

# Next Generation Deep Packet Inspection: An Overview of Requirements and Applications



**Network Strategy Partners, LLC**

MANAGEMENT CONSULTANTS TO THE NETWORKING INDUSTRY

[www.nspllc.com](http://www.nspllc.com)

**March, 2007**

**Network Strategy Partners, LLC (NSP)** — Management Consultants to the networking industry — help service providers, enterprises, and equipment vendors around the globe make strategic decisions, mitigate risk and affect change through custom consulting engagements. NSP's consulting includes business case and ROI analysis, go-to-market strategies, development of new service offers, pricing and bundling, as well as infrastructure consulting. NSP's consultants are respected thought-leaders in the networking industry and influence its direction through confidential engagements for industry leaders and through public appearances, whitepapers, and trade magazine articles. Contact NSP at [www.nspllc.com](http://www.nspllc.com).

---

## TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>1</b>
<b>KEY BUSINESS DRIVERS FOR DPI.....</b>	<b>2</b>
Maximize Service Revenue and Profitability .....	2
Minimize Negative Impact to the Network.....	3
<b>THE PROBLEM WITH L2/L3 NETWORK TECHNOLOGY.....</b>	<b>4</b>
<b>WHAT IS DPI?.....</b>	<b>4</b>
<b>TECHNICAL REQUIREMENTS FOR ADVANCED DPI PRODUCTS.....</b>	<b>6</b>
DPI Baseline Requirements .....	6
DPI Premium Requirements .....	7
DPI Service Provider Requirements.....	8
DPI System Security Requirements .....	9
Requirements Summary .....	10
<b>EXAMPLES OF DPI NETWORK APPLICATIONS .....</b>	<b>10</b>
DNS DDOS Attack .....	10
VoIP Lawful Intercept .....	11
Internet VoD Service.....	11
<b>SUMMARY .....</b>	<b>12</b>
<b>ADVANCED DPI REQUIREMENTS REFERENCE TABLE.....</b>	<b>1</b>

## Introduction

The convergence of traditional network services to a common IP infrastructure has resulted in a major paradigm shift for many service providers. IP networks were originally used to carry best effort Internet traffic, however, today many service provider IP networks carry core network services including Internet, Voice over IP (VoIP), Broadcast TV (IPTV), and Video-on-Demand (VoD). IP convergence has resulted in both business opportunities and challenges for service providers.

A recent Oracle-sponsored global communications industry survey conducted by Economist Intelligence Unit, reported that over 80 percent of industry executives believe voice calls will significantly decline and will no longer be the major revenue source for communication carriers within six years. In addition, 60 percent of senior executives predict that this transition will happen faster, within four years. According to 75 percent of executives surveyed the best strategy for service providers to negate declining voice calls is to introduce new services. In other words, service providers must successfully offer new services or perish.

The development of new IP services and applications has led to a new set of traffic management problems for service providers. In order to address these problems, first generation Deep Packet Inspection (DPI) products have been installed in networks. These products typically solve problems such as Peer-to-Peer (P2P) traffic management. While first generation DPI products are adept at managing P2P traffic, which is an urgent problem for service providers, they are not always capable of solving new problems or facilitating new services. A one-problem, one-box approach to DPI leads to deployment of armies of appliances which is not a viable long term strategy. As a result a second generation of DPI products has emerged to solve a broader set of problems. Designed as multi-purpose L2-L7 traffic management systems, these products can mitigate current and future security threats, manage traffic from specific subscribers and applications, and craft new IP services. This ‘Advanced DPI’ employs comprehensive and broad-based traffic management and security capabilities to solve current and future problems, plus these products operate at 10 Gbps<sup>1</sup>.

DPI functionality is a critical component of converged services IP networks. The objective of this paper is to help service providers define business drivers for DPI and outline the requirements for next generation DPI products. More specifically the paper addresses the following questions:

- *What is DPI and the different flavors of DPI in the market place?*
- *Why should service providers care about DPI and what are the business drivers?*
- *What fundamental network problems are service providers trying to solve with DPI?*

---

<sup>1</sup> Service Provider aggregation networks for triple play and commercial Ethernet services are migrating to 10 GbE line speeds.

