The Cloud on the Networking Horizon

Cloud networking is on the near horizon for IT pros. Make your network “future proof” by learning about networking as a service, hybrid cloud networking and other soon-to-be-everyday tech.
Coping with the Coming ‘Good Old Days’

**There’s no denying it:** Change can be scary. And when faced with the intricacies of today’s networking challenges, it’s tempting to long for the good old days—when life was simpler, people were happier and packets followed a straightforward path from a source to a destination.

But the reality about nostalgia is that the good old days never existed, or at least not as we remember them. Life was always as messy, and when networking technologies like frame relay and ATM first emerged, many engineers struggled with their complexity.

Cloud networking—that is, routing traffic within and between cloud computing environments—is the latest challenge for enterprise network engineers. But unlike ATM and frame relay, it’s not going away anytime soon. As the network becomes increasingly virtualized and enterprises continue expanding the use of cloud services, the need to understand cloud networking is going to grow.

Whether trying to define network architecture in a private cloud or build interconnections in a hybrid cloud, networking pros are finding the distributed nature of cloud services demands an entirely new approach. It requires new ways of thinking about Layer 2 and Layer 3 networking, as well as the relationship between networks and dynamic resources in the data center.

If this sounds daunting, then this Tech Guide is for you. We break down the concept of network as a service (NaaS) and its use in public, private and hybrid clouds. Included, too, is an in-depth look at what goes into hybrid cloud networking, and how the characteristics of cloud applications affect deployment.

Just remember: It won’t be long before these feel like the good old days of networking.

**Jessica Scarpati**

*Features and E-zine Editor, Network Evolution*
Network as a Service: The Core of Cloud Networking

One of the complexities of “the cloud” is the fact that the cloud model has so many variations—public, private, hybrid—and many implementation options driven by multiple cloud providers and cloud software vendors. One common element in all clouds is cloud networking, which is always essential in connecting cloud resources to users, and increasingly for making connections among cloud resources and providers. Any enterprise that’s building a cloud strategy has to build a cloud networking strategy, and that strategy has to be versatile enough to accommodate rather than limit cloud choices.

Where to Start
A good place to start is with the notion of network as a service, or NaaS. Public cloud services include NaaS features implicitly (the Internet is an “access NaaS” for most public clouds) or explicitly (with VPN capabilities), and private and hybrid clouds will almost always control network connections using a NaaS model.

NaaS, for a cloud network builder, is an abstract model of a network service that can be at either Layer 2 (Ethernet, VLAN) or Layer 3 (IP, VPN) in the OSI model. A cloud user defines the kind of NaaS that their cloud connection requires, and then uses public or private tools to build that NaaS. NaaS can define how users access cloud components, and also how the components themselves are connected in a private or hybrid cloud.

The best-known example of NaaS in the public cloud space is Amazon’s Elastic IP address service. This service lets any cloud host in EC2, wherever it is located, be represented by a constant IP address. The Elastic IP NaaS makes the cloud look like a single host. This is an example of an access-oriented NaaS application.
In the private cloud, the most common example of NaaS comes from OpenStack’s Neutron APIs, which let users build models of network services at Level 2 or Level 3 and then add their virtual machine (VM) instances to these models. This NaaS model builds inter-component connections that connect cloud application elements with each other, and also defines internetwork gateways to publish application services to users. Not all private cloud stacks have NaaS or Neutron-like capabilities, though, and where they don’t exist it will be necessary to use management/orchestration tools, popularly called DevOps tools, in the cloud to build NaaS services in a private cloud deployment.

**NAAS FOR HYBRIDS**

For hybrid clouds—the direction most cloud users expect to be going with their own cloud plans—NaaS is likely to be a three-step process. First, you’ll need to define the “public cloud” NaaS service, then the cloud networking you’ll need for your private cloud, and finally the bridge between them. In most cases, this “hybrid bridge” is a gateway between the two NaaS services in your cloud, but it’s often a gateway that operates on two levels. First, it has to provide an actual network connection between the public and private cloud, which in many cases will mean setting up a router device or software-based router. Second, it has to ensure that the directories that provide addressing for cloud application components (DHCP to assign addresses, DNS to decode URLs to addresses) are updated when components are deployed or moved. This is actually a part of cloud integration, and it may be done using DevOps tools or commercial products for cloud integration.

