

MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI
FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

“AL-FARG‘ONIIY AVLODLARI”

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI



3-SON 1(3)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON



O'ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
FARG'ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali.

Chop etish tili: O'zbek, ingliz, rus. Jurnal texnika fanlariga ixtisoslashgan bo'lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo'nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.

Язык издания: узбекский, английский, русский.

Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.

Language of publication: Uzbek, English, Russian.

The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №3
Vol.1, Iss.3, 2023 y

ELEKTRON ILMIY JURNALI

ELECTRONIC SCIENTIFIC JOURNAL

«Al-Farg'oniylar avlodlari» («The descendants of al-Fargani», «Potomki al-Fargani») O'zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro'yxatdan o'tgan.

Tahririyat manzili:

151100, Farg'ona sh., Aeroport ko'chasi 17-uy, 201A-xona

Tel: (+99899) 998-01-42

e-mail: info@al-fargoniy.uz

Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG'ONA - 2023 YIL

TAHRIR HAY'ATI

Maxkamov Baxtiyor Shuxratovich,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti rektori, iqtisodiyot fanlari doktori, professor

Muxtarov Farrux Muhammadovich,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali direktori, texnika fanlari doktori

Arjannikov Andrey Vasilevich,
Rossiya Federatsiyasi Sibir davlat universiteti professori, fizika-matematika fanlari doktori

Satibayev Abdugani Djunosovich,
Qirg'iziston Respublikasi, Osh texnologiyalari universiteti, fizika-matematika fanlari doktori, professor

Rasulov Akbarali Maxamatovich,
Axborot texnologiyalari kafedrasida professori, fizika-matematika fanlari doktori

Yakubov Maksadxon Sultaniyazovich,
TATU «Axborot texnologiyalari» kafedrasida professori, t.f.d., professor, xalqaro axborotlashtirish fanlari Akademiyasi akademigi

Bo'taboyev Muhammadjon To'ychiyevich,
Farg'ona politexnika instituti, Iqtisod fanlari doktori, professor

Abdullayev Abdujabbor,
Andijon mashinosozlik instituti, Iqtisod fanlari doktori, professor

Qo'ldashev Abbasjon Hakimovich,
O'zbekiston milliy universiteti huzuridagi Yarimo'tkazgichlar fizikasi va mikroelektronika ilmiy-tadqiqot instituti, texnika fanlari doktori, professor

Ergashev Sirojiddin Fayazovich,
Farg'ona politexnika instituti, elektronika va asbobsozlik kafedrasida professori, texnika fanlari doktori, professor

Qoraboyev Muhammadjon Qoraboevich,
Toshkent tibbiyot akademiyasi Farg'ona filiali fizika matematika fanlari doktori, professor, BMT ning maslahatchisi maqomidagi xalqaro axborotlashtirish akademiyasi akademigi

Naymanboyev Raxmonali,
TATU FF Telekommunikatsiya kafedrasida faxriy dotsenti

Polvonov Baxtiyor Zaylobiddinovich,
TATU FF Ilmiy ishlar va innovatsiyalar bo'yicha direktor o'rinbosari

Zulunov Ravshanbek Mamatovich,
TATU FF «Dasturiy injiniringi» kafedrasida dotsenti, fizika-matematika fanlari nomzodi

Saliyev Nabijon,
O'zbekiston jismoniy tarbiya va sport universiteti Farg'ona

filiali dotsenti

G'ulomov Sherzod Rajaboyevich,
TATU Kiberxavfsizlik fakulteti dekani, Ph.D., dotsent

G'aniyev Abdusalil Abduljalilovich,
TATU Kiberxavfsizlik fakulteti, Axborot xavfsizligi kafedrasida t.f.n., dotsent

Zaynidinov Hakimjon Nasritdinovich,
TATU Kompyuter injiniringi fakulteti, Sun'iy intellect kafedrasida texnika fanlari doktori, professor

Abdullaev Temurbek Marufovich,
TATU Farg'ona filiali direktorining o'quv ishlari bo'yicha o'rinbosari, texnika fanlar bo'yicha falsafa doktori

Zokirov Sanjar Ikromjon o'g'li,
Ilmiy tadqiqotlar, innovatsiyalar va ilmiy pedagogik kadrlarni tayyorlash bo'limi boshlig'i, fizika-matematika fanlari bo'yicha falsafa doktori

Otakulov Oybek Hamdamovich,
fakultet dekani, texnika fanlar nomzodi, dotsent

Daliyev Baxtiyor Sirojiddinovich,
fakultet dekani, fizika-matematika fanlari bo'yicha falsafa doktori

Teshaboev Muhiddin Ma'rufovich,
Ta'lim sifatini nazorat qilish bo'limi boshlig'i, falsafa fanlari bo'yicha falsafa doktori

Bilolov Inomjon O'ktamovich,
pedagogika fanlar nomzodi

Ibroximov Nodirbek Ikromjonovich,
kafedra mudiri, fizika-matematika fanlari bo'yicha falsafa doktori

Kochkorova Gulnora Dexkanbaevna,
kafedra mudiri, falsafa fanlari nomzodi

Kadirov Abdumalik Matkarimovich,
falsafa fanlar bo'yicha falsafa doktori

Nurdinova Raziya Abdixalikovna,
kafedra mudiri, texnika fanlari bo'yicha falsafa doktori, dotsent

Obidova Gulmira Kuziboyevna,
kafedra mudiri, falsafa fanlari doktori

Rayimjonova Odinaxon Sodiqovna,
kafedra mudiri, texnika fanlari bo'yicha falsafa doktori, dotsent

