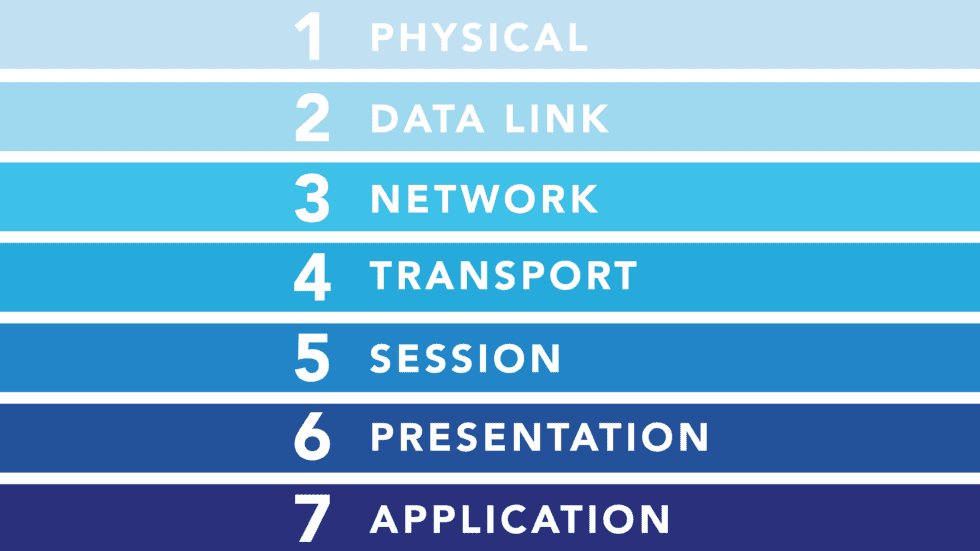
OSI MODEL



1. **Physical Layer:-**

**Definition**

The physical layer is the first layer of the Open Systems Interconnection (OSI) model, which is a conceptual framework used to understand and describe how different networking technologies and protocols interact. The physical layer is responsible for the transmission and reception of raw data bits over a physical medium, such as copper wires, fibre-optic cables, or wireless channels.

Protocols Linked

**Ethernet**: Ethernet is a widely used protocol for local area networks (LANs) that operates at the physical and data link layers.

**Fast Ethernet:** Fast Ethernet is an extension of the Ethernet protocol that supports higher data transfer rates, typically 100 Mbps.

**Gigabit Ethernet:** Gigabit Ethernet is another extension of the Ethernet protocol that provides even higher data transfer rates, typically 1 Gbps.

**Fibre Distributed Data Interface (FDDI):** FDDI is a protocol used for high-speed data transmission over fibre-optic cables. It operates at both the physical and data link layers and is commonly used in backbone networks.

**Asynchronous Transfer Mode (ATM):** ATM is a protocol that uses

fixed-size cells to transmit data over various physical media, including copper wires and fibre-optic cables. It operates at the physical, data link, and network layers.

**Common attacks**

**Physical Tapping:** An attacker physically taps into the communication medium, such as a network cable or fiber-optic line, to eavesdrop on the transmitted data.

**Interference and Jamming:** Attackers can introduce electromagnetic interference or intentionally transmit strong signals to disrupt or jam the communication on the physical medium.

**Wiretapping:** Similar to physical tapping, wiretapping involves intercepting signals by attaching monitoring devices or sniffers to the physical cables.

**Denial of Service (DoS):** In a physical layer DoS attack, the attacker overwhelms the physical medium by flooding it with excessive noise, signals, or traffic.

**Case study**

**Fiber Optic Cable Damage at a Financial Institution:**

A financial institution experienced network connectivity issues that impacted its ability to process transactions and provide services to customers.

Investigation revealed that a construction crew accidentally damaged a crucial fibre optic cable while performing excavation work near the institution. The physical layer failure disrupted data transmission, resulting in significant downtime and financial losses.

## **Power Outage Impacting a Data Center:**

A data centre relied on stable power supply to ensure uninterrupted network operations. However, a power outage caused by severe weather conditions resulted in a complete loss of power to the facility. Without power, the physical layer infrastructure, including network devices and communication links, became non-functional, leading to a complete network outage.

**Mitigation**

**Physical Security Measures:**Control physical access to network equipment and infrastructure by implementing restricted areas, card-based access systems, or biometric authentication.

**Redundancy and Resilience:**Implement redundancy measures, such as backup links, diverse physical paths, and redundant cabling, to ensure failover capabilities in case of physical layer failures.Deploy redundant power systems, such as uninterruptible power supplies (UPS) and backup generators, to maintain power supply to network devices and infrastructure.

