

OSI Reference Model Cheat Sheet

OSI MODEL CHEAT SHEET



STATIONX
THE CYBER SECURITY COMPANY

What is the OSI Reference Model?

The Open Systems Interconnection (OSI) model is a way to represent how devices communicate with one another. It consists of seven layers:

1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

You receive data from layers 1 through 7 and transmit data in the opposite direction. That's because every layer of the OSI Model handles a specific job and passes data to and from the layers above and below itself.

Although building computing devices doesn't require the OSI model, it's proven helpful in troubleshooting computer networking problems. That's because the OSI model gives technicians an in-depth method to dissect the network problem to find its root cause. The solution often becomes clear by narrowing it down to a specific model layer.

OSI Layers

The infographic below summarizes the seven layers of the OSI reference model. If you need a quick refresher, this is the image to download.

The 7-Layer OSI Model

No.	Layer	Function	Data unit	Hardware	Protocols
7	Application 	Human-computer interaction through applications that access network services	Message/data	Gateway	UPnP, DHCP, DNS, HTTP, HTTPS, NFS, NTP, POP3, SMTP, SNMP, FTP, Telnet, SSH, TFTP, IMAP
6	Presentation 	Data formatting and encryption/decryption	Message/data	Gateway redirector	TLS, SSL, AFP
5	Session 	Inter-host communication	Message/data	Gateway	NetBIOS, RPC, SMB, Socks
4	Transport 	Data transmission	TCP: segment; UDP: datagram	Gateway	TCP, UDP, SCTP
3	Network 	Path determination and logical addressing	Packet, datagram	Router, Brouter	ARP, IP, NAT, ICMP, IPsec, ICMP (ping)
2	Data Link 	Physical addressing	Frame, cell	Switch, bridge, NIC	ARP, Ethernet, L2TP, LLDP, MAC, NDP, PPP, PPTP, VTP, VLAN
1	Physical 	Binary signal transmission over physical media	Bit, frame	Cables, modem, hub, repeater, NIC, multiplexer	Ethernet, IEEE802.11, ISDN, USB, Bluetooth

The given examples of protocols are for your reference only. For a complete list, check out our [Ports and Protocols Cheat Sheet](#).

What Does Each Layer Do

Let's consider the scenario of receiving an email on your smartphone. How did the email arrive? What has been going on right up to the moment you got the "New Email" notification?

According to the OSI reference model, the following events have transpired:

Layer 1: The Physical Layer

The virtual world is fascinating, but [the matrix](#) requires a physical component. The physical layer of the OSI model is a tangible or intangible medium through which our devices send and receive electronic signals.

Wired **Ethernet** cables are a well-worn example of the physical layer. Still, given the ubiquity of smart devices, we want our illustration in this article to be relevant to the times.

Suppose you've connected your phone to a Wi-Fi **access point (AP)**. The AP receives electromagnetic signals of ones and zeros called bits all day, some of which correspond to the email message we've mentioned.

The physical layer takes out the portions corresponding to the **preamble**, **start frame delimiter (SFD)**, and the **frame check sequence (FCS)**. It then passes the rest to the data link layer as a frame.

Definitions:

- **Ethernet:** the traditional cabling technology for connecting telecommunication devices in a wired network
- **AP: (wireless) access point;** a networking hardware device that allows other Wi-Fi devices to connect to a wired network
- **Preamble:** an indicator of the end of header information used to synchronize a data transmission
- **SFD: start frame delimiter;** a data field in the header of a transmission frame that marks the start of data
- **FCS: frame check sequence;** an error-detecting code added to a frame in a communication protocol

1. Physical



STATIONX

Layer 2: The Data Link Layer

The data link layer is usually a **network interface card (NIC)** in a switch or a bridge. Your smartphone contains networking and routing components, so it has no separate NIC. The NIC or networking circuitry reads the source and destination **MAC addresses**, which it expects to map to devices on the **local area network (LAN)**, itself included.