Sabirov Salim Satiyevich,
Kafedra mudiri, fizika-matematika fanlari nomzodi, dotsent

To'xtasinov Dadaxon Farxodovich,
Kafedra mudiri, pedagogika fanlari bo'yicha falsafa doktori

Jurnal quyidagi bazalarda indekslanadi:



MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

F.Muxtarov, XAVF-XATARLARNI KELITIRIB CHIQARUVCHI OMILLAR, XAVF-XATARLARNI ANIQLASH USULLARI, MUAMMO VA YECHIM	5-9
Б.З.Полвонов, А.Ш.Уринбоев, СПЕЦИФИКА ЛЮМИНЕСЦЕНЦИИ ПОЛЯРИТОНОВ В ПОЛУПРОВОДНИКОВЫХ СТРУКТУРАХ НА ОСНОВЕ ХАЛЬКОГЕНИДОВ КАДМИЯ	10-17
Р.М.Зулунов, Б.Н.Солиев, ИСПОЛЬЗОВАНИЕ PYTHON ДЛЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ	18-24
D.X.Tojimatov, CISCO PACKET TRACER YORDAMIDA HUSUSIY KORXONALAR UCHUN MAXSUS HIMOYALANGAN TARMOQ KANALI ISHINI LOYIHALASH	25-32
А.Ж.Махмудова, Ш.М.Тошпулатов, Ф.М.Тошпулатова, МАТРИЧНЫЙ ФОТОПРИЁМНИК ИНФРАКРАСНОГО ИЗЛУЧЕНИЯ ДЛЯ ИЗМЕРЕНИЯ ЛЕЙКОЗА	33-37
B.M.Polvonova, SO'Z QO'SHILMALARIDA VARIANTLILIK	38-41
I.I.Bakhoviddinov, SUSTAINABLE DEVELOPMENT IN THE DIGITAL ECONOMY: BALANCING GROWTH AND ENVIRONMENTAL CONCERNS	42-50
S.I.Abdurakhmonov, Sh.M.Ibragimov, USING VISUAL LEARNING ENVIRONMENTS IN TEACHING OBJECT-ORIENTED PROGRAMMING	51-55

UO‘K 004.056

CISCO PACKET TRACER YORDAMIDA HUSUSIY KORXONALAR UCHUN MAXSUS HIMOYALANGAN TARMOQ KANALI ISHINI LOYIHALASH

D.X.Tojimatov,
TATU Farg‘ona filiali katta o‘qituvchisi

Annotatsiya. Ushbu maqola amaliy ahamiyatga ega bo‘lib, maqolada cisco packet tracer yordamida hususiy korxonalar uchun maxsus himoyalangan tarmoq kanali ishi loyihalash bosqichma bosqich ko‘rsatib o‘tilgan. Hususiy korxonalar va ularni hududiy filiallarini maxsus himoyalangan kanal orqali ma‘lumotlar uzatishni ta‘minlash maqsadida mahsus tarmoq qurishda foydalaniladigan qurilmalar va ularni xavfsizlik parametrlarini sozlash batafsil tushuntirib o‘tilgan. Natijada amaliy ahamiyatga ega mahsus tarmoq loyihasi bajarilishiga erishilgan.

Kalit so‘zlar: cisco packet tracer, kanal, Lan, UTP, MAN, ASA, server, router, switch, Host.

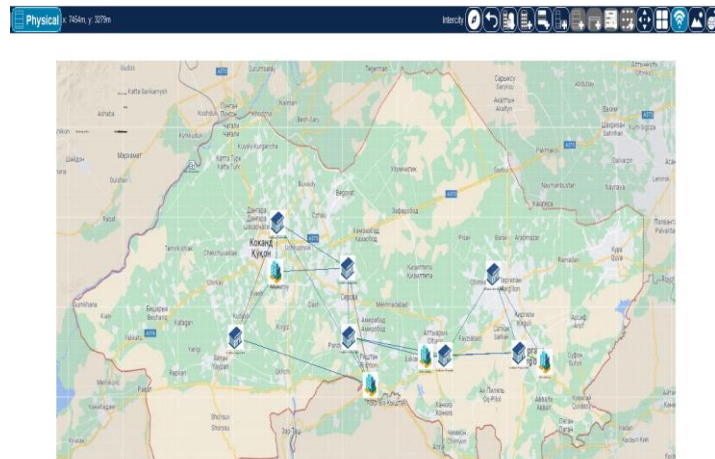
Kirish. Ushbu bo‘limda tadqiqot natijalariga ko‘ra Cisco Packet Tracer simulatori yordamida hususiy korxonalar bosh ofisi ham ularni hududiy filiallari o‘rtasida kompyuter tarmoqlari yordamida maxsus aloqa kanalini yaratish loyihasi taqdim etilgan. Buning uchun bizga Cisco Packet Tracer dasturini 8.2.1 versiyani kompyuterimizga o‘rnatish talab etiladi. Loyihani amalga oshirishda reallikga urg‘u bergan holda Farg‘ona viloyatida Oltiariq tumani “Taraqqiyot omad eksport” MCHJ korxonasi uchun Oltiariq tumani bosh ofisi, Farg‘ona shahar, Rishton tumani, Qo‘qon shahar, hududiy filiallari o‘rtasida o‘zaro malumot almashish uchun maxsus kanali loyihasini ishlab chiqish maqsad qilib olingan. Oraliq tarmoqlardan foydalanishda “O‘zbektelekom” AK ATClaridan foydalanilgan.

