

**O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA
INNOVATSIYALAR VAZIRLIGI**

**“TOSHKENT IRRIGATSIYA VA QISHLOQ XO‘JALIGINI
MEXANIZATSIYALASH MUHANDISLARI INSTITUTI” MILLIY
TADQIQOT UNIVERSITETI**

E.O.BOZOROV, M.M.ISMAILOV, M.SH.ABDULLAYEV

**AXBOROT TIZIMLARINING ISHONCHLIGI VA XAVFSIZLIGI
ASOSLARI**

O‘QUV QO‘LLANMA



Toshkent 2024

E.O. Bozorov, M.M. Ismailov, M.SH. Abdullayev. Axborot tizimlarining ishonchliligi va xavfsizligi asoslari. (O‘quv qo‘llanma) – T.: 2024. – 146 bet

Annotatsiya

“Axborot tizimlarining ishonchliligi va xavfsizligi asoslari” fani bo‘yicha o‘quv qo‘llanma “60610200 – Axborot tizimlari va texnologiyalari” bakalavr yo‘nalishi talabalari uchun mo‘ljallangan. O‘quv qo‘llanmada axborot tizimlarining ishonchliligi va axborot xavfsizligi nima ekanligi, qanday tahdidlar mavjudligi va nima uchun muhimligi haqidagi asosiy tushunchalar bilan birga tarmoq simulyatorlari haqida umumiy tushunchalar, ularning imkoniyatlarini o‘rganish Cisco Packet Tracerda ishlash misolida keltirilgan. Qo‘llanmada axborot tizimlari, kompyuter tarmoqlari, dasturiy ta‘minot va texnik vositalarning asosiy ishlash tamoyillari Cisco Packet Tracerda qurilgan misollar orqali keltirilgan. Bundan tashqari, kriptografiyaning asosiy tamoyillari va uning ma‘lumotlarni himoya qilishda, shifrlashda va autentifikatsiyalashda qanday qo‘llanilishi ko‘rib chiqilgan va aks etgan. Axborot tizimlarining ishonchliligi va xavfsizligi asoslari kursi bo‘yicha ma‘ruzalarda talabalar olgan bilimlarini mustahkamlashga yo‘naltirilgan.

Аннотация

Учебное пособие по предмету «Надежность и безопасность информационных систем» предназначено для студентов бакалавриата «60610200 – Информационные системы и технологии». В учебном пособии наряду с основными понятиями о том, что такое надежность и информационная безопасность информационных систем, какие угрозы существуют и почему они важны, даны общие понятия о сетевых симуляторах, изучение их возможностей на примере работы в Cisco Packet Tracer. В руководстве основные принципы работы информационных систем, компьютерных сетей, программного и аппаратного обеспечения представлены на примерах, встроенных в Cisco Packet Tracer. Кроме того, рассматриваются и иллюстрируются основные принципы криптографии и то, как она используется для защиты, шифрования и аутентификации данных. Лекции по основам надежности и безопасности информационных систем направлены на закрепление полученных знаний студентами.

Annotation

The textbook on the subject “Fundamentals of Reliability and Security of Information Systems” is intended for students of the bachelor's degree program

“60610200 - Information Systems and Technologies”. The manual provides basic concepts about what reliability and information security of information systems are, what threats exist and why they are important, as well as general concepts about network simulators, studying their capabilities using the example of working in Cisco Packet Tracer. The manual presents the basic principles of operation of information systems, computer networks, software and hardware using examples built in Cisco Packet Tracer. In addition, the basic principles of cryptography and its application in data protection, encryption and authentication are considered and reflected. The course is aimed at consolidating the knowledge gained by students in lectures on the Fundamentals of Reliability and Security of Information Systems.

Taqrizchilar:

- Raxmatov A.J. – “Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti” Milliy tadqiqot universiteti “Elektr ta‘minoti va qayta tiklanuvchan manbalari” kafedrası dotsenti, texnika fanlari nomzodi.
- Isakov A.F. – IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrası boshlig‘i o‘rinbosari, texnika fanlari bo‘yicha falsafa doktori (PhD)

UDC: 004.056

© “Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti” Milliy tadqiqot universiteti - 2024 yil.

Kirish

Axborot tizimlari zamonaviy tashkilotlarda qarorlar qabul qilish, operatsiyalar va aloqalarni qo'llab-quvvatlashda muhim rol o'ynaydi. Ushbu tizimlarning ishonchliligi va xavfsizligini ta'minlash ularning samaradorligi, yaxlitligi va tizimdagi nosozliklar, kiberhujumlar va ruxsatsiz kirish kabi xavflarga chidamliligini ta'minlash uchun muhim ahamiyatga ega.

Axborot tizimlarining ishonchliligi deganda axborot tizimining o'z vazifalarini xatolarsiz, uzluksiz bajarish qobiliyati tushuniladi. Ishonchli tizimlar axborot tizimlarining ishlamay qolish vaqtini kamaytiradi va ma'lumotlar yaxlitligini saqlaydi. Ishonchlilikka ta'sir qiluvchi asosiy omillar: 1. Tizim arxitekturasi: Yaxshi ishlab chiqilgan arxitektura to'siqlar va tizimning ishdan chiqishini oldini oladi. 2. Ortiqchalik: zaxira tizimlari, yuklamalarni muvozanatlash va nosozliklarga chidamlilik mexanizmlari. 3. Monitoring va texnik xizmat ko'rsatish: muntazam diagnostika, yangilanishlar va oldini olish muammolarini ta'mirlash. 4. Masshtablilik: unumdorlikni pasaytirmasdan ortib borayotgan yuklamarni boshqarish uchun mo'ljallangan tizimlar.

Axborot tizimlarining xavfsizligi axborot tizimlarining maxfiyligi, yaxlitligi va mavjudligini tahdidlardan himoya qilishni o'z ichiga oladi. Asosiy xavfsizlik tamoyillari: 1. Maxfiylik: faqat ruxsat berilgan foydalanuvchilar ma'lumotlarga kirishini ta'minlash. 2. Butunlik: ma'lumotlarni ruxsatsiz o'zgartirishdan himoya qilish. 3. Mavjudlik: kerak bo'lganda ma'lumotlar va resurslar vakolatli foydalanuvchilar uchun ochiqligini ta'minlash.

Axborot xavfsizligi bo'yicha ushbu o'quv qo'llanmada axborot texnologiyalaridan foydalanishning asosiy jihatlari, shuningdek, axborot xavfsizligini ta'minlash usullari va vositalari to'liq yoritilgan.

Axborot xavfsizligi raqamli va jismoniy axborotning barcha shakllarini himoya qiladi. Kiberxavfsizlik raqamli ma'lumotlarning barcha shakllarini, jumladan, kompyuterlar, portativ qurilmalar, bulut va tarmoqlarni himoya qiladi va axborot xavfsizligining kichik to'plami deb hisoblanishi mumkin.

Axborotni kiberhujumlar, ma'lumotlarning sizib chiqishi, ijtimoiy muhandislik va kiberjinoyatlarning boshqa turlari kabi turli tahdidlardan himoya qilishga alohida e'tibor qaratilmoqda.

Ushbu o'quv qo'llanma axborot tizimlari va taxnologiyalari yo'nalishlarida tahsil oladigan informatika va axborot xavfsizligiga qiziquvchi talaba va o'qituvchilar uchun mo'ljallangan.

Введение

Информационные системы играют важную роль в поддержке принятия решений, операций и коммуникации в современных организациях. Обеспечение надежности и безопасности этих систем имеет решающее значение для обеспечения их эффективности, целостности и устойчивости к таким рискам, как системные сбои, кибератаки и несанкционированный доступ.

Надежность информационных систем означает способность информационной системы безошибочно и непрерывно выполнять свои задачи. Надежные системы сокращают время простоя информационных систем и поддерживают целостность данных. Ключевые факторы, влияющие на надежность: 1. Архитектура системы. Хорошо спроектированная архитектура предотвращает возникновение узких мест и сбоев системы. 2. Резервирование: системы резервного копирования, механизмы балансировки нагрузки и отказоустойчивости. 3. Мониторинг и обслуживание: регулярная диагностика, обновления и профилактический ремонт. 4. Масштабируемость. Системы предназначены для обработки растущих рабочих нагрузок без ущерба для производительности.

Безопасность информационных систем включает защиту конфиденциальности, целостности и доступности информационных систем от угроз. Основные принципы безопасности: 1. Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям. 2. Целостность: защита данных от несанкционированной модификации. 3. Доступность: обеспечение доступности информации и ресурсов авторизованным пользователям при необходимости.

Данное образовательное пособие по информационной безопасности полностью охватывает основные аспекты использования информационных технологий, а также методы и средства обеспечения информационной безопасности.

Информационная безопасность защищает все формы цифровой и физической информации. Кибербезопасность защищает все формы цифровых данных, включая компьютеры, портативные устройства, облако и сети, и может рассматриваться как часть информационной безопасности.

Особое внимание уделяется защите информации от различных угроз, таких как кибератаки, утечка данных, социальная инженерия и другие виды киберпреступлений.

Данное учебное пособие предназначено для студентов и преподавателей, интересующихся информатикой и информационной безопасностью, изучающих области информационных систем и технологий.

Introduction

Information systems play a vital role in supporting decision-making, operations, and communication in modern organizations. Ensuring the reliability and security of these systems is critical to ensuring their effectiveness, integrity, and resilience to risks such as system failures, cyber-attacks, and unauthorized access.

Reliability of information systems refers to the ability of an information system to perform its works without error and without interruption. Reliable systems reduce information system downtime and maintain data integrity. Key factors affecting reliability: 1. System architecture. A well-designed architecture prevents bottlenecks and system failures. 2. Redundancy: backup systems, load balancing, and fault tolerance mechanisms. 3. Monitoring and maintenance: regular diagnostics, updates, and preventive maintenance. 4. Scalability. Systems are designed to handle growing workloads without compromising performance.

Security of information systems includes protecting the confidentiality, integrity, and availability of information systems from threats. Key security principles: 1. Confidentiality: ensuring that only authorized users have access to information. 2. Integrity: Protecting data from unauthorized modification. 3. Availability: Ensuring that information and resources are available to authorized users when needed.

This educational guide to information security fully covers the main aspects of using information technology, as well as methods and means of ensuring information security.

Information security protects all forms of digital and physical information. Cybersecurity protects all forms of digital data, including computers, portable devices, the cloud, and networks, and can be considered a part of information security.

Particular attention is paid to protecting information from various threats, such as cyberattacks, data leaks, social engineering, and other types of cybercrime.

This educational guide is intended for students and teachers interested in computer science and information security, studying the fields of information systems and technology.

Amaliy ish № 1

TARMOQ SIMULYATORLARI BILAN TANISHISH. TARMOQ SIMULYATORLARI HAQIDA UMUMIY TUSHUNCHALAR, ULARNING IMKONIYATLARINI O'RGANISH. CISCO PACKET TRACERNI O'RNATISH.

Ishning maqsadi: Tarmoq simulyatorlari va emulyatorlarini o'rganish. Cisco Packet Tracer dasturini o'rnatish va ishga tushirish.

Tarmoq administratorlari va muhandislari axborot tizimlarini loyihalash, nazorat yoki tahlil qilish uchun turli xil dasturiy vositalaridan foydalanadilar. Tarmoq infratuzilmasi nosozliklari bilan to'la bo'lgan haqiqiy tarmoqlarda tajriba o'tkazmaslik uchun tarmoq administratorlari bu maqsadda tarmoqni modellashtirish vositalaridan foydalanadilar. Bunga simulyatorlar misol bo'la oladi.

Simulyator bu tizim va uning interfeyslarining harakatini taqlid qiladigan dastur hisoblanadi. Emulyator va simulyator o'rtasidagi farqni tushunish ahamiyatga ega masala hisoblanadi. Emulyatorlar kompyuter yoki boshqa qurilma modelini yaratish va uning ichida asl dasturiy ta'minotni ishga tushirish imkonini beradi. Qurilmaning barcha asosiy komponentlari, jumladan protsessor, xotira va kiritish-chiqarish qurilmalari emulyatsiya qilinadi. Cisco emulyator dasturida, marshrutizatorning modeli yaratiladi va uning ichida haqiqiy Cisco IOS operatsion tizimini ishga tushiradi. Natijada bizga kerak bo'lgan to'liq funksiyada ishlaydigan routerga ega bo'lishimiz mumkin.

GNS3 asoslari

Grafik tarmoq simulyatori (Graphical Network Simulator). GNS ingliz tilidan so'zma-so'z tarjima qilinganda, bu grafik tarmoq simulyatori manosini anglatsaham, aslida bu emulyator vazifasini bajaruvchi vosita hisoblanadi. Ushbu emulyator bizga kompyuterda turli xil tarmoq topologiyalarini modellashtirishga imkon yaratadi. Ko'p hollarda GNS har xil tarmoq texnologiyasi yoki sxemasini sinab ko'rish uchun amaliy mashg'ulot stendi vositasi sifatida foydalaniladi.

GNS3 – turli ko'rinishdagi tarmoqning topologiyalarida tarmoqda mavjud qurilmalarning o'zaro ta'sirini kuzatib borish imkonini beruvchi eng mashhur tarmoq emulyatsiyasi dasturlaridan biri bo'lib sanaladi. Xalqaro sertifikatlashtirish o'qitish tarmog'ining integratsiyalashgan segmentida ushbu emulyator dasturiy ta'minot vositasi bo'lib hisoblanadi. Tarmoqni muvaffaqiyat bilan modellashtirish kerak bo'lganda, ushbu dasturiy vosita zamonaviy va hamma tushunadigan bo'lib hisoblanadi. Emulyatorni o'rnatish va dastur interfeysida ishlash qulay bo'lganligi, uni havaskorlar va professionallar orasida eng ommabop tanlovlardan biriga aylantirdi.



1.1-rasm - GNS3 emulyatori

EVE-NG: Emulated Virtual Environment Next Generation yoki EVEN-NG - bu o'ziga o'xshash simulyator turlari orasida, uncha katta bo'lmagan korxonalar hamda va jismoniy shaxslar uchun mo'ljallangan ko'p foydalanuvchili tarmoq simulyatori bo'lib hisoblanadi. Ushbu simulyatorida virtual tarmoqni modellashtirishni amalga oshirish ham pullik, ham bepul bo'lishi mumkin. Bepul versiyada har bir amaliy mashg'ulot ishi uchun 63 tagacha uzeldan foydalanish mumkin. Tarmoqda qurilmalarni virtualizatsiya qilish, ulash va sozlash uchun serverga qo'shimcha ravishda dasturni yuklab olish va o'rnatishning hojati yo'q. Tarmoqda topologiyalarini loyihalash, ularning ulanishi va boshqaruvi integratsiyalangan HTML5-mijozi yordamida osonlik bilan amalga oshirish mumkin.



1.2-rasm - EVE-NG simulyatori

EVE-NGni tarmoqni modellashtirishda eng yaxshi vositalaridan biriga aylantiruvchi muhim omil shundaki, dastur bir vaqtning o'zida tarmoqlar topologiyasiga o'zgartirishlar kiritish imkonini berib, vaqtni tejaydi. Bundan tashqari, u Ethernet va ketma-ket interfeyslar uchun ham mos keladi.

Va oxirigisi, Cisco Packet Tracer - bu ma'lumotlarni uzatish tarmog'i simulyatori bo'lib hisoblanadi va Cisco Systems tomonidan ishlab chiqarilgan. Cisco simulyatori, qo'llanilishi mumkin bo'lgan tarmoq modellarini yaratish, marshrutizatorlar va kommutatorlarni sozlash (Cisco IOS buyruqlari yordamida) va bir nechta foydalanuvchilar o'rtasida (bulut orqali) o'zaro aloqada bo'lish imkonini beradigan dastur bo'lib hisoblanadi.

Simulyator bir qator Cisco 800, 1800, 1900, 2600, 2800, 2900 marshrutizatorlarini va Cisco Catalyst 2950, 2960, 3560 kommutatorlarini, shuningdek, ASA 5505 xavfsizlik ekrani bilan ishlash amalga oshirilgan. Simsiz qurilmalar Linksys WRT300N routeri, kirish nuqtalari va uyali aloqa minoralari bilan ifodalanadi. Bundan tashqari, DHCP, HTTP, TFTP, FTP, DNS, AAA,

SYSLOG, NTP va EMAIL serverlari, ish stantsiyalari, kompyuterlar va marshrutizatorlar uchun turli modullar, IP telefonlar, smartfonlar, hublar, shuningdek, WANni emulyatsiya qiluvchi bulutlar mavjud. To'g'ridan-to'g'ri va teskari patch kabellar, optik va koaksiyal kabellar, ketma-ket kabellar va telefon juftlari kabi turli xildagi kabellar yordamida tarmoq qurilmalarini ulash imkoni mavjud.



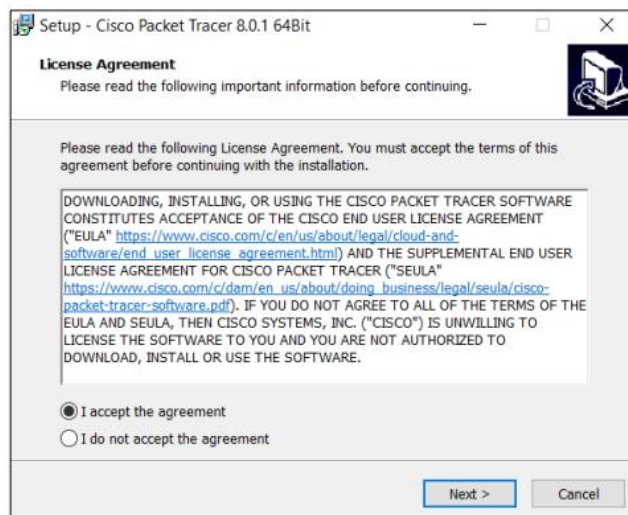
1.3-rasm - Cisco Packet Tracer Simulator

Bu simulyator hatto murakkab tarmoq sxemalarini yaratish va tarmoq topologiyasini ishlash qobiliyatini tekshirish imkonini beradi. Biroq, qurilmalarning amalga oshirilgan funkcionalligi cheklangan va haqiqiy uskunaning barcha imkoniyatlarini ta'minlay olmaydi. Cisco Packet Tracer dasturidan Cisco Networking Academy dasturi ishtirokchilari bepul foydalanishlari mumkin.

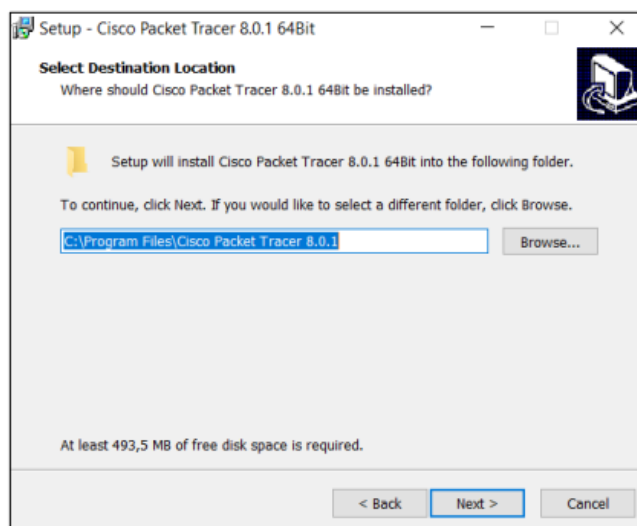
Cisco Packet Tracer ning o'quv jarayonida GNS3 ga nisbatan asosiy afzalligi shundaki, GNS3 da kommutatorlar yo'q, bundan tashqari GNS3 tizimi kompyuter resurslariga ham yuqori talablarga ega. Shuning uchun ushbu fanimizda amaliy ishlarni bajarosh Cisco Packet Tracer simulyatorida ishlashga asoslangan.

Cisco Packet Tracer 8-avlodini kompyuterga o'rnatish. Dasturning so'nggi versiyasini olish uchun Cisco Network Academyda ro'yxatdan o'tishimiz kerak, so'ngra "setup.exe" o'rnatish faylini yuklab olgandan so'ng, uni ishga tushirishimiz kerak.

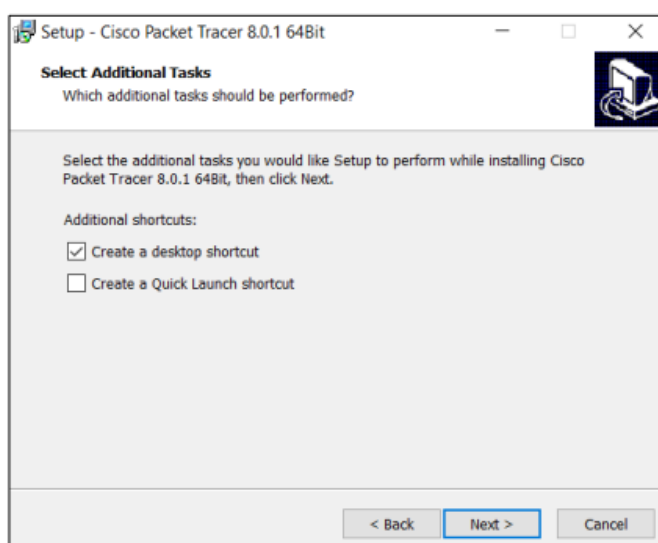
Setup.exe dasturini ishga tushirgandan so'ng, o'rnatish ustasi paydo bo'ladi:



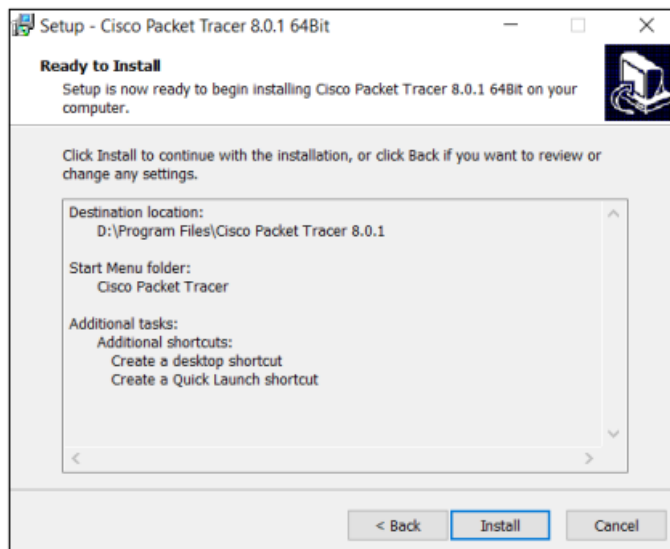
1.4-rasm. Litsenziya shartnomasi



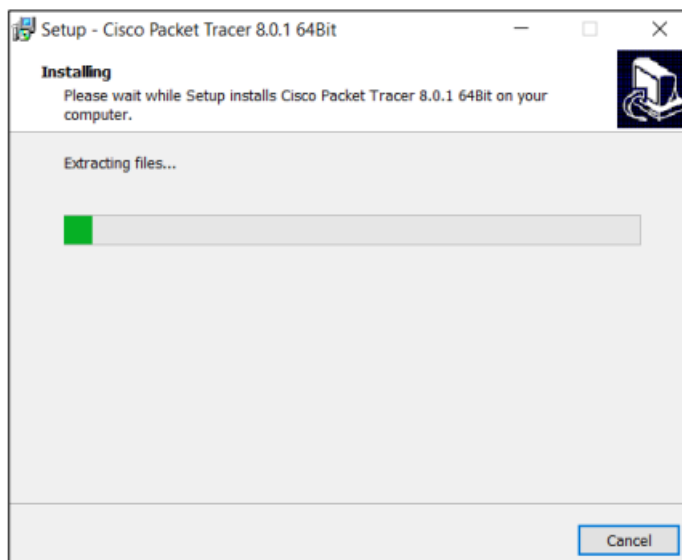
1.5-rasm - O'rnatish uchun katalogni tanlash.



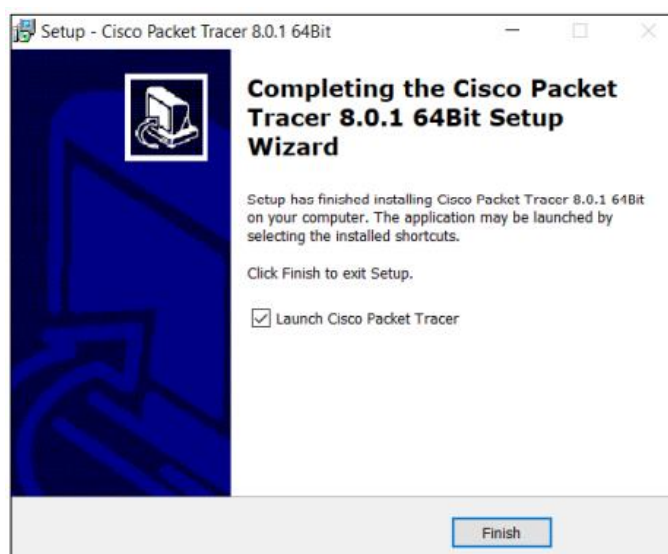
1.6-rasm - Qo'shimcha o'rnatish sozlamalari.



1.7-rasm - O'rnatish sozlamalarini tasdiqlash.



1.8-rasm - O'rnatish jarayoni.



1.9-rasm - O'rnatishning tugashi.

Dasturni ishga tushirgandan so'ng, foydalanuvchi o'z akkauntini Networking Academy yoki Skills for All bilan avtorizatsiya qilishi kerak.



1.10-rasm - Dasturni ishga tushirish. Avtorizatsiya



1.11-rasm – Dasturning ishchi oynasi

1-amaliy ish mashg'ulotiga topshiriq:

Kompyuteringizda yoki noutbukingizda Cisco Packet Tracer simulyatorini o'rnatib. Hamda dastur interfeysi bilan tanishib chiqing.

Nazorat savollari:

1. "Tarmoqni modellashtirish" deganda nimani tushunasiz?
2. Modellashtirish so'zi yana qayerlarda ishlatiladi?
3. GNS3 haqida nimani bilasiz.
4. Cisco Packet Tracer nima va uni nima maqsadlarda qo'llaymiz.
5. EVE-NG haqida nima bilasiz?
6. Cisco Packet Tracer ning GNS3 va EVE-NG ga nisbatan afzalliklarini sanab bering.

Amaliy ish № 2

CISCO KOMMUTATORLARI BUYRUQ INTERFEYSI BILAN ISHLASH VA BOSHLANG'ICH KONFIGURATSIYANI SOZLASH. CISCO PACKET TRACERDA LAN TARMOQINI LOYIHALASH VA QURISH

Ishning maqsadi: Cisco Packet Tracer dasturida LAN mahalliy tarmoqni loyihalash va qurishni o'rganish.

LAN qisqartmasi **Local Area Network** - ulangan qurilmalar o'rtasida aloqa o'rnatish imkonini beruvchi qurilma tarmog'idir. LAN oddiygina tarmoq orqali bir-biriga ulangan va bir xil jismoniy joyda - odatda bitta binoda, masalan, ofis yoki uyda joylashgan kompyuterlar va boshqa qurilmalar guruhi sifatida ta'riflanadi. Ammo keling, biroz chuqurroq o'rganaylik.

Mahalliy tarmoq deganda nimani tushunamiz?

LAN (Local Area Network) — bu kompyuterlar va boshqa qurilmalarni bir-biriga bog'lab, kichik geografik hududda (odatda bir bino yoki bir nechta yaqin binolarni o'z ichiga olgan hududda) faoliyat yuritadigan tarmoq turi. LAN, ko'pincha ofislar, maktablar, fabrikalar, yoki uylar kabi kichik hududlarda ishlatiladi.

LANning asosiy xususiyatlari:

1. **Geografik hudud:** LAN odatda kichik hududlarda ishlaydi. Misol uchun, bir ofis yoki binoda bir necha kompyuterlar va qurilmalarni bog'lash uchun ishlatiladi. LANning kattaligi bir necha yuz metr yoki bir necha kilometr bo'lishi mumkin, lekin u asosan bir yoki bir nechta bino ichida bo'ladi.
2. **Yuqori tezlik:** LANlar odatda yuqori tezlikda ma'lumot uzatishni ta'minlaydi. Ethernet va Wi-Fi texnologiyalari orqali bu tezlik 1 Gbps dan ortiq bo'lishi mumkin.
3. **Resurslarni baham ko'rish:** LAN yordamida foydalanuvchilar bir-birlariga fayllar, printerlar, skanerlar va boshqa resurslarni osonlik bilan baham ko'rish imkoniyatiga ega bo'lishadi.
4. **Arzon narxdagi qurilmalar:** LAN tarmoqlarida ishlatiladigan qurilmalar nisbatan arzon va o'rnatish oson bo'ladi. Masalan, Ethernet kabeli yoki Wi-Fi routerlar arzon va keng tarqalgan qurilmalardir.
5. **Tarmoq qurilmalar:** LANda ishlatiladigan qurilmalar quyidagilardan iborat bo'lishi mumkin:
 - **Switch (Kommutator):** Bu qurilma tarmoqdagi kompyuterlar va boshqa qurilmalar o'rtasidagi ma'lumotlarni yo'naltiradi. Switch orqali kompyuterlar o'rtasida ma'lumot almashish amalga oshiriladi.
 - **Router (Yo'riqchi):** LAN tarmog'ini tashqi tarmoqlarga (masalan, Internetga) ulash uchun ishlatiladi.
 - **Access Point (AP):** Wi-Fi tarmog'ini yaratish uchun ishlatiladi.
 - **Modem:** Internetga ulanish uchun tarmoqqa kirish nuqtasi bo'ladi.
6. **Tarmoqning ishonchliligi va xavfsizligi:** LANlar, odatda, yuqori xavfsizlikni ta'minlash uchun maxsus texnologiyalarga ega. Kompyuterlar o'rtasida xavfsiz ma'lumot almashish uchun turli shifrlash, autentifikatsiya va foydalanuvchi huquqlari tizimlari qo'llaniladi.

LAN tarmog'ining tuzilishi

LAN tarmog'i bir nechta tarmoq komponentlari yordamida tashkil etiladi:

1. **Kabel tizimi:** LANda kabel orqali bog‘lanish keng tarqalgan. Ethernet kabeli (CAT5e, CAT6 kabi) tarmoqdagi qurilmalar o‘rtasida ma'lumotlarni uzatadi.
2. **Wi-Fi tarmog‘i:** Boshqa LAN tarmoqlariga o‘xshash holda, Wi-Fi tarmoqlari simsiz bog‘lanishni ta'minlaydi. Wi-Fi tarmoqlari mobil qurilmalar va noutbuklar kabi qurilmalarning simsiz ulanishini ta'minlaydi.
3. **IP manzillar:** Tarmoqda har bir qurilmaga yagona IP manzil beriladi. Bu tarmoqdagi har bir qurilma uchun identifikatsiya vositasi bo‘lib, ma'lumotlar uzatish va qabul qilishda muhim rol o'ynaydi.
4. **Tarmoq protokollari:** LANlar Ethernet va Wi-Fi kabi protokollarni ishlatadi. Bu protokollar tarmoqdagi qurilmalar o‘rtasida ma'lumot uzatishni boshqaradi. TCP/IP protokoli ko‘pincha LAN tarmog‘ida asosiy protokol sifatida ishlatiladi.

LAN tarmog‘ini o‘rnatish

LAN tarmog‘ini yaratish jarayonida quyidagi bosqichlar amalga oshiriladi:

1. **Tarmoq qurilmalarini tanlash:** Switch, router, access point kabi qurilmalarni tanlash zarur.
2. **Kabel va simsiz ulanishni tashkil etish:** Ethernet kabeli yoki Wi-Fi tizimini o‘rnatish.
3. **Tarmoqni sozlash:** IP manzillarini tayinlash va tarmoq konfiguratsiyasini sozlash.
4. **Xavfsizlikni ta'minlash:** Firewally o‘rnatish, autentifikatsiya va parol xavfsizligi bilan himoya qilish.

LANning afzalliklari

1. **Tezlik:** LAN tarmoqlari yuqori tezlikda ishlaydi, bu esa ma'lumotlarni tez uzatishni ta'minlaydi.
2. **Ishlab chiqarish samaradorligi:** Resurslar, masalan, printerlar, serverlar va ma'lumotlar bazalarini bir tarmoq orqali baham ko‘rish ish samaradorligini oshiradi.
3. **Arzon xarajatlar:** LANni yaratish va saqlash nisbatan arzon.

LANning kamchiliklari

1. **Cheklangan masofa:** LAN faqat kichik hududda ishlaydi, bu esa katta hududlarga tarqalishiga to‘sqinlik qiladi.
2. **O‘zgartirishlar talab qiladi:** Yangi qurilmalarni tarmoqqa qo‘shish yoki kengaytirish jarayoni tarmoqning mavjud tuzilishini o'zgartirishni talab qiladi.
3. **Xavfsizlik xatarlari:** Agar xavfsizlik choralari yetarli bo‘lmasa, LANga hujumlar va noto'g'ri foydalanishlar yuzaga kelishi mumkin.

LANning turlari

- **Ethernet LAN:** Bu LAN turida simli ulanishlar ishlatiladi. Ethernet tarmog‘ining yuqori tezlikdagi uzatish imkoniyatlari mavjud.
- **Wi-Fi LAN:** Simsiz tarmoq bo‘lib, Wi-Fi texnologiyasi yordamida qurilmalar bir-biriga ulanishi mumkin.

LAN — bu kichik hududdagi tarmoq bo‘lib, foydalanuvchilarga o‘zaro ma'lumot almashish, umumiy resurslarga (printerlar, fayl serverlari) kirish, va

Internetga ulanish imkoniyatlarini taqdim etadi. LANlar yuqori tezlikda ishlaydi va arzon narxlarda o'rnatilishi mumkin, ammo ular faqat kichik hududda samarali ishlaydi.

Kommutator yoki Switch

Switch yoki **Tarmoq kommutatori** (Inglizchadan. Switch - kommutator) bu bitta tarmoq segmentida kompyuter tarmog'ining bir nechta tugunlarini ulash uchun mo'ljallangan qurilma bo'lib, bitta ulangan qurilmadan boshqalarga trafikni yuboradigan hubdan farqli o'laroq, ma'lumotlarni faqat qabul qiluvchiga yuboradi. Barcha tarmoq tugunlariga translyatsiya qilingan trafik (MAC manziliga FF:FF:FF:FF:FF:FF) bundan mustasno. Natija esa tarmoq unumdorligi va xavfsizligini oshirish, boshqa segmentlarni ularga murojaat qilinmagan ma'lumotlarni qayta ishlash zarurati yoki imkoniyatlaridan chiqarib tashlashdir.

Kommutatorni ishlash jarayoni

Kommutatorning (kommutatorning) ishlash printsipli paketli kommutatsiya texnologiyasidan foydalangan holda mahalliy tarmoq (LAN) ichida ma'lumotlarni uzatishga asoslangan. Kommutator OSI modelining ikkinchi qatlamida (ma'lumotlar havolasi qatlami) ishlaydi, bu unga tarmoqdagi qurilmalarning MAC manzillari asosida ma'lumotlar uzatishni boshqarish imkonini beradi.

Kommutatorning ishlashining asosiy tamoyillari

1. MAC manzillar jadvalini shakllantirish:

Qurilma kalitga ulanganda va ma'lumotlarni yuborganda, kalit Ethernet ramka sarlavhasidan jo'natuvchining MAC manzilini o'qiydi.

U o'zining ichki MAC manzillar jadvaliga manzilni ma'lum bir port bilan bog'laydigan yozuvni qo'shadi.

Ushbu jadval dinamik ravishda yangilanadi va har bir qurilma qaysi port orqali kirish mumkinligi haqidagi ma'lumotlarni saqlaydi.

2. Ma'lumot uzatish:

Ma'lumotlar ramkasi qabul qilinganda, kalit MAC manzilini aniqlash uchun uning sarlavhasini tahlil qiladi.

Keyin ushbu manzilni MAC manzillar jadvali bilan taqqoslaydi:

Agar manzil topilsa, ramka faqat mos keladigan portga yo'naltiriladi.

Agar manzil noma'lum bo'lsa, ramka qabul qilingan portdan tashqari barcha portlarga (efirga) yuboriladi.

3. Trafik izolyatsiyasi:

Kommutator ma'lumotlarni boshqa portlarga ta'sir qilmasdan ikkita qurilma o'rtasida uzatish imkonini beradi.

Bu tarmoqdagi nizolar (to'qnashuvlar) sonini kamaytiradi, tarmoqli kengligidan samarali foydalanishni ta'minlaydi.

4. Translyatsiya xabarlarini qayta ishlash:

Agar kadr translyatsiya qilingan MAC manziliga (masalan, FF:FF:FF:FF:FF:FF) yo'naltirilgan bo'lsa, u barcha portlarga uzatiladi.

Bu tarmoqdagi qurilmalarni topish yoki DHCP orqali IP manzilini olish kabi vazifalar uchun zarur.

Kommutatorlarning asosiy funksiyalari:

1. Paketlarni almashtirish: kadrlarni faqat kerakli portga yo'naltiradi.
2. To'qnashuvni minimallashtirish: tarmoqni alohida to'qnashuv domenlariga bo'lish.
3. Yaxshilangan tarmoq ishlashi: tarmoqli kengligidan samarali foydalanish.
4. VLAN boshqaruvi (boshqariladigan kommutatorlar uchun): Tarmoqni VLAN-larga bo'lish.
5. Qo'shimcha funktsiyalar: QoS (xizmat sifati), portni aks ettirish, kirishni boshqarish va boshqalar.

Kommutatorlarning xususiyatlari va turlari

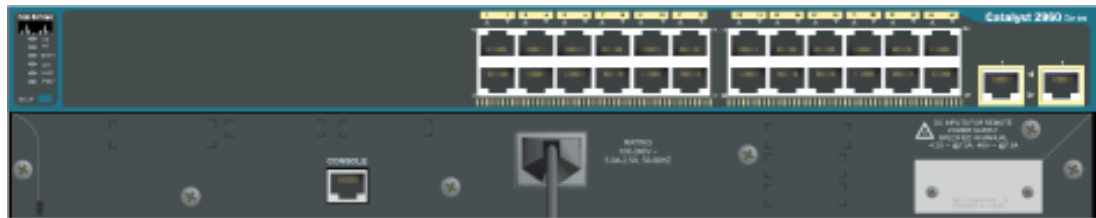
	
Модели общего назначения	Модели Fast Ethernet
<ul style="list-style-type: none">• Gigabit Ethernet (GE) для нужд высокой пропускной способности• 8 x, 16 x, 24 x или 48 x данных GE или нисходящие каналы PoE+• 2 или 4 фиксированных восходящих канала 1 GE SFP• Без вентилятора (кроме модели с 48 портами PoE)• Бюджет мощности до 740 Вт	<ul style="list-style-type: none">• Совместимость с устаревшей кабельной инфраструктурой• 24 x или 48 x 10/100 Мбит/с для передачи данных или нисходящих каналов PoE+• 4 x GE SFP и 2 x RJ-45 комбинированных восходящих канала• Безвентиляторный (24-портовые модели)• Беспроводной Bluetooth-доступ

2.1-rasm Cisco kommutatorlari va ularning xarakteristikasi

Ko'pgina boshqariladigan kommutatorlar qo'shimcha funktsiyalarga ega va ular quyidagilar: VLAN, QoS, yig'ish, aks ettirish. Murakkab kommutatorlarni bitta mantiqiy qurilmaga birlashtirish mumkin - portlar sonini ko'paytirish uchun (masalan, siz 4 ta kommutatorni 24 port bilan birlashtirib, $(4 * 24 - 6 = 90)$ portli yoki 96 port bilan (agar stacking uchun maxsus portlar ishlatilsa) mantiqiy kommutatorni olishingiz mumkin. Amaliy ishlarning aksariyati Cisco Catalyst 2960 model switchida amalga oshiriladi.



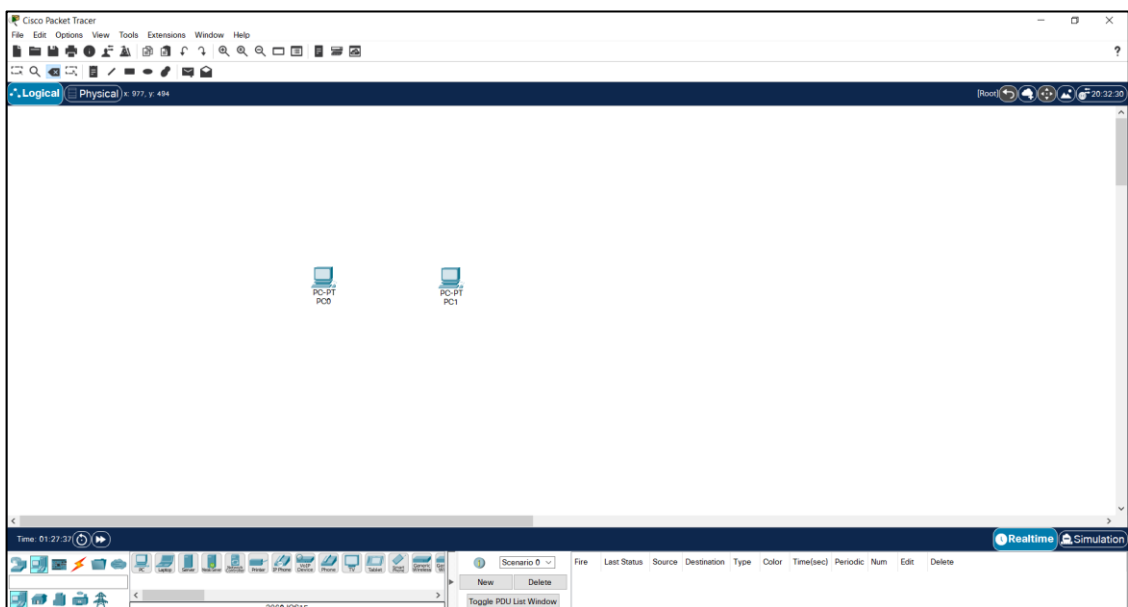
2.2 –rasm. Cisco Catalyst 2960 kommutatori



2.3-rasm. Cisco Packet Tracerdagi Cisco Catalyst 2960 kommutatorining orqa paneli

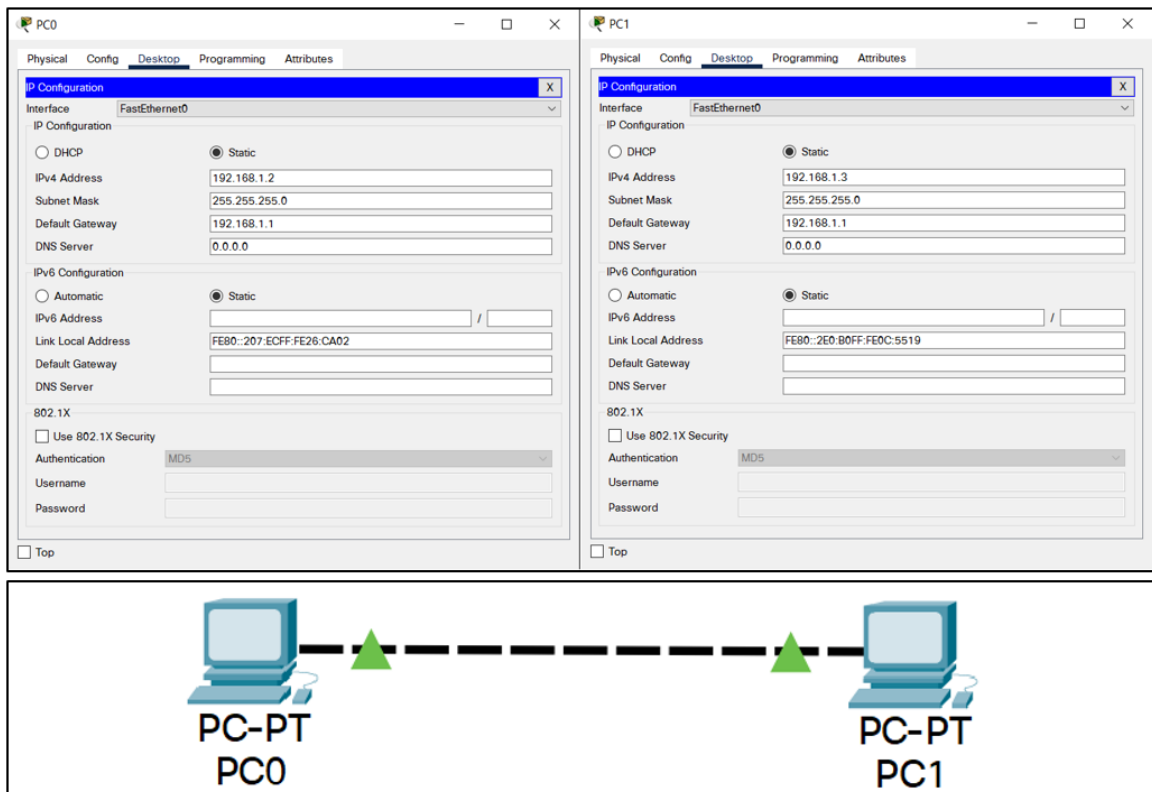
Ishning amaliy qismi:

Cisco Packet Tracerni dasturini oching. Chapda turgan pastki uskunalar panel qismidan End devices (oxirgi qurilmalar) ro'yxatini ochamiz. Oddiy shaxsiy kompyuterni tanlaymiz va ishchi oynaga ikkita shaxsiy kompyuterni sichoqchening chap tugmasini bosgan holda keltiramiz. (2.4-rasm)



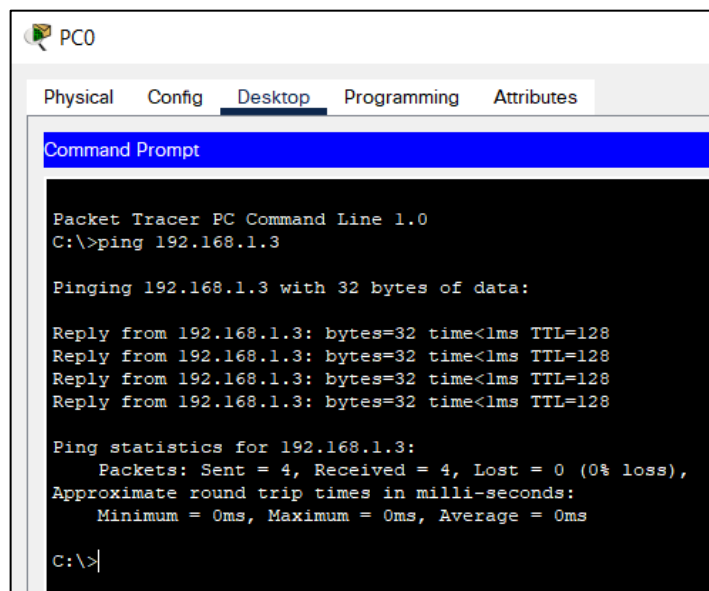
2.4-rasm - Cisco Packet Tracer ishchi sohasi.

So'ngra ikkala shaxsiy kompyuterda IP-manzil va pastki tarmoq niqobini sozlash uchun ularga ma'lumot kiritamiz. Shundan so'ng kompyuterlarni bir-biriga kabel orqali ulaymiz. (2.5-rasmga qarang)



2.5-rasm. Kompyuterda IP manzillarni o'rnatish va ularni bir-biriga ulash.

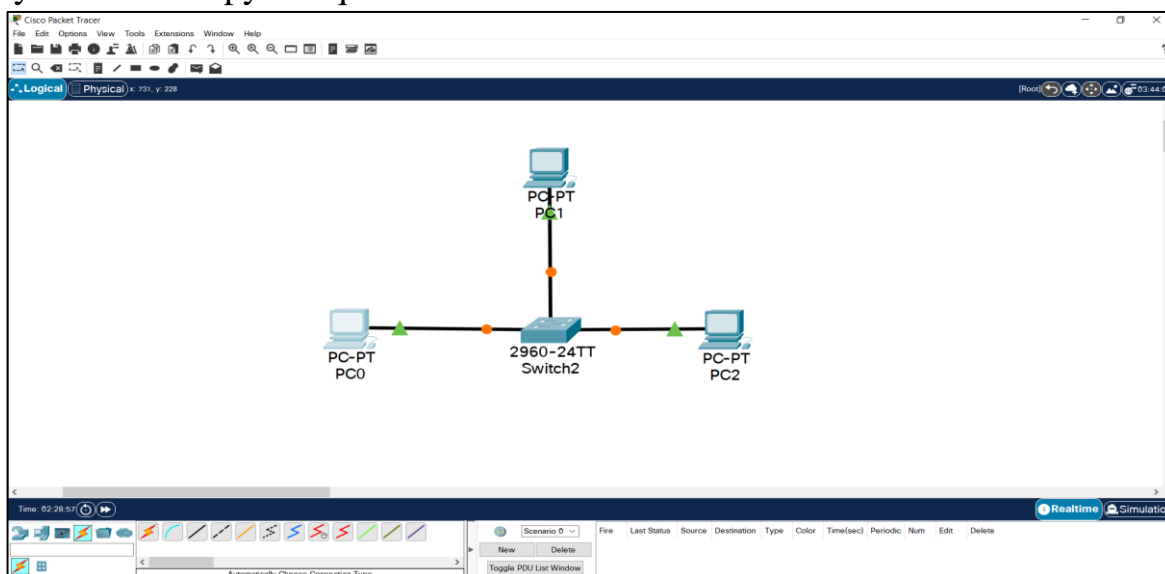
Kompyuterlarning Command prompt sozlamasiga kirib Ping orqali ulanishni tekshirish. Agar qutilma to'g'ri sozlangan bo'lsa, unda yo'qolgan paketlar bo'lmaydi (Yo'qotilgan = 0) yoki 50% dan kam (ba'zan uzatish paytida paket yo'qolishi mumkin) bo'lishi talab etiladi.



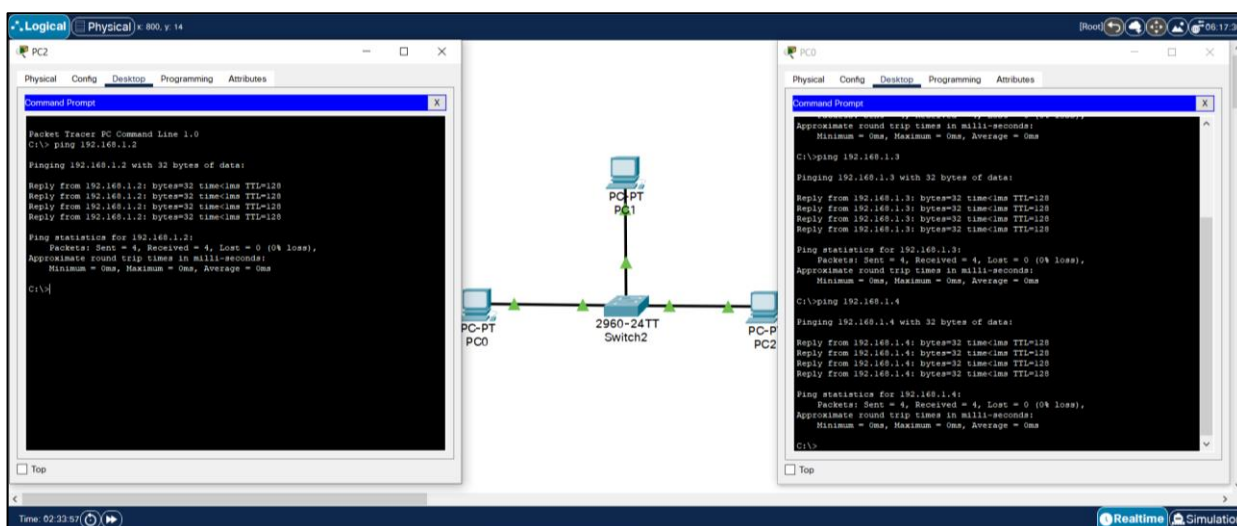
2.6-rasm - PC0 dan PC1 Ping berib ko'rish.

Keyinchalik, xuddi shu uskunalar panelida, tarmoq uskunalari bo'limiga o'tamiz va Cisco Catalyst 2960 model kommutatorini tanlaymiz. Uni ish maydoniga

o'tkazamiz. Bir-biridan oldin ulangan shaxsiy kompyuterlar kommutatorga ulanadi va yana 1 ta kompyuter qo'shiladi.



2.7-rasm. Kommutator orqali ulangan 3 ta shaxsiy kompyuterdan iborat tarmoq.



2.8-rasm. Portlarning ko'tarilishini kutmoqdamiz (to'q sariq nuqta o'rniga yashil uchburchaklar yonadi) va tugallangan tayyor uskunalar ping orqali tekshiriladi.

C:\>ping 192.168.0.3 //Ulanish tekshirilmoqda

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168. 0.3: bytes=32 time<1ms TTL=128

Reply from 192.168. 0.3: bytes=32 time<1ms TTL=128

Reply from 192.168. 0.3: bytes=32 time<1ms TTL=128

Reply from 192.168. 0.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168. 0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168. 0.4

Pinging 192.168. 0.4 with 32 bytes of data:

Reply from 192.168. 0.4: bytes=32 time<1ms TTL=128

Reply from 192.168. 0.4: bytes=32 time<1ms TTL=128

Reply from 192.168. 0.4: bytes=32 time<1ms TTL=128

Reply from 192.168. 0.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168. 0.4:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

2-sonli Amaliy mashg'ulotga topshiriq:

- Kommutator orqali ulangan 2.1-jadvalda berilgan variant bo'yicha N ta kompyuterdan iborat tarmoqni tuzing.
- Jadvaldan tanlanadigan Variantlar bo'ticha kompyuterlarga IP manzillarni kiriting.
- Quyidagi jadvaldagi variantlar bo'yicha tarmoqni yarating.

