

Perform a Packet Capture on SD-WAN vManage

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

Introduction

This document describes how to do a Packet Capture on a Cisco SD-WAN vManage.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Packet analyzer

Components Used

This document is based on these software and hardware versions:

- vManage 20.9.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Background information contains the explanation of what is the Packet Capture feature on a vManage, the benefits to use this tool and the number protocols that can be used to filter the interested traffic.

The Packet Capture on the vManage allows to capture and analyze packet traffic on the SD-WAN network. Here are some important benefits to use this tool:

Problem Diagnosis: Packet capture is a valuable tool for troubleshooting network problems. This can be used to analyze packets and determine the cause of performance, latency, or packet loss issues.

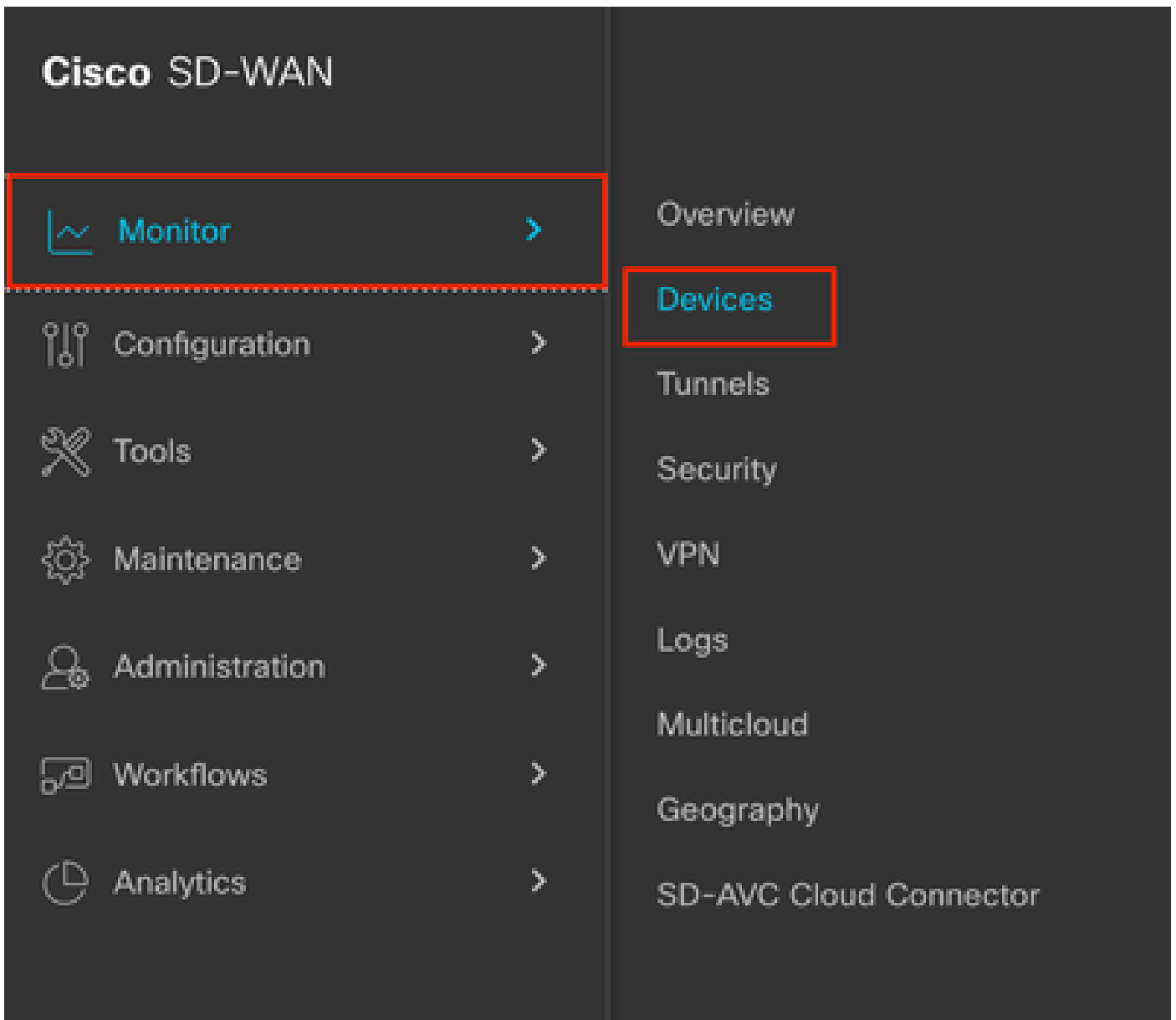
Filtering and Selective Capture: vManage allows you to configure filters to capture only relevant traffic, which reduces the load on the network and makes it easier to analyze specific packets.

