ホワイトペーパー

イン-メモリ・データベースとパケットリングバッファ

異なる目的のための2つのデータベース

Allegro ネットワーク マルチメータは、ネットワークの問題を検出するための強力なリアルタイム ネットワーク マルチメータです。 レイヤ 2 からレイヤ 7 までの多くのパフォーマンス パラメータを測定し、トラブルシューティングとネットワーク分析に使用されます。
トラフィック履歴グラフ (MAC アドレス、IP アドレス、プロトコル、接続) を含む、デバイスによって記録されたすべての情報をリアルタイムで利用できます。さらに、グラフ㊋クリックして特定の時間枠にズームインし、その時間枠の結果のみを表示することができます。Allegro ネットワーク マルチメータは、記録された情報の表示と処理に 2 つの異なるデータベースを使用します。

- イン - メモリ・データベース
- HDD または SSD 上のパケットリングバッファ

このホワイトペーパーでは、さまざまなアプリケーション領域と実際の使用法について説明します。

図 1　Allegro ネットワーク マルチメータのアーキテクチャ

図 1 は、ネットワーク パケットを詳細に分析できるようにする、パケット処理の機能コンポーネントを簡略化して示しています。 IP アドレスや接続情報、パケットカウンタなどのメタデータはメインメモリ (=インメモリ) に保存されます。

Web ベースのインターフェイスに表示される値は、メインメモリから取得されます。 より深い履歴分析を可能にするために、これらのパケットは HDD/SSD 上の循環型リング バッファに保存され、キャプチャされたリクエストを後で詳細に検査できるようになります。

イン-メモリ・データベース

Allegro ネットワーク マルチメータは、メモリ内データベースを使用して、処理されたパケットのメタデータを保存します。これは、記録されたすべての測定データが時間のかかるディスクアクセスなしで利用可能であり、瞬時に検索するために呼び出すことができることを意味します。

Allegro マルチメータは、内部または外部ハードディスクなしで動作でき、メタデータにはメモリ内のみを使用します。つまり、データはハードディスクに書き込まれません。

インメモリ データベースの容量は、モデルに応じて 2 GB ～ 1.5 TB の間で異なります。 概算として、1 ギガバイトのインメモリ データベース毎に約 150,000 の接続履歴とその集計を保存できます。

Allegro ネットワーク マルチメータは、トラフィック量に合わせてメモリ構成を調整します。 常にすべてのデータを保存します。 メモリがいっぱいになると、最も長く非アクティブな接続と IP アドレスが削除されます。これは、小規模なネットワークではデバイスが履歴データを長期間保存するのに対し、大規模なネットワークではデバイスがより多くの IP アドレスと関連情報を保存しますが、保存期間は短期間であることを意味します。

Allegro システムのメモリは、できるだけ長く測定データを提供するために、時間の経過とともに自動的にいっぱいになります (メモリ予約を除く)。 その後、最適なシステム メモリを確保するために古いデータが自動的に削除されます。

Allegro ネットワーク マルチメータの Web インターフェイスの「情報」サブメニューのシステム情報ページには、現在のメモリ使用量とデータが利用可能な期間が表示されます。 保存時間はデータ トラフィックの種類によって異なります。

デフォルトでは、すべてのグラフはネットワーク トラフィックを 1 秒の解像度で表示します。 古く記録されたネットワークトラフィックの詳細レベルは、自動的に最大 1 分に削減されます。 管理者は、システム設定でグラフィック解像度と縮小値の両方を調整することができます。 これらの設定により、グラフィックがより詳細になったり、データの保存時間が長くなったりする可能性があります。 グラフ解像度は 1 ミリ秒まで下げることができます。

インメモリ データベースに保存されているメタデータは、Allegro ネットワーク マルチメータの処理が停止すると (更新、シャットダウン、再起動、再起動) 失われます。 メタデータは停電の場合にも失われます。

Allegro ネットワーク マルチメータはネットワーク情報を永続的に保存しないため、デバイスはセキュリティが厳しいエリアでも使用できます。 記録された情報の復元や、過去のパケットを個別に抽出したい場合は、パケットリングバッファの使用をお勧めします。

リングバッファ

パケット リング バッファを使用する場合、パケットは接続された記憶媒体に保存されます。 この目的には次のシステムを使用できます。

- 内蔵 HDD または SSD (Allegro 500 以降)、
- USB3 経由の外付け HDD (全 Allegro マルチメータ)
- 管理ポート経由の iSCSI (全 Allegro マルチメータ)

