



IP-BASED NETWORKS SUPPORT DEFENSE TRANSFORMATION

Services and Defense Agencies Can Achieve Their Goals of Operating More Effectively and Efficiently By Migrating Their Operations to a Network-Centric Model Using Standards-Based IP. IP-Based Networks Improve Interoperability, Resilience/Survivability, Security, and Efficiency Through the Convergence of Data, Voice, and Video onto a Single Infrastructure.

A Cisco Intelligent
Network White Paper



WHITE PAPER

IP-BASED NETWORKS SUPPORT DEFENSE TRANSFORMATION

Services and defense agencies can achieve their goals of operating more effectively and efficiently by migrating their operations to a network-centric model using standards-based IP. IP-based networks improve interoperability, resilience/survivability, security, and efficiency through the convergence of data, voice, and video onto a single infrastructure.

SUMMARY

Information technology plays a key role in delivering the actionable information that the defense establishment needs to deal with new threats to security and stability around the world. Today, defense operations are largely based on proprietary, point-to-point networks. These networks hamper the flow of information in several ways, including: a lack of interoperability, which results in inaccessibility of information, limited access to computing and communications resources due to a lack of ubiquitous connectivity, and the inability of proprietary networks to adapt and support modernization.

In the commercial world, companies have migrated to IP-based infrastructures in order to respond to global competition and adapt to fast changing market demands. This transformation has demonstrated how standards-based IP networks can make organizations more responsive and adaptable. Similarly, IP-based networks can help enable services and defense agencies to streamline information flow, integrating the complex array of proprietary networks, systems, and applications that support military operations.

The benefits of moving to IP-based networks include the ability to run a wide variety of applications over a unified network, solve the problem of incompatible radio communications, and promote collaboration between military personnel, joint forces, coalition partners, and even civilian agencies for disaster relief.

Originally designed for the military, a packet-switching IP network is also designed to provide greater resilience and survivability by retransmitting and rerouting packets around any broken segments.

In addition, IP-based networks can be secured as well as or better than proprietary networks, using a defense in-depth strategy based on a combination of secure connectivity, threat defense, and trust and identity management.

Lastly, network-centric operations based on IP provide the foundation for convergence. The ability to transport and manage voice, data, and video over a unified infrastructure offers services and defense agencies substantial cost savings in network administration and recurring communications costs. Beyond cost-savings, agencies can take advantage of a virtually unlimited variety of advanced applications that can contribute significantly to the effectiveness and efficiency of defense operations and Homeland Security.

CHALLENGE

In order to defeat smaller, more agile adversaries, services and defense agencies are redefining themselves to operate with a higher level of effectiveness and preparedness. Traditionally monolithic and highly centralized, today's forces are relying more heavily on stealth, precision weaponry, and reduced manpower. Decision-making cycles are being shortened at all levels. Collaboration and information sharing are becoming increasingly important for geographically dispersed personnel, joint forces, and coalition partners. Military branches must now deploy troops in new multilevel, multifunction reach operations or split-based operations without cutting them off from vital information.

This transformation requires extending the power of information to every aspect of the organization. By putting timely, accurate information in the hands of the right people in the right location, agencies can gain a significant strategic and tactical advantage over a threat. In other words, defense superiority is strongly dependent on information superiority.

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.”*

Network-centric operations describes a real-time operational model designed to securely deliver actionable information throughout the chain of command anytime, anywhere. In warfare, actionable information can come in the form of intelligence, surveillance, or reconnaissance. Actionable information is also key to command and control and logistics. Consider the advantages this information could provide if it were all simultaneously broadcast from a single network across the chain of command down to battlefield operating systems.

Today, the defense industry is built on disparate communications systems including proprietary, point to point networks that make it virtually impossible to access and share critical information. These networks hamper the transformation of services and defense agencies for the following reasons:

- Lack of interoperability creates silos of information, making it expensive, inefficient, and sometimes impossible to share intelligence or resources located on other systems.
- Information scattered across disparate systems—including proprietary enterprise systems; Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance (C5ISR) Systems; weapons and sensor systems; and service provisioning or logistics systems—makes it difficult for personnel to obtain the complete picture they need for fast, confident decision-making.
- Point-to-point communication limits access to computing and communications resources; as a result, either the information is unavailable, or military personnel and staff must travel to get it.
- Legacy and proprietary networks offer limited scalability to support thousands of simultaneous users.
- Proprietary systems are more expensive to maintain, diverting resources from other programs.
- Proprietary systems are not easily adaptable, which hinders modernization and the ability to readily adapt and change.

SOLUTION

Commercial enterprises, large and small alike, have responded to intense global competition by moving to standards-based networks based on the Internet Protocol (IP). This transformation has gaining momentum in the defense sector as well.

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

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

IP-based networks can provide a more robust, resilient, flexible, and secure foundation upon which all defense inter-process and inter-system communications can be built. These are some of the things that make IP compelling for the defense establishment:

- Interoperability
- Efficiency
- Resilience/survivability
- Security
- Convergence for adaptability and modernization

INTEROPERABILITY

Interoperability is the ability of dissimilar computers, networks, operating systems, and applications to “talk” to each other effectively and dynamically (i.e., without special programming or extensive reconfiguration). IP promotes interoperability in multiple ways:

As the TITAAN project demonstrates, applications can be developed independently of the network layer of the IP protocol stack. This means that agencies can run a wide variety of custom and off-the-shelf applications over a unified network infrastructure, rather than having to build special-purpose applications for special-purpose networks.

