New opportunities for studying digital information transmission technologies using Cisco equipment

L. V. Prosviryakova, *K.* A. Osipov*, and *A.* A. Dmitriev

Irkutsk National Research Technical University, Institute of High Technologies IRNRTU, Irkutsk, Russian Federation

Abstract. The article describes a methodology for studying network technologies using Cisco equipment to create a model of a digital three-level information transmission network with further analysis of the network state and network traffic research. The article briefly describes the main stages of designing and configuring a digital communication network using Cisco equipment, describes and analyzes the main network status protocols, equipment connection protocols, addressing and routing protocols, and IP telephony protocols.

1 Introduction

In today's rapidly developing world, more and more there is a need for reliable, fast and high-quality communication. The latest information and communication technologies are being created and successfully implemented, which require a high level of training from the personnel. Therefore, along with a good knowledge of the theory, students, of course, are required to have sufficient practical skills in the operation of digital communication networks. At the Irkutsk National Research University (IrNITU) at the Department of Radio Electronics and Telecommunication Systems, a hardware-software complex DIP was developed and a methodology was created for teaching students how to work with Cisco equipment

This article discusses the next stage in the development of the complex - designing multi-layer networks, debugging using Cisco equipment, analyzing network operation using the Wireshark program.

In addition to gaining skills in working with a real multi-layer network, an important task is to analyze the traffic passing through the network.

Among IT and network professionals, the skills to analyze traffic, identify network problems and improve the stability of IP networks are no less in demand than the ability to install and configure its physical elements, such as routers or switches.

Therefore, in addition to developing a methodology for introducing a laboratory stand based on Cisco into training, the task was also to understand the technology of analyzing

* Corresponding author: osipov_k_a@outlook.com

network traffic using available software, and providing the results of the study in the form of practical work for students.

All network equipment emulators can be divided into two main categories:

1. Hardware-implemented emulators;
2. Software-implemented emulators.

The first group includes, as a rule, highly specialized equipment that allows, when real telecommunications equipment is connected to it, to simulate the operation of a real telecommunications network, or some part of it (as a rule, communication channels). In hardware emulators, at the hardware level, the processes that occur in real networks are implemented - the occurrence of delays, packet losses, distortion of transmitted data, etc. events. The main goal of developing and using hardware emulators is to study the operation of real telecommunications equipment in various conditions and with various channel characteristics.

The second group of emulators includes specially designed programs that allow you to simulate the operation of equipment and communication channels, as well as the operation of command interfaces of active network equipment. The main purpose of using software emulators is to use them as a research activity, for setting up scientific experiments. Also, these programs are often used as training systems for training personnel in working with network equipment.

We will use the available Cisco equipment as network equipment:

1. Cisco 1710 router;
2. Cisco 3725 router;
3. Cisco 7200 router;
4. L2 and L3 Catalyst IOS on Linux switches, which means that the switch is software-based and based on the Linux OS, since it is almost impossible to emulate a real switch on a computer due to very large system requirements.

In addition, Cisco IP Communicator and 3CX phone softphones are used in the work.

Let's take a closer look at the most popular emulators that allow you to create multi-level models of data networks, as well as emulate the operation of network equipment.

Cisco Packet Tracer. It is worth starting with the fact that Cisco Packet Tracer is not an emulator, but a simulator, that is, it simulates the operation of software-implemented hardware, which means that it is not identical to the real one. In addition, this simulator imitates only Cisco equipment, that is, it is a highly specialized software package. This simulator was considered earlier in the final qualifying work for the bachelor's degree "Modeling small and medium office networks using Cisco equipment."

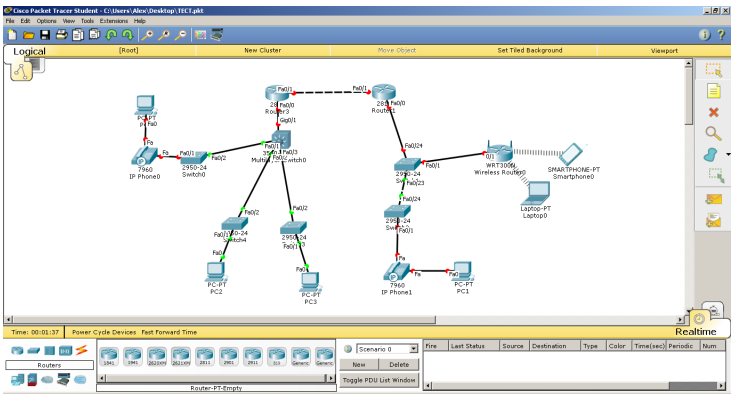

Fig. 1. Cisco Packet Tracer Interface.

Of the advantages of the software product, it is worth noting that the simulator is not demanding on the technical characteristics of the user's personal computer, and is also widely used to prepare and pass the following courses and exams:

1. CCNA R&S program;
2. CCNA Security;
3. Cyber Security Essentials;
4. Introduction to IoT;
5. 5 Introduction to Packet Tracer;
6. IoT Fundamentals;
7. IT Essentials;
8. Mobility Fundamentals;
9. Networking Essentials.

