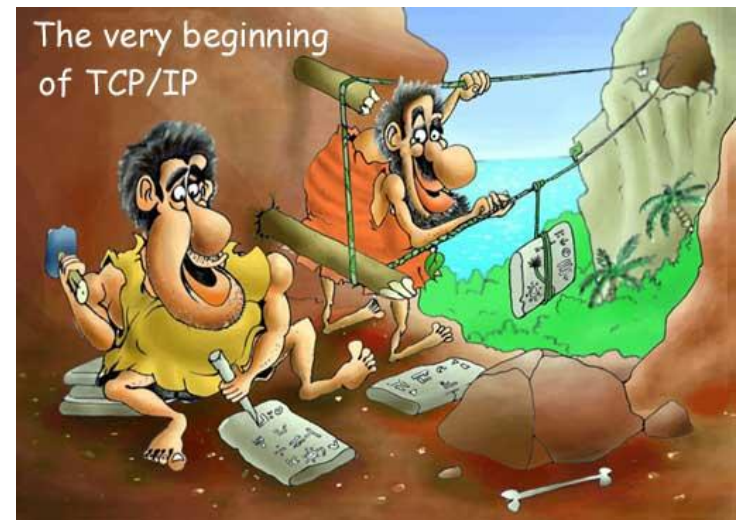


# ***Theme 02. Stack of TCP/IP Protocols***

## **Topics of the lecture 2:**

1. Protocols, stack of protocols and other essential concepts.
2. Common review of the TCP/IP stack of protocols
3. Protocols of the Network interface layer
4. Protocols of the Internet layer
5. IP routing protocols of the Internet layer
6. Protocols of the Transport layer
7. Protocols of the Applications layer



# ***Protocol, Protocol Suite, Stack of Protocols***

---

In computer networking a **protocol** is a document (a technical description) that standardizes a procedure related to data transmission. The protocol defines rules of data processing and formats of data representation.

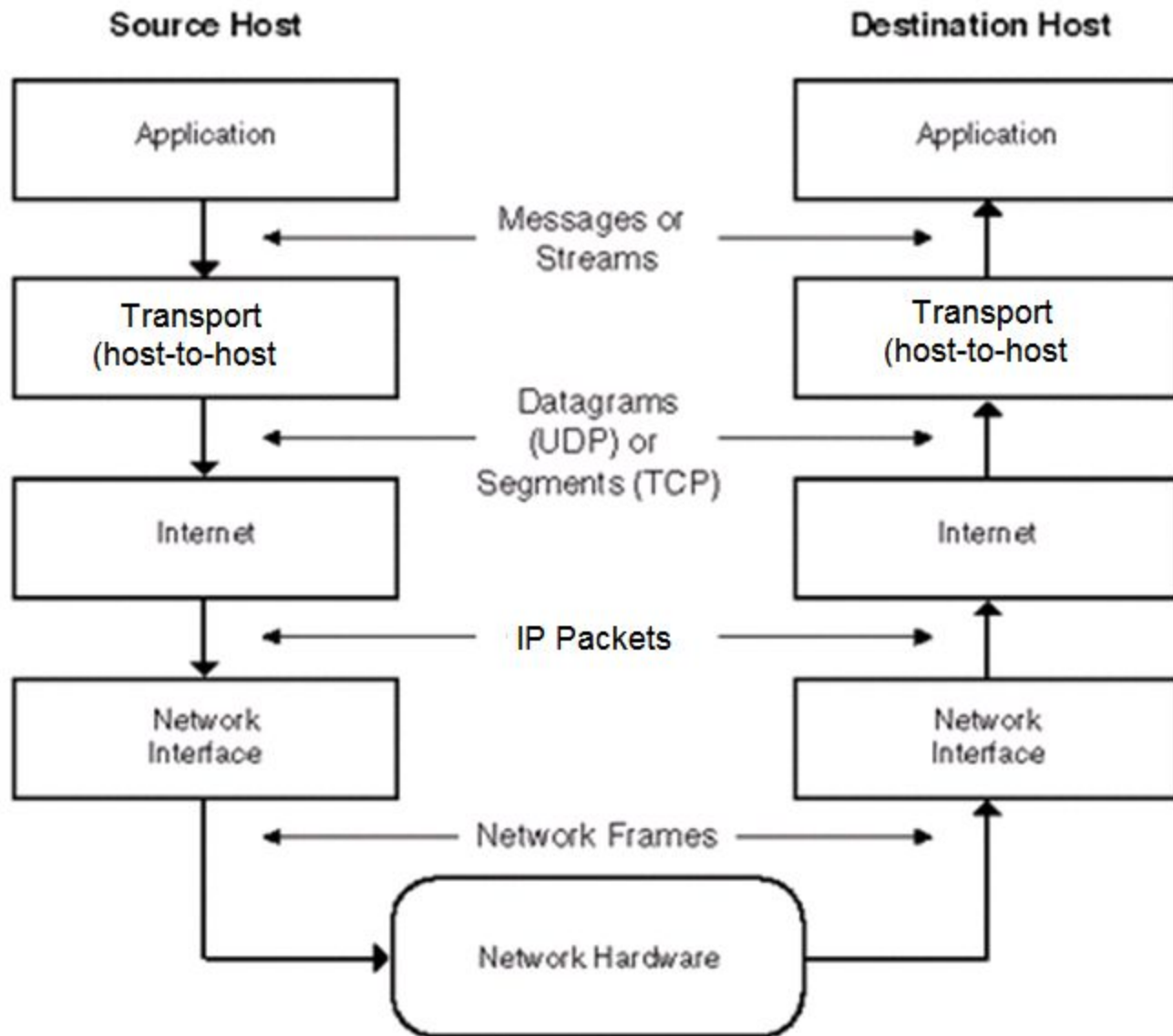
**A protocol suite** is a set of interacted network protocols determining the solving all problems related to the functioning of a computer network.

**The TCP/IP suite** is a set of protocols created on the basis of such regional networks as ARPANet and NSFNet.

**A stack of protocols** is a suite of protocol arranged accordingly to a network model. One of the known models -**TCP/IP Model** was created in the 1970s by DARPA - an agency of the United States Department of Defense (DOD). The model was designed to describe the ARPANet architecture, which was the world's first wide area network and a predecessor of the Internet.

