Journal of Computer Hardware Engineering(2018)

Original Research Article

Computer Network Failure and Solution

Yunzhou Han,Xianglin Zhao,Jianbin Li

School of Computer Engineering, Nanchang University of Technology, Jiangxi, China

ABSTRACT

This paper introduces the basic concept of network and router, briefly introduces the network layered diagnosis technology, discusses the diagnosis of various interfaces of the router, and summarizes the troubleshooting of Internet connectivity fault.

KEYWORDS: network internet router fault diagnosis

1. Introduction

1.1. Background and purpose of the project

From an international perspective, the military network management and fault diagnosis has gone through the process from scratch, and now from the primary to the advanced, from imperfect to perfect, from the concentration to the decentralized development goals. To achieve the scientific and standardized fault diagnosis has become a sustained, high-speed, healthy development of the major issues. In the US '2010 Joint Concept', the first communication failure management as 'dominate the mobile, precision strike, full-dimensional protection,' one of the four principles of combat.

1.2. Overview of Computer Networks

1. The computer network is composed of a computer set plus communication facilities, that is, the use of various means of communication, the geographical dispersion of the computer together to achieve mutual communication and sharing software, hardware and data resources and other systems. The computer network according to its computer distribution range is usually divided into local area network and wide area network. LAN coverage of the geographical range is small, usually in the number of meters to tens of kilometers. Wide coverage of the geographical area, such as campus, between cities, and even the world. The development of computer networks leads to various forms of connection between networks. The use of a unified protocol to achieve the interconnection of different networks, so that the Internet can easily be extended. The Internet is in this way to complete the network between the network connections. The Internet uses the TCP / IP protocol as a communication protocol to connect world-wide computer networks to become the world's largest and most popular international network.

1.3. Common computer network fault classification and impact

Network fault diagnosis should achieve three purposes:

Determine the network point of failure to restore the normal operation of the network;

Identify poor network planning and configuration to improve and optimize network performance;

Observe the operation of the network, and timely predict the quality of network communications.

Network fault diagnosis is based on knowledge of network principles, network configuration and network operation. From the fault phenomenon, to network diagnostic tools as a means to obtain diagnostic information to determine the network failure point, find the root cause of the problem, troubleshooting, restore the normal operation of the network. Network failure usually have the following possibilities: the physical layer of physical equipment connected to each other failed or hardware and line itself; data link layer network equipment interface configuration problems; network layer network protocol configuration or operation error; transport layer equipment Performance or communication congestion problems; upper three layers of CISCO IOS or web application errors. The process of diagnosing a network

failure should proceed from the physical layer along the OSI seven-layer model. First check the physical layer, and then check the data link layer, and so on, try to determine the failure of the communication point, until the system communication is normal.

Network diagnostics can use a variety of tools, including LAN or WAN analyzers: router diagnostic commands; network management tools and other troubleshooting tools. CISCO provides enough tools to exclude the vast majority of network failure. Look at the routing table is a good place to solve the network failure. ICMP's ping, trace command, and Cisco's show command, the debug command is a network tool that gets useful information for troubleshooting. We usually use one or more commands to collect the corresponding information, in a given case, to determine what command to use to obtain the required information. For example, the common method of using the IP protocol to determine whether a device can be reached is to use the ping command. Ping sends an ICMP packet from the source point to the destination. If successful, the ping packet returned will confirm that all the physical layer, the data link layer, and the mesh layer function from the source point to the target are running normally. How to run the Internet after the understanding of its information to understand whether the network is running, monitor and understand the network under normal conditions to run the details, to understand the situation of failure. Monitor those contents? Using the show interface command, you can easily get information about each interface to be checked. In addition show buffer command to provide regular display buffer size, use and use of the situation. The Show proc command and the show proc mem command can be used to track processor and memory usage, which can be collected on a regular basis and used for diagnostic references when a failure occurs. Network failure is manifested in a symptom that includes general (like a user cannot access a server) and a more specific (if the router is not in the routing table). Use a specific troubleshooting tool and method for each symptom to find out one or more of the cause of the failure.

