
Troubleshooting A Switched Network

Switches are intelligent devices which run software and can exhibit quirks. We delve into a few of the common problems you might experience on your switched network, and explain how to solve them.

**By Neil Briscoe
Network Consultant**

Over the last five years or so, switches have been replacing simple hubs in the server room. The reasons for this are several. Hubs are passive devices; their only benefit is that they take standard RJ45 connections, thereby saving you from running the older Thick or Thin Ethernet. However, they still act just as Ethernet segments always have, and they will do nothing to protect you from collisions on the segment they provide, should they occur.

Switches, on the other hand, are intelligent devices, and they are manageable. These days, switches also provide VLANs so that you can segment off different logical networks, but use a single switch for all devices. In a larger network, where you may have multiple switches, it's possible for all VLANs to be available on all switches, so that you can arrange your virtual networks precisely how you like.

In general, switching technology works well, but it is not without its pitfalls. Switches, being manageable, run software, and that means that every so often a bug can occur which can cause seemingly strange errors on your network. Often, as with all computer devices, a reboot will fix the problem - until the next time it recurs. However, sometimes the simple reboot approach will not work, and then you have to delve into other possibilities.

Spanning Tree

Just before we enter the world of troubleshooting switches, a word on Spanning Tree. The Spanning Tree Protocol was first created to assist bridged networks. In a complicated bridged network, it might be that connections between segments have been made in such a way that one segment may have multiple paths over which to transmit its data to another segment. This wouldn't be such a problem, were it not for broadcast packets. As you recall, when a broadcast packet is transmitted, and every device on a subnet will "hear" it. They may, or may not, choose to respond. Should an ECHO REQUEST be sent to the broadcast address, then all nodes will respond.

A bridged network with multiple data paths between segments that responds to such a broadcast request may cause the network to suffer a broadcast storm, as the original broadcast packet makes its way over multiple links, such that some devices respond to the single broadcast multiple times. The Spanning Tree Protocol ensures that there is precisely one path used between any two segments, even if there are multiple choices. Generally, a network administrator specifies relevant cost metrics on various paths so that, providing all links are up, the most effective (quickest) path will be used.

Bridges With More Ports

Why all this talk about bridges in an article about switched networks? It's essentially because switches are bridges with more ports. A bridge generally only has two ports - either two LAN ports, or a LAN port and a WAN port. Switches have multiple ports. It's not uncommon to find them with 12, 24, 48 or even more ports. The similarity is that both learn which devices are connected to which ports by seeing which port a particular MAC address transmits on. They both also run the Spanning Tree Protocol by default. Bridges generally don't grant you the option of disabling Spanning Tree; switches generally do, although there are some which don't.

Switches and bridges will, once they've learned which port a device is connected to, only transmit a packet down a port if the Ethernet address on the packet is for a device that exists on that port, or if the packet is a broadcast or multicast packet.

Common Problems

With some basic definitions out of the way, we can now start discussing common problems and their solutions.

Moving A Device

Our first problem involves the inability of a device to communicate with any other device if it is suddenly plugged into a different port on the switch, or even a port on a different switch on a multi-switched network. The reason for this one is simple. As described above, switches learn where a device is by seeing which port its packets appear from. If you move a device's network connection from one port to another on the same switch, it will take a short while (normally five minutes) before it forgets the original port the MAC address was on and starts listening for that device again.

Since switches are managed devices, the fix is generally simple. If you've had to physically move a device, connect to the switch and erase its ARP (Address Resolution Protocol) entry for the device in question. Having done this, the switch is forced to use the ARP protocol to learn the device's new location. This fix works even in a multiple switch environment: the switch the device is actually connected to will see it as connected to that physical port, whilst any other switch in the network will see it on the port that connects it to the switch. The only difference is that you may have to clear the ARP entry for the device on multiple switches. If, however, you are running a switched network between multiple sites, by the time you have physically relocated a server from one site to the other, the switches will normally have cleared their ARP cache of the entry and you'll have to do nothing.

Disabling Spanning Tree

As stated earlier, whilst all switches run the Spanning Tree Protocol by default, most permit you to disable it if you don't require it. (You don't require it if you ensure you have only one data path between any two switches on your network or, indeed, if you have only one switch.) However, there are some devices, for instance the Cisco Catalyst 2900 series, which don't allow you to disable Spanning Tree. You may feel that, if you only have a single switch on your network, this won't be a problem.

