Software-Defined Branch

Transforming branch infrastructure for the digital economy

Introduction

What makes a good branch? Whether it's a retail location, an office, or an industrial facility, the most important characteristics are the location, the people, and the IT infrastructure. Today's businesses require an ever-increasing agility to meet changing customer demands, competitive pressures, and legislative requirements. That agility must be delivered without adding cost; IT infrastructure should be an enabler, not a drag.

All too often, the installed infrastructure is too rigid and inflexible, engineered to meet a requirement that has since evolved beyond the branch IT's capability to adapt. The only constant is change. Branch applications, security posture, the need for encrypted communications, bandwidth: all of these continue to evolve. Yet the infrastructure has remained static, resulting in IT moving from being part of yesterday's solution to today's problem.

A typical branch IT installation consists of multiple point products, each having a specific function, engineered into a rigid topology. Changing something in that chain, be it adding a new function or connection, increasing bandwidth, or introducing encryption, affects multiple separate products. This introduces risk, increases time to test, and increases roll-out time. If any piece of equipment requires a physical change, the time and personnel costs multiply.

There is another way. Virtualization, long since adopted in data centers, but until recently less so in the branch network, has come of age. Network Function Virtualization (NFV) is the concept of taking multiple functions previously existing as discrete hardware appliances and instead deploying these as Virtual Network Functions (VNFs) hosted on an x86-based compute platform. NFV delivers physical consolidation, saving space and power and fewer points of failure, and substantially improves IT agility. Changes can be made quickly, automated, and delivered without truck rolls.

This paper explores what the SD-Branch is, the features that it should support, and how it should be engineered to deliver on-demand network services.

Contents

Transforming branch infrastructure for the digital economy

Designing a branch infrastructure using a combination of a router and individual appliances can work. Careful selection of individual components can yield an overall solution well matched to current business requirements. Indeed, headroom can be engineered into the solution to accommodate future growth.

Unfortunately, that headroom needs to be repeated across multiple appliances, and there's no capacity sharing. This exacerbates the cost, especially when multiplied across a number of locations. The result is that organizations often underprovision this extra capacity, further constraining the IT capability to respond to changing business needs.

The headroom for future growth is normally limited to increases in traffic volume. A completely new business requirement might need the addition of a new function and hence the integration of a new appliance with associated cost and timeline, plus effects on adjacent components in the infrastructure. For example, many businesses are looking to realize efficiency gains through IoT solutions such as smart lighting and smart HVAC only to find their current infrastructure cannot support these new requirements.

In some cases, the requirement for a new function might be accommodated by a firmware upgrade offered by a point product vendor. If that's the case, great, but what if the new software needs extra compute the appliance doesn't have? What if the vendor doesn't offer quite what the business is looking for? Inevitably, device sprawl and upgrade cycles become out of step with one another.

The discrete components in the traditional solution each need space, power (sometimes specific cooling requirements), and critically support. Vendor support contracts cover both hardware and software. To mitigate against lengthy outages, an enterprise will often pay for next-day or even same-day replacement for critical hardware. This cost, when multiplied across several components, is significant. Some organizations will keep a spare onsite or close by if they have colocated sites. This can help, but still requires a technician to affect the swap.

Consolidation of one or more appliances into software running on a compute blade hosted in the site's router or even running in a virtual container on the router's own multi-core processor addresses many of these concerns. This strategy is actually a validation of the SD-Branch approach, discussed next.

Software-Defined Branch

With SD-Branch, network functions run inside a virtualized environment. SD-Branch deployments can even split up virtual appliances into discrete functions and then centralize these functions (such as any related to enterprise policy) into the headquarters, private data center, or hybrid cloud, rather than have to configure and deploy it all in branches. This approach is known as a Software-Defined WAN (SD-WAN).

What is SD-WAN?

The network infrastructure dynamically makes routing decisions based on business intent, defined centrally and implemented locally. The routing decision is based on network conditions, application requirements and security needs. This is software-defined WAN, or SD-WAN.

Purpose-built routers (physical or virtualized) have traditionally made local routing decisions based on policies configured into them individually. These policies can take into account WAN and peer connection state and often dynamic conditions. However, at some point it makes sense to push the policies and much of the decision making into a separate function (or control plane), which does not need to be colocated in the branch. The IT needs at the branch then change significantly; WAN routing in the branch is greatly simplified. Complex policy-based decision making is hosted at the optimum location in the network: the private data center, cloud, or hybrid cloud.

For those taking a phased implementation approach to SD-WAN, there is the possibility of freeing up resources in existing routers and using them as the new data plane in the SD-WAN. An example is Cisco® vEdge, which has a software-based data plane. It can operate on traditional router hardware or on more computing-oriented hardware.

Uniquely, SD-WAN has enabled low-cost branch rollouts that can scale across both small and large sites. The same software runs in every branch. Deploying the same routing and virtual network functions is just a matter of selecting the correct bandwidth and the desired hardware if legacy systems are currently installed. Recent hardware released by vendors such as Cisco supports SD-WAN either natively or with a compute card added. Newer hardware is purpose-built to be SD-WAN and VNF ready.

The inability of legacy solutions to provide IT flexibility for new business opportunities, improvements, scalability, or any significant cost reduction is driving SD-Branch. We see several trends that require, or benefit from, SD-Branch as a delivery mechanism.

