

**MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI
UNIVERSITETI**



Infokommunikatsiya injiniringgi yo'nalishi
3-bosqich 431-22-guruh talabasi
Shodibekov Jamshidbekning
Kompyuter tarmoqlari
fanidan bajargan amaliy ishi

Bajardi: Shodibekov Jamshidbek

Tekshirdi: Temirova Dilfuza

AMALIYOT ISHI № 13-14
CISCO PACKET TRACER DASTURIDA DHCP, DNS, WEB,
FTP VA EMAIL SERVERLARINI SOZLASH

1. Ishning maqsadi

Ushbu laboratoriya ishidan maqsad quyidagilar hisoblanadi:

- Web serverni ishlash tamoyillarini va uni sozlashni o'rganish;
- DHCP serverni ishlash tamoyillarini va uni sozlashni o'rganish;
- DNS serverni ishlash tamoyillarini va uni sozlashni o'rganish;
- FTP serverni ishlash tamoyillarini va uni sozlashni o'rganish;
- Email serverni ishlash tamoyillarini va uni sozlashni o'rganish;

2. Qisqa nazariy ma'lumotlar

Qoida tariqasida, *server* o'z resurslarini *tarmoqqa* beradi va mijoz ushbu manbalardan foydalanadi. Shuningdek, serverlarga ixtisoslashtirilgan *dasturiy va apparat ta'minoti* o'rnatilgan. Bir vaqtning o'zida bir nechta server dasturlari bitta kompyuterda ishlashi mumkin. Server xizmatlari ko'pincha ularning nomlarini aniqlaydilar:

HTTP (WEB) server – eng oddiy veb-sahifalarni yaratishga va serverning 80-portida paketlarning o'tishini tekshirishga imkon beradi. Ushbu serverlar veb-sahifalarga va rasmlar kabi tegishli manbalarga kirishni ta'minlaydi.

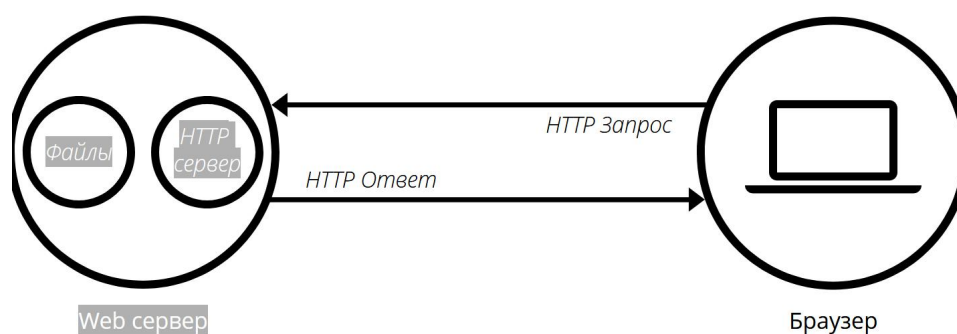
Veb-server tushunchasi ham apparat, ham dasturiy ta'minotni (DT) nazarda tutishi mumkin.

1. Uskuna nuqtai nazaridan veb-server veb-sayt resurslarini (HTML hujjatlari, CSS uslublari, JavaScript fayllari va boshqalarni) saqlaydigan va ularni oxirgi foydalanuvchi qurilmasiga (vab-brauzer va

boshqalar) etkazib beradigan kompyuterdir. Odatda u Internetga ulanadi va unga tuit.uz kabi domen nomi orqali kirish mumkin.

2. Dasturiy ta'minot nuqtai nazaridan veb-serverga veb-foydalanuvchilarning serverda joylashgan fayllarga kirishini boshqaradigan ba'zi narsalar kiradi, bu HTTP-serverning minimal darajasi. HTTP server – bu URL (veb-manzillar) va HTTP (brauzeringiz veb-sahifalarni ko'rish uchun foydalanadigan protokol) ni tushunadigan dasturiy ta'minot.

Bir so'z bilan aytganda, brauzerga veb-serverda joylashtirilgan fayl kerak bo'lganda, brauzer uni HTTP orqali so'raydi. So'rov kerakli veb-serverga (apparat) yetib kelganda, HTTP server (dasturiy ta'minot) so'ralgan hujjatni, yana HTTP orqali yuboradi (1-rasm).



1-rasm. HTTP serverni ishlash tamoyili

Veb-saytni namoyish qilish uchun sizga statik yoki dinamik veb-server kerak.

Statik veb-server yoki stek HTTP-server (dasturiy ta'minot) o'rnatilgan kompyuterdan (apparat) iborat. Biz buni "statik" deb ataymiz, chunki server unda joylashtirilgan fayllarni o'zgartirmasdan brauzerga yuboradi.

Dinamik veb-server statik veb-server va qo'shimcha dasturlardan iborat bo'lib, ko'pincha ilovalar serverlari va ma'lumotlar bazasidan iborat.

Biz buni "dinamik" deb ataymiz, chunki dastur serveri HTTP orqali brauzeringizga yuborishdan oldin manba fayllarini o'zgartiradi.

Masalan, brauzerda ko'rgan yakuniy sahifani olish uchun dastur serveri HTML shablonini ma'lumotlar bazasidagi ma'lumotlar bilan to'ldirishi mumkin. MDN (Mozilla Developer Network) yoki Vikipediya kabi saytlar minglab veb-sahifalardan iborat, ammo ular haqiqiy HTML hujjatlari emas, faqat bir nechta HTML shablonlari va ulkan ma'lumotlar bazalari. Ushbu tuzilma veb-ilovalarni saqlash va tarkibni etkazib berishni osonlashtiradi va tezlashtiradi.

Veb-sahifani yuklash uchun, aytganimizdek, brauzer veb-serverga so'rov yuboradi, u so'ralgan faylni o'z xotirasida qidirishni boshlaydi. Faylni topgandan so'ng, server uni o'qiydi, kerak bo'lganda qayta ishlaydi va brauzerga yuboradi. Keling, ushbu qadamlarni batafsil ko'rib chiqaylik.

Fayl xostingi

Birinchidan, veb-server veb-sayt fayllarini, ya'ni barcha HTML hujjatlarni va tegishli manbalarni, shu jumladan rasmlar, CSS uslublari, JavaScript-fayllar, shriftlar va videolarni saqlaydi.

Texnik jihatdan, ushbu fayllarning barchasini kompyuteringizga joylashtirishingiz mumkin, ammo ularni maxsus veb-serverda saqlash juda qulay:

- har doim yuklanadi va ishlaydi;
- doimiy Internetda tarog'ida;
- har doim bir xil IP-manzilga ega.

Shunday qilib, yaxshi hosting provayderini tanlash veb-saytni yaratishda muhim qism hisoblanadi. Kompaniyalarning turli xil takliflarini ko'rib chiqing va ehtiyojlaringiz va byudjetingizga mos taklifni tanlang (takliflar oyiga bepul dan ming dollargacha).

HTTP bo'yicha aloqa

Ikkinchidan, veb-server HTTP (gipermatnli uzatish protokoli) ni qo'llab-quvvatlaydi. Nomidan ko'rinib turibdiki, HTTP gipermatnni (ya'ni, bog'langan veb-hujjatlarni) ikkita kompyuter o'rtasida qanday o'tkazilishini belgilaydi.

Protokol – bu ikkita kompyuter o'rtasidagi aloqa qoidalari to'plami. HTTP – bu matnga asoslangan, holatni saqlamaydigan protokol.

HTTP mijoz va server qanday aloqa o'rnatishi to'g'risida qat'iy qoidalarni belgilaydi. Quyida uchbu qoidalaridan ba'zilari keltirilgan:

- Faqat mijozlar HTTP so'rovlarini yuborishi mumkin va faqat serverlarga. Serverlar faqat mijoz HTTP so'rovlariga javob beradi.
- Jismoniy fayl so'ralganda, mijoz fayl URL-manzilini yaratishi kerak (*fayl:///var/log/syslog*)
- Veb-server har bir HTTP so'roviga kamida xato xabari bilan javob berishi kerak.

Veb-serverda HTTP-server kiruvchi so'rovlarni qayta ishlash va javob berish uchun javobgardir.

1. So'rovni olayotganda, HTTP server avval manba berilgan URL manzilida mavjudligini tekshiradi.
2. Agar shunday bo'lsa, veb-server fayl tarkibini brauzerga qaytarib yuboradi. Agar shunday bo'lmasa, dastur serveri kerakli resursni yaratadi.
3. Agar buning iloji bo'lmasa, veb-server xato haqida xabarni brauzerga qaytaradi, ko'pincha "404 topilmadi". (Bu xato shunchalik keng tarqalganki, ko'plab veb-dizaynerlar 404 xato sahifalarini loyihalashtirish uchun ko'p vaqt sarflashadi.)

DHCP server – tarmoq interfeyslarini avtomatik sozlash uchun tarmoq sozlamalari pullarini tashkil qilish imkonini beradi. *Dynamic Host Configuration Protocol* IP-manzillarni tarmoqdagi kompyuterlar o'rtasida

avtomatik ravishda taqsimlashni ta'minlaydi. Ushbu texnologiya umumiy Internet ulanishi bilan mahalliy tarmoqlarda keng qo'llaniladi.

DHCP – bu Dinamik Xost Konfiguratsiya Protokoli. Nomidan ko'rinib turibdiki, DHCP uzoqdagi server orqali xostni sozlash uchun mo'ljallangan. DHCP ko'pgina zamonaviy operatsion tizimlarda sukut bo'yicha qo'llab-quvvatlanadi va server yoki biriktirilgan qurilma uchun tarmoq sozlamalarini muntazam ravishda qo'lda sozlash uchun ajoyib alternativani beradi.

Ushbu protokol "Mijoz-Server" modeli asosida ishlaydi. Protokol sifatida DHCP mijoz va server o'rtasida xabar almashish usuliga ega. 6.1-jadvalda DHCP xabarining tarkibi keltirilgan.

1-jadval

DHCP xabarning tarkibi

Maydon	Uzunlik (bayt)	Ta'rif
op	1	Xabar turi
htype	1	Apparat qismi adresi turi
hlen	1	Apparat qismi adresi uzunigi
hops	1	Retranslyatsiya agentlarining qo'llanilish miqdori. Mijozlar qiymatiga 0 o'rnatiladi.
xid	4	Seans paytida mijoz va server tomonidan ishlatiladigan tranzaktsiya ID (unikal identifikatsiya raqami)
secs	2	Mijoz jarayonni boshlashni so'raganidan beri o'tgan vaqt (soniyalarda)

flags	2	Bayroqlarning qiymati
ciaddr	4	Mijozning IP-manzili (agar ilgari mavjud bo'lsa)
yiaddr	4	Server tomonidan mijozga taqdim etilgan IP-manzil
siaddr	4	Server IP-manzili
giaddr	4	Relay agenti (retranslyatsiya agenti) IP-manzili
chaddr	16	Mijozning apparat vositasi manzili (ko'pincha MAC)
sname	64	Server nomi
file	128	Yuklanadigan fayl nomi
Options	o'zgarmali	Qo'shimcha imkoniyatlar

DHCP asoslarini bilish turli xil tarmoq muammolarini bartaraf etishga yordam beradi. Quyida biz protokolning ishlash tamoyillariga to'xtalamiz.

DHCP qanday ishlaydi? Ushbu maqsadga erishish jarayonini o'rganishdan oldin, ushbu jarayonda qo'llaniladigan turli xil ma'lumot almashish tamoyillarini tushunish kerak.

DHCPDISCOVER. Ushbu xabar mijoz va server o'rtasida DHCP aloqasining boshlanishini belgilaydi. Ushbu xabar tarmoqqa ulangan mijoz (kompyuter yoki qurilma) tomonidan yuboriladi. Ushbu xabar etkazib berish IP-si sifatida 255.255.255.255 dan foydalanadi, asl manzili esa 0.0.0.0

DHCPOFFER. Ushbu xabar DHCP-serverdan DHCPDISCOVER-ga ulangan mijozlar uchun javob sifatida yuboriladi. Ushbu xabar kerakli tarmoq sozlamalarini o'z ichiga oladi.

DHCPREQUEST. Ushbu xabar DHCPOFFER-ga javob bo'lib, mijoz yuborilgan sozlamalarni qabul qilganligini bildiradi.

DHCPACK. Ushbu xabar mijozning DHCPREQUEST javobi sifatida DHCP-serverga yuboriladi. Xabar DHCPDISCOVER xabari bilan boshlangan jarayon tugaganligini bildiradi. Ya'ni, DHCPACK – bu

server tomonidan mijozning avtorizatsiyasi boshlanganligi va serverdan boshida qabul qilingan konfiguratsiya parametrlari qabul qilinganligi haqidagi tasdiqlashdan boshqa narsa emas.

DHCPNAK. Ushbu xabar yuqorida tavsiflangan DHCPACK-ning teskarisidir. Mijozning DHCPREQUEST parametrlarini qondira olmasa, u serverga yuboriladi.

DHCPDECLINE. DHCP-da tayinlangan IP-manzil allaqachon ishlatilgan bo'lsa, mijoz tomonidan serverga xabar yuboriladi.

DHCPINFORM. DHCP mijoziga statik IP-manzil tayinlangan bo'lsa, xabar serverga yuboriladi, ammo konfiguratsiya sozlamalari dinamik manzilni talab qiladi.

DHCPRELEASE. Tarmoq manzilidan foydalanish jarayoni tugagandan so'ng, mijozlarga xabar yuboriladi.

DHCP-dagi turli xil xabarlar bilan tanishganimizdan so'ng, biz yaxshiroq tasavvurga ega bo'lish uchun butun jarayonni bosib o'tishimiz mumkin. Quyidagi qadamlar barcha sozlamalar odatiy o'rnatilgan holat bo'yicha tavsiflanadi.

1-qadam. Mijoz (kompyuter yoki qurilma) yuklashda yoki tarmoqqa ulanganda serverga DHCPDISCOVER xabari yuboriladi. Agar qo'shimcha konfiguratsiya ma'lumotlari bo'lmasa, u holda xabar 0.0.0.0 dan 255.255.255.255 gacha yuboriladi. Agar DHCP-server mahalliy subnetda bo'lsa, u xabarni to'g'ridan-to'g'ri qabul qiladi, agar u boshqa subnet-da bo'lsa, u holda retranslyatsiya agenti DHCP-serverga so'rov yuborish uchun ishlatiladi. 67-port orqali UDP uzatish protokoli ishlatiladi. Mijoz ushbu bosqichda avtorizatsiya bosqichini boshlaydi.

2-qadam. Server DHCPDISCOVER so'rovini olgan lahzada, javob sifatida DHCP OFFER xabarini yuboradi. Avval aytib o'tganimizdek, ushbu xabar mijoz tomonidan talab qilingan barcha kerakli konfiguratsiya parametrlarini o'z ichiga oladi. Masalan, mijoz talab qiladigan IP-manzil,

shuningdek subnet mask qiymati va shlyuz ma'lumotlari. Shuningdek, server zudlik bilan CHADDR maydonidagi MAC manzil qiymatlarini to'ldiradi. Xabar to'g'ridan-to'g'ri mijozga 255.255.255.255 manzilidan yuboriladi va agar server boshqa subnetda bo'lsa, u holda xabarning etkazib berilishini ta'minlash uchun javobgar bo'lgan retranslyatsiya agentlari ishlatiladi. Bunday holda UDP 68 port orqali uzatish uchun ishlatiladi. Ushbu bosqichda mijoz parametrlarni tanlashni boshlaydi.

3-qadam. Mijoz serverdan DHCPOFFERga javob beradigan DHCPREQUEST xabarini ishlab chiqaradi, bu unga yuborilgan konfiguratsiya parametrlarini qabul qilishini bildiradi. Agar bir nechta DHCP-serverlar mavjud bo'lsa, mijoz bir nechta DHCPOFFER xabarlarini ham qabul qilar edi, ammo mijoz konfiguratsiya uchun konfiguratsiya parametrlarini to'ldirib, faqat bitta serverga javob beradi. Shunday qilib, ma'lum bir DHCP-serverdan IP-manzil olishga vakolat berilgan. Boshqa serverlardan kelgan barcha xabarlar bloklangan. Agar mijoz hanuzgacha DHCPOFFER xabarida olingan IP-manzillardan foydalana olmasa, DHCPREQUEST xabarida 0.0.0.0 manba manzili saqlanib qoladi. Ushbu bosqichda mijoz o'z so'rovlariga javob oladi.

4-qadam. Server mijozdan DHCPREQUESTni qabul qilishi bilanoq, DHCPACK xabarini yuboradi, endi mijoz unga tayinlangan IP-manzildan foydalanishi mumkin. Mijoz nihoyat tarmoqqa va sozlangan parametrlarga ulanadi.

DNS server. DNS server – domen nomini aniqlash xizmatini tashkil qilish imkonini beradi. DNS serverning vazifasi serverlarning domen nomlarini IP manzillariga tarjima qilishdan iborat.

Domen nomi tizimi ikkita asosiy funktsiyani bajarish uchun zarur bo'lgan DNS-server orqali ishlaydi:

- domen nomining ma'lum bir IP-manzilga muvofiqligi to'g'risidagi ma'lumotlarni saqlash,

- boshqa DNS-serverlarning resurs yozuvlarini keshlash.

Agar foydalanuvchi boshqa mamlakatda joylashgan saytga kirmoqchi bo'lsa, unda doimiy ravishda so'rovlarni asosiy serverga yuborish uzoq vaqt talab etadi va sahifalarni sekin yuklanishiga olib keladi. Bunday noqulayliklarga yo'l qo'ymaslik uchun sizning qurilmangiz yonida joylashgan DNS-server oldindan so'ralgan IP-manzillar to'g'risidagi ma'lumotlarni keshlaydi va keyingi kirishda ularni chiqaradi.

Resurs yozuvlarini saqlash manbalari – bu domenlar va xost tarmoq manzillari o'rtasidagi dastlabki aloqalarni o'z ichiga olgan manba DNS-serverlari.

Qoida tariqasida ikkita serverdan foydalanish tavsiya etiladi: birlamchi va ikkilamchi. Bu sizning domeningizga kirishni ta'minlaydi, chunki agar bitta server ishlamay qolsa, boshqasi javob beradi.

DNS-serverlar qanday ishlaydi. DNS so'rovlariga javob berish uchun mo'ljallangan dasturlarning bosqichma-bosqich ishlashini ko'rib chiqamiz:

1. Brauzer foydalanuvchidan so'rov oladi va uni tarmoqning DNS-serveriga yuboradi, u domen nomi va tarmoq manzili o'rtasida moslikni qidiradi. Agar javob topilsa, darhol sayt sahifasi yuklanadi. Aks holda, so'rov yo'qori darajadagi yoki ildiz (asosiy) serverga yuboriladi.

2. Ildiz-server so'rovni birinchi darajali serverga yuboradi, bu esa ikkinchi darajali serverga yuboradi. Ushbu harakat nom va IP-manzil o'rtasida mos kelguniga qadar davom etadi.

3. Brauzer uning so'roviga javob oladi, uni xostingga yo'naltiradi va sahifa ochiladi.

Teskari protsedura ham mumkin – so'ralgan IP-manzilga mos keladigan DNS-serverda domen nomini qidirish. Masalan, bu elektron pochta serveri bilan ishlashda yuz beradi.

DNS-serverlar qayerda joyashadi? Domen nomlari bo'yicha so'rovlarni qayta ishlash uchun asos – bu ildiz DNS zonasi uchun mas'ul bo'lgan ildiz serverlari. Ularni serverlarning uzluksiz ishlashini ta'minlaydigan turli xil operatorlar boshqaradi. Birinchi ildiz serverlari Shimoliy Amerikada paydo bo'lgan, ammo vaqt o'tishi bilan ular dunyoning boshqa mamlakatlarida paydo bo'la boshladilar. Bugungi kunda dunyoning turli burchaklarida joylashgan 123 ta ildiz-serverlar mavjud (Butunjahon Internet tarmog'idan foydalanish intensivligiga qarab).

DNS-serverning yozuv turlari. Bir nechta tarmoq manzillari bitta domenga mos kelishi mumkin, masalan, Internet sayti va pochta serveri. Bundan tashqari, har bir domen nomi bir yoki bir nechta subdomenlarni o'z ichiga oladi.

Domen va uning IP-manzillari o'rtasidagi barcha mosliklar DNS-serverdagi faylda saqlanadi, uning mazmuni DNS zonasi deb nomlanadi. DNS tizimiga ma'lumot kiritish uchun manba yozuvlarini ro'yxatdan o'tkazish kerak.

DNS-serverda saqlanadigan bir nechta asosiy turdagi yozuvlar mavjud:

- A - kiritilgan domen nomiga mos keladigan veb-resursning manzili.
- MX - pochta serveri manzili.
- CNAME - analogning o'zingizning domen nomingiz bilan bog'lanishini belgilaydi. Ko'pincha subdomenni biriktirish uchun ishlatiladi. Masalan, www.tuit.uz veb-manzilini tuit.uz domeni uchun haqiqiy saytga bog'lashingiz mumkin.

