BGP-Based Routing Configuration Management for Multidomain Mobile Networks

J. Krygier, K. Maslanka, K. Wolszczak
Military University of Technology
Faculty of Electronics
Kaliskiego 2 str., 00-908 Warsaw, Poland

{jkrygier, kmaslanka}@wel.wat.edu.pl

ABSTRACT

The paper presents the mechanisms designed for automatic BGP-based routing configuration in a network composed of the mobile autonomous systems (domains). Each autonomous system can be attached to other automatons system using one or more links, detached or can be moved to other position and attached again. This situation is a typical for military multinational operations. The proposed mechanisms extend the network management system to exterior routing configuration in dynamically changed topology.

1.0 INTRODUCTION

Routing in the Internet in is mostly based on BGP protocol [1]. The Internet is in fact the composition of autonomous systems (AS), each of them is independently administrative. Routes are chosen based on the calculation of the shortest path given by the number of ASs that need to be traversed.

From communication point of view, the tactical network is characterized by mobility often in a low bandwidth environment. All functions deployed in this environment should be adapted to be sustainable in mobile, link-impaired conditions. Applications and protocols that have been designed to work in static networks, do not necessarily behave as expected in the tactical domain. This is also valid for routing protocols between autonomous systems. Since BGP is mandatory for NATO Network and Information Infrastructure Services (NIIS) [2][3], especially in multinational operations, we have to propose the mobility support mechanisms that can be applied in multidomain IP network.

It is important, because the BGP protocol have to be configured in advance in border routers, mostly by hand, knowing peering associations. It is because the BGP uses the TCP protocol in order to reliably carry the routing messages. To start TCP sessions it is necessary to statically configure peers in both border BGP routers. It is problem when BGP is used in military tactical networks, where connections between peers could be often changed because of AS movement or other reason of connection lost. It need to get involve administrative entities in both disconnected ASes and in AS where new connection is established. This could exclude BGP protocol in dynamic tactical environments.

A problem also exists with long convergence time in the networks using BGP protocol. BGP was designed to be used in networks with stable inter-AS connections. Convergence problems were widely considered in the past and were summarised in [4], [5] and [6]. For example, in [4] the problem with inter AS connection in mobile military network is discussed. The BGP-based network mobility problem was also considered by Global Information Grid Routing Working Group and was discussed in [7] and [8]. Solution for IPv6 mobile networks connecting to the GIG using big address space and IPv6 multihoming, supported by DHCPv6 protocol was proposed in [9]. Also Dul in [10] and [11] presented implementation of the mobility method used for commercial aircraft to allow global IPv4 network mobility using BGP protocol and satellite network architecture. In [12] routing architecture for the future IP-based Airborne Network is

presented. BGP is used there as an internal and external routing protocol.

The solution described in this paper is dedicated to the multidomain, multisystem mobile military networks based on the TCP/IP protocols stack with BGP as an exterior gateway protocol.

Figure 1 shows an example of multidomain mobile network composed of many autonomous systems. Also three cases of autonomous system mobility are shown here. The thirst one represents the system that appears in the network and the border routers have to be configured to see their appropriate peers.

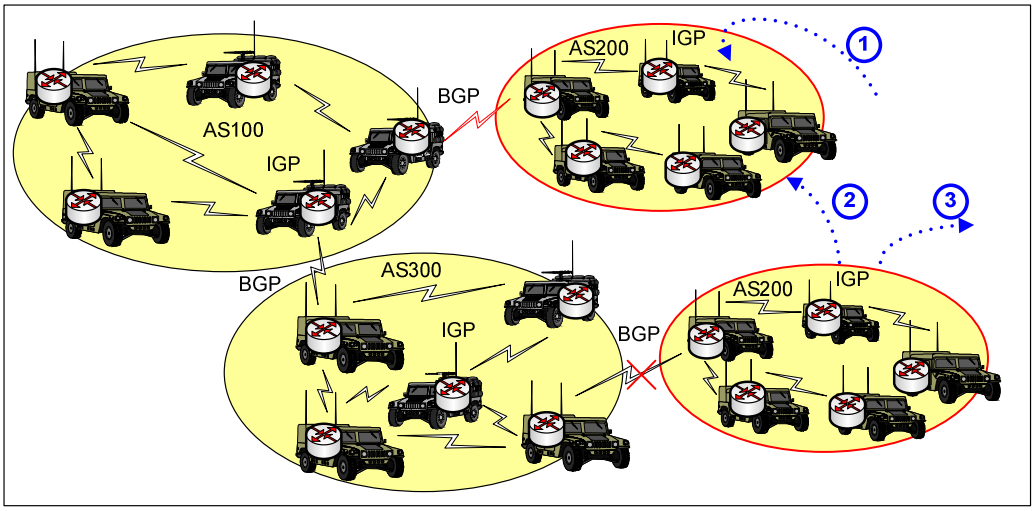


Figure 1: Multidomain mobile network

The second case represents a movement of the system to a new position. All current external BGP connections have to be terminated and the new peers have to be associated. The third case applies to the situation in which an AS leaves the network and the remaining routers have to clear their configuration. All these cases show that additional mechanisms should be applied in the network in order to configure an external routing automatically.

