A Methodology for Performance Management of Networks

Ádrian Bonfá Drago, Anilton Salles Garcia, Maxwell E. Monteiro

Federal University of Espírito Santo – LPRM – Av. Fernando Ferrari, s/n –Campus de Goiabeiras – CT VII-Informática –Vitória E.S. – Brazil – CEP 29060-900.
Telephone and Fax: 055 27 3352667

Abstract This paper proposes a proactive performance management methodology, based on Performance Analysis, Capacity Planning and Discreet Events Simulation Tools. The main objective is to provide a practical framework to aid the network operators and managers to keep up the network performance. A case study based on the application of the proposed methodology for a large-scale enterprise network and its results is presented.

Keywords: Performance Analysis, Network Management, Discreet Event Simulation, Traffic Characterization

I. INTRODUCTION

The Network Management has been an important activity in the operation and maintenance of the computer Networks.

Among the five functional areas described by OSI (Open Systems Interconnection) 7498-4 document [11] is Performance Management. This document specifies the activity groups that are responsible for monitoring and controlling the network resources utilization, guaranteeing minimum quality requirements for the supported services. However, this is a very important activity and it is Known that it isn't receiving real attention from computer networks operators and managers. Several reasons can be suggested as cause of that process: the great effort spent by another management activities, the lack of a computer management tool in order to facilitate the solution of performance problems, the complexity of mathematical tools embedded in the analysis and decision making process, the lack of a practical methodology to allow the connection between the day-to-day of network operators and the theory of Performance Analysis and Capacity Planning [9].

The objective of this paper is to propose a pragmatical methodology for proactive computer networks performance management. The main idea is to integrate classical techniques and methodologies such as performance analysis, capacity planning and discreet events simulation in a pragmatical approach. In addition to that, our preference is the application of standard management protocols and public domain tools.

II. CONSIDERATIONS ABOUT PERFORMANCE MANAGEMENT

Among the most important management standards such as: CMISE/CMIP (Common Management Information Service Element / Common Management Information Protocol) [2], RMON (Remote MONitoring) [11], SNMP (Simple Network Management Protocol) [11] and [5] and TMN (Telecommunications Management Network) [2], SNMP is broadly used. It is a standard specified by the Internet Community and has acquired a large popularity in the network management environment. Another important feature found in the SNMP is the open data format exchanged between its elements, allowing easy manipulation and treatment by word processors, electronic worksheets and so on. Then, SNMP becomes an important tool in the data acquisition (monitoring) necessary to Performance Management.

Besides the existing management tools, a technique known as Sniffing appears. The use of Sniffers on the network monitoring comes to supply the limitations of some standards mentioned above. For example, it is not possible to obtain all necessary management information from higher layers of the OSI Model (information related to applications and network resources).

Management standards like SNMP and RMON implement remote management facilities, using network resources for this.

On the other hand, Sniffers have the advantage of using passive data collection so that they don't spend network resources. As a disadvantage, it is necessary to place one Sniffer in each monitored segment what is very expensive when the network is distributed in a large geographical area.

The management standards and Sniffers are just means for obtaining data from traffic flows on network. Although, collected data must be treated to generate the necessary information for analysis of network traffic behavior.

Another important tool that helps to find solutions for the performance problems is the Discreet Events Simulator [6]. When a real network model is built inside the simulator, it can virtually show the possible changes and new investments that could be done, without interfering in the real network. It avoids that the network remains down for a long time or unnecessary investments [7]. The simulation also allows appraising, with great margin of success, the

41

impact of new systems and applications that use network services.

Finally, we conclude that a practical way for the solution of the performance problems should involve the following steps: data capturing using consolidated management standards, the use of public domain computer tools for data treatment, information analysis through graphical reports and the use of discreet events simulation.

III. PERFORMANCE MANAGEMENT METHODOLOGY

To allow a better understanding of the proposed methodology, it becomes necessary to create a model that presents a computer network environment under a more appropriate viewpoint. Thus, it is proposed a model, composed by three main resource groups, classified by its functionality, that represents the network environment (Figure 1).
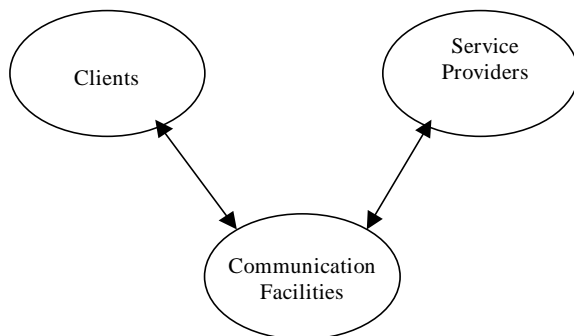

Figure 1 – Performance management model

III.1. GROUP 1 - CLIENTS

The clients are terminals or workstations, which are the users of network available services. The elements of this group can or not present processing capacity, being subject, in the affirmative case, to the performance management. In other words, Clients are, at the same time, workload source and destination.

III.2. GROUP 2 - COMMUNICATION FACILITIES

It represents the elements involved in the traffic transport and routing into the network. In this group the communication mediums and the active network equipment are classified. This group has a privileged vision of all traffic between " Clients " and " Services Providers". Besides supplying management data about its own elements, it reveals useful information from other groups.