- *How should DPI be implemented in the network and what are the important capabilities of DPI products?*
- *What are service provider requirements for Advanced DPI products?*
- *What are some examples of Advanced DPI applications?*

## Key Business Drivers for DPI

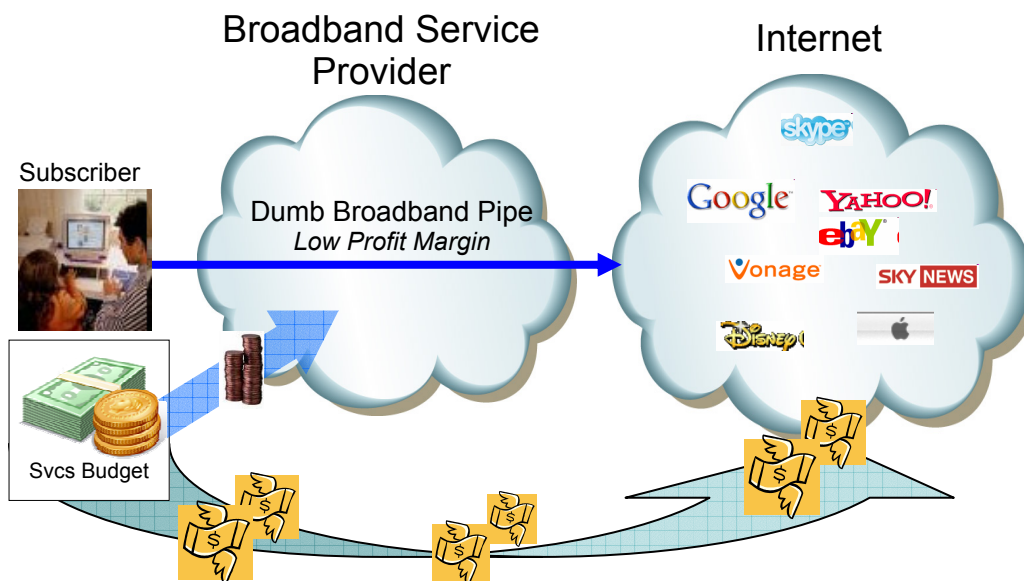
Most service providers use DPI technology to solve two fundamental business problems:

- Maximize Service Revenue and Profitability (Positive Cash Flow)
- Minimize negative impact to the network due to rogue applications or attacks (Negative Cash Flow)

The following subsections address these two fundamental business drivers.

### Maximize Service Revenue and Profitability

Many broadband networks use L2/L3 technologies, which have limited service control capabilities. As a result, broadband network service providers are at risk of losing a significant percentage of their subscribers' service budgets to other emerging service providers. For example, if a service provider sells a "dumb broadband pipe" at a commodity price, it is likely that subscribers will buy higher margin services (such as VoIP, IPTV, VoD, Email, online gaming, and other emerging services) from other Internet content service providers, as shown in Figure 1. This is a serious problem for network service providers that have made significant investments in their broadband infrastructure and don't want to see revenues funneled away to Internet-based content providers.



*Larger percentages of subscribers' budgets going to Internet Content*

**Figure 1**

## Subscriber Loss of Revenue with a “Dumb Broadband Pipe” L2/L3 network

The solution is a “smart broadband pipe,” which offers service providers visibility into how subscribers and applications use the network, thus allowing them to implement service monitoring and control, and to participate in the service value chain. A *service aware* network infrastructure enables high margin service offerings such as high speed gaming, bandwidth-on-demand, and Internet VoD services. Figure 2 depicts the “smart broadband pipe” service infrastructure. Advanced DPI affords network operators complete visibility of network applications, flexible traffic control, and the economies of one device-many applications to convert “dumb broadband pipes” into a *service aware* network. By using a “smart broadband pipe” enabled by Advanced DPI, service providers can efficiently deliver high margin services and partner with content providers to retain a larger percentage of the subscriber’s service budget.

