Ovum
TMT intelligence | informa

2019 Trends to Watch: Network Services

SD-WAN, cloud connectivity leap forward, NFV shuffles ahead, and portals pull it all together

Publication Date: 15 Nov 2018 | Product code: ENS004-000044

Brian Washburn

Summary

Catalyst

For network providers, 2018 is a year of progress. Software-defined wide-area network (SD-WAN) platforms and services expanded beyond widespread enterprise trials. SD-WAN is also extending deeper into enterprise commercial deployments, both up- and down-market. As enterprises add SD-WAN they also accelerate the move to hybrid networking, replacing dual-MPLS/dual-router private networks. Enterprise network functions virtualization (NFV) has been low profile in comparison to SD-WAN. Enterprises are testing premises-based virtualized and universal customer premises equipment (vCPE/uCPE) but it still has a small managed services customer base. This report updates these trends – SD-WAN, NFV, hybrid networking, cloud connectivity services, and the back-office capabilities that support these new network services and tie them all together.

Ovum view

In Ovum's 2018 discussions with large enterprise decision-makers, several trends are clear. First, enterprises need to connect to many clouds, in a range of ways. Some applications need secure, high-performance private connections; others work with best-effort internet VPN; still more use a hybrid approach. Second, SD-WAN continues moving to mainstream deployment. Whether decision-makers decide to deploy SD-WAN themselves or turn to managed service providers for help, there is mainstream enterprise interest, initial adoption, and continued brisk adds for these platforms. Third, enterprise decision-makers are heavily involved with virtualization on multiple fronts, including NFV platforms and services. But provider-managed NFV for enterprises – especially virtual functions sitting on customer premises equipment (CPE) cloud stacks – remains uncommon. Enterprises and service providers expect SD-WAN and NFV to have a relationship, even as each of them continues to evolve individually. They also see a need for new services and platforms somehow to fold back into common systems, so their portals can provide visibility into and manage ICT estates that are increasingly fragmented. Enterprises that adopted various technologies independently for their benefits now want one centralized portal to view, monitor, and control their services.

Key messages

- The concepts behind SD-WAN are now mainstream among larger enterprises. But many enterprises still have not gone beyond trials. They will need to be convinced of the benefits of partnering with a service provider for managed SD-WAN over a do-it-yourself approach.
- Enterprises have embraced virtualization elsewhere in their IT operations. But when it comes to commercial managed NFV-based services, deployments are limited, with most still dabbling. NFV's benefits remain somewhat abstract compared to SD-WAN's practical new features.
- Industry players call many different things "SD-WAN" or an "SD-x" variant. There is no enforceable definition. Industry association MEF aims to bring some order to the market, but the industry is still some way off basic SD-WAN commonality and compatibility.
- SD-WAN works flexibly across disparate access types and different underlay networks. That invigorates enterprise acceptance of internet VPNs, including broadband and wireless access

as a complement – or even full-blown alternative – to private IP over dedicated access. The industry continues to test the extent to which enterprises are comfortable pulling the plug on MPLS VPNs in favor of internet VPNs.

- SD-WAN variants, NFV-based services, bandwidth on demand, WAN/cloud connectivity, and hybrid networking are all managed services aspects, yet each comes from a different source. Network providers add value when they consolidate these services into consistent, cross-platform reporting and management interfaces, with APIs for enterprises to connect portal intelligence with their own management systems.