リング バッファを使用すると、記録されたすべてのパケットを 1 つ以上の外部ストレージ デバイスに保存する固定サイズのパケット バッファを作成できます。 バッファがいっぱいになると、バッファ内の最も古いパケットが新しいパケットに置き換えられます。

イン - メモリ データベース

- ✓ すべての測定データへの直接アクセス
- ✓ 高速な問題検索とネットワークレイヤの関連付け
- ✓ 過去のすべての接続へのアクセス
- ✓ データ保護に関する評価用途

リングバッファ

- ✓ 生データの永続的な自動記録
- ✓ 過去のネットワークパケットを対象に抽出
- ✓ ネットワークアクセスを必要としない、保存されたネットワークパケットの遡及分析
- ✓ 保存されたパケットを再分析することにより、インメモリデータベースのすべての機能にアクセ 2

リング バッファは複数のハードディスク上に作成することもできます。 数ペタバイトのリング バッファを持つ最大 64 台のハードディスクがサポートされます。 さらに、0 から 3 までの冗長性を備えたデータ冗長性がサポートされています。
悪用を防ぐために、ストレージ デバイスを AES256 暗号化でフォーマットできます (注意：パスワードなしでその後ディスクにアクセスすることはできません)。

パケット リング バッファは、パケット キャプチャ ファイルの分析にも使用できます。 さらに、パケット リング バッファは、パケットの抽出を簡素化するために pcap ファイルの分析にも使用されます。 パケット リング バッファの過去の内容はすべて削除されることに注意してください。 したがって、意図しない削除を防ぐために、この動作はファイル分析ダイアログで明示的に有効にする必要があります。

使用例 1　過去のpcapファイル抽出

Allegro ネットワーク マルチメータ上の HDD パケットリングバッファを使用すると、過去のトラフィックを抽出し、そこから pcap を作成することができます。 パケット リング バッファは、内部ストレージ デバイスと外部ストレージ デバイスの両方に設定できます。 Allegro ネットワーク マルチメータがストレージ デバイスとともに出荷される場合、リング バッファは事前設定されており、利用可能な容量の 75% を使用します。 それ以外の場合、リング バッファは、Web インターフェイスの対応するページ上のフォーマット済みストレージ デバイス上に直接作成できます。
「パケット リング バッファ」統計ページには、リング バッファの使用状況に関する情報と、保存されたトラフィックの複数のグラフが表示されます (図 2)。 フィルタを使用して、どのパケットをリング バッファに保存するかを設定できます。デフォルトでは、すべてのパケットが保存されます。

図 2　パケット リング バッファの統計と構成

キャプチャ機能はリングバッファの内容にアクセスし、過去のデータトラフィックを抽出できます。 Web インターフェイスのすべてのページに pcap シンボルがあります。 パケットを抽出する統計の横にある pcap アイコンをクリックします。
これにより、対応するダイアログ ウィンドウが開き、適切な期間といくつかのオプションが提案されます。

期間や提案されるオプションを変更することができます。 録画の開始時刻がパケットリングバッファの開始時刻より前の場合、録画の開始時刻は自動的に調整され、図 3 のメッセージが表示されます。

