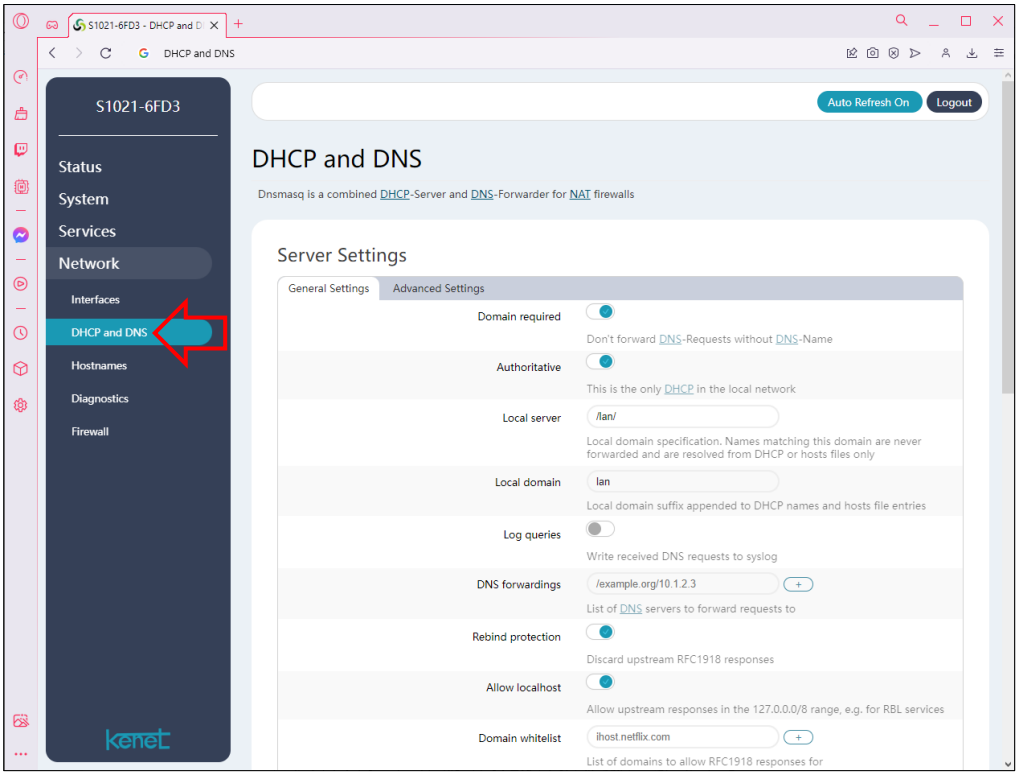


۶-۲-۴ بخش Global network options

- گزینه های عمومی شبکه



۶-۳ قسمت DHCP and DNS



۶-۳-۱ معرفی DHCP and DNS

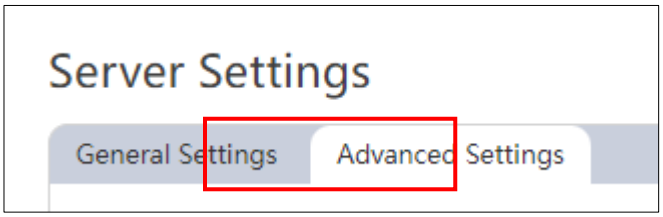
- در این بخش ، dns و dhcp پیکربندی می شود.
- این بخش از ۴ قسمت زیر تشکیل شده است :
  - Server Settings
  - Active DHCP Leases
  - Active DHCPv6 Leases
  - Static Leases

۶-۳-۲ بخش Server Settings

- این بخش از ۲ قسمت زیر تشکیل شده است:
  - General Settings
  - Advanced Settings

۶-۳-۲-۱ قسمت General Settings

- تنظیمات کلی در این بخش قرار دارد.



- از بخش های زیر تشکیل شده است:

- Domain required

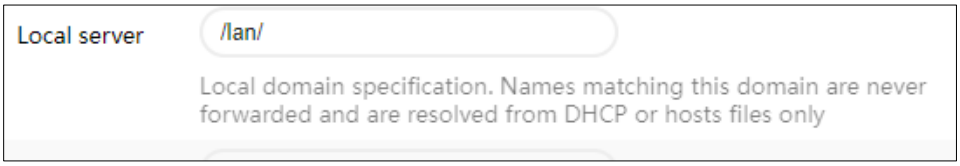
درخواست‌های DNS را بدون DNS-Name فوروارد نکنید.

- Authoritative

این تنها DHCP در شبکه محلی است

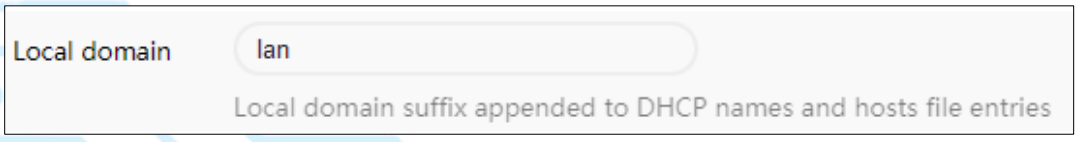
- Local server

سرور محلی؛ مشخصات دامنه محلی نام‌های مطابق با این دامنه هرگز ارسال نمی‌شوند و فقط از فایل‌های DHCP یا میزبان حل می‌شوند.



- Local domain

دامین محلی؛ پسوند دامنه محلی به نام های DHCP و ورودی های فایل میزبان اضافه شده است.



- Log queries

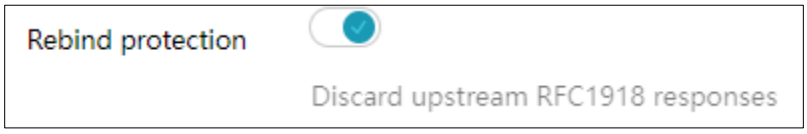
درخواست های DNS دریافتی را در syslog بنویسید.

- DNS forwardings

لیست سرورهای DNS برای ارسال درخواست ها

- Rebind protection

پاسخ‌های RFC1918 بالادست را کنار بگذارید

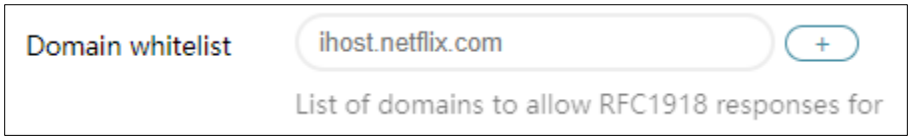


- Allow localhost

پاسخ‌های بالادستی را در محدوده ۱۲۷.۰.۰.۰/۸ مجاز کنید، به عنوان مثال. برای خدمات RBL

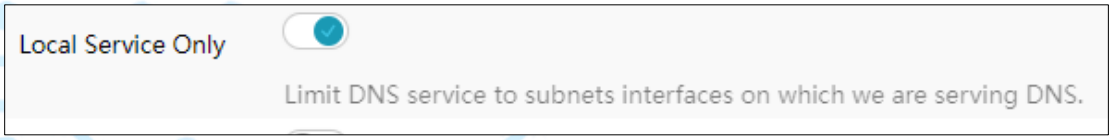
- Domain whitelist

فهرست دامنه‌هایی که اجازه پاسخ‌های RFC1918 را می‌دهند.



- Local Service Only

سرویس DNS را به واسطهای زیرشبکه‌ای که در آن DNS ارائه می‌کنیم محدود کنید.

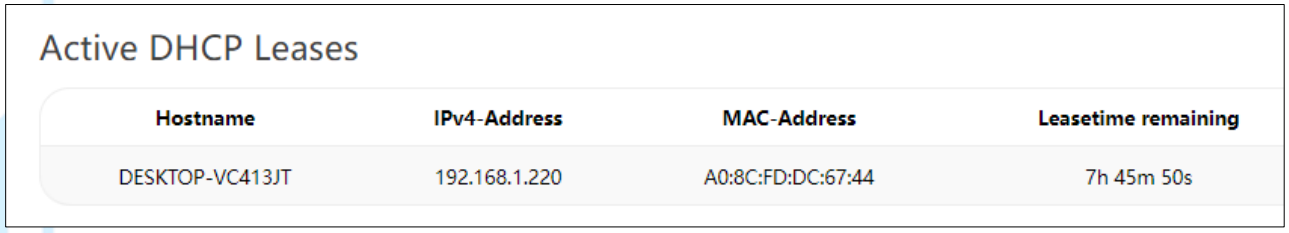


- Non-wildcard

فقط به اینترفیس‌های خاص متصل شود نه آدرس عام.

