A SNMP-base broadcast storm identification method in VLAN

Zhang Chunjin[1,2]**, Ji Shujuan**[3]

[1]Collage of Mechanical and Electronic Engineering, Shandong university of Science and Technology, Qingdao 266590, China
[2] Center of Modern Education, Shandong University of Science and Technology, Qingdao 266590, China
[3]Collage of Information Science and Engineering, Shandong university of Science and Technology, Qingdao 266590, China
zhangchjin@163.com, jane_ji2003@yahoo.com.cn

Abstract - How to discover, identify, and stop a broadcast storm is an important problem that has to be considered in the design of networks and in the implementation of network security policies. This paper first studies the factors that cause a broadcast storm and the dynamic change rules of interfaces' traffics when broadcast storms break out, and then gives a method to identify the source of a broadcast storm. Experimental results show that the broadcast storm identification method given in this paper can rapidly locate the source of broadcast storms, therefore can effectively reduce the negative impacts of broadcast storm and improve the stability of network.

Index Terms-Broadcast storm; Virtual Local Area Network; Interface traffic; Simple network management protocol

1. Introduction

In computer network, broadcasting refers to transmitting a packet that will be received by every device on the network. In practice, the scope of the broadcast is limited to a broadcast domain. The destination media access control (MAC) address of a broadcast frame head is a hexadecimal number that can be denoted as “FF.FF.FF.FF.FF.FF”. It represents all hosts that can receive packet that is broadcasted in the network. Broadcast storm means that there are a huge number of broadcast packets flooded in the network. They often use up most of network bandwidth, which will make the normal business can not be run, cause slowly response of host computer. Even worse, if a network switch processor is operating under high load, the core switches will be affected. That will cause extensive network latency, offline, or even paralyzation of the whole network [1].

There are many reasons that result in the broadcast storm. The first reason is the existence of loop circuits. Generally, in offices where there are many people connect to the Internet, one or more HUB are usually used as the connection devices. As the general users have less knowledge of the network, they often put the two ends of a cable directly or indirectly connected to a HUB. That forms a loop circuit, which will lead to broadcast storms. The broadcast storm lead by this reason can swiftly affect other users, and even will make the whole network of the building paralyzed. To identify the broadcast storm problem caused by wrong wiring in network, the spanning tree protocol (STP) network switches integrated with the loopback detection function can be used. However, this kind of method can not deal with the broadcast storm that is caused by the HUB or non-managerial switches [2].

The second reason that may cause a network broadcast is the network virus, or hacker attacks. Some network viruses such as worms or ARP attack can induce a broadcast storm. That is because one computer will send broadcast packets to other computers in the domain, if it is infected by viruses. It will also attack other computers that have vulnerable system. In these cases, there should be large quantities of broadcast packets in the whole domain. Therefore, the network viruses as well as the hacker attacks can cause network bandwidth loss, and lead to network congestion. The avoidance of this kind of storms mainly depends on installing antivirus software or hack-proof software in the host computer.

The third reasons that may cause a broadcast storm is the hardware circuit problem such as damage of switch interfaces, failure of network card or short-circuit of network cable. If an interface of a switch is broken down, a network card is damaged, or a short-cut is caused because the worn of cable insulation, large quantities of broadcast packets will be generated swiftly. These packets will occupy a lot of bandwidths, which slow the network speed significantly. To identify this kind of broadcast storms, we often use the MRGT (Multi Router Traffic Grapher) software to check whether the interface of each network device is in proper condition.

The identification methods introduced in above paragraphs can be taken when a network broadcast storm break out. These methods can effectively deal with the issue of broadcast storm in a small network. However, using these methods, one has to take a long time to find the reason of a broadcast storm in large-scale networks. That is to say, in the large-scale network environment, above storm identification methods not only will delay process time, but also may cause a fatal blow to the network users. Hence, for a large-scale network administrator, it is a very important and difficult problem to find the source of the broadcast storm timely and control the broadcast storm in its first time. This paper aims at studying the identification and process method of broadcast storm in large-scale network.

Other sections of this paper are organized as follows. Section 2 introduces the statistics principles of interface traffic in Virtual Local Area Network (VLAN). Section 3 introduces the reading method of interface traffic in VLAN. The effectiveness of this method is verified in section 4 by experiments. Section 5 summarizes this paper.

2. Calculation principles of interface traffic

In this section, we will introduce the calculation principles when there is not any broadcast storm and when broadcast storms break out in a VLAN.

