

Trend

State of Wi-Fi in the Indian enterprise

With the explosive growth and widespread availability of wireless networking products and services, substantial challenges lie ahead for enterprise network admins. *By Manjari Juneja*

The Indian Wireless LAN (WLAN) equipment market has evolved rapidly. From the provisioning of public hot spots to enterprise deployment, interest in deploying WLAN has been rising continuously.

Suresh Balasubramanian, National Sales Director, Cisco Consumer Products, India, said, "India is at the forefront of adopting new wireless technologies, largely fuelled by the rapid growth in broadband penetration. Consumers are demanding more from their networks due to the increase in shared content, online gaming and media downloads. Clearly, the growth rates in Tier 2, 3, and 4 locations are higher than in traditional metro locations."

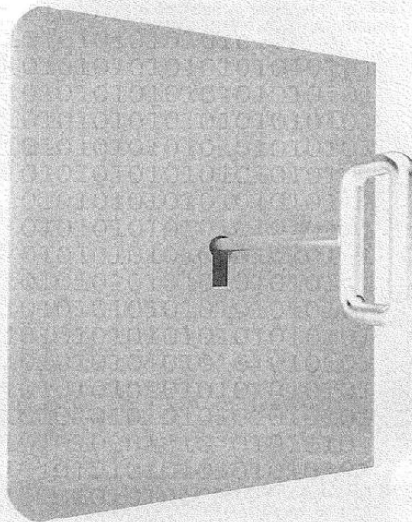
Ashok Saraf, Product Marketing Manager - Wireless, Extreme Networks Inc. USA, said, "Wireless LAN delivers the most cost-effective network access solution. A mobile workforce is more productive resulting in a lower operating cost for the enterprise. Customers can deploy value-added mobility applications over a wireless network without additional capital investment in network infrastructure."

The WLAN market

Wireless Networking is catching on fast in India. The growth momentum is expected to continue in 2010-11 with approximately 20% growth in the current fiscal.

The ratification of the 802.11n standard has fuelled demand for wireless products. 802.11n offers up to six times the throughput when compared to existing 802.11a/g networks. N standard based solutions empower network administrators to have better control, security, redundancy, and reliability to scale and manage their wireless networks easily and efficiently. Unified Access Points supporting 802.11n can be flexibly deployed as standalone wireless access points or as thin managed access points manageable from a wireless switch. Demand has been generated from educational campuses, manufacturing, hospitality, consumers, government etc.

Mouli Sankaran, Technical Director, Networking Components Division (NCD), LSI India Research & Development Pvt. Ltd., said, "With the current wireless teledensity of 52% in India, there is a huge market that needs to be tapped. With the introduction of 3G, demand for networking products to support demands on the



backbone networks would also increase exponentially. The adoption of 4G technologies in the future, both WiMAX and LTE, are going to drive sales of wireless equipment in India."

Major trends

A wireless network is no longer a nice-to-have service for enterprises. An up to 83% increase in the average number of access points over the next two years is projected.

Prem Nithin, (CISSP, CISA), Information Security Specialist, Cisco, said, "Early deployments tended to be limited in their scope but, increasingly, the trend is to create pervasive deployments as companies experience the benefits of mobility and realize its profound impact on productivity and customer and partner satisfaction. Changing employee demographics are also fueling this trend, as a new generation of workers who expect instant connectivity anytime and anywhere join the workforce."

The latest trend is in terms of commercialization of high speed and resilient 802.11n wireless LAN technology which will accelerate the adoption of WLAN by enterprises. It becomes a viable alternative to 10/100 Mbps wired access. The integration of wired and wireless edge with unified service and policy management would help simplify network deployment and management. Advances in radio and client management would enable better utilization of radio resources, optimize performance and enhance the user experience.

Mohit Anand, Managing Director, India Subcontinent, Belkin India, said, "India's wireless market is a test bed for alternative infrastructure, handsets, billing systems, business models and marketing strategies that will likely prove applicable to other developing countries. Wireless technology is clearly the future of networking."