2.1-jadval

№2 Amaliy mashg'ulotning bajarilish variantlari raqamlari

Variant	IP manzili	Variant	IP manzili
1.	192.168.10. ...	16.	192.168.25. ...
2.	192.168.11. ...	17.	192.168.26. ...
3.	192.168.12. ...	18.	192.168.27. ...
4.	192.168.13. ...	19.	192.168.28. ...
5.	192.168.14. ...	20.	192.168.29. ...
6.	192.168.15. ...	21.	192.168.30. ...
7.	192.168.16. ...	22.	192.168.31. ...
8.	192.168.17. ...	23.	192.168.32. ...
9.	192.168.18. ...	24.	192.168.33. ...
10.	192.168.19. ...	25.	192.168.34. ...
11.	192.168.20. ...	26.	192.168.35. ...
12.	192.168.21. ...	27.	192.168.36. ...
13.	192.168.22. ...	28.	192.168.37. ...
14.	192.168.23. ...	29.	192.168.38. ...
15.	192.168.24. ...	30.	192.168.39. ...

Nazorat savollari:

1. LAN deganda nimani tushunasiz?
2. Kommutator qanday ishlashini tushuntirib bering.
3. Cisco Catalyst 2960 kommutatorini tavsiflang va nimaga aynan ushbu kommutatordan foydalanganligimizni tushuntiring.

4. Kommutator yoki switch nima?
5. Kommutatorlarning qanday turlarini bilasiz?

Amaliy ish № 3

CISCO PACKET TRACERDA TELNET, SSH PROTOKOLLARINI O'RGANISH. TELNET VA SSH PROTOKOLLARI YORDAMIDA QURILMALARNI SOZLASH.

Ishning maqsadi: Cisco packet tracerda Telnet, SSH orqali kommutator va routerga ulanishni o'rnatish.

Telnet - Telnet (TELEcommunication NETwork) - matnga asoslangan interfeys orqali qurilmalarni masofadan boshqarish uchun ishlatiladigan protokol. Bu buyruqlarni kiritish va ularni bevosita ularning oldida turgandek boshqarish uchun masofaviy serverlar yoki qurilmalarga ulanish imkonini beradi.



3.1-rasm – Tarmoqni TELNET orqali ulanishi

Telnet qanday ishlaydi?

1. Foydalanuvchi o'z qurilmasida Telnet mijozini ishga tushiradi.
2. Ulanmoqchi bo'lgan server yoki qurilma manzilini kiriting.
3. TCP orqali masofaviy qurilma bilan aloqa o'rnatiladi (odatda 23-portda).
4. Muvaffaqiyatli autentifikatsiyadan so'ng foydalanuvchi masofaviy qurilmaning buyruq qatoriga kirish huquqiga ega bo'ladi.
5. Mijozga kiritilgan buyruqlar serverga yuboriladi, u ularni qayta ishlaydi va javob qaytaradi.

Telnetning asosiy xususiyatlari:

1. Matn interfeysi:
 - Telnet buyruq qatoriga kirishni ta'minlaydi.
 - Foydalanuvchi buyruqlarni bajarishi, qurilmalarni sozlashi, ma'lumotlarni qabul qilishi va hokazo.
2. Ilova darajasida ishlash:
 - Telnet dastur darajasida ishlaydi (OSI modelining 7-qatlami).
 - Transport protokoli sifatida TCP dan foydalanadi, odatda 23 porti orqali.
3. Shifrlash yo'q:
 - Ma'lumotlarni uzatish (shu jumladan login va parollar) shifrlanmagan shaklda amalga oshiriladi.

- Bu Telnet-ni zamonaviy tarmoqlarda, ayniqsa ommaviy yoki ishonchsiz muhitlarda foydalanish uchun xavfli qiladi.

Telnet qayerda ishlatiladi?

1. Tarmoq qurilmalarini boshqarish:

- Kalitlar, marshrutizatorlar, serverlar va boshqa qurilmalar.

2. Tarmoq diagnostikasi:

- Portlar, ulanishlar va xizmatlar mavjudligini tekshirish.

3. Eski tizimlarni boshqarish:

- Ba'zi eski tizimlar va qurilmalar faqat Telnet-ni qo'llab-quvvatlaydi.

Telnetning afzalliklarga foydalanish osonligi, qurilmalarni ulash va boshqarish osonligi, izolyatsiya qilingan, ishonchli tarmoqlarda foydalanish uchun javob berishini misol qilib keltirsa bo'ladi.

Ammo shunga qaramay Telnetning bir qancha kamchiliklari mavjud, bular:

- Shifrlash yo'q: Hamma narsa aniq matnda uzatiladi.

- Hujumlarga qarshi zaiflik: Loginlar, parollar va ma'lumotlarni snifferlar yordamida osongina ushlab olish mumkin.

- Eskirish: Zamonaviy tizimlarda Telnet SSH (Secure Shell) kabi xavfsizroq protokollar bilan almashtirilmoqda.

Secure Shell (SSH) - kriptografik tarmoq protokoli bo'lib, qurilmalar, serverlar va ma'lumotlar uzatishni xavfsiz masofadan boshqarishni ta'minlaydi. SSH ulanishni shifrlashni ta'minlaydi, uzatilgan ma'lumotlarni (jumladan, loginlar, parollar va buyruqlar) ushlab va buzishdan himoya qiladi.

SSH ning asosiy xususiyatlari:

1. Xavfsizlik:

- Barcha ma'lumotlar shifrlangan shaklda uzatiladi.

- simmetrik va assimetrik shifrlash usullaridan, shuningdek, ma'lumotlarni himoya qilish uchun xeshlashdan foydalanadi.

2. Ko'p qirralilik:

- Tizimlarni masofadan boshqarishni qo'llab-quvvatlaydi.

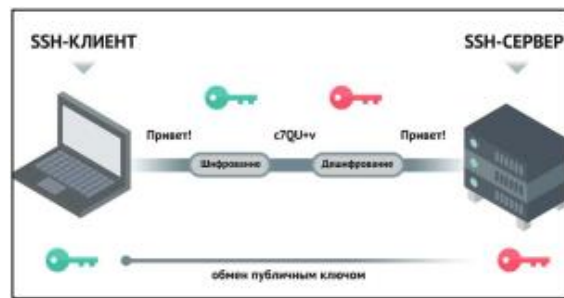
- Fayllarni xavfsiz uzatish uchun foydalanish mumkin (SCP yoki SFTP orqali).

- Boshqa tarmoq ulanishlarini himoya qilish uchun tunnellarini (portni yo'naltirish) yaratishga imkon beradi.

3. Ilova darajasida ishlash:

- SSH OSI modelining 7-qatlamida ishlaydi.

- Odatda port 22 (standart), lekin xavfsizlikni yaxshilash uchun portni o'zgartirish mumkin.



3.2-rasm - SSH ishlash prinsipi.

SSH qanday ishlaydi?

1. Aloqa o'rnatish:

- SSH mijoz (masalan, Linuxda `ssh`) SSH serveriga ulanishni boshlaydi.
- Server mijozga ma'lumotlarni shifrlash uchun foydalaniladigan o'zining ochiq kaliti bilan ta'minlaydi.

2. Autentifikatsiya:

- Mijoz autentifikatsiyadan foydalanishi mumkin:
- Parol (kamroq xavfsiz usul).
- SSH kalitlari (afzal usul): mijoz bir juft kalitni yaratadi - shaxsiy va ochiq.

Ochiq kalit serverga uzatiladi va shaxsiy kalit faqat mijozda qoladi.

3. Ma'lumotlar almashinuvi:

- Xavfsiz kanal o'rnatilgach, barcha ma'lumotlar (shu jumladan buyruqlar, javoblar va fayllar) shifrlangan holda uzatiladi.

SSH qayerda ishlatiladi

1. Server boshqaruvi:

- SSH tizim ma'murlariga dunyoning istalgan nuqtasidan serverlarni xavfsiz boshqarish imkonini beradi.

2. Fayl uzatish:

- Ma'lumotlarni uzatish uchun ****SCP (Secure Copy)**** va ****SFTP (Secure File Transfer Protocol)**** protokollaridan foydalanish.

3. Tunnellash (portni yo'naltirish):

- SSH tunnel orqali boshqa ulanishlarni (masalan, ma'lumotlar bazasi, veb-ilovalar) himoya qilish.

4. Vazifalarni avtomatlashtirish:

- SSH masofaviy buyruqlarni avtomatlashtirilgan tarzda bajarish uchun skriptlarda qo'llaniladi.

SSH ning afzalliklari:

- Shifrlash va ma'lumotlarni himoya qilish.
- Kalitlar orqali autentifikatsiya (parollarga qaraganda xavfsizroq).
- Moslashuvchanlik va tunnel ochish kabi ilg'or xususiyatlar.
- Deyarli barcha operatsion tizimlarni qo'llab-quvvatlaydi.

SSH kamchiliklari:

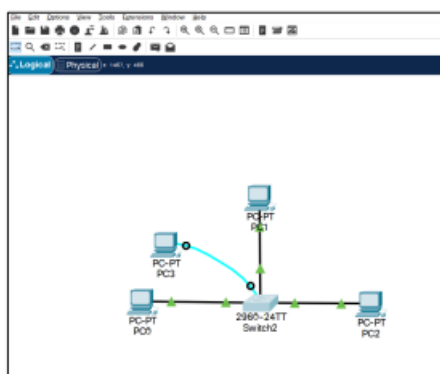
- Agar to'g'ri sozlanmagan bo'lsa, hujumlarga qarshi zaif bo'lishi mumkin (masalan, qo'pol kuch).
- Ikkala tomondan (mijoz va server) o'rnatish va sozlashni talab qiladi.

- Agar shaxsiy kalitingizni yo'qotib qo'ysangiz, yuzaga kelishi mumkin bo'lgan muammolar.

Ishning amaliy qismi.

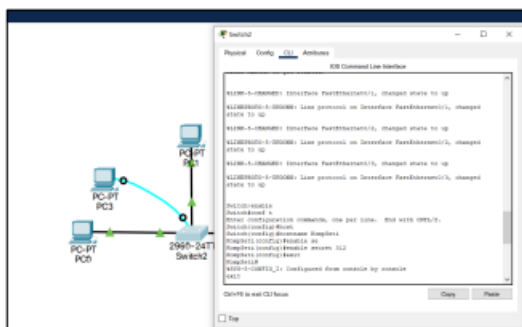
Ulanishni Telnet protokoli orqali sozlash.

Dastlab 2-sonli Amaliy mashg'ulotda ishlab chiqilgan kichik tarmoq qurilgan faylni oching. Kommutatorni sozlash uchun yangi PC3 ni qo'shing va konsol kabeli orqali kommutatorga ulang (3.3-rasm). Buni amalga oshirish uchun siz konsol simini PC3-dagi "RS232" portiga va kommutatordagi "Konsol" portiga ulashingiz kerak:



3.3-rasm – PC3 ni konsol kabeli orqali kommutatorga ulash.

Avvalo, kompyuter konsoli orqali kirish uchun kommutator nomini belgilashingiz va parolni o'rnatishingiz kerak (3.4-rasm).



3.4-rasm – Kommutatorga kirish uchun nom va parolni belgilash.

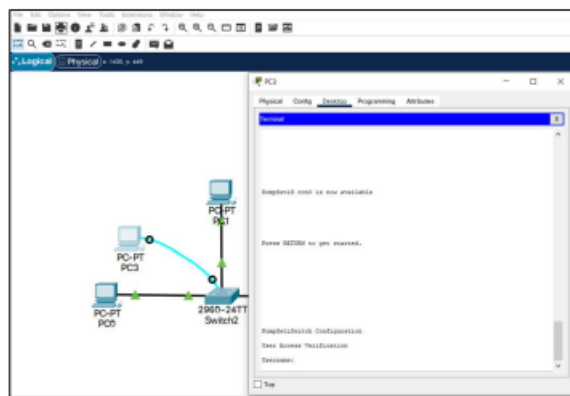
Kommutatorni oching, CLI bo'limiga o'ting va quyidagi sozlamalarni kiriting:


```

Switch>enable (en)
// Imtiyozli rejimga kiring
Switch#config terminal (conf t)
//Global konfiguratsiya rejimiga kiring
Switch(config)#hostname KompTarmoqS
//Uskunaga nom berish
KompTarmoqS(config)#enable secret 312
//Parol yarating. Maxfiy (Secret) va parol o'rtasidagi farq shundaki, maxfiy
(secret) shifrlangan va parol shifrlangan emas.
KompTarmoqS(config)#exit
// konfiguratsiya daraxti orqali orqaga qadam qo'ying

```

Keyinchalik, biz PC3 ga kiramiz (3.5-rasm), konsolni ochamiz, buning uchun siz yuqori yorliqda tanlashingiz kerak: Desktop → Terminal → OK.



3.5-rasm – Kompyuter konsolidan kommutatordagi sozlamalarning to'g'riligini tekshirish.

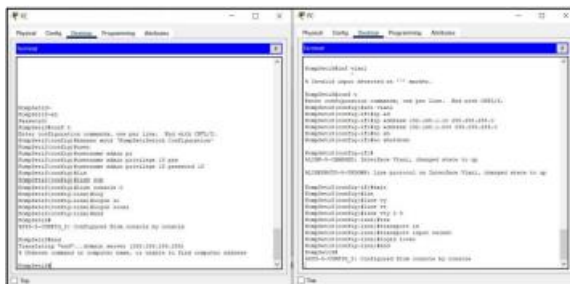
Global konfiguratsiya rejimiga o'tamiz (3.6-rasm), 'KompTarmoqSwitch Configuration' deb nomlangan banner yaratamiz, foydalanuvchi nomi "admin", "15" parolini o'rnatamiz, shuningdek, qurilmaga masofadan kirish uchun "15" imtiyoz darajasini o'rnatamiz. Bundan tashqari, masofadan boshqarish uchun login local buyrug'i yordamida foydalanuvchi autentifikatsiya usulini ko'rsatishingiz kerak.

```

KompTarmoqS(config)#banner motd 'KompTarmoqSwitch Configuration'
//banner yarating
KompTarmoqS(config)#username admin privilege 15 password 15
//Login, imtiyozlar darajasi va parolni sozlash
KompTarmoqS(config)#line console 0
//Konsol uchun chizikli konfiguratsiya rejimi, "0" birinchi konsol interfeysi
KompTarmoqS(config-line)#login local
//Mahalliy akkaunt ma'lumotlar bazasi yordamida autentifikatsiyani sozlash
KompTarmoqS(config-line)#end
//Konfiguratsiya rejimidan to'liq chiqish

```

Avvalo Vlan1ni yaratamiz va switch uchun IP-manzilni "192.168.1.20" kiritamiz, bir qancha sozlashlardan so'ng masofadan kirish turida Telnet protokolini o'rnatamiz (3.6-rasm).



3.6-rasm – Telnet orqali kommutatorga PC3 ulanishini sozlash.

```
KompSeti(config)# interface vlan 1
//Interfeys konfiguratsiya rejimidan foydalangan holda Vlan 1 portini sozlang
KompTarmoqS(config-if)#ip address 192.168.1.20 255.255.255.0
//Portga IP-manzilni belgilash (manzil, niqob)
KompTarmoqS(config-if)#no shutdown
// Yoqish interfeysi ( ko'tarish interfeysi )
KompTarmoqS(config-if)#exit
KompTarmoqS(config)#line vty 0 4
//Vty kanaliga masofadan kirishga ruxsat beruvchi 0 dan 4 gacha parol
tayinlang
KompTarmoqS(config-line)#transport input telnet
//Telnet protokolini ulanish uchun sozlash
KompTarmoqS(config-line)#login local
KompTarmoqS(config-line)#end
```

Kompyuterning buyruq qatori orqali "PC3" (3.7-rasm) biz terminalda yozgan kodlarning to'g'riligini, shuningdek Telnet protokoli sozlamalarini tekshiramiz.

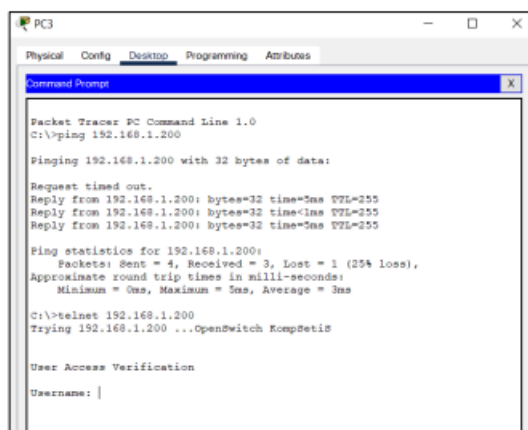
Buni amalga oshirish uchun avval IP-manzil ping buyrug'i yordamida kommutatorga to'g'ri tayinlanganligini tekshiring:

```
C:\>ping 192.168.1.20
```

Keyinchalik, biz Telnet protokoli yordamida ulanishlarni tekshiramiz:

```
C:\>telnet 192.168.1.20
```

```
Trying 192.168.1.20 ... KompTarmoqSwitch Configuration
```



3.7-rasm – “ping” va “telnet” orqali tekshirish

SSH orqali ulanishni o'rnatish:

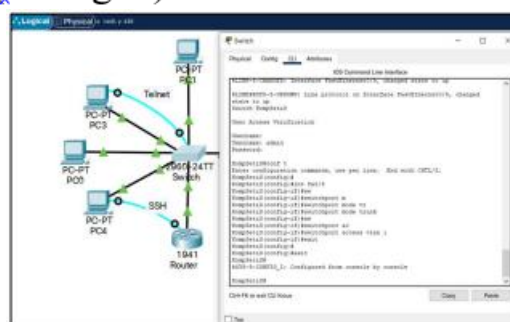
Dastlab oxirgi foydalanuvchilar panelidan (PC4) ni tanlab olamiz so'ngra maydonga Routerni qo'shamiz, qo'shilgan PC4 hamda router kommutatorga misi kabel Ethernet orqali ulanishi kerak. PC4 bilan routerga konsol kabelini ulashingiz talab etiladi. Biz oxirgi qo'shilgan kompyuterdan routerda SSH protokolni sozlash uchun foydalanamiz. Marshrutizatorning keyingi sozlamasi kompyuteri (PC3) orqali davom ettiriladi.

Ishning keying qismida kommutatordan (3.8-rasm) routerga ulangan portlarni ko'tarishimiz kerak bo'ladi:

```

KompTarmoqS(config)#int fastethernet0/5
//Fastethernet0/5 portini magistral rejimiga sozlash
KompTarmoqS(config-if)#switchport mode trunk
//Magistral rejim uchun portni sozlash
KompTarmoqS(config-if)#exit

```



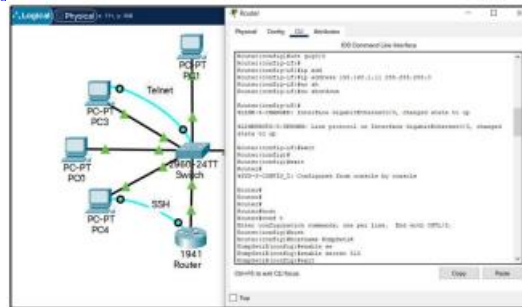
3.8-rasm – PC4 ni routerga konsol kabeli yordamida ulash. Kommutatorni sozlash.

Shundan so'ng, kompyuter konsoli orqali kirish uchun IP manzilini, router nomini va parolni o'rnatishingiz kerak. Routerni ochgandan so'ng (3.9-rasm), CLI bo'limiga o'ting va quyidagi sozlamalarni kiriting:

```

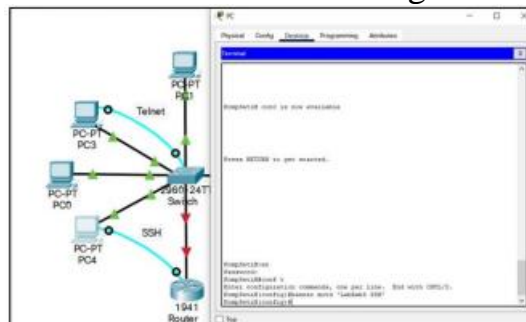
Router>en
Router#conf t
Router (config)#hostname KompTarmoqR
KompTarmoqR(config)#enable secret 312
KompTarmoqR(config)#int gig0/0
KompTarmoqR(config-if)#ip address 192.168.1.21 255.255.255.0
KompTarmoqR(config-if)#no shutdown
KompTarmoqR(config-if)#exit

```



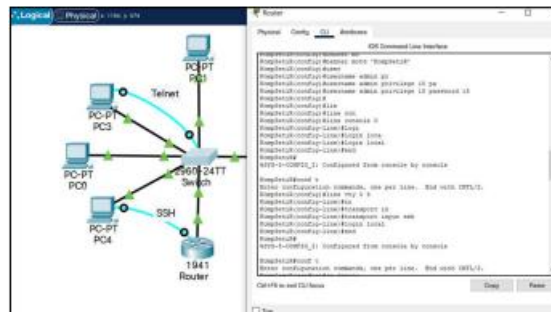
3.9-rasm – Routerga kirish uchun nom va parolni belgilash.

Keyin, kompyuter PC4ga kiring (3.10-rasm), konsolni oching, buning uchun yuqori yorliqda Desktop → Terminal → OK ni tanlang.



3.10-rasm – Routerda kompyuter konsolidan to'g'ri sozlamalarni tekshirish.

Administrator akkauntini yarating va parol va imtiyozlar darajasini o'rnating (3.11-rasm):



3.11-rasm – Akkaunt qaydnomasini yaratish va masofadan kirishni sozlash

```

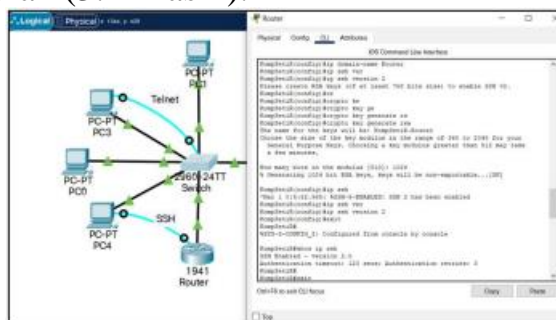
KompTarmoqR(config)#banner motd 'KompTarmoqRouter Configuration'
KompTarmoqR(config)#username admin privilege 15 password 15

```

Biz virtual ulanishni ko'taramiz, terminal liniyalari konfiguratsiyasini kiritamiz va masofaviy ulanish turini (SSH) tanlaymiz:

```
KompTarmoqR(config)#line console 0
KompTarmoqR(config-line)#login local
KompTarmoqR(config-line)#end
KompTarmoqR(config)#int vlan 1
KompTarmoqR(config)#line vty 0 4
KompTarmoqR(config-line)#transport input ssh
//Ssh ulanish protokolini sozlash
KompTarmoqR(config-line)#login local
KompTarmoqR(config-line)#end
```

SSH protokoli orqali ulanishni o'rnatish uchun siz domen nomini (Router) o'rnatishingiz, kriptografik kirish kalitini yaratishingiz va SSH protokolining 2-versiyasini yoqishingiz kerak (3.12-rasm).

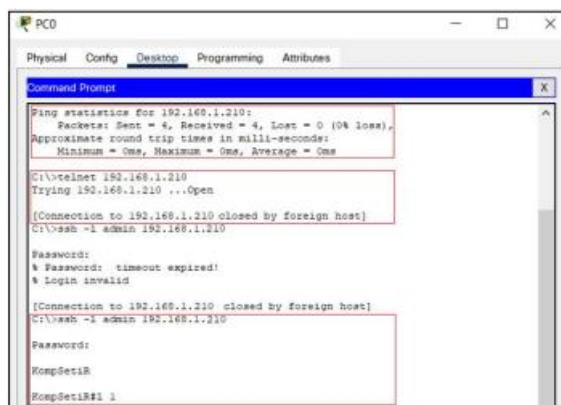


3.12-rasm – SSHni sozlash

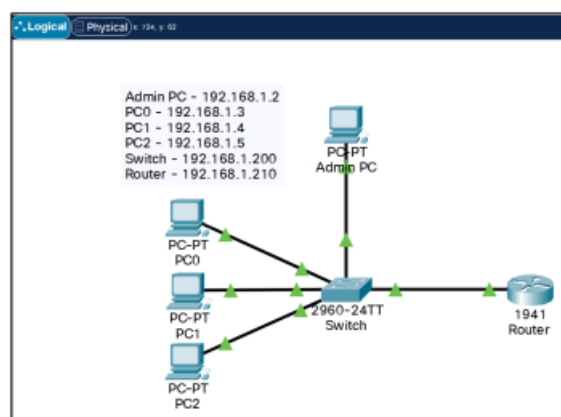
```
KompTarmoqR(config)#ip domain-name Router
KompTarmoqR(config)#ip ssh version 2
KompTarmoqR(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
% 1024 bitli RSA kalitlari yaratilayotganda kalitlar eksport qilinmaydi...[OK]
KompTarmoqR(config)#ip ssh version 2
*Mar 1 0:47:18.582: %SSH-5-ENABLED: SSH 2 has been enabled
```

Routerga masofadan kirishni ssh protokoli orqali tekshiramiz. Birinchidan, biz Ping buyrug'idan foydalanamiz (3.13-rasm), keyin biz Telnet protokoli orqali ulanishga harakat qilamiz, biz muvaffaqiyatsizlikni ko'ramiz, shundan so'ng biz ssh protokoli orqali ulanishga harakat qilamiz.

```
C:\>ping 192.168.1.21
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\>telnet 192.168.1.21
Trying 192.168.1.21...Open
[Connection to 192.168.1.21 closed by foreign host]
C:\>ssh -l admin 192.168.1.21
Password: «parolni kiritamiz»
KompTarmoqR#
```



3.13 –rasm. SSH orqali masofadan kirishni tekshirish



3.14-rasm – Tarmoqning yakuniy versiyasi.

4-sonli Amaliy mashg'ulotning oxirida (3.14-rasm), barcha konsol kabellarini olib tashlagan holda, bizda quyidagi IP manzillari va nomlari bilan 1 ta kommutator, 1 ta router va 4 ta kompyuterni o'z ichiga olgan tarmoq mavjud bo'ladi:

Yo'q.	Ism	IP manzili
1	Switch (KompTarmoqS)	192.168.1.20
1	Router (KompTarmoqR)	192.168.1.21
1	Administrator kompyuteri	192.168.1.2
2	Kompyuter 0	192.168.1.3
3	Kompyuter 1	192.168.1.4
4	Kompyuter 2	192.168.1.5

Switch (KompTarmoqS): Username: admin; Password: 15

Router (KompTarmoqR): Username: admin; Password: 15

3-sonli Amaliy mashg'ulotga topshiriq:

- Administrator kompyuterdan Telnet yordamida kommutatorga ulanishni o'rnatish;
- Administrator kompyuterdan SSH orqali routerga ulanishni o'rnatish;
- Keyingi amaliy ishlarini bajarish uchun tarmoqni tayyorlang.

Nazorat savollari

- 1.Nima uchun Telnet protokoli kerak?
- 2.Telnet protokolidan foydalanishning afzalligi nimada?
- 3.Telnet va SSH o'rtasidagi farq nima?
- 4.Nima uchun Telnet xavfsizlik xavfi hisoblanadi?
- 5.SSH protokolidan foydalanishning afzalligi nimada.

Amaliy ish № 4

CISCO ROUTERLARINING BUYRUQ INTERFEYSI BILAN ISHLASH VA DASTLABKI KONFIGURATSIYANI SOZLASH. CISCO PACKET TRACERDA VLANNI LOYIHALASH

Ishning maqsadi: Cisco Packet Tracerda VLAN orqali tarmoq qurish.

VLAN (inglizcha “Virtual Local Area Network” dan) — virtual mahalliy tarmoq bo‘lib, jismoniy tarmoqni bir nechta mantiqiy izolyatsiya qilingan tarmoqlarga bo‘lish imkonini beradi. Bunga qurilmalarni jismoniy joylashuvidan qat'i nazar, bitta virtual tarmoqqa guruhlash orqali erishiladi. VLAN-lar tarmoq infratuzilmasida tarmoqlarning xavfsizligi, ishlashi va boshqarilishini yaxshilash uchun keng qo'llaniladi.

VLAN ning asosiy xususiyatlari:

1. Mantiqiy ajratish: Bir xil kalitga ulangan qurilmalar turli VLAN-larga birlashtirilishi mumkin va aksincha, turli VLAN-larning qurilmalari turli kalitlarda bo'lishi mumkin.

2. Traffic izolyatsiyasi: Xuddi shu VLANdagi qurilmalar muloqot qilishi mumkin, lekin aniq konfiguratsiya qilinmasa (masalan, marshrutlash orqali) bitta VLANdan boshqasiga trafik yuborilmaydi.

3. Yaxshilangan xavfsizlik: Tarmoqni VLAN-larga bo'lish turli segmentlar o'rtasida ma'lumotlarni ajratishga yordam beradi, bu esa ma'lumotlarning sizib chiqishi xavfini kamaytiradi.

4. Yaxshilangan samaradorlik: VLAN translyatsiya domenining hajmini kamaytirish imkonini beradi, bu esa tarmoqdagi yukni kamaytiradi.

5. Boshqaruv moslashuvchanligi: Administratorlar jismoniy ulanishlarni o'zgartirmasdan qurilmalarni VLAN-lar o'rtasida osongina ko'chirishlari mumkin.

VLANning ishlatilishiga misol:

Aytaylik, kompaniyada uchta bo'lim mavjud: buxgalteriya, IT va marketing. Uchta VLAN (masalan, VLAN 10, VLAN 20 va VLAN 30) yaratish orqali siz tarmoqni har bir bo'limning o'z izolyatsiyalangan tarmog'iga ega bo'lishi uchun ajratishingiz mumkin, garchi hammaning qurilmalari bir xil jismoniy kommutatorga ulangan bo'lsa ham.

Ishlash texnologiyasi:

- VLAN teglari: IEEE 802.1Q standartidan foydalanilganda, Ethernet freym sarlavhasiga maxsus VLAN tegi qo'shiladi, bu freym qaysi VLANga tegishli ekanligini ko'rsatadi.

- Darajalar: VLAN OSI modelining ikkinchi qatlamida ishlaydi (bog'lanish qatlami).

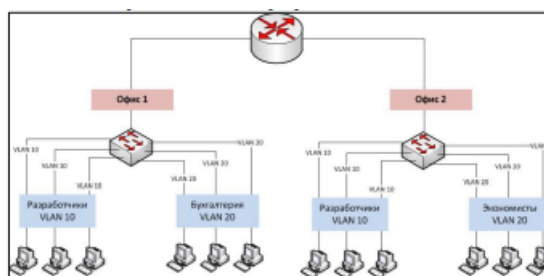
- VLAN-lar orasidagi marshrutlash: VLAN-lar o'rtasida ma'lumotlarni uzatish uchun odatda yo'riqnoma yoki L3 kaliti ishlatiladi.

Sozlamalar:

1. VLAN-lar kommutatorlarda yaratiladi (masalan, CLI buyruqlari yoki boshqaruv interfeysi orqali).

2. Kommutator interfeyslari maxsus VLAN-larga tayinlangan.

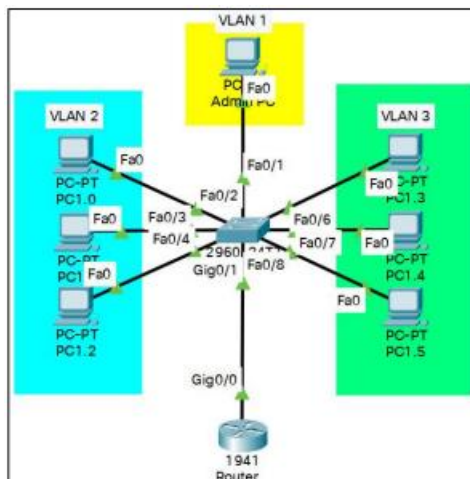
3. (Ixtiyoriy) VLAN-lar orasidagi marshrutlash, agar ma'lumotlar almashinuvi zarur bo'lsa, sozlanadi.



4.1-rasm – Tarmoqni korxonada misolida VLAN lar orqali segmentlarga ajratish.

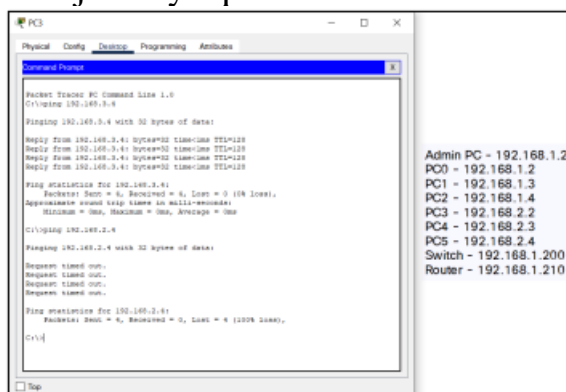
Ishning amaliy qismi

3-sonli Amaliy mashg'ulot oxirida tayyorlangan loyihalangan tarmoqni ochamiz (4.2-rasm). Ushbu tarmoqqa yana 3 ta kompyuterni qo'shamiz va kommutatorda VLAN-ni sozlashni davom ettiramiz. Oldin tarmoqni bir nechta qismlarga bo'lishimiz kerak bo'ladi. Keling, Bosh (ya'ni ma'mur) kompyuterni VLAN1 da qolganligi uchun unga tegmaymiz. 3 ta chapda o'rnatilgan kompyuterlarni VLAN2 ga, 3 ta o'ngda o'rnatilgan kompyuterlarni VLAN3 ga bog'laymiz. Natijada, tarmoqdagi kompyuterlar tomonidan kommutator va router konfiguratsiyasini o'zgartirish imkoniyatini beramiz, bu esa loyihalangan tarmoqlarning xavfsizligini oshiradi.



4.2-rasm – Tarmoqning pastki VLANlarga vizual bo'linishi.

Kompyuterlarda IP manzillarini (pastki tarmoq qiymatlarini) o'zgartirgandan so'ng, "ping" buyrug'i bilan turli tarmoq segmentlari orasidagi ulanishlarni tekshiramiz. Birinchi bo'lib PC3 - PC5 dan ping berib tekshirib ko'ramiz, pastdagi skrinshotda ko'rib turganimizdek, ping muvaffaqiyatli javob qaytdi (4.3-rasm). Keyinchalik, biz boshqa tarmoq segmentida joylashgan kompyuterga ping qo'yamiz, shundan so'ng PC3 - PC2 dan ping berib tekshiramiz, skrinshotda ko'rib turganimizdek, ping berganda javob yo'q.



4.3-rasm – “ping” buyrug'i yordamida tekshirish

"Ping" buyrug'i bilan tekshirishni tugatgandan so'ng, biz turli xil pastki tarmoqlardagi yoki turli jismoniy jihozlarga ulangan kompyuterlar o'rtasidagi o'zaro ta'sirni ta'minlash uchun kommutatorlarda VLAN pastki tarmoqlarini sozlashni davom ettiramiz. Buni amalga oshirish uchun Administrator kompyuteridan kommutator sozlamalariga o'ting va ikkita yangi VLAN yarating.

```
C:\>telnet 192.168.1.20
```

```
Trying 192.168.1.20 ...Open KompTarmoqSwitch
```

```
Configuration
```

```
User Access Verification
```

```
Username: admin
```

```
Password:
```

```
KompTarmoqS#conf t
```

```
KompTarmoqS(config)#vlan 2
```

```
// VLAN 2ni sozlash
```

```
KompTarmoqS(config-vlan)#name VLAN2
```

```
// VLAN 2ga nom berish
```

```
KompTarmoqS(config-vlan)#exit
```

```
// VLAN 2ning sozlashidan chiqish
```

```
KompTarmoqS(config)#vlan 3
```

```
KompTarmoqS(config-vlan)#name VLAN3
```

```
KompTarmoqS(config-vlan)#exit
```

VLAN- larga ulangan portlarni tayinlaymiz (4.4-rasm):

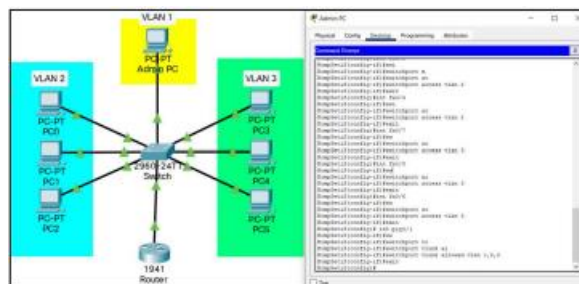
- 1-port sukut bo'yicha Vlan 1 da qoladi
- 2, 3, 4 portlar Vlan 2 ga tayinlangan
- 6, 7, 8 portlar Vlan 3 ga tayinlangan

Buning uchun biz yozamiz:

```
KompTarmoqS(config)#int fa0/2
KompTarmoqS(config-if)#switchport mode access
//Portni kirish rejimiga o'tkazing
KompTarmoqS(config-if)#switchport access vlan 2
KompTarmoqS(config-if)#exit
```

VLANlar o'rtasida ma'lumot almashish uchun yo'riqnoma ulangan portni sozlaymiz, buning uchun biz yozamiz:

```
KompTarmoqS(config)# int fa0/1
KompTarmoqS(config-if)#switchport mode trunk
KompTarmoqS(config-if)#switchport trunk allowed vlan 1,2,3
Vlan 1,2,3 dan paketlarni uzatishga ruxsat beramiz
KompTarmoqS(config-if)#exit
```



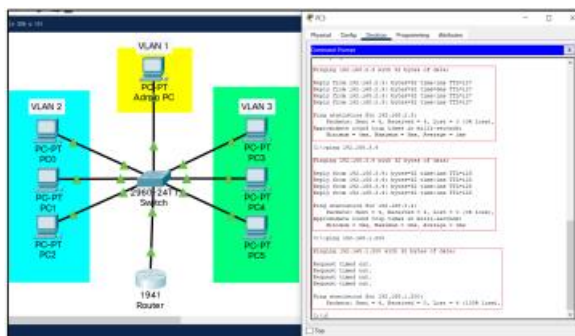
4.4-rasm – VLAN 2, 3 ni sozlash

Keyinchalik, turli tarmoq segmentlari (turli VLANlar) bitta port orqali ma'lumotlarni almashishi uchun yo'riqnomadagi inkapsulyatsiya sozlamalariga o'tamiz.

```
KompTarmoqR(config)#int gig0/0.2
KompTarmoqR(config-subif)#encapsulation dot1Q 2
//dot1Q inkapsulyatsiyasi (IEEE 802.1q ning qisqa versiyasi)
KompTarmoqR(config-subif)#ip address 192.168.2.1 255.255.255.0
KompTarmoqR(config-subif)#no shutdown
KompTarmoqR(config-subif)#exit
KompTarmoqR(config)#int gig0/0.3
KompTarmoqR(config-subif)#encapsulation dot1Q 3
KompTarmoqR(config-subif)#ip address 192.168.3.1 255.255.255.0
KompTarmoqR(config-subif)#no shutdown
KompTarmoqR(config-subif)#exit
```

Routerning asosiy porti boshqaruvchi shaxsiy kompyuter joylashgan VLAN1 quyi tarmog'iga sozlanganligi sababli, u uchun virtual port yaratishga hojat yo'q. Bundan tashqari, VLAN1 uchun inkapsulyatsiyasiz, kommutator sozlamalariga

kirish cheklangan edi. Turli pastki tarmoqlar orasidagi pingni tekshiramiz (4.5-rasm).



4.5-rasm. Konfiguratsiya qilingan VLAN pastki tarmoqlarini tekshirish.

Ushbu Amaliy mashg'ulot yakunida 1 ta kommutator, 1 ta router va 7 ta kompyuterni o'z ichiga olgan tarmoq mavjud bo'lib, ular 3 ta segmentga bo'lingan, quyidagi IP manzillari, nomlari va VLANlari mavjud:

Yo'q.	Ism	IP manzili	VLAN №
1	Switch (KompTarmoqS)	192.168.10.20	1
1	Router (KompTarmoqR)	192.168.10.21	1
1	Administrator kompyuteri	192.168.10.2	1
2	PC0	192.168.20.2	2
3	PC 1	192.168.20.3	2
4	PC 2	192.168.20.4	2
5	PC3	192.168.30.2	3
6	PC4	192.168.30.3	3
7	PC5	192.168.30.4	3

Switch (KompTarmoqS): Username: admin; Password: 15

Router (KompTarmoqR): Username: admin; Password: 15

4-sonli amaliy mashg'ulot topshirig'i:

- Qurilgan tarmoqqa qo'shimcha kompyuterlar qo'shing;
- Yuqorida tavsiflangan misol bo'yicha butun tarmoqni 3 xil VLANga bo'ling;
- Keyingi amaliy ishlarini bajarish uchun tarmoqni tayyorlang.

Nazorat savollari:

1. VirtLAN deganda nimani tushunasiz?
2. Enkapsulyatsiya nima?
3. VLANdan qo'llashning asosiy afzalliklari nimada?
4. VLANni ishlatilishiga misollar keltiring.
5. Cisco-da port terminologiyasini tavsiflang.

Amaliy ish №5

KORXONA VA TASHKILOTLARNING KOMPYUTER TARMOG'INI LOYIHALASH

Ishdan maqsad: Korporativ kompyuter tarmoqlari qurish asoslarini o'rganish, tarmoqqa qo'yiladigan talablarni ishlab chiqish va korxonada tarmog'ida foydalaniladigan texnologiya va protokollarni tadqiq etish.

Nazariy ma'lumot

Korporativ kompyuter tarmog'ini loyihalash prinsiplari quyidagilarni o'z ichiga oladi:

1. Tarmoq arxitekturasi: Kompyuter tarmog'ini loyihalash va ishlab chiqish jarayoni tarmoq arxitekturasi deb ataladi². Arxitektura tushunchasi tarmoqning fizik tarkibiy qismlarini, ularning funktsional ob'ektlari, konfiguratsiyasini, prinsiplari va ishlash tartiblarini va foydalaniladigan aloqa protokollarini aniqlashni ifodalaydi.

Tarmoq arxitekturasi shuningdek, tarmoq arxitekturasi aloqa tarmog'i orqali taqdim etiladigan xizmatlar va ularning batafsil tavsiflarini, taqdim etiladigan xizmatlarni hisob-kitob qilish va hisob-kitob tuzilmalarini o'z ichiga oladi.

Tarmoq arxitekturasi eng ko'p ishlatiladigan ikki turi mavjud: peer-to-peer va mijoz-server¹. Global miqyosidagi kompyuter tarmoqlarining o'zaro bog'lanishi natijasida Internet tarmog'i tashkil topadi¹. Internet tarmog'ining arxitekturasi, avvalambor, tarmoqdagi tugunlarni yoki tugunlarni ulash uchun ma'lum bir modelda yoki apparat ulanishlarining ma'lum turlarida foydalanishda emas, balki Internet protokollari (TCP/IP) arxitekturasiidan foydalanishni ifodalaydi.

Har bir texnologiya orqali loyihalashtiriladigan tarmoq o'zining arxitekturasi ega bo'ladi, masalan, OSI, TCP/IP, umumfoydalanish telefon tarmog'i, mobil aloqa tarmoqlari va boshqalari

2. Mahalliy korporativ tarmoqni loyihalash va yaratish: Korporativ tarmoqni loyihalash jarayoni kompaniya tarkibidagi bo'limlarning mahalliy tarmoqlarini birlashtirish va korxonaning asosiy faoliyatini yanada rejalashtirish, tashkil etish va boshqarish uchun moddiy-texnika bazasini yaratishni o'z ichiga oladi.

3. Korporativ tarmoqni qurish: Foydalanuvchilar o'rtasida axborot almashinuvini ta'minlovchi ma'lumotlar, platformalar va ilovalarning izchil va rivojlangan arxitekturasi asoslanadi.

4. Ma'lumotlar bazasini saqlash va himoya qilish: Faol korporativ tarmoqni olish qo'shimcha ravishda ma'lumotlar bazasini saqlash va himoya qilish vositalarini ishlab chiqishni o'z ichiga oladi.

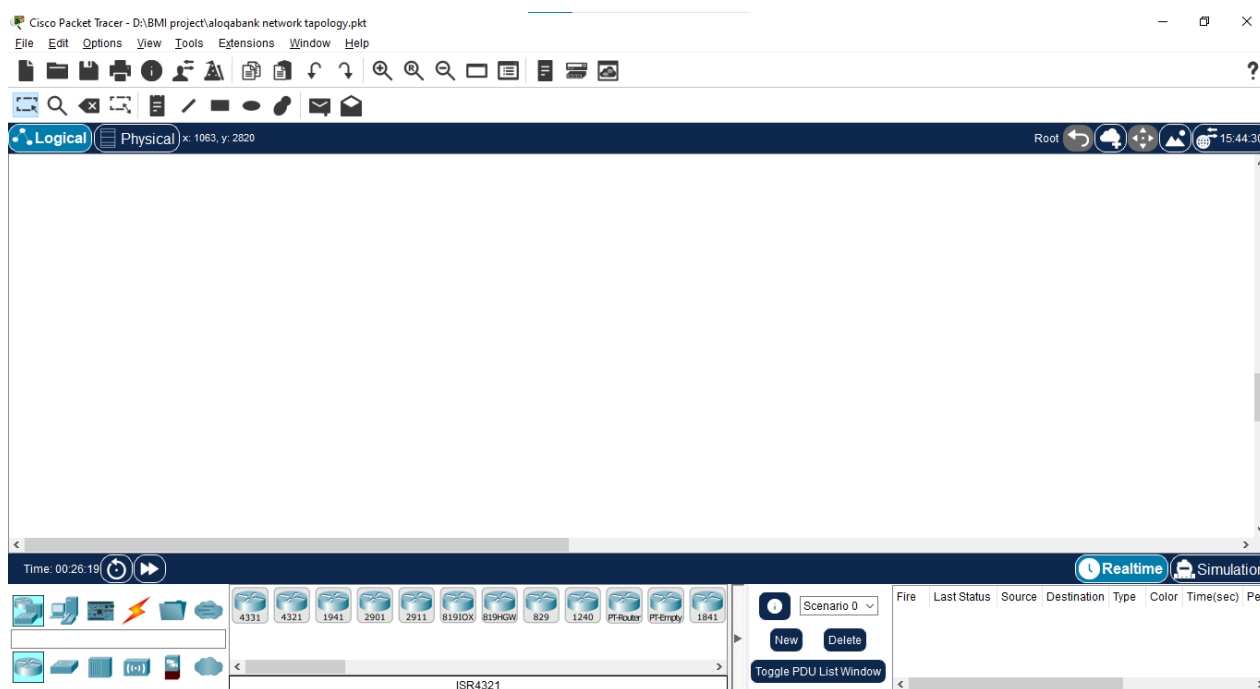
5. LAN (Local Area Network): Zarur ma'lumotlarning barqaror almashinuvini va foydalanuvchilarning kirish huquqlarini boshqarishni ta'minlaydigan mahalliy kompyuter tarmog'i.

6. SCS (Structured Cabling System): Telekommunikatsiya infratuzilmasi – kompaniyaning barcha kompyuter qurilmalari to'plami bo'lib, ular o'rtasida real vaqt rejimida ma'lumotlar almashinuvi amalga oshiriladi.

Bu prinsiplar asosida korporativ tarmoqni loyihalash va yaratish jarayoni amalga oshiriladi.

Cisco Packet Tracer simulyatorida tarmoqni qurish jarayoni

1-qadam: Cisco Packet Tracer-ni ishga tushiring va yangi bo'sh loyiha yarating. Kompyuteringizda yoki noutbukda Packet Tracer-ni ishga tushiring. Ish stolingizdagi Packet Tracer belgisini ikki marta bosib yoki Packet Tracer bajariladigan faylini o'z ichiga olgan katalogga o'ting va Packet Tracer-ni ishga tushiring. Packet Tracer rasmda ko'rsatilganidek bo'sh standart Mantiqiy topologiya ish maydoni bilan ochilishi kerak.



5.1-rasm. Yangi loyiha interfeysi

2-qadam: Topologiyani yarating. Ish maydoniga tarmoq qurilmalarini qo'shing.

Qurilmani tanlash oynasidan foydalanib, topologiya diagrammasida ko'rsatilganidek, tarmoq qurilmalarini ish maydoniga qo'shing. Qurilmani ish maydoniga joylashtirish uchun, avvalo, Qurilma turini tanlash oynasidan qurilma

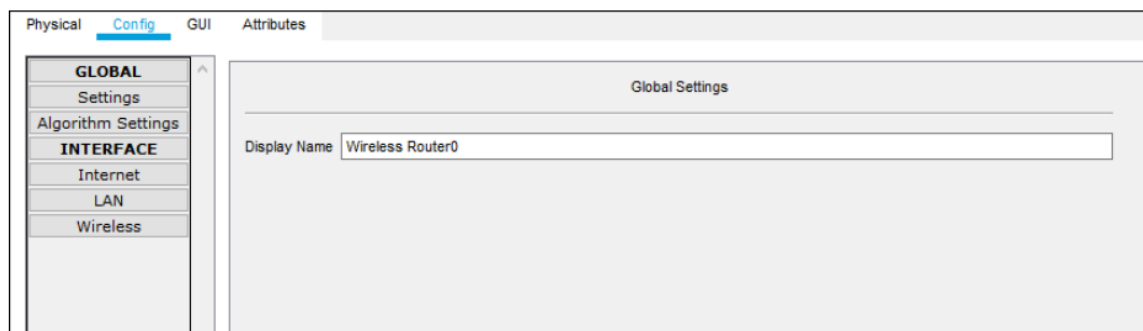
turini tanlang. Keyin, "Qurilma uchun maxsus tanlash" oynasidan kerakli qurilma modelini bosing. Nihoyat, qurilmangizni o'sha joyga qo'yish uchun ish joyidagi joyni bosing. Agar siz tanlovingizni bekor qilmoqchi bo'lsangiz, ushbu qurilma uchun Bekor qilish belgisini bosing. Shu bilan bir qatorda, "Qurilma uchun maxsus tanlash" oynasidan qurilmani bosib, ish maydoniga sudrab olib borishingiz mumkin.

3-qadam. Ish maydoniga tarmoq qurilmalarini qo'shing.

Qurilmani tanlash oynasidan foydalanib, topologiya diagrammasida ko'rsatilganidek, tarmoq qurilmalarini ish maydoniga qo'shing. Qurilmani ish maydoniga joylashtirish uchun, avvalo, Qurilma turini tanlash oynasidan qurilma turini tanlang. Keyin, "Qurilma uchun maxsus tanlash" oynasidan kerakli qurilma modelini bosing.

4-qadam. Tarmoq qurilmalarining ko'rsatiladigan nomlarini o'zgartiring.

Tarmoq qurilmalarining ko'rsatiladigan nomlarini o'zgartirish uchun Packet Tracer Logical ish maydonidagi qurilma belgisini bosing, so'ngra qurilma konfiguratsiyasi oynasidagi Config yorlig'ini bosing. Quyidagi rasmda ko'rsatilganidek, Display nomi oynasiga qurilmaning yangi nomini kiriting.



5.2-rasm. Konfiguratsiya menyusi.

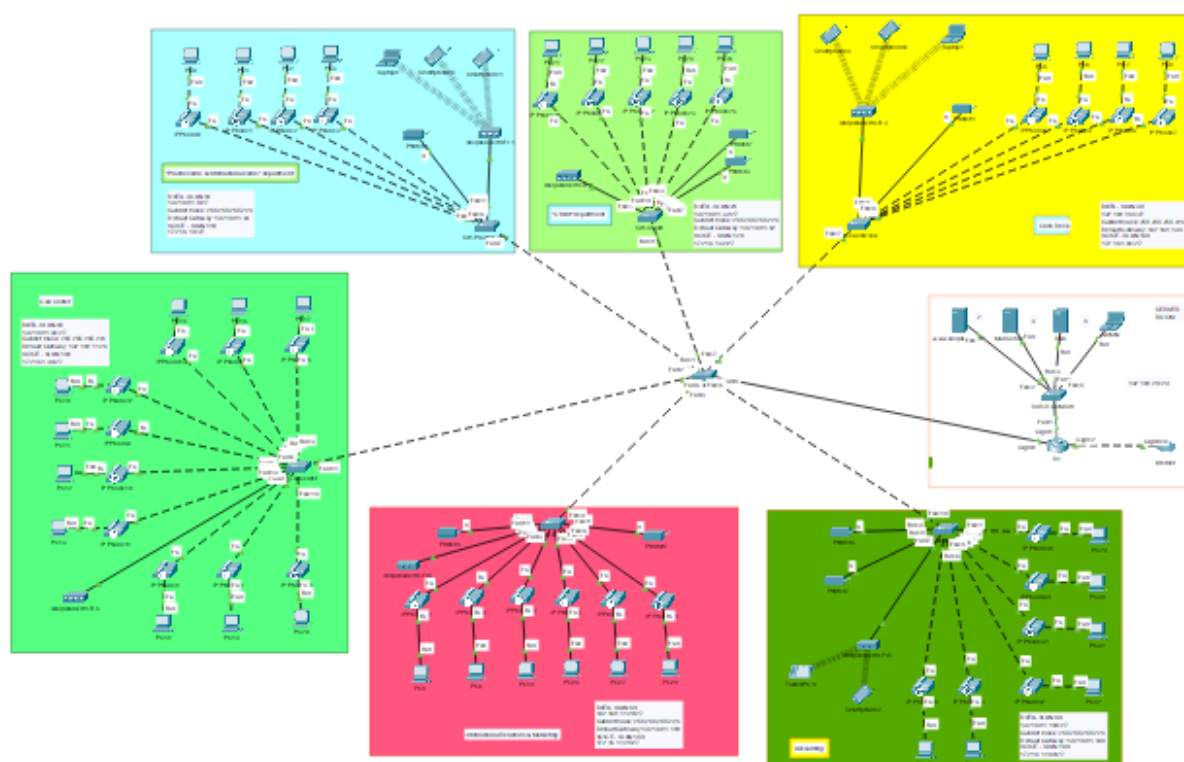
5-qadam: Ish stolidagi qurilmalar o'rtasida jismoniy kabel qo'shing. Qurilmani tanlash oynasidan foydalanib, topologiya diagrammasida ko'rsatilganidek, ish joyidagi qurilmalar orasiga jismoniy kabel qo'shing.