Recommendations

Recommendations for enterprises

- Enterprises need to pin down the problem they want SD-WAN to solve. Cisco Viptela, VMware VeloCloud, Nokia Nuage Networks, or Versa Networks have a different focus from Cisco Meraki, Cradlepoint, Silver Peak, or Riverbed. FatPipe and Aryaka SD-WAN also have a different focus, as do various in-house-designed controller platforms by AT&T, Tata Communications, and Masergy.
- Ovum research finds that the great majority of enterprises exploring SD-WAN think they can go it alone, without provider-managed services. SD-WAN resolves router complexity but introduces a centralized controller to host, new options for applications management, and increased complexity of hybrid network management.
- SD-WAN and hybrid networking go hand in hand for enterprises. SD-WAN eases the way for hybrid WAN. Displacing private IP with internet VPN decreases costs. SD-WAN also tends to have licensing costs, potentially dual CPE at each end location and a centralized controller to manage, which can eat into expected savings.
- Managed SD-WAN service provider partners help by shouldering deployment responsibility and risk. Enterprises should look for a SD-WAN partner that has integrated overlay and on-net/off-net underlay views available or on its near-term roadmap. This is a valuable feature for full service visibility, management, and trouble resolution.
- Enterprises should think through in advance how they might extend SD-WAN to their cloud destinations for end-to-end monitoring and management. They might be able to source and deploy SD-WAN virtual network functions (VNFs). Some providers host managed SD-WAN gateways located adjacent to major cloud locations. Some providers support managed SD-WAN VNFs that the customer embeds in its cloud services.
- Enterprises have several routes to commercial NFV services. If an enterprise's goal is large-scale deployment in its organization with multiple VNFs, Ovum strongly recommends seeking out a partner provider. The service provider should already have built NFV orchestration and assembled a multivendor VNF environment. These efforts are costly and complex.
- Especially in new technology areas such as SD-WAN and NFV, enterprises should look for customer referrals across the partners and vendor platforms they are considering. The solutions the enterprise is considering should have referral customers of a similar size and scope willing to discuss their experience.

Recommendations for network providers

- There are many SD-WAN vendors and platforms to choose from, each emphasizing different features and strengths. In 2019, major providers should support managed services from at least two SD-WAN platforms, possibly more to cover a wider range of needs and price points. Providers tend to select Cisco (Viptela and/or Meraki), plus one or more platform(s) depending on their focus on partner, cost, performance, and features.
- From Ovum's discussions, it is clear that service providers must participate in SD-WAN, and not just for revenues. Much of SD-WAN's value comes from pulling through network-services sales and renewals. SD-WAN also helps sell advisory professional services and other managed services.
- Network providers have opportunities to adapt their business internet services to the needs of hybrid networks. Providers might use traffic management on their internet backbone to support performance guarantees – if the enterprise buys its managed internet services. Providers might also offer better SLAs paired with detailed internet performance reporting by using tools such as in-network agents and endpoint probes.
- The first fully orchestrated, commercial enterprise NFV service platforms were costly and time consuming to build. Key NFV vendors such as Red Hat, VMware, Juniper, and Cisco are growing the knowledge base, and integrators are developing better prefabricated environments. Operators can check back to see whether a commercial enterprise NFV platform that was unaffordable two years ago might now be within reach.
- Can operators turn to SD-WAN platforms as a backdoor way to offering NFV-based services? VMware VeloCloud, Nokia Nuage Networks, and Versa Networks, for example, can host third-party applications. Today they mainly pair with firewall and security vendors. The idea seems solid, as Ovum has found enterprises trialing one are likelier to dabble in the other. For smaller providers, SD-WAN that also hosts one or two third-party VNFs may be a viable business bundle if the price and performance are right.
- Providers need to think about how they will tie new offers such as SD-WAN and NFV back to their overall network management systems. Enterprises do not draw solid lines between physical and virtual network devices, between on-net and off-net segments, or between overlays and underlays. To them, it is all the enterprise network. If there is a service issue, enterprises expect a fast way to find the issue and expedite resolution.
- Providers have a niche they may be able to hold, front-ending managed multicloud connectivity. The concept is to front-end cloud locations with secure, dynamic port setup/teardown and bandwidth control; a range of hosted VNFs; and a rule set for enforcing regulatory and corporate cloud compliance. Cloud exchange players are likely also to try and take on this space.

SD-WAN concepts are mainstream, but differences abound on definitions

What is and is not SD-WAN?