III.3. GROUP 3 - SERVICE PROVIDERS

This equipment group is responsible for supplying the services used by Clients. In a great number of situations, these elements will correspond to the traditional computer network servers. In this paper, a more generic designation (Service Providers) will be used.

The Service Providers receive requests, or calls, from Clients, through its service access elements (sockets, named pipes and so on) .

IV. A GENERAL METHODOLOGY FOR PROACTIVE PERFORMANCE MANAGEMENT.

Considering the proposed functional model in the previous section, a general Performance Management Methodology will be presented. It is able to give a consistent guideline in the performance analysis and capacity planning of all groups (Clients, Communication Facilities and Services Providers) .

This methodology is composed by four phases, organized in accordance to the strong necessity of the problem solution and investigation. The Figure 2 below illustrates the proposed methodology.
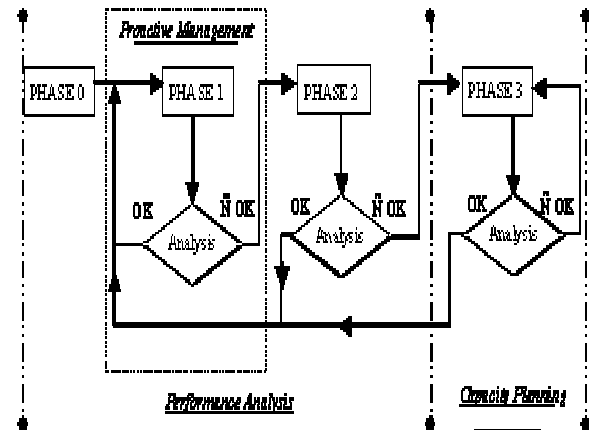

Figure 2 – Methodology diagram

IV.1. ZERO PHASE

This phase is responsible for the establishment of the initial conditions for methodology application. In this phase are defined:

- Group of the functional model to which the methodology will be applied;
- Appropriate period of monitoring;
- Performance and Quality of Service patterns that will be used as control points of the chosen group.

The performance and quality of the service patterns should be chosen in accordance with the selected functional group for the methodology application. They will inform the limits between the acceptable and unacceptable performance. It is worthwhile to remember that the patterns considered attractive for the service providers group can't be the same for the communication facility group. It is important to choose a minimum pattern set to make possible the proactive monitoring of the elements of the chosen group, causing the minimum impact of management activity over the network environment.

It is also very important an exact characterization of the monitoring meaning period in order to avoid problems with the manipulation of a large amount of non-significant data.

IV.2. FIRST PHASE

Based on performance and quality of service patterns, defined in the Zero Phase, the data collection referring to the monitoring of the system performance current indicators is done. After the data collection phase, the performance indicators should be extracted and compared with the patterns chosen in the Zero Phase. The analysis of the comparisons will reveal possible performance problems, suggesting the application of the following phase. If there aren't any performance problems, the process is maintained in the First Phase. This phase must be repeated frequently, even if performance problems are not found. It corresponds to the methodology's proactive portion. Through these analyses, a network manager can view the network performance changing before it becomes a serious problem.

IV.3. SECOND PHASE

At the end of the First Phase, it is possible to know which performance indicators were violated (out of the desired pattern). Then, an investigation of the performance violation reasons is started. For each indicator with " bad behavior" a different data set should be collected with the most useful information for the re-establishment of normal performance conditions.

The choice of the new data that'll be collected will depend on the managed resources group type. A problem and data tree to be investigated must be presented in that phase. The most expert operator can investigate and report the performance problem collecting a few numbers of information. After investigation, the network manager should have reached enough information to understand whether the performance problem can be solved or not. Thus, three situations can appear:

1. Adjustment hardware or software configuration;
2. Physically repair in the evolved equipment's;
3. To add capacity to the network environment.

In the cases 1 and 2, after the manager's intervention, the process should go back to the First Phase . If lack of capacity is the main problem, the process should go ahead for the Third Phase.

IV.4. THIRD PHASE

The Third Phase means to enter in the study of Capacity Planning. The approach chosen here is the Discreet Event Simulation [7] and [2]. As mentioned before, simulation has several benefits and it helps to find solutions in an easier way.

To execute the Third Phase, the following steps are needed:

1. Collection of the right information to proper event characterization;
2. Stochastic modeling of the events, including, when pertinent, its association with other important objects for the study (flow matrix, response time and so on.);

3. Adjusting of the Simulation model;
4. Running of the Simulation model for new scenarios, trying to find best approaches to solve Capacity problems.

If the simulation doesn't reach satisfactory results, the items from 1 to 4 should be reviewed, going back to the beginning of the Third Phase again.

V. PROPOSED METHODOLOGY APPLICATION FOR A TYPICAL COMPUTER NETWORK.

It's important to observe that the general methodology previously proposed could be applied to a wide range of performance problems. Putting the focus on computer network environment, some specialization's are necessary.

V.1. GENERAL RECOMMENDATIONS

Due to privileged vision that the Communication Facilities Group has over the whole data of network system, it is recommended, at first, to apply the methodology over that group.

