Asia/Pacific Headquarters: 80 Anson Road, #38-00 Singapore 079907 P.65.6226.0330 www.idc.com

WHITE PAPER

Regional IP VPN Services: A Strategic Proposition for Greater China Enterprises

Sponsored by: DYXnet

Sherlin Pang Adrian Dominic Ho

November 2010

IN THIS WHITE PAPER

With the rising adoption of bandwidth-hungry applications as well as today's increasingly geographically dispersed and mobile workforce, IP VPNs provide significant benefits and opportunities to service providers and enterprises facing network-related challenges. Drawing on a custom survey commissioned by DYXnet to understand the requirements of enterprises with IT decision-making responsibilities and operations in Greater China, this IDC White Paper provides insights into the key factors when selecting a regional service provider, as well as their usage experience. The survey found that what respondents liked most about their main cross-regional IP VPN provider were their competitive prices and reliability. This paper also features three case studies on how Guess, "K" Line and ASUSTek Computer have benefited from using DYXnet's regional IP VPN services, and outlines the key considerations for enterprises when choosing network providers in the region.

SITUATION OVERVIEW

Rapid Take-Up of IP VPN in Asia/Pacific

The Asia/Pacific region has seen a sharp and speedy recovery from the last global economic crisis, with many countries in the region reporting solid growth. Reflecting positive business sentiments, organizations, especially the global multinational corporations (MNCs), have begun to reinstate their investment dollars in the region. More Asian MNCs are also eagerly expanding their footprint to capture larger market share.

This rise in business expansion, in turn, drives network requirements in Asia/Pacific, as reflected in IP VPN revenue growth. According to IDC's *APEJ Fixed Line Telecommunications Services Tracker 2H09*, IP VPN revenue in the Asia/Pacific, excluding Japan (APEJ) region, is expected to grow at a compound annual growth rate (CAGR) of 17.8%, from US$3.55 billion in 2009 to US$8.06 billion in 2014. In the Greater China region (i.e., PRC, Taiwan and Hong Kong), IP VPN revenue is expected to grow at a CAGR of 26% during the same period.

Key Drivers for IP VPN Growth

- **Rapid regional business expansion**: The popularity of IP VPN services in Greater China is partly due to multinational corporations (MNCs), many of which have offices in Hong Kong, Taiwan or the PRC, and are expanding in the region. Global MNCs have been expanding their businesses into the PRC to take advantage of lower production costs and to tap the increasingly affluent Chinese market. Chinese MNCs are also expanding rapidly within Greater China and into other regions such as India, United States and Africa. Enterprises that are expanding geographically expect a more cost-efficient way to connect multiple sites for data sharing and communication. For enterprises with more than two sites, IP VPN services offer greater cost efficiency and flexibility for a secured network connectivity across regions and borders.

- **The rise of cloud and on-demand applications**: More organizations that were skeptical about cloud in 2009 now hold a more positive view. According to IDC's research, cloud services revenue is forecast to reach US$1.3 billion in 2010 and US$4.9 billion in 2014, registering a CAGR of 40%. With the adoption of cloud computing and on-demand applications, enterprises need network connectivity that enable them to easily scale up or scale down bandwidth anytime. IDC believes that multiprotocol label switching (MPLS)-based IP VPN will be the network of choice for enterprises as they move toward virtualization and embrace on-demand cloud services to enhance productivity and improve overall business efficiency. In addition, with network-based IP VPN, connections to enterprises' additional sites can be easily configured by the provider within its own network, reducing lead time to deployment. Hence, unlike legacy services, enterprises do not need to subscribe to large bandwidth circuits to cater to future needs since an IP VPN service enables enterprises to scale their bandwidth as they expand.

