

2. How does the internet work - TCP & IP

Packet Switching

The internet is a vast network of interconnected computers and devices that communicate using a method called packet switching. In packet switching, data is broken down into small chunks called packets. Each packet contains the sender's address, the recipient's address, and a portion of the data being transmitted.

These packets are then sent through the network, hopping from one device to another until they reach their destination. The receiving device reassembles the packets in the correct order to reconstruct the original data.

Addresses and Identity

Every device connected to the internet has a unique identification system to facilitate communication. Here are the key components:

URL (Uniform Resource Locator)

A URL is a human-readable address that identifies the location of a resource on the internet. For example, <https://www.example.com/page.html>.

Port

Ports are logical channels that allow different applications on the same device to communicate over the network. Common ports include 80 (HTTP) and 443 (HTTPS).

DNS (Domain Name System)

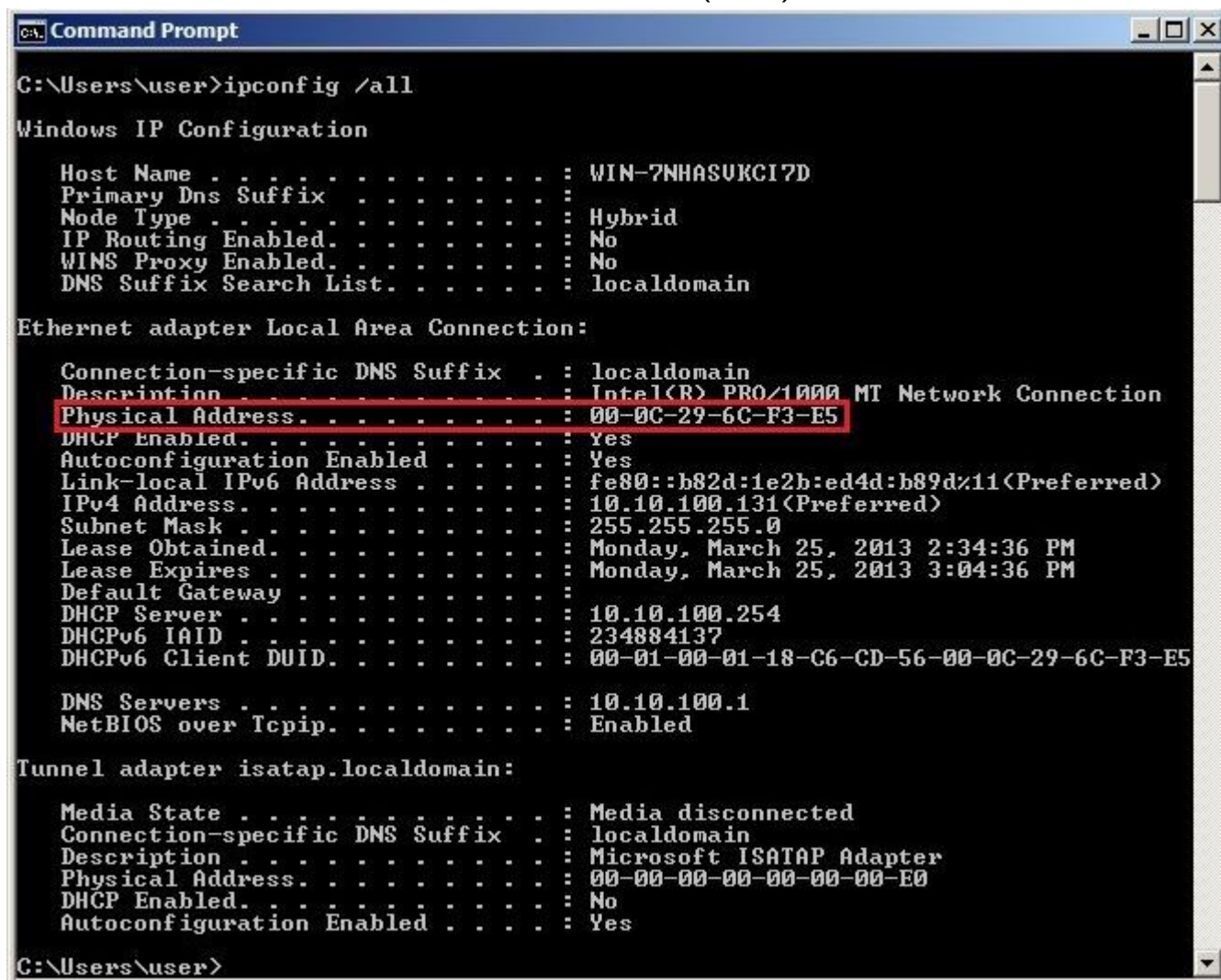
DNS is a distributed database that translates human-readable domain names (like www.example.com) into numerical IP addresses that computers can understand.

