IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

BAN: ACLs and Route-Redistribution

Vishesh S[1], Nidhi AJ[2], Manaswini S[2], Preethi R[3], Pratiksha D Bhandarkar[3], Murugheshgouda VH[3]

B.E, Department of Telecommunication Engineering, BNM Institute of Technology, Bangalore, India[1]

Student, Department of Telecommunication Engineering, DSCE, Bangalore, India[2]

Student, Department of Telecommunication Engineering, DSCE, Bangalore, India[3]

Abstract: Intra-body communication or intra-BAN and inter-body communication or inter-BAN are the two classifications under Body Area Networks (BAN). Body Area Network or BAN is a field of networking in which communication takes place between different sensors or network elements or other electronic components at the nodes within the body called intra-BAN and between two or more bodies called inter–BAN. In our previous paper [1] titled "BAN: intra-BAN and inter-BAN" with D01 10.17148/1JARCCE.2017.6756 we have successfully established communication between different routers /sensors at the node with the help of wireless communication protocols. Each node forwards packets to the destined location by selecting the optimal route for the packet to be transferred from the source to the destination. In this paper we configure Access Control Lists (ACL) or simply Access-list on routers placed at different nodes of the human body. The main purpose behind this configuration is for router packet filtering and traffic control. ACL or simply Access-list are a set of permit and deny commands to provide a powerful way to control traffic in and out of a network forwarding packets. It also provides additional security by denying host or IP addresses. In case of inter-BAN or inter-body communication, the two human bodies handshaking with each other may be running different routing protocols. In this case, route –redistribution needs to be done at the boundary routers which acts as a translator between the two routing protocols and the IPs advertised in one body can also be seen in the other human body running different routing protocols. In this paper the above configuration will be done and the results will be presented in a systematic manner.

Keywords: Access Control Lists (ACL), denying host or IP addresses, handshaking, router packet filtering and traffic control.

I. INTRODUCTION

Unlike Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network whose range/span/radius ranges from a few metres to several kilometres, Body Area Network consists of sensors, networking elements and other resourceful gadgets connected in a network within the human body of an individual. It may be embedded on or inside the body. The area of the body is the possible space for the packets to be sent and /or received by the components at the node. They forward packets to the destination nodes using dynamic routing protocols, static routes (when needed) and optimal route selection based on few predefined policies by the network admin. In this paper we attempt one such task in which ACL will be applied at the nodes which can actively filter the packets and control the traffic flow of packets.

Access Control List (ACL) or set of deny or permit statements to provide a powerful way to control traffic in and out of a network forwarding packets. It also provides additional security. In this paper we also perform route-redistribution at the boundary routers to connect two human bodies considered to have their own autonomous internal routing protocols and are different from one other. The above two configurations will be dealt with in the coming sections.

II. INTRA-BODY NETWORK

Intra-body network also called intra-BAN [2] is the communication that is established within an autonomous human body consisting of electronic components or networking elements at the nodes of the human body connected in a network using wireless connectivity and routing protocols. In our previous paper we have configured [3] IGP ie; OSPF on inter-body network which is a dynamic routing protocol.we have also used stratic routes wherever necessary. Figure 1 shows an intra-body network of interest.

Suppose an IP 1.1.1.1 on router at the head has tobe denied in the lower parts of the body but must be permitted in the upper parts. We use ACL to achieve this .We block the IP 1.1.1.1 at the inbound of R7 and R10 at S1/0 and S1/0 respectively. As a result IP 1.1.1.1 will no longer be advertised in the lower body network. Figure 2 and 3 shows the configuration of ACL at the inbound of router R7 and R10 respectively.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

III. INTER-BODY NETWORK

Inter-body network also called inter-BAN [2] is the communication that is established between two autonomous human bodies running their own routing protocols. Following conditions have to be taken care in case of Inter-BAN.

