Networking Fundamentals

Introduction

In this module of Networking Fundamentals, the learner is introduced to the world of Networking. The learner is expected to learn the overview of networking, Structure, network types, topologies, proxies, networking workflow (Networking models, the OSI model, the TCP/IP model); Addressing (Network layer, IPv4 addresses, subnetting, MAC Addresses, IPv6 Addresses), Protocols & Terminology (Networking key terminology, common protocols, wireless networks, virtual private networks, vendor specific information), Connection establishment (Key Exchange Mechanisms, Authentication protocols, TCP/UDP connections, cryptography).

Now, let's roll the sleeves because the **network** is about to go up.

Activities

Networking Overview

For computers, mobile phones, IP phones, printers and servers to communicate with each other they require a network connection. There are lists of topologies (will explain later on) – (mesh/star/tree), mediums (Ethernet/fiber/coax/wireless) and protocols (TCP/UDP/IPX) are used to facilitate the network.

As a Security Analyst – now the learner, it's good to have a sound knowledgeable and good understanding of the computer network fundamentals.

Networking Types

This is ideally the structure of the network and how it can be set up

Network Type	**Definition**
Wide Area Network (WAN)	Internet
Local Area Network (LAN)	Internal Networks (Ex: Home or Office)
Wireless Local Area Network (WLAN)	Internal Networks accessible over Wi-Fi
Virtual Private Network (VPN)	Connects multiple network sites to one LAN

WAN

The WAN (Wide Area Network) is commonly referred to as The Internet.. The WAN one is the address that is generally accessed by the Internet. It is not inclusive to the Internet; a WAN is a large number of LANs joined together. Many large companies or government agencies tend to have an "Internal WAN" (also called Intranet, Airgap Network, etc.). The primary way we identify if the network is a WAN is to use a WAN Specific routing protocol such as BGP and if the IP Schema in use is not within RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

LAN/WLAN

LANs (Local Area Network) and WLANs (Wireless Local Area Network) typically assign IP Addresses designated for local use (RFC 1918, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Devices are assigned a routable (internet) IP Address from joining their LAN - much less common. WLAN's introduce the ability to transmit data without cables mainly for a security designation.

VPN

There are three main types Virtual Private Networks (VPN), all have the same goal of making the user feel as if they were plugged into a different network.

Site-To-Site VPN

This is a type of VPN where the client and server are Network Devices, typically either Routers or Firewalls, and share entire network ranges. Most commonly used to join company networks together over the Internet, allowing multiple locations to communicate over the Internet as if they were local.

Remote Access VPN

This involves the client's computer creating a virtual interface that behaves as if it is on a client's network. E.g., Hack The Box usage of OpenVPN, makes a TUN Adapter allowing access of the labs. An important piece to consider is the routing table that is created when joining the VPN. If the VPN only creates routes for specific networks (ex: 10.10.10.0/24), this is called a **Split-Tunnel VPN**; - the Internet connection is not going out of the VPN. This is great for Hack The Box because it provides access to the Lab without the privacy concern of monitoring your internet connection. However, for a company, split-tunnel VPN's are typically not ideal because if the machine is infected with malware, network-based detection methods will most likely not work as that traffic goes out the Internet.

SSL VPN

This is essentially a VPN that is done within the web browser and is becoming increasingly common as web browsers are becoming capable of doing anything. These will stream applications or entire desktop sessions to the web browser. A great example of this would be the **HackTheBox Pwnbox**.

Terms Definition

Network Type	Definition
Global Area Network (GAN)	Global network (the Internet)
Metropolitan Area Network (MAN)	Regional network (multiple LANs)
Wireless Personal Area Network (WPAN)	Personal network (Bluetooth)

GAN

A worldwide network like the Internet is known as a **Global Area Network (GAN)**. GANs use the glass fibers infrastructure of wide-area networks and interconnect them by international undersea cables or satellite transmission.

MAN

Metropolitan Area Network (MAN) is a broadband telecommunications network that connects several LANs in geographical proximity. High-performance routers and high-performance connections based on glass fibers are used, which enable a significantly higher data throughput than the Internet. The transmission speed between two remote nodes is comparable to communication within a LAN.

Internationally operating network operators provide the infrastructure for MANs. Cities wired as Metropolitan Area Networks can be integrated supra-regionally in Wide Area Networks (WAN) and internationally in Global Area Networks (GAN).

PAN / WPAN

Modern end devices such as smartphones, tablets, laptops, or desktop computers can be connected ad hoc to form a network to enable data exchange. This can be done by cable in the form of a Personal Area Network (PAN).

The wireless variant Wireless Personal Area Network (WPAN) is based on Bluetooth or Wireless USB technologies. A wireless personal area network that is established via Bluetooth is called Piconet. PANs and WPANs usually extend only a few meters and are therefore not suitable for connecting devices in separate rooms or even buildings.

In the context of the Internet of Things (IoT), WPANs are used to communicate control and monitor applications with low data rates. Protocols such as Insteon, Z-Wave, and ZigBee were explicitly designed for smart homes and home automation.

Networking Topologies

A network topology is a typical arrangement and physical or logical connection of devices in a network. Computers are hosts, such as clients and servers, that actively use the network. They also include network components such as switches, bridges, and routers which have a distribution function and ensure that all network hosts can establish a logical connection with each other. The network topology determines the components to be used and the access methods to the transmission media.

The transmission medium layout used to connect devices is the physical topology of the network. For conductive or glass fiber media, this refers to the cabling plan, the positions of the nodes, and the connections between the nodes and the cabling. In contrast, the logical topology is how the signals act on the network media or how the data will be transmitted across the network from one device to the devices' physical connection.

Let’s see entire network topology - both for wired and wireless connections, Nodes (Network Interface Controller) and Classifications.

Wired connections	**Wireless connections**
Coaxial cabling	Wi-Fi
Glass fiber cabling	Cellular
Twisted-pair cabling	Satellite
and others	and others

Nodes - Network Interface Controller (NICs)

Repeaters	Hubs	Bridges	Switches
Router/Modem	Gateways	Firewalls	

Network nodes are the transmission medium's connection points to transmitters and receivers of electrical, optical, or radio signals in the medium. A node may be connected to a computer, but certain types may have only one microcontroller on a node or may have no programmable device at all.

Classifications

We can imagine a topology as a virtual form or structure of a network. This form does not necessarily correspond to the actual physical arrangement of the devices in the network. Therefore these topologies can be either physical or logical. For example, the computers on a LAN may be arranged in a circle in a bedroom, but it is very unlikely to have an actual ring topology.

Network topologies are divided into the following eight basic types:

Point-to-Point

Star

Mesh

Hybrid

Bus

Ring

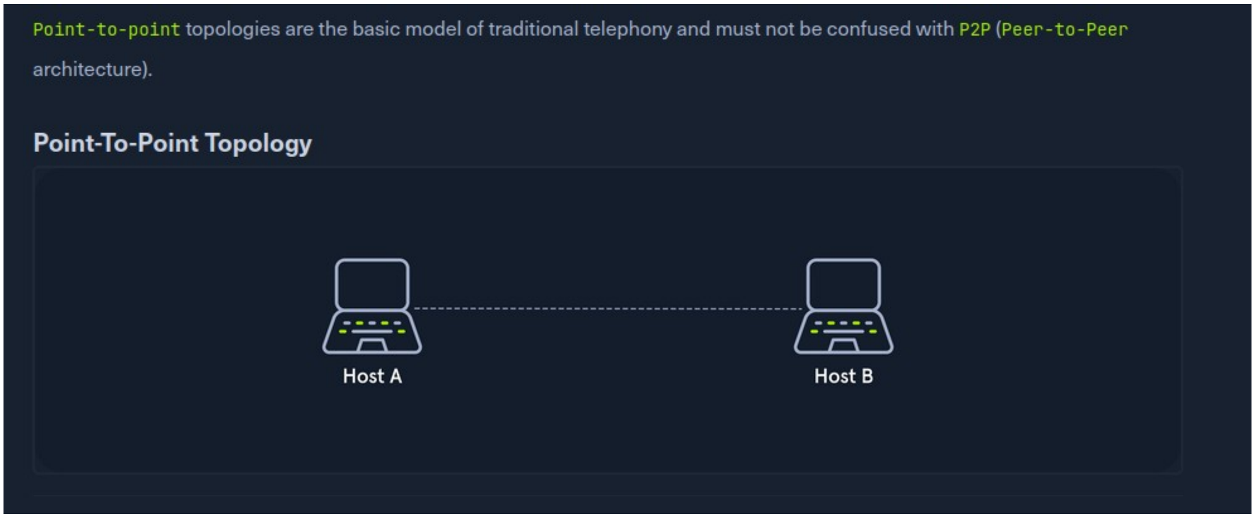
Tree

Daisy Chain

More complex networks can be built as hybrids of two or more of the basic topologies mentioned above.

Point – to – point

Point-to-point topology is the simplest network topology with a dedicated connection between two hosts, a direct and straightforward physical link exists only between two hosts.



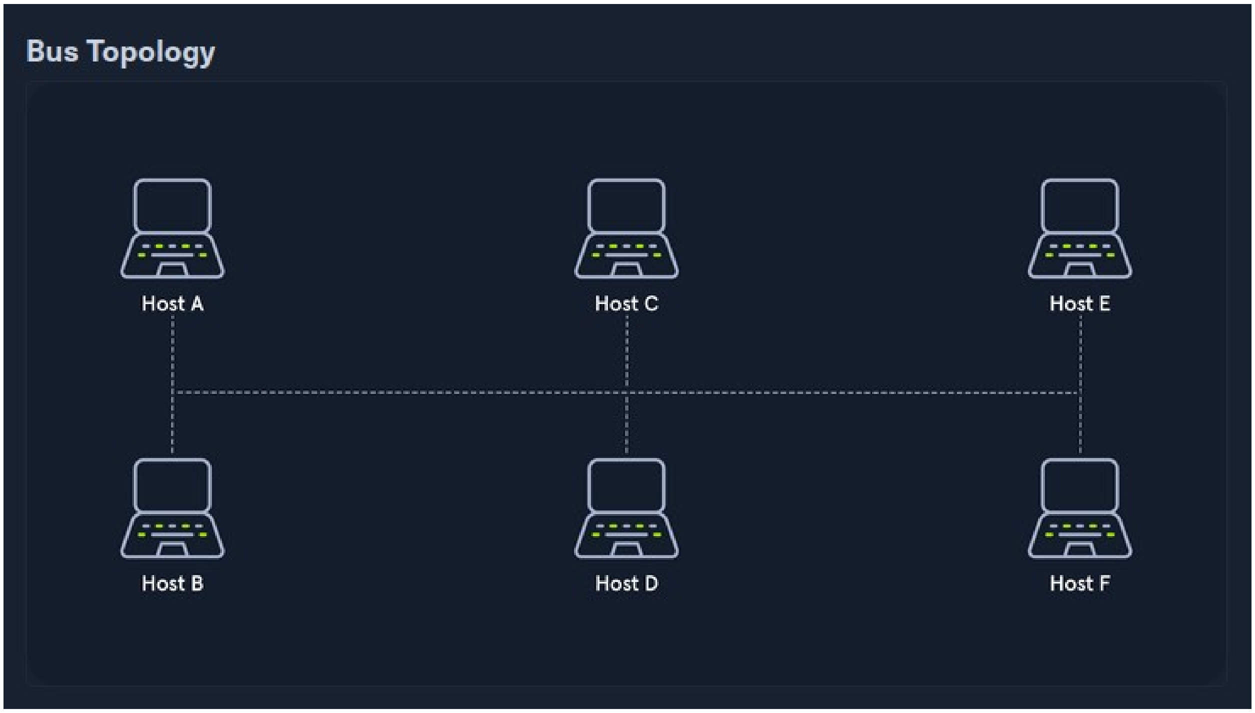
`Point-to-point` topologies are the basic model of traditional telephony and must not be confused with `P2P` (`Peer-to-Peer` architecture).

Point-To-Point Topology

Bus

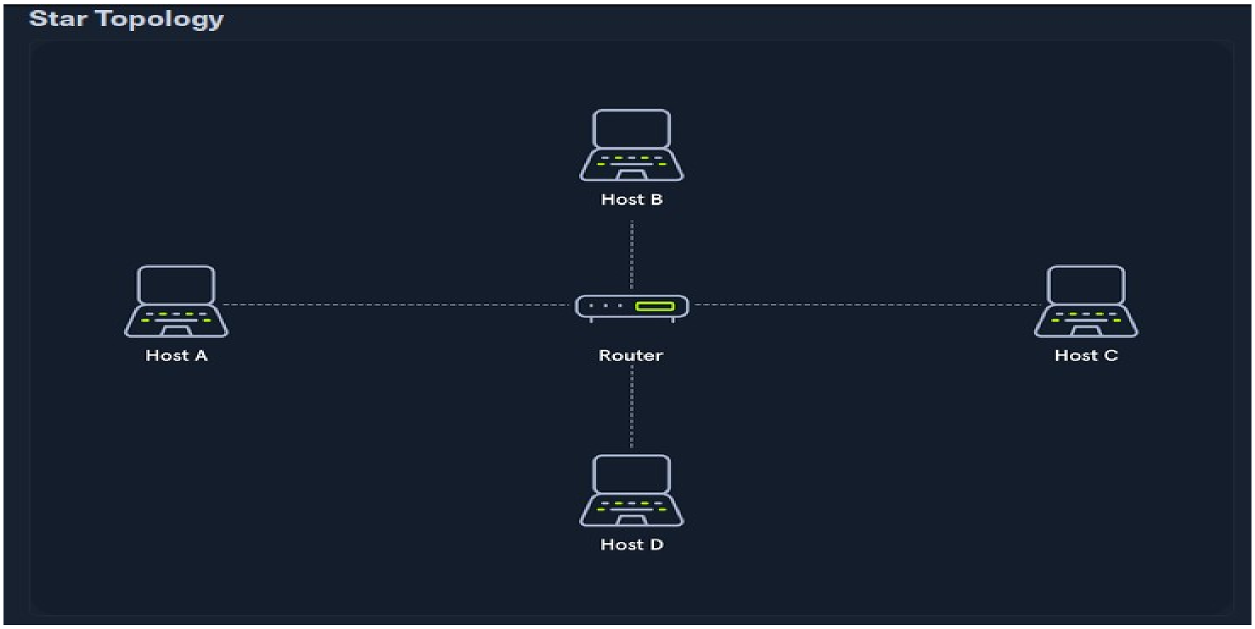
In the bus topology all hosts are connected via a transmission medium. Every host has access to the transmission medium and the signals that are transmitted over it. There is no central network component that controls the processes on it. The transmission medium can be a coaxial cable.