2. The common computer network failure to judge

2.1. To solve the meaning of computer network failure

At the turn of the century, the rapid development of the global Internet. Seize the opportunity to meet the challenges of China's network construction in the ascendant. Government Internet project kicked off, the new upsurge of network construction has arrived. Network diagnosis is one of the important technical tasks to manage and make good use of the network and make the network play the greatest role. This paper first briefly introduces the basic concepts of network and router, briefly introduces the hierarchical diagnosis technology, discusses the diagnosis of various interfaces of the router, and summarizes the troubleshooting of Internet connectivity faults.

2.2. Computer network failure classification

2.2.1 Classification of computer network faults

Although there are a variety of network failure, but all the fault can be divided into physical failure and logical failure, which is commonly referred to as hardware failure and software failure.

Hardware failure and software failure

Hardware failure has a network card, network cable, hub (Hub), switches, routers and so on.

The most common situation in a software failure is network protocol problems or network anomalies or failures due to network device configuration reasons.

Computer network fault judgment procedure

1.First check the network card is normal.

Each card is equipped with LED indicator, the location is generally in the main chassis on the back of the green light that is connected to the normal some green and red light should be bright, red light that connection failure, no light that no connection or line barrier. Depending on the size of the data flow, the indicator will flash slowly. Under normal circumstances, when the data is not transmitted, the network card light flashes slowly, when sending data, flashing faster.

2. Connect the computer and other network equipment jumper, cable is smooth. The failure of the network connection usually includes the network line internal fracture, twisted pair, RJ-45 crystal head bad contact. Can be used to detect the line.

3. Both sides of the RJ-45 head is inserted.

4. Whether the information outlet is faulty.

Cause of issue

Although the reasons for the failure of a variety of, but in general nothing more than hardware problems and software problems, put it some more, these issues are network connectivity issues, configuration file options and network protocol issues.

1. Network connectivity

2. Network connectivity is the first time after the failure should be considered. Connectivity problems usually involve network cards, jumpers, information outlets, network cables, Hub, Modem and other equipment and communication media. Among them, any one of the equipment damage, will lead to interruption of network connection. Qualification can usually be software and hardware tools for testing and verification. The following are the same as the '

Excluding the improper configuration of the computer network protocol and the possibility of failure, you should check the network card and Hub indicator is normal, measuring the cable is smooth.

2. Configuration files and options

Servers, computers have configuration options, configuration files and configuration options are not properly set, the same will lead to network failure.

2.2.2 Computer network failure symptoms

1. Connectivity failure

Fault performance

Connectivity failures are usually expressed in the following cases:

The computer cannot log in to the server;

1. computer cannot access the Internet through the LAN;

2. computer in the 'Network Neighborhood' can only see themselves, and cannot see other computers, which cannot use other computers on the shared resources and shared printers;

3. computer cannot be achieved within the network access to other computer resources;

4. some of the computer in the network running speed is unusually slow.

2. The cause of the malfunction

The following causes may cause connectivity failure:

1. NIC is not installed, or is not installed correctly, or with other equipment conflict;

2. network card hardware failure;

3. network protocol is not installed, or set incorrectly;

4. cable, jumper or information outlet failure;

2.3. Various tools for network diagnostics

2.3.1. The software tool is ping

Ping is undoubtedly the most frequent gadget in the network, it is mainly used to determine the network connectivity issues. The ping program uses the ICMP (Internet Message Control Protocol) protocol to simply send a network packet and request a response. The destination host receiving the request sends back the same data again using ICMP, so that ping can send and receive each packet time to report and report the percentage of packets without impact, which is useful in determining whether the network is properly connected and the status of the network connection (packet loss rate). Ping is one of the Windows operating system integrated TCP / IP applications that can be executed directly in 'Start-Run'

(1) Command format:

Ping the hostname or ping the hostname -t

Ping the IP address or ping the IP address -t

(2) The application of the ping command

Ping the local computer name (ie. the computer that performs the operation)

Such as ping liu or ping local IP address

Such as ping127.0.0.1 (any computer will be 27.0.0.1 as its own IP address)

You can check whether the computer has a network card installed; whether the correct installation of the TCP / IP protocol; correctly configured IP address and subnet mask or host name.