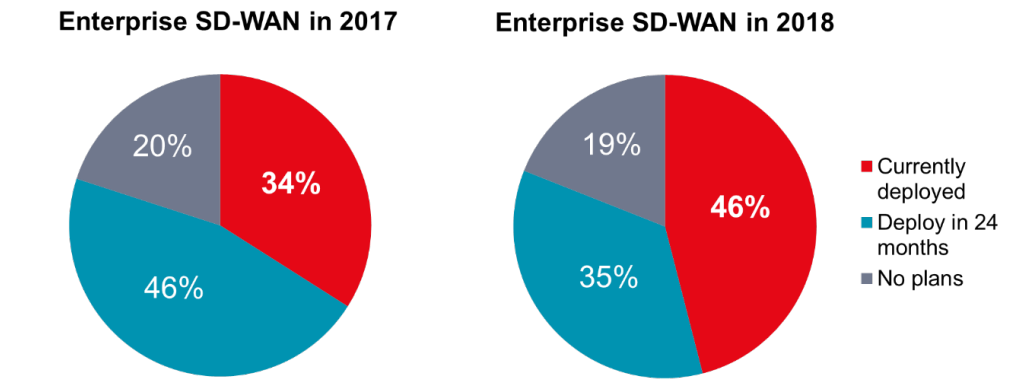
Since its *Enterprise Network Services Survey 2017*, Ovum has seen progress in the rate of adoption by large enterprises of SD-WAN platforms and services (see Figure 1). SD-WAN is not yet nearly as pervasive as the 46% enterprise adoption rate suggests. Many enterprises are still in trials or proofs of concept, or have limited commercial deployments. Enterprises also have different ideas of what SD-WAN is, because many vendors and service providers create their own definitions, sowing confusion.

SD-WAN adoption becomes even blurrier when taking into account products and services that companies describe as "SD-WAN." Many platforms might claim to be "software-defined wide-area networks." But there is great variance in platform features. It is generally accepted that Cisco Viptela, Versa Networks, and VMware VeloCloud adhere to the definition of SD-WAN. Nokia Nuage Networks and Juniper each leverage their respective heritage as major networking-equipment providers. Other players extend the model and incorporate their respective strengths. Silver Peak, Riverbed, and Citrix leverage their traffic optimization heritage, while Fortinet and Infovista bring their respective background expertise to their SD-WAN platforms. Cisco Meraki leverages centralized controllers and wireless LAN, and describes the result as SD-WAN. One of the few commonalities these platforms have is centralized management through a controller.

But vendors are only part of SD-WAN's history. Specialty managed service providers such as FatPipe, Aryaka, and TeloIP sold applications optimization services years before the term SD-WAN existed. Other specialty service providers such as Cradlepoint, Teridion, Netrolix, and even Akamai handle intelligent traffic delivery differently from conventional SD-WAN. They produce traffic management and traffic optimization results that either complement or compete with other SD-WAN platforms and services. Industry association MEF has published an SD-WAN specification and is looking toward a certification process for standards adherence in 2Q19, but SD-WAN platforms will also stay very different from one another.

Most major enterprise network providers have at least one formal SD-WAN vendor partner. Many have rolled out two or three primary partners, with some supporting more (NTT Com claims support for more than 10 SD-WAN platforms). There are also house-branded SD-WAN solutions from Aryaka, AT&T, Masergy, Hughes Network Systems, and Tata Communications. The features of these SD-WAN platforms differ greatly from one service provider to the next. The common point for provider-developed in-house SD-WAN services is a focus on cutting costs and/or preserving the client's installed base of CPE as an alternative to going with costlier third-party SD-WAN vendor licensing.

Figure 1: Major global, regional, and national operators have adopted SD-WAN platforms



Note: Surveys used different sampling criteria.

Source: Ovum

Provider challenges in enterprise SD-WAN deployment plans

Ovum sees strong enterprise momentum for SD-WAN in both its quantitative surveys and its qualitative enterprise discussions. But with it come some new complications and challenges for service providers that would host, manage, and/or support enterprise SD-WAN.

First, Ovum finds that a large majority of enterprise executives considering SD-WAN at first assume deployment and self-management is easy. Therefore, they plan to deploy their own SD-WAN from scratch. Enterprises may be sold on the benefits of centralized controllers, zero-touch provisioning, and easy management under a "single pane of glass." They have yet to experience separate underlay and overlay layers, variations in on-net versus off-net visibility, the management headaches of aggregating carriers, the complexity of hosting a SD-WAN controller, or dealing with applications-performance troubleshooting. They also have not yet begun migrating CPE and network models or dealt with resulting shifts in traffic patterns that affect other connected resources.