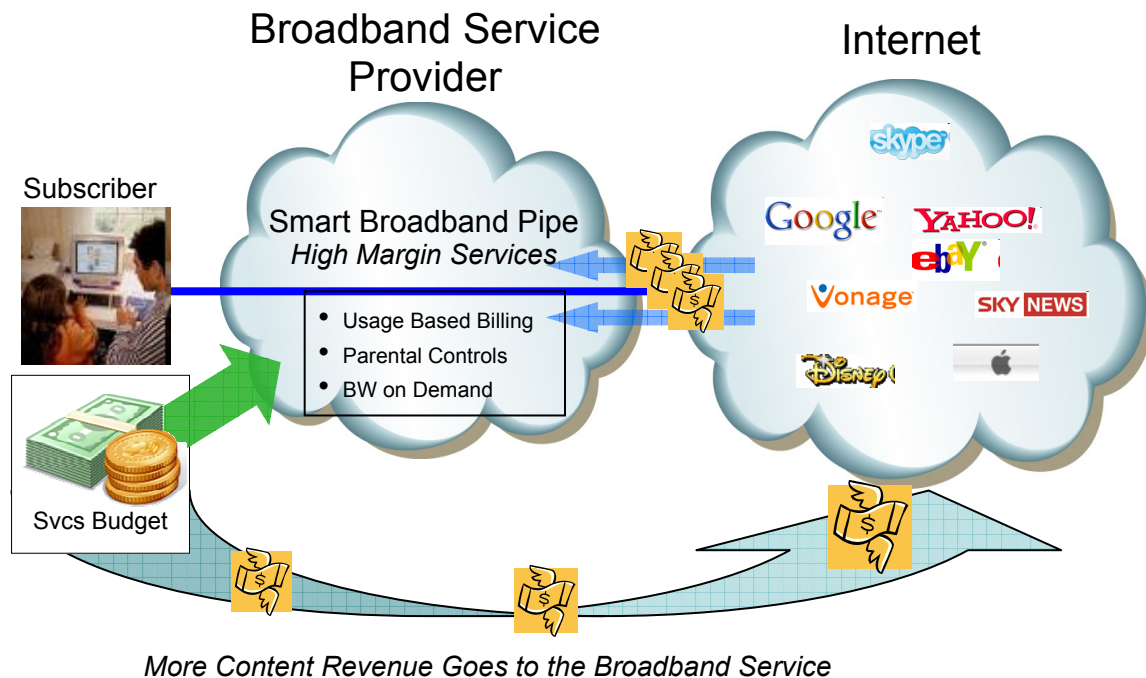


Figure 2

## Broadband Service Provider with “Smart Broadband Pipe” and Retail Services Infrastructure

### Minimize Negative Impact to the Network

Minimizing negative impact to the network due to rogue applications or attacks is the second fundamental business driver for DPI. Because IP networks have become critical components of network infrastructure, outages and/or performance problems due to rogue applications and network attacks contain serious financial implications. Unlike discrete service networks, each service in a unified network is subject to all the ills of the other services.

For example, Peer-to-Peer (P2P) traffic generated by users sharing music and video files generates large amounts of traffic with random distribution patterns. Such traffic can disrupt network performance and necessitate unplanned increases in network capacity. While most P2P traffic is generated by customers with good intentions, another class of traffic is created by hackers with the express intention of disrupting network services and performance: for example DDOS attacks, worm propagation, VoIP service hijacking, toll fraud, credit card fraud, etc. These attacks come in multiple forms and, as defenses are created for known attacks, persistent adversaries continue to develop new attacks. DPI technology can protect the network from rogue applications, such as P2P, and deliberate attacks, by monitoring, identifying, and throttling traffic at all layers of the Open Systems Interconnect (OSI) model.

## **The Problem with L2/L3 Network Technology**

IP networks are primarily built with L2/L3 switching and routing technology. The fundamental elegance of the layered network architecture and the IP protocol suite has allowed the Internet to scale to an unimaginable size. However, the layered model can also hide the details of the higher layers of the protocol stack from the network infrastructure, effectively rendering it ‘content blind’. While this simplifies network design and implementation, it causes big problems for service providers trying to manage and control network traffic at the applications layer.

L2/L3 switches and routers have extremely limited visibility into the application layer. For example, all web traffic is classified as a single application using TCP port 80. Given that most new Internet services are web based, L2/L3 switches have virtually no visibility into the service layer. While they can determine source and destination IP addresses and TCP ports, they cannot determine the nature of the application, the user, the content downloaded from a web site, or other aspects of the higher layer protocols and applications. As another example, new SIP-based services transact in layer 7 and use a text based protocol. An L2/L3 network has no SIP awareness. Therefore, an L2/L3 IP network is a “dumb broadband pipe” which makes it difficult for service providers to maximize revenue with premium services or minimize negative impact on the network due to rogue applications and attacks.

