



## Network Traffic

March 2012

### In This Article:

- SiteAudit's Traffic Impact
- How SiteAudit Discovery Works
- Why Traffic is Minimal
- How to Measure Traffic

---

Minimal network traffic is the result of SiteAudit's design. The information below explains why network traffic is minimized.

### Network Traffic

Traffic can also be impacted based upon the way the network is designed and the number of networks, and its sub-netting and routing. This latter variance is of course true for any network application.

SiteAudit follows the "good citizen" principle of being unobtrusive and not adversely impacting the resources available to others in the environment.

- What is the traffic impact?

During normal operations the traffic impact cannot be measured, as it is minimal. There is no measurable impact on the network's bandwidth and quality of service.

If 'Discover networks automatically' is selected, SiteAudit will use broadcasts to find networks and devices. Broadcast can be disabled and discovery scoped to suite your environment. During the discovery cycle network traffic is measured at about 3%-to-5%.

*This is the peak for SiteAudit.* SiteAudit allows IP network discovery information to be imported to facilitate quick and easy setup. (See Knowledge Base article "Importing Data").

### How Discovery Works

If desired, SiteAudit is designed to discover all printer assets. Broadcasts, if enabled, are sent during the discovery cycle only. Broadcast packets are of the following types:

- SNMP
- ICMP

The discovery process works as follows:

- 1) For each network on the list that is included determine the addresses in that list
- 2) Determine if any of these addresses are excluded (either via another network or via a range)

- 3) For an included address send an ICMP packet to that address
- 4) If the address responds to ICMP
- 5) Determine if it supports SNMP, use each of the specified community strings to determine which community string should be used
- 6) SiteAudit scans the following ports to find printers:

Port	Protocol	Description
161	UDP	SNMP to see if SNMP is available. SNMP is used to collect data
80	TCP	HTTP to see if there is an embedded web server. HTTP is used to collect data
9100	TCP	Print protocol for printers, used to collect data
1650	TCP	Same as 9100
135	TCP/UDP	RPC, used to detect a Windows host for directly connected printers
631	TCP/UDP	IPP – print protocol, used to collect data

- 7) If it supports the Standard Printer MIB then it is a networked printer
- 8) If it supports SNMP but not the Standard Printer MIB and it supports Port 9100 (or equivalent) then it is a networked printer.
- 9) If it responds to ICMP but is not a networked printer determine if it serves Port 135.
- 10) If it supports Port 135 attempt to connect using WMI and one of the provided credentials
- 11) If the credentials worked, determine if there are any local printers or print queues on this host
- 12) The discovery process also scales to use multiple threads and connections depending on the host that it is running on and the resources

## Discovery Scans Timing

The length of time that a discovery scan takes depends on a number of factors. These factors include:

- 1) The host that SiteAudit is running on and the resources available on that host (i.e. processor, memory, network bandwidth).
- 2) The number of network addresses to be scanned.
- 3) Network bandwidth including the bandwidth of all of the networks that have to be scanned
- 4) Density of the networks and ranges that are to be scanned. Sparsely populated networks will take significantly longer to scan. This is due to the fact that in sparsely populated networks a number of addresses will not respond to ICMP which in turn will require retries *after* the timeout period which causes the scan for these networks to last longer.

The discovery scan is scheduled to run in 7 day intervals. For example, if the discovery scan takes 2 days to complete, the next scan will begin in 5 days. If a discovery scan takes longer than 7 days, the next one begins upon completion of the previous scan.

## Why Traffic is Minimal

SiteAudit data collection can be characterized as a *slow, steady receipt of packets*. This results in a smaller percent of the network bandwidth being used.

In contrast, applications like Web JetAdmin send blasts over the network. As a consequence, these types of applications require scheduling of data collection, typically during off-peak hours. *This is a product design difference* that shows up in the timing of when data is available and the amount of network traffic generated.

