MANAGING USERS, APPLICATIONS AND RESOURCES WITH RMON2

L. P. Gaspary[1,2] and L. R. Tarouco[1]

[1]Universidade Federal do Rio Grande do Sul
Instituto de Informática
Campus do Vale, Bloco IV - Bento Gonçalves, 9500 - Agronomia - CEP 91591-970
Porto Alegre, RS - Brasil

[2] Universidade do Vale do Rio dos Sinos
Centro de Ciências Exatas e Tecnológicas
Instituto de Informática
Av. Unisinos, 950 - CEP 93022-000
São Leopoldo, RS - Brasil

E-mail: paschoal@inf.ufrgs.br, liane@penta.ufrgs.br

Abstract

The increasing growth of the amount and complexity of applications and protocols executed on computer networks has hindered the work of their administrators. They need to justify the ever-increasing investments accomplished on network equipment acquisition and on communication links leasing. For such, they must: identify who, and with which purpose, most consumes these resources, know if users and resources are located so that the presence of bottlenecks in the network is minimized and detect if some intruder, by means of a high-layer protocol is trying to invade it. An appropriate and current solution capable to answer these subjects is the use of RMON2, MIB that operates above the link layer, providing information needed to monitor client-server applications and end-to-end communications. This work presents the results of a study accomplished on this MIB, aiming at extracting from it means to control the users' activities, to monitor protocols and applications, to optimize the localization of users and resources and to accomplish security management.

1. Introduction

The investments accomplished in the expansion and maintenance of computer networks have surprisingly grown in the last years. Their popularization brought about the appearance of a high number of distributed applications and protocols, leading managers and administrators to investigate effective management solutions in order to reduce costs, provide high availability and, at least, maintain the quality of service once noticed.

As most of the time users regard the network as an inexhaustible resource, they incorporate more and more applications and protocols to their daily routine, which for the administrator means the need for constant alterations in the network infrastructure. These modifications involve costs and, therefore, they need to be justified. This is possible if the administrator can answer simple questions such as: Which users or departments use the network? When is it most used? Which applications are executed? What are the activities of a certain user? Do users perceive an appropriate level of service? Are resources correctly allocated?

Answers to these subjects can be obtained with the use of accounting mechanisms. A good alternative to accomplish this task is the use of RMON2, MIB that operates with protocols above the data link layer, providing information to monitor high-layer protocols and distributed applications [1]. The information collected by this MIB allows administrators to have a detailed view of the behavior of applications and protocols being executed as well as of the resources usage rates and of the users who most consume them. With such information, these administrators can redefine network traffic flows aiming at better resources usage. Besides, they can observe who communicates with whom and which applications are being used, which makes possible the establishment of policies to guarantee the appropriate use of the network.

This work presents how the information provided by RMON2 MIB may benefit the maintenance of network control and its usage profile discovery, which is an important task for the company to evaluate if investments on networking technology converge or not for the business interests. The paper is organized as follows. Section 2 presents an overview of RMON2 [2]. Sections 3,4,5 and 6 present the results of the study. Section 3 describes how to monitors the user activities on the network. Section 4 presents how to trace the global usage profile of the network. Section 5 treats of the procedures to be accomplished to determine if users and resources are appropriately positioned. Section 6 describes how to use RMON2 to detect non-authorized users. Finally, in section 7 the final considerations are presented.

2. Overview of RMON2

The largest contributions to the group of SNMP standards are RMON and RMON2 specifications [3]. Their use has been increasing the efficiency and reducing costs in remote network monitoring and in protocol analysis. While RMON aims at identifying physical problems in the network looking at traffic from router to router, RMON2 monitor network usage patterns, observing the content of the packets of high-layer protocols and applications. When monitoring high-layer protocols such as network and application-layer protocols, it is possible to entirely visualize the network instead of individual segments. The new groups defined in RMON2 MIB are:

- protocol directory (*protocolDir*): repository that indicates all the protocols that the probe is capable to interpret;
- protocol distribution *(protocolDist):* statistics about the amount of traffic generated by each protocol observed by the probe;
- address map *(addressMap):* associates each network-layer address to the respective MAC address, storing them in a table;
- network-layer host *(nlHost):* collects statistics about the amount of input/output traffic of the hosts based on their network-layer address;
- network-layer matrix *(nlMatrix):* provides statistics about the amount of traffic between host pairs based on their network-layer address;
- application-layer host *(alHost):* collects statistics about the amount of input/output traffic of the hosts based on their application-layer address;
- application-layer matrix *(alMatrix):* provides statistics about the amount of traffic between host pairs based on their application-layer address;
- user-history collection *(usrHistory):* periodically samples objects specified by the user (manager) and stores the collected information in accordance with parameters also defined by the user;
- probe configuration *(probeConfig):* defines configuration parameters for RMON probes;
- rmon conformance *(rmonConformance):* describes conformity requirements for RMON2 MIB.

3. Statistics on User Activities

If the administrator is interested in tracing the network usage profile it is very important to obtain information about how a certain user or department uses it. What users most use the network? With whom do these users communicate? Which applications and protocols do they execute? Such information enable the administrator to observe users' activities and verify if they fit the company interests.

3.1. Volume of Accesses

Information related to the volume of network accesses accomplished by a certain user can be obtained through requests to RMON2 network-layer host group. It decodes packets based on their network-layer address. Thus, administrators can observe beyond the routers that connect the sub-networks and identify the real hosts that are communicating [3].

Requests to *nlHost* group may help administrators to find out which users most use the network and when it occurs. In this context, the user history group can be used to store object values in different time instants. A simple formula to calculate the network usage rate (n.u.r), in percentage, by a certain user (host) during a time interval between t_1 and t_2 is presented below (1). *ifSpeed* denotes the speed of the network technology of the segment to where the probe is attached. Figure 1 shows an example of a graph, which can be generated by polling the *nlHost* group and applying the formula just presented.

$$n.u.r = \frac{\left(\frac{[(nlHostInOctets_{t2} + nlHostOutOctets_{t2}) - (nlHostInOctets_{t1} + nlHostOutOctets_{t1})] \bullet 8}{ifSpeed}\right)}{t_2 - t_1} \bullet 100 \qquad (1)$$

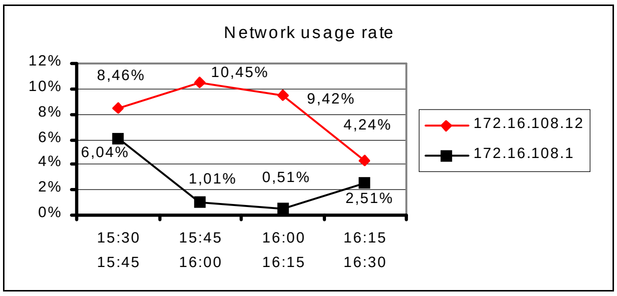


Figure 1: Network utilization rate by two hosts

3.2. Applications and Protocols Used

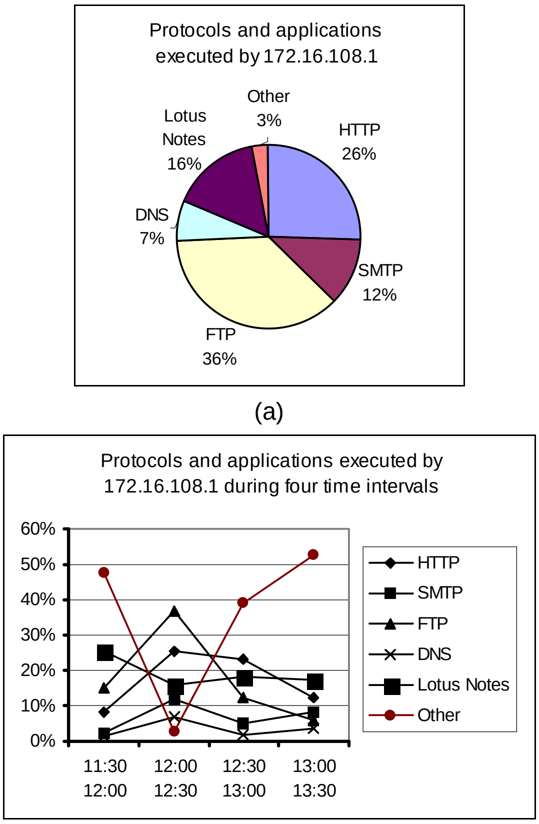
Determining user network usage patterns relies on the knowledge of the administrator about the protocols and applications that each user executes as well as when it happens. Such information can be obtained in application-layer host group. It provides the administrator with input/output traffic statistics of hosts, considering application-layer protocols. The term application-layer refers to all protocols above the MAC-layer.

