Myricom ARC ネットワーク アダプタ 機能

Sniffer10G
ファームウェアとソフトウェア

完全なパケットキャプチャ機能を安価に実現するパッケージ

Sniffer10Gは、CSPiのMyricom® ネットワークアダプタ ARCシリーズ向けのパケットキャプチャ機能です。不要な機能にかかるコストを省きながら、先進的なアプリケーションとネットワーク装置の製作を実現します。Sniffer10Gは、FPGAファームウェアとソフトウェアライブラリがバランス良く組合わされ、Sniffer10Gでのパケットキャプチャは、アプリケーションからの要求に応じて、 先進の機能を柔軟に利用できるように、設計されています。

完全なパケットキャプチャ

本アダプタは、3つの領域の機能を提供します。
(1) ゼロ損失、(2) 高精度タイムスタンプ、(3) パケットキャプチャ関わる重要機能です。

Sniffer10Gが、イサーネットパケットサイズの全範囲で、ゼロ損失の機能を維持することは、安全保障に関わる研究を行っている米国サンディア国立研究所(*)により、確認されています。カーネルバイパスを行い、"ring"の大きさを任意に変えて、パケットをユーザ空間へ直接送ることができ、パケットキャプチャのゼロ損失を確立しています。

また、Sniffer10Gは、パケットキャプチャとタイムスタンプをラインレートでサポートすることにより、ネットワークの要求に応えます。10GbEのラインあたりの最大可能速度は、14.8ミリオンパケット／秒です。また、タイムスタンプは、非常に高い精度で行います。ARCシリーズは、内部に水晶クロックを持ちます。高い精度を必要とするユーザには、GPS信号等の時計と接続することができます。

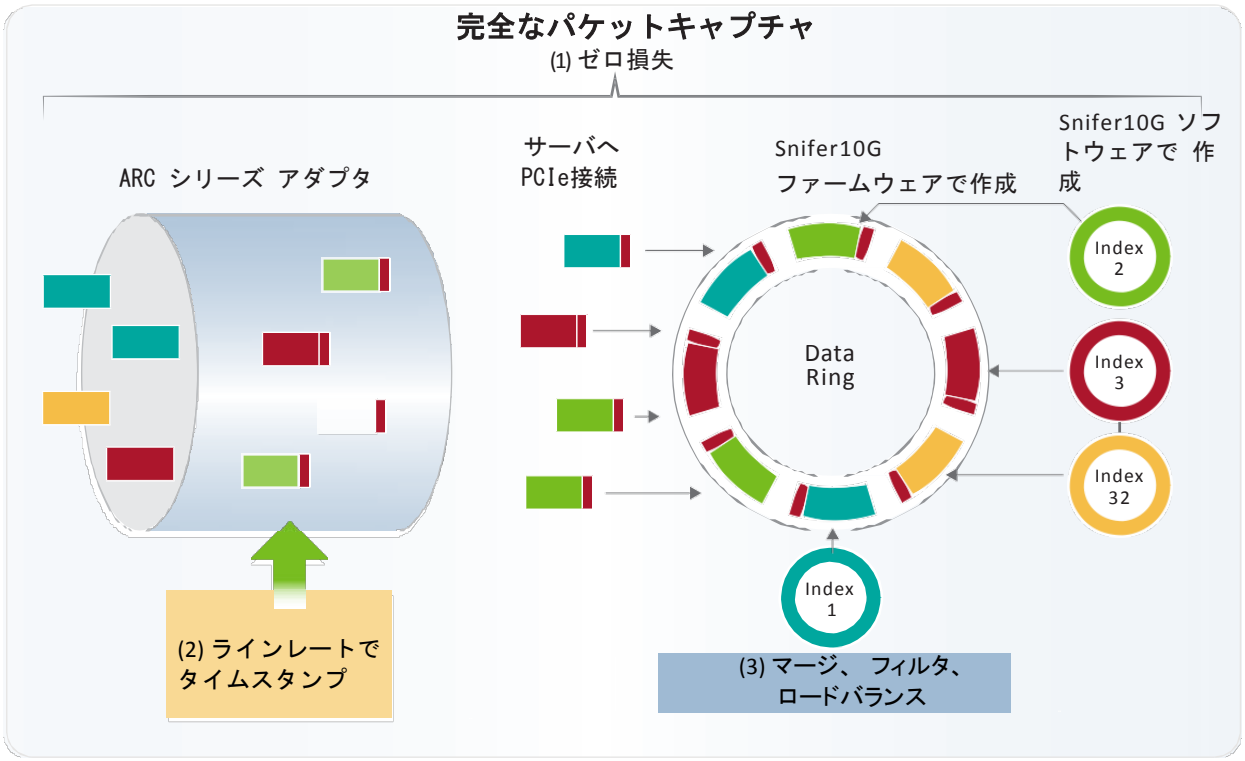
さらに、Sniffer10Gは、主たる機能であるパケットキャプチャのほか、重要機能として、その中で、時刻情報に基づく マージ、フィルタリング、ロードバランスを提供します。これらの機能は、Sniffer10G API、及び、業界標準ライブラリである libpcap、 WinPcap あるいは PF_RING を活用することができるので、アプリケーションレベルでコントロールできます。

