

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION
FEDERAL STATE AUTONOMOUS EDUCATIONAL
INSTITUTION OF HIGHER EDUCATION
"NORTH CAUCASUS FEDERAL UNIVERSITY"

SUGGESTIONS FOR TEACHING

for the performance of practical work
in the discipline "Personal cybersecurity"
for students of the field of study

11.03.02 Infocommunication Technologies and Communication Systems
Profile

"Intelligent Data Processing in Infocommunication Systems and Networks"

LessonNo 1.

Creation of the cyber world

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Be able to configure the basic components of the server.
3. Acquire skills in deploying FTP, email, DNS, NTP, AAA, and web services on multiple servers.
4. To acquire the skills of analysis and generalization of the results obtained.

Educational issues of the lesson

1. Setting up an FTP server
2. Setting up a web server
3. Setting up an email server
4. Setting up a DNS server
5. Configuring the NTP Server
6. Setting up an AAA server

Equipment and materials

PC with Packet Tracer installed

Overview/scenario

In this job, you will configure the basic components of the server. Configure IP to match the addressing table. Use the Services tab to deploy FTP, e-mail, DNS, NTP, AAA, and Web services to multiple servers.

Addressing Table

Device	IP address	Subnet mask	Website
Сервер FTP/Web	10.44.1.254	255.255.255.0	Metropolis Bank HQ
Сервер Email/DNS	10.44.1.253	255.255.255.0	Metropolis Bank HQ
Сервер NTP/AAA	10.44.1.252	255.255.255.0	Metropolis Bank HQ
File Backup Server	10.44.2.254	255.255.255.0	Gotham Healthcare Branch

Учебный вопрос 1: Setting up an FTP server

Шаг 1: Activate the FTP service.

- a. Open the Metropolis Bank HQ object and select the FTP/Web server.
- b. Go to the Services tab and select the FTP section.
- c. Enable the FTP service using the selective button at the top of the window.

Шаг 2: Give users access to the FTP server.

- a. Create user accounts named bob, mary, and mike, and assign a cisco123 password to each.
- b. Each account must have full permissions (RWDNL) to access the FTP/Web server.

Учебный вопрос 2: Configuring a Web Server

Шаг 1: Activate the HTTP service.

- a. Open the Metropolis Bank HQ object and select the FTP/Web server.

- b. Go to the Services tab and select HTTP.
- a. Enable HTTP and HTTPS services using the selective buttons at the top of the window.

Шаг 2: HTTP service health check.

- a. Select the computer named "Sally" and click the Desktop tab.
- b. Click the Web Browser icon. Go to www.cisco.corp.
- c. Using a web browser, go to the IP address 10.44.1.254.

For example, suppose an IP address fails correctly, but you can't fail over using a fully qualified domain name. What could be the reason?

Учебный вопрос 3: Setting up a DNS server

Шаг 1: Activate the DNS service.

- a. Open the Metropolis Bank HQ object and select the Email/DNS server.
- b. Go to the Services tab and select DNS.
- c. Enable the DNS service using the selective button at the top of the window.

Шаг 2: Create DNS A records.

- a. Create a record A email.cisco.corp with an IP address of 10.44.1.253. Click Add to save the record.
- b. Create an A record of www.cisco.corp with an IP address of 10.44.1.254. Click Add to save the record.

Шаг 3: Check the health of the DNS service.

- a. Select the computer named "Sally" and click the Desktop tab.
- b. Click the Web Browser icon. Go to www.cisco.corp.

Why does a user successfully navigate to the specified fully qualified domain name?

Учебный вопрос 4: Setting up an email server

Шаг 1: Activation of email services.

- a. Open the Metropolis Bank HQ object and select the Email/DNS server.
- b. Go to the Services tab and select the EMAIL section.
- c. Enable SMTP and POP3 services using the selective buttons at the top of the window.

Шаг 2: Create email accounts for your users.

- a. Create a cisco.corp. domain name.
- b. Create user accounts named phil, sally, bob, dave, mary, tim, and mike, assigning each account a cisco123 password.

Шаг 3: Set up custom email clients.

- a. Select the computer named Sally and click the Desktop tab.
 - b. Click the Email icon and enter the following information:
Name: Sally
Email Address: sally@cisco.corp
Incoming&OutgoingEmailServer(s): email.cisco.corp
Username: sally
Password: cisco123
 - c. Repeat step 3b on the computer named Bob, replacing the name sally with bob.
Why do I need to activate SMTP and POP3 services at the same time for my email service to work?
-
-

Учебный вопрос 5: Configuring an NTP Server

Шаг 1: Activate the NTP service.

- a. Open the Metropolis Bank HQ object and select the NTP/AAA server.
- b. Go to the Services tab and select NTP.
- c. Enable the NTP service using the selective button at the top of the window.

Шаг 2: Protect the NTP service.

- a. Enable the NTP authentication function using the appropriate selective button.
- b. Assign the cisco123 password to Key 1.

Учебный вопрос 6: Configuring an AAA Server

Шаг 1: Activate the AAA service.

- a. Open the Metropolis Bank HQ object and select the NTP/AAA server.
- b. Go to the Services tab and select AAA.
- c. Enable the AAA service using the selective button at the top of the window.

Шаг 2: AAA network configuration.

- a. Enter the Client Name HQ_Router, the Client IP address 10.44.1.1, and the password cisco123. Click Add to save the client settings.
- b. Set up an AAA admin user account with a cisco123 password. Click Add to save the user information.

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 2. Setting up a web server	Step 2	2	
Question 3. Setting up a DNS server	Step 3	2	
Question 4. Setting up an email server	Step 3	2	
Questions		6	
Packet Tracer Score		94	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. Let's assume that the IP address fails correctly, but you cannot fail over using the FQDN. What could be the reason?
2. Why does the user successfully navigate to the specified fully qualified domain name?
3. Why do I need to activate SMTP and POP3 services at the same time for my email service to work?

LessonNo 2.

Communication in cyber world

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Be able to transmit electronic messages from user to user.
3. Acquire skills in uploading files to / from the server via FTP protocol.
4. Be able to remotely access the router of the corporate network using the Telnet protocol.
5. Be able to remotely access the router of the corporate network using the SSH protocol.
6. To acquire the skills of analysis and generalization of the results obtained.

Educational issues of the lesson

1. Transfer of electronic messages from user to user.
2. Uploading files to/from the server via FTP.
3. Remote access to the router of the corporate network via the Telnet protocol.
4. Remote access to the router of the corporate network via SSH.