The information provided by *alHost* group can be used to draw graphs that indicate both the protocols and applications in use by a certain host and the amount of traffic generated by each of them. Figure 2a shows an example of a chart that can be obtained by polling the probe in two time instants (t_1 and t_2). It presents the usage rate of each protocol by the host 172.16.108.1 based on the total volume of packets observed coming from and addressed to it during the interval t_2-t_1. The formula to calculate it follows:

$$a.u.r = \frac{\left(alHostInOctets_{t2\ prot} + alHostOutOctets_{t2\ prot}\right) - \left(alHostInOctets_{t1\ prot} + alHostOutOctets_{t1\ prot}\right)}{\sum_{i}\left(alHostInOctets_{t2\ prot\ i} + alHostOutOctets_{t2\ prot\ i}\right) - \left(alHostInOctets_{t1\ prot\ i} + alHostOutOctets_{t1\ prot\ i}\right)} \bullet 100 \qquad (2)$$

Figure 2b shows the protocol usage rate considering four consecutive time intervals. This type of historical graph aids the administrator to determine user access patterns. In this graph, protocol usage rate was calculated based on the speed of the monitored segment. Thus, it is possible to observe the impact that a protocol in use by a certain user is causing to the network. The formula to obtain this information is:

$$a.u.r = \frac{\left(\frac{\left[\left(alHostInOctets_{t2} + alHostOutOctets_{t2}\right) - \left(alHostInOctets_{t1} + alHostOutOctets_{t1}\right)\right] \bullet 8}{ifSpeed}\right)}{t_2 - t_1} \bullet 100 \qquad (3)$$



(a)

(b)

Figure 2: Charts depicting protocol usage rates

3.3. Established Communications

It is important to identify who are the local/remote peers of each established communication to further understand the behavior of network users. The application-layer matrix group has an important role in this process. It collects traffic statistics between communicating host pairs based on their network-layer address.

Through periodic requests to the RMON2 probe or by means of configured reports in user history group, it is possible to determine with whom a certain host is communicating, the protocols being used and the amount of traffic generated by them. Table 1 shows the communications established by host 172.16.108.12 during a time interval between instants t_1 and t_2. It is easy to notice that the user on this host is currently accessing Alta Vista® and the web site of the own company. Besides, it maintains an FTP connection with Microsoft®.

Table 1: Communications established by 172.16.108.12

Destination Address	Protocol	Bytes
altavista.digital.com	HTTP	24.322
ftp.microsoft.com	FTP	34.967
172.16.108.1	HTTP	13.452

4. Network Global Usage Profile

In the previous section, mechanisms to control and to monitor host-based (user) network activities were presented. However, in many situations the administrator must further investigate the network usage profile taking into consideration the whole company or some departments. For instance, such information is essential if the administrator wants to find out the departments that most consume network resources, when the network is overloaded and which users/departments contribute to intensify this problem.

The protocol distribution group counts the number of octets and packets monitored by the probe for each supported protocol encapsulation. The accomplishment of periodic requests to this group or the retrieval of historical reports from it makes possible the observation on the variation of protocols usage rate during a certain time period (see figure 3).