In addition, IP can be used to communicate across any set of interconnected networks and is equally well suited for LAN and WAN communications.

IP can also help solve one of the biggest obstacles to communications in the field — incompatible radio communications (e.g., VHF, HF, or UHF). Thanks to the emergence of IP, vendors now offer solutions for connecting different radio networks across an IP network. This is a revolution that can help save lives, as demonstrated in recent military exercises in the United States and Australia.

For example, one of the objectives of the Joint User Interoperable Communications (JUICE) ‘04 exercise was to validate secure, IP-enabled interoperable voice communications in an emergency situation. During the exercise, the National Guard’s network, GuardNet, successfully connected with the radio networks operated by Homeland Security, the local police, highway patrol and others. Multiple radio base stations were all connected over an IP network, allowing them to communicate with each other regardless of radio frequency.

The JUICE exercise used products that were available commercially, to ensure that the demonstrated interoperability could be duplicated in small agencies. This breakthrough offers a new level of effectiveness for joint and combined operations. Whether fire, police, and ambulances are responding to a civilian emergency or military organizations are engaged in maneuvers, IP interoperability has helped break down the walls that previously kept agencies from communicating effectively with each other.

EFFICIENCY

One of the limitations of today’s stove-piped systems is the inefficient use of expensive bandwidth. Circuit-based telephony requires dedicated bandwidth whether circuits are in use or not. For example, if a field operation runs separate circuits for voice calls and data transmissions, there is no way to share bandwidth even if one application is idle and another is at bogged down due to high volume. With a converged IP-based network services and defense agencies can share bandwidth among multiple multi-media applications, using quality of service to provide service guarantees to mission-critical or delay-sensitive applications. This frees up circuits to connect more military units on land, sea, or air.

IP-based networks also facilitate the use of RF technologies, such as wireless, to support rapid deployment of military personnel in remote areas.

RESILIENCE/SURVIVABILITY

The development of IP-based networks traces back to a study commissioned by the U.S. Air Force in the 1960s on maintaining command and control over missiles and bombers after a nuclear attack. A packet-switched network that ensures if packets are lost at any given point, the message can be resent by the originator.

One of the key attributes of an IP-based network is that it offers this level of resilience. If the most direct route is not available, IP routers can direct traffic around the network via alternate routes.

Another dimension of IP's resilience is the fact that, unlike older communications systems, IP was designed to be agnostic to the underlying physical medium. This means IP packets can be routed or rerouted over wired networks, like copper wire, coaxial cable, and fiber optic, and over the entire RF spectrum, such as wireless, line of sight, satellite communications, and laser.

SECURITY

There is a popular belief that proprietary networks are more secure networks, but, as recent security breaches of government networks by hackers has demonstrated, this simply isn't the case. There are two important advantages to securing IP networks: the ability to implement a defense in-depth strategy and the ability to secure a converged network with a single security system.

Defense in-depth: With an IP infrastructure, agencies can create a "defense in-depth strategy" to prevent unauthorized network access, mitigate worm attacks, and circumvent denial of service attacks. A defense in-depth security solution includes secure connectivity, threat defense, and trust and identity management. This comprehensive safeguarding of network assets enables military organizations to maximize network uptime and productivity, while minimizing threat impact.

Secure convergence: Today's systems are "stove piped," that is, agencies create separate networks for voice, video, and data applications. This means that each network, circuit, and application has to be secured separately, adding greatly to cost and management complexity and creating obstacles to systems interoperability. An IP-based network creates a common, converged infrastructure that allows agencies to run voice, data, and video applications on one network with one security system, while facilitating interoperability.

CONVERGENCE FOR ADAPTABILITY AND MODERNIZATION

The adoption and integration of new and improved technologies, capabilities, concepts, and processes into defense establishment planning and operational activities is important to the modernization of the military. A converged network can play a critical part in enabling agencies to identify new ways to facilitate collaboration and increase organizational flexibility while reducing operational costs.

Convergence alone can cost-justify the migration to an IP network. The cost savings include:

- Saving on the cost of investing in and maintaining separate networks
- Freeing up IT and telephony staff for strategic projects
- Saving on a wide range of telephony costs, including long distance charges between locations, cell phone costs, and telephone lines

Beyond cost-savings, however, is the broader benefit is the ability to deploy new applications that can take advantage of converged network capabilities. For example, CENTRIXJ, the bilateral network between the U.S. and Japan for maritime operations, adds voice over Internet Protocol (VoIP) to a data network. This provides the foundation for services like an on-line directory of military personnel accessible from IP phones.

CONCLUSION

For hundreds of years, information has been an important part of military strategy and tactics. Confronted with new types of enemy threats and the need for more coordinated efforts with other military and civilian agencies and allies, services and defense agencies recognize that they must transform their technology infrastructures to deliver real-time access to actionable information, anytime, anywhere. As the U.S. Department of Defense states in its "Network Centric Warfare" report, "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." Using standards-based IP networks is a critical step in helping break down the silos of information and "help lift the fog of war."

**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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, 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, TeleRouter, 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. (0502R) 205341.B_ETMG_KW_6.05