Whose Fault is It?

Getting to problem resolution in multi-vendor environments

Contents

Introducing Mean Time to Innocence

Getting to the root of the problem in complex networking applications is almost always a challenge. Long gone are the homogenous voice networks where Class 4 and 5 switches handed off calls between service providers. Today, in the era of real-time VoIP traffic competing with traffic of all sizes and priorities traversing multiple vendor networks, the root cause of voice quality can be elusive.

Consider the following – a 25-person business to which you're providing Hosted Unified Communications and other managed services. This customer is paying about $1,000 per month – easily $40,000-$60,000 over the life of the customer relationship. In this high value customer relationship, you need issues to be solved quickly and decisively.

However, you're relying on a number of other providers – some of which you don't have a business relationship with – to provide this service. There's the ISP providing last mile data access (and across your customer base there will be many of these), your own network, and VoIP termination provider(s), to say nothing of the customer's LAN environment. Getting to the root cause – and in many cases this is a vendor – is critical in your efforts to deliver a high degree of customer satisfaction.

At Ribbon, we've coined a term that captures this phenomenon – Mean Time to Innocence, or MTTI. MTTI is the time required to identify the root of the problem and provide sufficient data to the offending party. Fundamentally, MTTI is getting to "it's not me, it's you – and here's why". Done quickly and with sufficient information, service providers can sort out problems, inform the offending party with specific data, and inform their customers as to issue resolution.

Whether you're an Over the Top (OTT) provider or a provider with end-to-end network assets, you'll need to confront MTTI. OTT deployments obviously have it harder as there are more variables and unknowns, but facility-based service providers (that provide their own circuits) have similar issues in problem resolution.

What is in the Mix?

The path to MTTI is difficult when there are many components in the customer/service provider relationships, including:

- **Service Provider Assets:** ISP connection (yours or someone else's), demarcation equipment, soft switches, application servers, Core SBC's, PSTN gateways.
- **Customer Side Assets:** Customer premises equipment such as routers and firewalls, existing legacy telecom equipment, IP and TDM endpoints, wireless access points.

The customer/service provider relationship is complicated enough. However, stepping into the middle of the ecosystem means finding a way to properly translate communications between all the different systems and having visibility to identify root causes quickly.

Many times, the lack of a clear MTTI leads to knee jerk hardware replacements. The "shotgun" repairs involve expediting and installing customer edge equipment, hoping that solves the issue. This can obviously get expensive quickly.

MTTI and the OTT deployment

When it comes to OTT, most service providers immediately think of the large, nationwide providers (8x8 and RingCentral come to mind) that exclusively deliver services over someone else's access circuit. However, likely all service providers have deployed OTT sites (or will in the future). If you have limited geographic reach and have a customer with multiple sites, invariably some of those sites will be beyond your reach. OTT will be your only option.

This is probably the most challenging case for MTTI. For instance, it's one thing to isolate the issue to the last mile connection (a faulty router, congestion, etc.) but really aids MTTI is the level of detail you can provide the offending party. Specificity is critical in this regard – just a generic "we think it's you" will not get the problem addressed rapidly, as the offending party will have to undertake their own research to solve the issue.

Facilities-Based Service Providers Are in the Same Boat

If you own and manage your own network, you are not immune to rapid problem resolution. In many cases, facilities-based providers (particularly the larger ones) have network operations centers (NOCs) that separate the service side from the network side. Because service-side employees aren't trained with the NOC's network management systems, they must submit service tickets in cases of customer complaints. Despite the perceived level of control a Tier 1 provide has, they deal with network performance issues the same way an end customer would—by calling support.

What is being deployed: Nothing is being put onsite

Service Provider Network

Customer Premises

Customer CPE

Pros: Inexpensive

Cons: Limited to no tools in place for service management or problem analysis
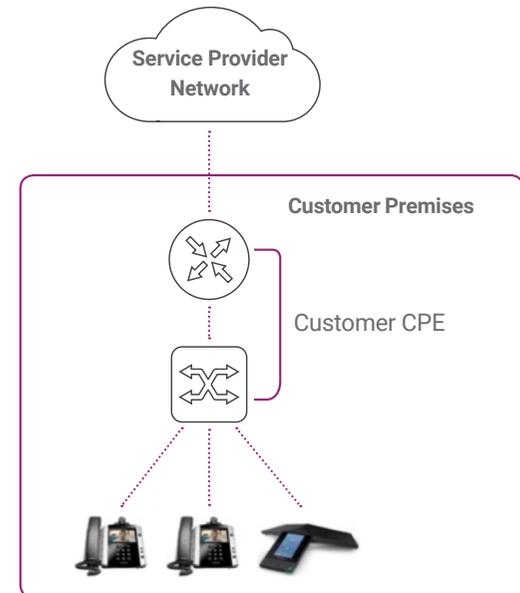
Control Over MTTI Depends on Deployment Methods

