AUTOMATIC CONFIGURATION AND RECONFIGURATION IN DYNAMIC NETWORKS[1]

A. McAuley*, D. Chee, J. Chiang, S. Das, K. Manousakis[2], R. Morera, L. Wong, K. Young
Telcordia Technologies, Inc.
Morristown, NJ, 07960

ABSTRACT

The Objective Force requires rapidly deployable and survivable networks. To support these requirements the entire tactical battlefield network, possibly consisting of thousands of hosts, routers and MANET nodes, must be autoconfigured. Moreover, the networks must be rapidly reconfigured as conditions or requirements change. This paper presents an approach to plug-and-play and survivable networking using our IP Autoconfiguration Protocol Suite (**IPAS**). We describe the protocols, how they do server reconfiguration, and their interworking with non-IPAS (e.g., COTS-based) nodes.

1. INTRODUCTION

Today, it takes a day to configure even small networks (e.g., 50 node), and the resulting network is fragile and unable to adapt to changing environments. Larger networks, such as Task Force XXI, can take weeks to design and build. Efforts in the Internet community are focused on the more limited objective of autoconfiguring static hosts and small networks (e.g., using DHCP [Droms97] and IPv6 stateless autoconfiguration [Thomson98]). This paper presents our radical approach to configuring and reconfiguring an entire network (routers, servers, hosts…), possibly consisting of tens of thousands of nodes. Section 2 describes the modular components in our IP Autoconfiguration Protocol Suite (IPAS). Section 3 describes its application to FCS and section 4 gives some experimental results.

2. IPAS MODULES

At the heart of IPAS (see Figure 1) is the Dynamic Configuration Distribution Protocol (**DCDP**) [McAuley01]. DCDP is a robust, scalable, low-overhead, lightweight (minimal state) protocol designed to distribute configuration information on address-pools and other IP configuration information (e.g., DNS Server's IP address, security keys, or routing protocol). Designed for dynamic wireless battlefield, it operates without central coordination or periodic messages. Moreover, DCDP does not rely on a routing protocol to distribute information.

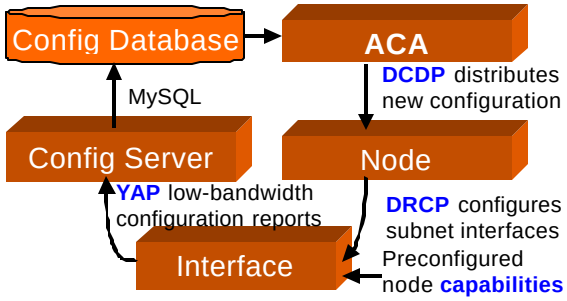

Figure 1 IPAS components

DCDP relies on the Dynamic and Rapid Configuration Protocol (**DRCP**) to actually configure the interfaces. DRCP borrows heavily from DHCP, but adds features critical to roaming users. DRCP can automatically detect the need to reconfigure (e.g., due to node mobility) through periodic advertisements. In addition, DRCP allows for: a) efficient use of scarce wireless bandwidth, b) dynamic addition or deletion of address pools to support server fail over, c) message exchange without broadcast, and d) clients to be routers.

The Configuration Database Update Protocol (**YAP**) is a simple bandwidth efficient reporting mechanism for dynamic networks. YAP has three elements: 1) Clients running on every node periodically report its node's capabilities, configuration, and operational status, 2) Relays forwarding information from clients to a server, and 3) Server storing the information in a configuration database (see Figure 1). The *capabilities* say, for example: "This node can be a DNS server with priority 0" or "a YAP server with priority 3" (priority reflecting a node's willingness to perform a function). Other YAP information includes name and IP address, Rx/Tx packets, bit rate, link quality, routing table, and address pool.

The brain of IPAS is the Adaptive Configuration Agent (ACA). The ACA can even reset the network and distribute a new address pool from human input or from a

[1] This work was supported by the U.S. Army Research Laboratory. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.
[2] Kyriakos Manousakis is currently pursuing a Ph.D. at the University of Maryland. This work was done during summer internship at Telcordia.

predefined private address pool (e.g., 10.x.x.x). Through the Configuration Database (filled by YAP), ACA observes the state of the network, which allows it to initiate reconfiguration based on its rules or policies.