The authors proposed distributed management layer that is responsible for exchanging routing policy messages between the external routing configurations managers located in each autonomous system. Configuration managers are also responsible for border routers configuration. Appropriate protocols were elaborated for AS interoperability points for internal configuration.

2.0 REQUIREMENTS

In order to support autonomous systems mobility, the border routers have to be able to automatically reconfigure their routing daemons depending on the mobility action. It is assumed that IP network domains can also be autonomous systems, and they have to be connected to other autonomous systems, disconnected from the network, move to another location and connect to the network again and finally they can organise more than one links to another autonomous systems. All this actions have to be performed automatically. An autonomous system border router (ASBR), equipped with the BGP functionality, is responsible for appropriate traffic routing and routing policy.

Typically, border routers with BGP are configured by hand or automatically, but with known peering and routing policy information in advance. On the contrary to the interior routing protocols (i.e. OLSR), the BGP is not equipped with the neighbour discovery mechanism. The peer router addresses and the peer

autonomous systems numbers have to be known in advance in order to configure the router. Also traffic management policy has to be agreed in advance.

In order to elaborate the BGP-based routing configuration management mechanisms, following requirements have been assumed:

1) Autonomous systems routing policy have to be managed centrally. Supervisor/manager is responsible for configuration of ASBRs using accessible network configuration protocol and appropriate manager's application.

2) Autonomous system border routers have to be equipped with at least one interface dedicated to communication with other autonomous systems. This interface should be based on the common data link technique with broadcast capabilities (i.e. the Ethernet).

3) Each ASBR has to be equipped with a routing management agent that is able to communicate to the manager application.

4) Appropriate configuration management protocol has to be used (elaborated) between the manager application and the agents.

5) The ASBRs have to be able to detect exterior peering routers.

6) The BGP-based routing configuration management mechanisms have to support:

    a. Exterior link detection and neighbor discovery.

    b. Automatic discovery of active routing configuration agents.

    c. Automatic exterior interface IP address configuration.

    d. Management communication between AS managers, managers and routing agents and between routing agents.

We have also initially assumed that configuration management mechanisms will be used for BGPv4 (IPv4). Nevertheless, they can be easily extended to the MP-BGP (IPv6).

3.0 CONCEPT OF BGP-BASED ROUTING CONFIGURATION MANAGEMENT MECHANISMS

We have assumed that each autonomous system has its own traffic management policy, handled by the central manager located in some element of the network. The manager is able to manage the border routers (ASBRs) via the agents located in the managed routers. The manager IP address is known by each agent, and then active agents can register themselves in the manager.

Let us assume three basic autonomous system mobility scenarios depicted in Figure 2. The ASBR with BGP has to detect its exterior neighbor routers during new ASs attachment (a) or during attachment additional ASBR (b). It is possible by the exterior link detection procedure described below. Also the agent located in the router has to inform its manager that new AS has been attached. After the link detection process the peer agents communicate each other in order to transfer information about the AS numbers (ASN) allocated to their ASs, and information about the IP addresses of the neighboring managers. After that, each agent transfers this information to its home manager. Based on this information the managers elect the main manager, which is responsible for global addresses allocation to the common

link between the ASs. The main manager selects the addresses from its address pool and informs its agent. The agent receiving the message with the new addresses, informs its peering agent from the new AS, and then the neighboring (slave) manager. Now both managers can start ASBR configuration procedure.

