

Resolving Duplicate IP Addresses

October 2009

In This Article:

- Feature Overview
- IP Resolution Plans
- Procedure for Resolving Duplicates
- Competitive Advantage

SiteAudit 3.0 provides a new feature that allows users to resolve device address problems and retire devices that are no longer in use.

Feature Description

Duplicate Addresses exist for devices that have been assigned addresses, typically via DHCP, which might have changed while SiteAudit has been monitoring the devices. SiteAudit distinguishes devices based upon their IP addresses. Address conflicts can cause data from more than one device to be assigned to a single device producing erroneous results. Address conflicts can now be resolved with the new Address Resolution feature introduced in SiteAudit 3.0.

Scenarios That Cause Address Conflicts

There are several IP address assignment scenarios that will cause addressing conflicts. These scenarios and their effects on data collection are explained below.

Scenario #1

New IP Address



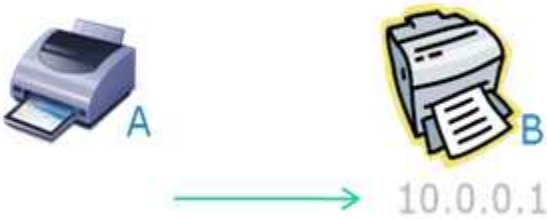
In this scenario, a device that is monitored by SiteAudit is given a new IP address. In this case, SiteAudit will contain two instances of the same device. Both will be present in the Inventory view. The device instance, 10.0.0.1, contains all of the data that was collected until the IP address changed. Assuming that address 10.0.0.1 is not assigned to another device, no more data is collected for it and it will eventually be detected as Unreachable. SiteAudit continues to collect data for the device under a new IP address of 10.0.0.3.

However, this does not include any data that had been collected when the device was assigned the IP address 10.0.0.1.

Resolving duplicate addresses combines the data collected for both IP addresses into one data collection for the active IP address, 10.0.0.3, so that the entire history of collected data is maintained under one device instance. Additionally, the device instance, 10.0.0.1, is removed from the SiteAudit inventory if the address is no longer in use.

Scenario #2

Transfer IP Addresses



In this scenario, SiteAudit had been monitoring a device at IP address, 10.0.0.1 when the IP address is reassigned to a new device. This type of change can cause erroneous data to appear in SiteAudit views and reports for this device. Suppose the device initially assigned the 10.0.0.1 address was a black and white inkjet printer and the address is reassigned to a color laser printer. SiteAudit will display color pages for a device that indicates it supports only black and white paper.

When address resolution is performed, the data collected for 10.0.0.1 is parsed such that the data collected for device A is separated from the data that was collected for the device B. The device A is given a new IPv6 address whereas the device B retains the 10.0.0.1 address. This allows the data collected for each device to be appropriately related.

Scenario #3

Switch IP Addresses



In Scenario #3, two devices have swapped IP addresses. Assume that the device at 10.0.0.1 is an HP LaserJet 4L and the device at 10.0.0.22 is a Canon iR C5870. The HP 4L is a black and white laser printer and the Canon is a color printer. SiteAudit collects and displays data correctly for both devices. Once the IP addresses are swapped, SiteAudit

collects data from the Canon printer and stores it for the HP and vice versa. This causes discrepancies for both devices.

Performing address resolution separates the data appropriately and applies it to the correct device. The IP addresses are changed appropriately to reflect the current addresses of the devices.

Resolve Duplicate Address Conflicts: Resolution Plans

Address conflicts can be resolved in SiteAudit by opening the **Resolve duplicate address conflicts** dialog and clicking the **Resolve addressing conflicts** button.

