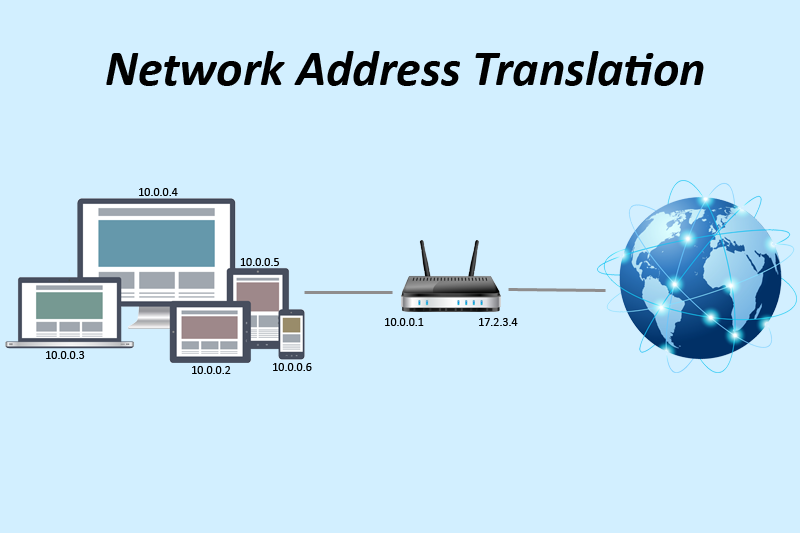
# C4. #5 What is Network Address Translation?



***Share*** the knowledge!

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.

Internet requests that require Network Address Translation (NAT) are quite complex but happen so rapidly that the end user rarely knows it has occurred. A workstation inside a network makes a request to a computer on the Internet. Routers within the network recognize that the request is not for a resource inside the network, so they send the request to the firewall. The firewall sees the request from the computer with the internal IP. It then makes the same request to the Internet using its own public address, and returns the response from the Internet resource to the computer inside the private network. From the perspective of the resource on the Internet, it is sending information to the address of the firewall. From the perspective of the workstation, it appears that communication is directly with the site on the Internet. When NAT is used in this way, all users inside the private network access the Internet have the same public IP address when they use the Internet. That means only one public addresses is needed for hundreds or even thousands of users.

Most modern firewalls are stateful - that is, they are able to set up the connection between the internal workstation and the Internet resource. They can keep track of the details of the connection, like ports, packet order, and the IP addresses involved. This is called keeping track of the state of the connection. In this way, they are able to keep track of the session composed of communication between the workstation and the firewall, and the firewall with the Internet. When the session ends, the firewall discards all of the information about the connection.

There are other uses for Network Address Translation (NAT) beyond simply allowing workstations with internal IP addresses to access the Internet. In large networks, some servers may act as Web servers and require access from the Internet. These servers are assigned public IP addresses on the firewall, allowing the public to access the servers only through that IP address. However, as an additional layer of security, the firewall acts as the intermediary between the outside world and the protected internal network. Additional rules can be added, including which ports can be accessed at that IP address. Using NAT in this way allows network engineers to more efficiently route internal network traffic to the same resources, and allow access to more ports, while restricting access at the firewall. It also allows detailed logging of communications between the network and the outside world.

Additionally, NAT can be used to allow selective access to the outside of the network, too. Workstations or other computers requiring special access outside the network can be assigned specific external IPs using NAT, allowing them to communicate with computers and applications that require a unique public IP address. Again, the firewall acts as the intermediary, and can control the session in both directions, restricting port access and protocols.

NAT is a very important aspect of firewall security. It conserves the number of public addresses used within an organization, and it allows for stricter control of access to resources on both sides of the firewall.

