

CiscoAssure Policy Networking

Enabling Business Applications through Intelligent Networking

Introduction

Today, enterprise networks provide the foundation for business. The advent of networked business applications such as intranets, extranets, and electronic commerce over the Internet has created a boom in productivity and fostered unprecedented global commerce opportunities.

However, as more business applications are deployed over the network, which is clearly the industry-wide trend, the business becomes dependent on an intelligent network. As a result, enterprise network managers require the capability to control the use of the network and to allocate and prioritize network resources for different applications and user groups.

The Need for Policy Networking

Network managers need policy control over bandwidth-hungry applications, which consume bandwidth at the expense of performance and drive up the cost of expensive wide-area resources.

A mis-behaved application can potentially shut-down the business.

The need for policy networking is being driven top-down by business requirements dictated by market and competitive forces. The network manager needs to be able to map these business requirements into specific policies that link the business needs with the desired network behavior. For example, if an organization is running an enterprise

resource planning (ERP) application (e.g., SAP R/3, Oracle Financials, Baan, Peoplesoft), for strategic competitive advantage, a policy can be established that gives ERP traffic priority to network resources. The business policy is automatically translated into network behavior, such as Quality of Service (QoS) mechanisms, to prioritize ERP traffic ahead of other traffic.

The intelligent network provides a rich set of QoS and security mechanisms to enable business applications. However, utilizing these features can be a complex exercise for network managers. There is a real need to provide dynamic and automatic configuration of features in the

intelligent network. Network devices must be dynamically tuned to support increased user mobility and new classes of applications such as Internet webcasting and multimedia applications that support data, voice, and video simultaneously.



Cisco is addressing customer requirements for policy-based networking through its CiscoAssure Policy Networking initiative.

CiscoAssure Policy Networking

CiscoAssure Policy Networking enables business users and applications to use the intelligence that is embedded in a network. Simply put, CiscoAssure Policy Networking makes it easier for a network manager to take advantage of distributed network intelligence features.

The CiscoAssure Policy Networking architecture is based upon four building blocks:

- **Intelligent Network**

Intelligent network devices—that is, routers, switches, and access servers running Cisco IOS™ software—enable and enforce policy services in the network. (See Figure 1 below.)

- **Policy Services**

Policy services translate business requirements into network configurations and activate policies for quality-of-service (QoS), security, and other network services.

- **Registration and Directory Services**

Registration and Directory services provide the dynamic binding between addresses, application profiles, user names, and other information data stores.

- **Policy Administration**

Policy administration provides the capability to centrally configure rule-based policies that control services within the network infrastructure.

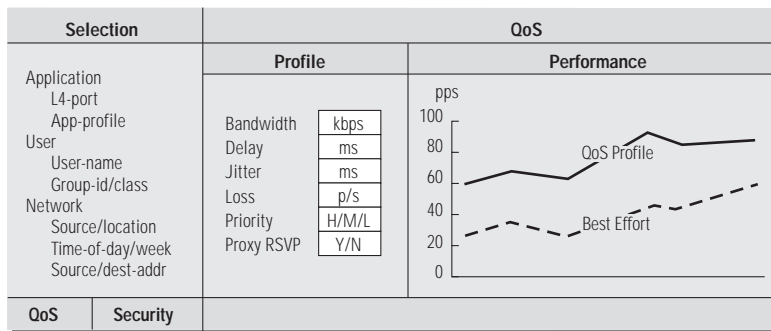
The Role of QoS

QoS has been a critical requirement for wide-area networks for years. Bandwidth, delay, and delay variation requirements are at a premium in the wide area. The importance of end-to-end QoS is increasing because of the rapid growth of intranet and extranet applications that have placed increased demands on the entire network. QoS can protect mission critical applications from bandwidth hungry applications such as multimedia, web-casting, and real-time video applications.

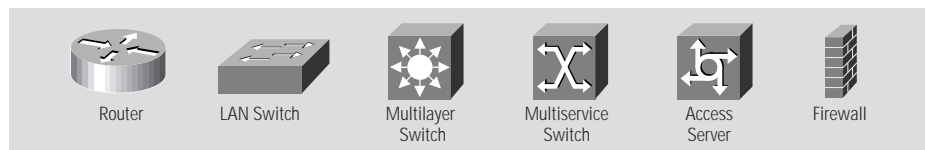
QoS provides a number of important roles.