- Open the SiteAudit Viewer
- Select the **Resolve Duplicate Address Conflicts...** menu item from the **Tools** menu

The following dialog is displayed:

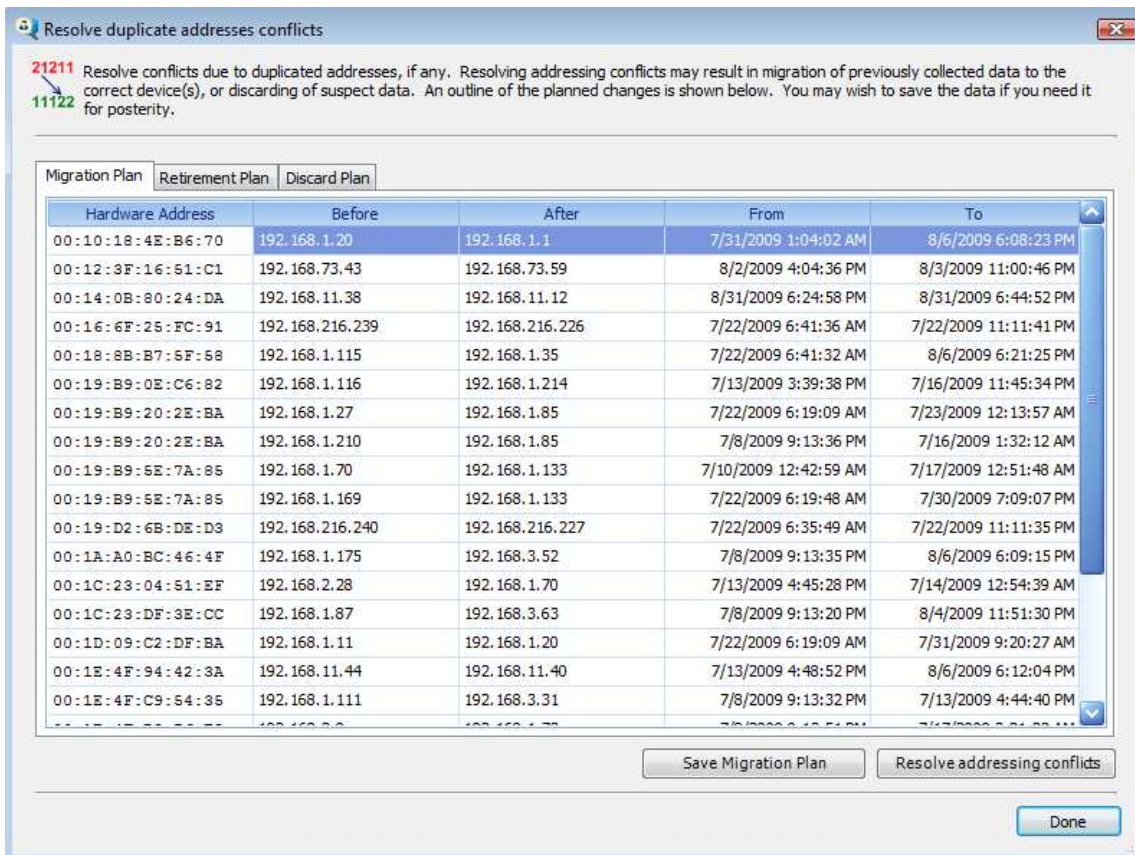


Figure 1: Migration Plan

Migration Plan

The migration plan shows the MAC address, which is unique to each device, and the IP addresses assigned to this device for a specific time period. The data from the migration plan can be saved if desired. See Figure 1 for an example migration plan.

Retirement Plan

The retirement plan shows all devices that are no longer available on the network. This occurs when a situation similar to Scenario #1 occurs. The retirement plan shows the MAC address for the device and the IPv6 address that will be assigned to the device. It is important to note that retired devices are not deleted from the SiteAudit collection. This allows one to retrieve the data if desired. Additionally, if the device is ever returned to service, SiteAudit will detect it and begin storing newly collected data for it. Figure 2 shows a sample retirement plan. The data from the retirement plan can be saved if desired.