- NS - boshqa resurs yozuvlari tarkibiga mas'ul bo'lgan DNS-server manzili.
- TXT - domen haqidagi har qanday matnli ma'lumot.
- SPF - ko'rsatilgan domen nomidan xabar yuborishga ruxsat berilgan serverlar ro'yxatini ko'rsatuvchi ma'lumotlar.
- SOA - namunaviy domen nomlari haqidagi ma'lumotlarni o'z ichiga olgan server haqidagi ma'lumotlarni o'z ichiga olgan asl zona yozuvi.

Nima uchun DNS-serverlarni ro'yxatdan o'tkazishingiz kerak. Siz hozirda domenni ro'yxatdan o'tkazganingizni tasavvur qiling. Qolgan serverlarda sizning domeningiz borligi to'g'risida ma'lumot olish uchun siz resurs yozuvlarini ro'yxatdan o'tkazishingiz kerak. Birinchi qadam - domen uchun DNS-serverlarni sozlash va ro'yxatdan o'tkazish.

Ushbu formatdagi serverlar 24 soatgacha yangilanadi, shu vaqt ichida sayt ishlamay qolishi mumkin. Shuning uchun, ularni tayinlaganingizdan keyin bir kun kutishingiz kerak.

Ushbu serverlar ko'pincha juftlik bilan belgilanadi. Har bir domenda bitta asosiy va 12 tagacha ikkinchi darajali serverlar mavjud. Bu saytning ishonchliligini ta'minlash uchun kerak. Agar ulardan biri o'chib ketsa, domen va resurs ishlaydi.

DNS-serverlarni hujumlardan himoya qilish. Oxirgi vaqtlarda xakerlarning DNS-ga ta'sir qilish xavfi global bo'lib qoldi. Ilgari, ushbu formatdagi serverlarga hujumlar allaqachon sodir bo'lgan, bu Jahon Internet tarmog'ida, ayniqsa taniqli ijtimoiy tarmoqlarda ko'plab xatolarga olib keldi.

IP-manzil ma'lumotlarini saqlaydigan ildiz serverlarida eng xavfli hujumlar deb hisoblanadi. Masalan, 2002 yil oktyabr oyida 13 ta yuqori darajadagi serverlardan 10 tasiga DDoS hujumi tarixga kirdi.

DNS protokoli UDP foydalanuvchi datagram protokoli yordamida so'rovlar natijalarini oladi. Axborot xavfsizligi va yaxlitligini ta'minlash uchun UDP ulanishsiz ma'lumotlarni uzatish modelidan foydalanadi. Shunday qilib, ushbu protokolga qarshi hujumlarning aksariyati IP-manzillarni soxtalashtirish orqali amalga oshiriladi.

DNS-serverni xakerlik hujumlaridan himoya qilish uchun tuzilishi mumkin bo'lgan bir nechta sxemalar mavjud:

- *URPF (Unicast Reverse Path Forwarding) texnologiyasi.* Mazmuni shundan iboratki, ma'lum bir qurilmada ma'lumotlarni yuborish uchun ma'lum bir yuboruvchi manzili bo'lgan paketni qabul qilish imkoniyatini aniqlash. Qabul qilingan tarmoq interfeysi ushbu paketning manzili bilan ma'lumot almashish uchun mo'ljallangan bo'lsa, paket tekshiriladi va qabul qilinadi. Qarama-qarshi vaziyatda paket o'chiriladi. Ushbu usul soxta trafikni aniqlash va qisman tanlashga yordam beradi, ammo soxtalashtirishdan ishonchli himoyani kafolatlamaydi. URPF ma'lumotlar aniq manzilga aniq interfeys orqali yuborilishini taxmin qiladi. Agar bir nechta provayderlar paydo bo'lsa, vaziyat yanada murakkablashadi.

- *IP Source Guard funksiyasini qo'llash.* URPP texnologiyasi va DHCP paketlarini tekshirishga asoslangan. IP Source Guard Internetdagi DHCP trafigini kuzatib boradi va qabul qilingan tarmoq qurilmalarining IP manzillarini aniqlaydi. Bu o'rnatishning ba'zi portlarida soxta trafikni aniqlashga imkon beradi. Shundan so'ng, ma'lumotlar to'planadi va DHCP paketlarini tekshirish natijalarining umumiy jadvalida qayd etiladi. Keyinchalik, IP Source Guard ushbu jadvalga kalitni qabul qilgan paketlarni tekshirish uchun murojaat qiladi. Agar paketning IP-manzili manba manziliga to'g'ri kelmasa, u holda paket keyinga qoldiriladi.

- *dns-validator utilitasidan foydalanish.* Ushbu dastur barcha DNS-paketlarning uzatilishini nazorat qiladi, so'rovni javob bilan o'zaro bog'laydi va nomlar mos kelmasa, foydalanuvchiga xabarnoma yuboradi.

EMAIL.

Pochta serveri – elektron pochta xabarlarini yuboradigan va qabul qiladigan dastur. Pochta provayderi ko'plab pochta serverlariga ega bo'lgan va sizga pochta qutisini yaratishga imkon beradigan xizmatdir.

Biz uchun eng mashhur pochta provayderlari quyidagilar:

- Mail.ru;
- Gmail;
- Rambler;
- Yandex;
- Umail.uz;
- Inbox.uz.

Ular shaxsiy pochta qutilarini ham, korporativ qutilarini ham joylashtiradilar. Ushbu xizmatlar veb-mijozdan pochta xabarlariga kirishni ta'minlaydi.

Pochta serverlaridan kompaniya mijozlariga xatlarni ommaviy ravishda jo'natish uchun ham foydalaniladi. Biz yuqorida aytib o'tgan provayderlar ushbu maqsadlar uchun mos emas – ular faqat shaxsiy yozishmalarga ruxsat berishadi. Ommaviy yuborish uchun quyidagilar kabi pochta xizmatlaridan foydalaniladilar: UniSender, Mailchimp, GetResponse, E-Xat.

Pochta serveri qanday ishlaydi. Keling, pochta serveri qanday ishlashini oddiy misollar bilan ko'rib chiqamiz. Masalan, Gmail-dan Mail.ru-ga elektron pochta xabarini O'zbekistondan Frantsiyaga oddiy elektron pochta xabarlarini yuborish bilan taqqoslash mumkin.

Elektron pochta	Oddiy pochta
Siz elektron pochta xabarini yozasiz va "Yuborish" tugmasini bosasiz. Dastur xatni server tomoniga yuboradi.	Siz jismoniy xat yozasiz va uni qutiga tashlaysiz
Gmail.com pochta serveri xatni Mail.ru serveriga yuboradi.	Pochta aloqasi xodimlari konvertdagi manzilga qarab, yorlig'ini yozib, Frantsiyaga ko'plab xatlar bilan birga yuborishadi.
Mail.ru ushbu xat kimga tegishli ekanligini tanib oladi va xatni kerakli foydalanuvchiga yuboradigan dasturga uzatadi.	Fransiya pochtasi maktubni kimga yuborganingizni tanib oladi va pochtachi xatni oluvchining qutisiga olib keladi.
Xat sizning Kirish qutingizga (yoki Spam) tushadi va siz uni o'qiydiz.	Qabul qiluvchi xatni o'qiydi.

Faqat elektron pochta hamma narsa juda tez, avtomatik ravishda va odamlarning ishtirokisiz sodir bo'ladi.

Ommabop pochta serverlaridan tashqari (Mail.ru, Gmail) siz o'zingizning pochta serveringizni joylashtirishingiz mumkin.

O'z pochta serverlari ikki maqsadda ishga tushiriladi:

- kompaniyadagi elektron pochta xabarlar: mijozlar, sheriklar va kompaniyadagi xodimlar o'rtasida xatlarni qo'lda yuborish;
- mijozlarning manzillariga ommaviy pochta orqali yuborish.

O'zingizning pochta serveringiz – bu pochta jo'natish va qabul qilish, fayllarni uzatish, ommaviy xatlar yuborish uchun moslashuvchan ko'pkomponentli tizim. O'zingizning pochta serveringizning afzalliklari va kamchiliklari bor.

Ijobiy tomonlari.

Xavfsizlik. Gmail va Mail.ru pochta serverlari yirik veb-loyihalarning bir qismidir, ular pochtdan tashqari boshqa xizmatlarni o'z ichiga oladi: qidiruv tizimlari, ijtimoiy tarmoqlar, veb-masterlar uchun vositalar. Bepul pochta qutisini yaratish imkoniyati evaziga ular sizning ma'lumotlaringizdan reklama profillarini tuzish uchun foydalanadilar. Ma'lumki, sizning xatlaringizni hech kim o'qimaydi. Pochta algoritmlar bo'yicha tahlil qilinadi va shaxssiz foydalanuvchi profillari shakllanadi: 22 yosh, jins, ayol, qiziqishlar - masalan, dekorativ kosmetika va fantastika. Ammo ularning ismlari va shaxsiy ma'lumotlari yo'q.

Banklar, maxfiy xizmatlar va moliya institutlari ko'pincha xatlarni shifrlashadi, chunki ular ma'lumotlar xavfsizligi haqida qayg'uradilar va bu ma'lumotlarni pochta provayderlariga berishni xohlamaydilar. Shuning uchun ular o'zlarining serverlarini saqlab qolishadi.

Ammo Gmail yoki Mail.ru-ning xavfsizlik darajasi o'zingizning serveringiz va unga xizmat ko'rsatadigan bitta xodim bilan erishishingiz mumkin bo'lgan narsalarga qaraganda ancha kuchli. Shuning uchun, maxfiy ma'lumotlar bilan ishlaydigan yirik korporatsiyalar o'zlarining pochta serverlariga muhtoj, ammo hisob-fakturalarni pochta orqali yuboradigan va mijozlar bilan aloqa qiladigan kichik kompaniyalar – muhtoj emas.

Internetga ulanishda mustaqillik. Ma'lumotlar va pochta xabarlari ichki tarmoq orqali uzatiladi. Internet bo'lmasa ham, tarmoq ichidagi xatlarni yuborish va qabul qilish mumkin.

Trafikni tejash. Agar sizning xodimlaringiz bir-biriga ulkan fayllarni yuborishsa (masalan, 3D formatida ishlash uchun maxsus dasturlarda arxitektura inshootlarining to'liq o'lchamdagi modellari) va bunday xodimlar ko'p bo'lsa, siz o'zingizning pochta serveringizdagi fayllarni uzatish orqali trafikni tejashingiz mumkin.

Kamchiliklari.

Spam bilan kurashish. Spam-filtrlar, qora ro'yxatlar, to'g'ri yetkazib berish qobiliyati – sizning sysadmin-serveringiz buni kuzatib borishi va pochta serverini doimiy ravishda sozlashi kerak, chunki muhim elektron pochta xabarlarini o'tkazib yubormaslik va spamlarni blokirovka qilish kerak. Bundan tashqari, kompaniyaning IP-manzillari doimiy ravishda elektron pochta mijozlari tomonidan qora ro'yxatga olinadi. Xatlar oluvchilarga muammosiz etib borishi uchun, bu bilan ham kurashish kerak.

Doimiy ravishda qo'lda sozlash va qo'llab-quvvatlash. Pochta agentlari, spam-filtrlar, pochta serveridagi kalendarlar qo'lda saqlanishi kerak. Bundan tashqari, pochta serveri sizga veb-pochta dasturiga kirishni, ya'ni brauzer orqali kirishni ta'minlamaydi. Buni alohida sozlash kerak bo'ladi.

Pochtani saqlash uchun alohida xodim yoki autsorser. Maxsus bilimsiz pochta serverini boshqarish deyarli mumkin emas.

Agar biror narsa buzilsa, siz Gmail qo'llab-quvvatlash xizmatiga yozolmaysiz yoki ko'rsatmalarni o'qiy olmaysiz. Buni tuzatish uchun siz (yoki boshqa xodim) aniq nima va qanday tuzilganligini aniqlab olishingiz kerak bo'ladi.

FTP – fayl serveri.

Fayl serverining vazifalariga fayllarni saqlash va ularga shaxsiy kompyuterlar uchun, masalan, FTP orqali kirishni ta'minlash kiradi. Fayl-server resurslari tarmoqdagi barcha kompyuterlar uchun ochiq bo'lishi yoki identifikatsiya tizimi va kirish huquqlari bilan himoyalangan bo'lishi mumkin.

Vizual taqdimot tizimga kirganingizga bog'liq. Ma'lumotlar odatiy Total Commander shaklida namoyish etiladigan FileZilla kabi maxsus dasturlar mavjud.

Ko'plab xosting xizmatlari o'zlarining boshqaruv tizimiga ega; shuningdek, tanish papkalar va fayllar to'plamiga o'xshaydi.

FTP-ning asosiy vazifasi fayllarni uzatishdir.

Ma'lumotni to'ldirish va tushirishdan tashqari, fayllar va kataloglarni boshqarish uchun turli xil buyruqlar mavjud:

- Autentifikatsiya talab qilinadi.
- Har bir ulanish uchun ajratilgan kanal mavjudligi.
- Ma'lumotlarni uzatishning 2 rejimini qo'llab-quvvatlash: matnli va ikkilik. Ikkinchi variant vaqtni va trafikni qisqartiradi.
- Kamida ikki kanalli bir nechta ulanishlardan foydalanish. Birinchidan, boshqaruv buyruqlari uzatiladi va qayta ishlangan javoblar qaytariladi. Boshqalarning yordami bilan fayllarni uzatish har biri uchun ajratilgan kanal stavkasi bo'yicha amalga oshiriladi.

Serverga kirish uchun avtorizatsiya shaklini to'ldirishingiz kerak, boshqacha qilib aytganda autentifikatsiyadan o'tishingiz kerak. Kirish (foydalanuvchi) va parol (o'tish) kiritilgandan so'ng ushbu ma'lumotlar tizimga o'tkaziladi. Agar u qabul qilinsa, mijoz taklifnoma oladi va ish sessiyasi ochiladi.

Ro'yxatdan o'tish ma'lumotlarini ko'rsatmasdan kiritish uchun imkoniyatlar mavjud. Bunday holda, mehmon uchun mavjud bo'lgan imkoniyatlar cheklangan bo'ladi.

FTP-serverga kirish uchun yana bir variant mavjud – anonim kirish. Odatiy bo'lib, kirish "anonim" kirishda kirganda yuz beradi, imlo harflar bilan farq qilishi mumkin. Biroq, elektron pochta manzilidan foydalanib kirishni taklif qilishning eng keng tarqalgan usuli. Ushbu kirish opsiyasi dasturiy ta'minot yangilanishlarini yuboradigan ko'plab FTP-xostlar tomonidan qo'llaniladi.

Ulanish uchun siz veb-brauzerdan yoki Total Commander, FileZilla kabi fayl menejerlaridan foydalanishingiz mumkin. Fayllarni

brauzer orqali ko'rishingiz va yuklab olishingiz mumkin, ammo siz o'zgartirish kiritolmaysiz.

FileZilla mijoz dasturi orqali ishlash qulayroq (uni erkin yuklab olishingiz mumkin).

Biz yangi ulanishni quyidagicha yaratamiz:

"Xost" maydoniga ftp-server manzilini kiritamiz.

"Foydalanuvchi nomi", "Parol" va kerak bo'lganda "Port" maydonlarini to'ldiramiz.

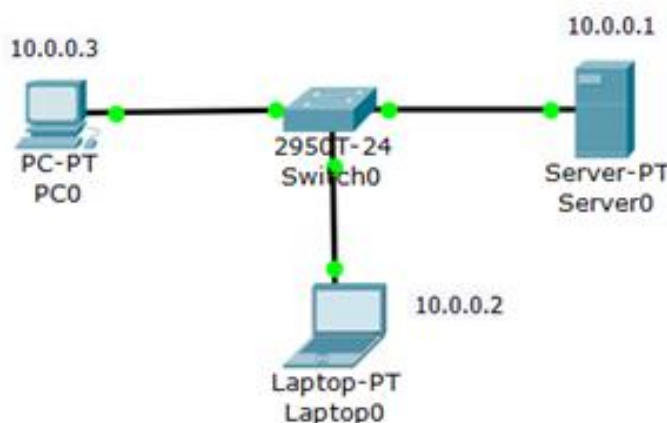
O'g'rilik va hujumlardan zaif himoya. Texnik xususiyatlar tufayli nafaqat serverlar, balki mijozlar ham zarar ko'rishi mumkin. Shuning uchun maxfiy ma'lumotlar ularda saqlanmasligi kerak.

Ma'lumotlarni uzatish paketining manbasini tasdiqlash mavjud emas, bu DDoS hujumlari zaifligiga olib keladi.

3. Vazifa

3.1. VEB-serverni sozlaymiz.

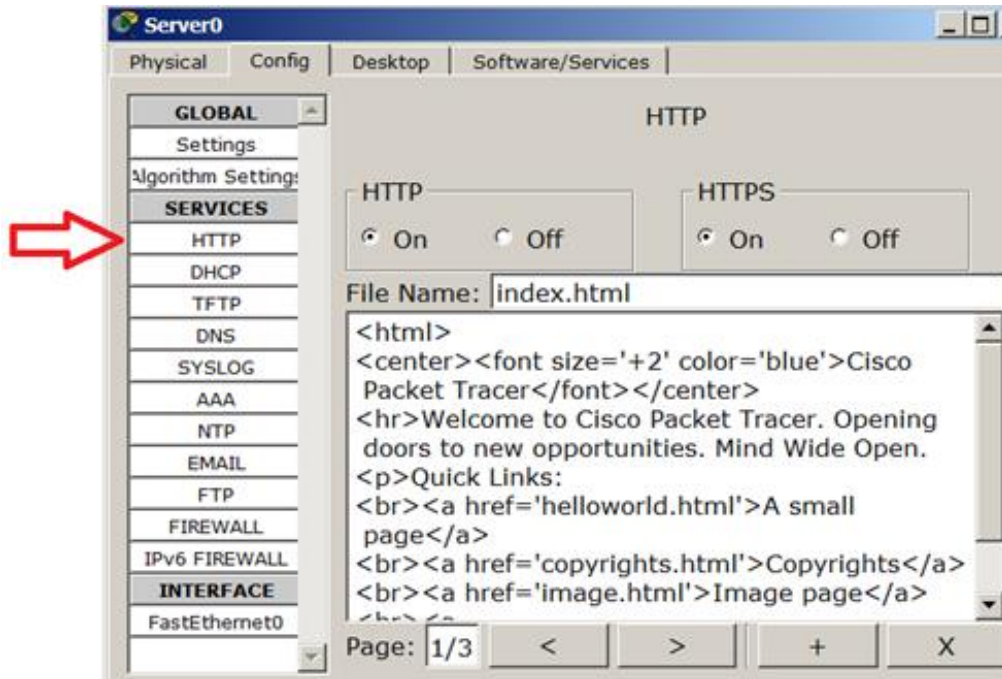
Veb-serverni sozlash uchun tarmoq sxemasi 6.2-rasmda keltirilgan.






2-rasm. Tarmoq sxemasi

Serverda VEB hujjatni yaratamiz

HTTP serverini yaratish uchun serverda HTTP yorlig'ini oching va saytning index.html nomli birinchi sahifasini tahrirlang. HTTP xizmatini On tugmasi bilan yoqing (6.3-rasm).



3-rasm. Config oynasi, HTTP serveri xizmati

Eslatma. Ushbu oynada  tugma bilan yangi sahifa qo'shishingiz yoki  tugma bilan mavjud sahifani o'chirishingiz mumkin. Bir nechta varaqlarni almashtirish  tugmalar yordamida amalga oshiriladi.

html kod oynasida *index.html* saytining birinchi sahifasining matnini yarating. 1-variant (6.4-rasm). *Har bir talaba kamida uchta sahifadan iborat o'z veb-saytini yaratadi.*

```
<html>
<body>
<h1>Welcome to WEB-Server CISCO!</h1>
<p>Server working: <font color="red"><b>OK!</b></font></p>
</body>
```

</html>



4-rasm. Web-sahifa matni, 1-variant

Yoki 2-variant (5-rasm).

<html>

<center>Welcome to Cisco Packet

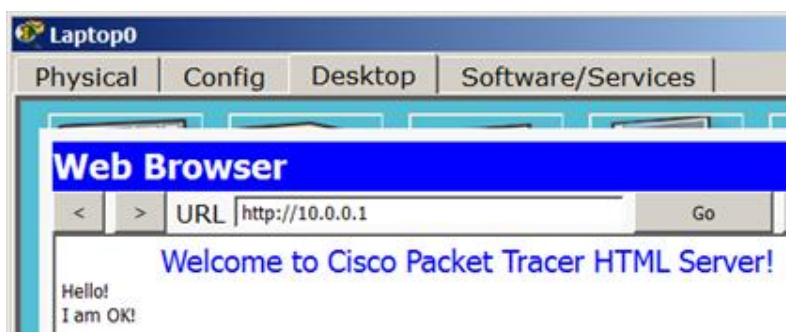
Tracer HTML Server! </center>

<body>

Hello!
I am OK!

