

5 common network problems with Windows workstations

This article will show the five most common errors with Windows network and workstation systems, and provide some tips to help overcome or minimize the impact of these problems.

Network administration - A network is a system consisting of one or more workstations connected to a server to share resources.

Common resources include printers, storage devices, and folders containing data that many users need to use. The network is used to create centralized access (secure access) to shared resources. Currently the entire network is using the largest shared resource, the World Wide Web.

This article will show the five most common errors with Windows network and workstation systems, and provide some information to help you overcome or mitigate the impact of these problems.

5. Initial configuration error

The first problem makes the network unstable because of an error when configuring the network, configuring the system and configuring the resource usage. A network system usually has too many components while the scale and number of users can increase making it more complex and thus the problem is always permanent. With the development of telecommunications in the past 10 years, and the development of the hardware and software market, many users have installed the system and the network themselves, even without a certain knowledge of the network.

If we want to install and configure Windows or a Linksys router, we need some understanding of this work. For example, if you want to connect your computer to the Internet, then at least we need to know something about the TCP / IP address scheme, DHCP protocol, cable, .

When installing the system, the main problems that caused it were power failure, incorrect cable setup (or Wifi configuration), missing or misconfigured protocols (such as IP) and problems with Windows systems. (as network services are misconfigured). Another problem to consider is to configure the workstation method to access shared resources, such as network printers. If a server is used to provide centralized access, then we need to configure properties on the print server, or if the print server is located and controlled on a server We need to configure the workgroup or the relationship between the client and the server. The relationship between the workstation and the server is one of the major obstacles for people working with network-connected Windows workstations. After completing the configuration and testing the network, we need to store configuration information so that when problems arise we can quickly detect the cause of the error.

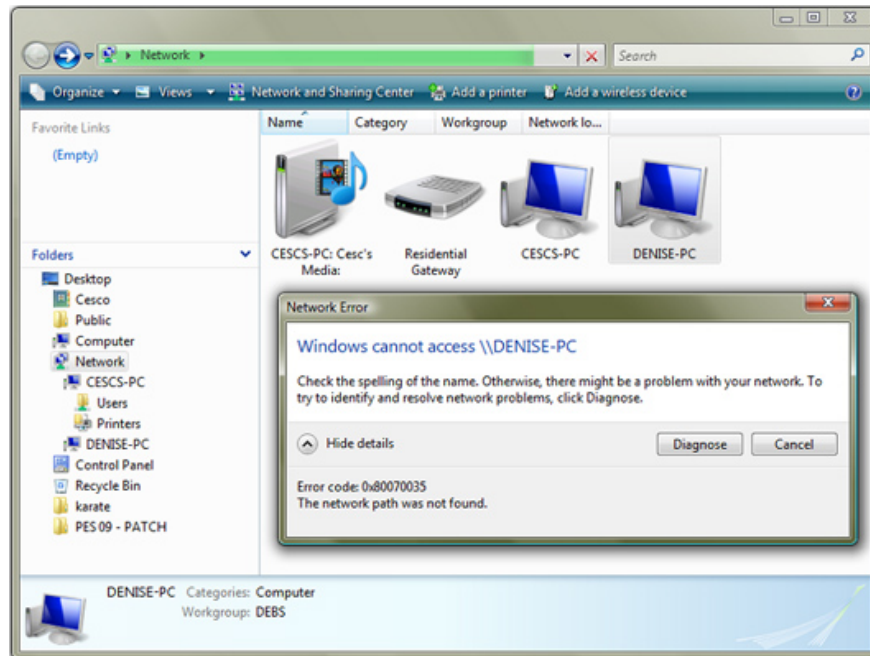


Figure 1: Error accessing other computers on the network.

If you want to use Wifi connections through cable connections, the initial design and configuration is very important. OSI Model is very useful when troubleshooting these problems. First, cable connection is often accompanied by a physical error, such as a broken cable, affected by distance or power problem, incorrect connection (wrong type or point), or simply a cable Fully connected. Signal interference is a common problem, especially when the cable is pulled over a power source or light source (with fiber optic cable). Wifi connections are often more complicated because they need the support of software and hardware (such as drivers or application software).

