Military Messaging: Distribution and Profiling

Isode

This white paper looks at capabilities for distribution of messages to multiple recipients, which are used in Military Messaging but have wider applicability. It also looks at how these capabilities are provided in Isode's M-Switch product. It covers two key functions:

1. Message Distribution: distribution of messages to a list of recipients using specialized distribution list capabilities.

2. Profiling: distribution of messages based on message content.

Military Messaging

A description of Military Messaging and Isode's solution is given in the Isode white paper Isode's Military Messaging Handling Solution. Distribution of messages to multiple recipients is a critical function that this white paper explores. There are some aspects of military messaging that are important to understanding message distribution:

1. Military messages are sent between organizations, but mailboxes belong to roles which prepare and receive the messages on behalf of the organization, with users having access to one or more roles.
2. Military messages distinguish strongly between "Action" and "Information" recipients, where action recipients have formal responsibility for handling messages in specified timescales.
3. ACP 127 was the original military message handling system, and understanding how this operates is key to understanding overall requirements.

Message Distribution

Simple message distribution is essentially the function provided by email distribution lists, which send a message to multiple recipients.

ACP 127: CADs and AIGs

ACP 127 specifies two quite similar mechanisms for distributing messages: Collective Address Designators (CADs) and Address Information Groups (AIGs). CADs are often used to support distribution to Task Forces, Task Groups and Task Units, leading to names such as "TF 22".

CADs and AIGs work by local expansion on each node (identified by Routing Indicator (RI)) so that there is no single point expansion as in a standard email list. Messages are routed to all relevant RIs to ensure expansion.

The key distinction between CADs and AIGs is that AIGs distinguish between Action and Information members of the AIG, whereas CADs do not.

M-Switch Management of CADs and AIGs

M-Switch manages CADs and AIGs as global lists, following the model specified in ACP 133. This is done with a GUI that allows CADs and AIGs to be managed and shows membership and hierarchy of the lists. This global specification allows each node to perform local expansion and allows the first node to handle a CAD or AIG to correctly route the message to the other RIs that need to expand the list.

Limitations of CADs and AIGs

A significant limitation of CADs and AIGs is that they are restricted to ACP 127 and can only be used on an ACP 127 network and not on a military messaging network using modern protocols. A related problem is that CADs and AIGs are named globally (as unique strings) on the ACP 127 network where they are operated. This is fine on a small, closed network but would present significant problems in a more distributed environment.

NATO ALE

There is no open standard equivalent of AIGs for open protocols. However, in two procurements for the NATO Messaging System, NATO have specified detailed capability identified as Address List Expansion (ALE), which defines a list expansion mechanism that can provide AIG and CAD capabilities using STANAG 4406 or SMTP messaging. Key features of ALE

1. Membership distinguishes Action and Information recipients.
2. Nested expansion performs full duplicate address elimination.

M-Switch Distribution Capabilities

M-Switch provides a Military Distribution List capability that meets the NATO ALE requirements and provides a number of additional capabilities:

- Configuration and membership management (action and information) using Isode's Cobalt Web interface (shown above). Note that this is in support of organisational messaging, and so lists will typically contain organizations as members.
- List policy to control the message priority of expanded messages.
- Control of who can submit messages to the list.
- Control of attachments and maximum size, which can be important in constrained network environments and when lists have members receiving messages over ACP 127.

Profiling

Traditional email lists expand based on a set of list members. Profiling is an approach of distributing messages based on message content. This approach was core to ACP 127 operation, and it was expected that ACP 127 systems performed message profiling. The mechanisms for achieving this are not specified in ACP 127; this appears to have been left to vendor choice.

NATO have provided help here with NATO Messaging System specification issued in 2005 and 2018. The earlier specification specified detailed Profiler capabilities in the context of STANAG 4406, and the latter specification gave a more generic definition. Isode M-Switch provides a profiling capability that is aligned to both of these specifications, which is discussed in more detail below.

Protocol Independent

A key goal of the M-Switch Profiler implementation is to be protocol independent and to be able to work with STANAG 4406, ACP 127 and SMTP deployments. The profiler has full support for STANAG 4406 and SMTP operation, noting that management is oriented towards SMTP, which makes it convenient for use in conjunction with Isode's Harrier Military Messaging client. ACP 127 is supported by protocol conversion.

STANAG 4406 and SMTP use the modern messaging architecture of separating message header and envelope. ACP 127 does not have this distinction, which avoids the problem noted next. For content-based distribution, it is important that the original message is preserved, as this is the message being considered. However, a receiving client needs to be aware of action and information recipients to perform correct processing. This is achieved by forwarding the message so that both profile information and the original message are distributed. This can then be picked up by the client, as shown below:

This message has been sent from organization "JOINT HQ" to organizations "ROME" and "NAVCOM". The message has been profiled for "NAVCOM" and delivered to the role mailbox "COMMANDING OFFICER". This message is recognized as a profiled message by Harrier and details of profiling information are expanded. Points to note:

1. The original message is clearly displayed for the user to see and process
2. The message is clearly marked as "not processed" with a precedence dependent target action time shown.
3. Profiling details show the action and information recipients, indicating clearly that the current mailbox is an action recipient.
4. The priority of the profiled message is FLASH, as NAVCOM is action recipient with FLASH priority and COMMANDING OFFICER has been profiled as an action recipient at NAVCOM.

