MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE”

Oleshchenko L.M.

COMPUTER SYSTEMS AND NETWORKS FUNDAMENTALS

Laboratory Work Tutorial

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для студентів, які навчаються
за спеціальністю 121 «Інженерія програмного забезпечення»
(освітня програма «Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем»)

Kyiv
Igor Sikorsky Kyiv Polytechnic Institute
2023

Рецензенти: Чумаченко Сергій Миколайович, д-р техн. наук, проф.
Мошенський Андрій Олександрович, канд. техн. наук, доц.

Відповідальний редактор Легеза Віктор Петрович, д-р техн. наук, проф.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 3 від 01.12.2022 р.)
за поданням Вченої ради факультету прикладної математики
(протокол № 4 від 28.11.2022 р.)

Electronic online educational publication

Oleshchenko Liubov Mykhailivna, PhD, Associate Professor

COMPUTER SYSTEMS AND NETWORKS FUNDAMENTALS

LABORATORY WORK TUTORIAL

Computer Systems and Networks Fundamentals: Laboratory Work Tutorial [Електронний ресурс]: tutorial is aimed at students of the speciality 121 “Software Engineering” (educational program «Software Engineering of Multimedia and Information Retrieval Systems») / Igor Sikorsky Kyiv Polytechnic Institute; Liubov M. Oleshchenko. – Electronic text data. – Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2023. – 85 p.

This tutorial is developed for familiarizing students with basic theory and practical methods of computer network components configuration. The tutorial includes the introduction and 4 sections devoted to a certain laboratory work. There are a work objective, a description of the task, theoretical information, and methodological instructions for every laboratory task; questions for self-assessment and a list of recommended literature. The tutorial is aimed at students of the speciality 121 “Software Engineering”, educational program “Software Engineering of Multimedia and Information Retrieval Systems” of the Faculty of Applied Mathematics of Igor Sikorsky Kyiv Polytechnic Institute.

CONTENTS

INTRODUCTION

Computer networks are used in all areas of human life: for education, communication, purchase of goods and services, recreation, remote work, control of intelligent devices of smart houses and city infrastructure devices, control of agricultural devices for soil condition monitoring, automatic watering of plants depending on environmental conditions and making managerial decisions in business. To manage smart devices, IT specialists must know not only programming technologies, but also data transmission technologies over the network, the principles of computer networks and their components, network applications, and the specifics of using network protocols for various applied tasks.

The discipline "Computer Systems and Networks Fundamentals" is part the of professionally-oriented disciplines cycle for bachelors of the speciality 121 “Software Engineering”.

This tutorial is developed for familiarizing students with theory and practical methods of computer systems and networks and requirements for laboratory works.

The purpose of the tutorial is to gain skills in creation and configuration of a local area network, configuration of network devices, IP addressing, checking the quality and security of network communications. Students also gain skills in Packet Tracer network simulation environment and Wireshark – the widely-used network protocol analyzer. The tutorial includes the introduction and 4 sections devoted to a certain laboratory work. There are a work objective, a description of the task, theoretical information and methodological instructions for every laboratory task; questions for self-assessment and a list of recommended literature.

The tutorial is aimed at students of the educational program “Software Engineering of Multimedia and Information Retrieval Systems” of the Faculty of Applied Mathematics of Igor Sikorsky Kyiv Polytechnic Institute.

LABORATORY WORK № 1. NETWORK DEVICES AND COMMUNICATIONS. PACKET TRACER SIMULATION ENVIRONMENT

Objective: to get acquainted with the main network devices and tools of data transmission of computer networks using the simulation environment Packet Tracer, learn how to add new devices to the simulator, make connections, configure nodes and test connections.

Theory and methodological instructions

Network Components

Network infrastructure contains three categories of network components:

- Devices;
- Media;
- Services.

End Devices

An end device is where a message originates from or where it is received. Data originates with an end device, flows through the network, and arrives at an end device.

Intermediary Network Devices

An intermediary device interconnects end devices in a network. Examples are: switches, wireless access points, routers, and firewalls.

Network Media

Types:

- Metallic wires within cables, such as copper.
- Glass, such as fiber optic cables.
- Wireless transmission.

Twisted-Pair is a type of copper cable. TP is the most common type of network cabling.

Coaxial Cable is usually made of copper or aluminum. It is used by cable television companies to provide service, and for satellite communication systems.

Fiber-optic cables are made of glass or plastic. They have a very high bandwidth, so they can carry vast amounts of data. Fiber-optic is used in backbone networks, large enterprise environments, and large data centers.

Twisted pair, coaxial cable and fiber optic lines are most often used as tools of communication. When choosing the type of cable take into account the following indicators:

- Cost of installation and service;
- Speed of information transfer;
- Restrictions on the amount of information transmission distance;
- Data security.

The main problem in the design computer networks are simultaneously providing these indicators. For example, the highest data rate is limited to the maximum possible data transmission distance, while still providing the required level of data protection. The expansion of the cable system affects its cost and security of data transmission.

Submarine communications cable

A submarine communications cable is a cable laid on the sea bed between land-based stations to carry telecommunication signals across stretches of ocean and sea (Fig.1.1.) [1].

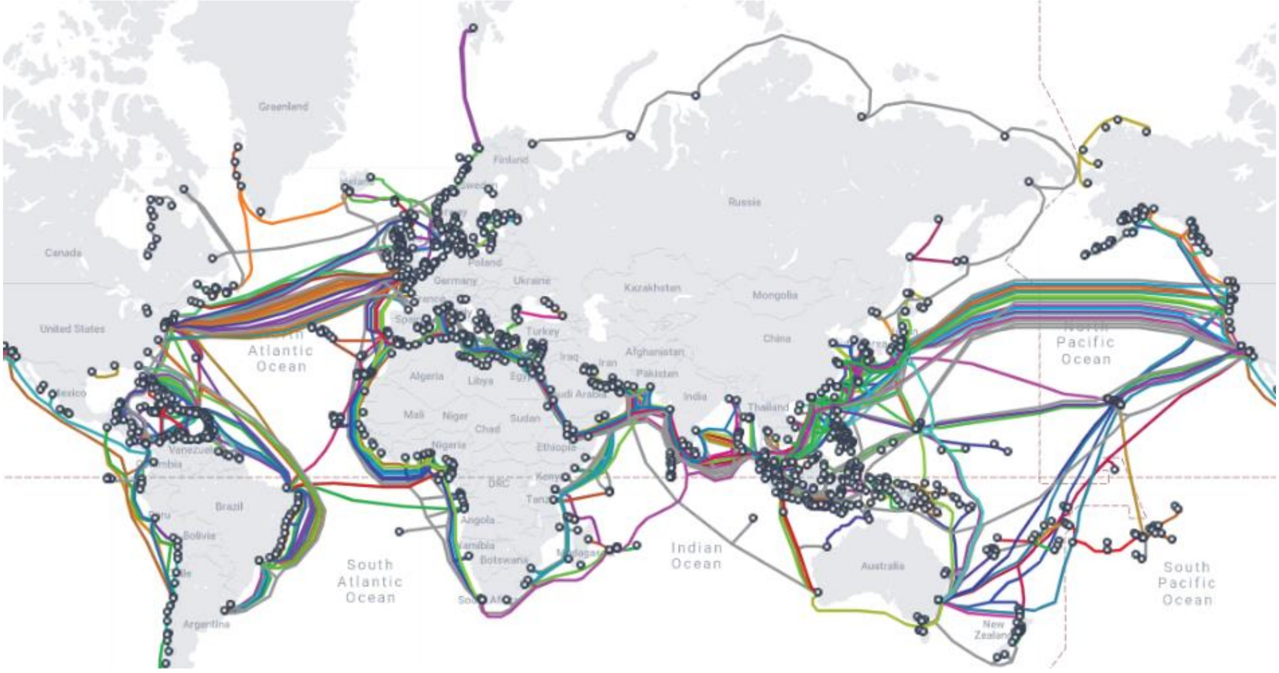
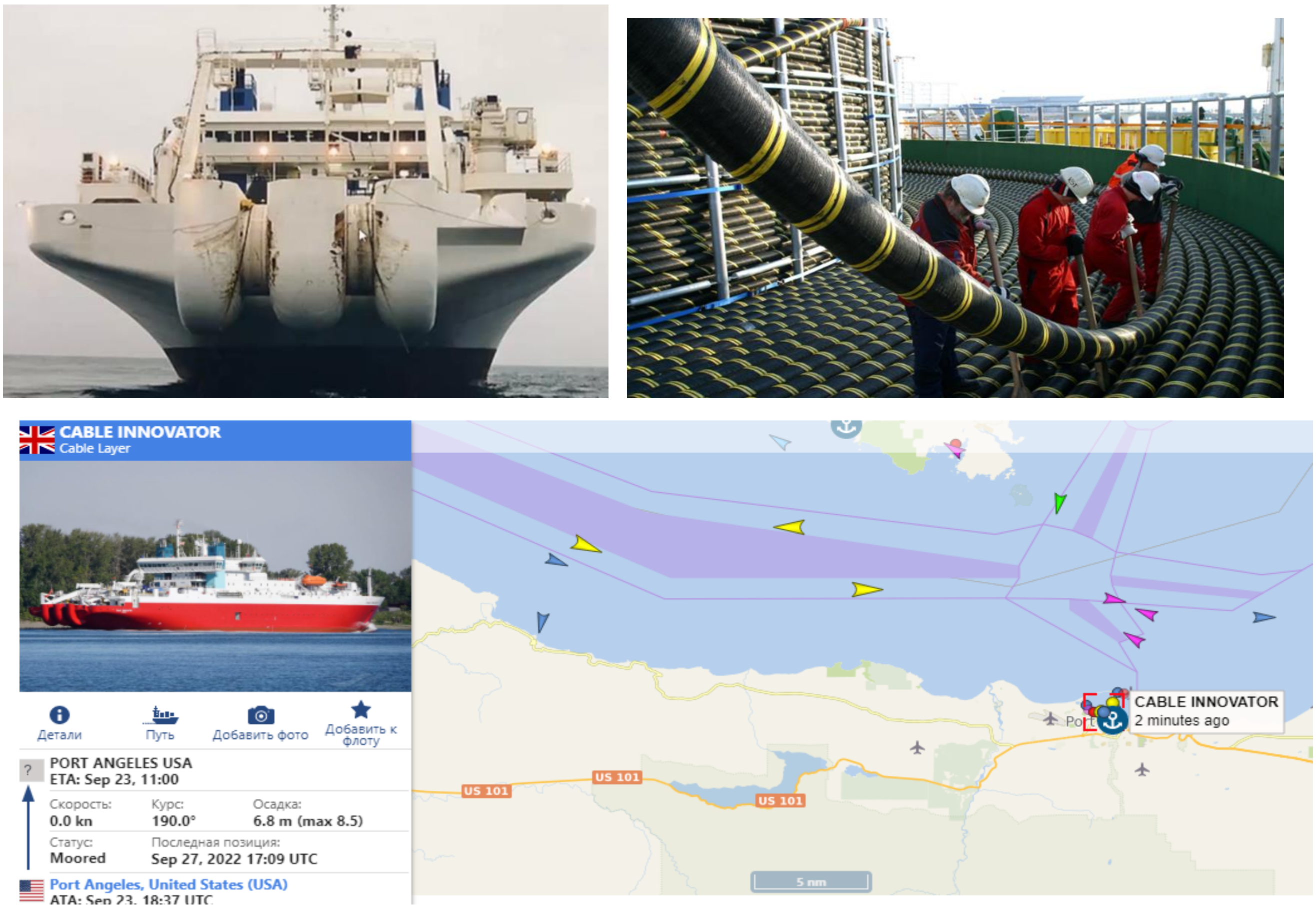


Fig.1.1. Submarine Cable Map

The first submarine communications cables laid beginning in the 1850s carried telegraphy traffic, establishing the first instant telecommunications links between continents, such as the first transatlantic telegraph cable which became operational on 16 August 1858. Subsequent generations of cables carried telephone traffic, then data communications traffic. Modern cables use optical fibre technology to carry digital data, which includes telephone, Internet and private data traffic.

Modern cables are typically about 25 mm in diameter and weigh around 1.4 tonnes per kilometre (2.5 short tons per mile; 2.2 long tons per mile) for the deep-sea sections which comprise the majority of the run, although larger and heavier cables are used for shallow-water sections near shore. Submarine cables first connected all the world's continents (except Antarctica) when Java was connected to Darwin, Northern Territory, Australia, in 1871 in anticipation of the completion of the Australian Overland Telegraph Line in 1872 connecting to Adelaide, South Australia and thence to the rest of Australia. For planning and installing cables in the ocean, we need a lot of technology, effort and money (Fig.1.2).



CABLE INNOVATOR
Cable Layer

PORT ANGELES USA
ETA: Sep 23, 11:00

Скорость: 0.0 kn
Курс: 190.0°
Осадка: 6.8 m (max 8.5)

Статус: Moored
Последная позиция: Sep 27, 2022 17:09 UTC

Port Angeles, United States (USA)
ATA: Sep 23, 18:37 UTC

Fig.1.2. Cable Innovator (carries up to 8500 cables and lays it under water) [2]

Networks of Many Sizes

- **Small Home Networks** – connect a few computers to each other and the Internet.
- **Small Office/Home Office** – enables computer within a home or remote office to connect to a corporate network.
- **Medium to Large Networks** – many locations with hundreds or thousands of interconnected computers.
- **World Wide Networks** – connects hundreds of millions of computers world-wide – such as the Internet.

Clients and Servers

Servers are computers that provide information to end devices on the network. For example, email servers, web servers, or file server

Clients are computers that send requests to the servers to retrieve information such as a web page from a web server or email from an email server.

Client and server software usually run on separate computers.

Peer-to-Peer

Each device (known as a peer) can function as both a server and a client. These networks are called peer-to-peer networks.

Peer-to-peer networking advantages: easy to set up, less complex, and lower cost.

Disadvantages: no centralized administration, not as secure, not scalable, and slower performance.

Common P2P networks include:

- G2;
- Bitcoin;
- BitTorrent;
- eDonkey.

Some P2P applications are based on the Gnutella protocol, where each user shares whole files with other users. Many P2P applications allow users to share pieces of many files with each other at the same time – this is BitTorrent technology.

Types of networks

Local Area Network (LAN) – spans a small geographic area owned or operated by an individual or IT department. Spans a small geographic area such as a home, school, office building, or campus. Usually administered by a single organization or individual. Provides high speed bandwidth to end and intermediary devices within the network.

Wide Area Network (WAN) – spans a large geographic area typically involving a telecommunications service provider. WANs interconnect LANs over wide geographical areas such as between cities, states, or countries. Usually administered by multiple service providers.

WANs typically provide slower speed links between LANs.

Other types of networks:

- Metropolitan Area Network (MAN).
- Wireless LAN (WLAN).
- Storage Area Network (SAN).

The Internet

The Internet is a worldwide collection of interconnected LANs and WANs. LANs are connected to each other using WANs. WANs are then connected to each other using copper wires, fiber optic cables, and wireless transmissions.

Data Centers

Cloud computing is possible thanks to Data Centers. Data center is a building in which computer systems and components are located, such as:

- Connecting cables for data transmission.
- High-speed virtual servers (clusters).
- Backup data storage systems.
- Reserve power.
- Aair conditioning systems.
- Safety devices.

The data center can be one room in the building, one or several floors or the entire building. Modern data centers are used for cloud computing and virtualization to effectively process large amounts of data. Data centers are usually expensive to create and maintain (Fig. 1.3).

Fig.1.3. Data center example.

Network Security Solutions

Network security components for home or small office network:

- Antivirus software.
- Firewall filtering.

Larger networks have additional security requirements:

- **Dedicated firewall system** to provide more advanced firewall capabilities.
- **Access control lists (ACL)** – used to filter access and traffic forwarding.
- **Virtual private networks (VPN)** – used to provide secure access for remote workers.

Network Protocols

Networking protocols define a common format and set of rules for exchanging messages between devices. Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).

Internet Standards

- **Internet Society (ISOC)** – promotes open development and evolution of Internet use globally.
- **Internet Architecture Board (IAB)** – management and development of Internet standards.
- **Internet Engineering Task Force (IETF)** – develops, updates, and maintains Internet and TCP/IP technologies.

Internet Corporation for Assigned Names and Numbers (ICANN) – coordinates IP address allocation and management of domain names.

Internet Assigned Numbers Authority (IANA) – manages IP address allocation, domain name management, and protocol identifiers for ICANN.

Internet Research Task Force (IRTF) – focused on long-term research related to Internet and TCP/IP protocols.

OSI model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network (Table 1.1).

Table 1.1. OSI Layer Description

OSI Layer	OSI Layer Description
7. Application	contains protocols used for process-to-process communications.
6. Presentation	provides for common representation of the data.
5. Session	provides services to the presentation layer to organize its dialogue and to manage data exchange**.**
4. Transport	defines services to segment, transfer, and reassemble the data.
3. Network	provides services to exchange the individual pieces of data over the network between identified end devices.
2. Data Link	provides methods for exchanging data frames between devices over a common media.
1. Physical	describes the mechanical, electrical, functional, and procedural means to transmit bits across physical connections.

IP Addressing

Each end device on a network (e.g., PCs, laptops, servers, printers, VoIP phones, security cameras) require an IP configuration consisting of:

- IP address.
- Subnet mask.
- Default gateway.

Interface Addressing Verification

The IP configuration on a Windows host is verified using the **ipconfig** command.

To verify the interfaces and address settings of intermediary devices like switches and routers, use the **show ip interface brief** privileged command.

End-to-End Connectivity Test

The **ping** command can be used to test connectivity to another device on the network or a website on the Internet. The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.

If a reply is not received within the timeout, ping provides a message indicating that a response was not received. It is common for the first **ping** to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

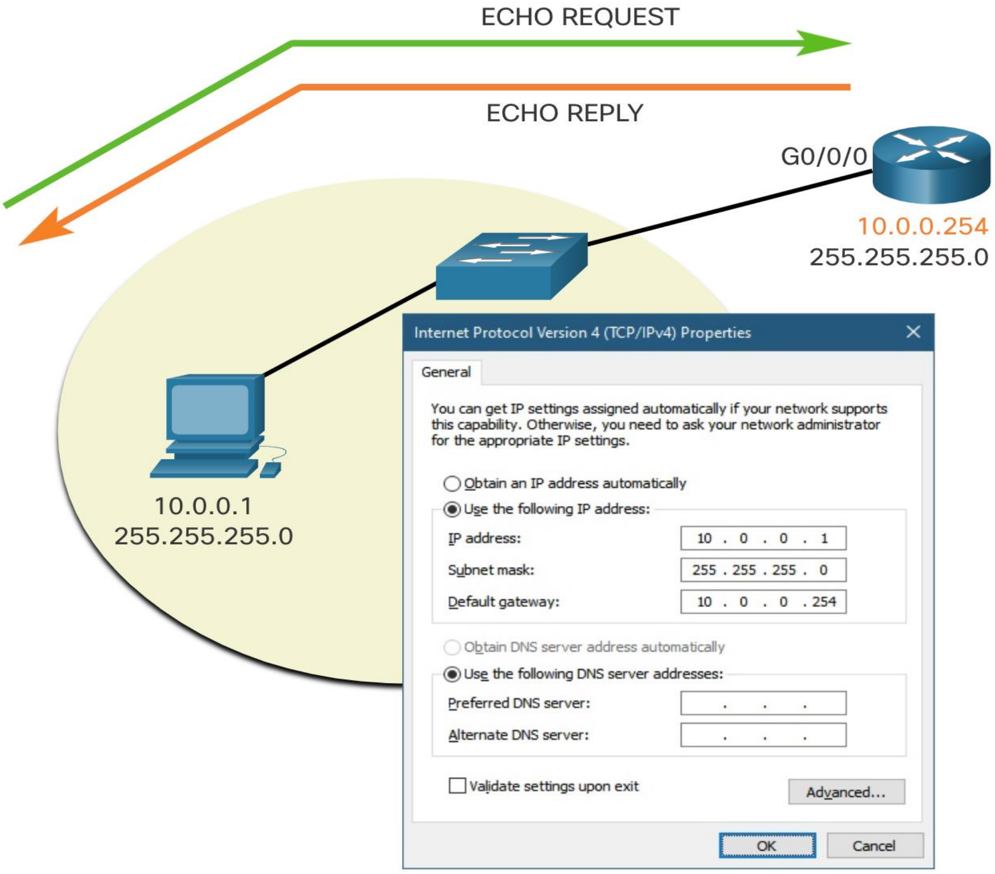
Ping the Loopback

Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, ping the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).

A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host.

Ping the Default Gateway

The **ping** command can be used to test the ability of a host to communicate on the local network. The default gateway address is most often used because the router is normally always operational. A successful ping to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network. If the default gateway address does not respond, a ping can be sent to the IP address of another host on the local network that is known to be operational.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Fig.1.4. Ping the Default Gateway.

Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork. A local host can ping a host on a remote network. A successful ping across the internetwork confirms communication on the local network. Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a ping response could be due to security restrictions.

Network devices

Networks card, network adapter, Ethernet adapter, NIC (*network interface card*) is responsible for the transfer of information between network units. Any network card consists of a connector for a network conductor and a microprocessor that encodes / decodes network packets and from auxiliary software and hardware complexes and services. Each network card has its own physical **MAC address** (*Media Access Control*) – a unique identifier of the device.

This is an identifier that is compared to different types of equipment for computer networks. In the case of Ethernet networks, this is a unique identifier (number) of the network card. MAC address format – 6 pairs of numbers and letters, usually separated by a hyphen or a colon. For example: **00: 1D: 72: 1F: AC: 95** or: **00-3D-42-3F-SC-95** .

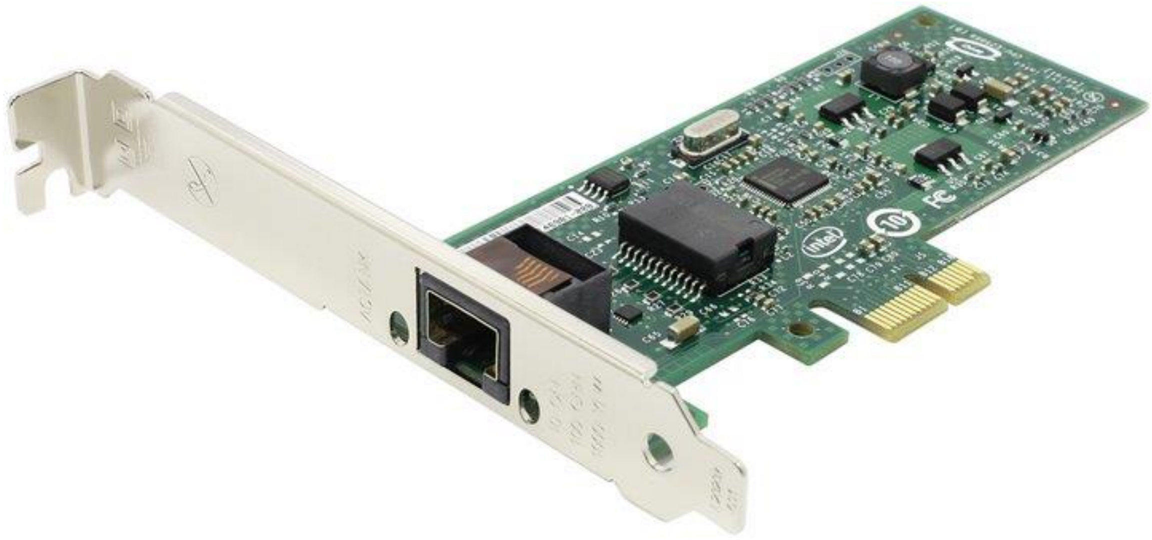


Fig.1.5. Network card

Network environment

Modern networks use mainly three types of environments that connect devices and provide the path through which data is transmitted. These types of environments include:

- **metal wires inside the cable;**
- **glass or plastic fibers (fiber optic cable);**
- **radio communication.**

The encoding of the signal required for transmission is different depending on the type of medium.

In metal wires, the data is encoded in the form of electrical pulses that correspond to certain patterns.

Transmission in **fiber-optic networks occurs in the form of light pulses, in the range of infrared radiation or visible light**.

In **wireless transmission, electromagnetic radiation patterns are used to describe different bit values**.

Copper cables

There are three main types of copper cables in network technologies:

- **coaxial cable;**
- **unshielded twisted pair (UTP);**
- **shielded twisted pair (STP).**

These cables are used to connect LAN nodes and network infrastructure devices such as switches, routers, and wireless access points. Each type of connection and the corresponding devices have certain requirements for cables provided by physical level standards.

Coaxial cable

Coaxial cable has an average price, is well noise-proof and is used for long-distance communication (several kilometers). A coaxial cable is so named because the **two conductors in it use the same axis.**

Coaxial cable consists of the following elements:

- copper conductor for transmission of electrical signals;
- copper conductor surrounded by elastic plastic insulation;
- insulating material surrounded by copper braid or metal foil.

This screen reduces the number of external electromagnetic interference.

The entire cable is covered with a cable sheath to protect against minor physical damage.

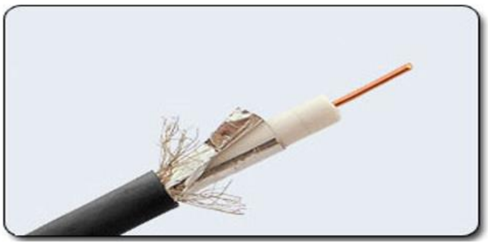


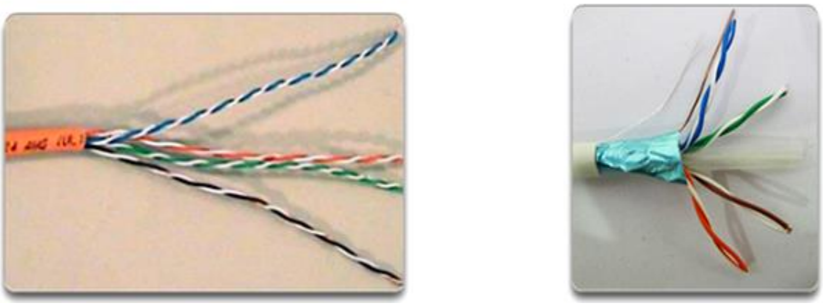
Fig.1.6. Coaxial cable

The data transfer rate is from 1 to 10 Mbit / s, in some cases up to 50 Mbit / s. Coaxial cable is used for basic and broadband information transmission.