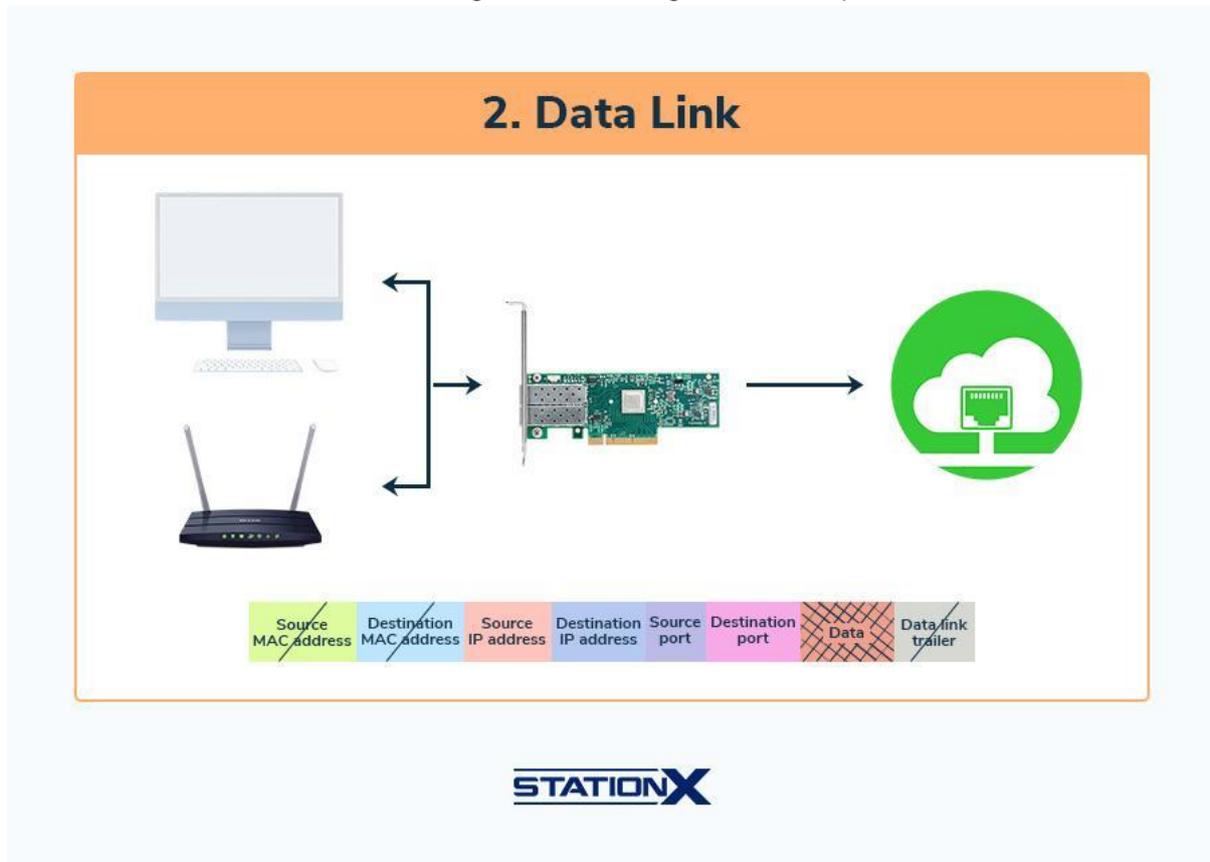
Next, it compares the destination MAC address against the MAC address burned into it. If they match, this layer sends the frame to the network layer as an IP packet. Otherwise, they're undeliverable and discarded because MAC addresses only make sense within a LAN.

As for the source MAC address, the data link layer keeps it in its memory in case the network layer requires it in a return route. In that scenario, this layer attaches the source MAC address to the data frame as the new destination MAC address.