IP Address (Internet Protocol Address)

An IP address is a unique numerical label assigned to each device connected to the internet. IPv4 (e.g., 192.168.0.1) and IPv6 (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334) are the two most common versions.

MAC Address (Media Access Control Address)

A MAC address is a unique identifier assigned to a device's network interface controller (NIC). It is used for communication within local area networks (LANs).



```
C:\Users\user>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-7NHASUKCI7D
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-6C-F3-E5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b82d:1e2b:ed4d:b89d%11(Preferred)
IPv4 Address. . . . . : 10.10.100.131(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, March 25, 2013 2:34:36 PM
Lease Expires . . . . . : Monday, March 25, 2013 3:04:36 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 10.10.100.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-C6-CD-56-00-0C-29-6C-F3-E5

DNS Servers . . . . . : 10.10.100.1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.localdomain:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

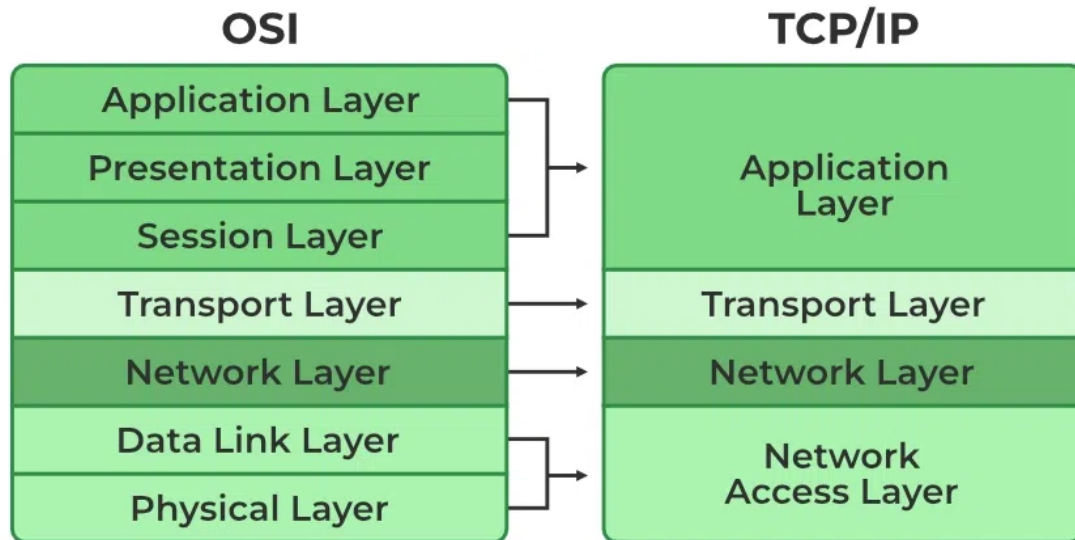
C:\Users\user>
```

TCP/IP Layers

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of protocols that defines how data is transmitted over the internet. It consists of four layers:

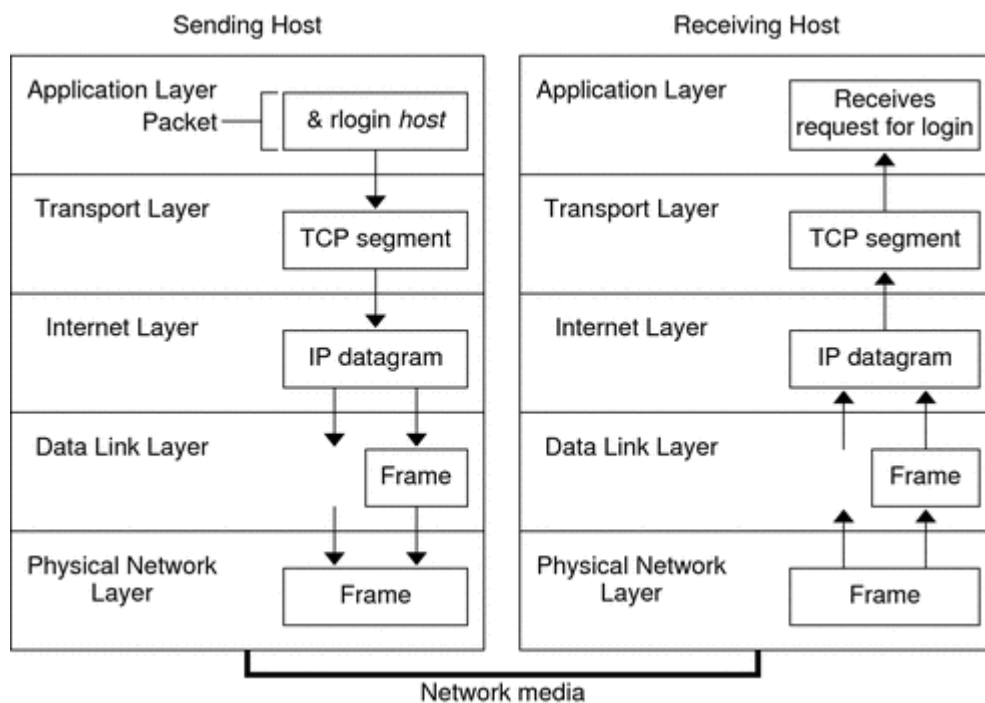
1. **Application Layer:** This layer is responsible for providing services to applications, such as HTTP for web browsing, SMTP for email, and FTP for file transfer.
2. **Transport Layer:** This layer ensures reliable data transfer between applications. It includes protocols like TCP, which guarantees reliable, ordered, and error-checked delivery of data, and UDP, which provides a faster but less reliable service.
3. **Internet Layer:** This layer handles logical addressing and routing of data packets across the network. The primary protocol at this layer is IP (Internet Protocol).

4. **Network Access Layer:** This layer defines how data is transmitted over the physical medium, such as Ethernet or Wi-Fi.



TCP/IP Encapsulation and Layering

TCP/IP follows a layered architecture, where each layer encapsulates the data from the layer above and adds its own header information. This process is called encapsulation.



Routing: How Packets Find Their Way

Routers are the devices responsible for forwarding packets across the internet. They use routing tables and protocols like Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) to determine the best path for packets to reach their destination.

Routers examine the destination IP address in the packet's header and consult their routing tables to determine the next hop in the path. This process continues until the packet reaches its final destination.

TCP/IP Communication

TCP/IP communication involves two main protocols:

1. **TCP (Transmission Control Protocol):** TCP is a connection-oriented protocol that ensures reliable data delivery. It establishes a virtual connection between the sender and receiver, dividing the data into segments, and reassembling them at the destination. TCP also handles error checking, flow control, and retransmission of lost or corrupted data.
2. **UDP (User Datagram Protocol):** UDP is a connectionless protocol that provides a faster but less reliable data transfer service. It does not establish a virtual connection, and data is sent as individual datagrams without error checking or retransmission mechanisms.

Sockets: How Programs Communicate Using Networking

Sockets are software interfaces that allow programs to communicate over a network using TCP/IP. They create an endpoint for sending and receiving data, and are identified by an IP address and a port number.

For example, when you visit a website, your web browser creates a socket and initiates a TCP connection with the web server's socket. Data is then exchanged between the two sockets until the connection is terminated.

Local IP Addresses

In addition to public IP addresses assigned by Internet Service Providers (ISPs), devices on local networks use private IP addresses for internal communication. These addresses are not directly accessible from the internet and are commonly used for home networks, office LANs, and other private networks.

Common private IP address ranges include:

- ◆ 10.0.0.0 to 10.255.255.255

- ◆ 172.16.0.0 to 172.31.255.255
- ◆ 192.168.0.0 to 192.168.255.255

Network Address Translation (NAT) is a technique that allows multiple devices on a private network to share a single public IP address for internet access.

See Also [4. IPv4 vs IPv6](#)