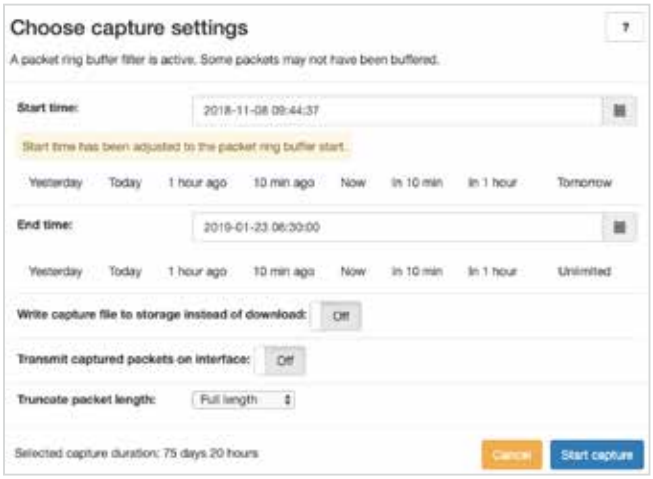

図 3: リング バッファ内の利用可能な時間間隔に時間調整を行ったキャプチャ ダイアログ

リング バッファがアクティブになると、システム全体で pcap キャプチャ ボタンの動作が変わります。ユーザインターフェイスがライブモードでキャプチャが開始される場合は、キャプチャをいつ開始するかを指定できるダイアログが表示されます。これにより、例えば、ある時点からの IP アドレスのトラフィックをキャプチャすることが可能になります。 ユーザインターフェイスが「バックインタイム」モード (過去から定義された期間が選択されている) の場合、キャプチャの開始時にダイアログ ボックスが表示され、キャプチャが選択した期間を正確にカバーしていることを確認します。　選択した期間が処理された後、キャプチャは自動的に停止します。
追加のオプションを使用すると、pcap ファイルをハードディスクに直接保存したり、パケットの先頭のみを転送したりすることができます。

どちらも、Allegro ネットワーク マルチメータの帯域幅が限られている場合に特に役立ちます。 VPN トンネル経由。 ここで、キャプチャはまずメモリに保存され、次に [一般] -> [データ キャリア] を介してダウンロードできます (図 4)。

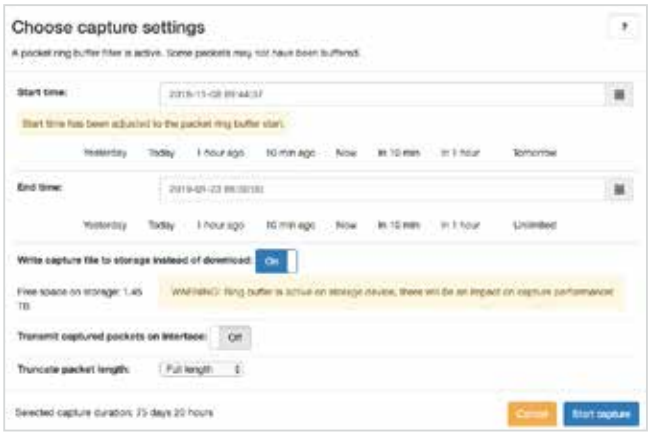

図 4: ダウンロードではなくデータ メディアに記録する代替方法

Allegro Packets ツールを使用すると、過去のトラフィックをネットワーク インターフェイスから再生ができます。 これは、分析目的でネットワーク内のエラーを再現する場合に非常に役立ちます。

Allegro Packets ツールを使用すると、過去のトラフィックをネットワーク インターフェイスから再生ができます。 これは、分析目的でネットワーク内のエラーを再現する場合に非常に役立ちます。

図 5 では、すべてのトラフィックが 10 MBit/s 帯域幅のポート 4 で再生されます。 トラフィックは、設定可能な速度でリアルタイムに再生することもできます。

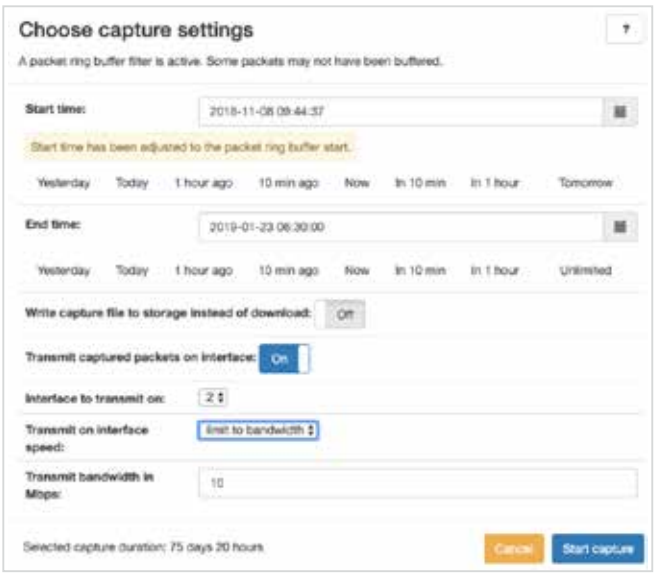

図 5: ポート 4 でのネットワーク トラフィックの繰り返し再生

使用例2　パケットリングバッファのプレフィルタ

デバイス、デバイスのグループ、またはアプリケーションのデータは、リング バッファに記録および保存されます。 これは、Allegro システムの「統計」の「パケット リング ストレージ」ページで設定できます。 このための前提条件は、接続されたストレージ デバイスが事前にフォーマットされており、その上にリング バッファが作成されていることです。
Allegro Packets ツールは、たとえば次のフィルタ機能を提供します。