C5. #1

Critique of osi

**bad timing**

if standards are written too early: subject is badly understood and bad standards

if standards are written too late so many companies may have already made investments in doing the sam e thing with different other ways

TCP/IP already in use by research universities by  
time ISO OSI appeared

**bad technology**

flow control, error control, addressing is multiple

session and presentation(Empty), Network and DL(Full)

**bad implementation**

initial implementations were slowISO OSI-7 layer model was associated with badqualityTCP/IP available within Berkeley UNIX  
was free and reasonably good **bad politics**

TCP/IP & UNIX was much loved in academia  
ISO OSI-7 layer model thought to be a creature of:  
European telecommunication  
European community  
and government of USA  
also thought to be technically inferior to TCP/IP  
people on the ground reacted badly to this and  
supported TCP/IP

C5. #3There are two types of Internet Protocol (IP) traffic. They are **TCP** or **Transmission Control Protocol** and **UDP** or **User Datagram Protocol**. TCP is connection oriented – once a connection is established, data can be sent bidirectional. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

## Comparison chart

Differences — Similarities —

| TCP versus UDP comparison chart | | |
| --- | --- | --- |
| [Edit this comparison chart](https://www.diffen.com/difference/Special:EditTable?diffenVal1=TCP&diffenVal2=UDP) | **TCP** | **UDP** |
| **Acronym for** | Transmission Control Protocol | User Datagram Protocol or Universal Datagram Protocol |
| **Connection** | TCP is a connection-oriented protocol. | UDP is a connectionless protocol. |
| **Function** | As a message makes its way across the [internet](https://www.diffen.com/difference/Internet_vs_World_Wide_Web) from one computer to another. This is connection based. | UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship. |
| **Usage** | TCP is suited for applications that require high reliability, and transmission time is relatively less critical. | UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients. |
| **Use by other protocols** | HTTP, HTTPs, FTP, SMTP, Telnet | DNS, DHCP, TFTP, SNMP, RIP, VOIP. |
| **Ordering of data packets** | TCP rearranges [data](https://www.diffen.com/difference/Data_vs_Information) packets in the order specified. | UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer. |
| **Speed of transfer** | The speed for TCP is slower than UDP. | UDP is faster because error recovery is not attempted. It is a "best effort" protocol. |
| **Reliability** | There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent. | There is no guarantee that the messages or packets sent would reach at all. |
| **Header Size** | TCP header size is 20 bytes | UDP Header size is 8 bytes. |
| **Common Header Fields** | Source port, Destination port, Check Sum | Source port, Destination port, Check Sum |
| **Streaming of data** | Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries. | Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent. |
| **Weight** | TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control. | UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP. |
| **Data Flow Control** | TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control. | UDP does not have an option for flow control |
| **Error Checking** | TCP does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination. | UDP does error checking but simply discards erroneous packets. Error recovery is not attempted. |
| **Fields** | 1. Sequence Number, 2. AcK number, 3. Data offset, 4. Reserved, 5. Control bit, 6. Window, 7. Urgent Pointer 8. Options, 9. Padding, 10. Check Sum, 11. Source port, 12. Destination port | 1. Length, 2. Source port, 3. Destination port, 4. Check Sum |
| **Acknowledgement** | Acknowledgement segments | No Acknowledgment |
| **Handshake** | SYN, SYN-ACK, ACK | No handshake (connectionless protocol) |

Or shortly

## DIFFERENCE BETWEEN TCP AND UDP

TCP (Transmission Control Protocol) is connection oriented, whereas UDP (User Datagram Protocol) is connection-less. This means that TCP tracks all data sent, requiring acknowledgment for each octet (generally). UDP does not use acknowledgments at all, and is usually used for protocols where a few lost datagrams do not matter.

Because of acknowledgments, TCP is considered a reliable data transfer protocol. It ensures that no data is sent to the upper layer application that is out of order, duplicated, or has missing pieces. It can even manage transmissions to attempt to reduce congestion.