Twisted pair

The cheapest cable connection is a twisted twisted pair wire connection. Supports data transmission at a distance of up to 100 meters. At long distances the signal is not recognized due to attenuation; if long-distance data transmission is still required, you have to use a repeater, or use a coaxial cable. The advantages are low price and trouble-free installation.

Unshielded twisted pair consists of eight wires. Each wire is insulated separately; all eight wires are assembled in four twisted pairs. Curling wires prevents cross-barriers caused by adjacent pairs and external sources. All four pairs are placed in a common shell.



a) unshielded twisted pair (UTP); b) shielded twisted pair (STP)

Fig.1. 7. Twisted pair

Shielded twisted pair is often used, ie twisted pair placed in a shielding sheath, similar to a coaxial cable shield. This increases the cost of twisted pair and brings its price closer to the price of coaxial cable.

Twisted pair has supplanted coaxial cable due to several obvious advantages. The twisted pair cable consists of eight separate wires, which makes it more flexible than coaxial and, accordingly, facilitates its laying. The minimum set of equipment for a twisted -pair network includes the following elements:

- network adapters (by the number of computers connected to the network);
- UTP connectors RJ-45;
- cable segments with RJ-45 connectors at both ends (according to the number of computers connected);
- switch that has as many UTP ports with RJ-45 connectors as you have to connect computers.

Cable categories

There are several categories of twisted pair cable, which are numbered from **CAT 1** to **CAT 8.2** . A higher category cable usually contains more pairs of wires and each pair has more turns per unit length.

Categories of unshielded twisted pair are described in EIA / TIA 568 .

Fiber optic lines

The most expensive are fiber optics, or fiberglass cables.

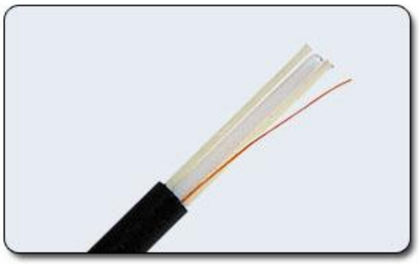


Fig. 1. 8. Fiber Optic

Permissible distance of more than 50 km. External action of obstacles is practically absent. This is currently the most expensive connection. It is used where there are electromagnetic interference fields or the need to transmit information over very long distances without the use of repeaters. They have anti-eavesdropping properties, as the technique of branches in fiber optic cables is very complex.

The transmission of information is via two fiber-optic cables that transmit signals in different directions. Sometimes two-wire fiber-optic cables containing two cables are used in a common outer sheath, but more often two single cables.

Contrary to popular belief, the cost of fiber optic cable is not very high (it is close to the cost of thin coaxial cable). However, in general, the equipment in this case is significantly more expensive, as it requires the use of expensive fiber-optic transceivers.

The main advantages of data transmission over fiber-optic communication lines are:

- High data rate – 3GHz, while for copper cable this value is not more than 500 MHz.
- Insensitivity to electromagnetic interference .
- Absence of electromagnetic radiation during data transmission .
- Providing galvanic isolation between transmitter and receiver.

Fiber optic cable consists of the following components: optical fiber, optical shield, protective shield.

Own transmission medium – optical fiber is a glass or plastic core, the thickness of which, depending on the purpose of the cable can vary from units to hundreds of microns.

Cables with a fiber diameter of 10 microns are called **single-mode** by the name of the radiation mode of the transmitting element – the laser. Cables with a fiber diameter of 60 microns or more are called **multimode**.

Single mode fiber optic cables (*Single Mode Fiber* – SMF) are more difficult to manufacture and operate, however, they are able to provide a long range of information signal. Cheaper in manufacture and more convenient in operation multimode (*Multi Mode Fiber* – MMF) cables provide a shorter range of information signal.

Features of wireless environment

With the help of ultra-high frequencies, wireless data carriers transmit electromagnetic signals that represent bits of transmitted information.

Unlike copper and fiber optic cables, wireless network as a network environment is not limited to conductors. Wireless data transmission medium is characterized by the greatest mobility. The number of wireless devices is constantly growing. That's why wireless networking has become an environment for home networks. Also, the popularity of wireless networks is growing rapidly due to the growing bandwidth of the network.

However, the wireless network has some **problem areas:**

- **Coverage area**. Wireless data technologies work well in open spaces. However, some structural materials used in buildings as well as terrain conditions may limit the coverage area.
- **Obstacles**. The wireless network is susceptible to cross-interference, and its operation may be impaired by conventional devices, such as cordless telephones, television receivers, certain types of fluorescent lamps, microwave ovens, and other wireless communications.
- **Security.** Wireless coverage is not limited to terms of access to the environment. Therefore, unauthorized users and devices can access the transfer. Therefore, network security tools are a key component of wireless network administration.

Three data transmission standards apply to wireless networks.

IEEE 802.11 Standard: Wireless Local Area Network (WLAN) technology, commonly referred to as Wi-Fi, uses a competing or non-deterministic multiple access system (CSMA / CA).

IEEE 802.15 standard: a wireless personal area network standard known as Bluetooth; for data transmission at distances from 1 to 100 meters requires a close location of two devices.

IEEE 802.16 standard: known as the Broadband Radio Protocol (WiMAX); uses a point-to-point topology to provide wireless broadband access.

Although the popularity of wireless desktops is growing, copper and fiber optic cables are the most popular networking environment on the physical layer. There are a number of principles for building networks based on the components discussed above. Such principles are also called topologies.

Topologies of computer networks

Star topology

This is the apology of a network with a clearly defined center to which all other subscribers are connected. The exchange of information is exclusively through the central computer, which bears a greater load, so nothing but the network, he usually can not do. The network of central subscriber equipment must be significantly more complex than the equipment of peripheral subscribers. The central computer is the most powerful, it is entrusted with all the functions of exchange management. No conflicts in the network with the " star " topology are in principle possible, because the control is completely centralized.

If we talk about the resilience of the star to computer failures, the failure of the peripheral computer or its network equipment does not affect the functioning of the network, but any failure of the central computer makes the network completely inoperable. In this regard, special measures should be taken to increase the reliability of the central computer and its network equipment .

Network bandwidth is determined by the computing power of the node and is guaranteed for each workstation. Data collisions do not occur.

The cable connection is quite simple, as each workstation is connected to a node. The cost of laying cables is high, especially when the central node is not geographically located in the center of the topology.

When expanding network , previously made cable connections cannot be used: a separate cable from the network center must be laid to the new workstation.

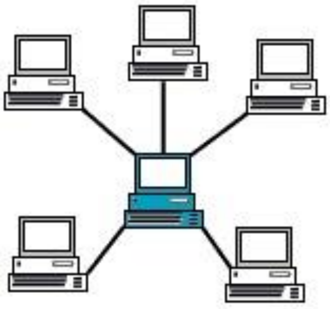


Fig. 1.9. Star topology

Star topology is the fastest of all topologies and computer networks , because the transmission of data between workstations passes through a central node (with its good performance) on individual lines used only by these workstations. The frequency of requests for information transfer from one station to another is low compared to that achieved in other topologists .

Central control node – the file server implements the optimal mechanism of protection against unauthorized access to information. The entire network can be managed from its center.

Ring topology

In a ring network topology, the workstations are connected to each other in a circle, ie workstation 1 with workstation 2, workstation 3 with workstation 4, and so on. The last workstation is connected to the first. The communication link is closed in a ring. Laying cables from one workstation to another can be quite complex and expensive, especially if the geographical location of the workstations is far from the shape of the ring (for example, a line).

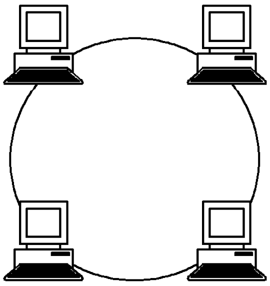


Fig. 1.10. Ring topology

Messages circulate regularly in a circle . The workstation sends information to a specific destination address, having received a request from the ring in advance.

Sending messages is very efficient, as most messages can be sent over the cable system one by one. It is very easy to make a ring request to all stations. The duration of information transfer increases in proportion to the number of workstations included in the computer network.

The main problem with the ring topology is that each workstation must be actively involved in sending information, and in the event of failure of at least one of them, the entire network does not work . Connecting a new workstation requires a short emergency shutdown, as the ring must be open during installation. There is no limit to the length of the computer network, as it is determined solely by the distance between the two workstations.

Bus topology

In a bus topology, the information transmission medium is presented in the form of a communication path, accessible to all workstations to which they must all be connected. All workstations can come into direct contact with any workstation available on the network.

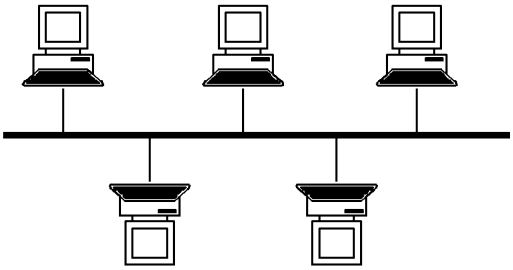


Fig. 1.11. Bus topology

Workstations can be connected to or disconnected at any time without interrupting the entire network. The operation of the network does not depend on the state of the individual workstation. Due to the fact that workstations can be connected without interrupting network processes and communication environment, it is very easy to listen to information.

The main characteristics of the three most typical network topologies data transfers are shown in table 1.2.

Table 1.2. Basic characteristics of computer network topologies

FEATURES	NETWORK TOPOLOGIES		
	Star	**Ring**	**Bus**
The cost of expansion	Insignificant	Average	Average
Connecting subscribers	Passive	Active	Passive
Failure protection	Insignificant	Insignificant	High
System size	Arbitrary	Arbitrary	Limited
Eavesdropping	Good	Good	Insignificant
Connection cost	Insignificant	Insignificant	High
Behavior of the system at high loads	Good	Satisfactory	Bad
Ability to work in real time	Very good	Good	Bad
Cable distribution	Good	Satisfactory	Good
Service	Very good	Average	Average

Tree topology

The combined or tree-like structure is formed in the form of combinations of the above – mentioned topologies of computer networks. The base of the network tree (root) is located at the point where the communication lines of information (tree branches) gather.

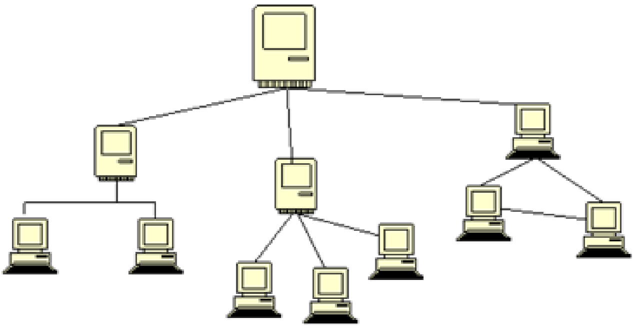


Fig. 1.12. Tree structure of the network

Networks with a tree structure are used where the direct use of basic network structures in its pure form is not possible. Network amplifiers and switches are used to connect a large number of workstations in accordance with adapter boards.

Packet Tracer simulation environment

Cisco Packet Tracer allows to create network topologies from a wide range of routers and switches, workstations and network connections such as Ethernet , Serial , ISDN . This function can be performed for both training and work, for example, to perform network settings at the planning stage or to create a copy of the working network to troubleshoot. To run Packet Tracer needs to run the executable file **PacketTracer.exe.** The general view of the program is shown in Fig.1.13.

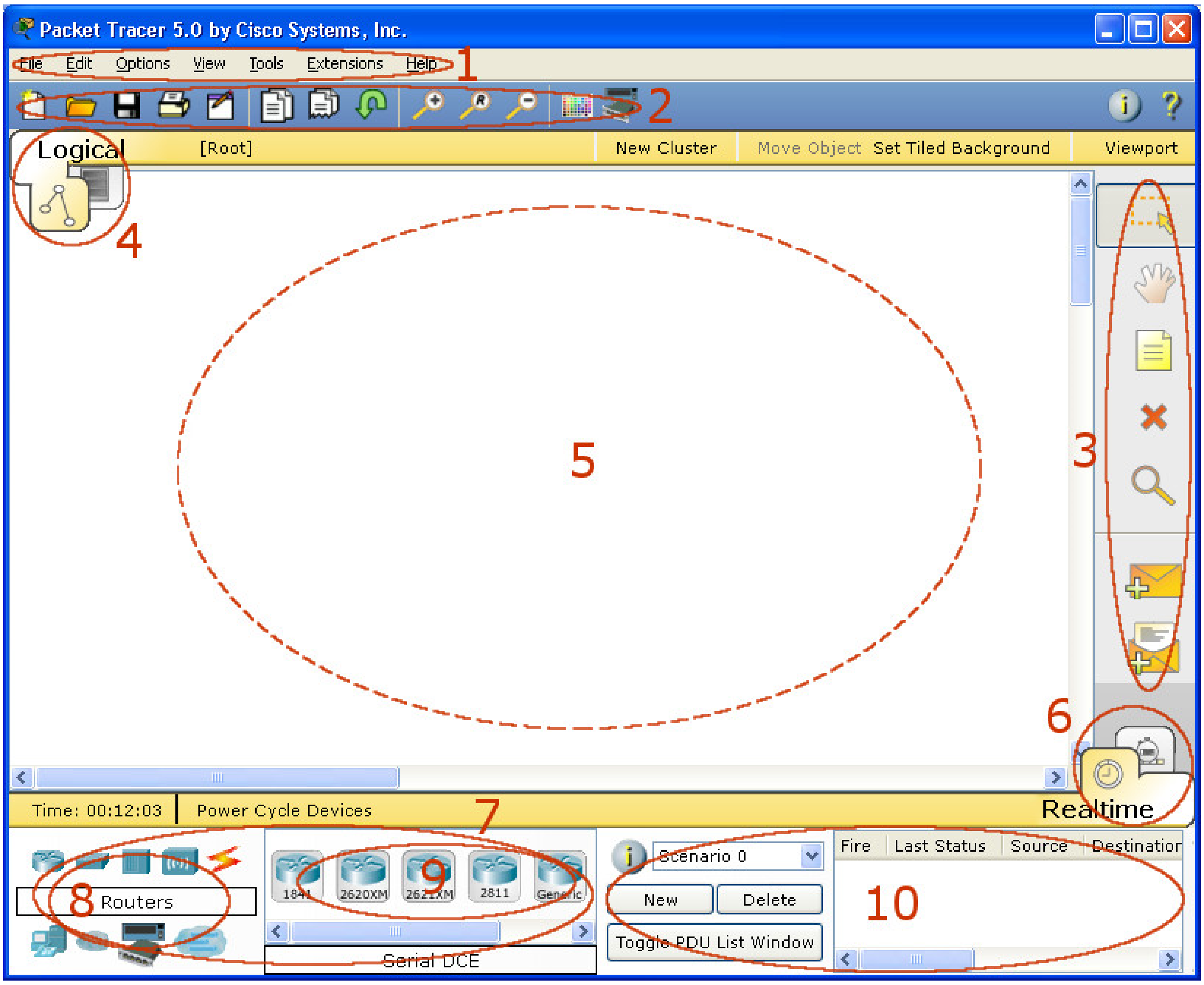


Fig.1. 13. Cisco Packet Tracer simulation environment

The working area of the program window consists of the following elements:

1. **Menu Bar** – a panel that contains the menu File, Edit, Options, View, Tools, Extensions, Help.
2. **The Main Tool Bar** contains graphic images of shortcuts to access the menu commands File, Edit, View and Tools as well also Network Information button.
3. **Common Tools Bar** is a panel that provides access to the most used tools of the program: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU and Add Complex PDU.
4. **Logical / Physical Workspace and Navigation Bar** – a panel that gives possibility switch working area : physical or logical , and also allows move between levels cluster .
5. **Workspace** – the area in which the network is created, simulation observations are carried out, various information and statistics are visible.
6. **Realtime / Simulation Bar** – Use the tabs in this panel to switch between Realtime mode and Simulation mode. It also contains Power Cycle Devices buttons, Play Control buttons and an Event List switch in Simulation mode.
7. **Network Component Box** – the area in which devices and connections are selected to place them on the workspace. She contains Device area – Type Selection and Device area – Specific Selection.
8. **Device - Type Selection Box** – area contains available types devices and connections in Packet Tracer. The Device – Specific Selection area changes depending from selected device .
9. **Device - Specific Selection Box** – an area used to select specific devices and connections needed to build in the network workspace.
10. **User Created Packet Window** – this window manages packets that were created on the network during the simulation of the script.

To create a topology, we have to select a device from the **Network Component panel**, and then select the type of the selected device from the **Device - Type Selection panel.**

Then we have to click the left mouse button in the field of the workspace of the program (**Workspace**). We can also move the device directly from the **Device - Type Selection area**, but the default device model will be selected.

To quickly create multiple instances of the same device, hold down the **Ctrl key**, click on the device in the **Device – Specific Selection area**, and release the **Ctrl key**. You can then tap the workspace several times to add copies of the device.

Network evices are presented in Packet Tracer:

- routers;
- switches;
- end devices – PCs, servers, printers, IP phones;
- wireless devices: access points and wireless routers;
- other devices – cloud, DSL modem and cable modem, etc.

Add the necessary elements to the work area of the program as shown in Fig.1. 14.

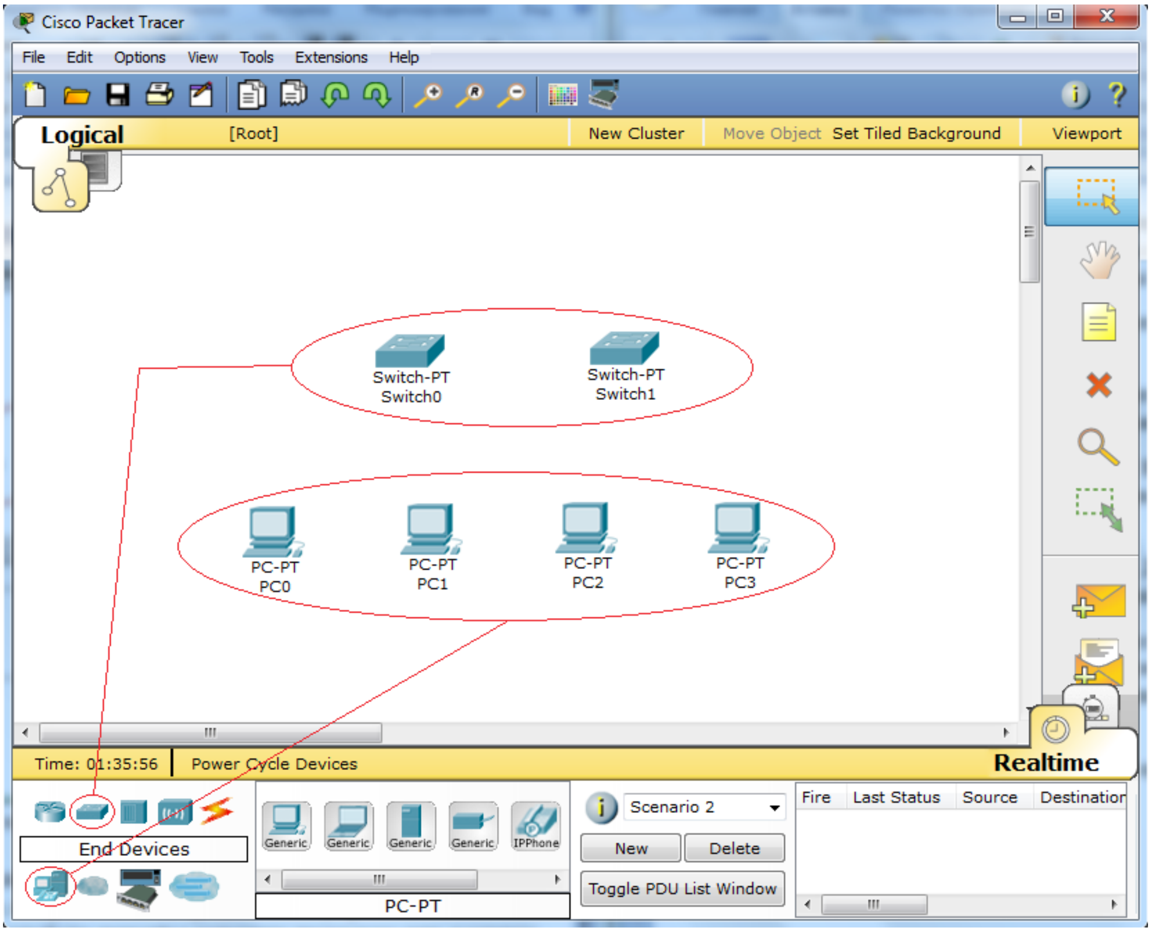


Fig.1. 14. Adding network elements

When adding each element, the user has the opportunity to give it a name and set the necessary parameters. To do this, left-click on the desired item and go to the **Config** tab in the device dialog box.

The properties dialog box for each item has two tabs: **Physical** – contains the graphical interface of the device and allows to simulate working with it on a physical level. **Config** – contains all the necessary parameters for configuring the device and has a user-friendly interface.

Depending on the device, the properties may have an additional tab to control the operation of the selected item: **Desktop** (if the end device is selected) or **CLI** (if a router is selected) and so on. Use the **Delete** (Del) button to remove unwanted devices from the application workspace. We will connect the added elements with the help of connecting links. To do this, select the **Connections tab** from the **Network panel Component Box** . We will see all possible types of connections between devices. Select the appropriate cable type. The mouse pointer changes to the "connection" cursor. Click on the first device and select the appropriate interface to which you want to connect, and then click on the second device, performing the same operation. You can also connect using **Automatically Choose Connection Type** (automatically connects elements in the network). Select and click on each of the devices to be connected. A cable connection will appear between the devices, and the indicators at each end will show the connection status (for interfaces that have an indicator).

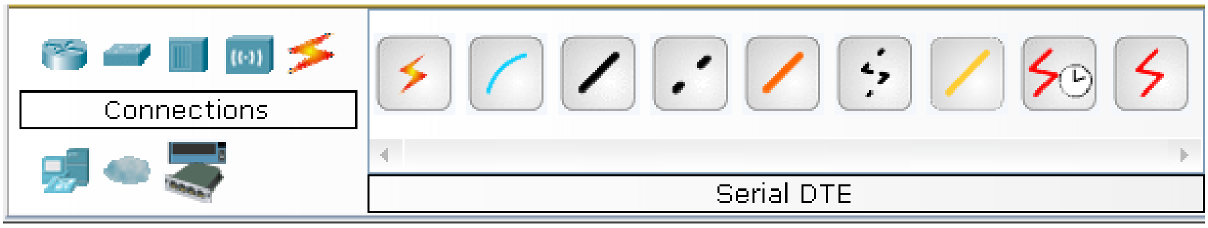


Fig. 1.15. Types of cables supported in Packet Tracer

Packet Tracer supports a wide range of network connections (see Table 1.3). Each cable type can only be connected to certain types of interfaces.

Table 1.3. Connection types in Packet Tracer

Cable type	Description
Console	The console connection can be made between a PC and routers or switches. The requirements for a PC console session must be met: the connection speed on both sides must be the same.
Copper Straight - through	This type of cable is a standard Ethernet transmission medium for connecting devices that operates at different levels of OSI. It must be connected to the following types of ports: copper 10 Mbps (Ethernet), copper 100 Mbps (Fast Ethernet) and copper 1000 Mbps (Gigabit Ethernet).
Copper Cross - over	This type of cable is an Ethernet transmission medium for connecting devices that operate on the same OSI levels. It can be connected to the following types of ports: copper 10 Mbps (Ethernet), copper 100 Mbps (Fast Ethernet) and copper 1000 Mbps (Gigabit Ethernet).
Fiber	Fiber optic media is used to connect between optical ports (100 Mbps or 1000 Mbps).
Phone	A telephone line connection can only be made between devices that have modem ports. The standard representation of a modem connection is an end device (such as a PC) that is called into the cloud network.
Coaxial	Coaxial medium is used to connect between coaxial ports, such as a cable modem connected to the cloud.
Serial DCE and DTE	Serial ports are often used for WAN connections. To set up such connections, you must set up synchronization on the DCE side of the device. The DCE side can be identified by a small clock icon next to the port. When you select a Serial DCE connection type, the first device to which the connection is applied becomes a DCE device, and the second automatically becomes a DTE.

After creating the network, you have to save it by selecting **File -> Save** or icon **Save** on panels **Main Tool Bar**. File saved topology has expansion *** .pkt.**

Packet Tracer gives possibility simulate work with interface command line (**CLI - Command Line Interface**) operating room iOS system installed on all switches and routers. Once connected to a device, we can work with it the way we work with the console of a real device. The simulator provides support for almost all commands available on real devices.

We can connect switches or routers to the CLI by clicking on the desired device and going to the CLI tab in the properties window.

To simulate the operation of the command line on the end device (computer), you must select the **Desktop tab in the properties**, and then click on the **Command Prompt shortcut** .

Working with the simulator

Packet Tracer allows the user to save the configuration of devices, such as routers or switches, in text files. To do this, go to the properties of the desired device and in the **Config tab,** click on the **"Export"** button to export the **Startup Config** or **Running Config** configuration. This will give us a dialog box to save the required configuration to a file with the extension * .txt. The text of the **running** configuration file , config.txt (default name), is similar to the text of the information obtained when using the **show running - config command** on iOS devices.

The configuration of each device is stored in a separate text file. The user also has the ability to manually change the configuration of the saved file using any text editor. To provide the device with saved or edited settings, click the **Load** button in the **Config tab** to load the required **Stàrtup Config configuration** or the **"Merge" button** to load the **Running Config configuration**.

The size of real networks is much larger than most of the networks we work with, to see the network in full, we have to resize the Packet Tracer window.

Access Packet Tracer help sections, tutorials, and interactive materials

There are two ways to access Packet Tracer help topics:

- click the question mark in the upper right corner of the toolbar menu;
- open the **Help menu** and select **Contents**.