Equipment and materials

PC with Packet Tracer installed

General information

By completing this task, you will enable communication over remote networks using shared network services. Configure IP addressing, networking, and services according to the addressing table. You will use client devices that are located in different geographic regions. From these devices, you will connect to other client devices and servers.

Addressing Table

Device	Private IP address	Public IP address	Subnet mask	Website
Сервер FTP/Web	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Сервер Email/DNS	10.44.1.253	209.165.201.4	255.255.255.0	Metropolis Bank HQ
Сервер NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ
File Backup Server	10.44.2.254	—	255.255.255.0	Gotham Healthcare Branch

Учебный вопрос 1: User-to-user e-mail transmission

Шаг 1: Open the email client on the Mike user's computer.

- a. Open the Gotham Healthcare Branch object and select the computer named Mike.
- b. Click the Desktop tab and click the Email icon.

Шаг 2: Send an email to a Sally user.

- a. Click the Compose button to create an e-mail message.
- b. In the To: field, enter the address.

In the Subject: field, enter the text "Urgent- Call me".

In the Message box, type the following text: "Call me when you are free today to discuss the new sale."

- c. Click the Send button to send the email.

What protocol was used to send the email to the email server?

Шар 3: Sally user mail verification.

- a. Open the Metropolis Bank HQ object and select the computer named Sally.
- b. Click the Desktop tab and click the Email icon.
- c. Click the Receive button to receive an email sent by Mike.

What protocol was used to receive the email from the e-mail server?

Учебный вопрос 2: Uploading files to the server via FTP

Шар 1: Configuring the packet sniffer to intercept traffic on the appropriate port.

- b. Zoom to the geographic (root) view to view all three deleted features.
- c. Select the Cyber Criminals Sniffer traffic analyzer.
- d. Select Port1 to capture packets on that port.
- e. Leave the Cyber Criminals Sniffer traffic analyzer open and visible until the end of this part of the job.

Шар 2: Remote connection to an FTP server.

- a. Open the Healthcare at Home object and select the computer named Mary.
- b. Click the Desktop tab and click the Command Prompt icon.
- c. Connect to the FTP/Web server of the Metropolis Bank HQ object. To do this, enter the ftp command 209.165.201.3 at the command prompt.
- d. Enter your mary username and cisco123 password.

Шар 3: Upload the file to an FTP server.

- d. At the ftp prompt prompt> type the dir command to view a list of files stored on the remote FTP server.
- e. A Mary user has a file with confidential information about new customers of a medical institution. Upload the newclients.txt file to an FTP server. To do this, enter the put newclients.txt command.
- f. At the ftp prompt prompt> type the dir command to verify that the file is newclients.txt now on the FTP server.

Why is FTP upload considered an insecure way to transfer files?

Шар 4: FTP traffic analysis.

- a. Zoom to the geographic (root) view to view all three deleted features.
- b. Select the Cyber Criminals Sniffer traffic analyzer.
- c. On the GUI (Graphical Interface) tab on the left, select the first available FTP package. After that, scroll down the contents of the window displayed on the right.

What information from the FTP header is displayed in plaintext?

- d. On the left, select the second available FTP package. After that, completely scroll down the contents of the window displayed on the right. Repeat the same steps with the third FTP package.
 - e. What sensitive information from the FTP header (other than the username) is displayed in plain text?
-

Учебный вопрос 3: Telnet remote access to the corporate network router

Шаг 1: Connect remotely to the corporate network router.

- d. Open the Healthcare at Home object and select the computer named Dave.
- e. Click the Desktop tab and click the Command Prompt icon.
- f. Ping the router on the corporate network to verify that the router is connected. To do this, enter the ping command 209.165.201.2.
- g. Use the telnet command 209.165.201.2 to establish a Telnet connection to the router on the corporate network that is assigned the specified IP address.
- h. Authenticate to the corporate network router using the admin username and cisco123 password.
- i. Enter the show users command to display information about the active Telnet connection to the corporate network router.

Why is Telnet considered an insecure remote device management tool?

Учебный вопрос 4: Remote SSH access to the corporate network router

Шаг 1: Connect remotely to the corporate network router.

- a. Open the Gotham Healthcare Branch object and select the computer named Tim.
- b. Click the Desktop tab and click the Command Prompt icon.
- c. Ping the router on the corporate network to verify that the router is connected. To do this, enter the ping command 209.165.201.2.
- d. Use the ssh -l admin 209.165.201.2 command to SSH to the router on the corporate network that is assigned the specified IP address.
- e. Authenticate to the router on the corporate network using the cisco123 password.
- f. Enter the show users command to display information about an active SSH connection to the corporate network router.

Why is SSH considered a secure tool for remote device management?

- g. Switch to the global configuration mode. To do this, enter the configure terminal command.
- h. Use the enable secret command to create a Cisco password. To do this, enter the enable secret cisco command.

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 1. Transmission of electronic messages from user to user	Step 2	2	
	Step 3	2	
Question 2. Uploading files to/from the server via FTP	Step 2	2	
	Step 3d	2	
	Step 3e	2	
Question 3. Remote access to the corporate network router via the Telnet protocol	Step 1	2	
Question 4. Remote access to the corporate network router via SSH protocol	Step 1	2	
Questions		14	
Packet Tracer Score		86	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. What protocol is used to send an email to the email server?
2. What protocol is used to receive an email from an email server?
3. Why is FTP upload considered an insecure way to transfer files?
4. What information from the FTP header is displayed in plaintext?
5. What sensitive information from the FTP header (other than the username) is displayed in plain text?
6. Why is SSH considered a secure tool for remote device management?

LessonNo 3.

Encrypt files and data

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Be able to search for FTP account details.
3. Be able to upload confidential data to the server via the FTP protocol.
4. Be able to upload confidential data to the server via the FTP protocol.
5. Acquire the skills to decrypt the contents of a file.
6. To acquire the skills of analysis and generalization of the results obtained.

Educational issues of the lesson

1. Find FTP account details for Mary's laptop.
2. Uploading confidential data to the server via the FTP protocol.
3. Find FTP account details for Bob's computer.
4. Downloading confidential data from the server via the FTP protocol.
5. Decryption of the contents of the clientinfo.txt file.

Equipment and materials

A PC with Packet Tracer installed.

General information

In this task, you will access the encrypted contents of several files and transfer the file over the Internet to a central FTP server. Then, another user will download the file from the FTP server and decrypt the contents of the file. Configure IP addressing, network, and services according to the addressing table. Using client devices that are located in different geographical regions, you will transfer a file with encrypted data from one device to another.

Addressing Table

Device	Private IP address	Public IP address	Subnet mask	Website
Сервер FTP/Web	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Mary	10.44.3.101	—	255.255.255.0	Healthcare at Home
Bob	10.44.1.3	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Find FTP Account Data for Mary Laptop

Шаг 1: Accessing a text document on Mary's laptop.

