Article ECORFAN Journal-Mexico
COMPUTING June 2015 Vol.6 No.14 1156-1161

Troubleshooting process in computer networks

MENDOZA, Luis*†, HERRERA, Francisco and SAMPERIO, Emmanuel

Received January 8, 2014; Accepted June 12, 2015

Abstract

One of the hardest things for administrators of computer networks is the solution of the problems that may arise in the infrastructure they manage. Troubleshooing is defined as the process of solution to a problem where the analysis and solution is included. Here are different methods and troubleshooting procedures exist to give the best solution to the problems that may arise in different types of computer networks of an organization or company.

Troubleshooting, Top-Down, Botton-Up, SNMP, Netflow, ping.

Citation: Mendoza, Luis, Herrera, Francisco and Samperio, Emmanuel. Troubleshooting process in computer networks. ECORFAN Journal-Mexico 2015, 6-14: 1156-1161

* Correspondence to Author (email: mendozaaustrial@hotmail.com)
† Researcher contributing first author.

© ECORFAN Journal-Mexico

Introduction

You could say that one of the hardest things for computer network administrators is the solution of the problems that may arise in the infrastructure they manage.

Troubleshooing [1] is defined as the process of solution to a problem where the analysis and solution is included.

The answer can be proactive, in the case of being the same person doing the troubleshooting who has found the problem or reactive if it has reached as trouble ticket or otherwise reported by a user or group.

The first step to take when the problem comes, the administrator is to gather as much information as possible related changes that had been made during the time that the problem occurred, etc., so that you can identify the root cause more precisely.

The selection and removal of all information relating not prevent the loss of time or even possible confusion.

Since the root cause of the problem is known to be looking for the best approach to resolve and depending on the situation can be a quick action (eg fix an RJ45 connector) or may take some time (eg replace an ethernet card), in If you can not resolve the problem instantly the next step is to ask whether a client is being affected, if so, should try to solve the connectivity for the client while the root cause is solved (for example, changing the port to which it is I connected that client).

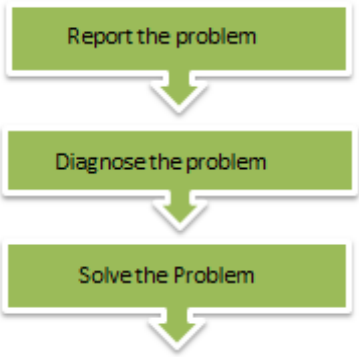

Figure 1 Steps to solving a problem

We present the methods, procedures and basic tools to be used for the best solution to a network problem, because if a structured process troubleshooting plan is not followed it may be that not remember something already done or just someone come to the aid and can not explain exactly what steps have been followed and in what order.

Schematic of a structured plan

A constitution a figure (Figure 1) showing the steps in a structured way, to reach the best solution to a problem of networks that we present is as follows:

ISSN-Print: 2007-1582- ISSN-On line: 2007-3682
ECORFAN® All rights reserved.

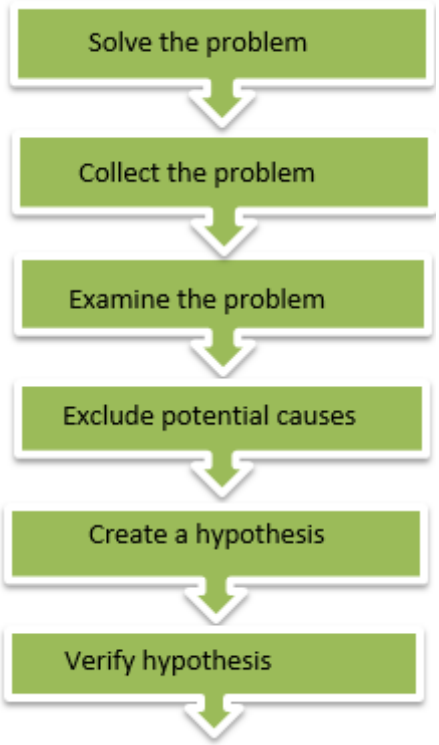

Figure 2 structured plan

However it may happen that the problem you have is familiar and already knows how to solve it. This method is commonly referred to shoot from the hip.

