

APRIL 2001

WHITEPAPER



# IP VPNs and the Land Run for New Revenue

Prepared for Celox Networks by Telechoice, Inc.



# Table of Contents

- An Expanding IP VPN Opportunity.....1**
- The Evolving Enterprise Landscape .....2**
- The Impact on Service Providers .....3**
- Enter IP VPNs.....4**
  - Current Status of IP VPN Solutions .....4
  - Concerns of CPE-Based IP VPNs.....6
  - Key Market Lessons Learned From CPE-Based IP VPNs.....7
  - The Future of IP VPNs.....7
- The Bottom Line: Strong IP VPN Revenue Opportunities.....8**
  - A Quick Look at the Numbers.....8
  - Strategic Opportunities for New Land Grabs and New Revenue.....9
- Summary of Service Provider Market Opportunities.....11**
- Laying Tomorrow’s Foundation Today.....12**
  - Network-Based Solutions ..... 12
- Summary.....14**

## An Expanding IP VPN Opportunity

Today's service providers are facing an increasingly agile and aggressive environment. The enterprise is smaller, faster, more specialized, and more concerned about time-to-market than ever before. As a result, they require vendors and partners who are able to operate and deliver under similar circumstances. Slower service providers who lag behind the frontline requirements of today's market will find it increasingly difficult to establish the kind of value-added partner relationships sought by modern customers in their vendor arrangements.

The rules of the game have changed substantially. Specifically, entire industries have begun to internalize the network as part of their product or service. A simple example of such internalization is the bundling of Internet access connectivity with wireless PDAs. From a technology perspective, greater value can be created through enhanced network intelligence and connectivity. With broadband connectivity moving increasingly towards the edge of the network and end-user applications into the core of the network, modern communications are becoming more dynamic, accessible, and individualized than ever before.

### General Trends Impacting Service Providers:

- Increasing competition, technology innovation, and high investor expectations
- Industries have begun to internalize the network as part of product/service
- Value is created through network abundance and connectivity
- Broadband is moving to the edge of the network
- Content and applications are moving to the core of the network
- End users are becoming focused on content, context, and community
- Telecom industry is separating into vertically focused segments: infrastructure providers, service providers, and retailers

In order to keep pace with these changing market requirements, service providers have become increasingly specialized, segmenting themselves into infrastructure providers, service providers, and retailers. In this model, infrastructure providers handle the core transport responsibilities and service providers add enhanced management and provisioning capabilities at the edge, while retailers "own" and directly manage specific market niches. Service providers today may fulfill two or three of these roles simultaneously; therefore, for the purposes of this paper, all three segments are collectively referred to as service providers.

Regardless of their chosen segment, all service providers have encountered the same issue. As competition balloons and margins and differentiation among providers fade, traditional services such as frame relay and simple Internet access have become increasingly commoditized.

In response to these pressures, many service providers are seeking higher-margin services to move themselves away from playing the singular role of simple infrastructure provider. To survive the spiraling threat of obsolescence via the commoditization of basic transport services, they must incorporate more value-added services—not just scaled bandwidth for decreased delivery costs.

One particular value-added application that has gained considerable traction in the market is the IP VPN. Like public Internet access, frame relay, and ATM services before it, the IP VPN will also eventually become a commodity transport. However, IP VPNs are well positioned as the launching pad for the value-added services that tomorrow's enterprise will require. The IP VPN of tomorrow is capable of being seamlessly integrated with the delivery of higher-value solutions that will leverage its features and functionality.

## The Evolving Enterprise Landscape

Enterprise requirements are demanding and will only increase going forward. Today's traditional networking options fall far short of the market's two baseline requirements:

1. Accessible, reliable, and flexible network bandwidth
2. Security

Private frame relay and ATM networks require that endpoints, bandwidth, and QoS parameters be predefined at least a month in advance. Today, it is becoming more and more difficult for end users to accurately anticipate the exact endpoints, the bandwidth, and the QoS for each and every one of their communications paths. Thankfully, accessing a traditional IP network can be much easier than frame or ATM. However, security, bandwidth guarantees, and QoS may be non-existent when using traditional Internet access services.