• データ ストリームの特定の部分のみが記録されます。
1 つのデバイスまたはアプリケーションのデータがリング バッファに記録および保存されます。

• データ ストリームの下位 3 層のみが分析や次の処理に必要です。

最初のケースでは、Allegro ネットワーク マルチメータ ルールにより、特定のパケットがパケット リング バッファに保存されなくなります。

2 番目のケースでは、パケット リング バッファに格納されるパケットの記録長を定義するルールを設定できます。この場合、パケットの元の長さに関する情報はキャプチャに保持されます。リング バッファ フィルタ ルールを作成する場合、次のオプションが提供されます。

● **ルール条件**：すべてのパケット、または特定の MAC アドレス、IP アドレス、TCP/UDP ポート、VLAN タグ、または特定の値のインターフェイス
● **無効条件**：以前に定義された制限が逆にチェックされます (たとえば、特定の IP アドレスを記録する代わりに、特定の IP アドレスが除外されます)。
● **アクション**：適切なパッケージの処理方法を定義します。
- Recording length: パケットは、入力フィールドで指定された最大長で記録されます。 パケットが大きい場合、残りのバイトは破棄されます。
- Discard: パッケージ全体は記録されません。
- Full length: パケット全体が記録されます。
- Header: パケットヘッダのみが記録されます。

「L3」が選択されている場合、レイヤ 2 およびレイヤ 3 ヘッダ、つまり MAC および IP 情報が保存されます。
「L4」が選択されている場合、TCP または UDP ヘッダを含むレイヤ 2、3、および 4 が保存されます。

例：フルロードされた 10 GBit/s リンクが分析されます。 接続したハードディスクは最大 1GBit/s の記録が可能です。 また、すべてのデータが必要なわけではありません。 代わりに、1 つの SIP サーバとその接続のみを記録する必要があります。 このため、リング バッファには次の 2 つのルールが定義されています (図 6)。

- ルール 1: SIP サーバからの IP アドレス ->
  Recording Length: Flull length
  （パケット全体が記録されます。）
- ルール 2: その他の全てのパケットは破棄

これらのルールの利点は、Allegro ネットワーク マルチメータがより高いリンク帯域幅を処理し、それらを遡及的に長期間バッファリングできることです。

2 番目のステップでは、レイヤ 4 までのデータのみが保存されるようにルール 2 を変更できます。 これは、L4 ヘッダを含むすべての通信が利用可能であり、大幅に低い帯域幅でメモリに書き込むことができることを意味します。 平均パケット サイズが 700 バイトの場合、データ レートは約 80 % ~ 90 % 減少し、比較的遅い USB3 HDD 上でも 1 GBit/s を超えるリンクを分析できるようになります。
注：すべてのパケットがリング バッファに保存されていない場合でも、メタデータはすべてのトラフィックのメモリ内で利用できます。

図 6: IP 192.168.1.23 を完全に記録し、その他のパケットを破棄するフィルタルール

使用例３　リングバッファのフォレンジック(事後)分析

データ分析中に Allegro ネットワーク マルチメータのパケット リング バッファがアクティブになったとします。 すべてのパケットはパケット リング バッファに格納されます。 分析完了後に Allegro ネットワーク マルチメータのスイッチをオフにすると、測定データから取得したメタデータはメインメモリから削除されます。 ただし、パケットリングバッファに記録されたデータは、デバイスの電源がオフになった後も保持されます。
デバイスの電源が再びオンになると、管理者はパケット リング バッファの分析を開始できます。 これは、Web インターフェイスの [全般] -> [パケット リング ストア] -> [パケット リング ストアの分析] を介して開始されます (図 7)。

図 7: リングバッファに以前に記録されたパケットの再分析

パケット リング バッファに保存されているすべてのパケットは、Allegro ネットワーク マルチメータによって分析され、すべてのメタデータが再度生成されます。 すべての時間測定値とタイムスタンプが記録時間に正確に対応していること、およびすべての応答時間測定値にパケット内の時間値も含まれていることを確認する必要があります。

例： Allegro ネットワーク マルチメータは郵便で支社に送付され、従業員によって接続されます。 ネットワーク接続のみが、準備され事前構成されたポートに接続されます。 管理ポートへの接続は必要ありません。デバイスのスイッチをオンにすると、すべてのデータ パケットがリアルタイムでリング バッファに書き込まれます。
試用期間の終了後、Allegro デバイスの電源がオフになり、中央の IT 施設に返却されます。
デバイスは、中央 IT 施設の実験室またはテスト環境で再びオンになります。 ただし、ここでは管理ポートが使用され、パケット リング バッファに保存されているすべてのデータ / 統計情報は、[一般] -> [パケット リング メモリ] -> [パケットリング メモリの分析] を使用して復元されます。その後、管理者はすべての分析を (リアルタイム データと同様に) 実行し、必要に応じて対応する pcap を抽出できます。