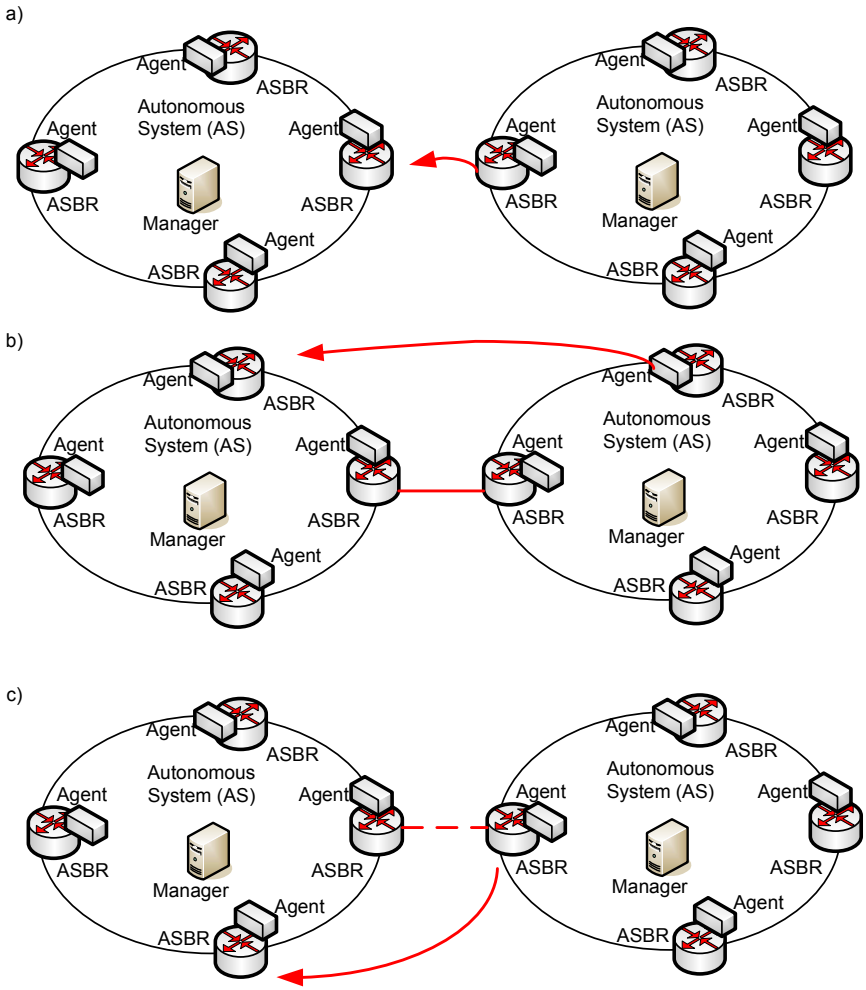


Figure 2: AS mobility scenarios

The ASBR configuration procedure is responsible for:

- Router addresses configuration.
- BGP pearing configuration.
- Security configuration (traffic management policy).

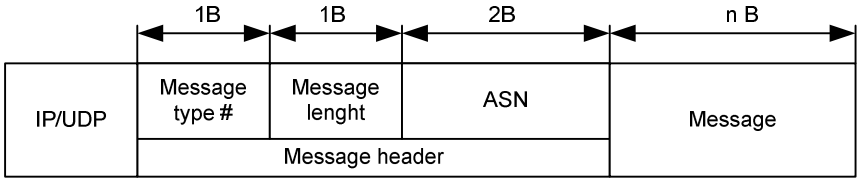
The AS can also move to a new possession what enforce a need of ASBR reconfiguration (c). The agent located in the ASBR has to detect inaccessibility of the neighboring router and has to send information to the manager in order to reconfigure the ASBR.

Each ASBR in autonomous system is responsible for detection of attached router belonging to the

neighboring AS. It than requires a link detection and neighbor discovery mechanism. Our solution was initially planned to be used in IPv6 networks and than the proposed mechanism is based on the IPv6 Multicast Listener Discovery Protocol [15] run in the ASBR. Additionally, the exterior interfaces of the ASBR have to be appropriately configured in order to handle the IPv6 Neighbour Discovery Protocol [14]. Attaching a new border router to the ASBR each router starts sending the Multicast Listener Report (MLR) to the all nodes IPv6 multicast address (FF02::1). Even though the border router is not a part of some multicast group, it should send the MLRs from the router's link-local addresses. These messages are next used by the remaining routers on the link for extracting the sender's link-local address.

Flow diagram of BGP-based routing configuration management mechanisms is presented in Figure 3. The diagram presents a set of messages flow in two scenarios: the ASs are not connected together before the link detection procedure (as in Figure 2a) and the ASs are already connected together via another link (as in Figure 2b). All used messages are listed in Table 1.

In first case, after agents activation in the border routers belonging to different ASs (ASN 100 and ASN 200 in our example) each agent registers itself in the manager using message type 0 (Msg type 0). After mutual connection of the ASs, the border routers send the IPv6 MLR message in the exterior links. If the ASN100 border router receives this information it learns the IPv6 source link-local address and sends the message type 1 with the ASN100 manager address and the ASN (detailed format of the messages is shown



in

Figure 4).

