Design and Implementation of Multicast Policy Automatic Deployment System

Dandan Li[1]

Computer Network Laboratory,National University of Defense Technology, Changsha, 201503, China

E-mail: `lidandan9104@126.com`

Xiaomei Chen

Computer Network Laboratory,National University of Defense Technology, Changsha, 201503, China

With the widespread attention and application of the multicast technology, defects and disadvantages of multicast policy's traditional manual configuration mode are also increasingly evident. It is inefficient with high error rate. For this problem, we designed and implemented multicast policy automatic deployment system (MPADS) based on the concept of policy-based network management (PBNM). The system not only supports the device type transparent, protocol independent multicast (PIM) port automatic selection and bootstrap router border (BSR-Border) automatic detection, but also implements high-speed real-time topology extraction based on improvement of the traditional topology extraction technology. In this paper, firstly, we introduced the overall system architecture of MPADS, and then studied the key technologies of the system; finally, experiments on implementation of the key technologies are tested.

[1]Speaker

1. Introduction

In recent years, high-bandwidth multimedia applications emerge endlessly, such as the network video conferencing and the multimedia distance education, etc. The traditional point-to-point communication mode is designed to ensure the reliability of data transmission, which will increase network traffic load, cause a network congestion. But the multicast brings the possibility of alleviating the traditional network problems. In the multicast network which provides one-to-many communication strategy, the backbone bandwidth is not required to increase even when the users are doubled. This advantage enables the multicast technology to be widely used.

With the increasing demand for multicast applications, multicast policy deployment becomes more important. With the traditional SNMP-based network management, users need to master a lot of MIB information. And in large-scale network environment, lots of manual configuration is needed for PIM port selection and PIM domain partition. In addition, the device heterogeneity has greatly increased requirements on the administrator's professional level; thus the traditional management is of high cost and inefficient.

In order to solve the traditional network management problems, we designed and implemented the multicast policy automatic deployment system (MPADS) based on the concept of PBNM. Policy-based network management can effectively simplify the network management process and separate the control behavior and the concrete realization [1]. In this way, the administrator just needs to establish policies and the device configuration is fully completed by MPADS, which avoids the grasp of MIB libraries and configuration commands[2] In addition, the system supports the heterogeneous network devices and makes the device type transparent to users by shielding technology of device heterogeneity. It also simplifies the deployment of multicast network greatly based on the implementation of automatic PIM port selection technique and automatic BSR-Border detection technology. Realization of this system has significantly improved the management efficiency and the intelligent level of multicast policy deployment.

2. MPADS Architecture

In this system, the web-based client is designed to provide a graphical interface for policy deployment[3].Complex works, like configuration commands generation and sending, network interaction etc. are completed by the background processes, which will make the administrator to be free from the complicated configuration works. As shown in Fig.1, in order to facilitate understanding and handling configuration requests of the background processes, the policy parameters need to be symbolized according to policy description model. When the policy is finalized, the background policy processing module and the topology extraction module receive and handle symbolized configuration requests from the client, therein, the policy processing module maps requests commanding the translation mapping library according to device type to execute command translation and save to a .txt file. Afterwards, the executable script generation module converts the .txt files to executable .expect script. At last, the policy execution module executes the expect script to send remote commands to appropriate network device and feedback execution results to the client. Similarly, the topology information extraction module maps symbolized requests to information extraction mapping library according to the device type and the process information extraction [4].

As the automatic policy deployment has been widely used in QOS (quality of service) and ACL (access control list), etc., its overall architecture has been matured, so we does not elaborate this in this article [5]. Here we designed and implemented MPADS based on this architecture, and mainly researched the key technologies, which primarily included the following aspects: Firstly, as the network topology display is an important aspect of multicast policy deployment, in order to improve convenience of the multicast policy deployment, the topology information extraction technology is proposed to provide network topology dynamical update [6]; secondly, the larger of the network size is, the larger workload of PIM port selection