There are three deployment methodologies to keep in mind, each with their own advantages and disadvantages:

"Naked" Deployment
Consider the large OTT providers. The end customer already has a data network. The OTT service provider will set up the customer in their network and send IP phones to the customer site for self-install. Little consideration to service quality management is made. The OTT provider relies on a large, unconstrained data connection to deliver real-time communications. No customer edge hardware is provided.

Rip and Replace Deployment

The service provider replaces all customer LAN hardware (switches, routers) and provides a dedicated voice connection. In some cases the service provider will run dedicated CAT 5 wiring for each endpoint. As the deployment is brand new from phone to the core, rip and replace deployments are reliable and easy to troubleshoot.

What is being deployed: Everything is being put on site

Service Provider Network

Customer Premises

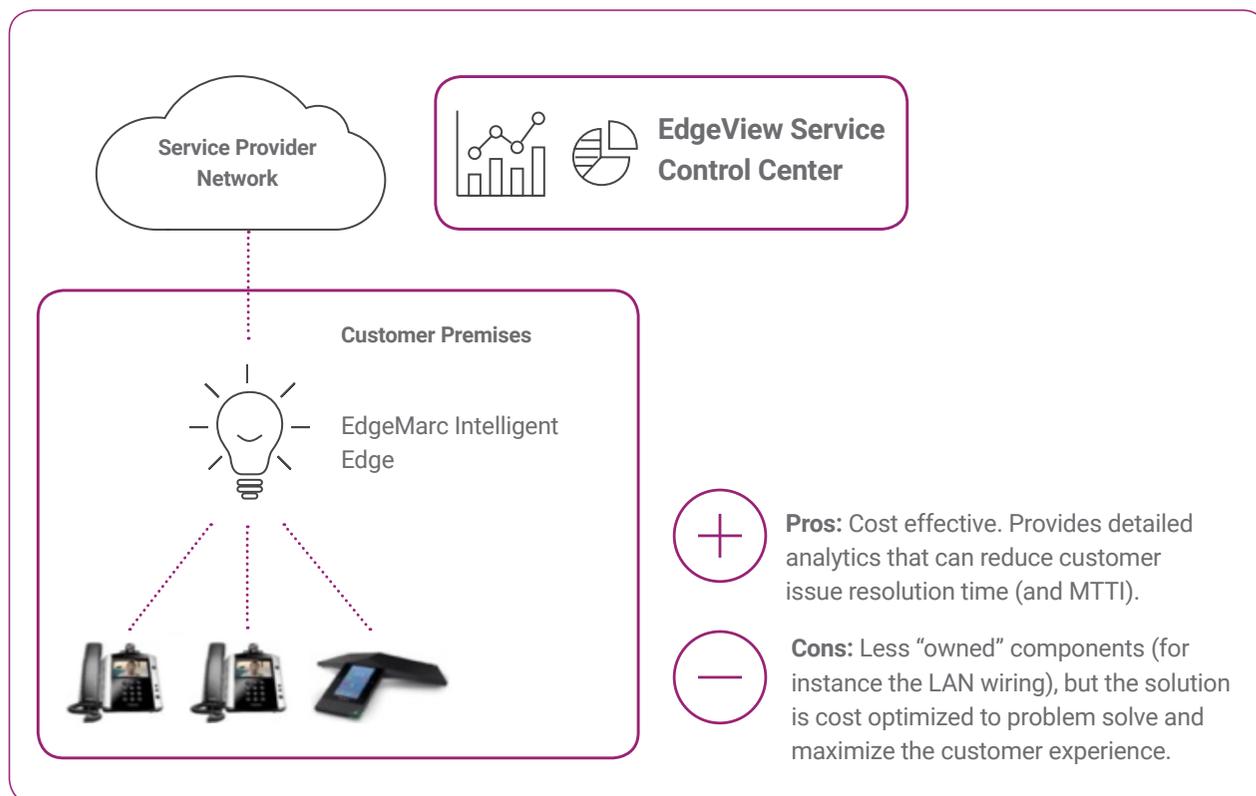Service Provider Supplied CPE
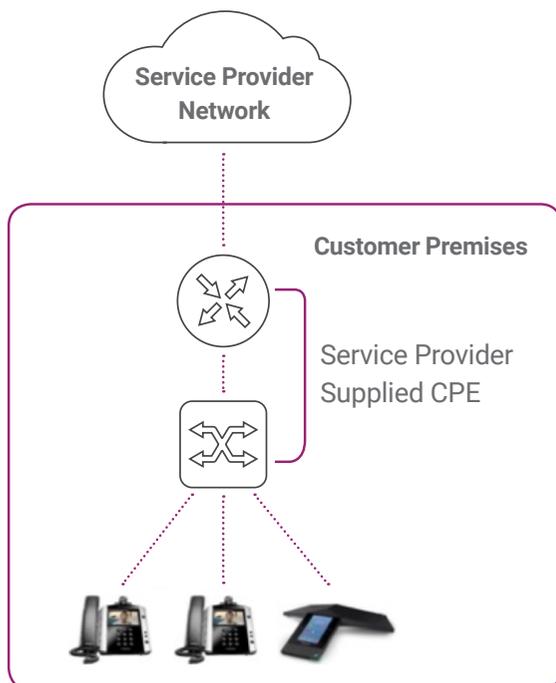
Pros: Highly reliable

