

راهنمای کاربر نهایی

مدل های سری S1021



شرکت طیف پردازان اسپادانا

ویرایش ۱,۰,۲۳

فهرست موضوعی مطالب

بخش اول	الزامات راه اندازی مبدل S1021
بخش دوم	پنجره ی پیکر بندی تنظیمات مبدل
بخش سوم	معرفی بخش Status
بخش چهارم	معرفی بخش System
بخش پنجم	معرفی بخش Services
بخش ششم	معرفی بخش Network
بخش هفتم	نرم افزار ها و فایل های مورد نیاز
بخش هشتم	پشتیبانی و شرایط گارانتی

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.

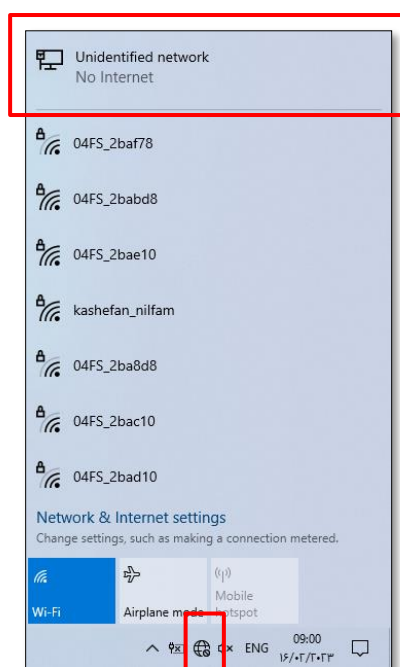


۲- پنجره ی پیکر بندی تنظیمات مبدل

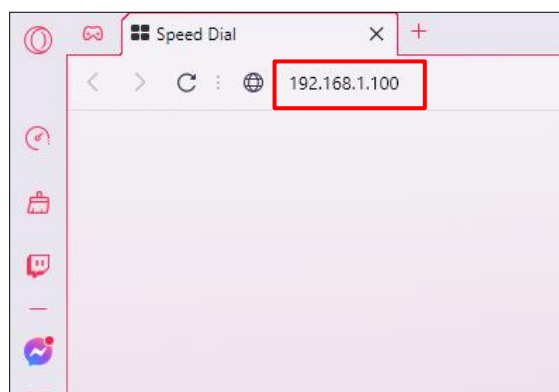
در این بخش به معرفی پنجره پیکربندی مبدل پرداخته می شود.

۲-۱ ورود به پنجره تنظیمات پیکربندی :

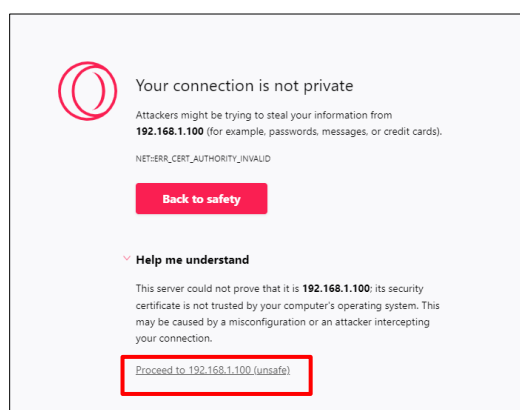
- می بایست الزامات گفته شده در فصل گذشته را فراهم کنید.
- از اتصال صحیح کابل برق اطمینال حاصل کنید.
- از اتصال کابل LAN بین کامپیوتر و مبدل اطمینال حاصل کنید.
- اگر به وای فای دیگری متصل هستید ، از آن شبکه خارج شوید.



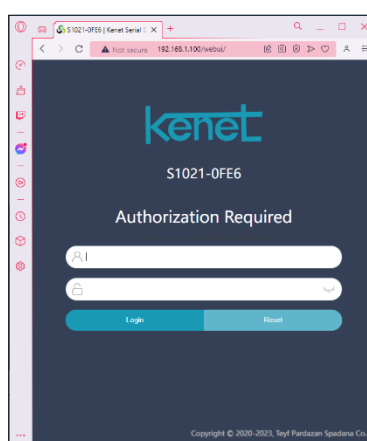
- ممکن است پس از اتصال به مودم، آیکن بخش اینترنت ویندوز شما عدم وجود اینترنت را نشان دهد.
- مطمئن شوید که کارت شبکه سیستم شما، مبدل را شناخته باشد.
- سپس مرورگر خور را باز کرده و در نوار آدرس مرورگر خود، **IP Default Gateway** مبدل را وارد کنید(۱۹۲.۱۶۸.۱.۱۰۰).



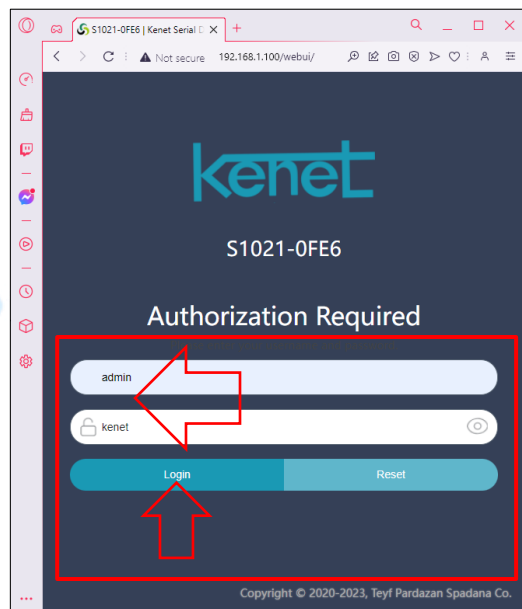
- ممکن است مرورگر، هشدار غیرایمن بودن صفحه را به شما بدهد؛ در این صورت شما، ادامه به صورت غیر ایمن را انتخاب کنید.



- 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.

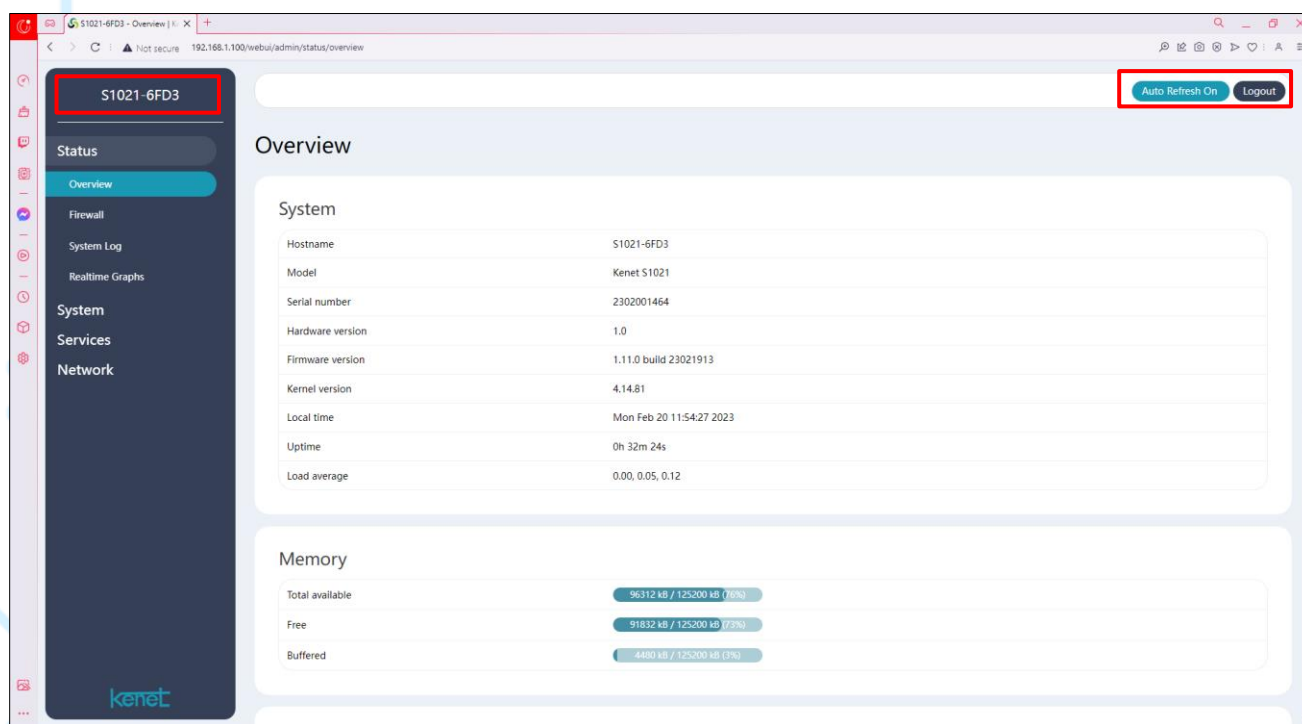
۲-۲-۳ بخش SERVICES

- کلیه سرویس هایی که این مبدل ارائه می دهد ، در این بخش قرار دارد.
- تنظیمات پیرامون پورت های RS232 و RS485 ، سرویس ها ، SNMP و VPN در این قسمت قرار دارد.

۲-۲-۴ بخش NETWORK

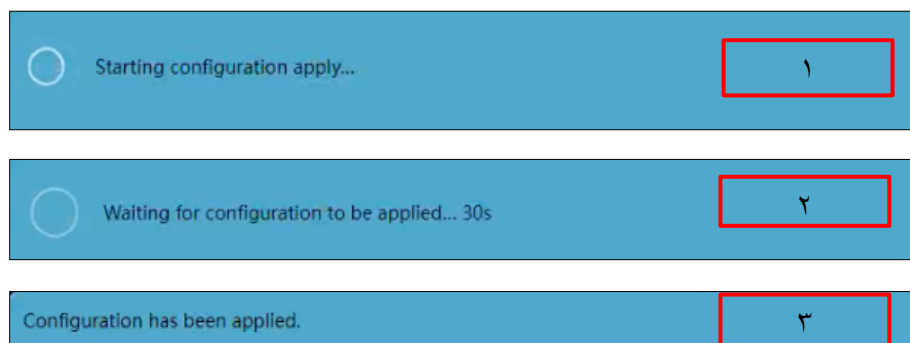
- تنظیمات پیرامون شبکه در این قسمت قرار دارد.
- تنظیماتی از جمله عوض کردن IP پیشفرض ، تعریف مد کاری مبدل ، IP های اختصاص داده شده توسط مبدل ، مسیر های تعریف شده توسط LAN ، PORT FORWARDS در این بخش قرار دارد.

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 در صورت 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.

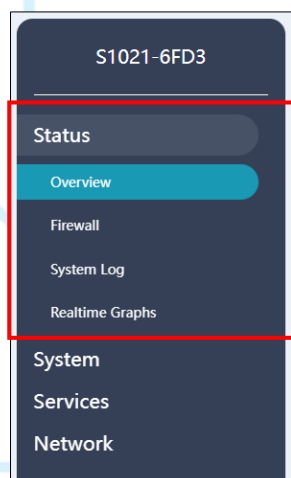
۱-۳ قسمت های بخش STATUS

- قسمت Overview

- قسمت Firewall

- قسمت System Log

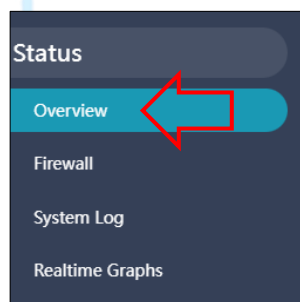
- قسمت Realtime Graphs



Overview قسمت ۳-۲

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:

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

System	
Hostname	S1021-0FE6
Model	Kenet S1021
Serial number	2302001463
Hardware version	1.0
Firmware version	1.10.0 build 23020529
Kernel version	4.14.81
Local time	Tue Feb 14 17:14:00 2023
Uptime	0h 25m 11s
Load average	0.00, 0.00, 0.00

۳-۲-۳ زیر بخش Memory

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

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

Memory	
Total available	96652 kB / 125200 kB (77%)
Free	92184 kB / 125200 kB (73%)
Buffered	4468 kB / 125200 kB (3%)

۳-۲-۴ زیر بخش Network

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

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

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

Network

IPv4 Upstream

Protocol: **Static address**
 Address: 192.168.1.100
 Netmask: 255.255.255.0
 Gateway: 192.168.1.1
 DNS 1: 192.168.1.1
 Connected: 0h 37m 41s

Device: Ethernet Adapter: "eth0"
 MAC address: AC:9A:20:5D:0F:E6

IPv6 Upstream

Protocol: *Not connected*
 Address: ::
 Gateway: ::

Device: -

Active Connections 93 / 16384 (0%)

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 : آدرس IP ویرایش ۴ دستگاه متصل
- MAC-Address : آدرس MAC دستگاه متصل
- Leasetime remaining : زمان باقی مانده از اختصاص ip

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
DESKTOP-VC413JT	192.168.1.220	A0:8C:FD:DC:67:44	11h 13m 58s

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 : آدرس 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	000100012a697b1fa08cfdcc6744	11h 15m 30s

۳-۳ قسمت Firewall

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).

The screenshot shows the 'Firewall Status' page in the Kenet management interface. The page is divided into several sections:

- Navigation:** A sidebar on the left contains 'Status', 'Overview', 'Firewall' (highlighted with a red arrow), 'System Log', 'Realtime Graphs', 'System', 'Services', and 'Network'.
- Firewall Status:** The main content area is titled 'Firewall Status' and has two tabs: 'IPv4 Firewall' (selected) and 'IPv6 Firewall'. A red box highlights these tabs.
- Table: Filter:** A table showing the configuration for the 'Chain INPUT' policy. The table has columns for 'Pkts.', 'Traffic', 'Target', 'Prot.', 'In', 'Out', 'Source', 'Destination', and 'Options'. The 'Chain INPUT' table shows several rules, including 'input_rule', 'syn_flood', and 'zone_lan_input'. A red box highlights the 'Reset Counters' and 'Restart Firewall' buttons in the top right corner of the table area.
- Chain FORWARD:** A table showing the configuration for the 'Chain FORWARD' policy.
- Chain OUTPUT:** A table showing the configuration for the 'Chain OUTPUT' policy.

۳-۳-۲ اجزای بخش IPV4 FIREWALL

- از ۴ جدول برای نمایش دیتا ها استفاده می کند:
- **Filter** : جدول پیش فرض 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 Filter جدول

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

NAT جدول ۳-۳-۲-۲

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)

Pkt s.	Traffic	Target	Pro t.	In	Out	Source	Destinatio n	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)

Pkt s.	Traffic	Target	Pro t.	In	Out	Source	Destinatio n	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)

Pkt s.	Traffic	Target	Pro t.	In	Out	Source	Destinatio n	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 Raw و Mangle :

این جدول ها هم مشابه جدول های قبلی، در صورت 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:

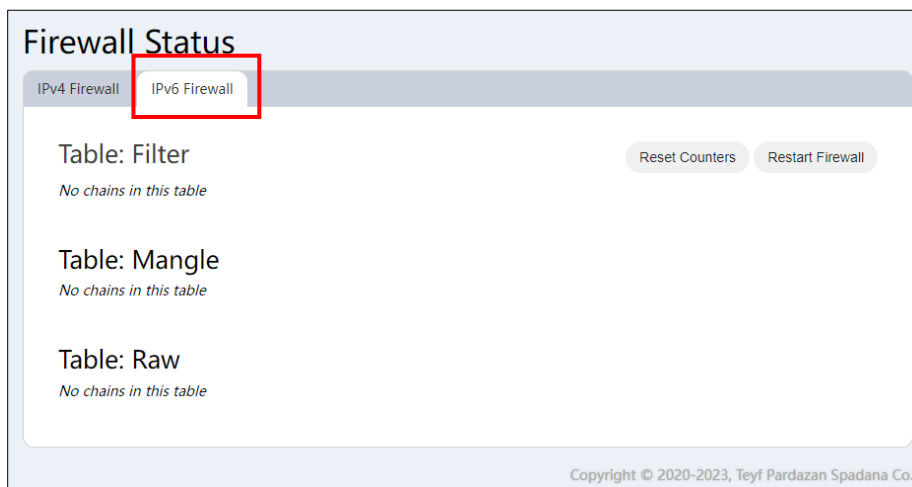
- **Filter** : جدول پیش فرض مورد استفاده **iptables** است که برای فیلتر کردن پکت

های ورودی و خروجی مورد استفاده قرار میگیرد.

- **Mangle** : از طریق این جدول میتوان تغییراتی را در **header** پکت ها ایجاد نمود.

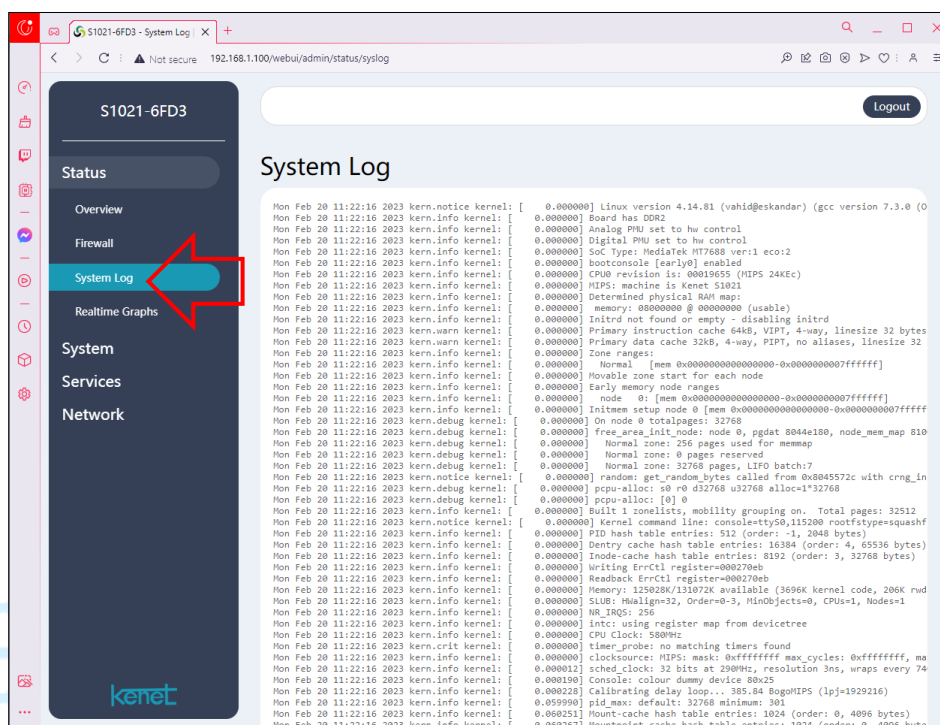
- Raw : این جدول این امکان را فراهم میکند تا با پکت ها قبل از این که کرنل بر اساس state آنها اقدامی انجام دهد کارکرد.

