White Paper

Innovation in Communications Services: Breaking With the Past Without Waiting for the Future

Prepared by

Patrick Donegan
Chief Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.nominum.com

April 2016

The Top-Line Growth Imperative for CSPs

In one sense, the business landscape for communications service providers (CSPs) hasn't changed at all in the last five years. As a global sector of the economy, the service provider community has found it consistently challenging to grow revenues and certainly to increase average revenue per user (ARPU).

A minority of service providers have certainly bucked the trend by successfully driving strong annual revenue growth; a minority have also suffered disproportionately, seeing significant revenue declines. Despite their best efforts, the majority have tended to see revenues approximately flat-line, rendering that the aggregate picture for the sector as a whole.

In terms of the business models and tools available to grow service provider revenues, however, the landscape has changed very significantly. There is now a strong industry-wide consensus that the traditional approach of investing in new proprietary hardware- based solutions for new service innovation is starting to become outdated. The capex and opex costs are recognized to be too high. Moreover, the time to market that this approach typically required isn't competitive in a market where more nimble Web-scale players such as Google and Facebook are able to spin up competing new services in days or hours.

Digital Transformation Is the New Means to an Old End – But When?

The last couple of years have seen an equally strong industry consensus emerge that digital transformation, modeled on what the Internet giants have done, and embracing cloudification of network functions through network functions virtualization (NFV) and software-defined networking (SDN), represents the new way forward. The vision that service providers are now aligned on is a single "cloudified" network architecture, including an NFV Infrastructure (NFVI) hardware and software platform. This is the new universal platform on which different revenue-generating applications or virtual network functions (VNFs) from multiple vendors can be introduced in software, hence very much faster, all supported by a next-generation management and orchestration (MANO) layer.

So, is it really a case of out with the old and in with the new when it comes to the approach to protecting and growing service provider revenues? Not quite. As the experience of some of the world's leading service providers is showing, "cloudification" and digital transformation are going to be a multi-year process – perhaps a little more multi-year than some originally assumed.

Consider the example of AT&T: So far, AT&T, a clear world leader in digital transformation, has executed on its strategy pretty much as planned. And, yet, at the end of 2015, the company had virtualized just 5 percent of its network functions as VNFs. According to AT&T's own cutting edge roadmap, the company won't get to 75 percent before 2020.

Having taken the initial steps of their digital transformation journey, some of AT&T's global peers have had to row back of late, however. Take Telefónica, for example: Earlier this year, Telefónica announced that while it had learned a lot from Phase I of its UNICA transformation roadmap, it is nevertheless having to change out its primary network integration partner for Phase II. Keeping on track to virtualize 30 percent of its network functions by the end of 2016 may now prove challenging as Telefónica strives to become an "On-Life Telco" by 2020.

A Third Way That Bridges Old & New Models

The above examples demonstrate that while cloudification and digital transformation are the right evolutionary path for service providers, these tools won't get them to the promised land of universal new service innovation any time soon.

And since that is true for AT&T and Telefónica, it is even more true of most service providers that lack anything like the resources of these huge global technology leaders. This is why service providers must be open to any cost-effective approaches to delivering new services and reducing customer churn, as well as continuing to leverage legacy dedicated hardware-based infrastructure models for new services and plotting a course for digital transformation.

Any such approach, which can be thought of as offering a third way in new service innovation, should deliver a better cost model and preferably faster time to market than legacy approaches. They should also be entirely aligned with the service provider's digital transformation roadmap without necessarily being implemented according to the end target architecture from day one.

A "Third Way" Transformation Path Using DNS

One possibility is for service providers to leverage their existing domain name server (DNS) infrastructure as a means of providing new services to their customers. The DNS is the gateway infrastructure that mediates between the end user and their service interactions with the World Wide Web. Most service providers are used to thinking of the DNS as a passive infrastructure that provides impartial look-up functions and connects users to the Web server resources of their choice.

But with the right additional investment, existing DNS server infrastructure can also be leveraged as an active intelligent network resource that is capable of delivering new services that deliver value to the end user, as well as revenue protection or revenue growth for the service provider. Because of its gateway function between the end user and the Internet, the DNS infrastructure can have excellent visibility into cyber threat intelligence, especially when that threat intelligence is pooled and shared across DNS server resources throughout the world. Used correctly, that threat intelligence can then be leveraged by service providers for network level filtering to protect the end user and materially improve their online experience.