2.1 Calculation principle when there is not broadcast storm

Generally, different network devices have different data velocity. Besides, HUB usually transmits data in a sharing mode. For example, if a host wants to send data to another host by a HUB, this host will broadcast its data to all interfaces of the HUB. Whether a host which connects to the HUB should receive the data is determined by its network card. In contrast, switches transmit data in switching mode, by which the data will be sent directly to the specified interface. Other interfaces will not receive the data. Suppose there is a HUB who has N interfaces. And the input amount of interface *I* is denoted as I_{in}, the output amount of interface *I* is denoted as I_{out}. According to the characteristics of the HUB, the relationship between input traffic and output traffic of these *N* interfaces satisfy formula (1) [3].

$$\sum_{i=1}^{N} I_{in} = N \sum_{i=1}^{N} I_{out} \qquad (1)$$

Similarly, if the network connection device is a switch, the input traffic and output traffic of these interfaces satisfy formula (2)[3]：

$$\sum_{i=1}^{N} I_{in} = \sum_{i=1}^{N} I_{out} \qquad (2)$$

From formula (1) we can see that the input traffic of each interface is the sum of connected computers' output traffics when HUB is used as a network device. While, according to formula (2), the input traffics and output traffics of each interface is balance when a switch is used. That is because when switches are used, hosts' output packets are only sent to the target interfaces. Based on this principle, we should draw a conclusion that switching devices (e.g., switches) is better than sharing devices (e.g., HUB), therefore we should be chosen as the connection devices in the access layer.

2.2 Calculation principle when broadcast storms break out in a VLAN

Virtual local area network (VLAN) is a virtual kind of local area network, in which equipments are logically (not physically) divided into small segments to realize the data exchange technology of the virtual working group. The difference between VLAN and traditional network is that the former kind of network is not affected by the physical location of network user. Therefore, users can form a local area network (LAN) beyond the geographic restrictions. Within a VLAN, broadcast traffics will not be forwarded to other VLAN, which limits the domain of broadcasting, saves bandwidth, and improves the process ability of a network.

The formation of a broadcast storm is formed because of large amounts of traffic in the network interfaces, which make the network full of broadcast packets, and finally causes blocks and interruptions in normal network communication. As VLAN has the function of isolating broadcast packets, a broadcast storm can only spread in a VLAN, once it break out in this VLAN. Therefore, the broadcast storms in VLAN have following characteristic. First, the host that has some problems input large quantities of packets to the connected switch in the VLAN. Second, the switch forward these broadcast packets to all the other hosts that connected with it in the same VLAN. Therefore, in a VLAN, only one interface has a large number of input traffics, while, all the other interfaces simultaneously output equal numbers of packets respectively. The interface that input large numbers of packets is the source interface of a broadcast storm, and the interfaces that output large numbers of packets are the recipients of the broadcast storm.

Under normal circumstances, the sum of input traffics and the sum of output traffics of a switch is equal to each other. Therefore, formula (2) can be used as the calculation function. However, when a broadcast storm breaks out, the sum of output traffics will increase greatly. As that situation when broadcast break out is similar to the working principle of HUB, hence, formula (1) should be selected as the calculation function when a broadcast storm breaks out. These two formulas are the theoretical foundation of identifying the source of a broadcast storm.

3. A SNMP-based interface traffic getting and process methods

Based on the calculation principles given in section 2, this section focuses on studying the method about how to get traffic data of each interface. That can be implemented by reading dynamic interface traffics of the switch under the support of Simple Network Management Protocol (SNMP). However, these values do not represent traffics we need because the starting times of these traffics are not similar. A feasible method is to read each interface's traffic at the same time. And then, read each interface's traffic simultaneously again after a period of △T. The difference between the values gotten in the adjacent reading is the corresponding interface's traffic within time △T. Based on this principle, following subsections will illustrate the management model of SNMP protocol, the method of reading data flow based on SNMP, and the data process method.

3.1 The SNMP protocol management model

The SNMP protocol was first put forward by the Internet Engineering Task IETF team in order to solve the management problems of internet router. It is consisted of a series of protocols and norms, which provide a method to collect management information from network devices. This management system (see figure 1) is mainly composed of workstation, management node, management information base, and network management protocol [4].

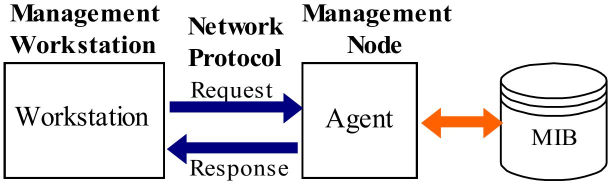

Fig. 1 The architecture of network management system

Using the network management process reside in it, the management workstation realize the monitoring and controlling of the entire. The network management agent resides in the management node device constantly monitor and respond to the query or set commands that come from the network management station. The managed objects are abstracted network elements, which correspond to specific operational data in the network. The set of these managed objects constitutes the Management Information database (MIB) of managed devices. MIB provides information about the managed network devices. These kinds of information can be used in the management tasks such as network configuration, network failure, network performance, security and billing. Network management protocol is used to encapsulate and exchange the commands or responses between the management station and the management node. Besides, it specifies the interaction process rules and the data format that is exchanged between agents and the workstation.