</body>

</html>



5-rasm. Web-sahifa matni, 2-variant

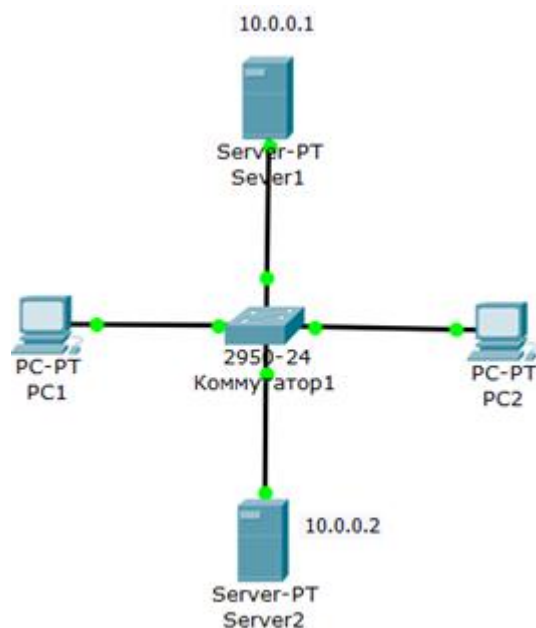
Maslahatlar. Matn ushbu oynaga almashish buferi orqali uzatilishi mumkin. Bu faqat ingliz tilida bo'lishi mumkin.

Serverimizning ish faoliyatini tekshirish uchun mijoz mashinasini (10.0.0.2 yoki 10.0.0.3) oching va ish stolida web-brauzer dasturini ishga

tushiring. Keyin biz WEB-serverimiz 10.0.0.1 manzilini yozamiz va GO tugmasini bosim. Veb-serverimiz ishlayotganiga ishonch hosil qiling.

3.2. DNS, DHCP va WEB tarmoq xizmatlarini sozlash

6.6-rasmda ko'rsatilgan tarmoq sxemasini yarating.

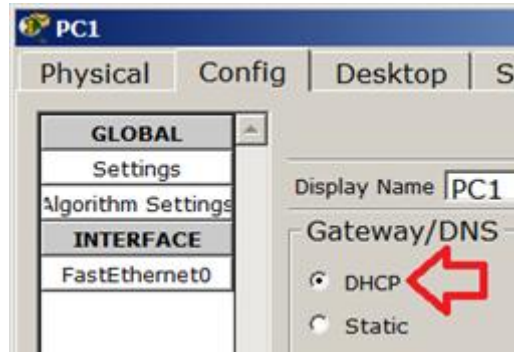


6-rasm. Tarmoq sxemasi

Bizning vazifamiz Server1 ni DNS va veb-server sifatida va Server2-ni DHCP-server sifatida sozlash. Sizga shuni eslatib o'tamizki, DNS serverining vazifasi serverlarning domen nomlarini IP manzillariga tarjima qilishdir. DHCP server tarmoq interfeyslarini avtomatik konfiguratsiya qilish uchun pullarni tashkil qilish imkonini beradi, ya'ni tarmoqdagi kompyuterlar o'rtasida IP manzillarini avtomatik ravishda taqsimlashni ta'minlaydi. Boshqacha qilib aytganda, bizning holatlarimizda, kompyuterlar DHCP Server2 xizmati tufayli IP manzillarini olishadi va masalan, Server1-da veb-sayt ochishadi.

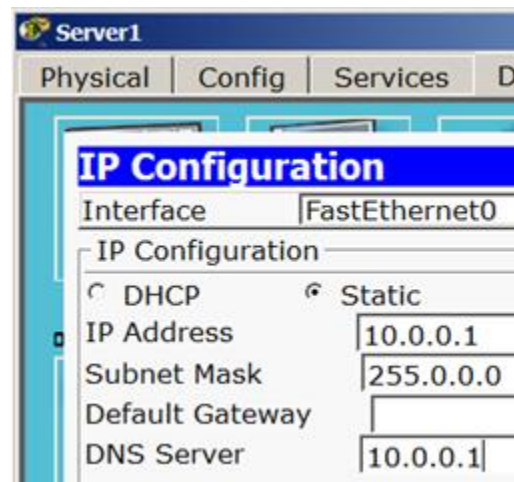
Kompyuterda serverlarning va DHCP-ning IP manzillarini sozlaymiz.

PC1 va PC2 konfiguratsiyasiga kiring va DHCP server orqali IP-ni sozlang (6.7-rasm).

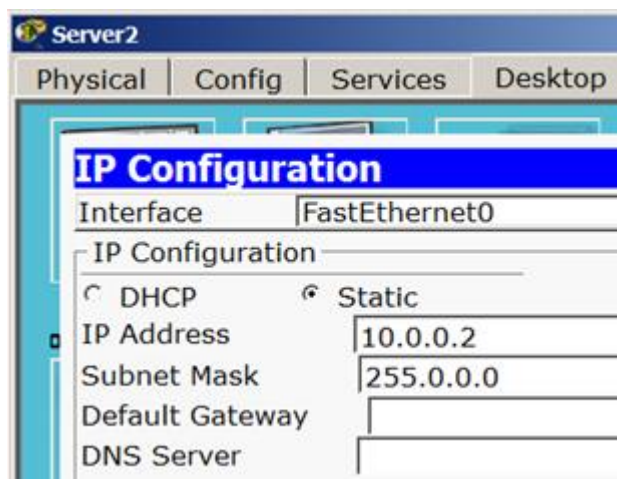


7-rasm. PC1-da IP-ni sozlash

Server konfiguratsiyasida IP sozlamalarini o'rnatish: Server1 – 10.0.0.1 (8-rasm), Server2 – 10.0.0.2 (9-rasm). Ichki tarmoq maskasi avtomatik ravishda 255.0.0.0 sifatida o'rnatiladi.



8-rasm. Server1 da IP sozlamalarini o'rnatish



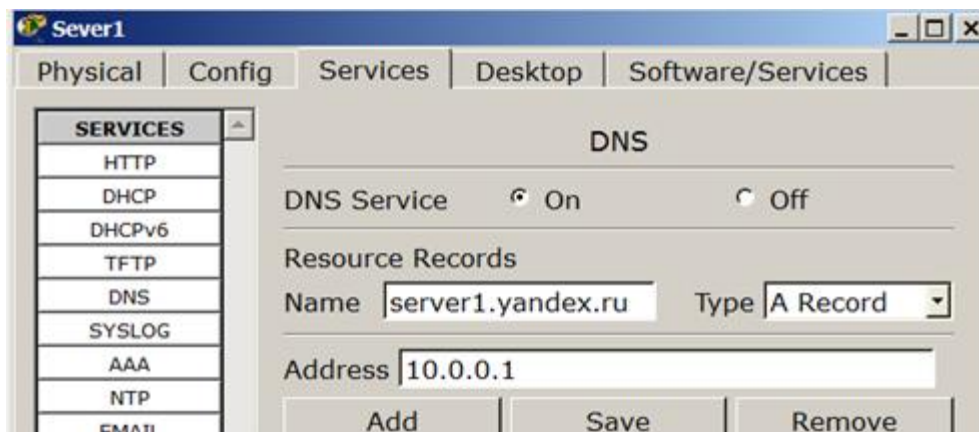
9-rasm. Server2 da IP sozlamalarini o'rnatish

Server1-da DNS va HTTP xizmatlarini sozlash.

Server1 konfiguratsiyasida DNS yorlig'iga o'ting va oldinga yo'naltirilgan DNS zonasida ikkita Resurs yozuvini (Resource Records) aniqlang.

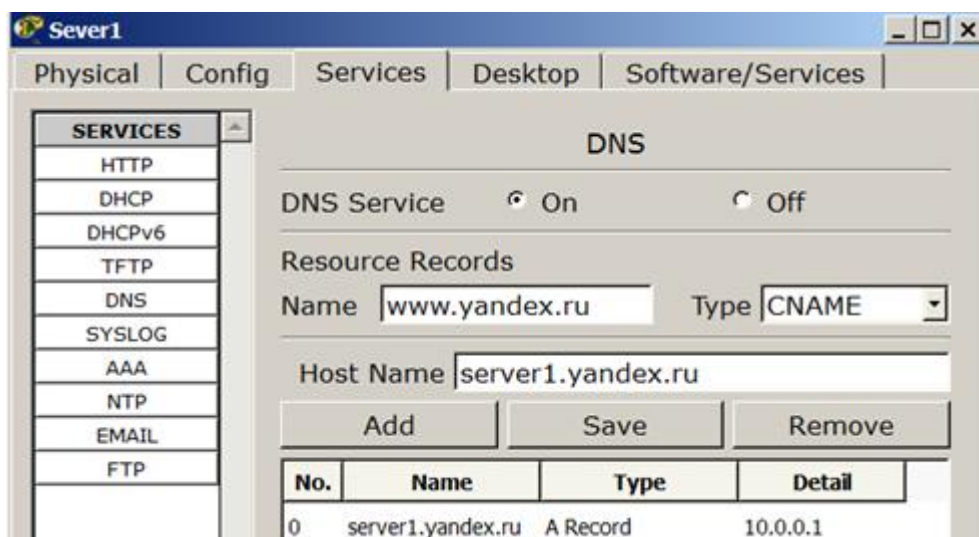
Yangi atama. **DNS zonasi** – butun domen nomi serverida (DNS serverida) joylashtirilgan domen nomi daraxtining qismi (resurs yozuvlari bilan birga). To'g'ridan-to'g'ri izlash zonasida domen nomi so'roviga IP-manzil shaklida javob beriladi. IP orqali teskari qidiruv zonasida biz kompyuterning domen nomini topamiz.

Birinchidan, A Record tipidagi manbali yozuvda server1.yandex.ru kompyuterining domen nomini uning 10.0.0.1 IP-manzili bilan bog'lang va *Add* ("Qo'shish") tugmachasini bosing va *On* ("Yoqish") -ni yoqing (6.10-rasm).



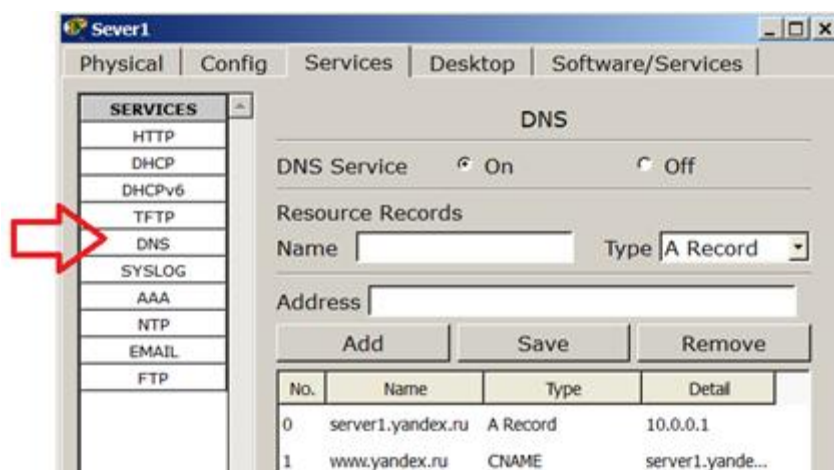
10-rasm. A Record tipidagi manbalar yozuvini kiritish

Keyinchalik, *CNAME* turidagi resurs yozuvida sayt nomini server bilan bog'lang va *Add* ("Qo'shish") tugmachasini bosing (6.11-rasm).



11-rasm. CNAME resurs yozuvini kiritish

Natijada quyidagilar bo'lishi kerak (12-rasm).



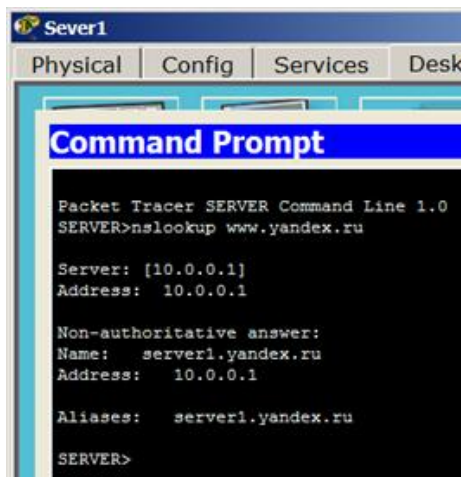
12-rasm. To'g'ridan-to'g'ri zonada DNS xizmati

Endi HTTP xizmatini sozlaylik. Server1 konfiguratsiyasida HTTP yorlig'iga o'ting va sayt uchun boshlang'ich sahifani yarating (6.13-rasm).

```
<html>
<center><font size='+2' color='green'>Web Server</font></center>
www.yandex.ru
<p>
Hello!<br/>I am Server1
</html>
```

13-rasm. Saytning bosh sahifasi

Server1-da buyruq so'rovini yoqing va DNS xizmatini sinab ko'ring. To'g'ridan-to'g'ri DNS server zonasi to'g'ri ishlayotganligini tekshirish uchun *SERVER>nslookup* -ni kiriting. Agar hamma narsa to'g'ri sozlangan bo'lsa, siz tarmoqdagi DNS serverining domen nomini va uning IP-manzilini ko'rsatgan holda so'rovga javob olasiz (14-rasm).

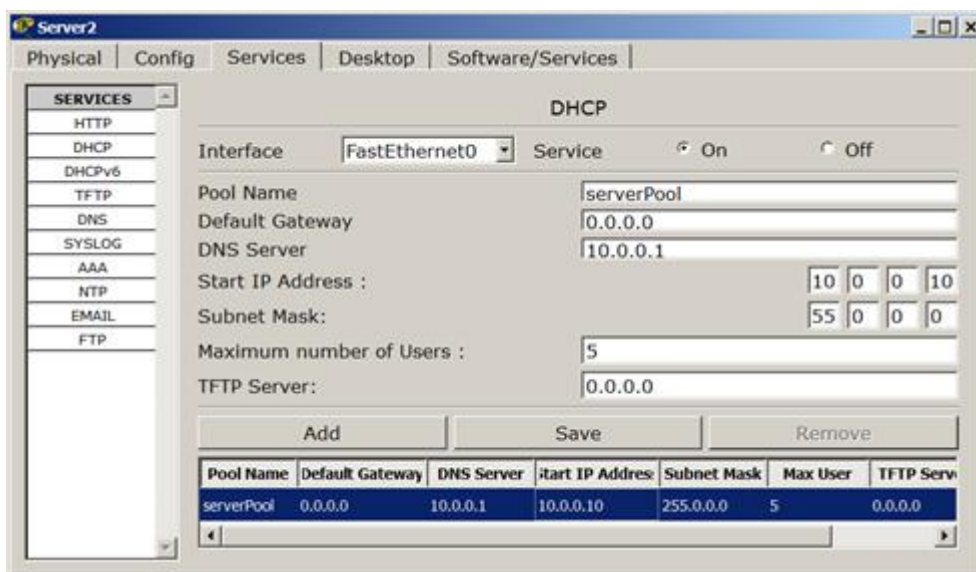


14-rasm. Server1-da to'g'ridan-to'g'ri DNS zonasida DNS xizmati to'g'ri sozlangan

Eslatma. nslookup buyrug'i IP manzilini domen nomi bo'yicha aniqlash uchun ishlatiladi (va aksincha).

Server2-da DHCP xizmatini sozlash.

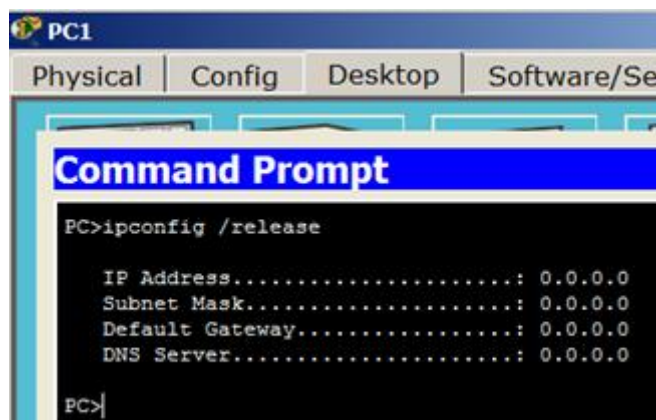
Server2 konfiguratsiyasiga kiring va DHCP yorlig'ida DHCP xizmatini sozlang. Buning uchun pulning yangi qiymatlarini kiriting, *On* tugmachasini o'rnatib va *Save* (Saqlash) tugmachasini bosib (6.15-rasm).



15-rasm. DHCP serverni sozlash.

Mijozlar ishini tekshirish.

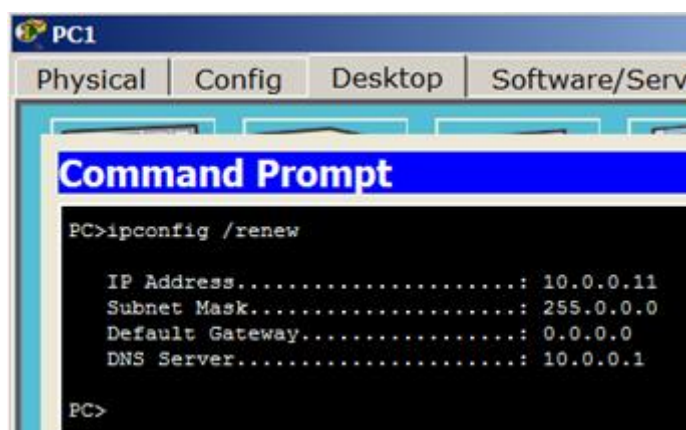
PC1 va PC2 konfiguratsiyasiga kiring va buyruqlar qatorida TCP/IP protokolini sozlang. Buning uchun eski IP-manzil parametrlarini tiklash (tozalash) uchun *PC> ipconfig /release* buyrug'idan foydalaning (15-rasm).



15-rasm. Barcha adapterlar uchun IP-konfiguratsiyani olib tashlash

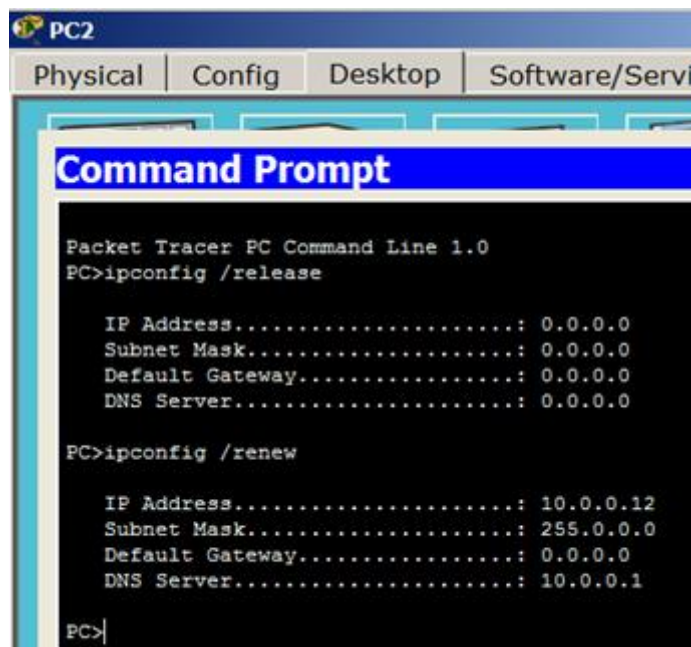
Eslatma. *ipconfig/release* buyrug'i DHCP serveriga joriy DHCP konfiguratsiyasini chiqarish va barcha adapterlar uchun IP-manzil konfiguratsiyasini o'chirish uchun DHCP RELEASE xabarini yuboradi (agar adapter ko'rsatilmagan bo'lsa). Ushbu kalit IP manzillarini avtomatik ravishda olish uchun sozlangan adapterlar uchun TCP/IP protokolini o'chiradi.

Endi *PC>ipconfig/renew* buyrug'i yordamida DHCP serveridan yangi parametrlarni oling (17-rasm).



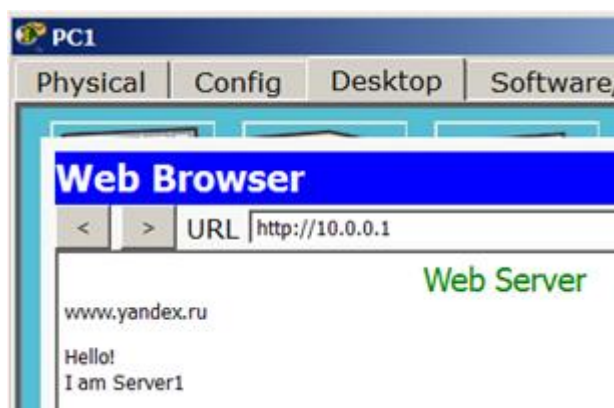
17-rasm. DHCP serveridan TCP/IP mijoz protokoli konfiguratsiyasi

PC2 uchun ham xuddi shunday qiling (18-rasm).



