Turning VPN Complexity into **IP Services Success**

September 2004

STYLUS TELECOMMUNICATIONS, LLC

in association with

SYNDESIS

Turning VPN Complexity into IP Services Success

Every communications service provider's (CSP) future rests with IP applications. The services playing field has moved from the access pipe itself, to the applications that ride over it. Telcos, cable operators and IP application service providers (ASPs) are battling for the high ground, each with their own advantages. Telcos have a reputation for reliability and scalability, which they must bring forward into the IP world. Cable has a robust last mile, and the most experience with content. ASPs have the advantage of speed and innovation, as well as the ability to deliver services over other CSPs' networks.

Each group is tasked with marrying the reliability and security telecommunications customers often take for granted with the speed and flexibility IP applications demand. VPNs can make this marriage work, but only if the CSP can change VPN complexity from a hindrance to an advantage. Having pioneered VPN and IP services deployment and management with companies like Cisco Systems, Bell Canada, Telecom Italia and SBC, Syndesis has the technology, experience and resources to help telcos and cable operators conquer this complexity and thrive in the IP services market.

The Market for IP Services

There is no longer any question that IP services are becoming the staple and lifeblood of the communications industry. The question today is which CSPs will dominate IP services markets. "Every one of our customers, be they large telcos, mobile operators, or cable operators, is tasking us to help them dominate in IP by taking their traditional strengths and carrying them over into the new market," says John Lochow, President and CEO of Syndesis.

Large telcos, cable operators and the new breed of application service providers coming from hosting, ISP, CLEC and various technology roots will all contend for IP success. Mobile operators are also showing great success and profit from downloadable content and personalized applications. Network-based CSPs – telcos and cable operators in particular – need to have speed, quality, reliability and scalability advantages, lest they lose revenue to more nimble ASPs that use telco, cable and mobile connections to deliver their services to market first.

Hurdles Complicate the IP Transition

Although most CSPs are unique from an operations systems and process perspective, most face common hurdles as they move to IP. For example, network functionality and application capabilities are vast, but not enough have been translated into services. Service, network and operational complexity is increasing at an exponential rate, but there is not enough automation to contain it. New processes and expenses are entering the picture, but there is not enough speed in operations. New CSPs, satellite providers, and ASPs are bringing competition with new services, but are also chipping away at traditional revenue streams. Margins are shrinking because prices have declined, yet operations costs continue to rise. Each of these hurdles must be overcome to

"Every one of our customers, be they large telcos, mobile operators, or cable operators, is tasking us to help them dominate in IP by taking their traditional strengths and carrying them over into the new market," says John Lochow, President and CEO of Syndesis.

win in an IP market where price, features, speed, quality and security are the competitive factors.

Clearing the hurdles to IP success, and creating an organization that can truly support IP applications, takes an understanding of what the IP world will look like once it is reached. The vision is of an always-on environment where users can plug into a network – or a community of services – and access whatever they need, whenever and wherever they need it. "There are no geographic barriers," says Derek Bell, Senior Product Manager for Syndesis. "You don't have to be locally situated as long as you are connected. This is the ubiquity of IP married with content or applications, and it gives customers access to their services from everywhere."

The IP Services Vision

On a grand scale, corporations will connect into applications networks or communities where new services are provisioned at the click of a mouse. These services will include applications from VoIP – which will integrate into other applications as a staple service – to hosted applications including CRM and sales force management, or even streaming video used for training, education and entertainment. The environment customers plug into to access their services will provide not only security, connectivity, and access, but also presence and even mobility.

If a user can access an IP connection – at her desk, at home, in a hotel room, in an airport lounge, through a mobile device, etc. – she should be able to tap into all of the services for which she has permission. A business traveler, for example, should not be less effective or have fewer resources just because she is away from the PC and telephone in her office. She shouldn't have to check three voice mailboxes because she has three phone numbers. And when she taps into the network, it should know who she is, what she can use, what her layout preferences are on screen, and how she likes to take her calls – regardless of where she's physically located.

