**CCNP and CCIE Enterprise Core ENCOR 350-401**

**CCNP و CCIE هسته سازمانی**

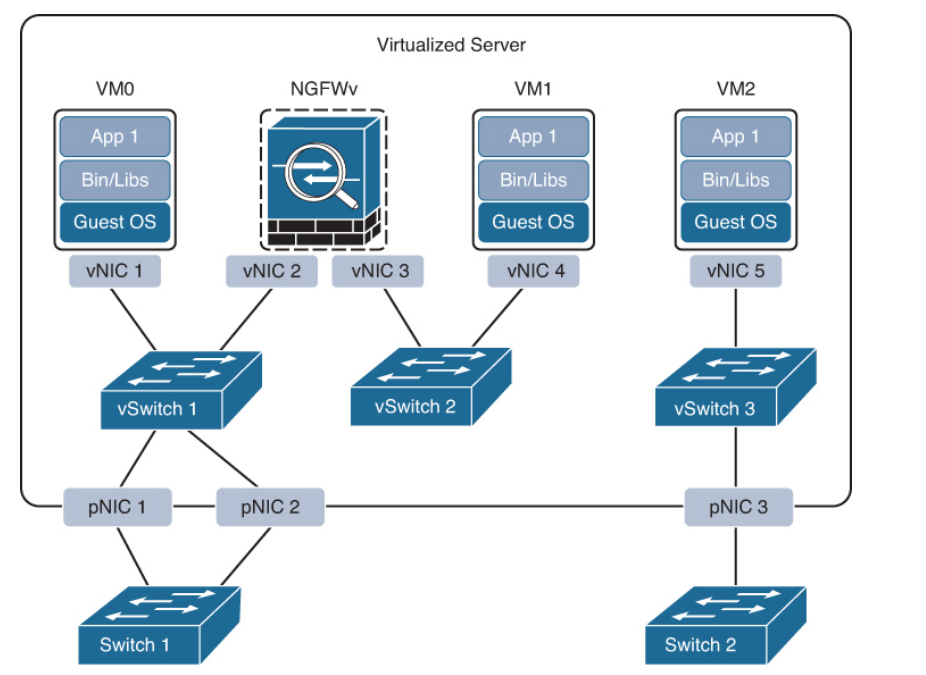
# تعویض مجازی

سوئیچ مجازی ( vSwitch ) سوئیچ لایه 2 مبتنی بر نرم افزار است که مانند سوئیچ اترنت فیزیکی کار می کند. vSwitch VM ها را قادر می سازد تا از طریق کارتهای رابط شبکه فیزیکی ( pNICs ) با یکدیگر در یک سرور مجازی و با شبکه های فیزیکی خارجی ارتباط برقرار کنند. vSwitch های چندگانه را می توان تحت یک سرور مجازی ایجاد کرد، اما ترافیک شبکه نمی تواند مستقیما از یک vSwitch به vSwitch دیگر در یک هاست جریان یابد، و vSwitch ها نمی توانند همان pNIC را به اشتراک بگذارند.

محبوب ترین vSwitcheها شامل موارد زیر است:

* سوئیچ مجازی سری Cisco Nexus 1000VE
* سوئیچ مجازی کاربردی Cisco ( AVS )
* باز کردن vSwitch (OVS)
* IBM DVS 5000v
* سوئیچ vSphere

شکل 27-5 یک سرور مجازی با سه vSwitches متصل به کارتهای رابط شبکه مجازی ( vNICs ) از VM ها و همچنین pNIC را نشان می دهد. vSwitch1 و vSwitch3 برای دسترسی به شبکه فیزیکی به ترتیب با pNIC 1 و pNIC 3 متصل هستند ، در حالی که vSwitch2 به هیچ pNIC متصل نیست. از آنجا که ترافیک شبکه نمی تواند از یک vSwitch به دیگری جریان یابد ، ترافیک شبکه از VM1 که به شبکه خارجی یا VM0 اختصاص داده شده است ، باید از طریق فایروال نسل بعدی مجازی ( NGFWv ) جریان یابد.



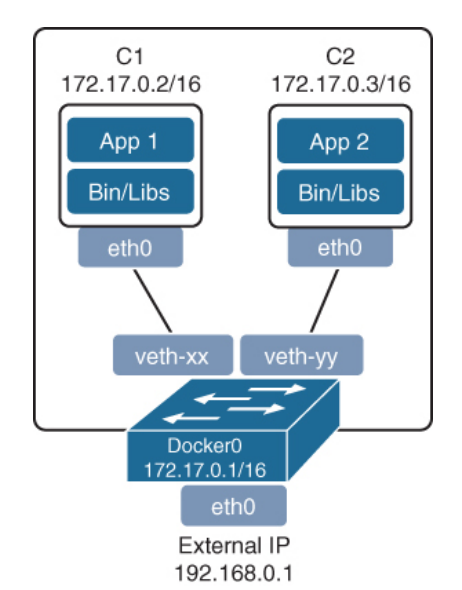
شکل 27-5 سرور مجازی شده با vSwitches

یکی از معایب vSwitches استاندارد این است که هر vSwitch که بخشی از یک دسته از سرورهای مجازی است ، باید در هر میزبان مجازی به صورت جداگانه تنظیم شود. این مشکل با استفاده از سوئیچینگ مجازی توزیع شده حل می شود ، ویژگی ای که vSwitches را با هم از یک خوشه از سرورهای مجازی جمع می کند و با آنها به عنوان یک سوئیچ مجازی توزیع شده رفتار می کند. اینها برخی از مزایای تعویض توزیع شده است:

* مدیریت متمرکز پیکربندی vSwitch برای چندین میزبان در یک خوشه، که مدیریت را ساده می کند.
* مهاجرت آمار و سیاست های شبکه سازی با ماشین های مجازی در طول مهاجرت زنده VM.
* سازگاری پیکربندی در تمام میزبان هایی که بخشی از سوئیچ توزیع شده هستند.

مانند VMs، کانتینرها بر vSwitches (که به عنوان پل های مجازی شناخته می شوند)برای ارتباط درون یک گره (سرور)یا دنیای خارج اعتماد می کنند. به عنوان مثال، Docker، به طور پیش فرض یک پل مجازی به نام Docker0 ایجاد می کند، و به آن بلوک زیرشبکه پیش فرض ۱۷۲.۱۷.۰.۱/۱۶ اختصاص داده می شود. این زیرشبکه پیش فرض می تواند سفارشی شود، و پل های سفارشی کاربر تعریف شده نیز می تواند استفاده شود.

شکل 27-6 نشان می دهد که چگونه به هر کانتینر ایجاد شده توسط Docker یک رابط اترنت مجازی ( veth ) در Docker0 اختصاص داده می شود. رابط veth به عنوان eth0 به کانتینر می رسد. رابط eth0 یک آدرس IP از بلوک زیر شبکه پل اختصاص داده شده است. از آنجا که کانتینرهای بیشتری توسط Docker در گره ایجاد می شوند ، به هر یک از آنها یک رابط eth0 و یک آدرس IP از همان فضای آدرس خصوصی اختصاص داده می شود. همه کانتینرها فقط در صورت وجود گره در یک گره می توانند با یکدیگر ارتباط برقرار کنند. کانتینرهای موجود در گره های دیگر به طور پیش فرض قابل دسترسی نیستند و این کار را می توان با استفاده از مسیریابی در سطح سیستم عامل یا با استفاده از شبکه همپوشانی مدیریت کرد.