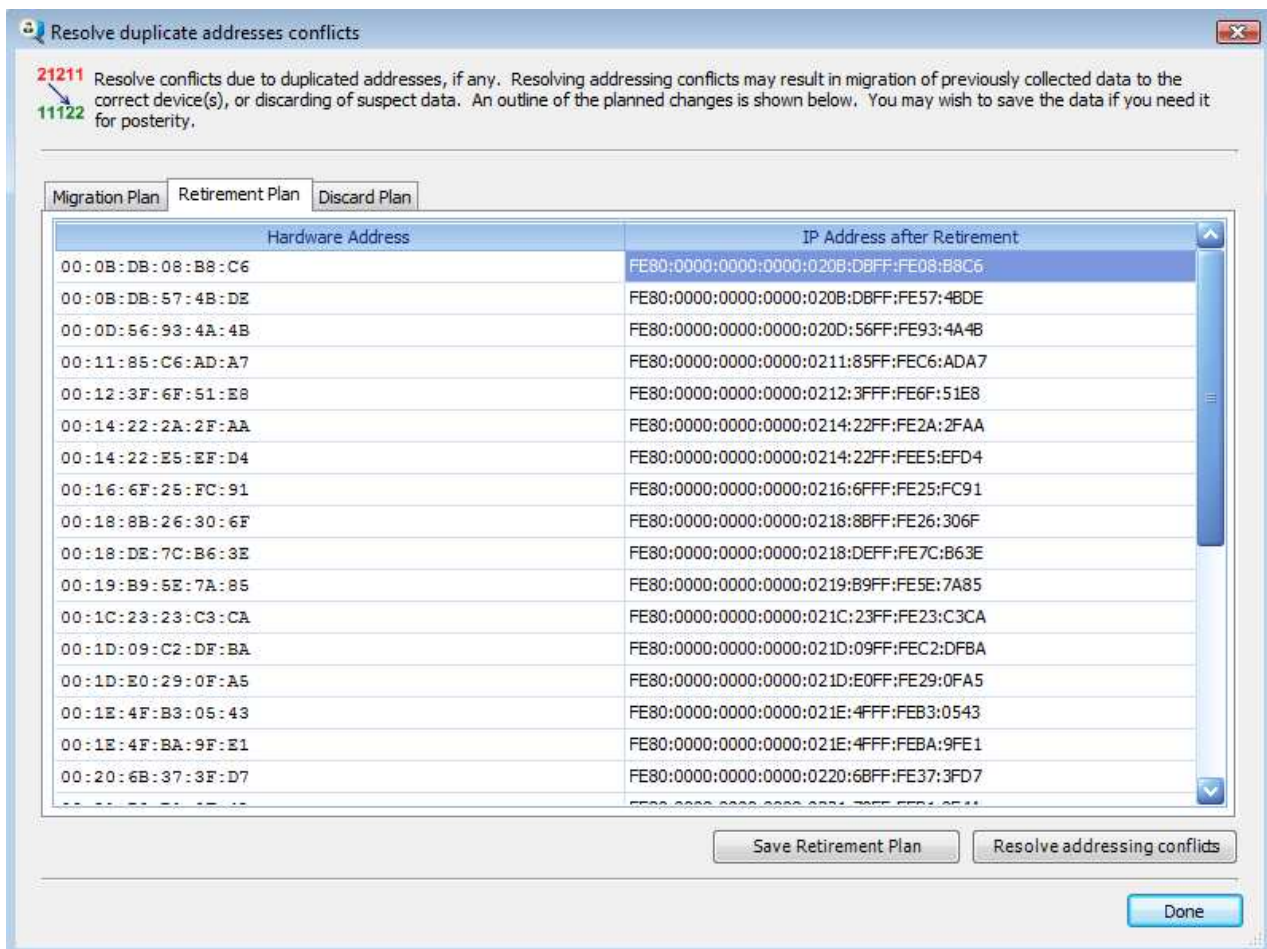