Only one host can send, and all the others can only receive and evaluate the data and see whether it is intended for itself.



Star

The star topology is a network component that maintains a connection to all hosts. Each host is connected to the central network component via a separate link. This is usually a router, a hub, or a switch. These handle the forwarding function for the data packets. To do this, the data packets are received and forwarded to the destination.



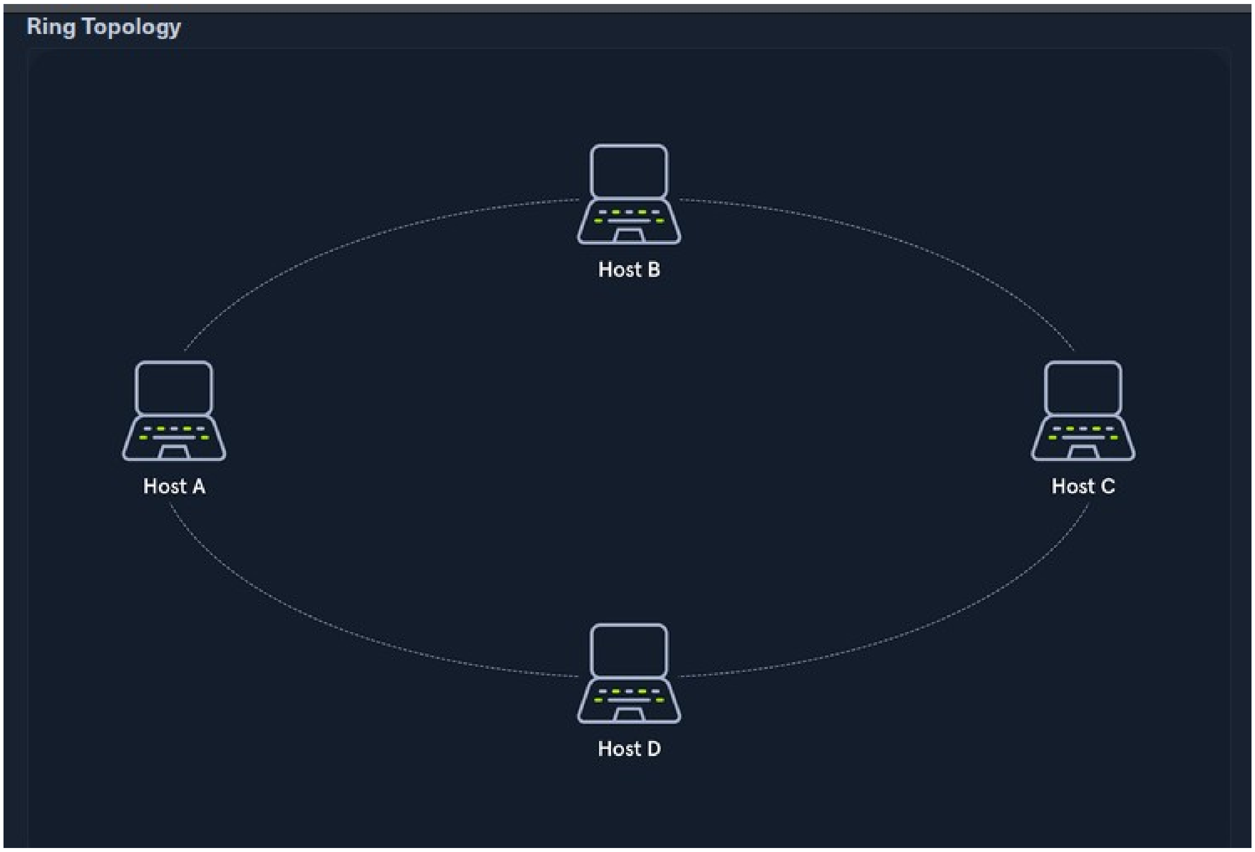
Ring

The physical ring topology is such that each host or node is connected to the ring with two cables:

- One for the incoming signals and
- the another for the outgoing ones.

This means that one cable arrives at each host and one cable leaves. The ring topology typically does not require an active network component. The control and access to the transmission medium are regulated by a protocol to which all stations adhere.

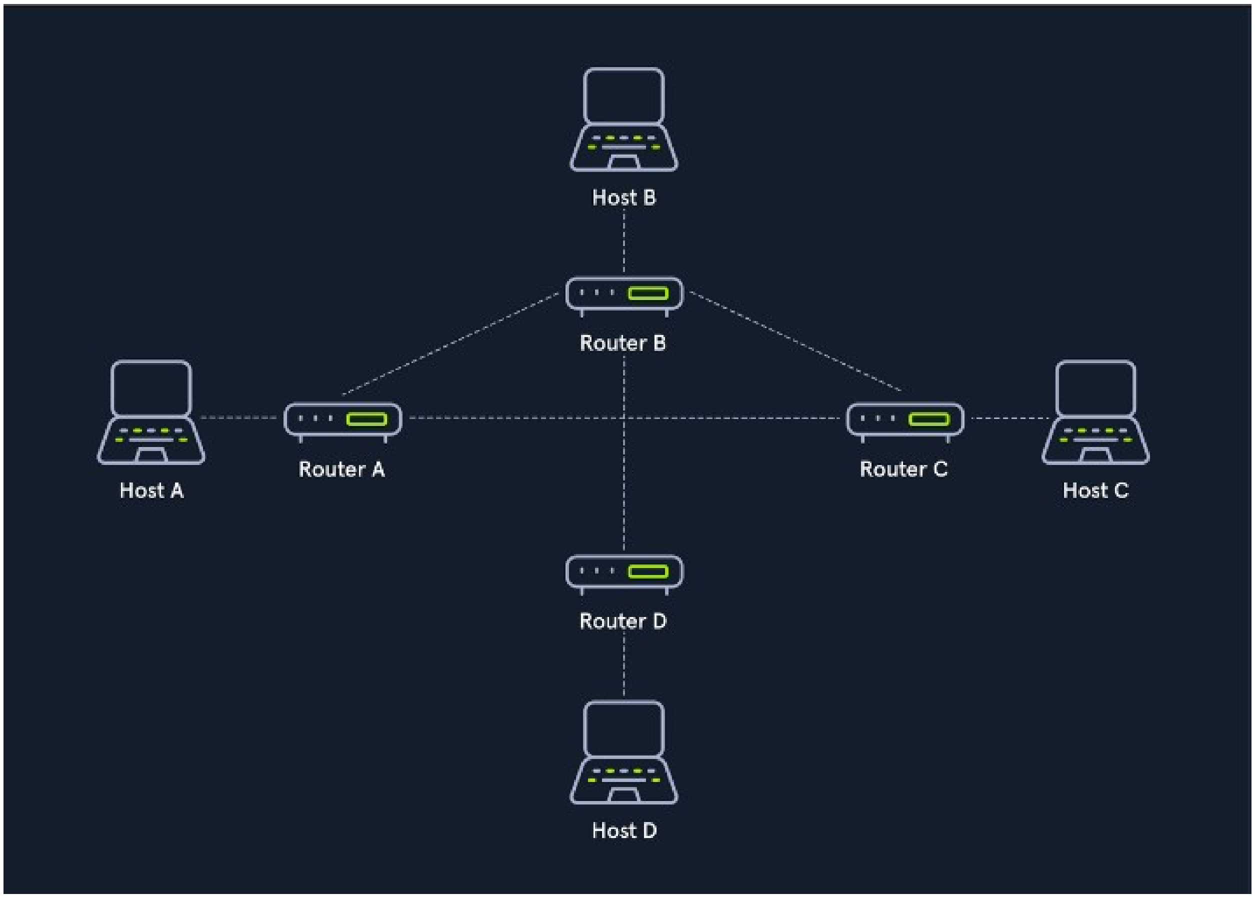
A logical ring topology is based on a physical star topology, where a distributor at the node simulates the ring by forwarding from one port to the next.



Mesh

Many nodes decide about the connections on a physical level and the routing on a logical level in meshed networks. Therefore, meshed structures have no fixed topology. There are two basic structures from the basic concept: the fully meshed and the partially meshed structure.

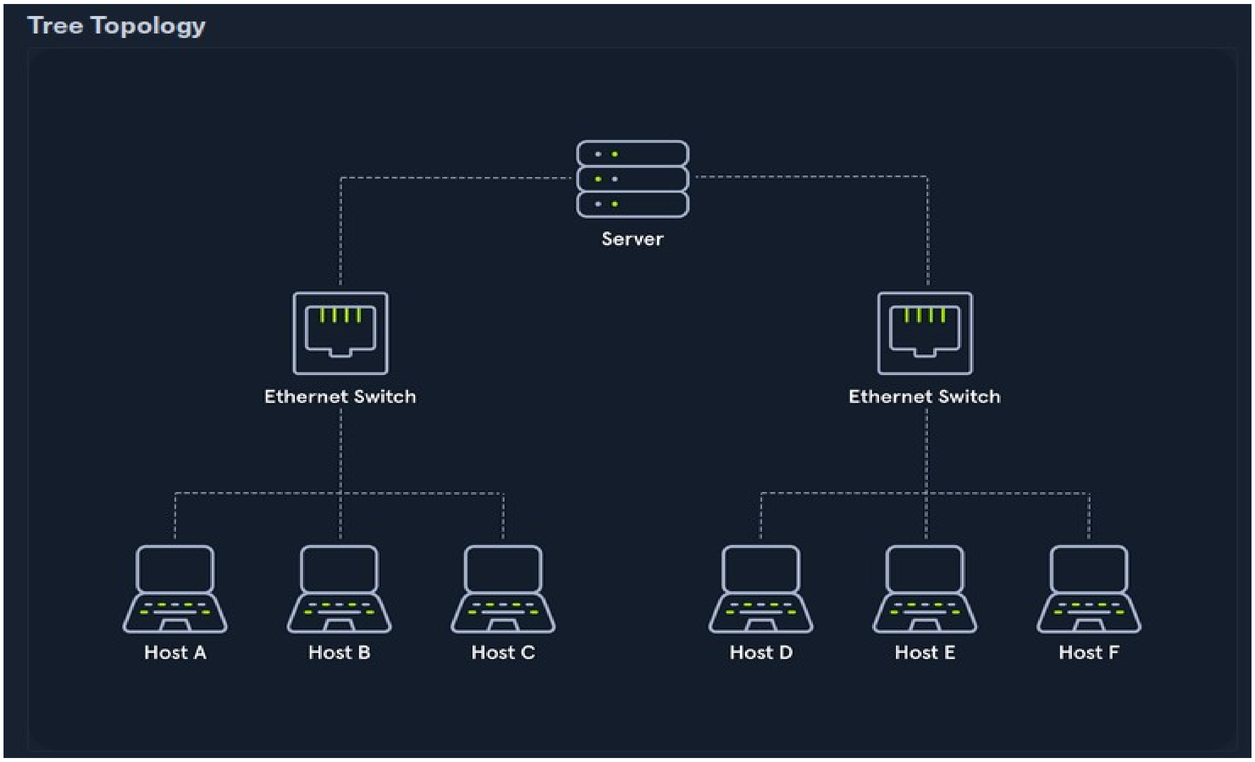
Each host is connected to every other host in the network in a fully meshed structure. This means that the hosts are meshed with each other. This technique is primarily used in WAN or MAN to ensure high reliability and bandwidth.



Tree

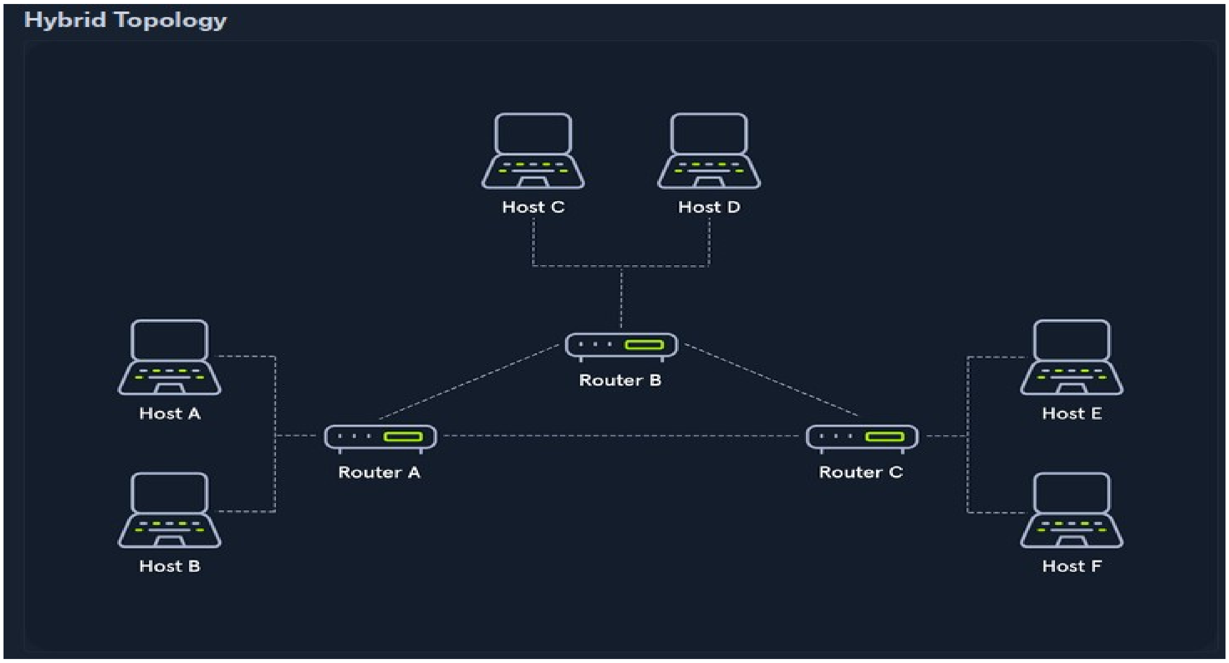
The tree topology is an extended star topology that more extensive local networks have in this structure. This is especially useful when several topologies are combined. This topology is often used, for example, in larger company buildings.

There are both logical tree structures according to the spanning tree and physical ones. Modular modern networks, based on structured cabling with a hub hierarchy, also have a tree structure. Tree topologies are also used for broadband networks and city networks (MAN).