The results obtained from methodology application over Group Two (Communication Facilities) can show that the performance problems are in the other Groups. It suggests that the methodology should be applied, with other specialization, over the new target Group. To allow a better understanding of this paper's scope, the performance problems in the other two groups (Clients and Services Providers) will be considered as different problems. Thus, it won't be analyzed in this paper.

V.2. ZERO PHASE

V.2.1. CONSIDERATIONS AND SPECIALIZATION

In this phase, a set of typical computer network performance indicators was chosen. This set must be as little as possible. The objective here is to apply a small and efficient proactive monitoring job on the network. The chosen indicators were based on the Raj Jain work [8]. The Table 1 shows the chosen indicators:

PHASE 0	Quality Patterns
Physical Errors	$<10^{-4}$ a second.
Response Time	<15 seconds.
Bandwidth Utilization	< 65% in networks without dispute for physical middle OR < 20% in networks with dispute for physical middle
Collisions (when applicable)	< 15 a second.
Token Delay(when applicable)	< 250 milliseconds.

Table 1 – Basic performance indicators

V.2.2. PRACTICAL RECOMMENDATIONS

According to the computer network technology, other performance indicators could be chosen. The indicators presented here are intended to be typical

43

802.X LAN. Collisions and Token Hold Time, for example, must be monitored just when feasible (LAN technology dependent).

V.3. First Phase

V.3.1. Considerations and Specialization

In this phase the data collection and analysis are done. No specialization is needed for this phase, but it's better to remind that every analysis should have an objective in order to provide a guideline for network performance problem solution. The analysis can be viewed on the Table 2.

PHASE 1 Activities	ANALYSIS 1

Collecting of the indicators chosen in the Phase 0	Comparison with the Quality Patterns
	IF (patterns = OK)
	THEN Continue PHASE 1
	ELSE
	GO TO PHASE 2

Table 2 – Analysis of the collected indicators

V.3.2. Practical Recommendations

Most of the needed indicators in this phase can be extracted by using SNMP or RMON standard platforms. The indicated SNMP objects for this phase are presented on Table 3:

Indicators	Variables
Physical Errors	IfErrorIn/IfErrorOut
Bandwidth Utilization	IfOctetsIn/IfOctetsOut
Collisions (when applicable)	IfCollision
Token Delay(when applicable)	IfTokenHolding

Table 3 – Recommende SNMP objects

The Response Time is very hard to be gotten. Some alternatives to get this parameters are shown on the Table 4. A good computational alternative to do this is a sniffer tool. There are also commercial sniffers, especially built for response time acquisition, but it isn't a tool broadly used. The manual measurement of the response times (made by observation) from a client workstation can show the delay of the communication and processing between clients and servers. Whatever the used method, the results must be put into a worksheet. Information like average and standard deviation response time must be gotten.

Indicators	Variables
Response time	Sniffer/ Chronometer /Interview

Table 4 – Tools to collect time

In general, the collected data doesn't bring all information needed for analysis in the First Phase. Thus, the data needs to be treated and arranged in a better presentation. The treatment consists in eliminating wrong samples (data without physical meaning or out of reality. Ex.: bytes rate above the

physical capacity of the segment) to synchronize the collected data from different sources (if data is collected simultaneous from different SNMP devices, there isn't time synchronization guarantee between samples) and to build the necessary graphs. It is recommended that the collected data is treated (processed) by worksheets (MS-EXCEL, STAR-OFFICE or other).

The obtained information after treatments are better presented using graphical viewing. It is recommended some kinds of graphs:

- LAN Utilization;
- Collisions Rates (when applicable);
- Physical Errors;
- Response Time;
- Token Holding Time (when applicable) .

For each one above, it is also interesting to calculate information like average, standard deviation and variation.

V.4. Second Phase

For each possible problem found in the First Phase a specific monitoring must be done. At this time, monitoring is addressed only to the suspicious elements or responsible entities for the network performance degradation (see the Table 5). The new data (that will be collected in this phase) must be chosen in agreement with the problem found in the first phase and also its easy acquisition.

PHASE 2 Situation Found in the Phase 1	PROCEDURES FOR COLLECTION OF NEW INFORMATION
IF Physical Errors $> 10^{-4}$ a second.	To collect Information about: ♦ NIC (Network Interface Card); ♦ Cabling
IF Utilization > 85% in networks without dispute for physical middle OR Utilization > 20% in networks with dispute for physical middle	To collect Information about: ♦ Hosts that more use the network; ♦ Protocols more used (BROADCAST) ♦ Frame size.
IF Collisions (when applicable) > 15 a second.	To collect Information about: ♦ Size of network segments; ♦ Difference of access speed between NIC's (when it be not caused by use excess).
IF Response Time > 15 Seconds.	To collect Information about: ♦ Network Delay; CPU Utilization + buffers of the network equipment involved; ♦ Time in Service (Servers); ♦ Processing Time in the client.