Simsiz routerga ulanish uchun kompyuterga to'g'ridan-to'g'ri mis simi kerak bo'ladi. Qurilmalarni tanlash oynasida to'g'ridan-to'g'ri mis kabelni tanlang va uni shaxsiy kompyuterning FastEthernet0 interfeysiga va simsiz routerni Ethernet 1 interfeysiga ulang. Simsiz routerga simli modemga ulanish uchun to'g'ridan-to'g'ri mis simi kerak bo'ladi. Qurilmani tanlash oynasida to'g'ridan-to'g'ri mis kabelni tanlang va uni simsiz routerni Internet interfeysiga va kabel modemning 1-port interfeysiga ulang. Kabel modemga Internet bulutiga ulanish uchun koaksiyal kabel kerak bo'ladi. Qurilmani tanlash oynasida koaksiyal kabelni tanlang va uni kabel modemning Port 0 interfeysiga va Internet bulutining koaksiyal interfeysiga ulang.

Tarmoq topologiyasining umumiy ko'rinishi

(VLANs va foydalanilgan qurilmalar)

VLANs	Network Devices used
"Plastic cards & International cards" department	5 phones, 5 computers, 2 printers, 1 Access Point
"Credit" department	6 phones, 6 computers, 3 printers, 1 Access Point
Cash Desk	3 phones, 3 computers, 1 printers, 1 Access Point
Call Center	10 phones, 10 computers, 5 printers, 1 Access Point
International Relations & Marketing	7 phones, 7 computers, 2 printers, 1 Access Point
Accounting	7 phones, 7 computers, 7 printers, 1 Access Point



5.3-rasm. Tarmoq topologiyasining yakuniy holati

VLAN yaratish uchun tarqatish kommutatorida ishlatiladigan buyruqlar:

```
Switch>enable
```

```
Switch#conf
```

```
Switch#conFigure t
```

```
Switch#conFigure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#
```



```
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#do wr
Switch(config-vlan)#exit
Switch(config)#interface range fast
Switch(config)#interface range fastEthernet 0/1-7
Switch(config-if-range)#switchport mode trunk
```

VLAN yaratish uchun kirish kommutatorlarida ishlatiladigan buyruqlar:

```
Switch>enable
Switch#conf
Switch#conFigure t
Switch#conFigure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface range FastEthernet0/1-24
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 110
```

SSHni sozlash:

```
en
conf t
hostname
enable password cisco
line console 0
password cisco
login
exit
banner motd ##RUXSATSIZ KIRISH TA'QIQLANADI!!!##
service password-encryption
no ip domain lookup
do wr
username cisco password cisco
```



```

ip domain name cisco.net
crypto key generate rsa general-keys modulus 1024
line vty 0 15
login local
transport input ssh
exit
do wr

```

Cisco ROAS ni sozlash (Router on A Stick - barcha VLAN-larni bitta jismoniy interfeys orqali bog'lash imkonini beradi. Jismoniy interfeys mantiqiy interfeyslarga (subterfeyslar deb nomlanadi) har bir VLAN uchun bittadan bo'linadi).

```

R1(config)#int Gi0/0
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)#int Gi0/0.1
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1,
changed state to up
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#ip address 10.0.3.1 255.255.255.0
R1(config-subif)#int Gi0/0.2
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.2,
changed state to up
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 10.0.10.1 255.255.255.0
R1(config-subif)#int Gi0/0.3
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.3,
changed state to up
R1(config-subif)#encapsulation dot1q 5
R1(config-subif)#ip address 10.0.5.1 255.255.255.0

```

Nazorat savollari:

1. Korporativ tarmoqning asosiy maqsadi nima?
2. Korporativ tarmoq qanday tuzilishi kerak?

3. Tarmoqda qanday qurilmalar ishlatiladi?
4. Tarmoqda qanday dasturiy ta'minotlar ishlatiladi?
5. Tarmoqning xavfsizligi qanday ta'minlanadi?
6. Tarmoqning ishlashini nazorat qilish uchun qanday vositalar ishlatiladi?
7. Tarmoqning samaradorligi qanday o'lchovchi vositalar orqali tekshiriladi?
8. Tarmoqda qanday axborot almashinuvi protokollari ishlatiladi?
9. Tarmoqda qanday ma'lumotlar saqlanadi va ularga qanday kirish mumkin?
10. Tarmoqning qanday texnik xizmat ko'rsatish tizimi mavjud?
11. Tarmoqning kengaytirish imkoniyatlari nima?
12. Tarmoqning qurilish jarayonida qanday muammolar yuz berishi mumkin?
13. Tarmoqning qanday texnik xususiyatlari bor?
14. Tarmoqning qanday ishlab chiqarish xususiyatlari bor?
15. Tarmoqning qanday iqtisodiy xususiyatlari bor?
16. Tarmoqning qanday ma'lumotlar bazasi bor?
17. Tarmoqning qanday axborot xavfsizligi bor?
18. Tarmoqning qanday axborotlarni saqlash va ularga kirish imkoniyatlari bor?
19. Tarmoqning qanday axborotlarni saqlash va ularga kirish imkoniyatlari bor?
20. Tarmoqning qanday axborotlarni saqlash va ularga kirish imkoniyatlari bor?

Amaliy ish № 6

VPN TUNNELLARI ORQALI KORXONA KORPORATIV TARMOQLARINI INTERNET ORQALI ULASH VA MOBIL QURILMALAR YORDAMIDA TARMOQQA MASOFADAN ULANISH IMKONIYATINI YARATISH

Ishdan maqsad: VPN ishlash tamoyillarini o'rganish, VPN tarmoqlarini qurish va ishga tushirish, VPN tunnelli orqali korxonada korporativ tarmoqlarini o'zaro ulashni tadqiq etish

VPN (inglizcha ****Virtual Private Network****, virtual xususiy tarmoq so'zidan) — foydalanuvchi qurilmasi va Internet orqali masofaviy tarmoq o'rtasida xavfsiz va shifrlangan ulanishni yaratish imkonini beruvchi texnologiya. VPN ma'lumotlar uzatish uchun maxfiylik va xavfsizlikni ta'minlaydi, shuningdek, boshqa tarmoqda joylashgan yoki geografik sabablarga ko'ra cheklangan resurslarga kirish uchun ishlatilishi mumkin.

VPNning asosiy xususiyatlari:

1. Ma'lumotlarni shifrlash: VPN orqali uzatiladigan barcha ma'lumotlar shifrlangan bo'lib, uni buzg'unchilar, ayniqsa, umumiy Wi-Fi tarmoqlarida tutib olishdan himoya qiladi.
2. IP-manzilni yashirish: Internetdagi foydalanuvchi faoliyati anonimlikni ta'minlab, VPN serverining IP manzili orqasida yashiringan.
3. Geografik cheklovlarni chetlab o'tish: mintaqangizda cheklangan kontentga kirish imkonini beradi (masalan, oqim xizmatlari, bloklangan saytlar).
4. Xavfsiz masofaviy kirish: VPN kompaniyalar tomonidan xodimlarga dunyoning istalgan nuqtasidan korporativ resurslardan foydalanish imkoniyatini ta'minlash uchun keng qo'llaniladi.
5. Izolyatsiya va tsenzuradan himoyalanih: VPN qat'iy internet tsenzurasi bo'lgan mamlakatlarda bloklarni chetlab o'tishga yordam beradi.

VPN qanday ishlaydi:

1. Ulanishni o'rnatish: Foydalanuvchi qurilmasi VPN serveriga ulanadi.
2. Tunnellash: Barcha ma'lumotlar qurilma va VPN server o'rtasidagi xavfsiz virtual "tunnel" orqali o'tadi.
3. Shifrlash: Ma'lumotlarni uzatish shifrlangan shaklda amalga oshiriladi (masalan, AES-256 protokollari yordamida).
4. IP-manzilni almashtirish: Foydalanuvchi o'zining haqiqiy manzilini maskalab, VPN-serverning IP-manzilini oladi.

VPN protokollari:

- OpenVPN: Eng xavfsiz va mashhur ochiq kodli protokollardan biri.
- L2TP/IPSec: shifrlash va tunnellashni ta'minlovchi birlashtirilgan protokol.
- PPTP: Eski va kamroq xavfsiz protokol, lekin yuqori tezlikni ta'minlaydi.
- IKEv2/IPSec: Ulanish o'zgarishlariga chidamliligi tufayli mobil qurilmalar uchun mos keladi.
- WireGuard: Yuqori tezlik va sozlash qulayligi bilan zamonaviy protokol.

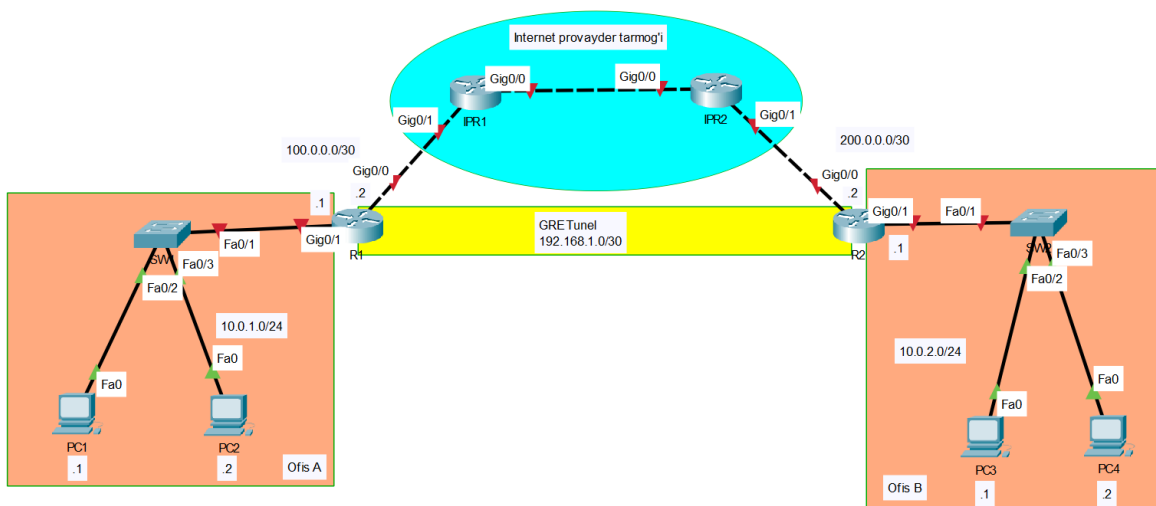
VPN qo'llanilishi:

- Shaxsiy foydalanuvchilar uchun:
- Umumiy Wi-Fi tarmoqlarida ma'lumotlarni himoya qilish.
- Bypass blokirovkasi va tsenzura.
- Internetda ishlashda maxfiylikni saqlash.

- Biznes uchun:
- Xodimlar uchun korporativ tarmoqqa xavfsiz masofadan kirishni tashkil qilish.
- kompaniya filiallari o'rtasida uzatishda ma'lumotlar himoyasini ta'minlash.

Amaliy ishni bajarish tartibi

1. Cisco Packet Tracer simulatorida dastlab quyidagicha topologiyani yaratib olib, tegishli ulanishlarni amalga oshiramiz.



6.1-rasm. Amaliy ishning tarmoq topologiyasi.

2. Keyingi bosqichda topologiyada berilgan kompyuter, switch va routerlarga ko'rsatilgan IP manzillarni o'rnatamiz.
3. So'ngra, R1 va R2 routerlar o'rtasida virtual xususiy tarmoqni hosil qilish uchun GRE tunellarni yaratamiz. Buning uchun R1ning G0/0 interfeysiga quyidagi buyruqlarni yozamiz:

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 0
Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#tunnel source g0/0
Router(config-if)#tunnel destination 200.0.0.2
Router(config-if)#ip address 192.168.1.1 255.255.255.252

Router(config-if)#do sh ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down

```

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 0
Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#tunnel source g0/0
Router(config-if)#tunnel destination 200.0.0.2
Router(config-if)#ip address 192.168.1.1 255.255.255.252

Router(config-if)#do sh ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
GigabitEthernet0/2 unassigned YES unset administratively down down
Tunnel0 192.168.1.1 YES manual up down
Vlan1 unassigned YES unset administratively down down

```

Shunga o'xshash, R2ning G0/0 interfeysiga quyidagi buyruqlarni yozamiz:

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface tunnel 0

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#tunnel source g0/0
Router(config-if)#tunnel destination 100.0.0.2
Router(config-if)#ip address 192.168.1.2 255.255.255.252
Router(config-if)#do sh ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
GigabitEthernet0/2 unassigned YES unset administratively down down
Tunnel0 192.168.1.2 YES manual up down
Vlan1 unassigned YES unset administratively down down

```

4. Keyingi bosqichda R1 va R2 routerlar uchun “default route” ni sozlaymiz:

```
Router>en
```

```
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1
```

```
Router(config)#
```

```
Router>en
```

```
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 100.0.0.1
```

```
Router(config)#
```

5. Endi R1 va R2 o'rtasidagi bog'lanishni tekshirish uchun R1 dan R2 ga va aksincha xususiy tarmoq orqali ping beramiz

```
Router(config)#do ping 192.168.1.2
```

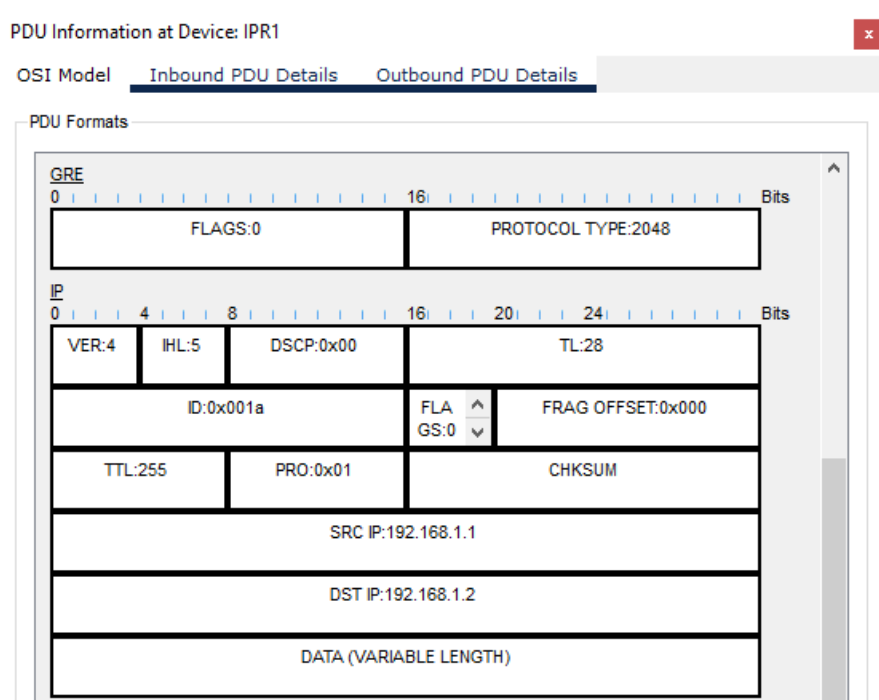
```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Simulyatsiya rejimida paketlar harakatini kuzatib, ularning tarkibini tahlil qilsak, ko'rinadiki, paketlar R1 dan R2 ga borishda xususiy tarmoq orqali o'tyapti.



6.2-rasm. Amaliy ish oynasi.

Nazorat savollari:

1. VPN nima?
2. VPN qanday ishlaydi?
3. VPN nima uchun kerak?
4. VPN qanday qurilishga ega?
5. VPN xavfsizligi qanday ta'minlanadi?
6. VPN orqali internetga ulanish qanday amalga oshiriladi?
7. VPN orqali internet trafikini kimlar kuzatishi mumkin?
8. VPN-dan foydalanish qonuniy mi?
9. VPN-dan foydalanishda qanday xavflar bor?
10. VPN-dan foydalanish internet tezligini qanday ta'sir qiladi?
11. VPN-dan foydalanish qanday qilib anonimlikni ta'minlaydi?
12. VPN-dan foydalanish geo-blokdan qanday qilib qochishga yordam beradi?
13. VPN-dan foydalanish qanday qilib torrentlarni yuklashga yordam beradi?
14. VPN-dan foydalanish qanday qilib Wi-Fi xavfsizligini oshiradi?
15. VPN-dan foydalanish qanday qilib IP manzilni yashirishga yordam beradi?

Amaliy ish № 7

BULUTLI TEXNOLOGIYA YORDAMIDA ZAHIRA MA'LUMOTLAR BAZALARI VA TIZIMINI YARATISH

Ishdan maqsad: Bulutli hisoblash (cloud computing) dan foydalangan holda ma'lumotlar bazalari va kompyuter tizimlarini zahiralashni usul va vositalari hamda buni amalga oshirish mexanizmini o'rganish.

Nazariy ma'lumotlar

Cloud texnologiyasi, yoki bulutli texnologiyalar, internet orqali kompyuter resurslarini taqdim etish texnologiyasidir. Bu texnologiya, foydalanuvchilarga ma'lumotlarni saqlash, ishlash va ularga istalgan joydan va istalgan vaqtda kirish imkoniyatini beradi.

Cloud texnologiyasi, serverlar, saqlash, dasturlar, tarmoqlar va boshqa IT resurslarni internet orqali xizmat sifatida taqdim etadi. Bu texnologiya, foydalanuvchilarga ularga kerak bo'lgan resurslarni sotib olish, o'rnatish va boshqarishga sarf bo'lgan vaqt va mablag'ni tezda kamaytiradi.

Bulutli texnologiyalar uch turli hisoblanadi:

1. Infrastruktura sifatida xizmat (IaaS): Bu, foydalanuvchilarga virtual serverlar va tarmoq infrastrukturasi taqdim etadi.
2. Dastur sifatida xizmat (PaaS): Bu, dasturlash muhitlari, dasturlar ishlab chiqarish, test qilish va boshqarish uchun kerak bo'lgan platformalarni taqdim etadi.
3. Dastur sifatida xizmat (SaaS): Bu, internet orqali taqdim etiladigan dasturlardir. Foydalanuvchilar brauzer orqali kirib, ulardan foydalanishadi.

Bulutli texnologiyalar, bizneslarga o'sish, moslashuvchanlik va samaradorlikni oshirishga yordam beradi. Bu texnologiyalar, axborot texnologiyasini sifatida xizmat ko'rsatishning asosiy usullaridan biriga aylangan.

Bulutli zahira nusxasi, shuningdek, onlayn zahira yoki masofaviy zaxira sifatida ham tanilgan, jismoniy yoki virtual fayl yoki ma'lumotlar bazasi nusxasini uskunaning ishlamay qolishi, sayt halokati yoki insonning noto'g'ri ishlashi holatlarida saqlash uchun ikkinchi darajali, saytdan tashqari joyga yuborish strategiyasidir. Zaxira serveri va ma'lumotlarni saqlash tizimlari odatda uchinchi tomon buluti yoki SaaS provayderi tomonidan joylashtiriladi, bu esa zaxira mijozdan saqlash maydoni yoki foydalanilgan sig'im, ma'lumotlarni uzatish o'tkazish qobiliyati, foydalanuvchilar soni, serverlar soniga qarab takroriy to'lov oladi.

Bulutli ma'lumotlarni zaxiralashni amalga oshirish IT xodimlarining ish yukini oshirmasdan tashkilotning ma'lumotlarini himoya qilish, biznesni davom ettirish va tartibga solishga rioya qilish strategiyalarini kuchaytirishga yordam

beradi. Mehnatni tejaydigan foyda muhim bo'lishi mumkin va ma'lumotlarni uzatish to'lovlari kabi bulutli zahira bilan bog'liq qo'shimcha xarajatlarning bir qismini qoplash uchun etarli bo'lishi mumkin.

Ko'pgina bulutli obunalar oylik yoki yillik asosda ishlaydi. Dastlab, asosan, iste'molchilar va uy ofislari tomonidan foydalanilgan bo'lsa, onlayn zaxira xizmatlari hozirda kichik va yirik korxonalar tomonidan ma'lumotlarning ba'zi shakllarini zaxiralash uchun keng qo'llaniladi. Kattaroq kompaniyalar uchun bulutli ma'lumotlarni zaxiralash qo'shimcha zaxira shakli sifatida xizmat qilishi mumkin.

Bulutli zahiradan foydalanish holatlari va yondashuvlari

Tashkilotning ma'lumotlar markazida zaxira ilovasi ma'lumotlarni nusxalaydi va uni qayta tiklash holatida qulay foydalanish uchun turli xil muhitda yoki boshqa saqlash tizimida saqlaydi. Saytdan tashqari zaxiralashning bir nechta varianti va yondashuvlari mavjud bo'lsa-da, bulutli zahira o'chirilgan bo'lib xizmat qiladi. -ko'p tashkilotlar uchun sayt ob'ekti. Korxonada kompaniya o'zining shaxsiy bulut xizmatiga ega bo'lsa, saytdan tashqari serverga ega bo'lishi mumkin, ammo agar kompaniya bulutli zahira muhitini boshqarish uchun xizmat ko'rsatuvchi provayderdan foydalansa va zaxira nusxasini saqlash uchun muntazam hisob-kitob olsa, to'lovni qaytarish usuli o'xshash bo'ladi. va xizmatlar.

Tashkilotning ma'lumotlar markazida zaxira ilovasi ma'lumotlarni nusxalaydi va uni qayta tiklash holatida qulay foydalanish uchun turli xil muhitda yoki boshqa saqlash tizimida saqlaydi. Saytdan tashqari zaxiralashning bir nechta varianti va yondashuvlari mavjud bo'lsa-da, bulutli zahira o'chirilgan bo'lib xizmat qiladi. -ko'p tashkilotlar uchun sayt ob'ekti. Korxonada kompaniya o'zining shaxsiy bulut xizmatiga ega bo'lsa, saytdan tashqari serverga ega bo'lishi mumkin, ammo agar kompaniya bulutli zahira muhitini boshqarish uchun xizmat ko'rsatuvchi provayderdan foydalansa va zaxira nusxasini saqlash uchun muntazam hisob-kitob olsa, to'lovni qaytarish usuli o'xshash bo'ladi.

Tashkilotning mavjud ma'lumotlarini himoya qilish jarayoniga osongina mos keladigan mavjud xizmatlarga ega bulutli zahiraga turli xil yondashuvlar mavjud. Bulutli zaxira turlariga quyidagilar kiradi:

To'g'ridan-to'g'ri ommaviy bulutga zaxiralash. Tashkiliy ish yuklarini saqlash usullaridan biri umumiy bulutdagi resurslarni takrorlashdir. Bu usul to'g'ridan-to'g'ri AWS, Google Cloud yoki Microsoft Azure kabi bulutli provayderlarga ma'lumotlarni yozishni o'z ichiga oladi. Tashkilot bulutli saqlash xizmatiga yuborish uchun ma'lumotlar nusxasini yaratish uchun o'zining zaxira dasturidan foydalanadi. Keyin bulutli saqlash xizmati ma'lumotlar uchun maqsad va saqlanishini ta'minlaydi, lekin u maxsus zaxira ilovasini ta'minlamaydi. Ushbu

stsenariyda zaxira dasturiy ta'minot bulutning saqlash xizmati bilan o'zaro aloqada bo'lishi muhimdir. Bundan tashqari, ommaviy bulut opsiyalari bilan IT mutaxassislari zaxiralangan ma'lumotlarni himoya qilish uchun ma'lumotlarni shifrlash, shuningdek, identifikatsiya va kirishni boshqarish kabi qo'shimcha ma'lumotlarni himoya qilish tartib-qoidalarini ko'rib chiqishlari kerak bo'lishi mumkin.

Xizmat ko'rsatuvchi provayderga zaxiralash. Ushbu stsenariyda tashkilot boshqariladigan ma'lumotlar markazida zaxira xizmatlarini taklif qiluvchi bulut xizmatiga yoki SaaS provayderiga ma'lumotlarni yozadi. Kompaniya o'z ma'lumotlarini xizmatga yuborish uchun foydalanadigan zaxira dasturiy ta'minoti xizmatning bir qismi sifatida taqdim etilishi mumkin yoki xizmat tijoratda mavjud bo'lgan maxsus zaxira ilovalarini qo'llab-quvvatlashi mumkin.

Bulutdan bulutga (C2C) zaxira nusxasini tanlash. Ushbu xizmatlar bulutli zaxira maydonidagi eng yangi takliflar qatoriga kiradi. Ular SaaS ilovasi yordamida yaratilgan ma'lumotlar yoki bulutli zahira xizmatida saqlangan ma'lumotlar sifatida bulutda allaqachon yashovchi ma'lumotlarning zaxira nusxasini yaratishga ixtisoslashgan. Nomidan ko'rinib turibdiki, C2C zaxira xizmati ma'lumotlarni bir bulutdan boshqa bulutga ko'chiradi. Bulutdan bulutga zaxiralash xizmati odatda ushbu jarayonni boshqaradigan dasturiy ta'minotni o'z ichiga oladi.

Onlayn bulutli zaxira tizimlaridan foydalanish. Bundan tashqari, bulutli zaxira xizmatiga ma'lumotlarni zaxiralashni osonlashtiradigan apparat alternativlari ham mavjud. Bu qurilmalar zaxira serveri bilan bir qatorda zahiraviy dasturiy ta'minot va disk hajmini o'z ichiga olgan barcha birda-bir zaxira mashinalaridir. Uskunalar zaxira nusxasini olish imkoni bo'lganidek, ulash va o'ynashga yaqin va ularning aksariyati bir yoki bir nechta bulutli zaxira xizmatlari yoki bulut provayderlari bilan uzluksiz aloqani ta'minlaydi. Bulutli interfeyslarni o'z ichiga olgan zaxira qurilmalarni taklif qiluvchi sotuvchilar ro'yxati uzoq, Quantum, Unitrends, Arcserve, Rubrik, Cohesity, Dell EMC, StorageCraft va Asigra ushbu maydonda faol. Bu qurilmalar, odatda, eng so'nggi zaxira nusxasini mahalliy darajada saqlaydi, uni bulutli zahiraviy provayderga nusxalash bilan bir qatorda, mahalliy zaxira nusxasidan har qanday kerakli tiklashni amalga oshirish, vaqt va uzatish xarajatlarini tejaydi.

Ma'lumotlar qanday yig'iladi

Bulutli zahira xizmatlari odatda xarid qilingan xizmat darajasi va mijozning talablari bilan belgilanadigan jadval asosida ishlaydigan mijoz dasturiy ilovasi atrofida quriladi. Misol uchun, agar mijoz kunlik zahira nusxalari uchun shartnoma tuzgan bo'lsa, dastur har 24 soatda ma'lumotlarni yig'adi, siqadi, shifrlaydi va bulutli

xizmat ko'rsatuvchi provayder serverlariga uzatadi. Iste'mol qilinadigan tarmoqli kengligi miqdorini va fayllarni uzatish uchun zarur bo'lgan vaqtni kamaytirish uchun xizmat ko'rsatuvchi provayder faqat dastlabki to'liq zahiradan keyin qo'shimcha zaxira nusxalarini taqdim etishi mumkin.

Bulutli zaxira xizmatlari ko'pincha tashkilot ma'lumotlarini himoya qilish uchun zarur bo'lgan dasturiy ta'minot va apparat vositalarini, shu jumladan Microsoft Exchange va SQL Server ilovalarini o'z ichiga oladi. Mijoz o'zining zaxira ilovasidan yoki bulutli zahira xizmati taqdim etadigan dasturiy ta'minotdan foydalansa ham, tashkilot zaxiralangan ma'lumotlarni qayta tiklash uchun o'sha dasturdan foydalanadi. Qayta tiklashlar fayl bo'yicha, hajmi bo'yicha yoki to'liq zaxira nusxasini to'liq tiklash bo'yicha bo'lishi mumkin. Fayllarni birma-bir qayta tiklash odatda afzal qilingan usuldir, chunki bu biznesga butun hajmlarni tiklash uchun vaqt va xavfni olishdan ko'ra, yo'qolgan yoki shikastlangan fayllarni tezda tiklashga imkon beradi.

Qayta tiklanadigan ma'lumotlar hajmi juda katta bo'lsa, bulutli zahira xizmati ma'lumotlarni to'liq saqlash massiviga yuborishi mumkin, bunda mijoz o'z ma'lumotlarini tiklash uchun o'z serverlariga ulanishi mumkin. Bu, aslida, teskari ekish jarayonidir. Tarmoq orqali katta hajmdagi ma'lumotlarni qayta tiklash tashkilotning qayta tiklash vaqti maqsadiga (RTO) qarab, qabul qilib bo'lmaydigan darajada uzoq vaqt talab qilishi mumkin.

Bulutli zaxira nusxalarini tiklashning asosiy xususiyati shundaki, ular deyarli har qanday kompyuterdan istalgan joyda amalga oshirilishi mumkin. Misol uchun, tashkilot o'z ma'lumotlarini to'g'ridan-to'g'ri boshqa joyda, agar uning asosiy ma'lumotlar markazi mavjud bo'lmasa, falokatni tiklash saytiga tiklashi mumkin.

Zaxiralash turlari

Bulutli zaxiralashning turli yondashuvlariga qo'shimcha ravishda, ko'rib chiqilishi kerak bo'lgan bir nechta zaxira usullari ham mavjud. Bulutli zaxira provayderlari mijozlarga ularning ehtiyojlari va ilovalariga eng mos keladigan zaxira usulini tanlash imkoniyatini berishsa-da, uchta asosiy tur o'rtasidagi farqni tushunish muhimdir.

To'liq zahira nusxalari har safar zaxira boshlanganda butun ma'lumotlar to'plamini nusxalaydi. Natijada ular eng yuqori darajadagi himoyani ta'minlaydi. Biroq, aksariyat tashkilotlar tez-tez to'liq zaxiralashni amalga oshira olmaydi, chunki ular ko'p vaqt talab qilishi va juda ko'p ma'lumotlarni saqlash hajmini egallashi mumkin.

Qo‘shimcha zahira nusxalari faqat oxirgi to‘liq zaxira nusxasi emas, balki oxirgi zahira o‘shidan keyin o‘zgartirilgan yoki yangilangan ma‘lumotlarning zaxira nusxasini yaratadi. Bu usul vaqt va saqlash joyini tejaydi, lekin to'liq tiklashni qiyinlashtirishi mumkin, chunki har qanday zaxira qo'shimchasi yo'qolsa yoki shikastlansa, to'liq tiklash imkonsiz bo'ladi. Incremental bulutli zaxiralashning keng tarqalgan shaklidir, chunki u kamroq resurslardan foydalanadi.

Differentsial zaxiralar qo'shimcha zahiraga o'xshaydi, chunki ular faqat o'zgartirilgan ma'lumotlarni o'z ichiga oladi. Biroq, differentsial zaxiralar umuman oxirgi zahiradan ko'ra, oxirgi to'liq zaxiradan keyin o'zgargan ma'lumotlarning zaxira nusxasini yaratadi. Ushbu usul qo'shimcha zaxira nusxalari bilan yuzaga kelishi mumkin bo'lgan qiyin tiklash muammosini hal qiladi.

Eng yaxshi amaliyotlar

Strategiyalar, texnologiyalar va provayderlar juda xilma-xil bo'lsa-da, korxonada bulutli zaxiralashni amalga oshirishda kelishilgan bir qancha eng yaxshi amaliyotlar mavjud. Mana bir nechta ko'rsatmalar:

Bulutli zaxira provayderi xizmati darajasidagi kelishuvning (bulutli SLA) barcha jihatlarini tushunib oling, masalan, ma'lumotlarning zaxira nusxasi va himoyasi, sotuvchi idoralari qayerda joylashgani va vaqt o'tishi bilan xarajatlar qanday to'planishi kabi. Provayderning javobgarligi chegaralarini va agar kerak bo'lsa, yordam va tuzatishni qanday izlash kerakligini biling.

Zaxiralash uchun biron bir usul yoki ma'lumotlarni saqlash vositasiga ishonmang. 3-2-1 zaxiralash metodologiyasi korporativ zaxiralar uchun markaziy siyosat bo'lib qolmoqda.

Favqulodda vaziyatlarda ularning yetarli ekanligiga ishonch hosil qilish uchun zaxira strategiyalari va ma'lumotlarni qayta tiklash nazorat ro'yxatlarini sinab ko'ring. Zaxira nusxalarini tasdiqlang va kerak bo'lganda qayta tiklash uchun texnologiyalar va xodimlarning malaka to'plamlari yetarli ekanligiga ishonch hosil qilish uchun tiklash jarayonlarini vaqti-vaqti bilan sinab ko'ring.

Jarayonlar muvaffaqiyatli va buzilmaganligiga ishonch hosil qilish uchun administratorlarga bulutli zahira nusxalarini muntazam ravishda kuzatib boring.

Oson kirish mumkin bo'lgan va mavjud ma'lumotlarni qayta yozmaydigan ma'lumotlarni qayta tiklash manzilini tanlang.

Axborotning biznes operatsiyalari uchun muhimligiga asoslanib zaxiralash uchun muayyan ma'lumotlar yoki fayllar haqida qaror qabul qiling - barcha ma'lumotlar bir xil tarzda yaratilmaydi, shuning uchun turli xil biznes ma'lumotlar turlarining ahamiyati va qiymatini aks ettiruvchi zaxira nusxalarini amalga oshiring.

Muayyan fayllarni tezkor joylashtirish va tiklashni yoqish uchun metama'lumotlardan to'g'ri foydalaning.

Maxfiy qolishi kerak bo'lgan ma'lumotlar uchun shaxsiy shifrlashdan foydalanishni o'ylab ko'ring.

Faqat kerakli ma'lumotlarning zaxira nusxasini yaratish uchun ma'lumotlarni saqlash siyosati va ma'lumotlarni boshqarish usullaridan foydalaning -- ayniqsa, takroriy xarajatlar to'planadigan bulutda.

Cloud zahiralash imkoniyatini beruvchi xizmatlar

Onlayn zaxira xizmatlariga yondashuvlar har xil, shuning uchun tashkilot provayderni tanlashdan oldin SLA, narx rejalari va uzoq muddatli xarajatlarni diqqat bilan ko'rib chiqishi kerak. Bulutli ma'lumotlarni zahiralash sotuvchisi opsiyalariga misollar quyidagilarni o'z ichiga oladi:

Acronis. Ushbu sotuvchi Cyber Backup, gibrid bulutli zahirani xizmat sifatida taqdim etadi. Acronis Cyber Backup virtual, jismoniy va bulutli muhitlarni himoya qiladi va u har doimgidek to'lash biznes modelini o'z ichiga oladi.

Arcserve. Zetta-ni sotib olish bilan Arcserve o'zining yagona ma'lumotlarni himoya qilish (UDP) taklifini kengaytirdi. Mahsulot Arcserve UDP Cloud Direct to'g'ridan-to'g'ri bulutga DR va zaxira nusxasini o'z ichiga oladi. Bulutli himoya o'rta bozorga qaratilgan.

Asigra. Bulutli zahiraviy kashshof, Asigra's Cloud Backup to'lov dasturining zahiraga tushishiga yo'l qo'ymaslik uchun o'rnatilgan zararli dastur dvigatellariga ega.

Backblaze. Ushbu sotuvchi shaxsiy va biznes bulutli zaxira nusxasini, shuningdek bulutli saqlashni taklif qiladi. Backblaze o'zining ochiq manbali Storage Pods apparat platformasida va bulutga asoslangan Backblaze Vault fayl tizimida ma'lumotlarni saqlaydi. Backblaze orqali ma'lumotlarning zaxira nusxasini mobil qurilmalar va kompyuterlardagi veb-brauzer orqali olish mumkin. Qayta tiklashlar SSL orqali yuklab olinadi.

Carbonite. Iste'molchilarga, SMB va korxonalariga sotish, kompaniyaning takliflari hujjatlar, elektron pochta, musiqa, fotosuratlar va sozlamalarning zaxira nusxasi va Windows va Mac foydalanuvchilari uchun mavjud. 2018-yil mart oyida Carbonite Dell EMC'dan raqib Mozy'ni sotib oldi va xizmatlarini o'z takliflariga kiritdi. 2019 yilda Carbonite kiberxavfsizlik sotuvchisi Webrootni sotib oldi. Keyinchalik 2019 yilda kontentni boshqarish sotuvchisi OpenText Carbonite-ni sotib oldi.

CrashPlan. Ushbu sotuvchi kichik biznes va korporativ zaxira variantlarini taklif qiladi. U mahalliy drayverlarga to'liq disk zaxira nusxalarini qo'llab-quvvatlaydi va Linux va macOS tarmoq drayverlarini himoya qiladi.

Druva. Bu bulutli zahira sotuvchisi uchta asosiy taklifga ega. Korporativ darajadagi Druva inSync so'nggi nuqtalarga mo'ljallangan bo'lib, jismoniy va ommaviy bulutli saqlash bo'ylab ma'lumotlarning zaxira nusxasini yaratadi, Gibrid ish yuklari uchun Druva esa taqsimlangan jismoniy va virtual serverlar uchun bulutdagi ma'lumotlar to'plamlarini zaxiralash va tiklash uchun foydalaniladigan dasturiy ta'minot agentidir. Bundan tashqari, 2018 yilda Druva AWS ma'lumotlarini himoya qilish uchun CloudRanger'ni sotib oldi.

IDrive. Iste'molchilar va kichik biznes uchun mo'ljallangan IDrive oniy suratlar, sinxronlash xizmati va gibrid ma'lumotlarni himoya qilishni o'z ichiga oladi.

Microsoft Azure zaxira nusxasi. Ushbu xizmat avtomatik ravishda Azure bulutiga zaxira nusxalarini yuboradi. Azure Site Recovery xususiy Windows infratuzilmasini zaxiralash uchun replikatsiyani avtomatlashtiradi.

Rubrik. Kuchli xavfsizlik va tezkor tiklashga ixtisoslashgan Rubrik gibrid va ko'p bulutli muhitlarni qo'llab-quvvatlaydigan bulutli ma'lumotlarni boshqarish platformasini taklif etadi.

SpiderOak One Zaxira. Ushbu SMB gibrid bulutli zaxira taklifi cheksiz miqdordagi qurilmalarni, shu jumladan tashqi qurilmalarni himoya qiladi va 5 TB saqlash chegarasini taklif qiladi.

Unitrendlar. Ushbu sotuvchi mijozlarga Forever Cloud yordamida shaxsiy bulutda cheksiz vaqtga zaxiralash imkonini beradi va qayta tiklash uchun bir nechta DRaaS variantlarini taklif qiladi.

Veeam dasturiy ta'minot. Veeam o'zining Cloud Connect mahsuloti orqali bulutli zahirani taqdim etadi. Xizmat ko'rsatuvchi provayderlar bulutda zaxira va tiklash maqsadini yaratish uchun Veeam bilan hamkorlik qilishlari mumkin.

Veritas NetBackup. Veritas bir oyna oynasidan boshqarilishi mumkin bo'lgan jismoniy, virtual va ko'p bulutli muhitlar uchun yagona ma'lumotlarni himoya qilishni ta'minlaydi.

Ishning amaliy qismi

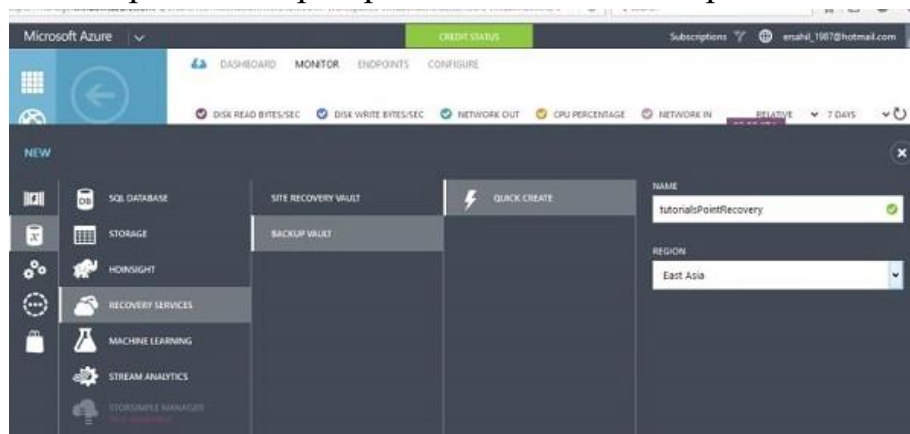
Azure zaxira nusxasi bulutda mahalliy ma'lumotlarni zaxiralash uchun ishlatilishi mumkin. Ma'lumotlar shifrlangan rejimda saqlanadi. Quyidagi bo'limlarda Azure yordamida buni qanday qilish kerakligi batafsil tasvirlangan. Ushbu jarayonda biz avval ma'lumotlarimiz saqlanadigan zaxira omborini yaratamiz va keyin ma'lumotlarning mahalliy kompyuterimizdan qanday zaxiralanishi mumkinligini ko'rib chiqamiz. Kompyuterda o'rnatilgan zaxira agenti avval

ma'lumotlarni shifrlaydi va keyin uni tarmoq orqali Azure-dagi saqlash joyiga yuboradi. Sizing ma'lumotlaringiz butunlay xavfsiz va xavfsiz.

Zaxira nusxalar omborini yaratish

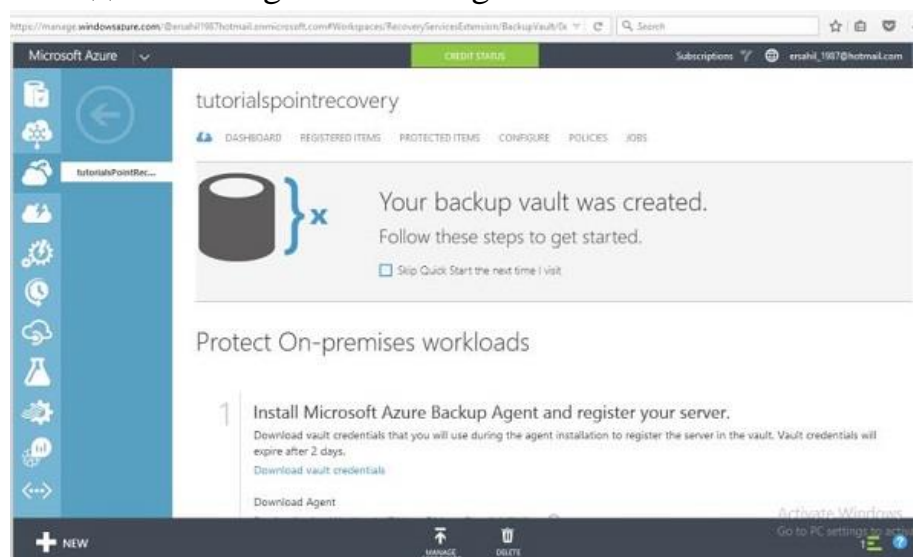
1-qadam - boshqaruv portalingizga kiring.

2-qadam - Pastki o'ng burchakda Новый → Службы данных → Службы восстановления → Хранилище резервных копий → Быстрое создание tanlang.



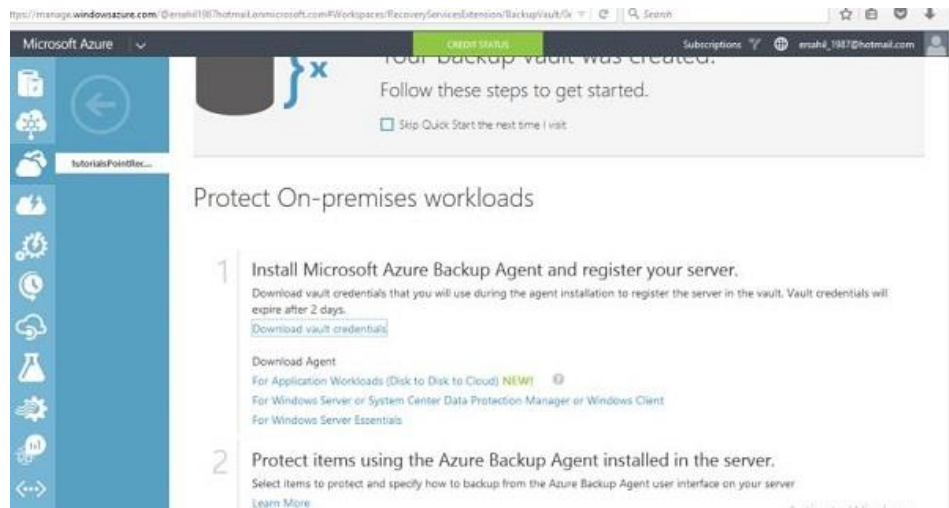
3-qadam - Ombor nomini kiriting va mintaqani tanlang. U yaratiladi va boshqaruv portalingizda ko'rsatiladi.

4-qadam - Yaratilgan omborni tanlang va quyidagi rasmda ko'rsatilganidek, "Скачать учетные данные" tugmasini bosing.



5-qadam - Bu sizning kompyuteringizda hisob ma'lumotlari faylini saqlaydi.

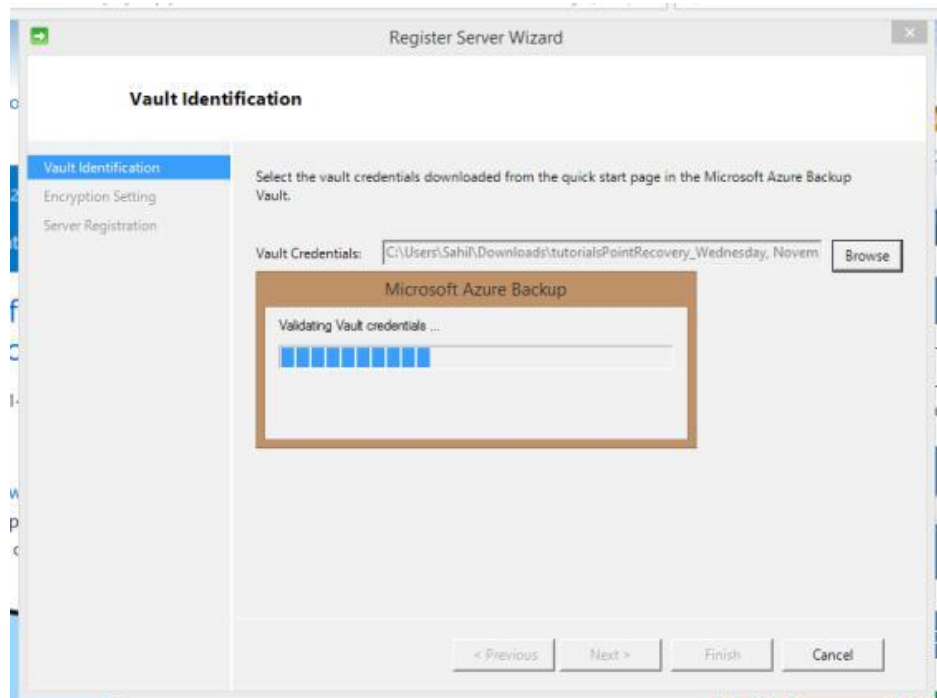
6-qadam - Endi Azure-da xuddi shu sahifani pastga aylantiring va "Скачать агент" ostida uchta variantni ko'rasiz. Tegishli variantni tanlang. Keling, ushbu misoldagi ro'yxatdagi uchinchi variantni tanlaylik.



7-qadam – Agent sozlamalari kompyuteringizda saqlanadi. Uni o'rnatish uchun ko'rsatmalarga amal qilishingiz kerak bo'ladi. O'rnatish jarayoni juda oddiy.

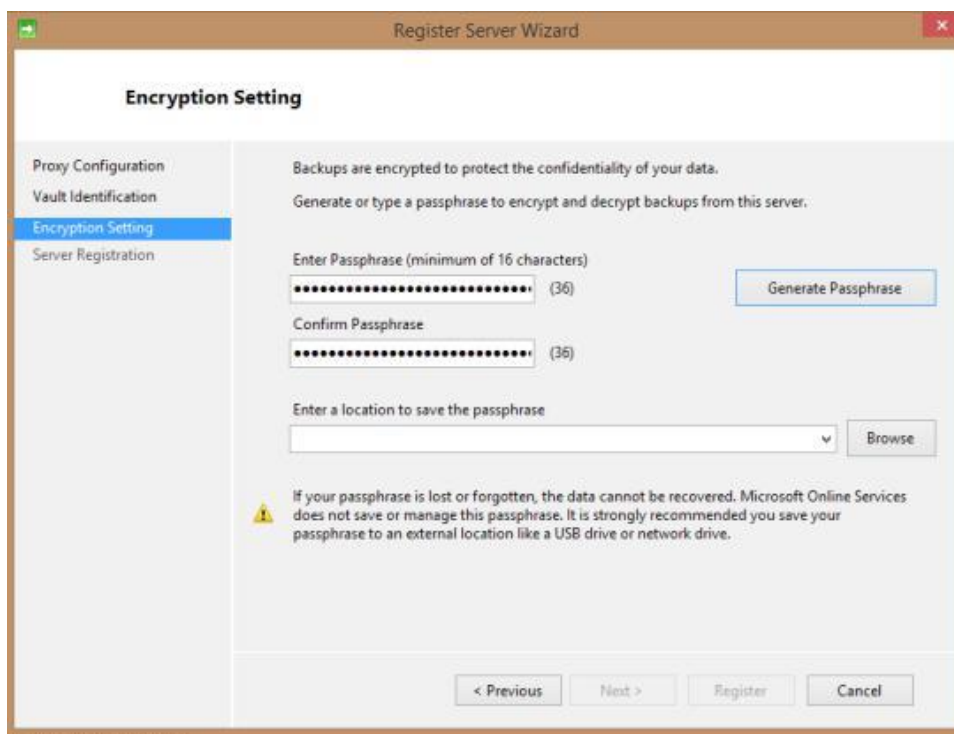
8-qadam - O'rnatish oxirida siz qalqib chiquvchi oynaning pastki qismida "Перейти к регистрации" tugmachasini ko'rasiz. Ushbu tugmani bosing va quyidagi ekran paydo bo'ladi.

9-qadam - Birinchi qadam - bu omborni aniqlash. Kompyuteringizda oxirgi bosqichda saqlangan hisob ma'lumotlari faylini ko'rib chiqing.



10-qadam - Ro'yxatga olish ustasidagi keyingi qadam shifrlash sozlamalarini tanlashdir. Siz o'zingizning parolingizni kiritishingiz yoki sehrgarga uni o'zi yaratishiga ruxsat berishingiz mumkin. Bu erda "Parol iborasini yaratish" ni tanlaymiz.

11-qadam - Parol iborasini saqlamoqchi bo'lgan joyni ko'rib chiqing. Ushbu parol faylini xavfsiz saqlash juda muhim, chunki usiz zaxira nusxalarini tiklay olmaysiz.

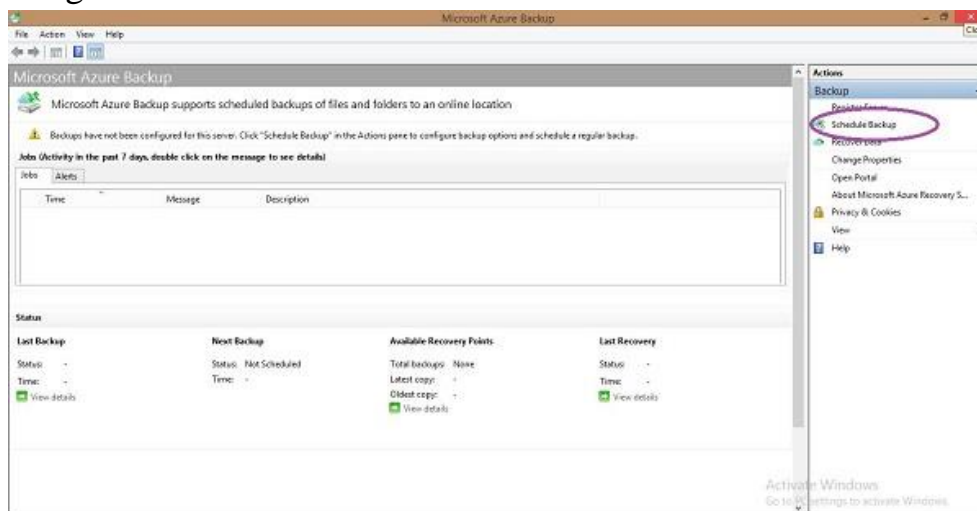


12-qadam - "Keyingi" tugmasini bosib va fayl siz tanlagan joyga saqlanadi.

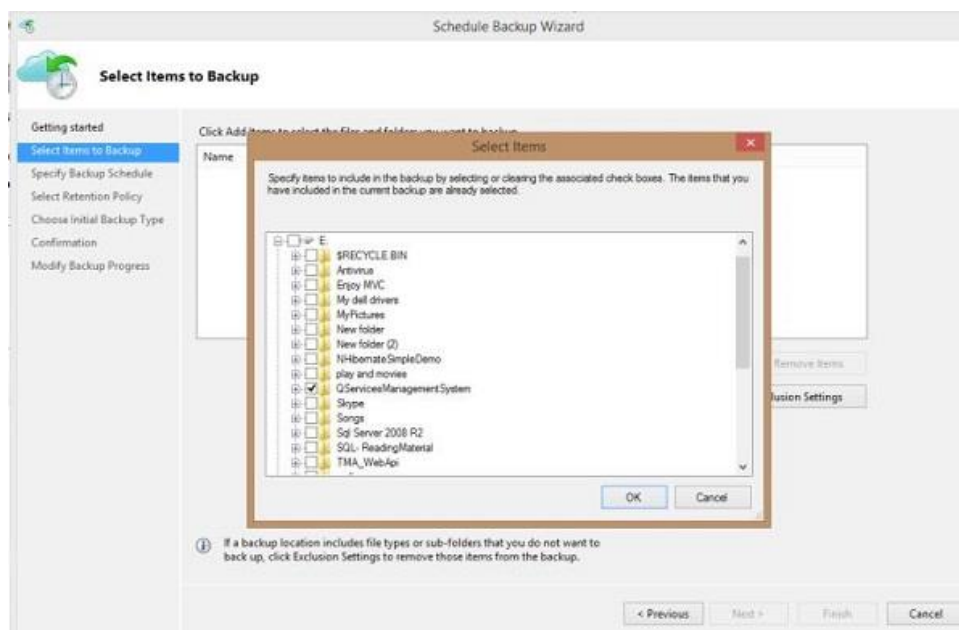
Zaxira nusxalashni rejalashtirish

Yuqoridagi bo'limdagi jarayon tugagandan so'ng, oldingi bosqichda o'rnatilgan, kompyuteringizda ishlaydigan quyidagi dasturni ko'rasiz. Siz Azure-da zaxira nusxasini yaratmoqchi bo'lgan kompyuteringizdan ma'lumotlar papkasini va ushbu jarayonda zaxiralash chastotasini tanlaysiz.

