Military University of Technology

Faculty of Electronics

Ph.D. Thesis Abstract

The management of border routers configuration in tactical IP networks

Author: **kpt. mgr inż. Krzysztof MAŚLANKA**
Supervisor: **prof. dr hab. inż. Marek AMANOWICZ**
Auxiliary Supervisor: **ppłk dr inż. Jarosław KRYGIER**

To achieve information superiority during future tactical operations, a robust command and control technical infrastructure is required. Soldiers must be equipped with a capability to exchange information on a battlefield in a timely and correct manner. Most of the current military networks are based on the Internet Protocol (IP) technology.

To achieve better management abilities, the IP-based tactical networks are divided on the Autonomous Systems. Moreover, such topology is a natural network architecture in multinational operations. Thus, it is important to ensure interactions between the autonomous systems without any central regulator, in plug and operate mode. Communication between the autonomous systems is achieved by gateways (border routers), located at the borders of these systems. The routing information exchange between the ASs is typically performed using the Border Gateway Protocol (BGP), which is the standard for the exterior gateway routing in the IP-based networks.

However, the BGP was constructed to the relatively static networks. In its standard implementations, it requires manual configuration to establish connections between BGP peers. Such configuration of the BGP routers cannot be acceptable in tactical networks, therefore additional mechanisms for automatic configurations and reconfigurations are needed. To solve this problem a new SYstem of Border Router Autoconfiguration (SYBRA) is elaborated. Following thesis is proved in this PhD dissertation: the peer-to-peer

(p2p) technology can effectively support BGP-based border routers autoconfiguration in tactical networks with dynamically changing topology.

The p2p system is a set of equivalent entities (nodes) that communicate each other to exchange information in order to share resources without any central element. It is assumed that the BGP-based border routers are the p2p nodes. The resources shared between them create reliable distributed database that contains the information necessary for routers configuration during network creation and in case of network topology change.

The SYBRA enables BGP routers to automate the process of discovering peers in adjacent autonomous systems and the process of establishing connections between them. Additionally, it enables BGP speakers that belong to an autonomous system to discover and monitor the main border router to maintain iBGP connections during splitting and merging the autonomous system. Moreover, if isolated border router is discovered, the SYBRA allows to connect this router to the other autonomous system. Each abovementioned mechanisms allow limiting the effects of the loss of network consistency in disruptive tactical environment.

The SYBRA was implemented in a Linux-based routers and its functionality and effectiveness was examined in emulated network topologies. An autoconfiguration response time measured in border routers equipped with SYBRA not exceed 40 seconds in worst case, while a traditional, manual configuration of equivalent networks would require even tens of minutes. The cost of the configuration flexibility is an additional signalling traffic generated in the network that should be considered in particular SYBRA usage. Thereby, it was proved that the p2p system can effectively support border routers autoconfiguration in dynamically changed network environment.