- **Voice, data and video convergence**: The emergence of IP has resulted in the convergence of voice, data, video and other emerging technologies. In the Greater China region, the growing trend of enterprises adopting IP applications such as VoIP, Web and videoconferencing has also led to the accelerated adoption of IP VPN in the region. Enterprises are beginning to embrace collaboration tools such as unified messaging, IP telephony, videoconferencing and the more immersive videoconferencing service such as telepresence to help reduce operational costs and enhance productivity. IP VPN has the needed quality-of-service (QoS) features that allow traffic prioritization on the network, ensuring low latency and packet loss which is critical for voice and video applications. For enterprises that are moving toward voice/video/data convergence applications, IP VPN provides a more cost-efficient platform to do so than any legacy services.

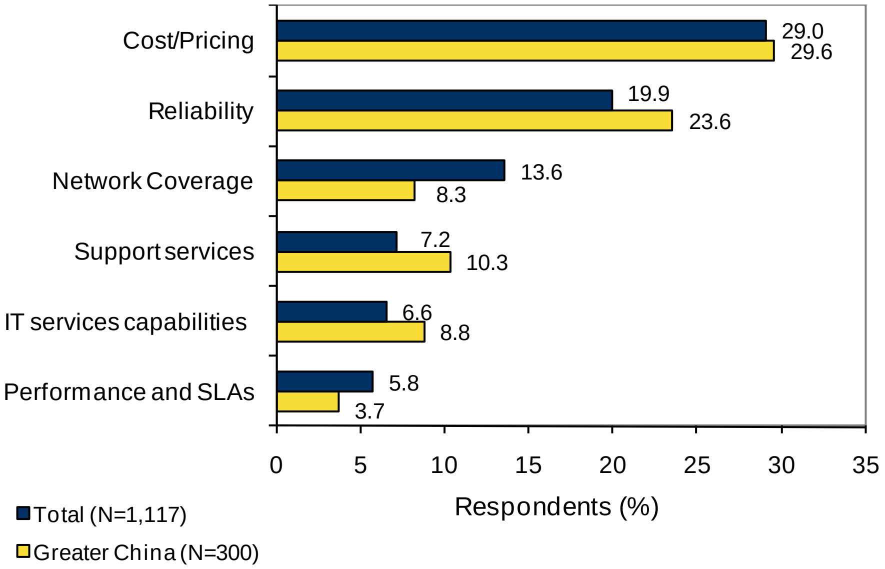
Understanding Enterprises' Selection Criteria for Telecom Service Providers

While organizations are investing once again after the global crisis, they are also prudent in their IT spending, especially after adopting aggressive cost-cutting measures in 2009. Cost/pricing remains a major concern when selecting a telecom service provider, as indicated by IDC's *APEJ Telecommunications and WAN Usage Study 2009* (see Figure 1). However, their concern over cost/pricing (29%) is not only about getting the lowest quote. IDC believes it relates to liquidity management, one of the top priorities of organizations after the crisis. Enterprises are seeking to preserve their capital for future business expansion and are less inclined to incur upfront costs on their network or IT infrastructures. With greater adoption of IP applications and, hence, higher bandwidth requirements, network expenses tend to escalate. Increasingly, enterprises prefer an opex to a capex model on network investment, where they pay a predictable monthly fee or on a usage basis.

The other key selection criterion is network reliability (19.9%). As more bandwidth-intensive IP applications sit on top of the core network and as enterprises move their business applications and infrastructure into the "cloud," network reliability becomes ever more important. Enterprises are concerned because any serious network outage can be detrimental; it can affect an organization's reputation, result in revenue loss, or pose risk to the chief technology officer's position. Note that network reliability was more important to enterprises in Greater China region than across APEJ in general. In larger countries such as the PRC and Taiwan, differing network infrastructure and technologies across provinces can lead to inconsistent network performance. This may explain why support and IT service capabilities were also important in Greater China than across APEJ.

