سودار

23.04

سودار

Jun 26, 2023

فهرست مطالب

فصل 1

اَمنِت

1.1 مشخصات اَمنِت

محصول اَمنِت با استفاده از محصولات سودار و همدار راه حلی یکپارچه و امن برای ارتباطات شبکه سازمانی ارائه می کند. در این محصول تمامی ارتباطات کاربران با سَرویسهای شبکه از ابتدا به صورت امن برقرار می گردد و کاربران صرف نظر از مکان خود هویت خود را حفظ نموده و تمامی فعالیتهای آنها در کل شبکه قابل شناسایی است.

هسته محصول اَمنِت دارای ویژگیهای زیر است:

1. جدا سازی اطلاعات امنیتی مهم شبکه در یک سیستم مجزا و ایجاد قابلیت کنترل امنیتی سیستم در مرکز
2. پشتیبانی از شبکه های همپوشان لایه 2 و لایه 3 به صورت همزمان
3. یافتن کلیه نودهای شبکه فقط با اتصال به یک نود و ایجاد اتوماتیک تونلهای امن شبکه بین نودها
4. ارتباط Full-Mesh تمام اتوماتیک بین نودهای شبکه بدون نیاز به تنظیمات
5. ناحیه بندی نودهای شبکه و اتصال Full-Mesh در هر ناحیه و امکان ارتباط بین ناحیه ای با تونلهای امن
6. امکان توزیع ترافیک از چند مسیر و استفاده از مسیرهای جایگزین در صورت قطعی یک مسیر
7. وجود امنیت در سراسر شبکه از نقطه شروع در موبایل‌ها و پایانه های کاری دسکتاپ لینوکس و ویندوز تا انتهای مسیر
8. تنظیمات سهل و روان در نودها برای جلوگیری از اتلاف وقت و اشتباهات مدیر سیستم
9. انجام تنظیمات محلی هر نود توسط مدیر محلی سیستم یا به صورت مرکزی توسط یک مدیر از طریق شبکه مجزا
10. پشتیبانی از شبکه مجزا جهت مدیریت نودها برای حفظ امنیت سیستم
11. انجام تنظیمات امنیتی به صورت offline برای تمام شبکه
12. مجتمع سازی با محصول همدار

سالیان درازی است که برای ایجاد امنیت ارتباطات بین شبکه ها از VPN استفاده می‌شود. از مشکلات مهم در VPN های مرسوم پیچیدگی تنظیمات و هزینه نگهداری آنهاست. از طرفی ایجاد امکانات و تنظیمات مختلف می‌تواند باعث شود مدیران شبکه به پیاده سازی برخی حالتهای خاص بپردازند ولی از سوی دیگر این پیچیدگی باعث ایجاد مشکلات مختلفی می‌گردد. مخصوصا زمانی که تعداد VPN ها زیاد باشد.

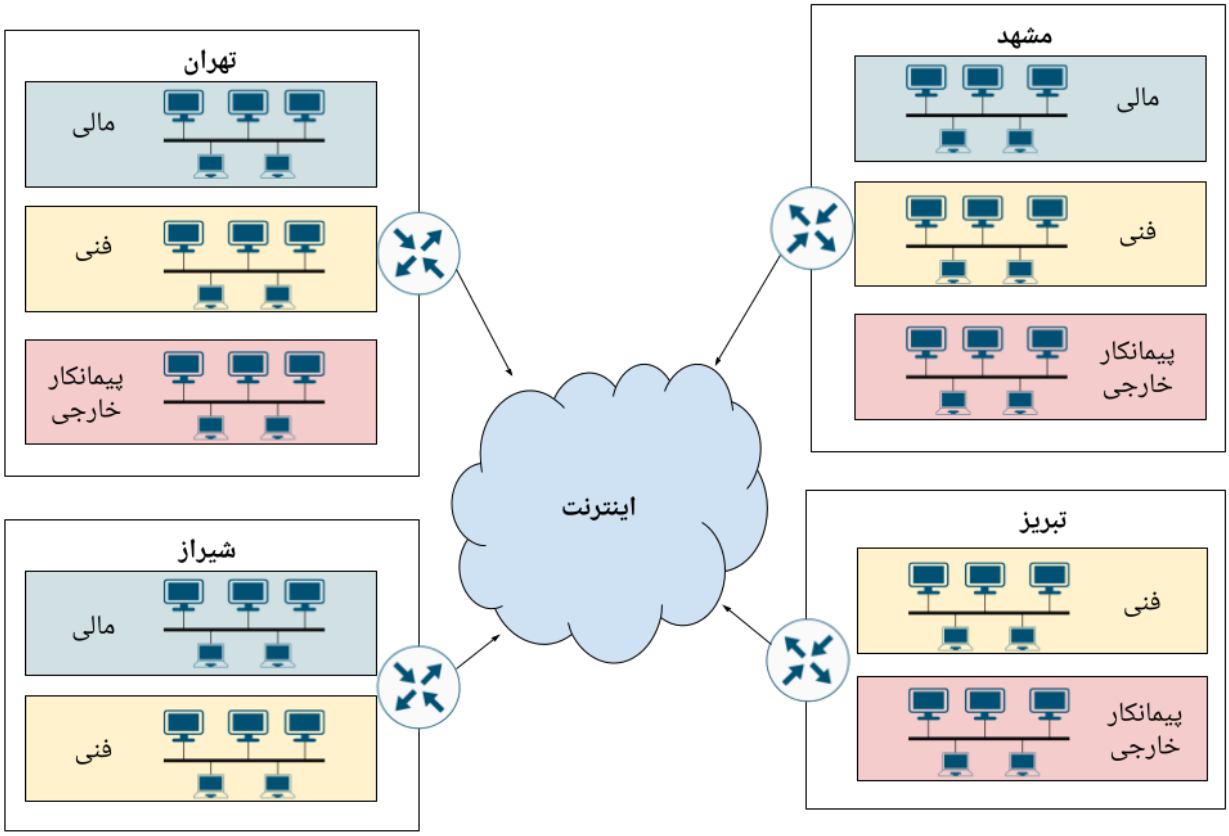
1. کاهش امنیت سیستم به علت اشتباهات مدیران شبکه
2. نیاز به دانش فنی بالا برای مدیران شبکه جهت تنظیم امن سیستم
3. صرف وقت و هزینه زیاد جهت ایجاد و نگهداری شبکه امن در سطح وسیع

از طرفی پیچیدگی همیشه باعث می‌شود یک سیستم کوچک بماند و سیستم های پیچیده به سادگی قادر نیستند بزرگ شوند.

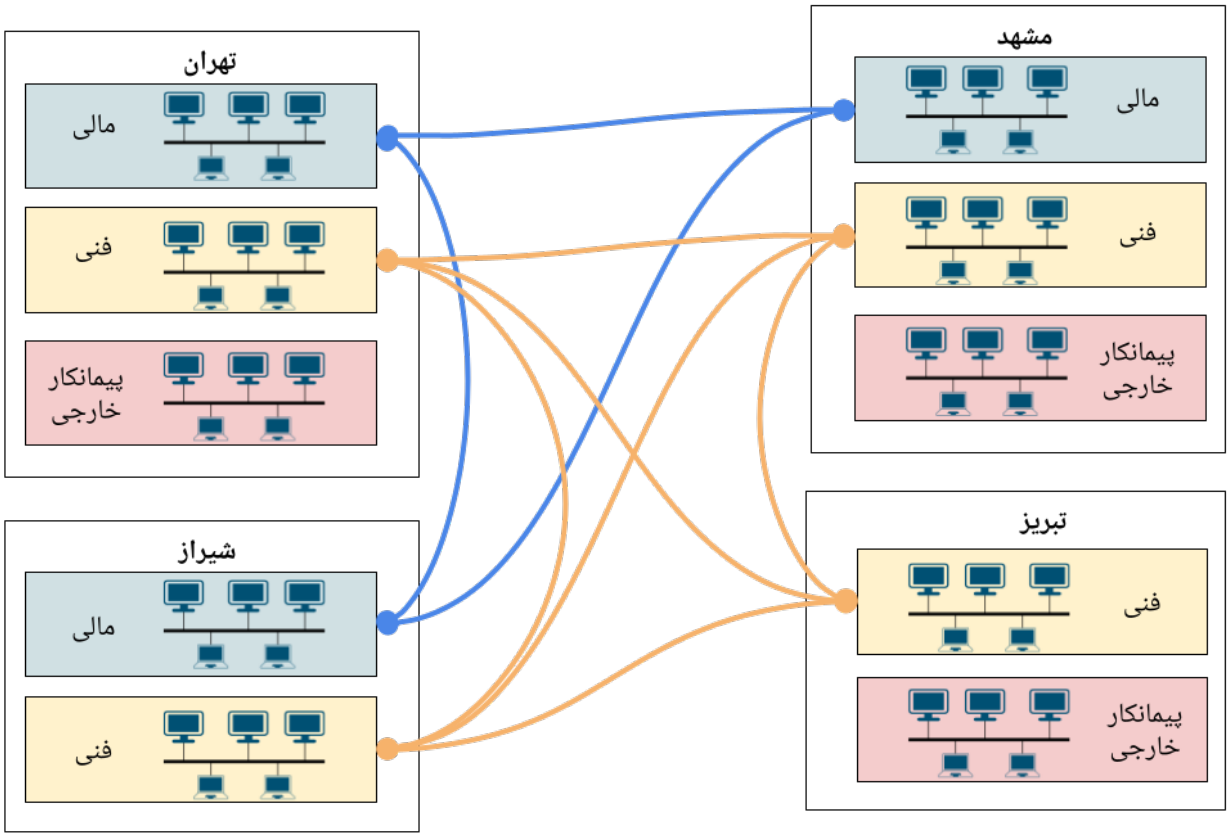
محصول اَمنِت با استفاده از تکنولوژی ها و پروتکلهای مختلف در بستر روتر سودار، امکان ایجاد شبکه های همپوشان مجزا را در سطح شبکه های مختلف سازمان ایجاد می نماید. این محصول سازمانها را قادر می سازد تا تمامی شبکه های خود را با کمترین پیچیدگی و به صورت امن به هم متصل سازند.

2.1 معرفی اَمنِت با یک نمونه شبکه

جهت معرفی محصول، سازمانی را در نظر بگیرید که در نقاط مختلف جغرافیایی شبکه ها و کاربران مختلفی دارد و میخواهد از طریق بستر هایی مانند اینترنت و اتصالات اختصاصی خود، ارتباط بین این مراکز را به صورت امن با هم برقرار سازد. همچنین کاربران این سازمان در چندین گروه مختلف قرار دارند که هر کدام از این گروهها به صورت مستقل می خواهند شبکه اختصاصی خود را داشته باشند. در ادامه با استفاده از این مثال به بررسی امکانات قسمتهای مختلف اَمنِت می پردازیم.



در شبکه بالا در نودهای اَمنِت که به صورت نود لبه شبکه تعریف شده است، هر کدام از شبکه های مالی، فنی و پیمانکار خارجی به یک پورت مجزای نود اَمنِت متصل می گردد. نودهای اَمنِت با اتصال به همدیگر به ازای هر گروه از کاربران یک شبکه Full-Mesh مجزا ایجاد می‌کنند.



در شکل بالا مشاهده فرمایید که برای کاربران شبکه مالی اتصالات Full Mesh بین سه شهر تهران، مشهد و شیراز برقرار شده است و همچنین به صورت مجزا ارتباط بین کاربران فنی در شهرهای مختلف، 6 تونل برقرار شده است. این تونلها به صورت اتوماتیک ایجاد می‌گردد و نیازی به تنظیمات کاربر جهت اتصالات تونلها نیست. فقط کافی است مدیر شبکه هر شهر، شبکه های محلی خود را تقسیم بندی نموده و هر کدام را در یک VNet مجزا قرار دهد.

1.2.1 تنظیم نودها و ایجاد شبکه نمونه

در اینجا بر اساس نمونه شبکه ارایه شده در بالا، به کارهایی که هر مدیر شبکه باید انجام دهد تا این شبکه تنظیم گردد اشاره میکنیم. در ابتدا کافی است تا به سیستم مدیریت امنیت شبکه که یک نرم افزار آفلاین است مراجعه کرده و سایت خود را تعریف نمایید و به ازای هر نود شبکه یک دانگل امنیتی دریافت نمایید و بعد از نصب روتر سودار اختصاصی اَمنِت بر روی هر دستگاه آن را روشن نمایید و سپس در هر نود تنظیمات زیر را انجام دهید:

1. ما به هر کدام از شبکه های بالا یک عدد اختصاص می دهیم و این VNet ها را در نرم افزار وب هر کدام از نودها تعریف میکنیم. توجه شود که تبریز شبکه کاربران مالی ندارد بنابراین نباید در این شهر این VNet تعریف گردد.
   - 201 برای شبکه لایه 2 فنی
   - 301 برای شبکه لایه 3 مالی
   - 302 برای شبکه لایه 3 پیمانکار خارجی
2. کارتهای شبکه متصل به شبکه های محلی را از لحاظ آدرس IP تنظیم کرده و آنها را در VNet مربوطه قرار میدهیم. توجه شود که کارتهای شبکه که قرار است در VNet لایه 2 قرار گیرد نیازی به تنظیم IP ندارد. همچنین کارتهای شبکه متصل به اینترنت را تنظیم میکنیم و همچنین کارتهای شبکه که قرار است به شبکه مدیریتی متصل گردد را نیز تنظیم میکنیم
3. کافی است در نودهای تبریز، مشهد و شیراز آدرس IP مربوط به نود تهران به عنوان هماهنگ کننده وارد گردد.

از این پس تمامی کارهای دیگر به صورت اتوماتیک انجام شده و تونلها متصل می گردد. می توانید برای بررسی مشکلات و دیدن وضعیت تونلها از طریق نرم افزار وب اقدام کنید. به همین راحتی کل شبکه طراحی شد و همه نودها به همدیگر متصل شدند. در ادامه به مفاهیم اصلی موجود در اَمنِت می پردازیم.

3.1 مفهوم VNet

در آمنِت به یک شبکه همپوشان مجزا از شبکه های دیگر VNet می‌گویند. در مثال بالا در کل شبکه، VNet های زیر را داریم:

- VNet فنی: این VNet برای اتصال تمامی قسمت های فنی در کل شبکه به همدیگر استفاده می‌شود
- Vnet مالی: این VNet برای اتصال تمامی قسمتهای مالی در شهرهای مختلف استفاده می‌گردد
- VNet پیمانکار خارجی: این VNet برای اتصال کاربران یک پیمانکار خارجی موجود در شهرهای مختلف که برای سازمان کار می‌کنند، به همدیگر مورد استفاده قرار می‌گیرد.

هر VNet دارای مشخصات زیر است:

1. می‌تواند به صورت لایه 2 یا لایه 3 شبکه های خصوصی پشتی را به همدیگر متصل نماید. که در صورت اتصال لایه 2 تمامی کاربران به عنوان یک شبکه بزرگ LAN به همدیگر متصل می‌گردند و می‌توانند در یک شبکه IP قرار گیرند. اتصال لایه 2 بین شبکه های مختلف اکثرا با استفاده از MPLS میباشد که در اینجا دیگر نیازی به این پروتکل نیست. اتصال لایه 2 در مراکز داده برای اتصال شبکه های مشتریان مورد استفاده قرار می گیرد.
2. برای ارتباط بین دو نود مجزا، از تونلهای امن Wireguard استفاده می شود که در قسمت دیگری به تفصیل در مورد Wireguard صحبت میشود. تنظیمات مربوط به تونلهای Wireguard اتوماتیک بوده و نیازی به ورود تنظیمات توسط مدیر سیستم نمی‌باشد.
3. برای مسیریابی پویا در ارتباطات لایه 3 از OSPF استفاده میگردد. این پروتکل درون تونلهای امن با همتایان خود در VNet مربوطه صحبت میکند. بنابراین کل این پروتکل در بیرون قابل مشاهده نیست و خطر امنیتی برای سیستم ایجاد نمیکند. تمامی تنظیمات این پروتکل به صورت اتوماتیک صورت می پذیرد و نیازی به انجام تنظیمات در این قسمت نیست.
4. برای اتصال شبکه های لایه 2 از VXLAN استفاده میگردد. ترافیک VXLAN از درون تونلهای امن عبور میکند و از بیرون قابل مشاهده نیست. تمامی تنظیمات این پروتکل به صورت اتوماتیک صورت می پذیرد.
5. هر کارت شبکه فیزیکی نود به یک VNet منصوب می گردد. در ابتدا تمامی کارتهای شبکه در VNet مدیریتی قرار دارند و باید آنها توسط مدیر محلی شبکه در VNet های مربوطه قرار گیرد.

در این محصول برای VNet ها می‌توان لایه اتصال را مشخص نمود یعنی به عنوان نمونه ما می توانیم تمامی اتصال‌های مربوط به کاربران فنی را به صورت لایه 2 معرفی نماییم. و مابقی VNet ها به صورت لایه 3 تعریف گردند.

برای سهولت استفاده و جلوگیری از خطای تایپی برای هر VNet متعلق به کاربر از یک شماره استفاده می‌گردد که بسته به نوع VNet در بازه های عددی مختلف قرار می‌گیرند.

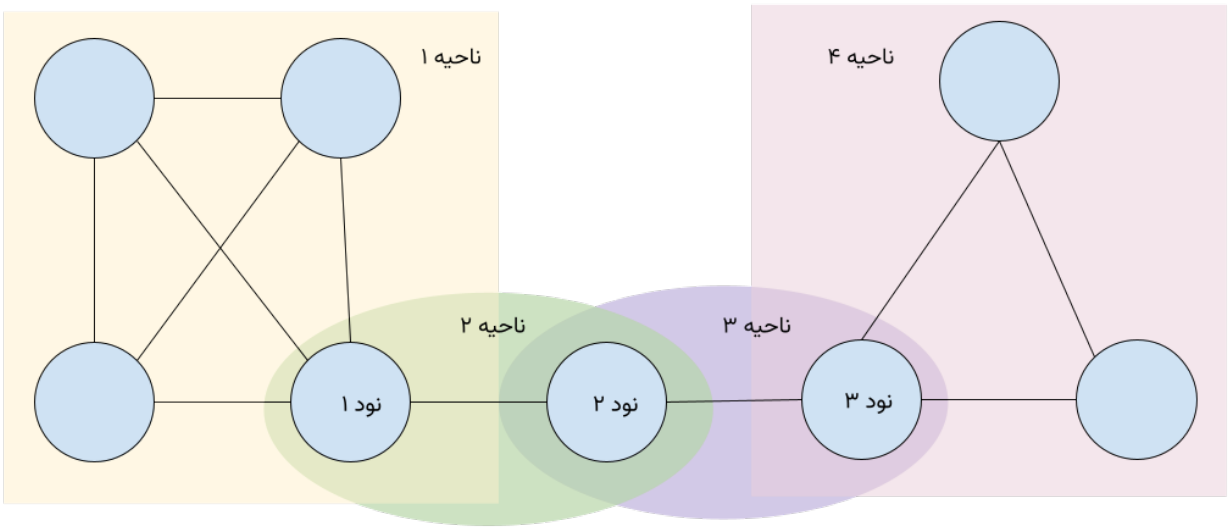
- 200-299: برای VNet های لایه 2 مورد استفاده قرار می‌گیرد و اگر شماره یک VNet را در این بازه وارد کردیم این VNet به صورت اتوماتیک لایه 2 معرفی می‌گردد.
- 300-399: برای VNet های لایه 3 مورد استفاده قرار می‌گیرد و اگر شماره یک VNet را در این بازه تعریف نماییم، این VNet به صورت اتوماتیک لایه 3 تعریف می‌گردد.
- 1-199 : برای کاربردهای داخلی مورد استفاده قرار میگیرد که شامل موارد زیر است:
  - VNet مدیریت شبکه که به صورت اتوماتیک در تمامی نودها ایجاد میشود و کاربر نمی تواند آن را تغییر دهد. این شبکه برای اتصال مدیران شبکه به نود ها و تنظیم هر نود مورد استفاده قرار می‌گیرد. این شبکه از شبکه های دیگر مجزا شده تا امنیت نودها افزایش یابد. تمامی ترافیک مربوط به مانیتورینگ نودها نیز از این شبکه منتقل می‌گردد.
  - VNet شبکه های عمومی که به صورت محلی در هر نود تعریف شده و سراسری نیست. این VNet ها برای امنیت درونی نودها ایجاد می‌گردد تا پروسه‌های عمومی نود را که نیاز به ارتباط با شبکه عمومی دارند، از دیگر پروسه ها مجزا نماید

VNet های سیستمی توسط نرم افزار و به صورت اتوماتیک ایجاد می‌گردد و هر VNet کاربرد خاص خود را داراست.

1.3.1 ناحیه بندی

اتصال Full Mesh تونلهای شبکه امکان خوبی است برای اینکه داده ها با کمترین تاخیر به مقصد برسند و همچنین سربار پردازشی در طول شبکه نداشته باشیم. اما از طرفی، ما همیشه قادر به اتصال Full Mesh نیستیم یا به دلایل مدیریتی یا سیاستهای ترافیکی نمی خواهیم این اتفاق بیافتد. همچنین اگر تعداد نودهای شبکه زیاد باشد تعداد تونلها زیاد شده و مشکلاتی را بوجود می آورد. برای حل این مشکل از ناحیه بندی نودها استفاده می شود.

هر نود میتواند در یک یا چند ناحیه قرار داشته باشد. هر نود با تمام نودهای همه نواحی که در آن قرار دارد اتصال Full Mesh برقرار میکند.



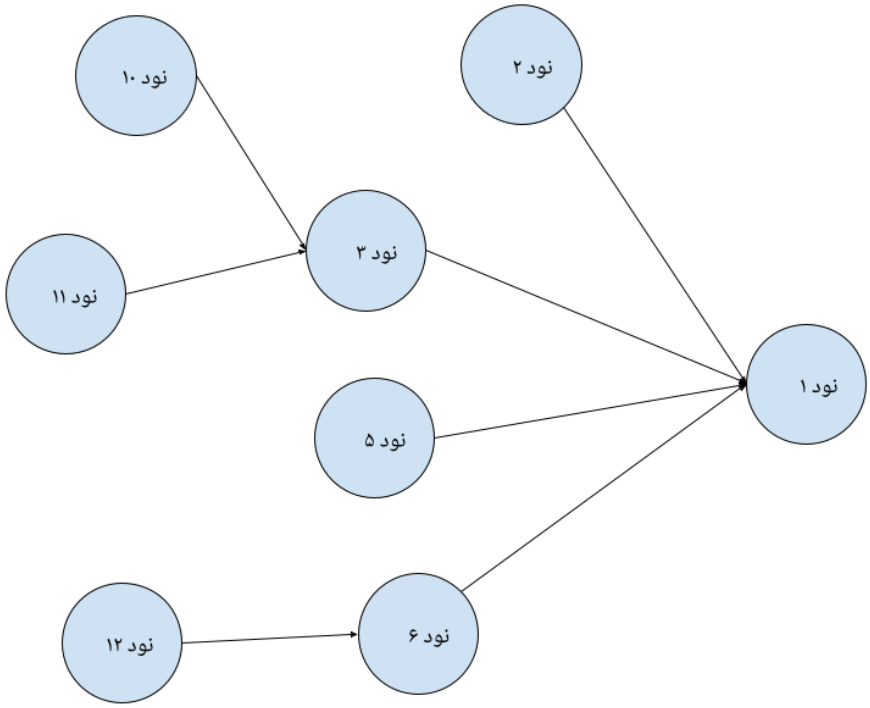
4.1 شناسایی و اتصال اتوماتیک - Control Plane

تا اینجا مشخص شد که در هر نود فقط کافی است یک نود هماهنگ کننده را مشخص نماییم، از آن پس تمامی نودها به هم متصل می‌شوند. توجه شود که این اتصال با اتصال مربوط به تونل داده ها متفاوت است و فقط برای هماهنگی با همدیگر و تبادل اطلاعات مربوط به VNet ها مورد استفاده قرار میگیرد. و سپس با استفاده از تنظیمات دریافتی، تونل‌ها بین نودها ایجاد می گردد.

این ارتباط برای همیشه برقرار می ماند و در صورت ایجاد اشکال در این ارتباط مشکلی برای تونلهای قبلی بوجود نمی آید، فقط تغییرات جدید را این نود نمی تواند دریافت نماید.

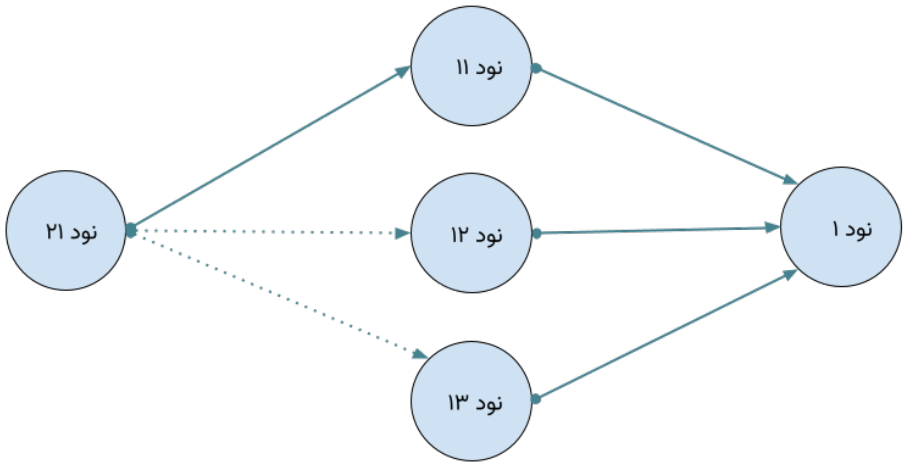
در اینجا قصد داریم تا به تشریح طریقه اتصال نودها و دریافت تنظیمات بپردازیم. در ابتدا یک نود را به عنوان نود اولیه در نظر گرفته و در همه نودهای دیگر این نود را به عنوان مرجع هماهنگی تنظیمات معرفی نمایید. اگر نودی وجود داشت که نمیتوانست به نود اولیه متصل شود شما میتوانید یک نود دیگر که در

شبکه وجود دارد را به عنوان مرجع معرفی کنید. توجه کنید که این قضیه می تواند به همین شکل ادامه یابد ولی نباید در مراجعات بین نودها حلقه رخ دهد. مثلا اگر نود1 به نود 2 اشاره میکند و نود 2 به نود 3، نود 3 نمیتواند به نود 1 اشاره کند.



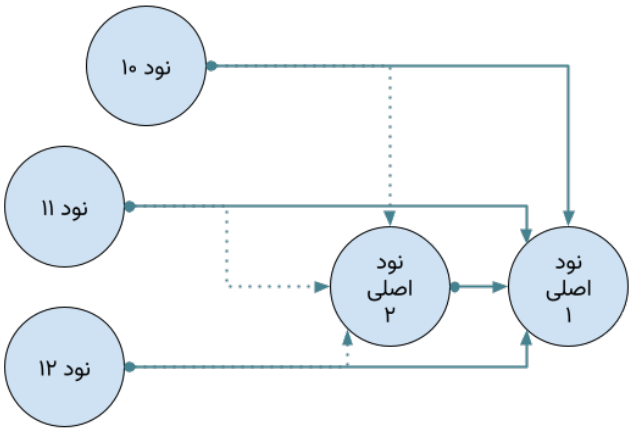
در شکل بالا نود1 به عنوان هماهنگ کننده اولیه قرار دارد که مابقی نودها به آن اشاره دارند و از طریق این نود هماهنگ می شوند و برخی نودها مثل نود 10 به نود 3 اشاره میکند که او نیز از طریق نود 1 هماهنگی ها را انجام میدهد.

برای تحمل پذیری بیشتر، می توان برای هر نود، چند اشاره گر مشخص نمود که به هر کدام از آنها که قادر بود متصل می شود. در این حالت به اولین نودی که توانست متصل شود، هماهنگی صورت می پذیرد و همزمان به چند نود متصل نمیشود. توجه شود که باز هم باید دقت شود که در هر کدام از این اتصالها که برقرار شد، حلقه بوجود نیاید.