A second challenge for network providers is enterprises that believe SD-WAN with business internet services is good enough, and that enterprises can "ditch" their expensive, inflexible IP/MPLS services. It may work, if the enterprise uses performance-tolerant applications and keeps redundancy, and if partner ISPs offer strong enough performance (e.g., low oversubscription ratios) that their internet traffic gets through even at peak times. The reality, according to several network providers, is that 80–90% of enterprises that use MPLS VPNs and add SD-WAN services retain MPLS VPN to various degrees for now.

There is an all-internet option that can maintain performance guarantees. Some network providers offer internet-performance guarantees between locations, if the company uses that provider's dedicated access services and managed internet backbone. Providers that support internet backbone performance include AT&T, CenturyLink, Singtel, and Tata Communications, though there are certainly others. Providers tend not to broadcast their on-net managed-internet performance guarantees because of limits on where and how these services are available.

A third challenge for network providers is enterprises that partner with them to launch open-ended SD-WAN proofs of concept (PoCs), and then sit on one or more PoCs indefinitely. When SD-WAN was still fresh, network providers made onboarding easy through generous, no-charge SD-WAN "try

before you buy" policies. Some enterprises took the offer and now continue to use one or more PoCs without cost, deadline, purchase commitment, or consequence. Network providers make an investment when they set up SD-WAN PoCs, and indefinite trial periods drain those resources.

Network providers that did not set up-front limits on customer SD-WAN trials are in a quandary how to proceed. Some large enterprises are just slow decision-makers. If the provider partner forcefully pulls the plug on a SD-WAN trial, the enterprise might disqualify them. Providers are now trying to clamp down by qualifying enterprise opportunities and setting fixed trial terms. One operator, for example, aims to get more of a commitment from prospects by wrapping trials with contracts. Its goal is to sign a contract before it ships gear for a trial period. The contract has a delayed start and an "out" clause, and the enterprise can cancel or delay if the trial exposes problems. If the enterprise does not trigger the "out" clause before the trial expires, the full commercial contract goes into effect. At least as a concept, this goal may help rein in companies not yet serious about SD-WAN.

What to look for in 2019

Enterprises continue to show healthy demand for SD-WAN platforms and their pragmatic, practical feature sets. The distinctions between conventional router, SD-WAN, and other network functions will blur further in 2019. On the vendor front, Juniper already supports its SD-WAN controller via Contrail orchestration across its SRX, NFX, and MX routers. In 2018 Cisco added some Viptela SD-WAN features to its ISR and ASR routers. Nokia Nuage Networks, VMware VeloCloud, and Versa Networks support some third-party VNFs inside their SD-WAN endpoints, edging into NFV platform territory.

With all the different provider and vendor variants claiming to be SD-WAN, it will be no easier in 2019 to pin down SD-WAN subcategories and expected features. Standards efforts have started, and there is an effort to set some common management API calls, but any SD-WAN platform standardization is probably further out. Enterprises considering SD-WAN confront a barrage of marketing messages. For enterprises, the easy (if not always the best) answer is to block out the noise and turn to known and trusted partners for a solution.

For 2019, network providers will introduce SD-WAN platforms and features with consolidated enterprise portals for better visibility and management control. In-network gateways, overlay/underlay integration, and pairing SD-WAN applications intelligence with underlying SDN-based WAN and cloud connectivity services are some of the ways that network providers will incorporate SD-WAN with their other services to differentiate from over-the-top SD-WAN. Network providers will support more platforms, and they will draw on past projects to make adoption faster and easier for new clients. At the same time, Ovum expects service providers to tighten up their SD-WAN trial policies, to weed out indefinite tests and target serious buyers.

Meanwhile, hybrid networking already had healthy acceptance prior to SD-WAN, and SD-WAN accelerates this trend. SD-WAN lets enterprises mix disparate wireline and wireless access types together freely. This is a boon to providers with deep wireless assets to leverage for business services. Many operators stand to benefit, particularly providers focused on wireless assets such as Vodafone, Telefónica, Sprint, and América Móvil. Though 4G LTE wireless backup is popular today, the bandwidth and performance promise of 5G wireless broadband will further build the potential for wireless broadband secure-access services.

