Deep packet inspection (DPI) is a technique with many different use cases, delivering information about packet flows and content as well as allowing network operators and service providers to ensure quality of service at an application level. As more and more use cases are being implemented in the market, a common set of requirements has developed. These requirements have driven a set of architectures that deliver the level of performance, throughput and statistical data collection required to fulfill the respective task at hand.

This white paper will analyze use cases, define a set of common requirements for DPI applications and outline several architectures and building blocks that simplify the creation of scalable, reliable DPI appliances.
Deep packet inspection, or DPI, is a form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for defined criteria to decide what, if any, action should be taken by the network on that packet.

A classified packet may be redirected, marked/tagged, blocked, rate limited, or reported to a reporting agent in the network. Many DPI devices can identify packet flows (rather than packet-by-packet analysis), allowing control actions based on accumulated flow information.

Typical identification parameters include source and destination IP and ports. Some devices support far deeper inspection of packets to examine the meta data of protocols used and may use these for reporting and classification.

DPI enables a range of network services including network optimization, flow inspection, data flow management, security and application monitoring. These services may be called many things - such as user experience optimization, policy definition and enforcement, quality of service, tiered services, or lawful intercept, but can be fundamentally grouped into classes of application with similar requirements.

Use Cases
There are many different application models where DPI can be used to improve overall application usability and security.

Network Optimization
Network optimization deals with the fact that unmonitored and uncontrolled traffic flow through a network operator’s network can result in undesired interruption of service due to overload conditions at various places in the network.

This can be caused by peer-to-peer (P2P) traffic, distributed denial of service (DDoS) attacks and other events.

As a result, the undesired interruption of service can endanger customer loyalty by impairing the operator's quality of service (QoS). In order to avoid such events, operators use a variety of techniques that can all be summarized as DPI applications, and that can all be brought together in the deployment of a common kind of DPI system.

Flow Inspection
Flow inspection analyzes the network traffic based on flows (connection between a given client and a given server). This connection is analyzed and classified in order to align with carrier policies and requirements, thus allowing the carrier to monitor network usage by both application and total load.

This, in turn, enables network operators to review their policies and take appropriate steps to ensure data flow and network integrity.

Improved Data Flow
Deep packet inspection can also be used to optimize the data flow inside a network. Knowing which flows are dominant at what time of day (and what day), allows dynamic configuration of the network to the respective load factors, thus improving user experience.

This knowledge additionally allows network operators to throttle traffic that is not preferred at a given time, adding headroom to priority traffic.
Depending on the level of background information available in the operator’s network, this capability can be used to manage service levels.

Security and Application Monitoring
Finally, an area where DPI is used extensively is the intelligent application monitoring and security arena. DPI techniques can be used to understand and interpret network messages between web server, application server, and actual applications in high-load applications.

DPI can be adapted to find the right messages, analyze the content and remove malformed or malicious content that was injected in order to break into the application.

Similar techniques are applicable for security applications, where, in this case, the traffic is being monitored to protect the inside of the network, keeping out malicious content.

Another potential application is filtering content based on parameters such as parental controls for adult material.

DPI enables a deep understanding of the connections taking place and allows operators to apply policies to these.

Common Requirements for Use Cases
When reviewing the above use cases, it can be noted that there are several requirements that are common across the different use cases.

Some may be only partly applicable, while others are always applicable.

Transparency
The system being used to execute DPI applications should not be visible to the traffic passing through.

Terminology
Before starting to explain the requirements, definition of several terms that will be used going forward to ensure a common understanding and clarity of the following discussion is necessary.

Left/Right side
When discussing DPI applications, there is always a client (or internal) network side, and an external network, e.g. the Internet, which the packets pass through to reach the opposite side. The internal network normally is termed “left” side, and the open network will be called “right” side.

Packet Flow
A packet flow is the complete communication between an entity on the left side (example: an Internet browser on a PC) and an entity on the right side (example: a web server delivering the web page with dynamically generated content coming from a database).

Load Balancing
In the application of DPI, load balancing means distributing packet flows over multiple inspection devices, while ensuring that a given flow will always go to the same inspection device, thus allowing that device to analyze a complete conversation between entities rather than single packets.

Flow Fingerprints
Flow fingerprints are the characteristics used to identify applications and functions in a given conversation. Certain applications have certain behaviors in their communication that make them uniquely identifiable.

This means, assuming no action is taken, that all traffic and packages passing from left to right will not notice there is an inspection system in between.

That extends also to packets that would normally be used to configure networks, such as routing...
information protocol (RIP) and border gateway protocol (BGP) packets, even though there is frequently a switching device present inside the inspection system.