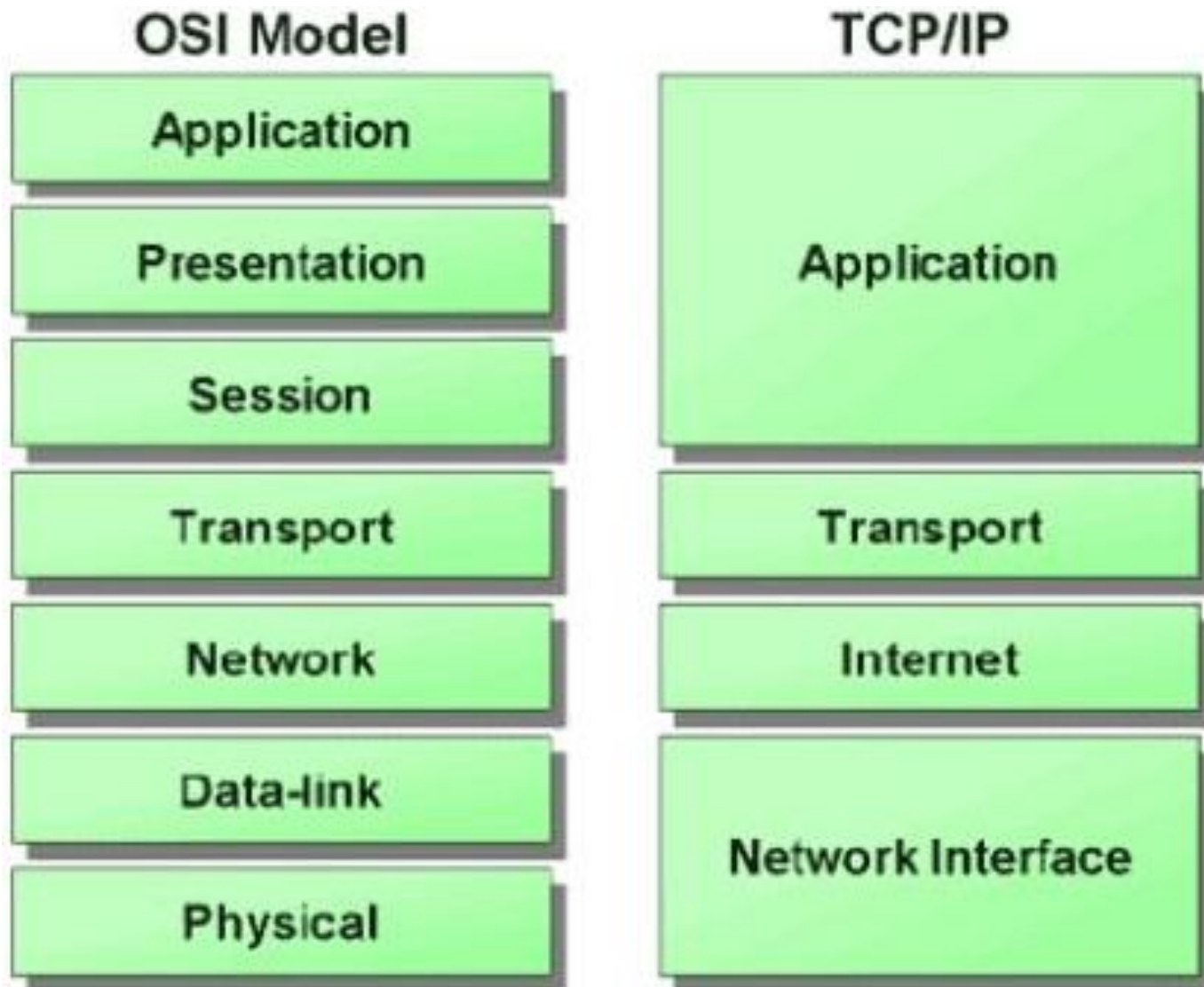
According to the TCP/IP protocols stack terminology, end devices sending or receiving data are called a **hosts**. Hence a TCP/IP network provides data exchange between hosts.

# The TCP/IP Architectural Model



# *The Accordance Between Two Models*

---



# ***Some TCP/IP Stack Features***

---

The TCP/IP stack of protocols provides computer network with quite essential properties:

- **Hardware independence** - protocols of the stack can be used on a Mac, PC, mainframe, or any other computer.
- **Software independence** - software of different vendors and applications should support protocols of the TCP/IP stack.
- **High level of failure recovery** - after elimination of network failure TCP/IP protocols should help to renew the network performance.
- **The ability to handle a big range of transfer errors** - protocols of the TCP/IP stack are able to determine large quantity of data transmission errors and perform recovery of network performance in automatic mode.

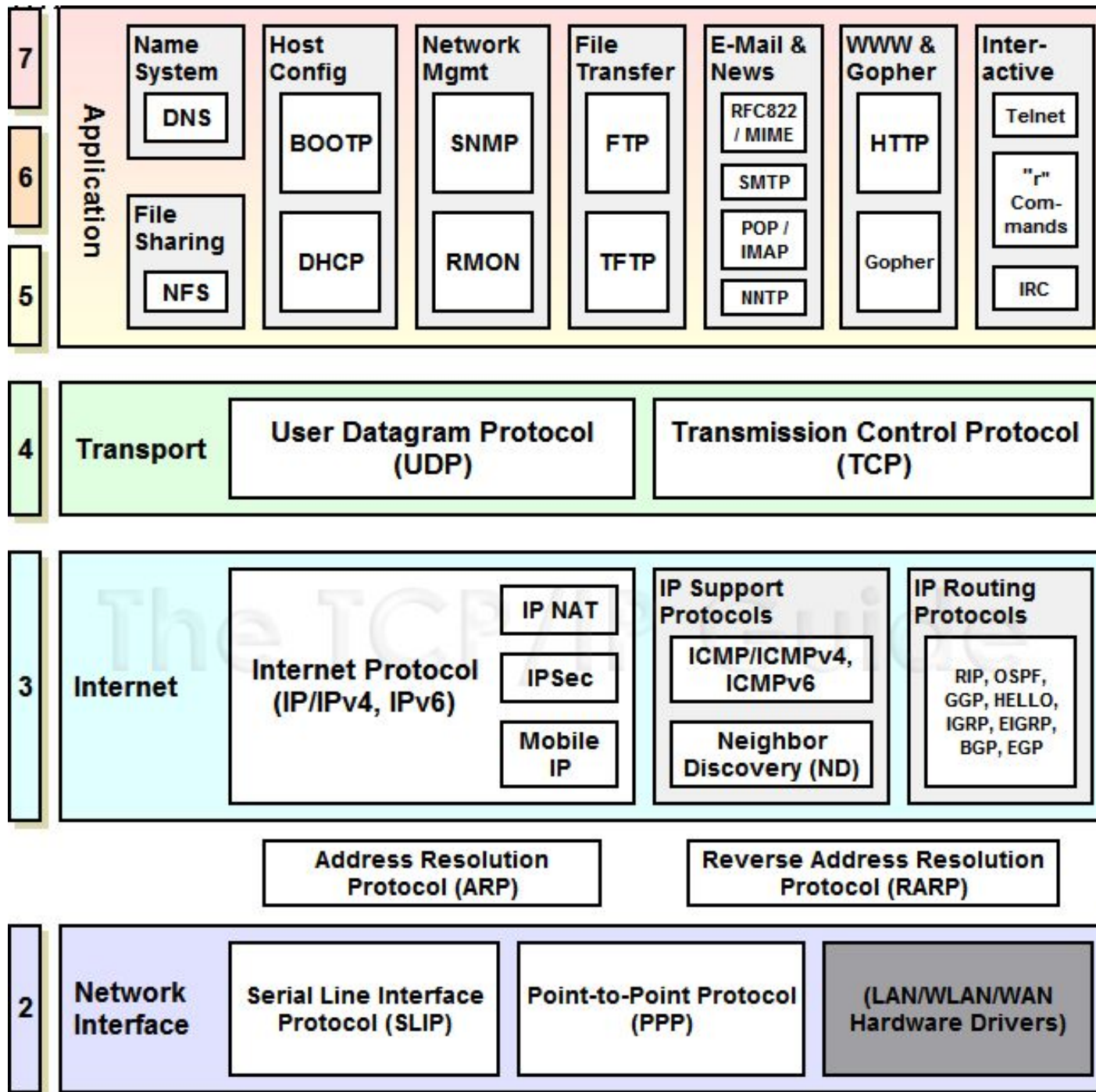
# *The “core” of the TCP/IP Stack*

---

The core protocols of the TCP/IP stack are:

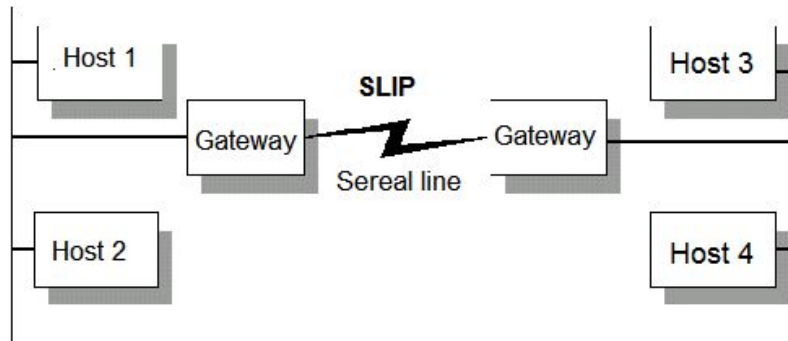
- Internet Protocol (IP),
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP).

