



WHITE PAPER

NETWORK-CENTRIC OPERATIONS

EXECUTIVE SUMMARY

A primary goal of any defense establishment is to operate more efficiently and effectively than its adversaries. Defense organizations are working to transform themselves into smaller, lighter, more agile forces to meet the demands that result from evolving adversaries, and from the changing expectations that governments place on the military. The best way to accomplish this is to shorten the decision cycle—to operate inside the adversary’s decision cycle with quality, dynamic, and mission-critical information. An essential element of this transformation is the migration to network-centric operations.

The adoption and integration of new or improved technologies, capabilities, concepts, and processes into planning and operational activities will determine future success. To possess information superiority, an organization must have a robust network that can support the demands of today’s operations, and that provides a foundation of existing investments that can evolve and grow as technology and needs change.

Today’s networks reflect this ongoing transformation. Infrastructure and mindsets are migrating from sequential, point-to-point, and compartmentalized to an agile, networked, collaborative environment that is rapidly evolving. Proprietary solutions are being replaced by open, interoperable systems. Point solutions are being replaced by ubiquitous solutions. A robust, resilient, flexible, and secure network is the desired result.

Cisco Systems® is the leader in defense networking, providing integrated solutions that securely and smoothly connect the entire chain of command to mission-critical information. As the individual components of the military complex evolve into endpoints on interconnected networks, the features and capabilities provided across the network must enhance the availability, reliability, and survivability of the intervening networks and interconnected systems. Cisco IP Communications solutions enable organizations to lay the foundation necessary for network-centric operations. Converged networks enable communications across previously impenetrable “stovepipes.” Collaborative tools enhance the decision-making process by enabling all parties to share and evaluate the same information at the same time. Cisco Mobile and Wireless solutions offer an expanding suite of mobile services to empower military personnel with vital communications in a dynamic environment. Cisco Security solutions provide a multilayered approach to securing assets from external threats, as well as those within the network. And Cisco Solutions for Continuity of Operations (COOP) help ensure continued optimal performance of military operations in the event of unexpected events that can sever vital communications.

Cisco augments its technologies with an experienced consulting organization, industry-leading best practices, and a wide array of partners. Its comprehensive solutions provide an intelligent network that lets defense organizations rapidly transform themselves into network-centric operations.

INFORMATION IS POWER: APPLYING NETWORK CENTRIC OPERATIONS TO DEFENSE

As global defense agencies face new threats to security and stability, maintaining a high level of effectiveness and preparedness is more critical than ever. Forces are relying more heavily on stealth and precision weaponry, and must operate more efficiently with reduced staff. Improved communications and collaboration are increasingly important for geographically dispersed personnel, joint forces, and coalition partners.

To meet these new priorities, defense agencies are redefining themselves by investing in IT to create a closely integrated, tightly synchronized force. By putting timely, accurate information in the hands of the right people in the right location, a force can gain a significant strategic and

tactical advantage over a threat. This type of mission-critical information plays an even more crucial role today, as defense establishments look to new technology to extend the power of information to every aspect of their organizations.

According to a report prepared by the U.S. Department of Defense entitled *Network-Centric Warfare*, “The challenge for DoD is to harness the power of information technologies to develop concepts of operation and command and control approaches that will be information-driven rather than uncertainty-driven.”¹

To develop the mission-critical information they require, defense agencies are investing in network-centric operations (NCO) initiatives that create an integrated, tightly synchronized force. NCO is a real-time operation model designed to securely deliver mission-critical information throughout the chain of command—anytime, anywhere—to achieve an advantage over an adversary. Its goal is to use relevant information to achieve the desired results of a military operation with minimal casualties, and at minimal cost. NCO affects all levels of military activity, from the tactical to the strategic. At the operational level, it gives commanders the capability to perform precisely, at an efficient operational tempo.

In its “*Network-Centric Warfare*” report, the U.S. Department of Defense states, “Network-centric capabilities allow the force to attain an improved information position that can partially ‘lift the fog of war’ and enable commanders to improve their decision making and fight in ways that were not previously possible.”

In the future, NCO will play a vital role in creating environments that empower the military to take proactive measures such as minimizing the impact of a natural disaster, or dissuading a potential adversary from taking a threatening course of action. Forces will be able to access information quickly enough to anticipate the impact of a situation and positively influence the outcome.