4. Issues of rights, licenses and licenses

If we have configured everything correctly and all the workstations are connected without any problem, is there any mistake? The answer is yes. The first problem must be mentioned with Windows workstations is permissions, licenses and licenses. This is when we cannot access the server, or we cannot access resources even though we are logged into the server.

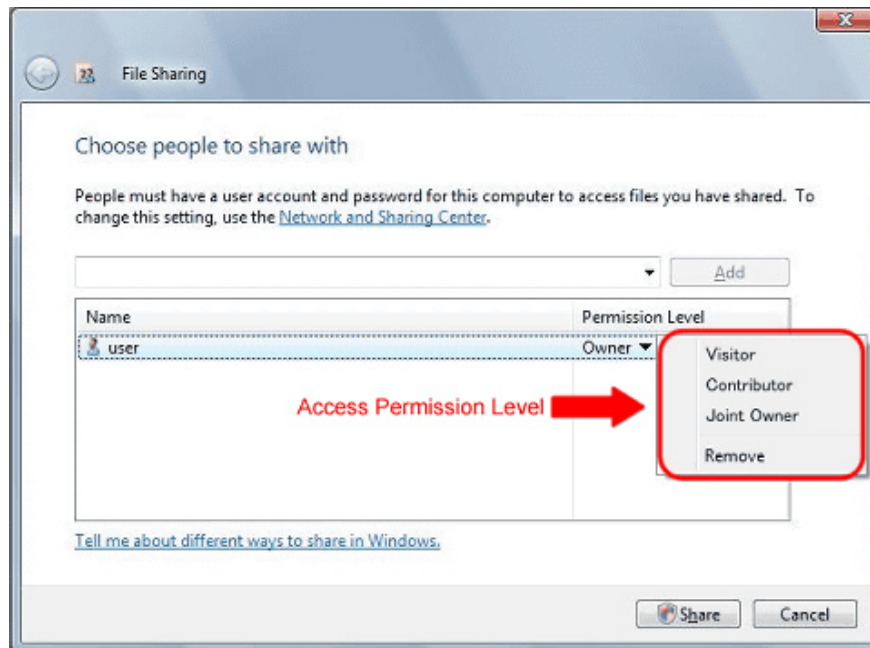


Figure 2: Shared file access licensing levels.

When encountering this problem, we need to change some configuration. There are some things that we need to pay attention to. First, the Windows system forces us to change passwords periodically. In other words, after an unused period, some accounts become obsolete or forget their password. If this happens we can fix it ourselves instead of asking the admin. We only need to access the account and log in the information in Windows to reconfigure the necessary items. In addition, we may be using a working group without centralized source access control and having to log into multiple systems just to use one resource. Workgroups cause a lot of problems for this reason, so we should not use a workgroup with a network of 10 or more computers.

If you can log in and check, we can use Windows Event Viewer to detect errors in the network. Failure to access resources over the network is a common mistake and can be easily overcome by a more appropriate structure, or a plan to restore forgotten login information.

3. Network performance

Perhaps this is the most common incident. With Windows operating systems, there are many good weaknesses that affect performance. For example, if we configure a computer without taking into account the applications that will be operated over the network. The most common applications often require a relationship between the client and the server, which means that the workstation installed on the Windows desktop must communicate and transfer data over the network to operate. If the network performance is affected, it is because the network is too slow, or the application has not been deployed to the network. Fixing this kind of problem is quite complicated, usually we have to analyze it carefully and need to use a tool like package analyzer.

The problem of speed and latency may be due to slow connections, or because a network loads too much data. For example, if using a gigabit Ethernet card for servers, cable connections will speed up to 1000 Mbps. Some users are unaware that switching to Wi-Fi will have a significant impact on network communication because many home Wi-Fi systems will not have transmission speeds greater than 100 Mbps.

