



12 Things To Know When Troubleshooting Your Network

Dheeraj (Raj) Tolani, Global Knowledge Instructor

Introduction

You work for a small organization where you wear many hats. You are the network admin for PCs and your routers and switches. Anything that's broken is YOUR problem and only your fault. So, you walk into your office one morning, and you hear the phone ringing. You have an irate user on the other end telling you that the "network is down." I always love those calls where a user, who has no networking background, tells you that the network is down without any analysis tools or technical background. After years of working in networking, you probably know that if the network were really down, then the whole department would probably be calling you and not just this one same user every morning.

This white paper approaches this situation with some of the common troubleshooting things that, you as a network administrator, know or maybe should know.

Mental Preparation

The first and foremost concept for troubleshooting is not to panic. It might sound like the simplest thing, but that is the reason why some new administrators make mistakes. Then, they dig themselves deeper because they panic. A calm mind can identify the problem and approach the problem with a systematic method. Sometimes, if you have been working with the problem for a long time, it will not hurt to just walk away from the problem and look at it after taking a break. You'll see that there are some very obvious things you missed. I also like the buddy system. You might want to have someone else look at the problem rather than you seeing or not seeing the same issue - which was probably staring right at you.

Now, we know that in real life you can't just walk away from a problem; your management might not appreciate that. You might be losing many millions of dollars while the network is down. I can tell you that in certain medical environments, you want to fix the problem fast since someone's life might depend on that piece of equipment that you are trying to fix.

Systematic Approach

So, let's visit our caller from the beginning of the paper. We are going with an assumption that this user is running the most common operating system available out there – some Windows platform. Common mistakes that new administrators make are that they believe the user and assume that the network is really down. I would strongly recommend against that. I am not asking you to argue with the user. I would like to check out the problem on my own.

Physical Layer Verification

One of the first things you should do it to check the cable. Do you have a green light at the back of your machine? You will find many times that the problem might just be a cabling problem. I have seen, in some rare cases, that inexperienced users just didn't have the monitor plugged in so it was just a loose cable. Although, in my example, it could be the monitor cable, it could also be a network cable that is unplugged.

Network Layer Verification

If I see that the cable is plugged in, then I would ensure that there is an IP address assigned on the system. Now, with Windows systems, you can go to the command prompt and checking the IP address using the "ipconfig" command. You want to make sure that you see that the IP address/subnet mask that are assigned are correct for that segment. Keep in mind that the command to verify your IP address and subnet mask will vary, depending on the system you are working on. For Windows systems, it's ipconfig or ipconfig /all for more detailed information. For Cisco routers, the command show interface will show you the IP address and subnet mask. So, please, consult your documentation for the systems you are working on.



Interviewing the User

I have had many instances where, after all the work you do, you find out that someone had just moved this machine to this location from a different office, or floor, or segment, and it still has the IP address/subnet mask from a different part of the network. Maybe this system has both wired and wireless cards, but the IP address was incorrectly configured on the wireless card rather than on the wired connection. Maybe it would've been wise to ask the user if something changed in the environment related to machines being moved.

Reviewing the Logs: If You Have Them

I hope that your company has a central change log procedure where all things are documented, and you can refer to the logs before you even approach the user. Besides the company change logs, I hope you are also using a central syslog facility that is collecting alerts from various systems in your organization. You can find many free syslog products on the internet for download.

Knowing Your Company Policy

It is also wise to ask the user the last time they were able to successfully connect to the network from this machine. I had a user once who kept insisting that the company internet was down so he couldn't do web browsing related to his job. After further investigation, we found out that the websites this particular user was trying to visit were banned by the company and therefore prohibited. It is a very good idea to know your own company's security and ethical policies. I would recommend having the disclaimers in writing approved by your senior management.

Isolating the Problem Using Tools

It also makes sense to do a basic ping command to try to get a response to/from different systems on or off your network. If you can reach the local systems but not the remote systems, then there is a possibility that your default gateway is down, or missing, or configured incorrectly. It is also possible that your default gateway (router) doesn't know how to route the packets to that particular destination, or maybe it's possible that your company doesn't allow ICMP protocol, which is what ping uses. Again, it makes perfect sense to know your company policies.

Sometimes, you can ping the remote systems with their IP address but not with their names. This implies that there is no name resolution method available to resolve from the name to the IP address. It could also be that the name resolution method is resolving it to the wrong IP address.

In Windows systems, you can also check to see if your TCP/IP stack is loaded correctly. You can ping the localhost address (127.0.0.1), which can be done at the command prompt. DNS does the translation from the name to IP address. You can see what your DNS is configured for using the ipconfig/all command at the command prompt.

You can also use the traceroute command (tracert on Windows Systems) to see if you can see where the packets are failing. You can see a hop by hop packet flow using the tracert command. Tracert command output is explained in various Microsoft and Cisco courses offered at Global Knowledge.

Here is a sample partial output of tracert command.

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.
All rights reserved.

C:\Users\dt>tracert 10.0.0.1

Tracing route to test [10.0.0.1]
over a maximum of 30 hops:

  0  <1 ms <1 ms <1 ms . [192.168.2.1]
  1  6 ms 7 ms 5 ms 10.58.160.1
  2  6 ms 7 ms 7 ms gig-2-0-nycmnyu-rtr2.nyc.rr.com
    [24.29.98.189]
.....<output omitted>.....
```

Have an Up-To-Date Network Diagram (Not an Outdated One)

Let's say you did all those things, and you see that all those things are configured correctly or not prohibited by your company policy. What should you do next? It's always good to have a network topology map to consult to see where this particular system is supposed to be plugged in. If there is nothing wrong on the PC, then the next logical approach will be to go to the switch where the user is plugged in. In this white paper, we will only use Cisco Systems routers and switches in our examples.

Checking the Switch

Now that we are on the switch where the user is plugged in, and you have found the port number where the user is plugged in, let's see how that particular port is configured. You can use the show run int gi 0/2 command to see what is currently running for that particular interface (in this example gigabit 0/2 port)

Here is a partial output from the **show run int** command.