# TCP/IP Protocols





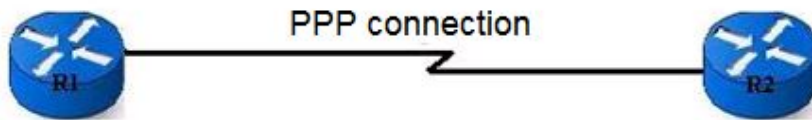
# Network Interface Layer (OSI Layer 2) Protocols



**Serial Line Internet Protocol (SLIP):**  
provides basic TCP/IP functionality by creating a layer-two connection between two devices over a *serial line*.

In computing, a **serial line** is a serial communication physical interface through which information transfers **one bit at a time** (in contrast to a parallel port).

The individual signals on a serial port are unidirectional and when connecting two devices **the outputs of one device** must be connected to **the inputs of the other**.



***A long-haul communication –  
далекий магістральний зв'язок***

## Point-to-Point Protocol (PPP):

provides layer-two connectivity like SLIP, but is much more sophisticated and capable.

PPP is itself a suite of protocols (or “sub-protocols”) that allow for functions such as authentication, data encapsulation, encryption and aggregation, facilitating TCP/IP operation over WAN links.



# ***Network Interface / Network Layer (“OSI Layer 2/3”)***

---

## **Address Resolution Protocol (ARP):**

used to map IP addresses (third layer addresses of the OSI) to physical network addresses (second layer addresses of the OSI).

## **Reverse Address Resolution Protocol (RARP):**

determines the third layer address of a network device (OSI) from its second layer address (OSI).

Now RARP is superseded by BOOTP and DHCP.

# *Internet Layer (OSI Layer 3) Protocols (1)*

---

**IP (Internet Protocol)**, *also known as IP version 4 - IPv4*, is the primary network protocol used on the Internet. It was developed in the 1970s.

The IP provides an encapsulation of a transmitted data into **IP-packets** and connectionless delivery of the packets over a TCP/IP network. IP is the protocol by which data is sent from source host to destination host through an internetwork of any complexity.

Internet Protocol also responsible for addressing. It uses IP addresses of four bytes (32 bits) in length.

**Internet Protocol version 6 (IPv6)** is the newest version of the Internet Protocol (IP). IPv6 is intended to replace IPv4. It was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 uses addresses of 16 bytes (128 bits) in length

# ***Internet Layer (OSI Layer 3) Protocols***

---

## **IP Network Address Translation (IP NAT):**

allows addresses on a private network to be automatically translated to different addresses on a public network.

(Note that some specialists don't consider IP NAT to be a protocol in the strict sense of that word.)

## **IP Security (IPSec):**

a set of IP-related protocols that improve the security of IP transmissions. IPsec network protocol supports encryption and authentication (*ауаентифікацію*).

## **Mobile IP (or MIP):**

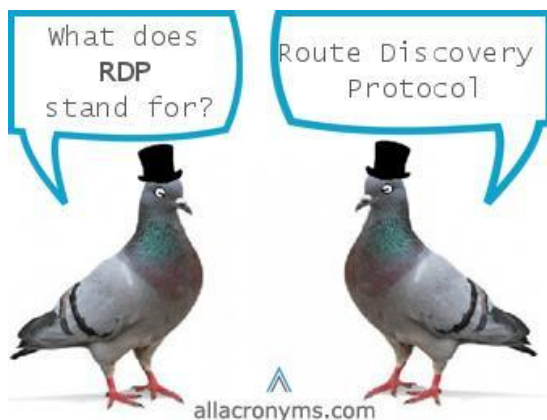
is an *Internet Engineering Task Force (IETF)* standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.

# IP supporting protocols

---

**Internet Control Message Protocol – ICMP (ICMPv4, ICMPv6):**  
a “support protocol” for IPv4 and IPv6. It provides error-reporting and information request-and-reply capabilities to hosts.

**Neighbor Discovery Protocol (NDP)** – *(протокол виявлення сусідів)* - a new “support protocol” for IPv6. It includes several functions performed by ARP and ICMP with purpose of supporting the IP.



**The Router Discovery Protocol (RDP)** is an IETF standard protocol used to inform hosts of the existence of routers.

# Routing and Router

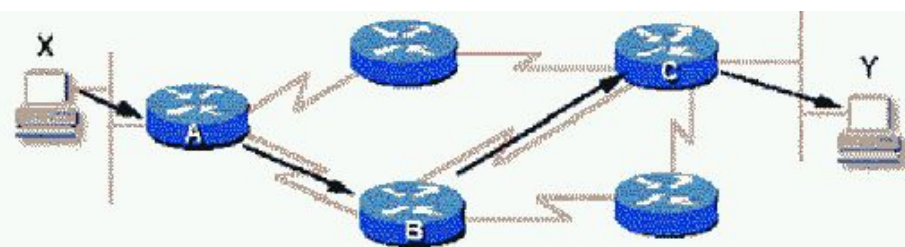
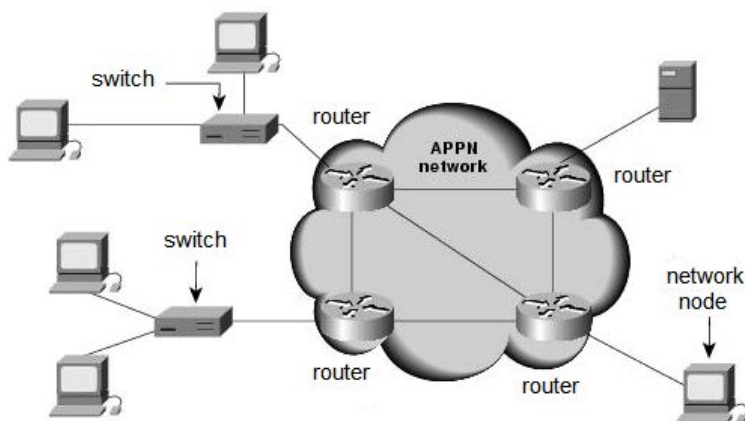
The term '**routing**' refers to choosing the best path for a packet transmission from a source host to a destination host through network.

**Routing** is an action that should be performed before sending information through a network.

A **router** is an intermediary network device that operates at the OSI Layer 3. The primary function of the router is accomplishing of routing. Other its function is moving data from one network to another along the best path to destination.

Routers typically:

- connect a few networks together creating internetwork.
- connect subnets with each other and connect subnets to the main enterprise network.



*Route – маршрут;*

*Router – маршрутизатор;*

*Routing – маршрутизація, вибір маршруту.*

# IP Routing & IP Routing Protocols

**IP routing** is the process of a best path calculation between two host within TCP/IP network.

**An IP routing protocol** is a set of rules that determines how routers on TCP/IP network communicate and exchange information with each other, enabling them to select the best routes to remote networks.