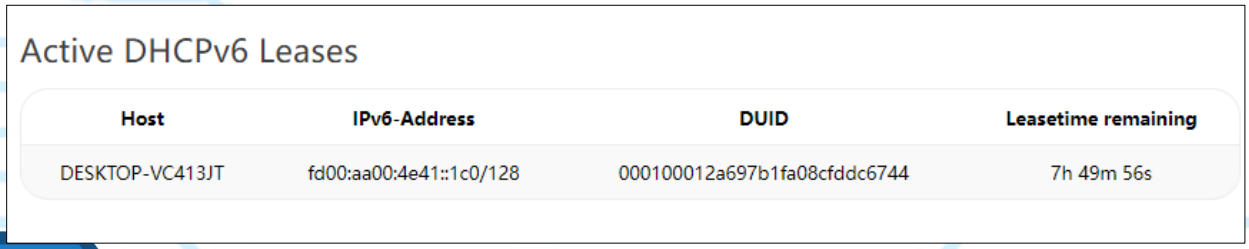
۶-۳-۳ بخش Active DHCP Leases

- جدول اختصاص های فعال dhcp
- از جدولی با ۴ ستون زیر تشکیل شده است:
  - Hostname : نام دستگاه
  - IPv4-Address : ادرس IPV4
  - MAC-Address : ادرس mac
  - Leasetime remaining : زمان باقی مانده از اختصاص ip



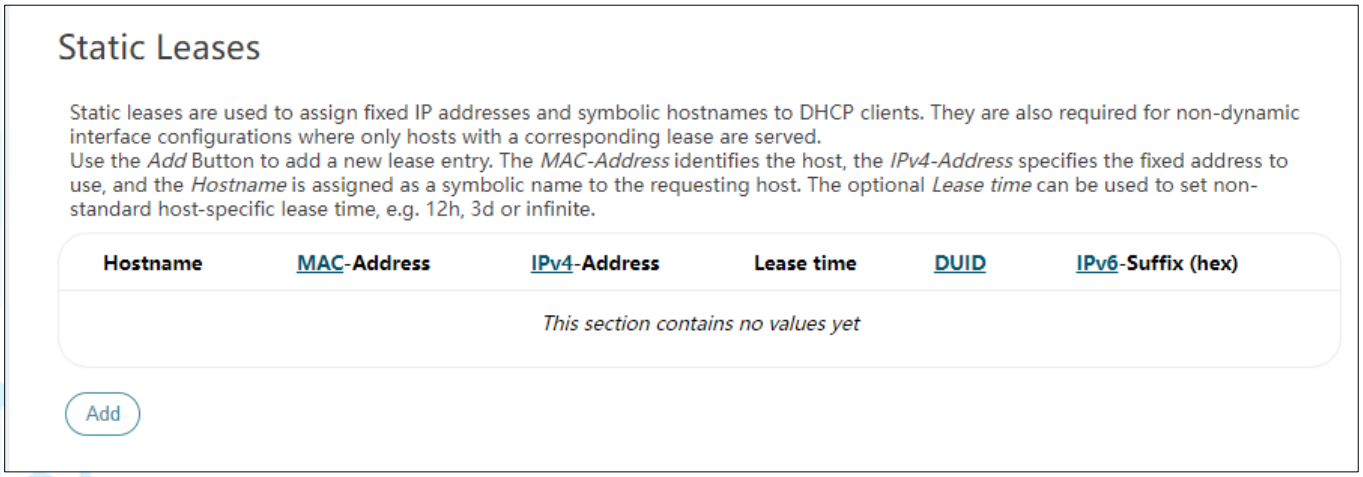
۶-۳-۴ بخش Active DHCPv6 Leases

- جدول اختصاص های فعال dhcp ویرایش۶
- از جدولی با ۴ ستون زیر تشکیل شده است:
  - Hostname : نام دستگاه
  - IPv4-Address : ادرس ipv4
  - DUID : شناسه اختصاصی dhcp
  - Leasetime remaining : زمان باقی مانده از اختصاص ip

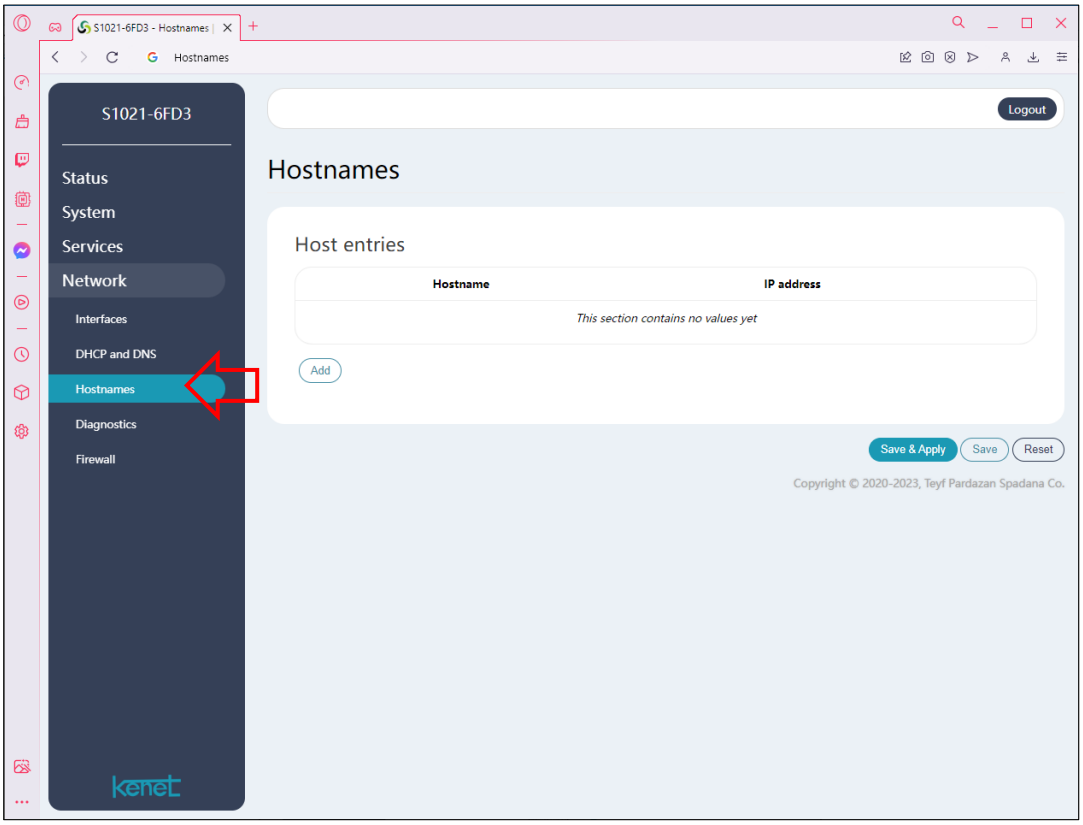


۵-۳-۶ بخش Static Leases

- اختصاص ثابت ip فارغ از سرور dhcp
- از جدولی با ۶ ستون زیر تشکیل شده است:
  - Hostname : نام دستگاه
  - MAC-Address : ادرس mac
  - IPv4-Address : ادرس ipv4
  - Lease time : زمان باقی مانده از اختصاص ip
  - DUID : شناسه اختصاصی dhcp
  - IPv6-Suffix (hex) : Pv6-Suffix به صورت هگزادسیمال



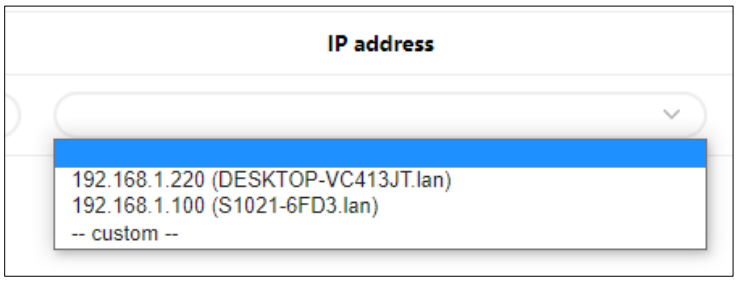
۶-۴ قسمت Hostnames



- تخصیص یا اختصاص یک هاست نیم به یک ip خاص در dns سرور
- این بخش از قسمت Host entries تشکیل شده که ۲ فیلد زیر را دارا می باشد:
  - Hostname
  - IP address
- هم چنین شما می توانید با زدن گزینه add، دستگاه های ورودی خود را اضافه کنید.

- پس از زدن این گزینه یک ردیف خالی برای شما اضافه می شود.