THE NETWORK IS THE STRATEGIC FABRIC

An intelligent network allows an organization to more closely align its network with its processes, making the network more responsive, more flexible, and more effective at addressing everyday operations, as well as high-tempo operations experienced during contingencies and emergency responses. And it enables an organization to embed security deep within its infrastructure, to protect military assets and respond quickly to threats. Since the network can be a hacker’s target, it must include appropriate security mechanisms that will allow the military to use the efficiencies and effectiveness gained by moving to a networked environment, without placing their operations at risk.

An intelligent network is the strategic fabric that streamlines and synthesizes the flow of information, integrating the complex array of proprietary networks, systems, and applications that provide support for military operations. Under an NCO model, military resources can be simply considered nodes on the network. Each of these resources or “networked vehicles” in the field of operation can enjoy complete access to voice, data, video, and command and control—to and from headquarters.

Leading military organizations are moving away from traditional centralized thinking and planning, and toward an edge-centered approach to information sharing and availability. An intelligent network provides the foundational elements, such as collaborative tools, storage, security, messaging, and mediation, creating a common platform that supports the full array of services and applications used by military forces. These services can be used across service or agency boundaries—transparently to the user. An intelligent network is also central to an environment where users can pull the information they require, without relying on a top-down, “push” approach to intelligence and decision making. This ability to “reach back” also reduces the forward footprint necessary for military operations, dramatically reducing costs and risks to personnel.

To deliver mission-critical information, the network must meet stringent requirements. It must be resilient enough to ensure that information is always available, protected from network outages, service spikes, and security breaches. And it must be responsive enough to serve up multiple types of information—including voice, video, and data—from multiple sources, to provide the highest degree of shared situational awareness.

In a defense environment, mission critical information is essential to command and control and other logistics, and can come in the form of intelligence, surveillance, or reconnaissance. Consider the advantages this information could provide if it were simultaneously broadcast from a single network across the chain of command down to battlefield operating systems.

¹ *Network-Centric Warfare Report to Congress*, July 31, 2001

OVERCOMING CHALLENGES

Today's defense agencies must contend with a disparate communications environment. Their communications infrastructures likely include legacy equipment and systems that have accumulated over several years. Some of this equipment may be proprietary, making connectivity with other systems difficult. Or the communications infrastructure may be a collection of different systems that have been pieced together. In demanding situations, the disparity in capabilities of the networked elements can dramatically reduce the effectiveness of operations. All too often, current infrastructures are:

- **Inaccessible**—Legacy systems and networks offer limited capability, information accessibility, and scalability. They do not provide the necessary network intelligence to support advanced communications, security, and wireless capabilities.
- **Incomplete**—Because the military information domain is scattered between disparate systems, it is difficult for decision makers to obtain a complete picture. Insight and planning are hampered by proprietary enterprise systems; Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, and Reconnaissance (C4ISTAR) Systems; weapons and sensor systems; and service provisioning or logistics systems—each focusing on only limited areas.
- **Irrelevant**—Different lines of service and coalitions use systems that are deliberately segmented, due to security constraints. Sharing relevant information between these systems in a timely manner is difficult or impossible.

Inability to provide shared situational awareness can have catastrophic results. Defense establishments need to achieve the highest degree of situational awareness to facilitate fast, accurate decisions, and promote self-synchronized action across the entire chain of command.

SEIZING THE INFORMATION DOMAIN

Defense agencies recognize that immediate information is vital to mission effectiveness in military operations, and are looking to networking technology to increase the real-time availability of information. An intelligent network provides the foundation to integrate surveillance, reconnaissance, military intelligence, weapon and IT systems, and applications required to run successful command and control operations.

For example, the Royal Netherlands Army faced the challenge of replacing its European Command (EUROCOM)1-based mobile communications network with a solution that allows fully integrated services. This new solution, the Theatre-Independent Tactical Army and Air Force Network (TITAAN), uses a Cisco IP infrastructure as support for integrated voice, data, and video services. A revolutionary network solution, TITAAN is one of the first tactical military networks almost completely based on commercial off-the-shelf software and hardware components.