18-rasm. PC2 DHCP server Server2-dan IP-manzilga ega bo'ldi

WEB server Server1 ishini tekshirish va saytni PC1 yoki PC2 brauzerida ochish qoladi (19-rasm).



19-rasm. Server1-da HTTP xizmatini sinab ko'rish

3.3. Email va FTP serverlarini o'zingiz sozlang.

4. Hisobot tarkibi

Hisobotda quyidagilar keltirilishi lozim:

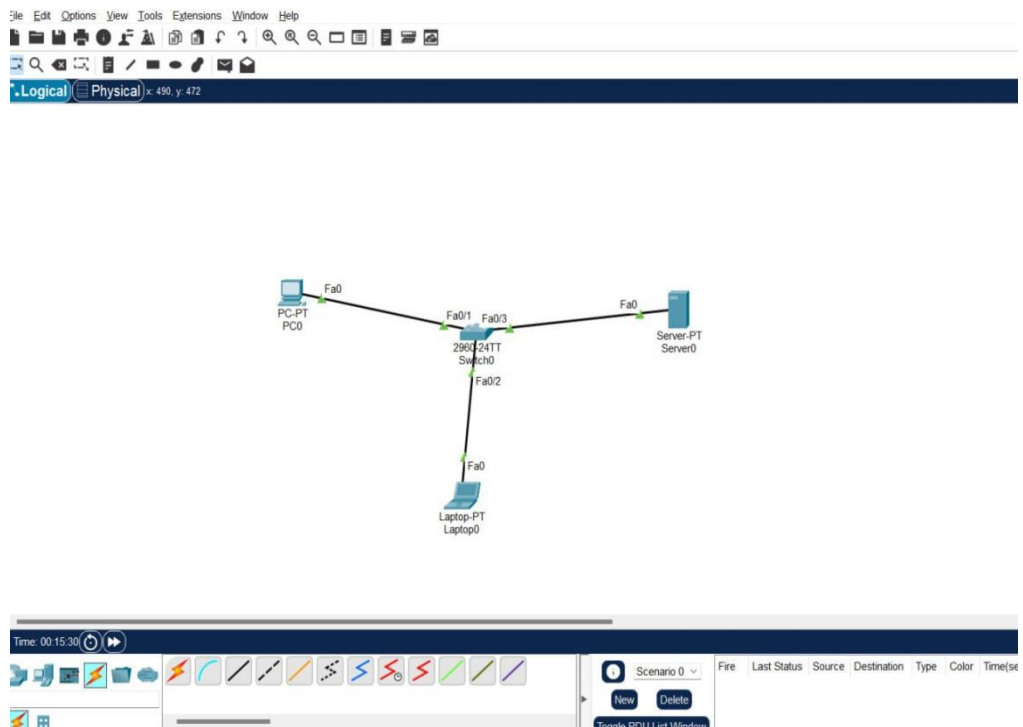
- Ishning nomi va maqsadi.
- Ishni bajarilganligini ko'rsatuvchi "screen shot" lar.
- Ishning natijasi.
- Nazorat savollariga qisqacha javoblar.

5. Nazorat savollari

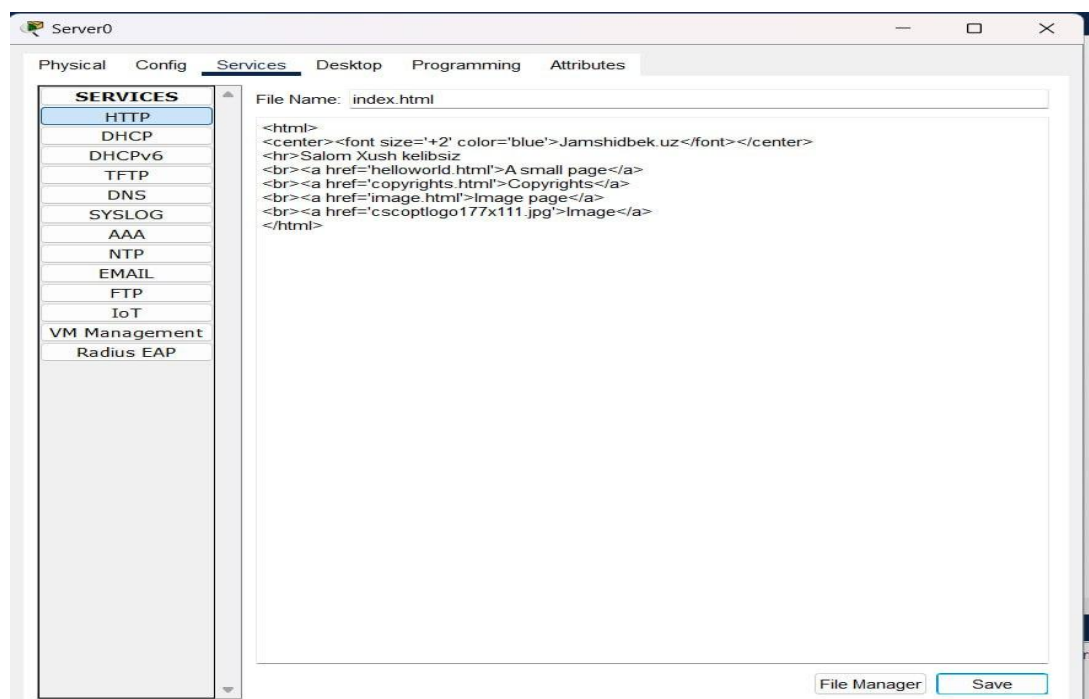
1. Web serverning ishlash tamoyillarini aytib bering.
2. DNS serverning ishlash tamoyillarini aytib bering.
3. DHCP serverning ishlash tamoyillarini aytib bering.
4. FTP serverning ishlash tamoyillarini aytib bering.
5. Email serverning ishlash tamoyillarini aytib bering.

AMALIYOT ISHI № 13

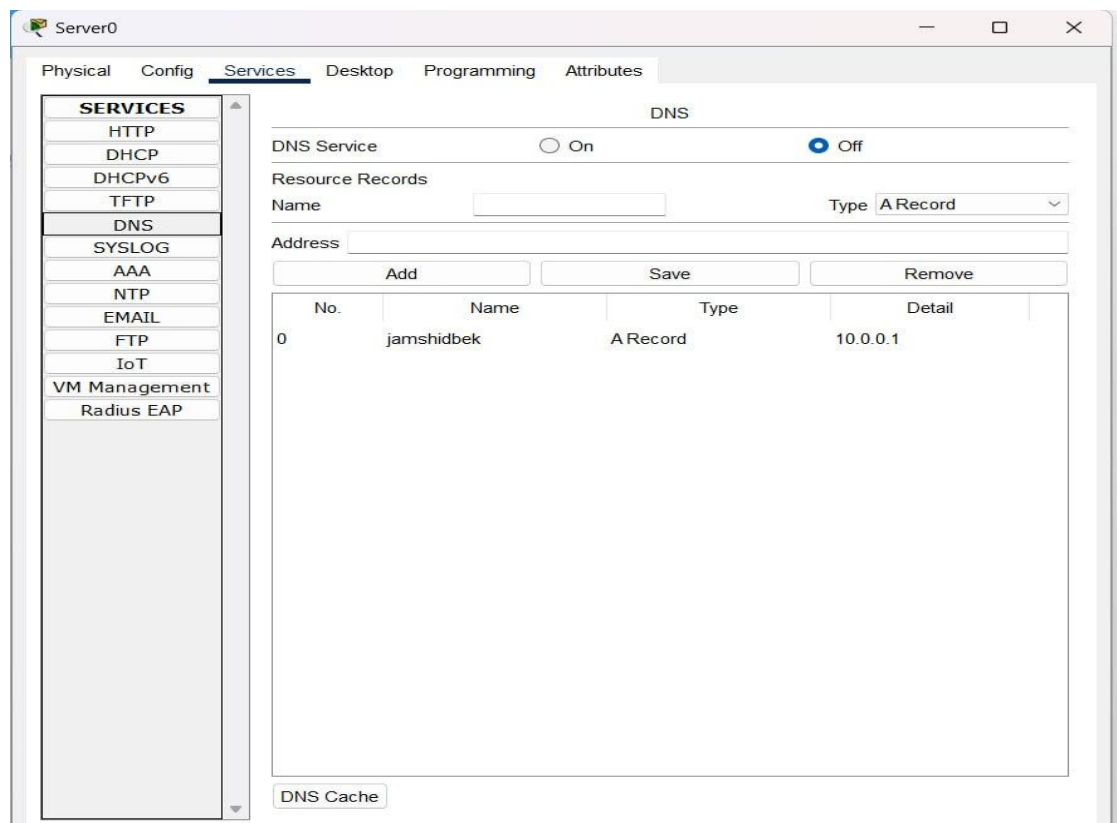
Bajarilgani:



Topologiyaning tuzulishi



Config oynasi, HTTP serveri xizmati



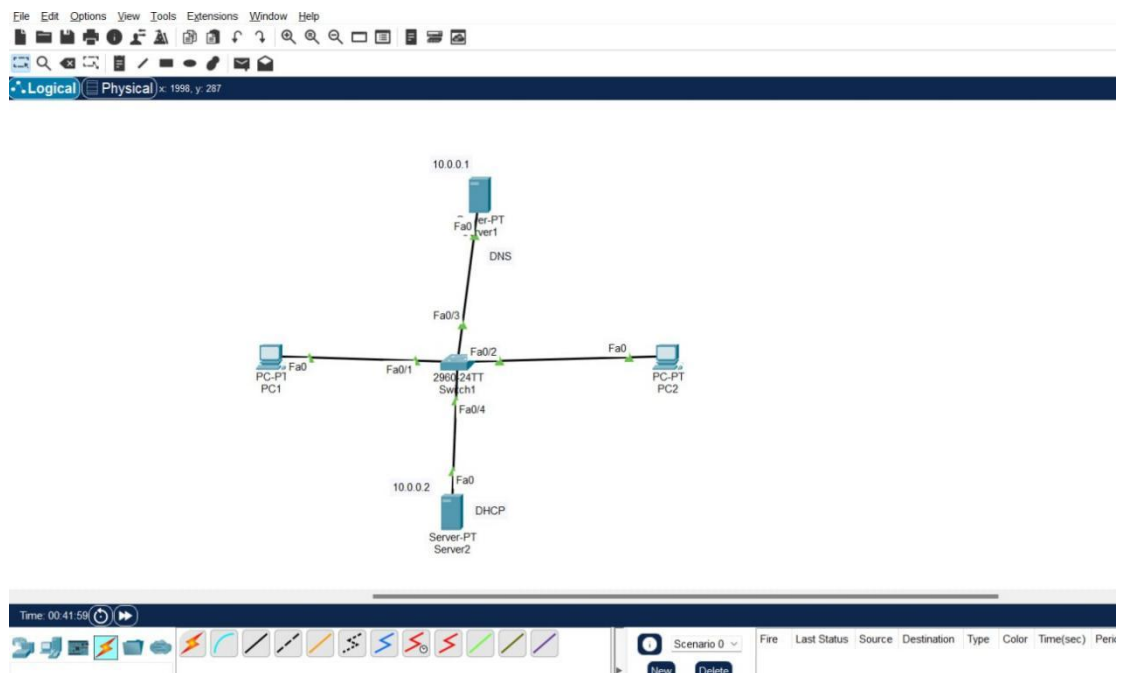
DNS serverda web sahifa yaratish



Web-sahifa matni

AMALIYOT ISHI № 14

Bajarilgani:



Topologiya tuzulishi

Server1

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 10.0.0.1

Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::201:96FF:FE99:326

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Serverga Statik 1ga ip berish jarayoni

Server2

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 10.0.0.2

Subnet Mask 255.0.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::210:11FF:FED0:ADE3