(3) Common mistakes that occur after using the Ping command

Error messages are usually divided into four types:

1.Unknown host

Unknown host (unknown host), this error message means that the name of the remote host cannot be converted to an IP address by a named server. The cause of the failure may be that the naming server is faulty, or its name is incorrect, or that the communication line between the network administrator's system and the remote host is faulty.

2.3.2 Diagnostic hardware tools

You can use this tester to test the continuity of the cable. General station does not have this kind of equipment, but it is very simple to use, the two ends of the network cable were inserted into the tester, open the tester's power, which has eight lights, if the light is the cable is through. If there is no network test with a three-meter test cable off the line, just need two people with two tables tested.

3. Common computer network failure solution

3.1. To solve the theoretical basis of network failure (basic principles)

3.1.1 International Standardization Organization (ISO) open system interconnection reference model

Physical layer is the reference model of the lowest level. The layer is the network communication data transmission medium, by connecting different nodes of the cable and equipment together constitute. The main function is: the use of transmission media for the data link layer to provide a physical connection, responsible for handling data transmission and monitoring data error rate for the transparent transmission of data flow.

The data link layer is the second layer of the reference model. The main function is to establish a data link connection between the entities of the communication based on the services provided by the physical layer and transmit the data packets in units of 'frames', and adopt the error control and flow control method to make the error physical lines into an error-free data link.

The network layer is the third layer of the reference model. The main function is to create a logical link for data transmission between nodes, to select the most suitable route for the packet through the communication subnet, and to implement congestion control and network interconnection through the routing algorithm.

Transport layer is the reference model of the fourth layer. The main function is to provide users with reliable End-to-End services, handling packet errors, packet order, and other key transport issues. The transport layer shields the upper layer from the upper layer of the details of the underlying data communication, so it is a critical layer in the computer communication architecture.

Session layer is the reference model of the first five layers. The main function is to maintain the transmission link between the two nodes in order to ensure that point-to-point transmission is not interrupted, and the management of data exchange and other functions.

Presentation layer is the sixth layer of the reference model. The main function is to deal with the exchange of information in two communication systems, including data format conversion, data encryption and decryption, data compression and recovery functions.

Application layer is the reference model at the highest level. The main function is: for the application software provides a lot of services, such as file servers, database services, e-mail and other network software services.

3.1.2 Network communication protocol

Commonly used three network protocols

Different workstations in the network, the server can transfer data, from the existence of the agreement. With the development of the network, different developers have developed different ways of communication. In order to make the communication successful and reliable, all hosts in the network must use the same language, cannot bring dialect. Many protocols have been developed, but only a few have been retained. What are the reasons for the elimination of those agreements - poor design, poor implementation or lack of support. And those who have survived the agreement has gone through the test of time and become an effective communication method. The three most common protocols in today's LAN are MICROSOFT NETBEUI, NOVELL's IPX / SPX and cross-platform TCP / IP.

1: NETBEUI

NETBEUI is a non-routing protocol developed for IBM for communicating with NETBIOS. NETBEUI lacks routing and networking

Layer addressing function, both its biggest advantage, but also its biggest drawback. Because it does not require additional network addresses and network layer head and tail, so quickly and very effective and applies only to a single network or the entire environment are bridging the small workgroup environment. Because routing is not supported, NETBEUI will never become the primary protocol for enterprise networks. The only address in the NETBEUI frame is the Data Link Layer Media Access Control (MAC) address, which identifies the network card but does not identify the network. The router forwards the frame to the final destination by the network address, and the NETBEUI frame is completely lacking the information. The bridge is responsible for forwarding traffic between networks according to the data link layer address, but there are many drawbacks. The NETBEUI specifically includes the count of broadcast traffic and relies on it to resolve naming conflicts. In general, bridging NETBEUI networks rarely exceeds 100 hosts. In recent years, networks that rely on Layer 2 switches have become more common. The complete conversion environment reduces the utilization of the network, although the broadcast is still forwarded to each host in the network.