1-qadam - O'ng paneldagi " Планировать резервное копирование " tugmasini bosib.

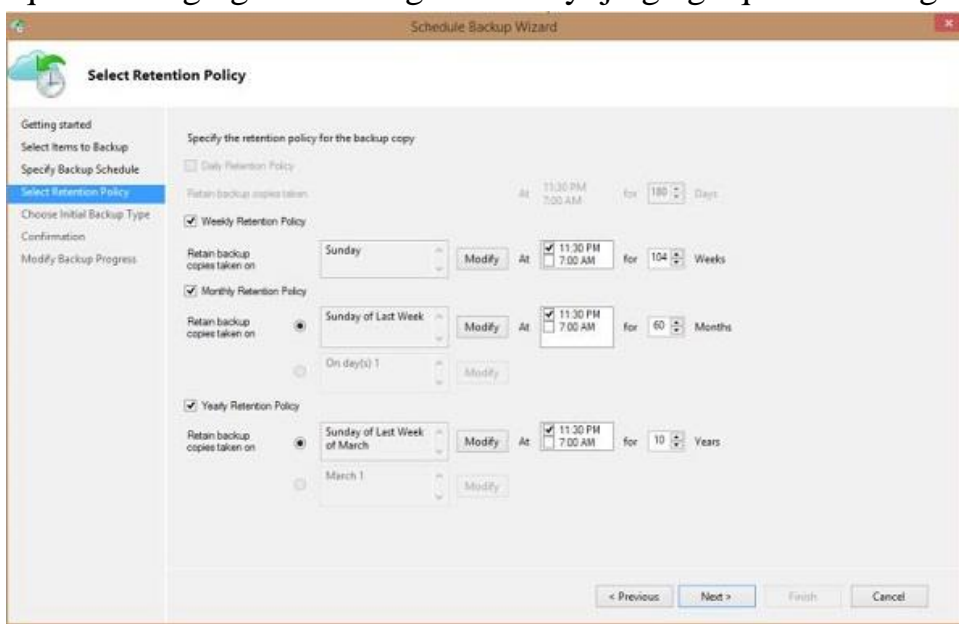


Ushbu misolda "QServicesManagementSystem" nomli ma'lumotlar papkasini tanlaylik.

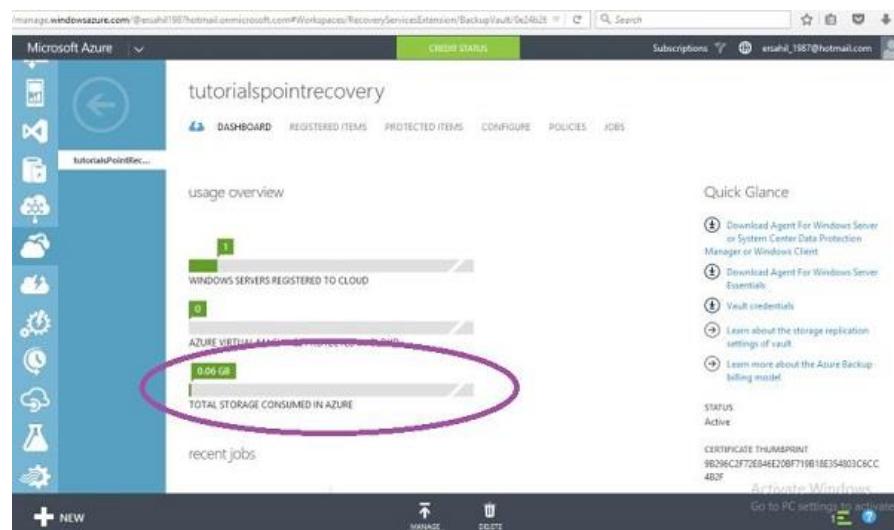


Ekranda qalqib chiquvchi qadamlarni bajaring va juda tushunarli. Sizga maksimal 3 marta zaxira nusxasini yaratishga ruxsat berilgan va siz kunlik va haftalik chastotalardan birini tanlashingiz mumkin.

2-qadam – Keyingi bosqichda zaxira nusxasini onlayn xotirangizda qancha vaqt saqlamoqchi ekanligingizni tanlang. Uni ehtiyojingizga qarab sozlang.

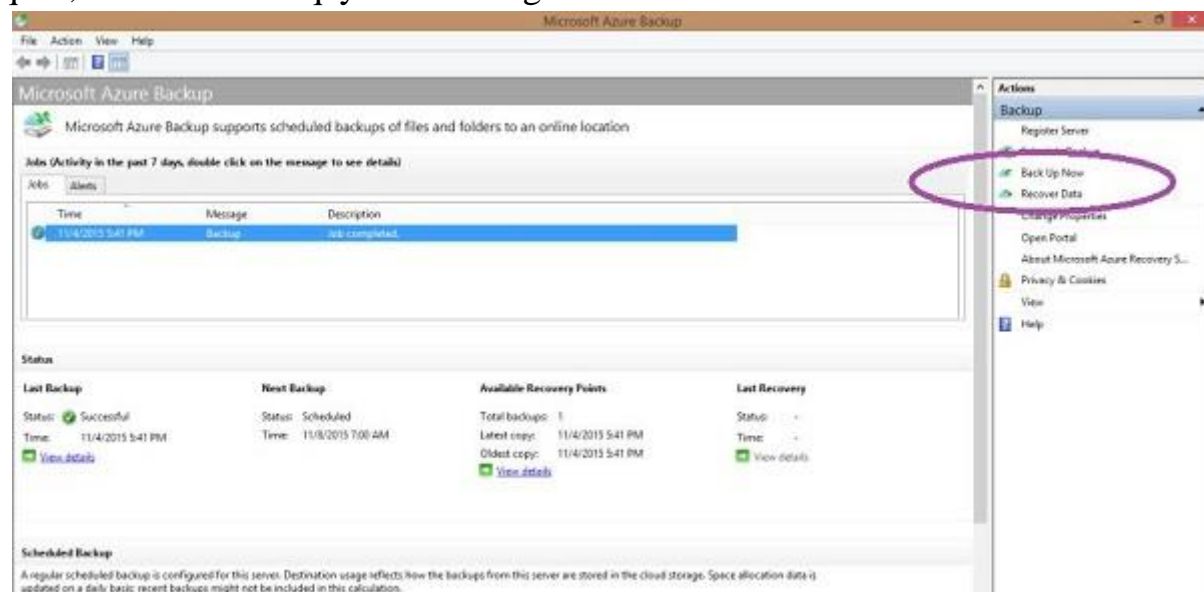


3-qadam - Zaxira agentining chap panelida "Сделать резервную копию сейчас " ni tanlashingiz mumkin. Bu sizning ma'lumotlaringizning nusxasini o'sha paytda saqlaydi. Keyin siz zaxira omborini tanlab, uning boshqaruv paneliga o'tib, uni boshqaruv portalida ko'rishingiz mumkin.



Quyidagi rasmda "Задания" bo'limida bitta element borligini ko'rishingiz mumkin, chunki "hozir zahiralash сделать резервную копию сейчас" ni tanlash orqali ma'lumotlar zahiralangan. Ushbu bo'lim zahira vazifasidagi barcha harakatlarni ko'rsatadi. Zahira jadvalining tafsilotlari "Состояние" bo'limida ko'rsatiladi.

4-qadam - Zahira agentida "Восстановить данные" ni tanlab, sehrgarga amal qilib, ma'lumotlarni qayta tiklashingiz mumkin.



Nazorat savollari:

1. Bulutli zahiralash nima?
2. Bulutli zahiralashning asosiy xususiyatlari qandaydir?
3. Bulutli xizmatlardan foydalangan holda qanday tijorat faoliyatlarini olib borish mumkin?
4. Bulutli xizmatlardan foydalangan holda xavfsizlikni ta'minlash uchun qanday chora-tadbirlar qilingan?
5. Bulutli xizmatlarni qanday tartibda amalga oshirish mumkin?

6. Hibrid bulutlar nima? Ular qanday ishlaydilar?
7. Bulutli xizmatlardan foydalanishning iqtisodiy tuzilishi qandaydir?
8. IaaS, PaaS, va SaaS nima ma'noni anglatadilar? Ular qanday turdagi bulut xizmatlarini ifodalaydi?
9. Bulutli xizmatlar qanday ta'minoti qilinadi?
10. Serverless (server yo'q) computing nima? Uning afzalliklari qandaydir?
11. Bulutli zahiralashda qanday tizimlardan foydalaniladi?
12. Bulutli xizmatlardan foydalangan holda ma'lumotlar qanday saqlanadi?
13. Bulutli xizmatlardan foydalangan holda xavfsizlik huquqiy yo'nalishlari qanday muhofaza qilinadi?
14. Bulutli xizmatlarni o'zgartirishga qanday qo'llaniladi?
15. Bulutli zahiralash sohasidagi eng so'nggi yangilanishlar qanday yo'lga qo'yilmoqda?

Amaliy ish № 8

PoE TEXNOLOGIYASIDAN FOYDALANISH

Ishdan maqsad: PoE (Power over Ethernet – Ethernet orqali quvvat uzatish) texnologiyasi bilan tanishish, uning ishlash prinsipi va turlarini tadqiq qilish.

Nazariy ma'lumot

PoE (Power over Ethernet) texnologiyasi bu o'ralgan-juft Ethernet kabel (UTP yoki STP) orqali ma'lumotlar oqimi bilan birgalikda elektr quvvatini ham uzatish imkonini beruvchi tizimni ifoda etadi. Bu simsiz ulanish nuqtalari (WAP – Wireless Access Point), IP kameralar va VoIP telefonlari kabi tarmoqqa ulanuvchi qurilmalarga bir vaqtning o'zida, bitta kabel orqali ham ma'lumot almashinish, ham yetarli elektr quvvati bilan ta'minlash imkonini beradi.

Power over Ethernet (PoE) texnologiyasi Ethernet tarmoq bir qator protokollarini qo'llab-quvvatlaydi. Ushbu texnologiya quvvat va ma'lumotlarni bir vaqtning o'zida Ethernet kabeli orqali uzatishga imkon beradi.

PoE texnologiyasi quyidagi Ethernet tarmoq protokollari bilan ishlaydi:

- 10BASE-T: Bu Ethernet tarmoq protokoli 10 Mbit/s tezlikda ishlaydi.
- 100BASE-TX: Bu Ethernet tarmoq protokoli 100 Mbit/s tezlikda ishlaydi.
- 1000BASE-T va undan tezroq: Bu Ethernet tarmoq protokollari Gigabit Ethernet va undan yuqoriroq tezliklarda ishlaydi.

Ethernet kabeli orqali quvvatni uzatishning bir qancha umumiy usullari mavjud. Ulardan uchtasi 2003 yildan beri “Elektr va elektronika muhandislari instituti” (IEEE) tomonidan IEEE 802.3 standarti bilan standartlashtirilgan.

Bular:

1. A-tur: 10BASE-T va 100BASE-TX odatdagi Cat 5 kabelidagi ma'lumotlar uchun ishlatadigan to'rtta signal juftligidan ikkitasini ishlatadi.
2. B-tur: 10BASE-T/100BASE-TX uchun ma'lumotlar va quvvat o'tkazgichlarini ajratib, muammolarni bartaraf etishni osonlashtiradi.
3. 4PPoE, barcha to'rtta o'ralgan juftlarni parallel ravishda ishlatib, erishish mumkin bo'lgan quvvatni oshiradi.

A-tur 10 va 100 Mbit/s Ethernet variantlari uchun ma'lumotlar bilan bir xil simlar orqali quvvatni uzatadi. Bu kondensatorli mikrofonlarni quvvatlantirish uchun keng qo'llaniladigan fantom quvvat texnikasiga o'xshaydi. Quvvat ma'lumotlar o'tkazgichlarida har bir juftga umumiy kuchlanish berish orqali uzatiladi. O'ralgan-juft Ethernet differensial signalizatsiyadan foydalanganligi sababli, bu ma'lumotlarni uzatishga xalaqit bermaydi. Umumiy rejimdagi kuchlanish standart Ethernet impuls transformatorining markaziy krani yordamida osongina chiqariladi. Gigabit Ethernet va undan yuqori tezlikda, ikkala muqobil A va B simli juftlikdagi transport quvvati ham ma'lumotlar uchun ishlatiladi, chunki barcha to'rt juftlik ushbu tezliklarda ma'lumotlarni uzatish uchun ishlatiladi.

4PPoE barcha to'rt juft o'ralgan simi yordamida quvvatni ta'minlaydi. Bu pan-tilt-zoom kameralari (PTZ), yuqori samarali WAP-lar yoki hatto noutbuk batareyalarini zaryadlash kabi amaliyotlar uchun yuqori quvvatni ta'minlaydi.

Asl IEEE 802.3af-2003 PoE standarti har bir portda 15,4 Vtgacha doimiy quvvatni (minimal 44 V DC va 350 mA) ta'minlaydi. Kabelda ba'zi quvvat sarflanganligi sababli quvvat bilan ta'minlangan qurilmada atigi 12,95 Vt quvvatga ega bo'lishi kafolatlangan.

IEEE 802.3at-2009 PoE standarti, shuningdek, PoE+ yoki PoE plus deb nomlanadi, 2-toifa qurilmalar uchun 25,5 Vtgacha quvvat beradi. 2009 yilgi standart quvvat bilan ta'minlangan qurilmaning barcha to'rt juftlikdan quvvat olish uchun foydalanishini taqiqlaydi. Ushbu ikkala standart ham IEEE 802.3-2012 nashriga kiritilgan.

IEEE 802.3bt-2018 standarti 802.3at quvvat imkoniyatlarini yanada kengaytiradi. U PoE++ yoki 4PPoE sifatida ham tanilgan. Standart ikkita qo'shimcha quvvat turini taqdim etadi: 51 Vtgacha etkazib beriladigan quvvat (3-toifa) va 71,3 Vtgacha etkazib beriladigan quvvat (4-toifa). Har bir juft o'ralgan juftlik 600 mA (3-toifa) yoki 960 mA (4-toifa) gacha bo'lgan oqimni boshqarishi kerak. Bundan tashqari, 2.5GBASE-T, 5GBASE-T va 10GBASE-T qo'llab-quvvatlanadi. Ushbu ishlanma yangi ilovalar uchun eshikni ochadi va yuqori samarali simsiz ulanish nuqtalari va kuzatuv kameralari kabi ilovalardan foydalanishni kengaytiradi.

IEEE 802.3bu-2016 avtomobil va sanoat ilovalari uchun mo'ljallangan bir juftlik Ethernet standartlari 100BASE-T1 va 1000BASE-T1 uchun bir juftlik ma'lumot uzatish liniyalari (PoDL)ni joriy qildi. Ikki juftlik yoki to'rt juftlik standartlarida juftlikning har bir o'tkazgichiga bir xil quvvat zo'riqishida qo'llaniladi, shuning uchun har bir juftlik ichida uzatilgan ma'lumotni ifodalovchi farqli kuchlanish yo'q. Bir juftlik Ethernet bilan quvvat ma'lumotlarga parallel ravishda uzatiladi. PoDL dastlab 0,5 dan 50 Vt gacha bo'lgan o'nta quvvat sinfini aniqladi (PDda).

Keyinchalik, PoDL bir juftlik 10BASE-T1, 2.5GBASE-T1, 5GBASE-T1 va 10GBASE-T1 variantlariga qo'shildi va 2021 yilga kelib qo'shimcha oraliq kuchlanish va quvvat darajalariga ega jami 15 ta quvvat sinfini o'z ichiga oladi.

Qo'llanilishi



8.1-rasm. PoE texnologiyasida ishlovchi qurilmalar

PoE orqali quvvatlanadigan qurilmalarga misollar:

- VoIP telefonlari
- IP kameralar, shu jumladan PTZ
- WAPlar
- IP TV (IPTV) dekoderlari
- Tarmoq routerlari
- Mini tarmoq "switch"lari

Power over Ethernet (PoE) texnologiyasi quyidagi tarmoq qurilmalarini qo'llab-quvvatlaydi:

- **IP kameralar:** IP kameralar tarmoq orqali video ma'lumotlarini uzatish uchun ishlatiladi. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi.

- **VoIP telefonlar:** VoIP telefonlar internet orqali ovozli muloqot uchun ishlatiladi. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi.

- **Wireless Access Points (WAP):** WAP-lar tarmoq ulanishini kengaytirish uchun ishlatiladi. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi.

- **Alarm tizimlari:** Alarm tizimlari xavfsizlik maqsadida ishlatiladi. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi.

- **PTZ kameralar:** PTZ kameralar harakatlanish, burilish va zoomlash xususiyatlariga ega bo'lgan video monitoring qurilmalaridir. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi.

- **Harakatni kuzatuvchi kameralar:** Harakatni kuzatuvchi kameralar harakatni aniqlash xususiyatiga ega bo'lgan video monitoring qurilmalaridir. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi.

- **Masofadan boshqariladigan kompyuter terminallari:** Masofadan boshqariladigan kompyuter terminallari masofadan boshqarish uchun ishlatiladi. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi.

- **Biometrik sensorlar:** Biometrik sensorlar shaxsiyatni tasdiqlash uchun ishlatiladi. Ular PoE texnologiyasidan foydalanish orqali bir kabel orqali quvvat va ma'lumotlarni olishadi¹.

PoE texnologiyasi quvvat talabini oshirish orqali yana ko'proq tarmoq qurilmalarini qo'llab-quvvatlashga imkon beradi.

Power over Ethernet (PoE) texnologiyasining bir nechta afzalliklari bor:

- O'rnatish xarajatlarini kamaytirish: Bir kabel orqali quvvat va ma'lumotlarni bir vaqtning o'zida yetkazish mumkinligi tufayli, PoE o'rnatish xarajatlari kamayadi. Shuningdek, PoE tizimlari o'rnatish uchun malakali elektrik talab etilmaydi.
- Xavfsizlik: PoE tizimlari juda xavfsizdir. Quvvat manba qurilmalari (PSE) faqatgina PoE qurilmalarini aniqlashda quvvat yetkazadilar.

- Moslashuvchanlik: PoE texnologiyasi tarmoq qurilmalarini o'rnatishda katta moslashuvchanlik beradi. Elektr rozetkasiga bog'liq bo'lmagan holda, siz qurilmalarni eng kerakli joyga o'rnatishingiz mumkin.
- Kengaytiriladigan: PoE texnologiyasi tarmoqni kengaytirishga imkon beradi. Ushbu texnologiya yana bir qurilmani qo'shish yoki olib tashlashda tarmoqni to'xtatmasdan ishlaydi.
- Ma'lumotlarni yig'ish: PoE texnologiyasi ma'lumotlarni yig'ish uchun juda qulay.
- Quvvat manbasi talablarini kamaytirish: Har bir o'rnatilgan qurilma uchun talab qilingan quvvat manba sonini kamaytiradi, bu esa pulni tejaydi.

Bu afzalliklar tufayli, PoE texnologiyasi tarmoq qurilmalarini o'rnatish va boshqarishni osonlashtiradi.

Power over Ethernet (PoE) texnologiyasining bir nechta kamchiliklari bor:

- Chegaraviy quvvat chiqishi: PoE standartiga qarab, qurilmaga yetkaziladigan quvvatning miqdori cheklangan bo'lishi mumkin, bu esa ba'zi yuqori quvvat talab qiladigan qurilmalar uchun yetarli bo'lmaydi.
- Masofa cheklovlari: PoE Ethernetning maksimal kabel uzunligi, odatda 100 metr (328 fut) bilan cheklangan.
- Bir nechta qurilmalarni bir vaqtning o'zida qo'llab-quvvatlash: Agar bir PoE quvvat manbasi yoki switch bir nechta qurilmalarga ulangan bo'lsa, agar shu PoE tarmoq qurilmalaridan birida muammo yuzaga kelsa, barcha qurilmalar ishlashni to'xtatadi.
- Quvvat yetkazish muammolari: So'nggi avlod PoE quvvat manbalari ba'zi quvvat yetkazish muammolari bilan bog'liq. Ayniqsa, ular standart pan, tilt va zoom kameralariga katta miqdorda quvvatni yetkaza oladilar, lekin ular yuqori quvvat iste'mol qiladigan qurilmalar uchun, masalan, tarmoq PTZ kameralari uchun yetarli elektr energiyasini ta'minlay olmaydilar.

Bu kamchiliklar tufayli, PoE texnologiyasini ishlatishda ehtiyot bo'lish kerak.

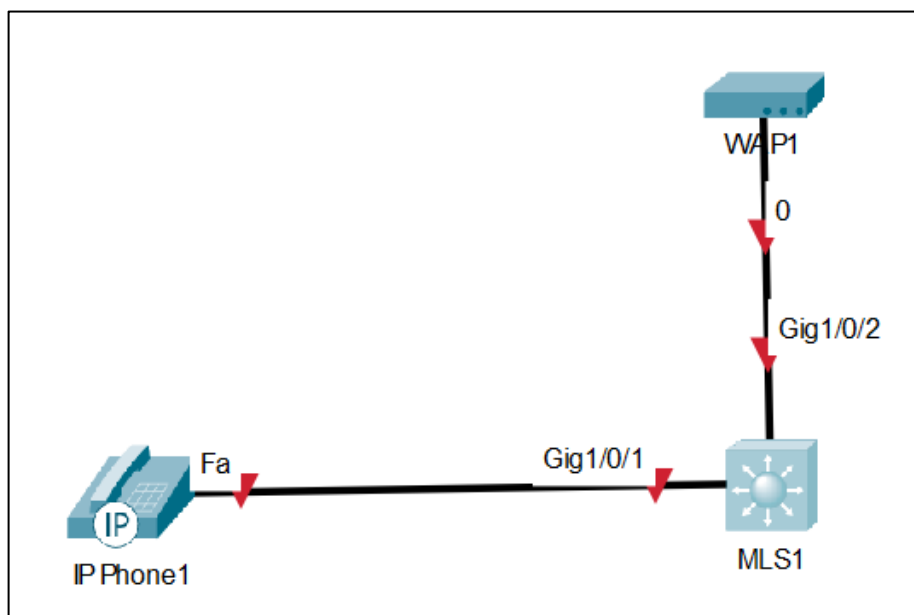
Power over Ethernet (PoE) texnologiyasi quyidagi standartlarga asoslangan:

- IEEE 802.3af: Bu standart 2003 yilda tasdiqlangan va quvvatni yoki ma'lumotlarni uzatish uchun ishlatiladigan simlar to'g'risida talablar beradi.
- IEEE 802.3at (PoE+ yoki Type 2): Bu standart 2009 yilda tasdiqlangan va quvvatni 30W gacha oshiradi²⁴.
- IEEE 802.3bt (4PPoE Type 3 va Type 4): Bu standart 2018 yilda tasdiqlangan va quvvatni 60W (Type 3) va 90W (Type 4) gacha oshiradi.

Har bir yangi standart oldingi barcha standartlar bilan uyg'un holda ishlashni va moslashuvchanligini ta'minlaydi va portga yetkaziladigan minimal quvvat miqdorini belgilaydi. Bu minimal talab kabelning uzunligi bo'yicha quvvat yo'qolishini hisobga oladi, bu esa maksimal uzunlikni 100m (328 fut) gacha belgilaydi. Har bir quvvat oshirish bilan, kabel talablari ham oshadi, Cat 5 kabeli Type 3 (60W) va Type 4 (90W) PoE uchun minimal talab bo'lib qoladi.

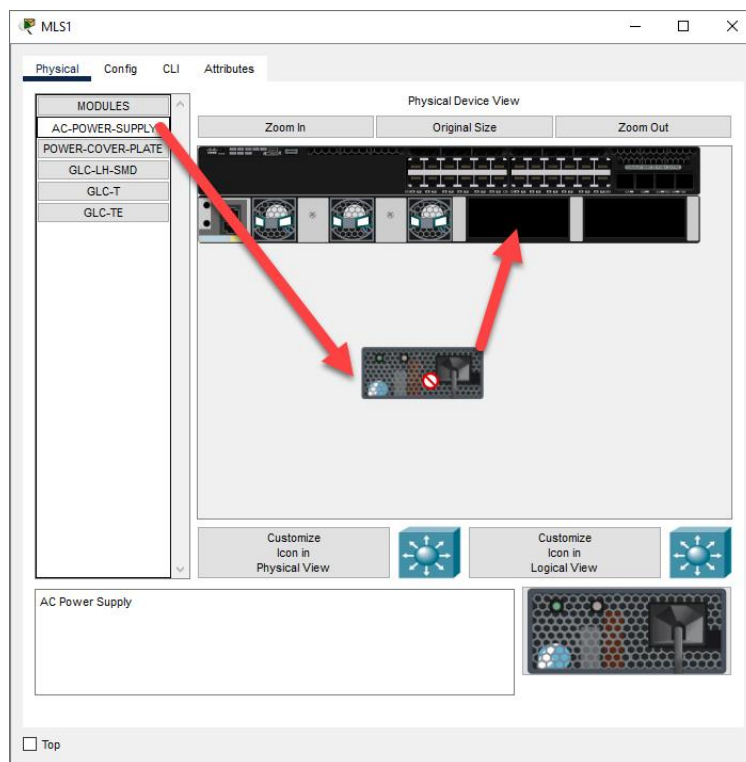
Amaliy ishni bajarish tartibi:

1. Avvaliga "Cisco Packet Tracer" simulatorida PoE texnologiyasini qo'llab-quvvatlovchi WAP va IP telefon mavjud bo'lgan sodda topologiya qurib olamiz. Cisco 3-pog'ona kommutator IP phone va WAPni ish maydoniga qo'shgandan so'ng, biz barcha qurilmalarni kabellar bilan ulaymiz.



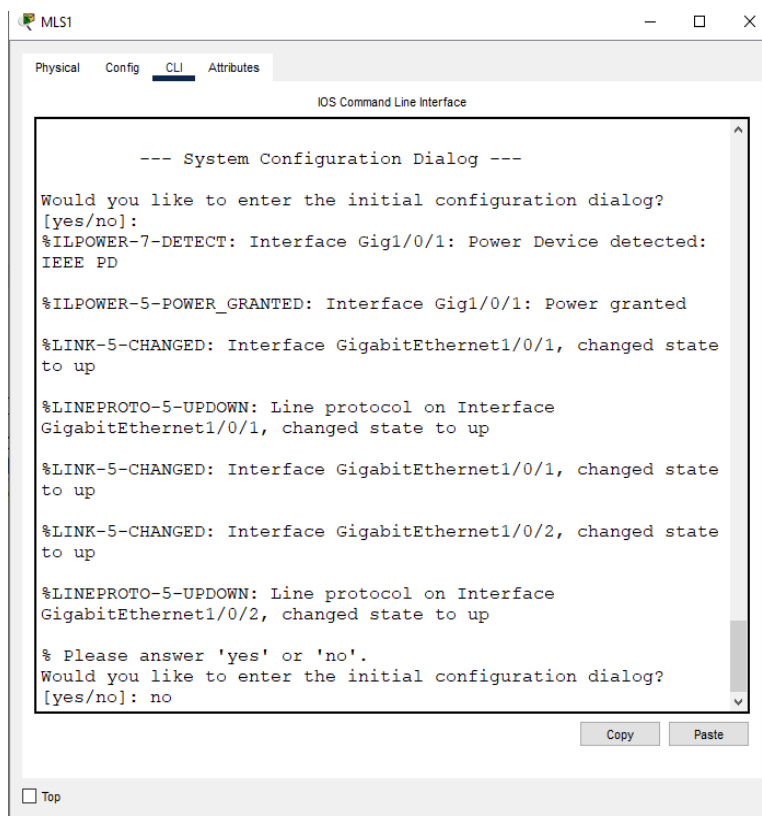
8.2-rasm. Tarmoqni qurish

2. So'ngra esa "MLS1"ni ustiga bir marta sichqonchanning chap tomoni bilan bosib, ochilgan oynaning "Physical" bo'limiga o'tamiz. U yerdan "MLS1"ning qo'shimcha modullari ro'yhatidan "AC-POWER-SUPPLY" quvvat manbasini tanlab, sichqonchanning chap tomonini bosib turgan holda ushlab, kommutatorga ulaymiz.



8.3-rasm. Quvvat blokini oʻrnatish

3. CLI buyruq satrini ochish uchun kommutatorni ikki marta bosing. Dastlabki oʻrnatishni oʻtkazib yuborish uchun "No" deb yozing va Enter ni bosing.



8.4-rasm. Qurilmani sozlash

4. Keyingi bosqichda kommutatorning quvvat sozlamalari ko‘rish uchun **show power inline** buyrug‘uni beramiz va natijada quyidagicha natija olamiz:

```
Switch>en
Switch#show power
Switch#show power inline
Available:390.0(w) Used:10.0(w) Remaining:380.0(w)
Interface Admin Oper PowerDevice Class Max
(Watts)
-----
Gig1/0/1 autoon10.0 Switch 79603 30.0
Gig1/0/2 autooff 0.0 n/a n/a30.0
Gig1/0/3 autooff 0.0 n/a n/a30.0
Gig1/0/4 autooff 0.0 n/a n/a30.0
Gig1/0/5 autooff 0.0 n/a n/a30.0
Gig1/0/6 autooff 0.0 n/a n/a30.0
Gig1/0/7 autooff 0.0 n/a n/a30.0
Gig1/0/8 autooff 0.0 n/a n/a30.0
Gig1/0/9 autooff 0.0 n/a n/a30.0
Gig1/0/10 autooff 0.0 n/a n/a30.0
Gig1/0/11 autooff 0.0 n/a n/a30.0
Gig1/0/12 autooff 0.0 n/a n/a30.0
Gig1/0/13 autooff 0.0 n/a n/a30.0
Gig1/0/14 autooff 0.0 n/a n/a30.0
Gig1/0/15 autooff 0.0 n/a n/a30.0
Gig1/0/16 autooff 0.0 n/a n/a30.0
Gig1/0/17 autooff 0.0 n/a n/a30.0
Gig1/0/18 autooff 0.0 n/a n/a30.0
Gig1/0/19 autooff 0.0 n/a n/a30.0
Gig1/0/20 autooff 0.0 n/a n/a30.0
Gig1/0/21 autooff 0.0 n/a n/a30.0
Gig1/0/22 autooff 0.0 n/a n/a30.0
Gig1/0/23 autooff 0.0 n/a n/a30.0
Gig1/0/24 autooff 0.0 n/a n/a30.0
```

Natija shuni ko‘rsatyaptiki, kommutatorning har bir porti maksimal 30 Vt quvvat ta‘minlab, umumiy hisobda 390 Vt quvvat yetkazib bera oladi.

Amaliy ish bo'yicha savollar:

1. PoE texnologiyasi nima?
2. PoE texnologiyasi qanday ishlaydi?
3. PoE texnologiyasi qanday qurilmalarni qo'llab-quvvatlaydi?
4. PoE texnologiyasi qanday foydalar keltiradi?
5. PoE texnologiyasi qanday kamchiliklarga ega?
6. PoE texnologiyasi qanday standartlarga asoslangan?
7. PoE+ nima?
8. PoE+ va UPOE orasidagi farq nima?
9. IEEE 802.3at PoE+ standarti qachon tasdiqlandi?
10. PoE texnologiyasi qanday tarmoq qurilmalarini qo'llab-quvvatlaydi?
11. PoE texnologiyasi qanday ishlab chiqaruvchilar tomonidan ishlatiladi?
12. PoE texnologiyasi qanday sohalarda foydalaniladi?
13. PoE texnologiyasi qanday xavfsizlik muammolari bilan bog'liq?
14. PoE texnologiyasi qanday texnik xususiyatlarga ega?
15. PoE texnologiyasi qanday tarmoq standartlari bilan ishlaydi?
16. PoE texnologiyasi qanday tarmoq protokollari bilan ishlaydi?
17. PoE texnologiyasi qanday tarmoq topologiyalarida ishlaydi?
18. PoE texnologiyasi qanday tarmoq qurilmalariga mos keladi?
19. PoE texnologiyasi qanday tarmoq qurilmalariga mos kelmaydi?
20. PoE texnologiyasi qanday tarmoq qurilmalarini qo'llab-quvvatlash uchun qanday quvvat talab qiladi?

Amaliy ish № 9

TARMOQDAGI TRAFIK OQIMINI BOSHQARISH

Ishdan maqsad: Kompyuter tarmoqlaridagi trafikni boshqarish usul va vositalarini o'rganish, mavjud amaliy dasturlar bilan tanishish.

Tarmoq trafigini boshqarish deganda tarmoq trafigini "tutib olish" (*capture*) va tahlil qilish hamda ustuvorliklar asosida trafikni optimal resurslarga yo'naltirish jarayoni tushuniladi. Tarmoqingizni yaxshiroq boshqarish uchun kuzatilishi kerak bo'lgan asosiy komponentlar qatoriga tarmoq unumdorligi, trafik va xavfsizlik kiradi. Tarmoq trafigini boshqarish vositasi tarmoqning kengligi va tarmoq unumdorligini monitoring qilish, to'siqlarni aniqlash va oldini olish uchun trafik naqshlarini kuzatish, tarmoq xavfsizligini tahlil qilish va tarmoqning optimal ishlashini ta'minlash uchun optimallashtirish kabi boshqaruv usullaridan foydalanadi. Bu tarmoq tiqilib qolishi va tahdidlarni oldini olish orqali tarmoqning ishlashi va xavfsizligini maksimal darajada oshirishga yordam beradi.

Tarmoq trafiginı boshqarish dasturining afzalliklari:

- *Uzilishlarning oldini olish:* real vaqtda tarmoq unumdorligi ma'lumotlarini ko'rish imkonini beradi hamda yuzaga kelishi mumkin bo'lgan muammolar va uzilishlarni aniqlash va oldini olishga yordam beradi.
- *Muammolarni tez va samarali hal qilish:* real vaqt rejimida tarmoqdagi to'siqlarni va boshqa tarmoq muammolarini, jumladan, trafik harakati va konfiguratsiya o'zgarishlaridagi tartibsiz o'zgarishlarni aniqlash orqali muammolarni hal qilishni osonlashtiradi.
- *Tarmoq o'zgarishlarini boshqarish:* Tarmog'ingizdagi o'sish va o'zgarishlarga moslashishga, g'ayritabiiy tebranishlar yoki tahdidlarni aniqlash uchun ularni kuzatishga, trafik harakatini bashorat qilishga va tarmoq talablariga mos kelishini ta'minlash uchun talablarni rejalashtirishga yordam beradi.
- *Xavfsizlik tahdidlarini aniqlash:* tarmoq xatti-harakatlarini tahlil qilish orqali sizga kerak bo'lgan xavfsizlik darajasini xavfsizlik tahdididan yoki nol kunlik bosqin kabi jiddiy narsadan farqlash uchun beradi.

Tarmoq trafiginı boshqarish vositasi:

Haqiqiy vaqtda tarmoq trafiginı boshqarish vositalarining aksariyati tarmoqli kengligi monitoringi va optimallashtirish xususiyatlarini o'z ichiga olgan bo'lsa-da, ularning echimlari faqat shu bilan cheklangan. Tarmoq trafiginı boshqarishning deyarli har doim e'tibordan chetda qoladigan eng muhim jihatlaridan biri bu tarmoq xavfsizligi va xatti-harakatlar tahlilidir. Tarmoq trafiginı kuzatuvchiga qo'shimcha ravishda kuchli xavfsizlik yechimiga ega bo'lmaslik tarmog'ingizni hujumlarga qarshi himoyasiz qoldirishi mumkin.

Ideal tarmoq trafiginı boshqarish vositasi:

- Tarmoqqa real vaqtda ko'rinishni ta'minlash;
- Xulq-atvor namunalarini tahlil qiling va trafikni faol ravishda boshqaring;
- Tez va samarali diagnostika va muammolarni bartaraf etish;
- Tarmoqingizni nol kunlik (*zero-day*) hujumlar, ichki tahdidlar va noma'lum qurtlardan (*worms*) himoyalash;

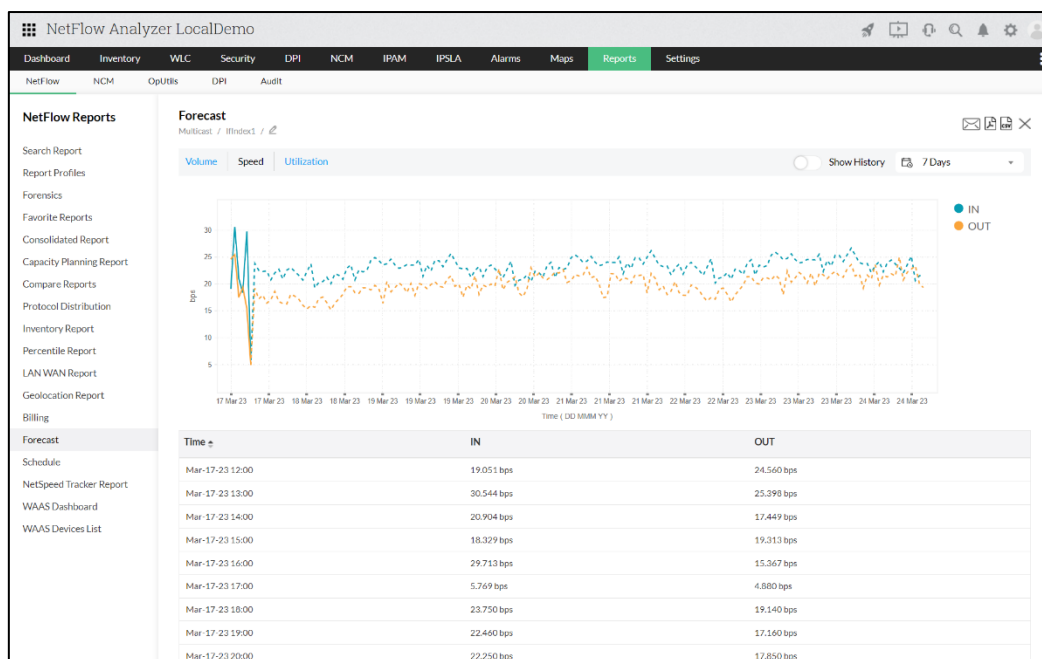
NetFlow Analyzer yordamida real vaqtda tarmoq trafiginı boshqarish

Tarmoq trafiginı nazorat qilish va boshqarish sizning tarmog'ingizdan maksimal darajada foydalanishni ta'minlash uchun juda muhimdir; NetFlow Analyzer kabi tarmoq trafiginı boshqarishning to'liq yechimi tarmog'ingizda nima sodir bo'layotganini tushunishni ancha osonlashtiradi. NetFlow Analyzer

biznesingiz uchun muhim bo'lgan ilovalarning ustuvorligini ta'minlashdan tashqari, o'tkazish qobiliyatini cheklab qo'yishiga yo'l qo'ymaslik bilan bir qatorda, NetFlow Analyzer boshqa turli xil afzalliklarni taklif etadi, jumladan, tarmog'ingizni uzilishlardan himoya qilish, muammolarni tezroq bartaraf etish va tuzatishga yordam berish, yuzaga kelishi mumkin bo'lgan to'siqlarni oldindan ko'rish va oldini olish, boshqaruv Rivojlanayotgan tarmog'ingiz, xavfsizlik tahdidlarini yanada samarali aniqlash va natijada ROI ni oshirish.

Tarmoq traficinging “end-to-end” monitoring:

Tarmog'ingizdagi uzilishlar yoki tirbandliklarning ko'p sabablari mavjud, jumladan, inson xatosi va xavfsizlikka tahdidlar kabi. Tarmoq traficingingizning real vaqt rejimida ko'rinishi tarmoq unumdorligiga ta'sir qilishi mumkin bo'lgan har qanday muammolarni proaktiv tarzda kuzatish va aniqlashga yordam berish uchun zarur. NetFlow Analyzer tarmoq traficingini boshqaruvchi sizga 50 dan ortiq sozlanishi mumkin bo'lgan hisobot va grafiklar bilan tarmog'ingiz haqida to'liq ma'lumot beradi. U tarmog'ingizda nimalar sodir bo'layotgani haqida turli ko'rsatkichlar, masalan, har bir qurilma va ilova uchun tarmoqli kengligidan foydalanish, eng yaxshi foydalanuvchilar va suhbatlar, kechikish va jitter haqida aniq tasvirni ko'rsatadi. NetFlow Analyzer shuningdek, ovoz balandligi, tezlik va foydalanishga asoslangan chegara ogohlantirishlarini o'rnatishga yordam beradi va sizni elektron pochta, SMS, SNMP tuzog'i yoki yordam stoli chiptasi orqali xabardor qiladi.



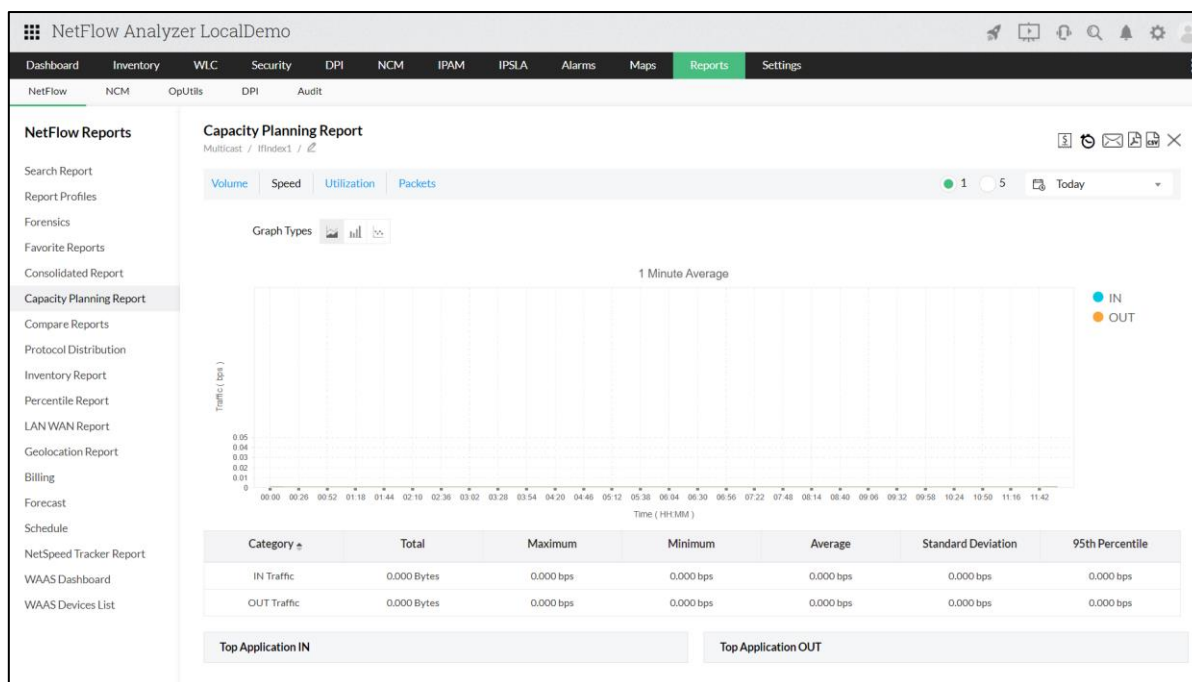
9.1-rasm. NetFlow Analyzer yordamida trafik sarfini bashorat qilish

Ko'pgina IT-ma'murlar (adminlar) to'siqlar va boshqa nosozliklarni aniq bashorat qiladigan va ular paydo bo'lishidan oldin ishlash bilan bog'liq

muammolarni hal qilishga imkon beradigan tarmoq trafigini boshqaruvchiga ega bo'lishni xohlashadi. NetFlow Analyzer tarmoqli kengligidan foydalanish tendentsiyalarini prognoz qilish uchun avtokorrelyatsiya, mavsumiylik tendentsiyasini yo'qotish dekompozitsiyasi va regressiya kabi usullardan foydalanadi. O'zining sig'imini rejalashtirish xususiyati bilan u sizga istalgan tanlangan vaqt oralig'ida trafik faolligingiz va tarmoqli kengligidan foydalanish tendentsiyalari, trafigingiz va ilovalaringizning o'sishining yaxlit ko'rinishini beradi, shuningdek, o'tkazish qobiliyatiga bo'lgan talablaringizni rejalashtirish va har qanday anomaliyalarni aniqlash bo'yicha asosli qarorlar qabul qilishingizga yordam beradi. trafikning o'sishi.

Yaxshiroq tarmoq trafigini boshqarish tizimi uchun trafikni shakllantirish:

Tarmoq trafigini boshqarish ma'lum ilovalar va foydalanuvchilarga o'tkazish qobiliyatini cheklash, trafik va ilovalarga ustuvorlik berish va barcha foydalanuvchilar uchun ma'lum bir maksimal yoki minimal tarmoqli kengligini ta'minlashni o'z ichiga oladi. Trafikni shakllantirish - bu biznes uchun muhim bo'lmagan ilovalar va foydalanuvchilar tomonidan iste'mol qilinadigan tarmoqli kengligini sezilarli darajada cheklaydigan boshqaruv usuli. Yuqori ustuvor vazifalar va ilovalarning optimal bajarilishini ta'minlash uchun muayyan oqimlarni yoki paketlarni kechiktiradi.

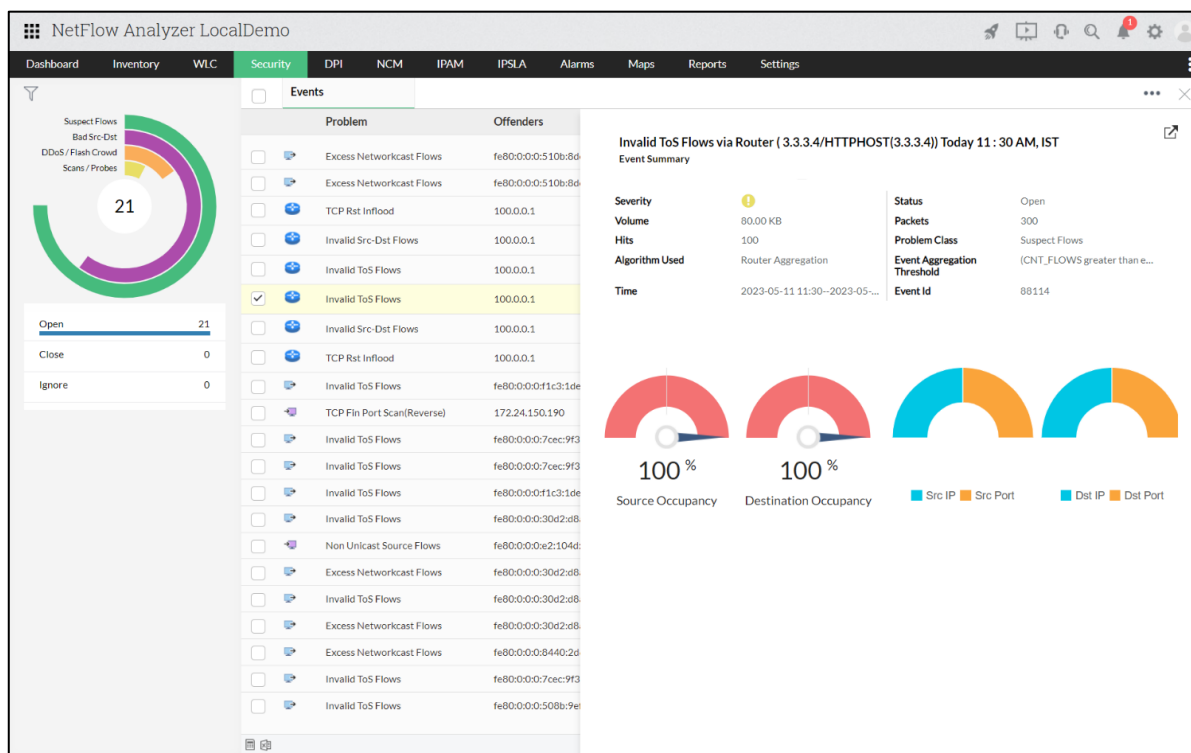


9.2-rasm. Tarmoq o'tkazuvchanligini rejalashtirish

NetFlow Analyzer sizga xizmat ko'rsatish sifati siyosatlarini qayta sozlashda yordam berish uchun kirishni boshqarish ro'yxati (ACL) va Xizmat siyosati kabi trafikni shakllantirishning turli usullaridan foydalanadi. Bu muhim bo'lmagan IP va o'tkazish qobiliyatini oshiruvchi ilovalarni cheklash yoki blokirovka qilish orqali tarmoqning yaxshi ishlashini ta'minlashga yordam beradi. NetFlow Analyzer'ning Cisco CBQoS tizimi sizga sinfga asoslangan trafik namunalarini ko'rish imkonini beradi, bu sizning siyosatlarigiz va ularning ishlashini tekshirishga yordam beradi.

Tarmoq xavfsizligi va xatti-harakatlarini tahlil qilish

Tarmoq xavfsizligi uchun bir nechta xavfsizlik devorlariga qo'shimcha ravishda hujumni aniqlash vositalariga ega bo'lish har doim ham oson yoki mumkin bo'lgan variant emas. NetFlow Analyzer'ning ilg'or xavfsizlik tahlili moduli xavfsizlik devoridan oshib ketgan har qanday hujum yoki hujumni aniqlashga yordam beradigan oqimga asoslangan xavfsizlik tahlili va anomaliyalarni aniqlash vositasidir. Bu sizga tarmoqning umumiy ishlashiga ta'sir qilishi va uni to'xtatib qo'yishi mumkin bo'lgan botnetlar, tarqatilgan xizmat ko'rsatishni rad etish hujumlari, nol kunlik hujumlar va zondlar kabi keng ko'lamli ichki va tashqi tahdidlar yoki tajovuzlarni aniqlash uchun amaliy razvedka beradi. NetFlow Analyzer tahdid hujumga aylanishidan oldin tarmog'ingizni himoya qilish uchun har bir oqimni kuzatib boradi va bu ma'lumotlarni bitta ko'rinishda taqdim etadi.



9.3-rasm. NetFlow Analyzerning xavfsizlik imkoniyatlari

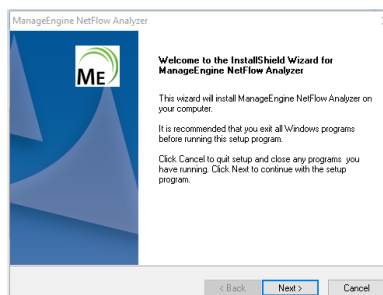
NetFlow Analyzer - o'tkazish qobiliyati monitoringi va yagona trafik tahlilini taklif qiluvchi mustahkam va kengaytiriladigan platformadir.

“NetFlow Analyzer”ni o'rnatish:

1. NetFlow Analyzerni Windows kompyuterga o'rnatish uchun uning EXE-o'rnatuvchisini quyidagi havola orqali o'rnatib olish kerak:

<https://www.manageengine.com/products/netflow/>

2. Yuklab olingandan keyin, o'rnatuvchisi ustiga sichqonchanning o'ng tomoni bilan 2 marta bosamiz va ketma-ketlikda “Keyingi” tugmalarini bosib, dasturni o'rnatamiz.



3. Dastur o'rnatilishi tugaganidan keyin, NetFlow Analyzer dasturi avtomatik tarzda, veb-ilova ko'rinishda, brauzerda ishga tushadi. Dastur birinchi marta ishga tushirilganda tizimga kirish uchun login va parolni bilish talab etiladi. Login va parol dastlabki holatda admin/admin shaklida bo'ladi.

"NetFlow Analyzer"ning asosiy imkoniyatlari quyidagilardan iborat:

1. Tarmoq Bandwidth va Traffik Tahlili: NetFlow Analyzer, tarmoq bandwidth ishlab chiqarishini real vaqtda ko'rish uchun flow texnologiyalaridan foydalanuvchi to'liq trafik tahlil vositasi¹. U tarmoq bandwidth va trafik namunalari haqida umumiy tasavvur beradi¹.
2. Tarmoq Forensik va Xavfsizlik Tahlili: NetFlow Analyzer, tarmoqning tashqi va ichki xavfsizlik tahdidlarini aniqlash uchun Continuous Stream Mining Engine texnologiyasidan foydalanadi¹. U tarmoqni shubhali faoliyatlar uchun monitoring qiladi¹.
3. Ilova-centric Monitoring va Traffik Shaping: NetFlow Analyzer, tarmoq bandwidthini egallaydigan standartdan tashqari ilovalarni aniqlash va sinflandirish uchun Cisco NBAR'dan foydalanadi¹. U ACL yoki sinf-asosida siyosat orqali trafik shaping texnikasini qayta konfiguratsiya qilish orqali bandwidth-oshiq ilovalar ustida nazorat olish imkoniyatini beradi¹.

4. Capacity Planning va Billing: NetFlow Analyzer, bandwidth o'sishiga oid ma'lumotlar asosida ma'lumotli qarorlar qabul qilish uchun capacity planning hisobotlarini taqdim etadi¹. Uzun muddatli hisobotlarning yordamida bandwidth o'sishini o'lchash mumkin¹.

5. Multivendor Support va Flow Texnologiyasi: NetFlow Analyzer, asosiy qurilmalar, shu jumladan Cisco, 3COM, Juniper, Foundry Networks, Hewlett-Packard, extreme va boshqa bir nechta yetakchi vendorlardan oqimlarni yig'ib, tahlil qiladi¹.