Cloud networking is critical for the cloud’s success, and approaching it as the union of NaaS domains is a good way to plan and implement the necessary elements and keep them running optimally for efficient cloud use.

—Tom Nolle
Hybrid Cloud Networking Is Coming Fast

When it comes to the hybrid cloud, enterprises live in a world of parallel play, where some applications live in the public cloud while others reside safely in the on-premises cloud. Yet the two are rarely interconnected.

This scenario falls far short of the promise of a hybrid cloud where VMs could be provisioned, migrated and managed as one across multiple sets of data center resources. And, in large part, it’s the network that stands in the way.

“You can create dynamic network infrastructures within [a hosted cloud] environment, and you can create dynamic internal network infrastructures, but they have to stay within those environments,” said Eric Hanselman, chief analyst at 451 Research. Binding a dynamic network in the hosted cloud to the on-premises data center becomes complicated.

The problem starts with plain old physics—or the speed of light. Once you break up tiered applications and place the different elements far away from each other in dispersed data centers, latency becomes an issue. Requesting more fiber in the ground for capacity is not only costly, but also takes too long in a world of dynamic provisioning.

In addition, companies struggle to stretch network services, like firewalling and load balancing, across disparate sets of resources. Then there’s the issue of managing two separate sets of IP ranges that would have to be combined to enable automated VM provisioning and migration across clouds.

Yet with so many more cloud providers offering hosted virtual private clouds, and enterprises realizing they needed distributed computing, both are seeking answers. These solutions will likely emerge in a combination of software-defined networking (SDN), network virtualization and expanded orchestration tools.
HYBRID CLOUD NETWORKING: CONNECTIVITY IS IMMATURE

Network connectivity for hybrid cloud infrastructure is still immature and can be expensive.

Most enterprises connect into the hosted cloud over Layer 3 using either an IP VPN or MPLS connection, but both require heavy lifting and can be costly.

“A lot of cloud providers have various VPN technologies, but you need someone to help set that up,” said Bob Plankers, a virtualization and cloud architect at the University of Wisconsin at Madison.

Providers typically charge an enterprise to establish and maintain the connection, and the enterprise will need engineering resources to maintain its own end of the tunnel.

Additionally, VPN-based hybrid cloud networks can also become a bottleneck on a global WAN.

“If they are public-facing Web systems, a VPN may not be too much of a drawback because [users] are accessing them through the public cloud,” said Jason Edelman, a senior solutions architect at Presidio.

But for internal enterprise applications, the VPN can become complex. “If you have four or five sites in an enterprise that have access to a system in the public cloud, and that public cloud is building a VPN tunnel to a corporate head-end VPN concentrator, then all four of your other sites have to go through corporate and then through the Internet to the VPN tunnel. So you lose that any-to-any [architecture],” Edelman added.

An enterprise could avoid the bottlenecks by establishing a full mesh VPN network with the cloud provider, but that arrangement will add complexity to the network, and the enterprise will be paying for multiple VPN connections with its cloud provider, he said.

Some enterprises with deep pockets can bypass VPNs and try direct Layer 3 peering to

Enterprises live in a world of parallel play, where some apps live in the public cloud and others reside safely in the on-premises cloud.
a provider. “I was talking to a large customer last week who was doing a one-off scenario for [high performance computing],” Edelman said. “They’re going to peer directly to a cloud provider leveraging BGP.”

THE FIRST STEP TO INTEGRATION: EXTENDING SERVICES ACROSS HYBRID CLOUD NETWORKS

Z Gallerie, a Los Angeles-based furniture retail chain, maintains a typical example of what’s possible with hybrid cloud networking today. It maintains its customer-facing website in a Virtual Private Cloud (VPC) on Amazon Web Services while maintaining its enterprise systems in both a traditional private data center, as well as a hosted private cloud.

