



Customer Success Story

Cisco Helps Network Appliance, Inc. Create a Networked Office-in-a-Box to Facilitate Rapid Growth

Executive Summary

Customer Name

Network Appliance, Inc.

Network Solution

- Cisco 3845 Series Integrated Services Router; Cisco 2800 Series Router for small branch offices
- Cisco 7206 VXR Router
- Cisco 7609 Router
- Cisco Catalyst 6509 Switch

Business Value

- Standardizes deployment of networking equipment for branch offices around the world
- Simplifies network management, as all critical routing, switching, security, and voice capabilities were converged on a single platform
- Supports a wide range of connectivity options, which vary greatly from location to location
- Provides scalability and decreases WAN link costs
- Enables wire-speed concurrent services

Network Appliance, Inc. is a world leader in unified storage solutions, which include specialized storage hardware, software, and services for open network environments. The company is growing rapidly – in its fiscal year 2005, Network Appliance, Inc. added nearly 1000 new people, bringing the number of employees to 3900. At the same time, the company recorded record revenues and an increase in income of 48 percent over 2004.

Rapid growth is motivating the company to add, move, or re-configure network connections. Many offices are requiring greater bandwidth and new networking capabilities to efficiently manage WAN traffic and meet the needs of a diverse range of users. To meet these challenges, Network Appliance, Inc. created an “office in a box” using the Cisco® 3845 Series Integrated Services Router, which provides integrated routing, switching, security, and voice capabilities.

Growth Drives New Requirements

“We are adding new offices and moving several of our large locations,” says Matthew Light, senior network engineer within Network Appliance, Inc.’s WAN Engineering Group. “To connect these locations, we were looking for a single high-performance routing solution that would include security functionality, capabilities for implementing voice over IP (VoIP) in the future, and of course, accommodate routing and switching.”

Ideally, the solution would minimize the amount of equipment required, yet meet demanding performance and scalability requirements. The corporate WAN Engineering Group wanted to ship only one router to each office location and ensure that it was simple enough for the local staff to deploy.

“We briefly considered other brands of routers, but they didn’t have the capabilities that Cisco has,” says Light. “We were comfortable with Cisco networking equipment and we had already made the decision to implement Cisco IP Telephony solutions in the future. The Cisco 3845 Integrated Services Router met our immediate performance and scalability requirements, and would allow us to implement IP telephony without having to replace the routers. And it offered the ease of deployment that was so important to us in setting up new offices.” The Cisco 3845 Integrated Services Router became the standard solution for Network Appliance, Inc.’s new locations. As existing offices were moved, the Cisco 3845 Integrated Services Router also replaced older Cisco 3640 and Cisco 2621 routers.

The Network Appliance, Inc. Network

At the time of the router deployment, Network Appliance, Inc. had been a valued Cisco Systems® customer for approximately three years, using Cisco networking equipment in its WAN and LAN architectures. Network Appliance, Inc. field offices were using a variety of Cisco routers but relied primarily on the Cisco 2621 Router. The company's simplified LAN deployment approach was to use the Cisco 2621 routers in most field offices to terminate Frame Relay T1 and fractional T1 circuits. In some instances, Cisco 3600 Series routers, or Cisco 3640, 3526, or 3745 routers were also used.