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

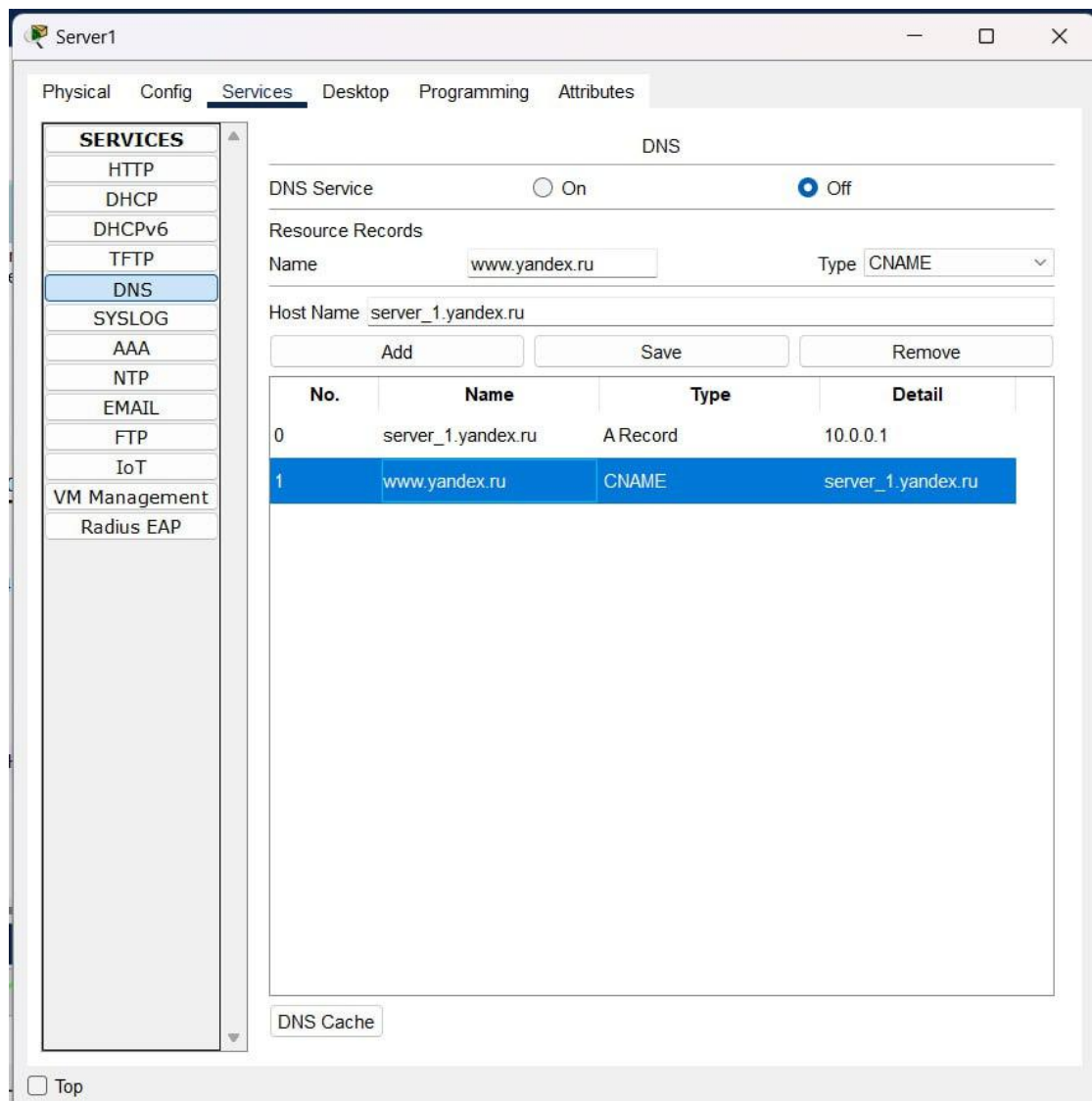
Authentication MD5

Username

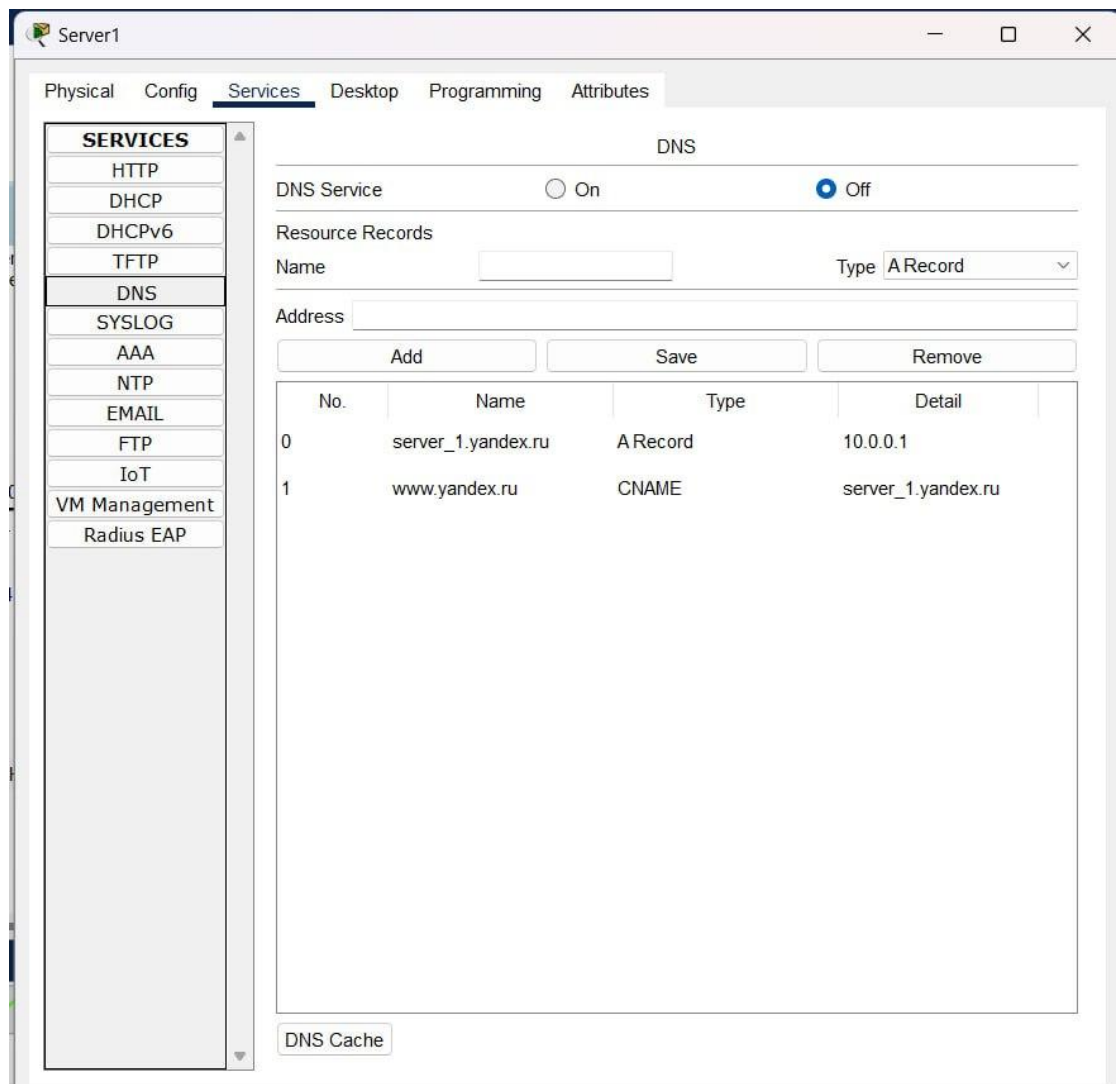
Password

☐ Top

Serverga Statik 2ga ip berish jarayoni



A Record tipidagi manbalar yozuvini kiritish va
CNAME resurs yozuvini kiritish



To'g'ridan-to'g'ri zonada DNS xizmati

Server2

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

InterfaceFastEthernet0ServiceOnOff

Pool NameJamshidbek

Default Gateway0.0.0.0

DNS Server10.0.0.1

Start IP Address : 100010

Subnet Mask: 255000

Maximum Number of Users : 5

TFTP Server: 0.0.0.0

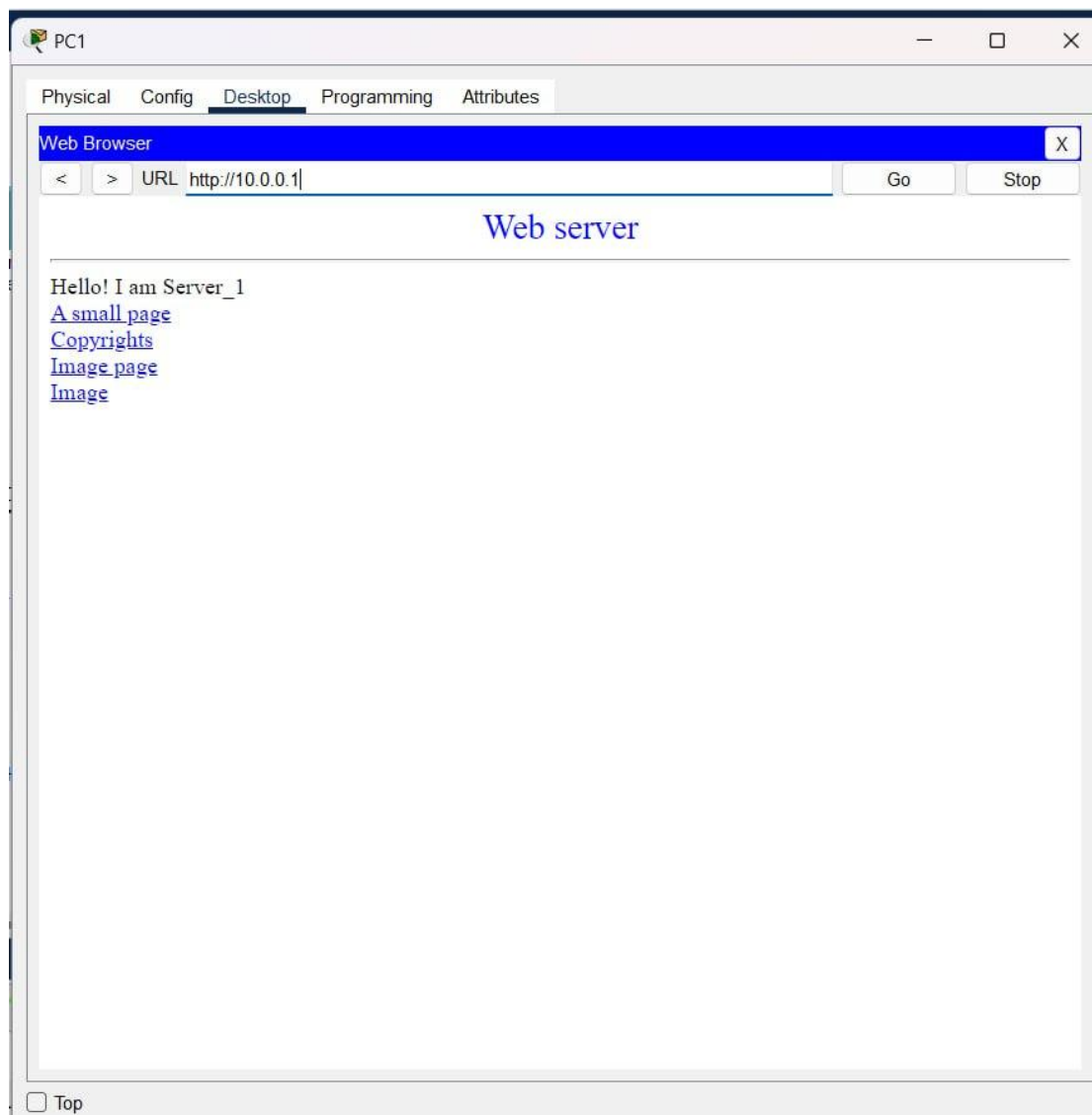
WLC Address: 0.0.0.0

AddSaveRemove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Jamshidbek	0.0.0.0	10.0.0.1	10.0.0.10	255.0.0.0	5	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.0.0.0	255.0.0.0	512	0.0.0.0	0.0.0.0

☐ Top

DHCP serverni sozlash.



Server1-da HTTP xizmatini sinab ko'rish

AMALIYOT ISHI № 15

KORPORATIV TARMOQLARNI LOYIHALASH

1. Ishning maqsadi

Ushbu laboratoriya ishidan maqsad quyidagilar hisoblanadi:

- Kichik korporativ tarmoqlarni sozlash bo'yicha ko'nikmalarga ega bo'lish;
- Katta korporativ tarmoqlarni sozlash bo'yicha ko'nikmalarga ega bo'lish.

2. Qisqa nazariy ma'lumotlar

Korporativ tarmoq – bu asosiy maqsadi muayyan korxona yoki tashkilotning ishi va ichki jarayonlarini imkon qadar samarali, yergonomik va xavfsiz qilishdir.

Korporativ tarmoq xizmatlarining iste'molchisi faqat shu korxona xodimlaridir. Tashkilot ichidagi murakkablik, struktura va ierarxik bo'linish korxonaning o'z ko'lami va u hal qiladigan vazifalarning murakkabligi bilan belgilanadi.

Muayyan korxonada korporativ tarmoqni amalga oshirish masalasi barcha ish jarayonlari va ichki texnik va inson kommunikatsiyalarini jiddiy tadqiq qilish va tahlil qilish asosida ko'tarilishi kerak. Ichki tarmoqni tashkil yetish uchun sarflangan mablag'lar va sa'y-harakatlar korxonaning mexanizmlari va maqsadlarini tushunishga noprofessional, yuzaki yondashuv tufayli to'lanmaydigan holatlar tez-tez uchrab turadi.

Korxonada korporativ tarmoq salohiyatidan oqilona foydalanish quyidagi afzalliklarni ta'minlaydi:

- Kuchli, lekin avtonom hisoblash qurilmalari mavjudligida yerishib bo'lmaydigan parallel hisoblash jarayonlarini malakali tashkil yetish tufayli mehnat unumdorligining aniq o'sishi .
- Tizimning alohida yelementlarining uzilishlari va uzilishlariga qarshilik bu yelementlar bitta tarmoqqa birlashtirilsa ancha kam og'riqli o'tkaziladi.
- Har xil turdagi tarmoq axborot vositalari to'g'risidagi ma'lumotlarni takrorlanishi, so'rov va jarayonlarni ishchan segmentlarga o'tish ichki tarmoq, dinamik va statik qayta konfiguratsiya imkoniyatlari-bu korporativ tarmoqdan uzilishlar holatlarida foydalanishdir.
- Bir necha tezlashtirish va ichki tarmoq aloqa yengillashtirish. Bir vaqtning o'zida ko'plab turli vazifalarni bajarish, umumiy natijaga yerishish maqsadida, tashkilotning turli tuzilmalari va bo'linmalari o'rtasida uzluksiz aloqa o'rnatilganda sezilarli darajada soddalashtiriladi.
- Tijorat va texnik xavfsizlikni nazorat qilish, muhim korporativ ma'lumotlarni himoya qilish bir vaqtning o'zida barcha dasturiy ta'minot va apparat yelementlari va atrof-muhit qurilmalariga kirish imkonini beradi.

Ishlab chiqarish xarajatlarini kamaytirish, mijozlarga xizmat ko'rsatish so'rovlarini jadallashtirish va yangi mahsulotlarni ishlab chiqish va amalga oshirishni qisqartirish korporativ tarmoqning samarali va malakali qurilayotganidan dalolat beradi.

Korporativ tarmoq- asosiy maqsadi ushbu tarmoqqa ega bo'lgan muayyan korxonaning ishlashini ta'minlashdir. Korporativ tarmoq foydalanuvchilari faqat ushbu korxona xodimlari hisoblanadi. Aloqa operatorlari tarmoqlaridan farqli o'laroq, korporativ tarmoqlar, umuman, boshqa tashkilotlarga yoki foydalanuvchilarga xizmat ko'rsatmaydi.

Korxonaning hajmiga, shuningdek, hal qilinadigan vazifalarning murakkabligi va xilma – xilligiga qarab, bo'lim tarmoqlari, kampus tarmoqlari va korporativ tarmoqlar (bu tasnifdagi "korporativ" atamasi tor ma'noga ega-katta korxona tarmog'i) turlarga ajratiladi. Ushbu turdagi tarmoqlarning har birining o'ziga xos xususiyatlarini muhokama qilishdan oldin, korxonalarni o'z kompyuter tarmog'iga ega bo'lishiga olib keladigan omillarga e'tibor qaratamiz.

Tarmoqlardan foydalanish afzalliklari

1. Integral afzallik-korxonaning ish samaradorligini oshirish.
2. Parallel hisob-kitoblarni amalga oshirish imkoniyati , buning natijasida ishlash va xatolarga chidamlilik kuchayishi mumkin.
3. Ba'zi amaliy vazifalarning taqsimlangan arxitekturasiga mos keladi.
4. Ma'lumotlar va qurilmalardan birgalikda foydalanish imkoniyati.
5. Tizim bo'ylab ishlarni moslashuvchan taqsimlash imkoniyati.
6. Keng korporativ ma'lumotlarga tezkor kirish.
7. Kommunikatsiyalarni takomillashtirish.

Muammolar

1. Taqsimlangan tizimlar uchun tizim va dasturiy ta'minotni ishlab chiqish murakkabligi.
2. Tarmoq orqali ma'lumotlarni uzatishning ishlashi va ishonchliligi bilan bog'liq muammolar.
3. Xavfsizlik muammosi.

Albatta, kompyuter tarmoqlaridan foydalanishda, asosan, taqsimlangan tizimlarning alohida qismlarining samarali o'zaro ta'sirini tashkil qilish bilan bog'liq muammolar mavjud.

Birinchidan, bu dasturiy ta'minotdagi muammolar: operatsion tizimlar va ilovalar. Taqsimlangan tizimlar uchun dasturlash markazlashtirilgan tizimlar uchun dasturlashdan tubdan farq qiladi. Shunday qilib, tarmoq operatsion tizimi, umuman olganda, kompyuterning mahalliy resurslarini

boshqarish uchun barcha funktsiyalarni bajaradi, bundan tashqari, tarmoq xizmatlarini taqdim etish bilan bog'liq ko'plab muammolarni hal qiladi. Tarmoq dasturlarini ishlab chiqish turli xil mashinalarda ishlaydigan qismlarning birgalikda ishlashini tashkil qilish zarurati tufayli murakkablashadi. Ko'p muammolar tarmoq tugunlarida o'rnatilgan dasturiy ta'minotlarningning mosligini ta'minlash bilan ham bog'liq.

Ikkinchidan, kompyuterlar orasidagi aloqa kanallari orqali xabarlarni tashish bilan bog'liq ko'plab muammolar mavjud. Bu erda asosiy vazifalar ishonchlilikni ta'minlash (uzatilgan ma'lumotlar yo'qolmasligi va buzilmasligi uchun) va ishlash (ma'lumotlar almashinuvi maqbul kechikishlar bilan amalga oshirilishi uchun) jarayonini ta'minlashdir. Hisoblash tarmog'ining umumiy xarajatlari tarkibida "transport masalalari" ni hal qilish xarajatlari muhim ahamiyatga ega, markazlashtirilgan tizimlarda esa bu muammolar umuman yo'q.

Uchinchidan, bu kompyuter tarmog'ida avtonom ishlaydigan kompyuterga qaraganda ancha murakkab bo'lgan xavfsizlikni ta'minlash bilan bog'liq masalalar. Ba'zi hollarda, xavfsizlik ayniqsa muhim bo'ladigan hollarda, tarmoqdan foydalanishdan voz kechish yaxshiroqdir.

Ko'plab "afzalliklar" va "qarshiliklarni" sanash mumkin, ammo tarmoqlardan foydalanish samaradorligining asosiy dalili ularning keng tarqalganligida namoyon bo'ladi. Bugungi kunda shaxsiy kompyuterlarning kamida bitta segmentli tarmog'i bo'lmagan korxonani topish qiyin; yuzlab ish stantsiyalari va o'nlab serverlari mavjud ko'plab tarmoqlar mavjud bo'lib, ba'zi yirik tashkilotlar minglab kilometr masofadagi filiallarini birlashtiradigan xususiy global tarmoqlarga ega. Har bir alohida holatda, tarmoq yaratish uchun asoslar bor edi, lekin umumiy holat ham borligi to'g'ri: bu tarmoqlarni qurishda aniq bir maqsad bor.

Bo'lim tarmoqlari

Bo'lim tarmoqlari-korxonaning bir bo'limida ishlaydigan nisbatan kichik xodimlar guruhi tomonidan foydalaniladigan tarmoqlar. Ushbu xodimlar umumiy muammolarni hal qilishadi, masalan, buxgalteriya hisobi yoki marketing bilan shug'ullanadi. Bo'lim 100-150 xodimlarga ega hajmda bo'lishi mumkin, deb hisoblashadi.

Bo'lim tarmog'ining asosiy maqsadi ilovalar, ma'lumotlar, lazer printerlari va modemlar kabi tarmoq resurslarini ajratishdir. Odatda bo'lim tarmoqlari bitta yoki ikkita fayl serveriga ega, o'ttizdan ortiq foydalanuvchi yo'q (shakl. 9.8) va pastki tarmoqlarga bo'linmaydi. Ushbu tarmoqlarda korxona trafikining katta qismi mahalliyashtirilgan. Bo'lim tarmoqlari odatda bitta tarmoq texnologiyasi-Ethernet, Token Ring asosida yaratilgan. Bunday tarmoq ko'pincha bir yoki maksimal ikki turdagi operatsion tizimlardan foydalanadi. Foydalanuvchilarning oz miqdori Windows 98 kabi peer-to-peer tarmoq OS lardan bo'lim tarmoqlarida foydalanish imkonini beradi.



Bo'lim tarmog'i namunasi

Bo'lim doirasi tarmog'ining namunasi

Bo'lim darajasida tarmoqni boshqarish vazifalari nisbatan sodda: yangi foydalanuvchilarni qo'shish, oddiy xatolarni bartaraf etish, yangi tugunlarni o'rnatish va dasturiy ta'minotning yangi versiyalarini o'rnatish. Bunday tarmoqni ma'mur vazifalarini faqat o'z vaqtining bir qismini

bajarishga bag'ishlangan xodim boshqarishi mumkin. Ko'pincha bo'limning tarmoq administratori maxsus treningga ega emas, lekin u kompyuterlarda eng yaxshi tushunadigan bo'limdagi shaxs bo'lib, u tarmoqni boshqarish bilan shug'ullanadi.

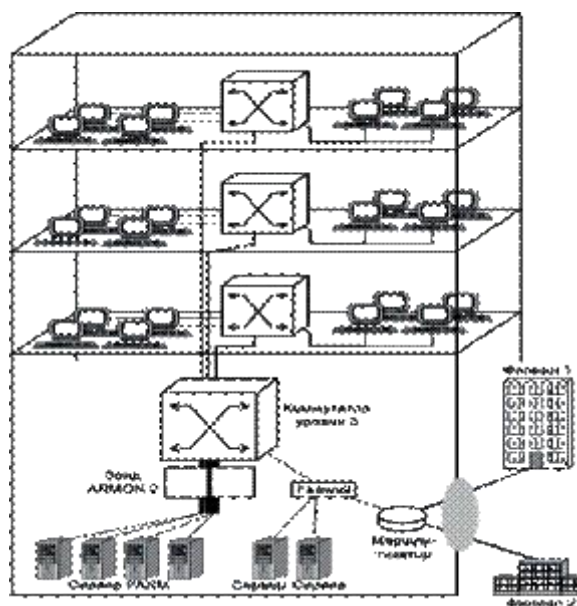
Bo'lim tarmoqlariga, ishchi guruh tarmoqlariga yaqin bo'lgan boshqa turdagi tarmoqlar mavjud. Bunday tarmoqlar 10-20 kompyuterlariga qadar bo'lgan juda kichik tarmoqlarni o'z ichiga oladi. Ishchi guruhlar tarmoqlarining xususiyatlari yuqorida tavsiflangan bo'lim tarmoqlarining xususiyatlaridan deyarli farq qilmaydi. Tarmoqning soddaligi va bir xilligi kabi xususiyatlar bu erda eng ko'p namoyon bo'ladi, bo'lim tarmoqlari ba'zi hollarda kampus tarmoqlarining navbatdagi turiga yaqinlashishi mumkin.

Kampus tarmoqlari

Kampus tarmoqlari o'z nomini ingliz tilidagi campus-talabalar shaharchasidan oldi. Kampus hududida bir nechta kichik tarmoqlarni bir-biriga ulash zarurati tez-tez paydo bo'ldi. Endi bu nom talabalar shaharchalari bilan bog'liq emas, balki har qanday korxona va tashkilotlarning tarmoqlariga murojaat qilish uchun ishlatiladi.

Kampus tarmoqlari bir korxonaning turli bo'limlarining turli tarmoqlarini alohida bino yoki bir necha kvadrat kilometrlik maydonni o'z ichiga olgan bir hududda birlashtiradi. Shu bilan birga, kampus tarmoqlarida global aloqalar qo'llanilmaydi. Bunday tarmoqning xizmatlari bo'lim tarmoqlari, korxona umumiy ma'lumotlar bazalariga kirish, umumiy faks serverlariga kirish, yuqori tezlikdagi modemlar va yuqori tezlikdagi printerlarni o'z ichiga oladi. Natijada, korxonaning har bir bo'limi xodimlari boshqa bo'limlarning ayrim fayl va tarmoq resurslaridan foydalanishlari mumkin. Kampus tarmoqlari qaysi turdagi kompyuterlar joylashgan bo'lishidan qat'i nazar, korporativ ma'lumotlar bazalariga kirishni ta'minlaydi.

Kampus tarmog'i darajasida geterogen apparat va dasturiy ta'minotni integratsiya qilish muammolari mavjud. Har bir bo'limdagi kompyuter turlari, tarmoq operatsion tizimlari, tarmoq apparatlari har xil bo'lishi mumkin. Shuning uchun kampus tarmoqlarini boshqarishning murakkabligi mavjud. Administratorlar bu holatda ko'proq malakali bo'lishi kerak va tarmoqni tezkor boshqarish vositalari yanada samarali bo'lishi kerak.

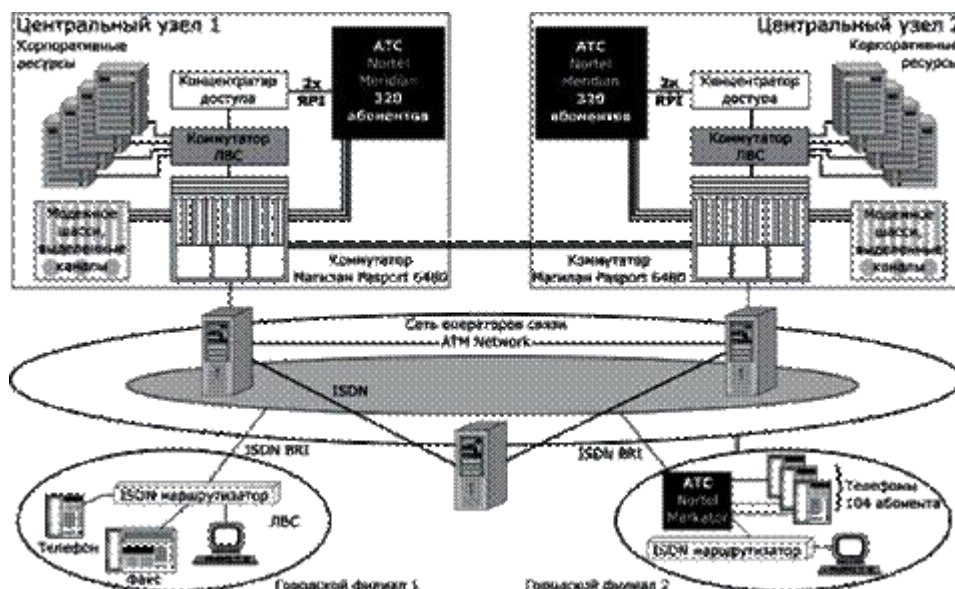


Kampus tarmog'i na'munasi

Korxona tarmoqlari

Korxona tarmoqlari, shuningdek, ushbu turdagi tarmoqlarni ifodalash uchun ingliz tilidagi adabiyotda ishlatiladigan "enterprise-wide networks" atamasining to'liq tarjimasiga mos keladigan korxona miqyosidagi tarmoqlar deb ataladi. Korxona miqyosidagi tarmoqlar (korporativ tarmoqlar) alohida korxonaning barcha hududlarida ko'plab kompyuterlarni birlashtiradi. Ular bilan bog'lanish qiyin bo'lishi mumkin va shaharni, mintaqani yoki hatto qit'ani qamrab olishi mumkin. Foydalanuvchilar va kompyuterlar soni minglab bilan o'lchanishi mumkin, va serverlar soni – yuzlab, ayrim hududlarning tarmoqlari orasidagi masofalar global bog'dan foydalanish kerak. Uzoq mahalliy tarmoqlarni

va shaxsiy kompyuterlarni korporativ tarmoqqa ulash uchun turli xil telekommunikatsiya vositalari, jumladan, telefon kanallari, radio kanallari, sun'iy yo'ldosh aloqalari qo'llaniladi. Korporativ tarmoq telekommunikatsiya muhitida suzuvchi "lan orollari" shaklida ifodalanishi mumkin.