در شکل بالا نود 21 به سه نود اشاره میکند که اتصالش با نود 11 برقرار شده است. بنابراین نیازی به اتصال با نودهای بعدی ندارد. ولی در صورت قطع شدن ارتباط با نود 11 می تواند به نود 12 یا 13 متصل شود.

پیشنهاد میشود که برای مقاوم سازی شبکه از ساختار زیر استفاده شود:

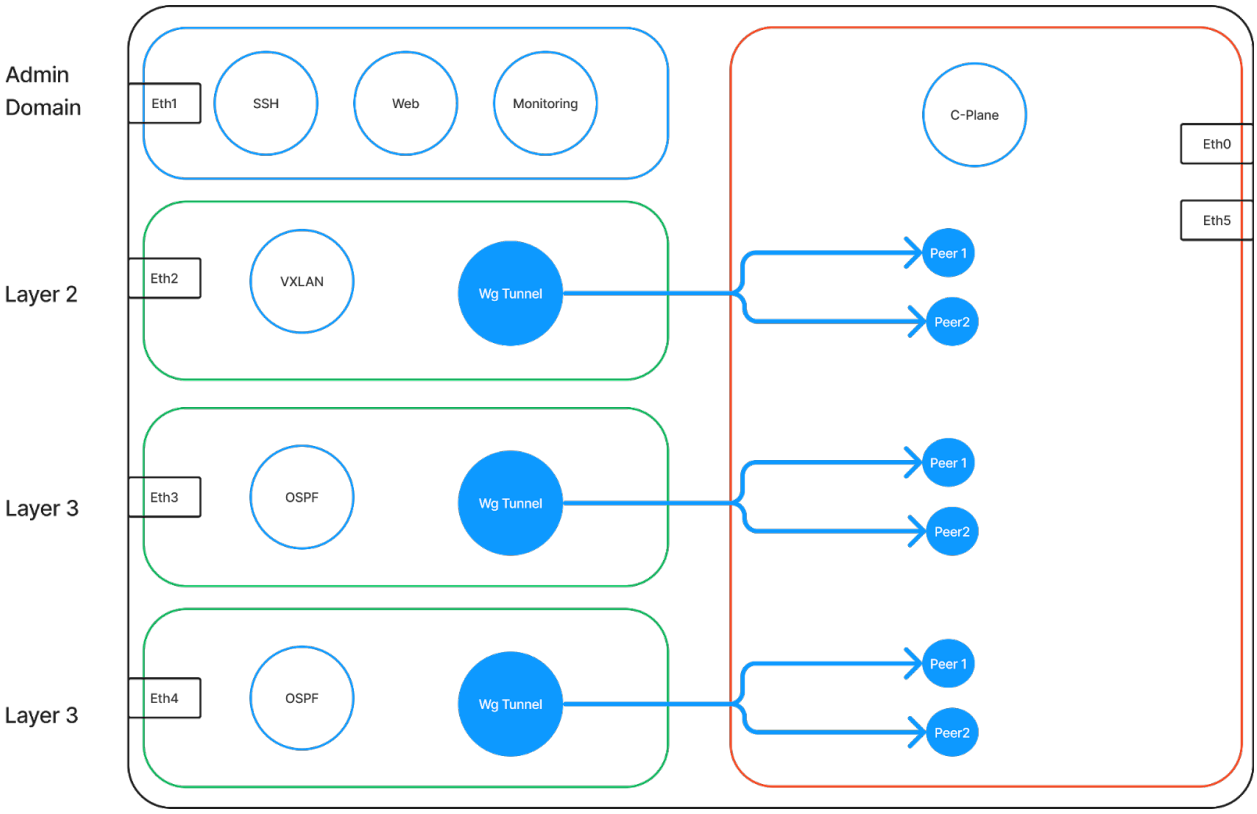


در این ساختار اگر نود 1 خاموش شود همه نودها از نود 2 استفاده میکنند و در صورت قطع شدن نود2 همه با استفاده از نود1 با همدیگر هماهنگ میشوند. در این حالت لینک بین نود1 و نود2 بسیار مهم می شود و حتما باید این لینک همیشه متصل باشد در غیر اینصورت دو جزیره مجزا خواهیم داشت.

البته چون ساختار اتصالات تونلها وابسته به اتصالات مربوط به Control Plane نیست، اگر در ابتدای کار نودها همدیگر را پیدا کرده و بتوانند تنظیمات را با هم همگام کنند، دیگر نیازی به این اتصالات نیست. و فقط زمانی که تغییری در تنظیمات VNet نودها رخ داد ما نیاز داریم که نودها با همدیگر هماهنگ شوند.

5.1 امنیت اَمنِت

در طراحی المانهای سیستم عامل امنت، قسمت مجزایی برای مدیریت سیستم در نظر گرفته شده است که تمامی سرویسهای مدیریتی در این فضا محبوس می شود. و این امر باعث میشود که سرویسهای درون روتر از شر دیگران در امان باشد. دسترسی به این سرویسها فقط از طریق شبکه اختصاصی مدیریتی امکان پذیر است.

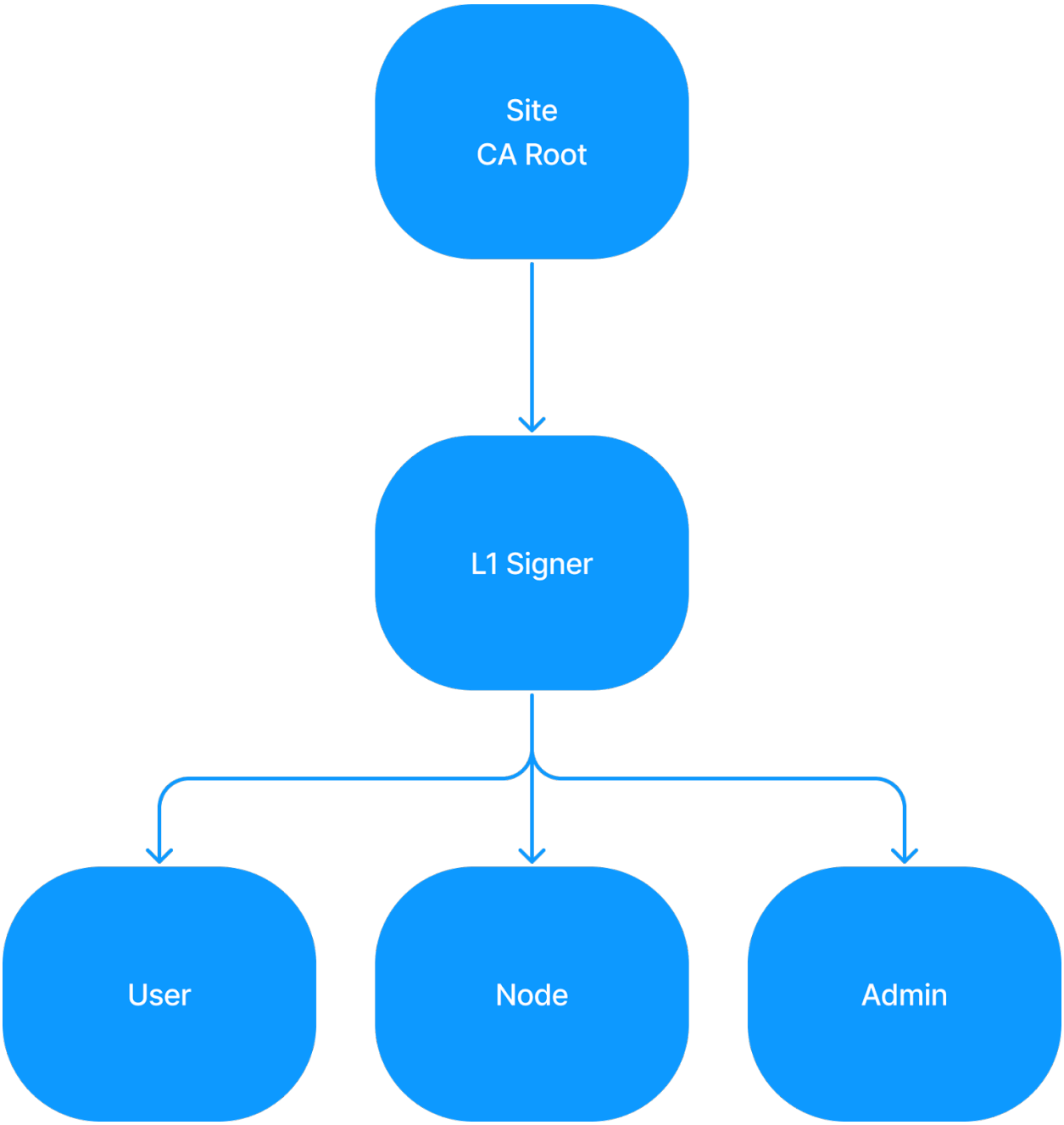


در طراحی اَمنِت، تمامی تنظیمات ریشه امنیتی در یک سیستم طراحی امنیتی Offline قرار گرفته شده است و مدیر محلی نودها نمی تواند تنظیمات امنیتی را تغییر دهد. در سیستم امنیتی مرکزی المانهای زیر ایجاد می گردد:

PKI 1.5.1

در نرم افزار مدیریت امنیتی مرکزی یک ساختار کلید عمومی ایجاد میگردد که برای امنیت اتصالات TLS مربوط به Control Plane بین نودها و همچنین برای امنیت ارتباط TLS سرویسهای وبی مورد استفاده قرار میگردد. قسمت های زیر در این نرم افزار ایجاد می گردد:

1. کلید ریشه PKI کل شبکه: قسمت عمومی این کلید توسط دانگل به تمامی نودها منتقل میگردد و همچنین برای Browser مدیر شبکه نیز باید مورد استفاده قرار گیرد.
2. کلید PKI هر نود: این کلید که توسط کلید ریشه (البته کلید مرحله 1) امضا می گردد به طور کامل(قسمت عمومی و قسمت خصوصی) درون دانگل قرار گرفته و به نودها منتقل میگردد.
3. کلید PKI هر کاربر: این کلید که توسط کلید ریشه (البته کلید مرحله 1) امضا می گردد به طور کامل(قسمت عمومی و قسمت خصوصی) درون دانگل قرار گرفته و مورد استفاده برنامه کاربر قرار می گیرد.



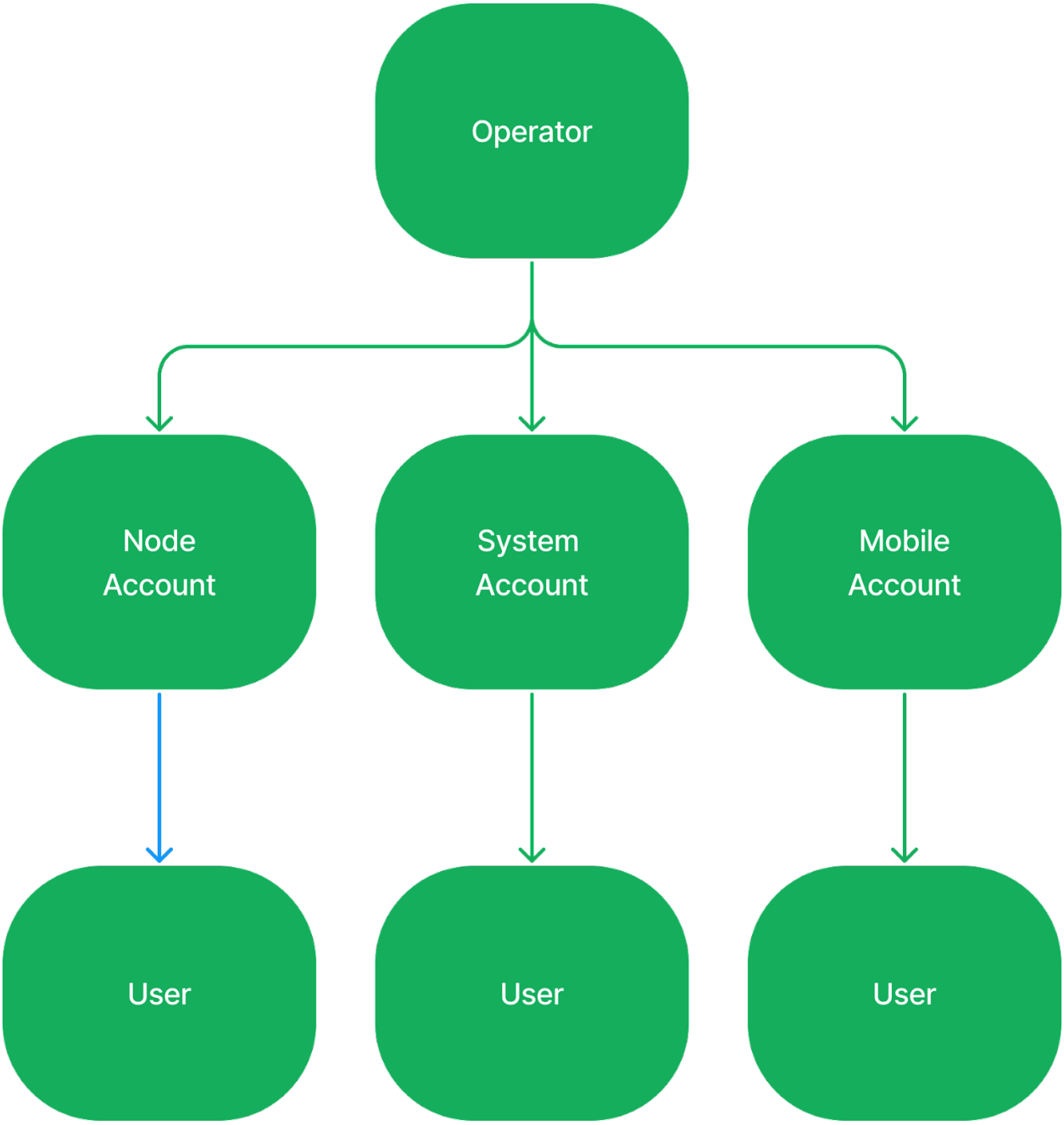
2.5.1 ساختار تایید هویت نودها

گرچه ارتباط بین نودها توسط TLS و به صورت امن صورت میگیرد ولی برای تایید هویت هر نود در زمان اتصال به نودهای هماهنگ کننده در Control Plane تایید هویت جداگانه ای انجام می شود که ساختاری شبیه به PKI دارد. تمامی کلیدها دارای دو قسمت خصوصی و عمومی هستند. قسمت خصوصی که باید مخفی بماند ولی قسمت عمومی دارای اطلاعات Authorization نیز می باشد.

این ساختار دارای المانهای زیر است:

1. کلید اصلی کل شبکه: این کلید که قسمت عمومی آن در تمامی نودها قرار میگیرد برای امضای کلید مرحله 1 مورد استفاده قرار میگیرد.

2. کلید های مرحله 1 : قسمت عمومی این کلید که توسط کلید اصلی امضا شده در تمامی نودها قرار می‌گیرد.
3. کلید تایید هویت: این کلید که توسط یک کلید مرحله 1 امضا میشود حاوی اطلاعات هویتی و محدودیتهای کاربر نیز میباشد. این کلید به ازای هر نود یا کاربر، جداگانه تولید می‌شود و هر دو قسمت عمومی و خصوصی آن به نود مربوطه یا کاربر منتقل می‌گردد.



WireGuard 3.5.1

WireGuard یک VPN بسیار ساده و در عین حال سریع و مدرن است که از رمزنگاری پیشرفته استفاده می کند. این پروتکل سریع‌تر، ساده‌تر، چابک‌تر و مفیدتر از IPsec می‌باشد. البته عملکرد بسیار بهتری نسبت به OpenVPN دارد. در حال حاضر این پروتکل به عنوان امن ترین، سهل‌ترین و ساده ترین راه حل VPN در صنعت می‌باشد.

هر تونل WireGuard برای اتصال فقط نیاز به داشتن موارد زیر است:

1. کلید عمومی و خصوصی نود محلی
2. کلید عمومی و آدرس IP طرف مقابل

مابقی موارد توسط WireGuard مدیریت می‌شود. WireGuard از ساختار رمزنگاری پیشرفته زیر استفاده میکند:

- پروتکل Noise
- الگوریتم های : Curve 25519 و ChaCha20 و Poly1305 و BLAKE2 و SipHash24 و HKDF

این انتخاب‌ها با دقت محافظه‌کارانه و منطقی انجام شده و توسط رمزنگاران بررسی شده است.

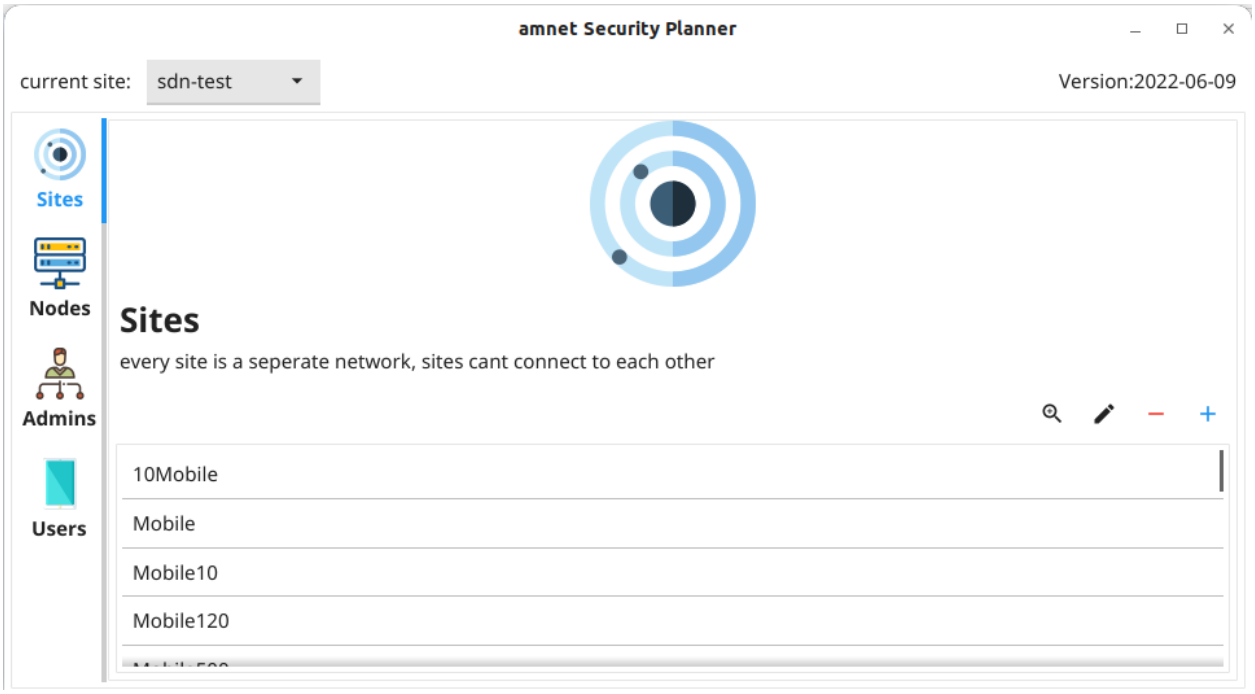
6.1 معرفی

این Software Defined Network یا SDN شبکه هایی هستند که به جایی تنظیم دستی تک تک دستگاه های شبکه توسط ادمین ، به صورت نرم افزاری تنظیم می شوند حال این تنظیم خودکار و نرم افزاری می تواند سطوح و جنبه های متفاوتی را در بگیرد. محصول اَمنت نیز بدین صورت طراحی شده است که یکسری شبکه های امن تفکیک شده به صورت خودکار برای هر سازمان فراهم کند . در این شبکه ها تنظیم دستی به صورت کاملا حداقلی و تنها در حد تعریف ip اینترفیس ها و مشخص کردن vnet هایی که هر روتر در آن قرار دارد می باشد و کلیه تنظیمات و بقراری تونل ها و تشکیل vnet ها توسط control plane انجام می گردد . توسعه و افزایش نود های شبکه به راحتی و بسیار سریع انجام می گیرد کافی است ip ها تنظیم گردد و یک نود فعال را به عنوان معرف شبکه مشخص کنیم از آن پس از طریق همان معرف کل نود های شبکه را خواهد شناخت و تونل ها و vnet ها برای نود جدید خودکار وصل می گردد. علاوه بر نود های شبکه ، کاربران desktop و موبایل ها هم در این شبکه قرار می گیرند و ارتباط امن در vnet خود خواهند داشت .

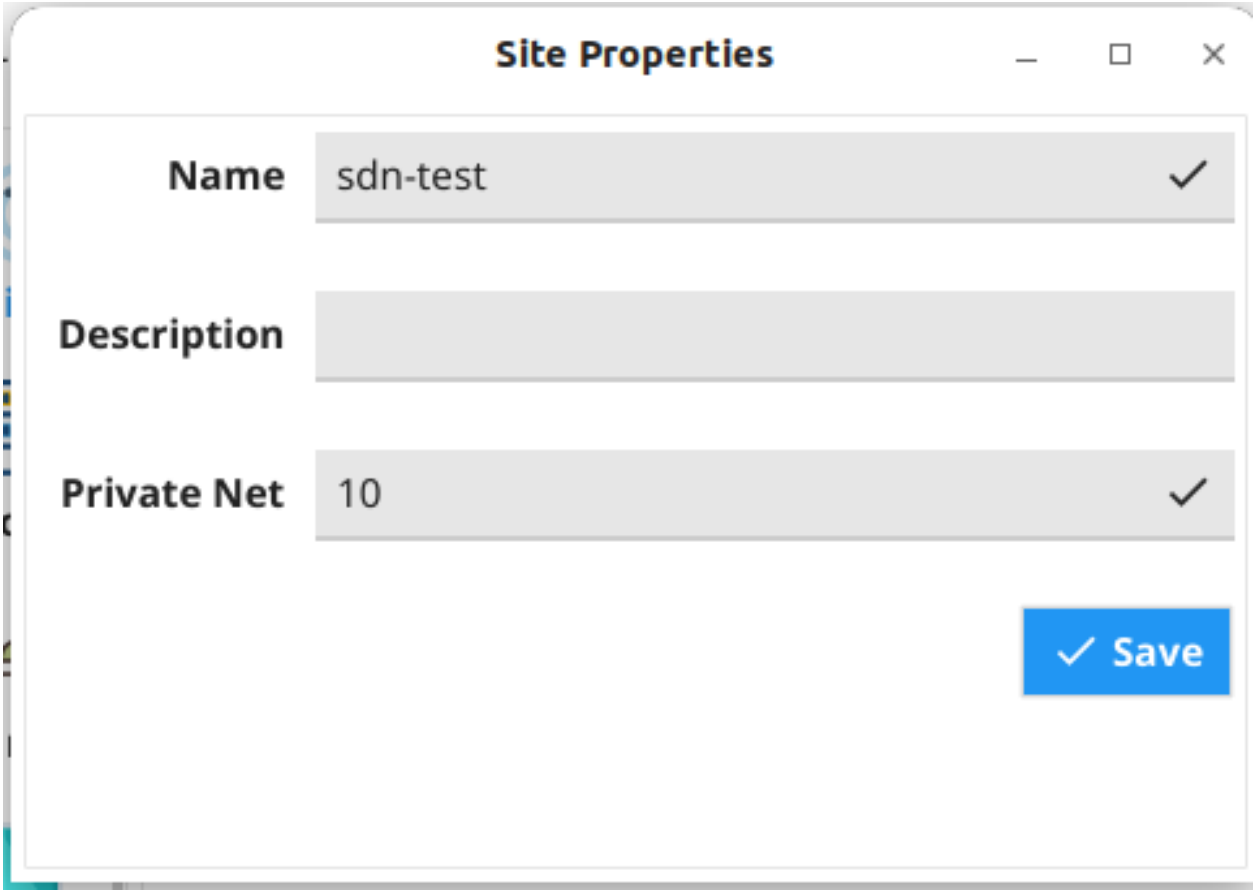
تنظیمات امنیتی و ایجاد قفل امنیتی برای نود ها و کاربران desktop و موبایلی در نرم افزار security planner انجام می گیرد . در این قفل کلید ها و certificate های لازم برای هر نود قرار دارد که نود توسط آن می توان به شبکه اَمنت متصل شود . برای موبایل ها این قفل یک فایل است که به موبایل انتقال داده می شود.

security planner 7.1

پس از اجرای نرم افزار محیطی به شکل زیر خواهید داشت که در آن لیست سایت های اضافه شده را می بینید . اگر سایتی اضافه نکرده باشید این جدول برای شما خالی است :



ابتدا باید یک سایت ایجدا کنیم و یک نام و یک prefix برای private ip هایی که به نود ها اختصاص داده می شود انتخاب کنیم :



با تنظیم prefix به 10 :
آدرس private ip ادمین های این سایت از 10.1.0.1 تا 10.3.255.255 خواهد بود یعنی شما می توانید بیش از 250,000 کاربر ادمین در این سایت

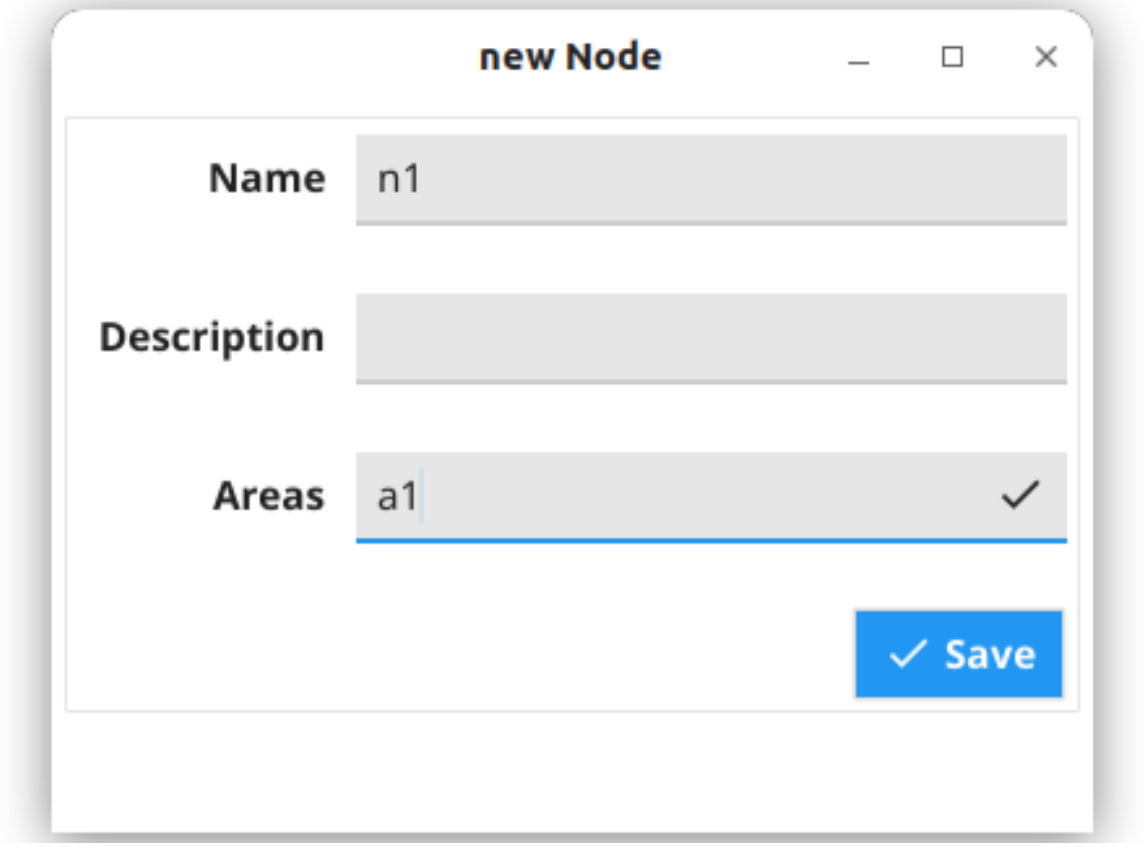
تعریف کنید .
آدرس private ip روتر های این سایت از 10.4.0.1 تا 10.7.255.255 خواهد بود یعنی شما می توانید بیش از 250,000 روتر در این سایت تعریف کنید .
آدرس private ip کاربر های این سایت از 10.8.0.1 تا 10.255.255.255 خواهد بود یعنی شما می توانید بیش از 16,000,000 کاربر (موبایل و لینوکس و ویندوز)در این سایت تعریف کنید .