## **What is DPI?**

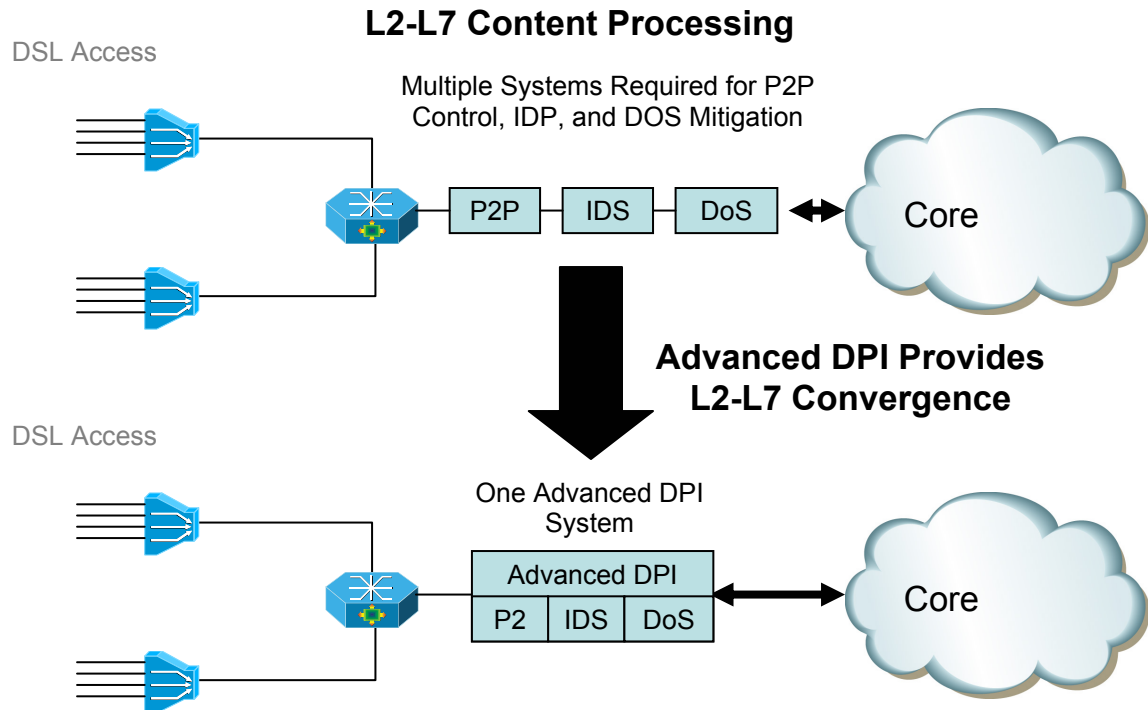
Today, a wide variety of products are used in networks to control traffic based on content. These products operate on information contained at all levels of the protocol stack with a heavy focus on the application layer. The primary current application of DPI is control of P2P traffic. As P2P has grown in popularity for MP3 and other file sharing protocols, service providers found that network traffic was not following the traditional routes used in their network engineering plans. P2P also creates a large magnitude of traffic requiring expensive upgrades to network infrastructure. First generation DPI was one of the solutions to address this problem. By monitoring and throttling P2P traffic, expensive network upgrades are avoided and fair network service is provided to all subscribers.

In conjunction with the P2P problems, service providers typically deploy Intrusion Detection and Prevention systems, IDS & IPS, to mitigate the threat of various network attacks. These systems also operate at all layers of the protocol stack, but focus on detecting and preventing intrusions from hackers, worms, and viruses.

First generation DPI and IDP products focus on solving specific and important problems and have been widely deployed in networks as a result. However, the nature of application services and threats from intelligent adversaries is such that the capabilities of layer 2-7 content processing products must constantly change to address new needs. The current approach to solving this problem is deploying additional L2-L7 point products into the network. Clearly this is not an efficient long term solution to the problem of managing changing requirements. Because of this, a new generation of DPI technology has emerged with increased content and application processing capabilities designed to perform a wide range of functions, and execute several applications simultaneously. By deploying Advanced DPI with broad, line-speed content processing capabilities, service providers avoid deploying multiple point products for every problem, as shown in Figure 3. This leads to reductions in both CAPEX and OPEX, including reduced expenses in the following areas:

- Engineering, installation, and wiring
- Network care (provisioning, surveillance, monitoring, capacity planning, data collection, maintenance, and fault isolation)
- Network upgrades and patches
- Training
- Sparing
- Service contracts
- Environmental expenses (floor space, power, and cooling)

The processing capacity of Advanced DPI devices afford network operators leverage for their DPI investment, while the functional flexibility and easy repurposing capabilities promises protection of that investment against future needs and threats.



