**O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI**

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

**R.I. Isayev, D.X. Ibatova**

# MULTIMEDIALI ALOQA TARMOQLARI


**Toshkent 2018**

**UDK: 621.391**
**BBK 32.94**
**G95**

**Авторлар: R.I.Isayev, D.X.Ibatova. Multimediali aloqa tarmoqlari. / Muhammad al-Xorazmiy nomidagi TATU. Toshkent, 2018 y. 350 b.**

Davlat tilida yozilgan ushbu darslikda multimediali aloqa tarmoqlarining tuzilish prinsiplari, xizmatlar, protokollar, sinxronizatsiya, multimediali aloqa tarmoqlarini boshqarish, konvergent tarmoqlar, multimediali aloqa tarmoqlarini loyihalashtirish va axborot xavfsizligini ta’minlash masalalari yoritilgan.

Ushbu darslik 5350100–Telekommunikatsiya texnologiyalari bakalavriat yo‘nalishi bo‘yicha ta’lim oluvchi talabalar uchun mo‘ljallangan.

Taqrizchilar:

“Telekommunikatsiya injiniringi”
kafedrasi dotsenti N.X.Gulturaev

“UNICON. UZ” bo‘lim boshlig‘i I.R.Berganov

# KIRISH

O‘zbekiston Respublikasi Prezidenti Sh. Mirziyoyevning 2017 yil 7 fevraldagi “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha harakatlar strategiyasi to‘g‘risida” PF-4947-sonli Farmoni tasdiqlandi. Harakatlar strategiyasining maqsadi olib borilayotgan islohotlar samaradorligini tubdan oshirishdan, davlat va jamiyatning har tomonlama va jadal rivojlanishini ta’minlash uchun shart-sharoitlar yaratishdan, mamlakatni modernizatsiyalash va hayotning barcha sohalarini erkinlashtirishdan iboratdir. Ayni vaqtda mamlakatimiz bosib o‘tgan taraqqiyot yo‘lining chuqur tahlili, bugungi kunda jahon bozori kon’yunkturasi keskin o‘zgarib, globallashuv sharoitida raqobat tobora kuchayib borayotgani davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish uchun mutlaqo yangicha yondashuv hamda tamoyillarni ishlab chiqish va ro‘yobga chiqarishni taqazo etmoqda [1].

Bugungi kunda telekommunikatsiya va iqtisodiyot sohasida, axborot tarmoqlari oldida turgan vazifalar va maqsadlar tubdan o‘zgardi. O‘zbekistonda makro iqtisodiyot va moliyaviy barqarorlik o‘rnatildi, iqtisodiyotning samarador yetakchisi sifatida olingan telekommunikatsiya sohasida takomillashtirish va texnik jixatdan qayta qurish ishlari amalga oshirilmoqda. Ushbu sohani yanada rivojlantirish uchun zarur bo‘lgan barcha shart–sharoitlar yaratilgan. Jahon axborot – telekommunikatsiya maydonida integratsiyalash ishlari amalga oshirilmoqda.

Respublikada global axborot tizimlari va texnologiyalarining keng qamrovli milliy axborot tizimiga kirishni shakllantirishga alohida e’tibor qaratilgan va bu esa o‘z navbatida XXI asrda mamlakatning o‘sishida hal qiluvchi vazifa hisoblanadi.

“O‘zbektelekom” AK Telekommunikatsiya tarmoqlarini rivojlantirish va zamonaviy xizmatlarni joriy etish bo‘yicha qator katta investitsiya loyihalarini amalga oshirdi. Iqtisodiyotimiz va jamiyatimiz hayotida axborot-kommunikatsiya texnologiyalarining alohida va muhim o‘rin tutishini hisobga olib, 2013 yilda 2013-

2020 yillarda O‘zbekiston Respublikasining Milliy axborot-kommunikatsiya tizimini rivojlantirishni kompleks dasturi qabul qilindi.

Bugungi kunda O‘zbekiston Respublikasi telekommunikatsiya tarmoqlarida juda katta o‘zgarishlar sodir bo‘lmoqda. So‘nggi yillar mobaynida axborot-kommunikatsiya texnologiyalarining rivojlanishi natijasida, mamlakatimiz aloqa sohasida yuqori natijalarga erishilmoqda. Telekommunikatsiya tarmoqlarini modernizatsiyalash, zamonaviy texnologiyalarni qo‘llash, yangi raqamli texnika vositalarini o‘rnatish, ularni optimallashtirish ishlari natijasida, jahon axborot integratsiyalashuvi jarayoniga O‘zbekistonning jadal suratda qo‘shilishi ko‘zga tashlanmoqda.

Telekommunikatsiya tarmoqlarini rivojlanishi uch omilga asosan aniqlanadi: trafikni o‘sishi, jamiyatni yangi xizmatlarga bo‘lgan talabini oshishi va texnologiyalar sohasida yutuqlarga erishish. Bu omillar mustaqil hisoblanmaydi, biroq ularning har biri elektr aloqani rivojlanish g‘oyasini aniqlaydi. Qurilmalarni yetkazib beruvchilar orasidagi raqobat va texnologik yutuqlar qurilmalarning narxini tushishiga olib keldi, bu esa o‘z navbatida trafikni o‘sishi va yangi xizmatlarni ishlab chiqarishni rag‘batlantiradi.

XX – asrning 90-yillari boshidan telekommunikatsiya raqamlashtirish yo‘nalishi bo‘yicha rivojlandi. Bu nafaqat axborotlarni uzatishda, balki taqsimlash, saqlash va qayta ishlashda ham tejamkor usullarni ta’minlovchi bosh yo‘nalishlardan biri bo‘lib qoldi. Raqamli telekommunikatsiya tarmoqlarini jadallik bilan rivojlanishini, analog uzatish tizimlari bilan solishtirganda bir qancha afzalliklari bilan farq qiladi, masalan: yuqori shovqinbardoshliligi, aloqa liniyasining uzunligiga uzatish sifatining kuchsiz bog‘lanishi, aloqa kanallarining elektrik parametrlarini mo‘tadilligi, diskret xabarlarni uzatishda o‘tkazuvchanlik qobiliyatini qo‘llashning samaradorligi va boshqalar.

Bir vaqtning o‘zida aloqa xizmatlarining soni oshishi bilan, oddiy telefon xizmatidan tortib to integral raqamli aloqa tarmoqlarini ta’minlovchi multimedia

xizmatlarigacha ularning sifati o‘zgardi. Ko‘pgina mutaxassislar, telekommunikatsiya texnologiyalarining keyingi evolyutsiyasi, axborotlarni uzatish tezligini oshirish, tarmoqni intellektuallashtirish va foydalanuvchilarning mobilligini ta’minlash yo‘nalishi bo‘yicha ketadi deb ta’kidlashmoqda.

1999 yilda “Telekommunikatsiyalar to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni qabul qilindi. Ushbu Qonunning asosiy maqsadi telekommunikatsiyalarni yaratish, ishlatish va rivojlantirish sohasidagi ijtimoiy munosabatlarni tartibga solishdan iborat. Ushbu qonunda quyidagi asosiy tushunchalar qo‘llaniladi:

- telekommunikatsiyalar – signallar, belgilar, matnlar, tasvirlar, tovushlar yoki axborotning boshqa turlarini o‘tkazgichli, radio, optik yoki boshqa elektromagnit tizimlardan foydalangan holda uzatish, qabul qilish, qayta ishlash;

- telekommunikatsiyalar tarmog‘i – uzatishning bir yoki bir necha turini: telefon, telegraf, faksimil, ma’lumotlar uzatish va xujjatli xabarlarning boshqa turlarini, televizion va radioeshittirish dasturlarini translyatsiya qilishni ta’minlovchi telekommunikatsiya vositalarining majmui;

- telekommunikatsiya vositalari – elektromagnit yoki optik signallarni kommutatsiyalash, shakllantirish, uzatish, qabul qilish, qayta ishlash, hamda ularni boshqarish imkonini beruvchi texnik qurilmalar, asbob-uskunalar, inshootlar va tizimlar;

- telekommunikatsiya inshootlari – telekommunikatsiya tarmoqlari va vositalarining ishlashi hamda ulardan foydalanishni ta’minlovchi binolar, qurilmalar, telekommunikatsiya liniyalari, moslamalar, tayanchlar, machtalar va boshqa inshootlar;

- oxirgi (terminal) qurilmalar – telekommunikatsiya tarmoqlari bilan o‘zaro ta’sirlashuvchi hamda telekommunikatsiya tarmoqlari orqali uzatiladigan yoki qabul qilinadigan signallarni hosil qilish, o‘zgartirish, qayta ishlashga mo‘ljallangan foydalanuvchilarning texnik vositalari (telefon, faksimil, radio-teleqabulqilgichlar va boshqa qurilmalar);

- tarmoqlararo ulanishlar – foydalanuvchilar orasida axborotlarni uzatish va qabul qilishni ta’minlovchi, telekommunikatsiyaning turli operatorlarini telekommunikatsiya tarmoqlari orasida texnologik o‘zaro ta’sirlashishi;

- telekommunikatsiya operatori – mulk huquqi yoki boshqa ashyoviy huquq asosida telekommunikatsiya tarmog‘iga ega bo‘lgan, uning ishlashi, rivojlanishini ta’minlovchi va telekommunikatsiya xizmatlarini ta’minlovchi yuridik shaxs;

- telekommunikatsiya xizmatlari provayderi – foydalanuvchilarga operatorlar tarmog‘i orqali tijorat asosida telekommunikatsiya xizmatlarini ko‘rsatuvchi yuridik shaxs;

- telekommunikatsiya xizmatlari – telekommunikatsiya tarmog‘i orqali turli axborotlarni va signallarni uzatish, qabul qilish, qayta ishlash bo‘yicha operator va provayderning faoliyat mahsuli;

- raqamlash tizimi – operatorlar, provayderlar va foydalanuvchilarning oxirgi (terminal) qurilmalari orasida raqamlarni berish (raqam kombinatsiyasi yoki belgi) va taqsimlash tartibi;

- raqamlash rejasi - operatorlar, provayderlar va foydalanuvchilarning oxirgi qurilmalari o‘rtasidagi aniq raqamlarning berilishi;

- telekommunikatsiya xizmatlaridan foydalanuvchi (keyinchalik-foydalanuvchi) – telekommunikatsiyalar xizmatlarining iste’molchisi hisoblangan yuridik yoki jismoniy shaxs;

- universal xizmatlar – umum foydalanish telekommunikatsiya tarmoqlari orqali barcha foydalanuvchilarga ko‘rsatiladigan belgilangan sifatdagi majburiy xizmatlar to‘plami (foydalanuvchilarning bu tarmoqdan foydalanishini ta’minlash, mahalliy, shaharlararo va xalqaro telefon so‘zlashuvlari, telegrammalar jo‘natish va boshqalar).

Axborot uzatish tezligining yuqoriligi tasvirlar, televizion tasvirlar, multimediali ilovalarda turli ko‘rinishdagi axborotlar integratsiyasi, lokal, shahar va mahalliy tarmoqlarning aloqasini tashkil etish uchun zarur.

Telekommunikatsiya tarmog‘i, tarmoqning moslashuvchanligi va ishonchliligini oshirish, global tarmoqlarni boshqarishni ancha osonlashtirish imkonini beruvchi intellektuallikka ega bo‘lishi kerak. Tarmoqlarning intellektualligi tufayli xizmatlardan foydalanuvchi passiv foydalanuvchidan faol mijozga aylanadi, ya’ni mijoz zarur bo‘lgan xizmatga buyurtma bergan holda, o‘zi tarmoqni faol boshqarishi mumkin.

Foydalanuvchining terminal qurilmasi mobil bo‘lishi kerak. Elektron qurilmalarni kichiklashtirish sohasidagi muvoffaqiyatlar, ularning narhini pasayishi, oxirgi mobil qurilmalarni keng tarqalishiga zamin yaratadi. Bu har qanday joyda va har qanday vaqtda har bir talabgorga aloqa xizmatlarini taqdim etishni haqiqiy masalasi hisoblanadi.

Hozirgi kunda dunyoning axborot telekommunikatsiya infratuzilmasi orqali uzatiladigan axborot hajmi har 2-3 yilda ikki martaga oshib bormoqda.

Kelajakdagi aloqa tarmoqlari quyidagi talablarga javob berishi lozim:

- multiservislik deganda, transport texnologiyalariga xizmatlarni yetkazuvchi texnologiyalarning bog‘liq emasligi tushuniladi;

- keng polosalilik deganda, odatda foydalanuvchi talablariga bog‘liq holda keng diapazonda axborotni uzatish tezligini mos holda va dinamik o‘zgarish imkoni tushuniladi;

- multimedialik deganda, tarmoqni haqiqiy vaqtda va murakkab ulanish konfiguratsiyasini qo‘llagan holda, ko‘p komponentli axborot (ovoz, video, audio)larni shu komponentlar uchun zarur bo‘lgan sinxronizatsiya bilan uzatish qobiliyati tushuniladi;

- intellektuallik deganda, foydalanuvchi yoki xizmatlarni ta’minlovchi tomondagi chaqiriq yoki ulanish xizmatlarini boshqarish imkoni tushuniladi;

- invariantlik ulanish deganda, qo‘llanilayotgan texnologiyalarga bog‘liq bo‘lmagan holda xizmatlarga ulanishni ta’minlash imkoni tushuniladi;

- ko‘p operatorlik deganda, xizmatlarni taqdim etishda va ularning ma’suliyatini faoliyat sohasiga mos holda taqsimlashda bir nechta operatorlarning qatnashishi tushuniladi.

XXI asrda dunyo hamjamiyati o‘zining, global axborot jamiyati (GAJ) deb nomlangan yangi rivojlanish erasiga o‘tdi. GAJ ning asosiy fazilati shundan iboratki, unda bilim va axborot tashqi ishlab chiqarish rolini egallaydi, ya’ni jamiyat mavjudligining material asosi bo‘lib qoladi. Yuqori texnologiyalarni qo‘llash mahsuslashtirilgan yangi soha, birinchi navbatda infokommunikatsiya muhitida dasturiy mahsulotlarni samarali taqsimlash amalga oshadi. GAJ ning boshqa xarakterli xususiyati, telekommunikatsiya xizmatlarining juda yuqori darajada o‘sishidir. Masalan faqatgina telefon, tele va radio eshittirish xizmatlaridan foydalanishning o‘zi bir yilda 800 milliard dollarni, infokommunikatsiya xizmatlari bozori (internet, lokal kompyuter tarmoqlari, harakatdagi aloqa tarmoqlari va b.q.) bilan birga esa 1,5 trln. dollarga yetdi va kengayish hali davom etmoqda.

Dunyo telekommunikatsiya tarmog‘iga har yili 200 mlrd. dollarlik telekommunikatsiya qurilmalari o‘rnatiladi. Yuqorida qayd etib o‘tilgan barcha ma’lumotlarni samarali uzatish va taqsimlash uchun GAJ tuzilishida butun dunyo aloqa tarmog‘i (World Wide Communication Network) yaratildi va rivojlanmoqda. Bu tarmoq, yer yuzidagi o‘zaro bog‘langan barcha milliy aloqa tarmoqlarining majmuasidan iborat. Barcha zamonaviy aloqa tarmoqlarining texnik asosini, ishlab chiqaruvchidan foydalanuvchiga axborotlarni standart yoki me’yorlashtirilgan raqamli oqimlar ko‘rinishida yuqori sifat va buzilishsiz uzatishga mo‘ljallangan axborotli transport tarmoqlari tashkil etadi.

Bugungi kunda global axborot jamiyatida turli xil xizmatlar, ya’ni videotelefoniya, videokonferens aloqa, teleeshittirish, radioeshittirish va ovozli eshittirish, yuqori tezlikda raqamli ma’lumotlar almashish, katta hajmdagi fayllarni uzatish, yuqori tezlikli telesignalizatsiya va telenazorat, yuqori sifatli tasvirlarni uzatish, axborot-ma’lumot tizimlari, masofadan o‘qitish kabi xizmatlarni o‘z ichiga

olgan zamonaviy va istiqbolli telekommunikatsiya xizmatlari doirasi kengaymoqda. Foydalanuvchilar turli xizmatlarga ulanish imkoniyatiga ega bo‘ldilar. Telekommunikatsiya tizimlarini kelgusi rivoji va raqobatbardoshligi, aloqa operatorlarini abonent tarmoqlarini modernizatsiya qilishdagi tanlagan yechimlariga bog‘liqdir.

Bugungi kunda mavjud bo‘lgan O‘zbekiston Respublikasi hududidagi ma’lumotlarni uzatishga mo‘ljallangan milliy tarmoqlar quyidagilarni amalga oshiradi:

- har tamonlama axborot uzatishga bo‘lgan talablarni qondirish maqsadida elektron axborotlarni almashtirishni amalga oshirish;

- Respublikaning yagona axborotli muhiti asosidagi transport-kommunikatsiyasini va uning jahon axborot hamjamiyatiga kirishini ta’minlash;

- Respublikaning ma’lumotlarni uzatuvchi operatorlarini (provayder) dunyoning markazlashtirilgan tarmog‘iga ulash, shu jumladan INTERNET ga;

- davlat va boshqaruv organlarini markazlashtirilgan elektron xizmat almashish bilan ta’minlash uchun sharoit yaratishdan iborat.

Yuqorida ta’kidlanganlarni inobatga olganda, zamonaviy davr jamiyatni axborotlashtirish jarayonini keskin rivojlanishga olib kirmoqda. Bu jarayon axborot-kommunikatsiya xizmatlaridan foydalanuvchilarni telekommunikatsiya tarmoqlariga yuqori tezlik bilan (keng polosali) ulanishga undaydi. Bunday talab Internetdan foydalanuvchilarning keskin oshib borishi va multimedia, videokonferensiya, elektron raqamli imzodan foydalanish, elektron tijorat, elektron xujjat aylanish va boshqa bir qancha zamonaviy xizmatlarni hayotga kirib kelishidan chiqib kelyapti.

# 1. MULTIMEDIALI TRAFIKNING UMUMIY TAVSIFLARI

## 1.1. Multimedia tushunchasi. Multimedianing xususiyatlari

Multimedia, multi – ko‘p, media — muhit deb tarjima qilinadi. Multimedia, turli (matn, grafika, rasm, tovush, animatsiya, video) ko‘rinishdagi axborot bilan bog‘liq. Bunda ma’lumot turli axborot tashuvchilarda mavjud bo‘lishi mumkin (magnit va optik disklar).

Multimedia – texnologiyalarining asosiy maqsadi – tovush, video, animatsiya va boshqa vizual effektlar bilan ta’minlangan dasturiy mahsulotlarni yaratishdan iboratdir.

1945 yilda amerikalik olim Vanniver Bush “MEMEX” nomli xotirani tashkil qilish g‘oyasini taklif qilgan, bu esa multimedia texnologiyalarini rivojlanishining g‘oyaviy sababi bo‘ldi. “MEMEX” nomli xotiraning asosiy g‘oyasi shundan iboratki, axborot belgilar, raqamlar, indekslar yoki alfabit tartibi bo‘yicha emas, balki mazmuniga qarab qidiriladi. “MEMEX” nomli xotira asosida gipermatn va gipermedia tizimlari yaratilgan.

Gipermatn - bu matnli ma’lumotlar bilan ishlash tizimi. Gipermedia - bu grafika, tovush, video va animatsiya bilan birgalikda ishlash tizimi hisoblanadi. Gipermatn va gipermedia tizimlarining birgalikdagi rivojlanishi multimedia yo‘nalishini kelib chiqishiga olib keldi.

80 – yillar oxirida amerikalik kompyuter mutaxassisi Bill Geyts “National Art Gallery of London” - “Londonning milliy san’at galereyasi” nomli dasturiy mahsulotni yaratgan. Bunda multimedia dasturini yaratishda turli muhitlardan – tasvir, tovush, animatsiya, gipermatn va gipermedia tizimlaridan foydalanilgan.

Multimedia texnologiyalarining asosiy afzalliklari va xususiyatlariga quyidagilar kiradi:

- bitta axborot tashuvchida katta hajmli turli ma’lumotlarni saqlash imkoniyati (20 ta tomga yaqin matnlar, 2000 va undan ham ko‘p yuqori sifatli tasvirlar, 30–45 minutli video yozuvlar, 7 soatga teng tovush ma’lumotlari);

- ekranda tasvirni yoki uning ayrim fragmentlarini kattalashtirish imkoniyati (“lupa” rejimi). Tasvirning sifatini saqlab qolgan holda 20 marotabagacha kattalashtirish mumkin. Bu imkoniyatdan tarixiy xujjatlar va san’at asarlarini taqdimot qilganda foydalanish mumkin;

- tasvirlarni taqqoslash va turli dasturiy vositalar yordamida ularni qayta ishlash;

- matnlar yoki turli ko‘rgazmali materiallarda kerakli joylarni belgilash va ular yordamida boshqa tushuntiruvchi ma’lumotga ega bo‘lish (gipermedia va gipermatn texnologiyasi);

- Internet global tarmog‘iga ulanish imkoniyati.

Uzatish nuqtai nazaridan multimedia haqiqiy vaqtda uzatiladigan (Real Time–RT) yoki haqiqiy vaqtda uzatilmaydigan (Non Real Time–NRT) sinflarga bo‘linishi mumkin. Birinchi turdagi multimedia (RT), paketlarni kechikishiga cheklashlarni talab etadi, xuddi shu vaqtda multimedianing ikkinchi turi (masalan matn va tasvir) bunday cheklashlarni talab etmaydi, lekin ularni uzatishda xatoliklar paydo bo‘lmasligi uchun qat’iy cheklashlarga ega.

Multimediali ma’lumotlarni uzatishda xatoliklarni nazorat qilish uchun ikkita asosiy yondashushlar mavjud. Birinchi yondashish, yo‘qolgan yoki shikastlangan paketlarni uzatishda avtomatik takrorlashga (Automatic Retransmission reQuest – ARQ) asoslangan. Bu yondashish transport sathidagi TCP (Transport Control Protocol) protokolida TCP/IP protokoli stekida qo‘llaniladi. NRT-axborotni xatolarsiz uzatishni talab qiluvchi ilova, odatda aynan shu protokolni talab etadi.

Ikkinchi yondashishda (Forward Error Correction – FEC), paketlarni qayta uzatmasdan xatoliklarni aniqlash va to‘g‘rilash imkonini beruvchi ortiqcha axborotlar uzatiladi. Bunday yondashuv TCP/IP protokolining shu stekida transport sathining

boshqa protokoli UDP (User Datagram Protocol) da qo‘llaniladi. Multimediali ma’lumotlarni almashuvchi, xatoliklarga yo‘l qo‘yuvchi (RT kabi NRT da ham) ilova, odatda paketlarni takroran uzatishda vaqt yo‘qotishlarini oldini olish uchun UDP ni qo‘llaydi.

RT - multimediali ma’lumotlarni diskret yoki uzluksiz oqim bilan uzatilishiga bog‘liq ravishda diskret (Discrete media – DM) va uzluksiz (Continuous media – CM) multimediaga bo‘linadi. O‘z navbatida SM xatoliklarga ruxsat beradigan va xatoliklarga ruxsat bermaydigan turlarga bo‘linishi mumkin. Birinchi turdagi RT-multimediaga misol qilib ovozli va videokonferensiyalarni o‘tkazishda qo‘llaniladigan ovozli va video oqimlarni olish mumkin. Ikkinchi turdagi RT-multimediaga misol qilib esa olisdagi kompyuterda ishga tushirilgan ilovani tushunish mumkin.

Quyidagi bo‘limlarda multimedianing turlari va ularning xarakteristikalari, o‘tkazish qobiliyati, ruxsat etiladigan xatoliklar va real vaqt rejimining o‘ziga xos xususiyatlari keltirilgan.

## 1.1. Matn

Matn boshqa multimedia turlaridan eng ommaviysi hisoblanadi. U Internet tarmog‘ida turli shakllar, shu jumladan turli uzatish protokollarini FTP (File Transfer Protocol: ikkilik va ASCII - fayllarni uzatish uchun), HTTP (Hyper Text Transfer Protocol: HTML - sahifalarni uzatish uchun) yoki SMTP (Simple Mail Transfer Protocol: pochta xabarlarini almashlash uchun) qo‘llaydigan fayllar yoki xabarlar orqali ifodalanadi. Matn ikkilik ko‘rinishda 7 - bitli US-ASCII, 8 - bitli ISO-8859, 16 - bitli Unicode yoki 32 - bitli ISO 10646 kodlash jadvallarida, qo‘llaniladigan til va davlatga bog‘liq ravishda ifodalanadi. Matnli ma’lumotlar uchun o‘tkazish qobiliyatiga talablar asosan uning o‘lchamiga bog‘liq bo‘ladi, ya’ni axborotlarni siqishni turli sxemalari qo‘llanilganda jiddiy kamayishi mumkin (1.1-jadvalda).

1.1-jadval

Matnni siqish usullari

| Siqish usuli | Izohlar |
|---|---|
| Shennon-Fano kodlashi | Yuqori paydo bo‘lish ehtimolligiga ega simvollar qisqaroq kodli so‘zlarga almashtiriladi |
| Xaufman kodlashi | Yuqoridagidek |
| LZW | Simvollar qatorini yagona kod bilan almashtirish. Matnni tahlil qilish bajarilmaydi. Buning o‘rniga simvollarni har bir yangi qatori qatorlar jadvaliga qo‘shiladi. |
| Unix-siqish | Kengayadigan lug‘atli LZW qo‘llaniladi. Dastlab lug‘at 512 elementlardan iborat bo‘ladi va zarurat bo‘lganida ikkilantiriladi |

Matnni uzatishda ruxsat etiladigan xatoliklar darajasiga talablar asosan qo‘llaniladigan ilovalarga bog‘liq bo‘ladi. Matnli fayllarni uzatadigan ilovalar xatoliklar to‘liq bo‘lmasligini talab qiladi va TCP protokolini qo‘llaydi. Boshqa ilovalar xatolikli ma’lumotlarni qandaydir foiziga ruxsat etishi mumkin va UDP protokolini qo‘llaydi.

Faqat matn bilan ishlaydigan ilovalar real vaqtda uzatish bilan bog‘liq bo‘lgan cheklashlarga ega emas. Shu bilan bir vaqtda, uzatiladigan uzluksiz xabarlar oqimi, ularni uzatishda kechikishlar qiymatiga sezilarli cheklashlarni qo‘yadi.

### 1.1.2. Tovush

Tovushli ma’lumotlarni diskretlash (sampling) va kvantlashni (quantization) qo‘llash bilan raqamli shaklga o‘zgartirilgan ma’lumotlar hisoblanadi. Raqamlashtirilgan tovush signali tarmoq bo‘ylab diskret paketlar oqimi sifatida uzatiladi. Tarmoqning o‘tkazish qobiliyatiga talablar tovushning tavsifiga bog‘liq.

Masalan, telefon bo‘yicha tovush 12 dan 8 bitgacha axborotlarni yo‘qotishli siqiladi. Bu uzatish tezligini 96 dan 64 Kbit/s gacha kamaytiradi. 1.2-jadvalda tovush fayllari uchun siqishni ayrim sxemalari ko‘rsatilgan.

1.2-jadval

Tovushni siqish usullari

| Tovush kodeki | Qo‘llanilishi | Tezligi (Kbit/s) |
|---|---|---|
| Impuls kodli modulyatsiya (G.711) | Tor polosali nutq (300-3300 Hz) | 64 |
| GSM | Shuning o‘zi | 13 |
| CS-ACELP (G.729) | » | 8 |
| G.723.3 | » | 6,4 va 5,3 |
| Adaptiv differensial impuls kodli modulyatsiya (G.726) | » | 32 |
| SBC (G.722) | Keng polosali nutq (50-7000 Hz) | 48/56/64 |
| MPEG layer III (MP3) | CD sifatli keng polosali nutq (10-22 KHz) | 128.112 |

Tovushli ma’lumotlar uzatish jarayonidagi xatoliklarni bo‘lishiga qat’iy talablarni qo‘ymaydi. 1...2 % paketlarning yo‘qotilishi uning sifatiga deyarli ta’sir qilmaydi. Bugungi kunda tovushni uzatishda qo‘llaniladigan ko‘plab multimediali ilovalar, yo‘qotilgan paketlarni takroran kiritish mexanizmiga ega.

Tovush uchun real vaqt talablari qatnashuvchi tomonlarning kutiladigan interaktivlik darajasi bilan qat’iy bog‘langan. Ikki tomonlama o‘zaro ta’sirlashishni ko‘zda tutadigan Internet-telefoniya kabi ayrim ilovalar yuqori interaktivlik darajasiga va qisqa chaqiriq vaqtlariga ega. Bu holda ma’qul tovush sifatini ta’minlash uchun paketlarning kechikishiga qat’iy talablar qo‘yiladi. Bunday multimedia turini qo‘llaydigan ilovalar haqiqiy vaqt rejimiga bog‘liq (Real-Time Intolerant - RTI)

ilovalar deyiladi. Ko‘plab RTI - ilovalarda 200 ms dan ortiq bo‘lmagan kechikishga ruxsat etiladi.

### 1.1.3. Grafika va animatsiya

Bu guruhga ham statik raqamli tasvirlar, ham flash-taqdimotlar kabi dinamik tasvirlar kiradi. Siqilmagan raqamli tasvir piksellar massividan tashkil topgan, bu yerda har bir piksel o‘z parametrlari bilan xotirada ma’lum bitlar miqdorida saqlanadi. Matnga qaraganda raqamli tasvir ancha katta xotirani talab qiladi. Masalan, 4 o‘lchamli tasvir 480 ekranni 640 piksellarga ruxsat etishida 6 dyumga va 24-bitli rangda bir megabayt atrofidagi xotirani talab qiladi. Bunday tasvirni tarmoq bo‘ylab 56,6 Kbit/s tezlikda uzatish taxminan ikki minutni egallaydi. Agar tasvir 10 martagacha siqilsa, 100 Kbayt atrofidagi xotira talab qilinadi va uzatish taxminan 14 sekundni egallaydi. Siqishni ayrim ommaviy sxemalari 1.3-jadvalda keltirilgan.

1.3-jadval

Tasvirni siqish usullari

| Siqish usuli | Izohlar |
|---|---|
| Graphics Interchange Format (GIF) | 256 tagacha ranglarni qo‘llaydi. LZWni (Lempel-Ziv-Welch) ishlatadi. Animatsiyali ma’lumotlarni yo‘qotishsiz siqish |
| Portable Network Graphics (PNG) | Istalgan sondagi ranglar qo‘llanadi. Siqiladigan bloklarni adaptiv filtrli zlib siqish sxemasi qo‘llaniladi. Ma’lumotlar yo‘qotishli va animatsiya qo‘llanilmaydigan sxema. |
| Joint Photographic Experts Group (JPEG) | Ko‘p sonli rangli tuslarga (yoki kul rang tusli) ega oq-qora va rangli fotosuratlarni siqish uchun eng yaxshi tarzda to‘g‘ri keladi. Siqishning bu standarti Xaufman kodi bo‘yicha va tasvir bloklari koeffitsientlarini diskret kosinusli o‘zgartirish jarayonida |

| | |
|---|---|
| | turkumlar uzunliklari kodlarini qo‘llashga asoslanadi. Siqish natijasida ma’lumotlarni yo‘qotilishi yuz beradi. Standart JPEG satr oralatib yoyishga ruxsat etmaydi, lekin u progressiv format (Progressive JPEG) qo‘llaydi. Progressive JPEG tasvirning yirik bloklarini keyingi ularni detallashtirish bilan boshlaydi. |
| JPEG-2000 | Tasvirlarning keng spektri uchun to‘g‘ri keladi, shuning uchun portativ raqamli kameralarda ishlatiladi. Ma’lumotlarni bloklarda emas, balki ma’lumotlar oqimida saqlaydigan veyvletlarga (wavelet) asoslangan joriy etilgan texnikani qo‘llaydi. Bu sxema ma’lumotlarni masshtablanadigan yo‘qolishiga ham olib keladi. |
| JPEG-LS | Bitta tonli tasvirlar uchun to‘g‘ri keladi. Sxema HP da ishlab chiqilgan LOCO-I (Low Complexity LOssless Compression for Images) algoritmiga asoslangan. Bu ma’lumotlarni yo‘qotishsiz yoki deyarli yo‘qotishsiz sxema. |
| Joint Bi-level Image Experts Group (JBIG) | Oq-qora tasvirlar uchun to‘g‘ri keladi. Ma’lumotlarni yo‘qotishsiz ko‘p tomonlama arifmetik kodlash sxemasi qo‘llaniladi. |

Ko‘plab zamonaviy siqish sxemalari o‘sish xarakteriga ega, bu kommunikatsiya tarmoqlari bo‘yicha tasvirlarni uzatishda juda muhimdir. Bunday tasvir olinganida foydalanuvchi dastlab past sifatli variantni ko‘radi, keyin u asta-sekin yaxshilanadi. Odatda u haqda umumiy tasavvurni olish uchun 5...10% tasvirni olish yetarli bo‘ladi. Tasvirlar qandaydir uzatish xatoliklari darajasiga bog‘liq, shuning uchun yo‘qotilgan ma’lumotlarni qayta tiklash mumkin. Bundan tashqari, ular haqiqiy vaqtda uzatishga cheklashlarni qo‘ymaydi.

### 1.1.4. Video

Video odatda sekundiga 24 yoki 30 kadrlar ma’lum tezlikda ko‘rsatiladigan kadrlarning ketma-ketligi hisoblanadi. Raqamli video, raqamlashtirilgan ovoz kabi tarmoq bo‘yicha diskret paketlar oqimida uzatiladi.

1.4-jadval

Videoni siqish usullari

| Siqish usuli | Izohlar |
|---|---|
| MPEG-I | CD-ROM ga (CD-I va CD-Video formatlari) yozish uchun VCRNTSC (352 x 240) formatdagi va 1,2 Mbit/s uzatish tezligidagi siqish uchun qo‘llaniladi. |
| MPEG-II | Audio va videoni kodlash uchun umumiyroq standart. Uzatish rejimida xatoliklardan himoyalashni qo‘llaydi. DVB va High Definition Television (HDTV) uzatish sifatidagi siqishni qo‘llaydi. MPEG-2, 4 ta variantdagi ruxsat etishni qo‘llaydi: past (low) (352x240), asosiy (main) (720x480), yuqori - 1440 (high-1440) (1440x1152) va yuqori (high) (1920x1080). Ma’lumotlarni uzatish tezligi 3...100 Mbit/s intervalda bo‘ladi |
| MPEG-IV | Past o‘tkazish qobiliyatli tarmoqlar (64 Kbit/s) uchun siqishni qo‘llaydi. Bu format multimedianing barcha komponentlarini bir xil yaxshi siqadi |
| H.261 | ISDN bo‘yicha 64 Kbit/sga karrali bo‘lgan tezliklarda videoni uzatishni qo‘llaydi. Sxema ham freymlar ichida, ham ular orasida siqishga asoslangan |
| H.263 | Sxema juda past o‘tkazish qobiliyatli (18.64 Kbit/s) simsiz tarmoqlar bo‘yicha videoni uzatish uchun mo‘ljallangan |

O‘tkazish qobiliyatiga talablar har bir kadrda, ham ularning ketma-ketligidagi ortiqchalik darajasiga bog‘liq bo‘ladi. Bu har ikkala ma’lumotlarni ortiqchalik turlari videoni siqish algoritmlari uchun ishlatilishi mumkin. 1.4-jadvalda ayrim keng tarqalgan videoni siqish usullari keltirilgan. Uzatish va haqiqiy vaqtda uzatish xatoliklari bo‘lishiga cheklashlar ovoz uchun cheklashlarga o‘xshash.

## 1.2. Tarmoq bo‘ylab multimedili ilovalarni uzatishga bo‘lgan talablar

Bu bo‘limda biz taqsimlangan multimediali ilovalarni uzatish tarmog‘iga qo‘yiladigan talablarni ko‘rib chiqamiz. Ular ikki toifaga bo‘linishi mumkin: trafikka bo‘lgan talablar va funksional talablar. Trafikka bo‘lgan talablar real vaqt talablarini (kechikish va nostabillik, o‘tkazish qobiliyati va ishonchlilik), funksional talablar esa multimedia xizmatlarini (multikasting, xavfsizlik, mobillik va seanslarni boshqarish) qo‘llashni o‘z ichiga oladi.

Trafikka bo‘lgan talablarni faqat Internetning bazaviy arxitekturasini kengaytirish bilan qoniqtirish mumkin, shu bilan bir vaqtda funksional talablarni TCP/IP protokollar stekiga yangi protokollarni kiritilishi bilan bajarish mumkin. Funksional talablar shu ma’noda absolyut zarur hisoblanmaydi, ya’ni taqsimlangan multimediali ilovalar ilovaning o‘ziga zarur bo‘lgan funksiyalarni kiritilishi bilan yuqori unumdorlikda ishlashi mumkin.

### 1.2.1. Real vaqt xarakteristikalari

Yuqoridagi bo‘limlarda ko‘rib chiqilganidek, tovush va video kabi multimedia komponentlari real vaqt rejimida uzatish bo‘yicha talablarni qo‘yadi. Masalan, ular raqamlashtirilgan tezlikda qayta ishlanishi kerak. Uzatishdagi istalgan kechikishda bu birdaniga aniqlanadi. Internet-telefoniyada inson 200 ms dan ortiq bo‘lmagan kechikishlarga xotirjam munosabatda bo‘lishi mumkn. Shunday qilib, real vaqtda

multimediani uzatish paketlarning kechikishi va ularnig kelish intervallariga qat’iy talablarni qo‘yadi.

### 1.2.2. Yuqori o‘tkazish qobiliyatiga bo‘lgan talablar

Ravshanki, multimediali ilovalar ilgari keng tarqalgan matnli ilovalarga qaraganda tarmoqlarning sezilarli yuqori o‘tkazish qobiliyatini talab qiladi. Shu bilan birga, multimediali oqimlar tarmoqning o‘ta yuklanishini nazorat qilish mexanizmiga ega bo‘lmagan UDP protokolidan foydalanish bilan uzatiladi.

1.5-jadval

Multimediani turli elementlari uchun o‘tkazish qobiliyatiga bo‘lgan talablar

| Ovoz | Tanlash tezligi | Bitlar soni | Bitlardagi tezlik |
|---|---|---|---|
| Telefon bo‘yicha ovoz ( 3,4 kHz gacha) | 8000 m/s | 12 | 96 Kbit/s |
| Keng polosali nutq ( 7 kHz gacha) | 1600 m/s | 14 | 224 Kbit/s |
| Ikki tomonlama keng polosali nutq (20 kHz gacha) | 44,1 m/s | kanalga 16 | Har ikkala kanalga 1,412 Mbit/s |
| Tasvir | Piksellar | bit/piksel | Bitli tezlik |
| Rangli tasvir | 512x512 | 24 | 6,3 Mbit/s |
| CCIR TV | 720x576x30 | 24 | 300 Mbit/s |
| HDTV | 1280x720x60 | 24 | 1.327 Gbit/s |

1.5-jadvalda eng keng tarqalgan multimedia turlari uchun o‘tkazish qobiliyatiga bo‘lgan talablar keltirilgan. Ma’lumotlarni yo‘qotishli va yo‘qotishsiz siqish turlari mavjud. Ma’lumotlarni yo‘qotishli siqishda ma’lumotlardan ortiqcha ma’lumotlarni o‘chirishdir, bu ko‘pincha buzilishlar yoki shovqinlarni paydo bo‘lishiga olib keladi. Ma’lumotlarni yo‘qotishsiz siqishda ma’lumotlar yo‘qolmaydi va olinadigan ma’lumotlar uzatiladigan ma’lumotlar bilan bir xil bo‘ladi. Odatda ma’lumotlarni yo‘qotishli siqish ma’lumotlarni yo‘qotishsiz siqishga qaraganda katta siqish darajasini beradi. Lekin ayrim ilovalarda ma’lumotlarni yo‘qotilishiga ruxsat etilmaydi (masalan, tibbiyot telemetriyasini uzatishda).

### 1.2.3. Xatoliklarga bo‘lgan talablar

Yuqorida ta’kidlanganidek, turli multimedia turlarini tarmoq bo‘ylab uzatishda xatoliklarni bo‘lishiga turli talablar qo‘yiladi. Xatoliklar paketlarning shikastlanishida va yo‘qolishida vujudga keladi. Uzatishda xatoliklarga ruxsat etiladigan ilovalarning ko‘pchiligi xatoliklarni niqoblash texnikasini qo‘llaydi (error concealment techniques - FEC), u boshqa paketlardagi ma’lumotlar asosida yo‘qotilgan ma’lumotlarni qayta tiklash imkonini beradi.

FECdan foydalanilganda paketlar oqimida bo‘lishi mumkin bo‘lgan xatoliklarni tuzatish uchun qo‘shimcha ma’lumotlar qo‘shiladi. Lekin, paketlarni uzatish jarayonida FEC darajasidan tashqarida xatoliklar paydo bo‘lsa, ular aniqlanmay qolishi mumkin. Demak, paketlarni xatoliksiz uzatish uchun FECni kerakli drajasini ta’minlash uchun, multimediali ilova uchun kommunikatsiya tarmoqlarida qo‘llaniladigan xatoliklar turini bilish muhim. Masalan, simsiz tarmoqlar simli tarmoqlarga qaraganda xatoliklardan yuqoriroq himoyalanish darajasini talab qiladi, chunki ularda paketlarni yo‘qolish ehtimolligi sezilarli yuqori. FECdan foydalanish bilan erishiladigan, paketlarni takroran uzatilishini minimallashtirish simli tarmoqlarda juda qimmat bo‘lishi mumkin, chunki ularda

paketlarni yo‘qolish ehtimolligi juda kichik. FECni qo‘shimcha ma’lumotlarini uzatish uchun tarmoqni o‘tkazish qobiliyatini oshirishga ham qo‘shimcha harajatlar talab qilinadi.

### 1.2.4. Multikastni qo‘llash

Multikastda bitta manba bir vaqtda bir necha multimediali ma’lumotlarni oluvchiga qo‘llaniladi. U eng ommaviy taqsimlangan multimediali ilovalarni qo‘llaydi. Masalan, bir necha qatnashuvchilar bilan videokonferensiya Internet-telefoniyadagi eng keng qo‘llaniladigan xizmatlardan biri hisoblanadi.

Multikastni ikki tomonlama ma’lumotlarni uzatishga qaraganda bir tomonlama ma’lumotlarni uzatishda ta’minlash oson. Masalan, Internet-radiodan foydalanishda multikast ma’lumotlarni jo‘natuvchiga balanddan, uni oluvchiga tarmoqli va daraxt tugunlarida mos zahiralangan paketlarni aloqa daraxtini yaratish bilan ta’minlanadi. Lekin ikki tomonlama kommunikatsiyada, masalan, Internet-telefoniyada bir necha qatnashuvchilar uchun turli qatnashuvchilardan ovozli oqimlarni to‘g‘ri aralashtirish uchun qandaydir funksiyaga ega bo‘lish zarur. Aks holda har bir qatnashuvchini qolganlar bilan ko‘plab ikki tomonlama aloqa kanallarini qo‘llashga to‘g‘ri keladi, bu uzatish tarmog‘iga juda yuqori yuklamani berishi mumkin.

### 1.2.5. Seanslarni boshqarish

Seanslarni boshqarish quyidagilarni o‘z ichiga oladi:

• Multimedia turining tavsifi. Bu ma’lumotlar multimedia (ovoz, video yoki ma’lumotlar), kodlash sxemalari, seansning boshlanishi va oxiri, xostlar ishlatadigan IP-adreslari va boshqalar kabi seansning parametrlarini ko‘rsatish uchun taqsimlangan multimediali ilovalar zarur. Ko‘pincha sessiyani uning boshlanishigacha tavsiflash muhim, chunki seans qatnashchilari multimediani qabul

qilish bo‘yicha turli imkoniyatlarga ega bo‘lishi mumkin.

• Seans haqida ogohlantirish. Qatnashuvchilarni bo‘lajak seans haqida ogohlantirishga imkon beradi. Masalan, Internetda turli kanallar bo‘yicha tarqaladigan yuzlab radiostansiyalar mavjud. Seans haqida ogohlantirish bunday radiostansiyalarga potensial tinglovchilar uchun tarqatish jadvali haqidagi ma’lumotlarni tarqatishga imkon beradi.

• Seansni identifikatsiyalash. Multimediali seans ko‘plab oqimlardan, shu jumladan uzluksiz (ovoz, video) va diskret (matn, tasvir) oqimlardan tashkil topgan. Masalan, jo‘natuvchi bitta kanal bo‘yicha ovoz va videoni ikkita turli oqimlar sifatida jo‘natishi mumkin, ular olinganida sinxronlashgan bo‘lishi kerak. Yoki aksincha, jo‘natuvchi ovoz va videoni birgalikda jo‘natishi, lekin qayta tiklashni oluvchilarning imkoniyatlariga bog‘liq ravishda sifat bo‘yicha bir necha darajalarga bo‘lish mumkin.

• Seansni boshqarish. Turli oqimlardagi ma’lumotlar ichki aloqalarga ega bo‘lishi mumkin va bu uni uzatishda hisobga olinishi kerak. Bu multimediani sinxronlashtirish deyiladi va vaqt belgilarini (time stamps) uzatiladigan paketlarga qo‘yib chiqilishi bilan erishilishi mumkin. Shu bilan birga, bunday oqimli multimediani oluvchilar oddiy videomagnitofonlarda bajariladigandek qayta eshittirishni boshqarish imkoniyatiga ega bo‘lishni istab qolishi mumkin

### 1.2.6. Xavfsizlik

Multimediani uzatish jarayonini muhokama etishda ko‘pincha xavfsizlik masalalari haqida unutib qo‘yiladi. Lekin real vaqt xizmatlaridan foydalanishning ortishi bilan xavfsizlik masalalari yetarlicha muhim bo‘lib qoladi. Bunday multimedia uchun xavfsizlik uchta jihatlar – yaxlitlik, asliga to‘g‘rilik, shifrlanish bilan ifodalanadi. Masalan, ommaviy uzatish ma’lumotlarni yaxlitligi va asliga to‘g‘riligini, xususiy uzatish esa shifrlanishini talab qiladi. Buning uchun turli kriptografik sxemalarni qo‘llash mumkin.

Yana bir muammo multimedia komponentlariga mualliflik huquqlarini saqlanishi hisoblanadi. Masalan, dastlabki to‘lov bo‘yicha filmlarning yetkazib berilishini ko‘rib chiqamiz. Olingan filmlardan tijorat maqsadlarida foydalanish imkoniyati mavjud. Multimediaga qo‘shimcha ma’lumotlarni qo‘shadigan zamonaviy raqamli texnologiyalar bunday buzishlarning oldini olishga yordam berishi mumkin.

### 1.2.7. Mobillikni qo‘llash

Simsiz va sotali tarmoqlardan yanada keng foydalanish multimedia ilovalarini mobillikka tortadi. Sotali tarmoqlar juda katta maydonlarni qamrab oladi va yuqori mobillik darajasini ta’minlaydi. IEEE 802.11x kabi simsiz tarmoqlar nisbatan uncha katta bo‘lmagan oraliqlarni qamrab oladi va cheklangan mobillik darajasiga ega. Lekin bunday tarmoqlar katta uzatish tezliklariga ega va foydalanuvchilarni ulash uchun qulayroq.

Mobillik jihati multimediali tarmoqlarni o‘zgarishiga olib keladi. U mobil terminallarni marshrutlashtirish, simli va simsiz tarmoqlarning o‘zaro ta’sirlashishi va boshqa muammolarni ko‘taradi.

## 1.3. Multimediali trafik klassifikatsiyasi

**Multimediali trafik.** Multimediali trafik deganda insonning sezgi organlari qabul qilib oladigan turli xil axborotlarni o‘z ichiga olgan ma’lumotlarning raqamli oqimi (odatda tovushli va/yoki video axborot) tushuniladi. Ma’lumotlarning multimediali oqimlari uzoqlashtirilgan interaktiv xizmatlarni taqdim etish maqsadida telekommunikatsiya tarmoqlari bo‘yicha uzatiladi. Tarmoq foydalanuvchilariga taqdim etiladigan multimediya xizmatlarining bugungi kunda eng ko‘p tarqalganlari videotelefoniya, multimediali ma’lumotlarni yuqori tezlikda uzatish hisoblanadi.

Taqdim etiladigan xizmatlarning turiga bog‘liq holda multimediali trafikning ikkita asosiy turi ajratiladi:

1. Foydalanuvchilar o‘rtasida haqiqiy vaqt miqyosida axborotni uzatish uchun multimediyali xizmatlarni taqdim etadigan haqiqiy vaqt trafigi.

2. Zamonaviy telekommunikatsiya tarmog‘ining an’anaviy taqsimlangan xizmatlari bilan tashkil etiladigan oddiy ma’lumotlar trafigi, jumladan, elektron pochta, fayllarni uzatish, virtual terminal, ma’lumotlar bazasiga uzoqlashtirilgan kirish va boshqalar.

Haqiqiy vaqt trafigini qo‘llab-quvvatlovchi xizmatlarga misol sifatida quyidagilarni keltirish mumkin: IP-telefoniya, yuqori sifatli tovush, videotelefoniya, videokonferens aloqa, masofadan turib tibbiy xizmat ko‘rsatish (diagnostika, monitoring, maslahat), videomonitoring, keng eshittirishli video, raqamli televideniya, radio va televizion dasturlarni olib ko‘rsatish.

**IP-telefoniya.** Mazkur xizmat tarmoqning ikki abonenti o‘rtasidagi tovush trafigini (nutqni) uzatadi, unda tarmoq trafigi sifatida IP protokol (Internet Protocol)dan foydalaniladi. “IP-telefoniya” xizmatini tashkil etish uchun mahalliy, korporativ, global tarmoqlar, hatto Internet tarmog‘idan foydalanish mumkin. Umumiy foydalanishda qo‘llaniladigan maxsus shlyuzlar yordamida telefon tarmoqlari abonentlari va ma’lumotlar uzatish tarmoqlari abonentlari o‘rtasida IP-telefoniya aloqasi ta’minlanadi.

**Yuqori sifatli tovush.** Yuqori sifatli tovush deganda shunday xizmat tushuniladiki, bu xizmat yuqori sifatli tovushni, masalan, musiqa, konsertlardagi chiqishlarni va eshittirishni uzatishni amalga oshiradi.

**Videotelefoniya.** Mazkur xizmat ikki abonent o‘rtasida insonlar nutqini uncha yuqori bo‘lmagan sifatdagi uning tasviri bilan birga uzatishni amalga oshiradi. Bu xizmat mijozlari tegishli kommutatsiya qurilmasi orqali haqiqiy vaqt rejimida bir-birlarini eshitishlari va ko‘rishlari mumkin.

**Videokonferensiya.** Mazkur xizmat abonentlar guruhi o‘rtasida tovushli va videotrafikni uzatishni amalga oshiradi, bunda tovush va videosignallar bir-biriga bog‘liq bo‘lmagan holda (turli transport birikmalari bo‘yicha) tarmoq orqali uzatiladi, ularning qabul qilishdagi sinxronlanishi transport darajasidagi tegishli protokol bilan ta’minlanadi.

**Masofadan tibbiy xizmat ko‘rsatish.** Mazkur xizmat bemorlarni masofadan tibbiy tekshirish, tashxis qo‘yish va maslahat berishni ta’minlaydi. Mazkur xizmat trafigi haqiqiy vaqt miqyosida uzatilgan tovush va video ma’lumotlarni, tekshiruv natijalarini va boshqalarni o‘z ichiga oladi.

**Videomonitoring.** Mazkur xizmat xonalarning videokuzatuvini amalga oshiradi, turli vazifalarni bajaruvchi hududlarni qo‘riqlash, turli xil noan’anaviy vaziyatlar to‘g‘risida tezkor xabardor qilish, odamlar to‘planadigan joylarni doimiy monitoring (haqiqiy vaqt rejimida) qilish uchun qo‘llaniladi.

**Radio va televizion dasturlarni olib ko‘rsatish.** Mazkur xizmat radio va televizion kanallarni raqamli telekommunikatsiya tarmog‘i orqali uzatib ko‘rsatishni amalga oshiradi.

**Raqamli televideniya.** Mazkur xizmat uning mijozlari talabiga ko‘ra yuqori sifatli raqamli televideniya ko‘rsatuvlarini (badiy filmlar, musiqali videokliplar, sport translyatsiyalari) amalga oshiradi.

Zamonaviy telekommunikatsiya tarmoqlarining rivojlanishida asosiy yo‘nalish xizmatlarning turli xil ko‘rinishlarini, shu jumladan, multimediali xizmatlarni ham qo‘llab-quvvatlash hisoblanadi. Multimediali trafikning turli xil ko‘rinishlarining tarmoq resurslariga bo‘lgan talablari juda jiddiy tarzda farq qilishi mumkin. Masalan, oddiy trafik, odatda, uni foydalanuvchiga yetkazib berish vaqtiga alohida cheklashlar qo‘yilmaydi. Bunday trafikka qo‘yiladigan talablarning hammasi – bu yangi minimal o‘tkazish qobiliyatini ajratishdir. Haqiqiy vaqtda videokonferensiya o‘tkazish uchun trafik boshqa misol bo‘lishi mumkin. U katta o‘tkazish qobiliyatinigina emas, balki qabul qiluvchiga videokadrlarni yetkazib berish vaqtini minimallashtirishni talab etadi.

Bundan tashqari, agar axborotli paketlarning kechikishlari nihoyatda nomuntazam xususiyatga ega bo‘lsa, videokonferensiya seansini o‘tkazish sifati qoniqarli bo‘lmaydi. Mazkur holda, tarmoq resurslariga ko‘pgina parametrlar bo‘yicha qat’iy talablar qo‘yiladi. Bu parametrlar quyida batafsil ko‘rib chiqiladi.

Zamonaviy telekommunikatsiya tarmoqlarida multimediali trafikni tavsiflash, tahlil qilish juda murakkab va qiyin vazifa hisoblanadi. Bunday qiyinchiliklarning asosiy belgilari quyidagilardan iborat:

- uzatish tezliklarining keng diapazoni – telefon trafigini uzatishdagi kabi bir necha Kbit/s dan to videokonferensiyani uzatishdagi kabi yuzlab Mbit/s gacha;

- uzatilayotgan multimediali axborot oqimlarining turli xil statistik xossalari (haqiqiy vaqt trafigi tarmoq resurslariga qat’iy talablar qo‘yadi);

- tarmoq konfiguratsiyalarining juda katta xilma-xilligi, uzatish texnologiyalari va protokollarining ko‘pligi (Gigabit Ethernet, ATM, MPLS va boshqalar);

- uzatilayotgan axborotlarga ko‘p darajali ishlov berishni, buning oqibatida xizmat ko‘rsatish sifati ishlov berishning bir necha darajasiga bog‘liq bo‘lib qoladi.

## 1.4. Multimediali trafik parametrlariga umumiy yondashuv

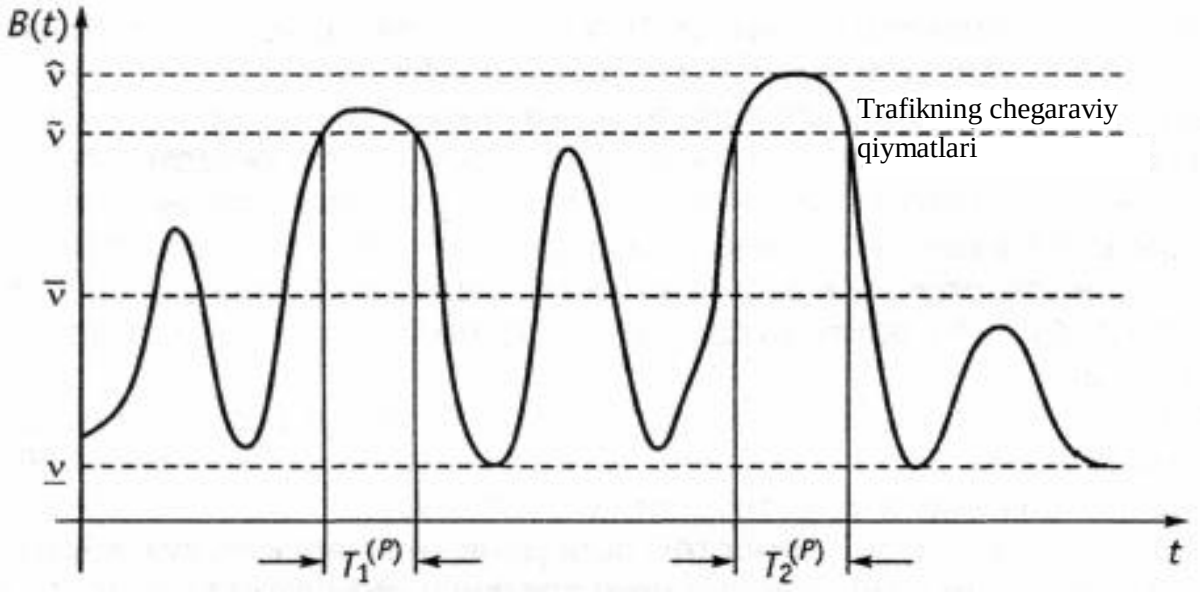
Turli telekommunikatsiya tarmoqlarida trafik tavsifining juda ko‘p modellari mavjud. Umumiy holda biror xizmatning multimediyali trafigi tasodifiy jarayon ko‘rinishida taqdim etiladi. Trafikning oniy qiymatlari – vaqt birligi ichida mos xizmatni qo‘llab-quvvatlaydigan axborot bloklari sonidan iborat bo‘lsin. U holda, yanada umumiy holda tasodifiy B(t) jarayon $F_{B(t)}$ (x) taqsimlanishlar funksiyasi oilasi bilan tavsiflanadi, bunda

$$F_{B(t)}(x) = Bep\{B(t)\hat{O}\tilde{o}\}. \qquad (1.1)$$

Tavsiflashning bunday usulidan amaliy foydalanish juda qiyin (umumiy ko‘rinishdagi bunday nobarqaror yuklanish sifatining parametrlarini baholashni

ta’minlovchi matematik qurilma yaratilmagan, $F_{B(i)(x)}$ taqsimlash funksiyasi oilasini adekvat baholashda murakkabliklar mavjud).

Multimediali trafikning parametrlarini o‘rganish uchun, odatda, ITU-T tavsiyanomalari bilan aniqlangan bir qator tavsiflardan foydalaniladi. Bu tavsiflar B(t) tasodifiy jarayonning integral parametrlarini ifodalaydi, uni amalga oshirish namunasi 1.1-rasmda keltirilgan.




1.1-rasm. Multimediali trafikning asosiy parametrlari

Turli xil multimediali xizmatlar bilan ta’minlanadigan trafikning tavsiflariga quyidagilar kiradi:

-trafikning qiymatlari (oniy, maksimal, cho‘qqi (eng yuqori), o‘rta va minimal), bit/s;

- trafikning bo‘laklilik koeffitsienti (pulsatsiya);

- cho‘qqi trafikning o‘rtacha davomiyligi;

- aloqa seansining o‘rtacha davomiyligi;

- trafik elementlari formatlari;

- paketning maksimal, o‘rtacha va minimal o‘lchamlari;

- trafikning jadalligi.

*Trafikning maksimal qiymati* $\hat{\nu}$ . Tegishli xizmat vaqt birligida beradigan axborot bloklarining maksimal soni quyidagi tarzda aniqlanadi.

$$\hat{\nu} = \max B(t) \ . \tag{1.2}$$

Trafikning cho‘qqi qiymati tegishli xizmatning trafigi bo‘lib, u uning uchun belgilangan cho‘qqi bo‘sag‘a $\hat{\nu}$ dan ortiq bo‘ladi.

*Trafikning o‘rtacha qiymati* $\bar{\nu}$ . Tegishli xizmat vaqt birligida ta’minlaydigan axborot bloklarining o‘rtacha soni quyidagicha aniqlanadi,

$$\bar{\nu} = \frac{1}{T^{(s)}} \int_0^{T^{(s)}} B(t)dt \tag{1.3}$$

bu yerda $T^{(s)}$ – aloqa seansining davomiyligi.

*Trafikning minimal qiymati* $\underline{\nu}$ . Tegishli xizmat vaqt birligida axborot bloklarining minimal soni quyidagicha aniqlanadi.

$$\underline{\nu} = \min_t B(T) \ . \tag{1.4}$$

*Trafikning pachkalilik (bo‘laklilik) koeffitsienti K*. Tegishli xizmatning maksimal va o‘rtacha trafigi o‘rtasidagi nisbat tarzida aniqlanadi. Bo‘laklilik koeffitsienti quyidagi nisbat orqali aniqlanadi.

$$K = \frac{\hat{\nu}}{\bar{\nu}}. \tag{1.5}$$

*Cho‘qqining o‘rtacha davomiyligi* $\bar{\tau}^{(P)}$ . Tegishli xizmat cho‘qqi trafigini to‘ldiradigan vaqt oralig‘ining o‘rtacha davomiyligi quyidagi munosabat orqali aniqlanadi:

$$\bar{T}^{(P)} = \frac{1}{N^{(P)}} \sum_{i=1}^{N^{(P)}} T_i^{(P)} \qquad (1.6)$$

bu yerda *N(P)* – aloqa seansi davomida cho‘qqilar soni, $T_i^{(P)}$ – *B(t)* jarayonning *i*-cho‘qqisi davomiyligi, $i = \overline{1, N^{(P)}}$, *i*-cho‘qqining davomiyligi quyidagi ifodalar bilan aniqlanadi:

$$T_i^{(P)} = t_i^{(e)} - t_i^{(s)}, \qquad (1.7)$$

bu yerda $t_i^{(s)}$ va $t_i^{(e)}$ - *i*-cho‘qqining boshlanish va tugash vaqtlari, ular quyidagi ifodalar bilan aniqlanadi:

$$t_i^{(s)} = \min_{\substack{B(t)>\bar{\nu} \\ t>t_{i-1}^{(s)}}} t, \; t_i^{(e)} = \min_{\substack{B(t)>\bar{\nu} \\ t>t_i^{(s)}}} t, \quad \text{bu yerda} \quad t_0^{(s)}, \; t_0^{(e)} = 0 \qquad (1.8)$$

Yuqorida sanab o‘tilgan parametrlar tegishli xizmat trafigini tavsiflash uchun abonent xizmati bilan bir seans aloqa mobaynida foydalaniladi.

*So‘rovlar intensivligi* $\lambda$ – tegishli xizmatda tarmoq abonentlarining xizmatni olishga talablari vaqt birligida kelib tushgan talablarning o‘rtacha soni tarzida aniqlanadi.

*Aloqa seansining o‘rtacha davomiyligi* $\bar{T}^S$ – tegishli xizmat kelib tushgan talabga xizmat ko‘rsatadigan vaqt oralig‘ining o‘rtacha davomiyligi.

*Paketning maksimal o‘lchami* $S$ – trafikning bit hisobidagi elementlarining maksimal o‘lchami (trafik elementi adresga yagona butun tarzda uzatiladi).

*Paketning o‘rtacha o‘lchami* $\bar{s}$ – trafikning bit hisobidagi elementining o‘rtacha o‘lchami.

*Paketning minimal o‘lchami* $\breve{s}$ – trafikning bit hisobidagi elementining minimal o‘lchami.

Tegishli manbaalar bilan to‘ldiriluvchi trafikning ayrim umumiy parametrlari 1.6-jadvalda keltirilgan.

1.6-jadval

Multimediali xizmatlar trafigining parametrlari

(umumiy qiymatlar)

| Multimediali xizmatlar turi | Multimediali trafiklarning parametrlari | | | | | |
|---|---|---|---|---|---|---|
| | J, Mbit/s | $\nabla$, Mbit/s | K | $T_0^{(p)}$ | $T_0^{(s)}$ | $\lambda$, seans/sut |
| IP-telefoniya | 0.064 | 0.064 | 1 | 100 | 100 | 5 |
| Yuqori sifatli tovush | 1 | 1 | 1 | 53 | 53 | 3 |
| Videotelefoniya | 10 | 2 | 5 | 1 | 10 | 6 |
| Videokonferensiya | 10 | 2 | 5 | 1 | 1000 | 6 |
| Masofadan tibbiy xizmat ko‘rsatish | 10 | 2 | 5 | 1 | 1000 | 3 |
| Videomonitoring | 10 | 2 | 5 | - | - | 6 |
| Radio va televizion dasturlarni olib ko‘rsatish | 34 | 34 | 1 | - | - | 6 |
| Raqamli televideniya | 34 | 34 | 1 | - | 5400 | 6 |

## 1.5. O‘ziga o‘xshash trafik to‘g‘risida tushuncha

Turli mamlakatlarning olimlari tomonidan keyingi 10 yilliklar mobaynida o‘tkazilgan juda ko‘p tadqiqotlar shuni izohlaydiki, paketlar kommmutatsiyasi asosidagi zamonaviy telekommunikatsiya tarmoqlarining trafigi, telefon tarmoqlarini kanallar kommutatsiyasida o‘zini yaxshi namoyon etgan Markov modellari va Erlang

formulalariga asoslangan odatdagi usullardan foydalanishga imkon bermaydigan alohida tuzilmaga ega. Teletrafikaning bu xususiyatlariga e'tibor qilmaslik, yuklanishni to‘g‘ri baholamaslikka va o‘zini oqlamaydigan qarorlar chiqarishga olib keladi.

Bu xususiyat teletrafikaning o‘ziga o‘xshashlik effektini namoyon bo‘lishi bilan bog‘liq. O‘ziga o‘xshash trafikda nisbatan past, o‘rta daraja sharoitida ma'lum miqdordagi yetarlicha kuchli chiqarib tashlashlar bo‘ladi, bu esa xatto trafikning o‘rtacha intensivligi mazkur kanalda uzatish mumkin bo‘lgan darajadan ancha past bo‘lganida ham o‘ziga o‘xshash trafikni tarmoq orqali o‘tishidagi kechikishlari va djitterlari ancha ortadi.

O‘ziga o‘xshash jarayonlar uzun xotirali jarayonga kiradi, bu esa ularning nisbatan yaqindagi o‘tishini bilgan holda ularning kelajagini bashorat qilish imkonini beradi. Shuni ta'kidlash kerakki, teletrafikani bashorat qilish xizmat ko‘rsatish sifatini (QoS) oshirishni ta'minlovchi tarmoqlarning ishlash algoritmini ishlab chiqishda nihoyatda muhim. Xizmatlar provayderlari uchun tarmoqlarning yuklanishini bashorat qilish, ularni o‘z vaqtida rivojlanishini rejalashtirishga imkon beradi.

Hozirgi vaqtga kelib, Ethernet, SS7, VoIP, TCP va boshqa keng tarqalgan protokollardan foydalanishda o‘tkazuvchi tarmoqlarda trafik o‘ziga o‘xshash tuzilmaga ega bo‘lishi keltirilgan. Xuddi shunga o‘xshash omillar paketlar kommutatsiyali uyali telefon tarmoqlarida ham aniqlangan. Bundan keyin o‘ziga o‘xshash jarayonlarning xususiyatlarini tasvirlab beruvchi ayrim holatlarni ko‘rib chiqamiz.

Faraz qilaylik, X =([X1, X2,…) – diskret argument (vaqt) $t \in N \cong \{1,2...\}$ning keng ma'nodagi barqaror tasodifiy jarayonning yarim cheksiz kesmasi.

X jarayonning o‘rtacha va dispersiyani mos holda $\mu<\infty$ va $\sigma^2<\infty$ orqali, X jarayonning avtokorrelyatsion funksiyasi esa quyidagicha,

$$r(k) \cong \frac{\overline{(X_{t+k} - \mu)(X_t - \mu)}}{\sigma^2}, \quad b(k) \cong \sigma^2 r(k), \quad k \in Z_+ \cong \{0,1,2...\}. \quad (1.9)$$

X jarayon keng ma'noda barqaror bo'lgani uchun o'rtacha μ, dispersiya $D\{x\}=\sigma^2=b(0)$, korrelyatsiya koeffitsienti r(k) va avtokorrelyatsiya b(k) t vaqtga bog'liq emas va r(k)=r(k), b(k)=b(-k).

Quyida keng ma'noda qat'iy o'ziga o'xshash jarayonning ta'rifini keltiramiz.

**Ta'rif**. Agar

$$r_m(k) = r(k), \; k \in Z_+, \; m \in \{2,3,...\}$$

bo'lsa, N=1-(β/2), 0<β<1 parametr bilan X jarayon keng ma'noda qat'iy o'ziga o'xshash (KMQO'O') deyiladi, ya'ni KMQO'O' jarayon o'zining korrelyatsiya koeffitsientini m uzunlik bloklari bo'yicha o'rtachalashtirilgandan so'ng o'zgartirmaydi.

Boshqacha aytganda, agar ulanish $X^{(m)}$ jarayon ikkinchi tartibli statistik tavsiflarga nisbatan kamida dastlabki X jarayondan farq qilmasa, u holda X – KMQO'O' bo'ladi.

**Ta'rif.** Agar

$$\lim_{m\to\infty} r_m(k) = g(k), \quad k \in N$$

bo'lsa, u holda N=1-(β/2), 0<β<1 parametri bilan X jarayon keng ma'noda asimptotik o'ziga o'xshash (KMAO'O') (second-order asymtotical self-similarity) deyiladi. Bu ta'rifning ma'nosi shundan iboratki, agar m uzunlikdagi bloklar bo'yicha o'rtachalashtirilgandan so'ng va m→∞ bo'lganida, u KMQO'O' jarayonga yaqinlashsa, u holda X jarayon KMAO'O' jarayon bo'lib hisoblanadi.

KMQO'O' tushunchasi bilan birga oddiy o'ziga o'xshash jarayon tushunchasi mavjud bo'lib, uni atamada ko'proq farqlash uchun tor ma'noda o'ziga o'xshash (TMShO') jarayon deb ataymiz.

**Ta’rif.** Agar

$$m^{1-H} X^{(m)} = X \ , \quad m \in N$$

ifoda o‘rinli bo‘lsa, H=1(β/2), 0<β<1 parametrli X jarayon tor ma’nodagi o‘ziga o‘xshash deyiladi.

## 1.6. Tarmoqlarda multimediali trafikka xizmat ko‘rsatish sifati parametrlari

Turli xil ko‘rinishdagi trafikni uzatishda har bir foydalanuvchiga telekommunikatsiya transport ulanishi taqdim etilishi kerak bo‘lib, u shu trafikka mos xizmat ko‘rsatish sifatini xalqaro tavsiyalar va standartlarga muvofiq ta’minlashi kerak.

Ulanish sifatining quyidagi asosiy parametrlari ajratiladi: ulanish o‘rnatilgan vaqti; ulanishni o‘rnatish ehtimolligi; ulanishning uzilish ehtimolligi; kechikish; yo‘qolish ehtimolligi; djitter.

*Ulanishni o‘rnatilish vaqti* $t^{(cn)}$ – abonent tomonidan tegishli multimediali xizmatni taqdim qilishga talabnoma bergan paytda, bu xizmatni taqdim etish boshlangan paytgacha bo‘lgan vaqt oralig‘i tarzida aniqlanadi.

*Ulanishni o‘rnatish ehtimolligi* $P^{(cn)}$ – tegishli xizmat taqdim etilgan talabnomalar sonining shu xizmatni taqdim etishga talabnomalarning umumiy soniga nisbatidir.

*Ulanishning uzilish ehtimoli* $P^{(rj)}$ – tegishli xizmat to‘liq taqdim qilinmagan talabnomalar sonining xizmat ko‘rsatilgan talabnomalarning umumiy soniga nisbati tarzida aniqlanadi.

*Kechikish* $\tau_i$ – *i*-bloki jo‘natuvchilariga tegishli xizmatning trafigi ma’lumotlarini *i*-blok jo‘natuvchilariga uzatishning boshlanishi bilan va foydalanuvchining shu blokni qabul qilib olishining tugashi vaqti orasidagi vaqt oralig‘i tarzida aniqlanadi. $\tau_I$ kechikish uzatilayotgan ma’lumotlar bloklarining

telekommunikatsiya tarmog‘i uzellari orasidagi aloqa kanallari bo‘yicha paketlashtirish, uzatish va tarqatish vaqtlari, shuningdek, bu bloklarni oraliq kommutatorlar va tarmoq marshrutizatorlari navbatlarida kutishlari vaqti yig‘indisidan tashkil topadi.

Asinxron telekommunikatsiya tarmog’ida ma’lumotlar bloklarining kechikishi har bir blok uchun har xil bo‘lishi mumkin va u tasodifiy kattalikni ifodalashi mumkin bo‘lib, u quyidagi tarzda ifodalanadi:

$$\tau_i = \tau_i^p + \sum_{k=1}^{M} \tau_{ik}^{pr} + \sum_{j=1}^{N} (\tau_{ij}^{sr} + \tau_{ij}^{wt}), \qquad (1.10)$$

bu yerda: $\tau_i^p$ - trafikning *i*-ma’lumotlar blokini paketlashning tasodifiy vaqt kattaligi, M – xizmatning ikki abonent o‘rtasidagi aloqa kanallarining umumiy soni; N – xizmatning ikki abonent orasida joylashgan kommutatsiyalash qurilmalari soni; $\tau_{ik}^{pr}$ - aloqa kanali bo‘yicha trafikning *i*-ma’lumotlar bloki tarqalish vaqtining tasodifiy kattaligi; $\tau_{ij}^{sr}$ - *j*-kommunikatsiya qurilmasida trafikning *i*-ma’lumotlar blokiga xizmat ko‘rsatish vaqtining tasodifiy kattaligi; $\tau_{ij}^{wt}$ - *j*-kommutatsiya qurilmasida trafikning *i*-ma’lumotlar blokining navbatda kutish vaqtining tasodifiy kattaligi.

*O‘rtacha kechikish* $\bar{\tau}$ uzatilayotgan ma’lumotlar bloklarining barcha kechikishlarining o‘rtacha qiymati sifatida aniqlanadi:

$$\bar{\tau} = \frac{1}{N^{(b)}} \sum_{i}^{N^{(b)}} \tau_i , \qquad (1.11)$$

bu yerda $N^{(b)}$ – yetkazib berilgan ma’lumotlar bloklarining umumiy soni.

*Yo‘qotishlar ehtimolligi* $P^{(rs)}$ - manzilga yetkazib berilmagan ma’lumotlar blokining, topshirilganlarning umumiy soniga nisbati bilan belgilanadi.

*Djitter* $\sigma^{(\tau)}$ – mos xizmat trafigining ma’lumotlar blokini uzatishni kechikishi $\tau^{(max)}$ va $\tau^{(min)}$ o‘rtasidagi farqi sifatida aniqlanadi:

$$\sigma^{(\tau)} = \tau^{(max)} - \tau^{(min)} , \qquad (1.12)$$

bu yerda

$$\tau^{(\min)} = \bar{\tau} - \sqrt{D\left[\bar{\tau}\right]}, \qquad \tau^{(\max)} = \bar{\tau} + \sqrt{D\left[\bar{\tau}\right]}, \tag{1.13}$$

dispersiya esa

$$D[\tau] = \frac{1}{N^{(b)}} \sum_{i=1}^{N^{(b)}} (\tau_i - \bar{\tau})^2 . \tag{1.14}$$

Transport ulanish parametrlarining abonentlarga taqdim etilayotgan xizmat sifatiga ta’siri 1.7-jadvalda keltirilgan.

1.7-jadval

Transport ulanish parametrlarining xizmatni taqdim etish sifatiga ta’siri

| Sifat parametrlari | Xizmat turi | | | |
|---|---|---|---|---|
| | Telefon | Videokonferensiya | Talabga ko‘ra video | Ma’lumotlar uzatish |
| Kechikish | Katta | Katta | O‘rtacha | Kam |
| Ulanishni o‘rnatish vaqti | Katta | Katta | O‘rtacha | O‘rtacha |
| Djitter | Katta | Katta | Katta | Kam |
| Yo‘qotish ehtimolligi | O‘rtacha | O‘rtacha | O‘rtacha | Katta |
| Ulanishni o‘rnatish ehtimolligi | Katta | Katta | Katta | Katta |
| Ulanishni uzilish ehtimolligi | Katta | Katta | Katta | Kam |

Eslatma. Katta, o‘rtacha, kam atamalari quyidagilarni aniqlaydi: katta – telekommunikatsiya ulanishining xizmatni taqdim etish sifatiga kuchli ta’siri. Bu parametrning katta qiymatiga yo‘l qo‘yilmaydi; O’rtacha – taqdim etilayotgan xizmat sifatiga telekommunikatsiya ulanishining paramertlarini o’rtacha ta’siri. Bu parametrning uncha katta bo‘lmagan qiymatiga yo‘l qo‘yiladi; Kam – taqdim

etilayotgan xizmat sifatiga telekommunikatsiya ulanishining paramertlarini kuchsiz ta’siri. Bu parametrning katta qiymatiga yo‘l qo‘yiladi.

Yetkazib berish vaqti va djitterning qiymatlari haqiqiy vaqt masshtabida amalga oshiriladigan xizmatlar uchun tarmoqning muhim tavsiflari hisoblanadi.

Telekommunikatsiya sohasida Yevropa tadqiqot markazining (RACE - Research on Advanced Communication in Europe) tadqiqotlari natijasida olingan multimediali xizmatlarning asosiy turlari uchun aniqlangan ulanishni o‘rnatish va ulanishni uzish ehtimolligi vaqti, ulanishni o‘rnatish ehtimolliklari, paketni yo‘qolish ehtimolligi, djitter, kechikishlarni yo‘l qo‘yilgan qiymatlari 1.8-jadvalda keltirilgan.

1.8-jadval

Multimediali trafikni uzatishda xizmat ko‘rsatish sifati parametrlarining ruhsat etiladigan qiymatlari

| Xizmat turi | Xizmat ko‘rsatish sifat parametrlari | | | | |
|---|---|---|---|---|---|
| | $t^{(cn)}$,c | $R^{(rj)}$ | $\tau$, ms | $R^{(rs)}$ | $\sigma_\tau$ , c |
| IP-telefoniya | 0.5...1 | $10^{-3}$ | 25...500 | $10^{-3}$ | 100...150 |
| Videokonferensiya | 0.5...1 | $10^{-3}$ | 30 | $10^{-3}$ | 30...100 |
| Talab bo‘yicha raqamli video | 0.5...1 | $10^{-3}$ | 30 | $10^{-3}$ | 30...100 |
| Oddiy ma’lumotlarni uzatish | 0.5...1 | $10^{-6}$ | 50...1000 | $10^{-6}$ | - |
| Televizion ko‘rsatuvlar | 0.5...1 | $10^{-8}$ | 1000 | $10^{-8}$ | - |

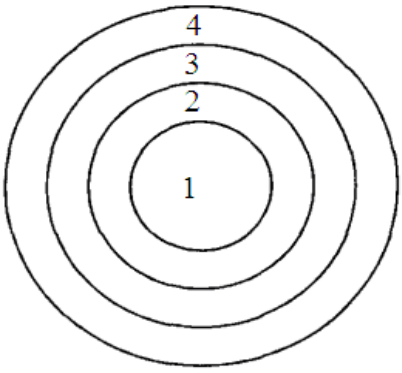
## Nazorat savollari

1. Zamonaviy tarmoqlarga qanday talablar qo‘yilgan?
2. Zamonaviy aloqa tarmoqlarida qanday xizmatlar yuzaga kelgan?
3. Multimedia deganda nimani tushunasiz?
4. Multimedia yo‘nalishini kelib chiqishi nimaga asoslangan?
5. Nima uchun multimediaga bo‘lgan talab oshib bormoqda?
6. Multimedia texnologiyalarining afzalliklari va xususiyatlari to‘g‘risida tushuncha bering.
7. Multimedianing qanday sinflarini bilasiz, tushuncha bering?
8. Multimediali ilovalarni uzatish tarmog‘iga qanday talablar qo‘yiladi?
9. Multimediali trafikning qanday turlari mavjud va ularni qisqacha tavsiflang?
10. Multimediali trafik qanday parametrlar bilan xarakterlanadi?
11. O‘ziga o‘xshash trafik tushunchasi nima?
12. Multimediali trafikni xizmat ko‘rsatish sifati qanday parametrlar bilan xarakterlanadi?

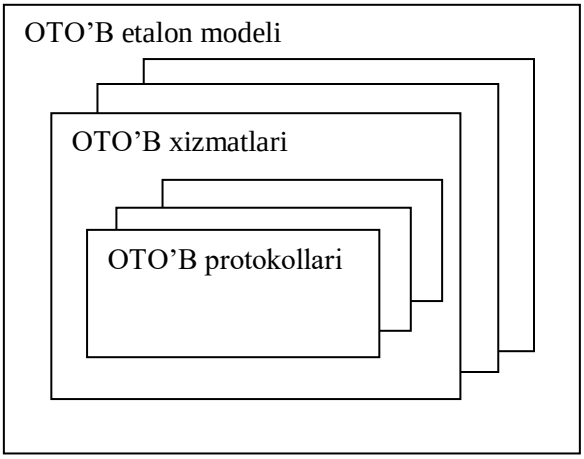
# 2. **MULTIMEDIALI ALOQA TARMOG‘IDA QO‘LLANILADIGAN TEXNOLOGIYALAR**

## 2.1. Ochiq tizimlarning o‘zaro bog‘lanish etalon modeli

Aloqa bu tarmoq va aloqa xizmati yig‘indisini o‘zida namoyish etadi (2.1-rasm). Telekommunikatsiya xizmati – bu xizmatlardan foydalanuvchilarni ta’minlovchi vositalar majmuasidir. Ikkilamchi tarmoqlar telekommunikatsiya xizmatlarida signallarni kommutatsiyalash, transportlashni ta’minlaydi. Birlamchi tarmoqlar ikkilamchi tarmoqlarni ta’minlaydi. Mos keluvchi xizmatni tarkibiy qismi foydalanuvchilarda joylashgan oxirgi qurilma hisoblanadi.




2.1-rasm. Aloqa arxitekturasi:
1-telekommunikatsiyaning birlamchi tarmog‘i;
2-telekommunikatsiyaning ikkilamchi tarmoqlari;
3-telekommunikatsiya vazifalari;
4- telekommunikatsiya xizmatlari.




2.2-rasm. OTO‘B uchun standartlar ishlab chiqish strukturasi

Xizmat namunasi sifatida telefon aloqasini keltirish mumkin. U telefon aloqa, ma’lumotlar uzatish va boshqa xizmatlarni taqdim qiladi. Telefon tarmog‘i bo‘yicha ma’lumotlar uzatish (telefon xizmatini qo‘llab) telefon kanallari bo‘ylab ma’lumotlar uzatish xizmati sifatida ko‘riladi. Telefondan foydalanuvchi o‘zining kompyuterini modem yordamida telefon tarmog‘iga ulashi mumkin. Ma’lumotlar uzatish xizmati sifatida biz ma’lumotlar uzatish uchun mahsus yaratilgan aloqa tizimini tushunamiz, ya’ni qurilma va dasturiy vositalar majmui, qayta ishlash usullari, taqsimlash va ma’lumotlar uzatish. Shu vaqtning o‘zida ma’lumotlar uzatish xizmati telefon aloqa xizmatini ham taqdim etishi mumkin.

Telekommunikatsiyaning barcha xizmatlarida axborot almashish avvaldan belgilangan aniq qoidalar bo‘yicha amalga oshishi kerak. Bu qoidalar (standartlar) elektr aloqaning bir nechta xalqaro tashkilotlari tomonidan ishlab chiqiladi. 1978 yilda standartlashtirish bo‘yicha xalqaro tashkilotda SC16 komiteti tashkil etildi. Uning vazifasi - ochiq tizimlarning o‘zaro bog‘lanishi uchun xalqaro tavsiyalar ishlab chiqarishdir.

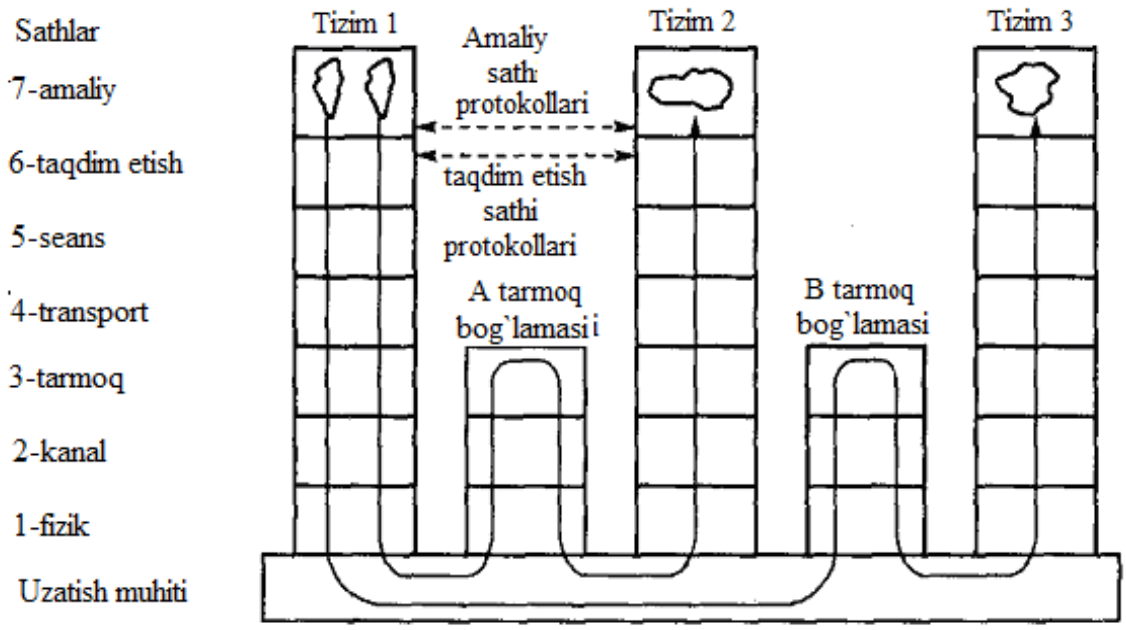
Ochiq tizim deb – ochiq tizimlar talablarini qondiruvchi, turli tizimlar bilan o‘zaro ta’sirlashishi mumkin bo‘lgan tizim tushuniladi. Agar tizim ochiq tizimlarning o‘zaro bog‘lanish (OTO‘B) etalon modeliga mos kelsa, u ochiq tizim hisoblanadi.

OTO‘B etalon modeli – standartlar tuzilishining umumiy strukturasi. U alohida standartlar orasidagi o‘zaro bog‘lanish prinsipini aniqlaydi va OTO‘B uchun talab etiladigan ko‘pgina standartlarni bir vaqtda ishlab chiqish imkonini ta’minlash uchun asos hisoblanadi. Biroq OTO‘B standarti faqatgina etalon modelni aniqlabgina qolmay, balki etalon modelni qondiruvchi aniq xizmatlar to‘plamini, shuningdek xizmatlarni ta’minlovchi protokollar to‘plamini aniqlashi zarur. Bunda protokol deb, bir-biri bilan ishlovchi sathlarni o‘zaro ta’sirlashish qoidalarini va jarayonlarini aniqlaydigan xujjat tushuniladi.

1983 yilda etalon model sifatida yetti sathli model tasdiqlangan (2.3-rasm). Bunda ochiq tizimlarga taalluqli barcha jarayonlar o‘zaro bog‘langan sathlarga

bo‘linadi. Yetti sathli modelda (1-3) quyi sath protokollari axborot uzatishga, yuqori sath (5-7) protokollari axborotlarni qayta ishlashga mo‘ljallangan. Transport sath protokollari ba’zida alohida ajratiladi, u axborot uzatish bilan bevosita bog‘liq emas. Biroq bu sath o‘zining vazifalari bo‘yicha quyi sathlarga yaqin bo‘lgani uchun quyi sathga tegishlidir.

Barcha yettita sathning vazifasi amaliy jarayonlarni ishonchli o‘zaro ta’sirini ta’minlashdir. Bunda amaliy jarayonlar sifatida foydalanuvchilarning ehtiyoji uchun axborotlarni berish, kiritish, saqlash va qayta ishlash jarayonlari tushuniladi. Har bir sath o‘zining vazifasini bajaradi. Biroq sathlarning xavfsizligi uchun ular bir-birining ishini tekshiradi.




2.3-rasm. OTO‘B etalon modelining tuzilishi

Amaliy sath *(application)* – tarmoqda uzatiladigan axborot manbalari va foydalanuvchilari hisoblanuvchi amaliy jarayonlar va tarmoq terminallarini boshqaradi. Bu sathning vazifasi foydalanuvchining dasturini ishga tushirish, ularni bajarishni, ma’lumotlarni kiritish-chiqarishni, terminallarni boshqarish va tarmoqni

ma’muriy boshqarishdir. Bu sathda foydalanuvchilarga turli xizmatlarni taqdim etish ta’minlanadi. Bu sathda ma’lumotlar uzatish infratuzilmasini sozlash hisoblanuvchi texnologiyalar ishlaydi: elektron pochta, tele va videokonferensiya, resurslarga ulanish, internetda ishlash va b.q.

Taqdim etish sathi *(presentation)* – tarmoqda uzatiladigan ma’lumotlarni amaliy jarayonlar uchun qulay bo‘lgan ko‘rinishga o‘zgartirish va izohlash. Ma’lumotlarni moslashtirilgan formatda va tuzilishda taqdim etish, turli tillardan izohlash dasturi, translyatsiyalash, ma’lumotlarni shifrlashni ta’minlaydi.

Seans sathi *(session)* – amaliy jarayonlar orasidagi aloqa seanslarini o‘tkazish va tashkil qilish (tarmoq abonentlari orasidagi seanslarni ta’minlash, ma’lumotlar uzatish rejimini va navbatini boshqarish: simpleks, yarimdupleks, dupleks). Bu sathning ko‘pgina funksiyalari, ulanishni o‘rnatish va amaliyotda ma’lumotlar almashish tartibini ta’minlash transport sathda amalga oshiriladi, shuning uchun seansli sath protokollarini qo‘llash chegaralanishga ega.

Transport sathi *(transport)* – ma’lumotlarni segmentlashtirishni boshqarish (segment – transport sathni ma’lumotlar bloki) va manbadan foydalanuvchiga (abonentlar orasidagi logik kanalni o‘rnatish va axborotni boshqarishni almashtirish, ma’lumotlar uzatish sifatini ta’minlash) ma’lumotlarni ikki tomonlama uzatish. Bu sathda tarmoq sathga taqdim etiladigan xizmatlar qo‘llanilishi optimallashtiriladi, ya’ni kam xarajatlarda maksimal o‘tkazish qobiliyati ta’minlanadi. Transport sath protokollari juda keng rivojlangan va amaliyotda jadal qo‘llaniladi. Bu sathda uzatilayotgan axborotning ishonchliligini nazoratiga katta ahamiyat berilgan.

Tarmoq sathi *(network)* – tarmoqda ma’lumotlar uzatishni logik kanalini boshqarish (ma’lumotlarni marshrutlash va adreslash, kommutatsiyalash: kanallar, xabarlar, paketlar va multipleksorlash). Bu sathda tarmoqning bosh telekommunikatsiya vazifasi – foydalanuvchilarning aloqasini ta’minlash amalga oshiriladi. Tarmoqning har bir foydalanuvchisi albatta bu sathning protokollarini qo‘llaydi va tarmoq sathi protokollari qo‘llaniladigan o‘zining yagona tarmoq

adresiga ega. Bu sathda ma’lumotlarni strukturalash bajariladi – ma’lumotlarni paketlarga joylashtirish va paketlarga tarmoq adreslarini berish (paket–tarmoq sathini ma’lumotlar bloki).

Kanal sathi *(data-link)* – tarmoq sathi ob’ektlari orasida ma’lumotlar uzatishni fizik kanalini boshqarish va shakllantirish, fizik ulanishlarni shaffofligini ta’minlash, uzatishdagi xatoliklarni to‘g‘rilash va nazorat qilish. Bu sathning protokollari ko‘p sonli va o‘zining funksional imkoniyatlari bilan bir-biridan farqlanadi. Bu sathda ko‘p kanalga ulanish protokollari mavjud. Boshqarish kadrlar sathida bajariladi (kadr–kanal sathidagi ma’lumotlar bloki).

Fizik sath *(physical)* – tarmoqni fizik kanal bilan ulanishini uzish va ushlab turish, o‘rnatish. Boshqarish raqamli bitlar sathida (impulslar, uning amplitudasi, formasi) va analog (uzluksiz signalni fazasi, amplitudasi va chastotasi) sathda bajariladi. Sathlar orasida uzatiladigan axborot bloklari standart formatga ega: sarlavha, xizmat axboroti, ma’lumotlar va oxir. Har bir sath axborot blokini quyida turuvchi sathga uzatishda, uni o‘zining sarlavhasi bilan ta’minlaydi. Yuqori turuvchi sathni sarlavhasi quyi turuvchi uzatiluvchi ma’lumotlar singari qabul qilinadi.

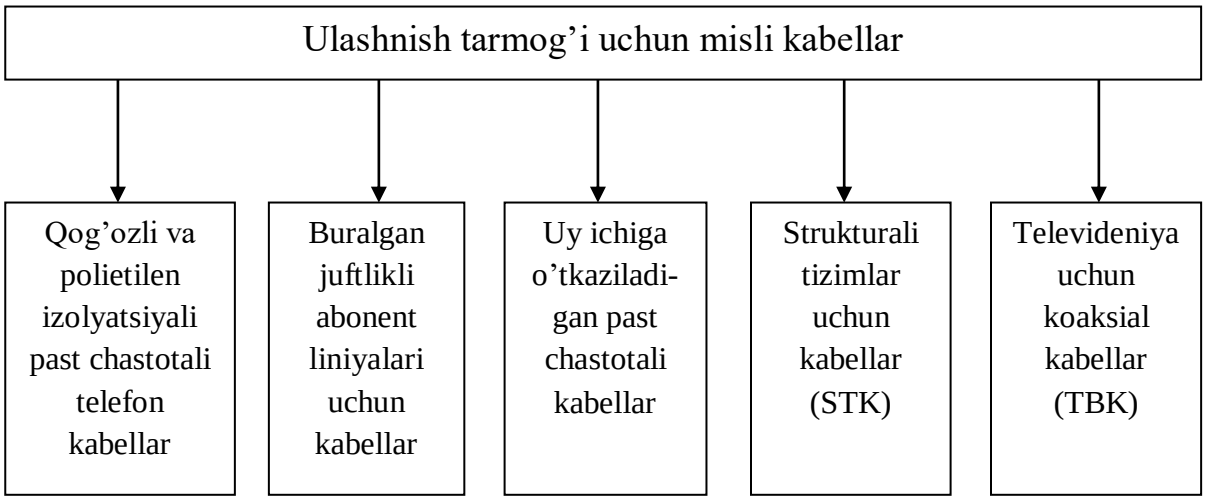
## 2.1. Fizik sath. Uzatish muhiti

Axborotni uzatish muhiti sifatida mis kabellar, tolali optik kabellar va atrof fazo (simsiz aloqa) bo‘lishi mumkin. Magistral aloqa uchastkalarida asosan optik kabellar keng qo‘llaniladi. Keng polosali ulanish tarmog‘ida asosan mis kabellar qo‘llaniladi. Shuning uchun asosan ulanish tarmoqlarida qo‘llaniladigan misli kabellar turini ko‘rib chiqamiz.

### 2.1.1. Misli kabellar

Ulanish tarmoqlarida qo‘llaniladigan misli kabellarning turlarini klassifikatsiyasi 2.4-rasmda keltirilgan.

Bu kabellarni tok o‘tkazuvchi simlari 0.32; 0.4; 0.5 va 0.7 mm diametrli misli simdan tayyorlangan va polietilen bilan izolyatsiyalangan. Izolyatsiyalangan simlar juft yoki to‘rtta ko‘rinishda o‘ralgan. Kabellarni ishonchliligini oshirish uchun va qobiqqa namlikni kirmasligi uchun gidrofrob to‘ldirgich bilan germetiklangan kabellar ishlab chiqilgan.




2.4-rasm. Misli kabellarning turlari

TPEPZ – telefon, polietilen izolyatsiyali, alyumin folgali ekranli, gidrofrob to‘ldirgichli, polietilen qobiqli;

TPPZPB - TPEPZga aynan o‘xshash, lekin bronlashgan lenta qatlamli va polietilen shlangali.

Ko‘rsatilgan past chastotali kabellar ko‘pgina tarmoqlarda qo‘llaniladi. Tarmoq rivoji uchun bu kabellarni imkoniyatlarini bilish zarur. Avvalo chastotalardagi uzatish

xarakteristikalarini 2 dan yoki 10 MHz gacha. Ko‘rsatilgan diapazonlarda, terminallardan abonentgacha yuqori tezlikli trafikni uzatish imkoni baholanadi.

Bunda aniqlanadigan xarakteristikalar quyidagilar hisoblanadi:

- turli haroratda misli juftlikni so‘nishi kilometrda (α [dB/km]);
- yaqin va uzoq oxirlardagi misli juftliklar orasidagi o‘tuvchi so‘nish (A) [dB]; $A_1$[dB];
- o‘tuvchi va tashqi halaqitlar kattaligi;
- to‘lqinli qarshilik ($IZ_bI$ Om);
- shleyfning qarshiligi $R_0$ [Om/km].

2.1-jadval

TPVAD turidagi kabel

| Kabel markasi | Qo‘llanilish muhiti |
|---|---|
| TPVAD 1x2x0.5<br>2x2x0.5<br>3x2x0.5<br>4x2x0.5 | Bino ichida 200 kHz chastotagacha signallarni uzatish uchun silindr o‘zakli kabellar |
| TPVAD 2(1x2x0.5)<br>2(2x2x0.5)<br>2(4x2x0.5) | Bino ichida 2048 kHz chastotagacha signallarni uzatish uchun ikkita parallel ekranlashtirilgan guruhli kabellar |

Past chastotali kabellarni qo‘llash muhiti–abonent ulanuvchi tarmoqdir:

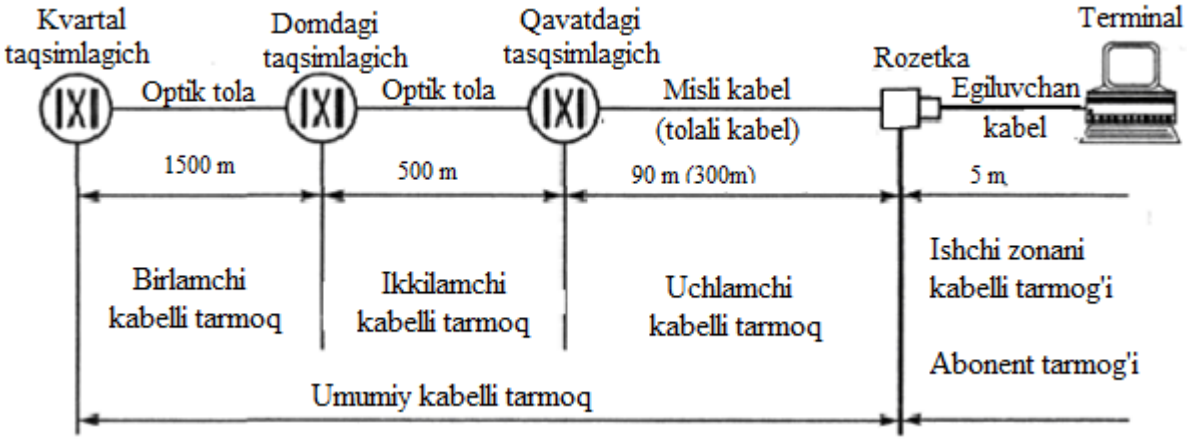
- 200 kHz gacha ekranlashtirilgan va ekranlashtirilmagan;
- 2048 kHz gacha faqat ekranlashtirilgan.

Bu kabellarning konstruksiyasi 0.1, 100, 200 kHz chastotalarda, qurilish uzunligida yaqindagi oxirda zanjirlar orasidagi o‘tuvchi so‘nishni ta’minlaydi, mos holda 90, 80, 70 dB.

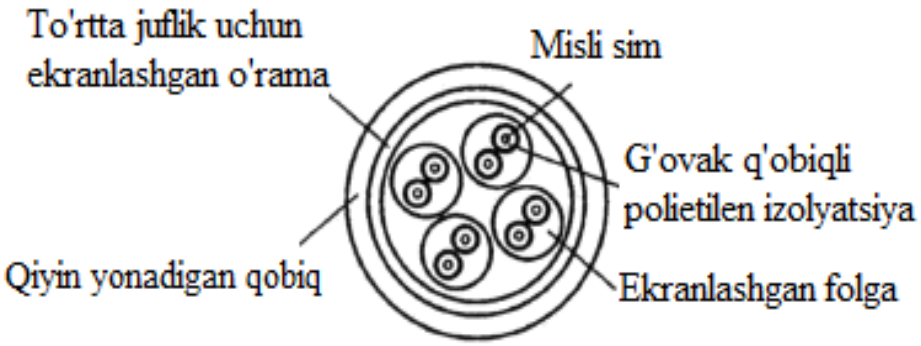
Strukturalashgan kabelli tizimlar (SKT) (Structured Cabling System, SCS) – lokal tarmoqlar uchun universal kabel yotqazishni tashkil etadi. SKT markaziy elementi misli va bimetall juftlikli kabeldir. Kabelni shakllantirishda misli juftliklar o‘zaro qo‘shimcha tarzda o‘raladi va hosil bo‘lgan o‘ram ekranlashgan yoki ekranlashmagan izolyatsiyali qobiqqa joylashtiriladi.

Quyida SKT kabelning xarakteristika va tuzilishi keltirilgan:

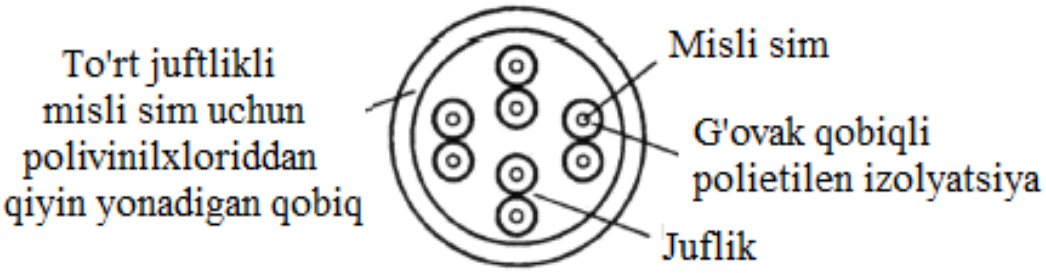
- UTP (Unshielded Twisted Pair) – ekranlashtirilmagan juftlik;
- STP (Shielded Twisted Pair) – ekranlashgan juftik.




2.5-rasm. EN 50173 standarti bo‘yicha kabelli tarmoqni umumiy tuzilishi




2.6-rasm. Ekranlashtirilgan kabelning tuzilishi S-STP 600/900/1000/1200




2.7- rasm. UTP 300 ekranlashtirilmagan kabelning tuzilishi

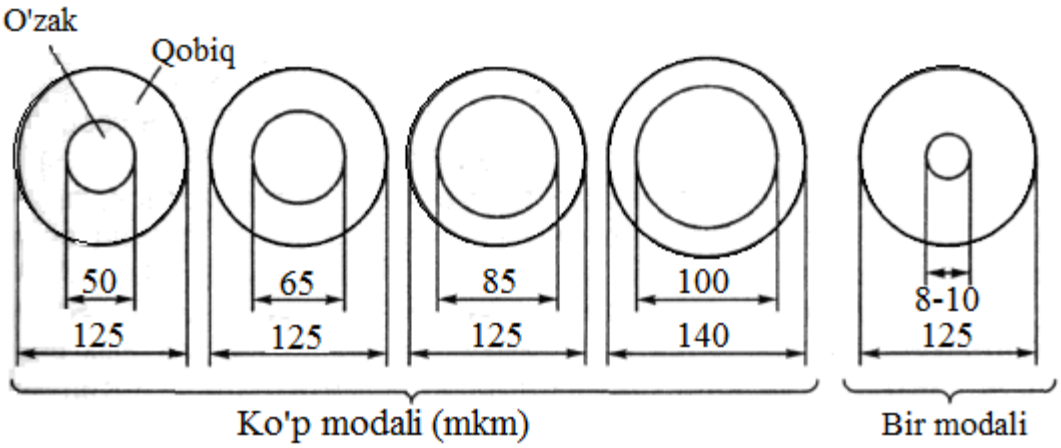
### 2.1.2. Tolali optik kabellar

Multiservisli tarmoq haqidagi zamonaviy tushuncha abonent terminaligacha yoki oraliq tugallanishgacha (gibrid usul tola-mis) qo‘llaniluvchi tolali-optik kabellar bilan uzluksiz bog‘liq.

Optik tolalarda yorug‘lik nurini aks qaytish effekti qo‘llaniladi. Tola silindr yoki to‘g‘ri burchakli ko‘rinishda ishlab chiqariladi. To‘g‘ri burchakli tolalar mikrosxemalarda, silindr ko‘rinishidagi tolalar kabellar asosida qo‘llaniladi (2.8-rasm.).

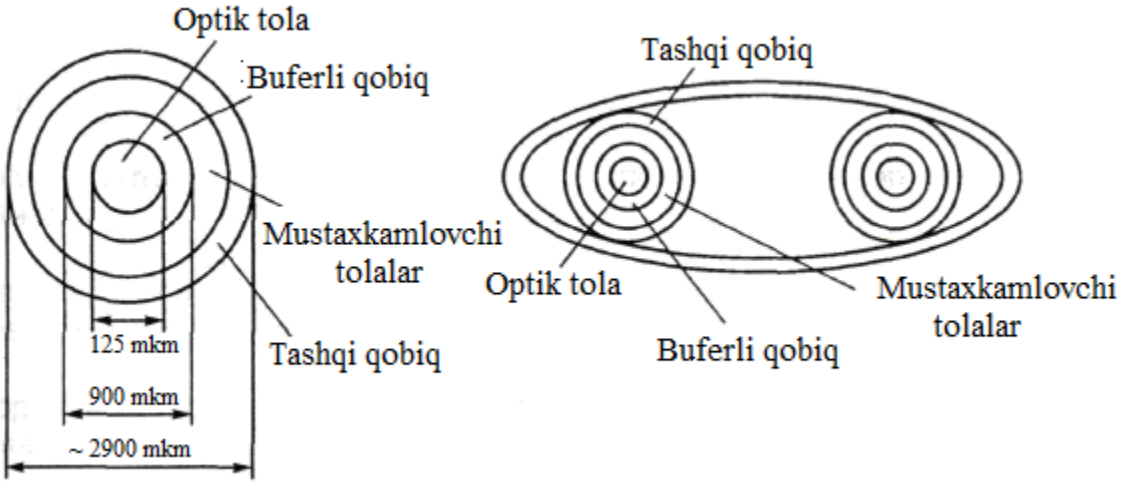
Ulanish tarmoqlarida qo‘llaniladigan kabellar quyidagi talablarga javob berishi kerak:

- narxining nisbatan pastligi;
- talab etilgan o‘tkazish oralig‘i;
- ulanish uchastkalarida so‘nishning kichikligi;
- nurlanish manbalari va qabul qilgichlar bilan oddiy ulanish;
- turli haroratlarda ishlashi;
- namlikka, bosimga va tebranishlarga chidamlilik.



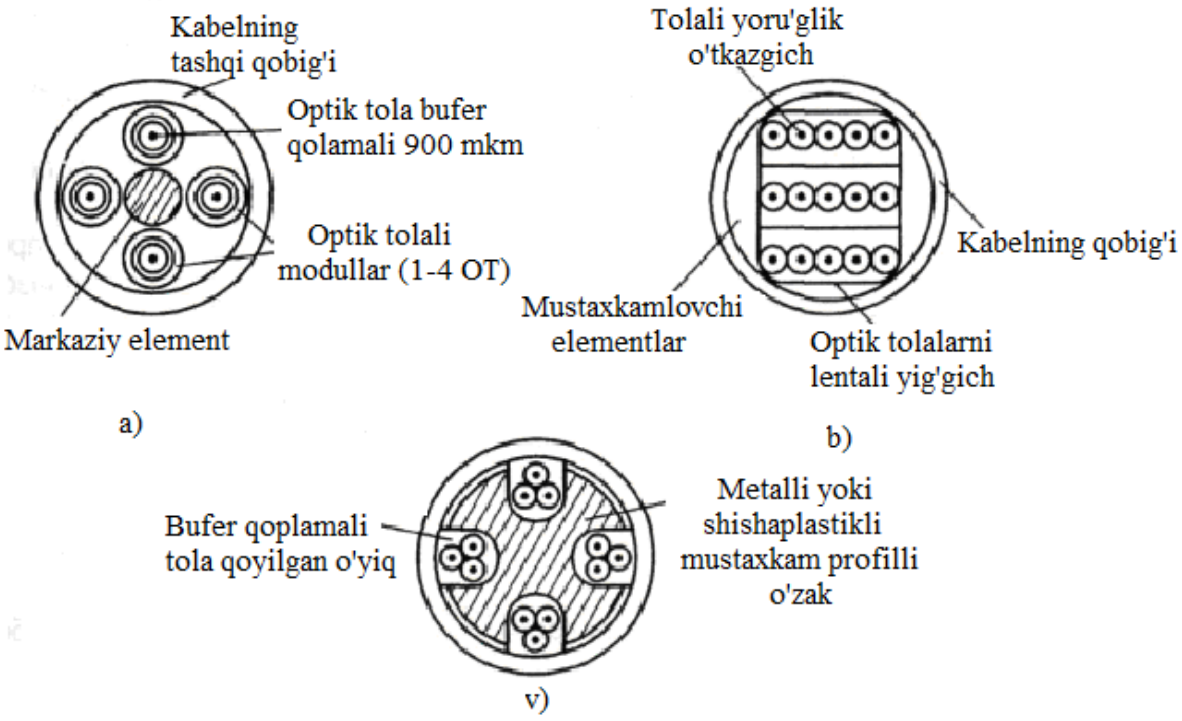

2.8-rasm. Optik tolalarning tuzilish namunasi

Optik kabellar ulanish tarmoqlarida qo‘llanilishiga qarab ob’ekt, taqsimlagich va magistral turlarga ajraladi. Ob’ektlarda qo‘llaniladigan optik kabellar (abonent liniyasi) 1-2 tolali ko‘rinishda tayyorlanadi (2.9-rasm).




