Pipeline
Your OSS/BSS Information Source.
www.pipelinepub.com Volume 7, Issue 4

Stepping Towards the Edge

By Tim Young Editor-In-Chief

Ask anyone who suffers from severe acrophobia: The edge is a complicated place.

The ledge of a building. The rim of a cliff. The outermost edge of a tower. These are beautiful and potentially terrifying locations, whether literal or metaphorical.

The edge of reason. The edge of darkness. The edge of the world.

And the word carries a wealth of other dangerous associations. A razor's edge, sharp and dangerous, gleaming with purpose and malice, all at once. On one hand, without the blade, where would our society be? Ragged and wanting for homes and fields and pathways forged through underbrush. And yet, a blade can cut deep. It is its usefulness that makes it dangerous, and its danger that makes it useful.

"The security on the edge has become more complex as an increasing number of network users refuse to stay put."

Within the communications context, the network edge maintains a balance between vast potential and substantial risk and danger.

Ginsberg and Hattar's Implementing IP Services at the Network Edge, defines the network edge as the area in which "the network joins various access technologies such as DSL, cable, and wireless connections with the high-speed routed and optical core," which is a definition as apt as any.

It's a pivotal region for several reasons. First of all, it's a particularly vulnerable area for security systems. The handoff between the core and the periphery is tricky under the most ideal circumstances. Furthermore, QoS can be an issue as well, as the edge is more difficult to monitor than the central network. Let's look a bit more at these issues.

Security

When I speak to industry leaders about the network edge, the concept of security comes up often. Simply put, the security on the edge has become more complex as an increasing number of network users refuse to stay put. Mobile devices (which pose a variety of other issues we'll address in a bit) and guest users pose security concerns for network operators and enterprise customers alike.

The complexity and sophistication of edge switches has improved greatly, and VPN access is becoming more stable over time. Still, especially in the case of an internet edge, neither enterprises nor CSPs have a great deal of control over the types of packets that reach their edge. However, in determining what packets get through and which get denied, the network operator walks a fine line between allowing in a possible flood of problematic traffic and throwing out the proverbial baby with the bathwater. Stop too little and your network is overrun. Stop too much and your network becomes so unwieldy that its core value prop is undermined.

Technologies like distributed firewalls have been ready for primetime for a decade, but the edge is still overlooked by a number of hardware and software solutions. A well designed service management platform will integrate edge controls, and the better ones do. However, the level of agility required by the network edge dictates that there is still a great deal of

> **"The network edge is a problematic area for CSPs due to the sheer volume of devices occupying space on the edge."**

> **"It's essential that the network edge be given its proper level of consideration and care, as it's not becoming any simpler."**

growth that must take place.

As at least one other author in this issue notes, in order for OSS/BSS solutions to be able to aid in providing the level of security (and service quality) that is required for optimal network flow, that OSS/BSS provider must have the most intimate picture of the network available to them. It makes sense that this should already be occurring across every network, but that's not always the case. Until that level of access can be obtained, OSS/BSS providers will sometimes be forced to fight with one hand tied behind their backs.

QoS

The network edge is also an important frontier for making sure that quality of service is supplied at exactly the level to which a particular customer is entitled. Again, a proper OSS/BSS suite with proper network monitoring tools with proper visibility of the edge can do the trick, for the most part. Traffic prioritization is part of the key to high levels of QoS, and high QoS is integral for churn reduction and increased ARPU. Therefore, keeping an eye on the edge can keep your cashflow positive.

However, even more can happen on the edge. With the right tools in place on the network edge, a provider can easily throttle service in accordance with usage guidelines. This can be done quickly and effectively, and can help put the kibosh on activity that violates terms of use or creates a strain on the network that isn't in keeping with the agreement between provider and customer. In short, a cop on the street can be worth ten back at headquarters.

A QoS safeguard on the edge can help maintain top-shelf service for customers who've paid for the privilege to receive such service, and ensure that those who are less keen on paying their fair share are not given undue access to the network.

Devices

Furthermore, the network edge is a particularly problematic area for modern CSPs due to the sheer volume of devices occupying space on the edge. However, it isn't just the number that's an issue. The configuration of each of these devices is often handled in a completely off-site manner. As the use of complex devices like femtocells increases, operators must far-too-often resort to costly customer service time or, even worse, expensive truck-rolls every time an end user mistakenly alters a device setting or improperly resets a device.

However, new techniques in parameter management are starting to emerge to the point where many of these issues can be watched over from a central network ops center, and forays into customer homes are kept to a cost-saving minimum.

The Edge to Come

The increased challenges of the edge are far from being completely solved. In fact, for all of the discussion I hear from individuals heavily involved with network operations about the edge, the entire topic is given disgracefully little coverage in the wider communications space.

It's essential that the network edge be given its proper level of consideration and care, as it's not becoming any simpler. As network devices increase in number and complexity, and users demand more and more varied uses from their devices, the decentralization of network control will only further complicate issues. How we approach the network edge will tell us a great deal about how prepared we are, in the communications space, to approach the future.