شکل 27-6 پل زدن کانتینر

اگر Docker با استفاده از پیکربندی پیش فرض روی گره دیگری نصب شود ، با همان آدرس IP به عنوان اولین گره به پایان می رسد, و این باید بر اساس گره به گره برطرف شود. یک روش بهتر برای مدیریت و مقیاس کانتینرها و اتصال شبکه بین آنها در داخل و در سراسر گره ها استفاده از یک هماهنگ کننده کانتینر مانند Kubernetes است.

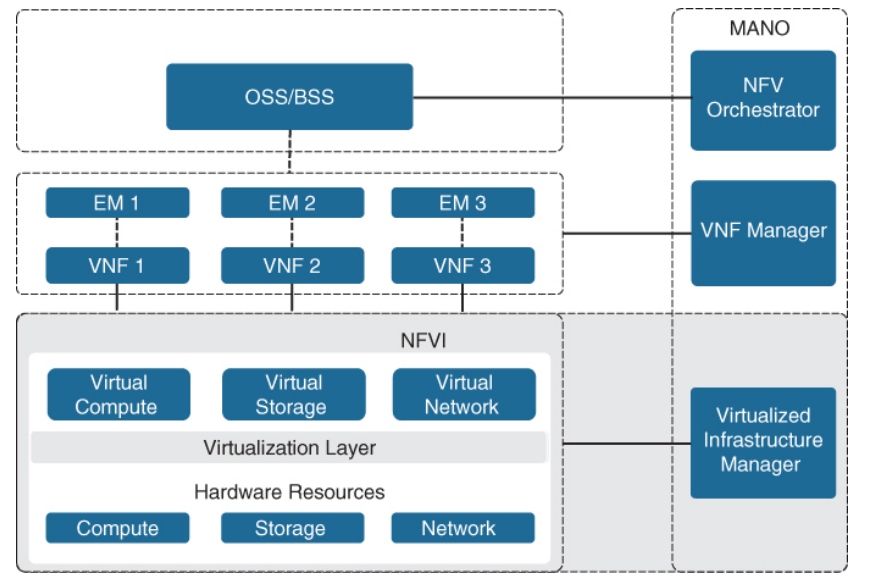
# مجازی سازی کارکردهای شبکه

مجازی سازی کارکردهای شبکه ( NFV ) یک چارچوب معماری است که توسط موسسه استاندارد مخابراتی اروپا ( ETSI ) ایجاد شده است و استانداردها را برای جدا کردن کارکردهای شبکه از تجهیزات اختصاصی مبتنی بر سخت افزار تعریف می کند و آنها را به صورت نرم افزار روی سرورهای استاندارد x86 اجرا می کند. همچنین نحوه مدیریت و سازماندهی کارکردهای شبکه را تعریف می کند. کارکرد شبکه ( NF ) به عملکردی است که توسط یک دستگاه فیزیکی انجام می شود ، مانند فایروال یا تابع روتر اشاره دارد.

برخی از مزایای NFV شبیه به مزایای مجازی سازی سرور و محیط های ابری است:

* کاهش هزینه های سرمایه ( capex ) و هزینه های عملیاتی ( opex ) از طریق کاهش هزینه های تجهیزات و راندمان در فضا ، نیرو و سرمایش
* زمان عرضه سریعتر برای بازاریابی ( TTM ) زیرا VM ها و کانتینرها راحت تر از سخت افزار هستند
* بهبود بازگشت سرمایه ( ROI ) از خدمات جدید
* توانایی مقیاس بالا / خارج و پایین / در ظرفیت در صورت تقاضا ( الاستیسیته )
* آشنایی با بازار لوازم خانگی مجازی و فروشندگان شبکه نرم افزار خالص
* فرصت هایی برای آزمایش و استقرار خدمات نوآورانه جدید بصورت عملی و با ریسک کمتر

شکل 27-7 چارچوب معماری ETSI NFV را نشان می دهد.



شکل 27-7 چارچوب معماری ETSI NFV

# زیر ساخت NFV

زیرساخت NFV ( NFVI ) تمام اجزای سخت افزاری و نرم افزاری است که محیط سیستم عامل را تشکیل می دهد و در آن توابع شبکه مجازی ( VNFs ) مستقر می شوند.

# توابع شبکه مجازی

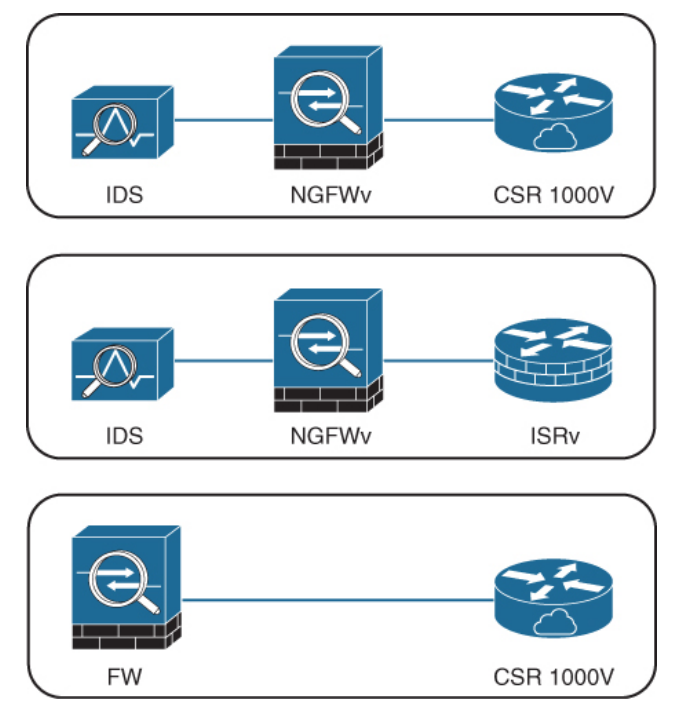
عملکرد شبکه مجازی ( VNF ) ، همانطور که از نام آن پیداست ، نسخه مجازی یا نرم افزاری یک NF است ، و به طور معمول به عنوان یک VM روی یک هایپروایزر اجرا می شود. VNF ها معمولاً برای توابع لایه 4 از طریق لایه 7 استفاده می شوند ، مانند مواردی که توسط ترازکننده­های بار ( LBs ) و کنترل کننده های تحویل برنامه ( ADCs ) ، فایروال ها ، سیستم های تشخیص نفوذ ( IDSs ), و وسایل بهینه سازی WAN ارائه می شود. با این حال ، آنها محدود به توابع لایه 4 از طریق لایه 7 نیستند. آنها همچنین می توانند توابع سطح پایین لایه 2 و لایه 3 مانند توابع ارائه شده توسط روترها و سوئیچ ها را انجام دهند.

برخی از نمونه های VNF های سیسکو شامل موارد زیر است:

* روتر خدمات ابر سیسکو 1000V ( CSR 1000V )
* پلتفرم خدمات ابری سیسکو ۲۱۰۰ (CSP ۲۱۰۰)
* روتر مجازی خدمات یکپارچه سیسکو ( ISRv )
* نرم افزار مجازی دیوار آتش سیسکو NextGen (NGFWv)
* نرم افزار امنیتی تطبیقی سیسکو ( ASAv )

# مدیر زیرساخت مجازی

مدیر زیرساخت مجازی NFVI ( VIM ) مسئولیت مدیریت و کنترل منابع سخت افزاری NFVI ( محاسبه ، ذخیره سازی و شبکه ) و منابع مجازی را بر عهده دارد. همچنین مسئولیت جمع آوری اندازه گیری عملکرد و اطلاعات مربوط به خطا را بر عهده دارد. علاوه بر این ، مدیریت چرخه عمر ( راه اندازی ، نگهداری و تعمیر ) از کلیه منابع NFVI و همچنین زنجیره خدمات VNF را انجام می دهد. زنجیره خدمات به زنجیره VNF ها در کنار هم برای ارائه خدمات یا راه حل NFV اشاره دارد ، همانطور که در شکل 27-8 نشان داده شده است.