Challenges for enterprise networks

Enterprise networks stand to gain with explosive growth happening in the wireless and backhaul transport networks in India. Bandwidth requirements on the WAN infrastructure that enterprises depend upon are increasing with their increased dependence and adoption of cloud computing and virtual private data centers.

Currently, wireless LAN is deployed as an overlay over a wired infrastructure. With widespread deployment, wireless LAN becomes a strategic corporate resource. Customers would need to develop a set of best practices for the design, deployment and operation of their wireless networks. Scalability, manageability along with security would be the major challenges. Unified wired and wireless access at the edge with common user and network policies would simplify deployment and management. With a greater than six-fold increase in wireless traffic, switching wireless traffic at the edge helps improve network performance and avoids the expenditure of re-engineering the core network. A unified management platform for wired and wireless services simplifies network operation, reduces IT overhead and improves IT response time.

Jayesh Kotak, VP - Product Marketing, D-Link (India) Ltd., said, "A mobile workforce and Wi-Fi environments are common these days. On the one hand, these trends support businesses and, on the



Vishal Dhupar,
MD, Symantec India

Whether it is the smartphone or a laptop, enterprises today need to take the same information-centric approach as they would with other endpoints—a risk-based proactive approach to security. This means that they should define clear-cut policies for the use of these devices within the enterprise



Jayesh Kotak,
VP - Product Marketing, D-Link (India) Ltd.

Regarding wireless threats, the first concern is that of uncontrolled wireless devices inside a network and the second is that of wireless attackers. Therefore, it is essential that IT managers move to an architecture that provides a single point of management control



Prem Nithin, (CISSP, CISA), Information Security Specialist, Cisco

The trend is to create pervasive deployments as companies experience the benefits of mobility and realize its profound impact on productivity and customer and partner satisfaction. A new generation of workers expect instant connectivity anytime, anywhere



Kartik Shahani, Country Manager, India and SAARC, RSA

Security solutions must be information- and transaction-centric versus perimeter-centric. Given the rapid proliferation of malware and attacks, and the increasingly dynamic nature of IT infrastructure, our solutions must take into account facts and circumstances that can be correlated to better mitigate risk

other, they pose a high security vulnerability. With mission-critical applications running on networks, protection against exploitation of network-attached resources is now an area of concern for many businesses. IT managers and administrators are constantly faced with two types of wireless threats. The first concern is that of uncontrolled wireless devices inside a network and the second is that of wireless attackers. Therefore, it is essential that IT managers move to an architecture that provides a single point of management control."

Wireless LAN deployments have evolved from workgroups to campus-wide networks. To manage these larger-scale installations, enterprises have shifted from standalone intelligent access points to centralized wireless LAN controller solutions (sometimes referred to as wireless switches) to simplify configuration and management. An important optimization issue in such an integrated system is how to minimize the overall communication cost by intelligently utilizing the available heterogeneous wireless technologies while, at the same time, meeting the quality-of-service requirements of users.

Limiting usage

IT departments are busy drawing up policies and implementing them to restrict usage of the Internet by employees to ensure that social networking and other unwanted downloads don't hog their network resources. To this end, they need to implement access control mechanisms to ensure that client devices comply with corporate security policies before they are allowed access to the network. This includes client device integrity check and mechanisms to automatically configure a device over the network to match the access policy established for the user and the device. Identity management with location attributes ensures that access policies follow the user across the enterprise. User identity, location-based access control, wired port access control and time of day access control are all used to limit usage.

Vishal Dhupar, MD, Symantec India, said, "Over a third of the respondents of a survey by the Enterprise Strategy Group, commissioned by Symantec, revealed that employees with mobile devices can access, receive and store company confidential data, customer data, regulated data and intellectual property. This new found mobility coupled with the availability of sensitive information on mobile devices, makes attacks on mobile phones a serious problem. While the phenomenon of the Indian workforce going mobile or that of them accessing company information on these mobile devices is not something enterprises can always limit, securing them is possible. Whether it is the smartphone or a laptop, enterprises today need to take the same information-centric approach as they would with other endpoints—a risk-based proactive approach to

security. This means that they should define clear-cut policies for the use of these devices."