- ACL [4]
- Route-Redistribution [5]
- Virtual-Links [6]
- Encryption

i. ACL

Access Lists are applied on the routers between the two communicating Autonomous bodies so that packets are filtered and only desired traffic is allowed to be shared. We have configured ACL on router R11 (inbound) to deny IP 1.1.1.1 at the inbound interfaces S1/2 and S1/0 of the network topology as shown in figure 4. Figure 5 and 6 shows the configuration of ACL at the inbound to router R11 at S1/2 and S1/1 respectively.

ii. Route-Redistribution

Suppose in figure 4, human body 1 is running OSPF protocol and human body 2 is running RIP or EIGRP then route-redistribution has to be done on the boundary routers, for the two bodies to effectively share packets. Figure 7 shows the configuration of Route-redistribution on the boundary routers.

iii. Virtual-Links

Figure 4 shows the use of Virtual-Links to connect area 0 to other area n, where $n \neq 0$, and $n = 0, 1, 2, \ldots\ldots$

iv. Encryption

Encryption was carried out to enhance the security and avoid any possible/potential intrusions.

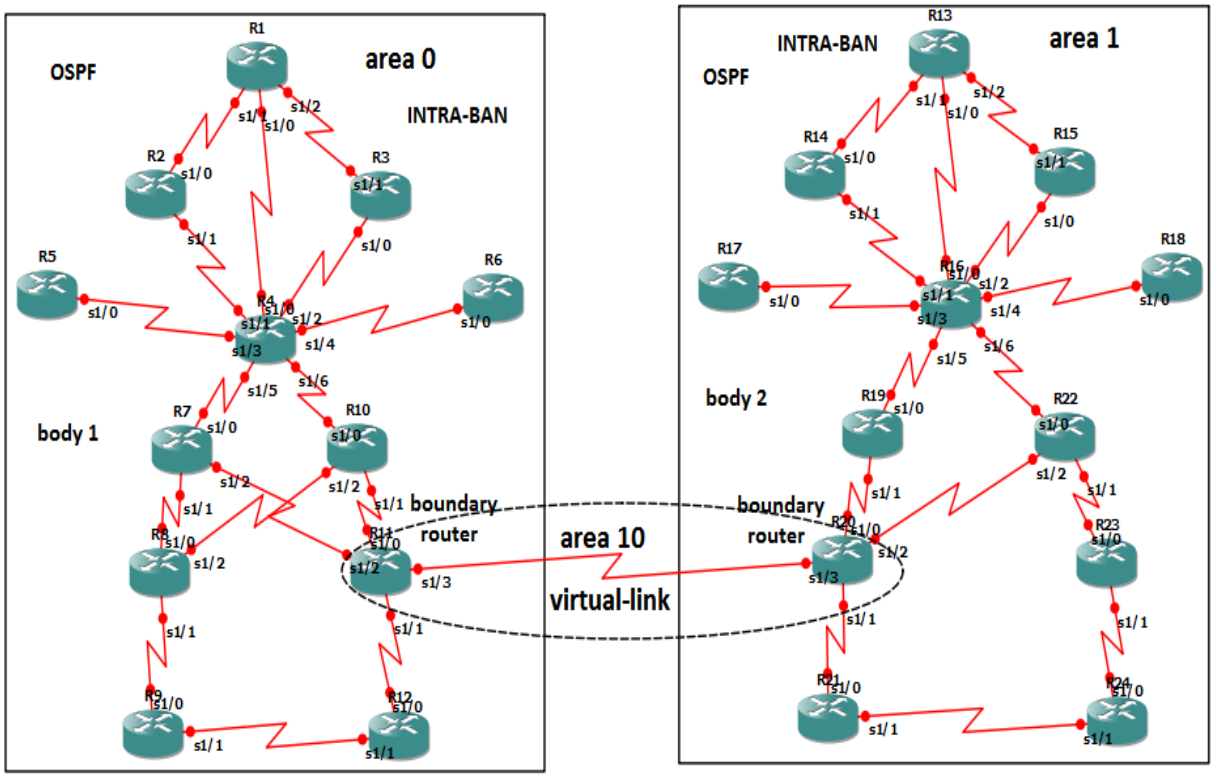

Figure 4 shows inter body communication.