Hybrid

Hybrid networks combine two or more topologies so that the resulting network does not present any standard topologies. For example, a tree network can represent a hybrid topology in which star networks are connected via interconnected bus networks. However, a tree network that is linked to another tree network is still topologically a tree network. A hybrid topology is always created when two different basic network topologies are interconnected.

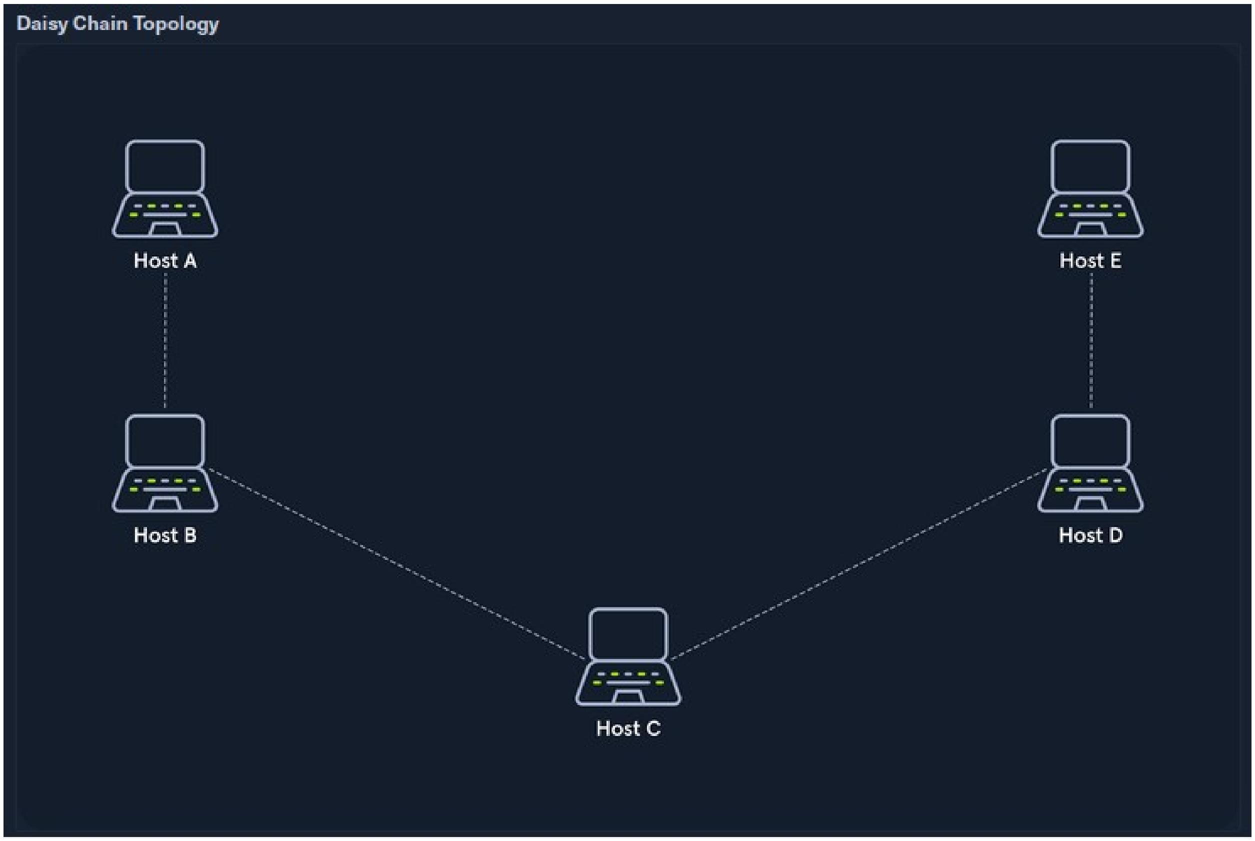


Daisy Chain

In the daisy chain topology, multiple hosts are connected by placing a cable from one node to another.

Since this creates a chain of connections, it is also known as a daisy-chain configuration in which multiple hardware components are connected in a series. This type of networking is often found in automation technology (CAN).

Daisy chaining is based on the physical arrangement of the nodes, in contrast to token procedures, which are structural but can be made independent of the physical layout. The signal is sent to and from a component via its previous nodes to the computer system.



Proxies

A proxy is when a device or service sits in the middle of a connection and acts as a mediator. The mediator is the critical piece of information because it means the device in the middle must be able to inspect the contents of the traffic. Without the ability to be a mediator, the device is technically a gateway, not a proxy.

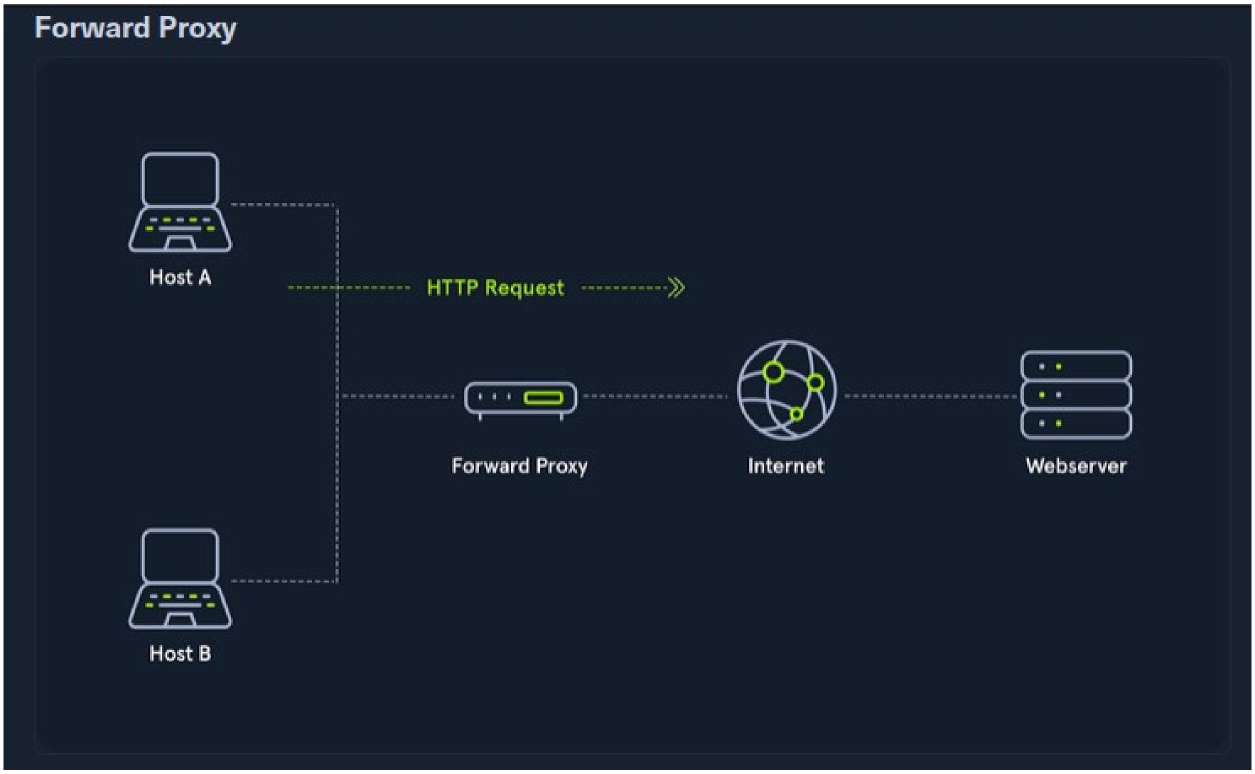
Prooxies will almost always operate at Layer 7 of the OSI Model. There are many types of proxy services, but the key ones are:

- Dedicated Proxy / Forward Proxy

- Reverse Proxy
- Transparent Proxy

Dedicated Proxy / Forward Proxy

A Forward Proxy is when a client makes a request to a computer, and that computer carries out the request.

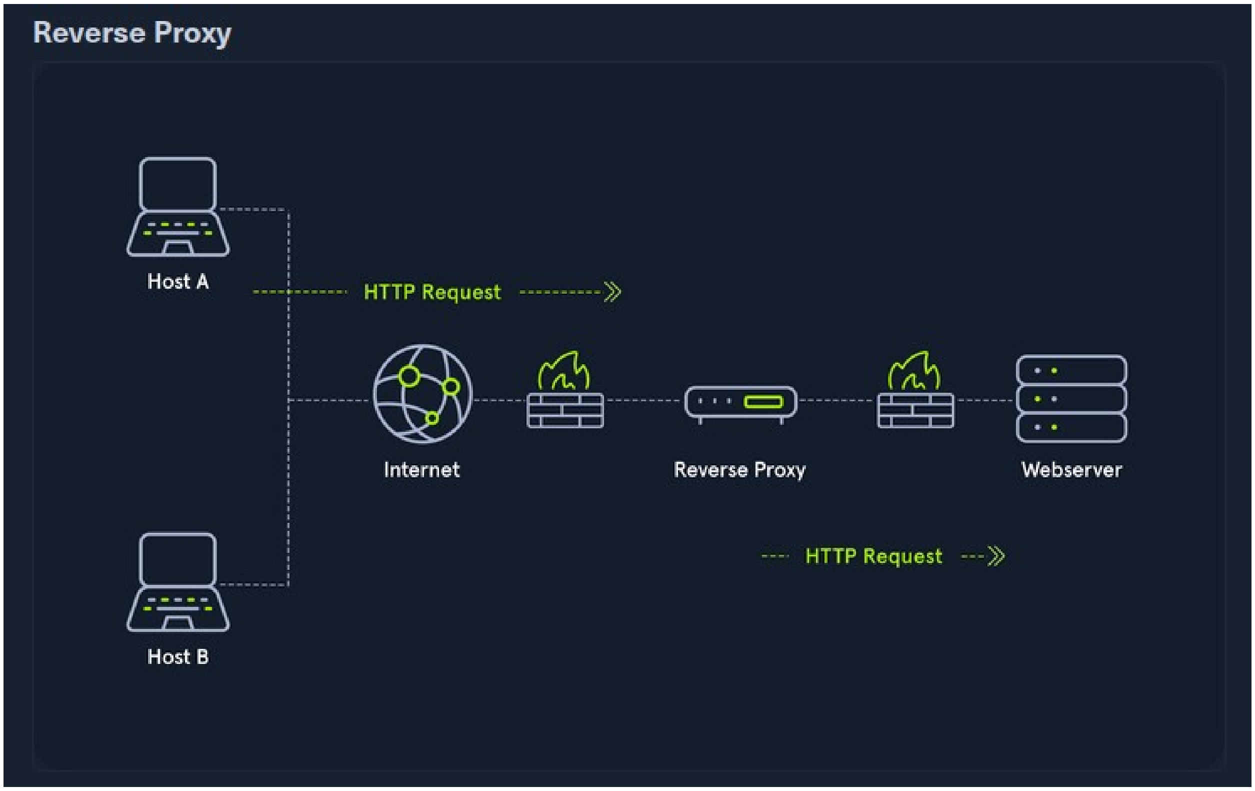


Reverse Proxy

Instead of being designed to filter outgoing requests, it filters incoming ones. The most common goal with a Reverse Proxy, is to listen on an address and forward it to a closed-off network.

Many organizations use CloudFlare as they have a robust network that can withstand most DDOS Attacks. By using Cloudflare, organizations have a way to filter the amount (and type) of traffic that gets sent to their webservers.

As a Penetration Tester you will configure reverse proxies on infected endpoints. The infected endpoint will listen on a port and send any client that connects to the port back to the attacker through the infected endpoint. This is useful to bypass firewalls or evade logging. Organizations may have IDS (Intrusion Detection Systems), watching external web requests. If the attacker gains access to the organization over SSH, a reverse proxy can send web requests through the SSH Tunnel and evade the IDS.



(Non-) Transparent Proxy

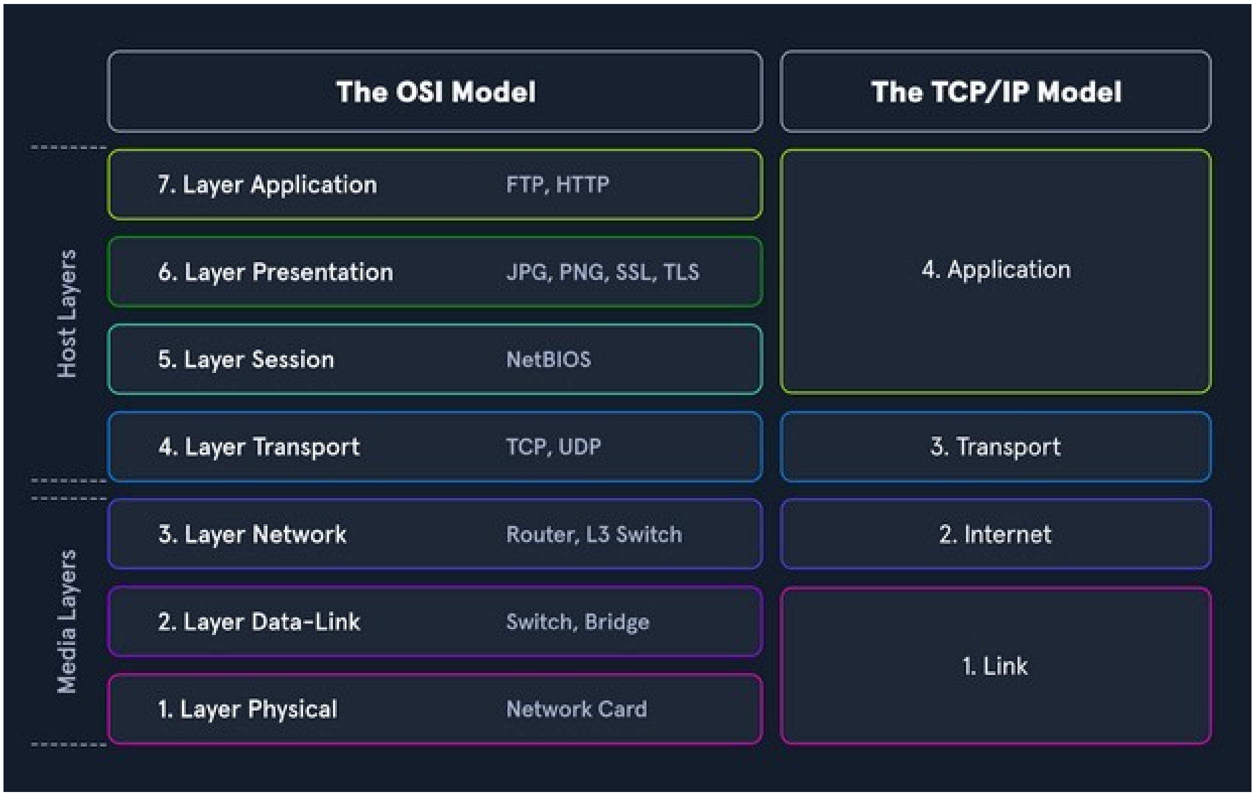
All these proxy services act either transparently or non-transparently.