Security: This feature can be used to identify malicious traffic patterns or suspicious activity on the network.

Decimal	Initials	Protocol	RFC
1	ICMP	Internet Control Message Protocol	RFC 792
2	IGMP	Internet Group Management Protocol	RFC 1112
4	IP	IP en IP (encapsulación)	RFC 2003
6	TCP	Transmission Control Protocol	RFC 793
8	EGP	Exterior Gateway Protocol	RFC 888
9	IGP	Interior Gateway Protocol	
17	UDP	User Datagram Protocol	RFC 768
41	IPv6	Encapsulación IPv6	RFC 2460
47	GRE	Generic Route Encapsulation	
50	ESP	Encapsulating Security Payload	RFC 2406
88	EIGRP	EIGRP	
89	OSPF	Open Shortest Path First	RFC 1583
112	VRRP	Virtual Router Redundancy Protocol	RFC 3768

Procedure

Step 1. Navigate to **Monitor > Devices**.



Step 2. Filter the device and click on the blue letters.



Note:

For 20.8.x and older releases bidirectional option is not present. Therefore, there are two scenarios to use packet capture feature:

Unidirectional: If **Source IP**, **Destination IP**, or both are filtered, the packets are captured only in one direction (from source to destination).

Bidirectional: If none of Traffic Filter options are used, the packets are captured in both directions.

For 20.9.x and later releases: **Bidirectional** option is present in these versions. Therefore, if **Source IP**, **Destination IP**, or both are filtered, the direction can be selected as Unidirectional or Bidirectional.

Cisco Catalyst SD-WAN | Select Resource Group | All Sites | Monitor - Devices

Overview | **Devices** | Tunnels | Applications | Security | VPN | More - 3

Devices

Devices | Certificates | Licensing

Device Group: All

Devices (1/7) [Export](#)

Search: rEdge-02

As of: Oct 06, 2023 08:30 AM

Hostname	Device Model	Site Name	System IP	Health	Reachability	vSmart Control	WFO	TLOC	Up Since	CPU Load	W	Actions
rEdge-02	CSR1000v	NYE_HQ	1.1.30.20			2 / 2	1 / 1	1 / 1	Jul 26, 2023 05:18 PM	10.7%		...

Items per page: 10 | 1 - 1 of 1 | < >

Step 3. Navigate to **Security Monitoring > Troubleshooting**.

SECURITY MONITORING

Firewall

Intrusion Prevention

URL Filtering

Advanced Malware Protection

TLS/SSL Decryption

Umbrella DNS Re-direct

Control Connections

System Status

Events

ACL Logs

: For this document the protocol 17 (UDP) was selected but you can use the protocol needed, to do this please refer to the list of the most important protocols on this document.



The screenshot shows the Cisco Catalyst SD-WAN Packet Capture configuration page. The breadcrumb navigation is "Devices > Troubleshooting > Packet Capture". The page title is "Monitor - Devices - Device 360". The selected device is "cEdge-02 | 1.1.30.20", Site Name is "102", and Device Model is "CSR1000v". The "VPN" is set to "VPN - 0" and the "Interface for VPN - 0" is "GigabitEthernet1 - ipv4 - 172.12.2.95". Under the "Traffic Filter" section, the "Source IP" is "172.12.2.95", "Destination IP" is "172.12.1.177", and "Protocol" is "17". A "Start" button is located at the bottom right of the configuration area.

Step 7. Once you have all the needed values to do the capture click on **Start**.