- Protects mission-critical applications such as ERP or sales automation systems.
- Prioritizes groups of users based on business functions such as sales and engineering.
- Enables multimedia applications such distance learning or desktop videoconferencing.

Figure 1 Cisco Assure Policy Networking Architecture



Policy Administration



Intelligent Network Devices

A network manager may need to provide different service levels for applications. For example, when a sales manager enters an order at the end of the quarter, the network can recognize the application and can prioritize it over other types of traffic.

Today, the QoS mechanism in Cisco IOS software enable networks to control and predictably service a wide variety of networked applications and traffic types. Key Cisco IOS QoS capabilities include:

- **Weighted Random Early Detection (WRED)**

WRED provides preferential treatment for premium traffic classes under congestion situations by allowing network managers to specify a different RED policy per traffic class.

- **Weighted Fair Queuing (WFQ)**

WFQ segregates packet traffic into either flows or classes, and then schedules packet output to meet specified bandwidth allocation or delay bounds. WFQ classes may be assigned either by IP Precedence, application ports, IP protocol, or incoming interface.

- **Resource Reservation Protocol (RSVP)**

RSVP enables applications to dynamically request and reserve network resources necessary to meet their specific QoS requirements. Through proxy RSVP capabilities, Cisco routers utilize RSVP to request resources on behalf of applications that are not yet RSVP-enabled

- **IP Precedence**

IP Precedence signals differentiated QoS throughout the network by using existing IP Precedence-aware queuing mechanisms (e.g., WFQ, WRED)

- **Policy Based Routing (PBR)**

PBR defines customized routing paths for selected packets based on criteria such as source address and application port and can also be used to classify packets and mark packets via the IP Precedence field, enabling backbone routers to give priority treatment when congestion occurs.

QoS Policy

Historically, configuration of QoS has been complex and error-prone due to its static nature, thus limiting its application to the wide-area network edge. QoS mechanisms had to be manually configured on each device. Now through CiscoAssure Policy Networking, policy configuration is simplified to enable active policies in the network and deployment of QoS end-to-end.

CiscoAssure Policy Networking enables QoS policies based on application type, user group identity, and other classifications such as time of day, day of week, or even physical port information derived from the topology of the network itself. These identity classifications take advantage of CiscoAssure policy and registration services as well as other important network information services like management systems that provide topology and device information.