With the advent of the Internet and the World Wide Web, the rules of business have shifted dramatically. Bricks and mortar are no longer necessary to assemble, house, and leverage top personnel, information, and resources to operate a successful business. Seemingly overnight, specialized and very aggressive new business ventures are springing up to stake their claim on increasingly lucrative markets.

In order for companies to successfully manage their businesses in the new virtual world, reliable communications links between vendors, partners, employees, and customers are essential. Moreover, the confines of these increasingly virtual enterprises have begun to extend well beyond the borders of the US and into varied international markets. Also, with greater specialization and focus on core competencies, businesses are less inclined to manage internal IT networking skills themselves.

In short, businesses are becoming increasingly dependent on highly reliable, flexible, and highly secure networks, but they are also much more willing to outsource such functionality.

### Summary of the Enterprise Evolution:

- Globalization and hypercompetitive markets
- Decentralization and the rise of telecommuting and mobile workers
- The increasing ubiquity of IP in the network
- Web enablement of internal processes for bottom-line savings
- Integration of the supply chain for strategic and cost advantages
- Growing desire to outsource and focus on the core business
- More infrastructure value for less expense
- Increased need for highly reliable, flexible, and yet highly secure networks

## The Impact on Service Providers

As a result of the ballooning opportunities across the enterprise market, others have come to join established service providers in competing for this newfound wealth. For example, ASPs (Application Service Providers) essentially did not exist five years ago, yet they are poised to stake an impressive claim on the market's available pool of network dollars.

Existing service providers are finding themselves adopting more defensive postures to protect their customer base from the flood of agile and highly aggressive new competitors. However, given that enterprises are looking toward their service provider for direction and implementation more than ever before, service providers have begun using sophisticated, value-added solutions to proactively counteract these new competitive pressures.

The key to acquiring and retaining customers with value-added services is the underlying infrastructure that service providers use to support enterprises' basic networking requirements. Once these basic connectivity needs have been quickly and effectively implemented, it is much easier for service providers to begin layering in value-added solutions such as QoS and policy-based services.

It is important to note, however, that enterprise customers are fighting for a toehold in today's new whirlwind business environment. Time-to-market and time-to-scale issues are key to these customers' survival—and hence, to service providers' survival as well.

### The Evolving Enterprise's Impact on Service Providers:

- Expanding enterprise needs bring additional service provider competitors
- Must protect existing base in order to drive new revenue sources
- Sophisticated, high-value, business-enhancing solutions at cost-effective levels
- Enterprise looking to the service provider for direction and implementation more than ever
- Underlying infrastructure or connectivity provided by service provider to the enterprise is the basis from which the service provider will begin to offer and layer revenue-generating, enhanced solutions
- Time-to-market and time-to-scale are key to customer survival—and hence, to service provider survival as well

## Enter IP VPNs

Fortunately, the IP VPN seeks to combine the strengths of the frame relay/ATM world with those of the public Internet. Specifically, it hopes to combine the security and reliability of frame relay/ATM with the simplicity, scalability, and flexibility of the Internet. Given the geographically diverse and ever more remote nature of today's workforce, IP VPNs appear well poised to become the common denominator behind the solutions offered to this ever-shifting market.

Like an electric power grid, the IP VPN model disguises its sophisticated capabilities behind its apparent simplicity. Residential electric customers need only to match an electrical outlet with a power cord from electrical appliances as far-ranging as coffeepots and refrigerators. The power grid behind such electrical outlets has already been equipped with the intelligence needed to feed only the amount of power that each appliance "requests." All of the complicated steps involved with precisely gauging, provisioning, and adjusting power levels between individual customer appliances and the electrical network have been internalized and automated in a way that is similar to IP VPNs. Customers no longer have to preplan specific endpoints, average bandwidth levels, or QoS parameters for every possible communications path existing inside their VPN.