However, if you have an NT network, it will be. By the time the Spanning Tree algorithms have run (on a 2924 they run on all VLANS and on all ports), clients which successfully connected to their Domain Controller when you first plugged them in will suddenly claim that there is no Domain Controller available, and start logging in using cached information. This is fine for a short while, but allow it to continue and your domain will become very sick.

Fortunately there is a command in the 2924 that allows you to fix this. It is, however, a port-level command, which means you need to set it for each physical port on the switch. At the `enable` prompt type the commands shown in Figure 1. Considering you have to type the sequence 24 times, learn the short form methods on a Cisco. The command

```
span portf
```

suffices to type the spanning tree command itself, and normally

```
int Fast x/y
```

will suffice to select the relevant port. This setup will ensure that your NT clients can always see their Controller. If you don't set this, you can reboot your switch as many times as you like; the problem may go away briefly, but it will come back to haunt you before you manage to leave the site.

New Devices

Now consider the case where you have a switch which is providing a perfectly good service to an entire network of office users, and now you connect two new devices to it and they simply refuse to see anything. They refuse to see any other

“Switches are bridges with more ports. A bridge generally only has two ports - either two LAN ports, or a LAN port and a WAN port. Switches have multiple ports.”

device on the same segment, and they won't talk to each other. Naturally, since switches work on MAC addresses, check to see if the devices are getting entries in their ARP cache. On both Unix and NT the command to run is

```
arp -a
```

and see what is revealed. The commands on particular switches vary between manufacturers' devices, but they generally all have a means to allow you to examine their ARP cache. If you find the computers claim their ARP entries are incomplete, you can be certain there is a problem. This will normally mean that a switch won't tell you which port a device is connected to, either. If you are fortunate enough to have a multi-switch environment with EtherChannel trunking between them, then try to plug your devices into another switch. Ensure, if necessary, that you configure the ports to be on the same VLAN as they would have been on the original switch.

If they can now be seen then you probably need to reboot the original switch, since, if it can pick up the MAC addresses on the port by which it is connected to the second switch but not on its own physical ports, there is some sort of problem. Having done this, you eventually need to reconnect the device back to the original switch, and either await ARP timeout, or clear ARP entries, to determine whether the problem was a software bug on the switch or a physical problem with the switch port.

Ports Marked As Down

Consider the case where a switch suddenly marks a port as down, of its own accord. This will normally only occur on Trunk ports. Trunk ports are those used to connect one switch to another so that multiple VLAN traffic can be transited between switches. It isn't the multiple VLAN-ness of the port that is generally the cause of the problem - the problem is more likely to be the Spanning Tree Protocol.

Consider a network which contains three switches, A, B and C. A is connected to B and C. B is also connected to C. Clearly, therefore, you have an unholy triangle, since packets could run from any switch to any other switch by one of two separate paths. However, Spanning Tree, which runs by default, will generally have ensured that only one path is used between any two switches. Part of the Spanning Tree Protocol causes "Hello" packets to be transmitted from a port at regular intervals. A switch is likely to take a port out of service if a port sees its own "Hello" packet return. If such a case occurs, you have a topology in use that is not being properly controlled by the Spanning Tree Protocol. Either you need to modify the metrics on various switches, or you need to physically modify the topology of your network.

Alteon Issues

Being Layer 4 switches, Alteons are capable of doing Layer 3 routing, and they add an additional level of hassle into the troubleshooting process. If you don't want your Alteons to route packets, possibly very important if you're trying to hide two separate VLANS behind firewalls in two separate sites, ensure you turn forwarding off; either at the port level, or at the global level if you don't need your switch to route anything at all.