Definitions:

- **NIC: network interface card;** for connecting a computer to a computer network
- **MAC address: media access control address;** a unique identifier assigned to a NIC for use as a network address in communications within a network segment

- **LAN: local area network;** a series of computers connected as a network in a circumscribed location
- **IP: Internet Protocol;** for logical addressing across computer networks



Layer 3: The Network Layer

You can no longer rely on MAC addresses to send data packets across distributed networks larger than a LAN, such as in the broader Internet. The network layer is where we use logical addressing, such as IP addresses, to identify different nodes in large networks.

The network layer, usually a router, picks up an IP packet from the previous layer. Using network layer protocols such as **Address Resolution Protocol (ARP)** and **Network Address Translation (NAT)**, it reads the source and destination IP addresses, saves the source IP address for sending responses, and checks if the destination IP address is your device's.

If yes, it strips both IP addresses of the packet, and the remainder, which is often a **TCP** segment or a **UDP** datagram, moves upward to the transport layer. If not, the IP packet is lost because the network layer has discarded it.

Your phone is also a router, so it does the above automatically. As an aside, this is also why you can use your phone as a Wi-Fi hotspot.

Definitions:

- **ARP: Address Resolution Protocol;** for uncovering the MAC address associated with an IP address
- **NAT: Network Address Translation;** the process of mapping an IP address to another by changing the header of IP packets while in transit via a router
- **TCP: Transmission Control Protocol;** a connection-oriented protocol that helps establish and maintain connections until the applications on both ends have completed data exchange.
- **UDP: User Datagram Protocol;** a connectionless protocol that enables data transfer before reaching an agreement with the receiving party.



Layer 4: The Transport Layer

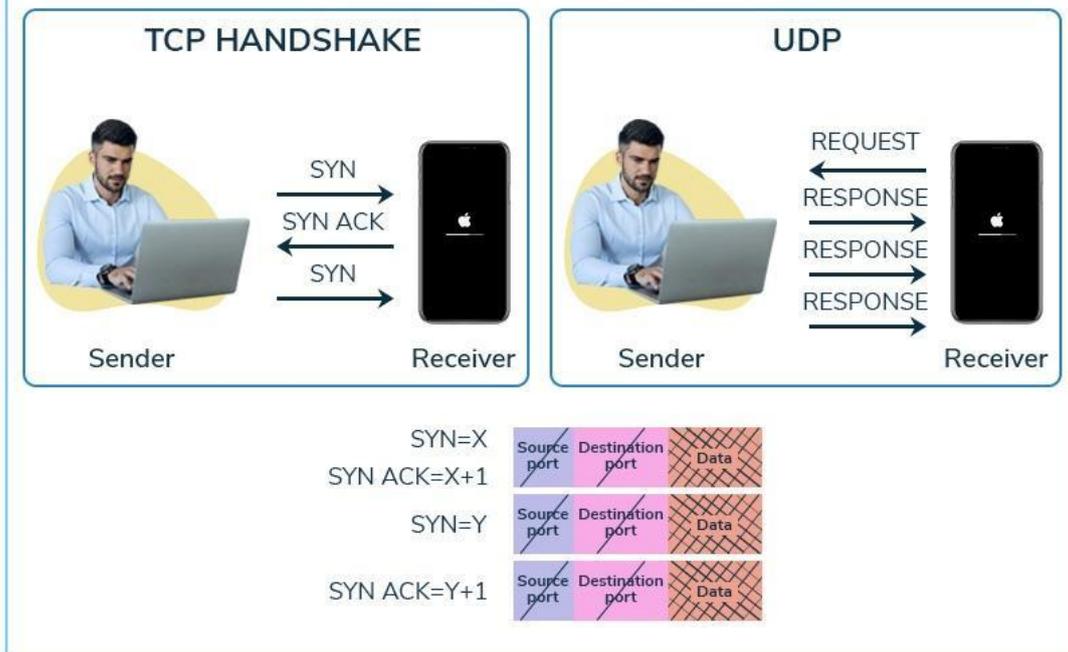
The transport layer is for processing chunks of data called TCP segments and UDP datagrams. The purpose of this layer is to assemble and disassemble these different pieces of incoming data.