The simulator is well suited to gain basic knowledge of configuring Cisco equipment, and prepare for further training.

The first step is the basic network setup [3], which includes several computers and IP phones. First, the DHCP server is configured on the router, since almost all phones are by default configured to receive an IP address in exactly this way than on personal computers (hereinafter referred to as PCs) - there you need to enable automatic assignment of an IP address via DHCP protocol. Next, the IP telephony service is raised, and the number of base stations and the number of lines are configured, as well as the Telnet protocol is configured for remote control of equipment (Telnet is configured in all laboratory work). When performing this work, it is worth considering that for the IP phone to work correctly, it must be reset to factory settings.

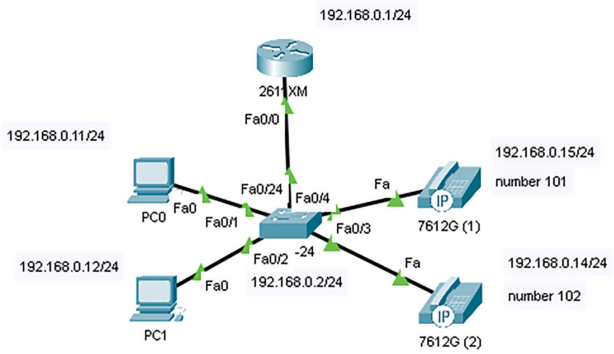

Fig. 2. The simplest network model with IP phones.

Table 1. Hardware configuration.

2611XM Router Configuration		**2950-24 Switch Configuration**
enable secret admin line vty 0 15 transport input telnet login local int fa0/0 no sh ip address 192.168.0.1 255.255.255.0	default-router 192.168.0.1 option 150 ip 192.168.0.1 telephony-service max-ephone 4 max-dn 4 auto assign 1 to 4 ip source-address 192.168.0.1 port 2000 ephone-dn 1 number 101	enable secret admin line vty 0 15 transport input telnet login local int vlan 1 ip address 192.168.0.2 255.255.255.0 no sh int range fa0/1-24 switchport voice vlan 1

ip dhcp excluded-address 192.168.0.1 192.168.0.10 ip dhcp pool Vlan1 network 192.168.0.0 255.255.255.0	ephone-dn 2 number 102	

For normal collaboration of two network layer devices of the OSI model (router and L3 switch), it is necessary to register static routes (ip route).

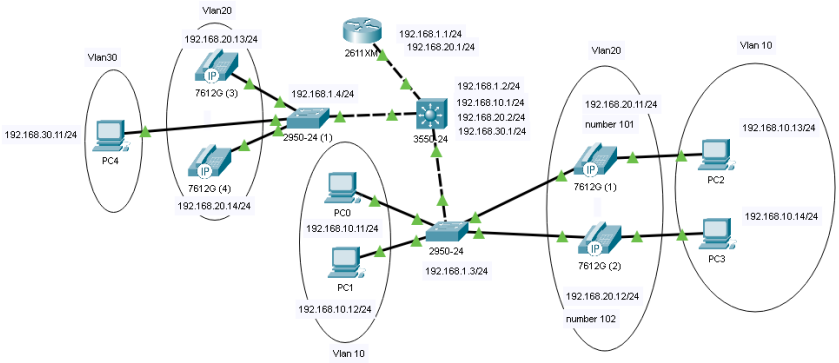

Fig. 3. Three-level network model with Ip-phones.

Table 2. Show run hardware configuration.

2611XM	**3550-24**		**2950-24**	**2950-24(1)**
ip dhcp excluded-address 192.168.20.1 192.168.20.10 ip dhcp pool Voice network 192.168.20.0 255.255.255.0 default-router 192.168.20.1 option 150 ip 192.168.20.1 int Fa0/0.1 encapsulation dot1Q 1 native ip address 192.168.1.1 255.255.255.0 int Fa0/0.20 encapsulation dot1Q 20 ip address 192.168.20.1 255.255.255.0	ip dhcp excluded-address 192.168.10.1 192.168.10.10 ip dhcp excluded-address 192.168.30.1 192.168.30.10 ip dhcp pool Vlan10 network 192.168.10.0 255.255.255.0 default-router 192.168.10.1 ip dhcp pool Vlan30 network 192.168.30.0 255.255.255.0 default-router 192.168.30.1 ip routing int range Fa0/1-2	int Gi0/1 switchport trunk encapsulation dot1q switchport mode trunk interface Vlan1 ip address 192.168.1.2 255.255.255.0 interface Vlan10 ip address 192.168.10.1 255.255.255.0 interface Vlan20 ip address 192.168.20.2 255.255.255.0 interface Vlan30 ip address 192.168.30.1 255.255.255.0	Int range Fa0/1-2 switchport access vlan 10 switchport mode access Int range Fa0/3-4 switchport access vlan 10 switchport mode access switchport voice vlan 20 int Fa0/24 switchport mode trunk interface Vlan1 ip address 192.168.1.3 255.255.255.0 ip default-gateway 192.168.1.2	Int Fa0/1 switchport access vlan 30 switchport mode access int range Fa0/2-3 switchport voice vlan 20 int Fa0/24 switchport mode trunk interface Vlan1 ip address 192.168.1.4 255.255.255.0 ip default-gateway 192.168.1.2

ip route 0.0.0.0 0.0.0.0 192.168.1.2	switchport trunk encapsulation dot1q switchport mode trunk	ip route 0.0.0.0 0.0.0.0 192.168.1.1		

The diagram above is a model of a network located within the same building or office. In practice, networks are connected to other branches, offices and the Internet, in order to bring the created model closer to reality, it is necessary to create a multi-level network.