Policy is the key

The security risks of wireless technology often outweigh the benefits. Business users require secure and seamless roaming, which requires reliable mobile connections. This means that user-based policies and authentication and centralized AP coordination are a practical necessity. Moreover, technologies like Wi-Fi phones and seamless roaming, which are not just 'nice-to-have' features but rather a requirement for user satisfaction.

Network administrators need to know and control the location and identity of all users on the LAN. They need to know how many users are on a particular AP and they need the ability to examine the activity of each user when security concerns arise.

IT managers must look for a solution that provides for the management of multiple access points across the network with capabilities such as a Web-based management interface to manage all access points on a WLAN, group management capabilities, mass firmware upgrading by group, mass configuration by group including QoS settings required for VoIP, video and other high bandwidth, low latency applications, fault management, real-time monitoring and reporting. Today, newer wireless technologies and tools allow for policy-based usage as well as the tools for rogue access points to be tracked and shut down to prevent any kind of misuse.

Policies and control should be applied to any device over any network. Enterprises have many requirements around mobility initiatives. Strategic initiatives will address a broader set of mobility requirements within the organization and they represent a tighter, policy-driven approach to the management of mobile solution; and tie closely into the overall corporate business strategy.

Subhashini Prabhakar, Chief Technology Manager, Dax Networks, said, "As companies develop their plans for strategic mobility, they must consider incorporating a broader set of technologies and mobile tools to create a true mobility package for end users. This includes integration and coordination between voice, data and remote access services. Many companies have used traditional wireline remote access services for their mobile workforce, with some firms incorporating 802.11 wireless and hot spot access into these solutions."

All large and publicly traded companies have IT and security policies that they need to enforce. Policies are based on internal best practices and external regulations with implementation often driven by frameworks such as ITIL, COBIT, ISO and others. Policies are critical because they provide the basis for deciding what types of information need to be protected, in what manner, at

what cost, who has access to what information, and how long specific types of information should be retained. The challenge is to more effectively define and manage policy creation and distribution, as well as provide evidence of supporting processes that include technical and procedural controls.

Maintaining security

Enterprises need to ensure regulatory compliance by setting up a comprehensive security framework that can ensure information integrity and meet the compliance requirements of regulations such as Sarbanes-Oxley, HIPAA, and PCI.

A wireless network is vulnerable, because anyone can try to break into a network broadcasting a signal. Older WLANs employing Wired Equivalent Privacy (WEP) are vulnerable to intrusion. Wi-Fi Protected Access or WPA is a better idea. It provides greater security to wireless networks than a WEP security set up. The use of firewalls will help with security breaches which can help to fix security problems in some wireless networks that are more vulnerable.

Unsecured WLANs can be a gateway to trouble not only for enterprise resources but also for threats from virus and worm outbreaks. Organizations find themselves frequently adding equipment, relocating access points, modifying settings and upgrading firmware just to keep up with demand. The process of managing, upgrading and configuring multiple access points has become time-consuming and resource-draining.

Security can be maintained by 24x7 monitoring of network, devices and users. Enterprises should implement robust access control policies for users and devices across wired and wireless networks, intrusion detection and prevention mechanisms should be implemented to protect the network from attacks over wired and wireless networks. The highest available level of encryption should be implemented for traffic across wireless media. A unified management platform shall be able to provide audit trails and compliance reporting.

Kartik Shahani, Country Manager, India and SAARC, RSA, said, "Organizations today are realizing the need for a holistic and comprehensive approach towards security. They are not looking out for point solutions but rather for a complete strategic approach which may include multiple products and solutions. Security solutions must be information- and transaction-centric versus perimeter-centric. Given the rapid proliferation of malware and attacks and the increasingly dynamic nature of IT infrastructure, our solutions must take into account facts and circumstances that can be correlated to better mitigate risk. A good security strategy would have DLP as its core with other access and data controls supporting it. Most companies are waking to this reality today."

manjari.juneja@expressindia.com