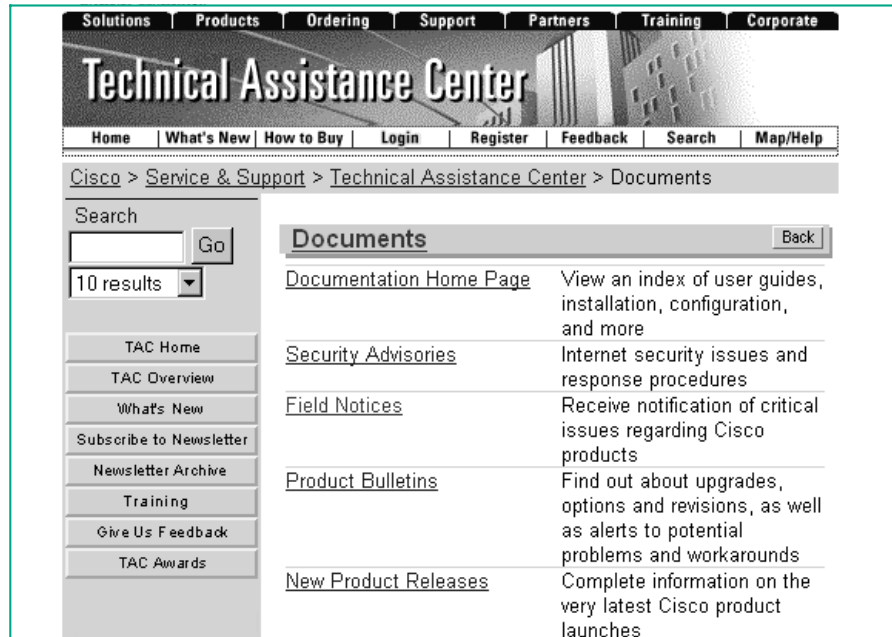
Traffic Monitoring

One of the biggest problems on switched networks is that it is difficult to do network traffic monitoring. On any individual port, a device will only see traffic destined for itself (or any other device on its segment), and broadcast or multicast traffic. If you, as a troubleshooter, need to run a promiscuous packet listener, it isn't, by default, going to see very much of the picture.

```
conf t interface FastEthernet 0/1 spanning-tree portfast
exit interface FastEthernet 0/2 spanning-tree portfast
exit ... interface FastEthernet 0/24 spanning-tree port-
fast exit exit copy run start
```

Figure 1 - Port-level command sequence to ensure NT clients can always see their Controller.

“Most switches have the means of enabling one of their ports as a network monitoring port. It is normally configured to be inactive by default, since it puts a heavy load on the switch.”



Fortunately most switches have the means of enabling one of their ports as a network monitoring port. It is normally configured to be inactive by default, since it puts a heavy load on the switch. However, to properly monitor the LAN you may need to enable it. Then, connect your promiscuous listener to the port you have configured as the network monitor and watch the packets fly by.

This, of course, is the solution to a large number of network problems which might occur, and you can learn much. You can also drown in the deluge of information, so ensure you know how to drive your listener properly, and apply the correct filters, so that you only get information that is relevant to the problem at hand.

Multiple Problems

As you start your switched network, it won't appear much more than a hubbed network, and you'll wonder what the fuss is all about. If you stay that way, with a single switch and a single VLAN, or even multiple switches and a single VLAN, you won't generally have many problems. Start to add multiple VLANS, Ether-Channel Trunks and multiple switches and your problems, when they occur, will then become much more difficult to resolve.

The rules, however, are simple. You need to understand the physical and the logical topologies present on the network. They may be the same, or they may be different. You need to have a good understanding of IP - particularly IP subnetting - so that you can readily identify devices that should be able to talk to each other directly, and those that ought to be communicating via a router. Finally, if all else fails, remember a switch is a computer with a specific task - a reboot may be all you need.

Finding Solutions

Stuck for a solution? Then don't forget the Web. The problem I related above regarding the Cisco 2924 I resolved by using the Web. Cisco has a wealth of information on its Web site (www.cisco.com); use the search engine provided. It took me about five minutes to find the white paper which explained why I needed to use Spanning Tree portfast. Most other switch vendors have Web sites, with associated support documentation. For HP Procurve switches take a look at www.hp.com/go/procurve. For Alteon switches look at www.alteon.com.

“Switches provide VLANS so that you can segment off different logical networks, but use a single switch for all devices.”

PCNA

Copyright ITP, 2000

Recent Reviews from [Tech Support Alert](#)

[Reviews of the Best Windows Backup Software](#)

In this detailed comparative review, we checked out eighteen backup software utilities designed for home or SOHO use. Many of the products reviewed were disappointing. However 6 products passed our tests with flying colors and 2 of these were so impressive, they were awarded our "Editor's Choice."

[Suppliers of Cheap Inkjet Printer Cartridges Reviewed and Rated](#)

With hundreds of companies all claiming to have the "*cheapest and best inkjet printer cartridges*," our editors decided to put their claims to the test. Not unexpectedly, many suppliers flunked but we did manage to come up with a number of web sites that sell good quality inkjet printer cartridges at heavily discounted prices.

[The Best Anti Trojan Software](#)

Our editors took a close look at the 6 leading anti-trojan/trojan remover software utilities. Unfortunately, they found only 2 products that were effective in their ability to detect and remove dangerous modern polymorphic and process injecting trojans.

[The 46 Best Ever Freeware Utilities](#)

This is our Editor, Ian "Gizmo" Richards, personal selection of the best freeware utilities. He's hunted down some real gems, many of which perform better than expensive commercial products.