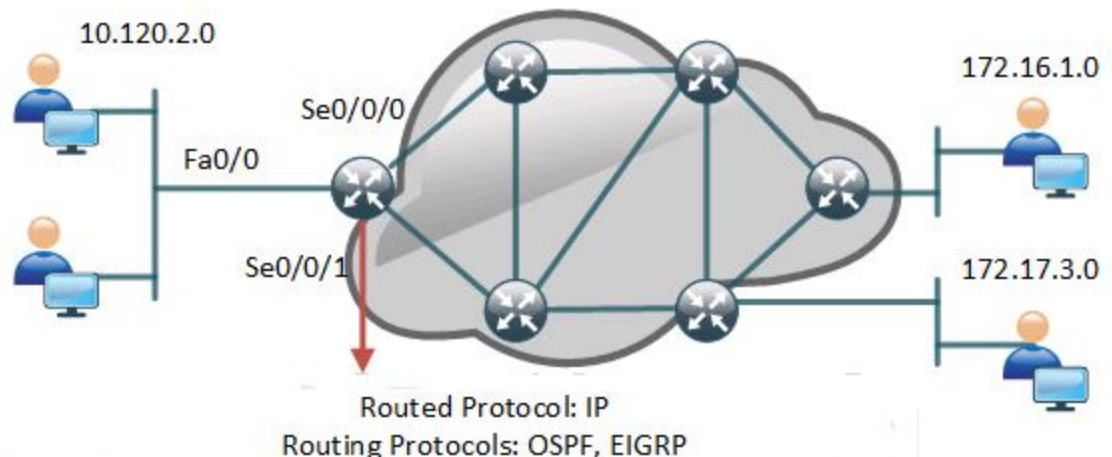
**IP** is responsible for forwarding a packet through network. It uses previously chosen best paths and the destination host address that is located in this packet. Also IP helps to control broadcast traffic or unnecessary traffic.

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol network will be directed.

A routing protocol is only used between routers. It makes possible for routers to build and maintain routing tables.

There are **three classes of routing protocols**:

- distance-vector protocols,
- link state protocols,
- hybrid protocol.



# ***A Routed Protocol***

---

**A routed protocol** is a protocol by means of which data can be routed through a network, or data can be transmitted throughout internetwork in accordance with route that is formed by routers.

**IP** is responsible for forwarding a packet through a network. It uses:

- previously determined best path and
- the destination host address that is located in the packet.

A routed protocol carries user traffic such as e-mails, file transfers, web traffic etc.

The **Internet Protocol** is the most widely used Routed Protocol.



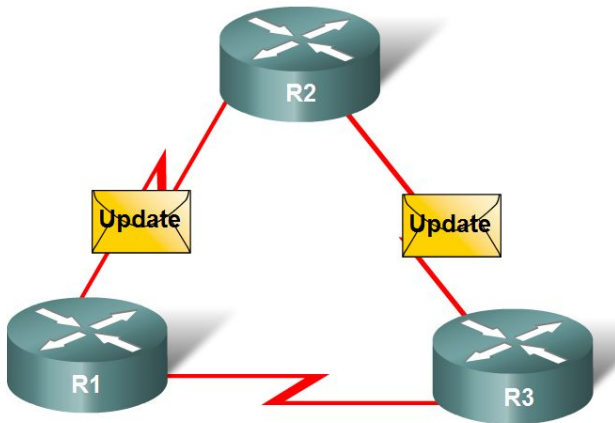
# Dynamic IP Routing Protocols

Routing Protocols learn and **dynamically** share information about the networks connected to each other therefore these protocols are called **dynamic protocols**.

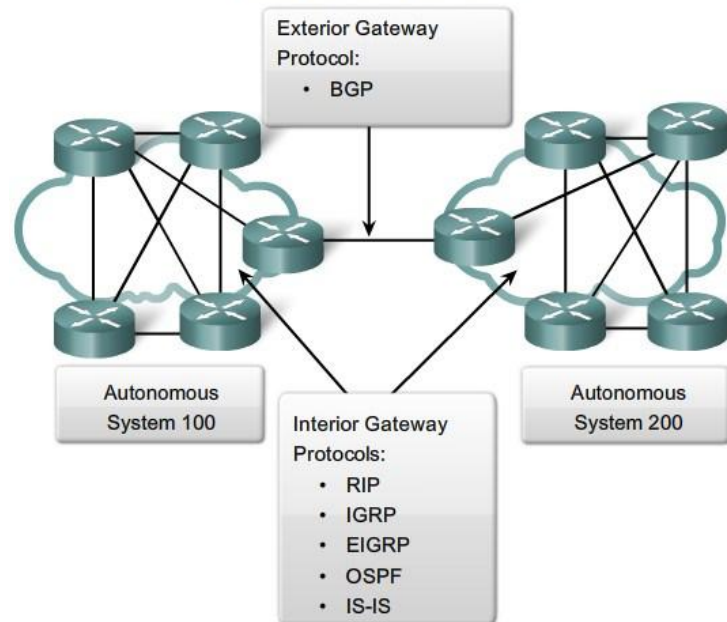
There are quite many dynamic routing protocols for routing IP packets. The most common protocols are:

- **RIP** (Routing Information Protocol);
- **IGRP** (Interior Gateway Routing Protocol);
- **EIGRP** (Enhanced Interior Gateway Routing Protocol);
- **OSPF** (Open Shortest Path First);
- **IS-IS** (Intermediate System-to-Intermediate System) (*pronounced "i-s i-s" or more commonly "Eye-Sis"*);
- **BGP** (Border Gateway Protocol).

Routers Dynamically Pass Updates



IGP vs. EGP Routing Protocols



# *The list of important Routing Protocols related to Routed Protocols*

---

Routed Protocol	Routing Protocols
IP	RIP, IGRP, OSPF, EIGRP
IPX	RIP, NLSP, EIGRP
Appletalk	RMTP, AURP, EIGRP

## **Routing Protocols:**

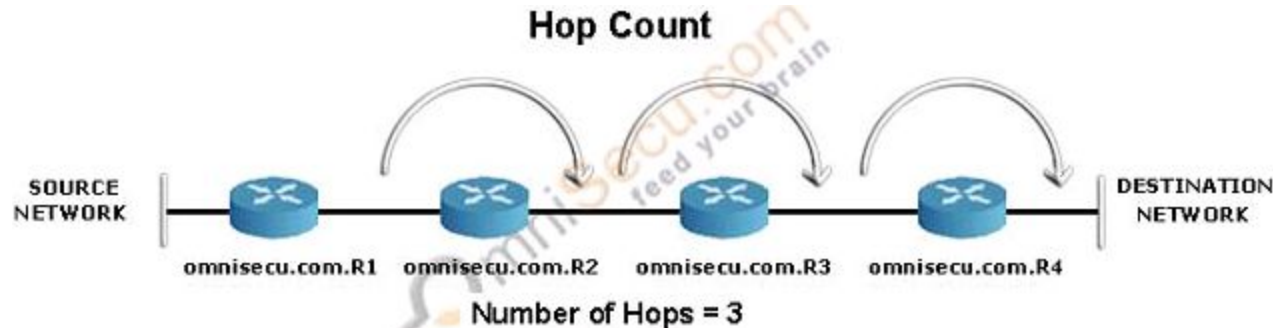
- RIP (Routing Information Protocol);
- IGRP (Interior Gateway Routing Protocol);
- EIGRP (Enhanced Interior Gateway Routing Protocol);
- OSPF (Open Shortest Path First).

# RIP Protocols

**Routing Information Protocol (RIP or RIP1)** is a standards-based, classful, distance-vector, interior gateway protocol (IGP) used by routers to exchange routing information.