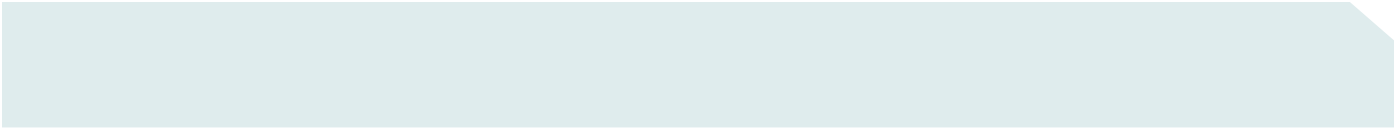
The U.S. Department of Defense is also actively transforming itself to take advantage of the benefits of NCO. Its "Network-Centric Warfare" report cites four main tenets:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness facilitates collaboration and self-synchronization, and enhances sustainability and speed of command
- These, in turn, dramatically increase mission effectiveness

NCO is changing the institutional culture of the military by enabling defense establishments to respond quickly to the changing landscape. The following benefits facilitate these changes.

Shared Situational Awareness

An intelligent network enables defense forces to deliver mission-critical information throughout the chain of command. Organizations can share situational awareness, regardless of the location or time of day.



An intelligent network enables the protection of sensitive information, helping to ensure that sensitive communications and data are available only to authorized personnel. And it streamlines the delivery of information, even from multiple sources and locations. By offering support for data, voice, and video transmissions, an intelligent network gives forces a complete picture of a combat situation.

Because it is based on standards-compliant components and technologies, an intelligent network can interoperate smoothly with existing systems. And it can scale to support thousands of users on the network at the same time.

In its report to Congress, the U.S. Department of Defense underscored the ability of NCO to provide unique advantages to armed forces:

“Network-centric operations provide a force with access to a new, previously unreachable region of the information domain. The ability to operate in this region provides warfighters with a new type of information advantage. This advantage is enabled by the dramatic improvements in information sharing made possible by networking. With this information advantage, a warfighting force can achieve dramatically improved shared situational awareness and knowledge.”

Whether at peace, at war, or engaged in a humanitarian effort, forces need information in a timely and secure fashion to make proactive decisions and successfully achieve their missions.

Greater Mission Effectiveness

An intelligent network boosts mission effectiveness. It gives defense forces the ability to understand a situation more fully, and allows dispersed personnel to simultaneously and accurately evaluate and respond to each situation.

The network improves communications, coordination, and collaboration, to create greater operational efficiencies. And it boosts the effectiveness of military personnel in achieving goals or targets, enabling them to do things they couldn't do before in the field.

For example, the Royal Netherlands Army's new TITAAN system enables the organization to carry its phone traffic and several information systems over a single IP network infrastructure. According to Lieutenant Colonel Bertil Sundquest, Chief Current Ops, “With TITAAN, we can run, on any workstation, command-and-control information, planning, and support systems such as ADAMS, BICES, JOIS, or LOCE. We can also display digital maps and aerial photos, if required, overlaid on each other, using the 3M projector systems mounted overhead in our headquarters.”

Support for Ad-Hoc Operations

A network-centric strategy gives military agencies an unprecedented capability to address high-risk situations, wherever they occur. For example, a secure, ubiquitous network infrastructure can support instantaneous collaboration between military branches of service and coalition partners. Standards-based networking also allows that network to extend out to forces that are on the move, freeing them from dependence on a static location. The network's support for mobile operations can provide a tactical commander with new levels of field visibility.

Because an intelligent network integrates a broad range of networks, advanced systems, and applications, defense forces can collaborate more effectively and share information as an operation unfolds.

Continuity of Operations

Continuity of operations (COOP) is a critical requirement for any defense agency. The interruption of communication, at any level, can jeopardize a mission. An NCO strategy provides the advanced technologies and best practices necessary to protect the network and information assets from unplanned outages and security threats. It also provides the critical emergency response systems to handle new threats and unforeseen situations.

Reduced Operational and Capital Costs

NCO lowers operational and capital costs by converging multiple networks together on a single intelligent network. And, because it consolidates multiple communications systems onto a common infrastructure, it enables military organizations to reduce the costs of provisioning, installing, integrating, and managing the network.