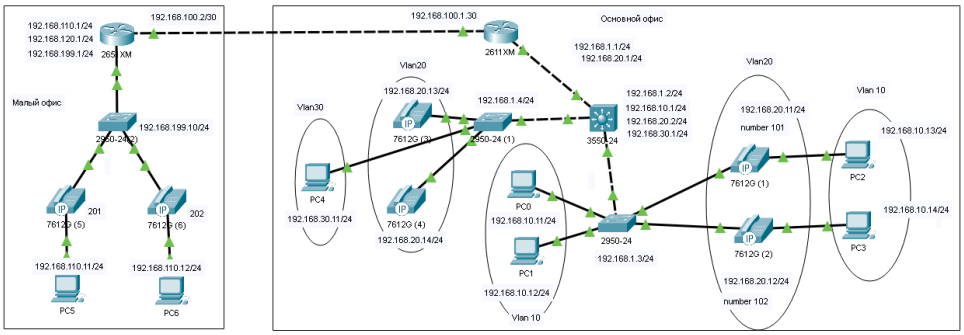

Fig. 4. Network model consisting of two offices.

The small office shown in figure 4 on the left is configured similarly to the scheme shown in figure 2, the difference is only in IP addresses and phone numbers. Also, in order for PCs from different offices to “communicate” with each other, it is necessary to register static routes on routers: ip route 0.0.0.0 0.0.0.0 192.168.100.1 on the 2651XM router and ip route 0.0.0.0 0.0.0.0 192.168 .100.2 on a 2611XM router. But this will not be enough to be able to communicate between offices via IP phones. To do this, you must configure Dialplan on each router.

Table 3. Hardware configuration.

Cisco 2611XM	Cisco 2651XM
dial-peer voice 1 voip destination-pattern 20. session target ipv4:192.168.100.2	dial-peer voice 1 voip destination-pattern 10. session target ipv4:192.168.100.1

GNS3 (Graphical Network Simulator) - literally translated as a graphical network simulator. It's actually a network emulator, not a simulator. The emulator allows you to create a model of a computer or other device and run original software inside. All major components of the device are emulated: processor, memory, and I/O devices. The simulator, on the other hand, simulates the behavior of the system and its interfaces, without using original software images (for example, Cisco Packet Tracer).

This software package makes it possible to emulate various network topologies without real hardware, using only the original software image, on a personal personal computer. GNS3 is a full-fledged laboratory stand for the practical study of communication networks.

Main advantages of GNS3 over other emulators/simulators:

1. Full functionality of emulated devices;
2. Ability to build heterogeneous networks;

3. Adding real workstations, servers or real local networks to the topology of networks;
4. Free.

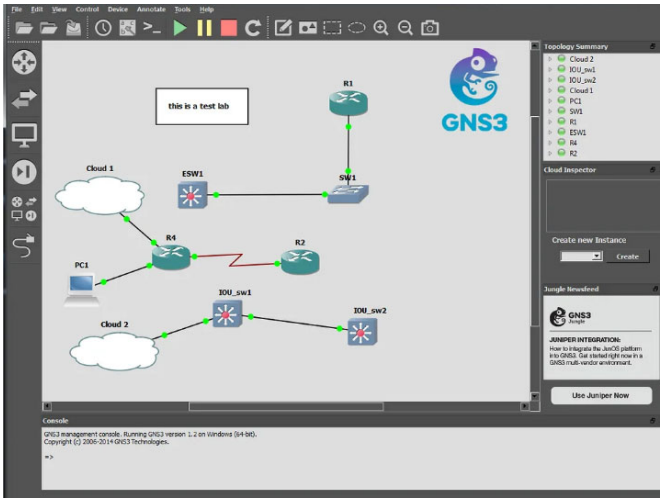

Fig. 5. GNS3 program interface

The disadvantage of the program is the inability to emulate D-link devices, but thanks to the ability of the program to connect to real devices, networks and even the Internet, we will only emulate routers from Cisco. This will bring our model as close as possible to real network topologies, because such separation of brands often occurs due to price differences. it is generally necessary to put a large number of switches at the access level, increasing the capacity of the ports, and not everyone can afford these switches to be Cisco.

EVE-NG (Emulated Virtual Environment - Next Generation) is a network emulator, which is a multi-user platform for modeling and creating virtual networks, various laboratories, supporting an impressive list of telecommunications equipment. Thus, the conceptual novelty of the EVE-NG software product is the ability to run and use the program between different platforms and different device manufacturers. An example of a graphical interface is shown in Figure5.