Cons: Expensive. You will need significant revenue potential to make these deployments economically viable.

The Intelligent Edge

In this deployment model, [EdgeMarc Intelligent Edge devices](#) are placed at each customer site. In addition to SIP security and QoS management, the EdgeMarc provides detailed analytics on each session (call) traversing the network. This is reported into the cloud-based EdgeView Service Control Center for use by technicians for troubleshooting.

Generally speaking, an EdgeMarc is all that is required on the edge (other than phones). Existing customer switches and firewalls stay intact, and VLAN tagging is used so existing CAT 5 wiring can be used.

Service Provider Network

EdgeView Service Control Center

Customer Premises

EdgeMarc Intelligent Edge

+ Pros: Cost effective. Provides detailed analytics that can reduce customer issue resolution time (and MTTI).

− Cons: Less "owned" components (for instance the LAN wiring), but the solution is cost optimized to problem solve and maximize the customer experience.

The Benefits of Network Edge Orchestration for MTTI

Edgewater Networks Network Edge Orchestration provides the tools and intelligence required to minimize MTTI. The EdgeMarc Intelligent Edge collects real-time LAN-side and WAN-side metrics such as MOS scores, voice and video statistics (jitter, packet loss), and key resource utilization. The EdgeView Service Control Center then gives service providers an opportunity to view trends from all this real-time data.

While provisioning and element management are important functions of the EdgeView Service Control Center, these functions stand out as important getting to MTTI:

Monitoring and Alerting: Event-based triggers help service providers kick-off enhanced troubleshooting automatically. These can all be created within whatever parameters you select – for instance, 3 successive low MOS score calls kick off a packet capture and notifies the technical team that a problem exists.

Troubleshooting and Remediation: The Root Cause ID provided by EdgeView is a main benefit for MTTI. Service providers won't just diagnose problems, they'll pinpoint exactly where they exist. When the problem falls within the service provider's control, troubleshooting can be targeted effectively. However, even when the problem exists with another vendor or provider, service providers can offer detailed forensics that will help remediate the issue faster (regardless of who controls the components involved).

For instance, an event-based trigger can automatically set up a packet capture. This PCAP identifies the last mile provider's router as the root cause. Your NOC can quickly create a trouble ticket to the last mile provider, attaching the PCAP as evidence. This minimizes MTTI.

Even the most robust network will require troubleshooting. The key to maintaining the customer experience is to find the root cause quickly and resolve it. This is true even when your services aren't at fault. Customers care about having consistent, high-quality service and minimizing MTTI can help you make this a reality.

If you want to learn more about the Network Edge Orchestration approach from Edgewater Networks, contact us today for a free demo of the Cloud2Edge Complete solution.

About Ribbon Communications

Ribbon is a company with two decades of leadership in real-time communications. Built on world class technology and intellectual property, Ribbon delivers intelligent, secure, embedded real-time communications for today's world. The company transforms fixed, mobile and enterprise networks from legacy environments to secure IP and cloud-based architectures, enabling highly productive communications for consumers and businesses. With locations in 28 countries around the globe, Ribbon's innovative, market-leading portfolio empowers service providers and enterprises with rapid service creation in a fully virtualized environment. The company's Kandy Communications Platform as a Service (CPaaS) delivers a comprehensive set of advanced embedded communications capabilities that enables this transformation.

To learn more visit RibbonCommunications.com