- a. Open the Healthcare at Home facility and select your Mary laptop.
- b. Click the Desktop tab and click the Text Editor icon.
- c. In the Text Editor window, select the File >Open menu options.
- d. Select the ftplogin.txt document, and then click OK.

Шаг 2: Decryption of Mary's FTP account details.

- a. Select all the text contained in the ftplogin.txt file and copy it.
- b. Open a web browser on your personal computer and go to the website.
- c. Place your cursor in the white box that is on the right side of the website and paste the ciphertext.

To decrypt the text, click the Decipher It button and enter the decryption password maryftp123. Click Decrypt.

What credentials (username and password) correspond to Mary's FTP account?

Учебный вопрос 2: Uploading confidential data to the server via FTP

Шаг 1: View a confidential document on Mary's laptop.

- a. Open the Healthcare at Home facility and select your Mary laptop.
- b. Click the Desktop tab and click the Text Editor icon.
- c. In the Text Editor window, select the File >Open menu options.
- d. Select the clientinfo.txt document, and then click OK.

In what form is the data presented?

Шаг 2: Remote connection to an FTP server.

- a. Open the Healthcare at Home facility and select your Mary laptop.
- b. Click the Desktop tab and click the Command Prompt icon.
- c. Connect to the FTP/Web server of the Metropolis Bank HQ object. To do this, enter the ftp command 209.165.201.3 at the command prompt.
- d. Enter the username and password found in Step 2 in Part 1.

Шаг 3: Upload the file to an FTP server.

- a. At the ftp prompt prompt> type the dir command to view a list of files stored on the remote FTP server.
- b. The user Mary has a file with encrypted information about the clients of a medical institution. Upload the file clientinfo.txt to an FTP server. To do this, enter the put clientinfo.txt command.
- c. At the ftp prompt prompt> type the dir command to verify that the file is clientinfo.txt on an FTP server.

If cybercriminals intercept a file while it is being transmitted over the Internet, what information can they obtain in plaintext?

Учебный вопрос 3: Find FTP account information for Bob's computer

Шаг 1: Accessing a text document on Bob's computer.

- a. Open the Metropolis Bank HQ object and select Bob's computer.
- b. Click the Desktop tab and click the Text Editor icon.
- c. In the Text Editor window, select the File >Open menu options.
- d. Select the ftplogin.txt document, and then click OK.

Шаг 2: Decryption of Bob's FTP account data.

- a. Select all the text contained in the ftplogin.txt file and copy it.
- b. Open a web browser on your personal computer and go to the website.
- c. Place your cursor in the white box that is on the right side of the website and paste the ciphertext.

- d. To decrypt the text, click the Decipher It button and enter the decryption password bobftp123. Click Decrypt.

What credentials (username and password) correspond to Bob's FTP account?

Учебный вопрос 4: Downloading confidential data from the server via FTP

Шаг 1: Remote connection to an FTP server.

- a. Open the Metropolis Bank HQ object and select Bob's computer.
- b. Click the Desktop tab and click the Command Prompt icon.
- c. Connect to the FTP/Web server of the Metropolis Bank HQ object. To do this, enter the ftp command 10.44.1.254 at the command prompt.
- d. Enter the username and password found in Step 2 in Part 3.

Шаг 2: Download the file to Bob's computer.

- a. At the ftp prompt prompt> type the dir command to view a list of files stored on the remote FTP server.
- b. User Mary uploaded a clientinfo.txt file with encrypted information about the clients of a medical institution to the server.
Download the clientinfo.txt file to Bob's computer. To do this, enter the get clientinfo.txt command.
- c. At the ftp prompt> enter the quit command.
- d. At the command prompt PC> enter the dir command to verify that the file is clientinfo.txt on Bob's computer.

If cybercriminals intercept a file while it is being transmitted over the Internet, what information can they obtain in plaintext?

Учебный вопрос 5: Decrypt the contents of the clientinfo.txt file

Шаг 1: Receiving the decryption key from the user Mary.

- a. Open the Metropolis Bank HQ object and select Bob's computer.
 - b. Click the Desktop tab and click the Email icon.
 - c. In the Email application window, click the Receive button.
 - d. Select the email with the subject "Decryption Key" and write down the decryption key below.
What decryption key is needed to access the sensitive information contained in the clientinfo.txt file?
-

Шаг 2: Decryption of the contents of the clientinfo.txt file.

- a. Open the Metropolis Bank HQ object and select Bob's computer.
- b. Click the Desktop tab and click the Text Editor icon.
- c. In the Text Editor window, select the File >Open menu options.
- d. Select the clientinfo.txt document, and then click OK.
- e. Select all the text contained in the clientinfo.txt file and copy it.
- f. Open a web browser on your personal computer and go to the website.

- g. Place your cursor in the white box that is on the right side of the website and paste the ciphertext. To decrypt the text, click the Decipher It button and enter the decryption password you received in the email from Mary. Click Decrypt.

What is the name of the first account in the clientinfo.txt file?

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 1. Finding FTP Account Data for Mary Laptop	Step 2	2	
Question 2. Uploading confidential data to the server via the FTP protocol	Step 1	2	
	Step 3	2	
Q3. Finding FTP Account Data for Bob's Computer	Step 2	2	
Question 4. Downloading confidential data from the server via the FTP protocol	Step 2	2	
Question 5. Decryption of the contents of the clientinfo.txt file	Step 1	2	
	Step 2	2	
Questions		14	
Packet Tracer Score		86	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. What identification information (username and password) corresponds to Mary's FTP account?
2. If cybercriminals intercept a file while it is being transmitted over the Internet, what information will they be able to obtain in plain text?
3. What identification information (username and password) corresponds to Bob's FTP account?
4. What decryption key is required to access sensitive information contained in the clientinfo.txt file?
5. What is the name of the first account in the clientinfo.txt file?

Lesson No 4.

Verify the integrity of files and data

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Be able to verify the integrity of files using hashing.
3. Acquire the ability to verify the integrity of critical files using the HMAC mechanism.

Educational issues of the lesson

1. Download customer information files to the Mike user's computer.
2. Downloading files with client information to Mike's computer from the Backup File backup server.
3. Verifying the integrity of files with client information using hashing.
4. Verify the integrity of critical files using the HMAC mechanism.

Equipment and materials

A PC with Packet Tracer installed.

General information

In this task, you will verify the integrity of the files using hash sums to ensure that the contents of the files have not been tampered with. Files whose integrity is in doubt should be transferred to the user's Sally computer for further analysis. Configure IP addressing, networking, and services according to the addressing table. You will inspect and forward suspicious files using client devices that are located in different geographic regions.