In 2019 and for a few years beyond, MPLS will be in a controlled deceleration rather than falling off a cliff. Enterprises that already have private IP services in 2019 will continue to hold on to their primary links while shifting to internet VPN use for secondary links and small branch offices.

NFV fires a telco revolution while early commercial enterprise services smolder

Many approaches to virtualization

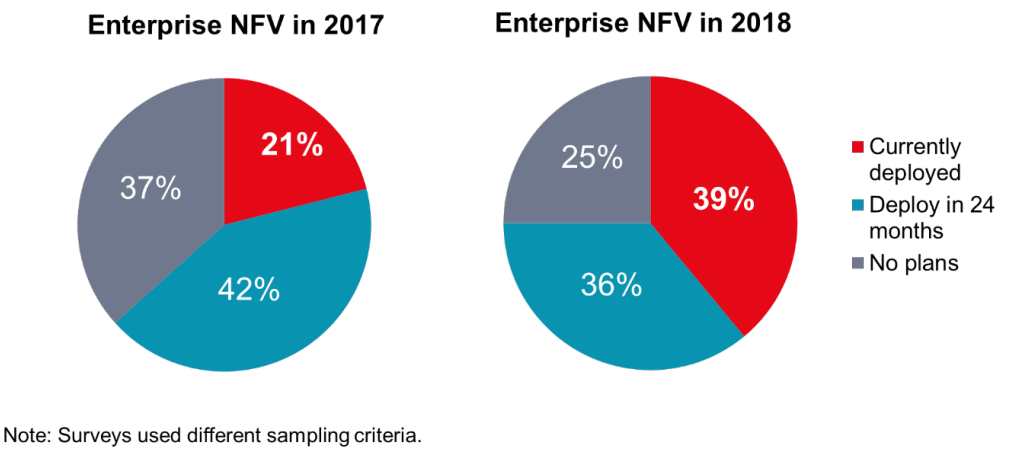
Network functions virtualization takes many different roles inside service providers. Based on its discussions with operators, Ovum has broadly categorized service provider NFV efforts:

- **Drop-in replacement of conventional physical gear with virtual equivalents.** A common example here is in wireless networks: 4G introduced drop-in virtualized evolved packet core (vEPC) components that are functionally identical to conventional EPC. 5G goes further in supporting virtualized network infrastructure.
- **Replacement of specialized vertical functions.** Big operators have long needed high-performance hardened servers for very specialized tasks. Examples include toll-free voice routing and DNS lookups. They could also use high-performance compute for other special functions such as BGP route reflection, large-scale NAT, and MPLS multicast. But the most interesting facet here is multitenant network gateways: these can move off static router appliances and onto more flexible NFV platforms.
- **Commercial NFV services – centralized/cloud-based.** These are hosted VNF services sold to businesses. The most common example is centralized virtual-enterprise firewall and unified threat management. This category also includes VNFs that an enterprise might deploy in a data center or public cloud, managed by the service provider.
- **Commercial NFV services – premises based.** This is the x86-based hardware "white box" or "gray box" that hosts an array of VNFs, managed by the service provider. When enterprises think of NFV, they may think of this first: a box on their premises that runs network software – router, firewall, SD-WAN, and/or other functions.

Telcos widely deploy the first two types of NFV, usually because the virtualized version saves money (e.g., through lower-cost gear or more efficient use of resources). They are also more future proof (i.e., NFV hardware can be expanded and repurposed as needed), and in some cases are easier to deploy than physical appliances, which must be shipped, connected, and activated.

Network providers have been slower to introduce commercial NFV services, and large enterprises have been slower to adopt NFV platforms and services, though interest has grown fast (see Figure 2). As with SD-WAN adoption, enterprise adoption rates can be misleading. In its qualitative interviews with enterprises, Ovum finds most are still dabbling with NFV platforms and/or services.

Figure 2: Enterprises are adding commercial NFV platforms and services into their ICT mix



Note: Surveys used different sampling criteria.