**Cable Management and Maintenance:**Establish proper cable management practices, including cable labelling, organising, and securing, to prevent accidental disconnections or damage.Regularly inspect and maintain physical cables, connectors, and network equipment to identify and address potential issues before they cause disruption.

**Conclusion**

The physical layer in the OSI model establishes and maintains reliable communication links between network devices. It defines encoding, signaling, transmission mediums, and connectors/interfaces. Implementing physical security, redundancy, proper cable management, and disaster recovery planning ensures the integrity and reliability of the physical layer. It forms the foundation for data transmission and supports higher-layer protocols.

1. **Data Link Layer:-**

**Definition**

The Data-link layer is the second layer from the bottom in the [OSI](https://www.geeksforgeeks.org/layers-of-osi-model/) (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data. Its major role is to ensure error-free transmission of information. DLL is also responsible to encode, decode and organize the outgoing and incoming data. This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers.

**Protocols Linked**

Synchronous Data Link Protocol (SDLC) –

SDLC is basically a communication protocol of computer. It usually supports multipoint links even error recovery or error correction also. It is usually used to carry SNA (Systems Network Architecture) traffic and is present precursor to HDLC.

[High-Level Data Link Protocol (HDLC)](https://www.geeksforgeeks.org/basic-frame-structure-of-hdlc/) –

HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols sit. It is also adopted as a part of X.25 network. It was originally created and developed by ISO in 1979. This protocol is generally based on SDLC.

[Serial Line Interface Protocol (SLIP)](https://www.geeksforgeeks.org/slip-full-form/) **–**

SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user over a dial-up link.

**Common attacks**

### MAC Flooding :Every switch in the Ethernet has a Content-Addressable Memory (CAM) table that stores the MAC addresses, switch port numbers, and other information. The table has a fixed size. In the MAC flooding attack, the attacker floods the switch with MAC addresses using forged ARP packets until the CAM table is full.

### Port Stealing: Ethernet switches have the ability to learn and bind MAC addresses to ports. When a switch receives traffic from a port with a MAC source address, it binds the port number and that MAC address.

**Case study**

**Mitigation**

**Conclusion**

1. **Network Layer:-**

**Definition**

The network layer is the third layer in the Open Systems Interconnection (OSI) model. It is responsible for managing network connectivity and addressing to enable communication between hosts or devices on different networks. The network layer uses logical addressing, routing protocols, and packet forwarding to ensure data packets are correctly routed from the source to the destination across multiple network nodes.

**Protocols Linked**

**Internet Protocol (IP):** IP is a fundamental protocol of the network layer that provides logical addressing for devices connected to an IP-based network. It defines the IP address format and packet structure, enabling the routing of data packets across interconnected networks.

**Internet Control Message Protocol (ICMP):** ICMP is a protocol used by network devices to communicate error messages and provide feedback about network conditions. It is commonly used for diagnostics, troubleshooting, and managing network connectivity.

**Internet Group Management Protocol (IGMP):** IGMP is a protocol used for managing multicast group membership within a network. It enables devices to join or leave multicast groups, allowing efficient distribution of data to multiple recipients.

**Common attacks**

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:** These attacks aim to disrupt the availability of network resources or services by overwhelming them with a flood of illegitimate traffic. They can target any layer of the OSI model, including the physical layer (e.g., flooding a network with excessive traffic to exhaust bandwidth) or the application layer (e.g., overwhelming a web server with HTTP requests).

**Man-in-the-Middle (MitM) Attacks:** In a MitM attack, an attacker intercepts and possibly alters communication between two parties without their knowledge. This can occur at various layers, such as the physical layer (e.g., tapping into a network cable) or the network layer (e.g., spoofing IP addresses to redirect traffic).

**Packet Sniffing:** This attack involves capturing and analyzing network traffic to intercept sensitive information, such as usernames, passwords, or other confidential data. Packet sniffing attacks can occur at the data link layer or network layer, where the attacker gains access to network packets.

**Case study**

**Case Study 1:** In 2013, retail giant Target experienced a massive data breach that affected millions of customers. Attackers gained access to Target's network by exploiting a vulnerability in a third-party HVAC system. Once inside, they navigated to the network layer and deployed malware that captured payment card data from point-of-sale (POS) systems.

Impact and Consequences:

Data Compromise: The attackers stole approximately 40 million payment card details and personal information of over 70 million customers. This breach exposed customers to the risk of identity theft and financial fraud.