RIP uses **hop count** to determine the best path between two locations. Hop count is the number of routers the packet must go through till it reaches the destination network. The maximum allowable number of hops a packet can traverse in an IP network implementing RIP is 15 hops.

**RIPv2** is a classless, distance vector routing protocol. The **classless** term means that the protocol uses the subnet mask with the network addresses. These data it stores in routing table and transmits in case of the routing updates.



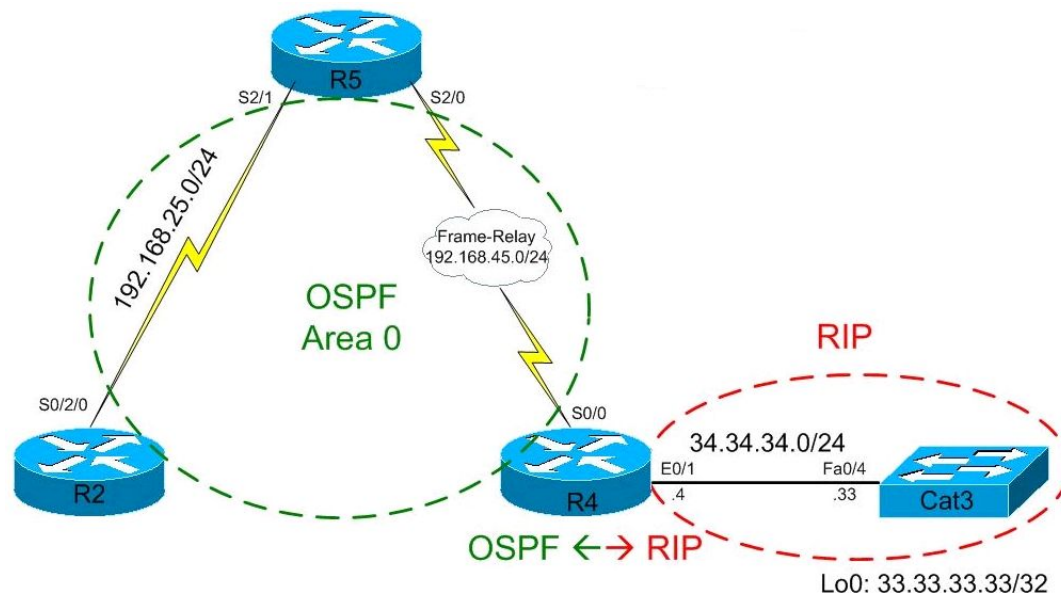
# Open Shortest Path First (OSPF)

**Open Shortest Path First Protocol (OSPF)** was developed as a scalable, open-standards routing protocol for large IP internetworks. OSPF is a **link state protocol** in contradistinction to RIP protocol that is **distance-vector protocol**.

It allows routes to be selected dynamically based on the current state of the network.

OSPF also includes numerous advanced features, for example:

- support for a hierarchical topology;
- automatic load sharing amongst routes.



The **IS-IS (Intermediate System - Intermediate System)** protocol is one of a family of IP Routing protocols. It is an Interior Gateway Protocol (IGP) for the Internet. It is used to flood link state IP routing information throughout a single Autonomous System in an IP network.

IS-IS is a **link-state routing** protocol, which means that the routers exchange topology information with their nearest neighbors.

Like the OSPF protocol, IS-IS uses Dijkstra's algorithm for computing the best path through the network.

*to flood link state information – розсилати інформацію про стан зв'язків лавинним способом.*

# ***Interior Gateway Routing Protocol***

---

**Interior Gateway Routing Protocol (IGRP)** was designed by the Cisco company. The IGRP is a new distance-vector routing protocol that is similar to RIP but can provide greater functionality and solve of RIP's inherent problems. It was designed specifically to be a replacement for RIP.

IGRP overcomes two key limitations of RIP:

- the use of only hop count as a routing metric;
- the hop count limit of 15.

IGRP keeps simplicity of the RIP.

# ***Enhanced Interior Gateway Routing Protocol***

---

**Enhanced Interior Gateway Routing Protocol (EIGRP)** is Cisco's proprietary routing protocol, based on IGRP.

EIGRP is a distance-vector routing protocol, with optimizations to minimize routing instability incurred after topology changes.

EIGRP evolved from IGRP and routers using either EIGRP and IGRP can interoperate because the metric used with one protocol can be translated into the metrics of the other protocol.

EIGRP can be used not only for Internet Protocol (IP) networks but also for AppleTalk and Novell NetWare networks.

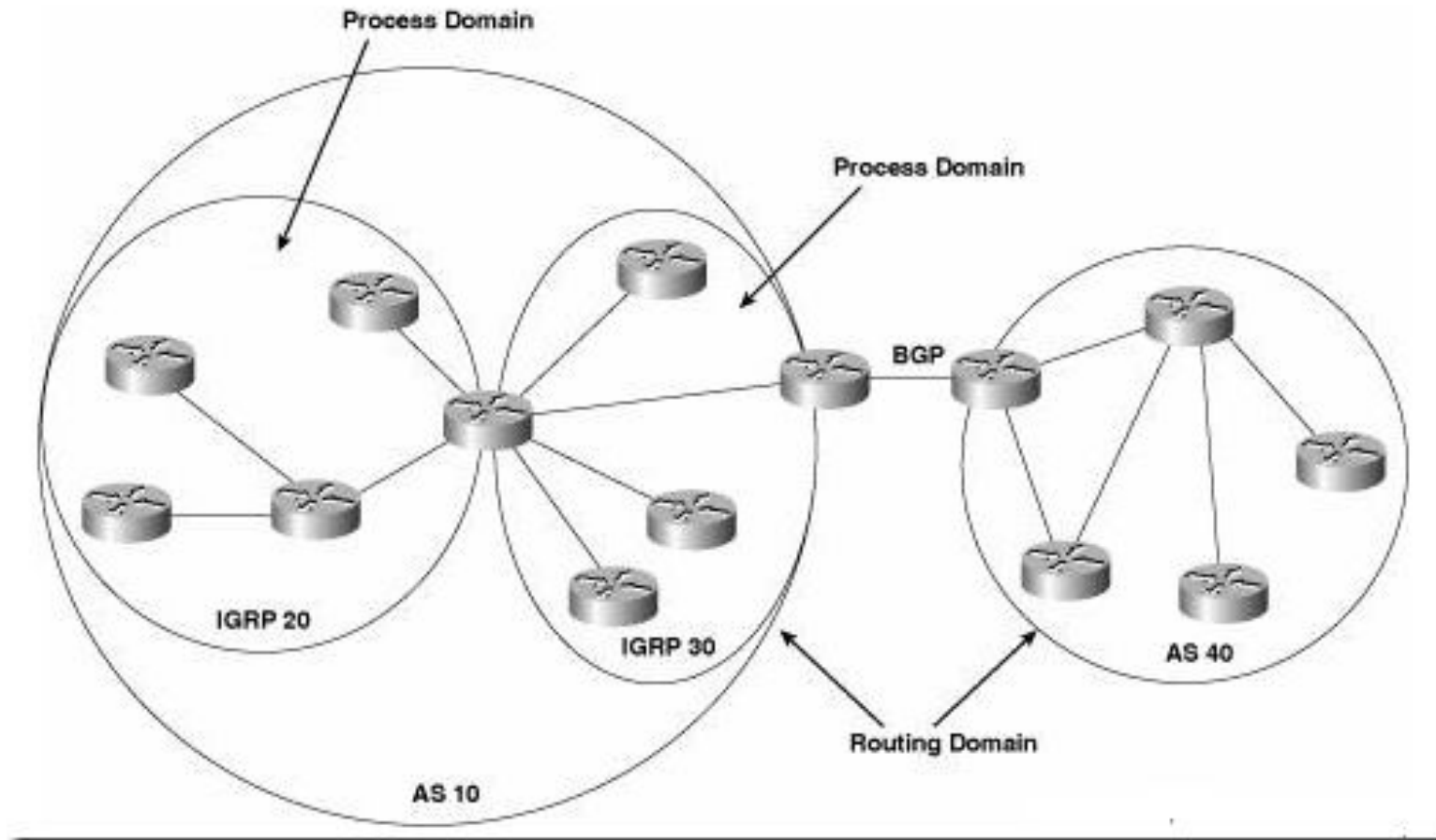
EIGRP uses the Diffusing-Update Algorithm (DUAL), which guarantees loop-free operation and provides fast router convergence.



