

How Cisco IT in India Overcame Regulatory Constraints to Build an Enterprise Network

Reliable, cost-effective, high-performance network improves communications among employees and partners.

Cisco IT Case Study / Routing and Switching / Enterprise Network in India: This case study describes how Cisco IT India overcame regulatory constraints to build a highly reliable, cost-efficient, high-performance network in India that serves both Cisco employees and partners. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

“From the earliest days of Cisco’s presence in India, it has been our policy to work closely and amicably with regulatory authorities to create a reliable, cost-effective, high-performance network that enables Cisco employees and partners to perform their jobs productively.”

– Balaji V., manager, Cisco IT, APAC Network Operations

BACKGROUND

Cisco has a significant presence in India today with a comprehensive network serving more than 4500 users. This network seamlessly connects Cisco India employees and strategic partners through a high-speed WAN, VPN connections, Internet and intranet access, remote access services, and wireless LAN services to applications and individuals across India as well as San Jose, while service provider diversity and redundancy ensures maximum availability of the network.

CHALLENGE

Technologies deployed and services available in India are typical of those that users would expect to see in San Jose, Research Triangle Park (RTP), or most major Cisco locations. Unlike most other major Cisco locations, however, regulatory constraints hindered the deployment of many aspects of the current network. Cisco IT had to work closely with regulators over several years to gain reasonable relief from these restrictions.

SOLUTION

Between 2000 and 2005, Cisco India IT worked with regulators to gain approval for services in seven different technology areas, including Closed User Group, Remote Access Service, Local Internet Gateway, Wireless LAN, VPN Concentrator, Service Provider Redundancy, and Softphone Remote Access. These services are discussed in the chronological order in which they were approved by Indian regulators.

Closed User Group Approval

Cisco's first presence in India was its sales offices. Then, in 1996, Cisco established engineering operations through its partner, HCL, in Chennai, India. A second engineering partner, Wipro was added in 1998. In 1999, Cisco established its own engineering operations in Bangalore. In each instance, communications with San Jose was critical. HCL and Wipro each had direct international private line circuits (IPLCs) to San Jose. Cisco India Sales initially connected to San Jose through a Primary Rate Interface (PRI) ISDN link to Singapore until 1999 when Sales and the newly established Cisco India engineering sites deployed a single joint IPLC to San Jose. Arun Joshi, hired to manage Cisco India IT operations in 1999, reasoned that significant economies could be generated by consolidating

these individual IPLCs into a single circuit that all Cisco India and Cisco partners in India could share.

Arun Joshi approached regulators and found that companies located in India and connected to their parent company outside India cannot connect to any private or public networks (known as Closed User Groups or CUGs) within India without first seeking approval by the Department of Telecommunications (DoT), India's regulatory authority. "Connecting HCL and Wipro to the Cisco network raised issues of security, since HCL and Wipro are competitors, as well as network ownership issues, and whether Cisco was acting as a service provider," says Balaji (Bala) V., manager, Cisco IT, APAC Network Operations.

Because local regulators did not have authority to grant CUG approval, Arun Joshi had to make the trip to New Delhi, India's capital, nearly 1000 miles from Bangalore, to plead his case for CUG approval. Not until mid-2000, after several visits to New Delhi, a number of follow-up calls, and answering many questions, did Cisco India receive permission to set up the CUG. By that time, a third partner, Infosys, was brought on, which extended the approval process.

As with the initial application, each new partner subsequently added to the CUG must be approved by the DoT. Beginning in 2001, however, the local authorities in Bangalore were given the power to grant such approvals. Applications must include a detailed network diagram, partner organization information, bandwidth of the circuit, and the Cisco Network Operations Center (NOC) responsible for the circuit. "Because of the growing complexity of the CUG diagram, authorities requested that we number each circuit and supply a separate spreadsheet listing the end points of each numbered circuit," says Bala. Today, more than a half dozen partners are represented in the CUG.