PHASE 2 Resultados Obtidos na Coleta	ANALYSIS 2

Informartion collected in the PHASE 2	IF (Problem is out of the Facilties Group of Transmission)
	THEN
	  PROCEDURE: New process for the Group of responsible elements for the problem
	  GO TO Phase 1
	IF (Possibility of Adjustment of Configuração Software/Hardware)
	THEN
	  PROCEDIMETO: To adjust Configuration
	  GO TO Phase 1
	OTHERWISE
	  GO TO Phase 3

Table 5 – Hypotheses to be investigated

At the end of this phase, it is expected to define if performance problem belongs to Transmission Facilities Group or not. In the affirmative case, there are two possibilities:

1. The problem can be solved by a simple software adjustment (parameters configuration) or fixing broken equipment.

44

2. Capacity problem was detected, so that the Third Phase must be applied.

It is possible that, at the end of this phase, the collected information shows that performance problem belongs to other two groups (Clients or Services Providers or both). Thus, the methodology should be started again over those groups. This new universe won't be part of this paper.

V.4.1. PRACTICAL RECOMMENDATIONS

In the Phase Two, RMON and Sniffer tools should collect data. Once again, It is important to remember that open tools or standard protocols are still a better way to collect data.

The tools and its recommended objects for that phase are on the Table 6:

Investigated indicators	Tools/Variables
To collect Information about: ♦ NIC; ♦ Cabling; and ♦ Size of Network Segments	**Sniffer/ Equipments of Certification of Cabling**
To collect Information about: ♦Hosts that more use the network; ♦Protocols more used (BROADCAST). Frame size ♦Difference of access speed between NIC's (when it be not caused by use excess).	**RMON2 using the groups:** ♦**Hosts Top N** ♦**Protocols (RMON2)** ♦**Packet Size (Variable Etherstat: Pkts X to Y Octets))** **OR** **Sniffer using RMON similar reports.**
To collect Information about: ♦Network Delay; CPU Utilization + buffers of the network equipment involved; ♦Time in Service (Servers); ♦Processing Time in the client.	**Sniffers or group of softwares of service time measure inside of servers and stations.**

Table 6 – Objects recommended for the Second Phase

As in the First Phase, data treatment can be necessary. New information must be acquired from collected data. Again, the use of electronic worksheet is recommended to make it.

The most important issues of this Phase are:

- Error Rate per network segment.
- Identification of cabling problems.
- Error Rate per network interface per segment.
- Traffic Matrix per network segment;
- Traffic amount per application per network segment;
- Network Latency per sub network;
- Processing Time of applications in the Customers (workstations).
- Frames/cells/packets discarded on the network equipment.
- Network equipment Memory, Disk and CPU Usage.

V.5. THIRD PHASE

If there is a capacity problem in Transmission Facilities, the Third Phase is applied. This phase has the traffic analysis as objective. Thus, It's necessary to characterize the network traffic, allowing the Capacity Planning study. The next steps are on the Table 7:

PHASE 3	PROCEDURES AND ANALYSIS 3 Collection and Analysis of Data for the Planning of Capacity
Collection of Data for traffic Characterization	To collect from each host: ♦Used service. ♦The medium volume of traffic generated by transaction of each service. ♦The medium time among transactions of each service.
Choose of the depth of traffic Characterization	To decide on: ♦Creation of users' profiles and applications (to group user of same behavior). ♦The necessary flexibility degree to the wanted Inferences (it is either in group or desirable to move user individually).
Traffic Characterization	Stochastic Modelling of the events: ♦To find the average, the standard deviation and the coefficient of variation of the events collected in the beginning of that Phase. ♦To Provide an approach of the probability distribution curves for each collected event.
Identification of the installed Capacity	Study of the Installed Capacity ♦To identify logical and physical network topology. ♦To identify individual capacities of each element of the network (usually contemplated through the Throughput parameters and speed of Transmission or Processing).
Construction of the Simulation Model	Introduction of the Data Characterized in the Simulation Environment ♦Entering of the capacity data in order to create the Structural model. ♦Entering of the traffic characterization in order to create the Transaction model
Aferição do Modelo (repetir até refletir a realidade)	Fittings of the simulation model to reflect the reality ♦Identifying of the trust Interval ♦Adjusts Fine until reaching the Interval of Trust.

Table 7 – Third Phase implementation

V.5.1. PRACTICAL RECOMMENDATIONS

Network traffic characterization demands the usage of a Sniffer or in some cases RMON platforms. It is important to characterize the workstation workload, as well as its service composition (application and protocols). The most part of sniffers can make network traffic detailed logs. The resulting data should be treated (using any electronics worksheet application). The treatment consists of the following steps:

1. To separate the workstation traffic.
2. 2. For each workstation, to separate the service traffic.
3. For each service, to calculate the average and the standard deviation of
- The traffic amount per service occurrence,
- Time between occurrences of the same service
- The approximated curves of probability distribution, for both.

It can be made by a macro inside some electronic worksheets.

V.5.2. USERS PROFILES AND GROUPING

Sometimes two or more stations will present very similar workload behaviors. In this situation, it is possible to represent it as a single entity with double or n times more workload than the single one. It makes easier the simulation modeling. When simplifications (like grouping in users' profiles) are made, simulation inferences will be less flexible. The solution is to choose a good balance between both.

Sometimes it isn't easy to characterize the workload. A simpler approach is to do only the first step. Thus, it can avoid complex data treatment required in the other steps. In this way, traffic amount (represented by network utilization for example) becomes the simulation key.