Firstly, it is clear that SD-Branch reduces waste: branch platforms can be fine-tuned to support functionality for today and the future, and hardware can even be repurposed to smaller sites as larger ones grow. To take one example, renegotiating WAN connection charges left one business with a heap of redundant WAN optimization appliances: hardware resources that could have been redeployed for other functions if it were an SD-Branch-based solution.

SD-WAN adoption is a trend gathering momentum. It radically shifts compute requirements between branch and headquarters for WAN-related functions. Therefore the business needs a platform and a supporting SD-Branch infrastructure that allows network functionality, data plane, control plane and services plane to be portable compared to a traditional appliance approach.

Some businesses will prefer continuing with local routing and policy-based decision-making using a virtualized router in each site. Both approaches require SD-Branch-capable infrastructure to be able to tunnel data-plane packets through high-performance acceleration features built into CPUs today, to push data to Ethernet and other network interfaces rapidly.

And there are industry-specific trends that are rapidly gaining ground. In the retail vertical, we see businesses moving forward with radio- and sensor-based inventory and logistics, improving the purchase and checkout processes and building up useful datasets to understand their customers purchasing patterns. In the manufacturing sector, extensive data filtering and rapid decision making control are needed, with the ability to host and execute functions in the best location possible.

Nearly all proposed methods require local computing capability and a mechanism to deliver applications to branches in a maintainable manner and all of these trends can benefit from SD-Branch.

Isn't SD-Branch just virtualization?

SD-Branch is different from an IT project that just virtualizes applications. Some early adopters (in particular service providers and small enterprises that had dedicated UNIX staff) had no choice prior to SD-Branch and tried to formulate their own custom stack of hypervisor, software router and firewall running on a PC. They found it complicates branches, because each site still needs additional hardware for WAN connectivity, and the early adopters also found significant training and skill retention issues with this custom approach. From a technical perspective, there were also issues with using general software stacks assembled into something that didn't meet modern security needs and didn't have the flexibility or the deployment and management capabilities that the business required.

How does SD-Branch work?

The shift from a traditional WAN to an SD-WAN echoes a demand for the same flexibility from network appliances. It never made sense to have disparate infrastructure, management and configuration systems for supporting fundamental services such as virtual private networks and security, WAN acceleration, wireless control, voice- and application-level gateways, and so on. In the application world, there have been innovations in virtualization and container technology, but this is just one piece of the puzzle to be solved. Deploying at scale is a challenge too, as is making sure that critical services can cooperate, share resources, and function reliably. Deploying new sites rapidly and securely and managing them effectively are things that the new IT infrastructure must support. Here are the core features required for branch virtualization:

- Ability to deploy full applications (including, where necessary, their own OS or containerized microservices) from potentially any vendor
- Service chaining: the capability to define the order application flows are processed by relevant functions
- Ability for functions to use hardware acceleration to optimize traffic flows and encryption workloads
- Complete operational support, including zero-touch deployment of hardware infrastructure, virtual network functions and ongoing monitoring and management

Centralized Orchestration and Management

Use centralized orchestration and management to add, change, and delete services without disrupting overall service, and help ensure that services are delivered on-demand – all without having on site IT personnel to make the changes.

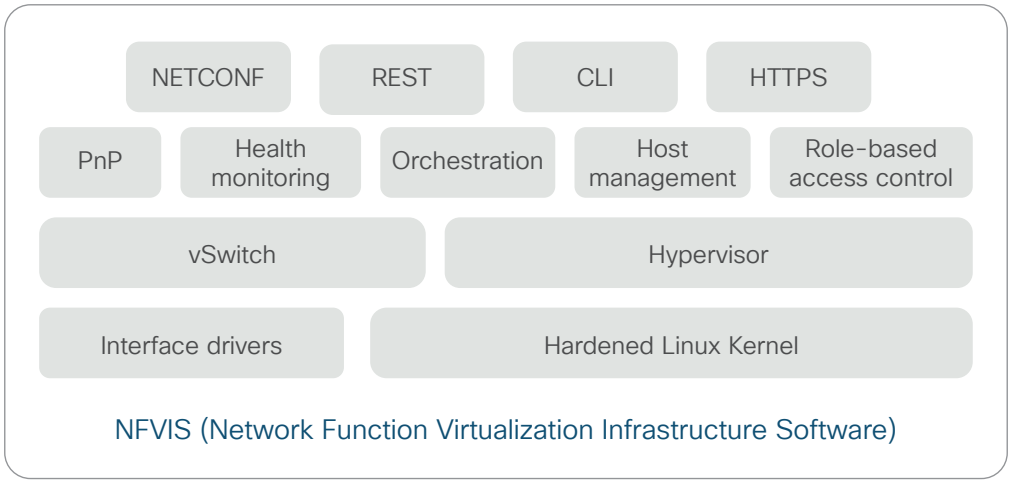
Centralized orchestration and management is about aligning the business request with the applications, data, and infrastructure. It defines the policies and service levels through automated workflows, provisioning, and change management. This creates an intent based infrastructure that can be scaled up or down based on the needs of each application and duplicated across the network.

It can deliver high-quality services faster and more easily through network automation For example, centralized orchestration reduces the time and effort for deploying multiple instances of a single application. This will save time and costs; as the need for more resources or a new application is triggered, automated tools now can perform tasks that previously could only be done by multiple administrators operating on their individual pieces of the physical stack.