and BSR-Border configuration will be. It has become an important bottleneck which hinders the deployment efficiency of multicast policy; in this sense, the automatic PIM port selection technique and automatic BSR-Border detection technology are proposed to simplify the deployment of multicast policy. It can avoid manual configuration of PIM port and BSR-Border and further improve the deployment automaticity; thirdly, the policy processing module uses the shielding technology of device heterogeneity to support the heterogeneous network devices [7].
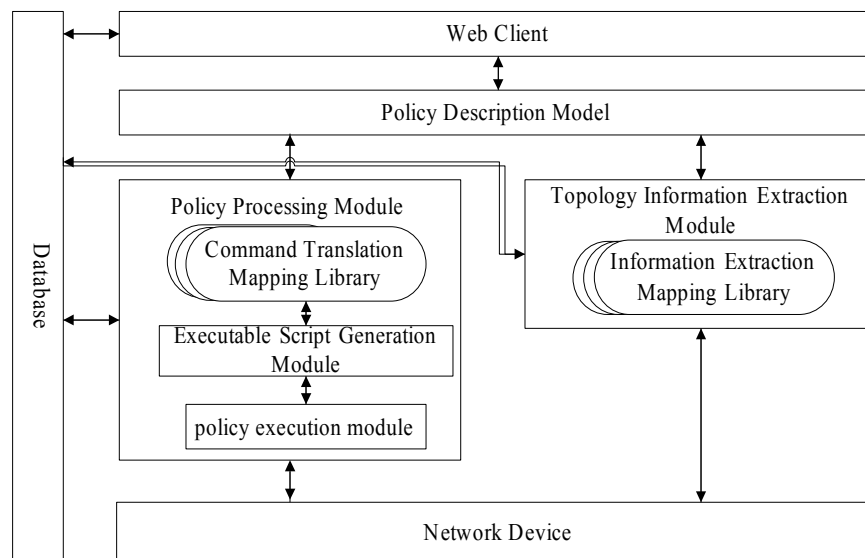
Figure 1: Architecture

3. Key Technologies Of MPADS

3.1 Topology Information Extraction Technology

Currently, there are many researches on the topology extraction, all of which are insufficient [8]. For example, simple network management protocol (SNMP) based topology extraction needs SNMP management software for supporting, thus it is of high-cost. Open shortest path first interior gateway protocol (OSPF) based topology extraction algorithm requires a lot of link state information transmission, thus it is of slow convergence and bandwidth consumption. Address resolution protocol (ARP) based topology extraction has a flaw that arp information cannot be updated in real-time; however, ARP-based Topology Extraction is fast and simple, so this system has improved this algorithm by addressing the above-mentioned shortcomings.

The improved ARP-based topology extraction adds port state judgment before the link judgment. When a link is DOWN, this link ports' arp information will exist for a certain time, but the ports' UP/ DOWM status will update immediately; as a result, if both link ports' status are UP, we can process the link judgment. If the link ports' ip address belongs to the same network segment and ones' arp information contains another, it will be identified to be a direct link [9].

3.2 Automatic BSR-Border Detection Technology

As to the automatic BSR-Border detection technology, the administrator divides the pim domain by device on the displayed topology and the system automatically detects and configures BSR-Border upon division. There is no use of manual selection.

BSR-Border automatic detection problem can be attributed to the cutting-edge set finding problem when the graph partition is determined. Currently, the cutting-edge set finding algorithms include Minimum cut algorithm and tarjan etc.; but all of them are finding cutting-

edge set under the situation of unknown graph division and they are not fit for the automatic BSR-Border detection problem; therefore, based on the thinking of cutting-edge, we designed a cutting-edge finding algorithm case of known graph partitioning-point-colored detection algorithm, which is shown as follows:

Step 1: all network devices will be colored and the devices of different PIM domains have different colors; while in the same PIM domain, they have the same color.

Step2: color all device ports with each port of the same color and its belonging device.

Step3: traverse all topology links and compare the two ports of each link if they are of the same color, different then the corresponding port bsr-border-flag is set to 1; otherwise set to 0.