### Current Status of IP VPN Solutions

Because service providers did not initially have the ability or market pressure to support managed IP VPNs, customers were often forced to build their own CPE-based solutions. At the time, the benefit was that the customer realized immediate cost savings from such networks over traditional VPN alternatives such as frame relay and ATM. There simply was no similar option offered by service providers.

Many of the original benefits of CPE-based IP VPNs are still reassuring for customers and are hence today perceived as valid benefits toward which customers still gravitate. Overall, the central theme behind these benefits is that customers retain ultimate internal control over their own IP VPN. Some internal IT departments are willing to invest the time and energy needed to design and manage such networks to ensure that they are using only the best-in-class technology for each specific need. Further, many of these customers do not like to be too closely dependent on their service provider and therefore prefer to maintain internal control over their corporate networks.

Eventually, service providers added CPE-based IP VPNs to their managed service portfolios. Customers are now able to outsource all of the headaches and hassles associated with installing and managing the equipment needed to support a wide area IP network. Unfortunately for carriers, the piecemeal problems associated with IP

| <b>Benefits of CPE-Based IP VPN Solutions</b>  |  |
|--|--|
| <b>Perceived Customer Benefits</b>   | <b>Perceived Service Provider Benefits</b>   |
| <ul style="list-style-type: none"> <li>• Control, control, control</li> <li>• Control over security credentials, systems, and practices used to access network                             <ul style="list-style-type: none"> <li>✓ Full end-to-end encryption (including local access)</li> <li>✓ Dedicated aggregation and encryption equipment</li> <li>✓ End-user access can be managed by either customer or service provider</li> </ul> </li> <li>• Maintain ISP/Carrier independence</li> <li>• Control over best-in-class equipment purchases</li> <li>• Can better fine tune solutions to match network requirements on a site-by-site basis</li> </ul> | <ul style="list-style-type: none"> <li>• Small upfront capital investment per site</li> <li>• Greater perception of last-mile security (end-to-end encryption)</li> <li>• Ability to leverage certain customers' preference for control over solution (i.e., large enterprises likely to maintain CPE-based VPN and firewalls over sophisticated environments for some time)</li> <li>• Does not require major shift in thinking on the part of the customer (customers were inadvertently trained to manage things themselves in the world of frame and ATM)</li> <li>• Additional sales opportunities for other managed services (e.g., managed routers, Ethernet switches, etc.)</li> </ul> |

VPNs have simply been passed from customers to themselves. However, there are a number of compelling reasons why many carriers have elected to initially absorb the costs of CPE-based solutions on behalf of their customers.

There is, of course, a completely separate set of benefits and trade-offs for service providers who elect to support their customers' IP VPN requirements with CPE-based solutions. In general, IP VPN vendors heavily leverage the market's perception that CPE-based solutions are more secure than network-based solutions. However, many other customers and carriers readily dispute such claims and contend that dedicated local loops to customer sites are often one of the most secure of all network components. Finally, the last key benefit of CPE-based solutions is that they require less upfront investment by the service provider, and services can therefore be deployed much more quickly and cheaply than network-based infrastructures.

## Concerns of CPE-Based IP VPNs

While CPE-based IP VPNs are guiding the industry in the right direction, there are still some lingering concerns from customers and service providers alike.