Direct interconnection between the CUG network and partner networks is strictly prohibited. All partners maintain separate buildings where employees are dedicated to Cisco projects and only have access to the Cisco CUG network. Partner employees may have a need, however, to occasionally access data on the partner network, such as their own payroll information. "We had to open a few ports to the Internet to allow them that access," says Bala, "But the connection is purely logical. There is no physical connection between networks."

Today, one DS3 circuit in Bangalore connects most Cisco India employees and many of the partners (a combined 3000+ users) with San Jose. For redundancy/back-up purposes, a second DS3 circuit in Chennai at an HCL facility provides connectivity with San Jose for 1000+ users. Should the Bangalore circuit ever fail, all CUG traffic would be diverted to the Chennai circuit. Similarly, Bangalore can back up Chennai. Compared with individual IPLCs between each partner and San Jose, the CUG has enabled Cisco to save significantly on circuit costs.

Remote Access Service

There are a number of scenarios that require Cisco India employees to be able to access the Cisco network from their homes. For example, if an engineer is asked to respond during non-business hours to a major customer network problem resulting from a bug in a Cisco product, significant time might be lost before the engineer can commute from home to the office and begin working on the problem. A remote access service was essential for enabling connectivity from employees' homes. Before 2001, companies in India had two choices: subscribe to a remote access service (RAS) from the only private provider offering the service, or seek approval and pay a fee to Bharat Sanchar Nigam Limited (BSNL), the incumbent service provider, allowing Cisco to deploy its own internal RAS service. Cisco India IT considered the private provider, but their service was unreliable and very slow. In addition, the RAS service would have to be customized to match the specific network environment within Cisco India. While soft token-based authentication was widely used throughout Cisco, for example, Cisco India used a Challenge Handshake Authentication Protocol (CHAP)-based authentication method. CHAP authentication was not offered by the private provider.

Cisco India set up a pilot RAS server in Bangalore at the end of 2000 to evaluate the requirements of users and test the equipment. Five BSNL ISDN PRI (2 Mbps) circuits were installed to support the traffic. Users required an ISDN line (128 kbps) in their homes to access the RAS server.

RAS service required approval by DoT and an annual license fee per circuit, which varies per company. Once the fee was paid, Cisco received approval for RAS in January 2001. Today, 300+ users have access to the RAS service in Bangalore.

Local Internet Gateway

Cisco employees and partners need access to information available on the Internet to perform their normal business functions. Until 2003, traffic intended for the Internet was forced to traverse the Cisco WAN to the nearest Internet access connection, which was in San Jose. This resulted in significant delays in getting information, and also added extra traffic on the WAN that can delay other business traffic and drive up WAN costs as Cisco tries to maintain low trunk utilization. The best solution would be to provide a local Internet access connection in India

Cisco India IT considered deploying a local Internet gateway in Bangalore, which would divert traffic from the international WAN and reduce latency. After investigating this solution, however, Cisco found that an Internet gateway couldn't be implemented in a CUG, according to DoT regulations. "Regulators didn't want companies becoming Internet service providers for the other companies on their CUG networks," says Bala.

Cisco India IT filed an application with DoT through BSNL seeking permission to deploy an Internet gateway in Bangalore. After making its case and providing supporting documentation, DoT approved Cisco India IT's application in December 2001. Some time passed before the gateway was deployed while Cisco IT evaluated and selected a service provider for Internet access.

Wireless LAN

For years, Cisco recognized the potential for wireless LAN (WLAN) technology to increase employee flexibility, mobility, and time savings, generate higher productivity enterprise-wide, and provide users with a more dynamic and reactive workplace, unlimited by physical constraints. WLAN networks were fully deployed in San Jose, RTP, and most other major Cisco sites by 2000. WLAN was not implemented in India until the second half of 2003, in part because of regulatory issues.

Prior to January 2003, Regulators in India required companies to obtain both import licenses and operational licenses for wireless LAN equipment. Any organization that wanted to use wireless equipment operating in the 2.4 GHz frequency range (e.g., 802.11b) had to first apply for an import license. A second license, for operation of wireless equipment, had to be applied for because various Indian government organizations, such as the Army, railways, and traffic police, used this spectrum for communications. The entire process could be very lengthy.