FIGURE 1

Asia/Pacific (Excluding Japan) Top 3 Telecommunications Service Provider Selection Criteria, 2009



Note: % is based on number of responses as one respondent can give up to three responses

Source: IDC's *Asia/Pacific (Excluding Japan) Telecommunications and WAN Usage Survey, 2009*

As Network Services Become Similar, Value-Added Services Will Be the Differentiator

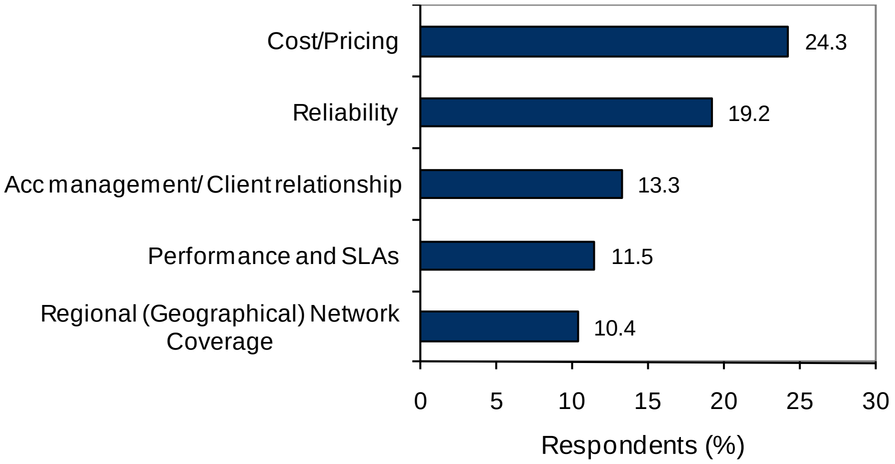
Asia/Pacific, and specifically the PRC, has been a major growth region in recent years and will continue to be the impetus of growth moving forward. As discussed earlier, both global and Asian MNCs are growing rapidly within Greater China and the Asia/Pacific region, accelerating demands for secured, reliable networks.

To further understand the usage behavior of enterprises in Greater China, IDC interviewed 100 enterprises with less than 500 office employees and have IT decision-making responsibilities and operations across Greater China. In the DYXnet-commissioned survey, IDC asked the respondents to name their primary provider for cross-regional IP VPN connectivity. DYXnet was cited by the largest number of respondents – almost one-third or 29% of the survey pool.

IDC asked a further question on the top three factors that enterprises liked about their main cross-regional service provider. Cost/pricing, reliability, and account management/client relationships took the top spots, as shown in Figure 2.

FIGURE 2

Top 3 Attributes Enterprises Like About Their Main Cross Regional IP VPN Providers



Note 1: % is based on the number of responses as one respondent can give up to three responses.

N = 272 total responses

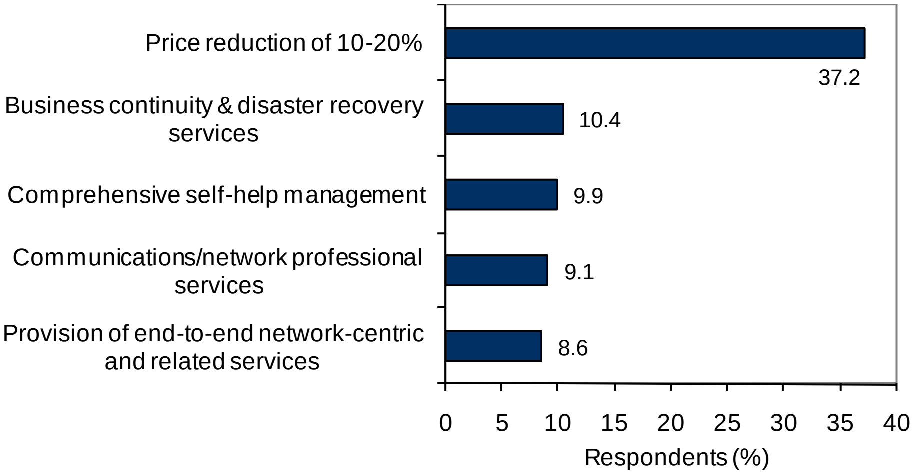
Note 2: responses less than 10% are not listed here.