This address is then sent via the message type 2 to the ASN200 manager. In the mean time the ASN200 border router receives the MLR messages from the ASN100 router. Similarly, it send the message type 2 to the ASN100 manager, informing about the ASN200 IP address and the ASN. Based on the information about the neighbouring ASN and comparing to its own ASN, each manager selects the maser manager as the manager with the lower ASN (ASN100 in our case). Then the ASN100 manager sends the message type 3 to its agent informing the agent about the network global IP address selected to the exterior link configuration. This information is then resend via the message type 4 to the neighbouring agent IPv6 link-local address, and finally via the message type 5 to the ASN200 manager. After this sequence both managers start configuration their ASBRs (addresses and peering) using NETCONF SSH session [16].

In the second case, when the systems have been already connected via another link, the managers already know the parameters of this connation (managers addresses and the ASNs). Then, after link detection procedure using MLR protocol and after sending of messages type 1 and 2, the master manager sends the message type 7 directly to the slave manager, informing about the selected network global IP address which should be allocated to the new exterior link.

If the exterior link disconnection is detected by the border routers (as in Figure 2c), each ASBR sends the message type 8 to the managers. After this sequence both managers start reconfiguration their ASBRs (clearing the addresses and peering) using NETCONF SSH session.

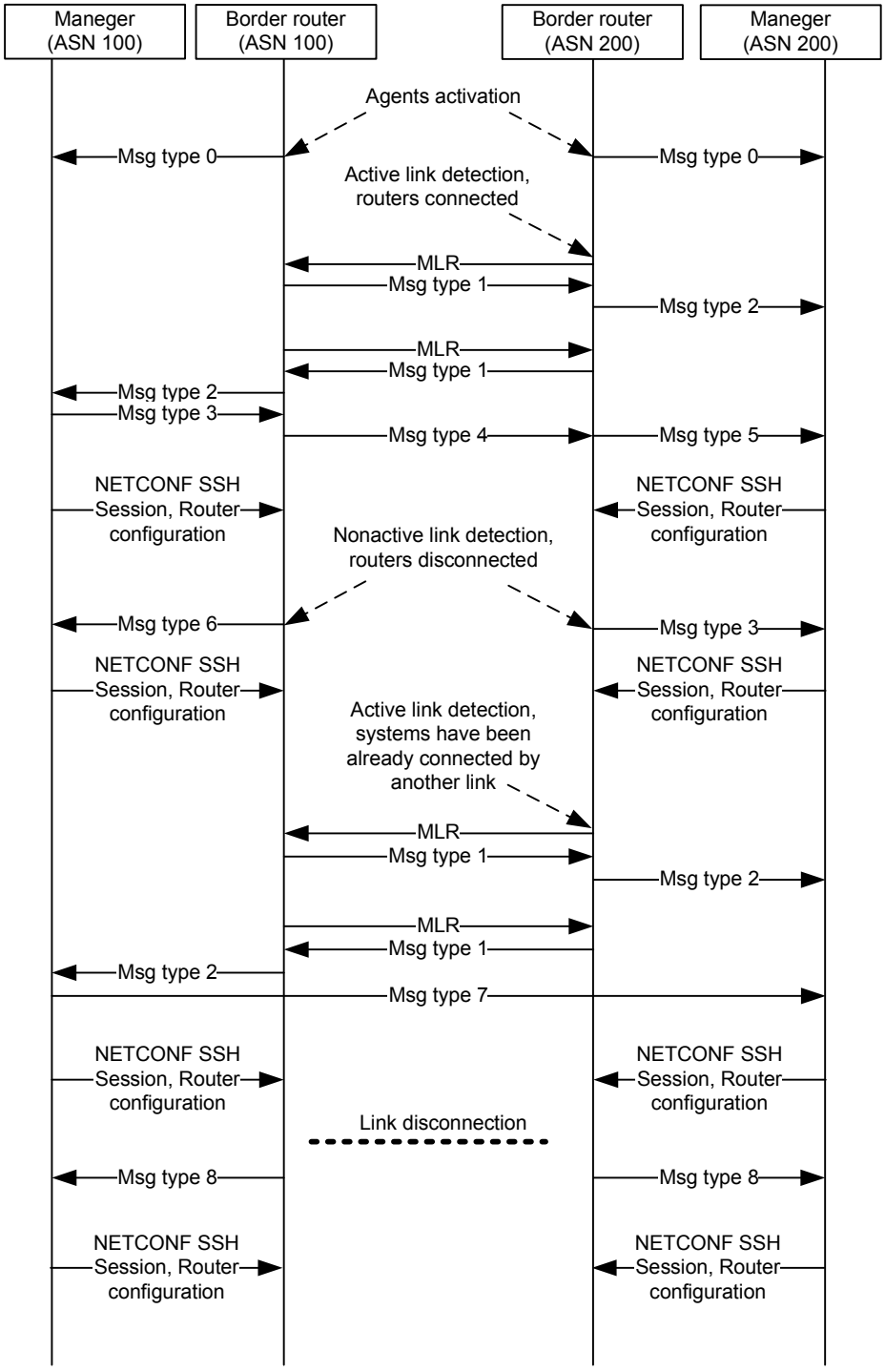


Figure 3: Flow diagram of BGP-based routing configuration management mechanisms

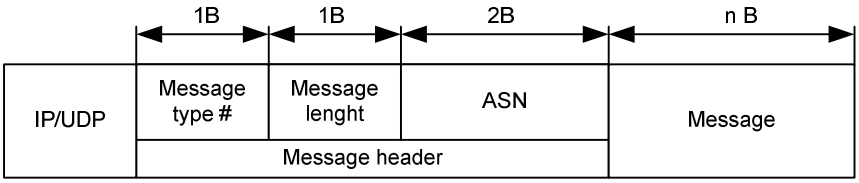


Figure 4: Format of link detection and configuration messages

Table 1: Link detection and configuration messages

Message type #	Message length [B]	Message	Message description
0	4	Agent IP address	Message sent by the agent to the manager. Message informs the manager about the IP addresses of its agents and border routers.
1	4	Manager IP address	Message sent by the agent to peer exterior router (agent) to inform its correspondent about the ASN and the manager IP address.
2	4	Manager IP address	Message sent by the agent to the manager. Message is sent after receiving message type # 1. It informs the manager about the ASN and the manager IP address of the exterior system
3	4	Network address	Message sent by the master manager to the agent in response to message type # 2. It informs the agent about the network address delegated to the link between the autonomous systems.