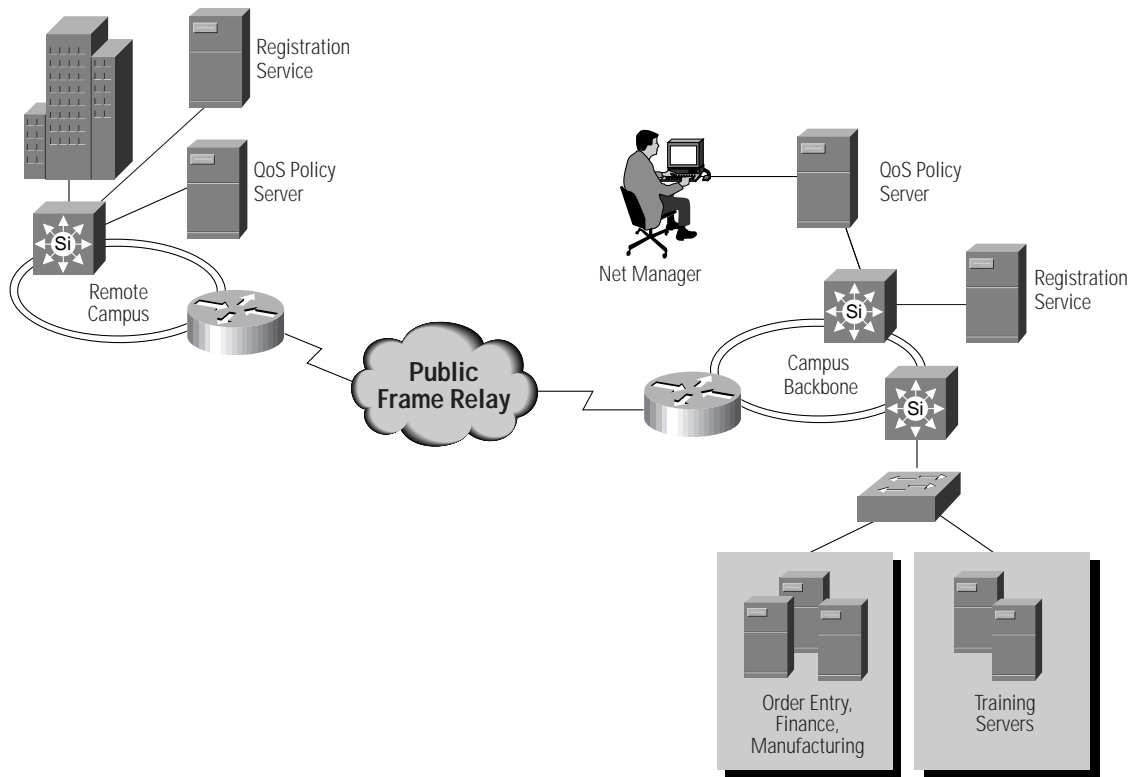
Figure 2 QoS Policy Binding

QoS Policy Binding		
Identifier	QoS	Accept/Deny
SQLnet	High	Accept
NetMeeting	Medium	Accept
Video	< 100Kbps	Accept

To set up a QoS policy, the network manager uses the “drag and drop” Policy Administration graphical-user-interface (GUI) to specify a policy based on business rules. A QoS policy binding is then created and activated by QoS Policy Servers. The Common Open Policy Service (COPS) protocol provides policy exchange between the policy servers and the Cisco IOS software embedded in the intelligent network devices. The Cisco IOS software translates the policy binding into local QoS enforcement mechanisms such as Weighted Fair Queuing (WFQ) or Weighted Random Early Discard (WRED).

After the policy is activated, specific policy-aware network devices identify and classify traffic and execute the appropriate policy dynamically without requiring manual intervention. As a result, the network manager can focus on specifying business policies and leveraging the intelligent network to recognize and enforce the policies automatically.

Figure 3 QoS Policy by Application and User Group



Registration Services

The DNS/DHCP Registry product is an active CiscoAssure Policy Networking registration service. The DNS/DHCP Registry dynamically allocates addresses according to policy classification and creates a binding between a user group and the policy server. For example, the engineering or sales group may require a specified class of service for a particular time of day or application type. This coordination of user classification and policy server binding provides a powerful mechanism that enables the network manager to control the use of the network resources.

As another example, the enterprise network manager may need to support multimedia applications but restrict their use in certain parts of the network. With policy control, the network manager can create a policy for certain users to limit bandwidth available for specific multimedia applications. For example, the remote office may only support a 256-kbps link. In this case, the network manager can set a policy to limit the multimedia traffic to a maximum of 100 kbps. This policy protects the mission-critical traffic that must share the lower-speed remote access link with higher bandwidth applications.

Without policy control, the network gives up critical network resources to any bandwidth-hungry or “misbehaved” applications. With QoS policy control, the business and business critical applications are assured.

The Role of Security

Security policies also play a critical role for an enterprise. Security policies define rules that identify which users have access rights to enterprise resources. Today, security policies must support not only the users within the enterprise but also users outside the enterprise such as partners, customers, and employees accessing corporate resources from the Internet.

Cisco offers a comprehensive suite of security technologies that enable a custom security solution for any business.

Today, Cisco provides comprehensive security solutions for the enterprise, including:

- **CiscoSecure Access Control Server (ACS)**

CiscoSecure simplifies remote access policy control by providing central authentication and authorization of remote users. The CiscoSecure database maintains all user IDs, passwords, and privileges. CiscoSecure access policies can be downloaded in the form of access control lists (ACLs) to network access servers such as the Cisco AS5300 Network Access Server.

- **Firewalls**

The Cisco PIX™ Firewall and Cisco IOS Firewall Feature Set protect valuable resources from unauthorized access.

Many existing security control mechanisms are based on static access control lists (ACLs) that inspect traffic at the network layer, or at most, the transport layer. Now with Context-based Access Control (CBAC), dynamic application inspection and control capabilities are available. CBAC is an important new feature in the Cisco IOS Firewall Feature Set.

CBAC adds intelligence by examining and tracking application-layer protocol state information. CBAC dynamically creates and deletes ACL entries according to session state information. In addition, CBAC monitors packet control channels and recognizes application-specific commands in the control channel. This is an important capability since many application protocols (e.g., H.323, FTP, RPC) involve multiple channels created as a result of dynamic negotiations in the control channel.