شکل 27-8 زنجیره خدمات

# مدیران عنصر

مدیران عناصر ( EM ) ، همچنین به عنوان سیستم های مدیریت عنصر ( EMSs ) شناخته می شوند ، مسئولیت مدیریت عملکردی VNF ها را بر عهده دارند. به عبارت دیگر ، آنها خطا ، پیکربندی ، حسابداری ، عملکرد, و امنیت ( FCAPS ) برای VNF ها را انجام می دهند. یک EM تنها می تواند یک یا چند VNF را مدیریت کند ، و یک EM نیز می تواند یک VNF باشد.

# مدیریت و هماهنگ سازی

هماهنگ کننده NFV وظیفه ایجاد ، نگهداری و تعمیر خدمات شبکه VNF را بر عهده دارد. اگر چندین VNF بخشی از یک سرویس شبکه باشند ، هماهنگ کننده NFV ایجاد یک سرویس شبکه پایان به پایان را از طریق چندین VNF امکان پذیر می کند. مدیر VNF چرخه عمر یک یا چند VNF و همچنین FCAPS را برای اجزای مجازی یک VNF مدیریت می کند. ارکستر NFV و مدیر VNF در کنار هم به عنوان مدیریت و هماهنگ سازی NFV ( MANO ) شناخته می شوند.

# سیستم پیشتبانی عملیات ( OSS ) / سیستم پشتیبانی تجاری( BSS )

OSS یک پلتفرم است که به طور معمول توسط ارائه دهندگان خدمات ( SPS ) و شبکه های بزرگ شرکت برای پشتیبانی از تمام سیستم ها و خدمات شبکه خود اداره می شود. OSS می تواند به آنها در حفظ موجودی شبکه ، ارائه خدمات جدید ، پیکربندی دستگاه های شبکه و حل مشکلات شبکه کمک کند. برای SP ها ، OSS به طور معمول با BSS همراه است تا تجربه کلی مشتری را بهبود بخشد. BSS ترکیبی از مدیریت محصول ، مدیریت مشتری ، صورتحساب مدیریت درآمد و سیستم های مدیریت سفارش است که برای اجرای عملیات تجاری SP استفاده می شود.

# عملکرد VNF

در راه حل های NFV ، ترافیک داده ها دارای دو الگوی متفاوت است: شمال – جنوب و شرق – غرب. ترافیک شمالی – از طریق NIC فیزیکی ( pNIC ) به سرور میزبان وارد می شود و به VNF ارسال می شود; سپس از طریق VNF به سیم فیزیکی از طریق pNIC ارسال می شود. ترافیک شرق – غربی از طریق pNIC به سرور میزبان می آید و به VNF ارسال می شود. از آنجا, می توان آن را به سرویس VNF ( دیگری که زنجیر شده ) است و احتمالاً سرویس زنجیر شده به VNF های بیشتری ارسال می شود ارسال کرد و سپس از طریق pNIC به سیم فیزیکی ارسال شد. همچنین می توان ترکیبی از این دو را داشت, جایی که یک VNF از یک الگوی ترافیک شمالی – برای داده های کاربر و یک الگوی ترافیک غربی – غربی استفاده می کند تا ترافیک را به VNF ارسال کند که فقط جمع آوری آمار است یا فقط برای سیاهه های مربوط یا ذخیره سازی مورد استفاده قرار می گیرد. این الگوهای و هدف VNF ها هنگام تصمیم گیری در مورد استفاده از فناوری برای تغییر ترافیک بین VNF ها و همچنین به دنیای خارج ، مهم هستند. انتخاب فن آوری های مناسب اطمینان حاصل می کند که VNF ها به توان و عملکرد بهینه دست می یابند. محبوب ترین فن آوری ها برای دستیابی به عملکرد و توان بهینه VNF در این بخش توضیح داده شده است ، اما قبل از توصیف آنها ، درک اصطلاحات زیر حائز اهمیت است:

* ورودی / خروجی ( I / O ): ارتباط بین سیستم محاسباتی ( مانند سرور ) و دنیای خارج. ورودی داده های دریافت شده توسط سیستم محاسباتی است و خروجی داده های ارسال شده از آن است.
* دستگاه I / O: دستگاه جانبی مانند ماوس ، صفحه کلید ، مانیتور یا کارت رابط شبکه ( NIC ).
* درخواست قطع ( IRQ ): سیگنال سخت افزاری که توسط یک دستگاه I / O ( مانند NIC ) به CPU ارسال می شود تا هنگام انتقال داده ، به CPU اطلاع دهد. هنگامی که CPU وقفه ( IRQ ) را دریافت می کند ، وضعیت فعلی خود را ذخیره می کند ، به طور موقت کارهایی را که انجام می دهد متوقف می کند و یک روال کنترل کننده قطع شده را در ارتباط با دستگاه اجرا می کند. کنترل کننده وقفه علت وقفه را تعیین می کند ، پردازش لازم را انجام می دهد ، یک حالت CPU را بازیابی می کند, و دستورالعمل بازگشت از وقفه را برای بازگشت کنترل به CPU صادر می کند تا بتواند آنچه را که قبل از وقفه انجام می داد از سر بگیرد. هر دستگاه I / O که IRQ تولید می کند دارای یک کنترل کننده قطع کننده همراه است که بخشی از درایور دستگاه است.
* درایور دستگاه: یک برنامه رایانه ای است که یک دستگاه I / O را کنترل می کند و به CPU اجازه می دهد تا با دستگاه I / O ارتباط برقرار کند. NIC نمونه ای از دستگاه I / O است که به یک درایور نیاز دارد تا با CPU کار کند و رابط کند.
* دسترسی مستقیم به حافظه ( DMA ): یک روش دسترسی به حافظه که به دستگاه I / O اجازه می دهد تا با عبور از CPU ، داده ها را مستقیماً از طریق حافظه اصلی, برای سرعت بخشیدن به عملکرد کلی رایانه ارسال یا دریافت کند.
* هسته و فضای کاربر: قسمت اصلی یک سیستم عامل ( OS ) و یک منطقه حافظه که برنامه ها و کتابخانه های مرتبط با آنها در آن قرار دارند. هسته ( “ هسته ” به زبان آلمانی ) برنامه ای است که (هسته اصلی) یک سیستم عامل است. این سیستم به طور مستقیم اجزای سخت افزاری رایانه ای ، مانند RAM و CPU را مدیریت می کند و خدمات سیستم را به برنامه هایی که نیاز به دسترسی به هر مؤلفه سخت افزاری از جمله NIC و ذخیره داخلی دارند ، ارائه می دهد. از آنجا که هسته اصلی یک سیستم عامل است ، هسته در یک منطقه محافظت شده از حافظه اصلی ( فضای هسته ) اجرا می شود تا از تأثیرگذاری سایر فرآیندها جلوگیری کند. فرآیندهای غیر هسته ای در یک منطقه حافظه به نام فضای کاربر اجرا می شوند ، جایی که برنامه ها و کتابخانه های مرتبط با آنها ساکن هستند.