IV. CONCLUSIONS

In this project module of our research work we have successfully configured. ACLs on the Intra-body and Inter-body networks thereby enabling router filtering and traffic flow control. We have carried out encryption to avoid potential

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

intruders into the secured network. We have also implemented Route-Redistribution to allow two different autonomous human bodies running different routing protocols to systematically handshake. Applying ACLs is as important as setting up a network for packet communication and running dynamic and static routing protocols on it. Route selection process goes hand in hand with route filtering.

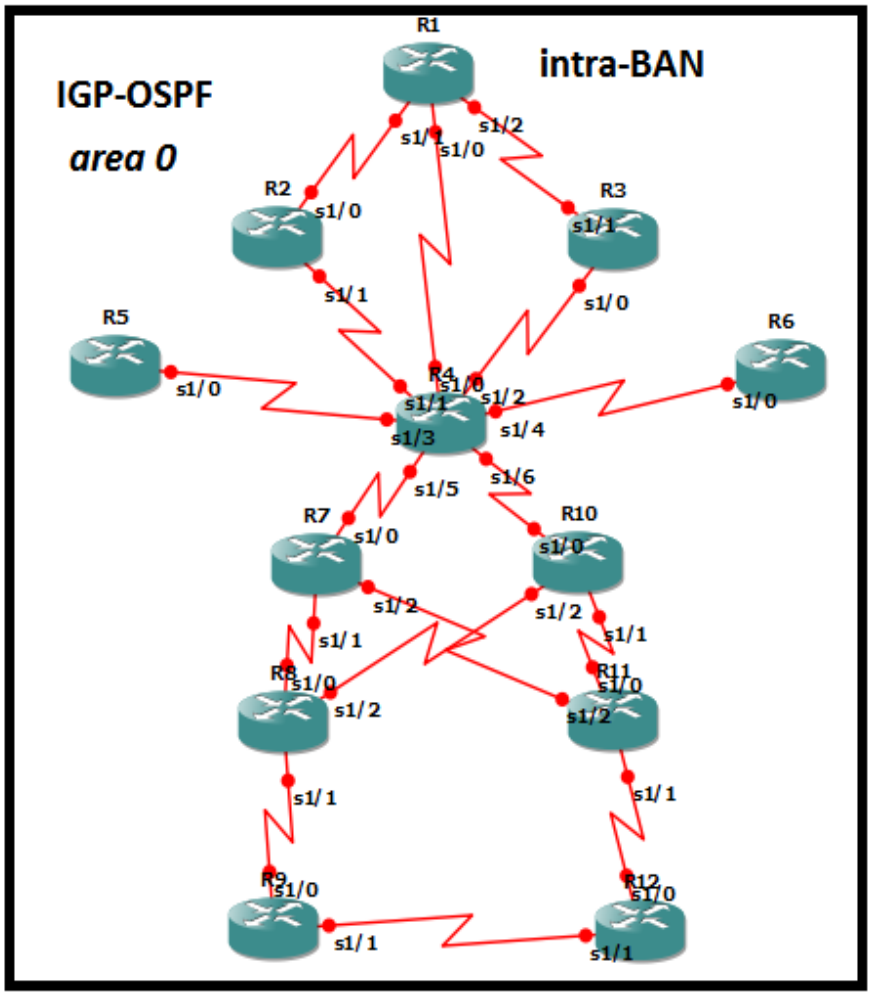

Figure 1 shows intra body communication network.

```
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R7(config)#acce
R7(config)#access-list 1 deny 1.1.1.1 0.0.0.0
R7(config)#router ospf 100
R7(config-router)#
*Aug 15 23:25:13.155: %OSPF-4-NORTRID: OSPF process 100 failed to allocate unique router-id and cannot start
R7(config-router)#dis
R7(config-router)#distr
R7(config-router)#distribute-list 1 in s1/0
```

Figure 2 shows the configuration of ACL at the inbound of router R7.