توجه

این private ip ها به طور خودکار اختصاص می یابد .
ip اختصاص داده شده در کل سایت منحصربفرد است و برای هر المان شبکه ثابت و تغییر ناپذیر خواهد بود .

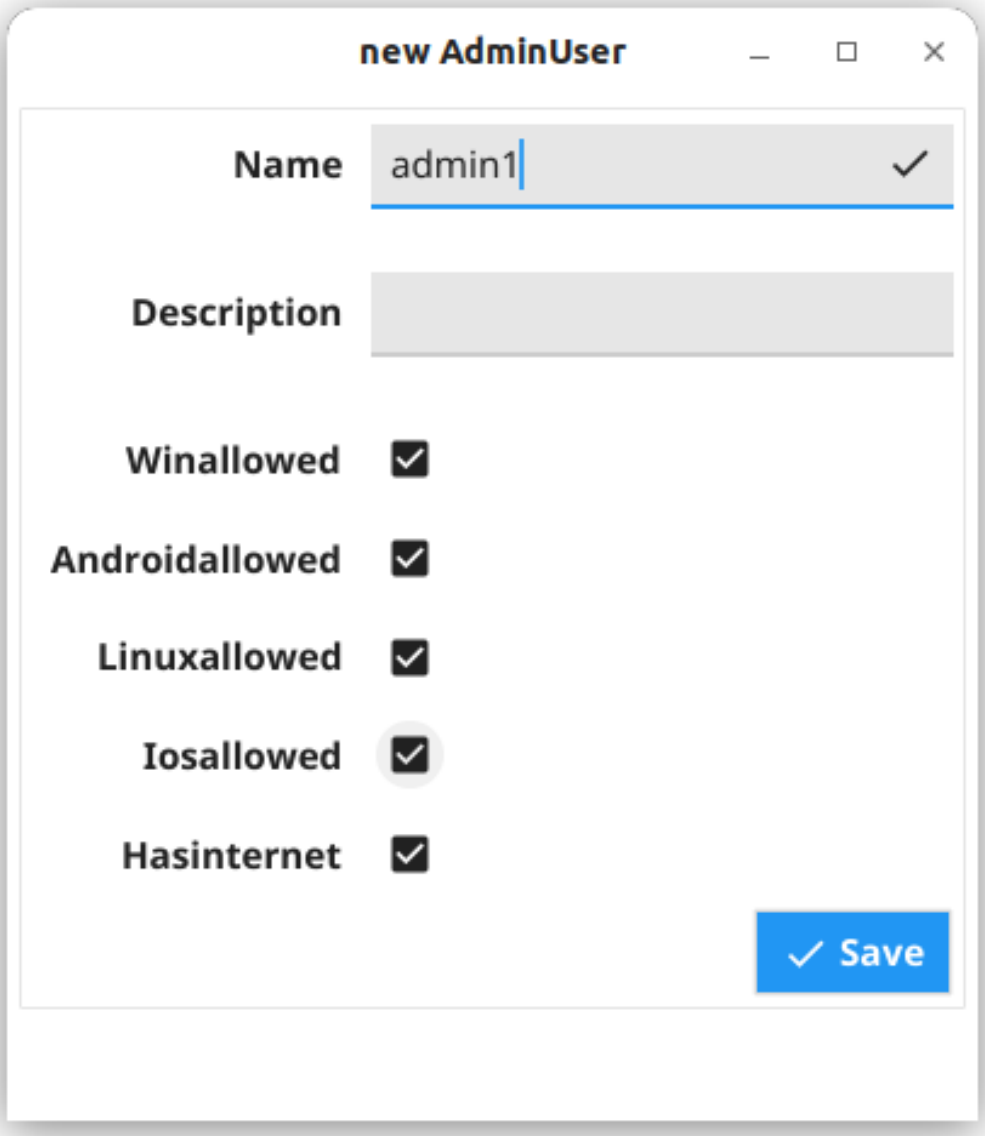
1.7.1 اضافه کردن روتر(نود)

برای اضافه کردن یک نود، یک نام (hostname) و یک area برای روتر مشخص می کنیم :



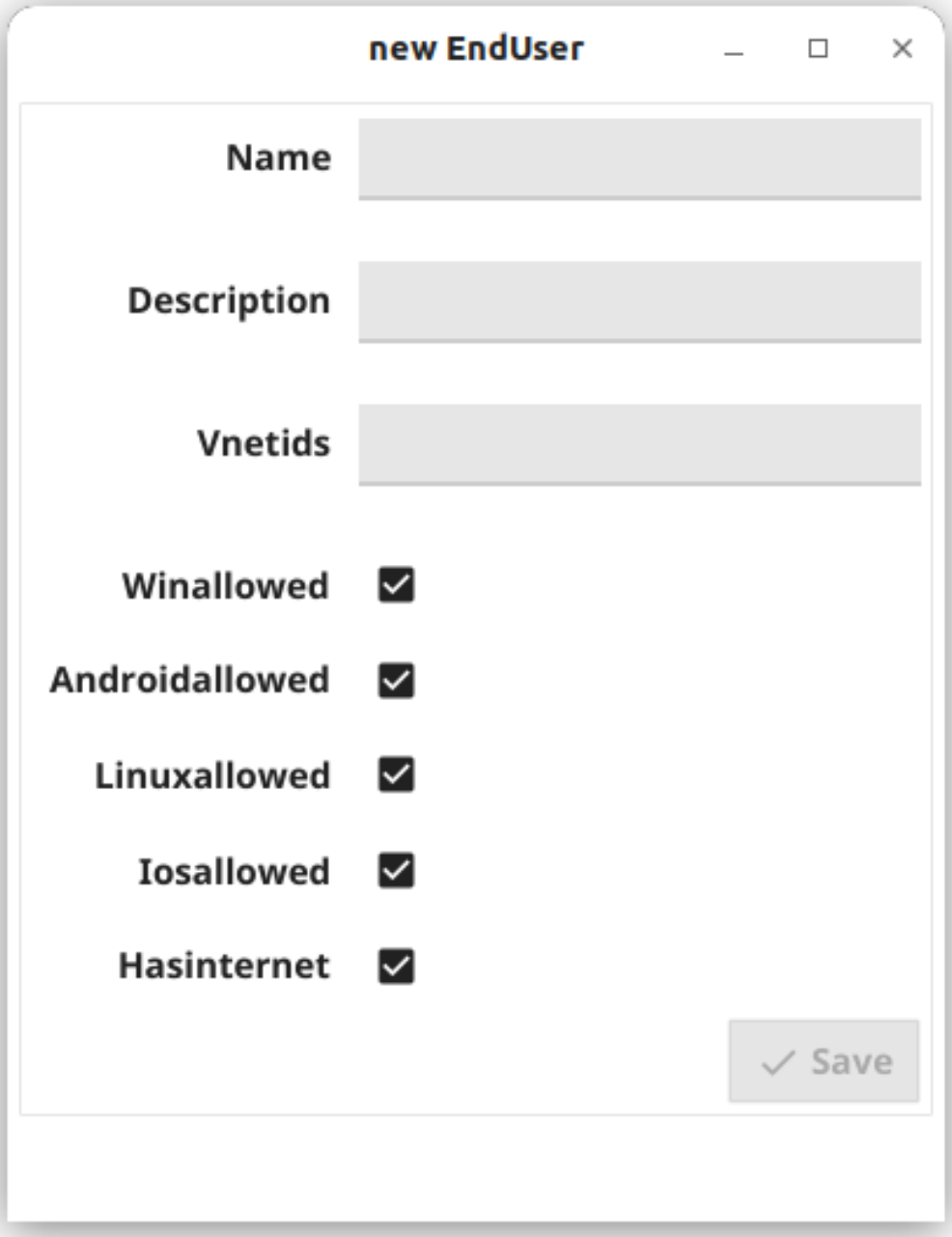
2.7.1 اضافه کردن ادمین

برای اضافه کردن یک ادمین، یک نام مشخص می کنیم :



3.7.1 اضافه کردن کاربر

برای اضافه کردن یک کاربر، یک نام مشخص می کنیم :



در نهایت برای روتر ها و ادیمن ها و کاربران desktopی قفل سخت افزاری که یک دانگل usb است توسط secrity planner تولید می شود و برای کاربران موبایلی هم فایل دانگل تولید می گردد .

8.1 Amnet Entry Point (نقطه اتصال به Amnet)

هر روتر برای وصل شدن به شبکه Amnet باید یک نقطه اتصال داشته باشد تا بتواند اطلاعات نود های موجود را بدست آورد و تونل ها و ارتباطات خود را شکل دهد .

توجه

1. هر نودی که در شبکه Amnet قرار داشته باشد می تواند نقطه اتصال نود های دیگر باشد
2. هر نود می تواند چندین نقطه اتصال داشته باشد که در آن واحد فقط با یکی از آن ها در ارتباط خواهد بود .
3. در تعریف نقاط اتصال دقت شود که نباید loop رخ دهد و ارتباطات به شکل درختی تعریف گردد .

9.1 Vnet

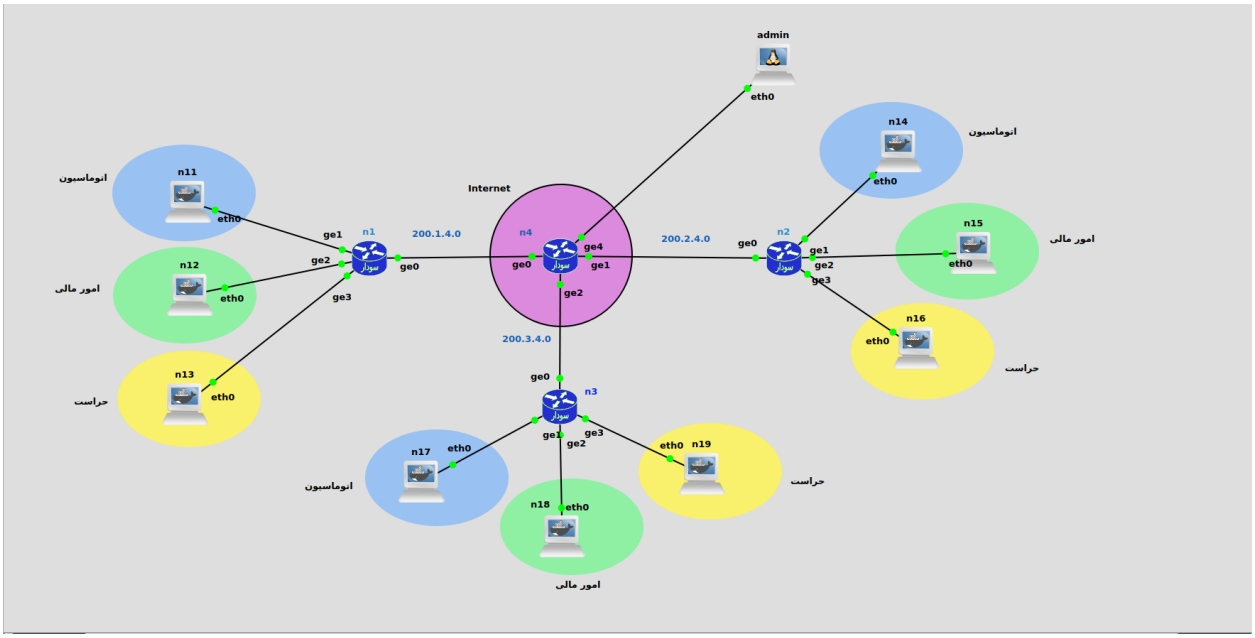
با برقراری تونل بین روتر هایی که در شبکه Amnet قرار دارند می توان از یک تونل چندین شبکه خصوصی مجزا را عبور داد که به هر یک از این شبکه ها vnet می گوییم . مشخصه هر vnet یک عدد است که برای شبکه های لایه3 این عدد بین 300 تا 399 و برای شبکه های لایه 2 بین 200 تا 299 میتواند تنظیم گردد . روال کار بدین شکل است که ادمین در هر روتر ضمن تنظیم Entry Point در روتر ، vnet هایی که این روتر قرار است داشته باشد را نیز مشخص می کند سپس این اطلاعات توسط control plane بین روترها تبادل می گردد و تونل ها و شبکه های خصوصی مد نظر اضافه می گردد و ارتباطات شبکه خصوصی در کل سایت شکل می گیرید .

توجه

1. هر نودی که در شبکه Amnet حذف یا اضافه شود بلافاصله اطلاعات آن بین همه نود ها توزیع می شود و تونل ها لازم حذف یا می گردد
2. هر نودی که vnetی را حذف یا اضافه شود بلافاصله اطلاعات آن بین همه نود ها توزیع می شود و تونل های لازم حذف یا اضافه می گردد .
3. در تعریف نقاط اتصال دقت شود که نباید loop رخ دهد و ارتباطات به شکل درختی تعریف گردد .

10.1 تنظیم روتر ها

فرض کنید ما سایتی شبیه شکل زیر داریم که شامل سه شعبه مختلف می باشد و قصد داریم سه شبکه مجزا از یکدیگر امور مالی و اتوماسیون و حراست را به هم متصل کنیم به نحوی که شبکه امور مالی کلیه شعب در یک شبکه خصوصی جداگانه از شبکه اتوماسیون و حراست قرار داشته باشد و همچنین شبکه حراست و اتوماسیون شعب جدا از دیگر بخش ها با هم در ارتباط باشند :

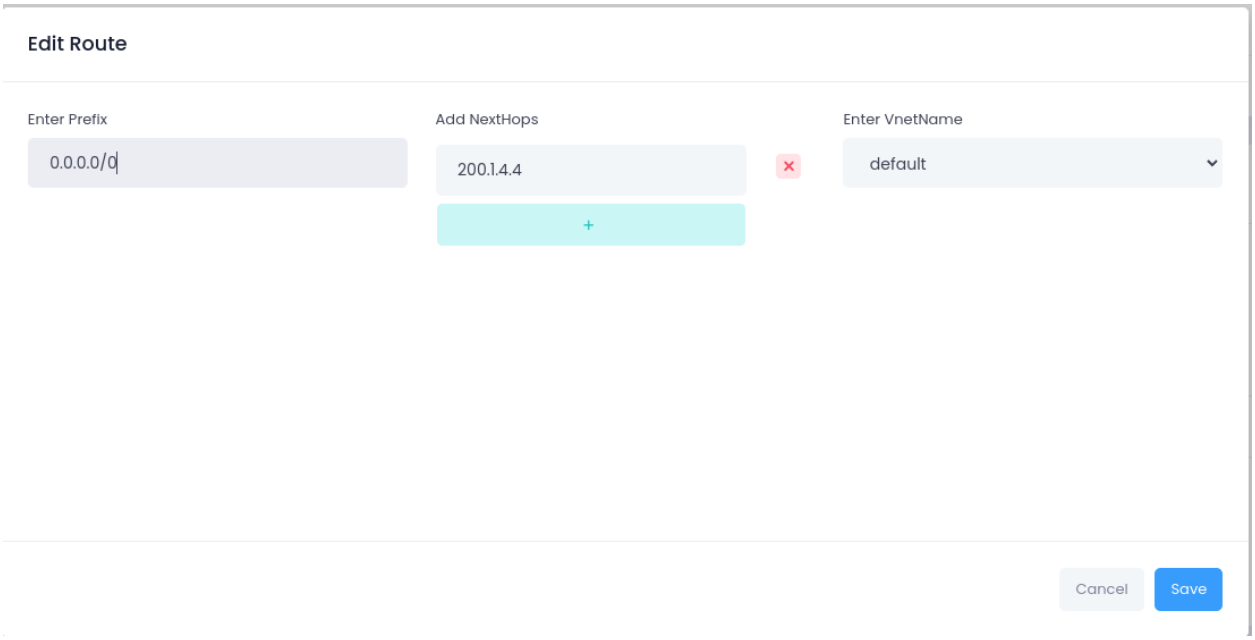


در این سناریو ما 3 vnet تعریف می کنیم که دو vnet لایه 3 و با شماره های 300 و 310 و یک vnet لایه 2 با شماره 200 است . این شماره vnet ها به دلخواه و با توجه به ارتباط لایه2 یا 3 مورد نظر شما می تواند تغییر کند .
ابتدا باید به webconfig روتر ها وصل شویم و به شکل زیر vnet ها و همچنین Entry Point را در روتر اضافه نماییم .

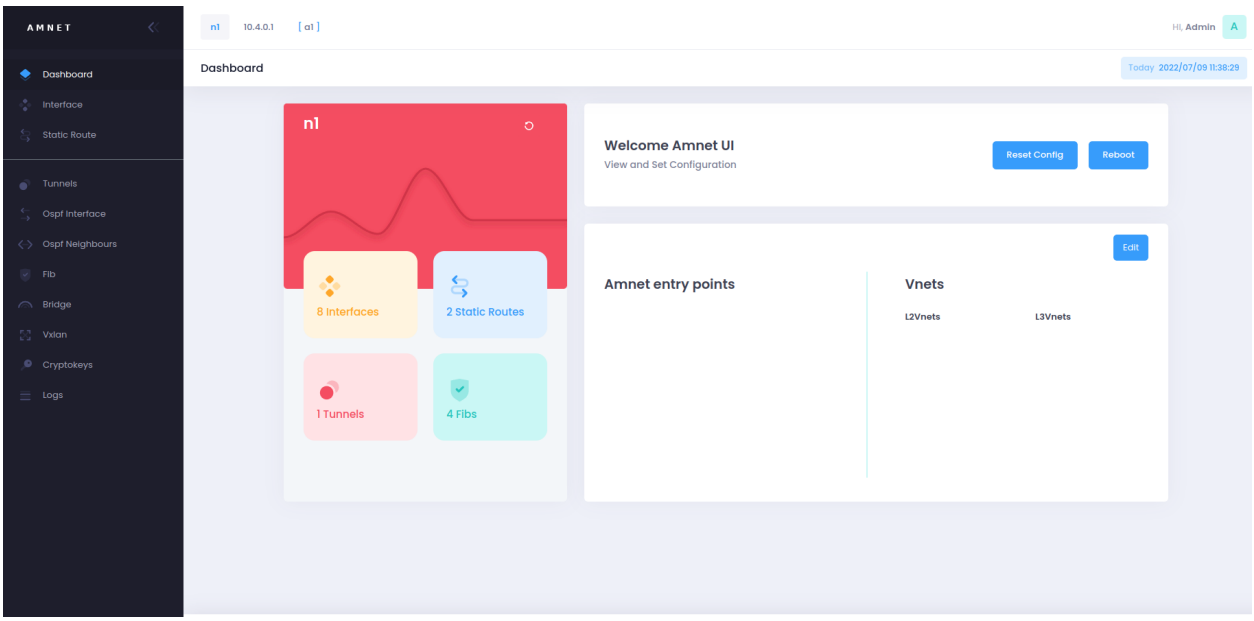
توجه

1. به صورت پیش فرض آدرس ip اولین اینترفیس در سودار برابر با 192.168.1.55/24 است .
2. باید قفل سخت افزاری به روتر وصل باشد تا بتوانید به webconfig وصل شوید .
3. برای وصل شدن به webconfig باید به ip ای وصل شوید که در vnet مربوط به admin(default) قرار داشته باشد یا اینکه با یک کاربر admin به روتر تونل بزنید و سپس private ip روتر را برای وصل شدن در مرورگر وارد نمایید.

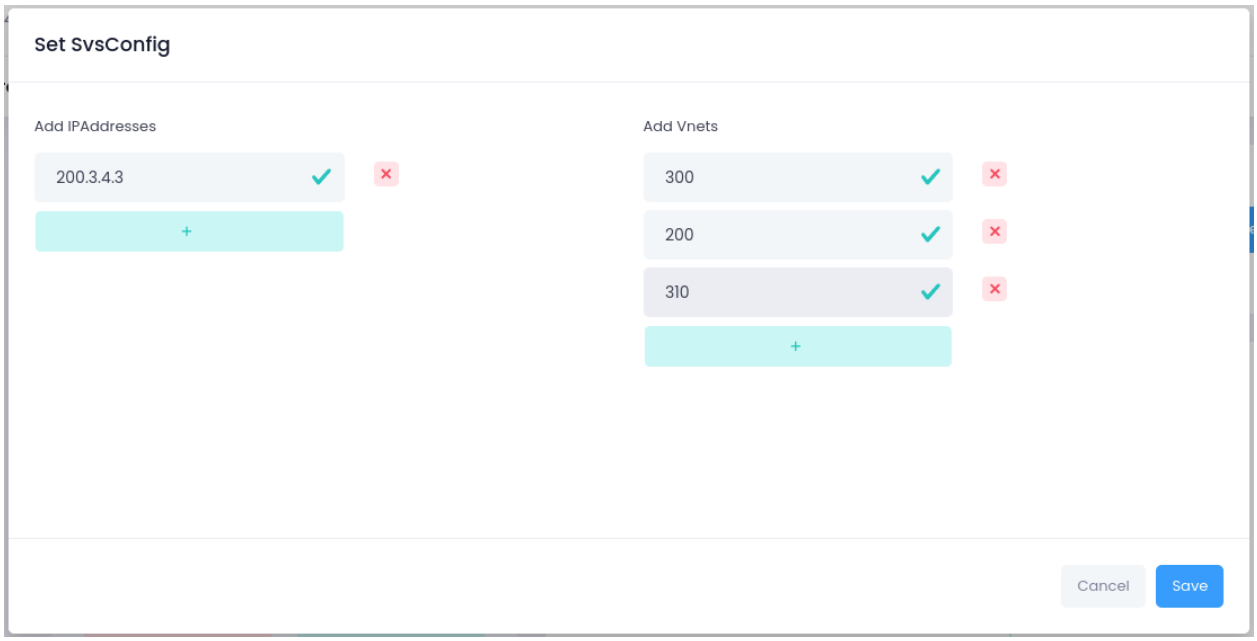
طبق سناریوی فوق به اینترفیس های ge0 در روترها آدرس های 200.1.4.1/24 و 200.2.4.2/24 و 200.3.4.3/24 را اختصاص می دهیم و static route را نیز اضافه می کنیم . نحوه اضافه کردن static route در n1 برای نمونه در شکل زیر آورده شده است :



پس از اتصال به نود شما دشبورد نود را مشاهده می کنید که در آن اطلاعات وضعیت جاری را نشان می دهد. در نوار بالای نام روتر و همچنین private ip و area روتر مشخص شده است . در پنل های دیگر تعداد اینترفیس ها و تونل ها و روت ها و اطلاعاتی از vnet های جاری روتر قابل مشاهده است :

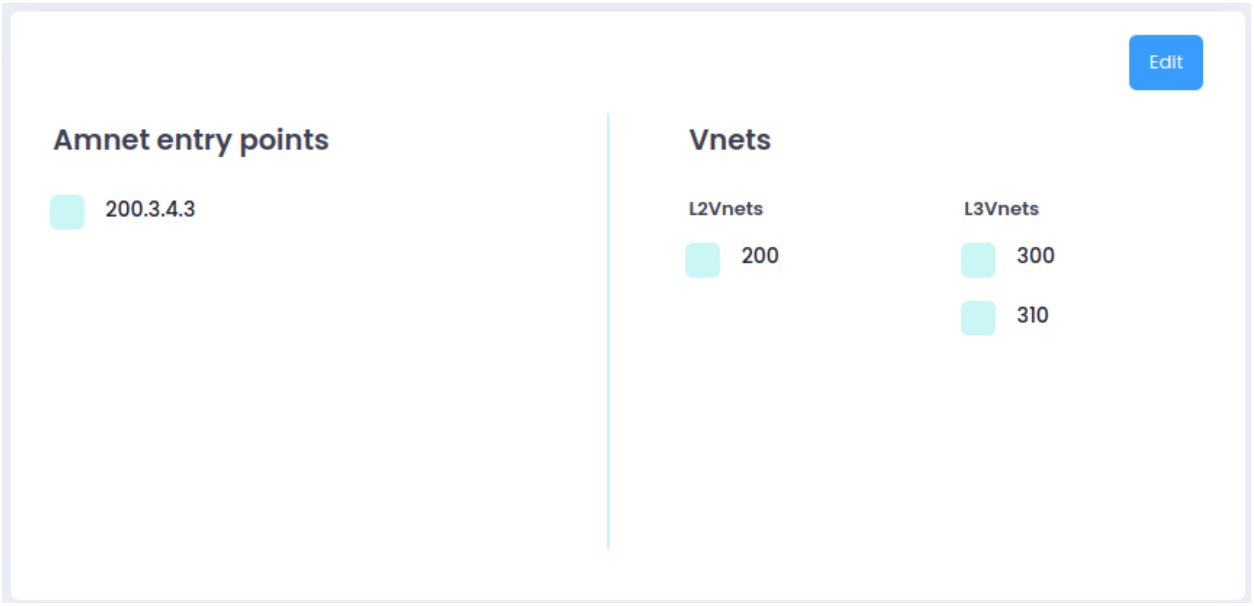


به شکل زیر vnet ها و Entry Point را در روتر n1 مشخص مشخص می کنیم :



توجه

در این سناریو در نود های n2 ، n1 نود n3 را به عنوان Entry Point تعریف کرده ایم و آدرس 200.3.4.3 را برای آن تنظیم کرده ایم و چون نود n3 با دو نود n2 ، n1 در ارتباط است و حداقل یک نود را در شبکه amnet می شناسد دیگر لازم نسیت در n3 یک Entry Point تعریف شود و اگر تنظیم شود loop اتفاق می افتد و رفتار شبکه ناپایدار می شود .



تنظیمات در **n2**

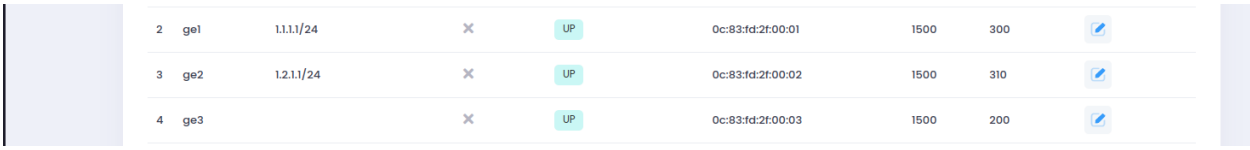
تنظیمات در **n3**

نکته

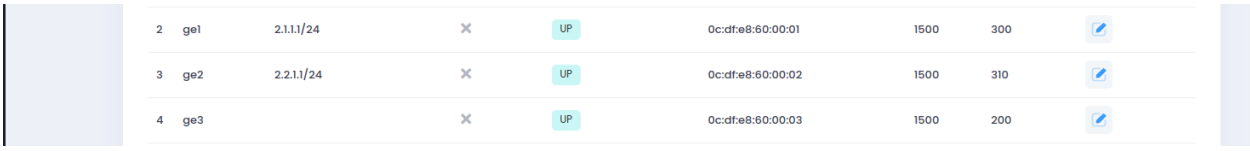
روتر های در هر Area به تمامی روتر های موجود در Area که vnet مشترکی با هم دارند تونل می زنند . در واقع در هر Area به ازای هر vnet تونل ها به صورت fullmesh بین روتر ها ایجاد می گردد .