2: IPX / SPX

IPX is the protocol group for NOVELL for the NETWARE client / server, avoiding the weakness of NETBEUI. But brought new different weaknesses. IPX has full routing capabilities that can be used for large enterprise networks. It includes a 32-bit network address, allowing a number of routing networks in a single environment. IPX's scalability is limited by its high-level broadcast traffic and high overhead. The Service Advertising Protocol (SAP) limits the number of hosts in the routing network to thousands. Although the limitations of SAP have been overcome by intelligent routers and server configurations, the administrators of large-scale IPX networks are still very difficult to work.

3: TCP / IP

Each network protocol has its own advantages, but only TCP / IP allows full connection with the Internet. TCP / IP was developed by the Massachusetts Institute of Technology and some commercial organizations for the US Department of Defense in the 1960s, and even if most of the networks were destroyed by nuclear attacks, TCP / IP was able to maintain effective communications. ARPANET is developed by protocol-based and developed into an Internet that communicates as a scientist and engineer. TCP / IP also has the scalability and reliability requirements.

3.1.3 CISCO routers and switches

Network diagnosis is a comprehensive technology, involving all aspects of network technology. To facilitate the following discussion, first of all, a brief review of the basic concepts of network and router.

1. A computer network is a system consisting of a computer set plus a communication facility that uses a variety of means of communication to connect geographically dispersed computers to communicate with each other and share resources such as software, hardware, and data. The computer network according to its computer distribution range is usually divided into local area network and wide area network. LAN coverage of the geographical range is small, usually in the number of meters to tens of kilometers. Wide coverage of the geographical area, such as campus, between cities, and even the world. The development of computer networks leads to various forms of connection between networks. The use of a unified protocol to achieve the interconnection of different networks, so that the Internet can easily be extended. The Internet is in this way to complete the network between the network connection. The Internet uses the TCP / IP protocol as a communication protocol to connect world-wide computer networks to become the world's largest and most popular international network.

2. In order to complete the communication between computers, the function of each computer interconnection is divided into a well - defined level, which stipulates the protocol and the interface and service between the adjacent layers. The layers and the same layer process protocol between the communication and the interface between the adjacent layers are collectively referred to as the network architecture. The Open Systems Interconnection Reference Model (OSI) proposed by the International Organization for Standardization (ISO) is at the heart of the contemporary

computer network technology system. The model divides the network function into seven levels: the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer and the application layer.

3. TCP / IP is the transmission protocol and the interconnection protocol is a set of network protocols. TCP / IP originated in the United States ARPANET network, the development has become the Internet to use the standard communication protocol. Using TCP / IP enables computers that use different operating systems to exchange data in an orderly manner.

3.2. To solve the fault of the work steps

3.2.1 Network Fault Hierarchical Diagnostic Technology

1. Physical layer and its diagnosis

The physical layer is the most basic layer of the OSI hierarchical architecture. It is based on the communication medium, realizes the physical interface between the system and the communication medium, transparently transmits the data link entities, establishes, holds and dismantles The physical connection between the computer and the network provides services.

The physical layer fault is mainly manifested in the physical connection of the equipment is appropriate; connection cable is correct; MODEM, CSU / DSU and other equipment configuration and operation is correct.

The best way to determine whether a physical port of a router port is intact is to use the show interface command to check the status of each port, to interpret the screen output information, to view the port status, protocol setup status, and EIA status.

2. Data link layer and its diagnosis

The main task of the data link layer is to make the network layer to obtain reliable transmission without having to understand the characteristics of the physical layer. The data link layer is used to package and unpack the data through the link layer, error detection and certain correction capability, and coordinate the shared media. Before the data link layer exchanges data, the protocol is concerned with the formation of frames and synchronization devices.

To find and troubleshoot the data link layer, you need to check the configuration of the router and check the encapsulation of the same data link layer of the connection port. Each pair of interfaces must be the same as other devices that communicate with it. Check the encapsulation by checking the configuration of the router, or use the show command to view the encapsulation of the interface.