- **Encryption**

Encryption enables the secure transmission of sensitive information without unauthorized review or modification. Cisco provides hardware- and software-based encryption solutions. Cisco IOS software encryption is available on a broad range of Cisco products, and supports both the 56-bit and 40-bit Digital Encryption Standard (DES). In addition, Cisco provides hardware encryption for the Cisco 7200 and 7500 routers to boost encryption performance for high-throughput applications over high speed interfaces.

Cisco has taken a leadership role working through the Internet Engineering Task Force (IETF) and with partners such as Microsoft to bring end-to-end, standards-based security solutions to market. As an example, Cisco is delivering IPsec security solutions. IP Sec (IP Security) is a group of IETF draft

standards that act as the framework for interoperable encryption and authentication between IP devices. IPsec will facilitate the broad deployment of Internet applications such as virtual private networks (VPNs) and virtual private dial networks (VPDNs).

Security Policy

Security policies are critical for the enterprise. They include campus security, remote access security for mobile users and telecommuters, and Internet-based VPDNs and virtual private networks VPNs among others.

Remote Access Policy

Cisco's remote access security policies can be implemented for employees who telecommute or for mobile users who dial-in over Integrated Services Digital Network (ISDN) or public switched telephone network (PSTN). The security policy is enforced at the corporate campus with CiscoSecure and the AS5300 Network access server.

For example, first the employee dialing-in is identified. When the employee dials in, the AS5300 passes the user ID and password information to CiscoSecure for authentication. The AS5300 and CiscoSecure communicate using a standard protocol such as RADIUS or TACACS+. These protocols allow CiscoSecure to communicate with Cisco routers, network access servers, and firewalls. CiscoSecure then checks the password against its database, and authenticates the user. Once authenticated, CiscoSecure sends an acknowledgment back to the AS5300. This acknowledgment includes the user privileges, so that the AS5300 can prevent unauthorized access to corporate resources.

CiscoSecure also supports more advanced techniques for authenticating users such as token cards. An increasingly popular authentication method is the one-time password supported by token cards or soft tokens. This method of authentication is often used to authenticate the access of mobile users.

Virtual Private Dial Network Policy

Many enterprises are using or planning to use the Internet to connect remote offices, mobile users, and partners to the enterprise. This area is expected to grow tremendously over the next few years because network managers want to provide low cost connectivity from anywhere in the world.

In this example, enterprise remote access security policies can be extended across the Internet, yet controlled at the enterprise by CiscoSecure. Remote telecommuters or mobile users dial into their local Cisco Powered Network Internet service provider (ISP) and are connected to the enterprise headquarters through a secure VPDN connection. The ISP provides this capability with the Cisco Global Roaming Server (GRS) to coordinate login identity and passwords with the enterprise CiscoSecure console. The VPDN solution works with Cisco IOS firewall products to provide secure remote access to the corporate network across the Internet.

In this case, the enterprise corporate router uses RADIUS or TACACS+ to request that CiscoSecure verify the username, password, or token card of the employee dialing in remotely. After the user is authenticated, CiscoSecure informs the enterprise gateway router of the user's authorization rights and the router informs the ISP's universal access server that the call was accepted, and then allocates an address to the remote user. The user is then allowed access to authorized corporate resources through an encrypted tunnel over the Internet. The encrypted tunnel is supported by the emerging IETF Layer 2 Tunneling Protocol (L2TP) standard.

Virtual Private Network Policy

A VPN allows the use of the public Internet to form an extended enterprise network. Using the Internet as a replacement for expensive WAN services can cut costs significantly. However, for an Internet-based VPN to be considered as a viable replacement for leased-line or Frame Relay services, it must be able to offer a comparable level of security, quality of service, and reliability.

VPN policy requires a secure tunnel to be established between remote offices or partners and the enterprise campus headquarters. Before data leaves the remote office router, it is

encapsulated using a tunneling protocol. The Cisco VPN solution provides interoperable authentication and encryption services using technologies such as L2TP and IPSec to ensure privacy of data over a public Internet infrastructure.