Provisioning is Logical

From a network perspective, the shift has already begun where head-ends and central offices will look more like application hosting centers than typical switch sites. With services resident in the network and accessible from anywhere, it is possible to move to a logical, rather than physical, provisioning model. This model accommodates customer changes through logical configurations, rather than making changes to physical pipes and equipment.

In this environment, users can tap into a community to access not only their regular services, but also on-demand services that can be highly profitable to the CSP.

Provisioning becomes a matter of changing software permissions rather than calling on an engineer or rolling a truck. Intervals can shrink from days to minutes and the cost to provision services and manage changes can drop significantly. VPNs are the critical enabler because they the dynamic connectivity, security and QoS each service needs, as well as the virtual boundaries that let CSPs create many distinct service communities over the same network infrastructure.

Take Control of VPNs

Making the technology, economics and services work, however, means taking charge of VPN creation and definition. "The number of nodes and instructions in the configuration process is so voluminous and complex that if you just use scripts, utilities, or tools that only do small sub-sets or rely on manual processes, the number of operators, the cost of their skills, and the time involved become outrageous," says Mark Nicholson, CTO and Vice President of Product Management for Syndesis.

Today, too many highly paid engineers are stuck chasing VPN order backlogs using manual processes that cannot handle the escalating volume. VPNs, and the Layer 2 networks they traverse, have become disorderly and can be too unstable to provide the QoS, security and reliability they are supposed to. It is time for CSPs to adopt automated VPN controls that can enforce stability, consistency, automation and speed while freeing engineers to focus on activities that build customer loyalty rather than pushing paper and terminal keys.

Combine Reliability with Flexibility

Communications may be headed towards more applications and content, but in the end people and businesses rely on bullet proof communications. IP services must become carrier-grade to win and keep enterprise customers. ASPs might be the exciting new guys, but most are not yet robust enough to take on the needs of a major enterprise. Telcos have fulfilled quality expectations for years, and they must continue to do so in the IP world. Cable operators must improve their reputation for reliability and innovative services to tap into the strong revenue streams that enterprises, and other consumers of high-profit IP services, can generate.

The trick for any CSP will be to marry a perception of reliability to the flexibility and dynamism that define IP services. This marriage must happen in a very real sense both in the network and in back office operations. On the network, what makes this marriage happy is VPN technology. "VPNs are what enable CSPs to put dynamic IP applications over an industrial, sometimes static network. They can marry flexibility and on-demand services to traditional network reliability. If they want to deliver utility computing, downloadable items that generate billions in profit, and other services, they need to have the VPN piece automated and married to the stability of the transport/core network," says Bell.

Bell further explains that if CSPs are going to make VPNs work to support the IP capabilities they can enable, VPN complexity must change from a hindrance to a market advantage. Manual processes are breaking down under increasing demand and volume, and those with the ability to automate VPN complexities will be faster, more efficient, better able to create and deliver new services, and more profitable.

There are no geographic barriers. You don't have to be locally situated as long as you are connected. This is the ubiquity of IP married with content or applications, and it gives customers access to their services from everywhere.

VPN's Challenges

To understand VPN's challenges, it is necessary to look at its dependencies. After all, a VPN is a Layer 3 service, which means it has a dependent relationship with lower network layers. A VPN cannot be reliable or dynamic if it is not riding on rock solid transport at Layer 2. "CSPs need to make sure their Layer 2 networks are optimized so that the QoS they want to deliver at Layer 3 will work correctly," says Nicholson. The junction between Layers 2 and 3, in a very real sense, is where network stability must support or marry IP flexibility.

CSPs need to make sure their Layer 2 networks are optimized so that the QoS they want to deliver at Layer 3 will work correctly.