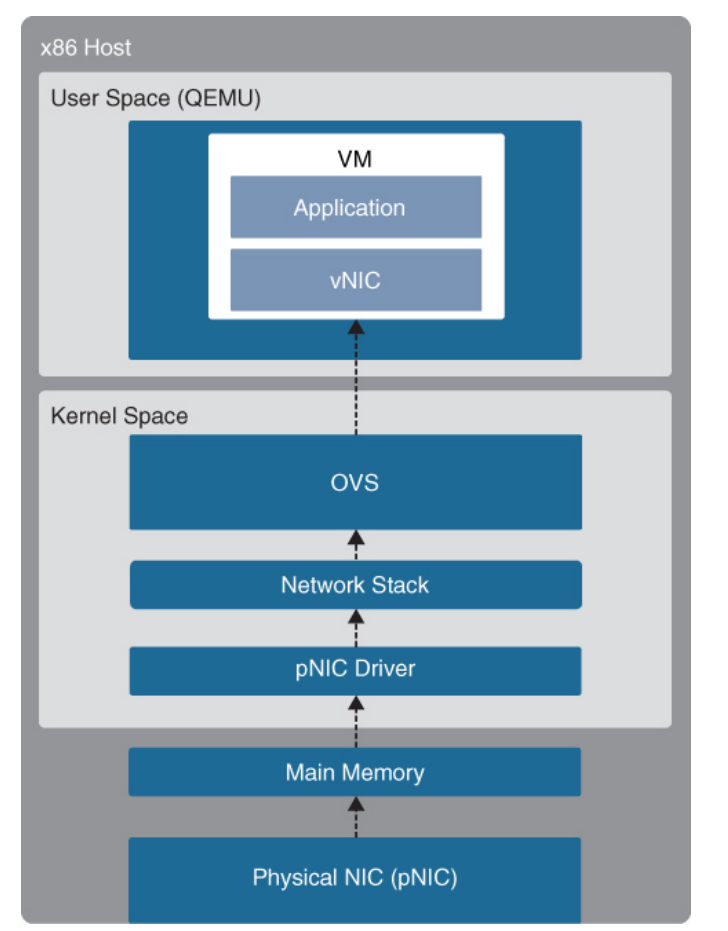
شکل 27-9 هسته و فضای کاربر سیستم عامل و همچنین دستگاههای معمولی I / O را که با سیستم عامل ارتباط برقرار می کنند نشان می دهد.



شکل 27-9 هسته سیستم عامل و فضای کاربر

در محیط های غیر مجازی ، ترافیک داده توسط یک pNIC دریافت می شود و سپس از طریق فضای هسته به یک برنامه در فضای کاربر ارسال می شود. در یک محیط مجازی ، pNIC ها و NIC های مجازی ( vNICs ) و یک مشاور عالی با سوئیچ مجازی بین آنها وجود دارد. ه و سوئیچ مجازی وظیفه دارند داده ها را از pNIC بگیرند و آن را به vNIC VM / VNF و در آخر به برنامه ارسال کنند. افزودن لایه مجازی ، پردازش اضافی و سربار مجازی سازی بسته را معرفی می کند ، که تنگناها را ایجاد می کند و توان بسته I / O را کاهش می دهد.

جریان بسته برای یک سیستم مجازی با معماری Open vSwitch ( OFS ) در شکل 27-10 نشان داده شده است.



شکل 27-10 x86 میزبان با OVS

مراحل جریان بسته های سطح بالا برای بسته های دریافت شده توسط pNIC و تحویل برنامه در VM به شرح زیر است:

مرحله 1. ترافیک داده توسط pNIC دریافت می شود و در صف Rx ( بافر حلقه ) در pNIC قرار می گیرد.

مرحله 2. pNIC بسته و توصیف کننده بسته را از طریق DMA به بافر اصلی حافظه می فرستد. توصیف کننده بسته فقط شامل مکان حافظه و اندازه بسته می باشد.

مرحله 3. pNIC IRQ را به CPU می فرستد.

مرحله 4. CPU کنترل را به درایور pNIC ، که IRQ را سرویس می کند ، بسته را دریافت می کند و آن را به پشته شبکه منتقل می کند, جایی که سرانجام وارد سوکت می شود و در یک سوکت بافر دریافت می شود.

مرحله 5. داده های بسته از بافر دریافت سوکت به سوئیچ مجازی OVS کپی می شوند.

مرحله 6. OVS بسته را پردازش می کند و آن را به VM منتقل می کند. این امر مستلزم تعویض بسته بین هسته و فضای کاربر است که از نظر چرخه CPU گران است.

مرحله 7. بسته به NIC مجازی ( vNIC ) VM می رسد و در صف Rx قرار می گیرد.

مرحله 8. vNIC بسته و توصیف کننده بسته را از طریق DMA به بافر حافظه مجازی ارسال می کند.

مرحله 9. vNIC IRQ را به vCPU ارسال می کند.

مرحله 10. vCPU کنترل را به درایور vNIC ، که IRQ را سرویس می کند ، بسته را دریافت می کند ، و آن را به پشته شبکه منتقل می کند, جایی که سرانجام وارد سوکت می شود و در یک سوکت بافر دریافت می شود.

مرحله 11. داده های بسته در VM کپی شده و به برنامه ارسال می شوند.

هر بسته دریافت شده باید همان فرآیند را طی کند ، که نیاز به قطع مداوم CPU دارد. تعداد وقفه ها هنگام استفاده از NIC های پر سرعت ( به عنوان مثال ، 40 گیگابیت بر ثانیه ) افزایش می یابد و اندازه بسته ها اندک است زیرا نیاز به پردازش بیشتر بسته ها در ثانیه است. وقفه ها سربار زیادی را اضافه می کنند زیرا هر فعالیتی که CPU انجام می دهد باید متوقف شود ، حالت باید ذخیره شود ، وقفه باید پردازش شود, و روند اصلی باید احیا شود تا بتواند آنچه را که قبل از وقفه انجام می داد از سر بگیرد.

برای جلوگیری از تمام سربار و افزایش توان بسته ، چندین فناوری I / O توسعه داده شده است. شایع ترین این فناوری ها موارد زیر است:

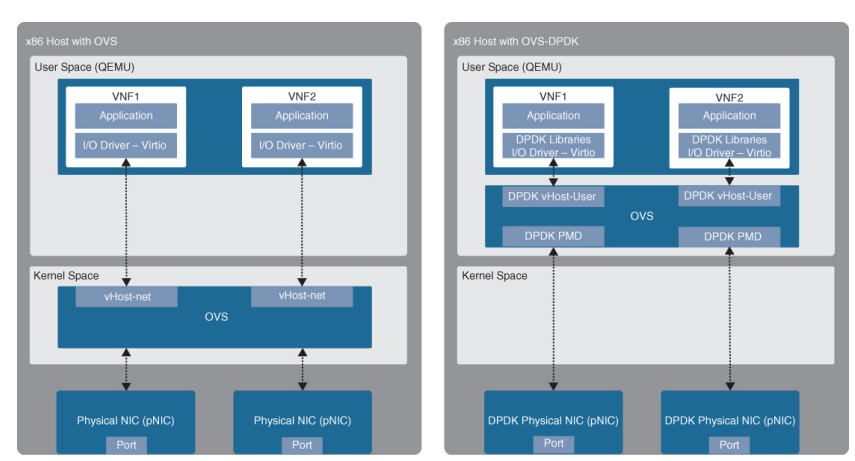
* کیت توسعه داده های OVS ( OFS-DPDK )
* گذرگاه PCI
* مجازی سازی I / O تک ریشه ( SR-IOV )

یادداشت

برای اینکه بتوانید این فناوری های I / O را پیاده سازی کنید ، NIC های فیزیکی که از آنها پشتیبانی می کنند لازم است.