DOI10.17148/IJARCCE.2017.6810

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Figure 3 shows the configuration of ACL at the inbound of router R10.

Figure 5 shows the configuration of ACL at the inbound to router R11 at S1/2

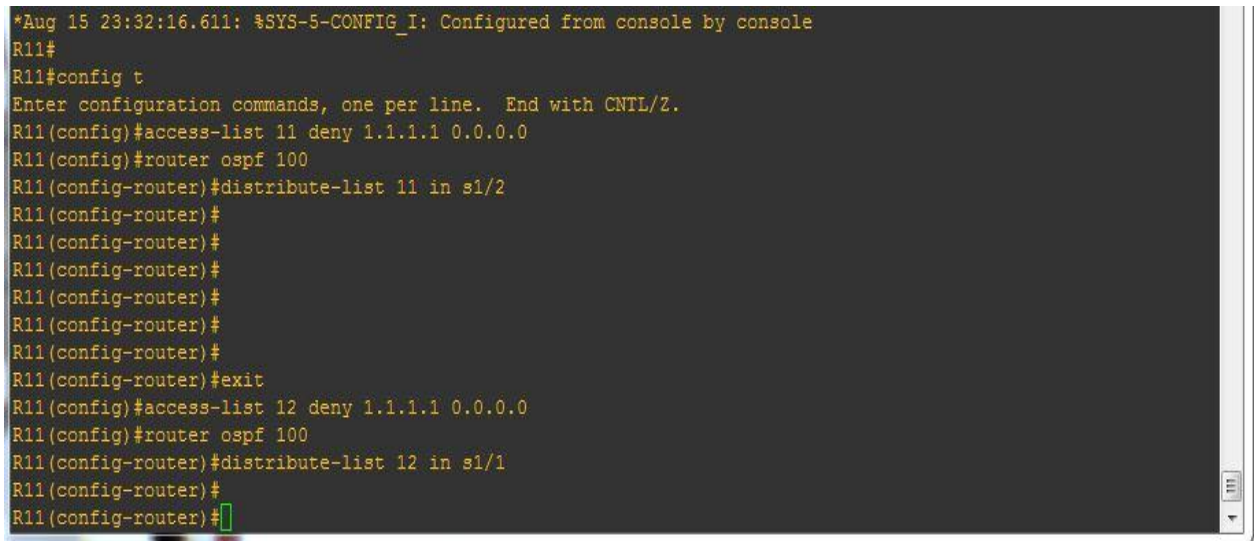

Figure 6 shows the configuration of ACL at the inbound to router R11 at S1/1

DOI10.17148/IJARCCE.2017.6810

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

```
router ospf 2
 log-adjacency-changes
 redistribute rip subnets
 network 10.1.54.5 0.0.0.0 area 0
!
router rip
 version 2
 redistribute ospf 2 metric 2
 network 10.0.0.0
 no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
```

Figure 7 shows the configuration of Route–redistribution on the boundary routers.

REFERENCES

[1] BAN: intra-BAN and inter-BAN-DOI10.17148/IJARCCE.2017.6756
[2] Conceptual Study of Wireless BAN using Bluetooth/IEEE 802.11n- http://www.ijarcce.com/upload/2016/november-16/IJARCCE%2084.pdf
[3] Simulation of Wireless BAN using Network Simulation Tool- http://www.ijarcce.com/upload/2017/january-17/IJARCCE%2081.pdf
[4] Access Control List: Route-Filtering and Traffic Control- http://www.ijarcce.com/upload/2017/july-17/IJARCCE%2061.pdf
[5] Route Redistribution-A Case Study - ijarcce- www.ijarcce.com/upload/2017/june-17/IJARCCE%2042.pdf
[6] Open Shortest Path First (OSPF) Routing Protocol and the Use of Virtual-Links- http://www.ijarcce.com/upload/2017/july17/IJARCCE%2033.pdf