3.2.2 Hardware diagnosis

1. Serial troubleshooting

Serial connectivity problems, in order to rule out the serial port failure, usually from the show interface serial command to start, analyze its screen output report content, find out where the problem lies. The serial interface reports the status of the interface and the status of the line protocol. The possible combinations of interfaces and line protocols are as follows: 1) Serial operation, line protocol operation, which is complete operating conditions. The serial port and the line protocol have been initialized and are exchanging the protocol's survivor information. 2) The serial port is running and the line protocol is off. This display indicates that the router is connected to the device that provides the carrier detection signal, indicating that the carrier signal is present between the local and remote modems, but does not correctly exchange the protocol survivable information at both ends of the connection. Possible failures occur when a router configuration problem, a modem operation problem, a leased line interference, or a remote router failure, a digital modem clock problem, and two serial ports connected through a link are not on the same subnet. 3) serial and line protocols are closed, may be the telecommunications sector line failure, cable failure or a modem failure. 4) The serial port management closes and the line protocol is closed. In this case, the shutdown command is input in the interface configuration. Open the administrative shutdown by entering the no shutdown command.

Both the interface and the line protocol are running, although the basic communication of the serial link is established, there may still be many potential fault problems due to packet loss and packet errors. Normal communication interface input or output packets should not be lost, or the amount of loss is very small, and will not increase. If the packet loss is regularly increased, it indicates that the traffic transmitted through the interface exceeds the traffic that the interface can handle. The solution is to increase the line capacity. Look for other causes of loss of packets, see the status of the input and output queue in the output report of the show interface serial command. When it is found that the number of packets in the keep queue reaches the maximum allowable value of the information, the size of the queue can be increased.

2. Ethernet interface troubleshooting

Typical fault problems for Ethernet interfaces are: excessive use of bandwidth; frequent collision collisions; use of incompatible frame types. Use the show interface ethernet command to view the throughput, collision, packet loss, and frame type of the interface.

1) You can detect the use of the network by looking at the throughput of the interface. If the percentage of webcast packets is high, network performance begins to decline. Fiber-optic network conversion to the Ethernet segment of the packet may be drown Ethernet port. Internet this can happen with the optimization of the interface, that is, the Ethernet interface using the no Ip route-cache command to disable fast conversion, and adjust the buffer and keep the queue.

2) When two interfaces attempt to transmit packets to the Ethernet cable at the same time, a collision occurs. Ethernet requires a small number of conflicts, different network requirements are different, the general situation found that there are 3,5 times per second conflict should find the reasons for the conflict. The cause of the conflict is usually due to the laying of the cable is too long, excessive use, or 'deaf' node. The Ethernet network should be considered in the physical design and laying of cable system management, and super-standard laying of cables may cause more conflicts to occur.

3.3. Network Security

1. Firewall technology

At present, the firewall has two key technologies, one packet filtering technology, the second is the proxy service technology.

(1) Packet filtering technology

Packet filtering technology is mainly based on the routing technology, that is, based on static or dynamic filtering logic, in the packet before forwarding the packet according to the destination address, source address and port number to filter the packet. Packet filtering cannot identify user information and file information in packets, and can only provide protection for the entire network. In general, the packet filter must use two network cards, that is, a card connected to the public network, a network card connected to the network, in order to achieve real-time and two-way online communication control.

Packet filtering technology has the advantages of fast running and basically independent of the application, but the packet filtering can only operate according to the security rules of the existing packet filtering, and cannot carry out various requirements of the service on some protocols Are dealt with separately, that is, only to allow or reject a certain type of service mechanically, and cannot control a specific operation in the service. Therefore, for some services from unsafe servers, relying solely on packet filtering cannot play the role of protecting the internal network.

(2) Agency service technology

Proxy services, also known as application-level firewall, proxy firewall or application gateway, generally for a particular application to use a specific proxy module. The proxy service consists of the proxy client of the client and the proxy server of the firewall. It not only understands the information of the packet header, but also understands the contents of the application information itself. When a remote user connects to a network running a proxy service, the proxy server at the firewall is connected and the IP packets are forwarded forward and forward.

2. Antivirus technology

Internet communication and exchange of information for the human at the same time, but also for the spread and development of computer viruses provide a good platform for the network virus is at an alarming rate, toward a more destructive, more subtle, higher infection rate, spread faster, more types, to adapt to the broader direction of the development platform. Computer network security to prevent an important content is to fully ensure the safety of computer networks and the impact of the minimum impact on the premise of the computer network, effectively prevent the invasion of computer viruses. In Internet access such as firewall, router, proxy

3.4. Resolving an example of a computer network failure

Before starting to troubleshoot, it is best to prepare a pen and a notepad, and then, the fault will be carefully recorded. In the observation and record must pay attention to the details of the exclusion of large-scale network failure so, generally more than a dozen small computer network failure is also true, because sometimes it is some of the smallest details make the whole problem becomes clear.

