**How Deep Packet Inspection Works**

Deep packet inspection is a form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems Interconnection's application layer.

Deep packet inspection [evaluates the contents](https://cis-india.org/internet-governance/blog/deep-packet-inspection-how-it-works-and-its-impact-on-privacy) of a packet that is going through a checkpoint. Using rules that are assigned by you, your Internet service provider, or the network or systems administrator, deep packet inspection determines what to do with these packets in real time.

Deep packet inspection is able to check the contents of these packets and then figure out where it came from, such as the service or application that sent it. In addition, it can work with filters in order to find and redirect network traffic from an online service, such as Twitter or Facebook, or from a particular IP address.

**Deep Packet Inspection vs. Conventional Packet Filtering**

Conventional packet filtering only reads the header information of each packet. This was a basic approach that was less sophisticated than the modern approach to packet filtering largely due to the technology limitations at the time. Firewalls had very little processing power, and it was not enough to handle large volumes of packets. In other words, conventional packet filtering was similar to reading the title of a book, without awareness or evaluation of the content inside the cover.

With the advent of new technologies, deep packet inspection became feasible. As it became more thorough and complete, it became more comparable to picking up a book, cracking it open, and reading it from cover to cover.

**Use Cases for Deep Packet Inspection**

There are several uses for deep packet inspection. It can act as both an intrusion detection system or a combination of intrusion prevention and intrusion detection. It can identify specific attacks that your firewall, intrusion prevention, and intrusion detection systems cannot adequately detect.

If your organization has users who are using their laptops for work, then deep packet inspection is vital in preventing worms, spyware, and viruses from getting into your corporate network. Furthermore, using deep packet inspection is based on rules and policies defined by you, allowing your network to detect if there are prohibited uses of approved applications.

Deep packet inspection is also used by network managers to help ease the flow of network traffic. For instance, if you have a high priority message, you can use deep packet inspection to enable high-priority information to pass through immediately, ahead of other lower priority messages. You can also prioritize packets that are mission-critical, ahead of ordinary browsing packets. If you have problems with peer-to-peer downloads, you can use deep packet inspection to throttle or slow down the rate of data transfer. DPI can also be used to enhance the capabilities of ISPs to prevent the exploitation of IoT devices in DDOS attacks by [blocking malicious requests](http://blog.catchpoint.com/2017/07/19/guide-deep-packet-inspection/) from devices.

Mobile service operators and other similar service providers also use deep packet inspection to tailor-fit their offerings to individual subscribers allowing them to differentiate data usage as “all you can eat,” wall garden, or value added. Record labels and other copyright holders can also request ISPs to block their content from being downloaded illegally – a process achieved through deep packet inspection.

Other times, deep packet inspection is used to serve targeted advertising to users, lawful interception, and policy enforcement. Deep packet inspection can also prevent some types of buffer overflow attacks.

Lastly, deep packet inspection can help you prevent anybody from leaking information, such as when e-mailing a confidential file. Instead of being able to successfully send out a file, the user will instead receive information on how to get the necessary permission and clearance to send it.

As with other technologies, deep packet inspection can also be used for less than admirable purposes, such as eavesdropping and censorship. In fact, the [Chinese government](https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/) has been known to use deep packet inspection to monitor the country's network traffic and censor some content and sites that are harmful to their interests. This is how China has been able to block out pornography, religious information, materials concerning political dissent, and even popular websites such as Wikipedia, Google, and Facebook.

While DPI has many potential use cases, it can easily detect the recipient or sender of the content that it monitors, so there are some concerns around privacy. This is primarily a concern when DPI is used in the context of marketing and advertising, through monitoring the behavior of users and selling browsing and other data to marketing or advertising companies.