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



۳-۴ قسمت System Log

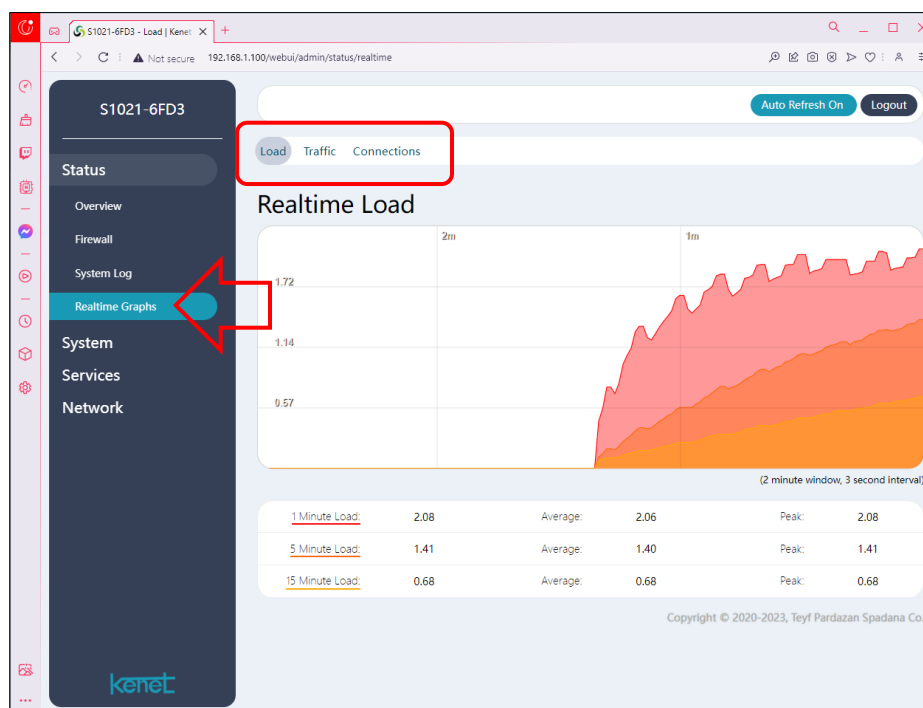
- تاریخچه فعالیت های اتفاق افتاده در مبدل را نمایش می دهد.



۳-۵ قسمت Realtme Graphs

۳-۵-۱ معرفی Realtme Graphs

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



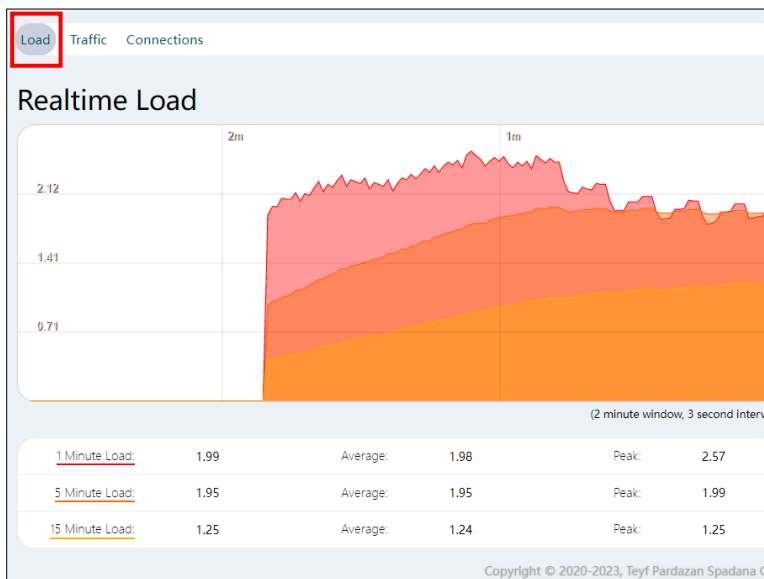
۳-۵-۲ اجزای قسمت Realtme Graphs

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

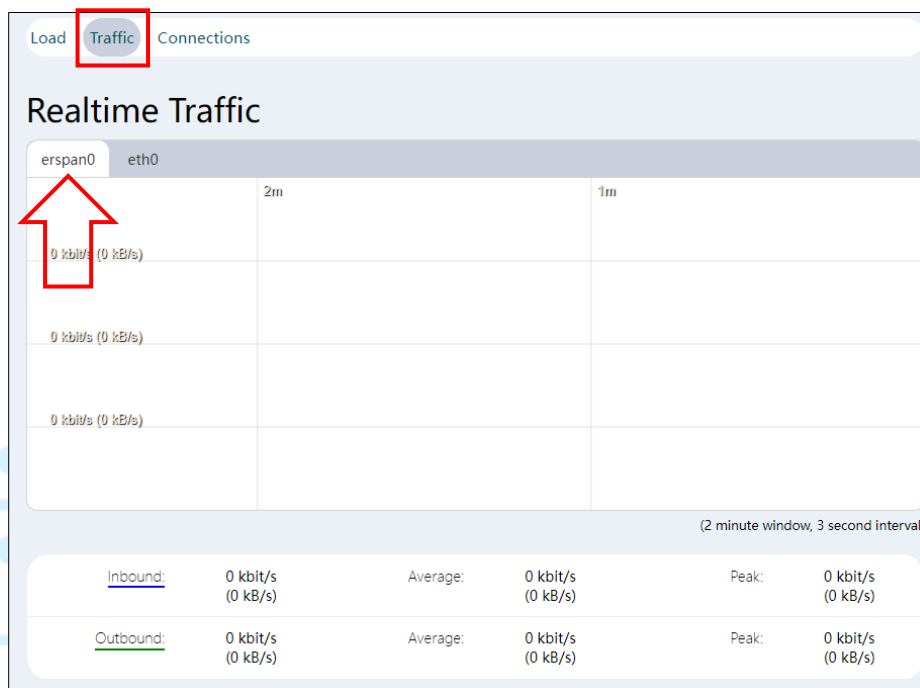
۳-۵-۳ نمودار Load

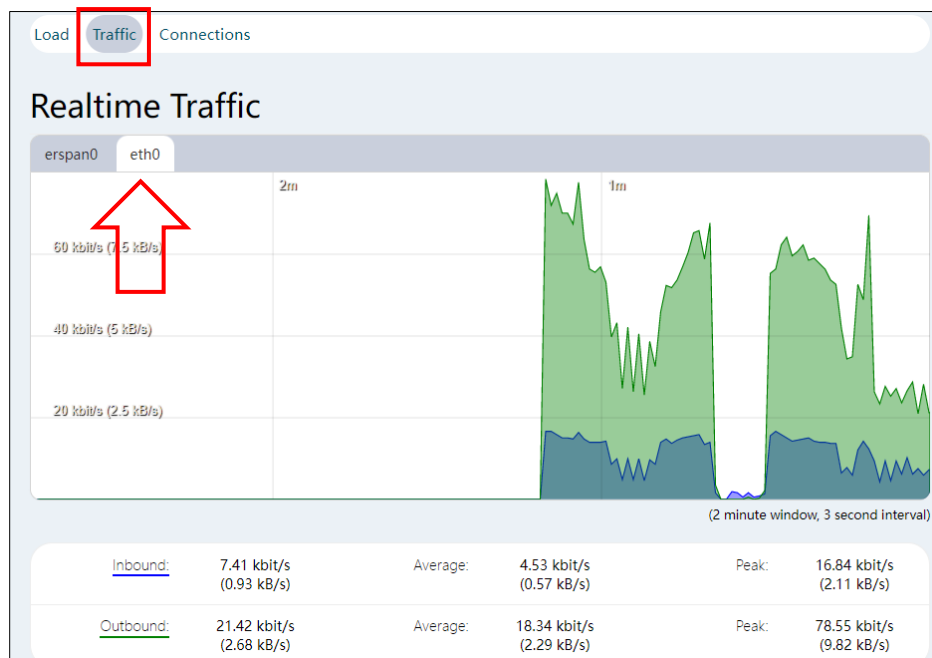
- نمودار مقدار بارگزاری مبدل فاصله ۲ دقیقه ای اخیر



۳-۵-۴ نمودار Traffic

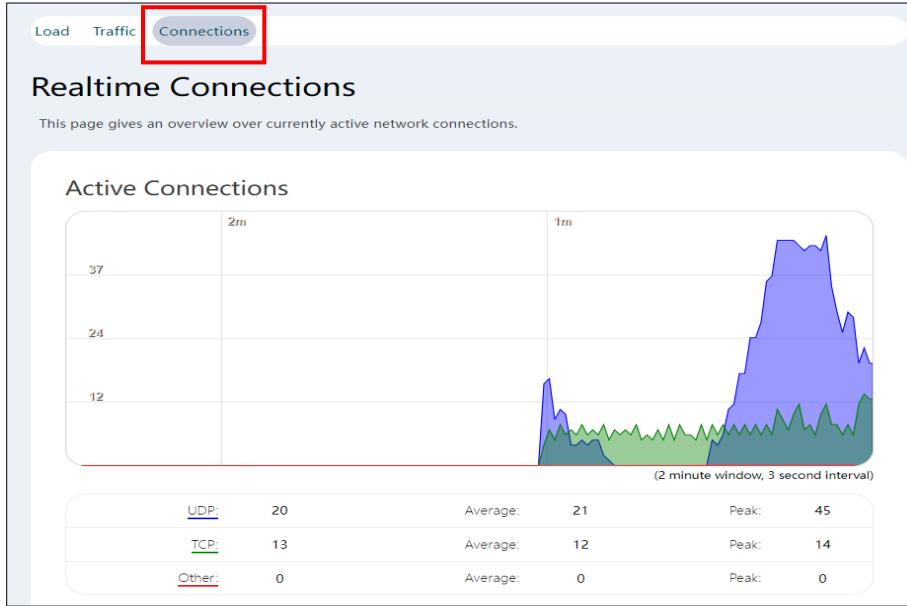
- نمودار میزان ترافیک لحظه ای مبدل در فاصله ۲ دقیقه اخیر
- به ۲ صورت eth0 و erspan0 قابل مشاهده است.





۳-۵-۵ نمودار Connection

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



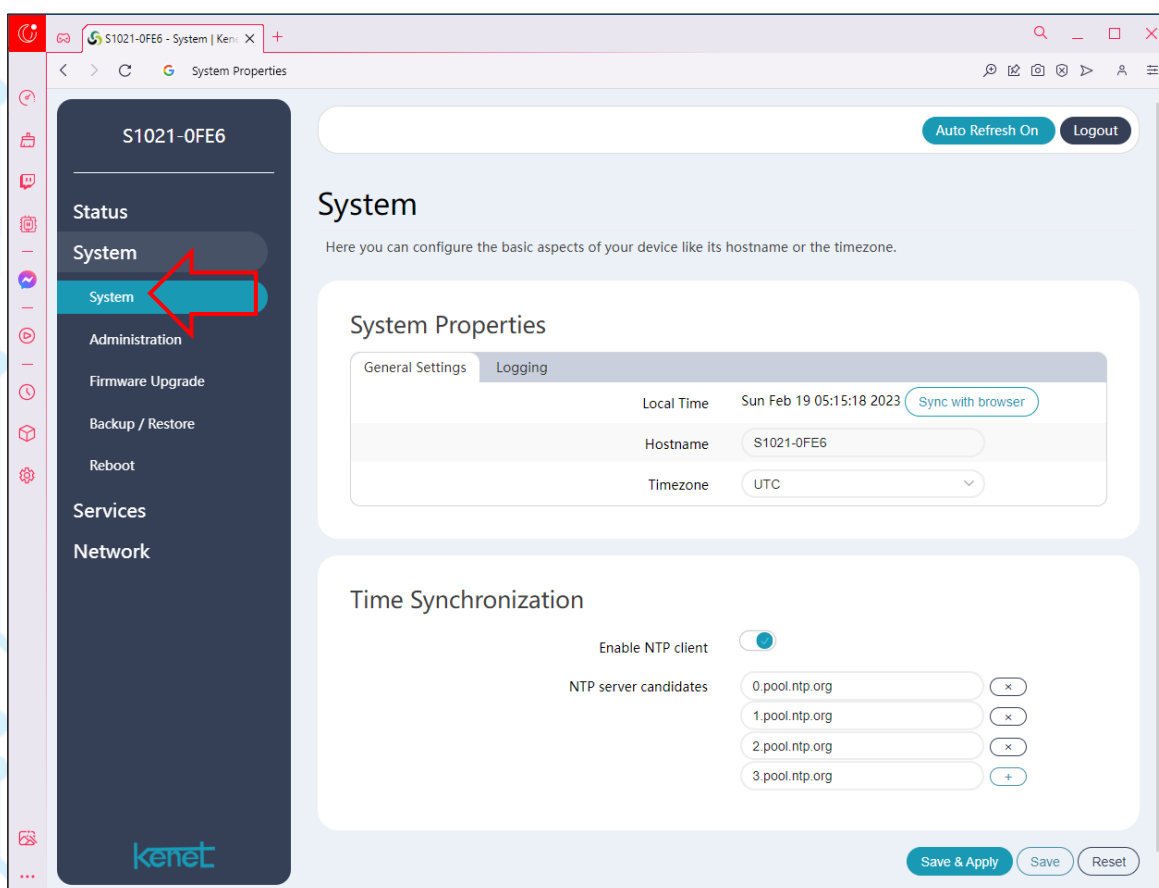
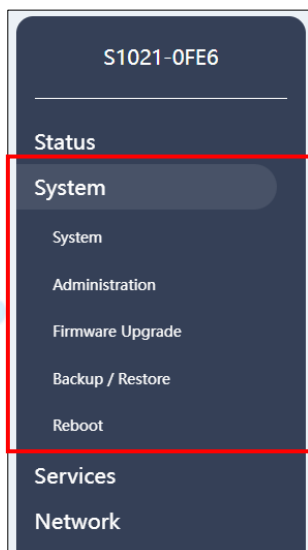
Network	Protocol	Source	Destination	Transfer
IPV4	TCP	DESKTOP-VC413JT.lan:4915	S1021-0FE6.lan:443	14.78 KB (32 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4919	S1021-0FE6.lan:443	13.31 KB (31 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4917	S1021-0FE6.lan:443	4.02 KB (19 Pkts.)
IPV4	TCP	DESKTOP-VC413JT.lan:4925	S1021-0FE6.lan:443	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 Administration
- قسمت Firmware 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.

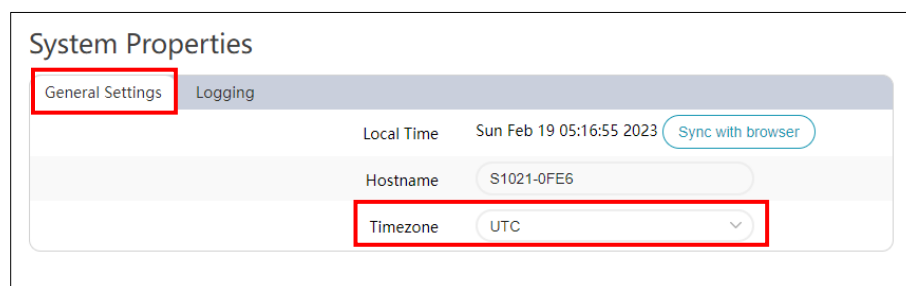
- System Properties : ویژگی های سیستم
- Time Synchronization : همگام سازی زمانی

۴-۲-۲ زیر بخش System Properties

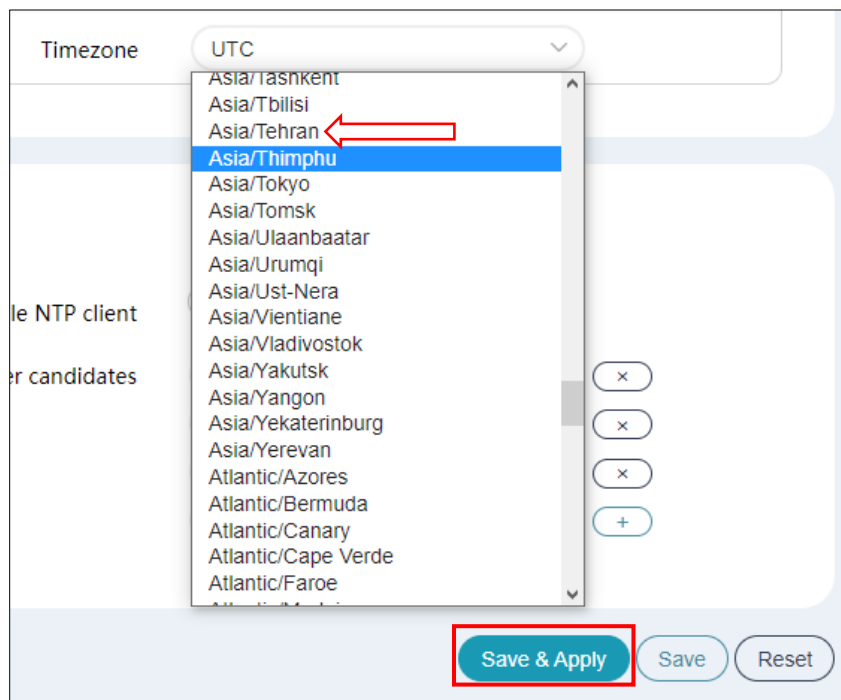
- این بخش از ۲ قسمت زیر تشکیل شده است.
- General Settings : تنظیمات کلی
- Logging : گزارشات سیستم

۴-۲-۲-۱ General Settings بخش

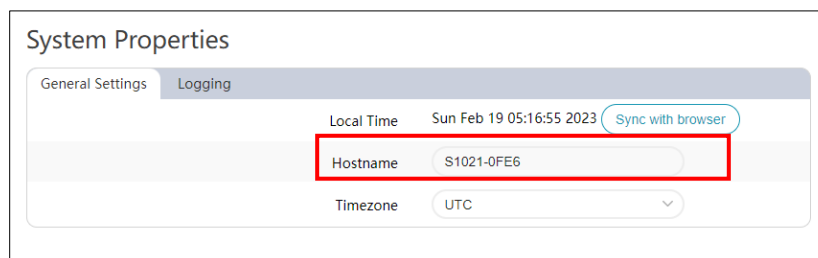
- از فیلد های زیر تشکیل شده است:
- Local Time : زمان محلی
- Hostname : نام مبدل (قابل تغییر)
- Timezone : منطقه زمانی (قابل تنظیم)



- می توانید منطقه زمانی خود را، با باز کردن 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.