With a transparent proxy, the client doesn't know about its existence. The transparent proxy intercepts the client's communication requests to the Internet and acts as a substitute instance. To the outside, the transparent proxy, like the non-transparent proxy, acts as a communication partner.

If it is a non-transparent proxy, we must be informed about its existence. For this purpose, we and the software we want to use are given a special proxy configuration that ensures that traffic to the Internet is first addressed to the proxy. If this configuration does not exist, we cannot communicate via the proxy.

Networking Models

Two networking models describe the communication and transfer of data from one host to another, called **ISO/OSI model** and the **TCP/IP model**.



The OSI Model

The OSI model, often referred to as ISO/OSI layer model, is a reference model that can be used to describe and define the communication between systems. The reference model has seven individual layers, each with clearly separated tasks.

The term OSI stands for Open Systems Interconnection model, published by the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO). Therefore, the OSI model is often referred to as the ISO/OSI layer model.

The TCP/IP Model

TCP/IP (Transmission Control Protocol/Internet Protocol) is a generic term for many network protocols. The protocols are responsible for the switching and transport of data packets on the Internet. The Internet is entirely based on the TCP/IP protocol family. However, TCP/IP does not only refer to these two protocols but is usually used as a generic term for an entire protocol family.

For example, ICMP (Internet Control Message Protocol) or UDP (User Datagram Protocol) belongs to the protocol family. The protocol family provides the necessary functions for transporting and switching data packets in a private or public network.

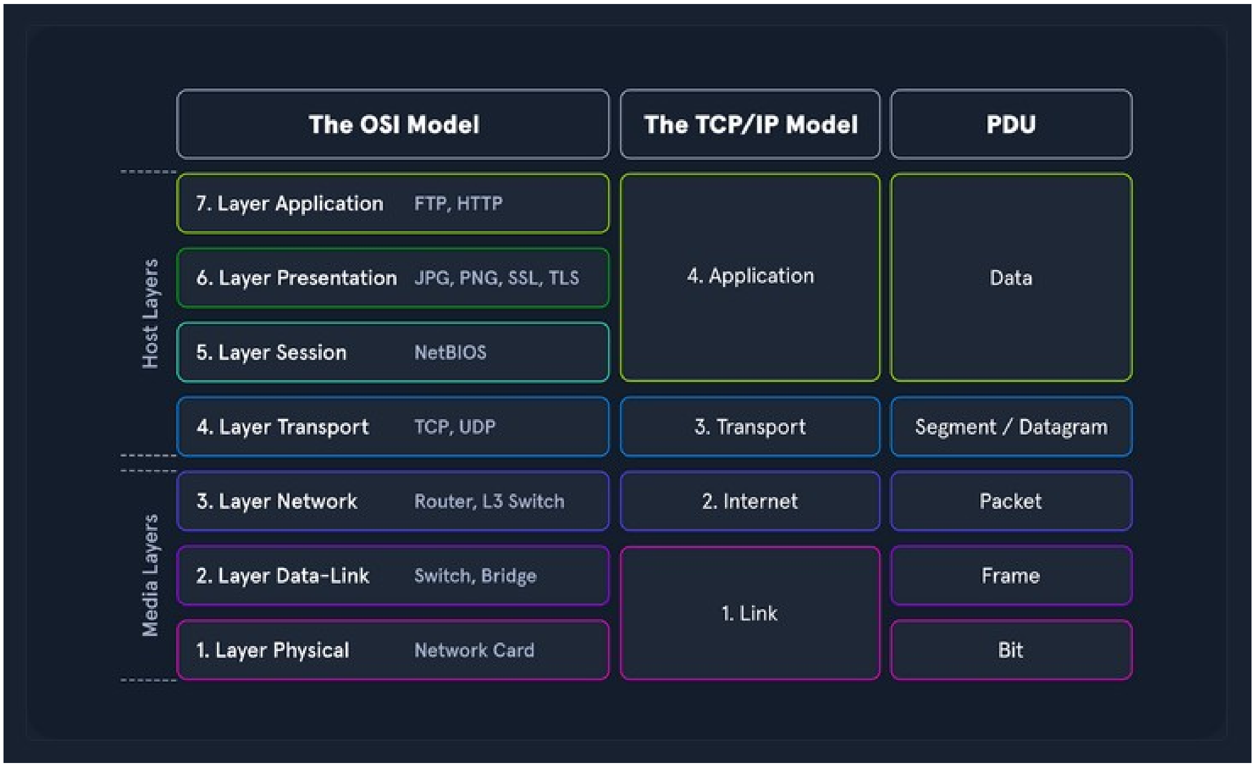
ISO/OSI vs. TCP/IP

TCP/IP is a communication protocol that allows hosts to connect to the Internet. It refers to the Transmission Control Protocol used in and by applications on the Internet. In contrast to OSI, it allows a lightening of the rules that must be followed, provided that general guidelines are followed.

OSI, on the other hand, is a communication gateway between the network and end-users. The OSI model is usually referred to as the reference model because it is older. It is also known for its strict protocol and limitations.

Packet Transfers

In a layered system, devices in a layer exchange data in a different format called a protocol data unit (PDU).



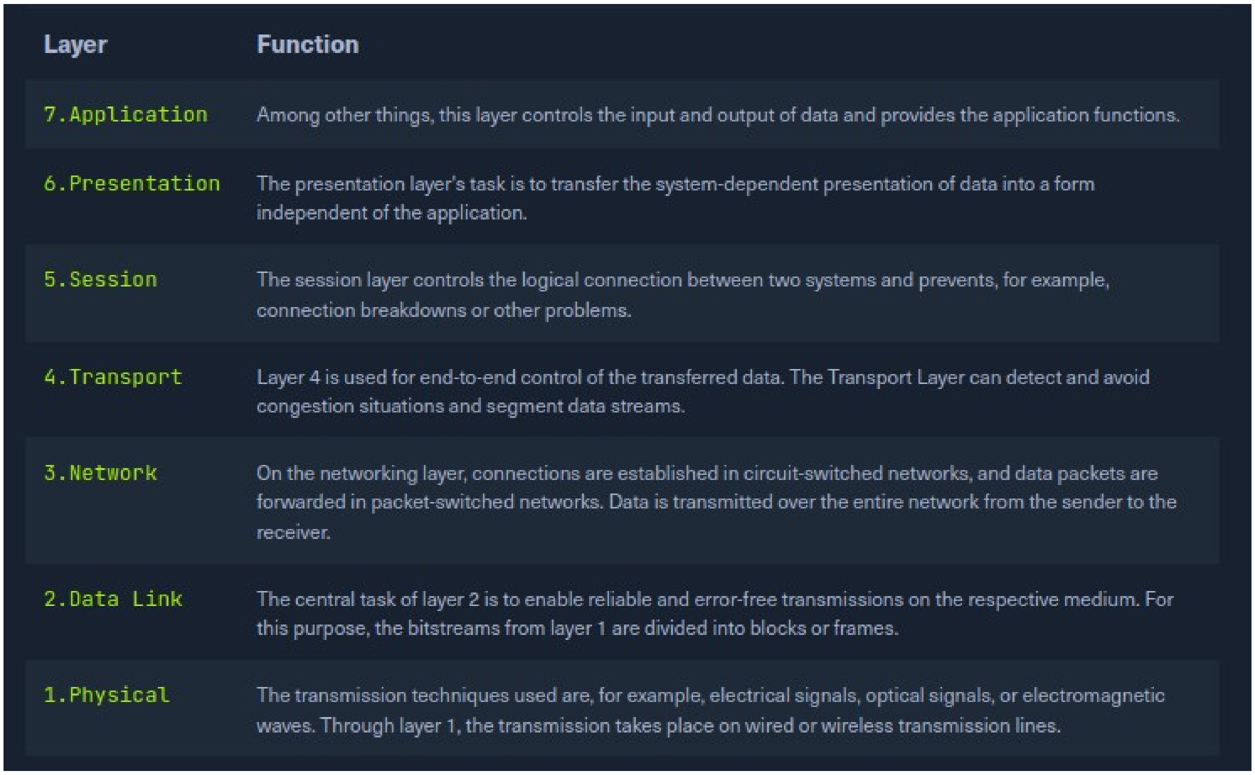
	The OSI Model		The TCP/IP Model	PDU
Host Layers	7. Layer Application	FTP, HTTP	4. Application	Data
	6. Layer Presentation	JPG, PNG, SSL, TLS		
	5. Layer Session	NetBIOS		
	4. Layer Transport	TCP, UDP	3. Transport	Segment / Datagram
Media Layers	3. Layer Network	Router, L3 Switch	2. Internet	Packet
	2. Layer Data-Link	Switch, Bridge	1. Link	Frame
	1. Layer Physical	Network Card		Bit

During the transmission, each layer adds a header to the PDU from the upper layer, which controls and identifies the packet. This process is called encapsulation. The header and the data together form the PDU for the next layer. The process continues to the Physical Layer or Network Layer, where the data is transmitted to the receiver. The receiver reverses the process and unpacks the data on each layer with the header information. After that, the application finally uses the data. This process continues until all data has been sent and received.

With TCP/IP, we can quickly understand how the entire connection is established, and with ISO, we can take it apart piece by piece and analyze it in detail. This often happens when we can listen to and intercept specific network traffic. We then have to analyze this traffic accordingly.

The OSI Model

The goal in defining the ISO/OSI standard was to create a reference model that enables the communication of different technical systems via various devices and technologies and provides compatibility. The OSI model uses ***seven*** different layers, which are hierarchically based on each other to achieve this goal. These layers represent phases in the establishment of each connection through which the sent packets pass.



Layer	Function
`7.Application`	Among other things, this layer controls the input and output of data and provides the application functions.
`6.Presentation`	The presentation layer's task is to transfer the system-dependent presentation of data into a form independent of the application.
`5.Session`	The session layer controls the logical connection between two systems and prevents, for example, connection breakdowns or other problems.
`4.Transport`	Layer 4 is used for end-to-end control of the transferred data. The Transport Layer can detect and avoid congestion situations and segment data streams.
`3.Network`	On the networking layer, connections are established in circuit-switched networks, and data packets are forwarded in packet-switched networks. Data is transmitted over the entire network from the sender to the receiver.
`2.Data Link`	The central task of layer 2 is to enable reliable and error-free transmissions on the respective medium. For this purpose, the bitstreams from layer 1 are divided into blocks or frames.
`1.Physical`	The transmission techniques used are, for example, electrical signals, optical signals, or electromagnetic waves. Through layer 1, the transmission takes place on wired or wireless transmission lines.

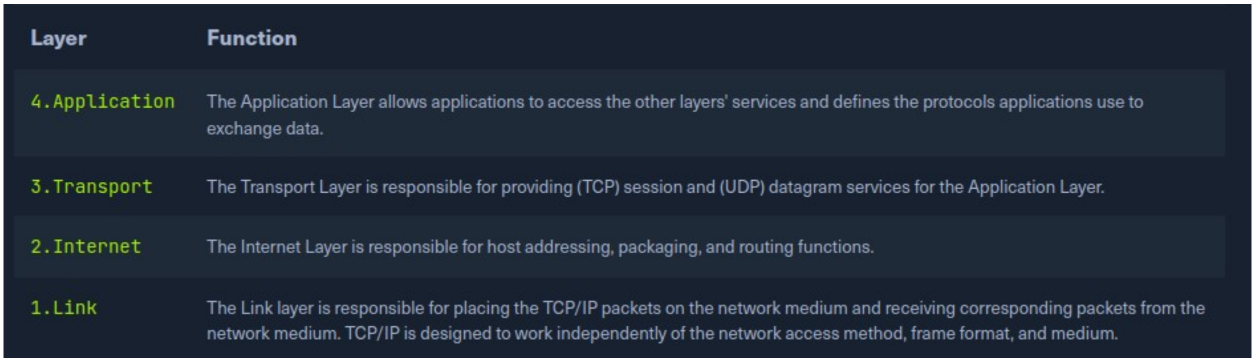
The layers 2-4 are **transport oriented**, and the layers 5-7 are **application oriented layers**. In each layer, precisely defined tasks are performed, and the interfaces to the neighboring layers are precisely described. Each layer offers services for use to the layer directly above it. To make these services available, the layer uses the services of the layer below it and performs the tasks of its layer.

If two systems communicate, all seven layers of the OSI model are run through at least twice, since both the sender and the receiver must take the layer model into account.

When an application sends a packet to the other system, the system works the layers shown above from layer 7 down to layer 1, and the receiving system unpacks the received packet from layer 1 up to layer 7.