# Autonomous System

**An autonomous system (AS)** is a single network or a group of networks that is controlled by a common network administrator (or administration body) that supports a common routing strategy and routing policies.

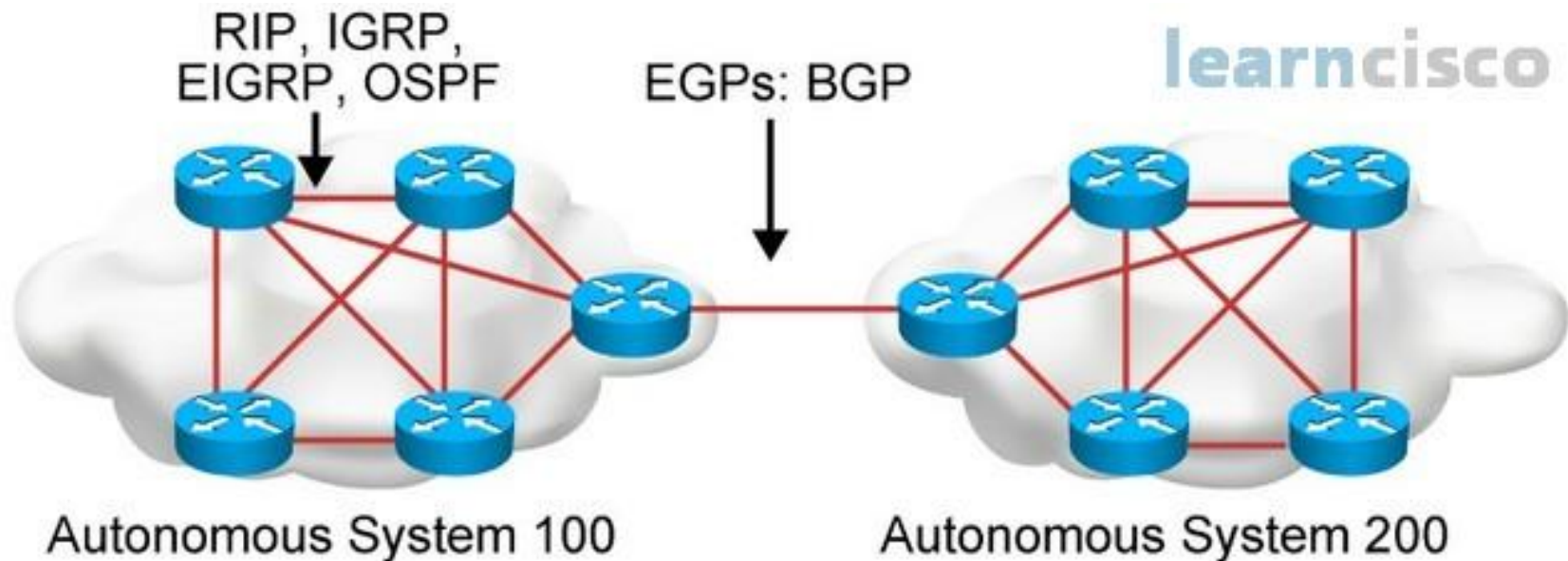
An autonomous system is assigned a globally unique number, sometimes called an **Autonomous System Number (ASN)**. It has a common routing strategy and routing policies.



# *Interaction of Autonomous Systems*

**Interior Gateway Protocols (IGPs)** are protocols for exchanging routing information between routers within an autonomous system (for example, a system of corporate Local Area Networks).

**Exterior Gateway Protocols (EGPs)** are protocols for exchanging routing information between neighbor gateway hosts in a network of autonomous systems.



# *Exterior Gateway Protocol*

---

The **Exterior Gateway Protocol (EGP)** is a routing protocol that was designed for the Internet.

At first it has been widely used in the U.S. Data Defence Network (DDN) and National Science Foundation Network (NSFNet).

Then it was used for routing information exchange between neighbouring gateway routers in autonomous systems.

**EGP is a distance vector protocol** that uses polling to retrieve routing information.

EGP has been superseded by BGP.

# ***Border Gateway Protocol***

---

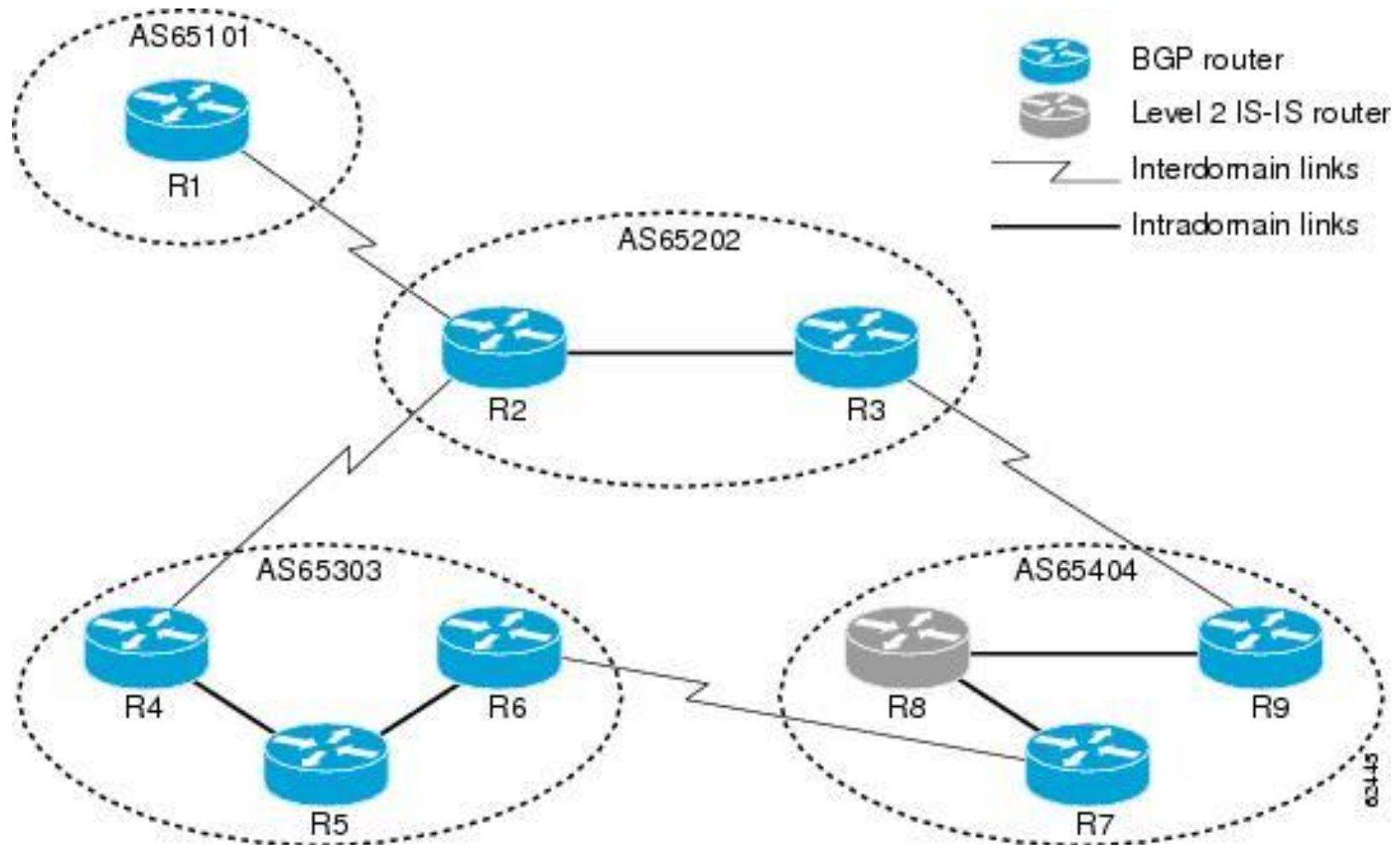
**Border Gateway Protocol (BGP)** is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems.