11.1 تنظیم اینترفیس های Private

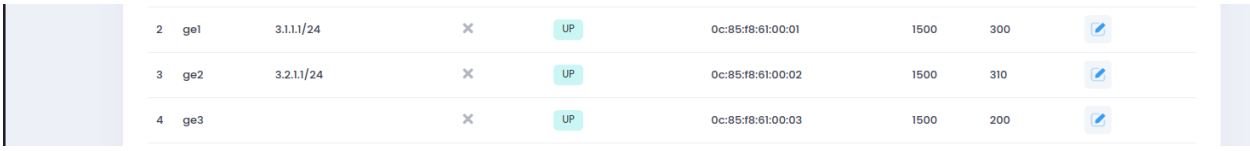
در بخش اینترفیس می توان تنظیمات IP و vnet اینترفیس ها را انجام داد . در این سناریو ما کلیه اینترفیس های ge1 را در vnet شماره 300 و اینترفیس های ge2 را در vnet شماره 310 و اینترفیس های ge3 را در vnet شماره 200 قرار داده ایم. بنابراین تنظیمات به شکل زیر خواهد بود :



در n1



در n2

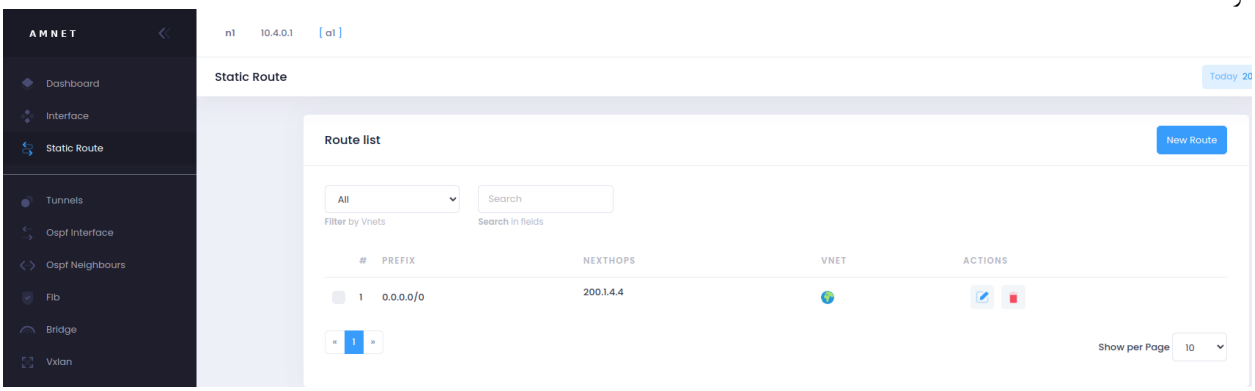


در n3

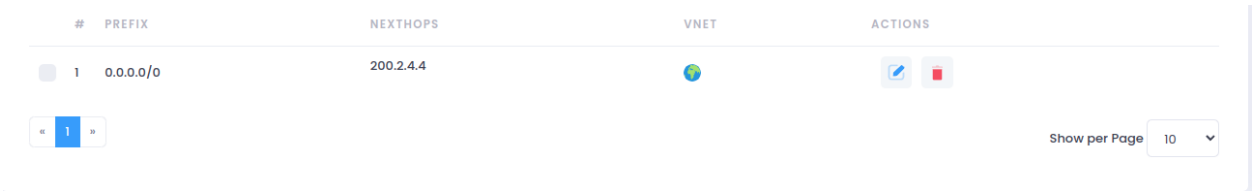
12.1 تنظیم static route

برای اینکه روتر ها در Vnet Public با هم در ارتباط باشند لازم است Static route اضافه کنیم . در روتر ها یک default route در Public اضافه کرده ایم :

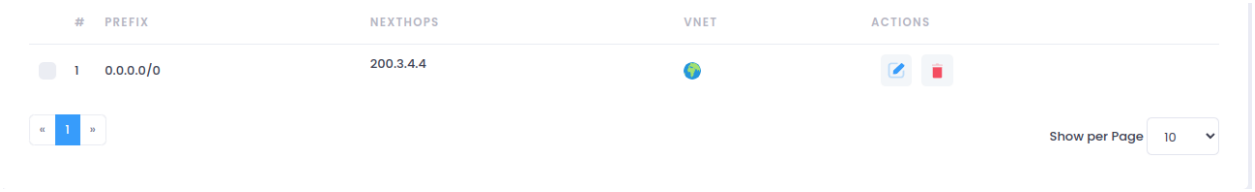
در n1



در n2



در n3



13.1 تنظیم اینترفیس Public

در آخرین مرحله نیز اینترفیس ge0 را در vnet Public قرار می دهیم .

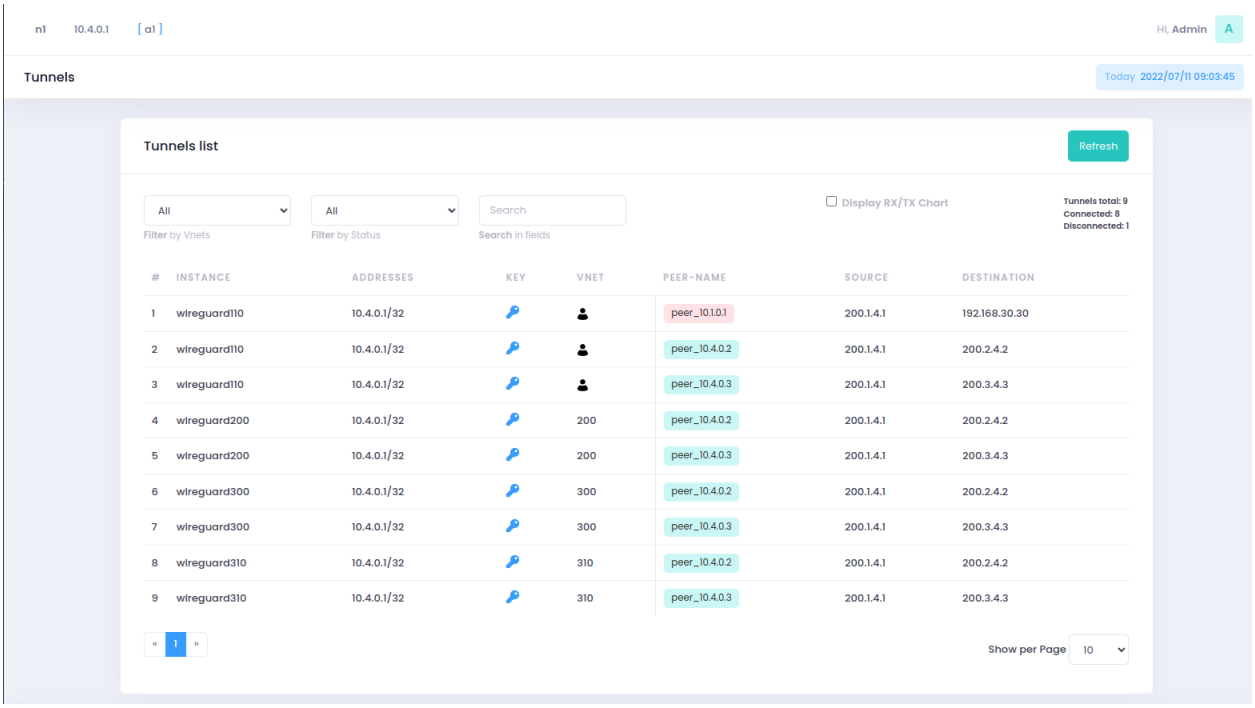
نکته

1. Public vnet به صورت پیش فرض در روتر های شبکه Amnet اضافه می گردد.
2. لازمه اینکه روتر بتواند با control Plane کارکند و همچنین تونل ها بین روترها برقرار شود این است که روتر حداقل یک اینترفیس در vnet با نام **Public** داشته باشد .

14.1 مشاهده تونل ها

در بخش Tunnels می توان وضعیت تونل ها مشاهده نمود . تونل ها در vnet های مختلف و با peer های متفاوت در جدول قرار دارند . تونل های سبز رنگ وصل و تونل های قرمز رنگ قطع هستند.

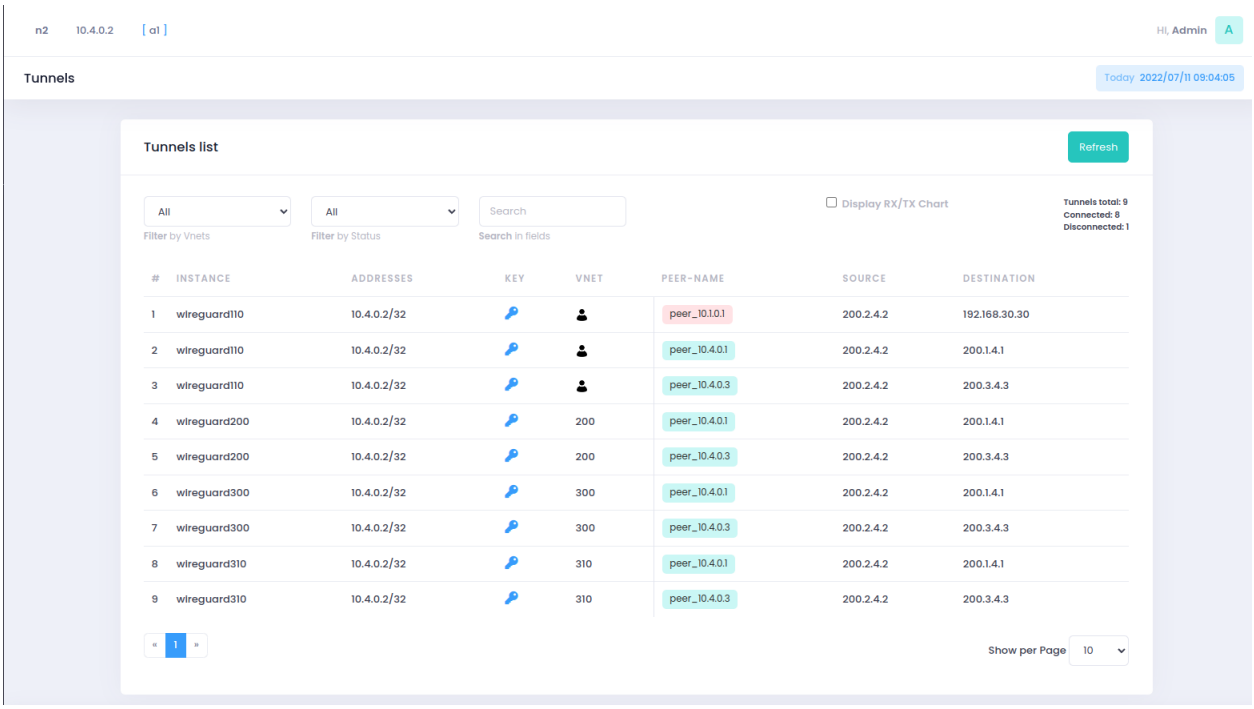
در n1



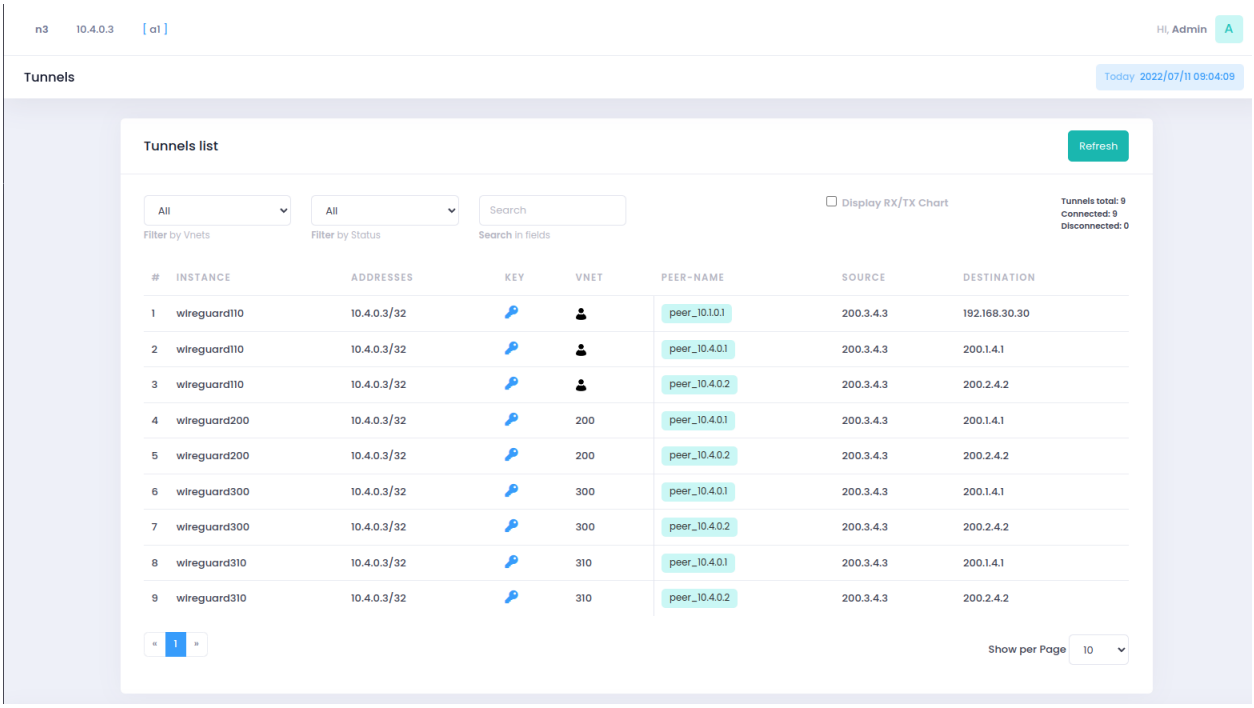
توجه

تونل به peer__10.1.0.1 قطع است . این تونل مربوط به کاربر ادمین است که یکبار به نود وصل شده است و اکنون قطع است .

در n2

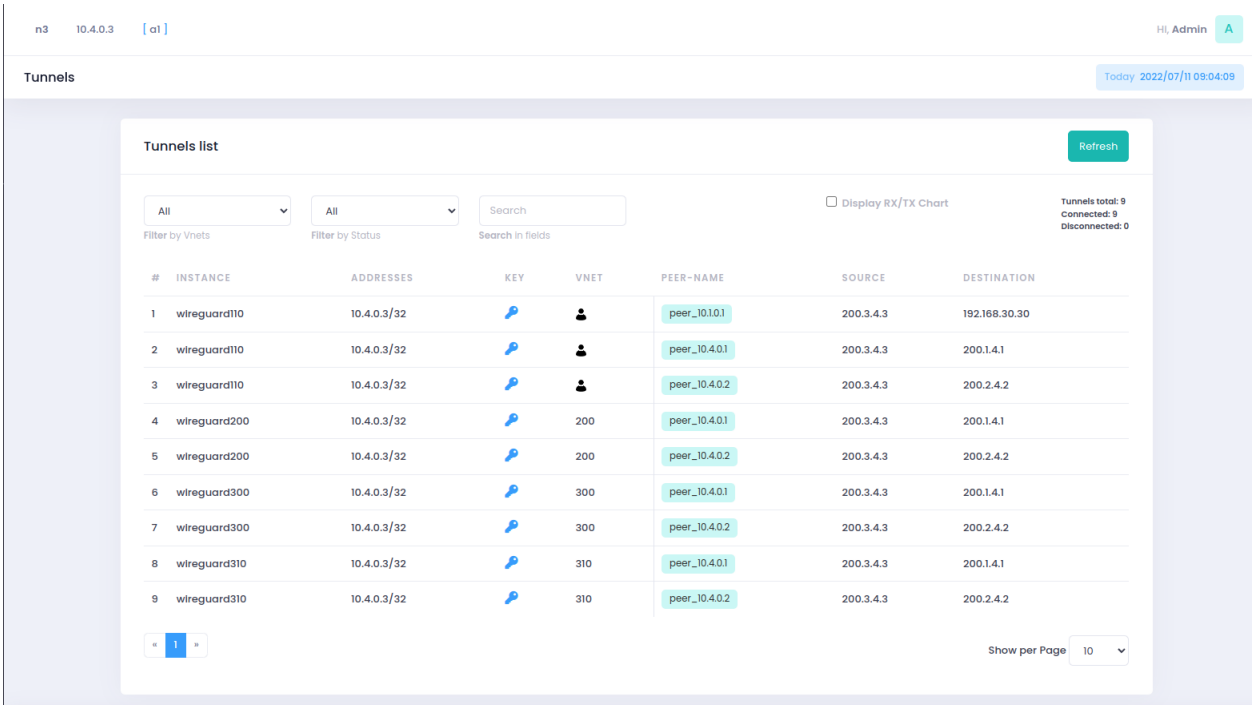

n2 10.4.0.2 [a1]
Hi, Admin A
Tunnels
Today 2022/07/11 09:04:05
Tunnels list
Refresh
All
Filter by Vnets
All
Filter by Status
Search
Search in fields
Display RX/TX Chart
Tunnels total: 9
Connected: 8
Disconnected: 1
INSTANCE ADDRESSES KEY VNET PEER-NAME SOURCE DESTINATION
1 wireguard110 10.4.0.2/32 peer_10.1.0.1 200.2.4.2 192.168.30.30
2 wireguard110 10.4.0.2/32 peer_10.4.0.1 200.2.4.2 200.1.4.1
3 wireguard110 10.4.0.2/32 peer_10.4.0.3 200.2.4.2 200.3.4.3
4 wireguard200 10.4.0.2/32 200 peer_10.4.0.1 200.2.4.2 200.1.4.1
5 wireguard200 10.4.0.2/32 200 peer_10.4.0.3 200.2.4.2 200.3.4.3
6 wireguard300 10.4.0.2/32 300 peer_10.4.0.1 200.2.4.2 200.1.4.1
7 wireguard300 10.4.0.2/32 300 peer_10.4.0.3 200.2.4.2 200.3.4.3
8 wireguard310 10.4.0.2/32 310 peer_10.4.0.1 200.2.4.2 200.1.4.1
9 wireguard310 10.4.0.2/32 310 peer_10.4.0.3 200.2.4.2 200.3.4.3
« 1 »
Show per Page 10

در n3 :


n3 10.4.0.3 [a1]
Hi, Admin A
Tunnels
Today 2022/07/11 09:04:09
Tunnels list
Refresh
All
Filter by Vnets
All
Filter by Status
Search
Search in fields
Display RX/TX Chart
Tunnels total: 9
Connected: 9
Disconnected: 0
INSTANCE ADDRESSES KEY VNET PEER-NAME SOURCE DESTINATION
1 wireguard110 10.4.0.3/32 peer_10.1.0.1 200.3.4.3 192.168.30.30
2 wireguard110 10.4.0.3/32 peer_10.4.0.1 200.3.4.3 200.1.4.1
3 wireguard110 10.4.0.3/32 peer_10.4.0.2 200.3.4.3 200.2.4.2
4 wireguard200 10.4.0.3/32 200 peer_10.4.0.1 200.3.4.3 200.1.4.1
5 wireguard200 10.4.0.3/32 200 peer_10.4.0.2 200.3.4.3 200.2.4.2
6 wireguard300 10.4.0.3/32 300 peer_10.4.0.1 200.3.4.3 200.1.4.1
7 wireguard300 10.4.0.3/32 300 peer_10.4.0.2 200.3.4.3 200.2.4.2
8 wireguard310 10.4.0.3/32 310 peer_10.4.0.1 200.3.4.3 200.1.4.1
9 wireguard310 10.4.0.3/32 310 peer_10.4.0.2 200.3.4.3 200.2.4.2
« 1 »
Show per Page 10

15.1 مشاهده جدول routing

برای نمونه جدول مسیریابی در روتر n3 را مشاهده می کنید . route های اضافه شده در روتر یا connected هستند یا از طریق ospf یا wg یا به صورت static اضافه شده اند . در هر route مشخص است که در چه vnet ی اضافه شده است .
برای مثال شبکه 1.2.1.0/24 از طریق 10.4.0.1 (روتر n1) قابل دسترس است و این route در vnet 310 اضافه شده است و از vnet های دیگر در دسترس قرار ندارد .

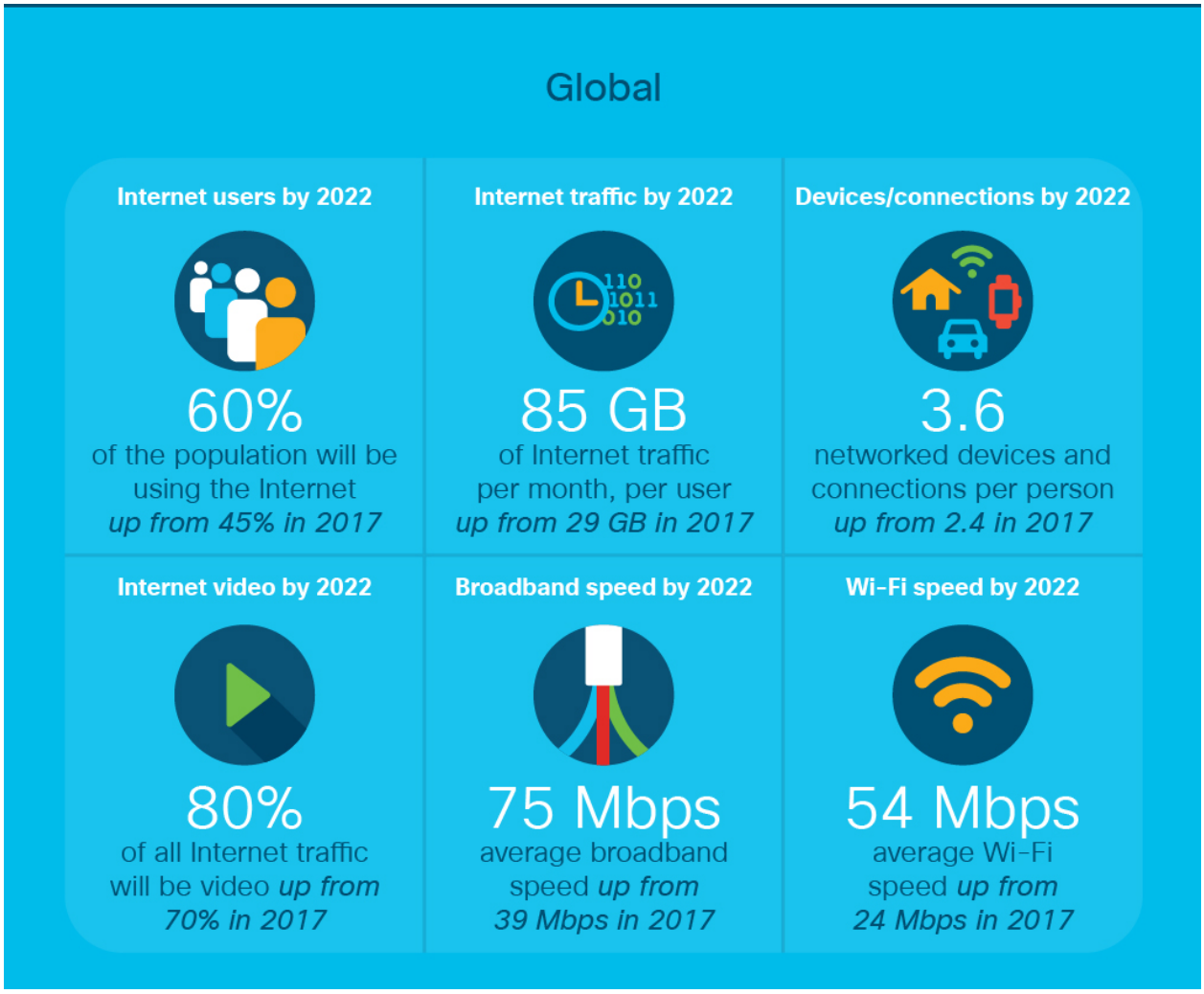


فصل 2

سودار

1.2 معرفی

در سالهای اخیر اتصال به شبکه برای همگان به یک ضرورت تبدیل شده است از سویی دیگر دسترسی به محتوای تصویری به صورت برخط در بین مردم رواج یافته است. این روند باعث افزایش حجم داده تبادلی در شبکه ها شده است. این روال با ورود نسل 5 ارتباطی سرعت بیشتری می گیرد. در زیر آمار تغییرات رفتار ترافیکی کاربران در سال 2022 نسبت به 2017 پیش بینی شده است که رشد سه برابری ترافیک اینترنت را نشان می‌دهد.



با فراهم شدن بستر ارتباطی نسل 5، تکنولوژی هایی مانند IoT توانایی عملیاتی شدن می یابند و این فرایند، انقلابی در کاربردها ایجاد می نماید. این انقلاب به خاطر سرعت بیشتر در نسل 5 بوجود نمی آید، بلکه به این علت است که بستر شبکه می تواند به عنوان یک بستر زمان واقعی(Real-Time) مورد استفاده قرار گیرد. این بستر این امکان را فراهم می آورد که دستگاه‌های متصل به شبکه نسل 5(مانند تلفن‌های همراه هوشمند) مشکلی در ارتباط دوسویه با دیگر المانهای شبکه و استفاده از منابع شبکه(اعم از اطلاعات، تصاویر، ویدیوها و...) نداشته باشند و این ارتباطات دوسویه و منابع دیگر شبکه به گونه‌ای در دسترس می باشند که برنامه‌ها می توانند از آنها به صورت آنی استفاده نمایند. این قابلیت ارتباطی در برنامه‌ها، رویکردهای نوینی را در زمینه معماری و طراحی برنامه‌های کاربردی خلق می کند. بنابراین وجود روترهایی که توانایی مسیریابی حجم بالای ترافیکی را داشته باشند و همچنین زمان-واقعی را در بستر شبکه فراهم نمایند الزامی است.

از سوی دیگر مسائل امنیتی و سیاسی کشور ایجاب می کند که ما به دنبال بومی سازی محصولات استراتژیک مورد استفاده باشیم. همانطور که شبکه های انتقال آب و برق و گاز بسیار حیاتی تلقی شده و بروز یک معضل اساسی فاجعه به بار می آورد، شاید بتوان گفت که مشکلات اساسی در شبکه های اطلاعاتی چه بسا آثار مخرب تری را بوجود می‌آورند. بنابراین اگر در این زمینه ما تمام تلاش خود را انجام ندهیم، در آینده هزینه گزافی بابت آن پرداخت خواهیم کرد. در صورت ایجاد بستر روترهای سریع می توان صادرات آن به کشورهای منطقه را در نظر گرفته که این امر ورود ارز به کشور را در پی دارد.

با توجه به نیاز کنونی بازار و تغییرات بسیار وسیع در بستر شبکه ها در آینده نزدیک، نیاز به روتر های پرظرفیت و کم تاخیر نه تنها در هسته شبکه ها بلکه در لبه شبکه ها نیز بوجود می آید. از روی دیگر تجهیزات کنونی اکثرا بر اساس برندهایی مانند سیسکو می باشد که به دلیل عدم امکان استفاده از پشتیبانی و همچنین دسترسی داشتن به بخش حیاتی از زیرساخت شبکه کشور مشکلات امنیتی فراوانی برای شبکه های ارتباطی کشور ایجاد می نماید. بر این اساس شرکت امنش با تکیه بر بیش از یک دهه فعالیت در حوزه امنیت و شبکه، از سال 2017 به پیاده سازی روتر با ظرفیت بالا و تاخیر پایین پرداخته است. این روتر بر روی سخت افزارهای مناسب، توانایی گذردهی بیشتر از 1 ترابیت در ثانیه را داراست. روتر سودار یک پروژه جوان و پویا است. ولی با توجه به انتخاب درست هسته پردازشی، تکیه بر پروژه ای دارد که به صورت کاربردی در برخی روتر های سطح بالای سیسکو در شبکه های بزرگ مورد استفاده قرار می گیرد. سودار در این مرحله دارای امکانات متعدد یک روتر پیشرفته می باشد و برای آینده آن برنامه های مختلفی را مد نظر گرفته ایم.

