INTERNET PROTOCOL COLLABORATIVE MOBILITY

Norman L. Hanson*
TRW Systems, Tactical Systems Division
Carson, California 90746

ABSTRACT

In Objective Force mobile tactical network environments, critical capabilities are required for allowing nomadic users to migrate from one system to another without man-in-the-loop or network management interactions. This summary presents Internet Protocol Collaborative Mobility (IPCM), a new approach to serving mobile users in such communication environments.

1. INTRODUCTION

Mobility in the Objective Force tactical environment takes many forms. *Mobility* is commonly used in reference to physical motion of a person, vehicle, or group of vehicles. Another form of mobility—*user mobility*—is the changing association of a person, vehicle, or group of vehicles between groups (subnets). As elements physically move about, user mobility network mechanisms must be able to track and deliver information to wherever an element has migrated.

Internet Protocol Collaborative Mobility (IPCM) is a user mobility mechanism that operates completely above the session layer and does not burden the network layer with tracking and location of mobile users. The IPCM specific approach targets the collaboration of currently available commercial off-the-shelf (COTS) software and hardware, guided by intelligent agents, providing required mobility functionality above the session layers.

2. USER MOBILITY REQUIREMENTS

Objective Force User Mobility requires mobile users to maintain communication within the organizational group and when moving from group to group. Supporting continuous communication, two modes of operations are required:

Mode 1: Break before Make - where a user moves between two groups and is not able to maintain continuous link connectivity.

Mode 2: Make before Break - where a user moves between two groups and maintains physical link connectivity to both groups for a short period.

3. IPCM APPROACH

IPCM achieves user mobility using standard network services that include Lightweight Directory Access Protocol (LDAP) Directory Service (DS), Domain Name Service (DDNS) with Dynamic Update, and Dynamic Host Configuration Protocol (DHCP) coupled with intelligent agents in both clients and servers.

IPCM achieves collaboration between the user and standard network services by employing intelligent agents (both client and server based) operating above the network layer. This approach requires no modification to network layer routing and supports both unicast and multicast operations. End-point host hardware, operating system, networking software, and application software remain unchanged with the addition of IPCM since intelligent agents facilitate the necessary mobility services.

Agents will replace man-in-the-loop operations (user or interactive management) by detecting migration events and initiating DHCP reaffiliations (without power down or restart of the host), managing parameter updates, and executing service migrations. IPCM agents implement collaboration between the standard services, client operating systems, and server operating systems.

The primary responsibility for user migration detection and re-homing is within the mobile client, in the form of the IPCM client agent (IPCMcA). IPCMcA accomplishes mobility by monitoring link metrics and traffic source addressing within the current group. When mode 1 or mode 2 changes are detected, the user is autonomously re-homed.

An IPCM server agent (IPCMsA) will communicate with the IPCMcA and determine what server-based services (e-mail, etc.) require migration to the new home group. Migration decisions and re-homing of a client do not rely on modification of standard network and link layer protocols. IPCM moves the mobility task out of the network and link layers. IPCM uses the application through session layers for managing, tracking, and migrating users with transparent (no user interaction required after initial login) operations.

4. IPCM COMPARISON WITH MOBILE IP

The Mobile IP approach imposes a series of restrictions that are sub-optimal in Objective Force tactical mobile environments. Mobile IP assumes a degree of overall network stability that tactical networks may not possess. Connectivity to the mobile user depends on the survival of the Mobile IP Home Agent (HA) to complete the communication path. Under tactical conditions, however, survival of the HA is by no means ensured. IPCM re-homes the mobile user rather than relying on the HA to complete the connection to the visiting user. Once re-homing is complete, the visiting user is no longer vulnerable to loss of the HA.

A Mobile IP visiting user carries an original IP address with any devices (the devices are still *homed* in the original group). Routers serving the new group become unable to summarize address resolution fully, resulting in negative effects on routing scalability. By re-homing the users, use of the original IP addressing is removed, allowing the network layer to use summarization techniques unmodified, specifically unburdening the network layer from resolving complete IP addresses.

Because the Mobile IP visiting user's device generates packets using its original address as the source address, the ingress filters of the routers serving its new group normally would refuse to transmit its packets as part of a standard technique to combat distributed denial-of-service attacks. IPCM avoids this issue because the mobile user is re-homed and uses native IP addresses for the new group.

5. IPCM DESIGN, DEVELOPMENT, AND DEMONSTRATION

In 2001, prototypes and proof-of-concept demonstrations focused on the design and implementation of the IPCMcA for Mode 1 (Break before Make) operations.

The IPCMcA is a machine-level entity that stands in for a human user and executes all required activity necessary to re-home a client without requiring human user interactions.

IPCMcA software monitors the association to the current subnet by polling the status of the client LAN card for its associated access point. When detecting new associations, the IPCMcA initiates a DHCP release and renew to obtain an IP address for the new association.

The IPCMcA interfaces as an upper filter driver residing above the Aironet supplied device driver. Keeping the interface to the driver as high level as possible, a dynamic-link library (DLL) manages the interface to the filter driver.

IPCM prototypes have been successfully implemented using a combination of COTS software, Panasonic ToughBook laptop computers, Cisco Aironet 802.11b wireless networking, and development of the IPCMcA software.

Simple integration is the goal in assembling a proof-of-concept demonstration IPCM system. The required LDAP DS, DDNS, and DHCP standards-based services are available for Unix operating systems (Linux, etc.) and are part of the software suite delivered with the Windows 2000 server. Using the Windows 2000 server represented the minimal effort to construct a proof-of-concept environment since complete integration of the services required configuration only (no integration). Additionally, external routers were not required because the Windows 2000 server software release contains integral routing functions. The mobile user (client) OS selected was Windows 2000 Professional.

The system architecture consists of a number of sub networks, and groups, connected via wireless bridges. Each group has one server providing the required network services (LDAP DS/DDNS/DHCP). Demonstration system addressing uses IPv4. IPv6 is a viable choice as IPCM is independent of address structure; however, ease of integration is the driving factor for using IPv4.

ACKNOWLEDGMENTS

Contributors to the IPCM effort include: Frank Belz – Chief Engineer; Jeffery Smith – Software Development; and Mark Walter – System Administration.

CONCLUSION

Functional performance of the IPCM prototype shows that the mobility concept works extremely well. Clients may move freely between groups in the demonstration system with the IPCMcA managing the users migration, completely without human intervention.

The proof-of-concept system exhibits a lag in being able to locate a freshly re-homed client. An anticipation of lag in DNS location is inherent due to replication needs between group LDAP DS. Approaches exist for reducing the inherent lag and will be manageable for Objective Force tactical deployment.

The proof-of-concept demonstrates the ease in achieving user mobility with the IPCM approach. IPCM has the potential of being added to legacy tactical systems, such as the Army's Battle Command System (ABCS) applications, allowing mobility in their operation.