An NCO strategy also allows military organizations to more easily upgrade and support intelligent network services such as converged voice and data applications—which can dramatically improve operational efficiency. With careful planning, the strategy can also reduce the costs of performing incremental upgrades, with network downtime and consumption of IT resources. One example of standards-based networks helping to reduce costs is in applying wireless in the field environment. By connecting field operations through wireless networking, field operations can save significant time and money in airlift, sealift, and excavation costs, compared to laying cable.

NCO enhances reliability and reduces troubleshooting costs, using embedded technologies and services such as integrated security, telephony, management, caching, and content management. These technologies, found on Cisco integrated services routers, protect the network from unplanned network outages, slow service, and security breaches. Training and administrative costs—a significant portion of network cost of ownership—are reduced, because network administrative staff can use a common interface to manage and administer the network. By employing open standards-based technologies, organizations can also avoid the costly pitfalls and limited interoperability associated with proprietary systems.

For example, Cisco and Scientific Research Corporation (SRC) collaborated to deliver a “push to talk” system to soldiers. The system requires minimal configuration, is self-healing, and provides ample bandwidth for military applications. By using standards-based, off-the-shelf components in the design, partners were able to create a valuable, innovative solution that cost significantly less than proprietary systems. It also improves interoperability across different vendor systems, and enables faster rollout of new capabilities. Using an open standards-based architecture gives military organizations unprecedented flexibility, enabling them to more closely attune their infrastructures to highly specific needs—and quickly adjust when those needs change.

POWERFUL, INTEROPERABLE NETWORK SOLUTIONS

Cisco Systems, the emerging leader in defense networking, offers a range of integrated solutions that securely and automatically provide the entire chain of command with access to mission-critical information. Cisco network solutions help ensure that the information that captures and communicates a complete picture built around converged data, voice, and video is delivered securely and immediately. And Cisco products offer the resilience necessary to help ensure that mission-critical information is available and timely—even in crisis situations.

Cisco augments its technologies with a consulting organization that has extensive experience in the design, operations, management, and support required to transform the way the military conducts missions. Its multidisciplinary team is a seasoned organization specializing in providing customized, collaborative assistance through each stage of deployment.

Cisco also provides a comprehensive set of best practices, including its High-Availability Networking Capabilities, which includes deployment blueprints, advanced technical capabilities, case studies, and workshops that are designed to align the network with the operations and to maintain those operations through disruption.

Cisco’s expertise in NCO is not limited to its own organization. Cisco also collaborates with best-of-breed partners in the networking industry to deliver additional networking capabilities. These partners offer added expertise for specialized applications, and can accelerate the performance and improve the effectiveness of a wide range of defense operations. For example, Cisco is a founding member of the Network-Centric Operations Industry Consortium (NCOIC), which focuses on industry working together to provide customers with network-centric environments, where all classes of information systems interoperate by integrating open standards into a common evolving global framework. The mission of the consortium is to help accelerate the achievement of increased interoperability within and between all levels of government in the United States and its allies involved in joint, interagency, and multinational (JIM) operations.

Cisco network solutions and partnerships with the worldwide defense establishment provide an intelligent information network that serves as a technical foundation for defense organizations that are transforming into network-centric operations. The solutions provide the entire chain of command with secure access to mission-critical information from any point on the network, without the barriers of time or location. Combatant and noncombatant personnel around the world—including troops on the move—can accomplish their tasks better, faster, and more securely.

Cisco IP Communications Foster Collaboration

Defense agencies are already replacing legacy telephone systems with IP systems. These converged platforms enable organizations to take advantage of sophisticated and streamlined communications, as well as collaborative tools that dramatically improve the effectiveness of personnel across the chain of command. Cisco IP Communications solutions consist of a U.S. Department of Defense-certified set of mission-grade capabilities, including advanced IP telephony, IP Communications PBX, unified communications, IP video- and audioconferencing, and surveillance and critical emergency response solutions.

Designed for mission-critical applications, Cisco IP Communications solutions conform to demanding government and industry standards, such as Federal Information Processing Standards (FIPS), Common Criteria standards, and IPv6. Together, Cisco IP Communications solutions provide sophisticated and streamlined communications.