To open Packet Tracer training videos, choose **Help> Tutorials**. These videos clearly present information from the Help sections, as well as various features of Packet Tracer software. Watch the **Interface Overview** video in the Getting **Started section** of the tutorials.

Switch between real-time and simulation modes

Find the word **Realtime** in the lower right corner of the Packet Tracer interface. In real time, the network always acts as real, whether you work with it or not. The settings are applied in real time, and the network responds to them in near real time.

Click the tab directly after the **Realtime** tab to switch to **Simulation** mode. In simulation mode, the network is displayed at a lower speed, allowing you to monitor data acquisition paths and check data packets. Open the simulation panel and click the **Auto capture / Play** button. Now you should see data packets represented by envelopes of different colors moving between devices.

Press the **Auto capture / Play button** again to stop simulation.

Click the **Capture / Forward button** to enable step-by-step simulation. Press the button a few more times to see the process in action. In the network topology on the left, click one of the envelopes on the intermediate device and examine its contents.

Switching between logical and physical representation

Find the word **Logical** in the upper left corner of the Packet Tracer interface. You are now in the Logical workspace; You will use it most often when working with networks (building networks, setting up, studying and troubleshooting them , etc.).

Click the tab below the **Logical area to switch to the Physical** workspace . The **Physical workspace** contains the physical dimensions of the logical network topology. It allows to estimate the scale and location of elements (for example, how the network can look in a real environment).

Tasks for laboratory work 1

Part 1 of laboratory work 1

Add two Switch-PT switches to the working area of the simulation environment. By default, they are named Switch0 and Switch1.

Add to the workspace four computers with default names PC0, PC1, PC2, PC3.

Connect the devices to the Ethernet network, as shown in Figure 1.16.

Save the created topology by clicking the **Save** button (in the **File -> Save menu**).

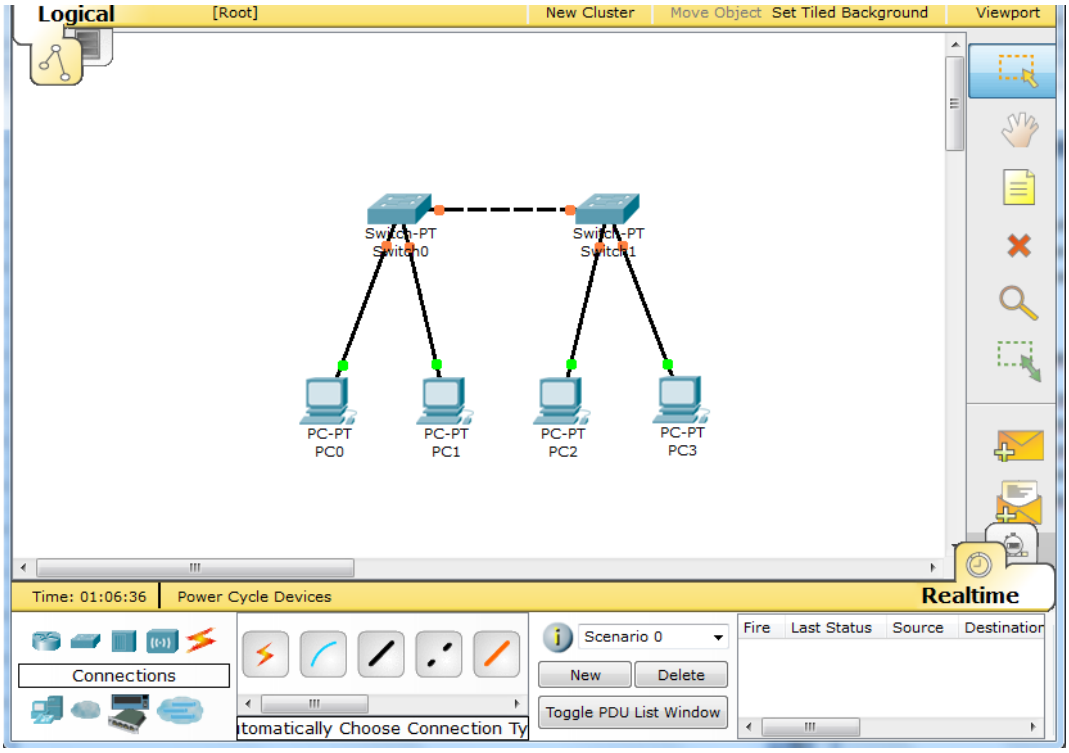


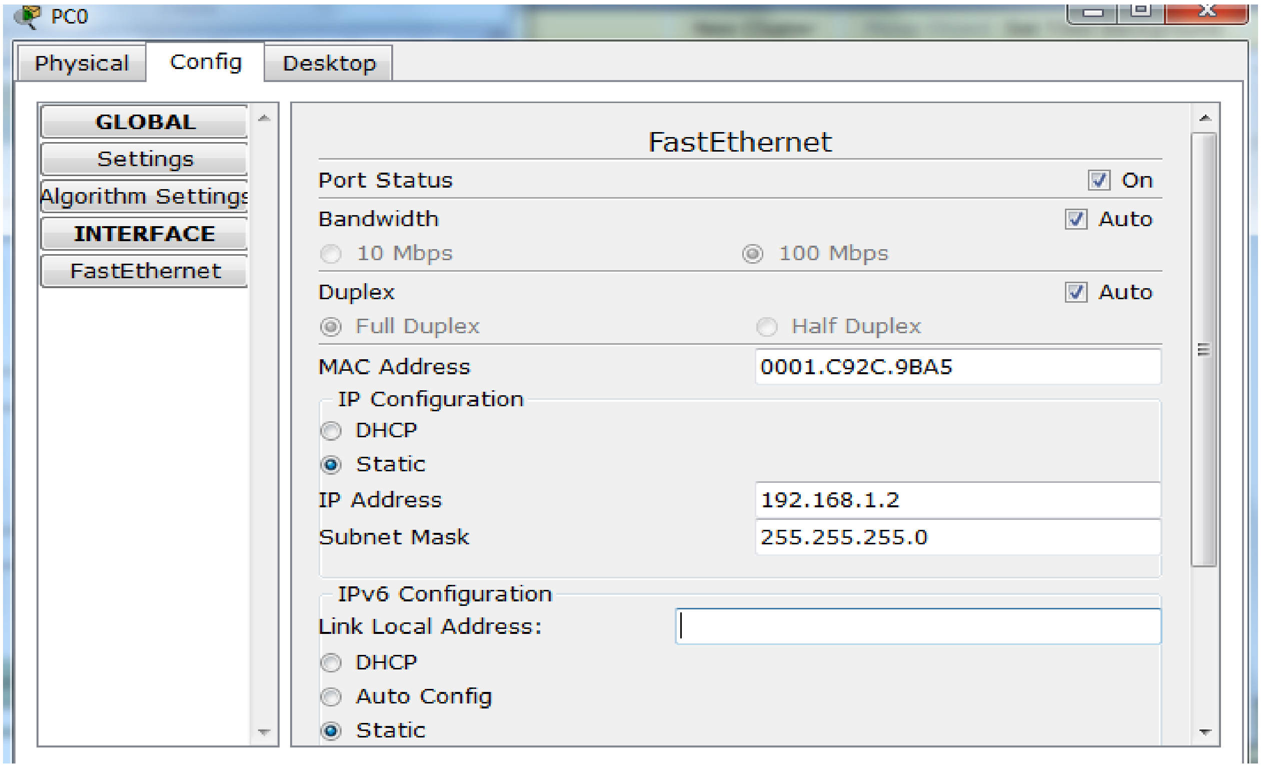
Fig.1. 16. Simple network model consisting of two switches and four nodes

Open the properties of the PC0 device by clicking on its image. Go to the **Desktop tab** and simulate the work of **running** by clicking **Command Prompt**.

Receive the list of commands if we enter " **?** " And we press Enter. To configure the computer, use the **ipconfig** command from the command line, for example:

```
ipconfig 192.168.1.2 255.255.255.0
```

The IP address and network mask can also be entered in the user-friendly graphical interface of the device (Fig. 1.17). The DEFAULT GATEWAY field is the gateway address not yet required, as the network being created does not require routing.



FastEthernet

Port Status ☑ On

Bandwidth ☑ Auto

○ 10 Mbps ● 100 Mbps

Duplex ☑ Auto

● Full Duplex ○ Half Duplex

MAC Address 0001.C92C.9BA5

IP Configuration

○ DHCP

● Static

IP Address 192.168.1.2

Subnet Mask 255.255.255.0

IPv6 Configuration

Link Local Address:

○ DHCP

○ Auto Config

● Static

Device	IP ADDRESS	SUBNET MASK
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

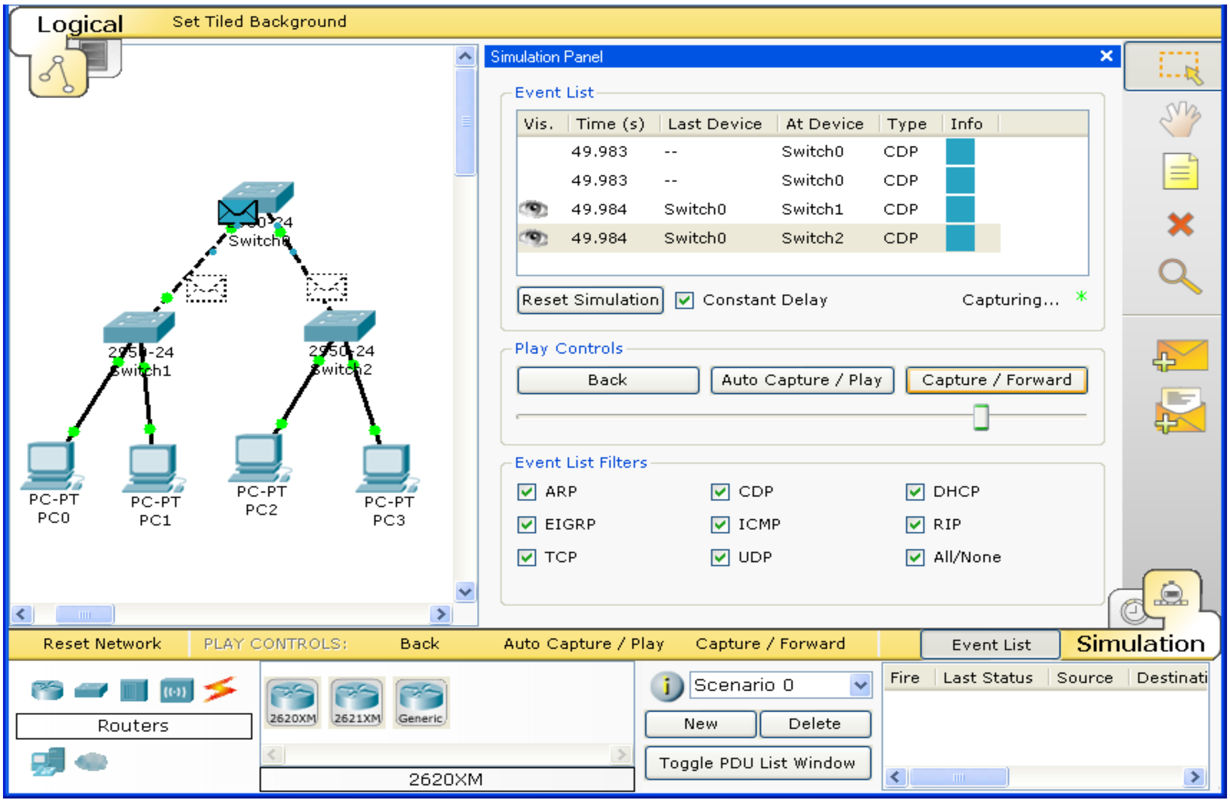
Fig.1. 17. Node settings

On each computer look at the assigned addresses by the **ipconfig** command without parameters.

Packet Tracer provides a simulation mode that describes in detail and shows how the ring utility **works**.

Therefore, you have to switch to this mode by clicking on the icon of the same name in the lower left corner of the work area, or by pressing **Shift+S**.

The Simulation Panel will open, displaying all events related to the **ping** process (Fig. 1.18).



Event List

Vis.	Time (s)	Last Device	At Device	Type	Info
	49.983	--	Switch0	CDP	🟦
	49.983	--	Switch0	CDP	🟦
👁	49.984	Switch0	Switch1	CDP	🟦
👁	49.984	Switch0	Switch2	CDP	🟦

Reset Simulation ☑ Constant Delay Capturing...

Play Controls

Back | Auto Capture / Play | Capture / Forward

Event List Filters

☑ ARP ☑ CDP ☑ DHCP
☑ EIGRP ☑ ICMP ☑ RIP
☑ TCP ☑ UDP ☑ All/None

Scenario 0

Fire	Last Status	Source	Destinati

Fig.1.18. Panel simulation in Packet Tracer

Restart the **ping** process. After its launch, you can minimize the "Simulation Panel" to monitor the sending / receiving of packets in the diagram of the designed network.

The "Automatic" button means modeling the entire **ping** process in a single process, while "Step by Step" allows to display it step by step.

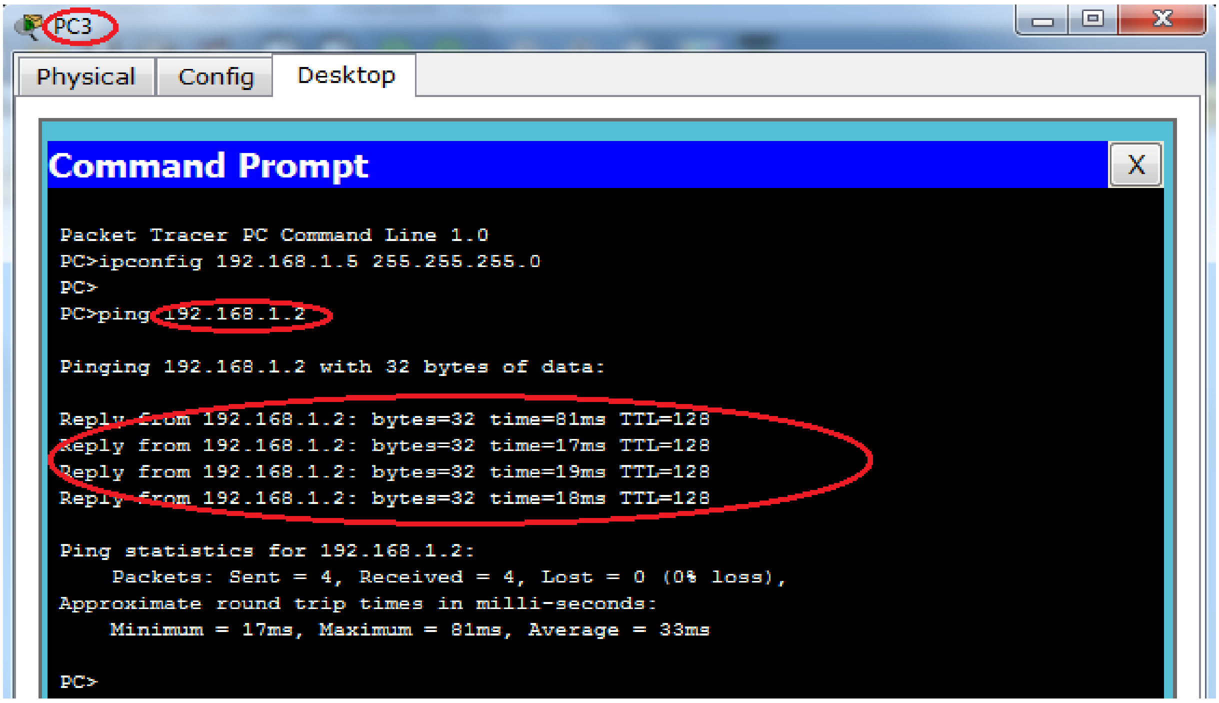
To identify the information contained in the package, its structure, just right-click on the colored square in the "Information" column.

Simulation stops either when the **ping** process is completed or when the "Edit" window of the corresponding workstation is closed.

If done correctly, we will be able to ping any PC from any computer.

For example, go to PC3 and ping PC0.

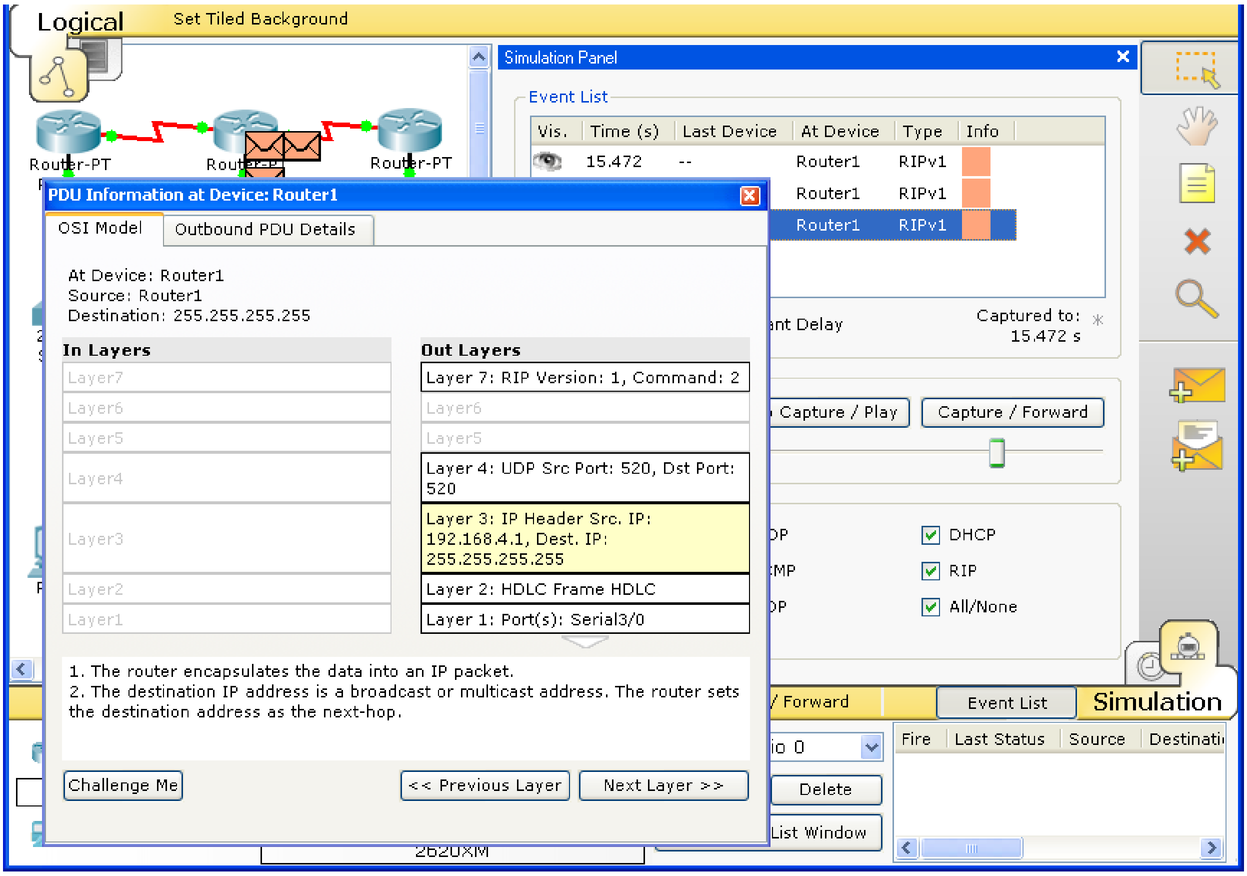
We should see a ping report similar to fig. 1.19.



```
Packet Tracer PC Command Line 1.0
PC>ipconfig 192.168.1.5 255.255.255.0
PC>
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=81ms TTL=128
Reply from 192.168.1.2: bytes=32 time=17ms TTL=128
Reply from 192.168.1.2: bytes=32 time=19ms TTL=128
Reply from 192.168.1.2: bytes=32 time=18ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 81ms, Average = 33ms

PC>
```

Fig. 1. 19. Execution of the **ping** command in the command line

In the "Simulation Mode" you can not only track the protocols used, but also to see which of the seven levels of the OSI model this protocol is involved (Fig . 1.20).



Vis.	Time (s)	Last Device	At Device	Type	Info
👁	15.472	--	Router1	RIPv1	
			Router1	RIPv1	
			Router1	RIPv1	

PDU Information at Device: Router1

OSI Model | Outbound PDU Details

At Device: Router1
Source: Router1
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer 7: RIP Version: 1, Command: 2
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 520, Dst Port: 520
Layer3	Layer 3: IP Header Src. IP: 192.168.4.1, Dest. IP: 255.255.255.255
Layer2	Layer 2: HDLC Frame HDLC
Layer1	Layer 1: Port(s): Serial3/0

1. The router encapsulates the data into an IP packet.
2. The destination IP address is a broadcast or multicast address. The router sets the destination address as the next-hop.

Challenge Me | << Previous Layer | Next Layer >>

Fig. 1.20. Analysis of the seven-level OSI model in Packet Tracer

Part 2 of laboratory work 1

1. Create the network topology shown in Fig. 1.21.

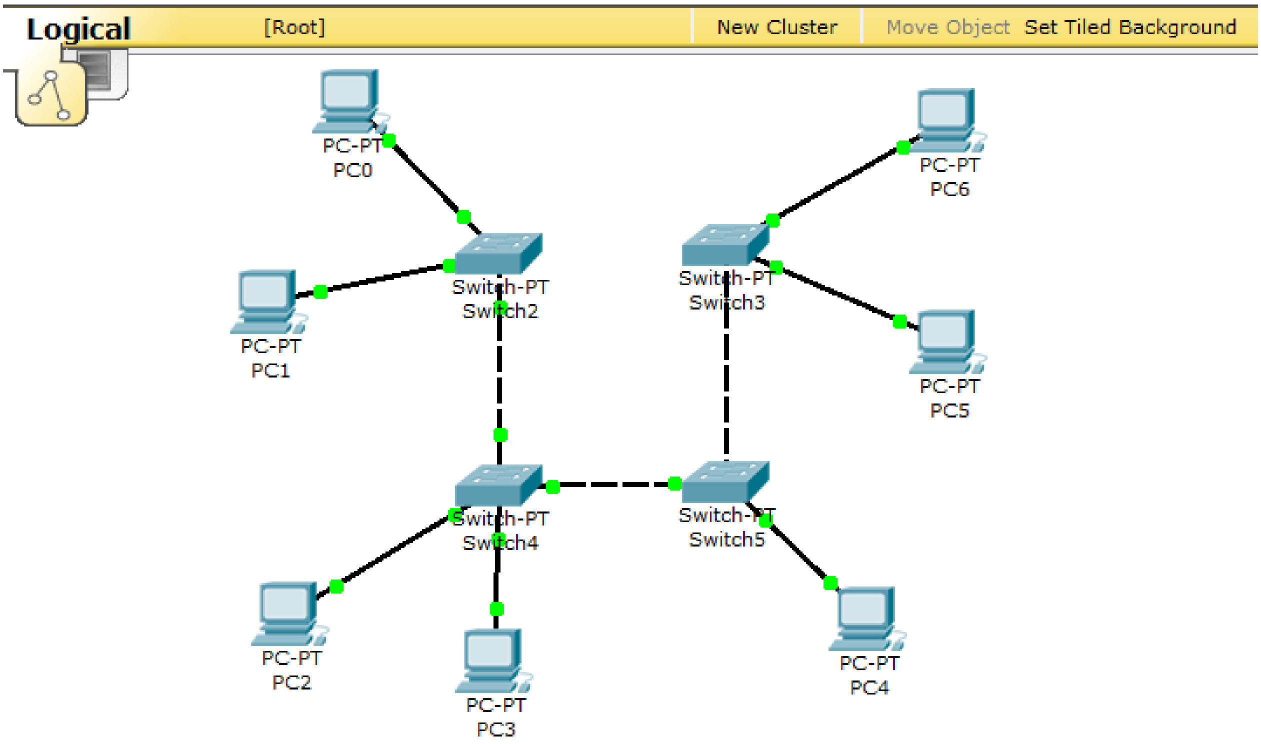


Fig.1.21. Network topology for research

2. Assign addresses to computers, according to the option on list v in the table (v is the serial number of the student in the group list):

Device	IP ADDRESS	SUBNET MASK
PC0	192.168.v.1	255.255.255.0
PC1	192.168.v.2	
PC2	192.168.v.3	
PC3	192.168.v.4	
PC4	192.168.v.5	
PC5	192.168.v.6	
PC6	192.168.v.7	

If done correctly, we can prop up any computer from any other computer.

Use **ping** utility according to the table:

Option	Ping source	Ping destination
1	PC0	PC6
2	PC1	PC6
3	PC2	PC0
4	PC3	PC1
5	PC4	PC2
6	PC6	PC3
7	PC6	PC4
8	PC6	PC5
9	PC0	PC5
10	PC1	PC5
11	PC2	PC0
12	PC3	PC1
13	PC4	PC2
14	PC6	PC3
1 5	PC0	PC4
16	PC1	PC4
17	PC2	PC0
18	PC3	PC1
19	PC4	PC2
20	PC6	PC3
21	PC6	PC2
22	PC0	PC3
23	PC1	PC2
24	PC2	PC0
25	PC3	PC1

4. In Simulation Mode, track packet traffic and protocols used.

a) In "Simulation Mode" consider and explain the process of ICMP communication between devices (by executing a ring command **from** one computer to another), explain the role of ARP in this process. Include a detailed explanation in the report.

b) Make sure that all network objects are within the IP protocol.

Report requirements for laboratory work 1

The report should include:

1. Title page.

2. Individual task for laboratory work (screenshot of the network topology according to and addressing nodes with a decent option in).

3. Progress. This section consists of a sequential description of the significant steps to be performed (indicating their nature), an explanation of the **ping** command, and the contents of the protocols.

4. Conclusions.

Questions for self-assessment

1. Which network components do you know?
2. Describe submarine communications cable.
3. Describe the difference between Clients and Servers.
4. Which types of networks do you know?
5. Describe OSI model layers.
6. What are network cards used for?
7. What is the MAC address it has in the form of a record?
8. Which t types of network environment do you know?
9. What are the types of copper cables?
10. What is the structure and features of the use of coaxial cable?
11. What is the structure and features of the use of twisted pair? What are the types of twisted pair?
12. What is the structure and features of the use of fiber optic lines?