Maxsus kanal hosil qilishda Mesh topologiyasidan foydalangan holda MAN tarmog‘i va ichki LAN tarmog‘i qurishda chiziqli, yulduz topologiyalaridan foydalanamiz. Umumiy tarmog‘da Routerlar, ASA firewalllar, switchlar, server kompyuterlar, shaxsiy kompyuterlar, WiFi routerlar kabi qurilmalardan hamda serial koaksial, UTP kabellaridan foydalanilgan.

Adabiyotlar tahlili va metodologiya. Maqolani yozishda Mulayam Singh. CISCO PACKET TRACER LABS kitobidagi laboratoriya ishlaridan, Наполова Е.И. Кожевников С.В. Защита компьютерных сетей на основе технологии virtual private network mavzusidagi va D.Tojimatovning “Kiberxavfsizlik: tahdilar, muammolar, yechimlar” mavzusidagi hamda D.Tojimatovning “Use of Artificial Intelligence

Opportunities for Early Detection of Threats to Information Systems” mavzusidagi maqolalari o‘rganib chiqilib, tahlil qilingan. Yuqorida nomi keltirilgan tadqiqotchilarning ilmiy maqolalaridan foydalanib iqtiboslar keltirilgan.

Natijalar. Kompyuterimizda Cisco Packet Tracer dasturini ishga tushiramiz va loyiha tushunarli bo‘lishi uchun hudud, kompaniya, ATC fizik hususiyatlarini 1-rasmdagi ko‘rinishdagidek holatga keltiramiz.



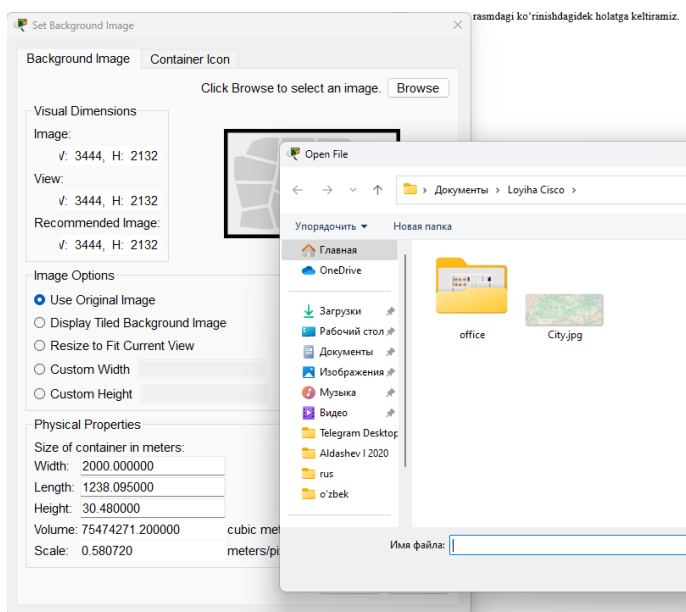
1-rasm. “Taraqqiyot omad eksport” MCHJ korxonasi hududiy binolarini Cisco Packet Tracer dasturining fizik qismida tarmoq orqali bog‘lanishi.

Bunday ko‘rinishga keltirishda google mapsdan Farg‘ona viloyatini kartasini rasmini qirqib kompyuter xotirasiga saqlab olamiz, Cisco Packet Tracer uskunalar qatoridan “Create New City” bo‘limidan yangi shahar kartasini yaratib olamiz. Hamda kartani

tanlagan holda "Set Background Image" bo'limini "Browse" qismidan xotiradagi Farg'ona viloyati kartasini yuklab qo'yamiz.

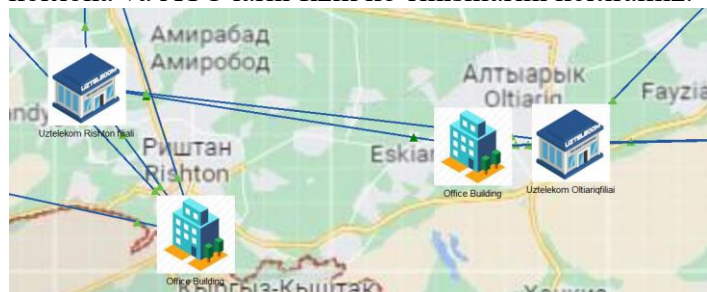


2-rasm. Cisco Packet Tracer dasturida alohida shahar kartasini qo'shish uchun uskunalar panelida "Create New City" bo'limini tanlash tugmasi.



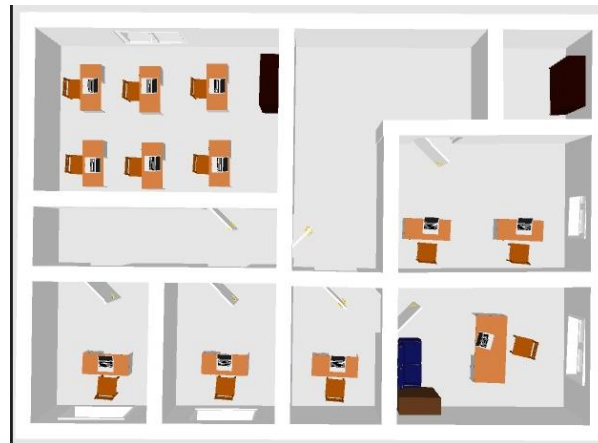
3-rasm. "Create New City" bo'limidan shahar kartasini qo'shish jarayoni.