۴-۲-۲-۲ بخش Logging

- از فیلدهای 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

System Properties

General Settings **Logging**

System log buffer size kiB

External system log server

External system log server port

External system log server protocol

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

External system log server protocol

Time Synchronization ۴-۲-۳ زیر بخش

- 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

Time Synchronization

Enable NTP client

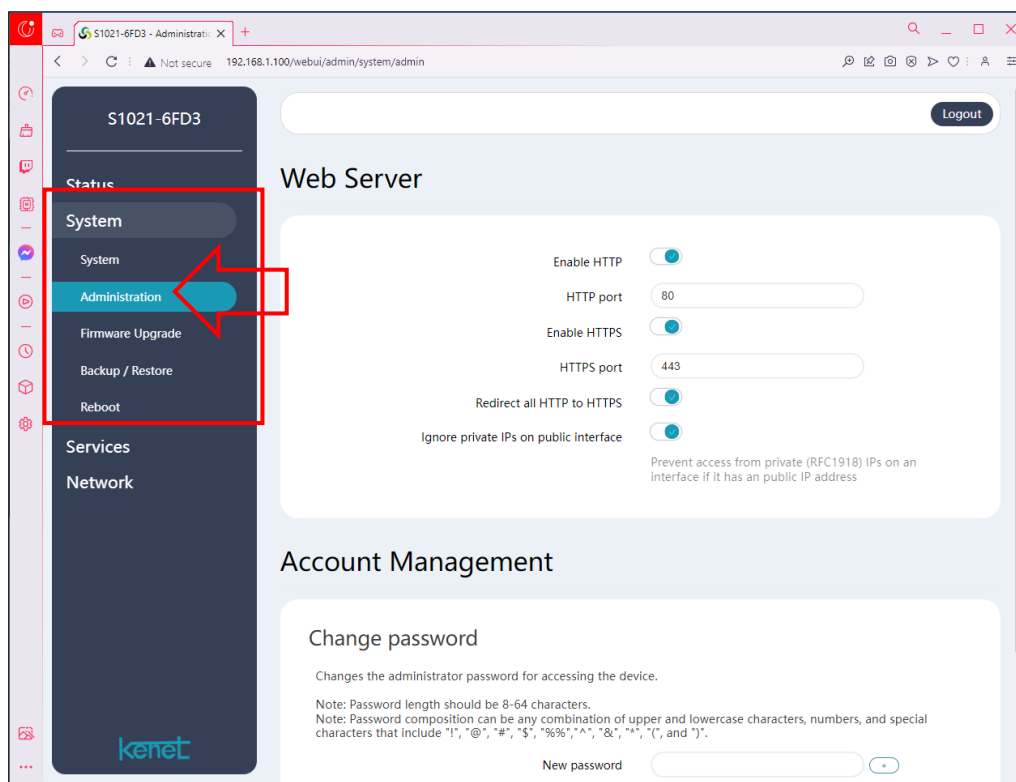
- در صورت فعال کردن این بخش ، فیلد های زیر برای شما نمایش داده می شود.

Time Synchronization

Enable NTP client

NTP server candidates

Adminstration قسمت ۴-۳

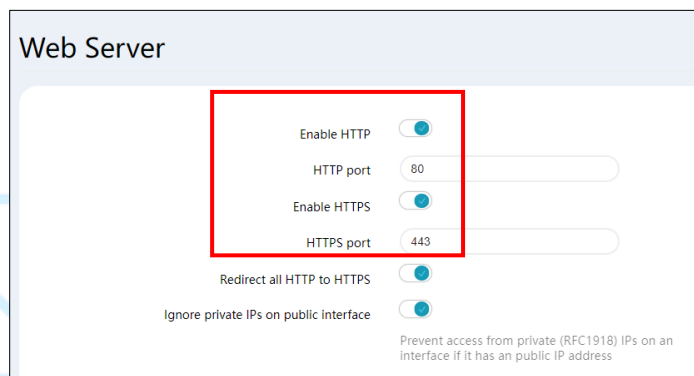


Adminstration معرفی ۴-۳-۱

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

Web Server بخش ۴-۳-۲

- 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 ۴-۳-۳).
- هم چنین می توانید فعال بودن یا نبودن ERROR RFC 1918 را مدیریت کنید.

Web Server

Enable HTTP

HTTP port 80

Enable HTTPS

HTTPS port 443

Redirect all HTTP to HTTPS

Ignore private IPs on public interface

Prevent access from private (RFC1918) IPs on an interface if it has a public IP address

بخش ۴-۳-۳ Account Management

Account Management

Change password

Changes the administrator password for accessing the device.

Note: Password length should be 8-64 characters.
Note: Password composition can be any combination of upper and lowercase characters, numbers, and special characters that include "!", "@", "#", "\$", "%", "^", "&", "*", "(", and ")".

New password

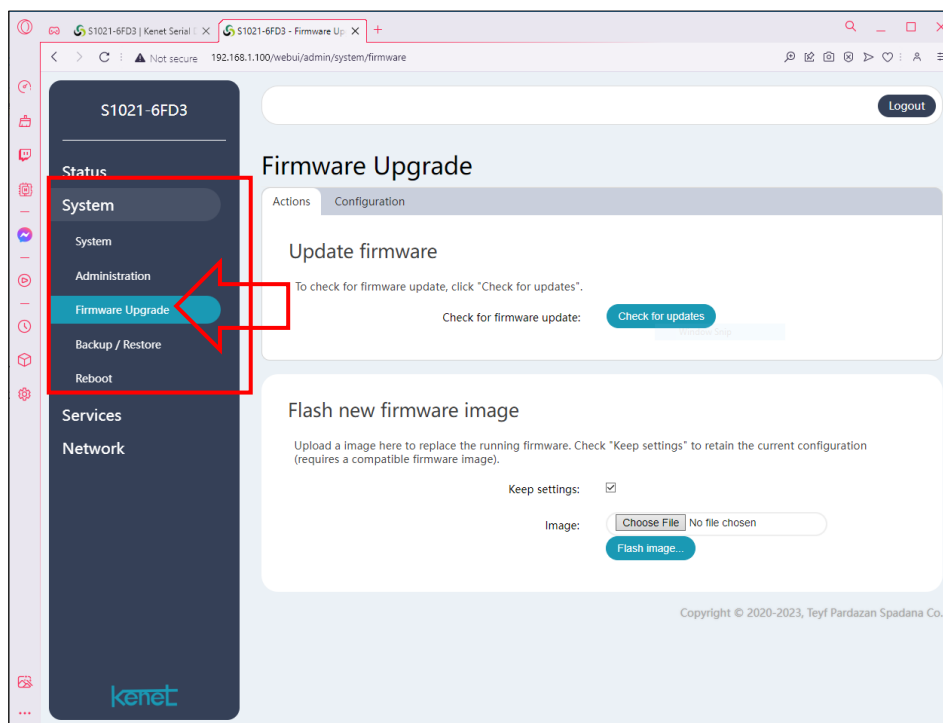
Confirmation

Save & Apply Save Reset

- در این بخش می توان پسورد خود را تغییر دهید.
- پس از وارد کردن پسورد جدید ، یکبار دیگر آن 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 :

- "(", ")", "*", "&", "^", ":", "\$", "#", "@", "!",

Firmware Upgrade قسمت ۴-۴



۴-۴-۱ معرفی Fireware Upgrade

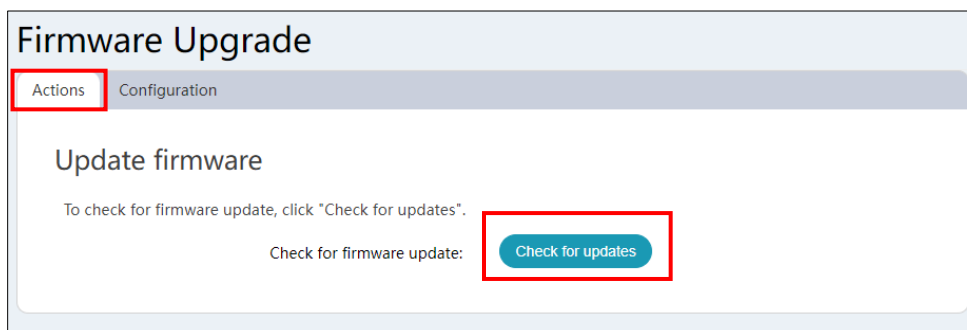
- با کمک این بخش می توانید برنامه مبدل را به روز رسانی نمایید.
- این بخش از ۲ قسمت زیر تشکیل شده است :
 - Actions : بررسی به روز رسانی
 - Configuration : تنظیمات به روز رسانی

۴-۴-۲ بخش Actions

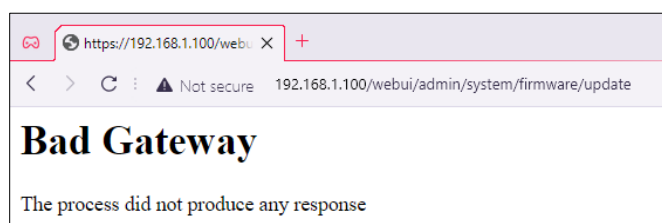
- این بخش از ۲ زیر بخش زیر تشکیل شده است :
 - Update firmware : بررسی به روزرسانی موجود
 - Flash new firmware image : بروزرسانی توسط فایل با پسوند .img

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.

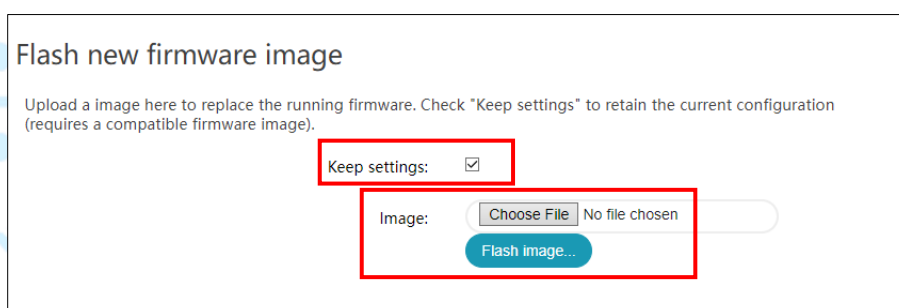


- در صورت عدم دسترسی مبدل به اینترنت صفحه زیر به شما نشان داده خواهد شد.



۴-۴-۲-۲ 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 آخرین 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 .



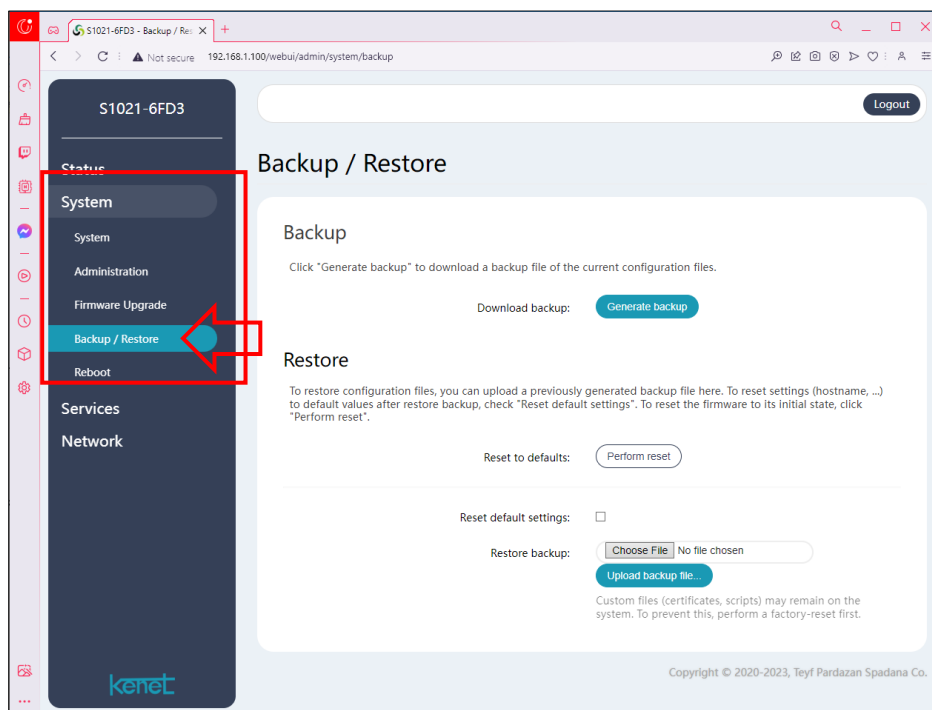
۴-۴-۳ بخش Configuration

- 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 آن 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.

Backup / Restor قسمت ۴-۵

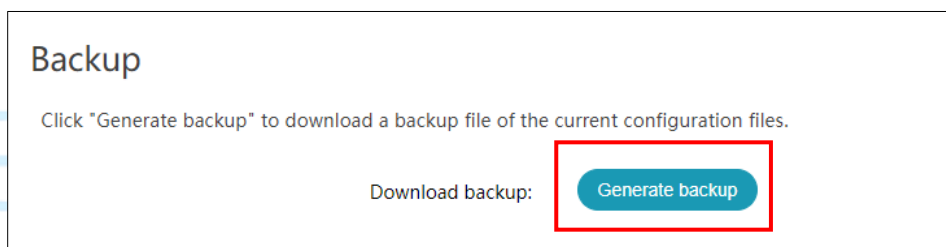


Backup / Restor معرفی ۴-۵-۱

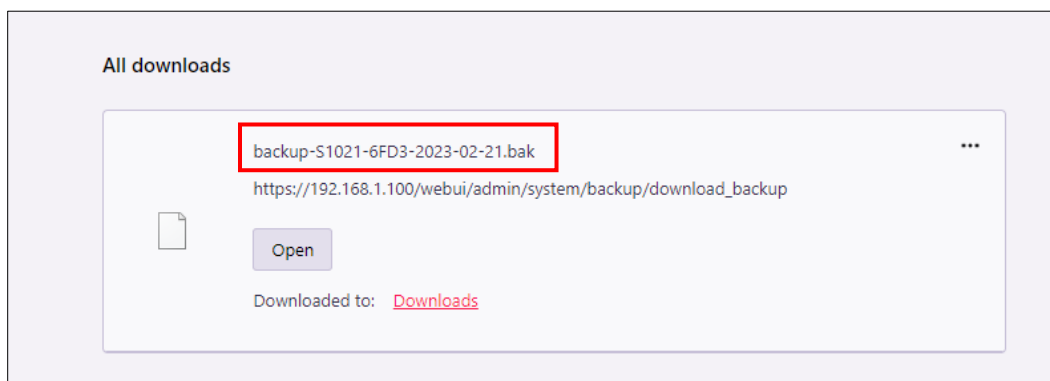
- با کمک این بخش می توانید از تنظیمات نسخه پشتیبان تهیه نمایید.
- این بخش از ۲ قسمت زیر تشکیل شده است :
 - Backup : ایجاد فایل پشتیبان از تنظیمات
 - Restore : بازگردانی تنظیمات پشتیبانی گرفته شده

Backup بخش ۴-۵-۲

- 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 : بازبانی به تنظیمات کارخانه
- Reset default settings : برگشت تنظیمات به مقدار پیشفرض
- Restore backup : انتخاب فایل پشتیبان

Restore

To restore configuration files, you can upload a previously generated backup file here. To reset settings (hostname, ...) to default values after restore backup, check "Reset default settings". To reset the firmware to its initial state, click "Perform reset".

Reset to defaults:

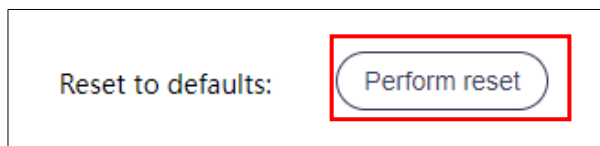
Reset default settings:

Restore backup: No file chosen

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

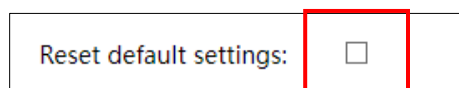
۴-۵-۳-۱ بخش Reset to defaults

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



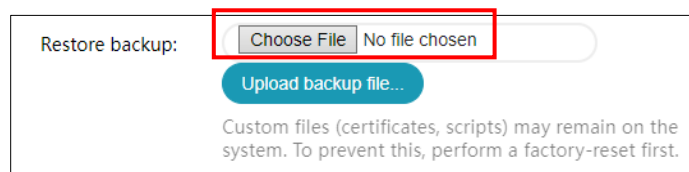
Reset default settings بخش ۴-۵-۳-۲

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



Restore backup بخش ۴-۵-۳-۳

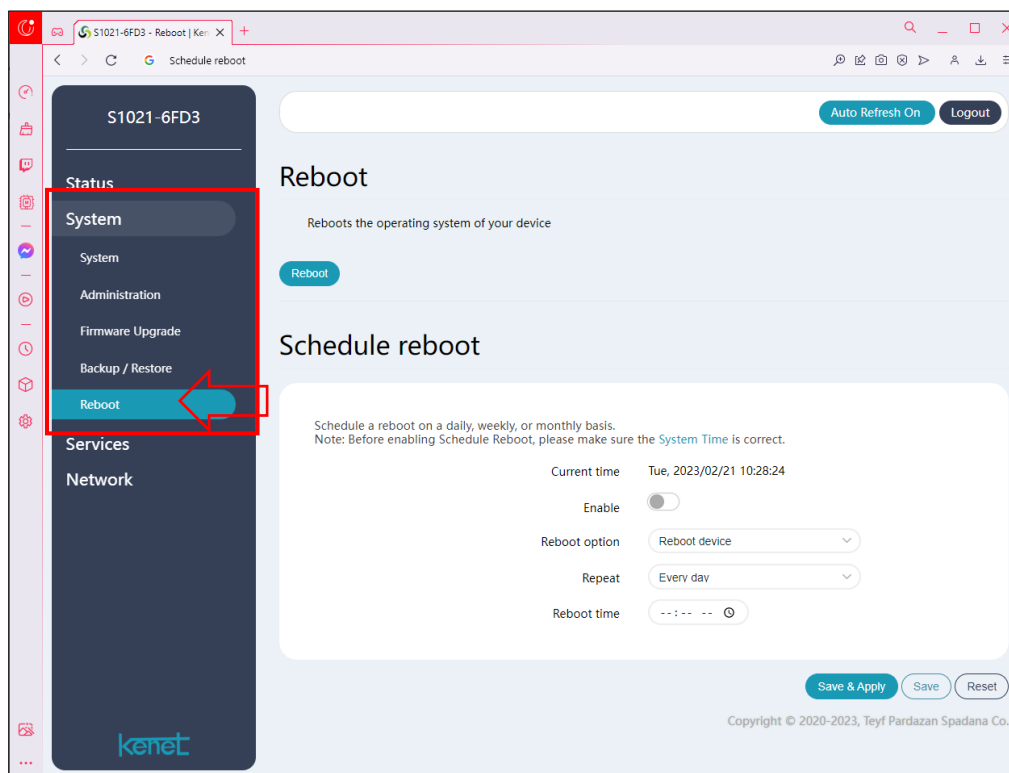
- از طریق این بخش می توانید فایل تنظیمات پشتیبان گرفته شده خود را انتخاب و بازیابی را شروع نمایید.