**Deep Packet Inspection Techniques**

Two primary types of products utilize deep packet inspection: firewalls that have implemented features of IDS, such as content inspection, and IDS systems that aim to protect the network rather than focus only on detecting attacks. Some of the [main techniques](http://www.infosectoday.com/Articles/Deep_Packet_Inspection_Technologies.htm) used for deep packet inspection include:

● **Pattern or signature matching** – One approach to using firewalls that have adopted IDS features, pattern or signature matching, analyzes each packet against a database of known network attacks. The downside to this approach is that it’s effective only for known attacks, and not for attacks that have yet to be discovered.  
● **Protocol anomaly** – Another approach to using firewalls with IDS features, protocol anomaly uses a “default deny” approach, which is a key security principle. Using this technique, protocol definitions are used to determine which content should be allowed. This differs from the approach of simply allowing all content that doesn’t match the signatures database, as occurs in the case of pattern or signature matching. The primary benefit of protocol anomaly is that it offers protection against unknown attacks.  
● **IPS solutions** – Some IPS solutions implement DPI technologies. These solutions have similar functionality to in-line IDS, although they have the ability to block detected attacks in real-time. One of the biggest challenges in using this technique is the risk of false positives, which can be mitigated to some extent through the creation of conservative policies.

Some limitations exist with these and other DPI techniques, although vendors offer solutions aiming to eliminate the practical and architectural challenges through various means. Additionally, DPI solutions are now offering a range of other complimentary technologies such as VPNs, malware analysis, anti-spam filtering, URL filtering, and other technologies, providing more comprehensive network protection.

**Challenges of Deep Packet Inspection**

No technology is perfect, and deep packet inspection is no exception. It has three distinct weaknesses:

1. Deep packet inspection is very effective in preventing attacks such as denial of service attacks, buffer overflow attacks, and even some forms of malware. But it can also be used to **create similar attacks**.

2. Deep packet inspection can make your current firewall and other security software you use more **complicated and harder to manage**. You need to be sure that you constantly update and revise deep packet inspection policies to ensure continued effectiveness.

3. Deep packet inspection can **slow down your network** by dedicating resources for your firewall to be able to handle the processing load.

Bron: <https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more>

## Deep Packet Inspection (DPI)

As mentioned in the introduction above, the state of firewall/filtering techniques has evolved over the years. Initially, we had **Static/Stateless filtering** where traffic is checked against rules that match on source/destination IP addresses/ports.

In this technique, every packet (irrespective of whether that packet is standalone or part of a traffic flow) is checked against the filtering rules. While this technique still has its place in today’s network (i.e. [Access Control Lists](https://www.pcwdld.com/guide-to-access-control-lists)), it doesn’t scale well for current security needs.

We then moved on to **Stateful filtering** (or **Stateful Packet Inspection**) which basically keeps track of the state of connections. For example, when a stateful firewall sees a SYN packet, it keeps track of that TCP connection expecting to see the corresponding SYN+ACK and ACK packets.

If there is any funny business happening in the exchange (e.g. SYN+ACK is seen without an initial SYN packet), the firewall knows that is probably a security attack.

But as firewall techniques got better, so did hackers. How about if everything is fine at the IP and Transport layers (referencing the OSI model), but the real threat is contained in the data portion of the packet?

For example, many applications (e.g. Skype, P2P torrent applications) run on standard HTTP and HTTPS ports. A firewall using static and/or stateful filtering will allow traffic from those applications thinking it is normal web traffic.

This brings us to the third type of firewall technology: **Deep Packet Inspection**. Basically, DPI is able to not just inspect the general information carried by a packet but also inspect the contents of the packet itself. So DPI is able to say, “while the port being used is HTTP, the application carried is actually Skype”. This opens up a whole new world of opportunities and challenges.

**Note**: We are using the term “packet” loosely here to mean any application layer data/payload that has been encapsulated with lower-level protocols (e.g. TCP, IP, Ethernet). Basically, “Packet” in this article means **Headers+Payload**.

Therefore, we can say that static and stateful filtering look at the headers while DPI looks deep into the payload.

## How DPI works

There are several techniques used to perform DPI on traffic. Let’s look at some of them here.

### Port-based Detection

This is the simple method of matching applications/protocols to their most common/standard ports. For example, BitTorrent uses the TCP ports 6881-6889 by default.

One of the challenges with this method is that many applications can modify their port behavior either by design or to prevent detection. For example, FTP starts on one port and then moves to another dynamic port to transfer data. Also, applications like BitTorrent may use their standard ports if unblocked, but can also move to other ports if filtering is being done.

Another challenge with port-based detection is that some applications can ride on standard ports fooling detection systems. For example, Skype used to be able to fall back to TCP port 80 (HTTP standard port) when its normal ports are blocked. In recent times, it mostly uses TCP port 443.

### Signature Matching

Even when applications/protocols change their ports, there are still some strings or patterns that may be recognizable in such applications. For example, this [paper](http://www.cs.columbia.edu/~salman/skype/Ehlert_SkypeSignature_2006.pdf) discusses a signature matching algorithm for an old version of Skype and one of the things to check is for a packet with a hexadecimal pattern that begins with “80 46 01 03 …”.

One of the issues with this technique is that applications are constantly changing and being updated which means that new signatures will have to be developed for these applications. This results in a cat-and-mouse game.

### Heuristic and Behavior Analysis

By studying an application/protocol, you can understand its behavior. This can be done by measuring packet sizes, the timing between packets, and so on. Even if the application/protocol changes its signature, the behavior is likely to remain (fairly) the same allowing for a high degree of accuracy in detection. For example, Voice over IP (VoIP) traffic usually starts with session initiation and then many small-sized UDP packets are used to carry the call traffic (or [call details](https://www.pcwdld.com/call-details)) itself.

While the three techniques discussed above are the common techniques used in DPI implementations, newer forms of detection are being developed especially those that rely on Machine Learning (ML) and Artificial Intelligence (AI).

Finally, keep in mind that most DPI tools will implement a mixture of these techniques in a bid to improve detection and increase accuracy.

## Why DPI?

The whole point of any type of inspection is the ability to do something about traffic that fits a profile. This could be as simple as generating an alert or triggering an action such as dropping the packet or limiting the bandwidth available to that traffic. In this subsection, we will look at some of the ways DPI is being used across the industry.

### Network and Endpoint Security

By looking inside the contents of a packet/traffic flow, firewalls and intrusion detection systems can identify malicious traffic and prevent attacks that will normally be caused by viruses, worms, ransomware, and so on. This is similar to how antivirus programs work on end devices. The difference is that detection can now happen at the network layer even before it gets to the end users.

DPI can also be used for Data Loss Prevention (DLP) purposes in a bid to prevent sensitive information from leaving a company’s network.

### QoS/Traffic Shaping

One of the major uses of DPI is in the ISP environment. Using DPI, ISPs are able to “snoop” into the contents of the traffic flowing through their network. They can then use this information to improve the user experience on their network. For example, a user that is downloading large files using torrents may negatively impact the experience of other users who simply need to browse websites. In such a case, an ISP may perform traffic shaping such that the traffic of the user downloading large files is rate limited.

### Target Advertising

The ability to look inside the contents of network traffic makes it easier to tailor adverts to users. For example, my continuous visit to booking.com may mean that I have a trip coming up and I may get served an advert for airline tickets or car rentals.

## DPI Challenges

Having discussed some of the uses and benefits of DPI, let us now turn our attention to the challenges faced by DPI.

### DPI and Performance

DPI is processor-intensive because not only does it look into individual packets, it also looks into traffic flows (a flow is a collection of related packets). This is combined with the fact that inspection needs to be done in real-time meaning that latency needs to be reduced to a manageable level. Also, since most firewalls already do so much (stateful packet inspection, NAT, VPN, etc.), adding DPI increases the complexity of the entire system. This can lead to a greater attack surface.

The good news is that performance/processing power increases with time usually at a lower cost than was available in previous years (Moore’s Law).

### DPI and Privacy

DPI raises a lot of privacy issues: should anyone (apart from the end user and destination service) know the contents of a user’s traffic? While we have seen the benefits like being able to thwart security attacks, where do we draw the line? This issue also borders on the topic of Net Neutrality, which aims for ISPs to treat all traffic equally without discrimination.

### DPI and Encryption

Encryption has particularly been a challenge to DPI: if you can’t look into the contents of the packet, how can you make effective decisions? This is one issue that would not be going away as more applications and websites are enabling encryption. For example, all Skype traffic is fully encrypted. About 93% of all Google traffic (including Gmail, Google maps, Google Drive, YouTube, etc.) is secured using HTTPS. Finally, it is estimated that about 73% of all Internet traffic is now encrypted.

To tackle this “problem” of encryption (even though it is supposed to be a good thing?), companies use various techniques. One of such techniques is SSL inspection where the traffic is decrypted, scanned (possibly with DPI), re-encrypted, and sent to its original destination. Apart from the privacy issues, SSL inspection can also have harmful results when not implemented correctly.

Another DPI technique used to look into encrypted traffic is based on heuristic analysis as we discussed above. One of such DPI implementations that is able to inspect encrypted traffic without decrypting it is Cisco’s Encrypted Traffic Analytics ([ETA](https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html)). By looking at the initial packets used to encrypt the session (those packets are initially unencrypted), you are able to get some insight into the traffic (e.g. server’s certificate name). Also, once encryption has kicked it, you can measure things like packet size, distribution, and so on.

How about when end-to-end encryption is being used by the user as in the case of VPNs? This presents more challenges for DPI (which is why torrent sites usually advise you to use VPN \*grin). In this kind of situation, it seems heuristic analysis will still be effective but probably to a lower degree of accuracy.

## Deep Packet Inspection Software and Tools

In this subsection, we will look at different Software and Tools that have DPI capability. While there are standalone DPI tools, most of the DPI implementations are usually used inside another device/application. Moreover, in most cases, DPI only provides the analysis – another tool acts on it (e.g. drop traffic).

Some DPI tools include:

* **Protocol and Application Classification Engine** ([PACE](https://www.ipoque.com/products/dpi-engine-rsrpace-2)) by Rohde&Schwarz is a software library that provides DPI functionality using various techniques such as pattern matching and heuristic analysis. This tool is proprietary (you cannot download it) and is used inside other products such as [Lancope StealthWatch](https://www.ipoque.com/sites/default/files/media/documents/2017-01/ipoque_Case_Study_Lancope-web.pdf) (which is now [part of](https://www.cisco.com/c/m/en_us/products/security/cisco-lancope.html) Cisco).
* [**nDPI**](https://www.ntop.org/products/deep-packet-inspection/ndpi/) which is an open source DPI tool based on the now extinct OpenDPI library. While the source code for this tool is [available](https://www.ntop.org/get-started/download/) (standalone), it is installed as part of the [ntop](https://www.ntop.org/products/traffic-analysis/ntop/) and [nProbe](https://www.ntop.org/products/netflow/nprobe/) It supports the classification of many protocols including Skype, WhatsApp, and BitTorrent. It can even classify various websites such as Facebook and Google. Finally, it can identify encrypted protocols and applications relatively well. You can download nDPI (as part of ntop) for free [here](http://packages.ntop.org/) and it is supported on Windows, Mac, and Linux operating systems.
* **Cisco Network-Based Application Recognition** ([NBAR](https://www.cisco.com/c/en/us/products/ios-nx-os-software/network-based-application-recognition-nbar/index.html)) which is available on many Cisco ISR and ASR devices. It supports over 1000+ classification of applications and sub-applications and can match based on individual applications (e.g. Skype) or groups of applications (e.g. Email). When used in conjunction with [Cisco IOS](https://www.pcwdld.com/cisco-commands-guide) QoS, various policies, like reclassification and dropping, can be applied to matched traffic.

Other examples include Qosmos [ixEngine](http://www.qosmos.com/products/deep-packet-inspection-engine/), Netify Agent ([Netifyd](https://www.netify.ai/developer/netify-agent)), NetFort [LANGuardian](https://www.netfort.com/languardian/), SolarWinds [Network Performance Monitor](https://www.pcwdld.com/go/solarwinds-topics-deep-packet-inspection/l/inline/) (has deep packet inspection and analysis), ManageEngine [NetFlow Analyzer](https://www.manageengine.com/products/netflow/deep-packet-inspection.html) (has deep packet inspection capability), Cisco [ETA](https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html) (mentioned above), and so on.

## Case Study: nDPI

Let’s now look at one of the DPI tools, nDPI, and see what kind of information it can provide. You can download the installer from [here](http://packages.ntop.org/) and install it on your system (you may need to restart your computer).

Once the application is installed, you can log in at 127.0.0.1:3000.

Bron: https://www.pcwdld.com/deep-packet-inspection