Huddi shu amallarni "Create New Building" bo'limi yordamida yangi binolarni yaratgan holda korxonalar va ATC larni fizik ko'rinishlarini keltiramiz.



4-rasm. "Create New Building" bo'limi orqali korxonalar binolarini qo'shish jarayoni.

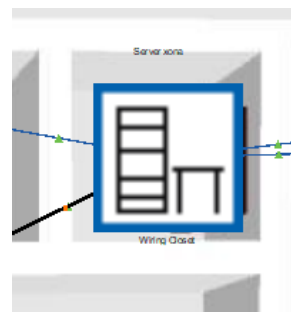
Endi korxonamizning ichki xonalari va tarmoq qurilmalari joylashuvini fizik ko'rinishlarini rasmda ko'rsatilganidek tayyorlab olamiz.



5-rasm. Korxonalar ichki tuzilmasini ko'rinishi.

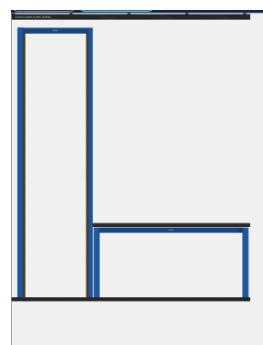
Buning uchun bino ko'rinishidagi raimni ichiga "Create New Building" orqali xona sxemasi rasmini yuklab olamiz.

Tarmog'imizni fizik ko'rinishini yaratib olgandan so'ng, server xona uchun "Create New Closet" uskunasi orqali server xonani ishchi shkafi va stolini serverxona sifatida keltirilgan xonamizga joylashtiramiz.



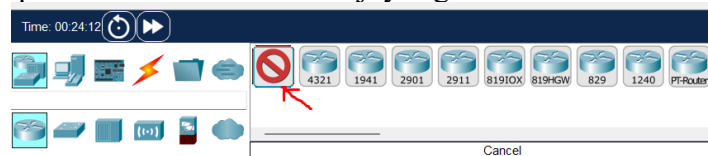
6-rasm. "Create New Closet" bo'limi orqali serverxona qo'shish.

Rasm ustiga sichqonchani o'ng tugmasini bosganimizda qurilmalarni joylash uchun shkaf va stolni ko'rinishimiz mumkun.

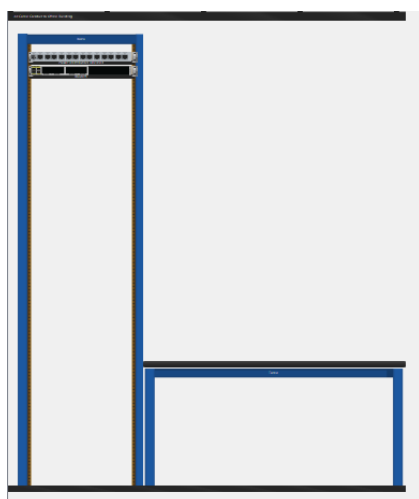


7-rasm. Serverxona uchun server shkafi va stolini ko'rinishi.

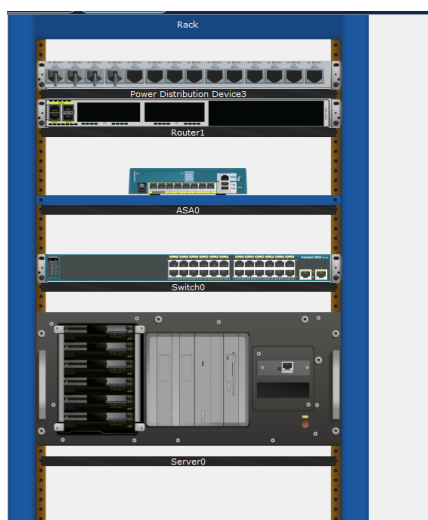
Server shkaf uchun Cisco Packet Tracerni qurilmalar bo'limidan tarmoq uchun kerakli qurilmalarni tanlab olamiz. Bizga server xona uchun Router, Server kompyuter, ASA firewall, Switch va administrator uchun kompyuter kerak bo'ladi. Kerak qurilmalarni tanlab kerakli joylarga o'rnatamiz.



8-rasm. Serverxona uchun tarmoq qurilmalarini tanlab qo'yish jarayoni.



9-rasm. Server shkafiga router shlyuzni o'rnatgandagi holat.

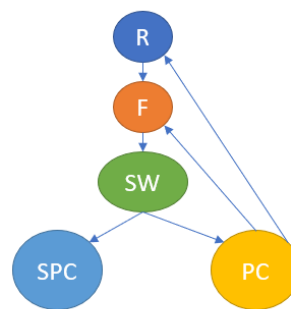


10-rasm. Server shkafiga router, firewall, switch, server qurilmalarini o'rnatgandagi holat



11-rasm. Server stoliga kompyuter o'rnatgandagi holat.

Qurilmalar tanlab olingandan keyin UTP kabeli (Coper Straight-Through) yordamida qulimalarni bir biriga quyidagi rasmda keltirilgan model yordamida ulaymiz.



R=Router, F=Firewall, SW=Switch, SPC=Server, PC=Shaxsiy kompyuter

12-rasm. Serverxona tarmoq qurilmalarini kabel orqali bir-biriga ulanish modeli.



13-rasm. Serverxona qurilmalarini to'liq ishchi holatga keltirilgandagi ko'rinish.