- 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.؟

Reboot قسمت ۴-۶

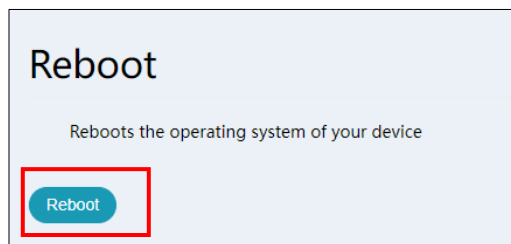


۴-۶-۱ معرفی

- 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

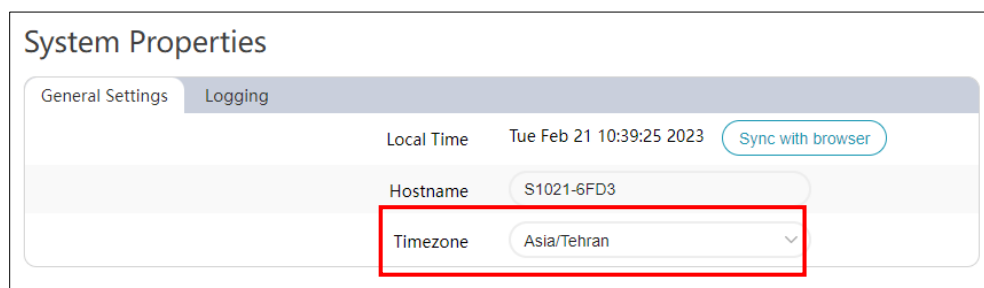
۴-۶-۲ بخش Reboot

- 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

Schedule reboot

Schedule a reboot on a daily, weekly, or monthly basis.
Note: Before enabling Schedule Reboot, please make sure the System Time is correct.

Current time Tue, 2023/02/21 11:42:56

Enable

Reboot option

Repeat

Reboot time

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.

Enable

- 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

Reboot option

Repeat

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

Repeat

boot time

- 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.

Current time Tue, 2023/02/21 11:54:21

Enable

Reboot option Restart network

Repeat **Every day**

Reboot time --:-- -- ⌚

dy, or monthly basis.
boot, please make sure th

Current time

Enable

Reboot option

Repeat

Reboot time --:-- -- ⌚

11	55	AM
12	56	PM
01	57	
02	58	
03	59	
04	00	
05	01	

- 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.

Repeat **Weekly**

Day(s) of week Sunday Monday Tuesday Wednesday
 Thursday Friday Saturday

Reboot time --:-- -- ⌚

- 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.

Repeat **Monthly**

Day(s) 1st 2nd 3rd 4th 5th 6th
 7th 8th 9th 10th 11th 12th
 13th 14th 15th 16th 17th
 18th 19th 20th 21th 22th
 23th 24th 25th 26th 27th
 28th 29th 30th 31th

Reboot time --:--:--

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

Save & Apply Save Reset

۵- بخش SERVICES

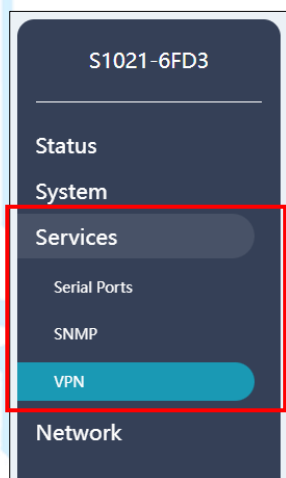
در این بخش به معرفی بخش SERVICES مبدل پرداخته می شود.

۱-۵ قسمت های بخش SERVICES

- قسمت Serial Ports

- قسمت SNMP

- قسمت OpenVPN



Serial Ports قسمت ۵-۲

The screenshot shows the Kenet web interface for configuring serial ports. The left sidebar is dark blue with a red box around the 'Serial Ports' menu item, which has a red arrow pointing to it. The main content area is light blue and displays the 'Serial Ports' configuration page. At the top, there's a 'Logout' button and a 'Port1: RS232 Port2: RS485' indicator. Below that, the title 'Serial Ports' is followed by a message: 'Below is a list of serial ports and their current state'. A table lists the ports with columns: Name, Interface, Serial Settings, Flow Control, Mode, Protocol, Started, and Enable. Two rows are shown: 'Port1' with interface 'RS232' and 'Port2' with interface 'RS485'. Both have 'Serial Settings' of '9600 8 N 1', 'Flow Control' of 'None', 'Mode' of 'TCP Client' and 'TCP Server' respectively, and 'Protocol' of 'Protocol-transparent'. The 'Started' column has 'No' and the 'Enable' column has a toggle switch and an 'Edit' button. At the bottom, there are 'Save & Apply', 'Save', and 'Reset' buttons. A copyright notice 'Copyright © 2020-2023, Teyf Pardazan Spadana Co.' is at the very bottom.

Name	Interface	Serial Settings	Flow Control	Mode	Protocol	Started	Enable
Port1	RS232	9600 8 N 1	None	TCP Client	Protocol-transparent	No	<input type="checkbox"/> Edit
Port2	RS485	9600 8 N 1	None	TCP Server	Protocol-transparent	No	<input type="checkbox"/> Edit

۵-۲-۱ معرفی

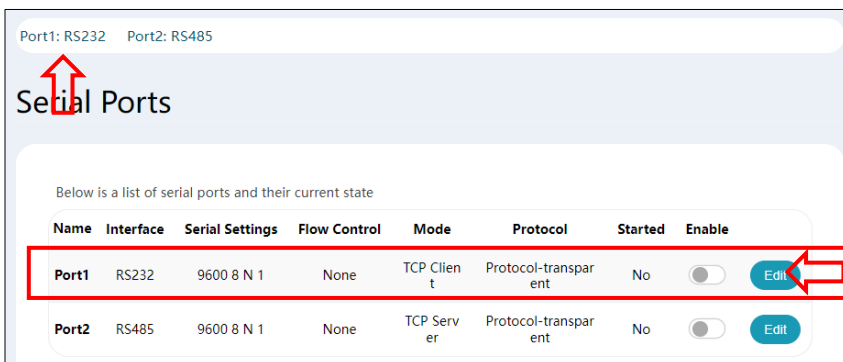
- این بخش اطلاعاتی پیرامون پورت های RS485 و RS232 ارائه می دهد.
- از ۲ بخش زیر تشکیل شده است:

- RS232 : تنظیمات پیکربندی RS232

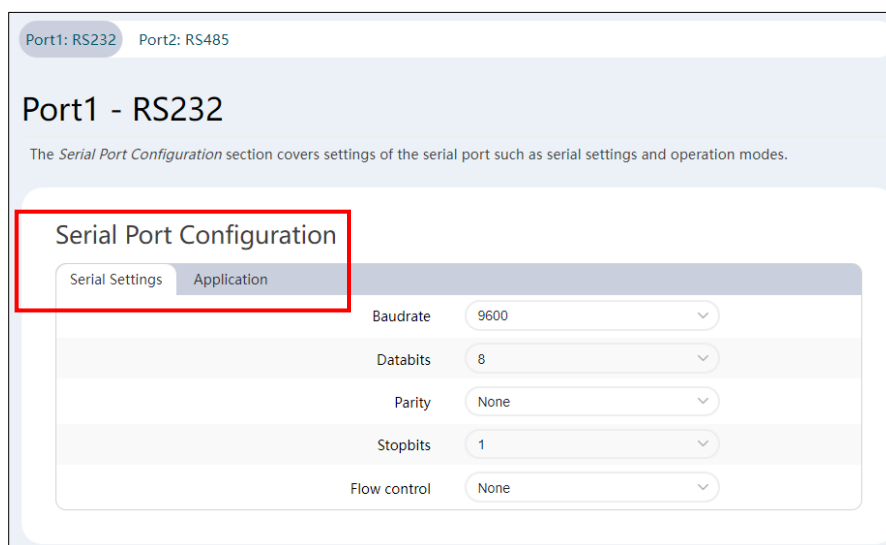
- RS485 : تنظیمات پیکربندی RS485

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.

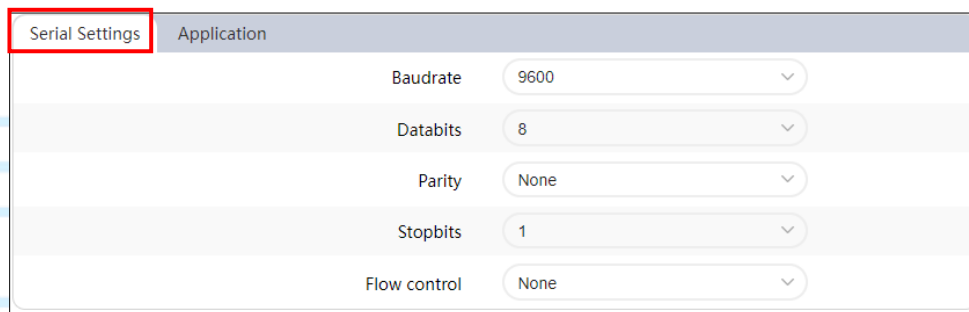


- هم چنین شما می توانید از بالای صفحه ، بر روی PORT1:RS232 انتخاب نمایید.
- پس از باز شدن بخش پیکربندی RS232 ، پنجره ی زیر برای شما نمایش داده می شود.



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

Serial Settings بخش ۵-۲-۲-۱



- 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.

Baudrate	9600
Databits	110 300 600 1200 2400 4800
Parity	9600
Stopbits	14400 19200 38400 57600 115200 230400
Flow control	

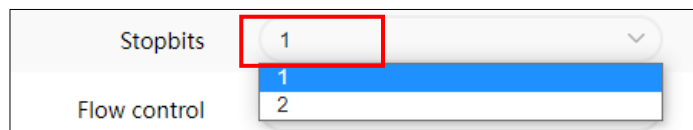
- در قسمت Databits مقادیر زیر قابل انتخاب هستند.
- ۴ مقدار ۵ و ۶ و ۷ و ۸ بیت ، برای طول دیتا قابل انتخاب می باشند.

Databits	8
Parity	5 6 7 8
Stopbits	

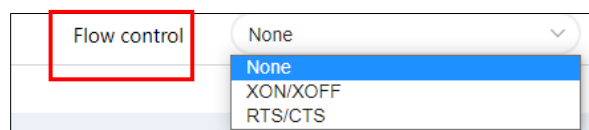
- در قسمت Parity مقادیر زیر قابل انتخاب هستند.
- ۳ مقدار ، زوج - فرد - بدون مقدار ، برای تصحیح خطای ارسال قابل انتخاب می باشد.

Parity	None
Stopbits	None Odd Even

- در قسمت Stopbits مقادیر زیر قابل انتخاب هستند.
- ۲ مقدار ، ۱ و ۲ 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.

بخش ۵-۲-۲-۲ 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

حالت TCP CLIENT ۵-۲-۲-۲-۱

Serial Port Configuration

Serial Settings Application

Mode TCP Client

Protocol Protocol-transparent

TCP keep-alive Send TCP keepalive packets

Inactivity timeout 60 0 - 86400 second(s), Use 0 to persist connection

Connection timeout 20 3 - 600 second(s), Connection request timeout

Client connection timeout 10 1 - 3600 second(s), Time between consecutive requests

Connection control Persistent

Destination address1 0.0.0.0

Destination port1 0

Destination address2 0.0.0.0

Destination port2 0

Destination address3 0.0.0.0

Destination port3 0

Destination address4 0.0.0.0

Destination port4 0

- در این بخش فیلدهای 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 tcp ip Modbus به modbus rtu

The screenshot shows a configuration window with a 'Protocol' dropdown menu. The 'Protocol' label is highlighted with a red box. The dropdown menu is open, showing 'Protocol-transparent' as the selected option and 'Modbus gateway' as an alternative option. Below the dropdown, there is a 'TCP keep-alive' checkbox.

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

The screenshot shows the 'TCP keep-alive' checkbox, which is checked. Below it, the text 'Send TCP keepalive packets' is visible.

- 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.

The screenshot shows the 'Inactivity timeout' input field with the value '60'. Below the input field, the text '0 - 86400 second(s), Use 0 to persist connection' is visible.

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

The screenshot shows the 'Connection timeout' input field with the value '20'. Below the input field, the text '3 - 600 second(s), Connection request timeout' is visible.

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

Connection control	Persistent
Destination address1	Persistent
	On Data Available

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

- Destination address : آدرس مقصد

- Destination port : پورت مقصد

Destination address1	0.0.0.0
Destination port1	0
Destination address2	0.0.0.0
Destination port2	0
Destination address3	0.0.0.0
Destination port3	0
Destination address4	0.0.0.0
Destination port4	0

۵-۲-۲-۲-۲ حالت TCP SERVER

Serial Port Configuration

Serial Settings Application

Mode TCP Server

Protocol Protocol-transparent

TCP keep-alive
Send TCP keepalive packets

Inactivity timeout 60
0 - 86400 second(s), Use 0 to persist connection

TCP port 4001

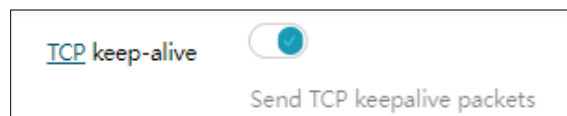
Max. connections 1
Maximum number of concurrent connections

- در قسمت Protocol مقادیر زیر قابل انتخاب هستند.

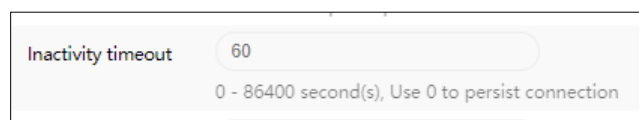
Protocol	Protocol-transparent
TCP keep-alive	Protocol-transparent
	Modbus gateway

- 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 .

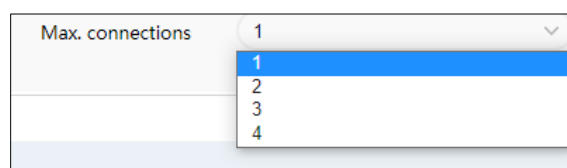


- در قسمت **TCP port** باید یک پورت را وارد کنید.



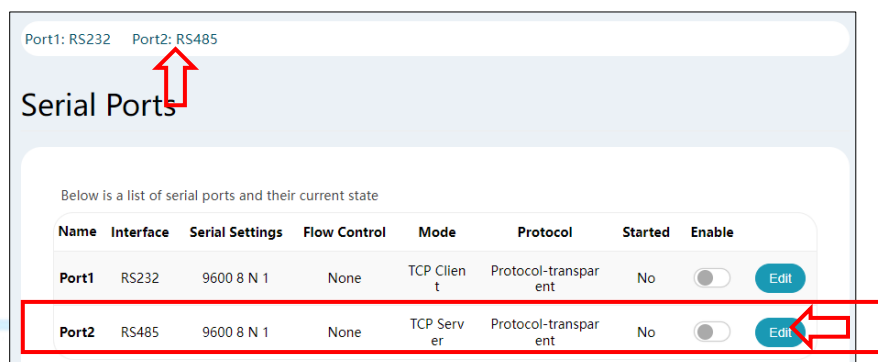
- در قسمت **Max connections** ، بیشترین تعداد کلاینت متصل را تعیین نمایید.

- 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.

Port1: RS232 Port2: RS485

Port2 - RS485

The *Serial Port Configuration* section covers settings of the serial port such as serial settings and operation modes.

Serial Port Configuration

Serial Settings Application

Baudrate	9600
Databits	8
Parity	None
Stopbits	1
Flow control	None

- تنظیمات پیکربندی پورت RS485 به ۲ بخش زیر تقسیم می شود:
 - Serial Settings : تنظیمات کلی بخش پورت RS485
 - Application : پیکربندی تنظیمات تخصصی RS485
- ۱-۳-۲-۵ بخش Serial Settings

Serial Settings Application

Baudrate	9600
Databits	8
Parity	None
Stopbits	1
Flow control	None

- 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.

Baudrate	9600
Databits	110 300 600 1200 2400 4800
Parity	9600 14400 19200 38400 57600 115200 230400
Stopbits	
Flow control	

- در قسمت Databits مقادیر زیر قابل انتخاب هستند.

- ۴ مقدار ۵ و ۶ و ۷ و ۸ بیت ، برای طول دیتا قابل انتخاب می باشند.

Databits	8
Parity	5 6 7 8
Stopbits	

- در قسمت Parity مقادیر زیر قابل انتخاب هستند.

- ۳ مقدار ، زوج - فرد - بدون مقدار ، برای تصحیح خطای ارسال قابل انتخاب می باشد.

Parity	None
Stopbits	None Odd Even

- در قسمت Stopbits مقادیر زیر قابل انتخاب هستند.

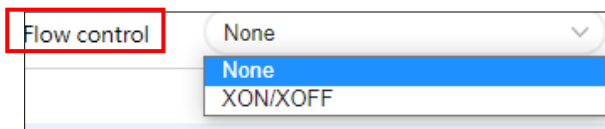
- ۲ مقدار ، ۱ و ۲ بیت ، برای پایان دیتا قابل انتخاب می باشند.

Stopbits	1
Flow control	1 2

- 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

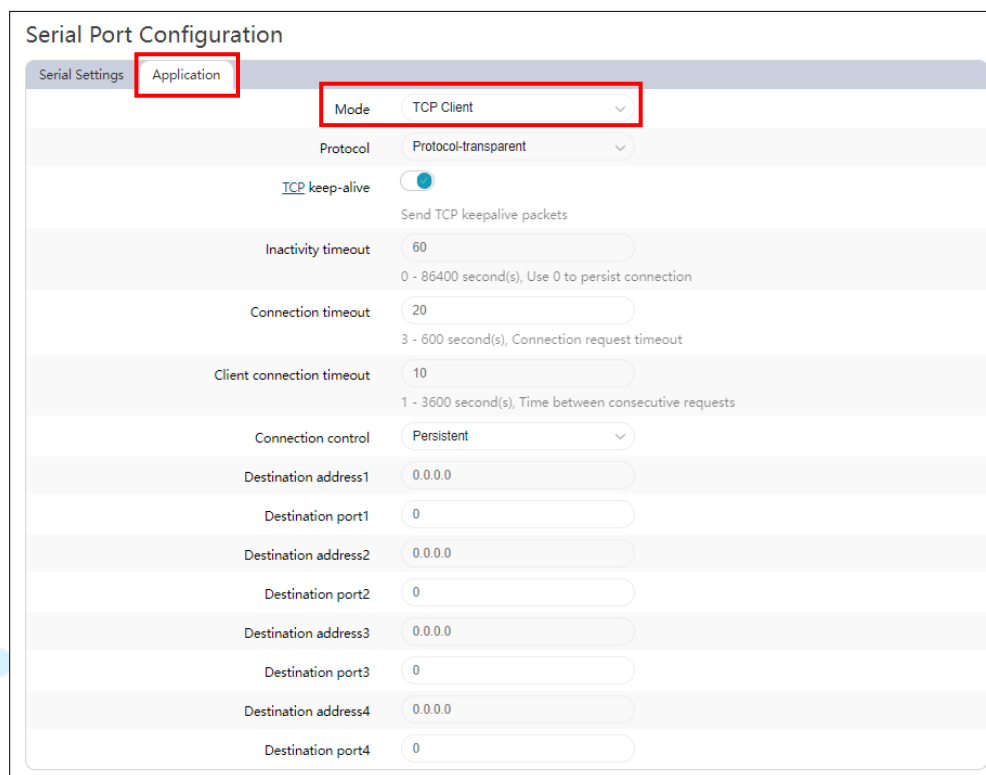
- این بخش با توجه به فیلد MODE بخش های متفاوتی دارد.

