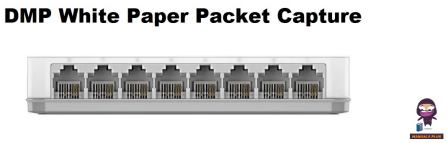


DMP White Paper Packet Capture User Guide

Contents

1 DMP White Paper Packet Capture
2 Product Information
3 FAQ
4 Introduction
5 Starting a Packet Capture
6 Contact
7 Documents / Resources
7.1 References
8 Related Posts

DMP White Paper Packet Capture

Product Information

This product is a Packet Capture Guide that provides instructions on how to start a packet capture using Wireshark software.

Specifications

- **Product Name:** Packet Capture Guide
- **Software:** Wireshark
- **Recommended Usage:** Capturing alarm panel traffic

FAQ

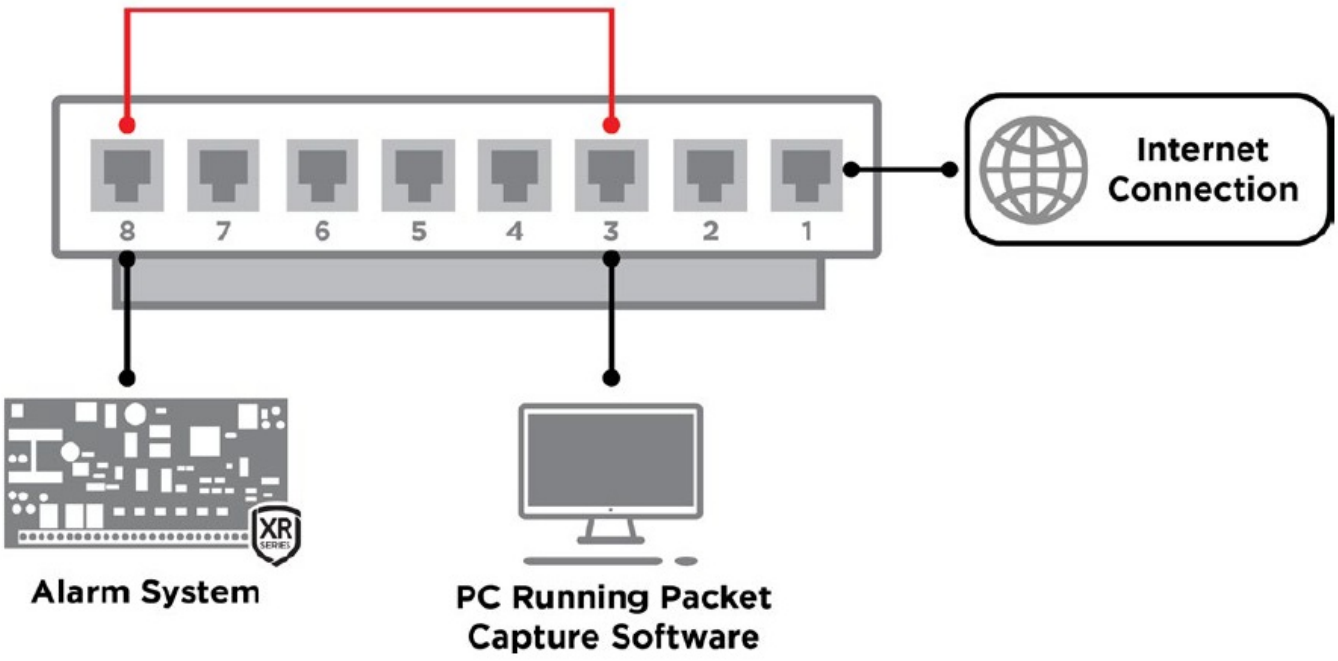
- **Q:** What software is recommended for packet capture?
  - **A:** Wireshark is a common and free packet capture software recommended for capturing network traffic.
- **Q:** How often are files saved during a capture?
  - **A:** Files are automatically saved every 10 megabytes during a capture process.

Introduction

If you're having issues with your customer's network, please be aware of the White Paper entitled, "**Important Ports for DMP Product Compatibility**." If you're still having issues, this guide can help you attain a packet capture so your appropriate person or IT team is able to investigate the issue with you.

First, a bit about Port Mirroring: Network engineers or administrators use port mirroring to analyze and debug data or diagnose errors on a network. Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic such as an intrusion detection system. Port mirroring on a Cisco Systems switch is generally referred to as Switched Port Analyzer (SPAN) or Remote Switched Port Analyzer (RSPAN). Other vendors have different names for it, such as Roving Analysis Port (RAP) on 3Com switches. **Source: Wikipedia**.

Example: Port 3 is mirroring Port 8. Only the traffic from Port 8 is captured.



Starting a Packet Capture

A common and free packet capture software is called Wireshark. Once Wireshark has been installed, there are very few steps required to start a capture. DMP prefers an unfiltered capture of the alarm panel traffic from a mirrored port on the same switch as the alarm panel.

1. Connect the PC running the packet capture software to the port on the switch that is mirroring the alarm panel's port on the switch. For specific setup instructions for your switch, please consult the manufacturer's guide.
2. If you will be leaving the capture running to identify an intermittent issue, continue to Step 3. If you are going to perform a short capture and save, skip to Step 6.
3. Open the Wireshark software and click the Capture Options icon .
4. Select the "Output" tab and then fill in the appropriate settings. You will need to select a file name, output format (pcapng is default and works well) and check the "Create a new file automatically" box. To allow the capture to be easily shared with the appropriate group, you can set the file size to 10 megabytes. This allows the file to be emailed instead of needing a server to host a large capture.
5. Once the information is set, click "Start" and the capture will begin. Files will automatically be saved every 10 megabytes and a new file will be created.
6. If you skipped steps 3-5, simply click the "Start Capture" icon . When you are finished with your capture, select the "Stop" icon then select "File" and "Save As" and save your file in the appropriate location.
7. Send your Wireshark capture to the appropriate person/IT group who will be investigating this with you.

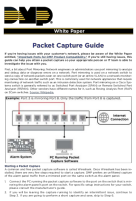
Contact

INTRUSION • FIRE • ACCESS • NETWORKS

- 866- 266-2826
- DMP.com
- 2500 North Partnership Boulevard Springfield, Missouri 65803-8877

LT-2537 24104 © 2024 Digital Monitoring Products, Inc.

Documents / Resources

	DMP White Paper Packet Capture [pdf] User Guide White Paper Packet Capture, White Paper Packet Capture, Paper Packet Capture, Packet Capture, Capture

References

- User Manual

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.