V5.3. SIMULATION

The simulation consists on representing the network-installed capacity and to simulate the network behaviors under a defined workload. The best computational simulators for this job are Discreet Event Simulators. Several Discreet Event Simulators are available. Many of them are made for general purpose, other especially designed for networks simulation. General-purpose simulators can be found free in books or in the Internet. But its operation will demand larger efforts because it doesn't bring network equipment templates or facilities to modeling a network. Specific Network simulators bring lots of network equipment templates providing an easy modeling process. Although, they aren't for free.

The entirely simulation model should be tuned as a guarantee to the model fidelity. Several simulations running should be made until the model reaches a close real behavior.

After simulation model tuning, new scenery can be tested until it reaches an interesting solution. For each one of the scenarios, several running (simulations) should be made, assuring the result qualities.

V.5.4. CHANGES IN THE REAL SYSTEM

Based on simulation results, the real system should be modified in order to follow the solution found by the simulator. After the changes, it's expected that the problem is solved. The methodology goes back to the First Phase in order to confirm It. Otherwise, the Phase three must be done again, more carefully and with more details. Sometimes, successive methodology application can be necessary to refine the problem until the network fine tune.

VI. CASE STUDY

To illustrate the methodology application, a case study, which was made inside a large enterprise computer network, will be presented.

This network is composed by 1500 workstations, 100 servers and some dozens of manageable network equipment. The network architecture consists of a

large optic fiber ring FDDI (Fiber Distributed Dates Interface) [10] backbone. Each Company section has a local computer network, generally standard IEEE 802.3z (Ethernet) [10], connected to the backbone.

It was observed that 83% of the financial/productive/administrative processes are executed over computer applications into the network.

The methodology was applied in 8 (eight) of 13 subnetworks, coming up to 40 (forty) Ethernet segments. In this paper, the most interesting case, a specific subnetwork, referred as X.X.16.0, will be presented.

VI.1. THE ZERO PHASE

The indicators chosen were:
- Utilization;
- Collision rate;
- Error rate
- Application Response Time;

It was defined that the periods between 09:00AM - 11:00AM and 14:00PM - 16:00PM are representative for data capturing.

VI.2. THE FIRST PHASE

A summary of the obtained results in the subnetwork monitoring is presented below. The Table 8 presents the values corresponding to segment average use, the standard deviation and the variation of that use. The table also presents: collisions and errors rates, and the response time.

Hub	Medium use	Standard Deviation	Variation Coefficient	Collisions	Errors	Response Time
HUB-16.80	1,09%	0,61%	56,04%	Normal	Don't exist	Normal
HUB-16.82	5,46%	2,43%	44,43%	Normal	Don't exist	Normal
HUB-16.83	7,04%	3,33%	47,34%	Normal	Don't exist	Normal
HUB-16.84	4,32%	2,62%	60,56%	Normal	Don't exist	Normal
HUB-16.85	5,93%	1,72%	29,01%	Normal	Don't exist	Normal
HUB-16.86	5,58%	4,63%	82,89%	Normal	Don't exist	Normal
HUB-16.87	2,70%	2,08%	76,96%	Normal	Don't exist	Normal
HUB-16.88	8,52%	5,88%	69,00%	Normal	Don't exist	Normal
HUB-16.90	2,48%	1,23%	49,62%	Normal	Don't exist	Normal
HUB-16.92	21,43%	8,43%	39,35%	Normal	Don't exist	High
HUB-16.93	5,07%	1,26%	24,85%	Normal	Don't exist	Normal
HUB-16.94	1,84%	1,59%	86,05%	Normal	Don't exist	Normal

Table 8 – Information about segment X.X. 16.0

The computer SNMP tool used in this stage was Accton ACCView [1].

VI.3. THE SECOND PHASE

In this phase, the EcoSCOPE tool [4] was used, and the collected data shows the workstations that consume more network resources in terms of traffic volume.

These stations consume services as File Server, IPX NCP and Mail (services in the local server). Besides, the response times for these applications are

low, in the milliseconds order, which doesn't justify the delay in the used applications.

It is observed that a small part of the traffic that flows by the router xx.xx.240.50, being routed to the sub-net xx.xx.238.0. This portion of the traffic represents all database service (SQL Server) that flows in the network segment. Comparing the traffic SQL with File Server traffic, it is observed that the first represents less than 1% (0,79%) of the traffic generated by the second one.

In addition to that, it was observed that in spite of the fact that the traffic SQL is small (in byte number), the response times for this application are quite high. Some transactions got to last around 4 minutes.

In the Figure 3 an example of performed transactions by the workstation "F" with the database server whose IP address is xx.xx.16.24 is shown. You should observe that some of the transactions present response time superior to 1 minute. This time is very long and it is the main cause of the delay in the applications that access the database.

Figure 3 Data about SQL transactions

As observed above, the database response times are much higher than the applications that only access the file server. Besides, the amount of traffic generated by database queries is clearly small when confronted with the total traffic on the segment.

Looking carefully, it can be observed that 90% (approximately) of time spent in one query transaction comes from database Server (Figure 4)

Figure 4 – Data about response time

With data above (Figure 4), can be calculated the percentage of time spent in the server. In this example, the time spent in the server is 4min 6sec (246 sec), and the total time of the transaction is 4min 10sec (250 sec). In other words, 98,4% of the total transaction time is spent in the server.