Hypervisor/Complete Operating System– NFVIS

Figure 1 shows an example SD-Branch stack environment. Cisco's Network Function Virtualization Infrastructure Software (NFVIS) as a whole can be considered to be a complete Operating System (OS) for the SD-Branch. Designed for high uptime, it is built on a hardened Linux kernel with embedded drivers that take advantage of modern CPU capabilities such as Single-Root Input/Output Virtualization (SR-IOV) for plumbing high-speed interfaces directly into virtual network functions, and accelerators supporting encryption workloads.

Figure 1. NFVIS software



For new deployments, there are opportunities to roll out the technology more smoothly and cost-effectively than was ever possible with discrete appliances; this is explored next.

NFVIS: a path to better deployments

Any business will want to be sure that its deployment will go smoothly. Interestingly, SD-Branch offers unprecedented characteristics to achieve this compared to conventional IT rollouts.

Straight from the starting line, there is great return on investment to justify these projects. It is clear there are consolidation savings because of the elimination of appliances and associated support contracts. There are also huge gains in reliability, because vendors can offer validated designs where the full stack and best-practice network functions have already been tested at scale. The decreased equipment count also reduces the number of possible failure points. Prior to deployment, existing network traffic can be examined to determine scale needs. This takes a lot of risk and sizing issues out of the project in one go.

Day-zero, day-one, and ongoing operations should be zero-touch to reduce deployment costs. NFVIS takes advantage of the burned-in security certificate in new hardware to do this securely. There is no need to pre-stage equipment or send staff to remote sites during a deployment.

NFVIS technologies allow businesses to focus on their applications and business needs both during deployment and into the future, rather than spend effort learning how to glue appliances and protocols together. There are huge operations savings to be realized because NFVIS and virtual network functions will have been tested together and can be supported in a single contract with a single point of accountability.

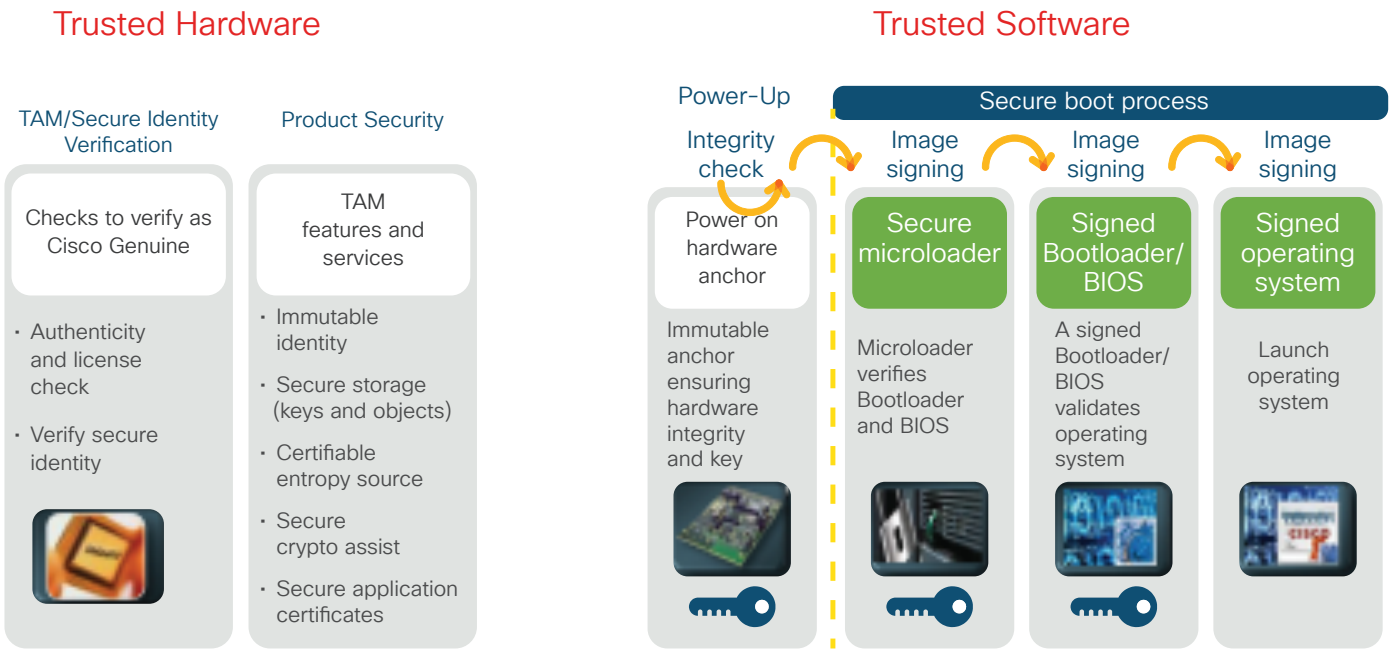
Is NFVIS secure?

One important question is whether VNFs and the underlying OS are secure. There are things that can be done at the hardware and software level to provide a secure environment providing multiple levels of resiliency. This includes secure boot capability, a hardware trust anchor, counterfeit protection, runtime defenses, OS validation and supporting secure standards for certificate authentication and ciphers for encryption. All this relies on close cooperation between the NFVIS and the underlying hardware.