Z Gallerie wanted to integrate its Amazon VPC into its corporate network to connect its enterprise resource planning (ERP) and point-of-sale systems with its website.

“We needed one single, unified network so we could work seamlessly [between those systems],” said Howard Kolodny, vice president of IT at Z Gallerie. “We wanted to integrate our firewall and VPN concentrator between our public and private clouds to provide a pathway to move data between systems securely and easily.”

Z Gallerie, however, is a Cisco shop and Amazon does not support Cisco firewalls and routers natively. Kolodny turned to virtual routing and VPN technology from Vyatta, a company recently acquired by Brocade. The Vyatta technology, which is billed as an alternative to a Cisco ASR 1000, is supported natively by Amazon and was able to establish the necessary VPN tunnel with Kolodny’s Cisco infrastructure.

With Vyatta’s technology, Kolodny was able to get the VPN between his private and public cloud resources up and running. Now “it just runs,” he said.

Cisco is launching a software-based Cloud Services Router (CSR) 1000v that will eventually work in Amazon and Microsoft’s Azure cloud. But Z Gallerie’s experience with unsupported firewalls points directly to the challenges enterprises face with hybrid cloud networking. Establishing network connections between public and private clouds, and maintaining consistent network policies and Layer 4...
through 7 services in both environments, isn’t easy when cloud providers don’t always support an enterprise’s vendor of choice.

Establishing network connections between public and private clouds isn’t easy when cloud providers don’t always support an enterprise’s vendor of choice.

“We’re just starting to see tools come out that can help manage both sides of things simultaneously,” said Plankers of the University of Wisconsin. “Extending security controls and networking [from private to public cloud] is a big problem. It depends on the cloud provider and what technologies they might have installed to enable people. It’s a pretty immature space right now.”

Cloud provider Tier3 is one of these companies. Its enterprise customers can create MPLS VPN connections into the hosted cloud from their own enterprise clouds and then establish an isolated VLAN to route traffic back and forth that is protected by their own firewalls and policy. Through a simple user interface, they can apply these policies to VMs and resources inside the hosted cloud.

“They can actually extend core services for identity management,” said Jared Wray, Tier3 CTO. Through Tier3’s interface, customers have visibility of resources in both public and private clouds, which helps them apply policy.

—Shamus McGillicuddy and Rivka Gewirtz Little
Stretching Layer 2 Across Hybrid Cloud Networks

**Integrating Network Services** is one thing, but if the true promise of the hybrid cloud is to enable provisioning and migration of VMs across clouds using a single orchestration system, it will take an extended Layer 2. A shared Layer 2 network will mean that both sets of cloud resources could be managed as a single IP range. The problem is, the technology to do this doesn’t quite exist yet.

But NTT Communications, a global IP network provider that delivers a fully dynamic software-defined network inside its virtual private clouds, sees the technology very close on the horizon.

In NTT’s virtual private cloud, software-defined networking (SDN) and OpenFlow give users an interface to provision network segmentation on demand. The NTT cloud has VMware hypervisors that are controlled by VMware’s vCloud Director. But NTT also runs NEC’s OpenFlow switches and controllers to enable dynamic network provisioning.

“Through the customer portal, an engineer would define different network segments and create the virtual machines, deciding which network segments to place them on,” said Len Padilla, senior director of technology at NTT. “Then they would connect them directly to firewalls and load balancers.”

NTT’s homegrown orchestration system ties all of these resources together and then feeds connectivity into Cisco Catalyst 6500 series switches that sit on the edges of the virtual data center and connect out to the enterprise’s VPN. Everything in the network can be automated all the way until it reaches the outside connection.

“The next step is to let those [outside] connections be manipulated,” said Padilla. “We are looking at giving customers one pipe that connects them to the NTT network, but within that, being able to establish virtual network
segments. Then they can come in through the portal and configure an IPsec tunnel.”

Once NTT’s network is extended into the enterprise data center, NTT will enable users to establish overlay networks, which will allow them to use a single IP addressing scheme for the VMs in both data centers, he said.