Each gateway host belongs to its autonomous system. Each gateway provides an access to routers that are constituted autonomous system.

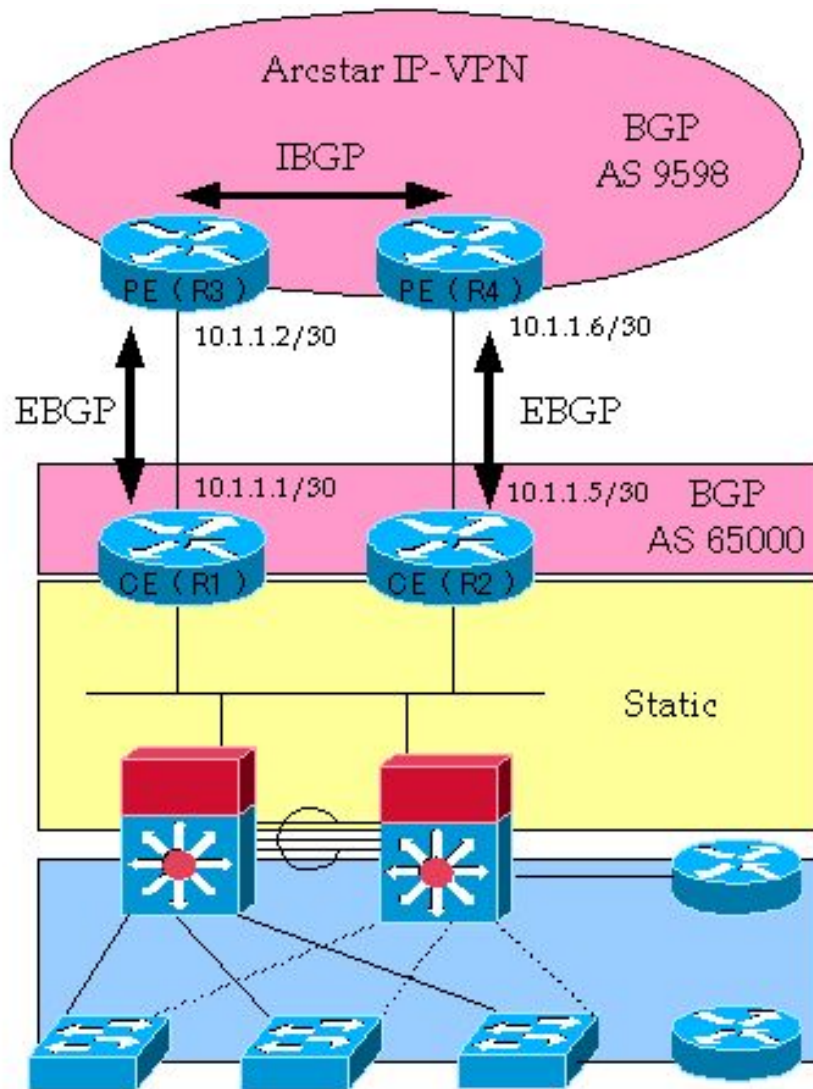
BGP protocol is often used between gateway hosts on the Internet.

**BGP-4**, the latest version, lets administrators configure cost metrics based on policy statements.

# ***A sample of Autonomous Systems***



# Internal BGP (IBGP)



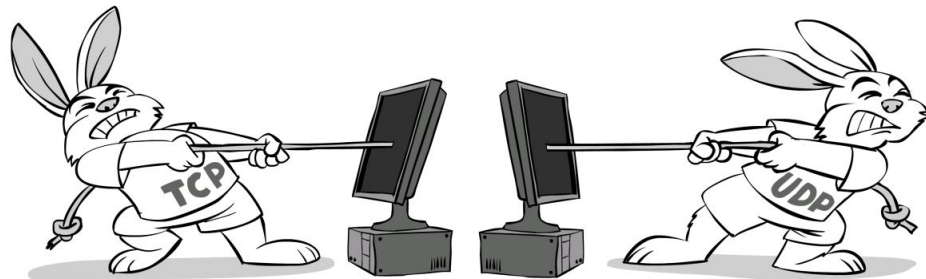
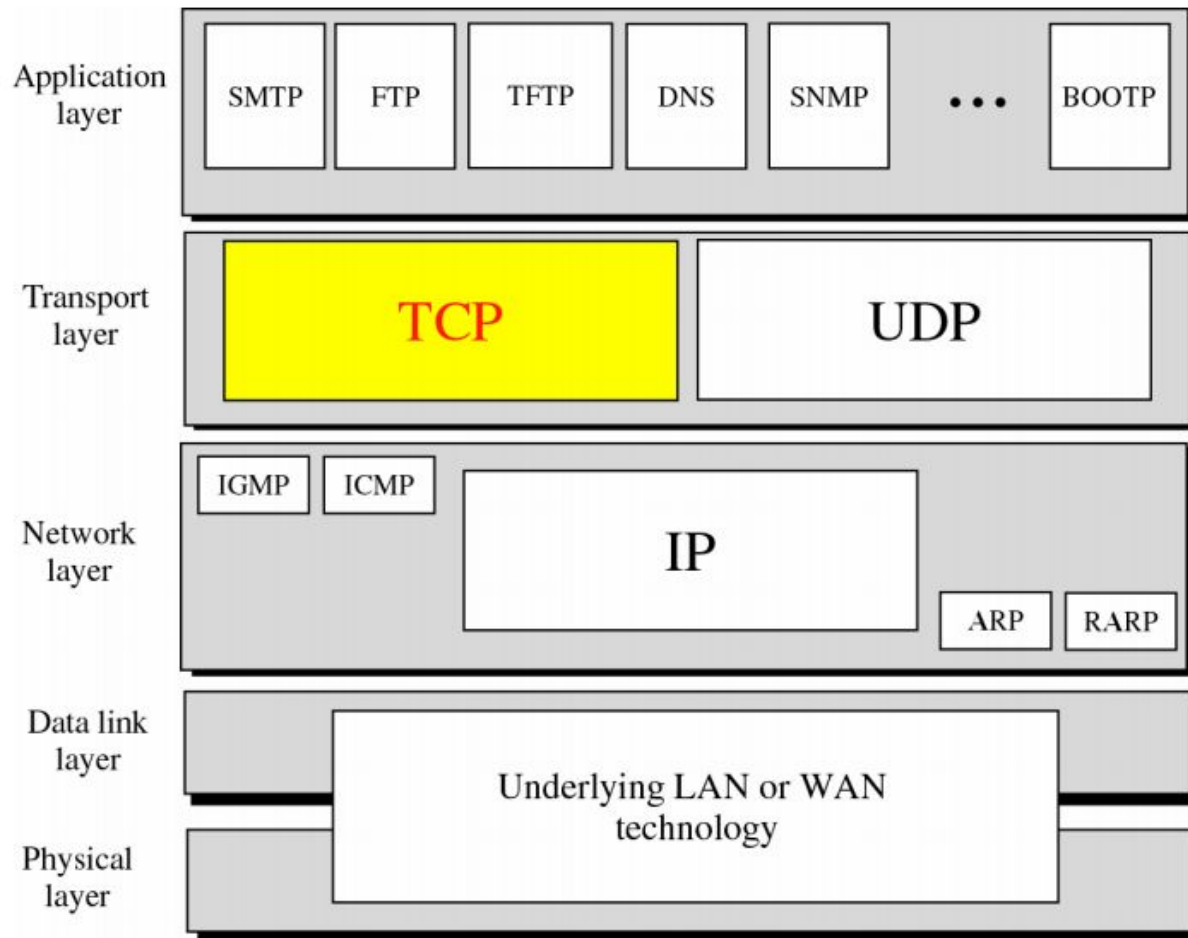
BGP communicates with autonomous networks using Internal BGP (IBGP) since it doesn't work well with Interior Gateway Protocols.