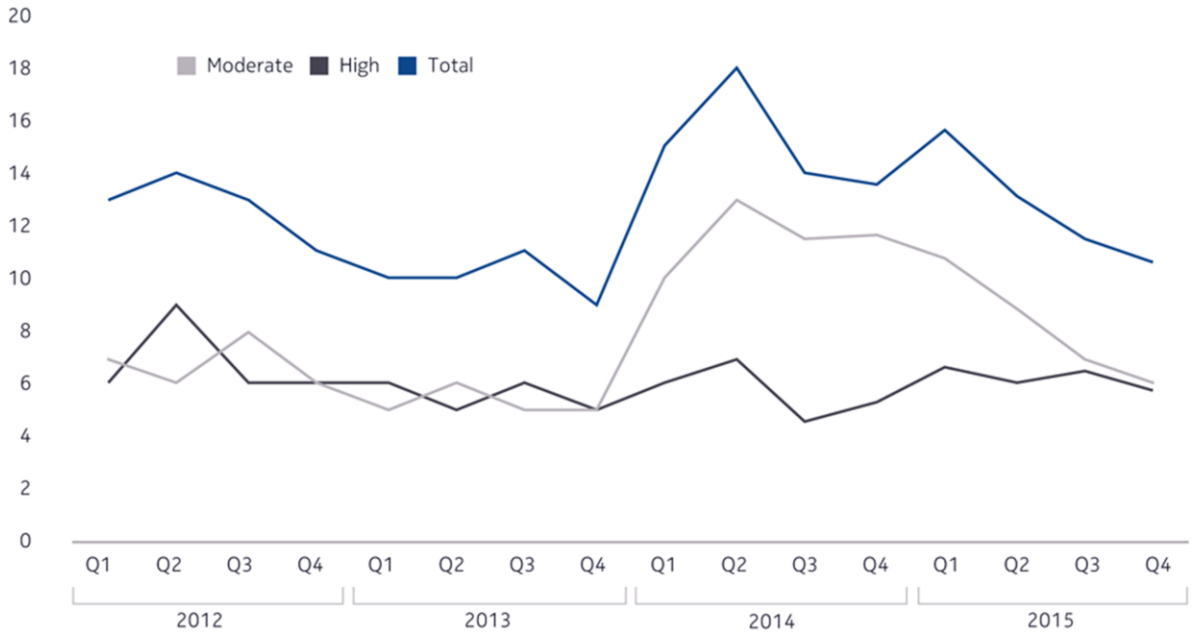
When you consider the insight that the DNS has into the online usage patterns and sites visited of individual users, that customer data could also be leveraged to offer personalized new service propositions. And when you consider the amount of attention that users pay every day to their Web browser, service providers can also leverage that as a messaging channel for enhanced customer communications.

Protecting & Enhancing the User Experience

As shown in **Figure 1,** around 13 percent of home PCs throughout the world are infected with malware. What looks like a declining trend at the end of 2015 is better thought of as a return to trend following an unusual spike from mid-2014 to mid-2015 that was almost entirely due to moderate-threat-level "adware" activity. Infection rates on smartphones are typically a lot lower today but are expected to increase.

Malware poses two specific risks to the end-user experience. One is the risk of subscriber information being stolen and exposed, including for financial fraud. The other is reduced – or substantially reduced – performance of PCs and other devices once they are infected, for example when they form part of a botnet. No matter how it got there, no matter whether the user was partially or wholly at fault in how it got there, users have a tendency to blame their service provider when they are victims of a cyber scam or when they have to endure slow Internet access.

Figure 1: Malware Infection Rates for Household PCs (%)



Source: Nokia Threat Intelligence Report, 2H15

A universal network-based filtering capability that automatically blocks user access to malicious websites is a valuable tool for the service provider. So, too, is the ability to block automated botnet activity to maintain network uptime. Safeguarding the end user against one of the primary sources of cyber attacks can cut off a key source of end-user complaints that is known to drive up customer care calls and put upward pressure on the service provider's churn rate. It also has value in relation to protecting end points in Internet of Things (IoT) deployments.

Personalizing the End-User Experience Via DNS

For any service provider intent on positioning itself as a premium provider with a strong focus on quality, network-level filtering to block access to malicious websites is an important value proposition; however, there are opportunities to go further and leverage the DNS infrastructure to enable more personalized content filtering.