Several of the key concerns shared by customers and service providers are the adverse cost and performance issues associated with CPE-based IP VPNs. For example, because CPE-based IP VPNs require a separate truck roll to each and every site associated with a customer's VPN, the installation times can be extremely protracted. For the customer, such lengthy installation times mean frustrating service delays. For the service provider, such delays translate to lost revenue for the duration of the installation period.

| Concerns of CPE-Based IP VPN Solutions   |   |
|--|---|
| Customer Concerns  | Service Provider Concerns   |
| <ul style="list-style-type: none"> <li>• Long installation times</li> <li>• No carrier-grade reliability and redundancy built into CPE</li> <li>• Customer must devote time to participate in all installation and troubleshooting processes</li> <li>• Limited scalability: Limited ability to add or expand services or functionality with existing equipment</li> <li>• Requires use of single equipment vendor for all sites included within customer's VPN</li> </ul> | <ul style="list-style-type: none"> <li>• Long installation times = Delayed revenues</li> <li>• High installation costs: Installation requires truck roll to <u>every</u> site on VPN (including remote or difficult sites)</li> <li>• High management/maintenance costs: Upgrades and some maintenance problems require an additional truck roll to customer site</li> <li>• Lower performance levels due to dependence on non-carrier-grade CPE</li> <li>• Must involve customer in nearly all installation and troubleshooting processes</li> <li>• Limited scalability: Difficult to sell customers expanded or improved services or functionality</li> <li>• Limited management capability: Limited remote management capabilities and visibility, as well as support of multiple vendor platforms</li> </ul> |

The distributed nature of CPE-based solutions also balloons the costs associated with ongoing maintenance, management, and upgrade costs. Similar to installation efforts, subsequent management of the CPE-based IP VPN often requires truck rolls to all customer sites affected. This makes customers all the more hesitant about ordering new services from the service provider, as expansion of existing services or the addition of new functionality sometimes requires forklift upgrades to the CPE and a new set of management headaches. Finally, considerable frustration for customers and service providers alike still emerges when sub-par performance issues materialize due to the use of CPE that was never designed with carrier-grade reliability and redundancy in mind.

## Key Market Lessons Learned From CPE-Based IP VPNs

While most of the first-generation IP VPNs are still CPE-based, two baseline demands have emerged from the market overall. First, end users expect their service provider to manage their IP VPN for them. While some customers are not always willing to outsource all functions of the IP VPN, most large businesses clearly recognize the benefits of the model. Hence, those managed service offerings that are not only comprehensive but also flexible are capturing the most interest from the market.

Secondly, customers are adamant that security across IP VPNs be as good, if not better, than comparable frame relay and ATM services. Specifically, customers expect security management options to include basic firewall functions, encryption, and tunneling, in addition to digital certificate authentication and ongoing, managed PKI (Public Key Infrastructure).

## The Future of IP VPNs

While managed services and security capabilities are today's baseline requirements, the market continues to express recurring preferences, which offers insight into what their new demands will look like tomorrow.

First, applications that pass across IP VPNs are expanding well beyond the boundaries of internal email and Internet access. Businesses have begun to expand the breadth and depth of IP VPN responsibilities by creating Extranets that help businesses create increasingly sophisticated and specialized communications links with both their partners and their customers. The result is that companies are able to enjoy quick, reliable, streamlined communication with all entities—both internal and external—that hold a stake in the company's success.

Second, customers are demanding increased control over their IP VPNs. Specifically, they are demanding greater visibility and management capabilities over their

### The Market's Evolving IP VPN Trends:

- IP VPNs are not yet mass market but are seen as the foundation for new enterprise services
- Network-based IP VPN solutions are gaining momentum over traditional CPE-based IP VPN solutions to serve mass market efficiently
- #1 market mandate about IP VPNs: Security
- Combination of hardware and software-based security solutions employed with VPNs
- Combination of CPE-based and network-based VPN delivery mechanisms
- New broadband access options for VPNs: xDSL, cable, burstable Ethernet, etc.
- New QoS standards/mechanisms for VPNs: DiffServ, MPLS, traffic shaping, etc.
- Increased demand for policy-based services (across applications, users, and groups)
- Increased demand for end-user visibility and control (e.g., CNMS tools enabling self-provisioning and online monitoring of applications, users, and groups)



networks. Such improved information about their networks allows customers to manage and control network reliability more proactively in concert with the service provider. Not only do customers feel more aware of the status of network problems, but proactive resolution with the service provider also helps minimize the outage time and impact on end users. Such capabilities are typically extended to customers of other services via Web-based CNMS (Customer Network Management Systems). The expected functionality of CNMS tools for IP VPNs would, at a minimum, include customer-controlled QoS management, end-user access, and the assignment of priority privileges. The bottom-line theme of CNMS is that customers are able to fully outsource responsibility to the carrier for managing their network, yet still retain control over key service parameters.