The hardware trust anchor validates the integrity of boot code (before the OS is even run). It does this by only allowing a micro loader to function if the hardware trusts it; the microloader then executes and checks the bootloader, which then checks the OS. In other words, the chain of trust begins with the hardware trust anchor. These steps help ensure that hardware that has been tampered with, or firmware or software that has been modified, will not run.

Unique secure device identifiers, often with antitheft and antitamper chip designs, are embedded in modern hardware. A key pair in a cryptographically secure X.509 certificate is bound into the hardware during manufacture. In recent years, good network OS implementations also support runtime defenses that can detect attacks such as malicious code insertion and buffer overflow exploits.

Figure 2. Trustworthy System capabilities



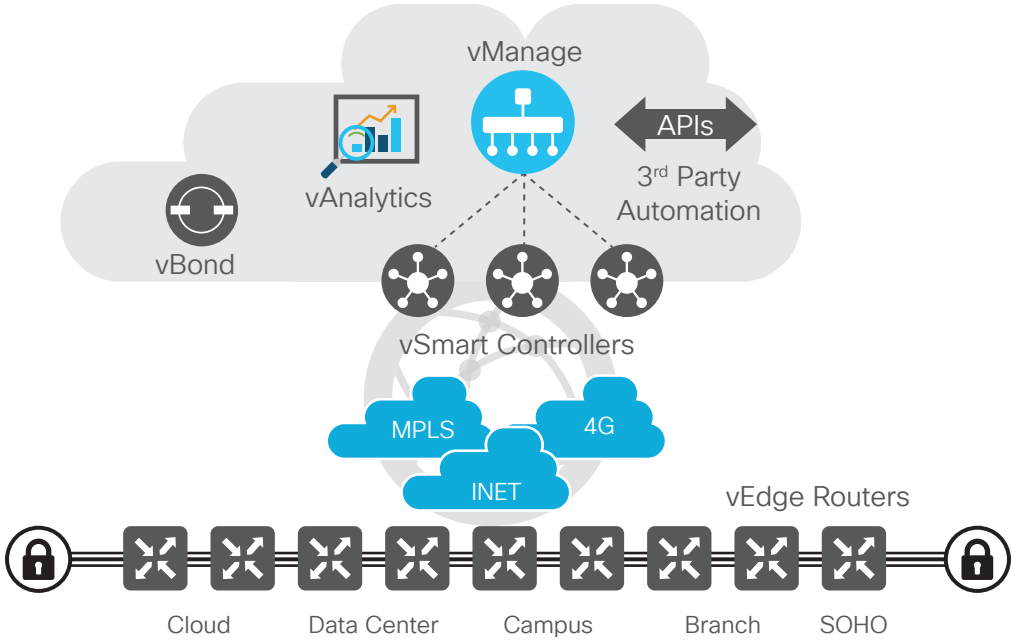
Virtual Network Functions

VNFs for routing and SD-WAN

It has been shown that VNFs can be used for running specific functions such as security or application acceleration. However, it is also possible to run branch LAN and WAN packet switching and routing operations, in lieu of running those tasks in traditional router architectures, even if traditional router hardware is used. You can separate the packet forwarding and switching tasks from the existing router software and run them inside a virtual machine, effectively as another VNF. There are several ways to do this. One straightforward way is to take the same software that runs on traditional routers and just run it as a virtual machine. This approach has helped businesses connect to, and make use of, private, public and hybrid clouds to deploy new services, achieve scale and save costs. One example is Cisco IOS® XE Software, which is a router OS that resides in everything from small desktops to large router appliances, but also works equally well in virtualized versions known as ISRv and CSR1000v, which run as a VNF in NFVIS and in clouds, respectively.

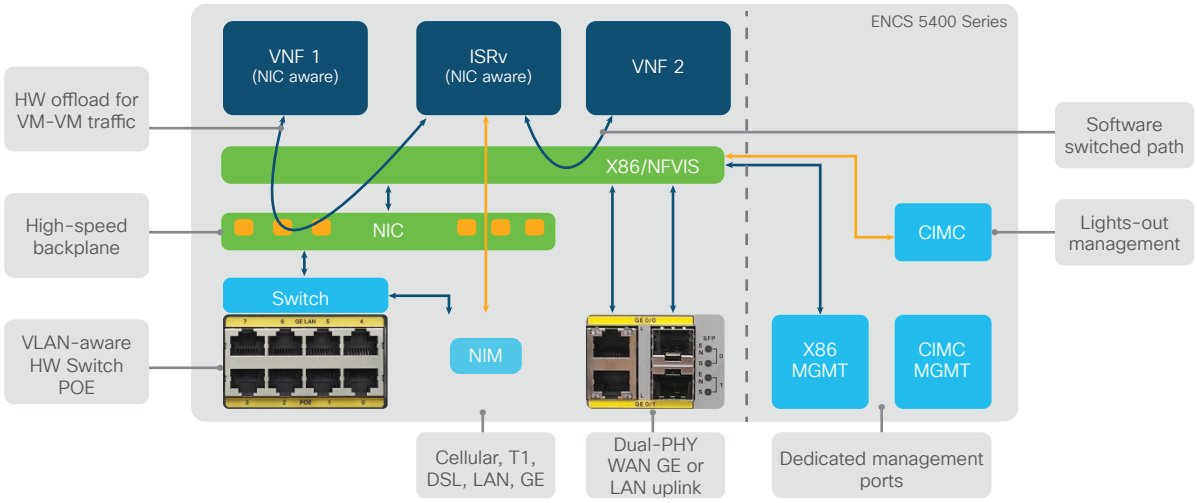
Virtualization alone does not reduce complexity; it stays the same. It is an enabler, however. For example, consider SD-WAN adoption. There is no need to run a full router such as ISRv as a VNF, and instead the monolithic traditional network appliance entity is broken up such that just the routing data plane runs in the branch. This is the Cisco SD-WAN approach. Cisco vEdge is run as a VNF at the branch; the control and management planes are centralized. It strips complexity out of the branch. Figure 3 shows how end-to-end connections are made through vEdge data-plane instances running as VNFs while high-touch services are abstracted away to a centralized location.