Financial Loss: Target incurred significant financial losses due to the breach, including legal expenses, regulatory fines, card reissuance costs, and a decline in customer trust, resulting in decreased sales and stock prices.

**Case Study 2:** Stuxnet Attack on Iranian Nuclear Facilities

Scenario: The Stuxnet worm, discovered in 2010, targeted the control systems of Iranian nuclear facilities. It specifically aimed at the physical and data link layers of the OSI model to disrupt and sabotage Iran's nuclear program.

Impact and Consequences:

Physical Damage: Stuxnet caused physical damage to the centrifuges used in Iran's uranium enrichment process by manipulating their rotational speeds. This sabotage significantly impacted Iran's nuclear operations.

Cyber Espionage: The attack provided valuable intelligence to the attackers, allowing them to gather insights into Iran's nuclear capabilities and potentially compromising sensitive information.

**Mitigation**

**Network Segmentation**: Divide the network into logical segments using VLANs or subnetting. This restricts the reachability of devices and limits the impact of potential network attacks or breaches.

Routing Security.

**Implement Routing Policies**: Utilise routing policies, such as route filters and route maps, to control the flow of routing information. This helps ensure the integrity and authenticity of routing updates and prevents unauthorised route propagation.

**Intrusion Detection and Prevention Systems (IDPS):** Deploy IDPS solutions that monitor network traffic in real-time, alerting administrators to potential attacks and enabling them to take preventive actions. Encryption and Virtual Private Networks (VPNs).

**Conclusion**

The Network Layer in the OSI model facilitates reliable communication between network devices by handling packet routing and addressing. It enables interconnectivity, defines routing protocols, and establishes logical connections. Implementing security measures like access control, routing security, and network monitoring enhances network reliability and protects against unauthorised access and attacks.

1. **Transport Layer:-**

**Definition**

The Network Layer in the OSI model facilitates reliable communication between network devices by handling packet routing and addressing. It enables interconnectivity, defines routing protocols, and establishes logical connections. Implementing security measures like access control, routing security, and network monitoring enhances network reliability and protects against unauthorised access and attacks.

**Protocols Linked**

## **UDP**: UDP stands for User Datagram Protocol.UDP is a simple protocol and it provides nonsequenced transport functionality.UDP is a connectionless protocol.This type of protocol is used when reliability and security are less important than speed and size.UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.

## **TCP**: TCP stands for Transmission Control Protocol.It provides full transport layer services to applications.It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

**Common attacks**

Social reconnaissance attacks: In this type of attack, a hacker uses social engineering to gather information about the target. Users share a lot of personal and business information on social networking sites. A hacker can use social networking sites to gather information about the target. For example, if the target is a company, the hacker can use social networking sites to reveal information about the company's employees.

Public reconnaissance attacks: In this type of attack, a hacker collects information about the target from public domains. Companies share location and business model information on their websites. A hacker can use this information to determine the location of the target. From this information, a hacker can also determine what kind of infrastructure the target uses. For example, most web hosting companies share information about their servers and security equipment. Companies share this information to attract new customers and gain the trust of existing customers.

**Case study**

This case study chains together several of the items learned within the chapter to perform a successful scan of a network. This case study trails Evil Jimmy the Hacker as he scans a small company called Little Company Network (LCN). He uses DNS to gather information before moving onto NMap for some scanning as he attempts to start his diagramming of the network.

The scene is set as LCN rejects Evil Jimmy for a position. He is skilled in penetration testing, and because LCN obviously did not even read to the end of his rèsumè, Jimmy plans to make use of his skills in an unauthorized manner. Jimmy knows the DNS names of his target LCN.com, so he plugs his laptop into the wall and begins his attack. Knowing that preparation is vital to a successful outcome, Jimmy starts by making a plan and gathering his tools. The following steps illustrate the execution.

**Mitigation**

Can disable all unused ports on servers. Can use the masking service to hide sensitive information on the **who is** database. Can use NAT to hide the internal structure of the network. Can use software or hardware firewall to filter all specious traffic. That's all for this tutorial. In this tutorial, we discussed what reconnaissance attacks are and how they work in detail.

**Conclusion**

Manuscripts should conform to the standard format as indicated in the Information for Authors section of the [Manuscript](https://www.comsoc.org/publications/magazines/ieee-communications-magazine/author-guidelines/manuscript-submission) [Submission Guidelines](https://www.comsoc.org/publications/magazines/ieee-communications-magazine/author-guidelines/manuscript-submission). Please, check these guidelines carefully before submitting since submissions not complying with them will be administratively rejected without review.