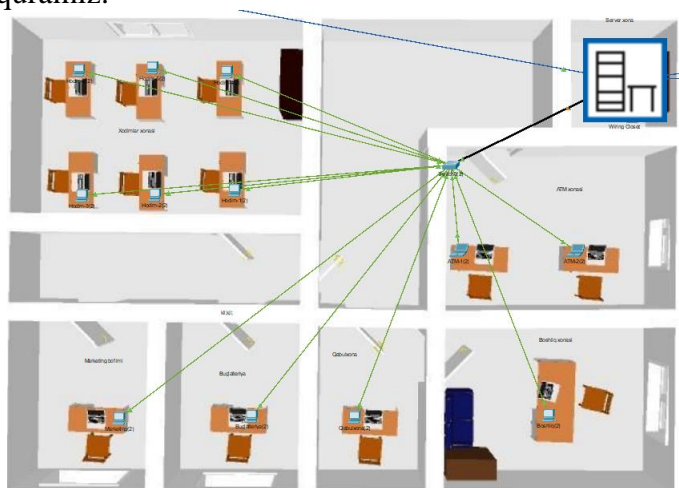
Server xonani qurilmalarini ulab olgandan so'ng, korxonani ishchi xonalarini tarmoqqa ulaymiz. Buning

uchun "Orqaga" strelkasi yordamida server xonadan asosiy xonalar ko'rsatilgan sxemaga qaytib olamiz.



14-rasm. Cisco Packet Tracerni uskunalar qatorida Closset, Building, City bo'limlaridan chiqish tugmasi.

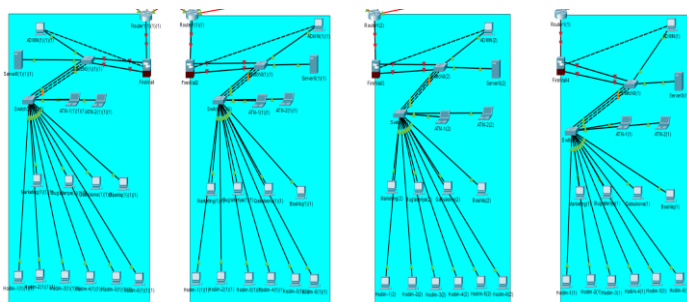
Xonalarni ATM (Axborot texnologiyalar markazi) ikkita ishchi kompyuter va switch qurilmasi, boshliq xonasi boshliq kompyuteri, qabulxona 1 ta kompyuter, bug'alteriya 1 ta kompyuter, marketing 1 ta kompyuter, hodimlar bo'limi 6 ta kompyuter joylab tarmoqni rasmda ko'rsatilgandek topologiya asosida quramiz.



14-rasm. Korxonalarini Lan tarmog'i orqali ulangandagi holat.

Bizni bitta korxonalar binosi uchun LAN tarmog'imiz tayyor bo'ldi. Endi huddi shunday ko'rinishdagi tarmoqni korxonalar filiallari uchun xam yaratib olamiz.

Cisco Packet Tracerni Logical (mantiqiy) rejimida biz qurgan tarmoq quydagicha ko'rinishga ega bo'ladi.



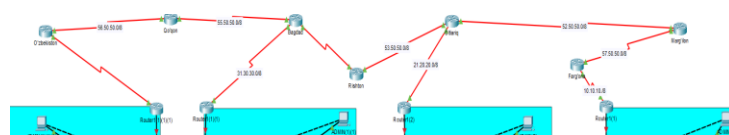
15-rasm. Korxonalar binolari uchun qurilgan Lan tarmoqlarni Cisco Packet Tracerni mantiqiy ko'rinishi.

Yaratilgan LAN tarmog'larni oraliq ATClar yordamida bir biriga bo'g'lash uchun xar bir ATCga bitatan Router qurilmasini o'rnatib olamiz. Bizni loyihada Far'ona shahar, Marg'ilon shahar, Oltiariq tumani, Rishton tumani, Bog'dod tumani, Qo'qon shahar, O'zbekiston tumanida joylashgan "O'zbektelekom" AK ning 7 ta ATC misol sifatida ko'rsatilgan.



15-rasm. "O'zbektelekom" AKni hududiy filiallarini tasvirlab beruvchi belgi va tarmoqni marshrutizatsiya qilish uchun tashqi oraliq qurilmasi.

Avvaliga korxonalar routerlarini o'ziga yaqin joylashgan ATC routerlariga Gigabite Ethernet kanali orqali bog'laymiz. So'ngra ATClarni bir-biriga ulaymiz. Routerlarni mantiqiy bog'lanishini rasmda ko'rsatilgan holatga keltiramiz.



16-rasm. Tashqi tarmoq marshrutizatorlarini bir-biriga ulanish sxemasi.

Oraliq tashqi tarmoq routerlariga RIP (Routing Information Protocol) protokoli yordamida marshrutizatsiya rejimini sozlab qo'yamiz. Buning uchun routerni barcha ulangan portlariga alohida ip manzillar berib chiqish va portlarni yoqish hamda turli ip manzillarga ega portlarda paketlar marshrutizatsiya bo'lishi uchun RIP buyrug'larini kiritishtalab qilinadi.