Bu dastur tarmoq administratorlariga tarmoq bandwidth va trafik tahlilini osonlashtiradi, shuningdek, bandwidth ishlatilishini optimallashtirish, tarmoq forensik, tarmoq trafik tahlili va tarmoq oqim monitoringini amalga oshiradi.

Nazorat savollari:

1. Tarmoq trafigi boshqaruvi nima?
2. Tarmoq trafigi boshqaruvi nima uchun zarur?
3. Tarmoq trafigi boshqaruvi qanday amalga oshiriladi?
4. Tarmoq trafigi boshqaruvi uchun qanday dasturlar mavjud?
5. Tarmoq trafigi boshqaruvi uchun qanday uskunarlar kerak?
6. Tarmoq trafigi boshqaruvi qanday tarmoq muammolarini bartaraf etishga yordam beradi?
7. Tarmoq trafigi boshqaruvi tarmoq xavfsizligiga qanday ta'sir qiladi?
8. Tarmoq trafigi boshqaruvi tarmoqning ishlash tezligiga qanday ta'sir qiladi?
9. Tarmoq trafigi boshqaruvi tarmoqning ishonchli ishlashini qanday ta'minlaydi?
10. Tarmoq trafigi boshqaruvi tarmoq administratoriga qanday yordam beradi?
11. Tarmoq trafigi boshqaruvi tarmoqning samaradorligini qanday oshiradi?
12. Tarmoq trafigi boshqaruvi tarmoqning resurslari qanday ishlatilishini qanday ta'sir qiladi?
13. Tarmoq trafigi boshqaruvi tarmoqning yuklanishini qanday nazorat qiladi?
14. Tarmoq trafigi boshqaruvi tarmoqning yuklanishini qanday optimallashtiradi?
15. Tarmoq trafigi boshqaruvi tarmoqning yuklanishini qanday hisoblash uchun qanday usullar mavjud?

Amaliy ish № 10

CISCO PACKET TRACER DASTURIDA STATIK MARSHRUTLASHNI SOZLASH

Ishdan maqsad: Marshrutizator orqali statik marshrutlash bilan ishlash ko`nikmasiga ega bo`lish.

Nazariy qism

Marshrutlash - bu tarmoqlar o'rtasida yoki tarmoq ichida ma'lumotlarni uzatish yo'lini tanlash jarayoni. Bir nechta asosiy marshrutlash usullari mavjud bo'lib, ular ishlash tamoyillari, algoritmlari va ishlatiladigan protokollari bilan farqlanadi.

Marshrutlash usullarining tasnifi:

1. Statik marshrutlash

- Administrator har bir tarmoq qurilmasida marshrutlarni qo'lda o'rnatadi.
- Marshrutlar belgilangan va tarmoq topologiyasi o'zgarganda avtomatik ravishda o'zgarmaydi. Ijobiy tomonlari:

- Kichik tarmoqlarda oson sozlash.
- Qurilma protsessoriga yuk yo'q.

Kamchiliklari:

- Katta tarmoqlarda mehnat talab qiladigan sozlash va boshqarish.
- Moslashuvchan bo'lmagan: nosozliklar bo'lsa, marshrutlar qayta tiklanmaydi.

2. Dinamik marshrutlash

- Tarmoqdagi o'zgarishlar asosida marshrutlash jadvallarini avtomatik yangilaydigan marshrutlash protokollaridan foydalanadi.

- Protokollarga misollar: OSPF, RIP, EIGRP, BGP. Ijobiy tomonlari:
- Moslashuvchanlik: nosozliklar yoki topologiya o'zgarganda marshrutlar qayta quriladi.

- Katta tarmoqlarda boshqarish qulayligi.

Kamchiliklari:

- Keyinchalik sozlash murakkablasha boradi.
- Marshrut hisob-kitoblari tufayli protsessor va marshrutizatorlar xotirasiga yuklash.

Qo'llanilishi sohalari:

- o'rta va katta tarmoqlar.
- Internet provayderlari, korporativ tarmoqlar.

3. Birlamchi marshrutlash

- Qurilma maxsus marshrut mavjud bo'lmagan barcha trafikni "standart marshrut" ga yo'naltiradi.

- Masalan, barcha tashqi so'rovlar ISP shlyuziga yuboriladi. Ijobiy tomonlari:

- Konfiguratsiyani soddalashtiradi, ayniqsa tashqi tarmoqlar bilan ishlashda.

Kamchiliklari: - Agar sozlamalar noto'g'ri bo'lsa, muammolar paydo bo'lishi mumkin (masalan, pastadirlar).

4. **Qoidalarga asoslangan marshrutlash (PBR)**

- Marshrut tanlash nafaqat marshrutlash jadvallari asosida, balki boshqa mezonlar bo'yicha ham amalga oshiriladi: trafik turi, IP-manzillar, portlar. Ijobiy tomonlari: - Yo'l harakati boshqaruvida moslashuvchanlik.

- Yuklarni taqsimlash uchun javob beradi.

Kamchiliklari: - Keyinchalik murakkab sozlash.

- Qurilmadagi yuk ortdi.

Qo'llanilish sohasi:

- korporativ tarmoqlarda trafikni optimallashtirish.

- Trafikni farqlash (masalan, VoIP ustuvorligi uchun).

5. Multicast marshruting

- Paketlarni bir vaqtning o'zida bir nechta oluvchilarga etkazish uchun foydalaniladi (masalan, videoni translyatsiya qilishda).

- Protokollar: PIM (Protocol Independent Multicast), IGMP. Ijobiy tomonlari: - tarmoq resurslaridan samarali foydalanish.

Kamchiliklari: - Qo'shimcha uskunalarni konfiguratsiyasini talab qiladi.

Ilova: - Videokonferensaloqa tizimlari, IPTV, striming.

Marshrutlash protokollariga quyidagilar misol bo'ladi:

Ichki marshrutlash protokollari (IGP): - RIP (Routing Information Protocol): kichik tarmoqlar uchun mos keladigan oddiy protokol.

- OSPF (Open Shortest Path First): yirik tarmoqlar uchun murakkab, ammo samarali protokol.

- EIGRP (Enhanced Interior Gateway Routing Protocol): Cisco kompaniyasining gibril protokoli.

- Tashqi marshrutlash protokollari (EGP):

- BGP (Border Gateway Protocol): Internetda marshrutlash uchun foydalaniladi.

Xulosa qilib quyidagi Tavsiyalarni olish mumkin:

- Kichik tarmoqlar uchun "statik marshrutlash" dan foydalaning.

- O'rta va katta tarmoqlarda “dinamik marshrutlash” (OSPF yoki EIGRP) dan foydalaning.

- Prioritetlashtirish yoki optimallashtirish bilan murakkab tarmoq stsenariylari uchun “qoidali marshrutlash” dan foydalaning.

Standart shlyuz yoki default gateway — mahalliy tarmoqdan boshqa tarmoqlarga, masalan, Internetga ma'lumotlarni uzatish uchun yo'riqnoma vazifasini o'taydigan tarmoqdagi qurilma. Agar kompyuter yoki boshqa qurilma maqsadli tarmoqqa paketni qanday yuborishni bilmasa, uni standart shlyuz orqali o'tkazadi, bu esa o'z navbatida ma'lumotlarni kerakli tarmoqqa yo'naltiradi. Nega bizga standart shlyuz kerak?

Qurilma (masalan, kompyuter) mahalliy tarmog'ida bo'lmagan manzilga (masalan, Internet) ma'lumotlarni yuborishga harakat qilganda, u ushbu ma'lumotlarni standart shlyuzga yuboradi. Standart shlyuz:

1. Trafikni tashqi tarmoqqa yo'naltiradi, agar u o'zining marshrut jadvalida mos marshrutni topa olmasa.

2. Agar qurilma u yerga qanday borishni bilmasa, Internetga trafikni yo'naltiradi (yoki boshqa masofaviy tarmoq).

3. Lokal tarmoq ichida jo'natib bo'lmaydigan barcha paketlar uchun chiqish nuqtasi sifatida ishlaydi.

Birlamchi shlyuz qanday ishlaydi?

Aytaylik, sizda IP diapazoni 192.168.1.0/24 bo'lgan mahalliy tarmoq mavjud va 192.168.1.10 IP manzilli kompyuteringiz mahalliy tarmog'ingizdan tashqaridagi veb-saytga (masalan, example.com) kirishga harakat qilmoqda. .

1. Kompyuter veb-sayt IP-manzili (masalan, 93.184.216.34) uning tarmog'ida (192.168.1.0/24) mavjudligini tekshiradi.

2. Ushbu manzil mahalliy tarmoq oralig'ida bo'lmaganligi sababli, kompyuter standart shlyuzga (masalan, 192.168.1.1) so'rov yuboradi.

3. Standart shlyuz trafikni Internetga qanday yo'naltirishni hal qiladi va uni tegishli tashqi routerga yo'naltiradi.

Standart shlyuzni sozlash bosqichlari:

1. Kompyuterda (Windows/macOS/Linux):

- Windows-da standart shlyuzni tarmoq ulanishi sozlamalari orqali sozlash mumkin. Ko'pgina hollarda, agar kompyuteringiz routerga ulangan bo'lsa, standart shlyuz avtomatik ravishda DHCP (Dynamic Host Configuration Protocol) orqali tayinlanadi.

- Qo'lda sozlash uchun:

- Tarmoq sozlamalarini oching va ulanish xususiyatlarida "Standart shlyuz" ni toping.

- Routerning IP manzilini kiriting, masalan, 192.168.1.1.

2. Routerda:

- Routerlarda ko'pincha Internetga kirish uchun standart shlyuzdan foydalaniladi. Bu odatda router ISP ga ulanganda avtomatik ravishda sozlanadi.

- Qo'lda sozlash uchun yo'riqnoma interfeysiga o'ting va ISP tomonidan taqdim etilgan standart shlyuzni belgilang (odatda ISP IP-manzili).

3. Korporativ yoki murakkabroq tarmoqlarda:

- Standart shlyuz router yoki server darajasida sozlanishi mumkin.

- Murakkab marshrutlar uchun ****dinamik marshrutlash**** dan foydalanish mumkin (masalan, OSPF yoki BGP protokollari yordamida).

Tarmoqdagi standart shlyuzning roli

- Mahalliy tarmoqdan tashqarida ma'lumotlarni yuborish: Tarmoqdagi qurilmalar o'zlarining quyi tarmog'idan tashqarida ma'lumotlarni qanday yuborishni bilmasa, ular standart shlyuzdan foydalanadilar.

- Traffic konsolidatsiyasi: shlyuz filtrlash, xavfsizlik va boshqa funksiyalarni ta'minlab, Internetga kirishni markazlashtirilgan tarzda boshqarishga yordam beradi.

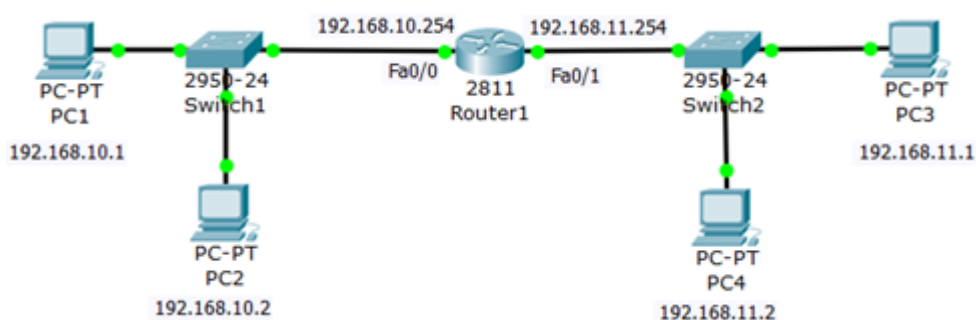
Standart shlyuzlarning odatiy misollari

- 192.168.0.1 yoki 192.168.1.1: Bular uy routerlarida (masalan, TP-Link, D-Link, Netgear va boshqalar) eng keng tarqalgan standart shlyuz IP manzillari.

- 10.0.0.1: Ko'pincha yirikroq yoki korporativ tarmoqlarda qo'llaniladi.

Amaliy ishni bajarish tartibi

Marshrutizator orqali ikkita tarmoqning ulanishini sozlash ko'rib chiqamiz (10.1-rasm).

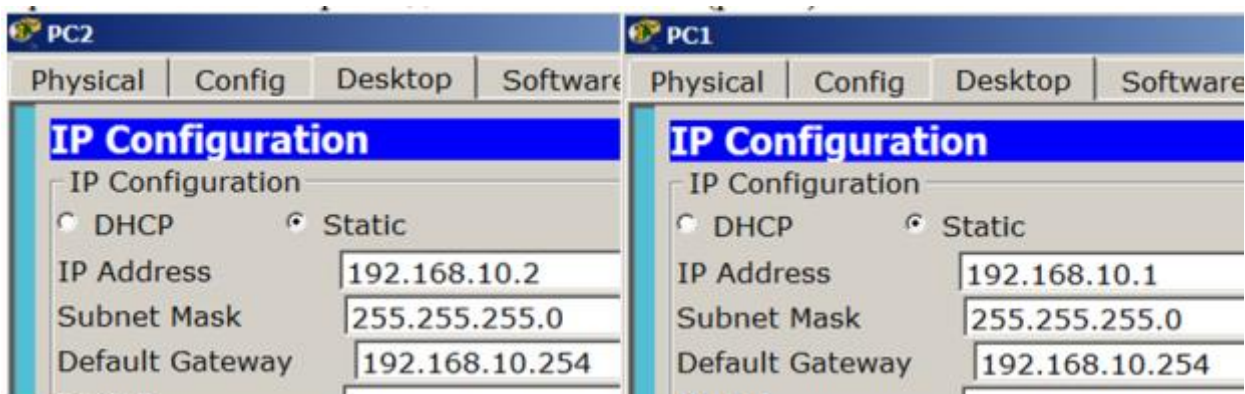


10.1-rasm. Masalaning qo'yilishi

Bizning maqsadimiz - marshurizator orqali ikkita tarmoqning ulanishini sozlash.

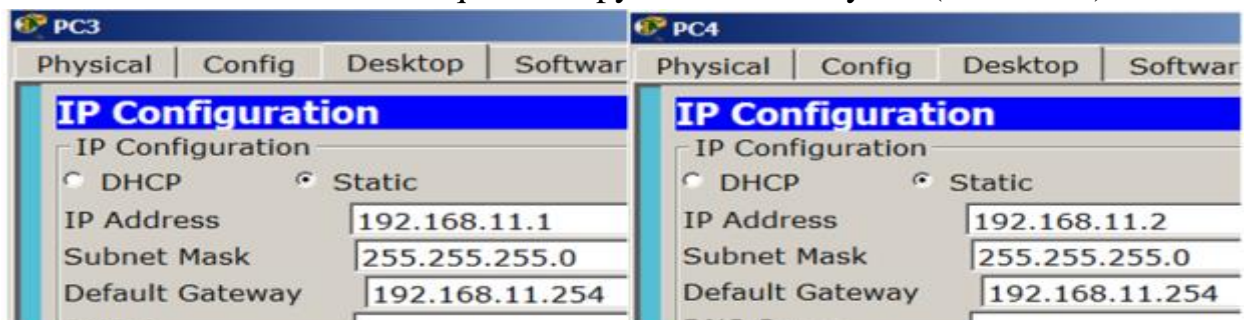
1-Qadam. Kompyuterni sozlash

Biz 192.168.10.0 kichik tarmog'ida kompyuterlarni sozlaymiz (10.2-rasm).



10.2-rasm. 192.168.10.0 kichik tarmoq'ida kompyuterlarni sozlash

Biz 192.168.11.0 tarmoqosti kompyuterlarni sozlaymiz (10.3-rasm).



10.3-rasm. 192.168.11.0 tarmoqosti kompyuterlarni sozlash

2-Qadam. Routerni (marshrutizatorni) sozlash

Biz marshrutizatorni Fa0/0 interfeysidagi birinchi tarmoq uchun 192.168.10.254 shlyuzi sifatida sozlaymiz (10.4-rasm).

```

Router1
Physical | Config | CLI
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#no sh
Router(config-if)#ip addr 192.168.10.254 255.255.255.0
Router(config-if)#exit
Router(config)#
  
```

10.4-rasm. Buyruqni kiritish oynasi

Bu yerda quyidagi buyruqlar tasvirlangan: imtiyozli rejim, konfiguratsiya rejimi, interfeysga kiramiz, ushbu interfeysni yoqamiz, IP-manzil va port maskasini o'rnatib, chiqamiz.

Xuddi shunday, biz marshrutizatorni Fa0/1 interfeysidagi ikkinchi tarmoq uchun 192.168.11.254 shlyuzi sifatida sozlaymiz (10.5-rasm).

```

Router1
Physical | Config | CLI |
IOS Command Line Interface
Router(config)#int fa0/1
Router(config-if)#no sh
Router(config-if)#ip addr 192.168.11.254 255.255.255.0
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#

```

10.5-rasm. R1-ni ikkinchi tarmoq uchun 192.168.11.254 shlyuzi sifatida sozlash

3-Qadam. Tarmoq ulanishini tekshirish

Marshurizator jadvalini **show ip route** buyrug‘i bilan tekshiramiz (10.6-rasm).

```

Router1
Physical | Config | CLI |
IOS Command Line Interface
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C     192.168.10.0/24 is directly connected, FastEthernet0/0
C     192.168.11.0/24 is directly connected, FastEthernet0/1
Router#

```

10.6-rasm. R1 marshrutizatorining marshrutlash jadvalini tekshirish

Bizning marshurizator ikkita tarmoqqa xizmat qiladi. Marshrutizator va kompyuter o‘rtasidagi aloqani tekshiramiz (10.7-rasm).


```
Router1
Physical Config CLI
IOS Command Line Interface

Router#ping 192.168.10.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.0, timeout is 2 seconds:

Reply to request 0 from 192.168.10.1, 0 ms
Reply to request 0 from 192.168.10.2, 0 ms
Reply to request 1 from 192.168.10.1, 0 ms
Reply to request 1 from 192.168.10.2, 0 ms
Reply to request 2 from 192.168.10.1, 0 ms
Reply to request 2 from 192.168.10.2, 0 ms
Reply to request 3 from 192.168.10.1, 0 ms
Reply to request 3 from 192.168.10.2, 0 ms
Reply to request 4 from 192.168.10.1, 0 ms
Reply to request 4 from 192.168.10.2, 0 ms

Router#ping 192.168.11.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.0, timeout is 2 seconds:

Reply to request 0 from 192.168.11.1, 0 ms
Reply to request 0 from 192.168.11.2, 0 ms
Reply to request 1 from 192.168.11.2, 0 ms
Reply to request 1 from 192.168.11.1, 0 ms
Reply to request 2 from 192.168.11.2, 0 ms
Reply to request 2 from 192.168.11.1, 0 ms
Reply to request 3 from 192.168.11.2, 0 ms
Reply to request 3 from 192.168.11.1, 0 ms
Reply to request 4 from 192.168.11.2, 0 ms
Reply to request 4 from 192.168.11.1, 0 ms

Router#
```

10.7-rasm. Marshrutizatorning barcha shaxsiy kompyuterlar bilan aloqasi mavjud

Marshrutizatorning ulanishini tarmoq osti bilan tekshiramiz (10.8-rasm).

```
Router1
Physical Config CLI
IOS Command Line Interface

Router#ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

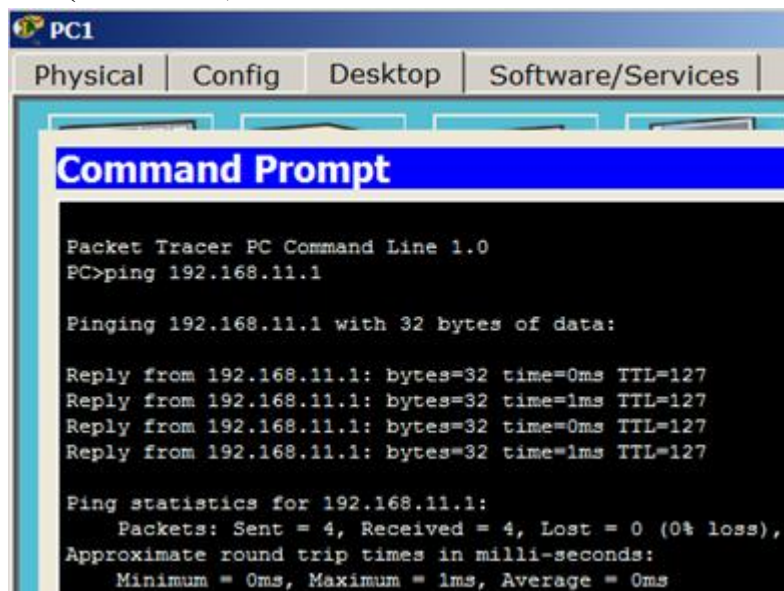
Router#ping 192.168.11.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

10.8-rasm. Marshrutizatorning tarmoqostilar bilan ulanishini tekshiramiz

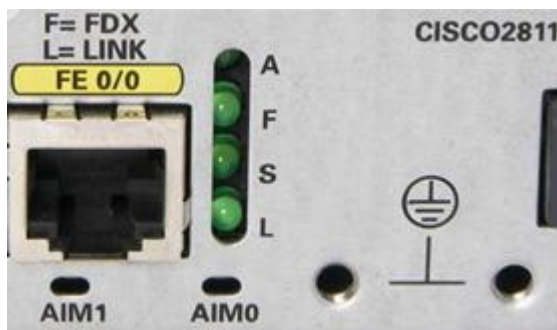
Ping buyrug‘i ulanishni tekshirish uchun ICMP so‘rov (exo paket) yuboradi. Yuqoridagi misolda bitta sorov tranzit vaqti belgilanganidan oshib ketdi, buni davr ko‘rsatib turibdi.

Shuningdek, turli xil tarmoqlarning shaxsiy kompyuterlari o‘rtasidagi aloqani tekshirib ko‘ramiz (10.9-rasm).



10.9-rasm. PC1 va PC3 aloqa tekshiruvi

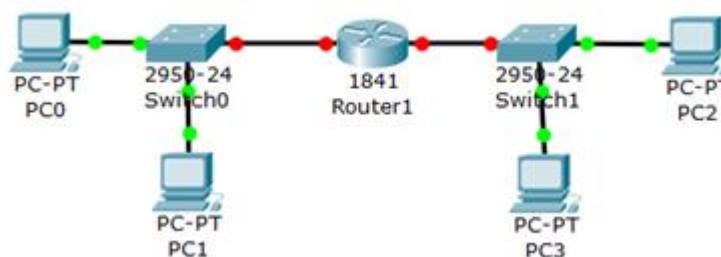
10.10-rasmda marshrutizator porti keltirilgan. Ko‘rib turganingizdek, unga RJ-45 kabeli kiritilgan.



10.10-rasm. CISCO 2811 marshrutizatorning Ethernetport 0/0

Amaliy ish bo‘yicha topshiriqlar

1-Topshiriq. Cisco qurilmalarida statik marshrutlashni sozlash



10.11-rasm. Tarmoq sxemasi

Quyidagi 10.11-rasmda keltirilgan Ikki tarmoq o'rtasida aloqa o'rnatishning barcha misollarini bajaring:

2. Kompyuterni sozlang
3. Marshrutizatorni sozlang
4. Tarmoq ulanishini tetslab ko'ring
5. Qaysi protokol tarmoqda takrorlanadigan IP-manzillar yo'qligini ta'minlashini aniqlang.
6. Tarmoq tugunlari uchun standart shlyuz marshrutizator portlari bilan qanday bog'langanligini ko'rsatib bering.

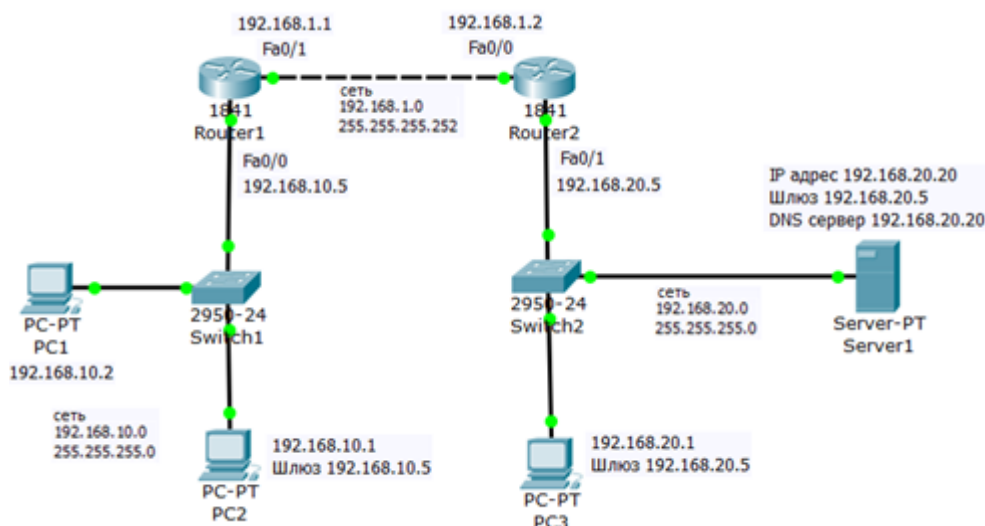
Topshiriqni bajarish jarayonida quyidagilarni bajarish kerak:

1. Marshrutizatorlarning tarmoq interfeyslariga, kommutatorlarning boshqaruv interfeyslariga va lokal kompyuterlarning tarmoq interfeyslariga IP-manzillarni tayinlash;
2. Ketma-ket tarmoq interfeysi orqali qo'shni marshrutizatorlar o'rtasida jismoniy va kanal darajalarida aloqa o'rnatish;
3. Qo'shni tarmoq ob'ektlari (C1-S1, C1-R1, S1-R1, R1-R2, R2-S2, R2-C2 va boshqalar) o'rtasida IP protokoli orqali ma'lumotlarni uzatish imkoniyatiga erishish;
4. R2 marshrutizatorida C1, C3 lokal kompyuterlari tarmoqlariga statik marshrutlarni sozlang
5. R1, R3 marshrutizatorlarida mos ravishda C2-C3 va C1-C2 lokal kompyuterlar tarmoqlariga mos holda "standart" marshrutlarni sozlang;
6. Har qanday tarmoq ob'ektlari o'rtasida IP orqali ma'lumotlarni uzatish qobiliyatiga erishish (ping);
7. "Simulyatsiya rejimi" ga o'tib, qurilmalar o'rtasida ICMP protokoli yordamida ma'lumotlar almashinuvi jarayonini ko'rib chiqing va tushuntiring (Ping buyrug'ini bitta kompyuterdan boshqasiga bajarish orqali), bu jarayonda ARP protokolining rolini tushuntiring.

2-Topshiriq. WEB-server bilan uchta tarmoqni sozlash. Standart marshrut tushunchasi.

Biz amaliy ishda quyidagi qurilmalardan iborat sxema bilan ishlaymiz:

- ikkita 2950-24 kommutator, 192.168.10.0 tarmog'ida 255.255.255.0 niqobli ikkita kompyuter;
- 25.1.255.255.0 niqobli 192.168.20.0 tarmog'idagi server va kompyuter.
- 255.255.255.252 niqobli 192.168.1.0 marshrutizator o'rtasidagi tarmoq (1841 markali).
- 192.168.10.0 tarmog'idagi kompyuterlar 192.168.20.0 tarmog'idagi DNS-serverga etib borishi kerak (10.12-rasm).

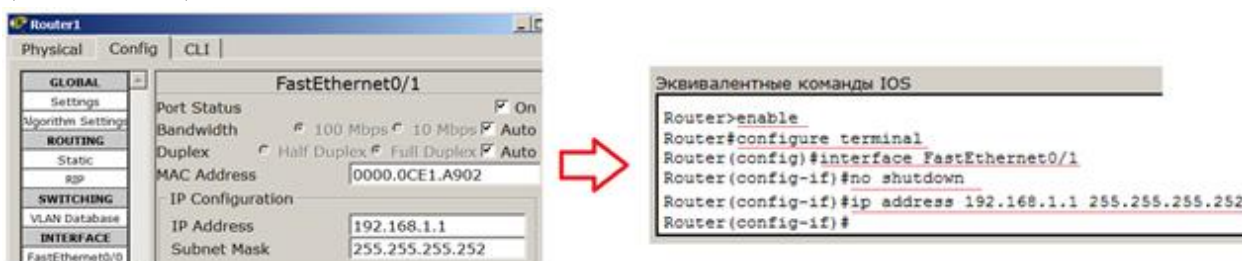


10.12-rasm. Tarmoq loyihasi

Bizning tarmoq murakkab emas, ko'p shaxsiy kompyuterlar mavjud emas, shuning uchun biz dinamik emas, balki statik marshrutizatsiyadan foydalanamiz.

Marshrutizatorlar uchun tarmoq interfeysini sozlash

R1 uchun Fa0 / 1 va R2 uchun Fa0 / 0 portlari orqali marshrutizatorlarning ulanishini sozlaymiz. Biz Router1-ni 192.168.1.0 marshrutizatorlari orasidagi tarmoq 255.255.255.252 maskasi bilan masalamimg qo'yilishiga asoslanib sozlaymiz. Shuning uchun biz Fa 0/1 portiga 192.168.1.1 IP manzilini tayinlaymiz (10.13-rasm).

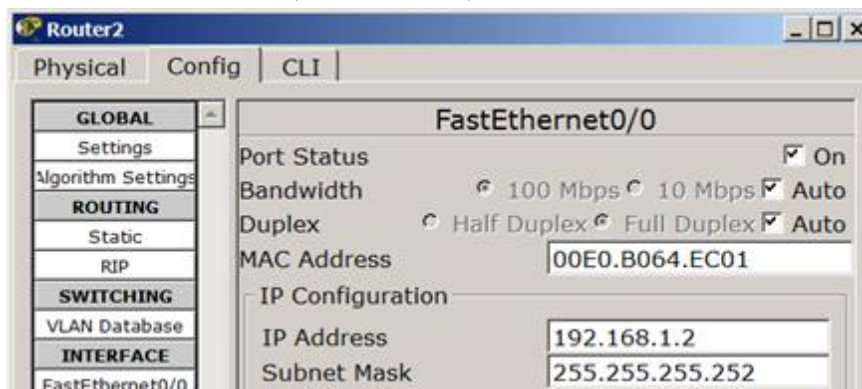


10.13-rasm. R1 marshrutizator uchun 0/1 portni sozlash oynasi

Web-interfeys orqali konfiguratsiya qilishda **nosh** buyrug'iga teng bo'lgan **On** bandiga belgi qo'yganingizga ishonch hosil qiling.

Shu bilan bir qatorda, marshrutizatorning barcha parametrlarini CLI yorlig'idagi buyruq satridan quyidagi buyruqlar bilan sozlash mumkin: **enable** (imtiyozli rejimni yoqish), **config terminal** (konfiguratsiya rejimiga kiring), **interface fastethernet0/1** (100mb Ethernet 0/1 interfeysini sozlang), **ip address 192.168.1.1 255.255.255.252** (interfeys ip manzili va marshurizator tarmog'ining niqobini yozing), **no shutdown** (interfeysni yoqing - sukut bo'yicha hamma narsa o'chirilgan), **exit** (interfeysni sozlash rejimidan chiqish), **end** (tugatilgan tahrirlash), **write** (konfiguratsiyani saqlash).

Xuddi shunday, biz Router2-ni 192568 marshrutizatorlari orasidagi tarmoq 255.255.255.252 maskasi bilan masalani qo`yilishi asosida tuzamiz. Fa0/0 portiga 192.168.1.2 IP-manzil beriladi (10.14-rasm).



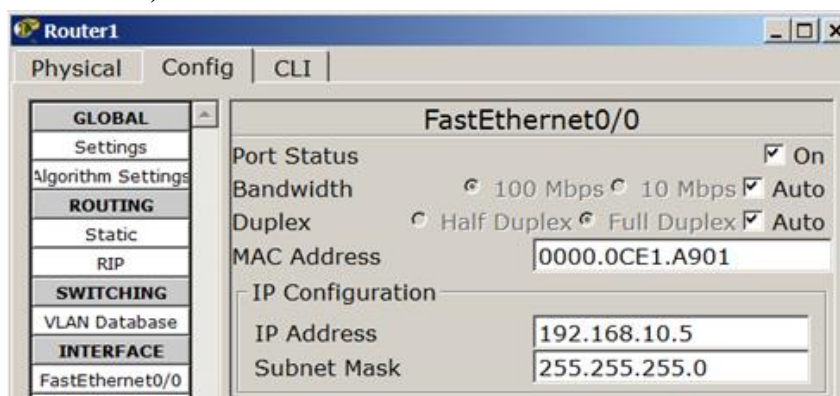
10.14-rasm. R2-ni sozlash oynasi

Buyruqning satridan marshrutizatorni sozlashda siz yozish buyruqlarining qisqartirilgan shaklidan foydalanishingiz mumkin: **en** (kengaytirilgan rejimni yoqish). **conf t** (konfiguratsiya rejimiga o`ting). **int fa0/0** (100 mb interfeysni sozlash. Ethernet 0/0). **IP addr192.168.1.2 255.255.255.252** (interfeys ip manzili va tarmoq maskasini ro`yxatdan o`tkazing). **No shut** (interfeysni yoqing - u sukut bo`yicha o`chirilgan). **exit** (interfeysni sozlash rejimidan chiqish). **end** (tahrirlashni tugatish). **wr** (konfiguratsiyani saqlash).

Natijada, marshrutizatorlarni sozlashdan so`ng, portlarda yashil markerlar yonadi, ya`ni ular o`rtasida bog`liqlik mavjud. Marshrutizatorlar orasidagi tarmoq ishlamoqda, ammo marshrutlash hali mavjud emas, ya`ni bitta tarmoqdan boshqasiga o`tish mumkin emas.

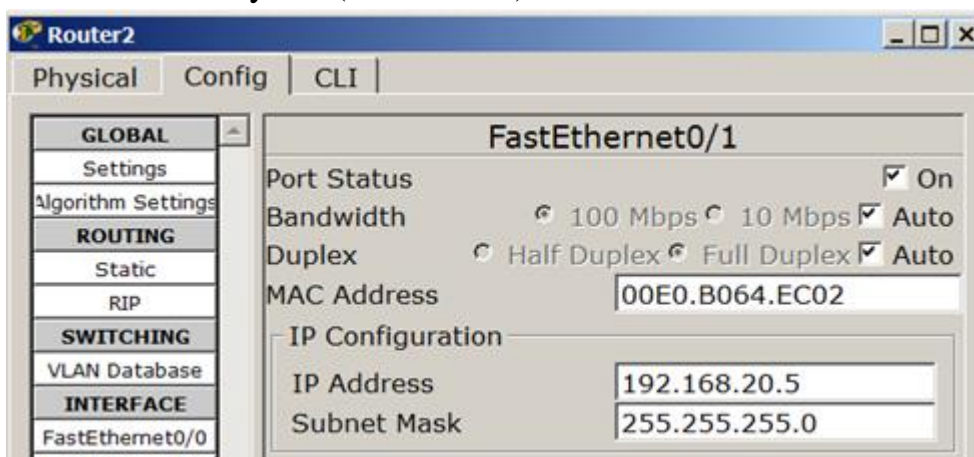
Marshrutizatorlarning tarmoq osti bilan ulanishini sozlash

R1 marshrutizatorining Fa0/0 portini 192.168.10.0 tarmog`i bilan ishlashga sozlaymiz (10.15-rasm).



10.15-rasm. R1 marshrutizatorining Fa0 / 0 portini 192.168.10.0 tarmog`i bilan ishlash uchun sozlash oynasi

Xuddi shu tarzda, R2 marshrutizatorining Fa0 / 1 porti 192.168.20.0 tarmog‘i bilan ishlash uchun sozlaymiz (10.16-rasm).

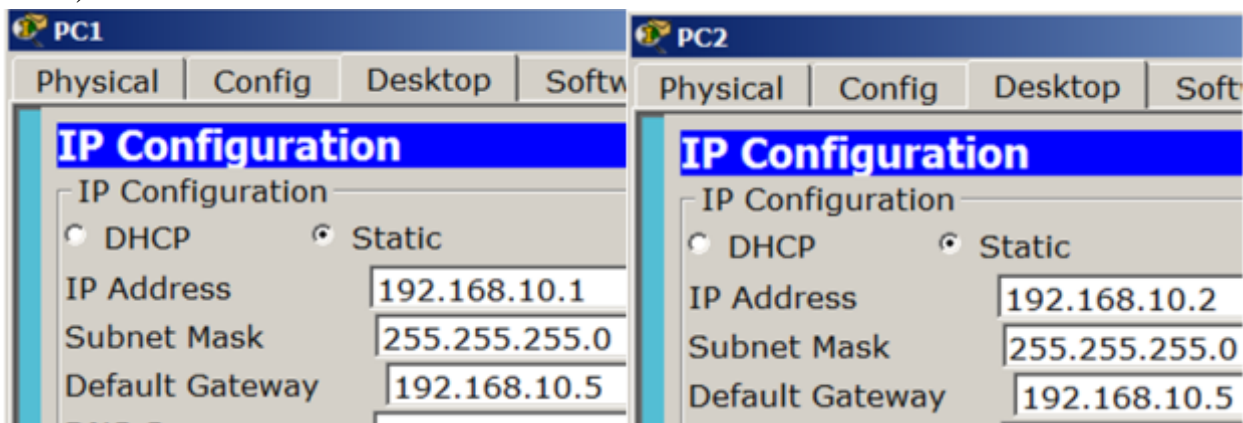


10.16-rasm. R2 marshurizator Fa0 / 1 porti 192.168.20.0 tarmog‘i bilan ishlash oynasi

Markerlardan ko‘rinib turibdiki - tarmoq ko‘tarildi (Up), ya‘ni barcha ko‘rsatkichlar yashil rangga ega.

PC1 va PC2-ni sozlash

192.168.10.0 tarmog‘idagi kompyuterlarni ishlashni va sozlashni davom ettiramiz, ya‘ni kompyuterlarning IP-ni, tarmoq maskasini va standart shlyuzni o‘rnatishingiz kerak. Muammoning dastlabki shartlariga ko‘ra, bizda chap tomonda 192.168.10.0 tarmog‘idagi 255.255.255.0 niqobli juft kompyuterlar mavjud (10.17-rasm).

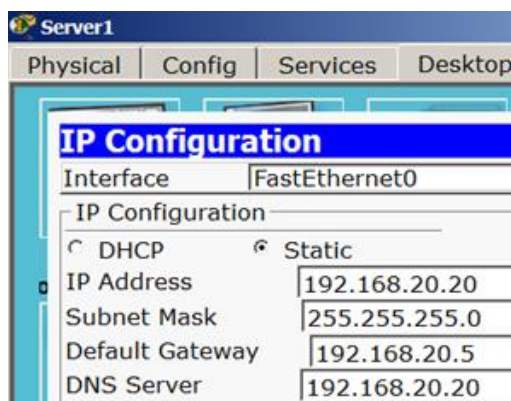


10.17-rasm. PC1 va PC2-ni sozlash oynasi

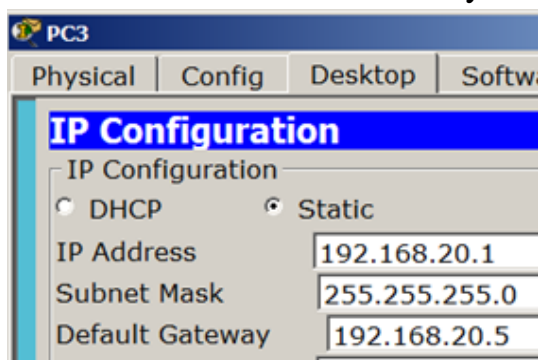
Standart shlyuz (Default Gateway) - bu kompyuter paketni qayerga yuborishni bilmasa, uni yuboradigan manzil. Masalan, B xosti A xostiga ma‘lumotlarni A xostga aniq manzilsiz yuborishga harakat qilganda, B xost uchun mo‘ljallangan TCP / IP trafigini standart shlyuzga yo‘naltiradi.

Server va PC3-ni sozlash

Keyin PC3 va serverni 192.168.20.0 tarmog'ida sozlashingiz kerak (10.18-rasm va 10.19-rasm).



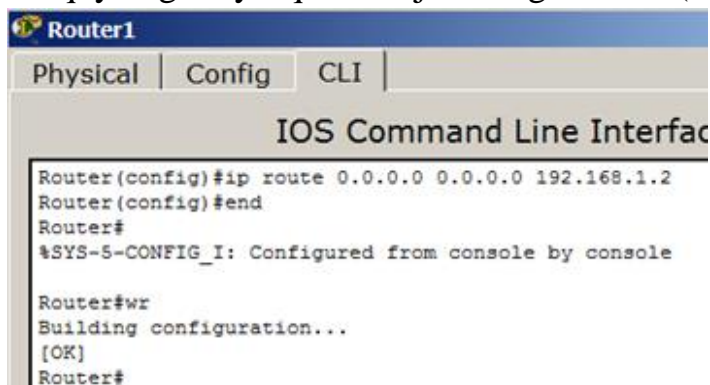
10.18-rasm. Serverni sozlash oynasi



10.19-rasm. PC2-ni sozlash oynasi

Marshrutizatorlarda marshrutni sozlash (standart yo'nalish)

Tarmoqlarga ping yuborishingiz va vaziyatning quyidagicha ekanligiga ishonch hosil qilishingiz mumkin: tarmoqdan so'rovlar ... 10.0 tarmoqqa ... 20.0 o'tish amalga oshirilayapti, ammo javoblar yo'q. Shuning uchun marshrutizatorlarda standart yo'nalishlarni ro'yxatdan o'tkazishingiz kerak. Eslab o'tamiz, biz 192.168.1.1 IP manzilini Fa0 / 1 portiga va 192.168.1.2 ni Fa0 / 0 portiga tayinladik. Shuning uchun, 192.168.1.1 IP-manzili bilan Fa0/1 porti uchun R1 marshrutizatorida siz quyidagi buyruqlarni bajarishingiz kerak (10.20-rasm).



10.20-rasm. Standart yo'nalishni R1-da ro'yxatdan o'tkazish oynasi

Yozuv shuni anglatadiki, marshrutlar tayinlanmagan barcha so‘rovlar R1 tomonidan 192.168.1.2 raqamiga, ya’ni R2 ga yuboriladi.

R2 uchun biz ham xuddi shunday qilamiz (10.21-rasm).



```
Router2
Physical | Config | CLI
IOS Command Line Interface
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)# exit
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

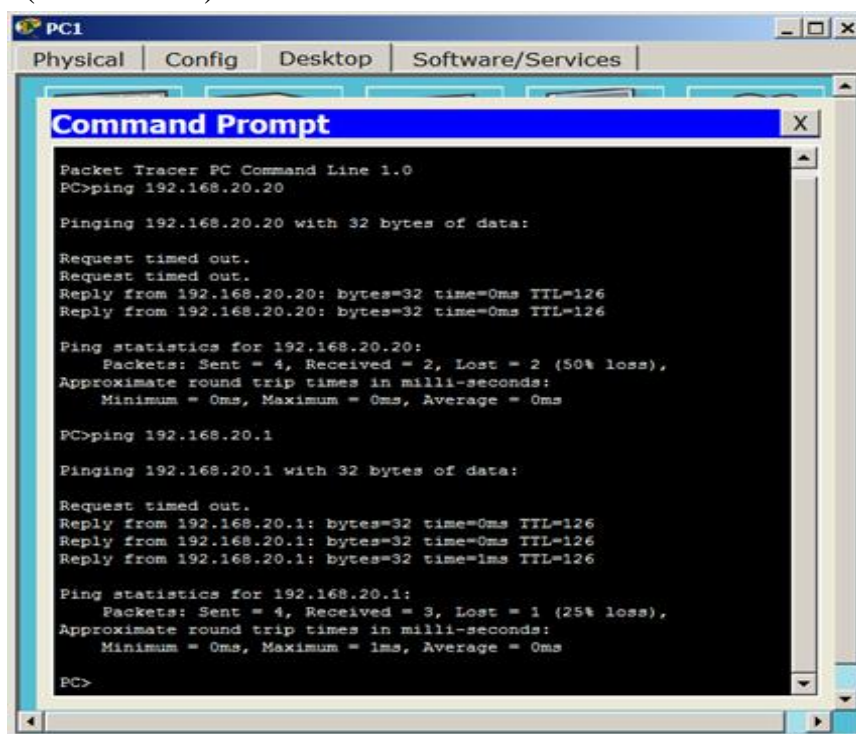
Router#wr
Building configuration...
[OK]
Router#
```

10.21-rasm. Standart yo‘nalishni R2 da ro‘yxatdan o‘tkazish oynasi

Yozuv shuni anglatadiki, marshrutlar ro‘yxatdan o‘tkazilmagan barcha so‘rovlar R2 tomonidan 192.168.1.1 raqamiga, ya’ni R1 ga yuboriladi.

Tarmoq ishlashini tekshirish

Marshrutizatorlarni sozlashdan so‘ng, tarmoqni sinab ko‘rish mumkin, buning uchun bitta tarmoqdan kompyuterlarni boshqa tarmoqdagi kompyuterlarga pinglash qilish kerak - (10.22-rasm).

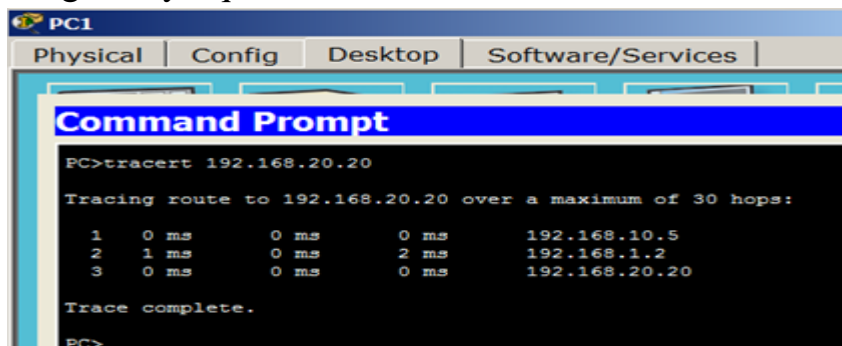


```
PC1
Physical | Config | Desktop | Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.20
Pinging 192.168.20.20 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.20.20: bytes=32 time=0ms TTL=126
Reply from 192.168.20.20: bytes=32 time=0ms TTL=126
Ping statistics for 192.168.20.20:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.1: bytes=32 time=0ms TTL=126
Reply from 192.168.20.1: bytes=32 time=0ms TTL=126
Reply from 192.168.20.1: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>
```

10.22-rasm. Aloqa tekshirish oynasi

Ishonch hosil qilish uchun, paketlarning xostlardan qanday o‘tishini ko‘rib chiqamiz va buning uchun **tracert 192.168.20.20** buyrug‘idan foydalanamiz (10.23-rasm).

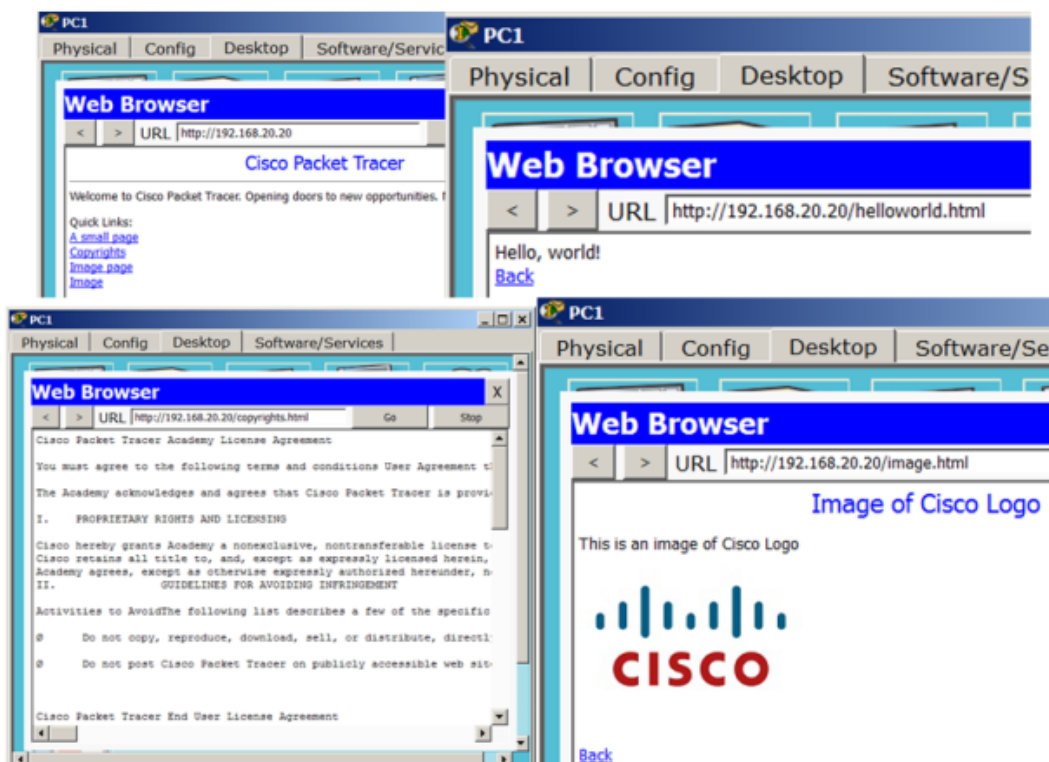
Tracert - bu TCP / IP tarmoqlarida ma’lumotlar yo‘nalishlarini aniqlash uchun mo‘ljallangan buyruq.



10.23-rasm. Paketlarning kompyuter segmentidan serverga qanday o‘tishini kuzatish oynasi

Skrinshotdan ko‘rinib turibdiki, paketlar avval 192.168.10.5 (R1 - Fa0 / 0 port), keyin 192.168.1.2 (R2 - Fa0 / 0 port) ga o‘tib, so‘ngra 192.168.20.20 serveriga keladi - barchasi to‘g‘ri!

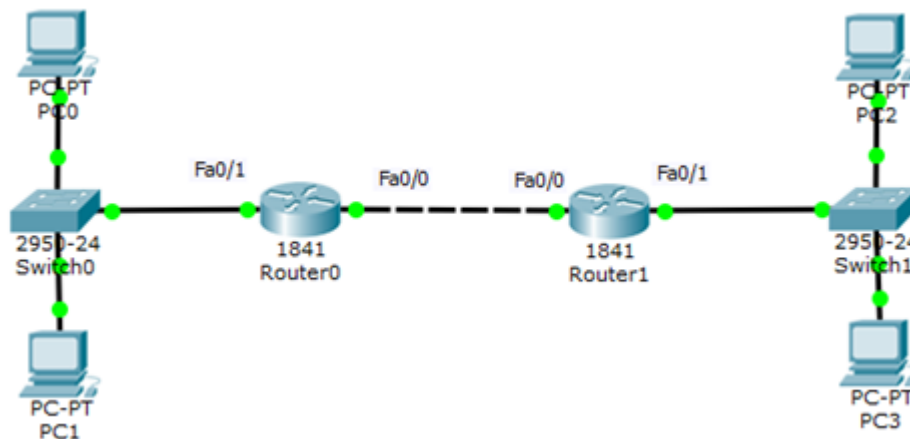
Biz serverda veb-sahifalar yaratmadik, lekin ular dastlab u yerda sukut bo‘yicha mavjud edi. Veb-brauzerni ishga tushiring va bunga o‘zingiz ishonch hosil qiling (10.24-rasm).



10.24-rasm. HTTP xizmati ishlaydigan server oynasi

3-Topshiriq. Ikki marshrutizatorda tarmoq yaratish

Bu ishimizda ikkita amaliy misol yordamida mahalliy tarmoqlarda statik marshrutni o‘rganamiz. Statik marshrutlashni sozlash uchun tarmoq sxemasi 10.25-rasmda keltirilgan.



10.25-rasm. Tarmoq loyihasi

Agar R0 va R1 uchun marshrutlash jadvalini ko‘rish uchun endi **show ip route** buyrug‘idan foydalansak, biz quyidagilarni ko‘ramiz (10.26-rasm va 10.27-rasm).