1. **Session Layer:-**

**Definition**

The Session Layer is the 5th layer in the Open System Interconnection (OSI) model. This layer allows users on different machines to establish active communications sessions between them. It is responsible for establishing, maintaining, synchronizing, terminating sessions between end- user applications. In Session Layer, streams of data are received and further marked, which is then resynchronized properly, so that the ends of the messages are not cut initially and further data loss is avoided.

**Protocols Linked**

* AppleTalk Data Stream Protocol (ADSP): ADSP is that type of protocol which was developed by Apple Inc. and it includes a number of features that allow local area networks to be connected with no prior setup. This protocol was released in 1985.
* Real-time Transport Control Protocol (RTCP): RTCP is a protocol which provides out-of- band statistics and control information for an RTP (Real-time Transport Protocol) session. RTCP’s primary function is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistical information such as transmitted octet and packet counts or packet loss to the participants in the streaming multimedia session.
* Point-to-Point Tunneling Protocol (PPTP): PPTP is a protocol which provides a method for implementing virtual private networks. PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP (Point-to-Point Protocol) packets.

**Common attacks**

Cross-site scripting: XSS attacks enable attackers to inject client-side scripts into web pages. It causes running codes, which is treated as trustworthy because it appears to belong to the server, on the victim computer. It allows the attacker to obtain a copy of the cookie or perform other operations.

Session side jacking: where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie.

Malware and unwanted programs can use browser hijacking to steal a browser’s cookie files without a user’s knowledge.

**Case study**

Case 1:

In 2007, a session hijacking attack known as the Firesheep attack gained prominence. This attack exploited the lack of encryption on unsecured Wi-Fi networks, allowing attackers to intercept session cookies and gain unauthorised access to users' online accounts.

Case 2:

Session fixation is an attack where an attacker forces a user's session identifier (SID) to a known value, enabling them to hijack the session later. In 2011, an exploit was discovered in a widely used open-source PHP framework called CodeIgniter. This vulnerability allowed attackers to set the session ID before the session was created, potentially granting them unauthorised access to user accounts.

**Mitigation**

Encryption: Implement strong encryption protocols, such as Transport Layer Security (TLS) or Secure Socket Layer (SSL), to protect session data from unauthorized access or interception. Encryption ensures the confidentiality and integrity of session information.

Secure Session Management: Implement robust session management practices, including session timeouts, strong session ID generation, and secure session storage. Session timeouts automatically terminate idle sessions, reducing the risk of session hijacking or fixation.

Two-Factor Authentication (2FA): Implement 2FA to add an extra layer of security to session authentication.By requiring users to provide a second form of verification, such as a one-time password (OTP) or biometric authentication, the risk of unauthorized access to sessions is significantly reduced.

**Conclusion**

Internet of Things (IoT) Security: With the proliferation of IoT devices, session layer security becomes crucial. IoT devices often communicate through sessions, and vulnerabilities in session management could lead to unauthorized access, data breaches, or device manipulation. Quantum Computing Threats: Quantum computing has the potential to break many of the cryptographic algorithms that currently secure session layer communications.

1. **Presentation Layer:-**

**Definition**

The Presentation Layer is the sixth layer of the OSI (Open Systems Interconnection) model, which is a conceptual framework that standardizes the functions of a communication system. The primary role of the Presentation Layer is to ensure the compatibility of different systems by handling the syntax. It acts as a translator or mediator between the application layer and the lower layers of the OSI model.

**Protocols Linked**

**ASCII (American Standard Code for Information Interchange):** ASCII is a character encoding scheme widely used in the presentation of text-based data. It assigns unique numeric codes to represent characters, allowing systems to exchange textual information in a standardised format.

**Unicode**: Unicode is an international character encoding standard that extends ASCII to include characters from different writing systems, languages, and symbols. It enables the representation of a wide range of characters and supports multilingual communication.

**MIME (Multipurpose Internet Mail Extensions):** MIME is a protocol that extends the capabilities of email systems by allowing the transmission of non- textual data such as images, audio, and video. It provides a mechanism to encode and format such data for reliable delivery.

**Common attacks**

**Format String Attacks**: Format string vulnerabilities occur when an application does not properly validate user-supplied input, allowing an attacker to inject malicious formatting characters. If an application uses input provided by the user directly in format strings without proper sanitization, an attacker can exploit this vulnerability to execute arbitrary code or leak sensitive information.

**Malicious File Formats**: Attackers can create malicious files in specific formats that take advantage of vulnerabilities in parsers or rendering engines. When a vulnerable application processes such files, it can lead to code execution, denial of service, or other adverse consequences. Examples include PDF, Microsoft Office documents, and image file formats.