UDP is a very lightweight protocol defined in RFC 768. The primary uses for UDP include service advertisements, such as routing protocol updates and server availability, one-to-many multicast applications, and streaming applications, such as voice and video, where a lost datagram is far less important than an out-of-order datagram.\*

| **TCP** | **UDP** |
| --- | --- |
| Reliable | Unreliable |
| Connection-oriented | Connectionless |
| Segment retransmission and flow control through windowing | No windowing or retransmission |
| Segment sequencing | No sequencing |
| Acknowledge sequencing | No acknowledgment |

## C5. #4**Layer 2 (Data Link Layer)**

## [ARCnet](https://en.wikipedia.org/wiki/ARCnet)　Attached Resource Computer NETwork

* [ATM](https://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode) Asynchronous Transfermm Mode
* [CDP](https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol) Cisco Discovery Protocol
* DCAP Data Link Switching Client Access Protocol
* [Distributed Multi-Link Trunking](https://en.wikipedia.org/wiki/Distributed_Multi-Link_Trunking)
* [Distributed Split Multi-Link Trunking](https://en.wikipedia.org/wiki/Distributed_Split_Multi-Link_Trunking)
* [Dynamic Trunking Protocol](https://en.wikipedia.org/wiki/Dynamic_Trunking_Protocol)
* [Econet](https://en.wikipedia.org/wiki/Econet)
* [Ethernet](https://en.wikipedia.org/wiki/Ethernet)
* [FDDI](https://en.wikipedia.org/wiki/Fiber_distributed_data_interface) Fiber Distributed Data Interface
* [Frame Relay](https://en.wikipedia.org/wiki/Frame_Relay)
* [ITU-T](https://en.wikipedia.org/wiki/ITU-T) [G.hn](https://en.wikipedia.org/wiki/G.hn) [Data Link Layer](https://en.wikipedia.org/wiki/Data_Link_Layer)
* [HDLC](https://en.wikipedia.org/wiki/High-Level_Data_Link_Control) High-Level Data Link Control
* [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) WiFi
* [IEEE 802.16](https://en.wikipedia.org/wiki/IEEE_802.16) WiMAX
* [LACP](https://en.wikipedia.org/wiki/Link_Aggregation_Control_Protocol) Link Aggregation Control Protocol
* [LattisNet](https://en.wikipedia.org/wiki/LattisNet)
* [LocalTalk](https://en.wikipedia.org/wiki/LocalTalk)
* [L2F](https://en.wikipedia.org/wiki/L2F) Layer 2 Forwarding Protocol
* [L2TP](https://en.wikipedia.org/wiki/L2TP) Layer 2 Tunneling Protocol
* [LAPD](https://en.wikipedia.org/wiki/Link_Access_Procedures,_D_channel) Link Access Procedures on the D channel
* [LLDP](https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol) Link Layer Discovery Protocol
* [LLDP-MED](https://en.wikipedia.org/wiki/LLDP-MED) Link Layer Discovery Protocol - Media Endpoint Discovery
* [PAgP](https://en.wikipedia.org/wiki/Port_Aggregation_Protocol) - Cisco Systems proprietary link aggregation protocol
* [PPP](https://en.wikipedia.org/wiki/Point-to-Point_Protocol) Point-to-Point Protocol
* [PAP](https://en.wikipedia.org/wiki/Password_Authentication_Protocol) Password Authentication Protocol
* [CHAP](https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol) Challenge Handshake Authentication Protocol
* [Q.710](https://en.wikipedia.org/wiki/Message_Transfer_Part) Simplified [Message Transfer Part](https://en.wikipedia.org/wiki/Message_Transfer_Part)
* [Multi-link trunking](https://en.wikipedia.org/wiki/Multi-link_trunking) Protocol
* [NDP](https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol) Neighbor Discovery Protocol
* [RPR](https://en.wikipedia.org/wiki/Resilient_Packet_Ring) IEEE 802.17 Resilient Packet Ring
* [SLIP](https://en.wikipedia.org/wiki/Serial_Line_Internet_Protocol) Serial Line Internet Protocol (obsolete)
* [StarLAN](https://en.wikipedia.org/wiki/StarLAN)
* [STP](https://en.wikipedia.org/wiki/Spanning_Tree_Protocol) Spanning Tree Protocol
* [Split multi-link trunking](https://en.wikipedia.org/wiki/Split_multi-link_trunking) Protocol
* [Token ring](https://en.wikipedia.org/wiki/Token_ring) a protocol developed by IBM; the name can also be used to describe the token passing ring logical topology that it popularized.
* [VTP](https://en.wikipedia.org/wiki/VTP) VLAN Trunking Protocol
* [VLAN](https://en.wikipedia.org/wiki/VLAN) Virtual Local Area Network
* [MAC](https://en.wikipedia.org/wiki/Media_Access_Control) Media Access Control