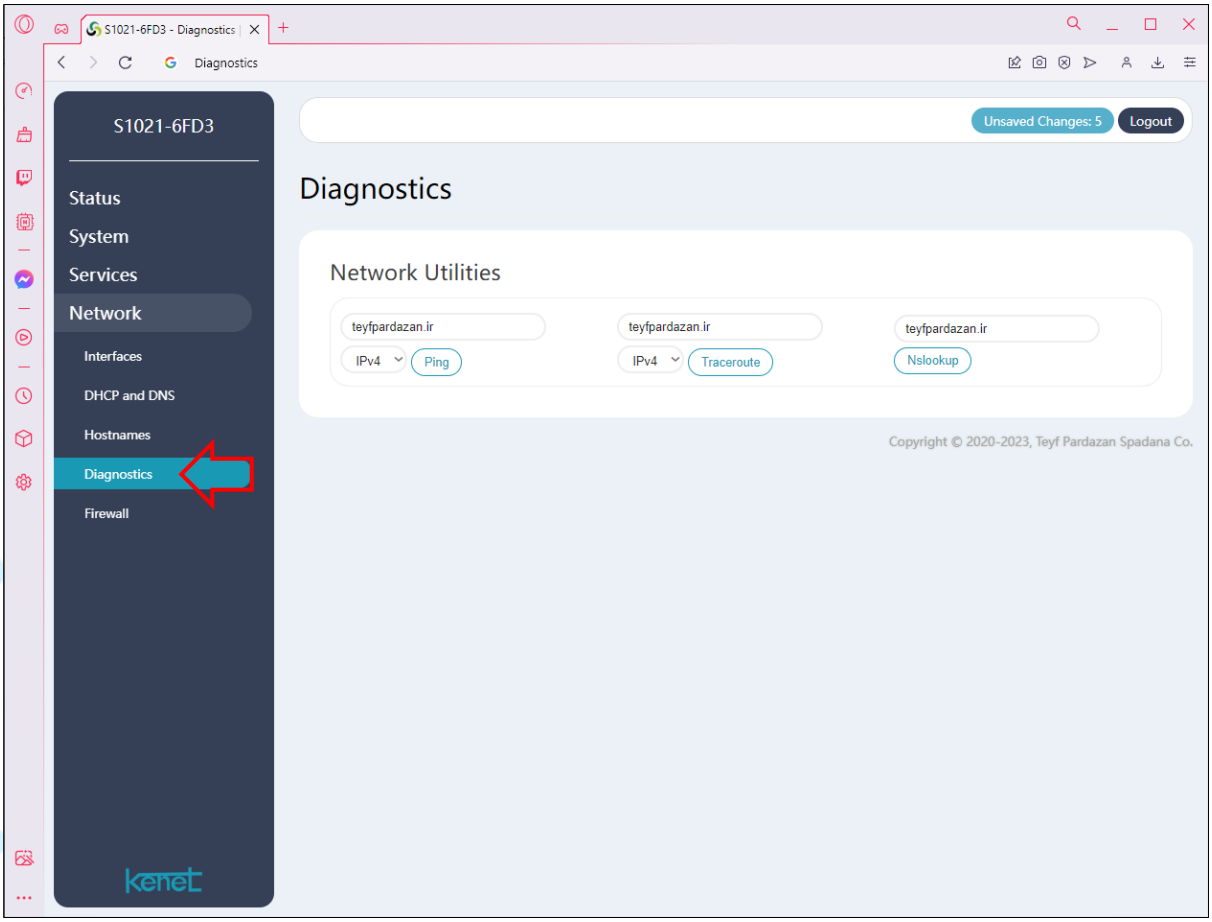
- در قسمت hostname می توانید نام مد نظر خود را وارد کنید.
- هم چنین در قسمت ip address می توانید ادرس ip مد نظر خود را برای این ردیف تنظیم کنید.



- از سمت راست هم ، زا زدن delete می توانید این ردیف را حذف کنید.

- در اخر گزینه save & apply را باید انتخاب کنید.

۶-۵ قسمت Diagnostics



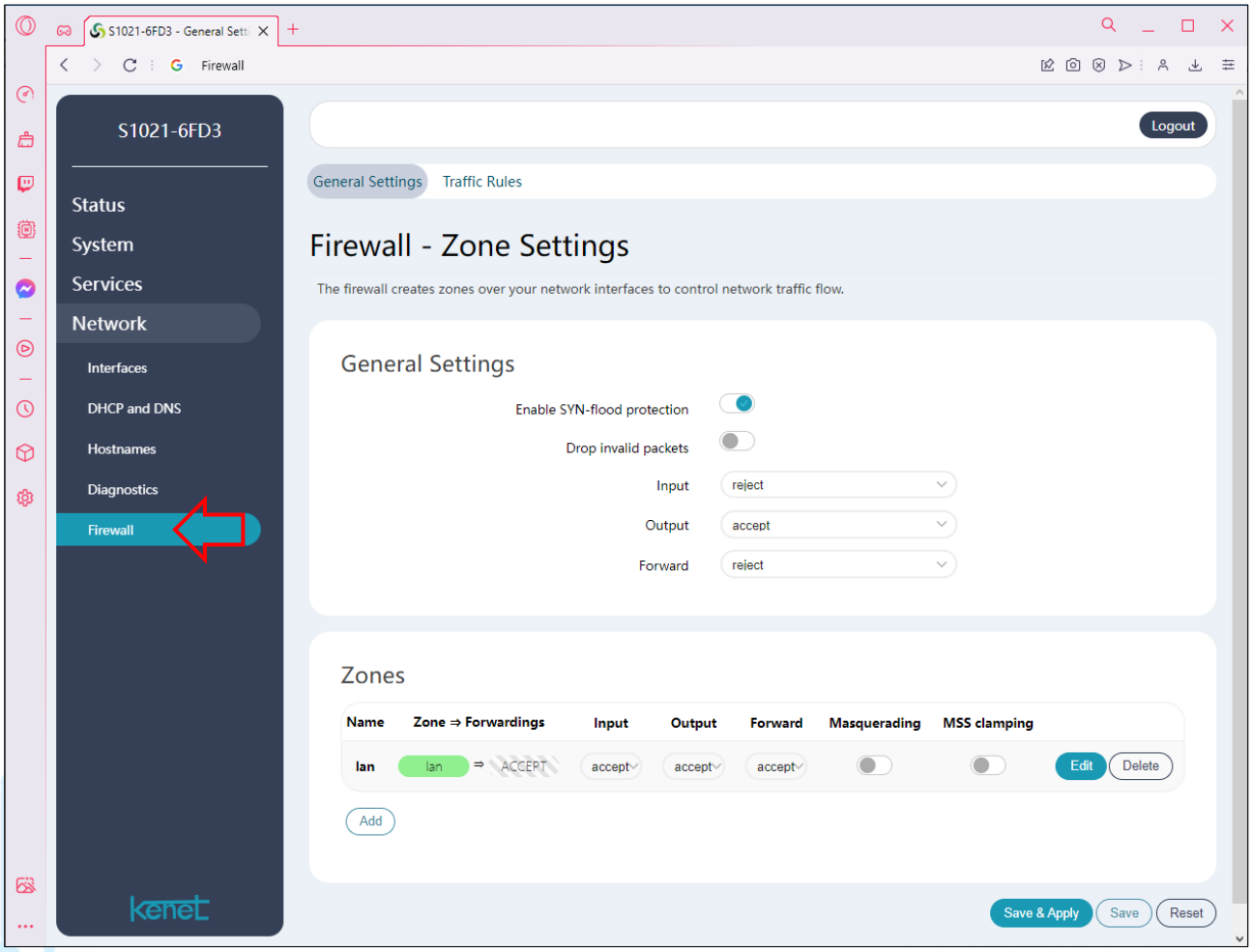
- از این بخش برای عیب یابی می توانید استفاده کنید.
- این بخش از قسمت Network Utilities تشکیل شده که ۳ فیلد زیر را دارا می باشد:
  - Ping

    پینگ کردن یک ای پی مشخص
  - Traceroute

    انجام عملیات مسیریابی
  - Nslookup

    استعلام ای پی یک دامنه از سرور دی ان اس

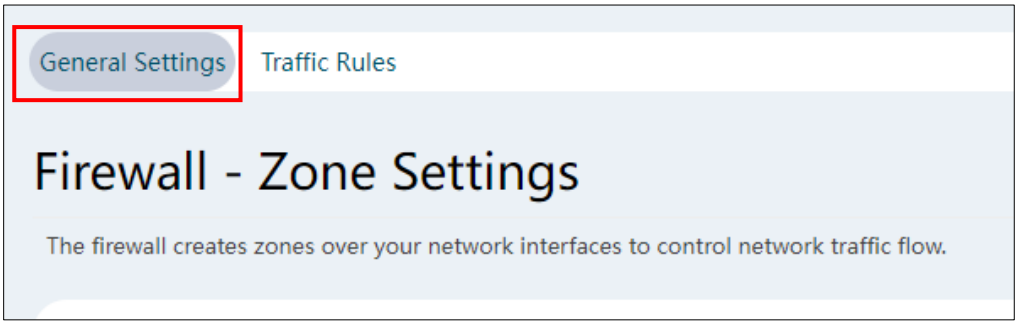
۶-۶ قسمت Firewall



۶-۶-۱ معرفی firewall

- در این قسمت یکسری تنظیمات مربوط به فایروال مبدل قابل انجام است.
- تنظیمات به صورت پیش فرض قرار دارد ، اگر همه بخش ها روی accept قرار داده شوند ، فایروال به درستی کار نمی کند.
- این بخش این ۲ قسمت زیر تشکیل شده است:
  - Zone Settings
  - Traffics rules

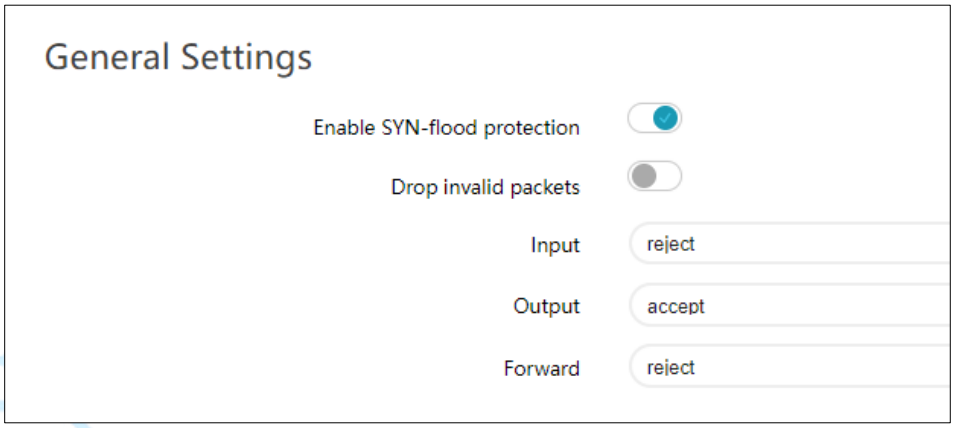
۲-۶-۶ بخش Zone Settings



- این بخش از ۲ بخش زیر تشکیل شده است:
  - General Settings
  - Zones

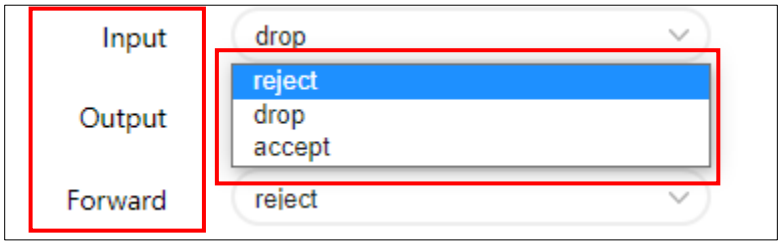
۱-۲-۶-۶ بخش General Settings

- در این بخش تنظیمات کلی انجام می پذیرد ؛ که از فیلد های زیر تشکیل شده است:
  - Enable SYN-flood protection : فعال کردن SYN-flood
  - Drop invalid packets : رها کردن بسته های نا معتبر
  - Input : ورودی
  - Output : خروجی
  - Forward : هدایت