13. What are the main characteristics of a wireless environment?

14. What do you know about wireless data standards?

15. What types of network topologies do you know?

16. What are the features of the "star" apology?

17. What are the features of the "ring" apology?

18. What are the features of the "bus" apology?

19. What are the features of the "tree" apology?

20. Describe the main comparative characteristics of topologies of computer networks.

21. How to switch between logical and physical representation in Packet Tracer?

22. What is the purpose of the **ipconfig** utility?

23. What is the purpose of the **ping** utility?

24. What is the purpose of the ICMP protocol?

25. What is the purpose of the ARP protocol?

References

1. Submarine Cable Map. URL: https://www.submarinecablemap.com/
2. Cable Innovator. URL: https://globalmarine.co.uk/vessels-trenching-assets/cable-innovator/
3. Network topologies. URL: https://www.javatpoint.com/computer-network-topologies
4. OSI model. URL: https://www.javatpoint.com/osi-model
5. MAC address. URL: https://slts.osu.edu/articles/whats-a-mac-address-and-how-do-i-find-it/
6. IP address. URL: https://www.javatpoint.com/ipv4-vs-ipv6
7. ICMP protocol. URL: https://www.javatpoint.com/icmp-protocol
8. ARP protocol. URL: https://www.javatpoint.com/arp-commands

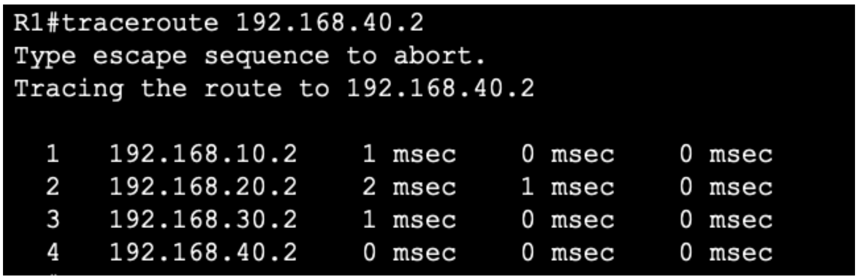
LABORATORY WORK №2. TRACKING THE ROUTE TO A REMOTE SERVER FROM THE COMMAND LINE, SOFTWARE AND WEB TOOLS

Objective: to learn how to test the connection to a remote server, to learn how to route to a remote server using the command line and various software and web tools.

Theory and methodological instructions

Route-tracing software is a utility that contains lists of networks that must pass data from the user's sending end device to the remote destination network.

Traceroute (tracert) is a utility that is used to test the path between two hosts and provide a list of hops that were successfully reached along that path.



```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2    1 msec    0 msec    0 msec
  2   192.168.20.2    2 msec    1 msec    0 msec
  3   192.168.30.2    1 msec    0 msec    0 msec
  4   192.168.40.2    0 msec    0 msec    0 msec
```

Traceroute provides round-trip time for each hop along the path and indicates if a hop fails to respond. An asterisk (*) is used to indicate a lost or unreplied packet.

This information can be used to locate a problematic router in the path or may indicate that the router is configured not to reply.

Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.

The first message sent from traceroute will have a TTL field value of 1. This causes the TTL to time out at the first router. This router then responds with a ICMPv4 Time Exceeded message.

Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets time out further down the path. The TTL field continues to be increased until the destination is reached, or it is incremented to a predefined maximum.

To start the trace process, you must enter the following on the command line:

tracert <destination network name or end device address>

(for Microsoft Windows family of operating systems)

or

traceroute <destination network name or end device address>

(for Unix operating systems)

Route trace utilities allow you to define paths or routes, as well as calculate the delay time in the IP network. There are several tools to perform this function.

The **traceroute** tool (or **tracert**) is used to find and troubleshoot network problems. It displays a list of routers passed and allows you to determine which path was used to reach a destination on one network or when switching between multiple networks. Each router is a connection point between two networks through which data packets are sent. The number of routers is the number of "transitions" made by the data from the source to the destination.

The list that appears helps determine what data issues are occurring when we try to access a service, such as a website. The list can also be used when downloading data. If the same file is available on multiple websites (mirrors), we can check the route for each mirror and choose the fastest option.

Two route traces performed between the same source and destination nodes, but at different times, may give different results. This may be due to the "fully connected" nature of interconnected networks, consisting of the ability of the Internet and Internet protocols to choose different cable channels for sending packets.

Route tracing using the command line are usually embedded in the operating system of the end device (node).

One PC (Windows 7, Vista or XP with Internet access) is used for this laboratory work. Using an Internet connection and three different route tracing utilities, you have to track the path of data packets over the Internet to destination networks. This uses a computer, an Internet connection, and command line access. First we use the "**tracert**" utility built into Windows, then **the web tools** for tracing the route (http://www.subnetonline.com/pages/network-tools/online-traceroute.php).

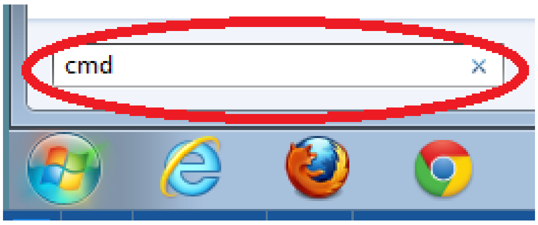
ICMP (Internet Control Message Protocol) echo responses used by **ping** echo requests and trace commands are disabled. Before you begin this task, verify that there are no local restrictions associated with ICMP datagrams. This paper assumes that ICMP datagrams are not restricted by any local security policies.

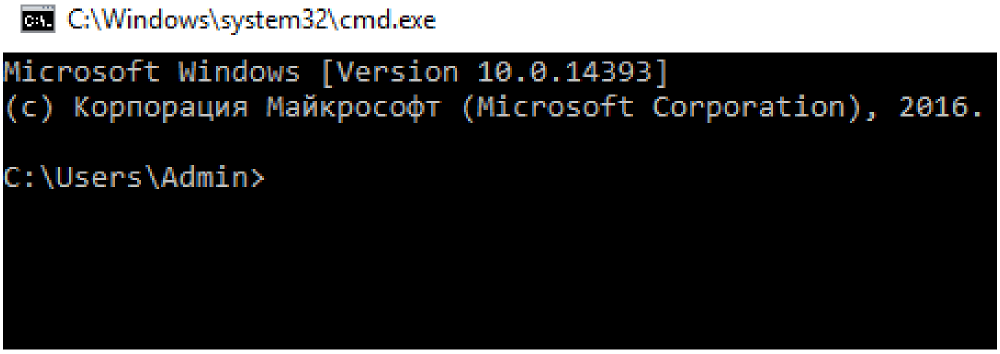
Check the network connection with an echo request using the ping command

Check if a remote server is available. To route to a remote network, the PC must be connected to the Internet.

First, use the echo query with the **ping** command. An echo query with the **ping** command is a means to check the availability of a node. Information packets are sent to the remote host with a response request. The local PC determines whether a response is received for each packet , and calculates how long it takes to send these packets over the network. The name "echo request" came from the area of active sonar, where it meant an audible signal sent underwater and reflected from the bottom or other ships.

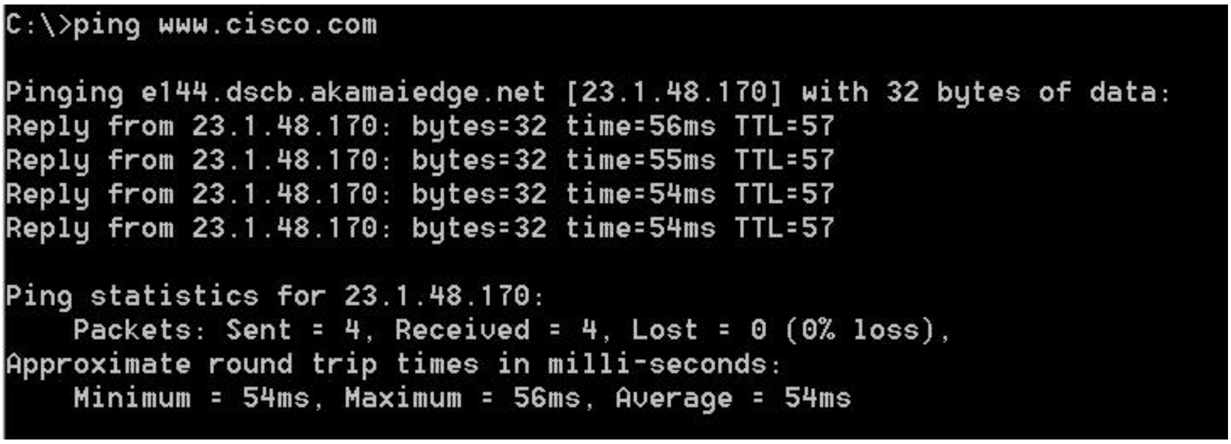
Click *Start* on the computer screen, type **cmd** in the *Find programs and files box*, and then press ENTER.





```
Microsoft Windows [Version 10.0.14393]
(c) Корпорация Майкрософт (Microsoft Corporation), 2016.

C:\Users\Admin>
```

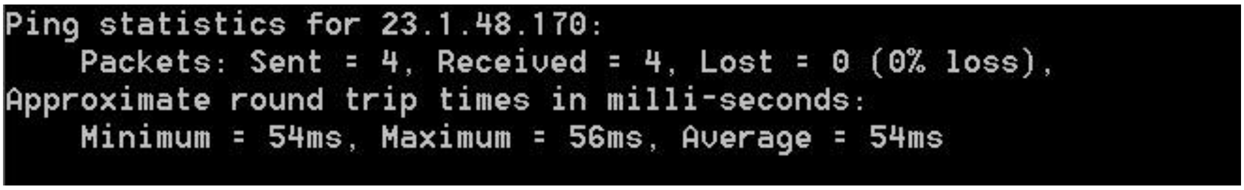
At the command prompt, enter **ping www.cisco.com**



```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

The first line of the received data displays the fully qualified domain name (FQDN) **e144.dscb.akamaiedge.net**. This is followed by the IP address **23.1.48.170**. Cisco Web sites that contain the same information are hosted on different servers (so-called **mirrors**) around the world. This means that the FQDN name and IP address will differ depending on your location.

Let's take some of the results:

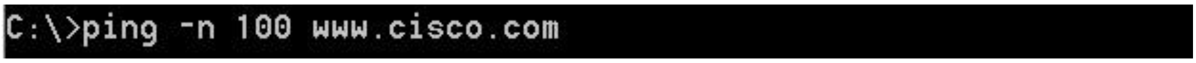


```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

It shows that four echo requests were sent using the **ping** command , each of which was answered. The response to all echo requests was received using the **ping** command, so there are no packet losses (0% of losses). On average, 54 ms (milliseconds) are required to transmit packets over the network.

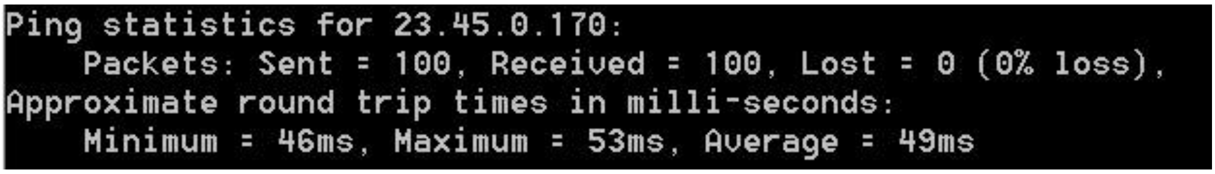
If the waiting time for the first ICMP packet has expired, this may be due to the PC converting the destination address. This will not happen if the echo request is repeated with the **ping** command when address caching.

Loss of packets or slow network connection primarily affects the quality of streaming video and online games. To determine the speed of the Internet connection more accurately, you can send not 4 echo requests using the default **ping** command**, but 100.** To do this, use the following command.



```
C:\>ping -n 100 www.cisco.com
```

The result will look like this.

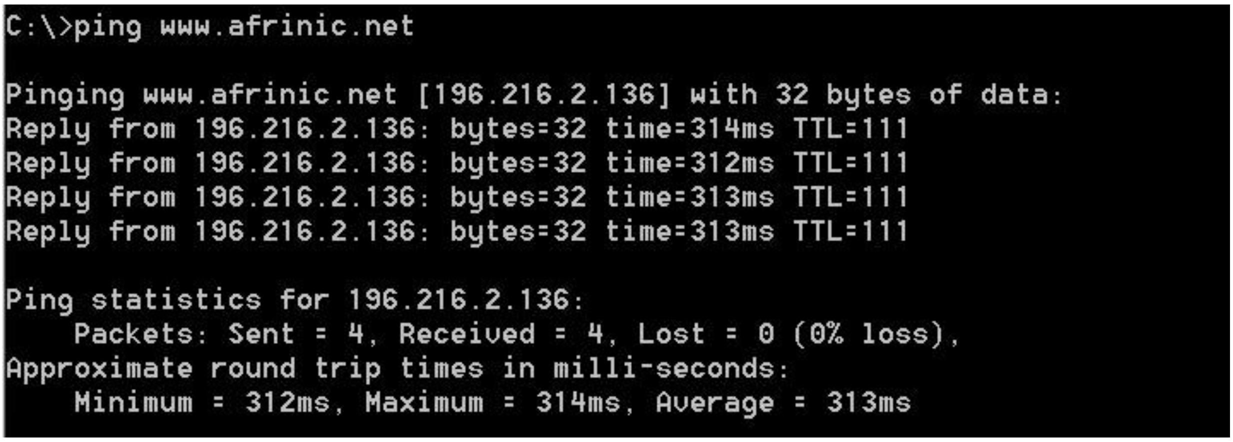


```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

Now let's look at the case where all **ping** echo requests were sent from a computer located in the United States to regional Internet Registry (RIR) websites located in different parts of the world.

Africa:

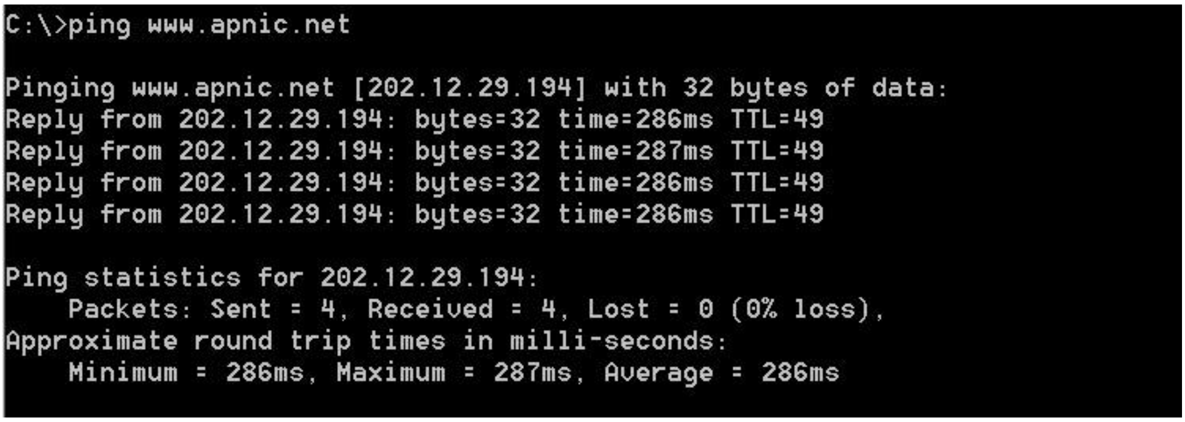
C: \> **ping www.afrinic.net**



```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Australia:

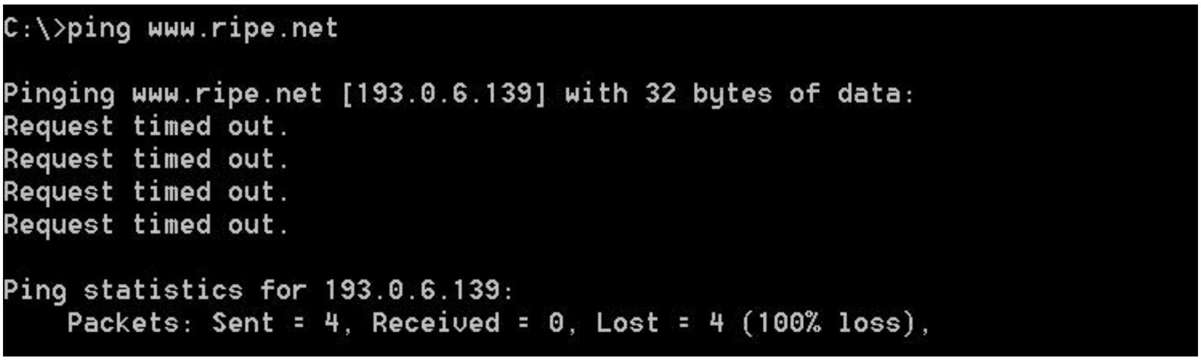
C: \> **ping www.apnic.net**



```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Europe :

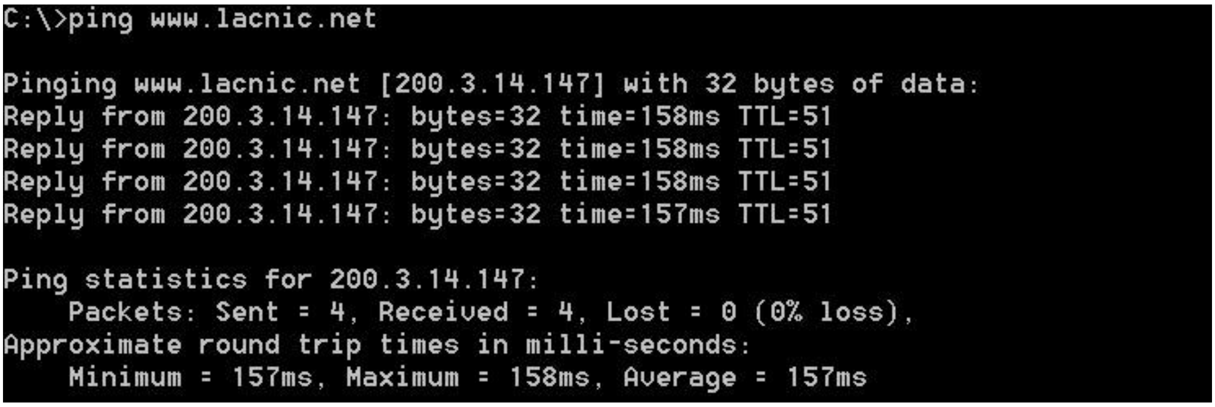
C: \> **ping www.ripe.net**



```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

South America:

C: \> **ping lacnic.net**



```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

When data is transmitted using the **ping** command within one continent (North America), the average echo request time (in milliseconds) increases significantly compared to when data from North America is transmitted to other continents. In this case, echo requests using the **ping** command sent to the European website from the United States were not successful.

Trace a route to a remote server with the traceroute tools

Determine which route of all Internet traffic is directed to a remote server. After checking the reach with the **ping** utility, you should take a closer look at each network segment through which the data passes. To do this, use the **tracert** command.

At the command prompt, enter **tracert www.cisco.com.**

Save the results obtained after entering the **tracert** command in a text file by following the steps below.

2) Right-click on the title bar of the command prompt and select Edit> Select All.

3) Right-click the title bar of the command prompt again and select Edit> Copy.

4) Open Windows Notepad. To do this, click Start and select All Programs> Accessories> Notepad.

5) To paste data into Notepad, choose Paste from the Edit menu.

6) On the File menu, click Save As, and then save your Notepad file to your desktop as tracert1.txt.

Run the **tracert** utility for each destination website and save the results to sequentially numbered files.

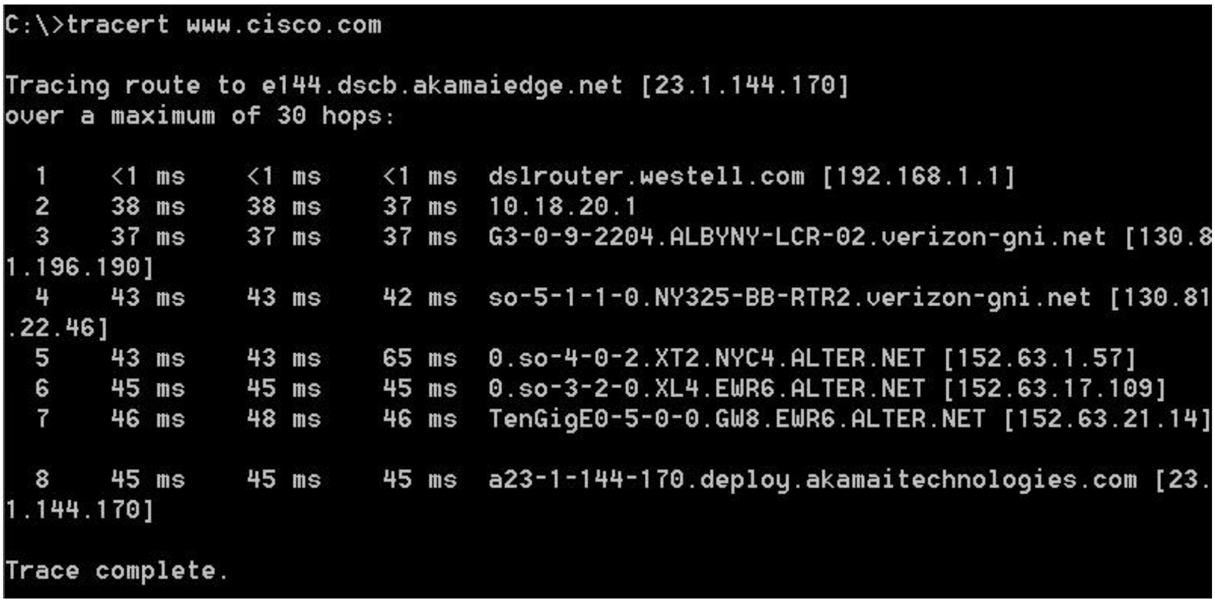
C: \> **tracert www.afrinic.net**

C: \> **tracert www.lacnic.net**

Depending on the coverage area of ISP and the location of the source and destination nodes, tracked routes can cross many transitions and networks.

Each transition is one router. A router is a special computer that is used to redirect traffic over the Internet. Imagine that we went on a trip on the roads of several countries. During your journey, you constantly come to a fork where you have to choose one of several destinations. Now imagine that at each fork there is a device that indicates the right path to the final destination of our journey. The router for packets on the network does the same.

Because computers use the language of numbers, not words, routers are assigned unique IP addresses (xxxx numbers). The **tracert** utility shows which way the data packet goes to the final destination. You can use the **tracert** utility to determine how fast traffic passes through each network segment. Each router receives three packets on the data path, the response time of which is measured in milliseconds. Using this information, analyze the results obtained with the **tracert** utility when sending packages to **www.cisco.com** . Below is the entire route of the route.

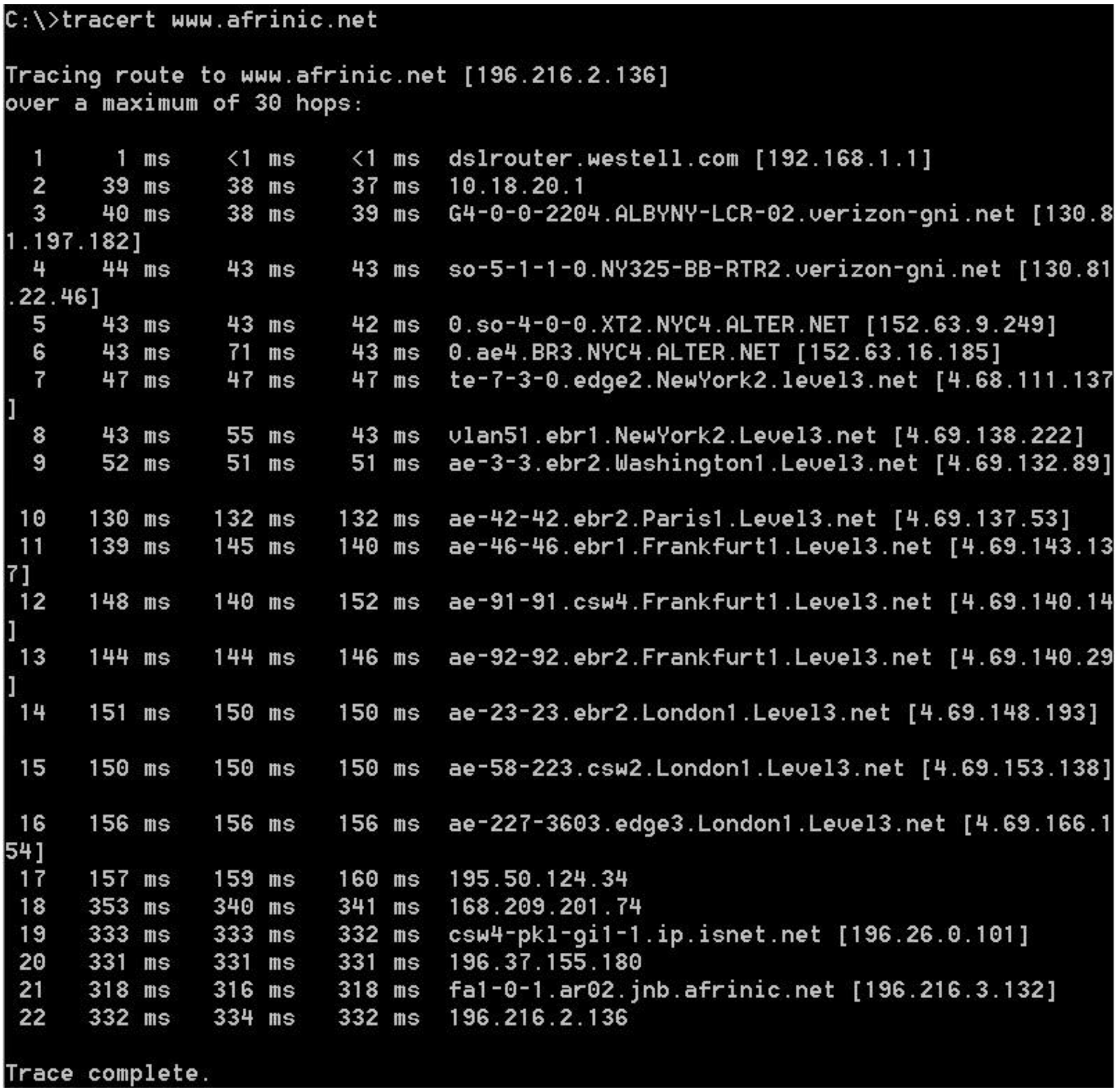


```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

In this example, packets sent by the **tracert** utility are forwarded from the source PC to the primary gateway of the local router (transition 1: 192.168.1.1) and then to the router at the POP connection point (transition 2: 10.18.20.1). Each provider has many POP routers. They mark the boundaries of the ISP's network and serve as Internet connection points for customers. The packets are transmitted over the Verizon network, cross two transitions and end up in a router owned by alter.net. This may mean that the packets have reached another ISP. This point is very important, because packets can be lost when sending packets from one provider to another, and it is important to remember that not all ISPs are able to provide the same data rate. How to determine whether alter.net is the same or a different ISP?