Currently, NTT’s orchestration system makes sure that “everything is going out on the right VLAN” once it hits the Cisco switches at the edge. The company has even been able to customize individual use cases where this process is automated, but “the next step is getting that to happen in a standardized way,” Padilla explained.

“As these edge and core and backbone switches become SDN aware, ... we will strip away pieces of the control software we have built and replace it.”

—LEN PADILLA, NTT

with OpenFlow or not—we will strip away pieces of the control software we have built and replace it,” he said.

Cisco’s new Nexus 1000v Intercloud software enables Layer 2 overlays between public and private cloud infrastructure. Nicira, the SDN and network virtualization startup acquired by VMware, appears to be working on a similar solution, Edelman noted. Many engineers also believe that tunneling protocols like VXLAN could extend Layer 2 domains into the public cloud if the protocol’s requirements for multicast networks are eliminated in future iterations.

IN HYBRID CLOUD NETWORKING, GETTING SMARTER ABOUT APPLICATION PLACEMENT

In early hybrid cloud scenarios, many enterprises looked to divide tiered applications between public and private clouds. The goal was to host the tiers that required rapid scaling in the cloud, while placing static, core components like database servers in the enterprise data center.

“When people say the word ‘workload’, they usually are thinking about a single virtual
machine,” said Dante Malagrino, CEO and co-founder of Embrane, a developer of SDN services appliances. “In reality, customers’ IT organizations think in terms of applications ... a combination of multiple virtual machines interconnected by network segments and secured by firewalls and accelerated by load balancers.” Splitting those segments across public and private clouds can cause countless problems, including the inability to extend firewall and load-balancing policy across disparate IP schemes.

So some enterprises are approaching the hybrid cloud differently. Rather than splitting application tiers across public and private infrastructure, they choose to migrate an entire application to the cloud, leaving only small but necessary hooks to the applications within the private cloud, such as authentication and authorization systems.

“If you have 10,000 applications, it’s more interesting to think about migrating 100 applications into the cloud because you want to free resources for more mission-critical applications in your data center, versus splitting your applications in half,” said Marco De Benedetto, CTO and co-founder of Embrane.

In those cases, De Benedetto said the enterprise can free up internal resources for the critical applications that have much stricter service level agreements (SLAs).

**APPLICATION REPLICAION IN THE HYBRID CLOUD**

Other enterprises choose to place application replications in the hosted cloud to tackle the problem of distance and latency, or simply to provide redundancy.

“You could have one instance of an application that runs in your own data center and one that runs in [a hosted environment],” said Hanselman. “Then you don’t have to build a second data center. This buys you a separate

Some enterprises choose to place app replications in the hosted cloud to tackle the problem of distance and latency, or to provide redundancy.
location where you have the same operational capability.”

It is important to ensure that the data source is consistent in different environments, and that can be a challenge, said George Reese, CTO at enStratus, a provider of cloud infrastructure management tools. In some cases, even if the data can’t be as equally consistent, enterprises take the chance to avoid latency.

Using an orchestration system that provides visibility into available resources in private and hosted clouds allows enterprises to account for geography, available capacity and even the need for failover when doing VM provisioning.

“We get visibility into what exists, and we use our own automation logic to construct network pathways to talk to virtual machines and monitor them. If we detect failure in one part, we can bring up resources [somewhere else] so we can move data around,” said Reese.

Nevertheless, Reese has high hopes for deeper levels of hybrid cloud integration that won’t involve taking such risks.

—Shamus McGillicuddy and Rivka Gewirtz Little
**TOM NOLLE** is president of CIMI Corporation, a strategic consulting firm specializing in telecommunications and data communications since 1982.

**RIVKA GEWIRTZ LITTLE** is the executive editor for TechTarget’s Networking Media Group and has covered telecommunications and networking since deregulation of the FCC in 1996.

**SHAMUS MCGILLCUDDY** is the director of news and features for TechTarget Networking Media Group. He writes about networking, security, data centers, network management and other topics for SearchNetworking.com and manages overall news coverage for TechTarget’s other networking sites, including SearchUnifiedCommunications.com, SearchEnterpriseWAN.com and SearchCloudProvider.com.