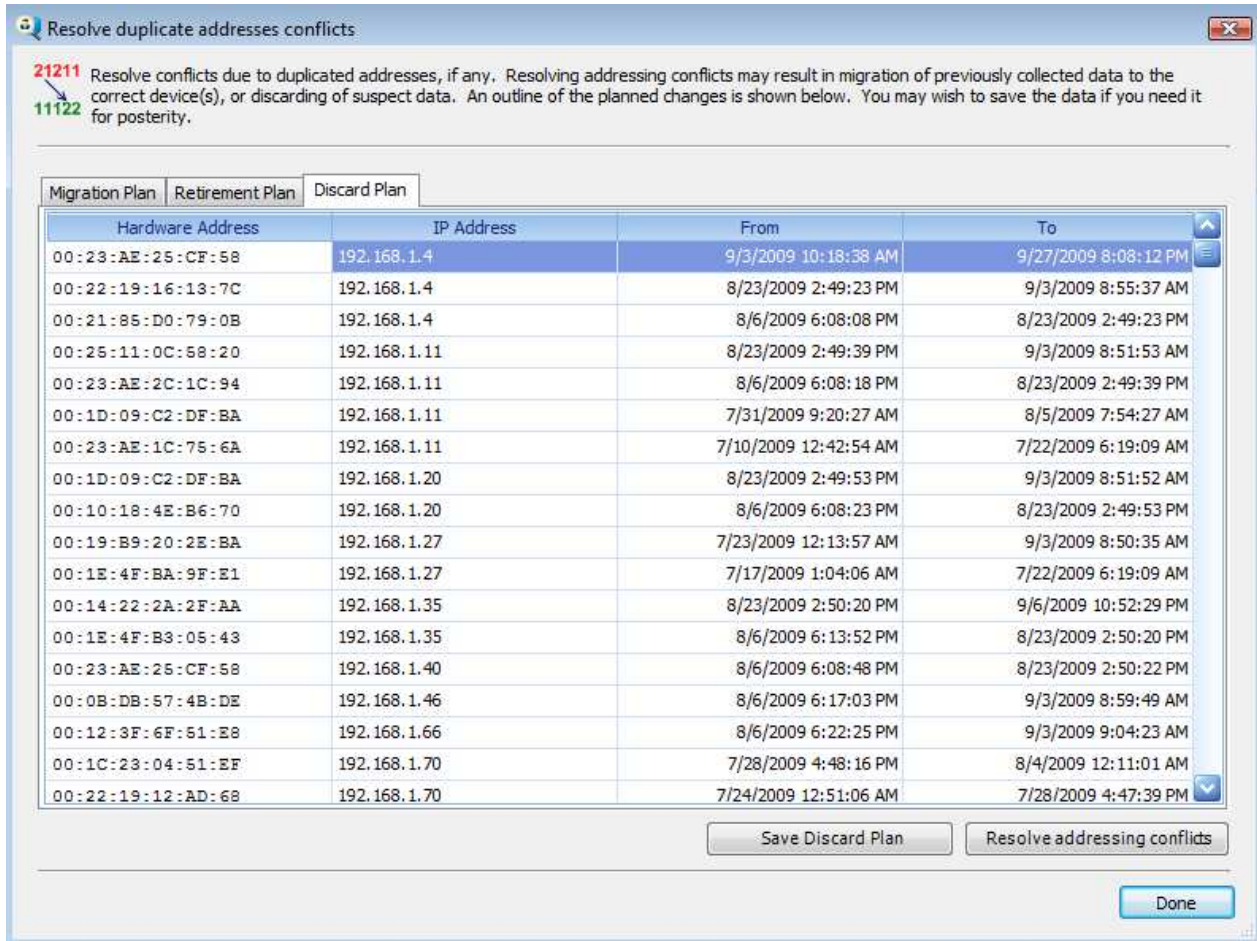