- در بخش های input و output و forward فیلد های زیر قابل انتخاب هستند:
  - Reject : رد کردن

- Accept : قبول کردن
- Drop : رها کردن



۲-۲-۶-۶ بخش zone

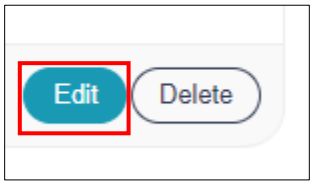
- بخش zone ها در این قسمت نمایش داده می شود.
- که Lan در این قسمت قرار دارد و قابل ویرایش است.

- همان طور که مشاهده می کنید از ۷ عنوان تشکیل شده است:

- Name : نام
- Zone Forwardings : هدایت کردن zone ها
- Input : ورودی
- Output : خروجی
- Forward : هدایت شده
- Masquerading : فعال کردن قابلیت Masquerading
- MSS clamping : فعال کردن قابلیت MSS clamping

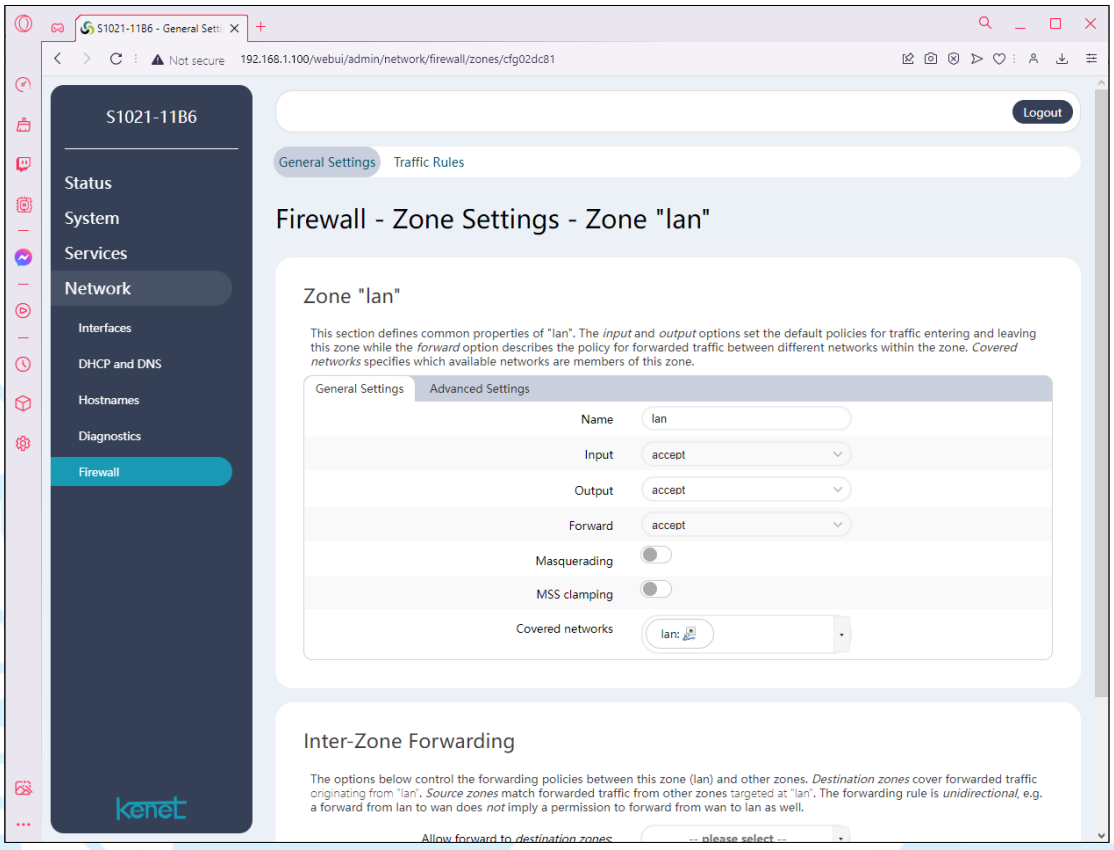
- هم چنین بخش های Input و output و forward را می توانید در ۳ حالت گفته شده قرار دهید.

- با استفاده از ۲ گزینه کناری می توانید lan را ویرایش و یا حذف کنید.



۱-۲-۶-۶ بخش edit

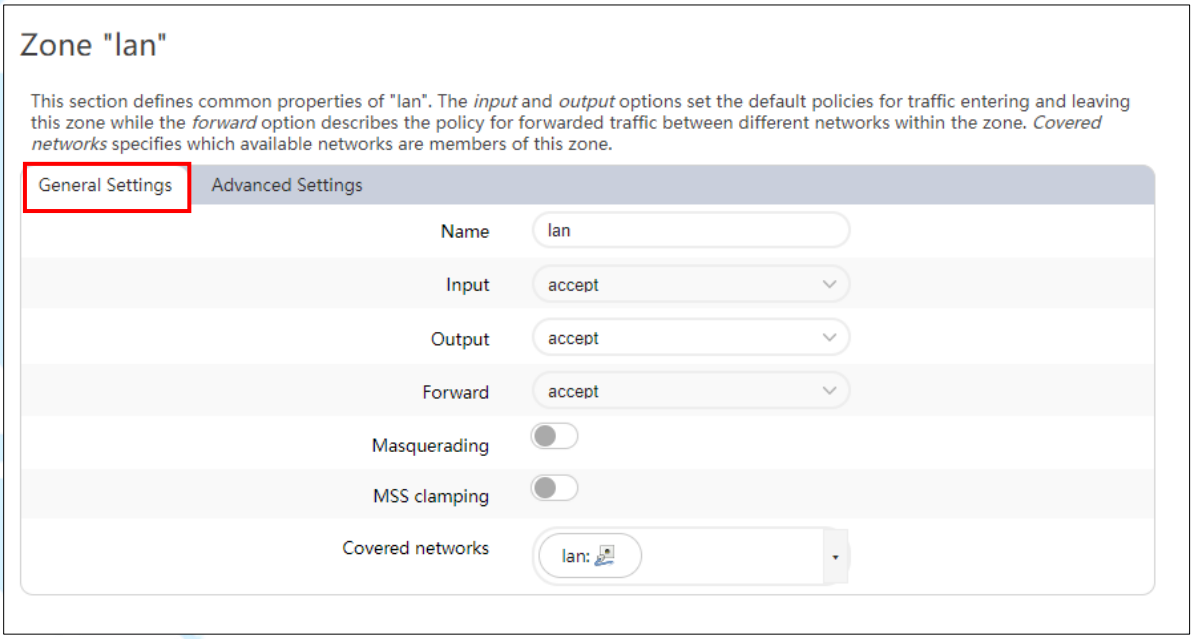
- پس از انتخاب این گزینه به صفحه ی زیر هدایت می شوید.



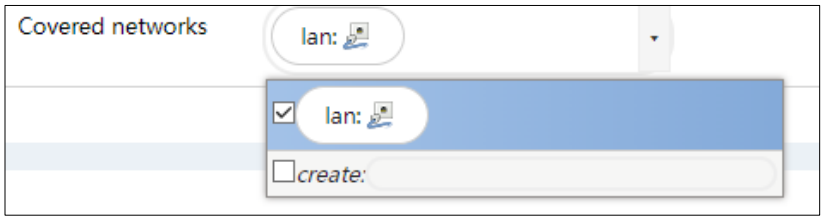
- بخش edit از ۲ قسمت زیر تشکیل شده است:
  - Zone lan
  - Inter-Zone Forwarding
- هم چنین بخش zone lan از ۲ بخش زیر تشکیل شده:
  - General Settings
  - Advanced Settings

۱-۱-۲-۲-۶-۶ قسمت General Settings

- در این بخش تنظیمات زیر قابل اعمال هستند:
  - Name : نام
  - Input : ورودی
  - Output : خروجی
  - Forward : هدایت شده
  - Masquerading : فعال کردن Masquerading
  - MSS clamping : فعال کردن MSS clamping
  - Covered networks : اینترفیس های شامل شده؟



- هم چنین در بخش convert network می توانید ، تنظیمات جدیدی را ایجاد کنید.