```
Switch#show running-config int gi0/2
Building configuration...

Current configuration : 85 bytes
!
interface Gigabit0/2
 no ip address
 switchport
 switchport mode access
...<output omitted>
Switch#
```

Another thing to check on the port would be to see if the port is in the right VLAN. VLAN is a logical grouping of ports.

VLAN assignment can be checked on Cisco switches using the **Show vlan** output.

Here is a partial output from one of the switches showing the ports that are assigned to the two VLANs (namely VLAN1 and VLAN2). Gigabit 0/2 – Gigabit 0/5 are assigned to VLAN1 and Gigabit 0/6 – Gigabit 0/12 are assigned to VLAN2).

```
Switch# show vlan
VLAN          Name             Status          Ports
-----
1             default          active          Gi0/2, Gi0/3, Gi0/4, Gi0/5
2             VLAN0002         active          Gi0/6, Gi0/7, Gi0/8, Gi0/9
                Gi0/10, Gi0/11, Gi0/12
..... <output omitted>.....
```

All ports in the same VLAN form a logical grouping called a broadcast domain. Broadcasts stay within these ports. In our output example, Gi0/2 – Gi0/5 form one broadcast domain, and ports Gi0/6 – Gi0/12 forms the other broadcast domain. All systems plugged in the same VLAN should have same subnet IP address. (It's very important to have a very solid understanding of how subnetting works. This is also a typical problem in most environments.

Now that you have verified that the VLAN assignment is correct on the switch, you might want to ensure that there are no other restrictions on the switch port, such as port-security restricting that port to be used for only certain MAC addresses. Typically, in organizations, it is common to see that companies implement MAC address-based security and then move machines around. Perhaps the port is still only allowing the old machine and not this new system. Remember, this could be a new machine assigned to the same user, or it could be that particular cubicle was used by someone else and now this is the new user. Remember, both of these things could've been answered with a good conversation with the user or maybe looking at the log file we discussed in the beginning.

If the user is trying to talk to systems that are outside of its broadcast domain, then there has to be a device that will take you outside this grouping of ports (VLANs). How do we go out of our room? Well, that's simple, we just use the door. So, what is the equivalent of the door in the networking world? Your router is the door that takes you outside of your local network segment.

Checking the Router

Let's visit the router. Is your router up? Do you see the lights? Again, the same basic question is whether it is powered up. The port on the router that you are using as your default gateway for the PC should be plugged into the same VLAN.

Let's say we verified that the router is plugged in, and you are now connected to the router. Does the router have a path to the destination where this particular person is trying to go? Does the router know how to route to that destination? You can always use the show ip route command to see if the routes exist to the destination. However, in bigger environments, this might be very cumbersome since you might have hundreds or even thousands of routes.

Here is a sample output of **show ip route**, looking only for 10.0.0.1 destination. As you can see, you have a route to that destination. In advanced routing classes, you learn what the other fun parameters mean. The Global Knowledge BSCI class covers this in great detail.

```
Router# show ip route 10.0.0.1
Routing entry for 10.0.0.1/32
  Known via "isis", distance 115, metric 20, type level-1
  Redistributing via isis
  Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
  Routing Descriptor Blocks:
  * 10.22.22.2, from 10.191.255.247, via Serial12/3
    Route metric is 20, traffic share count is 1
.....<output omitted>.....
```

Now that you know that you have a route to that destination, you can try pinging the destination. Remember, just because you have a path to some destination, that doesn't mean that the remote site has connectivity with you. How do you know that there is a return path available? If both of these sites are in your offices, then you can ping from the remote site. Also remember, it could be that your company doesn't allow ping (or entire ICMP protocol). Have you considered using something other than ping? You might try to do a telnet or even FTP to the remote site? If the remote site is running the Telnet or the FTP daemon, then you will succeed. If they are not running that, then maybe you need to find some other test application.

Most people think that since they couldn't get in the remote site using Telnet or FTP, it means a failure. As long as you even get a prompt for a password, that is a success. You don't have to be connected. Getting the dialog box for password is a success.

Document, Document, Document

I hope you had success in one of these steps, and you have isolated the problem. One of the most important things in troubleshooting is to document your findings. Now, the best approach would be to have a company knowledge base or maybe a database of all issues and your resolutions so in future, if you have the same problem, you can just look at this knowledge base and can troubleshoot the problem easier and faster without getting stressed.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

Understanding Networking Fundamentals

TCP/IP Networking

CCNA Boot Camp v2.0

ICND1 - Interconnecting Cisco Network Devices 1

ICND2 - Interconnecting Cisco Network Devices 2

TCN - Troubleshooting Cisco Networks v1.0

For more information or to register, visit www.globalknowledge.co.uk or call **01189 123456** to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Dheeraj (Raj) Tolani has been working with Global Knowledge as a contract instructor teaching various networking courses including CCNA, CCDA, CCNP, CCDP, CCIP, CCVP tracks. He has been in the industry for over 17 years working with various technologies and multiple vendors including Cisco, Banyan Vines, Microsoft, Comptia, and Novell. Dheeraj has worked as a consultant for various medical, financial, legal, government, and publishing companies. He runs a consulting company based out of New York City, which provides IP integration solutions. You can visit his web site at www.rajtolani.com.