Корпоратив тarmoqlar na'munasi

Bunday murakkab va keng ko'lamli tarmoqning ajralmas xususiyati-geterogenlikning yuqori darajasi (geterogenlik) – minglab foydalanuvchilarning bir xil turdagi dasturiy ta'minot va apparat vositalari yordamida ehtiyojlarini qondirish mumkin emas. Korporativ tarmoq har xil turdagi kompyuterlardan – ota-onalardan xodimlarga, bir nechta operatsion tizimlarga va turli xil ilovalardan foydalanishga ishonch hosil qiladi. Korporativ tarmoqning geterogen qismlari bir birlik sifatida ishlashi kerak, bu esa foydalanuvchilarga kerakli barcha resurslarga qulay va qulay foydalanish imkonini beradi.

Korxona tarmoqlari (korporativ tarmoqlar) alohida korxonaning barcha hududlarida ko'plab kompyuterlarni birlashtiradi.

Korporativ tarmoq uchun quyidagilar xos:

- masshtablilik-minglab maxsus kompyuterlar, yuzlab serverlar, katta hajmdagi saqlangan va ma'lumotlar uzatish liniyalari bo'ylab uzatiladigan, turli xil ilovalar;
- yuqori darajadagi geterogenlik darajasi – turli xil kompyuterlar, aloqa uskunalari, operatsion tizimlar va ilovalar;
- global aloqalardan foydalanish – filiallar tarmoqlari telekommunikatsiya vositalari, jumladan, telefon kanallari, radio kanallari, sun'iy yo'ldosh aloqasi orqali ulanadi.

Korporativ tarmoqlarning paydo bo'lishi-bu miqdorning sifatga o'tishi haqidagi mashhur postulatning yaxshi namunasidir. Turli shaharlarda va hatto mamlakatlarda filiallari bo'lgan yirik korxonaning alohida tarmoqlarini birlashtirganda, Birlashgan tarmoqning ko'plab miqdoriy xususiyatlari bir tarmoqqa o'tadi, buning ortidan yangi sifat boshlanadi. Bunday sharoitda korporativ tarmoqlar uchun kichikroq tarmoqlarning an'anaviy muammolarini hal qilishning mavjud usullari va yondashuvlari yaroqsiz bo'lib chiqdi. Ish guruhlari, bo'limlar va hatto kampus tarmoqlarida ikkinchi darajali ahamiyatga ega bo'lgan yoki hech qanday namoyon bo'lmagan vazifalar va muammolar birinchi o'ringa chiqdi. Misol uchun, eng oddiy (kichik tarmoqlar uchun) vazifa tarmoq foydalanuvchilari haqida hisobga olish ma'lumotlarini saqlashdir.

Uni hal qilishning eng oson usuli-har bir Foydalanuvchining hisobga olish ma'lumotlarini har bir kompyuterning mahalliy hisobga olish ma'lumotlar bazasiga joylashtirishdir. Kirish uchun harakat qilganda, bu ma'lumotlar mahalliy hisob bazasidan olinadi va ularga asoslangan holda yoki kirish imkoni yo'q. 5-10 kompyuterlardan tashkil topgan kichik tarmoqda va taxminan bir xil foydalanuvchilar soni, bu usul juda yaxshi ishlaydi. Biroq, agar tarmoqda bir necha ming foydalanuvchi mavjud bo'lsa, ularning har biri bir nechta o'nlab serverlarga kirishga muhtoj bo'lsa, unda bu yechim juda samarasiz bo'ladi. Administrator har bir

Foydalanuvchining hisobga olish ma'lumotlarini kiritish operatsiyasini bir necha o'n marta (serverlar soni bo'yicha) takrorlashi kerak. Foydalanuvchining o'zi ham yangi server resurslariga kirishga muhtoj bo'lgan har safar mantiqiy kirish tartibini takrorlashga majbur. Katta tarmoq uchun ushbu muammoni yaxshi hal qilish, ma'lumotlar bazasida barcha tarmoq foydalanuvchilari hisoblari saqlanadigan markazlashtirilgan yordam xizmatidan foydalanishdir. Administrator bir marta foydalanuvchi ma'lumotlarini ushbu ma'lumotlar bazasiga kiritish operatsiyasini amalga oshiradi va foydalanuvchi bir marta alohida serverga emas, balki butun tarmoqqa mantiqiy kirish tartibini amalga oshiradi.

Tarmoqlarning oddiy turlaridan yanada murakkabroq – bo'lim tarmoqlaridan korporativ tarmoqqa o'tishda-qamrov hududi ortadi, kompyuterlar aloqalarini saqlab qolish tobora qiyinlashib bormoqda. Tarmoq miqyosi oshgani sayin, uning ishonchliligi, ishlashi va funktsional imkoniyatlari uchun talablar ortadi. Tarmoq tobora ortib borayotgan ma'lumotlarning aylanishini ta'minlaydi va ularning xavfsizligi va xavfsizligini ta'minlash va mavjudlik bilan ta'minlash kerak. Bularning barchasi korporativ tarmoqlar eng kuchli va turli xil apparat va dasturiy ta'minot asosida qurilishiga olib keladi

3. Vazifa

Ushbu laboratoriyada quyidagi vazifalarni bajarish lozim:

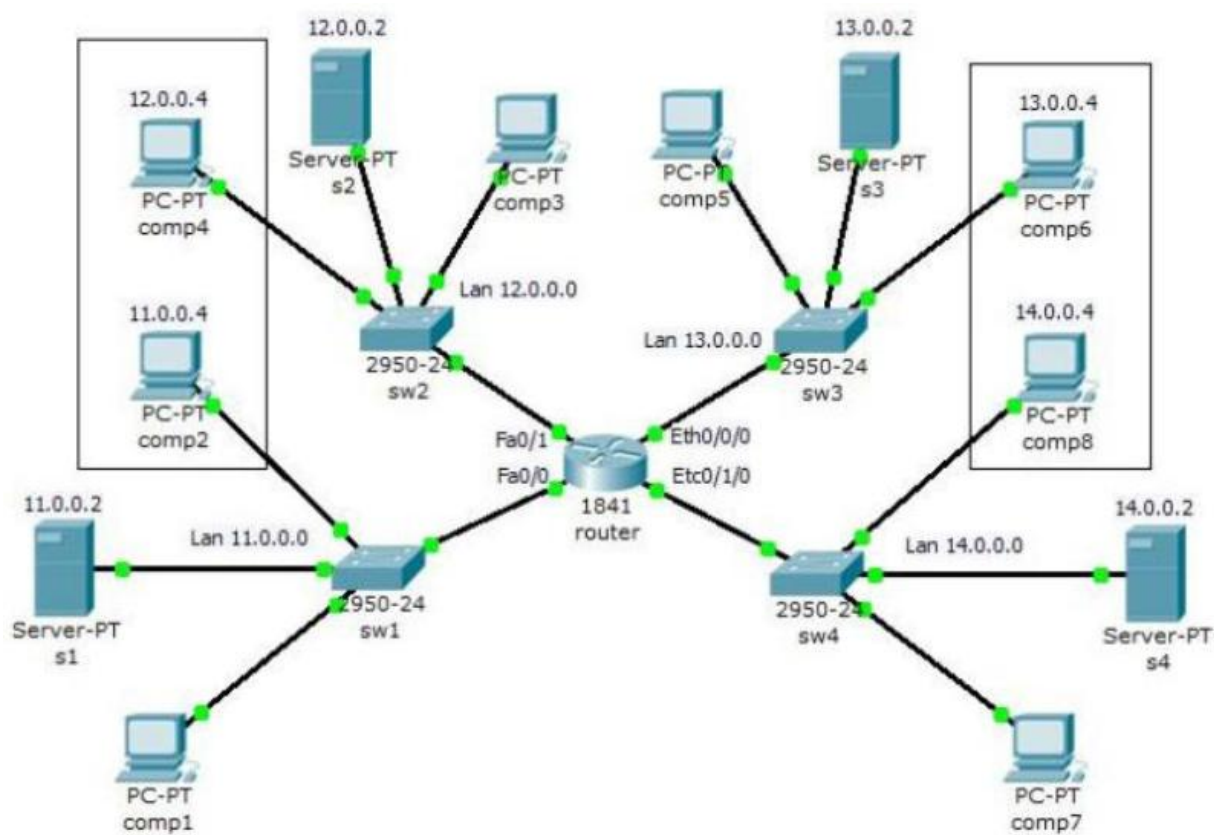
3.1 Ishni bajarish namunasiga asoslanib o'z variantingizning kichik korporativ tarmog'ini loyihalang.

Variant	Tarmoq raqami
1	Tarmoq №1
2	Tarmoq №2
3	Tarmoq №3

4	Tarmoq №4
5	Tarmoq №1
6	Tarmoq №2
7	Tarmoq №3
8	Tarmoq №4
9	Tarmoq №1
10	Tarmoq №2
11	Tarmoq №3
12	Tarmoq №4
13	Tarmoq №1
14	Tarmoq №2
15	Tarmoq №3
16	Tarmoq №4
17	Tarmoq №1
18	Tarmoq №2
19	Tarmoq №3
20	Tarmoq №4
21	Tarmoq №1
22	Tarmoq №2
23	Tarmoq №3
24	Tarmoq №4
25	Tarmoq №1

Tarmoq №1

4-rasmda berilgan tarmoqni loyihalang.



4-rasm. Korporativ tarmoq sxemasi

Korporativ tarmoq 4 ta tarmoqdan iborat:

Tarmoq 1 – 11.0.0.0/8; Tarmoq 2 – 12.0.0.0/8; Tarmoq 3 – 13.0.0.0/8; Tarmoq 4 – 14.0.0.0/8.

Har bir tarmoq serverida veb sayt mavjud.

Vazifa:

comp2 kompyuteriga faqat o'z tarmog'i kompyuterlari va comp4 ga ulanishga ruxsat bor.

comp4 kompyuteriga faqat o'z tarmog'i kompyuterlari va comp2 ga ulanishga ruxsat bor.

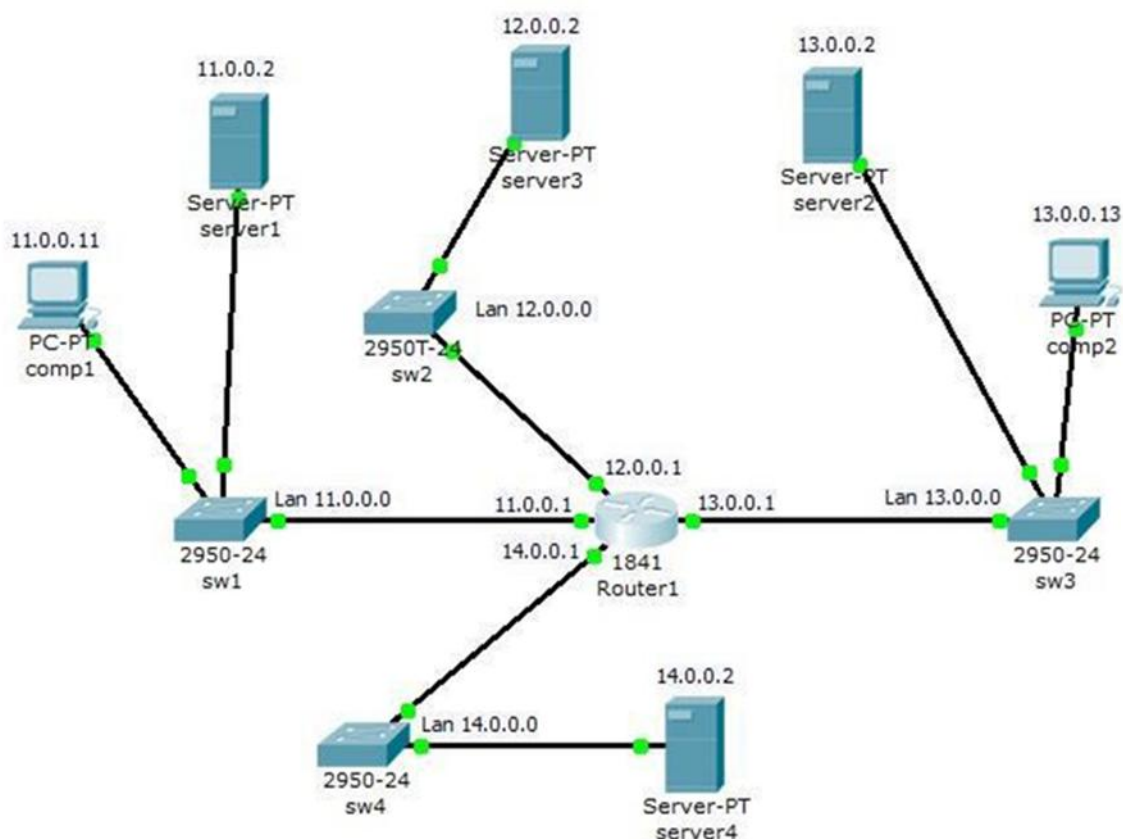
comp8 kompyuteriga faqat o'z tarmog'i kompyuterlari va comp6 ga ulanishga ruxsat bor.

comp6 kompyuteriga faqat o'z tarmog'i kompyuterlari va comp8 ga ulanishga ruxsat bor.

comp1, comp3, comp5 va comp7 lar S1, S2, S3 va S4 serverlardagi barcha saytlarni ochishlari kerak.

Tarmoq №2

5-rasmda berilgan tarmoqni loyihalang.



5-rasm. Korporativ tarmoq sxemasi

Korporativ tarmoq 4 ta tarmoqdan iborat:

Tarmoq 1 – 11.0.0.0/8; Tarmoq 2 – 12.0.0.0/8; Tarmoq 3 – 13.0.0.0/8; Tarmoq 4 – 14.0.0.0/8.

Har bir tarmoq serverida veb sayt mavjud.

Vazifa:

1) 14.0.0.0 tarmog'i 11.0.0.0 tarmog'i uchun yopiq ya'ni kirishga imkonsiz.

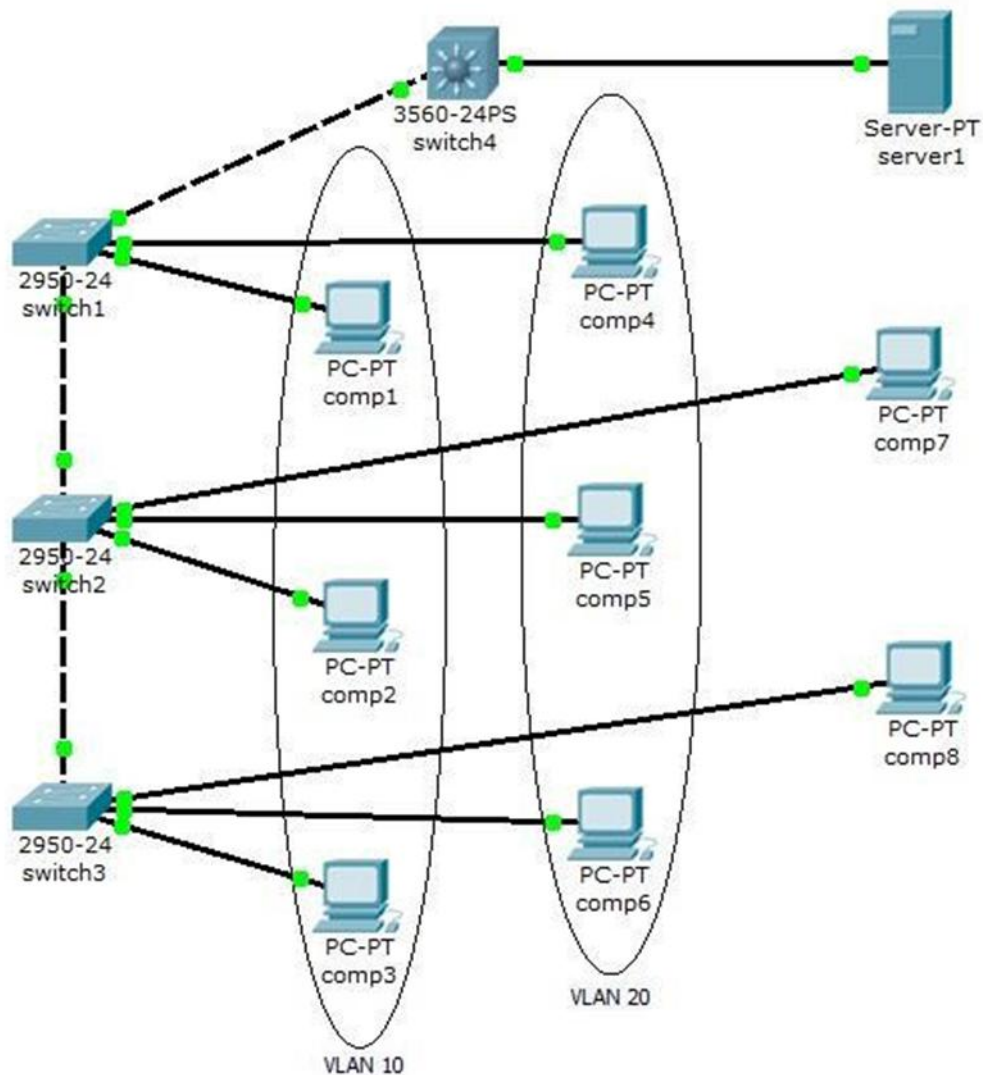
2) comp1 va comp2 kompyuterlarga server3 dagi saytni ochishga ruxsat bor, ammo server3 ga ping orqali murojaatning imkoniyati bo'lmasin.

3) comp1 kompyuteriga server2 ga murojaat qilish mumkin bo'lsin, ammo bu serverdagi saytgacha kira olmsligi ta'minlansin.

4) comp2 kompyuteriga server1 ga ulanish ruxsat berilsin (ping), ammo undagi saytni ochishga ruxsat berilmasin, server4 ulanishga va saytiga kirishga ruxsat berilsin.

Tarmoq №3

6-rasmda berilgan tarmoqni loyihalang.



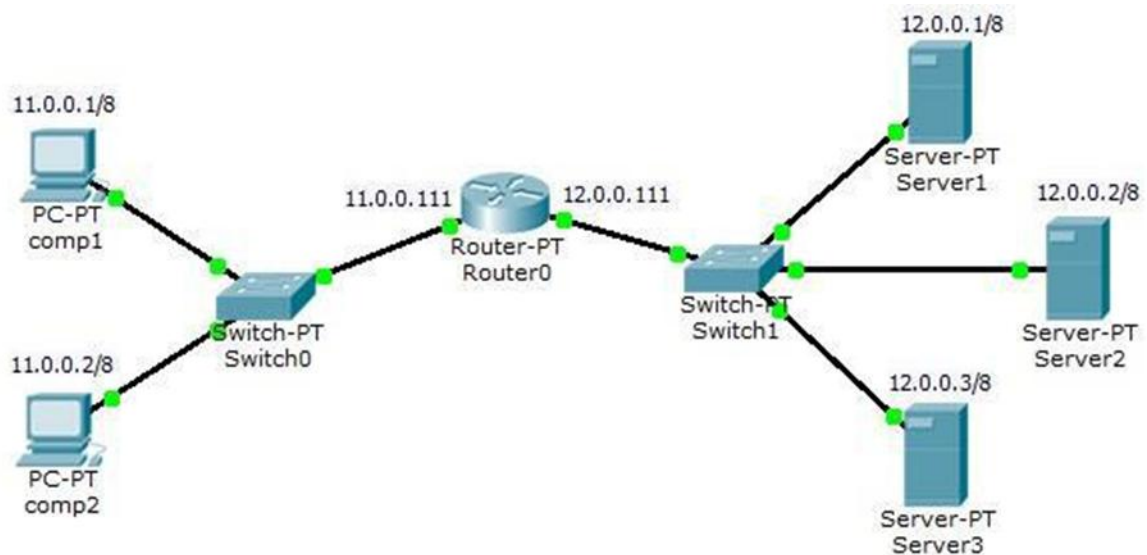
6-rasm. Korporativ tarmoq sxemasi

Vazifa:

- 1) comp1, comp2 и comp3 kompyuterlari VLAN 10 ga tegishli, faqat bir-biriga murojaat qila oladi va server1 ga ulana oladi.
- 2) comp4, comp5 и comp6 kompyuterlari VLAN 20 ga tegishli, faqat bir-biriga murojaat qila oladi va server1 ga ulana oladi.
- 3) comp7 и comp8 kompyuterlari faqat bir biriga murojaat qila oladi va server1 ga ulana oladi.

Tarmoq №4

7-rasmda berilgan tarmoqni loyihalang.



7-rasm. Korporativ tarmoq sxemasi

Barcha serverlarda Web va FTP ko'tarilgan.

Comp 1 va Comp2 uchun quyidagilarni ta'minlang:

Kompyuter comp1 uchun:

Server1 dagi FTP ga ; Server2 dagi Web ga; Server3 dagi Web va FTP ga ulanish imkoni berilsin.