# OVS-DPDK

برای غلبه بر تأثیر عملکرد بر توان به دلیل وقفه ، OVS با کتابخانه های توسعه داده پلن ( DPDK ) بهبود یافت. OVS با DPDK کاملاً در فضای کاربر کار می کند. درایور حالت نظرسنجی DPDK ( PMD ) در نظرسنجی های OVS برای داده هایی که وارد pNIC می شوند و آن را , دور زدن پشته شبکه و لزوم ارسال وقفه به CPU هنگام دریافت یک بسته — به عبارت دیگر ، با دور زدن کامل هسته پردازش می کنند. برای انجام این کار ، DPDK PMD به یک یا چند هسته CPU اختصاص داده شده برای رای گیری و رسیدگی به داده های دریافتی نیاز دارد. هنگامی که بسته در OVS است ، در حال حاضر در فضای کاربر قرار دارد و می توان آن را مستقیماً به VNF مناسب تغییر داد و در نتیجه مزایای عملکرد بسیار خوبی را به همراه داشت. شکل 27-11 میزبان x86 با OVS استاندارد را در مقایسه با میزبان x86 با OVS با DPDK نشان می دهد.



شکل 27-11 استاندارد OVS و OVS-DPDK

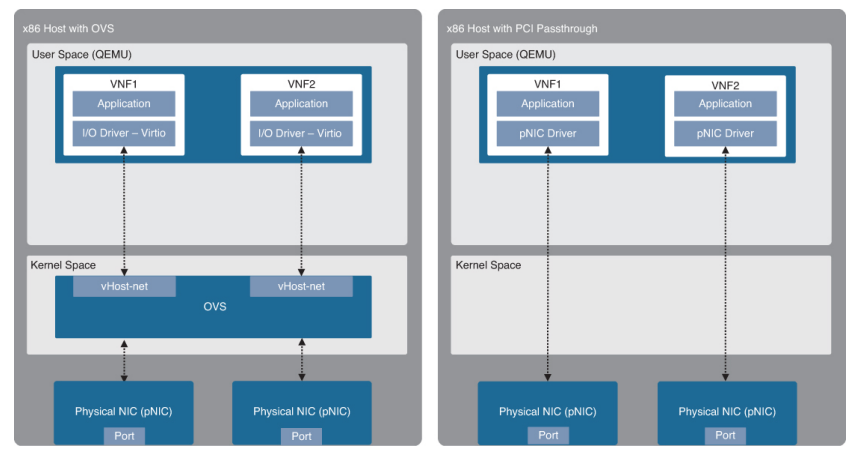
# گذرگاه PCI

گذرگاه PCI به VNF ها اجازه می دهد تا مستقیماً به دستگاههای PCI فیزیکی دسترسی داشته باشند ، که به نظر می رسد و رفتار می کنند انگار که از نظر جسمی به VNF متصل شده اند. این فناوری می تواند برای نقشه برداری از pNIC به یک VNF واحد استفاده شود ، و از دیدگاه VNF ، به نظر می رسد که مستقیماً به pNIC متصل است.

گذرگاه PCI مزایای عملکرد بسیاری را ارائه می دهد:

* نقشه برداری اختصاصی تک به تک
* هایپروایزر بیسیم
* دسترسی مستقیم به منابع I / O
* کاهش استفاده از CPU
* کاهش تأخیر سیستم
* افزایش توان I / O

نکته منفی در مورد گذرگاه PCI این است که کل pNIC به یک VNF اختصاص داده شده است و توسط سایر VNF ها قابل استفاده نیست, بنابراین تعداد VNF هایی که می توانند از این فناوری استفاده کنند با تعداد pNIC های موجود در سیستم محدود شده است. شکل 27-12 میزبان x86 را با یک OVS استاندارد و یک میزبان x86 با گذرگاه PCI نشان می دهد.



شکل 27-12 استاندارد OVS و گذرگاهPCI

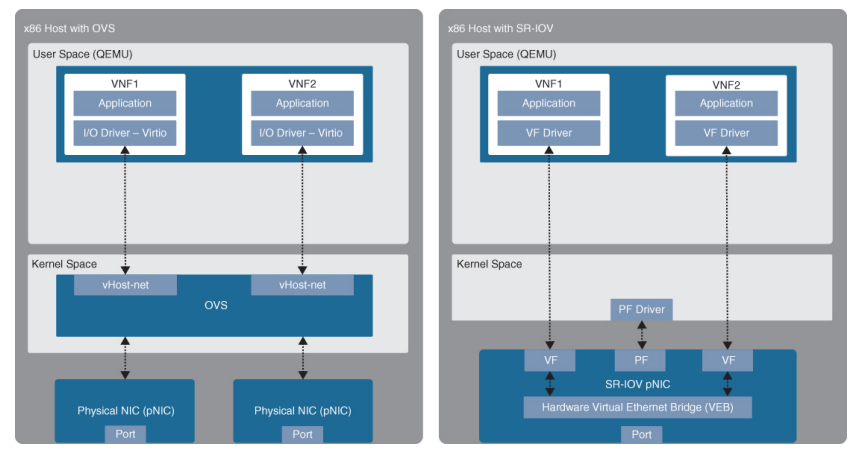
SR-IOV

SR-IOV یک پیشرفت برای گذرگاه PCI است که به چندین VNF اجازه می دهد تا همان pNIC را به اشتراک بگذارند. SR-IOV چندین دستگاه PCIe را در یک دستگاه PCIe ( مانند pNIC ) تقلید می کند. در SR-IOV ، دستگاه های PCIe شبیه سازی شده توابع مجازی ( VFs ) نامیده می شوند ، و دستگاه های PCIe فیزیکی توابع فیزیکی ( PFs ) نامیده می شوند. VNF ها با استفاده از فناوری گذرگاه PCI ، مستقیماً به VF ها دسترسی دارند.

یک pNIC با قابلیت SR-IOV از دو حالت مختلف برای تغییر ترافیک بین VNF پشتیبانی می کند:

* پل اترنت مجازی (VEB): ترافیک بین VNF های متصل به همان pNIC سخت افزاری است که مستقیماً توسط pNIC تغییر می یابد.
* جمع کننده پورت اترنت مجازی ( CEPA ): ترافیک بین VNF های متصل به همان pNIC توسط یک سوئیچ خارجی تغییر می یابد.

شکل 27-13 میزبان x86 با OVS استاندارد را در مقایسه با میزبان x86 با SR-IOV نشان می دهد.