3. APPLICATION TO FCS

The IPAS just described meets the rapidly deployable and survivable requirements in FCS as it a) automatically configures the network through DCDP and DRCP b) reacts to node mobility by reconfiguring nodes when they move from one subnet to another (through DRCP) and c) reconfigures servers (DNS) without any manual intervention.

IPAS provides robustness for server failure. The ACA detects when the DNS server has not reported for some time, i.e. the server has lost connectivity with the YAP servers or failed. Then, ACA selects a new node to provide this service (based on nodes capabilities) and advertises it as the new server through the configuration protocol (e.g., DCDP/DRCP). This automatic reconfiguration provides a high degree of server survivability that is more powerful than merely having preconfigured backup servers. However, ACA must use a different method to replicate itself (bootstrap problem), as the ACA node can also fail. Each node having the capability of being an ACA listens to periodic hello messages multicast by the current ACA. If a node does not hear this message for some time, it assumes that the ACA failed or connectivity has been lost and randomly self-elects based on its capabilities. The self-elected node immediately broadcasts messages to all other nodes.

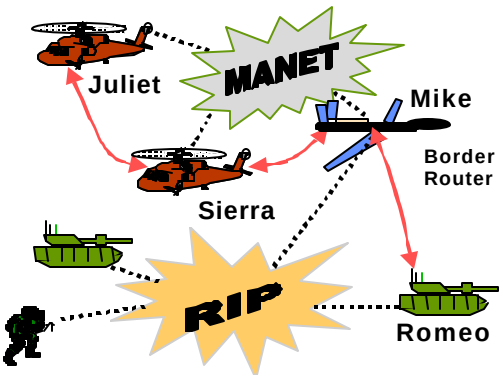

Figure 2 Two-Domain Testbed

Figure 2 represents six Linux laptops in our laboratory demonstration. IPAS configures nodes running both a conventional routing protocol (i.e., RIP) and a MANET routing protocol (i.e., AODV). Other experiments have demonstrated the interoperability of IPAS configured nodes with manually configured nodes (e.g., CISCO routers). By tunneling IPAS messages through non-IPAS nodes, the manually configured nodes can even be located in the middle of the IPAS configuration domain.

4. PERFORMANCE ANALYSIS

Figure 3 shows the configuration time for different types of network topologies as a function of number of nodes. These results are based on mathematical extrapolation from experimental results obtained from chains of between 2 and 10 nodes. The minimum time of just over 4 seconds is due to DRCP initially checking for an existing DRCP server (this is a settable parameter). The "linear network" gives the worst-case configuration time, assuming all nodes are routers in a sequential chain. The "single subnet" gives the best-case configuration time, assuming all nodes are on a single subnet. The "distributed network" gives a more typical network, with the networks made up of subnets connected in a mesh pattern and configuration being initiated in one corner.

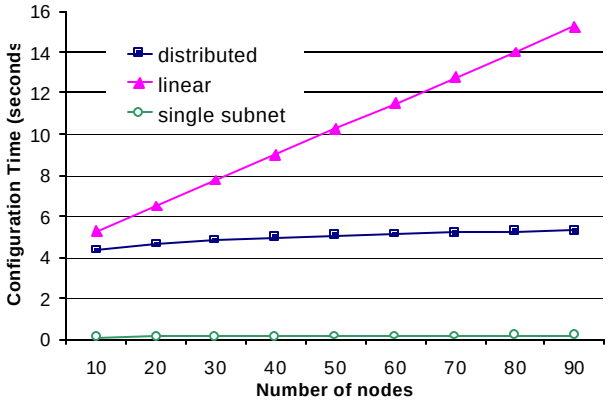

Figure 3 IPAS Configuration Time

REFERENCES

Droms, R., "Dynamic Host Configuration Protocol," RFC 2131, March 1997.

McAuley, A., Misra, A.,Wong, L., Manousakis, K, "Experience with Autoconfiguring a Network with IP addresses," IEEE Milcom, October 2001.[i]

Thompson, "IPv6 Stateless Address Autoconfiguration," RFC 2462, December 1998.

CONCLUSION

The IP Autoconfiguration Suite (IPAS) here described, not only reduces dramatically configuration time (minutes rather than days or weeks in large networks) by automatically configuring entire networks (routers, servers, hosts…); but also, meets the survivability requirements in FCS by reconfiguring mobile nodes and servers without any manual intervention. This makes IPAS very attractive for future battlefield network configuration.

---

[i] The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied of the Army Research Laboratory or the U.S. Government