The size of a data link frame has an upper limit, such as 1500 bytes for an Ethernet frame, so the payload of a segment/datagram may be a portion of a larger set of data. The transport layer rearranges these portions as appropriate and either joins them to recover the entire body of data received or splits them up before transmission.

In the case of the email reaching your phone, the transport layer pieces together the TCP segments corresponding to various components of your message—sender, recipient, timestamp, subject line, content, attachments—and passes the data on to the session layer.

4. Transport

TCP vs UDP Communication



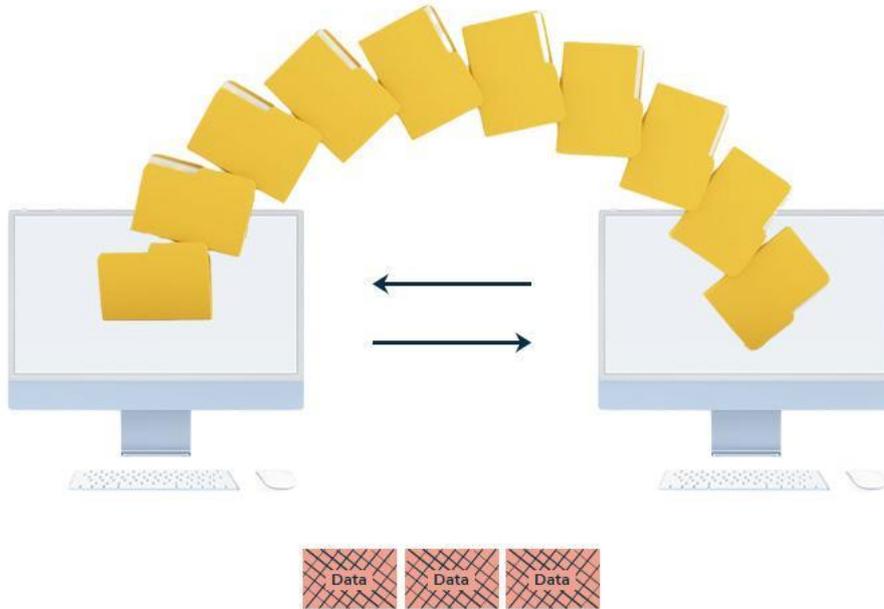
Layer 5: The Session Layer

The session layer makes and maintains connections between your local host and remote hosts. Data can travel between your phone's mail client and the email server if they share an established connection via TCP or UDP.

The data containing your email has reached the session layer, which saves the source and destination port information. It uses the source port number to send data back, such as an acknowledgment receipt or an error message, such as a nonexistent addressee or a full mailbox unable to receive new mail.

Now that the session layer has received the reassembled email data and your mailbox has space, this layer pushes the data forward to the port number of your phone's email client.