- 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 -

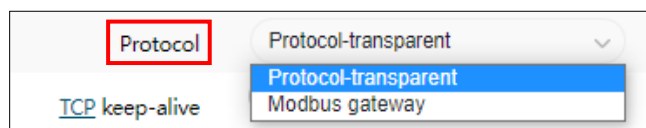
Inactivity timeout -

Connection timeout -

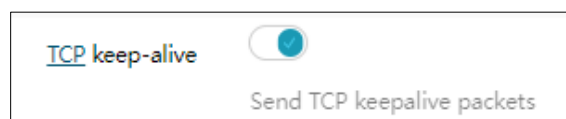
Client connection timeout -

- 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 :

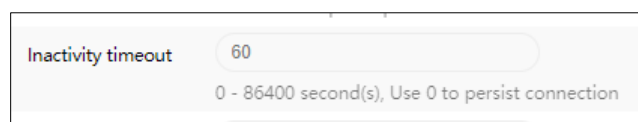
تبدیل modbus rtu به modbus tcp ip



- قسمت TCP keep-alive قابل فعال سازی می باشد.
- ارسال دوره ای بسته ای 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.

Connection timeout
3 - 600 second(s), Connection request timeout

- در قسمت Connection control مقادیر زیر قابل دریافت هستند.

- Persistent : مداوم
- no data available : بدون داده موجود

Connection control
Destination address1

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

- Destination address : آدرس مقصد
- Destination port : پورت مقصد

Destination address1	0.0.0.0
Destination port1	0
Destination address2	0.0.0.0
Destination port2	0
Destination address3	0.0.0.0
Destination port3	0
Destination address4	0.0.0.0
Destination port4	0

۵-۲-۳-۲-۲ حالت TCP SERVER

Serial Port Configuration

Serial Settings

Mode

Protocol

TCP keep-alive
Send TCP keepalive packets

Inactivity timeout
0 - 86400 second(s), Use 0 to persist connection

TCP port

Max. connections
Maximum number of concurrent connections

- در قسمت Protocol مقادیر زیر قابل انتخاب هستند.

Protocol	Protocol-transparent
TCP keep-alive	<ul style="list-style-type: none"> Protocol-transparent Modbus gateway

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

TCP keep-alive	<input checked="" type="checkbox"/>
Send TCP keepalive packets	

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

Inactivity timeout	60
0 - 86400 second(s), Use 0 to persist connection	

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

TCP port	4001
----------	------

- در قسمت Max connections ، بیشترین تعداد کلاینت متصل را تعیین نمایید.

- تعداد ۱ الی ۴ کلاینت قابل انتخاب است.

Max. connections	1
<ul style="list-style-type: none"> 1 2 3 4 	

Serial Ports بخش نکات ۴-۲-۵

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

Serial Port Configuration

Serial Settings Application

Baudrate 9600

Databits 8

Parity None

Stopbits 1

Flow control None

Back to Overview Save & Apply Save Reset

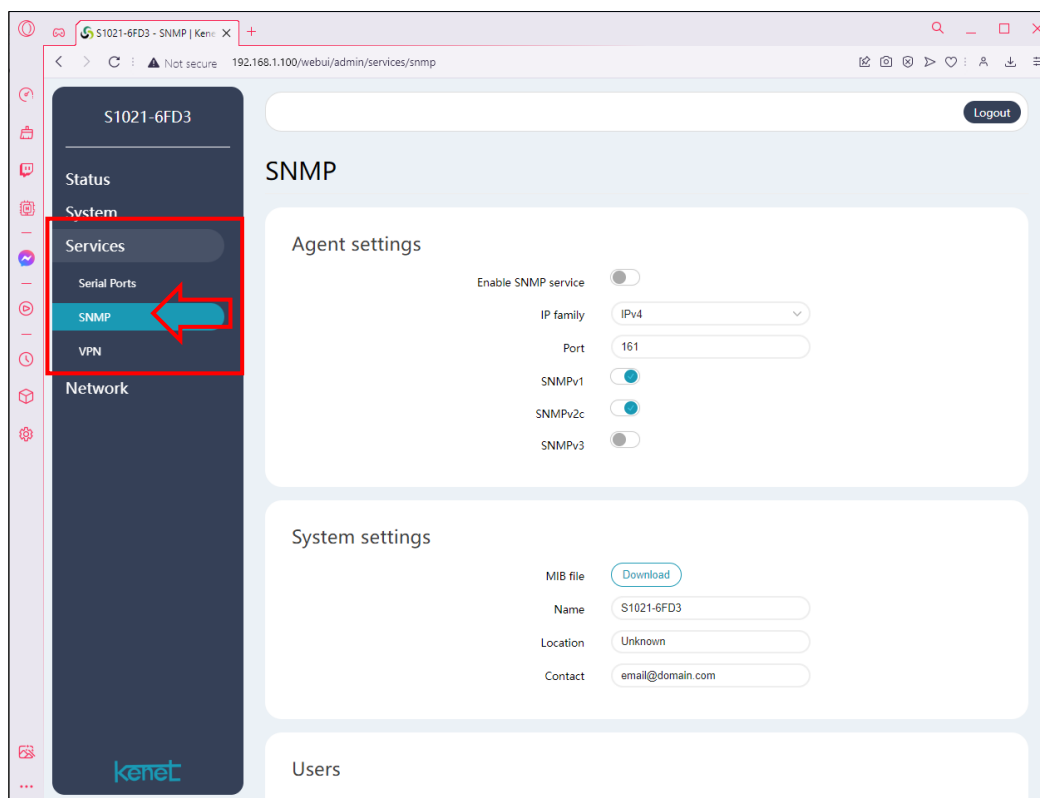
- سپس بعد از فعال کردن پورت مورد نیاز دیگر ذخیره و اعمال را دوباره انتخاب نمایید.

Serial Ports

Below is a list of serial ports and their current state

Name	Interface	Serial Settings	Flow Control	Mode	Protocol	Started	Enable
Port1	RS232	9600 8 N 1	None	TCP Client	Protocol-transparent	No	<input checked="" type="checkbox"/> Edit
Port2	RS485	9600 8 N 1	None	TCP Server	Protocol-transparent	No	<input type="checkbox"/> Edit

Save & Apply Save Reset



۵-۳-۱ معرفی SNMP

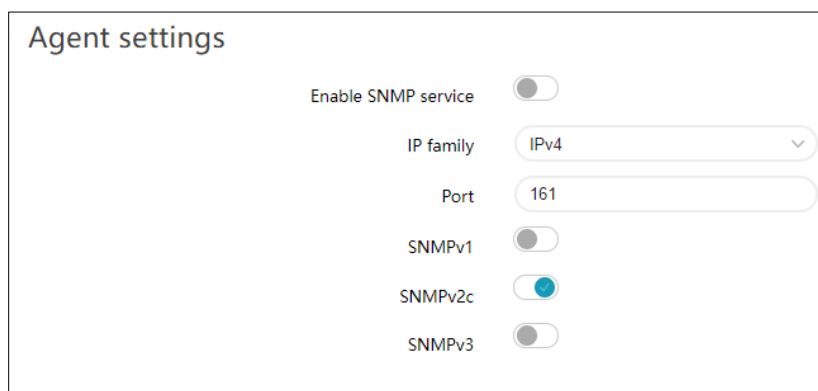
- مخفف عبارت Simple Network Management Protocol می باشد.
- پروتکل SNMP یکی از پروتکل های لایه Application است که امکان نقل و انتقال اطلاعات مدیریتی را بین عناصر شبکه ایجاد می کند و در واقع قسمتی از پروتکل TCP/IP می باشد. این پروتکل به طور وسیعی برای مانیتورینگ و مدیریت اجزاء شبکه استفاده می شود. بسیاری 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 مانیتور کردن ارجاع داده می شود.
- از ۵ بخش زیر تشکیل شده است:

- Agent settings : تنظیمات نماینده
- System settings : تنظیمات سیستم

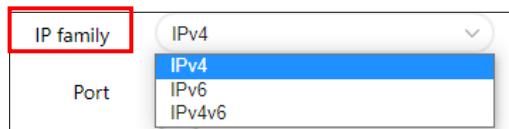
- Users : کاربران
- SNMP community : جامعه SNMP
- SNMP IPv6 community : جامعه SNMP IPv6

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

System settings

MIB file Download

Name S1021-6FD3

Location Unknown

Contact email@domain.com

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

Downloads

s1021.mib
Download complete

Clear Show more

۵-۳-۴ 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.

Users

Below is a list of SNMPv3 users.

Name	Security level	Authentication type	Privacy type	Access mode	Enable
<i>This section contains no values yet</i>					

Name Add

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

SNMP user

ho3j

Enable

Security level: No authentication / No privacy

Access Mode: Read-only

MIB subtree:

- 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:

Security level: No authentication / No privacy

Access Mode: No authentication / No privacy

Authentication / No privacy

Authentication and privacy

- No authentication / no authentication

بدون احراز هویت و بدون حریم خصوصی

- Authentication / no privacy :
با احراز هویت و بدون حریم 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

Access Mode: Read-only (selected)
MIB subtree: Read/Write

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

Users
Below is a list of SNMPv3 users.

Name	Security level	Authentication type	Privacy type	Access mode	Enable	
ho3j	No authentication / No privacy	-	-	Read/Write	<input checked="" type="checkbox"/>	Edit Delete

[Add](#)

- هم چنین می توانید ، کاربران فعلی را غیر فعال کنید و یا اطلاعات آنان 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 : آدرس 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.

SNMP community

Below is a list of SNMP communities.

Name	IP address	Net mask	Access mode	
public	0.0.0.0	0	Read-only	Edit
private	127.0.0.1	32	Read/Write	Edit

۱-۳-۵ ویرایش بخش عمومی

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

Name	IP address	Net mask	Access mode	
public	0.0.0.0	0	Read-only	Edit
private	127.0.0.1	32	Read/Write	Edit

- سپس پنجره زیر برای شما نمایش داده خواهد شد:

SNMP community

Community name

IP address

Net mask

Access mode

- شما می توانید فیلدهای زیر را ویرایش نمایید:

- Community name : نام
- IP address : آدرس IP
- Net mask : تفکیک ۲ قسمت هاست و شبکه
- Access mode : حالت دسترسی

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

Access mode Read-only
Read-only
Read/Write

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

۵-۳-۵-۲ ویرایش بخش خصوصی

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

Name	IP address	Net mask	Access mode	
public	0.0.0.0	0	Read-only	<input type="button" value="Edit"/>
private	127.0.0.1	32	Read/Write	<input type="button" value="Edit"/>

- سپس پنجره زیر برای شما نمایش داده خواهد شد:

SNMP community

Community name

IP address

Net mask

Access mode

- شما می توانید فیلد های زیر را ویرایش نمایید:

- Community name : نام
- IP address : آدرس IP
- Net mask : تفکیک ۲ قسمت هاست و شبکه
- Access mode : حالت دسترسی

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

Access mode Read-only
Read-only
Read/Write

- 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.

SNMP IPv6 community

Below is a list of SNMP IPv6 communities.

Name	Source	Access mode	
public	default	Read-only	<input type="button" value="Edit"/>
private	default	Read/Write	<input type="button" value="Edit"/>

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.

SNMP IPv6 community

Below is a list of SNMP IPv6 communities.

Name	Source	Access mode	
public	default	Read-only	<input type="button" value="Edit"/>
private	default	Read/Write	<input type="button" value="Edit"/>

- سپس پنجره زیر برای شما نمایش داده خواهد شد:

SNMP community

Community name:

Source:

Access mode:

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

Access mode

- Read-only
- Read-only**
- Read/Write

- 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.

SNMP IPv6 community

Below is a list of SNMP IPv6 communities.

Name	Source	Access mode	
public	default	Read-only	<input type="button" value="Edit"/>
private	default	Read/Write	<input type="button" value="Edit"/>

- سپس پنجره زیر برای شما نمایش داده خواهد شد:

SNMP community

Community name

Source

Access mode

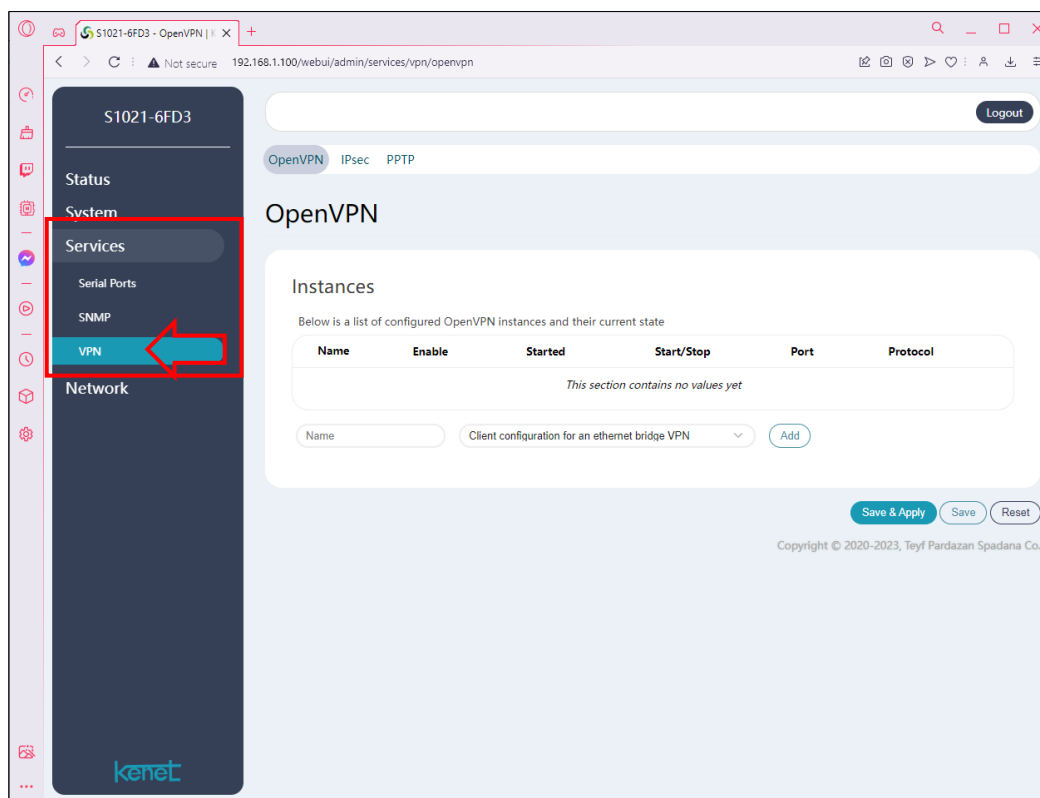
- شما می توانید فیلدهای زیر را ویرایش نمایید:
- Community name : نام ارتباط
- IP address : آدرس IP
- Access mode : حالت دسترسی
- حالت Access mode ۲ حالت زیر را دارا می باشد:

Access mode

- Read-only
- Read/Write

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

۵-۴ قسمت VPN



۵-۳-۱ معرفی VPN

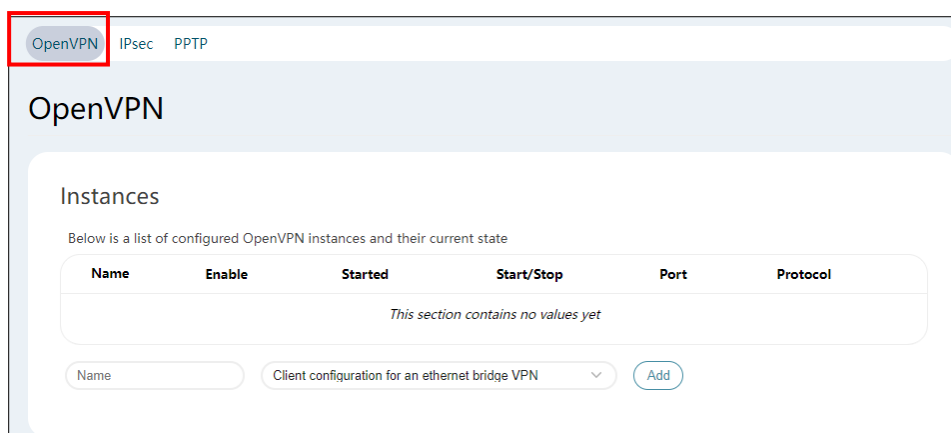
- Virtual private network به جای اینکه شما را به یک فضای نا امن و شلوغ در اینترنت متصل کند شما را به یک شبکه خصوصی از اینترنت انتقال میدهد که تنها به خودتان اختصاص دارد.
- از ۳ بخش زیر تشکیل شده است:

Open Source	- OpenVPN :
IP Security	- IPsec :
Point-to-Point Tunneling Protocol	- PPTP :

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.

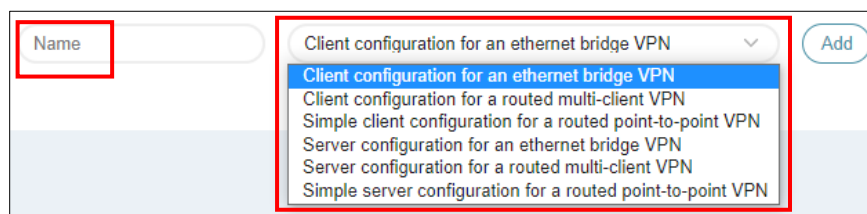
- در لیست سرویس‌های تمام ارائه دهندگان وجود دارد و به دلیل منبع باز بودن آن، هر کدام تغییراتی در این پروتکل اعمال کرده و به کاربر ارائه می دهند.



- 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.