After January 2003, partial deregulation eliminated the need to apply for an operational license as long as the wireless equipment would be confined within a building; i.e., not interfere with governmental communications. The process of applying for an import license consisted of providing officials with the brand, model number, serial numbers, and description of where devices would be used. Cisco IT India applied for a license in June 2003 and received approval within approximately eight weeks. Today the application and approval process takes about one week.

Cisco IT India set up a pilot WLAN deployment in August 2003 that placed Cisco Aironet Access Points in a half dozen conference rooms within Divyashree Chambers. A number of users were fitted with wireless adapter cards in their laptops and asked to test the service over a one-month period. Based on the results of this pilot, Cisco IT implemented Phase Two, completed in October 2003, which deployed Access Points throughout all the Cisco research and development centers and sales sites within India. Approximately 55 Access Point were deployed. Today, that has grown to nearly 80 access points.

Local VPN Concentrator

Many of the engineers employed by Cisco India's partners work at least a portion of the time from their homes. Some are part-time teleworkers who telecommute a few days a week, while others are day extenders who telecommute

evenings or weekends to stretch their workday. From their office, connected to the CUG, they have direct access to data files and applications on the Bangalore servers, as well as access to the World Wide Web. But from home, they must connect through a Virtual Private Network (VPN) connection. Prior to 2003, any employee of a Cisco India partner accessing the Cisco network from home via a VPN connection traversed the Cisco WAN network to San Jose where the VPN tunnel would be terminated and the user authenticated, and then connecting to the Internet, frequently to access web servers located back in India. Backhauling this network traffic over costly international circuits was not efficient and resulted in significant latency, which affected performance. Cisco India IT recognized that a VPN concentrator deployed in Bangalore could provide local authentication and termination, which would eliminate the need to travel to San Jose and back again, and dramatically reduce latency. But as with the local Internet gateway, telecom regulators feared that such a device could allow companies to act as service providers to other companies connected to their CUG. When implemented, the service was installed for incoming VPN traffic, as the existing international private links provided ample bandwidth for outgoing traffic.

Cisco India IT noticed a press release wherein a spokesperson from the India telecom regulators had announced legal approval for VPN services in India, and began to submit requests to allow deployment of a local VPN concentrator in Bangalore. In September 2003, the DoT approved the request. Cisco India IT quickly deployed the concentrator. Today, latency has been reduced from 230 milliseconds to between 40 and 50 milliseconds, improving performance and productivity for more than 100 VPN users.

Service Provider Redundancy

Reliability and availability of the Cisco India network is extremely important. Cisco's corporate IT policy stresses the need for redundancy and back-up capabilities at all levels of the network to ensure uninterrupted business operation. Not only should critical circuits be redundant but, where possible, diversity of service providers should also be considered. Until 2002, however, India's telecom industry was completely dominated by one service provider, BSNL. No alternative carriers existed.

Telecom deregulation had begun in 2000 when the Department of Telecom (DoT), India's incumbent carrier and regulator, split off the carrier business into the wholly owned subsidiary, BSNL. By the second half of 2002, several private service providers began offering competitive services. Cisco India IT was very interested in evaluating some of these private carriers, which could provide a level of diversity on the Cisco India CUG not available up to that point. Concerned about loss of revenue and market share to competitors, BSNL notified its customers, including Cisco India, that if they purchased circuits from a private service provider, BSNL would immediately terminate all services it supplied to those customers.

Cisco India sent several letters to BSNL and its parent organization, DoT, explaining the importance of service provider diversity in its network. This correspondence was met with a reiteration of its earlier notice. Because BSNL was the incumbent carrier, nearly all of Cisco's circuits would be affected. This posed too much risk for Cisco India IT.