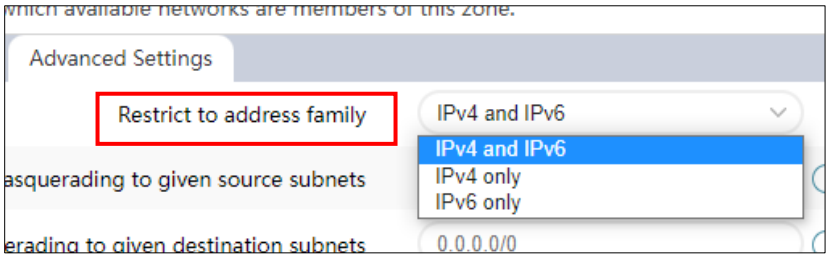


۲-۱-۲-۲-۶-۶ قسمت Advanced Settings

- در این بخش تنظیمات زیر قابل اعمال هستند:

Restrict to address family -

تعیین نوع ادرس ip

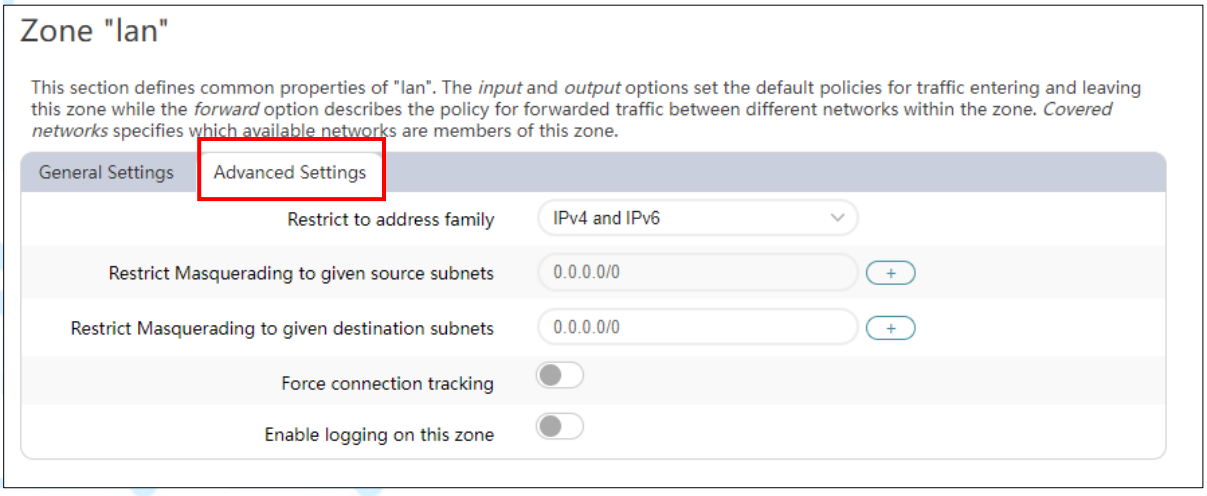


Restrict Masquerading to given source subnets -

Restrict Masquerading to given destination subnets -

Force connection tracking -

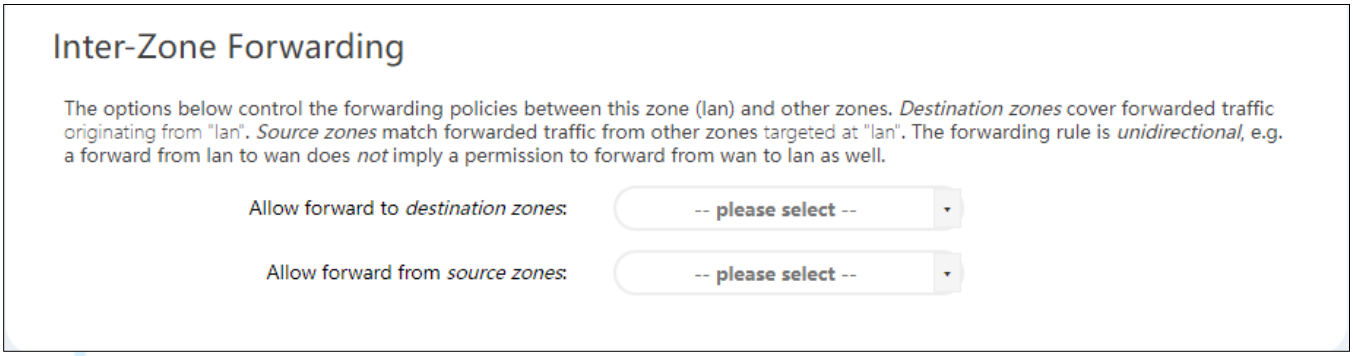
Enable logging on this zone -



- در صورت فعال کردن بخش Enable logging on this zone بخش زیر نمایش داده می شود.

۳-۱-۲-۲-۶-۶ قسمت Inter-Zone Forwarding

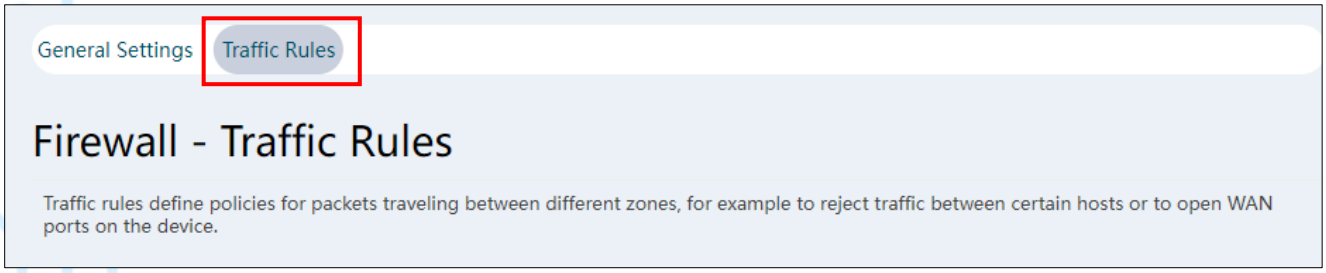
- در این بخش تنظیمات زیر قابل اعمال هستند:
- Allow forward to destination zones
  اجازه باز ارسالی به ناحیه مقصد
- Allow forward from source zones
  اجازه باز ارسالی از ناحیه مبدا



۲-۲-۶-۶ بخش delete

- با استفاده از این بخش هم می توانید zone lan را حذف کنید.

۳-۶-۶ بخش Traffic Rules



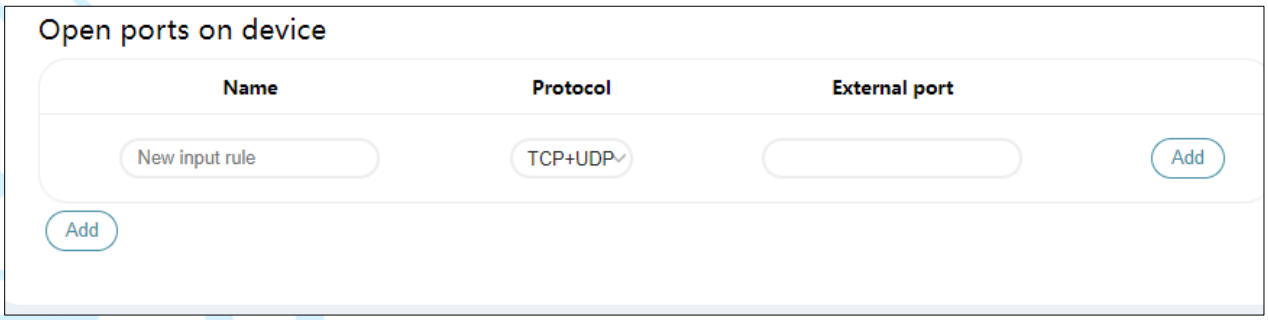
- این بخش از ۳ بخش زیر تشکیل شده است:
- Traffic Rules : کنترل ترافیک قوانین
- Open ports on device : پورت های باز شده
- Source NAT : عملیات source nat

۱-۳-۶-۶ بخش Traffic Rules

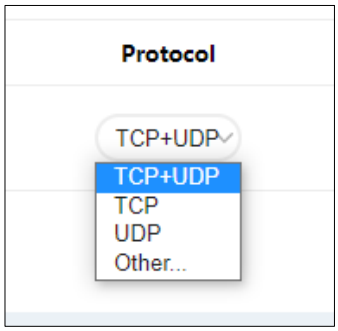
- در این قسمت ، Rule های تعریف شده قابل نمایش است.
- این بخش از فیلد های زیر تشکیل شده است:
  - Name : نام
  - Match : توضیح قوانینی که با این قانون ترافیکی تطبیق دارند.
  - Action : عملیات
  - Enable : فعال / غیرفعال نمودن