The BGP itself can be divided into two parts:

- External BGP (EBGP) and
- Internal BGP (IBGP).

An EBGP session connects two BGP routers which reside in different Autonomous Systems (AS), while an IBGP session links two BGP routers which belong to the same AS.

# Position of TCP in TCP/IP Protocols Stack





# ***Transmission Control Protocol (TCP)***

---

**Transmission control protocol** is a network communication protocol designed to provide sending data packets over the Internet.

**TCP** is a transport layer protocol in the OSI layer and is used to create a connection between remote computers by transporting and ensuring the delivery of messages over supporting networks and the Internet.

**The Transmission Control Protocol (TCP)** is a critically important part of the TCP/IP stack. It's also a fairly *(достаточно)* complicated protocol, with a lot of important concepts and mechanisms.

# *Characteristics of TCP*

---

**TCP is connection-oriented protocol.** Two process which desire to communicate using TCP must first request a creation of a connection.

A connection is closed when communication is no longer desired.

**Reliability** means that there is isome mechanisms which help to provide the guarantees of data transmission.

# ***UDP: User Datagram Protocol***

---

**UDP** is a connectionless and unreliable transport protocol.

User Datagram Protocol is used, in place of TCP, when a reliable delivery is not required. However, UDP is never used to send important data such as web-pages, database information, etc.

Streaming media such as video, audio and others use UDP because it offers speed.

# *Differences between TCP and UDP*

---

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

UDP & TCP were primarily designed for data. But popularity of carrying Voice over IP networks forced engineers to design a new transport layer protocol called **SCTP (Stream Control Transmission Protocol)**.

# Differences between TCP and UDP (2)

## Reliable vs Unreliable:

- **Reliable Protocols.** A reliable protocol requires that each transmission is acknowledged (*підтверджена*) by the receiving host. The sender retransmits, if necessary.
- **Unreliable Protocols.** An unreliable protocol does not require that each transmission is acknowledged by the receiving host.

## Connection-oriented vs. Connectionless

- **Connection-Oriented Protocols:** With connection-oriented protocols, one must establish a logical connection with the communication partner before exchanging data.
- **Connectionless Protocols:** With connectionless protocols, establishing a connection before sending data is not necessary.

# Differences between TCP and UDP (3)

## **Stateful (збереження стану) vs. Stateless Protocols**

This characteristics are networking concept. A server receives requests from clients. The transaction either takes place in a series of exchanges or it is a single request followed by (слідуюча) a response.

Stateful protocol means the server remembers what a client has done before. A stateful server keeps state between connections. Both systems keep track of the state of the communication session. (A "stateful" process requires the server to record the results of transactions so they can be recalled or resumed.)

**A stateless protocol** is one that does not maintain a relationship between requests. Each request is unrelated to any previous requests. An example of a stateless protocol is HTTP. Neither the client nor the server has an obligation to keep track of the state of the communication session.

# *Inventors of the TCP*

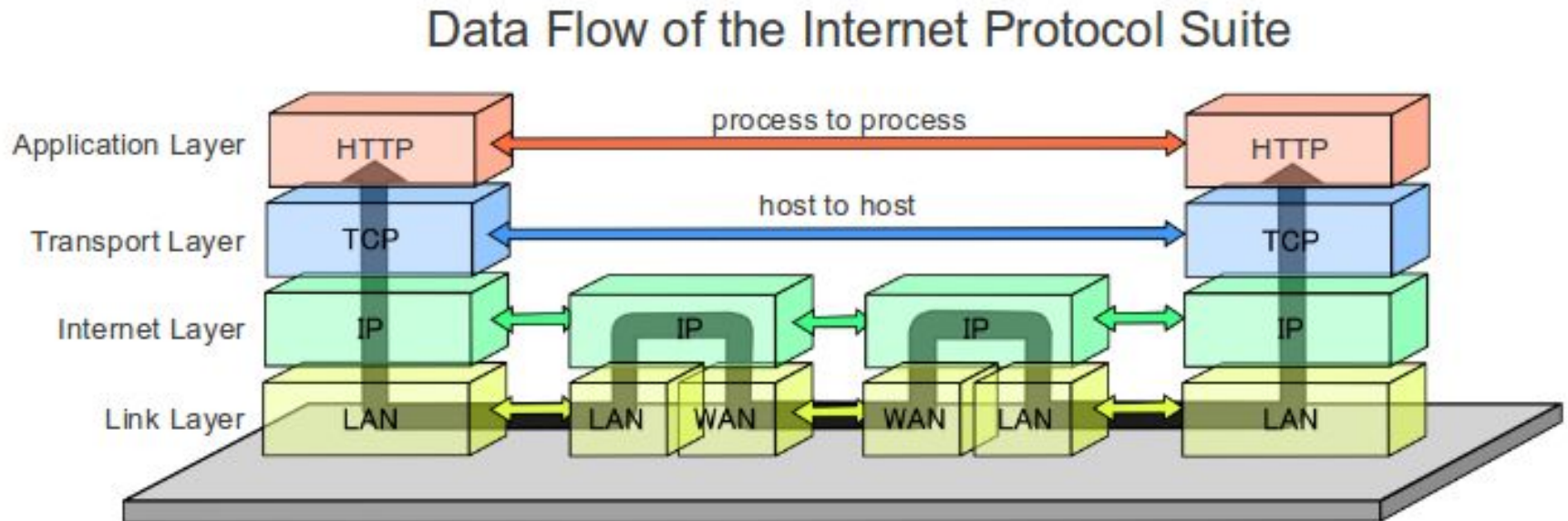
---



In May, 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper titled "A Protocol for Packet Network Interconnection." The paper's authors -- Vinton Cerf and Robert Kahn -- described a protocol called "TCP" that incorporated both connection-oriented and datagram services.



# *Transferring data in accordance with the TCP/IP stack.*



[https://commons.wikimedia.org/wiki/File:Data\\_Flow\\_of\\_the\\_Internet\\_Protocol\\_Suite.PNG](https://commons.wikimedia.org/wiki/File:Data_Flow_of_the_Internet_Protocol_Suite.PNG)