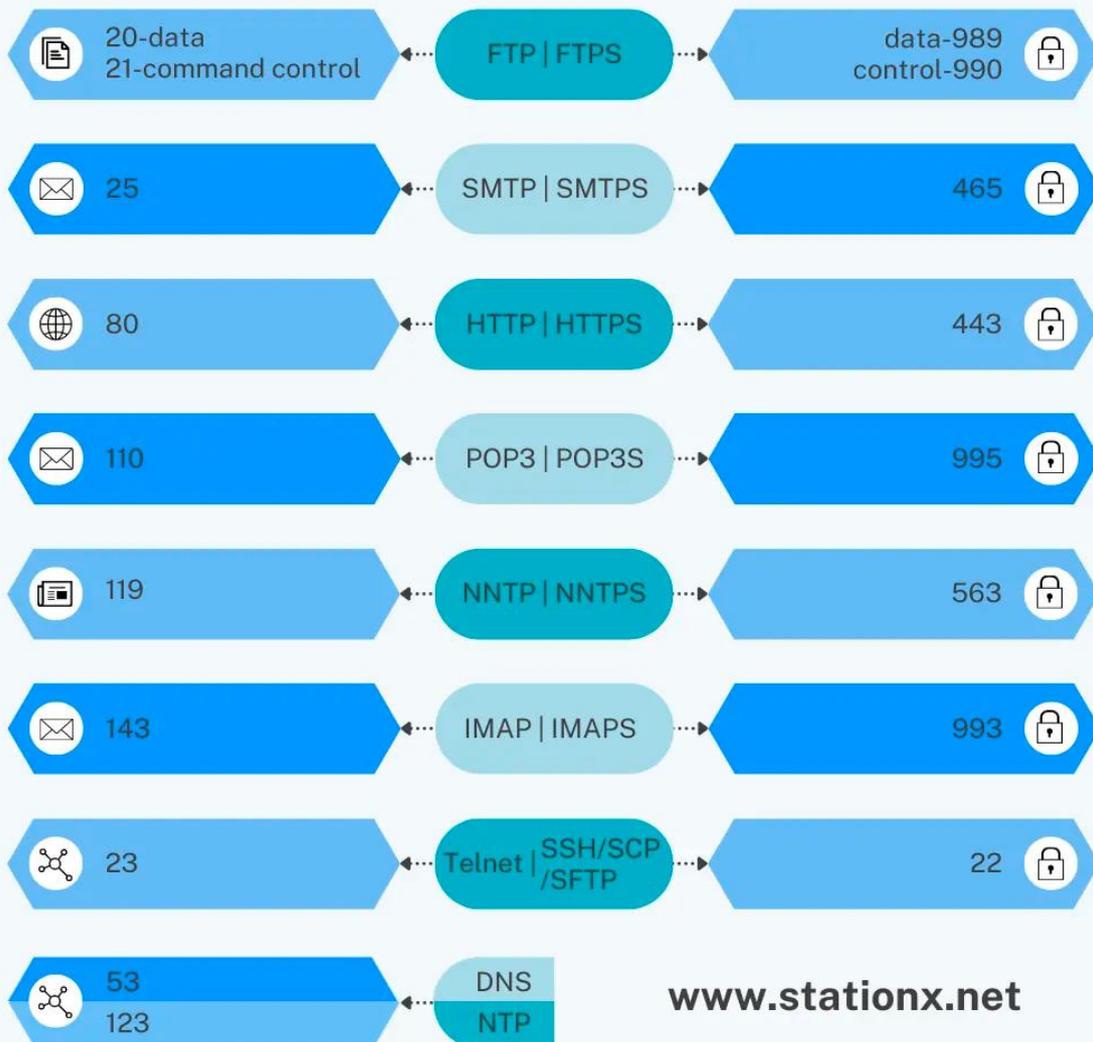
5. Session



STATIONX

Well-Known Ports: Unencrypted vs Encrypted

Must-know commonly used ports to memorize



From our [Ports and Protocols Cheat Sheet](#)

Layer 6: The Presentation Layer

The conventional function of the presentation layer is to ensure the correct application receives the data from the previous layer for processing and that the data is in a valid format for viewing. Data encryption and decryption happen at this layer.

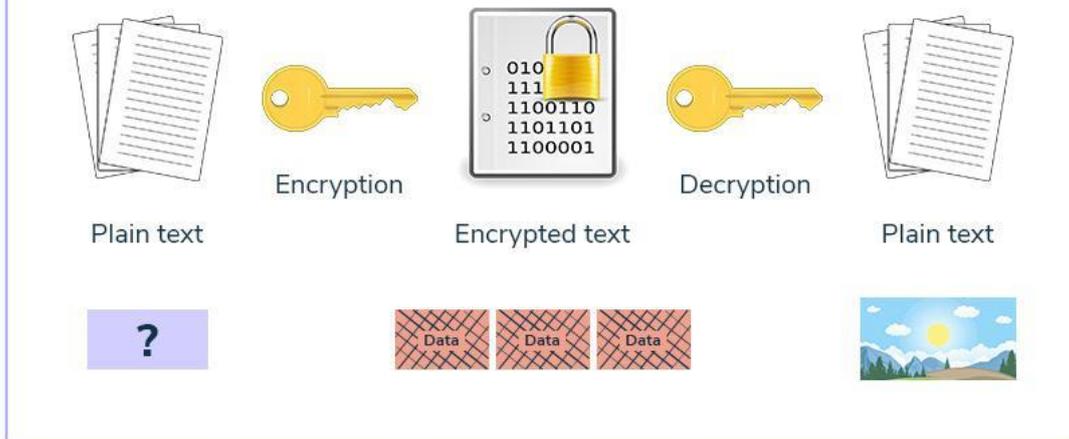
Most email services support the POP3S and IMAPS protocols for receiving emails. The TLS/SSL portion of these protocols belongs to the presentation layer. Or, if you use end-to-end encrypted email services such as [Protonmail](#) or [Tutanota](#), this is the layer where your emails stay encrypted until you click each subject line.