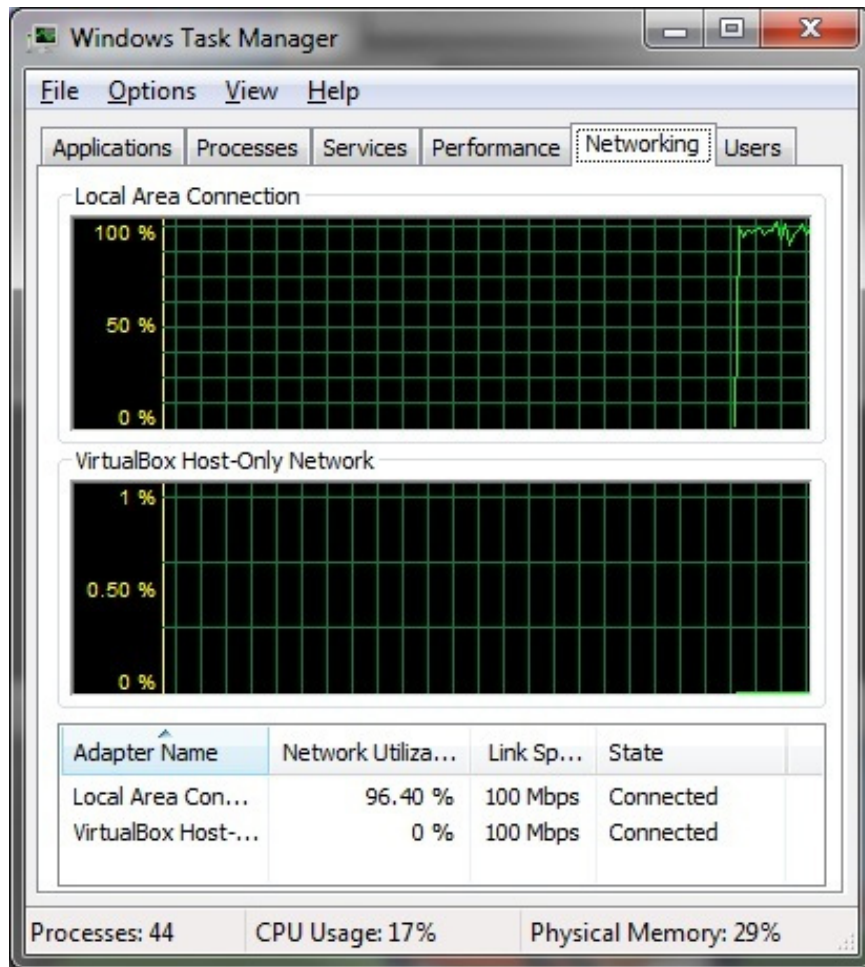


Figure 3: Diagram showing network performance.

Also, using an access server instead of a network switch can cause big problems with speed and latency. The use of non-hierarchical structures in which the main component of the network operates at the highest speed and the access layers in this main component operating at a slower rate may create bottlenecks. Two-way settings and unmatched speeds on NIC cards are also common causes of network performance problems. And using a converter to create a loop may cause the network to crash completely.

Windows home users always face Internet problems. If you have checked hardware and software that we cannot fix these problems, it may not really be a problem. Sometimes, problems arise from the provider's service. In those cases, we need to contact the supplier to find a solution.

Other issues affecting network performance are security issues that prevent access to resources, or make services inoperable.

