TallyGenicom TechNote Net-001

Performing Network Printer Captures

Products: Network

Summary: Network captures are an essential part of printer troubleshooting in today's environment. A network sniffer consisting of a laptop with network interface(s) and sniffing software can be used to perform a network trace. This document outlines methods of making the network connection.

Notes:

- This document presumes a familiarity with the Windows operating system and with networks.
- It is recommended that the techniques listed here are practiced before performing on site.

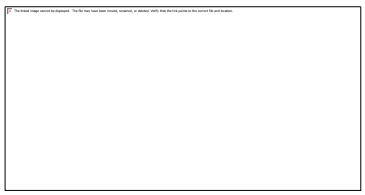
Solution/Action:

1 - Plugging directly to the hub/switch

The traditional method of capturing network traffic consists of plugging the network sniffer directly into an existing hub or switch on the customer's network. Most modern hubs and switches are non-promiscuous, thus this method is no longer useful.

Promiscuous hub/switch:

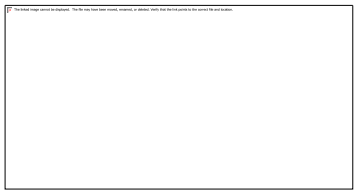
A promiscuous hub will send network data out to every port. Any device that the data is not addressed to will simply reject the incoming data. A network sniffer can be attached to any port on the hub and can trap the data intended for the printer.



This does create a lot of network traffic and is not secure, thus these types of hubs are generally no longer in use.

Non-Promiscuous hub/switch:

A non-promiscuous hub will send data only to the port where the destination device is attached. This creates a lot less traffic than a promiscuous hub, and enhances network security. A network sniffer attached to the hub will not see data intended for the printer.

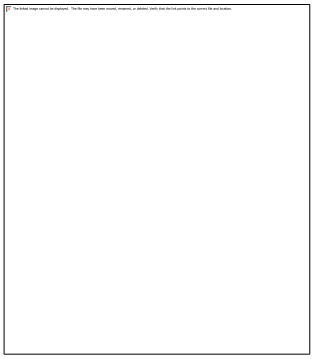


Some hubs may have a monitor port that is promiscuous, however the port may be disabled or set to non-promiscuous mode.

Since all network traffic is available on a monitor port, the network administrator will usually not allow trapping of data from these ports due to security concerns.

2 - Using a mini-hub

Another traditional method is to use a small hub to attach the printer and the sniffer to the customer network.

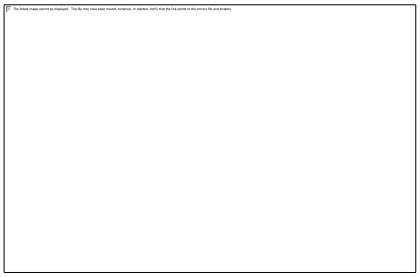


Again, this only works with a non-promiscuous hub. Most modern mini-hubs are non-promiscuous and cannot be configured.

One must also consider the 'hop limit'. Generally, network traffic will only pass through a maximum of three hubs or switches. If the mini-hub is the fourth device, network traffic will not pass to the printer.

3 - Using a laptop as a router

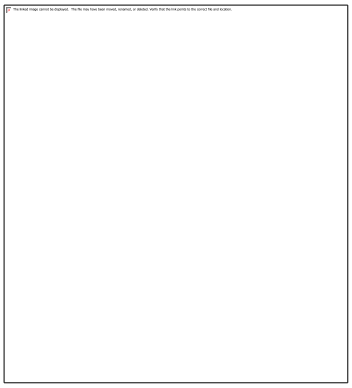
The preferred method is to use a laptop configured as a router. The laptop must be running Windows 2000 or XP, have two network interfaces and be connected to the printer with an ethernet crossover cable.



The laptop must be configured with two network interfaces. Many modern laptops have one interface built in, or, it can be added as an option. The second interface can be from a docking station or port replicator, a PC Card/CardBus (PCMCIA) option, or a USB option. If multiple PC Cards are to be used, they must be able to physically co-exist in the available slots.

Setup:

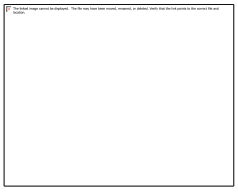
The network interfaces and drivers should be installed per the vendors instructions.



If the customer network uses DHCP, the primary interface (the one connected to the customer network) should be set to DHCP. If the customer network uses static addressing, the interface should be set with an IP address, subnet mask and default gateway obtained from the customer.

To create a bridge, open the Network Connections dialog, right click on each interface and select Add to Bridge. Connect the user network to the primary interface with a standard ethernet cable. Connect the printer to the secondary interface with the crossover cable.

When starting the sniffer capture, ensure the bridge is selected as the interface.



Need help? Call our knowledgeable sales staff at: ***708-597-4222***