*Comparing Ring-buffer-based Packet capture solutions :Report SAND2015-9378R, Steven Andrew Barker

CSPi
High Performance Products

Sniffer10Gは、Myricom ARCシリーズアダプタに、ゼロ損失のパケットキャプチャ、ラインレートでの高精度タイムスタンプ、アプリケーションへのサポートとして、時刻ベースのマージ、フィルタリング、ロードバランスといった機能を提供します。開発者は、Sniffer10Gのユニークな能力を使用して、データセットを、任意の領域で、32個迄の リングに、分割できます。PCAPをSniffer10Gで活用するには、対応するlibpcap または、 WinPcapのライブラリに、リンクを行います。このためユーザはアプリケーションの開発を効率良く進めることができます。Sniffer10Gは、 タイミング機能を拡張しており、オープンソースのパケットキャプチャアプリケーションを利用できます。Sniffer10Gのファームウェアとソフトウェアライブラリの組合せは、サーバの負担を抑え、機能と柔軟性を低価格で提供します。

図１－ 完全なパケットキャプチャ



マルチコア アプリケーションを柔軟にサポート

Sniffer10Gは、パーティショニングにより、CPUコア全てをパケット解析に使用させることができます。入力してくるTCPと UDPパケットフローは、複数のアプリケーションに、同時に、配信できます。この時、各アプリケーションは、一個以上の コアを制御しています。アダプタは、全てのアプリケーションが同じパケットを処理することを可能にし、各アプリケーショ ンが処理を終えた時のみ、パケットを開放するようにします。市販アダプタの中で独特ですが、あらゆるアプリケーションが、それぞれの特定のデータフロー パーティションニングスキームでサポートされます。

アプリケーション開発者は、前もって確立されたルールセットに従って、32個迄のリングにパケットをパーティションし たり、Sniffer10G APIにユーザ定義のルールを実装できます。APIにより、開発者は、アプリケーションでの、任意の入力トラフィックに基づくパーティショニングに関する要求にも、対応できるようになります。この機能により、複数のコアに またがり、各コアが同量の入力パケットを解析するといったフローのバランスをとることが出来ます。ディープパケットインスペクションを必要とするアプリケーションでは、パケット速度が高負荷となっている際には、切迫している処理時間を緩 めることができます。フィルタリングに関しては、バークレイパケットフィルタリング(BPF)言語を利用することができるので、開発の際に、フィルタが特定のセットに縛られることがありません。

CSPi
High Performance Products

入力トラフィックは、複数の手段でマルチコアに分割できます。例えば:

- スタンダードフローハッシング:Ethernet VLAN タグ、IP, UDP ヘッダー、 TCP ヘッダーに基づく、ユーザ選択可能なフローハッシング
- 移動体アプリケーションのためのGTPプロトコルハッシング
- カスタムハッシング:Sniffer10Gが持つ独自の能力であり、ソフトウェア定義のハッシングにより、開発者に対し選択的にパケットを送り出すことができます。