Buning uchun xar bir routerni CLI (Command Line) bo'limiga o'ziga beriladigan ip manzilni tanib olgan holda quyidagicha buyruqlarni berib chiqamiz.

```
Router>  
Router>en  
Router#conf t
```


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

```
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip address 11.10.10.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface
GigabitEthernet0/0/0, changed state to up
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ip address 192.168.1.1
255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface
GigabitEthernet0/0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.0.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#exit
```

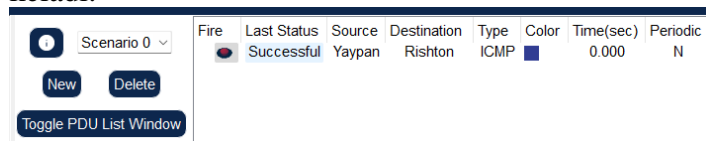
Yuqorida keltirilgan sozlama buyruqlari xar bir
ichki va tashqi routerlarga o'ziga tegishli o'zgaruvchi
ip manzillar kiritgan holda kiritiladi.

Barcha routerlarni sozlab bo'lgach ularda
axborot ketishini tekshiramiz. Buning uchun Cisco
Packet Tracerni taxrirlash uskunalaridan "Add Simple
PDU" konvertini tanlaymiz va bir routerdan
boshqasiga paket jo'natib ko'ramiz.



17-rasm. Cisco Packet Tracerda uskunalar qatorida
paket jo'natib tekshirish belgisi.

Agar marshrutizatsiya sozlamalari to'g'ri
sozlangan bo'lsa hodisalar bo'limida "Successful"
yozuvi paydo bo'ladi. Xato bo'lgan taqdirda "Failed"
yozuvi chiqib paket qurilmalar orasida ketmaydi.
Bunda sozlamalarni qayta ko'rib chiqishga to'g'ri
keladi.



18-rasm. Qurilmalar o'rtasida tarmoq orqali
pakatlarni jo'natish va qabul qilish to'g'ri amalga
oshirilganlik yozuvi.

Barcha jarayonlar to'g'ri bajarilsa korxon va
uning filiallarida ochiq kanal orqali ma'lumot
almashish mumkin bo'ladi.

Endi bu yaratilgan ochiq kanalni VLAN va VPN
texnologiyalari yordamida maxsus kanalga aylantirib
olamiz.

Muhokama. Birinchi navbatda tashkil etilgan
korxon tarmog'ining ichki tarmog'iga ichki
axborotlarni sizib chiqishidan himoyalash uchun
korxon tuzilmasidan kelib chiqib Vlan texnologiyasi
asosida maxsus kanallar hosil qilib olamiz.

Bizni holatda korxon tarkibi "Server xona",
"ATM bo'limi", "Boshliq xonasi", "Qabulxonasi",
"Bug'alteriya", "Marketing bo'limi", "Hodimlar
xonasi" dan iborat.

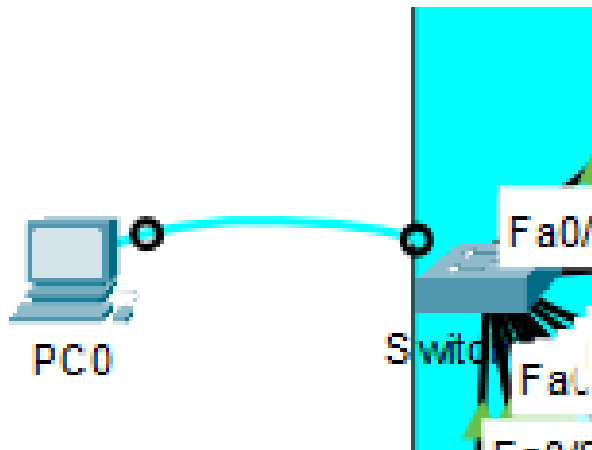
Korxon uchun quyidagi ko'rinishda va
nomlar bilan alohida ajratilgan maxsus kanal hosil
qilishni tavsiya etamiz.

- Administrator kanali;
- Boshqaruvchilar kanali;
- Hodimlar kanali.

Administratorlar kanali bog'lanuvchilari
tarmoqda to'liq boshqaruv huquqi bo'lganligi bois
server xona va ATM bo'limini kompyuterlariga barcha
qurulmalarga ulanish huquqini beramiz. Boshqaruv
kanaliga boshliq xonasi, bug'alteriya, marketing
bo'limini bog'laymiz va boshliq uchun bu kanaldan
tashqari boshqa kanallar bilan ham bog'lanish huquqini
beramiz. Hodimlar kanaliga qabulxonasi va hodimlar
bo'limidagi kompyuterlarni bog'laymiz. Bularni
barchasini markaziy boshqariladigan SWITCH
qurulmasida amalga oshiramiz. SWITCH orqali
yuqorida nomi keltirilgan kanallarni hosil qilib,
ulangan portlarni statusiga qarab kanallarga birlashtirib
chiqamiz.

Bu SWITCH qurilmasiga quyidagi ketma-
ketlikda buyruqlarni kiritish orqali amalga oshiriladi.

1. Telnet yoki SSH protokoli yoki SWITCHni konsol
portiga admin kompyuterini ulagan holda CLI
oyinasida SWITCHni Configurationsiga (sozlamalari)
kirib olamiz. Agar masofadan bog'lanish uchun telnet
yoqilgan bo'lmasa avvaliga konsol port orqali ulanib
telnetni yoqib olish tavsiya etiladi.



19-rasm. Konsol kabel orqali kompyuterni RS-232 portini switchni konsol portiga ulash.