Step 8. The vManage then starts to capture the packets with the filters specified, you can stop it as soon as you get enough packets sent.

1

Packet Capture In Progress

Packet Capture will stop:

- In **4:54** Minutes, or
- 5-MB file is downloaded, or

 **Click** to stop packet capture

Step 9. Wait the vManage to prepare the file to be downloaded.

2

Preparing file to download

Loading...



Don't refresh or navigate away from this page.

Step 10. Then Download the Packet Capture file.

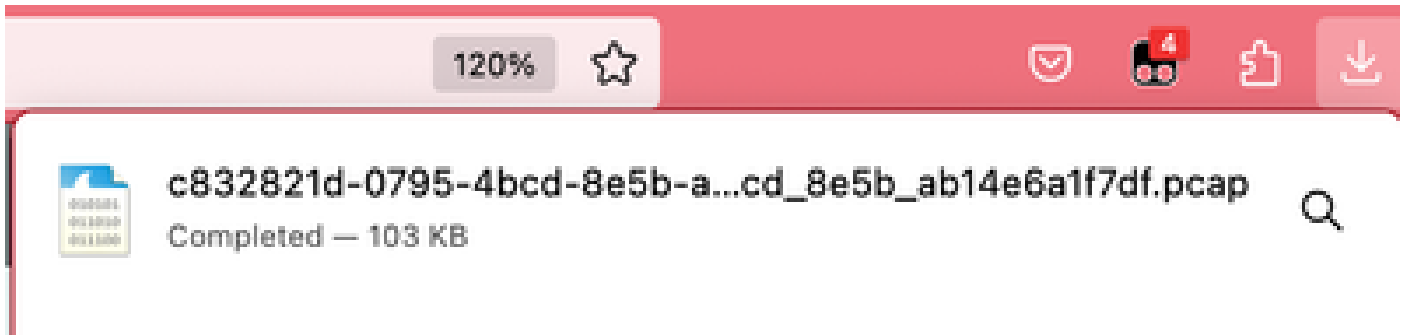
3

File ready

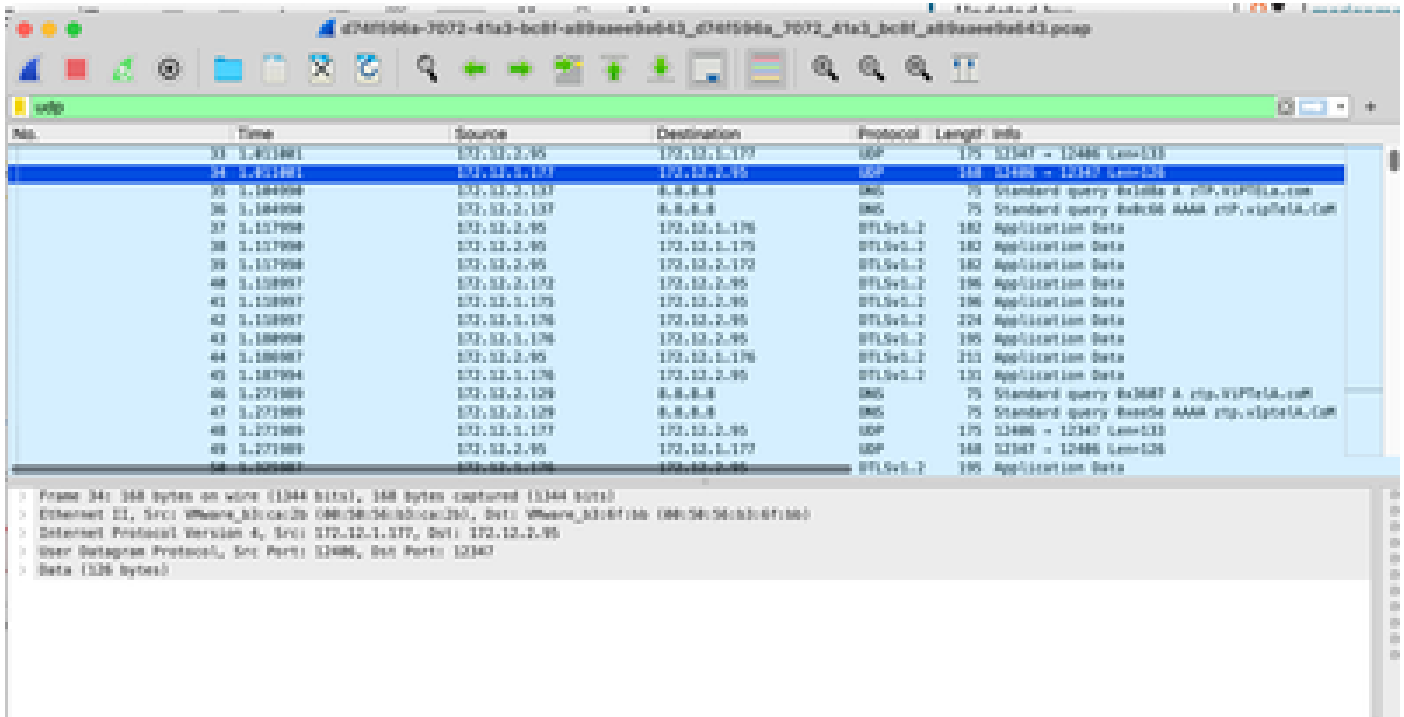


Click here to download
(105.54 KB)

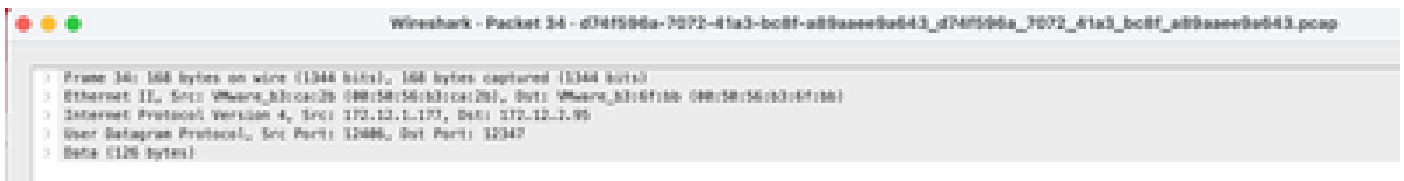
Step 11. The capture is now on your files, open it with a Packet analyzer such as Wireshark.



As you can see, there is a lot useful information that the capture can give, here the UDP packets were captured as expected.



When you open the UDP packet you see the information contained on it.



On frame information you can see information such **Arrival Time**, **Coloring Rule Name**, **Coloring Rule String**.

```

Frame 34: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 6, 2023 08:39:21.681956000 CST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1696403161.681956000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 1.011001000 seconds]
Frame Number: 34