**High Throughput**
The inspection system must have enough bandwidth available so all traffic coming from left or right can be passed through, to avoid the inspection system being a bottleneck in itself, causing network congestion and - most undesirable - becoming visible as a function in the network as a result of that. This requirement has follow-on requirements such as high (enough) processing capability, low latency, high availability and scalability.

**High (Enough) Processing Capabilities**
Analyzing data connections based on single or multiple packets is not an easy function. If additionally, content needs to be analyzed in order to protect applications from injected malicious content, the performance requirements are very high. This, paired with the fact that application profiles typically are held in a large in-memory database, this calls for highest-end computing and high memory capacity in the system.

Splitting up connections (load balancing) across multiple entities as described above, eases this load to a level where real time processing becomes possible. Still massive compute capabilities together with enough memory for the in-memory database of fingerprints is required.

**Low Latency**
Low latency, so a minimal time loss inside the inspection device, is an important requirement. After all, first, the system should not be visible in the flow, and some connections such as VoIP are very susceptible to latency. Second, latencies add up, creating slowness in connections, and causing bad user experiences.

**High Availability**
An inspection device should be operational at any time in order to ensure complete coverage of what needs inspecting.

Additionally, these machines are inside a connection, so any unavailability causes unavailability of certain connections, which, in the worst case, can result in loss of revenues.

Users today expect 24x7x365 availability, and, in some countries, even have legal rights to this. In 2010, Finland was the first country to make broadband a legal right for every citizen. And in 2013, Germany's Federal Court of Justice stated that Internet connection is a modern necessity, on par with the right to mobility, such that people can sue their Internet providers for damages if connection is lost.

**Scalability**
DPI applications are monitoring internet traffic, which keeps growing with double-digit percentage rates all over the world. As a result, DPI devices must be able to easily adapt to these growing bandwidth requirements, preferably seamlessly.

This needs to be a given for many years to come, so an architecture is needed that allows gradual adjustments in line with the growing requirements.


**Solution Architectures**

From the previous discussions, it can be seen that a DPI device must fulfill a variety of functions that are best distributed over several functional units that best support the respective required function.

Additionally, it must be possible to route packet flows from left or right port to the same inspection unit, even for a large number of external connections.

In general the steps to take for DPI are as follows:

1) Identify packet source (physical link)

2) Execute pre-classification (optional, may be needed for very high bandwidth, very high port count environments)

3) Distribute evenly over classification units, with packets for the same flow going to the same classification unit for both directions.
   a) An additional function that may be implemented at this level is a health check function that goes beyond checking for physical presence of the DPI inspection units. This is typically achieved by adding special “check” packets to the packet flows and ensuring these packets flow through the entire inspection stack and appear again after processing in a reasonable time frame. If this is not the case, the respective inspection unit will be considered inoperable until a new check proves it is operational again. The goal here is to spot hung inspection applications early on and ensure appropriate reaction of the system.

4) Actual Deep Packet Inspection. This includes multiple functions and has some requirements for maximum performance as well as maximum insight into the packet flows.
   a) Internal forwarding of the flow inside the unit. This step ensures that always the same processing unit (frequently referred to as Logical Core, LCore; this may be an actual CPU core dependent on the CPU architecture) sees all packets comprising the flow, and that in both directions.
   
   b) Execute the actual processing. Extract as little data as needed to figure out whether a flow triggers the need for further inspection. If that is the case, continue processing, potentially set up forwarding to another, deeper-level inspection unit and execute the rules set up for this case.

5) Apply policies, if needed, for the given flow using the flow fingerprints, ensuring that the possibly modified packet returns to its original path as quickly as possible.

In a nutshell, behave like an active, slightly longer direct cable between left and right physical ports.

The above steps define the building blocks that should be used to compose the chain of steps needed, while ensuring all other requirements that were mentioned above are satisfied.

**General Architecture Review**

There are several bladed architectures available today that allow the building of appliances fulfilling the requirements laid out earlier in this whitepaper.

A particularly suitable architecture would however be AdvancedTCA® or ATCA®. ATCA has been designed to support an all-IP network running at very high bandwidth, while possessing all the additional capabilities required to support high availability.
Yet, the ATCA standard has been created in a way that does not require the use of these features from the outset, but allows them to be added over time as needed to build the application.

Hot swap support and built-in management features, together with scalability from very few to many blades make ATCA a perfect basis for DPI applications.

ATCA is built around an architecture that has two separate networks, Base (control plane) and Fabric (data plane). Today’s systems feature redundant switch blades and Fabric running at 40G, resulting in a total of 1.2Tbps aggregated bandwidth in the backplane, or 80Gbps per blade.

Hot swappable node blades and switches allow continued operation even in the case of hardware failures, as well as seamless in-operation insertion of additional blades, ensuring upgradeability of the system without interruption of service.