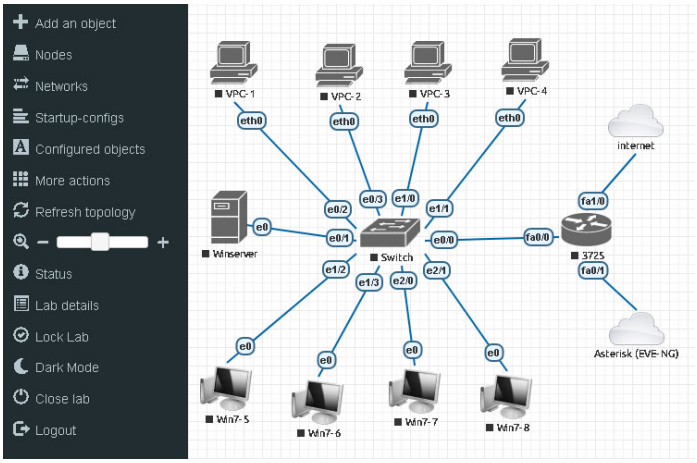

Fig. 6. EVE-NG program interface.

Currently, the EVE-NG emulator is also used as a tool for preparing and passing exams for various Cisco certifications. It is used not only by beginners to prepare for CCNA / CCNP, but also by professionals for preparing and passing CCIE Routing and Switching, CCIE Security. In addition to modeling, EVE-NG is used in network engineering, as well as for a systematic approach in identifying and eliminating the causes of network problems (troubleshooting). [1,2]

EVE-NG is a fork of the famous UNetLab that is no longer maintained or developed. UNetLab was launched in 2014 and at the stage of its existence was a serious competitor for GNS3 and Cisco Packet Tracer emulators, having a huge number of advantages in its arsenal. The new EVE-NG project for 2022 is far superior to all of them, product development is ongoing, bugs are being identified and various updates are being released to expand the functionality of the program and the list of supported devices.

Using EVE-NG allows you to move away from the traditional approach of using stand-alone virtual machines to emulate various network devices, and create digital or WEB labs based on software emulators QEMU, IOU / IOL, Dynamips and Docker, combining all the necessary modules within one platform.

The UNetLab project was completely free, which is not the case with EVE-NG. The project is divided into two versions:

1. Community - completely free, the number of concurrent users is 63, no internal chat, the inability to use Docker;
2. Professional - paid, the number of concurrent users is 1024, built-in Docker, internal chat, various roles for users, etc.

As part of this work, to demonstrate all the advantages of this emulator, it is quite enough to use the free version, since this does not affect the modeling of data networks and their analysis in any way.

Of the advantages, it is also worth mentioning that this emulator is deployed on the Ubuntu operating system, which provides a number of advantages, for example, OS security, as well as the ability to independently modify the emulator by adding new modules, such as the Asterisk virtual PBX.

Based on a general comparative analysis of network equipment emulator software platforms, EVE-NG and GNS3 can be singled out as the most relevant and effective. It should be noted that EVE-NG has a number of technical advantages compared to GNS3, with the help of which an increase in functionality is achieved and, as a result, an expansion of the portfolio of services in the field of network design. A comparative analysis of the functional characteristics of the EVE-NG and GNS3 network equipment emulator platforms is given in Table 4. [4-6]

Table 4. Comparative analysis of the functional characteristics of platforms.

Characteristic	EVE-NG	GNS3
GUI	A convenient single graphical user interface based on WEB technology is automatically installed with the platform.	The graphical user interface in the form of a specialized platform client is installed by the user on a PC and is separate from the platform.
Specialized software	No need for separate clients to use the platform	Requires installation of a specialized client for subsequent use of the platform
Functionality	Full support for channel and network emulation (L2 and L3) without restrictions	Partial support for channel and network emulation (L2 and L3)
Multiplayer mode	Multi-user functionality, the ability to work with several users at the same time	Strictly single user system

RAM	No RAM limits for emulating QEMU devices	QEMU supports up to 2 GB of RAM
Number of connections	No limit on the number of connections between devices in QEMU virtualization conditions	Limitation of 16 connections between devices within QEMU virtualization
Scalability	Images run and run within the same virtual machine or physical server	The need to create a separate virtual machine to run images in GNS3
Native symbol support	The user interface provides native support for custom symbols	Support for organizing device eigenvalues is partially present

Based on the presented analysis of the EVE-NG and GNS3 software products, the EVE-NG emulator has clear advantages, and that is why it was chosen as the emulator.

As mentioned earlier [3], there are many software products for this type of activity in the IT industry market and on the Internet. The choice fell on Wireshark, since the program is absolutely free, constantly updated and has integration with most emulators that act as laboratory stands. In addition, this program is easily integrated into the popular Windows operating system, and can also be used on real hardware. It is for these reasons that the software traffic analyzer Wireshark was chosen.