Addressing Table

Device	Private IP address	Public IP address	Subnet mask	Website
Сервер FTP/Web	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Резервный файловый сервер Backup File	—	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Internet
Mike	10.44.2.101	—	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	—	255.255.255.0	Metropolis Bank HQ
Bob	10.44.1.3	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Downloading customer information files to Mike's computer

Шаг 1: Accessing the FTP server from Mike's computer.

- a. Open the GothamHealthcare Branch object and select the computer named Mike.
- b. Go to the Desktop tab and click the Web Browser icon.
- c. Enter the URL <http://www.cisco.corp> and click Go.
- d. Click here to download the latest versions of your files.

What protocol was used to access this web page on the Backup File backup server?

Шаг 2: The file server has been compromised. This must be notified to the Sally user.

- Open the GothamHealthcare Branch object and select the Mike computer.
- Click the Desktop tab and click the Email icon.
- Create an email reporting that the file server has been compromised and send it to .

Учебный вопрос 2: Downloading client information files to Mike's computer from the Backup File backup server

Шаг 1: Accessing an external FTP server from a Mike user's computer.

- Open the GothamHealthcare Branch object and select the Mike computer.
- Go to the Desktop tab and click the Web Browser icon.
- Enter the URL `https://www.cisco2.corp` and click Go.
- Click here to view a list of the newest files and their corresponding hash sums.

What protocol was used to access this web page on the Backup File backup server?

What are the names and hashes of the files on the backup file server?

Шаг 2: Download customer information files to the Mike user's computer.

- Open the GothamHealthcare Branch object and select the Mike computer.
- Click the Desktop tab and click the Command Prompt icon.
- Establish a connection to the Backup File Backup Server. To do this, enter the ftp command `www.cisco2.corp`.
- Enter your `cisco123` username and password.
- At the ftp prompt `prompt>` type the `dir` command to view a list of files stored on the remote FTP server.
- Download six files with client information (`NEclients.txt`, `NWclients.txt`, `Nclients.txt`, `SEclients.txt`, `SWclients.txt`, `Sclients.txt`) to the user Mike's computer using the `get FILENAME.txt` command, where "FILENAME" is the name of the file to be downloaded.

```
ftp>get NEclients.txt
```

```
Reading the NEclients.txt file from www.cisco2.corp:
File transfer in progress...
```

```
[Transfer Complete - 584 bytes]
```

```
584 bytes copied in 0.05 secs (11680 bytes/sec)
```

- Once you have downloaded all the files, enter the quit command at the command prompt `ftp>`.
- At the command prompt `PC>` enter the `dir` command to verify that the customer information files are indeed on Mike's computer.

Учебный вопрос 3: Verify the integrity of client information files using hashing

Шаг 1: Checking the hash sums on the Mike user's computer.

- a. Open the GothamHealthcare Branch object and select the Mike computer.
- b. Click the Desktop tab and click the Text Editor icon.
- c. In the Text Editor window, select the File >Open menu options.
- d. Select the NEclients.txt document, and then click OK.
- e. Copy the entire content of the text document.
- f. Open a web browser on your personal computer and go to the website.
- g. Place the cursor in the white input field and paste the contents of the text document. Make sure that the md2 algorithm is selected. Click the Hash this! button.
- h. To verify that the contents of the file have not been tampered with, compare the resulting hash with the corresponding hash from the list of files you received in step 1 in Part 2.
- i. Repeat steps d-h for each customer information file and compare the resulting hash sums with the original hashes from the list of files you received in step 1 in Part 2.

Which file has an invalid hash sum (i.e., has been corrupted)?

Шаг 2: Downloading a suspicious file to Sally's computer.

- a. Open the Metropolis Bank HQ object and select the Sally computer.
- b. Click the Desktop tab and click the Command Prompt icon.
- c. Establish a connection to the Backup File Backup Server. To do this, enter the ftp command `www.cisco2.corp`.
- d. Enter your sally username and cisco123 password.
- e. At the ftp prompt `prompt>` type the `dir` command to view a list of files stored on the remote FTP server.
- f. Download the malformed file identified in step 1 in Part 3 from the server.
- g. At the ftp prompt `>` enter the `quit` command.
- h. At the command prompt `PC>` enter the `dir` command to verify that the malformed file has been successfully downloaded to the user's computer for later analysis.

Учебный вопрос 4: Verify the integrity of critical files using the HMAC mechanism

Шаг 1: Calculation of the HMAC sum of a critical file.

- a. Open the Metropolis Bank HQ object and select Bob's computer.
- b. Click the Desktop tab and click the Command Prompt icon.
- c. At the command prompt `PC>` enter the `dir` command to verify that the critical file is `income.txt` on Bob's computer.
- d. Click the Desktop tab and click the Text Editor icon.
- e. In the Text Editor window, select the File >Open menu options.
- f. Select the `income.txt` document, and then click OK.
- g. Copy the entire content of the text document.
- h. Open a web browser on your personal computer and go to the website.

- i. Place the cursor in the white input box and paste the contents of the text document. Enter the cisco123 secret key. Make sure that the SHA1 algorithm is selected. Click the Compute HMAC button.

What is the HMAC sum of the contents of the file?

Why is the HMAC mechanism safer than regular hashing?

War 2: Check the received HMAC amount.

- a. Open the Metropolis Bank HQ object and select Bob's computer.
- b. Go to the Desktop tab and click the Web Browser icon.
- c. Enter the URL <https://www.cisco2.corp> and click Go.
- d. Click here to view a list of the newest files and their corresponding hash sums.

Does the resulting hash sum of the HMAC file match income.txt the hash in the list?

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 1. Downloading customer information files to Mike's computer	Step 1	2	
Question 2. Downloading client information files to Mike's computer from the Backup File	Step 1	2	
	Step 1	6	
Question 3. Checking the integrity of files with customer information using hashing	Step 1	5	
Q4. Integrity check of critical files using the HMAC mechanism	Step 1	5	
	Step 1	5	
	Step 2	5	
Questions		30	
Packet Tracer Score		70	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. What protocol was used to access the web page on the backup file server Backup File?
2. What are the names and hashes of the files on the backup file server?
3. Which of the files has an incorrect hash sum (i.e. was distorted)?
4. What is the HMAC sum of the contents of the file?
5. Why is the HMAC mechanism safer than conventional hashing?

6. Does the resulting hash sum of the HMAC file income.txt match the hash sum in the list?

LessonNo 5. WEP/WPA2 PSK/WPA2 RADIUS

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Be able to set up WEP on site.
3. Be able to configure WPA2 PSK on site.
4. Be able to configure WPA2 RADIUS.
5. To acquire the skills of analysis and generalization of the results obtained.