Outline of a shoot from the hip plan

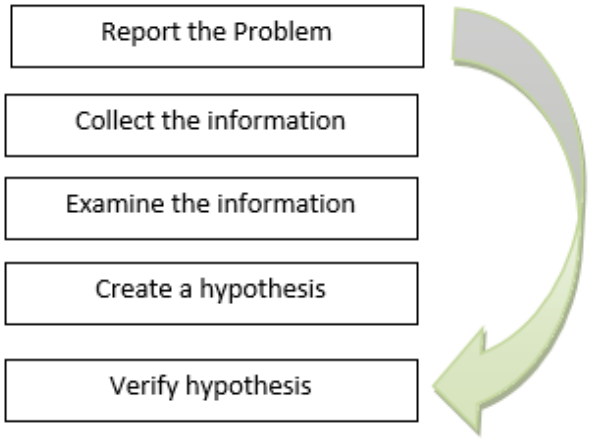

Figure 3 Schematic plan of a shoot from the hip

Methods troubleshooting

Then several troubleshooting methods widely used are:

Top-Down Method: Based on start searching for the problem in the higher layers of the OSI model, assuming that if certain layer operates there under so will.

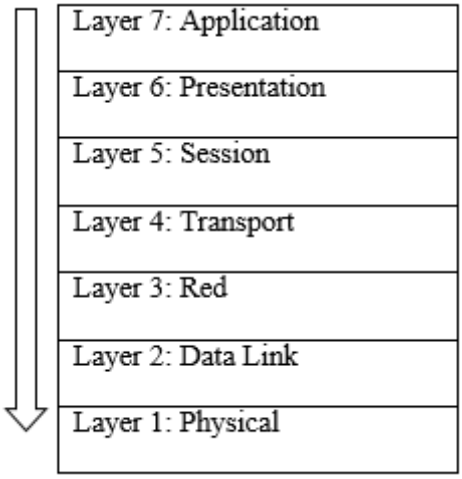

Figure 4 Top-down method

Bottom-Up Method: This is the opposite case of the above method. It can be very effective but slow in large networks.

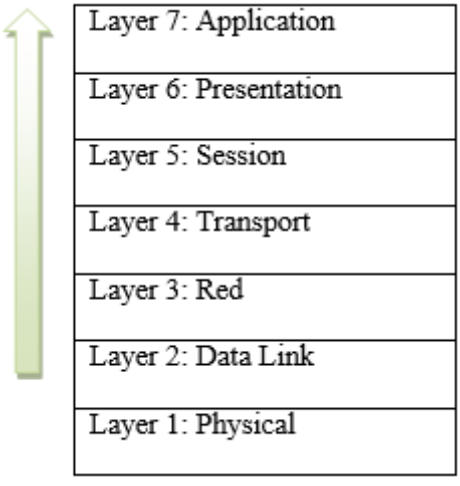

Figure 5 Bottom-Up Method

ISSN-Print: 2007-1582- ISSN-On line: 2007-3682
ECORFAN® All rights reserved.

Divide and Conquer Method: In this method should first check the intermediate layers of the OSI model, the test is successful if it is assumed that the part relating to the first is correct to focus on the second part. Otherwise the problem is sought in the first half.

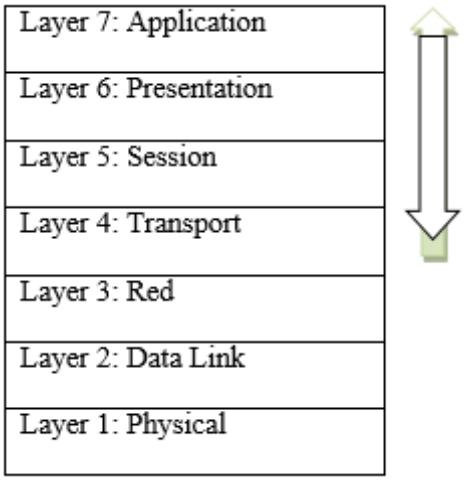

Figure 6 Method Divide and Conquer

Traffic monitoring method: Based on the analysis of the devices between the origin and destination traffic.

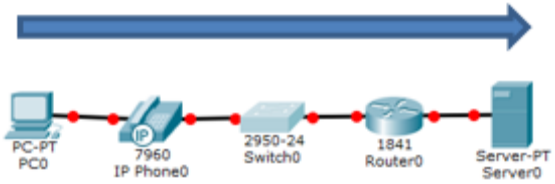

Figure 7 Method traffic monitoring

Method to compare configurations: It is especially useful in cases where after making a change in network problems occur. It is simply based on comparing the current configuration with the last known good.

Method of replacing parts: It consists physically replace parts that form the network segment where there are problems. It is very useful when you are doing troubleshooting and error level 1 of the OSI model are verified, for example by failing to Internet on a host physically first check the network card, cable, connector port router, etc.

Troubleshooting procedures

A good structured troubleshooting process helps to more efficiently use resources in an enterprise and, in case an administrator must continue the work of another will be easier to take. Through the combination of the above steps, the following process is obtained structured:

Report of the problem. Normally it gives someone who makes use of network resources, and often this information is inaccurate and sometimes erroneous. Someone reporting problems primarily serve to identify that part of the network has been affected, which devices or group is responsible for the failure.