Layer 2 has grown and changed significantly over the past decade. Layer 2 networks generally consist of a mix of technologies from Frame Relay and ATM to Gigabit Ethernet. Despite their design differences, technologies must work together to deliver carrier-grade reliability and manageable QoS as a backbone for IP services.

Because many Layer 2 networks were built in haste, however, there are some lingering problems.

The various Layer 2 technologies are often not meshed well and it becomes difficult to provide consistent service quality across a multi-technology connection. Rarely are Layer 2 networks managed with a multi-technology view, much less a multi-layer view. As a result, there are too many dangling circuits and notable capacity is unused, loosely configured or lost. Switching assets are sitting cold in the network or lost in the warehouse because no systems can manage them. In plain words, to get to the point where IP success is feasible, it will first take an investment in some housekeeping to mesh, stabilize and optimize Layer 2.

Above Layer 2, VPNs have some similar challenges. VPNs are extremely complex because of the number of options, modes and functions they involve. "The configuration of a new VPN is a factor of 10 times more complex than a Layer 2 or Layer 1 circuit," explains Nicholson. Most VPNs are manually configured, and often the designs won't support fail-over, redundancy or other reliability factors. Manual configurations, because they are generally inconsistent, also struggle to optimize capacity and can't really provide a predictable basis for service quality. With fast changes happening often, network databases rarely reflect the network accurately which can undermine everything from service creation to billing.

The demand for VPNs – and the applications that run over them – is plainly growing, so the management burden and related problems are growing exponentially. Manual operations will not be able to keep up with all of the complexity multiplied by increasing volume demands, much less fix the problems that already exist. If wrestling with these problems, a CSP will not be in a position to compete on price, speed, care, quality or features. This will open the door to more nimble competitors that can be first to market with the services customers want. To keep that door shut, telcos and cable operators can turn their ability to manage complexity, volume and scale into a major strategic advantage in IP.

Strengthening the Foundation for IP

The first set of tasks in the process to contain complexity involves some of the housekeeping mentioned earlier, which will pay dividends in short order. For beginners, the network configuration problems need to be addressed. As a solution example, Syndesis® NetDiscover™ runs an automated discovery and upload process that not only identifies the physical equipment in the network, but also how it is all interconnected from end to end. It captures logical attributes of the network, like capacity and other factors that involve the networks' true ability to deliver services. NetDiscover also captures network topology; or a view of services and how they currently traverse networks.

This data is organized in information models that provide visibility into the IP layer from Layer 2, so the dependencies between layers become visible and manageable. The discovery and network modeling capability is coupled with functionality to configure and activate network elements – Syndesis® NetProvision™ – which is critical both to the "housekeeping" and to the end goal of automated VPN provisioning.

Verify that all the Data Agrees

Once the network data is gathered, the next step is to verify it against provisioning records and SLA contracts. "CSPs need to look at what SLAs say and ask if they are providing the right level of service because various fixes have been put in place. We reverse engineer from the provisioning record to make sure things are set up the way they are supposed to be," explains Nicholson. Making these types of comparisons requires an OSS that not only makes integration with existing databases simpler, but that also communicates well with the network.

While many OSS vendors have made great strides in application interfaces using technology like XML, few can talk directly to network devices. As a result, many OSSs lose network data integrity very rapidly and have no means to keep themselves up to date. This is an area in which Syndesis delivers significant advantages. Not only is network communication inherent to Syndesis' architecture so that data is accurate, but the breadth and depth of network devices Syndesis supports – and its ability to keep its Equipment Modules in lockstep with major equipment manufacturers' release cycles – is proven to be second to none.

Comparing accurate, discovered network data to provisioning accomplishes two major tasks. It helps to update provisioning records and inventory databases and it ensures that services are configured to deliver what customers order. Further, comparing service data to SLAs also reveals which services are in jeopardy or are failing to meet SLA guarantees because of an improper configuration. Once identified, configuration problems can be repaired immediately.