Finally, there is increased interest in applying QoS and priority levels across different users, groups, applications, or flows. While QoS will enable customers to increase the amount and type of traffic carried across IP VPNs, the ability to adjust priority levels will help them manage associated costs as well.

## **The Bottom Line: Strong IP VPN Revenue Opportunities**

### **A Quick Look at the Numbers**

Even a cursory review of the numbers underlying the revenue opportunities for IP VPNs is impressive, to say the least. Frost & Sullivan projects that revenue from the US IP VPN market alone will explode from approximately \$1 billion in 1999 to \$13.5 billion in 2004.

Moreover, a study by Infonetics Research predicts that by the end of 2001, the number of individual remote users accessing VPNs will mushroom to 15.5 million. The number of organizational sites and Extranet partners using VPNs worldwide will also expand to 1.4 million and 1.3 million, respectively.

Combined, these two numbers point to the fact that carriers will likely be facing a market that requires more network connections and endpoints than ever before, with a penchant for IP VPNs in particular. Without a doubt, IP VPNs are expected to be the very foundation upon which customers will begin layering a myriad of current and future applications. Hence, like the other VPN technologies before it, once basic IP VPN networks become commoditized, value-added services and their associated margins will soon help to drive carriers' overall profitability.

In short, carriers that are not prepared to provide customers' foundational IP VPN networks today stand little chance of capitalizing on the plump margins of value-added requirements that will certainly follow tomorrow.

## **Strategic Opportunities for New Land Grabs and New Revenue**

Even without the addition of new value-added services of the future, carriers still face the prospect of mining lucrative opportunities from the IP VPN market today. In fact, there are two separate veins of opportunities in the form of new markets and new services that are exposed today and ready for carriers to exploit.

### **New Market Opportunities**

The first key benefit of IP VPNs for carriers is the enhanced capability and lower price points for new services that enable carriers to target entire new market segments.

#### **Small and Medium Businesses**

One of the most obvious new markets for IP VPN carriers is the small or medium-sized business. In the past, traditional VPNs were only accessible or viable for larger commercial enterprises, due primarily to their cost. However, with IP VPNs presenting extremely aggressive cost/benefit ratios over frame relay and ATM, small and medium-sized businesses are now able to leverage a valuable communications tool that had previously been beyond the grasp of many. With IP VPNs, small and medium-sized companies no longer have to passively accept such glaring communications (and competitive) disadvantages to their deep-pocketed counterparts.

Moving forward, as carriers are able to improve their internal cost of service delivery for IP VPNs to this segment of the market, they will have the opportunity either to realize improved margins internally and/or to offer more aggressively priced services while passing on savings to the enterprise. Specifically, IP VPNs could offer current frame relay or ATM VPN customers superior network functionality at prices that are comparable or lower than those that businesses currently pay for the more baseline functionality of traditional VPN services. The win-win scenario in this case delivers greater functionality to the customer in exchange for more lucrative margins by the carrier.

#### **Business-to-Business Communications**

Another market expansion opportunity enabled by IP VPNs is the ability of carriers to position themselves as the glue in business-to-business communications. With traditional VPNs, carriers simply provided private, self-contained communications infrastructure for each commercial enterprise. However, these traditional VPNs were never really positioned to privately link two or more companies together (e.g., communications channels between a company and its suppliers, distributors, customers, etc.).

Through the reach and flexibility of IP networks, private links to key commercial partners can be enabled easily under the umbrella of an IP VPN. The IP VPN's single network access point can be used to communicate with multiple business partners rather than purchasing separate networks for every private communications link required. As a result, carriers can serve as the commercial market's trusted courier for establishing and managing private, secure communications links between customers and their business partners. Through the use of firewalls, encryption,

tunneling, and managed PKI, carriers can use IP VPNs to create an accessible and highly flexible network that is truly conducive for secure business-to-business communications.

## New Service Opportunities

In addition to attracting new market segments to carriers' services, IP VPNs will also enable these same carriers to offer enhanced services to further attract and retain new customers. For example, carriers could easily bundle complementary services to their core IP VPN Intranet and Extranet solutions in a way that would tighten customers' business processes to the carrier and thereby increase customer retention.

Carriers provide a secure, reliable environment, complete with redundant network connections, for hosting companies' various servers. There are several

types of commercial enterprise applications that could be advantageous to outsource to a carrier. Examples of applications that would fit well with carriers' managed hosting service include a company's public Web server, email gateway and server, domain name server, corporate directory, etc. The more business processes carriers can help customers tie into their basic IP VPN network, the harder it will be for customers to leave their chosen carrier. The carriers first to support IP VPN services are more likely to retain that portion of their existing customer base that may already be looking to migrate to IP VPNs. In addition, such carriers will also be one of the few options new customers will have for such services. Hence, through their base IP VPN offerings, leading-edge carriers should be able to quickly establish a large, ready-made customer base, to which they can also up-sell enhanced services that will help further bind customers to them.

### New Revenue Sources From IP VPNs:

- Capture new revenue from new market segments (e.g., small and medium-sized businesses) that were previously unable to afford VPN services
- First real opportunity to offer customer-facing SLA (Service Level Agreement) management and SLA verification tools for IP VPNs
- Managed VPN security solutions (e.g., firewall services, encryption, tunneling, managed PKI, etc.)
- Create new services that help establish secure communications links for private business communities (e.g., managed Extranet services)
- Acquire new users/customers faster via sales through managed Extranet VPN services (i.e., selling to other entities along existing customers' supply chains, like suppliers, customers, or associated business communities, rather than to each individual company)
- Retain existing and future customer revenue by tying customers' internal networks and applications closer to the carrier (e.g., providing managed data hosting facilities for company websites, email servers, corporate directory, etc.)

## Summary of Service Provider Market Opportunities

Today's carriers enjoy the benefit of sitting at the crossroads of two exciting trends. First, the market is quickly beginning to migrate away from traditional VPN technologies such as frame and ATM toward IP VPNs. Secondly, customers' appetite for enhanced services is growing in parallel with the increasingly distributed nature of their workforce and their tendency to intertwine processes and communications with those of their suppliers, partners, and customers.

With customers conducting business across such wide-ranging geographic and commercial boundaries, the services needed to support their ballooning requirements are becoming increasingly sophisticated. Such enhanced services can potentially translate into very lucrative margins for service providers that already own the IP VPN customer base. Carriers should consider the infrastructures ability to support network based VPNs and the platforms ability to layer additional services on the same infrastructure. Carriers then become better positioned to win the market's frantic land grab war by quickly capturing IP VPN accounts before the high-margin, value-added service opportunities begin to take root.

In short, customers' internal organizations and processes are becoming more and more dependent on VPNs and are looking toward IP VPNs (and new IP VPN service providers) as a better solution for their new networking requirements. With the market already beginning its mass migration from traditional VPN services to their IP counterparts, service providers would be well advised to elbow their way into an optimal market position that is best prepared to capitalize on this impending flood.