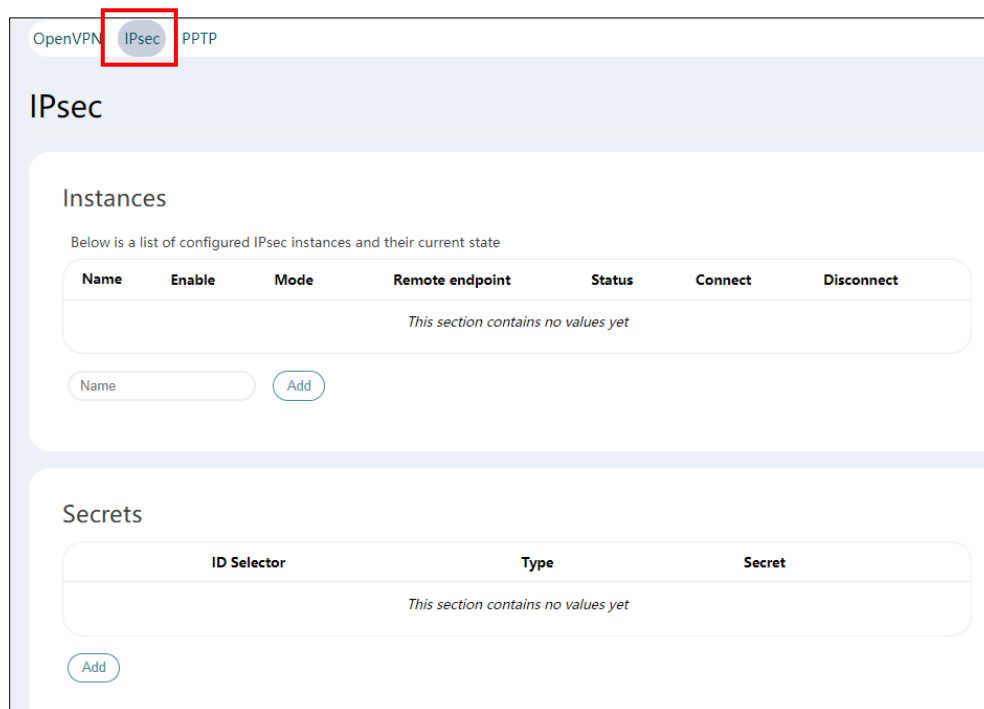
- ۶ حالت به صورت نمونه قابل انتخاب است:

- 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

۵-۳-۱-۲ 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 -

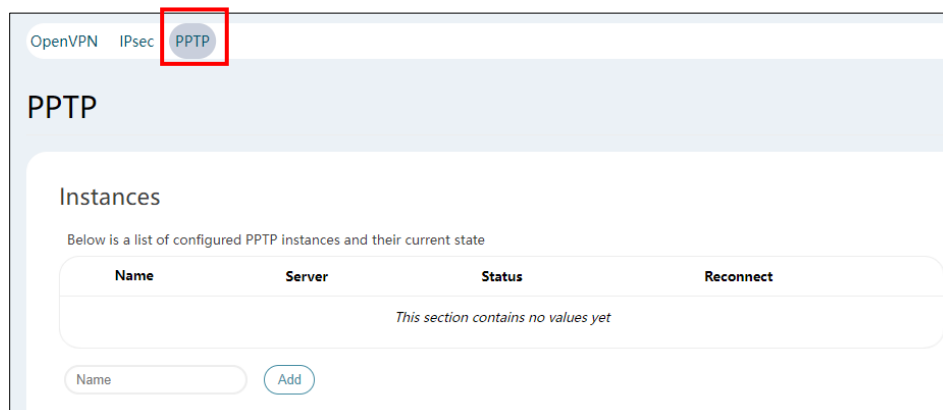
Remote endpoint : نقطه پایانی از راه دور -

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

۵-۳-۱-۳ پروتکل PPTP

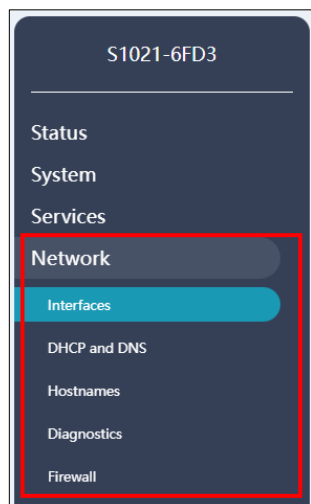
- PPTP یکی از رایج ترین و البته ضعیف ترین پروتکل‌هایی است که در ارتباطات VPN استفاده می‌شود.
- PPTP مخفف Point-to-Point Tunneling Protocol است توسط شرکت مایکروسافت ایجاد شده است که برای تونلینگ استفاده شده و با پروتکل MPPE رمزگذاری می‌شود.



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

۶- بخش network

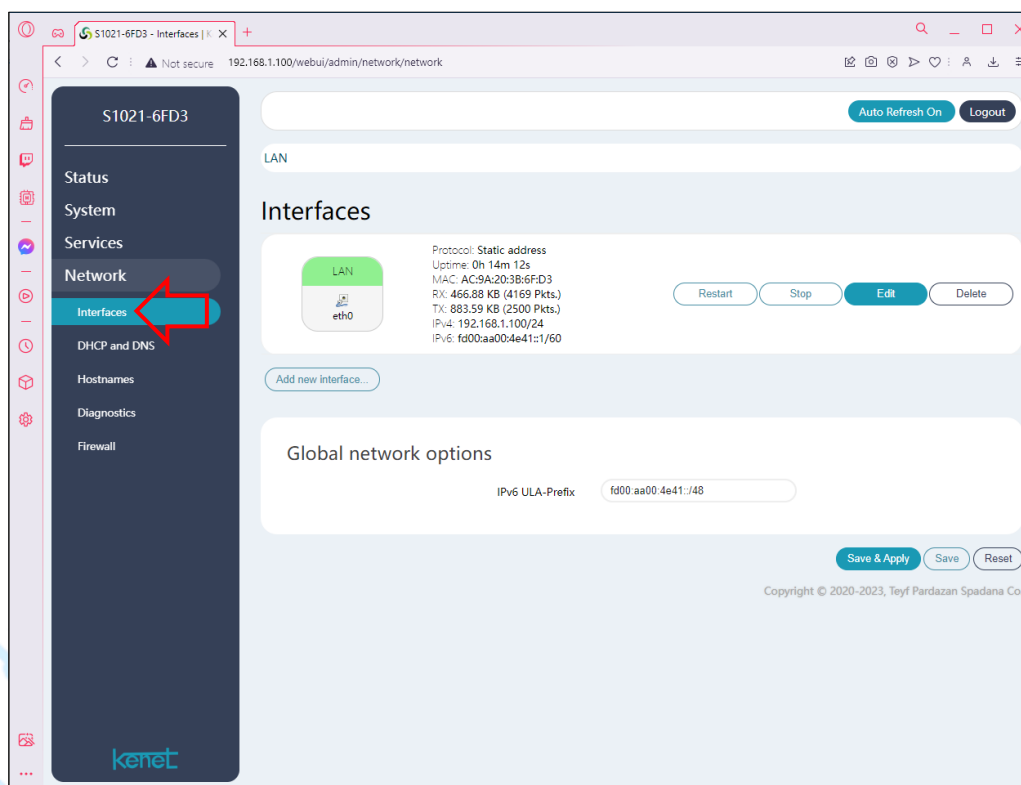
در این بخش به معرفی بخش network مبدل پرداخته می شود.



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 -

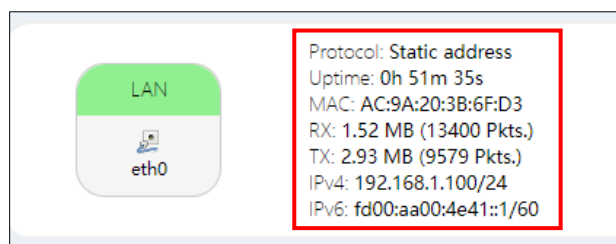
۶-۲-۲ بخش LAN

- 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 : آدرس MAC پورت LAN
- RX : میزان PKs های دریافتی
- TX : میزان PKs های ارسالی
- IPv4 : آدرس IP ویرایش ۴
- IPv6 : آدرس IP ویرایش ۶



Protocol: Static address
 Uptime: 0h 51m 35s
 MAC: AC:9A:20:3B:6F:D3
 RX: 1.52 MB (13400 Pkts.)
 TX: 2.93 MB (9579 Pkts.)
 IPv4: 192.168.1.100/24
 IPv6: fd00:aa00:4e41::1/60

۶-۲-۲-۲ دکمه های کنترلی LAN

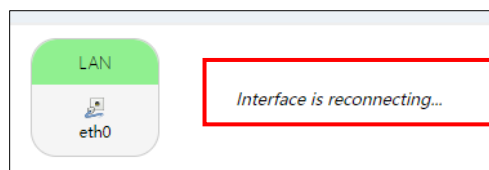
- RESTART : راه اندازی مجدد LAN
- STOP : توقف فعالیت LAN
- EDIT : ویرایش LAN
- DELET : حذف LAN



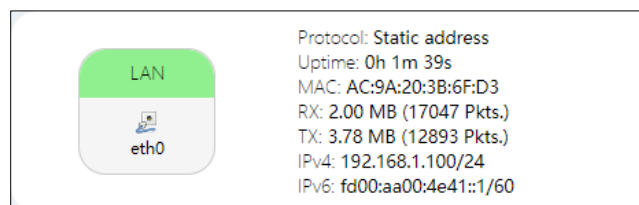
Restart Stop Edit Delete

۶-۲-۲-۲-۱ بخش RESTART

- این بخش باعث اتصال مجدد پورت LAN می شود.

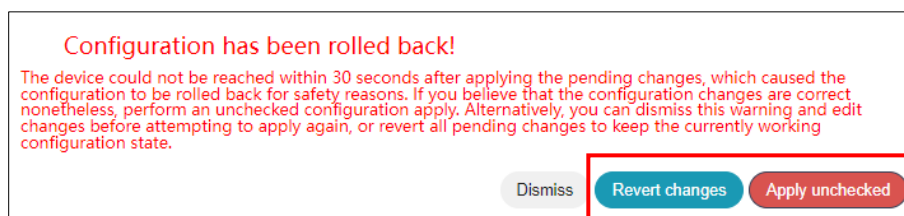


- در نهایت ، LAN مجددا راه اندازی می شود.



STOP بخش ۶-۲-۲-۲-۲

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

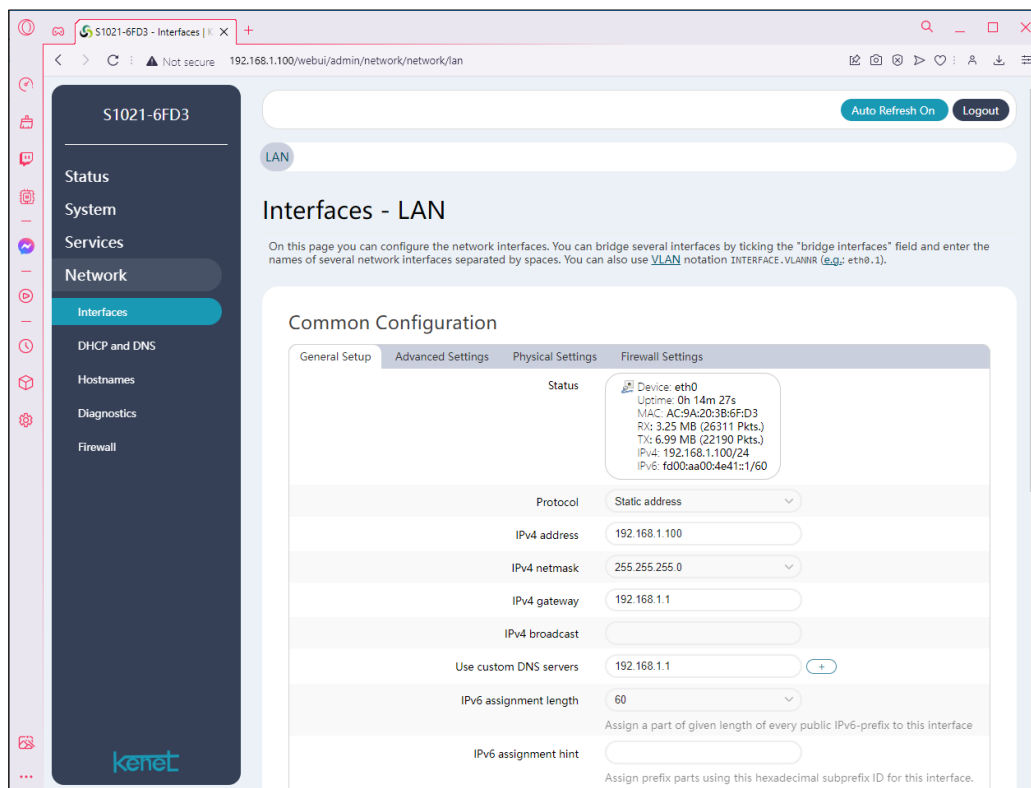


- در صورتی که قصد توقف LAN را دارید گزینه APPLY UNCHECKED را انتخاب نمایید؛ در غیر این صورت برای بازگرداندن این عمل ، گزینه REVERT CHANGES را انتخاب نمایید.
- در نظر داشته باشید در صورتی که گزینه APPLY را انتخاب کنید ارتباط شما با مبدل قطع می شود.

EDIT بخش ۶-۲-۲-۲-۳



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



- این بخش از ۲ زیر بخش زیر تشکیل شده است.

- Common Configuration
- DHCP Server

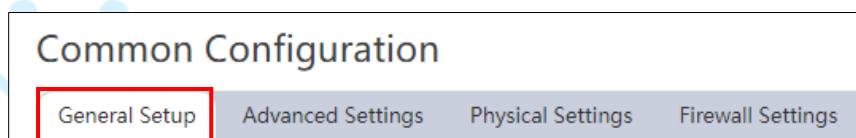
۱-۳-۲-۲-۶ زیر بخش Common Configuration

- 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

۱-۳-۲-۲-۶-۱ 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.

Status	 Device: eth0 Uptime: 1h 15m 43s MAC: AC:9A:20:3B:6F:D3 RX: 2.14 MB (18907 Pkts.) TX: 3.26 MB (11718 Pkts.) IPv4: 192.168.1.100/24 IPv6: fd00:aa00:4e41::1/60
--------	--

Protocol -

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

Protocol	Static address
IPv4 address	Static address
IPv4 netmask	DHCP client
IPv4 gateway	Unmanaged
	DHCPv6 client
	PPP
	PPPoE
	PPPoE

IPv4 address -

آدرس IP ویرایش ۴ مبدل را می توانید ویرایش کنید.

IPv4 address	192.168.1.100
--------------	---------------

IPv4 netmask -

NETMASK را می توانید انتخاب کنید.

IPv4 netmask	255.255.255.0
IPv4 gateway	255.255.255.0
IPv4 broadcast	255.0.0.0
	-- custom --

IPv4 gateway -

IP GATEWAY خود را می توانید ویرایش کنید.

IPv4 gateway	192.168.1.1
--------------	-------------

IPv4 broadcast -

می توانید ادرس IP برای BROADCAST خود را وارد کنید.

IPv4 broadcast

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.

Use custom DNS servers

IPv6 assignment length -

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

IPv6 assignment length
Assign a part of given length of every public IPv6-prefix to this interface

IPv6 assignment length
60
64
disabled
-- custom --
IPv6 assignment hint
Assign prefix parts using this hexadecimal

IPv6 assignment hint -

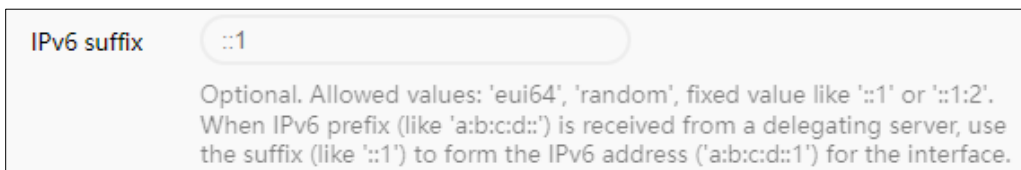
قسمت پیشوند را با استفاده از این شناسه ، زیر پیشوند هگزادسیمال برای این رابط اختصاص دهید.

IPv6 assignment hint
Assign prefix parts using this hexadecimal subprefix ID for this interface.

IPv6 suffix -

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

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.



Advanced Settings بخش ۶-۲-۲-۲-۳-۱-۲

- تنظیمات تخصصی در این بخش قرار دارد.



- این بخش از قسمت های زیر تشکیل شده است:

Bring up on boot -

فعال کردن در بوت

Bring up on boot

Use builtin IPv6-management -

استفاده از مدیریت داخلی ipv6

Use builtin IPv6-management

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)؟

Force link



Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).

Override MAC address -

باز نویسی آدرس MAC

Override MAC address

AC:9A:20:3B:6F:D3

Override MTU -

باز نویسی mtu

Override MTU

1500

Use gateway metric -

استفاده متریک دروازه

Use gateway metric

0

Physical Settings بخش ۶-۲-۲-۲-۳-۱-۳

- تنظیمات لایه فیزیکی شبکه در این بخش قرار دارد.

Common Configuration

General Setup

Advanced Settings

Physical Settings

Firewall Settings

- این بخش از قسمت های زیر تشکیل شده است:

Bridge interfaces -

ایجاد یک brifge بین چند اینترفیس

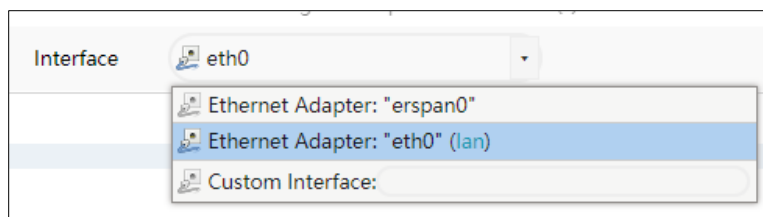
Bridge interfaces



creates a bridge over specified interface(s)

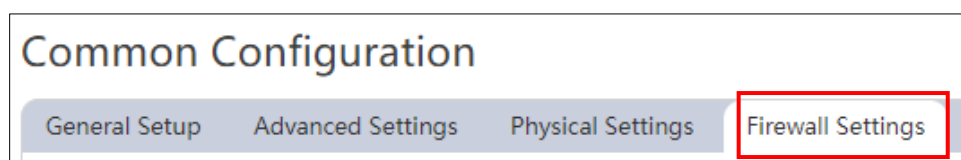
Interface -

اینترفیس

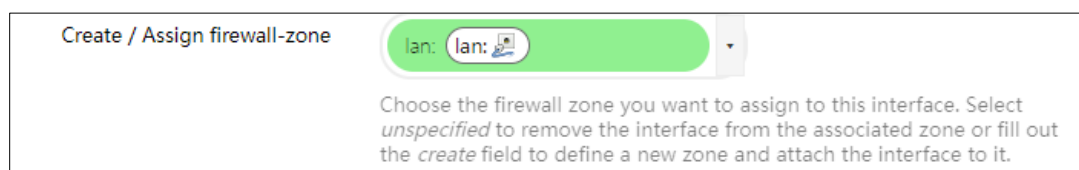


۶-۲-۲-۲-۳-۱-۴ بخش Firewall Settings

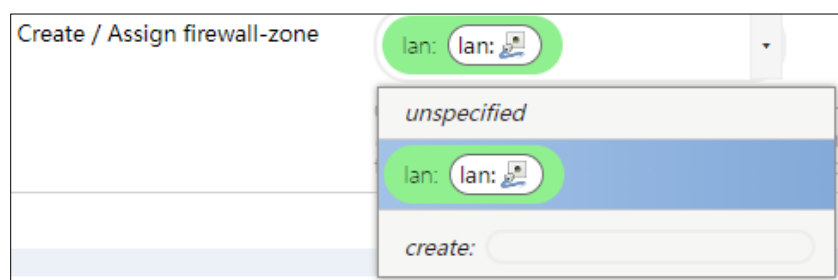
- تنظیمات Firewall شبکه در این بخش قرار دارد.