۲-۳-۶-۶ بخش Open ports on device

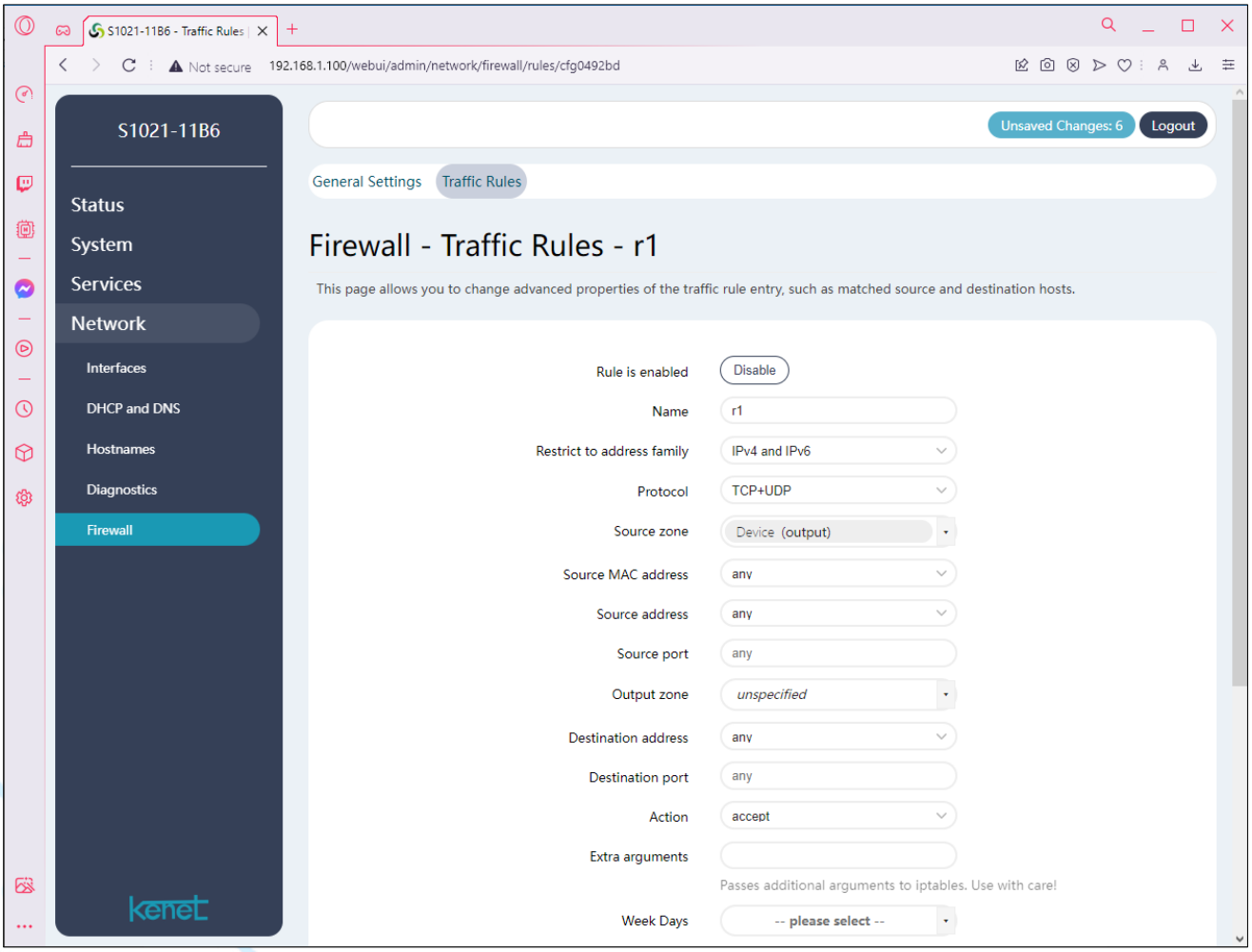
- در این بخش پورت های باز شده روی دستگاه (فایروال اجازه دسترسی داده) قابل پیکربندی است.
- این بخش از فیلد های زیر تشکیل شده است:
  - Name : نام
  - Protocol : پروتکل
  - External port : پورت خارجی
- برای اضافه کردن ، کافی است اطلاعات خواسته شده را درج و گزینه add را انتخاب کنید.



- در قسمت پروتکل ، موارد زیر قابل انتخاب هستند:



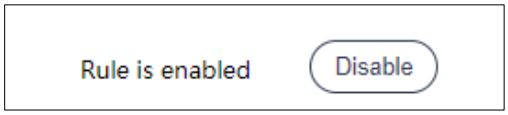
- در صورت پر کردن فیلد های خواسته شده و انتخاب بر روی گزینه add صفحه زیر برای شما نمایش داده خواهد شد.



۱-۲-۳-۶-۶ بخش add

- در این قسمت به انجام تنظیمات rule ای که قصد اضافه کردن ان را دارید می پردازید.
- موارد زیر قابل ویرایش و تنظیم هستند:
  - Rule is enabled

