



Photo courtesy of the Department of Defense.

IP and the military

IP has already been adopted as the standard for the US DoD and European MoDs and the next generation Internet Protocol IPv6 is being implemented. GMC looks at the impact that IP is having on the battlefield and the platforms that support it.

The Internet Protocol (IP) is the method by which data is sent from one computer to another on the Internet. Every host, or computer, on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that reads the destination address and forwards the packet to an adjacent gateway that reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate domain. That gateway then forwards

the packet to the computer whose address is specified.

IP does not involve connections, which means that there is no continuing connection between the end points that are communicating. The packets are independent units of data. IPv4 is the version that is used today but the introduction of IPv6 is starting to happen. This version has wider capabilities and will facilitate new applications.

Why is IP suitable for the military

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 US 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'.

We are all familiar with the term network centrality, and we know that in the field of war today, accurate and timely decision-making is paramount. The dissemination of information to the right people at the right time and reaching those in geographically dispersed locations, in harsh environments is crucial...and no-one, not one of those troops can be left out of the circle of information. Network centrality relies heavily upon the provision of real time information. The military need to know when and where something happens when it happens. A few minutes delay is not acceptable and could affect the outcome of a decision that is taken. If information can be simultaneously broadcast down the chain of command the advantages would be invaluable.

IP can bring together the various different communications systems under one umbrella, one standard, and can allow interoperability and therefore information sharing to all who require it. This may be achieved with Commercial-Off-The-Shelf (COTS) products – a sure way to reduce costs of implementation.

Internet Protocol is the standard that can support all the applications required by the military today. In fact, IP was originally designed for use by the military. Today many communication providers are asked by military customers for full IP technology and a wide range of platforms due to its flexibility and simplicity.

Applications supported by IP include:

- Imagery;
- Email;
- Voice;
- Video;
- Instant messaging;
- COTM; and
- VoIP.

IP is expected to play a very significant role in facilitating network centric warfare. This will fall to the fact that IP is an interoperable standard and that it is widely accepted. This also makes it cost effective. It is the ideal standard and bedrock for a new generation of defence systems. Since the early days of IP, things have significantly improved in terms of security, QoS management, mobility and multicasting. At the end of the day, IP-based networks offer interoperability, resilience, security and efficiency through a single infrastructure that delivers the vital data, voice and video services required by today's forces.

The defence industry does have specific requirements for IP such as real time networks and radio communications and it must be acknowledged that when the initial military systems were deployed IP was an emerging technology and migration to the next phase – IPv6 – will take time. However, it has been acknowledged that IP will be the key to network centric warfare.

Cisco and EADS to deliver IP for military

Defence and Communications Systems, an integrated business unit of EADS DS, and Cisco announced at DSEi 2007, that they have entered into a memorandum of understanding to define areas of collaboration in the development and delivery of Internet Protocol (IP)-based networking solutions. The collaboration is planned to reach across research and development and go-to-market business activities internationally to deliver future technologies in defence and se-

curity.

Leaders in the fields of systems integration and highly secure communications, EADS DS and Cisco will work together to advance current IP-based communications networks to support more rapid and more secure information sharing, collaboration and situational awareness for frontline forces.

As military and civil protection forces depend increasingly on IP-based networks, the assurance of timely, highly secure and reliable communication - particularly in mission-critical situations - is both a growing priority and an increasing challenge. At the same time, new challenges come with the unprecedented diversity of roles required of the armed forces and the complexity of threats they face, which demands new capability for their IP communications. For example, it is essential that their networks allow communication between personnel in the air, on land and at sea, as well as with other national or international forces.

Hervé Guillou, CEO of Defence and Communications Systems said, "This is a progressive response to evolving key requirements in defence and security markets. We aim to utilise our respective technologies to make new solutions and Network Enabled Capability a reality earlier. The EADS DS /Cisco collaboration will provide customers with a unique level of expertise and knowledge, and the ability to deliver better products in a more timely and cost effective way."

"Today, Internet Protocol networks are an essential part of business, education, government and home communications, and Cisco IP networking solutions are the foundation of these networks. Global defence organisations are increasingly moving to IP as an efficient means to transform the way military units, which are increasingly mobile and multinational, can seamlessly and securely exchange information with industry-leading security to improve decision making," said Chris Dedicoat, President of European markets for Cisco. "Using the expertise of both our companies, this collaboration with EADS shows our commitment to developing innovative solutions for the defence industry."

The memorandum of understanding builds on a history of successful teamwork between the two companies. EADS DS has worked with Cisco to adapt and customise its technologies and products for a range of high-profile projects. As early as 1995, EADS DS incorporated Cisco technology into a local data communications network for the UK's Royal Air Force and both companies continue to work together successfully deploying solutions on the UK MoD's Defence Information Infrastructure Programme and on Skynet 5, EADS' next generation military satellite communications programme.