また、Sniffer10Gは、バーストバッファリングとトンネリングといった問題に対し、先進的な機能を提供します。アプリケーションからの操作で、最適化を行えるため、Sniffer10Gを備えたARCシリーズアダプタは、多くの方面で、良いソリューションを提供します。

低コスト、高機能、サーバへのインパクト軽減

ARCシリーズアダプタは、サーバの負担を抑えつつ、広範囲のアプリケーションに適用できるよう作られています。Sniffer10G APIから呼び出されるルーチンは、性能の最適化が施されており、OSの関与なしに、ユーザ空間から入力パケットにアクセスすることができます。コストを抑える設計を行うことにより、ハードとソフトにバランスのとれた機能を実現しています。ソフトウェアは、業界標準ライブラリ (libpcap, WinPcap 或は PF_RING) 又は、Sniffer10GのAPIを使用できます。ARCシリーズは、高機能でありながら、サーバにおけるオーバヘッドを抑制する、価格的にも優れたアダプタです。

PCAPユーザへ大きな利点　簡単実装

パケットキャプチャのアプリケーションは、 Sniffer10Gが用意しているライブラリにリンクを変更するだけで、libpcap と WinPcap を利用できるようになるため、ユーザは大変便利になります。すなわち:

- **CPU使用の削減** – Sniffer10G は、OSカーネルの介在なしに、すべてのパケットを、直接、アプリケーションに届けることにより、CPUサイクルを解放します。
- **取りこぼし無しのパケットキャプチャ** – Sniffer10Gでは、ユーザはリングサイズを定義できるため、アプ リケーションは任意のサイズのメモリキューを設定できます。この柔軟性により、ハードとソフトの間の速度の整合の問題でパケットを落とすことがありません。
- **並列するアプリケーション** – ひとつのパケットキャプチャ ストリームに対し、複数のlibpcapコ ピーをはしらせることができます。すなわち、バックグラウンドでゼロコピーで、同じパケットに対 し、同時に複数のアプリケーションをはしらせることができます。
- **正確なタイムステップ** – 高品質の時刻信号を同軸ケーブルから入力することにより、精度 ±0.5ナノセカンドで、タイムスタンプが行えます。
- **低オーバーヘッド** – Sniffer10Gは、パケットを落とすことなく、最大速度で、4ポートの10Gbit イサーネットを、1台のサーバーにキャプチャすることができる効率を持ちます。
- BPF – Sniffer10Gは、バークレイ パケット フィルタ 全機能をサポートします。

CSPi
High Performance Products

Sniffer10Gは、Linuxドライバーとともに、標準であるlibpcap と WinPcap ライブラリが使え、CSPi Myricomが行ったオープンソースの機能拡張を含みます。CSPi Myricomは、これらのモジュールを、ソース、及び、コンパイル版で提供し、Sniffer10Gとインターフェースをとっています。

用　途	最適ツール
記録装置	libpcap, WinPcap, PF_RING
組込解析装置	Sniffer10G API
試験装置	Sniffer10G API

業界標準ソフトウェアを豊富にサポート

Sniffer10Gでは、多くのオープンソースのパケットキャプチャツールがサポートされています。例として：

1. Linux ユーティリティ tcpdump
2. Wireshark ネットワークプロトコルアナライザー
3. Bro ネットワークイントルージョンディテクションシステム
4. Snort イントルージョンプリベンションシステム
5. Suricata ネットワークイントルージョンディテクション セキュリティ モニターリング
6. Sniffer10G APIでの利用のために移植したPF_RING™ パケットキャプチャネットワークソケット