**Figure 3**  
**Convergence using Advanced DPI**

The next section of this paper specifies the technical requirements for Advanced DPI products with general content processing capability.

## Technical Requirements for Advanced DPI Products

DPI convergence makes good business sense; however, it is a complex problem requiring robust and flexible content processing technologies. This section outlines *key requirements* enabling a DPI product offering to fulfill this role.

### *DPI Baseline Requirements*

DPI baseline requirements are table stakes for any vendor to play in the DPI game. These are necessary conditions but not sufficient for deployment in a service provider network. The DPI baseline requirements are presented below.

#### **Scan Packet Payloads at all layers (L2-L7)**

In order to monitor and control traffic without limitation, it is necessary to scan packets from the first bit to the last. Only this way can you ensure all layers of the protocol stack are addressed. In fact, this is the definition of *Deep Packet Inspection*.

For maximum applicability, payload scanning capabilities should include application content and transactions that traverse multiple packets. When appropriate, DPI products must be able to reassemble content before scanning.

#### **Application Classification, Measurement, and Reporting**

DPI products must have the ability to classify applications, measure throughput, and create application traffic reports. This provides network managers with the visibility essential for strategic traffic planning, tiered broadband access, and usage based billing.

#### **Set Policies for Prioritization, Blocking, or Shaping**

Based on packet payload scans, application classification, and a set of policies for managing traffic, DPI products must prioritize, block, or rate limit traffic. This function provides one of the fundamental controls that used for offering tiered services and for controlling problem applications such as P2P.

#### **Session vs. Packet Identification**

One of the premium requirements for Advanced DPI is session identification and state change tracking. Moreover, Advanced DPI products must be able to analyze session behavior along with packet behavior. This is important because many applications or attacks can *only* be analyzed in the context of a session.

### ***DPI Premium Requirements***

While the DPI baseline requirements are table stakes, DPI premium requirements are necessary to create flexibility for handling both current and future problems and providing flexible service control. DPI premium requirements are the key to DPI equipment convergence resulting in capital and operating cost savings.

#### **Modification of the Packet Envelope**

DPI engines must be capable of modifying packet envelopes in order to implement new services and prevent attacks. This capability must be configurable, programmable, and sufficiently granular to allow maximum flexibility in packet processing. Packet envelope modification examples include:

- Modify routing information in support of content-based routing policies
- Expand the packet length to add VLAN/MPLS tags/labels
- Contract packet length to enable removal of tunnel labels
- Support multiple layers of labeling/tagging as needed

As Carrier Ethernet and MPLS networks become more prevalent in service provider networks the ability to modify packet envelopes becomes more critical.

### **Modification of Packet Payload Content**

In addition to modifying the packet envelope, DPI engines must be capable of modifying payload content. Based on dynamic packet and session monitoring, DPI packet content modification can carry out functions such as:

- Removing viruses
- Transforming content to support gateway functions (e.g. IPv4-to-v6)
- Enforcing network use policy (e.g., no high bandwidth Codecs, or IPv6 only)
- Solving problems related to the rapid pace of change in service protocols (e.g., SIP)
- Addressing future unknown problems

Sometimes problems can only be resolved by modifying packet content.

### **Generating Packets**

In some instances, the preferred method for securing services infrastructure or providing gateway functions requires the generation of packets. A premium DPI requirement is the ability to build a packet with all the appropriate content and envelope information to be injected into the network. Example uses of packet generation include:

- Building a protocol or application proxy
- Gracefully resetting a TCP session from an unwanted host
- In-band signaling between network infrastructure (e.g. DPI device-to-DPI device)

### **Adaptable Functionality**

Future services and threats are unknown and potentially *more complex* than current services and threats. Therefore, it is essential that algorithms in next generation DPI systems that analyze the content and behavior of packets in a session and take appropriate action based on that behavior and content are adaptable. Moreover, this function ‘adaptability’ should be accessible directly by network operators and their solutions partners. This creates the flexibility necessary for quickly crafting new service offerings and the ability to defend the network against new attacks.