FALCON

BAE Systems Insyte has been awarded a contract to provide the British Army with an information infrastructure system - FALCON, valued in excess of £200m, which is due to enter service in 2010.

FALCON will support the Army's command systems by providing a new high capacity, secure information system infrastructure capability at the operational and tactical levels of command that can be deployed rapidly by air into any theatre of operations. The system has greatly improved data throughput, multi-level security, mobility and manpower efficiencies compared with current systems.

The Bowman tactical system and Cormorant command system will feed information into FALCON, which will be able to link back to UK headquarters using the Skynet 5 satellite communications system. In line with the Defence Industrial Strategy, FALCON is key to the 'Resilient Information Infrastructure' of Network Enabled Capability (NEC) by providing the modern, secure communications infrastructure required by deployed formations and operating bases.

Martin Sheppard, IPT Leader Theatre and Formation Communications Systems (TFCS) said: "BAE Systems and its FALCON Partner companies bring a unique blend of expertise to this project. Their combined experience, together with the solution they are providing will equip senior commanders with one of the world's most advanced



The decision to move towards IP as a standard for all military systems seems to make perfect sense. It is cost effective, may be implemented using COTS equipment, even for military purposes, it is interoperable and it can support all required military applications. Photo taken by Mass Communications Specialist, Seaman Stephen Rowe. Photo courtesy of US Navy.

and powerful digital communications network for controlling combat operations at Corps, Divisional and Brigade level. The signing of this contract represents a very important step in support of network-enabled operations."

BAE Systems Integrated System Technologies (Insyte) partners include SELEX Communications, Thales, Cisco, Dytechna, Flagship and ASA.

Clive Richardson, Managing Director of Insyte said: "BAE Systems is delighted to be awarded this significant contract, we will work hard with our partners and customer to make FALCON a resounding success, through the entire life of the system."

FALCON will introduce the IP technology that is used in the commercial sector to the military. Here, it will meet new challenges and threats and will operate in a very different environment.

Trilogy Mercury

Based in the UK and US, Trilogy supplies audio communications and infrastructure equipment to broadcast, defence, emergency management and commercial and industrial sectors. Its Mercury IP Audio Communications System provides an ideal platform for use in the military context.

The Trilogy Mercury IP Audio Communications System is comprised of one or more Mercury PCI Cards, Mercury USB devices or Mercury Interface Units (MIU). These devices, known as Mercury hosts, are equipped with 8 to 32 IP audio channels. IP audio channels are dynamically allocated to support two-way communications over an IP network. Multiple IP channels can be used simultaneously to conduct communications with any combination of other Mercury hosts distributed on the enterprise. Examples of call types include point-to-point, group and conference calls. Communications capacity grows when Mercury is deployed on multicast-enabled networks. Multicast conferencing makes it possible for hundreds of users to communicate using bandwidth efficiently. If required, IP audio

channels can be reserved for use as static audio trunks or for emergency communications.

The Mercury product line also includes a variety of hardware or software panels with up to 256 one-touch buttons or keys. Panels provide users with a single, unified method of communicating with any other device incorporated in the Mercury enterprise. Because Mercury is a multichannel intercom platform, users can monitor and engage in multiple voice communications simultaneously. Combined, these features can dramatically improve the speed and agility of voice communications within an organisation.

Mercury is an all in one communications platform that allows an organization to leverage every voice communications asset across the enterprise. In addition to providing intercom capability as a Mercury host, the Mercury Interface Unit is designed to provide interoperability with a wide variety of communications devices in a space-efficient manner. Each unit can be equipped with any combination of four internal hardware expansion modules. Audio, radio and telephone options provide enterprise-wide interoperability with:

- Mercury intercom panels;
- Legacy intercom systems or other 4-wire audio devices;
- Radios of all types;
- Conventional telephones, cell phones, satellite phones (FXS, FXO, E&M); and
- SIP phones and SIP PBXs.

Unlike many other IP communications and interoperability products, there is no need to add external interconnect hardware and audio conversion devices. At 2U high, the MIU uses very little rack space and is simple to install, integrate and manage.

Once in place, any combination of devices can conduct two-way communications locally or over the network - intercom-to-intercom, intercom-to-radio/telephone/SIP phone, radio-to-radio, and so on. This



enables powerful communications capabilities such as connecting a cell phone user at one site to a two-way radio user at another. Dynamic and static conferencing between radios of different types is possible on a local or world-wide basis. A landline connected to an MIU in one country can be made available to Mercury users anywhere on the globe. The communications capability is limited only by what is determined to be suitable for the application.

For applications that don't require communications over IP, the Mercury Interface Unit can be used as a standalone intercom or interoperability platform with no reliance on an external PC or network.

All Mercury products are designed to operate with standards-based IT and network technologies - no special routers, switches or gateways are required. A Mercury system can be constructed using network infrastructure ranging from something as simple as a five port switch to a global terrestrial and satellite based network.