Other companies had been similarly appealing to BSNL, with the same result. Ultimately, the issue came to the attention of Telecom Regulatory Authority of India (TRAI). TRAI had been formed to regulate the telecommunications services, adjudicate disputes, dispose of appeals, protect the interests of services providers and consumers, and promote and ensure orderly growth of the telecom industry. TRAI subsequently wrote to BSNL, advising them that they did not have the authority to restrict competition since BSNL was just another service provider.

Cisco India IT sent a copy of this letter to BSNL, seeking permission to proceed with the purchase of competitive services. Immediately, Cisco India IT received a reply yet again reiterating its intention to terminate any BSNL circuits of customers who purchased competitive services. At this point, Cisco IT turned to Cisco's Legal department for advice. Legal reviewed all relevant documents, including the terms and conditions that Cisco India had agreed to when it contracted with BSNL for services. Legal determined that, based on the letter from TRAI, the rule on purchasing competitive services was no longer valid. However, a clause in the service contracts that Cisco India IT

had signed stipulated that there shall be no interconnection with private operators.

A number of large companies in India had ignored BSNL's threat and proceeded to purchase competitive services. But Cisco was intent on working amicably with BSNL and regulators. Arun Joshi and Bala considered a different approach. "We sent them a letter stating that service-provider diversity would mean a more stable network infrastructure, which would enable greater growth for Cisco India, which in turn would mean more jobs and an increase in foreign exchange," says Bala. "We laid out the expansion projects that were planned and explained how it would be good for their business and good for India. It was an argument they couldn't refuse.

Finally, in November 2003, BSNL asked to meet with Bala to describe in detail what the network would look like at each location. "We wanted to have one BSNL link and one private operator link," says Bala. BSNL agreed in writing, stipulating that the primary circuit should be purchased from BSNL and the back-up circuit from the private provider. If the two differed in bandwidth, BSNL would supply the higher bandwidth circuit.

Throughout India, Cisco IT uses E1 circuits to provide connectivity between Cisco India and partners. As traffic increases, additional E1s are added. In November 2003, Cisco had at least two E1s connecting each of the partner sites. It was very easy to replace one BSNL E1 circuit with a private service provider E1 circuit to achieve service provider diversity. In situations where there were more than two circuits, Cisco replaced just one BSNL circuit with a private service provider circuit. Throughout India, Cisco has attained service provider diversity, ensuring the highest level of availability across its network.

Softphone Remote Access

In deploying VoIP in India, Cisco IT had to abide by regulatory constraints that forbid the interconnection of VoIP and the Public Switched Telephone Network (PSTN). These rules were established to protect the revenue base of local and long distance service providers in India. If, for example, a residential or business telco customer in India calls a friend or business associate in the US, they are routed over the PSTN and pay the toll-call rate. But what if they could pick up their PSTN phone and dial into a local connection of a VoIP network? The VoIP network would carry them to the US to an exit point closest to the number they were calling (a technique known as tail-end hop-off), at which point the call would interconnect to the local PSTN in the US. The IXC in India would receive nothing and the ILEC might receive little or nothing for the local call.

Fearing substantive loss of revenue from such arrangements, the telecommunications regulatory body, known as Telecom Regulatory Authority of India (TRAI), established stringent rules against PSTN/VoIP interconnection. The 13.5-hour time difference (between Bangalore and San Jose) often made communication between Cisco employees in India and the US inconvenient. Employees in India must attend conference calls hosted by San Jose from time to time, but 9:00am in San Jose is already 10:30pm in India. The alternatives were to either place a costly long distance call to San Jose from the Cisco India employee's home, or go into the office in India at odd hours where they could access the WAN directly.

Cisco petitioned the regulatory body in India to allow an exception to the PSTN/VoIP interconnection rule enabling employees of Cisco India to call from their home. In June 2003, regulators in India approved a new service called "IN Exchange" that allowed voice calls to terminate at the local Cisco office in India and be carried over the WAN to San Jose. Cisco pays a one-time activation fee of Rs108 (about US\$2.50) and Rs 4.25 (about US\$0.10) per minute (both incoming and outgoing) per connection to enable this service on the Cisco India employee's residential phone line.