Source: Ovum

Commercial NFV services need a stronger adoption catalyst

Many inhibitors keep commercial enterprise NFV services rollout tepid. Building the underlying multivendor orchestration systems to support NFV has been costly and resource intensive. This effort was at first too daunting for many operators. The barriers to entry are lessening, as NFV specialists build up their NFV knowledge base. Enterprises still need bigger incentives to make the leap. By itself, the offer to replace some physical appliances with compute hardware and virtual software is only interesting. Swapping out a physical router for a virtual one does not introduce radical new router features or dramatically drop costs. Many enterprises expect virtualization to mean major direct-cost savings, which is unrealistic.

There are also some NFV quirks that can give enterprises pause. Some service providers offering NFV services have bridged physical and virtual network views successfully. But others still have separate management interfaces. That means an enterprise that would prefer to migrate gradually may end up swapping between many different management interfaces, for example physical router, virtual router, physical firewall, and virtual firewall views. Another potential issue is that most managed CPE hardware from managed NFV services remains closed and expensive, with a few recurring suppliers (e.g., Juniper, Cisco, ADVA). Verizon has already opened its NFV services to support inexpensive white-box CPE; other providers have third-party CPE vendors on their roadmaps.

More minor issues of gauging NFV CPE software performance and platform stability/reliability can be shown through testing. But an intractable problem is enterprises that have three, four, or more functions at each location, and initially only one or two of them are supported by the NFV platform. It is particularly problematic if the enterprise has a router and firewall that can be virtualized at either end but an unsupported probe between them: the platform cannot support a virtual-physical-virtual service chain. A "bring your own VNF" capability could add a lot of value for enterprises; service providers are keen to release such a capability but also are extremely cautious. There are many complications to accepting enterprise-supplied software into the carrier's NFV ecosystem.

On a positive note, the community around NFV orchestration continues to mature. Red Hat and VMware have growing partner ecosystems for their respective NFV stacks. Systems integrators such as Netcracker and Amdocs continue to evolve prefabricated NFV environments with their partners to

make it faster and cheaper for providers to offer commercial NFV services. Juniper (with Contrail and Tungsten Fabric) and Cisco (with ACI) bridge the gap to managed CPE.

For service providers that do not plan to add commercial NFV enterprise services, SD-WAN platforms that bundle third-party VNFs remain a possibility. Nokia Nuage Networks, VMware VeloCloud, and Versa Networks support third-party VNFs, mainly from common security vendors such as Palo Alto Networks, Fortinet, and Check Point. BT has deployed this capability from Nokia as one of its platform options. Ovum has not yet had discussions with enterprises using SD-WAN bundled with third-party VNFs.

What to look for in 2019

Virtual network functions recreate physical appliances in software, with almost all the same features and functionality. That means enterprises have not had an urgent reason to swap CPE. In 2019, the biggest service providers – those most heavily invested in premises-based NFV services – will iron out more gaps in orchestration and service chaining. They will also need to handle adding NFV-based platforms and services smoothly into brownfield environments. More providers will converge management of physical appliances and virtual functions, at least for key brand-name vendors. When enterprises can combine elements of both under a single pane of glass, it should make CPE-based NFV services more accessible to them. The second half of 2019 should bring the first attempts at "bring your own VNF" options. This will start to address another roadblock to enterprise adoption of premises-based NFV services. SD-WAN and NFV should each be a driver for the other. Providers do not need to have unified services today, but they do need a services-convergence roadmap.

Meanwhile, enterprises increasingly rely on NFV whether they realize it or not. Major providers have capped physical network gateways and have shifted new growth to software-based VNFs inside the network. Centralized firewall services similarly can cap proprietary multitenant hardware and shift to software in an open NFV environment. There is no detectable change in services, except maybe for faster responsiveness and accelerated rollout of new features.

The barrier to entry for a network provider to deploy a commercial enterprise NFV services platform continues to drop in 2019. Systems are more mature and there are more prefabricated components, meaning shorter development times and lower overall cost. But an operator's cost to add commercial NFV services to its portfolio still depends on what level of integration the provider wants for "minimum viable product." Ovum expects in 2019 many enterprises will stay on the sidelines with regard to premises-based NFV services as maturation continues.