# C5. #5 PDU

Stands for "Protocol Data Unit." A PDU is a specific block of information transferred over a [network](https://techterms.com/definition/network). It is often used in reference to the [OSI model](https://techterms.com/definition/osi_model), since it describes the different types of data that are transferred from each layer. The PDU for each layer of the OSI model is listed below.

1. Physical layer – raw [bits](https://techterms.com/definition/bit) (1s or 0s) transmitted physically via the [hardware](https://techterms.com/definition/hardware)
2. Data Link layer – a frame (or series of bits)
3. Network layer – a [packet](https://techterms.com/definition/packet) that contains the source and destination address
4. Transport layer – a segment that includes a [TCP](https://techterms.com/definition/tcp) header and datra
5. Session layer – the data passed to the network connection
6. Presentation layer – the data formatted for presentation
7. Application layer – the data received or transmitted by a software [application](https://techterms.com/definition/application)

C6. #2

## Definition - What does *Virtual Local Area Network (VLAN)*mean?

A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain.

A virtual LAN (Local Area Network) is a logical subnetwork that can group together a collection of devices from different physical [LANs](https://www.lifewire.com/local-area-network-816382).

### Benefits of a VLAN

When set up correctly, virtual LANs can improve the overall performance of busy networks. VLANs are intended to group together client devices that communicate with each other most frequently. The traffic between devices split across two or more physical networks ordinarily needs to be handled by a network's core [routers](https://www.lifewire.com/how-routers-work-816456), but with a VLAN that traffic can be handled more efficiently by [network switches](https://www.lifewire.com/definition-of-network-switch-817588)instead.

VLANs also bring additional security benefits on larger networks by allowing greater control over which devices have local access to each other.

### Static and Dynamic

# C6. #3Media Access Control (MAC)

## Definition - What does *Media Access Control (MAC)* mean?

Media access control (MAC) is a sublayer of the data link layer (DLL) in the seven-layer OSI network reference model. MAC is responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel.

C6. #6

Wan protocols are protocols that govern the communication of wan devices

### **Asynchronous Transfer Mode**

ATM is a packet switching protocol that enables encoding of data traffic into small predetermined sized cells. This protocol is based on connection-oriented technology. It operates by establishing between two end points, a virtual circuit even before exchange of data commences.

### PPP(point to point)

PPP is a data link protocol that is used to directly connect two nodes across serial cables, telephone line, trunk line, cellular phone, exclusive radio links, or fiber optic links. Point-to-point protocol is a WAN protocol widely used by customers for dial-up access to the Internet.

### Framerelay

Frame Relay, a WAN protocol based on packet switching technology, is exclusively for internetworking Local Area Networks (LANs), that is, transmission of data between LANs and WAN end points. A cost-efficient method, frame relay is widely used by network providers as an encapsulation method for voice and data, and used between LANs across a Wide Area Network.

### **SONET/SDH**

Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are multiplexing WAN protocols, which enable transport of multi digital bit streams across the same optical fiber by using Light Emitting Diodes (LEDs) or lasers.

### **X.25**

### X.25 is packet-switched network based WAN protocol for WAN communications. It delineates data exchange and control of information within a user appliance, Data Terminal Equipment (DTE) and a network node, Data Circuit Terminating Equipment (DCE).