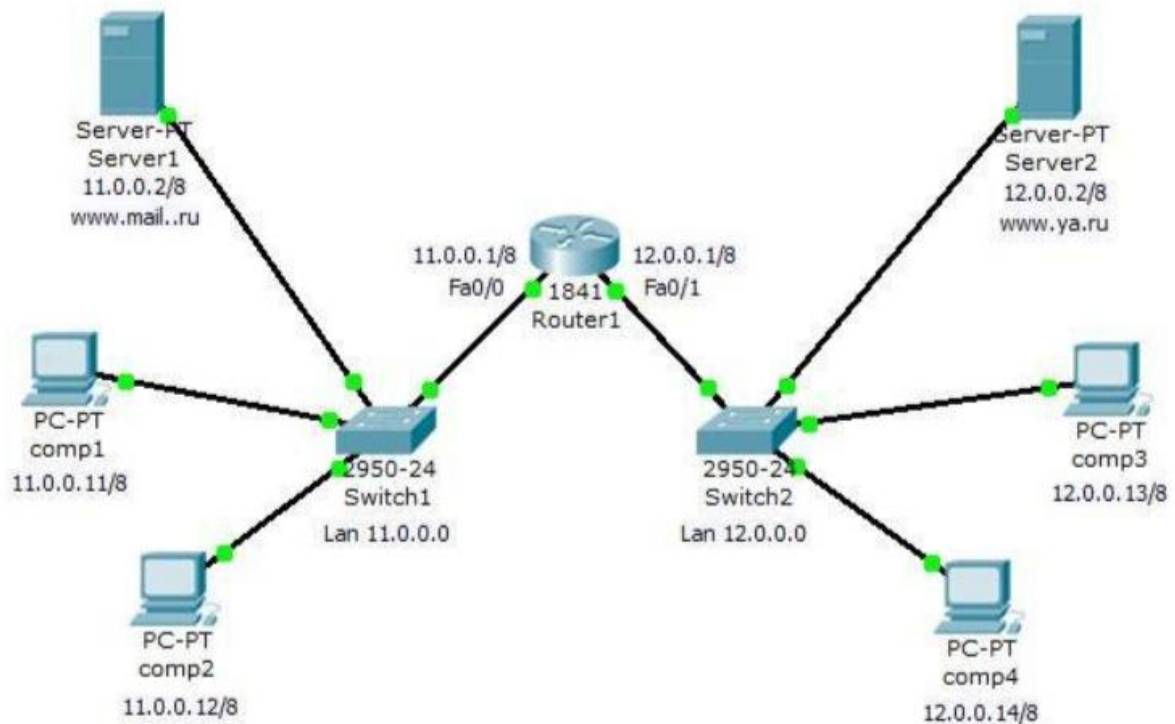
Kompyuter comp2 uchun:

Server1 dagi Webga; Server2 dagi FTP ga; Server3 dagi Web va FTP ga ulanish imkoni berilsin.

3.2. O'z kelajak ofisingiz uchun mustaqil ravishda korporativ tarmoq loyihalang.

Ishni bajarishga namuna:

8-rasmda berilgan tarmoqni loyihalang.



8-rasm. Korporativ tarmoq sxemasi

Vazifa:

- 1) comp1 va comp2 kompyuterlar barcha saytlarni ocha olsin ammo ularga comp3 va comp4 larga ulanish ta'qiqlansin.
- 2) comp3 va comp4 lar faqat bir-biriga kira oladi, faqat o'z tarmog'i saytiga kira oladi, 11.0.0.0 tarmog'i ular uchun yopiq.

Ishning bajarilishi

Standart ulanishlar ro'yxatini tuzamiz, unda comp3 va comp4 larga hostlarni bloklash qoidalarini joriy qilamiz va shu ro'yxatni Fa0/0 interfeys chiqishiga joriy qilamiz. Router konfiguratsiyasiga quyidagilarni kiring:

```
Router1>en
```

```
Router1#conf t
```

Standart ulanishlar ro'yxatini tuzamiz va ulanish qoidalarini beramiz:

```
Router1(config)#ip access-list standard 10
```

```
Router1(config-std-nacl)#deny host 12.0.0.13
```

```
Router1(config-std-nacl)#deny host 12.0.0.14
```

```
Router1(config-std-nacl)#permit any
```

Bu orqali quyidagi manzillardan tashqari barcha trafikka ruxsat o'chdik: 12.0.0.13 va 12.0.0.14.

Yaratilgan ro'yhatni tekshiramiz, buning uchun router konfiguratsiyalash rejimidan chiqish va buyruqni kiritish lozim:

```
Router1#sh access-list
```

Standard IP access list 10 deny host 12.0.0.13 deny host 12.0.0.14 permit any

```
Router1#
```

Yaratilgan ro'yhatni Fa0/0 interfeys chiqishi uchun joriy qilamiz:

```
Router1#
```

```
Router1#conf t
```

```
Router1(config)#interface fa0/0
```

```
Router1(config-if)#ip access-group 10 out
```

Ro'yxat 11.0.0.0 interfeysi uchun joriy qilinganligi uchun quyidagiga ega bo'ldik:

1) Routerga 11.0.0.0 tarmog'idan kiruvchi paketlar 12.0.0.13 va 12.0.0.14 adreslariga jo'natilmaydi ya'ni bloklanadi;

2) Tarmoq 11.0.0.0ga router orqali kirayotgan paketlarga hech qanday cheklovlar yo'q, faqat 12.0.0.13 va 12.0.0.14 manzillari 11.0.0.0 ga kirishga ruxsati yo'q.

Konfiguratsiyani tekshiramiz:

```
Router1(config-if)#exit
```

```
Router1(config)#exit
```

```
Router1#
```

```
Router1#sh running-config
```

Bunda router konfiguratsiyasi shu jumladan dostuplar ro'yhatining interfeyslarga joriy qilinganligini ham ko'rish mumkin.

```
interface FastEthernet0/0
```

```
ip address 11.0.0.1 255.0.0.0 ip access-group 10 out duplex auto
```

```
speed auto
```

Natijalarni tekshirib oling!

4. Hisobot tarkibi

Hisobotda quyidagilar keltirilishi lozim:

- Ishning nomi va maqsadi.
- Ishni bajarilganligini ko'rsatuvchi "screen shot" lar.
- Ishning natijasi.
- Nazorat savollariga qisqacha javoblar.

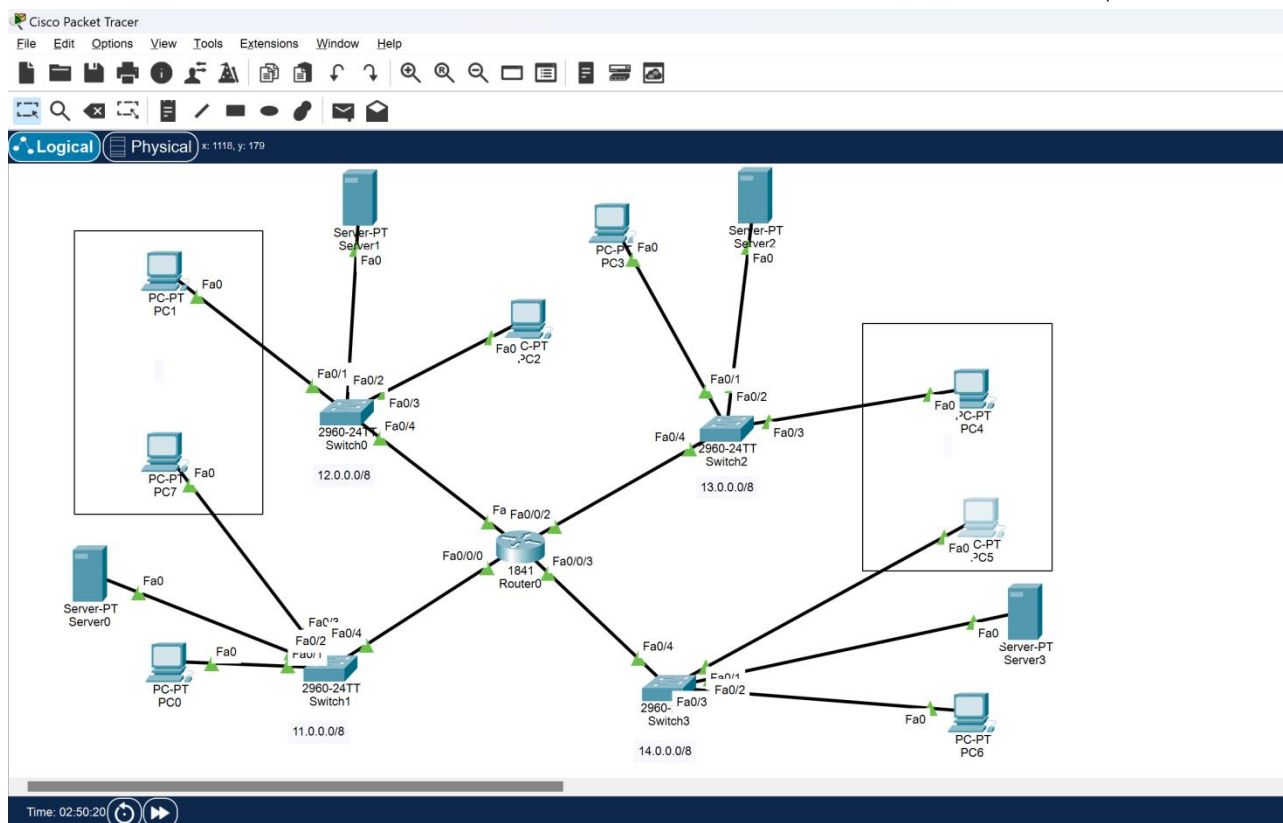
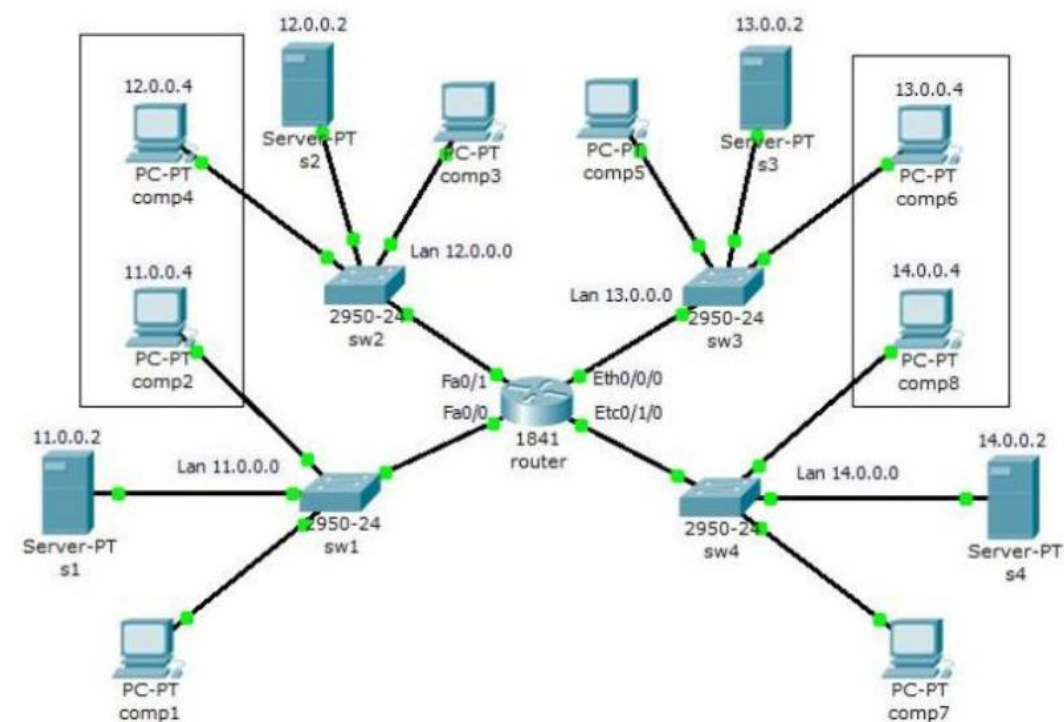
5. Nazorat savollari

1. Qaysi variantlar kengaytirilgan kirish ro'yxatlarini nazorat qiladi?
2. Xostdan barcha veb-serverlarga paketlarni uzatish imkonini beruvchi buyruqlar misolini keltiring.
3. Kirish ro'yxatlarining asosiy turlarini sanab bering.
4. Tarmoq osti niqobining namunasi nima va uni kirish ro'yxatlarida ishlatish misollarini keltiring.
5. Tarmoq trafagini qayta ishlash qoidasi quyidagi kirish ro'yxatini belgilaydi: ip access-list 111 deny TCP har qanday eq 80
6. Mahalliy tarmoq fa0/0 interfeysi orqali bilan bog'lanadi va tashqi tarmoq Fa0/1 interfeysi orqali ulanadi. Mahalliy tarmoqdan tashqi tarmoqqa kirish taqiqlanadi va tashqi tarmoqdan ichki tarmoqda joylashgan FTP serveriga kirish taqiqlanadi. Ushbu qoidalarni amalga oshirish uchun kirish ro'yxati yaratildi. Yaratilgan kirish ro'yxatini

qo'llash kerak bo'lgan interfeysni va qaysi yo'nalishda (kirish yoki chiqish uchun) ekanligini ayting.

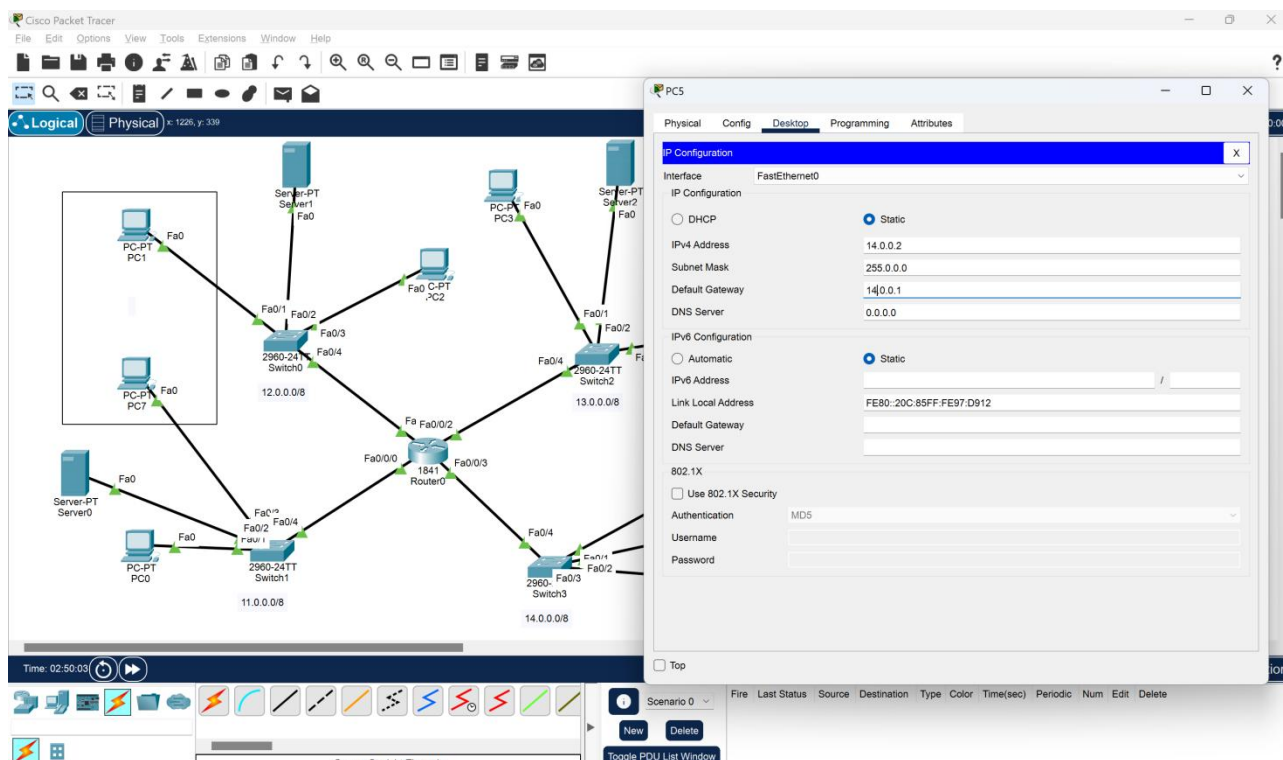
KORPORATIV TARMOQLARNI LOYIHALASH

Tarmoq №1



Topologiyaning tuzulishi

Har biriga ip larni berib chiqamiz



Har bir tarmoq serverida veb sayt mavjud.

Korporativ tarmoq 4 ta tarmoqdan iborat:

Tarmoq 1 – 11.0.0.0/8; Tarmoq 2 – 12.0.0.0/8; Tarmoq 3 – 13.0.0.0/8;

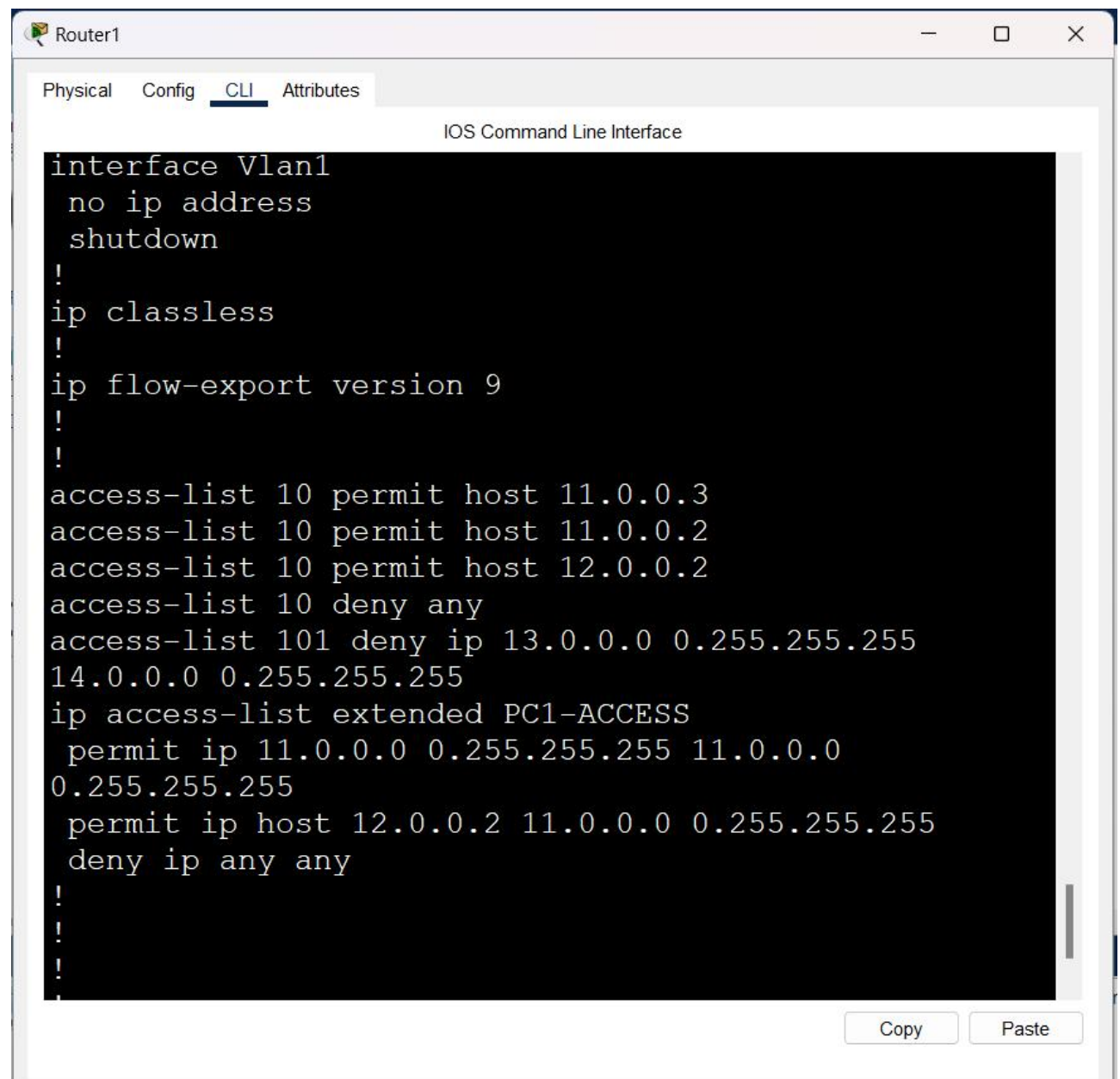
Tarmoq 4 – 14.0.0.0/8.

Har bir tarmoq serverida veb sayt mavjud.