General troubleshooting mode is as follows: The first step, when the analysis of network failure, we must first clear the fault phenomenon. The symptoms of the failure and the underlying cause should be specified. To this end, to determine the specific phenomenon of failure, and then determine the cause of such a fault phenomenon of the

type. The second step is to collect the information needed to help isolate the cause of the possible failure. To the user, network administrators, managers and other key figures to mention some and fault-related issues. Extensive collection of useful information from network management systems, protocol analysis trails, output reports of router diagnostic commands, or software manuals. The third step, according to the collected situation to consider the possible causes of failure. Can be excluded according to the relevant circumstances of some of the reasons for the failure. The fourth step, according to the final possible cause of the failure, to establish a diagnostic plan. Start with only one of the most likely cause of failure to diagnose the activities, so you can easily return to the original state of failure. If you consider more than one failure at the same time, trying to return to the original state of the fault is much more difficult. The fifth step, the implementation of the diagnostic plan, do a good job every step of the test and observation, until the symptoms disappeared. The sixth step, each change a parameter to confirm the results. Analysis of the results to determine whether the problem is resolved, if not resolved, continue until resolved.

1. Identify the fault phenomenon

2. As a manager, before you fail, you must also know exactly what problems on the network in the end, is not able to share resources, or cannot find another computer, and so on. Know what problems and be able to identify in a timely manner, is the most important step to successfully remove the fault. In order to compare with the phenomenon of failure, as an administrator you must know how the system works under normal circumstances, on the contrary, you are not good on the problem and fault positioning.

To identify the phenomenon of failure, you should ask the operator the following questions:

(1) What process is running when the logged fault occurs (what the operator is doing with the computer).

(2) Has this process been run before?

(3) Before the operation of this process is successful?

(4) When the last successful operation of this process is what time?

(5) Since then, which has changed?

With these questions to understand the problem, in order to prescribe the fault.

2. The failure of a detailed description of the phenomenon

A detailed description of the fault phenomenon is particularly important when dealing with problems reported by the operator. If only their side of the word, and sometimes it is difficult to conclusions, then you need to personally operate the administrator just wrong procedures, and pay attention to error messages. For example, when using a Web browser to browse, regardless of which site to enter the 'page cannot be displayed' and the like. When using the ping command, regardless of which IP address is displayed, the timeout information is displayed. An error message such as this will provide a lot of valuable information for narrowing the scope of the problem. Before you can troubleshoot, you can follow these steps:

(1) To collect information about the phenomenon of failure;

(2) A detailed description of the problem and the phenomenon of failure;

(3) Attention to detail;

(4) Write down all the questions;

(5) Do not rush to conclusions.

3. Lists the reasons that may lead to errors

As a network administrator, you should consider what may be the cause of the failure to view the information, such as network card hardware failure, network connection failure, network equipment (such as hubs, switches) failure, TCP / IP protocol settings and so on.

Note: Do not worry about the conclusions, according to the possibility of error to these reasons to sort the priority level, one by one to exclude.

4. Narrow the search range

Test all of the listed causes that may lead to errors, and do not determine that a region's network is functioning properly or not, based on a test. In addition, do not think that you have identified the first mistake.

In addition to testing, the network administrator should also pay attention: Do not forget to look at the network card, Hub, Modem, router panel LED lights. Normally, the green light indicates that the connection is normal (the modem needs several green and red lights), the red light indicates that the connection is faulty and does not indicate that

there is no connection or line. Depending on the size of the data flow, the indicator will flash slowly. At the same time, do not forget to record all the means of observation and testing and results.

5. Isolated error

After you have some toss, then you basically know the fault of the site, for the computer error, you can start to check whether the computer network card is installed, TCP / IP protocol is installed and set up correctly, Web browser connection Whether the settings are appropriate and everything related to the known fault phenomenon. And then the rest of the thing is troubleshooting.