Only a small part of the time is spent in the customer and into the network. Observing the data, it is shown that, independently of the client workstation to be close or distant of the database server, the percentage of response time spent keep the same. This characteristic suggests that the response time problem is not into the network (utilization isn't the main cause of performance problem).

Thus, the problem can be broken in two:
- Problem of transmission capacity;
- Problem of performance of the database server (SQL server);

The database performance problem was reported to the competent division, especially worried about database management. If it was necessary, database performance problem could be treated using a special adaptation of the same methodology.

VI.4. THIRD PHASE

In the Third Phase, the work focus on the high utilization segment.

Then, the work was divided into the following tasks:

1. **Getting up the traffic matrix of each segment:** using EcoSCOPE [4], the data about application was collected.

Application	Utilization	Response Time (ms)
[B] IPX NLSP	0,015%	0
[B] IPX RIP	0,025%	0
[B] IPX SAP Response	0,130%	0
[B] RIP	0,005%	0
Access	0,007%	2,5
Acesso a contas de usuários	0,006%	0,888888889
Add – Desenvolvimento	0,008%	0,5
Amipro	0,014%	1,444444444
Apoper	0,002%	0,714285714
Correio	0,157%	1,75
Dicionário	0,008%	1
Emulador Telnet	0,010%	1,9
File Server	9,066%	1,75
IPX	0,025%	0
IPX NCP	0,302%	1,583333333
IPX RIP	0,002%	0
Login	0,018%	1,25
Lotus 123	0,021%	1
MS Windows 3.11	0,025%	1,9
Netscape	0,004%	0,857142857
NetWare Adm	0,061%	0,909090909
Power Builder	0,007%	1,090909091
Schedule do HelpDesk	0,049%	1
SIAB – Desenvolvimento	0,186%	1
SisEng	0,001%	0,5
Sistema de Abastecimento	0,013%	0,9
Sistema Financeiro	0,001%	0,857142857
SQL Server	0,092%	220,25
Telnet	0,023%	24,08333333
TFTP	0,035%	0
Tivoli Object Dispatcher	0,037%	20,5
Unibanco	0,026%	1

Table 9 – Traffic matrix

47

Soon after, the traffic matrix was built using macros that were developed in Microsoft Excel®. As an example, the Table 9 presents the traffic matrix of the HUB-X.X.16.92´s segment:

2. **Characterization of the service traffic**: Starting from the generated files by EcoSCOPE, the fundamental parameters (average time between arrivals and average size of the messages) are extracted. Those parameters are also automatically obtained by macros. The Table 10 presents an example of average size of the messages of one application. Four applications were considered as the heaviest workload over the network and defined as base of simulation parameters (see the Table 11).

Class (Byte Number)	Middle Point	Frequency
224 a 4692	2212,2	13
4692 a 9160	6233,4	8
9160 a 13828	10254,6	10
13828 a 18096	14275,8	15
18096 a 22564	18297	4
22564 a 27032	22318,2	2
27032 a 31500	26339,4	1
31500 a 35968	30360,6	4
35968 a 40436	34381,8	3
40436 a 44904	38403	1
44904 a 49372	42424,2	1
49372 a 53840	46445,4	1
53840 a 58308	50466,6	0
58308 a 62776	54487,8	0
62776 a 67244	58509	1
67244 a 71712	62530,2	0
71712 a 76180	66551,4	1
76180 a 80648	70572,6	0
80648 a 85116	74593,8	0

Table 10 – Traffic characterization (message size)

Application Name	Inter arrival Time (average)	Size (average)
File Server	155.118	220985.5175
Correio	286.3836	60448.04
SIAB	271.08	125869
IPX/NCP	93.01967	48558.9974

Table 11 – Simulation parameters

3. **Adjusting or fitting of distribution curves:** the simulator also needs the curves of characterized services probability distribution. Here, it is necessary to use curve-fitting software. The chosen tool was GraphPad Prism® of GraphPad Software Incorporated. This process concludes the characterization of the traffic for the simulation step. The Figure 5 presents an example of a curve that was fitted from the collected data. All application data passed through this step. The exponential distribution was considered the best fitting curve for both application parameters.
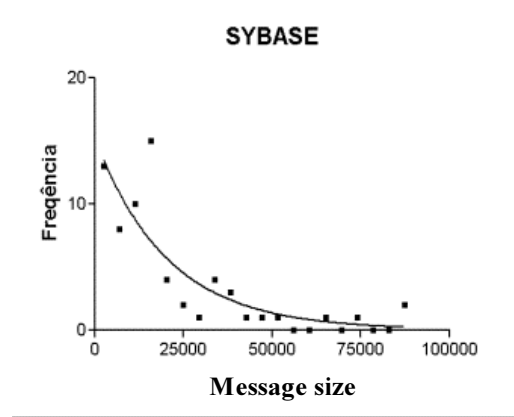