The TCP/IP Model

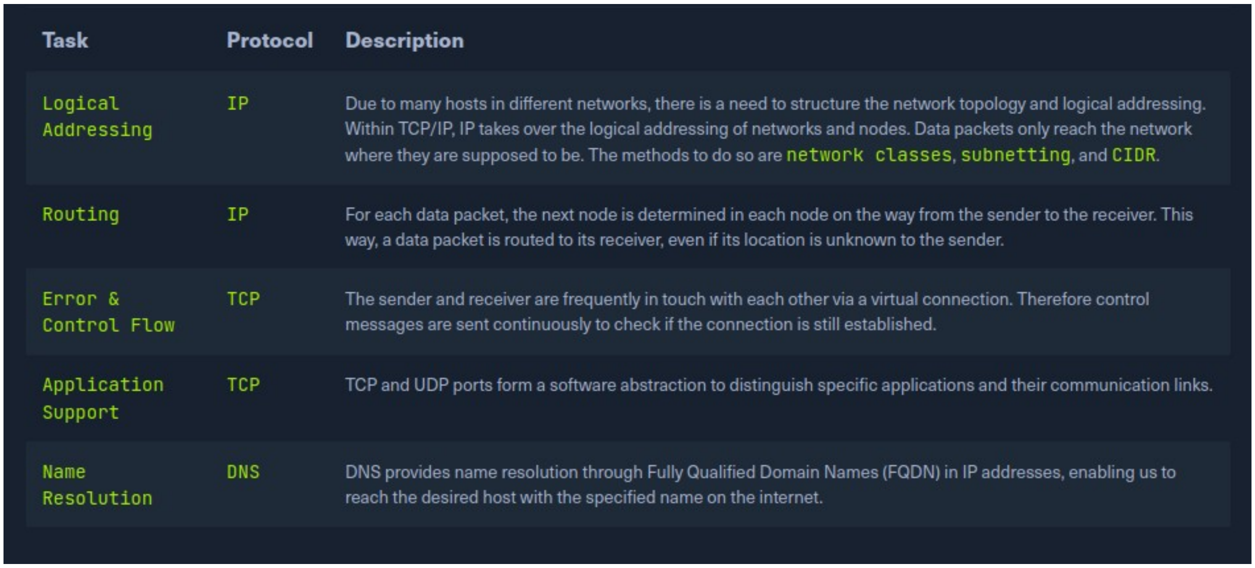
The TCP/IP model is also a layered reference model, often referred to as the **Internet Protocol Suite**. The term TCP/IP stands for the two protocols **Transmission Control Protocol (TCP)** and **Internet Protocol (IP)**. IP is located within the **network layer (Layer 3)** and TCP is located within the **transport layer (Layer 4)** of the OSI layer model.



Layer	Function
`4.Application`	The Application Layer allows applications to access the other layers' services and defines the protocols applications use to exchange data.
`3.Transport`	The Transport Layer is responsible for providing (TCP) session and (UDP) datagram services for the Application Layer.
`2.Internet`	The Internet Layer is responsible for host addressing, packaging, and routing functions.
`1.Link`	The Link layer is responsible for placing the TCP/IP packets on the network medium and receiving corresponding packets from the network medium. TCP/IP is designed to work independently of the network access method, frame format, and medium.

With TCP/IP, every application can transfer and exchange data over any network, and it does not matter where the receiver is located. IP ensures that the data packet reaches its destination, and TCP controls the data transfer and ensures the connection between data stream and application. The main difference between TCP/IP and OSI is the number of layers, some of which have been combined.

Important tasks of TCP/IP are:



Task	Protocol	Description
`Logical Addressing`	`IP`	Due to many hosts in different networks, there is a need to structure the network topology and logical addressing. Within TCP/IP, IP takes over the logical addressing of networks and nodes. Data packets only reach the network where they are supposed to be. The methods to do so are `network classes`, `subnetting`, and `CIDR`.
`Routing`	`IP`	For each data packet, the next node is determined in each node on the way from the sender to the receiver. This way, a data packet is routed to its receiver, even if its location is unknown to the sender.
`Error & Control Flow`	`TCP`	The sender and receiver are frequently in touch with each other via a virtual connection. Therefore control messages are sent continuously to check if the connection is still established.
`Application Support`	`TCP`	TCP and UDP ports form a software abstraction to distinguish specific applications and their communication links.
`Name Resolution`	`DNS`	DNS provides name resolution through Fully Qualified Domain Names (FQDN) in IP addresses, enabling us to reach the desired host with the specified name on the internet.

Network Layer

The network layer (Layer 3) of OSI controls the exchange of data packets, as these cannot be directly routed to the receiver and therefore have to be provided with routing nodes. The data packets are then transferred from node to node until they reach their target. To implement this, the network layer identifies the individual network nodes, sets up and clears connection channels, and takes care of routing and data flow control. When sending the packets, addresses are evaluated, and the data is routed through the network from node to node.

The network layer is responsible for the following functions:

- Logical Addressing
- Routing

Protocols are defined in each layer of OSI, and these protocols represent a collection of rules for communication in the respective layer and most used protocols on this layer are:

- IPv4 / IPv6
- IPsec
- ICMP
- IGMP
- RIP
- OSPF

IP Addresses

Each host in the network located can be identified by the so-called Media Access Control address (MAC). This would allow data exchange within this one network. If the remote host is located in another network, knowledge of the MAC address is not enough to establish a connection. Addressing on the Internet is done via the IPv4 and/or IPv6 address, which is made up of the network address and the host address.

The representation of MAC and IPv4 / IPv6 addresses as follows:

- IPv4 / IPv6 - describes the unique postal address and district of the receiver's building.
- MAC - describes the exact floor and apartment of the receiver.

It is possible for a single IP address to address multiple receivers (broadcasting) or for a device to respond to multiple IP addresses. However, it must be ensured that each IP address is assigned only once within the network.

IPv4 Structure

The most common method of assigning IP addresses is IPv4, which consists of a 32-bit binary number combined into 4 bytes consisting of 8-bit groups (octets) ranging from 0-255. These are converted into more easily readable decimal numbers, separated by dots and represented as dotted-decimal notation.

Thus an IPv4 address can look like this:

Notation	Presentation
Binary	0111 1111.0000 0000.0000 0000.0000 0001
Decimal	127.0.0.1

The IPv4 format allows 4,294,967,296 unique addresses. The IP address is divided into a host part and a network part. The router assigns the host part of the IP address at home or by an administrator. The respective network administrator assigns the network part. On the Internet, this is IANA, which allocates and manages the unique IPs.

IP network blocks are divided into classes A - E. The different classes differed in the host and network shares' respective lengths.

Class	Network Address	First Address	Last Address	Subnetmask	CIDR	Subnets	IPs
A	1.0.0.0	1.0.0.1	127.255.255.255	255.0.0.0	/8	127	16,777,214 + 2
B	128.0.0.0	128.0.0.1	191.255.255.255	255.255.0.0	/16	16,384	65,534 + 2
C	192.0.0.0	192.0.0.1	223.255.255.255	255.255.255.0	/24	2,097,152	254 + 2
D	224.0.0.0	224.0.0.1	239.255.255.255	Multicast	Multicast	Multicast	Multicast
E	240.0.0.0	240.0.0.1	255.255.255.255	reserved	reserved	reserved	reserved

Subnet Mask

A further separation of these classes into small networks is done with the help of subnetting. This separation is done using the netmasks, which is as long as an IPv4 address. As with classes, it describes which bit positions within the IP address act as network part or host part.

Network and Gateway Addresses

The two additional IPs added in the IPs column are reserved for the so-called network address and the broadcast address. Another important role plays the default gateway, which is the name for the IPv4 address of the router that couples networks and systems with different protocols and manages addresses and transmission methods. It is common for the default gateway to be assigned the first or last assignable IPv4 address in a subnet.

Broadcast Address

The broadcast IP address's task is to connect all devices in a network with each other. Broadcast in a network is a message that is transmitted to all participants of a network and does not require any response. In this way, a host sends a data packet to all other participants of the network simultaneously and, in doing so, communicates its IP address, which the receivers can use to contact it. This is the last IPv4 address that is used for the broadcast.

Binary system

The binary system is a number system that uses only two different states that are represented into two numbers (0 and 1) opposite to the decimal-system (0 to 9).

An IPv4 address is divided into 4 octets, as we have already seen. Each octet consists of 8 bits. Each position of a bit in an octet has a specific decimal value. Let's take the following IPv4 address as an example:

- IPv4 Address: 192.168.10.39

Values:	128	64	32	16	8	4	2	1
Binary:	1	1	0	0	0	0	0	0

Octet:	1st		2nd		3rd		4th
Binary:	1100 0000	.	1010 1000	.	0000 1010	.	0010 0111
Decimal:	192	.	168	.	10	.	39

CIDR

Classless Inter-Domain Routing (CIDR) is a method of representation and replaces the fixed assignment between IPv4 address and network classes (A, B, C, D, E). The division is based on the subnet mask or the so-called CIDR suffix, which allows the bitwise division of the IPv4 address space and thus into subnets of any size. The CIDR suffix indicates how many bits from the beginning of the IPv4 address belong to the network. It is a notation that represents the subnet mask by specifying the number of 1-bits in the subnet mask.

The following IPv4 address and subnet mask as an example:

- IPv4 Address: 192.168.10.39
- Subnet mask: 255.255.255.0

Now the whole representation of the IPv4 address and the subnet mask would look like this:

- CIDR: 192.168.10.39/24

The CIDR suffix is, therefore, the sum of all ones in the subnet mask.

Subnetting

The division of an address range of IPv4 addresses into several smaller address ranges is called ***subnetting***. A subnet is a logical segment of a network that uses IP addresses with the same network address.

With the help of subnetting, we can create a specific subnet by ourselves or find out the following outline of the respective network:

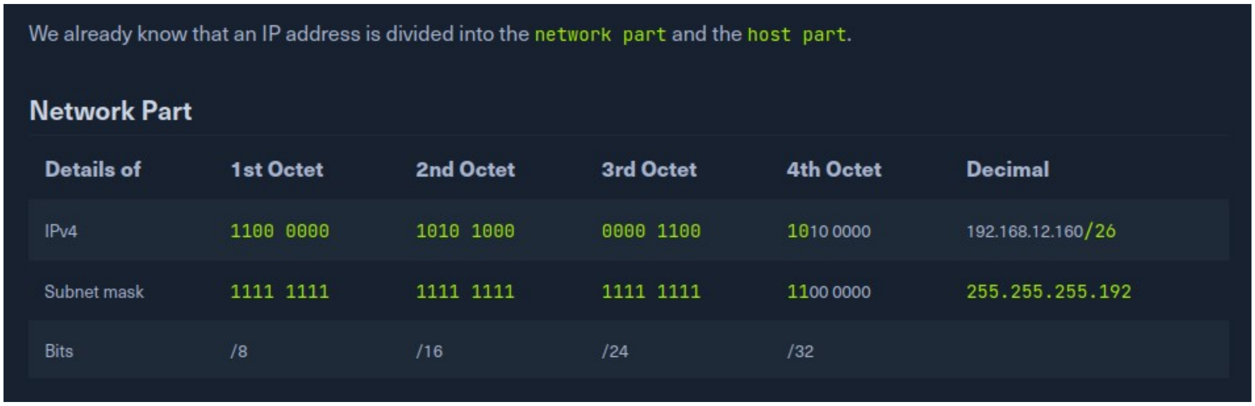
- Network address
- Broadcast address
- First host
- Last host
- Number of hosts

Take the following IPv4 address and subnet mask as an example:

IPv4 Address: 192.168.12.160

Subnet Mask: 255.255.255.192

CIDR: 192.168.12.160/26



We already know that an IP address is divided into the `network part` and the `host part`.

Network Part

Details of	1st Octet	2nd Octet	3rd Octet	4th Octet	Decimal
IPv4	1100 0000	1010 1000	0000 1100	1010 0000	192.168.12.160/26
Subnet mask	1111 1111	1111 1111	1111 1111	1100 0000	255.255.255.192
Bits	/8	/16	/24	/32	

In subnetting, we use the subnet mask as a template for the IPv4 address. From the 1-bits in the subnet mask, we know which bits in the IPv4 address cannot be changed. These are fixed and therefore determine the "main network" in which the subnet is located.

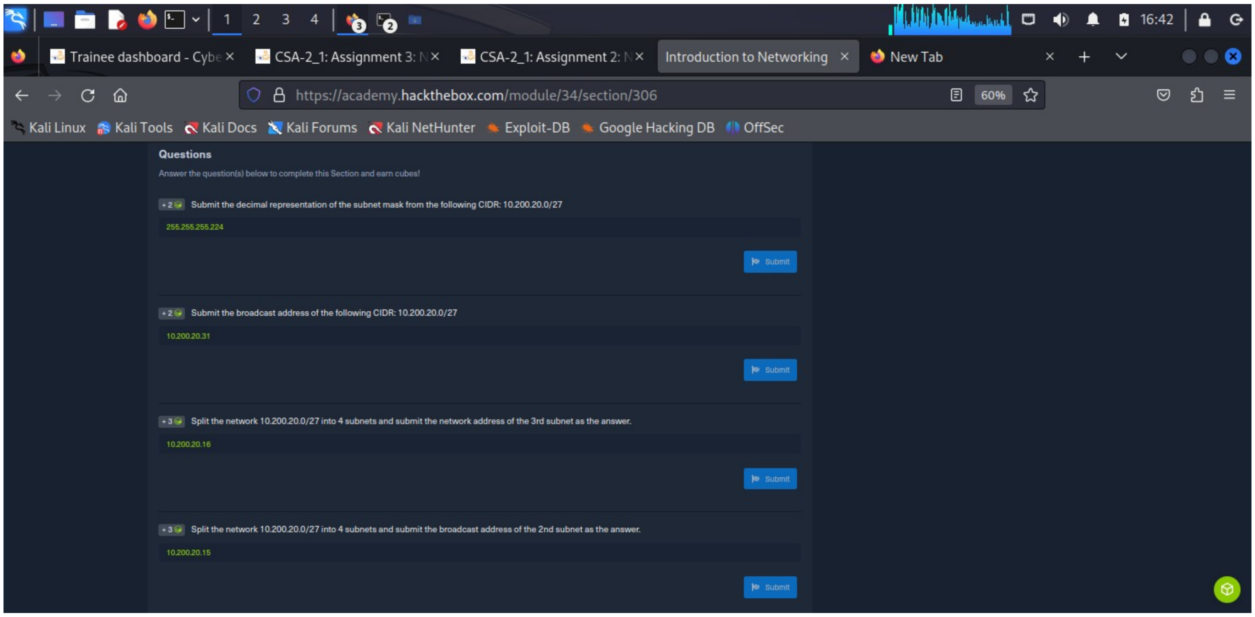
Host Part

Details of	1st Octet	2nd Octet	3rd Octet	4th Octet	Decimal
IPv4	1100 0000	1010 1000	0000 1100	1010 0000	192.168.12.160/26
Subnet mask	1111 1111	1111 1111	1111 1111	1100 0000	255.255.255.192
Bits	/8	/16	/24	/32	

The bits in the host part can be changed to the first and last address. The first address is the network address, and the last address is the broadcast address for the respective subnet.

The network address is vital for the delivery of a data packet. If the network address is the same for the source and destination address, the data packet is delivered within the same subnet. If the network addresses are different, the data packet must be routed to another subnet via the default gateway.

The subnet mask determines where this separation occurs.



Questions

Answer the question(s) below to complete this Section and earn cubes!

+2 Submit the decimal representation of the subnet mask from the following CIDR: 10.200.20.0/27

255.255.255.224

Submit

+2 Submit the broadcast address of the following CIDR: 10.200.20.0/27

10.200.20.31

Submit

+3 Split the network 10.200.20.0/27 into 4 subnets and submit the network address of the 3rd subnet as the answer.