Multiple Profiles & Profile Management

The NATO model is that profiles can be shared between organizations. Where this happens, profiling is done at the same time for all of the organizations in the profile, for each organizational recipient of the message. This reflects the overlapping nature of some organizations and ensures that roles will only receive one copy of a given profiled message. It also allows organizations to share profiling rules.

Profiling makes use of a Profile and an M-Switch server will be configured with a single profile that reflects the list of organizations being profiled by the server. In a high availability scenario with active/active M-Switch servers, multiple M-Switch servers will use the same profile.

Profiles are stored in an M-Vault ACP 133 directory, which can be highly replicated to provide reliability. Multiple M-Switch servers can access the same profile. An M-Switch server will cache the current profile and will monitor M-Vault for updates.

The Profile is managed by Cobalt, which is used for user, role and organization provisioning and described in the Isode white paper Provisioning for Military Messaging Handling Systems. This is a natural place to manage profiles. In particular:

- Cobalt manages the profiled organizations, so these can be easily selected.

- Cobalt manages role based mailboxes for the organizations, so these can be easily selected as action and information recipients in profile rules.

Cobalt can manage multiple profile versions. One profile is always marked “active”, which is the one which M-Switch will use. This versioning has two benefits:

1. Version management, so that profiles can be updated and tested, with fall back to older versions when needed.
2. Support of multiple scenarios and rapid switch between them. For example, scenarios could be maintained for "war" and "peace", or a special temporary scenario developed in support of an exercise.

Rules

The core of the Profiler function is a set of rules, which determine how the set of action and information recipients for a given message are determined. This section starts by looking at the SIC (Subject Indicator Code) rule as an example of how rules work. SICs are used in Military Message to specify what the message is about and are often central to the choices on message distribution. NATO SICs are three letters, and national SICs are usually “letter digit letter”. A message will typically have a small number of SICs to clearly indicate topic.

The UI for an SIC rule is shown above. Key points to note:

1. Rules are independent objects that can be independently created and edited, with each rule named.
2. Rules have different types, with UI appropriate to the type. This one is an SIC rule.
3. There is a list of target organizations, which can be selected from known organizations. This is important where multiple organizations are being profiled, to specify which organizations the rule applies to. If omitted, the rule applies to all organizations being profiled.
4. SIC or SIC pattern. In this example an exact SIC ("CCC") is specified, but it is also possible to specify SIC patterns such as CC* or *C, which enable a rule to be defined for a range of SICs.
5. Action and Information recipients are specified for the rule.

A set of SIC rules can be specified to give coverage for messages with any combination of SIC values. Cobalt provides a UI to show for every SIC which action and information addresses will be used, which will enable an operator to review that all SCIs are handled appropriately.

In addition to the SIC rules, the following additional rules are supported.

- Local. This provides a default rule that can be used to define default handling for an organization if no other rules match.
- Originator. A rule based on matching the message originator, so handling can be controlled based on which organization a message came from.
- Address List. This rule functions as match on recipients specified in the message. The intended use of this is for when a message is sent to an address list which contains a local organization. This rule enables special handling for this situation.
- Keyword. This rule provides a free text search of a keyword on message subject or message body. It can be used to define handling of messages with specific words in.

- Instructions. This rule provides a match with Message Handling and Message Instruction fields, so that specific handling can be defined for messages with certain instructions.

This set of rules gives a comprehensive and flexible profiling capability.

There is an additional rule type, "out of hours", which is rather different to the other rules. There is a model of "working hours" during which the standard rules apply. At other times, the standard rules still apply, but out of hours rules allow for additional recipients to be assigned, based on message priority. This supports a model where routine messages can be left for processing until working hours start, but higher priority messages should also go to a duty officer who can determine if expedited processing is needed.

Manual Profiling

It is anticipated that Profiling will usually be a fully automatic function. There are two situations where this is not possible:

1. At the end of rule processing, it is possible that no recipients have been identified for a given message.
2. A message contains a special SIC, which NATO defines as AAA, ABA, ACA and ADA. In this case, manual processing is mandated.

In this case, profiled messages are handled by the web UI shown above, which allows an operator to inspect a message and to manually assign action and information recipients.

Conclusions

This whitepaper has given an overview of Isode M-Switch support for message distribution comprising:

- ACP 127 AIGs and CADs
- Military distribution lists providing all AIG and CAD functionality with modern protocols and comprehensive distribution going beyond standard distribution lists.
- Profiling to distribute messages based on message content.

Isode

www.isode.com

14 Castle Mews, Hampton
Middlesex, TW12 2NP

Secure, Seamless Communication Solutions