The Internet browser application may also cause problems especially when infected with a virus or the settings in this application have blocked the page being accessed. For example, in Internet Explorer 8, if we use all security settings, such as a Phishing Filter, the time it takes to determine the page will increase and as a result slow down the session. counter. There is also a reason when people blame the network when something goes wrong, because that's always the obvious. However, in reality, the network is just one of the many causes of the

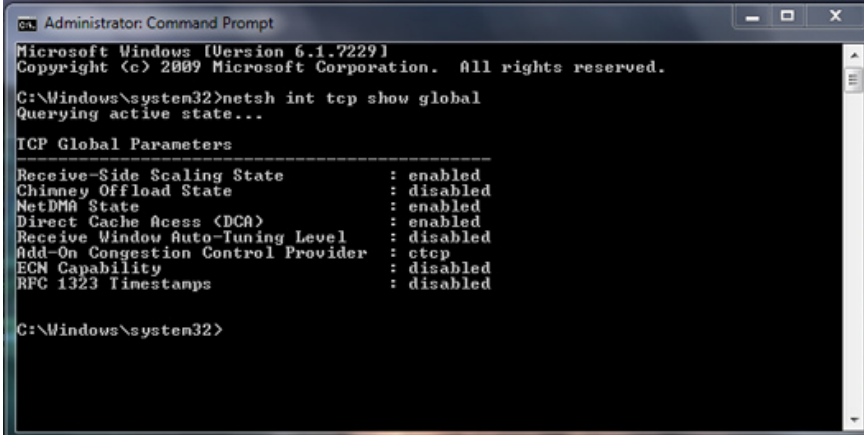
problem, in which system resources, through communication, . can cause the network to be slow. As we operate many applications and services through a link that cannot be processed, the system will freeze if those applications respond poorly.

2. Problems with TCP / IP and other protocol issues

There are many reasons why the protocol becomes a problem in the network, these issues include: ISP protocol issues, DHCP, APIPA, DNS, IP address and use of a protocol other than TCP / IP in the network. We can solve TCP / IP related problems by:

Using a updated network topology, although the network has only a few computer systems. Using graphics is useful when troubleshooting network problems, or you can easily add a new server to the network without causing problems. Even if we use DHCP, we need to consider using IP tools like tracert, netstat, ping and pathping, and there are many other tools that we can use when troubleshooting other problems.

If you have not configured a network protocol, you cannot communicate over the network. There are many protocols in TCP / IP, such as DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name System) which are the culprits that often cause connectivity problems, as well as network performance problems. For example, if the workstation cannot connect to the server that provides it for the IP address, the workstation will be disconnected from the network. If this problem occurs, APIPA (Automatic Private IP Addressing) will give this workstation a different IP address (possibly not routing or not routing in the network) which will cause many troubles. Workstations always try to connect. If a physical connection (such as a cable and a power source) is disconnected, or the system cannot be logged on or the network is available, or the protocol is incorrectly configured, we will not be able to connect or connect limit.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7229]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh int tcp show global
Querying active state...

TCP Global Parameters
-----
Receive-Side Scaling State      : enabled
Chimney Offload State          : disabled
NetDMA State                   : enabled
Direct Cache Access (DCA)     : disabled
Receive Window Auto-Tuning Level : disabled
Add-On Congestion Control Provider : ctcp
ECN Capability                 : disabled
RFC 1323 Timestamps           : disabled