10.200.20.16

Submit

+3 Split the network 10.200.20.0/27 into 4 subnets and submit the broadcast address of the 2nd subnet as the answer.

10.200.20.15

Submit

Since we now know that the IPv4 addresses 192.168.12.128 and 192.168.12.191 are assigned, all other IPv4 addresses are accordingly between 192.168.12.129-190. Now we know that this subnet offers us a total of 64 - 2 (network address & broadcast address) or 62 IPv4 addresses that we can assign to our hosts.

Hosts	**IPv4**
Network Address	192.168.12.128
First Host	192.168.12.129
Other Hosts	...
Last Host	192.168.12.190
Broadcast Address	192.168.12.191

Subnetting Into Smaller Networks

Let us now assume that we, as administrators, have been given the task of dividing the subnet assigned to us into 4 additional subnets. Thus, it is essential to know that we can only divide the subnets based on the binary system.

Exponent	**Value**
2^0	= 1
2^1	= 2

Exponent	**Value**
2^2	= 4
2^3	= 8
2^4	= 16
2^5	= 32
2^6	= 64
2^7	= 128
2^8	= 256

Therefore we can divide the 64 hosts we know by 4. The 4 is equal to the exponent 2^2 in the binary system, so we find out the number of bits for the subnet mask by which we have to extend it. So we know the following parameters:

- Subnet: 192.168.12.128/26
- Required Subnets: 4

Now we increase/expand our subnet mask by 2 bits from /26 to /28, and it looks like this:

Details of	**1st Octet**	**2nd Octet**	**3rd Octet**	**4th Octet**	**Decimal**
IPv4	1100 0000	1010 1000	0000 1100	1000| 0000	192.168.12.128/28
Subnet mask	1111 1111	1111 1111	1111 1111	1111| 0000	255.255.255.240
Bits	/8	/16	/24	/32	

Next, we can divide the 64 IPv4 addresses that are available to us into 4 parts:

Hosts	**Math**	**Subnets**	**Host range for each subnet**
64	/	4	= 16

So we know how big each subnet will be. From now on, we start from the network address given to us (192.168.12.128) and add the 16 hosts 4 times:

Subnet No.	**Network Address**	**First Host**	**Last Host**	**Broadcast Address**	**CIDR**
1	192.168.12.128	192.168.12.129	192.168.12.142	192.168.12.143	192.168.12.128/28
2	192.168.12.144	192.168.12.145	192.168.12.158	192.168.12.159	192.168.12.144/28
3	192.168.12.160	192.168.12.161	192.168.12.174	192.168.12.175	192.168.12.160/28
4	192.168.12.176	192.168.12.177	192.168.12.190	192.168.12.191	192.168.12.176/28

Mental Subnetting

Each octet repeats itself, and everything is a power of two, so there doesn't have to be a lot of memorization. The first thing to do is identify what octet changes.

1st Octet	2nd Octet	3rd Octet	4th Octet
/8	/16	/24	/32

It is possible to identify what octet of the IP Address may change by remembering those four numbers. Given the Network Address: 192.168.1.1/25, it is immediately apparent that 192.168.2.4 would not be in the same network because the /25 subnet means only the fourth octet may change.

The next part identifies how big each subnet can be but by dividing eight by the network and looking at the remainder. This is also called Modulo Operation (%) and is heavily utilized in cryptology. Given our previous example of /25, (25 % 8) would be 1. This is because eight goes into 25 three times (8 * 3 = 24). There is a 1 leftover, which is the network bit reserved for the network mask. There is a total of eight bits in each octet of an IP Address. If one is used for the network mask, the equation becomes 2^(8-1) or 2^7, 128. The table below contains all the numbers.

Remainder	Number	Exponential Form	Division Form
0	256	2^8	256
1	128	2^7	256/2
2	64	2^6	256/2/2
3	32	2^5	256/2/2/2
4	16	2^4	256/2/2/2/2
5	8	2^3	256/2/2/2/2/2
6	4	2^2	256/2/2/2/2/2/2
7	2	2^1	256/2/2/2/2/2/2/2

By remembering the powers of two up to eight, it can become an instant calculation. However, if forgotten, it may be quicker to remember to divide 256 in half the number of times of the remainder.

The tricky part of this is getting the actual IP Address range because 0 is a number and not null in networking. So in our /25 with 128 IP Addresses, the first range is 192.168.1.0-127. The first address is the network, and the last is the broadcast address, which means the usable IP Space would become 192.168.1.1-126. If our IP Address fell above 128, then the usable ip space would be 192.168.129-254 (128 is the network and 255 is the broadcast).

MAC Addresses

MAC is the physical address for our network interfaces. Each host in a network has its own 48-bit (6 octets) Media Access Control (MAC) address, represented in hexadecimal format. There are several different standards for the MAC address:

- Ethernet (IEEE 802.3)
- Bluetooth (IEEE 802.15)
- WLAN (IEEE 802.11)

This is because the MAC address addresses the physical connection (network card, Bluetooth, or WLAN adapter) of a host. Each network card has its individual MAC address, which is configured once on the manufacturer's hardware side but can always be changed, at least temporarily.

Let's have a look at an example of such a MAC address:

MAC address:

- DE:AD:BE:EF:13:37
- DE-AD-BE-EF-13-37
- DEAD.BEEF.1337

Representation	**1st Octet**	**2nd Octet**	**3rd Octet**	**4th Octet**	**5th Octet**	**6th Octet**
Binary	1101 1110	1010 1101	1011 1110	1110 1111	0001 0011	0011 0111
Hex	DE	AD	BE	EF	13	37

It is also to be noted that Address Resolution Protocol (ARP) is used in IPv4 to determine the MAC addresses associated with the IP addresses.

The last two bits in the first octet can play another essential role. The last bit identifies the MAC address as Unicast (0) or Multicast (1). With unicast, it means that the packet sent will reach only one specific host.

With multicast, the packet is sent only once to all hosts on the local network, which then decides whether or not to accept the packet based on their configuration. The multicast address is a unique address, just like the broadcast address, which has fixed octet values. Broadcast in a network represents a broadcasted call, where data packets are transmitted simultaneously from one point to all members of a network. It is mainly used if the address of the receiver of the packet is not yet known. An example is the ARP (for MAC addresses) and DHCP (for IPv4 addresses) protocols.

Address Resolution Protocol

MAC addresses can be changed/manipulated or spoofed, and as such, they should not be relied upon as a sole means of security or identification. Network administrators should implement additional security measures, such as network segmentation and strong authentication protocols, to protect against potential attacks.

There exist several attack vectors that can potentially be exploited through the use of MAC addresses:

MAC spoofing: This involves altering the MAC address of a device to match that of another device, typically to gain unauthorized access to a network.

MAC flooding: This involves sending many packets with different MAC addresses to a network switch, causing it to reach its MAC address table capacity and effectively preventing it from functioning correctly.

MAC address filtering: Some networks may be configured only to allow access to devices with specific MAC addresses that we could potentially exploit by attempting to gain access to the network using a spoofed MAC address.

Address Resolution Protocol

Address Resolution Protocol (ARP) is a network protocol. It is an important part of the network communication used to resolve a network layer (layer 3) IP address to a link layer (layer 2) MAC address. It maps a host's IP address to its corresponding MAC address to facilitate communication between devices on a Local Area Network (LAN). When a device on a LAN wants to communicate with another device, it sends a broadcast message containing the destination IP address and its own MAC address. The device with the matching IP address responds with its own MAC address, and the two devices can then communicate directly using their MAC addresses. This process is known as ARP resolution.

ARP is an important part of the network communication process because it allows devices to send and receive data using MAC addresses rather than IP addresses, which can be more efficient. Two types of request messages can be used:

ARP Request

When a device wants to communicate with another device on a LAN, it sends an ARP request to resolve the destination device's IP address to its MAC address. The request is broadcast to all devices on the LAN and contains the IP address of the destination device. The device with the matching IP address responds with its MAC address.

ARP spoofing, also known as ARP cache poisoning or ARP poison routing, is an attack that can be done using tools like Ettercap or Cain & Abel in which we send falsified ARP messages over a LAN. The goal is to associate our MAC address with the IP address of a legitimate device on the company's network, effectively allowing us to intercept traffic intended for the legitimate device.

We can use ARP poisoning to perform various activities, such as stealing sensitive information, redirecting traffic, or launching MITM attacks. However, to protect against ARP spoofing, it is important to use secure network protocols, such as IPSec or SSL, and to implement security measures, such as firewalls and intrusion detection systems.

IPv6 Addresses

IPv6 is the successor of IPv4. In contrast to IPv4, the IPv6 address is 128 bit long. The prefix identifies the host and network parts. The Internet Assigned Numbers Authority (IANA) is responsible for assigning IPv4 and IPv6 addresses and their associated network portions. In the long term, IPv6 is expected to completely replace IPv4, which is still predominantly used on the Internet. In principle, however, IPv4 and IPv6 can be made available simultaneously (Dual Stack).

IPv6 is a protocol with many new features, which also has many other advantages over IPv4:

- Larger address space
- Address self-configuration (SLAAC)
- Multiple IPv6 addresses per interface
- Faster routing
- End-to-end encryption (IPsec)
- Data packages up to 4 GByte

There are four different types of IPv6 addresses:

Unicast	Addresses for a single interface.
Anycast	Addresses for multiple interfaces, where only one of them receives the packet.
Multicast	Addresses for multiple interfaces, where all receive the same packet.
Broadcast	Do not exist and is realized with multicast addresses.

In total, the IPv6 address consists of 16 bytes. Because of its length, an IPv6 address is represented in a hexadecimal notation. Therefore the 128 bits are divided into 8 blocks multiplied by 16 bits (or 4 hex numbers). All four hex numbers are grouped and separated by a colon (:) instead of a simple dot (.) as in

IPv4. To simplify the notation, we leave out leading at least 4 zeros in the blocks, and we can replace them with two colons (::).

An IPv6 address can look like this:

- Full IPv6: fe80:0000:0000:0000:dd80:b1a9:6687:2d3b/64
- Short IPv6: fe80::dd80:b1a9:6687:2d3b/64

An IPv6 address consists of two parts:

- Network Prefix (network part)
- Interface Identifier also called Suffix (host part)

The Network Prefix identifies the network, subnet, or address range. The Interface Identifier is formed from the 48-bit MAC address of the interface and is converted to a 64-bit address in the process.

In RFC 5952, the aforementioned IPv6 address notation was defined:

- All alphabetical characters are always written in lower case.
- All leading zeros of a block are always omitted.
- One or more consecutive blocks of 4 zeros (hex) are shortened by two colons (::).
- The shortening to two colons (::) may only be performed once starting from the left.

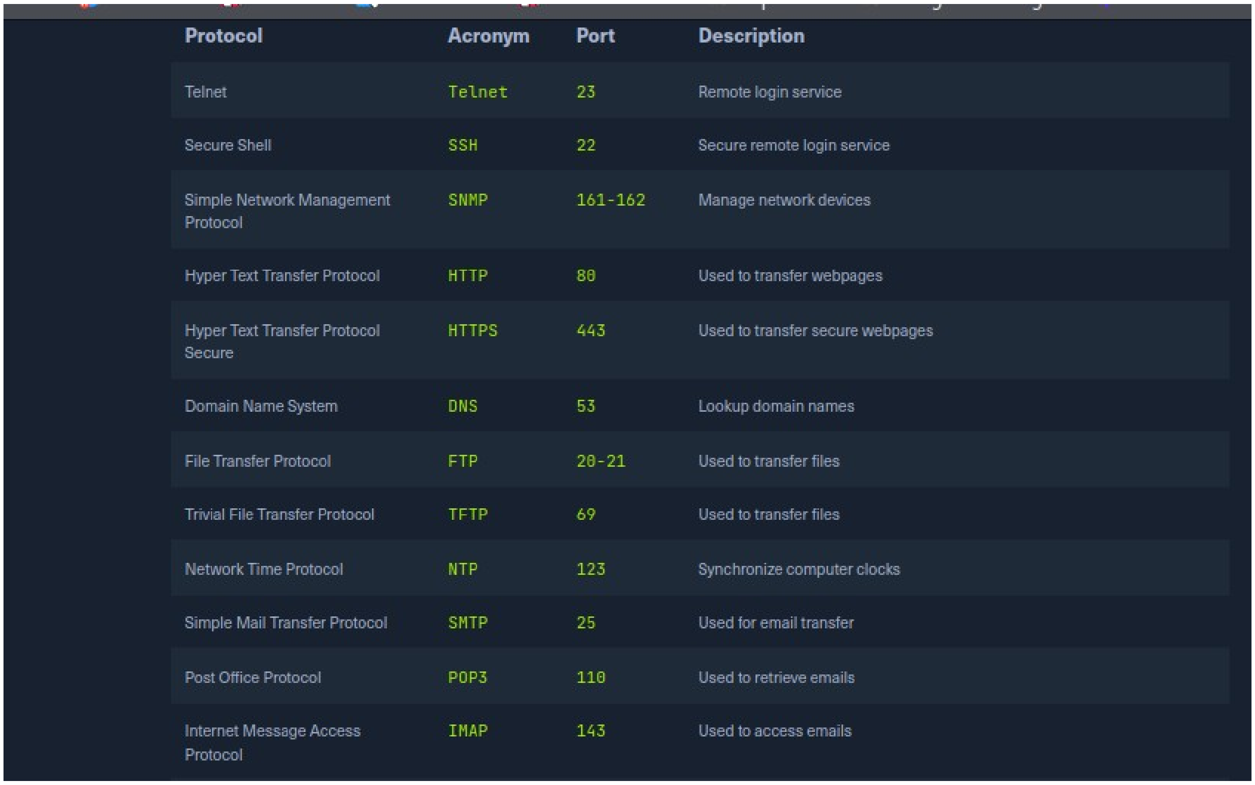
Common Protocols

Internet protocols are standardized rules and guidelines defined in RFCs that specify how devices on a network should communicate with each other. They ensure that devices on a network can exchange information consistently and reliably, regardless of the hardware and software used.

The two main types of connections used on networks are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Transmission Control Protocol

TCP is a connection-oriented protocol that establishes a virtual connection between two devices before transmitting data by using a Three-Way-Handshake. This connection is maintained until the data transfer is complete, and the devices can continue to send data back and forth as long as the connection is active.

