Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- Welcome to Blue Team Level 1!
  - 4 Topics
- Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

- Introduction to Security Fundamentals
  - 1 Topic
- Soft Skills
  - 7 Topics
- Security Controls
  - 5 Topics | 1 Quiz
- Networking 101
  - 6 Topics | 1 Quiz
  - Section Introduction, Networking 101
  - Network Fundamentals
  - The OSI Model
  - Network Devices
  - Network Tools
  - Ports and Services
  - Activity) End of Section Review, Networking 101
- Management Principles
  - 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

- PA1) Introduction to Emails and Phishing
  - 7 Topics | 1 Quiz
- PA2) Types of Phishing Emails
  - 10 Topics | 2 Quizzes
- PA3) Tactics and Techniques Used
  - 12 Topics | 2 Quizzes
- PA4) Investigating a Phishing Email
  - 8 Topics | 2 Quizzes
- PA5) Analysing URLs, Attachments, and Artifacts
  - 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions
  - 12 Topics | 1 Quiz
- PA7) Report Writing
  - 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge
  - 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

- TI1) Introduction to Threat Intelligence
  - 7 Topics
- TI2) Threat Actors & APTs
  - 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence

# The OSI Model

In order to understand how communication between networks work, you need to associate this with real-life cases (after all, the computer world is an abstraction of the real world). So, let's review the following scenario:

Imagine that you want to send a gift to a friend who lives in a different city, but you can't go and visit him/her directly; So, in order to do this, you must use a person who acts as an intermediary between you and your friend. This person tells you that you must carry out a certain number of tasks in order for him/her to deliver this package correctly, so this person asks you to do the following:

- You must give your residence address so that the person can come to your house and pick up the gift you want to send.
- You must carefully wrap the gift so that it is not damaged during shipping.
- And you must clearly label the gift with the name of the person to whom it is addressed and its residence address.

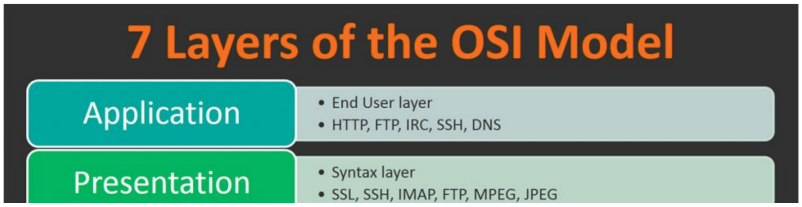
Once you have fulfilled each and every one of the requirements requested by that person, you proceed to call them to come to your home and pick up the package. This person arrives at your home, checks that all the requirements are in order and proceeds to make your delivery. Starts its vehicle and begins the journey to the address you provided; leaves your city, goes to your friend's city, looks for his/her home address and once found knocks on the door, verifies its identity, and delivers the gift successfully.

As you can see, this is a daily scenario, and did not have too many steps that allowed everything to work properly... Well, something like this happens in the IT world too, since, in order to send and receive messages, files, videos, and even funny images, our computers must perform a similar process, but in a digital way.

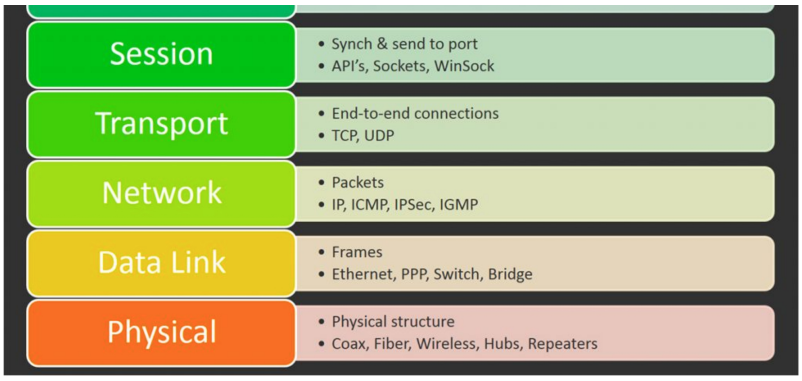
For this very reason (and in order to have more control over the operation of our communications networks), the OSI model was created.