Frame Length: 168 bytes (1344 bits)
Capture Length: 168 bytes (1344 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

```

You can see also the Source, Destination IP addresses such as the Source and Destination ports that you set previously.

```

Ethernet II, Src: VMware_b3:ca:2b (00:50:56:b3:ca:2b), Dst: VMware_b3:6f:bb (00:50:56:b3:6f:bb)
  Destination: VMware_b3:6f:bb (00:50:56:b3:6f:bb)
    Address: VMware_b3:6f:bb (00:50:56:b3:6f:bb)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Source: VMware_b3:ca:2b (00:50:56:b3:ca:2b)
    Address: VMware_b3:ca:2b (00:50:56:b3:ca:2b)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0000)
Internet Protocol Version 4, Src: 172.12.1.177, Dst: 172.12.2.95
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 154
  Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x1e6a [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.12.1.177
  Destination Address: 172.12.2.95

  0050 11010101 00010000 00000000 00000000 00000000 00000000 00000000
User Datagram Protocol, Src Port: 12406, Dst Port: 12347
  Source Port: 12406
  Destination Port: 12347
  Length: 134
  > Checksum: 0x0000 [zero-value ignored]
  [Stream index: 4]
  > [Timestamps]
  UDP payload (126 bytes)
Data (126 bytes)
  Data: a0000191000111cb0000000002daaa7018b69b6c2e9971c26126c75dcc1de300b48440bff_
  [Length: 126]

```

Related Information