Vazifa:

1. PC7 kompyuteriga faqat o'z tarmog'i kompyuterlari va PC1 ga ulanishga ruxsat

bor



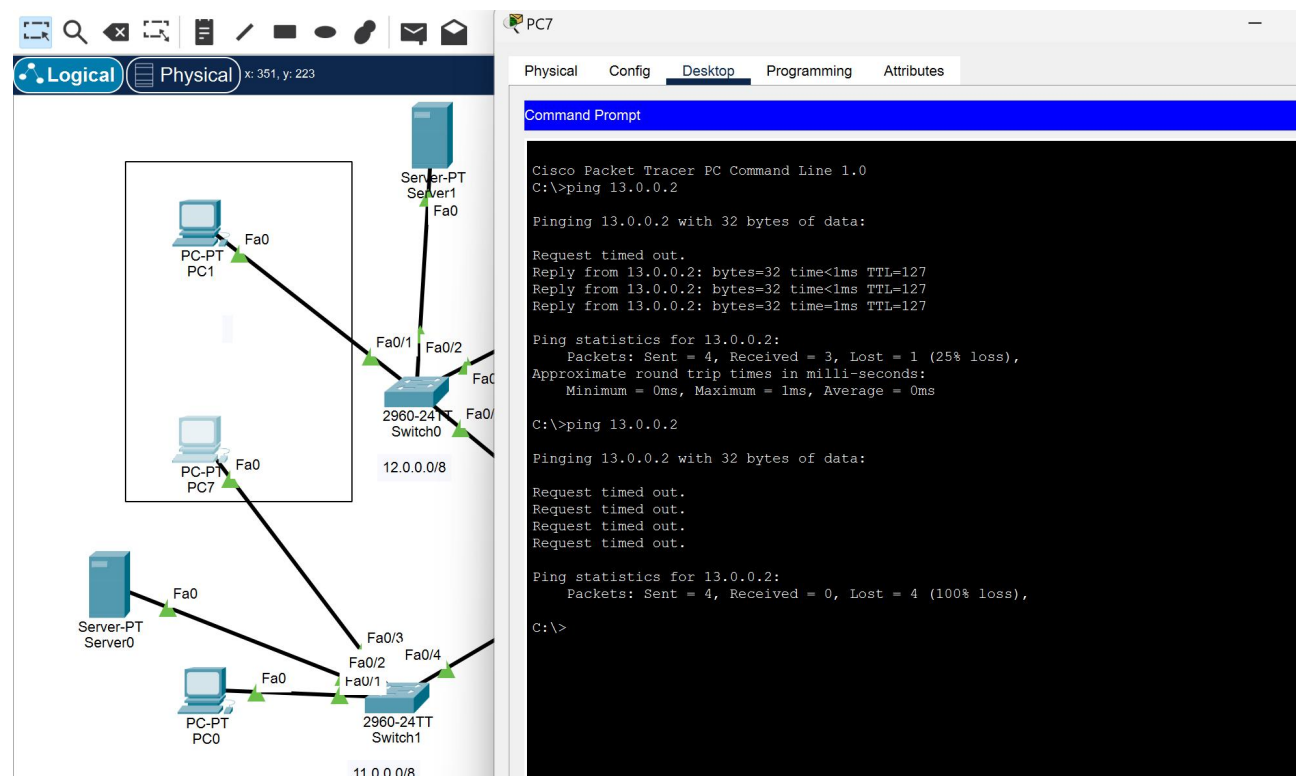
The screenshot shows a Cisco Router1 CLI window with the following configuration commands entered:

```
interface Vlan1
  no ip address
  shutdown
!
ip classless
!
ip flow-export version 9
!
!
access-list 10 permit host 11.0.0.3
access-list 10 permit host 11.0.0.2
access-list 10 permit host 12.0.0.2
access-list 10 deny any
access-list 101 deny ip 13.0.0.0 0.255.255.255
14.0.0.0 0.255.255.255
ip access-list extended PC1-ACCESS
  permit ip 11.0.0.0 0.255.255.255 11.0.0.0
0.255.255.255
  permit ip host 12.0.0.2 11.0.0.0 0.255.255.255
  deny ip any any
!
!
!
```

At the bottom right of the window, there are 'Copy' and 'Paste' buttons.

2. PC1 kompyuteriga faqat o'z tarmog'i kompyuterlari va PC7 ga
ulanishga ruxsat

bor.



The image shows a Cisco Packet Tracer network diagram and a command prompt window for PC7. The network diagram includes two switches, 2960-24T Switch0 and 2960-24T Switch1, connected via their Fa0/24 ports. Switch0 has PC1 (10.0.0.2) on Fa0/1, PC7 (12.0.0.8) on Fa0/2, and Server1 (13.0.0.2) on Fa0/24. Switch1 has PC0 (11.0.0.8) on Fa0/1, PC6 (12.0.0.2) on Fa0/2, and Server0 (13.0.0.2) on Fa0/24. The command prompt window for PC7 shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 13.0.0.2

Pinging 13.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 13.0.0.2: bytes=32 time<1ms TTL=127
Reply from 13.0.0.2: bytes=32 time<1ms TTL=127
Reply from 13.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 13.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 13.0.0.2

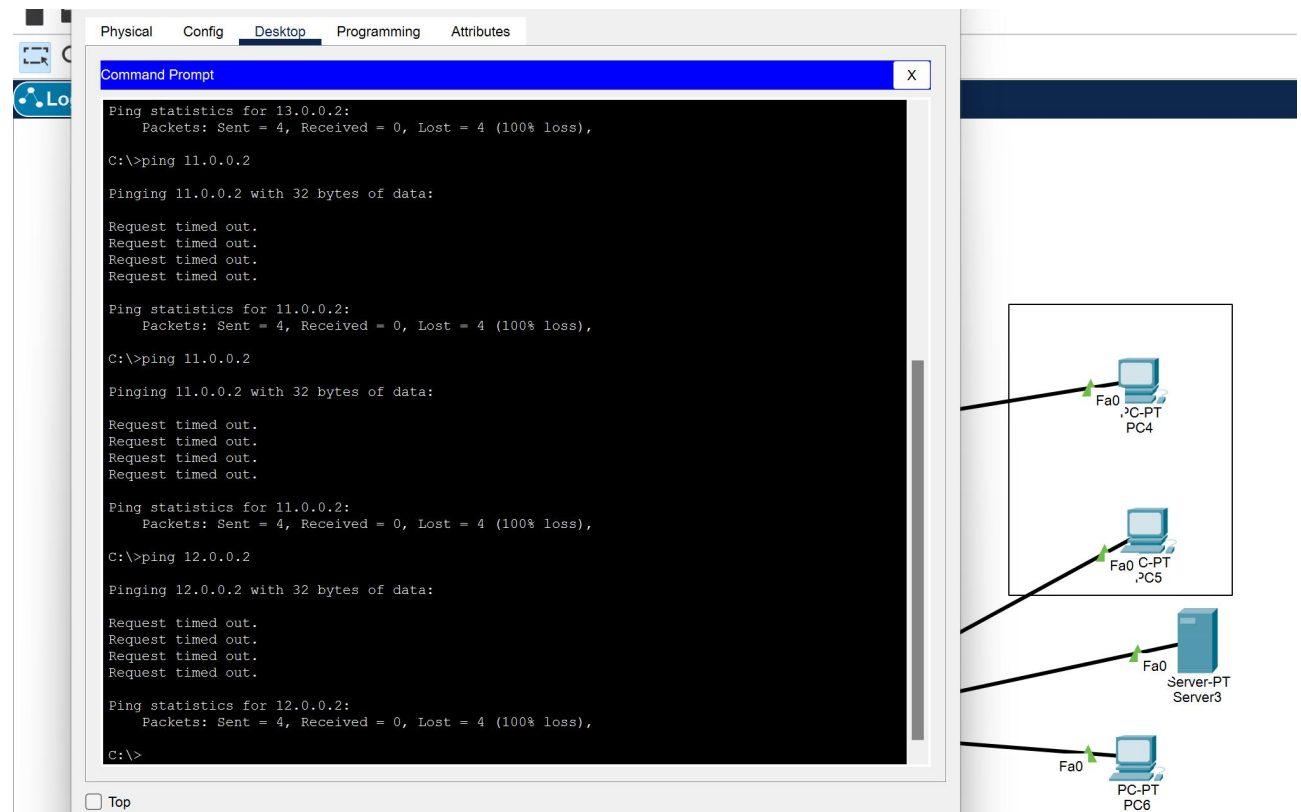
Pinging 13.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

3. PC5 kompyuteriga faqat o'z tarmog'i kompyuterlari va PC4 ga ulanishga ruxsat bor.



The image shows a Cisco Packet Tracer network diagram and a command prompt window for PC5. The network diagram includes a switch connected to PC4 (10.0.0.2) on Fa0/1, PC5 (12.0.0.2) on Fa0/2, and Server3 (13.0.0.2) on Fa0/24. The command prompt window for PC5 shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 13.0.0.2

Pinging 13.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 12.0.0.2

Pinging 12.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```


4. PC4 kompyuteriga faqat o'z tarmog'i kompyuterlari va PC5 ga ulanishga ruxsat bor.

5. PC0, PC2, PC3 va PC6 lar Switch1, Switch0, Switch2 va Switch3 serverlardagi barcha saytlarni ochishlari kerak.

1.

The screenshot shows a network topology in Cisco Packet Tracer. The network consists of several devices: PC-PT PC1, PC-PT PC2, PC-PT PC3, PC-PT PC4, PC-PT PC5, PC-PT PC6, PC-PT PC7, Server-PT Server0, Server-PT Server1, 2960-24T Switch0, 2960-24T Switch1, 2960-24T Switch2, 2960-24T Switch3, and 2811 Router1. The topology is as follows: PC1 is connected to Switch0 (Fa0/1 to Fa0/2). PC2 is connected to Switch0 (Fa0/3 to Fa0/4). PC3 is connected to Switch0 (Fa0/5 to Fa0/6). PC4 is connected to Switch0 (Fa0/7 to Fa0/8). PC5 is connected to Switch0 (Fa0/9 to Fa0/10). PC6 is connected to Switch1 (Fa0/1 to Fa0/2). PC7 is connected to Switch1 (Fa0/3 to Fa0/4). Server0 is connected to Switch1 (Fa0/5 to Fa0/6). Server1 is connected to Switch1 (Fa0/7 to Fa0/8). Switch0 is connected to Switch1 (Fa0/9 to Fa0/10). Switch1 is connected to Router1 (Fa0/0 to Fa0/1). Switch2 is connected to Router1 (Fa0/2 to Fa0/3). Switch3 is connected to Router1 (Fa0/4 to Fa0/5). Router1 is connected to the Internet (GigabitEthernet0/0/0 to GigabitEthernet0/0/1). The PC command prompt window shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 11.0.0.3

Pinging 11.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 11.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 11.0.0.3

Pinging 11.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 11.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2.

The screenshot shows a network topology in Cisco Packet Tracer. The network consists of several devices: PC-PT PC1, PC-PT PC2, PC-PT PC3, PC-PT PC4, PC-PT PC5, PC-PT PC6, PC-PT PC7, Server-PT Server0, Server-PT Server1, 2960-24T Switch0, 2960-24T Switch1, 2960-24T Switch2, 2960-24T Switch3, and 2811 Router1. The topology is as follows: PC1 is connected to Switch0 (Fa0/1 to Fa0/2). PC2 is connected to Switch0 (Fa0/3 to Fa0/4). PC3 is connected to Switch0 (Fa0/5 to Fa0/6). PC4 is connected to Switch0 (Fa0/7 to Fa0/8). PC5 is connected to Switch0 (Fa0/9 to Fa0/10). PC6 is connected to Switch1 (Fa0/1 to Fa0/2). PC7 is connected to Switch1 (Fa0/3 to Fa0/4). Server0 is connected to Switch1 (Fa0/5 to Fa0/6). Server1 is connected to Switch1 (Fa0/7 to Fa0/8). Switch0 is connected to Switch1 (Fa0/9 to Fa0/10). Switch1 is connected to Router1 (Fa0/0 to Fa0/1). Switch2 is connected to Router1 (Fa0/2 to Fa0/3). Switch3 is connected to Router1 (Fa0/4 to Fa0/5). Router1 is connected to the Internet (GigabitEthernet0/0/0 to GigabitEthernet0/0/1). The PC command prompt window shows the following output:

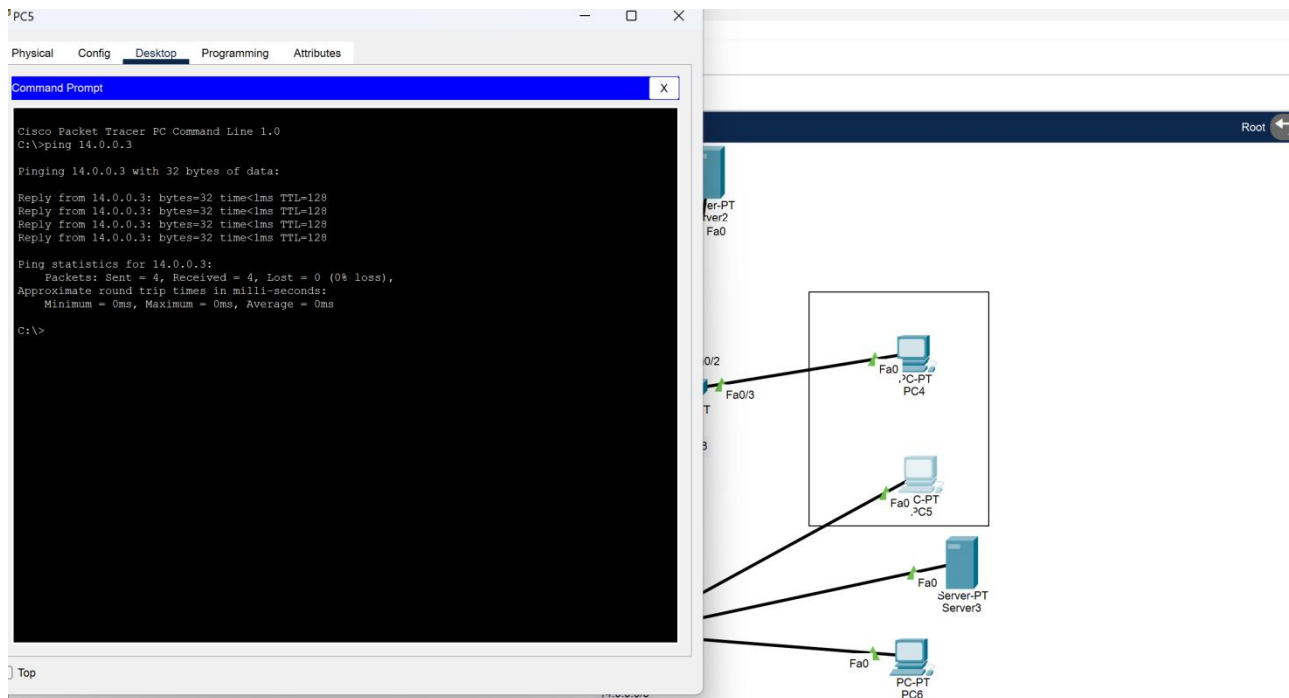
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 14.0.0.2

Pinging 14.0.0.2 with 32 bytes of data:

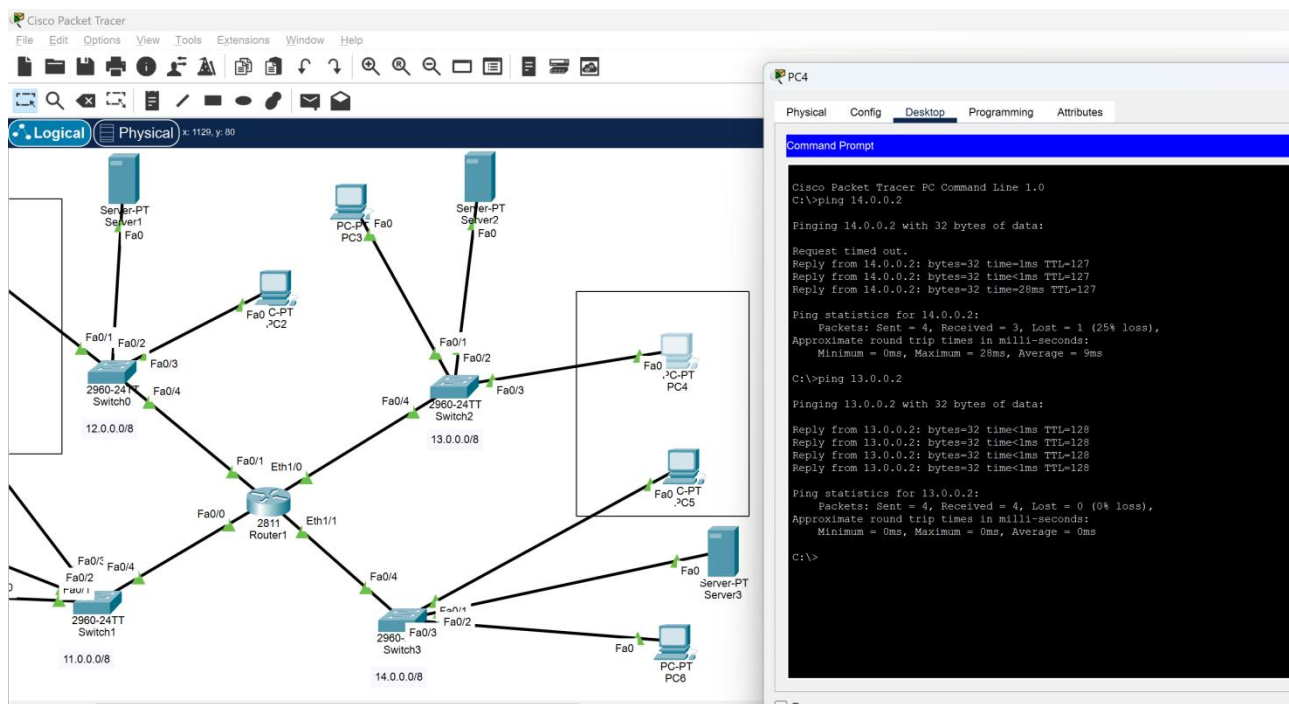
Request timed out.
Reply from 14.0.0.2: bytes=32 time=1ms TTL=127
Reply from 14.0.0.2: bytes=32 time=1ms TTL=127
Reply from 14.0.0.2: bytes=32 time=28ms TTL=127

Ping statistics for 14.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 28ms, Average = 9ms

C:\>
```



3.



4.

5.

The image shows a Cisco Packet Tracer network diagram and the configuration of PC0. The network diagram includes two switches, 2960-24TT Switch0 and 2960-24TT Switch1, connected via their Fa0/24 ports. Switch0 has a 12.0.0.0/8 network and is connected to Server-PT Server1 (Fa0/1) and PC-PT PC1 (Fa0/2). Switch1 has a 11.0.0.0/8 network and is connected to Server-PT Server0 (Fa0/24) and PC-PT PC0 (Fa0/24). PC0 is also connected to Switch0 via its Fa0/24 port. The PC0 configuration window shows the Desktop tab with a Web Browser. The Web Browser URL is http://11.0.0.4, and the page content is "Welcome my website 0".

PC0 Configuration:

- Physical: x: 1081, y: 76
- Config: Desktop, Programming, Attributes
- Web Browser: URL http://11.0.0.4, Go, Stop
- Page Content: Welcome my website 0
- Text: Lorem ipsum dolor sit amet consectetur adipisicing elit. Maxime mollitia, molestiae quas vel sint commodi repudiandae consequuntur voluptatum laborum
- Quick Links: [A small page](#), [Copyrights](#), [Image page](#), [Image](#)

The image shows a Cisco Packet Tracer network diagram and the configuration of PC2. The network diagram includes three switches, 2960-24TT Switch0, 2960-24TT Switch2, and 2960-24TT Switch3, connected via their Fa0/24 ports. Switch0 has a 12.0.0.0/8 network and is connected to Server-PT Server1 (Fa0/1) and PC-PT PC2 (Fa0/2). Switch2 has a 13.0.0.0/8 network and is connected to Server-PT Server2 (Fa0/1) and PC-PT PC3 (Fa0/2). Switch3 has a 14.0.0.0/8 network and is connected to PC-PT PC4 (Fa0/1) and PC-PT PC5 (Fa0/2). A central 2811 Router1 is connected to all three switches via its Fa0/0, Fa0/1, and Fa0/2 ports. The PC2 configuration window shows the Desktop tab with a Web Browser. The Web Browser URL is http://13.0.0.4, and the page content is "TUIT rasmiy websayti".

PC2 Configuration:

- Physical: x: 939, y: 63
- Config: Desktop, Programming, Attributes
- Web Browser: URL http://13.0.0.4, Go, Stop
- Page Content: TUIT rasmiy websayti
- Text: Lorem ipsum dolor sit amet consectetur adipisicing elit. Maxime mollitia, molestiae quas vel sint commodi repudiandae consequuntur voluptatum laborum
- Quick Links: [A small page](#), [Copyrights](#), [Image page](#), [Image](#)

