

WHAT YOU NEED TO KNOW TO REDUCE IP CONFLICTS NOW



INTRODUCTION

Computer scientist and science fiction author, Vernor Vinge coined the phrase, “Even the largest avalanche is triggered by small things.” Many network and systems administrators know firsthand that an IP conflict is indeed a very small (and often avoidable) thing that can snowball into an avalanche of unwanted consequences. This paper addresses why IP conflicts occur, and explores methods for minimizing their risks and havoc they can cause.

WHY DO IP CONFLICTS OCCUR?

An IP conflict occurs when two devices connected to the same network receive the same IP address. It's analogous to two houses sharing the same mailing address, or two individuals sharing the same social security number. When the network cannot uniquely distinguish a system, communication errors occur.

IP conflicts exhibit symptoms in ways that are inconsistent, which suggests a number of possible root causes. The following story illustrates this point:

Someone brought a new desktop computer into work and plugged it into the network. Soon after, all remote connections to the accounting server went down.

Not knowing why this happened, IT started investigating the problem. First, they rebooted the remote access server. Next, they changed the switch port and network cables. They even tried unplugging all devices from the switch. When they did this, the problem went away.

That's how they knew another device connected to the switch was causing the problem. They started looking for an IP conflict, and much later they found the outside computer plugged into the network.

IP conflicts occur for many reasons, which means they constantly put your network at risk of outages and lost productivity. They often disrupt service continuity and require skilled resources to find and fix. Fortunately, there are ways you can minimize the risk and impact of IP conflicts.

Inadequate network segmentation

Networks with a diverse range of device types that use static and dynamic IPs are more vulnerable to IP conflicts than those comprising little more than a workstation and email server.

DHCP errors

DHCP server errors prevent IP addresses from being properly reserved or renewed. Further, client-side DHCP errors prevent a device from properly releasing a DHCP lease.



BYOD

Consumer-grade devices are often the leading cause of IP conflicts. Devices brought from home can cause conflicts in the workplace because work networks may use the same address range used by consumer devices (192.168.0.xxx). Home routers and wireless access points can also duplicate DHCP services (see Dueling DHCP).

Bad IP address recordkeeping

In large networks, you need to track and record IP address assignments. Track details like subnets, addresses used within each subnet, and details about the associated device in a spreadsheet. Clear, error-free recordkeeping helps ensure that the underlying data used to make IP address assignments is correct, which lowers the risk of future IP conflicts.

Human error

Human error is responsible for many IP conflicts. Transposing numbers when configuring an IP address, or forgetting to reserve a static address with DHCP can lead to future conflicts. Failing to properly update IP records, or relying on a simple ping result to determine an address status can also cause errors.

Inactive hardware

When a device fails to operate properly, is temporarily taken offline, or goes into hibernation, that device's address can be reclaimed and re-used. A conflict may occur when that device returns to service.

Dueling DHCP

A duplicate DHCP server can assign IP leases concurrent with another DHCP server. However, because these DHCP servers operate without coordination, each can issue IP leases that conflict with the other. This often occurs when a home router, or a misconfigured WAP, or a multi-function router is connected to the network.

How do you resolve an IP conflict?

The process for finding and fixing an IP conflict is fairly straightforward, but that doesn't mean it's easy. The initial difficulty is determining whether an IP conflict is actually the cause of a problem. However, once you confirm that an IP conflict is the root cause, you can use the following process to find the affected systems.

Let's assume you have a user who cannot access email.

Step 1. What does your documentation say? Does it jive with the network? What is the IP of the email server, and is the email server using the IP it's supposed to be using?

Step 2. Do you have network connectivity between the client and the server? Start by pinging the email server. Open the command prompt and enter this command: PING XXX.XXX.XXX.XXX.

“Even the largest avalanche is triggered by small things.”

— Vernor Vinge



Does the ping reply? Because the workstation is experiencing difficulty, it's likely the IP belonging to the system is causing the conflict. Now that you have an IP, you can trace it to a physical system by identifying its unique MAC address and the switch the device is connected to.

Step 3. From the command prompt, run a local ARP command. Use ARP - a to see what MAC address is associated with the IP returned by PING. If for any reason this ARP command does not provide a MAC address, you need to identify the router connected to your current subnet, and examine the router table. Once you have a MAC address, you can find the device on the network. The best way to do this is to identify which switch and switch port the device is connected to.

Step 4. Go to your switches and examine the MAC tables using this (Cisco iOS®) command: **SHOW MAC-ADDRESS TABLE**. See if the switch has a port associated with the MAC address in conflict. Repeat this process on all subnet-connected switches until you find the MAC and switch port.

Step 5. You can locate the actual device once you locate the MAC and switch port. Determine whether the device is using the conflicted IP, and fix it by isolating the system and reconfiguring it with another IP address.

Step 6. Identify and correct the root cause. Why did the conflict occur in the first place? How can you prevent it from happening again?

BEST PRACTICES FOR REDUCING IP CONFLICTS

To reduce IP conflicts, implement controls that address common causes, and quickly find and fix issues when they occur. Here are some other best practices:

Use network segmentation.

Use physical or virtual subnets to group similar devices together. For example, put end-user devices like PCs, laptops, and printers into their own dedicated networks. Why? Because you can better control critical systems and insulate them from mistakes that could result from managing end-user devices. This also allows you to reserve a dedicated pool of IP addresses. For servers, these may be static, manually managed IPs; for end-user devices, these may be dynamic IP leases managed by a DHCP server.

Avoid using an address space used by consumer-grade devices.

You can easily avoid an IP conflict if your company's network uses an address space that is different from the default used by a home device. When a personal device is plugged into a dissimilar network segment, the worst that will happen is the device does not route properly, which prevents it from accessing other internal systems. Furthermore, if a DHCP server associated with a home router or wireless access point is connected, that DHCP server will lease IP addresses, which are external to the host network. In this case, it will likely not route, and therefore cause little to no harm.



Use reliable and vendor-supported DHCP services.

IP conflicts can occur if your DHCP software (server or client) has programming defects. Avoid conflicts by using DHCP software provided by reliable vendors who support their product with alerts and software updates.

Use **IP Address Management (IPAM)** software. If you are managing more than 250 IPs, use IPAM to help avoid IP conflicts. IPAM software offers the following benefits:

- » Concurrent, multi-user access.
- » Automatic address management.
- » Integration with DHCP and DNS.
- » Proactive alerting when errors occur.
- » Roles and permissions, allowing you to safely delegate IP administration.
- » Alerting and reporting.

Use tools that help you find and fix IP conflicts. When a conflict occurs, time matters. Don't rely on users to report problems, or use outdated methods to troubleshoot IP conflicts. Look for tools that show which addresses are in conflict, how the conflict occurred, what types of devices are involved, who uses the devices, and where the devices are located.

By adopting these best practices, you can sensibly eliminate the small things that can lead to an IP conflict.



SOLARWINDS IP CONTROL BUNDLE

SolarWinds® IP Control Bundle can help you significantly reduce IP conflicts. It combines DHCP, DNS, and IP address management with switch port monitoring to find and fix IP conflicts fast. With IP Control Bundle, you can replace IP tracking spreadsheets with automated IP address management, and actively detect IP conflicts. For more information visit <http://www.solarwinds.com/lp/ip-control-bundle.aspx>.