Educational issues of the lesson

1. Configure WEP at a Healthcare at Home facility.
2. Configure WPA2 PSK at a Gotham Healthcare Branch facility.
3. Configure WPA2 RADIUS on a Metropolis Bank HQ facility.

Equipment and materials

A PC with Packet Tracer installed.

General information

In this exercise, you'll configure Wi-Fi networks at all three sites. In this exercise, you'll work with WEP, WPA2 PSK, and WPA2 RADIUS protection. This will introduce you to the different configurations of Wi-Fi networks and how to secure them. In the Healthcare at Home facility, you'll configure WEP protection. In the Gotham Healthcare Branch and Metropolis Bank HQ sites, you'll need to configure WPA2 PSK and WPA2 Radius protection, respectively. Configure IP addressing, networking, and services according to the addressing table. You'll configure multiple secure wireless networks using wireless routers and client devices that are located in different geographic regions.

Addressing Table

Device	Private IP address	Public IP address	Subnet mask	Website
Сервер NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Configuring WEP at a Healthcare at Home Facility

Шаг 1: Set up a wireless network SSID.

- a. Open the Healthcare at Home object and select PC0.
- b. Click the Desktop tab. Click Command Prompt. Enter the ipconfig command at the command deadline.

```
PC>ipconfig
```

```
FastEthernet0 Connection:(default port)
```

```
Link-local IPv6 Address.....: FE80::20B:BEFF:FEB4:1262
IP Address.....: 10.44.3.100
```

Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.44.3.1

What is the default IP address assigned to the gateway?

-
- c. Go to the Web Browser application and enter the default gateway IP address. Enter admin as your username and password. Click OK.
 - d. In this network infrastructure, the default gateway is the Wireless Router. Click the Wireless tab.
 - e. Change the SSID from DefaultWIFI to Home.
 - f. Enable SSID transfer. To do this, select Broadcast.
 - g. Click the Save Settings button. Click Continue.

Шар 2: Configure wireless network protection.

- a. Select the Wireless Router and go to Wireless >WirelessSecurity).
- b. From the Security Mode drop-down menu, select WEP.
- c. The Encryption option has a default value of 40/64-bits (40/64 bits). Do not change this value. For Key 1, enter 0123456789.
- d. Click the Save Settings button. Click Continue.

WEP protection and 0123456789 key are not secure. Why is WEP considered insecure?

Шар 3: Connecting client devices.

- a. Open the Healthcare at Home object and select your Dave laptop.
- b. Go to the Desktop tab and click the PC Wireless icon.
- c. Go to the Connect tab and click the Refresh button.
- d. Select the name of the Home wireless network and press the Connect button.
- e. For WEP Key 1, enter the 0123456789 key and click Connect.
- f. Repeat steps a-e on your Mary laptop.

Учебный вопрос 2: Setting up WPA2 PSK at a Gotham Healthcare Branch facility

Шар 1: Set up a wireless network SSID.

- a. Open the Gotham Healthcare Branch facility and select PC1.
- b. Click the Desktop tab. Click Command Prompt. Enter the ipconfig command at the command deadline.

Make a note of the default gateway IP address.

-
- c. Go to the Web Browser application and enter the default gateway IP address. Enter admin as your username and password. Click OK.
 - d. Click the Wireless tab.
 - e. Change the SSID from DefaultWIFI to BranchSite.
 - f. Change the Standard Channel setting to 6 - 2.437GHz.
 - g. Enable SSID transfer. To do this, select Broadcast.
 - h. Click the Save Settings button. Click Continue.

Шаг 2: Configure wireless network protection.

- a. Select the Wireless Router and go to Wireless >WirelessSecurity).
- b. From the Security Mode drop-down menu, select WPA2 Personal.
- c. The default Encryption setting is AES. Do not change this value. Enter ciscosecure as your passphrase.
- d. Click the Save Settings button. Click Continue.

Шаг 3: Connecting client devices.

- a. Open the Gotham Healthcare Branch object and select Computer Tim.
- b. Go to the Desktop tab and click the PC Wireless icon.
- c. Go to the Connect tab and click the Refresh button.
- d. Select the name of the BranchSite wireless network and click the Connect button.
- e. Enter the ciscosecure PSK key and click Connect.
- f. Repeat steps a through e on your Mike computer.

Учебный вопрос 3: Configuring WPA2 RADIUS on a Metropolis Bank HQ Facility

Шаг 1: Set up a wireless network SSID.

- a. Open the Metropolis Bank HQ object and select the Sally computer.
- b. Go to the Web Browser app and enter the IP address of your wireless router (10.44.1.251). Enter admin as your username and password. Click OK.
- c. Go to the Wireless tab. Change the SSID from DefaultWIFI to HQ.
- d. Change the Standard Channel setting to 11 - 2.462GHz.
- e. Enable SSID transfer. To do this, select Broadcast.
- f. Click the Save Settings button. Click Continue.

Шаг 2: Configure wireless network protection.

- a. Select the Wireless Router and go to Wireless >WirelessSecurity).
- b. From the Security Mode drop-down menu, select WPA2-Enterprise.
- c. The default Encryption setting is AES. Do not change this value. Enter the following RADIUS server parameters:
RADIUS SERVERIP (IP-адрессервераRADIUS): 10.44.1.252
Shared Secret: ciscosecure
- d. Click the Save Settings button. Click Continue.

Шаг 3: Configure the RADIUS server.

- a. Open the Metropolis Bank HQ object and select the NTP/AAA server.
- b. Go to the Services tab and select the AAA section.
- c. Enter the following information in the Network Configuration area:
Client Name:..... HQ
Client IP: 10.44.1.251
Secret: ciscosecure
ServerType: Radius

- d. TapAdd.
- e. Enter the following information in the User Setup area, and then click Add to add a new user name.

Username:	bob	Password:	secretninjabob
Username:	phil	Password:	philwashere

War 4: Connecting client devices.