Wireshark is a program designed to capture and analyze network traffic, an indispensable thing for education and troubleshooting (troubleshooting - troubleshooting, working on a problem), that is, finding problems on the network.

Wireshark provides a real-time view of all passing network traffic.

At the same time, Wireshar understands most modern protocols and allows you to parse network packets by displaying the values of each field.

The main advantages of Wireshark:

Has a graphical interface, available for most operating systems: UNIX-like systems, including GNU / Linux, Solaris, FreeBSD, NetBSD, OpenBSD, macOS, and Windows.

Wireshark is completely free, and it also integrates with EVE-NG, which we work with in this work, and allows you to capture packets anywhere in the virtual network, which is very convenient. It is for these reasons that this particular product is used.

Wireshark is one of the must-have software among serious networking professionals and helps to understand various network protocols and network related issues. In addition, knowledge of all of the above will help in successfully passing various certification exams for various "giants" of the network industry, such as:

1. Cisco certification (CCNA, CCNP, CCDP, CCIP);
2. Huawei certification (HCIE);
3. Mikrotik certification (MTCNA);
4. Juniper certification (JNCIA), etc.

When doing practical work, students will get acquainted with the interface of the Wireshark program, as well as the study of network state protocol traffic, such as ICMP, STP, CDP, LOOP. In addition, based on basic examples, the traffic of the DHCP, ARP, Telnet, SSH protocols will be studied.

When creating a model, you need to assemble a fairly simple scheme using the built-in VPCS virtual computers, an L2 switch and any two routers, and run it:

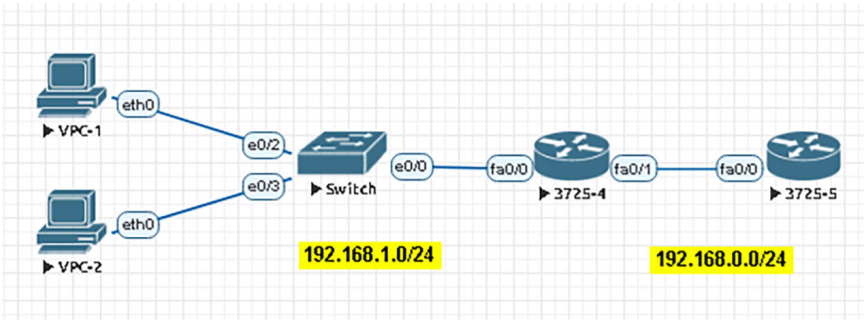

Fig. 7. The simplest circuit.

As an experiment, let's set the IP address to the "fa0/0" port on the "3725-4" router, and try to remove traffic from it. To do this, right-click on it, then "capture" and select the appropriate port.

As noted in the previous section, if Wireshark gives an error when starting, you need to log into the EVE-NG server through any terminal client using the SSH protocol in order for the security key to be generated and received.

After Wireshark has been launched, you can see that the program is already monitoring some protocols, although the network is not configured and there is no network activity yet:

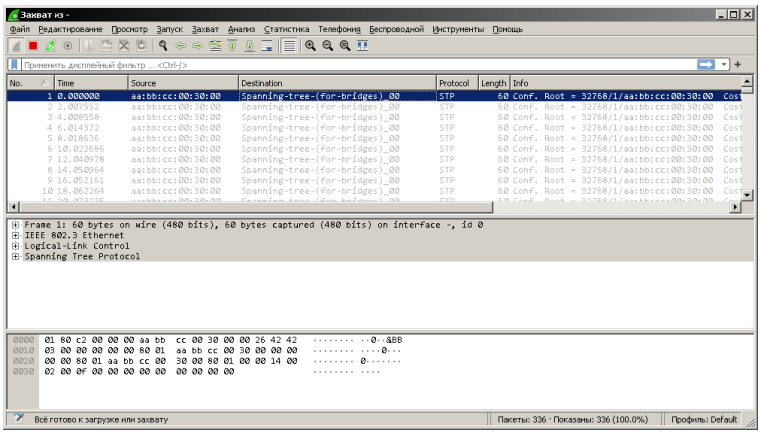

Fig. 8. Screenshot of the Wireshark interface.

As you can see in the figure above, the Wireshark program window is divided into 3 segments:

1. Filtering line: in it you can set a specific filter by which to display packages;
2. Table showing all captured packets in real time;
3. Package details - all information about the selected package. Here the package is decomposed into the levels of the OSI model;
4. The raw data of the package, i.e. in the form in which the packet is transmitted over the network.

The table of captured packets is in turn divided into the following columns:

1. Package number;
2. Capture time;
3. Mac address of the source of the package "source";
4. The destination of the package "destination";

5. Protocol;
6. Message length;
7. Information.

STP and CDP protocol. The protocol highlighted in the figure above is called the Spanning-tree Protocol (STP), a spanning tree protocol that is enabled by default on all Cisco devices to avoid loops in the network topology.