There are five basic operations in the SNMP commands, by which the management system can effectively communicate with the management node. These commands are illustrated as follows.

(1) Get_request: request for a variable from the network management agent.

(2) Get - Response: network management agent's reply to the response of Get_Request that is sent by management station.

(3) Get_Next_Request: request for next variable from the network management agent.

(4) Set_Request: set a value to the variable in the network management agent.

(5) Trap: The unsolicited messages that network management agent initiatively report to the management when a specific event occurs.

To use these commands, we should first initialize the parameters of them, and then use these commands to read the parameters of switch, and finally process the reading results. The architecture of SNMP Network management [4] is shown in figure 2.

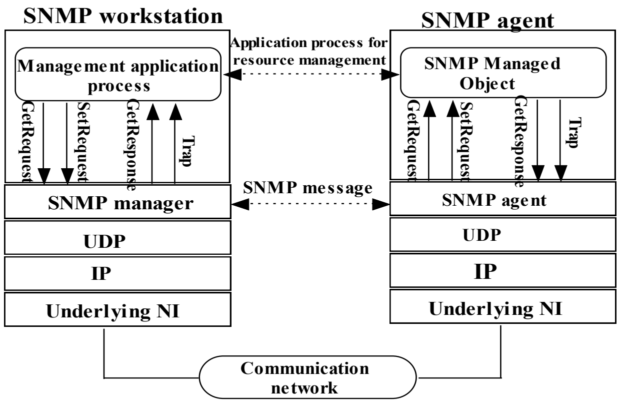

Fig. 2 Architecture of SNMP Network management

3.2 A SNMP-based data flow getting method

In this paper, the traffic of interfaces are gotten by polling the switch in each △T period. The basic operation steps are as follows. First, assign a value for the access right (i.e. community property) of the devices that we want to poll. Second, design a method to read the data flow of switch's interfaces. The flow chart of the traffic getting method is shown in figure 3.

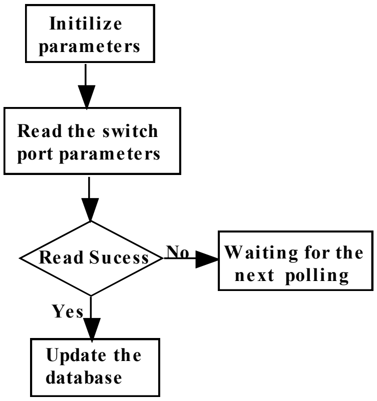

Fig. 3 Flow chart of traffic getting method

3.3 Data process method

As the ratio of a interface's input and output will be changed when a broadcast storm break out, we can conclude that the interface which has largest input and output traffic ratio is the source interface of broadcast storm. Therefore, we can locate the source interface by calculating the input/output ratio of each interface when a broadcast storm breaks out. That is the basis of the data process method. To differentiate the source interface and the normal interfaces, we set 100 and 0.01 as the bench marks of input/output ratio according to experiences.

The main idea of the data process method can be divided into four steps. First, calculate the input and output traffic ratio of every interface in each VLAN. Second, judge whether there is an interface, which ratio is larger than 100. If exist, then we can preliminary confirm that the corresponding interface trigger a broadcast storm. Third, to make sure that there really is a broadcast storm, we should check whether all the other interfaces' ratios are around 0.01. If all the other interfaces' ratio is around 0.01, then we can confirm that a broadcast storm break out. And the interface which ratio is larger than 100 is the source of it. Fourth, to stop the broadcast storm, we can use the SNMP SET command to shut down the corresponding interface by assigning 0 to parameter ifAdminStatus. The core code of this method is given in figure 4.

4. Experiment and results

To verify the feasibility of the method given in this paper, this section designs an experiment. Following subsections illustrate the experiment setup and the identification process of the broadcast storm that is triggered by this circuit circle.