Figure 3. SD-WAN Data Plane and Control Plane



When VNFs are installed and virtually connected, the functions rely on the OS (NFVIS) for data flow and acceleration features. In Figure 4, the VNFs shown at the top have their data paths (shown in blue lines) either using software switching (to interwork with older VNFs) or with hardware-accelerated connections. When selecting an OS for NFV, it is important to make sure that performance will scale. This can be achieved through close collaboration between the OS vendor and the CPU manufacturer. SR-IOV is a contemporary technology that meets today's needs, but vendors should have a roadmap to use future advanced technologies too.

Figure 4. Cisco ENCS 5400 Architecture



In summary, with the proper infrastructure, it is evident that it is possible to create an environment that can scale easily and offers tremendous opportunity for cost saving. For many businesses, the compelling reason to do this is to have the agility to deploy rich services that will really affect their customers in positive and unique ways. It is worth exploring how that is possible with SD-Branch. We start with security.

Intrusion detection and prevention and malware protection

The threat landscape has changed significantly this decade, and networks need to protect against malware, denial-of-service attacks, and data protection breaches. Customers are rightly willing to vote with their wallets and shift loyalty if their data privacy is not respected. One way SD-Branch can help is by allowing the best-in-class security functions to run in branches when previously separate appliances would be cost prohibitive. Some traditional features such as secure Virtual Private Networks (VPNs) can be baked into the routing VNF, but others can be inserted into branches too, to support firewalling, intrusion detection and prevention, malware detection and Data Loss Prevention (DLP).

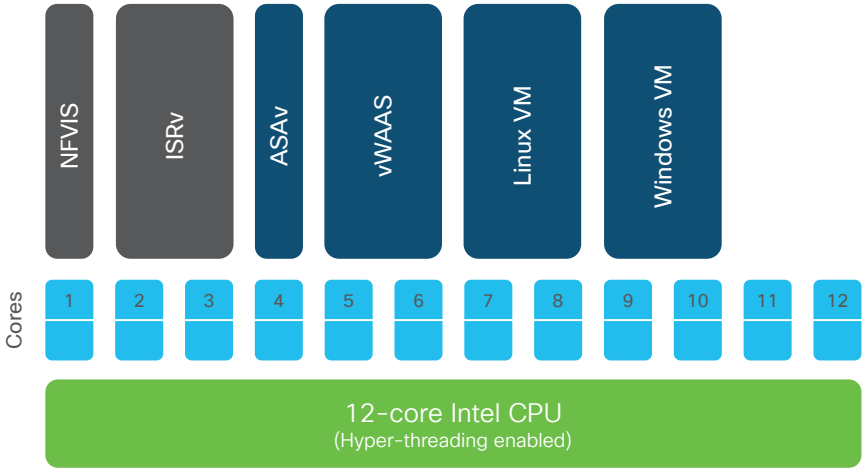
Other features are also worth examining when specifying your IT design. How easy is it to provide user-centric and data-centric access not just across sites, but even in the same branch? Is there a need for someone in the accounts department to access something private or sensitive in the legal department? How will the network automatically detect and physically block that? Does the infrastructure provide the necessary features to do this to standards that are acceptable for military or financial organizations; why should your customers expect any less?

Running branch applications

The past decade has seen the rapid adoption of cloud-based services; today enterprise applications run across private, hybrid, and public clouds. However, changing technologies mean that computing capability will have new uses in branches and industry. A good example of this is enterprise IoT; as more sensors are connected to networks, there is a growing need to filter data and make rapid local decisions at IoT gateways. There are also requirements to connect and power sensors and radio devices. Even with an all-cloud strategy, businesses require the ability to locally interface with sensors and output devices to process data, ultimately to make cost savings, improve a process, or significantly change the way staff and customers interact. SD-Branch makes it quick to do this and rapidly roll out these applications, whether to dozens or thousands of sites.

Any NFVIS architecture should support customer and third-party applications. Typically the applications and other VNFs would just slot in as with any virtualized architecture, but with some unique benefits, which we will discuss next. (See Figure 5.)