For example, governments are replacing antiquated and proprietary emergency conferencing systems with Cisco advanced IP Communication solutions that provide more sophisticated and streamlined communications and collaboration capabilities to prepare forces for any kind of emergency or disaster, including acts of terrorism. Cisco MeetingPlace, a Defense Collaboration Tool Suite (DCTS)-certified solution that is part of the Cisco IP Communications portfolio, enables critical emergency response through rich media conferencing capabilities that create a virtual command and control center for handling crisis communications, crisis team management, and crisis monitoring. It empowers military commanders with a more collaborative environment to precisely and securely dispatch mission-critical information instantaneously across the chain of command when a crisis occurs. Cisco MeetingPlace enables military organizations to provide a far more effective response in handling emergency situations, including a single point of accountability.

Cisco Mobile and Wireless Solutions Enable Ad-Hoc Operations

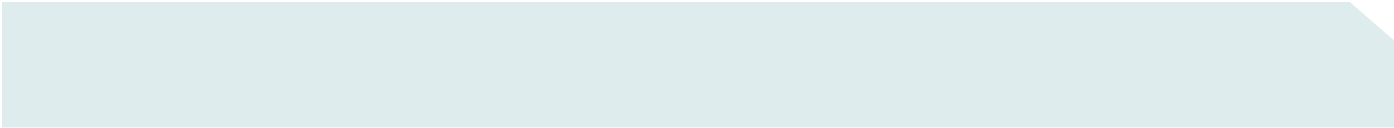
Combatant and noncombatant operations depend on personnel on the move. Cisco Mobile and Wireless solutions consist of a wireless intelligent information network infrastructure that includes high-performance LAN/Wi-Fi and WAN services. Cisco Mobile and Wireless solutions offer an expanding suite of mobile services to extend network access beyond the limits of wires. Mobile solutions are an efficient and flexible way to empower troops and other military personnel with vital communications, regardless of location. These solutions offer military forces more flexibility and maneuverability while providing greater access to communications and information.

For example, as part of its collaborative project with SRC, Cisco has begun testing its Scalable Mobile Architecture for Tactical Communications at Ft. Bragg, North Carolina, and at the National Training Center in Ft. Irwin, California.

Using standards-based 802.11 technology, military units can roam freely and securely between wireless coverage areas. These roaming models can support tactical communications as complex as a vehicle on the move with a wireless bridge, associating and disassociating as it moves through the battlefield. Depending on the combination of output power and antenna gain, distances up to 14 kilometers can be achieved with omnidirectional antennas, and even longer distances can be achieved with directional antennas. In the past, similar tactical communications often required a direct line of sight back to a communications node, which imposed limits on maneuverability and mobility.

Cisco Security Solutions Safeguard Vital Assets

Defense establishments have put the highest priority on protecting and securing communications and other important military assets. Cisco offers a wide range of highly reinforced, tightly integrated security solutions, including secure connectivity, threat defense, and trust and identity management. Cisco solutions provide a multilayered approach in securing assets from external and internal threats, providing rapid response to both known and unknown security issues.



Cisco security solutions prevent unauthorized network access, mitigate worm attacks, and circumvent denial of service attacks. They conform to government regulations and include commercial-grade encryption technology that has been certified for use in government and military applications. This comprehensive safeguarding of network assets enables military organizations to maximize network uptime and productivity, while minimizing threat impact.

As part of its security portfolio, Cisco also supports Network Admission Control (NAC), a Cisco Systems-sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network resources. This strict policy enforcement initiative is designed to limit damage from viruses and worms. Using NAC, the military can provide network access to endpoint devices, such as PCs, PDAs, and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources. When combined with Cisco's broad array of security technologies, NAC can actually respond to threats so quickly that the network becomes self-defending. When combined with other standards-based technologies like 802.1X (also supported in Cisco network switches and router switch modules) that restrict access to network resources to authorized endpoints, NAC demonstrates Cisco's multilevel, integrated approach to security.

Cisco Solutions for COOP

Cisco Solutions for COOP are an offensive measure that helps ensure continued optimal performance of military operations in the event of disruptions, including natural disasters or other unexpected events that can sever vital communications.