فعال کردن Rule تعریف شده

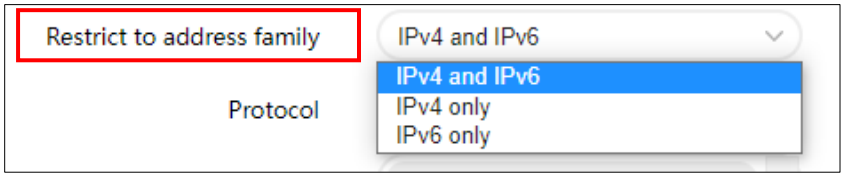


  - Name

نام

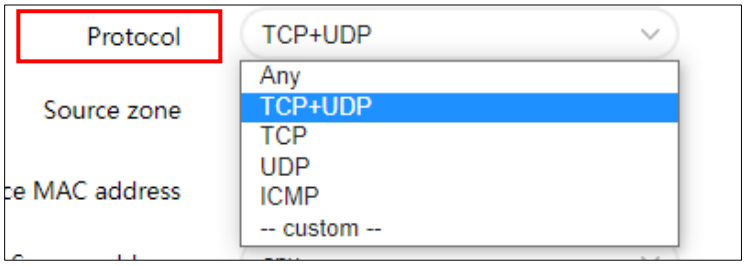
  - Restrict to address family

محدود کردن نوع ادرس دهی ip



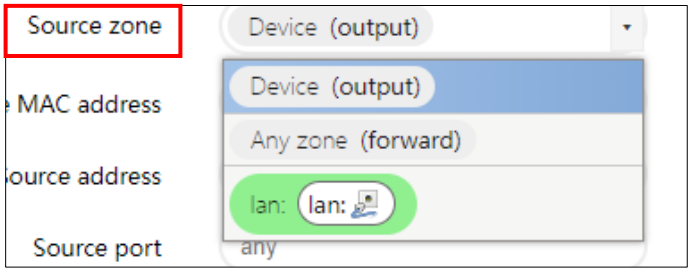
  - Protocol

پروتکل



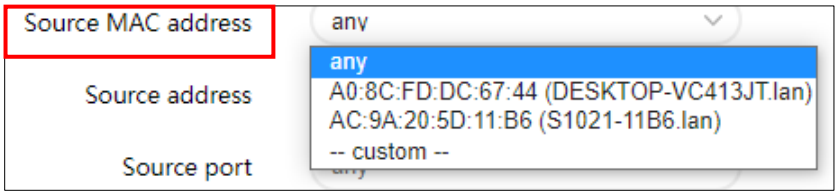
  - Source zone

ناحیه مبدا



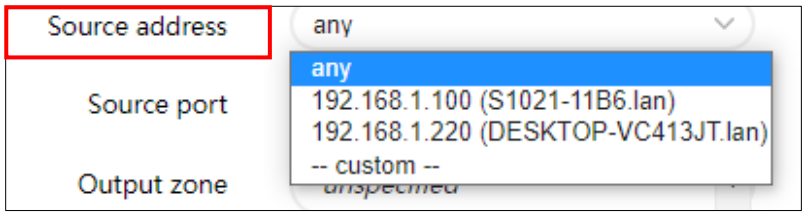
Source MAC address -

ادرس mac مبدا



Source address -

ادرس مبدا

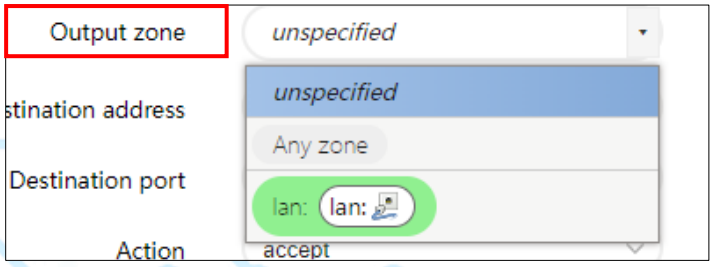


Source port -

ناحیه داخلی

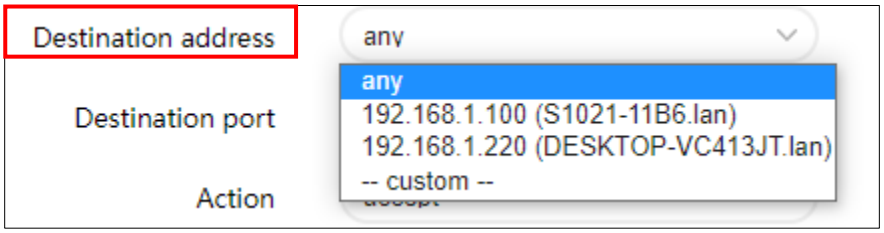
Output zone -

ناحیه خارجی



Destination address -

ادرس مقصد

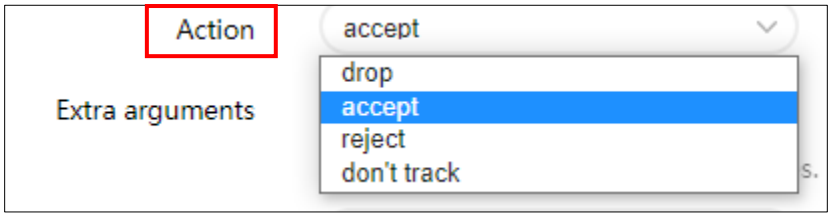


- Destination port

پورت مقصد

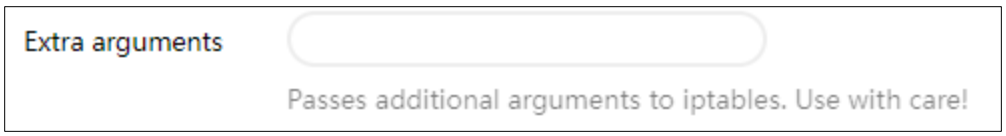
- Action

عملیات



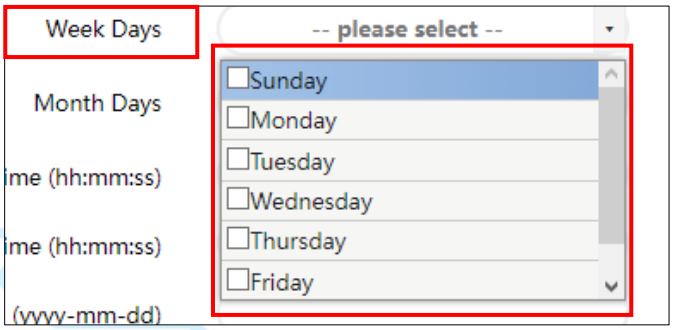
- Extra arguments

ارسال پارامتر های اضافه به ip tables



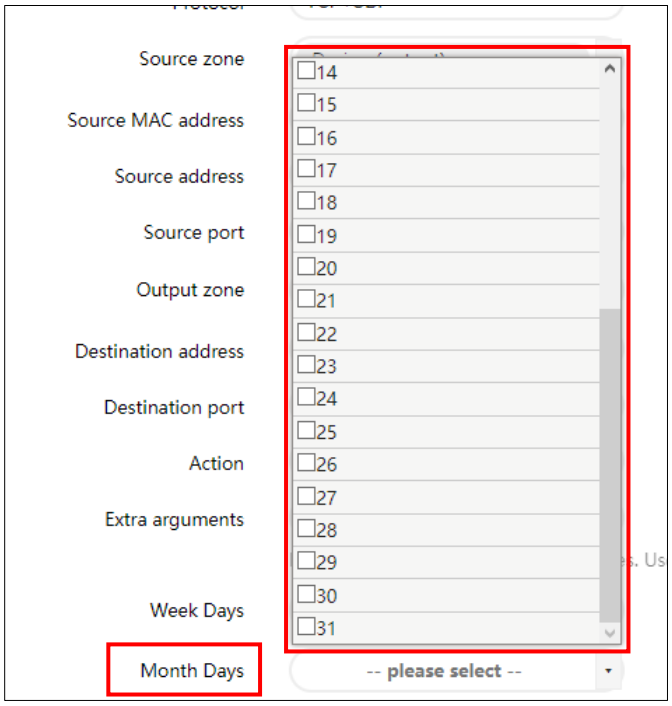
- Week Days

روز های هفته



- Month Days

روز های ماه



- Start Time (hh:mm:ss)

زمان شروع

- Stop Time (hh:mm:ss)

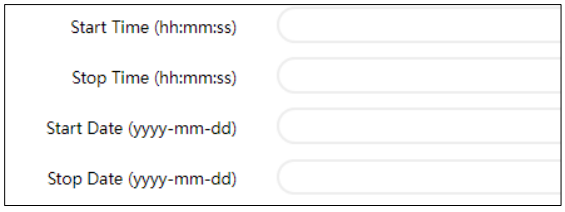
زمان توقف

- Start Date (yyyy-mm-dd)

تاریخ شروع

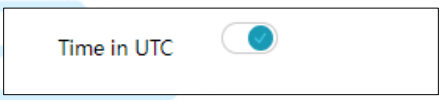
- Stop Date (yyyy-mm-dd)

تاریخ توقف

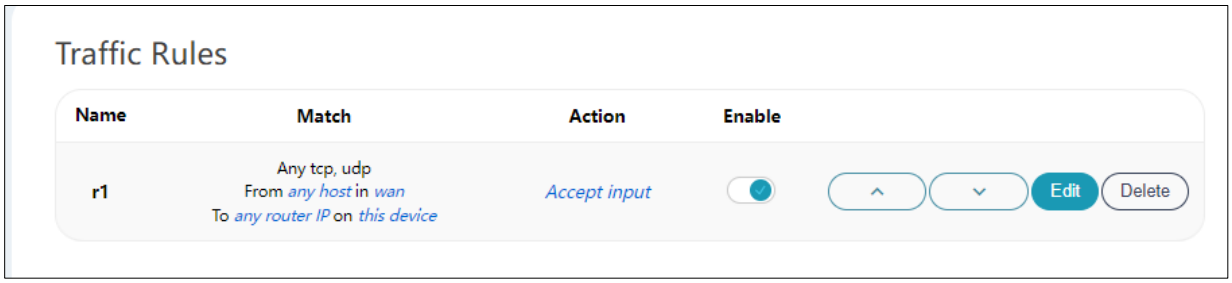


- Time in UTC

زمان بر حسب utc

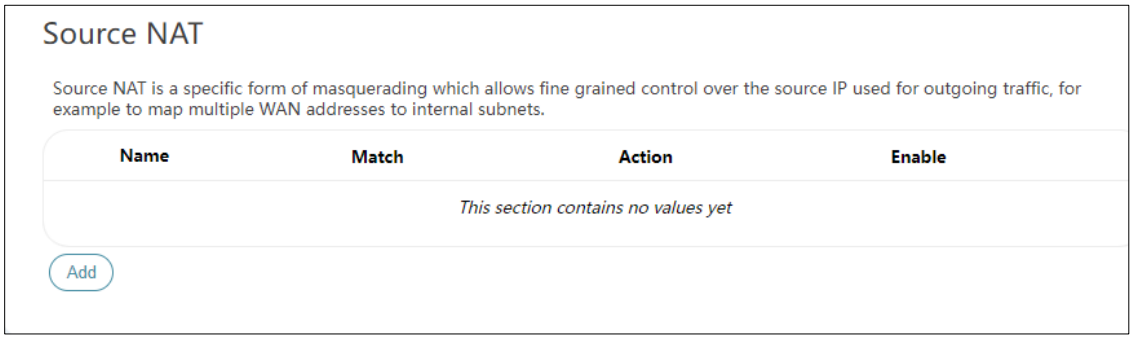


- پس از اعمال تنظیمات ، در بخش traffic rules قابل نمایش هست.



۳-۳-۶-۶ بخش Source NAT

- در این بخش تنظیمات Source NAT قابل پیکر بندی است.
- این بخش از فیلد های زیر تشکیل شده است:
  - Name : نام
  - Match : تطبیق
  - Action : عمل
  - Enable : فعال / غیرفعال



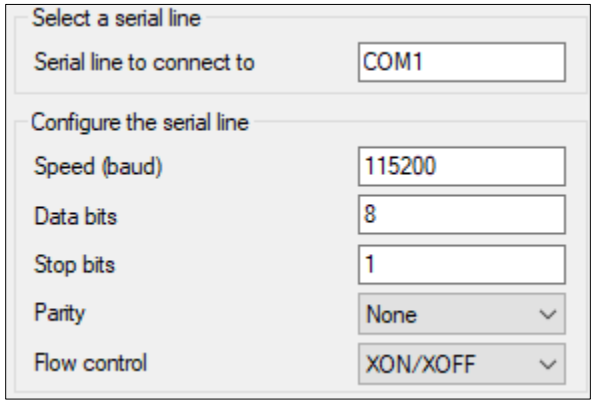
۷- نرم افزار ها و فایل های مورد نیاز

۷-۱ نرم افزار های ارتباط با کنسول

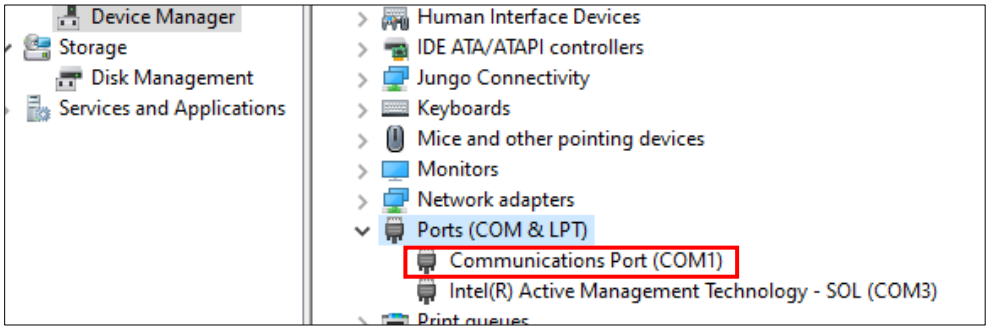
- جهت کار با کنسول مبدل شما احتیاج به یکی از نرم افزار های زیر خواهید داشت:
  - Puty
  - Termit
  - Hercules
  - Realterm
- شما می توانید هر یک از نرم افزار های فوق را از سایت سازنده دریافت نمایید.