- تخصیص ناحیه فایروال



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



۶-۲-۲-۲-۳-۲ زیر بخش DHCP Server

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

General Setup بخش ۶-۲-۲-۲-۳-۲-۱

- تنظیمات کلی در این بخش قرار دارد.

DHCP Server

General Setup
Advanced Settings
IPv6 Settings

- این بخش از قسمت های زیر تشکیل شده است:

Ignore interface -
نادیده گرفتن اینترفیس

Ignore interface

Disable [DHCP](#) for this interface.

Start -
شروع

Start

Lowest leased address as offset from the network address.

Limit -
محدود کردن

Limit

Maximum number of leased addresses.

Lease time -
مدت زمان اختصاص ip توسط سرور dhcp

Lease time

12h

Expiry time of leased addresses, minimum is 2 minutes (2m).

Advanced Settings بخش ۶-۲-۲-۲-۳-۲-۲

- تنظیمات تخصصی در این بخش قرار دارد.

DHCP Server

General Setup
Advanced Settings
IPv6 Settings

- این بخش از قسمت های زیر تشکیل شده است:

Dynamic DHCP -

فعال کردن سرویس تخصیص ip خودکار

Dynamic [DHCP](#)

Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force -

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

Force

Force DHCP on this network even if another server is detected.

IPv4-Netmask -

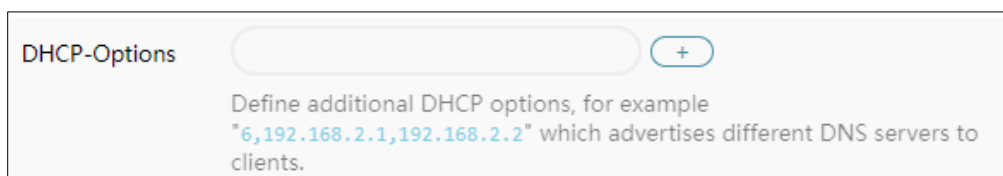
Netmask ارسال شده به مشتریان را بازنویسی کنید. معمولاً از زیر شبکه ای که ارائه می شود محاسبه می شود.

IPv4-Netmask

Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

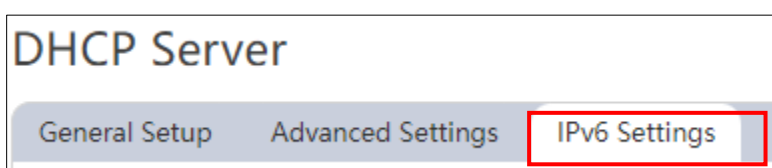
DHCP-Options -

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



IPv6 Settings بخش ۶-۲-۲-۲-۳-۲-۳

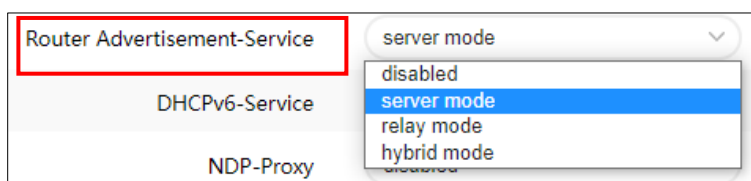
- تنظیمات IPV6 در این بخش قرار دارد.



- این بخش از قسمت های زیر تشکیل شده است:

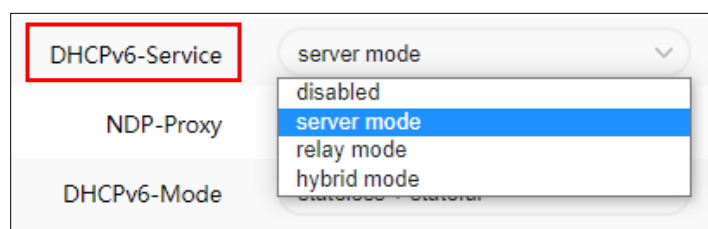
- Router Advertisement-Service

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.

NDP-Proxy disabled
 DHCPv6-Mode disabled
 relay mode
 hybrid mode
Default is stateless + stateful

DHCPv6-Mode -

تعیین حالت کاری dhcpv6

حالت پیشفرض stateless + stateful است.

DHCPv6-Mode stateless + stateful
 stateless
 stateless + stateful
 stateful-only

Always announce default router -

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

Always announce default router
 Announce as default router even if no public prefix is available.

Announced DNS servers -

تنظیم DNS servers

Announced DNS servers +

Announced DNS domains -

تنظیم DNS domains

Announced DNS domains +

ADD NEW INTERFACE بخش ۶-۲-۳

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

Add new interface...

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

The screenshot shows the 'Create Interface' page in the Kenet web interface. The page has a dark sidebar on the left with navigation links: Status, System, Services, and Network. The main content area is titled 'Create Interface' and contains the following form elements:

- Name of the new interface:** A text input field with a placeholder. Below it, a note states: 'The allowed characters are: A-Z, a-z, 0-9 and _'.
- Note: interface name length:** A note stating: 'Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)'.
- Protocol of the new interface:** A dropdown menu currently set to 'Static address'.
- Create a bridge over multiple interfaces:** A toggle switch that is currently turned off.
- Cover the following interface:** A dropdown menu currently set to 'erspan0'.

At the bottom of the form, there are 'Cancel' and 'Submit' buttons. The footer of the page reads 'Copyright © 2020-2023, Teyf Pardazan Spadana Co.'.

- از قسمت زیر تشکیل شده است:

Name of the new interface -

انتخاب نام برای اینترفیس جدید

Name of the new interface

The allowed characters are: A-Z, a-z, 0-9 and _

Note: interface name length

Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)

Protocol of the new interface -

تخصیص پروتکل برای اینترفیس جدید

Protocol of the new interface

Static address

Static address

DHCP client

Unmanaged

DHCPv6 client

PPP

PPTP

PPPoE

Create a bridge over multiple interfaces -

ایجاد یک bridge برای چندین رابط

Create a bridge over multiple interfaces

Cover the following interface -

این اینترفیس شامل چه دستگاهی شبکه ای هست.

Cover the following interface

erspan0

Ethernet Adapter: "erspan0"

Ethernet Adapter: "eth0" (lan)

Custom Interface:

Global network options بخش ۶-۲-۴

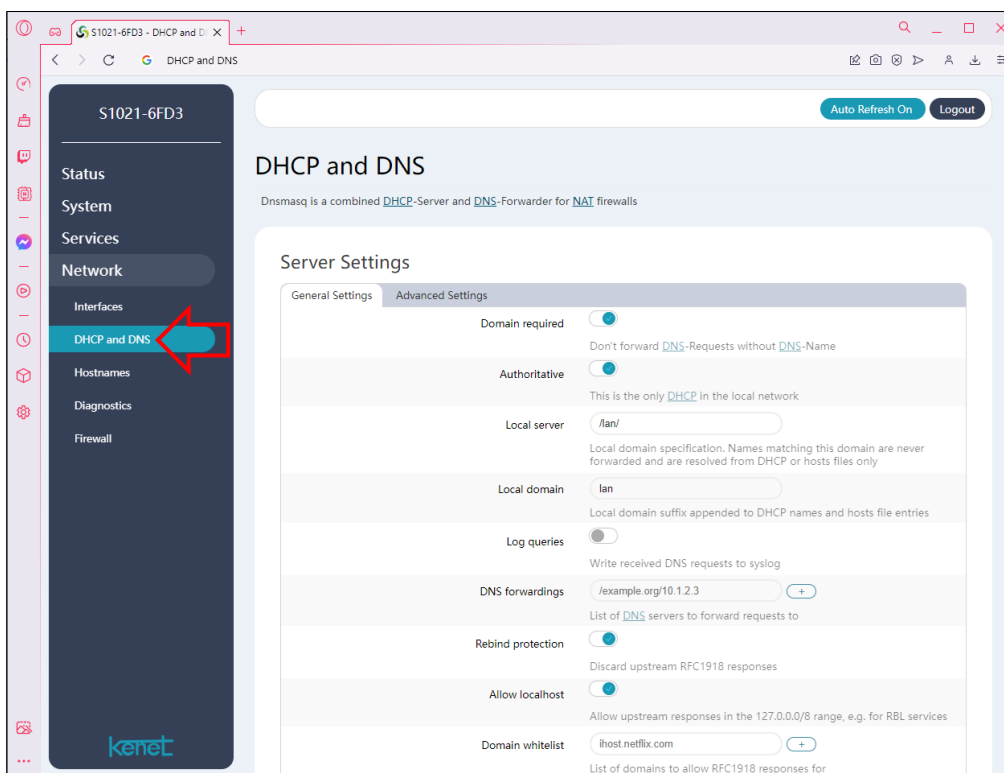
گزینه های عمومی شبکه -

Global network options

IPv6 ULA-Prefix

fd00:aa00:4e41::/48

۶-۳ قسمت DHCP and DNS



۶-۳-۱ معرفی DHCP and DNS

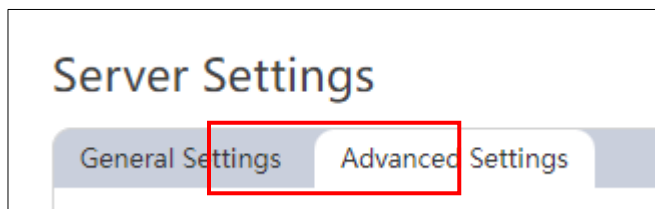
- در این بخش ، dns و dhcp پیکربندی می شود.
- این بخش از ۴ قسمت زیر تشکیل شده است :
 - Server Settings
 - Active DHCP Leases
 - Active DHCPv6 Leases
 - Static Leases

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

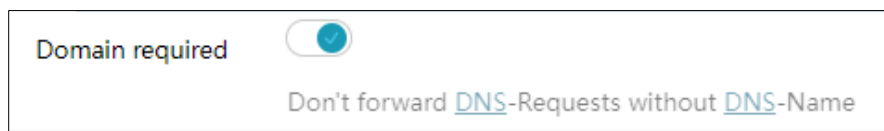
- تنظیمات کلی در این بخش قرار دارد.



- از بخش های زیر تشکیل شده است:

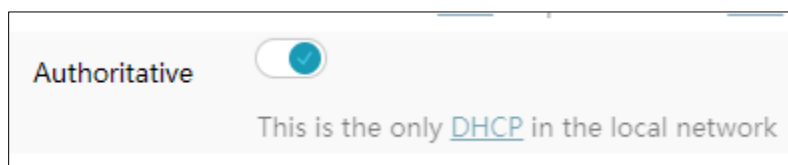
Domain required -

درخواست های DNS را بدون DNS-Name فوروارد نکنید.



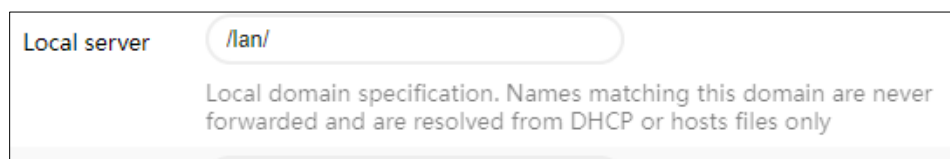
Authoritative -

این تنها DHCP در شبکه محلی است



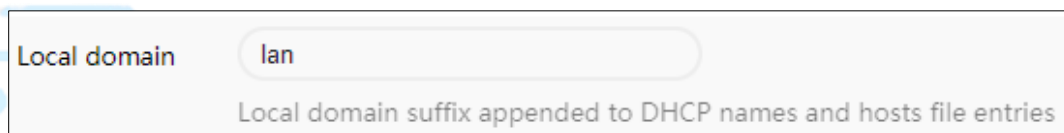
Local server -

سرور محلی؛ مشخصات دامنه محلی نام های مطابق با این دامنه هرگز ارسال نمی شوند و فقط از فایل های DHCP یا میزبان حل می شوند.



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.

Log queries



Write received DNS requests to syslog

DNS forwardings -

لیست سرورهای DNS برای ارسال درخواست ها

DNS forwardings

List of [DNS](#) servers to forward requests to**Rebind protection** -

پاسخهای RFC1918 بالادست را کنار بگذارید

Rebind protection



Discard upstream RFC1918 responses

Allow localhost -

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

خدمات RBL

Allow localhost



Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist -

فهرست دامنه‌هایی که اجازه پاسخهای RFC1918 را می‌دهند.

Domain whitelist



List of domains to allow RFC1918 responses for

Local Service Only -

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

Local Service Only



Limit DNS service to subnets interfaces on which we are serving DNS.

Non-wildcard -

فقط به اینترفیس‌های خاص متصل شود نه آدرس عام.

Non-wildcard

Bind only to specific interfaces rather than wildcard address.

Active DHCP Leases بخش ۶-۳-۳

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

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
DESKTOP-VC413JT	192.168.1.220	A0:8C:FD:DC:67:44	7h 45m 50s

Active DHCPv6 Leases بخش ۶-۳-۴

- جدول اختصاص های فعال dhcp ویرایش ۶
- از جدولی با ۴ ستون زیر تشکیل شده است:
- Hostname : نام دستگاه
- IPv4-Address : آدرس ipv4
- DUID : شناسه اختصاصی dhcp
- Leasetime remaining : زمان باقی مانده از اختصاص ip

Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
DESKTOP-VC413JT	fd00:aa00:4e41::1c0/128	000100012a697b1fa08cfddc6744	7h 49m 56s

Static Leases بخش ۶-۳-۵

- 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

Static Leases

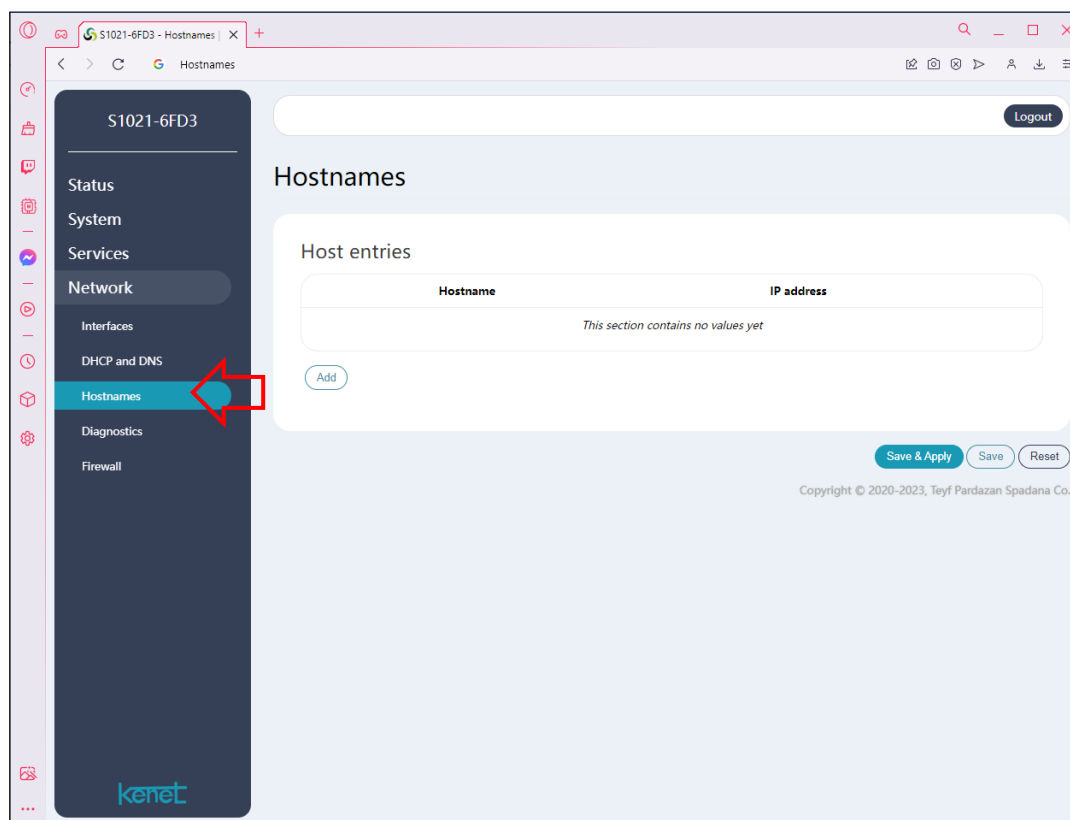
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

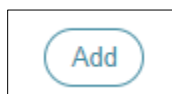
Hostname	<u>MAC-Address</u>	<u>IPv4-Address</u>	Lease time	<u>DUID</u>	<u>IPv6-Suffix (hex)</u>
<i>This section contains no values yet</i>					

Add

Hostnames قسمت ۴-۶



- 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.