Source: IDC's *IP VPN Survey 2010*, Sponsored by DYXnet

However, enterprises are also constantly in search for better deals to stretch their IT budget; a price reduction offered by another provider may, therefore, entice them to switch providers. The survey results indicated that as many as 37.2% of the enterprises surveyed would switch providers if the competitor offered a 10% to 20% price reduction from their current contract, as shown in Figure 3.

FIGURE 3

Top 3 Reasons Enterprises Would Churn



Note: % is based on number of responses as one respondent can give up to three responses.
N= 258 total responses

Source: IDC's IP VPN Survey 2010, Sponsored by DYXnet

With improved network infrastructures and technologies, the level of quality and reliability for connectivity services are becoming similar across providers. Enterprises that only purchase "plain vanilla" connectivity services will tend to take cost/price as their key decision criterion. In order to reduce churn and gain market share, providers should build up and offer complementary services on top of their network services to differentiate themselves. These complementary services include managed security services, WAN optimization, UC&C, cloud computing, and professional services.

FUTURE OUTLOOK

VPN has been the preferred method for wide area network (WAN) connectivity involving multiple sites due to its cost effectiveness over legacy services while, at the same time, providing secured access to an organization's network. There are two main protocols of VPN that have gained popularity over the past years: IPSec and MPLS VPN. Of the two, MPLS VPN has been greatly adopted by expanding organizations because of its scalability to support a wider range of VPN deployments, end-to-end QoS and provide greater security as the service is provided over the provider's own network. Below are some of the key developments in the MPLS VPN space and essential guidance for enterprises when choosing between different network services for their IP VPN needs:

- **Growth in Ethernet-over-MPLS VPN service**: Due to its inherent nature (i.e., scalable, ubiquitous, easy to manage, cost effectiveness and IT managers' familiarity of Ethernet technology), Ethernet service as LAN/WAN connectivity has been catching on fast in the enterprise market. Ethernet-over-MPLS VPN (generally known as virtual private LAN service or VPLS) offers the benefits of an MPLS network and gives enterprises full control over their IP routing. Enterprises can take advantage of both MPLS VPN and VPLS for their connectivity needs. Enterprises should ensure that their service provider has a suite of MPLS VPN services to meet their diverse needs such as VPLS for high-speed data center-to-data center connectivity, or transmission of critical applications that require in-house IP routing control and MPLS VPN for fully managed connectivity to multiple sites across region.

- **Emergence of cloud services and increased adoption of IP applications**: With cloud computing the latest industry buzzword, almost every IT manager is looking at how cloud computing can benefit the enterprise. The adoption of cloud computing requires the network to be scalable, reliable, resilient as well as secured. In addition, expanding enterprises are adopting various network-based applications such as VoIP, remote application access, and UC&C to improve productivity, business-to-business/customer relations and streamline operational costs. MPLS VPN remains the foundational platform for the deployment of cloud computing and IP applications. Enterprises that have plans to deploy cloud services and converge voice, data and video traffic onto a single network, should consider migrating their legacy services to the MPLS VPN platform. They should select a provider that not only provides good MPLS connectivity but also has experience integrating cloud services and IP applications into the network.

- **Enterprises looking to outsource or outtask their network management**: The WAN is becoming more complex and difficult to manage as business units layer more bandwidth-intensive business applications onto the core network. Enterprises are resorting to outsourcing the maintenance and management of their WAN network to IT/network providers so as to reduce operational costs and focus on their core business. Enterprises that are on the MPLS VPN network will find it easier to outsource or outtask network management to a third party, as MPLS VPN can be fully managed outside the customer's premise.

PROFILE OF DYXNET

"Dynamic" would be an appropriate phase to describe DYXnet. Founded just a decade ago, DYXnet (www.dyxnet.com) has risen to become a leading information and communications technology (ICT) service provider in Greater China. This can be attributed to its laser-sharp focus in providing MPLS VPN connectivity to enterprises within the Greater China region. To date, DYXnet is the only Sino-foreign joint venture in China that has license to operate IP contact centers, Internet datacenters (iDCs) and MPLS VPN services in this largely regulated country. The company has six iDCs located in Hong Kong, Beijing, Shanghai and Taipei as well as four IP contact centers in Beijing, Shanghai and Guangzhou.