New convergence vision links hybrid WAN, SDx, NFV, and cloud management

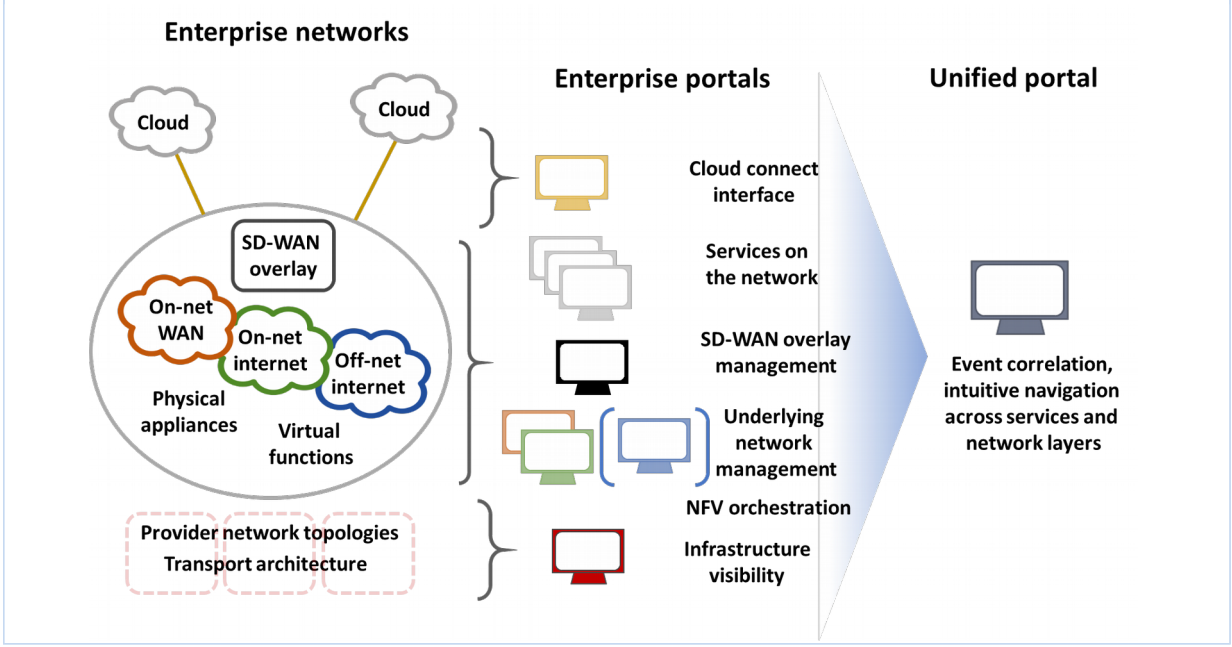
The telco portal-management singularity

Software-defined services, virtualization, hybrid networking, and the cloud together mean a sea change in the way enterprises approach their networks. Old-school enterprise WANs are on-net, end-to-end, static private networks. Supporting enterprise CPE has multiyear lifetimes. Because it is all on-net and predictable, the enterprise has excellent visibility into all performance aspects of this old-school WAN.

SD-WAN and hybrid networking fragment the network into a separate overlay and underlay, mixing on-net and off-net routes where traffic patterns shift constantly. NFV lets the enterprise add or swap functions in CPE at any time; dynamic bandwidth to the cloud and other endpoints let enterprises assign bandwidth and class of service where and when they need it. Each new dynamic service option might seem good for administrators, but put them together, and each tool may report differently, and a change to one element potentially affects the others. How does the enterprise keep its network management house in order? The enterprise needs consistent reporting views, intuitive navigation that spans its services, and intelligence that can pinpoint the source of a problem and recommend best actions for resolution. Instead, there are many "panes of glass" to manage it all.