In addition to the STP protocol, you can also see the CDP protocol:

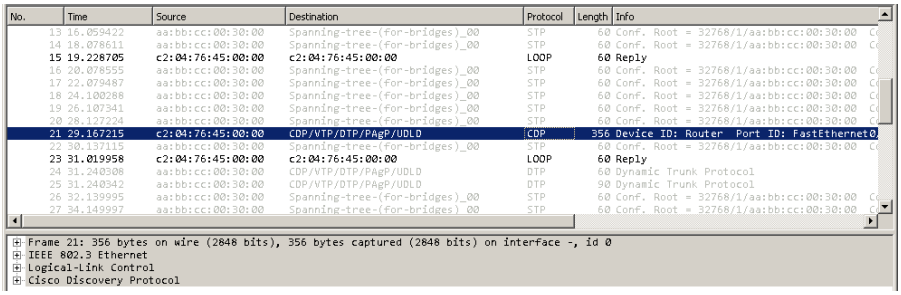

Fig. 9. CDP Protocol Packet.

CDP (Cisco Discovery Protocol) is a Cisco proprietary protocol used to discover neighboring devices such as switches and routers. Let's consider it in more detail:

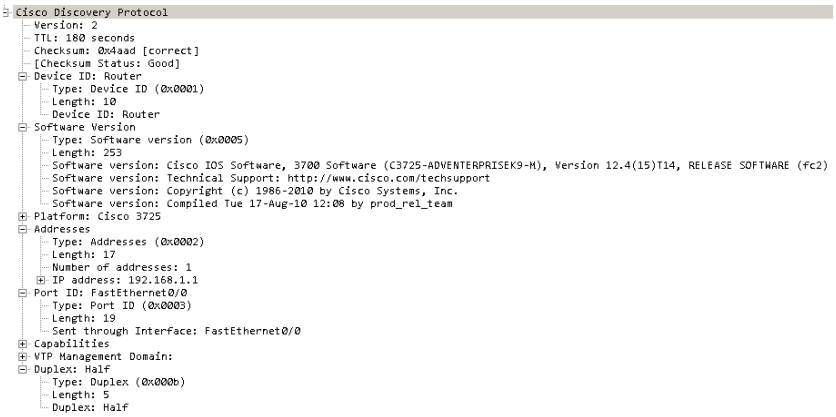

Fig. 10. Structure of the sent CDP packet.

As you can see in the screenshot above, there is a lot of information about this protocol presented here. This packet was sent from the router, so here you can see all the information about it:

1. Protocol version: 2;
2. Device ID: router – router device type;
3. Software version: c3750-Adventerprisek9-M, ver. 12.4(15)T14;
4. Platform: Cisco 3725;
5. IP address of the interface from which we remove traffic;
6. Port ID: port number;
7. Physical port settings: half-duplex, which corresponds to the port speed from 10 to 100Mbps.

In addition to CDP packets that are sent by the router, there are CDP packets received that carry all the same information, only from a neighboring device:

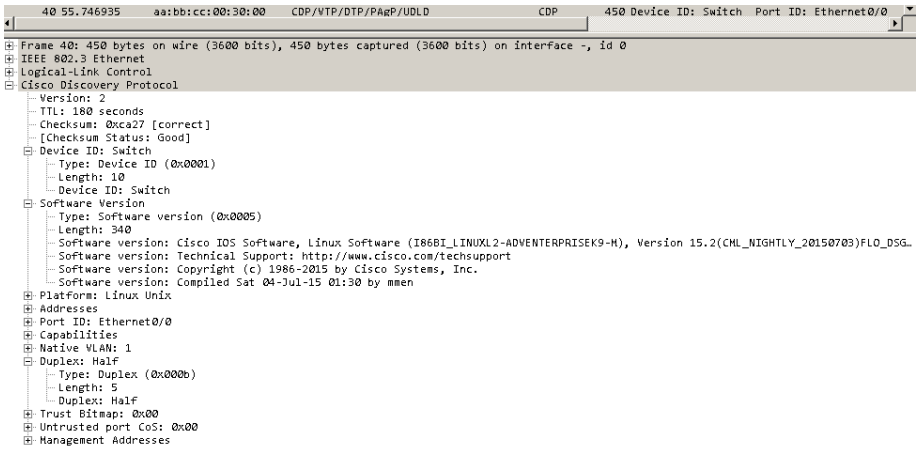

Fig. 11. Structure of the received CDP packet.

In this case, it is the "Device ID: Switch" switch. In addition to the data described above, data about the Native VLAN: 1 virtual interface also comes from the switch.

loop protocol. You can also see packages called "Loop":

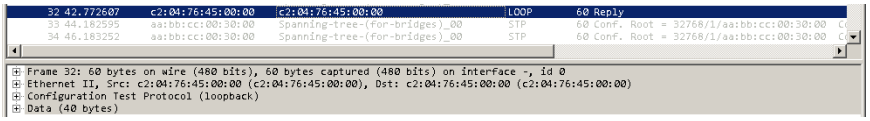

Fig. 12. Package "Loop".

As you can see in the screenshot above, this protocol is called "Configuration Test Protocol (loopback)". This is a built-in protocol, and it runs on the default hardware. Every 10 seconds, “keepalive” frames (frame) are sent to the Ethernet interfaces, they are necessary to evaluate the health of the “link”, as well as provide additional protection against loops, in addition to STP. This protocol can be compared with the ICMP "Ping" protocol - only "ping" works at the 3rd layer of the OSI model, and "keepalive" at the second.

Next, we will consider, using the example of the same scheme shown in Figure 6, such a protocol as DHCP.

Dynamic Host Configuration Protocol (hereinafter referred to as DHCP) is a dynamic host configuration protocol that allows devices connected to a network to automatically obtain an IP address and, if necessary, other parameters to operate on a TCP/IP network. This is justified in cases where the computer and the user often change places, physically and logically. Each time you connect to the network, the device will automatically obtain an IP address and netmask. Thus, the use of the DHCP protocol greatly simplifies the assignment of IP addresses to various devices, and the administration of all assigned addresses from one server. This protocol is configured on the device of the third network layer of the OSI model - a router (in some cases, on a third-layer switch).

You need to request an IP address from the virtual computer via DHCP:

```
VPCS> ip dhcp
DDD
Can't find dhcp server

VPCS>
```

Fig. 13. Requesting a VPC Address via DHCP.

The virtual machine could not find a DHCP server. Let's see what packets were currently captured in the Wireshark program:

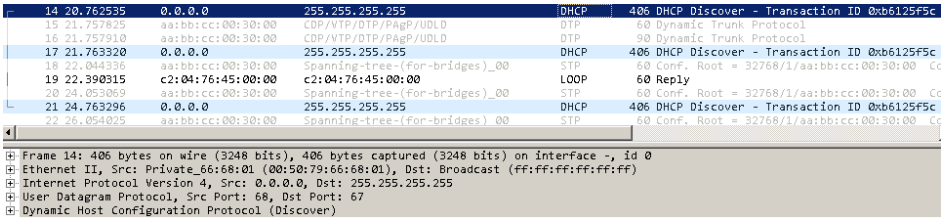

Fig. 14. DHCP Discover Packet.

As you can see, the router received three DHCP Discover packets. The source is "0.0.0.0" because the virtual machine does not yet have an IP address, and the destination is specified with a broadcast request of "255.255.255.255". All three packages have the same transaction number, which is listed in the package information column.

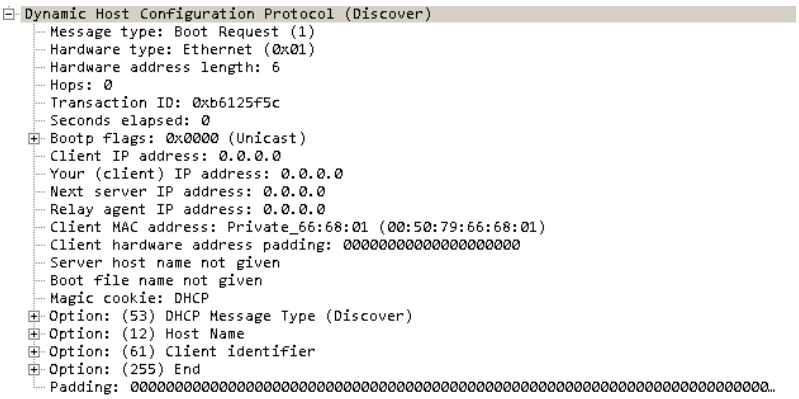

Fig. 15. DHCP Discover Structure.

If you expand the details about this package, the same transaction number can also be seen here "Transaction ID". This number is needed so that the router can distinguish and recognize different requests from different devices. In addition, here you can see the MAC address of the source device.

No other DHCP packets are visible because DHCP is not configured on the router. Need to fix this:

- Router(config)#ip dhcp pool TEST
- Router(dhcp-config)#network 192.168.1.0 255.255.255.0
- Router(dhcp-config)#default-router 192.168.1.1
- Router(dhcp-config)#dns-server 8.8.8.8
- Router(dhcp-config)#exit
- Router(config)#service dhcp

After that, you need to request IP again on the virtual machine via DHCP and see what will be displayed in Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
612	932.574416	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x92474307
613	932.603201	c2:04:76:45:00:00	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
614	932.695762	aa:bb:cc:00:30:00	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:30:00 Cost
615	933.574473	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x92474307
616	934.154752	192.168.1.1	192.168.1.2	DHCP	342	DHCP Offer - Transaction ID 0x92474307
617	934.169522	192.168.1.1	192.168.1.2	DHCP	342	DHCP Offer - Transaction ID 0x92474307
618	934.604080	aa:bb:cc:00:30:00	CDP/VTP/DTP/PAgP/UDLD	CDP	450	Device ID: Switch Port ID: Ethernet0/0
619	934.699444	aa:bb:cc:00:30:00	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:30:00 Cost
620	936.578857	0.0.0.0	255.255.255.255	DHCP	406	DHCP Request - Transaction ID 0x92474307
621	936.588144	192.168.1.1	192.168.1.2	DHCP	342	DHCP ACK - Transaction ID 0x92474307
622	936.703775	aa:bb:cc:00:30:00	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:30:00 Cost
623	937.582136	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.2 (Request)
624	938.165390	c2:04:76:45:00:00	c2:04:76:45:00:00	LOOP	60	Reply
625	938.583150	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.2 (Request)
626	938.705092	aa:bb:cc:00:30:00	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/aa:bb:cc:00:30:00 Cost
627	939.584251	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.2 (Request)

Fig. 16. DHCP packets in Wireshark.