### Summary of Service Provider Market Opportunities:

- Market is already beginning migration from traditional VPN technologies (e.g., frame relay and ATM) toward IP VPNs
- Customers' increasingly distributed workforce and dependence on intertwining the processes and communications of partners, suppliers, and customers are ballooning their requirements for enhanced services
- Customers are demanding and budgeting for such services
- Higher-value services lead to increased profitability
- Customer retention increases as customers purchase more services from a single provider
- Enhanced services will lead to other product sales
- The competition is offering enhanced services
- Helping customers meet their business objectives is a much more strategic position for a service provider than merely providing them with bandwidth
- First goal of service providers should be to win the land grab for capturing IP VPN accounts
- The sale of high-margin, enhanced services will soon take hold on service providers' existing IP VPN accounts

## Laying Tomorrow's Foundation Today

Service providers can support IP VPNs using two very different types of solutions. The earliest type of IP VPN was initially pieced together by customers themselves using CPE-based solutions. However, now that service providers have begun to recognize the market's groundswell toward such solutions, they have just recently begun to consider incorporating centralized IP VPN capabilities into their own networks.

While certain service providers and customers favor CPE-based IP VPN solutions, others are recognizing the need for network-based solutions. Hence, it is important for a service provider to understand the benefits and possible downside surrounding each option before choosing its respective IP VPN infrastructure strategy.

### Network-Based Solutions

With service providers now watching their customers take fairly drastic steps to leap outside of traditional network service offerings in order to find IP VPN solutions, the wake-up call has been sounded. Service providers have realized that they need to adapt to the market's new prevailing

winds or be swept away by a wave of customers leaving them for other providers that could support IP VPNs. As a short-term response, the world's largest carriers began to offer CPE-based IP VPN solutions. However, the same hurdles that appear when service volumes exceed carriers' ability to manage them in a piecemeal fashion are now beginning to loom on the horizon.

For example, the high costs of truck rolls for each and every site, in addition to higher

management and maintenance costs associated with such distributed solutions, only grow larger as customers migrate to IP VPNs. Under a CPE-based IP VPN solution, carriers are unable to step away from their linear cost models to realize higher margins from scaling benefits, even after

| Benefits of Network-Based IP VPN Solutions   |   |
|--|---|
| Perceived Customer Benefits  | Perceived Service Provider Benefits   |
| <ul style="list-style-type: none"> <li>• Lower overall costs (fewer personnel, capital, and other resources devoted to internal management of network)</li> <li>• Faster planning, design, and deployment</li> <li>• Easier, faster addition of new sites</li> <li>• Eliminates risk of technological obsolescence, with upgrades carried out within the carrier network rather than within the CPE</li> <li>• Flexibility to easily add/activate new functionality and security options</li> <li>• Easier maintenance efforts (i.e., no long waiting lists for hardware/software upgrades)</li> <li>• New services become available without changing equipment</li> </ul> | <ul style="list-style-type: none"> <li>• Overall: Fatter and faster profits</li> <li>• Highly scalable architecture</li> <li>• Mass customization now possible</li> <li>• No truck rolls</li> <li>• Flexibility to easily add/activate new functionality and security options via centralized management capability</li> <li>• Faster service turn-up and associated revenue flows</li> <li>• Security equal to FR and ATM (including last mile)</li> <li>• Logical aggregation of thousands of customers</li> <li>• Lower-cost, centralized, and flexible provisioning</li> <li>• Opens new SMB market to service providers for the sale of VPN solutions</li> <li>• Superior time-to-market and time-to-scale advantages at the onset of market's early-majority adoption of IP VPNs</li> <li>• Retain existing subscribers while upselling new services</li> </ul> |

their total number of customers explodes. Higher margins from scale aside, many service providers find it difficult to even locate and hire enough qualified people to help support such labor-intensive solutions.

As a result of the scaling pressures surrounding both static profitability and labor shortages, service providers have begun looking toward network-based solutions from vendors such as Celox Networks to help better address the mass market's move towards IP VPNs. With the market now validated through CPE-based solutions, service providers are gravitating toward network-based IP VPNs' promise of higher margins and lower personnel and support requirements, as well as faster installation times.