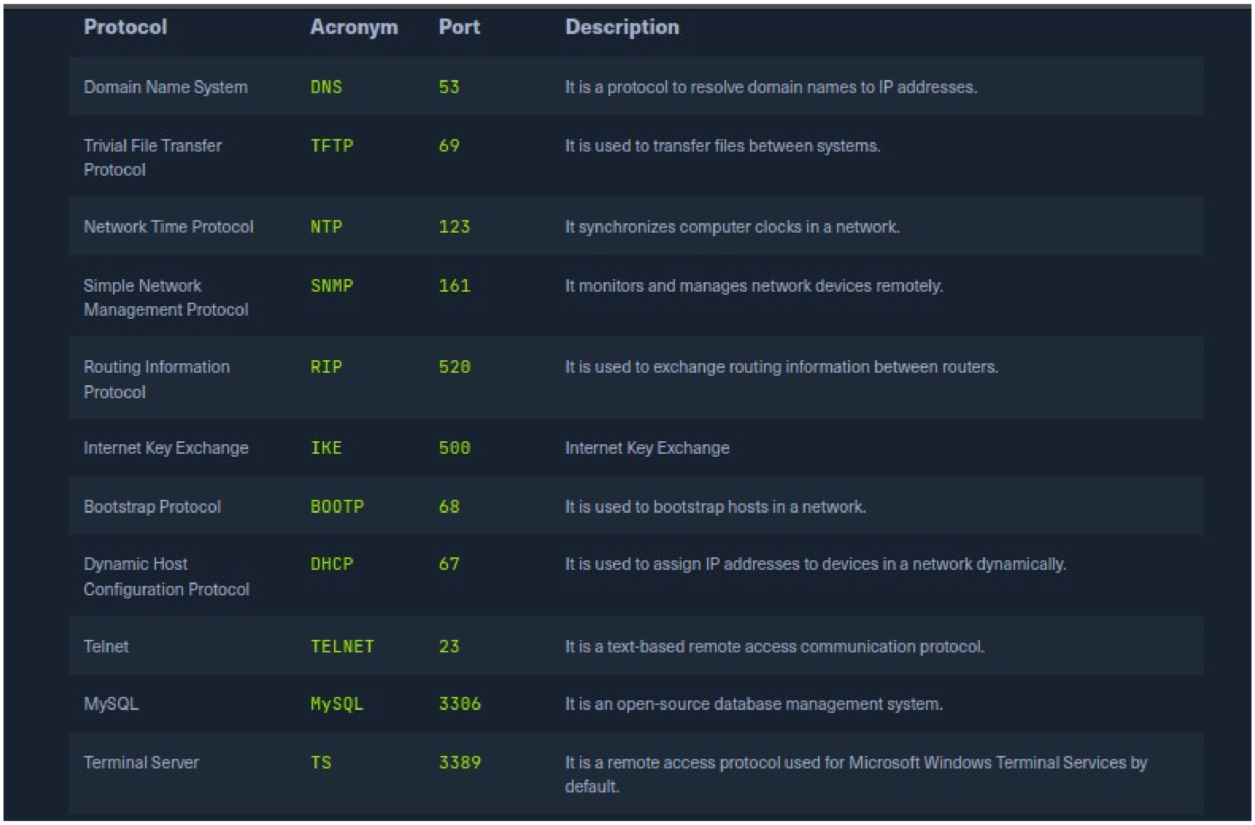


Protocol	Acronym	Port	Description
Telnet	Telnet	23	Remote login service
Secure Shell	SSH	22	Secure remote login service
Simple Network Management Protocol	SNMP	161-162	Manage network devices
Hyper Text Transfer Protocol	HTTP	80	Used to transfer webpages
Hyper Text Transfer Protocol Secure	HTTPS	443	Used to transfer secure webpages
Domain Name System	DNS	53	Lookup domain names
File Transfer Protocol	FTP	20-21	Used to transfer files
Trivial File Transfer Protocol	TFTP	69	Used to transfer files
Network Time Protocol	NTP	123	Synchronize computer clocks
Simple Mail Transfer Protocol	SMTP	25	Used for email transfer
Post Office Protocol	POP3	110	Used to retrieve emails
Internet Message Access Protocol	IMAP	143	Used to access emails

User Datagram Protocol

UDP is a connectionless protocol, which means it does not establish a virtual connection before transmitting data. Instead, it sends the data packets to the destination without checking to see if they were received.

This makes UDP faster than TCP but less reliable because there is no guarantee that the packets will reach their destination.



Protocol	Acronym	Port	Description
Domain Name System	DNS	53	It is a protocol to resolve domain names to IP addresses.
Trivial File Transfer Protocol	TFTP	69	It is used to transfer files between systems.
Network Time Protocol	NTP	123	It synchronizes computer clocks in a network.
Simple Network Management Protocol	SNMP	161	It monitors and manages network devices remotely.
Routing Information Protocol	RIP	520	It is used to exchange routing information between routers.
Internet Key Exchange	IKE	500	Internet Key Exchange
Bootstrap Protocol	BOOTP	68	It is used to bootstrap hosts in a network.
Dynamic Host Configuration Protocol	DHCP	67	It is used to assign IP addresses to devices in a network dynamically.
Telnet	TELNET	23	It is a text-based remote access communication protocol.
MySQL	MySQL	3306	It is an open-source database management system.
Terminal Server	TS	3389	It is a remote access protocol used for Microsoft Windows Terminal Services by default.

ICMP

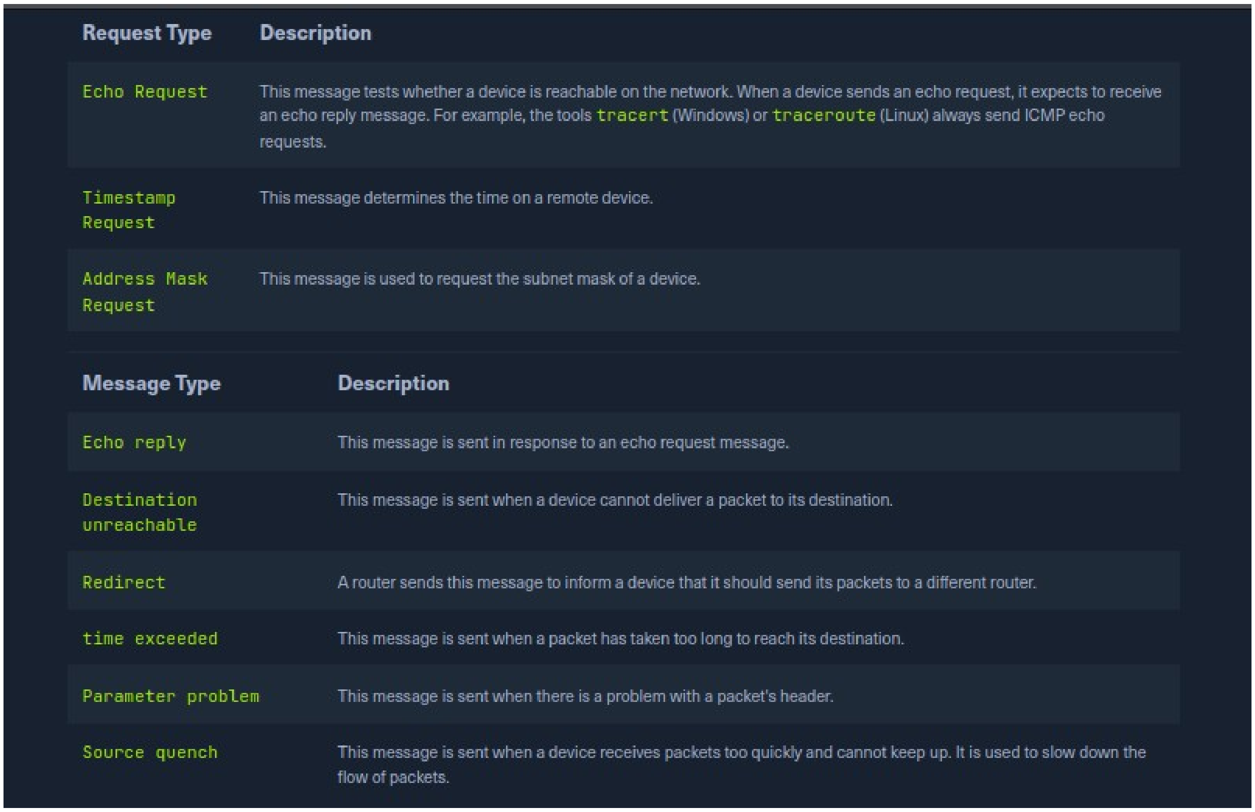
Internet Control Message Protocol (ICMP) is a protocol used by devices to communicate with each other on the Internet for various purposes, including error reporting and status information. It sends requests and messages between devices, which can be used to report errors or provide status information.

ICMP Requests

A request is a message sent by one device to another to request information or perform a specific action. An example of a request in ICMP is the ping request, which tests the connectivity between two devices. When one device sends a ping request to another, the second device responds with a ping reply message.

ICMP Messages

A message in ICMP can be either a request or a reply. In addition to ping requests and responses, ICMP supports other types of messages, such as error messages, destination unreachable, and time exceeded messages. These messages are used to communicate various types of information and errors between devices on the network.



Request Type	Description
`Echo Request`	This message tests whether a device is reachable on the network. When a device sends an echo request, it expects to receive an echo reply message. For example, the tools `tracert` (Windows) or `traceroute` (Linux) always send ICMP echo requests.
`Timestamp Request`	This message determines the time on a remote device.
`Address Mask Request`	This message is used to request the subnet mask of a device.

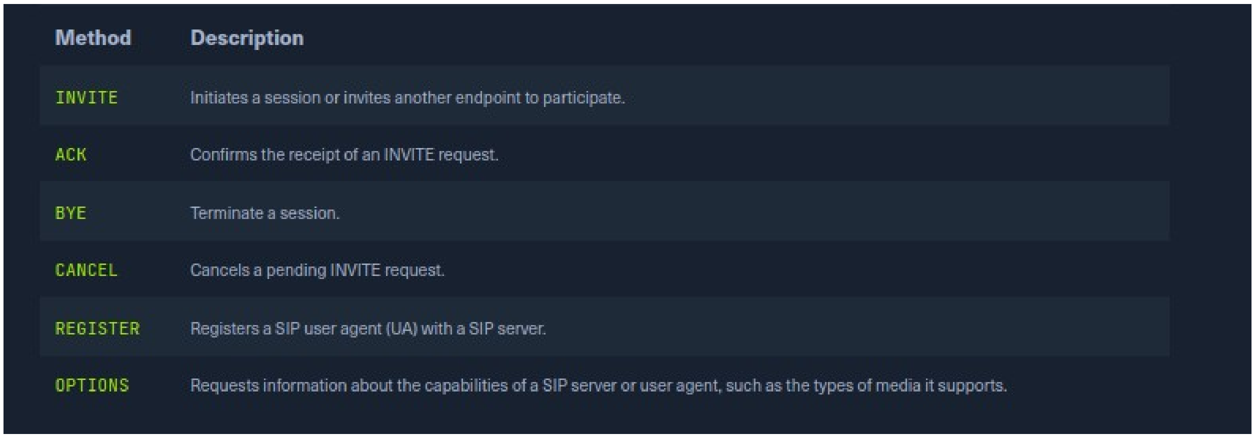
Message Type	Description
`Echo reply`	This message is sent in response to an echo request message.
`Destination unreachable`	This message is sent when a device cannot deliver a packet to its destination.
`Redirect`	A router sends this message to inform a device that it should send its packets to a different router.
`time exceeded`	This message is sent when a packet has taken too long to reach its destination.
`Parameter problem`	This message is sent when there is a problem with a packet's header.
`Source quench`	This message is sent when a device receives packets too quickly and cannot keep up. It is used to slow down the flow of packets.

Time-To-Live (TTL) field in the ICMP packet header that limits the packet's lifetime as it travels through the network. It prevents packets from circulating indefinitely on the network in the event of routing loops. Each time a packet passes through a router, the router decrements the TTL value by 1. When the TTL value reaches 0, the router discards the packet and sends an ICMP Time Exceeded message back to the sender.

We can also use TTL to determine the number of hops a packet has taken and the approximate distance to the destination.

VoIP

Voice over Internet Protocol (VoIP) is a method of transmitting voice and multimedia communications. For example, it allows us to make phone calls using a broadband internet connection instead of a traditional phone line, like Skype, Whatsapp, Google Hangouts, Slack, Zoom, and others.



Method	Description
INVITE	Initiates a session or invites another endpoint to participate.
ACK	Confirms the receipt of an INVITE request.
BYE	Terminate a session.
CANCEL	Cancels a pending INVITE request.
REGISTER	Registers a SIP user agent (UA) with a SIP server.
OPTIONS	Requests information about the capabilities of a SIP server or user agent, such as the types of media it supports.

Wireless Networks

Wireless networks are computer networks that use wireless data connections between network nodes. These networks allow devices such as laptops, smartphones, and tablets to communicate with each other and the Internet without needing physical connections such as cables.

WiFi Connection

The device must also be configured with the correct network settings, such as the network name / Service Set Identifier (SSID) and password. So, to connect to the router, the laptop uses a wireless networking protocol called IEEE 802.11. This protocol defines the technical details of how wireless devices communicate with each other and with WAPs. When a device wants to join a WiFi network, it sends a request to the WAP to initiate the connection process. This request is known as a connection request frame or association request and is sent using the IEEE 802.11 wireless networking protocol.

Virtual Private Networks

A **Virtual Private Network** (VPN) is a technology that allows a secure and encrypted connection between a private network and a remote device. This allows the remote machine to access the private network directly, providing secure and confidential access to the network's resources and services.

Requirement	Description
VPN Client	This is installed on the remote device and is used to establish and maintain a VPN connection with the VPN server. For example, this could be an OpenVPN client.
VPN Server	This is a computer or network device responsible for accepting VPN connections from VPN clients and routing traffic between the VPN clients and the private network.
Encryption	VPN connections are encrypted using a variety of encryption algorithms and protocols, such as AES and IPsec, to secure the connection and protect the transmitted data.
Authentication	The VPN server and client must authenticate each other using a shared secret, certificate, or another authentication method to establish a secure connection.

Key Exchange Mechanisms

Key exchange methods are used to exchange **cryptographic keys** between two parties securely.