Figure 2 Retirement Plan

Discard Plan

The discard plan displays the MAC address and IP address of a device, and a To and From time. The *To* and *From* times indicate the time span in which SiteAudit is unable to determine which device to associate its data. When SiteAudit cannot determine which device to associate its data, the data is discarded since it cannot be reliably assigned to a specific printer. Users have the option to save the discard plan. See Figure 3 for a sample discard plan.



The screenshot shows a dialog box titled "Resolve duplicate addresses conflicts". It contains a message about resolving conflicts and a table with the following data:

Hardware Address	IP Address	From	To
00:23:AE:25:CF:58	192.168.1.4	9/3/2009 10:18:38 AM	9/27/2009 8:08:12 PM
00:22:19:16:13:7C	192.168.1.4	8/23/2009 2:49:23 PM	9/3/2009 8:55:37 AM
00:21:85:D0:79:0B	192.168.1.4	8/6/2009 6:08:08 PM	8/23/2009 2:49:23 PM
00:25:11:0C:58:20	192.168.1.11	8/23/2009 2:49:39 PM	9/3/2009 8:51:53 AM
00:23:AE:2C:1C:94	192.168.1.11	8/6/2009 6:08:18 PM	8/23/2009 2:49:39 PM
00:1D:09:C2:DF:BA	192.168.1.11	7/31/2009 9:20:27 AM	8/5/2009 7:54:27 AM
00:23:AE:1C:75:6A	192.168.1.11	7/10/2009 12:42:54 AM	7/22/2009 6:19:09 AM
00:1D:09:C2:DF:BA	192.168.1.20	8/23/2009 2:49:53 PM	9/3/2009 8:51:52 AM
00:10:18:4E:B6:70	192.168.1.20	8/6/2009 6:08:23 PM	8/23/2009 2:49:53 PM
00:19:B9:20:2E:BA	192.168.1.27	7/23/2009 12:13:57 AM	9/3/2009 8:50:35 AM
00:1E:4F:BA:9F:E1	192.168.1.27	7/17/2009 1:04:06 AM	7/22/2009 6:19:09 AM
00:14:22:2A:2F:AA	192.168.1.35	8/23/2009 2:50:20 PM	9/6/2009 10:52:29 PM
00:1E:4F:B3:05:43	192.168.1.35	8/6/2009 6:13:52 PM	8/23/2009 2:50:20 PM
00:23:AE:25:CF:58	192.168.1.40	8/6/2009 6:08:48 PM	8/23/2009 2:50:22 PM
00:0B:DB:57:4B:DE	192.168.1.46	8/6/2009 6:17:03 PM	9/3/2009 8:59:49 AM
00:12:3F:6F:51:E8	192.168.1.66	8/6/2009 6:22:25 PM	9/3/2009 9:04:23 AM
00:1C:23:04:51:EF	192.168.1.70	7/28/2009 4:48:16 PM	8/4/2009 12:11:01 AM
00:22:19:12:AD:68	192.168.1.70	7/24/2009 12:51:06 AM	7/28/2009 4:47:39 PM

Buttons at the bottom: Save Discard Plan, Resolve addressing conflicts, Done.

Figure 3 Discard Plan

Procedure for Resolving Duplicate Address Conflicts

1) BACKUP THE EXISTING DATABASE. The Duplicate Address Resolution tries to associate an IP address with a device MAC Address. There is a window within which it is possible that an IP address may not be definitively associated with a MAC Address. Since the resolution of address conflicts cannot be undone, it is important to backup your database prior to resolving conflicts.

***NOTE:** It is important to be sure that SiteAudit monitoring is stopped prior to resolving address conflicts. Run the address resolution from the machine where SiteAudit monitoring is installed or if running the address resolution from a SiteAudit viewer, be sure monitoring is turned off before resolving address conflicts.*

The address resolution must be run from the machine where SiteAudit monitoring is installed

2) To use this feature, select the menu item **Tools -> Resolve Duplicate Address Conflicts.** This will bring up a dialog that shows

- a) Migration Plan - This shows which IP address a device will be migrated to
- b) Retirement Plan - This shows the list of printers that SiteAudit believes have been removed. The IP addresses of retired devices are converted to IPv6 addresses to be able to distinguish them from non-"retired" devices.
- c) Discard Plan - This shows the list of printers for which data will be discarded and the time period over which this data will be discarded.
- d) You can save any/all of this data by clicking the Save Plan button and saving the results.
- e) Click the Resolve addressing conflicts to resolve the duplicate addresses

3) If a problem with the Address Resolution feature is suspected, contact support@netaphor.com. It may be necessary to upload your database, in which case you will be provided ftp site credentials to do so.

Competitive Advantage

SiteAudit v3.0 offers a competitive advantage over other MPS software tools. By resolving IP addresses print volume is not lost. Other MPS tools simply delete IP addresses to avoid duplicates.

The problem with deleting IP addresses is print volume is lost—as well as all stored printer history. For example, if a new printer is added during the first half of the month and uses the old IP address, deleting the old printer will eliminate the click charges for the first half of the month. Furthermore, if the old printer is someday added back to the network, its history is lost. SiteAudit IP resolution does not have this problem and so history and print counts are preserved.

Action: Please compare IP resolution features when evaluating competitive MPS solutions.