4	4	Network address	Message sent by the agent to the exterior router (agent) after receiving the message type # 3 from the manager. It informs the exterior agent about the network address delegated to the link between the autonomous systems.
5	4	Network address	Message sent by the agent to the slave manager after receiving the message type # 4 from the exterior router (agent). It informs the exterior agent about the network address delegated to the link between the autonomous systems.

6	4	Agent IP address	Message sent by the agent to the manager after disconnection detection between the systems. It informs about the agent IP address.
7	4	Network address	Message sent directly from the master to the slave manager, after correctly configured BGP parameters in border routers. This message is used to configure another link between the systems. The message informs the slave manager about the network address delegated to the new link configuration.
8	2	N/A	Message sent by the agent to the manager after detection of the exterior link disconnection.

4.0 IMPLEMENTATION

All the proposed mechanisms was implemented and tested in the network composed of the Linux-based routers with Quagga [17] routing software with BGPv4 daemon. The Ensuite (YencaP, YencaP-manager) open source application was used for quagga routers configuration. EnSuite is a network management platform prototype based on NetConf. It aims at providing to the network management community an open source environment not only to test the NetConf configuration protocol, but also to test new features [16][18]. EnSuite is composed of two applications: Netconf Manager and Netconf Agent. Both applications was used to perform BGP protocol configuration in the ASBRs.

The proposed in section 3 mechanisms was implemented in Python programming language. Following new modules was implemented:

1) Management agent - located in the ASBR (besides the YencaP agent), responsible for neighbour detection and retransmission of the prepared messages.

2) Manager – located in some device in the autonomous system, typically in the same device as the YencaP-manager. The manager is able to communicate with the YencaP-manager, in order to transfer the information about the parameters which have to be configured in the ASBR via the NETCONF protocol.

The communications between the managers and the agents was secured using SSH protocols.

5.0 VERIFICATION RESULTS

Functional tests

The mechanisms were verified in the lab testbed composed of two autonomous systems with interior and border router. A simplified scenario is shown in Figure 5. Two types of tests were used: functional and constraints tests. The goal of functional tests was to verify a correctness of the code, formats of messages and behaviour of the appropriate devices.