```
Router0
Physical Config CLI
IOS Command Line Interface
Router#sh ip route
Gateway of last resort is not set
C 10.0.0.0/8 is directly connected, FastEthernet0/1
C 192.168.1.0/24 is directly connected, FastEthernet0/0
Router#
```

10.26-rasm. 1-marshurizator bo‘yicha marshrut jadvali oynasi

```
Router>en
Router#sh ip route
Gateway of last resort is not set
C 10.0.0.0/8 is directly connected, FastEthernet0/1
C 192.168.1.0/24 is directly connected, FastEthernet0/0
Router#
```

10.27-rasm. 2-marshurizator bo‘yicha marshrutlash jadvali oynasi

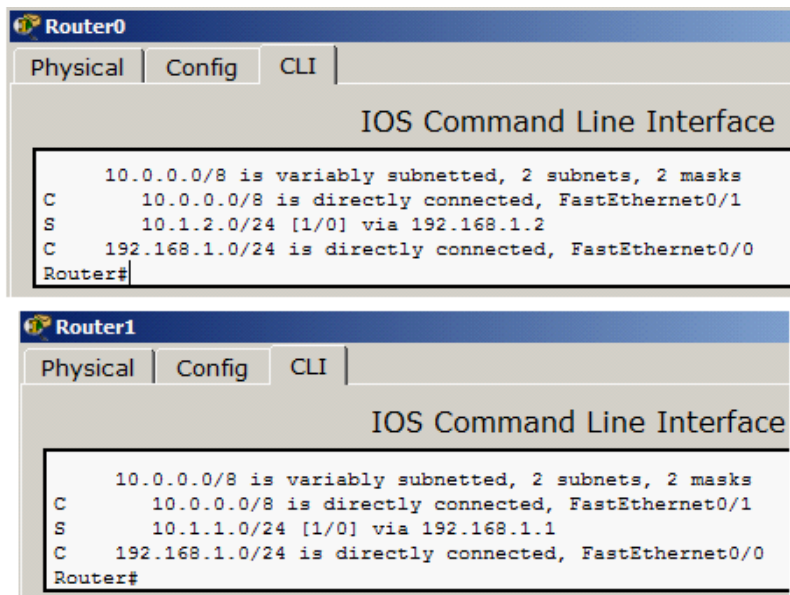
Ayni paytda bizning jadvalimizda faqat to‘g‘ridan-to‘g‘ri bog‘langan tarmoqlar mavjudligini ko‘rishimiz mumkin. R0 10.1.2.0 tarmog‘ini va R1 10.1.1.0

tarmog'ini bilmaydi. Shuning uchun marshrutizatsiyani sozlash uchun ushbu marshrutlarni marshurizator jadvallariga qo'shing:

R0 (config)#ip route 10.1.2.0 255.255.255.0 192.168.1.2

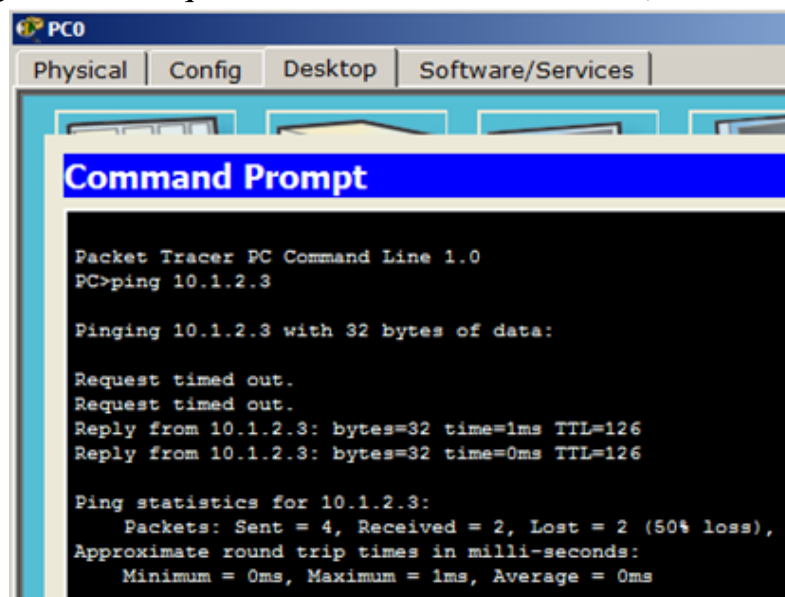
R1 (config)#ip route 10.1.1.0 255.255.255.0 192.168.1.1

Endi biz qurilmalarimiz marshrut jadvallarini yana namoyish etamiz (10.28-rasm).



10.28-rasm. Marshrut tuzilgan (sozlangan) oynasi

Endi 1-marshurizator 10.1.2.0 tarmoqostiga yo'naltirilgan paketlarni marshrutizatorga 192.168.1.2 ip manzili bilan uzatilishi mumkinligini biladi va 2-marshurizator 10.1.1.0 tarmoqostiga yo'naltirilgan paketlarni 192.168.1.1. ip manzili bilan marshrutizatorga yuborish mumkinligini biladi. Shaxsiy kompyuterning turli tarmoqlardan ulanishini tekshiramiz (10.29-rasm).



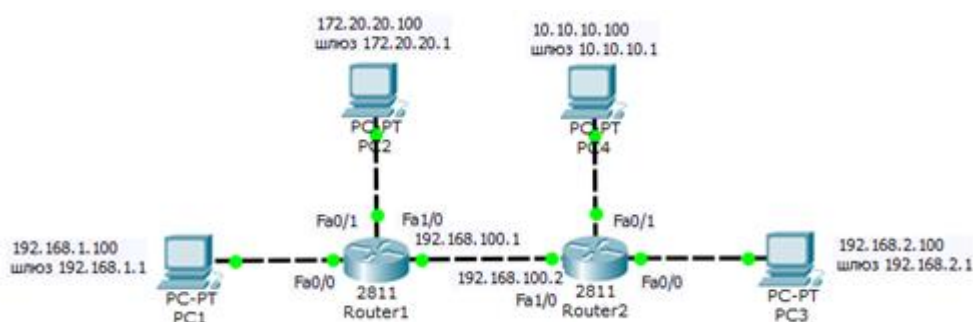
10.29-rasm. Statik marshrutlash tuzilgan - PC0 PC3 bilan aloqani tekshirish oynasi

Beshta tarmoq va uchta portli marshurizator uchun statik marshrutlash

Ushbu misolda biz quyidagi tarmoq sxemasini tuzamiz va sozlaymiz (10.30-rasm).

Tarmoq sxemasi

Ushbu sxemada beshta tarmoq mavjud: 192.168.1.0, 172.20.20.0, 192.168.100.0, 10.10.10.0 va 192.168.2.0. Har bir kompyuterda standart shlyuz sifatida ulangan marshrutizatorning interfeysi mavjud. Barcha shaxsiy kompyuterlarda bir xil niqob mavjud - 255.255.255.0. Har bir port uchun marshurizator maskasi har xil: Fa0 / 0 - 255.255.255.0, Fa0 / 1 - 255.255.0.0, Fa1 / 0 - 255.255.255.252.



10.30-rasm. Marshrutizatorlar orqali tarmoqlarni ulash

Keyinchalik, marshrutizatorlarni bir-biriga bog'laymiz, marshrutizatorga NM-1FE-TX interfeys kartasini qo'shishimiz kerak (NM - Tarmoq moduli, 1FE - bitta FastEthernet portini o'z ichiga oladi, TX - 10 / 100MBase-TX-ni qo'llab-quvvatlaydi). Buning uchun marshrutizatorning konfiguratsiya oynasiga o'ting, uni yoqish tugmachasini bosib o'chiring. Shundan so'ng, NM-1FE-TX interfeys platasini marshurizator razyomiga torting (10.31-rasm). Karta qo'shilgandan so'ng uni yoqish uchun marshrutizatorning almashtirish tugmachasini yana bir marta bosing. Ikkinchi marshurizator uchun xuddi shu amallarni takrorlang.



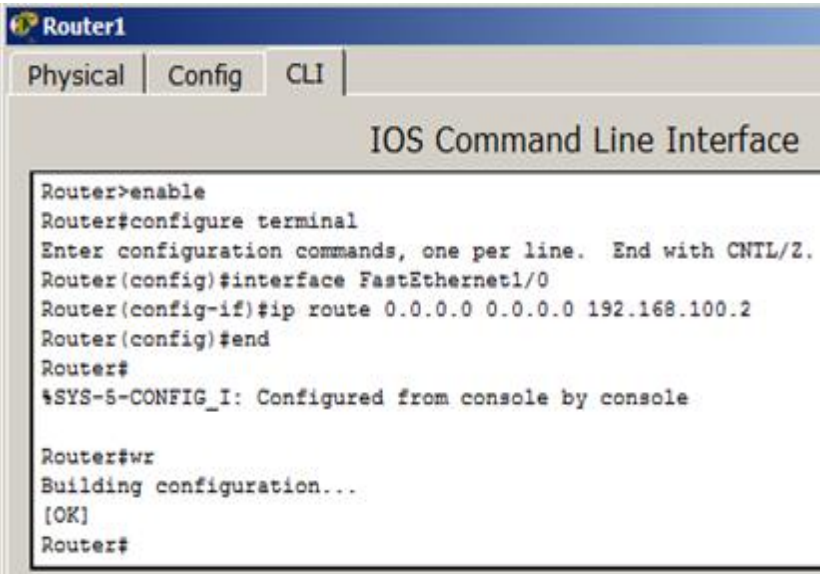
10.31-rasm. Interfeys platasini marshrutizatorga joylashtirish oynasi

Masalani qo'yilishi

Biz barcha shaxsiy kompyuterlar bir-biri bilan bog'lanishlari uchun kerakli sozlamalarni o'rnatishimiz kerak, ya'ni o'zaro turli xil tarmoqlardan kompyuterlar mavjudligini ta'minlash kerak.

Marshrutni sozlash (standart yo'nalish)

Ayni paytda, biz R2 marshrutizatorining 192.168.100.2 IP-manzili bilan Fa1 / 0 interfeysiga 192.168.1.100 IP-manzili bilan PC1-dan paket yuborsak, u holda ICMP paketi chapdan ushbu marshrutizatorga yetib boradi, ammo 192.168.100.2 dan 192.168.1.100 gacha ICMP paketlarini teskari yo'nalishda yuborganda muammo paydo bo'ladi. Haqiqat shundaki, R2 marshrutizator o'z marshrut jadvalida 172.20.20.0 tarmog'i haqida ma'lumotga ega emas, chunki biz hali ham standart shlyuzni ro'yxatdan o'tkazmaganmiz va R2 marshrutizator so'rovga javoblarni qaerga yuborishni bilmaydi. Tarmoqosti tarmoqlarda marshrutizatsiyani o'rnatishning eng oson usuli bu standart marshrutni qo'shishdir. Buning uchun konfiguratsiya rejimida R1 marshrutizatorida quyidagi buyruqlarni bajaring (10.32-rasm).



```
Router1
Physical | Config | CLI
IOS Command Line Interface

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet1/0
Router(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr
Building configuration...
[OK]
Router#
```

10.32-rasm. Standart yo'nalishni R1-ga o'rnatish oynasi

Ushbu buyruqlarda 0.0.0.0 raqamlarning birinchi guruhi maqsadli tarmoqning IP-manzilini, keyingi 0.0.0.0 raqamlar guruhi uning niqobini bildiradi va oxirgi raqamlar - 192.168.100.2 - bu tarmoqqa kirish uchun paketlarni yuborish kerak bo'lgan interfeysning IP-manzili hisoblanadi. Agar biz 0.0.0.0 niqobli tarmoq manzili sifatida 0.0.0.0 ni belgilasak, u holda bu marshrut sukut bo'yicha yo'nalishga aylanadi va manzillari to'g'ridan-to'g'ri marshrut jadvalida ko'rsatilmagan barcha paketlar unga yuboriladi.

O'ngdagi R2 marshrutizatorida biz xuddi shu tarzda harakat qilamiz (10.33-rasm).


```

Router2
Physical | Config | CLI |
IOS Command Line Interface

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet1/0
Router(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.100.1
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr
Building configuration...
[OK]
Router#

```

10.33-rasm. Standart yo‘nalishni R2-ga o‘rnatish oynasi

IP-manzil 192.168.1.100 bo‘lgan PC1-dan paketni R2 marshrutizatorining 192.168.100.2 IP-manzili bilan Fa1 / 0 interfeysiga yuboramiz va nima o‘zgarganligini ko‘rib chiqamiz (10.34-rasm).

```

PC1
Physical | Config | Desktop | Software/Services |
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.2: bytes=32 time=0ms TTL=254
Reply from 192.168.100.2: bytes=32 time=0ms TTL=254
Reply from 192.168.100.2: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>

```

10.34-rasm. 192.168.1.100 IP-manzilga ega PC1 kompyuteridan biz R2 marshrutizatorning 192.168.100.2 IP-manzili bilan Fa1 / 0 interfeysini tekshrish oynasi

Amaliy ishimiz yakunida shuni aytishimiz mumkinki, aytaylik, biz PC1 kompyuteridan 192.168.1.100 manzili (chap tarmoqdan) PC4 kompyuteriga 10.10.10.100 IP-manzili (o‘ng tarmoqdan) bilan ping qilishni xohlaymiz. 192.168.1.100 manzili bo‘lgan kompyuterdagi standart shlyuz - bu R1 marshrutizatorining Fa0 / 0 interfeysining 192.168.1.1 manzili hisoblanadi. Birinchidan, kompyuter 10.10.10.100 manzilini marshrutlash jadvalida ko‘rib chiqadi va uni topmagandan so‘ng, ICMP paketlari standart manzilga, ya’ni

192.168.1.1 (port Fa0 / 0) bilan R1 marshrutizator interfeysiga yuboriladi. Paketni olgandan so'ng, R1 manzilni ko'rib chiqadi - 10.10.10.100 va uni marshrut jadvalida ham topishga harakat qiladi. Uni ham topa olmaganida, paket Fa1 / 0 interfeysiga, R2 marshrutizatorning 192.168.100.2 manziliga yuboriladi. R2 marshrutizatori o'z marshrut jadvalida 10.10.10.100 gacha marshrutni topishga harakat qiladi. Bu muvaffaqiyatsiz tugaganda, marshrutizator 10.0.0.0 tarmog'iga yo'nalishni qidiradi. Ushbu tarmoq haqidagi ma'lumotlar marshrutizator jadvalida joylashgan bo'lib, marshrutizator ushbu tarmoqqa kirish uchun paketlarni to'g'ridan-to'g'ri ushbu tarmoq ulangan FastEthernet0 / 1 interfeysiga yuborish kerakligini biladi. Bizning misolimizda butun 10.0.0.0 tarmog'i faqat bitta kompyuter bo'lgani uchun, paketlar darhol manziliga, ya'ni 10.10.10.100 IP-manzili bo'lgan kompyuterga etib boradi. ICMP javob paketlarini yuborishda barchasi xuddi shu tarzda sodir bo'ladi. Biroq, faqat standart yo'nalishlarni belgilash bilan har doim ham imkoni bo'lmaydi. Keyinchalik murakkab tarmoq konfiguratsiyalarida har bir tarmoq uchun marshrutni alohida-alohida yozish kerak bo'lishi mumkin. Bu oson bo'lmaydi. Shuning uchun katta tarmoqlarda odatda statik emas, balki dinamik marshrutlash qo'llaniladi.

Amaliy ish bo'yicha savollar

1. Marshrutlash jadvali necha xil usulda yaratilishi mumkin?
2. Statik marshrutlash nima?
3. Statik marshrutlashning afzalligi nimadan iborat?
4. . Statik marshrutlash bilan dinamik marshrutlashning qanday farqi bor?
5. Standart shlyuz (default gateway) nima?
6. ICMP nima?
7. Marshrutlash halqasi (Routing loop, Петля маршрутизации) qanday hodisa?
8. Marshrutizatorni sozlashda qanday buyruqlardan foydalanisiz?
9. Tracert qanday buyruq?

Amaliy ish № 11

CISCO PACKET TRACER DASTURIDA DINAMIK MARSHRUTLASHNI SOZLASH

Ishdan maqsad: RIP va EIGRP protokollari bo'yicha dinamik marshrutlash ko'nikmasiga ega bo'lish

Nazariy qism

Marshrutlash - bu paketdagi manzilga yetib borishi mumkin bo'lgan tarmoqdagi eng yaxshi yo'lni aniqlash jarayoni. Dinamik marshrutni bir yoki bir

nechta protokollar (RIP v2, OSPF va boshqalar) yordamida amalga oshirish mumkin.

Dinamik marshrutlash - bu bir yoki bir nechta marshrutlash protokollari (RIP, OSPF, EIGRP, BGP) yordamida marshrutlash jadvali to'ldiriladigan va avtomatik ravishda yangilanadigan marshrutlash turi.

Har bir marshrutlash protokoli marshrutni baholash tizimidan (metrikadan) foydalanadi. Belgilangan tarmoqlarga marshrutni tayinlash quyidagi mezonlarga asoslanadi:

- retranslyatsion o'tishlar soni
- aloqa kanalining o'tkazuvchanligi
- ma'lumotlarni uzatishning kechikishi

Marshrutizatorlar UDP orqali xizmat paketlari yordamida bir-birlari bilan marshrut ma'lumotlarini almashadilar. Ushbu ma'lumot almashinuvi tarmoqdagi qo'shimcha trafik mavjudligini va ushbu tarmoqdagi yukni oshiradi. Shuningdek, marshrutizatorlardagi marshrutlash jadvallari bir-biri bilan kelishishga ulgurmasligi mumkin, bu esa noto'g'ri marshrutlar paydo bo'lishiga va ma'lumotlarning yo'qolishiga olib kelishi mumkin.

Marshrutlash protokollari uch turga bo'linadi:

- Vektorli masofali protokollar (RIP)
- Kanallarning holatini kuzatuvchi protokollar (OSPF)
- Aralash protokollar (EIGRP)

RIP protokoli

RIP - bu optimal yo'lni topish uchun Bellman-Ford algoritmidan foydalanadigan masofaviy vektorli marshrutlash protokoli. RIP marshrutlash algoritmi - bu eng oddiy marshrutlash protokollaridan biri. U har 30 soniyada marshrutlash jadvalini tarmoqqa uzatadi. Protokollarning asosiy farqi shundaki, RIPv2 (RIPv1dan farqli o'laroq) multicast-da ishlashi mumkin, ya'ni uni multicast manziliga yuborishi mumkin. RIP1-da ruxsat etilgan maksimal hoplar soni (belgilangan joyga qadar) 15 (15-metrik) hisoblanadi. 15-hop cheklovi RIP-ning katta tarmoqlarda ishlatilishiga yo'l qo'ymaydi, shuning uchun protokol ko'pincha kichik kompyuter tarmoqlarida uchraydi. Protokolning ikkinchi versiyasi - RIP2 protokoli 1994 yilda ishlab chiqilgan va birinchisining takomillashtirilgan versiyasidir. Ushbu protokol qo'shimcha marshrutlash ma'lumotlarini kiritish orqali xavfsizlikni yaxshilaydi. Masofaviy vektor protokoli printsipi: har bir marshrutizator RIP protokolidan foydalangan holda vaqti-vaqti bilan qo'shnilariga ushbu marshrutizator ma'lum bo'lgan barcha tarmoqlarga masofani (metrika (o'lchov) bilan o'lchanadigan) o'z ichiga olgan maxsus vektor paketini uzatadi. Bunday vektorni olgan marshrutizator vektorning tarkibiy qismlarini o'ziga qo'shni bilan

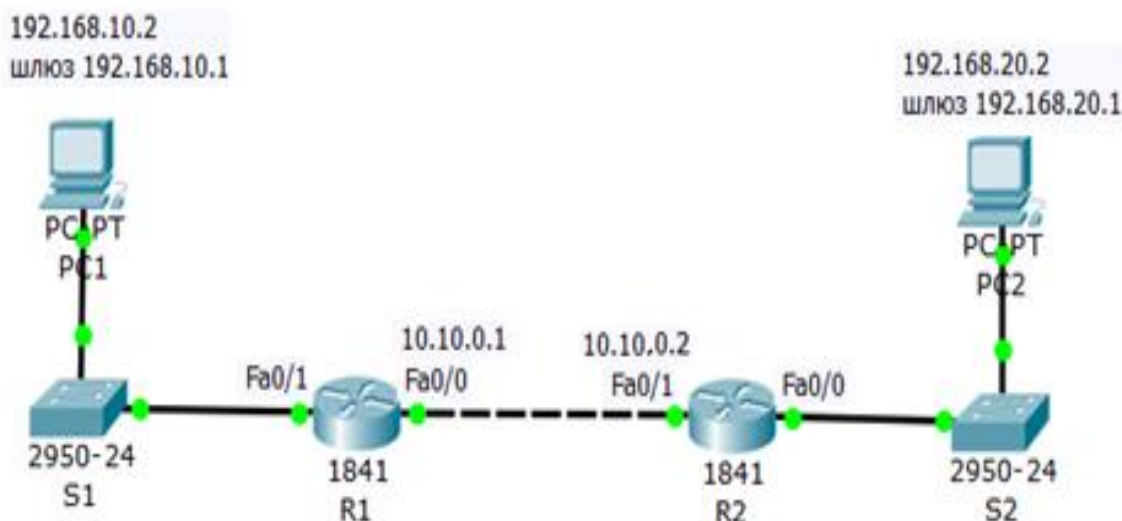
masofani ko'paytiradi va vektorni to'g'ridan-to'g'ri o'ziga ma'lum bo'lgan yoki boshqa marshrutizatorlar bu haqda ma'lum qilgan tarmoqlar yoki tarmoqlar haqidagi ma'lumotlar bilan to'ldiradi. Router kengaytirilgan vektorni barcha qo'shnilariga yuboradi. Router bir necha muqobil marshrutlardan eng past metrik qiymatiga ega marshrutni tanlaydi va bunday marshrut haqida ma'lumot uzatgan marshrutizator keyingi o'tish (**next hop**) sifatida belgilanadi.

Protokol katta tarmoqlarda ishlashga yaroqsiz, chunki u tarmoqni katta trafik bilan to'sib qo'yadi va tarmoq tugunlari kanallarning holati va tarmoq topologiyasi to'g'risida aniq ma'lumotga ega bo'lmagan holda faqat masofa vektorlari bilan ishlaydi. Bugungi kunda, hatto kichik tarmoqlarda ham protokol yuqori darajadagi EIGRP va OSPF protokollari bilan almashtiriladi.

11-amaliy ishni bajarish tartibi

Olti qurilmali tarmoq uchun RIPv2 versiyasini sozlash

Bizning vazifamiz. 11.1 - rasmda ko'rsatilgan sxema marshrutini sozlash



11.1-rasm. Tarmoq loyihasi

Tarmoqni sozlashda portlarni yoqishni unutmang.

R1 marshrutizatorida RIP marshrutizator protokolini sozlash

Router konsoli konfiguratsiyaga kiring va quyidagi sozlamalarni bajaring (11.2-rasm).

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.1
Router(config-router)#network 10.10.0.1
Router(config-router)#end
Router#
```

11.2-rasm. Router1 marshrutizatorida RIPv2 protokolini sozlash oynasi

Router (config) #router rip (RIP marshrutizatorini konfiguratsiya rejimiga kirish). **Router (config-router) #network 192.168.10.1** (S1 tugmachasi tomonidan mijoz tarmog‘ini marshrutizatorini ulash). **Router (config-router) #network 192.168.20.1** (Ikkinchi tarmoqni, ya’ni marshrutizatorlar orasidagi tarmoqni ulash). **Router (config-router) #version 2** (RIP protokolining ikkinchi versiyasidan foydalanishni belgilaydi).

R2-marshrutizatorida RIP protokolini sozlash

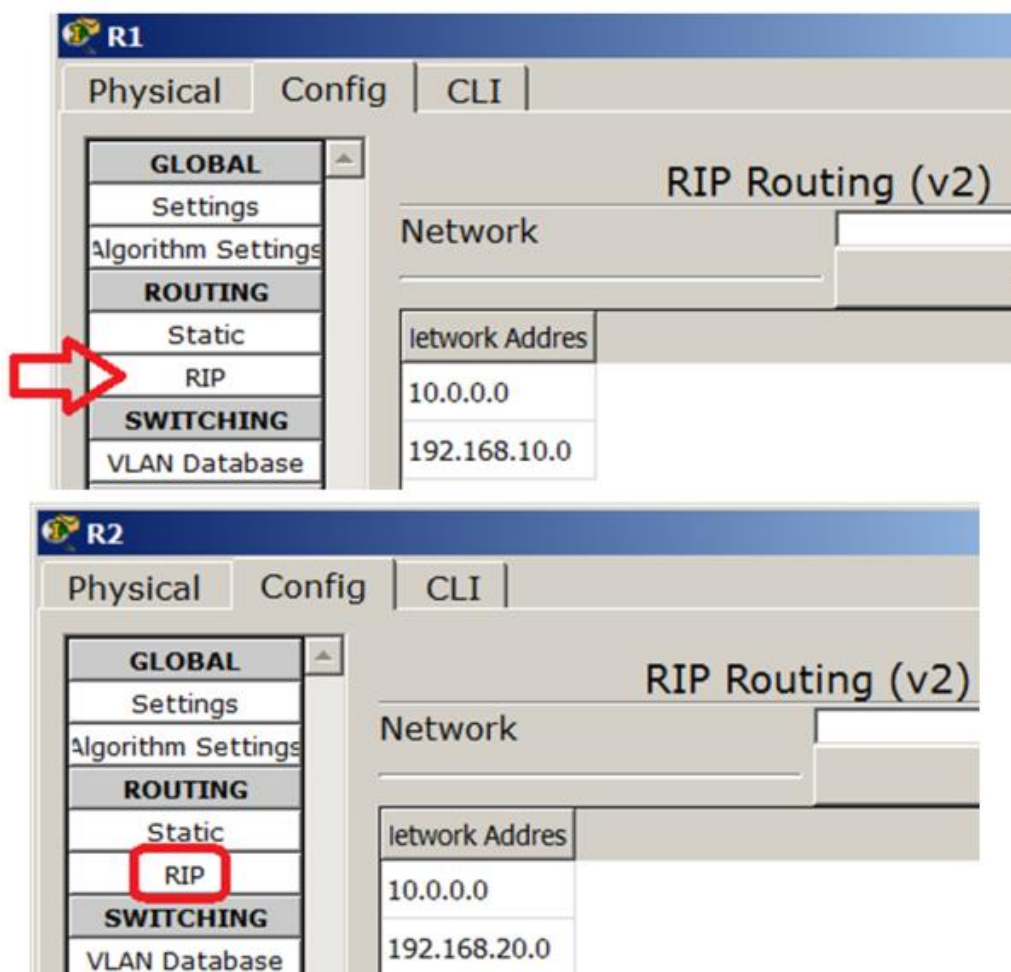
2-marshrutizator konfiguratsiyasini kiriting va quyidagi sozlamalarni bajaring (11.3-rasm).

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.20.1
Router(config-router)#network 10.10.0.2
Router(config-router)#version 2
Router(config-router)#exit
Router(config)#
```

11.3-rasm. R2- marshrutizatorida RIPv2-protokolini sozlash

Kommutator sozlamalarini va RIP protokolini tekshirish

R1 va R2 marshrutizatorlarida RIPv2 protokoli sozlamalarini ko'rib chiqamiz (11.4-rasm).



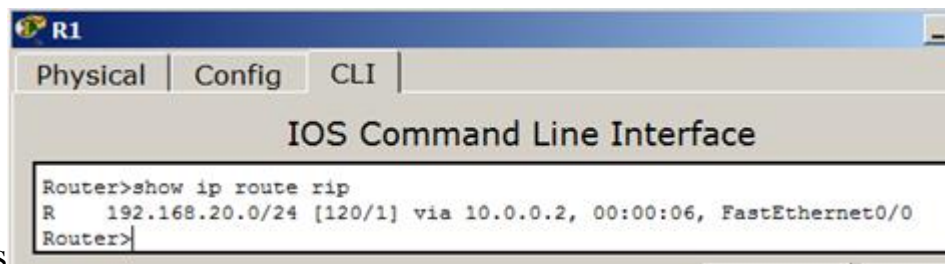
11.4-rasm. R1 va R2 marshrutizatorlarining sozlamalari oynasi

Marshrutizatorlarning haqiqatan ham to'g'ri tuzilganligini va to'g'ri ishlashini tekshirish uchun RIP marshrutizator jadvalini quyidagi buyruq yordamida ko'ring: **Router # show ip route rip** (11.5-rasm va 11.6-rasm).

```
Router>show ip route rip
R   192.168.10.0/24 [120/1] via 10.10.0.1, 00:00:12, FastEthernet0/1
Router>
```

11.5-rasm. R1 marshrutlash jadvali oynasi

Ushbu jadval 192.168.10.0 tarmog'iga faqat bitta marshrut mavjudligini ko'rsatadi: R 1 orqali (10.10.0.1 tarmoq).



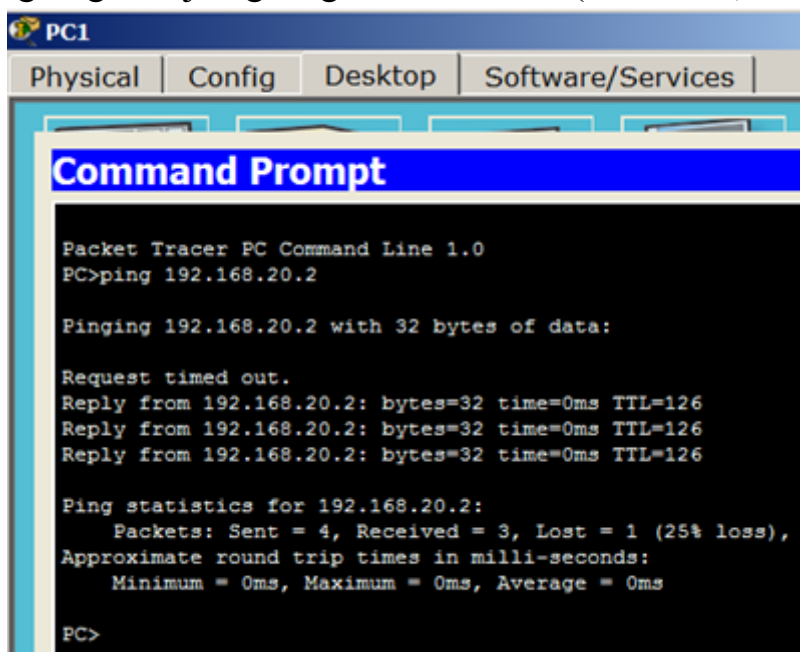
S

11.6-rasm. R2 marshrutlash jadvali oynasi

Ushbu jadval 192.168.20.0 tarmog‘iga bitta marshrut mavjudligini ko‘rsatadi: R2 orqali (tarmoq 10.10.0.2).

PC1 va PC2 o‘rtasidagi aloqani tekshirish

Marshrutning to‘g‘ri bajarilganligini tekshiramiz (11.7-rasm).

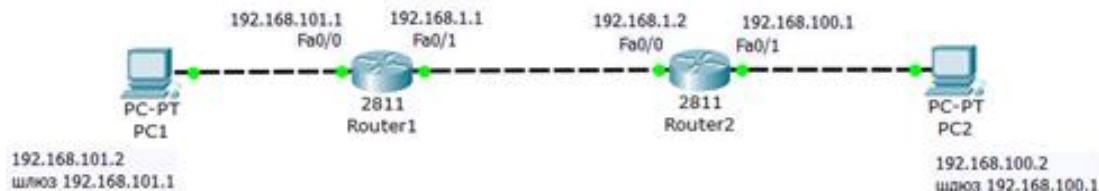


11.7-rasm PC1-dan PC2-ga ping berish oynasi

Amaliy ishni bajarish bo‘yicha topshiriqlar

1-Topshiriq. To‘rt qurilmali tarmoq uchun RIP 2-versiyasini sozlash

11.8-rasmda biz RIPv2 marshrutlash protokolini sozlash uchun foydalanadigan tarmoq ko‘rsatilgan.



11.8-rasm Marshrutlash protokollarini sozlash uchun tarmoq loyihasi

Birinchiidan, R1 ni sozlaymiz (11.9-rasm).

```

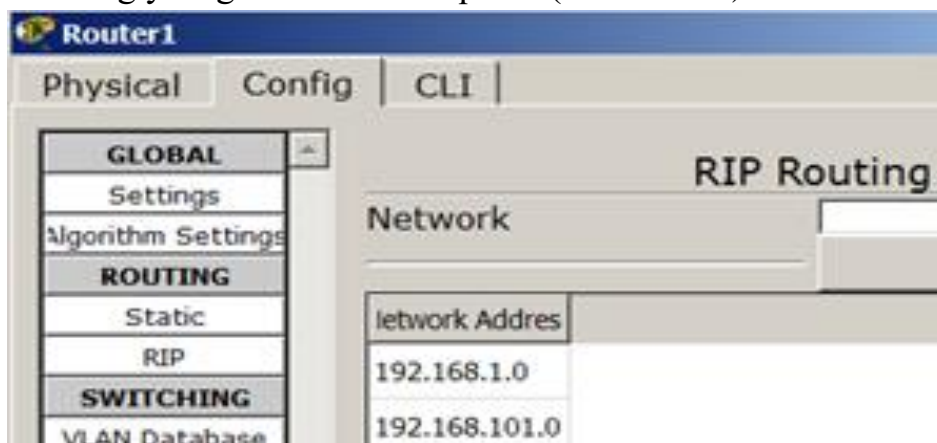
Router1
Physical | Config | CLI
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.101.1
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

```

11.9- rasm R1 marshrutizatorida RIP-protokolini sozlash oynasi

Natijani Config yorlig‘ida ko‘rib chiqamiz (11.10-rasm).



11.10-rasm. R1 marshrutizator oynasi, Config yorlig‘i oynasi

R2-marshrutlashni sozlaymiz (11.11-rasm).

```

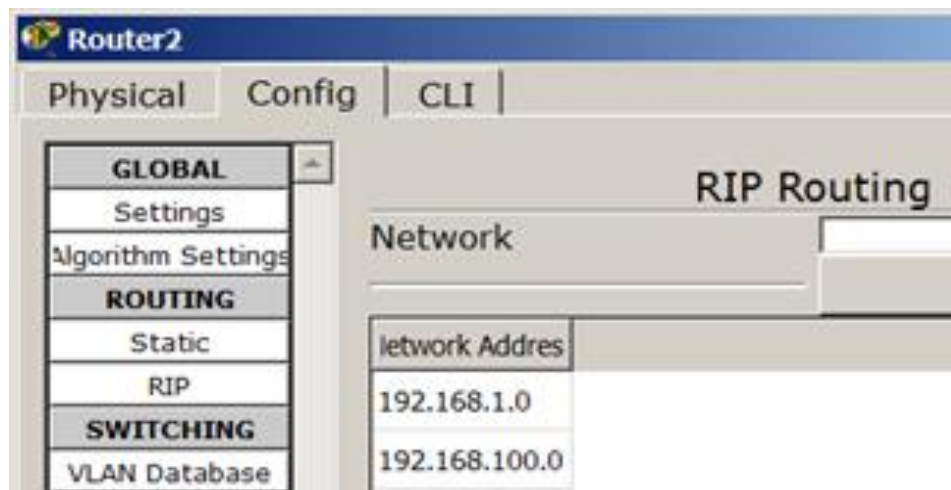
Router2
Physical | Config | CLI
IOS Command Line Interface

Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.100.1
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

```

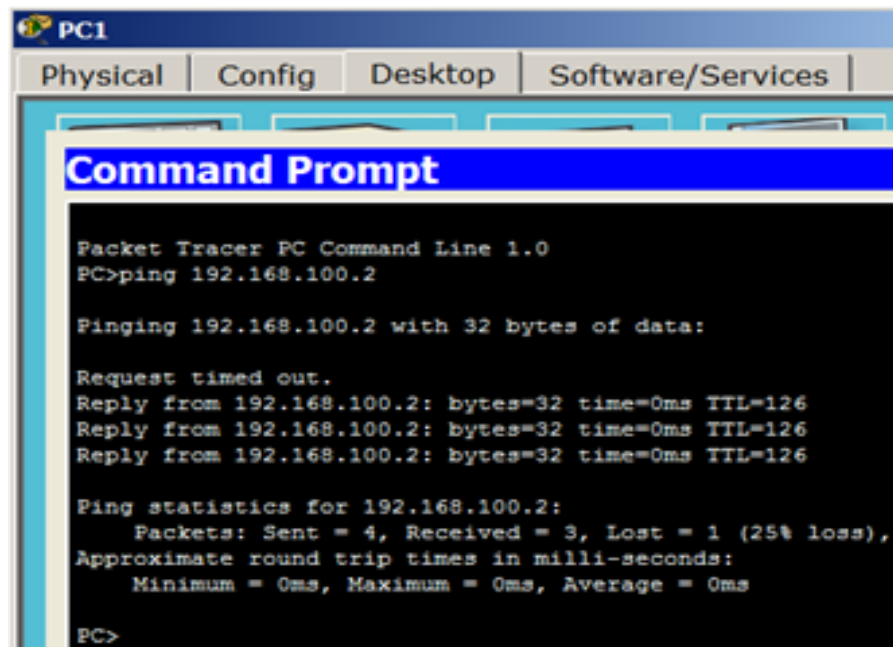
11.11-rasm. R2-marshrutizatorida RIP-protokolini sozlash oynasi

Biz natijani kuzatamiz (9.12-rasm).



11.12-rasm. R2 marshrutizator oynasi, Config yorlig‘i oynasi

Turli xil tarmoqlardan shaxsiy kompyuterlar mavjudligini tekshiramiz (11.13-rasm).



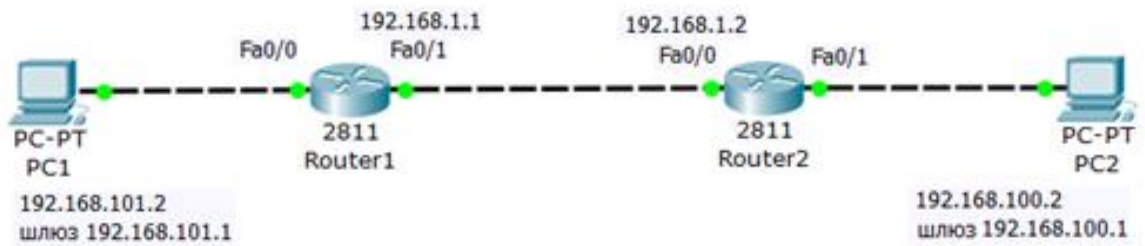
11.13-rasm. RIP protokolini yo‘naltirish natijasi oynasi

EIGRP marshrutlash protokoli

EIGRP protokolini amalga oshirish osonroq va marshrutizatorning hisoblash resurslariga OSPFga qaraganda kam talabchandir. EIGRP-da metrikani hisoblash algoritmi yanada rivojlangan. Metrikani hisoblash formulasida paketning yo‘lidagi interfeyslarning yuklanishi va ishonchliligini hisobga olish mumkin. EIGRP protokolining kamchiligi uning faqat Cisco uskunalarida cheklangan foydalanishidir.

2-Topshiriq. EIGRP protokolini sozlash

Tarmoq sxemasi 11.14-rasm.



11.14-rasm. EIGRP konfiguratsiyasi loyihasi

EIGRP-ni sozlash RIP-ni sozlash bilan juda o‘xshash.

R1 marshrutizatorini dasturlash

R1-ni sozlaymiz (11.15-rasm).

```

Router1
Physical | Config | CLI |
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 192.168.101.1
Router(config-router)#exit
Router(config)#

```

11.15-rasm. R1- marshrutizatorni sozlash oynasi

R2 dasturlash

R2-ni sozlaymiz (11.16-rasm).

```

Router2
Physical | Config | CLI |
IOS Command Line Interface

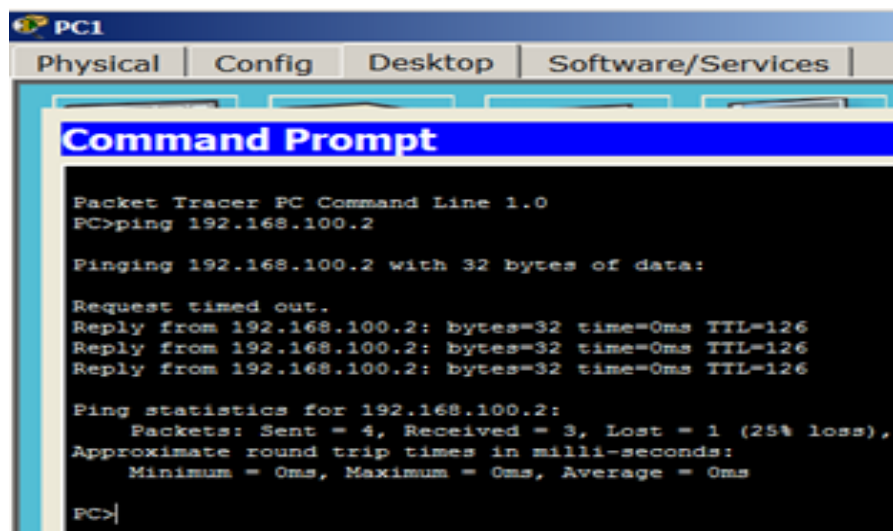
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 192.168.100.1
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

```

11.16-rasm. R2-ni sozlash oynasi

Tarmoq ishini tekshirish

Marshrutizatorning ishlashini tekshiramiz (11.17-rasm).



```
PC1
Physical | Config | Desktop | Software/Services |
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

11.17-rasm. Tarmoq holatini tekshirish natijasi oynasi

OSPF protokoli

OSPF dinamik marshrutlash protokoli har bir marshrutizator qaysi tarmoqlarga ulanganligini tavsiflovchi barcha marshrutizatorlar tomonidan yagona ma'lumotlar bazasidan foydalanishga asoslangan. Har bir kanalni tavsiflashda marshrutizatorlar u bilan metrikani bog'lashadi - bu kanal "sifatini" tavsiflovchi qiymat. Bu OSPF marshrutizatorlarga (barcha kanallar teng bo'lgan RIPdan farqli o'laroq) kanalning haqiqiy o'tkazuvchanligini ko'rib chiqish va eng yaxshi marshrutlarni aniqlashga imkon beradi.

OSPF (Open Shortest Path First) - bu link-state (LSA) texnologiyasiga asoslangan dinamik marshrutlash protokoli bo'lib, eng qisqa yo'lni topish algoritmgiga asoslangan. Kanal holatini kuzatib borish zonadagi mavjud bo'lgan barcha marshrutizatorlarning faol interfeyslariga kanal holatidagi e'lonlarni (LSA) yuborishni talab qiladi. Ushbu e'lonlarda marshrutizator ustidagi har bir kanalning tavsifi va har bir kanalning narxi ko'rsatilgan. LSA xabarlarini faqat tarmoqdagi o'zgarishlar yuz bergan taqdirda yuboriladi, ammo har 30 daqiqada bir marta LSA xabarlarini majburan yuboriladi. Protokol avtonom tizimni zonalarga (hududlarga) bo'linishini amalga oshiradi. Zonalardan foydalanish tarmoq va marshrutizator protsessorlariga tushadigan yukni kamaytirishi va marshrutlash jadvallari hajmini kamaytirishi mumkin.

OSPF protokolining ishlashi

OSPF (Open Shortest Path First) — bu tarmoqda marshrutlashni amalga oshiruvchi dinamik protokol bo'lib, asosan link-state (bog'lanish holati) algoritmiga asoslanadi. OSPF protokoli tarmoqdagi marshrutlarni tez va samarali aniqlash uchun ishlatiladi, va bu protokol IPv4 va IPv6 tarmoq protokollari uchun qo'llaniladi. OSPF protokoli asosan katta tarmoqlarni samarali boshqarish uchun mo'ljallangan, chunki u katta tarmoqlarda osonlik bilan ishlaydi va tarmoqdagi o'zgarishlarga tezda javob beradi.

To'g'ri va teskari maska

Cisco uskunalari ba'zida teskari maskani ishlatish kerak bo'ladi, ya'ni odatdagi 255.255.255.0 (Subnet mask – to'g'ri maska) emas, balki 0.0.0.255 (Wildcard maskai - teskari maska). Teskari maska kirish ro'yxatlarida (access list) va OSPF protokolida tarmoqlarni tavsiflashda ishlatiladi. To'g'ri maska boshqa barcha holatlarda qo'llaniladi. Maskalarning farqi shundaki, to'g'ri maska tarmoqlarda, teskari esa xostlarda ishlaydi. Teskari maska yordamida siz, masalan, barcha tarmoqosti tarmoqlarda ma'lum manzilga ega xostlarni tanlashingiz va ularga Internetga kirishga ruxsat berishingiz mumkin. 255.255.255.0 maskali 192.168.1.0 kabi manzillar ko'pincha mahalliy tarmoqlarda ishlatilganligi sababli, eng keng tarqalgan Wildcard maskasi (shablon maskasi yoki teskari maska yoki invers maska) 0.0.0.255 maskasidir.

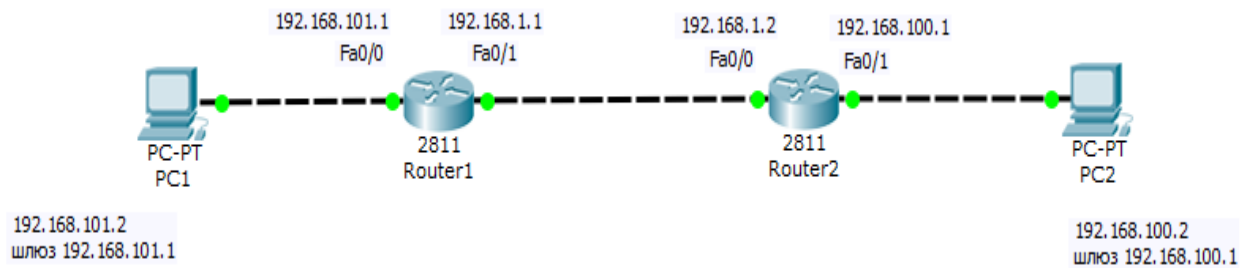
Shablon maskasi (wildcard mask) - bu tarmoqdagi xostlar sonini ko'rsatadigan maska. Tarmoqosti tarmoq maskasiga to'ldiruvchi hisoblanadi. Tarmoqosti tarmoq maskalarining har bir oktetlari uchun 255-tarmoqosti tarmoq maskalari sifatida baholandi. Masalan, tarmoq 192.168.1.0 va tarmoqosti maskasi 255.255.255.242 uchun shablon maskasi 0.0.0.15 ga ko'rinishida bo'ladi. Shablon maskasi ba'zi marshrutlash protokollarining konfiguratsiyasida ishlatiladi, shuningdek kirish ro'yxatlarini cheklash uchun qulay parametrdir.

Shablon maskasini niqoblash

To'g'ri va teskari maska o'rtasida bog'liqlik mavjud: jami har bir bit uchun bu maskalar yig'indisi 255 ga teng bo'lishi kerak. Bizning tarmoq 192.168.32.0 / 28 bo'lsin. Shablon maskasi quyidagicha hisoblaydi: prefiks / 28 - 255.255.255.240 yoki 11111111.11111111.11111111.11110000. Shablon maskasi uchun bizga faqat nollar kerak bo'ladi, ya'ni 11110000 raqamini o'nli raqamga o'tkazamiz va hisoblaymiz: $128/64/32/16/8/4/2/1$ u $8 + 4 + 2 + 1 = 15$ bo'ladi, ya'ni. bizning shablon maskamiz 0.0.0.15 bo'ladi.

4-Topshiriq. 4 ta qurilma uchun OSPF protokolini sozlash

9.18-rasmda ko'rsatilgan sxemani yig'ing.



11.18-rasm OSPF protokolini sozlash loyihasi

Marshrutizatorlarni sozlash

R1 ni sozlaymiz (11.19-rasm).

```

Router1
Physical Config CLI
IOS Command Line Interface
Router(config)#router ospf 1
Router(config-router)#network 192.168.101.0 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#exit
  
```

11.19-rasm. R1- marshrutlashni sozlash oynasi

Endi R2 marshrutlash uchun sozlamalarni oʻrnatamiz (9.20-rasm).

```

Router2
Physical Config CLI
IOS Command Line Interface
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.100.1 0.0.0.255 area 0
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
  
```

11.20-rasm. R2 sozlamalari oynasi

Agar CPT-da marshrutizator sozlamalarini tiklashingiz kerak boʻlsa, uning quvvat tugmachasini oʻchirib qoʻying va keyin uni qayta yoqing.

Natijani tekshirish

Marshrutni tekshirish uchun biz turli xil tarmoqlardan shaxsiy kompyuterlarni ping bilan oʻtkazamiz (11.21-rasm).

```
PC2
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.101.2

Pinging 192.168.101.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.101.2: bytes=32 time=0ms TTL=126
Reply from 192.168.101.2: bytes=32 time=0ms TTL=126
Reply from 192.168.101.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.101.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

```
PC1
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.100.2: bytes=32 time=0ms TTL=126
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126
Reply from 192.168.100.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

11.21-rasm OSPF ishlashini tekshirish natijalari oynasi

Amaliy ish bo'yicha savollar

1. Marshrutlash nima?
2. Dinamik marshrutlash nima?
3. EIGRP qanday protokol?
4. BGP qanday protokol?
5. OSPF qanday protokol?
6. RIP qanday protokol?
7. Marshrutlash protokollari necha turga bo'linadi?

Amaliy ish № 12

CISCO PACKET TRACER DASTURIDA DHCP SERVERINI SOZLASH

Ishdan maqsad: Cisco Packet Tracer dasturi yordamida DHCP serverini o‘rganish va qo‘llash ko‘nikmasiga ega bo‘lish.

Nazariy qism

DHCP (Dynamic Host Configuration Protocol) tarmoqdagi qurilmalarga IP manzillari, quyi tarmoq maskalari, standart shlyuz va boshqa tarmoq konfiguratsiya parametrlarini avtomatik ravishda tayinlaydigan protokoll. DHCP tarmoqlarni sozlash va boshqarishni sezilarli darajada osonlashtiradi, ayniqsa qurilmalar soni juda ko‘p bo‘lishi mumkin bo‘lgan yirik tashkilotlarda. DHCP qanday ishlaydi?

1. So‘rov (DHCP Discover):

Qurilma (masalan, kompyuter yoki smartfon) tarmoqqa ulanganda va IP-manzilni olish kerak bo‘lganda, u DHCP serverini topish uchun tarmoqqa “DHCP Discover” so‘rovini yuboradi.

2. DHCP taklifi:

DHCP serveri so‘rovni qabul qilgandan so‘ng “DHCP Taklifi” bilan javob beradi va qurilmaga IP-manzil va boshqa konfiguratsiya parametrlarini taklif qiladi, masalan:

- Subnet maskasi
- Standart shlyuz
- DNS serverlari
- IP-manzilni ijaraga olish vaqti

3. “So‘rov (DHCP so‘rovi):”

Qurilma takliflardan birini tanlaydi (agar bir nechta bo‘lsa) va uning tanlovini tasdiqlovchi serverga “DHCP so‘rovini” yuboradi.

4. Tasdiqlash (DHCP ruxsati):

DHCP serveri qurilma so‘rovini “DHCP Ack” bilan tasdiqlaydi, bu qurilma tayinlangan IP manzilini va boshqa konfiguratsiya parametrlarini olganligini ko‘rsatadi.

5. IP manzilni ijaraga olish:

DHCP serveri ma‘lum vaqt (lizing) uchun IP-manzilni tayinlaydi. Bu vaqt o‘tgandan so‘ng, agar u hali ham tarmoqqa ulangan bo‘lsa, qurilma yana yangi IP manzilini so‘rashi kerak.

DHCP afzalliklari:

1. Avtomatlashtirish: DHCP IP manzillari va boshqa tarmoq parametrlarini belgilash jarayonini avtomatlashtiradi, xatolar ehtimolini kamaytiradi va boshqaruvni soddalashtiradi.

2. Markazlashtirilgan boshqaruv: Barcha IP manzillar va parametrlar DHCP serverida markazlashtirilgan tarzda sozlangan bo'lib, tarmoq sozlamalarini o'zgartirishni osonlashtiradi.

3. Moslashuvchanlik: DHCP IP manzillarini dinamik ravishda belgilash imkonini beradi, bu qurilmalar tez-tez ulangan va uzilib qolgan tarmoqlar uchun ideal.

4. Ijara muddatini boshqarish:

Mavjud manzillardan samarali foydalanishni ta'minlash uchun ma'murlar IP-manzillar uchun ijara muddatini sozlashi mumkin.

DHCP-ni qanday sozlash mumkin?

1.Routerda DHCP-ni sozlash:

- Routingizda DHCP serverini yoqing (agar u ushbu xususiyatni qo'llab-quvvatlasa).

- Router qurilmalarga beradigan IP manzillar diapazonini sozlang.

- Standart shlyuz, DNS serverlar va ijara vaqti kabi qo'shimcha parametrlarni belgilang.

Cisco routeridagi konfiguratsiya namunasi:

```
Router(config)# ip dhcp pool my_pool
```

```
Router(dhcp-config)# tarmoq 192.168.1.0 255.255.255.0
```

```
Router(dhcp-config)# sukut bo'yicha router 192.168.1.1
```

```
Router(dhcp-config)# dns-server 8.8.8.8
```

```
Router(dhcp-config) # ijarasi 7
```

2.Mijozdagi konfiguratsiya:- Mijoz qurilmalarida (kompyuterlar, smartfonlar va boshqa qurilmalar) avtomatik ravishda (DHCP orqali) IP-manzilni olish uchun sozlamani yoqing. Bu odatda sukut bo'yicha yoqilgan.

Windows uchun misol:

- Tarmoq va almashish markazini oching.

- "Adapter sozlamalarini o'zgartirish" ni tanlang.

- Tarmoq ulanishini o'ng tugmasini bosing> "Xususiyatlar".

- Internet Protocol Version 4 (TCP/IPv4) > IP-manzilni avtomatik ravishda olish-ni tanlang.

3. Alohida serverda DHCP server konfiguratsiyasi:

- Katta tarmoqlarda DHCP server alohida qurilma yoki IP manzillarni taqsimlashni boshqaruvchi server bo'lishi mumkin.

- Masalan, Windows Serverda DHCP serveri "Server Manager" orqali sozlangan, Linuxda esa "dhcpd" (ISC DHCP server) xizmatidan foydalaniladi.

DHCP ijarasi turlari

1. "Doimiy" IP-manzilni ijaraga olish (Statik DHCP):

- Ba'zan serverlar yoki printerlar kabi ba'zi qurilmalar "doimiy" IP manzillar bilan sozlanishi mumkin. Buni DHCP serverida MAC manzili asosida ma'lum bir qurilma uchun statik IP manzilini ko'rsatish orqali amalga oshirish mumkin.

2. "Dinamik" IP-manzilni ijaraga olish (Dynamic DHCP):

- Ko'pgina hollarda, DHCP har safar qurilma ulanganda o'zgarishi mumkin bo'lgan vaqtinchalik (dinamik) IP manzillarni tayinlaydi.