Due to the bladed design, very little cabling is required to connect a system.

A common requirement of all the systems is a very fast separation of traffic that needs further inspection from traffic which does not—in order to avoid overloading the inspection units. This also enables reduced latency both for all traffic flows.

Pre-Processing Stage (optional)
Due to the switched nature of the ATCA backplane architecture together with the large variety of available blades, an optional pre-processing stage can be introduced in the system by adding either an application-specific or general-purpose blade that supports the required function.

An example here could be the termination of tunnels that use a proprietary protocol, thus making the content of these available for inspection.

Another function might be pre-classification of certain traffic types, thus ensuring proper delegation to the correct inspection units in a later stage.

Switching and Load Balancing of Packet Flows
Switching – a cornerstone of the application architecture
On the switching side, only the fabric - high-bandwidth - part of a system is of interest for the application. Here, several requirements must be met. Today’s typical ATCA switch blades such as the Emerson Network Power ATCA-F140 feature
up to 160Gbps external connectivity, resulting in 320Gbps external connectivity in the case of a redundant configuration. Next-generation product will offer even more. Connectivity to a node slot today is 40Gbps.

This leaves enough headroom inside the system to allow processing and inspection blades to be able to forward traffic to deeper inspection stages if required.

The even distribution of front and rear ports allows the cascading of multiple chassis if more processing power is required to process the traffic coming through.

Load Balancing – FlowPilot ensures balanced system load and reliable flow distribution. Another core feature required for these applications is load balancing as an inherent function of the switch blade.

Emerson’s FlowPilot™ add-on package enables this functionality, using software and hardware capabilities of the 40G switch on the ATCA-F140. This ensures fast packet handling inside the system, with multiple configuration options to tailor the function of FlowPilot to the feature set actually required.

Emerson’s FlowPilot™ software offers load balancing as an inherent function of the ATCA-F140 40G ATCA switch blade.
More important, FlowPilot will distribute flows across a number of configured blades according to configured parameters, ensuring they remain constant over time, and the same inspection device receives the entire flow. Additional functions include health check on an application level and link transparency, connecting left side and right side cables to a virtual connection.

**Packet Processing and Inspection Units**

The actual processing of packets takes place in these units. These units need to look into the packet header to retrieve information of source and destination, understand the protocols and understand the different fingerprints of certain applications in order to handle these appropriately.

Additionally, en-and decryption functions must be implemented in these units as well. All functions must be executed at extremely high speed to ensure minimal latency, while guaranteeing maximal throughput.

Today, out of a large number of possible contenders, two architectures in particular have risen to prominence in the market:

- Intel®, using the Intel® Data Plane Development Kit (DPDK), which allows high-speed handling and processing of packets using standard x86 architecture
- Cavium OCTEON is a packet processing engine that has been designed specifically for handling high-throughput, deep inspection of packet streams

Emerson Network Power has created two blades that use these main architectures to support packet processing and inspection functions.

**ATCA-7470, 40G High Performance, x86 Packet Processing**

The ATCA-7470 is a 40G, dual 8-core Intel® Xeon® E5-2600 processor blade that due to its architecture is uniquely suited for packet processing functions taking advantage of the DPI support capabilities of the Intel® Communications Chipset 89x0.

The ATCA-7470 also allows the mounting of a mezzanine module featuring two more Intel Communications Chipset 8920, to take further advantage of the offload capabilities.

Each CPU is connected to one 40G Mellanox Connectix 3 Ethernet controller, allowing maximum throughput between controller and memory, and direct connection to a processing unit.

Additional 10G ports to the external world to add pre-processing capabilities can be added using an Rear Transitioning Module (RTM, a plug-in card that is connected to the rear of a blade inside the chassis to add interfaces and features) with 4-6 10G ports.

Using this blade allows for a flexible system architecture, as blades can be dynamically assigned to either packet processing or general purpose functions, which also has advantages on the provisioning side, just a single blade type is required, regardless of the intended function.
ATCA-9405, 40G High-Performance Dual Cavium OCTEON II-based Packet Processing

Based on two Cavium OCTEON II CPUs, the ATCA-9405 is purpose-built for packet processing functions in 40G ATCA systems, while expanding the number of cores massively for packet processing.

Existing software that has been created earlier for the Emerson’s ATCA-9305 or similar blades based on the Cavium OCTEON I processor can easily be ported, while also taking advantage not only of the far higher throughput but also extended processing capabilities due to the expanded number of cores available.

A market-leading RTM with massive 160Gbps external connectivity means this blade is also very well suited to serve as pre-processing stage in a DPI system.