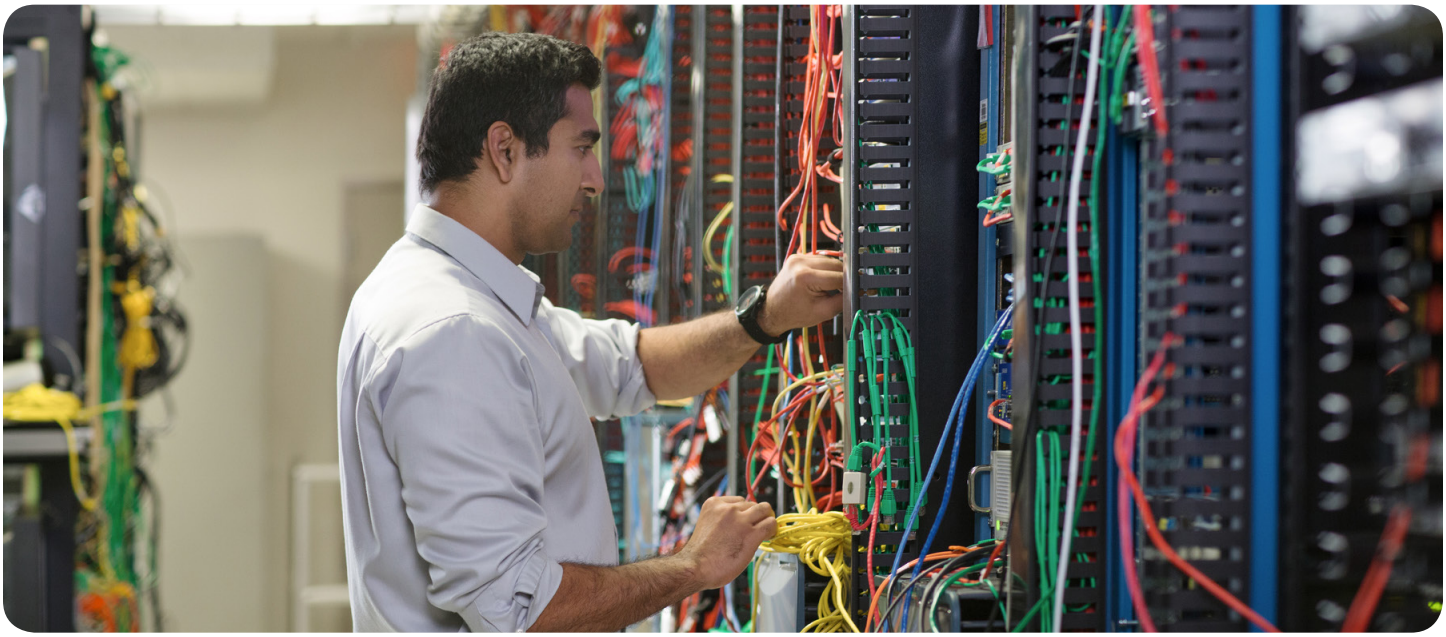
Figure 5. NFVIS and Example Network Functions



Hardware

As we have seen, building an SD-Branch has particular demands on the NFV infrastructure and the close interaction with the hardware for performance, security, and scale. How does one assemble a functioning and manageable deployment from commercial off-the-shelf computer hardware and various software frameworks without achieving a wobbly stack of uncertainty?

Figure 6. IT can be messy without SD-Branch



First, a primary consideration is that through careful design of resource allocation, it must be guaranteed that no critical services will be starved of CPU or memory. The NFVIS infrastructure is able to pin itself and primary functions to particular CPU cores to provide sustained performance.

Another consideration is maintaining flexibility for branch and operations transformations through applications and IT. Modern CPUs have many cores with hyperthreading, and with the correct selection of CPU and hardware resources, the end result is an astonishing amount of network functions and customer applications can be run on platforms as small as a single rack unit, ideal for space-constrained branches such as retail sites.

Continuing to examine the close relationship between the software infrastructure and the underlying hardware, it is clear the software infrastructure and the hardware security features must work together to support primary functionality such as zero-touch secure configuration and chain of trust. Hardware, interfaces, and software must be designed to prevent malicious modification and malware when migrating from discrete appliances.

The hardware matters. Often there are difficulties with just inserting a traditional workstation or server in the branch. The fact is, for some sites (especially retail) a physically large PC or server is a severe compromise. They end up sitting on the floor, in a small office, fans clogged with dust, or worse, on or behind the store counter, perhaps integrated into the monitor, simply because there isn't space elsewhere. Consumer-grade PCs are cheap but unserviceable when components such as motherboards become obsolete.

Server-grade PCs can have a longer product life and better support options, but there often is little room for a large rack full of multivendor gear. There could even be support implications if different-vendor equipment is inside a rack supplied by one of the vendors. These are all important things to consider when deciding how to deploy SD-Branch and other third-party applications.