## ***DPI Service Provider Requirements***

Next generation DPI products need to meet specific requirements for deployment onto service provider networks. These requirements are specified below.

### **Support Common Service Provider Network Interfaces**

In order to achieve effective integration of DPI products, it is necessary that DPI products support a full suite of network interfaces. More specifically, the product should support:

- SONET and SDH Interfaces
- Ethernet Interfaces (100/1000 Mbps and 10 Gbps Ethernet)

By supporting a full suite of service provider interfaces, DPI products can be placed in any part of the network<sup>2</sup>. For example, it might be most convenient to place the DPI system between a router and a SONET ADM using an OC-48 interface. If the DPI product does not support OC-48, then additional network equipment will be needed to support this configuration. This not only adds to CAPEX, but also increases operational complexity and reduces network reliability.

### **All DPI Functions Must Operate at Line Speed**

In order to scale networks effectively it is necessary that *all DPI functionality* specified in the previous sections scale to full line speed.

### **DPI Equipment Must Support Common Protocols in Service Provider Networks**

Many service provider networks use a variety of protocols that are not always present in enterprise networks. Protocol examples include:

- VLANs
- Q-in-Q (VLAN Tag stacking)
- MPLS
- Packet over SONET
- Packet over SDH
- IPv6

Effective integration into service provider networks requires support of service provider protocols.

### ***DPI System Security Requirements***

Because DPI systems are essential to network security, it is critical that Advanced DPI products themselves are completely secure. All DPI devices must protect themselves from attacks. The following DPI security requirements provide a strong foundation to achieve this objective.

- DPI systems must operate in *stealth mode* such that they are not visible in the network
- The DPI device management plane and data path must be separated by design, with only a tightly controlled, protected interface between them
- All DPI provisioning should be done *out-of-band*
- DPI products should have *security accreditations*

---

<sup>2</sup> It should be noted that many DPI products only support Ethernet interfaces. Therefore if they need to be placed in an area of the network that uses SONET or SDH interfaces a router must be inserted to translate SONET/SDH to Ethernet. This incurs additional capital and operation expenses.

## Requirements Summary

Advanced DPI products must satisfy the broad set of requirements, that have been defined above. To recap, the requirement sections include

- *DPI Baseline Requirements*
- *DPI Premium Requirements*
- *DPI Service Provider Requirements*
- *DPI Security Requirements*

DPI products that meet these requirements are candidates for providing the framework for service control and security in next generation service provider networks. Advanced DPI requirements are essential for service providers striving to meet the business objectives to maximize service revenue and profitability and minimize the negative impact to the network infrastructure. The table in Appendix A summarizes these requirements and could be used as the basis for DPI vendor evaluations or within an RFP.

## Examples of DPI Network Applications

The following examples show how Advanced DPI content controllers are used in service provider networks to *create new service revenue* and *minimize negative impact* to the network due to rogue applications or attacks.

### *DNS DDOS Attack*

The following real life example outlines a Distributed Denial of Service (DDoS) attack on a DNS service providing a free DNS service provider to some 100,000 domains. This service provider was overwhelmed by DNS queries in a DDoS attack. In order to respond to the attack, they first used filters in the routers to reject some of the DNS queries. While this initially helped reduce the traffic load, the attack increased in magnitude, which overwhelmed the router filters and slowed router throughput to a crawl. The result was that thousands of web sites were unreachable.

Fortunately, DPI solved the problem. The service provider deployed an Advanced DPI product with the ability to monitor protocols, packet content, and implement custom algorithms. In several hours, a custom algorithm was written and deployed that inspected all incoming DNS requests for validity and dropped the invalid requests. Afterward, although 900 Mbps of total DNS requests were coming into the Advanced DPI engine, only 2 Mbps of the DNS requests proved to be valid, and were forwarded to the DNS servers. The DNS server infrastructure could easily manage the reduced query load.