- a. Open the Metropolis Bank HQ object and select Bob's computer.
 - b. Go to the Desktop tab and click the PC Wireless icon.
 - c. Click the Profiles tab and click the New button.
 - d. Enter a name for the RADIUS profile, and then click OK.
 - e. Click Advanced Setup.
 - f. In the Wireless Network Name field, enter HQ and click Next.
 - g. Without changing your network settings, click Next again.
 - h. From the Wireless Security drop-down menu, select WPA2-Enterprise and click Next.
 - i. Enter your username bob and password secretninjabob. Click Next.
 - j. Click Save, then click Connect to Network.
 - k. Bob's computer will connect automatically.
 - l. Repeat steps a-j on Phil's laptop using the authentication information provided in step 3e.
- Why is it wiser to use WPA2 RADIUS mode instead of WPA2 PSK in a large organization?
-
-

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 1. Setting up WEP at a Healthcare at Home facility	Step 2	5	
Q3. Configuring WPA2 RADIUS at the Metropolis Bank HQ facility	Step 4	5	
Questions		10	
Packet Tracer Score		90	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. What is the default IP address assigned to the gateway?
2. WEP protection and 0123456789 key are not secure. Why is WEP considered insecure?
3. Write down the default IP address of the gateway.
4. Why is it more reasonable to use WPA2 RADIUS instead of WPA2 PSK in a large organization?

LessonNo 6.

Configuring VPN Transport Mode

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Be able to transmit unencrypted FTP traffic.
3. Be able to transmit encrypted FTP traffic.
4. Acquire the ability to configure a VPN client on site.
5. To acquire the skills of analysis and generalization of the results obtained.

Educational issues of the lesson

1. Transfer of unencrypted FTP traffic.
2. Setting up a VPN client at the Metropolis facility.
3. Transfer of encrypted FTP traffic.

Equipment and materials

A PC with Packet Tracer installed.

General information

In this task, you will monitor the transmission of unencrypted FTP traffic between the client and the remote site. Next, you will configure the VPN client to connect to the Gotham Healthcare Branch facility and begin transmitting encrypted FTP traffic. Configure IP addressing, network, and services according to the addressing table. You will transfer encrypted and unencrypted FTP data using a client device that is located within the Metropolis Bank HQ facility.

Addressing Table

Device	Private IP address	Public IP address	Subnet mask	Website
Private_FTP server	10.44.2.254	—	255.255.255.0	Gotham Healthcare Branch
Public_FTP server	10.44.2.253	209.165.201.20	255.255.255.0	Gotham Healthcare Branch
Branch_Router	—	209.165.201.19	255.255.255.248	Gotham Healthcare Branch
Phil's Computer	10.44.0.2	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Transfer of unencrypted FTP traffic

Шаг 1: Gaining access to the Cyber Criminals Sniffer traffic analyzer.

- a. Select the Cyber Criminals Sniffer traffic analyzer and go to the GUI (Graphical Interface) tab.
- b. Click the Clear button to delete any previously collected traffic entries.
- c. Minimize the window of the Cyber Criminals Sniffer traffic analyzer.

Шаг 2: Establish an insecure FTP connection to the Public_FTP server.

- a. Open the Metropolis Bank HQ object and select the Phil laptop.
- b. Go to the Desktop tab and click the Command Prompt icon.
- c. Enter the ipconfig command to display the current IP address of Phil's computer.

- d. Establish a connection to the server Public_FTP the Gotham Healthcare Branch facility. To do this, enter the ftp command 209.165.201.20 at the command prompt.
- e. Enter your Cisco username and publickey password to log in to Public_FTP server.
- f. Use the put command to upload the PublicInfo.txt file to the Public_FTP server.

Шаг 3: View traffic information with the Cyber Criminals Sniffer traffic analyzer.

- a. Expand the previously minimized Cyber Criminals Sniffer traffic analyzer window.
- b. In Traffic Analyzer, select FTP messages and scroll through the full contents of each message. What information is displayed in plaintext?

- c. Type quit to end the session on the Public_FTP server.

Учебный вопрос 2: Setting up a VPN client on Phil's computer

- a. On Phil's computer, run the ping command using the IP address of the router Branch_Router. The first few ping requests may not be answered because they have timed out. Enter the ping command. You should receive answers to four ping requests.
- b. Go to the Desktop tab and click the VPN icon
- c. In the VPN Configuration window, enter the following parameters:
GroupName: VPNGROUP
Group Key: 123
Host IP (Server IP) (IP-адрес хоста (IP-адрес сервера)): 209.165.201.19
Username: phil
Password: cisco123
- d. Click the Connect button and then click OK in the next window.
What client IP address is used to establish a client-to-object VPN connection?

Учебный вопрос 3: Transfer of encrypted FTP traffic

Шаг 1: View the current IP addressing settings on Phil.

- a. Open the Metropolis Bank HQ object and select the Phil computer.
- b. Go to the Desktop tab and click the Command Prompt icon.
- c. Use the ipconfig command to display the current IP address of Phil's computer.
Do you see an additional IP address that didn't appear earlier in step 2c in Part 1? What is this address?

Шаг 2: Sending encrypted FTP traffic from Phil's computer to Private_FTP's server.

- a. Establish a connection to the server Private_FTP the Gotham Healthcare Branch facility. To do this, enter the ftp 10.44.2.254 command at the command prompt.
- b. Enter your cisco username and secretkey password to log in to the Private_FTP server.
- c. Upload the PrivateInfo.txt file to the Private_FTP server.

War 3: View Traffic Information with Cyber Criminals Sniffer Traffic Analyzer

- a. Expand the previously minimized Cyber Criminals Sniffer traffic analyzer window.
- b. Select FTP messages in the Traffic Analyzer window.

Are there any FTP messages that display an internal password or information about uploading a PrivateInfo.txt file to the server? Please explain.

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 1. Transfer of unencrypted FTP traffic	Step 3	20	
Q2. Setting up a VPN client on Phil's computer	Step 1	10	
Question 3. Transfer of encrypted FTP traffic	Step 1	10	
	Step 3	20	
Questions		60	
Packet Tracer Score		40	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. What information is displayed in plaintext?
2. What client IP address is used to establish a client-to-object VPN connection?
3. Do you see an alternate IP address that didn't appear earlier in step 2c in Part 1? What is this address?
4. Are there any FTP messages in FTP messages that display an internal password or information about uploading a PrivateInfo.txt file to the server? Please explain.

LessonNo 7.

Router and Switch Redundancy

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Acquire the ability to monitor network infrastructure failover using redundant routers.
3. Acquire the ability to monitor network infrastructure failover using redundant switches.
4. To acquire the skills of analysis and generalization of the results obtained.

Educational issues of the lesson

1. Monitor network infrastructure failover using redundant routers.
2. Monitor network infrastructure failover using redundant switches.

Equipment and materials

A PC with Packet Tracer installed.

General information

In this job, you will observe a successful failover of the Metropolis network infrastructure. Multiple routers are used by default for gateway redundancy. Then, a successful failover will be performed on the failure of the Gotham network infrastructure. Redundancy of network routes will be provided by multiple switches. Configure IP addressing, networking, and services according to the addressing table. To test routes before and after a successful failover on a network infrastructure failure, you will use client devices in different geographic regions.