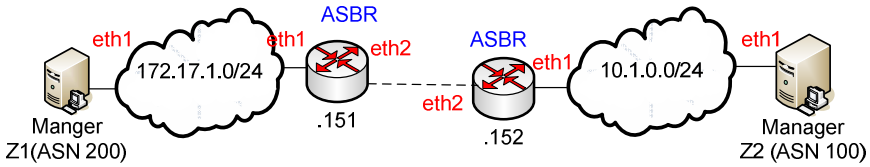


Figure 5: Simplified testbed for implemented applications verification

For example in the network from Figure 5, at the beginning the agents located in the routers .151 and .152 have to be registered in the managers (Figure 6 and Figure 7).

```
[root@v7-151 agent]# python agent.py
----------------------------------------
Activation info sent: my ASN: 200, my IP: 172.17.1.151
Activation info sent: my ASN: 200, my IP: 172.17.1.151
Activation info sent: my ASN: 200, my IP: 172.17.1.151
```

Figure 6: Listing in the agent located in router .151 (Activation info sent)

```
[root@v7-150 manager]# python manager.py
----------------------------------------
Agent active
Message type: 0
ASN: 200
IP: 172.17.1.151
```

Figure 7: Listing in the manager (agent activation)

Based on the MLR messages the border routers detect the IPv6 source link-local addresses of the MLR messages, and sends the message type 1 to their neighbours (Figure 8) and next to the neighbouring manager.

```
[root@v7-151 agent]# python agent.py
----------------------------------------
Neighbouring router's interface detected: fe80::217:9aff:fe7b:a943
Sending msg type 1 to neighbour: ASN 200, manager IP: 172.17.1.150
```

Figure 8: Agent discovered a neighbouring router

The neighbouring manager elect itself as the master manager and allocates the common network address between the systems, sending the message to its neighbouring manager via message type 3 (Figure 9).

```
[root@v7-153 manager]# python manager.py
----------------------------------------
Network address was selected: 172.18.1.0
Sending msg type 3
```

Figure 9: Maser manager allocates the network address between the systems

After these sequences, the managers configure the links and BGP protocol in the borders routers. Figure 10 shows the routing table in the router (which is also the manager) inside the system with ASN 200. We can see that there are visible routes to the networks from the systems with ASN100. Pings confirm the correctness of the configuration.

```
[root@v7-150 manager]# route -n
Destination     Gateway         Genmask         Flags  Metric Ref    Use    Iface
172.18.1.0      172.17.1.151    255.255.255.0   UG     2      0      0      eth1
10.1.0.0        172.17.1.151    255.255.255.0   UG     2      0      0      eth1
172.17.1.0      0.0.0.0         255.255.255.0   U      5      0      0      eth1
[root@v7-150 manager]# ping 10.1.0.153
PING 10.1.0.153 (10.1.0.153) 56(84) bytes of data.
64 bytes from 10.1.0.153: icmp_seq_=1 ttl=62 time=0.345 ms
64 bytes from 10.1.0.153: icmp_seq_=2 ttl=62 time=0.245 ms
64 bytes from 10.1.0.153: icmp_seq_=3 ttl=62 time=0.305 ms
```

Figure 10: Routing table in the router (manager) inside the system with ASN 200

Operation conditions

Besides the functional test, additional tests were performed to check the conditions in which the proposed mechanisms can be applied in multisystem environment [13]. Especially we were interested in the impact of the narrowband links or part of the network (typical in military networks) on the configuration management procedures efficiency. The tests were performed using testbed shown in Figure 11. The network is composed of two autonomous systems (ASN100 and ASN200). The systems are connected (disconnected) via the LanForge network emulator [19] used here in order to change the bandwidth between the systems. The network emulator is also located inside the AS (ASN200), but between the manager and the agent.

Two main tests were performed in order to check:

1) Time of neighbour discovery phase.

2) Time of automatic BGP configuration in the ASBRs.

Time of neighbour discovery phase was measured as the time between starting of connection of both systems together to the moment in which two workstations in each system (connected directly to the ASBR) can communicate each other. Time of automatic BGP configuration in the ASBRs is the time between receiving of the configuration request message by the manager and finishing the BGP configuration process (TCP connection is closed in NetConf session). In both cases, bandwidth was changed, affecting flow of messages (between the systems and between the manager and ASBR).