Cisco Directory Services

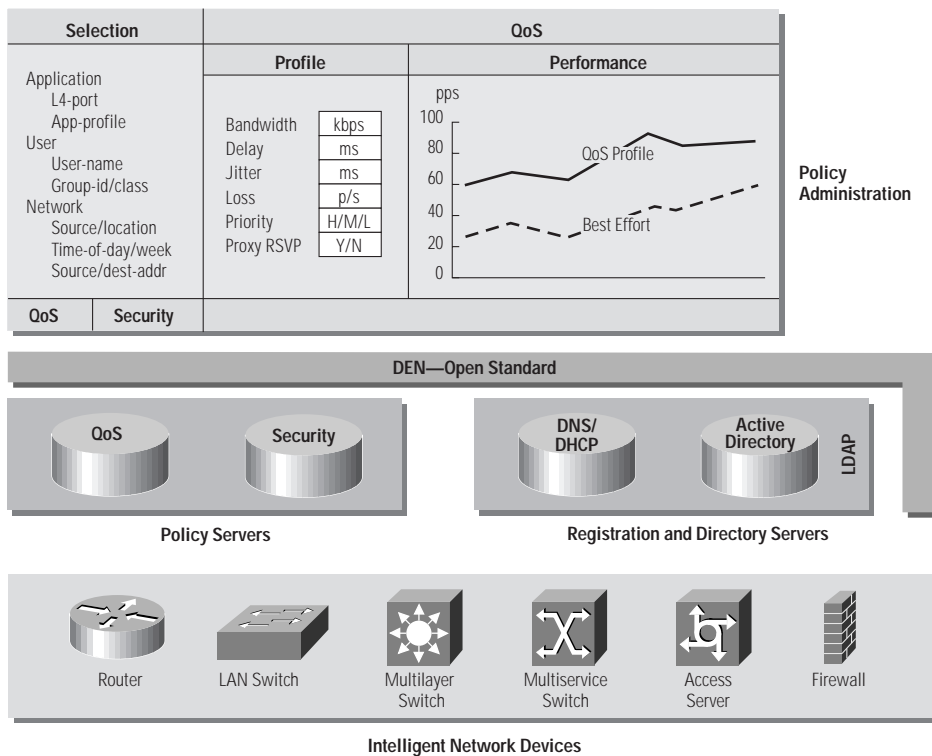
An important part of CiscoAssure Policy Networking is the integration of intelligent network policy with standards-based directory services. The directory provides a central repository and a common naming service for all network resources—including systems, printers, and applications. Through directory integration, the network manager only has to go to one place to add new users or change access rights.

Initially, CiscoAssure Policy Networking will integrate with standard Lightweight Directory Access Protocol (LDAP) v3 compliant directories. This will allow integration with existing LDAP-based directory services and will be a core data access protocol for Microsoft's Active Directory technology.

Active Directory technology supports key Internet standards such as LDAP, DNS, HTTP and X.500 and can be used to provide uniform network services for customers of all sizes as well as to tailor network services on a group or individual basis.

Cisco has licensed Active Directory technology from Microsoft and is jointly developing extensions to Active Directory technology including Cisco IOS network service capabilities. Microsoft and Cisco are enhancing Active Directory technology for Microsoft™ Windows NT™ 5.0 to provide support for advanced network services such as on-demand bandwidth management. In addition, Cisco will implement Active Directory technology on UNIX-based platforms.

Figure 4 CiscoAssure Directory Integrated



In addition to joint development, Cisco and Microsoft are working together with key vendors and customers to define an industry-wide Directory Enabled Networks (DEN) specification. The DEN specification defines the information model, usage, and detailed schema for integrating intelligent networks with directory services.

Several open DEN specification reviews have been hosted as part of an open design review process, the results of which have been submitted to the Desktop Management Task Force (DMTF) for standardization.

Active Directory technology will provide an integrated system for replication and synchronization of directory and policy information across a large-scale infrastructure. Through the integration of CiscoAssure Policy Networking with Microsoft Active Directory, all aspects of managing enterprise resources are tightly integrated, simplifying their administration and maintenance and ensuring scalability and reliability.

CiscoAssure Roadmap

The CiscoAssure Policy Networking initiative will be delivered in a phased approach. Throughout each phase, the Cisco intelligent network will become more application-aware and QoS and security-enabled.

Phase I

Currently, Cisco is delivering Phase I. Many of the intelligent network services required for end-to-end policy control are already available through Cisco IOS software.