## WHAT IS THE OSI MODEL?

Well, the Open Systems Interconnection Model (commonly known as OSI model) is a reference scheme developed by the International Organization for Standardization (ISO) in 1984 with the purpose of abstracting in a detailed way the operation of the communication networks, showing the different phases through which the files must pass in data transmission and especially, displaying how the different protocols are executed along with this communication



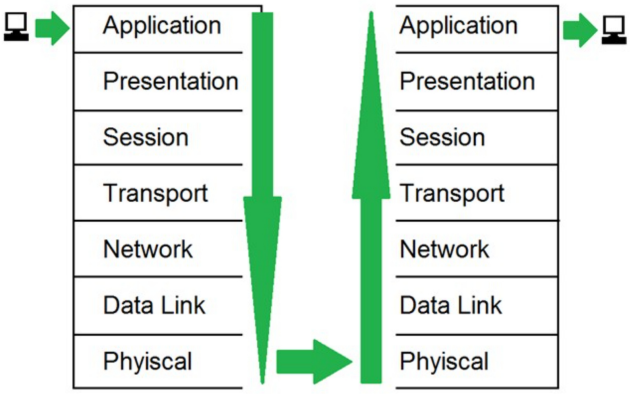
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 2 Quizzes
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation




*Provided by **bmc blogs*** (https://www.bmc.com/blogs/osi-model-7-layers/)

The OSI model is divided into 7 layers, where each layer plays a specific role in communication and each one serves and is served by its directly superior and directly inferior layers respectively, working together to carry out data transmission between computers, between applications and between networks. Want an easy way to remember the order of the layers?

- **Top to Bottom =** All People Seem To Need Data Processing (**APSTNDP**)
- **Bottom to Top =** Please Do Not Throw Sausage Pizza Away (**PDNTSPA**)




*Provided by **Paladin Group LLC*** (https://slideplayer.com/slide/6224155/)

# SEVEN LAYERS EXPLAINED

Below we will walk through the seven layers of the OSI model so that you fully understand what happens at each level. In this example, we will be taking a top-down approach – this is what happens when the initiating computer is attempting to connect with another system, with the message starting at Layer 7 Application, moving down to Layer 1 Physical.

### Step 1. The Application Layer (Layer 7)

This layer (also known as a high-level layer) is one of only 2 layers that the user can interact with. The Application layer is in charge of providing an interface to the user to interact, communicate, and even give commands to the computer. In this one, you will find e-mail applications, web browsers, file transfer applications, etc.

Some application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

### Step 2. The Presentation Layer (Layer 6)

This layer is considered as the "translator" between the machine and the user. It is in charge of guaranteeing that the data is understandable for the applications that will be operated by the user, allowing its correct visualization. And is also responsible for the encryption and decryption of the incoming and outgoing data.

Using RDP and SSH
How to Start Your Exam

### Step 3. The Session Layer (Layer 5)

The session layer is responsible for managing sessions between machines to enable communication between them. It is responsible for handling the opening, closing and resetting of sessions (to ensure proper communication between both parties), and is in charge of establishing the order of communication between a sender and a receiver, among many other activities of this nature.

### Step 4. The Transport Layer (Layer 4)

The transport layer is responsible for the transparent transfer of data between two computers. It assembles and fragments the packets that will be sent in the communication, while provides different mechanisms for verifying the integrity, to ensure that the information reaches the system accurately (some of these are error control, flow control, control of congestion and re-sending of information, in case there is a failure in the communication).

### Step 5. The Network Layer (Layer 3)

The network layer is responsible for redirecting the connection and transferring the data between two different networks by physical means, in search of the best path that allows this data to reach its destination in the shortest time possible.

### Step 6. The Data Link Layer (Layer 2)

This layer is in charge of the addressing and physical transmission of the data, carrying out its encapsulation, and separating them into frames that will be easily directed by the physical transfer media.

### Step 7. The Physical Layer (Layer 1)

This layer (also known as a low-level layer) is another of the 2 layers that can be manipulated by the user, since, in this case, it includes the physical elements of the networks (ethernet cables, optical fiber, etc.) responsible for the topology and the global connections from the computer to the network that allows the transmission and the physical operation of the system.

Previous Topic
Back to Lesson
Next Topic

Privacy & Cookies Policy
Privacy - Terms