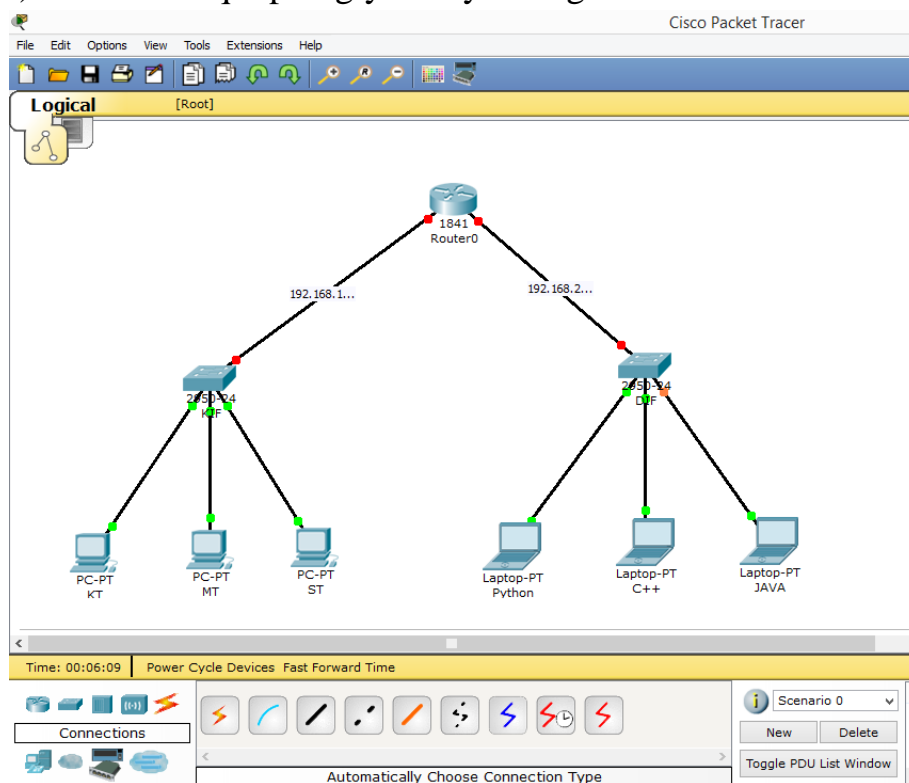
3. Kengaytmali ijara (DHCP Renew):

- Agar u hali ham tarmoqqa ulangan bo'lsa, qurilma joriy IP-manzil ijarasini kengaytirishni so'rashi mumkin.

Xulosa qilib aytganda DHCP avtomatik tarmoq konfiguratsiyasi uchun muhim protokol bo'lib, qurilma boshqaruvi va konfiguratsiyasini sezilarli darajada osonlashtiradi. U avtomatik ravishda IP manzillarini tayinlaydi, bu tarmoqni tez va samarali sozlash imkonini beradi, ayniqsa katta, dinamik muhitda.

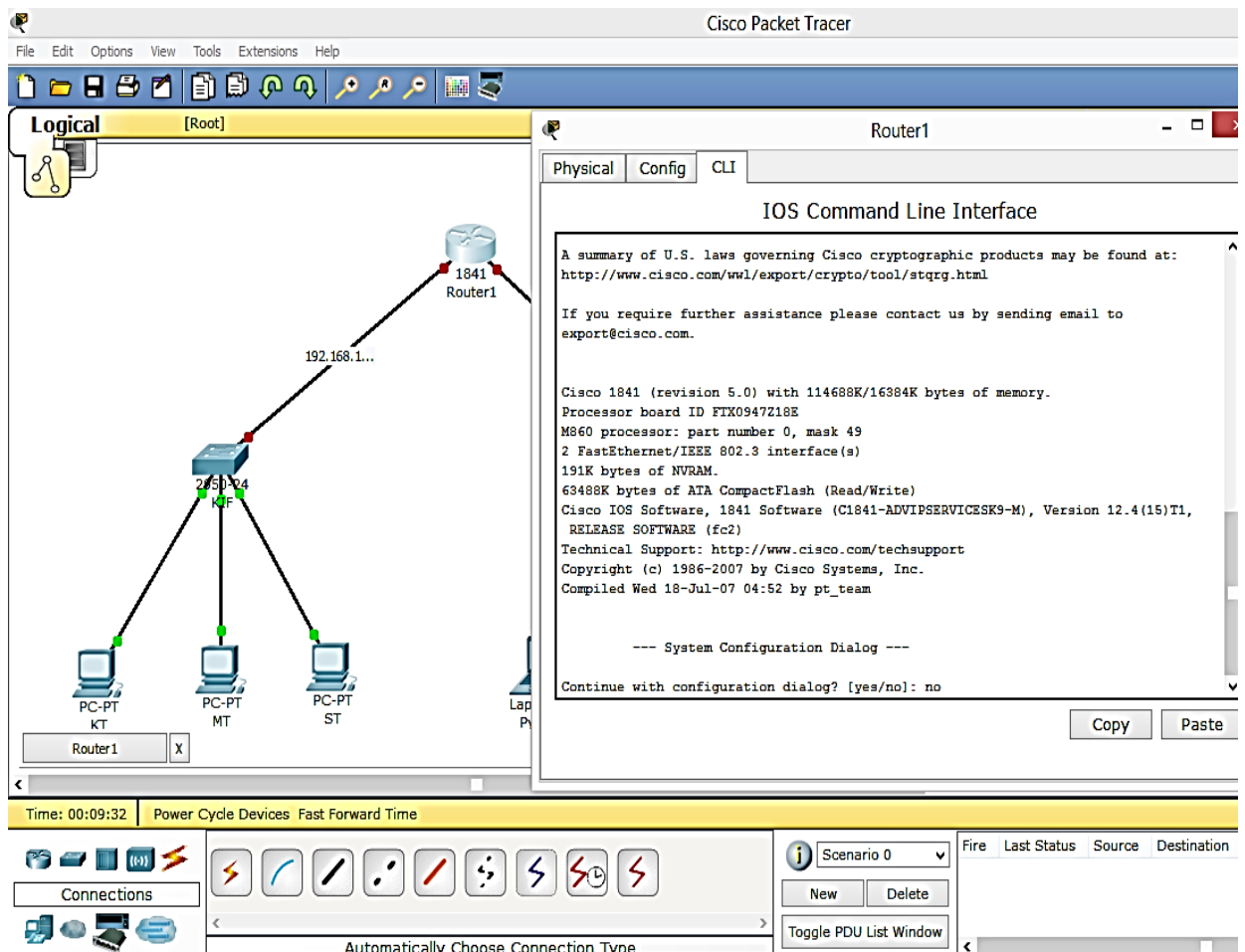
Amaliy ishni bajarish tartibi

Cisco Packet Tracer dasturida ikkita alohida segment (192.168.1... va 192.168.2...) bilan tarmoq topologiyasini yarating.



12.1-rasm, Tarmoqni loyihalash jarayoni

Router ichki oynasida CLI buyrug'ini bosib va dastlabki konfiguratsiya ekranida (yes/no) NO ya'ni yo'q buyrug'ini tanlang va Enter tugmasini bosib. Agar siz ushbu ekranda YES ya'ni ha tugmasini tanlasangiz, Cisco router sizdan bosqichma-bosqich asosiy sozlamalarni bajarishni so'raydi.



12.2-rasm. CLI oynasi

DHCP ni Routerdan mijozga avtomatik ravishda tarqatish uchun quyidagi buyruqlarni bajarib yoping.

```

RouterR>enable
RouterR#conf t
RouterR(config)#interface fastEthernet 0/0
RouterR(config-if)#ip address 192.168.1.1 255.255.255.0
RouterR(config-if)#no shutdown
RouterR#conf t
RouterR(config)#interface fastEthernet 0/1
RouterR(config-if)#ip address 192.168.2.1 255.255.255.0
RouterR(config-if)#no shutdown
RouterR(config-if)#exit
RouterR(config)#ip dhcp pool LAN1
RouterR(dhcp-config)#network 192.168.1.0 255.255.255.0
RouterR(dhcp-config)#default-router 192.168.1.1
RouterR(dhcp-config)#dns-server 192.168.2.1
RouterR(dhcp-config)#exit

```



```
RouterR(config)#ip dhcp excluded-address 192.168.1.1
RouterR(config)#ip dhcp pool LAN2
RouterR(dhcp-config)#network 192.168.2.0 255.255.255.0
RouterR(dhcp-config)#default-router 192.168.2.1
RouterR(dhcp-config)#dns-server 192.168.2.1
RouterR(dhcp-config)#exit
RouterR(config)#ip dhcp excluded-address 192.168.2.1
RouterR(config)#end
RouterR#wr
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o up
```

12.3-rasm. Qurilma kodi

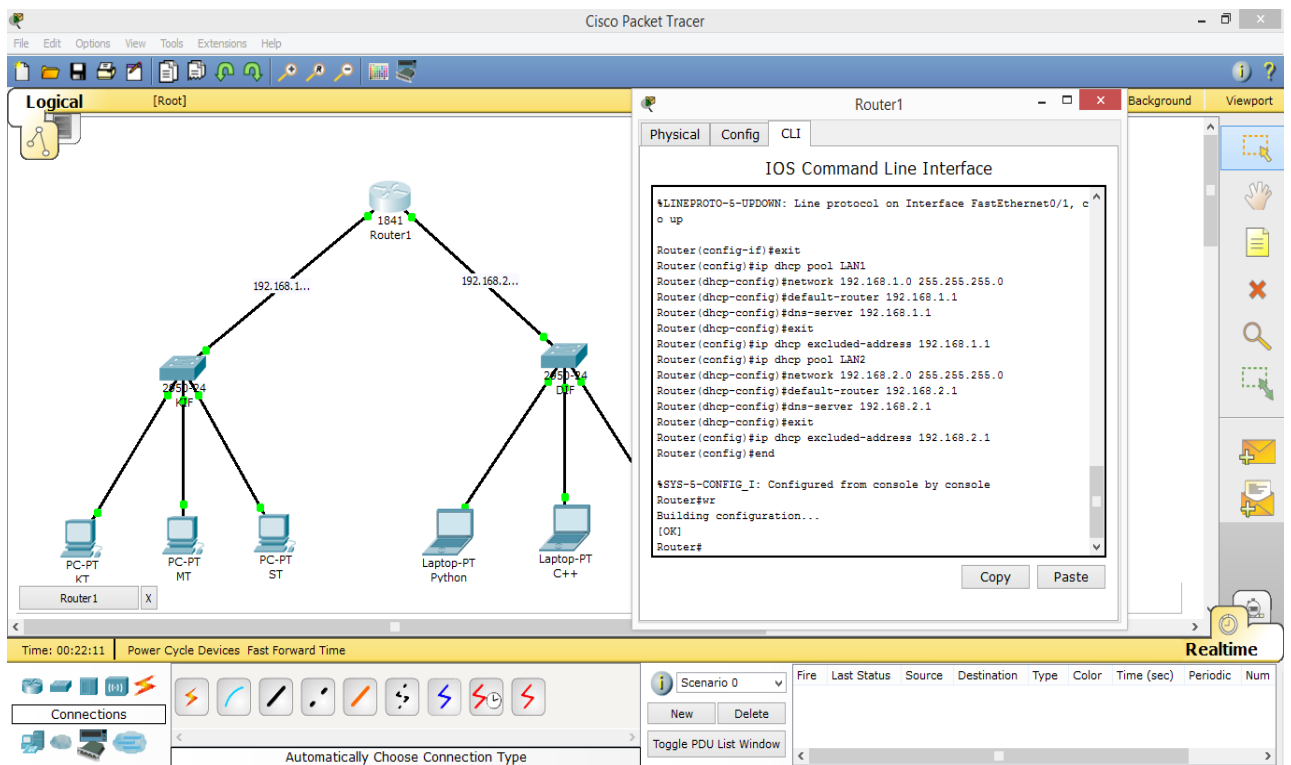

```

Router(config-if)#exit
Router(config)#ip dhcp pool LAN1
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 192.168.1.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#ip dhcp pool LAN2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.1
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.2.1
Router(config)#end

%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
Router#

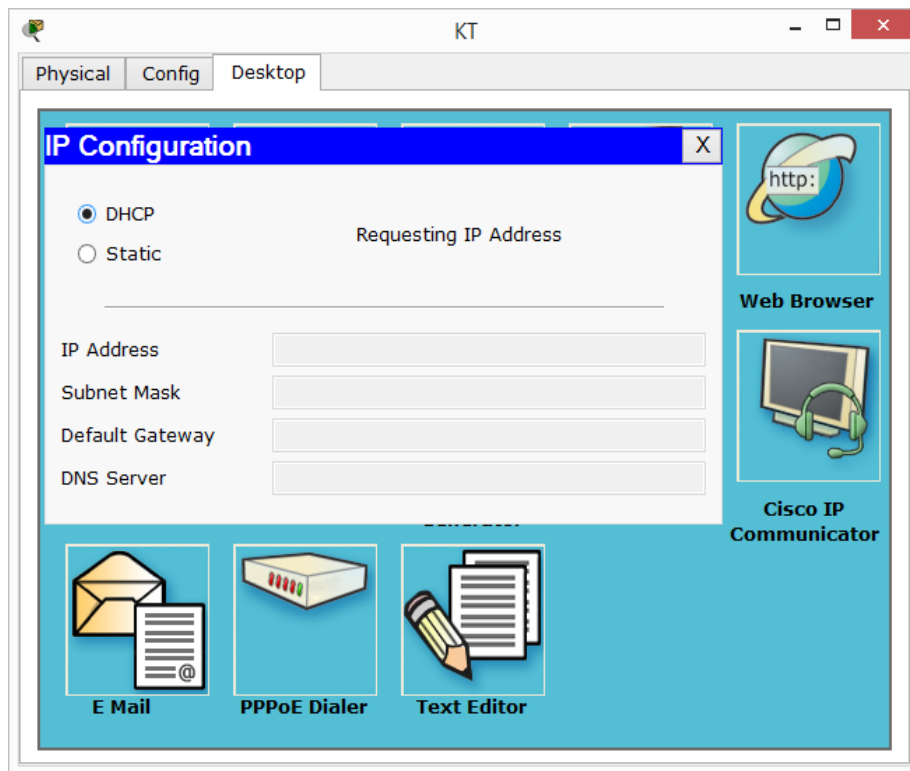
```

12.4-rasm. Qurilma kodi



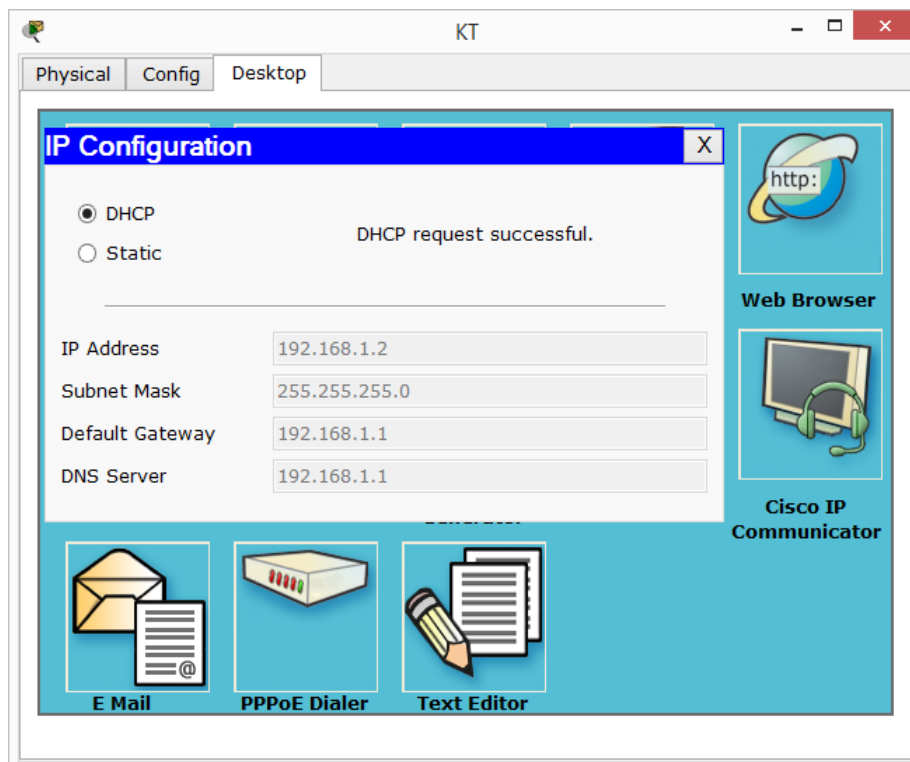
12.5-rasm. Loyihalashtirilgan tarmoqni sozlash

Cisco Tracerda DHCP buyruqlarini kiritganingizdan so‘ng, avtomatik IP manzil uchun dastur ish maydoniga qo‘shadigan kompyuterlarni sozlashimiz kerak. Buning uchun KT ni tanlaymiz, ochilgan oynada IP ni sozlashni bosamiz va keyin DHCP ni tanlaymiz



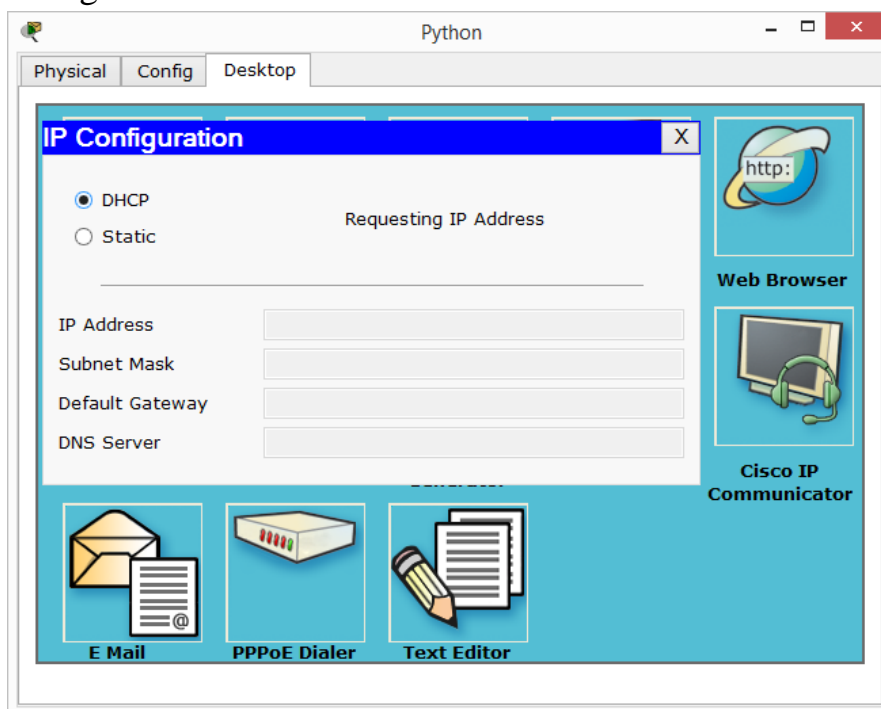
12.6-rasm. DHCP sozlash oynasi

KT da DHCP ni yopgandan soʻng, quyidagi rasmdagi kabi IP manzil soʻrovi yuboriladi. DHCP KT soʻroviga javob berish orqali IP manzilini ajratadi.



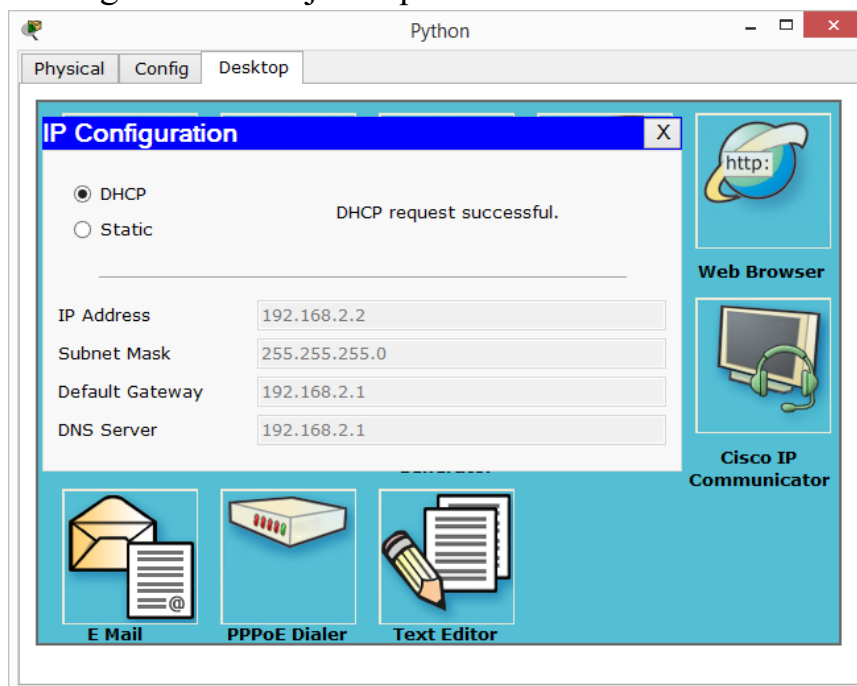
12.7-rasm. DHCP sozlash oynasi

192.168.2.... tarmog'idagi kompyuterlar uchun DHCP parametrini yoping va natijani tekshiring.



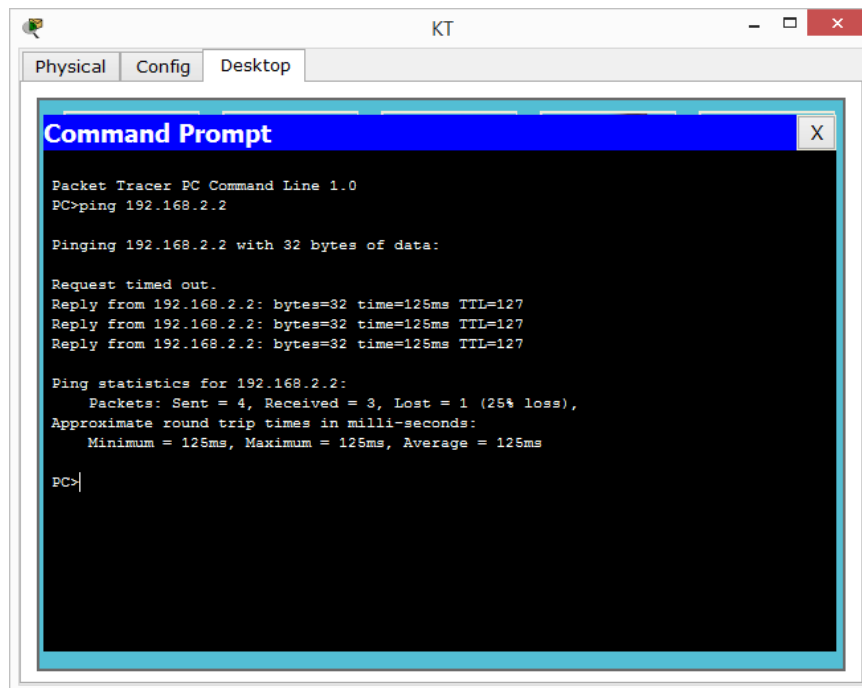
12.8-rasm. DHCP sozlash oynasi

Dastur IP manzilini muvaqqiyatli oladi, chunki DHCP Cisco yo'riqnomasida 192.168.2.... tarmog'i uchun natija chiqaradi.



12.9-rasm. DHCP sozlash oynasi

KT ni 2.0 ga ulab tarmoq ulanishini sinab ko'rsangiz, bu quyidagicha muvaffaqiyatli bo'ladi.



12.10-rasm. Desktop oynasi

Siz Routerda Show IP DHCP buyrug‘i bilan mijozlarga tayinlangan IP manzillari va MAC manzillarini ko‘rishingiz mumkin.

Router>show ip dhcp binding

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.2	0060.47C3.26A0	--	Automatic
192.168.2.2	00E0.B0CD.67BD	--	Automatic

12.11-rasm. Qurilma manzili

Amaliy ish bo‘yicha topshiriqlar variantlari:

Kompyuterlari 8 tadan va 2 ta marshrutizatorlardan lokal tarmoqni DHCP orqali bog‘lang.

Avtomatik tarzda berilgan IP manzillarni tekshirib natijalarga etibor qarating. Loyihalangan tarmoqdagi ishlarni. rasmlar va izohlar ko‘rinishida hisobot shaklida topshiring.

Nazorat savollari:

1. DHCP nima?
2. Marshrutizator vazifasi nimadan iborat?
3. IP manzillarni berishning qanday usullari bor?
4. Router qanday qurilma hisoblanadi?

Amaliy ish № 13

CISCO PACKET TRACER DASTURIDA TELNET VA SSH PROTOKOLI BILAN ISHLASH

Ishdan maqsad: Cisco Packet Tracer dasturida TELNET av SSH protokoli bilan ishlash ko'nikmasini hosil qilish.

Nazariy qism

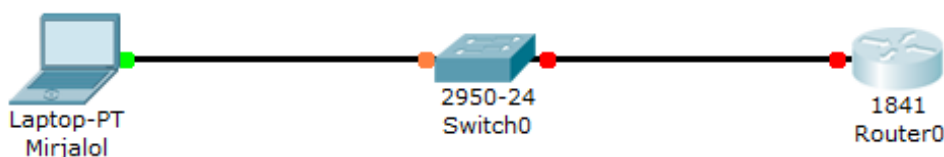
SSH va Telnet ikkita tarmoq protokoli bo'lib, ular masofadan turib kompyuterga tarmoq ichida yoki Internet orqali ushbu tizimga kirish orqali ulanishda va masofaviy buyruqlar yordamida tizimni boshqarish uchun ishlatiladi. Shunday qilib, ikkalasi ham terminal emulyatorlari deb hisoblanadi. SSH Secure Shell degan ma'noni anglatadi va SSH foydalanuvchi xavfsiz shifrlangan ulanishdan foydalangan holda tarmoqdagi kompyuterlar juftligi o'rtasida ma'lumot almashish imkoniyatini beradi. Telnet asosiy tarmoq protokoli bo'lib, u masofaviy tizim bilan matnli terminaldan deyarli foydalangan holda aloqa qilish uchun ishlatiladi.

SSH, Secure Shell - bu tarmoq protokoli bo'lib, u ikkita masofaviy xostlar o'rtasida Internet orqali yoki tarmoq ichida xavfsiz aloqani o'rnatish uchun ishlatiladi. SSH kompyuterlar o'rtasida ma'lumotlarni uzatish uchun shifrlangan formatdan foydalanadi, shuning uchun ushbu shifrlangan mexanizm almashinilayotgan ma'lumotlarning maxfiyligi va yaxlitligini ta'minlaydi. SSH masofadan kirish tizimlarida va yuqori darajadagi xavfsizlik mavjudligi sababli masofaviy buyruqlarni bajarish uchun keng qo'llaniladi. SSH-dan foydalanuvchi foydalanuvchi nomi, parol va boshqa buyruqlar kabi maxfiy ma'lumotlarni xavfsiz tarzda yuborishi mumkin, chunki bu ma'lumotlar shifrlangan formatda va ularni shifrlash va xakerlar tomonidan oson o'qilishi mumkin emas. SSH masofaviy tizimni autentifikatsiya qilish uchun ochiq kalitlarning kriptografiyasidan foydalanadi. SSH serverlari 22 portni TCP (Transmission Control Protocol) standarti orqali tinglaydi va ulardan jamoat tarmog'ida foydalanish mumkin. U ishonchli autentifikatsiya va xavfli kanallar orqali xavfsiz aloqa mexanizmini ta'minlaydi.

Telnet, shuningdek, tarmoqdagi yoki Internetdagi ikkita uzoq xostlar o'rtasida ma'lumotni ikki tomonlama yo'nalishda almashish uchun foydalaniladigan tarmoq protokoli. Ushbu protokol yordamida foydalanuvchilar masofaviy tizimga kirishlari va virtual terminal yordamida aloqa qilishlari mumkin, ammo bu Internet kabi ishonchsiz tarmoqlardan foydalanish uchun xavfli. Telnet oddiy matnda ma'lumotlarni almashadi, shuning uchun ushbu protokol yordamida foydalanuvchi nomlari va parollarini o'z ichiga olgan maxfiy ma'lumotlarni yuborish uchun mos emas, chunki boshqa kimdir ushbu matnni almashishni o'qiy oladi va xabarlarini osongina ushlay oladi. Odatda Telnet 23 port orqali TCP orqali ulanadi va boshqa portlar va xizmatlarga ham kirishi mumkin. U kam xavfsizlik tufayli xususiy tarmoqlarda ishlatilishi mumkin.

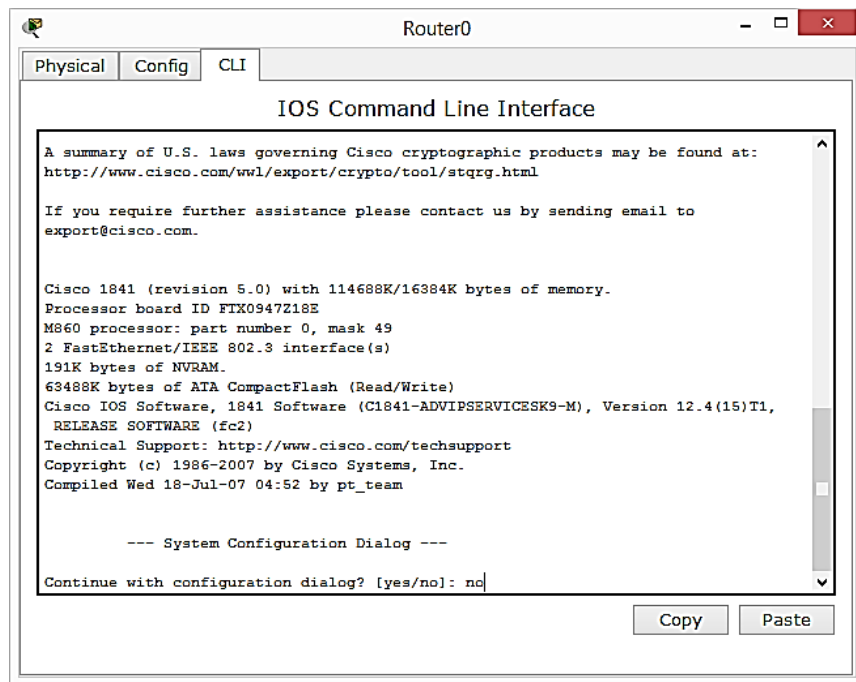
Amaliy ishni bajarish tartibi

1. Cisco Packet Tracer-da kichik bir topologiyani yarataylik. Mahalliy tarmoq orqali marshrutizatorga ulanish uchun Telnetni sozlaylik. Cisco marshrutizator, kommutator va kompyuterni ish maydoniga qo'shgandan so'ng, biz barcha qurilmalarni kabellar bilan ulaymiz.



13.1-rasm. Tarmoqni loyihalsh

CLI buyruq satrini ochish uchun Router-ni ikki marta bosing. Dastlabki o'rnatishni o'tkazib yuborish uchun "Yo'q" deb yozing va Enter ni bosing.



13.2-rasm. Qurilmani sozlash

Routerda Telnet-protokolini yoqish uchun quyidagi buyruqlarni bajaring:

```
Router>en
```

```
Router#enable
```

```
Router#conf t
```

```
Router(config)#interface fastEthernet 0/0
```

```
Router(config-if)#ip address 192.168.0.1 255.255.255.0
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
```

```
Router(config)#line vty 0 4
```

```
Router(config-line)#login local
```

```
Router(config-line)#password telnet123
```

```
Router(config-line)#privilege level 15
```

```
Router(config-line)#exit
```

```
Router(config)#username cisco privilege 15 password cisco123
```

```
Router(config)#end
```

```
Router#wr
```



```

      --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>en
Router#enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

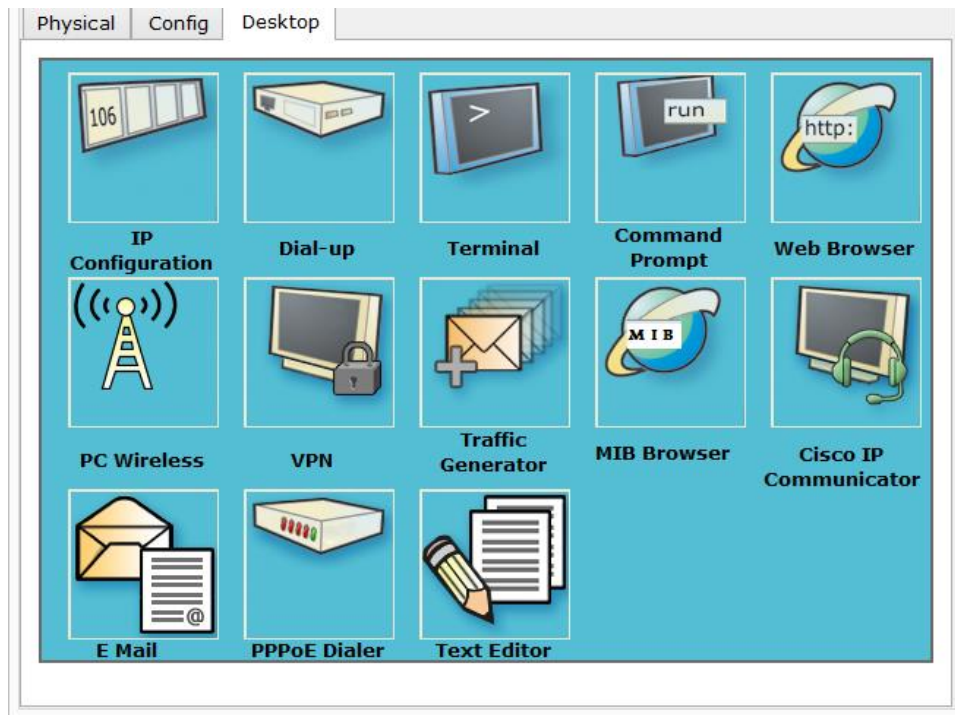
Router(config-if)#exit
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#password telnet123
Router(config-line)#privilege level 15
Router(config-line)#exit
Router(config)#username cisco privilege 15 password cisco123
Router(config)#end

%SYS-5-CONFIG_I: Configured from console by console
Router#wr
Building configuration...
[OK]
Router#

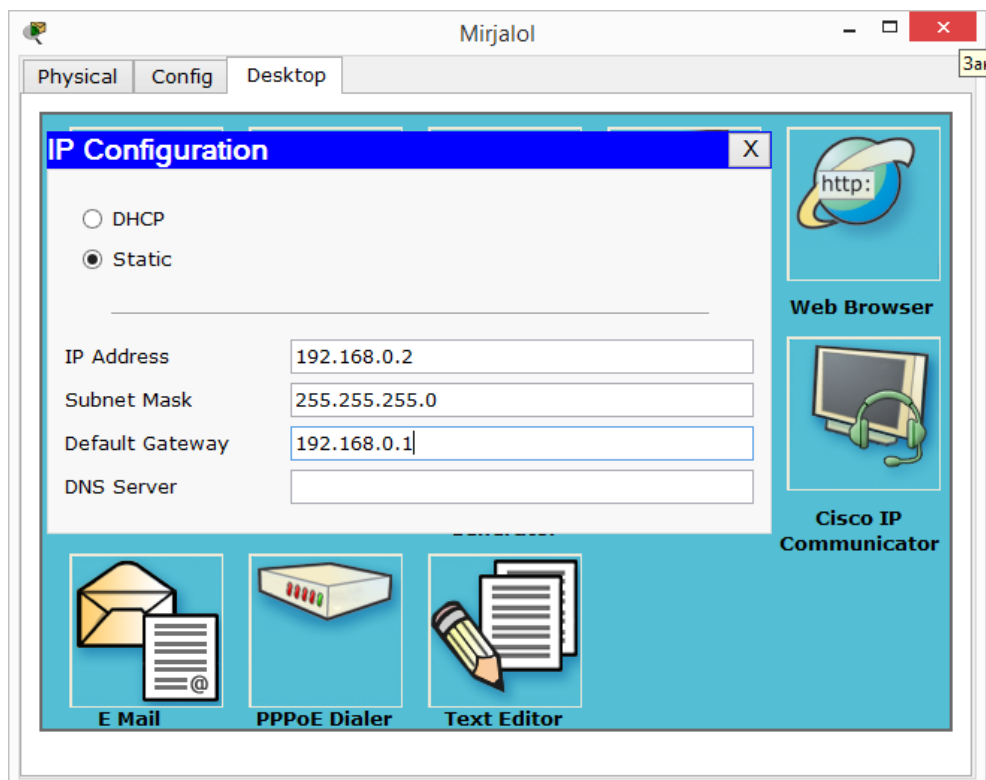
```

13.3-rasm. Qurilmaga kod yozish

4. Routerni sozlashdan so'ng, Cisco Telnet ulanishi uchun foydalanuvchi nomi va parolini yaratdi. Routerga ulanishdan oldin kompyuterda konfiguratsiyani ish joyida quyidagicha o'rnatish:



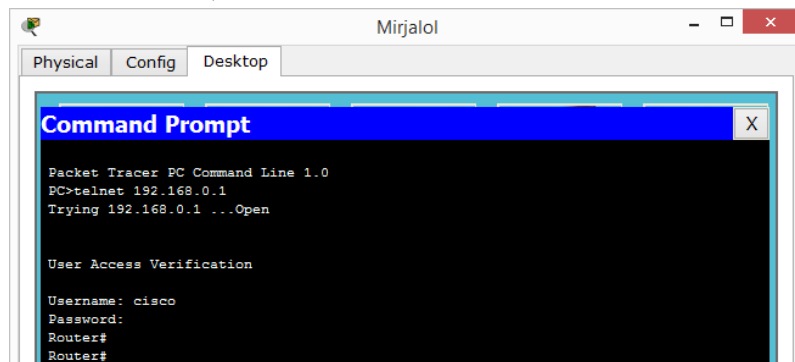
13.4-rasm. Desktop oynasi



13.5-rasm. Statik manzillash

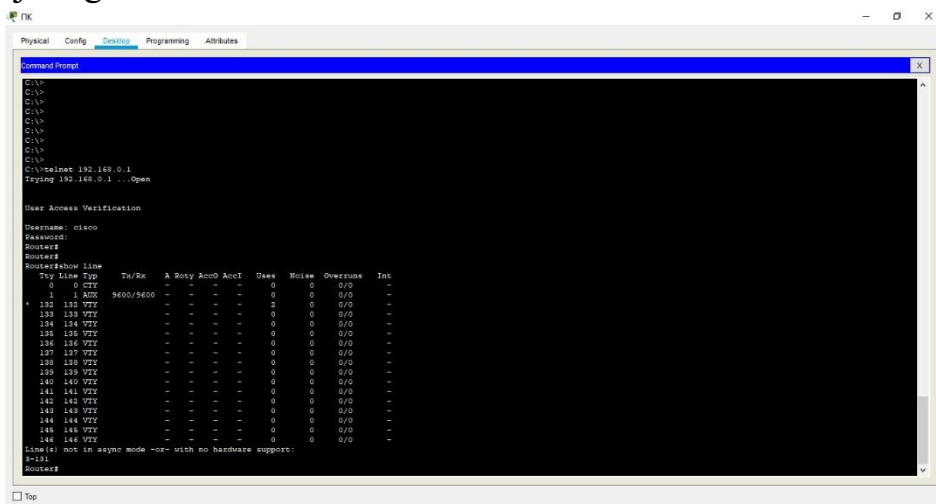
IP sozlamasini yoping va CMD buyruq satriga o'ting (Command prompt).

Buyruq satrida telnet 192.168.0.1 kiriting va Enter bosing. Keyin foydalanuvchi nomi va parol kiritiladi. Bunday holda, Username: cisco, Password: cisco123 (parolni kiritish ko'rinmas).



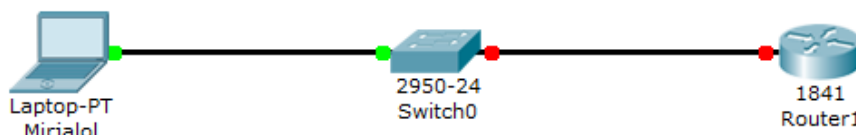
13.6-rasm. Buyruq satri oynasi

Cisco routeriga ulanganingizdan so'ng, siz LAN va WAN orqali qurilmangizni boshqarishingiz mumkin. Qurilmaga ulanishlarni ko'rish uchun **show line** buyrug'ini bajaring.



13.7-rasm. Qurilmaga ulanish oynasi

Endi SSH-ni kommutatorlarda sozlaylik - buning uchun siz hostname, domen nomini ko'rsatishingiz va shiflash kalitini yaratishingiz kerak.



13.8-rasm. Loyihalashtirilgan tarmoq

Router-ni ikki marta bosing va buyruq satriga o'ting. Dastlabki sozlamalarni o'tkazib yuborish uchun Enter tugmasini bosing .

Routingizga SSH-ni o'rnatish uchun quyidagi buyruqlarni tartibda bajaring.

```

Router>enable
Router#conf t
Router(config)#hostname ADMIN
ADMIN(config)#interface fastethrnet 0/0
ADMIN(config-if)#ip address 192.168.1.1 255.255.255 .0
ADMIN(config-if)#no shutdown
ADMIN(config-if)#ip domain name ciscoadmin
ADMIN(config)crypto key generate rsa

```

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ADMIN
ADMIN(config)#interfase fastEthernet 0/0
      ^
% Invalid input detected at '^' marker.

ADMIN(config)#int
ADMIN(config)#interface fas
ADMIN(config)#interface fastEthernet 0/0
ADMIN(config-if)#ip address 192.168.1.1 255.255.255.0
ADMIN(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

ADMIN(config-if)#ip domain name ciscoadmin
ADMIN(config)#cryoto key generatersa
      ^
% Invalid input detected at '^' marker.

ADMIN(config)#
ADMIN(config)#crypto key genera
ADMIN(config)#crypto key generate r
ADMIN(config)#crypto key generate rsa
The name for the keys will be: ADMIN.cisoadmin
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```

13.9-rasm. Qurilma kodi

```

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

ADMIN(config)#ip ssh version 2
*??? 1 0:9:16.396: %SSH-5-ENABLED: SSH 1.99 has been enabled
ADMIN(config)#ip ssh time-out 10
ADMIN(config)#ip ssh aut
ADMIN(config)#ip ssh authentication-retries 3
ADMIN(config)#line vty 0 4
ADMIN(config-line)#login local
ADMIN(config-line)#pri
ADMIN(config-line)#privilege le
ADMIN(config-line)#privilege level 15
ADMIN(config-line)#tra
ADMIN(config-line)#transport le
ADMIN(config-line)#transport level
ADMIN(config-line)#transport level 15
^
% Invalid input detected at '^' marker.

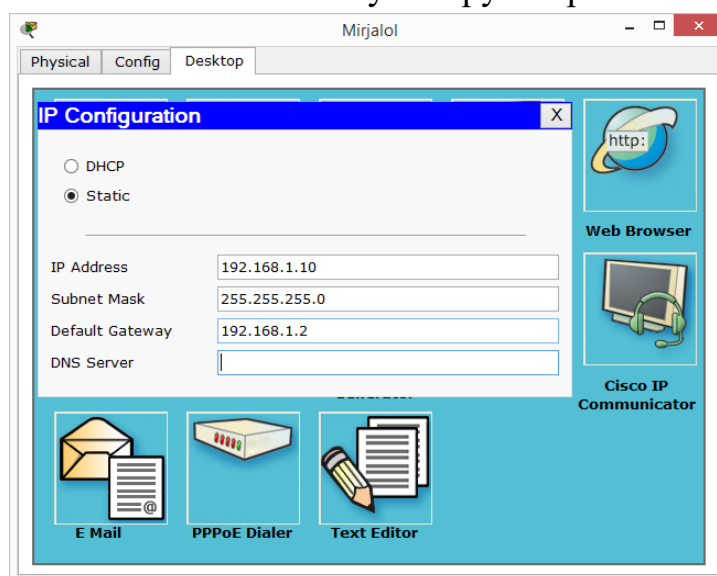
ADMIN(config-line)#tra
ADMIN(config-line)#transport input ssh
ADMIN(config-line)#exit
ADMIN(config)#username cisco pri
ADMIN(config)#username cisco privilege 15 pas
ADMIN(config)#username cisco privilege 15 password cisc
ADMIN(config)#username cisco privilege 15 password cisco123
ADMIN(config)#end

%SYS-5-CONFIG_I: Configured from console by console
ADMIN#wr
Building configuration...
[OK]
ADMIN#

```

13.10-rasm. Qurilma kodi

Endi IP-configuration bo‘limida shaxsiy kompyuter parametrlarini sozlaylik:



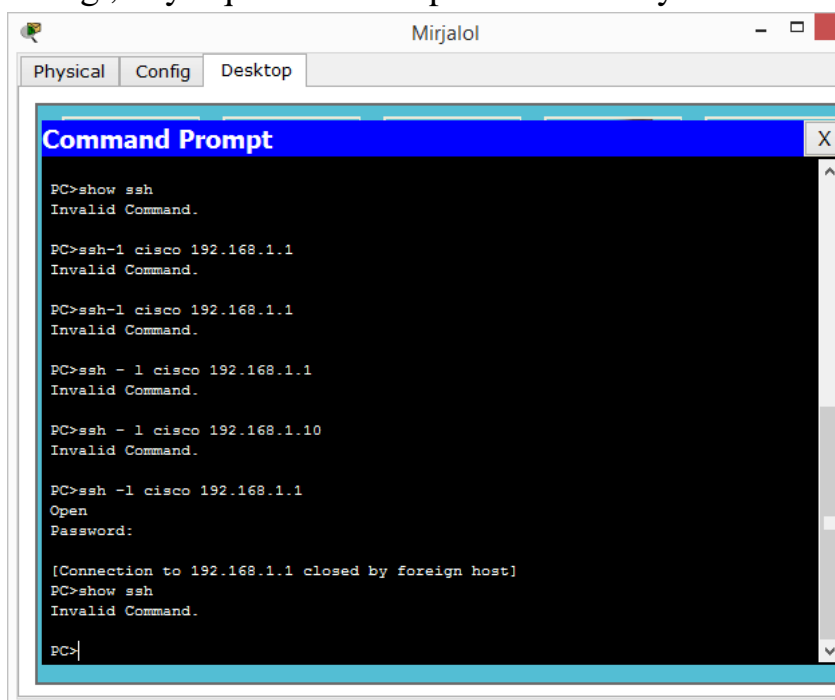
13.11-rasm. Manzillash

Ulanish uchun, kompyuterga buyruq satriga o`tib, quyidagilarni kiriting va Enter tugmasini bosing :

ssh -l cisco 192.168.1.1 -l – kirish (login) qiymati cisco – marshrutizatorga ulangan foydalanuvchi nomi .

192.168.1.1 - marshrutizatorning ip manzili.

Yaratilgan parolni kiriting va ulanish o`rnatiladi. **Show ssh** buyrug`i bajarilgandan so`ng , buyruq satrida SSH protokoli versiyasini tekshirish mumkin.

A screenshot of a Windows Command Prompt window titled "Mirjalol". The window has tabs for "Physical", "Config", and "Desktop". The Command Prompt shows the following sequence of commands and outputs:

```
PC>show ssh
Invalid Command.

PC>ssh-l cisco 192.168.1.1
Invalid Command.

PC>ssh-l cisco 192.168.1.1
Invalid Command.

PC>ssh - l cisco 192.168.1.1
Invalid Command.

PC>ssh - l cisco 192.168.1.10
Invalid Command.

PC>ssh -l cisco 192.168.1.1
Open
Password:

[Connection to 192.168.1.1 closed by foreign host]
PC>show ssh
Invalid Command.

PC>|
```

13.12-rasm. Testlash jarayoni

Amaliy ish bo'yicha topshiriqlar variantlari:

1. Lokal tarmoq loyihlashtiring hamda Telnet va SSH protokollari orqali aloqa o`rnating.
2. Tarmoqni testlab kuring va natijani tahlil qiling.
3. Bajarilgan ishlarni rasmlar va izohlar ko`rinishida hisobot shaklida topshiring.

Amaliy ish bo'yicha savollar:

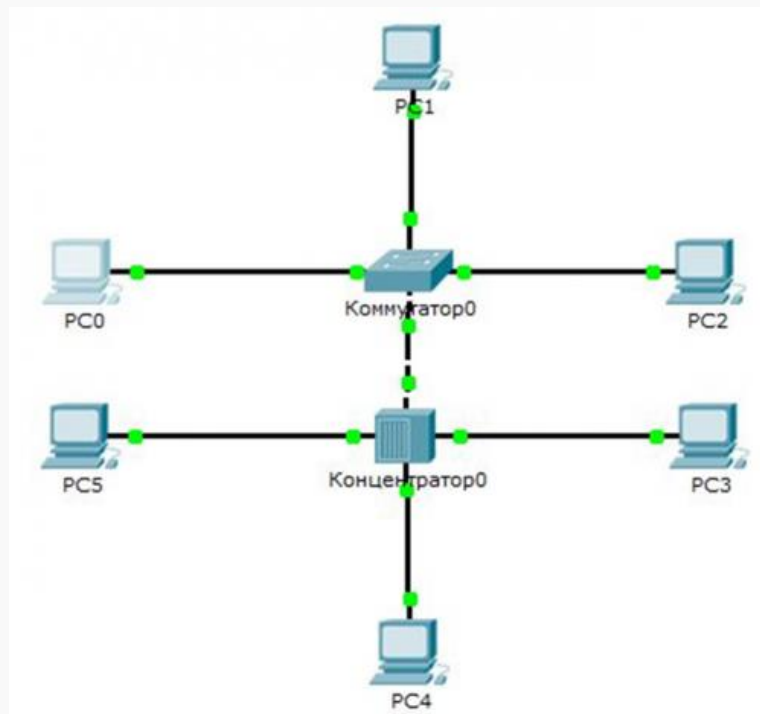
1. Telnet nima?
2. SSH nima?
3. Protokollarning qanday turlari bor?
4. Telnet va SSH protokollari nima vazofani bajaradi?

Amaliy ish № 14

KOMMUTATORNING PORT XAVFSIZLIK FUNKTSIYASINI O`RGANISH

Ishdan maqsad: Kommutatorning tarmoqni kommutatsiya jadvalini to'ldirishga qaratilgan hujumlardan himoya qilishga imkon beruvchi port-security funksiyasini o'rganish.

Cisco Packet Tracer-da lokal tarmoqni tashkil etish misoli keltirilgan. Tarmoq topologiyasi 14.1-rasmda keltirilgan. Quyida bosqichma-bosqich ko'rsatma berilgan.



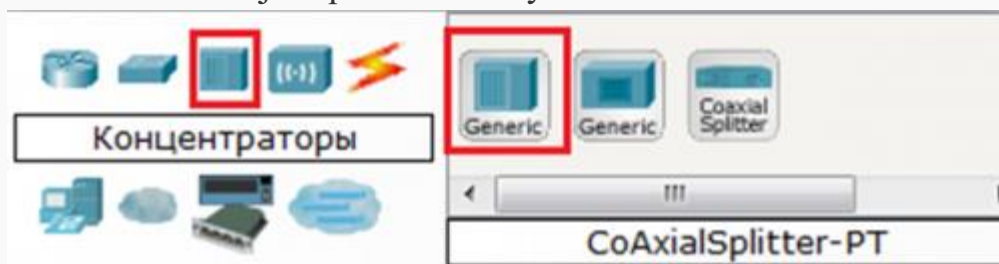
14.1-rasm - Tarmoq topologiyasi

Amalga oshiriladigan harakatlar ketma-ketligi:

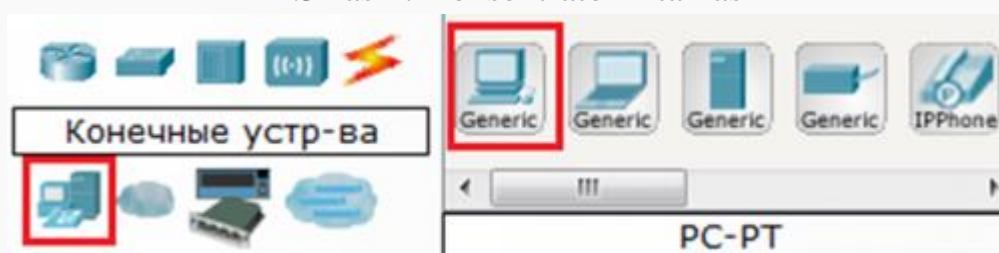
1. Packet Tracer-ning pastki chap burchagida "Сетевые коммутаторы" qurilmalarini tanlang va o'ng tomondagi ro'yxatda 2950-24 tugmachasini sichqonchani chap tugmasi bilan bosish orqali tanlang, uni ish joyiga qo'ying. 14.2-rasm, 14.3-rasm va 14.4-rasmga muvofiq biz tarmoq konsentratori (Hub-PT) va ish stantsiyalari (PC-PT) bilan ham shunday qilamiz.



14.2-rasm. Mavjud qurilmalar ro'yxatidan kommutatorni tanlash



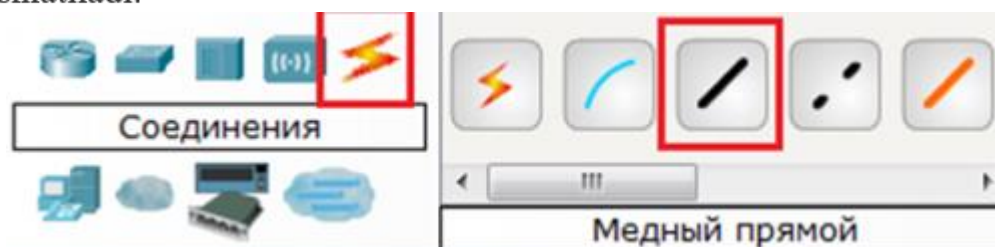
14.3-rasm. Konsentratorni tanlash



14.4-rasm. Kompyuterni tanlash

Kompyuterlarni, kommutatorlarni va konsentratorni ish joyiga joylashtirish 14.1-rasmda keltirilgan.

2. Keyinchalik, mos interfeyslardan foydalangan holda, 14.1-rasmda ko'rsatilgandek, qurilmalarni ulash kerak. 14.5-rasmga muvofiq "Copper straight-through", ya'ni "mis" kabellar kompyuterlarni kommutator va konsentratorga ulash uchun ishlatiladi.