2.9-rasm. Ob’ektda qo‘llaniladigan kabellarning tuzilish namunasi

Magistral va taqsimlagich liniyalar uchun modulli, lentali va profillashtirilgan tuzilishli kabellar qo‘llanilishi mumkin. Tolani erkin yotqazish mexanik va termik ta’sirlarni kompensatsiyalash imkonini beradi. Bu tolalarning tuzilishi 2.10-rasmda keltirilgan.



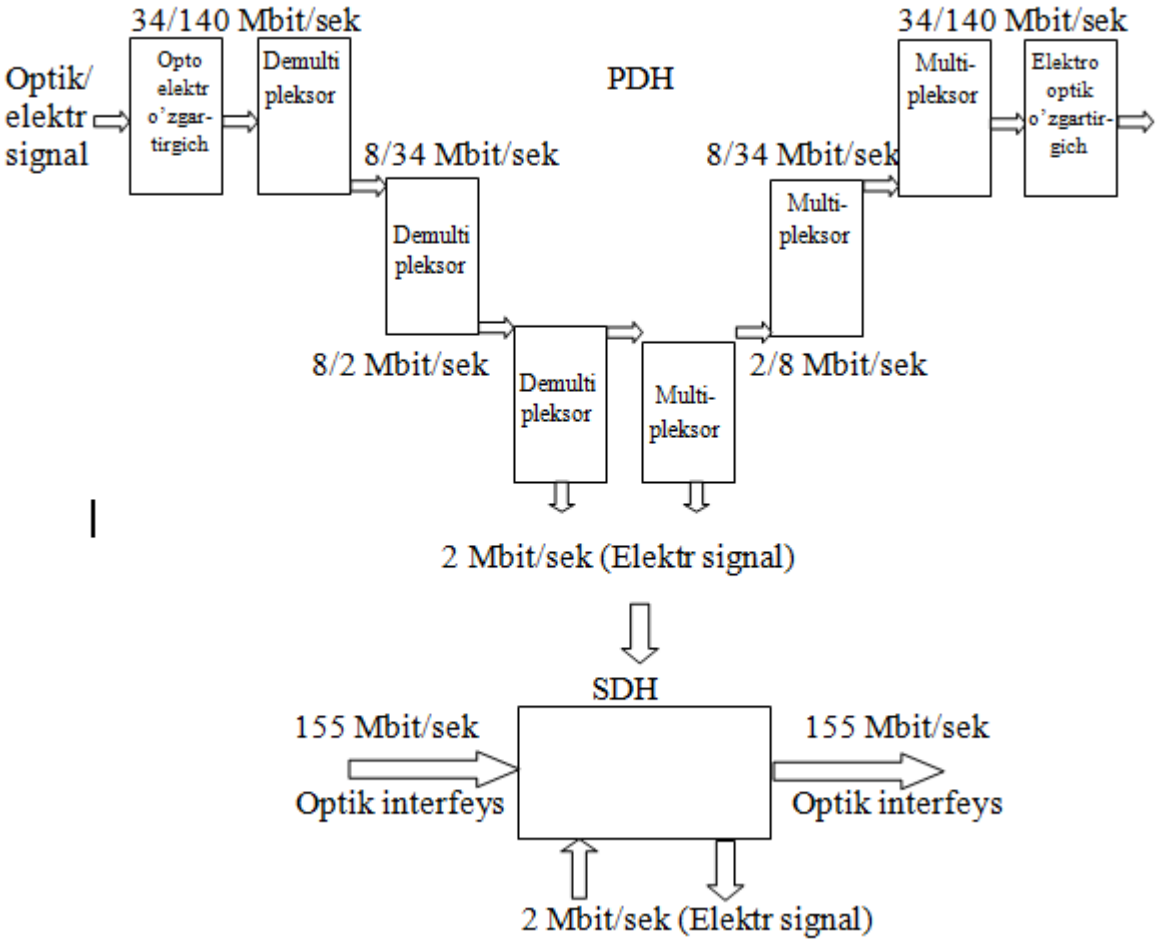

2.10-rasm. Optik kabellarning tuzilishi:

a) tolali taqsimlovchi optik kabel; b) 20 ta tolali taqsimlovchi optik kabel;

v) profil o‘zakli 12 ta tolali optik kabel

## 2.2. Sinxron raqamli ierarxiya

Hozirgi kunda telekommunikatsiya tarmoqlarida pleziaxron raqamli ierarxiya (PDH) va sinxron raqamli ierarxiyaning (Synchronous Digital Hierarchy, SDH) multipleksorlash qurilmalari qo‘llanilmoqda. Birinchi bo‘lib mahalliy birlamchi tarmoqning raqamli uzatish tizimlari (RUT) yaratildi: IKM-30 va uning turlari. So‘ngra shahar va hududiy tarmoqlarda qo‘llaniladigan PDH-RUT IKM-120, IKM-480, shuningdek tolali optik uzatish tizimlari ishlab chiqildi va qo‘llanildi. PDHda multipleksorlashni kamchiliklaridan biri raqamli oqimlarni ajratishni murakkabligi hisoblanadi. 140 Mbit/s raqamli oqimdan 2 Mbit/s tezlikli oqimni ajratib olish uchun u to‘liq demultipleksorlanishi kerak (2.11-rasm). SDH tizimlarida bu masalani bajarish oddiy.




2.11-rasm. PDH va SDH tizimlarida raqamli oqimlarni ajratish / birlashtirish jarayonlarini qiyoslash

Bu yerda 2 Mbit/s tezlikli oqimni kiritish va chiqarish kirish/chiqishli multipleksor (add/drop multiplexer, ADM) yordamida amalga oshiriladi.

ITU-T tavsiyasiga asosan SDH uzatish tizimining tezligi 155.52 Mbit/s. SDH RUT telekommunikatsiya tarmog‘i bo‘ylab signallarni transportlash uchun mo‘ljallangan, standartlashtirilgan axborot tuzilishining yig‘indisini tashkil etadi. Ulardan asosiysi N-tartibli STM-N sinxron transport modul hisoblanadi (2.2-jadval).

2.2-jadval

STM-N ning raqamli hajmi

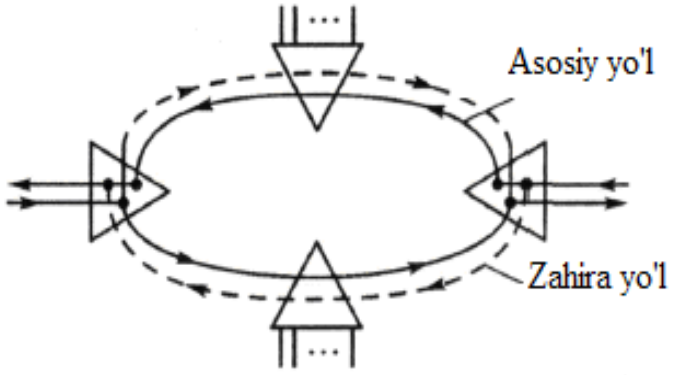
| SDH sathlari | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| STM turi | STM-1 | STM-4 | STM-16 | STM-64 | STM-256 |
| B, Gbit/s | 0.155 | 0.622 | 2.5 | 10 | 40 |
| $N_{E1}$ | 63 | 252 | 1008 | 4032 | 16128 |
| $N_{ARK}$ | 1 890 | 7 500 | 30 000 | 120 000 | 480 000 |

Izoh: B-uzatish tezligi; E1($N_{E1}$)-birlamchi raqamli oqimlar soni; $N_{ARK}$- asosiy raqamli kanallar soni.

SDH RUTning asosiy afzalligi ishonchli, boshqariluvchi transport tarmoq hisoblanadi, ular quyidagilar hisobiga bajariladi:

- har bir segmentni nazorat qiluvchi segmentlashtirilgan aloqa liniyasi;
- qurilmalarni, qurilma bog‘lamalarini, liniyani zahiralash va liniyani avtomatik zahira liniyaga o‘tkazish;
- TMN boshqarish tarmog‘i yordamida transport tarmoqni qayta tuzish imkoni.

SDHda tashkil qilinadigan liniyani zahiralashning keng tarqalgan usullaridan biri bu tarmoqni halqali topologiyasini qo‘llash hisoblanadi (2.12-rasm).




2.12-rasm. Bir yo‘nalishli halqa

Halqa tuzilishida axborot asosiy va zahira yo‘nalishi orqali uzatiladi. Halqaning qaysidir uchastkasida avariya bo‘lsa, o‘sha uchastkadan aylanib o‘tish zahira yo‘l orqali avtomatik tarzda amalga oshiriladi. SDH – bu zamonaviy axborot tarmog‘ining tuzilish qurilmasi – yashovchan, yuqori sifatli transport aloqa tarmog‘idir.

SDH quyidagilarga imkon beradi:

- ko‘p sifatli raqamli kanallarni tashkil qiladi;
- regeneratorlarsiz liniya traktini qurish;
- kross-konnektorlar va kirish-chiqish multipleksorlarni qo‘llash hisobiga oson tuzilishli va tarmoqlangan raqamli tarmoqni yaratish;
- operativ nazorat va ulanish qurilmasi hisobiga foydalanuvchilarga ishonchli kanallar va traktlarni taqdim etadi, shuningdek ishonchli tarmoq tuzilishi;
- tarmoqni operativ boshqarishni amalga oshiradi;
- ATM texnologiyasini qo‘llab yuqori ishlab chiqaruvchi raqamli tarmoq qurish.

## 2.4. To‘lqinli zichlashtirish texnologiyasi

Hozirgi vaqtda O‘zbekiston Respublikasi tarmoqlarida G.652 tavsiyasiga mos keladigan optik tolalar va optik kuchaytirgichlarsiz regeneratsiyalash uchastkasi uzunligi 100...200 km gacha bo‘lgan STM-16 (2,5 Gbit/s) sathidagi sinxron multipleksorlar qo‘llaniladi. Optik tolaning o‘tkazish qobiliyatini nazariy chegarasi uchinchi shaffoflik darchasida, ya’ni 193 GHz chastota tartibida taxminan $3\text{-}10^9$ ARKni tashkil etadi. STM-16 uchun ARK soni $3\text{-}10^5$ teng.

Internet tarmoqlariga ulanuvchi kanallar hajmining oshishi o‘z navbatida foydalanuvchilarga multimedialardan foydalanish imkonini beradi. Bu esa tarmoqqa ulanuvchi operatorlarning sonini oshirishga majbur qiladi, natijada kanallar soni singari ularning uzatish tezliklari ham oshadi. Lekin ma’lumotlarni uzatish hajmining oshishi va mavjud bo‘lgan optik tolalar orqali o‘tkazuvchanlik qobiliyatining tez to‘lishi yana muammolarni yuzaga keltirdi.

Aloqa sohasida axborotlarni uzatish tezligini oshirish nuqtai nazaridan talablarning oshishi, shuningdek yangi regionlarni qamrab olish yangi optik tolali texnologiyalarni, ayniqsa WDM (WDM -Wavelength Division Multiplexing) to‘lqin uzunligi bo‘yicha ajratishga ega bo‘lgan multipleksorlash deb ataluvchi texnologiyani yaratilishiga olib keldi. Bitta optik tolada uzatilayotgan to‘lqin uzunliklari soniga bog‘liq holda CWDM, DWDM va HDWDM texnologiyalari mavjud:

- 200 GHz dan kam bo‘lmagan kanallarni chastotaviy ko‘chiruvchi CWDM (Coarse WDM) tizimlari, ular 16 tadan ko‘p bo‘lmagan kanallarni multipleksorlash imkonini beradi;

- 100 GHz dan kam bo‘lmagan kanallarni chastotaviy ko‘chiruvchi DWDM (Dense WDM) tizimlari, ular 64 tadan ko‘p bo‘lmagan kanallarni multipleksorlash imkonini beradi;

- 50 GHz dan kam bo‘lmagan kanallarni chastotaviy ko‘chiruvchi HDWDM tizimlari, ular 64 tadan ko‘p bo‘lgan kanallarni multipleksorlash imkonini beradi.

WDM texnologiyasining afzalligi:

- kanallarning o‘tkazuvchanlik qobiliyatini yuqoriligi;
- ma’lumotlarni uzatish tezligining yuqoriligi;
- bitta optik tola orqali trafiklarni ikki tomonlama uzatish imkonining mavjudligi;
- tor oraliqli yarim o‘tkazgichli lezerlardan foydalanish imkoniga egaligi (spektr nurlanish kengligi 0.1 nm);
- keng polosali kuchaytirgichlardan va yaqin kanallarni ajratishda optik filtrlardan foydalanish imkoniyati;
- qo‘llaniladigan multipleksor va demultipleksorlarning narxini arzonligi.

## 2.5. IP – tarmoq texnologiyasi

Ethernet - kommutatorlarni ishlab chiqarishni jadal ravishda o‘sishi, 100 Mbit/s, 1 va 10 Gbit/s portlarning hosil bo‘lishi, abonent ulanish tarmog’ining o‘tkazish qobiliyatini sezilarli darajada oshirdi va keng polosali ulanish xizmatlarini ta’minlash imkonini berdi. Birinchi navbatda bu 50 Mbit/s gacha tezlikli trafik bitta foydalanuvchni axborotli oqimga generatsiyalanadigan audio va video oqimlarga taalluqli. IP tarmoq barcha axborotli oqimlarga xizmat ko‘rsatish imkoniga ega. IP tarmoq orqali VoIP tovush signalini va barcha raqamli formatdagi video tasvirlarni uzatishi mumkin.

Bugungi kunda multiservisli tarmoq deganda faqatgina kanal sathidagi turli xizmatlarni (FR, IP, ISDN, ATM, SDH xizmatlari) yoki tarmoq marshrutlashlarnigina (VLAN yoki VPN) emas, balki axborotli xizmatlarni (ISP, ASP va SSP) ham taqdim etish imkoni tushuniladi.

Operatorlik xizmati – bu, foydalanuvchi xizmatlari bilan shartnomali kelishuv va sifat kafolati. Shuning uchun umumiy foydalanish multiservisli tarmoqning operatori uchun xizmatlarni amalga oshirish mezoni, ularning sifati va kafolati hisoblanadi. Ya’ni parametrlarni sozlash va sifatni nazorat qilishning samarali mexanizmlarining mavjudligi, abonent foydalanadigan barcha xizmatlar paketini kafolatli taqdim etishning mavjudligi.

IP-texnologiyasini keng tarqalishi uning bir qator xususiyatlari bilan aniqlanadi.

**Universallik.** Hozirgi kunda IP protokollari barcha tarmoq segmentlarida qo‘llanilmoqda, lokal tarmoqlardan magistral tarmoqlargacha. IP texnologiyasi ovoz va video axborotlarni, ma’lumotlarni uzatish uchun qo‘llaniladi. IP asosida qayd etilgan va simsiz aloqa tarmoqlari quriladi.

**Masshtablashtirish.** Yirik masshtabli tarmoqlar oson rivojlanish imkoniga ega bo‘lishi kerak.

**Ochiqlik.** Internet tarmog‘i ochiq tizim prinsipiga asoslangan.

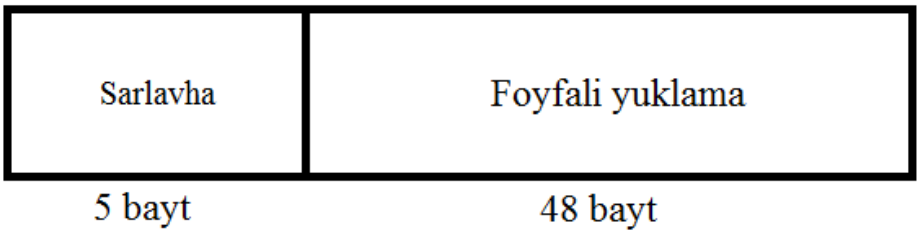
## 2.6. ATM texnologiyasi

ATM texnologiyasi ma’lumotlar uzatishni turli texnologiyalari qo‘llanilgan tuzilishli tarmoqlarni birlashtirish masalasini yetarli darajada samarali yechish imkoniga ega. Telekommunikatsiyaning barcha operatorlari bu texnologiyani qo‘llaydi va multiservisli tarmoqni yaratishda asosiy raqobat ATM va MPLS texnologiyalari orasidadir.

ATM texnologiyasida qayd etilgan o‘lchamdagi (53 bayt) paketlar qo‘llaniladi. Xatoliklarni aniqlash va to‘g‘rilash faqat sarlavhada amalga oshiriladi. Axborotli yacheyka ichidagi uchun xech qanday tekshirish va qayta tiklash bajarilmaydi va ulanishga mo‘ljallangan axborot uzatish qo‘llaniladi. ATMni amalga oshirish odatda qurilmali ta’minot yordamida amalga oshiriladi. Buning hammasi multipleksorlash bilan birgalikda kechikish vaqtini kamaytiradi, bu esa real vaqtdagi trafikni uzatishda zarurdir.

ATM texnologiyasi, trafikni boshqarish usullarini va xizmat ko‘rsatish sifati mexanizmlarini taqdim etadi. Bu shuni bildiradiki, ATM tarmoqlarida o‘tkazish qobiliyatini talab etilgan qiymatini kafolatlaydigan resurslarni, uzatishni kechikishi va yacheykalar yo‘qolish sathini zahiralashi mumkin.

Yacheykaning standart tuzilishi 2.13-rasmda keltirilgan. ITU standartiga binoan ATM yacheykasining uzunligi 53 baytni tashkil etadi. Yacheykaning sarlavhasi va foydali yuklama maydoni mos holda 5 va 48 baytdan iborat. Bundan tashqari foydali yuklama maydonida birdan ikki baytgacha uzunlikdagi katta bo‘lmagan sarlavha bo‘lishi mumkin. Foydali yuklama blokidagi foydalanuvchining ma’lumoti segmentatsiya deyiladi. Foydali yuklama blokiga sarlavhani qo‘shilishi inkapsulyatsiya jarayoni sifatida aniqlangan.




2.13-rasm. ATM yacheykasining tuzilishi

## 2.7. Ethernet texnologiyasi

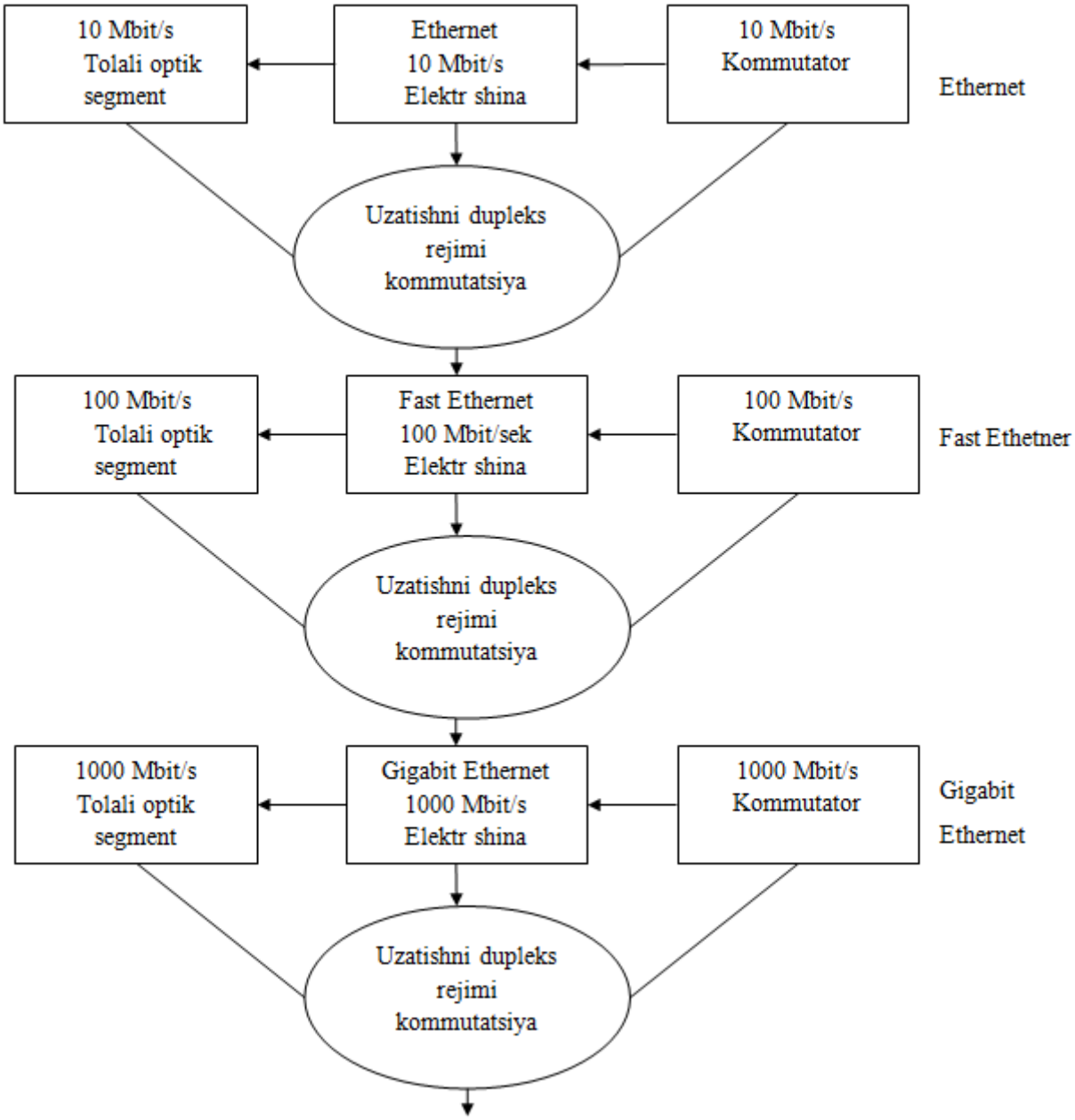
Hozirda ko‘pgina lokal tarmoqlar kanal sathidagi Ethernet texnologiyasi bo‘yicha qurilgan. Kanal sathidagi Ethernet texnologiyasini farq qiluvchi xususiyati uni ikkita sath bo‘yicha ajratishdir: muhitga ulanish bilan boshqarish (Media Access Control, MAC) va logik kanal bilan boshqarish (Logical Link Control, LLC). MAC sathi muhitga ulanish algoritmini, tarmoqda ishchi stansiyalar adresini aniqlaydi, shuningdek fizik muhitni birgalikda qo‘llanilish vazifasini qo‘llaydi. LLC sathi quyidagi xizmatlarni qo‘llaydi:

- ulanishni o‘rnatmasdan va tasdiqlamasdan xizmat ko‘rsatish;
- ulanishga mo‘ljallangan xizmat ko‘rsatish;
- ulanishni o‘rnatmasdan tasdiqlaydigan xizmat ko‘rsatish.

Texnologiyaning asosiy kamchiligi muhitga raqobatli ulanish hisoblanadi. Shuningdek bu kamchilik qurilma narxini yetarlicha kamaytirish imkonini beruvchi afzallik hisoblanadi.

Hozirgi vaqtda o‘ngigabitli Ethernet (Gigabit Ethernet, GE) fizik sathda DWDM texnologiyasini qo‘llaydi. Shuningdek Gigabit Ethernet texnologiyasi zamonaviy raqamli tarmoqlar uchun bazaviy tarmoq texnologiyasi tarkibiga kirgan. OTO‘B/OSI modelida GE standarti kanal va fizik sathga mos keladi. Ethernet ustidan ovoz, ma’lumotlar, videoni uzatish mumkin. Ko‘p adresli texnologiya har bir foydalanuvchiga chegaralanmagan sondagi televizion va telefon kanallarni yetkazish

imkoniga ega, ma’lumotlar uzatish muhitining tezligi sekundiga yuz megabit va gigabit tezliklarda foydalanuvchilarni xizmatlarga ulanish imkonini ta’minlaydi.



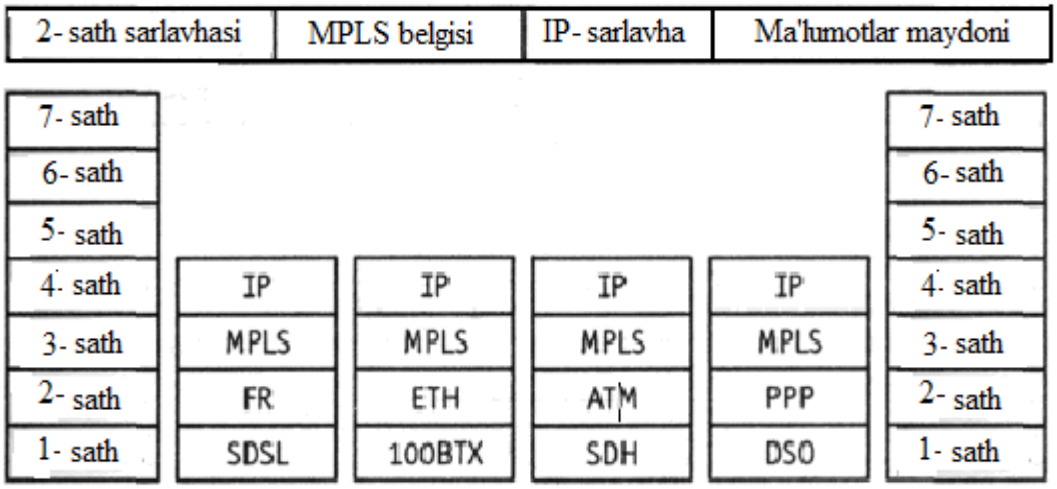

2.14-rasm. Ethernet texnologiyasining rivojlanish bosqichlari

## 2.8. MPLS asosidagi multimediali aloqa tarmog‘ining transport telekommunikatsiya texnologiyalari

Zamonaviy tarmoq infratuzilmasini qurishning istiqbolli yo‘nalishlaridan biri axborotni uzatish muhitlari va tizimlarining turli xil ko‘rinishlarini birlashtirishga imkon beruvchi yuqori tezlikli magistral tarmog‘ini va yagona signalizatsiya tizimini tashkil etish uchun optik texnologiyalardan foydalanish hisoblanadi. Bunday birlashtiruvchi texnologiya sifatida hozirgi vaqtda “Multiprotokol Label Switching - MPLS” (belgilar bo‘yicha ko‘p protokolli kommutatsiyalash) telekommunikatsiya texnologiyasi ko‘rib chiqiladi. Mazkur texnologiya IP-paketlarni ilgari surishni tezlashtirishga, trafikni boshqarish va ATM tarmoqlarida qo‘llaniladigan xizmat ko‘rsatish sifatini saqlab qolish mexanizmlari yordamida IP-tarmoqlar uchun xos moslashuvchanlikni saqlab qolishga urinishdan iborat. MPLS texnologiyasini joriy qilish IP-over-ATM arxitekturasiga tegishli bo‘lgan barcha yaxshi xususiyatlarni (samarali multipleksorlash va trafikning moslashuvchanligi, yuqori unumdorlik) saqlab qolishga imkon beradi va shu bilan birga u tarmoqlarning miqyosini yanada qo‘proq orttiradi, ularni qurishni va foydalanishni soddalashtiradi. Shunisi ham muhimki, MPLS faqat ATM bilangina qo‘llanilmasdan, balki kanal darajasidagi istalgan boshqa texnologiya bilan birga qo‘llanilishi mumkin. MPLS texnologiyasi X.25, Frame Relay tarmoqlarida qo‘llaniladigan virtual kanallar konsepsiyasini rivojlantiradi, bunda uni IP tarmoqlarni marshrutlashtirish protokollari yordamida olinadigan topologiya va joriy yuklanish to‘g‘risidagi axborot asosida yo‘llarni tanlash texnikasi bilan birlashtiradi. Bu SDH/WDM yoki IP/WDM texnologiyalari asosida Internet tolali-optik magistrallarini keyingi avlodiga o‘tishni soddalashtiradi.

MPLS - bu belgilardan foydalanishga asoslangan ko‘p protokolli tarmoqlarda paketlarning tez kommutatsiya qilish texnologiyasidir. MPLS o‘zida kanal darajasidagi texnologiyalar uchun xos bo‘lgan trafikni boshqarishni, tarmoq darajasidagi protokollarning miqyosliligi va moslashuvchanligini mujassamlashtirgan.

Texnologiyalarning nomidagi “ko‘p protokollilik” shuni anglatadiki, MPLS – inkapsulyatsiyalovchi protokol va boshqa protokollar to‘plamini tashishi mumkin (2.15-rasm). Bugungi kunda Internet provayderlar qatoridagi tarmoqlar ko‘p sathli model asosida tuzilgan, ya’ni mantiqiy marshrutlanuvchi IP–tarmoq ikkinchi sathning kommutatsiyalanuvchi topologiyasi (ATM yoki Frame Relay) ustida ishlaydi. Ikkinchi sathning kommutatorlari yuqori tezlikda ulanishni ta’minlaydi. Shunday qilib, MPLS - bu Internet tarmog‘ini evolyutsion rivojlantirish yo‘lida uning infratuzilmasini ikkinchi (kommutatsiya) va uchinchi (marshrutlashtirish) sathlari vazifalari integratsiyasi yo‘li bilan soddalashtirish tomoniga qo‘yilgan qadamlardan biridir.




2.15-rasm. IP-tarmoqlarda MPLS texnologiyasi va OSI/ISO modeli

MPLS texnologiyasi spesifikatsiyasida oqimlarni tashish va ularni boshqarish vazifalarini ajratish prinsipini asos qilib olinadi. Boshqaruvchi komponentlarni jo‘natuvchidan ajratish, ulardan har birini mustaqil ishlab chiqish va modifikatsiyalash imkonini beradi. Tabiiy majburiy talab shundan iboratki, bunda boshqariladigan komponentni uzatib beruvchi, komponentga axborotli paketlarni jo‘natish jadvali orqali uzatishi mumkin bo‘lsin. Boshqariladigan komponentning

boshqa marshrutizatorlar bilan axborot almashishi uchun marshrutlashtirishning standart protokollarini (JCPF, IS-IS, BGP-4) ishga tushiradi. Shu axborot asosida avval marshrutlashtirish jadvali, keyin esa har bir interfeysdagi qo‘shni tizimlar to‘g‘risidagi axborotni hisobga olgan holda paketlarni jo‘natish jadvali shakllantiriladi va modifikatsiyalanadi. Tizim yangi paketni olganda jo‘natuvchi komponentni, uning sarlavhasidagi axborotni tahlil qiladi, jo‘natish jadvalidagi tegishli yozuvni izlaydi va paketni chiqish interfeysiga yo‘naltiradi. Deyarli barcha ko‘p sathli kommutatsiya tizimlarining jo‘natuvchi komponenti, shu jumladan, MPLS ham paketlarning ketma-ket belgilaridan foydalanishga asoslangan. Belgi – bu paket sarlavhasida qayd qilingan uzunlikdagi qisqa maydondir.

MPLS yordamida quyidagi masalalarni hal etish mumkin:

- ATM va Fram Relay-ni IP bilan integratsiyasini;
- operator tarmog‘i ichida paketlarni eng qisqa an’anaviy marshrutlar bo‘yicha tezkor siljitish;
- virtual xususiy tarmoqlarni (VPN) yaratish;
- resurslarning (Traffic Engineering, TE) yuklanishini hisobga olgan holda yo‘nalishlarni tanlash va o‘rnatish.

### 2.8.1. MPLS tarmog‘i elementlari

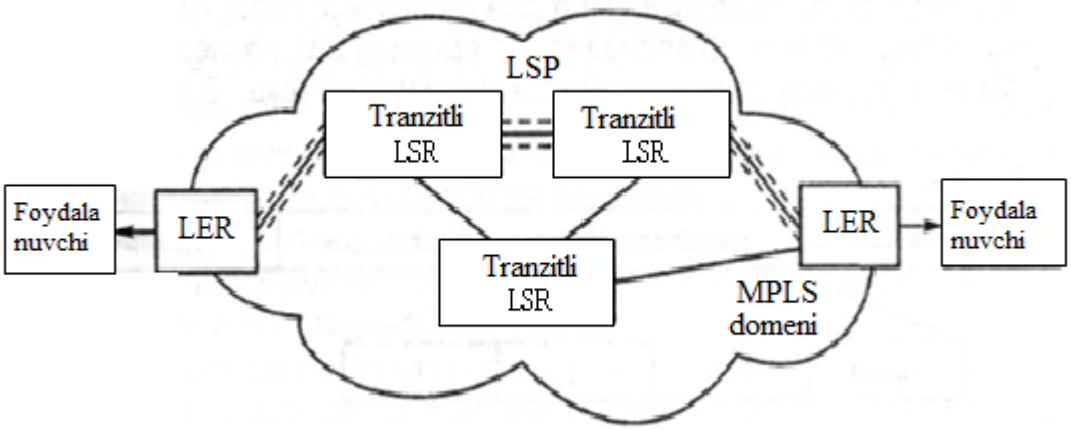
MPLS – belgilar bo‘yicha ko‘p protokolli kommutatsiyalash tarmoqlarida tarmoq uzellarining ikki turidan foydalaniladi. MPLS tarmog‘i chegaralarida joylashgan marshrutizatorlar kelayotgan IP-oqimlarni ajrata olishi va tahlil qila olishi va ularni to‘g‘ri keladigan marshrutlar bo‘yicha yo‘naltirishi kerak. Bu qurilmalar belgilar kommutatsiyasi bilan chegaraviy marshrutizatorlar deb ataladi (Label Edge Router-LER). Kiruvchi va chiquvchi LER bir-biridan farq qiladi. Kiruvchi LER oddiy marshrutizator kabi IP-sarlavhalarni tahlil qiladi va paketni keyingi uzatish uchun adresni tanlashda u ekvivalent xizmat ko‘rsatishning qaysi sinfiga (Forwarding

Eguivalencu Class - FEC) tegishli ekanini aniqlaydi. FEC - tarmoq darajasidagi paketlar sinfi bo‘lib, ular paketni yo‘naltirish yo‘lini tanlashda ham, resurslarga ulanish nuqtai nazaridan ham tarmoqdan bir xil xizmat ko‘rsatishni oladi.

Alohida paketlarni FEC ekvivalentlik sinfiga (yoki ekvivalent xizmat ko‘rsatish sinfiga, buning ikkalasi bir xil) abstraksiyalash, bir xil qayta ishlashni talab etuvchi katta miqdordagi trafik oqimlarini birlashtirish imkonini beradi. FEC ekvivalentlik sinfiga birlashtirilgan trafik oqimlari aynan bitta MPLS – belgi bilan identifikatsiyalanadi. Belgilangan tarmoq adresiga bog‘liq bo‘lmagan holda trafik oqimlarini birlashtirish imkoni qisman MPLSni masshtablashtirishga bo‘lgan imkoniyatini oshiradi, ya’ni marshrutizatorlarda belgilarni kommutatsiyalashning (LSR-marshrutizatorlari yordamida) qayta ishlanadigan, saqlanadigan va yo‘nalishlar haqidagi axborotlar hajmini kamayishi hisobiga.

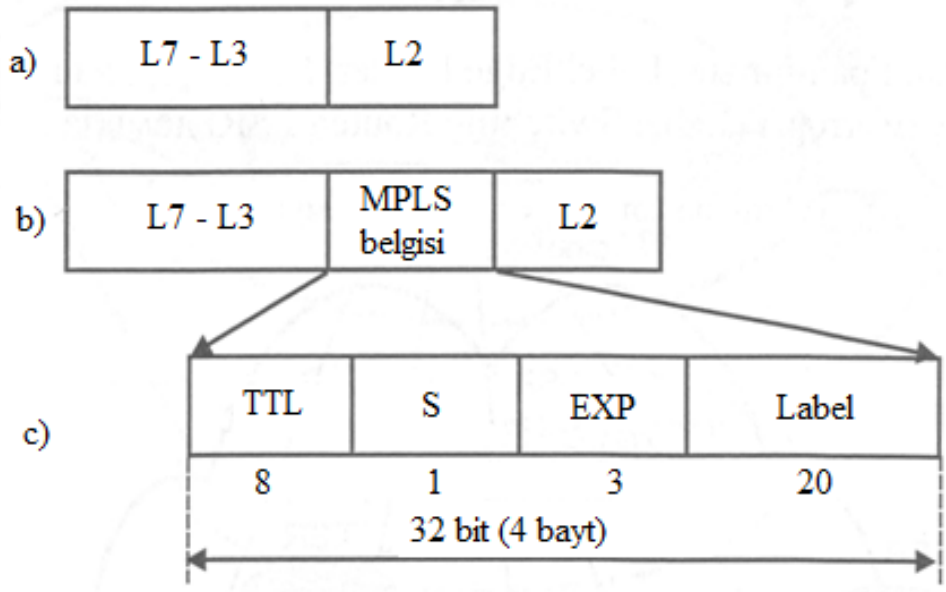
IP- deytagramma MPLS texnologiyasidagi protokolning (Protocol Data Unit, PDU) ma’lumotlar moduliga kiritiladi, MPLS sarlavha esa deytagrammaga biriktiriladi. Agar sarlavha xizmat ko‘rsatish sifati QoS (masalan, DiffServ) amali bilan birlashtirilgan bo‘lsa, kiruvchi LER marshrutizatori trafikni DiffServ qoidalariga binoan ko‘radi. So‘ngra LER berilgan paket uchun yo‘nalishni tanlash haqida qaror qabul qiladi, ya’ni paketni mos keluvchi tranzit belgilar kommutatsiyali marshrutizatorga (Label Switch Routers, LSR) yo‘llaydi.

Mazkur LSR uchinchi sathning sarlavhasini qayta ishlashni bajarmaydi (IP-sarlavha), balki jo‘natish to‘g‘risidagi qarorni marshrutlash jadvali asosida emas, balki paket belgisi asosida qabul qiladi va paketni jo‘natadi. So‘ng paket umumiy holda bir necha LSR orqali o‘tib, paket chiqish LER ga kelib tushadi, bu yerda LER PDU tahlil qilish operatsiyasini bajaradi, ya’ni paketdagi belgini olib tashlaydi, paketning sarlavhasini tahlil qiladi va uni MPLS - tarmog‘idan tashqarida joylashgan manzilga yo‘llaydi. (2.16-rasm)




2.16-rasm. MPLS tarmog‘i elementlari

FEC ning bitta sinfiga tegishli bo‘lgan paketlar, kirish LER dan to chiqish LER gacha belgilar bo‘yicha virtual kommutatsiyalanuvchi traktni yoki yo‘lni (Label Switched Parh, LSP) hosil qilib, juda ko‘p tranzit LSR lardan o‘tadilar. O‘rnatilgan ulanish simpleks hisoblanadi. Yarimdupleksli ulanishni tashkil etish uchun ikkita LSP o‘rnatilishi kerak. LSP doim tarmoqning chetidan boshlanadi va bir necha tranzit marshrutizatorlar orqali o‘tib qarama-qarshi tamonda tugaydi.

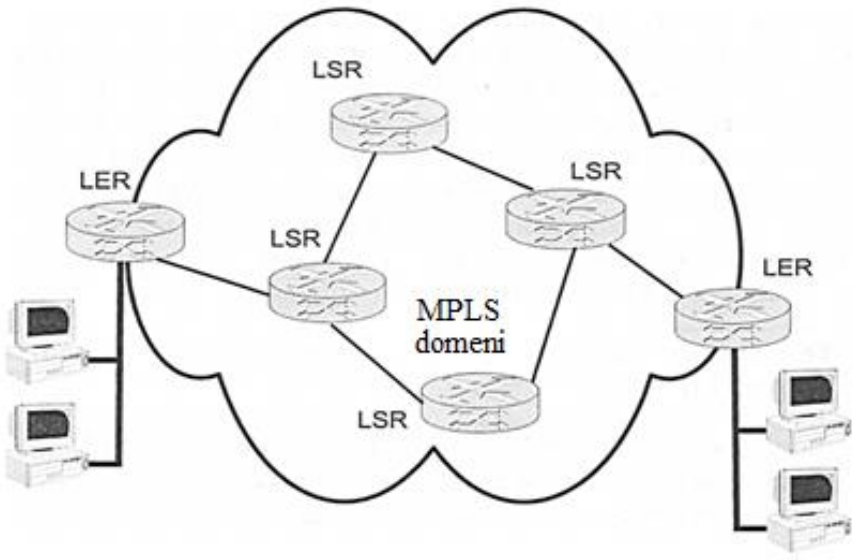



2.17-rasm. MPLS belgisining o‘rni va uning formati

MPLS texnologiyasi belgilar yordamida paketlar kommutatsiyasidan foydalanadi va axborotni NGN transport tarmog‘iga yetkazib berish uchun qo‘llaniladi (2.17-rasm).

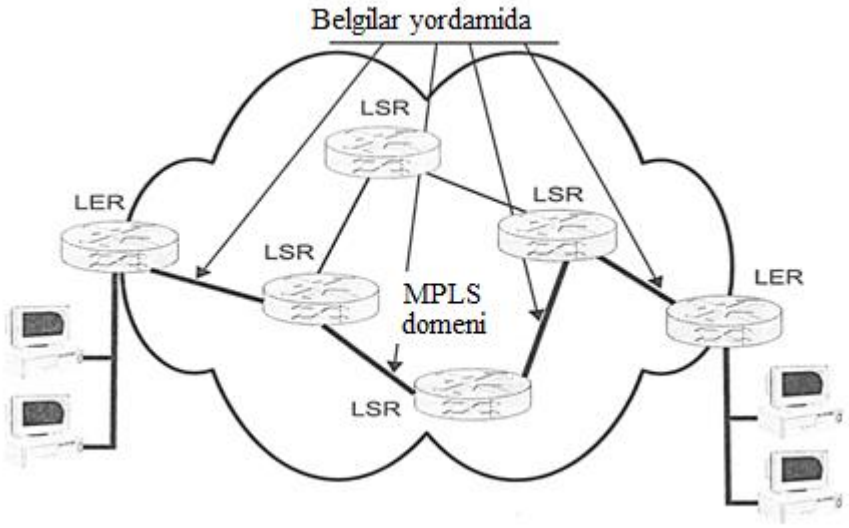
Belgi formatida to‘rtta maydon bor: paketning yashash vaqti (Time tolire) – 8 bit; belgilar stekining indikatori (Stek Mentilirs) – 1 bit (S=1- stekning oxirgi belgisi); kadrning ustunlilik belgisi (Exp) – 3 bit; belgining o‘zi (Label) – 20 bit.

2.18-rasmda belgilar yordamida paketlarni kommutatsiyalovchi MPLS domenining chegaraviy (Label Edge Router, LER) va tranzit marshrutizatorlari (Label Switshing Router, LSR) ko‘rsatilgan.




2.18-rasm. MPLS domenining chegaraviy (Label Edge Router, LER) va tranzit (Label Switshing Router, LSR) marshrutizatorlari

2.19-rasmda LSR yordamida ikkita chegaraviy marshrutizatorni bog‘lovchi yo‘l (Path) ko‘rsatilgan. LSRda paketlar belgilar yordamida kommutatsiyalanadi.

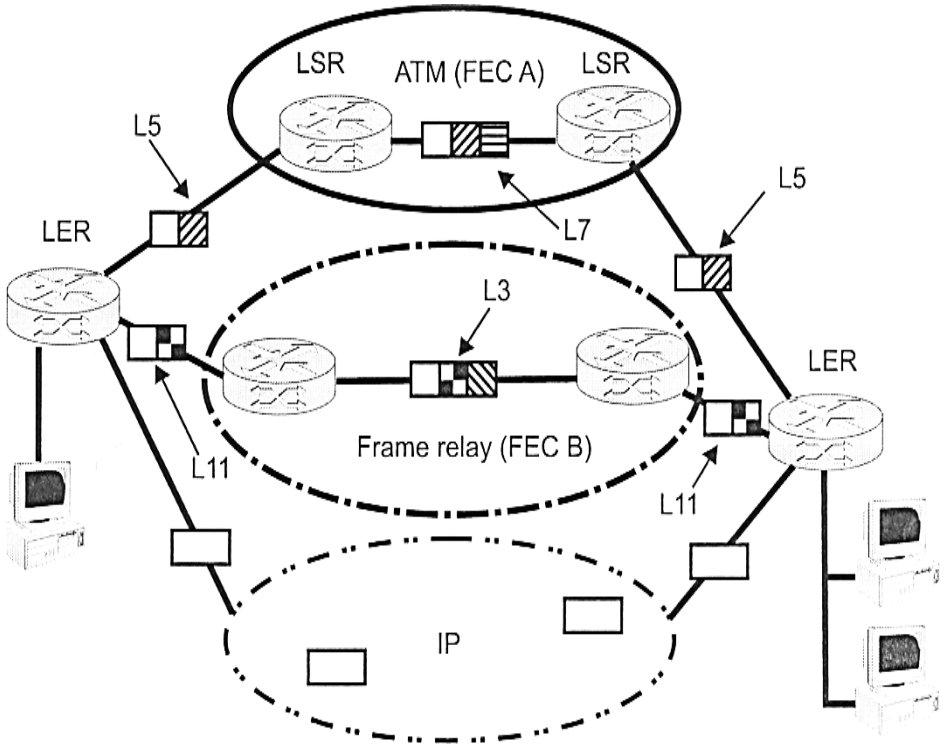



2.19-rasm. Ikki chegaraviy marshrutizatorni LSR yordamida bog‘lovchi yo‘l (Path); LSRda paketlar belgilar yordamida kommutatsiyalanadi

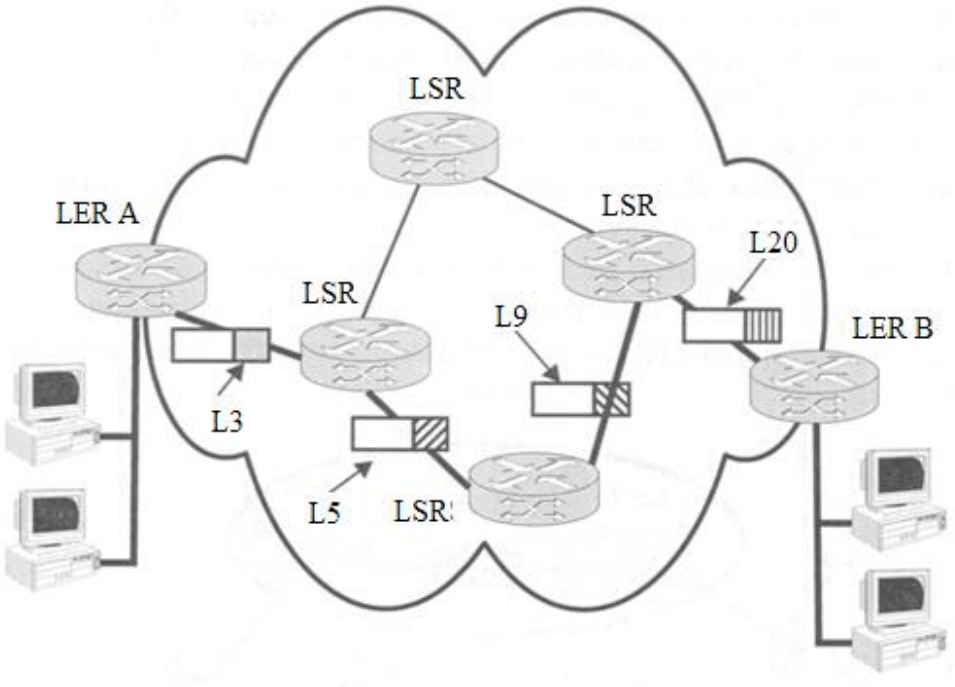
2.20-rasmda MPLS domenida ikki sinfdagi ma’lumotlarni yetkazib berish usuli (Forwarding Eguivaleme Class, FEC) ko‘rsatilgan.

IP paketlar oqimini Internet orqali eltib berish sifati kafolatlanmagan holda uzatiladi. Agar foydalanuvchilarning axboroti kechikishlarga, yo‘qolishlarga, kechikish djitteriga sezgir bo‘lsa, bu holda paketlar uchun MPLS domenida dastlabki yo‘l yaratilishi mumkin, unda eltib berish ko‘rsatkichlari sifati kafolatlanadi. Paketlarni eltib berishning har bir sinfi uchun (FEC) alohida yo‘l yaratilishi mumkin.

2.20-rasmda A (ATM texnologiyasi bilan domenning 1.5, 1.7 belgilar steki) va B (FR texnologiyasi bilan domenning 1.11, 1.33 belgilar steki) sinflaridagi belgilangan paketlar uchun axborotlarni aniq sifat kafolati bilan yetkazishni ikkita yo‘nalishi ko‘rsatilgan.




2.20-rasm. MPLS domenida ikki sinf (FEC – Formarding Eguivaleme Class) ma’lumotlarini yetkazib berish

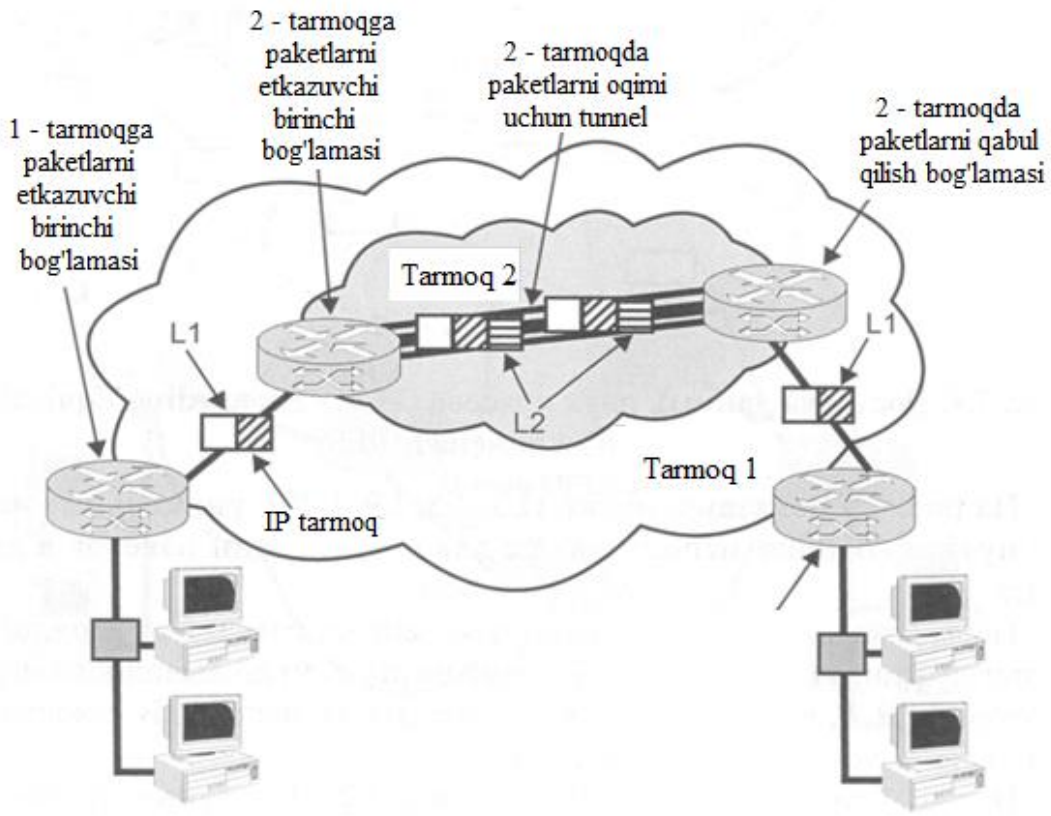



2.21-rasm. Har bir bo‘g‘inda noyob bo‘lgan belgilar MPLS domenida paketlar kommutatsiyasi uchun foydalaniladi

2.21-rasmda har bir yo‘lda noyob bo‘lgan belgilar (1.3, 1.5, 1.9, 1.20) va MPLS domenida paketlarni kommutatsiyalash uchun foydalaniladigan belgilar ko‘rsatilgan.

Belgilar qo‘yilgan paketlarni kiruvchi chegaraviy LER A marshrutizatordan (2.21-rasmda chapda) to chiquvchi LER B marshrutizatorgacha yetkazib berish uchun yaratilgan yo‘l bir necha bo‘g‘indan iborat bo‘lishi mumkin. Har bir bo‘g‘inda noyob belgidan foydalaniladi.

2.22-rasmda belgilar (L2/L1) steki (Push) va 2 tarmoq orqali paketlar oqimini tunellash ko‘rsatilgan.

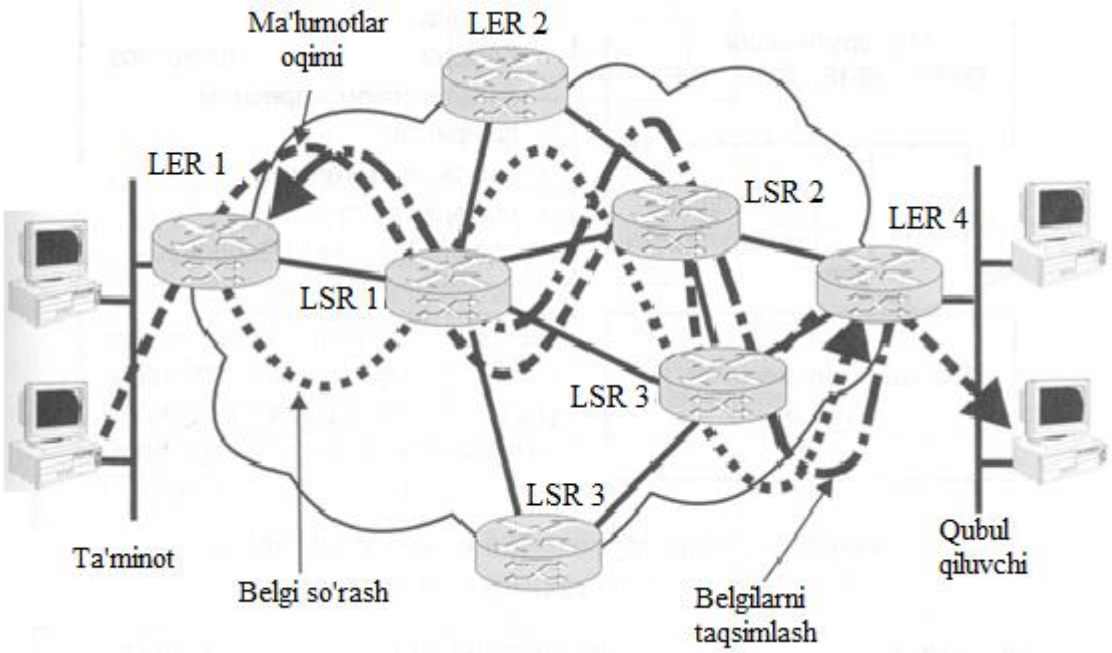



2.22-rasm. Belgilar steki (Push) va paketlar oqimini 2 tarmoq orqali tunellash

1-tarmoq bir operatorga, 2-tarmoq esa boshqa operatorga tegishli bo‘lishi mumkin. Belgi qo‘yilgan paketlarni eltib berish yo‘li ikki va undan ortiq tarmoq orqali o‘tishi mumkin. 1-tarmoqda ikki chegaraviy marshrutizator orasidagi paketlarni eltib berish uchun L1 stekning quyi belgisi qo‘llanilishi mumkin, 2-tranzit tarmoq

orqali paketlarni uzatish uchun L2 stekning yuqori belgisi qo‘llaniladi. Shu tarzda 2-tarmoqda L1 belgili belgilangan paketlar uchun tunnel shakllanadi.

2.23-rasmda belgilar yordamida kommutatsiyalanuvchi yo‘lning yaratilishi (Label Switehed Path, LSP) yordamida kommutatsiyalanadigan yo‘lni yaratish va IP paketlarni MPLS domenlari orqali eltib berish ko‘rsatilgan.




2.23-rasm. Belgilar (LSP) yordamida kommutatsiyalanadigan yo‘lni yaratish va IP paketlarni MPLS domenlari orqali eltib berish:

LER1 – kiruvchi chegaraviy marshrutizator;

LER4 – chiquvchi chegaraviy marshrutizator;

LSR1, LSR2, LSR3 – paketlarni belgilar yordamida kommutatsiyalovchi tranzit marshrutizatorlar.

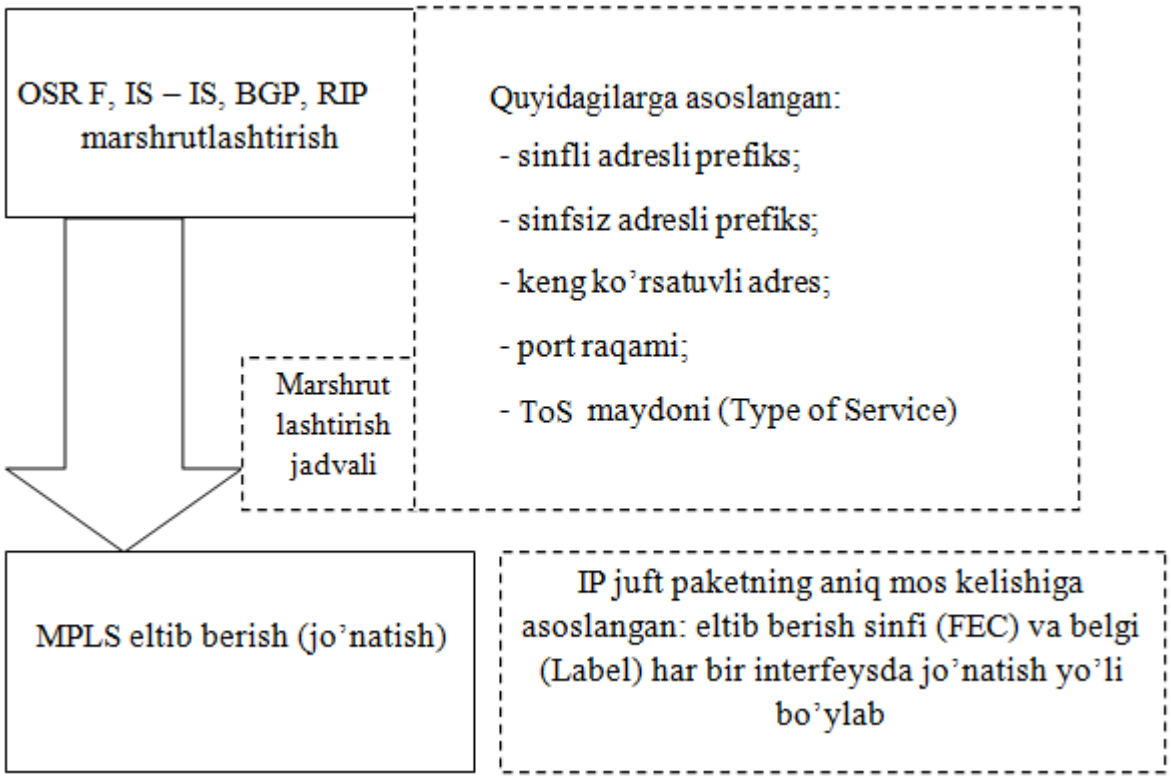
IP paketlarni eltib berish o‘z tabiatiga ko‘ra ulanishni o‘rnatishni talab etmaydi, chunki har bir paketning marshrutlanishi uning sarlavhasidagi axborot asosida amalga oshiriladi. LER1 kiruvchi portga kelayotgan paketlar yig‘indisiga eltib berish sinfi (Forwarding Eguavalence Class, FEC) beriladi. Bu paketlar yig‘indisini eltib berish

uchun LER1 belgini LER4 dan talab qilib oladi. Belgilarni taqsimlash protokoli (Label Distri Putіon Protocol - LDP) belgilar yordamida kommutatsiyalanuvchi yo‘l bo‘ylab belgilarni taqsimlab LER1 dan LER4 gacha bo‘lgan yo‘lni tayyorlaydi, Shundan so‘ng belgi qo‘yilgan paketlar manbadan (Source) oluvchiga (Destination) MPLS domenining “LER1–LER1–LER1–LER2–LER3–LER4” virtual birikmasi bo‘ylab uzatiladi. Belgilarni taqsimlanishi qo‘shni marshrutizatorlarda belgilarni FEC (eltib berish sinfi)ga bog‘lanishining umumiy akslanishi mavjudligini ta’minlaydi.

MPLS texnologiyasida marshrutlashtirish va eltib berishni (jo‘natilishini) ajratish prinsipi qo‘llaniladi. 2.24-rasmda amaliy sathdagi marshrutlashtirish protokollari keltirilgan bo‘lib, ular kommutatsiyalovchi LER va LSR marshrutizatorlari uchun marshrutlashtirish jadvallarini va kommutatsiyalash jadvallarini shakllantirish uchun axborotni taqsimlash rejasini va tarmoq topologiyasini qo‘llaydi.

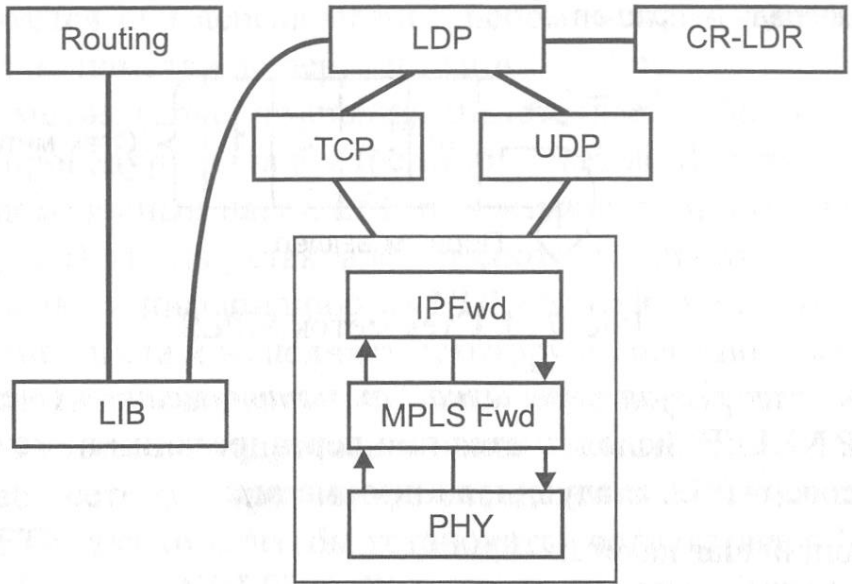
MPLS ning asosiy komponentlari quyidagi sathlarga bo‘lingan:

- tarmoq sathidagi marshrutlashtirish protokoli (network layer IP routig protocols);
- ma’lumotlarni tarmoq sathidan tashqarida eltib berish (edge of network layer forwarding);
- tarmoq yadrosida belgilardan foydalangan holda kommutatsiyalash (Core network label-pased switching);
- belgilar texnika sxemasi va detalizatsiyasi (label schematics and granularity);
- belgilarni taqsimlash uchun signalli protokol (signaling protocol for Cabel distribution);
- trafikni boshqarish (traffic engineering);
- ikkinchi protokol sathida ma’lumotlarni eltib berish variantlarining qo‘shilishi (ATM, Frame Relay, PPP).




2.24-rasm. MPLS texnologiyasi qo‘llanilganda marshrutlashtirish va eltib berish (jo‘natish)ning ajratilishi

2.25-rasmda MPLS protokollarining steki keltirilgan. Marshrutlashtirish va belgilarni taqsimlash (LDP) masalalari amaliy sathda hal etiladi. LDP protokolining signalli xabarlarini yetkazib berish, Internetning trasport darajasidagi TCP va UDP protokollari tomonidan amalga oshiriladi. Marshrutlashtirish va belgilarni taqsimlash protokollari dasturlar va ma’lumotlarning (LIB) tezkor axborotidan foydalanadi. MPLS funksiyali IP marshrutizatorining protokoli paketlarga belgi berish uchun kommutatsiyalash jadvalidan (MPLSFwd) foydalanadi. IP paketlar sarlavhasida bo‘lmagan va yuqori sathlarning protokollarini talablarini hisobga oluvchi qo‘shimcha ma’lumotlar, dasturlar va ma’lumotlar kutubxonasidan olinishi mumkin.




2.25-rasm. MPLS protokollari steki:

LDP (Label Distribuion Protokol) – belgilarni taqsimlash protokoli; CR–LDP–LDP+“Constraint” based “Routing” (belgilarni taqsimlash protokoli+cheklashlar asosida marshrutlashtirish); HB (Library)–dasturlar va ma’lumotlar kutubxonasi; MPLSFwd – ma’lumotlarni IP protokoli yordamida yetkazish; TCP (Transmission Control Protocol) – uzatishni boshqarish protokoli; UDP (Uzer Datagrem Protocol)– foydalanuvchining datagrammalarini uzatish protokoli

## Nazorat savollari

1. Aloqa arxitekturasini tushuntiring.
2. Ochiq tizimlarning o‘zaro bog‘lanish etalon modelining vazifasi nimadan iborat?
3. OTO‘B etalon modeli sathlarining vazifasini tushuntiring.
4. Axborotni uzatish muhiti sifatida qanday liniyalardan foydalaniladi?
5. Misli kabellarning qanday turlari mavjud va ular qayerda qo‘llaniladi?
6. Optik tolalarning qanday turlari mavjud?
7. Qaysi optik tola turi katta o‘tkazish oralig‘iga ega?
8. SDH ning vazifasi va sathlarini tushuntirish.
9. SDH qanday afzalliklarga ega?
10. Transport tarmoqda SDH ni qo‘llash qanday istiqbolga ega?
11. To‘lqinli zichlashtirish texnologiyasining mohiyati nimada?
12. CWDM, DWDM, HDWDM texnologiyalari nimasi bilan farqlanadi?
13. IP – texnologiyasining vazifasi va xususiyatlarini tushuntiring.
14. ATM - texnologiyasining vazifasi va yacheykasining tuzilishini tushuntiring.
15. Multiservisli aloqa tarmoqlarida Ehternet texnologiyasini qo‘llash qanday istiqbolga ega?
16. MPLS texnologiyasining vazifasi nima?
17. MPLS tarmog‘i elementlarini tushuntiring.
18. MPLS belgisi va uning formati tuzilishini tushuntiring?
19. MPLS ni asosiy komponentlari qanday sathlarga bo‘lingan?
20. MPLS stek protokollarining vazifasi nimadan iborat?

# 3. MULTIMEDIALI ALOQA TARMOQLARIDA XIZMAT KO‘RSATISH SIFATINI TA’MINLASH USULLARI VA VOSITALARI

## 3.1. Xizmat turlari va uni tashkillashtirish xususiyatlari

**Xizmatlar klassifikatsiyasining prinsiplari.** Hozirda aloqa operatorlarining xizmatlari ko‘pincha bir darajali prinsip bo‘yicha klassifikatsiyalanadi va bunday xizmatlarning ro‘yxatlarida IP, VPN, DSL, telefon aloqalarini ko‘rish mumkin. Xizmatlarning aniq bo‘lmagan klassifikatsiyasi tijorat siyosatidagi va marketingdagi muammolarga olib keladi, bu yaratilgan infrastruktura va kapital xarajatlar samaradorligida va muddatlarida namoyon bo‘ladi.

Shuning uchun aloqa operatori xizmatlarning ko‘p o‘lchamli strukturasini ishlatgan holda, klassifikatorlar tizimlariga asoslanib, klassifikatsiyalash maqsadga muvofiq bo‘ladi.

Ularning asosiylari muhimlilik darajasi bo‘yicha quyida keltirilgan:

- uzatilayotgan axborot turini tartibi bo‘yicha xizmatlar klassifikatsiyasi (kontent);
- mijozning xizmatga ulanishini ta’minlash usuli bo‘yicha xizmatlar klassifikatsiyasi;
- mijoz turi bo‘yicha xizmatlar klassifikatsiyasi;
- axborot almashish turi bo‘yicha xizmatlar klassifikatsiyasi.

Bundan tashqari, yuqorida keltirib o‘tilgan klassifikatsiyalardan tashqari, xizmatlarning har bir turi uchun ularni quyidagi belgilar bo‘yicha ajratish mumkin:

- tadbiq etish va muhimlilik darajasi bo‘yicha – asosiy xizmatlar va qo‘shimcha (narxlar qo‘shilgan xizmatlar) xizmatlar, bunda ko‘rsatilgan qo‘shimcha xizmatlar faqatgina asosiy xizmatlar mavjud bo‘lgandagina ko‘rsatiladi;
- marketing funksiyasi bo‘yicha – foyda olish uchun qaratilgan xizmatlar va mijozlarning e’tiborini o‘ziga tortishga qaratilgan xizmatlar (bunda mijozlarning

e’tiborini qaratish usuli bilan mijozlarni xizmatlardan foydalanishi hisobiga foyda olinadi).

Uzatilayotgan axborot turiga qarab xizmatlarni klassifikatsiyasi asosiy hisoblanadi. Biroq klassifikatsiyaning boshqa usullari ham kerakli hisoblanadi, chunki taqdim etilayotgan xizmatlarning xususiyatlarini ajratib beradi, bunda u uning qo‘llanilish sohalarini aniq ko‘rsatib beradi.

**Uzatilayotgan ma’lumot turiga qarab xizmatlar klassifikatsiyasi (kontent).** Ushbu usulga mos ravishda xizmatlar klassifikatsiyasi quyidagilarga bo‘linadi:

- telefon (va videotelefon) xizmatlari;
- ma’lumotlar uzatish xizmatlari;
- keng eshittirishli xizmatlar;
- ajratilgan kanallarning xizmatlari (uzatilayotgan ma’lumotlar turiga umuman bog‘liq bo‘lmagan xizmatlar);
- infrastrukturali xizmatlar.

Telefon xizmatlari deganda tovush uzatishni tushunish mumkin. Bunda oxirgi foydalanuvchi sifatida boshqa huddi shunday mijozlar bilan interaktiv rejimda o‘zaro munosabatda bo‘ladigan individual mijozlar bo‘lishi mumkin. Bu xizmatlar o‘z navbatida qayd etilgan va uyali telefon aloqasi xizmatlariga bo‘linishi mumkin. Bundan tashqari, hozirda ushbu turdagi xizmat turlaridan bosqichma bosqich video uzatish xizmat turi (videotelefoniya) ajralib chiqmoqda. Masalan, bu xizmatlarning asosiy turlaridan biri videokonferens aloqa hisoblanadi.

Hozirda sodir bo‘layotgan tarmoqlarning konvergensiyasida telefon va boshqa turdagi xizmat turlari orasidagi chegara unchalik ajratilmaydi. Biroq hozirgi kunda telefon xizmat turlarini boshqa xizmat turlaridan ajratishimizning asosiy sabablaridan biri, bu abonent tamonidan chaqiriladigan manzillar tahlili asosida kanallar kommutatsiyasi bilan bog‘liq.

Telefon xizmatining asosiy hisob birligi “ulash minuti” hisoblanadi va bu tarmoqning infrastrukturasiga (TDM, VoIP), mijoz turiga (subprovayderlarga va

korporativ mijozlarga “minutlar” ulgurji sotilishi mumkin) va ulanish turiga bog‘liq emas. Qo‘shimcha hizmatlar (masalan, intellektual tarmoq xizmatlari) ham “minut” birligi sifatida hisoblanadi. Trafikni “chegaralanmagan” tariflash xizmat turlari ham uchrab turadi. Agar minut bo‘yicha tariflash xizmati operator tomonidan olib borilmasa, telefon xizmatlariga berilgan xizmat mezonlariga bog‘liq holda operator tarmog‘ida telefon kanalini kommutatsiyalash amalga oshirilishi mumkin.

O‘z navbatida ma’lumotlar uzatish xizmatlari IP, ATM, FR, X.25 va boshqa shu kabi xizmatlarga bo‘linadi. Bu xizmatlar abonentni manzil (kommutatsiyalash) bilan ulashni amalga oshiradigan paketlar sarlavhasini tahlil qilish asosidagi protokollarga bog‘liqligi bilan farqlanadi. Hisoblashlar uzatiladigan trafikdan kelib chiqqan holda amalga oshiriladi, ya’ni bilvosita yoki bevosita o‘lchash amalga oshiriladi, masalan, xizmat ko‘rsatish sathi haqida kelishuv (SLA) asosida yoki kanal sig‘imi va uni ishlatish vaqtiga bog‘liq uzatilayotgan trafikdan kelib chiqqan holda amalga oshiriladi. Xizmat ko‘rsatish ko‘p protokolli ma’lumotlar uzatish muhitidan foydalanilgan holda taqdim etilganda va tarmoqda ko‘p turdagi trafik mavjud bo‘lganda xizmat turini “ajratish” oson bo‘lmaydi, ya’ni ulardan o‘tayotgan trafik qismini belgilash oson bo‘lmaydi. Bularni IP – paketlari, ATM – yacheykalari, FR va X.25 kadrlari asosida hisoblash oson bo‘ladi. Bu hisoblashlarning natijalarini foydalanuvchiga ishlatilgan pul qiymati sifatida uzatiladi. Ko‘p protokolli tarmoqda trafikning tarifikatsiyasi mavjud bo‘lmagan holatda, xizmat turini ajratilgan kanallar xizmati turiga kirgizishimiz mumkin.

Keng eshittirishli xizmatlar bir vaqtda ko‘p sonli mijozlarga ma’lumotlarni bir yo‘nalishda uzatishni taqdim etadi. Unga birinchi navbatda tele va radio eshittirishlar kiradi. Hozirda bu xizmat turlarini kengaytirish ishlari olib borilmoqda. Bu harakatlar tufayli interaktiv televideniya vujudga keldi.

Ajratilgan kanallar xizmatlari orqali ma’lumotlar yetkazib berish tarif siyosatiga ega kanallarni taqdim etadi. Bu siyosatda trafikning turi, qiymati va kanalni

ishlatish darajasi hisobga olinmaydi. Turli xil tariflarni farqini, kanalning turi va uning eng katta o‘tkazuvchanlik qobiliyati bo‘yicha ajratish mumkin.

Mijozlarga ma’lumotlar yetkazib berish bilan bog‘liq bo‘lmagan xizmatlarni infrastrukturali xizmatlar deb atash mumkin. Bu xizmat turlariga misol tariqasida infrastrukturani (qurilma yoki joy) ijaraga berishni va turli maslahatli xizmatlarni olish mumkin. Bundan tashqari bir turdagi ish ham bo‘lishi mumkin. Masalan, boshqa operator yoki korporativ mijozning telekommunikatsiya tarmog‘ini loyihalash yoki qurish.

**Mijoz turiga nisbatan xizmatlarni klassifikatsiyalash**. Mijoz turiga nisbatan xizmatlarni klassifikatsiyalash quyidagi xizmatlar guruhidan tashkil topgan:

- boshqa aloqa operatorlariga ko‘rsatiladigan xizmatlar (provayderlarga);
- korporativ mijozlarga ko‘rsatiladigan xizmat turlari;
- individual foydalanuvchilarga ko‘rsatiladigan xizmat turlari.

Bu guruhlar bir-biridan xizmatlar nomenklaturasiga va operator infrastrukturasini rivojlantirish darajasiga bo‘lgan talablarga nisbatan ajralib turadi.

Boshqa operatorlarga ko‘rsatilayotgan xizmatlar nomenklaturasi bir qator ustunliklarga ega. Chunki boshqa operatorlar bilan munosabat yoki resurslarni ulgurji sotish uchun “ulgurji operator” – “chakana operator” sxemasi asosida quriladi yoki ma’lumotlar almashish xizmatiga olib keladigan teng kuchli munosabat asosida quriladi.

Korporativ mijozlar, yirik va kichik bo‘lishi mumkin. Kichik korporativ mijozlar, individual foydalanuvchilar ishlata oladigan xizmatlar (bazaviy telefon, kommutatsiyalangan ulanish, DSL va boshqalar) to‘plamidan foydalanishlari mumkin.

**Mijozning ulanishi bo‘yicha xizmatlar klassifikatsiyasi**. Mijozning ulanishi bo‘yicha xizmatlar klassifikatsiyasi bazaviy xizmatlarni taqdim etish usulini aniqlashtirishga imkon yaratib beradi va ushbu xizmatni yetkazib berish uchun ishlatiladigan infrastruktura asosida yotuvchi tarmoq ierarxiyasining quyi sathlarini ko‘rsatadi. Ulanish usullari quyidagilar bo‘lishi mumkin:

- kommutatsiya qilinayotgan telefon kanallari yoki ISDN kanallari;
- turli xil o‘tkazuvchanlik qobiliyatiga ega SDH kanallari;
- turli xil o‘tkazuvchanlik qobiliyatiga ega Frame Relay kanallari;
- turli xil o‘tkazuvchanlik qobiliyatiga ega ATM kanallari;
- turli xil o‘tkazuvchanlik qobiliyatiga ega Ethernet kanallari;
- xDSL (ADSL, SDSL, SHDSL) texnologiyalari;
- passiv optik tarmoqlar (Passive Optical Network, PON);
- koaksial sim va optik tola asosidagi gibrid tarmoqlar (HFC);
- simsiz aloqa tarmoqlari.

Yuqorida keltirilgan klassifikatsiyalar asosida tavsiflab berilgan xizmatlarni aniqlashtirish mumkin. Masalan, «Internet tarmog‘iga Frame Relay kanali bo‘yicha va ADSL texnologiyasini ishlatgan holda ulanish» ikkita turli xil xizmatlarga bo‘linadi. Ulardan birinchisi operatorlar va korporativ mijozlar uchun mo‘ljallangan, ikkinchisi korporativ va individual mijozlar uchun mo‘ljallangan.

**Axborotlar almashish turi bo‘yicha xizmatlarni klassifikatsiyalash**.

Mijozlar va hamkorlar bilan munosabatlar teng huquqli bo‘lishi va teng huquqli bo‘lmasligi mumkin va shunga bog‘liq holda u quyidagi turlarga bo‘linadi:

- o‘zining tarmog‘idagi resurslardan foydalana olish (o‘zining tarmog‘idagi resurslar orqali boshqa tarmoq resurslaridan foydalanish);
- ikki tomonlama axborot almashish;
- tranzit;
- axborot almashish markazi (hisoblash markazi bilan yoki u bo‘lmagan holda).

Tarmoq resurslaridan foydalana olish huquqi – bu korporativ va individual mijozlar bilan o‘zaro munosabatning asosiy formasi, biroq bu xizmat operatorlarga ham ko‘rsatilishi mumkin. Shu bilan birga agar operator o‘zining tarmog‘i orqali boshqa tarmoq resurslariga ulanishni ta’minlasa, u holda ulanish hududiy, mahalliy va xalqaro turlarga bo‘linishi mumkin.

Axborotlar almashish haqidagi ikki tomonlama kelishishda (trafik terminatsiyasi), operatorlar xizmatlarni taqdim etishlari yoki hamkorning xizmatlaridan foydalana olishlari mumkin. Bunda ular trafik terminatsiyasidan yoki xizmat turiga bog‘liq holda trafikdan foyda oladilar. Bunday almashish kelishishga bog‘liq holda mahalliy, hududiy va xalqarolarga bo‘linishi yoki bo‘linmasligi mumkin. Tranzit haqida kelishish, ikkita yoki bitta operator (yoki korporativ mijoz) bo‘lgan nuqtalar orasida axborot uzatish uchun operator tarmog‘i resurslarini ishlatish imkonini beradi va hududiy prinsip bo‘yicha bo‘linishi mumkin. Uzatilayotgan trafik tarifikatsiyasi mavjud bo‘lmagan holda bunday xizmat turi ajratilgan kanalni ijaraga berish bilan mos tushadi.

Operatorda tranzit haqida katta miqdorda ikki tomonlama kelishish bo‘lgan holda, operator tarmog‘i asosidagi ma’lumotlar almashish Markazi (balkim – clearing house) bo‘lishi mumkin. Bu holda Markaz xizmatlaridan foydalanadigan operatorlar, boshqa operatorlar bilan o‘zaro ma’lumot almashish to‘g‘risida ikki tomonlama kelishish tuzmaydilar. Umuman olganda ular boshqa operatorlar bilan ma’lumot almashish uchun Markaz tomonidan yetkazib berilayotgan tranzit xizmatlardan foydalanishadi. Tabiiyki, bunday turdagi Markazni tashkil etish har biri bir-biri bilan ikki tomonlama kelishish bitta Markaz bilan kelishishga qaraganda kamroq foydaliroq bo‘ladi. Bu infrastruktura va umumiy harajatlarni kamaytirish hisobiga yuzaga keladi va bu qo‘shimcha xizmat turlarini yuzaga keltiradi.

Agar korporativ mijozlar uchun o‘zining ofislarini birlashtirib turadigan va turli xil ulanish texnologiyalari qo‘llaniladigan mobil va uy foydalanuvchilari uchun ma’lumotlar almashish Markazi xizmatini ko‘rib chiqadigan bo‘lsak, bu holda bu xizmat turi mijozning virtual hususiy tarmog‘i xizmatini namoyon etadi.

**Asosiy va qo‘shimcha xizmatlar. Katta foyda keltiruvchi va marketing funksiyasini amalga oshiruvchi xizmatlar.** Asosiy xizmatlar bilan birga beriladigan qo‘shimcha xizmatlar, asosiy xizmatlardan keladigan foyda bilan bir xil, ba’zi hollarda ko‘proq ham bo‘lishi mumkin. Ba’zi hollarda qo‘shimcha xizmatlar foyda

keltirmasligi ham mumkin, ba’zi hollarda esa, ya’ni asosiy xizmatlarni hisobga olmagan hollarda zarar keltirishi ham mumkin. Bu holni asosan mijozlarni asosiy xizmatga jalb qilishda ishlatilishida ko‘rish mumkin.

Bir necha bunday qo‘shimcha xizmatlarni keltirib o‘tamiz.

1. O‘zining tarmog‘ida Internetga kommutatsiyalanadigan ulanish serverini o‘rnatish. Bu xizmat turi operatorlar uchun foydali bo‘lib, tarif turiga qarab Internetdan foydalanuvchilardan qo‘shimcha foyda olishadi. Biroq umumiy foydalanish telefon tarmog‘ining (UFTT) barcha foydalanuvchilari tomonidan operator tarmog‘ida amalga oshirilayotgan qo‘ng‘iroqlar operator tarmog‘ida terminlashtiriladi. Shuning uchun har bir shunday qo‘ng‘iroq uchun operator qo‘shimcha “terminlashtirilgan minut”ga ega bo‘ladi. Bu “terminlashtirilgan minut” operatorlar orasida kelishish asosida bo‘lib, buning uchun qaysi operator bilan kelishish amalga oshirilganiga qarab operatorlar to‘lovlarni amalga oshiradilar. Shuning uchun Yevropa va AQSh da hozirda “Internetga bepul ulanish” xizmati mashhur bo‘lib ketgan. Bu shunchaki bepul emas, foyda Internetga ulanishdan olinmaydi, balki mijozning operatorlar to‘lovi asosida so‘zlashuvlarga vaqtinchalik xaq to‘lash hisobiga amalga oshiriladi.

2. Intellektual xizmatlarni taqdim etish ikki barobar foyda keltiradi. Birinchidan, bu xizmat turlari yaxshigina foyda keltiradi, shuningdek bunday har bir qo‘ng‘iroq avvalgi misolimizda ko‘rganimizdek qo‘shimcha foyda keltirgan holda operator kirish trafigidan oshib ketadi.

3. Xosting xizmati, masalan, mijozlarning Web-serverlari unchalik katta foyda keltirmaydilar. Biroq katta kontent-provayderning Web-sahifasi, ma’lum bir ma’lumotga murojat qiluvchi boshqa operatorlarning mijozlari hisobiga chiquvchi IP – trafigi oshib ketishi mumkin. Bu esa boshqa Internet (Internet Service Provider, ISP) provayderlari bilan tuzilgan axborot almashish shartnomasi bo‘yicha qo‘shimcha foyda keltirishi mumkin. Shuning uchun odatda bepul Web-xosting ham katta foyda olib kelishi va trafikni oshishiga olib kelishi mumkin.

**Telefon xizmati guruhiga kiruvchi xizmatlar.** Eng ko‘p ishlatiladigan xizmatlar bu individual mijozlarga ko‘rsatiladigan xizmatlardir. Shu bilan birga aloqa operatorlari va korporativ mijozlar uchun xizmatlar bozori, xizmatlarni umumiy sonda sotish hisobiga katta foyda olib kelishi mumkin. Shu tarzda, barcha uchta mijozlar segmentlari uchun xizmatlar to‘plamini baholash zarur.

Individual mijozlar uchun:

- telefon aloqasi xizmatlarini taqdim etish;
- qo‘shimcha narxlarga ega bo‘lgan qo‘shimcha xizmatlarni ko‘rsatish.

Aloqa operatorlari uchun (hududiy va xalqaro):

- xalqaro operatorlarning trafigining tranzit/terminatsiyasi;
- shaharlararo operatorlarning trafigining tranzit/terminatsiyasi;
- IP-telefoniya trafigining tranzit/terminatsiyasi;
- telefoniya va IP-telefoniya (clearing house) operatorlari orasidagi o‘zaro hisob kitob xizmatlarni taqdim etish;
- telefon va IP-telefoniya operatorlari uchun xalqaro ulanish shlyuzlarini tashkillashtirish;
- narxlar qo‘shilgan qo‘shimcha xizmatlarni taqdim etish (intellektual xizmatlar).

Korporativ mijozlar uchun (davlat tashkilotlari, tijorat tashkilotlari va boshqalar):

- telefon aloqasi xizmatlarini taqdim etish;
- “tovushli VPN”ni tashkillashtirish;
- xalqaro (shaharlararo) ulanish xizmatlarini tashkillashtirish;
- narxlar qo‘shilgan qo‘shimcha xizmatlarni taqdim etish (intellektual xizmatlar).

Bu yerda ajratilgan kanallarni taqdim etish bilan bog‘liq bo‘lgan telefon xizmatlari haqida alohida gapirilmayapti.

**Ma’lumotlar uzatish xizmatlari**. Yuqorida aytib o‘tilganidek, aloqa xizmatlarini tizimlashtirish bir muncha qiyinchiliklar yaratadi. Bunda ma’lumotlar uzatish xizmatlarini tartiblash ham oson bo‘lmaydi, chunki ularni turli xil klassifikatsiya bo‘yicha ko‘rib chiqiladi. Aloqa xizmatlari klassifikatsiyasining turlaridan biri axborot uzatish turi bo‘yicha xizmatlarni ajratish (kontent):

- ATM protokoli bo‘yicha ma’lumotlar uzatish xizmati;
- FR protokoli bo‘yicha ma’lumotlar uzatish xizmati;
- IP va boshqa protokollar bo‘yicha ma’lumotlar uzatish xizmati.

Biroq yuqoridagi ro‘yxat telekomunikatsiya tarmoqlari va qurilmalari bilan amalga oshiriladigan asosiy, formal funksiyalarni tavsiflaydi. Bu bo‘limda xizmatlarni axborot almashish turi bo‘yicha tizimlashtirish taklif etiladi. Bu holda xizmatlar nomenklaturasi yuqorida ko‘rsatilgan asosiy xizmatlarni kombinatsiyalashni amalga oshiradi va u quyidagi asosiy xizmatlardan tashkil topgan:

- IP, ATM, FR, X.25 protokollari asosida magistral aloqa tarmog‘i xizmatlari va resurslariga ulanishni taqdim etish;
- IP, ATM, FR, X.25 protokollari bo‘yicha ma’lumotlar trafigi bilan almashish;
- IP, ATM, FR , X.25 trafigining tranziti;
- IP, ATM, FR, X.25 protokollari asosida virtual xususiy tarmoqlarni tashkil etish.

Bundan tashqari, ma’lumotlar uzatishga asoslangan xizmatlar mavjud:

- ajratilgan kanallar xizmatlari, N*64 Kbit/s, E1, E3 tezlikdagi raqamli kanallarni ijaraga berish;
- keng polosali videokonferensiyalarni tashkil etish xizmatlari;
- tele va radioeshittirish dasturlarini taqsimlash tarmog‘ini tashkil etish xizmatlari.

Oxirgi yillarda ma’lumotlar uzatish xizmatlarining eng ko‘p qo‘llaniladigani, IP protokoli bo‘yicha ma’lumotlar uzatish xizmati hisoblanadi. Bu xizmatlarning ko‘p

tarqalishi Internetning va uning asosida taqdim etiladigan xizmatlarning tarqalishi hisoblanadi (oxirgi foydalanuvchilar va Internet provayderlar resurslariga ulanish, elektron savdo xizmatlari va boshqalar). Biroq Internet xizmatlarining keng qo‘llanilishining oshishi, ushbu xizmatlarni yetkazib beradigan aloqa operatorlarining foydasi ko‘payishidan dalolat bermaydi va bu Internet xizmatlari yetkazib beradigan tariflarning narxlarini tushib ketishiga olib keladi. Bundan tashqari odatiy muammolar: aholidan kam foyda kelishi va hududiy kompaniyalarning noodatiy siyosati. Buning oqibatiga aholining katta qismi Internet xizmatlarining doimiy foydalanuvchilari bo‘lib hisoblanadilar.

Biroq Internet xizmatlari bozori yetarlicha istiqbollidir, shuning uchun Internet xizmatlarini taqdim etish, boshqa ma’lumotlar uzatish xizmatlarini taqdim etish bilan bir qatorda yagona multiservisli aloqa tarmog‘i asosida tashkil etilishi zarur.

## 3.2. Telekommunikatsiya xizmatlarining sifat aspektlari

**Xizmat sifati konsepsiyasi (Quality of Service, QoS).** Telekommunikatsiya xizmatlarining sifati bo‘yicha asosiy tushunchalarni ko‘rib chiqamiz. ITU-T I.112 tavsiyalarida, telekommunikatsiya xizmatlarining barcha majmuasi ikki turga bo‘lingan:

- ma’lumotlarni eltish (bo‘lib yetkazish) (Bearer Service, BS);
- aloqani taqdim etish (Teleservice, TS).

Service tushunchasi quyidagilarni qamrab oladi:

- har xil aloqa turlari (telefon, ma’lumotlarni uzatish, faksimil, xujjatlarni izlash va boshqalar);
- asosiy va qo‘shimcha xizmatlar;
- har xil kommutatsiyalash usullarini qo‘llagan holda ma’lumotlarni uzatish (kanalli kommutatsiya, paketli kommutatsiya va gibrid);
- turli uzatish muhitlarini taqdim etish (simli, optik tolali, radio va boshqalar);

- standart tezliklari bilan farqlanuvchi (64 Kbit/s, 384 Kbit/s, 2.048 Mbit/s dan kichik, teng yoki katta) turli kanal va traktlarni taqdim etish;

- ijaraga olingan, maxsus kelishilgan vaqt davomida, seans vaqtida resurslarni taqdim etish.

*Ma'lumotlarni yetkazish xizmati* (Bearer Service), "foydalanuvchi-tarmoq" interfeyslari orasida foydalanuvchilarga ma'lumotlarni hech qanday tahlilsiz va uning tarkibini qayta ishlamasdan shaffof holda uzatishni ta'minlaydi.

*Aloqani taqdim etish xizmati* (Teleservice), bu shunday xizmat turiki, terminal qurilmalar va tarmoq protokollarining xususiyatlarini hisobga olgan holda foydalanuvchilarni aloqaning barcha imkoniyatlari bilan ta'minlaydi.

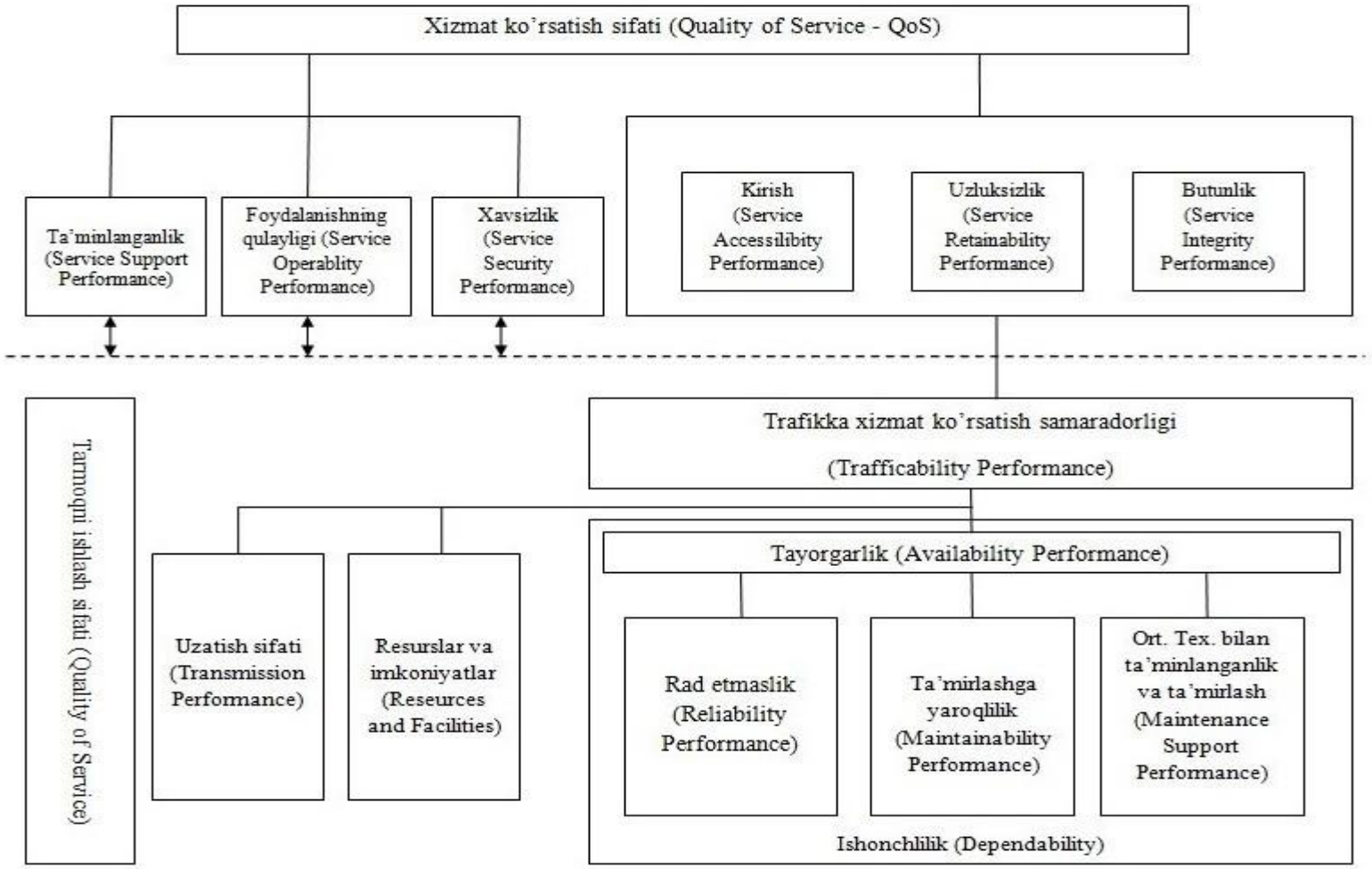
Mana shu ta'riflardan ko'rinib turibdiki, ma'lumotlarni taqdim etish xizmatlari, aloqani taqdim etish xizmatini tarkibiy qismi hisoblanadi.

Ma'lumotlarni eltish xizmatlari OTO'B modelining uchta quyi sathi funksiyasini, aloqani taqdim etish xizmatlari esa shu modelning yuqori sathining bir qismini yoki barcha yettita sathining vazifasini amalga oshiradi.

Kompyuter tarmoqlari va ma'lumotlar uzatish tarmoqlari uchun X seriyali tavsiyalarda (X.25, X.28, X.32, X.36) qo'shimcha (Supplementary) xizmatlar aniqlangan.

Telekommunikatsiya xizmatlari sohasidagi ierarxiya tushunchasi 3.1-rasmda keltirilgan (E.800 tavsiyasi). Xizmat ko'rsatish sifati amaliy natija, xavfsizlik, ta'minlanganlik va foydalanishga qulaylik tushunchalarini birlashtiradi.

Amaliy natijalar guruhi - ulanish, butunlilik va uzluksizlik bitta tushuncha bilan ifodalanadi - "foydalanish" (3.1-rasmning o'ng tarafidagi yuqori burchagida to'g'ri burchak bilan ajratilgan).




3.1-rasm. Xizmat ko'rsatish sifati sohasida va telekommunikatsiya tarmoqlarini ishlashi haqidagi tushunchaning ierarxiyasi

Xizmat ko‘rsatish sifati xuddi xususiyatlar majmuasi kabi ko‘riladi:

- ta’minlanganlik;
- foydalanishning qulayligi;
- xizmat ko‘rsatish xavfsizligi;
- xavfsizlik;
- ulanish;
- uzluksizlik;
- butunlik (tarmoq orqali transportlashda foydalanuvchi ma’lumotlarining mosligi) kiradi.

Foydalanish - xizmat ko‘rsatish xususiyati bo‘lib, har doim foydalanuvchiga zarur bo‘lgan seans vaqtida xizmatni taqdim etishdan iborat.

Foydalanish tushunchasining mohiyati quyidagicha aniqlanadi:

- kirish – xizmat ko‘rsatish xususiyati foydalanuvchiga zarur bo‘lganda har qanday joyda va lahzada taqdim etilishi kerak;

- butunlik - operatorning uzatish sifatini pasaytirmagan holda xizmatlarni taqdim etish qobiliyati;

- uzluksizlik - ma’lum bir ekspluatatsiya sharoitida, talab qilingan vaqt oralig‘i davomida, operatorning uzluksiz xizmat ko‘rsatishni taqdim etish xususiyati.

Xizmat ko‘rsatish sifatining qolgan uchta xususiyati quyidagi ta’riflar orqali ifodalanadi:

- ta’minlanganlik – foydalanuvchilar xizmatlarni qo‘llaganda aloqa operatorining xizmatlar majmuasini taqdim etishi va yordam berish qobiliyati;

- foydalanishning qulayligi - qo‘llashning soddaligidan iborat bo‘lgan xizmat ko‘rsatish xususiyati;

- xavfsizlik - bu xizmat ko‘rsatishning ruxsat etilmagan kirishlardan, yomon niyatlarda foydalanish va noto‘g‘ri foydalanish, ataylab (g‘arazli) buzish, tabiy ofatlar va insonlar xatosi kabilardan himoyalanganlik xususiyati.

Telekommunikatsiya tarmoqlarining ishlab turish sifati (Network Performance - NP), trafikka xizmat ko‘rsatish samaradorligini xarakterlaydi.

Telekommunikatsiya tarmoqlaridan foydalanuvchi odatda, telekommunikatsiya tarmoqlarining tuzilishi va zarur bo‘lgan xizmatlar qanday yetkazilishi bilan qiziqmaydi. Ayni shu paytda u shunga o‘xshagan xizmatlar bilan uni solishtirgan holda his qilib mazkur xizmat sifatini baholaydi.

Talablarni asoslash, foydalanuvchilarning kutishi va operatorning xarajatlarini optimallashtirish uchun quyidagilarni ta’minlash zarur:

- xizmatlar sifatiga tegishli bo‘lgan terminlarni qat’iy shakllantirish;

- kutish haqidagi ob’ektiv ma’lumotlarni, foydalanuvchi talablarini taqdim etish.

Xizmat ko‘rsatish sifati, “xizmat ko‘rsatish bilan foydalanuvchilarni qoniqqanlik darajasini aniqlovchi yig‘indi effekt” kabi ITU-T E.800 tavsiyasiga binoan aniqlangan.

Foydalanuvchi nuqtai nazaridan xizmat ko‘rsatish sifati, parametrlar majmui sifatida ifodalanishi mumkin. Bu parametrlar xizmat va foydalanuvchi terminlarida ham ifodalanadi va tarmoq tuzilishiga bog‘liq emas. Ular foydalanuvchi tomonidan qabul qilinadigan effektning afzalligiga mo‘ljallangan va foydalanuvchiga xizmatlar, xizmatlarga ulanishda (ITU-T I.350 tavsiyasi bo‘yicha) osongina obektiv o‘lchashni kafolatlashi lozim.

Tarmoq xarakteristikasi (NP), foydalanuvchilar orasida aloqani ta’minlash qobiliyati kabi aniqlanadi. NP deganda hisoblanishi va o‘lchanishi mumkin bo‘lgan parametrlar yig‘indisi tushuniladi. Tarmoq xarakteristikasi eng avvalo egasi tomonidan qo‘llaniladi. Ular tizimni ishlab chiqish, xalqaro yoki milliy darajada tarmoqni loyihalash, ekspluatatsiya qilish va texnik xizmat ko‘rsatishga mo‘ljallangan. Telekommunikatsiya tarmoqlari foydalanuvchilarga ma’lumotlarni yetkazish vazifasini amalga oshiradi.

3.1-jadvalda xizmat ko‘rsatish sifati va tarmoq xarakteristikasi orasidagi farq ko‘rsatilgan.

3.1- jadval

Xizmat ko‘rsatish sifati va tarmoq xarakteristikalari orasidagi farq

| Xizmat ko‘rsatish sifati (QoS) | Tarmoq xarakteristikalari (NP) |
|---|---|
| Foydalanuvchiga mo‘ljallangan | Tarmoq operatoriga mo‘ljallangan |
| Xizmatlarning xususiyatlarini tavsiflaydi | Ulanish elementlarining xususiyatlarini tavsiflaydi |
| Foydalanuvchi tomonidan qabul qilinadigan effektga mo‘ljallangan | Ishlab chiqish, loyihalash, ekspluatatsiya qilish va texnik xizmat ko‘rsatishga mo‘ljallangan. |
| Xizmatlarga ulanish nuqtalari orasida o‘lchanadi | Ulanish elementlarining imkoniyatlari va ikki tomonlama ulanishni tavsiflaydi |

Har bir xizmat xususiyatlar majmuasi bilan xarakterlanadi, ularning asosiylari xizmat ko‘rsatish sifatini aniqlaydi.

Tarmoq xarakteristikalari (parametrlari) foydalanuvchi qabul qiladigan xizmat ko‘rsatish sifatini aniqlaydi. Bunday tarmoq xarakteristikalariga trafik, chaqiriqlarning yo‘qolishi, aloqa yo‘nalishidagi samarali chaqiriqlar koeffitsienti va boshqalar misol bo‘lishi mumkin.

QoS va NP parametrlari orasida o‘zaro bog‘lanish bor. Tarmoq orqali foydalanuvchilarga samarali xizmat ko‘rsatish uchun ular orasidagi qiymatlarni mosligini o‘rnatish asosiydir. NP parametrlarini aniqlash, ulanish elementlari chegarasida kuzatish mumkin bo‘lgan hodisalarga va holatlarga asoslangan.

**Tarmoq xarakteristikasi konsepsiyasi.** Telekommunikatsiya tarmoqlarini ishlash sifati (Network Performance) – bu foydalanuvchilar orasida ma’lumotlar almashishni ta’minlash qobiliyatidir. Telekommunikatsiya tarmoqlarining asosiy xarakteristikasi – bu trafiklarga xizmat ko‘rsatish samaradorligidir (3.1-rasm).

Trafiklarga xizmat ko‘rsatish samaradorligi (o‘tkazuvchanlik qobiliyati), tarmoq ob’ekti kabi xizmat ko‘rsatish sifati va ma’lum bir texnik holatda (ishga qobiliyatli va qobiliyatli bo‘lmagan kanal/liniyalarning miqdoriy munosabati) ma’lum bir jadallik bilan tushayotgan trafiklarga xizmat ko‘rsatuvchi kommutatsiyalash tugunlarining xususiyatidir.

Kommutatsiyalash tugunining qobiliyati trafikga xizmat ko‘rsatishdan iborat. U trafikning ishonchliligi, uzatish sifati, ega bo‘lgan resurslari va imkoniyatlariga bog‘liq.

*Uzatish sifati* - bu tayyorgarlik holatida bo‘lgan tarmoq ob’ektining qabul qiluvchi punktida signalni qayta tiklash sathidir.

*Tarmoq resursi* deganda - kommutatsiyalash, marshrutlash, qayta qabul qilish, tarmoq ob’ektida ma’lumotni saqlash, rasmiyatchilik (bu tushuncha ITU-T tavsiyasida hali aniqlanmagan va aniqlashtirilmagan).

*Ishonchlilik* - umumlashtirilgan termin bo‘lib, tayyorgarlik xususiyatini, rad etmasdan ishlash xususiyatini, ta’mirlashga yaroqlilik, texnik xizmat ko‘rsatishni va ta’mirlashni tavsiflashda qo‘llaniladi.

*Tayyorgarlik* - tarmoq ob’ektining ixtiyoriy vaqt lahzalarida (rejalashtirilgan davrdan tashqari, bu davrda tavsiyaga ko‘ra ob’ektni qo‘llash ko‘rib chiqilmaydi) trafikni qayta ishlash va shu lahzadan boshlab berilgan vaqt oralig‘ida rad etmasdan ishlash qobiliyati.

*Rad etmasdan ishlash* - ob’ektning, berilgan vaqt davomida ishga qobiliyatliligini uzluksiz saqlash qobiliyati.

*Ishga yaroqlilik* - tarmoq ob’ektining xususiyati bo‘lib, ogohlantirishga moslashganlik va rad etish sabablarini aniqlash, texnik xizmat ko‘rsatish va ta’mirlashni o‘tkazish yo‘li bilan ishga yaroqlilik qobiliyatini qayta tiklashdan iborat.

*Texnik xizmat ko‘rsatish va ta’mirlashni ta’minlash* – tarmoq ob’ektlariga texnik xizmat ko‘rsatish uchun xizmat operatorining vositalarni ta’minlash qobiliyati

(belgilangan ekspluatatsiya sharoitlarida va qabul qilingan texnik xizmat ko‘rsatish usulida).

Xususiyatning har biri xarakteristikalar majmuasi bilan tavsiflanishi mumkin (ko‘rsatkichlar, atributlar). Masalan, xizmat ko‘rsatishga tayyorgarlik quyidagi xarakteristikalar bilan aniqlanadi: tarqalish muhitlari, qurilmaning ishga qobiliyatliligi, stansiyaning va tarmoq uzellarining o‘tkazuvchanlik qobiliyati.

ITU-T E.862 (1992 y.) tavsiyalarida texnik vositalarning rad etishi bilan bog‘liq bo‘lgan operatorning va foydalanuvchining iqtisodiy yo‘qotishlarini (rejalashtirishda, loyihalashtirishda, ekspluatatsiyada va telekommunikatsiya tarmoqlariga texnik xizmat ko‘rsatishda) hisobga olish mumkin bo‘lgan yondashishlar keltirilgan.

Tarmoq operatorlari, bozor sharoitida ishlagan holda, rad etishlar tufayli mumkin bo‘lgan yo‘qotishlarni baholash va o‘zining texnik vositalarining ishonchliligini oshirishga ketadigan xarajatlar bilan ularni qiyoslashga qiziqadi. Har bir xarakteristika bir yoki bir necha hodisalar, holatlar yoki ta’sirlar bilan bog‘liq.

Xizmat ko‘rsatish sifati va tarmoqning ishlash xarakteristikalarining (atributlarni) barcha yig‘indisi ikkita kategoriyaga bo‘linadi:

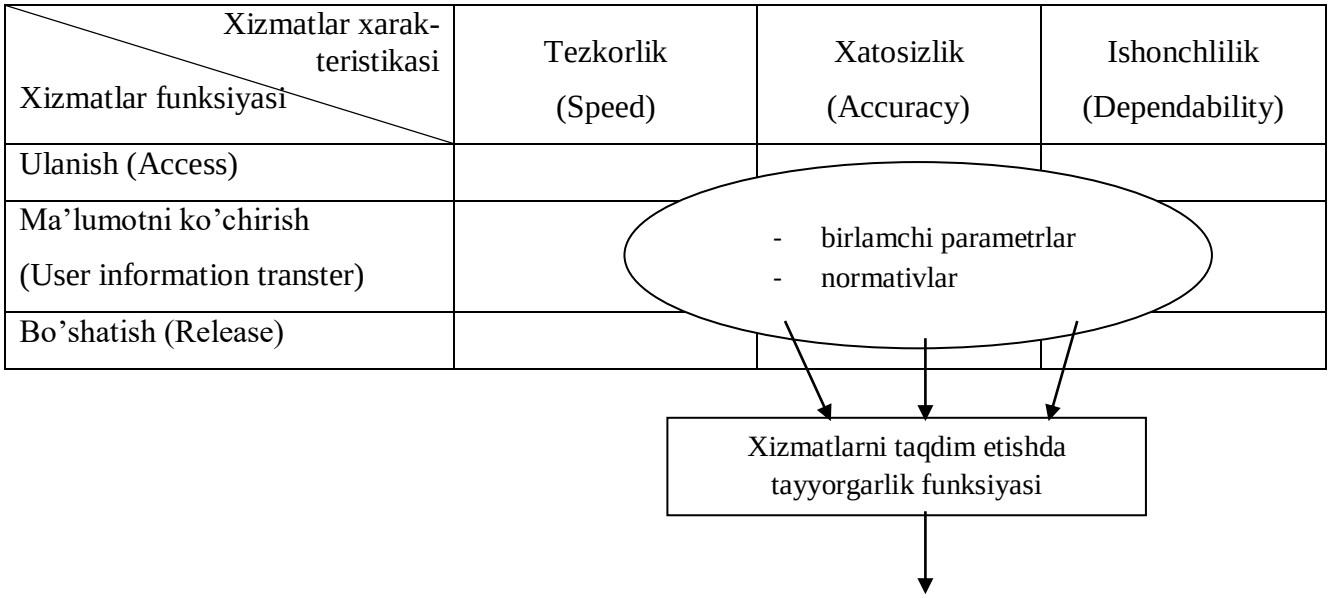
- birlamchi, xizmatga ulanish nuqtasida to‘g‘ri kuzatish yo‘li bilan aniqlanadigan va vaqtning ma’lum bir lahzalariga tegishli bo‘lgan (masalan, stansiyadan javobning kechikishi);
- keltirib chiqilgan, bir yoki bir necha birlamchi atributlarga yoki ayrim vaqt intervaliga yaqinlashtirishga asoslangan holda aniqlanadigan (masalan, tayyorgarlik koeffitsienti).

ITU-T I.350 tavsiyasida tarmoqda va uning xizmatida qo‘llaniladigan uchta funksiya va har bir funksiyada uchta xarakteristika aniqlangan. Xuddi shu tarzda to‘qqizta birlamchi parametr (“matritsa 3x3”) olingan. Ular QoS va NP spetsifik parametrlarni aniqlash uchun qo‘llaniladi (3.2-rasm):

- tezlik bilan ulanish;

- xatosiz ulanish;
- ulanishning ishonchliligi (resursga ulanishda rad etish ehtimolligi);
- ma’lumotlarni ko‘chirishning tezkorligi;
- ma’lumotlarni xatosiz ko‘chirish;
- ma’lumotlarni ko‘chirishning ishonchliligi;
- bo‘shatishning tezkorligi;
- bo‘shatishning xatosizligi;
- bo‘shatishning ishonchliligi.

Tarmoq xizmati aloqaning ikki funksiyasini qo‘llaydi (3.2-rasm): xizmat resursiga foydalanuvchilarni ulanishini ta’minlash, o‘rnatilgan ulanish bo‘yicha ma’lumotlarni ko‘chirish masalasini hal etadi va aloqa seansi tugaganidan keyin oldin taqdim etilgan resurslarni bo‘shatish. Ulanish deganda xizmatlar resurslarini olishga bo‘lgan imkon tushuniladi.




Ketma – ket vaqt lahzalari davomida tayyorgarlik holati

3.2-rasm. Tayyorgarlik holatini aniqlash uchun 3x3 matritsali usul

Ulanish jarayoni, “foydalanuvchi-tarmoq” interfeysida foydalanuvchidan so‘rov paydo bo‘lgan lahzadan boshlanadi va uning terminalida bir bitgina paydo bo‘lishi bilan tugaydi.

Foydalanuvchilarning ma’lumotlarini ko‘chirish jarayoni, ulanish tugagan lahzadan harakatga tushadi va aloqa seansi tugashidan darak bo‘lganda bo‘shatish so‘rovini uzatish lahzasida tugaydi.

Bo‘shatish jarayoni, bo‘shatish so‘rovi signali uzatish lahzasida amalga oshadi va har bir foydalanuvchi uchun aloqa seansi vaqtida ajratilgan xizmatlar resurslari bo‘shagandan keyin tugaydi.

Bo‘shatish jarayoni, xuddi bog‘lanish kabi oldingi mavjud ulanishni buzish va yuqori sath protokollarining ishini tugatilishi bilan bog‘liq.

Xizmatlar funksiyasini qo‘llashda xizmat sifati uchta parametr bilan tavsiflanadi: tezkorlik (tezlik), xatosizlik (aniqlik), ishonchlilik.

Tezkorlik, vazifani bajarish uchun zarur bo‘lgan vaqt oralig‘ini yoki bajarish tezligini xarakterlaydi.

Xatosizlik, vazifani bajarilishini to‘g‘riligining darajasini xarakterlaydi.

Ishonchlilik, ma’lum bir berilgan kuzatish vaqti oralig‘ida vazifani bajarishda ishonchlilik darajasini aniqlaydi (bajarish tezkorligi va xatosizligiga bog‘liq bo‘lmagan holda).

Xizmatlar sifatining har bir birlamchi parametri uchun me’yorlar o‘rnatilgan bo‘lishi kerak. Bu me’yorlar orqali xizmatlarni taqdim etish jarayonida o‘lchangan qiymatlarni solishtirish mumkin bo‘lishi kerak.

## 3.3. Xizmat ko‘rsatish sathi haqida kelishuv

Xizmat ko‘rsatish sathi haqida kelishuv (Service Level Agreements, SLA), telekommunikatsiya xizmatlari bozorida raqobatbardoshlik kuchaygan sharoitda mijozlarni jalb etish va saqlab qolish uchun juda kuchli vosita hisoblanadi.

Foydalanuvchilarning so‘rovidan aniqlanishi bo’yicha, bunday kelishuvning natijaviy imkoniyatlari ta’minlovchining xizmatlarini tanlashda muhim omillardan biridir. Qisqa qilib aytganda SLAning ma’nosi shundan iboratki, xizmatlarni ta’minlovchi va mijozlar orasidagi shartnomada, ta’minlovchi tomonidan bajarilishi kafolatlanadigan xizmat ko‘rsatish sifatiga (Quality of Service, QoS) bo‘lgan ma’lum bir talablar o‘rnatiladi.

Agar shu kafolatlar bajarilmasa, xizmatlarni ta’minlovchiga nisbatan jarima solinadi. Boshqa tomondan, kafolatlangan sifatni bergan ta’minlovchi o‘zining xizmatlarining narxini oshirish imkoniga ega bo‘ladi.

**Xalqaro tashkilotlar xujjatlari va ta’riflar.** Xizmat ko‘rsatish sathi bo‘yicha kelishuv xalqaro tashkilotlarning bir qator xujjatlarida ko‘rib chiqiladi:

- ITU-T (XEAI-T) E.860 tavsiyasi, “Framework of a Service Level Agreement”, 2002y. va E.801 “Framework for Service Quality Agreement”,1996 y.;
- ETSI - qo‘llanmasi EG. 202 009-3 “User Group; Quality of telecom services; Part 3: Template for Service Level Agreements (SLA)”, 2002 y.;
- Frame Relay Forum - FRF. 13 “Service Level Definitions Implementation Agreement”, 1998 y.; TeleManagement Forum (TMF) - GB917 “SLA Management Handbook”, 2001 y.

Bu ro‘yxatlarning ichida eng birinchi ITU-T E.801 yaratilgan. Unga “Xizmat ko‘rsatish sathi haqida kelishuv” (Service Quality Agreement, SQA) kiritilgan va u o‘zaro bog‘langan operatorlar yoki xizmatlarni ta’minlovchilar orasida, oxirgi foydalanuvchilar va boshqa talabgorlarni qoniqtirish uchun monitoringning rasmiy dasturlarini kiritish, o‘lchash va me’yorlarni o‘rnatish haqida.

Frame Relay Forum o‘zining FRF.13 tavsilotli ro‘yxatida, kadrlarni retranslyatsiya xizmati sifat parametrlarini o‘rnatdi va bu parametrlar SLA da qo‘llanilishi mumkin. Rasman bu xalqaro xujjatlarda birinchi marta ko‘rsatib o‘tilgan. So‘ngra TMF GB917 ma’lumotnomasida va ITU-T E.860 tavsiyasi ishlab chiqildi.

E.860 tavsiyasida xizmat ko‘rsatish sifati haqida yangi tushunchalar yuzaga keldi (SQA, boshqa nomi QoS Agreement): hozirda u xizmat ko‘rsatish sifatiga tegishli bo‘lgan SLA ning qismi kabi qaraladi. Shuning uchun ham E.860 tavsiyasida bu ta’rif aniqlashtirilgan va QoS deb atalgan. QoS - bu ta’minlovchidan foydalanuvchiga taqdim etilgan xizmat ko‘rsatish darajasiga moslik va ular orasidagi kelishuv.

Differensiallashgan xizmatlar (Differentiated Services, DiffServ) modelida qo‘llaniladigan yana bir yaqin tushuncha bor, IETF – tavsilotli ro‘yxatidagi xizmat ko‘rsatish sathi (Service Level Specification, SLS).

Birgalikda xizmat ko‘rsatishni aniqlaydigan bu parametrlar majmuasi va ularning qiymati, DiffServ domenida trafiklar oqimiga taqdim etiladi. DiffServ modelida QoS ni ta’minlash uchun qo‘llaniladigan SLS, SLAning bir qismi bo‘lishi mukin.

## 3.4. Oxirgi foydalanuvchilar oldida yagona javobgarlik

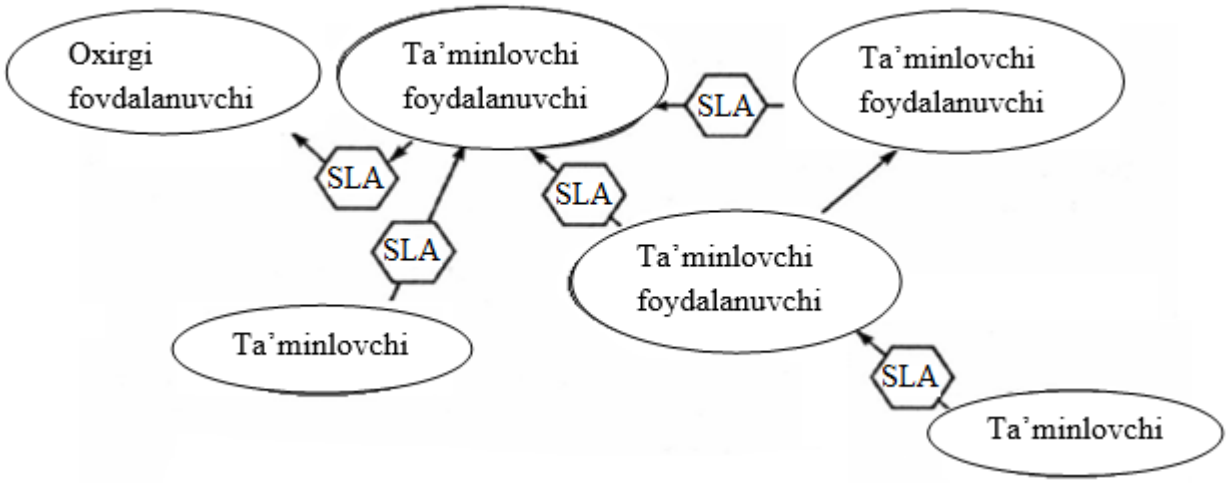
Mijozlar bilan o‘zaro bog‘lanishdan tashqari, u chekkadan bu chekkaga xizmatlarni taqdim etishda qatnashadigan xizmatlarni ta’minlovchilar orasidagi o‘zaro bog‘lanish ham muhim ahamiyatga ega bo‘lishi mumkin.

Bir necha ta’minlovchilar mavjud bo‘lgan holda xizmat ko‘rsatish sifatini ta’minlash juda murakkab bo‘lib qoladi. Bu muammoni yechishga oxirgi foydalanuvchi oldida yagona javobgarlik (one-stop responsibility) deb ataluvchi tushuncha yordam beradi. Boshqa ta’minlovchilarning xizmatlarini qo‘llash 3.3-rasmda ko‘rsatilgan.

**SLA ning xarakteri va tuzilishi.** Amalda qo‘llaniladigan SLA turlicha va doimiy emas. SLA ning xarakteristikalarini aniqlovchi asosiy omillarga quyidagilar kiradi:

- taqdim etiladigan xizmat turlari;

- xizmatlarni ta’minlovchida mavjud bo‘lgan texnik baza;
- foydalanuvchilarning talabi;
- sheriklarning muomalasi;
- raqiblarning xulq atvori.




3.3-rasm. Yagona javobgarlik prinsipini qo‘llash

Normativ xujjatlarning umumlashgan tavsiyasi va amaliy tajribalar, SLA ning quyidagi tarkibini tavsiya etishi mumkin:

- taqdim etiladigan xizmatlar tavsifi;
- sifat ko‘rsatkichlari va ular uchun me’yorlar;
- nazorat usullari va vositalari;
- foydalanuvchining shikoyatini qayta ishlash jarayoni;
- jarima sanksiyasi;
- xizmatlarni ta’minlovchilarning javobgarligini chegaralanganligi;
- hisobot;
- o‘lchash jarayonini kiritish;
- qo‘shimcha sharoitlar (sir saqlanishi, uni himoya qilishga javobgarlik va boshqalar).

**Xizmat ko‘rsatishning sifat ko‘rsatkichlarini tanlash va ular uchun normativlar.** SLA da markaziy o‘rinni xizmat ko‘rsatishning sifat ko‘rsatkichlari va ular uchun xizmat ko‘rsatish sathining me’yorlari deb ataluvchi me’yorlar (Service Level Objectives, SLO) egallaydi.

Bu yerda, SLA doirasida ta’minlanishi mumkin bo‘lgan, xizmat ko‘rsatish sathini aniqlovchi, ta’minlovchi va xizmatlar istemolchisi orasida kelishilgan sifat ko‘rsatkichlarining chegara qiymatlari nazarda tutilgan.

Xizmat ko‘rsatishning sifat ko‘rsatkichlari SLA bilan birgalikda ikki kategoriyaga bo‘linadi:

- maxsus - xizmatga yoki texnologiyaga bog‘liq bo‘lgan;
- umumiy - xizmatga yoki texnologiyaga bog‘liq bo‘lmagan.

Sifat ko‘rsatkichlari, ITU-T tavsiyasiga mos keluvchi xizmatlar yoki tarmoq turi va boshqa xalqaro tashkilot xujjatlari uchun o‘rnatilgan bo‘lsa maxsus hisoblanadi. Masalan, raqamli kanallarni ijaraga berishda bu tavsiya ITU-T G.82x seriyasi, ATM uchun ITU-T I.356 tavsiyasi va ATM Foruma Aftm-0056.000 tavsilotlar ro‘yxati, Frame Relay uchun ITU-T X.144-X.146 tavsiyalari va Frame Relay Foruma FRF.13 tavsilotlar ro‘yxati, IP uchun ITU-T Y.1540 va Y.1541 tavsiyalari shular jumlasiga kiradi.

Umumiy ko‘rsatkichlar sifatida odatda ishonchlilik (tayyorgarlik va ishga yaroqlilik) ko‘rsatkichlari qo‘llaniladi, shuningdek SLA da eng ko‘p tayyorgarlik ko‘rsatkichlari qo‘llaniladi. ITU-T E.800 tavsiyasiga binoan ishonchlilik xizmat ko‘rsatish sifatiga ta’sir ko‘rsatuvchi eng muhim omillardan biri hisoblanadi. Ishonchlilik konsepsiyasining markaziy o‘rnini tayyorgarlik (availability) egallaydi.

Bu, “Texnikada ishonchlilik. Ishonchlilik bo‘yicha talablarga berilgan umumiy qoidalar va tarkib” DAST 27.003-90 (davlat standarti) holatiga mos keladi va uzluksiz bog‘langan qayta tiklanadigan ob’ektlar uchun asosiy ishonchlilik ko‘rsatkichi hisoblanadi. Qoida bo‘yicha aloqa vositalari xuddi shunday ob’ekt hisoblanadi. SLA da qo‘llaniladigan tayyorgarlik ko‘rsatkichlarining turlari 3.2-

jadvalda keltirilgan. Tayyorgarlik koeffitsienti asosan muxandislik ishlarida hisoblashlar, solishtirishlar va e'lonlar uchun qulay.

3.2-jadval

Tayyorgarlik ko'rsatkichlarining turlari

| Ko'rsatkich | Formulalarni qayta hisoblash | Topshiriq namunasi |
|---|---|---|
| Tayyorgarlik koeffitsienti ($K_t$) | $K_t = 1-K_o = T-t_{n\Sigma}/T$ | 0,999 yoki 99,9% |
| Turib qolish koeffitsienti ($K_{t.q.}$) | $K_{t.q.} = 1-K_t = t_{n\Sigma}/T$ | 0,001 yoki 0,1% |
| Berilgan vaqt oralig'ida (T) turib qolish vaqtining o'rtacha yig'indisi ($t_n$) | $t_{n\Sigma} = K_{t.q.}T = (1-K_t)T$ | 8,76 soat bir yilda |

Biroq SLA da o'xshash vazifalarni tekshirish bir qator muammolarni tug'diradi. Agar shartlangan vaqt oralig'ida turib qolishning yig'indi vaqti me'yordan oshib ketmasa, unda talab bajariladi, agar oshib ketsa talab buziladi.

Shuningdek SLA da sutkaning 24 soatida, xaftaning 7 kunida va yilning 365 kunida qayta tiklanish vaqti kafolatlanadimi yoki bu faqat ishchi kuniga va soatiga taalluqliligi kelishiladi.

Ayrim hollarda turib qolishning davomiyligini chegaralanganligi o'rtacha tiklanish vaqtini qo'llashni taklif etadi, lekin bu ko'rsatkich murakkab kamchilikka ega. Odatda ko'pgina o'rtacha xarakteristikalar, turib qolishning davomiyligi juda ko'p qisqa sonlarning kompensatsiyalangani bo'lishi mumkin.

## 3.5. Zamonaviy multimediali ilovalar

Internet tarmoqlarida IP ustidan so'zlashuvni uzatish xizmati bilan bir qatorda, o'zining tarkibiga video, audio, matn, grafika va ma'lumotlarni kirituvchi

multimediali trafikni uzatish xizmatlari rivojlanib bormoqda. Bu texnologiyalarning yig‘indisi IP-telefoniya terminini yangi terminga o‘zgartirishga olib keldi.

*IP-kommunikatsiya.* Hozirgi kunda VoIP – texnologiyasi taxminan qayd etilgan telefon tarmoqlaridan 20% trafikni olish imkoniga ega bo‘ldi va ananaviy telefoniyada jiddiy raqobat sifatida ko‘riladi.

Rivojlanish boshidagi boshqa texnologiya – IPTV, operatorlarga istiqbolli multiservisli xizmatlarni taqdim etish imkoniga ega, ya’ni birinchi navbatda turli raqamli kontentga talablar bo‘yicha ulanish imkoniyati bilan bog‘langan.

So‘zlashuvni uzatish uchun IP tarmoqni qo‘llashning xususiyati shu bilan bog‘langanki, IP infrastrukturasi so‘zlashuv va signalli paketlarni VoIP tizimi elementlariga kafolatli yetkazishi kerak. Tarmoq, so‘zlashuv trafigi va ma’lumotlar trafigini turli usullarda qayta ishlashi kerak. Agar IP tarmoqda ikkala turdagi trafik uzatilsa, so‘zlashuv trafigiga ustunlik bo‘yicha xizmat ko‘rsatishni ta’minlash zarur. VoIP tarmog‘i va telefon tarmog‘i komponentlari orasida ma’lum bir moslik mavjud, biroq yetarli darajada katta farqga ega. Umum foydalanish telefon tarmoqlarida har bir aloqa seansida, kafolatlangan o‘tkazish oralig‘i bilan kanallarni ajratuvchi kanallarni kommutatsiyalash prinsipi qo‘llaniladi. IP tarmoqlarda, asosida statik zichlashtirish imkoniyati bo‘lgan paketlar kommutatsiyasi qo‘llaniladi. Xizmat ko‘rsatish sinfi tushunchasini kiritish shuki, aniq ilovalarga tegishli paketlar berilgan ustunlikka ega. Ustunlikli tizimni kiritish haqiqiy vaqtdagi ilovalar uchun talab etiladi, ya’ni so‘zlashuv trafigiga boshqa turdagi trafik ta’sir ko‘rsatmasligini kafolatlash uchun.

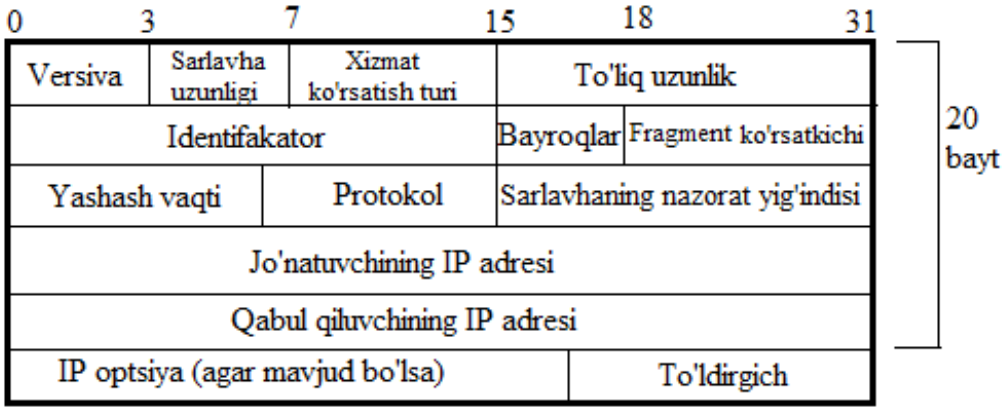
### 3.5.1. IPv4 va IPv6 sarlavhalarining tuzilishi

**IPv4 datagramma sarlavhasining tuzilishi.**

Foydali yuklamani tashuvchi IPning barcha datagrammasi o‘zining tarkibiga sarlavha va ma’lumotlarni kiritadi. 3.4-rasmda 4-turga mos keluvchi IP

datagrammasining sarlavhasi ko‘rsatilgan. 4-turni birinchi amalga oshirilgani 1980-yillar boshiga taalluqli va bu tur hozirgi kunda keng tarqalgan.

Sarlavha turli qo‘shimcha opsiyalarni ta’minlovchi 4 ta baytgacha qo‘shish yo‘li bilan kengaytirish imkoniyatiga ega bo’lgan kamida 20 baytdan iborat. Sarlavhani qulayligi uchun har biri 4 baytdan iborat bo‘lgan qatorlar to‘plami ko‘rinishida ifodalangan. Bunday maydonlarning umumiy soni 5 yoki 6 ga teng.




3.4-rasm. IP datagramma sarlavhasining fragmenti (IPv4 turi)

“Versiya” maydoni 4 bit, IP-sarlavhasini identifikatsiyalaydi. “Sarlavha uzunligi” maydoni sarlavha o‘lchamini aniqlaydi (20 yoki 24 bayt). “Xizmat ko‘rsatish turi” (Type of Service, ToS) maydoni 8 bitdan iborat. Birinchi 3 ta bit datagrammani ustunligini aniqlaydi (000 – ustunliksiz, 111 – ustunlikga ega). Keyingi uchta bit minimal ushlanib qolish, yuqori o‘tkazish qobiliyati va yuqori ishonchlilikni (har bir bit birga teng) aniqlaydi. Oxirgi ikkita bit qo‘llanilmaydi. Shuni aytish kerakki, 1990-yillarda Internet tarmoqlarida ToS maydoni qo‘llanilmagan.

“To‘liq uzunlik” maydoni 16 bit, datagrammani to‘liq uzunligini baytlarda aniqlaydi, ya’ni paketda uzatiladigan sarlavha va ma’lumotlar kiradi. Maydon uzunligi 16 bitga teng, datagrammaning maksimal uzunligi $2^{16}$-1=65535 baytga teng. Qochonki marshrutizatorlar to‘liq o‘lchamdagi datagrammaga ishlov bera olmasa,

uning uzunligiga bog‘liq holda datagramma bloklarga (fragmentlarga) bo‘linishi mumkin.

“Identifikator”, “Bayroq” va “Fragment ko‘rsatkichi” maydonlari qabul qilish oxirida fragmentlardan datagrammani qayta tiklashda qo‘llaniladi.

“Identifikator” maydoni 16 bit, belgilangan punktda fragmentdan datagrammani qayta tiklash imkonini beradi.

“Bayroq” maydoni 3 bit, qabul qilish oxirida datagrammani qayta tiklash uchun qo‘llaniladi. “Fragment ko‘rsatkichi” maydoni 13 bit, berilgan datagramma boshlanishiga nisbatan fragmentni siljishini aniqlaydi.

“Yashash vaqti” maydoni 8 bit, tarmoqda datagrammani mavjud bo‘lish davomiyligini chegaraviy vaqtini aniqlaydi.

Sakkiz bitli “Protokol” maydoni transport sathda qo‘llaniladigan protokolni aniqlaydi.

“Sarlavhani nazorat yig‘indisi” maydoni 16 bit, siklik kod yordamida sarlavhada (butun datagrammada emas, faqat sarlavhada) xatolikni nazorat qilish uchun mo‘ljallangan. Bu tekshirish har bir marshrutizator orqali datagramma yoki uning fragmenti o‘tganda amalga oshiriladi.

Keyingi 2 ta maydon jo‘natuvchi va qabul qiluvchining adreslari uchun mo‘ljallangan.

“Opsiya” maydoni, maksimum 4 bayt, turli vazifali testlashtirish va nazoratni kiritish uchun qo‘llaniladi.

“To‘ldirgich” maydoni “Opsiya” qatorini 32 bit to‘liq uzunligigacha to‘ldirish uchun qo‘llaniladi.

Datagramma va datagramma fragmetlarini uzatganda tarmoq uzellarida tushib qolishi yoki yo‘qolishi mumkin, yoki alohida fragmentlarning katta kechikishi tufayli datagrammalarni qabul qilish joyida uni yig‘ish jaroyonida yo‘qolishi mumkin. Shu tarzda 4-tur qo‘llanilganda IP rejim xizmat ko‘rsatish sifatini minimal sathini ta’minlaydi.

Biroq, hozirgi vaqtda IP-tarmoqlarda turli ko‘rinishdagi trafiklar uzatilmoqda, shu navbatda haqiqiy vaqtdagi interaktiv trafik kechikishlarga (IP ustidan so‘zlashuv, videokonferensiya, interaktiv o‘yinlar va boshqalar), shuningdek, ishonchlilikka, ruxsatsiz ulanishdan axborotni himoyalash va boshqalarga sezgir. Bu talablar Internet tarmoqlari uchun yangi protokollarni ishlab chiqishga olib keldi va bu kamchiliklarni bartaraf etish maqsadida IPv6 protokoli ishlab chiqildi.

**IPv6 datagramma sarlavhasining tuzilishi.**

90-yillar oxiridan boshlab Internetni jadal rivojlanish jarayoni boshlandi. Bu sharoitlarda abonentlar va turli qurilmalarni adresli muhitni qo‘llashi Internetni tarqalishini chegaralaydi.

Internet tarmog‘i rivojlanishi uchun adresli muhitga ulanishni oshirish zarur. Bu esa IP protokolini yangi IPv6 turini ishlab chiqilishiga olib keldi. Biroq yangi turni ishlab chiqishda adreslar muammosidan tashqari 4-turning bir qator kamchiliklari hisobga olindi.

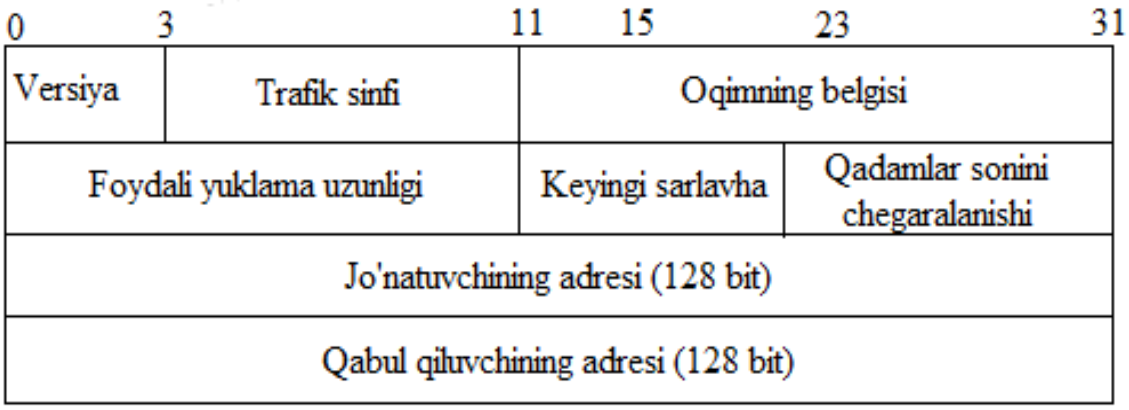
Sarlavha tuzilishi asosida olingan mukammallashgan IPv6 protokolning asosiy xususiyatlari quyidagilar hisoblanadi;

- ulanishli IP adreslar sonini oshirishni va ularning konfiguratsiya jarayonini soddalashtirishni ta’minlaydigan adres maydonining yangi o‘lchamini kiritish;

- xizmat ko‘rsatishning kafolatli sifatini ta’minlovchi mexanizmlarni ishlab chiqish;

- axborotni himoyalash va audentifikatsiya vositalarini qo‘llash imkoniyati.

3.5-rasmdan ko‘rinib turibdiki, IPv6 sarlavhasining uzunligi 40 baytga teng, bu 4-turga qaraganda ikki baravar katta. Birinchi 2 ta qator (8 bayt) nazorat vazifasini ta’minlaydi va bu 2 ta qatorning tuzilishi IPv4 sarlavhasining adresli qismining ustida joylashgan qator tuzilishidan farq qiladi.




3.5-rasm. IPv6 datagramma sarlavhasining formati

“Versiya” maydoni 4 bit, paket IPv6 sarlavhasiga egaligini ko‘rsatadi.

“Trafik sinfi” maydoni 8 bit va “Oqim belgisi” maydoni 20 bit, aniq manba adreslari jufti va belgilangan punkt uchun xizmat ko‘rsatish sifatining dastlabki belgilangan sathini aniqlaydi.

Internetda xizmat ko‘rsatish sifati tarmoqning o‘tkazish qobiliyati, paketlarni kechikishi va djitter, shuningdek paketlarni yo‘qolishi orqali aniqlanadi.

“Foydali yuklama maydoni uzunligi” maydoni 2 bayt, sarlavha uzunligidan tashqari baytlarda paket uzunligini aniqlaydi. Shuningdek maydon uzunligi 16-bitga va paketning maksimal uzunligi $2^{16}$-1=65535 baytga teng.

“Keyingi sarlavha” maydoni 8 bit, IPv6 asosiy sarlavhasidan keyingi keluvchi qo‘shimcha sarlavhalar turini aniqlaydi. Qo‘shimcha sarlavhalar joylashgan maydon, IP sarlavhasi, TCP va UDP sarlavhalari orasiga joylashtiriladi. Qo‘shimcha sarlavhalar o‘ziga katta funksiyalar yig‘indisini kiritadi, ular marshrutlash, fragmentlash, axborot xavfsizligi, autentifikatsiyadir.

“Qadamlar sonini chegaralash” maydoni 8 bit, 4-turdagi “Yashash vaqti” maydonining vazifalarini bajaradi.

Jo‘natuvchi va qabul qiluvchilarning adreslari har biri 16 baytga ega (128 bayt) ya’ni 4-turga qaraganda 4 marta ortiq.

IPv6 protokolni kiritish bilan bog‘liq ishlar 10 yildan ko‘p vaqt davomida olib borilishiga qaramay, IP tarmoqlarda apparat-dasturiy modulning asosiy qismini 4-turning IP protokoli amalga oshiradi. Bu bilan bog‘liq holda, IPv6 yangi tur protokollar oilasiga o‘tishda muammolar yuzaga keladi.

### 3.5.2. VoIP – texnologiyasi

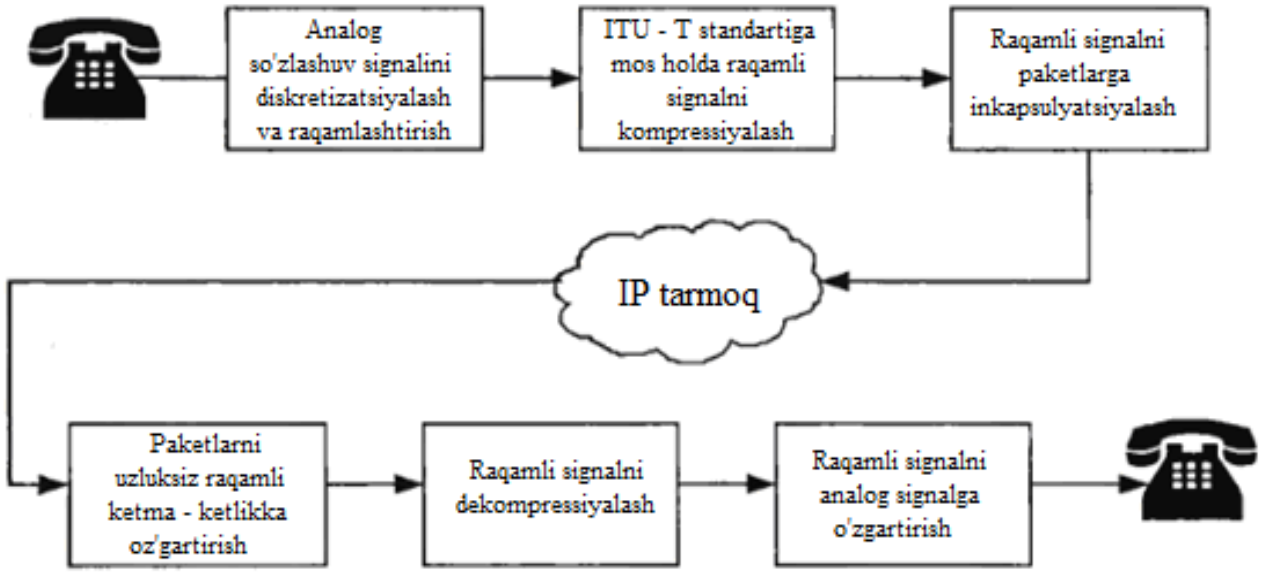
IP tarmoq orqali so‘zlashuv signalini uzatish tizimi arxitekturasiga o‘tishdan avval, VoIP texnologiyasida amalga oshiriladigan asosiy jarayonlarni ko‘rib chiqamiz. VoIP tizimi so‘zlashuv signaliga nisbatan, oddiy telefon tarmoqlari singari vazifalarni bajarishi kerak. Bu asosiy vazifalarga quyidagilar kiradi:

- *uzatuvchi tomonda* - analog signalni raqamli signalga o‘zgartirish va raqamli signalni tarmoq orqali uzatish uchun zarur bo‘lgan ko‘rinishda taqdim etish (IP tarmoq orqali); so‘zlashuv signali IP protokoli paketlariga inkapsulyatsiyalanadi;
- *IP tarmoqda* - telefonli chaqiriqqa xizmat ko‘rsatishni boshqarish (ulanishni yaratish, so‘zlashuv almashishni ta’minlash, uzish) va paketlarni transportlash;
- *qabul qilish qismda* - qabul qilingan paketlardan va diskret signaldan analog so‘zlashuv signalini qayta tiklash.

3.6-rasmda so‘zlashuv signali IP tarmoq orqali o‘tgandagi qayta ishlash jarayoni keltirilgan. Bu yerda bloklar ko‘rinishida yuqorida sanab o‘tilgan vazifalar keltirilgan - kodlash, IP paketlar ko‘rinishida ifodalash, tarmoq orqali paketlarni uzatish, paketlarni taqsimlash va analog so‘zlashuv signalini qayta tiklash.

Chaqiriqqa (ulanish, so‘zlashuv almashishni ta’minlash va uzish) xizmat ko‘rsatishni boshqarish. VoIP texnologiyasida telefon aloqasiga aynan o‘xshashi bo‘yicha abonentlar orasida ulanishni o‘rnatish zarur. Bu signalizatsiya tizimi bilan amalga oshiriladi, ya’ni terminal qurilma yordamida tarmoqda aloqa bo‘ladi, ya’ni chaqiriqqa xizmat ko‘rsatish uchun zarur bo‘lgan tarmoq elementlari ishini

koordinatsiyalaydi va faollashtiradi. VoIP tarmoqda signalizatsiyani, tarmoq komponentlari orasida IP datagrammalarni almashishi ta’minlaydi.




3.6-rasm. VoIP tarmog‘i orqali so‘zlashuv signalini uzatishda ishlov berish

Ulanish 2 ta oxirgi punktlar orasida o‘rnatiladi. Bu punktlarning identifikatsiyasi maxsus ma’lumotlar bazasi orqali ishlab chiqiladi. UFT tarmog‘i singari oxirgi punktni identifikatsiyalash uchun telefon nomerlari qo‘llaniladi. VoIP tarmog‘ida ham buning uchun ma’lumotlar bazasida saqlanuvchi IP-adres qo‘llaniladi. VoIP datagrammasini transportlash, IP marshrutizatorlarida so‘zlashuv paketlarini ketma-ket qabul qilish yo‘li orqali bajariladi.

### 3.5.3. IPTV texnologiyasining asosiy xususiyatlari

IPTV texnologiyasi - interaktiv rejimda va eshittirish rejimida IP tarmoqlari bazasida multimediali xizmatlarni (TV, audio/video, matn) yetkazish texnologiyasini o‘zida namoyish etadi.

IPTV texnologiyasi quyidagi asosiy xususiyatlar bilan xarakterlanadi:

- Interaktiv TV. IPTV imkoniyatlari, ikki tomonlama uzatishni ta’minlash, Operator-Provayderga interaktiv ilovalarning keng spektrida xizmat ko‘rsatish imkonini beradi; standart televideniya, yuqori aniqlikdagi televideniya, interaktiv o‘yinlar, Internetga yuqori tezlikda ulanish.

- Personalizatsiya. IPTV tizimi ikki tomonlama aloqani ta’minlaydi va foydalanuvchilarga, ularning xohishlariga binoan ko‘rish imkonini beradi (masalan, VoD - talab bo‘yicha video xizmati - abonent buyurtmasi bo‘yicha Operator videoserveridan filmlarning translyatsiyasi).

- Qoldirib ko‘rish. Videomagnitofon bilan IPTV kombinatsiyasi - keyin ko‘rish uchun IPTV kontentini yozish uchun mexanizmni ta’minlaydi.

- Turli tipdagi terminallar qo‘llanilgandagi IPTV xizmatiga ulanish - IPTV kontentini ko‘rish faqatgina televizion qabul qilgichlar orqali chegaralanmaydi. IPTV xizmatlariga ulanish uchun foydalanuvchilar o‘zlarining personal kompyuterlari va mobil qurilmalaridan foydalanishlari mumkin.

**IPTV arxitekturasi**

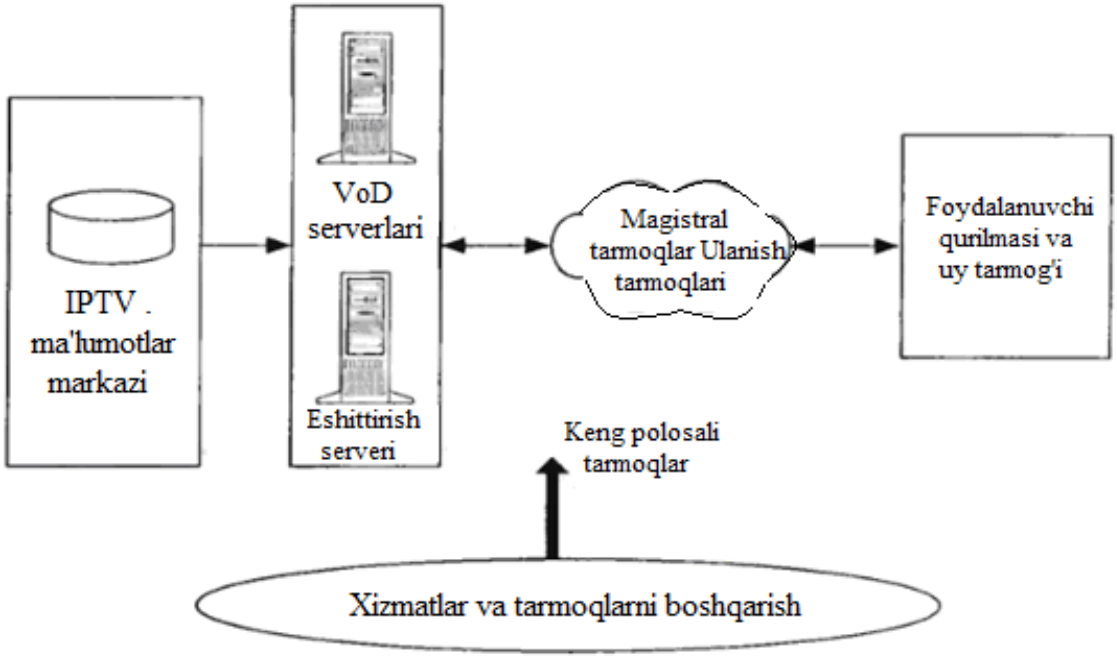
IPTV tizimi arxitekturasining umumiy ko‘rinishi 3.7-rasmda keltirilgan. Arxitektura o‘zining tarkibiga quyidagi funksional bloklarni kiritadi:

- kontent manbalari. Kontent manbai IPTV ma’lumotlar markazi sifatida aniqlanadi, ishlab chiquvchidan video kontentni qabul qiluvchi (eshittirish dasturlari, filmlar, o‘yinlar va boshqalar). So‘ngra kontent kodlanadi va foydalanuvchilarga uzatiladi yoki VoD xizmati uchun ma’lumotlar bazasida yig‘iladi;

- IPTV xizmati bog‘lamalari. Xizmatlar bog‘lamasi turli formatlardagi video oqimlarni qabul qilish komponentini o‘zida ifodalaydi. So‘ngra bu video oqimlar IP tarmoqda uzatish uchun paketlarga inkapsulyatsiyalanadi;

- keng polosali tarmoqlar. Magistral tarmoqlar va ulanish tarmoqlaridan iborat bo‘lgan keng polosali tarmoqlar, yuqori o‘tkazish qobiliyati, yuqori ko‘rsatkichli xizmat ko‘rsatish sifati va taqsimlovchi imkoniyatlar bilan xarakterlanadi. Bunday

tarmoqlarning asosiy xususiyati, xizmatlar bog‘lamasidan foydalanuvchilar qurilmasiga IPTV ma’lumotlar oqimini ishonchli taqsimlash uchun zarur bo‘lgan ko‘p adresli jo‘natish (multikasting) hisoblanadi. IPTV magistral tarmoqlarda tolali optik liniyalar, ulanish tarmoqlarida turli keng polosali - simli va simsiz texnologiyalar qo‘llaniladi;




3.7-rasm. IPTV tizimining soddalashtirilgan arxitekturasi

- foydalanuvchi qurilmasi. IPTV foydalanuvchi qurilmasi tarkibiga, keng polosali tarmoq oxiri bilan shakllanuvchi interfeys vositasi kiradi. Bu yerda uy tarmog‘ini tashkil qiluvchi shlyuzlar qo‘llanilishi mumkin. Foydalanuvchi qurilmasidagi IPTV trafikni terminallashtiruvchi funksional blok IPTV mijozi deyiladi. Odatda bu blok TV – qo‘shimcha ko‘rinishida qo‘llaniladi. TV-qo‘shimchaning asosiy vazifasi o‘zining tarkibiga xizmatlar bog‘lamasi bilan ulanishni o‘rnatish, video oqimlarni dekoderlash, foydalanuvchi tomonidan boshqarishni aks etishi va monitorga ulanishni kiritadi.

IPTV tarmoqlarida turli xalqaro tashkilotlar tomonidan ishlab chiqilgan standartlarning katta to‘plami qo‘llaniladi: ITU-T, ETSI, IETF, MPEG. TV – signalini siqish standartlari talab etilgan o‘tkazish oralig‘ini o‘n va yuz martaga kamaytirish imkonini beradi. Raqamli eshittirish standartlarini keng tarqalgani yevropa standarti DVB, amerika standarti ATSC va yaponiya standarti ISDB hisoblanadi. IPTV xizmatlarini taqdim etuvchi tarmoq protokollarining katta soni orasida quyidagi ayrimlarini aytamiz: transport protokollari UDP, RTP va RTCP; signalizatsiya protokollari SIP, H.323; mashrutizatsiya protokollari RIP, OSPF, ko‘p adresli jo‘natish protokoli IGMP.

### 3.5.4. Internet tarmog‘idagi xizmatlar

Internet tarmoqlarida amalga oshiriladigan ilovalarga World Wide Web (WWW), elektron pochta, haqiqiy vaqtda Internet orqali axborot almashish (chat rooms), oqimli video, muzikali saytlarga ulanish kiradi. WWW qo‘llanilgan holatda foydalanuvchi kompyuter ekranida matn va grafik ob’ektlarni ko‘radi, belgilangan ob’ektga sichqoncha tugmasini bosadi va mos kelgan sahifa ekranda paydo bo‘ladi.

Boshqa ilovalar oqimli video xizmati hisoblanadi. Oqimli video - video yozishni bajarish uchun manba va qabulqilgich mos keluvchi qurilmaga ega bo‘lishi kerak. Internet protokollari va vositalarini qo‘llash bilan video oqim manbadan qabul qiluvchiga jo‘natiladi. Bu xizmat talab bo‘yicha video (Video on Demand, VoD) ilovalardan biri singari ko‘rilishi mumkin.

Oxirgi serverda joylashgan, o‘chirilgan ma’lumotlar fayllariga ulanish usullaridan biri, mijoz so‘rovi bo‘yicha fayl nusxasini uzatish hisoblanadi. Bu maqsadda Internet tarmoqlarida standart protokol FTP (File Transfer Protocol) - fayllarni qayta uzatish protokoli qo‘llaniladi.

FTP protokoli server va mijoz orasida ma’lumotlar fayllarini almashish uchun qo‘llaniladi. Har bir oxirgi nuqta fayllarni uzatish va olish/so‘rash imkoniga ega.

Bunday fayllarga matn, grafika, tasvirlar, ovoz, video va multimediali axborot bo‘lishi mumkin. Shuningdek FTP protokoli, mijoz kompyuteriga dasturiy ta’minotni yuklash uchun ham qo‘llaniladi. Foydalanuvchi FTP protokoli yordamida olinadigan fayllarni to‘g‘rilashi mumkin (o‘chirish, nomini o‘zgartirish, nushalash va boshqalar).

Texnik nuqtai nazardan WWW, yagona HTTP (Hypertext Transfer Protocol) protokoli yordamida muloqot qilinadigan ko‘pgina mijozlar va serverlar sifatida ko‘riladi. Internetda gipermatnni aks ettirish, yaratish va saqlashni yengillashtirish uchun HTML (Hypertext Markup Language) dasturlash tili qo‘llaniladi. HTTP va HTML protokollarining kombinatsiyasi Internet global tarmog‘i orqali matn, grafika, ovoz, video va boshqa multimediali fayllarni yetkazishni ta’minlaydi.

Elektron pochta IP tarmoqda eng eski ilovalardan biri hisoblanadi. Hozirgi kunda millionlab odamlar har kuni elektron pochta orqali axborot almashadi. Bu almashish SMTP (Simple Mail Transfer Protocol – pochta xabarlarini eltishni oddiy protokoli) protokoli yordamida amalga oshadigan mijoz va server orasida ma’lumolar almashishni yana bir ko‘rinishi hisoblanadi.

### 3.5.5. IP tarmoqlarda multimediali trafik xususiyatlarini tahlil qilish

Hozirgi kunda Internetning barcha tarmoq trafigini ikki sinfga ajratish mumkin – TCP protokoli asosida boshqariladigan trafik va UDP protokoli asosida boshqariladigan trafik. Oxirgi 5 – 7 yil davomida TCP va UDP trafiklarining proporsiyasi juda keng o‘zgardi. Taxminan trafikning 90% TCP ulanishi orqali uzatiladi. TCP trafigining o‘sishiga ta’sir etuvchi ilovalar juda tez rivojlanmoqda, birinchi navbatda turli Web ilovalar va bir darajali tarmoqlararo ulanishlar tufayli. Xuddi shu vaqtda VoIP, IPTV va boshqa taniqli yangi ilovalarni o‘sishiga bog‘liq holda UDP trafigining taxminiy hajmi taxminan 90% ni tashkil etadi. Biroq yaqin yillarda bu trafik sinfining amaliy o‘sishini kutish kuzatiladi.

Shuningdek, IP tarmoqni boshqarish va signalizatsiyani turli protokollari bilan shakllanuvchi boshqarish trafigi mavjud. Boshqarish trafigini qayta ishlash tarmoqni normal ishlashi uchun zarur, uning hajmi nisbatan kam (1-1.5%) va tarmoq ishlashining xarakteristikalariga ta’sir qilmaydi.

Internet tarmoqlarida transport protokoli turiga bog‘liq holda sinflarga ajratishdan tashqari, trafikni 3 ta asosiy tipga farqlash qabul qilingan: elastik, oqimli va haqiqiy vaqtdagi.

Elastikli termini – TCP protokolini boshqaruvchi ma’lumotlar uzatishni yaratishdagi trafikka nisbatan qo‘llaniladi. Uning nomi, tarmoqda yuklama o‘zgarishiga javoban uzatish tezligi keng oraliqlarda o‘zgarishi mumkinligi bilan bog‘langan. Bu turdagi trafik yo‘qotishlarga sezgir va kechikishlarga nisbatan moil emas.

Oqimli trafik – audio va video axborot uzatish bilan bog‘liq bo‘lgan ilovalar natijasida yuzaga keladi. Bu ilovalar aloqa seansi vaqtida kechikishlarni chegaralash yo‘li bilan saqlangan, aniq uzatish tezligiga ega bo‘lgan paketlar oqimini generatsiyalaydi. Lekin bunda real vaqtdagi trafik bilan taqqoslash bo‘yicha kattaroq kechikishlarga yo‘l qo‘yilishi mumkin va bu turdagi trafik yo‘qotishlarga nisbatan kam sezgir.

Real vaqtdagi trafik – nisbatan katta bo‘lmagan uzunlikdagi kechikishlarni beradi va yo‘qotishlarga kam sezgir. Bu turdagi trafik IP-telefoniya tizimlarida va videokonferens aloqada mavjud. Oqimli trafik va real vaqtdagi trafik UDP protokoli boshqaruvi ostida uzatiladi.

IP klassik tarmoqlarda faqatgina best effort prinsipi bo‘yicha xizmat ko‘rsatilgan elastikli trafik mavjud edi. Barcha uchta turdagi trafik mavjud bo‘lgan zamonaviy IP tarmoqlar uchun, best effort sathi parametrlaridan boshlanib va haqiqiy vaqt trafigiga mos keluvchi parametrlar bilan tugaydigan xizmat ko‘rsatish sifatining parametrlarini ko‘rsatkichlarining keng ko‘lami talab etiladi.

### 3.5.6. IP tarmoqlarda turli ilovalar uchun taqsimot

Odatda tarmoq yadrosiga oqimlarni kelib tushish jarayoni katta sonli bir-biriga bog‘liq bo‘lmagan seanslarni super holatini o‘zida namoyon etadi. IP tarmoqlarda oqimlar xarakteri haqidagi statik ma’lumotlar shundan dalolat beradiki, kiruvchi oqim va xizmat ko‘rsatish vaqti keltiradigan taqsimlashning ko‘pgina holatlarini eksponensial hisoblash mumkin.

Shu o‘rinda elastikli trafikni statik tadqiq qilish shuni ko‘rsatadiki, oddiy taqsimlash bilan bir qatorda, kelib tushish hamda xizmat ko‘rsatish jarayonlari sekin so‘nuvchi taqsimlanishlar bilan tasvirlanishi mumkin. Shuningdek, ko‘pgina ilovalarda oqimli trafik va haqiqiy vaqtdagi trafikning tuzilishi sekin so‘nuvchi taqsimlanishlarga kiradi. Bunday taqsimlanishlarda dispersiya katta bo‘lishi mumkin.

Sekin so‘nuvchi taqsimlanishli tasodifiy jarayonlar o‘ziga o‘xshash jarayonlar sinfiga kiradi. Ko‘rsatilgan turni taqsimlanishini keng tarqalgani Pareto, Vebulla va mo‘tadilli taqsimlanish hisoblanadi.

3.3-jadvalda IP tarmoqlarda turli ilovalar uchun statik tadqiq qilishni umumlashtirilgan natijalari keltirilgan. Bu yerda A orqali kiradigan oqimlarni taqsimlanishi, V orqali bloklarning uzunligini taqsimlanishi belgilangan.

Jadvaldan ko‘rinadiki pochta trafigi (SMTP protokoli) eksponensial taqsimlash sifatida ifodalanadi, u holda taniqli IP ilovalarning katta soni sekin so‘nuvchi taqsimlanishga mos keladi.

3.3-jadval.

IP tarmoqlarda turli ilovalar uchun statik tadqiq qilishni umumlashtirilgan natijalari

| Trafik turi | IETF modeli sathi | Taqsimlanish | |
|---|---|---|---|
| | | A | V |
| VoIP/UDP | Ilovali / transportli | P | P |
| FTP/TCP | Ilovali / transportli | P | W va LN |
| SMTP/TCP | Ilovali / transportli | M | M |
| HTTP/TCP | Ilovali / transportli | P | LN va P |
| IP | Tarmoqli | P | P |
| Ethernet | Ma’lumotlar zvenosi | P | P |

Ilova: P – Pareto taqsimlanish;

M – eksponensial taqsimlanish;

W – Veybulla taqsimlanish;

LN – mo‘tadilli taqsimlanish.

## 3.6. Xizmat ko‘rsatish sifati sohasida terminlarni tushuntiruvchi ITU-T modeli

Ingliz tilida “Xizmat ko‘rsatish sifati” terminiga Quality of Service (QoS) so‘z birikmasi mos keladi. “Xizmat ko‘rsatish sifati” termini telefon tarmoqlarining ishlab turishida turli aspektlarning tavsiflarida qo‘llaniladi.

ITU-T xujjatlarida xizmat ko‘rsatish sifatiga tegishli bo‘lgan terminlar E.800 tavsiyasi bilan aniqlanadi. Bu tavsiyada QoS ko‘rsatkichlari, xizmat ko‘rsatish xarakteristikalarining birgalikda paydo bo‘lishi kabi qaraladi. Quyidagi 3.8-rasmda xizmat ko‘rsatish sifati komponentlarini va ularning o‘zaro aloqasini aniqlovchi model ko‘rsatilgan.

Kutiladigan xizmat ko‘rsatish sathi quyidagi xarakteristikalar bilan baholanadi:

– Xizmat ko‘rsatishni qo‘llab-quvvatlash (service support);

– Xizmat ko‘rsatishning qulayligi (service operability);

– Xizmat ko‘rsatishni taqdim etish (service ability);

– Xizmat ko‘rsatish xavfsizligi (service security).

Xizmat ko‘rsatishni qo‘llab-quvvatlash xarakteristikasi, operator xizmatini taqdim etish qobiliyatini va uning qobiliyatliligini qo‘llashni aks ettiradi. O‘z navbatida xizmat ko‘rsatishni taqdim etish xarakteristikasi quyidagi uchta guruhga bo‘linadi:

– Xizmatlarga ulanish (service accessability);

– Xizmat ko‘rsatish mo‘tadilligi (service retainability);

– Xizmat ko‘rsatishning to‘liqligi (service integrity).

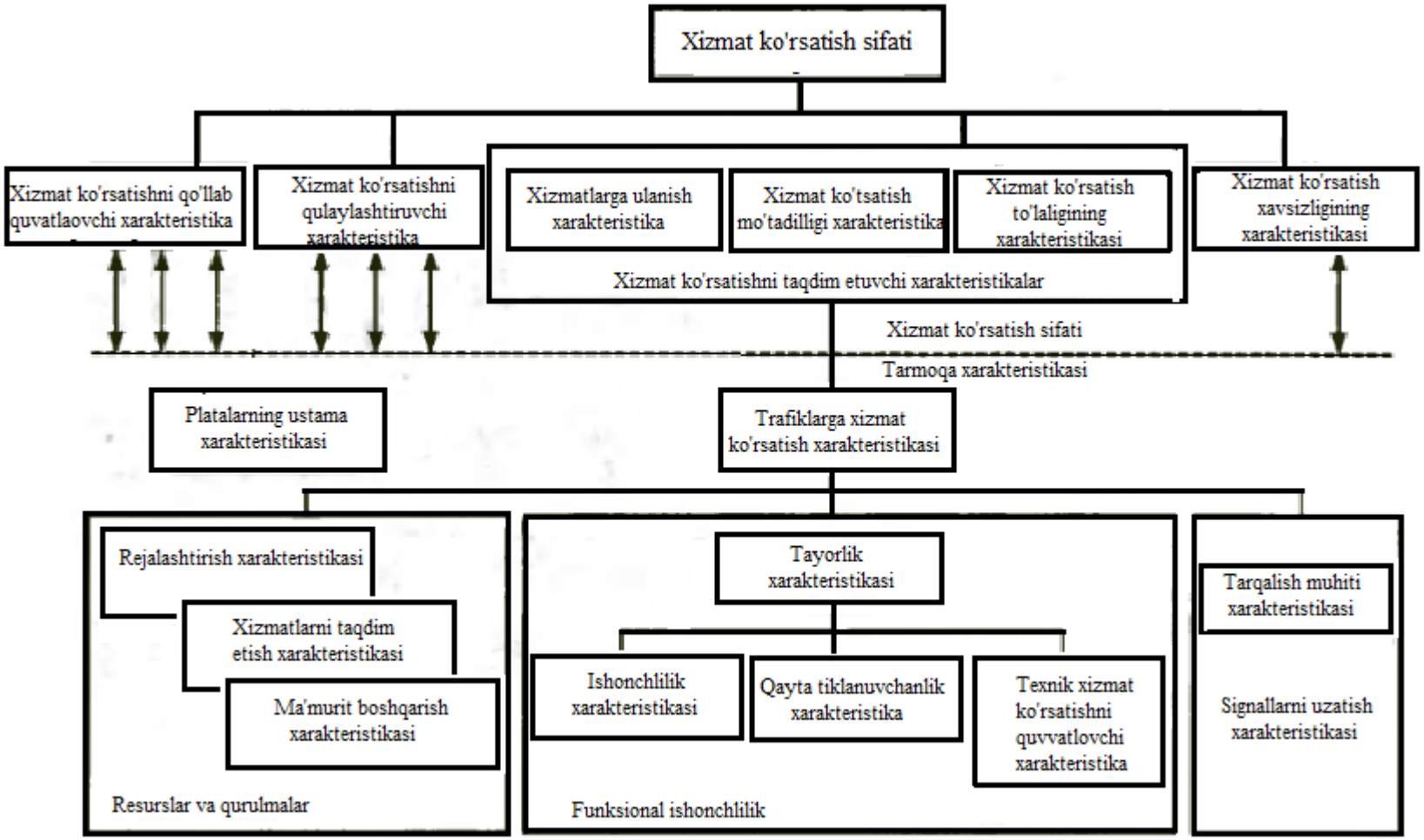
Xizmatlarga ulanish xarakteristikasi, foydalanuvchining talablari bo‘yicha ularni olish imkonini va so‘ralgan vaqt oralig‘ida yomonlashishi sezilmaydigan holatda xizmat ko‘rsatishni davom ettirishni baholaydi.

Xizmat ko‘rsatish mo‘tadilligining xarakteristikasi, so‘ralgan vaqt oralig‘i davomida berilgan atributlar bilan, olingan xizmatlardan foydalanish imkonini aniqlaydi.

Xizmat ko‘rsatishning to‘liqlilik xarakteristikasi, ko‘rsatiladigan xizmatlar to‘laligicha, yomonlashmasdan amalga oshiriladi.

Xizmat ko‘rsatish xavfsizligi xarakteristikasi, telekommunikatsiya tarmoqlarining quyidagi ishlash aspektlari bilan bog‘liq: ruxsat etilmagan monitoring, g‘irromlikni qo‘llash, buzuq niyatda shikast yetkazish, noto‘g‘ri qo‘llash, inson xatolari, tasodifiy falokatlar.

Yuqorida qayd etilgan barcha xizmat ko‘rsatish xarakteristikalari tarmoqning ishlash sifatiga, shuningdek funksional imkoniyatlariga bog‘liq. Mos keluvchi bog‘lanishlar 3.8-rasmning past qismida chiziq liniyalar bilan belgilangan.




3.8-rasm. Xizmat ko‘rsatish sifati sohasida terminlarni tushuntiruvchi ITU-T modeli

Platalarning ustama xarakteristikasi (charging performance), aloqa turi, belgilangan punkt, sutkadagi vaqt va ulanishning davomiyligi nuqtai nazaridan to‘g‘rilangan ustama platalar ehtimolligi orqali aniqlanadi.

Trafikka xizmat ko‘rsatish xarakteristikasi (traffic ability performance), ma’lum bir parametrga ega bo‘lgan trafikka xizmat ko‘rsatuvchi texnik vositalarning qobiliyatini aniqlaydi. Bu xarakteristika uchta katta guruhga bo‘lingan.

Birinchi guruh uchun terminlar, “Resurslar va qurilmalar” deb ataladi va ular hali aniqlanmagan. Umuman olganda rejalashtirish xarakteristikalari uchun ta’rif (planning performance), xizmatlarni taqdim etish (provisioning performance) va ma’muriy boshqarish yaqin vaqtlarda ishlab chiqiladi.

Ikkinchi guruh, funksional ishonchlilik (depend ability) deb ataladi. Bu yig‘ma termin, asosiy ta’sir qiluvchi omillarni inobatga olgan holda ishga qobiliyatlilik xarakteristikasida ko‘rsatiladi va to‘rtta muhim xarakteristika ajratiladi:

– tayyorgarlik (availability) – berilgan vaqt lahzasida yoki har qanday berilgan vaqt oralig‘i lahzasida texnik vositalarni talab qilingan vazifani bajarish qobiliyati (agar zarur bo‘lsa mos keluvchi tashqi resurslarni qo‘llagan holda);

– ishonchlilik (reliability) – ma’lum bir sharoitda, belgilangan vaqt oralig‘i davomida texnik vositalarni talab qilingan vazifani bajarish qobiliyati;

– qayta tiklanuvchanlik (maintainability) – o‘rnatilgan sharoitda texnik vositalarni qo‘llashda xuddi shunday holatda tiklanishini qo‘llab quvvatlash, shuningdek, belgilangan jarayon va resurslarni qo‘llash yordamida talab qilingan vazifani bajarishi mumkin bo‘lgan texnik xizmat ko‘rsatish qobiliyati tushuniladi;

– texnik xizmat ko‘rsatishni qo‘llab quvvatlash (maintenance support) – texnik xizmat ko‘rsatishni belgilangan qoidalarida, talab bo‘yicha ma’lum bir texnik vositalarni ishga qobiliyatliligini ta’minlash uchun zarur bo‘lgan resurslarni qo‘llash imkonini beruvchi ekspluatatsion kompaniyalarning qobiliyati tushuniladi.

Uchinchi guruhga, signallarni uzatish xarakteristikalari (transmission performance) kiradi. Ular ishga qobiliyatli holatda bo‘lgan aloqa tizimi orqali uzatilgan, qayta tiklangan signalning sathi kabi aniqlanadi.

ITU-T E.800 tavsiyasida tarqalish muhitining xarakteristikalari (propagation performance) ajratilgan. Ular, shu jarayonni sun’iy boshqarishsiz, belgilangan ulanish bilan signallarni o‘tishini ta’minlovchi muhit qobiliyati bilan aniqlanadi.

Bugungi kunda kanalli kommutatsiyalash va paketli kommutatsiyalash tarmoqlari IP-infrastrukturasiga asoslangan tarmoqlarga asta-sekinlik bilan birlashmoqda. Bunday tarmoqlar UFTT (umum foydalanuvchi telefon tarmog‘i) trafiklari kabi odatdagi Internet trafiklarini ham tashiydi. Konvergensiyaning bunday tuzilishi, texnologiyalarni birlashtirish orqali tannarxning kamayishiga olib kelishi kabi yangi xizmatlarni yaratish orqali industriyaning rivojlanishi yuz beradi. Lekin amalda konvergensiya juda sekin amalga oshmoqda. Texnik nuqtai nazardan eng qiyini xizmat ko‘rsatish sifatini ta’minlash muammolari bilan bog‘liq.

Odatdagi IP tarmoqlar foydalanuvchilarga taqdim etiladigan tarmoq resurslarining mumkin bo‘lgan haqqoniy ulushini sifatli “eng yaxshi urinish” (best effort)ni qo‘llaydi. Lekin bularni ishlab chiqarish sathida bajarilishi kafolatlanmaydi.

Best effort prinsipi haqiqiy bo‘lmagan vaqt masshtabida (elektron pochta, fayllarni uzatish) ilovalarni qo‘llab quvvatlash uchun yetarli darajada samarali va vaqtning haqiqiy masshtabiga yaqin bo‘lgan ilovalar (audio/video eshittirish, Web ni ko‘rish) uchun kengaytirildi. Biroq foydalanuvchilardan kutiladigan interaktiv ovozli telefoniya va haqiqiy vaqtning boshqa ilovalarining sifatini ta’minlash kam ehtimollidir, o‘tkazish qobiliyatini chegaralash, paketlarni yo‘qolishiga yoki kechikish kattaligini jiddiy ravishda oshishiga olib keladi.

Kelajakda, IP-tarmoqlariga asoslangan konvergensiyaning to‘liq foydali samaradorligini qo‘llash uchun, IP (VoIP)dan yuqori ovozga ega bo‘lgan ko‘p va turli tuman foydalanuvchi ilovalar uchun QoSni differensiallashni ishonchli ta’minlash qobiliyatiga ega bo‘lgan resurslarni taqsimlashni yangi prinsipini qo‘llash kerak.

QoSni boshidan oxirigacha IP uchun hal qilish, qo‘llanilishi mumkin bo‘lgan IP/UFTTni muvaffaqiyatli konvergensiyalash imkonini beradi, masalan quyidagi uchta qadamni:

- IP ni ishlab chiqish parametrlarining umumiy majmuasiga nisbatan tarmoq provayderlarining shartnomalari va QoS talablarini amalga oshirish;

- terminal uchastkada QoS ning belgilangan talablarini qo‘llab-quvvatlovchi tarmoq mexanizmlarini tarqatish;

- kafolatlangan QoS bilan IP-protokollari so‘rovi bo‘yicha signalizatsiya protokollarida QoS talablarini joriy qilish imkonini yaratish.

Oxirgi vaqtlarda IP tarmoqlarda xizmat ko‘rsatish sifati (QoS) savollari juda dolzarb bo‘lib qoldi, chunki bunday masalalarning hal qilinishi kelajakdagi XXI asr aloqa tarmoqlari bilan to‘g‘ridan to‘g‘ri bog‘liq.

O‘tgan bir necha yillar davomida IETF tashkiloti doirasida, QoS ni ta’minlash bilan bog‘liq bo‘lgan katta yoki kichik darajadagi bir qancha arxitekturalar va mexanizmlar taklif qilindi. Bulardan anchagina taniqli bo‘lgani va qo‘llanilgani IntSerf, DiffSerf, MPLS (GMPLS)lar, shuningdek majburiy marshrutlashtirish mexanizmi hisoblanadi.

## 3.7. Optik IP-tarmoqlarda xizmat ko‘rsatish sifatini ta’minlash xususiyatlari

Zich to‘lqin uzunligi bo’yicha zichlashtirishga (Dense Wavelength Division Multiplexing, DWDM) ega bo‘lgan texnologiya tomonidan tavsiya etilgan, yetarli chastota oralig‘i bilan birgalikda keng tarqalgan IP texnologiyasi, IP-over-DWDM kabi ma’lum va keyingi avlodning (Next Generation, NG) Internet tarmoqlarida katta masofalarga ma’lumotlarni uzatishda yetakchi hisoblanadi.

DWDM – bu zich to‘lqin uzunligi bo‘yicha zichlashtirish texnologiyasi bo‘lib, juda ko‘p chastotalarda yoki to‘lqin uzunliklarida ma’lumotlar paketlarini bir vaqtda uzatish orqali, optik tola resurslaridan samarali foydalanishga imkon beradi.

Ovozli paketlarni va videoni haqiqiy vaqt oralig'ida uzatish kabi ayrim xizmatlarni kafolatlash uchun xizmat ko‘rsatish sifatini QoS ta'minlash muammosi, optik magistrallar uchun amalda yechimini topmagan.

Optik DWDM texnologiyasi qo'llanilgan tarmoqlarda QoSni ta'minlash muammolari, elektron kommutatorlarda va marshrutizatorlarda qo‘llaniladigan QoS usullaridan bir qancha fundamental farq qiladi.

Eng asosiy farq DWDM qurilmalarida, kechiktiruvchi optik liniyalarda buferlanishi mumkin bo‘lgan paketlar navbati konsepsiyasining mavjud emasligidir. Kechikish liniyasi (Fiber Delay Line, FDL) - bu ma'lum bir vaqt oralig‘ida optik signalni kechiktirish uchun qo‘llaniladigan uzun optik tolali liniyadir.

Optik tarmoqlarda navbat alternativasi sifatida, kelgusida ma'lumotlarni optik kommutatsiyalash yo‘li orqali chastota oralig‘ini zahiralash uchun signalli axborotlarni qo‘shimcha uzatish qo‘llaniladi.

### 3.7.1. Optik kommutatsiyalash texnologiyalari

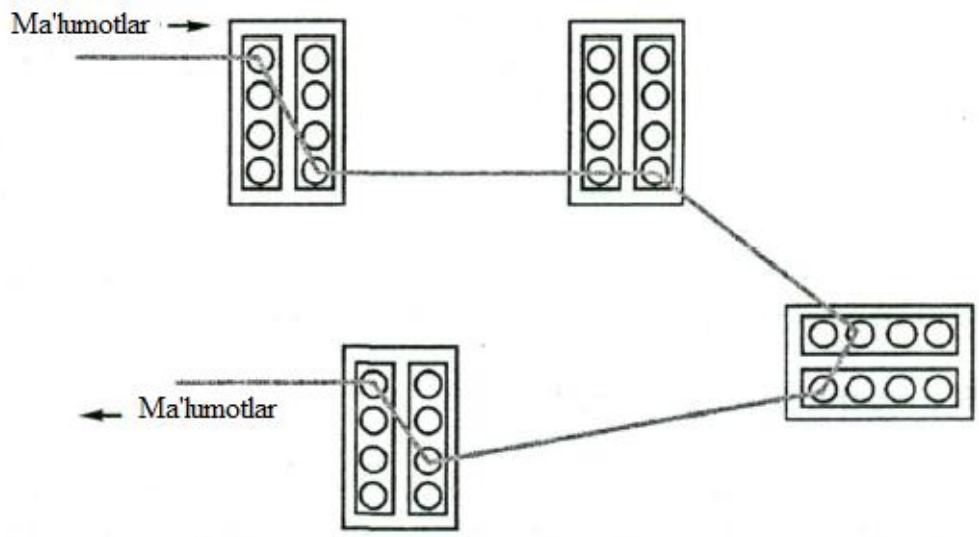
DWDM texnologiyasiga asoslangan optik tarmoq bo‘ylab IP-trafiklarni uzatish uchun uchta asosiy kommutatsiyalash texnologiyasi tavsiya etilgan. Shunga mos holda IP-over-DWDM tarmoqlari quyidagicha sinflanishi mumkin:

- to‘lqinli marshtutizatsiyaga ega bo‘lgan tarmoqlar (Wavelength Routing, WR);
- paketlarni optik kommutatsiyalashga ega bo‘lgan tarmoqlar (Optical Packet Switching, OPS);
- bloklarni optik kommutatsiyalashga ega bo‘lgan tarmoqlar (Optical Burst Switching, OBS).

**To‘lqin uzunligi bo‘yicha marshrutizatsiyalashga ega bo‘lgan tarmoqlar.**

To‘lqin uzunligi bo‘yicha marshrutizatsiyalashga ega bo‘lgan tarmoqlar (WR)da, tarmoqning ikkita yakunlovchi bog‘lamalari orasida to‘liq optik to‘lqinli

yo‘l yaratiladi. Bu optik yo‘l *yorug‘lik yo‘li* (lightpath) deb ataladi va 3.9-rasmda ko‘rsatilganidek yo‘l bo‘ylab har bir zveno uchun to‘lqinli kanalni zahiralash yo‘li orqali yaratiladi.




3.9-rasm. Yorug‘lik yo‘lini hosil bo‘lishi

Barcha ma’lumotlar uzatilganidan keyin yorug‘lik yo‘li bo‘shaydi. WR tarmoqlari, bir-biri bilan ihtiyoriy topologiyalar orqali, optik tolali liniyalar bilan ulangan *optik kross-konnektor* (OXS)lardan tashkil topgan. OXS qurilmalari, ma’lumotlar oqimini qaysi kirish portiga tushganini va ular qanday to‘lqin uzunliklariga egaligini farqlash qobiliyatiga ega. Natijada yorug‘lik yo‘lining ikkita oxirgi nuqtalari orasidagi oraliq bog‘lamalarda birorta qayta ishlashni, ya’ni elektro-optik E/O o‘zgartirishni yoki ma’lumotlarni buferlashni amalga oshirish zarurati tug‘ilmaydi.

Biroq WR tarmoqlarda, kanallarni kommutatsiyalashga ega bo‘lgan tarmoq turlari kabi resurslarni statik taqsimlash qo‘llanilmaydi, bu esa mumkin bo‘lgan chastota oralig‘ini juda past qo‘llashga olib keladi.

**Paketlarni optik kommutatsiyalashga ega bo‘lgan tarmoqlar.**

Paketlarni optik kommutatsiyalashga (OPS) ega bo‘lgan tarmoqlarda IP-trafik, «paket ketidan paket» prinsipi bo‘yicha har bir marshrutizatorda qayta ishlanadi va kommutatsiyalanadi. IP-paket sarlavhadan va foydali yuklamadan iborat. Paket sarlavhasi marshrutlash uchun zarur bo‘lgan axborotdan iborat va foydali yuklama kabi haqiqiy ma’lumotlarni taqdim etadi.

OPS tarmog‘ining kelajakdagi eng oliy maqsadi - optik muhit ichida paket sarlavhasini qayta ishlash. Texnologiyaning mazkur sathida bu mumkin emas. Bunday muammoning yechimi, optik muhitda foydali yuklamani saqlagan holda elektron muhitda sarlavhani qayta ishlash hisoblanadi.

OPSning asosiy afzalligi, chastotalar oralig‘ini taqsimlash uchun statik zichlashtirishni qo‘llash yo‘li bilan chastota diapazonini qo‘llashni oshirish imkonidir.

**Bloklarni optik kommutatsiyalashga ega bo‘lgan tarmoqlar.**

OBS tarmoqlari, oldin ko‘rib chiqilgan ikkita WR va OPS tarmoqlarning afzalliklariga ega. Bu yerda oraliq uzellarda buferlashtirish va elektr qayta ishlashga xojat qolmaydi. Ayni shu paytda OBS chegaralangan vaqt davomiyligida kanallarni zahiralash yo‘li orqali tarmoqni qo‘llash koeffitsientini oshiradi.

OBS tarmoqlarida asosiy kommutatsiyalash birligi bu blokdir. Blok (burst), kirish uzelidan chiqish uzeliga birgalikda uzatiladigan va oraliq uzellarda birgalikda kommutatsiyalanadigan paketlar ketma-ketligidir.

Bloklar shakllanishi uchun bir qancha yondashishlar mavjud, masalan: agregatsiyaning chegaralangan vaqtiga ega bo‘lgan konteynerlash texnikasi (Containerization with Aggregation-Time out, CAT).

Blok ikki qismdan iborat: sarlavha va ma’lumot. Boshqaruvchi blok (Control Burst, CB) deb ataluvchi sarlavha, birinchi beriladigan ma’lumotlar bloki (Data Burst, DB) deb ataluvchidan alohida uzatiladi va uning DB siga mos kelishi uchun butun yo‘l bo‘ylab chastota oralig‘ini zahiralaydi. Undan keyin DBning o‘zi SV uchun zahiralangan yo‘l bo‘ylab harakatlanadi.

### 3.7.2. IP-over-DWDM tarmoqlarda xizmat ko‘rsatish sifati

**WR tarmoqlarda QoS.** Bu yerda WR tarmoqlarda xizmatlarni ta’minlashni asosiy yo‘nalishlari ko‘rib chiqiladi. Bu usullar differensial optik xizmatlar (Differentiated optical Services, DoS) modelini kengaytiradi.

DoS modeli yorug‘lik yo‘nalishini ajoyib optik xarakteristikalarini e’tiborga tortadi. Bu optik parametrlarga quyidagilar kiradi: xatoliklarni yuzaga kelish chastotasi (Bit Error Rate, BER), kechikish, djitter va himoyalash, nazorat va ishonchlilik rejimlari. Bu optik parametrlar va rejimlar berilgan yo‘nalishga tegishli optik xizmatlar sifatini o‘lchash uchun asos hisoblanadi. Bu o‘lchashlarning maqsadi – IP da QoS ekvivalent sinflarida optik xizmatlar sinfini aniqlaydi.

QoS tuzilishi 6 ta komponentdan iborat.

*Xizmatlar sinfi.* QoSda xizmatlar sinfi yorug‘lik yo‘nalishi bo‘ylab uzatiladigan optik signallarni buzilishi va sifatini xarakterlaydigan parametrlar yig‘indisi bilan aniqlanadi. Bu parametrlar kechikish, BERning o‘rtacha qiymati, djitter va o‘tkazish oralig‘i yoki funksional vazifalarga asoslangan imkoniyatlar – nazorat, himoyalash, ishonchlilik bilan aniqlanishi mumkin.

*Marshrutlash algoritmi va chastotalar vazifasi.* Yorug‘lik yo‘nalishini yaratish uchun, unga mo‘ljallangan to‘lqin uzunliklari butun yorug‘lik yo‘nalishi o‘tadigan trassa bo‘ylab zahiralangan bo‘lishi kerak. Marshrutlarni tanlash uchun qo‘llaniladigan algoritm va yorug‘lik yo‘nalishini yaratishdagi to‘lqin uzunligi, marshrutizatsiya va to‘lqin uzunligi vazifasini (Routingand Wavelength Assignment, RWA) algoritmi sifatida ma’lum. WR tarmoqlarda QoSni ta’minlash uchun turli to‘lqinli kanallarning QoS xarakteristikasini hisobga oladigan RWA algoritmini qo‘llash zarur.

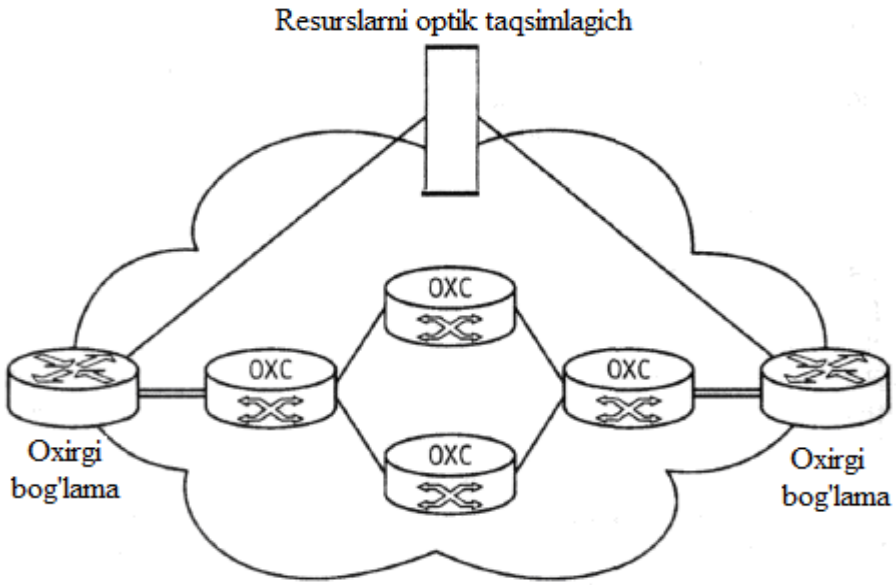
*Yorug‘lik yo‘nalishlari guruhlari.* Tarmoqda yorug‘lik yo‘nalishlari guruhlar bo‘yicha klassifikatsiyalanadi, ya’ni har bir guruh DoS xizmatiga mos kelishi kerak.

*Trafikning klassifikatsiyasi.* Joriy trafik tarmoq tomonidan ta’minlanadigan sinflardan biri bilan bog’lanadi. Tarmoq ichida yagona klassifikatsiya qo‘llaniladi.

*Yorug‘lik yo‘nalishlari vazifalarining algoritmi.* Xizmat ko‘rsatish sinflarini farqlash uchun adabiyotlarda yorug‘lik yo‘nalishi vazifalarini ko‘plab algoritmlari tavsiya etilgan. WR tarmoqlarda QoSni ta’minlash uchun turli to‘lqin uzunligidagi kanallarning QoS xarakteristikalarini hisobga oluvchi RWA algoritmini qo‘llash zarur.

*Ulanishni nazorati.* DiffServ arxitekturasida, DWDM tarmoqlarda, yorug‘lik yo‘nalishlarini dinamik ifodalash uchun mo‘ljallangan resurslarni optik taqsimlagich mavjud. Resurslarni optik taqsimlagich resurslar (tashuvchilar soni, kross-konnektorlar, kuchaytirgichlar) holatini kuzatadi va yorug‘lik yo‘nalishi xarakteristikalarini (BERni hisoblash) va funksional imkoniyatlarini (himoyalash, nazorat, ishonchlilik) baholaydi.

Shuningdek resurslarni optik taqsimlagich zanjir bo‘ylab oxirdan oxirgacha chaqiriqlarni birinchi o‘rnatishga javobgar, ya’ni yorug‘lik yo‘li bilan kesishadigan boshqa optik domenlarni ifodalaydigan.




3.10-rasm.WR tarmog‘i

Yuqorida ko‘rib chiqilgan komponentlarning barchasi tarmoqning oxirgi qurilmalarida va/yoki resurslarni optik taqsimlagichda mujassamlangan. 3.10-rasmda oxirgi qurilmalardan iborat, resurslarni optik taqsimlagichli va OXS ichki qurilmali WR tarmog‘ini tuzilishi keltirilgan. Ichki OXSlar faqatgina yorug‘lik yo‘lini o‘rnatishda, tarmoqni kommutatsiyalanadigan yadrosini konfiguratsiyasi uchun zarurdir.

**Paketlarni optik kommutatsiyalash tarmoqlarida QoS.** OPSni ko‘pgina usullari asosida yotadigan g‘oya – ma’lumotlar o‘tishi va axborotni boshqarish yo‘lini ajratishdir. Bu holda, marshrutizatsiya funksiyalari va qayta yo‘naltirish paket sarlavhasini O/E o‘zgartirishdan so‘ng elektron mikrosxemani qo‘llash bilan bajariladi. Aynan shu vaqtda foydali yuklama shaffof holda xech qanday o‘zgartirishlarsiz, optik domenda kommutatsiyalanadi. Hozirgacha OPS tarmoqlarda xizmatlarni ajratishni ta’minlashning bir necha usullari tavsiya etilgan. Bu shu bilan bog‘liqki, OPS – nisbatan yangi texnologiya va o‘zini yechimida yana ko‘pgina muammolar kutiladi. Paketlarni kommutatsiyalashni barcha usullarida nizolar yuzaga kelishi mumkin, qachonki paketlarni katta soni chegaralangan vaqt davomida kam sonli chiquvchi zvenolar orqali uzatilishi mumkin bo‘lsa. Asosan, OPS tarmoqlarda QoS texnologiyalari, nizolar yuzaga kelganda xizmatlarni ajratishni ta’minlash maqsadida, to‘lqinli ajratish algoritmini va FDLni qo‘llaydi.

Paketlarni optik kommutatsiyalashda xizmatlarni ajratish uchun ikkita algoritm mavjud. Bu algoritmlarni OPS tarmoqlarda QoSni ta’minlashni asosiy texnologiyasi sifatida ko‘rib chiqamiz.

*Eltuvchilarni taqsimlash* (Wavelength Allocation, WA). Bu usulda barcha erishish mumkin bo‘lgan eltuvchilar alohida ko‘pginalarga ajraladi va har bir ko‘pginalar ustunlikning turli sathlari bilan bog’lanadi, ustunlikning yuqoriroq sathi erishish mumkin bo‘lgan eltuvchilardan katta qismga ega. WA usuli xizmatlarni ajratish uchun faqat to‘lqin uzunligini qo‘llaydi va FDL buferlarini qo‘llamaydi.

*Chegaraviy tashlashli eltuvchilarni kombinatsiyali taqsimlash* (Combined Wavelength Allocation and Threshold Dropping, WATD). WA ga qo‘shimcha, bu usulda turli ustunliklar sinfi orasidagi farqni o‘rnatish uchun tashlab yuborish chegarasi qo‘llaniladi. Qachon FDL buferini to‘lishi o‘rnatilgan chegaradan oshsa, past ustunlikka ega paketlar tashlab yuboriladi. Bu jarayon paketning foydali yuklamasi, sarlavha to‘liq qayta ishlanmagungacha va paket sinflanmagunigacha ushlab turiladi, so‘ngra paketga eltuvchi belgilanadi. Biroq bunda kommutatsiyalash tezligini chegaralaydigan “paket paketdan keyin” prinsipi qo‘llaniladi.

**Bloklarni optik kommutatsiyalash tarmoqlarida QoS.** OBS tarmoqlarida QoSni ta’minlash signalli (zahiralash uchun) protokollarni talab etadi. Shuningdek, magistral kommutator bloklari uchun bloklarni loyihalashtirish algoritmi zarur. Bu algoritmning asosiy kamchiligi shundan iboratki, yuqori ustunlikli trafikni uzatishda yetarlicha kechikishni kiritadi.

*OBSda rejalashtirish.* Boshqaruvchi blok bog‘lamaga kelganida, mos kelgan ma’lumotlar bloki uchun kiruvchi zvenoda, to‘lqinli kanalni aniqlash uchun to‘lqinli kanallarni rejalashtirish algoritmi qo‘llaniladi. Rejalashtiruvchiga quyidagi axborotlar zarur, blokni kelish vaqti va boshqaruvchi blokka nisbatan uni siljishi. Rejalashtiruvchi har bir to‘lqinli kanalda erishish mumkin bo‘lgan vaqtli slotlarni kuzatadi. Agar bog‘lamada FDL qo‘llanilsa, ma’lumotlar blokini kechiktirish uchun bitta yoki bir necha FDLni tanlaydi, agar bu zarur bo‘lsa.

### 3.7.3. Xizmat ko‘rsatish sifati bilan bog‘liq bo‘lgan muammolar

Umumiy holda muammolar ikkita kategoriyaga ajraladi:

- tarmoq bilan bog‘liq bo‘lmagan;
- tarmoq bilan bog‘liq bo‘lgan.

Tarmoq bilan bog‘liq bo‘lmagan muammolarga quyidagilar kiradi:

*O‘ta yuklangan serverlar* (masalan, Web yoki pochta), foydalanuvchilar ulanishni o’natishga urinishi. Bu holda QoSni yaxshilashning umumiy yo‘nalishi serverlarni modernizatsiyalash yoki ular orasida yuklamani optimal ajratishli qo‘shimcha serverlarni qo‘llash hisoblanadi.

*Tarmoq ishining xatoliklari.* Marshrutizatorlar va kommutatorlarni konfiguratsiyalash jarayoni murakkab va tasdiqlangan xatoliklar hisoblanadi. Masalan, marshrutlash muammosiga olib keladigan xatolik tufayli IP-adresning dublikat konfiguratsiyasi tuzilishi mumkin.

Tarmoq bilan bog‘liq bo‘lgan muammolar:

*Qurilmalar muammolari.* Marshrutizatorlar va kommutatorlar sekundiga million paketlarni qayta ishlashi uchun zarur bo‘lgan murakkab qurilma va dasturiy ta’minlangan murakkab tizim hisoblanadi.

*Ulanish tarmog‘ining o‘tkazish qobiliyatini kamchiligi.* Iqtisodiy tomondan har doim past tezlikli ulanish kanallari (masalan, dial-up bo‘yicha) va o‘ta yuklangan kanallar mavjud. Berilgan muammo ko‘rinishi uchun texnik yechim oddiy va tushunarli:

- o‘tkazish qobiliyatini qo‘shish;
- keyingi qayta ishlash uchun trafikning klassifikatsiyasi va uni turli markirovkasi, ya’ni trafikni ko‘paytirish (policing) va chegaralashni (shaping) qo‘llash.

*Ba’zi kanallarning o‘ta yuklanganligi sababli trafikni notekis taqsimlanishi.* Bu magistral tarmoqlarda QoS bilan bog‘liq muammolarni umumiy sababi hisoblanadi. Bunday o‘ta yuklangan kanallar paketlarni katta kechikish vaqtiga, djitter yoki paketlarni yo‘qolishiga sabab bo‘ladi. Tarmoqda bunday “issiq nuqtalar”ning sababi quyidagilar bo‘lishi mumkin:

- kutilmagan holatlar, tola uzilishi yoki qurilmaning rad etishi;
- trafik modelining o‘zgarishi.

Magistral tarmoqda qo‘shimcha o‘tkazish oralig‘i har doim kerakli vaqtda va kerakli joyda yetarlicha bo‘lmasligi mumkin. Masalan, Web saytga kutilmagan ulanish yoki rejalashtirilmagan multimediali trafikni uzatish ba’zi bir kanallarning o‘ta yuklanishiga sabab bo‘lishi mumkin.

### 3.7.4. QoSni ta’minlashga bo‘lgan amaliy yondashuv

Yuqorida ko‘rib chiqilgan muammolarning yechimlariga yo‘nalishni ko‘rib chiqamiz.

*Birinchi qadam: tarmoqni tartibli holatga keltirish.* Boshida odatda tarmoq yaxshi loyihalashtiriladi va zahiralanadi. Qandaydir vaqtdan keyin tez va yaqinlashgan yechimlar tufayli muammolar yig‘iladi. Shuning uchun, doimiy “tozalash” ishlari olib borilishi kerak, bunda nosozliklarni alohida nuqtalari va tor joylari bartaraf etilishi kerak. Mos kelgan joylarga o‘tkazish qobiliyati shunday qo‘shilishi kerakki, xattoki kanallar va keskin marshrutlarni rad etishi, tarmoqni ortiqcha yuklanishiga olib kelmasligi kerak. Bu IP – tarmoqda QoSni ta’minlash uchun kerak bo‘lgan asosiy va foydali ishdir.

*Ikkinchi qadam: trafikni sinflarga bo‘lish*. Xizmat ko‘rsatishning uchta sinfi tavsiya etiladi:

- premium (Premium);
- kafolatlangan (Assured);
- eng yaxshi urinish (Best effort).

Premium - xizmat ko‘rsatish kichik kechikish va kam djitterli ishonchli xizmat ko‘rsatishni ta’minlaydi. Haqiqiy vaqtdagi trafik (masalan, vodeokonferensiya) va yo‘qotishlarga moil trafik (masalan, moliyaviy yoki tarmoqni boshqarish trafigi), shuningdek qandaydir xizmat ko‘rsatish foydasiga olinishi mumkin.

Assured - xizmat ko‘rsatish, ishonchli xizmat ko‘rsatishni ta’minlaydi. Virtual hususiy tarmoqlarning (Virtual Private Network, VPN) haqiqiy bo‘lmagan vaqtdagi trafigi shunday xizmat ko‘rsatishdan ustun chiqishi mumkin.

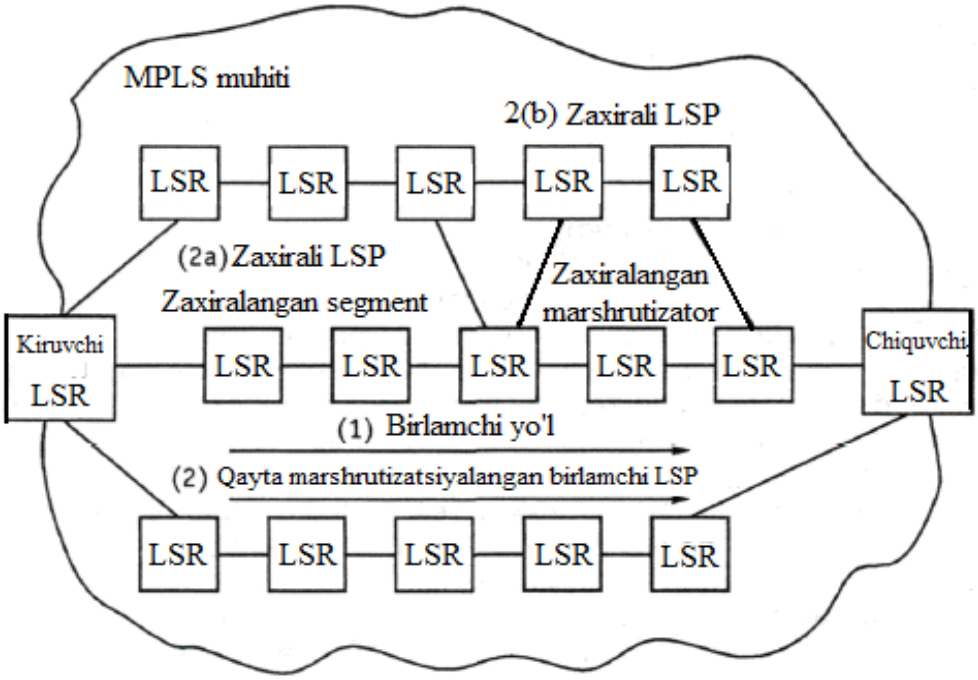
Best effort - xizmat ko‘rsatish an’anaviy Internet-xizmat ko‘rsatish.

*Uchinchi qadam: Premium trafikni himoyalash va trafik injiniringi.* Tavsiya etilayotgan yo‘nalishda belgilar bo‘yicha ko‘p protokolli kommutatsiyalash (Multiprotocol Label Switching, MPLS) texnologiyasi trafik injiniringi va himoyalash uchun qo‘llaniladi.

*Trafikni himoyalash.* Avval tarmoqda belgilar bo‘yicha kommutatsiyalash yo‘li konfiguratsiyalanadi (Label Switched Path, LSP). Har bir kiruvchi marshrutizator chiquvchiga nisbatan ikkita LSPga ega. Birinchi LSP – Premium trafik uchun qo‘llaniladi, ikkinchi LSP - Assured va Best effort trafik uchun birgalikda qo‘llaniladi. Premium LSP tez qayta marshrutlash ruxsatiga ega. Tez qayta marshrutlashning asosiy g‘oyasi, kanal, marshrutizator yoki ko‘pgina kanallar va marshrutizatorlardan iborat segment yo‘li uchun konfiguratsiyalashdan oldin LSP vaqtli ulanish mavjudligidadir, bunday kanal marshrutizator yoki segment yo‘li himoyalangan segment deyiladi.

Himoyalangan segmentda rad etish yuzaga kelsa, himoyalangan segmentni marshrutizatori ikkinchi sathdan ma’lumot oladi. LSPni vaqtli ulanishi nosozlikni aylanib o‘tishi uchun qo‘llaniladi. Bu himoyalanish 50... 100 ms oraliqda amalga oshirilishi mumkin. Tez qayta marshrutlash vaqtida, LSP tufayli qabul qilingan yo‘l shartli ravishda optimal bo‘lishi mumkin. Buni to‘g‘rilash uchun, himoyali marshrutizator axborotni LSPni kiruvchi marshrutizatoriga jo‘natadi, so‘ngra u LSP uchun yangi yo‘lni hisoblaydi va trafikni yangi LSP ga yo‘naltiradi. Bu jarayon 3.11-rasmda keltirilgan. Tez qayta marshrutlash, paketlarning yo‘qolishi yo‘l qo‘yilmaydigan ilovalar uchun zarur. Biroq tez qayta marshrutlash tarmoqning tuzilishini qisman murakkablashtiradi.

Tavsiya etilayotgan usulda Premium trafikni himoyalash, yuqori tayyorgarlikni ta’minlashga xizmat qiladi.




3.11-rasm. Tez qayta marshrutlash usuli

*Trafik injiniringi.* Tarmoqning topologiyasi va o‘tkazish qobiliyatini tez o‘zgartirib bo‘lmasligi natijasida, trafikni notekis taqsimlanishi tarmoqni ba’zi bir qismlarida o‘ta yuklanishga sabab bo‘lishi mumkin, xattoki tarmoqni umumiy o‘tkazish qobiliyati umumiy talablardan katta bo‘lsa ham. Tavsiya etilayotgan usulda har bir kiruvchi marshrutizator chiquvchiga nisbatan ikkita LSPga ega. Birinchi LSP – Premium trafik uchun qo‘llaniladi, ikkinchi LSP - Assured va Best effort trafik uchun birgalikda qo‘llaniladi. Mijozlardan keluvchi trafik kiruvchi marshrutizatorlarda, kiruvchi interfeyslarda klassifikatsiyalanadi va mos kelgan LSPga tushadi. Shuningdek tarmoq Operatorlari qo‘shimcha xizmatlar singari ko‘pgina maydonlar (jo‘natuvchi va qabul qiluvchining IP adresi, portlar raqami, protokollarning identifikatorlari va b.q ) bo‘yicha klassifikatsiyani taqdim etishi mumkin.

Trafik injiniringi ikkita maqsadda xizmat qiladi:

- trafikni notekis taqsimlash tufayli yuzaga keladigan o‘ta yuklanish holatini (maksimal imkoniyatli bosqichda) oldini olish;

- agar o‘ta yuklanish yuzaga kelsa, uni tez bartaraf etish.

*To‘rtinchi qadam: sinflarga bo‘lish asosida rejalashtirish va navbatlarni tashkil etish.* EXP maydoni asosida, turli sinflardagi MPLS paketlarining sarlavhasi turli navbatlarda joylashtiriladi. Ishlab chiqarishni konfiguratsiyasi va navbatlar o‘lchami qiyin masala hisoblanadi. Imkoniyatli yo‘nalishlardan birini ko‘rib chiqamiz. Interfeysdagi har bir navbatni kiruvchi oqim tezligi, LSP berilgan navbatdagi barcha o‘tuvchi tezliklarning yig‘indisi bilan aniqlanadi. Bu LSPlarning tezligi SNMP protokoli yordamida olinishi mumkin. Har bir sinfni nisbatan muhimligiga (masalan, pulli bahosi) bog‘liq holda, ularga turli og‘irliklar kiritish mumkin.

*Beshinchi qadam: boshqa trafikni boshqarish sxemalarini kiritish. Policing i Shaping.* Qachon mijoz xizmat ko‘rsatish tarmog‘iga yozilsa, u xizmat ko‘rsatish sathi haqida kelishuv tuzadi, (trafik Service, agar kerak bo‘lsa har bir sinf uchun), ya’ni foydalanuvchi jo‘natishi va qabul qilishi mumkin.

### 3.7.5. Yondashuvning samaradorligi

Ko‘rib chiqilgan yondashuvni quyidagilar nisbatida tadqiq etamiz:

- trafikning turli sinflarining differensiallash;
- kechikish va djitter bo‘yicha ilovalar talabini qondirish.

*Trafikning turli sinflarini differensiallash.* Qachonki kanal yoki marshrutizator rad etsa, sekunddan minutgacha qayta konfiguratsiyalash uchun IGP, MPLS va BGP zarur. Bu vaqt davri davomiyligida paketlar katta kechikishga uchraydi yoki yo‘qoladi. Tez qayta marshrutlash MPLS qayta konfiguratsiyalash davrida Premium trafikni himoyalashi mumkin. Shuning uchun tarmoq Assured trafikka qaraganda Premium trafik uchun ochiqroq. Bundan tashqari, Premium navbati uchun chiqish tezligini

kirish tezligiga nisbatini yuqori qiymati, Premium trafikka kichikroq kechikish va djitterga ega bo‘lish imkonini beradi. Best effort trafikka qaraganda Assured trafik uch marta katta resurslarni qo‘llashi mumkin. Ayniqsa rad etish va kanalda katta yuklanish yuzaga kelganda uni yetkazish uchun yaxshi sharoit bo‘ladi. QoSni ta’minlashni rejalashtiruvchi NSP amaliy faqat Premium va Best effort sinflarini qo‘llash bilan boshlanishi mumkin. Assured sinfi keyinroq zarurat yuzaga kelganida qo‘shilishi mumkin.

*Kechikish va djitter bo‘yicha ilovalar talabini qondirish.* Bu yondashuv global IP magistralida Global Crossihg operatorida to‘liq amalga oshirilgan. MPLS trafik injiniringi 1999 yildan rivojlana boshlandi va kechikish, djitter bo‘yicha ilovalarning talabini qisman qoniqtirib samarali usul hisoblanadi. Umuman olganda, transkontinental kechikish AQShda “uzatish va qaytish” 80 ms dan quyi sathda, djitter esa 2 ms dan pastdir. Bu tarmoq ishining juda yaxshi ko‘rsatkichlari hisoblanadi. ITU-T G.144 tavsiyalarida ilovalar uchun kechikishni eng yaxshi parametrlari keltirilgan (3.4-jadval).

3.4-jadval

Kechikishga taalluqli ITU-T G.144 tavsiyalari

| Bir tomonlama kechikish | Sifat xarakteristikalari |
|---|---|
| 0 - 150 ms | Ko‘pgina foydalanuvchi ilovalari uchun ma’qul |
| 150 - 450 ms | Ba’zi bir ilovalarni qoniqtirishi mumkin |
| 450 dan yuqori | Umumiy maqsad uchun tarmoqli rejalashtirishda to‘g‘ri kelmaydi |

Uzel yoki kanalning nosoz xolatida, trafik injiniringi trafikni avtomatik tarzda qayta marshrutlaydi va barcha o‘ta yuklanishlardan qutulish imkonini beradi. Bu trafikni ba’zi turlari uchun kechikishni katta bo‘lmagan ortishiga olib kelishi mumkin,

ya’ni uzunroq yo‘nalish tanlanadi, lekin paketlarni yo‘qolishini bartaraf etadi va tarmoq qayta tiklanganidan so‘ng kichik djitterni ta’minlaydi.

## Nazorat savollari

1. Qanday xizmatlar klassifikatsiyasiga asoslangan prinsiplarni bilasiz?
2. Uzatilayotgan ma’lumot turi bo‘yicha qanday xizmatlar klassifikatsiyasi mavjud?
3. Telefon xizmati turini boshqa xizmat turlaridan ajratishning asosiy sababi nimada?
4. Asosiy va qo‘shimcha xizmatlarga qanday xizmat turlari kiradi?
5. “Xizmat ko‘rsatish sathi haqidagi kelishuv” (SLA) tushunchaning ma’nosi nimadan iborat?
6. Xizmat ko‘rsatish sifati va tarmoq xarakteristikasi deganda nimani tushunasiz?
7. Xizmat ko‘rsatishning qanday sifat ko‘rsatkichlarini bilasiz?
8. IPv4 tarmoqlararo protokolning kamchiligi nimada?
9. IPv6 protokolini kiritish afzalligi nimada?
10. VoIP texnologiyasining vazifasi nima?
11. IPTV texnologiyasining vazifasi nima va u qanday xususiyatlarga ega?
12. Internet tarmog‘ida qanday zamonaviy ilovalar mavjud?
13. IP – optik tarmoqlarda xizmat ko‘rsatish sifatini ta’minlashning qanday xususiyatlari mavjud?
14. DWDM texnologiyasiga asoslangan optik tarmoqlarda IP trafikni uzatish uchun qanday kommutatsiyalash texnologiyalari qo‘llaniladi?
15. IP-over-DWDM tarmoqlarda xizmat ko‘rsatish sifati qanday ta’minlanadi?
16. Xizmat ko‘rsatish sifati bilan bog‘liq bo‘lgan muammolar nima tufayli yuzaga keladi?
17. Xizmat ko‘rsatish sifati bilan bog‘liq bo‘lgan muammolarning qanday yechimlari mavjud?

# 4. MULTIMEDIALI ALOQA TARMOQLARI STANDARTLARI

## 4.1. Xalqaro elektr aloqa tavsiyalari va standartlari

ITU-T turli mamlakatlarning telekommunikatsiya tarmoqlarini o‘zaro bog‘lanishini ta’minlash bilan bog‘liq bo‘lgan tavsiyalarni ishlab chiqarish bilan shug‘ullanadi.

Umuman bu tavsiyalarni standart deb hisoblab bo‘lmaydi, lekin shunga qaramay ko‘pgina mamlakatlar ITU tavsiyasiga xuddi standart kabi qarashadi. Bunday amaliyot elektr aloqa tarmoqlari operatorlari uchun telekommunikatsiya tizimlarini o‘zaro bog‘lanishini ta’minlash, qurilmalarni ishlab chiqaruvchilar uchun esa ularni boshqa mamlakat bozorlarida milliy standartlarga hech qanday o‘zgartirishsiz sotish imkonini beradi.

1855-yilning may oyida Parijda Xalqaro Telegraf Ittifoqini - International Telegraph Union yaratish haqidagi konvensiyaga qo‘l qo‘yilgan. 1932-yil Madridda o‘tkazilgan konferensiyada Xalqaro Telegraf Birlashmasini shunga o‘xshagan radioaloqa masalalari bilan shug‘ullanadigan tashkilot bilan birlashtirish hal qilindi. Natijada ITU (International Telecommunication Union) nomi paydo bo‘ldi. Bu o‘zgartirish ingliz tilida ITU qisqartmasini o‘zgartirishni talab etmadi. 1947-yildan boshlab ITU ning statusi o‘zgardi. U Birlashgan Millatlar Tashkilotining maxsus muassasasiga aylandi. 1948-yildan boshlab ITU ning masshtabi Jenevada joylashgan. O‘zbekiston Respublikasi 1992-yil iyuldan boshlab ITU a’zosi hisoblanadi va a’zolik vazifasini bajarish, axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligiga yuklatilgan. Hozirgi paytda (tuzilishlar bir qator o‘zgargandan keyin) ITU ning asosiy ishchi tashkilotlari uchta sektorda ifodalangan:

- telekommunikatsiyani standartlashtirish (ITU-T);
- radioaloqani standartlashtirish (ITU-R);
- telekommunikatsiyani rivojlantirish (ITU-D).

Uchta sektorning har birida asosiy faoliyat yuritadigan, ITU tavsiyalarini va boshqa xujjatlarni ishlab chiqaruvchi bir qator tadqiqot komissiyalari tuzilgan. Shuni ham aytish joizki, ITU aloqa sohasida standartlashtirishga tegishli bo‘lgan boshqa bir qator xalqaro, Yevropa, Shimoliy Amerika va Osiyo tashkilotlari bilan chambarchas bog‘liq holda ish olib boradi.

ITU tomonidan chiqariladigan, elektr aloqa standartlari sektorining tadqiqot komissiyasi ro‘yxati va tavsiyalarining seriya nomlarini http://www.itu.int saytidan topish mumkin. Bu saytda ITU tomonidan ishlab chiqilgan foydali xujjatlar joylashtirilgan.

1988-yil Yevropa Telekommunikatsiya standartlashtirish instituti – ETSI ta’sis etilgan. Uning standartlari turli milliy telekommunikatsiya tizimlarini moslashuvchanligini ta’minlash bilan bog‘liq, bu esa o‘z navbatida Yevropadagi integratsion jarayonning samarali sharti kabi qaraladi.

Rasman ETSI standartlari faqat Yevropa davlatlari uchun mo‘ljallangan. Yevropadan tashqarida joylashgan ayrim tashkilotlar ETSI a’zosi hisoblanadi. Bu bir qator sabablar bilan bog‘liq, shularning ichida ETSI ning samarali ishi va Yevropani xalqaro telekommunikatsiyani rivojlantirishdagi muhim hissasini aytib o‘tish joiz.

O‘zbekiston Respublikasidan ETSI ning a’zosi, O‘zbekiston Respublikasi axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi tarkibidagi – UNICON.UZ - Ilmiy texnik va marketing tadqiqotlari markazi hisoblanadi.

Standartlashtirish sohasida ETSI ning asosiy ishini texnik komitet olib boradi. Uning ro‘yxati http://www.etsi.org saytida keltirilgan. Bu saytdan ETSI ning tashkiliy va texnik aspekti ishlariga tegishli bo‘lgan mukammal ma’lumotlarni olish mumkin.

ITU va ETSI ko‘pgina muammolar bo‘yicha uyg‘unlikda ishlashi mumkin. Bundan tashqari ular boshqa xalqaro tashkilotlar bilan samarali hamkorlikda ishlaydi. Ko‘p hollarda ITU va ETSI o‘zining ishini, Internet tarmoqlari uchun shuningdek konsorsiumlar va forumlar uchun standartlar ishlab chiqishga javob beruvchi, Xalqaro

standartlashtirish tashkiloti (ISO), Xalqaro elektrotexnik komissiya (IEC), IETF (Internet Engineering Task Force) tashkilotlari bilan muvofiqlashtiradi.

ITU-T va ETSI standartlari tavsiyalariga misollar.

E.800 ga qo‘shimcha, QoS savollari E.860 tavsiyasining “Xizmat ko‘rsatish sathi haqidagi kelishuv” tuzilishi, ITU-T ning E.430 “Xizmat ko‘rsatish sifatini baholash aspekti” tavsiyasini, ITU-T ning Y.1514 “Aloqa xizmatlarini taqdim etish uchun tarmoqning ishlash parametrlari” tavsiyasini, ITU-Tning Y.1540 “IP-paketlarni ko‘chirishni sifat parametrlari” tavsiyasini, shuningdek ITU-T ning Y.1541 tavsiyalarini mundarijasini misol sifatida olish mumkin.

ETSIda QoS savollari bo‘yicha amaliy ishlar olib borilmoqda va shuning natijasida aloqa xizmatlarining sifatiga bo‘lgan umumiy talablarni aniqlovchi ETR 003 texnik hisobotlar va qayd etilgan telefon aloqasi tarmoqlari uchun ko‘pgina QoS ko‘rsatkichlarini aniqlaydigan ETR138 texnik hisobotlar yaratildi (bir yil ichidagi abonent liniyalaridan tushgan shikoyatlar, muvaffaqiyatsiz chaqiriqlar, ulanishni o‘rnatish vaqti, telefon o‘rnatish buyurtmasini bajarish muddati, bunday buyurtmalarni vaqtida bajarilganlik qismi, nosozliklarni sozlash vaqti, kelishilgan muddatda nosozliklarni bartaraf etish qismi).

IP-tarmoqlarida va UFT tarmoqlarida konvergensiyani qo‘llab-quvvatlash uchun, IP-tarmoqlari foydalanuvchilarining turli tuman ilovalari uchun, telefoniya bilan birgalikda, QoSning differensiallashgan ishonchliligini ta’minlash zarur. U oxirdan bu oxirgacha QoSni ta’minlash uchun, IP-tarmoqlarning provayderlari IP-paketlarni uzatish va QoS masalalarini ishlab chiqish parametrlarini umumiy majmuasini kelishishi lozim.

Xalqaro Elektr Aloqa Ittifoqi - ITU-Tning 13 tadqiqot guruhi yaqinda ikkita xalqaro standartni (tavsiyani) ishlab chiqdi.

Birinchi tavsiya - Y.1540, IP-tarmoqlarda paketlarni uzatish uchun ishlab chiqilgan parametrlarning standartlarini aniqlaydi.

Ikkinchi tavsiya - Y.1541, tarmoq interfeyslarini tutashtirishga bo‘lgan talablarning (tarmoq interfeysi network-interface-tonetwork-interface, NI-NI Y.1540 tavsiyalari parametrlari uchun) standartlarini aniqlaydi va IP-tarmoqlar uchun QoSning 6 ta sinfi bo‘yicha talablarni guruhlaydi.

Keyingi 5 ta tarmoq xarakteristikasi, ikki tomonlama xizmat ko‘rsatish sifatiga (manbadan foydalanuvchigacha) ularning ta’siri nuqtai nazaridan eng muhim bo‘lgan ITU-T Y.1540 tavsiyasida qarab chiqiladi. Ularga quyidagilar kiradi:

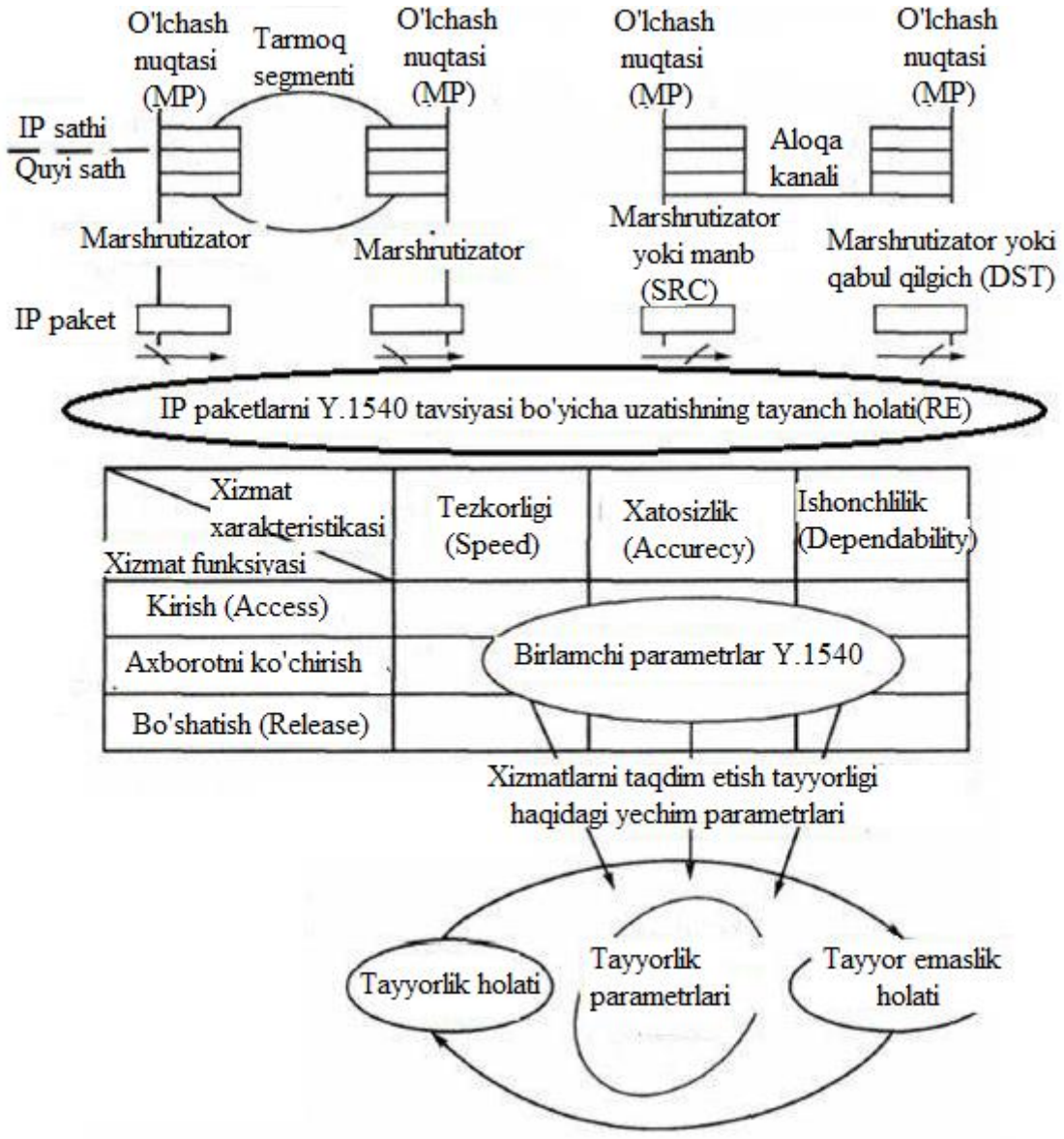
- tarmoqning o‘tkazuvchanlik qobiliyati;
- tarmoq /tarmoq elementlarining ishonchliligi;
- kechikish;
- kechikish variatsiyasi (djitter);
- paketlarning yo‘qolishi.

Tarmoqning o‘tkazuvchanlik qobiliyati (yoki ma’lumotlar uzatish tezligi), sekunddagi bitlarda o‘lchanadi va uzatishning samarali tezligi kabi aniqlanadi. ITU-T Y.1540 tavsiyasida turli ilovalar uchun o‘tkazuvchanlik qobiliyatining qiymatlari keltirilmagan. Lekin uning o‘rniga o‘tkazuvchanlik qobiliyati bilan bog‘liq bo‘lgan parametrlar ITU-T Y.1221 tavsiyasi yordamida aniqlanishi mumkin.

Tarmoq /tarmoq elementlarining ishonchliligi bir qator parametrlar bilan aniqlanadi, shularning ichida ob’ektning ishga qobiliyatlilik vaqtining kuzatish vaqtiga nisbati bilan aniqlanuvchi tayyorgarlik koeffitsienti eng ko‘p qo‘llaniladi. Ideal holatda tayyorgarlik koeffitsienti 1 ga teng bo‘ladi, bu esa tarmoqning tayyorgarligi 100% ekanligini bildiradi.

IP paketlarini eltish parametrlari. Umumiy holda aloqa seansi uchta fazadan tashkil topgan: ulanishni o‘rnatish, axborotni uzatish va uzish. ITU-T Y.1540 tavsiyasida bu fazalardan faqat ikkinchisi – IP paketlarini eltish fazasigina qarab chiqiladi. Bunday yondashish ulanishni o‘rnatishga mo‘ljallanmagan IP tarmoqlarning tabiatini aks ettiradi. ITU-T Y.1540 tavsiyasi IP-paketlarini eltishning quyidagi parametrlarini aniqlaydi:

IPTD (IP packet transfer delay) paketlarni eltishning kechikishi, ikki hodisa orasidagi $t_2$-$t_1$ vaqt, ya’ni tarmoqning kirish nuqtasiga $t_1$ lahzada paketning kirishi va tarmoqning chiqish nuqtasidan $t_2$ lahzada paketning chiqishi kabi aniqlanadi. Bu yerda $t_2 > t_1$ va $t_2 - t_1 \leq T_{max}$.




4.1 rasm. Y.1540 tavsiyasining harakat muhiti va etalon modeli

Umuman, IPTD barcha paketlar uchun manbadan foydalanuvchigacha paketni eltish vaqti kabi aniqlanadi. IP paketlarini eltishning o‘rtacha kechikishi, tanlangan

majmuada uzatilgan va qabul qilingan paketlarning o‘rtacha arifmetik kechikishi kabi aniqlanadi. Yuklamaning oshishi va ulanadigan tarmoq resurslarining kamayishi, tarmoq uzellarida navbatlarning oshishiga olib keladi, natijada eltishning o‘rtacha kechikishi oshadi.

Ovozli ma’lumotlar va birmuncha video axborotlar kechikishga sezuvchan bo‘lgan trafikka misol bo‘lishi mumkin, ayni shunga asosan ma’lumotlar ilovasi kechikishlarga kamroq sezgir. Unda paketni eltishdagi kechikish ma’lum bir qiymatdan $T_{max}$ oshadi va paket tashlab yuboriladi. Bu esa, haqiqiy vaqt ilovalarida (masalan, IP-telefoniyada, videokonferensiya tizimida) ovoz sifatini pasayishiga olib keladi.

$v_k$ – parametri, tarmoqning kirish va chiqish nuqtalari orasidagi IPDV (IP packet delay variation) IP-paketning kechikish variatsiyasi. Bu yerda k indeksga ega bo‘lgan paketlarni eltishdagi $x_k$ kechikish qiymati va tarmoqning xuddi shu nuqtalariga IP paketlarni eltishdagi kechikishning minimal qiymati - $d_{1,2}$ orasidagi $v_k= x_k - d_{1,2}$ farq.

IP paketlarining kechikish variatsiyasi (djitter), muntazam uzatilgan paketlar qabul qiluvchiga muntazam bo‘lmagan vaqt lahzasida yetib kelishi tufayli yuzaga keladi. Masalan, bu IP-telefoniya tizimlarida ovozni buzilishiga olib keladi, natijada nutq noaniq bo‘lib qoladi.

IPLR (IP packet loss ratio) IP-paketlarining yo‘qolish koeffitsienti, tanlangan to‘plamda uzatilgan va qabul qilingan paketlardagi, uzatilgan paketlarning umumiy sonini yo‘qolgan paketlarning yig‘indi soniga nisbati kabi aniqlanadi.

Agar paketlar yo‘qolsa, unda ma’lumotlarni uzatishda qabul qiluvchi tomonning so‘rovi bo‘yicha ular qayta uzatilishi mumkin. VoIP tizimlarida qabul qiluvchiga kechikish bilan kelgan paketlar $T_{max}$ dan yuqori bo‘lsa, tashlab yuboriladi. Bu o‘z navbatida qabul qilinadigan nutqning barbod bo‘lishiga olib keladi.

IPER (IP packet error ratio) IP-paketining buzilish koeffitsienti, buzilish bilan qabul qilingan paketlarning umumiy sonini, muvaffaqiyatli qabul qilingan

paketlarning va buzilish bilan qabul qilingan paketlarning yig‘indisiga nisbati kabi aniqlanadi.

ITU-T Y.1540 tavsiyasi, xalqaro ulanishlarda IP tarmoqlarda amalga oshirilishi kerak bo‘lgan parametrlar uchun me’yorlarning sonli qiymatini aniqlaydi. Bu me’yorlar, xizmat ko‘rsatishning kafolatlangan sifatini ta’minlash uchun ilovalarga va tarmoq mexanizmlariga bog‘liq holda aniqlanadigan QoS sinflari bo‘yicha ajratilgan. 4.1-jadvalda muayyan yuqori tarmoq xarakteristikalari uchun me’yorlar taqdim etilgan.

4.1-jadval

Xizmat ko‘rsatish sifati sinflari bo‘yicha taqsimlangan IP-tarmog‘i xarakteristikalari uchun me’yorlar

| Tarmoq xarakteristikalari | QoS sinflari | | | | | |
|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 |
| IP, IPTD paketlarini eltishdagi kechikishlar | 100 ms | 400 ms | 100 ms | 400 ms | 1ms | M |
| IP, IPDV paketlarini kechikish variatsiyasi | 50 ms | 50 ms | M | M | M | M |
| IP, IPLR paketlarni yo‘qolish koeffitsienti | $1*10^{-3}$ | $1*10^{-3}$ | $1*10^{-3}$ | $1*10^{-3}$ | $1*10^{-3}$ | M |
| IP, IPER paketlarni buzilish koeffitsienti | $1*10^{-4}$ | $1*10^{-4}$ | $1*10^{-4}$ | $1*10^{-4}$ | $1*10^{-4}$ | M |

Izoh: M–me’yorlanmagan

4.1-jadvalda keltirilgan parametrlarning qiymatlari mos holda, o‘rtacha kechikishlar uchun yuqori chegara, djitter, paketlarning yo‘qolishi va buzilishi uchun berilgan. Y.1541 tavsiyasi, xizmat ko‘rsatish sinflari va ilovalar orasida moslik o‘rnatadi, masalan:

0 sinf - djitterga sezuvchan bo‘lgan va interaktivlikning yuqori darajasi bilan xarakterlanuvchi (VoIP, videokonferensiya) haqiqiy vaqt ilovasi;

1 sinf - djitterga sezuvchan bo‘lgan interaktiv (VoIP, videokonferensiya) haqiqiy vaqt ilovalari;

2 sinf- interaktivlikning yuqori darajasi bilan xarakterlanadigan ma’lumotlar tranzaksiyasi (masalan, signalizatsiya);

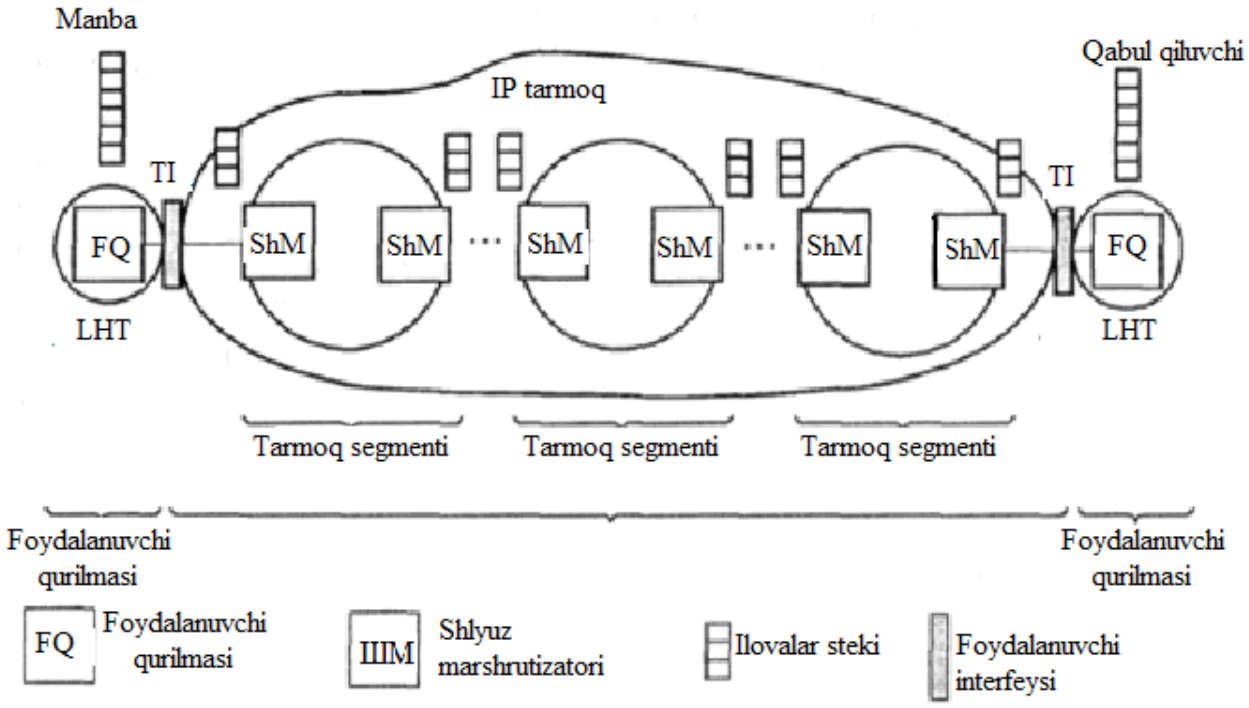
3 sinf - interaktiv ma’lumotlar tranzaksiyasi;

4 sinf - past sathli yo‘qotishlar mumkin bo‘lgan ilovalar (qisqa tranzaksiya, ma’lumotlar massivi, oqimlivideo);

5 sinf- IP tarmoqlaridagi an’anaviy ilova turlari.

**Y.1541 tavsiyasining etalon marshruti.** Y.1541 tavsiyalarida aniqlangan u oxirdan bu oxirga IP ishining xarakteristikalari, 4.2-rasmda ko‘rsatilganidek NI dan NI gacha qo‘llaniladi. IP- tarmog‘ida u oxirdan bu oxirga tarmoq marshruti, IP-paketlarni SRC dan DST gacha transportlaydigan tarmoq segmentlari, uzatish kanallari to‘plamidan iborat.

SRC va DST bilan birgalikda IP sathlarini o‘z ichiga olgan quyi ilovalar, IP-tarmog‘ining qismi kabi qaralishi mumkin. Tarmoq segmentlari operator sohasiga mos keladi va IP-tarmoqlariga ulanish arxitekturasidan iborat bo‘lishi mumkin. Mijoz uskunalari o‘ziga barcha terminal qurilmalarni, masalan xostlarni va boshqa har qanday oxirgi marshrutizatorlarni yoki lokal hisoblash tarmoqlarini birlashtirishi mumkin.




4.2-rasm. QoS vazifasi uchun manbadan qabul qilgichgacha bo‘lgan etalon yo‘l

## 4.2. Multimediali aloqa tarmoqlarining quyi sath protokollari

Quyi sath protokollari (1-4). OTO‘B modelidagi to‘rtinchi transport sathi, quyida joylashgan sathlarni qo‘llash bilan ikkita o‘zaro ta’sirlashuvchi tizimlar orasida axborotlarni uzatishni ta’minlash uchun xizmat qiladi. Bu sath yuqori turuvchi sathdan qandaydir ma’lumotlar blokini qabul qiladi va ularni uzoqdagi tizimlarga aloqa tarmog‘i orqali transportlashni ta’minlaydi. Transport sathidan yuqorida joylashgan sathlar, ma’lumotlar uzatiladigan tarmoqning o‘ziga xos xususiyatlarini hisobga olmaydi, ular faqat o‘zaro ta’sirlashuvchi uzoqdagi tizimlarni biladi. Transport sath, tarmoq qanday ishlashini, qaysi o‘lchamdagi ma’lumotlar blokini qabul qilishini bilishi kerak.

Keyingi uchta quyi sath tarmoq uzellarining ishlashini aniqlaydi. Bu sathning protokollari transport tarmoqga xizmat ko‘rsatadi. Barcha transport tizimlar singari, bu tarmoq axborotlarni transportlaydi, ya’ni uni tashkil etuvchilariga qaramaydi. Bu

tarmoqning asosiy vazifasi – axborotni tez va ishonchli eltishdir. Uchinchi sathning asosiy vazifasi – axborotni marshrutlash, bundan tashqari u axborotli oqimlarni boshqarishni, tashkil qilishni va transport kanallarni qo'llab quvvatlashni ta'minlaydi, shuningdek xizmatlarni taqdim etishni hisobga oladi.

4.2-jadval

Tizim sathlari bajaradigan vazifalar

| Sath | Sath nomi | Sath amalga oshiradigan vazifalar |
|---|---|---|
| 7 | Amaliy | Axborot resurslardan foydalanish yoki taqdim etish. Amaliy dasturlarni boshqarish |
| 6 | Taqdim etish | Amaliy jarayonlardagi axborotlar tarkibidagi ma'noni (qiymat) taqdim etish |
| 5 | Seans | Amaliy jarayonlar orasida o'zaro ta'sirlashish seanslarini o'tkazish va tashkil etish |
| 4 | Transport | Turli usullarda kodlangan axborotlar massivini uzatish |
| 3 | Tarmoq | Axborotlarni kommutatsiyalash va marshrutlash, ma'lumotlar oqimlarini boshqarish |
| 2 | Kanal | Ulanishni o'rnatish, ushlab turish va uzish |
| 1 | Fizik | Kanallarning fizik, mexanik va funksional xarakteristikalari |

Kanalni boshqarish sathi (ikkinchi sath) yoki kanal – jarayonlar kompleksini va fizik ulanish asosida tashkil qilingan ma'lumotlar uzatish kanalini boshqarish usullarini (ulanishni o'rnatish, uni qo'llab quvvatlash va uzish) ifodalaydi. U xatoliklarni topish va to'g'rilashni ta'minlaydi.

Fizik (birinchi) sath – uzatish muhiti bilan o‘zaro aloqani ta’minlaydi. U ulanish, ulanishni qo’llab quvvatlashni va fizik zanjirni (kanalni) o‘chirish uchun talab etiladigan elektrik va mexanik xarakteristikalarni aniqlaydi. Bu yerda fizik kanal orqali har bir bitni uzatish qoidasi aniqlanadi. Kanal bir nechta bitni bir vaqtda (parallel holda) yoki ketma-ket uzatishi mumkin. Sathlarning qisqacha xarakteristikasi 4.2-jadvalda keltirilgan.

Internet ikkita asosiy protokollarga asoslangan – IP protokoli va TCP protokoli. TCP va IP, shuningdek bir qator kuzatuvchi protokollarning yig‘indisi TCP/IP Internet protokollar steki sifatida aniqlanadi.

TCP/IP bazasidagi turli tarmoqlar, Internet muhitini shakllantirib IP marshrutizatorlari yordamida bir-biri bilan ulanadi.

IP protokoli IETF modelini uchinchi sathida joylashgan va bu protokolning vazifasi OSI modelining tarmoq sathi vazifalariga o‘xshash.

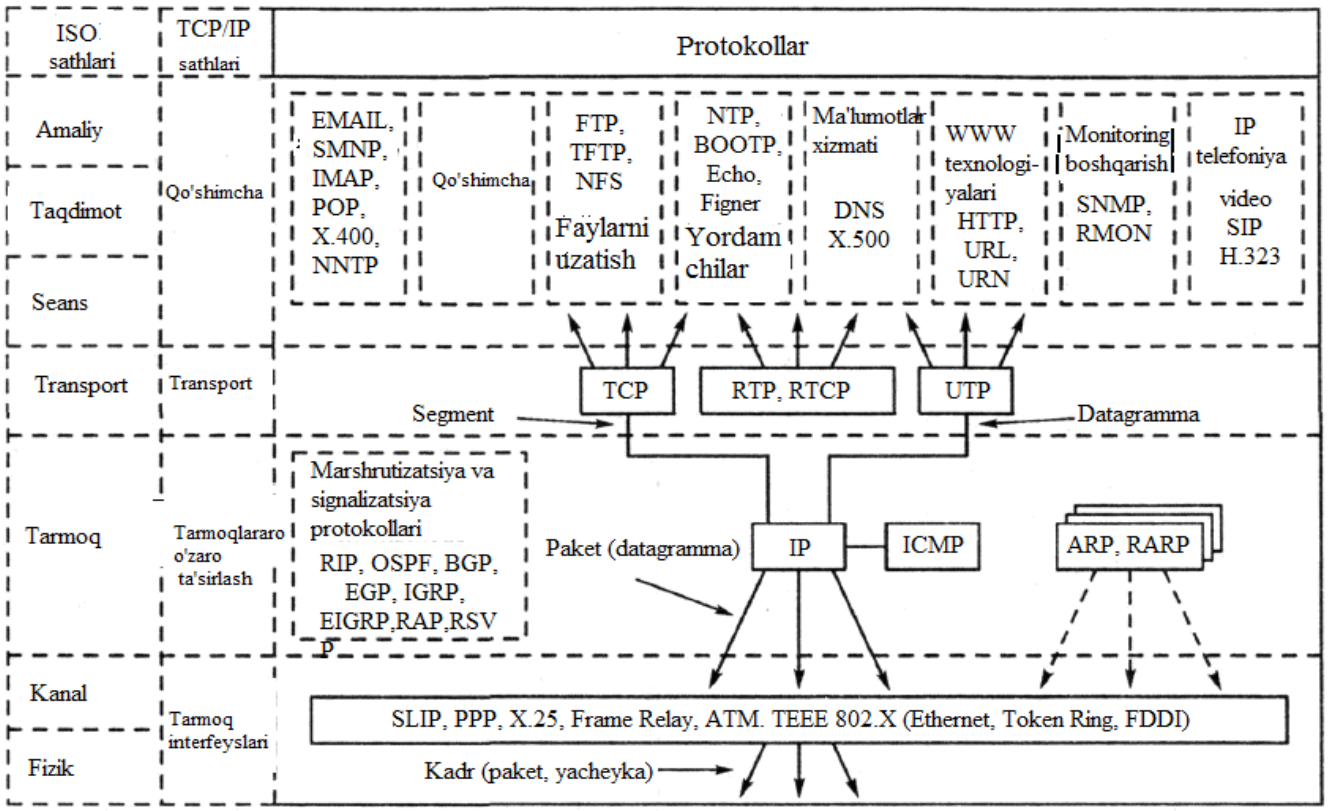
### 4.2.1. Transport sathi protokollari TCP, UDP, RTP

*TCP (Transmission Control Protocol) protokoli.* IP tarmoqlarda transportlashning ishonchliligini oshirish uchun 1974-yilda datagrammani sifatli eltishni ta’minlovchi transport sathidagi TCP protokoli ishlab chiqilgan. TCP protokoli ulanish uchun mo‘ljallangan, shuningdek TCP paketi segment deb ataladi.

*UDP (User Datagram Protocol) protokoli* – Internet tarmoqlarida transport protokolining boshqa namunasini o‘zida ifodalaydi. Shuningdek TCP protokoli singari, UDP protokoli datagrammani eltishni ta’minlaydi. Biroq oxirgi nuqtalar orasida ulanish o‘rnatilmagan rejimda ishlaydi.

Sarlavha va ma’lumotlar maydonidan iborat UDP protokolining paketi, UDP datagrammasi deyiladi. UDP protokoli datagrammani ishonchli yetkazishga moil emas, uning vazifasiga ma’lumotlar uzatishni boshqarish va qabul qilishni tasdiqlash

kirmaydi. Oxirgi bir necha yilda UDP protokoli Internet tarmoqlarida (Voice over IP, VoIP) so‘zlashuv axborotlarini uzatishda keng qo‘llanilmoqda.




4.3-rasm. TCP/IP protokollar stekining tuzilishi

*RTP (Real-time Transport Protocol) transport protokoli.* RFC 1889 va RFC 1890 tavsiyalarida yozilgan haqiqiy vaqt RTP (Real-time Transport Protocol) transport protokoli, haqiqiy vaqtda uzatiladigan ma’lumotlarni ikki tomonlama yetkazish xizmatini ta’minlaydi, masalan interaktiv audio va video trafiklarni. RTP protokoli foydali yuklama turini identifikatsiyasini, paketlar ketma-ketligini raqamlash, vaqt belgisini qo‘yish va yetkazishni nazorat qilishni ta’minlaydi. Protokolda quyidagi vazifalar ko‘rib chiqilgan:

- xatolarni aniqlash;
- axborotni himoyalash;

- tarmoqda paketni kelish vaqtini nazorat qilish;
- kodlash sxemasini identifikatsiyalash;
- etkazishni nazorat qilish.

RTP protokoli, RTCP (RTP Control Protocol) boshqarish protokoli bilan birga ishlaydi. RTCP protokoli VoIP seansi ishtirokchilariga boshqarish paketlarini uzatishni ta’minlaydi. Protokolning asosiy vazifasi shundan iboratki, RTP protokoli bilan taqdim etiladigan xizmat ko‘rsatish sifati sathi haqida ishtirokchilarni xabardor qiladi. RTCP protokoli uzatilgan va yo‘qolgan paketlar soni, kechikish va djitter qiymati haqidagi axborotni yig‘adi.

Turli arxitekturaga ega tarmoqlar orasida paketlarni uzatishni IP stekining asosiy protokoli ta’minlaydi. IP datagrammali protokol paketlarni ishonchli uzatishni kafolatlamaydi. Biroq ko‘pgina tarmoqlar orqali ma’lumotlar uzatishda o‘tkazish qobiliyatini oshiradi.

Shuningdek tarmoq sathida quyidagi protokollar qo‘llaniladi:

- ICMP (Internet Control Message Protocol) boshqarish protokoli, xatoliklar va uzatishdagi uzilishlar haqida tarmoq uzellariga axborot uzatadi;
- adreslar muammolarini yechish protokollari: ARP (Address Resolution Protocol) tarmoq uzelining fizik adresiga (MAC –stansiya adresi) IP adresni o‘zgartiradi; RARP (Reverse Address Resolution Protocol) teskari funksiyani bajaradi, ya’ni MAC adres yordamida IP adresni aniqlaydi.

### 4.2.2. Marshrutizatsiya va signalizatsiya protokollari: RIP, OSPF, IGRP, EIGRP, EGP, BGP

Tarmoq sathining ishini marshrutizatsiya va signalizatsiyaning bir qator protokollari bajaradi: RIP (Routing Internet Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP), BGP

(Border Gateway Protocol), RAP (Routing Access Protocol), RSVP (Resource Reservation Protocol) va boshqalar.

TCP/IP protokollar steki kanal sathida protokollarning katta soni va IP protokolning paketlarini inkapsulyatsiyalaydigan tarmoq texnologiyalari bilan o‘zaro ta’sirlashadi.

*Marshrutlash usullari.* Marshrutizatsiyalash protokollari o‘zida dinamik tarzda rivojlanayotgan Internet protokollarining murakkab guruhini ifodalaydi. Marshrutizatsiya deb – jo‘natuvchidan qabul qiluvchiga axborotni uzatishning optimal yo‘lini qidirish masalasini yechish tushuniladi. Bu masalani yechuvchi qurilma marshrutizator (router) deyiladi. IP-tarmoqlarda marshrutlashning asosiy parametri IP-protokoldagi adres hisoblanadi. Internet tarmog‘i domenlar (domains) yoki o‘zaro bog‘langan o‘zaro avtonom tizimlarning yig‘indisi sifatida tashkil etilgan. Avtonom tizim yagona ma’muriy boshqarish va umumiy marshrutlash strategiyasiga (policy routing) ega bo’lgan IP tarmoqdan iborat. Domenlar chegarasida ichki marshrutlash protokollari qo‘llaniladi (Interior Gateway Protocol, IGP), ular orasida tashqi marshrutlash protokollari (Exterior Gateway Protocol, EGP) qo‘llaniladi.

*RIP protokoli.* RIP protokoli – bu katta bo‘lmagan domenlar uchun mo‘ljallangan ichki marshrutlash protokoli. RIP protokolini birinchi turi RFC 1058, ikkinchisi - RFC 1722 xujjatlarda standartlashtirilgan. RIP protokoli axborotni uzatish uchun UDP (520 port) protokolini qo‘llaydi. RIP axboroti tarmoqning IP-adresidan va qadamlar sonidan (marshrutizatorlardan) iborat. Qadamlarning maksimal soni -15 ta. RIPning bitta xabarida 25 ta tarmoqlar haqida axborot bo‘lishi mumkin. RIP ishlaydigan marshrutizator boshqa marshrutizatorlardan RIP axborotini olib, boshqa tarmoqlarga yo‘nalishlar yozilgan o‘zining marshrutlash jadvalini har 30 daqiqada yangilaydi va ular yordamida tarmoq bo‘ylab paketlarning harakatlanishini bajaradi.

Protokolning kamchiligi:

- har doim eng samarali marshrutni tanlamaydi;

- sekin moslashishi tufayli logik ilmoqlar hosil bo‘ladi va marshrutizator ishida to‘xtab qolishdan keyin jadval sekin qayta yangilanadi;

- tarmoqqa yuklanadigan katta sondagi xizmat axborotlarini (marshrutlash jadvali) keng eshittirishli jo‘natmalari qo‘llaniladi;

- marshrutlash domenini o‘lchash chegaralangan (15 o‘tishlar);

- tarmoq tagi adreslari bilan ishlamaydi va avtonom tizimlarni farqlamaydi.

*OSPF protokoli* RFC 1370, 1578, 1793, 1850, 2328 xujjatlarda standartlashtirilgan. Kanallar holati algoritmini qo‘llash asosida ichki va tashqi marshrutizatlash uchun qo‘llaniladi. Bir nechta zonadan iborat bo‘lgan avtonom tizimga xizmat ko‘rsatishi mumkin. OSPF protokoli RIP protokolidan yetarli darajada samaralidir. OSPF protokoli asosida ishlaydigan marshrutizator, xizmat ko‘rsatish sifatini xarakterlaydigan metrikali tarmoq grafasini tahlil etib, yo‘nalishlarni optimallashtirish muammolarini yechadi.

Metrikalarning asosiy parametrlari quyidagilar hisoblanadi: o‘tkazish qobiliyati, kechikish, ishonchlilik, qo‘shimcha parametrlarga kanalning yuklanishi va xavfsizlik. Faqat tarmoq topologiyasi o‘zgarganda marshrutizator axborotlar bilan almashadi. RIPga qaraganda OSPF protokoli tez yo‘nalish jadvalini qayta tuzadi.

OSPF protokolining asosiy afzalliklariga quyidagilar kiradi:

- tarmoq topologiyasi o‘zgarganda qisqa axborotlarni guruhli uzatishni qo‘llash. Bu esa tarmoqni samarasiz yuklanishini kamaytiradi;

- o‘tkazish qobiliyatiga bog‘liq holda axborotlarni parallel kanallar bo‘yicha taqsimlashni ta’minlaydi. Bu esa butunlay tarmoq ishini yaxshilaydi.

*IGRP va EIGRP protokollari.* Bu protokollar Cisco Systems firmasi tomonidan ishlab chiqilgan va ichki marshrutlash uchun qo‘llaniladi. IGRP “vektor-masofa” algoritmini qo‘llaydi, RIP protokoliga qaraganda qisman yaxshi xarakteristikalarga ega:

- murakkab topologiyali tarmoqlarda ishonchli ishlaydi;

- RIPga qaraganda eng yaxshi moslashishga ega;

- xizmat axborotlarini uzatish hajmini qisman kamaytiradi;
- bir xil metrikali kanallar orasida axborotni taqsimlaydi.

Protokol metrikasiga kanalning quyidagi parametrlari kiradi: o‘tkazish qobiliyati, kechikish, yuklanish, ishonchlilik. Bu parametrlar keng oraliqlarda o‘zgarishi mumkin. Masalan, o‘tkazish qobiliyati 1200 bit/s dan 10 Gbit/s gacha o‘zgarishi mumkin.

EIGRP protokoli “vektor-masofa” va “kanallar holati” algoritmlarining barcha afzalliklarini birlashtiradi. Protokol – tarmoq topologiyasi o‘zgarganidan so‘ng marshrutizatorga ishini tez qayta yangilash imkonini beruvchi – taqsimlangan yangilash algoritmi bazasida (Distributed Update Algorithm, DUAL) amalga oshirilgan.

Protokol quyidagilarga ega:

- qo‘shnini topish imkoni;
- DUAL algoritmi;
- axborotni IP ga mukammal kiritish mexanizmi.

*EGP va BGP protokollari* – Internet tarmog‘ini tashqi marshrutlash protokollariga kiradi. Marshrutlashni ichki protokollari yordamida tizim haqidagi axborotni yig‘uvchi, turli avtonom tizimlarni ajratilgan marshrutizatorlari EGP protokoli yordamida o‘zaro ta’sirlashadi. EGP prtokolining kamchiliklariga quyidagilar kiradi: metrika qo‘llanilmaydi, ya’ni intellektual marshrutlash bajarilmaydi, yo‘nalishlar ilmog‘ini hosil bo‘lishi kuzatilmaydi, xizmat axborotlari katta o‘lchamga ega.

Oxirgi vaqtlarda EGP o‘rniga mukammalroq BGP protokoli qo‘llanilmoqda, o‘z navbatida xizmat axborotlarini uzatish uchun TCP protokoli qo‘llaniladi. TCP protokoli marshrutli axborotni yetkazishni kafolatlaydi. BGP to‘liq EGP protokolining kamchiliklarini bartaraf etadi. Metrika sifatida kanalda uzatish tezligi, uning ishonchliligi qo‘llaniladi. Hozirda BGP (3-tur) – bu oxirgi avtonom tizimlarga yo‘nalishni aniqlaydigan Internet tarmog‘ining asosiy protokoli hisoblanadi.

### 4.2.3. Tarmoq interfeysi protokollari X.25, Fram Relay

*X.25 protokoli.* X.25 protokoli asosidagi paketlarni kommutatsiyalash tarmog‘i – 1970 yillar oxirlarida, analog uzatish muhiti orqali ikkita uzoqdagi punktlar orasida ma’lumotlar uzatishni ta’minlash maqsadida ishlab chiqilgan. Ularni qo‘llanilishining asosiy muhiti terminallar va ishchi kompyuterlar orasidagi aloqa bo‘lgan. ITU-T da ishlab chiqilgan X.25 protokoli OTO‘B modelining uchinchi sathining protokoli hisoblanib, tarmoq orqali paketlarni uzatishni ta’minlaydi. X.25 protokolda axborotni butunligini saqlash masalasi tarmoqga qo‘yilgan, ya’ni halaqitlarga chidamli kodlarni qo‘llash, so‘rash va tarmoq uzellari orasida paketlarni takrorlash yo‘llari orqali erishilgan.

Qisqa masofali telefon tarmoqlari uchun ishlab chiqilgan X.25 protokollarida xatolik ehtimolligi ($10^{-3}$ - $10^{-4}$) katta (ma’lumotlar uzatish uchun), bu esa paketlarni yo‘qolishiga va ularni takror uzatish zaruratiga olib keladi. Yuqorida sanab o‘tilgan muammolarni yechimini Fram Relay texnologiyasi ta’minlaydi, ya’ni o‘zida X.25 protokolini soddalashtirilgan turini ifodalaydi.

*Fram Relay protokoli.* Fram Relay protokoli (kadrlarni kommutatsiyalash/retranslyatsiyalash) 90-yillar boshida standartlashtirilgan, kanalda xatolik ehtimolligi $10^{-6}$ tartibda. X.25 texnologiyasi singari Fram Relay protokoli ulanishni o‘rnatish uchun mo‘ljallangan. Fram Relay protokoli OTO‘B modelining birinchi ikkita sathida amalga oshiriladi. Fram Relay texnologiyasida protokolli bloklar sifatida kadrlar qo‘llaniladi. Fram Relay texnologiyasi kadrlarida foydali yuklama maydonining uzunligi 4096 baytgacha oshirilgan, X.25 protokolida esa 256 bayt.

## 4.3. Multimediali aloqa tarmoqlarining yuqori sath protokollari

*Yuqori sath protokollari (5-7). Amaliy sath protokoli* asosiy protokol hisoblanadi, aynan u tufayli qolgan barcha protokollar mavjuddir. U amaliy deyiladi, chunki u bilan boshqa ochiq tizimlarda joylashgan amaliy jarayonlar bilan birgalikda qandaydir masalani yechishi kerak bo‘lgan tizimning amaliy jarayonlari o‘zaro ta’sirlashadi. OTO‘B etalon modelning amaliy darajasi, ochiq tizimlar qandaydir oldindan ma’lum bo‘lgan masalani birgalikda yechishi jarayonida almashadigan ma’lumotlarning mazmuniy tarkibini aniqlaydi.

Oltinchi daraja *taqdim etish* darajasi deyiladi. U asosan uzatiladigan ma’lumotlarni kerakli tarmoq shaklida taqdim etish jarayonini aniqlaydi. Bu tarmoq turli oxirgi punktlarni (masalan, turli kompyuterlarni) birlashtirishiga bog‘liq. Agar tarmoqdagi barcha oxirgi punktlar bitta turda bo‘lganida edi, taqdim etish darajasini kiritish kerak bo‘lmas edi. Har xil turlardagi kompyuterlarni birlashtiradigan tarmoqda, tarmoq bo‘ylab uzatiladigan axborotlar ma’lum yagona taqdim etish shakliga ega bo‘lishi kerak. Aynan bu shaklni oltinchi daraja protokoli aniqlaydi.

Protokollarning navbatdagi beshinchi darajasi *sessiyalar* yoki *seanslar* protokoli deyiladi. Uning asosiy vazifasi amaliy jarayonlar orasidagi o‘zaro ta’sirlashish – amaliy jaryonlarning o‘zaro ta’sirlashishi uchun ularni ulash usullarini tashkil etish, jarayonlarning o‘zaro ta’sirlashishi va “ulanishni uzish” vaqtlari jarayonlari orasida ma’lumotlarni uzatishni tashkil etish hisoblanadi.

So‘ngra pastki makro sathning to‘rtta protokoli keladi. Pastki sath protokollarining asosiy vazifasi ma’lumotlarni tezkor va ishonchli uzatish hisoblanadi. Shuning uchun pastki sath protokollari ba’zan transport tarmog‘i protokollari deyiladi. Transport tarmog‘iga chiqish port orqali amalga oshiriladi. Har bir jarayon o‘z portiga ega bo‘ladi. Transport tarmog‘iga kirishdan oldin foydalanuvchining ma’lumoti, uni yaratgan jarayonning sarlavhasini oladi. Transport tarmog‘i pastki sath protokollarini qo‘llab, jarayon (xabar) sarlavhasiga ega foydalanuvchining ma’lumotini manzilga

(adresga) uzatishni ta’minlaydi. Internet protokollarining arxitekturalari to‘rtta sathli hisoblanadi. Keyinroq paydo bo‘lgan ISO etalon modeli protokollarining yetti sathli arxitekturasini TCP/IP ning keyingi rivojlanishi sifatida qarash mumkin. Haqiqatdan ham, ikkkita arxitekturaning farqi shundan iboratki, TCP/IP arxitekturasidagi OSI modelining uchta yuqori sathlari (amaliy, taqdim etish, seanslar) bitta amaliy darajaga birlashtirilgan (4.3-rasm). TCP/IP tarmoq interfeyslarining sathi, OSI modelining ikkita kanalli va tarmoq sathlariga mos keladi.

TCP/IP amaliy sathi quyidagi an’anaviy xizmatlarni qo‘llab-quvvatlaydi:

- elektron pochtani uzatishning oddiy protokoli SMNP (Simple Mail Transfer Protocol) yordamida ishlatiladigan elektron pochta va yangiliklarni almashish;
- IMAP (Internet Massage Access Protocol), POP (Post Office Protocol) va X.400 pochta protokollari; NNTP (Network News Transfer Protocol) yangiliklarni almashish tarmoq protokoli;
- Telnet protokoli yordamida amalga oshiriladigan virtual terminal;
- fayllarni uzatish FTP (Fail Transfer Protocol), TFTP (Trivial Fail Transfer Protocol) NFS (Network File Systems) protokollari yordamida amalga oshiriladi;
- ma’lumotnoma xizmatlari DNS (Domain Name System) domen nomlari va X.500 tizimlari yordamida amalga oshiriladi;
- yordamchi protokollar: shaxsiy identifikatorlarni olish;
- BOOTR, vaqt - NTP (Network Time Protocol), diagnostika;
- Echo va tizim haqidagi ma’lumotlar – Finger.

1990-yillar o‘rtalarida URL (Universal Recourse Locator) va URN dan (Universal Recourse Names) foydalanib gipermatnni uzatish protokoliga HTTP asoslangan WWW (World Wide Web) texnologiyasi bazasidagi xizmatlar faol joriy etildi. Bugungi kunda SIP (Session Initiation Protocol), RTP (Real-time Protocol), RTCP (Real-time Transport Control Protocol) protokollari, H.323 tavsiyalari asosidagi paketli IP-telefoniya xizmatlari ommaviy hisoblanadi.

Stekdagi alohida o‘rinni quyidagi monitoring va boshqarish protokollari egallaydi:

- SMNP (Simple Management Transfer Protocol) –boshqaruv uzatishni oddiy protokoli ;
- RMON (Remote Monitoring) – masofaviy monitoring.

Bu protokollar yordamida tarmoqning holati kuzatiladi va uni ma’murlashtirish o‘tkaziladi.

*FTP fayllarni qayta jo‘natish protokoli.* Olisdagi serverda joylashgan ma’lumotlar fayllariga ulanish usullaridan biri mijozning so‘rovi bo‘yicha fayl nusxasini uzatish hisoblanadi. Internet tarmog‘ida bu maqsad uchun FTP (File Transfer Protocol) standart protokoli – fayllarni qayta jo‘natish protokoli qo‘llaniladi. Eng eski protokollardan biri hisoblanadigan FTP protokoli (u oldingi asrning 70 - yillarning boshlarida ishlab chiqilgan) ilovalar sathi protokollariga kiradi va ma’lumotlarni uzatish uchun TCP transport protokolidan foydalanadi.

FTP protokoli mijozlar (mijozlar guruhi) va ma’lumotlarni saqlaydigan server (FTP serveri) orasida ma’lumotlar fayllarini almashish uchun qo‘llaniladi, binobarin, har bir oxirgi nuqta fayllarni uzatish va so‘rash/olish imkoniyatiga ega bo‘ladi. Bunday fayllar matnlar, grafik tasvirlar, tovushlar, video va multimediali ma’lumotlar bo‘lishi mumkin. FTP protokoli foydalanuvchining (mijoz) kompyuteriga dasturiy ta’minotni yuklash uchun ham ishlatiladi. FTP protokoli yordamida foydalanuvchi oladigan fayllarni to‘g‘rilashi (o‘chirishi, qayta nomlashi, ulardan nusxa ko‘chirishi va h.k.) mumkin. Ko‘pgina FTP-serverlarda yozish uchun ochiq bo‘lgan va server orqali fayllarni olishni ta’minlaydigan katalog (incoming, upload nomlarli va boshqalar) mavjud. Bu foydalanuvchilarga serverni yangi ma’lumotlar bilan to‘ldirishga imkon beradi.

XX asrning 90-yillar boshlanishigacha FTP protokoliniing hissasiga Internet tarmog‘idagi trafikning taxminan yarmi to‘g‘ri kelgan. Bugungi kunda ham protokol

olisdagi serverlar va xostlarga ulanish uchun qo‘llanilmoqda, lekin uning o‘rniga Butun Dunyo To‘ri texnologiyasiga asoslangan ulanish usullari kirib kelmoqda.

*HTTP gipermatnli xabarlarni yuborish protokoli va Butun Dunyo To‘ri.* 1989 yilda Tomas Berners-Li Jenevadagi Yadro tadqiqotlari bo‘yicha Yevropa kengashida (SERN) ishlashi bilan endi Butun Dunyo To‘ri (World Wide Web) sifatida ma’lum bo‘lgan loyihani taklif etdi. Loyihani amalga oshirish uchun Tomas Berners-Li, ularsiz zamonaviy Internetni tasavvur qilish mumkin bo‘lmagan uchta asosiy vositani - URI identifikatorlari, HTTP protokoli va NTML tilini ishlab chiqdi.

Texnik nuqtai nazardan WWW ni HTTP sifatida ma’lum bo‘lgan yagona protokol yordamida muloqot qiladigan ko‘pgina mijozlar va serverlar sifatida qarash foydali bo‘ladi. Butun Dunyo To‘rida gipermatnni yaratish, saqlash va aks ettirishni osonlashtirish uchun HTML gipermatnni belgilash tili qo‘llaniladi. HTTP va HTML protokollarining kombinatsiyasi matnlar, grafikalar, tovush, video va boshqa multimediali fayllarni Internet global tarmog‘i orqali yetkazishni ta’minlaydi.

*SIP protokoli.* IETF da VoIP tizimi uchun signalizatsiya protokollarini yaratish sohasidagi ishlar *draft-ietf-mmusic-cip-OO* spetsifikatsiyasini ishlab chiqilishi bilan boshlandi, bunda keyinchalik SIP/1.0 nomini olgan *Session Invitation Protocol* protokoli tavsif etilgan.

Bu hujjat faqat aloqa seansini o‘rnatilishiga so‘rovni spetsifikatsiyalaydi, lekin istiqbolda bu spetsifikatsiya o‘sha vaqtda yaratilgan konferensiyalarni multimediali arxitekturaga integratsiyalanishiga yo‘naltirildi, bu hujjatning nomi *MMUSIC - Multiparty Mulimedia Session Control*.

SIP protokoli foydalanuvchilar orasida aloqa seanslarini o‘rnatish uchun qo‘llaniladi.

*H.323 protokoli.* IP-telefoniya tarmoqlarini qurish uchun birinchi tavsiya H.323 tavsiyasi bo‘ldi. ITU tarixan UFTT muammolari bilan shug‘ullandi va taklif etilgan tavsiya haqiqatda IP-tarmoq ustiga qo‘yilgan ISDN (Integreted Services Digital Network) tarmog‘ini aniqlagan. Xususan, IP-telefoniya tarmog‘ida H.323 bo‘yicha

ulanishni o‘rnatish jarayoni Q.931 tavsiyaga asoslanadi va ISDN tarmoqlardagi jarayonga deyarli aynan o‘xshash bo‘ladi.

H.323 tarmog‘ining asosiy qurilmalari terminal, shlyuz va konferensiyalarni boshqarish qurilmasi hisoblanadi.

*SMTP elektron pochta protokoli.* Elektron pochta IP-tarmoqlardagi eng eski ilovalardan biri hisoblanadi. Bugungi kunda elektron pochta orqali ma’lumotlarni almashish kuniga millionlab insonlar tomonidan qo‘llanilmoqda. Mijoz va server orasidagi ma’lumotlarni almashishning yana bir shakli hisoblanadigan bu almashish SMTP (Simple Mail Transfer Protocol – pochta xabarlarini yetkazishning oddiy protokoli) protokoli yordamida qo‘llaniladi. RFC 822 tasnifi xabarning ikki qismini – sarlavha va asosni aniqlaydi. Har ikkala qismlar 7-razryadli ASCII kodi bilan kodlanadi. Shaxsiy pochta manzillari <username@domain> (foydalanuvchini ismi@tarmoq osti) ko‘rinishidagi formatga ega bo‘ladi. Pochta qutilarining bu manzillari SMTP sathida taniladi.

Odatda pochta xabari mijozdan SMTP lokal serveriga uzatiladi, ya’ni mijozlarning so‘rovi bo‘yicha pochtaning yetkazilishiga javob beradi. Serverda pochtaning qayta ishlanish jarayoni, har bir yuboruvchi va oluvchining manzili, shuningdek yuborish vaqtiga ega bo‘lgan keluvchi xabarlarni to‘plashdan iborat. Dastlabki xabarni olgan lokal server yuborish punktidagi olisdagi serverning IP-manzilini identifikatsiyalaydi va bu olisdagi server bilan TCP seansini o‘rnatishga urinishni amalga oshiradi. Ulanish o‘rnatilganidan keyin, yuborish serverida pochta xabaridan nusha ko‘chiriladi. Server-yuboruvchi muvaffaqiyatli uzatishga tasdiqlanishni olishi bilan, xabar lokal server xotirasidan o‘chiriladi. Keyin olisdagi foydalanuvchi o‘z serveriga ulanishni olishi va yetkazilgan xabarni qabul qilishi mumkin.

*MIME protokoli.* SMTP protokolini ishlab chiqishda elektron pochta faqat oddiy matnni uzatish uchun foydalanilishi ko‘zda tutilgan. 1993 yilda RFS 822 tasnifi har xil turlardagi ma’lumotlar – audio, video, Word hujjatlarini uzatishni ta’minlash

uchun kengaytirilgan. Bu maqsadlar uchun MIME (Multiprpose Internet Mail Extension – Internetning ko‘p maqsadli pochta kengaytirilishi) qo‘llaniladi. MIME protokoli elektron pochta yordamida har xil turlardagi ma’lumotlarni, shu jumladan ASCII kodidan farqli bo‘lgan kodlash turi qo‘llaniladigan tillardagi matnlar, musiqa, grafika va filmlarni uzatish mexanizmlarini aniqlaydi. MIME formatini o‘zgartirish odatda elektron xabarlarni uzatishda va qabul qilishda pochta serverlari yoki mijoz pochta dasturlari orqali amalga oshiriladi.

## Nazorat savollari

1. Qanday xalqaro elektr aloqa standartlarini bilasiz?
2. Multimediali aloqa tarmoqlarining standartlarini ayting?
3. O‘zbekiston Respublikasi qaysi standartlashtirish tashkilotlarga a’zo hisoblanadi?
4. O‘zbekiston Respublikasida telekommunikatsiya sohasi bo‘yicha qaysi standartlashtirish tashkilotlari javob beradi?
5. ITU-T Y.1540 tavsiyasi qanday standartlarni aniqlaydi?
6. ITU-T Y.1541 tavsiyasi qanday standartlarni aniqlaydi?
7. Quyi sath protokollarining vazifasi nimadan iborat?
8. Transport sathi protokollarining vazifasini tushuntiring.
9. TCP, UDP, RTP – transport protokollarini bir-biridan farqi nimada?
10. Marshrutizatsiya va signalizatsiyani qanday protokollari mavjud?
11. Tarmoq sathi protokollarining vazifasini tushuntiring.
12. TCP/IP ni amaliy sathi qanday xizmatlarni amalga oshiradi?
13. RIP – protokolining vazifasi va xususiyatlarini tushuntiring.
14. OSPF - protokolining vazifasi va xususiyatlarini tushuntiring.
15. FTP – prtokolining vazifasi nimadan iborat?

# 5. MULTIMEDIALI SIGNALIZATSIYA VA SINXRONIZATSIYA TIZIMLARI

## 5.1. Telefon aloqada signalizatsiyaning vazifasi

“Signalizatsiya” atamasining ta’rifi ITU tavsiyalarida keltirilgan. Signalizatsiya deb - ulanishni o‘rnatish va tugatish, shuningdek tarmoqni boshqarish va chaqiriqqa xizmat ko‘rsatish uchun maxsus mo‘ljallangan axborotlar almashish (avtomatik aloqada) tushuniladi.

Telefoniyada tarmoq ierarxiyasi nuqtai nazaridan ikki turdagi signalizatsiyani ajratish qabul qilingan: abonent va stansiyalararo. Ko‘pincha yana bir sinf kiritilgan – stansiya ichi signalizatsiyasi.

Signalizatsiya tizimini klassifikatsiyalashning yana bir foydali usuli, uzatilayotgan axborot vazifasiga asoslangan. Bu nuqtai nazardan odatda signallarni uchta turi ajratiladi:

- akustik, chaqiriqqa xizmat ko‘rsatishni (masalan, “Stansiya javobi” va “Chaqiriqni jo‘natish nazorati”) asosiy fazalari haqida abonentni xabardor qiladi;

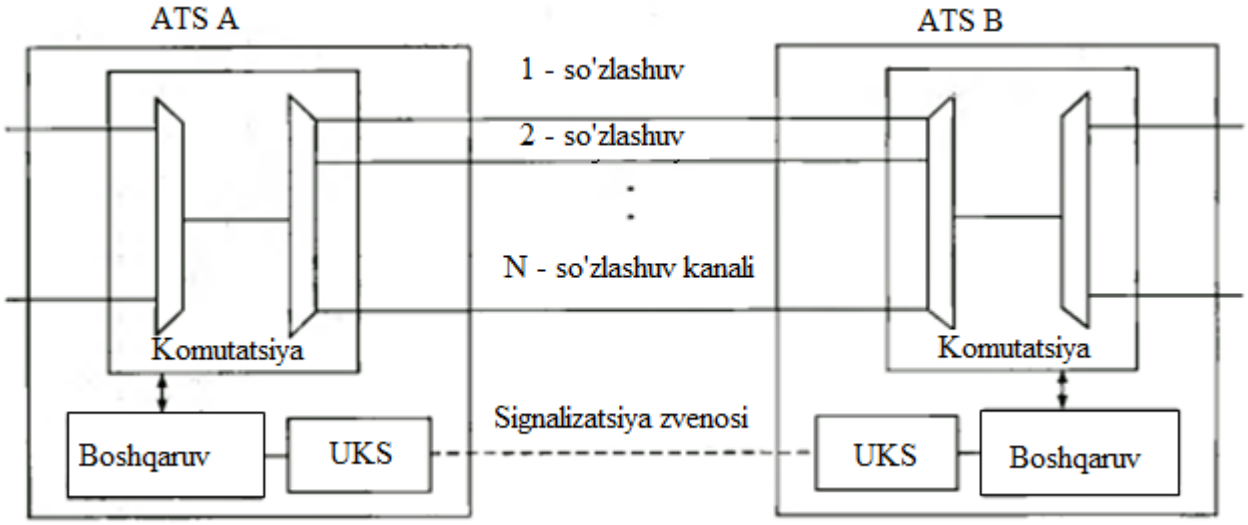
- liniyali, ulanishni o‘rnatish va tugatish jarayonida (jumladan, “Bandlik” va “Abonent javobi”) kommutatsiya qurilmasi va kanallar holatini aniqlaydi;

- boshqaruvchi, kanalli kommutatsiyaga ega bo‘lgan qayd etilgan telefon aloqa tarmoqlarida qo‘llaniladigan, stansiyalararo signalizatsiya aloqasini tashkil etish uchun zarur bo‘lgan, nomer va adres haqidagi xabardan iborat.

Hozirgi vaqtda UFTTda bitta va ikkita ajratilgan signalli kanal (ASK) bo‘yicha signalizatsiya qo‘llaniladi. Transport tarmoq raqamli uzatish tizimi (RUT) bazasi asosida qurilgan holatlarda, odatda ikkita ASKli signalizatsiya qo‘llaniladi. ASKni tashkil etish uchun, resurslarni taqsimlash algoritmi standartlashtirilgan, ya’ni IKM-30/32 uzatish tizimining 16-kanal intervalida hosil qilingan.

Impulslar va pauzalar yordamida chaqiruvchi abonent tergan nomerni uzatish, ulanishni o‘rnatish jarayonini sekinlashtiradi. Bu kamchilikni kamaytirish maqsadida ko‘p chastotali signalizatsiya kiritilgan. Unda qo‘llaniladigan ko‘p chastotali kodni signalli kombinatsiyalari ikkita sinusoidal signallardan iborat. Uzatiladigan signallar, oltita imkoniyatlidan ikkita turli chastota nominalini qo‘llaydi. Mos keladigan usul ko‘pincha “6 dan 2” kodi deyiladi.

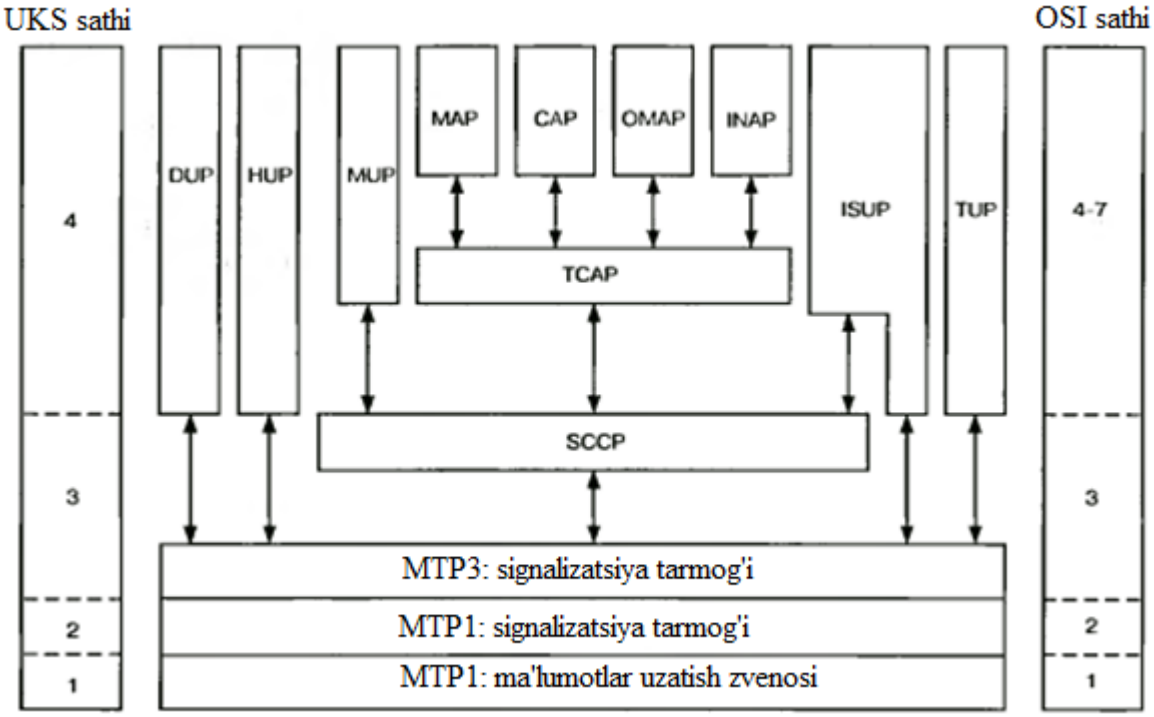
Umumkanal signalizatsiya (UKS) tizimi modelida funksional sathlarni ajratish prinsiplari bir qator spetsifik xususiyatlarga ega. Buning natijasida u OSI modelidan farqlanadi. 5.2-rasmda UKS tizimining modeli keltirilgan va standartlashtirish bo‘yicha xalqaro tashkilot tomonidan qabul qilingan, aynan o‘xshash tuzilishdan uni farqi ko‘rsatilgan. Bu yetti sathdan iborat tuzilish OSI abbreviaturasi bo‘yicha yaxshi ma’lum.




5.1-rasm. Umumiy kanal bo‘yicha signalizatsiya

UKS tizimining uchta quyi sathi MTP (Message Transfer Part) xabarini tashuvchi tarmoq tagini hosil qiladi. Bu MTP sathlarning funksional imkoniyatlari, avval mavjud bo‘lgan uchta “nimtarmoq – foydalanuvchilar” signalli yuklamaga xizmat ko‘rsatish uchun yetarli edi:

- ma’lumotlar uzatish tarmog‘i - DUP (Data User Part);
- xendover jarayoni - HUP (Handover User Part);
- telefon tarmog‘i - TUP (Telephone User Part).




5.2-rasm. Umumkanal signalizatsiya tizimining modeli

Signalli ulanishlarni boshqarish nimtarmoq SCCP (Signalling connection control part) OSI modelining 3-sathigacha MTRZ vazifalarini to‘ldiradi va keyingi “nimtarmoq – foydalanuvchilar” ishi uchun zarur:

- NMT-450 standartidagi harakatlanadigan aloqa - MUP (Mobile User Part);
- integral xizmat ko‘rsatuvchi raqamli tarmoq - ISUP (ISDN User Part).

Shuningdek SCCPning funksional imkoniyatlari, TCAP (Transaction Capabilities Application Part) tranzaksiyalarini qo‘llab-quvvatlash uchun nimtarmoq qo‘shimchalarida qo‘llaniladi. O‘z navbatida, TCAP nimtarmoq keyingi amaliy nimtarmoqlarini ishlashi uchun zarur:

- GSM standartidagi mobil aloqada - MAP (Mobile Application Part);

- ekspluatatsion boshqarish – OMAP (Operations, Maintenance and Administration Part);
- intellektual tarmoqlar - INAP (Intelligent Network Application Protocol);
- CAMEL protokoli - CAP (CAMEL Application Protocol).

## 5.2. Signalizatsiya tarmog‘ining tuzilishi

Dasturiy boshqarishga ega bo‘lgan kommutatsiya stansiyasini *signalizatsiya punkti* SP (Signaling Point) sifatida ko‘rish mumkin.

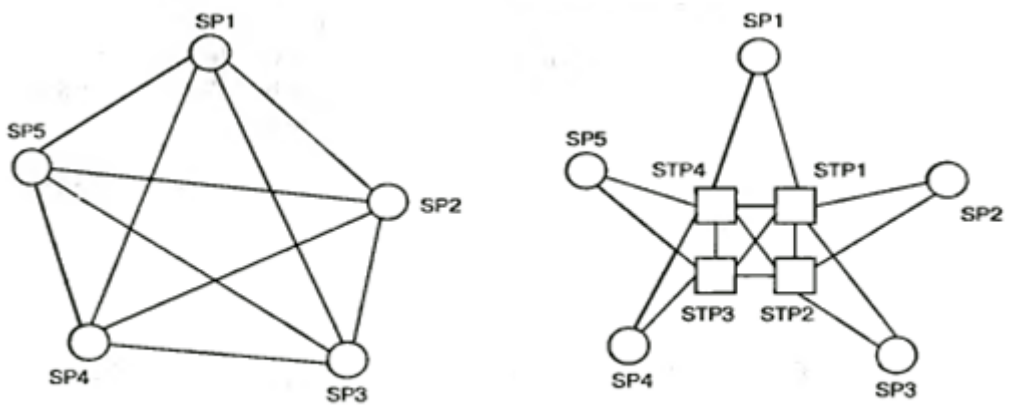
Signalizatsiya punkti signalli xabarlarni izohlash, shakllantirish, uzatish va qabul qilish vazifalarini bajaradi. Signalizatsiyaning ba’zi bir punktlari signalizatsiya signalini bir zvenodan boshqasiga o‘tishi vazifasini bajaradi. Ular signalizatsiyaning tranzit punktlari - STP (Signaling Transfer Point) deyiladi. SP va STP ning yig‘indisi, shuningdek ularni bog‘lovchi signalli zvenolar, o‘ziga hos tarmoqni hosil qiladi. U signalizatsiya tarmog‘i deyiladi.

Orasida signalli xabar almashish imkoniyati bo‘lgan har qanday ikkita SP, *bog‘langan* deyiladi. Ikkita SP ni bog‘lanishi signalli zvenolarning to‘g‘ri tutami yoki STP yordamida tranzit tashkillashtirilgan signalizatsiya tarmog‘i vositasida ta’minlanadi. Birinchi holatda ikkita SP (signalizatsiya tarmog‘i tuzilishi nuqtai nazaridan) - *o‘zaro bog‘langan*, ikkinchi holatda – *o‘zaro bog‘lanmagan* hisoblanadi. Signalizatsiya tarmog‘ida o‘zaro bog‘langan va o‘zaro bog‘lanmagan SPlarning mavjudligi shundaki, unda funksionallashni turli rejimlarini qo‘llash imkoniyati borligidir.

Zamonaviy signalizatsiya tarmoqlarida uchta ishlash rejimi qo‘llanilishi mumkin: *bog‘langan*, *bog‘lanmagan* va *kvazibog‘langan*. Kvazibog‘langan rejim bog‘lanmagan rejimni alohida holatini o‘zida ifodalaydi.

Tarmoq orqali o‘tuvchi signalli axborot yo‘li avvaldan belgilanadi va qaysidir vaqt davrida qayd etilgan hisoblanadi. Amaliyotda signalizatsiya tarmog’ining bog‘langan va kvazibog‘langan rejimlari qo‘llaniladi.

Bog‘langan va kvazibog‘langan tarmoqlarni tashkil qilish namunasi 5.3-rasmda keltirilgan. Ikkala holat uchun ham umumkanal signalizatsiya tizimi telefon tarmog‘i uchun yaratiladi deb tahmin qilinadi, ularda beshta kommutatsiyalash stansiyalari o‘rnatilgan. Barcha stansiyalar o‘zaro “bir-biri bilan” prinsipi bo‘yicha bog‘langan. Bu topologiyani bog‘langan signalizatsiya tarmog‘i takrorlaydi.




a) bog’langan signalizatsiya tarmog’I b) kvazibog’langan

5.3-rasm. Signalizatsiya tarmog‘ining tuzilishi

Kvazibog‘langan tarmoqda to‘rtta STP o‘rnatilgan. Ular o‘zaro “bir-biri bilan” prinsipi bo‘yicha bog‘langan. Beshta SP dan bittasi ikkita STPga tayanadi. Bunday yechim signalizatsiya tarmog‘ining yuqori ishonchliligini ta’minlaydi. Yuqori ishonchlilikdan tashqari, signalizatsiya tarmog‘i signalli xabarlarni tez o‘tishini ta’minlashi zarur. Bu talab UFTTda trafikka xizmat ko‘rsatish sifati ko‘rsatkichlariga, signalli xabarlarning kechikishini ta’siri bilan shartlanadi.

## 5.3. UKS protokollar stekining mobil ilovalari

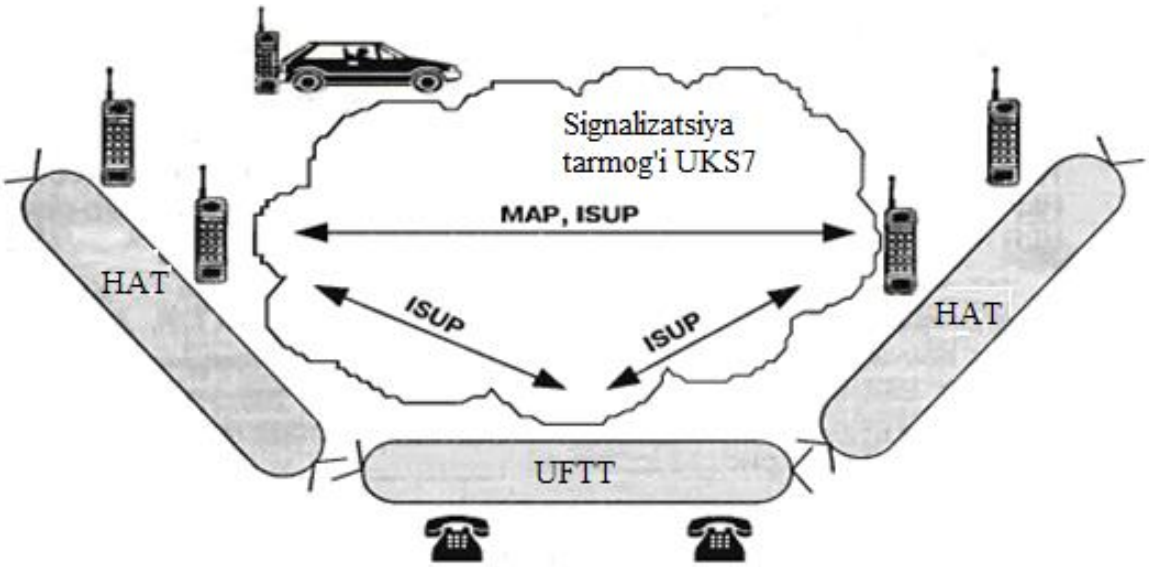
1988 yilda UKS stekiga mobil aloqani rivojlanish jarayonida yaratilgan MAP (Mobile Application Part) protokolining birinchi turi qo‘shilgan. Shuningdek boshqa protokol CAP (CAMEL Application Part) bilan ham UKS7 stekida shunday amal bajarilgan. Shuningdek MAP protokolini vazifasiga aynan o‘xshash bo‘lgan, Shimoliy Amerika uchun ishlab chiqilgan ANSI-41 protokoliga nisbatan haqqoniydir va 5.4-rasmda keltirilgan UKS7 protokollar stekini xuddi o‘sha sathida joylashadi. MAP va ANSI-41 axborotlari quyida joylashgan sathlarning MTP1, MTP2, MTP3, SCCP va TCAR protokollari bilan transportlanadi va inkapsulyatsiyalanadi.

MAP protokoli MSC, BTS, BSC, HLR, VLR, EIR, MS, shuningdek SGSN/GGSN ni GPRS (General Packet Radio Service)ga o‘xshagan harakatdagi aloqa tarmog‘ini (HAT) tarmoq komponentlari orasidagi amallarni aniqlash uchun qo‘llaniladi. GSM ni qo‘llab-quvvatlash maqsadida, kommutatsiyalash nimtizimlari uchun MAP ni beshta ilovalari (MAP-MSC, MAP-VLR, MAP-HLR, MAP-EIR, MAP-AuS) va BSC bazaviy stansiyani nazorati uchun BSSAP (BSS Application Part) ilovasi aniqlangan.

**MAP protokolining modeli.** Bu ishlab chiqilma uchun asos harakatdagi aloqa tarmog‘ining modeli xizmat qiladi (5.4-rasm), ya’ni bir kommutatsiyalash markazidan boshqasiga chaqiriqqa (xendover) xizmat ko‘rsatish bilan boshqarishni o‘tkazish usulini va harakatdagi aloqani turli tarmoqlari orasida abonentlarni mobilligini ushlab turuvchi MAP protokoli tavsiflaydi.

Harakatdagi aloqa tarmoqlarida tarmoqning maxsus xabarisiz abonentni turgan o‘rni jiddiy ravishda o‘zgarishi mumkin, masalan, abonent aeroportda o‘zining mobil telefonini o‘chirishi mumkin va bir necha soatdan so‘ng uni boshqa davlatning HATda yoqishi mumkin. Mobil abonentlarga chaqiriqlarga kiruvchilar uchun abonentni turgan o‘rni va mobil telefoni raqami orasida bevosita aloqa mavjud emas.

Chaqirilayotgan abonentning mobil terminaliga chaqiriqni uzatishni tashkil etishdan oldin, haqiqiy vaqtda uni turgan o‘rni haqidagi axborotni va boshqa xizmat axborotni olish zarur. Shuning uchun bunday chaqiriqlar, chaqiriqqa va/yoki aloqa seansiga bevosita taalluqli bo‘lmagan, katta sonli xizmat signallarini almashishni talab qiladi.




5.4-rasm. Ikkita UFT va HAT abonentlari orasida chaqiriqlarga xizmat ko‘rsatishni boshqarish modeli

## 5.4. VoIP signalizatsiya tizimlari

**SIP arxitekturasini yaratish.** VoIP tizimi uchun signalizatsiya protokollarini yaratish muhitidagi ishlar Session Invitation Protocol protokoli yozilgan draft-ietf-mmusic-sip-00IETF spetsifikatsiyani (tasniflash) chiqishi bilan IETFda boshlangan.

Bu xujjat faqat aloqa seansini o‘rnatish so‘rovini tasniflagan, biroq rivojlanishda bu tasniflash o‘sha vaqtda yaratilgan konferensiyani multimediali arxitekturasini integratsiyasiga mo‘ljallangan.

Seanslarni qayd etish protokolini birinchi tasnifi yaratilgunicha, hozirda SIP (Session Initiation Protocol) sifatida ma’lum, 1996 yil IETFda aloqa seanslarini o‘rnatishni ikkita protokoli raqib bo‘lgan: Simple Conference Invitation Protocol (SCIP) va SIP protokollari.

**IP ustidan UKS7 signalizatsiyasi.** IP-tarmoq orqali UKS7 axborotini uzatishni tashkil qilish masalasi bo‘yicha IETF tarkibiga kiruvchi Sigtran ishchi guruhi shug‘ullanadi. IP tarmoq bo‘ylab UKS7 axborotini ishonchli transportlash uchun Sigtran protokollar stekining asosi, IP tarmoqda signalizatsiyani oxirgi punktlari orasida signalli xabarlarni o‘tkazishni ushlab turuvchi, oqimlarni boshqarish protokoli SCTP (Stream Control Transmission Protocol) hisoblanadi.

| Moslashish protokollari<br>M2UA, M3UZ, M2PA, SUA, IUA |
|---|
| SCTP protokoli |
| Ip protokoli |

5.5-rasm. Sigtran protokollar steki

**SCTP oqimlarni boshqarish protokoli.** Signalli aloqani tashkil qilish uchun bir oxirgi punkt boshqa punktga o‘zining transport adreslari (SCTP portini nomeri bilan birgalikda IP-adresni) ro‘yxatini taqdim etadi.

SCTP protokoli turli oqimlarda signalli xabarlarni mustaqil tartiblash imkoniga ega va signalli axborotni qabul qilishni tasdiqlash bilan o‘tkazishni, har bir oqimning xabarini ularni o‘tish navbatini saqlash bilan yetkazish, bir nechta xabarlarni bitta SCTP paketiga birlashtirish imkoniyati, zarurat o‘lchami bo‘yicha ma’lumotlarni fragmentlash va o‘ta yuklanishga chidamliligini ta’minlaydi.

**M2UA, M2PA va M3UA moslashish protokollari.** IP tarmoqlarda ko‘rib chiqilgan MTP protokolining funksional imkoniyatlarini amalga oshirish uchun

Sigtran ishchi guruhi uchta yangi protokollarni tavsiya etdi - M2UA, M2PA va M3UA. Ularning har birini quyida qisqacha ko‘rib chiqamiz, lekin avval raqamli telefon tarmoqlari va IP tarmoqlar bo‘ylab MTP xabarini o‘tkazishga bo‘lgan ITU-T ning asosiy talablarini keltirib o‘tamiz:

- 3 MTP sathini bir darajali jarayoni uchun talab etilgan javob vaqti 500 ms dan 1200 ms gacha oraliqda bo‘lishi kerak;
- transport sathda rad etishlar tufayli xabarlarni yo‘qolish ehtimolligi $10^{-7}$ dan katta bo‘lmasligi kerak;
- transport sathda rad etishlar tufayli xabarni o‘z vaqtida yetkazmaslik ehtimolligi $10^{-9}$ dan katta bo‘lmasligi kerak.

2 MTP (MTP Level-2 User Adaptation Layer) sathi foydalanuvchilari uchun moslashish sathini M2UA protokoli, UKS7 oddiy stekida 2 MTP sathi 3 MTP sathiga taqdim etadigan xizmatlar majmuasini ko‘rib chiqadi.

Protokol, VoIP tarmoqlarda signalizatsiya shlyuzlari va transport shlyuzini kontrolleri orasida qo‘llaniladi. Signalizatsiya shlyuzi UKS7 xabarini, signalizatsiyaning oxirgi yoki tranzit punktidan MTPni 1 sath va 2 sath interfeysi orqali qabul qiladi. Shlyuz 2MTP sathida UKS7 zveno uchun oxiri hisoblanadi va 3MTP sathining axborotini va yuqori sathni transport shlyuzining kontrolleriga yoki IP tarmoqning boshqa oxirgi punktiga transportlaydi, ya’ni M2UA protokolni SCTP/IP ustidan qo‘llab.

Bir darajali foydalanuvchilar MTP2 (MTP2 User Peer-to-Peer Adaptation Layer) uchun moslashish sathining M2PA prtokoli, M2UA protokolidan farqli ravishda, IP tarmoq orqali o‘zaro ta’sirlashuvchi UKS7 tarmog‘ini ikkita bog‘lamalari almashadigan 3 MTP sathining xabarlarini to‘liq masshtabda qayta ishlash uchun qo‘llaniladi.

IP tarmog‘ining signalizatsiya punktlari, TCP/IP stekining protokollarini qo‘llab UKS7 oddiy bog‘lamalari singari ishlaydi.

M2PA protokoli, UKS7 signalizatsiyani qo‘llab kanalli kommutatsiya tarmog‘i bog‘lamalarini IP-telefoniya ma’lumotlar bazasiga va IP tarmoqni boshqa bog‘lamalariga ulanish imkonini berishi tufayli, OKS7 va IP tarmoqlarning integratsiyasini yengillashtiradi. Shuningdek teskarisi, M2RA protokoli IP-telefoniya ilovalarini UKS7 tarmog‘ining ma’lumotlar bazasiga ulanish imkonini beradi.

3 MTP (MTP Level-3 User-Adaptation Layer) foydalanuvchilar uchun moslashish sathining M3UA protokoli, SCTP protokoli vositalari yordamida, 3 MTP sathini nimtizim-foydalanuvchilar signalli xabarlarni IP tarmoq bo‘ylab o‘tkazish bilan bog‘liq (masalan, ISUP, SCCP).

M3UA protokoli, signalizatsiya shlyuzlari va transport shlyuzi kontrollerlari yoki IP-telefoniya ma’lumotlar bazalari orasida qo‘llaniladi. U IP–tarmoqni uzoqdagi oxirlarini qamrab, signalizatsiya shlyuzini 3 MTP sathi xizmatlariga ulanishini kengaytiradi.

**SUA va IUA protokollari.** SCCP foydalanuvchilari uchun moslashish sathining SUA protokoli, IP-tarmoq bo‘ylab SCCP foydalanuvchilarning signalli xabarlarini o‘tkazishni ta’minlaydi, masalan, TCAP yoki INAP, SUA protokoli IP-tarmoq signalizatsiyaning oxirgi punktlari va signalizatsiya shlyuzlari orasida qo‘llaniladi.

SUA protokoli, SCCP xizmatlar singari tartibsiz va tartiblangan yetkazish bilan ulanishsiz, ma’lumotlar oqimini boshqarishli yoki boshqarishsiz ulanishlarga mo‘ljallangan xizmatlar va xabarlarni o‘z vaqtida yetkazilmaganligi natijasidagi xatolar va xabarlarning yo‘qolganligini bilish xizmatlarini ta’minlaydi (ya’ni SCCP 0 dan 3 gacha xizmatlar sinfi). Ulanishsiz xizmat holatida SCCP va SUA protokollari signalizatsiya shlyuzida o‘zaro ta’sirlashadi.

ISDN - foydalanuvchi (IUA) uchun moslashish sathining protokoli IP tarmoq orqali Q.931 xabarni o‘tkazishni ta’minlaydi. IUA protokoli MTP protokolining qismini signalizatsiya tizimida qo‘llanilishini ta’qiqlaydi va yuqori sathning

ilovalarini SCTP transport protokollar bilan bevosita o‘zaro ta’sirlashishiga imkon beradi.

## 5.5. Multimediali aloqa tarmoqlarida sinxronizatsiya

Sinxronizatsiya deganda aloqa tarmog‘ining funksional elementlari bilan axborotni uzatish, kommutatsiyalash va ishlov berishning ayrim muhim elementlari orasida muvofiqlashtirish tadbiri tushuniladi. “Sinxronizatsiya” atamasi aloqa tarmog‘i va uning ayrim elementlarining faoliyat yuritishini turli jarayonlarini tavsiflash uchun qo‘llaniladi. Raqamli UFTTga nisbatan sinxronizatsiyaning uchta jixatini ko‘rib chiqish maqsadga muvofiqdir:

- taktli sinxronizatsiya;
- siklli sinxronizatsiya;
- tarmoq sinxronizatsiyasi.

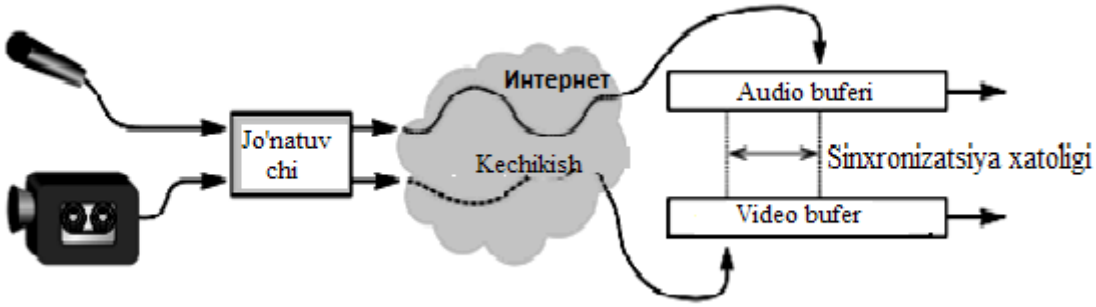
Taktli sinxronizatsiya, umumiy bitlar oqimidan sinxronizatsiya signalini ajratib olishga asoslangan. U bitlar darajasida (taktli intervallar) uzatish va qabul qilish qurilmalarining ishlashini vaqt bo‘yicha moslashtirish uchun zarur. Siklli sinxronizatsiya, turli manbalardan kelayotgan axborotlar, bitlarning umumiy oqimida axborotlar blokining boshi va oxirini aniqlash uchun zarur, ya’ni uni qabul qilishda to‘g‘ri taqsimlash uchun. Tarmoq sinxronizatsiyasi, axborot uzatishda yuqori sifat taminlanishi uchun tarmoqning turli nuqtalarida (shu jumladan xalqaro ulanishlarda) taktli signallarning uzoq muddatli aniqliligi va barqarorligining berilgan ko‘rsatkichlarini ta’minlaydi.

Tarmoq sinxronizatsiya uchun kvars va atom generatorlaridan foydalaniladi. Ular yuqori aniqlikdagi etalon signallarni ishlab chiqaradi. Masalan odatdagi kvars generatorining barqarorligi bir yilda $10^{-6}$ ni tashkil etadi. Rubidiyli, seziyli va vodorodli atom generatorlarining barqarorligi ancha yuqori. Xususan, seziyli generator bir yilda $10^{-13}$ barqarorlikni taminlaydi.

**Ovoz va tasvir sinxronizatsiyasi.**

Multimedia seansi bir nechta oqimlardan iborat bo‘lib, ularning har biri RTPning alohida seansida uzatiladi. Kodlash formatlari bilan bog‘liq kechikishlar amaliy farq qiladi, 5.6-rasmda ko‘rsatilganidek, turli xil oqimlarda boy berish vaqti har xil bo‘ladi.

Odatda sinxronizatsiya tovush va tasvir oqimlarini tenglashtirish uchun qo‘llaniladi, ammo mazkur texnologiya istalgan turdagi oqimlar uchun ham qo‘llanilishi mumkin. Ko‘pincha tovush va tasvirni alohida oqimlarga bo‘lishni sean ishtirokchilarining nimani afzal ko‘rishlariga bog‘liq bo‘ladi. Ba’zilar video konferensiyalarda faqat tovushni qabul qilishni afzal ko‘rishadi. Ayniqsa bu ishtirokchilar soni ko‘p bo‘lgan konferensiyalar uchun muhimdir.




5.6-rasm. Multimedia oqimlarining sinxronizatsiyasi

**Jo‘natuvchining o‘zini tutishi.** Jo‘natuvchi multimedia oqimlarini sinxronizatsiyalash jarayonida, umumiy va oqim vaqtini muvofiqlashtirish to‘g‘risida RTCP paketlari orqali davriy xabardor qilish va umumiy sathni ishga tushirish yo‘li bilan yordam beradi. Umumiy soat o‘zgarmas tezlikda yuradi, qabul qiluvchiga esa 5.6-rasmda ko‘rsatilganidek, oqimlardagi tezliklarni tenglashtirishga yordam beruvchi axborot beriladi.

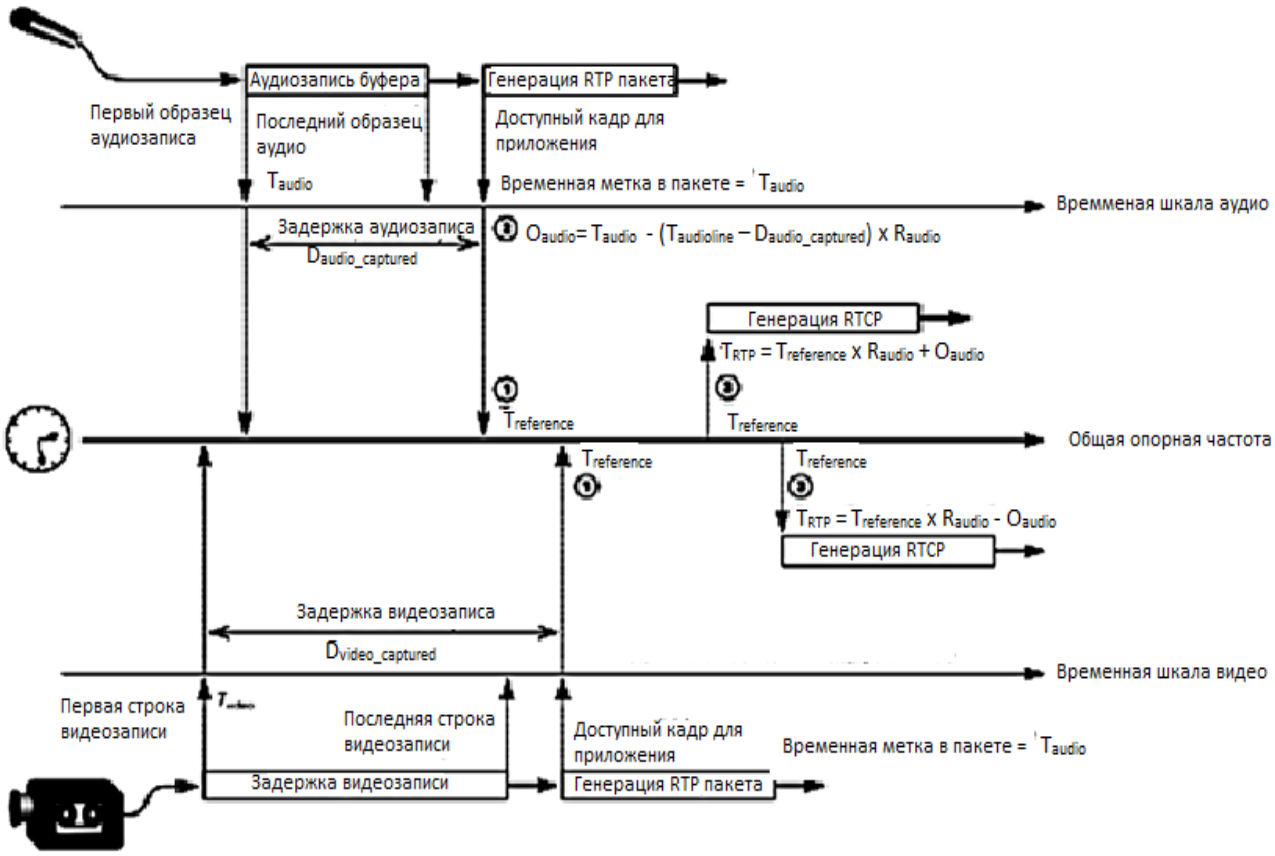
Umumiy va oqim vaqti orasidagi muvofiqlik RTCP paketini shakllantirish vaqtida aniqlanadi. Umumiy Treference vaqti RTP paketining vaqt belgisida aks ettiriladi:

$$TRTP = Treference \cdot Raudio + Oaudio$$

Bunday soatlarning siljishini (surilishiini) hosil qilamiz:

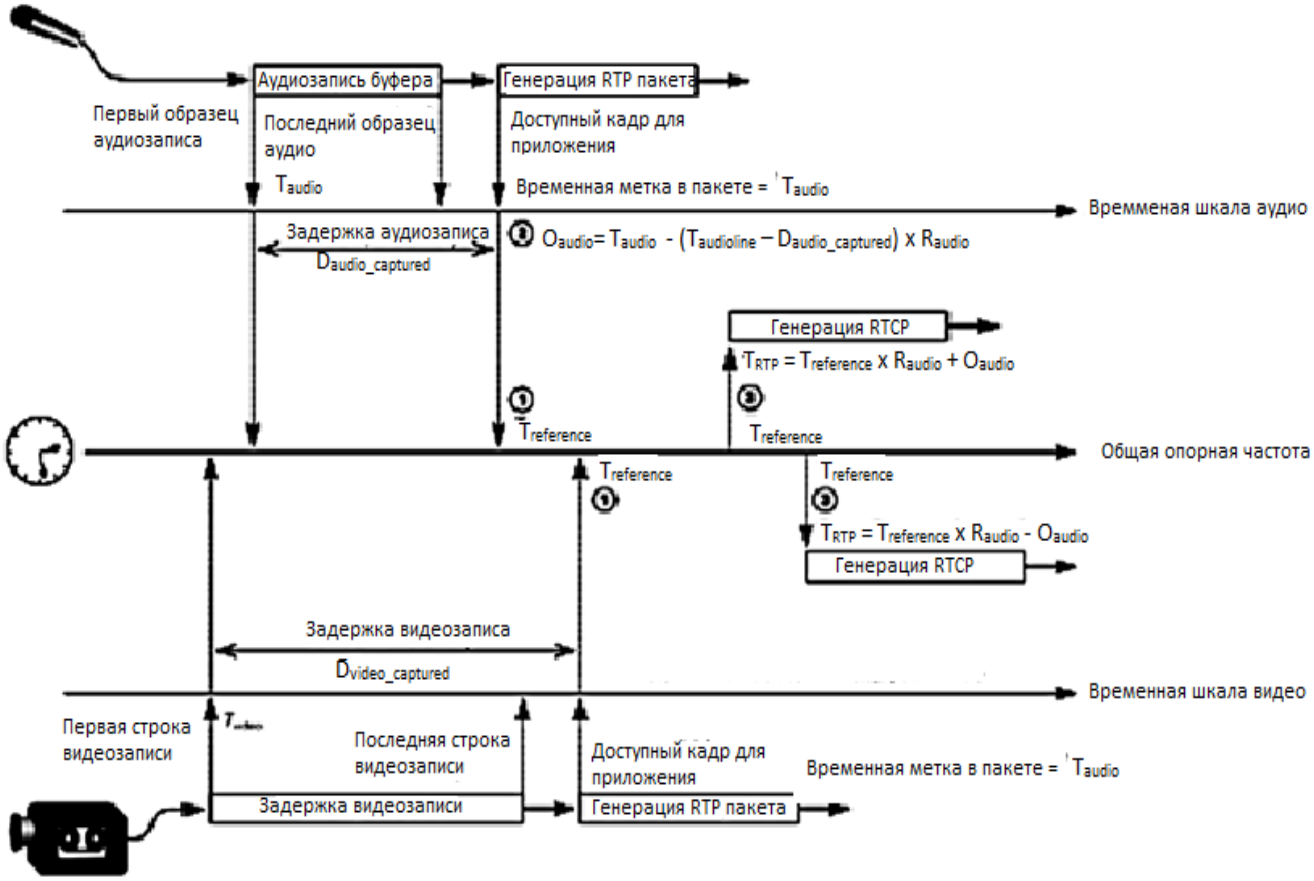
$$Oaudio = Taudio - (Tailable - Daudio\_capture) \cdot Raudio.$$

Tavailable - operatsion tizimdagi kechikishlar bilan, Daidio_capture esa ma'lumotlarni kechikish jarayonining davomiyligi bilan aniqlanadi. 5.7-rasmda multimedia oqimlari turli xil manbalardan olingan holatdagi soatlarni sinxronizatsiyalash zarurati keltirilgan.




5.7- rasm. Umumiy soat bo'yicha vaqtni tenglashtirish

Sinxronizatsiyaning yana bir muammosi - sinxronizatsiya qo‘llanilishi kerak bo‘lgan oqimlarni identifikatsiya qilishdir. Bu masalani RTP bog‘langan manbalarga umumiy nomlar (CNAME) berish yo‘li bilan hal qiladi, shuning uchun qabul qiluvchi bog‘liq bo‘lgan va bog‘liq bo‘lmagan oqimlarni farq qiladi.




5.8-rasm. Turli manbalardan kelayotgan oqimlarni sinxronizatsiyalash

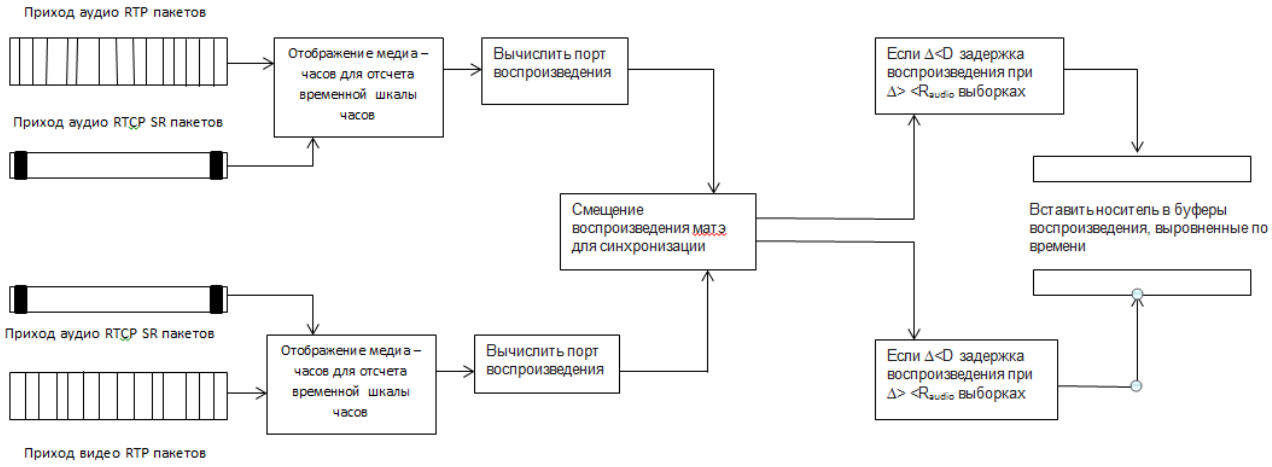
**Qabul qilib oluvchining vazifasi.** Qabul qiluvchi sinxronlanuvchi oqimlarni ajratishi va ularni eshitish oldidan tenglashtirishi kerak. Oqimlarni ajratishga turli oqimlarda bir xil CNAME nomlardan foydalanib juda oson erishiladi. Sinxronizatsiya tadbirining o‘zi ancha murakkabdir (5.9 va 5.10 rasmlar).

Qabul qilib oluvchi avval jo‘natuvchi belgilagan umumiy vaqt bilan sinxronlanuvchi oqimlar vaqti o‘rtasidagi muvofiqlikni RTP va RTCP paketlari

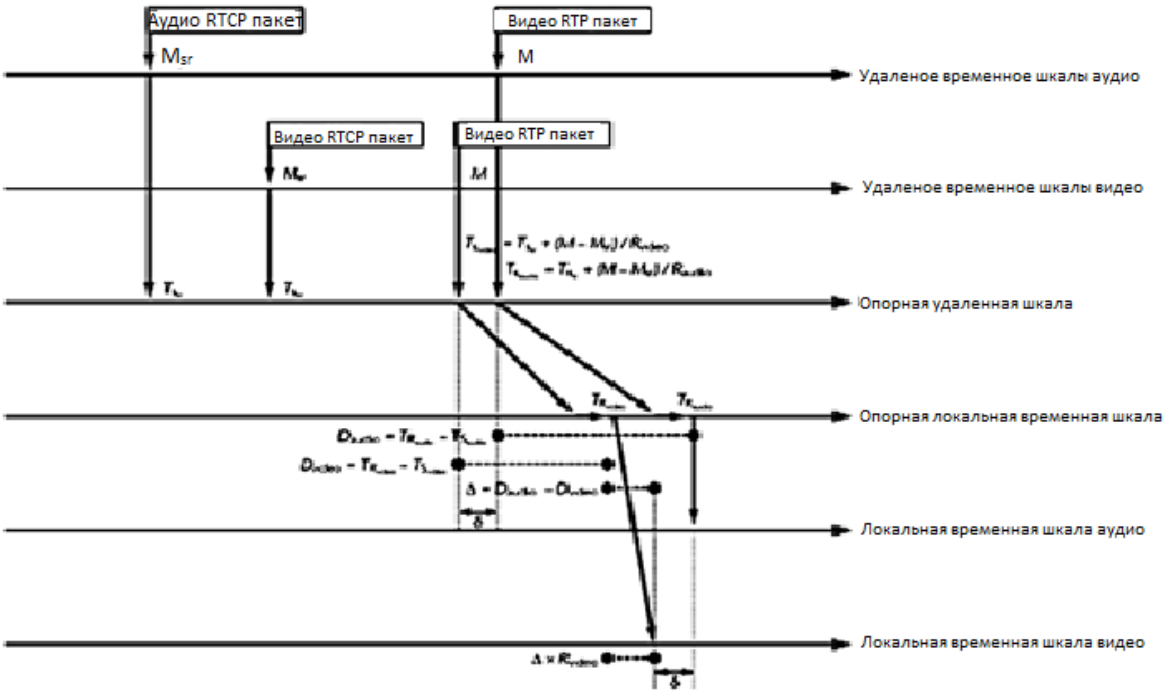
ma’lumotlarini taqqoslash yo‘li bilan aniqlaydi. *M* vaqt belgili RTP ma’lumotlar paketini qabul qilib olishda kechikish vaqti hisoblab topilishi mumkin:

$$T_s = \frac{T_{Ssr} + (M - M_{sr})}{R} \quad . \tag{4.1}$$

Bu yerda: $M_{sr}$ - oxirgi olingan RTCP paketda RTP vaqt belgisi; $T_{Ssr}$ - sekund hisobidagi umumiy vaqt; R - soatning gers hisobida berilgan nominal tezligi.




5.9-rasm. Foydalanuvchi tomonida tovush va tasvirning sinxronizatsiyasi




5.10-rasm. Foydalanuvchi tomonida vaqtlarning muvofiqligini o‘rnatish

Qabul qilib oluvchi ham mahalliy soatga muvofiq sinxronizatsiyalangan TR ma’lumotlarni chiqarish vaqtini hisoblaydi. U jo‘natuvchining umumiy vaqti bilan muvofiqlashtirilgan, dekoderlash uchun boy berish buferida musbat kechikish, aralashtirish va ishlov berish bilan moslashtirilgan paketning vaqt belgisiga teng.

Kechikish va boy berish vaqti ma’lum bo‘lganda, qabul qilib oluvchi har bir oqim uchun malumotlarni kechikishi va ularni boy berishi orasidagi nisbiy kechikishini hisoblashi mumkin. Agar ma’lumotlar TS vaqtida jo‘natuvchining umumiy vaqti bo‘yicha kechikkan va TR vaqtda qabul qilib oluvchining soati bo‘yicha chiqarilsa, u holda ular orasidagi D=TR-TS farq tasvirni kechikishi va uni chiqarish orasidagi kechikishning kattaligini beradi. Jo‘natuvchi va qabul qiluvchining soatlari sinxronlashtirilmaganligi uchun bu qiymat o‘z ichiga ular orasidagi noma’lum siljishni qamrab oladi, lekin uni e’tiborga olmasa ham bo‘ladi, chunki u barcha sinxronlanuvchi oqimlar uchun bir xildir, bizni esa faqat oqimlar o‘rtasidagi nisbiy siljish qiziqtiradi.

Tovush oqimi uchun ham, tasvirlar oqimi uchun ham bunday kechikishni hisoblagandan so‘ng, xususan D=Daudio–Dvideo oqimlar uchun sinxronizatsiyaning kechikishini hisoblash mumkin. Agar bu qiymat nolga teng bo‘lib chiqsa, u holda oqimlar sinxronlashgan bo‘ladi. Aks holda u oqimlar orasida sekundlar hisobidagi siljishni beradi.

Ilgarilovchi ma’lumotlar oqimi uchun sinxronizatsiyaning kechikishi, ma’lumotlarning vaqt belgisi formatiga qiymatlarni o‘zgartirish uchun ma’lumotlar oqimining nominal tezligiga ko‘paytiriladi va keyin vaqtni barcha hisoblanishlarida doimiy siljish qiymati tarzida foydalaniladi. Foydalanuvchi o‘z ustivorliklariga muvofiq sinxronizatsiyani qaysi oqim bo‘yicha o‘tkazishini tanlab olishi mumkin. Ko‘pchilik kodeklar uchun videoni kodlash va dekoderlash ustunlik qiluvchi oqim bo‘lib hisoblanadi, ammo tovush yuz berayotgan o‘zgarishlarga ancha sezgirroqdir. Sinxronizatsiyaning kechikishini oqimlardan istalganining kechikishi o‘zgarganda qayta hisoblash zarur. Bu shuningdek umumiy vaqt bilan oqim vaqti orasidagi nisbat o‘zgarganda ham zarurdir.

**Sinxronizatsiya aniqligi.**

Shunday savol tug‘ilishi mumkinki, oqimlar o‘rtasidagi kechikishning qanday qiymatini e’tiborga olmasa ham bo‘ladi? Bu savolga javob juda ko‘p omillarga bog‘liq bo‘ladi, shu jumladan nima sinxronlayotganiga va qanday maqsadda sinxronalayotganiga bog‘liq. Masalan, tovushni va tasvirni sinxronlash yetarlicha qat’iy bo‘lmasligi va videoning sifati hamda freymlarning tezligiga bog‘liq holda o‘zgarishi mumkin, ayni paytda tovush oqimlarini sinxronlash juda ham aniq bo‘lishi kerak. Tovush va tasvirni sinxronizatsiyalashda bir necha o‘nlab milli sekund aniqlik yetarli hisoblanadi. Video konferensiyalarni o‘tkazish bilan bog‘liq tajribalar 80…100ms tartibdagi chegaraviy qiymatni beradi, uning bu qiymatdan oshishiga yo‘l qo‘ymaslik kerak. Uzatilayotgan tasvirning sifati oshganda bu chegara kamayadi.

## Nazorat savollari

1. Telefon aloqada signalizatsiyaning vazifasi nimadan iborat?
2. Signalizatsiyaning qanday turlari bor?
3. Ajratilgan signalli kanal haqida tushuncha bering.
4. Signalizatsiya tarmog‘ini tuzilish pinsipini tushuntiring.
5. UKS tizimi modelining OSI modelidan farqi nimada?
6. UKS tizimini quyi MTP sathlarini vazifasi nimadan iborat?
7. MAP protokolining vazifasi nimadan iborat?
8. VoIP texnologiyasida signalizatsiya tizimini tushuntiring.
9. Sigtran protokollar stekini tushuntiring.
10. MTP xabarlarini uzatish bo‘yicha ITU-Tning qanday asosiy talablari mavjud?
11. Sinxronizatsiyaning vazifasi nimadan iborat va uning qanday turlari mavjud?
12. Multimediali oqimlarni sinxronizatsiyasini tushuntiring.
13. Jo‘natuvchini multimediali oqimlarni sinxronizatsiyalash jarayonini tushuntiring.
14. Qabul qiluvchi tomonidan tovush va tasvirning sinxronizatsiyasini tushuntiring.

# 6. MULTIMEDIALI ALOQA TARMOQLARINI BOSHQARISH

## 6.1. Multimediali aloqa tarmoqlarini boshqarish modeli

Telekommunikatsiya tarmoqlarini boshqarish sohasidagi asosiy modellardan biri M.3000-M.3100 seriyasidagi ITU-T tavsiyalarida batafsil tavsiflangan, Telekommunikatsiyalarni boshqarish tarmoqlari (Telecommunication Management Network, TMN) modeli hisoblanadi.

ITU-T ta’rifiga ko‘ra, TMN o’zida bir necha nuqtalarda bitta yoki juda ko‘p sondagi aloqa tarmoqlari interfeyslariga ega bo’lgan alohida tarmoqni ifodalaydi, bu tarmoqlar bilan axborot almashadi va ularning faoliyatini boshqaradi. TMNni aloqa tarmoqlaridan ajratish jismoniy yoki mantiqiy sathda amalga oshiriladi. Keyingi holatda TMN boshqarilayotgan tarmoqning infratuzilmasidan qisman foydalanishi mumkin. TMN tasniflarida boshqariluvchi resurslar umumiy “tarmoq elementlari” nomiga ega (Network, Element, NE). Boshqarish vazifalari amallarni ta’minlash tizimi (Operations Support System, OSS) zimmasiga yuklangan.

TMNni har biri telekommunikatsiya tarmoqlarini boshqarishning o‘z jihatini ifodalaydigan uchta arxitekturadan fodalanib tavsiflash mumkin.

Uchta arxitekturadan birinchisi – funksional arxitektura – funksional bloklar deb ataluvchi atamalarda TMN tarmog‘idagi funksional imkoniyatlarning taqsimlanishini tavsiflaydi. Har bir blok aniq turdagi tarmoq resurslari uchun aniqlangan, boshqaruvchi funksiyalar guruhini ifodalaydi.

TMN aritekturasida funksional bloklarning besh turi keltirilgan:

- tarmoq elementlarining vazifalari (Network Element Function, NEF): foydalanuvchi va aloqa tarmog‘i bilan ma’lumotlar almashinuvini ta’minlaydigan tayanch telekommunikatsiya funksiyalar (TMN tasniflarida aniqlashtirilmaydi) va tarmoq elementiga agent sifatida ishtirok etishga imkon beruvchi boshqaruv funksiyalari;

- operatsiyalarni ta’minlash tizimining vazifalari (Operation Support Sustem Functions, OSSF), ma’muriylashtirish jarayonini tashabbusini ta’minlaydi, aloqa tarmog‘ini turli vazifalarini muvofiqlashtirish va monitoring maqsadida, shu jumladan TMNning o‘zi bajaradigan boshqarish masalalarini xizmatchi axborotlarni qayta ishlashni ta’minlaydi. “Menedjer-agent” boshqaruv modelida ular menedjerning roliga mos keladi;

- ishchi stansiyaning vazifalari (Workstation Functions, WSF), tarmoq foydalanuvchilari uchun, xususan tarmoqdan foydalanuvchilar uchun qulay ko‘rinishda boshqaruvchi axborotni taqdim etish uchun javob beradi;

- Q-adapterning vazifalari (Q-Adapter Funkctions, QAF), tarmoq resurslarini TMN bilan bog‘lash imkonini beradi;

- vositachilik vazifalari (Monition Function, MF): NEF (yoki QAF) va OSSF bloklari orasida axborot almashish. MFni bitta bloki Q-adapteri yoki bir nechta tarmoq elementlari bilan amallarni ta’minlash tizimini ulashi mumkin.

TMNning fizik arxitekturasida bloklarning olti turi keltirilgan:

- Tarmoq elementi (Network Element, NE), NEFning vazifalarini bajaradi. Shuningdek u funksiyalarning boshqa bloklaridan istagan to‘plamini ham bajarishi mumkin.

- Vositachilik qurilmasi (Mediation Device, MD), operatsiyalarni ta’minlash tizimining mos axborot modeli interfeyslari va TMN mahalliy interfeyslar orasida oraliq bo‘g‘in hisoblanadi. Shuningdek u Q-adapter, OSS va ishchi stansiya vazifalarining bir qismini bajarishi mumkin.

- Q-adapter (Q-adapter, QA), TMN tarmog‘ining chegarasida uning boshqariluvchi tarmoq yoki boshqa boshqarish tizimlari bilan ulanishida vositachi vazifalarini amalga oshiradi. MDdan farqli ravishda, Q-adapter TMN ichida tutashtirish uchun qo‘llanilmaydi.

- Operatsiyalarni ta’minlash tizimi (Operation Support Sustem, OSS), OSSF guruhining vazifalari uchun javob beradi. Shuningdek u vositachilik (MF), tutashtirish (QAF) vazifalarini va ishchi stansiya vazifalarini (WSF) bajaradi.

- Ishchi stansiya (Work station, WS).

- Ma’lumotlarni uzatish tarmog‘i (Data Network, PN).

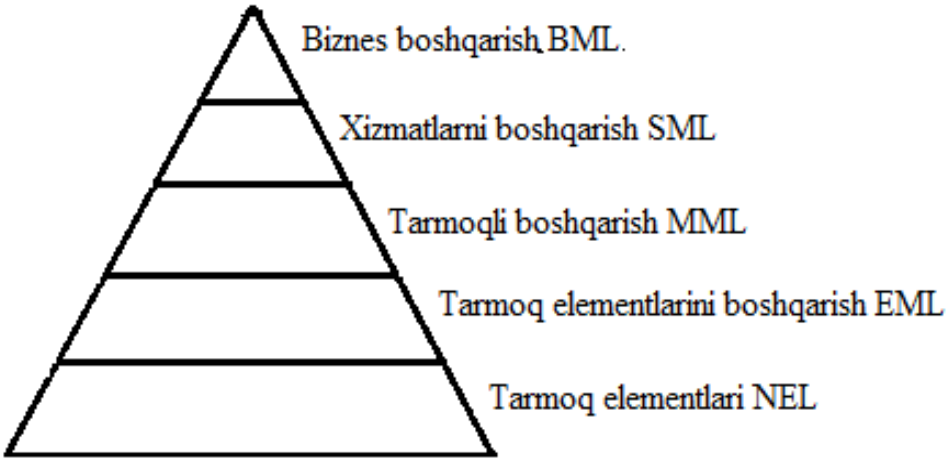
Axborot arxitekturasi, TMN funksional bloklari orasida boshqaruvchi axborotlarni uzatish algoritmlarini aniqlaydi, ular OTO‘B modelidan ikkita muhim elementni meros qilib olishgan: ob’ektli mo‘ljal olish va “menedjer-agent” arxitekturasi.

TMNda nazarda tutilgan, taqsimlangan boshqaruvchi ilovalar vazifalarining menedjer va agentga bo‘linishi, OSI standartini ta’minlovchi ma’muriylashtirish tizimlarida keng foydalaniladigan tamoyilni deyarli o‘zgarishsiz takrorlaydi. TMN funksional bloki bir paytda bitta boshqaruvchi komponentga (management entity) nisbatan menedjer rolida va boshqasiga nisbatan agent tarzida ishtirok etishi mumkin.

TMN axborot arxitekturasining ob’ektli yo‘naltirilganligi, telekommunikatsiya resurslari boshqariluvchi ob’ektlar sinflari ko‘rinishida ifodalanib, ular TMN interfeyslarini qo‘llash bilan o‘zgarishi va yaratilishi mumkin. Ob’ektning chegaraviy interfeysi mazkur ob’ektning tavsiflari bilan bog‘liq xizmatlar to‘plami, ruxsat etilgan operatsiyalar, javob xabarlari va bildirishlarni ta’minlashi shart. Ixtiyoriy aloqa tarmog‘ini boshqarish uchun foydalanish mumkin bo‘lgan ob’ektlar to‘plami universal tarmoq axborot modeli (Generic Network Informotion Model, GHIM) nomini oldi.

TMN axborot modeli telekommunikatsiya resurslari va boshqariluvchi ob’ektlar o‘rtasida o‘zaro bir qiymatli moslik bo‘lishiga, bitta resursni bir necha ob’ektlar tomonidan taqdim etilishi, mantiqiy resurslarni akslantirish uchun qo‘shimcha ob’ektlarni kiritish (qo‘llab-quvvatlash ob’ektlari deb ataluvchi), shuningdek, boshqariluvchi ob’ektlarni bir-birining ichiga kiritishga yo‘l qo‘yadi. Funksional, fizik va axborot arxitekturalaridan tashqari TMN konsepsiyasi aloqa

tarmoqlarini boshqarishga tegishli funksional komponentlarni va tadbirlarni taqsimlashning boshqa prinsipini ham taklif etadi. Aynan bir xil ma’muriy funksiyalar abstraksiyaning turli xil darajalarida amalga oshirilishi mumkinligi, mantiqiy ierarxiyali arxitekturani (Logical Lavered Architecture, LLA) aniqlashga imkon beradi. Aslida LLA arxitekturasi (ba’zida TMN- piramidasi deyiladi, 6.1-rasm) ma’muriy vazifalarni bajarish uchun javobgarlik ierarxiyasini aks ettiradi.




6.1-rasm. TMN piramidasi

Hozirgi vaqtda LLA arxitekturasida boshqarishning beshta sathi ko‘zda tutilgan:

- Tarmoq elementlari sathi (Network Element Layer, NEL) alohida qurilmada joylashgan xizmatchi axborotli ma’lumotlar bazasi (Management Information Base, MIB) va TMN infratuzilmasi orasida interfeys vazifasini bajaradi. Bu darajaga Q-adapterlar va xususan tarmoq elementlari kiradi.

- Elementlarni boshqarish sathi (Element Management Layer, EML), tarmoq elementlari guruhi ishini nazorat qiluvchi operatsiyalarni ta’minlash tizimlari funksiyalariga mos keladi. Bu sathda aniq ishlab chiqaruvchining qurilmasi uchun xos bo‘lgan boshqaruvchi funksiyalar amalga oshiriladi. Bunday funksiyalarga

quyidagilar misol bo‘ladi: qurilma xatolarini aniqlash, energiya iste’mol qilish va ishchi temperaturani nazorat qilish, statistik ma’lumotlarni to‘plash, hisoblash resurslaridan foydalanish darajasini o‘lchash, mikrodasturiy vositalarni yangilash. Mazkur sath o‘z ichiga vositachilik qurilmalarini qamrab oladi (jismoniy jihatdan ular yanada yuqori sathlarga tegishli bo‘lsa ham).

- Tarmoqni boshqarish sathi (Network Management Layer, NML), oldingi sathdagi operatsiyalarni ta’minlash tizimlari tomonidan uzatiladigan va u yoki bu shakldagi mahsulotning xususiyatlariga bog‘lanmagan alohida tarmoq elementlari to‘g‘risidagi ma’lumotlarga asoslanib, umumiy tarmoqni ifodalashni shakllantiradi. Boshqacha aytganda, bu sathda tarmoq elementlarining o‘zaro aloqalari ustidan nazorat amalga oshiriladi, xususan, xizmat ko‘rsatishning talab etilgan sifatiga erishish uchun chetki qurilma orasida ma’lumotlarni uzatish marshrutlari shakllantiriladi (Quality of Service, QoS), marshrutlashtirish jadvallariga o‘zgarishlar kiritiladi, ayrim kanallarning o‘tkazish qobiliyatidan foydalanish darajasi kuzatiladi, tarmoqning unumdorligi optimallashtiriladi va uning ishlashidagi to‘xtab qolishlar aniqlanadi.

- Xizmatlarni boshqarish sathi (Service Management Layer, SML), foydalanuvchilar bevosita duch keladigan (abonentlar yoki boshqa xizmat-provayderlar) tarmoqning faoliyat yuritishi jihatlarini qamrab oladi. LLA ning umumiy tamoyillariga muvofiq bu sathda NML sathdan kelib tushgan ma’lumotlardan foydalaniladi. Ammo endi bu yerda marshrutizatorlarni, kommutatorlarni, ulanishlarni bevosita boshqarishni amalga oshirib bo‘lmaydi. Xizmatlarni boshqarishga tegishli bo‘lgan ayrim funksiyalar quyidagilardir: QoSni va xizmat ko‘rsatish sathi to‘g‘risidagi bilimlar shartlarini nazorat qilish (Service Lerel Argeement, SLA), qayd qilinuvchi yozuvlarni, xizmatlar obunachilarini boshqarish, foydalanuvchilarni qo‘shish yoki kamaytirish, manzillarni berish, billing, boshqa provayderlar va tashkilotlarning boshqaruvchi tizimlari bilan o‘zaro aloqa.

- Biznesni boshqarish sathi (Business Management Layer, BML), aloqa tarmog‘ini kompaniya-operatorning umumiy biznes maqsadlari nuqtai nazaridan qarab chiqadi. U LLAning qolgan sathlari kabi tezkor boshqaruvga emas, balki strategik va texnik boshqaruvga tegishli. Bu yerda gap tarmoqni loyihalashda va uning rivojlanishini biznes vazifalarini hisobga olib rejalashtirish, budjetlarni tuzish to‘g‘risida boradi. Shunday qilib, LLA sathi tarmoqni boshqarish tadbirlarining funksional ierarxiyasini ma’muriy dasturiy ta’minotini jismoniy segmentatsiyasiz taqdim etadi. Bu ierarxiyaning paydo bo‘lish sababi – boshqarish funksiyalarini ularning guruhlari va tarmoq ulanishlariga taalluqli funksiyalardan alohida tarmoq elementlari bilan mantiqiy ajratish zarurligidadir. Ma’muriy tadbirlarning ularni ta’siri yo‘naltirilgan resurslarga yaqinlashishi boshqarish samaradorligini oshiradi.

Aloqa tarmoqlarini zamonaviy konvergensiyalash va intellektuallashtirish sharoitlarida, boshqarishga yondashuvlarni qayta ko‘rib chiqish zarurati yuzaga keldi. Bu zaruriylikning asosiy sabablarini ko‘rib chiqamiz.

Boshqarish nuqtai nazaridan keyingi avlod tarmoqlarining (Next Generation Networks, NGN) xususiyati shundaki, bu tarmoqlar har xil turdagi komponentlarning katta miqdoridan iborat. Boshqarish tizimi turli xizmatlarni taqdim etuvchi va turli ishlab chiqaruvchilarning qurilmalaridan iborat turli xil texnologiyalar negizida amalga oshirilgan tarmoqlarni boshqarishni ta’minlovchi qarorlar to‘plamidan iborat. NGNni boqarish tizimini ob’ektga yo‘naltirilgan taqsimlangan tuzilmadan foydalanib qurish maqsadga muvofiq. Ob’ektga yo‘naltirilganlik tizimni har biri o‘z xususiyatlariga (atributlariga) va bajarish mumkin bo‘lgan operatsiyalarga ega bo‘lgan ob’ektlar yig‘indisi ko‘rinishida tasavvur qilishdan iborat. Mazkur texnologiya murakkab tizimlarni tahlil qilishda, loyihalashda va dasturlashda foydalaniladi va unga oid asosiy ma’lumotnomalardan biri deb aytish mumkin.

Boshqaruv tizimini ishlab chiqishda yangi modullarni ishlab chiqishga va joriy qilishga, mavjud ilovalar bilan ishlashga va tizimning ishlayotgan modellarini oson

zamonaviylashtirishga imkon beruvchi ochiq modulli arxitektura konsepsiyasiga amal qilish zarur.

## 6.2. Tarmoqni boshqarish muammolari

Tarmoqni boshqarish tizimini tashkil etishda asosiy muammolardan biri, ko‘pincha operatorlarning turli yetkazib beruvchilarning qurilmalaridan foydalanishlari hisoblanadi. Odatda ularning har biri faqat o‘z qurilmasini boshqarishning yetarlicha kuchli va ko‘p funksionalli tizimini taklif etadi. Boshqa tomondan ochiq tizimlarning o‘zaro aloqa prinsiplari asosida qurilgan HP Open View (Hewlett - Packard), Net view (IBM) yoki Sun Net Manager kabi platformalar mavjud bo‘lib, ular turli xil qurilmalarning keng spektrini boshqarishga imkon beradi, lekin ular tarmoqni boshqarish uchun faqat asos bo‘lib hisoblanadilar. Tarmoqni ma’murlashtirishning bu platformalari bir konsoldan turli xil yetkazib beruvchilarning boshqaruv ilovalariga kirishini ta’minlaydi.

Aniq bir boshqarish tizimini amalga oshirish uchun tayyor yechimlar mavjud emas – hatto boshqarish tizimlari uchun ishlab chiqarilgan boshqaruvchi axborotning umumiy protokoli (Gommon Management Information Protocol, CMIP) va tarmoqni boshqarishning oddiy protokoli (Simle Nework Management Protocol, SNMP) kabi protokollarni hisobga olgan holda ham. Ma’lum bir kompaniya tomonidan amalga oshirilgan tarmoqni boshqarish tizimi, buyurtmachining talablariga to‘liq mos kelishiga kafolat berib bo‘lmaydi. Buning uchun, uni yangi buyurtmachining tarmoq xususiyatlarini hisobga olib qayta ishlashga to‘g‘ri keladi.

Tarmoqni boshqarish platformasini (TBP) malakali tarzda, ya’ni qo‘yilgan barcha vazifalarning yechimini ta’minlash uchun dasturlar kompleksini tanlash juda muhimdir. Agar operator tarmog‘i turli xil ishlab chiqaruvchilarning qurilmalaridan iborat bo‘lsa, u holda TBP kanallar kommutatsiyasiga ega tarmoqni ham (PSTN), paketlar kommutatsiyasi bo‘lgan tarmoqni (IP/MPLS, ATM, Fram Relay, X.25 va

boshq.) ham yuqori samaradorlik bilan boshqarishni ta’minlashi kerak. Tarmoqni boshqarish platformasi quyidagi masalalarni yechish uchun moslashgan bo‘lishi kerak:

- uzoqlashtirilgan uzellarlar, modullar, portlar, kanallarni grafik interfeys yordami bilan konfiguratsiyalash;

- foydalanuvchilarning talab qilingan miqdordagi kanallari va multipleksorlarni boshqarish;

- har qanday konfiguratsiyadagi ulanishlarni yaratish: “nuqta-nuqta”, “nuqta-guruh”, “guruh-guruh”;

- haqiqiy vaqt rejimida tarmoq holatini nazorat qilishni tashkil etish;

- tarmoqni sinxronlashtirishni akslantirish;

- tarmoq resurslaridan foydalanishni akslantirish;

- nosozliklarning oldini olish va bartaraf etish uchun tashxislashni o‘tkazish;

- quyidagi kontekstlardan birida tarmoq holatini ko‘rib chiqish: ob’ektga yo‘naltirilgan va mantiqiy yo‘naltirilgan.

Ob’ektga yo‘naltirilgan holda ko‘rib chiqish tarmoqning fizik komponentlarini, jumladan, multipleksorlar, modullar, portlar, kirish qurilmalari, kanallar kabi komponentlarni taqdim etishni amalga oshirishga imkon beradi. Tarmoq operatorining ishlashi qulay bo‘lishi uchun, kommunikatsiya uzellari guruhlashni har qanday prinsipi bo‘yicha guruhlarga yoki nimtarmoqlarga birlashtirilishi mumkin.

Mantiqan yo‘naltirilgan ko‘rib chiqish qo‘yilgan yuqori tezlikli (IP/MPLS domenlarida LSP traktlari, Frame Relay kanallari, virtual traktlar va ATM virtual kanallari) va past tezlikli tarmoqlarning “nuqta-nuqta” topologiyasi asosida ulanishi tashkil etilgan yo‘lni ko‘rsatish imkonini beradi.

Tarmoqni boshqarish platformasi quyidagilarni taqdim etishi kerak:

- tarmoq elementlariga texnik xizmat ko‘rsatishni tashkil etish uchun mablag‘lar va kompaniyaning texnik, hisob-kitob va marketing xizmatlarining o‘zaro aloqalari;

- qurilmaning konfiguratsiyasini boshqaruvchi va tarmoq holatini kuzatuvchi operatorlar va ma’muriyatlar uchun imkoniyatlarni keng spektri.

Telekommunikatsiya tarmog‘ining barqaror ishlashining asosi barcha xizmatlar orasida tezkor, statistik va boshqa axborotlarni taqsimlanishi, kompaniyaning barcha bo‘linmalarining yaxshi o‘zaro aloqalarini ta’minlash hisoblanadi.

Tarmoqni boshqarish platformasi tarmoqda rad etishlar yoki o‘ta yuklanishlar yuzaga kelganda quyidagi vazifalarni hal etishni ta’minlovchi dasturiy vositalarga ega bo‘lishi kerak:

- haqiqiy vaqt rejimida avariya to‘g‘risidagi xabarlarni kommutatsiya uzellari, aloqa liniyalari, interfeyslar va abonent oxirgi qurilmalari guruhlari bo‘ylab saralash va taqsimlash;

- yuzaga kelgan muammolarni tezkor yechish uchun zarur bo‘ladigan axborotlarni, avariya xabarlari bilan bir vaqtda olish;

- amalga oshirilgan harakatlar natijalari to‘g‘risida, nosozliklarni sababi to‘g‘risida, shuningdek mazkur muammo bilan shug‘ullangan avariya xizmati operatori yoki muhandisining ismi-sharifi to‘g‘risidagi axborotni qayd qilish;

- har bir tarmoq elementi bo‘yicha, shu jumladan foydalanuvchi axborotni uzatadigan uzel, modul, port yoki kanal bo‘yicha rad etishlar va to‘xtab qolishlarning miqdori va davomiyligi to‘g‘risida, statistik axborotni yig‘ish, to‘plash va o‘qish.

Bu axborot tarmoqning ishlash qobiliyatini tahlil qilish va mijozlar bilan o‘zaro hisob-kitob qilish uchun foydalanilishi kerak.

**Tarmoqni boshqarish jarayonlarini rejalashtirish va tashkil etish (E.412, E.413 tavsiyalari).** Telekommunikatsiya tarmog‘ining holati quyidagi sabablar natijasida vaqt bo‘yicha o‘zgaradi:

- foydalanuvchilar yaratadigan trafikning o‘zgarishi;
- qurilmalarning shikastlanishi;
- avariyalar;

- xizmatlar ishidagi rejalashtirilgan tanaffuslar.

*Katta yuklanish kunlarini rejalashtirish.* Katta yuklanishni yuzaga keltirishi mumkin bo‘lgan voqealar orasidan quyidagilarni ko‘rsatish mumkin:

- umumiy bayramlar – yangi yil, Navro‘z;
- har yilning aynan bir kuniga to‘g‘ri kelmaydigan diniy bayramlar, sportning ommaviy turlari bo‘yicha jahon chempionatlari yoki qit’a birinchiliklari;
- milliy bayramlar;
- nodavriy voqealar, jumladan, savdo yarmarkalari, davlat arboblarining rasmiy tashriflari, xalqaro konferensiyalar va yig‘ilishlar.

Katta yuklanish kunlari uchun rejalar tuzishda quyidagi chegaralarni nazarda tutish kerak:

- qo‘shimcha kanallarni ishga tushirish;
- kanallarni ikki tomondan band qilish yo‘nalishlaridan bir tomondan band qilishga o‘tkazish;
- trafikni odatda foydalanilmaydigan tranzit uzellar orqali marshrutlashtirishni nazarda tutadigan aloqa yo‘nalishlari rejasini o‘zgartirish;
- odatdagi tranzit uzellarning o‘ta yuklanishini bartaraf etish;
- katta yuklanishlar davrida yuzaga kelishi mumkin bo‘lgan qiyinchiliklar to‘g‘risida foydalanuvchilarni xabardor qilish;
- rejani ishlab chiqishda qo‘llaniladigan mezonlarni asoslash.

*Qurilmaning shikastlanish vaziyatlari.* Shikastlanishlarning oldini olish rejalarini tuzishda, agar shunday rejalarni tarmoq ob’ektlarini kuzatish tajribasidan kelib chiqib tuzish imkoni bo‘lsa, unga quyidagilarni kiritish zarur:

- shikastlanish miqyoslari aniqlanmagan sharoitda qabul qilinadigan dastlabki choralar;
- shikastlanish sabablari va miqyoslari aniqlangandan so‘ng qabul qilinadigan keyingi choralar;
- tarmoq ishida yuzaga kelgan sharoitlarni baholash.

Tarmoqda shikastlanishlarga aks ta’sir ko‘rsatish rejalariga quyidagi choralar kiritilishi kerak:

- shikastlanish ta’sir ko‘rsatgan punktlarni yoki boshqa ob’ektlarni identifikatsiya qilish;

- tarmoqni profilaktika qilish maqsadida shikastlangan yoki vaqtincha o‘chirib qo‘yilgan (uzib qo‘yilgan) uchastkalarini aylanib o‘tish uchun foydalaniladigan, aylanma yo‘llar bo‘yicha trafikni vaqtincha yo‘naltirish;

- foydalanuvchilar uchun maxsus yo‘riqnomalar;

- rejani bajarish mezonlari (mazkur reja foydalaniladigan shartlar ro‘yxati).

*Avariyalar*. Avariyalarni oldindan bilish muammoli masala, ammo ularning oqibatlarini ma’lum bir aniqlikda oldindan ko‘ra bila olish maqsadga muvofiqdir. Avariya holatlariga munosabat bildirish rejalariga quyidagilar kiritilishi kerak:

- manfaatdor ma’muriyatlar, xususiy tarmoq xizmatlari va foydalanuvchilarning xabarnomalari ro‘yxatlari;

- avariya sharoitida amalga oshirilishi kerak bo‘lgan harakatlar ro‘yxati;

- xodimlar shtatini oshirish va ish vaqti davomiyligini oshirish bilan bog‘liq choralar.

*Xizmatlar ishidagi rejali tanaffuslar*. Tarmoq uchastkalari, uzellari va stansiyalari ishida ko‘zda tutilgan tanaffuslar vaqtida quyidagi choralarni ko‘rish zarur:

- boshqa ma’muriyatlar talab qiladigan nazorat jarayonlari;

- manfaatdor operatorlar uchun mo‘ljallangan shoshilinch chaqiruvlarni o‘rnatish jarayonlari.

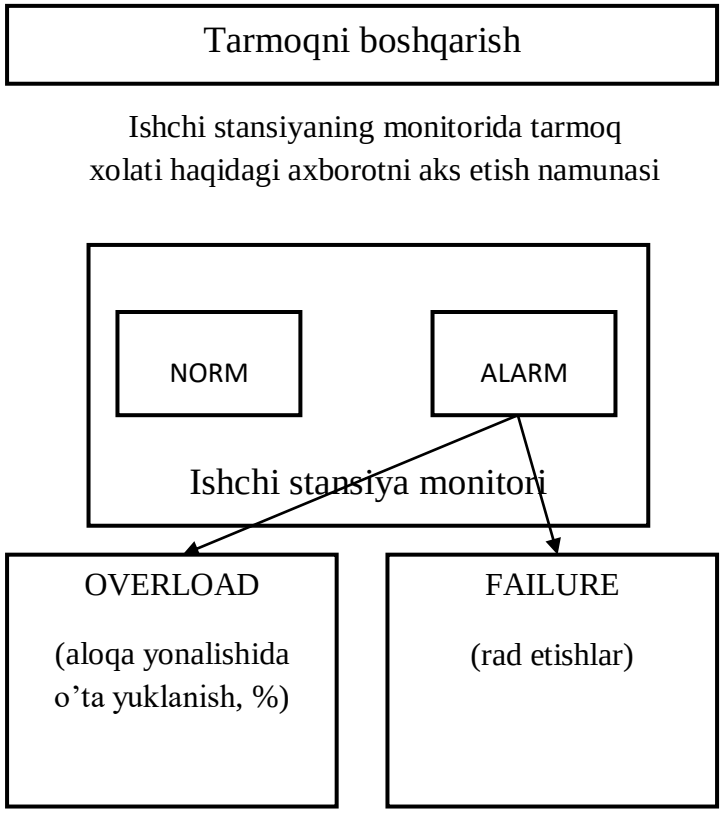
*Tarmoqni boshqarishni tashkil etish* (E.413 tavsiyasi). Tarmoqni boshqarishni tashkil etish quyidagilarni o‘z ichiga oladi:

- tarmoqni boshqarish uchun xizmatlarning o‘zaro ta’sirini tashkil etish va rejalashtirish;

- tarmoqni boshqarish buyruqlarini harakatga kiritish va chiqarish;

- tarmoqni boshqarish tizimini rivojlantirish.

*Ishchi stansiya monitorida tarmoqning holati haqidagi axborotning aks ettirilishi.* Tarmoq tomonidan taqdim etilayotgan xizmatlar sifati to‘g‘risidagi axborot, xizmatlarni boshqarish sathi ishchi stansiyasi (WS) monitorida tezkor tarzda aks ettirilishi kerak (6.2-rasm).




6.2-rasm. Ishchi stansiya monitorida tarmoq holatini aks ettirilish namunasi

Xizmat ko‘rsatish sifatining har bir ko‘rsatkichiga ma’lum bir chegara qo‘yilishi kerak. Agar xizmatlar sifatining birorta ham ko‘rsatkichlari chegaraga yetmasa, u holda monitorda «NORM» aks etadi. Aks holda «ALARM» aks etadi. Tahlikali holat quyidagi sharoitlarda yuzaga kelishi mumkin:

- aloqa yo‘nalishida o‘ta yuklanish (Overload), %;
- qurilmalarning rad etishlari (Failure).

## 6.3. Tarmoqni boshqarish masalalari

TMN ga tegishli ITU-T tavsiyalarida, vazifalarning barcha to‘plami quyidagi boshqarish guruhlariga bo‘linadi (6.1-jadval):

- biznes;
- tarmoq konfiguratsiyasi;
- rad etishlarni bartaraf etish;
- sifatni;
- axborotni himoyalash;
- o‘zaro hisob-kitoblar.

*Biznesni boshqarish deganda:*

- tarmoq operatorlarining tizimli maqsadlarini aniqlash va unga erishish;
- boshqa tarmoqlarning (zona, qit’a, dunyo) operatorlarini boshqarish tizimlarining o‘zaro aloqasi;
- tarmoqni boshqarishning usullari va vositalarini belgilab beruvchi, tartibga soluvchi xujjatlarni ishlab chiqish tushuniladi.

*Konfiguratsiyani boshqarish deganda* (Configuration Management, SM):

- tarmoqni raqamlash rejasini yaratish va kuzatib borish;
- tarmoqni shakllantirish va rivojlantirish;
- tarmoqni va uning ayrim elementlarining rekonfiguratsiyasi;
- rivojlanish bilan bog‘liq xizmatlar va ishlarni rejalashtirish;
- tarmoqni ma’lumotlar bazalarini yaratish va yuritish tushuniladi.

Bu vazifalar tarmoq parametrlarini va boshqariluvchi elementlarni konfiguratsiyalashdan iborat. Shlyuzlar, marshrutizatorlar, multipleksorlar va boshqa elementlar uchun bu vazifalar guruhi yordamida tarmoq manzillari, identifikatorlar, geografik holati aniqlanadi, tarmoq elementlari orasidagi aloqalar va foydalanish jarayonida bu aloqalarning o‘zgarishi, yangi mantiqiy yoki fizik kanallarning tashkil etilishi, kommutatsiyalash va marshrutlashtirish jadvallarining o‘zgarishi aks ettiriladi.

6.1-jadval

Tarmoqni boshqarish masalalari

| Tarmoqni boshqarish sathlari | Boshqarish masalalari | | | | |
|---|---|---|---|---|---|
| | Konfiguratsi-yalarni | Rad etish oqibatlarini bartaraf etish | Sifatni | O‘zaro hisoblashlarni | Axborotni himoyalashni |
| Biznesni | - | | - | - | - |
| Xizmatlarni | | | - | | |
| Tarmoqni | - | - | - | - | |
| Tarmoq elementlarini | | - | - | | - |

*Rad etishlar oqibatlarini bartaraf etishni boshqarish* (Fault Management, FM) deganda:

- nosozliklarni aniqlash, ularni ko‘payishiga yo‘l qo‘ymaslik va bartaraf etish;
- tarmoqning barcha muhim elementlari holatini haqiqiy vaqtda nazorat qilish;
- tarmoqni tezkor rekonfiguratsiyalash;
- nosozliklarni bartaraf etish;
- ishdan chiqqan aloqa qurilmasini tiklash jarayonlarini boshqarish;
- rad etishlar to‘g‘risidagi xabarlarni qayd etish, filtrlash va aks ettirish;
- nosozliklarni qayd etish qaydnomasini yuritish;
- foydalanilayotgan tarmoq modeli va uning elementlari asosida xabarlarni korrelyatsion tahlil qilish;
- tarmoqdagi reglamentli va avariya holatlaridagi ishlar haqida foydalanuvchilarni o‘z vaqtida xabardor qilish tushuniladi.

Vazifalarning bu guruhi yana o‘z ichiga tarmoq ishidagi to‘xtab qolishlar va rad etishlarning oqibatlarini aniqlash, tavsiflash va bartaraf etishni qamrab oladi. Bu sathda faqat xatoliklar to‘g‘risidagi xabarlarni qayd etishgina emas, balki ularni ma’lum bir korrelyatsion model asosida filtrlash, marshrutlash va tahlil qilish ishlari

ham bajariladi. Filtrlash, xatoliklar to‘g‘risidagi xabarlarning jadal oqimidan faqat eng muhim xabarlarni ajratib olishga imkon beradi. Marshrutlash, ularni kerakli elementga yetkazib berishni ta’minlaydi, korrelyatsion tahlil esa o‘zaro bog‘liq xabarlarning oqimini yuzaga keltirgan sababni (masalan, kabelning uzilishi, tarmoqlar va serverlarga kirish mumkin emasligi to‘g‘risida katta miqdordagi xabarlarning sababchisi bo‘lishi mumkin) topishga imkon beradi. Xatolarni bartaraf etish avtomatik tarzda ham, yarimavtomatik tarzda ham bo‘lishi mumkin.

*Taqdim etilayotgan xizmatlar sifatini boshqarish* (Performance Management, RM) deganda:

- trafikni boshqarish;
- xizmatlar sifatini oshirish va ularning turini kengaytirish;
- taqdim etilayotgan xizmatlarning sathi haqidagi bitimlarni ishlab chiqish, xulosa chiqarish va ijrosini nazorat qilish (SLA);
- tarmoqlar va ularning elementlarini faoliyat yuritishi to‘g‘risidagi statistik ma’lumotlarni to‘plash va tahlil qilish (tarmoq resurslaridan foydalanish samaradorligini hisobga olish va tarmoq hamda uning elementlari ishlashining ishonchliligini nazorat qilish);
- telekommunikatsiya tarmoqlarining ekspluatatsion tavsiflarini yaxshilash uchun aloqa xizmatlarini taqdim etishni yaxshilash va assortimentini kengaytirish uchun tavsiyalar ishlab chiqish;
- aloqa tarmoqlarini boshqarish usullarini takomillashtirish maqsadida boshqarish va nazorat qilish tizimlarining faoliyat yuritilishini tahlil qilish;
- xizmatlar sifatini boshqarish tizimining ta’sirchanligini tahlil qilish (u yaratilgandan so‘ng) va uni takomillashtirish tushuniladi.

Bu guruhning vazifalari to‘plangan statistik axborot asosida tizimning ta’sir ko‘rsatish vaqti, virtual yoki fizik aloqa kanalining o‘tkazish qobiliyati, tarmoqning kanallari va alohida segmentlarida trafikning jadalligi, tarmoq orqali ma’lumotlarni uzatishda ularning buzilish ehtimolligi, shuningdek tarmoqning tayyorgarlik

koeffitsienti kabi parametrlarini baholash bilan bog‘liq. Tarmoq resurslarini qo‘llash samaradorligini, tarmoq va uning elementlari ishonchliligini nazorat qilish funksiyasi, tarmoqni tezkor boshqarish singari tarmoqni rivojlantirishni rejalashtirish uchun ham zarurdir.

*O‘zaro hisoblashlarni boshqarish* (Accounting Management, AM) deganda:

- taqdim etilayotgan xizmatlar to‘g‘risida ma’lumotlar to‘plash;
- taqdim etilayotgan aloqa vositalari va xizmatlari uchun tariflar ishlab chiqish va takomillashtirish;
- taqdim etilayotgan xizmatlar hajmi va nomenklaturasini hamda ularning narxlarini hisobga olish;
- ko‘rsatilgan xizmatlar uchun to‘lovlar summasini hisobga olish;
- ko‘rsatilgan xizmatlar hajmi va nomenklaturasi hamda ularga to‘lovlar masalasi bo‘yicha abonentlarga ma’lumotnoma-axborotli xizmat ko‘rsatish;
- istalgan qonuniy shaklda xizmat ko‘rsatish uchun aloqa operatorlari bilan shartnomalar tuzgan abonentlarni ro‘yxatga olish va hisobini olib borish;
- taqdim etilgan xizmatlar uchun to‘lovlarni nazorat qilish.

Tarmoqni avtomatlashtirilgan boshqarish masalalarini hal etish uchun boshqarish tizimi (BT) va boshqarish ob’ektlari – tarmoq elementlari (NE) o‘rtasida jadal ma’lumotlar almashinuvi zarur. Tarmoqni boshqarish tizimlarining intellektual vazifalari, bir vaqtda faoliyat yurituvchi amaliy jarayonlar uchun hisoblash resurslarini ajratishni ta’minlovchi kuchli operatsion tizim va boshqarishning o‘ziga xos masalalarini yechishni ta’minlovchi amaliy dasturiy ta’minoti bo‘lgan kompyuterlar majmui bilan amalga oshiriladi.

*Axborotni himoyalashni boshqarish* (Security Management, SM) deganda:

- xususiy texnologik axborotni va foydalanuvchilarning maxfiyligini ta’minlash uchun me’yorlarni ishlab chiqish;
- noqonuniy ulanishdan tarmoqni xavfsizlik sathini sinfini ta’minlash;
- ma’lumotlarni taqdim etishda konfedensiallikka rioya etish;

- ma’lumotlarni butunligini himoyalash va saqlash;
- foydalanuvchilarni avtorligini nazorat qilish;
- aloqa xizmatlariga turli ulanish sathlarini ta’minlash;
- aloqa xizmatlariga noqonuniy ulanish xodisalari haqida hisobot tuzish;
- personallar uchun turli avtorlik sinflarini ta’minlash.

Bu guruh vazifalariga tarmoq resurslariga ulanishni nazorat qilish va ma’lumotlarni tarmoq orqali uzatishda ularni saqlash va butunligini ta’minlash kiradi.

Xavfsizlikni boshqarishni asosiy elementlari quyidagilar hisoblanadi:

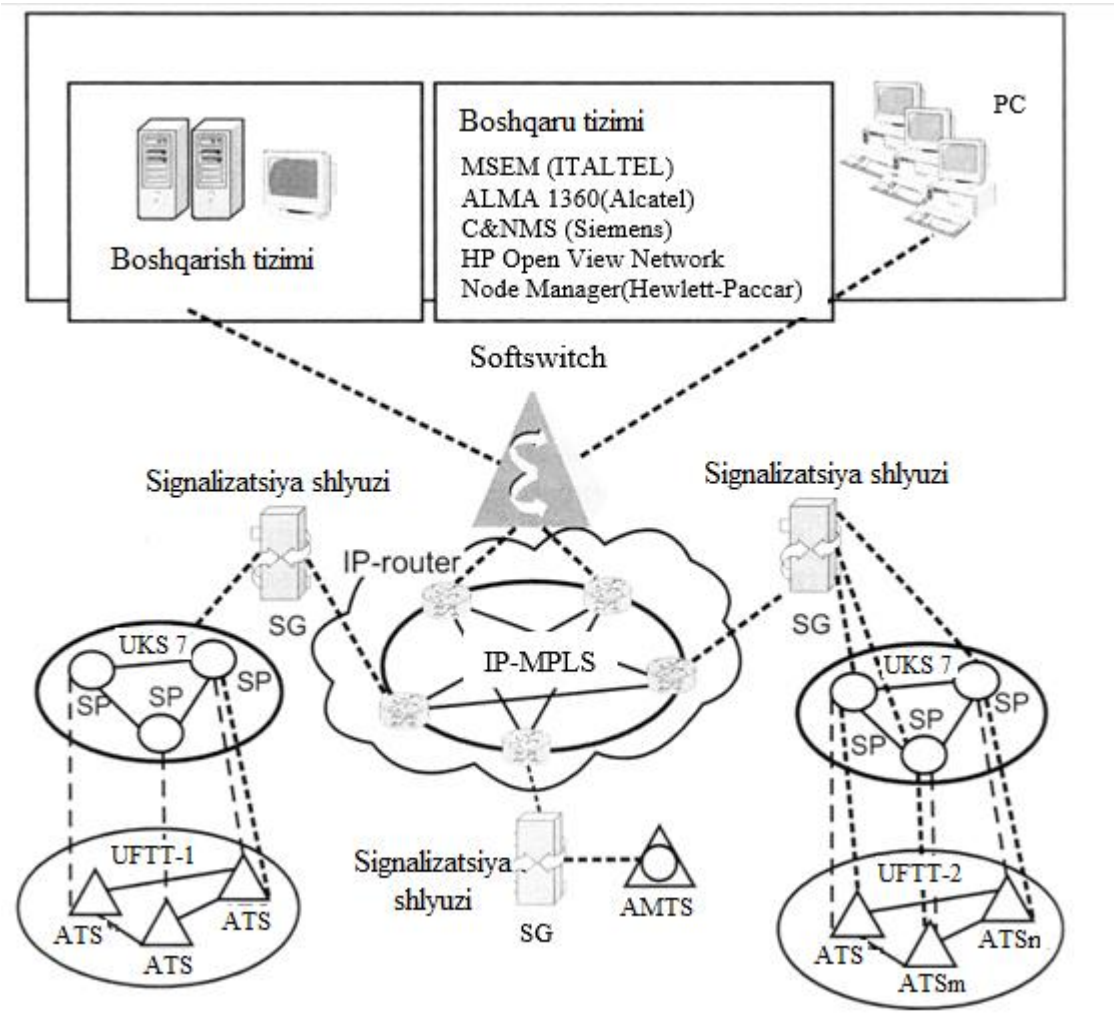
- foydalanuvchilarni autentifikatsiyalash jarayoni;
- tarmoq resurslariga ulanish huquqini tekshirish va belgilash;
- shifrlash kalitlarini qo‘llab-quvvatlash va taqsimlash, vakolat bilan boshqarish.

Tarmoqni boshqarishni kompleks masalalariga quyidagilar kiradi:

- ishga tushirishdan oldin:
- tarmoqni resurslari va tuzilishini rejalashtirish;
- ma’lumotlar bazasini yaratish;
- qurilmalarni o‘rnatish;
- foydalanish jarayonida:
- resurslarni ma’muriy boshqarish;
- trafikni boshqarish;
- tarmoq elementlari orasida yo‘qolgan aloqani qayta tiklash;
- xizmatlar sifatini nazorat qilish;
- foydalanuvchilar bilan hisoblarni boshqarish;
- tarmoqni modernizatsiyalash;
- trafikni oldindan aytish.

Tarmoqni avtomatlashtirilgan boshqarish masalasini yechish uchun boshqarish tizimi (BT) va tarmoq elementlari (NE) - boshqarish ob’ektlari orasida ma’lumotlar jadal almashishi zarur.

Boshqarish tizimi uchun platforma sifatida MSEM (Italtel), ALMA 1360 (Alcatel), C&NMS (Siemens), HP Open View Network Node Manager (Hewlett-Packard) foydalanilishi mumkin (6.3-rasm).




6.3-rasm. NGN ni boshqarish tizimi

BT va tarmoqlar hamda ularning elementlari (NE) o‘rtasida axborot almashinuvi IP/MPLS texnologiyasi qo‘llanilgan transport tarmog‘i va UKS7 signalizatsiya tarmog‘i tomonidan ta’minlanishi kerak. Bu tarmoqlarning tavsiflariga qat’iy talablar qo‘yilgan (yuqori tezlikda ma’lumotlar uzatish, xabarlarni jo‘natish ehtimolligining kichikligi, yashovchanlik darajasining yuqoriligi).

BT va boshqarish ob’ektlari orasidagi telekommunikatsiya infrastrukturasi hisoblanuvchi, transport tarmoqqa bo‘lgan talablar M.3010, Q.811, Q.812 tavsiyalarga mos kelishi kerak.

## 6.4. Transport tarmoq yadrosida trafikni boshqarish prinsiplari

Tarmoq trafigi bir necha belgilar bo‘yicha tasniflanishi mumkin:

- Internet xizmatlari va ilovalari turlari bo‘yicha (HTTP, FTP, Telnet va b.q.);
- manbalar turlari bo‘yicha;
- qabul qiluvchining manzili bo‘yicha;
- foydalanuvchilar guruhi bo‘yicha;
- Internet xizmatlari guruhi bo‘yicha;
- Internet resurslari bo‘yicha (masalan, o‘ziga xos URL bo‘yicha);
- yo‘nalishlar bo‘yicha (kiruvchi yoki chiquvchi);
- o‘tkazish oralig‘ini boshqarish mezonlari bo‘yicha.

MPLS texnologiyasi qo‘llanilgan tarmoqlarda trafikni boshqarish imkoniyatlari.

IP/MPLS texnologiyasiga ega tarmoqlarda trafikni boshqarish quyidagi funksional vositalar va imkoniyatlarning mavjud bo‘lishini nazarda tutadi:

- uzatilayotgan paketlarning birlashgan oqimlari bilan bog‘langan atributlar to‘plami;
- resurslar bilan bog‘liq bo‘lgan (topologik cheklanish) atributlar to‘plami;
- berilgan parametrlar to‘plamiga muvofiq marshrutni tanlashda qo‘llaniladigan cheklanishlar asosidagi marshrutlash.

Yuqorida keltirilgan barcha atributlar birgalikda boshqaruvchi o‘zgaruvchilarni ifodalaydi. Ular ma’murning harakatlari natijasida yoki avtomatik tarzda modifikatsiyalanishi mumkin.

Tarmoq faoliyati vaqtida, mazkur atributlar haqiqiy vaqt rejimida dinamik tarzda o‘zgarishi mumkin bo‘lsin.

## Nazorat savollari

1. Telekommunikatsiyani boshqarish tarmog‘ining vazifasi nimadan iborat?
2. TMN arxitekturasida funksional bloklarning vazifasini tushuntiring.
3. TMNning fizik arxitekturasi bloklarining vazifasini tushuntiring.
4. LLA arxitekturasida boshqarishning nechta sathi mavjud?
5. Tarmoqni boshqarishni asosiy muammolari nimadan iborat?
6. Tarmoqni boshqarish platformasi qanday masalalarni yechish uchun moslashgan?
7. Tarmoqda rad etish yoki o‘ta yuklanish bo‘lgan hollarda qanday vazifalarni hal etish kerak?
8. Tarmoqni boshqarish jarayonida nimalar rejalashtiriladi?
9. Tarmoqni boshqarish masalalari nimadan iborat?
10. Rad etish oqibatlarini bartaraf etish qanday boshqariladi?
11. Taqdim etilayotgan xizmatlar sifati qanday boshqariladi?
12. O‘zaro hisoblashlar qanday boshqariladi?
13. Axborotni himoyalash qanday boshqariladi?

# 7. MULTIMEDIALI ALOQA TARMOQLARINI MODELLASHTIRISH

## 7.1. IP-tarmoq bo‘ylab multimediali trafikni uzatish jarayonini modellashtirish

Multimediali aloqa tarmoqlari ko‘p miqdordagi abonentlarni IP-telefoniya, eshittirish, audio va video dasturlar, talab bo‘yicha televideniya kabi turli xil multimediali xizmatlarga haqiqiy vaqt miqyosida ulanishini ta’minlaydi. Kommunikatsiya qurilmalarni ishlab chiqarilishini tez o‘sishi, bu tarmoqlarda haqiqiy vaqt miqyosida multimediali ma’lumotlarni uzatish uchun TCP/IP protokolidan foydalanish imkonini beradi.

Multimediali xizmatlarni taqdim etish sifati, ma’lumotlarni uzatishda kechikishlarga va xizmatni taqdim etuvchi axborot serveri bilan abonent o‘rtasidagi dispersiyaga sezgirdir. Lokal IP-tarmoqda o‘rnatilgan transport ulanishi bo‘yicha video trafikni uzatishda, xizmat ko‘rsatish sifati QoS parametrlarini baholash uchun quyida keltirilgan modelni ko‘rib chiqamiz. Bu model katta o‘lchamdagi bir jinsli bo‘lmagan tarmoqlarga xizmat ko‘rsatish, berk telekommunikatsiya tarmoqlarini tahliliy modellash usuliga asoslanadi. U quyidagilarga imkon beradi:

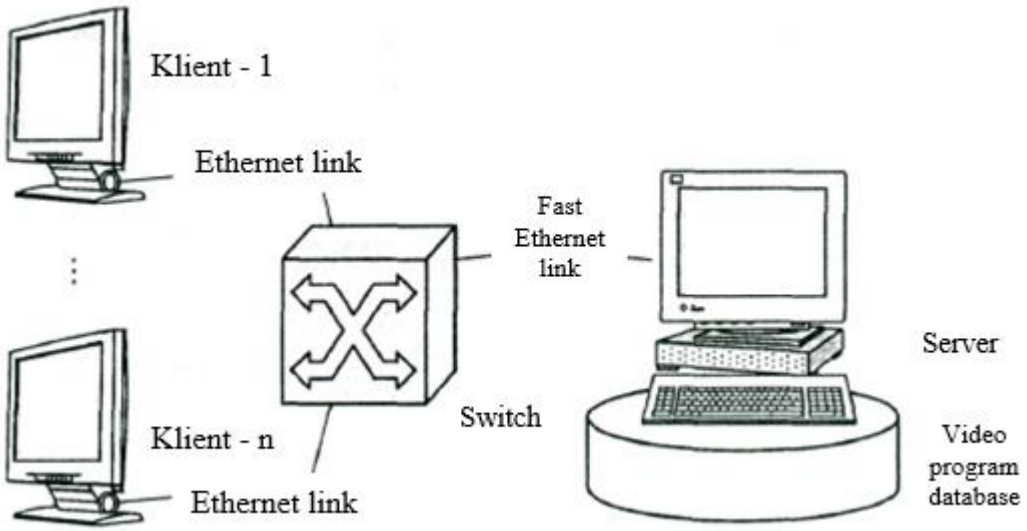
- yanada yuqori adekvatlik darajasi bilan telekommunikatsiya tarmog‘ining faoliyat ko‘rsatishining eng muhim tomonlarini aks ettirish;
- telekommunikatsiya tarmog‘ining ehtimoliy-vaqtli xarateristikalarini (EVX) keng to‘plamini baholash, shu jumladan tadqiq etilayotgan transport ulanishlarining QoS parametrlarini baholash.

Konseptual model.

Videodasturlarni mahalliy IP-tarmog‘i orqali uzatish jarayonini ko‘rib chiqamiz. Tarmoqning kommutatsiyalash muhiti (7.1-rasm) odatdagi besh qavatli uyning tarmog‘iga ulanish uchun eng ma’qul bo‘lgan, GISCO firmasining masalan, Catalysi 351 2XI (yoki Catalysi 352 4XI yoki Catalysi 354 8XI) faol kommutatori asosida

tashkil etilgan. Abonentning shaxsiy kompyuteri asosida tashkil etilgan ishchi stansiya, kommutatorga IFFF 8023.34 standartiga muvofiq Fast Ethernet porti orqali ulangan. Bunday port orqali ma’lumotlarni maksimal uzatish tezligi 100 Mbit/s ni tashkil etadi. Axborot serveri kommutatorga IFFF 8023.37 standartiga muvofiq Gigabit Ethernet porti orqali ulangan. Bunday port orqali maksimal uzatish tezligi 1000 Mbit/s ni tashkil etadi.

Faraz qilaylik, tarmoq abonentlari buyurtma qilingan video dasturlarni qabul qilish uchun axborot serveridan foydalanadilar. Shu maqsadda ular server bilan ulanishni o‘rnatadilar. Budjet identifikatsiya qilinganidan va tekshirilganidan so‘ng, ularni qiziqtiruvchi video dasturlar tanlab olinadi va ularni o‘z ishchi stansiyalarida haqiqiy vaqt masshtabida ko‘rishni boshlaydilar. Faraz qilaylik, ma’lum bir vaqtda abonent bir paytda server bilan TCP-transport ulanishni o‘rnatishdi va tanlangan dasturlarni ko‘rishmoqda, deylik.




7.1-rasm. Talab bo‘yicha videoxizmatni taqdim etish uchun telekommunikatsiya tizimining tuzilishi

Tarmoqda shunday topologiya bilan bunday xizmatni taqdim etish sifati parametrlarini baholash uchun model ishlab chiqilgan bo‘lib, ular quyidagi parametrlar sinfini hisobga oladi:

- axborot yuklanishi parametrlar;
- texnik parametrlar;
- dasturiy parametrlar.

**Axborot yuklanish parametrlar.** Abonentga olib ko‘rsatilayotgan videooqim MPEG standartiga muvofiq raqamli ko‘rinishda kodlanadi. Shu standartga muvofiq tasvirni regeneratsiyalash chastotasi sekundiga 26 yoki 30 ta kadrdan iborat bo‘lgan raqamli video oqim, video kadrlarning /W/Z guruhli ketma-ketlikdan iborat (GOP – group of puctures). Har bir guruh qayd qilingan uzunlikka va tuzilishga ega. Har bir guruh tarkibida uch turdagi video kadrlar ajratiladi (VOP – Video Object Plane):

- I – kadr (tayanch);
- P – kadr (bashorat qilingan);
- B – kadr (ikki tomonga yo‘naltirilgan).

Video oqimning har bir guruhi undagi yagona i-kadrdan boshlanadi. Video oqimning *M* parametri guruhdagi kadrlarning umumiy sonini, *Z* parametr esa P-kadrlar orasidagi intervalni aniqlaydi. Modelda hisobga olinadigan axborot yuklangan parametrlar 7.1-jadvalda keltirilgan.

Tarmoqning texnik parametrlariga quyidagilar tegishli bo‘ladi: foydalanilayotgan telekommunikatsiya muhitining tarkibi va tuzilmasi, foydalaniladigan aloqa liniyalari parametrlari (uzunligi, o‘tkazish qobiliyati, shuningdek bit xatolik ehtimoli (BER)), foydalanilayotgan (axborot serveri va ishchi stansiyalar) hisoblash texnikasi vositalarining samaradorligi, foydalanilayotgan kommutatsiya qurilmasining samaradorligi (kommutatsiya matritsaning samaradorligi va kommutatorning bufer xotirasining hajmi). Tarmoqning texnik parametrlari ro‘yxati 7.2-jadvalda keltirilgan.

7.1-jadval

Foydalanuvchining ishchi stansiyasiga keladigan video trafikning parametrlari

| | | | |
|---|---|---|---|
| i-foydalanuvchi uchun video trafik tavsiflari | | i-foydalanuvchi uchun VOP kirib kelishi intensivligi, $\lambda_i^{vop}$ | $\lambda_i^{vop} = 25$ VOP/s |
| | | VOP ning o‘rtacha o‘lchami, $S_i^{vop}$ | $S_i^{vop} = 360 \cdot 240$ piksel |
| | | I:P:B kadrlar kodlash sxemasi | 1:1 P:4 B:10 |
| Kadrlarning tavsifi | I | i-foydalanuvchi uchun 1-kadrlarning kirishi intensivligi, $\lambda_i^1$ | $\lambda_i^1 = 1{,}67$ kadr/s |
| | | 1-kadrning o‘rtacha o‘lchami, $S_i^1$ | $S_i^1 = 1457$ bayt |
| | P | i-foydalanuvchi uchun P-kadrlarning kelish intensivligi $\lambda_i^P$ | $\lambda_i^P = 6{,}67$ kadr/s |
| | | P-kadrning o‘rtacha o‘lchami, $S_i^P$ | $S_i^P = 486$ bayt |
| | B | i-foydalanuvchi uchun B-kadrlarning kelish intensivligi $\lambda_i^B$ | $\lambda_i^B = 16{,}67$ kadr/s |
| | | B-kadrning o‘rtacha o‘lchami, $S_i^B$ | $S_i^B = 182$ bayt |

Tanlangan video dasturni raqamli uzatishni tashkil etish uchun abonentning ishchi stansiyasidagi mijoz va raqamli video ko‘rsatuv serveri o‘rtasida TCP-ulanish o‘rnatiladi. Video kadrlar TCP-segmentlarga kiritiladi va IP-paketlar ko‘rinishida tarmoq bo‘ylab ishchi stansiyagacha uzatiladi. Uzatishda bu IP-paketlar tasodifiy kechikishga uchraydi, ular noto‘g‘ri qabul qilinishi yoki yo‘qolishi mumkin. Bularning hammasi tegishli TCP-segmentlarning takroriy uzatilishini yuzaga keltiradi va video kadrlarning qo‘shimcha kechikishiga, shuningdek ularning qayta tartibga solinishiga sabab bo‘ladi.

7.2-jadval

Telekommunikatsiya muhitining texnik parametrlari

| | | |
|---|---|---|
| Kommutatordan i-ishchi stansiyasigacha zveno | $L_i$ masofa | $l_i = 100$ m |
| | O‘tkazish qobiliyati | $V_i = 10^6$ bit/s |
| | BER, $p_1$ | $p_i = 10^{-6}$ $b^{-1}$ |
| Kommutatordan servergacha zveno | $I_x$ masofa | $I_x = 1000$ m |
| | O‘tkazish qobiliyati, $V_x$ | $V_x = 10^9$ bit/s |
| | BER, $p_x$ | $p_x = 10^{-6}$ $b^{-1}$ |
| Server | Unumdorlik, $V_{sv}$ | $V_s = 10^6$ MFLOP/c |
| i-ishchi stansiya | Unumdorlik, $V_i$ | $V_i = 10^5$ bit/s |
| Kommutator | O‘tkazish qobiliyati,$V_{Sw}$ | $V_{Sw}$=4.8 Mp/s |
| | Kommutatorning bo‘linadigan xotira o‘lchami $S_M$ | $S_M$=4 Mb |
| Kommutator porti 100BaseT | O‘tkazish qobiliyati (paketlar/s), $V_i$ | $V_i$=14880 p/s |
| Kommutator porti 1000BaseX | O‘tkazish qobiliyati (paketlar/s), $V_x$ | $V_x$=1488000 p/s |

Dasturiy parametrlarga quyidagilar kiradi: turli sathdagi ma’lumotlarni uzatishda foydalaniladigan protokollar, TCP/IP protokollarini har xil turdagi paketlarning maksimal o‘lchamlari, bu paketlardagi xizmat axborotlarining o‘lchamlari, TCP-ulanishlarini boshqarish jarayonlaridagi darchalarning o‘lchamlari, bu transport ulanishlarining taym-autlar davomiyligi. Tarmoqning dasturiy parametrlarining ro‘yxati 7.3-jadvalda keltirilgan.

7.3-jadval

Tarmoqning dasturiy parametrlari

| | | |
|---|---|---|
| Qo‘llaniladigan protokollar | Transport sathi | TCP |
| | Tarmoq sathi | IP |
| | Kanal va fizik sath | IEEE.802.3u |
| | | IEEE.802.3z |
| Protokollar parametrlari | TCP-segmentning maksimal o‘lchami, $s_i^{TCP}$ | 1500 bayt |
| | IP-paketning maksimal o‘lchami, $s_i^{IP}$ | 1500 bayt |
| | MAC-kadrning maksimal o‘lchami, $s_i^{MAC}$ | 1536 bayt |
| | TCP-oqimlarini boshqarish oynasini o‘lchami, $\tau_w$ | $\tau_w$=500 ms |
| | TCP-taym-aut o‘lchami, $\tau_{TO}$ | $\tau_{TO}$=200 ms |
| | TCP-segmenti sarlavhasining o‘lchami, $s^{TCP}$ | $s^{TCP}$=20 bayt |
| | IP-paketi sarlavhasining o‘lchami, $s^{IP}$ | $S^{IP}$=20 bayt |
| | Tasdiqlanish paketining o‘lchami, $s^{Ack}$ | $S^{Ack}$=20 bayt |
| | MAC-kadrning sarlavha o‘lchami, $s^{MAC}$ | $S^{MAC}$=20 bayt |
| Serverning dasturiy parametrlari | Bitta I-kadrni uzatish uchun serverga zarur MFLOPni o‘rtacha soni – $\alpha_I^{Sv}$ | $\alpha_I^{Sv} v_{Sv}^{-1}$=0.05 mls |
| | Bitta P- kadrni uzatish uchun serverga zarur MFLOPni o‘rtacha soni – $\alpha_P^{Sv}$ | $\alpha_P^{Sv} v_{Sv}^{-1}$=0.03 mls |
| | Bitta B- kadrni uzatish uchun serverga zarur MFLOPni o‘rtacha soni – $\alpha_B^{Sv}$ | $\alpha_B^{Sv} v_{Sv}^{-1}$=0.02 mls |
| | Bitta tasdiqqa ishlov berish uchun serverga zarur MFLOPni o‘rtacha soni – $\alpha_{Ack}^{Sv}$ | $\alpha_{Ack}^{Sv} v_{Sv}^{-1}$=0.02 mls |
| i-ishchi stansiyaning dasturiy parametrlari | Bitta I-kadrni qabul qilish uchun i-ishchi stansiyaga zarur MFLOPni o‘rtacha soni – $\alpha_I^i$ | $\alpha_I^i$=0.5 mls |
| | Bitta P- kadrni qabul qilish uchun i-ishchi stansiyaga zarur MFLOPni o‘rtacha soni– $\alpha_P^i$ | $\alpha_P^i$=0.3 mls |
| | Bitta B- kadrni qabul qilish uchun i-ishchi stansiyaga zarur MFLOPni o‘rtacha soni– $\alpha_B^i$ | $\alpha_B^i$=0.2 mls |

Axborot parametrlarining qiymatlari umumiy raqamli video oqimlar statistikasiga mos keladi. Yuqorida tavsiflangan lokal tarmoqning faoliyat yuritishi uchun asosiy algoritmlar, shuningdek asosiy texnik va dasturiy parametrlarning qiymatlari kommutatsiya qurilmaning tegishli standartlari va texnik xarakteristikalarining tavsifidan olingan.

## 7.2. Multimediali aloqa tarmoqlarini modellashtirishning asosiy masalalari

Multimediali aloqa tarmoqlarini matematik modellashtirishning asosiy vazifalari, zamonaviy raqamli aloqa tizimlari ham, bo‘lajak multiservisli tarmoqlar ham murakkab va katta texnik tizimlar hisoblanib, ularning faoliyat yuritishi statistik xususiyatga ega. Ularning faoliyat yuritish jarayonlari murakkab algoritmlar bilan amalga oshirilib, ular ko‘pincha evristik hisoblanadi. Multimediali aloqa tarmoqlari katta hududda taqsimlangan turli xildagi komponentlarning katta miqdoridan iborat bo‘ladi. Bu komponentlar murakkab tuzilishga va o‘zaro ta’sirlashuv algoritmlariga ega hamda ular ishonchsiz elementlar mavjud bo‘lganda, haqiqiy halaqitlar sharoitida, shuningdek passiv va aktiv qarshi ta’sir, shu jumladan axborot qarshi ta’siri sharoitida faoliyat yuritadi.

Multimediali aloqa tarmog‘ini ishlash va loyihalash bosqichlarida, uning haqiqiy faoliyat yuritishi va rivojlanishi sharoitida, xizmat ko‘rsatish sifati va ishonchlilikni, yashovchanligi va axborot xavfsizligini ta’minlash talablariga muvofiq ehtimoliy-vaqt xarakteristikalarni keng sinfini baholash masalasi yuzaga keladi. Bu shunday murakkab tizimlarni tahlil qilish uchun tegishli matematik apparatni ishlab chiqish, multiservisli tarmoqni monitoring qilish tizimini yaratish va tarmoqni haqiqiy vaqt masshtabida boshqarish zarurligini yuzaga keltiradi. Boshqarishning zarurligi tarmoqning faoliyat yuritish jarayonida turli xil, odatdan tashqari vaziyatlarning rivojlanishi va yuzaga kelishi natijasida vujudga kelishi mumkin. Bunday odatdan

tashqari vaziyatlarga quyidagilar kiradi: tarmoqning umuman o‘ta yuklanishi, uning alohida komponentlari yoki segmentlarining o‘ta yuklanishi, tarmoqning ayrim komponentlarini ishdan chiqishi, tarmoqning faoliyat yuritish me’yoridagi jarayonning atayin buzilishi. Odatdan tashqari vaziyatning turiga bog‘liq bo‘lmagan holda, murakkab tizim hisoblangan axborot tarmog‘ining holati nuqtai nazaridan, uning oqibatlari tarmoq komponentlarining to‘la yoki qisman ishdan chiqishidan, uning va alohida komponentlari samaradorligining pasayishidan, shuningdek abonentlarning ayrim qismlariga xizmat ko‘rsatish sifatining yomonlashishidan, u taqdim etayotgan axborotni buzilishidan yoki yo‘qolishidan iborat bo‘ladi. Bu komponentlar ham apparatli (marshrutizator yoki serverning vaqtincha ishdan chiqishi), ham dasturiy (xabarlarni paketlash dasturining noto‘g‘ri faoliyat yuritishi yoki trafikni noto‘g‘ri manzilga yo‘naltirish) bo‘lishi mumkin. Bunday holatlar, masalan, tarmoqda xaotik trafiklarning paydo bo‘lishiga olib kelishi mumkin. Shuni ta’kidlaymizki, modellashtirish nuqtai nazaridan apparatli va dasturli komponentlar turli qiymatlidir. Unisi ham bunisi ham axborotga ishlov berish va jo‘natish uchun mo‘ljallangan vositalarning mohiyatidir. Shunday qilib, sanab o‘tilgan bu barcha holatlar turli komponentlarni alohida olganda ham, barcha axborot tarmoqlarini to‘laligicha olganda ham ishonchsiz faoliyat yuritishga olib kelgani uchun biz loyihalash, ishlab chiqish, foydalanish va modernizatsiyalash bosqichlarida ularni har tomonlama va sinchiklab matematik tahlil qilish hamda modellashtirish zarurligiga kelamiz.

Uning asosida qarorlar qabul qilinadigan, axborotga ta’sir qiluvchi asosiy omillar quyidagilar hisoblanadi:

1. Multimediali aloqa tarmoqlarining faoliyat yuritishining taqsimlangan xususiyati.

2. Multimediali aloqa tarmoqlarida qo‘llaniladigan telekommunikatsiya texnologiyalarning ko‘p sonli ekanligi.

3. Multimediali aloqa tarmoqlarining komponentlarini butunlay, uning komponentlarini alohida oxirgi unumdorligi.

4. Multimediali aloqa tarmoqlarining ayrim komponentlarining ishonchsizligi.

5. Multimediali aloqa tarmoqlarida axborot xavfsizligining yetarli emasligi.

6. Multimediali aloqa tarmoqlarining vaqt bo‘yicha o‘zgaruvchi topologiyasi.

7. Multimediali aloqa tarmoqlarini tasodifiy nobarqarorligi va turli xil axborot yuklanishi.

8. Multimediali aloqa tarmoqlarida odatdan tashqari vaziyatlar turlarining xilma-xilligi.

## 7.3. Multimediali tarmoqlarni modellashtirishning matematik usullari

Multimediali aloqa tarmoqlarini tahlil qilish va loyihalash vazifalari ixtisoslashgan dasturiy vositalarni ishlab chiqishni va ularning modelini tayyorlashni maxsus texnologiyalaridan foydalanishni talab etadi. Matematik modellashtirishni qurilmali vositalardan foydalanish texnologiyasi (7.2-rasm) o‘z ichiga quyidagi bosqichlarni oladi:

- tadqiq etilayotgan tizimni tahlil qilish va uni modellashning maqsadlarini ifodalash;

- tadqiq etilayotgan tizim parametrlarining zarur to‘plamini tavsiflovchi konseptual modelni (KM) yasash;

- konseptual model ob’ektlarini dasturiy modelning ob’ektlari to‘plamida aks ettirishdan iborat bo‘lgan, tadqiq etilayotgan tizimning dasturiy modelini (DM) yasash;

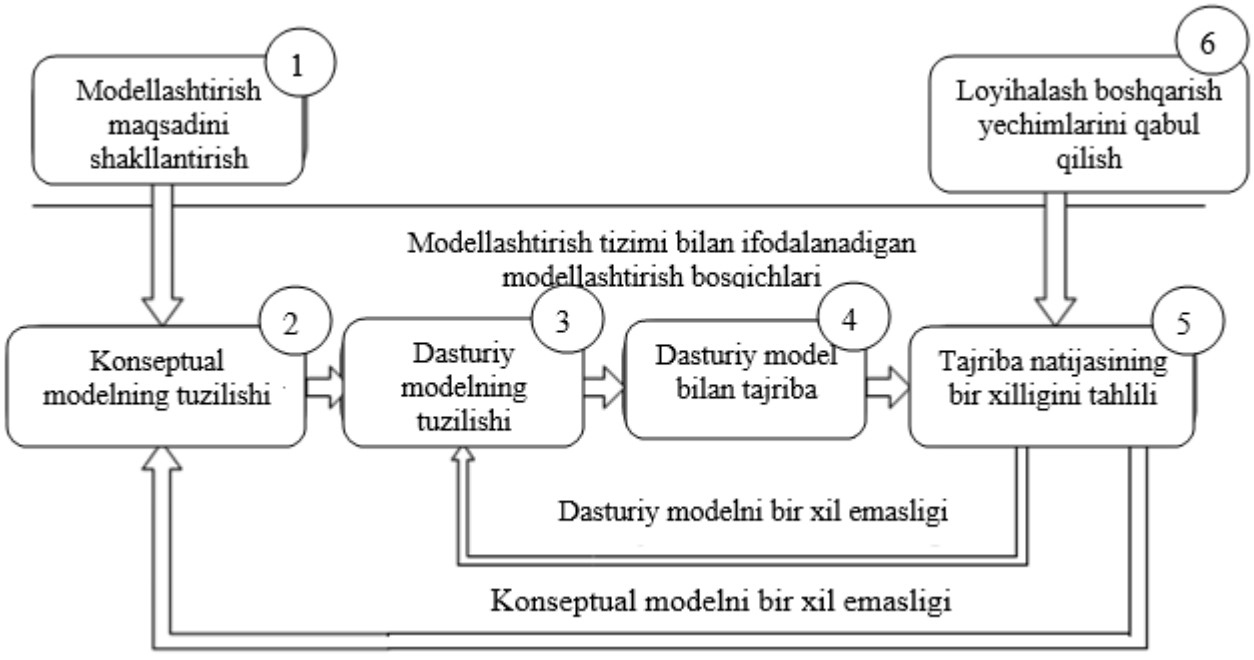
- dasturiy model bilan tajriba o‘tkazish (uning dasturiy kodini bajarish);

- modellar bilan o‘tkazilgan tajribalarning natijalarini tahlil qilish va talqin qilish;

- loyihaviy va boshqaruv qarorlarini qabul qilish.

Tadqiq etilayotgan tizimning konseptual va dasturiy modellarini tuzilishi, mos ob’ektlar to‘plamini (modelli va dasturiy) tanlashda va ular o‘rtasida tekshirilayotgan tizim elementlari aloqalari tuzilishiga mos keluvchi aloqalar tuzilmasini o‘rnatishdan iborat.

Multimediali aloqa tarmoqlarini matematik modelini tayyorlash tizimida uning matematik modeli ma’lum bir tanlangan konseptual model doirasida tavsiflanadi. Konseptual model – modeli tayyorlanayotgan tizimning kirish parametrlari to‘plamini, faoliyat yuritish algoritmlarini, shuningdek, modelni tayyorlash maqsadlari – model tayyorlanadigan tizimning tadqiq etilayotgan parametrlari to‘plamini tavsiflovchi matematik ob’ekt. Konseptual modelga mos holda dasturiy model qo‘yiladi (modellashtirishda qo‘llanidadigan ob’ektlarning ma’lum bir tuzilmasi bo‘lib, u konseptual modelni dastur ko‘rinishida amalga oshiradi).




7.2-rasm. Multimediali aloqa tarmoqlarini matematik modellashtirishning umumiy sxemasi

Ishlab chiqilgan dasturiy modelning kompyuterda bajarilishi, model bilan modelli tajriba sifatida aniqlanadi. Modelli tajriba, modeli tayyorlanayotgan parametrlarning baholarini berilgan aniqlikda hisoblashni ta’minlaydi. Multimediali aloqa tarmoqlarini tahlil qilish masalalarining murakkabligi, murakkab tizimlarning matematik modelini tayyorlash usullarining rivojlanish darajasi, hisoblash texnikasi unumdorligining darajasi va modellarni tayyorlash dasturiy vositalarining rivojlanish darajasi gibrid model tayyorlash usullaridan foydalanish ehtiyojini yuzaga keltiradi. Bu usullarning mohiyati shundaki, bunday masalalarni yechish uchun turli matematik modellarni tahlil qilishdan iborat. Gibrid modellardan foydalanishning dolzarbligi yana shu bilan tasdiqlanadiki, multimediali tarmoqlarning tadqiq etilayotgan parametrlarining barcha to‘plamini matematik modellarning bir sinfida adekvat ravishda tavsiflash, undan tashqari sonli baholarni olish amaliy jihatdan mumkin emas.

*Multimediali tarmoqlarning matematik modelini tayyorlash tizimini qurishning asosiy konsepsiyalari.* Murakkab va katta axborot tizimlarini amaliy modellashtirish tajribasi bilan belgilanadigan bu tizimlarning matematik modelini tayyorlashning (imitatsion, tahliliy va gibrid) nazariyasi va dasturiy vositalarini rivojlantirishning asosiy yo‘nalishlaridan biri gibridli modelni tayyorlash usullarini qo‘llab-quvvatlash hisoblanadi. Gibrid modellardan foydalanishning zarurligi axborot tizimlarini modellash masalalari sinfini kengaytirish, shuningdek uning o‘lchamlarini oshirish bilan belgilanadi. Imitatsion yoki tahliliy modellardan farqli ravishda, gibrid modeldeganda tadqiq etilayotgan ob’ektning bitta modeli emas, balki uning modellarining ma’lum bir tuzilmasi tushuniladi. Gibrid modellashni tavsiflash, ishlab chiqish va amalga oshirish uchun mazkur modellarni tavsiflashga imkon beruvchi tegishli rasmiy apparatni yaratish zarur.

Matematik modellash tizimida, tadqiq etilayotgan tizimni modellash vazifasi, umumiy holda gibrid hisoblanadigan konseptual model bilan tavsiflanishi nazarda tutiladi. Tadqiq etilayotgan tizimning konseptual modeli *cx* modellar majmui bilan

taqdim etilib, u model tayyorlashning usulini tavsiflash uchun mo‘ljallangan *C* turdagi tuzilmalashtirilgan komponent bo‘lib hisoblanadi.

## 7.4. Imitatsion modellashtirish usuli

Imitatsion modellashtirish, axborot tarmoqlarini (AT) tadqiq etishning e’tirof etilgan vositasi hisoblanadi. Buning sabablari bir nechta. Ulardan eng asosiysi ob’ektni, ya’ni uning tuzilishini, faoliyat yurtishining murakkab algoritmlarini yetarlicha aniq darajasida to‘liqligicha matematik jihatdan tavsiflanishning mumkin emasligi, shuning uchun ham murakkab va nobarqaror dinamik jarayonlar hisoblanadi. Odatda matematik vositalar bilan xususiy masalalarni yechish imkoni bo‘ladi. Markov jarayonlari va ommaviy xizmat ko‘rsatish modellari yordamida, tarmoqning ayrim uzellari va kanallarini yaxshi tahliliy modellari tayyorlanadi, ayni paytda esa umuman tarmoqning modelini tayyorlash tahliliy jihatdan ancha qiyinlashadi, ayniqsa, nomuntazam tuzulmalarda va bir jinsli bo‘lmagan qurilmada. Oqimlarni qayta taqsimlash va qurilmani tiklashning turli rejimlarini nazarda tutuvchi, tarmoqlarda rad etishlarni tahliliy modelini amalga oshirish murakkabdir. Shuningdek algoritmik jihatdan murakkab bo‘lgan taqsimlangan protokollarni tahliliy modellashtirish usuli bilan vaqt bo‘yicha va ishonchlilik tavsiflarini baholash ham yetarlicha qiyinchiliklarni yuzaga keltiradi. Bu va boshqa bir qator masalalarni hal etish imitatsion modellashtirish usuli bilan amalga oshirish mumkin va samarali hisoblanadi. Telekommunikatsiya tarmoqlarida va xususan multimediali tarmoqlarda kechikishlar va unumdorlikni imitatsion modellashtirish usuli asosida yotadigan matematik ob’ekt bo‘lib diskret dinamik tizimlar hisoblanadi.

## 7.5. Tahliliy modellashtirish usuli

Hozirgi vaqtga kelib ommaviy xizmat ko‘rsatish tizimlari tarmoqlari turli vazifalarni bajaruvchi, axborot tarmoq tizimlarining ehtimoliy vaqtincha tavsiflarini tahliliy modellashtirish usulining eng keng tarqalgan vositasi bo‘lib hisoblanadi. Bunday holat bu tizimlarning faoliyat yuritish algoritmlarini va bu tarmoqlarni hisob-kitob qilishning samarali usullari mavjudligi bilan aks etish imkoniyatlariga bog‘liqdir. Hozirgi vaqtga kelib ommaviy xizmat ko‘rsatish nazariyasi doirasida xizmat ko‘rsatish tarmoqlariga bevosita taalluqli bo‘lgan fundamental natijalar olingan bo‘lib, ular tadqiq qilinayotgan tarmoqlarning xossalarini va ularni tahlil qilish hamda hisoblash usullarining mazmunini jiddiy belgilab beradi. Shuni ta’kidlash kerakki, ommaviy xizmat ko‘rsatish tarmoqlari nazariyasining rivojlanishi ko‘pchilik hollarda imitatsion modellashtirishdan voz kechish va ma’lum darajada telekommunikatsiya tarmoqlari modellarini ishlab chiqishni tezlashtirish, ularning o‘lchamligini va adekvatligini oshirish imkonini beradi.

Ommaviy xizmat ko‘rsatish tarmog‘i ommaviy xizmat ko‘rsatish tizimlarining turli xil sinfdagi talablarining ma’lum bir to‘plami tuzilmasi sifatida aniqlanadi. Talablar ommaviy xizmat ko‘rsatish tizimlarida ma’lum bir berilgan xizmat ko‘rsatish tartibiga muvofiq xizmat ko‘rsatiladi, xizmat ko‘rsatish davomiyligi esa ma’lum bir berilgan taqsimlash funksiyasiga ega bo‘lgan tasodifiy kattalik hisoblanadi. Xizmat ko‘rsatishning bir tizimida xizmat ko‘rsatish yakunlanganida, talab xizmat ko‘rsatishni davom ettirish uchun boshqa tizimga kelib tushadi.

Ayni paytda ommaviy xizmat ko‘rsatish tarmoqlari quyidagi tarzda tasniflanadi:

- talablarning tashqi manbalarining mavjudligi bo‘yicha: ochiq, berk va aralash talablar farqlanadi;

- xizmat ko‘rsatilayotgan talablarning sinflari soni bo‘yi bir jinsli va jinsli bo‘lmagan talablar farqlanadi;

- talablarga xizmat ko‘rsatish davomiyligini taqsimlash vazifalarining turlari bo‘yicha ekspotensial tarmoqlar va umumiy ko‘rinishdagi tarmoqlar farqlanadi.

## Nazorat savollari

1. IP tarmoq bo‘ylab multimediali trafikni uzatish jarayonini modellashtirishning vazifasi nimadan iborat?
2. IP lokal tarmoq bo‘yicha vodeodasturni uzatish jarayonini tushuntiring?
3. Modelning qanday asosiy parametrlari mavjud?
4. Dasturiy parametrlarga nimalar kiradi?
5. Multimediali aloqa tarmoqlarini matematik modellashtirishning sxemasi qanday tuzilgan?
6. Konseptual modelning vazifasi nimadan iborat?
7. Asosiy baholanuvchi vaqt-ehtimolli xarakteristikalarni sanang?
8. Imitatsion modellashtirish usulini tushuntiring.
9. Tahliliy modellashtirish usulini tushuntiring.
10. Ommaviy xizmat ko‘rsatish tarmoqlari qanday tasniflanadi?

# 8. KONVYERGENT ALOQA TARMOQLARI

## 8.1. Telekommunikatsiya texnologiyalarining konvergensiyasi

Bir nechta maxsuslashtirilgan operatorlar tarmog‘ini birlashtirish (qayd etilgan aloqa, mobil aloqa va ma’lumotlar uzatish) va abonentlar uchun keskin kurashish, yangi xizmatlar sinfini yaratilishiga sabab bo‘ldi. U abonentlar uchun shaffoflikni, ya’ni telekommunikatsiya muhitida xizmatlar va tarmoqlarga o‘zaro o‘tishni ta’minlaydi. Bir muhit xizmatidan boshqa muhit xizmatiga o‘zaro o‘tish jarayoni konvergensiya deyiladi. Masalan, mobil aloqa va Internetning konvergensiyasi.

Hozirgi vaqtda multiservisli tarmoqlarni qurishda IP/ATM, IP/MPLS, IP/Gigabit Ethernet texnologiyalaridan foydalaniladi. Uzoq muddatli istiqbolda IP/MPLS texnologiyasining IP/ATM texnologiyasidan asosiy afzalligi, kengayuvchanligining - masshtablanishining (Scalability, extensibility) yanada yuqori darajadaligi, arxitekturani o‘zgartirmagan holda yangi elementlarni qo‘shish yoki eskirganlarini yanada mukammallariga almashtirishdan iborat. IP/MPLS texnologiyasini qo‘llashning ma’qulroq sohasi – transport tarmog‘i yadrosidir.

Shuningdek keng ko‘lamlilik katta miqdordagi foydalanuvchilar oqimlarini iqtisodiy qo‘llab-quvvatlashni anglatadi. Tejamkorlik, magistral orqali juda ko‘p miqdordagi oqimlarni, ulardan har birini kuzatmasdan, balki butun to‘plamni (birlashtirish yo‘li bilan) kuzatib uzatish imkonini nazarda tutadi. Oqimlarni birlashtirish ATM texnologiyasida ham MPLS texnologiyasida ham amalga oshiriladi. ATM da - bu aloxida virtual ulanishlarni (VCC) umumiy virtual yo‘lga VPS birlashtirish bo‘lsa, MPLS da esa bu turli xil foydalanuvchilarning oqimlarini umumiy yetkazib berish sinflariga (Forwarding Equvalence Class, FEC) birlashtirish va ularni umumiy yo‘l (Label Switching Path, LSP) bo‘ylab uzatishdir. Shuning bilan birga MPLS texnologiyasida birlashtirish mexanizmlari ancha moslashuvchan bo‘lib, avtomatlashtirishga moyil bo‘ladi. Agar ATM kommutatori virtual kanal

identifikatorlari (VCL) bo‘lgan faqat ikkinchi sath kommutatsiyalash jadvalidan va traktidan (VPI) foydalansa, u holda belgilar yordamida kommutatsiyalovchi MPLS marshrutizator (LSR) ikkinchi sath, uchinchi sath (IP-adres), to‘rtinchi sath (TCP/UDP portlari), ko‘pincha esa amaliy sathlar axborotlariga ulana oladi. Shuning uchun ma’muriyat virtual kanallar (VCC) ulanishlarini virtual traktlar ulanishlariga (VPC) qo‘lda ulanishini aks ettirishni konfiguratsiyalamasligi, balki trafikning turli belgilarini, shu jumladan yuqori sathligini hisobga olgan holda, ulanishning bir nechta qoidasini yozib qo‘yishi hamda keyingi ishlarini LSRga taqdim etishi mumkin. MPLS texnologiyasining keng ko‘lamliligini oshiruvchi yana bir farq qiluvchi xossasi, belgilar ierarxiyasi sathlarining cheksiz soni hisoblanadi va mos ravishda ATM texnologiyasida ikkita sath (VPC/VCC) o‘rniga yo‘llarni birlashtirish hisoblanadi.

ATM va MPLS texnologiyalari zamonaviy transport tarmoqlarida aynan bir xil vazifalarni bajaradi: kanal sathida virtual ulanishlarni yaratish. Virtual ulanishlarni yaratish quyidagilarni ta’minlaydi:

- foydalanuvchilarning ma’lumotlar oqimlarining har xil turlariga differensiallashgan xizmat ko‘rsatish (axborotni eltib berish xizmatlari sifati sathi haqida kelishuvni qo‘llab-quvvatlash - Service Level Agremeent, SLA;)

- tarmoq orqali ma’lumotlar oqimlarining kirish yo‘llarini oqilona tanlash asosida (trafikni boshqarish usullari yordamida - Traffic Engineering, TE) resurslardan optimal foydalanish.

ATM texnologiyasida bir qancha cheklashlar mavjud, ular tufayli uning keng miqyosliligi ma’lum chegaralardan tashqariga chiqmaydi. Eng jiddiy cheklash bu qayd etilgan va yacheykaning uncha katta bo‘lmagan o‘lchami - 53 bayt hisoblanib, ulardan 48 bayti axborotli ma’lumotlarni ko‘chirib o‘tkazadi. Yacheykaning kichik o‘lchamda bo‘lishi kechikishlarga sezgir bo‘lgan nutq axborotini 155 Mbit/c tezlik bilan magistral tarmoq orqali uzatishni yaratish maqsadida tanlab olingan (155 Mbit/c tezlik XX asrning 90-yillari boshlarida ATM tarmoqlarida eng keng tarqalgan edi).

O‘tgan 15 yil mobaynida transport tarmoqlari tezliklarining ko‘lami o‘zgardi, hozirgi vaqtda axborotni yetkazib berish texnologiyalari 10 Gbit/s (10 Gigabit Ethernet, 10 GE) va undan ortiq tezlikda ishlamoqda. Har qanday paketli kommutatsiyalash qurilmasining hisoblash quvvatini xarajatlari, ular qo‘llaydigan texnologiyalarga bog‘liq bo‘lmagan holda ishlov berilayotgan paketlar (kadrlar, yacheykalar) o‘lchamiga emas, balki miqdoriga proporsionaldir. Shuning uchun ATM kommutatorining unumdorligi, o‘lchami 4500-5500 oktetlar bo‘lgan paketlar bilan ishlovchi IP marshrutizatorning unumdorligiga qaraganda taxminan 100 marta katta bo‘lishi kerak. Bunday yacheykalar va paketlar o‘lchamlaridagi farq oqibatida, fizik sathda yetkazib berishda kechikishlar kattaligi nanosekundli kattaliklardan ortmaydi va tarmoq foydalanuvchilari tomonidan sezilmaydi.

ATMning afzalligi - ATM ning eng kuchli tomoni sifatida doimo qarab kelingan turli oqimlarga differensiallashgan xizmat ko‘rsatishni nozik va turlichaligini ta’minlashdir. Xaqiqatdan ham, texnologiyalarni ishlab chiqaruvchilar mavjud ma’lumotlar oqimlarining barcha turlarini har tomonlama tahlil qilishdi, ularni sinflarga ajratishdi, har biri uchun tegishli ko‘rinishdagi axborot turini eng ma’qul tarzda eltib berivchi aloxida xizmatlarni (CBR, rtVBR, nrtVBR, ABR, va UBR) yaratishdi.

Tarmoqni boshqarish deganda:

- tarmoq operatorlarining tizimli maqsadlarini aniqlash va unga erishish;
- boshqa tarmoqlar (zona, qit’a, dunyo) operatorlarining boshqarish tizimlarining o‘zaro aloqasi;
- tarmoqni boshqarishning usullari va vositalarini belgilab beruvchi tartibga soluvchi xujjatlarni ishlab chiqish tushuniladi.

Bunda ATM tarmog‘ining uzellari foydalanuvchining tarmoq ma’muriyati bilan tuzilgan bitimni yuqori darajada ta’minlab, har bir aloxida virtual ulanish uchun “Uchidan uchigacha” usul bo‘yicha axborotni yetkazib berish sifati parametrlarini nazoratini ta’minlaydi.

MPLS texnologiyali tarmoqning shu tarzda axborotni yetkazib berish sifatini ta’minlay olishga qodir emasligini juda ko‘pchilik mutaxassislar uning kuchsizligi va ATM texnologiyalarining magistral tarmoqlarda qo‘llanilishining bosh sababi deb hisoblaydilar. Shubhasiz IP/MPLS texnologiyali tarmoqlarda axborotni yetkazib berish sifatini ta’minlash bilan bog‘liq muammolar mavjud, ammo MPLS foydalanuvchining axborotini ATM darajasida eltib berish sifatini ta’minlay olmaydi. Bugungi kunda tarmoqning chekka qismlari uchun emas, balki uning yadrosi uchun mo‘ljallangan bunday texnologiyaning alohida roliga muvofiq, axborotni yetkazib berish sifatini ta’minlash usullarini MPLS uchun ITU-T va boshqa xalqaro tashkilotlarning standartlari hali mavjud emas. Shuni ta’kidlash kerakki, axborotni eltib berish sifatini ta’minlash MPLSga umuman qat’iy o‘rnatilmagan (agar sarlavhadagi Exr maydonining zahiraga olingan uchta biti hisobga olinmasa, ular kadrning ustunligi belgisini ko‘chirish uchun qo‘llaniladi). Bunday soddalashtirish ongli ravishda bajarilgan, ya’ni tayyorlovchilar va tarmoq integratorlariga harakat erkinligini va aloqa tarmoqlari operatorlarining ehtiyojlariga eng yaxshi tarzda javob beruvchi axborotni eltib berish sifatini ta’minlash mexanizmlarining mavjudlarini qo‘llash imkonini berish uchun qilingan. Bugungi kunda bunday tavsiya etiladigan mexanizm differensiallashgan xizmat ko‘rsatish (Diffserv) hisoblanadi, u IP tarmoqlar uchun ishlab chiqilgan va ATM dagi kabi aloxida foydalanuvchilar ulanishlari bilan emas, balki tarmoq trafigining bir qancha birlashtiriladigan sinflari bilan ishlash uchun mo‘ljallangan. Aynan shunday texnologiya transport tarmog‘i yadrosida ishlash uchun to‘g‘ri keladi.

XXI asrning boshida magistral tarmoqda IP/MPLS texnologiyalari birikmasini qo‘llanilish yo‘nalishi paydo bo‘ldi. Bunda ATM texnologiyasi kirish tarmoqlarida qo‘llanilishi mumkin. Dunyoning iqtisodiy rivojlangan mamlakatlarining ko‘pchilik aloqa operatorlari “ATM kirish tarmoqlarida va IP/MPLS transport tarmog‘i yadrosida” degan iborani oqilona va strategik jixatdan to‘g‘ri deb hisoblab bunday qarorni qo‘llab-quvvatlaydilar.

ATM texnologiyasi ilovalardan foydalangan holda afzalliklarga ega bo‘lib, ular uchun kafolatlangan o‘tkazish oralig‘i kerak, masalan, haqiqiy vaqt ilovalari uchun.

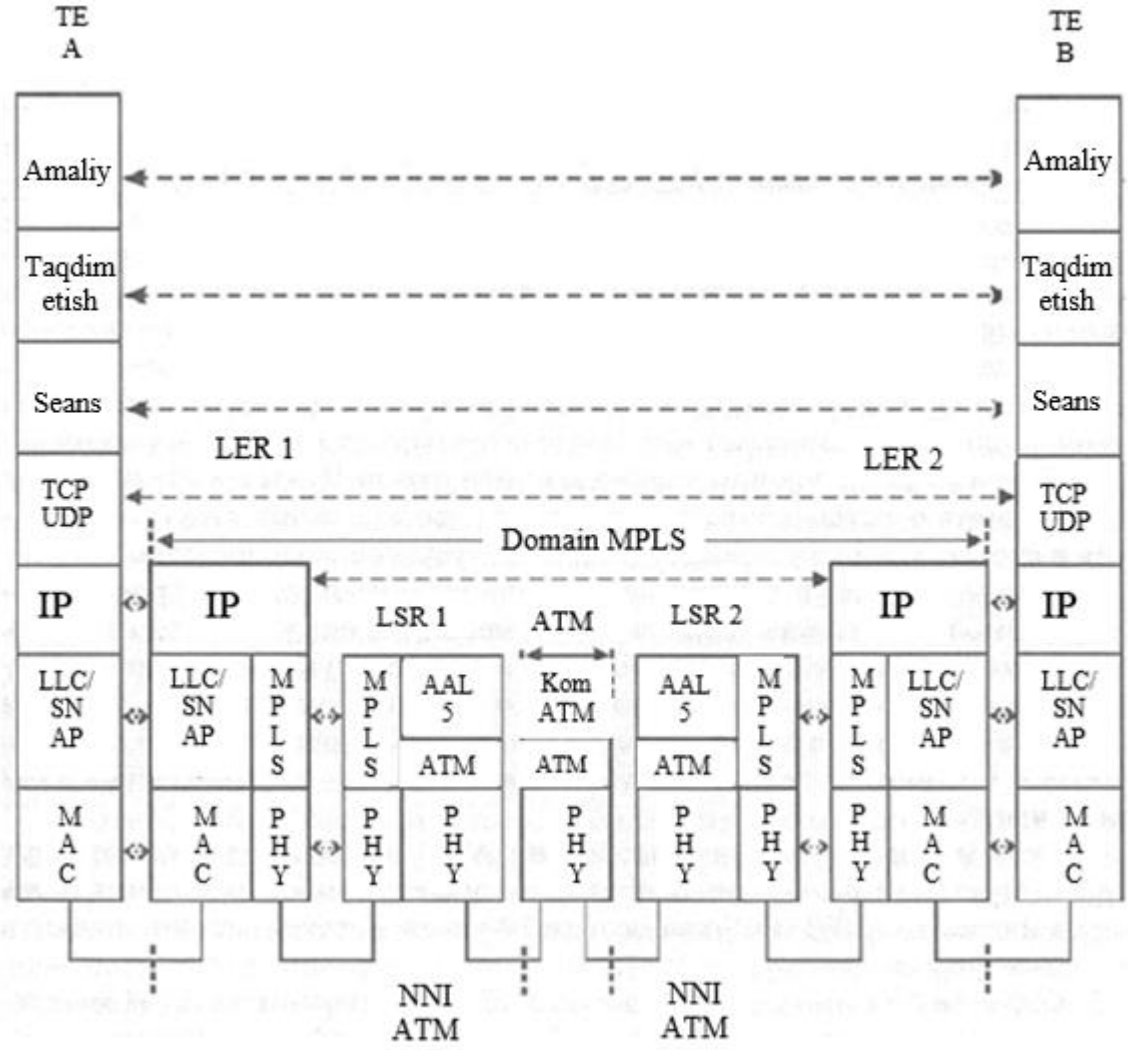
O‘zbekistonda ATM texnologiyasi dasturiy apparat-vositalarining qiymati yuqori bo‘lganligi tufayli ulanish tarmoqlarida qo‘llanilmaydi.

Kirish tarmog‘i magistral tarmoq bilan ikkinchi protokolli sathda o‘zaro ta’sirlashganda, birinchi yoki ikkinchi sathdagi ob’ektlardan generatsiyalanadigan raqamli oqimlar, ikkinchi sathning kadrlari yoki yacheykalariga bevosita inkapsulyatsiyalanadi. Bu esa mos holda ortiqcha xarajatlarni kamaytiradi.

Magistral tarmoq orqali ikkinchi sathdagi kadrlar oqimini yetkazib berish uchun belgilar yordamida kommutatsiyalanuvchi LSP yo‘lda ikkinchi sathni adreslarini aks ettirish jadvallari qo‘llaniladi. Bunda ikkinchi sath kadrining adresi tashlab yuborilmaydi, balki yodda saqlanib qolinadi va MPLS sarlavhasining ichki belgisi maydoniga joylashtiriladi, ya’ni kadrning sarlavhasida belgilar ierarxiyasi hisobiga iyerarxik yo‘llarni qo‘llab-quvvatlashdan iborat MPLS xossasidan foydalaniladi. IP/MPLS magistralidan kadr yoki yacheyka chiqib ketganda bu adresli axborot qayta tiklanadi va ma’lumotlar kirish tarmog‘ida qo‘llaniladigan texnologiyaga muvofiq belgilangan joy uzeliga yetkazib beriladi. Shunday qilib ikkinchi sathni kadrlar oqimini tunellash amalga oshiriladi. Bunda tunellar sifatida magistral tarmoqda yaratilgan yo‘llar (LSP)dan foydalaniladi. Agar kirish tarmog‘ida ATM texnologiyasi qo‘llanilsa, u holda virtual ulanish magistralning kirish qurilmasida tugallanmaydi, balki shaffof holda MPLS tunneli orqali o‘tadi va magistraldan chiqishda kirish tarmog‘ida belgilangan joy uzeliga davom etadi. ATM va MPLS ning tavsiflangan o‘zaro ta’sirlashish sxemalari bir-birini to‘ldiradi. Ularni birgalikda qo‘llab, operator IP/MPLS magistrali orqali IP-paketlar oqimlarini ham, boshqa formatdagi ma’lumotlar oqimlarini ham yetkazib berish imkoniyatini oladi .

MPLS texnologiyasining ATM texnologiyasiga nisbatan afzalliklaridan biri uning ikkinchi sathdagi mavjud texnologiyalarning amalda istagan kadrlar formatidan

ATM, Frame Relay, PPP, Ethernet yoki boshqa formatidan foydalanuvchi bir necha turlariga ega (A-MPLS, F-MPLS, P-MPLS va E-MPLS).




8.1 rasm. IP/MPLS va ATMning o‘zaro aloqa profili

MPLSning bunday protokolli mustaqilligi transport tarmog‘ida zarur bo‘lgan moslashuvchanlik va keng ko‘lamlilik (qurilmani almashtirmasdan tavsiflarni modifikatsiyalash imkoniyati)ning yuqori darajasini ta’minlaydi. Multimedia trafigining tavsifini o‘rgangandan so‘ng va MPLS texnologiyasidan foydalanishda tajriba to‘planganidan so‘ng operator boshqa sinflarga o‘tkazilgan oqimlarni, shu jumladan bugungi kunda eltib berish CBR va rt-VBR ATM xizmatlari yordamida

ta’minlanadigan, kechikishga sezgir bo‘lgan ma’lumotlar oqimlarini belgilar yordamida kommutatsiyalanuvchi yo‘llarga o‘tkazishni boshlashi mumkin. 8.1-rasmda IP/MPLS va ATM o‘zaro aloqa profili protokollarining steklari keltirilgan.

Internet (intranet) resurslariga kirishni ta’minlash uchun foydalanuvchi virtual liniya tarmog‘iga ulangan ikkinchi sathni LLC va MAC protokollari turlaridan birini qo‘llashi mumkin.

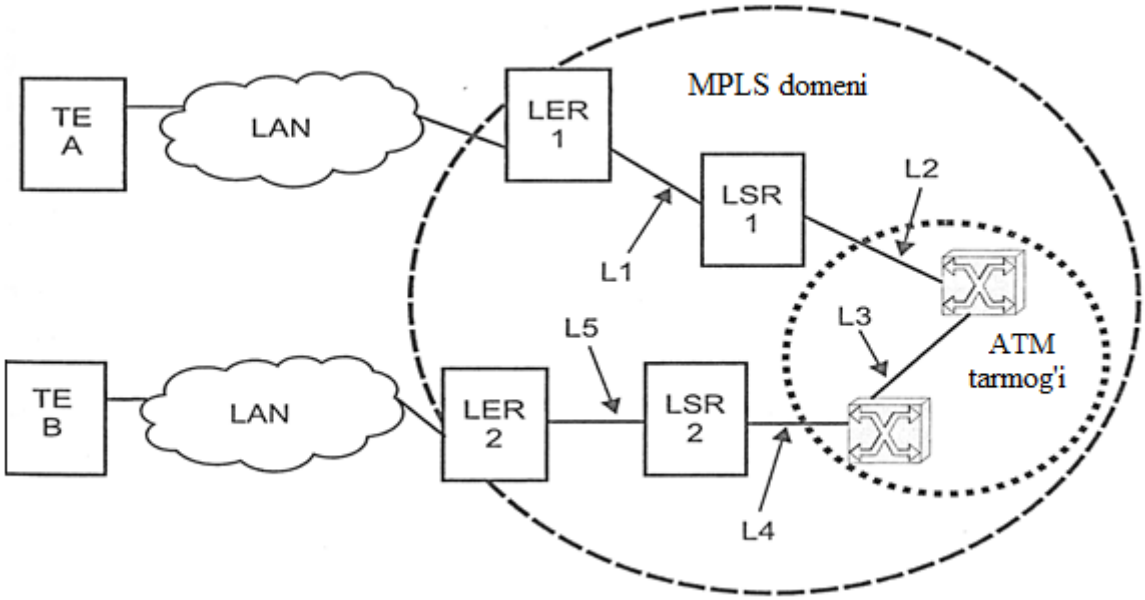
MPLS domenining LER1 (Label Edge Router) chegaraviy marshrutizatori LLC protokoli kadrlariga belgi qo‘yadi va belgilangan kadrlar oqimini marshrutlashtirish (masalan, OSPF) va belgilarni taqsimlash LDP (Label Distribution Protocol) protokollari yordamida tanlangan LSP yo‘li bo‘ylab yo‘naltiradi. LSP yo‘li quyidagi tarmoq ob’ektlari orqali o‘tadi: LER1, LSR1, IP/MPLS va ATM, LSR2, LER2 texnologiyali tarmoq kommutatori.

IP/MPLS va ATM texnologiyali tarmoqning tuzilish sxemasi 8.2-rasmda keltirilgan. ATM kommutatori shaxsiy belgilarni (VPI, VCI), “LSR1 - ATM kommutatori” va “LSR2 - ATM kommutatori” interfeyslarida IP-paketlarga biriktirish uchun qo‘llaydi. TE A terminaldan TE B terminalga oqim paketlari LSP yo‘l bo‘ylab MPLS domeni chegaralarida o‘tadi. MPLS domeni ob’ektlarida (kommutatsiyalovchi LER, LSR marshrutizatorlarida va ATM kommutatorlarida) paketlar L1, L2, L3, L4, L5 belgilar yordamida kommutatsiyalanadi. L2, L3, L4 belgilar sifatida ATM texnologiyasida qo‘llaniladigan VPI virtual traktlarning identifikatorlari qo‘llaniladi.

Keyingi avlod tarmog‘i yadrosida kanallar kommutatsiyasi yoki paketlar kommutatsiyasi bo‘lgan rejimlardan foydalanish kerakligi to‘g‘risidagi masala deyarli bir qiymatli hal qilingan. Tarmoq yadrosida qo‘yidagi sabablarga ko‘ra paketlar kommutatsiyasi rejimidan foydalaniladi:

- birinchidan, paketli ma’lumotlar trafigining jadalligi telefoniya trafigining jadalligidan katta bo‘ladi;

- ikkinchidan, kanallar kommutatsiyali tarmoqlar mavjud resurslardan samarali foydalanmaydi, bunda aloqa kanali ulanish o‘rnatilgan paytdan boshlab to to‘liq uzilishigacha band bo‘ladi (xatto foydalanuvchi axborot o‘zatmayotgan holatda ham).




8.2- rasm. IP/MPLS va ATM texnologiyali tarmoq tuzilishi

Undan tashkari, bu TCP/IP protokollar stekiga asoslangan paketlar kommutatsiyasi tarmog‘i bo‘ladi. TCP/IP stekining muvaffaqiyati, uning tayanch kommunikatsiya texnologiyalaridan (PPP, Ethernet, Token Ring, Frame Relay, ATM, IP/MPLS, SDH dan) deyarli istalgani bilan kelishish qobiliyati izohlanadi.

TCP/IP protokollaridan foydalanuvchi katta mikdordagi dasturlar va ilovalarning bozorda mavjudligi,TCP/IPni boshqa tarmoq protokollaridan afzalligiga imkon beradi. Nihoyat, TCP/Ipni hozirgi vaqtda eng tez rivojlanayotgan kompyuter tarmog‘i hisoblangan Internetda qo‘llanilishi, keyin avlod tarmog‘ida TCP/IP steki qo‘llanilishini yuqori darajadagi ishonch bilan aytishga imkon beradi.

## 8.2. Gigabit Ethernet texnologiyasi

Ko‘p yillar davomida korporativ va xususiy tarmoqlarda Ethernet texnologiyani qo‘llanilishi, keng polosali kirish tarmoqlarida qo‘llaniladigan boshqa barcha texnologiyalardan iqtisodiy ko‘rsatkichlari bo‘yicha amaliy jixatdan o‘zib ketdi. Umumiy foydalanish tarmoqlarida qo‘llashga mo‘ljallangan 10 Gigabit Ethernet (10GE) standarti tarmoqlarning tejamkorligini oshirishga imkon beradi.

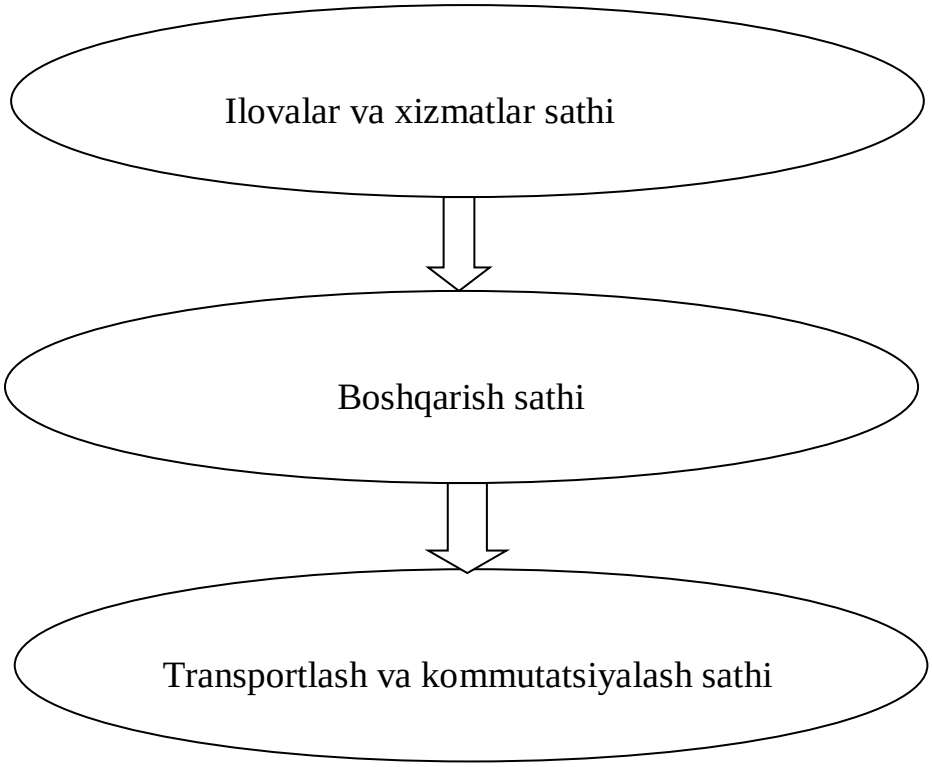
Bugungi kunda IP/Ethernet bog‘lami qo‘llaniladigan qurilmaning qiymati, IP/ATM yoki IP/SDH qurilmalari qiymatining taxminan o‘ndan birini tashkil etadi.

10 GE texnologiyasida GE, Fast Ethernet dagi texnologiya qo‘llaniladi, eltuvchini nazorat qilish va ziddiyatlarni aniqlash (CSMA/CD) bilan ko‘p stansion kirish protokoli va kadr formati saqlangan, ammo uzatish muhiti sifatida TOAL dan foydalaniladi. Axborotni eltib berishning bu texnologiyasi korporativ multiservisli tarmoqlar va NGN transport tarmoqlar magistralini qurishda qo‘llaniladi. 10 GE texnologiyasining ATM texnologiyasiga nisbatan afzalligi shundan iboratki, IP paketlari va Ethernet kadrlarining xajmlari bir xil, shuning uchun axborotlarni transport tarmog‘ida yetkazib berishda paketlarni kadrlarga (ATM yacheykalari) almashtirish va teskari almashtirish talab etilmaydi.

Eng muhim muammo shundan iboratki, kanallar kommutatsiyasi va paketlar kommutatsiyasiga asoslangan barcha taniqli xizmatlar, axborotlarni talab etilgan sifatda yetkazib berishni qanday ta’minlashdan iborat. Foydalanuvchilarga operatorda mavjud bo‘lgan xizmatlarning istalgan turlarini taqdim etish uchun shunday taqsimlangan tizimni yaratish kerakki, unda intellektual xizmatlarni tashkil etish va taqdim etish vazifalari, boshqarish vazifalaridan transport va kommutatsiya bilan ajratilgan bo‘lsin. Bu prinsip intellektual tarmoqlarni qurishda, to‘g‘rirog‘i telekommunikatsiya tarmog‘i ustiga intellektual ust qurilmalarni qurishda foydalanilgan.

Keyingi avlod tarmog‘ida xizmatlar va ilovalarni yaratish hamda taqdim etishni boshqarish vazifalarini, chaqiriqni va kommutatsiya resurslarini boshqarish vazifalaridan to‘liq ajratishga urinish, shuningdek bu vazifalarni bajaruvchi darajalar orasida standartlashtirilgan interfeyslarni yaratishga urinish amalga oshirilmoqda.

O‘z navbatida, xizmatlarni taqdim etish bozorida vujudga kelayotgan raqobat narxlarni pasaytirish, yangi xizmatlarni ishga tushirish muddatlarini kamaytirish va taklif etilayotgan xizmatlarning turini oshirishi kerak.




8.3- rasm. Keyingi avlod tarmog‘ining sathli arxitekturasi

Chaqiruvlarni nazorat qilishni qayta ishlash vositalari bir joyda to‘planadi, kommutatsiyalash va transport vositalari esa tarmoqning butun hududi bo‘yicha taqsimlanishi mumkin. Undan tashqari, bu ikki vazifani amalga oshiradigan

obektlarning resurslarini hajmining oshishi bir-biriga bog‘liq bo‘lmagan holda ta’minlanadi.

## 8.3. Global axborot infratuzilmasi

Jaxon madaniyati rivojining hozirgi bosqichi industrial jamiyatdan axborot jamiyatiga o‘tish bilan tavsiflanadi. Bunday o‘tish axborot va telekommunikatsiya texnologiyalaridan ommaviy foydalanishga asoslanadigan ijtimoiy va iqtisodiy faoliyatning yangi shakllari mavjud bo‘lishini nazarda tutadi.

Axborot jamiyatining texnologik asosi *Global axborot infratuzilmasi* (Global Information Infrastructure) GII hisoblanib, u sayyoradagi har bir kishi uchun kamsitishlarsiz axborot resurslariga kirish imkonini ta’minlashi kerak. Axborot infratuzilmasini, o‘zaro ta’sirlashuvchi aloqa tarmoqlari va foydalanuvchi terminallarini ma’lumotlar bazasi, axborotga ishlov berish vositalari yig‘indisi tashkil etadi.

Konseptual jixatdan GII o‘z ichiga quyidagi asosiy elementlarni qamrab oladi:

- axborot manbalari va qabul qiluvchilar (odamlar, ma’lumotlar bazalari, boshqariluvchi ob’ektlar va x.k);

- xususan axborot (nutq, matn, grafika, video) va bu axborotni o‘zgartiruvchi qurilmalar;

- ma’lumotlarni saqlash, izlash, siqish, ishlov berish, o‘zgartirish va axborot manbalariga kirishni tashkil etish uchun axborot qurilmalari (tarmoq uzellari – serverlar, shlyuzlar, ma’lumotlar bazalari, PC, TV, FAX terminallari, telefon apparatlar va x.k);

- uzoqdagi ob’ektlar (axborot manbalari va ularni qabul qilib oluvchilar) o‘rtasida axborotni ko‘chirishni ta’minlovchi kommunikatsiya infratuzilmasi.

Mazkur konsepsiyani amalga oshirish uchun tarmoqlar arxitekturasi evolyutsiyasi jiddiy o‘zgarishlarni o‘tkazdi (UfTT-IP-NGN konvergensiyasi).

GII axborot resurslariga kirish, axborot jamiyati xizmatlari yoki infokommunikatsiya xizmatlari nomini olgan, yangi turdagi aloqa xizmatlari vositasida amalga oshiriladi. Infokommunikatsiya xizmati deb, ulanishning ham kiruvchi, ham chiquvchi uchida hisoblash texnikasi vositalaridan foydalanish bilan axborotni talab bo‘yicha avtomatlashtirilgan ishlov berish, saqlash yoki taqdim etishni nazarda tutuvchi telekommunikatsiya xizmatiga aytiladi.

Hozirgi vaqtda kuzatilayotgan infokommunikatsion xizmatlarni taqdim etish xajmlarining yuqori sur’atlarda o‘sishi, ularni yaqin kelajakda aloqa tarmoqlarida ustuvor bo‘lishini bashorat qilishga imkon beradi. Bugungi kunda infokommunikatsion xizmatlarni rivojlanishi asosan Internet doirasida amalga oshiriladi, ya’ni xizmatlarga kirish an’anaviy aloqa tarmog‘i orqali ta’minlanadi. Shu bilan bir qator hollarda Internet xizmatlari, uning transport infratuzilmasi imkoniyatlarining cheklanganligi tufayli, axborot jamiyati xizmatlariga qo‘yiladigan zamonaviy talablarga javob bermaydi. Shu munosabat bilan infokommunikatsiya xizmatlarining rivojlanishi, aloqa tarmoqlarining funksionalligini bir vaqtda kengaytirish bilan axborot resurslarini samarali boshqarish masalalarini yechishni talab qiladi. O‘z navbatida bu Internet va an’anaviy aloqa tarmoqlarining qo‘shilish jarayonini rag‘batlantiradi.

Infokommunikatsiya xizmatlariga quyidagi talablar qo‘yiladi:

- mobillik (harakatchanlik);
- yangi xizmatlarni qulay va tez yaratish imkoniyatlari;
- sifat kafolatlari.

Infokommunikatsiya xizmatlariga qo‘yiladigan talablarga konvergensiya jarayoni katta ta’sir ko‘rsatadi, u bu xizmatlardan foydalanuvchilarga unga kirish usullariga bog‘liq bo‘lmagan holda foydalanish mumkinligiga olib keladi.

Infokommunikatsiya xizmatlarining xususiyatlarini e’tiborga olib, istiqboldagi aloqa tarmoqlariga quyidagi talablar belgilanishi mumkin:

- multiservislik - xizmatlarni taqdim etish texnologiyalarining transport texnologiyalariga bog‘liq emaslik xususiyati;

- keng polosalilik - foydalanuvchining odatdagi ehtiyojlariga bog‘liq holda keng diapozonda axborotni uzatish tezligini qulay va dinamik o‘zgartirish imkoniyati;

- multimedialik - tarmoqning ko‘p komponentli axborotni (nutq, ma’lumotlar, video, audio) haqiqiy vaqt rejimida zaruriy sinxronizatsiya bilan va ulanishlarning murakkab konfiguratsiyalaridan foydalanib uzatish qobiliyati;

- intelektuallik – xizmatlardan foydalanuvchi yoki uni taqdim etuvchining xizmat, chaqiruv va ulanishni boshqarish imkoniyati;

- ulanishning invariantligi - foydalanilayotgan texnologiyaga bog‘liq bo‘lmagan holda xizmatlardan foydalanishni tashkil etish imkoniyati;

- ko‘p operatorlik – xizmatlarni taqdim etishda bir nechta operatorlarning ishtirok etish imkoniyati va ularning javobgarligini ularning faoliyati sohasiga muvofiq ajratish.

ITU-T Y.100 tavsiyalarida telekommunikatsiya texnologiyalarning o‘zaro ta’siri to‘g‘risida ma’lumotlar keltiriladi. Global axborot infratuzilmasi tavsiflanishi mumkin bo‘lgan xossalarni tahlil qilish jarayonida, barcha mavjud telekommunikatsiya texnologiyalari va xizmatlari hamda xizmat ko‘rsatish turlarining tavsiflari hisobga olingan.

Global axborot infratuzilmasining standartlari dasturiy vositalar asosida, ham apparat vositalar asosida, ham ilovalarning va turli xil platformalarning juda katta xilma-xilligi orasida ulanishiga mo‘ljal olib (Connection – Oriented CO), ham ulanishiga mo‘ljal olmasdan (Connection less Oriented CL) ham o‘zaro ta’sirlashuv va o‘zaro aloqa imkoniyatini ta’minlashi kerak. Turli xil texnologiyalar (SC, PS, ATM, MPLS, SDH, WDM va boshqalar) qo‘llaniladigan telekommunikatsiya tarmoqlari (PSTN, DSN, ISDN, MN, IN, CN, OSN) hozirgi vaqtda ma’lumotlar va nutqni yuqori sifat bilan uzatishni ta’minlaydi va bir-biri bilan o‘zaro ta’sirlashadi.

TCP/IP protokolli tarmoqlar shunday platformani yaratadiki, u turli tarmoq infratuzilmalari bilan bog‘liq foydalanuvchilarga ilovalarning umumiy to‘plamiga ega bo‘lishga va eltib berish sifati kafolatlanmaydigan ma’lumotlar oqimlari bilan almashishga imkon beradi.

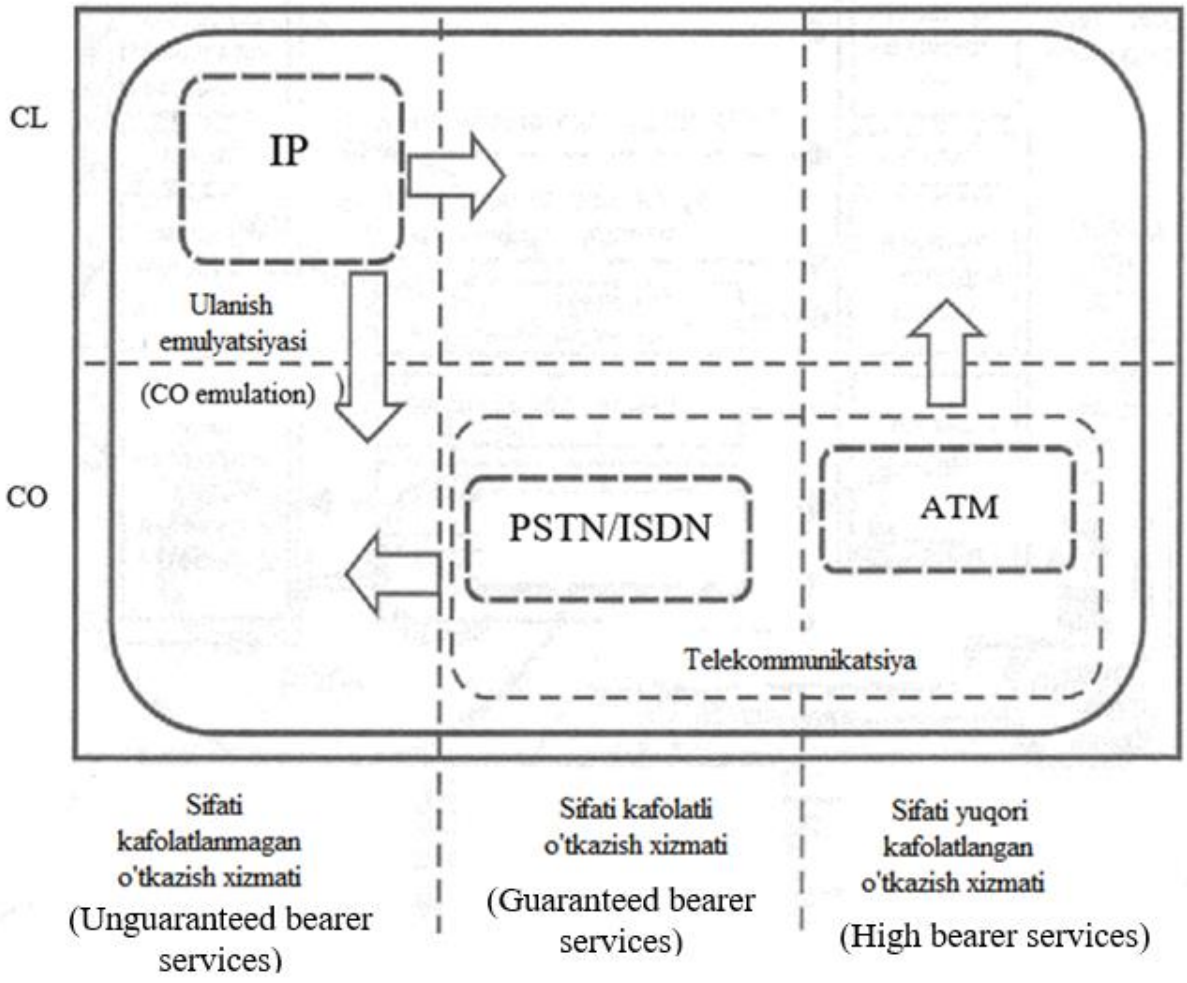
TCP/IP protokollar steki yuqori sifatli nutq, video, multimedia ilovalarini qo‘llab-quvvatlash maqsadida takomillashtiriladi (masalan IPv6). Tarmoq texnologiyalarini konvergensiyasining bu an’analari 8.4-rasmda keltirilgan. Konvergensiyaning yo‘nalishlari quyidagilarni o‘z ichiga qamrab oladi:

- ulanishlar o‘rnatilishi avval mo‘ljal qilinmagan (Sonnection less operation) paketlar kommutatsiyali texnologiyalar, masalan IP protokolidan foydalanuvchi kommutatsiyali texnologiyalar, virtual ulanishlarning (Connection-oriented) dastlabki o‘rnatilishi tufayli axborotni eltib berish sifatini oshirish maqsadida (Guaranted bearer services) takomillashtiriladi;

- kanallar kommutatsiyali tarmoq uzellari (PSTN va ISDN) paketlar kommutatsiyali yangi avlod transport tarmoqlari orqali axborot almashadilar (IP/MPLS), bu esa kechikishga, jitterga va paketlarni yo‘qolishiga sezgir bo‘lgan axborotni eltib berish sifatining pasayishiga (Unguaranted bearer service) olib keladi;

- har qanday ilovalarning axborotini yuqori sifat bilan eltib berishni ta’minlovchi (Guaranted bearer service) ATM texnologiyali tarmoqlar, ulanishga mo‘ljallangan va ulanishga mo‘ljallanmagan (masalan, LANE ATM) holda yetkazib berish xizmatlarini taqdim etadi.

Global axborot infratuzilmasi shunday telekommunikatsiya infratuzilmani yaratishga da’vo qiladiki, u o‘ziga axborotning barcha mumkin bo‘lgan turlarini (nutq, ma’lumotlar, multimedia) birlashtira olsin va ulardan har birining xizmat ko‘rsatish sifatiga bo‘lgan talablarini qanoatlantirsin ( Quality of Service, QoS).



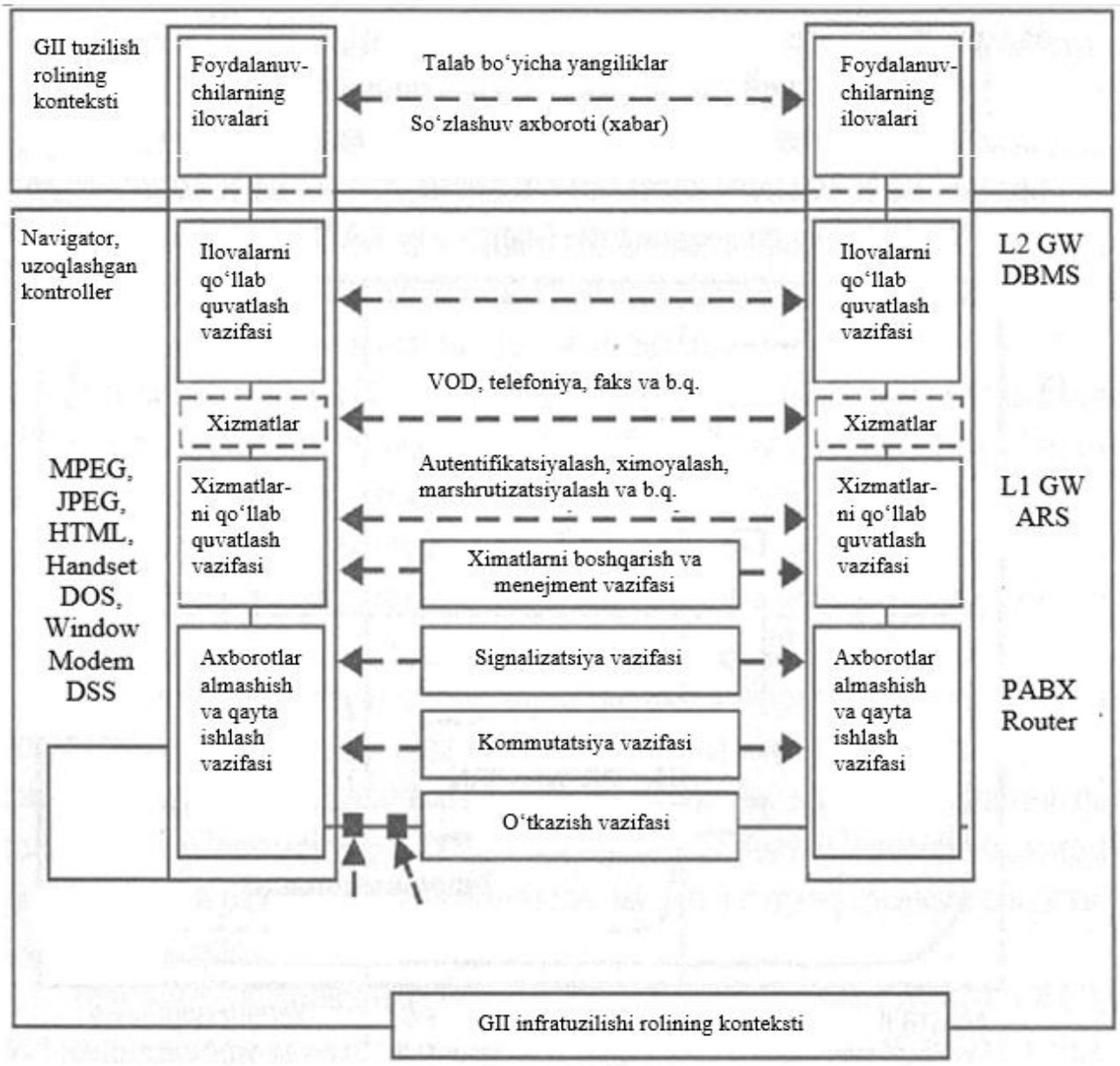

8.4 – rasm. Tarmoqlarning rivojlanish yo‘nalishi (texnologiyalar konvergensiyasi):

CO (Connectoin - oriented operation) - “ulanishni o‘rnatish” rejimida eltib berish;

CL (Connection less operation) “ulanishni o‘rnatmasdan” rejimida eltib berish;

⇨ - texnologiyaning rivojlanish yo‘nalishi.

8.5-rasmda GIIda infratuzilmaviy rollarning konfiguratsiyasini na’munasi keltirilgan. Infratuzilma roli deganda ko‘p marta foydalaniladigan resurslar to‘plami yordamida xizmatlarni ta’minlash tushuniladi.




8.5 – rasm. GII da infratuzilmaviy rollar konfiguratsiyasi namunasi:

DBMS - ma’lumotlar bazasini boshqarish tuzilmasi;

HTML - gipermatnlarni belgilash tili;

JPEG - tasvirlarni siqish standarti;GW - shlyuz;

MPEG - videoni siqish standarti;

FRS - marshrutizatorni avtomatik tanlash.

GII ilovalarning tuzilmaviy roli foydalanuvchilarni ish faoliyatlari bilan belgilangan bo‘lib, u ishlab chiqarish jarayonining bir qismi hisoblanadi. Shuning uchun ilovalar ham chetki foydalanuvchilar orasidagi “virtual o‘zaro tasir”ni yoki ish faoliyatni hisobga olgan holda ishlab chiqiladi. Odatda, ilova harakatlardan va harakatlar o‘rtasidagi munosabatlardan tuzilgan.

## 8.4. Aloqa xizmatlari va ilovalarning tuzilishi

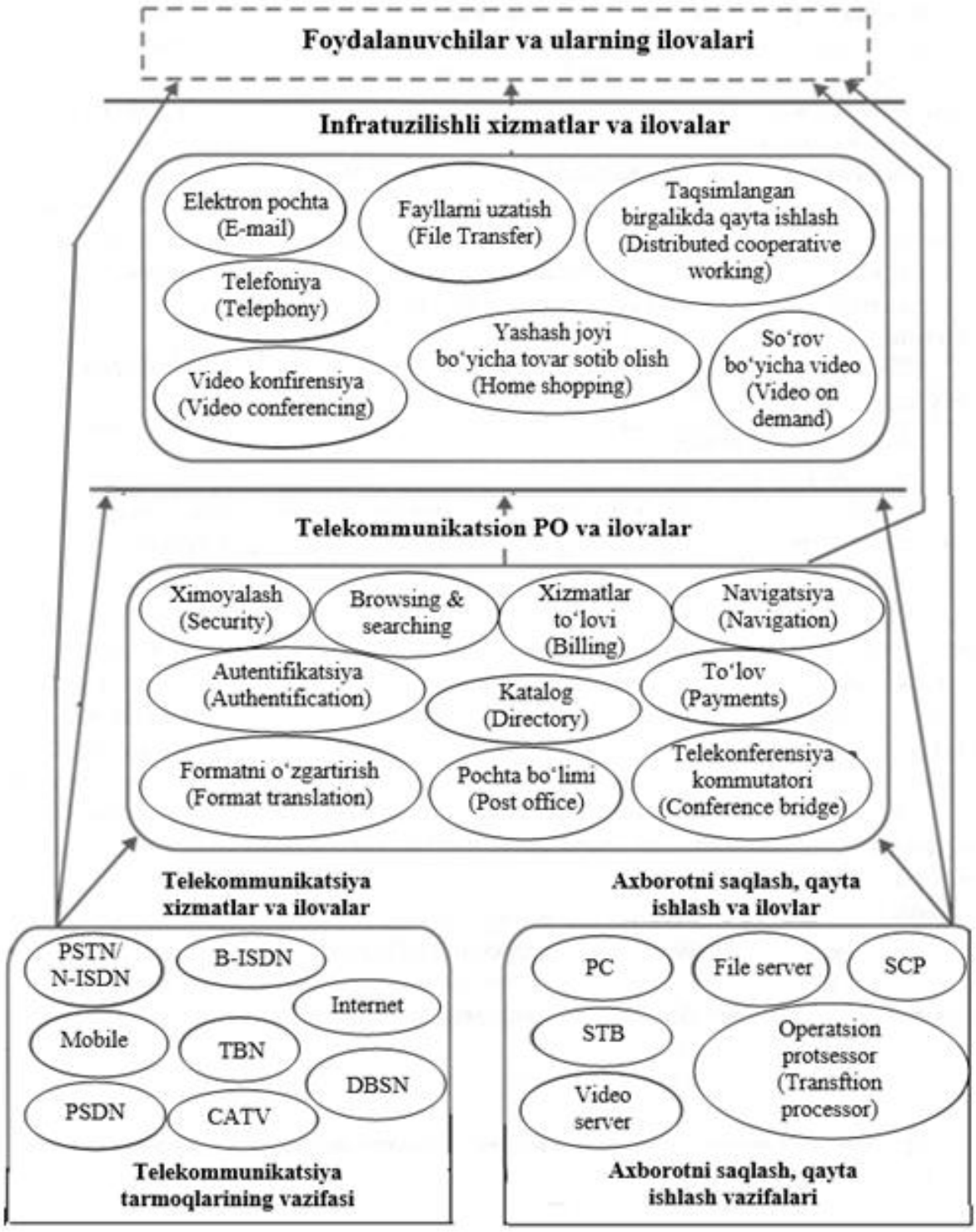
Agar xizmat, xizmatlar bozorining turli ishtirokchilarining javobgarligini ham o‘z zimmasiga olgan yuridik shaxslar o‘rtasida taqdim etilayotgan bo‘lsa, u holda xizmat ko‘rsatish bitim konteksida taklif etiladi va bitimni bajarilishi va tekshirilishi mumkinligi kafolatlanishi uchun yetarli to‘plamdagi parametrlarga ega bo‘lishi kerak.

Foydalanuvchilar bevosita GII xizmatlariga buyurtma berishlari yoki shaxsiy ilovalardan foydalanishlari mumkin, ularni qo‘llab-quvvatlash uchun GII xizmatlari zarur. Bundan tashqari, foydalanuvchi ilovasining komponentlari GII tomonidan taqdim etilishi va qo‘llab-quvvatlanishi mumkin.

GII taqdim etadigan xizmatlar va ilovalar, servisli va amaliy komponentlar shaklida yaratiladi.

Global axborot arxitekturasi quyidagi resurslarni birlashtiradi (8.6 rasm):

- inratuzilmaviy;
- tarmoq (network resources);
- axborotga ishlov berish va saqlash (processing and storage resources);
- telekommunikatsiya dasturiy ta’minoti (middle ware resources).




8.6- rasm. GII tomonidan taqdim etiladigan va qo'llab-quvvatlanadigan xizmatlar va ilovalar:

TBN- Teristrial Broadcast Network – yerusti radioeshittirish tarmog'i;

DBSN – Direct Broadcast Satellite Network - yuldoshli radioeshittirish tarmog'i.

Konvergentli GII da xizmatlar va ilovalar o‘rtasidagi farq shuning uchun ham muhimki, u ikkita turli xil tijorat sxemalari (biznes – sxemalar) ga mos keladi. Bu farq telekommunikatsiya tarmoqlari operatorlarining an’anaviy ravishda xizmatlar taklif etishlari, ayni vaqtda axborot texnologiyalari (AT) an’anaviy ravishda ilovalarni taklif etishlari holatini ham aks ettiradi. “Konvergentli GII” atamasi axborot infratuzilmasini ifodalab, unda trafikning xilma-xil turlari yagona texnologik platformada integratsiyalanadi (qo‘shiladi) va turli xil xizmatlar va ilovalar taqdim etiladi.

GII tomonidan foydalaniladigan umumiy ilovalar quyidagilar hisoblanadi:

- masofadan o‘qitish / elektron kutubxonalar;
- teletibbiyot;
- axborotga taqsimlangan holda ishlov berish;
- elektron savdo;
- elektron nashr;
- o‘yinlar.

## Nazorat savollari

1. Aloqa tarmoqlarini konvergensiyasi deganda nimani tushunasiz?
2. Multimediali aloqa tarmoqlarini qurishda qanday texnologiyalar qo‘llaniladi?
3. Zamonaviy transport tarmoqlarida ATM va MPLS texnologiyalarining vazifasi nimadan iborat?
4. Magistral tarmoqlarda IP/MPLS texnologiyalarining vazifasi nimadan iborat?
5. IP/MPLS va ATM texnologiyalari qo‘llanilgan tarmoq tuzilishini tushuntiring.
6. Nima sababli O‘zbekistonda ATM texnologiyasi qo‘llanilmaydi?
7. Yangi avlod tarmog‘i arxitekturasi qanday sathlardan iborat?
8. Infokommunikatsiya xizmatlariga qanday talablar qo‘yilgan?
9. Istiqbolli aloqa tarmoqlariga qanday talablar qo‘yilgan?

10. Infokommunikatsiya xizmatlariga tushuncha bering.
11. GIIni asosiy elementlari nimalardan iborat?
12. Konvergensiyaning yo‘nalishlari nimalarni o‘z ichiga oladi?
13. Global axborot infratuzilmasi deganda nimani tushunasiz?
14. GII tomonidan qanday xizmatlar va ilovalar taqdim etiladi?

# 9. IP - GA YO‘NALTIRILGAN MULTIMEDIALI TIZIM OSTI – IMS

## 9.1. IP Multimedia Subsystem konsensiyasi

Telekommunikatsiya qurilmalari va tizimlari, protokollar va ilovalarning doimiy ravishda murakkabligining ortib borishiga qaramay, universal tarmoq infratuzilmasini yaratish yo‘nalishidagi ishlar, integral xizmat ko‘rsatishli tor polosali raqamli tarmoqlar (ISDN tarmoqlari), keng polosali ISDN (V-ISDN) tarmoqlari, keyingi avlod tarmoqlari (KAT) bosqichlarini ketma-ket bosib o‘tib davom etmoqda. Nihoyat, IP-ga yo‘naltirilgan multimediali tizim osti – IMS konsepsiyasini yaratilishi, qurilma ishlab chiqaruvchilar, operatorlar va standartlashtirish tashkilotlarining fikriga ko‘ra shunday universal tarmoq infratuzilmasini qurishga yo‘l ochadi.

**IMSga o‘tishning muhim omillari**

IP Multimedia Subsystem (ISM) konsepsiyasi yangi tarmoq arxitekturasini tavsiflaydi, uning asosiy elementi kirishning barcha texnologiyalarini qo‘llab-quvvatlovchi va katta miqdordagi infokommunikatsiya xizmatlarni amalga oshirishni ta’minlovchi paketli transport tarmog‘i hisoblanadi. Uning muallifligi European Telecommunication Standartization Institute (ETSI) va bir nechta milliy standartlashtirish tashkilotlarini birlashtirgan Third Generation Partnership Project xalqaro hamkorlikka tegishli.

IMS dastlab IP protokoli negizida 3-avlod mobil tarmoqlarini qurishga nisbatan ishlab chiqilgan edi. Keyinchalik konsepsiya ETSI-TISPAN qo‘mitasi tomonidan qabul qilingan, uning butun kuchi IP protokollar stekidan foydalanib, statsionar (barqaror) tarmoqlarda xizmatlarning keng spektrini qo‘llab-quvvatlash va amalga oshirish uchun zarur protokollar va interfeyslarning spetsifikatsiyasiga yo‘naltirilgan edi.

Hozirgi vaqtda IMS arxitekturasi ko‘pchilik operatorlar va xizmat provayderlari tomonidan, shuningdek, qurilmani yetkazib beruvchilar tomonidan

keyingi avlod tarmoqlarini qurish uchun mumkin bo‘ladigan yechim sifatida va IP platformasida mobil (harakatdagi) va statsionar (barqaror) tarmoqlar konferensiyasi asosi sifatida qarab chiqiladi.

Mohiyatiga ko‘ra IMS konsepsiyasi UMTS tarmoqlari evolyutsiyasi natijasida, SIP protokoli asosidagi multimediali chaqiruvlar va seanslarni boshqarish sohasini 3G tarmoqlari arxitekturasiga qo‘shilganda vujudga keldi. IMS arxitekturasining asosiy xossalari orasida quyidagilarni alohida ajratish mumkin:

- ko‘p sathlik – transport, boshqarish va ilovalar sathlariga bo‘linadi;
- kirish muhitiga bog‘liq bo‘lmaslik – operatorlar va xizmat provayderlariga qayd qilingan va mobil tarmoqlarni konvergensiyalashga imkon beradi;
- haqiqiy vaqtda multimediali shaxsiy axborot almashinuvini (masalan, tovush, videotelefoniya) va odamlar hamda kompyuterlar o‘rtasida o‘xshashli axborot almashinuvini (masalan, o‘yinlar) qo‘llab-quvvatlash;
- multimediali ilovalarning haqiqiy va haqiqiy bo‘lmagan vaqtga to‘la integratsiyasi (masalan, oqimli ilovalar va chatlar);
- turli xil xizmatlarning o‘zaro aloqada bo‘lishi imkoniyati;
- bitta seansda bir nechta xizmatlarni qo‘llab-quvvatlash yoki bir vaqtda sinxronlashtirilgan bir nechta seanslarni tashkil etish imkoniyati.

## 9.2. IMS arxitekturasini standartlashtirish

IMS arxitekturasini standartlashtirish xalqaro tashkilotlarning vazifasi hisoblanadi, ya’ni keyingi avlod tarmog‘iga tomon yo‘nalishdagi tarmoqlar evolyutsiyasida IMSning asosiy roli tufayli. IMS konsepsiyasi uning hozirgi ko‘rinishida standartlashtirish bo‘yicha uchta xalqaro tashkilotlarning - 3GPP, 3GPP2 va ETST ish natijasi hisoblanadi.

3GPP hamkorligi 1998 yilning oxirida rivojlanuvchi GSM tarmoqlariga asoslangan 3-avlod mobil aloqa tarmoqlari (UMTS tarmoqlari) uchun texnik

spetsifikatsiyalar va standartlarni ishlab chiqish maqsadida ETSI instituti tashabbusi bo‘yicha tashkil etilgan edi.

3GPP2 hamkorlik 1998 yilda Xalqaro Elektraloqa Ittifoqi sha’feligida yaratilgan IMT-2000 loyihasi doirasida 3G tarmoqlar (CDMA-2000 tarmog‘i) standartlarini ishlab chiqish uchun ETSI va ITU tashabbusiga ko‘ra yuzaga keldi. U xuddi 3GPP holatidagidek deyarli o‘sha tashkilotlar tomonidan tashkil etilgan edi. 3G mobil tarmoqlar uchun standartlar rivojida 3GPP2 tashkilotning asosiy ulushi Multimedia Domain (MMD) umumiy nomdagi spetsifikatsiyada tavsiflangan CDMA-2000 tarmog‘ida (IP-transport, SIP-signalizatsiya) IMS konsepsiyasining tarqatilishi hisoblanadi.

Ikkala hamkorlik IETE qo‘mitasi tomonidan standartlashtirilgan IP-ga yo‘naltirilgan protokollarning keng qo‘llanilishiga mo‘ljallangan holda va KAT tarmoqlar arxitekturasining asosiy g‘oyalaridan foydalanib 3G tarmoqlari standartlarini ishlab chiqadi.

IMS konsepsiyasi birinchi marta 3GPP Release 5 xujjatida (2002 yil mart oyida) taqdim etilgan edi. Unda uning asosiy maqsadi – IP protokoli negizida mobil tarmoqlarda multimediali xizmatlarni ta’minlash ifodalangan edi va 2G simsiz tarmoqli IMS arxitekturasi negizida 3G mobil tarmoqlarining o‘zaro ta’sirlashish mexanizmlari ixtisoslashtirilgan edi.

3G tarmoqlar arxitekturasi IMS konsepsiyasiga muvofiq transport, chaqiriqlarni boshqarish va ilovalar sathlari bo‘yicha bo‘linib, bir necha sathlarga (tekislik) ega. IMS tizim osti kirish texnologiyalaridan to‘la mustaqil bo‘lishi va bir necha mavjud tarmoqlar – mobil va statsionar telefon, kompyuter va h.k. bilan o‘zaro aloqani ta’minlashi kerak.

3GPP Release 6 xujjatida (2003 yil dekabr) IMS ning bir qator konsepsiyalari aniqlashtirilgan, simsiz mahalliy tarmoqlar bilan o‘zaro aloqa va axborotni himoya qilish (kalitlarni, abonent sertifikatlarini qo‘llash) masalalari qo‘shilgan edi.

6-7- xujjatlarda SIP vositasida IP kommunikatsiyalarni amalga oshirish g‘oyasi belgilangan. Unga muvofiq SIP bevosita mobil terminaldan boshlanadi.

Release 7 spetsifikatsiyasi, statsionar tarmoqlarda muhim hisoblangan ikkita asosiy vazifalarni qo‘shadi:

- Network Attachment, statsionar tarmoqlarda zarur bo‘lgan va abonentlarni autentifikatsiyalash mexanizmini ta’minlaydi, chunki ularda foydalanuvchini identifikatsiyalash SIM-kartalari bo‘lmaydi;
- Resource Admission, aloqa seanslarini ta’minlash uchun statsionar tarmoqlarda tarmoq resurslarini zahiralaydi.

Statsionar tarmoqlarda IMS konsepsiyalarini kengaytirishga yo‘naltirilgan ishlar, TISPAN qo‘mitasi tomonidan olib boriladi. ETSI tomonidan IMS arxitekturasiga qiziqish, taniqli TIPHON (Telecommunications and Internet Protocol Harmonization Open Networks) guruhini va statsionar tarmoqlarni standartlashtirish uchun javob beruvchi SPAN (Services and Protocols for Advanced Networks) texnik qo‘mitani birlashtirgan (2003 yil) yangi ishchi guruhni yaratishga olib keladi.

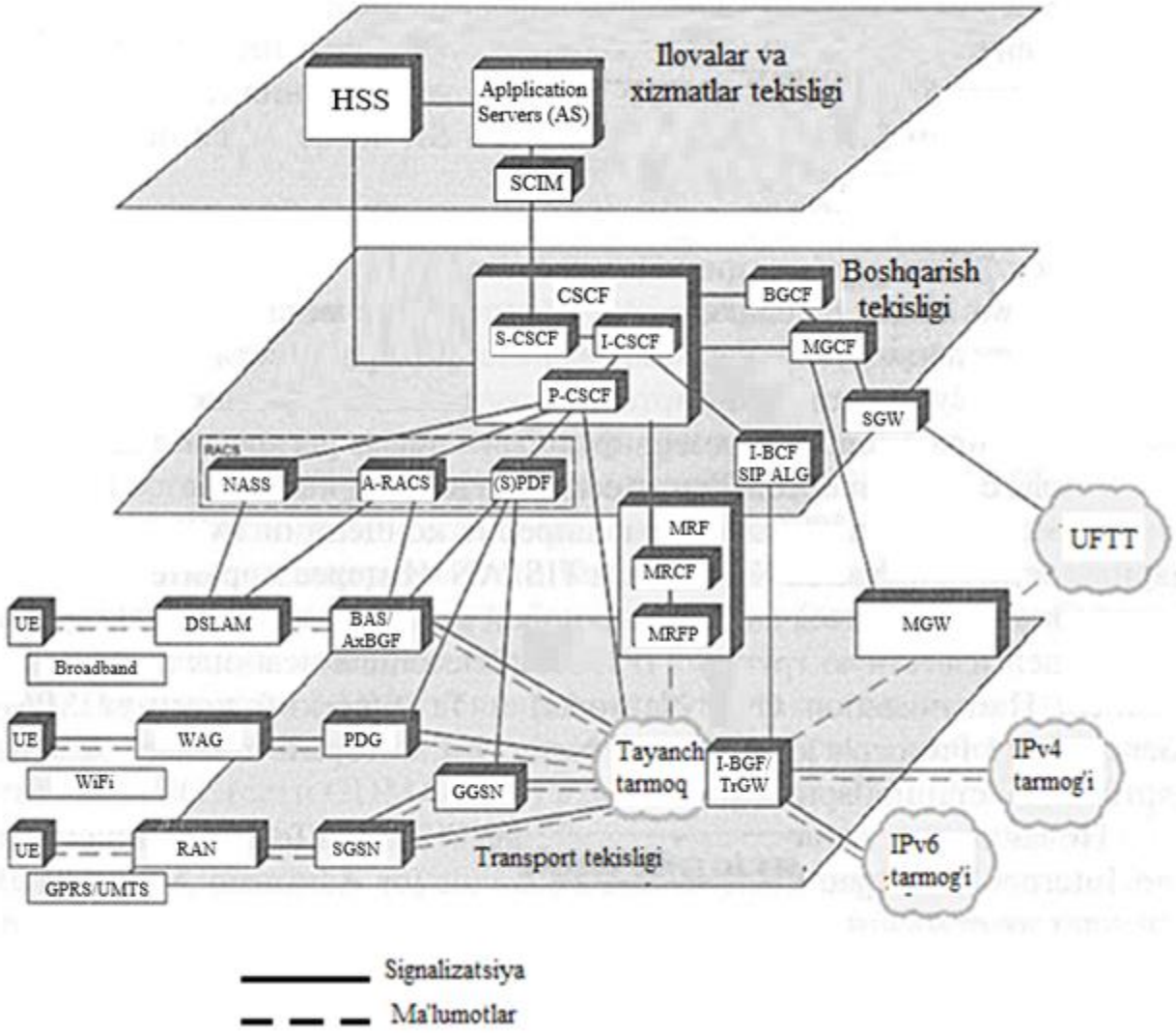
TISPAN (Telecommunication and Internet Converged Services and Protocols for Advanced Networking) nomini olgan yangi guruh zamonaviy va istiqbolli konvergensiyalanuvchi tarmoqlarni standartlashtirish uchun, shu jumladan, VoIP va KAT, shuningdek, IMS arxitekturasi bilan bog‘liq barcha masalalar uchun javob beradi.

## 9.3. IMS arxitekturasi

IMS konsepsiyasi quriladigan tamoyil shundan iboratki, bunda har qanday xizmatni yetkazib berish kommunikatsiya infratuzilma (o‘tkazish qobiliyati bo‘yicha chegaralash bo‘lmagan) bilan hech bir tarzda munosabatda bo‘lmaydi, o‘tkazish qobiliyati bo‘yicha cheklanishlar bundan mustasno. Bu tamoyilni timsoli IMS ni qurishda qo‘llaniladigan ko‘p sathli yondashuv hisoblanadi. U kirish texnologiyasiga

bog‘liq bo‘lmagan xizmatlarni yetkazib berishning ochiq mexanizmini amalga oshirishga imkon beradi, bu esa tarmoqda chetki xizmatlarni yetkazib beruvchilarning ilovalarini ishga tushirish imkonini beradi.

IMS tarkibida uchta sath ajratiladi: transport sathi, boshqarish sathi va xizmatlar sathi (9.1-rasm).




9.1-rasm. IMS arxitekturasining tuzilishi

**Transport sathi.** Transport sathi, abonentlarni IMS infratuzilmasiga foydalanuvchining qurilmasi vositasida ulanishi uchun javob beradi (User Equipment

UE). Mazkur qurilma o‘rnida istalgan IMS terminali ishtirok etishi mumkin (masalan, telefon, smartfon, Wi-Fi yoki keng polosali ulanish). Shuningdek, IMS bo‘lmagan terminal shlyuzlari (masalan, UfTT terminallari) orqali ulanish mumkin.

Transport tekisligining asosiy qurilmalari:

- MRF (Media Resource Function) – mediaserver. MRFP (Media Resource Function Processor) multimedia li resurslar protsessori va MRFC kontrolleridan tashkil topgan.

- MRFC konferens aloqa, xabardor qilish yoki uzatilayotgan signalni qayta kodlash kabi xizmatlarning amalga oshirilishini ta’minlaydi. MRFC, S-CSCT (Serving Call Session Control Function) uzeli orqali olinadigan SIP xabarlarni qayta ishlashi va MRFP protsessorni boshqarish uchun mediashlyuzni (MGCP, 11.248 MEGACO) boshqarish protokoli buyruqlaridan foydalanish nazarda tutiladi. Biroq hozir MRFC va MRFP orasidagi o‘zaro bog‘lanish uchun SIP/XML asosidagi protokolni ilgari siljitish bo‘yicha ish olib borilmoqda. Bundan tashqari MRFC, tarifikatsiyalash va billing tizimlariga zarur axborotlarni taqdim etishni ta’minlaydi.

- MRFR – MRFR protsessori tarmoq mediaresurslarini MRFC dan keladigan buyruqlarga muvofiq taqsimlaydi. Uning asosiy vazifalari quyidagilardan iborat:

- xabardor qilish xizmatlari va h.k. lar uchun oqimlarga, multimedia li ma’lumotlarga xizmat ko‘rsatish;

- kiruvchi multimedia li oqimlarni qayta ishlash, masalan, transkodlash;

- MGW (Media Gateway) – transport shlyuzi, RTP oqimlarini kanallarni kommutatsiyalash tarmoqlari (UfTT) oqimlariga to‘g‘ri va teskari o‘zgartirishni ta’minlaydi;

- I-BGF (Interconnect Border Gateway Function) – tarmoqlararo chegara shlyuzi, IPv4 va IPv6 tarmoqlari orasidagi o‘zaro aloqalarni ta’minlaydi. Xavfsizlik funksiyalarining ta’minlanishi uchun (NAPT adreslari va portlarini translyatsiya qilish, Firewall funksiyalari, QoS vositalari) javob beradi;

- GGSN (Gateway GPRS Support Node) – GPRSni shlyuz uzeli yoki marshrutlash uzeli; uyali tarmoqlar (uning GPRS qismi) va IMS o‘rtasidagi shlyuzni ifodalaydi. GDSN ning asosiy vazifasi SGSN orqali abonentga keluvchi va undan chiquvchi ma’lumotlar roumingi (marshrutlash) hisoblanadi.

- SGSN (Serving GPRS Support Node) – GPRS abonentlariga xizmat ko‘rsatish uzeli; GPRS tizimining paketli axborotni qayta ishlashning barcha funksiyalarini amalga oshirish bo‘yicha asosiy komponenti;

- RAN — Radio Access Network —radioulanish qurilmasi; uyali telekommunikatsiya tizimi va IMS ni o‘zaro aloqasini ta’minlaydi;

- PDG (Packet Date Gateway) – paketli shlyuz. Mazkur tarmoq elementi WLAN foydalanuvchilar qurilmasining IMSga ulanishini ta’minlaydi. Oxiridagi IP-adresning translyatsiyasiga va IMSda foydalanuvchilar qurilmasini ro‘yxatdan o‘tkazishga javob beradi, xavfsizlik vazifasini bajarishni ta’minlaydi;

- WAG (Wireless Access Gateway) – simsiz ulanish shlyuzi WLAN va IMS tarmoqlarining birikishini ta’minlaydi;

- A-BGF/BAS (Access Border Gateway Function/Broadband Access Switch) – keng polosali foydalanuvchilar qurilmasining IMSga kirishini ta’minlaydi. I-BGE ga aynan o‘xshash vazifalarni bajaradi;

- DSLAM (Digital Subscriber Line Access Multiplexer) – raqamli abonent kirish shlyuzi – keng polosali kirishdan (statsionar, masalan, xDSL, KTB tarmoqlari) foydalanuvchi abonentlarni ulanishini ta’minlaydi.

**Boshqarish tekisligi.** Boshqarish darajasi – bu aloqa seanslarini boshqarish bo‘yicha barcha amallarni bajaruvchi IMS funksiyalarining yig‘indisidir. Asosiy elementlari:

- CSCF (Call Session Control Function) – chaqiriqlar va seanslarni boshqarish funksiyali element. CSCF funksiyasi IMS-platformasining boshqarish tekisligida asosiy hisoblanadi. CSCF moduli SIP protokolidan foydalanib, IP transport vositasida haqiqiy vaqt xizmatlari to‘plamini yetkazib berishni ta’minlovchi vazifalarni bajaradi.

CSCF funksiyasi tarmoq resurslarini (chegaraviy qurilmalar, shlyuzlar va ilovalarning serverlari) foydalanuvchilarning va ilovalarning profiliga bog‘liq holda samarali boshqarish uchun dinamik axborotdan foydalanadi. CSCF moduli uchta asosiy funksiyalarni o‘z ichiga oladi:

- Serving CSCF (S-CSCF) – CSCF ga xizmat ko‘rsatuvchi. Chetki qurilmalar almashadigan barcha SIP-xabarlarni qayta ishlaydi;
- Proxy CSCF (P-CSCF) – u orqali IMS tizimiga barcha foydalanuvchilarning trafigi kelib tushadi;
- Interrogating CSCF (I-CSCF) – CSCF ni talab qilib oluvchi. U uy tarmog‘i bilan ulanish nuqtasini ifodalaydi. I-CSCF aniq bir abonent uchun S-CSCF ni topish uchun NSS ga murojaat qiladi;
- S-CSCF - ilovalar va foydalanuvchining profiliga bog‘liq holda IP transportning multimedia li xabarlarini yetkazib berish seanslarini boshqarishni, shu jumladan, terminallarni ro‘yxatga olish, NSS serveri bilan ikki tomonlama o‘zaro aloqa (undan foydalanuvchilar ma’lumotlarini olish), xabarlarni tahlil qilish, marshrutlash, tarmoq resurslarini boshqarishni (shlyuzlar, serverlar, chegaraviy qurilmalar) ta’minlaydi;
- P-CSCF – mazkur tarmoqning IMS terminallari uchun IMS yadrosi ichida signal sathidagi birinchi kontakt nuqtasini yaratadi. P-CSCF funksiyasi terminaldan yoki terminalga talabni qabul qiladi va uni IMS yadrosi elementlariga marshrutlaydi. Foydalanuvchining xizmat ko‘rsatiladigan terminali, qayd qilishning butun vaqtida tarmoqda ro‘yxatga olishda P-CSCF ning funksiyasiga mahkamlanadi. P-CSCF moduli foydalanuvchini autentifikatsiya qilish bilan bog‘liq funksiyalarni amalga oshiradi, hisobga olish yozuvlarini shakllantiradi va ularni to‘lovni hisoblash serveriga uzatadi. P-CSCF ning elementlaridan biri Policy Decision Function (FDE) hisoblanadi – axborot trafigi tavsiflari bilan amallar bajaruvchi (masalan, talab qilinadigan o‘tkazish qobiliyati) va seansni tashkil qilish yoki uni man qilish

imkoniyatini, seans parametrlarini o‘zgartirish zaruriyatini aniqlovchi siyosatni tanlash funksiyasi;

- I-CSCF mazkur tarmoqning abonentlari bilan barcha tashqi ulanishlar uchun IMS yadrosi ichida signal sathida birinchi kontakt nuqtasini yaratadi. I-CSCF modulining asosiy vazifasi – tashqi abonentning xizmatlardan foydalana olishi bo‘yicha imtiyozlarni identifikatsiya qilish, ilovalar serverini tanlash va unga kirishni ta’minlashdir;
- BGCF (Breakout Gateway Control Function) – shlyuzlarni boshqarish funksiyasi, kanallar kommutatsiyasi domeni (UfTT yoki GSM) va IMS tarmog‘i orasidagi chaqiriqlarni qayta uzatishlarni boshqaradi. Mazkur modul telefon raqamlari asosida marshrutlashni amalga oshiradi va IMS tarmog‘i orqali (BGCF serveri joylashgan joyda) UfTT yoki GSM bilan o‘zaro aloqada bo‘ladigan kanallar kommutatsiyasi (KK) domenida shlyuzni tanlaydi. Shuningdek, KK tarmoqlari abonentlari uchun to‘lovni hisoblash uchun tegishli hisob yozuvlarini ta’minlash amalga oshiriladi;
- MGCF (Media Gateways Control Function) shlyuzlarni boshqarish funksiyasi (Media Gateways) – H.248/MEGACOdan foydalanib IMS transport shlyuzlarida ulanishlarni boshqaradi;
- SGW (Signaling Gateway) – signal shlyuzi UfTT signalizatsiyani MGCF ga tushunarli ko‘rinishga o‘zgartirishni ta’minlaydi. IMS yadrosi bilan SIG-TRAN protokollar guruhi interfeyslari orqali bog‘langan;
- RACS (The Resource and Access Control) – resurslar va kirishlarni boshqarish tizimosti – kirishni boshqarish (ixtiyorida bo‘lgan mavjud resurslar, mahalliy siyosat asosida yuklash) va tarmoqqa shlyuzni boshqarish yordamida kirish (Gate Control), shu jumladan, tarmoq adreslari va portlarini almashtirishni boshqarish va ustuvorlikni biriktirish;
- PDF (Policy Decision Function) – axborot profili tavsiflari bilan amallarni bajaruvchi (masalan, talab etiladigan o‘tkazish qobiliyati) va seansni tashkil etish

mumkinligini yoki uni ta’qiqlash mumkinligini, seans parametrlarini o‘zgartirish zarurligini aniqlovchi siyosatni tanlash funksiyasi;

- NASS (Network Attachment Subsystem) – tarmoqning ulanish qism tizimi – uning asosiy vazifalariga IP-adreslarni dinamik tayinlash (DHCP dan foydalanib – Dynamic Host Configuration Protocol), IP sathda autentifikatsiya, tarmoqqa kirishni yuklash, IP sathda turgan joyni boshqarish kiradi.

**Ilovalar sathi.** IMS etalon arxitekturasining yuqori sathi ilovalar serverlari to‘plamini o‘z ichiga oladi, ular asosan IMS ning elementlari bo‘lib hisoblanmaydi. Yuqori tekislikning bu elementlari o‘z tarkibiga SIP protokoli negizidan IP-multimedia li ilovalarni ham, virtual uy muhiti negizida mobil tarmoqlarda amalga oshiriluvchi ilovalarni ham oladi.

IMS ilovalari arxitekturasi nihoyatda murakkab, lekin bu yerda asosiysi yangi ilovalarni yaratishda va an’anaviy ilovalar bilan integratsiyada yuqori darajada moslashuvchanlik hisoblanadi. Masalan, ma’lumotlarni uzatish muhiti telefon chaqiriqning an’anaviy xossalari bilan integratsiyalashi mumkin, masalan, teskari chaqiriq va chaqiriqni kutish Internet chaqirig‘i bilan. Buni bajarish uchun IMS arxitekturasi juda ko‘p xizmatlarni ishga tushirishga va ular orasida tranzaksiyalarni boshqarishga imkon beradi.

- SSIM (Service Capability Interaction Manager) – IMS yadrosi va ilovalar tekisligining o‘zaro ta’sirlashuvini boshqarishni ta’minlaydi;

- SIP AS (SIP Application Server) – SIP protokoliga asoslangan xizmatlarni bajarish uchun xizmat qiluvchi ilovalar serveri. IMS dagi barcha yangi xizmatlar aynan SIP AS da joylashadi deb kutiladi;

- OSA-SCS (Open Service Access – Service Capability Server) – bo‘lishi mumkin bo‘lgan xizmatlar serveri, u xizmatlarga ochiq kirishga asoslangan xizmatlarga interfeysni ta’minlaydi (OSA - Open Service Access). Maqsad xizmatlarga standart dasturiy interfeys ilovalari vositasida tarmoq fuknsiyalariga kirish imkonini ta’minlash hisoblanadi;

- IM-SSF (IP Multimedia – Service Switching Function) – xizmatlarni kommutatsiyalash serveri, u IMS tizim ostini mobil tarmoq tizimining mantiqini yaxshilash uchun ilovalardan foydalanuvchiga moslashgan tizimdagi xizmatlar bilan ulanish uchun xizmat qiladi (CAMFI – Customized Applications for Mobile Network Enhanced Logic). Gap GSM global mobil aloqa tizimi uchun ishlab chiqilgan xizmatlar to‘g‘risida bormoqda, IM-SSF funksiyasi (xizmatlarni kommutatsiyalash funksiyasi) yordamida mazkur xizmatlardan foydalanish IMS da ham mumkin;

- TAS (Telephony Application Server) – telefon ilovalari serveri SIP protokoli axborotlarini qabul qiladi va qayta ishlaydi, shuningdek, chiquvchi chaqiriq qay tarzda tashkil etilishi mumkinligini aniqlaydi. TAS xizmati mantiqi chaqiriqlarni qayta ishlashning tayanch xizmatlarini ta’minlaydi, shu jumladan, raqamlar tahlili, marshrutlash, chaqiriqlarni belgilash, kutish va yo‘nalishni o‘zgartirish, konferensaloqalarni ta’minlaydi. Agar chaqiriq UfTT da qayd etilgan yoki terminlashgan bo‘lsa, TAS serveri TDM (UfTT) nutq oqimi bitlarini IP RTP oqimga o‘zgartirishga va uni tegishli IP telefonning IP-adresiga yo‘naltirishga mediashlyuzlarga buyruq berish uchun MGCF funksiyasiga SIP signalizatsiyasi uchun javob beradi. IMS ning bitta xabarida abonent qurilmalarining turli xillariga ma’lum xizmatlar taqdim etuvchi bir necha TAS to‘g‘risidagi ma’lumotlar bo‘lishi mumkin. Masalan, bitta TAS serveri IP Centrex ga xizmatlarni ko‘rsatadi (raqamlashning xususiy rejalari, umumiy ma’lumotnomalar, chaqiriqlarni avtomatik taqsimlash va h.k.), boshqa server ATSni qo‘llab-quvvatlaydi va VPN xizmatlarini taqdim etadi. Bir nechta ilovalar serverlarining o‘zaro ta’sirlashuvi turlicha sinflardagi abonent qurilmalari orasidagi chaqiriqlarni tugatish uchun SIP-I signalizatsiya vositasida amalga oshiriladi;

- HSS (Home Subscriber Server) – uy abonentlari serveri – GSM tarmoqlari elementiga - HLR (Note Location Register) serveriga o‘xshash - foydalanuvchilar ma’lumotlari bazasi hisoblanadi. HSS serveri xizmatlar bilan bog‘liq foydalanuvchining shaxsiy ma’lumotlariga nisbatan yozuvni o‘qish rejimida ochiq

kirishni ta’minlaydi. Kirish turli xil chetki oxirgi nuqtalardan, jumladan, telefon, WEB va SMS ilovalar, set-top box turidagi televizion qo‘shimchalar va boshqalar orqali amalga oshiriladi. Shuningdek HSS da, SLF (Subscription Locator Function) funksiyasi amalga oshirilib, u I-CSCI modulidan yoki ilovalar serveridan savolga javob tariqasida aniq bir abonentning ma’lumotlarini o‘z ichiga olgan ma’lumotlar bazasining holatini aniqlaydi. Nihoyat, HSS serveri tarkibiga 2G tarmoqlari bilan ishlash uchun HLR va AuC (Autentification Center) modullari kiradi.

IMS muhitida HSS serveri har bir foydalanuvchi va abonent tomonidan ishga tushirilgan xizmatlar to‘g‘risidagi ochiq ma’lumotlar bazasi sifatida ishlaydi: foydalanuvchi qanday xizmatlarga obuna bo‘lgan, bu xizmatlar yuklatilganligi, foydalanuvchi tomonidan qanday boshqaruv parametrlari o‘rnatilganligi.

## Nazorat savollari

1. IMS nima maqsadda yaratilgan?
2. IMSning vazifasi nimadan iborat?
3. IMSga o‘tishning qanday muhim omillari mavjud?
4. IMS arxitekturasi qaysi tashkilotlar tomonidan standartlashtirilgan?
5. IMS arxitekturasining qanday asosiy xususiyatlarini bilasiz?
6. IMS arxitekturasi qanday sathlardan iborat?
7. IMSning transport sathining vazifasi nimadan iborat?
8. IMSning transport sathida qanday qurilmalar qo‘llaniladi?
9. IMSning boshqarish sathining vazifasi nimadan iborat?
10. IMSning boshqarish sathining elementlarini ayting.
11. IMSning ilovalar sathining vazifasi nimadan iborat?

# 10. MULTIMEDIA LI TARMOQLARNI LOYIHALASHTIRISH

## 10.1. Telekommunikatsiya tarmoqlarini loyihalashtirish uslubiyotlari

Loyiha xujjatlari quyidagi bo‘limlardan iborat bo‘lishi kerak:

- telekommunikatsiya qurilmalari va liniya inshoatlarining hajmi;
- xizmatlar, foydalanuvchilarning har bir toifasi uchun axborotni yetkazib berish sinflari, o‘tkazish oralig‘iga extiyoj;
- qurilmaning ishlash rejimi;
- qurilmani nomenklaturasi, yuzi va joylashtirish;

Telekommunikatsiya qurilmasi va liniya inshoatlarining hajmini hisoblash usuli quyida keltirilgan. Hisoblashning asosi yuklama, paketli texnologiyali tarmoqlarda xizmat ko‘rsatish sifati va axborotlarni yetkazib berish, taqdim etilayotgan xizmatlar ro‘yxati hisoblanadi.

Kirish shlyuzlarining (AGW) miqdori va sig‘imi abonentlar tarkibini, talablar miqdori va taqdim etilayotgan xizmatlarni hisobga olgan holda hisoblanishi kerak.

Paketli tarmoqlarda multimedia li axborotlarni eltib berish sifatining asosiy ko‘rsatkichlari quyidagilardir:

- virtual ulanishni o‘rnatish vaqti;
- multimedia li axborotlarni eltib berishning o‘rtacha kechikishi;
- paketlarni yuqolish ehtimolligi.

Ulanishni o‘rnatish vaqti - bu raqamni tergandan keyingi kechikish (Call Set up Time):

- mahalliy ulanish - 3 sekunddan kam;
- shaharlararo ulanish - 5 sekunddan kam;

- xalqaro ulanish - 8 sekunddan kam.

IP – paketlarni “uchidan - uchigacha” ko‘chirishning (bir yo‘nalishda) va yo‘qolgan IP-paketlar ulushining o‘rtacha kechikishlarqiymati Y.1541 tavsiyalardan olinishi mumkin.

**Multimedia li tarmoqlarni loyihalashtirishda yechimlarni asoslash.** Multimedia li aloqa tarmog‘ining loyihasi uch bosqichda amalga oshirilishi mumkin.

1 - bosqichda turli xizmatlarga buyurtma berilganda turli terminallar yuzaga keltirgan yuklama baholanadi. Loyihalashtirilayotgan tarmoq uzellariga xizmat ko‘rsatish zarur bo‘lgan yuklamani baholash uchun quyidagi ma’lumotlarga ega bo‘lish zarur:

- terminallar soni;

- terminallar buyurtma qiladigan xizmatlar turlari;

- har bir xizmatni buyurtma qilishda terminal tomonidan yaratiladigan solishtirma yuklama;

- har bir xizmatga mos keluvchi yuklamaning statistik xossalari;

- barcha turdagi xizmatlar va terminallar bo‘yicha yig‘indi yuklama;

- yuklamani yo‘nalishlar bo‘yicha taqsimlash.

Har bir terminal yuzaga keltiradigan yuklama mavjud statistik ma’lumotlar yoki normativlar asosida baholanishi mumkin.

Multimedia li tarmoqlarda asosan turli xil xizmatlarni ta’minlashga qodir funksional terminallardan foydalaniladi. Shuning uchun har bir xizmat bo‘yicha yuklamani baholash zarur.

Yo‘nalishlar bo‘yicha yuklamani taqsimlash uchun tortishish koeffitsientlarini hisoblashga asoslangan usullardan foydalaniladi.

Multimedia li tarmoqni loyihalashtirishning 2–bosqichida quyidagilar zarur bo‘ladi:

- transport tarmoqni amalga oshirish uchun texnologiyalarni qo‘llashni asoslash va tanlab olish;

- transport tarmog‘ini qurish topologiyasini tanlash va asoslash, shu jumladan fizik sathdagi topologiyani (shina, yulduz, halqa, aralash va xokozo), fizik sathda ulanishlarni tashkil etishning mantiqiy topologiyasini, shuningdek yuqoridagi sathlarda fizik yo‘llarni, mantiqiy kanallarni zahiralashni hisobga olgan holda va muqobil marshrutlarni tashkil etish;

- barcha tarmoq uzellari (kirish uzellari, kommutatorlar, multipleksorlar, marshrutizatorlar, portlar, shlyuzlar) bo‘yicha, shu jumladan tarmoq sathidagi xizmatchi protokollar (ICMP, IGMP, IGRP, RSVP, marshrutlash protokollari) bo‘yicha uchta quyi sathlarning protokollarini steklari va profillarini detallashtirish (u yoki bu protokol yordamida qo‘llab-quvvatlash zarurligini, protokol turini, uning stekdagi holatini baholash);

- chetki terminallar, shuningdek xizmatlarni ta’minlashning tarmoq uzellari uchun (web, E-mail, DNS, FTP, billing, SN xizmatlar serverlari) xizmatlarni ta’minlash uchun yuqori sathlarning protokollarini hisobga olgan holda protokollarning steklarini va profillarini detallashtirish;

- tanlangan texnologiya va o‘zaro ta’sirlashuvchi tarmoqlar turiga muvofiq tarmoq interfeyslari turlarini aniqlash, ularning o‘tkazish qobiliyatini keyinchalik hisoblab chiqish zarur.

Loyihalashtirishning 3-bosqichida quyidagi amallarni bajarish kerak:

- xizmatlarning har biri bo‘yicha axborot trafigini (U tekisligida), shuningdek konsentratsiyalash, multipleksorlash, tarmoqlar va kirish uzellari (AN) trafigini biriktirishning boshqa turlarining barcha xizmatlari bo‘yicha umumiy (yig‘indi) axborot trafigini hisoblash;

- trafikni tarmoq uzellari orasidagi yo‘nalishlar bo‘yicha (kommutatsiyalash-marshrutlashtirish uzellarini va xizmatlarni ta’minlash serverlarini ham inobatga olib) taqsimlashni hisobga olgan holda magistral tarmoq yadrosini (Core Network, CN) kommutatsiyalash va marshrutlash uzellarida barcha xizmatlarning axborot trafigini hisoblab chiqish;

- axborot protokollari, RTP/UDP/IP/MPLS protokollarining xizmatchi qismi kiritadigan ortiqcha trafik ulushini baholash;

- chaqiriqlarni boshqarish uchun (SIP, ISUP, Q 931, PSTN- V 5.2, H. 225 va boshqa signal protokollar);

- shlyuzlarni boshqarish (H. 245, H 248, MCCP RAS );

- marshrutlash, billing, mualliflash, DNS xizmatlarni boshqarish;

- talab etiladigan yetkazib berish sifat ko‘rsatkichlariga amal qilgan holda turli xizmatlar uchun navbatlarga xizmat ko‘rsatish intizomini tanlash;

- tarmoq uzellarining buferli xotirasi xajmlarini va bu uzellarning talab etilgan unumdorligini baholash;

- tarmoqning tanlab olingan topologiyasi uchun foydalaniladigan interfeyslarning o‘tkazish qobiliyatini baholash va hisoblash;

Multimedia li tarmoqni loyihalashning birinchi bosqichining mazmunini ko‘rib chiqamiz.

- *Terminallar sonini baholash.*

Terminallar sonini baholash uchun turli usullar qo‘llaniladi:

- marketing tadqiqotlari (umumiy foydalanish tarmoqlari uchun baholashlar asosida shaxsiy kompyuterlarni sotishning ortishi qo‘yilishi mumkin);

- o‘tgan davr uchun mavjud bo‘lgan ma’lumotlar asosida terminallarning ko‘payishini bashorat qilish (korporativ tarmoqlar uchun) .

Bashorat qilinayotgan o‘sish tatbiqiy dasturlar - Excel, Mathcad, Statistic va xokozolar negizida matematik usullardan foydalangan holda hisoblab chiqilishi mumkin.

- *Terminallar buyurtma beradigan xizmatlar turlari va ularni kirish uzellari bo‘yicha taqsimlash.*

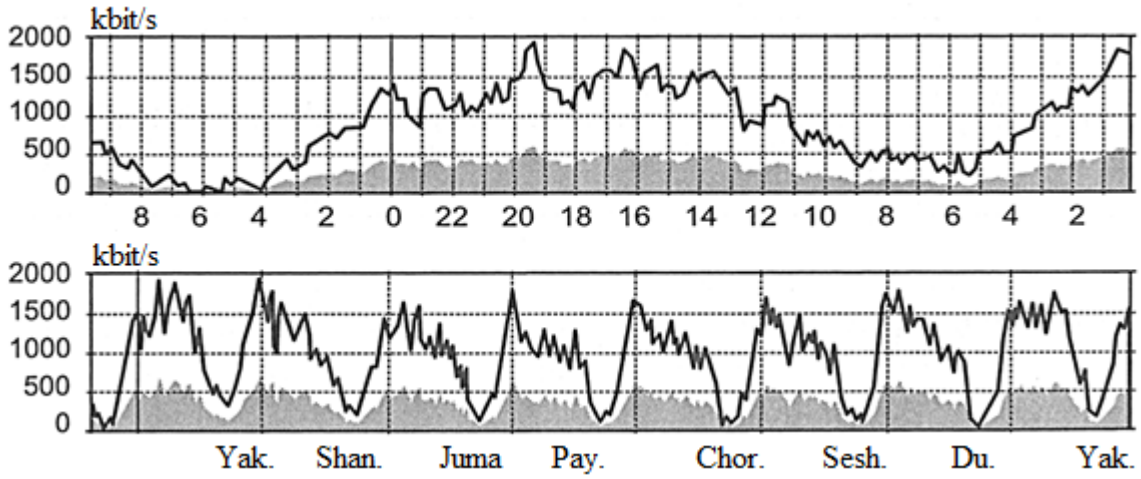
Terminallarning kirish uzellari bo‘yicha xizmatlar turlarini ko‘rsatgan holda grafik yoki jadval ko‘rinishida aks ettirish.

- *Har bir xizmatga buyurtma berilganda terminal yuzaga keltiradigan solishtirma yuklama.*

Har bir terminal yuzaga keltirgan yuklama, statik yoki normativ asosida baholanishi mumkin.

- *Har bir xizmatga mos yuklamani statik xususiyati.*

10.1-rasmda E1 interfeysning sutka soatlari va xafta kunlari bo‘yicha kompressorlangan nutq axboroti bo‘lgan paketlar oqimlari bilan yuklash grafiklari tasvirlangan.




10.1- rasm. E1interfeysning sutka soatlari (yuqorida) va xafta kunlari (pastda) bo‘yicha kompressorlangan nutq axboroti bo‘lgan paketlar bilan yuklash grafiklari

Rasmdan ko‘rinadiki uzatilayotgan axborotning cho‘qqi xajmlari va uzatilayotgan axborotning o‘rta hajmi orasidagi nisbat 2-3 diapazonida yotuvchi yetarlicha barqaror kattalik hisoblanadi.

Hisoblashlarda bu nisbatni 2,5ga teng qilib olish mumkin. Ma’lumotlarni uzatish xizmatlari uchun ham cho‘qqi va o‘rtacha yuklanishlar orasida xuddi shunday nisbatni kuzatish mumkin.

Interfeysda ma’lumotlar oqimi bilan hosil bo‘ladigan yuklanishni, axborotlarni IP-tarmoqda yetkazib berish vositalarini qo‘llash samaradorligi koeffitsientini, pachkalilik koeffitsientini va uzatish tezligini bilgan holda hisoblash mumkin.

Mavjud umumiy foydalanishdagi telefon tarmoqlaridan axborotlar oqimlarini paketli multiservisli tarmoqlarga ko‘chirish uchun UfAT (umumiy foydalanishdagi aloqa tarmoqlari, UfAT)da mavjud qaror topgan trafikni taqsimlash modelidan foydalanish mumkin.

Tarmoq serverlari xizmatlarini (web, E-mail, DNS, FTP, billing, SN va boshqalar) ta’minlashni talab etadigan manbalar hosil qiladigan yuklamani hisoblashda, bu serverlarning tarmoq uzellari (CN)ga ulanish nuqtalari bo‘yicha joylashtirishni hisobga olish zarur.

Barcha xizmatlar uchun axborotlarni yetkazib berishning talab etilgan sifatini ta’minlash uchun, trafikning barcha turlari orasida ma’lum nisbatga rioya qilish zarur. Kechikishlarga eng moyil bo‘lgan axborot turlari, bu haqiqiy vaqtda yetkazib berilishi kerak bo‘lgan axborotlar hisoblanadi.

Agar haqiqiy vaqt trafigi uchun talab etilayotgan o‘tkazish qobiliyati 30% ga yetsa, interfeysning umumiy o‘tkazish qobiliyatidan, u holda bu turdagi axborotni yetkazib berish sifati keskin pasayadi. Shuning uchun tarmoqni loyihalashtirish va tarmoqdan foydalanishning boshidagi bosqichda, barcha turdagi axborotlarni eltib berishning kafolatli sifati uchun haqiqiy vaqt trafigi / tranzaksiyalar / ma’lumotlar orasida 30/30/40 nisbatga amal qilish zarur.

Paketli tarmoq bo‘ylab (IP-telefoniya) so‘zlashuv axborotlarini uzatish uchun quyidagilarni baholash zarur:

- foydalanuvchilar soni;

- G.7xx/RTP/UDP/IP/MPLS (birlamchi tarmoq texnologiyalari) profili uchun ortiqcha trafik.

So‘zlashuv terminallari yaratgan yuklamani quyidagi uch usuldan biri bilan hisoblash mumkin:

- solishtirma yuklama qiymatlari bo‘yicha, erlang hisobida;

- IP texnologiyaning protokolli ortiqchaligi (Ethernet+IP+UDP+RTP protokollar sarlavhalari) va o‘tkazish oralig‘ini zahiralashni hisobga olgan holda, kodeksning har bir turi uchun ma’lumotlarni talab etilgan uzatish tezligi bo‘yicha, Kbit/s

- $T_s$ so‘zlashuv seansining o‘rtacha statistik uzunligida, s va audiokodeksning V tezligida Kbit/s uzatiladigan ma’lumotlarning hajmi bo‘yicha; (bir seans davomida $Q=T_s\ V$ Kbit hajmni uzatishi zarur).

Kechikishga sezgir bo‘lgan axborotni eltib berish sifatini oshirish uchun ustunliklar (Diff-Services) yordamida differensiallashgan mexanizmlardan hamda RSVP, RAS va boshqa protokollar yordamida interfeysda (Int-Services) kanalning zarur o‘tkazish oralig‘ini zahiralash mexanizmlaridan ham foydalanish mumkin.

Paketli tarmoqda bu ikki mexanizmdan foydalanishda kanalning emulyatsiyasi uchun sharoitlar yaratiladi. Bunday emulyatsiyalangan kanalning TDM telefoniyadagi kanaldan farqi, uning o‘tkazish oralig‘ini qulay holda prinsipial o‘zgartirish hisoblanadi.

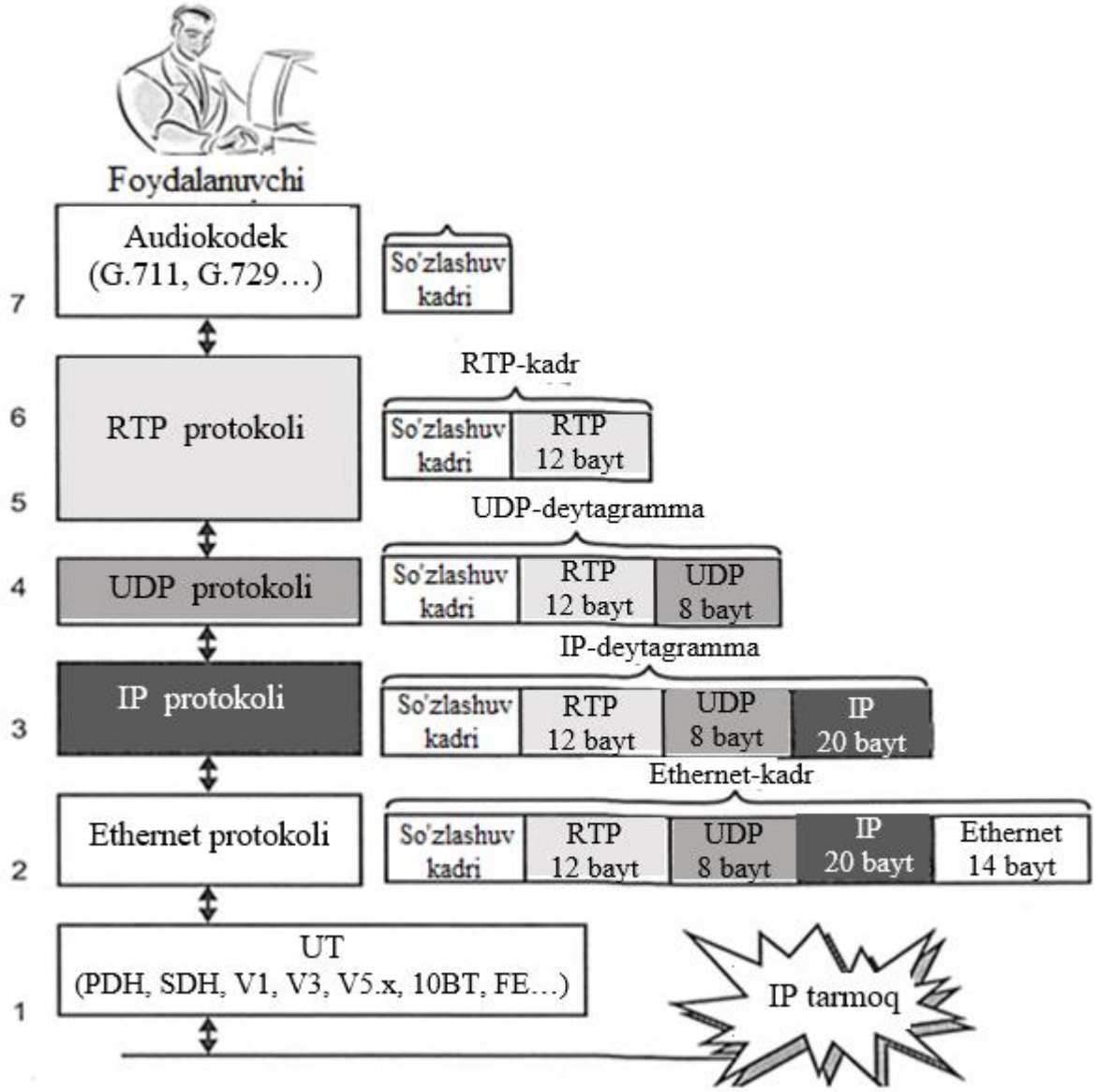
ATM, MPLS yoki VLAN/Ethernet texnologiyali transport tarmoqlarida axborotlarni eltib berishning quyidagi sinflari nazarda tutilgan:

- CBR (ATM) yoki EF(IP/MPLS);

- RT – VBR (ATM) yoki AF1 (IP/MPLS).

EF (IP/MPLS) deganda to‘siqsiz (tezkor) manzilli o‘zgartirish sinfi (Expedited Forwarding, EF), AF1 (IP/MPLS) deganda esa kafolatlangan manzilni o‘zgartirish sinfi (Assured Forwarding, AF) tushuniladi.

Paketlitarmoqda CBR/EF sinfi uchun minimal zarur bo‘lgan o‘tkazish oralig‘i zahiraga olinadi. Yetkazib berishning aynan ana shu xizmatlar sinfi boshqa tarmoqlardan kelib tushadigan axborotni qayta jo‘natish uchun paketlar kommutatsiyali tarmoqda kanallarni emulyatsiya qilishga imkon beradi.




10.2-rasm. IP-tarmog‘ida so‘zlashuv axborotini yetkazib berishni ta’minlovchi protokollar

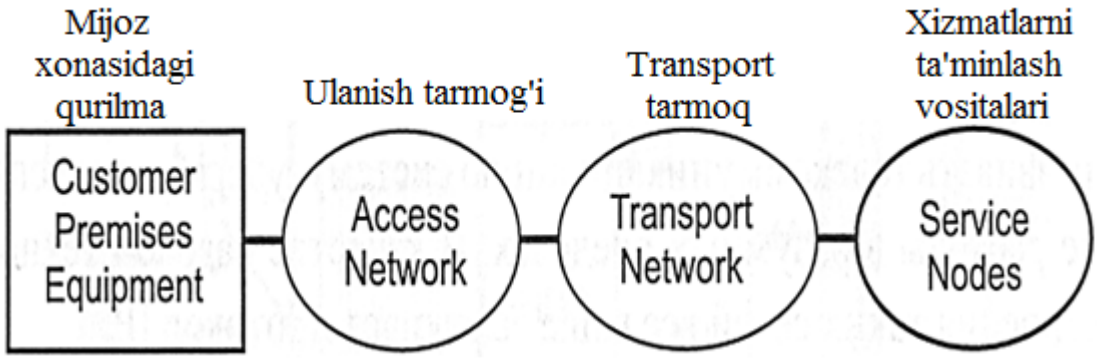
Bunda so‘zlashuv axborotni eltib berish uchun eng qulay sharoitlar yaratiladi. Biroq sifatning bu sinfi tarmoq orqali uzatilayotgan axborotning eng ko‘p ortiqchaligiga mos keladi. Masalan, G.711 audio kodekdan foydalanilganda (kodlash tezligi 64 Kbit/c) 128 Kbit/c tezlikka mos keluvchi o‘tkazish oralig‘ini zahiralashi zarur, bu esa TDM telefoniyaga nisbatan ikki marta kattadir. Agar tezligi ancha past

bo‘lgan audio kodeklardan foydalanilsa (masalan, G.729-8 Kbit/s) u holda ajratilayotgan kanalning o‘tkazish oralig‘ining kengligini ancha kamaytirish mumkin.

## 10.2. Ulanish tarmog‘ini loyihalashtirish

10.3-rasmda xalqaro elektraloqa ittifoqining Y seriyali tavsiyalarida taklif etilgan infokommunikatsiya tizimining modeli keltirilgan. Bu model infokommunikatsion tizimlarda kirish tarmog‘ining o‘rnini aniqlash imkonini beradi.

Abonent xonasidagi qurilmaga misol sifatida oddiy telefon apparati (xonadon sektori) hamda apparat-dasturiy vositalarning murakkab majmuasi – ATS, lokal Ethernet tarmog‘i va boshqa qurilma (ishlab chiqarish sektori) bo‘lishi mumkin.




10.3- rasm. ITU-T tavsiya etgan infokommunikatsiya tizimining modeli

Birinchi holda kirish tarmog‘i vazifalarini ikki simli fizik zanjirni ifodalovchi abonent liniyasi bajarishi mumkin. Ikkinchi holda kirish tarmog‘i tarkibiga (mavjud telekommunikatsiya tizimi uchun) quyidagilar kirishi kerak:

- ATS uzelini mahalliy telefon tarmog‘iga ulash uchun E1raqamli trakt (yoki bir necha shunday traktlar);

- mahalliy tarmoqni Internetga ulash uchun TCP/IP protokollar stekini qo‘llab-quvvatlovchi raqamli trakt;

- ijaraga olinuvchi liniyalar, agar ular telefon tarmog‘i yoki Internetdan foydalanmaydigan qurilmani ulash uchun zarur bo‘lsa.

Kirish tarmog‘ining asosiy vazifasi - operatorning imkoniyatli mijozlarining xonasida o‘rnatilgan barcha turdagi qurilmalar bilan tegishli tranzit tarmoqlar o‘rtasida ishonchli va yuqori sifatli aloqani ta’minlash. Kirish tarmog‘ining muhim xususiyatlaridan biri axborotni yetkazib berish texnologiyasidan uzoq vaqt foydalanishdir.

Kirish tarmog‘i eng katta sig‘imli hisoblanadi, shuning uchun telefon tizimining xech bir elementi kirish tarmog‘i kabi “stagnatsiya” holatida shunchalik uzoq bo‘lmagan.

Yuzaga kelgan vaziyat quyidagi ikki asosiy sabab bilan izohlanadi:

- yaqin vaqtgacha odatdagi (tor oraliqli) kirish tarmoqlarini ancha tejamli holda qurish mumkin bo‘lgan texnik vositalar mavjud emas edi;

- fizik zanjirlar axborot almashuviga bo‘lgan extiyojni (TCh kanalga qaraganda ancha quvvatli resurslarni talab qilmaguniga qadar) ta’minlaydi va yangi xizmatlarning ancha katta qismini qo‘llab-quvvatlaydi.

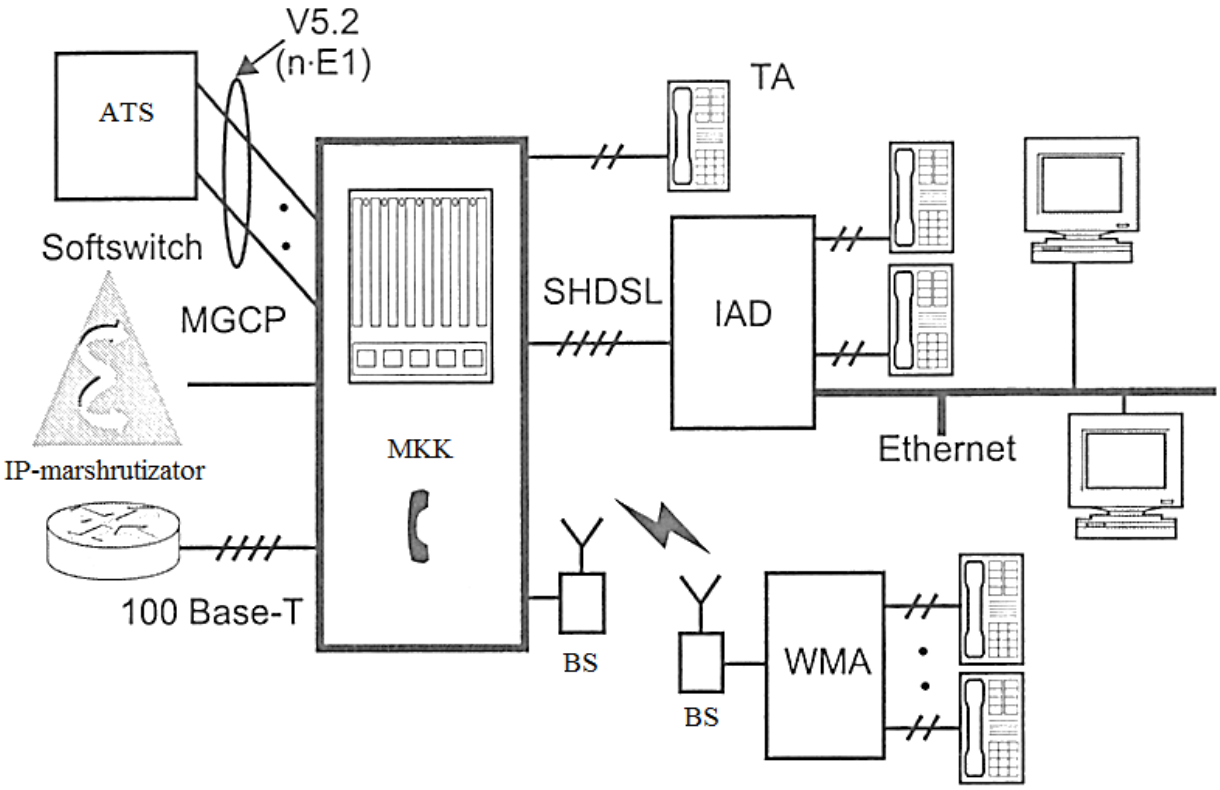
10.4- rasmda quyidagi belgilardan foydalaniladi:

- MGGP (Simple Gateway Control Protocol) - shlyuzni boshqarishni oddiy protokoli bo‘lib, u konsentratorlarni boshqarish, UfTT va boshqa tarmoqlar stansiyalari bilan o‘zaro ta’sirlashish uchun mo‘ljallangan;

- 100 Base-T - uzatish tezligi 100 Mbit/s (802.Zi standarti) bo‘lgan Fast Ethernet fizik sathining tasnifini belgilanishi. Mazkur texnologiyada uzatish muhiti sifatida tolali optik kabeldan foydalaniladi;

- Softwitch - ikki turdagi UfTT va IP tarmoqlar uchun maxsus yaratilgan dasturiy kommutator, bu tarmoqlardan har birida bu qurilma turlicha idrok etadi: UfTTda ishlash uchun Softwitch UKS7 signalizatsiya punkti vazifasini bajarishi va UfTTda signalizatsiyaning boshqa tizimlari (EDSSI, 2BCK, R2 va boshqalar)ni qo‘llab-quvvatlash uchun interfeyslarga ega bo‘lishi kerak. Paketli kommutatsiya

tarmoqlarida Softwitch, transport shlyuzlarini boshqarishning yagona qurilmasi (Media Gateway Controller, MGC) va/yoki signalizatsiya kontrolleri (Signalling Controller SC) H.323 dispetcheri va SIP (Signalling Initial Protocol) serverlari dispetcherisifatida ishtirok etadi;




10.4- rasm.‘‘Protey-MKK’’dan foydalanishni tasvirlovchi sxema

- SHDSL (High-bit-rate Digital Subscriber Line) - to‘rtta simli yuqori tezlikli raqamli abonent liniyasi bo‘lib, u bo‘ylab 2B1Q (ANSI tavsiyalari) turidagi kodlashdan foydalanib oqimni 2, 048 Mbit/s ($Ye_1$) tezlikda uzatish ta’minlanadi;

- LAD (Integrated Access Device) -integratsiyalangan kirish qurilmasi;

- WMA (Wireless Multiple Acess) - simsiz ko‘p martali kirish qurilmasi. WMA qurilmasi konsentrator tomonida E1 standart trakti bo‘yicha yoki abonent komplektlari orqali ulanishi kerak.

- MAK qurilmasi xizmat ko‘rsatilayotgan foydalanuvchilarni bir necha tarmoqqa ulashga imkon beradi;

Infokommunikatsiya xizmatlarining ayrim turlarini ta’minlash uchun dasturiy kommutator Softwitch bilan o‘zaro ta’sirlashish kerak bo‘lib qolishi mumkin. Bu vazifalar media shlyuzni boshqarish uchun mo‘ljallangan protokolni MGCP (Media Gateway Control Protocol) qo‘llashda amalga oshirilishi mumkin.

100 Mbit/s tezlikdagi Fast Ethernet 100 Base-T fizik sathdagi texnologiya EHMning lokal tarmoqlarida qo‘llaniladi. Base atamasi to‘g‘ri (modulyatsiyalanmagan) uzatishni ko‘rsatadi. T belgisi o‘ralgan juftlikdan (Twisted pair) foydalanishni ko‘rsatadi.

## 10.3. Transport tarmog‘ini loyihalashtirish

Infokommunikatsiya tizimi evolyutsiyasining boshlang‘ich bosqichida kanallar kommutatsiyasi bo‘lgan qurilma asosiy o‘rinni egallaydi. Umumiy transport tarmog‘ining asosiy resurslari so‘zlashuv axborotini eltib berish uchun qo‘llaniladi. Paketlar kommutatsiyasi bo‘lgan qurilma umumiy transport tarmog‘i resurslarining kichikroq ulushidan foydalanadi. Kanallar kommutatsiyasi tarmoqlaridan paketlar kommutatsiyasi tarmoqlariga so‘zlashuv axborotlarini uzatish, kompressiyalash va kommutatsiyalash masalalarini hal etish uchun media shlyuzlar o‘rnatiladi.

Transport tarmog‘i resurslarining bir qismi ikkala kommutatsiyalash tarmoqlari (KK va PK) bilan birgalikda qo‘llanilishi kerak. Bu agar ikkala tarmoqda ham soatdagi katta yuklama mos tushmagan holatlarda, o‘ta yuklanishlarni bartaraf etadi.

Infokommunikatsiya tizimi evolyutsiyasining oxiridan bitta oldingi bosqichida multimedia li axborotni eltib berishni ta’minlovchi paketlar kommutatsiyasi bo‘lgan qurilma asosiy o‘rinni egallaydi. Umumiy transport tarmog‘ining asosiy resurslari paketlar kommutatsiyasi rejimida multimedia li axborotlarni transportlash uchun qo‘llaniladi. Kanallar kommutatsiyasi bo‘lgan qurilma endi umumiy transport tarmog‘i resurslarining kamroq ulushidan foydalanadi.

Transport tarmog‘ining o‘tkazish qobliyati katta bo‘lishi kerak, bumultimedia li trafikda video axborotning mavjudligi bilan izohlanadi. Transport tarmog‘i resurslarining bir qismi ikkala kommutatsiyalash tarmoqlari tomonidan birgalikda qo‘llanishda davom ettiriladi.

Telekommunikatsiya tarmoqlarining deyarli barcha operatorlari duch keladigan muammolar o‘rtasida, kirish tarmog‘ini keyingi rivojlanishi uchun ssenariyni tanlash murakkabligini ta’kidlash kerak. Bunday holat juda ko‘p omillarga bog‘liq, ammo infokommunikatsiya xizmatlari bozorida talabni bashorat qilishdagi murakkablikni yetakchi deb hisoblash mumkin. Shuning uchun telekommunikatsiya tarmog‘i operatori uchun bozordagi talabga bog‘liq holda eng kam xarajatlar bilan o‘zgarishi mumkin bo‘lgan, tizimli-tarmoqli yechimlar juda katta amaliy qiziqish uyg‘otadi. Bunday shartlarni ‘‘Protey-MAK’’ga o‘xshash apparat-dasturiy vositalar qanoatlantiradi. Ular operatorlarga texnologiyalarni tanlashga talab qo‘ymaydi va xizmatlarning yangi turlarini kiritish jarayonlarini to‘xtatib qolmaydi.

*Tarmoqlarning o‘zaro ta’siri.*

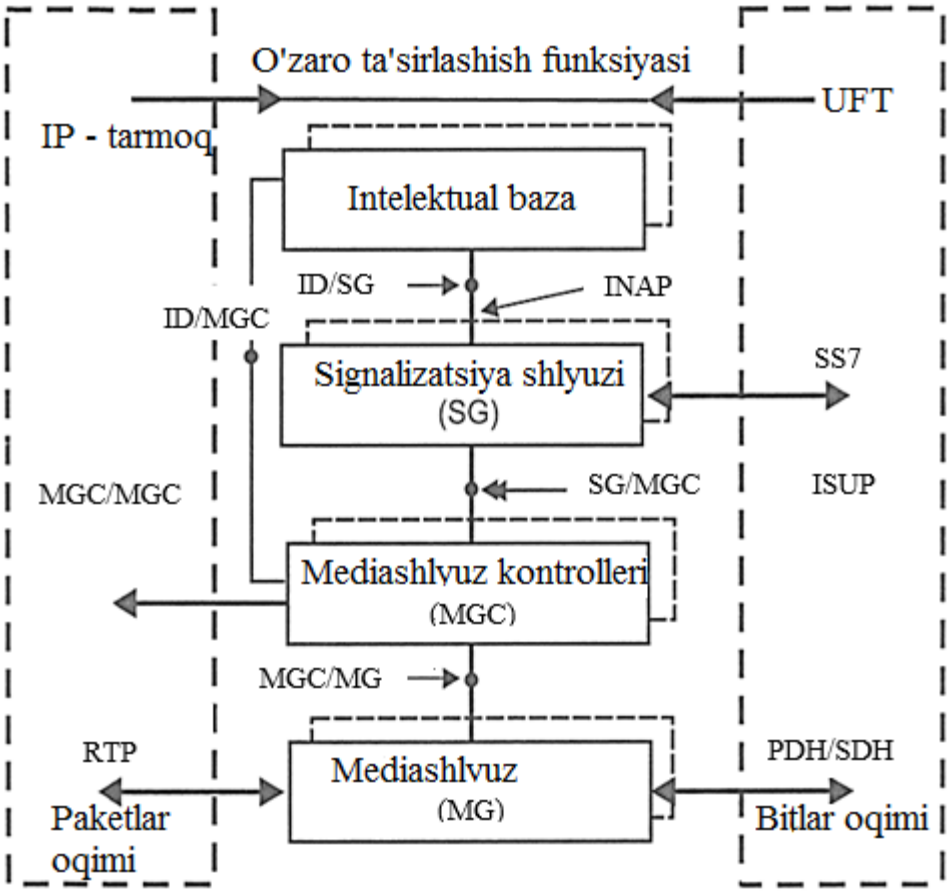
NGNning fizik arxitekturasi uchta sathni (platformani) o‘z ichiga olgan bo‘lib, ular orasida standart interfeyslar qo‘llaniladi, bu esa masshtablashtirishni, yetkazib beruvchilarga bog‘liq bo‘lmaslikni, investitsiyalarni saqlanishini va aloqa operatori uchun foydali bo‘lgan boshqa juda ko‘p xossalarning saqlab qolinishini ta’minlashga imkon beradi.

Keyingi avlod tarmog‘ining fizik arxitekturasi (8.5-rasm) o‘z ichiga quyidagilarni qamrab oladi:

- transport platformasi;

- yangi dasturiy-apparat majmualari negizida amalga oshiriluvchi boshqarish va signalizatsiya platformasi;

- zarur xizmatlar to‘plamini ta’minlovchi serverlar platformasi.




10.5- rasm. NGN arxitekturasi (Recommendation ITU-T Y.1001)

**Transport platformasi** quyidagi sathlarni o‘z ichiga oladi:

- transport tarmog‘i yadrosi sathi (Core Network, CN), multiservisli transport tarmoqlari texnologiyalari negizida amalga oshiriladigan (hozirgi vaqtda eng ko‘p ishlab chiqilgan ATM, IP/MPLS/all, IP/VLAN/Ethernet texnologiyalari);

- kirish tarmoqlari sathi (Access Network, AN), hozirgi vaqtda eng ko‘p tarqalgan kirish texnologiyalari quyidagilar hisoblanadi: xDSL, FTTH, Wi-Fi, Wi-Max, PON. ANda qo‘llaniladigan texnologiyalarning xilma-xilligi quyidagi holatlar tufayli yuzaga kelgan:

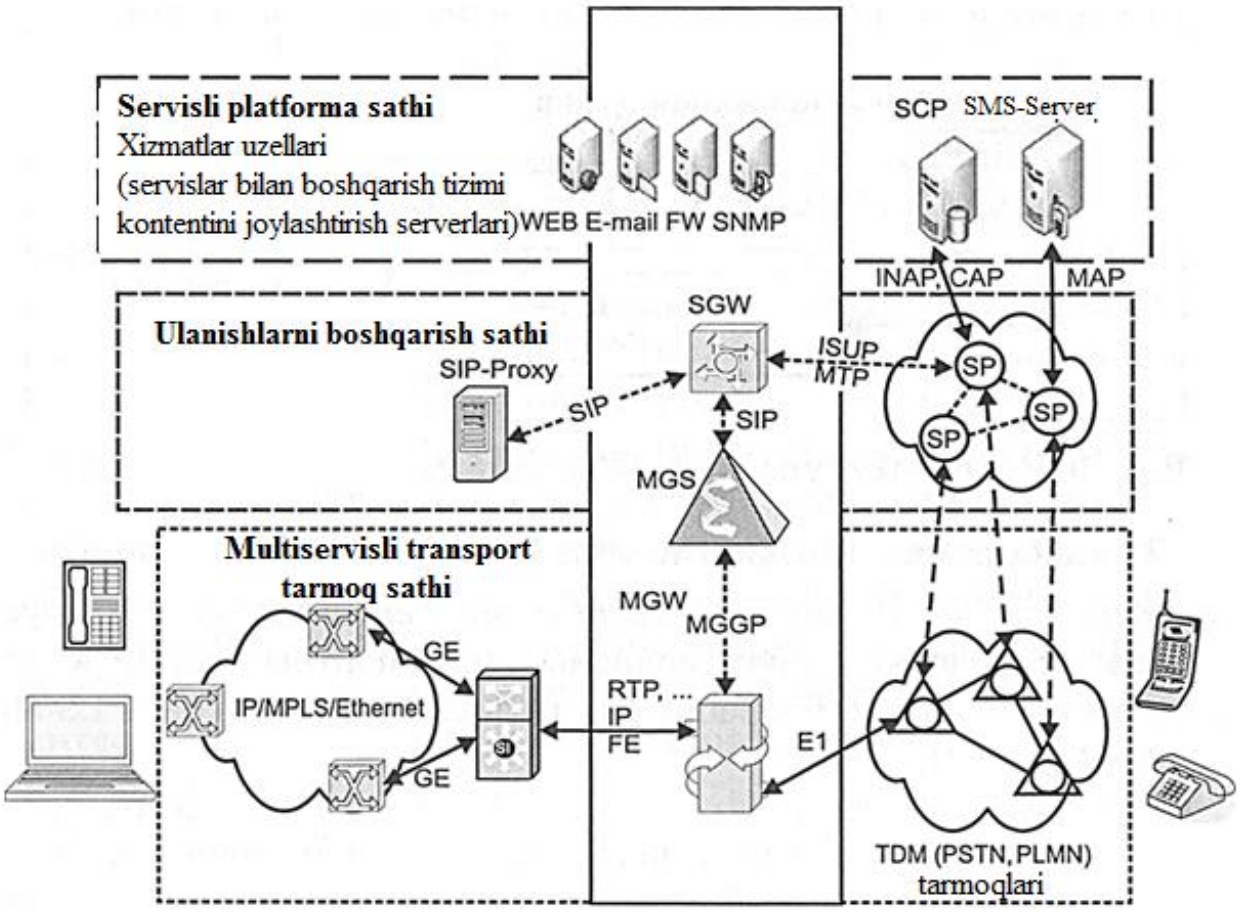
- qo‘llaniladigan uzatish muhitlarining xilma-xilligi bilan (ham yangi, masalan optik, avval kirish tarmoqlarida qo‘llanilmagan ham eski, masalan ko‘p juftlikli telefon kabellari va tor oraliqli simsiz kirish tizimlari);

-terminallar turlarining xilma-xilligi bilan (avvalgi sodda lekin arzon telefon apparatlaridan to barcha xizmatlarni ta’minlovchi ko‘p funksionalli terminallargacha).

**Boshqarish va signalizatsiya platformasi** yangi dasturiy-apparat majmualari negizida amalga oshirilib ularga Softwitch nomi (kommutatsiyani boshqarishning moslashuvchan tizimi) biriktirilgan.

**Serverlar platformasi** zarur bo‘lgan xizmatlar to‘plamini ta’minlaydi.

Hozirgi vaqtda bu platformalar orasidagi o‘zaro ta’sirni moslashuvchan holda sozlashga imkon beruvchi universal ochiq interfeyslar ishlab chiqilgan. 10.6-rasmda transport tarmoqlarning o‘zaro ta’sirlashishni tashkil etish sxemasi keltirilgan.




10.6-rasm. Tarmoqlarning o‘zaro ta’sirlashishini tashkil etish sxemasi

Mavjud tarmoqlarning (PSTN va PLMN) o‘zaro ta’sirlashishi uchun resurslarni MGW shlyuzi taqdim etadi. Chaqiriqlarga ishlov berish jarayonida signalizatsiya protokollarining konvertatsiyasi SGW signalizatsiya shlyuzi tomonidan amalga oshiriladi. Shlyuzlarni boshqarish uchun MGS kontrollerlaridan foydalaniladi.

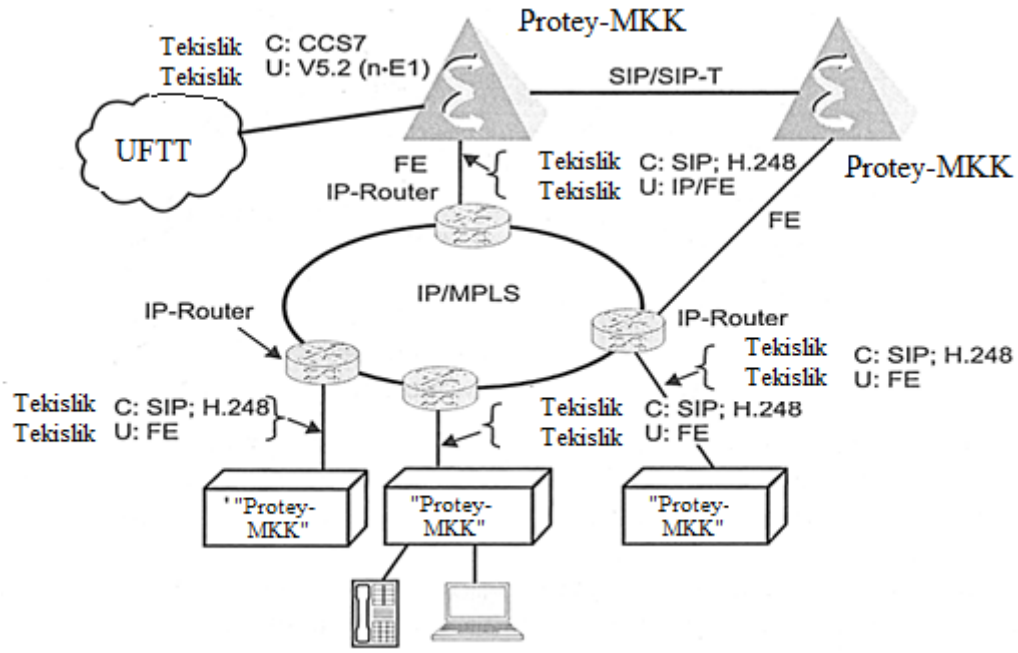
Dastlab N.323 tasnifi mahalliy tarmoqlarda videokonferensiyalarni ta’minlash maqsadida ishlab chiqarilgan edi. Foydalanuvchilararo yoki bir rangli (peer-to-peer) protokolni qo‘llab, intellektual terminalli mijozlar intellektual terminaldan foydalanuvchi boshqa mijozlar bilan ulanishni o‘rnatishlari mumkin edi.

N.323 ning keyingi versiyalari Gatekeeper Routed Model ni na’zarda tutar edi, unga muvofiq (Gatekeeper) barcha ulanishlarni o‘rnatishda va har bir chaqiriq uchun xizmatlar taqdim etishda faol ishtirok etishi kerak edi. Bunday modelda N.323 bir rangli protokol hisoblanmaydi. Shlyuz o‘ziga ko‘pgina an’anaviy xizmatlarni markazlashtirilgan holda taqdim etishni intellektual vazifalarini oladi.

Multiservisli tarmoq ilmiy tadqiqot markazini “Protey” (10.7-rasm) qurilmasini qo‘llab qurilishi mumkin.

“Protey-MKK” multiservisli kirish kommutatori (MKK), UfTTda aloqa xizmatlarini taqdim etish uchun mo‘ljallangan dasturiy-apparat majmuini ifodalaydi. Uning negizida shuningdek korporativ tarmoqlarni yaratish va ofislarda aloqani tashkil etish mumkin. Multiservisli kirish kommutatori multiservisli aloqa tarmoqlarida Softswich vazifasini bajaradi, ya’ni paketli tarmoqda so‘zlashuv va multimedia li axborot almashinuvini ta’minlaydi.

Multiservisli tarmoqlarda “Protey-MKK” Ethernet 100 Mbit/s interfeysi bo‘yicha transport IP-tarmog‘i bilan o‘zaro ta’sirlashadi va NGN uzellari bilan o‘zaro ta’sirlashishi uchun SIP, H.248/MEGASO signalizatsiya protokollaridan foydalaniladi. 10.8-rasmda “Protey-MKK”ni qo‘llanishning mumkin bo‘lgan variantlari keltirilgan.

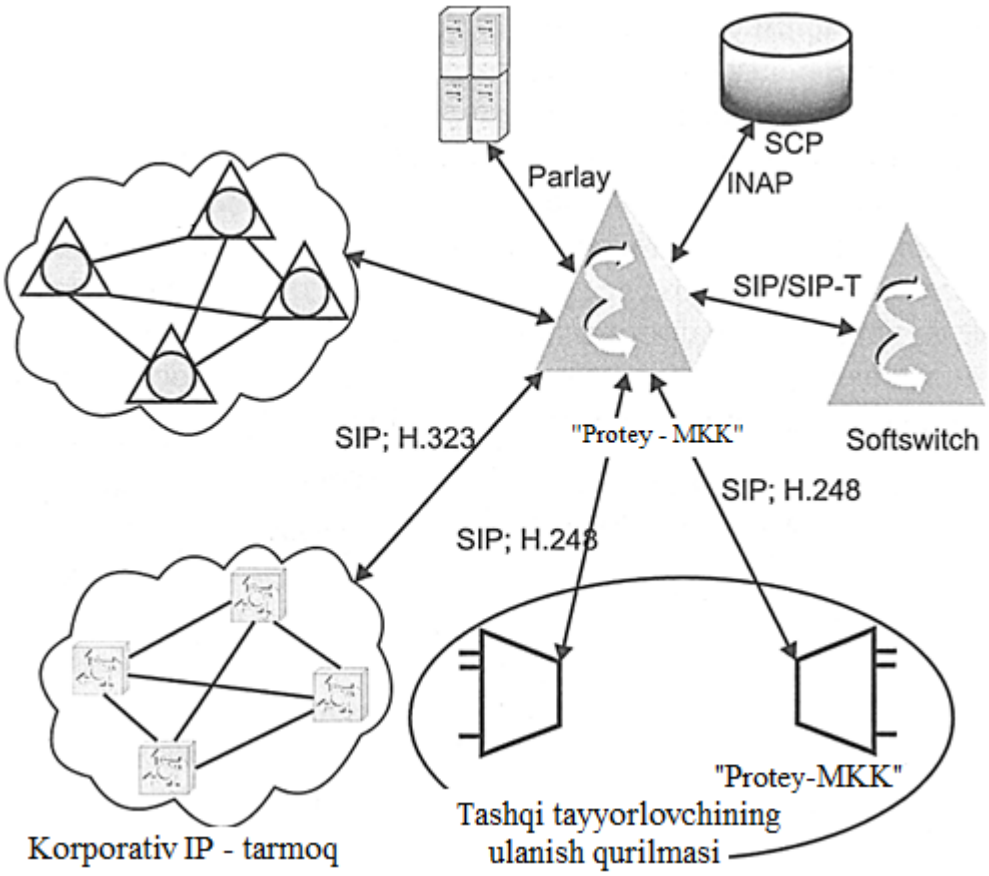



10.7-rasm. “Protey” ITM qurilmasi yordamida qurilgan multiservisli tarmoq sxemasi

“Protey-MKK”ning bitta tizimi negizida sig‘imi 25 ming raqamli telefon tarmog‘ini tashkil etish mumkin. Tarmoqni kengaytirish, chaqiriqlarga ishlov berishning qo‘shimcha modullarini (Call Processing Subsequent, CPS) o‘rnatish yordamida amalga oshirish mumkin.

“Protey-MKK” multiservisli kirish kommutatori quyidagi turdagi qurilmalar bilan o‘zaro ta’sirlashishi mumkin:

- E1interfeyslari bo‘yicha UfTT /IN bilan;
- E-DSSI; OKS 8 R1/5 protokollar bo‘yicha ATS uzellari, raqamli telefon stansiyalar;
- E-DSSI protokolli bo‘yicha kirish qurilmasi;
- “Protey-MAK” multiservisli abonent kirish konsentratori;
- INAP-R protokoli bo‘yicha xizmatlarni boshqarish uzellari (SCP);
- Ethernet 100/1000 Mbit/s interfeyslar bo‘yicha paketli kommutatsiyali tarmoqlar bilan;




10.8- rasm. “Protey-MKK”ning qo‘llanilish variantlari

- SIP/SIP-T, H.248/MEGACO protokollari bo‘yicha Softwitch bilan;

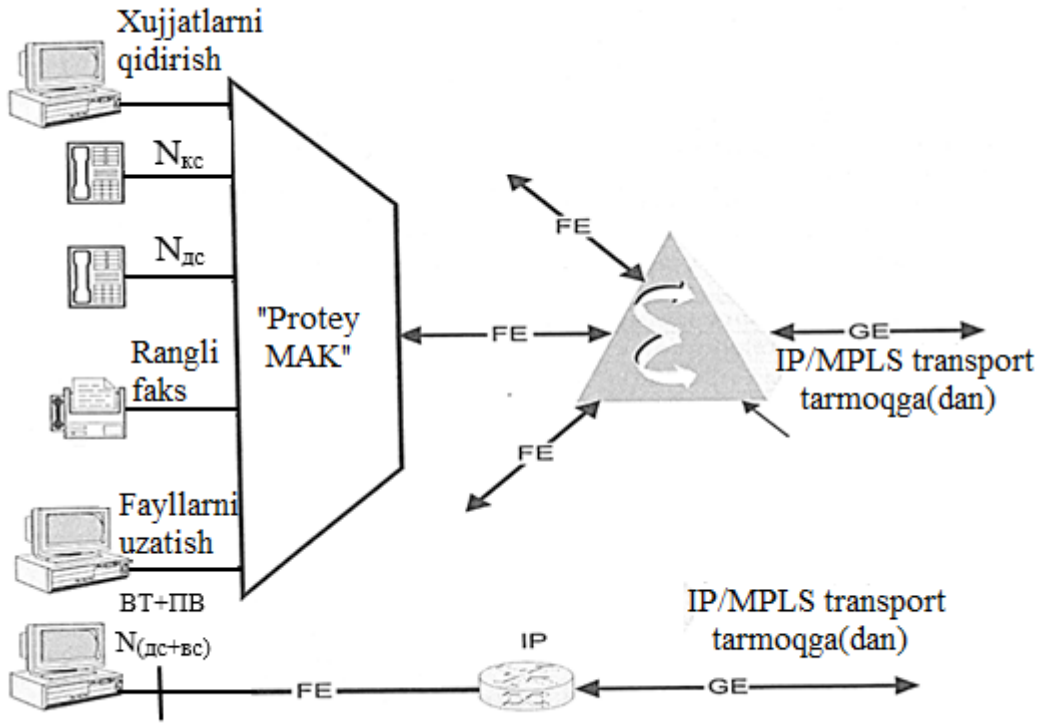
- multiservisli kirish qurilmasi bilan, shu jumladan SIP/SIP-T, H.248/MEGACO protokollari bo‘yicha “Protey-MAK” multiservisli abonent konsentratori bilan;

- SIP protokoli bo‘yicha proksi serverlar va boshqa SIP-domenlari uzellari bilan;

- Parlay API amaliy dasturlash tizimi yordamida ilovalarning serverlari bilan;

- IP-telefonlar, IP-telefoniya shlyuzlari bilan (shu jumladan “Protey-ITG” IP-telefoniya shlyuzlari bilan);

10.9-rasmda “Protey” firmasining dasturiy-apparat vositalaridan foydalaniladigan multiservisli tarmoq na’munasi keltirilgan.




10.9 rasm. Telefoniya foydalanuvchilari, xujjatlarni izlash, rangli faks, fayllarni uzatish, videotelefoniya, videoni izlash uchun kirish tarmog‘ining tuzilish sxemasi

## Nazorat savollari

1. Telekommunikatsiya tarmoqlarini loyihalashtirish uchun qanday loyihalashtirish xujjatlar tarkibi kerak?
2. Paketli tarmoqlarda multimedia li axborotlarni yetkazishni qanday asosiy sifat ko‘rsatkichlari bor?
3. Multimedia li tarmoqni loyihalashtirish nechta bosqichdan iborat?

4. Loyihalashtirilayotgan tarmoq uzellariga xizmat ko‘rsatish uchun zarur bo‘lgan yuklamani baholash uchun qanday ma’lumotlar kerak bo‘ladi?
5. Transport tarmoqni loyihalashtirishni tushuntiring.
6. Transport tarmog‘i yadrosi sathini vazifasi nimadan iborat?
7. Multimedia li tarmoqni loyihalashtirishning 2-bosqichida qanday ishlar amalga oshiriladi?
8. Multimedia li tarmoqni loyihalashtirishning 3-bosqichida qanday ishlar amalga oshiriladi?
9. Softswitch nima?
10. Ulanish tarmog‘ini loyihalashtirish bosqichlarini tushuntiring.

# 11. MULTISERVISLI ALOQA TARMOQLARINING AXBOROT XAVFSIZLIGINI TA’MINLASH

Zamonaviy multiservisli aloqa tarmoqlarini rivojlanishi, birinchi navbatda ularni inson xayot faoliyatini barcha jabhalariga kirishi va globallashishi bilan tavsiflanadi. Bunga misol sifatida – Internet. Biroq, Internet tarmoqlari noyob yangilik va “butun dunyo axborotini tashuvchi” hisoblanib, shaxsga, davlatga va jamiyatga alohida va o‘ziga xos tahdidlarning yangi to‘plamini o‘zining foydalanuvchilariga (axborot xizmatlaridan foydalanuvchilarga) taqdim etdi. Jarayonni bunday rivojlanishi multiservisli aloqa tarmoqlarida, shuningdek Internet tarmoqlarida axborotni himoyalash muammolarini keskinlashtirdi. Bundan tashqari, multiservisli aloqa tarmoqlarining axborot xavfsizligini (AX) ta’minlash bo‘yicha vositalar va takliflarning ko‘pligi, ishlab chiqaruvchilarni axborot xavfsizligi arxitekturasini yaratishga olib keldi.

## 11.1. Axborot xavfsizligini ta’minlash zarurati

Multiservisli aloqa tarmoqlarini yaratishda, axborot uzatishni turli vositalarini qo‘llab va turli abonent terminallari yordamida yuqori sifatli axborot almashishni ta’minlovchi funksiyalarning zarur to‘plamini kiritadi. Axborot almashishni tashkil etishda xatoliklar yuz berishi ehtimoli mavjud, ularning yuzaga kelishi butun tarmoqni va aloxida tarmoqni dasturiy-qurilmali komplekslarini ishlashining samaradorligi, shuningdek aloqa kanallaridagi (liniyalardagi) halaqitli muhit sabab bo‘ladi. Ushbu bo‘limda bunday xatoliklardan himoyalanish choralari ko‘rib

chiqilmaydi. Lekin, bugungi kunda multiservisli aloqa tarmoqlarining funksional xatoliklari ostiga yashiringan, faol xujum usullari mavjud.

Butun dunyo tarixi shuni ko‘rsatadiki, turli axborotlarni izlash bo‘yicha josuslik faoliyati har qanday davlat siyosatining “asosiy asosi” hisoblanadi. Insonni bilib bo‘lmaydi, bir tomondan - atrof muhit uni, aniq shaxslar tomonidan kirish chegaralangan maxfiy axborotni izlashga jalb etishi mumkin. Boshqa tomondan – har qanday maxfiy axborotning egasi uni begonalar xavfidan saqlashni xoxlaydi. Aynan multiservisli aloqa tarmoqlarini ishlashida va foydalanishda inson omilining mavjudligi, ochiq tizimlar uchun standart vazifalar to‘plamini to‘ldirish zaruratini yuzaga keltiradi, ya’ni multiservisli aloqa tarmoqlarining xavfsizligini ta’minlash vazifasi.

Elektron kommunikatsiya insonlarni yaqinlashtiradi: vaqt va masofa yo‘qoladi. Ya’ni, xalqaro Internet Yerning millionlab aholisini birlashtiradi va juda katta axborotlar soniga ishlov beradi. Shuning uchun Internet, kompyuter josusi sohasidagi mutaxassislar uchun “faoliyat yuritishning keng maydoni” hisoblanadi.

Internet axborotni himoyalash bo‘yicha keng xizmatlar spektrini taqdim etadi. Internet foydalanuvchilari uchun shuni bilish zarurki, AQShda davlat Prezidentining “Jamiyatda shifrlashni boshqarish” (Public Encryption Management) direktivasi mavjud bo‘lib, chiqariluvchi (davlatdan tashqariga) axborotlarni himoyalashni kriptografik vositalari AQShni elektron razvedka tashkilotlari uchun axborotlarni izlashga to‘siq bo‘lmasligi kerak. Ya’ni, Internetda qo‘llaniladigan axborotni himoyalashning har qanday dasturiy va qurilmali vositalari, AQShning maxsus xizmatlari uchun “shaffof” hisoblanadi.

## 11.2. Axborot xavfsizligiga tahdidni amalga oshirish oqibatlariva manbalari

Ko‘pgina rasmiy tashkilotlar tomonidan taklif etiladigan va tavsiya etiladigan multiservisli aloqa tarmoqlarining axborot xavfsizligiga tahdidning zamonaviy modellari, buzg‘unchining xulqini modellashtirish asosida tuzilgan, shuning uchun g‘oyat ulkan va eng asosiysi – o‘xshash emas.

Tahdidlarni va buzg‘unchining xulqini xaddan tashqari batafsil tekshirish yechiladigan masaladan “tashqariga ketish” mumkin. Ya’ni, xech kim oldindan buzg‘unchining xatti-harakatini bashorat eta olmaydi. Bundan tashqari, ko‘pgina xollarda shunday bo‘ladiki, buzg‘unchi qonunga qarshi ish qilmagan inson bo‘lishi mumkin.

Tahdidlar - turlanishi, o‘zgarishi va yangilanishi mumkin, bunday tahdidlar asosida xulqi oldindan aytib bo‘lmaydigan inson yotadi, lekin ularni amalga oshirish va natijaga erishish nuqtai nazaridan, ularning barchasini guruhlarga (turlar) birlashtirish mumkin bo‘lgan oqibatlarga olib keladi.

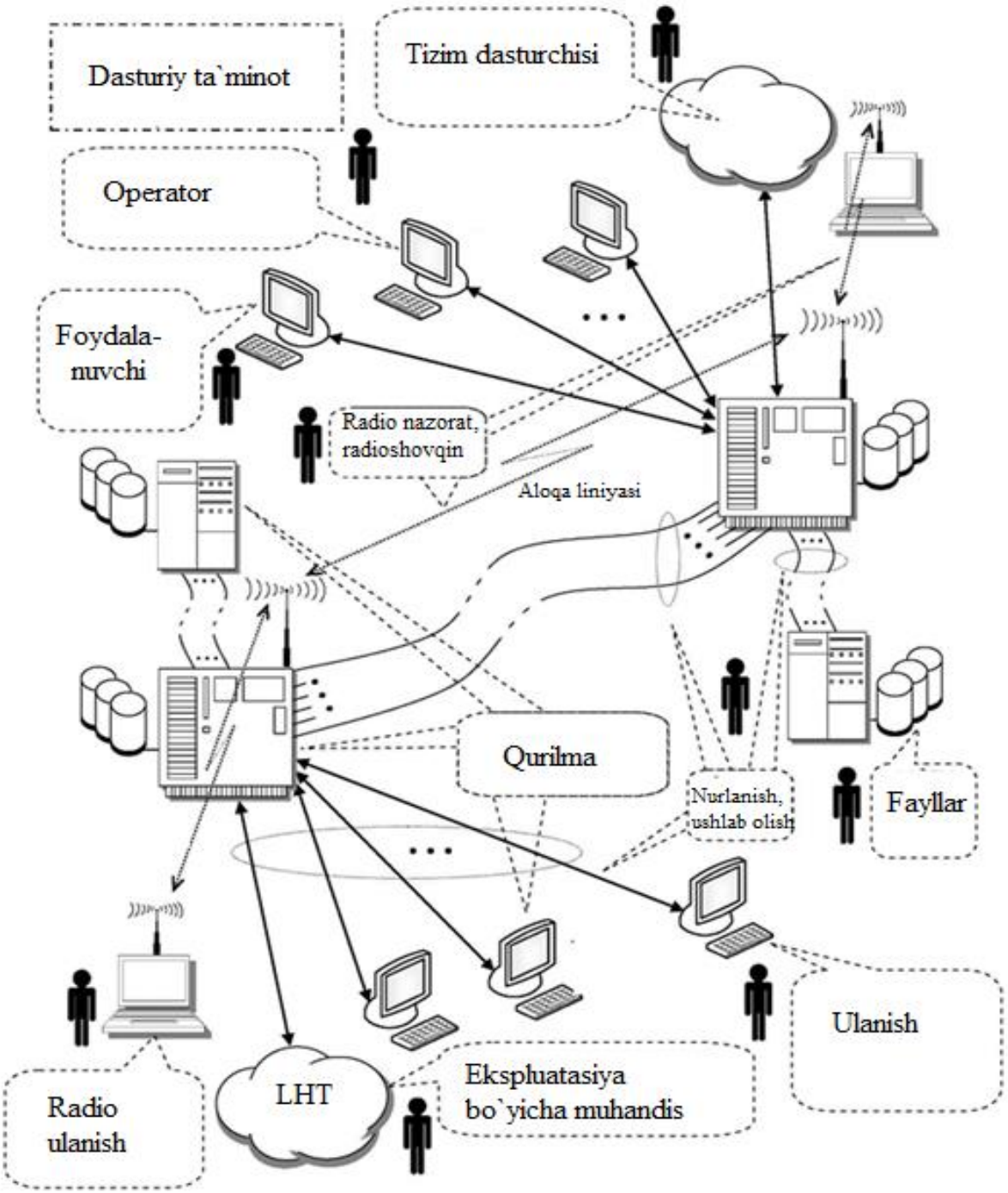
Internet da axborot xavfsizligi muammolari bilan shug‘ullanuvchi mutaxassislar tahdidlar oqibatini to‘rtta turini aniqlashgan: ochish, aldash, buzish, qo‘lga olish (tortib olish). Tahdidlarning ta’sir etish oqibati ITS tizimi xafvsizligining buzilishi hisoblanadi (11.1-rasm). Bu tahdidlar oqibatini, shuningdek ITS xavfsizlik tizimini obro‘sizlanishiga sabab hisoblanadigan turli tahdidlar ta’sirining ro‘yxati va mohiyatini ko‘rib chiqamiz. Tahdidiy harakat, tasodifiy xodisa (tabiy xodisa) natijasi hisoblanadi.

***A.*** “Ochish” (unauthorized disclosure): vaziyat yoki hodisa yordamida sub’ekt kirish mumkin bo‘lmagan qo‘riqlanadigan ma’lumotlarga (maxfiy) kiradi. Keyingi xavfli harakat ruxsatsiz ochishga sabab bo‘lishi mumkin:

1. “Fosh qilish” (exposure): Xavfli harakat tufayli qo‘riqlanadigan ma’lumotlar bevosita su’ektga ma’lum bo‘ladi. U quyidagilardan iborat:

1.1. “G‘arazli fosh qiluvchi” (deliberate exposure): Sub’ektni qo‘riqlanadigan ma’lumotlarga atayin kirishi. Xavfli harakatning bu turi, vijdonsiz qonuniy sub’ektning harakatiga asoslangan, ya’ni g‘arazli yoki jinoiy maqsadlarda boshqa

sub’ektga qo‘riqlanadigan ma’lumotlarga ega bo‘lishga ruxsat beradi. Bu inson omilining manfiy ta’siri. Bunday buzg‘unchiliklar bilan kurashish, maxsus tashkillashtirilgan - oldindan aytish va “chetlatishni” aniqlash bo‘yicha texnik tadbirlarni o‘tkazish taxmin qilinadi.




11.1-rasm. Multiservisli aloqa tarmoqlarida xavfsizlikka tahdid manbalari

1.2. “Ma’lumotlar qolganini ko‘rish” (scavenging): Qo‘riqlanadigan ma’lumotlarni ruxsatsiz olish maqsadida, tizimda qolgan kirish mumkin bo‘lgan ma’lumotlarni tadqiq etish. Quyidagi tahdid etish turi kerak bo‘lmagan ma’lumotlarni (fayllarni) yo‘q qilish bo‘yicha dasturiy ta’minot xususiyatiga asoslangan, qo‘riqlanadigan ma’lumotlarni yo‘q qilishda, faqatgina ular saqlangan fayl va katalogning nomlanishi o‘zgaradi (modifikatsiyalanadi). Bunday xolatda bu muammoni yechishni ikkita yo‘li mavjud: ma’lumotlarni shifrlangan ko‘rinishda saqlash (shifrlangan ma’lumotlarni yo‘q qilish); faqatgina fayl va kataloglarning sarlavhasini emas, balki barcha yo‘q qilinadigan ma’lumotlarni modifikatsiyalash bo‘yicha maxsus dasturlarni qo‘llash.

1.3. “Insonning xatosi” (human error): Sub’ekt tomonidan qo‘riqlanadigan ma’lumotlarni ruxsatsiz bilishnibeixtiyor o‘z ortidan tortadigan, insonning harakati yoki harakatsizlik faoliyati. Tahdidlarning bu manbai sub’ektning qonuniy xuquqlilik faoliyati bilan bog‘liq (inson omili). U ehtimoliy mohiyatga ega va ataylab qilingan harakat (harakatsiz) hisoblanmaydi. Bunday xolatlarda tizimning o‘zi bunday xatoliklardan himoyalanishning qo‘shimcha (intellektual) me’yorlarini ko‘rib chiqishi kerak.

1.4. “Dasturiy-qurilma xatosi” (hardware/software error): Sub’ekt tomonidan qo‘riqlanadigan ma’lumotlarni ruxsatsiz bilishni beixtiyor o‘z ortidan tortadigan, tizim xatoligi. Xatolikning bu turi, tasodifiylik ko‘rinishi ostida oldindan o‘ylab qo‘yilgan bo‘lishi yoki tasodifiy tabiatga ega bo‘luvchi, dasturiy-qurilma moslamalardagi noshtatli xolatlar bilan bog‘liq. Bunday turdagi ta’sirlarning halokatli oqibatlarini bartaraf etish uchun tizim avtomatik ravishda o‘zining faoliyatini (barcha tizimli va amaliy jarayonlarni to‘xtatish) to‘xtatishi va “kutish” rejimiga o‘tishi kerak.

***A.2.*** “Qo‘lga olish” (interception): Muxtor xuquqli manba va qabul qiluvchi o‘rtasida aylanadigan, qo‘riqlanadigan ma’lumotlarga bevosita ruxsatsiz ulanishga ega bo‘lgan sub’ekt vositasidagi tahdidli harakat. U quyidagilardan iborat:

2.1. “O‘g‘irlik” (theft): Fizik mohiyatiga bog‘liq bo‘lmagan holda, turli axborot to‘plovchilarni o‘g‘rilash yo‘li bilan qo‘riqlanadigan ma’lumotlarga kirishga erishish (masalan, magnit lentali kassetalar yoki magnit disklar va boshqalar). Bunday buzg‘unchiliklar bilan kurashish, prognozlash, “buzg‘unchini” aniqlash va qo‘riqlanadigan ma’lumotlar tushuvchini fizik himoyalash bo‘yicha maxsus tashkiliy-texnik tadbirlarni o‘tkazish talab etiladi.

2.2. “Eshitish” (passiv, wiretapping/passive): MATda ikkita terminal orasida aylanadigan ma’lumotlarni aniqlash va yozib olish. Bu turdagi buzg‘unchilikning mohiyati, uzatiladigan signallarga erkin ruxsatsiz ulanishning mavjudligi bilan bog‘liq. Ma’lumotlarni himoyalashning asosiy usullari, bu ma’lumotlarni niqoblash (shifrlash) hisoblanadi.

2.3. “Nurlanish tahlili” (emanations analysis): Xabarlarni uzatish uchun mo‘ljallanmagan, “ko‘chiriladigan” ma’lumotlar va tizim nurlantiradigan signalni aniqlash va ishlov berish yo‘li orqali, aloqa tizimida uzatiladigan xabarlarning ma’nosini bevosita olish. Bu turdagi buzg‘unchilikning mohiyati, uzatiladigan signallarga ruxsatsiz kirish manbai hisoblanadigan va ikkinchi darajali elektromagnit nurlanishlarning mavjudligi bilan bog‘liq. Ma’lumotlarni himoyalashning asosiy usullari, bu ma’lumotlarni shifrlash va zararli nurlanishlar sathini pasaytirish, shuningdek turli shovqin generatsiyalovchi texnik majmualarni qo‘llash hisoblanadi.

***A.3.*** “Xulosa chiqarish” (inference): Sub’ekt, aloqa tizimini “yordamchi mahsulotlari” yoki xarakteristikalarini anglash yo‘li orqali qo‘riqlanadigan ma’lumotlarga (uzatilgan xabarlardagi mavjud ma’lumotlargagini emas) ruxsatsiz ulanishga erishish vositasi asosidagi tahdidli harakat. U quyidagilardan iborat:

3.1. “Trafik tahlili” (traffic analysis): Ma’lumotlar uzatuvchi aloqa tizimi xarakteristikalarini o‘zgarishini kuzatish yo‘li bilan qo‘riqlanadigan ma’lumotlarni

bilishga erishish. Bu tahdidli harakatning mohiyati uzatiladigan trafikning xarakteristikasi va xususiyatlarini aniqlashdan iborat, ya’ni tahlil qilishda qo‘riqlanadigan ma’lumotlarga ruxsatsiz ulanish ta’minlanadi. Bunday tahdidlarni oldini olish uchun trafikni majburiy to‘ldirish va axborotni shifrlashni qo‘llash zarur.

3.2. “Signallar tahlili” (signals analysis): Xabarlarni uzatish uchun mo‘ljallanmagan, “ko‘chiriladigan” ma’lumotlar va tizim nurlantiradigan signalni aniqlash va tahlil qilish yo‘li orqali, aloqa tizimida uzatiladigan qo‘riqlanadigan ma’lumotlarni bilishga noqonuniy erishish. Bu turdagi tahdidli harakatning mohiyati, tarmoqni (tizimni) to‘liq ishlashini xarakteristikalari va xususiyatlarini aniqlashdan iborat, ya’ni qo‘riqlanadigan ma’lumotlarga ruxsatsiz ulanishni ta’minlaydi. Bunday tahdidlarning oldini olish uchun ma’lumotlarni himoyalashni bir necha vositalari va usullari qo‘llaniladigan kompleks yechimlarni, shu jumladan tashkiliy-texnik tadbirlarni qo‘llash zarur.

***A.4.*** “Bostirib kirish” (intrusion): Tahdidli harakat, sub’ekt tizimning xavfsizligini ta’minlash vositasini aldash yo‘li orqali qo‘riqlanadigan ma’lumotlarga ruxsatsiz ulanishni ta’minlaydi. U quyidagilardan iborat:

4.1. “Tajovuskorlik” (trespass): Axborotlarni himoyalovchi tizimli vositalarni aldash yo‘li bilan qo‘riqlanadigan ma’lumotlarga ruxsatsiz fizik ulanishga erishish. Bu taxdidli harakat turining maqsadi shundaki, buzg‘unchini (tashkiliy-texnik himoya vositalarini bartaraf qilish) qo‘riqlanadigan ma’lumotlarga ruxsatsiz ulanishidir. Buni bartaraf etish uchun qo‘riqlanadigan ma’lumotlarni tashuvchilarni va ob’ektlarni fizik himoyalash bo‘yicha maxsus tashkiliy-texnik tadbirlarni kuchaytirish zarur.

4.2. “Kirish” (penetration): Axborotlarni himoyalash tizimli vositalarni aldash yo‘li bilan qo‘riqlanadigan ma’lumotlarga ruxsatsiz logik ulanishga erishish. Bu xolatda buzg‘unchini axborotlarni himoyalashning parolli va shunga o‘xshash tizimini (kriptografik) buzish haqida so‘z boradi. Bunday buzg‘unchilikni bartaraf

etish uchun ruxsatsiz ulanishlardan yanada ishonchliroq himoyalash tizimlarini qo‘llash zarur

4.3. “Rekonstruksiya” (reverse engineering): Tizimli komponentning konstruksiyalarini taxlil qilish va dekompozitlash yo‘li bilan qo‘riqlanadigan ma’lumotlarni qo‘lga kiritish. Bunday buzg‘unchilik vakolatsiz sub’ektni “bo‘lakli” ma’lumotlarni olish yordamida qo‘riqlanadigan ma’lumotlarni qayta tiklash imkoniyati bilan bog‘liq. Bunday xolatni bartaraf etish uchun maxsus tashkiliy-texnik tadbirlarni kuchaytirish va axborotlarni himoyalashni “puxta” kriptografik vositalarini qo‘llash lozim.

4.4. “Kriptotaxlil” (cryptanalysis): Shifrlash jarayonlarining algoritmi va parametrlari haqidagi tekshirilmagan bilimlarsiz shifrlangan ma’lumotlarni ochiq matnga o‘zgartirish. Bu ko‘rinishdagi taxdid bilan kurashish uchun axborotlarni himoyalashni “puxta” kriptografik usullari va vositalarini qo‘llash zarur.

***V.*** “Yolg‘on” (deception): Vakolatli sub’ektdan buzilgan ma’lumotlarni to‘g‘ri sifatida qabul qilish xolati. Keyingi tahdidli harakat o‘zidan keyin quyidagi yolg‘onlarni olib keladi:

1. “Niqoblanish” (masquerade): Taxdidli harakat, sub’ekt vakolatli sub’ekt sifatida tizimga ruxsatsiz ulanishni oladi yoki buzuq niyatli harakatini amalga oshiradi.

1.1. “Aldash” (spoof): Sub’ektni vakolatli foydalanuvchi sifatida tizimga ruxsatsiz ulanishni amalga oshirishga urinishi. Bu kompyuter buzg‘unchiligining juda xavfli va o‘tkir ko‘rinishi hisoblanadi, u bilan kurashish uchun sub’ektning haqiqiy ligini tekshirish vositalari va ko‘p sathli quyidagi usullarini qo‘llash zarur: autentifikatsiyalash, turli kriptografik usullar va vositalar, avtorizatsiya, uchinchi shaxsni tasdiqlash va boshqa choralar.

1.2. “Buzg‘unchilik harakatlar uchun qurilma” (malicious logic): “Niqoblanish” nuqtai nazaridan, go‘yoki tizimni ishonchli va samarali ishlashi uchun mo‘ljallangan har qanday dasturiy-apparat qurilma yoki dasturiy ta’minot (masalan,

“troyan oti”), xaqiqatdan esa tizimli resurslarga ruxsatsiz ulanishni ta’minlaydi yoki boshqa buzuq niyatli ishni bajarish yo‘li bilan foydalanuvchini aldaydi.

2. “Soxtalashtirish” (falsification): Buzilgan ma’lumotlar orqali vakolatli sub’ektni adashtiradigan tahdidli harakat.

2.1. “Almashtirib qo‘yish” (substitution): Vakolatli sub’ektni aldash uchun xizmat qiladigan o‘zgartirishlar kiritish yoki haqiqiy ma’lumotlarni buzilgan ma’lumotlarga almashtirib qo‘yish. Bunday turdagi buzg‘unchiliklardan himoyalanish uchun axborotlarning yaxlitligini ta’minlash, ya’ni ma’lumotlarni istalgan ularni o‘zgartirilishidan himoyalay oladigan kriptografik usullar va vositalardan foydalanish zarur.

2.2. “Qo‘yilma” (insertion): Vakolatli sub’ektni aldash uchun xizmat qiladigan buzilgan ma’lumotlarni qo‘shish. Bunday turdagi buzg‘unchiliklardan himoyalanish uchun ma’lumotlarning yaxlitligini ta’minlash, ya’ni ma’lumotlarni istalgan ularni o‘zgartirilishidan himoyalay oladigan kriptografik usullar va vositalardan foydalanish zarur.

3. “Rad etish” (repudiation): Sub’ekt boshqa sub’ektni o‘zini qandaydir harakatiga ma’suliyatini soxta rad etish yo‘li bilan aldaydigan tahdidli harakatlar.

3.1. “Manbaning soxta rad etishi” (false denial of origin): Ma’lumotlar egasi bu ma’lumotlarga mualliflikka o‘zini ma’suliyatini rad etadigan harakat. Bunday turdagi buzg‘unchiliklardan himoyalanish uchun uchinchi o‘zaro ishonchli yuridik shaxs maxsuslashtirilgan apparat-dasturiy kompleksida (aloqa tugunida) axborot almashinuvi tartiblari ro‘yxatga olinishi (barcha xabarlardan nusxa ko‘chirilishi) bilan birga ma’lumotlarni yaxlitligini ta’minlashni kriptografik usullari va vositalaridan foydalanish zarur.

3.2. “Oluvchining soxta rad etishi” (false denial of receipt): Ma’lumotlarni oluvchi ularni olishni va ularga ega bo‘lishni rad etishi orqali harakati. Bunday turdagi buzg‘unchiliklardan himoyalanish uchun uchinchi o‘zaro ishonchli yuridik shaxs maxsuslashtirilgan apparat-dasturiy kompleksida (aloqa tugunida) axborot

almashinuvi tartiblari ro‘yxatga olinishi (barcha xabarlardan nusxa ko‘chirilishi) bilan birga ma’lumotlarning yaxlitligini ta’minlashni kriptografik usullari va vositalaridan foydalanish zarur.

C. “Buzish” (disruption): Tizim xizmatlarining to‘g‘ri ishlashi va zarur harakatlarni amalga oshirishga to‘sqinlik qiladigan yoki to‘xtatadigan holat yoki hodisa. Quyidagi tahdidli harakatlar buzishni keltirib chiqarishi mumkin:

1. “Zararkunandalik” (incapacitation): Tizimning komponentlarni ishdan chiqarish yo‘li bilan uni ishlashiga to‘sqinlik qiladigan yoki to‘xtatadigan tahdidli harakat.

1.1. “G‘arazli harakatlar uchun qurilma” (malicious logic): Zararkunandalik nuqtai nazaridan, tizimning ishlash qobiliyatini buzish yoki uning resurslarini yo‘q qilish uchun tizimga atayin o‘rnatiladigan istalgan apparat-dasturiy qurilma (masalan, “mantiqiy bomba”). O‘ta xavfli va qiyin aniqlanadigan kompyuter jinoyatkorligi, u bilan kurashish uchun faqat ishonchli apparat-dasturiy vositalari yoki dasturiy ta’minotdan foydalanish yoki bildirilmagan xossalarni aniqlash maqsadida dasturlar listinglarini olish, apparat qismini esa maxsus tekshirishdan o‘tkazish zarur.

1.2. “Fizik buzish” (physical destruction): Tizimning normal ishlashiga to‘sqinlik qilish yoki uni to‘xtatish maqsadida tizim komponentini atayin buzish. Buni oldini olish uchun “aybdorlarni” taxmin qilish va aniqlash bo‘yicha maxsus tashkiliy-texnik tadbirlarni kuchaytirish zarur.

1.3. “Inson xatosi” (human error): Insonning tizim komponentining ishdan chiqishiga atayin bo‘lmagan olib kelgan ta’siri yoki befarqligi. Bu tahdid manbai vakolatli sub’ekt faoliyatiga (inson omiliga) bog‘liq. U ehtimollikka ega va atayin ta’sir (befarqlik) hisoblanmaydi. Bunday hollarda tizimning o‘zi bunday xatoliklardan qo‘shimcha (intellektual) himoyalash vositalarini ko‘zda tutishi kerak.

1.3. “Apparat-dasturiy xatolik” (hardware or software error): Tizim komponentini shikastlanishiga olib keladigan yoki tizimning me’yorda ishlashini to‘xtashiga olib keladigan xatolik. Bu xatolik turi appparat-dasturiy qurilmalardagi

tasodifiy tabiatga ega bo‘lgan yoki tasodifiylik ko‘rinishi ostidagi atayin bo‘lgan shtatdan tashqari vaziyatlarga bog‘liq. Bunday ta’sirlarning halokatli oqibatlarini oldini olish uchun tizim o‘zining ishlashini avtomatik to‘xtatishi (barcha tizim va amaliy jarayonlarni to‘xtatish) va “kutish”rejimiga o‘tishi kerak.

1.4. “Tabiiy ofat” (natural disaster): Tizimning komponentlarini ishdan chiqishiga olib keladigan istalgan tabiiy hodisa (masalan: yong‘in, suv toshqini, zilzila, chaqmoq yoki bo‘ron). Bunday ta’sirlarning halokatli oqibatlarini oldini olish uchun tizim fizik himoyaga ega bo‘lishi kerak.

**2.** “Ishdan chiqarish” (corruption): Tizimning ma’lumotlari yokiishlash algoritmlarini zararli o‘zgartirish yo‘li bilan tizimning ishlashiga keraksiz o‘zgartirishlarni kiritadigan tahdidli harakat.

2.1. “Qalbakilashtirish” (tamper): “Ishdan chiqarish” nuqtai nazaridan, tizim funksiyalarini to‘g‘ri bajarilishini to‘xtatish yoki unga to‘sqinlik qilish maqsadida tizimning ma’lumotlari yoki boshqarish ma’lumotlarini dasturiy ta’minotini atayin buzish. Bunday turdagi buzg‘unchiliklardan himoyalash uchun ma’lumotlarni yaxlitligini ta’minlash, ya’ni ma’lumotlarni istalgan ularni o‘zgartirilishidan himoyalay oladigan kriptografik usullar va vositalardan, shuningdek dasturiy ta’minotdan nusxa ko‘chirishdan foydalanish zarur. Tashqi ruxsat etilmagan suqulib kirishlarning oldini olish uchun sub’ektning haqiqiyligini tekshirishni ko‘p darajali usullari – autentifikatsiyalash, kriptografik usullar va vositalar, mualliflashtirish, uchinchi shaxsni tasdiqlash va boshqa choralardan foydalanish zarur.

2.2. “G‘arazli ta’sirlar uchun qurilma” (malicious logic): “Ishdan chiqarish” nuqtai nazaridan, tizimning ishlash algoritmlari yoki tartiblari yoki uning ma’lumotlarini o‘zgartirish maqsadida tizimga atayin o‘rnatilgan istalgan apparat-dasturiy qurilma yoki dasturiy ta’minot (masalan, “kompyuter virusi”). DT tarkibida kompyuter viruslari va boshqa “zararli” dasturlarni aniqlash uchun maxsus dasturlarga ega bo‘lish kerak, shuningdek tizimning apparatli qismini maxsus nazorat qilinishni o‘tkazilishi maqsadga muvofiq. Tashqi ruxsat etilmagan suqulib

kirishlarning oldini olish uchun sub’ektning haqiqiyligini tekshirishni ko‘p darajali usullari – autentifikatsiyalash, kriptografik usullar va vositalar, mualliflashtirish, uchinchi shaxsni tasdiqlash va boshqa choralardan foydalanish zarur

2.3. “Inson xatosi” (human error): Insonning tizim komponentini ishdan chiqishiga atayin bo‘lmagan ta’siri yoki befarqligi. Bu tahdid manbai vakolatli sub’ekt faoliyatiga (inson omiliga) bog‘liq. U ehtimollikka ega va atayin ta’sir (befarqlik) hisoblanmaydi. Bunday hollarda tizimning o‘zi bunday xatoliklardan qo‘shimcha himoyalash vositalarini ko‘zda tutishi kerak.

2.4. “Apparat-dasturiy xatolik” (hardware or software error): Tizimning ishlash algoritmlari va tartiblari yoki uning ma’lumotlarini o‘zgarishiga olib keladigan xatolik. Bu xatolik turi appparat-dasturiy qurilmalardagi tasodifiy tabiatga ega bo‘lgan yoki tasodifiylik ko‘rinishi ostidagi atayin bo‘lgan shtatdan tashqari vaziyatlarga bog‘liq. Bunday ta’sirlarning halokatli oqibatlarini oldini olish uchun tizim o‘zining ishlashini avtomatik to‘xtatishi (barcha tizim va amaliy jarayonlarni to‘xtatish) va “kutish”rejimiga o‘tishi kerak.

2.5. “Tabiiy ofat” (natural disaster): Tizimning ishlash algoritmlari va tartiblari yoki uning ma’lumotlarini buzilishiga olib keladigan istalgan tabiiy hodisa (masalan: chaqmoq keltirib chiqaradigan quvvatli elektromagnit impulslar). Bunday ta’sirlarning halokatli oqibatlarini oldini olish uchun tizim fizik himoyaga ega bo‘lishi kerak.

**3.** “To‘siq” (obstruction): Tizim jarayonlarini sekinlashtirish yoki to‘sib qo‘yish maqsadida ularga ta’sir etish yo‘li bilan tizim xizmatlarining taqdim etilishini to‘xtatadigan tahdidli harakat.

3.1. “Halaqit” (interference): Bog‘lanishlar, foydalanuvchilar ma’lumotlari va boshqarish ma’lumotlarini to‘sib qo‘yish yo‘li bilan tizim jarayonlari va tartiblarini to‘xtatish. Bunday turdagi buzilishlardan himoyalash uchun ma’lumotlarni uzatishni muqobil (zahira) yo‘nalishlaridan foydalanish zarur.

3.2. “O‘ta yuklanish” (overload): Tizim komponentlarining funksional samaradorligini kamaytirish yoki ularni to‘sib qo‘yish maqsadida ulardagi “foydasiz” ma’lumotlarning o‘ta katta hajmini joylashtirish (zararli trafikni uzatish) bilan tizim jarayonlari va tartiblarini to‘xtatish. Bunday turdagi buzg‘unchiliklardan himoyalash uchun bunday zararli trafikni to‘sadigan (zararsizlantiradigan) maxsus to‘sish tizimlaridan foydalanish zarur.

D. “Qo‘lga kiritish/tortib olish” (usurpation): Tizimning xizmatlarini boshqarish va uning ishlashi noqonuniy sub’ektga o‘tishi natijasidagi holat yoki hodisa. Quyidagi tahdidli ta’sirlar “qo‘lga kiritishga” olib kelishi mumkin:

**1. “**Noqonuniy tayinlash” (misappropriation): Sub’ekt o‘ziga tizim resurslarini ruxsat etilmagan mantiqiy yoki fizik boshqarish funksiyalarini tayinlaydigan tahdidli ta’sir.

1.1. “Xizmatlarni o‘g‘irlash” (theft of service): Ob’ektning xizmatlardan ruxsat etilmagan foydalanishi. Tarmoq xizmatlaridan ruxsat etilmagan foydalanish va boshqarishga bog‘liq (boshqarishni haqiqatda “ikkinchi qo‘llarga” o‘tishi) kompyuter buzg‘unchiliklarining o‘ta xavfli turi. Himoyalash uchun tarmoqning barcha dasturiy elementlarini olisdan boshqarilishini oldini olish kerak. Har bir tizim dasturiy komponentini sozlashni faqat “konsol” kirish orqali sozlash maqsadga muvofiq. Aks holda boshqarish tizimlari bo‘yicha tarmoq (kommunikatsion) dasturiy komponentlari bilan bog‘liq bo‘lmagan (moslashmagan) trafikni filtrlash uchun apparat-dasturiy komplekslaridan foydalanish zarur

1.2. “Funksional imkoniyatlarni o‘g‘irlash” (theft of functionality): Tarmoq komponentlarining amaldagi apparat-dasturiy vositalari va dasturiy ta’minotini noqonuniy olish. Tarmoqni boshqarishni ruxsat etilmagan xolati bilan bog‘liq bo‘lgan (boshqarishni “ikkinchi qo‘llarga” o‘tishi) kompyuter buzg‘unchiliklarining o‘ta xavfli turi. Himoyalash uchun tarmoqning barcha dasturiy elementlarini olisdan boshqarilishini oldini olish kerak. Har bir tizimning dasturiy komponentini faqat “konsol” kirish orqali sozlash maqsadga muvofiq. Aks holda boshqarish tizimlari

bo‘yicha tarmoq (kommunikatsion) apparat-dasturiy komponentlari bilan bog‘liq bo‘lmagan (moslashmagan) trafikni filtrlash uchun apparat-dasturiy komplekslarni qo‘llash zarur.

1.3. “Ma’lumotlarni o‘g‘irlash” (theft of data): Ma’lumotlarni noqonuniy olish va ulardan foydalanish. Jinoiy maqsadlarda boshqarish ma’lumotlaridan ruxsat etilmagan xolda foydalanish yoki ulardan himoyalanadigan ma’lumotlarni olish uchun foydalanish bilan bog‘liq bo‘lgan kompyuter buzg‘unchiliklarining o‘ta xavfli turi. Himoyalash uchun tarmoq bo‘yicha boshqarish ma’lumotlarini uzatilishini oldini olish yoki tarmoqni boshqarish tizimiga barcha bo‘lishi mumkin ulanish kanallarni ishonchli himoyalash yoki o‘chirish zarur.

**2.** “Suiste’mol qilish” (misuse): Tizim komponenti orqali tizimning xavfsizligiga zarar yetkazadigan qandaydir xizmat ko‘rsatish funksiyalari yoki tartiblarini bajarilishi keltirib chiqaradigan tahdidli ta’sir.

2.1. “Qalbakilashtirish” (tamper): “Suiste’mol qilish” nuqtai nazaridan, tizimning ruxsat etilmagan xizmat ko‘rsatish funksiyalari yoki tartiblarini bajarishga majburlash maqsadida tizimning ma’lumotlari, dasturiy ta’minoti yoki boshqarish ma’lumotlarini atayin buzish. Jinoiy maqsadlarda boshqariluvchi DTni modifikatsiyalash bilan bog‘liq kompyuter buzishlarining o‘ta xavfli turi. Tarmoqni boshqarish tizimiga ulanuvchi barcha imkoniyatli kanallarni ishonchli himoyalash yoki o‘chirish maqsadga muvofiq.

2.2. “G‘arazli ta’sirlar uchun qurilma” (malicious logic): “Suiste’mol qilish” nuqtai nazaridan, ruxsat etilmagan xizmat ko‘rsatish funksiyalari yoki tartiblarini bajarish yoki boshqarish maqsadida tizimga atayin o‘rnatilgan istalgan apparat-dasturiy qurilma yoki dasturiy ta’minot. Jinoiy maqsadlarda boshqariluvchi DTni modifikatsiyalash bilan bog‘liq kompyuter buzg‘unchiliklarining o‘ta xavfli turi. Tarmoqni boshqarish tizimiga ulanuvchi barcha imkoniyatli kanallarni ishonchli himoyalash yoki o‘chirish maqsadga muvofiq. Bundan tashqari, faqat ishonchli apparat-dasturiy vositalar yoki DTdan foydalanish yoki deklaratsiya qilinmagan

xossalarni aniqlash maqsadida dasturlar listinglarini olish, apparatlar qismini esa maxsus tekshirishdan o‘tkazish zarur.

2.3. “Ruxsat etilgan buzg‘unchilik” (violation of permissions): Sub’ekt uchun ruxsat etilmagan funksiyalarni bajarish yo‘li bilan ruxsat etilgan tizim vakolatlarini oshirish ta’minlanadigan sub’ektning harakati. Tarmoqni boshqarish tizimiga ruxsatsiz suqulib kirish va bu asosda jinoiy maqsadlarda oshirilgan vakolatlarni olish bilan bog‘liq kompyuter buzishlarining o‘ta xavfli turi. Tarmoqni boshqarish tizimiga ulanuvchi barcha imkoniyatli kanallarni ishonchli himoyalash yoki o‘chirish maqsadga muvofiq.

Ko‘rsatilgan tahdidlar va ularning ta’siri oqibatlarini tahlil qilish shuni ko‘rsatadiki, ularning yakuniy maqsadi quyidagilar hisoblanadi:

-MATda uzatiladigan foydalanuvchilarning ma’lumotlari — ma’lumotlarning o‘qilishi va buzilishi yoki axborot almashinuvi tartibini buzilishi;

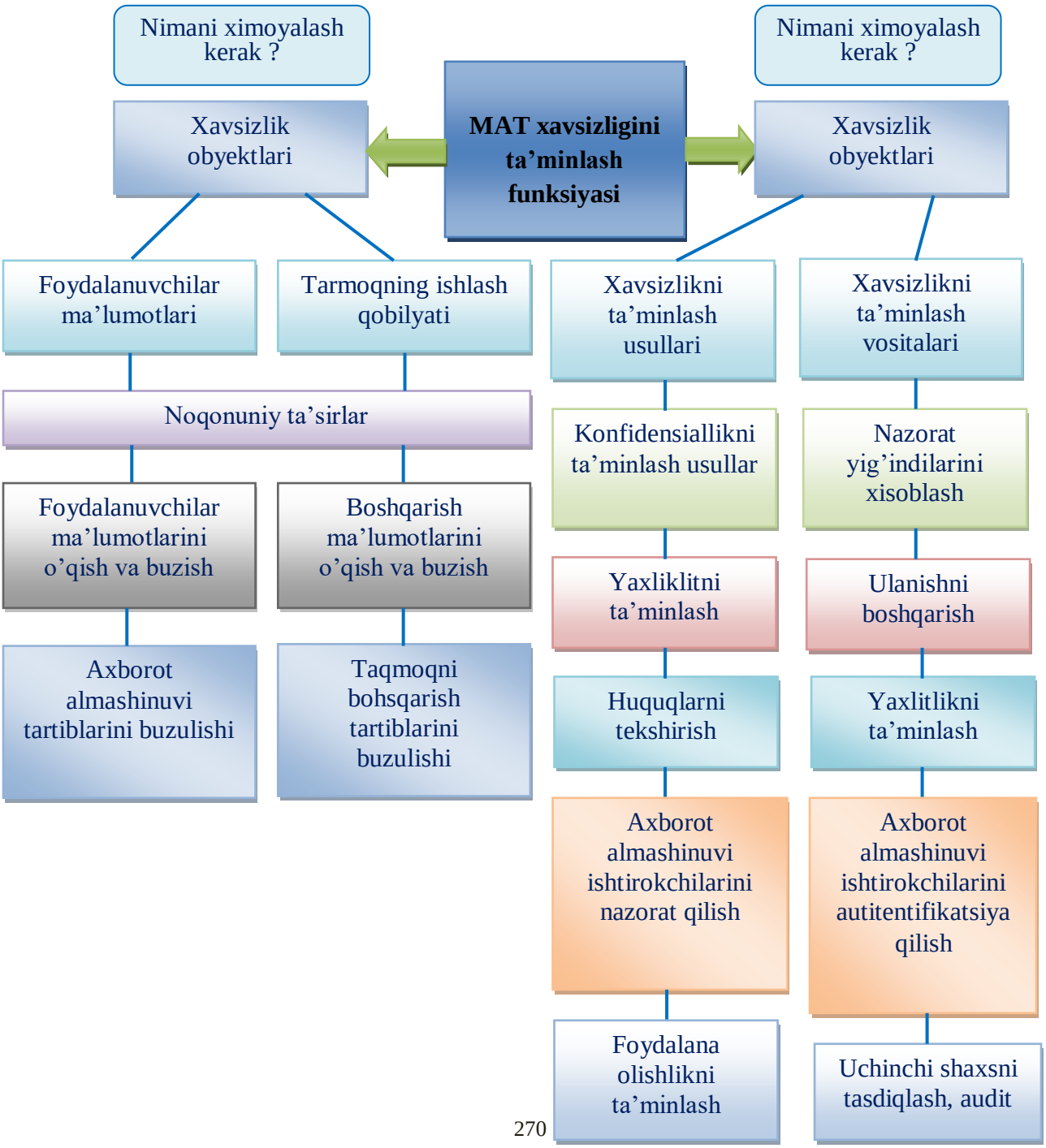
- MATning ishlash qobiliyati — boshqariladigan ma’lumotlarning o‘qilishi va buzilishi yoki tarmoq (tizim) komponentlari yoki butun tarmoqni (tizimni) boshqarish tartiblarini buzilishi.

## 11.3. Multimedia li aloqa tarmoqlarida axborot xavfsizligini ta’minlash vazifalari, usullari va vositalari

Bugungi kunga kelib, MATda axborot xavfsizligini ta’minlashni bir necha qarashlari mavjud. Bu Xalqaro elektr aloqa ittifoqi (ITU-T, X.800, 1991 yil), Standartlashtirish bo‘yicha xalqaro tashkilot (ISO), AQSh mudofaa vazirligi (Department of defense — DOD) va IETF (IRTF) Internet xavfsizlik bo‘yicha ishchi guruhlar xavfsizlik modellariga taa’luqlidir. Shu bilan birga, bu modellarni tahlil qilish shuni ko‘rsatadiki, istalgan tarmoq qo‘shimcha xavfsizlik funksiyalarini ta’minlashi kerak (istalgan ochiq tizim uchun funksiyalar to‘plamidan tashqari), ular

o‘z navbatida tarmoq xavfsizligi ob’ektlari va uni amalga oshirish jihatlarini aniqlaydi.

Tasvirlangan rasm (11.2-rasm) shuni ko‘rsatadiki, xavfsizlik funksiyalari nimfunksiyalarga “bo‘linadi” va tarmoqni himoyalashni ma’lum usullari va vositalari to‘plami orqali amalga oshiriladi. Har bir nimfunksiya ochiq tizimlarning o‘zaro bog‘lanish etalon modeli (OTO‘B EM) arxitekturasining aniq bir sathiga tegishli va mos bo‘lgan xavfsizlikni ta’minlash usullari va vositalari guruhini o‘z ichiga oladi.



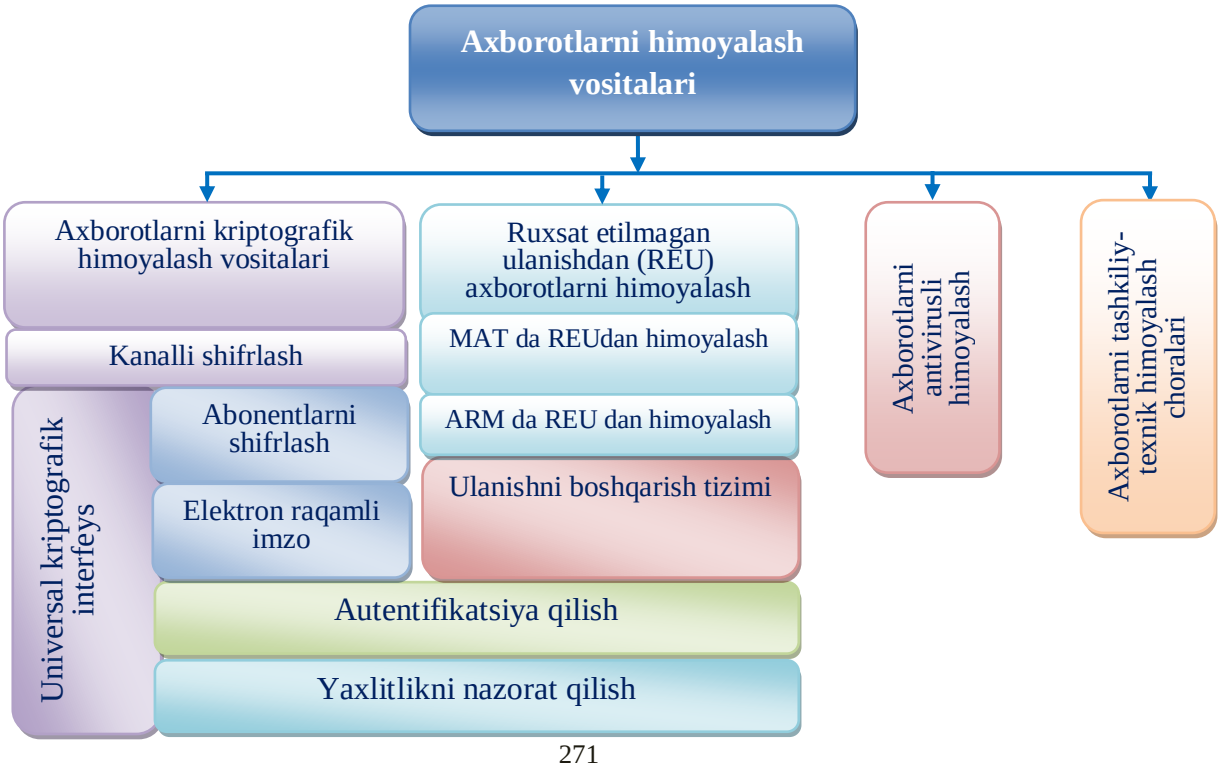
11.2-rasm. MAT AXni ta’minlash funksiyasining ob’ektlari va amalga oshirish jihatlari

Bunda o‘sha bir xil usullar va vositalar MAT arxitekturasining turli sathlarida qo‘llanilishi mumkin.

Axborot xavfsizligini ta’minlash usullari deganda axborotlarni himoyalash bo‘yicha aniq masala yechiladi yoki maqsadga erishishda amalga oshiriladigan qandaydir operatsiyalar va usullar majmui tushuniladi.

Axborot xavfsizligini ta’minlash vositasi deganda ma’lum xossalarga ega bo‘lgan va axborotlarni bir yoki bir necha himoyalash usullarini ishlatadigan texnik qurilmalar (apparat-dasturiy, dasturiy va boshqalar) majmui tushuniladi. Bunda bir necha turli vositalar bitta axborot xavfsizligini ta’minlash usulini amalga oshirishi mumkin.

11.3-rasmda MATda axborotlarni himoyalash vositalari tasvirlangan.



11.3-rasm. Axborotlarni himoyalash vositalari

Mavjud MAT AXni ta’minlash modellariga muvofiq, OTO‘B EM tarmoq arxitekturasining har bir boshqarish sathi nafaqat foydalanuvchilarning axborotlarini himoyalash, balki tarmoqning “me’yordagi” ishlash qobiliyatini qo‘llab quvvatlaydigan boshqarish funksiyalarining o‘zini himoyalashni ta’minlash bo‘yicha qo‘shimcha funksiyalarni o‘z ichiga oladi. Bu qo‘shimcha funksiyalar mos nimfunksiyalarga (o‘zining xavfsizlik usullari va vositalari bilan) bo‘lingan, bu nimfunksiyalar esa har bir boshqarish sathida mos axborot almashinuvi protokollariga “taqsimlangan va o‘rnatilgan”.

Xavfsizlik arxitekturasi deganda AXga tahdidlardan himoyalashni ta’minlash maqsadida xavfsizlikni ta’minlashning qo‘shimcha funksiyalarini MAT boshqarish arxitekturasi sathlari bo‘yicha taqsimlanishini tushunamiz, binobarin, har bir sathning vositalari faqat bu sathni eng zaif bo‘lgan aniq bir tahdidlar turidan himoyalashni ta’minlaydi yoki bu sathda himoyalashni yaratish boshqa sathlarda bu tahdid turidan xavfsizlikni ta’minlash funksiyalarini takrorlanishini (bunday funksiyalarni har bir sathda takroran bo‘lishi inkor qilinmasada) oldini olishga imkon beradi.

## 11.4. Ochiq tizimlarning o‘zaro bog‘lanish etalon modelini xavfsizlik arxitekturasi

Ochiq tizimlarni xavfsizlik arxitekturasini aniqlaydigan birinchi xalqaro standartlardan biri ITU-T X.800 tavsiyasidir. Bu standart OTO‘B EM MAT xavfsizligini ta’minlash funksiyasiga umumiy tavsiflarni beradi. Bu funksiya MAT AXni ta’minlash tizimi (AXTT) orqali bajariladi. Boshqacha aytganda, AXTT MAT AXni ta’minlashni kompleks masalasini yechadi.

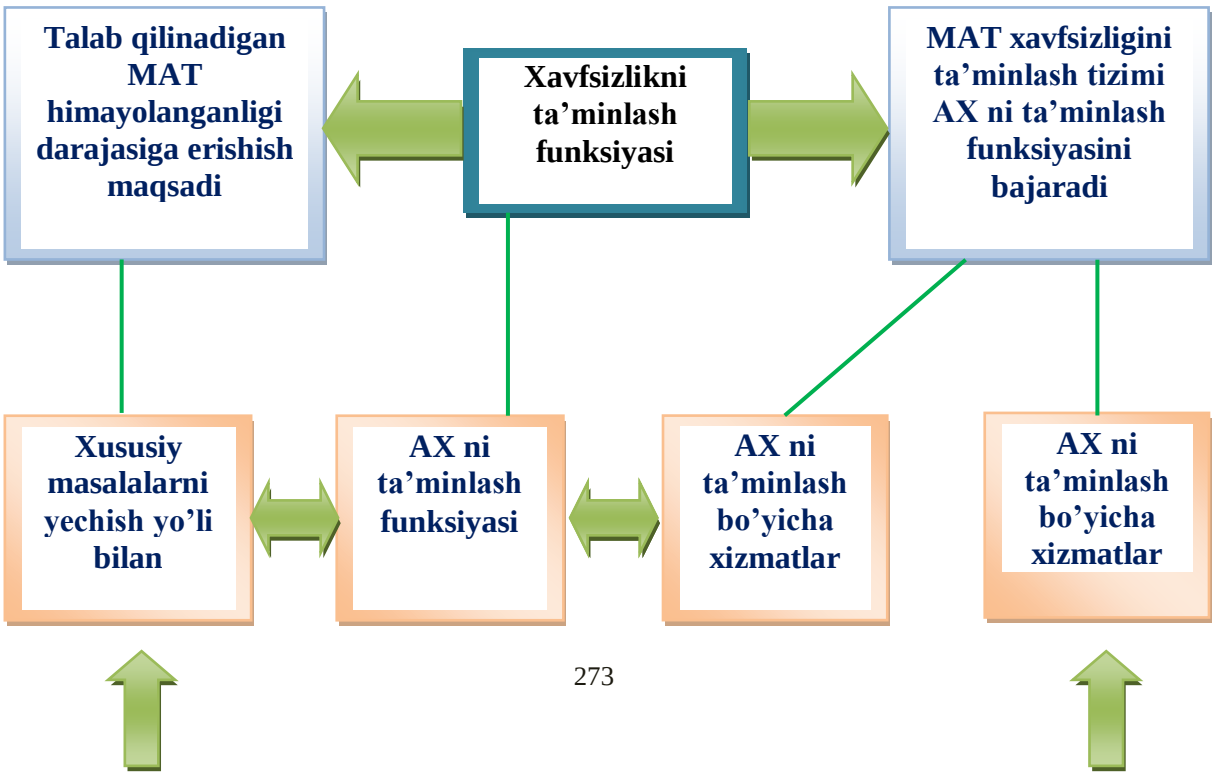
Xavfsizlikni ta’minlash masalasi qo‘shimcha (shart emas) hisoblanadi, uning bajarilishi esa foydalanuvchi yoki ITS egasining “istagiga” bog‘liq bo‘ladi, shuning uchun AXTT xavfsizlikni ta’minlash bo‘yicha xizmatlarni ko‘rsatish bilan uning oldiga qo‘yilgan maqsadlarga erishishni ta’minlaydi. AXTT doirasidagi xavfsizlikni ta’minlash nimtizimlari, axborot xavfsizligini ta’minlash bo‘yicha nimfunksiyalarni bajarish va xizmatlarni taqdim etish yo‘li bilan xususiy masalalarni yechadigan xizmatlar deyiladi (11.4-rasm).

ITU-T X.800 tavsiyasi quyidagi atamalar va tavsiflarni kiritadi:

- ulanishni boshqarish (access control) — mualliflashtirilmagan resursdan foydalanishning oldini olish, shu jumladan resursdan belgilanmagan usulda foydalanishning oldini olish;

- ulanishni boshqarish ro‘yxati (access control list) — resursga ulanishni taqdim etish uchun mualliflashtirilgan sub’ektlar ro‘yxati (ularning ulanish huquqlarini o‘z ichiga oladigan);

- identifikatsiyalanuvchanlik (accountability) — sub’ektning barcha harakatlari ularni sub’ektga aynan tegishliligini keyingi tasdiqlash maqsadida qayd etilishi mumkinligini kafolatlaydigan xususiyat;



11.4-rasm. MAT xavfsizligini ta’minlash tizimining vazifasi va tarkibi

- aktiv tahdid (active threat) — tizim holatini atayin bo‘lmagan mualliflashtirilmagan o‘zgartirish tahdidi;

- autentifikatsion axborotlar (authentication information) - sub’ektning haqiqiyligini tasdiqlash uchun ishlatiladigan axborotlar;

- autentifikatsion almashlash (authentication exchange) — axborot almashinuvi vositalari yordamida sub’ektning haqiqiyligini tasdiqlash usuli;

- mualliflashtirish (authorization) — ulanish huquqlari asosida ulanishni taqdim etishni o‘z ichiga oladigan huquqlarni qondirish;

- foydalana olishlik (availability) — mualliflashtirilgan sub’ektning so‘rovi bo‘yicha ochiq va texnik ma’qul ulanishni ta’minlaydigan xususiyat;

- ulanish mandati (capability) — resursga ulanishda identifikator sifatida ishlatiladigan belgi, binobarin, bunday belgiga ega bo‘lish resursga ulanish huquqini beradi;

- konfidensiallik (confidentiality) — mualliflashtirilmagan foydalanuvchilar, sub’ektlar yoki jarayonlar tomonidan axborotlarni ochilmasligi yoki foydalana olmaslikni ta’minlaydigan xususiyat;

- ishonish ma’lumotlari (credentials) — ob’ektning autentifikatsion axborotlarini shakllantirish uchun yetkaziladigan ma’lumotlari;

- kriptografik tekshirish yig‘indisi (cryptographic check value) — qandaydir simvollar ketma-ketligini kriptografik o‘zgartirishni amalga oshirish yo‘li bilan olingan axborotlar;

- ma’lumotlarning yaxlitligi (data integrity) — ma’lumotlarni o‘zgartirish yoki ularni qandaydir mualliflashtirilmagan usulda buzilishidan himoyalanishini ta’minlaydigan xususiyat;

- ma’lumotlar manbaini autentifikatsiyalash (data origin authentication) — olingan ma’lumotlar manbai haqiqatda o‘zini kimligini bildirgan hisoblanishini tasdiqlash;

- xizmat ko‘rsatishni rad etish (denial of service) — resursga mualliflashtirilgan ulanishga to‘sqinlik qilish yoki vaqt bo‘yicha chegaraviy hisoblanadigan tartiblarning uzilishi;

- raqamli (elektron raqamli) imzo (digital signature) — dastlabki simvollar ketma-ketligiga qo‘shilgan ma’lumotlar yoki kriptografik o‘zgartirilgan dastlabki simvollar ketma-ketligi, ular bu dastlabki simvollar ketma-ketligini oluvchiga bu ketma-ketlikni jo‘natuvchi va uning yaxlitligiga nisbatan ishonch hosil qilishga, shuningdek ularni, masalan, o‘sha oluvchi orqali soxtalashtirishdan himoyalashga imkon beradi;

- haqiqiylikni tekshirishga asoslangan xavfsizlik siyosati (identity- based security policy) — foydalanuvchilar yoki foydalanuvchilar atributlari, foydalanuvchilar guruhlari yoki foydalanuvchilar nomidan va ularni topshirig‘iga binoan ishlaydigan sub’ektlar va ulanish amalga oshiriladigan resurslar/ob’ektlarning haqiqiyligini tekshirishga asoslangan xavfsizlik siyosati;

- kalit yoki kriptokalit (key) — shifrlash va shifrni ochish tartiblarini boshqarishda bevosita qatnashadigan simvollar ketma-ketligi;

- kalitlarni boshqarish (key management) — xavfsizlik siyosatiga muvofiq kalitlarni generatsiyalash, saqlash, taqsimlash, yo‘q qilish, arxivlashtirish va qo‘llash;

- manipulyatsiyalashni aniqlash (manipulation detection) — ma’lumotlarni modifikatsiyalash dalillarini aniqlash (tasodifiy yoki atayin) uchun qo‘llaniladigan usul;

- maskarad (masquerade) — bitta sub’ek o‘zini boshqa sub’ekt sifatida ko‘rsatadigan vaziyat;

- notarial tasdiqlash (notarization) — uchinchi tomon orqali ishonilgan (UTI) ma’lumotlarni ro‘yxatga olish, bu keyinchalik ularning parametrlari va xarakteristikalarining, masalan, tarkib, manba, vaqt va yetkazilish aniqligini kafolatlashga imkon beradi;

- passiv tahdid (passive threat) — tizimning holatini o‘zgartirmasdan axborotlarni mualliflashtirilmagan ochish tahdidi;

- parol (password) — simvollar ketma-ketligi hisoblanadigan konfidensial autentifikatsion axborotlar;

- o‘zaro ta’sirlashadigan sub’ektni autentifikatsiyalash (peer-entity authentication) – bog‘lanishning qarama-qarshi tomonidagi sub’ekt axborot almashish tartibini (AAT) o‘tkazilishi zarur bo‘lgan sub’ekt ekanligini tasdiqlash;

- fizik xavfsizlik (physical security) — AXga atayin yoki tasodifiy tahdidlarni amalga oshirilishi oqibatlarida resurslarni fizik himoyalashni ta’minlash uchun ishlatiladigan tadbirlar kompleksi;

- maxfiylik (privacy) — foydalanuvchilarning hayot faoliyatiga bog‘liq qandaydir ma’lumotlarini to‘planishi va saqlanishi mumkinligini, shuningdek ular kim orqali va kimga ochilishi mumkinligini nazorat qilish yoki ta’sir etish huquqi;

- rad etish (repudiation) — AAT o‘tkazilishida o‘zaro ta’sirlashadigan sub’ektlardan birining bu tartibda yoki uning alohida bosqichlarida ishtirok etishni rad etishi;

- marshrutlashtirishni boshqarish (routing control) — retranslyatsiya oraliqlari, aloqa kanallari yokima’lum tarmoqlardarad etish yoki tanlash singari marshrutlash tartiblarini bajarilishida qoidalarning qo‘llanilishi;

- qoidalarning qo‘llanilishiga asoslangan xavfsizlik siyosati (rule-based security policy) — barcha foydalanuvchilar uchun mo‘ljallangan yagona qoidalardan foydalanishga asoslangan xavfsizlik siyosati. Bu qoidalar, odatda, ulanish uchun

mo‘ljallangan resurslarning chegaraviyligi va foydalanuvchilar nomidan ishlaydigan foydalanuvchilar, sub’ektlar yoki foydalanuvchilar guruhlarining mos atributlari egalari orasidagi kelishtirish hisoblanadi;

- xavfsizlik auditi (security audit) — boshqarish tizimi vositalarining mosligini baholash va ularni qabul qilingan xavfsizlik siyosatiga va qo‘llaniladigan funksional tartiblarga mosligini ta’minlash maqsadida, shuningdek AXni ta’minlash tizimidagi zaif joylarni aniqlash va boshqarish tizimi, xavfsizlik siyosati va mos tartiblarga o‘zgartirishlarni kiritish bo‘yicha tavsiyalarni ishlab chiqish uchun tizim yozuvlari va asosiy faoliyat yo‘nalishlarini mustaqil tekshirish va taftish qilish;

- xavfsizlik auditi uchun dastlabki berilganlar (security audit trail) — xavfsizlik auditini muvaffaqiyatliroq o‘tkazilishi uchun to‘plangan va real ishlatiladigan ma’lumotlar;

- xavfsizlik markeri (security label) — resurs (u simvollar ketma-ketligi bo‘lishi mumkin) bilan to‘g‘ridan-to‘g‘ri bog‘liq bo‘lgan belgi (belgini qo‘yilishi), u bu resursning xavfsizlik atributlarini ishlatishni belgilaydi yoki ko‘zda tutadi;

- xavfsizlik siyosati (security policy) — xavfsizlik xizmatlarining ishlashini to‘g‘riligini baholash mezonlari to‘plami;

- xavfsizlikni ta’minlash bo‘yicha xizmat (security service) — tizimlarni mos himoyalash va ma’lumotlarni yetkazilishini kafolatlaydigan OTO‘B EM arxitekturasi sathlaridan biri taqdim etadigan xizmat (qo‘shimcha nimfunksiya);

- alohida maydonlarni himoyalash (selective field protection) — uzatilishi kerak bo‘lgan xabarning ma’lum maydonlarini himoyalash;

- chegaraviylik (sensitivity) — resursning qiymati va ahamiyatini bildiradigan, shuningdek uning zaifligini o‘z ichiga olishi mumkin bo‘lgan resursning xususiyati;

- tahdid (threat) — xavfsizlikni potensial buzilishi;

- trafik oqimining konfidensialligi (traffic flow confidentiality) — trafikni tahlil qilish tahdidlarini zararsizlantirish uchun konfidensiallikni ta’minlash bo‘yicha xizmat;

- trafikni to‘lib ketishi (traffic padding) — ulanish uchun soxta so‘rovlar, soxta xabarlar yoki xabarlardagi soxta simvollar ketma-ketliklarini generatsiyalash;

- ishonchli ishlash (trusted functionality) — unga nisbatan u qandaydir mezonga muvofiq, masalan, xavfsizlik siyosatiga muvofiq to‘g‘ri bajarilayotganligini ko‘zda tutish mavjud bo‘lgan funksional jarayon.

## 11.5. Xavfizlikni ta’minlash xizmatlari va usullari

OTO‘B EM xavfsizlik arxitekturasi xavfsizlikni ta’minlash bo‘yicha quyidagi xizmatlarni o‘z ichiga oladi:

- autentifikatsiyalash (authentication). Bu xizmat quyidagi ikki turlarda bo‘lishi mumkin:

- o‘zaro ta’sirlashadigan sub’ektni autentifikatsiyalash (peer-entity authentication). Bu xizmat OTO‘B EM arxitekturasining n-sathi orqali ta’minlanadi va bu bilan (n+1) - sathni sub’ektiga ulanishning qarama-qarshi tomonidagi sub’ekt u bilan AAT o‘tkazilishi kerak bo‘lgan (n+1)-sathni sub’ekti ekanligini tasdiqlaydi;

- ma’lumotlar manbaini autentifikatsiyalash (data origin authentication). Bu xizmat OTO‘B EM arxitekturasining n-sathi orqali ta’minlanadi va bu bilan (n+1)-sath sub’ektiga kelgan ma’lumotlar manbai so‘ralgan (n+1)-sathni sub’ekti ekanligini tasdiqlaydi;

- ulanishni boshqarish (access control). Bu xizmat OTO‘B EM - tarmoqlar/tizimlar orqali mumkin bo‘lgan resurslardan ruxsat etilmagan foydalanishdan himoyalashni ta’minlaydi;

- ma’lumotlarning konfidensialligi (data confidentiality). Bu xizmat to‘rtta turda bo‘lishi mumkin:

- virtual ulanishning konfidensialligi (connection confidentiality). Bu xizmat OTO‘B EM arxitekturasining n-sathida bu sathda ulanish o‘rnatilganidan keyin foydalanuvchining barcha ma’lumotlarini konfidensialligini ta’minlaydi;

- ulanish o‘rnatilmasdan axborot almashinuvining konfidensialligi (connection less confidentiality). Bu xizmat OTO‘B EM arxitekturasining n-sathida bittalik deytagramma (xabarlarni yetkazishning deytagramma rejimi) jo‘natilgan xolatda foydalanuvchining barcha ma’lumotlari uchun konfidensiallikni ta’minlaydi;

- alohida maydonlarning konfidensialligi (selective field confidentiality). Bu xizmat OTO‘B EM arxitekturasining n-sathida foydalanuvchi tomonidan ulanish o‘rnatilgan rejimda yoki deytagrammali rejimda jo‘natilgan simvollar ketma-ketligidagi alohida maydonlarning konfidensialligini ta’minlaydi;

- trafik oqimining konfidensialligi (traffic flow confidentiality). Bu xizmat trafik oqimlarini kuzatishni olib borishda ajratib olish mumkin bo‘lgan axborotlarni himoyalashni ta’minlaydi;

- ma’lumotlarning yaxlitligi (data integrity). Bu xizmat quyidagi beshta turlardan bo‘lishi mumkin:

- ulanishni keyingi qayta tiklanishili ulanishning yaxlitligi (connection integrity with recovery). Bu xizmat OTO‘B EM arxitekturasining n-sathida, bu sathda ulanish o‘rnatilganidan keyin foydalanuvchining barcha ma’lumotlarini yaxlitligini, shuningdek deytagrammaning butun ketma-ketligi chegaralarida istalgan modifikatsiyani, soxta qo‘yilma, istalgan ma’lumotlarni soxta o‘chirilishi yoki takrorlanishini aniqlashni (butun ketma-ketlikni qayta tiklashga urinish bilan) ta’minlaydi;

- ulanishni uni keyingi qayta tiklanishisiz yaxlitligi (connection integrity with out recovery). Bu xizmat OTO‘B EM arxitekturasining n-sathida ulanish o‘rnatilganidan keyin foydalanuvchining barcha ma’lumotlarini yaxlitligini, shuningdek deytagrammaning butun ketma-ketligi chegaralarida istalgan modifikatsiyani, soxta qo‘yilma, istalgan ma’lumotlarni soxta o‘chirilishi yoki takrorlanishini aniqlashni (butun ketma-ketlikni qayta tiklashga urinishsiz) ta’minlaydi;

- virtual bog‘lanishni tashkil etishda alohida maydonlarning yaxlitligi (selective field connection integrity). Bu xizmat OTO‘B EM arxitekturasining n-sathida virtual ulanish bo‘yicha uzatiladigan bu sathni protokolli xabarlari doirasida foydalanuvchi xabarining alohida maydonlarini yaxlitligini ta’minlaydi, shuningdek ularni modifikatsiyalanishi tufayli “shikastlangan” alohida maydonlarni soxta qo‘yilmalar, soxta o‘chirish yoki takroran uzatishni aniqlash usulini tanlaydi;

- bog‘lanish o‘rnatilmasdan axborot almashinuvining yaxlitligi (connection less integrity). Agar bu xizmat OTO‘B EM arxitekturasining n-sathida taqdim etilsa, u holda u (n+7)- sath sub’ektini so‘rashda kafolatlangan yaxlitlikni ta’minlaydi. Bundan tashqari, bu xizmat bittalik deytagrammaning (xabarlarni yetkazishning deytagramma rejimi) yaxlitligini ta’minlaydi, shuningdek qabul qilingan deytagrammaning modifikatsiyalanganligini aniqlash usulini tanlashi mumkin. Shu bilan birga, u deytagrammalarni takroran uzatilishini aniqlash usulini (lekin barcha bo‘lishi mumkin bo‘lganlaridan istalganini emas) tanlashi mumkin;

- bog‘lanish o‘rnatilmasdan axborot almashinuvini tashkil etishda alohida maydonlarning yaxlitligi (selective field connection less integrity). Bu xizmat bittalik deytagrammaning (xabarlarni yetkazishning deytagramma rejimi) alohida maydonlarining yaxlitligini ta’minlaydi, shuningdek alohida maydonlarning modifikatsiyalanganligini aniqlash usulini tanlashi mumkin;

**-** rad etmaslik (non-repudiation). Bu xizmat quyidagi ikki turda bo‘lishi mumkin:

**-** manbaning soxta rad etishidan himoyalash (non-repudiation with proof of origin). Bu xizmat ma’lumotlar oluvchini, jo‘natuvchining bu ma’lumotlarni yoki uning komponentlarini uzatishni atayin rad etishidan himoyalaydi;

**-** oluvchining soxta rad etishidan himoyalash (non-repudiation with pro of delivery). Bu xizmat ma’lumotlar jo‘natuvchini, oluvchining bu ma’lumotlarni yoki uning komponentlarini olishni atayin rad etishidan himoyalaydi;

OTO‘B EM xavfsizlik arxitekturasi quyidagi xavfsizlikni ta’minlash usullarini o‘z ichiga oladi:

- shifrlash (encipherment). Shifrlash yordamida ma’lumotlar yoki trafik oqimi haqidagi ma’lumotlarning konfidensialligini ta’minlash mumkin. Bundan tashqari, shifrlash AXni ta’minlashning boshqa usullarida ham ishlatilishi mumkin;

- elektron raqamli imzo (ERI). ERIning qo‘llanilishi quyidagi ikkita tartiblarni bajarilishini ko‘zda tutadi:

- ERIni shakllantirish tartibining o‘zi (elektron xabarni imzolash). Bu tartibda sub’ekt imzo muallifi nuqtai nazaridan maxfiy (ya’ni noyob yoki konfidensial) axborotlar ishlatiladi. ERIni shakllantirish xabarni shifrlash yoki xabarning kriptografik yig‘indisini hisoblashni ko‘zda tutadi, buning uchun maxfiy kalit sifatida muallifning maxfiy axborotini ishlatadi;

- imzolangan elektron xabarni tekshirish tartibi. Bu tartibda umumiy ma’lum bo‘lgan, lekin ulardan imzo muallifining maxfiy axborotlarini olish mumkin bo‘lmaydigan qo‘shimcha tartiblar va axborotlar ishlatiladi.

ERIning asosiy xususiyati, imzo faqat ERI muallifining maxfiy axborotlaridan foydalanish asosida shakllantirilishi mumkinligi hisoblanadi. Shunday qilib, ERI tekshirilganidan keyin u keyinchalik (binobarin, istalgan vaqt onida) ishonchli uchinchi tomonga (masalan, sudyaga yoki betaraf sudga) tasdiqlab berilishi mumkin, ya’ni faqat u noyob maxfiy axborot egasi ERIni shakllantirishi (muallifi bo‘lishi) mumkinligini isbotlashi mumkin.

- ulanishni boshqarish. Ulanishni boshqarishda sub’ektning ulanish huquqlarini aniqlash va ta’minlash maqsadida sub’ekt shaxsini autentifikatsiyalash yoki sub’ekt haqidagi ma’lumotlar (masalan, ma’lum sub’ektlar guruhiga tegishlilik) yoki ulanish mandati ishlatilishi mumkin. Agar sub’ekt mualliflashtirilmagan resursdan yoki muallifashtirilgan resursdan ruxsat etilmagan usulda foydalanishga urinsa, u holda ulanishni boshqarish funksiyasi urinishni to‘sib qo‘yadi va AXTTni audit qilishni o‘tkazish uchun dastlabki ma’lumotlardagi to‘qnashuv haqidagi

yozuvlar yoki xavf signalini yoqish maqsadida to‘qnashuv haqida qo‘shimcha xabar qilishi mumkin. Deytagramma rejimida ma’lumotlarni uzatishda, uzatish tomonining unga ulanishda rad etishi haqidagi istalgan bildirilishi, faqat ma’lumotlar manbai bilan ulanishni boshqarish vositalarini aldash sifatida tushuntirilishi mumkin.

Ulanishni boshqarish usullari virtual ulanishning bir tomonida (yoki har ikkala tomonlarda) yoki istalgan oraliq nuqtasida joylashtirilgan mos himoyalash vositalari (ulanishni boshqarish vositalari) yordamida amalga oshirilishi mumkin:

- ma’lumotlarning yaxlitligi. Ma’lumotlarning yaxlitligini ta’minlash bo‘yicha quyidagi ikkita xizmat turlari mavjud:
- bittalik xabar yoki ma’lumotlar maydonining yaxlitligi;
- xabarlar oqimi yoki ma’lumotlar maydonlarining yaxlitligi.

Umuman olganda, bu ikkita xizmat turlarini amalga oshirish uchun birinchisi bajarilmasdan ikkinchisini bajarilishi ma’nosiz bo‘lsada, yaxlitlikni ta’minlashning turli usullari qo‘llaniladi. Bittalik xabar yoki ma’lumotlar maydonining yaxlitligini ta’minlash ikkita jarayonni ko‘zda tutadi, ulardan biri jo‘natuvchi orqali, boshqasi esa oluvchi tomonidan amalga oshiriladi:

- jo‘natuvchi xabarga uning funksiyasi hisoblanadigan parametrni qo‘shadi. Bu parametr o‘zi shifrlanadigan qo‘shimcha axborotlar (masalan, blokli tekshirish kodi yoki kriptografik tekshirish yig‘indisi) bo‘lishi mumkin;
- oluvchi mos parametrni shakllantiradi va uni olingan parametr bilan taqqoslaydi, ya’niuzatish jarayonida xabarni modifikatsiyalanganligi dalilini o‘rnatish maqsadida.

Faqat bitta bunday usul ishlatilganida “Xabarni takroran uzatish” turdagi hujumdan himoyalashni ta’minlash mumkin bo‘lmaydi. OTO‘B EM arxitekturasining mos sathlarida ma’lumotlar bilan manipulyatsiyalashni aniqlash bu yoki yuqoriroq sathda qayta tiklash tartibiga (masalan, takroran uzatish yoki xatolikni tuzatish yordamida) olib kelishi mumkin.

Virtual ulanish rejimida ma’lumotlarni yetkazishda xabarlar ketma-ketligining yaxlitligini ta’minlash (ya’ni, kelish tartibini buzilishi, yo‘qotishlar, takroran uzatish va qo‘yilma yoki xabarlarni modifikatsiyalashdan himoyalash), xabarlarni kelish tartibiga aniq rioya qilish, ya’ni xabarlarni ketma-ket raqamlash, ularga vaqt belgilarini qo‘yish yoki ularni kriptografik “bog‘lash” qo‘shimcha usullarini qo‘llashni talab qiladi.

Xabarlarni yetazishni deytagrammali rejimida “Xabarni takroran uzatish” turidagi hujumlarning ayrim turlaridan himoyalash uchun xabarga vaqt belgilarini kiritish tartibi ishlatilishi mumkin:

**-** autentifikatsiyali axborotlarni almashish. Bu usulni amalga oshiradigan himoyalash vositalari, o‘zaro ta’sirlashadigan sub’ektni autentifikatsiyalashni ta’minlash maqsadida OTO‘B EM arxitekturasining n-sathiga o‘rnatilishi mumkin. Agar sub’ektni autentifikatsiyalash vositasi uni autentifikatsiyalamasa, u holda bu ulanishni yo‘qotilishiga yoki to‘xtatishiga olib keladi va to‘qnashuv haqida AXTT ma’muriyatini ogohlantirishga va bo‘lib o‘tgan to‘qnashuv haqida yozuvli AXTT auditini o‘tkazish uchun dastlabki ma’lumotlarni to‘ldirishga olib kelishi mumkin.

AXni ta’minlashni bu usuli quyidagilardan foydalanishga asoslanishi mumkin:

**-** jo‘natuvchi jo‘natadigan va oluvchi tekshiradigan autentifikatsiyali axborotlar (masalan, parollar);

**-** kriptografik algoritmlar;

**-** sub’ektning o‘ziga xos xususiyatlari yoki mulki;

**-** trafikni to‘lishi. Trafikni to‘lishini amalga oshiradigan himoyalash vositalari, trafikni tahlil qilishdan turli himoyalash darajalarini ta’minlash uchun ishlatilishi mumkin. Bu usul faqatgina trafikning to‘lib ketishi konfidensiallik xizmatlari yordamida himoyalangan xolatda samarali bo‘lishi mumkin;

- marshrutlashni boshqarish. Yetkazish marshrutlari dinamik tanlanishi yoki faqat himoyalangan nimtarmoqlar, retranslyatsiya oraliqlari yoki aloqa kanallari/liniyalaridan foydalanish hisobga olinishi bilan rejalashtirilishi mumkin.

Oxirgi (amaliy) tizimlar ma’lumotlarni manipulyaiyalashga bog‘liq bo‘lgan doimiy hujumlarni aniqlash maqsadlarida tarmoq xizmatlari provayderidan turli marshrutlar qo‘llaniladigan ulanishlarni shakllantirishni talab qilishi mumkin.

Ma’lumotlarni ishonchli yetkazishni ta’minlash uchun xavfsizlik markerlari bunday ma’lumotlarni ishonchli nimtarmoqlar, retranslyatsiya oraliqlari yoki aloqa kanallari/liniyalari orqali uzatishda xavfsizlik siyosatiga muvofiq ta’qiqlanishi mumkin. Bundan tashqari, ulanishni uyushtiruvchi (yoki yetkazish deytagramma rejimi holida jo‘natuvchi) taqdim etiladigan yetkazish marshrutlariga nisbatan norozilik bildirishi mumkin va bunda ma’lum nimtarmoqlar, retranslyatsiya oraliqlari yoki aloqa kanallari/liniyalari yetkazish marshrutlaridan chiqarishni so‘rashi mumkin;

- notarial tasdiqlash. Ikki yoki undan ortiq sub’ektlar orasida aylanadigan ma’lumotlarning xususiyati (yaxlitlik, mualliflik, vaqt va oluvchi kabi), notarial tasdiqlash yordamida kafolatlanishi mumkin. Kafolat o‘zaro ta’sirlashadigan sub’ektlar ishonadigan va guvohlik berish yo‘li bilan kutiladigan kafolatni tasdiqlash uchun zarur ma’lumotlarni saqlaydigan uchinchi ishonchli tomon (UIT) rolida qatnashadigan notarius orqali beriladi. Axborot alashinuvining har bir tomoni notarius ko‘rsatadigan mos xizmatlar sifatida ERI vositalari, shifrlash va yaxlitlikni himoyalashdan foydalanishi mumkin. Notarial tasdiqlashni so‘rashda ma’lumotlar notarius bilan ham himoyalangan ulanishdan foydalangan holda o‘zaro ta’sirlashadigan sub’ektlar orasida aylanadi.

AXni ta’minlashni umumiy tizim usullariga (ya’ni OTO‘B EM arxitekturasiga bog‘liq bo‘lmagan) quyidagilar kiradi:

- ishlash ishonchliligi (kafolati). Ishlash ishonchliligini ta’minlash, birinchi navbatda, himoyalash vositalarida AXni ta’minlashning boshqa usullarini to‘g‘ri ishlatish uchun foydalaniladi. To‘g‘ridan-to‘g‘ri xavfsizlik usulini ishlatishni yoki xavfsizlikni ta’minlash bo‘yicha xizmatlarga ulanishni ta’minlaydigan istalgan tartib ishonchni oqlashi kerak;

- xavfsizlik markerlarini qo‘llash. Resurslar, shu jumladan ma’lumotlarning o‘zi, ular bilan to‘g‘ridan-to‘g‘ri bog‘langan xavfsizlik markerlariga, masalan, darajaning chegaraviyligini ko‘rsatish uchun xavfsizlik markerlariga ega bo‘lishi mumkin. Xavfsizlik markerlari translyatsiya qilinadigan ma’lumotlar bilan bog‘langan qo‘shimcha ma’lumotlar bo‘lishi mumkin. Mos xavfsizlik markerlari to‘g‘ri tekshirilishi uchun aniq identifikatsiyalanishi kerak. Bundan tashqari, ular bog‘langan ma’lumotlardan ajratilgan bo‘lishi (chegaraga ega bo‘lishi) kerak;

- xavfsizlikka ta’sir qiladigan hodisalarni aniqlash;

- xavfsizlik auditi uchun dastlabki ma’lumotlarni to‘plash va ularni qo‘llash;

- xavfsizlikni qayta tiklash. Bu usul boshq xavfsizlik usullarini ishlatadigan himoyalash vositalarini so‘rashga, qabul qilingan qoidalar asosida qayta tiklash protseduralarini bajarilishiga bog‘liq.

11.1-jadvalda xavfsizlikni ta’minlash usullari va xizmatlari orasidagi bog‘lanishlar keltirilgan.

OTO‘B EM xavfsizligi arxitekturasi sathlar bo‘yicha AXni ta’minlash xizatlarining quyidagi taqsimlash prinsiplariga ega:

- xizmatlarni amalga oshirishni muqobil variantlarining soni minimal bo‘lishi kerak;

- OTO‘B EM xavfsizligi arxitekturasida bir necha sathlarda xavfsizlikni ta’minlash bo‘yicha xizmatlarni o‘rnatish yo‘li bilan himoyalangan tizimlarni yaratishga ruxsat etiladi;

- AXTTda ishlatilgan qo‘shimcha funksiyalar zarurat bo‘lmaganida OTO‘B EMning mavjud funksiyalarini takrorlamasligi kerak;

- OTO‘B EM sathining funksional bog‘liqmasligini istalgan bo‘lishi mumkin bo‘lgan buzilishlari bo‘lmasligi kerak;

- amalga oshiriladigan ishonchli funksiyalarning soni minimal bo‘lishi kerak;

- sub’ekt, arxitekturaning pastki sathida sub’ekt o‘rnatgan himoyalash vositasi orqali amalga oshiriladigan AXni ta’minlash usuliga bog‘liq bo‘lgan hollarda,

istalgan oraliq sathlari xavfsizlikni xar qanday buzilishi bo‘lmaydigan xolatda ishlashi kerak;

- arxitekturaning aniq bir sathida amalga oshiriladigan qo‘shimcha xavfsizlik funksiyalari, mumkin bo‘lgan joylarda shunday aniqlanishi (tavsiflanishi) kerakki, bu ularni mustaqil modullar ko‘rinishida joriy etilishiga halaqit bermasin.

11.1-jadval

ITS AXni ta’minlash usullari va xizmatlari orasidagi bog‘lanishlar

| Usul / Xizmat | Shifrlash | ERI | Ulanishni boshqarish | Ma’lumotlar yaxlitligi | Autentifikatsiyali axborotni almashish | Trafikni to‘lishi | Marshrutlashni boshqarish | Notarial tasdiqlash |
|---|---|---|---|---|---|---|---|---|
| O‘zaro ta’sirlashadigan sub’ektni autentifikatsiyalash | + | + | | | + | | | |
| Ma’lumotlar manbaini autentifikatsiyalash | + | + | | | | | | |
| Ulanishni boshqarish | | | + | | | | | |
| Virtual ulanishning konfidensialligi | + | | | | | | + | |
| Ulanish o‘rnatilmasdan axborot almashinuvining konfidensialligi | + | | | | | | + | |
| Alohida maydonlarning konfidensialligi | + | | | | | | | |
| Trafik oqimlarining konfidensialligi | + | | | | | + | + | |
| Keyingi qayta tiklashli ulanishning yaxlitligi | + | | | + | | | | |
| Keyingi qayta tiklashsiz ulanishning yaxlitligi | + | | | + | | | | |
| Virtual ulanishni tashkil etishda alohida maydonlarning yaxlitligi | + | | | + | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Ulanish o‘rnatilmasdan axborot almashinuvining yaxlitligi | + | + | | + | | | | |
| Ulanish o‘rnatilmasdan axborot almashinuvini tashkil etishda alohida maydonlarning yaxlitligi | + | + | | + | | | | |
| Manbaning soxta rad etishidan himoyalash | | + | | + | | | | + |
| Oluvchining soxta rad etishidan himoyalash | | + | | + | | | | + |

Bundan tashqari, OTO‘B EM arxitekturasi so‘rov modeli, axborotli o‘zaro ta’sirlashishni himoyalangan xizmatlarini boshqarish va qo‘llashni o‘z ichiga oladi va u quyidagi tavsiflardan tashkil topgan:

- o‘zaro ta’sirlashadigan jarayonlarni himoyalash xususiyatlari;
- xavfsizlik xizmatlarini qo‘llash sharoitlari;
- ulanishni o‘rnatish rejimida himoyalangan axborot almashinuvining ishlashi;
- ulanish o‘rnatilmagan rejimda himoyalangan axborot almashinuvining ishlashi.

11.2-jadval.

OTO‘B EM arxitekturasi sathlari bo‘yicha xavfsizlik xizmatlarini taqsimlanishi (OTO‘B EM xavfsizlik arxitekturasi)

| OTO‘B EM xavfsizlik arxitekturasi / Xizmatlar | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| O‘zaro ta’sirlashadigan sub’ektni autentifikatsiyalash | | | + | + | | | + |
| Ma’lumotlar manbaini autentifikatsiyalash | | | + | + | | | + |
| Ulanishni boshqarish | | | + | + | | | + |
| Virtual ulanishning konfidensialligi | + | + | + | + | | + | + |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Ulanish o‘rnatilmasdan axborot almashinuvining konfidensialligi | | + | + | + | | + | + |
| Alohida maydonlarning konfidensialligi | | | | | | + | + |
| Trafik oqimlarining konfidensialligi | + | | + | | | | + |
| Keyingi qayta tiklashli ulanishning yaxlitligi | | | + | | | | + |
| Keyingi qayta tiklashsiz ulanishning yaxlitligi | | + | + | | | | + |
| Virtual ulanishni tashkil etishda alohida maydonlarning yaxlitligi | | | | | | | + |
| Ulanish o‘rnatilmasdan axborot almashinuvining yaxlitligi | | + | + | | | | + |
| Ulanish o‘rnatilmasdan axborot almashinuvini tashkil etishda alohida maydonlarning yaxlitligi | | | | | | | + |
| Manbaning soxta rad etishidan himoyalash | | | | | | | + |
| Oluvchining soxta rad etishidan himoyalash | | | | | | | + |

11.3-jadval

OTO‘B EM sathlari bo‘yicha xavfsizlikni ta’minlash usullarining taqsimlanishi

| Usul / OTO‘B EM sathi | Shifrlash | ERI | Ulanishni boshqarish | Ma’lumotlar yaxlitligi | Autentifikatsion axborotlarni almashish | Trafikni to‘lishi | Marshrutlashni boshqarish | Notarial tasdiqlash |
|---|---|---|---|---|---|---|---|---|
| 1 | + | | | | | | | |
| 2 | + | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | + | + | + | + | + | + | + | |
| 4 | + | + | + | + | + | | | |
| 5 | | | | | | | | |
| 6 | + | + | | + | | | | + |
| 7 | + | + | + | + | + | + | | + |

## 11.6. Internetda xavfsizlik arxitekturasi tamoyillari

Hozirgi kunda Internet xavfsizlik arxitekturasi oxirigacha aniqlanmagan va buning ustiga standartlashtirilmagan. MATda qator xavfsizlik modellari mavjud. Lekin OTO‘B EM xavfsizlik modeli Internet-tarmoqlari (RFC-791, RFC-1349, RFC-1958) uchun to‘g‘ri kelmaydi, chunki ularning arxitekturasi sathlar soni bilan farqlanadi (OTO‘B EMda 7 ta, Internetda esa 5 ta), shunga qaramay, OTO‘B EM xavfsizligi arxitekturasida aniqlangan xavfsizlikni ta’minlash xizmatlari va usullari, Internet xavfsizligi arxitekturasining turli variantlarida qo‘llaniladigan sathlarga o‘xshash. Shuning uchun Internet uchun eng to‘g‘ri keladigan xavfsizlik modellari Standartlashtirish bo‘yicha Xalqaro tashkilot (ISO), AQSh mudofaa vazirligi (DOD) va Internet IETF(IRTF) xavfsizlik bo‘yicha ishchi guruhi hisoblanadi.

Internet tarmoq xavfsizligi g‘oyasiga muvofiq xavfsizlikni ta’minlash bo‘yicha xizmatlar quyidagi tarzda taqsimlangan (11.4-jadval).

11.4-jadval.

Internet arxitekturasi sathlari bo‘yicha xavfsizlik xizmatlarining taqsimlanishi

(Internet xavfsizlik arxitekturasi )

| Internet arxitekturasi sathi / Xizmat | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| O‘zaro ta’sirlashadigan sub’ektni autentifikatsiyalash | | | + | + | + |

| | | | | | |
|---|---|---|---|---|---|
| Ma’lumotlar manbaini autentifikatsiyalash | | | + | + | + |
| Ulanishni boshqarish | | | + | | + |
| Virtual ulanishning konfidensialligi | | + | + | + | + |
| Ulanish o‘rnatilmasdan axborot almashinuvining konfidensialligi | | + | + | + | + |
| Alohida maydonlarning konfidensialligi | | | | | + |
| Trafik oqimlarining konfidensialligi | + | | + | | + |
| Virtual ulanishning yaxlitligi | | | + | + | + |
| Keyingi qayta tiklashsiz ulanishning yaxlitligi | | | + | + | + |
| Virtual ulanishni tashkil etishda alohida maydonlarning yaxlitligi | | | | | + |
| Ulanish o‘rnatilmasdan axborot almashinuvining yaxlitligi | | | | | + |
| Manbaning soxta rad etishidan himoyalash | | | | | + |
| Oluvchining soxta rad etishidan himoyalash | | | | | + |

### 11.6.1. ISO xavfsizlik arxitekturasi tamoyillari

ISO 7498-2 xalqaro standartda xavfsizlik arxitekturasining quyidagi yettita tamoyillari tavsiya etilgan:

1) tarmoq arxitekturasi sathlaridan faqat bittasida xavfsizlikni ta’minlashni u yoki bu usuli qo‘llanilishi kerak (u takroran qo‘llanilmasligi lozim);

2) tarmoq arxitekturasining ikki yoki undan ortiq sathlarida xavfsizlikni ta’minlashniu yoki bu usulidan foydalanishga ruxsat etiladi. Ravshanki, berilgan bu tavsiya birinchi tamoyilga ziddir;

3) xavfsizlikni ta’minlash usullari himoyalanadigan tarmoq arxitekturasida ko‘zda tutilgan axborot almashishni ta’minlash usullarini takrorlamasligi kerak. Agar usul, masalan, xabarlarning ketma-ket raqamlaridan foydalanish yoki xatoliklardan himoyalashni ko‘zda tutsa, u holda bu mexanizmlar mos axborot almashishni ta’minlash usullaridagi asosiy mexanizmlarni takrorlanishiga emas, balki faqat xavfsizlikni ta’minlashga yo‘naltirilishi kerak;

4) himoyalanadigan tarmoq arxitekturasi sathlarining bog‘liq emasligi, ularda xavfsizlikni ta’minlashning turli usullarini amalga oshirish tufayli buzilmasligi kerak. Bu tamoyilga rioya qilish zarurati ayon. Lekin bu tarmoq arxitekturasi sathlaridan biridagi xavfsizlikni ta’minlash usuli yaqindagi (yoki boshqa) sathdagi xavfsizlikni ta’minlash usulining ishlashini hisobga olmasligini bildirmaydi. Lekin bu o‘zaro ta’sirlashish ochiq bo‘lishi va standart interfeyslardan foydalanishga asoslanishi kerak;

5) qo‘llaniladigan xavfsizlikni ta’minlash usuli minimal xavfsizlik vositalari soni bilan amalga oshirilishi kerak. Bu tamoyilning natijasi,xavfsizlikni ta’minlash usullari, terminallar va foydalanuvchilar orasida axborot almashish amalga oshiriladigan o‘tish (end-to-end) ulanishini oxirgi nuqtalarida, xavfsizlik vositalarini jamlash maqsadida tarmoq arxitekturasining yuqoriroq sathlarida joylashtirilishi kerakligi hisoblanadi. Boshqacha aytganda, aloqa seansini oraliq ishtirokchilarining xavfsizlik vositalariga ishonish kerak emas;

6) agar tarmoq arxitekturasining bitta sathini xavfsizligini ta’minlash usuli (vositasi) boshqa sathning xavfsizligini ta’minlash usuli (vositasi) bilan o‘zaro ta’sirlashishsa, u holda bu o‘zaro ta’sirlashishga tizimning boshqa jarayonlari tomonidan ta’sir bo‘lmasligi kerak;

7) tarmoq arxitekturasi sathlaridan birida xavfsizlikni ta’minlash usullarining (vositalarining) kiritilishi oxirgi foydalanuvchilarni axborotli o‘zar ta’sirlashuvini ta’minlashning asosiy usullarini (vositalarini) imkoniyatli takomillashtirishga to‘sqinlik qilmasligi kerak. Bu tamoyil o‘zaro ta’sirlashni axborotli almashishni

yangi protokollari va interfeyslarini ishlab chiqish va amalga oshirishni soddalashtiradi, bu Internetda juda muhimdir.

### 11.6.2. DOD xavfsizlik arxitekturasi tamoyillari

MAT xavfizligini ta’minlashga DODning konseptual qarashlari quyidagi uchta asosiy g‘oyalarga asoslanadi:

1) konfidensiallikni ta’minlash — bu tarmoq xavfsizligini ta’minlashning asosiy usuli hisoblanadi;

2) maksimal yuqori xavfsizlik darajasini ta’minlash;

3) “kompyuterlarga prinsip jihatdan ishonish kerak emas”.

DOD taklif etgan xavfsizlik arxitekturasi o‘z kelib chiqishini Internetning asosini tashkil etadigan TCP/IP-protokollar to‘plamidan oladi. DOD dastlab xavfsizlik konsepsiyasi ishlab chiqilgan, u o‘z navbatida, keyingi MAT xavfsizlik arxitekturasini ishlab chiqilishiga katta ta’sir ko‘rsatdi. Umuman olganda DOD xavfsizlik arxitekturasi ochiq tizim sifatida zamonaviy Internet-tarmoq uchun to‘g‘ri kelmaydi, lekin uning tamoyillarini ko‘pchiligidan foydalanish mumkin. DOD xavfsizlik arxitekturasining asosiy tamoyillari quyidagilar:

- minimum imtiyozlar (“har bir o‘ziga joizni biladi”). U faqat ma’lumotlarga ishlov berish uchun qonuniy asosga ega bo‘lgan MAT elementlari, bu ma’lumotlarga ulanishga ega bo‘lishi kerakligini bildiradi. Bu tamoyil oraliq tarmoq komponentlariga bog‘liqlikni minimallashtiradi. Bu oraliq nimtarmoqlarda ishlatiladigan tarmoq texnologiyalariga bog‘liq bo‘lmagan va oraliq tizimlarga (masalan, marshrutizatorlarga) ta’sir qila olmaydigan usullar bilan oxirgi tizimlar orasida uzatiladigan ma’lumotlarni himoyalashga imkon beradi;

- vakolatlarni tekshirish tizimlari (reference monitors) sifatida ishlaydigan maxfiy (himoyalangan) operatsion tizimlarni ishlab chiqish. Bunday tizimlar, bir tomondan, ular himoyalaydigan resurslarga sub'ektlarning barcha murojaatlarini ta'minlashi, boshqa tomondan esa, resurslarni sub'ektlarning ruxsat etilmagan ulanishidan himoyalashi kerak;

- konfidensiallikning ustivorligi. Axborot xavfsizligining maqsadi ma'lumotlarning konfidensialligini ta'minlash hisoblanadi, bu boshqa usullarning (masalan, ma'lumotlarning yaxlitligini ta'minlash) rolini sezilarli kamayishini ko'zda tutadi;

- xavfsizlikni ta'minlash imkoniyati emas balki xavfsizlikni ta'minlashni kafolatlanganligi. Bu tamoyil aborot xavfsizligini ta'minlash vositalariga amal qiladi.

Qurilmali vositalar (hardware) yuqori (kafolatlangan) xavfsizlik darajasini ta'minlaydigan maxsus (sinchiklab ishlab chiqilgan) qurilmalar hisoblanadi. Bunday qurilmalarda dasturiy ta'minotning qo'llanilishi, uni MATda ishlatiladigan protokollar va interfeyslarga moslashtirish zarur bo'ladigan hollardan tashqari minimumga keltirilgan.

Tijorat (ommaviy) kompyuter qurilmalaridan foydalanish nuqtai nazaridan AQSh axborot xavfsizligi, xavfsizlikni ta'minlashning dasturiy vositalarini sinchiklab ishlab chiqish, tahlil qilish va ulardan foydalanishga asoslangan. Shu bilan birga, DOD haligacha dasturiy vositalar taqdim etadigan xavfsizlikni qurilmali vositalari ta'minlaydigan xavfsizlikdan ancha past hisoblaydi. Bundan tashqari, tarmoq xavfsizligiga DODning yondashishi himoyalanadigan kompyuter va u ulangan ma'lumotlarni uzatish tarmog'i orasida "oraliq bo'g'indan" (kafolatlangan xavfsizlik vositalari, masalan, vakolatlarni tekshirish tizimlaridan) foydalanish zaruratiga asoslanadi. Aks holda kompyuter tizimiga (xususan, operatsion tizimga) yuqori ishonch darajasini bo'lishi zarur bo'ladi. Bunga yaqin orada erishib bo'lmaydi.

**Tarmoq (IP) sathida konfidensiallikni ta'minlash**

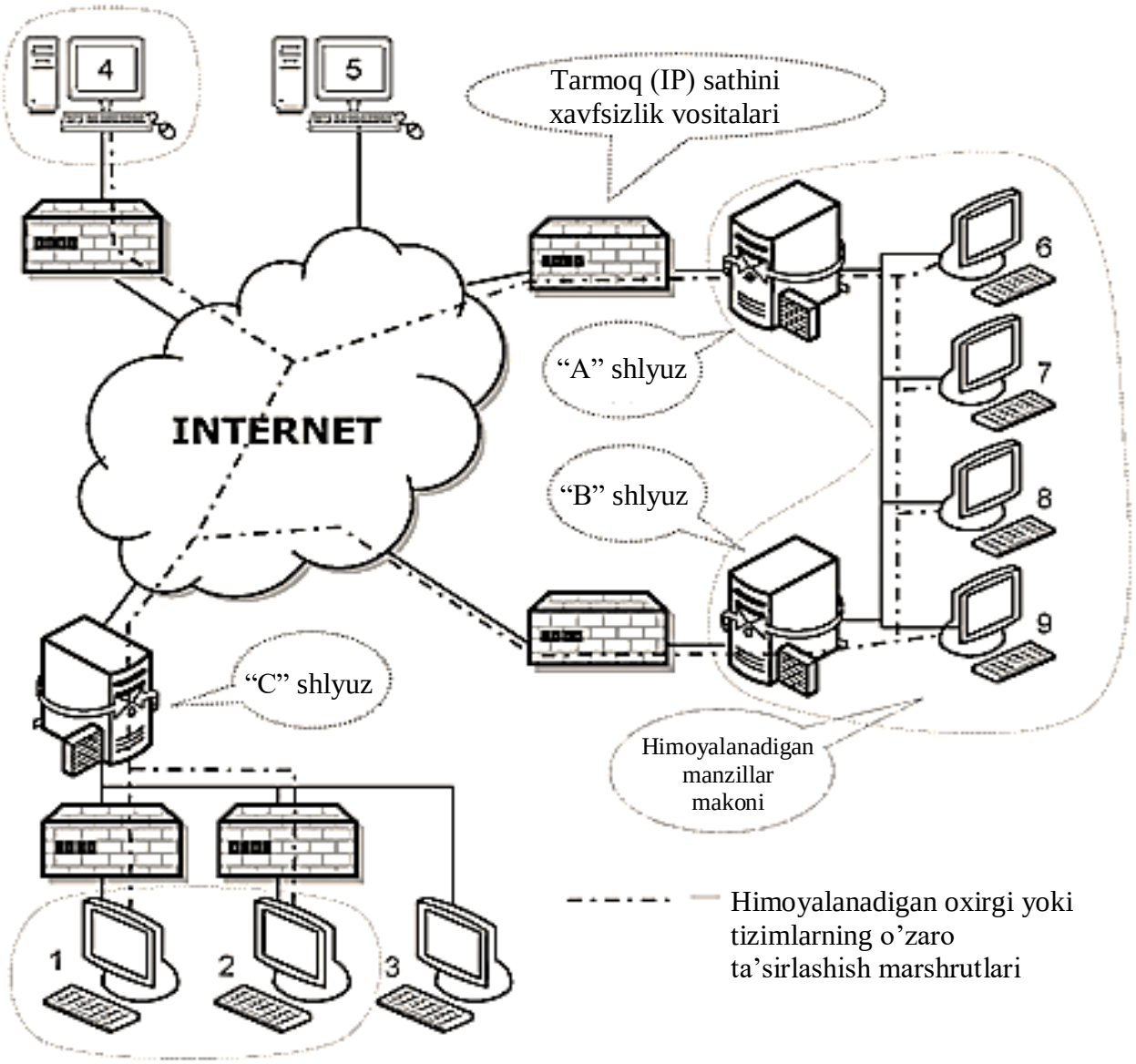
“Ishonchsiz paketlar kommutatorlariga” bog‘liqlikni minimallashtiradigan tarmoq xavfsizligi tizimini ta’minlash uchun DOD tarmoq sathi xavfsizligi vositalarini (qurilmalarini) ishlab chiqishga asosiy urg‘u berdi. Bunday qurilmalar oraliq kommutatorlarga bog‘liq bo‘lmagan holda, jo‘natuvchidan oluvchiga butun yo‘lda uzatiladigan xabarlarni himoyalashi mumkin. Bunda ular istalgan amaliy protokol xabarini bu protokol ulanish o‘rnatadigan yoki ulanish o‘rnatmaydigan protokol (ya’ni TCP yoki UDP) hisoblanishidan qat’iy nazar himoyalashi mumkin. Bu qurilmalar axborot xavfsizligini ta’minlashning konfidensiallik, ulanishni boshqarish, autentifikatsiyalash va yaxlitlik usullarini ishlatadi.

Lekin o‘ta muhimki, tarmoq (IP) sathida xavfsizlik usullarining ishlatilishi kompyuterlarga nisbatan tashqi (alohida) xavfsizlik vositalarini ishlab chiqish mumkin. Natijada, bunday vositalar ko‘p sonli “ishonchsiz kompyuterlar” manfaatlarida qo‘llanilishi mumkin. 11.5-rasmda bu vositalar qo‘llanilishi mumkin bo‘lgan joylar (LHT va global MAT) tasvirlangan.

Tarmoq darajasi xavfsizlik vositalarining boshqa muhim xususiyati, ular nafaqat alohida kompyuterlar, balki marshrutizatorlarda ham qo‘llanilishi mumkinligi hisoblanadi. Oxirgi holatda butun LHT himoyalanadi. Agar lokal (korporativ) tarmoqda ishonchsiz kompyuterlar bo‘lsa va ular bir xil konfidensiallik darajasili ma’lumotlarga ishlov bersa, u holda himoyalash darajasi talab qilinadigan darajaga mos tushadi. Agar lokal (korporativ) tarmoqda “ishonchli va ishonchsiz” kompyuterlar bo‘lsa, u hollarda tarmoq xavfsizligi vositalari, manbalari faqat bir yoki bir necha global tarmoqlar (masalan, Internet) hisoblangan tashqi tahdidlardan himoyalashni ta’minlaydi. Lekin himoyalash tizimining bunday konfiguratsiyasi eng kam imtiyozlar prinsipini qoniqtirmaydi, chunki barcha kompyuterlar (bitta lokal/korporativ tarmoqdagi) bir xil himoyalash darajasiga ega bo‘ladi, bu real sharoitlarda amalga oshmasligi mumkin.

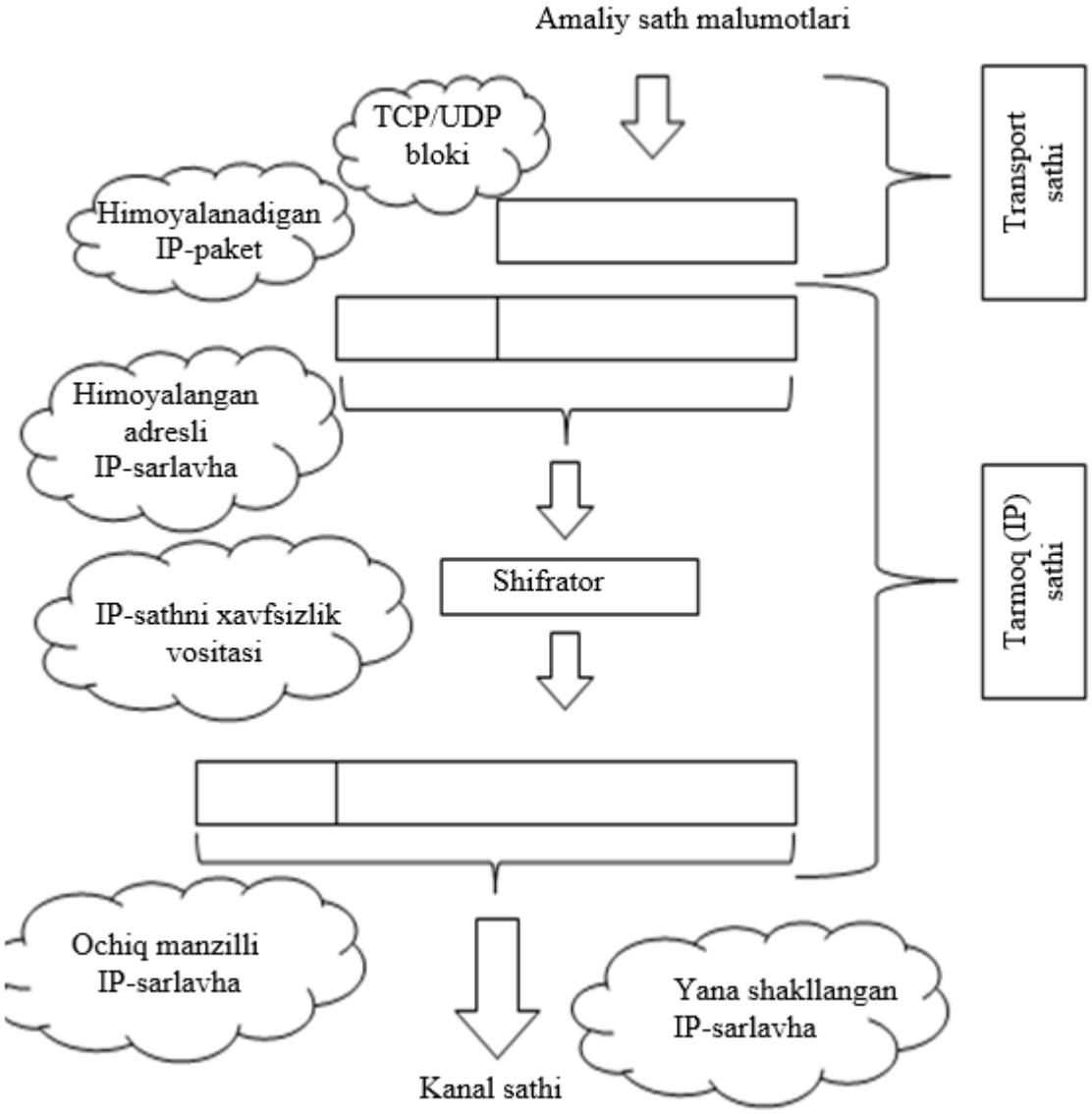
Eng kam imtiyozlar prinsipi amalga oshirilganida (ulanish darjalari bo‘linganida) ochiq tizimlarda tarmoqda bir vaqtda himoyalangan va

himoyalanmagan paketlar kommutatorlari (marshrutizatorlari) bir vaqtda ishlaganida “yashirin kanallarni boshqarish” muammosi vujudga keladi. Bir tomondan, tarmoqdagi mavjud barcha marshrutizatorlarga mumkin bo‘lgan IP-adreslashtirish tizimi zarur, boshqa tomondan esa IP-adreslashtirish tizimi himoyalangan marshrutizatorlar uchun zarur bo‘ladi. Agarbu ikkala adreslar tizimlari fizik ajratilmagan bo‘lsa va ular tarmoq bo‘ylab bir vaqtda translyatsiya qilinsa, u holda bunday vaziyat “troya otlari” uchun himoyalash vositalarini “chetlab o‘tish”, ya’ni aylanma marshrutlardan foydalanish bo‘yicha katta imkoniyatlarni beradi.



11.5-rasm. Tarmoq (IP) sathini xavfsizlik vositalari

“Aylanma marshrutlardan” foydalanish muammosini yechish va IP-paketlar sarlavhasidagi manzillar va boshqa ma’lumotlarni “inkor etish” uchun AQSh mudofaa vazirligi tomonidan “ikkilangan tarkibiy tarmoq” (catenet) modeli taklif etilgan. Bu modelda (11.5-rasm) IP-sathni xavfsizlik vositalari, IP-paketlarni ikkilangan (takroriy) shaklga solish funksiyasi yordamida adreslar muhitining chegarasi bo‘lib qoladi (11.6-rasm). Shuning uchun himoyalaydigan oxirgi va oraliq tizimlar qo‘llaydigan adreslar, himoyalanmaydigan oxirgi va oraliq tizimlar qo‘llaydigan adreslardan to‘liq farqlanadi.



11.6-rasm. IP-paketlarni ikkilangan (takroriy) shaklga solish funksiyasi

Shu bilan birga, ikkita adresli muhitlar ishlagan sharoitlarda ayrim oxirgi yoki oraliq tizimlar o‘zaro ta’sirlasha olmaydi. Masalan (11.5-rasm), "A" va "V" shlyuzlar (marshrutizatorlar) va 6, 7, 8 va 9-kompyuterlar “S” shlyuz (marshrutizator) bilan o‘zaro ta’sirlasha olmaydi.Va aksincha, 3 va 5-kompyuterlar (xavfsizlik qurilmalarisiz) "A" va "V" marshrutizatorlarning borligini bilmaydi, shuningdek, bu marshrutizatorlarga ulangan LHTning borligini ham bilmaydi.