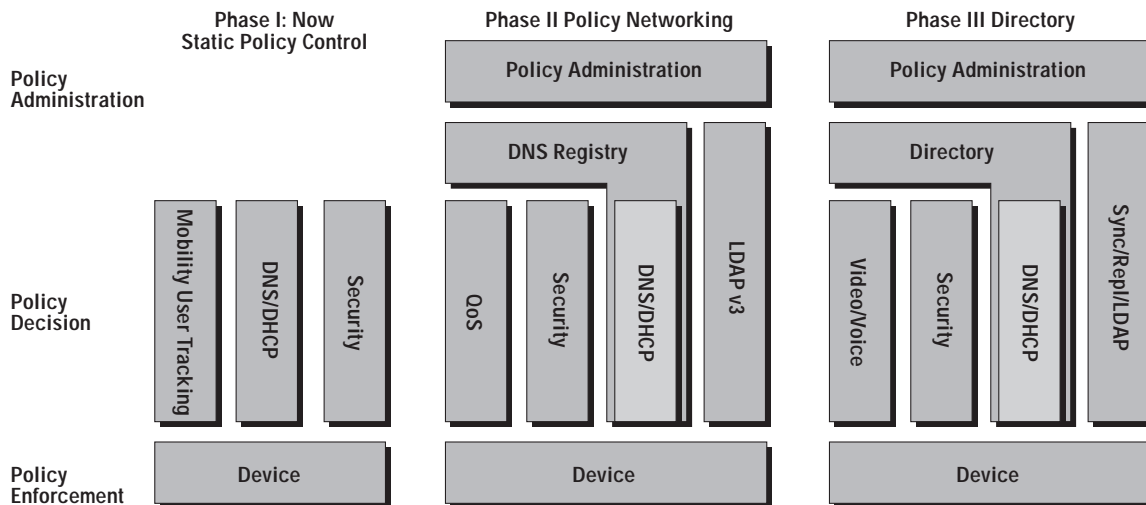
Some important QoS mechanisms include:

- Weighted RED (WRED)
- Weighted Fair Queueing (WFQ)
- IP Precedence
- Policy Based Routing (PBR)
- Resource Reservation Protocol (RSVP)
- Committed Access Rate (CAR)
- Generic Traffic Shaping (GTS)
- Frame Relay Traffic Shaping (FRTS)
- Link Fragmentation and Interleaving (LFI)
- BGP Policy Propagation

Selected security mechanisms include:

- CiscoSecure Access Control Server (ACS)
- CiscoSecure Global Roaming Server (GRS)
- Cisco PIX Firewall
- Cisco IOS Firewall Feature Set
- Context-based Access Control (CBAC)
- Cisco IOS IPSec

Figure 5 CiscoAssure Product Suite



In this initial phase, policies are statically defined within the infrastructure. Policy is administered locally at specific devices as well as through separate GUIs such as CiscoSecure for security or CiscoWorks for Switched Internetworks (CWSI) for mobility and user-tracking services.

Phase II

In Phase II, Cisco will deliver the Policy Administration GUI that centralizes and integrates policy configuration with the QoS Policy Server. The QoS Policy Server will activate policies in the Cisco infrastructure and take advantage of new developments such as the draft IETF COPS protocol to exchange policy information.

During Phase II, the DNS/DHCP Registry will also be delivered. The DNS/DHCP Registry is a next-generation DNS/DHCP solution. The DNS/DHCP Registry will support LDAP v3 and real-time dynamic DNS updates. The DNS/DHCP Registry will support the ability to classify users into groups according to dynamic registration information exchanged with the policy servers. In addition, security policy components will be enhanced to take advantage of dynamic DNS/DHCP Registry capabilities.

During this second phase, there will be enhancements to existing Cisco intelligent network devices. In addition to the existing Cisco IOS network services, Cisco will enhance Cisco IOS software to provide dynamic application recognition capabilities for QoS policy.

Phase III

In Phase III, Cisco will evolve CiscoAssure to provide tighter integration with the directory-enabled infrastructure. Integration with Microsoft Active Directory technology will take advantage of key synchronization and replication features as well as provide further DEN integration across CiscoAssure policy and registration services.

During this phase, Cisco will provide new services for video and voice policy. For example, policy mapping of H.323 telephone addresses, dialing permissions and video session control onto network addresses will be delivered.

Conclusion

CiscoAssure Policy Networking provides the basis for centralized policy control and enables deployment and enforcement of enterprise-wide policies for QoS and security.

As global businesses move on line and networks become the critical foundation of an enterprise, higher levels of reliability, security, and bandwidth control are necessary. CiscoAssure Policy Networking will set these new standards and ensure that network managers have the tools to break through the complexity barrier and provide ever higher levels of service on the network.

The ultimate goal is an intelligent network, one that delivers secure, business-enabling applications across the entire enterprise.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters

Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark
England • France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland •
Singapore