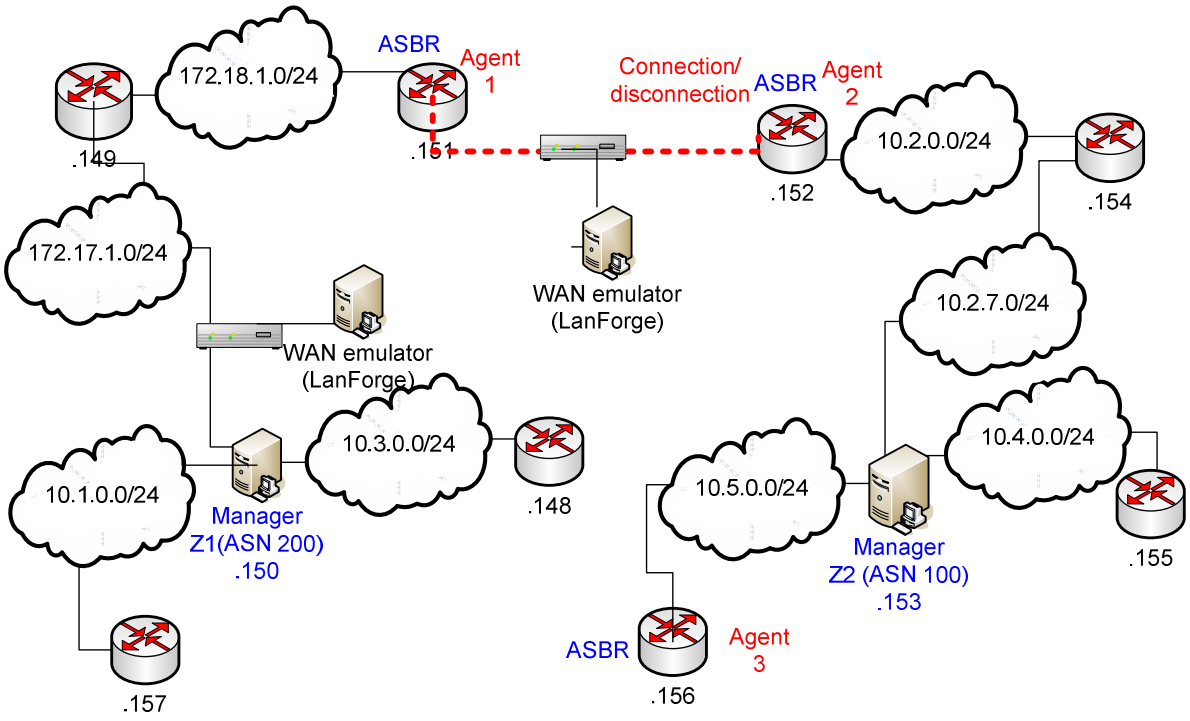


Figure 11: Testbed for validation tests

Figure 12 present the time of neighbour discovery phase while bandwidth between the ASs (using LanForge emulator) was changed from 2Mbps to 5kbps. We can observe that this time is drastically increased if bandwidth between the systems is lower than 30kbps. Below this level, the time of neighbour discovery phase does not exceed 2sec.

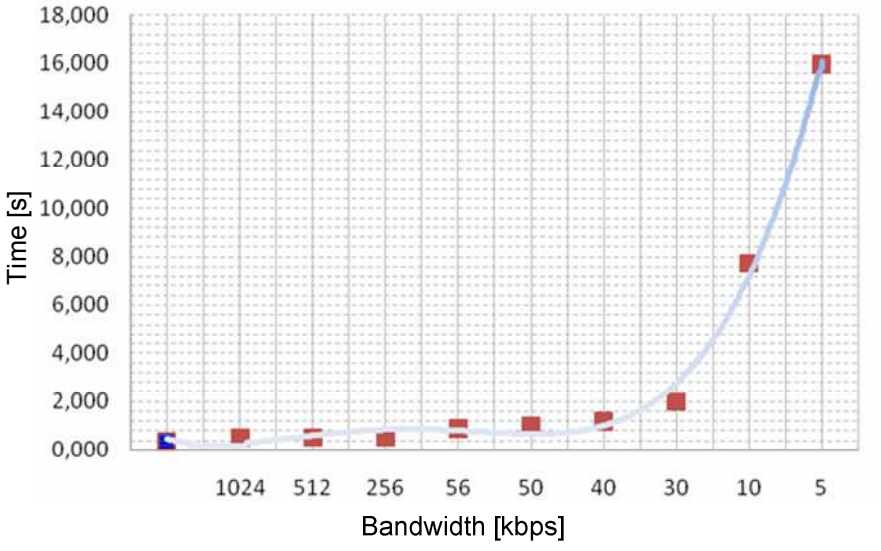


Figure 12: Time of neighbour discovery phase.

Time of automatic BGP configuration in the ASBRs is shown in Figure 13. In this case bandwidth was changed between the manager and the agent, also from 2Mbps to 5kbps. This time is significantly greater

than the time of neighbour discovery phase, but it mostly depends on the used routers reconfiguration time. Also this time is significantly increased while the bandwidth is lower than 30kbps.