Some instructors deem the presentation layer disposable because computer applications have become robust enough to read almost all data types or return relevant error messages. In other words, all data is now machine-readable, even if it outputs gibberish.

6. Presentation

Encryption

(used to protect sensitive information)



STATIONX

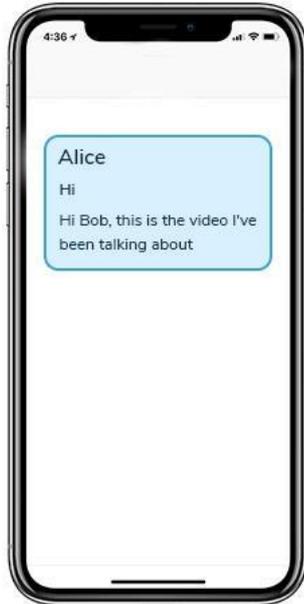
Layer 7: The Application Layer

Your phone buzzes. A new notification appears. You've got mail. Your email app is working as expected. Is that all to the application layer? For receiving emails, this is it. But for sending emails, no.

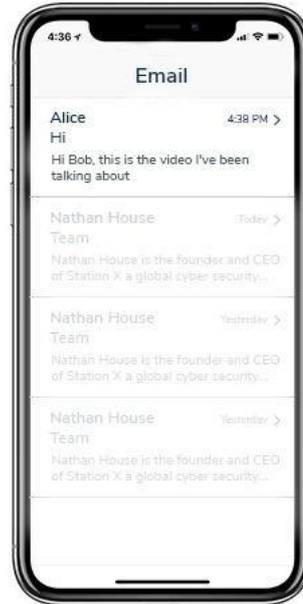
This layer is responsible for the features built into the application that make them aware of networks, such as an Application Programming Interface (API). Taking emails as an example, email APIs, such as [Mailchimp](#) or [Constant Contact](#), are for sending automated emails, such as payment receipts, password resets, and newsletters.