Mercury uses protocol stacks that are optimised for the types of communications involved. They are:

- **Trilogy Transparent Mode:** This protocol provides the fastest connections with the lowest latency. Intercom, radio, and 4-wire audio are transmitted using this method. It is reliable, faster, and uses less bandwidth than other Voice over IP protocols. First used over five years ago, this protocol is uniquely well-suited for multichannel communications over IP and is only available on Mercury.
- **Trilogy Switched Mode:** This protocol is used for handling conventional telephony over IP. It extends the reach of these communications assets over the IP network and makes them accessible to other communications devices that are a part of the Mercury enterprise.
- **Session Initiation Protocol (SIP):** Use of this protocol makes Mercury interoperable with SIP phones and SIP PBXs.

Security is implemented at the network level and standards-based encryption devices including VPN can be used transparently. The system is designed to give administrators precise control over all relevant system, network and security parameters including administrative access and speak and listen privileges for each user. Mercury has been deployed on multiple military networks around the globe following rigorous security and intelligence community scrutiny. In some cases Mercury is being used to provide an audio communications bridge between classified and unclassified networks.

Software for tactical IP networks

Twisted Pair Solutions has introduced WAVE 3.0, the latest version of its widely deployed and proven unified group communications software. With feature enhancements that significantly improve the ease and speed of deployment, operational resiliency and the security of mission-critical group communications networks, WAVE 3.0 is highly focused on the needs of defence and civilian government agencies, public safety and emergency management groups and large commercial operators in transportation, energy and finance.

"WAVE 3.0 delivers the next generation of unified group communications capability," said Tom Guthrie, Twisted Pair's President and CEO. "We've taken the industry's most trusted voice technology and made it more flexible, scalable and resilient. WAVE 3.0 and its associated software development kit further positions our solution development partners to create robust and market-specific products and hosted services to address critical operational integration, business continuity and interoperability needs."

WAVE 3.0 helps organizations of all types and sizes to take control of their unified group communications requirements by allowing multiple radio systems, IP and traditional telephony devices to seamlessly and securely interoperate across a wire line or wireless, terrestrial or satellite-based IP network. WAVE 3.0 is built on the WAVE Communications Framework which has been widely deployed

in mission critical environments and has thousands of users worldwide. WAVE 3.0 software addresses a critical need for secure and reliable unified group communications between networks of differing capability and performance. Network managers can quickly configure WAVE 3.0 to support any network type, enabling full communications interoperability across Multicast, Unicast and mixed-mode networks. Already trusted worldwide as a mission critical solution, WAVE 3.0 now enables continuous, uninterrupted group communications regardless of device, network or operator failures. Irrespective of failure type - PC hardware, operating system, Ethernet connection - WAVE 3.0 can be designed to instantly recognise the failure and self-heal so communications can continue uninterrupted.

A new WAVE Mobile Communicator client for PDAs allows users to turn their Windows Mobile 5 device into a multi-function radio. By allowing users to monitor and access multiple voice channels from a single screen, WAVE 3.0 combines unequalled communications access and user mobility.

WAVE 3.0 has been designed to reduce bandwidth requirements to a minimum while maintaining full communications connectivity. This is particularly important to emergency deployments where allocated WAN bandwidth can become congested. Superior security is further improved so that WAVE 3.0 deployments require fewer firewall configurations in a large WAN environment.

Essential data scalability

Renowned for its ability to allow scaling to thousands of real-time voice users without creating adverse network load, WAVE 3.0 also is enhanced with a highly scalable data distribution infrastructure enabling text messages, status and presence and, in future releases, GPS coordinate mapping.

As well as being the de facto standard for software managed voice interoperability, WAVE is the only standards-based software solution that offers a Software Development Kit (SDK) for wider application development. Six of the top ten US defence integrators and many in Europe, including NATO and Australia have used the WAVE SDK to develop their own custom applications for unified voice, video and data.

The future - IPv6

IPv6 will gradually replace IPv4, although the two versions will exist side by side for some years as part of the replacement process. The principal difference between the two versions is the fact that IPv6 increases the amount of address space from 32 to 128 bits, providing a virtually unlimited number of networks and systems. This new, 'next generation' of IP is ideally suited to the military (for which IP was originally developed anyway), as it supports QoS parameters for real time audio and video - vital applications that form a crucial part in network centric warfare. The US Department of Defense issued a mandate some time ago to move to an IPv6 platform by 2008 for all military and defence sectors.

IPv6 Offers:

- A much larger address space;
- Multicast;
- Jumbograms (a packet that is larger than the usual size limit for a given technology);
- Network layer security (Ipsec is an integral feature to IPv6); and
- Mobility (key for military users).

The right move

The decision to move towards IP as a standard for all military systems seems to make perfect sense. It is cost effective, may be implemented using COTS equipment, even for military purposes, it is interoperable and it can support all required military applications. IP fully supports the move towards a network centric military environment where the entire battlefield is connected and it could become a reality much sooner than we think. ■