Restore the "Service Intent"

Repairing a service means bringing it back into compliance with its "service intent." To make sure services are in compliance it is necessary to look at the

The configuration of a new VPN is a factor of 10 times more complex than a Layer 2 or Layer 1 circuit.

health of the physical equipment and look for problems in logical configurations that can affect service quality yet often go unidentified.

"Engineers make all kinds of changes to the network. They might fix a trunk, for example, but don't see the hundreds of services running over it. In the end, the connectivity may be fine, but the QoS and other logical aspects are not there and thus the change affects the service intent," says Nicholson. "Service intent" is a term Syndesis has coined to describe all of the quality, security, feature and behavior variables that can be elements of a service. A VPN that meets all of its guaranteed SLA parameters is one example of a service that meets its service intent.

Engineers make all kinds of changes to the network. They might fix a trunk, for example, but don't see the hundreds of services running over it.

For the large majority of repairs, rather than rolling an entire service out of the network to then re-design and re-provision it, Syndesis will identify the specific factor of the service that is causing trouble and repair it through automated provisioning. Such repairs could involve returning a VPN segment to its original route over a Layer 2 network, or resetting QoS parameters to ensure consistent quality across multi-technology segments at Layer 2. It could also include re-configuring a VPN to ensure reliable fail-over while weeding out unrecorded changes that waste network resources, thus creating consistency in how existing VPNs are configured.

As a result of this whole process, dangling circuits are groomed out of the network, transport networks are aligned with Layer 3 services above them, available capacity is recovered and optimized, and VPN-based services already provisioned in the network are restored or reconfigured to meet their service intent. Once this housekeeping is done, it is time to focus on delivering more new services.

Automate Provisioning

Provisioning and activation capabilities are at the core of service delivery, and are part of the process to restore "service intent." Automating these capabilities is proven to significantly reduce costs and time to market for any technology or service. In a VPN, it is a real necessity because of the vast complexity. VPNs can literally have thousands of configuration options that go into the design of a single circuit. This is why manual provisioning is so slow, complicated and prone to error. Ultimately, however, the number of options is finite and can be contained and made accessible with software automation.

For provisioning new services, Syndesis provides templates that allow IP experts to define the standard parameters for VPNs within various profiles, thus making the most complex aspects of VPN provisioning repeatable and able to be automated. "Our process involves two users. One is the IP expert who defines the network parameters and creates profiles that tune the hard parts of VPN configurations. A provisioner can then use a GUI, working off of the profiles, to configure three options instead of 25 for each VPN order," explains Patrick Rhude, Director of IP Product Management for Syndesis. A provisioner is far less expensive and less difficult to train than an engineer. From here the second user, a service representative – an even less expensive and trained person – can complete most orders. In an ideal, fully automated

architecture, orders can flow through directly into provisioning from an integrated ordering system.

Layer 2 provisioning takes place in this process as well, ensuring the Layer 3 VPN is riding the transport that is designed for it. In the process, this combines what would normally be separate orders and manual provisioning processes for IP and ATM into a single, automated transaction. This significantly reduces order fallout and shortens the time to fulfill every order and results in improved revenue realization and a reduced cost to provision each and every VPN.

For repair provisioning on services already in the network, Syndesis provides some more specific tools. For example, an engineer can use Syndesis® NetProvision™ to synchronize Layer 2 connections over multiple technologies. When the user selects a technology type, he will only be able to provision within the parameters that technology can provide. As the various segments are provisioned, the system can ensure the end-to-end connection and QoS are consistent across the technologies. This helps ensure consistency across technology domains, but also eliminates the mental gear-shifting for the engineer as he traverses Frame, ATM, Ethernet and IP networks.