شکل 27-13 استاندارد OVS و SR-IOV

# مجازی سازی توابع شبکه Cisco Enterprise ( ENFV )

# **دفاتر شعب سازمانی اغلب برای انجام وظایف شبکه مانند شتاب WAN ، محافظت از فایروال ، کنترلر LAN بی سیم ، پیشگیری از نفوذ ، خدمات همکاری و مسیریابی و سوئیچینگ به چندین دستگاه شبکه فیزیکی نیاز دارند. بعضی اوقات این دستگاه های فیزیکی با افزونگی مستقر می شوند و تعداد دستگاه های نصب شده و کار شده در شعبه را بیشتر می کنند. یک شرکت به طور معمول دارای چندین شعبه است و نیاز به مدیریت بسیاری از دستگاه های مختلف می تواند چالش های بسیاری را ایجاد کند.**

راه حل Cisco ENFV یک راه حل سیسکو است که بر اساس چارچوب معماری ETSI NFV ساخته شده است. این پیچیدگی عملیاتی محیط های شعبه شرکت را با اجرای توابع شبکه مورد نیاز به عنوان توابع شبکه مجازی ( VNFs ) در میزبان های استاندارد مبتنی بر x86 کاهش می دهد. به عبارت دیگر ، آن را جایگزین فایروال های فیزیکی ، روترها ، WLC ، بالانسورهای بار و غیره با دستگاه های مجازی که در یک پلت فرم x86 واحد کار می کنند. راه حل Cisco ENFV مزایای زیر را ارائه می دهد:

* تعداد دستگاههای فیزیکی را که باید در شعبه مدیریت شوند کاهش می دهد و در نتیجه کارآیی در فضا ، نیرو ، نگهداری و سرمایش ایجاد می شود
* نیاز به تعمیرکار و تکنسین را برای انجام نصب و راه اندازی سخت افزار یا به روزرسانی کاهش می دهد
* ارائه سادگی عملیاتی که به آن امکان می دهد خدمات جدید ، به روزرسانی های مهم ، VNF ها و مکان های شعبه را در عرض چند دقیقه گسترش دهد
* مدیریت را از طریق مرکز DNA سیسکو متمرکز می کند ، که طراحی ، تهیه ، به روزرسانی ، مدیریت و عیب یابی خدمات شبکه و VNF را بسیار ساده می کند
* انعطاف پذیری عملیات شبکه را با استفاده کامل از تکنیک های مجازی سازی مانند حرکت ماشین مجازی ، عکس های فوری و به روز رسانی ها تقویت می کند
* پشتیبانی از Cisco SD-WAN cEdge و vEdge روتر مجازی
* VNF های شخص ثالث را پشتیبانی می کند

# معماری راه حل Cisco ENFV

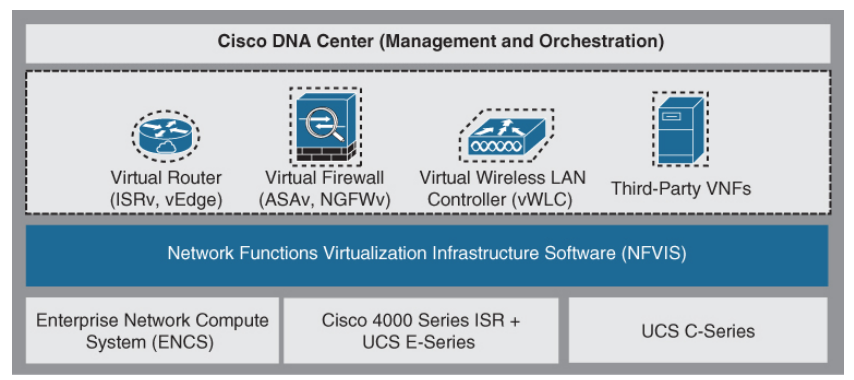
Cisco ENFV یک راه حل مجازی برای خدمات شبکه و برنامه برای دفاتر شعبه ارائه می دهد. این مجموعه از چهار مؤلفه اصلی تشکیل شده است که بر اساس چارچوب معماری ETSI NFV ساخته شده اند:

* مدیریت و هماهنگ سازی ( MANO ): مرکز دی ان ای سیسکو قابلیت مدیریت VNF و هماهنگ سازی NFV را فراهم می کند. این امکان را برای اتوماسیون آسان استقرار خدمات شبکه مجازی ، متشکل از چندین VNF فراهم می کند.
* VNFs: VNF ها عملکردهای شبکه مجازی مورد نظر را ارائه می دهند.
* توابع شبکه نرم افزار زیرساخت مجازی سازی ( NFVIS ): سیستم عامل که قابلیت های مجازی سازی را فراهم می کند و استقرار و بهره برداری از VNF ها و اجزای سخت افزاری را تسهیل می کند.
* منابع سخت افزاری: منابع محاسباتی مبتنی بر x86 که CPU ، حافظه و ذخیره سازی مورد نیاز برای استقرار و بهره برداری از VNF ها و اجرای برنامه ها را فراهم می کنند.

شکل 27-14 اجزای اصلی راه حل NFV Enterprise Cisco را نشان می دهد.

یادداشت

ارائه دهندگان خدمات مدیریت شده ( MSPs ) می توانند با استفاده از هماهنگ سازی سرویس شبکه سیسکو ( NSO ) یا شتاب دهنده خدمات مدیریت شده سیسکو ( MSX ) یک مؤلفه OSS / BSS را اضافه کنند.



شکل 27-14 مؤلفه های اصلی راه حل NFV Enterprise

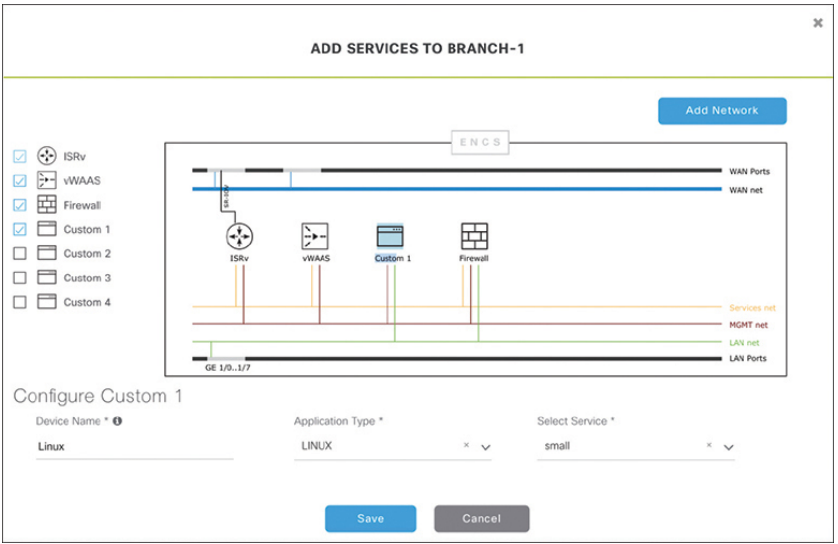
# مدیریت و هماهنگ سازی

مرکز DNA سیسکو عملکرد MANO را به راه حل Cisco Enterprise NFV ارائه می دهد. این شامل یک داشبورد متمرکز و ابزارهایی برای طراحی ، تهیه ، مدیریت و نظارت بر کلیه سایتهای شعبه در سراسر شرکت است. دو مورد از کارکردهای اصلی مرکز DNA ، ایجادمکانهای جدید شعبه یا استقرار VNF های جدید و خدمات مجازی است.