While filling a need, IN Exchange had one significant limitation: it was associated with a specific residential telephone line. Cisco India employees could not use the service when traveling. In March 2005, Bala approach service providers regarding the use of Cisco IP Softphone. Softphone is a Windows-based application for the PC. With Cisco IP Softphone running on a laptop, users can take their extension with them and receive calls wherever they are connected to the corporate network. Even dial-up connections while on the road can be used to check voicemail and place calls while online. It can even be used as a virtual conference room.

Bala reasoned with service providers that a call placed or received by a Cisco IP Softphone was an end-to-end packet-based call similar to a VPN connection—which was already allowed. After submitting a formal request in writing, service providers in India gave Cisco IT permission to implement the service.

RESULTS

The Cisco India network today is very reliable, efficient, cost effective, and maximizes communication between Cisco employees and partners. Although difficult at times, applying for and receiving regulatory approvals from telecom regulators was well worth the time and effort spent. Cisco India IT continues to have a close working relationship with regulators in India.

LESSONS LEARNED

Over the past half decade, Cisco India IT has learned that, to be successful in receiving approvals, it has to be aggressive, flexible, persistent, willing to compromise, and to expect demands from regulators. However, there is a major shift occurring within the telecom industry in India today. “It is no longer a service-provider market; it is a customer market now,” says Bala. “Incumbent providers once made demands. With competition among service providers growing, customers have more leverage. Privatization has helped us in negotiating better prices.”

Cisco India continues to leverage its size and presence to influence service providers and regulators in discussions about services or regulatory approvals. “We stress our growth here, the expanding number of job opportunities for Indians, and the foreign exchange created by our activities,” says Bala.

The prohibition against interconnecting multiple service provider circuits in a closed user group has been formally eliminated by TRAI. The regulatory body has ceded authority to individual service providers to decide whether they will allow multi-provider interconnection. Cisco India was able to convince service providers to allow interconnection, based on an extended history of regulatory compliance and working closely with regulators and service providers. Other businesses in India must also work to win such approvals with service providers. However, businesses should not acquiesce to the service providers if denied interconnection. Rather they should pursue approval aggressively.

NEXT STEPS

A new building, known as Subramanya Arcade, or SA, is being opened in Bangalore soon. As with the other Cisco India sites, SA will have WLAN coverage through the facility. However, while other sites use Cisco Aironet 350 series Access Points, the SA building will use the newer Aironet 1200 series Access Points equipped with 802.11g. Current regulatory restrictions limit 802.11g (54 Mbps) devices to operating in the 802.11b (11 Mbps) mode. Full deregulation of 802.11g devices is expected soon. For this reason, Cisco IT India decided to protect its investment by purchasing the higher-bandwidth devices now rather than buy older devices and have to replace them later.

Cisco India is also contracting out the deployment of WLAN equipment in SA. The India Transport team within Cisco India IT previously performed all site surveys and AP installation at the other sites, but without prior experience, expertise, and sophisticated testing equipment many “dead spots” were found. Cisco India IT decided that a professional team could ensure better coverage. In fact, the contractor will re-survey all the research and development and sales sites and fine-tune the network to eliminate coverage problems.

Before the advent of a more competitive telecom marketplace, BSNL, the incumbent service provider, largely dictated the terms and conditions of service. With a more open and competitive market today, Cisco India IT is seeking to change some of these terms. The 2002 agreement between Cisco India IT and BSNL stipulating that primary circuits should be purchased from BSNL and back-up circuits from the private provider is being challenged. Cisco India IT hopes to eliminate that clause and have the freedom to choose services from providers without restrictions.

Cisco India has just begun a pilot to evaluate Cisco IP Softphone for Cisco employees. The initial pilot phase will involve approximately 200 users. Once bandwidth requirements are established, the service will be rolled out to a

larger group, eventually giving all Cisco India the capability to make and receive remote calls. Cisco IP Softphone is being replaced globally by Cisco IP Communicator. Phase two of the rollout will likely involve the newer IP Communicator product.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)