3.3 Automatic PIM Port Selection Technology

The multicast protocol is only configured on the interconnect ports between devices. It can not only ensure the effectiveness of multicast network, but also greatly reduce the number of unnecessary multicast protocol communication messages while minimizing the impact on other network services. The traditional network management selects PIM port entirely by way of manual analysis, which is a huge job; therefore, this paper proposes automatic PIM port selection technique to reduce human intervention in policy deployment.

Automatic PIM port selection technique is realized based on link information extraction in topology extraction module. The technique is to extract link ports information in the multicast network from all the link information. To cope with the device-based command translation, the ports need to be classified by device. As a result, this paper proposes a device-mark detection algorithm:

Definition: the device set in multicast network $M=\{m_i|1<=i<=k\}$, m_i represents a single device and k refers to the total number of multicast network device.

Link set $L=\{L_i|1<=i<=s\}$, L_i on behalf of a link. Each L_i is a tuple like $<port_{start}$，$port_{end}>$, $port_{start}$ and $port_{end}$ are the two device ports of link .

All PIM port set $P=\{P_i|1<=i<=k\}$, P_i is the pim port set per device, $P_i=\{port_i |1<=i<=r\}$, Port number of Pi is unknown, but it must be greater than 1. P is the final result of desires.

```
for i=0 to k
mark（m_i）
end
for  i=0 to s
get belonging devices mj1, mj2 of each Li's port_start and port_end
if（marked( m_j1 )&&marked(m_j2)）
   Putinto(port_start, P_j1);
      Putinto(port_end, P_j2)
   end
end
```

Algorithm analysis: the key of the algorithm is a judgment whether the device exists in the set M. The traditional method for judgment is based on linear search, which will search once in M for each port's belonging device. The algorithm complexity may be up to o (2*s*k). Our algorithm uses the device mark way instead of linear search with the algorithm complexity reduced to o (k+s).

3.4 Shielding Technology of Device Heterogeneity

The configuration commands of devices from different manufacturers are largely different. In order to solve this problem, we proposed the heterogeneity shielding technology in policy processing module and topology extraction module of the same way. Here we make policy processing module as an example for introduction.

In order to ensure that each device type's commands translate work independently from each other and ease the maintenance and expansion, the command translation mapping library has a separate translation script for each type of network equipment, and provides translation mapping mechanism. The module firstly maps in mapping library according to device type, then

calls the translation script according to task type, and lastly generates the appropriate command sequence. When there is a network device image update, we only need to update the translation script of appropriate device type and the upgrade and maintenance is simple. When there is a new equipment join with the network, we just need to add a new translation module for the new device type in the mapping library, it is scalability [10]. The mapping mechanism is as shown in Fig. 2.
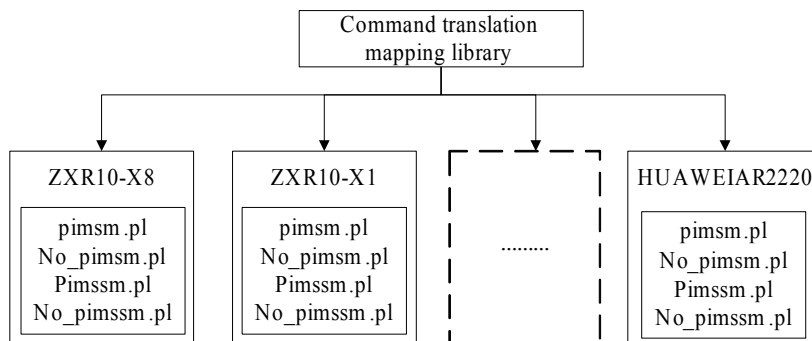