Note: Do not forget the static damage to the computer when opening the chassis, to properly remove the computer components.

6. Fault analysis

After dealing with the problem, as a network administrator, you must also figure out how the failure occurred, what is the cause of the failure occurred, how to avoid the occurrence of similar failures, the development of appropriate countermeasures, take the necessary measures to develop strict Rules and regulations.

3.5. Computer network troubleshooting methods

1. Confirm connectivity failure

When a network application fails, if you cannot access the Internet, first try to use other network applications, such as looking for other computers in the network, or use the LAN in the Web browser. If other network applications can be used normally, if you cannot access the Internet, but in the 'Network Neighborhood' to find other computers, or can ping to other computers, you can rule out the cause of connectivity problems. If other network applications cannot be achieved, continue to the following operation.

2. See LED lights to determine the failure of the card

First check the card's indicator is normal. Under normal circumstances, when the data is not transmitted, the network card light flashes slowly, when sending data, flashing faster. Whether it is not bright, or long bright immortal, that there are failures exist. If the card is not normal, you need to turn off the computer to replace the card. For the hub of the lights, those who plug the network cable, the lights are lit. Because it is Hub, so the role of the indicator can only indicate whether the port is connected to a terminal device, cannot display the communication status.

3. Use the ping command to exclude network card failure

Use the ping command, ping the local IP address or computer name (such as ybgzpt), check the network card and IP network protocol is installed intact. If you can ping, indicating that the computer's network card and network protocol settings are no problem. The problem lies in the connection between the computer and the network. Therefore, you should check the network and Hub and Hub interface status, if you cannot ping, only that TCP / IP protocol problems. Then you can in the computer's 'control panel' of the 'system' to see whether the network card has been installed or whether the error. If the network adapter is not found in the hardware list on the system, or if there is a yellow '!' In front of the network adapter, the network card is not installed correctly. Need to remove the unknown device or with a yellow '!' Network adapter, refresh, re-install the network card. And correctly install and configure the network protocol for the network card, and then apply the application test. If the card cannot be installed correctly, indicating that the card may be damaged, you must change a network card to try again. If the network card is installed correctly, the reason is that the protocol is not installed.

4. If the card and the agreement to determine the correct case, or the network barrier, can be initially concluded that the problem is Hub and twisted pair. In order to further confirm, you can change a computer with the same method to judge. If other computers and the machine is connected properly, the fault must be on the previous computer and Hub interface.

5. If you have determined that the Hub is faulty, you should check whether the indicator of the Hub is normal. If the interface between the previous computer and the Hub is off, the interface of the Hub is faulty. (The Hub indicator indicates the port of the network cable. Lights, the indicator cannot display the communication status).

Through the above fault compression, we can determine the fault in the network card, twisted pair or Hub.

Protocol failure

1. The performance of the agreement failure

Protocol failures are usually expressed in the following cases:

(1) The computer cannot log in to the server.

(2). computer in the 'Network Neighborhood' in both see themselves, cannot access other computers in the network.

(3). computer in the 'Network Neighborhood' can see themselves and other members, but cannot access other computers.

(4). computer cannot access the Internet through the LAN.

2. The cause of failure analysis

(1) Protocol is not installed: to achieve LAN communication, need to install NetBEUI protocol.

(2) Protocol configuration is not correct: TCP / IP protocol involves the basic parameters of four, including IP address, subnet mask, DNS, gateway, any one set wrong, will lead to failure.

3. The exclusion step

When the computer appears above protocol failure phenomenon, should follow the following steps to locate the fault:

(1) Check the computer whether to install TCP / IP and NetBEUI protocol, if not, it is recommended to install these two protocols, and TCP / IP parameters configured, and then restart the computer.