Network providers are well suited to build this unified portal concept that normalizes views, supports seamless navigation, and integrates controls across the layers – applications, services, networks, and infrastructure. But building a fully integrated digital customer portal experience will not be easy. Figure 3 shows the possible service components an enterprise may have. While a single "grand unified portal" that unites all services intelligently is still theory, operators have started to pull together key pieces, to make networks that have been fragmenting more manageable. Singtel is an example that is interlocking service components for its Liquid Infrastructure platform, unveiled October 2018. Many major operators have shown aspects of tying together functions in their enterprise portals: SD-WAN with WAN (e.g., Comcast Business, Masergy); physical appliances with virtual functions (e.g., Orange Business Services); on-net internet performance guarantees extended through off-net partners (e.g., CenturyLink, Tata Communications); and visibility into real-time performance across enterprises' off-net internet links (e.g., network providers collaborating with Akamai and others).

Figure 3: Hybrid networking, SD-WAN, cloud connectivity, and NFV



Source: Ovum

Cloud connectivity and cloud-centric network services

Network providers can pull together many different operating pieces to make it easier for enterprises to manage the mix of new network components. But there are providers that leverage a cloud-centric

approach for their network services. Aryaka is vocal in this space; others include Teridion, Netrolix, the Virtela business of NTT Com, and to an extent Akamai, Megaport, PCCW's Console Connect, and PacketFabric. Whether or not they use conventional network platforms, these operators draw heavily on cloud economics for their services. There is some overlap between business models, but in general Megaport, PCCW, and PacketFabric emphasize their ability to connect between data centers and clouds; Teridion and Aryaka optimize global network traffic through their cloud-based infrastructure; and Netrolix and Virtela (and again Aryaka) use their cloud-based infrastructure to push an array of managed network services out to enterprise locations.

While there are plenty of specialist network providers, data-center and cloud-services companies have not stayed on the sidelines. AWS, Microsoft Azure, Google Cloud, and others offer global network transfer between cloud locations. Equinix and Interxion offer network connectivity between their cloud exchanges. It seems a matter of time until big cloud and data-center players – experts in virtualization – add orchestrated NFV offerings for businesses. Some are publicly implementing NFV orchestration platforms: Microsoft Azure and Equinix participate in Linux Foundation's ONAP, and AWS works with open source MANO. Cloud players' NFV efforts can complement service providers, for example by hosting NFV infrastructure. They may also compete against them by offering businesses similar hosted-NFV deals. Big cloud players will not actively source enterprise network services, or resell or control them. But to the extent that SDN and NFV are automated and orchestrated, enterprises could order and spin up SDN-controlled capacity from the cloud and point their own procured NFV hardware at the cloud provider for a centralized interface.

Cloud-services providers are nowhere near the point of running comprehensive enterprise-wide network management. But given their knack for rapid development, Major data-center and cloud providers could launch basic, centralized hosted NFV offers within the next year.

What to look for in 2019

For service providers, making enterprise portals easier to navigate, more intelligent so they can extract useful analytics, and more capable of calling out and resolving issues is a constant process. In 2019, much of their attention will be on simplifying SD-WAN management and on linking information from SD-WAN overlays with network underlays.

Service providers will focus on the converged features that are most practical for their managed services. Comcast Business, for example, aims to create intuitive click-through between SD-WAN and underlying network resources. CenturyLink, for example, is hooking multicloud policy management into its dynamic bandwidth services controls. There are many, many more examples from major providers worldwide pulling together platforms and features to provide enterprises with ease of use.

Through 2019 enterprises should look forward to intelligent features, better navigation, improved service navigation, growing lists of portal API calls, and closed gaps in management functionality for network services. The umbrella of functionality also extends to managed security services that hew close to the network. This way, network providers will strengthen the case for enterprises to use their co-managed or fully managed services rather than have enterprises turn to equipment vendors to build self-managed platforms.

Appendix

Methodology

This Trends to Watch document is based on primary and secondary research with network and cloud-services providers, enterprises, and platform vendors. This research is bolstered by information from regular briefings and discussions with industry vendors and service providers. The document also draws from prior Ovum reports covering networking and cloud services.

Further reading

2018 Trends to Watch: Network Services , TE0005-001004 (October 2017)

Operator Perspectives 2025: The Future of Enterprise Network Services, ENS004-000036 (September 2018)

Bandwidth Central: Global Enterprises Shift Their Networks around Data Centers, ENS004-000029 (May 2018)

Author

Brian Washburn, Practice Leader, Network Transformation and Cloud

brian.washburn@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo