

Mist 運用マニュアル

手動パケットキャプチャー 取得手順

ジュニパーネットワークス株式会社
2022年8月 Ver 1.1

JUNIPER 
driven by Mist AI

はじめに

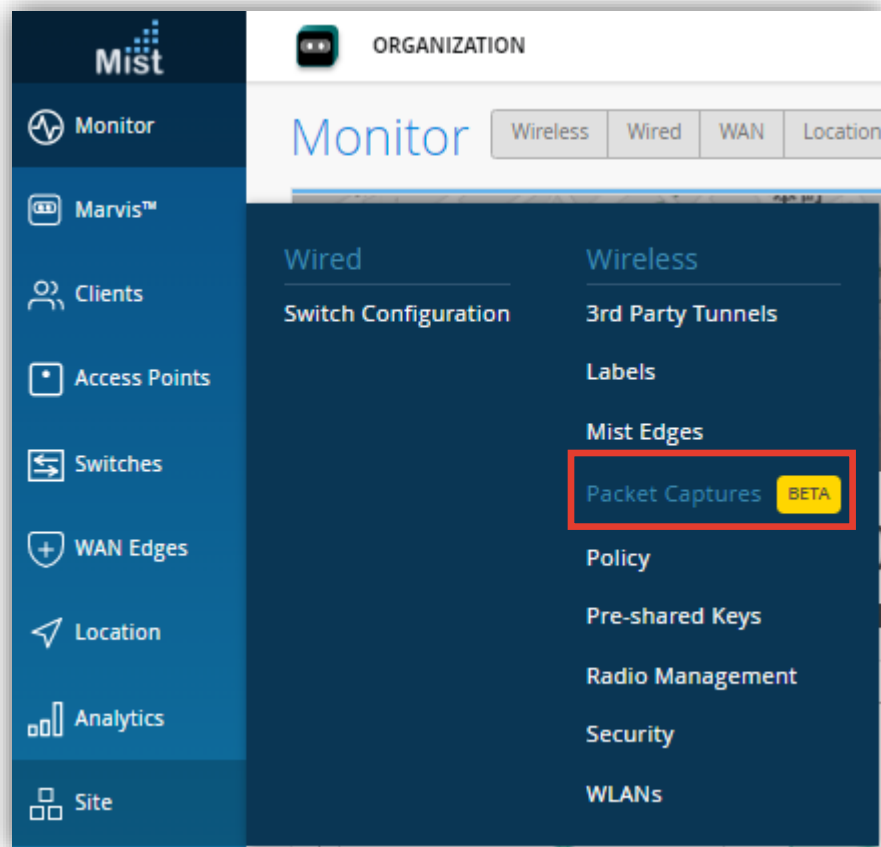
- ❖ 本マニュアルは、『手動パケットキャプチャー 取得手順』について説明します
- ❖ 手順内容は 2022年8月 時点の Mist Cloud にて確認を実施しております
実際の画面と表示が異なる場合は以下のアップデート情報をご確認下さい
<https://www.mist.com/documentation/category/product-updates/>
- ❖ 設定内容やパラメータは導入する環境や構成によって異なります
各種設定内容の詳細は下記リンクよりご確認ください
<https://www.mist.com/documentation/>
- ❖ 他にも多数の Mist 日本語マニュアルを「ソリューション&テクニカル情報サイト」に掲載しております
<https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html>

■ 運用ケース(例)

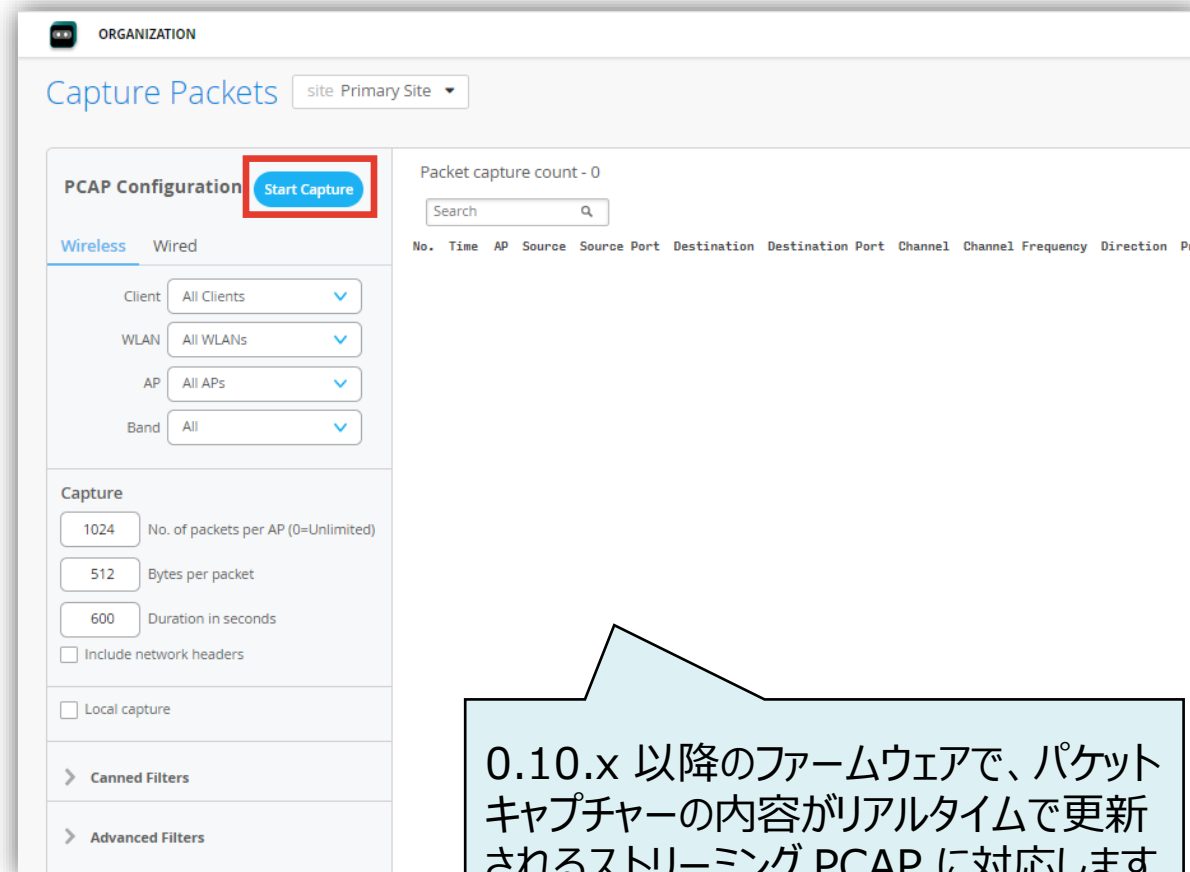
- パケットキャプチャーを手動で取得したい時

手動パケットキャプチャー 取得手順

1. [Site] から [Packet Captures]をクリックします



2. [Start Capture] をクリックします



0.10.x 以降のファームウェアで、パケットキャプチャーの内容がリアルタイムで更新されるストリーミング PCAP に対応します

手動パケットキャプチャー 取得条件の設定

3. パケットキャプチャー条件を設定できます

PCAP Configuration Start Capture

Wireless | Wired

Client: All Clients

WLAN: All WLANs

AP: All APs

Band: All

Capture

1024 No. of packets per AP (0=Unlimited)

512 Bytes per packet

600 Duration in seconds

Include network headers

キャプチャー対象を選択
※Wired は、AP の有線ポートを意味します

クライアントを指定

WLAN(SSID) を指定

AP を指定

Band(2.4, 5, 6)GHz
を指定

パケット数を指定

最大パケット長を指定

間隔を指定

ヘッダを含める場合指定

Local capture

▼ Canned Filters

Management

Control

Data

EAPOL

Beacons

Probes

0.10.x 未満の古いファームウェアでは、この [Local Capture] オプションを選択する必要があります

事前定義された汎用フィルタ
※ビーコンフレームをキャプチャするには、0.12.x ファームウェアが必要です

手動パケットキャプチャー 取得条件の設定

▼ **Advanced Filters**

TCPDUMP Expression

Use expression builder

Ethernet Host

Mac Address

MAC Address (Comma Separated)

tcpdump 形式のフィルタを適用できます

チェックすると、以下フィルタ作成メニューが表示されます

MAC アドレスを指定 (コンマ区切り)

IP Host

IP Address

IP Address (Comma Separated IPs or Host Names)

VLAN ID

Comma separated and Max 5

IP、または、ホスト名を指定 (コンマ区切り)

VLAN ID を指定※ (コンマ区切りで最大5)
※一部アカウントでのみ表示されるメニューです

手動パケットキャプチャー 取得条件の設定

IP Protocol

Select a Protocol ▼

Port / Port Range

Comma separated and Max 5

Broadcast

Ethernet IPv4

Multicast

Ethernet IPv4

プロトコルを指定

ポート、ポートレンジでの指定ができます
(コンマ区切りで最大5)

Broadcast/Multicast のキャプチャーを指定

手動パケットキャプチャー 取得開始/停止

4. パケットキャプチャーの取得が開始されると、リアルタイムで更新されます
基本的な分析に使用でき、さまざまな表示例とフィルタリングを使用できます

[Stop Capture] をクリックすると、パケットキャプチャーが停止します

フィルタ

ストリーミング PCAP ではリアルタイムで更新されます

パケットキャプチャーの経過時間が表示されます

クリックすると詳細表示

表示項目の設定ができます

ORGANIZATION

Capture Packets

PCAP Configuration

Stop Capture

Packet capture count - 164

Search

Wireless Capture

Client All Clients

WLAN All WLANs

AP All APs

No.	Time	AP	Source	Source Port	Destination	Destination Port	Channel	Channel Frequency	Direction	Protocol	RSSI	Length
1	02:44:55.56 PM, Aug 16	d4:20:b0:c1:64:63	56:de:4c:49:84:37		ff:ff:ff:ff:ff:ff		6	2437	tx	802.11	-67	188
2	02:44:55.77 PM, Aug 16	d4:20:b0:c1:64:63	a4:34:d9:64:73:dc		ff:ff:ff:ff:ff:ff		6	2437	tx	802.11	-49	117
3	02:44:55.77 PM, Aug 16	d4:20:b0:c1:64:63	d4:20:b0:e4:a8:81		a4:34:d9:64:73:dc		6	2437	tx	802.11	0	309
4	02:44:55.78 PM, Aug 16	d4:20:b0:c1:64:63	d4:20:b0:e4:a8:82		a4:34:d9:64:73:dc		6	2437	tx	802.11	0	307

00:01:59

Captured Files

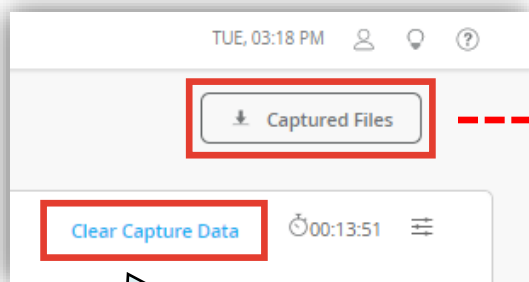
Table Settings

1. <input checked="" type="checkbox"/> No.	2. <input checked="" type="checkbox"/> Time	3. <input checked="" type="checkbox"/> AP
4. <input checked="" type="checkbox"/> Source	5. <input checked="" type="checkbox"/> Source Port	6. <input checked="" type="checkbox"/> Destination
7. <input checked="" type="checkbox"/> Destination Port	8. <input checked="" type="checkbox"/> Channel	9. <input checked="" type="checkbox"/> Channel Frequency
10. <input checked="" type="checkbox"/> Direction	11. <input checked="" type="checkbox"/> Protocol	12. <input checked="" type="checkbox"/> RSSI
13. <input checked="" type="checkbox"/> Length	14. <input checked="" type="checkbox"/> Frame Type	15. <input checked="" type="checkbox"/> Frame Subtype
16. <input checked="" type="checkbox"/> Datarate	17. <input checked="" type="checkbox"/> BSSID	

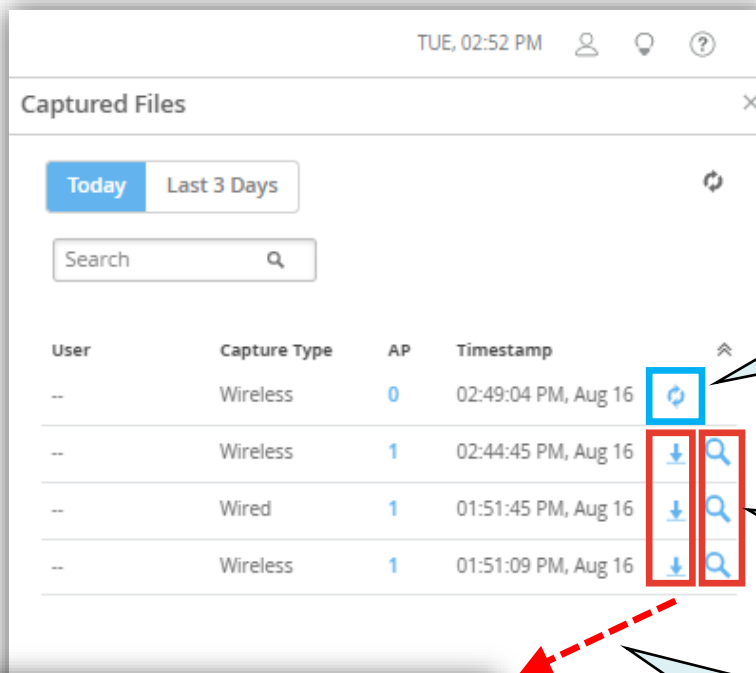
Time: 02:44:55.78 PM, Aug 16
AP: d4:20:b0:c1:64:63
AP MAC: d4:20:b0:c1:64:63
Source: d4:20:b0:e4:a8:83
Destination: a4:34:d9:64:73:dc
Content: 1860828696.007299 3415999104us tsft short preamble 1.0 Mb/s 2437 MHz 11g OdBm signal 1dBm noise antenna 0 Probe Response (MPSK-Radius) [1.0*

手動パケットキャプチャー 取得完了

5. パケットキャプチャーが終了すると、[Captured Files] から、パケットキャプチャーデータをダウンロードできます

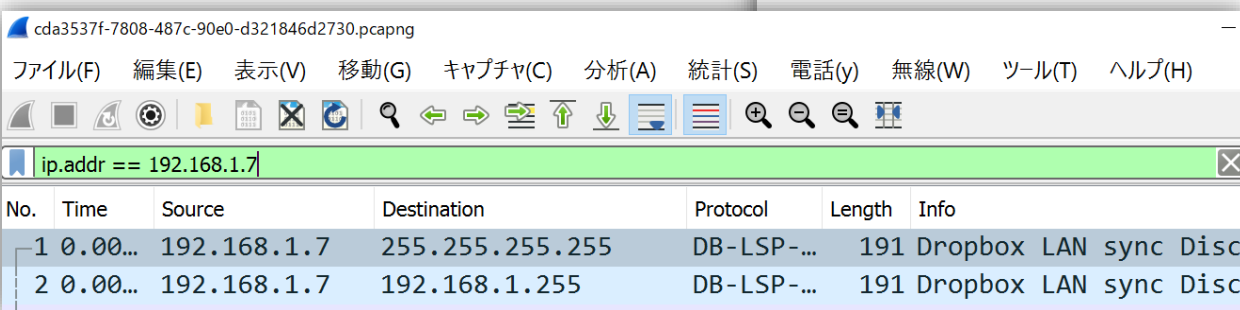


表示をクリアします
※キャプチャーデータは削除されません



実行中のパケットキャプチャーはダウンロードできません

CloudShark での解析ができます



ダウンロードして、Wireshark 等でパケットキャプチャーを確認できます
※20MB 超のファイルの場合、保存されるデータは最後の 20MB となります

Thank you

JUNIPER
driven by Mist AI 