## Collection by Data Type

SiteAudit printer data is of two types:

- Volatile Data (Data that can change frequently):
  - Page Counts - collected every 3 hours
  - Print Jobs – collected every 4 hours
  - Toner Information - collected every 40 minutes
  - Alerts - checked for changes every 10 minutes
  - Thresholds – checked every 30 minutes
  - Device Status – checked every 10 minutes
  - Move Add Change – checked every 10 minutes
  
- Stable Data: (Data that does not change frequently)
  - Network and Identification information - Checked every 12 hours
  - Configuration Information (input/output options) - Checked every 12 hours

SiteAudit also stores data about addresses that are discovered by SiteAudit but are not printers. This data includes

- SNMP Information, Port Information
- For Windows hosts, Make/Model/Last Reboot time and Logged in User.
- For Windows hosts that are print servers and have queues located on them, SiteAudit will also collect job data (if configured to).

## Network Traffic Volume

Network traffic is dependent on the number of devices that SiteAudit is monitoring. The following factors go into calculating the number of packets:

- **Discovery Traffic:**
  - ICMP: An ICMP packet is sent to each IP address for each network on the list for discovery. If the broadcast address for a network is included then an ICMP broadcast is sent to that network. The packet is retried 3 times for devices that do not respond.
  - SNMP: An SNMP packet is sent to each IP address for each network on the list for discovery. If the broadcast address for a network is included then an ICMP broadcast is sent to that network. The packet is retried 3 times for devices that do not respond. The packet is retried for each community string in the list of community strings that are provided. This particular packet type can be reduced by removing community strings that are not required from the list of pre-seeded community strings that have been provided.
  - Port Scan: Each device that responds to an ICMP packet will also receive port scan packets. The port numbers that are scanned for each device are 161, 80, 8080, 9100, 1650, 631 and 135. All these are TCP ports with the exception of port 161 which is a UDP port. Each scan is retried 3 times.
- **Monitoring Traffic:**
  - Volatile data: This depends on the type of the device and the number of counters and consumable information available for each device. Advanced devices support about 20 counts. Each count requires one packet. Typical devices support 3-4 counts. Each packet is 512 bytes. There are no retries. Consumable data is similar to count data. Advanced devices support 3-4 types of consumables and each consumable has 6 pieces of information required for it. Thus, 18-24 packets for advanced devices may be required. Alerts are polled by examining the alert table. If there are no changes in the alert table then it is not retrieved. The alert table has 7 individual pieces of data for it that is retrieved.
  - Stable data: Typically about 100 packets of data per device are retrieved per day.
- **Local Printers and Queue Data:**
  - All of this data is retrieved using WMI. WMI uses RPC and windows authentication. 5 separate queries per host that is to be polled are issued. The packets are TCP and the size and number of the packets depends on the network packet size, the type of authentication present and the query being issued.
- **SQL Traffic:** SQL traffic is used to update the DB when data changes. This is TCP traffic to the server. SQL traffic also exists for queries between SiteAudit viewer applications and the database. The amount of traffic depends on the number of devices present, the maximum size of the network packet and the type of authentication used. The traffic is only between the hosts running SiteAudit and the SQL server.

- **Other Traffic:** Other traffic may exist if email notifications need to be generated. Additionally, if scheduled reports are used then these reports will be emailed to the destinations. Email traffic is to the SMTP server.

## How to Measure Network Traffic

Of course, quantifying and forecasting network traffic is difficult based on each environment. Among the variables is the network configuration, the device types, for example a high-end MFP with many whistles and bells does generate more messages than a desktop monochrome laser printer. While SiteAudit has not had a problem relating to generation of excessive network traffic, testing this in the customer environment is important. A simple way to do this is run a network analyzer application in a small test lab to see what traffic is generated.

Netaphor can recommend a free application called Wireshark for testing. It is available at [www.wireshark.com/](http://www.wireshark.com/).