There is an online service **whois**, which can be used to identify the owner of a domain name. The **whois** service is available at **http://whois.domaintools.com/**.

Thus, Internet traffic starts on the home PC and passes through the home router (transition 1). It then connects to the ISP and is transmitted over its network (transitions 2-7) until it reaches a remote server (transition 8). This is a rather unusual example, in which only one provider is involved from start to finish. As can be seen from the following examples, most often two or more ISPs are involved in data transfer. Now let's look at an example of forwarding Internet traffic across multiple ISPs. Below are the results of using the **tracert** utility to www.afrinic.net.

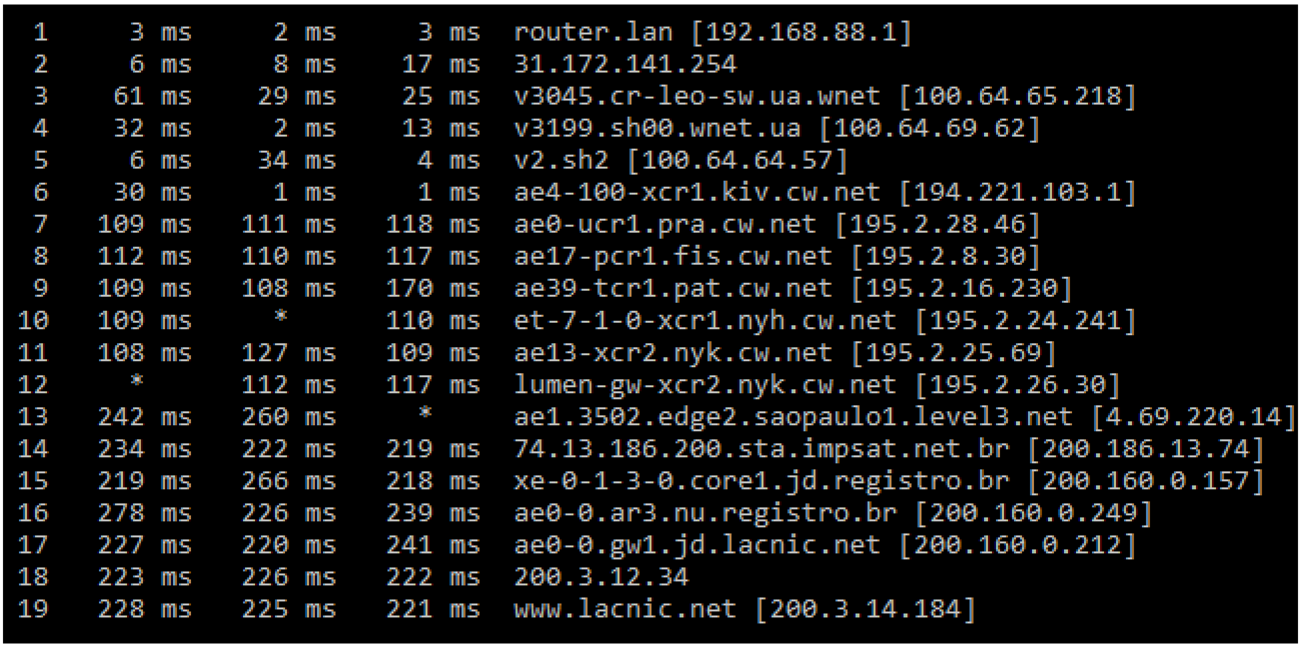


```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

What happens in transition 7? Is **level3.net** the same ISP as in transitions 2-6? To answer this question, use the **whois** service, where we determine that Internet traffic passes from the node **alter.net** to the node **level3.net**. The **whois** service reports that it is a separate company or other Internet provider.

What happens in transition 18? With the help of the **whois service** we will perform a search at the address 168.209.201.74. The transition time on one channel in the network increases from 159 to 340 ms. This may mean that traffic has moved from the Tier 3 backbone to another network. With the help of the **whois service** we establish that the IP address 168.209.201.74 belongs to the African Network Information Center.

Enter the **tracert www.lacnic.net.**



```
 1     3 ms     2 ms     3 ms  router.lan [192.168.88.1]
 2     6 ms     8 ms    17 ms  31.172.141.254
 3    61 ms    29 ms    25 ms  v3045.cr-leo-sw.ua.wnet [100.64.65.218]
 4    32 ms     2 ms    13 ms  v3199.sh00.wnet.ua [100.64.69.62]
 5     6 ms    34 ms     4 ms  v2.sh2 [100.64.64.57]
 6    30 ms     1 ms     1 ms  ae4-100-xcr1.kiv.cw.net [194.221.103.1]
 7   109 ms   111 ms   118 ms  ae0-ucr1.pra.cw.net [195.2.28.46]
 8   112 ms   110 ms   117 ms  ae17-pcr1.fis.cw.net [195.2.8.30]
 9   109 ms   108 ms   170 ms  ae39-tcr1.pat.cw.net [195.2.16.230]
10   109 ms     *      110 ms  et-7-1-0-xcr1.nyh.cw.net [195.2.24.241]
11   108 ms   127 ms   109 ms  ae13-xcr2.nyk.cw.net [195.2.25.69]
12     *      112 ms   117 ms  lumen-gw-xcr2.nyk.cw.net [195.2.26.30]
13   242 ms   260 ms     *     ae1.3502.edge2.saopaulo1.level3.net [4.69.220.14]
14   234 ms   222 ms   219 ms  74.13.186.200.sta.impsat.net.br [200.186.13.74]
15   219 ms   266 ms   218 ms  xe-0-1-3-0.core1.jd.registro.br [200.160.0.157]
16   278 ms   226 ms   239 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
17   227 ms   220 ms   241 ms  ae0-0.gw1.jd.lacnic.net [200.160.0.212]
18   223 ms   226 ms   222 ms  200.3.12.34
19   228 ms   225 ms   221 ms  www.lacnic.net [200.3.14.184]
```

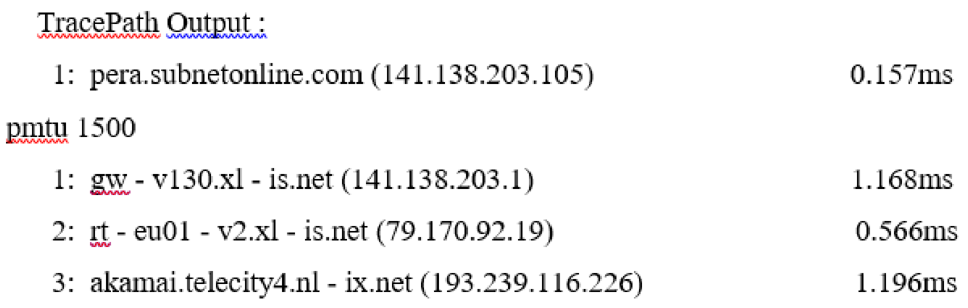
We see that during the transition the packet travel time on the network (in ms) can increase more than four times (route from Kyiv, Ukraine).

Track a route to a remote server using software and web tools

We will use the web tool for tracing the route. Use **http://www.subnetonline.com/pages/network-tools/online-tracepath.php** to track the route to www.cisco.com and www.afrinic.net .

www.cisco.com :

TracePath Output:



```
TracePath Output :
  1:  pera.subnetonline.com (141.138.203.105)          0.157ms
pmtu 1500
  1:  gw - v130.xl - is.net (141.138.203.1)            1.168ms
  2:  rt - eu01 - v2.xl - is.net (79.170.92.19)        0.566ms
  3:  akamai.telecity4.nl - ix.net (193.239.116.226)   1.196ms
```

www.afrinic.net :

TracePath Output:

1: pera.subnetonline.com (141,138,203,105) 0.175ms

1: gw - v130.xl - is.net (141.138.203.1) 0.920ms

```
2: rt - eu01 - v2.xl - is.net (79.170.92.19)                              0.556ms
3: xl - internetservices.nikhef.openpeering.nl (217.170.0.225)            10.679ms
4: r22.amstnl02.nl.bb.gin.ntt.net (195.69.144.36) asymm                   54.412ms
5: ae - 5.r23.londen03.uk.bb.gin.ntt.net (129.250.5.197)                  49.349ms
6: ae - 2.r02.londen03.uk.bb.gin.ntt.net (129.250.5.41) asymm             78.842ms
7: dimensiondata - 0.r02.londen03.uk.bb.gin.ntt.net (83.231.235.222) 18.080ms
8: 168,209,201.74 (168,209,201.74)                                         196.375ms
9: csw4 - pkl - gi1 - 1.ip.isnet.net (196.26.0.101) asymm                  10 186.855ms
10: 196.37.155.180 (196.37.155.180)                                        185.661ms
11: fa1 - 0-1.ar02.jnb.afrinic.net (196.216.3.132)                         197.912ms
```

In this example, the command line routing was completed on a server in Cambridge, Massachusetts. Tracing the route from a website in the Netherlands resulted in a mirror server in the same country. The cisco.com domain is hosted on several websites (mirrors) located around the world. This is done in order to minimize access time to the site from anywhere in the world.

Let's compare the results of tracing a route to Africa from part 1 with the results of tracing the same route through the web interface. What is the difference between them? The route through Europe is provided by another Internet provider.

There are many trunk channels on the Internet. They all connect at points of exchange. The network performance of one ISP may differ from the network performance of another.

In some route trace results, you can see the expression "**asymm**" – an abbreviation of the word **asymmetric**, ie "asymmetric". It means that the test package reached its destination one way and returned another. Imagine that you went by car to the city of Chernihiv. Along the way, you discovered what was created problems on the road and traffic are extremely difficult. We have decided to return home the other way, that is, you have chosen an asymmetrical path.

Comparison of tracing results

Let's compare the results of tracing the route to www.cisco.com to see if all the tracing tools used the same routes to www.cisco.com or different. Here are the addresses on the route to www.cisco.com, obtained using the **tracert** command:

192.168.1.1> 10.18.20.1> 130.81.196.190> 130.81.22.46> 152.63.1.57> 152.63.17.109> 152.63.21.14> 23.1.144.170.

Here are the addresses on the route to www.cisco.com, obtained through the web service **subnetonline.com:**

141,138,203,105> 141,138,203.1> 79,170.92.19> 19,239,116,226

Route tracing performed between the same source and destination nodes, but at different times, can give different results. This may be due to the "fully connected" nature of interconnected networks, consisting of the ability of the Internet and Internet protocols to choose different cable channels for sending packets.

Tasks for laboratory work 2

You have to check the ability to connect to a remote server (optional) using the **ping** utility, https://whois.domaintools.com/ and using three different route tracing tools (**tracert** utility, web interface https://www.subnetonline.com/pages/network-tools/online-tracepath.php). Compare and explain the results of the trace, as described in the instructions for the task.

Version	Remote server
1	www.facebook.com
2	www.java.com
3	www.netacad.com
4	www.intel.com
5	www.linkedin.com
6	www.google.com
7	www.av-intel.com
8	www.agri-intel.com

9	www.gmail.com
10	www.cisco.com
11	www.scopus.com
12	www.bbc.com
13	www.telegram.org
14	www.oracle.com
15	www.phyton.com
16	www.w3schools.com
17	www.apple.com
18	www.ford.com
19	www.facebook.com
20	www.netacad.com
21	www.google.com
22	www.meta.com
23	www.linkedin.com
24	www.scopus.com
25	www.microsoft.com

Report requirements for laboratory work 2

The report should include:

1. Title page.

1. Individual task for laboratory work (screenshot of the task with a decent option in).

2. Workflow (sequential description of the performed steps (with screenshots of execution), explanation of the work of the team of utilities, software and web tools for tracing the route to a remote server, comparing the results of tracing).

3. Conclusions.

Questions for self-assessment

1. What are the **ping**, **tracert** utilities used for? and **traceroute**?

2. What software and web resources do you know for tracing a route to a remote server?

3. Why the results of tracing by different means may differ?

4. What does the expression "**asymm**" mean in the route trace results?

5. Why we use web resources ONLINE TRACEPATH)?

References

1. Mapping the Internet https://www.academia.edu/12778956/
2. Online Tracepath. URL: https://www.subnetonline.com/pages/network-tools/online-tracepath.php
3. Whois Lookup. URL: https://whois.domaintools.com
4. What is Traceroute. URL: https://www.fortinet.com/resources/cyberglossary/traceroutes

LABORATORY WORK № 3. COLLECTION AND ANALYSIS OF ICMP DATA USING WIRESHARK

Objective: to learn to use the program Wireshark to collect and analyze ICMP data, to intercept the IP address of ICMP data packets and MAC addresses of Ethernet frames from local and remote nodes.

Theory and methodological instructions

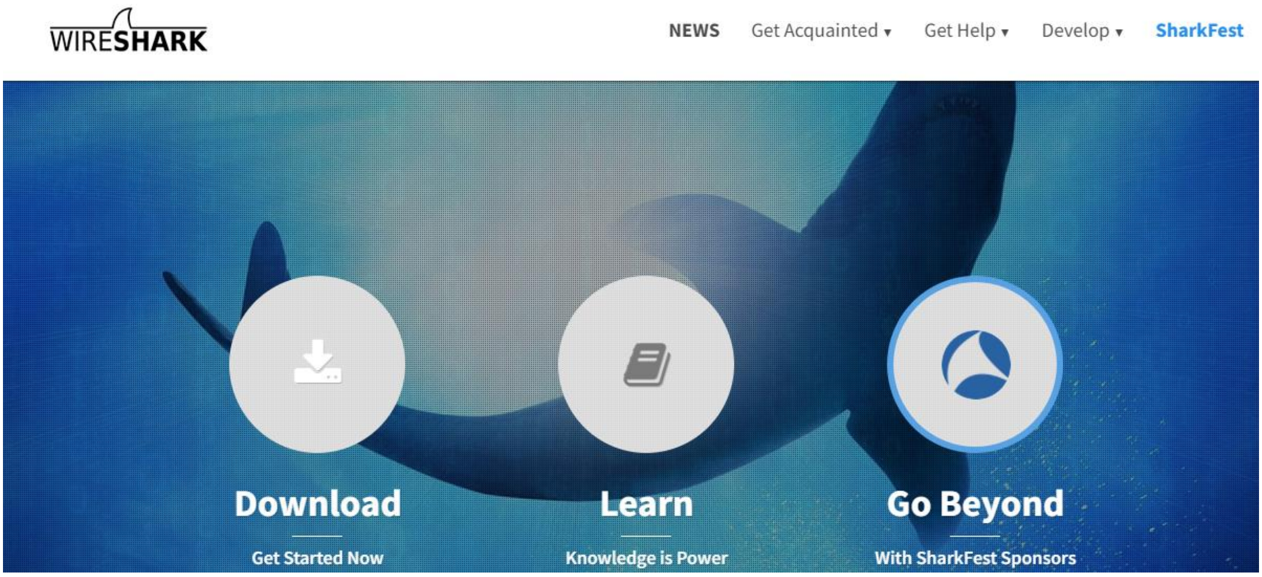
Wireshark is a protocol analysis program (packet analyzer) used to troubleshoot, analyze, develop software and protocols. As data flows over the network, the analyzer intercepts each protocol data unit (PDU) and then decrypts or analyzes its contents in accordance with the relevant RFC document or other specifications. Windows 7, Vista or XP with Internet access is used for laboratory work, additional PCs in the local network are needed to respond to echo requests (**ping** command**)** on other computers in the local network.

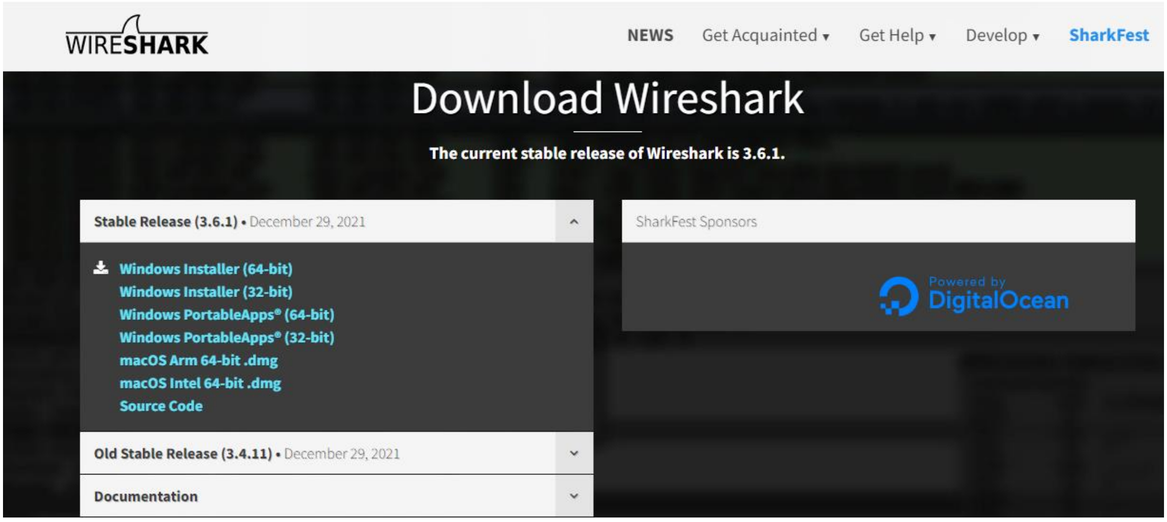
Wireshark installation procedure and screenshots may differ depending on the version of the program. This lab describes the use of Wireshark version 1.8.3 for Windows 7 (64-bit version).

Download and install Wireshark

Wireshark is a standard packet analyzer used by network engineers. Versions of this open source program are available for a variety of operating systems, including Windows, Mac, and Linux.

Download Wireshark at www.wireshark.org





Download Wireshark

The current stable release of Wireshark is 3.6.1.

Stable Release (3.6.1) • December 29, 2021

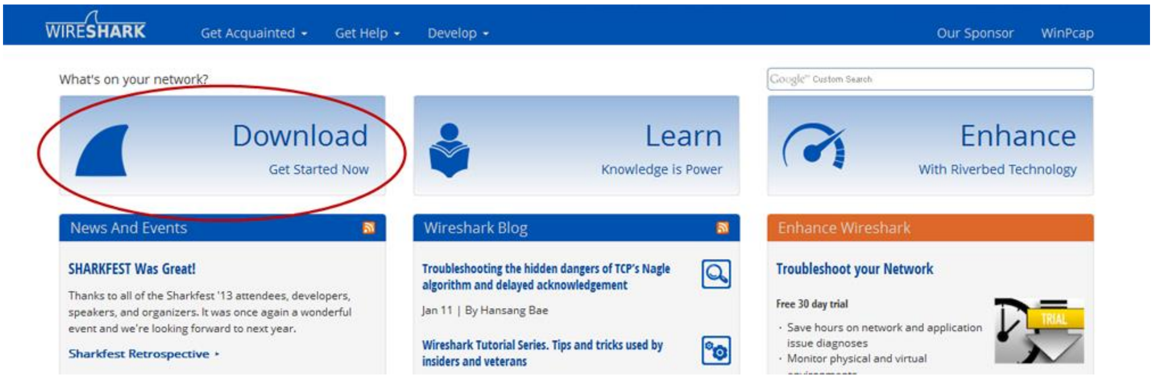
- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (64-bit)
- Windows PortableApps® (32-bit)
- macOS Arm 64-bit .dmg
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.4.11) • December 29, 2021

Documentation

SharkFest Sponsors

Powered by DigitalOcean



What's on your network?

SHARKFEST Was Great!

Thanks to all of the Sharkfest '13 attendees, developers, speakers, and organizers. It was once again a wonderful event and we're looking forward to next year.

Sharkfest Retrospective ▸

Troubleshooting the hidden dangers of TCP's Nagle algorithm and delayed acknowledgement

Jan 11 | By Hansang Bae

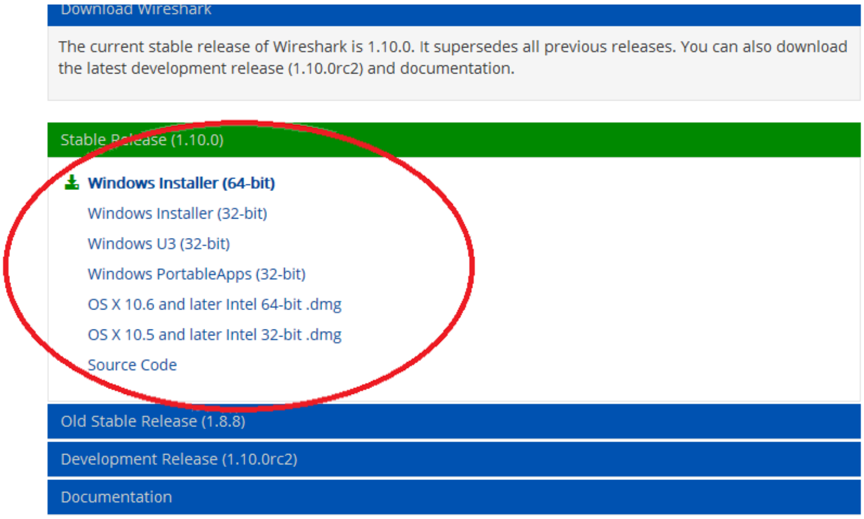
Wireshark Tutorial Series. Tips and tricks used by insiders and veterans

Troubleshoot your Network

Free 30 day trial

- Save hours on network and application issue diagnoses
- Monitor physical and virtual

Choose the version of the program according to the architecture and operating system of your PC. For example, if your PC is running a 64-bit Windows operating system, select Windows Installer (64-bit).



Download Wireshark

The current stable release of Wireshark is 1.10.0. It supersedes all previous releases. You can also download the latest development release (1.10.0rc2) and documentation.

Stable Release (1.10.0)

- **Windows Installer (64-bit)**
- Windows Installer (32-bit)
- Windows U3 (32-bit)
- Windows PortableApps (32-bit)
- OS X 10.6 and later Intel 64-bit .dmg
- OS X 10.5 and later Intel 32-bit .dmg
- Source Code

Old Stable Release (1.8.8)

Development Release (1.10.0rc2)

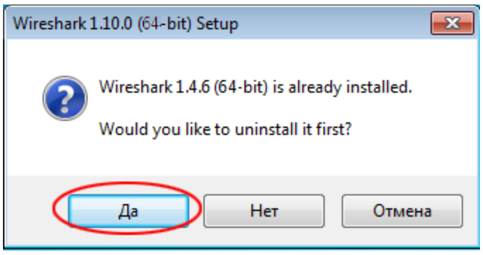
Documentation

The download will start immediately after that. The location of the downloaded file depends on the browser and operating system you are using.

The downloaded file is called **Wireshark - win64 - xxxexe**, where "x" corresponds to the number version of it . Double-click the file to begin the installation. Respond to all security messages that appear on the screen.

If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the program.

It is recommended that you uninstall the old version of the program before installing the new one. To uninstall a previous version of Wireshark, click **Yes**.

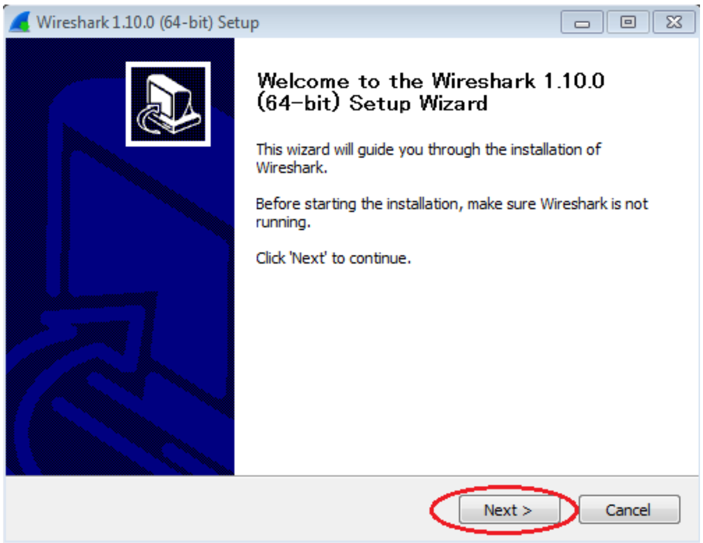


Wireshark 1.10.0 (64-bit) Setup

Wireshark 1.4.6 (64-bit) is already installed.

Would you like to uninstall it first?

If you are installing Wireshark for the first time or a previous version has been uninstalled, the Wireshark Installation Wizard will open. Click **Next**.



Wireshark 1.10.0 (64-bit) Setup

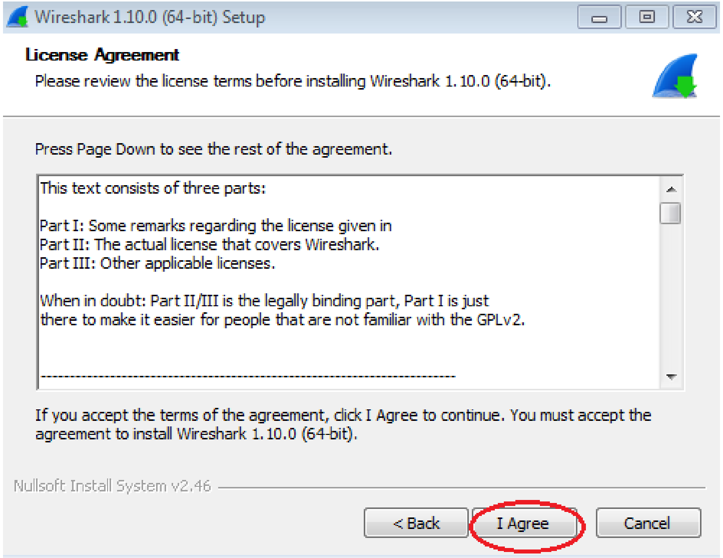
Welcome to the Wireshark 1.10.0 (64-bit) Setup Wizard

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

Follow the installation instructions. When the "**License Agreement**" window opens, click the **I accept** button.



Wireshark 1.10.0 (64-bit) Setup

License Agreement

Please review the license terms before installing Wireshark 1.10.0 (64-bit).

Press Page Down to see the rest of the agreement.

This text consists of three parts:

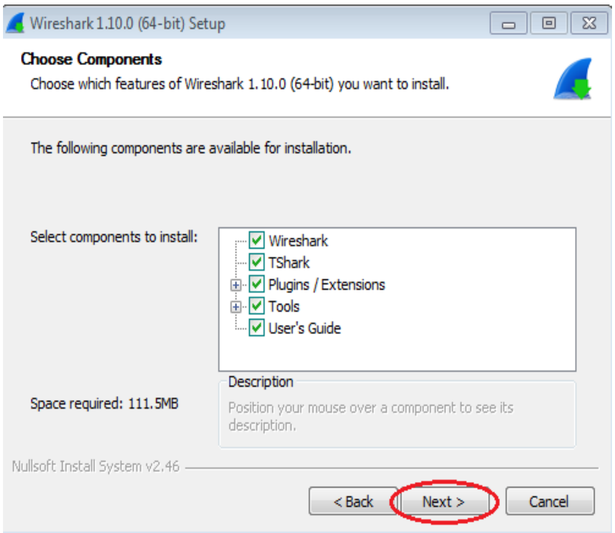
Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 1.10.0 (64-bit).

Nullsoft Install System v2.46

When selecting components, leave the default setting and click **Next**. Select the desired shortcuts and click **Next**.



Wireshark 1.10.0 (64-bit) Setup

Choose Components

Choose which features of Wireshark 1.10.0 (64-bit) you want to install.

The following components are available for installation.

Select components to install:

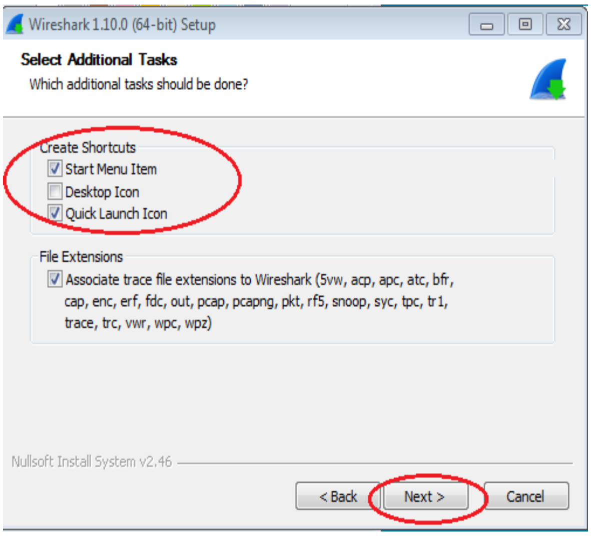
- ☑ Wireshark
- ☑ TShark
- ☑ Plugins / Extensions
- ☑ Tools
- ☑ User's Guide

Description

Position your mouse over a component to see its description.

Space required: 111.5MB

Nullsoft Install System v2.46



Wireshark 1.10.0 (64-bit) Setup

Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

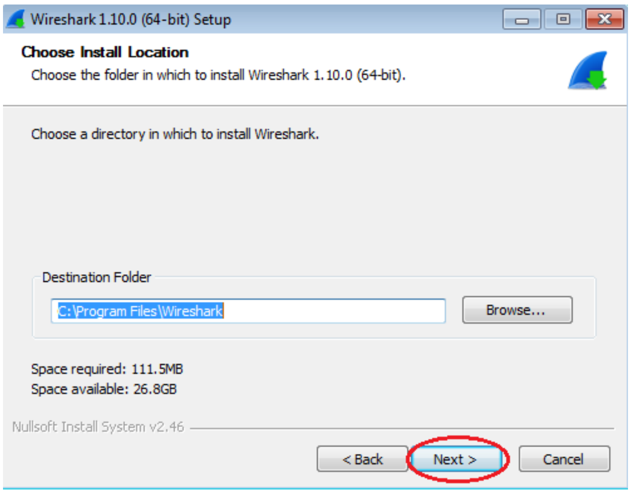
- ☑ Start Menu Item
- □ Desktop Icon
- ☑ Quick Launch Icon

File Extensions

- ☑ Associate trace file extensions to Wireshark (5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz)

Nullsoft Install System v2.46

If disk space is limited, we can change the installation directory, otherwise leave the default address.



Wireshark 1.10.0 (64-bit) Setup

Choose Install Location

Choose the folder in which to install Wireshark 1.10.0 (64-bit).

Choose a directory in which to install Wireshark.

Destination Folder

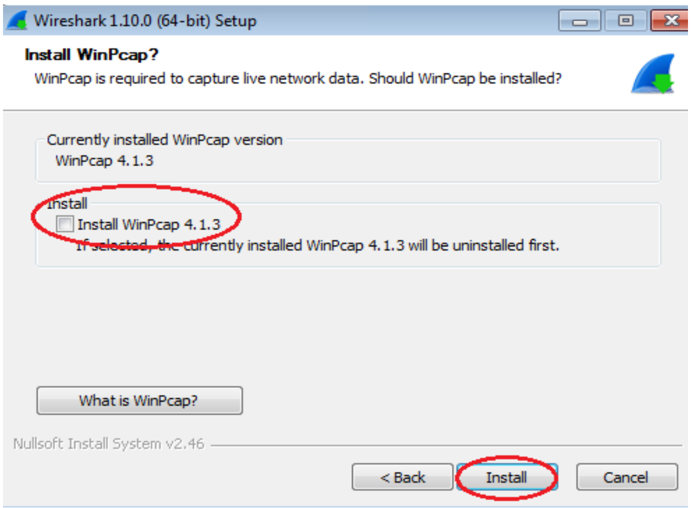
C:\Program Files\Wireshark

Space required: 111.5MB

Space available: 26.8GB

Nullsoft Install System v2.46

To collect network data on your PC you have to install **WinPcap**. If the installed version of WinPcap is older than the version included with Wireshark, you must install the newer version by clicking the check box next to **Install WinPcap xxx** (Install WinPcap xxx). If the installation is successful, close the WinPcap installation wizard.



Wireshark 1.10.0 (64-bit) Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version

WinPcap 4.1.3

Install

□ Install WinPcap 4.1.3

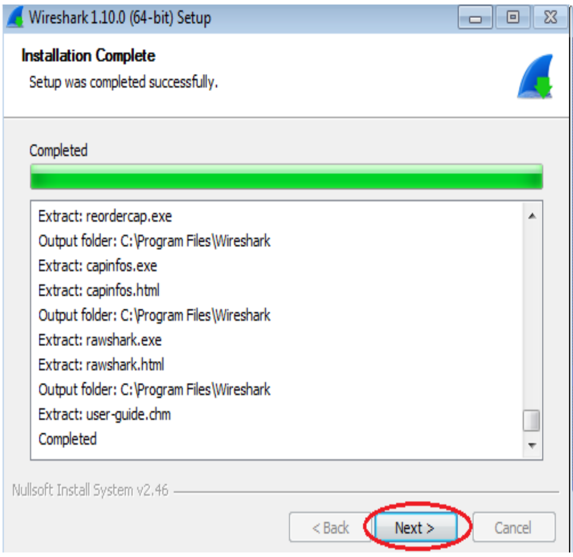
If selected, the currently installed WinPcap 4.1.3 will be uninstalled first.

What is WinPcap?

Nullsoft Install System v2.46

< Back | Install | Cancel

After that, the installation of Wireshark will begin. The status of the installation will be displayed in a separate window. When the installation is complete, click **Next**. Click **Finish** to complete the Wireshark installation process.



Wireshark 1.10.0 (64-bit) Setup

Installation Complete

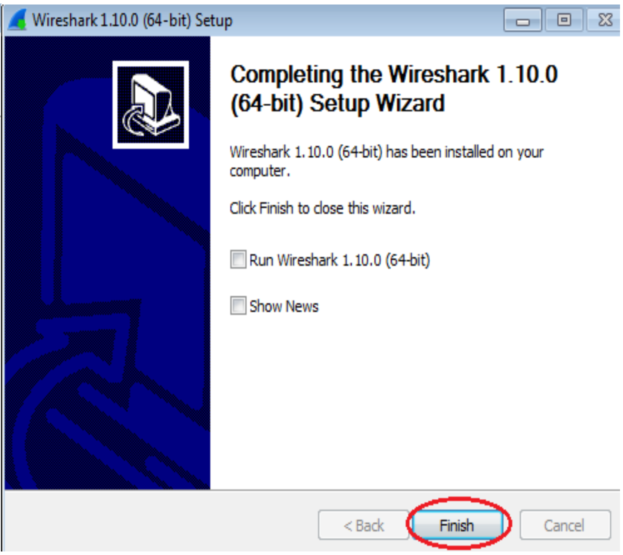
Setup was completed successfully.

Completed