使用例４　予約記録

Allegro ネットワーク マルチメータは、予約記録に使用できます。 たとえば、管理者がサーバの更新などの計画された操作のために事前に記録をスケジュールしたい場合です。
これを実現するために、Allegro ネットワーク マルチメータは、IP アドレスや MAC アドレス、リンク全体など、選択されたトラフィックの記録を開始します。 カレンダー アイコンを使用して、希望の開始時刻と終了時刻を選択できます。
(図 8)

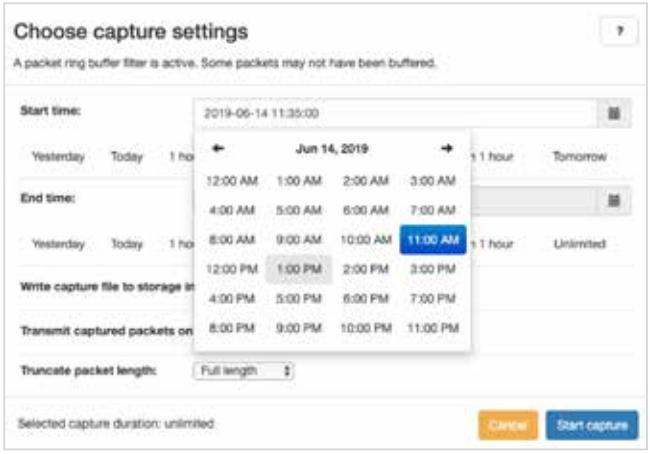

図 8: カレンダーによる予約記録の設定

キャプチャをハードディスクに直接書き込むことをお勧めします (図 9)。 高帯域幅のキャプチャを実行する場合は、ハード ディスクがリング バッファとファイルに 2 回書き込む必要がないように、キャプチャ中にリング バッファを無効にすることをお勧めします。

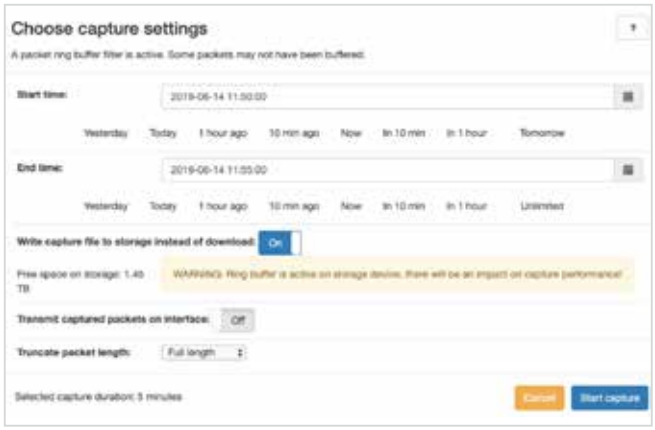

図 9: ハードディスクへの記録予約

キャプチャ機能はバックグラウンドで実行されるため、Allegro ネットワーク マルチメータの通常の測定および分析機能は影響を受けず、Allegro は引き続き正常に使用できます。
合計で最大 4 つの記録を同時に実行できます。

開発元：Allegro Packets GmbH
Leipzig | Germany
Phone +49 341 59 16 43 53
Email info@allegro-packets.com
Internet allegro-packets.com

Allegro ネットワーク マルチメータを使用すると、ネットワークのトラブルシューティングを迅速化できます。Allegro はネットワーク分析市場に革命をもたらす 史上初めての、モバイルデバイスで大量のパケットを分析できるようになりました。 この開発は、以前のソリューションの利点を組み合わせたデバッグ ツールを提供するという Allegro Packets の使命に基づいています。 その結果、ソフトウェアと同じく可搬型で、本格的なサーバと同じくらい強力なデバイスが誕生しました。

Allegro Packet社　国内総代理店
クオリティネットソリューションズ株式会社
東京都千代田区東神田２丁目４番６号　S-GATE秋葉原４F
Tel:03-5829-3671　E-mail:sales@qnetsolutins.co.jp
https://qnetsolutions.co.jp

お問合せ先