In the past 4-5 years, the company has expanded its service portfolio by offering a range of ICT solutions for enterprises. DYXnet has also recorded several achievements. It is said to be the first ICT service provider in Greater China to achieve the Cisco Premier Partner and Cisco Express Unified Communications certification; the first provider to launch UC solutions; and the first provider in Hong Kong to obtain the ISO20000 and ISO9001 certifications.

In terms of its network service portfolio, the company is focused on providing MPLS VPN services to enterprises, with a full array of cross-border MPLS VPN connectivity services under the brand name, "ONE VPN." Within the fully-managed DYXnet ONE VPN portfolio are ONE VPN Enterprise, ONE VPN Corporate Plus and ONE VPN Corporate, which offer various class of service (CoS) and cost structures suited for different corporate needs. There is also the ONE VPN Retail service which caters to the needs of retail/logistics businesses in Greater China, as well as the newly launched ONE VPN Ethernet, a Layer 2, point-to-point or point-to-multipoint VPLS, for enterprises that want to maintain control over their network routing. DYXnet's other offerings include Internet access, hosting service, content distribution, unified communication services, network security and contact center outsourcing solutions.

The company currently has POPs in 37 major cities in Asia (PRC, Hong Kong, Taiwan, Vietnam and Singapore) serving over 2,500 enterprise clients across the regions such as Guess Inc, McDonald's, Hitachi, Shell, "K" Line, P&G, HTC, ASUS, and BenQ. Of the 37 POPs, about 28 are within the PRC, mainly in the southern and eastern parts of China. DYXnet has about 400 employees, largely in providing network engineering support, logistics and onsite support in Hong Kong, China and Taiwan. It also has more than 1,300 IP contact center staff catering to the contact center outsourcing needs of its enterprise customers.

DYXnet has a clear strategy in the Greater China region, especially in providing MPLS VPN connectivity into the PRC. DYXnet believes its current 28 POPs are sufficient to serve the regional connectivity needs of its Hong Kong/Taiwan clients in the PRC, but it does not plan to stop there. The company's ambition is to be the largest network provider in the PRC and will continue to build presence within the country. With this high call ambition, the company will, in the next 24 months, expand its VPN network from the present 28 POPs to 40-45 POPs, all within the PRC. The new POPs will be located mostly in the north eastern part of China and capital cities of its Northwest provinces. With this expansion, DYXnet will have MPLS VPN connectivity coverage to almost every part of China.

DYXnet has been targeting global enterprises requiring network connectivity from Taiwan and Hong Kong into the PRC. While the company continues to focus on these clients, it is also expanding its strategy to target the domestic Chinese companies, especially in the logistics and retail verticals. It will offer different access options to cater to varying requirements (such as VPLS for customers requiring low latency services and control over IP routing, or ADSL over MPLS for the retail sector requiring lower per-site network cost). With a strong focus on the PRC moving forward, DYXnet is well-positioned to help address the connectivity needs of enterprises – both in the country and within the Greater China region.

CASE STUDIES

Case Study: Guess Inc

Guess Inc. is a globally recognized brand name in the fashion industry with offices across almost every market including Asia. Three years ago, it made inroads into Greater China, rapidly expanding its operations within the region. Today, the company has 70 to 80 retail branches in Beijing and Shanghai, with its regional office in Hong Kong. Within the PRC, it has two offices, one in Beijing and the other in Shanghai with a datacenter and a warehouse located in Shanghai.

Challenges

When Guess first started operations in the Greater China region, all network connectivity between the various sites within the PRC and into Hong Kong was via IPSec, a protocol used to secure IP traffic before it passes through the public Internet. However, as data was transmitted over the public Internet, Guess experienced network performance inconsistency and high latency issue, especially between offices in the PRC and Hong Kong or the rest of the world.