مرکز دی ان ای سیسکو سیاست های متمرکز را ارائه می دهد ، که سیاست های شبکه مداوم را در دفاتر شعبه شرکت امکان پذیر می کند. سیاست های متمرکز با ایجاد پروفایل های شبکه ایجاد می شوند. پروفایل های شبکه چندگانه ایجاد می شود که هر کدام دارای الزامات طراحی خاص و خدمات مجازی هستند. پس از ایجاد ، سایت های شعبه به پروفایل های شبکه که مطابق با نیاز شعبه است اختصاص می یابد. پروفایل های شبکه شامل اطلاعاتی از قبیل موارد زیر است:

* پیکربندی رابط های مجازی LAN و WAN
* خدمات یا VNF هایی که مورد استفاده قرار می گیرند ، مانند فایروال یا بهینه ساز WAN ، و الزامات آنها مانند پارامترهای زنجیره ای سرویس ، CPU و حافظه مورد نیاز
* پیکربندی دستگاه مورد نیاز برای VNF ها ، که می تواند با استفاده از الگوهای پیکربندی سفارشی ایجاد شده از طریق ابزار ویرایشگر قالب سفارشی شود

شکل 27-15 پنجره Cisco DNA Center Add Services را نشان می دهد ، جایی که می توان خدمات یا VNF ها را اضافه کرد و خدمات را می توان با استفاده از انواع مختلف رابط مانند LAN ، مدیریت و خدمات به یکدیگر متصل نمود.



شکل 27-15 پنجره خدمات اضافه مرکز DNA سیسکو

تهیه افزونه و پخش راهی برای تهیه خودکار و از راه دور و نصب دستگاه های جدید شبکه فراهم می کند. هنگامی که یک پلتفرم جدید ENFV برای اولین بار ایجاد شده است ، می تواند از Plug and Play برای ثبت نام در مرکز DNA استفاده کند. سپس مرکز سایت DNA را با مشخصات شبکه اختصاص داده شده برای سایت و سپس مقررات و پردازنده های دستگاه به طور خودکار مطابقت می دهد.

# وظایف و کاربردهای شبکه مجازی

مرکز DNA سیسکو عملکرد MANO را به راه حل Cisco Enterprise NFV ارائه می دهد. این شامل یک داشبورد متمرکز و ابزارهایی برای طراحی ، تهیه ، مدیریت و نظارت بر کلیه سایتهای شعبه در سراسر شرکت است. دو مورد از کارکردهای اصلی مرکز DNA ، بیرون کشیدن مکانهای جدید شعبه یا استقرار VNF های جدید و خدمات مجازی است.

مرکز دی ان ای سیسکو سیاست های متمرکز را ارائه می دهد ، که سیاست های شبکه مداوم را در دفاتر شعبه شرکت امکان پذیر می کند. سیاست های متمرکز با ایجاد پروفایل های شبکه ایجاد می شوند. پروفایل های شبکه چندگانه ایجاد می شود که هر کدام دارای الزامات طراحی خاص و خدمات مجازی هستند. پس از ایجاد ، سایت های شعبه به پروفایل های شبکه که مطابق با نیاز شعبه است اختصاص می یابد. پروفایل های شبکه شامل اطلاعاتی از قبیل موارد زیر است:

* پیکربندی رابط های مجازی LAN و WAN
* خدمات یا VNF هایی که مورد استفاده قرار می گیرند ، مانند فایروال یا بهینه ساز WAN ، و الزامات آنها مانند پارامترهای زنجیره ای سرویس ، CPU و حافظه مورد نیاز
* پیکربندی دستگاه مورد نیاز برای VNF ها ، که می تواند با استفاده از الگوهای پیکربندی سفارشی ایجاد شده از طریق ابزار ویرایشگر قالب سفارشی شود

شکل 27-15 پنجره خدمات افزودن مرکز دی ان ای سیسکو را نشان می دهد ، جایی که می توان خدمات یا VNF ها را اضافه کرد و خدمات را می توان با استفاده از انواع مختلف رابط مانند LAN ، رابط مدیریت و خدمات به یکدیگر زنجیر کرد.



شکل ۲۷-۱۵ پنجره خدمات افزودن مرکز دی ان ای سیسکو

تهیه افزونه و پخش راهی برای تهیه خودکار و از راه دور و نصب دستگاه های جدید شبکه فراهم می کند. هنگامی که یک پلتفرم جدید ENFV برای اولین بار ایجاد شده است ، می تواند از Plug and Play برای ثبت نام در مرکز DNA استفاده کند. سپس DNA Center سایت را با مشخصات شبکه اختصاص داده شده برای سایت و سپس مقررات و پردازنده های دستگاه به طور خودکار مطابقت می دهد.

# وظایف و کاربردهای شبکه مجازی

راه حل Cisco Enterprise NFV محیطی را برای مجازی سازی هر دو عملکرد شبکه و برنامه های کاربردی در شعبه شرکت فراهم می کند. هر دو Cisco و VNF های شخص ثالث را می توان روی محلول سوار کرد. برنامه های در حال اجرا در سرور لینوکس یا محیط سرور ویندوز همچنین می توانند در بالای NFVIS ( که بعداً در این فصل مورد بحث قرار می گیرد ، فوری شوند و توسط مرکز DNA پشتیبانی شوند.

VNF های پشتیبانی شده از سیسکو موارد زیر را شامل می شوند:

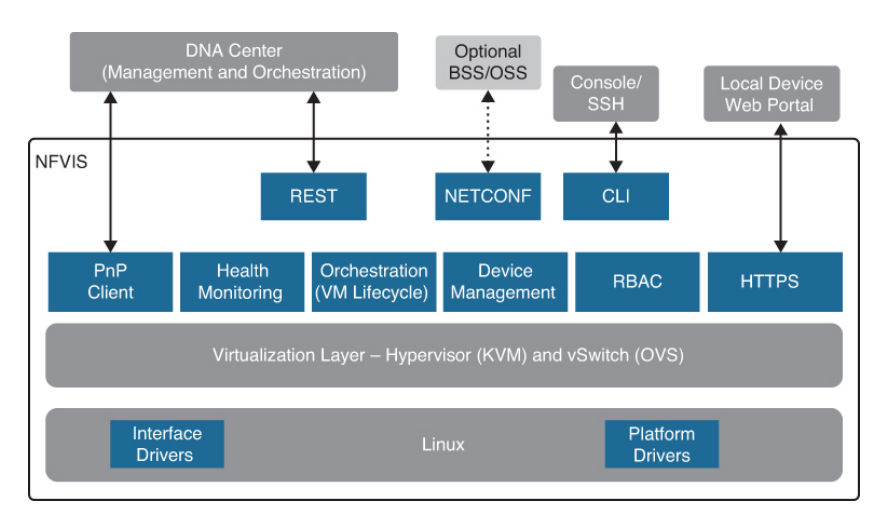
* روتر مجازی خدمات یکپارچه سیسکو ( ISRv ) برای مسیریابی مجازی
* نرم افزار مجازی امنیت تطبیقی سیسکو ( ASAv ) برای یک فایروال مجازی
* Cisco Firepower Firewall نسل بعدی مجازی ( NGFWv ) برای فایروال یکپارچه و تشخیص نفوذ و پیشگیری
* Viptela vEdge
* cEdge
* خدمات برنامه مجازی گسترده مجازی سیسکو ( vWAAS ) برای بهینه سازی WAN مجازی
* کنترلرهای LAN بی سیم مجازی سیسکو ( vWLCs ) برای کنترلرهای LAN بی سیم مجازی

VNF های شخص ثالث موارد زیر را شامل می شوند:

* ThousandEyes
* Fortinet
* PaloAlto
* InfoVista
* CTERA
* سرور ویندوز
* سرور لینوکس