In addition to DHCP, the ARP protocol is present here. Address Resolution Protocol - address determination protocol, that is, this protocol compares the MAC addresses of devices with their IP addresses, and writes a table to the ARP.

```
Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x92474307
    Seconds elapsed: 0
  + Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.2
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Private_66:68:01 (00:50:79:66:68:01)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  + Option: (53) DHCP Message Type (Offer)
  - Option: (54) DHCP Server Identifier (192.168.1.1)
        Length: 4
        DHCP Server Identifier: 192.168.1.1
  - Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (86400s) 1 day
  + Option: (58) Renewal Time Value
  + Option: (59) Rebinding Time Value
  + Option: (1) Subnet Mask (255.255.255.0)
  - Option: (3) Router
        Length: 4
        Router: 192.168.1.1
  - Option: (6) Domain Name Server
        Length: 4
        Domain Name Server: 8.8.8.8
```

Fig. 17. DHCP Offer Structure.

Let's consider in detail what happened during the request for an IP address via DHCP between the computer and the router:

1. The computer sent "DHCP Discover" looking for a DHCP server;
2. At this point, the router sent a broadcast request asking “who is 192.168.1.2? reply to 192.168.1.1" via ARP. Thus, the DHCP server polls the entire network until it finds the first free IP address;
3. The DHCP server responds to the "DHCP Offer" virtual machine within the same transaction. This packet contains the router, the "lease" time of the IP address, the IP address itself, the netmask, the DNS server:

1. Further, according to the rules of the DHCP protocol, the computer responds to the router with a “DHCP Request”, in which it “says” that the IP address “suits” it;

2. The last confirmation packet "DHCP ACK", which contains information that the computer has assigned itself an IP address, mask, default gateway and DNS from the DHCP server for 24 hours;
3. The virtual computer sends a broadcast packet via the ARP protocol that the address 192.168.1.2 is occupied by it.

If you request an IP address via DHCP from the second virtual computer, the same thing will happen: only the transaction number and IP address will differ:

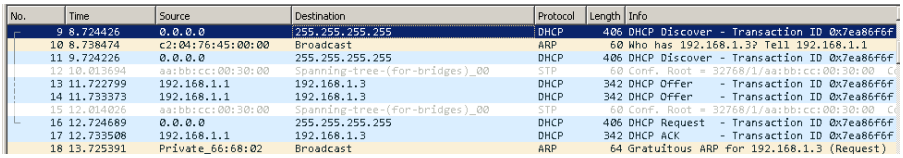

Fig. 18. Package transaction numbers.

Thus, using the Wireshark program together with the EVE-NG emulator and CISCO equipment will allow students not only to gain practical skills in designing and operating modern digital communication systems, but also learn how to analyze network traffic.

For convenience, the structure of the Cisco booth is made in accordance with the hierarchy of a real network: the lower the equipment is in the telecommunications rack, the lower the level of equipment. At the core level (topmost) are the IBM server and routers; at the distribution level there are two L3 Cisco 3550-24 switches; and at the access level four Cisco 2950-24 L2 switches.

Before students are allowed to work with real equipment, they must acquire a basic knowledge of setting up equipment. That is why, at first, students perform work, build network models and configure them in the Cisco Packet Tracer software package (hereinafter referred to as CPT). And only after receiving a workable model, students can implement it on a laboratory bench.

The disadvantages of GNS3 include high system requirements (at least 4 gigabytes of RAM is required), on which network devices will be emulated. For the same reason, there is no possibility to emulate switches - the program contains limited simulators, which are enough to gain basic knowledge.

Practical work compiled on the basis of the results of network traffic research will allow students to gain the necessary initial skills in the field of traffic analysis and further management of the main elements of an information transmission network. Get skills in working with a real multi-layer network using Cisco equipment, network analysis using the Wireshark program.

References

1. Brian Hill, *The Complete Guide to CISCO* (Sebastopol, McGraw-Hill Osborne Media, 2002)
2. A.A. Dmitriev, M.V. Ivanova, L.B. Prosviryakova, J. Phys.: Conf. Ser. **1691** 012035 **(**2020**)**
3. K.A. Osipov, A.A. Dmitriev, L.B. Prosviryakova, AIP Conference Proceedings **2647** 040052 (2022). https://doi.org/10.1063/5.0105250
4. V.A. Salnikov, L.V. Prosviryakova, Methodological issues of teaching information communication in higher education **9**, 18-24 (2020)
5. A. Leinvand, *Configuring Cisco Routers* (San-Jose, Cisco systems, 2001)
6. K. Packet, *Creation of networks of remote access Cisco* (San-Jose, Cisco systems, 2003)