Giving users the means to block specific types of content – such as adult content, violence or content relating to illegal drugs – according to their individual taste has high value for many users. Universal blocking of content, such as that relating to child sexual exploitation, is also being mandated by some regulators, such as in the

U.K. and Germany. The capability to enable users to choose from high, medium or low filtering settings in relation to specific types of content has existed for many years. What's become available in more recent years is the capability to carry out far more fine-grained filtering. This includes the ability to blacklist or whitelist specific websites and the ability at the level of an individual household to create a unique filtering profile for each individual device that connects to the network.

The most obvious application of this capability is for parental controls. Available solutions now allow the adults in the household to have content filtering settings applicable to their own devices, while the settings for their 15-year-old, 12-year-old and 9-year-old children can each be customized according to the parents' taste. Customization can even include time-of-day policies, such as whitelisting or blacklisting specific sites at specific hours of the day. And where a service provider has multiple access networks – such as home broadband, outdoor WiFi or mobile networks – a network-based filtering solution can enforce the exact same individually tailored content filtering policy for that device consistently across all three access networks.

Better Two-Way Customer Communications

Getting the customer's attention, better understanding their requirements, obtaining their feedback and ensuring they have an up-to-date view of your value propositions is critical for any business. And, of course, you have to fulfil all these requirements while not being intrusive to the point of irritating them and triggering a negative rather than positive customer reaction to that outreach.

Universal in-browser messaging is another capability that can be delivered off the DNS server infrastructure with a view to optimizing the quality of two-way communications between the service provider and its customers. This can be delivered in the form of simple text messages or in the form of short videos.

A format where the message appears in the browser, with the service provider's logo, addresses the user by name, and then fades out after a few seconds, is important. This helps differentiate the service provider's legitimate messages from malicious pop-ups. The latter tend to pop up in a separate window, tend to be anonymous and don't typically fade away of their own accord.

In-Browser Messaging Using DNS

The failings of other communications tools provides an important context for leveraging in-browser messaging. Many emails to customers go to defunct email addresses, into spam folders, or are never read. Real-time phone calls to or from customer care centers are expensive, while people often hang up on automated ones. Using in-browser messages can therefore be a useful supplement to a service provider's customer communications strategy.

Among the best use cases for service provider-driven, in-browser messaging are:

- Late payment reminder to avert a re-connection fee following impending disconnection (with link to payment site).
- Short video messages promoting new services (with link to purchase).
- Notification of malware infection (with link to remediation).
- Notification of data usage limit approaching (with link to top up or upgrade).

Case Study: Incumbent European Carrier (I)

Driven initially by a government requirement for major Internet service providers (ISPs) to introduce free content filtering and parental controls, this service provider launched new DNS-based services in December 2013. The company leveraged open application programming interfaces (APIs) into its DNS infrastructure to customize the user interface and integrate with its portal for a common look and feel.

The company branded its universal network protection service "Protect" and its parental control service "Parental Controls," offering consistent policy enforcement across its home broadband network, as well as its outdoor WiFi network.

Having initially left it open to customers to select their filter setting, this service provider subsequently simplified the user experience by making "light" the default setting. According to independent data from the regulator, two thirds of its customers opting in have gone with the default "light" setting, while about a quarter have opted for customized filtering.

This service provider was required by government not just to promote content filtering services to new and existing customers, but to extract from 100 percent of them a formal "yes" or "no" as to whether they wanted to use the services. The company has used in-browser messaging to target a large subset of these customers, but also used other messaging techniques in parallel to measure and compare the different response rates. The company also ran a supporting TV advertising campaign around parental controls, featuring advocacy by a prominent international sports star.

According to the regulator's data, as of June 2015, the company had seen adoption of network level filters or parental control by 24 percent of its customers whose households include children. The regulator also reports that during calendar year 2014, the page presented to the company's customers when a site was blocked was shown approximately 17,000 times a day, or a total of 6 million times during the year.

The company received just 0.01 percent reports of site miscategorization. Of these, 74 percent were actually found to have been correctly categorized, and 26 percent were re-categorized. Where sites had been correctly categorized, the company gives customers an option to add that site to their personal whitelist.

Case Study: Incumbent European Carrier (II)

In March 2016, this service provider began using in-browser messaging capabilities to communicate and interact with a subset of its home broadband customers. Having noticed that subscribers were consuming their Internet access quota much faster after they start using Netflix, the company is now using in-browser messaging to inform them that they are nearing the limit of their data allowance.