Telnetni yoqish uchun kompyuterni terminalidan -rasmida keltirilgandek buyruqlar kiritiladi.

```
Switch>
Switch>
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable pas
Switch(config)#enable password 12345
Switch(config)#int vlan 1
Switch(config-if)#ip add 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#line vty 15
Switch(config-line)#password 12345
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#
```

20-rasm. Terminal orqali SWITCH qurilmasida telnetni yoqish uchun sozlash.

Telnet sozlangandan so'ng admin kompyuterini CMD oynasidan telnet 192.168.1.1 orqali SWITCH konfiguratsiya bo'limiga kirish mumkin.

Vlan kanallar hosil qilish uchun -rasmida keltirilgan buyruqlarni kiritish kerak bo'ladi.

```
Switch(config)#vlan 2
Switch(config-vlan)#name Administrator
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name Boshqaruv
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name Hodimlar
Switch(config-vlan)#
```

21-rasm. SWITCHda Vlan kanallar hosil qilish. Vlan raqami va nomi kiritiladi.

Hosil qilingan kanallarga SWITCHni ulangan kompyuterlar portiga biriktirib chiqamiz.

```
Switch(config)#interface range fastEthernet 0/1-2
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#
```

22-rasm. SWITCH portlarini tashkil etilgan Vlan kanallarga biriktirish buyrug'i.

Qolgan bo'limlarga ulangan portlarni ham shu tartibda o'zlariga tegishli hosil qilingan Vlan kanallarga biriktirib chiqamiz.

Shunda quyi darajadagi kanalgaga bog'langan kompyuterlar boshqa darajadagi kanallarda axborot almashinuvi cheklanadi. Faqat yuqori darajadagi kanalga ulangan kompyuterlar (administrator kanali) barcha darajadagi portlarga TRUNK rejimi orqali ulangani bois aloqa o'rnatishi mumkin bo'ladi.

```
2 Administrator active Gi0/2
3 Boshqaruv active Fa0/1, Fa0/2
Fa0/6 Fa0/3, Fa0/4, Fa0/5,
4 Hodimlar active Fa0/7
Fa0/11 Fa0/8, Fa0/9, Fa0/10,
```

23-rasm. Vlan kanallarga bog'langan portlar tavsifi.

Yuqoridagi amallar orqali oddiy usulda ichki tarmoq uchun 3 ta mantiqiy jixatdan quyi, o'rta, yuqori darajalar uchun maxsus kanallar qurib chiqildi.

Endi korxonaning bosh offisi va hududiy filiallari orasida tashqi tarmoqda VPN orqali maxsus kanal hosil qilishni ko'rib chiqamiz.

Buning uchun korxonaning barcha binolarida joylashgan oraliq shlyuz routerlariga host-to-host VPN sozlamalarini sozlab chiqish talab etiladi.

Asosiy sozlamalarda paketlarni shifrlash va deshifrlash uchun umumiy kalit, tarmoqni tunellash uchun karta (map), kalitlarni solishtirish uchun xeshlash algoritmlaridan foydalaniladi.

Shlyuz routerga SWITCH konfiguratsiyasiga ulanganimiz kabi Telnet, SSH yoki konsol port orqali bog'lanamiz va quyidagicha buyruqlarni kiritamiz.

Korxonaning 1 binosi shlyuz routeriga kiritiladigan buyruqlar.

```
Router>enable
Router#conf t
Router(config)#int g 0/0/0
Router(config-if)#no shut
Router(config-if)#ip nat inside
Router(config-if)#ip address 192.168.1.1
255.255.255.0
Router(config)#int fa 0/1
Router(config-if)#no shut
Router(config-if)#ip address 10.10.10.1 255.0.0.0
Router(config-if)#ip nat outside
```

```
Router(config-if)#exit
Router(config)#ip access-list extended for-nat
Router(config-ext-nacl)#deny ip 192.168.2.0
0.0.0.255 192.168.3.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.2.0
0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list for-nat int fa
0/1 overload
Router(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
Router(config)#ip dhcp pool vl2
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 8.8.8.8
Router(dhcp-config)#exit
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config)#crypto isakmp key 123 address
20.20.20.1
Router(config)#crypto ipsec transform-set ts esp-aes
esp-md5-hmac
Router(config)#ip access-list extended for-vpn
Router(config-ext-nacl)#permit ip 192.168.2.0
0.0.0.255 192.168.3.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map Taraqqiyot 10 ipsec-
isakmp
Router(config-crypto-map)#match address for-vpn
Router(config-crypto-map)#set peer 20.20.20.1
Router(config-crypto-map)#set transform-set ts
Router(config-crypto-map)#exit
Router(config)#int fa 0/1
Router(config-if)#crypto map Taraqqiyot
*Jan 3 07:16:26.785: %CRYPTO-6-
ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit (VPN qurish jarayoni)
```

Korxonaning 2 binosi shlyuz routeriga kiritiladigan buyruqlar.

```
Router>enable
Router#conf t
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config-if)#ip nat inside
Router(config-if)#ip address 192.168.3.1
255.255.255.0
```

```
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#no shut
Router(config-if)#ip address 2.2.2.1 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip access-list extended for-nat
Router(config-ext-nacl)#deny ip 192.168.3.0
0.0.0.255 192.168.2.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.3.0
0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list for-nat int fa
0/1 overload
Router(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.2
Router(config)#ip dhcp pool vl3
Router(dhcp-config)#network 192.168.3.0
255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 123 address 1.1.1.1
Router(config)#crypto ipsec transform-set ts esp-aes
esp-md5-hmac
Router(config)#ip access-list extended for-vpn
Router(config-ext-nacl)#permit ip 192.168.3.0
0.0.0.255 192.168.2.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map Taraqqiyot 10 ipsec-
isakmp
Router(config-crypto-map)#match address for-vpn
Router(config-crypto-map)#set peer 1.1.1.1
Router(config-crypto-map)#set transform-set ts
Router(config-crypto-map)#exit
Router(config)#int fa 0/1
Router(config-if)#crypto Taraqqiyot
*Jan 3 07:16:26.785: %CRYPTO-6-
ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
```