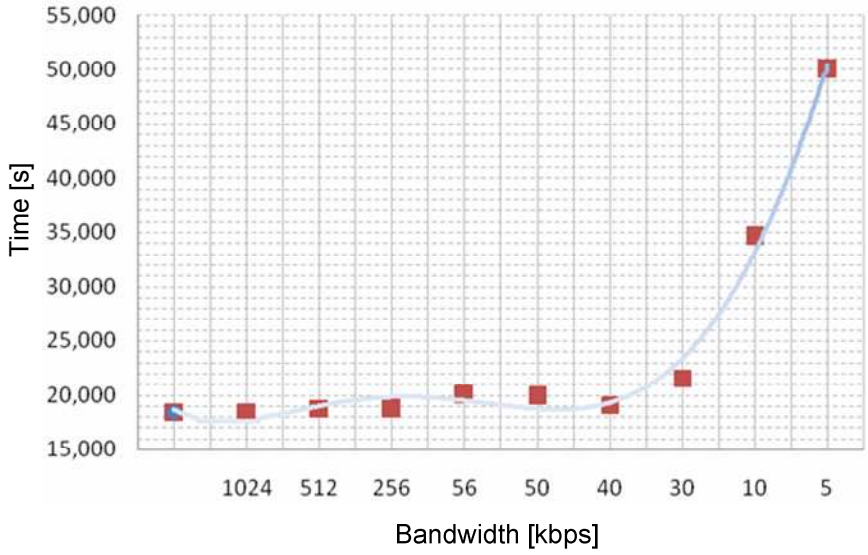


Figure 13: Time of automatic BGP configuration in the ASBRs

6.0 SUMMERY

The authors have proposed distributed management procedures that are responsible for exchanging routing policy messages between the external routing configurations managers located in each autonomous system. Configuration managers are also responsible for border routers configuration. After new link detection, global IPv6 addresses have to be configured on the external interfaces of the both border routers. The first communication is possible based on the IPv6 link-local addresses, after neighbour discovery phase. It gives a possibility to agree the common network addresses and peering information. This information is then transferred to the configuration managers, which enforce appropriate peering configuration.

The procedures were implemented and applied in the testbed composed of many autonomous systems (networks). A correctness of the implementations were checked by the functional tests. This paper presents only selected tests, but all tests confirm correctness of the implementation. Also tests performed to check the limitations of the network that can affect the procedures point out that it can be used in multidoamin network.

Application of these procedures and implementations in military environment should be preceded by improvement of the configuration time of the BGP-based routers and by elaboration and improvement of the security mechanism.

7.0 REFERENCES

[1] Y. Rekhter, T. Li, S. Hares: A Border Gateway Protocol 4 (BGP-4), IETF 01.2006

[2] Allied Data Publication 34: NATO Interoperability Standards and Profiles Volume 2, Version 2.0,

C3 CCSC NATO Open Systems Working Group, 02.2008

[3] NATO Network Enabled Capability Feasibility Study, 2005, NC3A,

[4] Ingvild Sorteberg, BGP Convergence in Military Coalition Networks, IEEE Military Communications Conference MILCOM 2004

[5] N. Kushman, S. Kandula, D. Katami, B. M. Maggi, RBGP: Staying Connected in a Connected World, NSDI '07: 4th USENIX Symposium on Networked Systems Design & Implementation, Cambridge 04.2007

[6] M. Yannuzzi, X. Masip-Bruin, O. Bonaventure, Open Issues in Interdomain Routing: A Survey, IEEE Network Magazine,Volume 19, 11.2005

[7] D. Street, Global Information Grid (GIG) Topology / Multicast Routing Requirements, GRWG Meeting 07.2006

[8] D. Street, IP Routing in the Global Information Grid (GIG) Problem Description / Requirements GIG Routing and Addressing Workshop (GRAW) 21/23 Feb 2007

[9] I. Sebüktekin, A. McAuley, Scalable and Secure IPv6 Solutions for Connecting Mobile Networks to the GIG, Communications and Networks Consortium, Telcordia Technologies Inc, Piscataway 11.2006

[10] A. Dul, Global IP Network Mobility using Border Gateway Protocol (BGP), Network Engineering – Connexion by Boeing 03.2006

[11] A. Dul, Global IP Network Mobility using Border Gateway Protocol (BGP), IETF 62, Minneapolis 03.2005

[12] S. V. Pizzi, A Routing Architecture for the Airborne Network, IEEE Military Communications Conference, MILCOM 10.2007

[13] K. Wolszczak: BGP configuration management mechanisms for multisystem IP networks (in Polish), M.Sc. thesis, supervisor: J. Krygier, MUT, Warsaw 2010,

[14] RFC 2461: Neighbor Discovery for IP Version 6 (IPv6), 1998

[15] RFC 2710: Multicast Listener Discovery (MLD) for IPv6, 1999

[16] RFC 4741: NETCONF Configuration Protocol, 2006

[17] http://www.quagga.net

[18] http://ensuite.sourceforge.net

[19] http://www.candelatech.com