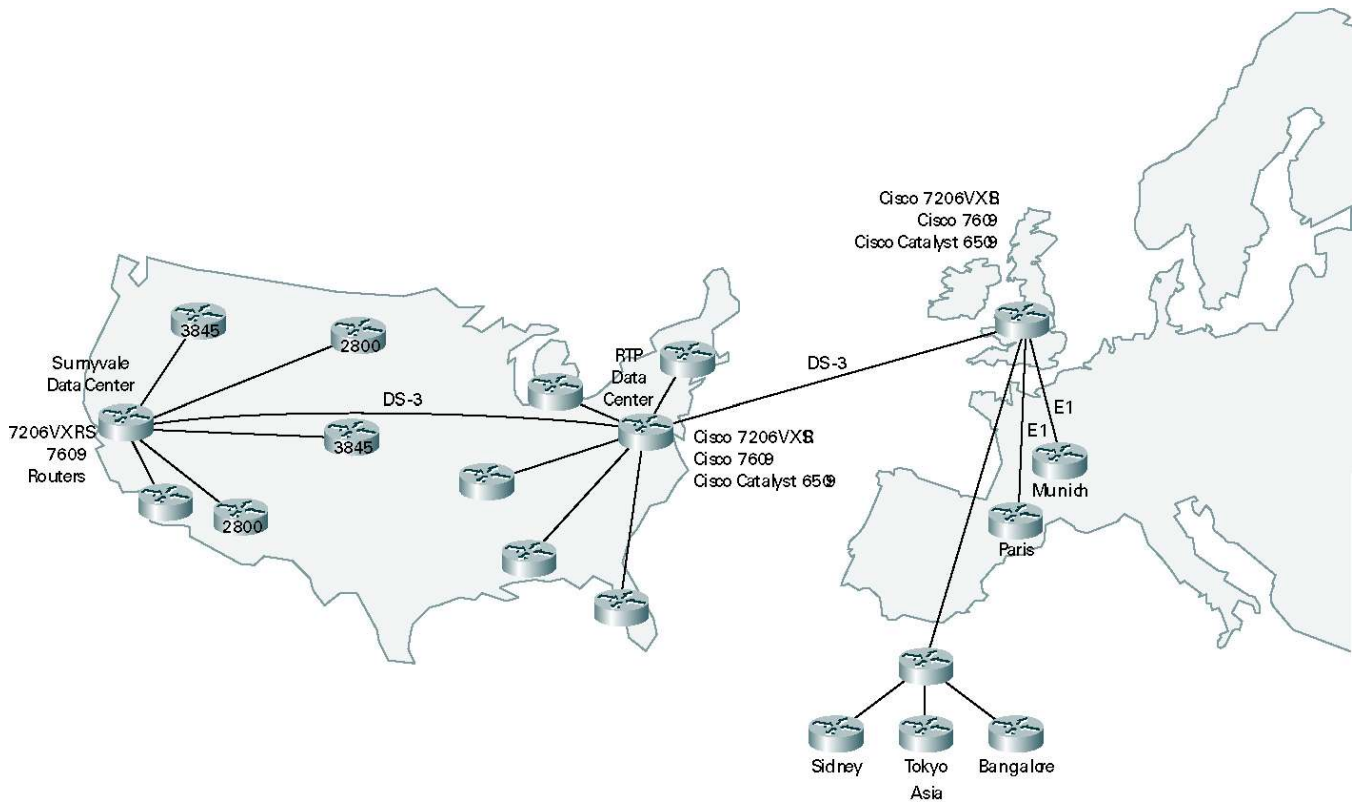
"We ran into capacity problems, however," says Light. "Some of our sales offices also house demonstration labs and post-sales support operations, which required higher routing capacity than the Cisco 2621 could deliver. Small engineering labs and customer support centers also taxed the systems."

Network Appliance, Inc.'s WAN Engineering Group devised a matrix that classified each office by number of employees, capabilities supported, and required level of redundancy. Tier 1 and Tier 2 offices received either single or redundant Cisco 3845 Series integrated services routers. Cisco 2800 Series routers were designated for Tier 3–5 offices.

Data Centers

In 2003, the company built a new data center in Sunnyvale, California, which is connected to Network Appliance, Inc.'s European data center in Hoofddorp, The Netherlands, and to a new data center in Research Triangle Park (RTP), Raleigh, North Carolina. Traffic west of the Mississippi River is routed to the Sunnyvale data center, while traffic east of the Mississippi is routed to RTP. The Hoofddorp center consolidates traffic from Europe. All three data centers are connected using point-to-point DS-3 (45 Mbps) connections with Cisco 7206 VXR routers forming the network backbone. The Sunnyvale site employs Cisco 7609 routers for its core enterprise network, and all of the company's server farms and external vendor networks connect to these devices.