# عملکرد شبکه زیرساخت مجازی سازی عملکرد شبکه Soware ( NFVIS )

NFVIS مبتنی بر لینوکس استاندارد است که دارای توابع اضافی برای مجازی سازی ، مدیریت چرخه عمر VNF ، نظارت ، برنامه نویسی دستگاه و شتاب سخت افزاری است. مؤلفه ها و قابلیت های ارائه شده توسط NFVIS در شکل 27-16 نشان داده شده است:



شکل 27-16 اجزاء NFVIS

* لینوکس: لینوکس سیستم عامل های سخت افزاری اساسی را (به عنوان مثال ، سرورهای ENCS ، Cisco UCS یا دستگاه های شبکه پیشرفته x86 ) و میزبان لایه مجازی سازی برای VNF ها ، رابط های API سوئیچینگ مجازی ، درایورهای رابط, درایورهای سیستم عامل و مدیریت هدایت می کند.
* هایپروایزر (Hypervisor):هایپروایزر برای مجازی سازی مبتنی بر ماشین مجازی مبتنی بر هسته ( KVM ) است و شامل شبیه ساز سریع ( QEMU ) ، Libvirt و سایر فرایندهای مرتبط است.
* سوئیچ مجازی ( vSwitch ): vSwitch Open vSwitch ( OFS ) است و ارتباط بین VNF های مختلف ( زنجیره خدمات ) و دنیای خارج را امکان پذیر می کند.
* مدیریت چرخه عمر VM: NFVIS عملکرد VIM را مطابق با چارچوب معماری NFV از طریق کنترلر خدمات الاستیک تعبیه شده NFVIS ( ESC ) Lite مشخص می کند. ESC-Lite از ایجاد پویا VNFs — ایجاد و حذف VNF ها و اضافه کردن هسته های CPU ، حافظه و ذخیره سازی پشتیبانی می کند. این همچنین شامل قابلیت نظارت داخلی VNF است که امکان راه اندازی مجدد خودکار VNF ها را هنگام پایین آمدن و ارسال آلارم ( SNMP یا syslogs ) فراهم می کند.
* کلاینت Plug and Play: این کلاینت به طور خودکار هر میزبان مبتنی بر NFVIS را خودکار می کند. کلاینت Plug and Play با یک سرور Plug and Play که در مرکز DNA سیسکو کار می کند ارتباط برقرار می کند و با پیکربندی مناسب میزبان تهیه می شود. همچنین یک مدل استقرار بدون لمسی واقعی را امکان پذیر می کند ( یعنی هیچ مداخله ای از انسان وجود ندارد) و امکان استقرار سریع و بدون خطا از خدمات شبکه را فراهم می کند.
* هماهنگ سازی: مدلهای ارتباطی REST ، CLI ، HTTPS و NETCONF / YANG برای هماهنگ سازی و مدیریت پشتیبانی می شوند.
* سرور وب HTTPS: سرور وب می تواند اتصال به NFVIS را از طریق HTTPS به پورتال وب یک دستگاه محلی فعال کند. از این پورتال امکان بارگذاری بسته های VNF، اجرای مدیریت چرخه عمر کامل، بالا و پایین کردن سرویس ها، اتصال به کنسول های VNF و نظارت بر پارامترهای مهم، بدون نیاز به دستورها پیچیده وجود دارد.
* مدیریت دستگاه: ابزارها برای پشتیبانی از مدیریت دستگاه در NFVIS بسته بندی می شوند, از جمله یک مدیر منابع برای دریافت اطلاعات در مورد تعداد هسته های CPU اختصاص داده شده به VM ها و هسته های CPU که قبلاً توسط VM ها استفاده می شوند.
* کنترل دسترسی مبتنی بر نقش ( RBAC ): کاربران دسترسی به سیستم عامل با استفاده از RBAC احراز هویت می شوند.

# x86 بسترهای میزبانی

Cisco Enterprise NFVIS در سیستم عامل های میزبانی زیر Cisco x86 پشتیبانی می شود:

* سیستم محاسباتی شبکه سیسکو ( ENCS )
* بسترهای نرم افزاری خدمات ابری سیسکو
* سری ISR های سیسکو ۴۰۰۰ با تیغه E-Series سیسکو UCS
* C-Series UCS

اینکه کدام پلتفرم را انتخاب کنیم به الزامات و ویژگی های مورد نیاز بستگی دارد، مانند صدا از طریق IP ( VoIP ) ، الزامات رابط های غیر اترنت ( مانند T1 یا DSL ) ، 4G-LTE ، I/فن آوری های O از ( به عنوان مثال ، SR-IOV ) و تعداد هسته های CPU مورد نیاز برای پشتیبانی از نیازهای خدمات موجود ( VNFs و خدمات ) و همچنین نیازهای آینده پشتیبانی می کنند.

**وظایف آماده سازی آزمون**

همانطور که در بخش “ نحوه استفاده از این کتاب ” در مقدمه ذکر شد ، شما چند گزینه برای آماده سازی آزمون دارید: تمرینات اینجا ، فصل 30 ، “ آماده سازی نهایی,” و سؤالات شبیه سازی امتحان در نرم افزار آماده سازی آزمون پیرسون به صورت آنلاین.

# بررسی همه موضوعات کلیدی

مهمترین مباحث موجود در فصل را که با نماد مباحث کلیدی در حاشیه بیرونی صفحه ذکر شده است ، مرور کنید. در جدول 27-2 این مباحث کلیدی و شماره صفحه ای که در آن یافت می شود ذکر شده است.

جدول 27-2 مباحث اصلی برای فصل 27

|  |  |  |
| --- | --- | --- |
| عنصر موضوع اصلی | شرح | صفحه |
| بخش | مجازی سازی سرور | 794 |
| پاراگراف | تعریف ماشین مجازی | 794 |
| لیست | انواع هایپروایزر | 795 |
| پاراگراف | تعریف کانتینرها | 796 |
| پاراگراف | تعریف سوئیچ مجازی | 797 |
| پاراگراف | تعریف NFV | 799 |
| پاراگراف | تعریف OVS-DPDK | 805 |
| پاراگراف | تعریف PCI passthrough | 805 |
| پاراگراف | تعریف SR-IOV | 806 |
| پاراگراف | تعریف NFV سازمانی | 807 |
| لیست | معماری NFV سازمانی | 808 |
| پاراگراف | تعریف NFV MANO Enterprise | 808 |
| بخش | وظایف و کاربرد های شبکه مجازی | 810 |
| بخش | نرم افزار زیرساخت مجازی سازی عملکرد شبکه ( NFVIS ) | 810 |

# تکمیل جداول و لیست­ها از حافظه

یک نسخه از پیوست B ، “ جداول حافظه ” ( موجود در وب سایت همراه ) یا حداقل بخش این فصل را چاپ کنید و جداول و لیست ها را از حافظه تکمیل کنید. ضمیمه C ، “ کلید پاسخ به جداول حافظه ، ” همچنین در وب سایت همراه ، شامل جداول و لیست های تکمیل شده برای بررسی کار خود است.

# تعریف اصطلاحات کلیدی

اصطلاحات کلیدی زیر را از این فصل تعریف کنید و پاسخ های خود را در واژه­نامه بررسی کنید:

کانتینر

تصویر کانتینر

هایپروایزر

عملکرد شبکه (NF)

مجازی سازی توابع شبکه (NFV)

زیرساخت NFV (NFVI)

سرویس دهی

دستگاه مجازی ( VM )

عملکرد شبکه مجازی ( VNF )

سوئیچ مجازی ( vSwitch )