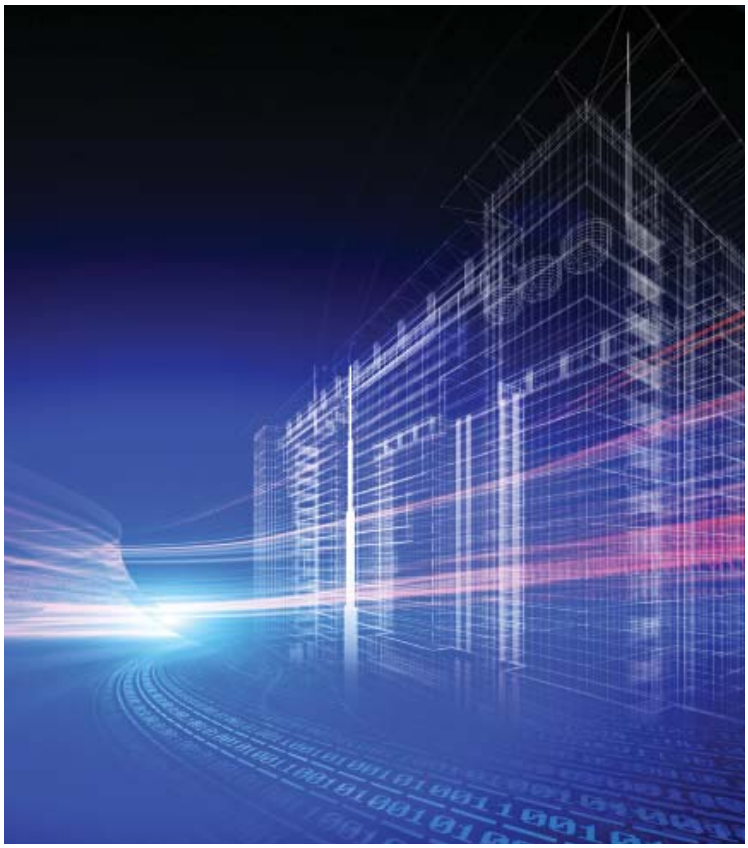
SUBISU NEWSLETTER
Vol. 1, Issue 4, MAY - JULY 2016

HIGHLIGHTS

MPLS Deployment



Subisu has been adapting new technology and is upgrading its network to cater its customers with better quality service. In this step of optimization, Subisu has deployed MPLS technology at many of our Point of Presence (PoP's) and is on process of continues deployment of MPLS technology at further more regions. Current deployment is being done at 60 PoP's all over Nepal. Following points elaborate the advantage of MPLS:

MPLS Advantages

1. Faster Speed: Due to the labeling technology, the speed of performing lookups for destinations and routing is much faster than the standard IP table lookups non-MPLS routers have to perform.
2. QoS: This is a big one. MPLS networks achieve greater Quality of Service for their customers. Quality of Service (QoS) means exactly that – you can expect a higher standard of service such as reliability, speed, and voice quality. This is for a few reasons, one already mentioned above.
3. In addition, MPLS networks are able to assign priorities to the different packets based on what the labels say about that packet. Packets with greater priority, voice over data for example, are given more bandwidth allocation. A packet that which is not deemed as high priority is given less. Obviously sending documents online don't need to be assured of the same bandwidth required for someone who is wanting to have a conversation.
4. Faster Restoration: MPLS networks are also able to restore interrupted connections at a faster speed than typical networks. Obviously, this is a benefit.
5. Security: MPLS offers greater security and are often required for companies which need enhanced privacy and security for their network needs. Some industries like the Health Care and Financial industries are examples of industries mandated by Federal law to comply to specific requirements for network security.
6. 24/7 Monitoring: Another benefit of MPLS is that the network is pro-actively monitored and managed at all times ensuring the extreme reliability and security.
7. Outsourced routing. With MPLS, the carrier handles WAN routing. This means users don't have to, which makes MPLS operationally simpler than managing a large routed network. This means, in turn, that companies can keep fewer WAN/router engineers on staff.

Hotel Annapurna partnered with Subisu for Clear TV Service

Nepal's premium 5 Star deluxe Hotel Annapurna has partnered with Subisu to provide the "Clear TV"service to its valued customers.

Mr. Abhinav Rana, GM of Hotel Annapurna and Mr. Binaya Mohan Saud, CEO of Subisu Cablenet (P.) Ltd jointly signed an agreement for the purpose. With this agreement, all the rooms of the hotels are now equipped with Subisu's premium Digital TV Service-Clear TV where Customers can experience digital contents in High Definition channels.

According to Mr. Abhinav Rana, GM, Hotel Annapurna, "Digital TV service has helped us offering the best TV viewing experience to our customers which is the need of the hour. Our partnership has delivered state-of-the-art entertainment to our esteemed customers providing TV & In-house Video Contents in High Definition (HD)".

CEO of Subisu, Mr. Binaya M. Saud says, "We are aware of the demands for better service and our Clear TV service is well placed to meet those expectations".

Nepal Government will be making Digital TV compulsory in all major cities from Magh 2073, whereby, currently available Analog TV signal will be switched off.

"Clear TV Cheer Up Euro 2016" Celebration

Subisu had brought an exciting offer on its Clear TV service targeting the much loved European Football Championship around the world: UEFA Euro Cup 2016.

Company had introduced Euro offer targeting the football lovers so that they could enjoy supporting their favorite team experiencing digital content of Clear TV Service.

Under the scheme "Clear TV Cheer Up Euro 2016", on purchase of Clear TV Package at Rs. 2999, subscribers were entitled to get Free Clear TV HD Set Top Box, 2 months subscription of premium package (30+HD and 100+SD channels) and onetime service installation & set up services.

TOP STORIES ▸▸▸

Dhalkebar-Janakpur Fiber Redundancy:

Understanding the value and need of dedicated service Subisu has optimized its existing network at Dhalkhebar –Janakpur region. Subisu has upgraded redundancy of the area by expanding the secondary network link via fiber connection at Dhalkebar-Janakpur.

Pokhara-Kusma-Baglung NEA:

Subisu has taken serious note of recent problem faced by customer at Kusma and Baglung area by upgrading the link via NEA fiber. Existing link will be upgraded via NEA fiber from Pokhara to Kusma and Baglung. Further network expansion is being planned to strengthen the link.

New Sales Outlet "Subisu Station "in Sukedhara, Kathmandu

Subisu had launched its new sales outlet "Subisu Station" in Sukhedhara, Kathmandu. Company's CEO, Mr. Binaya Mohan Saud inaugurated the outlet.

Through this Station, Subisu aims to facilitate its customers who live nearby, providing necessary retail based services information, new connections and after sales support in a convenient manner. Subisu aims to cater better pre- sales and post sales services to its valued customers through its competent and experience staffs.

Till current date, Subisu has successfully established its outlets, "Subisu Stations" in major streets of Kathmandu valley: Jhamsikhel-Lalitpur, Samakhushi-Ranibari and Sukedhara-Kathmandu and is continually planning to open more of such stations in more places in the days to come.

VARIETIES ▸▸▸

The Cyber Threat to Banking

In the last 10 years, digital technology has revolutionized economic and social interaction. It has transformed the way we do business, the way we educate ourselves, the way we sell and buy products and the way we share data. Internet use is growing and the methods by which it is accessed are diversifying. Malicious cyber actors are fully aware of this revolution and are taking full advantage of it. Firms have indicated that 2013saw an exponential increase in cyber-attacks and a recent PwC survey demonstrates that 93 per cent of large organizations last year suffered a security breach.

Defending and countering cyber-attacks whilst keeping up to date with evolving regulations and policy is a complex challenge. Coupled with changing business requirements, speed to market pressures, expansion into emerging markets, business innovation requirements and budget cuts, the challenge for managing cyber risk is significant. Firms are already investing heavily in cyber security. A recent BIS paper indicates that the UK financial sector is already spending over £700 million annually. The issue is also being managed at board level, with 86 per cent of banking and capital market CEOs identifying technological advances as the trend that will have greatest impact on their businesses.

e-Economic effects of cyber-attacks can reach far beyond simply the loss of financial assets or intellectual property. There are costs associated with loss of client confidence, the opportunity costs of service disruptions, "cleaning up" after cyber incidents and the cost of increased cyber security. More and more, damage to brand and reputation in the Aftermath of an attack is perceived as a critical risk to firms. In addition, as a key enabler of economic and social development, the banking sector needs to think about the critical infrastructure nature of its operations. Nearly 60 per cent of firms identify the speed of technological change as a threat to their growth prospects.

Cyber threat actors have a global reach and cyber threat mitigation strategies need to be considered through a global lens. Additionally firm's cyber responsibilities are often split between different departments and this can cause difficulties in not only understanding and prioritizing threats but responding to them. More widely the financial sector interconnects endless means that successful attacks on smaller firms or third party supply chains can significantly affect the wider market. Vendors, suppliers, customers and our colleagues are all critical components of a successful business, but come with risks, and successful attacks against these often perceived weaker links will have an indirect impact. The supply chain threat has most recently been demonstrated through the high-profile Target data breach and the identification of the Heart bleed vulnerability. Both examples illustrate the indirect impact of cyber incidents on banks. More than 70 percent of banking and capital market CEOs identify cyber insecurity as a threat to their growth prospects.

COMMON TOOLS AND TECHNIQUES

Malware

The development and deployment of financial Trojan malware is a key threat. The credentials harvested from customers and banks compromised IT systems are subsequently used for fraud. Financial Trojans of particular concern over the last 12-months continue to be variants of Zeus. The online availability of Trojan source code is a significant risk and the release of the Carberp source code in June 2013 could spawn an increase in variants for sale on criminal forums, as occurred when the Zeus code was released
in 2011. Point of sale and mobile malware attacks are causing increasing concern to banks, especially when criminals chase higher returns by targeting high-value accounts held by corporate or business clients.

Social engineering

Due to the improvements in online authentication methods, such as two-factor or out-of-channel, malware campaigns are increasingly paired with social engineering tactics, commonly through voice or email (vishing and phishing).14 Social engineering is still generally targeted at customers, although there have been examples of criminals targeting bank employees directly utilizing their online accesses or by tricking them into installing physical devices to networks. Firms also need to be vigilant when engaging incorporate social media, information derived from these open channels can be used by criminals looking to gain a foothold within companies.

Deployment techniques

The deployment of malware is optimized through the use of exploit kits. The exploit kits automate the process of identifying vulnerabilities in victims' web browsers and plug-ins (notably java and adobe) to enable the installation of malware. Less technical methods such as email, online adverts and social media are also being used to deliver malware directly (e.g. via attachments) or indirectly (e.g. through hyperlinks to compromised websites).

Botnets

Botnets provide the industrial scale of much of the online fraud threat. Botnets are versatile tools that are created through the successful deployment of malware, once established botnets can facilitate further Infections, denial of service attacks and anonymisation of criminal activities. Spam botnets are a global problem and often perceived as a mere nuisance. However, they are increasingly being used to facilitate malware deployment directly (i.e. via attachments). Customer confidence and bank reputation in delivering online services can be damaged from spam campaigns, so their threat should not be underestimated. Firms have observed that spam is becoming increasingly difficult to detect as not only are the emails well-crafted but the sender address often spoofed from familiar contact to make it appear even more legitimate.

Source-PwC 2013 Information Security Breach Survey