Figure 1



Cisco 7206 VXR routers that have recently been implemented employ the new Cisco 7200 Series Network Processing Engine NP-G1 (NPE-G1), which doubles processing capacity to help Network Appliance, Inc. meet increasing LAN performance demands.

The Cisco 7206 VXR routers also includes the Cisco IOS® Software firewall feature set with access control lists (ACLs) activated. Cisco IOS ACLs provide access control for routed traffic between virtual LANs (VLANs) and VLAN ACLs (VACLs) provide access control for *all* packets. Also enabled is modular quality of service (QoS), which separates traffic classes by marking them in different ways. Real-time applications such as voice over IP (VoIP) and video rely on Cisco Low-Latency Queuing (LLQ) for forwarding with the lowest levels of latency and jitter.

The data centers also support Cisco 7609 routers and Cisco Catalyst® 6509 switches. The Cisco Catalyst 6509 switches create a distribution layer for each data center, while the Cisco 7609 routers are deployed for engineering and software testing labs. Cisco content switching modules are installed in the Cisco 7609 routers deployed in data centers while the Cisco Catalyst 6509 distribution layer switches balance client traffic between numerous server farms. The Cisco 7609 routers are used in the company’s new technology center located near Pittsburgh, Pennsylvania. Labs in Munich, Germany, and Paris, France, use Cisco Catalyst 6509 switches. A new building expansion also deploys the Catalyst 6509 switches with 10-Gigabit Ethernet links, for a simpler, more cost-effective implementation.

The Catalyst 6509 switches provide core switching capabilities; Hot Standby Routing Protocol (HSRP) is implemented to provide failover to multiple VLANs. Each of the three data centers supports at least two external ISP connections, which, in addition to providing Internet access, can be employed to back up any of the other data centers using Cisco VPN generic routing encapsulation (GRE) IP security (IPSec) tunnels.

The WAN

Large hub sites in Europe, such as those in Munich and Paris, are connected to the company's WAN, as well as to sites in Sydney, Tokyo, and Bangalore. In-country field offices are connected to main hub sites. In Europe, field offices and main locations are connected to the main data center in Hoofddorp using a hub-and-spoke topology, E3 links, and VPNs. Cisco 7206 VXR routers aggregate T1/E1 and DS-3 links and deliver them to the core network. DS-3 Internet connections are terminated at Cisco 7206 VXR routers. Cisco 3000 Series VPN concentrators allow Network Appliance, Inc. teleworkers or home-based employees to connect to the network using a Cisco VPN client and the Cisco 870 Router. The Cisco 870 Router is used to allow remote workers access to printers and demonstration labs, which may be located regionally, and to extend routing, QoS, VoIP, and wireless capabilities to them over the corporate network.

Gaining the Required Scalability

One of the reasons Network Appliance, Inc. chose the Cisco 3845 Series Integrated Services Router was its ability to support a wide range of interfaces. In many places, Network Appliance, Inc. employees have multi-megabit DSL or cable modem Internet access at their homes and are accustomed to high-speed connectivity. In the offices, Network Appliance, Inc. often had to choose between T1/E1, Ethernet, or DS-3 connections – with little in between. In some cases the company had to bundle multiple T1 connections to achieve sufficient bandwidth. In other locations, cable modem access services offered Ethernet connectivity.

“The Cisco 3845 Integrated Services Router gave us great flexibility to use the connectivity options available to us in all of our locations,” says Light. “Because the routers also have Ethernet on board, we could support DSL or cable modem connectivity instead of having to pay for multiple T1/E1 links. It allows us to scale incrementally – and we can even deploy multiple DS-3 links to each router if necessary without having to replace the router itself.” Light and his team also deploy the Cisco 3845 with the VoIP feature set so that it is ready to activate when they are ready to begin their IP telephony deployment.

Deploying Security Features

The Cisco 3845 Integrated Services Router provides wire-speed performance for concurrent services such as security and voice, and advanced services at full T3/E3 rates. Network Appliance, Inc. has deployed the Cisco IPSec VPN feature, which includes IPSec encryption and tunneling protocols such as Triple Data Encryption Standard (3DES), GRE, Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), Dynamic Multipoint VPN (DMVPN), multi-VPN routing and forwarding (multi-VRF), and Multiprotocol Label Switching (MPLS) secure contexts.