This service provider now uses in-browser messaging to communicate with these users when they hit 80 percent of their allowance, and then again once they reach 100 percent and their bandwidth starts to be throttled. Embedded in these messages are an explanation to the customer of their current status and a link to log into their account. They can then pay to top-up or upgrade their monthly service package on a permanent basis.

Case Study: Incumbent Asia/Pacific Operator

As far back as 2011, this fixed and mobile incumbent began deploying content blocking solutions across both its fixed and mobile broadband services. This was consistent with the regulator's direction that specific sites needed to be blocked to prevent the distribution of child sexual exploitation content.

Subsequent to that, content filtering and parental control services were launched in 2015. This company has rolled these services out, initially to its home broadband customers and as part of a strategy to lead in the family household segment.

The company has positioned these "Broadband Protect" services as a high-value, premium service, rather than a universally available one with all its subscriptions. It is automatically included in this company's premium service bundles, thereby contributing to the company's efforts to drive additional revenue, as well as reduce customer churn. In addition, customers that don't want to pay for a premium service bundle are also able to purchase "Protect" filtering controls separately as an add-on service to their lower priced service bundle.

Figure 2: Summary of Real World Service Provider Use Cases

Market	Launch	New Services Deployed
Europe	December 2013	Compliance-driven site blocking. Threat protection, parental controls and in-browser messaging across home broadband and outdoor WiFi.
Asia/ Pacific	2011	Compliance-driven site blocking across fixed and mobile networks. Threat protection and parental controls on home broadband services.
Europe	March 2016	In-browser messaging to notify home broadband users they are about to exceed their data allowance.
South America	2014	Content filtering, as well as in-browser messaging

Source: Heavy Reading

Case Study: South American Operator

This operator is a wholesale satellite TV and ISP, providing services to several local service providers throughout the region. The company's satellite footprint covers the whole of South America. Local operators then resell services, typically in rural areas, to end users.

To date, this wholesale provider has leveraged content filtering and in-browser messaging in two different countries in the region. One has been using content filtering since 2014 in order to comply with regulatory requirements prohibiting access to certain websites.

More recently, since 2Q15, another has been using In-browser messaging to advise its home broadband customers that they are approaching the limit of their allowance. Upon nearing the 2 Gbit/s threshold, this company's customers are sent messages

giving the option to top-up in 1 Gbit/s increments. Prior to introducing in-browser messaging, this company wasn't notifying customers at all that their allowance was about to run out, which was generating a lot of negative reaction from customers.

Summary

A key feature of the "third way" approach to enhancing customer experiences and customer loyalty as outlined in this paper is that it leverages existing DNS infrastructure. Major investment in new capex and in new vendor integration efforts aren't required. It enables services providers to move on from aspects of the legacy approach without requiring that they align immediately with the end target of a fully cloudified digital operations model.

It's certainly critical that any "third way" approach aligns fully with the service provider's digital transformation roadmap. So, as well as being driven from existing network hardware, any such solutions also need to be made available in virtualized format and hence deployable as VNFs on third-party commodity hardware.

It's also important that "third way" solutions be architected in such a way as to avoid even the slightest impact on the existing infrastructure. So, in this case, new services must be deployed off the DNS infrastructure without in any way impacting the core look-up functionality of the DNS, upon which service providers and their customers are so heavily dependent.

About Nominum™

Nominum™, the world's DNS innovation leader, is the first company to create an extensible DNS-based platform and application suite to digitally transform communication service provider networks and business operations.

Nominum N2™ solutions leverage the company's market-leading Vantio™ DNS software and expert team of data scientists to forge a clear path for service providers to evolve beyond a homogeneous, network-centric value proposition to one that is highly differentiated and subscriber-centric. N2 provides an extensible framework that synchronizes service capabilities with people, processes and systems across the service provider organization to personalize the online experience and create greater subscriber value, fueling strong revenue growth, competitive advantage and brand loyalty.

Nominum is a global software company headquartered in Redwood City, California. With service provider deployments in over 40 countries, Nominum software supports more than 500 million subscribers generating 1.6 trillion queries around the globe each day—roughly 100 times more than the combined daily volume of tweets, likes, and searches taking place online. For more information, please visit nominum.com.