Figure 5 – Curve fitting

4. **Simulation modeling:** Identifying the installed capacity of the network (topology and network equipment features) and using the parameter from the previous steps, a model was built into the simulator. The Figure 6 presents an illustration about this step.
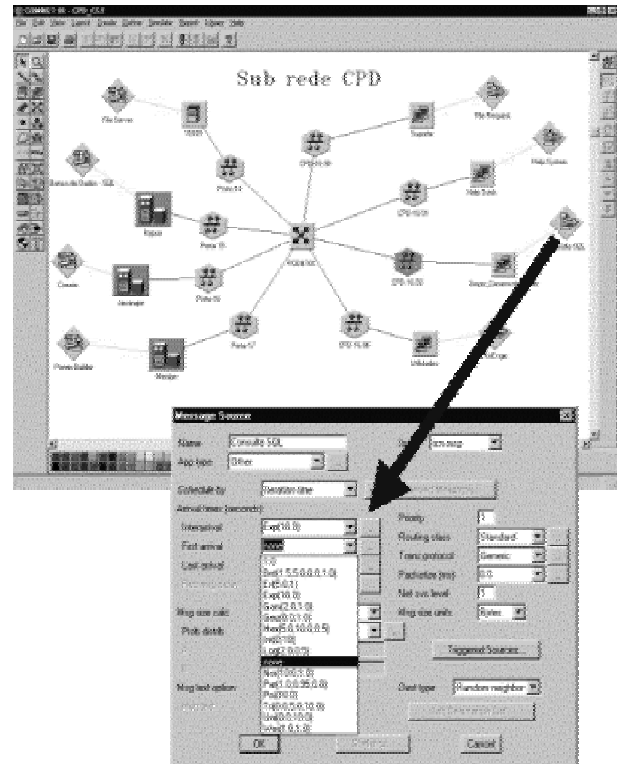

Figure 6 – Simulation model (data input)

5. **Model tuning:** some simulations running are made in order to compare the model with the real system. As soon as the model shows a good representation of the reality, it is considered calibrated. In order to tune the simulation model, it is necessary to do light changes in the curve parameters. In this case study, Network Utilization was used as reference to calibrate the model (segment X.X.16.92 utilization: approximately 21%).

6. **Simulation of the proposed changes:** the changes were simulated and the results were analyzed in order to determine the feasibility of the changes in the real system.

In this case study, a segment less loaded and physically close was chosen to receive a traffic fraction from the overloaded segment. That fraction is dependent of the overloaded segment workstation number. That allows the simulation of the workstation replacement in the segments. For example, the segment HUB-X.X.16.92 has 23 (twenty three) workstations, so we can consider that each workstation is responsible for 4,34% (approximately) of the total load in the segment. Such simplification becomes more valid when the users profile of the segment is more homogeneous. In the case of segment HUB-X.X.16.92, that condition was assumed provided that it was a segment of system development. In addition to that, all users are programmers and they use the same computer tools with very approximate use frequencies.

After three simulations, nine stations (three per "run") were moved from the segment HUB-X.X.16.92 to the segment HUB-X.X.16.90 (segment less loaded). However, the problem wasn't solved. The segment HUB-X.X.16.90 reached an average use above 11%, while the segment HUB-X.X.16.92 kept an average use considered high, above 15%. A second inference was tested to distribute users into the segments HUB-X.X.16.90 and HUB-X.X.16.86.

This second inference, after four simulations, allowed analyzing the load distribution in order to equal the use in all the modeled segments. All of them presented use around 10%. The Table 12 presents the results (load distribution).

CPD_inf2					
Segunda Inferência					
LINKS: CHANNEL UTILIZATION					
REPLICATION 1 FROM 5.0 TO 7200.0 SECONDS					
LINK	FRAMES DELIVERED	RST/ERR	TRANSMISSION DELAY (MS) AVERAGE	STD DEV	MAXIMUM	% UTIL
HUB-16.90	63632	0	0.753	11.500	1244.268	10.17
HUB-16.86	57080	0	0.658	7.297	1249.178	9.03
HUB-16.92	66011	0	0.766	10.608	1235.797	10.74
HUB-16.88	61229	0	0.572	1.342	219.194	9.57

Table 12 – Simulation results (load changing)

Nevertheless, another alternative was tested. The segment HUB-16.100 was added in order to contrast the cost and the benefit of investing in equipment, so the system capacity would be increased.

CPD_inf3					
Terceira Inferência					
LINKS: CHANNEL UTILIZATION					
REPLICATION 1 FROM 5.0 TO 7200.0 SECONDS					
LINK	FRAMES DELIVERED	RST/ERR	TRANSMISSION DELAY (MS) AVERAGE	STD DEV	MAXIMUM	% UTIL
HUB-16.90	15757	0	0.527	0.663	59.981	2.45
HUB-16.86	30957	0	0.561	1.419	176.574	4.80
HUB-16.92	63381	0	0.802	11.929	1253.554	10.33
HUB-16.88	50178	0	0.557	0.897	115.765	7.79
HUB-16.100	71417	0	0.788	12.131	1237.704	11.33

Table 13 Simulation results (new segment)

The involved segments in that third study presented use around 11%, what didn't modify the situation found (previous inference) a lot. It showed that the investment could be avoided if the average use of 11% were considered acceptable. The Table 13 presents the results with the insert of the new segment.