With the Cisco IOS Software firewall feature set, Network Appliance, Inc. can deploy VPNs from the Cisco 3845 Integrated Services Router to securely connect branch offices to the WAN and to Network Appliance, Inc. data centers, as well as secure an Internet connection from the same routing platform. This capability allows employees in small offices far from major hub locations to exchange files and data with customers, partners, and other Network Appliance, Inc. employees over the Internet without having to backhaul all of the traffic to Sunnyvale over the corporate network. Sending local traffic over the Internet provides incrementally improved performance, and still enables users to obtain content and resources from a major hub site if the main WAN link goes down.

Network Appliance, Inc. also implemented authentication, authorization and accounting (AAA) on its routers to help meet Sarbanes-Oxley compliance requirements by documenting router changes and simplifying log auditing. The Cisco IOS Firewall intelligently filters Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets based on application-layer protocol session information and can be used for intranets, extranets, and the Internet. It also enables Java blocking, prevents and detects denial of service (DoS) attacks, and provides real-time alerts and audit trails. Using the Cisco IOS Firewall, Network Appliance, Inc. can safely allow individuals and field offices to have direct access to the Internet. The Cisco IOS Firewall dynamically opens access to the Internet through the company's perimeter firewall from an internal trusted space. This enables Network Appliance, Inc. employees to improve customer support and obtain content from the Internet more easily.

Improving Performance with Quality of Service Features

Network Appliance, Inc. provides data storage solutions for companies and it must handle high volumes of point-to-point traffic, often from users sharing files and music. To distinguish this traffic from traffic generated by internal customer support, financial, engineering, and customer relationship management (CRM) applications, Network Appliance, Inc. has begun using the network-based application recognition (NBAR) feature within Cisco IOS Software. NBAR is a classification engine that recognizes a wide variety of applications, including Web-based and other difficult-to-classify protocols that rely on dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, the network can invoke specific services for that application, ensuring that network bandwidth is used efficiently. After building signatures into NBAR for point-to-point traffic, Network Appliance, Inc. can identify bandwidth abusers and then block them or apply rate-limiting policies to prevent network congestion.

Class-based weighted fair queuing provides support for user-defined traffic classes and Network Appliance, Inc. uses low-latency queuing to prioritize voice traffic traveling across the network between the company private branch exchange (PBX) systems and for voice generated during a pilot test of Cisco IP Telephony solutions. Traffic is marked at the access layer through Cisco Catalyst 3750 switches at field offices that initiate numerous high-bandwidth transfers – and in one of the data centers using the Cisco 7609 routers or Cisco Catalyst 6509 switches. When the traffic encounters the LAN routers, QoS policies are applied. Mission-critical traffic, such as Oracle and Siebel traffic, is also marked at the access layer and then queued at the WAN router.

Rate-limiting is also applied to ensure that multiple internal groups have the bandwidth they need to deliver customer service, protect financial data, test software, provide post-sales support, and access the company's CRM application.

Back-Up Options

The Cisco 3845 Integrated Services Router also offers Network Appliance, Inc. the option of using GRE VPN and GRE over IPsec VPN capabilities to back up its core networks. The three main data centers in Hoofddorp, Sunnyvale, and Raleigh are backed up by a VPN through ISP-provided DS3 circuits. Field offices have a direct WAN connection as well as an ISP connection; if the WAN link goes down, traffic can still get out over the ISP link and be routed through the main hub sites.

Results

Network Appliance, Inc. now has a standard implementation for its remote offices based on the Cisco 3845 Series Integrated Services Router. The company receives high-performance routing, significant flexibility for accommodating a wide range of interfaces, QoS and security features, and a VPN-based back-up routing solution in the event of a WAN link failure. Network Appliance, Inc. found its "office-in-a-box" in the Cisco 3845 Integrated Services Router.

**Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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. (0502R) DR/LW8961 08/05