Is this excitement warranted? To some degree, yes, the excitement is warranted. For example, while customers do not have infinite levels of flexibility as they would with CPE-based solutions built from the ground up, network-based IP VPN carriers do have the latitude to offer mass customization across certain service portfolios.

Security is another reason some segments of the market refuse to consider anything but CPE-based IP VPNs. While full end-to-end encryption is possible under CPE-based solutions, the security of network-based IP VPNs is no better or worse than that of the traditional frame and ATM networks that customers have trusted for nearly a decade. As with frame relay, network-based IP VPN customers trust their service providers to transmit communications from one site to the other with maximum security. The dedicated access facilities or local loops tying customer sites to the edge of their carrier's network are often identical to those used for frame relay networks. In short, because network-based IP VPNs are managed across a carrier's own (private) network in the same manner as traditional frame relay and ATM networks, then good or bad, security issues between the two networks are identical.

Time-to-market and time-to-scale have been another central concern about investing the time and energy it takes to create a network-based IP VPN infrastructure. One of the key benefits of CPE-based IP VPNs has been the fact that it is a solution that could be brought to market relatively quickly. This solution worked exceptionally well when the market for IP VPNs was in its nascent stage and volumes were low. However, CPE-based solutions seem to have exactly the opposite impact on time-to-market and ease-of-scaling issues once customer volumes balloon beyond critical mass. Beyond that point, network-based solutions gain and amplify their advantage over CPE-based solutions by enabling service providers to better leverage both time-to-market and time-to-scale variables.

Overall, carriers who support an expanding IP VPN market through network-based solutions will also enjoy the luxury of watching their margins rise with the addition of each new customer. Some of the newest network-based solutions are not only capable of attracting a large customer base with a myriad of service options, but these solutions also excel in providing greater aggregation densities, smoother scalability, and new service creation all on the same platform.

## Summary

Today's service providers are facing an increasingly agile and aggressive environment. The enterprise is smaller, faster, more specialized, and more concerned about time-to-market than ever before. As a result, they require vendors and partners who are able to operate and deliver under a similar business model. Slower service providers who lag behind the frontline requirements of today's market will find it increasingly difficult to establish the kind of value-added partner relationships sought by modern customers in their vendor arrangements.

In light of these changing business trends, the IP VPN has gained considerable traction in the market. However, like public Internet access, frame relay, and ATM services before it, the IP VPN will also eventually become a commodity transport in its basic format. But IP VPNs are also well positioned as the launching pad for the value-added services that will be required by tomorrow's enterprise. The IP VPN of tomorrow is therefore one that is capable of being seamlessly integrated with the delivery of even higher-value solutions that will leverage its features and functionality.

Today, service providers are faced with the question of exactly how they should address swelling demands for IP VPNs. Specifically, questions still linger about whether or not CPE-based or network-based solutions are better. During the nascent stage of the market, when only truly innovative and/or desperate customers ventured toward IP VPN solutions, CPE-based solutions offered service providers the best mix of time-to-market and profitability scales they needed for such small volumes. However, with the market now facing exponential growth projections for IP VPNs, piecemeal CPE-based solutions no longer appear to be the most financially sensible strategy for service providers to pursue. In light of this fact, carriers should begin studying the risks and rewards of network-based solutions as soon as possible. Service providers should be especially focused on learning how such networks could potentially impact their own market position before customers and competitors race ahead and discover the answer without them.

**Celox Networks, Inc.**  
**Two Park Central Drive**  
**Southborough, MA 01772**  
**508.305.7000**  
**508.305.7003**  
**[www.celoxnetworks.com](http://www.celoxnetworks.com)**

**TeleChoice, Inc.**  
**1307 S. Boulder Ave., Suite 120**  
**Tulsa, OK 74119**  
**918.382.0007**  
**918.382.0033**  
**[www.telechoice.com](http://www.telechoice.com)**