Once having arrived to satisfactory scenery, the alterations can be implemented in the real system. Until the elaboration of this paper, the real alterations were not ended.

VII. CONCLUSION

The proposed methodology in this paper for Computer Network Performance Management was considered quite useful, when used in a large computer network. It provided a direct and safe approach for performance problem and capacity planning solutions. In the case study, it allowed a fast detection of the main computer network performance problems. The phases of the methodology were led through a small platform to help the collection and data treatment, if necessary, for sniffer tools. In addition to that, it was possible to divide the performance evaluation problem in less complex sub-problems and, consequently, simpler to be analyzed. The real intervention was not concluded until the elaboration of this paper.

At this time we are investing efforts in the elaboration of a computer tool that consolidates the proposed methodology. Besides, we began a research work with the purpose of constructing an autonomous system of computer network management, associated to auxiliary tools, assuming the day-to-day tasks of a network Manager.

REFERENCES

[1] AccView®/*Open Network Management Software User's Guide*. Accton Technology Corporation, 1997.

[2] U. Black. *NetworkManagement Standards:SNMP, CMIP, TMN MIBs, and Object Libraries*. 2. ed. New York: MacGraw-Hill, 1995.

[3] CACI INC. *Reference Manual of Comnet III*. La Jolla, C.A. -USA – 1994.

[4] EcoSCOPE®/*EcoTools User's Reference Guide*. Compuware Corporation, 1998.

[5] Feit, S. *SNMP: A Guide to Network Management*. New York: MacGraw-Hill, 1995.

[6] Gordon, G. *System Simulation*, New Jersey: Prentice Hall, 1969.

[7] Gorrfried, B. S. *Elements of Stochastic Process Simulation*, New Jersey: Prentice Hall, Inc. – 1984.

[8] Jain, R. *The Art of Computer Systems Performance Analysis*. New York: John Wiley, 1991.

[9] Menascé, D., Almeida, V., Dowdy, L. *Capacity Planning and Performance Modeling*, New Jersey: Prentice Hall, 1994.

[10] Stallings, W. *Data and Computer Communications*. 5th ed. New Jersey: Printice

49

Hall, 1997.

[11] Stallings, W. *SNMPv1, SNMPv2, SNMPv3 e RMON 1 e 2*. 3$^{\underline{nth}}$. Massachusetts: Addison Wesley, 1999.

Ádrian Bonfá Drago é Engenheiro de Computação pela Universidade Federal do Espírito Santo (UFES), graduado em 1998, É Mestrando em Engenharia Elétrica – Automação pela UFES. Como aluno da UFES desenvolveu atividades de pesquisa e desenvolvimento e consultoria técnica especializada para empresas nas áreas análise e avaliação de desempenho de redes, Modelagem e simulação de tráfego de rede, Arquiteturas de Gerência de Redes. Professor da Fundação São João Batista (FSJB).
E-mail: adrian@inf.ufes.br

Prof. Dr. Anilton Salles Garcia é Engenheiro Mecânico pela Universidade Federal do Espírito Santo (UFES), graduado em 1976. É Mestre em Otimização e Pesquisa Operacional pela Universidade Estadual de Campinas (UNICAMP) em 1978 e Doutor em Engenharia Elétrica: Automação pela UNICAMP em 1987. Foi pesquisador por 05 (cinco) anos do Projeto UNICAMP/CPqD - Redes Digitais e Engenheiro de Projetos Sênior por 04 (quatro) anos da ELEBRA TELECOM Ltda, onde desenvolveu atividades de pesquisa e desenvolvimento e consultoria técnica especializada para empresas operadoras, nas áreas de Engenharia de Tráfego, Avaliação e Projeto de Sistemas de Comutação e Planejamento de Redes Telefônicas. Foi Consultor do Contrato UNICAMP/TELESP – Metodologia de Planejamento da Transmissão, no desenvolvimento de modelos e ferramentas computacionais para o planejamento do enfeixamento (bundling) em redes SDH. É Professor Adjunto (Licenciado) da UFES e Professor do Mestrado em Telecomunicações do INATEL. As principais áreas de atuação incluem Modelagem, Otimização e Projeto de Redes SDH, Modelagem de Tráfego e Avaliação de Desempenho de Redes, Análise e Projeto de Redes, Redes Multicamadas, Sistemas Distribuídos (CORBA), Redes Inteligentes e Arquiteturas de Gerência de Redes.
E-mail: anilton@inf.ufes.br

Maxwell E. Monteiro é Engenheiro de Computação pela Universidade Federal do Espírito Santo (UFES), graduado em 1997, É Mestre em Informática, concentração em Gerência de Redes de Computadores, UFES 2000. Professor da Fundação de Assistência e Educação – FAESA. Pesquisador do Laboratório de Pesquisa em Redes e Multimídia – LPRM. Consultor em Planejamento e Gerência de Redes de Computadores. Dentre as principais linhas de atuação e pesquisa estão: Sistema Especialistas para A Gerência de Redes, Arquiteturas para Sistemas Distribuídos, Planejamento de Capacidade de Sistemas Computacionais Distribuídos, Teste e Qualidade de Sistemas de Informação Distribuídos e Segurança de Redes.
E-mail: maxmonte@inf.ufes.br