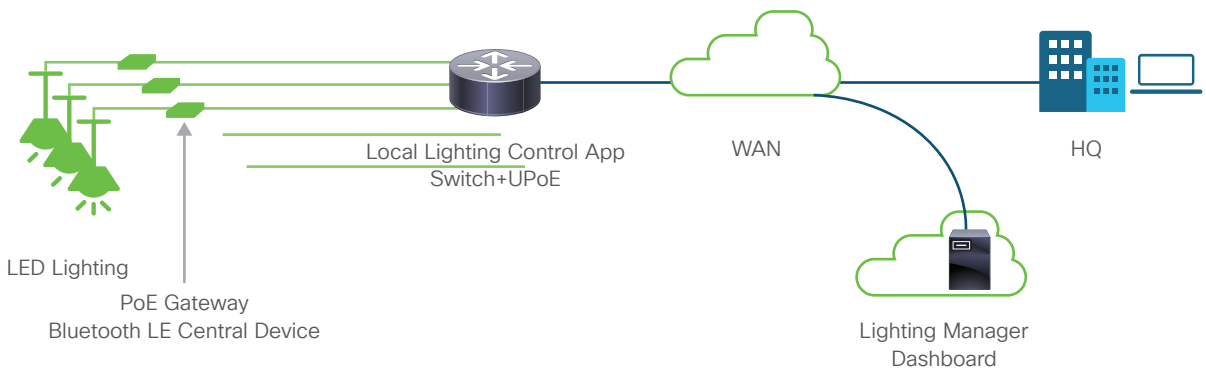
In terms of physical interfaces, Power over Ethernet (PoE) is highly attractive because many IoT sensors rely on this. Branches often also require WAN interfaces such as 4G LTE, essential not only for backup or load sharing, but also for rapidly deploying new sites prior to wired connections being available from the service provider. Some locations might require legacy TDM links too, so it is important to deploy platforms having the flexibility to support more than just Ethernet.

Other use cases

Energy management and connected lighting

There are huge opportunities to save costs with SD-Branch. An example is connected lighting. PoE allows for high-power lighting to be controlled by applications locally or in the cloud. A compute platform with built-in PoE and switch modules is highly desirable for powering lighting and sensors. The first 70 percent of lighting energy savings is achieved by moving to more efficient lamps, which many businesses have already done. But there are enough additional savings achievable to be worthwhile moving to connected lighting. (See Figure 7.)

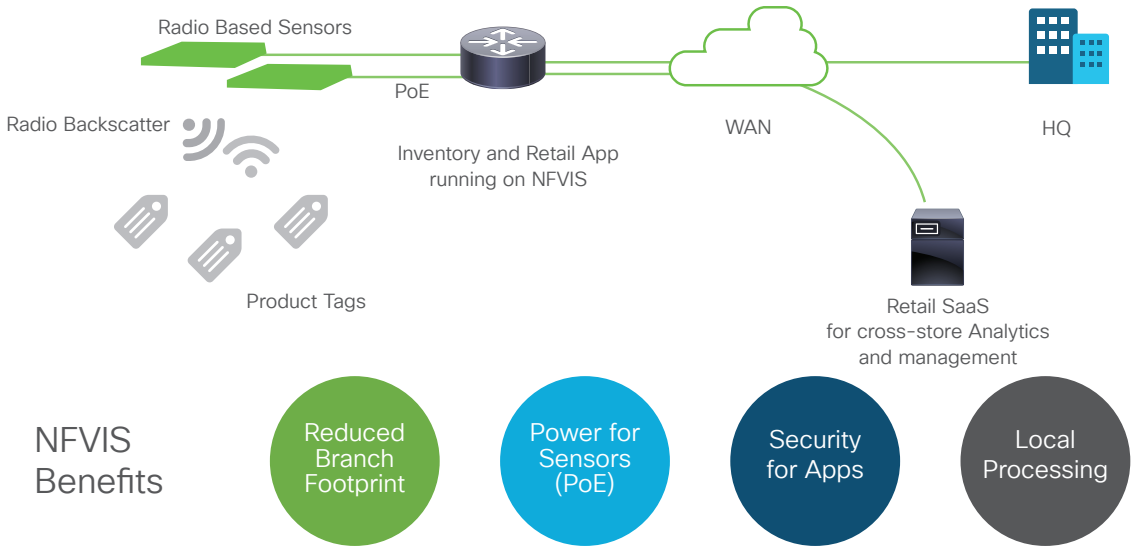
Figure 7. Retail Lighting



Internet of Things in retail

Virtually any application can be deployed on an NFVIS architecture, even those not envisioned initially by businesses. Better inventory tracking sounds like an internal process improvement, but through technology, businesses have found a way to turn such an advantage into a unique customer experience too. Radio modules that operate using PoE can be installed in retail stores, where they can scan passive tags attached to inventory. Using this method, there is branch-level awareness of the location of inventory throughout the retail space and the stockrooms. Mobile apps allow the store attendants to immediately locate any particular item, even if an item is moved by a customer from the cosmetics department to the shoe department, in a particular store. (See Figure 8.)

Figure 8. Retail Inventory Management



Industry 4.0

Manufacturing sites and customers of industrial equipment can see huge benefits in running applications locally and securely on reliable hardware. Privacy and data protection are a huge concern, and the ability to run security VNFs is attractive. There are two main scenarios in which integrated computing and NFVIS are useful.

The first scenario concerns manufacturing sites. The ability to digitize existing machine information, locally process it, and provide detailed reports allows manufacturers to better optimize their sites and improve machine and resource usage and work conditions. However, increasingly, manufacturers are finding that they can use the same systems to create new service offerings too.

Local computing can be used to make rapid decisions as well as long-term machine monitoring. It allows preemptive maintenance to become more accurate and businesses to offer such new services to their industrial customers for remote machine monitoring; a type of 'connected services' for industry. There is no reason why VNFs and applications cannot be deployed on oil rigs, aircraft, and ships from a technical perspective, provided the underlying hardware has network interface capabilities to suit the requirements. There have been deployments of virtual routing functions on rail networks too. These are all areas where stringent testing and certifications were needed. It is important to choose hardware that is designed for a long service life, even if it needs to be housed in enclosures or racks to suit particular deployments. Unlike off-the-shelf consumer-grade PCs, routers with integrated compute power are deployable in unusual environments such as ships, outdoor cell sites, and so on. Some hardware will even adapt to altitude and run fans at different speeds to optimize airflow.