Diffie-Hellman

One common key exchange method is the **Diffie-Hellman key exchange**, which allows two parties to agree on a shared secret key without any prior communication or shared private information. It is based on the concept of two parties generating a shared secret key that can be used to encrypt and decrypt messages between them. It is vulnerable to MITM attacks

RSA

Another key exchange method is **the Rivest–Shamir–Adleman** (RSA) algorithm, which uses the properties of large prime numbers to generate a shared secret key. It is not limited to:

- Encrypting and signing messages to provide confidentiality and authentication
- Protecting data in transit over networks, such as in the Secure Socket Layer (SSL) and TLS protocols
- Generating and verifying digital signatures, which are used to provide authenticity and integrity for electronic documents and other digital data
- Authenticating users and devices, such as in the Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) protocol used by the Kerberos network authentication system
- Protecting sensitive information, such as in the encryption of personal data and confidential documents

ECDH

Elliptic curve Diffie-Hellman (ECDH) is a variant of Diffie-Hellman key exchange that uses elliptic curve cryptography to generate the shared secret key. It has the advantage of being more efficient and secure than the original Diffie-Hellman algorithm, including but not limited to:

- Establishing secure communication channels, such as in the TLS protocol
- Providing forward secrecy, which ensures that past communications cannot be revealed even if the private keys are compromised
- Authenticating users and devices, such as in the Internet Key Exchange (IKE) protocol used in VPNs

ECDSA

The **Elliptic Curve Digital Signature Algorithm** (ECDSA) uses elliptic curve cryptography to generate digital signatures that can authenticate the parties involved in the key exchange.

Internet Key Exchange

Internet Key Exchange (IKE) is a protocol used to establish and maintain secure communication sessions, such as those used in VPNs. It uses a combination of the Diffie-Hellman key exchange algorithm and other cryptographic techniques to securely exchange keys and negotiate security parameters. Besides, it is a key component of many VPN solutions, as it enables the secure exchange of keys and other security information between the VPN client and server. This allows the VPN to establish an encrypted tunnel through which data can be transmitted securely.

Main Mode

The main mode is the default mode for IKE and is generally considered more secure than the aggressive mode. The key exchange process is performed in three phases in the main mode, each exchanging a different set of security parameters and keys. This allows for greater flexibility and security but can also result in slower performance compared to aggressive mode.

Aggressive Mode

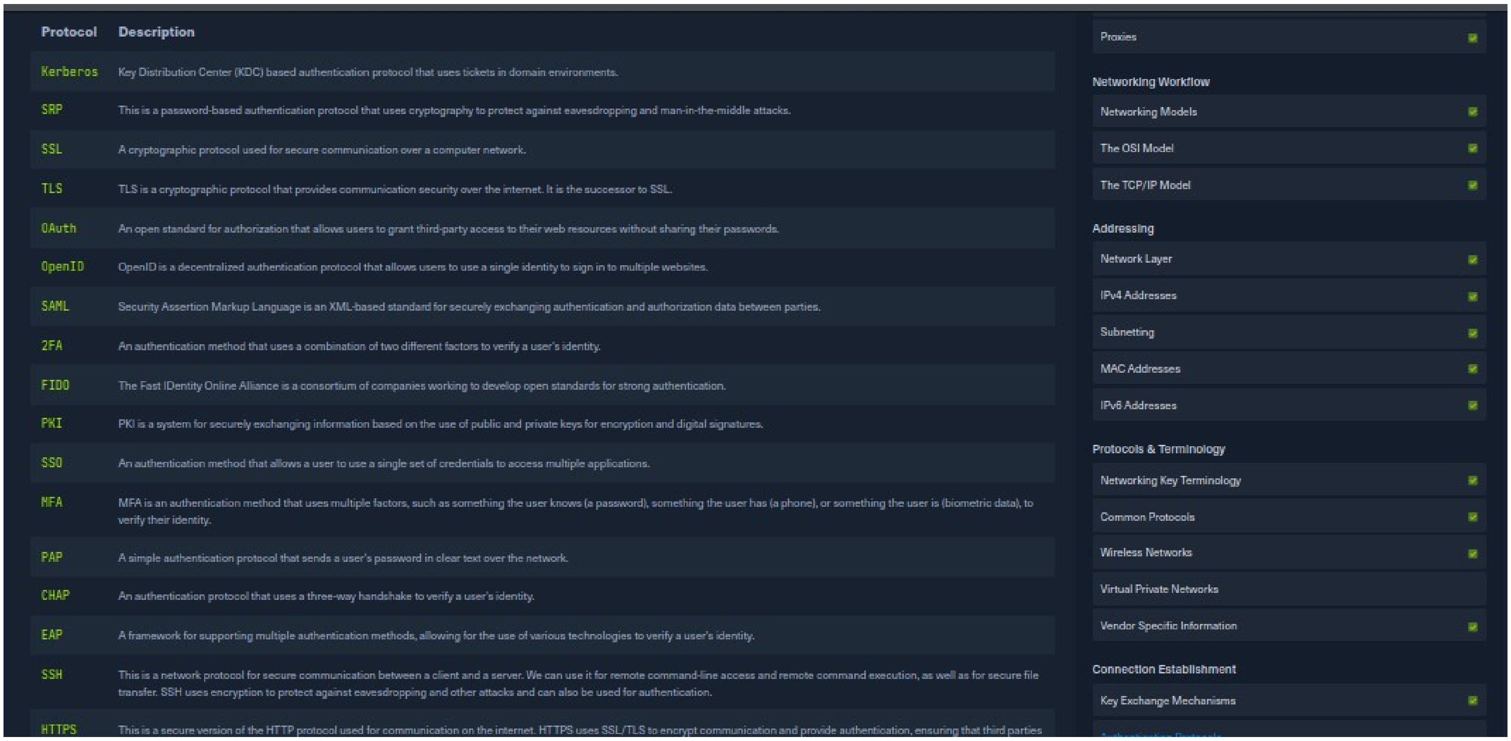
Aggressive mode is an alternative mode for IKE that provides faster performance by reducing the number of round trips and message exchanges required for key exchange. In this mode, the key exchange process is performed in two phases, with all security parameters and keys being exchanged in the first phase.

Pre-Shared Keys

In IKE, a Pre-Shared Key (PSK) is a secret value shared between the two parties involved in the key exchange. This key is used to authenticate the parties and establish a shared secret that encrypts subsequent communication.

Authentication Protocols

Protocols are essential because they provide a secure and standardized way of verifying the identity of users, devices, and other entities in a network. Without authentication protocols, it would be difficult to securely and reliably identify entities in a network, making it easy for attackers to gain unauthorized access and potentially compromise the network.



Protocol	Description
Kerberos	Key Distribution Center (KDC) based authentication protocol that uses tickets in domain environments.
SRP	This is a password-based authentication protocol that uses cryptography to protect against eavesdropping and man-in-the-middle attacks.
SSL	A cryptographic protocol used for secure communication over a computer network.
TLS	TLS is a cryptographic protocol that provides communication security over the internet. It is the successor to SSL.
OAuth	An open standard for authorization that allows users to grant third-party access to their web resources without sharing their passwords.
OpenID	OpenID is a decentralized authentication protocol that allows users to use a single identity to sign in to multiple websites.
SAML	Security Assertion Markup Language is an XML-based standard for securely exchanging authentication and authorization data between parties.
2FA	An authentication method that uses a combination of two different factors to verify a user's identity.
FIDO	The Fast IDentity Online Alliance is a consortium of companies working to develop open standards for strong authentication.
PKI	PKI is a system for securely exchanging information based on the use of public and private keys for encryption and digital signatures.
SSO	An authentication method that allows a user to use a single set of credentials to access multiple applications.
MFA	MFA is an authentication method that uses multiple factors, such as something the user knows (a password), something the user has (a phone), or something the user is (biometric data), to verify their identity.
PAP	A simple authentication protocol that sends a user's password in clear text over the network.
CHAP	An authentication protocol that uses a three-way handshake to verify a user's identity.
EAP	A framework for supporting multiple authentication methods, allowing for the use of various technologies to verify a user's identity.
SSH	This is a network protocol for secure communication between a client and a server. We can use it for remote command-line access and remote command execution, as well as for secure file transfer. SSH uses encryption to protect against eavesdropping and other attacks and can also be used for authentication.
HTTPS	This is a secure version of the HTTP protocol used for communication on the internet. HTTPS uses SSL/TLS to encrypt communication and provide authentication, ensuring that third parties

TCP/UDP Connections

Transmission Control Protocol (TCP) and *User Datagram Protocol* (UDP) are both protocols used in information and data transmission on the Internet. Typically, TCP connections transmit important data, such as web pages and emails. In contrast, UDP connections transmit real-time data such as streaming video or online gaming.

Blind Spoofing

Blind spoofing, is a method of data manipulation attack in which an attacker sends false information on a network without seeing the actual responses sent back by the target devices. It involves manipulating the IP header field to indicate false source and destination addresses. For example, we send a TCP packet to the target host with false source and destination port numbers and a false Initial Sequence Number (ISN). The ISN is a field in the TCP header that is used to specify the sequence number of the first TCP packet in a connection. The ISN is set by the sender of a TCP packet and sent to the receiver in the TCP header of the first packet. This can cause the target host to establish a connection with us without receiving the connection.

This attack is commonly used to disrupt the integrity of network connections or to break connections between network devices. It can also be used to monitor network traffic or to intercept information sent by network devices.

Cryptography

Encryption is used on the Internet to transmit data, such as payment information, e-mails, or personal data, confidentially and protected against manipulation. Data is encrypted using various cryptographic algorithms based on mathematical operations. With the help of encryption, data can be transformed into a form that unauthorized persons can no longer read. Digital keys in symmetric or asymmetric encryption processes are used for encryption.

Symmetric Encryption

Symmetric encryption, also known as secret key encryption, is a method that uses the same key to encrypt and decrypt the data. This means the sender and the receiver must have the same key to decrypt the data correctly.

Asymmetric Encryption

Asymmetric encryption, also known as public-key encryption, is a method of encryption that uses two different keys:

- a public key
- a private key

The public key is used to encrypt the data, while the private key is used to decrypt the data. This means anyone can use a public key to encrypt data for someone, but only the recipient with the associated private key can decrypt the data. Examples of asymmetric encryption methods include Rivest–Shamir–Adleman (RSA), Pretty Good Privacy (PGP), and Elliptic Curve Cryptography (ECC).

Data Encryption Standard

DES is a symmetric-key block cipher, and its encryption works as a combination of the one-time pad, permutation, and substitution ciphers applied to bit sequences. It uses the same key in both encrypting and decrypting data.

The key consists of 64 bits, with 8 bits used as a checksum. Therefore, the actual key length of DES is only 56 bits. And that is why one always speaks of a key length of 56 bits when referring to DES. To prevent the danger from frequency analysis, not single letters, but each 64-bit block of plaintext is encrypted to a 64-bit block of ciphertext.

Advanced Encryption Standard

Compared to DES, AES uses 128-bit (AES-128), 192-bit (AES-192), or 256-bit (AES-256) keys to encrypt and decrypt data. In addition, AES is faster than DES because it has a more efficient algorithm structure.

This is because it can be applied to multiple data blocks at once, making it faster. This means that AES encryption and decryption can be performed faster than DES, which is especially important when large amounts of data need to be encrypted.

Cipher Modes

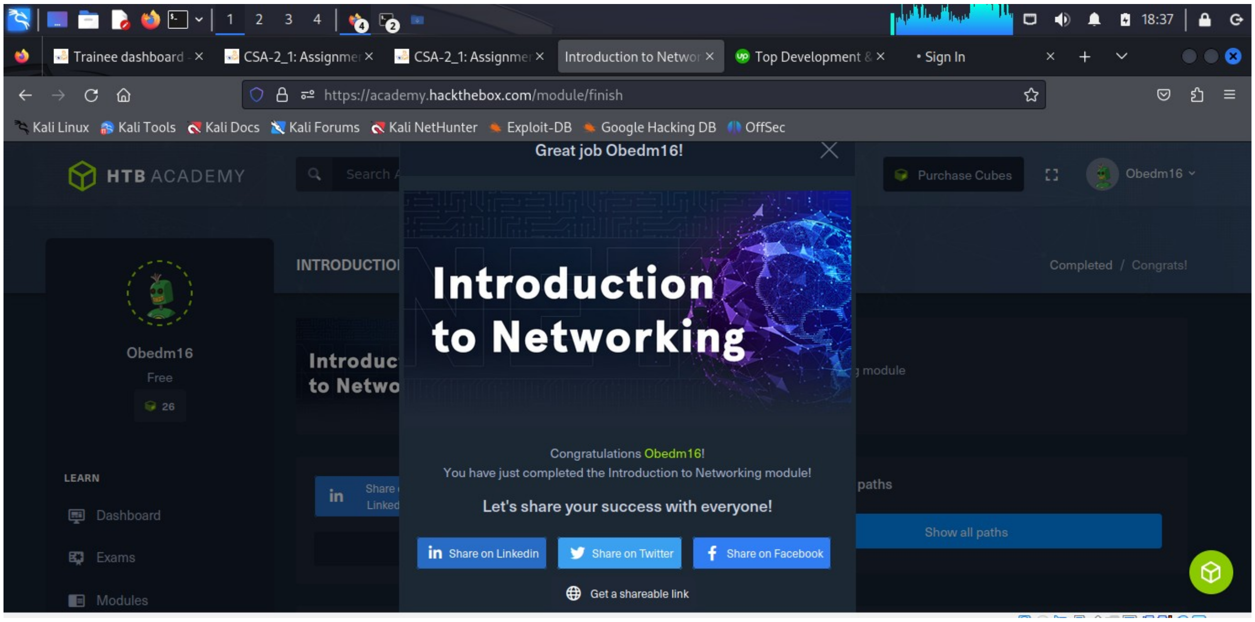
A cipher mode refers to how a block cipher algorithm encrypts a plaintext message. A block cipher algorithm encrypts data, each using fixed-size blocks of data (usually 64 or 128 bits). A cipher mode defines how these blocks are processed and combined to encrypt a message of any length.

Conclusion

Finally, the learner – as Security Analyst was able to grasp from the very basics of networking, understanding the OSI and TCP/IP models of network.

Also the learner learnt about Address Resolution protocol, network topology, Authentication protocols.

The materials were deep to even beginners understanding how to calculate the IPv4 and IPv6 addresses.



https://academy.hackthebox.com/module/finish

Great job Obedm16!

Congratulations Obedm16!
You have just completed the Introduction to Networking module!

Let's share your success with everyone!

https://academy.hackthebox.com/achievement/978332/34