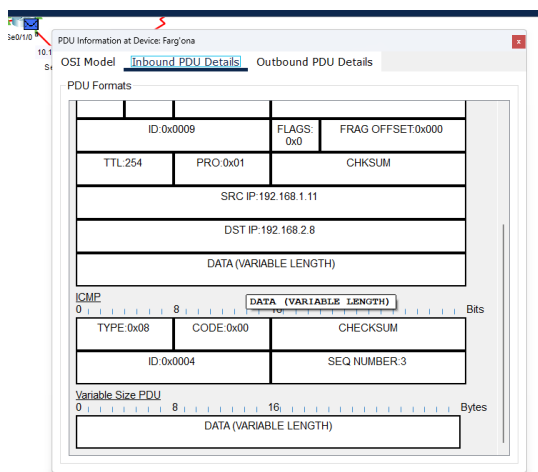
Buyruqlar shu tartibda uchunchi va to‘rtinchi binolariga ham kiritiladi. Bu yerda paketlarni shifrlash va deshifrlash kaliti 123 berilib AES shifrlash algoritmidan, shifrlangan axborotlarni butunligini

tekshirish uchun md5 xeshlash algoritmidan, ichki IP manzillarni yashirish uchun Nat texnologiyalaridan foydalanilgan. Tarmoqlarni karta orqali tanib olishda esa "Taraqqiyot" so'zi identifikator sifatida kiritilgan.

Quyida ochiq kanal va maxsus kanal orqali uzatiladigan axborotlarni tutib olingandagi holatini tahlil qilib chiqamiz.

Ochiq kanalda jo'natilgan paketlar shifrlanmaydi, IP manzillari yashirilmaydi, jo'natmalar TSP/IP tamoillariga ko'ra manzillarga jo'natiladi (bunda aynan qabul qiluvchini MAC manzili va IP manzili buzg'unchi tomonidan o'zlashtirilganda paket buzg'unchiga jo'natilishi mumkin), paket butunligi tekshirilmaydi (bunda o'rtadagi odam paketni qaysidir qismini o'zgartirib yoki yo'q qilib qayta yo'naltirishi mumkin).

Maxsus kanalda jo'natilgan paketlar shifrlanadi, ichki ip manzillar o'zgartiriladi, paket butunligi xeshlash orqali tekshiriladi, paket o'z kartasi bo'yicha qabul qiluvchiga to'g'ri yo'naltiriladi.



24-rasm. Paketlarni ochiq kanalda oraliq qurilmalar orqali tutib ochilgandagi VPNsiz himoyalangan ko'rinishi.

Xulosa. Yuqorida berilgan loyiha ma'lumotlari asosida hususiy korxonalar va ularning hududiy filiallari uchun xavfsiz ma'lumot almashishga asoslangan mahsus tarmoq qurish mumkin. Mahsus tarmoqning avzalliklari sifatida birinchi navbatda o'rtadagi odam hujumi, DDos hujumi, tarmoq uzulish xatoliklari kabi xavf-xatarlarini ko'rsatishimiz mumkin. Ishning amaliy yangiligi sifatida mesh texnologiyasi, stp protokoli, vpn texnologiyalarini birgalikda qo'llash avzalliklarini keltirishimiz mumkin. Berilgan loyihani model sifatida har qanday korxonalar va tashkilotlarda qo'llash va natijaga erishish

real tarmoqqa qo'llagan holda tekshirib ko'rilgan va ijobiy xulosa olingan.

Adabiyotlar ro'yxati

[1]. Mulayam Singh. CISCO PACKET TRACER LABS/ BookRix, 2019.

[2]. Наполова Е.И. Кожевников С.В. Защита компьютерных сетей на основе технологии virtual private network/ Экономика и качество систем связи. 2018

[3]. Dostonbek T., Jamshid M. Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems //Central Asian Journal of Theoretical and Applied Science. – 2023. – Т. 4. – №. 4. – С. 93-98.

[4]. MIRZAYEV J. B., TOJIMATOV D. H. O. G. L. I. KIBERXAVFSIZLIKNI TA'MINLASH, KIBERHUJUMLARNI OLDINI OLIISH BO'YICHA DAVLAT SIYOSATI YURITILISHI //ИНТЕРНАУКА Учредители: Общество с ограниченной ответственностью "Интернаука". – С. 36-37.

[5]. Tojimatov D. X. Kiberxavfsizlik: tahdilar, muammolar, yechimlar,“ //Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar” Respublika Ilmiy-texnik anjumani TATU Farg'ona filiali. – 2022.

[6]. Tojimatov D. u KIBER TAHDIDLARNI BASHORAT QILISH VA XAVF-XATARLARDAN HIMOYALANISHDA SUN'IY INTELEKT IMKONIYATLARIDAN FOYDALANISH: DX Tojimatov. Katta o'qituvchi, TATU Farg'ona filiali //Потомки Аль-Фаргани. – 2023. – Т. 1. – №. 2. – С. 41-44.