C:\Windows\system32>
```

Figure 4: Parameter list of TCP.

DHCP can cause some performance problems if the clients cannot determine the server to get the IP address. What DHCP must handle is a DNS server address for disconnected workstations, and these workstations will have to search the server list to find a suitable server. This process raises some network performance issues. It is

difficult for us to find out the cause of DNS failure if we do not understand its working method on the system. Suppose we want to access quantrimang.com.vn page, the workstation will need a IP address to communicate with ISP. In addition, it needs to know which DNS server contains information about quantrimang.com.vn website. If these servers do not allow access, or there is a problem with this page, then we can implement the following two methods to overcome this problem. First, configure another DNS server to troubleshoot problems for ISPs. For example, we can open the Command Prompt and then use the nslookup command to find the current DNS settings. If you are connected to the Internet, the ISP will send this information from a DHCP server. If the ISP then changes the DNS server, the client will not be able to respond to that information until the connection session ends, or we make a new connection. In addition, we can use the nslookup command to change the primary DNS to use and test another DNS to see if the DNS server has a problem.

Dynamic DNS is also the cause of network problems if we configure it incorrectly.

1. Common security incidents

The most common network problem with Windows clients is due to the poor services and features of security applications. In fact, all infections come from inside the network, or through Wifi connections when not using security tools to control, monitor and block Wifi. However, this does not mean that the PC or router cannot be secure. Currently, most hardware and software are integrated with some security support. Routers today function as a firewall, IDS (intrusion detection systems), and provide many detailed records of data transmitted through it. Intrusion is a common form of attack. That's when someone connects to your Wifi network and access resources in it.

Security for Wifi networks is not simple. Some of the previous tools like WEP keys are very easy to overcome. In addition, another popular method is to use the workstation's MAC addresses in the access point list to allow only some users. However, if there is no additional security measure for the system, there is no guarantee that this method is completely secure.

Whether we choose to use Windows Firewall or some third-party software, we should consider using a tool as a basic method to protect the server. Network intrusion detection tools can help secure data and prevent what signs of tampering.

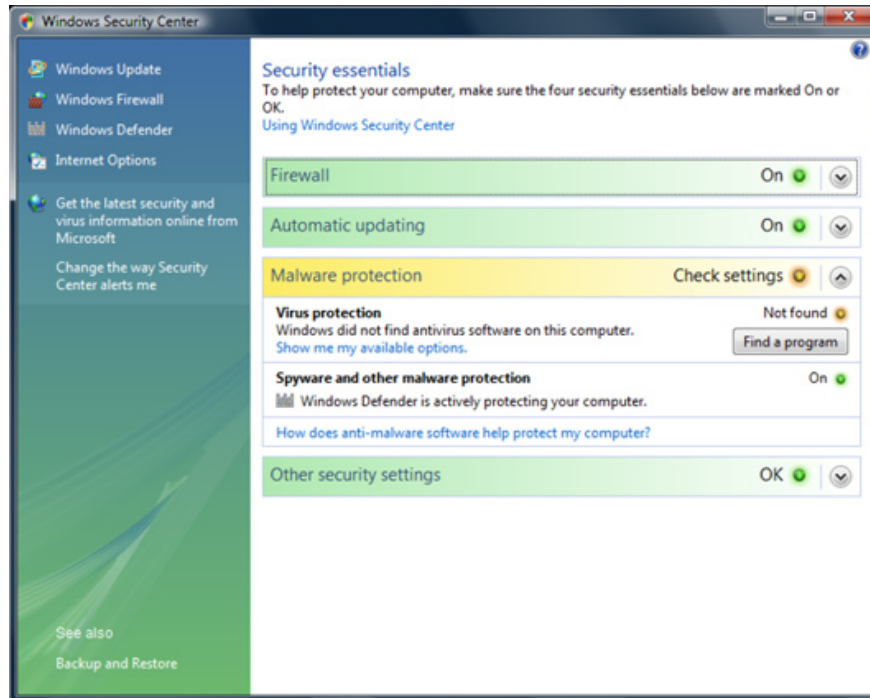


Figure 5: Use Windows firewall system to secure the network.

If the router being used has a firewall capability, we can use it to create log files that can monitor what is happening on the network. Firewall systems such as Windows Firewall can also perform this function on the server.

Antivirus software (as well as Network Access Protection or NAP) can be used to reduce performance and connectivity issues. Currently most types of viruses and worms often attack networks and servers.

Care should be taken to check and monitor security tools when implemented. If you do not often do this, it is best to use a number of different tools (Defense in Depth - use multiple security tools simultaneously), then check the logs when a problem occurs.

Conclude

The above are the 5 most common network problems with Windows clients. The purpose of the article is to provide some information about the causes and remedies. As we can see, working on the network always has many problems and risks, from slow connections to becoming victims of an attack. Perhaps it is impossible to avoid incidents with the network, but if we recognize the cause of these incidents, we can minimize their impact.

You finished reading the article "**5 common network problems with Windows workstations**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.