Defense organizations recognize that continuity of operations planning is crucial in ensuring that the military can function at full capacity, even in the event of a catastrophe. Cisco Solutions for COOP are based on four components: high-availability networking to ensure the highest degree of network uptime; data center and storage networking, including solid back and recovery of operational assets and interconnections for backup data centers; Cisco VirtualCOOP for field personnel to protect remote connections; and crisis management to notify first responders in the event of a crisis. Together, these components offer a heavily fortified infrastructure that provides mission-critical information that is accessible from alternative offices and other remote locations.

High-Availability Networking

A highly available network is at the core of Cisco Solutions for COOP. Studies have shown that most network failures are traced back to factors outside of network components, including inadequate policies and procedures, or power disruptions. Cisco High-Availability Networking is a preventive network outage blueprint, including best practice guidelines and resources for fortifying military grade networks. Cisco offers the most cohesive, collaborative approach for helping to ensure the nonstop delivery of advanced applications throughout the lifecycle of the network—even as new users, technologies, and network services are added to the network. This increases the operational efficiency of the military and transforms the network from an IT component to a strategic asset for combatant and noncombatant operations.

Data Center and Storage Networking

To keep their operations up and running, defense organizations require a fortified data center, including robust storage with strong backup and recovery capabilities. Cisco Data Center Networking consists of a highly adaptable data center network architecture that optimizes the performance and resilience of networked applications. A suite of integrated data center solutions includes a sound network infrastructure, powerful storage networking, reinforced data center security, application optimization, and business continuance networking. This enables a highly resilient, responsive data center environment that can securely support millions of users simultaneously. Because business continuance is designed into Cisco data and storage networking solutions, defense organizations can quickly and efficiently transfer operations to a resilient data center in the event of an emergency.

Cisco VirtualCOOP for Resource Dispersion

To achieve maximum mission effectiveness, military, intelligence, and relief personnel operating in remote locations require secure, continuous access to mission-critical information. Cisco VirtualCOOP is an IT-managed COOP system designed for personnel working in the field. It provides a highly available, highly secure solution that provides access to NCO systems, maximizing situational awareness. This improves continuity and increases effectiveness by providing defense personnel with mission-critical information, even during network disruptions or when resources are unable to reach their intended destinations. Additionally, Cisco VirtualCOOP can disperse resources to minimize the impact of a single geographic event.

Crisis Management

The Cisco Crisis Management Application gives defense organizations a single architecture for converged conferencing of voice, data, and video for emergency communications and collaboration. This conferencing solution employs traditional TDM and IP telephony converged architectures, together with highly scalable features, to give military personnel greater situational awareness over a crisis environment.

The system provides quadruple levels of redundancy for maximum reliability in the event of an emergency. It provides extensive conferencing features that give organizations greater flexibility in dispatching information instantaneously. For example, organizations can use broadcast dial features to quickly disseminate information and facilitate field agent emergency response. And the system supports IP videoconferencing for training, coordination, and conferencing to military personnel across the globe.

The Cisco Crisis Management Application lets military organizations expand the reach of their responses, increase their communications frequency, and reduce the limitations of location and time—saving lives in a crisis situation.

CONCLUSION

Defense organizations around the world have concluded that NCO should be the cornerstone of their strategic plans for the transformation of forces. Officials at the highest levels of government recognize the strategy's ability to create unique advantages for combatant and noncombatant operations. In its report to Congress, the U.S. Department of Defense stated that "the central hypothesis of network-centric warfare is that a force with these capabilities can increase combat power by better synchronizing effects in the battlespace, achieving greater speed of command, and increasing lethality, survivability, and responsiveness."

By adopting NCO, defense organizations can not only substantially increase their capabilities and access to critical information, but can also operate in a more fiscally efficient and effective manner. Cisco Systems is proving itself to be the leader in defense networking, providing the expertise, solutions, and partnerships to enable the military to take full advantage of all available information. With an effective NCO strategy, global defense agencies will be fully prepared to meet the challenges of a dynamic operational environment in the years to come.

For more information, please contact your Cisco account team or visit:

<http://www.cisco.com/go/defense>

BIBLIOGRAPHY

Cisco Systems White Paper:

Scalable Mobile Architecture for Tactical Communications

Cisco Systems White Paper:

Theatre-Independent Tactical Army & Air Force Network (TITAAN)

U.S. Department of Defense Report to Congress

Network-Centric Warfare, July 31, 2001

**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. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R) DP/LW7688 01/05