The benefit of this approach is that a common DPI device is deployed at multiple locations, meaning fewer appliance variants in the network. At this point, instead of sparing for each separate device, the service provider only needed to authorize a single device for deployment, develop one set of administration and management procedures, train operators on just one system, and inventory spares for the overall set of devices.

Moreover, with software-driven functionality additional features can be added easily to keep pace with changing needs.

### ***VoIP Lawful Intercept***

Lawful intercept is one of the legacy requirements for voice service. In legacy Time Division Multiplexing (TDM) networks lawful intercept was achieved using wire taps. Voice-over-IP (VoIP) networks create new challenges for lawful intercept. In order to tap a phone call it is necessary to identify a VoIP session in a high-speed packet stream, copy the VoIP packets, and send them to the lawful intercept monitoring point. In VoIP networks this process is further complicated by the fact that the signaling messages (SIP) can follow a different path in the network than the voice content (RTP). This functionality means that a DPI product must identify the session and redirect the RTP stream to a lawful intercept point where the content of the VoIP stream can be copied and recorded.

Advanced DPI capabilities are necessary for lawful intercept. It is impossible to implement this service with traditional L2/L3 routers.

### ***Internet VoD Service***

Video-on-Demand (VoD) is projected to be a popular network service. Today it is possible to get VoD over the Internet from content providers such as Movie Links and Cinema Now. In the near future larger content providers (such as Yahoo and Google) will offer Internet VoD service creating a significant business challenge for broadband network service providers: if users buy VoD from content providers, broadband service providers will be relegated to the lower margin transport business. VoD content providers are also faced with another business challenge: their VoD customers *must* have adequate network bandwidth to achieve a high quality user experience. DPI provides a solution to *both* of these problems.

If the broadband service provider uses DPI to offer a premium Internet VoD service, then customers subscribing to this premium service will be allocated *higher bandwidth* when they view VoDs. This will create additional high margin revenue for the broadband service provider and will create a much better quality of experience for the VoD customer, thus solving both business challenges.

There could be multiple ways to implement this service. One possible method is to specify all web sites offering VoD service and inspect HTTP URLs to determine if the user is accessing a VoD web site. This method requires a significant amount of maintenance and could have scalability problems as the number of VoD sites grow. Another method would be to inspect the content of the session to determine if the content is VoD and then allocate bandwidth based on that inspection. As the nature of VoD and the number of VoD service providers increase, it is vital that the DPI system have the flexibility to use different approaches to implementing this service.

## Summary

The telecommunications world is rapidly changing. Competitive VoIP services from Skype and others are threatening to diminish traditional voice revenues for established service providers. In order to survive and grow in this new world, service providers need to be offer new services and create partnerships with internet content providers, such as Yahoo and Google. At the same time, it is essential that service providers minimize the negative impact on their network from either new P2P applications or coordinated attacks.

This paper has shown that Advanced DPI technology is key to achieving both business objectives. Advanced DPI gives service providers the flexibility to tune their networks and offer new services in alignment with market drivers. Additionally, it provides the agility and flexibility necessary to protect the network from threats today and tomorrow. By being configurable, programmable, and flexible, Advanced DPI technology provides solutions for multiple problems in the network and reduces the number of appliances required for standard and special purpose network applications, which reduces both capital and operating expenses.

## Advanced DPI Requirements Reference Table

Baseline	Availability	Vendor Response
L2-L7 Packet Scan <ul style="list-style-type: none"> <li>– Visibility from 1st bit, to last</li> <li>– Reassemble content before scanning</li> </ul>		
Application Classification, Measurement, & Reporting		
Policies for Prioritization, Blocking or Shaping Traffic <ul style="list-style-type: none"> <li>– On aggregate or sub-specific traffic</li> <li>– No unprocessed packets on policy updates</li> </ul>		
Session & Packet-level Identification		
<b>Premium</b>		
Modification of Packet Envelope		
Modification of Packet Content		
New Packet Generation		
Adaptable Functionality <ul style="list-style-type: none"> <li>– End-user accessible</li> <li>– No unprocessed packets on updates</li> </ul>		
<b>Service Provider Requirements</b>		
Broad Interface Support		
Line-Speed Operation		
Comprehensive Protocol Support		
<b>Security</b>		
Stealth Mode Operations		
Data Path Interfaces not Accessible		
All DPI Provisioning Out-of-Band		
Security Accreditation		