سودار نسل جدید روترهای نرم افزاری است که با دور زدن پشته سیستم عامل، توانایی مسیریابی با سرعت بالا و تاخیر پایین را فراهم می کند. سودار می تواند بر

روی سخت افزارهای مناسب عمومی، سرعت بالای 1 ترابیت را نیز پشتیبانی نماید. روتر سودار از دو پایه نرم افزاری معتبر و تست شده برای Data-Plane و Control-Plane استفاده می کند. ما در روتر سودار ارتباط و هماهنگی این بسترها را پیاده سازی نموده ایم و یک رابط کاربری کاملا شبیه سیسکو برای مدیران شبکه فراهم کرده ایم. یکی از وظایف اصلی تیم فنی روتر سودار، پیاده سازی تست های اتوماتیک و پوشش تستی حداکثری عملکرد روتر می باشد. در این متن ضمن معرفی امکانات روتر سودار راه حل خود را برای پوشش نیازهای کاربران شبکه های با ظرفیت بالا ارائه می نماییم.

1.1.2 فناوری های پایه مورد استفاده

سودار یک روتر بومی بر پایه جدیدترین تکنولوژی های مورد استفاده در روترهای نرم افزاری می باشد. هدف اصلی این محصول ارائه روتر پرسرعت، امن، پایدار و دارای پروتکلها و تکنولوژیهای موجود در روترهای پیشرفته است که بتواند در هسته شبکه های بزرگ مورد استفاده قرار گیرد. این محصول برای راحتی مدیران شبکه، از لحاظ تنظیمات کاربری با روتر های سیسکو انطباق حداکثری را دارد.

روتر های موجود در بازار شامل دو گروه روترهای سخت افزاری و نرم افزاری می باشند، که با توجه به تحریم کشور و ممانعت از ورود روترهای سخت افزاری و نیز قیمت بسیار بالای آن ها تهیه و استفاده از آنها دارای مشکلاتی است. گروه دیگر، روترهای نرم افزاری هستند که غالب روترهای بومی در این دسته قرار دارند. یکی از مشکلات روترهای نرم افزاری سرعت پایین آنها می باشد. چون در تمامی این محصولات از شبکه ی سیستم عامل استفاده می شود و این استک در تمامی سیستم عاملها به صورت عمومی نوشته شده و در شبکه های پرظرفیت و حساس به تاخیر نمی تواند مورد استفاده قرار گیرد. گروه سودار برای حل این مشکل از چند سال پیش به سمت ایجاد یک روتر بومی پر سرعت حرکت کرد. در ابتدای امر به بررسی عوامل کندی سرعت و روشهای افزایش آن پرداخته شد و بعد از آن به ایجاد دانش بر روی بستر DPDK اقدام شد.

DPDK یک ابزار توسعه بستر داده می باشد که با حذف پشته‌ی شبکه سیستم عامل از مدار مستقیما بسته ها را از کارت شبکه دریافت نموده و پس از اتمام عملیات بسته ها را مستقیما بر روی کارت شبکه قرار می دهد. بنابراین تمامی سربار و ناکارآمدی سیستم عامل را حذف می‌کند. اما این بستر پروتکل های شبکه را پیاده سازی نکرده است. بدین منظور از VPP استفاده می گردد که بر روی DPDK بستری مناسب جهت مسیریابی سریع ایجاد کرده است.

استفاده از VPP باعث شده است که سودار بتواند کارتهای شبکه پر ظرفیت مانند 40Gbps/100Gbps را بر روی یک بستر سخت افزاری عمومی حمایت کند و با ترکیب مناسب تجهیزات سخت افزاری مانند پردازنده های چند هسته ای بتواند به ظرفیت بالای ترافیکی برسد. این محصول در مقایسه با دیگر روتر های موجود داخلی دارای سرعت بسیار بالا و امکانات شبکه ای بیشتر می باشد.

VPP فقط یک بستر داده در روتر است و هیچ گونه پیاده سازی از پروتکل های روتینگ ندارد. برای این منظور از FRRouting جهت پوشش پروتکل های روتینگ استفاده شده است. با استفاده از FRRouting انواع پروتکلهای روتینگ از قبیل OSPF , BGP, RIP, ISIS را در روتر می توانیم پشتیبانی نماییم. از سوی دیگر پیاده سازی IKE در VPP ابتدایی بوده و فاقد بسیاری از امکانات مورد نیاز برای یک روتر عملیاتی است. بنابراین از StrongSWAN برای IKE استفاده شده است که این امر مستلزم پیاده سازی تمامی ارتباطات لازم بین StrongSWAN و مابقی سیستم مانند VPP,FRRouting و سیستم مانیتورینگ میباشد.

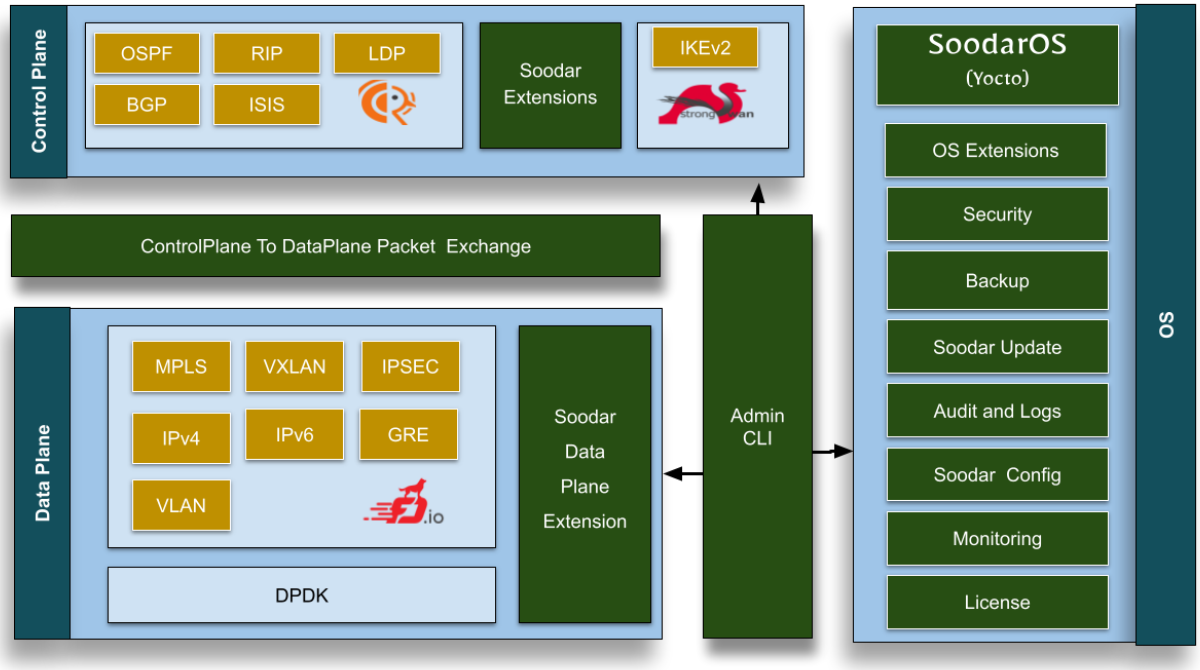
برای یک روتر فقط سرعت بالا و پشتیبانی پروتکلها در شبکه مطرح نیست مسائلی از قبیل امنیت سیستم، کارکرد صحیح سیستم، پایداری سیستم، به روزرسانی، پشتیبانی و تغییرات بر اساس نیاز مشتری از درجه اهمیت بالایی برخوردار است. بدین منظور انواع تستهای مختلف کارکردی از روترها گرفته می شود که شامل تست با سخت افزار واقعی و تست های اتوماتیک در شرایط شبیه سازی شده می باشد. ساز و کار به روز رسانی نیز مد نظر گرفته شده تا برای رفع مشکلات و ارائه نسخه جدید به کار گرفته شود. ما در این محصول می توانیم کارتهای شبکه Gbps10/25/40/100 را بر روی سخت افزارهای عمومی چند هسته ای به صورت ظرفیت کامل استفاده کنیم. بر اساس آزمایشهای انجام شده هر هسته پردازنده قادر است بین 10MPPs تا 15MPPs (بر اساس فرکانس پردازنده) را پشتیبانی نماید. این تعداد بسته در ثانیه برای هر بسته با طول متوسط 500 بایت سرعتی بیش از 40Gb/s را به ازای هر هسته پردازنده فراهم میکند. که بر این اساس برای داشتن یک روتر با 16 پورت 10Gbps می توان از یک پردازنده xeon یا Corei7 معمولی استفاده نمود. روتر سودار می تواند به راحتی جایگزین روترهای سخت افزاری سیسکو، با امکانات و سرعت مشابه شود.

با استفاده از روتر سودار می‌توانید با انتخاب سخت‌افزار متناسب، سرعت های تجمعی 50Gbp/s , 100Gbp/s , 400Gbp/s تا 800Gbp/s را تجربه کنید.

2.1.2 بلوک دیاگرام محصول

در شکل زیر یک نمای کلی از ساختار روتر سودار ارائه شده است. در شکل زیر تمامی المانهای سبز رنگ در شرکت امنش پیاده سازی گردیده است و نرم افزارهای open-source مورد استفاده نیز در آن مشخص شده است.

معماری داخلی روتر سودار



بر اساس بلوک دیاگرام بالا در روتر سودار از المانهای متن باز زیر استفاده شده است:

1. برای IO از DPDk استفاده شده است
2. برای Data-Plane از VPP استفاده شده است
3. برای Control-Plane از Frrouting و StrongSwan استفاده گردیده است
4. برای به روز رسانی سیستم عامل از Mender استفاده می‌شوود.

اما واحدهای زیر برای ایجاد عملکردهای لازم قسمتهای مختلف توسط تیم مهندسی شرکت امنش پیاده سازی گردیده است:

5. توزیع سیستم عامل مخصوص روتر سودار
6. واحد واسط مدیر شبکه با سودار
7. واحد تنظیم کننده Data-Plane که تنظیمات اعمال شده توسط مدیر شبکه را به Data-Plane اعمال می نماید.
8. واحد تنظیم کننده Control-Plane
9. تغییرات در Control-Plane برای پیاده سازی مواردی مانند VRF و تونلها
10. واحد به روز رسانی جدولهای مسیریابی IPv4,IPv6,MPLS,Multicast
11. واحد انتقال بسته های متعلق به پروتکلهای مسیریابی و اتصال امن مدیریتی از Data-Plane به سیستم و بالعکس
12. واحد به روز رسانی سیستم از سرور مرکزی امنش

13. واحد کنترل لایسنس و تنظیم کننده سیستم
14. و همچنین امکانات جانبی دیگر مانند SLA و Backup

البته این مواردی که اشاره شد همگی درون روتر سودار قرار می گیرند مواردی نیز در بیرون از روتر سودار پیاده سازی شده است.

1. سیستم نمونه سازی روتر سودار بر روی شبکه ای از کانتینر ها که با اعمال تغییرات در یک نرم افزار منبع باز صورت پذیرفته است
2. تست های برنامه نویسی شده و اتوماتیک که با استفاده از سیستم نمونه سازی پیاده شده است
3. سرور به روز رسانی و سرور لایسنس
4. سرور مانیتورینگ

3.1.2 پشتیبانی از شبکه های با مقیاس بزرگ

روتر بومی سودار قادر است شبکه‌های بزرگ در مقیاس هزاران عضو را پشتیبانی کند بدون اینکه در عملکرد آن تغییر محسوسی بوجود آید.

Data plane که در سودار استفاده شده است بسیار پر قدرت است و با توجه به سرعت بسیار بالای آن مناسب استفاده در شبکه های هسته می باشد و تست های متعدد با شبکه های بزرگ در محیط شبیه ساز را با موفقیت گذرانده است .

2.2 امکانات سودار

1.2.2 امکانات سیستمی

- دارای سیستم عامل اختصاصی و محیط کاربری CLI مشابه با سیسکو
- قابلیت بروز رسانی امن و مطمئن بصورت آنلاین و آفلاین با سرور اختصاصی به روز رسانی
- پشتیبان گیری/ بازنشانی تنظیمات به صورت محلی یا بر روی شبکه
- سیستم مجتمع ممیزی با قابلیت نمایش داده های ممیزی در هر روتر
- سرویس مرکزی اختصاصی مانیتورینگ و پشتیبانی از IPFIX ، SNMP و Prometheus در روتر
- Support ethernet, SFP, SFP modules(1G,2.5G,10G,25G,40G,100G+...)

IPv4/IPv6 2.2.2

- 14+ MPPS, per cpu core
- Multimillion entry fib
- Source RPF
- Thousands of VRFs
- Controlled cross-VRF lookups
- Multipath - ECMP

- Multiple million Classifiers - Arbitrary N-tuple
- VLAN Support - Single/Double tag
- Counters for everything
- Mandatory Input checks
- TTL expiration
- header checksum
- ARP resolution/snooping

3.2.2 IPv6

- Neighbor Discovery
- Router Advertisement

4.2.2 پروتکلهای مسیریابی:

روتر سودار از تمامی پروتکل های مورد استفاده و کاربردی در شبکه های امروزی پشتیبانی می کند. همچنین توانایی ارائه الگوریتم مسیریابی بومی که محصول شرکت است، نیز وجود دارد.

:BGP4

- BGP Community-List
- BGP Extended community-List
- IPv4/6 Unicast address family
- Route Reflector client
- Route Reflector server
- eBGP
- iBGP
- Soft-reconfiguration support
- Route selection customization
- Route Maps
- Capability negotiation
- Route Aggregation
- AS-Path access-list
- VRF Aware
- Route redistribution

RIP

- Version 1
- Version 2
- IPv6/ Version 3(RIPng)
- Route Maps
- Split-horizon
- Distribute-lists
- Offset-list
- Authentication
- VRF Aware
- Route redistribution

OSPF

- ABR/ ASBR router
- LSA Summary
- Area authentication
- Interface authentication
- Broadcast/ non-broadcast/ P2MP/ P2P networks
- Router priority
- Distribute-lists
- Default route originate
- Route maps
- VRF Aware
- Route redistribution
- Multi-instance support
- Full packet encryption(Soodar specific feature)

ISIS

- Level-1, level-2-only, level-1-2 circuit types
- Dynamic hostname support
- Interface authentication
- Area authentication
- VRF Aware
- Domain authentication
- Narrow/ wide metric styles
- Prefix-lists

MPLS 5.2.2

در شبکه های هسته استفاده از پروتکل MPLS برای پایین آوردن هزینه مسیریابی بسیار کارساز است همچنین برای ایجاد خدمات مهندسی ترافیک و ایجاد تونلینگ از MPLS استفاده می شود. روتر سودار پروتکل MPLS و پروتکل LDP را پشتیبانی میکند. و همچنین میتوان تونلهای VPLS را در شبکه MPLS ایجاد نمود.

- LDP(As described in RFC5036)
- MPLS L3VPN(MP-BGP)
- VPWS Tunnels
- MPLS-o-Ethernet
- Deep label stacks supported

ACL 6.2.2

- Standard ACLs(Source,Destination)
- Extended ACLs(Protocol, Source, Destination, Source port, Destination Port, ICMP codes, TCP flags)
- Named ACLs
- IPv4/ IPv6 Support
- Stateful

QoS 7.2.2

- Class Maps
- Policy Maps
- DSCP Marking
- Traffic Policing
- Class maps for traffic classification
  - Match packet against ACLs
  - Match packet against a source address
  - Match packet against a destination address
  - Match packet against a DSCP
  - Combine rules and match all/any of them
- Policy maps for defining policies for Class maps
  - Double criteria traffic policing.
  - Applied on interface 's ingress traffic'.

IP SLA 8.2.2

- Different SLA types
  - ICMP echo
    - Frequency
    - Timeout
    - Threshold
    - VRF
    - Payload length
  - ICMP jitter
    - Frequency
    - Timeout
    - Threshold
    - VRF
    - Number of packets and the interval between them in a burst
- Support reactions
  - Support of various parameters for reaction
    - Average jitter
    - Average jitter(percentile calculation)

    - RTT
    - Over threshold
    - Packet loss
    - Timeout
  - Support of various reactions criteria
    - Immediates
    - Average
    - Consecutive
    - XofY
  - Support of Log action and Trigger action
- Recurring schedules and infinite run of SLA

Tracks 9.2.2

- Track various objects in system
  - SLA
    - On SLA reachability
    - On SLA reaction
  - Interface state
  - Route reachability
    - Specific nexthop(IP or interface)
    - VRF
  - Boolean list
- Install/uninstall static routes based on the track state
- Install/uninstall policy-maps on an interface based on the track state

Tuning 10.2.2

- Limit Memory usage of different system services.
- Exclude CPUs from OS scheduler.
- Bind different system services to CPUs.
- CPU usage weight.
- System hugepages size and number.
- Change interface mapping.
- Set dataplane main and worker cores.

- Set dataplane heap memory size.
- Set dataplane buffers options.
- Enable dataplane polling sleep and set its intervals.

11.2.2 **DHCP**

- DHCP4 Server
  - DHCP pools
  - Lease time
  - DNS address
  - Router address
  - Domain name
  - NTP server address
- DHCP4 Client
  - Request/Deny router address
  - Request/Deny DNS address

12.2.2 تونل‌های لایه 2 و لایه 3:

- VXLAN Tunnels
  - Static defined P2P
  - VRF Aware
- GRE Tunnels
  - P2P
  - Protected with IPSec SA
  - VRF Aware(When not protected)
- IP-IP Tunnels
  - P2P
  - Protected with IPSec SA
  - VRF Aware(When not protected)
- IPSec
  - Route-based SAs
  - IKEv2 with PSK and RSA-Sig
  - Integrated with PKI system
  - IKEv2 Dead Peer Detection

- SA Initiator/ Responder
- SA Lifetime
- SA Rekeying
- Well-known encryptions
- Custom user defined encryptions
- Wireguard
  - Wireguard server
  - Wireguard client
  - Normal WG mode(Uses allowed IPs)
  - Routing WG mode(Uses static/OSPF .../routing)
  - Custom user defined encryptions
- VPLS and MPLS Tunnels

13.2.2 امکانات لایه 2:

- VLAN
  - Dot1Q
  - Q-in-Q
  - Tag rewrite(push and pop. currently no translation)
- Bridge
  - Supports split horizon group’s
  - No STP
  - BVI
- Bonding Interfaces
  - LACP
  - Active-Backup
  - Broadcast
  - Supports Load-Balancing(Available only in LACP)
- L2 forwarding with EFP/Bridge Domain concepts
- BFD
- SPAN Port
- LLDP
- Link Detection
- VTR - push/pop/translate
- Mac Learning - default limit of 50k addresses
- Bridging - Split-horizon group support/EFP filtering

- Proxy Arp
- Arp termination
- IRB - BVI Support with RouterMac assignment
- Flooding
- Port security

14.2.2 امکانات NAT

- Static NAT
  - Address Only NAT
  - Protocol NAT
  - Uses Inside and outside cisco-like NAT(not Source/ Destination like the ones in linux)
- Dynamic NAT
  - Uses IP Pool
  - PNAT
  - ACL based NAT
- Carrier Grade NAT(Deterministic NAT)
- Source NAT

15.2.2 امکانات PKI:

- RSA Key generation/ zeroization
- X25519 Key generation/ zeroization
- SSH Key generation
- Adding/ Removing Trustpoints
- Generating certificate signing request
- Importing signed certificates
- SSH authorized key management
- SSH known keys management

16.2.2 امکانات مانیتورینگ:

- Prometheus Metrics
  - node hardware metrics
  - network metrics
  - wireguard tunnel metrics
  - IPSec tunnel metrics
  - dataplane metrics
  - OS metrics
- Logs
  - Supports Syslog
  - TCP/UDP syslog client with TLS support
  - Vector client
- SNMPv3
- IPFIX
- SPAN Port
- LLDP
- CDP
- Packet capturing(with debugging dissectors)

17.2.2 سیستم به روز رسانی

- Automated rootfs rollback with dual A/B partition
- Full image atomic updates
- Secure TLS communication
- image signing for verification
- Root filesystem integrity checksum to avoid corruption during transfer or storage.

18.2.2 امکانات مدیریتی

- Cisco compatible CLI
- SSH and local console
- Config backup/restore via SCP and local
- PKI backup/restore via SCP and local

- System analyzer and crash management(exportable via SCP)
- Set system Date,Clock,timezone
- NTP
- DNS client
- Static host-name to address mapping

19.2.2 امکانات قابل پیاده سازی در صورت درخواست:

پایه این امکانات در هسته VPP موجود است و باید با کل سیستم مجتمع گردد و تستهای مورد نظر پیاده سازی گردند.

- NAT
  - NAT64
  - NAT66
  - CGNAT
- VRRP
- MGRE(And possibly DMVPN)
- L2VPN
- Unequal Cost Multipath
- DHCPv6 Proxy
- L2TPv3
- Segment Routing

3.2 سیستم عامل اختصاصی

سیستم عامل روتر سودار، SoodarOS می باشد که بر پایه لینوکس بوده و با استفاده از Yocto ساخته شده است.

1.3.2 امنیت روتر های سودار

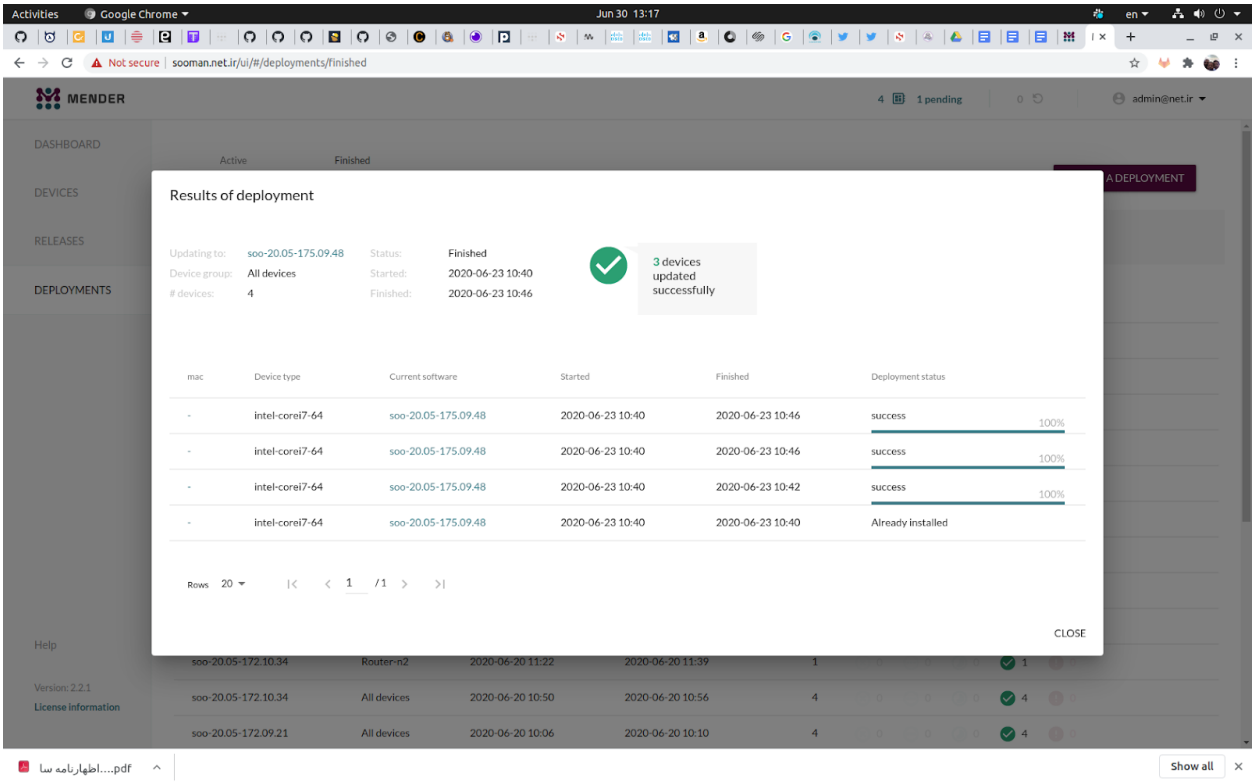
1. دارای سیستم عامل اختصاصی‌ست که بر اساس نیازهای روتر پیکره‌بندی شده است
2. کرنل سیستم عامل و تمامی نرم افزارها و کتابخانه های مورد نیاز به صورت دستی انتخاب ، کامپایل و پیکره‌بندی شده اند. بنابراین سطح حمله پذیری سیستم عامل کاهش یافته است
3. استفاده از آخرین نسخه های به روز شده امنیتی کرنل و نرم افزارها.
4. چک کردن اتوماتیک تمامی نرم افزارهای موجود در سیستم عامل با بانک اطلاعاتی CVE و شناسایی آسیب ها.
5. تمامی ارتباطات با روتر به صورت امن صورت می پذیرد و ارتباط ادمین ها با روتر با پروتکل SSH انجام می پذیرد
6. امکان جداسازی ترافیک مدیریتی از ترافیک شبکه

7. ارائه نسخه های به روز شده به صورت دوره ای و یا در زمان شناسایی هر گونه آسیب پذیری امنیتی

2.3.2 به روز رسانی امن و کارآمد

به روز رسانی امن، کارآمد و بدون ریسک با سرور به روز رسانی اختصاصی :

1. ایمیج به روز رسانی تایید شده: ایمیج به روز رسانی در زمان تولید در آزمایشگاه امضا می گردد و روترها ایمیج بدون امضای سازنده را قبول نمی کنند.
2. ارتباط امن با سرور به روز رسانی: ارتباط بین روترهای سودار و به سرور به روز رسانی به صورت امن با TLS و تاییدیه های PKI تزریق شده در روتر صورت می پذیرد.
3. تایید دو طرفه: هم روترها سرور به روز رسانی را تایید میکنند و هم مدیر سیستم تمامی روترهای خود را در سرور به روز رسانی تایید می کند.
4. حداقل زمان قطعی سرویس روتر: به روز رسانی در روتر سودار به صورت دو پارتیشنه انجام می شود و در زمان دانلود ایمیج جدید و تایید این ایمیج و همچنین به روز رسانی پارتیشن پشتیبان هیچ اختلالی در روال کاری روتر ایجاد نمی‌گردد و فقط در انتهای به روز رسانی موفق به این پارتیشن سوییچ میکند که روتر فقط به اندازه بالا آمدن سیستم عامل از سرویس دهی خارج می گردد.
5. بازگشت به نسخه قدیمی در صورت عدم تایید به روز رسانی: پس از انجام روال به روز رسانی سیستم عامل جدید بوت می شود و یک روال تایید را می گذراند. در صورت عدم موفقیت تستهای تایید، به روز رسانی لغو گردیده و به سیستم عامل قبلی سوییچ می شود.
6. امکان گروه بندی روترها در سرور به روز رسانی: در سرور به روز رسانی که برای هر شبکه ارائه می گردد امکان مدیریت به روز رسانی ها توسط مدیر شبکه فراهم می گردد.



3.3.2 مانیتورینگ پیشرفته روترها

مانیتورینگ پیشرفته روترها شامل مانیتورینگ خود سیستم و جریانهای داده عبوری و داده های ممیزی است که همراه با سرور اختصاصی ارائه می گردد :

1. پشتیبانی از استانداردهای روز مانیتورینگ: در سودار مانیتورینگ با پروتکل Prometheus ارائه می گردد. این پروتکل که استاندارد جدید مانیتورینگ سرویسهای کلود می باشد قابلیت گسترش و توسعه پذیری بالایی دارد.
2. پشتیبانی از پروتکل مانیتورینگ SNMP
3. دارای پروتکل IPFIX برای مانیتورینگ جریانهای داده عبوری
4. لاگ غیر قابل تغییر در روترها و با اطمینان ارسال به سرور
5. لاگ‌های با جزئیات از قسمت های مختلف سیستم از پروتکلهای روتینگ تا حسابرسی سیستم عامل
6. امکان اتصال داده های ممیزی به SOC سازمان
7. دارای سرور اختصاصی یکپارچه برای مانیتورینگ با پروتکل prometheus و داده های ممیزی
8. وجود سرویس اخطار رویدادها در سرور مانیتورینگ اختصاصی

4.2 روتر بومی پرسرعت سودار (دانش بنیان)

سودار یک روتر بومی بر پایه جدیدترین تکنولوژی های مورد استفاده در دنیای شبکه می باشد. هدف این محصول ارائه روتر با سرعت بالای 1Tbps و تاخیر پایین با انواع پروتکلها و امکانات موجود در روترهای پیشرفته است که بتواند در هسته شبکه های بزرگ مورد استفاده قرار گیرد.