**Code Injection**: Some attacks target the interpretation or execution of scripts or code within the Presentation Layer. For instance, an attacker may inject malicious code into a scripting language used for data representation, such as JavaScript embedded within HTML. If the application fails to properly validate and sanitise user input, the injected code can be executed, leading to unauthorised actions or system compromise.

**Case study**

**Data Corruption during Transmission:** In some cases, errors can occur during the formatting, compression, or encryption process in the Presentation Layer, leading to data corruption. This corruption may render the received data unusable or cause interpretation errors in the receiving system. Such incidents may happen due to software bugs, network disruptions, or misconfigurations.

**Incompatible Data Formats:** If there is a mismatch in data formats between the sender and receiver systems, it can lead to interpretation issues in the Presentation Layer. For example, if a legacy system uses a proprietary data format that is not supported by a newer system, data exchange problems may occur. This can result in data loss, incorrect rendering of information, or application crashes.

**Mitigation**

**Input Validation and Sanitization**: Ensure that all user-supplied input is thoroughly validated and sanitized before it is processed by the application. Implement strict input validation routines to prevent the injection of malicious code or formatting characters that could lead to vulnerabilities.

**Secure Coding Practices:** Follow secure coding practices when developing applications that interact with the Presentation Layer. This includes avoiding dangerous functions, properly handling buffers, and using parameterized queries to prevent code injection attacks.

**Use Secure Encryption and Compression Algorithms**: Choose strong and widely accepted encryption and compression algorithms for securing data at the Presentation Layer. Stay updated with any vulnerabilities or weaknesses identified in these algorithms and apply patches or updates promptly.

**Conclusion**

You have learned about the functions of the presentation layer, such as translation, encryption & decryption, and compression & decompression. You have understood that there are two sublayers of the presentation layer, which are the Common Application Service Element (CASE) and the Specific Application Service Element (SASE). You have gained knowledge of several protocols of the presentation layer, such as Network Data Representation (NDR), Independent Computing Architecture (ICA), NetWare Core Protocol (NCP), Apple Filing Protocol (AFP), Packet Assembler/Disassembler Protocol (PAD), eXternal Data Representation (XDR), and Lightweight Presentation Protocol (LPP).

1. **Application Layer:-**

**Definition**

The application layer, which is the top layer in the OSI model, is in charge of directly providing services to end-user applications. It serves as a link between the network's basic architecture and the application programs. Its fundamental objective is to make it possible for various apps operating on various devices to communicate and share data.

**Protocols Linked**

HTTP (Hypertext Transfer Protocol): This protocol is used for transferring text between web servers and browsers. It makes it possible to get and display online pages.

FTP (File Transfer Protocol): This protocol is primarily employed for file transfers between clients and servers. It has download, upload, and directory listing capabilities.

SMTP (Simple Mail Transfer Protocol): This protocol is used to transfer emails back and forth between mail servers. It guarantees dependable email delivery via networks.

**Common attacks**

SQL Injection: Attackers alter SQL queries to obtain unauthorised access to databases, retrieve private data, or change database content.

Cross-Site Scripting (XSS): Attackers insert malicious scripts onto web sites, which unwitting users subsequently execute, exposing private information or stealing cookies.

Remote Code Execution: Attackers use web application flaws to run arbitrary server-side code, giving them access to or control over the program.

Session Hijacking: Attackers steal session cookies or take over user sessions to access user accounts without authorization and carry out nefarious deeds.

**Case study**

Case 1:

The Equifax Data Breach (2017): A large data breach occurred as a consequence of attackers taking advantage of a weakness in a web application to access the personal data of around 147 million people.

Target Point-of-Sale (POS) Breach (2013): Attackers broke into Target's network via a vendor system that had been infiltrated, finally taking advantage of holes in their POS system to steal consumer credit card information.

**Mitigation**

Validate user input before sanitizing it to stop harmful material from undermining the program.

Use secure coding best practices to reduce vulnerabilities throughout the development process.

Web Application Firewalls (WAFs): Implement WAFs to thwart typical web application threats and filter out harmful traffic.

Regular Security Updates: To address known vulnerabilities, keep programs and systems up to speed with the most recent security patches.

**Conclusion**

Cloud computing: As cloud services are more widely used, it is important to secure applications in cloud settings to guard against unauthorised access and data breaches.

Mobile apps: To safeguard user data and stop mobile-based threats, mobile apps must be secured as they expand.

Internet of Things (IoT): The expansion of IoT devices poses new difficulties for managing device vulnerabilities and safeguarding application layer protocols.