۷-۲ نحوه ایجاد ارتباط کنسول با مبدل

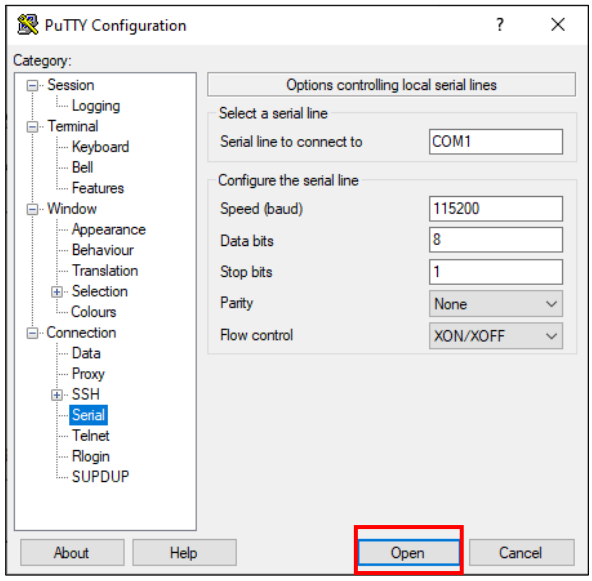
- از نصب بودن درایور های خود اطمینال حاصل فرمایید.
- ابتدا باید کابل کنسول مبدل که به همراه مبدل است را به درگاه کنسول مبدل متصل نمایید.
- سپس یکی از نرم افزار های معرفی شده را باز نمایید.
- اطلاعات زیر را در نرم افزار خود تنظیم نمایید.



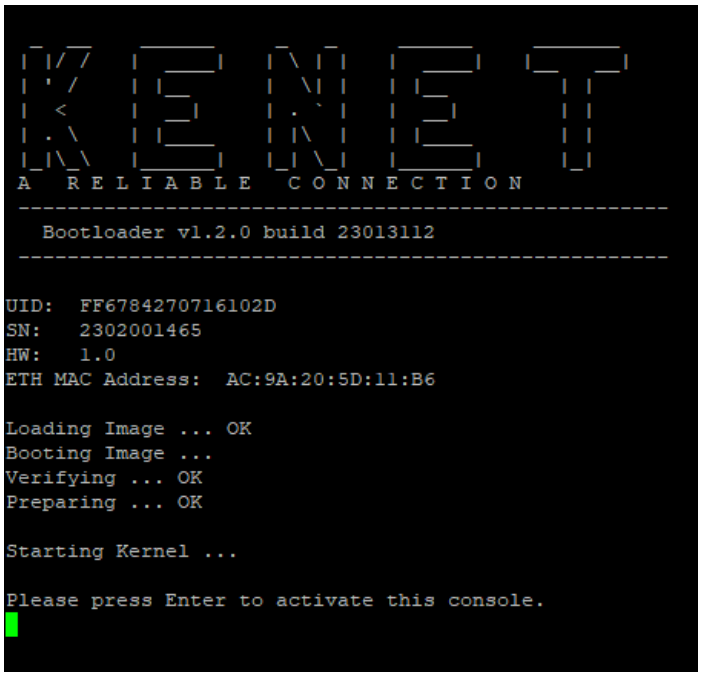
- دقت نمایید که پورت com خود را به درستی انتخاب کرده باشید؛ برای اطمینال از قسمت device manager کامپیوتر خود بخش ports را باز کرده و از عدد پورت com خود اطمینال حاصل فرمایید.



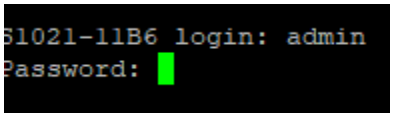
- پس از تنظیم کردن مقادیر ذکر شده ، صفحه ترمینال نرم افزار خود را باز کنید.



- پس از باز کردن ترمینال com ، صفحه سیاه رنگی برای شما نمایش داده می شود.
- برق مبدل خود را در این مرحله وصل کنید.
- پس از اتصال برق مبدل ، صفحه زیر برای شما نمایش داده خواهد شد.



- مشاهده می کنید که اطلاعات زیر برای شما نمایش داده خواهد شد:
  - Boot loader : نسخه بوت لودر مبدل
  - Uid : uid مبدل
  - Sn : سریال یکتا مبدل
  - Hw : نسخه سخت افزار مبدل
  - Eth mac : ادرس mac پورت lan
- سپس شما با زدن کلید enter به مرحله بعد خواهی رفت.
- در این مرحله شما باید نام کاربری و رمز عبور اینترفیس مبدل را وارد نمایید.
  - نام کاربری : admin
  - رمز عبور : kenet
- دقت کنید که این محیط به حروف کوچک و بزرگ حساس است.

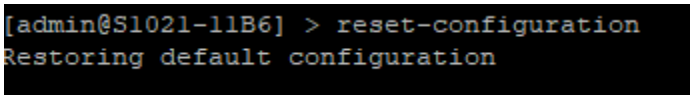


- پس از وارد کردن کردن مقادیر گفته شده ، کافی است کلید enter را بزنید.
- در نهایت محیط کنسول مبدل برای شما باز شده و اماده اجرای فرامین شماست.

۳-۷ نحوه بازیابی به تنظیمات کارخانه از طریق کنسول

- پس از اماده سازی موارد گفته شده در بخش قبلی ، دستور زیر را جهت بازگردانی به تنظیمات کارخانه وارد کنید.

- reset-configuration



- در صورت درست وارد کردن دستور بالا ، پیامی را به شما نشان خواهد داد و دستور اجرا خواهد شد.

۸- پشتیبانی و گارانتی

۸-۱-۱ پشتیبانی فنی محصول

- جهت دریافت پشتیبانی پیرامون مسائل فنی با شماره تماس زیر در ارتباط باشید.

۰۳۱-۳۳۹۳۱۲۲۲

- هم چنین شما می توانید در خواست های خود را به ایمیل زیر ارسال کنید.

support@teyfpardazan.ir

- لاز ب ذک اس فای ب پسوند img. را از پشتیبان فنی می توانید دریافت کنید.

۸-۱-۲ پشتیبانی خدمات پس از فروش

- جهت دریافت پشتیبانی پیرامون خدمات پس از فروش با شماره های زیر تماس حاصل فرمایید.

۰۳۱-۳۳۹۳۱۲۲۰

۰۹۳۰۰۳۶۴۲۲۹

- شما می توانید در خواست های خود را در پیام رسان های واتساپ ، ایتا و بله ارسال کنید.
- هم چنین شما می توانید در خواست های خود را به ایمیل زیر ارسال کنید.

info@teyfpardazan.ir

- خدمات پس از فروش ، در صورت عدم شرایط گارانتی با دریافت هزینه صورت می پذیرد.

۸-۱-۳ پشتیبانی خدمات بازرگانی

- جهت دریافت پشتیبانی پیرامون خدمات خرید با شماره های زیر تماس حاصل فرمایید.

۰۳۱-۳۳۹۳۱۲۲۰

۰۹۳۰۰۳۶۴۲۲۹

- شما می توانید در خواست های خود را در پیام رسان های واتساپ ، ایتا و بله ارسال کنید.

- هم چنین شما می توانید در خواست های خود را به ایمیل زیر ارسال کنید.

info@teyfpardazan.ir

۸-۱-۴ پشتیبانی مالی

- جهت دریافت پشتیبانی پیرامون خدمات مالی با شماره زیر تماس حاصل فرمایید.

۰۳۱-۳۳۹۳۱۲۲۱

- هم چنین شما می توانید در خواست های خود را به ایمیل زیر ارسال کنید.

tps-co@istt.ir

۸-۲ گارانتی محصول

۸-۲-۱ شرایط گارانتی

- جهت بهره مندی از گارانتی باید کارت گارانتی را نزد خود نگه داری کنید و جهت استفاده از خدمات گارانتی آن را به همراه محصول ، پس از هماهنگی با پشتیبانی خدمات پس از فروش، ارائه دهید.
- مدت زمان گارانتی محصول روی کارت محصول درج شده است.
- مواردی که باعث ابطال گارانتی خواهد شد:
  - آب خوردگی دستگاه
  - تماس یا نفوذ مواد شیمیایی
  - اتصال نامناسب به پورت های دستگاه
  - فرورفتگی یا آسیب ظاهری پورت ها
  - ضربه یا صدمه فیزیکی و نداشتن س لمت ظاهری
  - مخدوش یا کنده شدن بر چسب پلمپ روی دستگاه

۲-۲-۸ کارت گارانتی

- به همراه محصول یک کارت گارانتی در اختیار کاربر قرار خواهد گرفت .

- در پشت کارت گارانتی موارد زیر درج شده است :
  - سریال یکتا محصولت
  - مدل محصول
  - نام خریدار
  - تاریخ شروع گارانتی
  - تاریخ پایان گارانتی

۳-۲-۸ نحوه بهره مندی از شرایط گارانتی

- اطمینان حاصل کردن از شامل شدن شرایط گارانتی
- اطمینان حاصل کردن از معتبر بودن تاریخ گارانتی
- تماس با پشتیبانی خدمات پس از فروش
- هماهنگی برای ارسال دستگاه ها
- پیگیری مراحل و روند استفاده از خدمات گارانتی

برای خرید محصول از طریق لینک زیر اقدام نمایید:

https://istatajhiz.ir/product/convertor-rs485/