Host entries

Hostname	IP address	
<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/>
<input type="button" value="Add"/>		

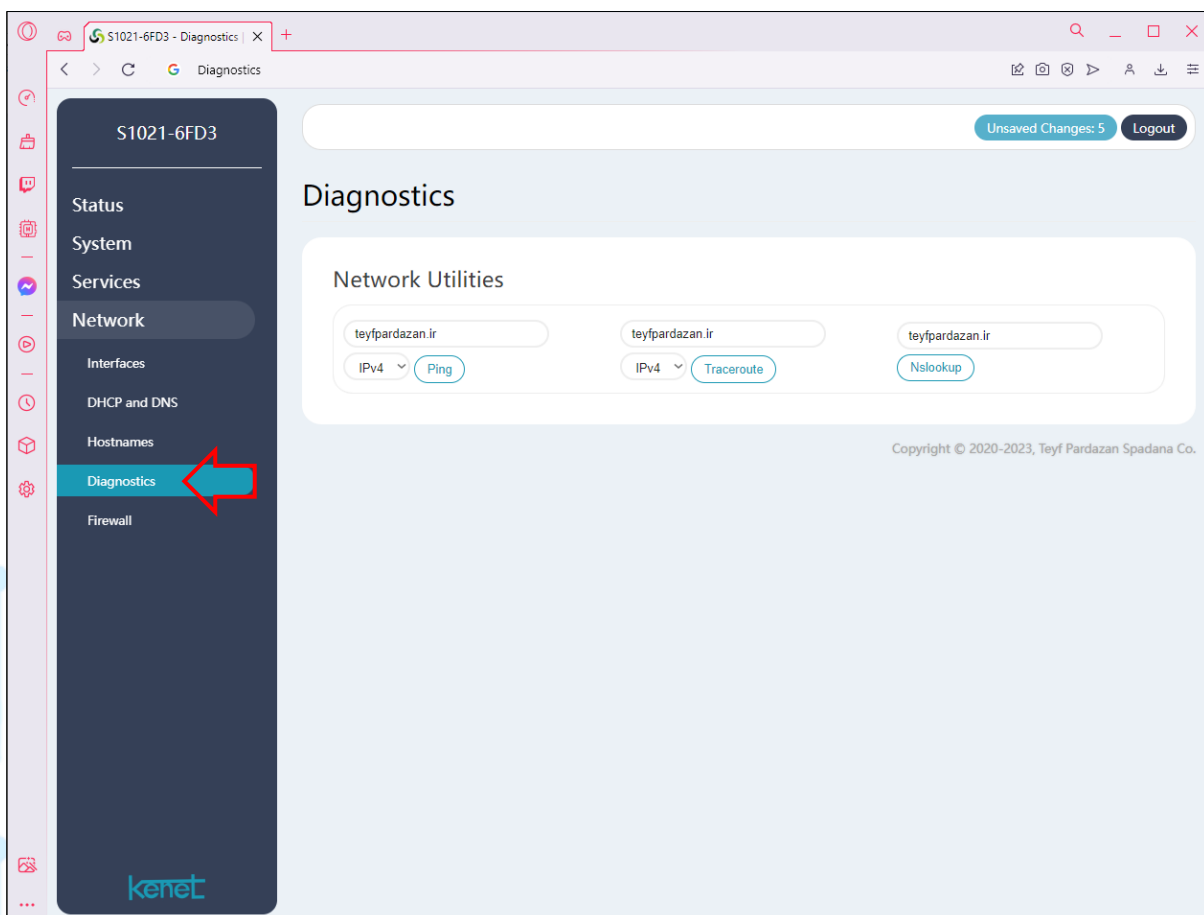
- در قسمت hostname می توانید نام مد نظر خود را وارد کنید.
- هم چنین در قسمت ip address می توانید ادرس ip مد نظر خود را برای این ردیف تنظیم کنید.

IP address

192.168.1.220 (DESKTOP-VC413JT.lan)
 192.168.1.100 (S1021-6FD3.lan)
 -- custom --

- از سمت راست هم ، زا زدن delete می توانید این ردیف را حذف کنید.
- در اخر گزینه save & apply را باید انتخاب کنید.

۵-۶ 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

The screenshot shows the Kenet Firewall configuration page. The left sidebar has a menu with 'Firewall' highlighted. The main area is titled 'Firewall - Zone Settings'. Under 'General Settings', there are two toggles: 'Enable SYN-flood protection' (checked) and 'Drop invalid packets' (unchecked). Below these are three dropdown menus: 'Input' (set to 'reject'), 'Output' (set to 'accept'), and 'Forward' (set to 'reject'). The 'Zones' section contains a table with the following data:

Name	Zone	Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan	lan	ACCEPT	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete

At the bottom of the 'Zones' section is an 'Add' button. At the bottom right of the main area are 'Save & Apply', 'Save', and 'Reset' buttons.

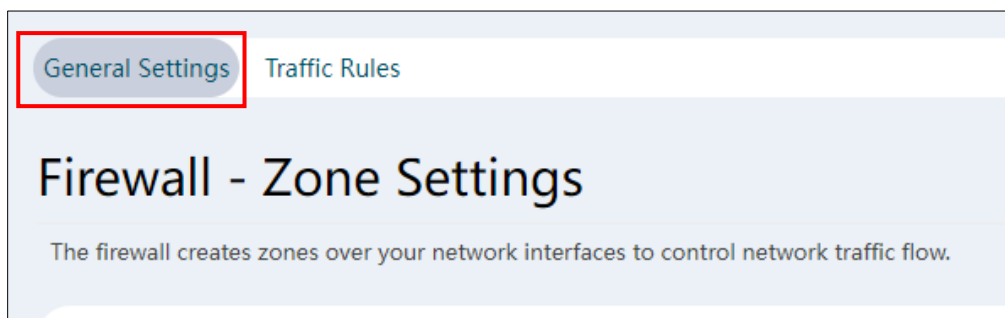
۶-۶-۱ معرفی firewall

- 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 -

Zone Settings بخش ۶-۶-۲



- این بخش از ۲ بخش زیر تشکیل شده است:

- General Settings

- Zones

General Settings بخش ۶-۶-۲-۱

- در این بخش تنظیمات کلی انجام می پذیرد ؛ که از فیلد های زیر تشکیل شده است:

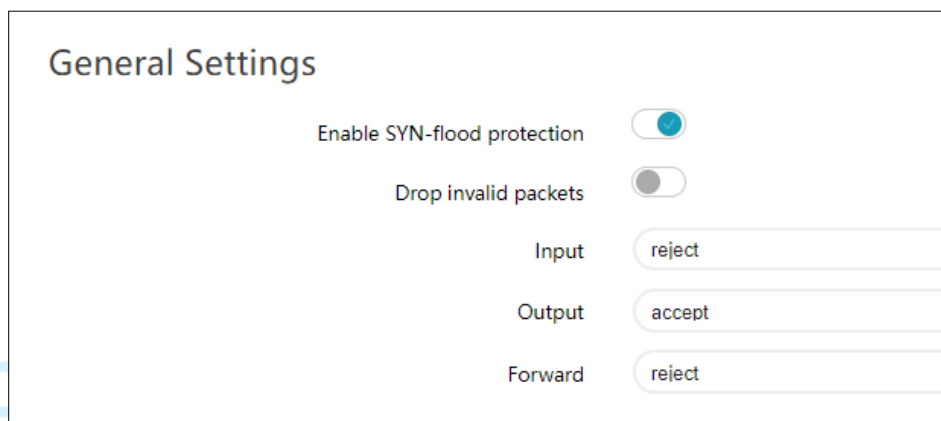
- Enable SYN-flood protection : فعال کردن SYN-flood

- 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 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.

Input	Output	Forward
<div style="border: 2px solid red; padding: 5px;"> accept reject drop accept </div>	accept	accept

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

Edit

Delete

۱-۲-۲-۶-۶ بخش edit

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

The screenshot shows the Kenet web interface for configuring the 'lan' zone. The 'Input' dropdown menu is open, showing options: accept, reject, drop, and accept. The 'Edit' button is highlighted with a red box. The interface includes a sidebar with navigation options like Status, System, Services, Network, and Firewall. The main content area displays the 'Zone "lan"' settings, including Name, Input, Output, Forward, Masquerading, MSS clamping, and Covered networks. The 'Inter-Zone Forwarding' section is also visible at the bottom.

- 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

General Settings قسمت ۱-۱-۲-۲-۶

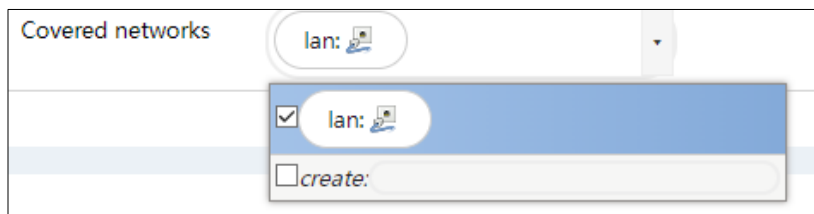
- در این بخش تنظیمات زیر قابل اعمال هستند:
 - Name : نام
 - Input : ورودی
 - Output : خروجی
 - Forward : هدایت شده
 - Masquerading : فعال کردن Masquerading
 - MSS clamping : فعال کردن MSS clamping
 - Covered networks : اینترفیس های شامل شده؟

Zone "lan"

This section defines common properties of "lan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

General Settings	Advanced Settings
Name	<input type="text" value="lan"/>
Input	<input type="text" value="accept"/>
Output	<input type="text" value="accept"/>
Forward	<input type="text" value="accept"/>
Masquerading	<input type="checkbox"/>
MSS clamping	<input type="checkbox"/>
Covered networks	<input type="text" value="lan:"/>

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

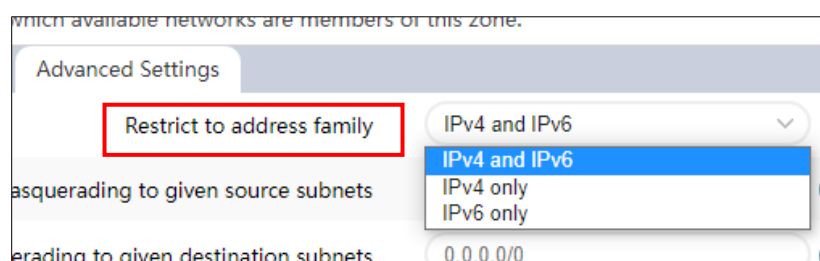


Advanced Settings قسمت ۶-۶-۲-۲-۱-۲

- در این بخش تنظیمات زیر قابل اعمال هستند:

- Restrict to address family

تعیین نوع آدرس ip



- Restrict Masquerading to given source subnets

- Restrict Masquerading to given destination

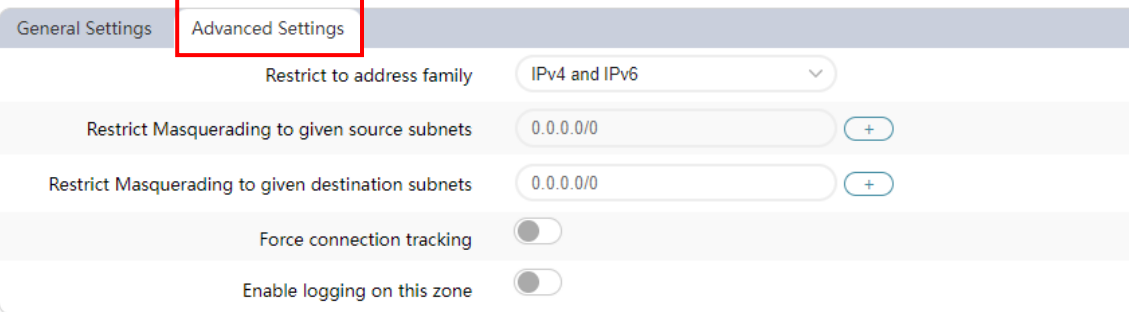
subnets

- Force connection tracking

- Enable logging on this zone

Zone "lan"

This section defines common properties of "lan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.



- در صورت فعال کردن بخش Enable logging on this zone بخش

زیر نمایش داده می شود.

Enable logging on this zone

Limit log messages 10/minute

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

- 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

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (lan) and other zones. *Destination zones* cover forwarded traffic originating from "lan". *Source zones* match forwarded traffic from other zones targeted at "lan". The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:

Allow forward from *source zones*:

delete بخش ۶-۶-۲-۲-۲

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

Traffic Rules بخش ۶-۶-۳

General Settings **Traffic Rules**

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the device.

- 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

Traffic Rules بخش ۶-۶-۳-۱

- 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

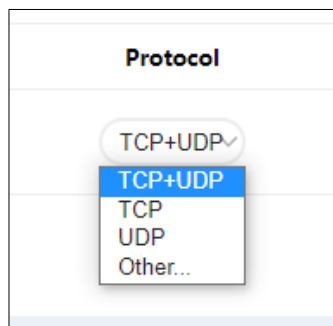
Traffic Rules			
Name	Match	Action	Enable
<i>This section contains no values yet</i>			

Open ports on device بخش ۶-۶-۳-۲

- 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.

Open ports on device			
Name	Protocol	External port	
<input type="text" value="New input rule"/>	<input type="text" value="TCP+UDP"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="button" value="Add"/>			

- در قسمت پروتکل ، موارد زیر قابل انتخاب هستند:



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

The screenshot displays the Kenet web interface for configuring a Firewall Traffic Rule. The browser address bar shows the URL: 192.168.1.100/webui/admin/network/firewall/rules/cfg0492bd. The page title is "Firewall - Traffic Rules - r1". The configuration fields are as follows:

- Rule is enabled: Disable
- Name:
- Restrict to address family:
- Protocol:
- Source zone:
- Source MAC address:
- Source address:
- Source port:
- Output zone:
- Destination address:
- Destination port:
- Action:
- Extra arguments:
- Week Days:

Additional text on the page includes "Unsaved Changes: 6" and "Logout" buttons in the top right, and "kenet" branding in the bottom left of the sidebar.

add ۶-۶-۳-۲-۱

- در این قسمت به انجام تنظیمات rule ای که قصد اضافه کردن آن 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 آدرس دهی ip

- Protocol

پروتکل

- Source zone

ناحیه مبدا

Source zone	Device (output)
MAC address	Device (output)
Source address	Any zone (forward)
Source port	lan: lan:

Source MAC address -
 ادرس mac مبدا

Source MAC address	any
Source address	any
Source port	A0:8C:FD:DC:67:44 (DESKTOP-VC413JT.lan) AC:9A:20:5D:11:B6 (S1021-11B6.lan) -- custom --

Source address -
 ادرس مبدا

Source address	any
Source port	any
Output zone	192.168.1.100 (S1021-11B6.lan) 192.168.1.220 (DESKTOP-VC413JT.lan) -- custom -- unspecified

Source port -
 ناحیه داخلی

Source port	any
-------------	-----

Output zone -
 ناحیه خارجی

Output zone	unspecified
Destination address	unspecified
Destination port	Any zone
Action	lan: lan: accept

Destination address -

ادرس مقصد

Destination address	any
Destination port	<ul style="list-style-type: none"> any 192.168.1.100 (S1021-11B6.lan) 192.168.1.220 (DESKTOP-VC413JT.lan) -- custom --
Action	accept

Destination port -

پورت مقصد

Destination port	any
------------------	-----

Action -

عملیات

Action	accept
Extra arguments	<ul style="list-style-type: none"> drop accept reject don't track

Extra arguments -

ارسال پارامتر های اضافه به ip tables

Extra arguments	
Passes additional arguments to iptables. Use with care!	

Week Days -

روز های هفته

Week Days	-- please select --
Month Days	<ul style="list-style-type: none"> <input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday
Time (hh:mm:ss)	
Time (hh:mm:ss)	
Time (yyyy-mm-dd)	

Month Days -

روز های ماه

Source zone

Source MAC address

Source address

Source port

Output zone

Destination address

Destination port

Action

Extra arguments

Week Days

Month Days

-- please select --

- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31

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

Start Time (hh:mm:ss)	<input type="text"/>
Stop Time (hh:mm:ss)	<input type="text"/>
Start Date (yyyy-mm-dd)	<input type="text"/>
Stop Date (yyyy-mm-dd)	<input type="text"/>

Time in UTC -

زمان بر حسب utc

Time in UTC

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

Traffic Rules			
Name	Match	Action	Enable
r1	Any tcp, udp From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/> ↑ ↓ Edit Delete

Source NAT بخش ۳-۳-۶

- 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

Source NAT			
Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.			
Name	Match	Action	Enable
This section contains no values yet			
Add			

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](#) -

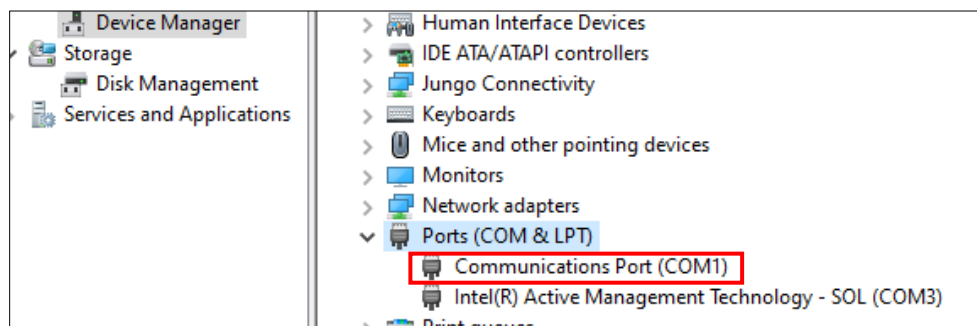
- شما می توانید هر یک از نرم افزار های فوق را از سایت سازنده دریافت نمایید.

۷-۲ نحوه ایجاد ارتباط کنسول با مبدل

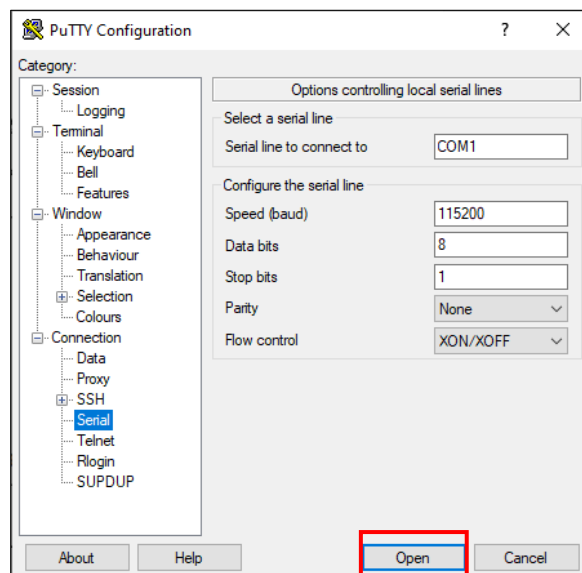
- از نصب بودن درایور های خود اطمینان حاصل فرمایید.
- ابتدا باید کابل کنسول مبدل که به همراه مبدل است را به درگاه کنسول مبدل متصل نمایید.
- سپس یکی از نرم افزار های معرفی شده را باز نمایید.
- اطلاعات زیر را در نرم افزار خود تنظیم نمایید.

Select a serial line	
Serial line to connect to	COM1
Configure the serial line	
Speed (baud)	115200
Data bits	8
Stop bits	1
Parity	None
Flow control	XON/XOFF

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

```

KENET
A RELIABLE CONNECTION
-----
Bootloader v1.2.0 build 23013112
-----
UID: FF6784270716102D
SN: 2302001465
HW: 1.0
ETH MAC Address: AC:9A:20:5D:11:B6

Loading Image ... OK
Booting Image ...
Verifying ... OK
Preparing ... OK

Starting Kernel ...

Please press Enter to activate this console.
█

```

- 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.

```

51021-11B6 login: admin
Password: █

```

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

```

kenLogin incorrect
S1021-11B6 login: admin
Password:
KENET
A RELIABLE CONNECTION
-----
S1021 v1.11.0 build 23021913
-----
[admin@S1021-11B6] >

```

۳-۷ نحوه بازیابی به تنظیمات کارخانه از طریق کنسول

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

- reset-configuration

```

[admin@S1021-11B6] > reset-configuration
Restoring default 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

- لازم است فایل به 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 لپت 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



۸-۲-۳ 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/>