(2) Use the ping command to test the connection with other computers;

(3) In the 'Control Panel' 'Network' attribute, click the 'File and Print Sharing' button, in the pop-up 'File and Print Sharing' dialog box to check to see if the 'Allow other users to visit my File 'and' allow other computers to use my printer 'check box, or one of them. If not, select all or select one. Otherwise it will not be able to use shared folders;

(4) After the system restarts, double-click 'Network Neighborhood', will display the network of other computers and shared resources. If you still cannot see other computers, you can use the 'find' command, can find other computers, all OK;

1. Fault performance and analysis

Configuration failure more time is the performance of the network cannot provide a variety of services, such as cannot access a computer and so on. Therefore, before modifying the configuration, you must make the original configuration of the record, and the best backup. Configuration faults are usually expressed as follows:

(1) computer can only communicate with some computers rather than all computers;

(2) The computer cannot access any other device.

2. Configure the troubleshooting steps:

First check the configuration of the failed computer. If found to be wrong, modify, and then test the corresponding network services can be achieved. If no error is found, or if the corresponding network service cannot be implemented, perform the following steps.

Test the system of other computers have a similar failure, if the same failure, that the problem lies in the network equipment, such as Hub. Instead, check that the computer being accessed is carefully checked for the services provided by the computer.

We first look from the appearance of the network card:

1. RJ45 connector problems RJ45 connector prone to failure, for example, the twisted pair of head did not top to the top of the RJ45 connector, stranded in accordance with the standard pin into the connector, or even the connector does not match the internal or broken twisted wire. The effect of the thickness of the gold-plated layer on the quality of the joint is also considerable, such as plating too thin, then the cable after three or five times after plugging, perhaps it worn away, and then was oxidized, of course, prone to disconnection.

2. Wiring failure or poor contact generally can be observed in the following places: twisted pair color and RJ-45 connector pin is consistent; thread head to the top of the RJ-45 connector, if not, the line will be poor contact To re - press again; observe the RJ - 45 side. Is the metal sheet pierced into the strand? If not, it is likely to cause the line unreasonable; observe the twisted pair of skin to remove the place, whether to use the stripping tool cut off the twisted pair (stranded copper wire has been broken, but the skin is not broken). If you cannot find the problem, then we can use the replacement method to exclude network cable and hub failure, that is, with the normal communication network cable to connect the fault machine, such as normal communication, is clearly a network cable or hub failure, and then convert the hub port to distinguish in the end Is the network cable or hub failure, many times the hub of the indicator can also indicate whether the hub is faulty, the normal corresponding port lights should be lit.

Finally, we use the ping command to check whether the network card can work properly.

1. Ping 127.0.0.1 127.0.0.1 is the local loop address. If the address cannot ping, it indicates that the local TCP / IP protocol does not work. If the ping address is correct, the TCP / IP protocol is normal. Go to the next step to continue the diagnosis.

2. Ping the IP address of the machine Use the ipconfig command to view the IP address of the machine and ping the IP address. If the ping succeeds, it indicates that the network adapter (network card or modem) is working normally. You need to go to the next step to check. The adapter is faulty.

3. The IP address of the local gateway local gateway is a known IP address. Ping the IP address of the local gateway. The ping indicates that the network line is faulty. If the network also contains a router, you can also ping the router in the network segment of the IP address of the port, then this section of the line is a problem, then the router in the same computer as the port of the same port IP address. If the pass, and finally the IP address of the destination machine. The

4. If you want to detect a network with a DNS service (such as the Internet), the last step of pinging the target computer's IP address. Still cannot connect to the machine, you can ping the machine's network name, such as: ping www.sohu.com.cn, under normal circumstances will appear the URL to the IP address, which indicates that the machine's DNS settings are correct and DNS The server is working properly, and vice versa may be one of the failures.

After the implementation of these steps, the network where the fault has been clear, we can correctly solve the problem.

4. Conclusion

Network failure is unavoidable. After the network is completed and run, network fault diagnosis is an important technical work of network management. Do a good job of network operation management and fault diagnosis work, improve the level of fault diagnosis need to pay attention to the following aspects: earnestly study the theory of network technology; clear network structure design, including network topology, equipment connection, system parameter settings and software use. Understand the normal operation of the network, pay attention to the normal operation of the network to collect a variety of status and report output parameters; familiar with the commonly used diagnostic tools, accurate description of the fault phenomenon.

References

1. Zhou Yantao. Computer Network Practical Course (2nd Edition). Publishing House: Electronic Industry Press
2. Li Bo. Network Security and Certification. Press: Chongqing University Press