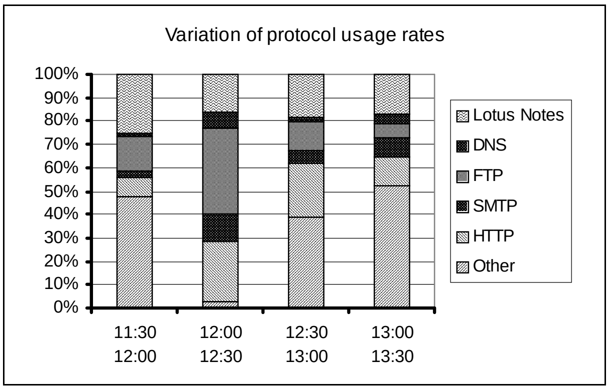


Figure 3: Protocol distribution during a time period

To determine the network usage rate of each department the administrator must know which hosts belong to each department. In this case, the group to be polled is network-layer host. The methodology to be used is the following: the probe counts input/output packets and octets for each identified host. At the end of an accounting interval, the network usage rate is calculated for each host using the formula presented in (1). Afterwards, hosts of each department are grouped and their usage rates are added.

The graph in figure 4 was drawn based on object values collected in two different time instants. In this case, the resulting information will reflect the peculiar situation of the network in that specific interval. Another possibility is to accomplish such measurements in several moments of the day, for several days, and to calculate the average of the obtained rates. This methodology provides the administrator with accurate information about network utilization in each department.

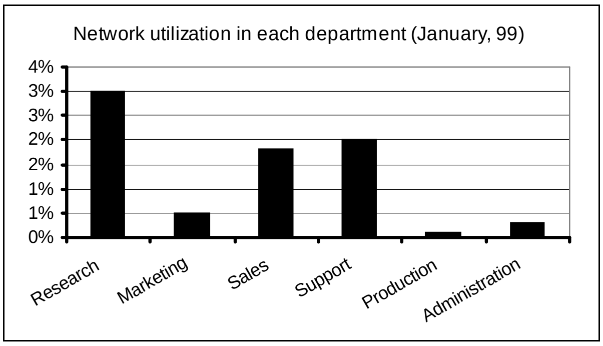


Figure 4: Departmental network usage rates

The type of information commented above can be decisive in cost allocation, once it helps the administrator to decide where to invest. In this context, the identification of the hosts that accomplish most of the accesses is also important. Such information can be found in *topN* tables from network-layer matrix group. The *topN* tables provide an efficient way for a management station to obtain a ranked listing of matrix table entries based on a chosen network statistic [1][3]. Figure 5 shows the users who most consume network resources.

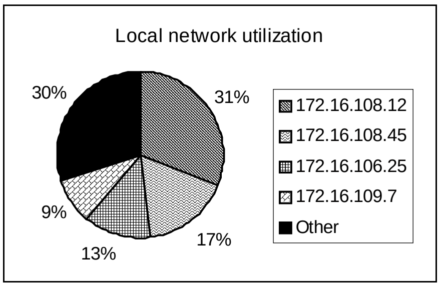


Figure 5: Users who most consume network resources

5. Optimization of Distribution and Positioning of Users and Resources

An important contribution of RMON2 is the possibility to verify if users and resources are adequately positioned in the network in order to maximize traffic confinement in each department of the company [4]. The group that provides this information is application-layer matrix previously, presented in section 3.3.

In some cases, users and resources are appropriately positioned, minimizing traffic between different network segments. However, some resources may be overloaded, which affects the response times of protocols and applications. In such cases, load balancing is needed. To do that, the administrator must measure the usage rate of a certain resource. This information is provided by application-layer matrix group.

The methodology used to determine the current activities on a certain resource is the following. The probe counts input/output packets and octets for each identified host pair. The monitoring can be accomplished in two time intervals (instants t_1 and t_2) or periodically. At the end of an accounting interval, all the entries whose source or destination address is the same of the monitored resource are selected. The selected entries are then grouped according to the application-layer protocol. Afterwards, for each group the input/output octets are added. Figure 6 shows an example of a graph, depicting network activities on a network server host along the day.