4.1 Experiment setup

In this experiment, we select an access layer switch in our university as an example. This switch is connected with 3 VLANs, i.e., VLAN10, VLAN20, VLAN30. VLAN10 has eight interfaces that are used by graduate students. VLAN 20 has twelve interfaces for office workers. VLAN 30 has 24 interfaces for multimedia classrooms. These interfaces are named as interface1, interface2, …, interface44 respectively. To make a broadcast storm, we set a circuit circle in this network.

```
//Triggered each time period
//Initializes variables parameters
for i=V1 to Vk  //k is the total number of records
{//Judge whether the record pointer is pointing to a new VLAN?
  if(Pointer->VLAN !=CurrentVLAN) {
   NumL=0;// Record number of interfaces whose  ratio is less than 0.01
   //Records the number of interface whose ratio is larger than 100 in this
   //VLAN
   occur=0;
   CurrentVLAN=Pointer->VLAN;
   if((occur==1)&&(NumL>0)) {
     //Output the broadcast storm VLAN, interface number etc.
    cout<<CurrentVLAN<<"A broadcast storm happened!!"<<endl;
    cout<<"Switch's IP address:"<<SwitchIP<<endl;
    cout<<"interface number"<<InterfaceNo<<endl;
    //shut down the interface
   Oid="1.3.6.1.2.1.2.2.1.7."+Pointer->InterfaceNo;
    m_snmp.Set(Pointer->SwitchIp,public,Oid,"2",0);
    }//if
  } //if
  else{
   if(Pointer->RateInOut>100) {//This variable is used to sign that the
     //VLAN interface has a ratio greater than 100
     occur=1;
    //Save the broadcast storm switch's address and interface number
     SwitchIP=Pointer->SwitchIP;
     InterfaceNo=Pointer->InterfaceNo; }
   if(Pointer->RateInOut<0.01) { NumL=NumL+1; }
  }//else
  Pointer ->MoveNext(); //Point to the next record.
}// for
```

Fig. 4 Core code of data process method

4.2 Getting traffics of interface in switches

Using the SNMP-based interface traffic getting method illustrated in section 3, we first obtain the traffic of each interface. Then, we classify the interfaces according to VLAN. Third, to statistic interfaces' traffics in each VLAN, we create a table (see table I) and add each interface's input and output traffics that are gotten by the traffic getting method into this table. Then the input/output ratio is calculated and added into this table. Therefore, table I has 7 columns, i.e., record number, VLAN ID, interface number, input traffic, out traffic and state of each interface. State is a Boolean value that signifies whether an interface is running or not.

4.3 Locating source interface of the broadcast storm in VLAN

Table I lists the network traffics when a broadcast storm breaks out. From the table we can see that the third interface's input/output ratio is very large (i.e. 4951.8), while other interfaces' ratio is zero. As the input traffic of an interface in the switch correspond to the output traffic of the connected computer(s). If an interface's input traffic is a large number, then we can know that the connected computer(s) is sending large numbers of broadcast packets to this interface. Therefore, according to the principles illustrated in section 2 we can conclude that a broadcast storm is break out, and interface 3 is the source of it.

After locating the source interface of this broadcast storm, we should further identify which computer is the source computer if there are many computers connect to the switch according to this interface. In the small network formed by these computers, the locating of source computer can be realized by observation, the network traffic analysis softwares, or the protocol analysis softwares such as sniffer, Ethereel[5]. Using these softwares to observe the internal computers' communication condition, observe the number and proportion of broadcast frames, we can finally find the host which cause the broadcast storm.

Table I Data traffic when broadcast storm breakout

No	VLAN	IntNo	InOctets	OutOctets	State	Ratio
1	10	1	2500	39614250	1	0.00
2	10	2	15000	39614250	1	0.00
3	10	3	39614250	8000	1	4951.8
4	10	4	6000	39614250	1	0.00
5	10	5	0	0	0	0
…	20	---	---	---	1	---

In order to improve the performance of the broadcast storm identification method, we exclude the interfaces whose state are "DOWN" (i.e., the state value is 0) in the same VLAN. Besides, according to experiences, the interfaces whose input and output traffic is within 200000 bytes are normal ones. Therefore, to improve the identification speed, we also exclude these kinds of interfaces.

5. Conclusion

This paper analyses the factors that may cause a broadcast storm. No matter because of what factors, broadcast storms will induce similar phenomena, i.e., unbalanced input/output ratio in the switch's interfaces. Based on this principle, this paper gives a set of feasible methods to identify a broadcast storm, locate the host that cause the broadcast storm and stop it.

These methods are relatively easy to be implemented, and can rapidly locate the broadcast storm source. Most importantly, the methods given in this paper can effectively reduce the bad impact of broadcast storm, and improve the stability of large-scale network.

6. References

[1] Mu Bao_lu, Wang Xing_cheng, "Multicast Technology to Suppress Broadcast Storm in Industrial Control System[J] ". *Measurement & Control Technology*, 2009 (8): 69-71.

[2] Wang Sheng, "Common causes and preventive measures of LAN broadcast storm[J] ". Fujian computer, 2008 (7): 69-70.

[3] Chen Yan_qiu, song Yin_hao, Diao Cheng_jia, "Solution method of physical network topology discovery question by port's traffic[J] ". Computer Engineering and Applications, 2007.43 (5): 150-152

[4] Zhang Chunjin, Lin Zedong ,Xue Fangfang,"Applying SNMP protocol to network equipment monitoring in campuses[J] ".Computer Application and Software,2010.11:209-301.

[5] Wang Qina, Tonghua,"Solving the Broadcasting Storm by the Sniffer[J] " Marine Electric & Electronic Engineering, 2008 (1): 60-61.