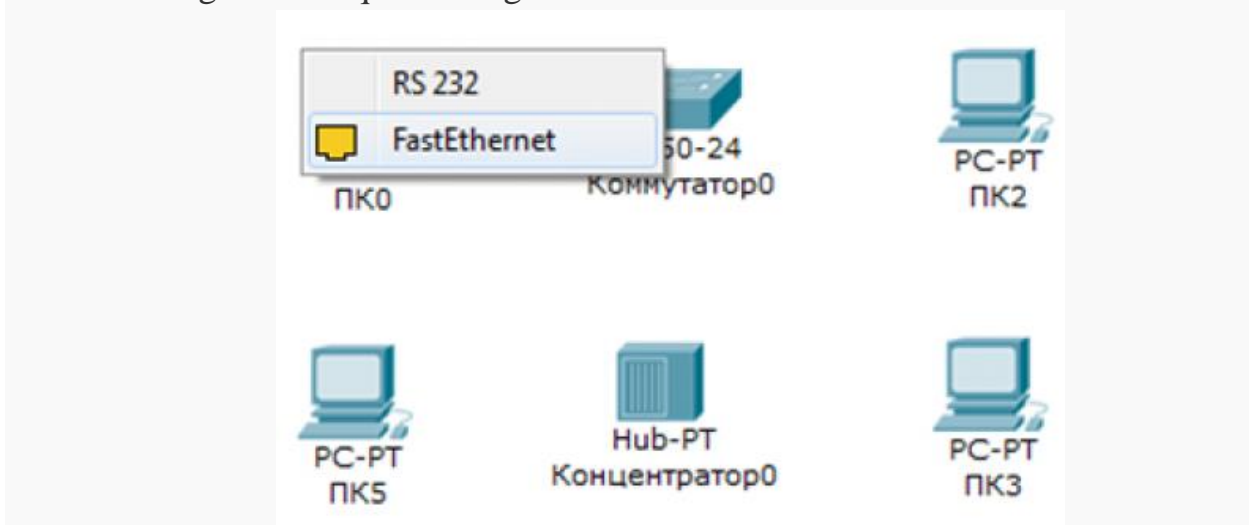
14.5-rasm. Mis kabelni tanlash

Kommutator va konsentratorni bir-biriga ulash uchun, 14.6-rasmda ko'rsatilgandek «copper cross-over» ya'ni mis o'tkazgich kabelidan foydalaniladi.

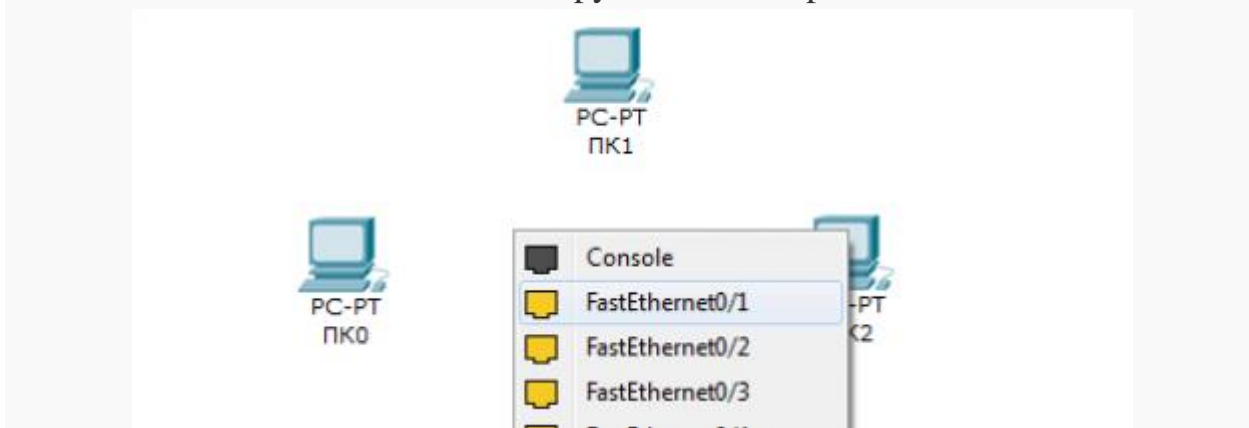


14.6-rasm. Krossover kabelini tanlash

Bundan tashqari, ikkita qurilmani ulash uchun mos keladigan kabel turini tanlash va bitta qurilmani (ixtiyoriy bo`sh FastEthernet portini tanlash) va boshqa qurilmani (shuningdek, ixtiyoriy bo`sh FastEthernet portini tanlash), 14.2, 14.3, 14.4-rasmlarga muvofiq bosishingiz kerak.



14.7-rasm. Kompyuterda bo`sh portni tanlash



14.8-rasm. Kommutatorda bo`sh portni tanlash

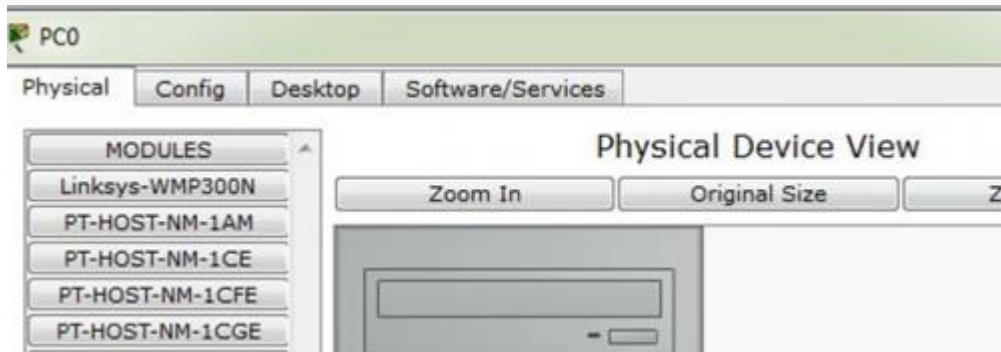


14.9-rasm. PC0 va kommutator0 to`g`ri mis kabel bilan ulash

Boshqa barcha qurilmalar uchun ulanish xuddi shu tarzda amalga oshiriladi. Kommutator va konsentrator o`rtasidagi aloqa crossover orqali amalga oshiriladi.

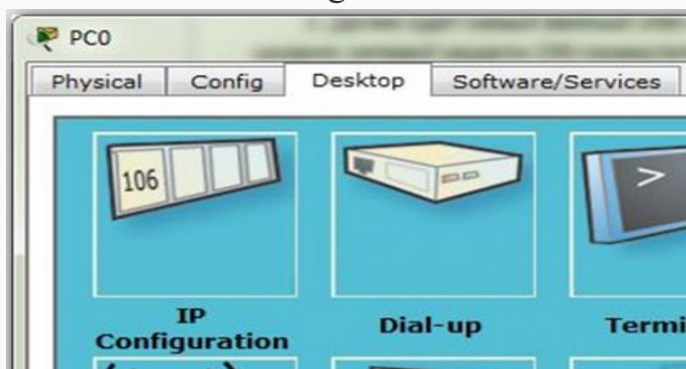
3. Keyingi eng muhim bosqich - sozlash hisoblanadi. OSI tarmog`i modelining dastlabki darajalarida ishlaydigan qurilmalarni ishlatayotganimiz sababli

(kommutator 2-daraja, konsentrator 1-daraja), ularni sozlashning hojati yo‘q. Faqatgina ish stantsiyalarini sozlash kerak, ya‘ni: IP-manzillar va pastki tarmoq maskalari. Quyida faqat bitta stantsiyani (PC0) sozlash keltirilgan, qolganlari xuddi shu tarzda amalga oshiriladi. Biz 14.7-rasmga muvofiq kerakli ish stantsiyasini ikki marta bosamiz.

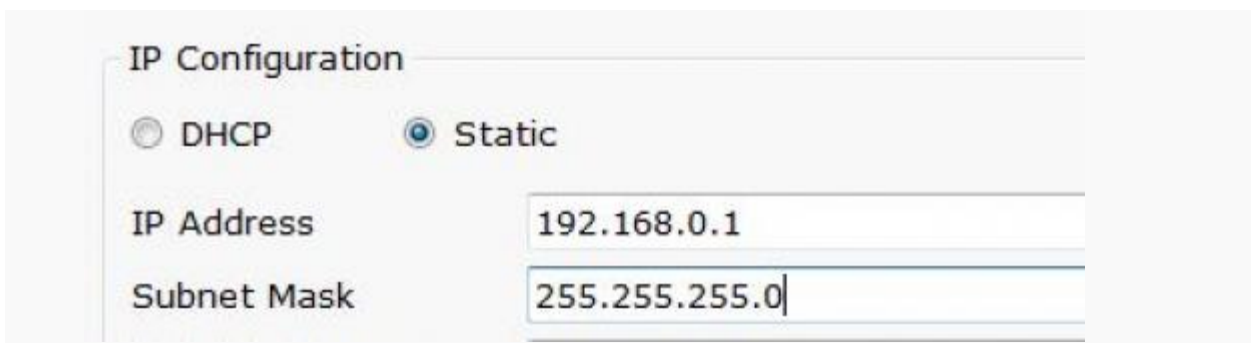


14.10-rasm. PC0 sozlash oynasi

Ochilgan oynada "desktop" yorlig‘ini tanlang, so‘ngra 14.11-rasmga muvofiq "IP konfiguratsiyasi" IP-manzilini o‘rnating.



14.11-rasm."Desktop" oynasi



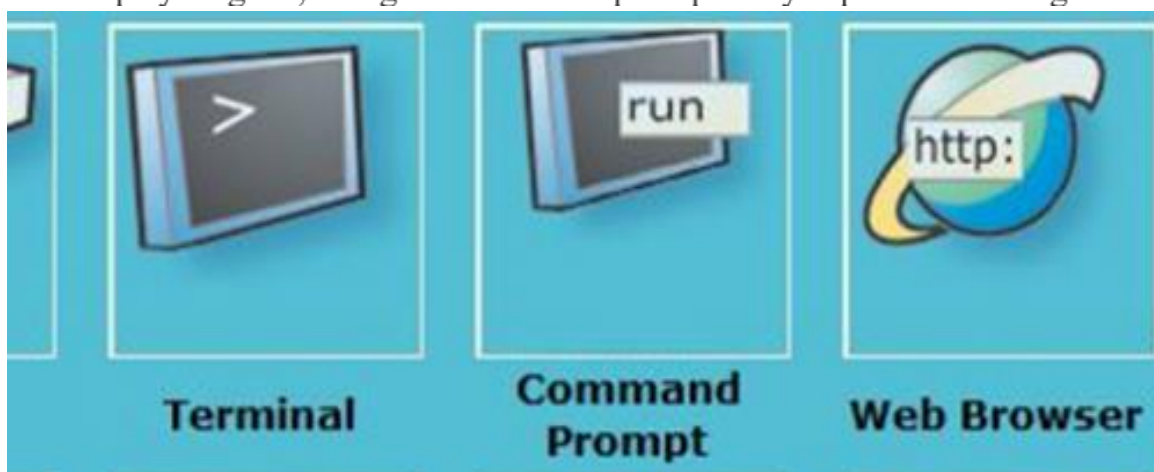
14.12-rasm - IP-manzilni tayinlash

Xuddi shunday, IP-manzillar boshqa barcha kompyuterlarga manzil jadvaliga muvofiq tayinlanadi.

Устройство	IP адрес	Маска подсети
PC0	192.168.0.1	255.255.255.0
PC1	192.168.0.2	255.255.255.0
PC2	192.168.0.3	255.255.255.0
PC3	192.168.0.4	255.255.255.0
PC4	192.168.0.5	255.255.255.0
PC5	192.168.0.6	255.255.255.0

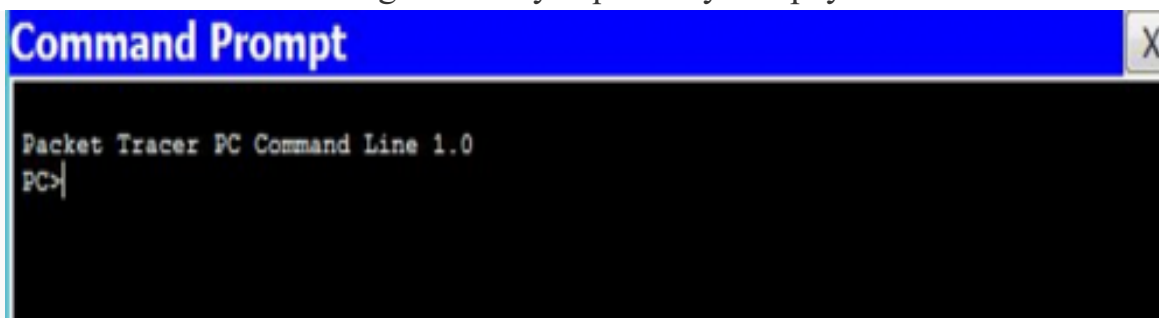
14.1-jadval. Adreslash jadvali

2. Sozlash tugagandan so'ng, ping jarayoni amalga oshiriladi. Masalan, u PC5 dan boshlanadi ya PC1 bilan aloqani tekshiradi, asosiysi, shart bajarilishi kerak: paketlar kommutator va konsentrator orqali uzatilishi kerak. Buning uchun kerakli ish stantsiyasini ikki marta bosing, ochilgan oynada 14.13-rasmga muvofiq "Desktop" yorlig'ini, so'ngra "Command prompt" buyruq satrini tanlang.



14.13-rasm - buyruq satri rejimini tanlash

14.14-rasmda ko'rsatilgandek buyruq satri oynasi paydo bo'ladi.



14.14-rasm. Buyruq satri oynasi

Buyruq satriga PC>ping 192.168.0.4 so'rovini kiritib, Enter bosamiz. Agar hamma sozlash to'g'ri bajarilgan bo'lsa, u holda 14.15-rasmda keltirilgan quyidagi axborot taqdim etiladi.

```

PC>ping 192.168.0.4

Pinging 192.168.0.4 with 32 bytes of data:

Reply from 192.168.0.4: bytes=32 time=1ms TTL=128
Reply from 192.168.0.4: bytes=32 time=0ms TTL=128
Reply from 192.168.0.4: bytes=32 time=0ms TTL=128
Reply from 192.168.0.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

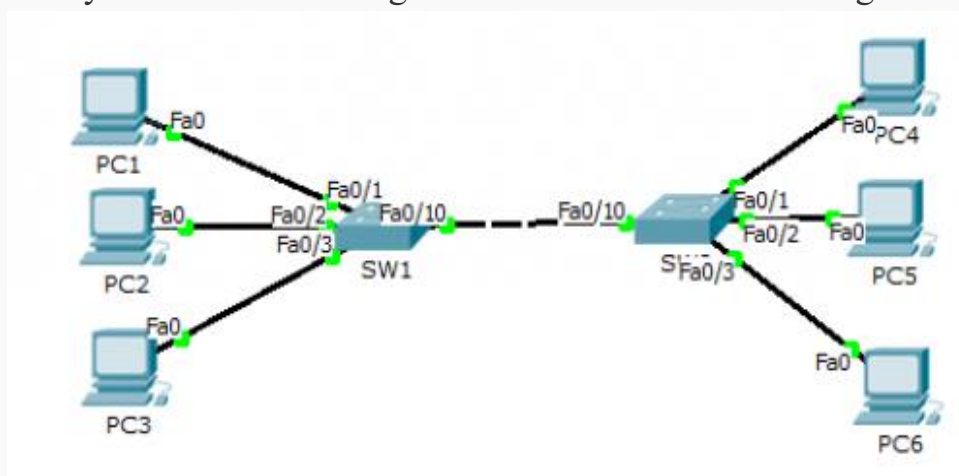
```

14.15-rasm. Ping utilitasining natijasi oynasi

Bu aloqa o`rnatilganligi va tarmoq ishlayotganini bildiradi.

Amaliy ishni bajarish tartibi

Berilgan topologiya bo`yicha Cisco Packet Tracerda tarmoq qurish talab etiladi. Tarmoq topologiyasidan so`ng jadvalda amaliy ish matnida aniq ko`rsatilganda foydalanish kerak bo`lgan manzillar sxemasi ko`rsatilgan.



14.16-rasm. Tarmoq topologiyasi

Qurilma	IP manzil	Tarmoqosti maska	Interfeys	Rejimlar (holatlar)
PC1	16.4.0.1	255.0.0.0	Fa0	n/a
PC2	16.4.0.2	255.0.0.0	Fa0	n/a
PC3	16.4.0.3	255.0.0.0	Fa0	n/a
PC4	16.4.0.4	255.0.0.0	Fa0	n/a
PC5	16.4.0.5	255.0.0.0	Fa0	n/a
PC6	16.4.0.6	255.0.0.0	Fa0	n/a
SW1	N/A	N/A	Fa0/1	Shutdown
SW1	N/A	N/A	Fa0/2	Restrict
SW1	N/A	N/A	Fa0/3	Protect
SW2	N/A	N/A	Fa0/1	Shutdown

SW2	N/A	N/A	Fa0/2	Restrict
SW2	N/A	N/A	Fa0/3	Protect

14.16 –rasm. Adreslash jadvali

Amalga oshirilgan harakatlar ketma-ketligi

1. SW1 va SW2-da portlarni kirish rejimiga o‘rnatish

```
Switch(config)#interface fastethernet0/10
Switch(config-if)#switchport mode access
```

⇨14.17-rasm - Portlarni kirish rejimiga o‘tkazish

2. Qurilmalar tomoniga qaragan SW1 va SW2 portlarida port xavfsizligini faollashtiring.

```
Switch(config-if)#switchport mode access
Switch(config-if)#
Switch(config-if)#switchport port-security
Switch(config-if)#
```

⇨14.18-rasm - Port xavfsizligini faollashtirish

3. Qurilmalar tomoniga qaragan SW1 va SW2 portlariga maksimal darajada secure-mac o‘rnatish.

```
Switch(config-if)#switchport port-security maximum 1
```

⇨14.19-rasm - xavfsiz mac-manzillar sonini belgilash

4. SW1-da secure-mac-ning dinamik ta’rifini o‘rnatish

```
Switch(config-if)#
Switch(config-if)#switchport port-security mac-address sticky
```

⇨14.20-rasm. sek-mac dinamik ta’rifini o‘rnatish

5. Fa0/1 SW1 portida va Fa0/1 SW2 portida sozlangan cheklovlar buzilgan holatdagi harakatni ko‘rsatish.

```
Switch(config-if)#
Switch(config-if)#switchport port-security violation shutdown
```

⇨14.21-rasm. Cheklovlar buzilgan taqdirda harakatlarni sozlash

Shutdown (O‘chirish) - xavfsizlikni buzish interfeysni error-disabled (xato o‘chirilgan) holatiga olib keladi va darhol o‘chadi va port LEDini o‘chiradi. Agar port error-disabled holatida bo‘lsa, uni ushbu holatdan chiqarish uchun errdisable recovery cause psecure-violation buyrug‘ini kiritish yoki interfeysni konfiguratsiya rejimida shutdown n no shutdown interfeysni yoqish orqali amalga oshirish mumkin. Bu standart rejim.

6. Fa0/2 SW1 portida va Fa0/2 SW2 portida sozlangan cheklovlar buzilgan taqdirda harakatni ko'rsating.

```
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#
```

14.22-rasm. Cheklovlar buzilgan taqdirda harakatlarni sozlash

Restrict (Cheklash) - xavfsiz MAC-manzillar soni portda sozlangan maksimal chegaraga yetganida, noma'lum manbali MAC-manzilga ega paketlar yetarli miqdordagi xavfsiz MAC-manzillar maksimal sonidan kam bo'lguncha yoki ruxsat berilgan manzillar ko'paytirilguncha olib tashlanadi. Ushbu rejimda, xavfsizlik buzilishi sodir bo'lganda ogohlantirish yuboriladi - SNMP trap, syslog xabari yuboriladi va qoidabuzarlik hisoblagichi (violation counter) oshiriladi

7. Fa0/3 SW1 portida va Fa0/3 SW2 portida sozlangan cheklovlar buzilgan taqdirda harakatni ko'rsating.

```
Switch(config-if)#
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#
```

14.23-rasm. Cheklovlar buzilgan taqdirda harakatlarni sozlash

Protect (Himoya qilish) - xavfsiz MAC-manzillar soni portda sozlangan maksimal chegaraga yetganda, noma'lum MAC-manzilga ega paketlar yetarli miqdordagi xavfsiz MAC-manzillar maksimal sondan kam bo'lmaguncha yoki ruxsat berilgan manzillar maksimal songa ko'paytirilguncha tashlab yuboriladi. Xavfsizlikni buzish to'g'risida ogohlantirish mavjud emas.

8. Natijani tekshiring

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/1    1          1          0          Shutdown
Fa0/2    1          1          0          Protect
Fa0/3    1          1          2          Restrict
-----
```

14.24-rasm - Show port-security buyrug'ining chiqarilishi

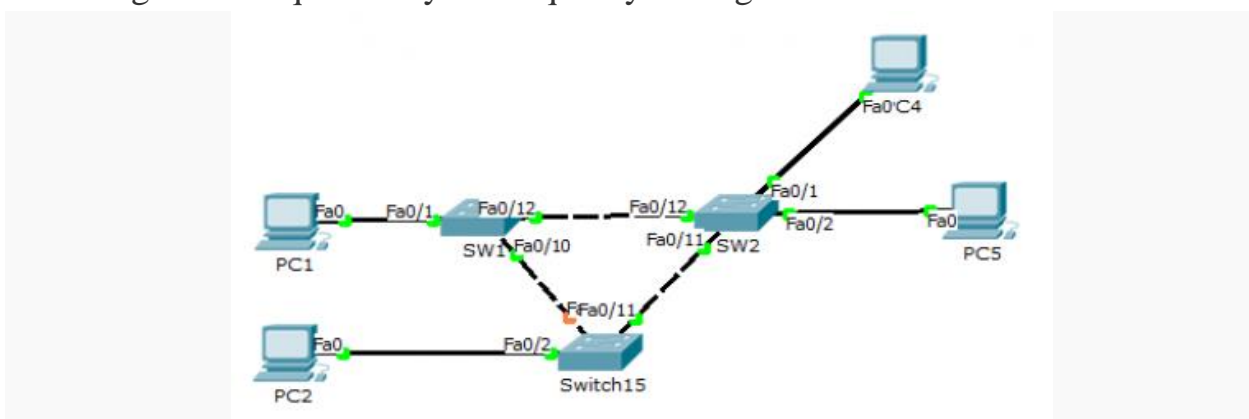
13.24-rasm asosida portlarning holatini ko'rishingiz mumkin. Fa0/1 -shutdown (o'chirish), Fa0/2 - protect (himoya qilish), Fa0/3 -restrict (cheklash). Security

Violation ustuni hisoblagich hisoblanadi. Ushbu ustundagi qiymat 2 ga teng, ya'ni xavfli mac-manzil orqali ulanishga urinish bo'lganida, u 2 marta ishlagan.

Amaliy ishlar natijasida port orqali ma'lumotlarni uzatish va tarmoqni kommutatsiya jadvalini to'ldirishga qaratilgan hujumlardan himoya qilish uchun ruxsat berilgan xostlarning MAC manzillarini belgilashga imkon beruvchi kommutatorning port – security funksiyasi ko'rib chiqildi.

Amaliy ish bo'yicha topshiriqlar variantlari:

1-Topshiriq. Kommutatorning port-xavfsizlik funksiyasini o'rganish. Ish talablariga muvofiq mahalliy tarmoqni loyihalang.



14.25 – rasm. Tarmoq topologiyasi

Qurilma	IP manzil	Tarmoqosti maska	Interfeys	Rejimlar (holatlar)
PC1	192.168.0.66	255.255.255.128	Fa0	n/a
PC2	192.168.0.67	255.255.255.128	Fa0	n/a
PC3	192.168.0.68	255.255.255.128	Fa0	n/a
PC4	192.168.0.69	255.255.255.128	Fa0	n/a
SW1	N/A	N/A	Fa0/1	Protect
SW2	N/A	N/A	Fa0/1	Shutdown
SW3	N/A	N/A	Fa0/2	Restrict
Switch15	N/A	N/A	Fa0/2	Shutdown

14.25-jadval. Adreslash jadvali

1. Fa0 / 1 - fa0 / 2 bilan barcha SW-larda portlarni kirish (access) rejimiga o'rnating.
2. Barcha SW portlarida qurilmalar tomonga qaragan holda port xavfsizligini faollashtiring.
3. Portlarda ikkiga teng bo'lgan maksimal secure-mac o'rnating.
4. Secure-mac ning dinamik ta'rifini o'rnating.

5. 14.25-jadvalga muvofiq sozlangan cheklovlar buzilgan taqdirda harakatni ko'rsating.

6. Natijani tekshiring. O'qituvchiga qilingan ish natijalarini ko'rsating va natijalarini asoslang.

Amaliy ish bo'yicha savollar:

1. Port xavfsizligi nima?
2. Xavfsiz mac-manzillar soni qanday belgilanadi?
3. Cheklovlar buzilgan taqdirda harakatlarni sozlash uchun qanday buyruqdan foydalaniladi?
4. Show port-security buyrug'idan foydalanganimizda qanday natija hosil bo'ladi?
5. Kommutatorning port – security funksiyasining asosiy maqsadi nima?

Amaliy ish № 15

POLIALIFBOLI SHIFRLASH USULLARINI TADQIQ QILISH

Ishning maqsadi : monoalifboli va polialifboli almashtirish shifrlarini tuzish tamoyillarini o'rganish. O'rnini bosuvchi shifrlarning xossalari o'rganish.

Nazariy qism

Monoalfavit almashtirish shifrlari sezilarli kamchilikka ega edi - ular chastotali kriptanalizga osonlikcha sezgir edi. Yana mustahkam shifrlash usullarini ishlab chiqish zarur. Shunday qilib, monoalfavitli shifrlar polialfavitli shifrlarga almashtirildi.

Vijener usuli polialfavit almashtirish shifrlaridan biridir. Kichik butun son m olinadi va har bir belgi almashtirishdan keyin alifbo m ta belgiga siljiydi.

Masalan, agar kalit *sichqoncha so'zi bo'lsa* (chap vertikal belgilar ustuniga qarang), u holda $m = 4$ va biz quyidagi jadvalni olamiz:

	абвгдеёжзийклмнопрстуфхцчшщъьыёюя
1	мнопрстуфхцчшщъьыёюяабвгдеёжзийкл
2	ьыёюяабвгдеёжзийклмнопрстуфхцчшщъ
3	шщъьыёюяабвгдеёжзийклмнопрстуфхцч
4	ёюяабвгдеёжзийклмнопрстуфхцчшщъы

Dastlabki matn m ta belgidan iborat guruhlariga bo'linadi (ko'rib chiqilayotgan holatda - 4). Har bir guruh uchun birinchi belgi birinchi alifbodagi tegishli harf bilan almashtiriladi, ikkinchisi - ikkinchisidan va hokazo. Masalan, "от улыбки каждый день светлей" iborasi quyidagicha o'zgartiriladi:

отул ыбки кажд ыйде ньсв етле й

Alifbo faqat harflar bilan cheklanmaydi, unga boshqa belgilar qo'shishingiz mumkin - bo'shliqlar, raqamlar, tinish belgilari. Ushbu o'zgartirish qabul qiluvchi tomonda dekodlashdan keyin matnni o'qishda noaniqlikdan qochish imkonini beradi (masalan, "bajarilmaydi" iborasiga vergul qo'yish muammosi).

Ishning borishi

O'qituvchingizdan individual topshiriq oling. Qabul qilingan topshiriqqa muvofiq dasturiy modulni amalga oshirish. Amalga oshirishda quyidagi fikrlarni hisobga olish kerak:

1) foydalanuvchiga har qanday tartibda joylashtirilgan har qanday belgilar to'plamidan iborat o'zining mutlaqo ixtiyoriy alifbosini belgilash imkoniyatini ta'minlash;

2) sinovdan o'tkazish va boshqa modullar bilan o'zaro ta'sir qilish qulayligi uchun manba ma'lumotlarini faylga kiritish va kriptografik konvertatsiya natijasini chiqarishni amalga oshirish.

Dasturiy ta'minot modulini amalga oshirgandan so'ng, kriptografik transformatsiyadan oldin va keyin matnning statistik tahlilini bajaring.

15-son amaliy ishga topshiriq:

- Familiyangiz, ismingiz va ota ismingizni shifrlash va shifrini ochish uchun Vigenère algoritmidan foydalanish;

- Gronsfeld algoritmidan foydalangan holda matnni shifrlash moduli, kalit so'z (10 belgigacha);

- O'zingizning konversiya algoritmingizni ishlab chiqing va familiyangiz, ismingiz va otangizning ismini shifrlash va parolini ochish;

Nazorat savollari:

1. O'rnini bosuvchi shifrlash nima?
2. Bitta belgidan iborat kalitdan foydalanganda Vigenere algoritmi qanday shifrnı amalga oshiradi?
3. Bir alfavit va polialfavıt almashtirish shifrlarining asosiy farqi nimada?
4. Besh belgidan iborat matnni oddiy almashtirishlar sonini hisoblang?
5. Polialfavıtli shifrlarga kriptozanalizning statistik usullarini qo'llash mumkinmi?

Amaliy ish № 16

O'RIN ALMASHTIRISH USULI BO'YICHA SHIFRLASH

Ishning maqsadi: O'rin almashtirish shifrlarini qurish tamoyillarini o'rganish. O'rin almashtirish shifrlarining xususiyatlarini o'rganish.

Nazariy qism

O'rin almashtirish usuli shundan iboratki, shifrlangan matnning belgilari shifrlangan blok ichidagi ma'lum qoidalarga muvofiq qayta tartibga solinadi, belgilarning o'zi esa o'zgarmaydi.

Eng oddiy almashtirish asl matni teskari yozish va shu bilan birga shifrnı beshta harfga ajratishdir. Masalan:

Boshlang'ich matn: пусть будет так, как мы хотели

tauyorlangan matn: пусть будет такка кмыхо тели

shifrlangan matn: илето хымка ккатт едубъ тсуп

Oxirgi guruhda (beshta) bitta harf etishmayapti. Bu shuni anglatadiki, asl iborani shifrlashdan oldin uni ahamiyatsiz harf bilan, masalan O, beshga karrali raqam bilan to'ldirish kerak:

пусть будет такка кмыхо телио

Keyin shifrlash quyidagicha ko'rinadi:

оилет охымк аккат тедубъ тсуп

Yana bir usul - asl matni bir necha qatorda yozish, masalan, har biri o'n besh harf (oxirgi qatorni ahamiyatsiz harflar bilan to'ldirish) bilan:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
п	у	с	т	ь	б	у	д	е	т	т	а	к	к	а
к	м	ы	х	о	т	е	л	и	к	л	м	н	о	п

Shundan so'ng, vertikal ustunlar besh harfga bo'lingan qatorga tartibda yoziladi:

пкумс ытхьо бтуед леитк тламк нкоап

Agar siz chiziqlarni qisqartirsangiz va qatorlar sonini ko'paytirsangiz, siz to'rtburchak - manba matni yozilgan panjara olasiz.

Misol:

1	2	3	4	5	6
п	у	с	т	ь	б
у	д	е	т	т	а
к	к	а	к	м	ы
х	о	т	е	л	и
а	б	в	г	д	е

М	Л	К	И	З	Ж
---	---	---	---	---	---

Yuqori chap burchakdan yuqoridan pastga diagonal ravishda shifrlasak, biz quyidagilarni olamiz:

УТЫ ЪКТ СТХ ТАО УАЛ ПЕМО ДКИ БКЕ

Ushbu shifrnin uchunchi turi: kalit bilan almashtirish. Siz kalitni bilishingiz kerak, masalan, "radiator". Alifbodagi harflarning joylashishiga ko'ra, A harfi 1 raqamini, ikkinchi harf A - 2, keyingi Д harfi - 3, keyin И - 4, О - 5, birinchi harf P - 6, ikkinchi P - 7 va T harfi - 8.

Natijada:

Р	А	Д	И	А	Т	О	Р
6	1	3	4	2	8	5	7
П	У	С	Т	Ь	Б	У	Д
Е	Т	Т	А	К	К	А	К
М	Ы	Х	О	Т	Е	Л	И
О							

Ustunlarni kalit harflarining raqamlariga mos ravishda yozib, biz quyidagilarni olamiz: uty ykt sth tao ual pemo dki bke

Oxirgi usulning modifikatsiyasi ikkita kalitdan foydalanishdir: biri ustunlarni almashtirish uchun, ikkinchisi esa satrlarni almashtirish uchun. Bu usul ikki marta almashtirish deb ataladi.

Boshqa almashtirish usuli - Cardano panjaralaridan foydalanish (kodi "Rotating lattice").

Ishning borishi

O'qituvchingizdan individual topshiriq oling. Qabul qilingan topshiriqqa muvofiq dasturiy modulni amalga oshirish. Amalga oshirishda quyidagi fikrlarni hisobga olish kerak:

- 1) foydalanuvchiga shifrlash parametrlarini belgilash imkoniyatini berish;
- 2) barcha foydalanuvchi sozlamalarini vizualizatsiya qilishni ta'minlash;
- 3) sinovdan o'tkazish va boshqa modullar bilan o'zaro ta'sir qilish qulayligi uchun manba ma'lumotlarini faylga kiritishni va kriptografik konvertatsiya natijasini chiqarishni amalga oshirish.

Dasturiy ta'minot modulini amalga oshirgandan so'ng, kriptografik transformatsiyadan oldin va keyin matnni bigramlar bo'yicha statistik tahlil qiling.

16-sonli amaliy ishga topshiriq:

- almashtirish usulidan foydalanib, familiyangizni, ismingizni va otangizning ismini shifrlash va parolini ochish;

- Ikki marta almashtirish algoritmidan foydalangan holda matnni ochish modulidan foydalanib, familiyangizni, ismingizni va otangizning ismini shifrlang va shifrlang;

Nazorat savollari:

1. O'zgartirish shifrlash nima?
2. Beshta belgidan iborat matnning mumkin bo'lgan oddiy almashtirishlar sonini hisoblang?
3. Almashtiruvchi shifrlar almashtiruvchi shifrlardan tubdan qanday farq qiladi?
4. O'rin almashish shifrlariga kriptanalizning statistik usullarini qo'llash mumkinmi?
5. Ikki marta almashtirish algoritmi yordamida matnni shifrlash modulining ishlash printsiipi.

Qisqartma soʻzlar

GNS - Graphical Network Simulator - Grafikli tarmoq simulyatori
LAN – (Local Area Network) – Mahalliy tarmoq
WAN (Wide Area Network) — Global tarmoq
MAN (Metropolitan Area Network) — Shahar darajasidagi tarmoq
MAC – (Media Access Control) - Media kirishni boshqarish
HTML – (HyperText Markup Language) - Gipermatnni murojaatlar tili
EVE-NG (Emulated Virtual Environment Next Generation) - kichik biznes va jismoniy shaxslar uchun mo'ljallangan yagona turdagi ko'p foydalanuvchili tarmoq simulyatori
OSI – (Open Systems Interconnection) - Ochiq tizimlarning o'zaro aloqasi
IoT – (Internet of Things) – Buyumalar Interneti
TELNET (Teletype Network) - tarmoq orqali matnli terminal interfeysini amalga oshirish uchun tarmoq protokoli
SSH – (Secure shell) - Himoya qobig'i
SCS (Structured Cabling System) - Strukturaviy kabel tizimi
PoE – (Power over Ethernet) - Ethernet orqali quvvatni uzatish
DHCP – (Dynamic Host Configuration Protocol) - Dinamik xost konfiguratsiya protokoli
API - Application Programming Interface) - Ilova dasturlash interfeysi
CSR – (Certificate Signing Request) - Sertifikatni imzolash so'rovi
CVSS – (Common Vulnerability Scoring System) - Umumiy zaifliklarni baholash tizimi
DDoS – (Denial-of-Service Attack) - Xizmatni rad etish hujumi
DDP – (Distributed Data Protocol) - Tarqatilgan ma'lumotlar protokoli
EDA – (Event-Driven Architecture) - Voqealarga asoslangan arxitektura
EDP – (Electronic Data Processing) - Elektron ma'lumotlarni qayta ishlash
EDR – (Endpoint Detection and Response) - Yakuniy nuqtani aniqlash va javob
ENISA – (European Union Agency for Cybersecurity) - Yevropa Ittifoqining kiberxavfsizlik agentligi
GDPR – (General Data Protection Regulation) - Umumiy ma'lumotlarni himoya qilish to'g'risidagi nizam
HIDS – (Host-based Intrusion Detection) - Xostga asoslangan hujumni aniqlash
HTTP – (HyperText Transfer Protocol) - Gipermatnni uzatish protokoli
IEC – (International Electrotechnical Commission) - Xalqaro elektrotexnika komissiyasi
IDS – (Intrusion Detection Systems) - Hujumlarni aniqlash tizimlari

ILM – (Information lifecycle management) - Axborotning hayot aylanishini boshqarish

IPS – (Intrusion Prevention System) - Hujumning oldini olish tizimi

ISM – (Information Security Manual) - Axborot xavfsizligi bo'yicha qo'llanma

ISO – (International Organization for Standardization) - Xalqaro standartlashtirish tashkiloti

NIDS – (Network Intrusion Detection System) - Tarmoqqa kirishni aniqlash tizimi

OWASP – (Open Web Application Security Project) - Veb ilovalar xavfsizligi loyihasini oching

RFID – (Radio-Frequency Identification) - Radiochastota identifikatsiyasi

SOA – (Service-Oriented Architecture) - Xizmatga yo'naltirilgan arxitektura

SQL – (Structured Query Language) - Strukturaviy so'rovlar tili

TLS – (Transport Layer Security) - Transport qatlami xavfsizligi

VLAN – (Virtual Local Area Network) - Virtual mahalliy tarmoq

VPN – (Virtual Private Network) - Virtual xususiy tarmoq

XSS – (Cross-Site Scripting) - Saytlararo skript yaratish

XULOSA

“Axborot tizimlarining ishonchliligi va xavfsizligi asoslari” nomli ushbu o‘quv qo‘llanma axborot tizimlari va texnologiyalari xavfsizligiga oid keng ko‘lamli mavzular bo‘yicha chuqur bilim manbai hisoblanadi. Qo‘llanmada talaba va mutaxassislariga tarmoq texnologiyalari, Cisco Packet Tracer, LAN, VLAN, VPN va bulutli tarmoq dizayni bo‘yicha asosiy tushuncha va ko‘nikmalarni samarali o‘zlashtirishga yordam beradigan qimmatli va amaliy yo‘naltirilgan materiallar mavjud.

O‘quv qo‘llanma talabalarga ishonchli va samarali tarmoq infratuzilmasini yaratishning asosiy elementi bo‘lgan tarmoq kabellarini o‘rnatish tamoyillari va usullarini to‘liq tushunish imkonini beradi. Cisco Packet Tracer dasturi tarmoqni modellashtirish va sozlash bo‘yicha noyob amaliy tajribani taqdim etadi, bu esa talabalarga tarmoq uskunalarining asosiy tamoyillarini o‘rganish imkonini beradi.

LAN, VLAN, VPN va bulutli tarmoqlarni loyihalash o‘quv jarayonining muhim qismidir, chunki u turli darajadagi murakkablikdagi tarmoq tuzilmalarini tashkil qilish tamoyillarini tushunishga yordam beradi. Qo‘llanmaning ushbu qismi talabalarga xavfsizlik va samaradorlikni hisobga olgan holda zamonaviy tarmoq arxitekturasini loyihalash va joriy etish haqida to‘liq tushuncha beradi.

Bundan tashqari, o‘quv qo‘llanma zamonaviy tarmoq infratuzilmasining muhim elementlari bo‘lgan PoE texnologiyasi va DHCP serverlaridan foydalanishni o‘rgatadi. Zamonaviy sensorlar asosida IoT tarmoqlarini rivojlantirish qonun va tartib sohasida tobora dolzarb va istiqbolli yo‘nalishga aylanib bormoqda.

Umuman olganda, Axborot tizimlarining ishonchliligi va xavfsizligi asoslari tarmoq va axborot tizimlarini muhofaza qilishga qiziqqan va bu sohada martaba ko‘tarilishni istagan har bir kishi uchun bebaho manbadir. Tarmoq texnologiyalari bo‘limi talabalarga qonun va tartibni saqlash sohasida zamonaviy tarmoq texnologiyalarini muvaffaqiyatli rivojlantirish va qo‘llash uchun barcha zarur vositalar va bilimlarni beradi.

ADABIYOTLAR RO‘YXATI

1. Matt Oswalt, Christian Adell, Scott S. Lowe, and Jason Edelman. Network Programmability and Automation Skills for the Next-Generation Network Engineer. O'Reilly Media, Inc., CA. – 2023. 828 p.
2. Моделирование систем безопасности : монография / М75 [В. И. Новосельцев, А. В. Душкин, В. И. Сумин, С. С. Кочедыков, Д. Е. Орлова] ; ФКОУ ВО Воронежский институт ФЦИН России. - Воронеж, 2019. - 197 с.
3. Simone Onofri, Donato Onofri. Attacking and Exploiting Modern Web Applications. Packt Publishing Ltd. Birmingham, UK. August 2023. – 338 p.
4. Левашов Петр. Киберкрепость: всестороннее руководство по компьютерной безопасности. - СПб.: Питер, 2024. - 544 с.
5. Austin R. Benson, Rediet Abebe, Michael T. Schaub, AliJadbabaie, and Jon Kleinberg. Simplicial closure and higher-order link prediction. ArXiv Preprint ArXiv:1802.06916, 2018.
6. Harper A., Harris S., Ness J., Eagle C. et al. Gray Hat Hacking: The Ethical Hacker's Handbook. - McGraw Hill, 2018.
7. Bishop M. Computer Security: Art and Science. - Addison-Wesley Professional, 2018.
8. Christopher Cowell, Nicholas Lotz, Chris Timberlake. Automating DevOps with GitLab CI/CD Pipelines. Packt Publishing Ltd. Birmingham, UK. 2023. -348 p.
9. Чекулаева, Е. Н. Основные средства защиты информационной безопасности в организации / Е. Н. Чекулаева // Сборник статей Международного научно-методического конкурса. -Петрозаводск: Новая наука, 2019. - 181 с.
10. Ashish Mishra. Cloud security handbook for architects. Orange Education Pvt Ltd, Delhi, India. 2023. -394 p.
11. Масалков А. С. Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.
12. John Paul Mueller. Machine Learning Security Principles. Packt Publishing Ltd. Birmingham, UK. 2022. -451 p.
13. Mark Ciampa. CompTIA Security+ Guide to Network Security Fundamentals, Seventh Edition Boston, USA. 2020. – 580 p.
14. Chen Chen, Ruiyue Peng, Lei Ying, and Hanghang Tong. Network connectivity optimization: Fundamental limits and effective algorithms. Proc. of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 1167–1176, 2018.
15. Chen Chen and Hanghang Tong. On the eigen-functions of dynamic graphs: Fast tracking and attribution algorithms. Statistical Analysis and Data Mining: The ASA Data Science Journal, 10(2):121–135, 2017.

16. Marshall Copeland, Matthew Jacobs. Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security. Apress Berkeley, CA. – 2021. - 285p.
17. Управление информационной безопасностью: учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. – Йошкар-Ола: Поволжский государственный технологический университет, 2020. – 154 с.
18. Jacob G. Oakley. Professional Red Teaming: Conducting Successful Cybersecurity Engagements. Apress Berkeley, CA. – 2019. -215p.
19. Ajay Singh Chauhan. Practical Network Scanning. Packt Publishing Ltd. Birmingham, UK. 2023. -348 p.
20. Ranran Bian, Yun Sing Koh, Gillian Dobbie, and Anna Divoli. Network embedding and change modeling in dynamic heterogeneous networks. Proc. Of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval, pages 861– 864, 2019.
21. Aleksandar Bojchevski and Stephan Günnemann. Adversarial attacks on node embeddings via graph poisoning. International Conference on Machine Learning, pages 695–704, PMLR, 2019.
22. Stephen Bonner, John Brennan, Ibad Kureshi, Georgios Theodoropoulos, Andrew Stephen McGough, and Boguslaw Obara. Temporal graph offset reconstruction: Towards temporally robust graph representation learning. IEEE International Conference on Big Data (Big Data), pages 3737–3746, 2018.
23. Daniel Zügner, Amir Akbarnejad, and Stephan Günnemann. Adversarial attacks on neural networks for graph data. Proc. of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 2847–2856, 2018.
24. José Manuel Ortega. Python for Security and Networking Third Edition. Packt Publishing. Birmingham, UK. 2023. -587 p.
25. Безопасность веб-приложений: лучшие практики и уязвимости. Октября 2023. URL: <https://itproger.com/news/bezopasnost-veb-prilozheniy-luchshie-praktiki-i-uyazvimosti>.
26. В.Олифер, Н.Олифер. Компьютерные сети. Принципы, технологии, протоколы. Учебник для ВУЗов., -СПб.: Питер, 2016. -992 с.
27. CISCO: “Cisco Visual Networking Index: Forecast and Methodology, 2009–2014,” Cisco Systems Inc., June 2010.
28. John Yani Arrasjid, Chris McCain, and Mark Gabryjelski. IT Architect Series: Foundation In the Art of Infrastructure Design: A Practical Guide for IT Architects. IT Architect Resource, LLC. 2017.
29. Kevin Clark, Peter Bradley. Computer Programming and Cybersecurity for Beginners: All You Need to Know to Get Started with Python for Data Science, Excel and Ethical Hacking. Kevin Clark Audio. 2022.
30. Джеймс Лэнс. Фишинг. Техника компьютерных преступлений. Издательство АСТ. Москва, РФ. 2008 г. 320 с.

31. Shashank Mohan Jain. A Brief Introduction to Web3: Decentralized Web Fundamentals for App Development 1st ed. Edition. Apress Berkeley, CA. - 2022. -200p.
32. Easttom C. Computer Security Fundamentals. - Pearson IT Certification, 2019.
33. Harper A., Harris S., Ness J., Eagle C. et al. Gray Hat Hacking: The Ethical Hacker's Handbook. - McGraw Hill, 2018.
34. Stuttard D., Burnett M. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws. - Spring, 2019.
35. Stamp M. Computer Security and Cryptography. - Wiley, 2021.
36. Stanislav M. Networks and Network Security.
37. Goodrich M. T., Tamassia R. Introduction to Computer Security. - Pearson, 2010.
38. Д.П.Зегжда, Е.Б.Александрова и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия –Телеком, 2020. -560 с.
39. Scardapane S. et al. Microphone array based classification for security monitoring in unstructured environments // AEU - International Journal of Electronics and Communications. -2015, -Vol. 68. –Xe 11. -P. 1715-1723.
40. Mohapatra S. K., Sahoo P. K., Wu S-L. Big data analytic architecture for intruder detection in heterogeneous wireless sensor networks // Journal of Network and Computer Applications. -2016. - Vol. 66. – P. 236-249.
41. Das S. K., Kant K., Zhang N. Handbook on Securing Cyber-Physical Critical Infrastructure. - Morgan Kaufmann, 2012.
- Heartin Kanikathottu. AWS Security Cookbook. Packt Publishing Ltd. Birmingham, UK. 2020. -434p.

MUNDARIJA

Kirish.....	3
1-amaliy ish. TARMOQ SIMULYATORLARI BILAN TANISHISH. TARMOQ SIMULYATORLARI HAQIDA UMUMIY TUSHUNCHALAR, ULARNING IMKONIYATLARINI O'RGANISH. CISCO PACKET TRACERNI O'RNATISH.....	4
2-amaliy ish. CISCO KOMMUTATORLARI BUYRUQ INTERFEYSI BILAN ISHLASH VA BOSHLANG'ICH KONFIGURATSIYANI SOZLASH. CISCO PACKET TRACERDA LAN TARMOQINI LOYIHALASH VA QURISH.....	10
3-amaliy ish. TELNET, SSH PROTOKOLLARINI O'RGANISH. CISCO PACKET TRACERDA TELNET VA SSH PROTOKOLLARI YORDAMIDA QURILMALARNI SOZLASH.....	18
4-amaliy ish. CISCO ROUTERLARINING BUYRUQ INTERFEYSI BILAN ISHLASH VA DASTLABKI KONFIGURATSIYANI SOZLASH. CISCO PACKET TRACERDA VLAN TARMOG'INI LOYIHALASH VA QURISH.....	28
5-amaliy ish. KORXONA VA TASHKIOTLARNING KOMPYUTER TARMOG'INI LOYIHALASH.....	35
6-amaliy ish. VPN TUNNELLARI ORQALI KORXONA KORPORATIV TARMOQLARINI INTERNET ORQALI ULASH VA MOBIL QURILMALAR YORDAMIDA TARMOQQA MASOFADAN ULANISH IMKONIYATINI YARATISH.....	42
7-amaliy ish. BULUTLI TEXNOLOGIYA YORDAMIDA ZAHIRA MA'LUMOTLAR BAZALARI VA TIZIMINI YARATISH.....	47
8-amaliy ish. PoE TEXNOLOGIYASIDAN FOYDALANISH.....	60
9-amaliy ish. TARMOQDAGI TRAFIK OQIMINI BOSHQARISH.....	69
10-amaliy ish. CISCO PACKET TRACER DASTURIDA STATIK MARSHRUTLASHNI SOZLASH.....	76
11-amaliy ish. CISCO PACKET TRACER DASTURIDA DINAMIK MARSHRUTLASHNI SOZLASH.....	95
12-amaliy ish. CISCO PACKET TRACER DASTURIDA DHCP SERVERINI SOZLASH	108
13-amaliy ish. CISCO PACKET TRACER DASTURIDA TELNET VA SSH PROTOKOLI BILAN ISHLASH.....	116
14-amaliy ish. KOMMUTATORNING PORT XAVFSIZLIK FUNKTSIYASINI O'RGANISH.....	124

15-amaliy ish. POLIALIFBOLI SHIFRLASH USULLARINI TADQIQ QILISH.....	134
16-amaliy ish. O'RIN ALMASHTIRISH USULI BO'YICHA SHIFRLASH Qisqartma so'zlar	136
Xulosa.....	139
Foydalanilgan adabiyotlar ro'yxati.....	141
	142

ОГЛАВЛЕНИЕ

Введение	3
1-практическое задание. Ознакомление с сетевыми симуляторами. Общие понятия о сетевых симуляторах, изучение их возможностей. Установка Cisco Packet Tracer.....	4
2-практическое задание. Работа с командным интерфейсом коммутаторов Cisco и настройка начальной конфигурации. Проектирование и создание локальной сети (LAN) в Cisco Packet Tracer.....	10
3-практическое задание. Изучение протоколов TELNET и SSH. Настройка устройств с использованием протоколов TELNET и SSH в Cisco Packet Tracer.....	18
4-практическое задание. Работа с командным интерфейсом маршрутизаторов Cisco и настройка начальной конфигурации. Проектирование и создание VLAN-сети в Cisco Packet Tracer.....	28
5-практическое задание. Проектирование компьютерных сетей для предприятий и организаций.....	35
6-практическое задание. Подключение корпоративных сетей предприятия через VPN-туннели через интернет и создание возможности удаленного подключения к сети с помощью мобильных устройств.....	42
7-практическое задание. Создание резервных баз данных и систем с помощью облачных технологий.....	47
8-практическое задание. Использование технологии Power over Ethernet (PoE).....	60
9-практическое задание. Управление трафиком в сети.....	69
10-практическое задание. Настройка статической маршрутизации в программе Cisco Packet Tracer.....	76
11-практическое задание. Настройка динамической маршрутизации в программе Cisco Packet Tracer.....	95
12-практическое задание. Настройка DHCP сервера в Cisco Packet Tracer	108

13-практическое задание. Настройка DHCP-сервера в программе Cisco Packet Tracer.....	116
14-практическое задание. Изучение функции безопасности портов коммутатора в Cisco Packet Tracer.	124
15-практическое задание. Исследование методов полиалфавитного шифрования.	134
16-практическое задание. Шифрование с использованием метода замены символов.....	136
Список условных сокращений	139
Заключение	141
Список использованной литературы.....	142

TABLE OF CONTENTS

Introduction.....	3
1-practical work. Introduction to network simulators. General concepts about network simulators, studying their capabilities. Installing Cisco Packet Tracer.....	4
2-practical work. Working with the command interface of Cisco switches and setting up the initial configuration. Designing and creating a local area network (LAN) in Cisco Packet Tracer.....	10
3-practical work. Studying the TELNET and SSH protocols. Configuring devices using the TELNET and SSH protocols in Cisco Packet Tracer.....	18
4-practical work. Working with the command interface of Cisco routers and setting up the initial configuration. Designing and creating a VLAN network in Cisco Packet Tracer.....	28
5-practical work. Designing computer networks for enterprises and organizations.....	35
6-practical work. Connecting corporate networks of the enterprise via VPN tunnels over the Internet and creating the ability to connect remotely to the network using mobile devices.....	42
7-practical work. Creating backup databases and systems using cloud technologies.....	47
8-practical work. Using Power over Ethernet (PoE) technology.....	60
9-practical work. Managing network traffic.....	69
10-practical work. Configuring static routing in Cisco Packet Tracer.....	76
	148

11-practical work. Configuring dynamic routing in Cisco Packet Tracer.....	95
12-practical work. Configuring a DHCP Server in Cisco Packet Tracer	108
13-practical work. Configuring a DHCP Server in Cisco Packet Tracer.....	116
14-practical work. Studying the switch port security function in Cisco Packet Tracer.	124
15-practical work. Studying polyalphabetic encryption methods.....	134
16-practical work. Encryption using the symbol substitution method.....	136
List of abbreviations	139
Conclusion	141
List of used literature.....	142

Bozorov Elmurod Ostanovich
Ismailov Mirvali Mirxalilovich
Abdullayev Mirshod Shuxratovich

AXBOROT TIZIMLARINING ISHONCHLIGI VA XAVFSIZLIGI ASOSLARI

O'quv qo'llanma

Muharrir:

Tuzatuvchi:
