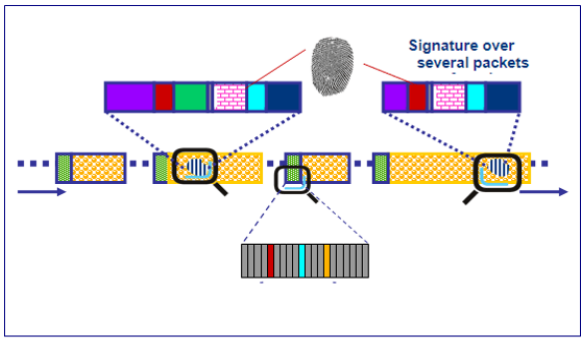
Deep Packet Inspection "DPI"

Deep Packet Inspection (DPI) is a form of data packet filtering that examines the data part (and possibly also the header) of a packet of computer network with high-speed traffic as it passes through an inspection point, searching for protocol non-compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information.

Figure (1): **Deep Packet Analysis**

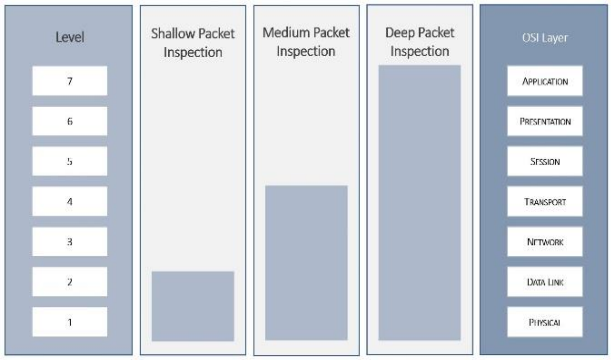


Deep Packet Inspection – analysis of encapsulated content over many packets

DPI Modules:

- Traffic Monitoring and Analysis
- Capacity Planning Analysis
- Subscriber Service Analysis
- Real-time Advertising or direct sales
- Risk Flows Analysis
- Monetization and Assurance
- Data Real-time Charging
- Usage-Based Services
- Parental Control
- Video QoE Analysis (Optional)
- Gaming QoE Analysis (Optional)

Figure (2): **DPI Data Analysis Layers**



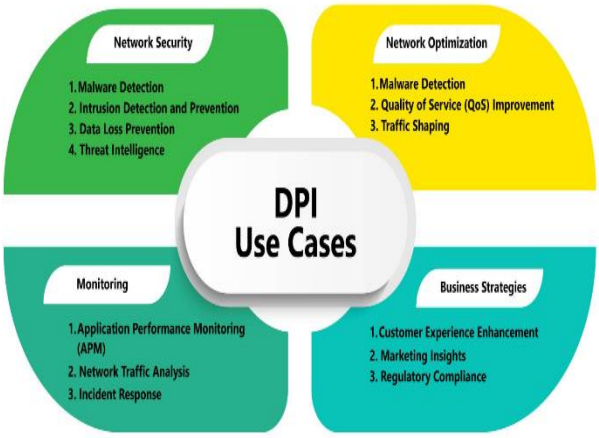
Why Our DPI?

- The only DPI does not need internet
- Support more than 6000 app signatures
- Open to add custom or local app signatures
- Support traffic speed above 8 TB/Sec.
- Equipped with 50+ risk flows analysis
- More than 500 network protocols
- Stores more than three years of historical data

DPI Used for:

- **Traffic Management**: Gain granular visibility and control over network traffic
- **Security**: Mitigate various cybersecurity threats, detect and block unauthorized access attempts
- **QoS (Quality of Service):** Ensuring that critical applications and services receive the necessary bandwidth and priority.
- **Content Filtering:** Control and block access to all types of content of your choice.
- **Analytics**: Intelligent reporting using AI for traffic in real-time
- **Data Real-time Charging**: Provides network operators * ISPs with real-time subscriber traffic usage and easy integration with Standard or nonstandard Charging or Billing systems

- **Real-time Advertising or direct sales integrations**: Translate all internet access behaviors in real-time to customers with suitable offer monetizing through advertising channels or direct sales



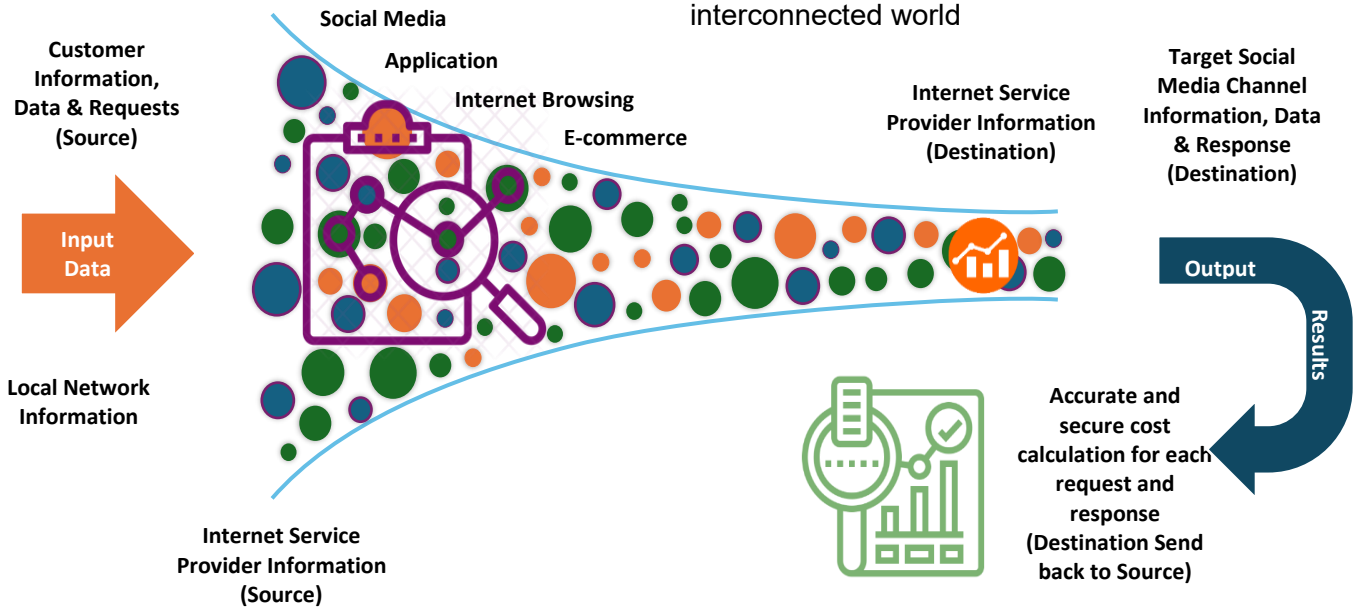
- **<u>DPI vs Firewall</u>:** DPI can identify dangerous data packets that may slip by firewalls in high-speed networks. DPI also gives advanced controlling options for traffic flow much beyond a firewall.

- **DPI used to capture all types of MITRE ATT&CK Framework Tactics**, which are (Initial Access, Command & Control, Data Exfiltration, Discovery, Collection, and Lateral Movement)
- **Offerings:** On-premises with annual subscription to guarantee 100% safety
- **Management:** Only updated and controlled within customers' network by their team.

How Does DPI Work?

- Packet Capture
- Packet Decoding
- Signature Matching
- Protocol Analysis
- Content Inspection
- Policy Enforcement
- Logging and Reporting

Following these steps, DPI enables network administrators to gain deep insights into network traffic, detect and mitigate security threats, enforce usage policies, and optimize network performance. It provides a powerful tool for enhancing network security, efficiency, and reliability in today's interconnected world



50GB/Sec. - 8+ TB/Sec.