The third network will be made possible by exploiting wide area networks, software defined networking and network functions virtualisation
Kevin Vachon,
Chief Operating Officer, MEF

SECURITY MAY BE KEY TO 'THE THIRD NETWORK'

The Metro Ethernet Forum's vision of a 'Third Network' promises unlimited profits for global business. But they'll have to pay. **Bill Boyle** reports from the debate at the NetEvents forum

In September this year at the NetEvents forum the Metro Ethernet Forum (MEF) announced its vision for The Third Network. This concept is based on the idea that business is already served by two types of data networks, Carrier Ethernet 2.0. and Internet/IP Network but needs an improved one. The (MEF), founded in 2001, is an industry consortium dedicated to adoption of Carrier Ethernet networks and services and it is generating some debate.

The MEF is composed of service providers, local exchange carriers, network equipment vendors, and other networking companies that share an interest in Metro Ethernet. It has approximately 160 members.

The aim of The Third Network is to match the ubiquity and immediacy of Internet connection with a level of service as good as the best Carrier Ethernet service, but available anywhere, on demand. In fact this amounts to Network as a Service that would allow any user to specify their needs in terms of bandwidth, latency, levels of protection etc, and to expect to log on anywhere and be sure of identical service levels – no matter who provides the access or how many intervening networks are needed to deliver the service.

THE VISION

How close are we to realizing this vision? There is obviously a long way to go before the Third Network is fully established, if it ever is, so the next question is where are we now and, from a business perspective, what would be the priorities for the mobile business user?

Simple connection is the obvious first priority. However poor the service, there is a world of difference between some connectivity and none. With the launch of CE 2.0, MEF has already making progress in simplifying and accelerating basic connectivity and access across multiple networks.

Martin Hingley, CEO of ITCandor, is intrigued by the MEF's offerings: "The way that the MEF seems to be approaching their solution is interesting – they are looking at the horizontal layer as opposed to asking companies to keep investing in something they already have to make a difference. I suppose the obvious example is software defined networking (SDN) where vendors are saying 'we can help you pool your existing storage and make it better' rather than the MEF approach which is saying, 'Let us make the investment and you can choose to buy it.'"

SECURITY IS THE KEY

For serious business use, however, security and privacy must generally become the second highest priority. TRUSTe's late 2013 report suggested that privacy is a growing concern for almost two thirds of Internet users, and mobile workers are especially at risk from malware. When providing connectivity as a service for different types of customers, the sort of data and network security taken for granted in a private, static network becomes a critical issue. So security will be a key indicator of a high quality network service as promised by the Third Network.

It is one thing to establish security across a single provider network, but to maintain consistent security as the signal passes into and across different networks is a major challenge. The power of carrier ethernet has been its flexibility to carry any required service, and this is possible because there are so many variables that can be set. But this is also why it has been so difficult to align services, and why e-Access has become so important in establishing a basic global standard for faster connection to access networks.

The most promising solution to this orchestration challenge has been proposed by Wedge Networks. It is to adopt the SDN principle and consider the traffic flow as a virtual network, rather than a string of hardware elements, and so define a distinct "security layer" to orchestrate Security as a Service.

The analogy with the Wedge approach is this: rather than trying to address security at that bottom level, you can virtualize the data flow to a level where it can be better managed as a service. There is a double advantage to this approach: as well as being able to orchestrate a personalized service across multiple network segments, it also enables ▶

Nan Chen, president MEF, vice-chair CENX. Robert M. Metcalf, advisory director MEF

very high levels of security and protection by creating the equivalent of an organism's immune system – with built-in automated security functions for all traffic flows.

IS YOUR WATER SAFE?

Today's Internet connection has been compared to a water supply without any guarantee of purity. If the tap water might be contaminated, it is the customer who has responsibility for filtering and sterilizing the water. This is how it is with today's Internet: users are expected to install their own anti-virus software, firewalls and other forms of security. Security as a Service (SaS), however would mean providing traffic that is already decontaminated. In fact the user, rather than "risk" vital documents to the Internet, might positively opt to send them into the Internet to ensure that they will be free of malware.

And what about machine to machine communications? The typical Internet of Things scenario does not include built in defence abilities, and we are already being warned of smart fridges being used to spread malware – who would want their business bankrupted by a malfunctioning kitchen appliance?

Although this security layer seems a radical approach to providing Security as a Service, it is already tried and tested in thousands of instances worldwide. Enterprises, small businesses and service providers have already adopted Wedge's high performance deep packet inspection security layer approach to ensure consistent, clean networking.

The greatest challenge now must be to extend this level of protection by orchestrating it across multiple providers' networks, and Wedge has just recently signed up as a member of the MEF in order to add its experience and expertise to the Third Network project.

According to MEF president, Nan Chen, the third network could provide people travelling on business access to their corporate network with guaranteed bandwidth, security and quality no matter where they were – for a fee. He said at NetEvents : "Wouldn't it be great if there was a button on your laptop called the 'third network' that, when you press it, automatically makes a private call from your laptop with a guaranteed quality of service? I'd certainly be willing to pay for that." And there's the rub – many people see this as the erosion of net neutrality. Speaking to The Sydney Morning Herald in the aftermath of the NetEvents announcement analyst Paul Brooks, principal of Layer10 Consulting said that the concept had been tried but had proved unsuccessful. "This sort of thing was first proposed back in the early 1990s," he said.

"It requires a protocol that goes end-to-end along the path to reserve the resources in the routers and switches. That protocol exists. It's called RSVP - resource reservation protocol. It was defined in September 1993. The architecture was originally called integrated services, IntServ, in the Internet Engineering Task Force."

NET NEUTRALITY

Mr Brooks did not see the need for the third network. "By and large virtual private networks over the internet work very well for what most people want to use them for today. You don't need guaranteed bandwidth, you don't need guaranteed limits on packet loss, latency and jitter to access corporate applications."

MEF believes that the Third Network will be made possible by exploiting wide area networks, software defined networking (SDN) and network functions virtualisation (NFV). SDN allows the switches and routers that direct traffic through data networks be instructed and controlled by software via standard interfaces.

NFV enables the combination of hardware and software traditionally needed to deliver a service over a network to be replaced by software running in a virtualised environment on standard hardware.

The development of both of these technologies is being talked up by telcos that see great potential for cutting costs and creating new services. Meanwhile the question of net neutrality is still being hotly debated. ■