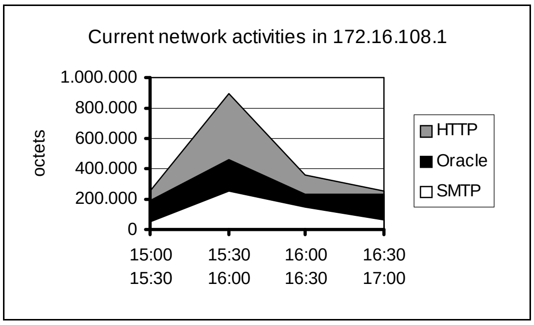


Figure 6: Activities observed on a network host

6. Security Management

Security is an essential issue to corporate networks. Nowadays, more and more mechanisms such as firewalls have been incorporated into the network in order to keep intruders away from strategic data of the company [3].

RMON2 can be used as an additional tool to detect the presence of intruders in the network. As already presented, the application-layer matrix group shows host pairs that are communicating (see section 3.3). Therefore, if the administrator periodically monitors this group, he can identify non-authorized users trying to establish communications with network hosts. It is also important to observe the protocol being used. Depending on the security policies of the company, a simple telnet may represent an attempt to invade the corporate network.

The graph in figure 7 shows the users that are accessing a certain resource. It is adequate to monitor strategic hosts where database, www and mail servers reside. It is generated with information retrieved from application-layer matrix group.

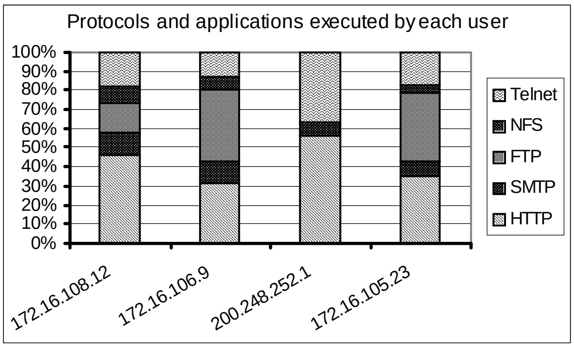


Figure 7: Users and protocols observed in a resource

In some cases, it may be useful to identify which protocols each observed user executes. This information can be obtained in *alHost* group, already presented in section 3.2. Figure 8 shows an example of a graph that can be generated with the retrieved data.

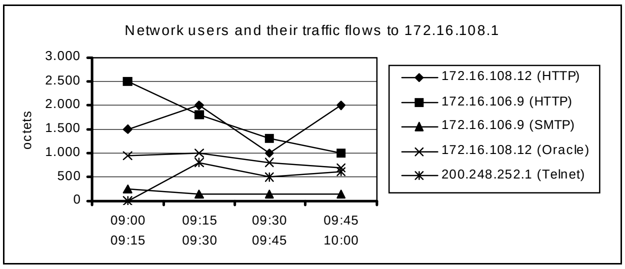


Figure 8: Users and the protocols executed by them

7. Conclusions

RMON2 represents a huge increase in capabilities [3]. In many cases, its functionalities supplant protocol analyzers, trend generation tools and other. This paper presented how to use this MIB to control user activities, to trace the network usage profile, to optimize the location of users and resources and also to accomplish security management. The contribution of this work is to show the administrator how to benefit from this MIB, which is powerful yet very complex.

Some of the objects and tables in RMON2 MIB were designed so that a simple display of their contents provides meaningful information [3]. Most of them, however, must be organized in easy-to-view formats; otherwise they are of little use. Depending on the company investments on network technology, it is not always possible to buy management applications, which do treat such information and automatically convert it to charts and other diagrams. In this context, this work helps network managers to create their own management applications. Through *script* languages or high-level management libraries, it is possible to develop systems adapted to the company's needs without many investments.

References

[1] WALDBUSSER, S. *Remote Network Monitoring Management Information Base Version 2 using SMIv2.* Request for Comments 2021, January 1997.

[2] WALDBUSSER, S. *Remote Network Monitoring Management Information Base.* Request for Comments 1757, 1995.

[3] PERKINS, David T. *RMON - Remote Monitoring of SNMP-Managed LANs.* First Edition. USA: Prentice Hall, 1998.

[4] STALLINGS, William. *SNMP, SNMPV2 and RMON. Practical Network Management.* Second Edition. USA: Addison Wesley, 1996.