Application-Ready Platforms

Emerson’s range of ATCA payload blades, including the ATCA-7470 and ATCA-9405 are optimized to work with the company’s range of Centellis™ ATCA system platforms which cover two-slot, six-slot and 14-slot variants that are designed to meet the need of both telecom central office and network data center environments.

Combined with Emerson’s 30+ years of system integration expertise, this portfolio enables equipment providers to develop and deploy DPI solutions faster, more cost effectively and with less risk. As the number one supplier of ATCA systems and blades*, Emerson Network Power has been a significant driver of innovation, performance and reliability in open standard telecom computing platforms.

Software Solutions

All these packet processing functions require support through software packages that make life easier in developing software for DPI.

Intel’s Data Plane Development Kit (DPDK) and Cavium’s Development Kit both offer starting points when developing new DPI applications.

The Intel DPDK offers a revolutionary approach to processing packets on x86 architecture at high speed, thus enabling a flexible design of applications as well as deployment phase flexibility with respect to which board gets assigned which tasks.

Cavium and the Cavium Development Kit for Octeon II offer a development environment that is specifically suited for the Cavium OCTEON II CPUs and their capabilities, allowing a detailed configuration to the required functionality utilizing the OCTEON II’s capabilities.

Emerson offers Board Support Packages for both of these software packages that enable direct configuration and application porting to the respective platform.

Both products are supported by external software packages that enable developers to get results faster on the respective platform, such as:

Qosmos’ protocol matching ixEngine: a Software Development Kit (SDK) composed of software libraries and tools that are easily integrated into new or existing solutions. Developers benefit from IP flow parsing technology to accelerate the delivery of application aware solutions.

Sensory Networks’ Hyperscan pattern matching libraries: a pattern matching engine that can match large groups of regular expressions against blocks or streams of data, ideal for applications that need to scan large amounts of data at high speed.

These software packages are augmented by:

- Wind River’s Intelligent Network Platform (INP): an integrated embedded software system that serves as a run-time foundation for network elements of all kinds. The platform integrates the key software components needed to design high-performance, intelligent network applications in a consolidated management and data plane system.

- Or Cavium’s TurboDPI package: a network-based multi-functional platform that helps OEMs and ODMs rapidly develop deep packet inspection (DPI) applications.

Emerson Network Power has partnered with these companies to give developers a choice, while taking advantage of the peace-of-mind of knowing that these packages have been validated and are known to work on the hardware platform they choose for their application.

**Summary**

There is no such thing as a definitive architecture for all DPI applications.

There are multiple building blocks, consisting of both software and hardware, which enable developers to create solutions that not only support their specific approach to solving the problem of packet inspection, but that also enable developers to take advantage of a pre-validated platform, thus de-risking this large project.

DPI remains at the core of development focus in the networking world, as it is being used for a variety of high-level applications that enable network operators to manage the traffic passing through their networks, so they can ensure optimal performance and service levels of the traffic present at any given time.

Emerson Network Power has developed building blocks, application-ready systems and integration expertise to support both developers and network operators in meeting their requirements, today and in the future. Please contact your local Embedded Computing sales representative or technical personnel for in-depth discussions.
About Emerson Network Power

Emerson Network Power is a business of Emerson (NYSE:EMR) and, through its Embedded Computing & Power business, is the trusted partner for scalable embedded computing technology and power supplies for the aerospace, defense, computing, healthcare, industrial and telecom markets.

The Embedded Computing business of Emerson Network Power enables original equipment manufacturers and systems integrators to develop better products quickly, cost effectively and with less risk. Emerson is a recognized leading provider of embedded computing solutions ranging from application-ready platforms, embedded computers, enclosures, motherboards, blades and modules to enabling software and professional services.

Emerson’s engineering and technical support is backed by world-class manufacturing that can significantly reduce time-to-market and help OEMs gain a clear competitive edge.

Let Emerson help your business improve time-to-market and shift development efforts to the deployment of new, value-add features and services that build market share.

Emerson, Emerson, Consider It Solved, Emerson Network Power, Centellis, and FlowPilot are trademarks of Emerson Electric Co. or one of its affiliated companies. AdvancedTCA and ATCA are registered trademarks of the PCI Industrial Computer Manufacturers Group. All other trademarks are the property of their respective owners. ©2013 Emerson Electric Co.

While every precaution has been taken to ensure accuracy and completeness in this literature, Emerson Network Power assumes no responsibility, and disclaims all liability for damages resulting from use of this information or for any errors or omissions.

EmersonNetworkPower.com

Emerson Network Power.

- AC Power
- Connectivity
- DC Power
- Embedded Computing
- Embedded Power
- Industrial Power
- Infrastructure Management & Monitoring
- Outside Plant
- Power Switching & Controls
- Precision Cooling
- Racks & Integrated Cabinets
- Services