Addressing Table

Device	IP address	Subnet mask	Default gateway	Website
External Web Server	209.165.201.10	255.255.255.0	—	Internet
R1	10.44.1.2	255.255.255.0	—	Metropolis Bank HQ
R2	10.44.1.3	255.255.255.0	—	Metropolis Bank HQ
Phil's Computer	10.44.1.12	255.255.255.0	10.44.1.1	Metropolis Bank HQ
Tim's Computer	10.44.2.11	255.255.255.0	10.44.2.1	Gotham Healthcare Branch

Учебный вопрос 1: Watch for failover when network infrastructure fails using redundant routers.

Шаг 1: Open a command prompt on Phil's computer.

- a. Select the Metropolis Bank HQ node and select the Phil laptop.
- b. Click the Desktop tab and click the Command Prompt icon.

Шаг 2: Trace the route to the external web server.

- a. Send a ping request to the External Web server on the Internet. To do this, enter ping 209.165.201.10 at a command prompt.
- b. Trace the route to the External Web server on the Internet. To do this, at the command prompt, type tracert 209.165.201.10.

- c. The IP addresses in the tracert command output represent the network devices through which network traffic flows.

Specify the IP addresses of the devices through which traffic passes from the user's Phil laptop to the external web server.

The first address that the tracert command outputs is the default network gateway (exit point).

- d. Compare the output of the tracert command with the addressing table at the beginning of the lab. Which router is currently the current default gateway?

Шар 3: Trigger a failover when the network infrastructure fails.

- a. In Metropolis Bank HQ, press Switch HQ_S1.
- b. Click on the Command Line Interface (CLI) tab.
- c. Enter the following commands to disable the Gig0/2 uplink port:

```
enable
configure terminal
interface GigabitEthernet0/2
shutdown
```

Шар 4: Trace the route back to the external web server.

- a. In the Metropolis Bank HQ node, click Phil laptop.
- b. Click the Desktop tab and click the Command Prompt icon.
- c. Send a ping request to the External Web server on the Internet. To do this, enter ping 209.165.201.10 at a command prompt.
- d. Trace the route to the External Web server on the Internet. To do this, at the command prompt, type tracert 209.165.201.10.

The IP addresses in the tracert command output represent the network devices through which network traffic flows.

Specify the IP addresses of the devices through which traffic passes from the user's Phil laptop to the external web server.

-
- e. The first address that the tracert command outputs is the default network gateway (exit point). Which router now works as the default gateway?

-
- f. At the command prompt that appears, enter the ipconfig command. The default gateway is shown the IP address 10.44.1.1, which does not match either the first (10.44.1.2) or the second (10.44.1.3) output of the tracert command. This indicates that the default 10.44.1.1 gateway traffic is actually routed through backup routers with different IP addresses: R1 with 10.44.1.2 or R2 with 10.44.1.3 if Router R1 is unavailable.

Учебный вопрос 2: Watch for network infrastructure failover using redundant switches.

Шар 1: Open a command prompt on Tim's computer.

- a. Select the Gotham Healthcare Branch node and select the Tim computer.
- b. Click the Desktop tab and click the Command Prompt icon.

Шар 2: Trace the route to the external web server.

- a. Send a ping request to the External Web server on the Internet. To do this, enter ping 209.165.201.10 at a command prompt.
- b. You can use the constant ping command to observe the failover of the network infrastructure.
Run the constant ping command on the External Web server. To do this, at the command prompt, enter ping -t 209.165.201.10.
Minimize the window for Tim's computer.

War 3: Trigger a failover when the network infrastructure fails.

- a. Gotham Healthcare Branchpressswitch S3.
- b. Go to the CLI tab.
- c. Enter the following commands to disable the Gig0/2 uplink port:

```
enable
configure terminal
interface GigabitEthernet0/2
shutdown
```

War 4: Trace the route back to the external web server.

- a. In the Gotham Healthcare Branch node, expand the window that displays Tim's computer.
- b. Wait 30-60 seconds. You can also watch the switching port connection LEDs in the Gotham Healthcare Branch network infrastructure.
- c. The output of the command on Tim's computer should be similar to the following:

```
PC>ping -t 209.165.201.10
Pinging 209.165.201.10 with 32 bytes of data:

Reply from 209.165.201.10: bytes=32 time=47ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=43ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 209.165.201.10: bytes=32 time=41ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
```

- d. Close the window.

What cable was used to send data when ping responses were received before the "Request timed out" message appeared?

What cable was used to send data when ping responses were received after the "Request timed out" message appeared?

- e. What feature does this scenario illustrate the redundancy of switches for switching when a Gigabit Ethernet port fails?

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 1. Monitoring the failover of the network infrastructure using redundant routers	Step 2	10	
	Step 2	10	
	Step 4	10	
	Step 4	10	
Question 2. Failover Monitoring of Network Infrastructure Failure Using Redundant Switches	Step 4	5	
	Step 4	5	
	Step 4	10	
Questions		60	
Packet Tracer Score		40	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. Specify the IP addresses of the devices through which traffic passes from the user's Phil laptop to the external web server.
2. Specify the IP addresses of the devices through which traffic passes from the user's Phil laptop to the external web server.
3. Which router works as the default gateway?
4. What cable was used to send data when ping responses were received before the "Request timed out" message appeared?
5. What cable was used to send data when ping responses were received after the "Request timed out" message appeared?
6. What is the redundancy of switches for switching in the event of a Gigabit Ethernet port failure in this scenario?

LessonNo 8.

Firewalls on the server and access control lists on the router

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the material received in lectures.
2. Be able to connect to a web server.
3. Be able to prevent unencrypted HTTP sessions.
4. Acquire the skills to access a firewall on an e-mail server.
5. Acquire the ability to form procedures for information security management.

Educational issues of the lesson

1. Connecting to a web server.
2. Prevent unencrypted HTTP sessions.
3. Access the firewall on the e-mail server.

Equipment and materials

A PC with Packet Tracer installed.

General information

In this task, you will access a user in the Metropolis node and connect via HTTP and HTTPS to a remote web server. Configure IP addressing, networking, and services according to the addressing table. Using a client device in the Metropolis node, you will test the connection to the remote web server. To ensure that the Metropolis node is secured, you will disable unencrypted connections to external web sessions.

Addressing Table

Device	Private IP address	Public IP address	Subnet mask	Website
Web server	—	209.165.201.10	255.255.255.0	Internet

Учебный вопрос 1: Connecting to a web server.

Шаг 1: Access the HQ Internet web server from Sally's PC over HTTP.