```
Extract: reordercap.exe
Output folder: C:\Program Files\Wireshark
Extract: capinfos.exe
Extract: capinfos.html
Output folder: C:\Program Files\Wireshark
Extract: rawshark.exe
Extract: rawshark.html
Output folder: C:\Program Files\Wireshark
Extract: user-guide.chm
Completed
```

Nullsoft Install System v2.46

< Back | Next > | Cancel



Wireshark 1.10.0 (64-bit) Setup

Completing the Wireshark 1.10.0 (64-bit) Setup Wizard

Wireshark 1.10.0 (64-bit) has been installed on your computer.

Click Finish to close this wizard.

□ Run Wireshark 1.10.0 (64-bit)

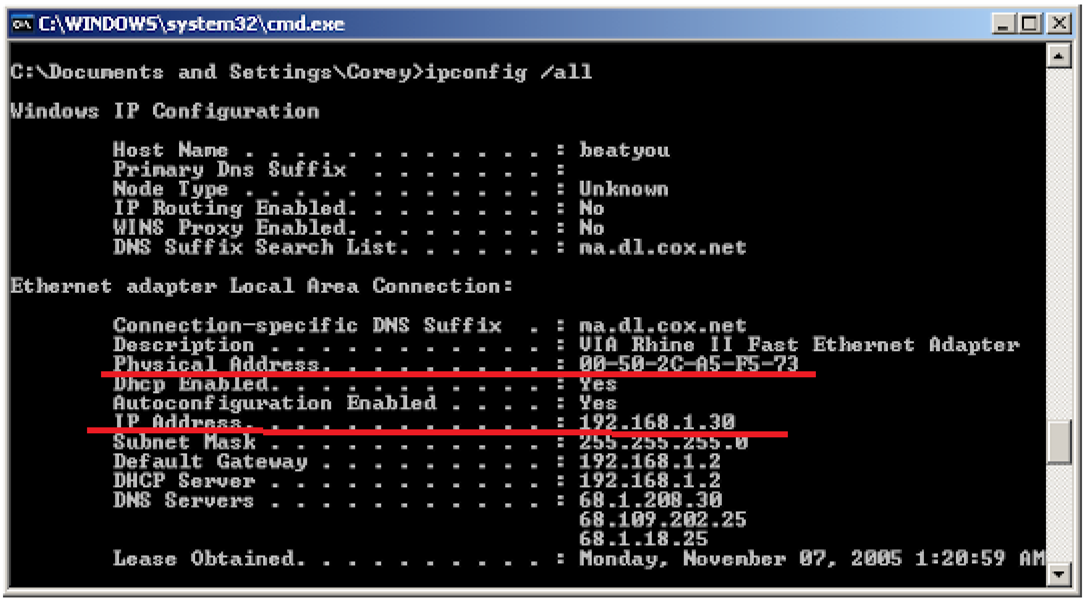
□ Show News

< Back | Finish | Cancel

Collection and analysis of ICMP data on local nodes in Wireshark

We send echo request using the **ping** command to another PC on the local network and intercept ICMP requests and feedback in Wireshark. At the same time, find the necessary information in the collected frames. This analysis will help understand how packet headers are used to transmit data to a destination.

Define the addresses of our PC interfaces. In this lab you have to find out the IP address of your computer and the physical address of the network adapter (MAC address). Open a command prompt window, type **ipconfig/all**, and then press ENTER. Write down the IP address of the PC interface and the MAC address.

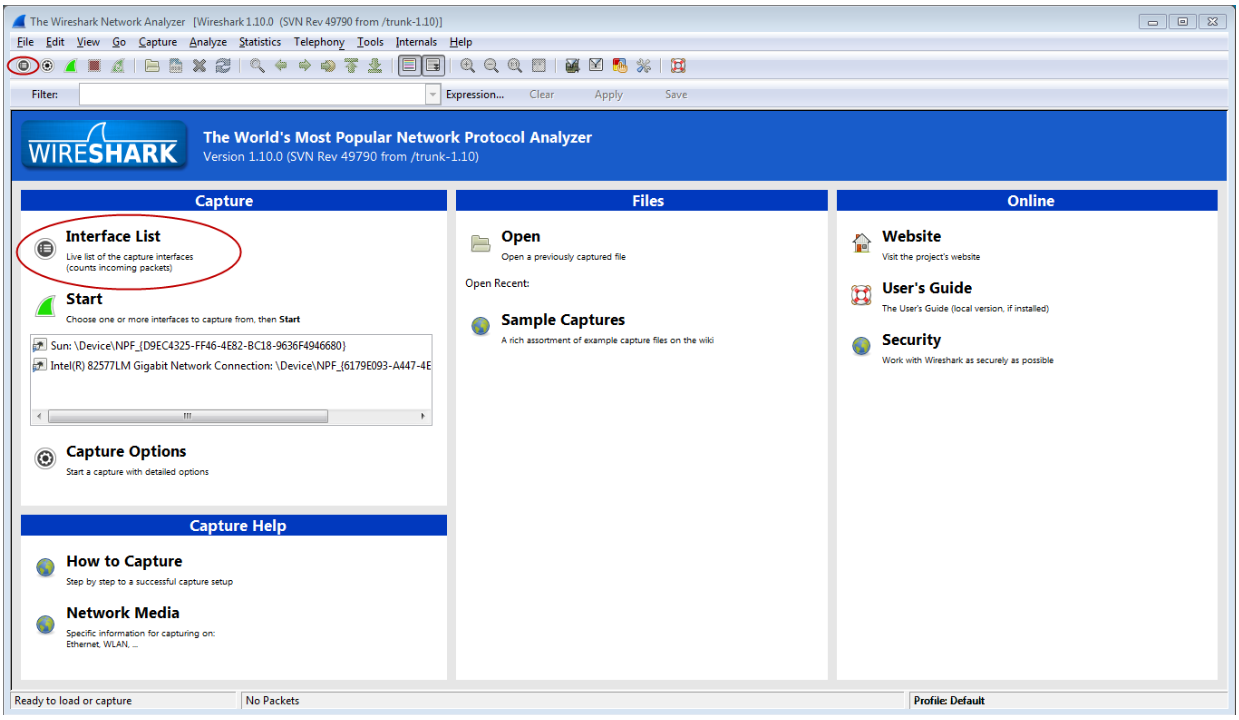


```
C:\Documents and Settings\Corey>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : beatyou
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : ma.dl.cox.net

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : ma.dl.cox.net
        Description . . . . . . . . . . . : VIA Rhine II Fast Ethernet Adapter
        Physical Address. . . . . . . . . : 00-50-2C-A5-F5-73
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.30
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.2
        DHCP Server . . . . . . . . . . . : 192.168.1.2
        DNS Servers . . . . . . . . . . . : 68.1.208.30
                                            68.109.202.25
                                            68.1.18.25
        Lease Obtained. . . . . . . . . . : Monday, November 07, 2005 1:20:59 AM
```

Share IP addresses with a colleague, but do not tell your MAC address yet. Start Wireshark and start intercepting data.

On your PC, click the Start / Wireshark button.

Wireshark program , click on the **Interface parameter list** (List of interfaces).



The World's Most Popular Network Protocol Analyzer
Version 1.10.0 (SVN Rev 49790 from /trunk-1.10)

Interface List: Live list of the capture interfaces (counts incoming packets)

Start: Choose one or more interfaces to capture from, then **Start**

Sun: \Device\NPF_{D9EC4325-FF46-4E82-BC18-9636F4946680}
Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4E

Capture Options: Start a capture with detailed options

How to Capture: Step by step to a successful capture setup

Network Media: Specific information for capturing on: Ethernet, WLAN, ...

Open: Open a previously captured file

Sample Captures: A rich assortment of example capture files on the wiki

Website: Visit the project's website

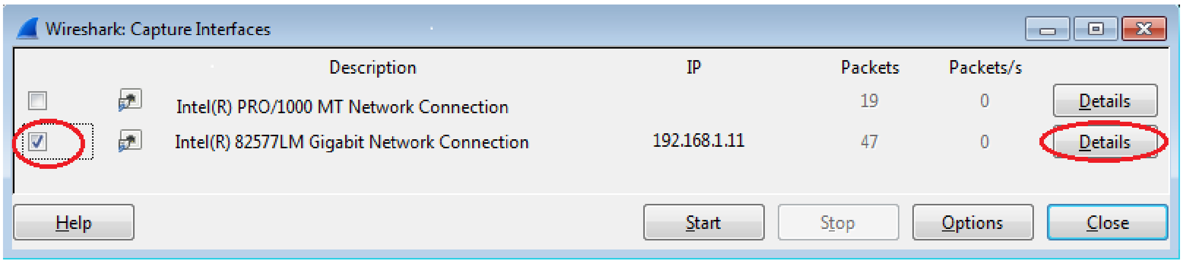
User's Guide: The User's Guide (local version, if installed)

Security: Work with Wireshark as securely as possible

Ready to load or capture | No Packets | Profile: Default

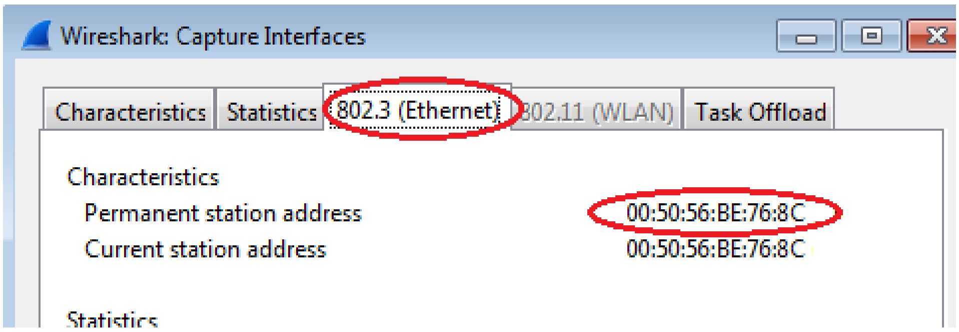
You can also open the list of interfaces by clicking on the icon of the first interface in a number of icons.

In the Wireshark **Capture Interfaces** window, select the check box next to the interface connected to your local network.



		Description	IP	Packets	Packets/s	
□		Intel(R) PRO/1000 MT Network Connection		19	0	Details
☑		Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details

If several interfaces are listed and you are not sure which one to choose, click the **Details button** and open the 802.3 (Ethernet) tab. Make sure that the MAC address a matches the result you received earlier. After making sure the interface is correct, close the information window.

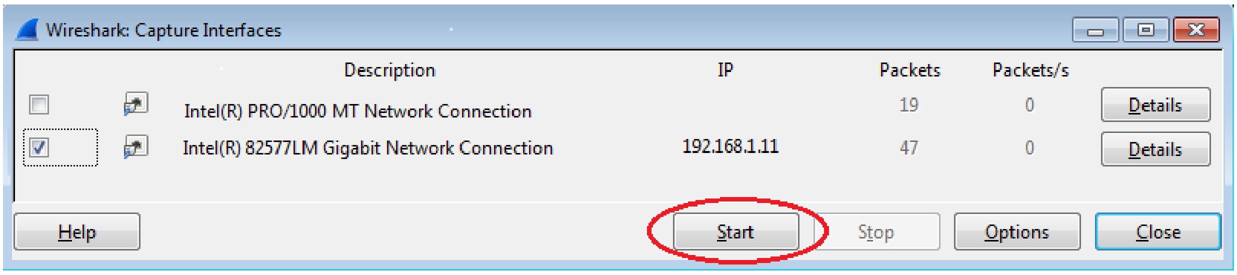


Characteristics

Permanent station address	00:50:56:BE:76:8C
Current station address	00:50:56:BE:76:8C

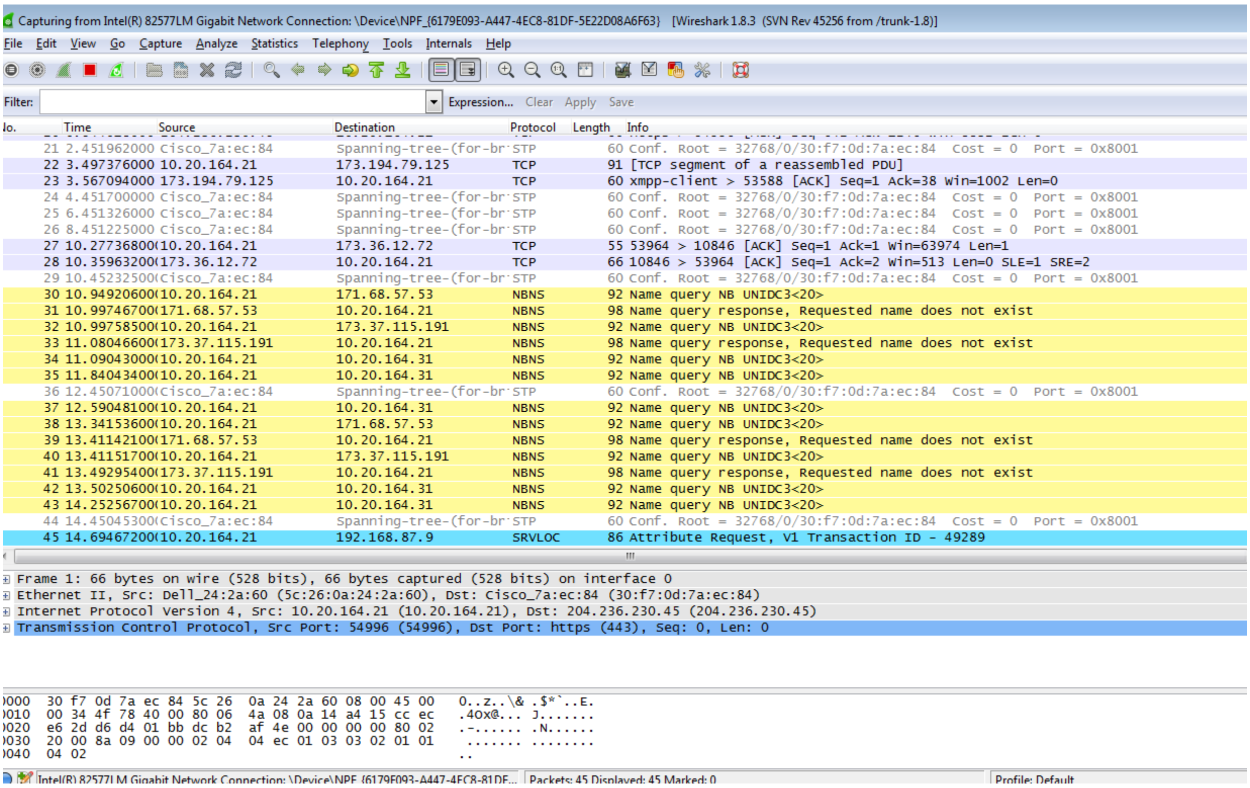
Statistics

Then click the **Start button** to start intercepting data.



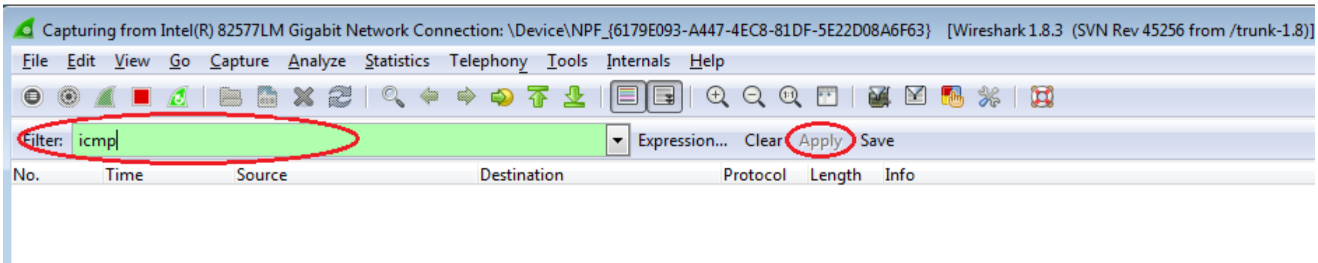
		Description	IP	Packets	Packets/s	
□		Intel(R) PRO/1000 MT Network Connection		19	0	Details
☑		Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details

Information will scroll to the top of the Wireshark window. Data strings are highlighted in different colors depending on the protocol.



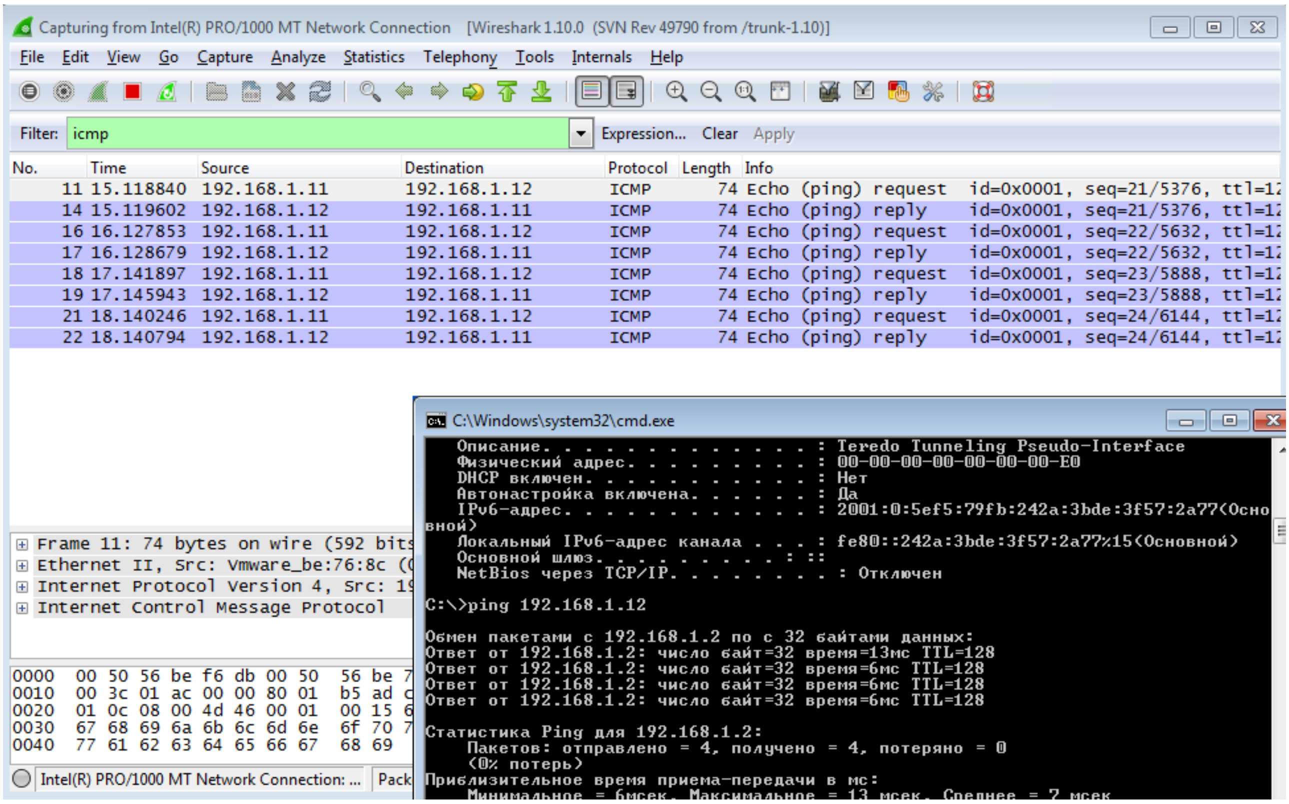
```
Capturing from Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF-5E22D08A6F63}   [Wireshark 1.8.3  (SVN Rev 45256 from /trunk-1.8)]