Sniffer10Gソフトウェアで、これらのツールを使うためのマニュアルがあります。

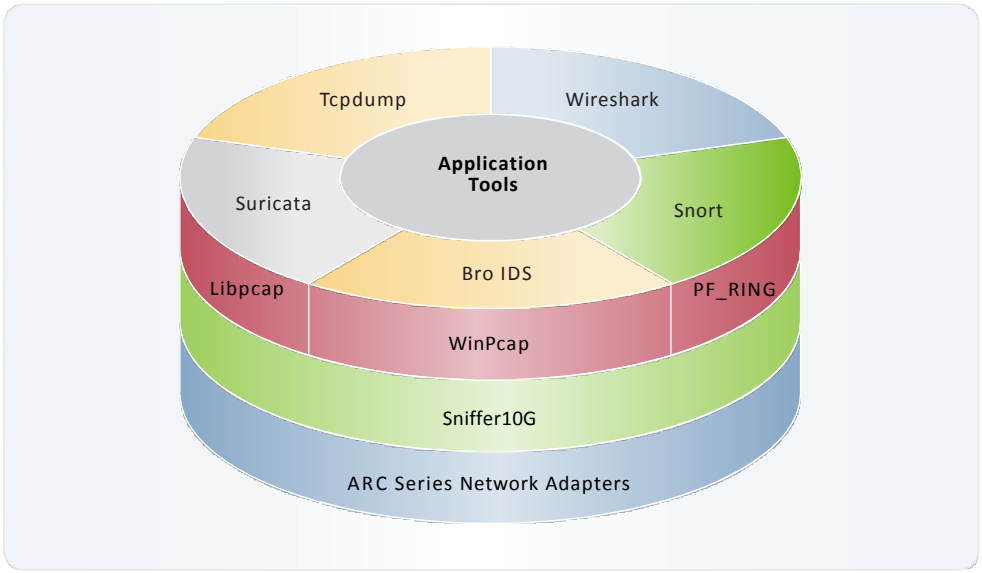


図2 – 業界標準パケットキャプチャ ソフトウェアをサポート

CSPi
High Performance Products

拡張されたタイミング機能

Sniffer10GとARCシリーズアダプタの組合せにより、先進のタイミング機能を提供可能にします。

- **タイミングの同期：** タイムスタンプの精度を拡張するために、外部オシロスレータ、または、GPSデバイスを接続して、PPSと10 MHzの接続が可能です。ARCアダプタには、±500ピコ秒の精度をサポートするように拡張されたバージョンがあります。
- **PPSと10 MHz デイジーチェーン：** アダプタの複数モジュールにわたる同調のほか、外部時間との同調に、使用します。デイジーチェーンは、構成が複雑な場合のアプリケーションにおいて、タイミング精度を拡張する簡単な手段です。
- **Aristaネットワーク DANZタイムスタンプのサポート：** Aristaスイッチを使用している場合、Sniffer10GソフトウェアはIPスタンダード独自拡張部分をデコードできるため、スイッチを通るパケットトラフィックフローにタイムスタンプを行うことができます。アプリケーションは、ネットワークアダプタに入った時刻ではなく、ローカルネットワークに入った時刻のパケットを使用できるようになります。

まとめ

Sniffer10Gは、Myricom ARCシリーズアダプタに、ゼロ損失のパケットキャプチャ、ラインレートでの高精度タイムスタンプ、アプリケーションへのサポートとして、時刻ベースのマージ、フィルタリング、ロードバランスといった機能を与えます。アプリケーション開発者は、Sniffer10Gのユニークな能力を使用して、任意の対象を基本に32個迄のリングにより、データフローを分割できます。

アプリケーション開発を合理化するため、PCAPユーザは、Sniffer10G 対応であるlibpcap または、WinPcapのライブラリに、リンクを変更することにより、Sniffer10Gを活用できます。Sniffer10Gは、タイミング機能の拡張を提供しているほか、オープンソースのパケットキャプチャアプリケーションをサポートしています。

Sniffer10Gのファームウェアとソフトウェアライブラリの組合せは、サーバへのインパクトを抑え、機能と柔軟性を低価格で提供します。

Myricom ARC ネットワーク アダプタ の評価、販売に関する問合せ先：

極東貿易株式会社
〒100-0004　東京都千代田区大手町2-2-1 新大手町ビル7F
TEL: 03-3244-3827 http://www.kbk.co.jp

CSPi
High Performance Products