Figure 2: Mapping Mechanism

4. Experiment Studying

4.1 Experiment Environment

The experiment uses ZTE and Huawei routers. ZTE router types include 6802,6804,8S and Huawei router types include 2220,2240,NE40E.In addition, a PC running MPADS is needed. Network topology is shown in Fig.3:
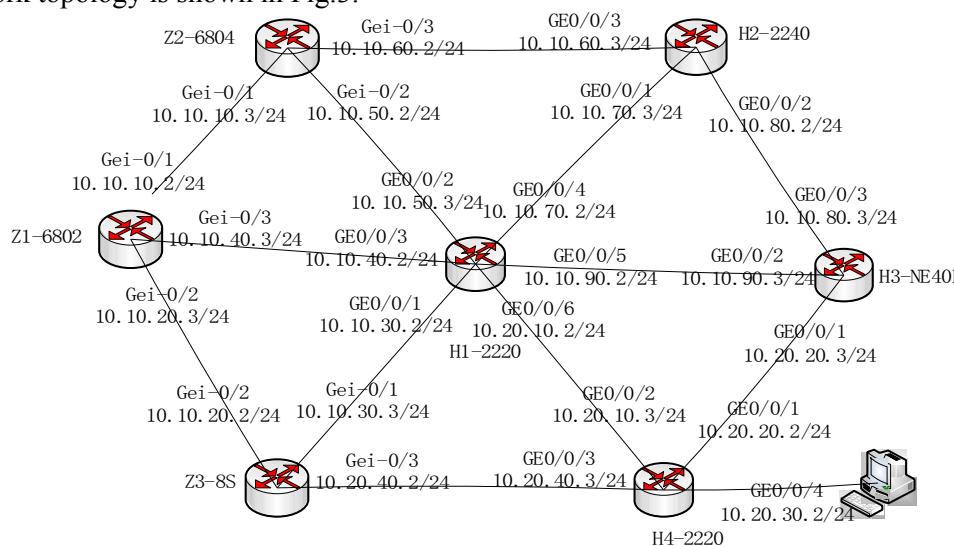

Figure 3: Topology

4.2 Experimental Procedure and Result

The simultaneous test is carried out on four key technologies by inter-domain PIM-SM Policy deployment.

Execute the topology information extraction procedure on all devices.

Select several network devices as shown in Fig. 3, and divide PIM domain as shown in Fig.4, and then set BSR and RP parameters. The blue represents BSR, the yellow represents RP, and the red represents the devices of RP and BSR.
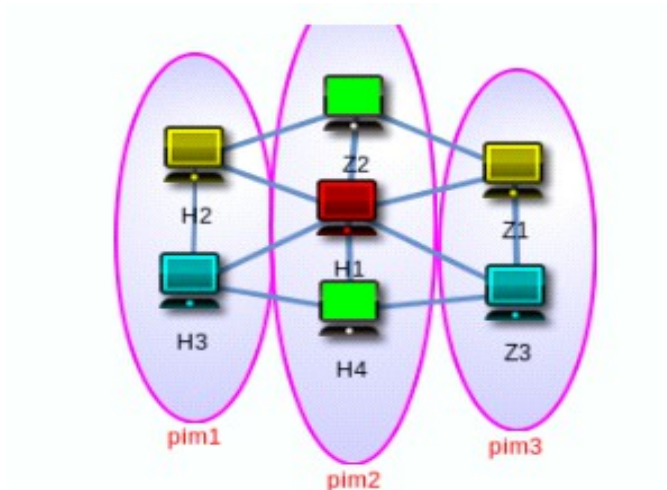
Figure 4: PIM division

Click next to complete BSR-Border automatic detection and the result is shown in Fig. 5.
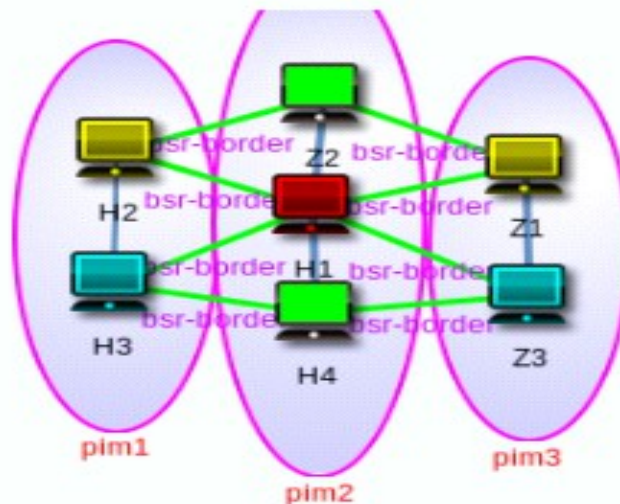
Figure 5: Bsr-Border Detection Result

After the BSR-Border detection, the system will automatically select PIM ports. As there are so many devices and ports, partial result are hereby listed.