سودار برای راحتی مدیران شبکه و عدم نیاز به یادگیری زبان تنظیمات کاربری جدید، انطباق حداکثری با روترهای سیسکو را داراست. سودار روتری متفاوت در میان روترهای نرم افزاری است که همزمان دارای خصوصیات زیر است:

- سرعت بالای پردازشی بر روی سخت افزارهای عمومی
- پشتیبانی از آخرین پروتکلها و امکاناتی که در روترهای جدید وجود دارد
- سیستم عامل اختصاصی و امن با امکان به روز رسانی مطمئن و مانیتورینگ و ممیزی مرکزی
- قابلیت اطمینان بالا با ایجاد سناریوهای تست برنامه نویسی شده اختصاصی

در گذشته به علت سرعت پایین پردازنده ها اغلب روترها به صورت سخت افزاری پیاده سازی می شد. این امر باعث میشد تا ایجاد و گسترش تکنولوژیهای جدید در روترها به کندی صورت پذیرد و همچنین این تغییرات هزینه بالایی داشته باشد. ولی امروزه با سریع شدن پردازنده های عمومی و تعداد زیاد هسته های پردازشی، در این سخت افزارها که می تواند به بیش از 100 هسته پردازشی در یک سیستم برسد، سازندگان روتر کنونی به سمت روترهای نرم افزاری حرکت کرده اند و فقط برخی عملیات محدود درون کارت شبکه یا سخت افزار خاص منظوره صورت می پذیرد.

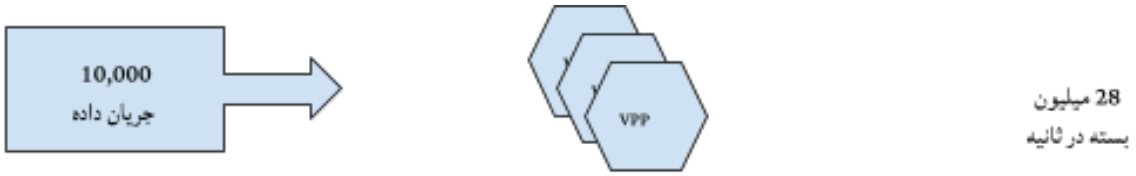
5.2 کارایی و توسعه پذیری

روتر سودار بر پایه VPP ایجاد شده است که سریعترین هسته روتینگ نرم افزاری را ارایه میکند. این روتر از چند جهت دارای امتیاز است:

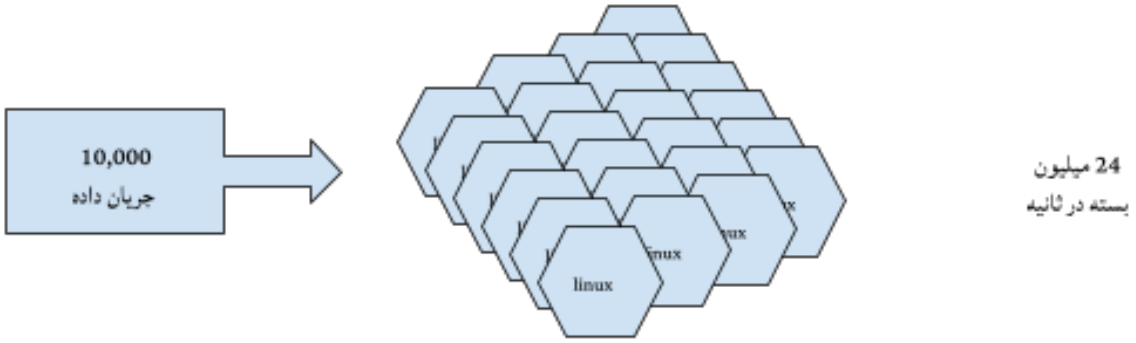
- تاخیر پایین در پردازش بسته ها
- کارایی بالا روتینگ در یک هسته پردازشی
- توسعه پذیری عالی نسبت به افزایش تعداد هسته های پردازشی
- حفظ کارایی با افزایش جدول روتینگ. با جدول روتینگ دارای چند میلیون روت هیچ تغییری در کارایی بوجود نمی‌آید.

- کارایی بالا در تونلهای IPSec. توانایی ایجاد تونلهای با گذردهی 40G
- پشتیبانی از تعداد رولهای ACL بالا
- پشتیبانی از تعداد تونلهای GRE و IPSec زیاد
- پشتیبانی از میلیونها VXLAN
- پشتیبانی از کارتهای شبکه سرعت بالا 10G-25G-40G-100G

برای مشاهده قدرت این روتر یک نمونه از مقایسه عملکرد روتینگ مشابه در لینوکس و VPP در زیر آورده شده است.



۳ هسته پردازنده - VPP



26 هسته پردازنده - لینوکس

در لینوکس با 26 هسته پردازنده فقط 24Mpps کارایی داشته ولی VPP فقط با 3 هسته پردازشی توانسته به کارایی 28Mpps دست یابد. کارایی VPP در تونلهای IPSEC و همچنین امکانات پایه فیلترینگ و امکانات دیگر این بستر بسیار بالاتر از مشابه های نرم افزاری خود می باشد.

Data Plane 6.2

برای چندین دهه، تنها راه برای سرعت بخشیدن به پردازش بسته ها افزودن سخت افزار سریعتر و یا استفاده از مدارهای مجتمع خاص منظوره(ASIC) بود. اما سرعت رشد سخت افزار با نیاز به سریعتر شدن پردازش بستهها متناسب نیست و استفاده از ASICها نیز باعث افزایش هزینهها و کاهش انعطاف پذیری دستگاهها میشود. اما پروژهای برای استفاده مفیدتر از سختافزارهای عمومی موجود برای پردازش بستهها وجود دارد: VPP.

با استفاده از پروژه متن باز VPP، دستگاه از طریق نرم افزاری که روی پردازنده های عمومی اجرا می شود، تا 100 برابر توان پردازش بسته بیشتر را ارائه می دهد. اما واقعا VPP چیست؟

1.6.2 پردازش بسته‌ها در کرنل سیستم عامل:

تا مدت‌ها مدل غالب پردازش بسته‌ها پردازش مبتنی بر کرنل بوده است. برای هر دستگاه شبکه‌ای که یک بسته را دریافت، بررسی و سپس به hop بعدی ارسال میکند، آن بسته در یک Interface شبکه دریافت می شود و مستقیما به سیستم عامل دستگاه ارسال میشود. این بسته تا کرنل سیستم عامل بالا میرود و در آنجا پردازش بسته انجام میگیرد.

هسته یا کرنل سیستم عامل، قلب تپنده‌ی سیستم عامل است. این قسمت عملکرد کامپیوتر و سخت‌افزارهای مهم آنCPU) و حافظه) را کنترل میکند. همچنین هسته‌ی سیستم عامل نسبتا کوچک و بخش حساس و حیاتی‌ای است و معمولا در هنگامی که پروسه‌های فراوانی نیاز به توجه دارند، بسیار مشغول است.

پردازش بسته ها در هسته بر مبنای اصل دریافت یک بسته در یک زمان، fetch کردن یک دستورالعمل از کش دستورالعمل‌ها، اجرای آن دستورالعمل روی بسته، fetch کردن دستورالعمل بعدی، اجرای آن دستورالعمل، و ... طراحی شده است. سپس آن بسته به مقصد خود ارسال می‌شود و بسته دوم وارد می شود و همان روال را طی می کند.

تشبیه FD.io برای توضیح این موضوع خوب است: مساله پشته ای از الوار را در نظر بگیرید که در آن هر تکه الوار باید بریده شود، سنباده زده شود و سوراخ هایی در آن ایجاد شود. دو راه برای انجام کار وجود دارد: 1- هر تخته را یکی یکی برش بزنید، سنباده بزنید و سوراخ کنید. یا، 2- همه تخته ها را برش دهید، سپس همه تخته ها را سمباده بزنید، سپس همه تخته ها را سوراخ کنید. رویکرد دوم باعث صرفه جویی در زمان می شود زیرا از تغییر ابزارها با هر مرحله فرآیند در هر الوار جلوگیری می کنید.

پردازش مبتنی بر هسته رویکرد اول است. در پردازنده‌های قوی، به‌عنوان مثال، پردازنده‌های کلاس Intel® Xeon®، ارسال بسته‌ها با لینوکس به 2 میلیون بسته در ثانیه (Mpps) می‌رسد - و به راحتی می‌توان با قفل کردن هسته‌های CPU به یک پروسه یا درگیر کردن کرنل سیستم عامل این عدد را به شدت کاهش داد. با استفاده از برخی امکانات آزمایشی، لینوکس در برخی معیارها(مانند حذف همه بسته‌های دریافتی) دستاوردهایی دارد، اما هنوز کار زیادی برای رسیدن به بهره‌وری بالا لازم است.

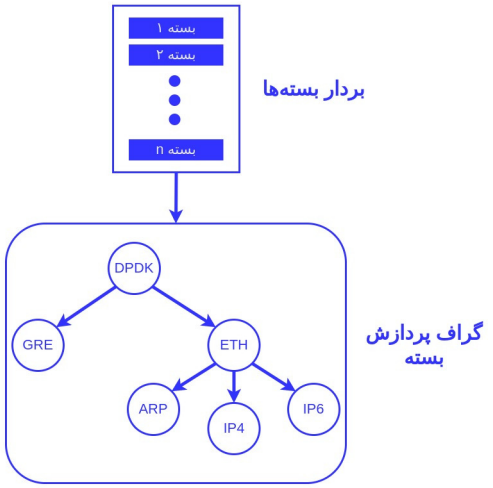
حال، اگر یکی از دستگاه های فوق دارای اینترفیس 10 گیگابیت بر ثانیه باشد، چگونه بسته ها را با سرعت کافی برای پر کردن خط پردازش می کنید؟ پردازش سرعت خط 10 گیگابیت بر ثانیه از کوچکترین بسته هایی که باید با آنها سروکار داشته باشیم (بسته های 64 بایتی که 84 بایت روی سیم است) معادل 14.88 میلیون بسته بر ثانیه است. چندین سیستم لینوکس که با یک Load balancer به هم متصل شده اند، هزینه، فضا، گرما و غیره زیادی را برای یک ارتباط 10 گیگابیت بر ثانیه مصرف می کنند. از طرف دیگر، می‌توانید ASICهای گران‌قیمت و اختصاصی تولیدکنندگان یا راه‌حل‌های مبتنی بر FPGA را انتخاب کنید که این انتخاب‌ها نیز ارزان نخواهد بود.

2.6.2 پردازش برداری بسته‌ها:

اکنون فرض کنید پردازش بسته‌ها از قید محدودیت‌های هسته سیستم عامل رها شده است و میتوان کش داده‌ها را به جای یک بسته در یک زمان، بر روی آرایه‌ای از بسته‌ها به شکل همزمان اعمال کرد. اینجاست که VPP معرفی میشود: نسخه‌ی متن باز از تکنولوژی پردازش برداری بسته‌های Cisco که در محصولات ASA و CSR به کار میرود و بنابراین تکنولوژی‌ای ثابت شده است. در اصل، VPP یک انتزاع گراف پردازش بسته ماژولار است، که در آن هر گره برداری از بسته‌ها را پردازش می‌کند تا Cache thrashing را کاهش دهد، و از طریق پلاگین‌ها قابل توسعه و تنظیم مجدد پویا می‌شود.

VPP حجم کاری پردازش بسته را از فضای کرنل به فضای کاربر منتقل می کند. فضای کاربر جایی است که برنامه ها و کتابخانه ها (که سیستم عامل برای تعامل با کرنل استفاده می کند، به عنوان مثال، نرم افزاری که ورودی/خروجی را انجام می دهد، آبجکت‌های Filesystem را دستکاری می کند، نرم افزارهای کاربردی و غیره) در آن قرار دارند. در نتیجه، فضای کاری بسیار بیشتری برای مدیریت مجموعه‌های دستورالعمل مبتنی بر Cache وجود دارد.

پس از دریافت آرایه‌ای از بسته‌ها، VPP آن بردار را از طریق یک گراف پردازش بسته پردازش می کند:



VPP به جای پردازش هر بسته از طریق کل گراف پردازش، و سپس واکشی بسته دوم و پردازش آن از طریق کل نمودار، بردار بسته ها را قبل از رفتن به گره گراف بعدی، به طور کامل از طریق گره گراف اول پردازش می کند. بسته اول در بردار instruction cache را گرم می کند، بنابراین بسته های باقی مانده را می توان بسیار سریع پردازش کرد - هزینه پردازش هر بسته بعدی در بردار را به شدت کاهش می دهد. این منجر به 1- عملکرد بسیار بالا برای پردازش یک بسته منفرد و 2- عملکرد قابل اعتماد آماری در پردازش تعداد زیادی بسته در طول زمان می شود. علاوه بر این، VPP اغلب آنچه را که بسته(های بعدی) می داند، از قبل واکشی می کند، و اطمینان حاصل می کند که CPU در زمانی که بسته بعدی از RAM واکشی می شود، متوقف نمی شود. در نتیجه، throughput همیشه بالا و latency به شکل پایداری پایین میباشد.

بیایید به مثال عملکرد خود در بالا برگردیم - جایی که توضیح دادیم تعدادی سیستم برای پر کردن یک لوله 10 گیگابیت در ثانیه با بسته های 64 بایتی با استفاده از پردازش هسته مورد نیاز هستند. و از آنجایی که این روزها سرعت 10 گیگابیت بر ثانیه نسبتاً رایج است، بیایید آن را کمی بالا ببریم. فرض کنید به شبکه 100 گیگابیت بر ثانیه نیاز دارید. VPP این امر را در نرم افزار قابل دستیابی می کند. 100 گیگابیت در ثانیه یک جهش 10 برابری بیش از 10 گیگابیت بر ثانیه است، بنابراین ما اکنون باید بین 8 تا 148 میلیون بسته در ثانیه پردازش کنیم - بسته به اندازه فریم بسته. اگر فریم‌های بسته بزرگ باشند، می‌توانیم 100 گیگابیت بر ثانیه - روی یک هسته واحد، ارسال کنیم. اگر بسته ها کوچک باشند، می توانیم 100 گیگابیت بر ثانیه را روی 10 هسته پردازش کنیم. ترافیک معمولی اینترنت ترکیبی است، بنابراین ما عملاً جایی در این بین خواهیم بود. در هر صورت، این منجر به کاهش چشمگیر هزینه‌ها نسبت به پردازش هسته می شود.

در حالی که VPP پردازش بسته مبتنی بر نرم افزار را بسیار جذاب می کند، هنوز زمان هایی وجود دارد که شتاب‌دهنده‌های سخت افزاری مناسب است. خوشبختانه، معماری گره گراف اجازه می دهد تا شتاب دهنده‌ی سخت افزاری به راحتی اضافه شود. به عنوان مثال، برنامه های پردازش ترافیک با محاسبات سنگین مانند شتاب دهنده‌های رمزنگاری سخت افزاری می توانند فقط به عنوان گره گراف دیگری ظاهر شوند.

7.2 سیستم تست کیفیت اختصاصی سودار

تست های محصول سودار به دو روش اتوماتیک و دستی انجام می پذیرد. مجموعه تستهای اتوماتیک با استفاده از زبان برنامه نویسی python و در دو سناریوی زیر انجام می پذیرد:

1. تست های اتوماتیک بر روی شبیه ساز اختصاصی
2. تست های اتوماتیک بر روی سناریوی فیزیکی شامل چند روتر سودار

تستهای دستی نیز بر اساس چک لیست های تهیه شده قبل از ارائه محصول توسط کارشناسان در آزمایشگاه صورت می پذیرد.

1.7.2 ویژگی های شبیه ساز اختصاصی سودار

شبیه ساز اختصاصی سودار که برای تست سودار ایجاد گردیده است دارای مشخصات زیر می باشد:

- قابلیت اجرای سناریو های کوچک چند نودی تا سناریو های چند صد نودی
- امکان قطع و وصل لینک های ارتباطی بین نود ها و اعمال پارامترهای delay , jitter , duplicate ،... روی خط
- ابزار هایی برای ارسال ترافیک های مختلف بین نود های سناریو
- قابلیت sniff و مشاهده ترافیک در هر نقطه و هر اینترفیس از نود های موجود در سناریو
- امکانات گرافیکی برای مشاهده و برجسته کردن ترافیک های در حال عبور در سناریو
- قابلیت اجرا سناریو به صورت اتوماتیک و استفاده از امکانات فوق به صورت برنامه نویسی شده .

2.7.2 تست های سودار

فرآیند ایجاد تست بدین صورت است که ابتدا هدف از تست مشخص شده و سپس سناریوی مد نظر برای تست طراحی می گردد بعد از آن تنظیمات و انتظارات و مشاهدات بعد از هر تنظیم در کدی که برای تست نوشته می شود لحاظ می گردد و در نهایت تست در شبیه ساز اجرا می گردد و پس از موفقیت روی دستگاه های فیزیکی نیز تست می شود .

3.7.2 دسته بندی تست ها

1. به ازای هر ویژگی که در سودار داریم و یا ویژگی جدیدی که اضافه می شود تست مربوطه اضافه می شود.
2. به ازای هر باگ یک تست ایجاد می شود تا در نسخه های باگ فیکس شده آن تست شود و همچنین از بروز آن باگ در نسخه های بعدی جلوگیری شود.
3. به ازای کاربرد هایی که روتر در شبکه های عملیاتی مختلف ممکن است داشته باشد تست هایی طراحی می گردد.
- استفاده به عنوان یک فایروال (ACL)
- استفاده از روتر در شبکه Core
- استفاده در ISP و جدا سازی شبکه های مشتری های خدمات گیرنده (VRF , VXLAN)
- تونل کردن IP6 روی تونل GRE با IP4
4. برخی تست ها مربوط به پایداری روتر در شبکه های بزرگ می باشد که تست هایی با کانفیگ های بزرگ و شبکه های بزرگ اضافه می گردد :
- کانفیگ های بزرگ ACL مثال : روتری شامل 1000 ACL
- کانفیگ های بزرگ VLAN مثال : روتری شامل 500 VLAN
- کانفیگ های بزرگ static route , dynamic route مثال: روتری با 20000 static route
- شبکه های بزرگ MPLS مثال: شبکه ای شامل 40 روتر که MPLS در آنها فعال است
5. تست هایی با هدف پوشش تغییرات متناوب و متفاوت که ممکن است توسط ادمین در تنظیمات ایجاد شود، اضافه می شود :
- حذف و اضافه کردن پروتکل های روتینگ
- ترکیب و توالی های مختلف از حذف و اضافه کردن تونل ها
- ترکیب و توالی های مختلف از حذف و اضافه کردن اینترفیس ها در VRF

6. تست هایی برای وارد کردن مقادیر اشتباه و نا معتبر که ممکن است توسط ادمین وارد شود، ایجاد می گردد. در این مواقع باید خطاها و یا پیغام های مورد نظر به ادمین داده شود و مشکلی برای روتر بوجود نیاید.
7. تست هایی جهت ارسال ترافیک با پروتکل های مختلف در شبکه وجود دارد.
8. شبکه هایی بزرگ و پیچیده شامل ترکیبی از تمامی ویژگی هایی که در روتر پشتیبانی می شود طراحی می گردد
9. در اکثر تست ها بسته هایی که در نقاط مختلف شبکه در حال انتقال هستند رصد شده و Header های بسته چک می شود که طبق تنظیمات مورد انتظار ,MPLS , ESP , Q-in-Q,GRE,ICMP)...) در شبکه در حال انتقال باشند
10. امکان تولید و ارسال انواع بسته شبکه با هدر های مختلف در سیستم تست وجود دارد که بیشتر برای تست بخش ACL و QoS استفاده می شود.
11. بیشتر تست ها شامل حلقه های تکرار هستند که تست و تنظیمات اعمال شده در روتر ها را تکرار می کنند مثال :
    - قطع و وصل کردن لینک ها
    - اینترفیس های تونل حذف و اضافه می شوند
    - Shutdown /No shutdown کردن اینترفیس
    - تغییر پروتکل های روتینگ و بررسی جدول روتینگ
    - فعال و غیر فعال کردن MPLS در شبکه
    - اعمال و حذف ACL در اینترفیس
12. در کل فرآیند تست پروسس هایی که در روتر باید اجرا باشند یا حذف شوند چک می شود تا صحت عملیاتی که در لایه زیرین سیستم در حال انجام است تایید شود

8.2 انتخاب سخت افزار در روتر سودار

1.8.2 مقدمه

روتر سودار قابلیت اجرا بر روی بسترهای اینتل 64 بیتی و همچنین معماری ARM را داراست. تا کنون این روتر فقط بر روی معمار اینتل تست شده است و در صورت نیاز می توان بر روی بسترهای ARM نیز تست ها انجام پذیرد.

چون روتر دارای استفاده های گوناگون در شبکه های مختلف است، انتخاب سخت افزار نیز بر اساس هر کدام از شرایط می تواند متفاوت باشد. البته اکثر روترهای بازار در رده های مختلف سخت افزار های مختلفی ارائه می کنند که برای محدوده خاصی از امکانات می تواند کارایی داشته باشد.

در اینجا ما ابتدا به قطعات اساسی در سخت افزار به صورت مجزا می نگریم و هر کدام را بررسی می کنیم و سپس برای موارد استفاده معمول به ارائه راه حل می پردازیم

2.8.2 پردازنده

پردازنده، مرکز اصلی انجام عملیات در روتر است و نه تنها جهت انجام عملیات روتینگ بلکه برای برنامه های مختلف موجود در یک روتر مورد استفاده قرار می گیرد. در روتر سودار حداقل یک هسته از پردازنده در اختیار سیستم عامل قرار می گیرد و عملیات مسیریابی در هسته های اختصاصی آن صورت می پذیرد. هسته های پردازنده مورد استفاده در عملیات روتینگ از سیستم عامل ایزوله بوده و اختصاصا برای این منظور مورد استفاده قرار می گیرد. البته بسته در شرایط پیشرفته بسته به کاربردهای مختلف باید تعداد هسته های رزرو شده برای سیستم عامل و همچنین عملیات روتینگ تغییر نماید.

پروسه های مهم سیستم عامل:

1. پروسه های مختلف جهت پروتکلهای روتینگ BGP,OSPF,ISIS,RIP و ...

2. پروسس جهت پروتکل IKE
3. پروسس های مانیتورینگ و مدیریتی

قسمتهای مختلف عملیات مسیریابی نیز می تواند بر روی هسته های مختلف از پردازنده ها مورد استفاده قرار گیرد. به صورت معمول یک هسته پردازنده می تواند برای انجام تمامی عملیات مورد استفاده قرار گیرد ولی در حالت پیشرفته می توان یک هسته را برای عملیات مدیریتی مانند اعمال تغییرات در جداول مسیریابی مورد استفاده قرار داد و هسته های دیگری را به عنوان Worker Thread استفاده میکند که انجام عملیات از ابتدای دریافت از کارت شبکه تا انتهای قرار دادن بر روی کارت شبکه را به عهده می گیرند. در ترافیک های پایین (کمتر از 20G) نیازی به استفاده از worker های متعدد و تنظیم آنها برای کارتهای شبکه خاص خود ضروری نیست و در سرعتهای بالاتر باید تنظیمات مخصوص را انجام داده و پس از تست شرایط از سرعت مورد نظر اطمینان حاصل نماییم.

بنابراین حداقل تعداد هسته های پردازنده برای روترهای ضعیف 2 هسته بوده و بسته به شرایط باید تعداد هسته ها را افزایش داد. البته نوع پردازنده نیز در کارایی روتر تاثیر گذار است که در رده های ضعیف می توان از پردازنده های Atom یا Core I3 استفاده نمود و برای روترهای پر ظرفیت حتما باید از پردازنده های Xeon استفاده گردد. مسائلی که برای انتخاب یک پردازنده در ظرفیتهای بالا تاثیر گذارند می تواند به موارد زیر اشاره نمود:

1. تعداد هسته های پردازنده و همچنین فرکانس کاری هر پردازنده
2. تعداد PCI Express Lane هایی که توسط پردازنده حمایت میشود.
3. مقدار کش پردازنده
4. مواردی مانند ECC در RAM برای اطمینان بیشتر داده های حافظه در روترهای سطح بالا

3.8.2 حافظه

در VPP حافظه مورد نیاز جهت انجام عملیات در ابتدای کار اختصاص می یابد و با این عمل پس از آن برای بسته های عبوری هیچ حافظه ای به صورت پویا از سیستم عامل تخصیص نمی یابد. بنابراین روتر سودار بر اساس سرعت و امکاناتی که مورد استفاده قرار می گیرد نیازمند حافظه اختصاصی می باشد.

مواردی که در VPP دارای تنظیمات حافظه اختصاصی خود می باشد:

1. مقدار حافظه Heap داخلی برای بسته های عبوری در سیستم که بر اساس ظرفیت عبوری روتر متغیر می باشد (پیش فرض 1G)
2. مقدار حافظه اختصاص یافته برای bufferها به ازای هر NUMA.

البته برای کاربردهای عادی زیر 20G نیازی به انجام تنظیم خاص و بهینه سازی تنظیمات نیست و در ترافیک بالاتر و همچنین وابسته به کاربردهای خاص می توان تنظیمات آن را محاسبه نمود و با انجام تست بر روی سخت افزار مورد نظر یک سخت افزار مناسب آن کاربرد ارائه نمود. به عنوان مثال اگر شما نیازمند تعداد رولهای ACL بالایی می باشید باید از تنظیمات اختصاصی حافظه برای این رولها نیز استفاده نمایید.

البته سیستم عامل و پروتکلهای روتینگ درون سیستم عامل نیز نیازمند حافظه جداگانه هستند که وابسته به تعداد حداکثر روتهای مورد استفاده در هر روتر باید 3 برابر حافظه مورد استفاده برای جداول روتینگ در نظر گرفت:

1. حافظه هر واحد روت در جدول روتینگ لینوکس
2. حافظه هر واحد روت در پروتکل مسیریابی
3. حافظه هر واحد روت در جدول روتینگ VPP

بر اساس مطالب گفته شده حداقل حافظه مورد نیاز برای روتر سودار 4G می باشد. البته برای روترهای ضعیف تر (زیر 10G) می توان مقدار حافظه کمتری نیز در نظر گرفت.

4.8.2 فضای ذخیره سازی

روتر سودار فقط برای لاگها و سیستم عامل اولیه به فضای ذخیره سازی نیازمند است بنابراین محاسبه خاصی برای این قسمت لازم نیست و حداقل 64G فضای ذخیره سازی برای کاربرد ما کفایت می کند مگر اینکه بخواهیم لاگها به صورت طولانی مدت بر روی روتر ذخیره گردد که می توان فضای لازم را به این مقدار افزود.

5.8.2 کارتهای شبکه

در کاربردهای زیر 20G کارتهای شبکه زیاد تاثیر گذار نیستند ولی برای زمانی که ما کارتهای شبکه بالای 10G مورد استفاده قرار می دهیم نیاز است تطبیق پذیری کارت شبکه با VPP مورد بررسی قرار گیرد. البته کارتهای شبکه بالای 10G از سازندگان زیر در vpp حمایت می گردد:

- Intel
- Mellanox

6.8.2 شرایط سخت افزاری دیگر

البته بر اساس حساسیت مکان مورد استفاده از روتر و همچنین کاربردهای آن می توان شرایط دیگری برای سخت افزار مد نظر گرفت. مثلا سخت افزار Rack Mount باشد یا Desktop. یا اینکه Power Redundancy داشته باشد. و مواردی از این قبیل که برای هر نوع سخت افزاری این موارد می تواند لازم باشد و ارتباطی با روتر ندارد بنابراین نیازی به عنوان کردن ندارد.