Gather your information. Once the bug has been reported and identified part of the network that has the problem, you should gather as much information as possible from both the affected devices, such as logs, historical changes, etc. In case there are network devices that do not have access will need to contact the relevant groups for this information.

Examine the information collected. After gathering all the necessary information must be thoroughly analyze it, always being aware of:

- Identify the root causes that target problem.
- Remove unnecessary information.

Depending on the degree of experience of the administrator must make some questions to be answered more or less quickly, you need to analyze all the information it collected, or just watching the behavior of network protocols, etc. These questions can be such as:

What is happening in the network?

What I should be happening?

ISSN-Print: 2007-1582- ISSN-On line: 2007-3682
ECORFAN® All rights reserved.

How should I be working?

Eliminates potential causes. Once the data considered must discard information on causes not own the problem and what is very important not imagine or wish to make based on data that are not on the information collected hypothesis.

Create a hypothesis for the cause. After eliminating potential causes, you should focus only on the cause believed to be the final. In case you have access to the device will proceed to try to solve the problem. Failure to access the device should look for an alternative solution through appropriate network administrator.

Verify the hypothesis. Once we know the cause can try to resolve it. It is important to think about how to act because the fact immediately implement the solution can cause network outages, then perhaps better plan for a better intervention, at night or when the impact is minimal now.

It is very important to document all the changes that apply to that case the intended solution does not solve the problem possible to step back and think of another solution.

Problem solution. Once the problem is solved, it should clearly documented as was the solution, and all parties are to receive an explanation of what happened and how it was solved.

Tools for maintenance and throubleshooting

He is also familiar with the important tools troubleshooting connectivity built, that come with the operating system you are using.

Some of these basic tools are:

Ping: the function uses ICMP echo (Internet Control Message Protocol) and is the lowest level test to determine if a host is connected. Ping is a tool that checks whether a remote computer is functioning properly and whether the network connections are intact [7].

Ping is extremely useful for troubleshooting at Layer 3 level, not only indicates whether a particular host is active or not, but also offers the possibility of extra parameters that provide much more information.

Traceroute (Tracert aka): Follow the path of a packet until it reaches its destination. That is measures how long it takes for a packet on its way through each hop to reach its destination [7].

Pathping: A routing tool that combines features of Ping and Tracert along with other information.

IPconfig: Check the IP configuration of your computer and outputs the information used to determine whether the computer has proper connectivity to the network.

Telnet: used to test connectivity from a remote host or server.

Netstat: Lists all the TCP / UDP ports listening to your server, including all active network connections to and from your server.

Network Monitor: Lets you capture the network packets for further analysis.

SNMP: Collects device statistics such as resource utilization, number of errors at different counters, etc. It employs a so-called pull station where NMS (Network Management Station) requested statistics periodically. This widespread, one can say that virtually any network device can use SNMP [6].

ISSN-Print: 2007-1582- ISSN-On line: 2007-3682
ECORFAN® All rights reserved.

Netflow: Collect samples of traffic. Uses a model called push. That is, the device from time to time send a sample of the traffic to another device called a collector. It is available only in routers and high-end switches.

Conclusions

A computer network is a complex system that cannot be created or working for you. The network administrator should be able to configure, monitor and properly plan their evolution. In addition, Network Manager is expected to quickly resuelver Network problems and derivatives users. It is vital to have the resources and skills to logically determine the cause of the problem and how to solve it.

With the application of methods and troubleshooting procedures presented in this document, the administrator can now formulate a methodology to detect and identify problems in a systematic and logical manner and thus arrive at the best solution for the problems in your network computer.

References

Ariganello E. (2011). Redes Cisco guía CCNP, México: Alfaomega

Stallings W. (2005). Redes e Internet de Alta Velocidad. Madrid: Pearson Prentice all

Barcia N., Fernandez C.Frutos S., (2005) Redes de computadores y arquitecturas de comunicaciones. Madrid: Prentice-Hall,

Behrouz A. F. (2006). Treansmisión de datos y redes de comunicaciones. Madrid: Mc Graw Hill

Ariganello E. (2011). Redes Cisco guía CCNA México: Alfaomega

Tanembaum A. (2014) Redes de computadoras. México: Pearson. 5ta Edición

Beasley J.S. (2008), "Networking". Michigan: Pearson Education

Academia de Networking de Cisco Systems (2008). Guía del segundo año CCNA 3 y 4". Madrid: Cisco Press.

Kurose James F., Ross Keith W., (2012), Redes de Computadoras. México: Pearson. 5ta Edición.

ISSN-Print: 2007-1582- ISSN-On line: 2007-3682
ECORFAN® All rights reserved.