The PIM ports of Z1 :gei-0/1 gei-0/2 gei-0/3

The PIM ports of H1:GE0/0/1 GE0/0/2 GE0/0/3 GE0/0/4 GE0/0/5 GE0/0/6

(5) Configure other parameters like RP and BSR priority, MSDP peer, etc. After all have been done, we can send the configure request. The system generates command sequences for each device.

4.3 Result Analysis

Fig.4 is the topology shows, upon the topology extraction, Fig.3 (topology drawn by hand) and Fig.4 are exactly the same when compared; moreover, repeated experiments prove that extract process is fast enough; thus we've achieved the expected results in respect of topology extraction.

Each device has a number of ports, as shown in 4.2(4). The pim protocol is enabled only on the interconnect ports between devices. As shown in Fig.5, the automatic bsr-border detection succeeds and the result is correct. While our test network is in small-scale, the artificial configuration way of pim bsr-border and pim-port needs to go through multiple steps, including analysis, finding and configuration. The time as requested will not be less than one

minute. While our system only needs several millisecond, the automatic BSR-Border detection technology and automatic PIM-port selection technology have greatly improved the efficiency and intelligence of the policy deployment and greatly reduced the workload of administrators.

This test used different types of network devices and successfully generated the corresponding sequence of commands as to every device; moreover, we did not need to distinguish device during the policy deployment process. As a result, the shielding technology of heterogeneity device ensured the device type transparency for users.

5. Conclusion

In this paper, we designed and implemented a multicast policy automatic deployment system based on the concept of policy-based network management. It has greatly improved the efficiency of multicast policy deployment and reduced the burden of network administrators, but there are also lots of aspects for improvement. As to the future researches, we plan to continue to expand in terms of the service type, such as the deployment of PIM-DM and PIM-SSM, etc.; besides, the delete-function when the policies do not need and the rollback-function when some configuration exceptions display are also our directions for improvement.

References

[1] D.C.Verma. Simplifying network administration using policy-based management [J]. Network, IEEE. 16(2), 20-26(2002)

[2] E.S.Al-Shaer, H.H.Hamed. *Modeling and management of firewall policies* [J]. IEEE Transactions on Network and Service Management.1(1),2-10(2004)

[3] C.J.Carcerano, J.D.Barnard, R.A.Wilson. *Browser-based network management allowing administrators to use web browser on user's workstation to view and update configuration of network devices* [J]: U.S. Patent 308(6), 205(2001)

[4] X.Wang, L.Wang, B.Yu. *Studies on network management system framework of campus network*[C].Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference. IEEE, U.S. pp, 285-289(2010)

[5] A.Clemm. *Network management fundamentals* [M]. Indianapolis: Cisco press, 2007:1-4

[6] Y.Chang, D.Xiao, H.Xu. *Design and implementation of NETCONF-based network management system*[C].Future Generation Communication and Networking, 2008. IEEE, U.S. pp, 256-259(2008)

[7]   Y.Liang, L.Wu, L.Han. *Research and design of user-participation campus network management system*[C].Information Science and Control Engineering 2012 (ICISCE 2012), IET International Conference. IET, UK. pp, 1-4(2012)

[8] A.Westerinen, J.Schnizlein, J.Strassner J. *Terminology for policy-based management*[R]. RFC 3198, November, 2001

[9] Y.Breitbart, M.Garofalakis, B.Jai. *Topology discovery in heterogeneous IP networks: the NetInventory system* [J]. IEEE/ACM Transactions on Networking (TON).12(3): 401-414(2004)

[10] B. Moore, E.Ellesson, J.Strassner. *Policy core information model–version 1 specification*[R]. RFC 3060, February, 2001