Solution

About two years ago, Guess decided to move some of its network connections to the MPLS VPN service to solve its network latency issue. According to Mr. Stanley Au, a Guess spokesperson, the company considered two MPLS VPN service providers during their selection process: DYXnet and another major provider in Hong Kong. During the evaluation process, DYXnet stood out, partly due to its good coverage between Hong Kong and the PRC. But, according to Guess, the main differentiator was DYXnet's competitive pricing.

The company has since subscribed to DYXnet's MPLS VPN service for secured, dedicated connections between its datacenter and warehouse in Shanghai as well as to its regional headquarters in Hong Kong. According to Guess, the company has greatly improved its network performance between the PRC and Hong Kong and has not experienced any major latency issue since it implemented the service.

Case Study: "K" Line

Kawasaki Kisen Kaisha Ltd ("K" Line) is a global transportation company offering liner services with offices across Asia. Within the Greater China region, the company has 20 offices across South and North China, and Hong Kong as the head office connecting to its head offices in United States and Japan. "K" Line's network infrastructure across Greater China is centralized in Hong Kong, and the MPLS VPN connects its 20 offices.

Challenges

According to Mr. Dennis Tsui, Senior Manager of IT, the company had been using CPCNet's MPLS VPN network to connect all 20 offices within the Greater China region for five years, and the company was satisfied with the provider's network service delivery. However, with continued business expansion within China and increasing bandwidth needs, "K" Line experienced escalating network cost across the offices. During its yearly contractual review with CPCNet, cost/pricing was its top priority and despite some price revision during the contract renewal, "K" Line felt that further price reduction could be achieved. However, as the company has numerous sites within the Greater China region, it was also apprehensive about switching providers and did not want to risk any network reliability issues or incur high re-installation costs.

Solution

In 2008, faced with escalating network costs, "K" Line began to source for an alternative provider that could meet its price and network requirements. A number of MPLS providers were evaluated, including DYXnet. Other than cost, "K" Line also considered the provider's MPLS coverage in China and if the provider had a well-established structure. After a long evaluation process, the company decided to fully migrate its MPLS VPN network to DYXnet in 2009. "K" Line told IDC that a total migration was not an easy decision and DYXnet met all its requirements. These included DYXnet's receptiveness to meet its price requirements in South China and Hong Kong, as well as a different pricing requirement for North China's offices, and absorbing a portion of the installation cost of equipment. In addition, DYXnet's willingness to work with the company's global provider, NTT Com, to ensure good network performance outside Greater China was a plus point. "K" Line has been satisfied with DYXnet in the whole network migration process. With the migration, "K" Line experienced 12% savings on its yearly network cost. Other than the MPLS VPN services, the company also subscribes to DYXnet's ADSL (as a backup service) and network security services.

Case Study: ASUSTek Computer Inc

ASUSTek Computer Inc., commonly known as "ASUS," is a well-known global technology brand that manufactures and sells motherboards, notebook computers and computer accessories. Incorporated in Taiwan, the company has presence across the globe in Asia, Europe and the United States.

Within the Greater China region, the company has more than 20 branches including four offices in Taipei, Shanghai, Suzhou and Hangzhou, which serve as their main traffic centers or data warehouses.

Challenges

With multiple branches and traffic centers across the region, ASUS needs secured network connectivity across these sites, which makes network costs a concern. According to Mr Curtis Chang, Senior Engineer of IT, as the company expands and begins to adopt IP-based applications such as video/voice conferencing and other collaborative tools in the near future, there are also concerns over escalating bandwidth and hardware costs arising from supporting these bandwidth-intensive applications. Besides controlling network costs, ensuring business continuity and maintaining network redundancy across the various sites are also top on the company's agenda.

Solution

Since the establishment of the traffic centers five years ago, ASUS has been subscribing to MPLS VPN services from DYXnet for connectivity services between its four offices. All other branches within the PRC and Taiwan are connected to the four centers via IPSec. To reduce network costs, all other branches within the PRC and Taiwan are connected to the four centers via IPSec. Since subscribing to DYXnet's MPLS VPN services, ASUS has been highly satisfied with its network service. On the company's plans to adopt IP-based applications over the network in the near future, Mr Chang says ASUS hopes to continue its partnership with DYXnet for the provision of a stable network backbone while keeping its IT budget under control.