Filter:

lo.   Time          Source               Destination              Protocol  Length  Info
  21 2.451962000 Cisco_7a:ec:84      Spanning-tree-(for-br STP      60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
  22 3.497376000 10.20.164.21        173.194.79.125        TCP      91 [TCP segment of a reassembled PDU]
  23 3.567094000 173.194.79.125      10.20.164.21          TCP      60 xmpp-client > 53588 [ACK] Seq=1 Ack=38 Win=1002 Len=0
  24 4.451700000 Cisco_7a:ec:84      Spanning-tree-(for-br STP      60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
  25 6.451326000 Cisco_7a:ec:84      Spanning-tree-(for-br STP      60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
  26 8.451225000 Cisco_7a:ec:84      Spanning-tree-(for-br STP      60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
  27 10.27736800(10.20.164.21        173.36.12.72          TCP      55 53964 > 10846 [ACK] Seq=1 Ack=1 Win=63974 Len=1
  28 10.35963200(173.36.12.72        10.20.164.21          TCP      66 10846 > 53964 [ACK] Seq=1 Ack=2 Win=513 Len=0 SLE=1 SRE=2
  29 10.45232500(Cisco_7a:ec:84      Spanning-tree-(for-br STP      60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
  30 10.94920600(10.20.164.21        171.68.57.53          NBNS     92 Name query NB UNIDC3<20>
  31 10.99746700(171.68.57.53        10.20.164.21          NBNS     98 Name query response, Requested name does not exist
  32 10.99758500(10.20.164.21        173.37.115.191        NBNS     92 Name query NB UNIDC3<20>
  33 11.08046600(173.37.115.191      10.20.164.21          NBNS     98 Name query response, Requested name does not exist
  34 11.09043000(10.20.164.21        10.20.164.31          NBNS     92 Name query NB UNIDC3<20>
  35 11.84043400(10.20.164.21        10.20.164.31          NBNS     92 Name query NB UNIDC3<20>
  36 12.45071000(Cisco_7a:ec:84      Spanning-tree-(for-br STP      60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
  37 12.59048100(10.20.164.21        10.20.164.31          NBNS     92 Name query NB UNIDC3<20>
  38 13.34153600(10.20.164.21        171.68.57.53          NBNS     92 Name query NB UNIDC3<20>
  39 13.41142100(171.68.57.53        10.20.164.21          NBNS     98 Name query response, Requested name does not exist
  40 13.41151700(10.20.164.21        173.37.115.191        NBNS     92 Name query NB UNIDC3<20>
  41 13.49295400(173.37.115.191      10.20.164.21          NBNS     98 Name query response, Requested name does not exist
  42 13.50250600(10.20.164.21        10.20.164.31          NBNS     92 Name query NB UNIDC3<20>
  43 14.25256700(10.20.164.21        10.20.164.31          NBNS     92 Name query NB UNIDC3<20>
  44 14.45045300(Cisco_7a:ec:84      Spanning-tree-(for-br STP      60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
  45 14.69467200(10.20.164.21        192.168.87.9          SRVLOC   86 Attribute Request, V1 Transaction ID - 49289

⊞ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: Dell_24:2a:60 (5c:26:0a:24:2a:60), Dst: Cisco_7a:ec:84 (30:f7:0d:7a:ec:84)
⊞ Internet Protocol Version 4, Src: 10.20.164.21 (10.20.164.21), Dst: 204.236.230.45 (204.236.230.45)
⊞ Transmission Control Protocol, Src Port: 54996 (54996), Dst Port: https (443), Seq: 0, Len: 0

)000  30 f7 0d 7a ec 84 5c 26  0a 24 2a 60 08 00 45 00   0..z..\& .$*`..E.
)010  00 34 4f 78 40 00 80 06  4a 08 0a 14 a4 15 cc ec   .4Ox@... J.......
)020  e6 2d d6 d4 01 bb dc b2  af 4e 00 00 00 00 80 02   .-...... .N......
)030  20 00 8a 09 00 00 02 04  04 ec 01 03 03 02 01 01    ....... ........
)040  04 02                                              ..

Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF...   Packets: 45 Displayed: 45 Marked: 0   Profile: Default
```

Information can scroll very quickly depending on the type of connection between the PC and the local network. You can apply a filter to make it easier to view and work with the data collected by Wireshark. In this lab, we only need the ICMP. To display only the ICMP (**ping** echo request**)** protocol blocks, enter **icmp** in the filter field at the top of the Wireshark window and press the ENTER key or the **Apply** button.



```
Capturing from Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF-5E22D08A6F63}   [Wireshark 1.8.3  (SVN Rev 45256 from /trunk-1.8)]

Filter: icmp

No.   Time   Source   Destination   Protocol   Length   Info
```

After that, all the data in the upper window will disappear, but the interception of traffic in the interface will continue. Open a command prompt window that you opened earlier and send an echo request using the **ping** command to the IP address obtained from another student. Note that the data will reappear at the top of the Wireshark window.


Capturing from Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
C:\Windows\system32\cmd.exe
Intel(R) PRO/1000 MT Network Connection: ...
Pack

Filter: icmp

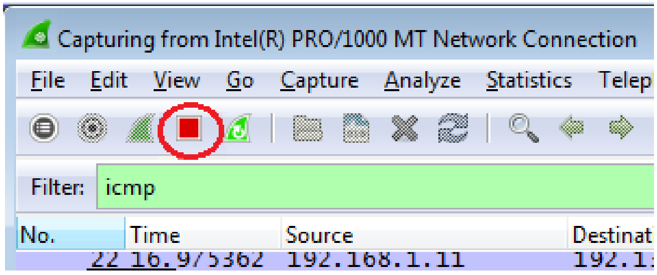
```
No.     Time       Source          Destination     Protocol Length Info
     11 15.118840  192.168.1.11    192.168.1.12    ICMP         74 Echo (ping) request  id=0x0001, seq=21/5376, ttl=1:
     14 15.119602  192.168.1.12    192.168.1.11    ICMP         74 Echo (ping) reply    id=0x0001, seq=21/5376, ttl=1:
     16 16.127853  192.168.1.11    192.168.1.12    ICMP         74 Echo (ping) request  id=0x0001, seq=22/5632, ttl=1:
     17 16.128679  192.168.1.12    192.168.1.11    ICMP         74 Echo (ping) reply    id=0x0001, seq=22/5632, ttl=1:
     18 17.141897  192.168.1.11    192.168.1.12    ICMP         74 Echo (ping) request  id=0x0001, seq=23/5888, ttl=1:
     19 17.145943  192.168.1.12    192.168.1.11    ICMP         74 Echo (ping) reply    id=0x0001, seq=23/5888, ttl=1:
     21 18.140246  192.168.1.11    192.168.1.12    ICMP         74 Echo (ping) request  id=0x0001, seq=24/6144, ttl=1:
     22 18.140794  192.168.1.12    192.168.1.11    ICMP         74 Echo (ping) reply    id=0x0001, seq=24/6144, ttl=1:
```

```
⊞ Frame 11: 74 bytes on wire (592 bits
⊞ Ethernet II, Src: Vmware_be:76:8c ((
⊞ Internet Protocol Version 4, Src: 19
⊞ Internet Control Message Protocol
```

```
0000  00 50 56 be f6 db 00 50  56 be 7
0010  00 3c 01 ac 00 00 80 01  b5 ad c
0020  01 0c 08 00 4d 46 00 01  00 15 6
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 7
0040  77 61 62 63 64 65 66 67  68 69
```

```
   Описание. . . . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Физический адрес. . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP включен. . . . . . . . . . . . : Нет
   Автонастройка включена. . . . . . . : Да
   IPv6-адрес. . . . . . . . . . . . . : 2001:0:5ef5:79fb:242a:3bde:3f57:2a77(Осно
вной)
   Локальный IPv6-адрес канала . . . . : fe80::242a:3bde:3f57:2a77%15(Основной)
   Основной шлюз. . . . . . . . . : ::
   NetBios через TCP/IP. . . . . . . . : Отключен

C:\>ping 192.168.1.12

Обмен пакетами с 192.168.1.2 по с 32 байтами данных:
Ответ от 192.168.1.2: число байт=32 время=13мс TTL=128
Ответ от 192.168.1.2: число байт=32 время=6мс TTL=128
Ответ от 192.168.1.2: число байт=32 время=6мс TTL=128
Ответ от 192.168.1.2: число байт=32 время=6мс TTL=128

Статистика Ping для 192.168.1.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 6мсек, Максимальное = 13 мсек, Среднее = 7 мсек
```

Stop data interception by clicking the **Stop Capture** icon.


Capturing from Intel(R) PRO/1000 MT Network Connection
File Edit View Go Capture Analyze Statistics Telep
No. Time Source Destinat

Filter: icmp

```
 22 16.975362  192.168.1.11    192.1:
```

Analyze the data obtained. If another student 's computer does not respond to your echo requests, it may be because your computer's firewall is blocking those requests.

Skip ICMP traffic through Windows Firewall

If ping commands from other computers **do** not pass to your PC, they may be blocked by a firewall. **Firewall** is a device that allows to deny, encrypt, pass through a proxy all computer traffic between areas of different security according to a set of rules and other criteria.

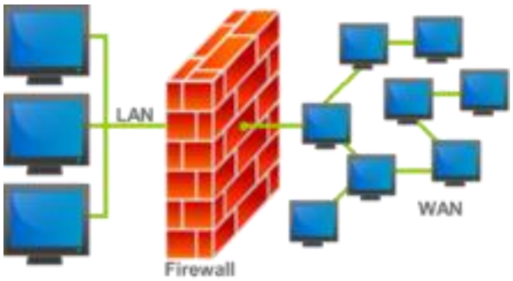


Fig. 4.1. Schematic representation of the firewall

The firewall can be as a stand-alone device (a router), or as software installed on a personal computer or proxy server. Depending on the active compounds being monitored, firewalls are divided into: **stateless** (simple filtering), which do not monitor current connections (eg. TCP), but filter the data flow solely on the basis of static rules; **stateful** (context-sensitive filtering), tracking current connections and skipping only those packets that satisfy the logic and algorithms of the relevant protocols and programs. These types of firewalls allow you to more effectively combat various DDoS attacks and vulnerabilities in some network protocols.

There are three types of firewalls: network layer, application layer and connection layer. Each of these types uses its own different approach to network protection.

Network-level firewalls are represented by and shielding and router. They control only the data of the network and transport levels of the service information packets. The disadvantage of such routers is that five more levels remain uncontrolled. Administrators working with shielding routers should keep in mind that most packet filtering devices do not have auditing and alarm mechanisms. In other words, routers can be attacked and repel large numbers, and administrators will not even be informed.

Branmauer applied level or proxy server and (proxy servers) establish a certain physical separation between the local network and the Internet, so they meet the highest security requirements, the proxy server uses faster computers.

To perform laboratory work it is necessary to pass echo requests by means of the **ping command** through a firewall and **to cancel a new firewall rule after lab work.** It is necessary to create a new rule that allows the passage of ICMP traffic through the firewall. To do this, in the control panel, select **System and Security**.

In the System and Security window, select **Windows Firewall**.

On the left side of the Windows Firewall window, select **Advanced Options**.

Inbound Connection Rules in the left sidebar, and then click **Create Rule** in the right sidebar.

The Create New Rules for Inbound Connections wizard opens. In the **Rule Type window,** select the **Customizable radio button**, and then click **Next**.

In the left pane, select **Protocols and Ports** and select **ICMPv4** from the protocol type drop-down menu.

Then click **Next**. In the left pane, select Name and enter **Allow in the appropriate field ICMP Requests**. Click the **Finish button**.

The created rule will allow another student to receive feedback from PC.

Disable and delete the new ICMP rule. At the end of the laboratory work, **you must disable or delete the newly created rule**. The **Disable rule option** will allow you to re-enable it if necessary. Deleting a rule completely will permanently remove it from the list of rules for incoming connections.

On the left side of the **Advanced Security Settings window,** select **Inbound Connection Rules** , and find the rule you created in step 1.

To disable a rule, select the **Disable Rule option**. It will then change to the **Enable Rule** option. The rule can be turned on and off. The status of the rule is displayed in the " **Enabled** " column of the list of rules for incoming connections.

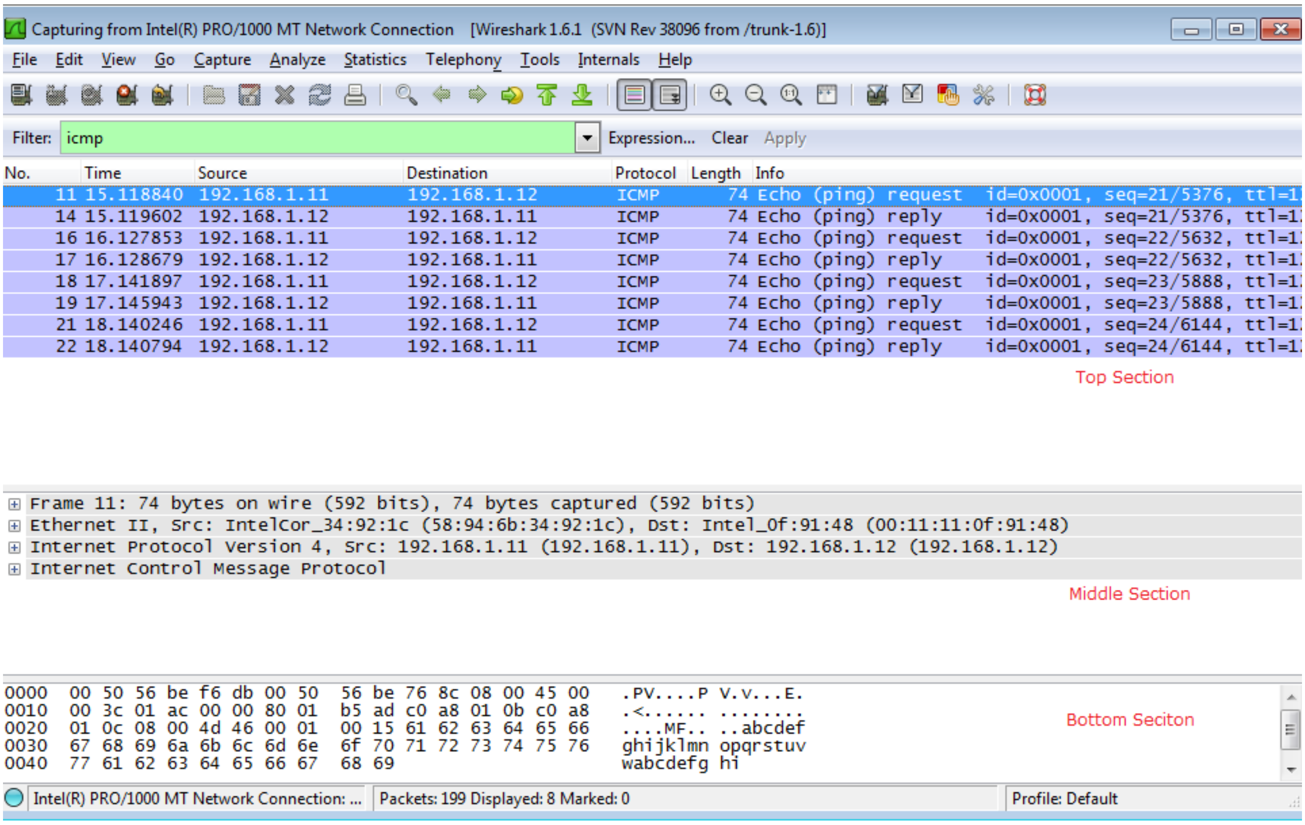
Delete option. You will then need to create this rule again to allow ICMP requests. Further you have to check the data generated by ho -queries using the **ping command of** another student's PC. Wireshark displays data in three sections:

1) the top section displays a list of received PDU frames with summary information about IP packets;

2) the middle section provides information about the PDU for the frame selected in the upper part of the screen, and the division of the PDU frame into layers of protocols;

3) the lower section shows the raw data of each level.

Raw data is displayed in both hexadecimal and decimal formats.



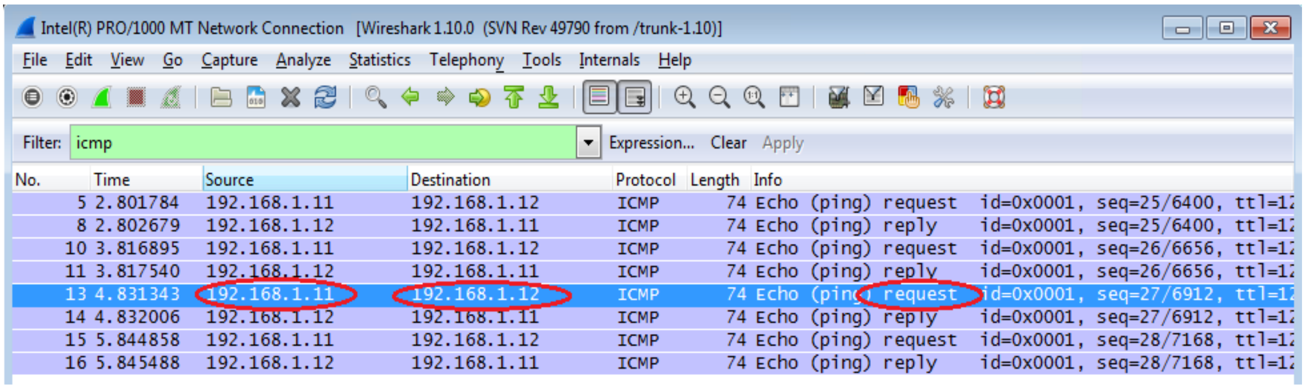
Capturing from Intel(R) PRO/1000 MT Network Connection [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
Expression... Clear Apply
Top Section
Middle Section
Bottom Seciton
Intel(R) PRO/1000 MT Network Connection: ...
Packets: 199 Displayed: 8 Marked: 0
Profile: Default

```
No.   Time       Source        Destination   Protocol Length Info
   11 15.118840  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=21/5376, ttl=1
   14 15.119602  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=21/5376, ttl=1
   16 16.127853  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=22/5632, ttl=1
   17 16.128679  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=22/5632, ttl=1
   18 17.141897  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=23/5888, ttl=1
   19 17.145943  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=23/5888, ttl=1
   21 18.140246  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=24/6144, ttl=1
   22 18.140794  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=24/6144, ttl=1
```

```
⊞ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: Intel_0f:91:48 (00:11:11:0f:91:48)
⊞ Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.12 (192.168.1.12)
⊞ Internet Control Message Protocol
```

```
0000  00 50 56 be f6 db 00 50  56 be 76 8c 08 00 45 00   .PV....P V.v...E.
0010  00 3c 01 ac 00 00 80 01  b5 ad c0 a8 01 0b c0 a8   .<...... ........
0020  01 0c 08 00 4d 46 00 01  00 15 61 62 63 64 65 66   ....MF.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

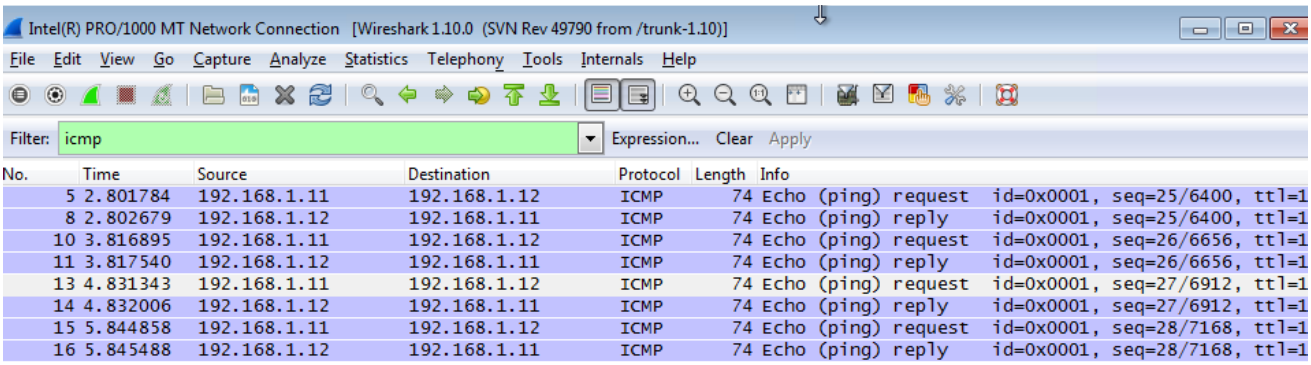
Select the PDU frame and the first ICMP request at the top of the Wireshark window. Note that the **Source** column lists the IP address of your computer, and the **Destination** column lists the IP address of the PC to which you sent the echo request using the **ping** command.



Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
Expression... Clear Apply

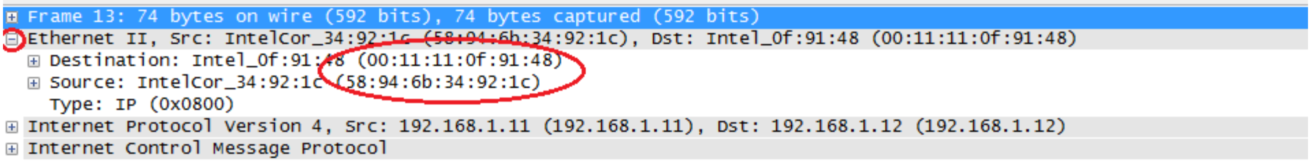
```
No.  Time      Source        Destination   Protocol Length Info
   5 2.801784  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=25/6400, ttl=1
   8 2.802679  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=25/6400, ttl=1
  10 3.816895  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=26/6656, ttl=1
  11 3.817540  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=26/6656, ttl=1
  13 4.831343  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=27/6912, ttl=1
  14 4.832006  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=27/6912, ttl=1
  15 5.844858  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=28/7168, ttl=1
  16 5.845488  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=1
```

Without changing the PDU frame selection in the top section of the program, go to the middle section. Click on the + symbol to the left of the "Ethernet II" line to see the MAC addresses of the source and destination.


Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Expression...
Clear
Apply

Filter: icmp

```
No.    Time       Source         Destination    Protocol Length Info
     5 2.801784   192.168.1.11   192.168.1.12   ICMP     74 Echo (ping) request  id=0x0001, seq=25/6400, ttl=1
     8 2.802679   192.168.1.12   192.168.1.11   ICMP     74 Echo (ping) reply    id=0x0001, seq=25/6400, ttl=1
    10 3.816895   192.168.1.11   192.168.1.12   ICMP     74 Echo (ping) request  id=0x0001, seq=26/6656, ttl=1
    11 3.817540   192.168.1.12   192.168.1.11   ICMP     74 Echo (ping) reply    id=0x0001, seq=26/6656, ttl=1
    13 4.831343   192.168.1.11   192.168.1.12   ICMP     74 Echo (ping) request  id=0x0001, seq=27/6912, ttl=1
    14 4.832006   192.168.1.12   192.168.1.11   ICMP     74 Echo (ping) reply    id=0x0001, seq=27/6912, ttl=1
    15 5.844858   192.168.1.11   192.168.1.12   ICMP     74 Echo (ping) request  id=0x0001, seq=28/7168, ttl=1
    16 5.845488   192.168.1.12   192.168.1.11   ICMP     74 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=1
```



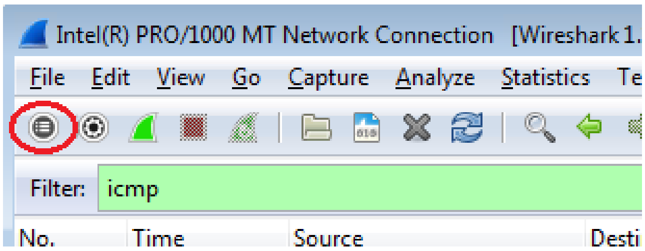
```
⊞ Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊟ Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: Intel_0f:91:48 (00:11:11:0f:91:48)
  ⊞ Destination: Intel_0f:91:48 (00:11:11:0f:91:48)
  ⊞ Source: IntelCor_34:92:1c (58:94:6b:34:92:1c)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.12 (192.168.1.12)
⊞ Internet Control Message Protocol
```

Does the source MAC address match your computer's interface?

Does the MAC address of the destination in Wireshark match the MAC address of another student? How did your PC determine the MAC address of the PC to which the echo request was sent using the **ping** command? In the intercepted ICMP request example, the ICMP protocol data is encapsulated within the IPv4 PDU packet (IPv4 header), which is then encapsulated in the Ethernet II frame packet (Ethernet II header) for transmission over the local network.

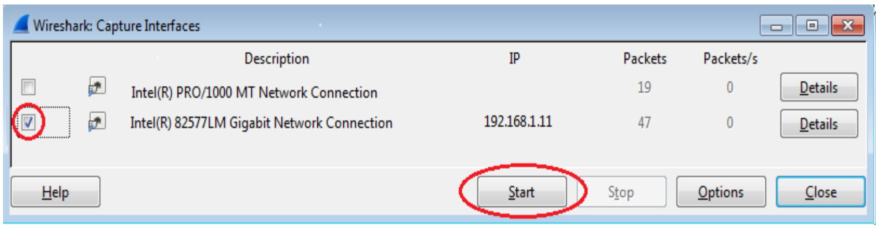
Collection and analysis of ICMP data on remote nodes in Wireshark

Next, you have to send echo requests using the **ping** command to remote nodes (nodes outside the local network) and examine the data generated by these requests. You will then identify the differences between this data and the data studied for the local network. Start data interception in the interface. Click on the Interface icon List to reopen the list of PC interfaces.



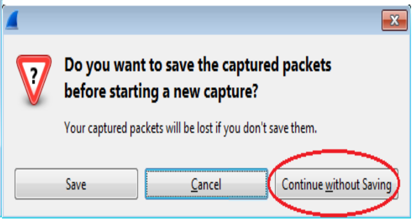
Filter: icmp

Make sure that a check box is selected in front of the LAN interface, and click the **Start** button.



Wireshark: Capture Interfaces

		Description	IP	Packets	Packets/s	
□		Intel(R) PRO/1000 MT Network Connection		19	0	Details
☑		Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details



Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.

A window will appear asking you to save the previously received data before starting a new interception. It is not necessary to keep this data. Click **Continue without Saving**.

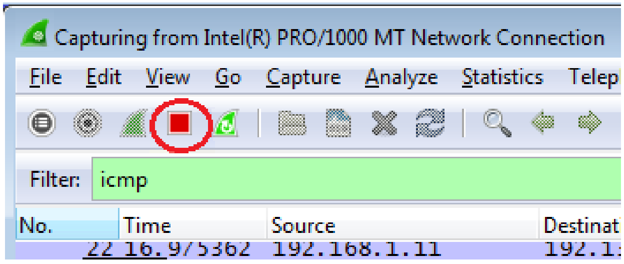
Tasks for laboratory work 3

1. Set up a local network with another student and collect ICMP data using Wireshark according to the instructions for the laboratory work. Check that you have correctly identified your own MAC address and the MAC address of another student (in the screenshot of this task you have to paint the first / last three characters of the received MAC addresses based on the confidentiality of information).

2. Intercept ICMP data for two remote servers. After enabling data interception, send a **ping** echo request to the URLs of Server 1 and Server 2 to verify connectivity.

When **ping** queries to the specified URLs, note that the Domain Name Service (DNS) will convert the URL to an IP address. Write down the IP addresses obtained for each URL (addresses may differ).

Stop data interception by clicking the **Stop Capture** icon.



Capturing from Intel(R) PRO/1000 MT Network Connection

Filter: icmp

```
No.    Time          Source         Destinat
  22 16.975362   192.168.1.11   192.1
```

Analyze the data obtained from remote nodes. View the data collected and examine the IP and MAC addresses of the websites you visit.

Enter the IP and MAC address and destination for the websites:

Server 1 : IP: _____._____._____._____ MAC: ___ _: _ ___: ____: ____: ____: ____

Server 2 : IP: _____._____._____._____ MAC: ___ _: _ ___: ____: ____: ____: ____

What is special about this data? Wireshark show the actual MAC address of local nodes but not the actual MAC address of remote nodes?

Version	Server 1	Server 2
1	www.java.com	www.yahoo.com
2	www.google.com	www.cisco.com
3	www.gmail.com	www.facebook.com
4	www.ford.com	www.gmail.com
5	www.cisco.com	www.phyton.com
6	www.apple.com	www.telegram.org
7	www.oracle.com	www.bbc.com
8	www.scopus.com	www.w3schools.com
9	www.linkedin.com	www.java.com
10	www.java.com	www.chevron.com
11	www.yahoo.com	www.scopus.com
12	www.gmail.com	www.verizon.com
13	www.chevron.com	www.linkedin.com
14	www.w3schools.com	www.google.com
15	www.linkedin.com	www.apple.com
16	www.microsoft.com	www.facebook.com
17	www.cisco.com	www.scopus.com
18	www.pepsico.com	www.aig.com
19	www.scopus.com	www.gmail.com
20	www.apple.com	www.cisco.com
21	www.google.com	www.yahoo.com
22	www.facebook.com	www.ford.com
23	www.w3schools.com	www.java.com
24	www.chevron.com	www.microsoft.com
25	www.scopus.com	www.cisco.com

Report requirements for laboratory work 3

The report should include:

1. Title page.

2. Individual task for laboratory work.

3. The course of work, sequential description of the steps performed with screenshots.

4. Conclusions.

Questions for self-assessment

1. What is the purpose of Wireshark and what are the features of its use?

2. What is the structure of the Wireshark window?

3. What is the sequence of actions for the collection and analysis of ICMP data by Wireshark ?

4. What is the purpose of a firewall?

5. What are the types of firewalls?

6. Why does Wireshark show the actual MAC address of local nodes but not the actual MAC address of remote nodes?

References

1. Wireshark. URL: www.wireshark.org
2. What Is Firewall. URL: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall
3. PDU. URL: https://www.geeksforgeeks.org/protocol-data-unit-pdu/

LABORATORY WORK № 4. IP ADDRESSING. NETWORK SUBNETTING

Objective: to learn to calculate the number of subnets and nodes by subnet prefix, to calculate the network address, as well as to use online calculators to calculate the basic quantitative and qualitative indicators of specified networks.

Theory and methodological instructions

IP addressing

IP addressing is used everywhere. When you post on social networks, watch videos on YouTube, or download programs, and it doesn’t matter if you have a computer or a smartphone – everywhere, IP addressing is used for communication.

In real life, when we send a letter to someone, we must include the recipient's address on the envelope as well as your address (sender's address). Without this, the letter will not find its recipient and you will not be able to receive a response to this letter. The same thing happens in computer networks – in order for one computer to send a message to another computer, it must know the address of the recipient computer, and also provide information about its address to receive a response. This address assigned to a computer is called an IP address.

To identify a computer or other network device, it is enough to know two parameters: IP address and netmask.

For example:

IP: 192.168.2.102

Netmask: 255.255.255.0

In fact, the IP address 192.168.2.102 and the Mask 255.255.255.0 are just an abstraction, representing a number in a decimal, human-readable format.

The computer sees these numbers in binary format. To store an IPv4 address, 32-bit variables are used, one byte is equal to 8 bits -> 4 * 8 = 32 – hence the four in IPv4, that is, these are 32-bit numbers consisting of a combination of 32 zeros and ones.

The IPv4 address and subnet mask for a computer looks like this:

Address: 11000000101010000000001001100110

Netmask: 11111111111111111111111100000000

As you can see, for a person, these zeros and ones say little, therefore, for ease of perception, these sequences of zeros and ones are divided into blocks of 8 bits, octets:

Address: 11000000.10101000.00000010.01100110

Netmask: 11111111.11111111.11111111.00000000

It’s already easier, but the problem has not gone away, even breaking a 32-bit number into 4 octets, the situation with perception has not improved, a person still perceives numbers written in decimal format most easily.

Address: 11000000.10101000.00000010.01100110 (192.168.2.102)

Netmask: 11111111.11111111.11111111.00000000 (255.255.255.0) /24

Instead of 11000000101010000000001001100110 -> 192.168.2.102. An IP address written in this format is much easier to remember.

Each of the four octets can take a value from 0 to 255 (255 = 2^8 - 1), in binary equivalent from 00000000 to 11111111.

Translating numbers from one number system to another

When working with computers and network devices, network professionals use binary, decimal, and hexadecimal numbers. Microsoft 's operating system includes a built-in calculator. The calculator version in Windows 7 includes a regular mode that can be used to perform simple arithmetic tasks, as well as advanced capabilities for software, scientific and statistical calculations. Click the Windows Start button and select All Programs. Open the "Standard" folder and click on "Calculator". When the calculator opens, select the "View" menu. Four modes are available: Normal, Engineering, Programmer and Statistics.

Several number systems are available in Windows Calculator Programmer mode : **Hex** (hexadecimal with base 16), **Dec** (decimal with base 10), **Oct** (octal with base 8) and **Bin** (binary with base 2). Computers and other electronic devices for storing and transmitting data, as well as numerical calculations, use a binary system consisting only of zeros and ones. All computer calculations are performed in binary (digital) form, regardless of the form in which they are displayed. Hexadecimal numbers are based on 16, and a combination of digits 0 to 9 and letters A to F is used to represent binary or decimal equivalents. Hexadecimal characters are used to represent IPv6 and MAC addresses.

Tasks for laboratory work 4

In this laboratory work you have to fill in all the blank fields of the tables and answer the questions posed in the instructions for laboratory work.

Use Windows 7 calculator to convert numbers between different number systems in "Programmer" mode.

Open the View menu and select **Programmer mode**. Convert the following numbers to binary, decimal, and hexadecimal:

Decimal format	Binary format	Hexadecimal format
175		
204		
19		
77		
56		
147		
228		

Convert IPv4 -address nodes and subnet masks to binary number system

IPv 4-addresses and subnet masks are expressed in decimal format with a semicolon (four octets), such as 192.168.1.10 and 255.255.255.0, respectively.

Each decimal octet in the address or mask can be converted to 8 binary digits. Octets are always 8 binary bits. So **The IPv 4 address will contain 32 bits of zeros and ones.**

Using the Windows calculator, convert the IP address 192.168.1.10 to binary format and write it in the following table:

Decimal format	**Binary format**
192	
168	
1	
10	

Subnet masks, such as 255.255.255.0, are also displayed in decimal format with a semicolon. The subnet mask always consists of four 8-bit octets, each of which is expressed as a decimal number. Use the Windows calculator to convert the eight possible decimal values of the subnet mask octets to binary numbers and write them in the following table:

Decimal format	**Binary format**
0	
128	
192	
224	
240	
248	
252	
254	
255	

Using a combination of IPv 4 addresses and subnet masks, you can determine the network part and calculate the number of nodes available in this IPv 4 subnet.

Determining the number of nodes in the network using two digits

You can determine the network part and the number of nodes available in the network by the IPv4 network address and subnet mask.

To calculate the number of nodes in the network, you must determine the network and node parts of the address.

The address and mask of the subnet are converted to binary numbers on the example of the address 192.168.1.10 with the subnet 255.255.248.0. When writing the results of data translation in binary numbers, set the bits.

IP address and subnet mask in decimal format	IP address and subnet mask in binary format
192.168.1.10	
255.255.248.0	

(Since the first 21 bits **in the subnet mask are consecutive units, this is the network part of the address**, the others **11 bits are a node of the address**).

Since the network number and the broadcast address use two addresses from the subnet, to determine the number of available nodes in the IPv4 subnet, you have to raise the number 2 to the power of the number of node bits and subtract 2.

Number of available nodes = 2 ^ (number of bits per node) - 2

Approximately 2046 nodes (2 ^ 11-2) are available in this network. Knowing the number of node bits, determine the number of available nodes and write this value in the table below.

Number of available node bits	Number of available nodes
5	
14	
24	
10	

For this subnet mask, determine the number of available nodes and write the answer in the table below.

Subnet mask	Binary subnet mask	Number of available node bits	Number of available nodes
255.255.255.0	11111111.11111111.11111111.00000000		
255.255.240.0	11111111.11111111.11110000.00000000		
255.255.255.128	11111111.11111111.11111111.10000000		
255.255.255.252	11111111.11111111.11111111.11111100		
255.255.0.0	11111111.11111111.00000000.00000000		

Convert MAC and IPv6 address to binary form

For convenience, the address of the control of access to the data medium and the address of the Internet Protocol version 6 (IPv6) are expressed in hexadecimal digits. However, computers are able to recognize and use only binary digits for calculations.

MAC address (physical address) is usually expressed by 12 hexadecimal digits grouped in pairs and separated by hyphens (-). On Windows computers, physical addresses are usually xx - xx - xx - xx - xx - xx , where x is a digit from 0 to 9 or a Latin letter from A to F. Each hexadecimal digit in the address can be converted into four binary digits understandable to a computer.

Convert IPv6 addresses to binary

For convenience, IPv6 addresses are also written in hexadecimal characters. For computers, these IPv6 addresses can be converted to binary digits. IPv 6-address is a binary number represented as a human-readable record: 2001: 0 DB 8: ACAD : 0001: 0000: 0000: 0000: 0001 or in short form: 2001: DB 8: ACAD : 1 :: 1 .

The length of the IPv6 address is 128 bits. Using the Windows calculator, convert the IPv6 address to binary number and record the result in the table below.

Hexadecimal format	Binary format
2001	
00DB8	
ACAD	
0001	
0000	
0000	
0000	
0001	

Convert IPv4 address to binary number system

Each IPv4 address consists of two parts – network and node. The network part of the address is the same for all devices that are on the same network. The node part defines a specific node within the corresponding network. **The subnet mask is used to determine the network part of the IP address.** Devices in one network can exchange data directly; an intermediate level 3 device, such as a router, is required to communicate between devices on different networks.

To understand the principle of operation of devices in the network, you need to see the addresses in the form in which they work with devices – in binary representation. To do this, you must convert the IP address and its subnet mask from a decimal representation with dots to binary. You can then determine the network address using the **AND** operation**.**

Consider the procedure for determining the network and node parts of the IP address. To do this, translate the addresses and subnet masks from the decimal representation with dots to binary format, and then apply the bitwise operation **AND.** Then use the information to determine the addresses in the network.

You must first convert the decimal numbers to the binary equivalent. After completing this task, convert IPv4 addresses and subnet masks from decimal points to binary.

Complete the table by converting a decimal number to an 8-bit binary value. The first number has already been converted for example. Remember that the eight binary values in the octet have a base of 2 and from left to right look like 128, 64, 32, 16, 8, 4, 2 and 1.

Decimal representation	**Binary representation**
192	11000000
168	
10	
255	
2	

IPv 4 addresses will be converted in the same way as described above. Fill in the table below with the binary equivalents of the addresses provided. To make your answers easier to understand, separate the binary octets with dots.

Decimal representation	**Binary representation**
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	
172.16.18.183	
10.86.252.17	
255.255.255.128	
255.255.192.0	

Using bitwise operation I to determine network addresses

the available node addresses using bitwise operation **I.** You must first convert the decimal IPv4 address and subnet mask to their binary equivalent. Having received the network address in binary format, we will convert it to decimal. When using operation **I,** the decimal value in each bit position of the 32-bit IP address of the node is compared with the corresponding position in the 32-bit subnet mask.

If there are two zeros or 0 and 1, the result of operation **I** will be 0. If there are two units, the result will be 1, as shown in the example.

Example. Determine how many bits should be used to calculate the network address.

Description	**Decimal representation**	**Binary representation**
IP address a	192.168.10.131	11000000.10101000.00001010.10000011
Subnet mask	255.255.255.192	11111111.11111111.11111111.11000000
Network address	192.168.10.128	11000000.10101000.00001010.10000000

To calculate the network address, bits are used, which in the binary mask of the subnet have a value of 1. In the above example, 26 bits are used to calculate the network address. Enter the missing information in the table below:

Description	**Decimal representation**	**Binary representation**
IP address a	172.16.145.29	
Subnet mask	255.255.0.0	
Network address		

Description	**Decimal representation**	**Binary representation**
IP address a	192.168.10.10	
Subnet mask	255.255.255.0	
Network address		

Perform operation AND to determine the network address.

Enter the missing information in the table below:

Description	**Dozens representation**	**Binary representation**
IP address a	192.168.68.210	
Subnet mask	255.255.255.128	
Network address		

Description	**Dozens representation**	**Binary representation**
IP address a	172.16.188.15	
Subnet mask	255.255.240.0	
Network address		

You have to calculate the network address for the specified IP address and subnet masks. After receiving the network address, write down the answers needed to perform this laboratory work.

Determine if the IP addresses are on the same network.

Set up two PCs for the network. The PC-A computer is assigned the IP address 192.168.1.18, and the PC-B computer is assigned the IP address 192.168.1.33. The subnet mask of both computers is 255.255.255.240.

What is the network address of the PC-A? ____________________________

What is the network address in PC-B? ____________________________

Will these PCs be able to interact with each other directly? _______

What is the largest address assigned to a PC-B computer that will allow it to be on the same network as the PC-A? ____________________________

Determine if the IP addresses are on the same network.

Set up two PCs for the network. The PC-A computer is assigned an IP address of 10.0.0.16, and the PC-B computer is assigned an IP address of 10.1.14.68. The subnet mask of both computers is 255.254.0.0.

What is the network address of the PC-A? __________________________

What is the network address in PC-B? __________________________

Will these PCs be able to interact with each other directly? ______

What is the smallest address assigned to a PC-B computer that will allow it to be on the same network as the PC-A? ____________

Set default gateway address

Your company has a policy of using the first IP address on the network as the default gateway address. The node in the local network has an IP address of 172.16.140.24 and a subnet mask of 255.255.192.0.

What is the network address on this network? __________________

What is the default gateway address for this host? ___________

Set default gateway address

Your company has a policy of using the first IP address on the network as the default gateway address. You have been instructed to configure a new server with an IP address of 192.168.184.227 and a subnet mask of 255.255.255.248.

What is the network address on this network? ___________

What will be the default gateway for this server? ___________________

Classification IPv 4 -address

You have to identify and classify several examples of IPv4 addresses.

Analyze the table below and determine the type of address (network address, host, multicast or broadcast).

The first line shows an example of completing the table.

IP address a	Subnet mask	Address type
10.1.1.1	255.255.255.252	node
192.168.33.63	255.255.255.192	broadcast
239.192.1.100	255.252.0.0	multicast
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

Analyze the table below and determine the type of address – public or private.

IP address a / prefix	Public or private
209.165.201.30/27	Public
192.168.255.253/24	Private
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

Calculation of IPv4 subnets

Ability to work with IPv 4 subnets and determine information about networks and nodes based on known IP addresses and subnet masks is required to understand the principles of IPv 4 networks. You have to calculate the IP address of the network based on the known IP address and subnet mask.

Knowing the IP address and subnet mask, we can set the following subnet data:

- networks to address y;
- broadcast in address y;
- total number of bits of nodes;
- number of nodes in the subnet;

Define for the specified IP address and subnet mask:

- networks to addresses in this subnet;
- broadcast to addresses in this subnet;
- the range of node addresses for this subnet;
- number of created subnets;
- k number of nodes for each subnet.

To determine the network address, you must perform binary operation **I** for IPv4 addresses, using the specified subnet mask. As a result, we get a network address. If the subnet mask has a decimal value of 255 in the octet, the result will ALWAYS be the initial value of that octet. If the subnet mask has a decimal value of 0 in the octet, the result for this octet will ALWAYS be 0.

Example.

IP Address 192.168.10.10

Subnet mask 255.255.255.0

======================

Result (network) 192.168.10.0

Knowing this, you can perform binary operation **AND** only for the octet whose value in the subnet mask is different from 255 or 0.

Example.

IP Address 172.30.239.145

Subnet mask 255.255.192.0

Analyzing this example, we see that the binary operation **AND** is required only for the third octet. In this subnet mask, the first two octets will give a result of 172.30, and the fourth - 0.

IP Address 172.30.239.145

Subnet mask 255.255.192.0

=====================

Result (network) 172 .30.?. 0

Perform binary operation **AND** for the third octet.

DecimalBinary	
239	11101111
192	11000000

=======

The result is 192,100,000

Analysis of this example will again give the following result:

IP Address 172.30.239.145

Subnet mask 255.255.192.0

=========================

Result (network) 172.30.192.0

You can calculate the number of nodes for each network in this example by analyzing the subnet mask. The subnet mask will be presented in decimal format with a semicolon, for example 255.255.192.0, or in the format of a network prefix, for example / 18. The IPv4 address always contains 32 bits. Subtracting the number of bits used by the network part (as shown in the subnet mask), you get the number of bits used for the nodes.

In our example, the subnet mask 255.255.192.0 is equal to **/ 18** in the prefix entry. Subtracting **18 bits** from 32 bits will give us **the remaining 14 bits for the node**.

Based on this, we can perform a simple calculation:

2 ^ (number of node bits) - 2 = number of nodes

2 ^ 14 - 2 = 16 382 nodes

Determine the network and broadcast addresses and the number of node bits for the IPv4 address and prefixes listed in the table below.

IPv4 address / prefix	**Network address**	**Broadcast address**	**The total number of node bits**	**Total number of nodes**
192.168.100.25/28	192.168.100.16	192.168.100.31	4	14
172.30.10.130/30				
10.1.113.75/19				
198.133.219.250/24				
128.107.14.191/22				
172.16.104.99/27				

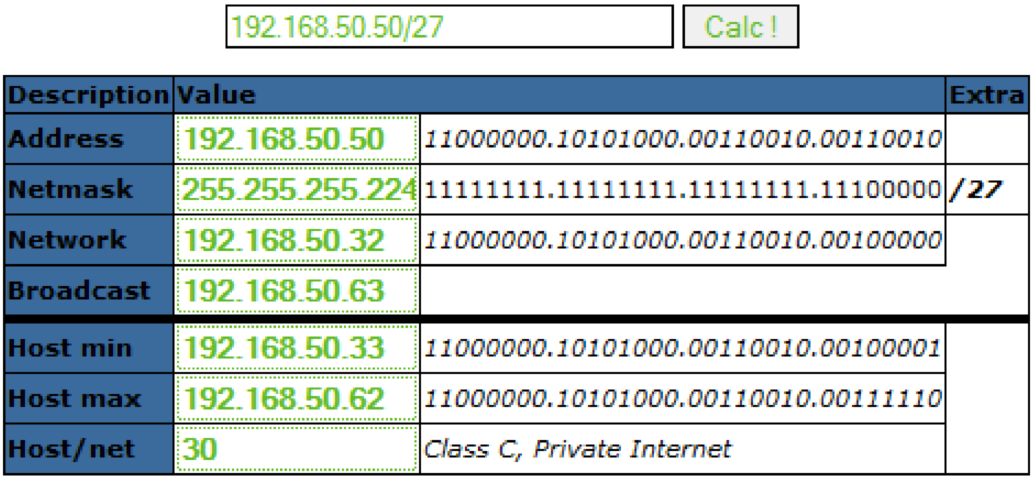
Subnet calculators

Understanding the principles of converting a decimal IP address to binary format and using operation **AND** to determine the network address is important, but the procedure itself is a time consuming process with a high probability of error.

To simplify calculations, many network administrators use **calculators for IP subnets**. There are a number of similar programs that can be downloaded and installed or run directly from the Internet.

In the **Application field**, enter 192.168.50.50/27 and click **Calc!** (Calculate). Below is a table with information about the network in decimal and binary formats.

Application:



192.168.50.50/27

Description	Value		Extra
Address	192.168.50.50	11000000.10101000.00110010.00110010	
Netmask	255.255.255.224	11111111.11111111.11111111.11100000	/27
Network	192.168.50.32	11000000.10101000.00110010.00100000	
Broadcast	192.168.50.63		
Host min	192.168.50.33	11000000.10101000.00110010.00100001	
Host max	192.168.50.62	11000000.10101000.00110010.00111110	
Host/net	30	Class C, Private Internet	

In this case: network address 192.168.50.32; subnet mask 255.255.255.224; the network supports 30 nodes; the smallest node address 192.168.50.33; the largest address of the node 192.168.50.62; broadcast address 192.168.50.63.

Calculation of network data using a subnet calculator

Fill in the tables using the web subnet calculator at **http://jodies.de/ipcalc**

1. Fill in the table below for address 10.223.23.136/10.

Description	Decimal representation	Binary representation
Address	10.223.23.136	
Subnet mask		
Network address		
Broadcast address		
Address of the first node		
Address of the last node		
Number of available nodes		Not available

Public or private address type? _______________

Report requirements for laboratory work 4

The report should include: title page, progress with screenshots of tasks and performed calculations (this section consists of a sequential description of the performed calculations (indicating their essence) and conclusions.

Questions for self-assessment

1. What is the advantage of programs and web calculators for calculating subnets?
2. What is the role in determining the network address of the subnet mask?
3. Why should you continue to study IPv4 addressing if the available IPv4 address space is exhausted?
4. What is the importance of the subnet mask when analyzing IPv 4 addresses?
5. What rules do you know for determining the network address of a node, determining the number of subnets and nodes by mask?
6. How can you determine the address of the first and last node, broadcast address?

References

1. Understanding IP Addresses, Subnets, and CIDR Notation for Networking / https://www.digitalocean.com/community/tutorials/understanding-ip-addresses-subnets-and-cidr-notation-for-networking

2. IP Calculator / http://jodies.de/ipcalc

3. Subnet Calculator / https://www.iplocation.net/subnet-calculator

4. IP Address, Get my IP, IPv4, IPv6, Internet Protocol / http://www.ip-adress.eu

5. Data Communication and Computer Network / https://www.tutorialspoint.com/data_communication_computer_network