7. Application

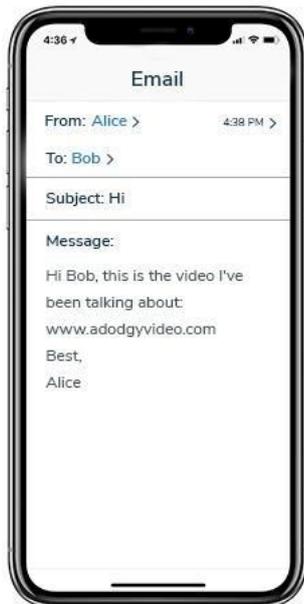
1



2



3



4

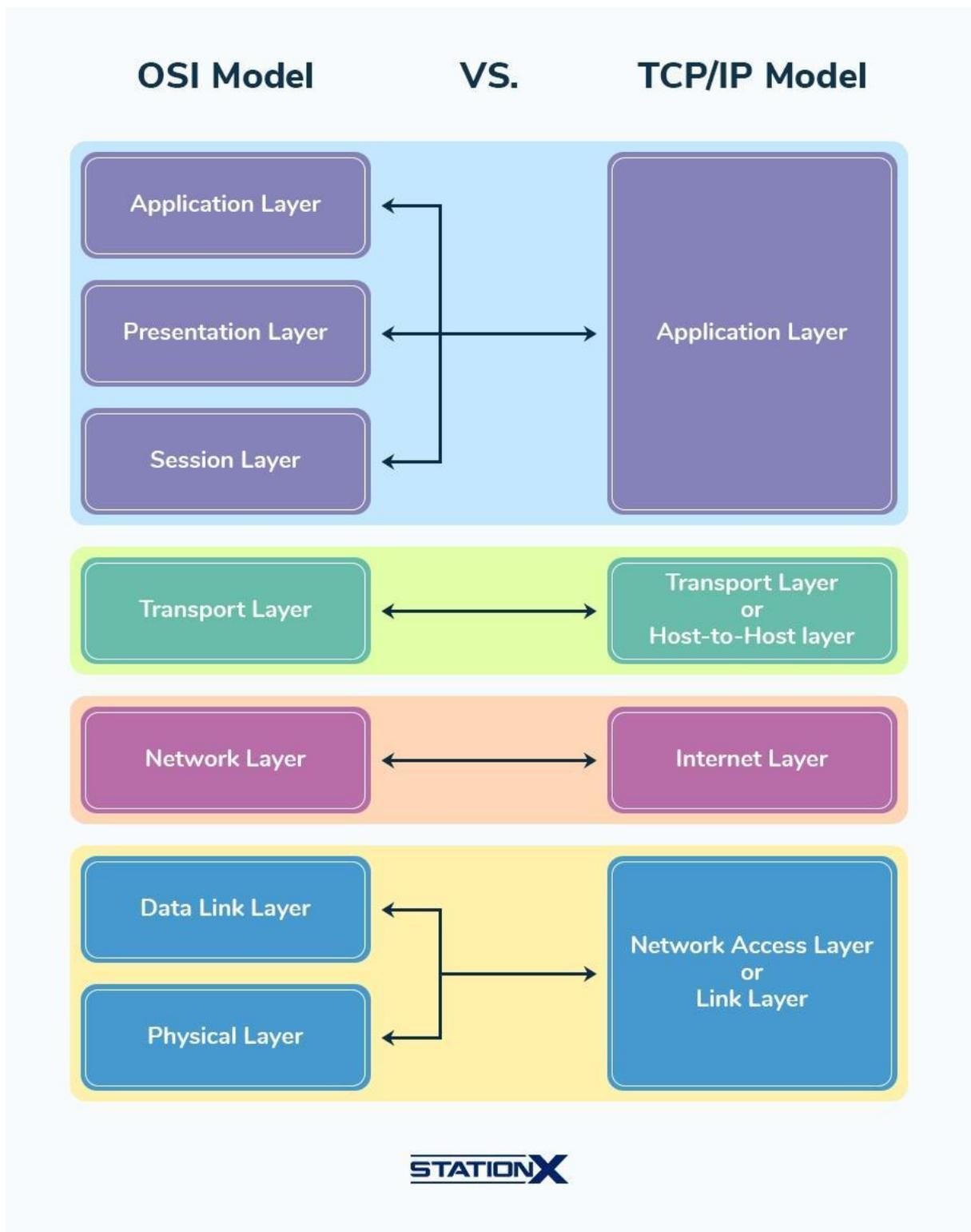


STATIONX

The TCP/IP Reference Model

The TCP/IP model is a model of digital communications which laid the foundation for the modern Internet and most Internet protocols we use today. Since it's older than the OSI model, it's more accurate to say the OSI model is an alternative to the TCP/IP model rather than the other way around.

Therefore, a [major point of criticism](#) raised against the OSI model was that it emerged too late in the history of the Internet to be a game-changer. Here's a graphic comparing both models:



Conclusion

Wherever you are in your IT learning journey, we hope this OSI model cheat sheet helps you understand the OSI reference model. Check out our other [networking articles](#) and [related courses](#) for more resources. Last but not least, if you're studying the OSI model for an upcoming exam, we wish you all the best.