- a. Select the Metropolis Bank HQ node and select PC Sally.
- b. Go to the Desktop tab and click the Web Browser icon.
- c. Enter the URL <http://www.cisco.corp> and click Go.
- d. Click the Login Page link.

Why should a user be concerned when submitting information through this website?

Шаг 2: Access the HQ Internet web server from Sally's computer over HTTPS.

- a. Open a web browser on your Sally's computer.
- b. Enter the URL <https://www.cisco.corp> and click Go.
- c. Click the Login Page link.

The user has less to worry about when submitting information through this website. Why?

-
- d. Close the Sally user's computer.

Учебный вопрос 2: Disallow unencrypted HTTP sessions.

Шаг 1: Set up your router HQ_Router.

- a. Open the Metropolis Bank HQ object and select HQ_Router router.
- b. Click the CLI tab and press Enter.
- c. Use the Cisco password to log on to the router.
- d. Enter the enable command and then configure terminal to access the global configuration mode.

To prevent unencrypted HTTP traffic from passing through the head router, network administrators can create and deploy access control lists (ACLs).

The following commands are beyond the scope of this course. They are used to demonstrate the ability to prevent unencrypted traffic from passing through the HQ_Router router.

- e. At the HQ_Router(config)# command prompt in global configuration mode, copy and paste the following ACL configuration into the HQ_Router.

```
!  
access-list 101 deny tcp any any eq 80  
access-list 101 permit ip any any  
!  
int gig0/0  
ip access-group 101 in  
!  
end
```

- f. Close the router HQ_Router.

Шаг 2: Access the HQ Internet web server from Sally's PC over HTTP.

- a. In the Metropolis Bank HQ node, click Sally's PC.
- b. Go to the Desktop tab and click the Web Browser icon.
- c. Enter the URL <http://www.cisco.corp> and click Go.

Can a Sally user's computer access the HQ Internet web server over HTTP?

Шаг 3: Access the HQ Internet web server from Sally's computer over HTTPS.

- a. Open a web browser on your Sally's computer.
- b. Enter the URL <https://www.cisco.corp> and click Go.

Can Sally's computer access the HQ Internet web server over HTTP?

- c. Close the Sally user's computer.

Учебный вопрос 3: Access the firewall on the e-mail server.

- a. In the Metropolis Bank HQ node, click Email server.
- b. Click the Desktop tab and select Firewall. No firewall rules are defined.

To prevent non-e-mail traffic from being sent or received through the e-mail server, network administrators can create firewall rules directly on the server. Alternatively, as shown earlier, access control lists (ACLs) can be used on a network device, such as a router.

Suggested Scoring Method

Lesson questions	Question Steps	Maximum Points	Points Earned
Question 1. Connecting to a web server	Step 1	15	
	Step 2	15	
Question 2. Preventing unencrypted HTTP sessions	Step 2	15	
	Step 3	15	
Questions		60	
Packet Tracer Score		40	
Total Points		100	

Contents of the report

The report on the practical lesson must contain:

1. The structure of the source data in Packet Tracer with IP addressing of devices.
2. Answers to questions posed during practical tasks.
3. Conclusions on the work done and the results obtained.

The results of the work should be reflected in the workbook and defended orally by each student.

Control questions

1. Why should a user be concerned when submitting information through this website?
2. The user has less to worry about when submitting information through the <https://www.cisco.com> website. Why?
3. Can Sally's computer access the HQ Internet web server over HTTP?
4. Can Sally's computer access the HQ Internet web server via HTTP?

LessonNo 9.

Practicing complex practical skills

Objectives of the lesson

As a result of this lesson and subsequent independent work, students should:

1. To consolidate the skills acquired in the process of mastering the educational material.
2. Gain comprehensive hands-on skills in setting up a wireless router, downloading and uploading files using FTP, securely connecting to a remote host using VPN, and securing your Cisco IOS router.

Equipment and materials

A PC with Packet Tracer installed.

Addressing Table

Device	UI	IP address	Subnet mask	Default gateway
HQ_Router	G0/0	10.44.1.1	255.255.255.0	—
	G0/1	209.165.201.2	255.255.255.248	—
VPN server	NOTHING	209.165.201.19	255.255.255.248	—
HQ_Wireless	LAN	10.44.1.254	255.255.255.0	10.44.1.1
Сервер FTP/Web	NOTHING	10.44.1.252	255.255.255.0	10.44.1.1
BackupFiles Server	NOTHING	10.44.2.10	255.255.255.0	10.44.2.1

Scenario

This final lesson will help you practice many of the skills you learned during the tutorial. You'll configure your wireless router, download and upload files using FTP, securely connect to a remote site using a VPN, and secure your Cisco IOS router.

Implementation

Note: You only have access to the Metropolis HQ node. You can access all servers and computers on that node to perform the scan.

Implement the following requirements:

Sally's computer - Metropolis Bank HQ

- Upload the secure.txt file to the FTP/Web server using the FTP protocol:
 - User sally, ftpaccess password
 - File to upload: secure.txt
 - Use the IP address of the FTP/Web server from the addressing table.
- Connect the user's Sally computer to the Gotham Healthcare Branch node over the client-to-node VPN:
 - Send a ping request to the VPN server using the IP address from the addressing table.
 - Connect the client-to-site VPN using the vpnsally username and password
 - Use VPNGROUP and key 123
- Using a VPN connection, download the transactions.txt file from the BackupFiles server via FTP:
 - Use the IP address of the BackupFiles server from the addressing table.
 - User sally, password securesally
 - Download: transactions.txt

Phil's Laptop – Metropolis Bank HQ

- Configure the router HQ_Wireless.
 - Use the router's IP address HQ_Wireless from the addressing table.
 - Use a web browser to configure the router HQ_Wireless from Phil's laptop.
 - Admin User, Password p@ssword
 - Replace the SSID with DefaultWIFI with HQwifi
 - Configure the SSID as visible (broadcast) for wireless clients.
 - Set up WPA2 Personal wireless security using the cisco321 passphrase.
- Protect your router HQ_Router.
 - Use the router's IP address HQ_Router from the addressing table.
 - Use the command prompt to connect to HQ_Router via SSH. Username phil, password securessh
 - Use the enable command and the Cisco password.
 - Activate the Cisco IOS Failover Configuration feature.
 - Set up a message of the day (motd) for the banner that includes the phrase Authorized Access Only

Gina's Laptop – Metropolis Bank HQ

- Connect the Gina user's laptop to the wireless network.
 - Create a connection with the HQwifi SSID
 - Use the cisco321 PSK key
 - Make sure your laptop is using DHCP

Suggested Scoring Method

Packet Tracer Score: 90 points.