CHALLENGES

The network is the bloodline of any enterprise. Service providers need to ensure the customer's network is always available, especially for the transmission of mission-critical applications. Providing consistent network performance across the Greater China region can be a daunting task due to the differences in network infrastructures used by local providers across provinces. In addition, enterprises require their provider to manage their network from end to end, ensuring high service availability and performance. In the PRC, due to regulatory constraints, foreign providers can only build their own POPs in major cities like Beijing, Shenzhen, and Guangzhou through partnerships with local providers, mainly China Telecom and China Unicom. For extended in-country coverage, MPLS network-to-network interfaces (NNIs) with local providers are established. Network availability will have to depend on the local provider's network, of which foreign provider has minimal control. To this end, DYXnet is at an advantaged position. It has been granted the nationwide IP VPN license in the PRC, allowing it to offer MPLS VPN services throughout the country. By building its own POPs, the provider is able to provide higher network quality assurance.

Other than network reliability and coverage, enterprises are also demanding service providers to have good service support and IT service capabilities. In large countries such as the PRC, a team of local technical expertise should be available to support enterprises' network needs for faster time-to-response/restore. DYXnet currently has about 200 staff providing onsite support in Greater China and a 24 x 7 technical support center in Hong Kong. With its expanding footprint into the north eastern and western parts of China in the next 24 months, the provider will need to build up its local support team to provide onsite technical support in these areas. In addition, enterprises are also expecting service providers to offer complete ICT solutions with a range of connectivity and managed services including cloud computing and professional IT services. With limited managed service capabilities, this could be a challenge for DYXnet to service enterprises requiring beyond managed network services. In terms of capturing new market opportunities, DYXnet recently launched a Cloud Dedicated Hosting (CDH) Service in the Greater China region for the SME market in partnership with Dell and VMware. This Infrastructure-as-a-Service (IaaS) cloud service offers SMEs flexibility on platform options, computing, storage, and bandwidth, enabling SMEs to cut costs and, at the same time, improve productivity.

DYXnet's ambition to be the largest value-added network service provider in the PRC could be challenged as the major local players, realizing that mobile growth is slowing down, have also signaled their ambitions to grow their businesses in the enterprise space, targeting both MNCs and SMEs. The current local players already have wide network coverage in the PRC as well as connectivity outside the country. With coverage largely limited to Greater China, the challenge for DYXnet is in its ability to continue serving those Chinese enterprises as they move out of the region and require connectivity beyond Greater China. These enterprises may eventually source for another provider that has deep NNI arrangements with the two incumbents as well as good global coverage.

CONCLUSION

As MNCs and enterprises expand their presence in Asia, and specifically into the Greater China region, they expect service providers to have good network coverage and reliable service to seamlessly connect their headquarters and branch offices across the region. MPLS VPN services have gained popularity among enterprises because of the many benefits compared to legacy services. These include scalability, cost effectiveness to link multiple sites, reliability, secured network and QoS features. MPLS is also a fundamental platform for the deployment of virtualization technology and cloud services. When selecting a cross-regional network provider in Greater China, enterprises should consider the provider's ability to deploy their own MPLS POPs within the countries and provide onsite support as this ensures greater network quality control and service support. To that end, IDC believes DYXnet is well positioned to help MNCs and enterprises meet their business requirements.

METHODOLOGY

This IDC White Paper draws on research insights from IDC's yearly APEJ Telecommunications and WAN Usage survey, a custom survey commissioned by DYXnet, and secondary research on the IP VPN market. IDC's custom IP VPN survey was administered over the phone in February 2010 among 100 enterprises with IT decision-making responsibilities and operations across the Greater China region. The featured case studies were based on in-depth interviews with DYXnet customers, Guess, "K" Line and ASUS. The objective of the case studies was to gain a better understanding of the end-user's experience in using cross-regional MPLS VPN services offered by DYXnet.

Copyright Notice