Benefits of SD-Branch for Enterprises

The SD-Branch is a natural evolution for enterprises. It is tearing down barriers that made business and IT solutions difficult to justify and deploy in the past. The SD-Branch and a software-defined network are about more than virtualization. They finally separate the monolithic appliances, virtual or otherwise, into a simpler system of functions that can be easily reconfigured to meet changing requirements.

Businesses can use SD-Branch to reduce costs and gain reliability, ease of management, and agility. Some will use SD-Branch as a launchpad for deploying innovation in their business. Others will use it to gain the trust of their customers through better security.

Benefits of SD-Branch for Managed Service Providers

Managed Service Providers (MSPs) will gain significant service agility using centralized orchestration and management to simplify the process of provisioning and controlling applications and services. SD-Branch and centralized orchestration decouples network services from specific components, while automatically configuring the network according to the service specifications.

As a result, the addition of new services and devices is faster and easier and no longer requires a truck roll to remote sites. The orchestrator reduces the time needed to design, deploy, and manage new services. It makes possible true, realtime service provisioning. It enables you to:

- Bring services to market faster
- Improve your service agility
- More quickly act on and identify new revenue opportunities
- Enhance operational efficiency

Summary

Cisco has developed purpose built hardware platforms for the SD-Branch running an OS and hypervisor (NFVIS) that is truly network services enabled and avoids the pitfalls of a generic x86 based Server or “white box” solution. The NFVIS implementation is designed for high levels of up-time by adopting a hardened Linux kernel and embedded drivers and low-level accelerations that can take advantage of modern CPU features such as Single-Root Input/Output Virtualization (SR-IOV), for plumbing high speed interfaces directly into virtual network functions. Security is burned-in, simplifying day-zero installations with plug-and-play, and ensuring that only trusted applications and services will boot up and run inside your network.

Now because you do not need specific hardware for each function the SD-Branch allows operators to deploy Network Function Visualization (NFV) services more quickly and with more flexibility – **now you can do it all with software**.

A key component of the Cisco SD-Branch is centralized orchestration and management of the WAN network, the branch platforms and the services running on that network. Orchestration provides the ability to manage and carry out the initial deployment, changes and new services additions to your IT environment from a single location – instead of expensive and time-consuming visits to each individual branch office.

The Cisco SD-Branch solution offers an open environment for the virtualization of both network functions and applications in the enterprise branch. Both Cisco and third-party VNFs can be on-boarded onto the solution. Applications running in a Linux or Windows environment can also be instantiated on top of NFVIS and can be managed by software known as Cisco DNA Center.

Some network functions that Cisco offers in a virtual form factor include:

- Cisco Integrated Services Virtual Router (ISRv) for virtual routing
- Cisco vEdge Router (vEdge) for virtual SD-WAN routing
- Cisco Adaptive Security Virtual Appliance (ASAv) for a virtual firewall
- Cisco Firepower™Next-GenerationFirewall Virtual (NGFWv) for integrated firewall and intrusion detection and prevention (IPS and IDS)
- Cisco Virtual Wide Area Application Services (vWAAS) for virtualized WAN optimization
- Cisco Virtual Wireless Controller (vWLC) for a virtualized wireless LAN controller

All businesses can benefit from NFVIS, and it is straightforward and cost-effective to deploy because many existing routers can be upgraded with x86 compute cards to become the physical host for NFVIS. For new or growing sites, new hardware can natively support NFVIS. It performs at scale too, taking advantage of accelerations in specific CPUs and hardware. Security is burned in, simplifying day-zero installations with plug-and-play and making sure that only trusted systems will boot up and run inside your network.

It is exciting to see the opportunity for real innovation in businesses that have their IT infrastructure designed for driving that innovation. The primary thing is simply flexibility. You cannot entirely predict all the innovations, new ways of working, and new customer experiences that will get adopted for success in the future, but getting there is a lot easier when the barriers to rapid deployment and effective management of applications are removed.

If SD-Branch has sparked your interest, and you're interested to learn more, check out the following blog posts and documents.

For more information

Cisco SD-Branch

https://www.cisco.com/go/sd-branch

Why Cisco SD-Branch is better than a 'white box'

https://blogs.cisco.com/enterprise/why-cisco-sd-branch-is-better-than-a-white-box

What is NFVIS?

https://blogs.cisco.com/enterprise/what-is-cisco-nfv-infrastructure-software

Enterprise NFV platform: ENCS 5000

https://www.cisco.com/c/en/us/products/routers/5000-series-enterprise-network-compute-system/index.html

Security

The World's Most Widely Deployed IPS Technology https://www.cisco.com/c/en/us/products/collateral/security/brief_c17-733286.html

Secure Internet Gateway in the Cloud

https://umbrella.cisco.com/

Detecting zero-day attacks with Stealthwatch

https://blogs.cisco.com/security/cisco-stealthwatch-learning-network-license-for-your-digital-ready-network

C11-740881-00 09/18