An Engine for Scale and Volume

For all of this complexity, there is no getting past the need for power and scalability. Many OSSs are linear and single-threaded, meaning they break down under high volumes and essentially cannot multi-task. The Syndesis solutions are built around a high volume, high throughput transaction management system that allows multiple concurrent transactions and future transaction scheduling. It can also handle high volume rollback in critical situations where network segments must be restored to their last known functional state. Syndesis customers run as many as 30,000 complex provisioning transactions through this engine every day and have not yet hit the limits of its performance.

Speeding Service Creation

With all of these capabilities in place, service creation can advance significantly. "The hurdle stands between defining a service and actually getting it onto the network," says Bell. What the OSS platform should do, and what Syndesis provides, is automatic translation from marketing's definition of a service to how that service is delivered and configured in the network. "CSPs must focus on what services they need to offer, and then tell the network engineering group so they can produce guidelines. Too often today, network engineers tell marketing what they can and can't sell, and this process is too confusing to be supported efficiently," says Bell.

Given the discovered and modeled network and service information, marketers can gain a clear view of the exact capabilities the network can offer and then create services that reflect what is actually deliverable. In an ideal scenario, this would allow marketing to create services and move them into provisioning without manual intervention. As a result, services are not

"The hurdle stands between defining a service and actually getting it onto the network."

Syndesis has been heavily involved in developing VPN management solutions since VPN technology was invented in the mid-nineties.

only created faster but also instantiated faster, providing a time-to-market and service innovation edge while speeding revenue recognition on new offerings.

With services well defined according to real capabilities, service provisioning is made consistent. For example, "gold level service" is always defined as providing 10 Mbps. The end result is a set of highly repeatable service components that can be combined into innovative offerings that are automatically provisioned in the network. This allows CSPs to deliver flexible, telco-grade IP services while winning on price, speed, features and quality.

Making it Real

This all sounds ideal, so the important question is who can deliver the OSS capabilities necessary to make it all real? In truth, there are very few OSS providers that have the combined technology, knowledge, field experience and financial depth to serve a large CSP and help it tackle its VPN and IP services challenges. Syndesis is perhaps the only vendor that holds up in each category and is one that CSPs should evaluate as an advantageous technology partner.

Syndesis has been heavily involved in developing VPN management solutions since VPN technology was invented in the mid-nineties. This is particularly evident in Syndesis' partnership with Cisco Systems, with which it has maintained OEM relationships for its provisioning solutions. Syndesis also invests in relationships with most of the major equipment manufacturers whose products make up telco networks today. Syndesis' test lab houses a large variety of network devices and rivals most major telcos and the U.S. Department of Defense in terms of its scope and complexity.

What speaks loudest for Syndesis, however, is its portfolio of powerful customers. Companies such as SBC, Bell Canada, and Telecom Italia have recognized Syndesis not only for its technology solutions like NetProvision, but also for its dedication to customer support and responsiveness. Syndesis has become a trusted technology partner to these major carriers. They have each made significant investments in Syndesis solutions at the core of their service delivery operations for services like ATM, DSL, VoIP and IP-VPNs.

Unlike many OSS providers, Syndesis is a strong, stable, growing company. Its leaders earned their stripes working as CSP staff and executives. Syndesis understands how to bring quality and reliability together for large scale CSPs, with the tools to manage IP's complexity and dynamism. IP applications are the next frontier. Customers are watching the pioneers, but expecting the CSPs they have always relied on to step up and deliver the IP applications they want and the speed, quality and reliability they often take for granted. To make it all happen, Syndesis is the right partner for a CSP that wants to wade into the battle for IP services with a clear path and the right technology to ensure victory.

SYNDESIS • Headquarters • 30 Fulton Way, Richmond Hill, ON **L4B 1E6 CANADA** • **+905-886-7818**
info@syndesis.com • All rights reserved • www.syndesis.com • Copyright © 2004 Syndesis Limited

Stylus Telecommunications LLC • Edward J. Finegold, General Partner • 56 Bluff Avenue, Greenwood Lake, NY 10925 • +845-920-8065
ejfinegold@styluscom.com • www.styluscom.com