7.8.2 نمونه سخت افزار برای کاربرد روتر عمومی

کاربرد نوع lrsphinxstyletheadfamily	پردازنده حداقل lrsphinxstyletheadfamily	حداقل RAM
10G زیر ظرفیت کم روتر	Atom یا Corei3 های پردازنده	4GB
20G زیر ظرفیت کم روتر	Corei7 های پردازنده	8GB

9.2 تست سرعت

این گزارش مربوط به نسخه 20.19 سودار بوده و نمونه گزارش تست کارایی روتر سودار بر اساس شرایط مختلف برای مقیاس پذیری تنظیمات و بر روی کارت‌های شبکه Gigabit Ethernet میباشد.

IPv4 Tagged	VLAN های تگ با IP4 تست
IPv4 Base	پایه IP4 تست
IPv4 20K FIB	مسیر هزار 20 با مسیریابی جدول با IP4 تست
IPv4 200K FIB	مسیر هزار 200 با مسیریابی جدول با IP4 تست
IPv4 1 Rule IACL 10K Flow	روتر از داده جریان هزار 10 عبور و فایروال رول یک با IP4 تست
IPv4 50 Rule IACL 10K Flow	روتر از داده جریان هزار 10 عبور و فایروال رول 50 با IP4 تست
IPv4 NAT44	NAT با IP4 تست
L2 BD Tagged	VLAN تگ و Bridge با 2 لایه تست
L2 BD Base	VLAN تگ و Bridge با 2 لایه تست
L2 BD 10K MAC Table	MAC Table در MAC آدرس هزار 10 با Bridge با 2 لایه تست
L2 BD 100K MAC Table	MAC Table در MAC آدرس هزار 100 با Bridge با 2 لایه تست

تست ها بر اساس سایزهای مختلف بسته صورت پذیرفته است. توجه شود که در بسته های 64 بایتی، به علت محدودیت فیزیکی کارت شبکه، نمی توان کل خط را پر نمود. بنابراین در این سرعت مقادیر عدد پایین تری را نشان میدهد. در صورتی که تعداد بسته در ثانیه تبادل شده در این طول بسته به بیش از 5.1 میلیون بسته در ثانیه می‌رسد.

سایز بسته IMIX: منظور شبیه سازی از طول بسته های مختلف است که یک معادل تقریبی از ترافیک معمول در اینترنت است. فرمول ترکیب IMIX به صورت زیر است:

- 4 بسته 1518 بایتی
- 16 بسته 570 بایتی
- 28 بسته 64 بایتی

NDR: کارایی بر این اساس است که نباید هیچ بسته‌ای در روتر از بین برود.

PDR: کارایی بر این اساس است که می توانیم تا 0.5 درصد اتلاف بسته داشته باشیم.

**

**

1.9.2 : گیگابیت در ثانیه (Gbps) به صورت Full-duplex

نوع/سایز	64B	1518B	9000B	IMIX
IPv4 Tagged	1.052	1.984	1.999	1.887
IPv4 Base	1.135	1.990	1.990	1.868
IPv4 20K FIB	1.145	1.990	1.990	1.868
IPv4 200K FIB	1.137	1.990	1.992	1.881
IPv4 1 Rule IACL 10K Flow	1.148	1.990	1.990	1.887
IPv4 50 Rule IACL 10K Flow	1.140	1.990	1.990	1.887
IPv4 NAT44	1.137	1.990	1.990	1.882
L2 BD Tagged	1.045	1.984	1.989	1.868
L2 BD Base	1.134	1.990	1.990	1.876
L2 BD 10K MAC Table	1.113	1.990	1.990	1.885
L2 BD 100K MAC Table	1.121	1.990	1.990	1.866

2.9.2 **PDR**: گیگابیت در ثانیه (**Gbps**) به صورت **Full-duplex**

IMIX	9000B	1518B	64B	نوع/سایز
1.915	1.999	1.994	1.057	IPv4 Tagged
1.915	2.000	2.000	1.169	IPv4 Base
1.915	2.000	2.000	1.172	IPv4 20K FIB
1.919	2.000	2.000	1.163	IPv4 200K FIB
2.000	2.000	2.000	1.164	IPv4 1 Rule IACL 10K Flow
1.915	2.000	2.000	1.180	IPv4 50 Rule IACL 10K Flow
1.920	2.000	2.000	1.170	IPv4 NAT44
1.915	1.999	1.994	1.060	L2 BD Tagged
1.914	2.000	2.000	1.157	L2 BD Base
1.914	2.000	2.000	1.145	L2 BD 10K MAC Table
1.913	2.000	2.000	1.132	L2 BD 100K MAC Table

3.9.2 **NDR**: بسته منتقل شده در ثانیه (**PPS**) به صورت **Full-duplex**

IMIX	9000B	1518B	64B	نوع/سایز
631.0 Kpps	27.70 Kpps	162.1 Kpps	1.565 Mpps	IPv4 Tagged
627.9 Kpps	27.71 Kpps	162.5 Kpps	1.694 Mpps	IPv4 Base
627.7 Kpps	27.71 Kpps	162.5 Kpps	1.709 Mpps	IPv4 20K FIB
632.4 Kpps	27.71 Kpps	162.5 Kpps	1.700 Mpps	IPv4 200K FIB
631.0 Kpps	27.71 Kpps	162.5 Kpps	1.717 Mpps	IPv4 1 Rule IACL 10K Flow
634.1 Kpps	27.71 Kpps	162.5 Kpps	1.705 Mpps	IPv4 50 Rule IACL 10K Flow
632.5 Kpps	27.71 Kpps	162.5 Kpps	1.701 Mpps	IPv4 NAT44
627.7 Kpps	27.70 Kpps	162.1 Kpps	1.562 Mpps	L2 BD Tagged
630.5 Kpps	27.71 Kpps	162.5 Kpps	1.696 Mpps	L2 BD Base
633.7 Kpps	27.71 Kpps	162.5 Kpps	1.665 Mpps	L2 BD 10K MAC Table
627.1 Kpps	27.57 Kpps	162.5 Kpps	1.676 Mpps	L2 BD 100K MAC Table

4.9.2 **PDR**: بسته منتقل شده در ثانیه **(PPS)** به صورت **Full-duplex**

نوع/سایز	64B	1518B	9000B	IMIX
IPv4 Tagged	1.573 Mpps	162.1 Kpps	27.70 Kpps	640.4 Kpps
IPv4 Base	1.739 Mpps	162.5 Kpps	27.71 Kpps	640.6 Kpps
IPv4 20K FIB	1.744 Mpps	162.5 Kpps	27.71 Kpps	640.4 Kpps
IPv4 200K FIB	1.731 Mpps	162.5 Kpps	27.71 Kpps	641.9 Kpps
IPv4 1 Rule IACL 10K Flow	1.732 Mpps	162.5 Kpps	27.71 Kpps	637.4 Kpps
IPv4 50 Rule IACL 10K Flow	1.757 Mpps	162.5 Kpps	27.71 Kpps	640.5 Kpps
IPv4 NAT44	1.742 Mpps	162.5 Kpps	27.71 Kpps	642.1 Kpps
L2 BD Tagged	1.578 Mpps	162.1 Kpps	27.70 Kpps	640.4 Kpps
L2 BD Base	1.722 Mpps	162.5 Kpps	27.71 Kpps	640.1 Kpps
L2 BD 10K MAC Table	1.703 Mpps	162.5 Kpps	27.71 Kpps	640.1 Kpps
L2 BD 100K MAC Table	1.684 Mpps	162.5 Kpps	27.71 Kpps	639.8 Kpps

10.2 سیستم عامل سودار و سرور به روز رسانی

1.10.2 مقدمه

سیستم عامل به عنوان بستر اجرایی تمامی سرویس ها و برنامه ها نقش به سزایی در امنیت و پایداری محصولات ایفا می کند. از سوی دیگر نبود سیستم به روز رسانی برخط، منجر به مشکلات فراوانی در توسعه و نگهداری شبکه می گردد. وجود یک سرور به روز رسانی برخط باعث می شود که به سرعت مسائل امنیتی بوجود آمده را در شبکه برطرف نماییم یا اینکه بتوانیم امکانات جدید را به آسانی در شبکه خود مهیا نماییم. البته مسائل امنیتی و قابلیت اعتماد فرایند به روز رسانی بسیار مهم است.

2.10.2 ساختار اصلی

تمامی مکالمات بین نودها و سرور به روز رسانی با HTTPS صورت می پذیرد و Auth نودها صورت می پذیرد. که در قسمت امنیت به آنها پرداخته ایم.

3.10.2 فرایند به روز رسانی

به ازای هر به روز رسانی یک فایل مخصوص تولید می شود که به امضای سیستم به روز رسانی رسیده است. این تصویر سپس به صورت آفلاین به سرور به روز رسانی منتقل می گردد و در آنجا به عنوان یک نسخه جدید ثبت می گردد. سپس بر اساس برنامه ریزی مورد نظر به روز رسانی شروع می شود هر بار می توان چند نود را به روز رسانی کرد یا تمامی نودها را یکجا به روز رسانی نمود. این فرایند در شکل زیر آمده است.

4.10.2 پایه سیستم عامل

در این محصول از yocto برای ایجاد سیستم عامل اختصاصی استفاده می شود. بر این اساس تمامی قسمتهای سیستم عامل به صورت اختصاصی بر روی هم گذاشته میشود تا امن ترین و کاراترین سیستم عامل را داشته باشیم. بنابراین برای هر سخت افزار مجزا ما یک سیستم عامل اختصاصی آن سخت افزار ارائه می کنیم و تمامی خصوصیات سخت افزاری را در زمان ساخت سیستم عامل مدنظر می گیریم.

Yocto یک بستر سازنده سیستم عامل است که شما با استفاده از آن می توانید سیستم عامل اختصاصی خودتان را بسازید. این محصول یک اکوسیستم انعطاف پذیر را برای توسعه دهندگان سیستم های embedded ایجاد کرده است تا بتوانند سیستم عاملهای سفارشی شده بر اساس لینوکس ایجاد کنند.

بر اساس این بستر آخرین نسخه های تمامی نرم افزارهای سازنده سیستم عامل در زمان ایجاد، داونلود میشود و بر اساس تنظیماتی که از قبل مشخص کرده ایم کامپایل می شوند و در نهایت ما تصویر قابل نصب سیستم عامل رو به عنوان خروجی داریم تا برای نصب نهایی بر روی نودها استفاده شود.

سیستم عامل نهایی دارای فایل سیستم فقط خواندنی در ریشه خود می باشد و مواردی که باید در طول زمان تغییر کنند در پارتیشن های دیگری نصب می گردد. مواردی مانند تنظیمات و log ها. فایل سیستم فقط خواندنی هم امنیت سیستم را افزایش می دهد هم برای به روز رسانی روش A/B مورد نیاز است.

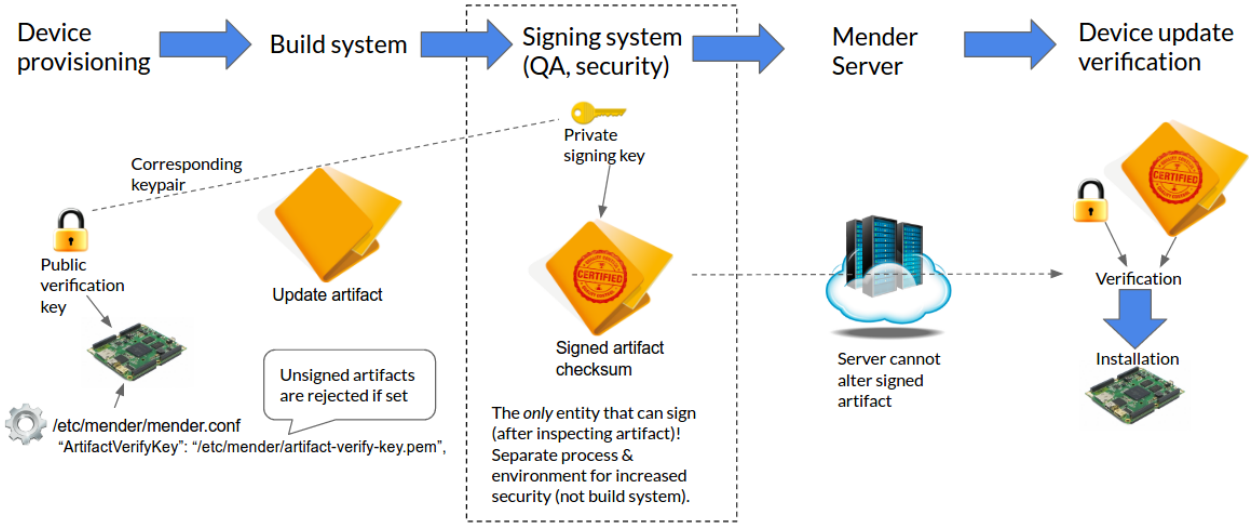
5.10.2 فرآیندهای امنیتی

در اینجا به فرآیندهای امنیتی درون سیستم پرداخته می شود. قبلا در قسمت ساختار اصلی به برخی مسائل امنیتی پرداخته شده است و ما در اینجا مسائل باقیمانده را مطرح می کنیم.

امنیت فایلهای به روز رسانی

در این ساختار باید فرآیند به روزرسانی به صورت ایمن صورت پذیرد. بخش مهمی از امنیت به روز رسانی مربوط به تایید فایلهای نهایی است که قرار است بر روی نود نصب شود. بنابراین نودها باید قادر باشند منبع تهیه این فایلها را تایید نمایند و مطمئن شوند که از یک منبع قابل اعتماد صادر گردیده است.

یکی از راه های دستیابی به این هدف ، امضای فایلهای به روز رسانی با استفاده از یک کلید خصوصی محافظت شده است. در هر نود ما کلید عمومی مربوط به سیستم تولید کننده فایلهای به روز رسانی را نگهداری می کنیم و به محض دریافت فایل مربوطه امضای آن را بررسی نموده و از صحت آن مطمئن می شویم. اگر امضا تایید شد، به روزرسانی از یک منبع قابل اعتماد صورت گرفته است. نمودار زیر جریان سطح بالایی از ایجاد و مدیریت کلیدها و امضاها را نشان می دهد که بخش اساسی فرآیند امضا و تایید فایلهای به روز رسانی است.



در طی مراحل نصب به روزرسانی ، دستگاه با استفاده از کلید عمومی ذخیره شده در دستگاه فایلهای به روز رسانی را تایید می کند. این به روز رسانی تنها در صورت موفقیت آمیز بودن این فرایند انجام می شود. اگر این فایلها امضا نشده بود یا تأیید انجام نشود، روند بروزرسانی قطع می شود و دستگاه خطایی را به سرور به روز رسانی گزارش می دهد.

الگوریتم های امضای پشتیبانی شده به صورت زیر است:

- RSA with recommended key length of at least 3072 bits
- ECDSA with curve P-256

فرایند تایید دستگاهها و اعتبار سنجی آنها

یک دستگاه یا یک سخت افزار مشخص دارای یک مشخصه منحصر به فرد است که آن را از دیگر سخت افزارها مجزا می سازد. این شناسه منحصر به فرد توسط مجموعه ای از خصوصیات هویتی (آدرس های MAC ، UID های تعریف شده توسط کاربر و غیره) مشخص می شود. برای به دست آوردن یک توکن اعتبار سنجی، دستگاه درخواست احراز هویت را که حاوی خصوصیات هویتی خود و کلید عمومی فعلی آن است، ارسال می کند. این درخواست با کلید خصوصی نود مربوطه امضا شده است (این کلید در دستگاه مخفی نگه داشته می شود) و سرور از کلید عمومی نود برای تأیید امضا استفاده می کند.

ممکن است یک دستگاه واحد به مرور زمان کلیدهای مختلفی را ارائه دهد، و مهم است که آن ها را نگهداری کرده و مدیر شبکه باید این اجازه اتصال را بپذیرد.

به روز رسانی هر دستگاه را به عنوان یک موجود در دنیای واقعی نگهداری کرده و همچنین مجموعه های تایید هویت متعدد آن (رابطه یک به چند) را نیز نگه می دارد.

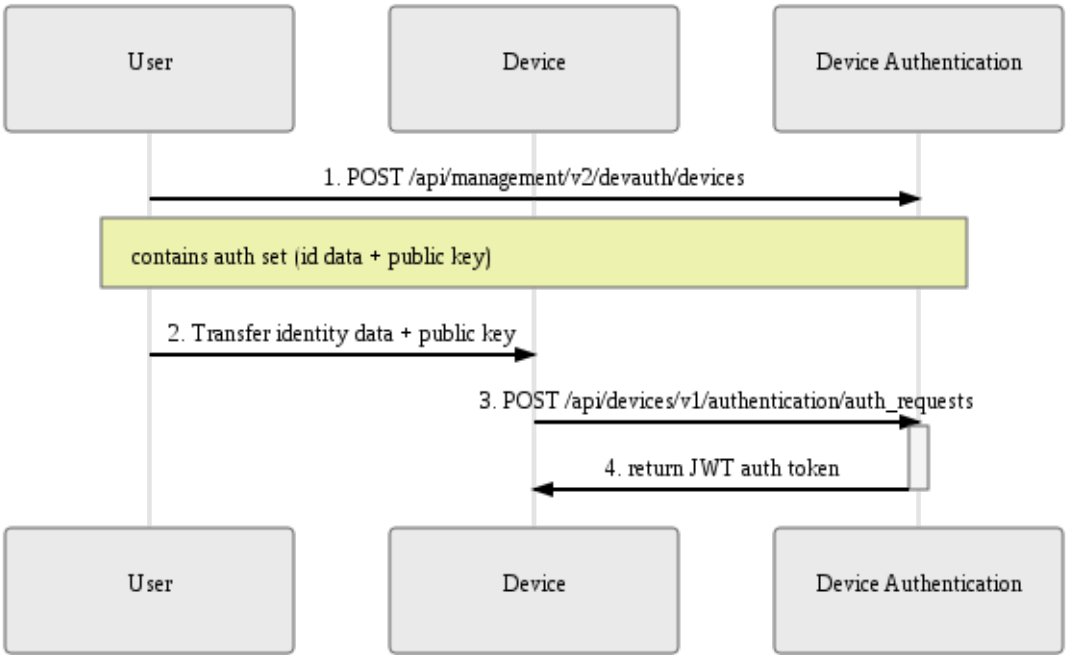
دو جریان مجوز دهی به نود ها وجود دارد که هر دو روش نیازمند رضایت صریح مدیر شبکه می باشد. در زیر شرح مفصلی از هر یک از آنها آورده شده است.

تایید از قبل نودها

در این روش قبل از اینکه نود برای اولین بار به سرور وصل شود، اجازه آن صادر می گردد. این مدل مشابه ایجاد حساب قبل از ورود به یک سرویس آنلاین است.

روال پیش تایید می تواند حتی قبل از استقرار نود انجام شود. کافی است کاربر یک مجموعه احراز هویت از پیش تعیین شده را در سرور وارد نماید. حالا هر زمانی که یک دستگاه با خصوصیات هویتی و کلید عمومی از قبل تایید شده درخواست تأیید اعتبار کرد بلافاصله و بدون مداخله مدیر شبکه، تایید می گردد. این حالت برای حالتی که تعداد دستگاهها زیاد است می تواند بسیار مفید باشد.

- هویت/کلیدهای دستگاه از قبل تعیین شده و در خارج از سرور به روز رسانی مدیریت می شوند
- از یک برنامه می توان برای افزودن اطلاعات هویتی و کلید عمومی این دستگاهها به سرور به روز رسانی استفاده نمود
- در زمان تولید نود می توان فایلهای هویتی و کلید های عمومی و خصوصی آن را به دستگاه منتقل نمود. این کار می تواند توسط توکن سخت افزاری صورت پذیرد.
- پس از اولین درخواست تأیید اعتبار ، هر دستگاه احراز هویت می شود و می تواند از سرور به روز رسانی استفاده نماید.



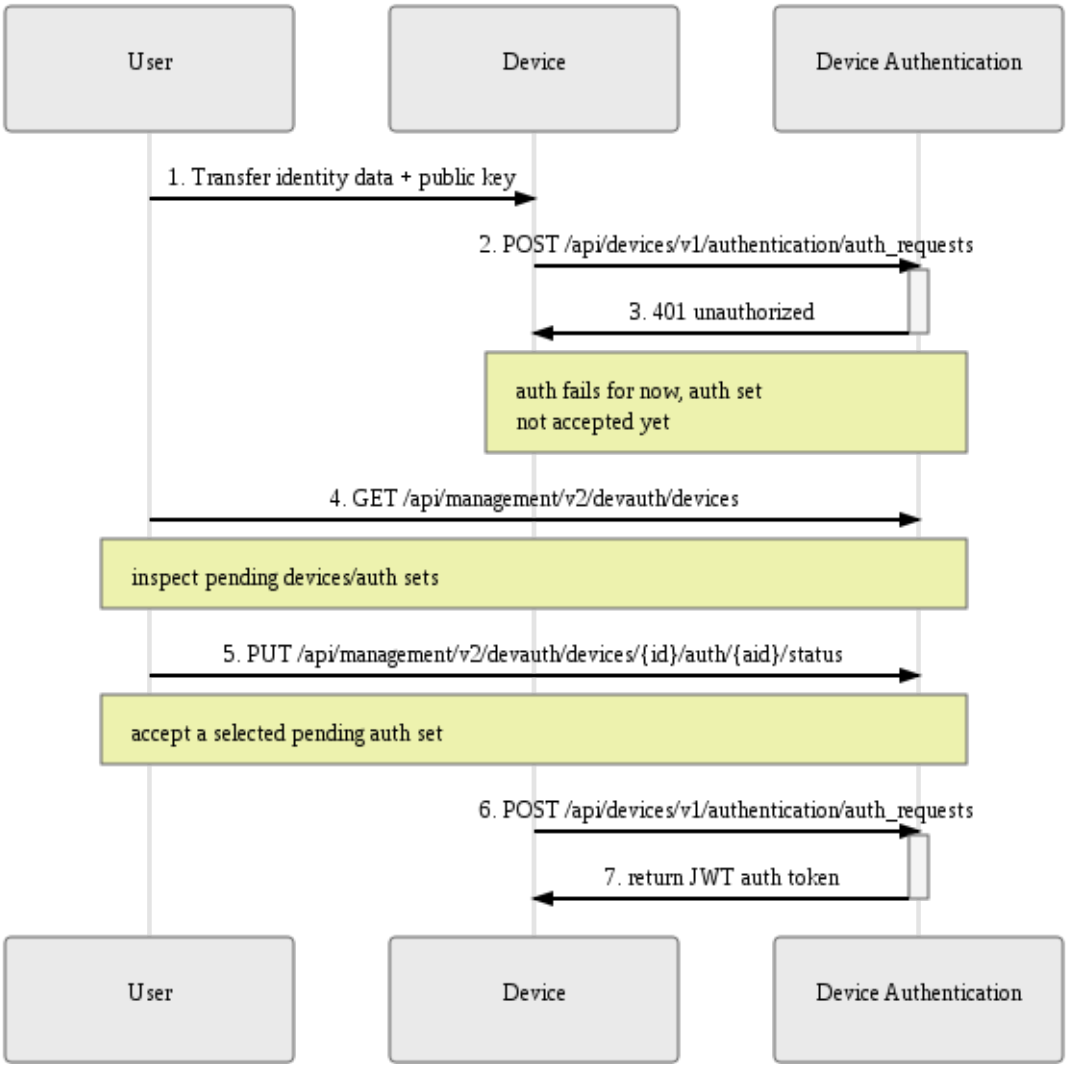
در تصویر بالا این روال را مشاهده می کنید.

پس از اخذ مجوز توسط دستگاه، درخواست Auth بعدی آن منجر به دریافت یک توکن احراز هویت می شود. این توکن توسط کلاینت یا همان نود ذخیره شده و آن را در هر اتصال به سرور به روز رسانی در هدر Authorization در درخواست HTTP قرار می دهد.

هر توکن دارای یک تاریخ انقضا (یک دوره یک هفته ای) است ، اما دستگاه پس از این دوره به صورت خودکار یک توکن جدید دریافت می کند. این روند بدون دخالت مدیر شبکه صورت می پذیرد.

تایید پس از اتصال نود

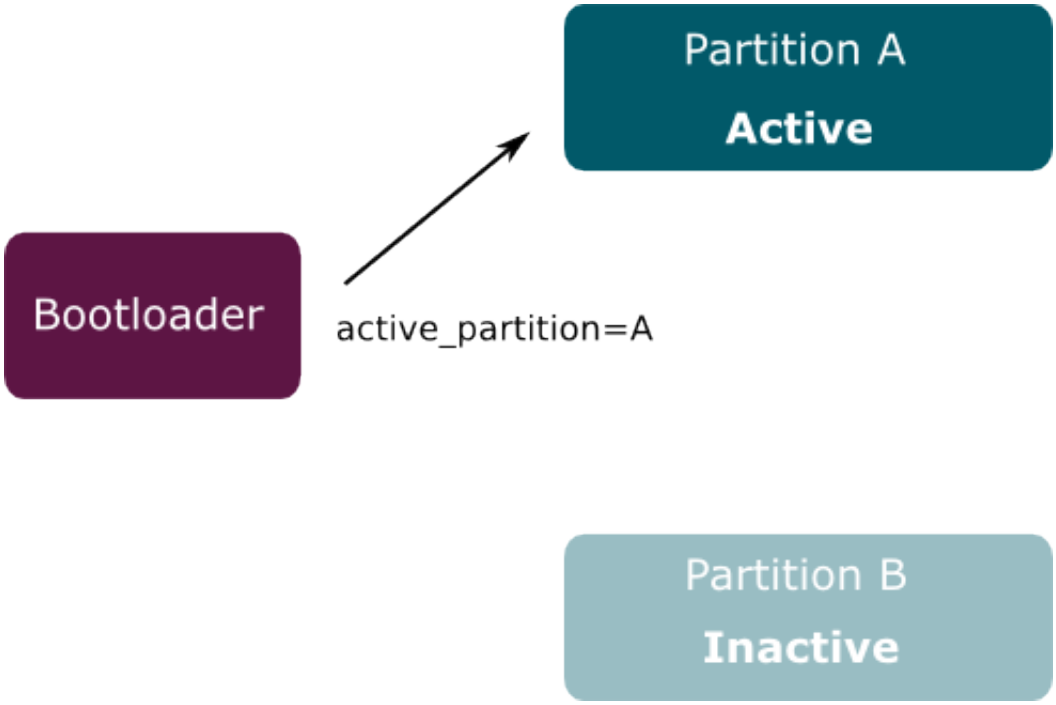
در این حالت نودها بعد از اتصال به سرور به روز رسانی در لیست انتظار برای تایید قرار می گیرند. سپس مدیر با کنسول وب به این دستگاهها اجازه اتصال می دهد. از این پس این دستگاهها قادر خواهند بود از سرور به روز رسانی استفاده نمایند.



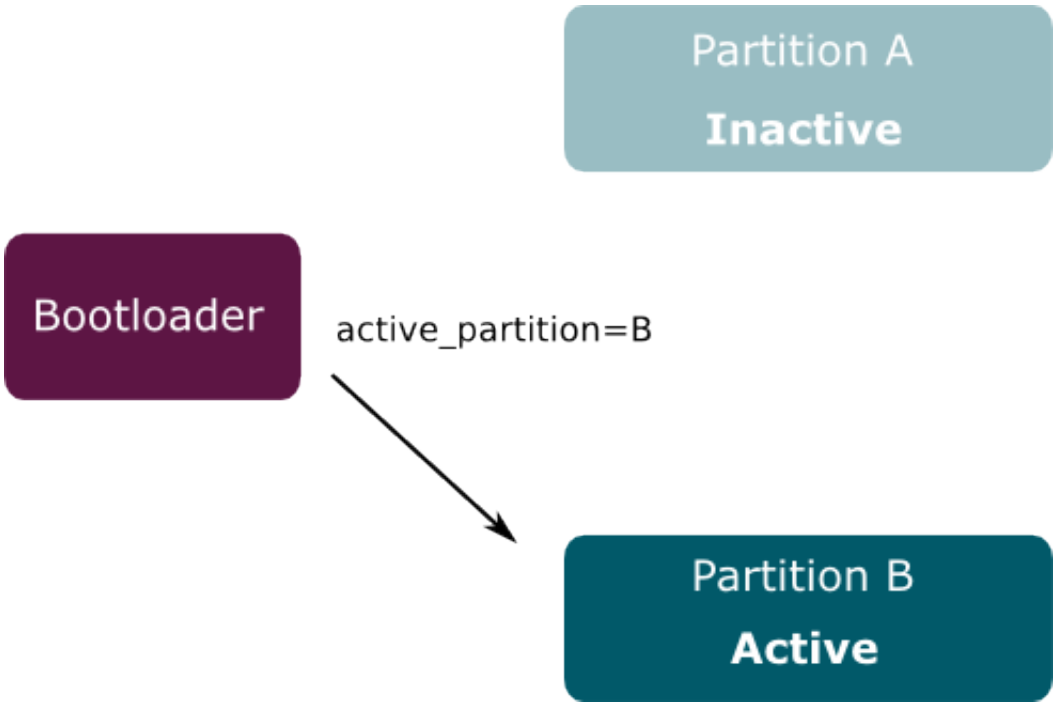
6.10.2 سیستم به روز رسانی

به روز رسانی در این سیستم عامل بر پایه نرم افزار Mender صورت می پذیرد که در قسمتهای مختلف آن تغییرات مورد نظر اعمال شده است. یکی از نیازهای اصلی بروزرسانی این است که این به روز رسانی باید به صورت مطمئن صورت پذیرد. اگر به هر دلیلی از جمله قطعی برق یا قطعی اتصال شبکه این به روز رسانی ناتمام بماند سیستم قابل بازیابی باشد و به حالت قبلی خودش برگردد.

بدین منظور از یک سیستم به روز رسانی دوگانه استفاده می گردد که برای سیستم عامل همزمان دو پارتیشن مورد استفاده قرار می گیرد که در زمان نصب هر دو پارتیشن یکسان بوده و دارای یک نسخه از سیستم عامل می باشد. و در ابتدا از یک پارتیشن استفاده می شود و یک پارتیشن دیگر برای به روز رسانی نگهداری می شود. به بخشی که در حال استفاده است پارتیشن فعال گفته می شود و نسخه پشتیبان آن پارتیشن غیرفعال نامیده می شود. هنگامی که سیستم عامل بوت می شود ، توسط بوت لودر از پارتیشن فعال استفاده می کند.

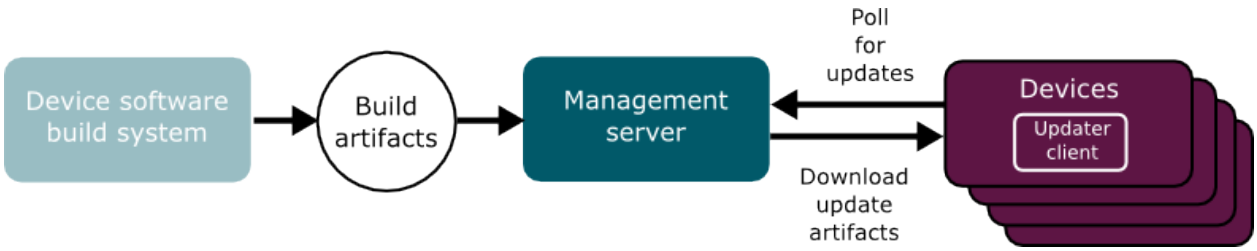


وقتی قرار است سیستم به روز رسانی شود بدون اینکه اختلالی در کار نود ایجاد شود پارتیشن غیر فعال به روز رسانی می شود و پس از اتمام به روز رسانی به این پارتیشن ریبوت می شود. اگر بعد از بوت شدن از پارتیشن جدید همه چیز به خوبی پیش رفت این پارتیشن به عنوان پارتیشن فعال در نظر گرفته میشود و پارتیشن فعال قبلی به صورت پشتیبان در می آید و اگر مشکلی پیش آمد مجددا به پارتیشن فعال قبلی برمی گردد و به روز رسانی ناموفق اعلام میگردد. همچنین اگر چیزی باعث شود که دستگاه قبل از انجام بروزرسانی مجدداً reboot مجدد شود ، bootloader می داند که اشتباهی رخ داده است ، و با چرخاندن دوباره پارتیشن های فعال و غیرفعال دوباره به نسخه قبلی برمی گردد.



بروزرسانی تمام فایلهای موجود در سیستم عامل را با نسخه های جدید جایگزین می کند، بنابراین فایل سیستم ریشه در سیستم عامل به صورت غیر قابل نوشتن است.

نمودار زیر نمای کلی از جریان داده ها در به روز رسانی نرم افزار را نشان می دهد.



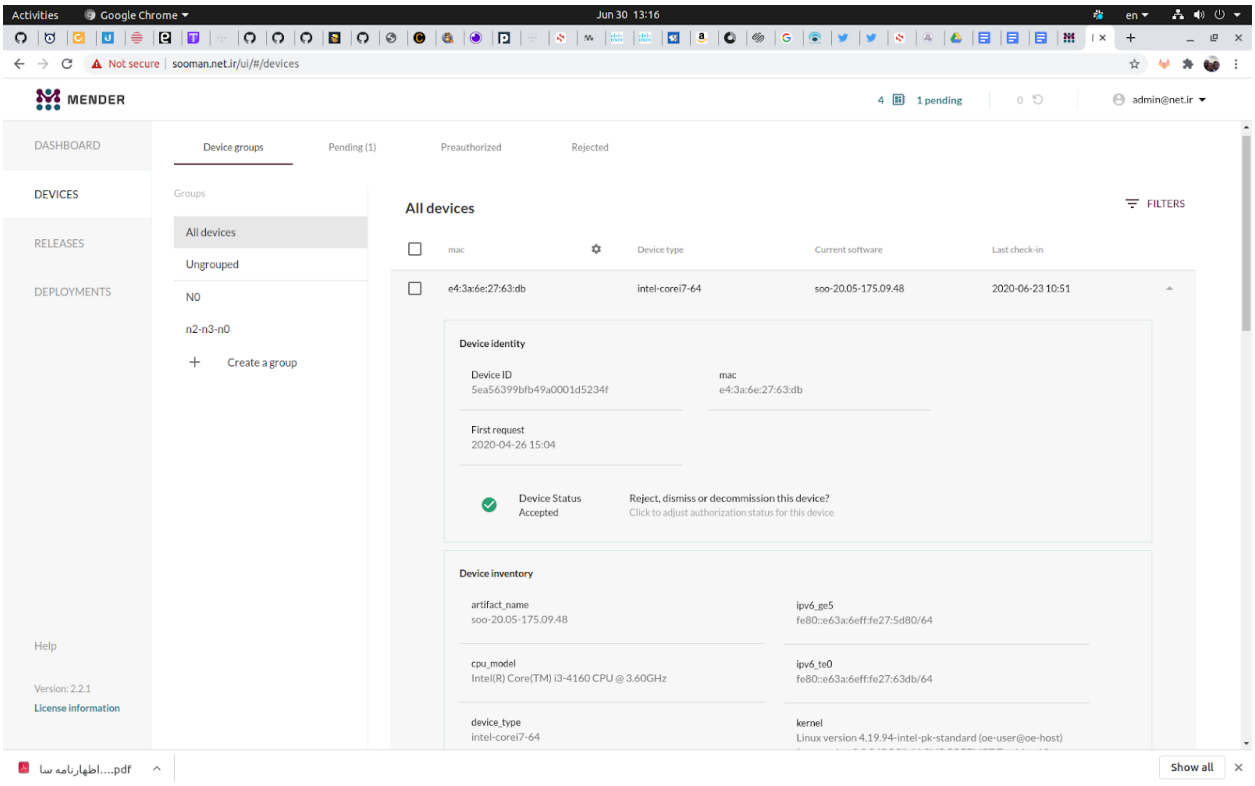
این فرآیند با تولید نسخه جدید سیستم عامل توسط Yocto برای یک دستگاه آغاز می شود. خروجی به روز رسانی به صورت یک فایل در قالب مورد نیاز دستگاه هدف ایجاد می گردد. برای هر نوع دستگاه مدیریت شده ، فایل به روز رسانی مجزا تولید می گردد. این فایلها امضای الکترونیکی میگردد و قابلیت تغییر ندارد. و در صورت خرابی یا تغییر در آن توسط نودهای نهایی نصب نمی گردد.

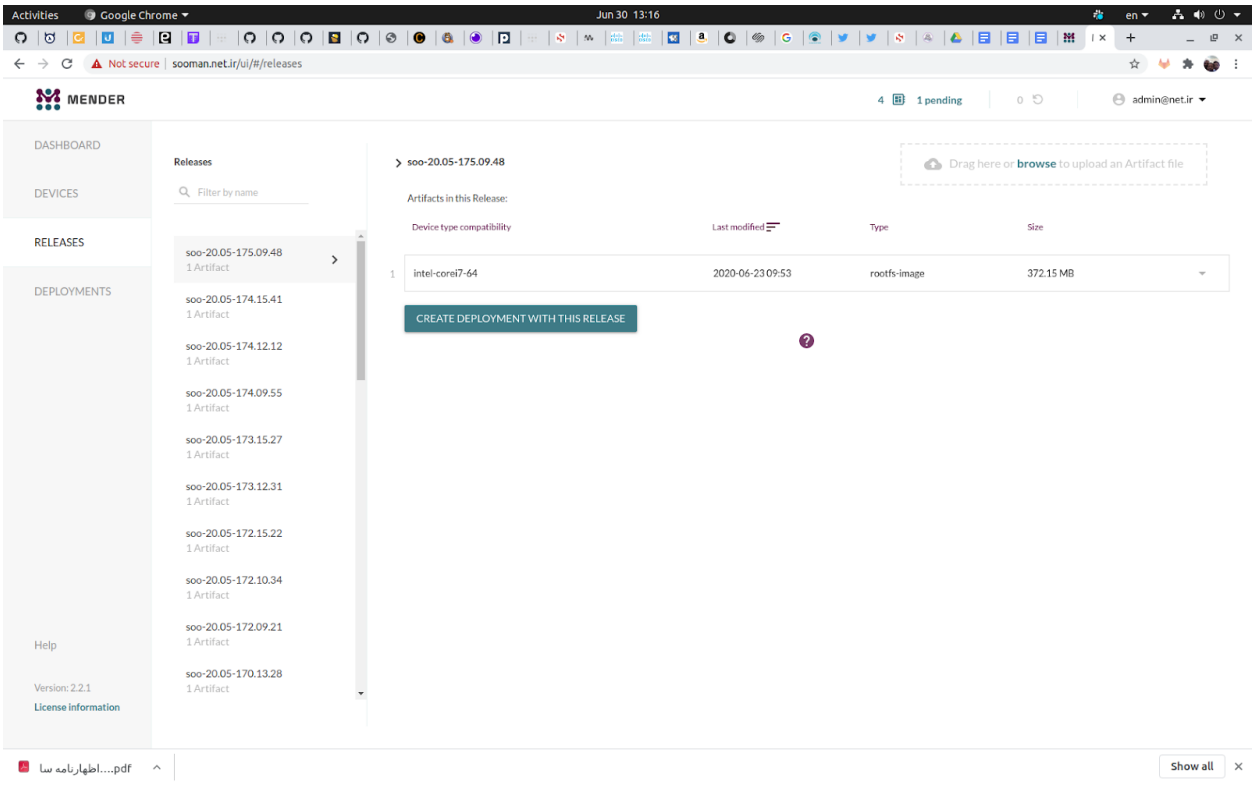
امکانات سرور به روز رسانی

تمامی نودها بعد از تنظیم جهت دریافت به روز رسانی های خود به سرور متصل شده و اطلاعات کلی خود را ارائه می کنند

اطلاعاتی از قبیل مدل پردازنده و ویرایش سیستم عامل موجود بر روی آن نود به سرور به روز رسانی ارسال می گردد.

در سرور مدیر می تواند این دستگاه را بررسی نموده و پس از تایید مشخصات آن را به عنوان دستگاه قابل اعتماد قبول نماید. از این پس این دستگاه می تواند در لیست دستگاهها برای دریافت ویرایش های جدید قرار گیرد.





هر به روز رسانی جدید می تواند بر روی گروه خاصی از نودها فعال گردد بدین صورت که شما می توانید ابتدا یک نود کم اهمیت تر را به روز رسانی نمایید و در صورت تست و عدم وجود مشکل آن را به چند نود دیگر اعمال نمایید و در نهایت در زمان مناسب به روز رسانی را در نودهای اصلی انجام داد.

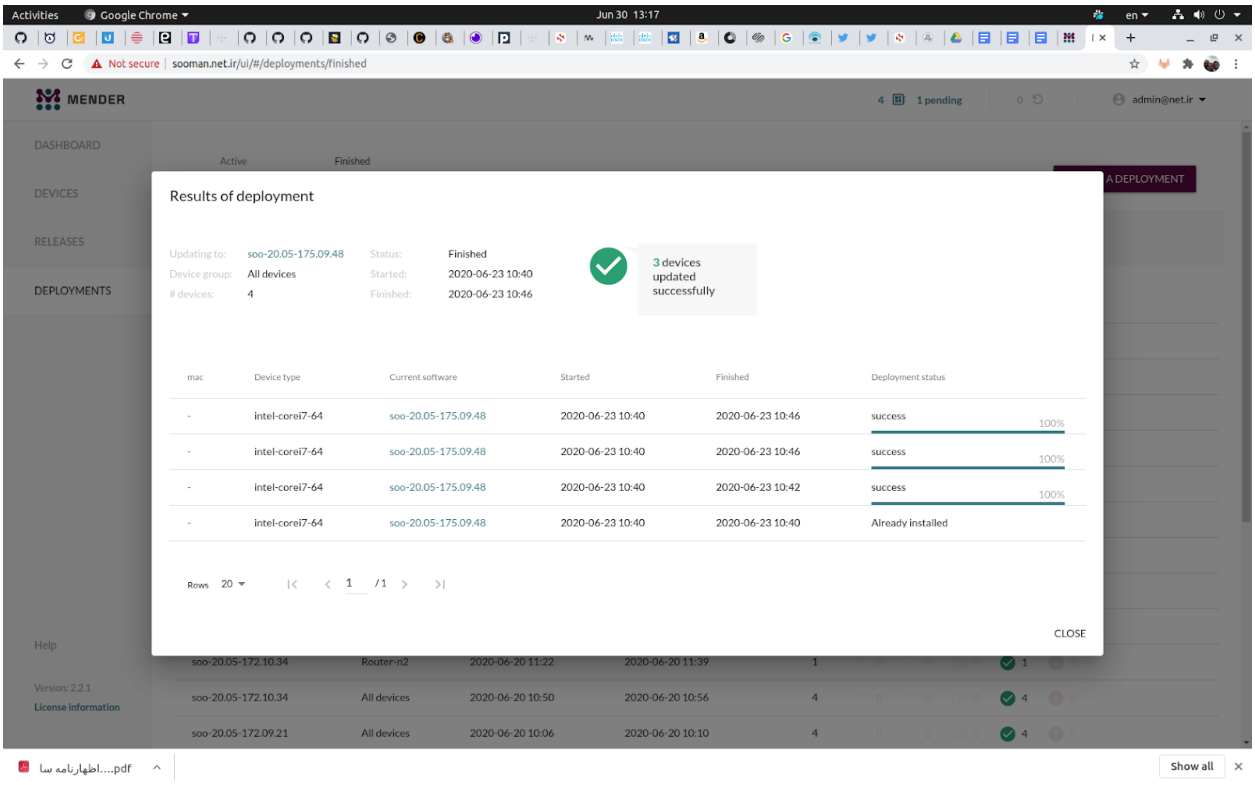
در نهایت مدیر می تواند وضعیت نودهای به روز شده را مشاهده نماید و لیستی از به روز رسانی های موفق و ناموفق را داشته باشد. همچنین علت عدم موفقیت را می تواند دریافت نماید.
.png4lrsphinxincludegraphicsmender-

به روز رسانی برخط

در این روش یک سرور به روز رسانی برای هر شبکه ارائه می گردد که در سمت شبکه خصوصی قرار می گیرد. این سرور بر پایه نرم افزار Mender میباشد. در این روش فایلهای به روز رسانی به سرور مدیریت به روز رسانی ها منتقل می شود، که نقطه اصلی برای به روزرسانی برای دستگاه های مختلف است. سرور Mender نرم افزار فعلی که بر روی هر دستگاه نصب شده است را پایش می کند و لیست نسخه های جدید را می توان برای گروههای مختلف از نوده برنامه ریزی نمود.

هر نود در یک بازه زمانی به سرور به روزرسانی سرکشی میکند و اطلاعات کلی از خودش ارایه می کند و همچنین از سرور میخواهد که در صورت وجود به روز رسانی جدید اعلام نماید.

البته این سرکشی می تواند با فرمان مدیر از طریق manager صورت پذیرد. یعنی نودها به صورت غیر فعال کار می کنند و زمانی که مدیر به یک نود دستور داد که به روز رسانی شود این کار را انجام می دهد.



**

**

11.2 مقایسه امکانات سودار با سیسکو

1.11.2 مقایسه امکانات

سرور DHCP:

- پشتیبانی از DHCP Client
- پشتیبانی از DHCP Server

سرور DNS: روتر سودار به عنوان سرور DNS نمیتواند مورد استفاده قرار گیرد. و تعبیه سرور DNS درون روتر می تواند مشکلات امنیتی عدیده ای برای شبکه ایجاد نماید. در حال حاضر در سودار میتوان به شکل ایستا تناظر یک به یک بین Hostname و IP تعریف کرد.

سرویس NAT: پشتیبانی از سرویس NAT در روتر سودار به شرح زیر است:

- پشتیبانی از Dynamic Translation
- پشتیبانی از Static Translation
- عدم پشتیبانی از Network static translation
- عدم پشتیبانی از دستورات ip nat outside: میتوان با قرار دادن یک اینترفیس در inside و outside به صورت همزمان و تعریف رول‌های outside به شکل inside به نحوی این کاستی را جبران کرد.

- عدم پشتیبانی از پارامترهای extendable، interface ,no-alias

سرویس NTP:

- پشتیبانی از NTP Version 3 / 4
- پشتیبانی از NTP Client
- عدم پشتیبانی از NTP Peering
- عدم پشتیبانی از NTP Server

برای امنیت بیشتر بهتر است از روتر برای سرور NTP استفاده نشود.

سرویس VRRP: در روتر سودار پشتیبانی نمی گردد.

مسیریابی OSPF:

- عدم پشتیبانی از Traffic Engineering(در صورت نیاز قابل پیاده‌سازی می‌باشد).

مسیریابی BGP:

- پشتیبانی از IPv4 Unicast و IPv6 Unicast
- پشتیبانی از L3VPN
- عدم پشتیبانی از EVPN

PBR:

- پشتیبانی از Route-map ها
- عدم پشتیبانی از PBR

سرویس MPLS:

- پشتیبانی از LDP
- عدم پشتیبانی از RSVP و Traffic engineering
- پشتیبانی از VPLS

سرویس Multicast:

- فعال بودن به شکل پیش فرض
- پشتیبانی از PIM در حالت Sparse mode

سرویس QoS:

- پشتیبانی از class-map
- پشتیبانی از match ACL
- پشتیبانی از match L3/L4 header params
- عدم پشتیبانی از match L2 params
- پشتیبانی از policy-map
- پشتیبانی از Policer
- عدم پشتیبانی از Shaper
- عدم پشتیبانی از bandwidth
- عدم پشتیبانی از fair-queue
- عدم پشتیبانی از priority
- عدم پشتیبانی از queue limit

- عدم پشتیبانی از random-detect
- عدم پشتیبانی از policy-map chaining
- عدم پشتیبانی از set-dscp(در policer میتوان set-dscp کرد)
- عدم پشتیبانی از set-mpls-experimental

سرویس SNMP: تمرکز اصلی روتر سودار برای ارائه اطلاعات مانیتورینگ بر روی سرویس Prometheus میباشد. اما پشتیبانی از SNMP نیز در دستگاه موجود است. با توجه به پشتیبانی از سرویس SNMP تنها در حالت RO و تنها Version 3، قابلیت تعریف SNMP Group و SNMP Community در دستگاه گنجانده نشده است و از یک گروه پیش فرض برای تمام کاربران استفاده میشود. همچنین SNMP Traps نیز در دستگاه غیر فعال است و نیازی به تعریف SNMP Host نمیباشد.

سرویس Netflow: روتر سودار از تکنولوژی جدیدتر و بروزتر IPFIX برای رهگیری اطلاعات Flowها استفاده میکند. در این تکنولوژی از دو مفهوم Exporter برای تعریف شیوه‌ی ارسال اطلاعات جمع‌آوری شده، و Monitor برای تعریف شیوه‌ی جمع‌آوری اطلاعات Flowها استفاده میشود

سرویس IPSec:

- پشتیبانی از تعریف به صورت سلسله مراتبی
- پشتیبانی از IPSec ESP
- پشتیبانی از IPSec AH به صورت Experimental
- پشتیبانی از الگوریتم‌های رمزنگاری AES، AES-CTR و AES-GCM
- پشتیبانی از الگوریتم‌های درهم‌سازی SHA1، SHA2-256، SHA2-384، SHA2-512
- پشتیبانی از گروه‌های Diffie-hellman 14,19,20,21,28,29,30,31,32
- عدم پشتیبانی از PFS
- پشتیبانی از حالت Transport
- پشتیبانی از Route Based Encryption
- عدم پشتیبانی از Policy Based Encryption(Crypto-map)
- پشتیبانی از IKEv2
- عدم پشتیبانی از IKEv1

سرویس 802.1x: این سرویس در سودار پشتیبانی نمی‌گردد. این امکان بیشتر در سوییچها و روترهای wireless مورد استفاده قرار می گیرد.

سرویس Tunnel:

- پشتیبانی از تونل‌های GRE و IP-IP
- پشتیبانی از تونل‌ها در دو حالت P2P و P2MP
- پشتیبانی از IPv4 و IPv6 برای تونل‌ها
- عدم پشتیبانی از تونل‌های 4to6 و 6to4
- پشتیبانی از Protect کردن تونل با IPSec Profile

سرویس SLA:

- پشتیبانی از icmp-echo
- پشتیبانی از icmp-jitter
- پشتیبانی از reactionها
- پشتیبانی از triggerها
- پشتیبانی از scheduling و recurred schedules
- پشتیبانی از محاسبه‌ی percentile

- عدم پشتیبانی از delay در reactionها
- عدم پشتیبانی از پارامترهای one-way در reactionها و نمایش‌ها
- عدم پشتیبانی از SNMP Trap

2.11.2 جدول زمان‌بندی پیاده‌سازی

Q0 = پیاده سازی در مدت یک هفته

Q1 = پیاده سازی در مدت دو تا سه هفته

Q2 = پیاده سازی در بازه یک فصل(2 تا 3 ماه)

Q3 = پیاده سازی در بلندمدت/ عدم برنامه برای پیاده سازی(نیاز به مذاکره و تماس برای بیان جزئیات)

نکته 1: در صورت نیاز به پیاده سازی دستورات نمایشی برای هر یک از سرویس‌ها، می توان کلاس زمان برای پیاده‌سازی آن را Q0 یا حداکثر Q1 تصور نمود.

ویژگی	سازی پیاده برای تخمینی زمان کلاس
NAT	
NAT static network translation	Q0
NAT outside	Q3
پارامتر افزودن interface به NAT دستورات	
سرویس VRRP	Q3
QOS	Q3
BGP	
از پشتیبانی EVPN	Q3
از پشتیبانی Multicast address family	Q3
افزودن PBR	Q2
IPSec	
از پشتیبانی PFS	Q0
از پشتیبانی Crypto maps	Q2
از پشتیبانی IKEv1	Q2
Tunnels	
4to6 و 6to4 تونل افزودن	Q2

**

12.2 برنامه های آینده روتر سودار

1.12.2 پیاده سازی بستر تست کاملتر

یکی از مشکلات اصلی برای پذیرش محصولات بومی کیفیت این محصولات است. این مسئله در محصولات شبکه نمود بیشتری دارد با بررسی های به عمل آمده در بازار، با اینکه مدیران به استفاده از محصولات بومی راغب می باشند ولی مدیران شبکه از آن دوری می جویند. در گذشته تجربه نامناسبی از محصولات مختلف بومی مانند فایروال بومی حاصل شده است و نگرانی مدیران شبکه برای ناپایداری شبکه باعث شده تا در مقابل استفاده از محصولات بومی مقاومت نشان دهند. به طوری که در صحبت های مختلفی که صورت پذیرفته اولین چیزی که به آن اشاره می شود، کیفیت پایین محصولات بومی است.

ما در گروه سودار اولین اولویت خود را کیفیت قرار داده ایم و برای این امر برنامه داریم. از ابتدای تولید محصول به پیاده سازی نرم افزاری تستهای اتوماتیک پرداخته ایم و هم اکنون دارای مجموعه ای از تستها در زمینه های مختلف می باشیم

2.12.2 افزودن سرویسهای جدید

در این مرحله ما بسیاری از پایه های اصلی روتر را دارا هستیم. از سویی بستر پرسرعت مورد استفاده برای روتر سودار این امکان را فراهم می سازد تا بتوانیم محصولات متنوعی ارائه دهیم که دارای سرعت بالا بوده و بتوان آنها را در بستر شبکه های بزرگ مورد استفاده قرار دهیم. محصولات زیر قابلیت پیاده سازی بر روی بستر سودار را دارند

- فایروال ظرفیت بالا برای تعداد session های زیاد
- توزیع کننده بار (Load Balancer) ترافیکی ظرفیت بالا
- تبدیل کننده آدرس (NAT) برای تعداد کاربران زیاد

3.12.2 بسترهای سخت افزاری

سرعت روتر سودار با افزایش سرعت پردازشی و تعداد پردازنده ها افزایش می یابد و این افزایش تقریبا خطی است یعنی با دو برابر شدن پردازنده ها به سرعت دو برابری در روتر خواهیم رسید. ارائه سودار برای سرعت های بیشتر از یک ترابیت نیازمند بررسی و تهیه بستر سخت افزاری مناسب می باشد. با بررسی های صورت پذیرفته در حال حاضر می توان از محصولات Lanner برای ارائه سرعت تا 3 ترابیت استفاده نمود که بستر HTCA-6600 دارای 6 کارت پردازشی می باشد که هر کدام دو پردازنده Xeon را حمایت میکند که در مجموع 12 پردازنده Xeon را داریم. بر روی این بستر دارای 6 اسلات برای شبکه است که می توان از کارتهای توسعه با ظرفیت 320G استفاده نمود که مجموعا حدود 2Tb جهت روتینگ استفاده نمود. توجه داشته باشید که برای مسیریابی ترافیک 2Tb نیازی به 12 پردازنده نیست و می توان از کارتهای پردازشی برای ارائه خدمات دیگر استفاده نمود.

روتر سودار می تواند بر روی بسترهای سخت افزاری ARM نیز اجرا گردد. برآنیم که سودار را بر روی برخی از نمونه های سخت افزاری قدرتمندی ARM پیاده سازی و ارایه نماییم. در حال حاضر سودار بر روی سخت افزار NanoPI R5S اجرا میگردد.

4.12.2 تکنولوژی های جدید

دیدن مسیر آینده در زمینه تکنولوژیهای شبکه یکی از الزامات سودار است. بر این اساس به دنبال توسعه تکنولوژیهای جدید هستیم و مواردی مانند SDN و Segment Routing را در دستور کار قرار داده ایم.

- پشتیبانی از Netconf و Yang
- ارائه API برای برنامه نویسان به صورت gRPC