**Kanal sathida konfidensiallikni ta’minlash**

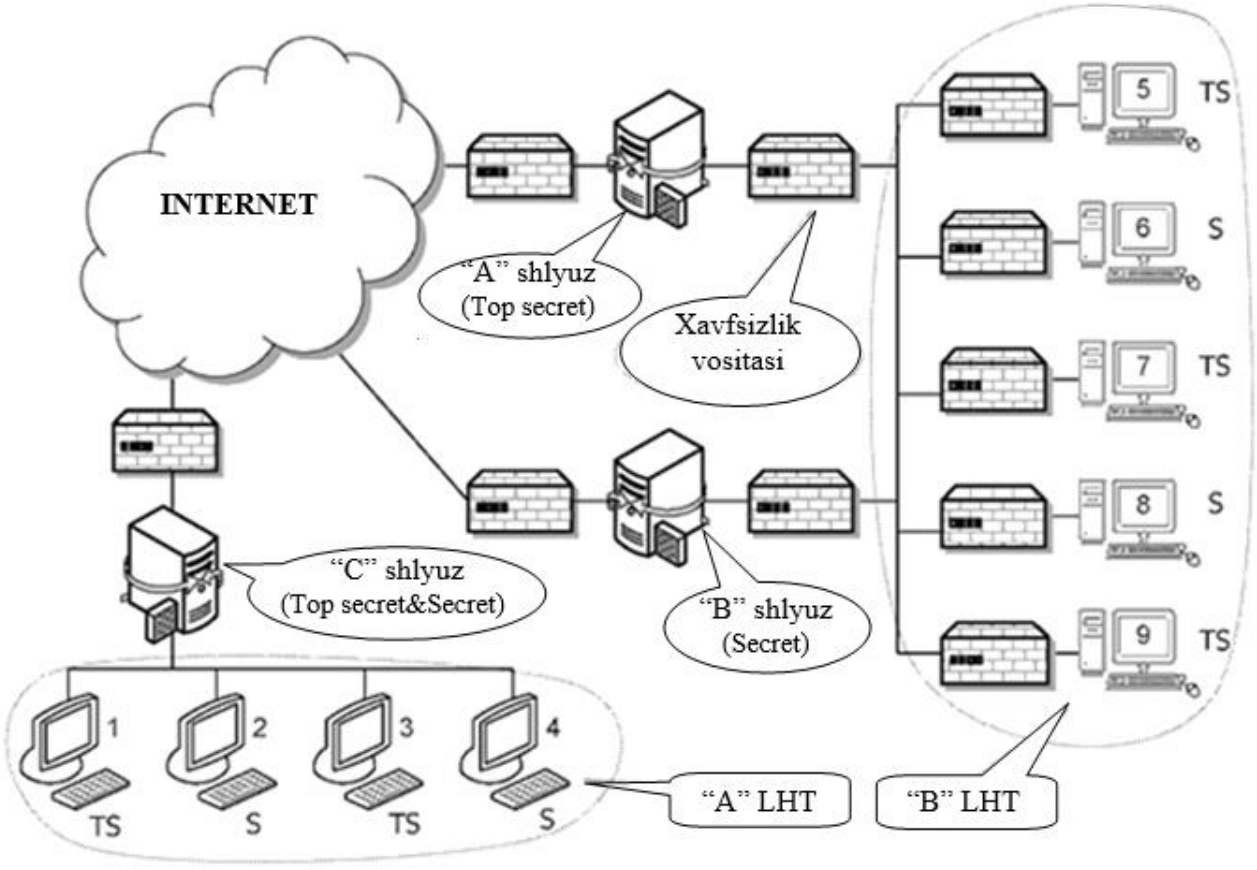
Prinsip jihatdan, IP-sathni xavfsizlik vositalari (qurilmalari) har bir kompyuterda mos interfeyslar bo‘lganida LHTda qo‘llanilishi mumkin. Lekin, DOD g‘oyasidan kelib chiqqan xolda, bunday qurilmalar LHTni global MATlarga (masalan, Internetga) ulash uchun qulayroq. Shuning uchun kanal sathining xavfsizlik vositalari IP-sathning xavfsizlik qurilmalariga nisbatan qo‘shimcha hisoblanadi. Shu bilan birga, ular ma’lumotlar uzatishni turli rejimlari va protokollarini ishlatadigan murakkab integral tarmoqlarda ishlaganda afzalroq. Kanal sathining xavfsizlik vositalarining muhim afzalligi ko‘p sathli maxfiy LHTlarni yaratish imkoniyati hisoblanadi, keyin ular IP-sathni xavfsizlik vositalarini qo‘llash bilan qurilgan ko‘p sathli global tarmoqlarga ulanishi mumkin.

Masalan, 11.7-rasm bunday bog‘lanishning ikkita usulini ko‘rsatadi. “A” va “V” LHTlarning har ikkalasi ko‘p sathli hisoblanadi, ularning har birida “Secret” va “Topsecret”konfidensiallik darajali kompyuterlar bo‘ladi. “A” LHT, konfidensial ma’lumotlarga cheklangan ulanishda ishchi stansiyalarda ishonchli dasturiy ta’minotga tayanadi. “V” LHT, undagi trafikni bo‘lish uchun tashqi kriptografik

qurilmalarni qo‘llaydi. “A” LHT, xabarlarda xavfsizlik griflari va kriptografik usullar yordamida ulanishni chegaralashni ta’minlay oladigan global tarmoqning xavfsizlik qurilmasiga ulanish uchun bitta ishonchli marshrutizatorni (“S”shlyuzni) qo‘llaydi.

“V” LHT ikkita “ishonchsiz” marshrutizatorni (“A” va “V” shlyuzlar – xar bir xavfsizlik sathiga bittadan) va global tarmoqni ikkita xavfsizlik qurilmalarini ishlatadi, ulardan har biri global tarmoqda o‘xshash ulanishlarni ta’minlash uchun faqat bitta xavfsizlik sathi bilan chegaralangan.

Prinsip jihatdan, har ikkala yondashishlar korporativ LHTlarda AXni ta’minlash uchun qo‘llanilishi mumkin.



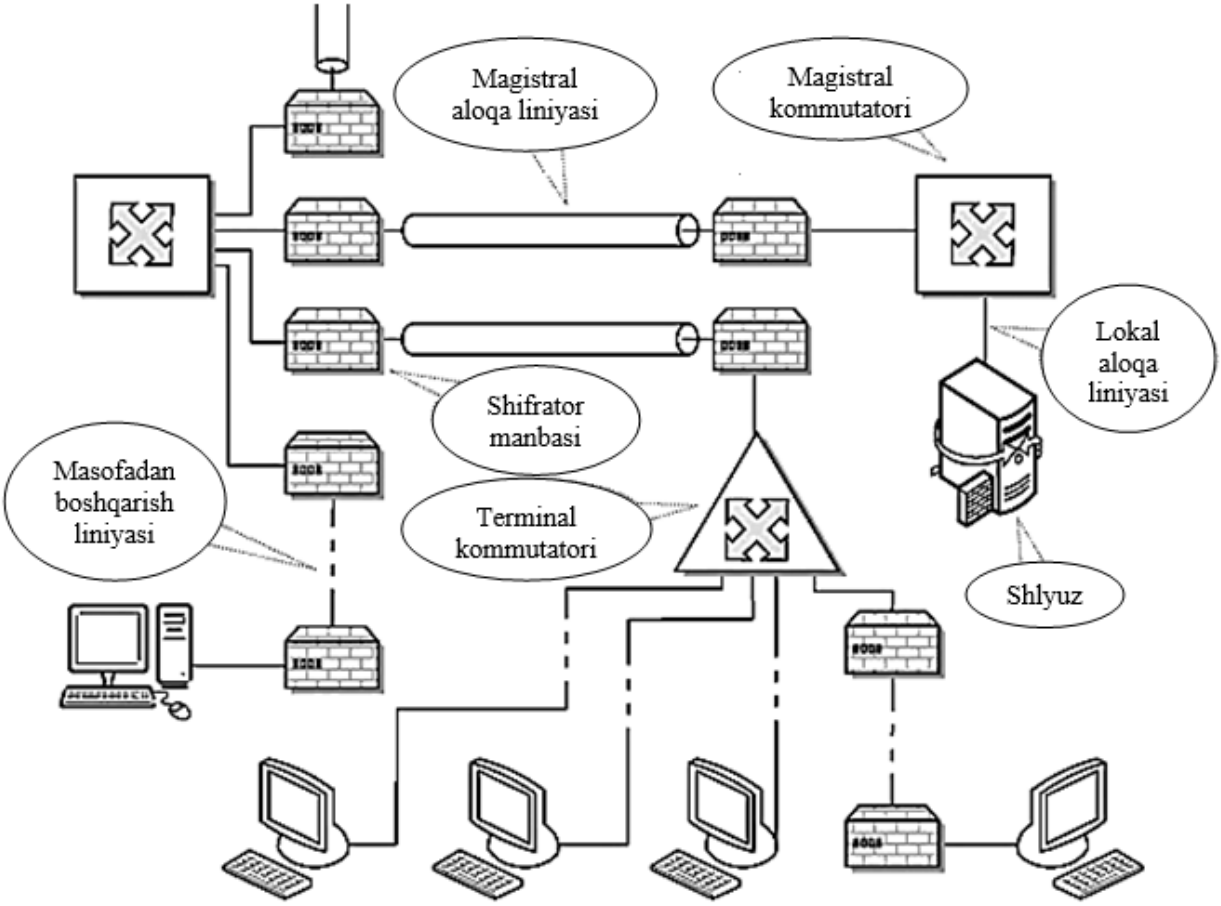

11.7-rasm. Kanal (MAC) sathining xavfsizlik vositalari

**Fizik sathda konfidensiallikni ta’minlash.**

Fizik sathning xavfsizlik vositalari (ko‘pincha kanal (liniyali) shifratorlari deyiladi) yangi tarmoq muhitida ma’lum kriptografik usullarni muvaffaqiyatli qo‘llanilishiga misol hisoblanishi bilan paketlar kommutatsiyasi tarmoqlar paydo bo‘lguncha qo‘llanilgan tarzda MATda ham qo‘llaniladi.

Bu vositalar konfidensiallikni, asosan, oxirgi qurilmalar orasidagi aloqa (point-to-point) liniyalarida (kanallarida) ma’lumotlar oqimining konfidensialligini ta’minlaydi. 11.8-rasm tarmoq muhitida fizik sathda shifrlash qurilmalari qo‘llanilishi mumkin bo‘lgan bir necha “nuqtalarni” ko‘rsatadi. Shifratorlar ajratilgan, kommutatsiyalanadigan va magistral aloqa liniyalarida qo‘llanilishi mumkin. Bu maxsus qurilmalar o‘zaro konstruktiv kanallarning o‘tkazish qobiliyatidagi farq tufayli farqlanishi mumkin, ularda qo‘llaniladigan asosiy kriptografik usullar esa bir xil bo‘ladi.

Fizik sathda shifrlash qurilmalari bilan himoyalangan global tarmoq, paketlarga shifrlanmagan ko‘rinishda ishlov beriladigan kommutatorlardan har birida zaif bo‘ladi. Fizik sathda faqat shifrlashni qo‘llaydigan tarmoq, kommutatorlar to‘g‘ri ishlayotganiga “ishonch hosil qilishi” kerak (aks holda, noto‘g‘ri marshrut bo‘yicha yo‘naltirilgan marshrut xavfsizlikni buzishi mumkin).




11.8-rasm. Fizik sathning xavfsizlik vositalari

Ma’lumki, agar tarmoq bir necha xavfsizlik darajalariga ega bo‘lsa(masalan, “Secret” va “Topsecret”) va faqat kanallarni shifrlash ko‘zda tutilsa (xatto, agar kommutatorlar yetarlicha ishonchli kommutatsiyalash mexanizmlari va algo-ritmlarini ishlatsa), u holda eng kam himoyalangan kommutator (fizik, xavfsizlik protsedurali va “inson omilining” mavjudligi nuqtai nazaridan) butun tarmoqni oshkor etishi mumkin bo‘lgan vaziyatni yuzaga kelish imkoni mavjud bo‘ladi.

**Gibrid tizimlar.** Real tizimlarda DOD xavfsizlik arxitekturasi barcha uchta sathda xavfsizlik vositalari va usullariga asoslanadi. 11.9-rasmda bunday tizimga misol keltirilgan, unda fizik, MAC- va IP-sathlar birgalikda axborot himoyasini ta’minlash uchun qo‘llaniladi, aynan:

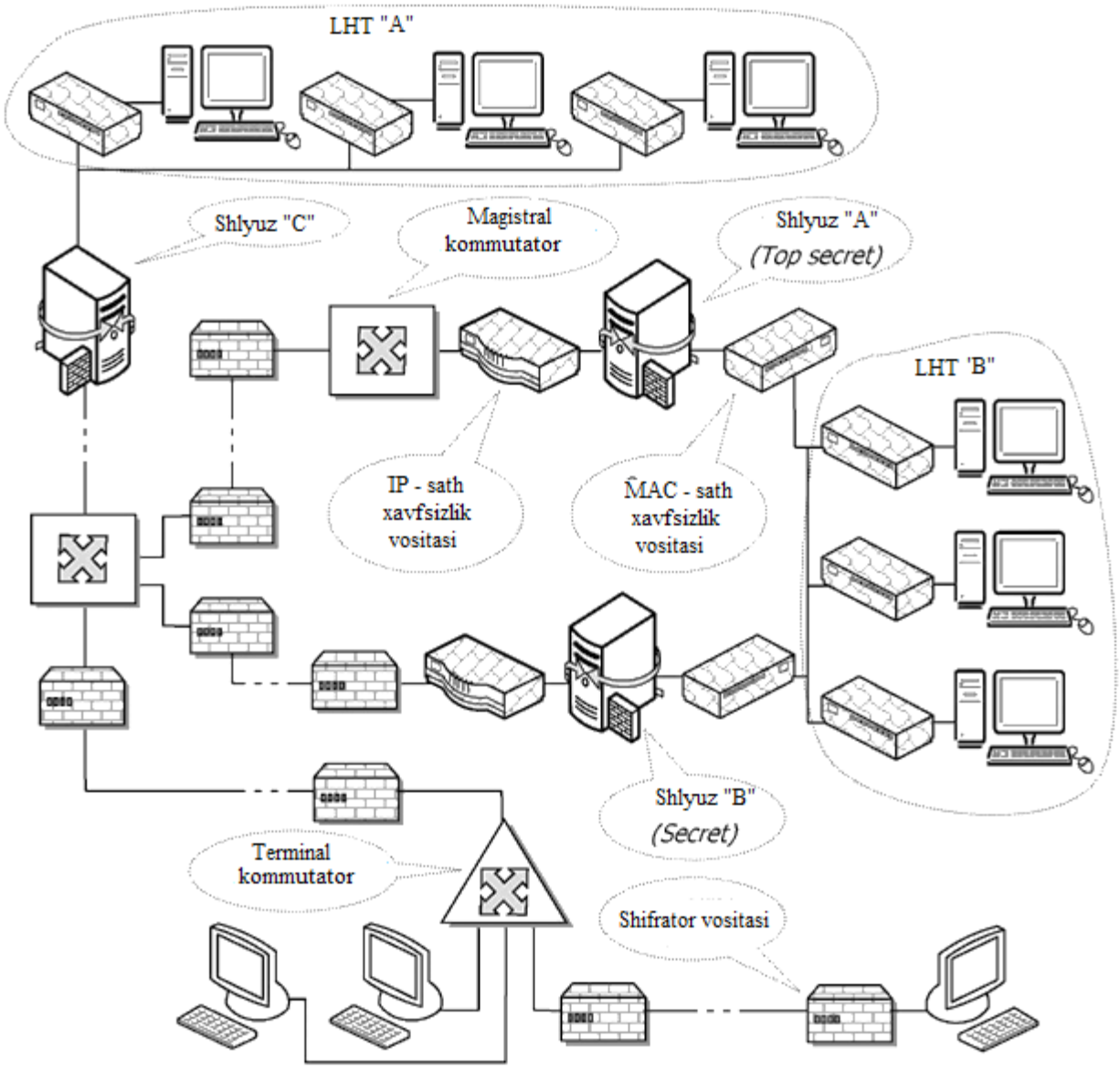
- fizik sath qurilmalari kommutatsiyalangan lokal aloqa liniyalarini himoya qilish uchun (abonent trafikini (konfidensiallikni ta’minlash) himoya qilish), global tarmoqlarga olisdanulanishuchun aloqa liniyalari (ma’lumotlar oqimi va abonent trafikini himoya qilish uchun (konfidensiallikni ta’minlash)), global tarmoqlarni kommutatorlari orasida magistral aloqa liniyalarida (ma’lumotlar oqimini himoya qilish uchun (konfidensiallikni ta’minlash)) qo‘llaniladi;

- LHTda MAC-sathni “A” qurilmasi konfidensiallikni, kirishni boshqarish, yaxlitlik va autentifikatsiyani (yoki bu xizmatlarni yanada yuqori sathlarda qo‘llab-quvvatlashni) ta’minlaydi;

- LHTda “V” va global tarmoqqa ulangan marshrutizatorlarda (shlyuzlar "A" va "V"), IP-sathni qurilmalari IP-paketlarni konfidensialligini, kirishni boshqarishni va IP-paketlar uchun yaxlitlikni, shuningdek ma’lumotlar manbaini autentifikatsiyasini ta’minlaydi.

DOD modelining kamchiliklari. Ma’lumki, DOD xavfsizlik arxitektura modelida amaliy sathni axborot xavfsizligi haqida hech nima deyilmagan. Bu - tasodif emas, bu o‘sha davrdagi DOD qarashlarining tabiiy o‘rinishlari, u davrda xavfsizlik arxitekturasi va paradigmalari yaratilgan.

Eng nozik bo‘g‘inlardan biri (DOD xavfsizlik arxitekturasi nuqtai nazaridan) Internet segment/sohalarini nomlash tizimi (DNS — Domain Name System) hisoblanadi. Birinchi navbatda DNS, amaliy sathning turli adreslash tizimlarini tarmoq adresida (IP-adres) aks ettirish masalalarini yechadi (HTTP, FTP, SMTP, NNTP va b.q) va IP-paketni yetkazib berish marshrutini aniqlashda ishtirok etadi. Shuning uchun, DOD xavfsizlik modeli umuman DNSdan foydalanishni rad etadi.




11.9-rasm. Uch sathli Internet - arxitekturasida (gibrid tizim) xavfsizlik vositalarini kompleks qo‘llanilishi

Bu vakolatlarni tekshirish tizimi sifatida ishlaydigan maxfiy (himoyalangan) operatsion tizimni qo‘llash, xavfsizlik arxitekturasining muhim prinsipi hisoblanadi.

Fizik, kanal (MAS) va IP-sathlarning xavfsizlik vositalari, vakolatlarni tekshirish tizimini amalga oshiradi. Bu vositalar kommunikatsion interfeyslar bilan ketma-ket ulangan tashqi apparat-dasturiy qurilmani aks ettiradi, bu o‘z navbatida o‘rnatilgan vakolatlarni tekshirish tizimlarini (himoyalangan operatsion tizim

yadrosida) ruxsatsiz ulanishdan (oxirgi va oraliq tizimlarda ishonchsiz DT) himoya qilish va himoyalangan ob'ektlarga kirishni nazorat qilish imkonini beradi. *DOD xavfsizlik arxitekturasiga muvofiq amaliy sathda axborot xavfsizligini samarali ta'minlash uchun himoya tizimi asosi sifatida maxfiy operatsion tizimni qo'llash kerak.*

DOD arxitekturasida amaliy sathni xavfsizligini mashxur bo'lmasligining yana bir sababi, kirishni qat'iy reglament asosida ma'muriy boshqarish hisoblanadi (ma'lum qoidalar asosida). Bunda har qanday o'xshashlik bo'lmay, ayniqsa foydalanuvchilar autentifikatsiyasi amaliy sathda amalga oshirilgani uchun (uchinchi sub'ekt axborot almashishni qo'llab - sertifikatlashtirish markazi yoki kalit axborotni taqsimlash markazi) foydalaniladi, tarmoq arxitekturasining uchta quyi sathlarida qo'llanilmaydi. DOD modelidagi asosiy urg'u (elektron pochtadan tashqari, unda jo'natuvchi va qabul qiluvchilarni identifikatorlari muhim) konfidensial axborotni turli sathlarga bo'luvchi va bu axborotga "troyan otlarining" ruxsatsiz kirishidan himoya qilishga qaratilgan qoidalarga beriladi.

Avvalombor, DOD xavfsizlik arxitekturasida avvalgidek asosiy e'tibor uchta quyi sathni xavfsizlik vositalariga qaratiladi. Shunga qaramay, amaliy sathni xavfsizlik vositalari qo'llanish doirasini topadi, faqat quyi sathning xavfsizlik vositalari kerakli xavfsizlik darajasini ta'minlay olmaganda. Tizimli va amaliy jarayonlar DODning yuqori talablariga javob beradigan, maxfiy axborot texnologiyalarini ishlab chiqish va amalga oshirish uchun yetarlicha kafolatni ta'minlaydi.

### 11.6.3. Internet (IETF) xavfsizlik arxitekturasi tamoyillari

Internet-tarmog'i ochiq tizim sifatida ISO xavfsizlik arxitekturasi prinsiplariga asoslanadi, qisman – DOD ning ba'zi boshqa prinsiplariga asoslanadi. Bundan tashqari, IETF quyidagi qo'shimcha prinsiplarni aniqlab berdi:

- xavfsizlik usullari va vositalari barcha Internet hamjamiyati foydalana olishi uchun sozlanuvchan va moslashuvchan bo‘lishi kerak. Bu prinsip Internet uchun juda dolzarbdir. Bu global tarmoqda katta miqdorda nimtarmoqlar, o‘zining turli noyob adresi va otiga ega kompyuter va foydalanuvchilar mavjud. Shuning uchun qo‘llaniladigan xavfsizlik usullari va vositalari (masalan, ulanishni boshqarish usullari va vositalari hamda autentifikatsiya) istalgan adresli ko‘pginalarga oson moslashishi kerak;

- xavfsizlik usullari va vositalari “shaffof” bo‘lishi kerak. Bu shuni anglatadiki, ularni tahlil qilish (qo‘llanilayotgan algoritmlar va protokollar) ular ta’minlab beradigan xavfsizlik darajasini aniqlash imkonini beradi. Shu munosabat bilan, protokollar va algoritmlarda ichki xatoliklar bo‘lmasligi kerak, ular algoritmik (funksional) “kuchsizlik” natijasi emas, ularni (nokorrekt) noto‘g‘ri amalga oshirish natijasidir;

- xavfsizlik usullari va vositalarini amalga oshirish faoliyatiga MAT topologiyasi ta’sir ko‘rsatmasligi kerak. Masalan, faqat bitta marshrutizator yordamida boshqa MATga ulangan alohida korporativ LHT uchun qo‘llanilishi maqsadga muvofiq emas;

- Internet da foydalanishga xalqaro foydalanish uchun mumkin bo‘lgan va ularni eksport/import qilishda hech qanday cheklovlarga ega bo‘lmagan, xavfsizlikning usul va vositalari qulay. Shunga qaramay, Internet xavfsizligi faqat shuning uchun qo‘llanishda chegaralangan. Axborot xavfsizligi sohasida eksport/import uchun chegaralangan juda ko‘p usul va algoritmlar (protokollar) mavjud. IETFda ilgaridan amaliy tajriba o‘rnatilgan, unga ko‘ra patent olgan texnologiyalarni standartlashtirish ANSI (American National Standards Institute - Amerika standartlashtirish bo‘yicha milliy instituti) va IEEE (Institute of Electrical and Electronics Engineers – Amerika elektrotexnika va elektronika sohasidagi injenerlar instituti) faoliyati bilan muvofiqlashtiriladi;

- xavfsizlikning ko‘pgina ma’lum usul va vositalari mos keluvchi qo‘shimcha tarmoq infratuzilmasidan foydalanishga, yaratishga, ishlatish va qimmat bo‘lishi mumkin bo‘lgan boshqarishga yo‘naltirilgan. Shuning uchun, xavfsizlikning mavjud yagona infratuzilmasiga yo‘naltirilgan, axborot xavfsizligining yangi texnologiyasini qo‘llash tavsiya qilinadi. Masalan, bunday tuzilma sifatida Xalqaro elektraloqa ittifoqi (ITU-T) yoki IETFRFC-1507 ("Distributed Authentication Security Service") va RFC-4120 ("The KERBEROS Network Authentication Service, v.5") standartlariga muvofiq bo‘lgan X.509 sertifikatsiya tizimi bo‘lishi mumkin;

- Internet da standart sifatida tanlangan kriptografik algoritmlar, mashhur, barcha qo‘llashi mumkin bo‘lgan va iloji bo‘lsa “ochiq adabiyotlarda vaqt davomida sinalgan” bo‘lishi kerak. Boshqa so‘z bilan aytganda, xattoki shifrlash algoritmlari, nazorat summasini hisoblash, elektron imzo va boshqa algoritmlarning yuqori ishonchliligini rasmiy isboti bo‘lmasa ham bunday algoritmlarning eng yaxshikafolati, ularni ochiq adabiyotlarda har tomonlama kritik tahlil qilish bo‘ladi. Albatta, bunday tahlilning o‘zi algoritm ishonchli ekanligini kafolatlamaydi, ammo uni standartlashtirish jarayonining muhim qismi hisoblanadi. Istalgan xususiy algoritmlarni bunday tahlillar uchun foydalanib bo‘lmaydi.

**Internet va DOD xavfsizlik arxitekturalari orasidagi farq.**

Asosan DOD hisoblanadigan Internet xavfsizlik arxitekturasi, DOD arxitekturasidan bir necha jixatlari bo‘yicha farq qiladi.

*a).* DOD arxitekturasi xavfsizlikni ta’minlashning asosiy usuli sifatida axborot konfidensialligini (shifrlashga) ta’minlashga asosiy e’tibor qaratadi, bunda ma’lumotlar ketma-ketligini konfidensialligi eng muhim hisoblanadi. Bunday yondashuv sabablari ma’lum: maxfiy axborotni himoyalash va “troyan otlari”dan himoyalash. Bundan tashqari, DOD arxitekturasida qat’iy belgilangan ulanishning ma’muriy boshqaruviga urg‘u beriladi (ma’lum qoidalar asosida).

Internet da axborotlarni shifrlash vositalari keng qo‘llaniladi, biroq global tarmoqda liniyali (kanalli) shifratorlarni qo‘llash kam uchraydi. Boshqa so‘z bilan

aytganda, Internet da ma’lumotlar oqimini konfidensialligini ta’minlashga qat’iy talablar yo‘q.

Shu bilan birga, xalqaro, milliy, regional va territorial Internet segmentlariga xizmat ko‘rsatuvchi tarmoq kompaniyalari, ma’lumotlar uzatish tarmog‘ining normal ishlashini ta’minlab beruvchi maxsus xizmat axborotlari uzatiladigan boshqaruv kanalini himoyalashga e’tibor qaratadi. Biroq, xizmat axboroti foydalanuvchi axboroti bilan bir oqimda uzatiladi, shuning uchun tarmoqning turli segmentlarini egalari, magistral kanallarni himoyasi uchun fizik sathda shifrlashni qo‘llab, bir vaqtning o‘zida ikkala ko‘rinishda uzatiladigan axborotlarni himoyalaydi (Internet foydalanuvchilari axborotni kriptografik himoyalashni talab qilmasa ham bo‘ladi). Shuning uchun ushbu aspektda aniq qarama-qarshiliklar mavjud.

*b)*. DOD arxitekturasining keyingi muhim jihati maxfiy (himoyalangan) operatsion tizim bo‘lib, vakolatlarni tekshirish tizimi sifatida faoliyat yuritadi (bu tijorat kompyuterlariga “ishonchsizlik” natijasi hisoblanadi).

DOD arxitekturasining ushbu prinsipini Internet arxitekturasi uchun ham qo‘llab bo‘lmaydi. Global tarmoq uchun (tijorat kompyuterlarini ommaviy qo‘llashga yo‘naltirilgan ochiq tizim sifatida) foydalanuvchilarga xavfsizlik usullari va vositalarini maksimal darajadagi spektrini taqdim qilish maqsadga muvofiq bo‘ladi, bunda axborotlarni himoyalash bo‘yicha har qanday kafolatlarni rad etadi. Masalan, Internetning ko‘pchilik foydalanuvchilari ishchi stansiya uchun qo‘shimcha dasturiy ta’minot o‘rniga, aloxida kompyuter uchun qo‘shimcha tashqi kriptografik qurilmaga (qimmat bo‘lgan) pul to‘lashini tasavvur qilish qiyin. Bundan tashqari, Internet foydalanuvchilarining ko‘pchiligini, xavfsizlik nuqtai nazaridan oxirgi va oraliq tizimlarda qo‘llaniladigan, xavfsizlik usullari va vositalarining ishonchliligi qiziqtirmaydi. Ularni ko‘proq axborotni himoyalashning tezkor vositalari qiziqtiradi.

Internet foydalanuvchilarning ko‘pchiligi noqonuniy ulanishlardan himoyalanish uchun IP-adreslash asosidagi paketli filtrlashni qo‘llaydi. Bunday filtrlash unchalik ishonchli emas. Shu bilan birga yuqori darajadagi xavfsizlik

usullari va vositalarini qo‘llash talab etiladi, axborot almashinish sub’ektlarini autentifikatsiyasi, xabarlar yaxlitligi va konfidensialligini ta’minlash hamda identifikatorlar asosida kirishni boshqarish shular jumlasidandir. Biroq bu usullar va vositalarning ishonchliligi eng minimal bo‘lishi mumkin.

*v).* Nihoyat, kriptografik kalitlarni boshqarish sohasida jiddiy farqlar mavjud. DODxavfsizlik arxitekturasi, o‘zining qoidalari asosida kirishning yuqori ishonchli boshqaruviga javobgarligi tufayli, faqat kalitlar orqali markazlashgan boshqaruv tizimlarini ko‘rib chiqadi. Buning sabablaridan biri DODni simmetrik kriptografik tizimlarga yo‘naltirish hisoblanadi, ya’ni juda murakkab bo‘lgan texnologik vazifani aks ettiruvchi “yuqori sifatli” kalitlar generatsiyasini nazarda tutadi, u qat’iy xavfsizlik sharoitida yaxshi amalga oshiriladi. Boshqa so‘z bilan aytganda, agar kirishni boshqarish kalitni tekshirish asosida amalga oshirilsa, u holda bu jarayon faqat yuqori ishonchlilikka ega tizim orqali amalga oshirilishi kerak.

Internet muhitida, kalitlar taqsimlangan asosda generatsiyalanadi, asosan har qanday muvofiqliksiz. Internet da autentifikatsiya asosida kirishni boshqarish qo‘llangani uchun, kalitlar va identifikatorlar orasida katta o‘zaroaloqa mavjud (yoki kalitlar va elektron sertifikatlar orasida). Autentifikatsiyalashni tarmoq tizimidan foydalanish, masalan X.509, hech qanday markazlashtirish talab etilmaydigan o‘zaro aloqani ta’minlaydi.

## 11.7. Internet tarmoqda AX ta’minlash usullari va vositalarini qo‘llash bo‘yicha IETF tavsiflari

AX ta’minlash usullari va vositalari faqatgina ishlashi himoyalangan Internet-protokollarga o‘rnatiladi. AX muammolarining ko‘pchiligi Axni ta’minlash usullarini noto‘g‘ri amalga oshirish natijasida vujudga keladi (o‘rnatishdagi xatoliklar). Biroq Axni ta’minlash usuli to‘g‘ri amalga oshirilgan taqdirda ham AX muammolari paydo bo‘lishi mumkin, chunki fundamental protokol o‘z-o‘zidan

amalda to‘g‘ri ishlashni talab qiladi. Aynan shunday himoyalangan protokolda amalga oshirish zarur bo‘lgan Axni ta’minlash usulida ham turlicha bo‘lishi mumkin, chunki himoyalangan protokol o‘zining shaxsiy ichki tuzilmasiga ega. Shunga qaramay, Internetda standartlashtirilgan AXni ta’minlash usullarini ko‘pgina protokollari mavjud. Usulning aniq tanlanishi turlicha bo‘lishi mumkin, chunki barchasi aniq vaziyatga bog‘liqdir. Ushbu tavsiyada, har birining vazifasi va xususiyatlari tushuntirgan Axni ta’minlash usullari keltirilgan.

Ma’lumki, Axni ta’minlash – bu san’atdir. Internet da Axni obro‘sizlantirish variantlari bir necha guruhlarga bo‘linishi mumkin, ya’ni “xizmat ko‘rsatishdan bosh tortish”dan IP-bog‘lamani obro‘sizlantirishgacha bo‘lgan butun diapazon bo‘ylab. “Xizmat ko‘rsatishdan rad etish” turidagi hujumlar shunga asoslanganki, translyatsiya qilinuvchi trafik ochiq hisoblanadi, biroq AXni obro‘sizlantiradigan bu guruh variantlari ushbu qo‘llanma talablaridan chetga chiqadi, hozirgi paytda bo‘lib o‘tayotgan bunday hujumlar ko‘p munozara va tadqiqotlar ob’ekti bo‘lishiga sabab bo‘lmoqda. Ta’kidlash joizki, bunday hujumlarning ko‘pchiligini amalga oshirish qiyin, chunki hozirgi paytda ulardan himoyalanish bo‘yicha katta tajriba to‘plangan. Avvalambor IP-bog‘lamani obro‘sizlantirish (umumiy hodisa sifatida xotiraning bufer qurilmalarining aniqlab bo‘lmaydigan o‘ta yuklanishi hisoblanadi), IP-bog‘lamada amalga oshirilgan protokollarning o‘zidagi kamchiliklardan ko‘ra, IP-bog‘lamaning dasturiy modulida AX ta’minlash usullarini aniq amalga oshirishdagi kamchiliklar natijasi hisoblanadi. Shunga qaramay, sinchkovlik bilan ishlangan protokollar bo‘lishi mumkin bo‘lgandan kamroq kamchiliklarga ega bo‘lishi mumkin va foydalanishda kamroq mehnat talab qilishi mumkin.

Biroq AXni obro‘sizlantirish variantlari mavjud, ular Internet-tarmoqda qo‘llaniluvchi protokollarning o‘zi bilan murakkablashtiriladi. Agar AX ta’minlash muammosi protokolga xos bo‘lsa, u holda ushbu muammoni rad etuvchi u yoki bu AX ta’minlash usulini amalga oshirish usuli mavjud emas.

Shuning uchun Internet- tarmoq uchun yaratiluvchi barcha protokollar AX ta’minlovchi funksional xususiyatlarga ega bo‘lishi hayotiy ahamiyatga ega. Buni himoyalovchi protokolga Axni ta’minlash usuli tatbiq etilgani kabi, himoyalanayotgan protokol o‘z ichki tuzilmasi asosida o‘zining funksional himoyalanganligini ta’minlashi kerak. Ko‘pgina xollarda AX ta’minlashning standartlashgan IETF usullarini to‘g‘ri qo‘llash, protokolning zarur bo‘lgan himoyalanganlik darajasini ta’minlashi mumkin.

Internet - tarmoqda AX ta’minlash uchun barcha usullardan foydalanish mumkin. Qandayusullardanfoydalanishesabirnechaomillargabog‘liqbo‘ladi.

*AX ta’minlash ilmiy natijalarni qo‘llash ilmi va san’atining kompleks muvofiqlashtirishdan iborat.* Ma’lumotlarni himoyalashning u yoki bu usulini tavsiya qilish falokatga olib kelishi mumkin. Har doimgidek, istalgan protokolni ishlab chiqishda uni har tomonlama testdan o‘tkazish zarur.

Shunday qilib, AX ta’minlash usullari qandaydir “mo‘‘jiza” hisoblanmaydi, ular yordamida protokollarni to‘liq himoyalash mumkin. AX ta’minlash usuli ko‘p vaqtga o‘rnatilmaydi. Yaxshi (ya’ni xavfsiz, shaffof va samarali) loyihalar AX ta’minlash usullarini protokoli bilan birgalikda ishlab chiqilganda hosil bo‘ladi. Kriptografiya aniq semantik nuqsonlarga ega protokollarni himoyalay olmaydi.

Yechim qabul qilishga ta’sir qiluvchi omillar. AX ta’minlash usulini tanlashdagi muhim omillardan biri, bu AX tahdidlar modeli hisoblanadi. Ya’ni kim hujum qilishi mumkin, qaysi axborot manbaiga va qaysi usullarni qo‘llab? Hujumning kam axborotli maqsadi, masalan $W^3$–server singari, ya’ni faqat ochiq axborotni taklif qilib, kuchli himoyaga ega bo‘lmasligi mumkin. Va aksincha, Internet-infratuzilmaning muhim komponentlarini himoyasiz qoldirgan manba, masalan asosiy magistral marshrutizator yoki ierarxiyaning yuqori sathidagi DNS-serveri, Axni ta’minlashni juda ishonchli usullari va vositalari yordamida himoyalangan bo‘lishi kerak. Muhimligi, hujum qilish maqsadiga bog‘liqligiga qarab buzg‘unchi ob’ektni tanlaydi. Agar hujum qilish maqsadi jiddiy axborot bo‘lsa (ya’ni bunday axborotga ulanish), u holda bunday axborot yordamida boshqariluvchi yoki unga kirish uchun vositachilik qiladigan

barcha tizimlar buzg‘unchi uchun muhim sanaladi. Agarda buzg‘unchini maqsadi zarar yetkazish bo‘lsa, tizimni normal ishlashi Internet- tarmog‘ini yirik segmentlariga bog‘liq.

Internet ga ulangan barcha tarmoqlar hech bo‘lmaganda minimal darajadagi himoyalanganlikni talab qiladi. 2000 yildan boshlab to hozirgi kungacha AX tizimlariga yangiturdagi hujumlar paydo bo‘lgan: "cherv" debnomlanuvchi dastur, izlaydigan va avtomatik tarzda tizimlarga hujum qiladigan tizim. Bunday “dasturiy chervlar” qisqa davr ichida minglab tizimlarni buzishi mumkin. (Bunday birinchi Internet-cherv 1988 yilda “Morris” bo‘lgan. Biroq, bu g‘oya 12 yil davomida bunday dasturlarda o‘z ishiningdavomini topmadi).

Barcha bu chervlar o‘z oldiga qo‘ygan maqsadga, protokollarni amalga oshirishda yo‘l qo‘yilgan dasturiy xatolar hisobiga erishgan, ular boshqa tomondan yetarlicha himoyalangan bo‘lgan. Biroq birgalikda qo‘llanilgan himoyalangan protokoldagi fundamental bo‘sh joyga yo‘nalgan hujumni tasavvur qilish qiyin. Shunga qaramay, qat’iy talab mavjud: ishlab chiqilayotgan protokollarda bunday bo‘sh joylarni kamaytirishga intilish kerak.

Buzg‘unchi uchun maqsadning ahamiyati uning joylashuv o‘rniga ham bog‘liq bo‘lishi mumkin. Magistral kabelda joylashgan tarmoq monitoringi serveri muhim nishon hisoblanadi, chunki u osonlik bilan tarmoq trafigini eshitish serveriga “aylanishi” mumkin. Tarmoq subsegmentida joylashgan va xabarlarni qayta ishlash uchun qo‘llaniladigan aynan o‘xshash server buzg‘unchida kamroq qiziqish uyg‘otadi va xavf-xatarga kamroq uchraydi.

Barcha vaziyatlarda trafikni eshitish AXga jiddiy tahdid sifatida qaralishi kerak. Oxirgi paytda, 1993 yildan boshlab trafikni qonunga qarshi eshitish (nazorat qilish) bilan bog‘liq ko‘p voqealar sodir bo‘ldi. Faol hujumlar natijasida ko‘pincha tizim xavf-xatarga uchraydi, ya’ni buzg‘unchi tomonidan asl IP-paketlarni o‘chirish yoki yolg‘onlarini qo‘yish orqali. Ta’kidlash joizki, bunday hujumlar hamma foydalanishi mumkin bo‘lgan vositalar yordamida amalga oshirilishi mumkin va ularni “tabiat”da kuzatish mumkin. Amaliy nuqtai nazardan, “aloqa seansiga bostirib

kirish” deb nomlanuvchi hujum turlari alohida qiziqish uyg‘otadi, unda “kimdir” o‘zaro ta’sir qiluvchi tomonlar orasida joylashib, autentifikatsiya jarayoni tugashini kutib, keyinchalik o‘zaro ta’sir qiluvchi tomonlardan birini tasvirlay boshlaydi va aloqa seansini boshqasi bilan davom ettiradi.

AX protokollarini ta’minlashda hamma foydalanishi mumkin bo‘lgan muhim vositalardan biri bu kriptografiya hisoblanadi. Kriptografiya ma’lumotlarni himoyalashning turli darajalarini ta’minlash imkonini beradi, ular tarmoq orqali translyatsiyalanib, tarmoqning himoyalanganlik darajasiga bog‘liq bo‘lmaydi. Oxirgisi o‘ta muhim hisoblanadi, chunki Internet-tarmog‘i o‘zining boshqarish va nazorat qilish muhitining taqsimlanganligi sababli axborot uzatishning ishonchli muhiti sifatida qaralmaydi. Uning xavfsizligi AX ta’minlash usullariga asoslangan, ular ma’lumotlar uzatish muhiti yoki tarmoq operatorlariga bog‘liq bo‘lmagan tarmoq protokollariga o‘rnatiladi.

Albatta, kriptografiyadan foydalanganda ma’lum moliyaviy harajatlar kerak bo‘ladi. Ammo bu sarf-harajatlar tezlik bilan kamayib boradi. “Mur qonuni”da protsessorlarning tez harakati har yili 1V barobar o‘sib boradi, hamda kriptografik komponentlar va ma’lumotlarni himoyalash vositalarining oson qo‘llanishi kriptografiyani AXni ta’minlashning ishonchli usullarini qo‘llash nuqtai nazaridan nisbatan oddiydir. Shunga qaramay, ba’zi istisnolar mavjud. Bu ochiq kalitli tizimlarga tegishli, ular avvalgidek juda qimmatbaho hisoblanadi. Bunday tizimlarga kirish shunday hollarda mumkin bo‘lmay qoladiki, qachonki ochiq kalitni shakllantirish bo‘yicha har bir jarayonning narxi oddiylarning (ya’ni qimmatbaho) juda kam qismini qoplaydi, shakllanish nuqtai nazaridan kalit sezilmas darajada u yordamida himoyalanadigan tomonidan qo‘llaniladi.

Agarda hech qanday cheklashlar bo‘lmasa, barcha protokollar uchun ishlatilishi mumkin bo‘lgan axborotni himoyalashning yanada ishonchli kriptografik usullaridan foydalanish tavsiya etiladi. Ko‘pincha axborotni himoyalashning eng ishonchli kriptografik usullari uncha ishonchli bo‘lmagan usullardan qimmat

bo‘lmaydi. Kriptoalgoritmni tezkorligini ta’minlash bilan bog‘liq real harajatlar, u ta’minlab beradigan himoyalanganlik darajasi bilan bog‘liq bo‘lmaydi. Kompleksning qo‘llaniladigan apparat qismiga qaraganda, kriptografik jarayonlar juda yuqori tezlik bilan amalga oshishi mumkin (1Gb/s), hatto dasturiy qo‘llanishda amalga oshirilayotgan kriptografik jarayonlarning tezkorligi bunday tezlikka yaqinlashadi.

*AX ta’minlashning majburiy usullari.* Internet–hamjamiyatida (IETF) “qo‘llash uchun majburiy bo‘lgan AXni ta’minlash usullari” tushunchasi standartlashtirilgan. Ushbu yondashuv shunday xavfsizlik protokolini ishlab chiqishni nazarda tutadiki, ushbu prokoldan foydalanuvchi turli amaliy xizmatlarning funksional mos kelishini kafolatlay olishi kerak. Agar protokol qo‘yilgan vazifani bajarish uchun bir necha qo‘shimcha funksiyalarni taklif qilsa, ammo u birgalikda ishlashi kerak bo‘lgan amaliy xizmatlarning hech bo‘lmaganda bittasida bo‘lsa ham amalga oshirilmasa, u holda bir necha amaliy xizmatlar funksional jihatdan to‘g‘ri kelmaydi. Bu turli amaliy xizmatlarning funksional to‘g‘ri kelmasligiga olib keluvchi AX ta’minlash usulini tanlashda yo‘l qo‘yilgan xatoliklar natijasidir.

Shunga qaramay, xavfsizlik protokoli bir yoki bir necha AXni ta’minlash usullarini o‘z ichiga oladi, bu usullar, o‘z navbatida, ko‘pincha bir necha kriptografik tizimlarni qo‘llashi mumkin. Kriptotizimlarning o‘zi esa ishonchlilik va tez ta’sir qilishi nuqtai nazaridan o‘zgarishi mumkin. Biroq xavfsizlik protokollarining ko‘pchiligida “qo‘llash uchun majburiy bo‘lgan” kriptotizimlarni aniqlash lozim, chunki istalgan ikkita amaliy xizmatlarga keyinchalik o‘zaro qabul qilinadigan kriptotizim moslashtirish qobiliyatini kafolatlaydi.

Boshidan aniq chegaralangan amaliy tizimlarda qo‘llash uchun ishlab chiqilgan xavfsizlik protokollari mavjud. Bunday protokollarni yaratishda uchraydigan dalillardan biri, mos keluvchi protokolning qo‘llanilish sohasi yetarlicha yaxshi aniqlangan, protokolning o‘zi esa ishonchli himoyalangan va AX ta’minlashning qo‘shimcha usullariga ehtiyoj yo‘q. Tarix bu dalillarni rad etadi.

Hatto “yaxshi protokollar” (agar ular ma’lum tarmoq segmenti chegarasida aniq amaliy masalalarni yechish uchun ishlab chiqilgan bo‘lsa) boshlanishidan xavfsizlikni ta’minlash vazifasi ko‘rilmagan chegara soxasi oralig‘ida o‘zining to‘g‘ri ishlashini to‘xtatadi. Bu muammoni yechish uchun IETF talab qiladiki, barcha xavfsizlik protokollari mos keluvchi AXni ta’minlash usullarini qo‘llab-quvvatlashi kerak (eng ishonchlilari bilan birga), hattoki ularning qo‘llanish sohasi boshidanoq chegaralangan bo‘lsa ham.

Shuni tushunish muhimki, AXni ta’minlashning majburiy usullari foydalanish uchun juda zarur (ular himoyalanganlikning yuqori darajasini ta’minlaydi). Biroq bu oxirgi foydalanuvchilar albatta shu usullarni qo‘llashi kerak degani emas. Agar oxirgi foydalanuvchi u foydalanayotgan tarmoq xavfsizligini ta’minlovchi protokolga ushbu usullar o‘rnatilganini bilsa ham, baribir foydalanuvchi AXni ta’minlash usullarining ishonchli bo‘lmagan (eng yaxshi bo‘lmagan) turini tanlashi mumkin, ammo u bularga ishonadi va ular o‘zlarining AXni ta’minlashga ketgan sarf-harajatlaridan kelib chiqib, himoyalanganlik darajasini ta’minlaydi deb o‘ylaydilar.

AXni ta’minlashning ishonchli usullarini qo‘llash majburiy deb belgilangan talablar shuni anglatadiki, bu usullarni amalga oshiruvchi protokol kerak bo‘lgan oxirgi foydalanuvchilar zarurat yuzaga kelganda ulardan foydalanishlari mumkin. Agar AXni ta’minlash usullari haqida gapirsak, ularni qo‘llashni majburiyligi shundan iboratki, “jimlik bo‘yicha” rejimida foydalaniladi, hatto foydalanuvchi ularni qo‘llashdan bosh tortsa yoki tizimni sozlash ularning qo‘llanilishini blokirovkalasa, u yanada ishonchli algoritmdan foydalanishi sharoitida undan bosh tortishi mumkin.

*Himoyaning taqsimlangan tizimi.* AXni ta’minlashning ba’zi usullari butun tarmoqni butunligicha himoyalashi mumkin. Bunday yondashuv qurilmali tarmoq komplekslarida tejash imkonini berishiga qaramay, u bunday tarmoqni ichki segmentini ichkaridan hujumlar uchun ochiq qoldirishi mumkin. Himoya tizimini

taqsimlanganligining kerakli darajasi hisoblanganda, protokol ishlab chiqaruvchilar uning qo‘llanish modellarini, protokol o‘rnatiladigan Internet-arxitektura darajalarini, shuningdek uning Internetda tarqalishini taxminiy darajasini e’tiborga olishlari kerak. Agar protokol biror himoyalangan kompyuterlar guruhi ichida foydalanilsa (masalan, tarmoqni boshqarish markazi), u holda tarmoq segmentining subsegmentlarga topologik bo‘linish darajasi turlicha bo‘lishi mumkin (maksimalgacha). Boshqa tomondan, AXni ta’minlashning ba’zi usullari faqat bitta amaliy xizmat uchun qiziqish uyg‘otsa, faqat shu amaliy protokolga yaxshi o‘rnatilishi mumkin, qiyoslash uchun, masalan, TCP-protokolda ko‘rish mumkin. Biroq, bu boshqa protokollarga ushbu usulni o‘rnatishda ma’lum qiyinchiliklarni tug‘diradi, demak uning Internetda tarqalishida qiyinchiliklarni keltirib chiqaradi.

Protokol o‘rnatiladigan Internet-arxitekturalar darajasi. AXni ta’minlash usullari Internet - arxitekturaning istalgan darajasida o‘rnatilishi mumkin. Umuman olganda, agar usulni arxitekturaning quyiroq darajasida o‘rnatilsa, u holda yuqori darajadagi protokollarning keng spektrini himoya qilish qobiliyatiga ega bo‘ladi, boshqa tomondan esa bu himoya yetarlicha ishonchli bo‘lmasligi mumkin. Kanal sathidagi shifrator (“linklayer”) faqat IP- paketlarni emas, balki ARP-paketlarni ham himoya qilishga qodir. Biroq u faqat bitta aloqa kanalini himoyalaydi. Va aksincha, bir nechta pochta server-retranslyatorlar orqali uzatilishi mumkin (“saqlash-uzatish” rejimida) bo‘lgan elektron raqamli imzo (ERI) yordamida imzolangan pochta xabarlari real jo‘natuvchini identifikatsiyalashga qodir, ERIning o‘zi esa xabar yetib borganidan keyin kechroq tekshirilishi mumkin. Shunga qaramay, ushbu holatda faqat bir turdagi xabar himoyalanadi. Oddiy formatdagi xabarlar, masalan, tarmoq yangiliklari, bunday xabarlar uchun xavfsizlik usullaridan biri moslashtirilmaguncha va ularni tarqatish dasturlariga o‘rnatilmaguncha himoyalanmaydi.

## 11.8. Xujum turlari, dunyo axborot oqimlarini nazorat qilish va xavflarni boshqarish

Xabar manbalari orqali trafikni marshrutlash (IP-paketlar). Odatda, IP-paketni yetkazib berishning real marshruti (qabul qiluvchi/yuboruvchining adreslari IP-sarlavhada keltirilgan), xabarni IP-bog‘lama/jo‘natuvchi va IP-bog‘lama/qabul qiluvchisi o‘rtasida joylashgan marshrutizatorlar orqali aniqlanadi. IP-paketning o‘zi “qayerga yuborilishini aytadi” (IP-qabul qiluvchi adresi), hamda “qanday u yerga borishi” haqida “hech nima aytmaydi”.

Marshrutni tanlash bo‘yicha qo‘shimcha funksiya mavjud, u IP-bog‘lama/yuboruvchiga IP-paketga axborotni kiritish imkoniyati xabarini beradi, u IP-paketni uzatishda qo‘llash maqsadga muvofiq bo‘lgan yetkazib berish marshrutini ko‘rsatadi. Bu qo‘shimcha funksiya (yoki yetkazish usuli) “xabar manbalari orqali IP-paketlarni yetkazib berish marshrutini tanlash”deb ataladi (“source routing” - SR-usul/marshrutlash). SE-tizimini ishlashi nuqtai nazaridan, bunday IP-paketlarni yetkazib berishni SR-usuli alohida e’tibor talab qiladi, chunki buzg‘unchi himoyalangan SE tarmog‘idan (ichki tarmoq) chiqadigan “o‘zini trafik o‘rnida ko‘rsatadigan” trafikni shakllantirishi mumkin. Umuman olganda, bunday trafik keraklicha SEga yo‘naltirilgan bo‘lmaydi (SE orqali marshrutga ega), lekin IP-paketlarda qo‘shimcha “SR-etkazish usuli” funksiyasi mavjud bo‘lganda, buzg‘unchini kompyuteri va hujum ob’ekti o‘rtasidagi barcha marshrutizatorlar trafikni SR-marshrutga nisbatan teskari yo‘nalishda qayta yo‘naltiradi. Bunday hujumni o‘tkazish juda oson, shuning uchun SEni ishlab chiquvchilar bunday hujumlar haqida esdan chiqarmasliklari kerak.

Real hayotda, SR-etkazib berish usuli (marshrutlash) kamdan-kam qo‘llaniladi. Haqiqatda, marshrutlashning bunday usuli faqat tarmoq nosozliklari aniqlanganda yoki trafikni maxsus ajratilgan aloqa liniyalari bo‘yicha marshrutlashda qo‘llaniladi, ular alohida vaziyatlarda boshqarishni ta’minlash uchun

mo‘ljallangan. SEni qurish va sozlashda qo‘shimcha SR-funksiyasi tizimning mos keluvchi nuqtasida blokirovkalangan bo‘lishi kerak. Ko‘pgina tijorat marshrutizatorlar ataylab SR-marshrutlashni bloklash bo‘yicha qo‘shimcha funksiyani o‘rnatadilar. SE-tizimlari tarkibida IP-bog‘lama/tayanchlarni qurishda qo‘llanishi mumkin bo‘lgan OS UNIXning ko‘pgina turlarida esa, SR-trafikni o‘chirish yoki rad etish funksiyasi nazarda tutilgan.

ICMP-paketlar yordamida trafikni qayta yo‘naltirish. Boshqaruv xabarlarini uzatish protokoli (ICMP-protokol) “trafikni qayta yo‘naltirish” maxsus funksiyasini aniqlaydi (“Redirect”). ICMP/redirect-paket IP-bog‘lamaga (bu paketni olgan) o‘z marshrutlash jadvalida belgilangan marshrutdan voz kechishi haqida xabar beradi. Bu ICMP-funksiyasi marshrutizatorlar tomonidan IP-bog‘lamalarga xabar berish uchun qo‘llaniladi, ular qulay bo‘lmagan yoki mavjud bo‘lmagan marshrutlarni aniq IP-bog‘lama/ belgilashgacha qo‘llaydi, ya’ni IP-bog‘lama o‘zining IP-paketini “xato” marshrutizatorga uzatgan xolda. Bu “xato” marshrutizator javobga ICMP/redirect-paketni uzatadi, u IP-bog‘lamaga to‘g‘ri (boshqa) marshrut tanlashi kerakligi haqida xabar beradi. Agar buzg‘unchi ICMP/redirect-paketlarni qalbakilashtira olsa va hujum qilish nishoni bo‘lgan IP-bog‘lama bu paketlarga ta’sirchan, u holda buzg‘unchi bu IP-bog‘lamaning marshrutlash jadvaliga o‘zgartirish kiritishi mumkin va bu bilan tarmoq ma’muriyati tomonidan nazorat ostida bo‘lmagan marshrut bo‘yicha trafikni qayta yo‘naltirish orqali uning xavfsizligini buzadi. ICMP/redirect-paketlar buzg‘unchi tomonidan “xizmat ko‘rsatishni rad etish” turidagi hujumlarni o‘tkazish uchun qo‘llanilishi mumkin. Bunday hollarda IP-bog‘lamaga ICMP/redirect-paket uzatiladi, u bu IP-bog‘lama bilan bog‘liqlikni ta’minlamaydigan marshrutni ko‘rsatadi yoki belgilangan tarmoqqa kirish mumkin emasligini ko‘rsatuvchi boshqa ICMP/network/unreachable-paket uzatiladi.

Ko‘pchilik SE ishlab chiquvchilar chiqish va ichki (korporativ) tarmoqni ICMP-trafikini aks ettiruvchi funksiyani ishga tushiradilar, bu tashqi IP-bog‘lama

uchun exo-paketlar/so‘rovlarni (“ping”) uzatish yoki o‘zining marshrutlash jadvallarini modifikatsiyalash imkoniyatini cheklaydi.

Barcha ICMP-paketlarni bloklash haqida xulosa chiqarishdan avval,TCR-protokoli qanday qilib IP-paketlarni yetkazib berish marshrutini ma’lum retranslyatsiya uchastkasida xabarni ruxsat etilgan maksimal o‘lchamini aniqlash vazifasini hal etishini tekshirish kerak, chunki bu boshqa tashqi IP-bog‘lamalar bilan bog‘liqlik buzilmaganligiga ishonch hosil qilishga imkon beradi. Agar ICMP-paketlarni to‘liq bloklash mumkin bo‘lmasa (xavfsiz bo‘lmasa), u holda trafikni marshrutlashga javob beradigan ob’ektlar tomonidan xizmat ko‘rsatiluvchi ICMP-paketlar turlarini tanlash lozim. Agar nimadir bloklanmay qolsa, u holda hech bo‘lmaganda korporativ marshrutizatorlar va IP-bog‘lamalar keng eshittirishli (ko‘padresli) exo- paketlar/so‘rovlarga e’tibor bermasligiga ishonch hosil qilish kerak.

“Xizmat ko‘rsatishni rad etish”. “Xizmat ko‘rsatishni rad etish” turidagi hujumning mohiyati shundaki, buzg‘unchi buzish, funksionalligini buzish, bloklash yoki o‘tayuklash yo‘llari orqali “korporativ tarmoq yoki marshrutizatorni befoyda qilishga urinadi”. Bu holda bunday hujumlar oqibatini oldindan aytib bo‘lmaydi, hujumlarning o‘zini esa oldindan bartaraf etib bo‘lmaydi. Shuning uchun taqsimlangan topologiya va tuzilishga ega tarmoqlarni yaratish maqsadga muvofiq: har bir tarmoqni IP-bog‘lamasi boshqa tarmoqlar orqali ulangan, ular o‘z navbatida boshqa tarmoqlar bilan ulangan va h.k. Tarmoq xavfsizligi ma’muriyati yoki Internet-provayder (Internet Service Provider — ISP) faqatgina bevosita yaqindagi bir nechta lokal tarmoq komponentlarini nazorat qilishi mumkin. Buzg‘unchi xar doim o‘zi boshqarayotgan kompyuter yordamida, foydalanuvchidan ISP-servergacha (“upstream”) virtual ulanishni “buzishi” mumkin. Boshqacha qilib aytganda, agar kimdir tarmoqni buzishni xoxlasa, qayerdan bo‘lsa ham u buni amalga oshirishi mumkin, bunga yoki tarmoqni o‘zini buzish yo‘li yoki bu tarmoq ulanishlarini buzish yo‘li orqali erishish mumkin. “Xizmat ko‘rsatishni rad etish”

turidagi hujumlarni amalga oshirishning ko‘p usullari mavjud, murakkablardan boshlab eng eskilarigacha “qo‘pol kuchni ishlatib” amalga oshirish mumkin. Muhim va mas’uliyatli vazifalarni yechishda o‘ta muhim hisoblanuvchi qandaydir amaliy xizmatlar extiyojida Internet-tarmoqni qo‘llash haqida xulosaga kelishdan avval, korporativ tarmoqni ishlashida mumkin bo‘lgan muammolar natijasida yuzaga keladigan katta xavflar bilan bog‘liq yechim ekanligiga kelishish kerak.

Tarmoqni korporativ segmentini “exo-paketlar” xizmati yordamida bloklash mumkin, bu buzg‘unchi tomonidan “zararli” xizmat trafikini generatsiyalash uchun qo‘llaniladi.

*Boshqa mumkin bo‘lgan hujumlar*. Har bir tarmoqni korporativ segmenti boshqa korporativ segmentdan kichik bo‘lsa ham o‘z farqiga ega, shuning uchun bunday tizimlarni xavfsizlik nuqtai nazaridan aniq hujumlar o‘zgarishi mumkin. Biroq ko‘pchilik holatlarda hujumlar o‘xshash bo‘lib, turli tizimlarda qaytarilishi mumkin.

SMTP-serverini egallash (xabarlarni avtorizatsiyasiz retranslyatsiyasi). SMTP-serverini egallash shunday joyda bo‘ladiki, “spammer” xabarlarning minglab nusxasini generatsiyalaydi va ularni katta miqdordagi pochta adreslariga tarqatish imkoniga ega. Bunday pochta adreslarni ro‘yxati ko‘pincha yomon bo‘lgani uchun, spammerlarning o‘zi esa pochta serveri faoliyati tezligini pasaytirish maqsadini ko‘zlagani uchun, ularning ko‘pchiligi kelib tushgan barcha pochta xabarlarini tarqatishga urinadigan SMTP-serverga o‘zlarining pochta qutilarining butun tarkibini oddiy o‘tkazish yo‘lini qo‘llaydi.

Albatta, barcha tanqidiy fikrlar, spam bo‘yicha e’tirozlar, ayanchli pochta xabarlari va yoqimsiz reklamalar retranslyator sifatida qo‘llaniladigan SMTP-serveriga kelib tushadi. Aslida, bularning barchasi ma’lum moliyaviy harajatlar bilan bog‘liq, asosan insonlar (foydalanuvchilar) spaming oqibatlarini o‘chirishni xohlaganlarida ro‘y beradi.

Amaliy xizmatlarda zararli “xatcho‘plar”. W$^3$-serverlari, pochta serverlari va boshqa amaliy Internet-xizmatlar serverlarining dasturiy ta’minotini turli usullari zararli dasturiy “xatcho‘p”ga ega, ular masofadagi Internet-foydalanuvchilarga (buzg‘unchilarga) “xohlaganini” bajarishga imkon beradi, ya’ni kompyuterlarni boshqarishni qo‘lga olishdan boshlab amaliy xizmatlarni buzishgacha, shuningdek mana shular chegarasidagi barcha buzg‘unchilik ishlarini amalga oshirishi mumkin.

Bu xavfning ta’siri faqat zarur bo‘lgan amaliy xizmatlardan foydalanish hisobiga, dasturiy ta’minotda yangilangan “yamoqlar”ni o‘z vaqtida o‘rnatish hisobiga va o‘zini ijobiy tomondan tavsiya qilgan dasturiy mahsulotlarni qo‘llash hisobiga pasayadi.

*Operatsion tizimlarda zararli “xatcho‘plar”.* Bunday “xatcho‘plar” odatda olisdagi foydalanuvchilar tomonidan qo‘llaniladi. IP-protokoli asosidagi tarmoq texnologiyalari uchun nisbatan “yangi” hisoblangan operatsion tizimlar muammoliroq hisoblanadi, “eski” operatsion tizimlar “o‘z ichki xatcho‘p” larini izlash va yo‘qotish uchun yetarli vaqtga ega edi. Buzg‘unchi yo o‘zining hujum qilish ob’ektini (hujum nishoni) doimo qayta yuklaydi, yo uni buzadi, yo uni tarmoq bilan ulanish imkonidan mahrum qiladi, yo kompyuterda fayllarni oddiygina o‘rnini ko‘chiradi.

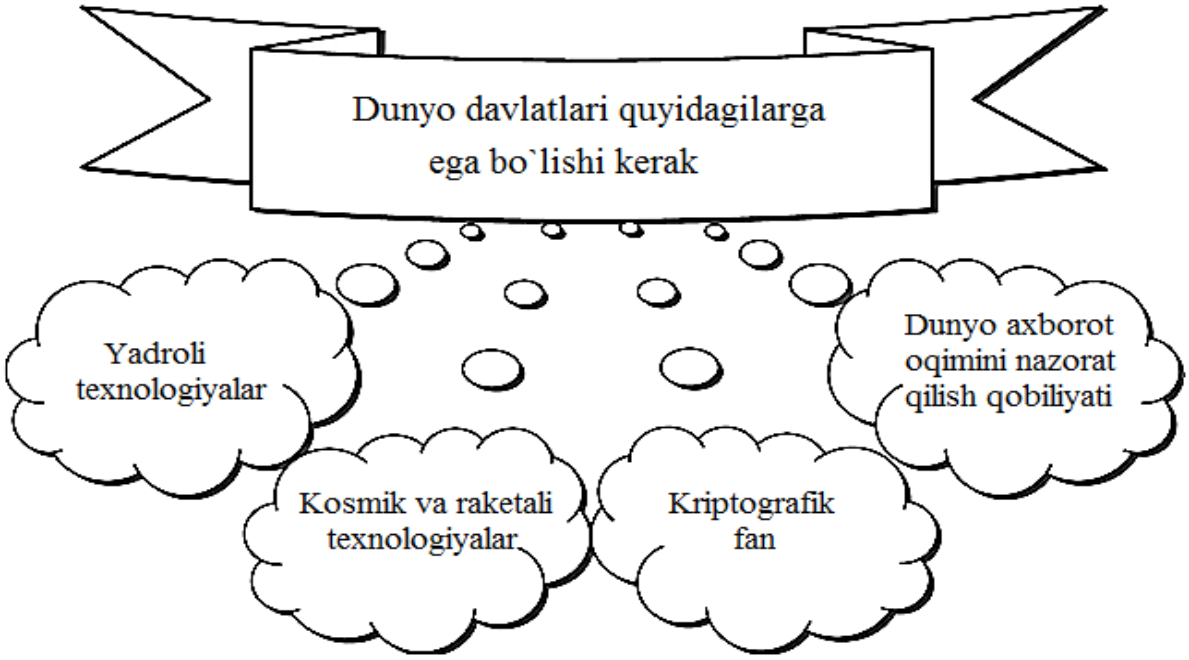
Ushbu holda, faqat bir necha operatsion tizimlar yordam berishi mumkin. Bundan tashqari, operatsion tizim oldida paket filtrini o‘rnatib, bu turdagi hujumlarning katta sonli ta’sirini pasaytirish mumkin. Albatta, turg‘un operatsion tizimni tanlab turib, bir qator hujumlarning oldini olish mumkin. Operatsion tizimni tanlashda “qancha qimmat bo‘lsa, shuncha yaxshi” deb o‘ylash kerak emas. Bepul operatsion tizimlar tijorat tizimlarga nisbatan ko‘pincha ishonchliroq.

**Dunyo axborot oqimlarini nazorat qilish.**

Hozirgi paytda jamiyatda faol muhokama etilayotgan eng muhim muammolardan biri axborotli qarshi kurash hisoblanadi. Bunday urush axborot quroli yordamida olib boriladi, u “mohir qo‘llarda” telekommunikatsiya va axborot

tizimlarini zararlaydigan qo‘rqinchli vosita bo‘lib qoladi. Davlatning telekommunikatsiya va axborot infratuzilmasining muhim ob’ektlarini zararlab, uning mudofaa qobiliyatini keskin tushirib yuborishi mumkin va shu yo‘sinda keyingi “issiq” urush oqibatlarini oldindan aniqlashi mumkin.

*Dunyo axborot oqimlarini nazorat qilish.* Amerika kriptografiya tarixchisi Devid Kann buyuk hukumatni aniqlash uchun uch mezonni kiritdi (11.10-rasm):




11.10-rasm. Dunyo davlatlarini aniqlash mezonlari

Sivilizatsiyani rivojlanishining zamonaviy bosqichida buyuk hukumat va boshqa qolgan dunyo orasidagi chegarani kuzatish mumkin. Bu birinchi navbatda buyuk hukumatni aniqlashda yangi mezonning paydo bo‘lishi bilan bog‘liq. Bu yangi mezonlar, davlat tomonidan dunyo axborot oqimlarini maksimal darajada nazorat qilishni ta’minlash qobiliyati hisoblanadi.

Bu mezondan foydalanishning muhimligini tushuntirish lozim:

- globallashtirish jarayonlari;

- dunyo sivilizatsiyasini yoppasiga axborotlashtirish va uni davlat, jamiyat va insoniyatning barcha faoliyat sohalariga kirib borishi;

- global elektron (tarmoq) axborot resurslarini yaratish, u to‘g‘ridan-to‘g‘ri davlat infratuzilmasini tashqi hamda ichki siyosiy faoliyatga va iqtisodning barcha sohalari ishining samaradorligiga, umumgumanitar va ijtimoiy dasturlarni (tibbiyot ham kiradi) amalga oshirishga, ilmiy potensialni oshirish, jamiyatning intellektual-madaniy ommasini saqlashga ta’sir qiladi;

- xalqaro terrorizmning o‘sishi va uning umumjahon stabilligiga putur yetkazishga urinishlari.

Dunyo axborot oqimlarini nazorat qilish (DAONQ) - bu nafaqat radioelektron razvedka (shpionaj) va axborot olish (RER). Bu yangi sifatli RER. Bu RER olib borishning odatiy usullaridan chetga chiqishdir. DAONQ asosida axborotlarni aniqlash va olishni tarmoq prinsiplari yotadi. Bu prinsiplar talab qilinadigan axborot va resurslarga kirishni “engillashtirish/soddalashtirish” maqsadidagi faol tadbirlarni ko‘zda tutadi. Buning uchun xizmat axborotiga maxsus kirish bo‘lishi kerak, u o‘z navbatida telekommunikatsiya tizimlari va tarmoqlarining normal ishlash qobiliyatini ta’minlaydi.

DAONQning yangiligi yana shundan iboratki, bu yerda gap axborot-telekommunikatsion muhitning yangi shakli, ko‘pincha “kibermuhit” deb ataluvchi haqida boradi. Kibermuhitning paydo bo‘lishi jahon sivilizatsiyasining rivojlanishi va uyg‘unlashishiga ijobiy hamda samarali omillarning ta’siri bilan birgalikda shaxs, jamiyat, davlat va butun insoniyatga yangi tahdid turlarini olib keldi. Shuning uchun DAONQ:

- bir tomondan, bu qarshi kurashishning, ayniqsa axborotli (axborot - texnologik), yangi turining paydo bo‘lishi;

- boshqa tomondan, bu yangi “kibertahdid”ni amalga oshirishda salbiy oqibatlarning aks etishi va ogohlantirish shakli. Bundan tashqari, DAONQ-bu davlat

milliy xavfsizligini, oxir oqibatda - jamiyat va shaxs erkinligini ta’minlash bo‘yicha ogoxlantiruvchi choralar.

DAONQ - bu yangi axborot-telekommunikatsiya usullari va ma’lumotlarni qayta ishlash, saqlash va yetkazib berish usullarini nazarda tutadigan kibermuhitni nazorat qilish. DAONQni to‘liqligi ikkita tashkil etuvchini nazarda tutadi:

- miqdoriy, ya’ni trafikning qanday hajmi nazorat qilinadi;

- sifatli, uzatilayotgan trafikning semantikasi qanchalik aniq tushunilishi. Boshqa so‘z bilan aytganda, uzatilayotgan axborot semantikasiga “singish chuqurligi qanday” (foydalanuvchi (iste’molchi) va xizmat), keyinchalik milliy xavfsizlikni ta’minlash bo‘yicha xulosaga kelish uchun olingan xabarlarni axborotlashgan tahlil o‘tkazish uchun qo‘llaniladi.

DAONQni to‘lqligini ta’minlovchi bu ikki tarkibiy qism maksimallashtirishni talab qiladi. Agar birinchi tarkibiy qism “o‘zi uchun gapirsa” (dunyo axborot oqimlari qamrab olish maksimal darajada bo‘lishi kerak), ikkinchi tarkibiy qism esa murakkab va bajarilishi qiyin hisoblanadi. Buni bir necha sabablari bor, ularni bir necha quyidagi guruhlarga ajratish mumkin:

- foydalanuvchilar tomonidan dunyo telekommunikatsiya tarmog‘ining (Internet ni ham kiritib) turli terminalli apparat-dasturiy komplekslarni qo‘llab, ayniqsa bu turli kompaniyalarning amaliy dasturiy mahsulotlariga tegishli bo‘ladi;

- katta miqdordagi korporativ va shaxsiy lokal axborot-hisoblash tizimi va tarmoqlarining yaratilishi bilan, ular tarmoqning turli texnik vositalari, operatsion va amaliy tizimlarini qo‘llaydi;

- telekommunikatsiya kompaniyalari va tarmoq provayderlari tomonidan katta miqdordagi turli xil texnikalarni (texnik vositalar kompleksi) hamda axborotni qayta ishlash, yetkazish, saqlash texnologiyalarini qo‘llash orqali;

- turli ko‘rinishdagi xizmat va tizimlarning ommaviy integratsiyasi bilan (ko‘rinishlari: telefoniya, ma’lumotlar uzatish, faksimil xabarlar, videoinformatsiya;

o‘tkazgichli aloqa tizimlari, optik-tolali aloqa tizimlari, sputnikli tizimlar, raqamli radiorele tizimlar, uyali va mobil aloqa tizimlari va h.k.);

- axborotni himoyalashning maxsus dasturiy va dasturiy-apparat komplekslarini keng tarqatish bilan, ba’zida ular malakaviy baholashga to‘g‘ri kelmaydi.

Shunday qilib, DAONQ natijasida qarshi kurashishning yangi shakli, aynan “axborot urushi” paydo bo‘ladi, uning ostida maqsadli harakatlar yotadi, bu harakatlar dushman ustidan axborot va axborot-texnologik ustunlikka erishish uchun uning axborotiga, axborot jarayonlariga, axborot tizimlariga, axborot resurslariga bir vaqtning o‘zida o‘z axborotini, axborot jarayonlarini, telekommunikatsiya axborot tizimlarini himoya qilib turib zarar yetkazishni amalga oshirish.

**Xavf ehtimolini boshqarish.**

Xavf ehtimolini boshqarish jarayonini amalga oshirishda shuni tushunish kerakki, qanday qilib xavf ehtimolini kamaytirish uchun u yoki bu telekommunikatsiya va axborot texnologiyalarini qo‘llash kerak. Xavf ehtimolini boshqarish quyidagi ko‘p ishlatiladigan terminlarni qo‘llash bilan bog‘liq:

- *zaiflik* - AXni ta’minlash tizimining kuchsizligi, unda qo‘llanadigan jarayon va/yoki jarayonlarga, loyiha xulosalariga, himoya usul va vositalarini amaliy tadbiq etishga, boshqarishning ichki tizimiga va boshqalarga taalluqli, ya’ni ruxsat etilmagan maqsadlarda ataylab qo‘llash yoki tizim xavfsizligini ta’minlash strategiyasini obro‘sizlantirishga ataylab olib kelishi mumkin;

- *tahdid manbai* - yoki bu xavfsizlikni ta’minlash tizimining zaifligini ataylab qo‘llash usuli, yoki zaiflikni keltirib chiqarishi mumkin bo‘lgan noshtat hodisa;

- *tahdid* - tahdid manbaining ma’lum zaiflikni paydo bo‘lishi yoki undan foydalanish qobiliyati;

- *xavf ehtimoli* - iqtisodiy vazifalarni yechish jarayoniga va asosiy faoliyatida ma’lum natijalarga erishish kuchli salbiy ta’sir qilishi (ketidan kuchli salbiy ta’sir ko‘rsatuvchi noshtat hodisalarning paydo bo‘lish ehtimoli), bu ma’lum tahdid

manbai tomonidan hosil bo‘lib, telekommunikatsiya tizimining zaifligi paydo bo‘lishiga olib keladi. Telekommunikatsiya va axborot texnologiyalarini qo‘llash bilan bog‘liq xavf ehtimoligi, yuridik javobgarlik yoki biznesni yo‘qotish (iqtisodiy faoliyat) natijasi hisoblanadi:

- axborotni avtorizatsiyalamay (g‘arazli, g‘arazli bo‘lmagan, tasodifiy) ochish, modifikatsiyalash, buzish;

- oldindan ko‘zlanmagan xato harakatlar va harakatsizlik;

- tabiat hodisalari yoki insonning buzg‘unchilik faoliyati natijasida telekommunikatsiya va axborotlashtirish tizimlarining buzilishi;

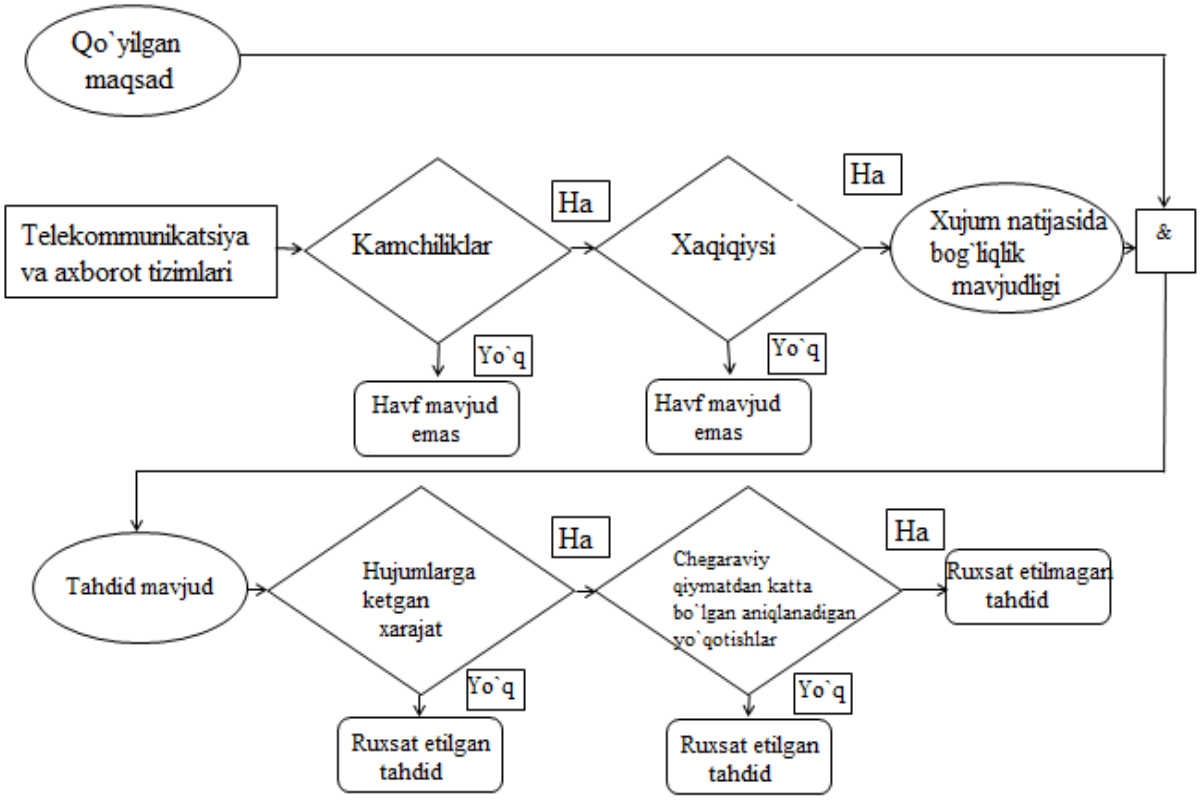
- telekommunikatsiya tizimlarini tatbiq qilish va ishlatishda e’tibor, ehtiyotkorlik va sinchkovlikning yo‘qligi.

11.11-rasmda oldindan ko‘zlangan hujumlarni amalga oshirish bilan bog‘liq xavf ehtimolini pasaytirishni umumlashgan algoritmi ko‘rsatilgan. Bu holatda “hujum” termini shuning uchun qo‘shtirnoq ichiga olinganki, bunday hujum natijasi “ataylab” bo‘lib, zarar keltirmaydi. Bu oldindan ko‘zlangan zararsiz maqsadli hujumlarning umumiy ko‘rinishi.

Bunday hujumlardan texnik vositalar bilan xavf ehtimolining pasayishi quyidagi algoritm bosqichlarida amalga oshishi mumkin:

- kamchilikning mavjudligi. Bartaraf etish usuli: kamchiliklarni paydo bo‘lish ehtimolini kamaytirish maqsadida ishonchli usul va vositalarning qo‘llanishi;

- kamchilik real hisoblanadi. Bartaraf etish usullari: ko‘p bosqichli himoyani qo‘llash va kamchilik oqibatlarini neytrallashtirish uchun qabul qilingan xavfsizlik arxitekturasini amalga oshirish;




11.11-rasm. “Xujumlar” ta’sirida xavfning pasayishini umumlashgan algoritmi

- hujumga sarf-harajatlar - hujum natijasi narxidan past. Bartaraf etish usullari: himoyalash usul va vositalarini qo‘llash, hujum sub’ekti tomonidan harajatlarning ma’lum darajada ko‘payishiga olib kelishini yengish;

- yo‘qotishlar juda katta. Bartaraf etish usullari: xavfsizlikni ta’minlashni qat’iy choralarini qo‘llash, xavfsizlikni qabul qilingan arxitekturasini amalga oshirish va yo‘qotishlarni kamayishiga olib keluvchi hujum diapazonini kamaytirish maqsadida himoyalashni texnik vositalarini tatbiq qilish.

## 11.9. Axborot xavfsizligini ta’minlashning standart usullari

Bir martalik parolli tizimlar. Bunday tizimlar (RFC-2289) oddiy parolli tizimlarga qaraganda ancha ishonchli hisobladi. Bunday tizimlarda IP-bog‘lama

foydalanuvchining parolining nusxasini saqlamasligi va uni tarmoq orqali yubormasligi kerak. Biroq ma’lum xavf ehtimollari mavjud. Uzatilayotgan ketma-ketlik (bir martalik parol) foydalanuvchi parolidan shakllangani uchun, hujumlar avvalgidek real va amalga oshishi mumkin deb taxmin qilish mumkin. Bunday hujumlarni amalga oshirish uchun dasturdan hamma foydalanishi mumkin. Bundan tashqari, tizimdan foydalanish uchun ro‘yxatdan o‘tgan murojatlarning ma’lum sonidan keyin foydalanuvchining tizimga kirishini to‘xtatish kerak. Ko‘pgina tizimlarda bu funksiya ajralmas bo‘lishiga qaramay, avvalo uautentifikatsiya jarayoni uchun ma’lumotlar bazasini qayta ishga tushirish usuli sifatida zarur, bu yangi parolni tarmoq orqali ochiq ko‘rinishda uzatishni talab etmaydi.

Hozirgi paytda tijorat tarmog‘ining uskunalarini autentifikatsiyalash uchun maxsus belgilar qo‘llaniladi. “Aloqa seansiga bostirib kirish” deb ataluvchi hujumlardan himoyalanish bilan bog‘liq muammolarni yechishdan tashqari, bunday tizimlarda eng maxsus belgilarni uzatish uchun qo‘shimcha protokolli xabarlar kerak bo‘lishi mumkin (odatda bunday belgilar “so‘rov/javob” rejimida uzatiladi, bunda server har bir autentifikatsiyalash jarayoni davomida noyob taxminiy raqamni uzatadi).

HMAC-tizimlar. HMAC-tizimlari asosida (HMAC: Keyed-Hashingfor Message Authentication – maxfiy kalitni qo‘llab xesh-funksiyani hisoblash asosida xabarlarni autentifikatsiyalash tizimi, RFC-2104) oldindan taqsimlangan maxfiy kalitni qo‘llab autentifikatsiyalash usuli yotadi. Agar ikkala qatnashuvchi umumiy maxfiy kalitni bilsa, u holda HMAC-tizim istalgan erkin xabarni autentifikatsiyalash uchun qo‘llanilishi mumkin. Bunday usul tasodifiy raqamlar (metka) so‘rovlarini o‘z ichiga oladi, bu NMAS-tizimning avvalgi aloqa seanslaridagi xabarlarni qaytadan uzatishdan himoyalash uchun moslashish qobiliyatini anglatadi.

Afsuski, NMAS-tizimi ulanishlar autentifikatsiyasi uchun to‘g‘ri kelmaydi, chunki maxfiy kalit ochiq ko‘rinishda axborot uzatishni har bir tomonida ma’lum bo‘lishi kerak, bu ayniqsa uzoq vaqtli kalitlardan foydalanganda nomaqbul.

Qabul qilinishicha, NMAS-tizim xavfsizlikning eskiroq usullariga nisbatan afzalroq bo‘lib qo‘llanishi kerak, ayniqsa bu kalitni qo‘llagan xesh-funksiya hosoblariga tegishlidir. MD5 (RFC-1321) algoritmi asosidagi kalitlarni qo‘llaydigan oddiy xesh-funksiyalar, masalan, BGP-protokol (RFC-2385) xavfsizlikni yangi protokollari ro‘yxatidan o‘chirib yuborilyapti, bu xesh-funksiyalari past ishonchlilikka egaligi haqida xulosa chiqarishga imkon beradi.

NMAS-tizim istalgan xesh-funksiya bilan birgalikda, MD5-algoritmi va SHA-1 algoritmlari (RFC-3174) bilan qo‘llanishi mumkin. SHA-1 algoritmi yangi xavfsizlik protokollari uchun afzalroq, chunki bu maqsadlar uchun ko‘proq qo‘llaniladi va ishonchliroq bo‘lishi mumkin.

Tushunish muhimki, NMAS-xavfsizlikni ta’minlash usulini har bir protokolli xabarni himoyalash uchun qo‘llash zarur (kanal sathining kadri). Agar NMAS-tizimini faqat TCP-aloqa seansini boshlang‘ich fazasini autentifikatsiyalash uchun qo‘llanilsa, keyingi TCP-xabarlar hech qanday himoyasiz uzatilsa, katta xatolikka yo‘l qo‘yilgan bo‘ladi.

Hujum qiluvchi dasturiy modullar mavjud, ular TCP-aloqa seanslarini obro‘sini tushirish imkonini beradi. Buning uchun buzg‘unchiga bunday TCP-aloqa seansini obro‘sini tushirish uchunshunday dasturiy modulni qo‘llash zarur, bu NMAS-autentifikatsiyalash jarayoni yakunlangach amalga oshiriladi.

IPsec-arxitekturasi. IP-sathda (tarmoq sathida) IPsec-arxitekturasining asosini tashkil qiladigan autentifikatsiyalash va shifrlash protokollari RFC-4301, RFC-4302, RFC-4303, RFC-4306 va RFC-4307 standartlarida ifodalangan. Mohiyati bo‘yicha ushbu xavfsizlik arxitekturasi yuqori sathdagi protokollarni, TCR- va UDP-protokollarini ham himoya qiladi. U himoyalashni bir tekis taqsimlanishini ta’minlaydi, ya’ni “IP-bog‘lama - IP-bog‘lama”, “IP-bog‘lama - xavfsizlik shlyuzi” va “xavfsizlik shlyuzi - xavfsizlik shlyuzi”. IPsec-arxitekturasining funksional xususiyatlari foydalanuvchining o‘ziga himoyani taqsimlashga imkon beradi, ammo bu kamdan-kam sodir bo‘ladi. Aslida, agar himoyani taqsimlash IP-bog‘lamaning

o‘zida bir jinsli bo‘lmasa, IPsec-arxitekturasini qo‘llash har qanday mazmunni yo‘qotadi.

Dasturiy IPsec-modul tarmoq sathining (IP-sath) dasturiy ta’minotiga o‘rnatilsa, u holda u bevosita dastur listingiga (dastur kodi) tatbiq etiladi. Bunday kiritish yo dasturiy-apparat qismni o‘zgartirishni, yo alohida protokollarni almashtirish bilan bog‘liq arxitekturani yangilashni talab qiladi. Boshqa tomondan, IPsec-arxitektura amaliy xizmatlar uchun mutlaqo shaffof. IPsec-protokollar ustida ishlaydigan amaliy xizmatlar o‘z protokollarida hech qanday o‘zgartirishlarsiz o‘z himoyalanganliklarini oshirishlari mumkin. Ammo hozir, IPsec-arxitekturasi Internet-tarmoqda birgalikdagi foydalanishni topguncha, ko‘pgina amaliy xizmatlar IPsec- protokollari ustidan faoliyat olib borishi haqida “taxmin” qilish kerak emas, bu ularni AXni ta’minlashni shaxsiy usullarida alternativi sifatida aks etadi. Ko‘pchilik zamonaviy operatsion tizimlar dasturiy IPsec-modul bilan birgalikda ishlay oladi, biroq, boshqarish nuqtai nazaridan ko‘pgina marshrutizatorlar - yo‘q. TLS-protokolni (Transport Level Security - TLS, RFC-2246) qo‘llaydigan amaliy xizmat, autentifikatsiyalashni ishonchli jarayonlarini o‘tkazishda shaxsiy xususiyatlarini hisobga olish uchun ko‘proq imkoniyatga ega. IPsec-arxitekturasi foydasiga kalitli axborotlarni boshqarish, elektron sertifikatlar yoki taqsimlangan maxfiy kalitlarni qo‘llashga asoslanadi. Bir nechta sabablarga ko‘ra sertifikatlar afzalroq, biroq ular tizim ma’muriyatiga “bosh og‘riq” bo‘lishi mumkin.

Hozirgi paytda IPsec-protokollari va NAT-modullarini (RFC-2993) ishlashi orasida jiddiy mojarolar mavjud. NAT-moduli istalgan protokol bilan birgalikda ishlay olmaydi, uning xabarlari qo‘shimcha joylashtirilgan IP-adreslarni o‘z ichiga oladi. Bu IPsec-protokollarga, agar ular sarlavhada bo‘lsa IP-adresga ega bo‘lgan yuqori sathdagi istalgan protokol xabarlari bilan har bir IP-paketga tegishli. Bu mojaroni ba’zida tunnellash rejimini (TR) qo‘llash hisobiga yechish mumkin, lekin bundan har doim ham bir necha sabablarga ko‘ra foydalanib bo‘lmaydi. IPsec-

paketlar bilan NAT-modullarni oson yengishni ta’minlovchi standartni yaratish bo‘yicha ishlar olib borilmoqda.

IPsec-protokollar virtual korporativ tarmoqlarda Virtual Private Network - VPN) yanada kengroq qo‘llaniladi. Boshqa cheklanishlar uchrashidan kelib chiqqan xolda, IPsec-protokollari VPN-tarmoqlar o‘xshash xolatlarda ko‘proq qo‘llaniladi, ya’ni olisdagi kirish usulida. Bunda olisdagi kompyuter IPsec-protokolidan foydalanib Internet orqali o‘zini korporativ tarmog‘ida teskari tunnelni shakllantiradi (himoyalangan virtual bog‘lanish).

TLS-protokoli. Transport sathni xavfsizlik protokoli (Transport Level Security - TLS, RFC-2246) kanalni shifrlash va autentifikatsiyalashni ta’minlaydi, u TCR-protokoli qo‘llangan amaliy protokol bilan shakllantirilgan. TLS-protokoli $W^3$– serverlarda qo‘llash uchun maxsus ishlab chiqilgan bo‘lishiga qaramay, bu uning qo‘llanish sohasini chegaralanishini anglatmaydi. Shunga qaramay, har bir amaliy protokol, TLS-protokolni qo‘llamoqchi bo‘lsa, oxirgining mantiqiy va jarayonli xarakteristikalariga moslashtirilgan bo‘lishi kerak. Odatda, server (“mijoz/server” ulanishida) doimo elektron sertifikat asosida autentifikatsiyalanadi. Foydalanuvchilar shuningdek sertifikatlarga ega bo‘lishi mumkin, uning yordamida autentifikatsiyalashni “qo‘lda” bajarish mumkin, shunga qaramay bu usul keng qo‘llanilmaydi. Afsuski, amaliyotda xatto serverni autentifikatsiyalash jarayoni kriptografik usullarga nisbatan unchalik himoyalanmagan, ular qo‘llanilishi mumkin, chunki amaliy protokollarning (xizmatlar) ko‘pchiligi foydalanuvchilarga autentifikatsiyalashning salbiy natijalarini rad etish imkonini beradi, foydalanuvchilarning ko‘pchiligi shunday qiladilar ham. Protokollarni ishlab chiquvchilar ochiq parollarni qo‘llash nuqtai nazaridan, hatto bog‘lanishlar TLS-protokollari yordamida himoyalangan bo‘lsa ham, ehtiyot bo‘lishlari kerak (agar amaliy xizmatlar server sertifikatsiyasi avtorizatsiyasini o‘tkazsa va aslligini verifikatsiyalay olsa bu talab bir oz yumshatilishi mumkin).

Amaliy xizmatga (protokol) o‘zgartirish kiritish zarurligiga qaramay, TLS-protokoldan foydalanish talab qilinadi, ayniqsa bunday xizmatni ta’minlaydigan

vositalar (bepul va tijorat) zarur bo‘lgan joylarda. Bunday vositalar amaliy protokolning listing dasturlariga joylashtirish uchun ishlab chiqilgan. TLS-protokolni qo‘llovchi amaliy xizmat, o‘zining funksional xususiyatlaridan kelib chiqib, faqat IPsec-protokollarni qo‘llaydigan amaliy xizmatlarga nisbatan xavfsizlikni ta’minlashni to‘g‘ri keladigan strategiyasini o‘rnatish qobiliyatiga ega bo‘ladi.

SASL-interfeysi. Mohiyati bo‘yicha, AXni ta’minlashni kelishilgan usullari orqali aniqlanadigan, himoyalanganlik sathining parametrlari. Xususan, agar Axni ta’minlashni kelishilgan usuli barcha keyingi xabarlarni autentifikatsiyalamasa yoki TLS-protokoli kabi asosida yotgan xavfsizlik protokolidan foydalanmasa, barcha TCR-aloqa seanslari“ aloqaseansiga bostirib kirish” turidagi hujumlarga zaif bo‘lib qoladi.

Agarda TLS-protokolini (yoki IPsec-protokollarni) SASL-interfeysi bilan birgalikda qo‘llash kerak bo‘lsa (Simple Authentication and Security Layer- oddiy autentifikatsiyalash va xavfsizlikni ta’minlash sathi), u holda savollar tug‘iladi: “nima uchun birinchi navbatda SASL-interfeysi haqida o‘ylash kerak?” va “Nima uchun autentifikatsiyalash jarayonini amalga oshirish va ularni amalda qo‘llash bo‘yicha TLS-protokolning funksional imkoniyatlaridan foydalanishga harakat qilib ko‘rish mumkin emas?”.

Javob juda oddiy. TLS-protokoli autentifikatsiyalash foydasiga elektron sertifikatlarni yanada kengroq qo‘llashga imkon beradi. Ammo boshqa tomondan, sertifikatlarni tarqatish bo‘yicha muammolar mavjud, chunki faqat serverlar bunday sertifikatga ega, ayni damda foydalanuvchilar autentifikatsiyalangan (TLS-protokoli).

SASL-interfeysi foydalanuvchiga autentifikatsiyaning odatiy bo‘lgan usullarini qo‘llashga imkon beradi, masalan parolli tizimlar (bir martalik va b.q.). Bunday hollarda, yanada samarali bo‘lgan usullarni kombinatsiyasini ko‘rib chiqish foydaliroq, ya’ni TLS-protokoli serverni asosiy himoyasini va autentifikatsiyasini ta’minlaydi, SASL-interfeysi asosidagi autentifikatsiya tizimi esa foydalanuvchilarni

tekshirishni ta’minlaydi. Eng jiddiy e’tibor “inson ulanish o‘rtasida” (Manin the Middle) turidagi hujumga bo‘lgan zaiflikni pasaytirishga qaratilishi kerak, ayniqsa dupleks ulanishning turli yo‘nalishlarida autentifikatsiyaning turli usullari qo‘llanilganda.

GSS-API-interfeysi. Yagona xavfsizlik xizmatining amaliy dasturiy interfeysi (Generic Security Service Application Program Interface-GSS-API, RFC-2744), autentifikatsiyalash jarayonlari, yaxlitlik va/yoki konfidensiallikni ta’minlashda amaliy xizmatlar foydasiga dasturiy vositalarni o‘zida ifodalaydi. SASL-interfeysidan farqli o‘laroq, GSS-API-interfeysi UDP-protokolda joylashgan amaliy xizmatlarni osonlik bilan qo‘llashi mumkin. GSS-API-interfeysi protokolli xabarlarda joylashishi mumkin bo‘lgan autentifikatsiyalash jarayonlari foydasiga kodli belgilarni generatsiyalash imkonini beradi. (Ilova. GSS-API-interfeysi taqdim qilgan xavfsizlik protokollari bilan ta’minlanadigan himoyalanganlik darajasi, AXni ta’minlashni bazaviy usullariga bog‘liq. Xuddi shu xolatdan bu protokollarning funksional mos kelishi ham ko‘rilishi mumkin.)

DNSsec-protokoli. DNSsec-protokolining asosiy vazifasi (RFC- 2535) -DNS-yozuvlarni ERI yordamida himoya qilish. ERI DNS-serverining kesh-xotirasida saqlanadigan DNS-yozuvlarni “kesh-xotirani ifloslanishi” turidagi hujumlardan himoyalaydi. Bu yozuvlar, o‘z navbatida, autentifikatsiyalash jarayonini buzish uchun DNS-nomi asosida, shuningdek trafikni buzg‘unchiga qayta yuborib yoki uni chetlab o‘tib qo‘llanishi mumkin. Oxirgisi DNS-tizimni AXni ta’minlashning boshqa usullarini juda kritik qilib qo‘yadi, ayniqsa bu IPsec-arxitekturasiga tegishli.

Odatda DNSsec-protokoli, IP-adresda DNS-nomlarni aks ettirishda ma’lumotlarni himoyalashni ta’minlashga imkon beradi. Shuningdek u aniq DNS-nom bilan bog‘liq boshqa DNS-ma’lumotlarni himoyalashda ham qo‘llanilishi mumkin. Bunday ma’lumotlar faqat xizmatchi bo‘lishi mumkin, bu ularni saqlaydigan DNS-serverning normal ishlashi uchun zarur bo‘ladi yoki himoyalangan virtual ulanish moslashtirilganda IPsec-arxitekturasini xavfsizlik protokollarida

qo‘llaniladigan kalit bo‘lishi mumkin. DNS-tizimida umumiy tayinlangan amaliy kalitlarni saqlash konsepsiyasi RFC-3445 standartida “rad etilgan” edi, lekin unga qaramay, ba’zi amaliy xizmatlar foydasiga va xususan IPsec-arxitekturasi uchun kalitlarni saqlash jarayonini standartlashtirish davom etmoqda.

Ko‘p blokli xabarlarning xavfsizligi.RFC-1847 standarti, MIME-protokoli (RFC-2045) bilan aniqlanuvchi ko‘pblokli (ko‘p elementli) tuzilishga (Security/Multiparts) ega bo‘lgan elektron pochta xabarlarini himoya qilish usulini aniqlaydi. Yanada aniqrog‘i, Security/Multiparts-usuli MIME-protokolini to‘ldiradi, u MIME-xabarlarini shifrlash tartibi va qoidalarini va/yoki ularni ERI joylashtirishni aniqlaydi. Odatda ikkita protokol S/MIME (RFC-3156) va Open PGP (RFC-4880) o‘zining xabarlarini himoya qilishda Security/Multiparts-usullaridan foydalanadi. Ko‘pblokli pochta xabarlari tuzilmasini bila turib, qabul qiluvchi osongina xatning shifrlangan elementlarini aniqlashi va rasshifrovka qilishi mumkin.

Security/Multiparts-usuli “shaxsiy (abonentlik) xavfsizlik”ni (“object security”) ta’minlashning shakllaridan birini aks ettiradi, unda oxirgi foydalanuvchi uchun uning shaxsiy xabarlarini himoyalash, uni yetkazib berish usuli va bu xabarlarni oraliqdagi saqlanishidan qat’iy nazarasosiy talab hisoblanadi. Hozirgi paytda Internet-tarmog‘ida “shaxsiy xavfsizlik”ni ta’minlashning yagona shakli yo‘q.

S/MIME-protokolini elektron pochtadan farqli boshqa doirada qo‘llashda aloqa seansini o‘rnatish protokoli hisoblanadi (Session Initiation Protocol, RFC-3261).

Elektron raqamli imzo. O‘zaro munosabatdagi tomonlarni “so‘rov/javob” (“challenge/response”) rejimida autentifikatsiyalashda ERIni qo‘llash autentifikatsiyalashning yuqori ishonchliligini ta’minlaydi. Ochiq kalitli kriptografiyani qo‘llash maxfiy kalitlar qo‘llanadigan tizimlarda eng afzali hisoblanadi, chunki server foydalanuvchining maxfiy kalitini nusxasini saqlashga muhtoj emas. Foydalanuvchi maxfiy kalitga, serverlar esa unga mos keluvchi ochiq

kalitga ega bo‘lsa maqsadga muvofiq bo‘ladi. Qat’iy aytganda, ERIni qo‘llash murakkab ish hisoblanadi. Foydalanuvchi hech qachon unga yuborilgan xabar/so‘rovga imzo qo‘ymasligi kerak.

Standart DSS-ERI (Digital Signature Standard - DSS, AQSh federal standarti) va RSA-ERI yaxshi ERI-algoritmlari hisoblanadi, ularning har biri o‘z afzalligiga ega. DSS-ERIni qo‘llash yaxshi ehtimollik xarakteristikali tasodifiy sonlar generatorini qo‘llashni talab qiladi (RFC-4086, Randomness Requirements for Security). Agar buzg‘unchi qandaydir ERI uchun tasodifiy sonni regeneratsiyalashga qodir bo‘lsa yoki agar foydalanuvchi bitta tasodifiy sonni ikkita har xil hujjatda qo‘llasa, u holda foydalanuvchining maxfiy kalitini aniqlash mumkin. DSS-ERI yangi maxfiy kalitlarni generatsiyasi nuqtai nazaridan RSA-ERIga nisbatan yaxshiroq parametrlarga ega, ERIni tekshirish nuqtai nazaridan RSA-ERI ancha yaxshi parametrlarga ega.

Open PGP-protokoli va S/MIME-protokoli. ERI “shaxsiy xavfsizlik”ni ta’minlovchi amaliy xizmatlarni qurishda qo‘llanishi mumkin, ularni elektron pochta protokoli kabi, xabarlarni saqlash va yetkazib berish protokollarida ma’lumotlarni himoyalash uchun qo‘llash mumkin.

Yuqorida ta’kidlab o‘tilganidek, elektronpochtaning ikkita turli himoyalangan protokollari OpenPGP (RFC-3156, RFC-4880) va S/MIME (RFC-2633), himoyalangan elektron pochtaning (Privacy Enhanced Mail - PEM) takomillashgan protokollarini o‘zgartirish uchun mo‘ljallangan. Bulardan qaysi biri muvaffaqiyatli bo‘lishi umuman aniq emas. Bularning ikkalasi himoyalangan elektron pochta bilan birgalikda ishlash uchun ishlab chiqilgan bo‘lishiga qaramay, ikkalasi ham boshqa protokollar tomonidan transportirovka qilinadigan ma’lumotlarni himoyalashga moslashtirilgan. Ikkalasi foydalanuvchilarni aniqlash uchun elektron sertifikatdan foydalanadi, ikkalasi pochta xabarlarining konfidensialligini va autentifikatsiyalashni ta’minlay oladi. Biroq sertifikatlarini formatlari ko‘pgina turlichadir.

Tarixan shunday bo‘lganki, pochta xizmatlari orasidagi asosiy farq (elektron pochta orqali xabarlarni yetkazib berish protokollari), OpenPGP va S/MIME, elektron sertifikatlar o‘zaro qanday bog‘langanligi turiga bog‘liq. S/MIME-xizmatda foydalanuvchilar X.509-sertifikatlarga ega (Tavsiyanoma ITU-T X.509), sertifikatlar bog‘langanligining tuzilmasi (sertifikatlash ustuni) uncha ko‘p bo‘lmagan “ildizli tugunlar”ga ega “daraxt”ni aks ettiradi. PGP - xizmatda umuman qarama-qarshi holat, unda “ishongan serverlar tarmog‘i”dan foydalaniladi, ya’ni istalgan foydalanuvchi kimningdir sertifikatini imzolashi mumkin. Bu holatda sertifikatlash ustuni haqiqatda erkin ustun yoki ustunlar yig‘indisini aks ettiradi.

Tarmoq ekranlari va topologiya. Tarmoq ekranlari (“firewall”) AXni ta’minlashni topologik usullarini aks ettiradi. Ya’ni, ular “yaxshi” tarmoq segmenti (korporativ tarmoqning ichki qismi) va segment bilan ulangan “yomon” tashqi tarmoq orasidagi aniq aniqlangan chegaraga bog‘liq, tarmoq ekranining o‘zi esa (TE) ular orasida bog‘lovchi bo‘g‘in bo‘lib xizmat qiladi, ular orqali axborot translyatsiya qilinadi. TE juda foydali bo‘lishiga qaramay, agar albatta ular tegishlicha qo‘llanilsa, tarmoqlarni himoyalash bo‘yicha ularning imkoniyatlarida ma’lum chegaralar mavjud.

Birinchi chegaralash shundan iboratki, TE o‘zi himoyalaydigan korporativ segmentlar ichidan boshlangan hujumlardan himoya bo‘la olmaydi. Bunday hujumlar oqibatining dolzarbligiga qaramay, bunday hujumlar salmog‘i noma’lum (ehtimol hech qachon ma’lum bo‘lmaydi ham), aynan shunday hujumlar AXni ta’minlashda ko‘pchilik muammolarning sababi bo‘lib qoladi. Agar bu muammoga kengroq nazar solsak, u holda TE aniq belgilangan chegarani talab qilishini taxmin qilib, shu darajagachaki, hatto bunday chegara yo‘qolib ketganda ham TE yordam bermaydi (umuman befoyda). Protokollar yordamida shakllanadigan istalgan tashqi ulanishlar, TE orqali xabarlarni atayin tarqatadigan, bir-biriga o‘tadigan tunnellashtirish rejimidagi istalgan aloqa kanallari, himoyalanmagan simsiz LHT yoki IP-bog‘lama bilan boshlanganto‘g‘ri tashqi ulanishlar korporativ hisoblanib,

himoyalanganlik darajasini pasaytiradi. Agar foydalanuvchilar TE orqali trafikni uzatish uchun xavfsizlik protokollarini tunnellashtirish rejimida qo‘llasalar va tunnelning oxirgi nuqtalarida himoyalanganlikning nomaqbul sathini tanlagan bo‘lsalar, TE past samaradorlikka ega bo‘ladi. Agar tunnellanadigan trafik shifrlansa, u holda TE uni ko‘rib chiqolmaydi (nazorat qilolmaydi). TEning ko‘pincha keltiriladigan afzalliklari shundan iboratki, ular korporativ tarmoqning ichki tuzilmasini “tashqi ko‘zlardan” berkitadi (korporativ IP-bog‘lamalar tarkibi). Axborotni “chiqib ketishini” e’tiborga olib, kompyuterlarni muvaffaqiyatli niqoblash ehtimoli juda past.

Yanada tor yondashuvda, TE Internet-tarmog‘i vaInternet-protokollarda bir-biriga o‘tadigan ulanish modelini buzadi. Albatta, hamma protokollar ham o‘z xabarlarini TE orqali oson va xavfsiz tarqatishi mumkin. O‘zini TE yordamida himoyalaydigan tarmoqni korporativ segmentlari, Internet-tarmoqda yangi va foydali axborot manbalaridan “uzilgan” bo‘lishi mumkin.

Agar TE xavfsizlikni umumiy tuzilmasining bir elementi sifatida qo‘llanilsa yaxshiroq ishlaydi. Masalan, aniq sozlangan TE belgilangan $W^3$-serverni funksional bo‘linishi uchun va ma’lumotlar bazasili serverda qo‘llanishi mumkin, ya’ni oxirgilar orasida faqat ochiq aloqa kanali bo‘lishi sharti (trafikni shifrlamasdan) bilan qo‘llaniladi. Xuddi shu tunnellashtirish rejimida faqat shifrlangan trafikni “o‘zidan o‘tkazadigan” TEga ham tegishli. Bunday TEni VPN-tarmoqning bitta segmentini himoya qilishda qo‘llash mumkin. Lekin boshqa tomondan, bu holatda VPN-tarmoqning boshqa segmenti xuddi shunday himoyalangan bo‘lishi kerak.

Kerberos-protokoli. Bu protokol (RFC-4120) ikkita o‘zaro ta’sirlashuvchi tomonlarning hamjihatlikdagi autentifikatsiyalash usuli va kalitli axborotlarni almashishni aniqlaydi. Foydalanuvchini dasturiy Kerberos-moduli maxsus “bilet” va “ishonch hujjatiga” ega. Keyinchalik bu xujjatlarning ikkalasi (ular shifrlangan ko‘rinishda saqlanishi kerak) foydalanuvchi va server o‘rtasida ulanishni o‘rnatish uchun qo‘llaniladi. Server keyin bu hujjatlarning haqiqiyligini tekshirishi mumkin.

Shundan so‘ng server va foydalanuvchi dasturiy Kerberos-moduldan so‘rab olib ularga seans kalit ajratishni so‘rashi mumkin, u ma’lumotlarni shifrlash va yaxlitligini himoyalash uchun qo‘llaniladi.

Dasturiy Kerberos-modul shaxsiy protokollar doirasida qo‘llanilishi mumkin. Biroq u SASL-interfeysi va GSSAPI-interfeysi yordamida AXni ta’minlash usuli sifatida ham qo‘llanilishi mumkin. Hozirgi paytda bu protokolning ba’zi zaif tomonlari ham ma’lum, ammo shunga qaramay u himoyalangan variantda qo‘llanilishi mumkin.

SSH-protokoli. Bu protokol (Secure Shell — SSH) UNIX-o‘xshash tizimlarni dasturiy ta’minoti tarkibiga kiradi, “mijoz/server” ulanishni himoyasini ta’minlaydi. Funksional jihatdan u TLS-protokolini eslatadi, biroq u terminallar bilan olisdagi ulanishlarga xizmat qilish uchun optimallashtirilgan. SSH-protokolining eng ratsional xususiyatlaridan biri, u SSH-protokoli bilan himoyalangan, TCR-protokoli ustida joylashgan boshqa amaliy protokollarning xabarlarini yetkazib berishda tunnelli rejimni ta’minlaydi. Bu xususiyat AX sohasini yaxshi tushunadigan foydalanuvchilarga turli funksiyalarni bajarish, ya’ni himoyalanmagan server hamda tarmoqlar orqali pochta xabarlarini yoki yangiliklarni o‘qish va uzatish imkonini beradi. Ushbu protokol VPN-protokollarni almashtirish uchun mo‘ljallanmagan, ammo u ularning o‘rniga qo‘llanishi mumkin.

## Nazorat savollari

1. MATda mumkin bo‘lgan xavfsizlik tahdidlarining manbalari nimalardan iborat?
2. Bostirib kirish deganda nimani tushunasiz?
3. Kirib borish deganda nimani tushunasiz?
4. Kriptotaxlil nima?
5. Manbaning yolg‘on rad etishi deganda nimani tushunasiz?
6. Xavfsizlik arxitekturasi deganda nimani tushunasiz ?
7. OTO‘Z EM xavfsizlik arxitekturasini tushuntiring.
8. Axborotni himoyalash vositalari nimalar?
9. Internetda xavfsizlik arxitekturasi prinsipini tushuntiring.
10. ISO xavfsizlik arxitekturasi prinsipini tushuntiring.
11. Xizmat ko‘rsatishni rad etishi deganda nimani tushunasiz?
12. Zarar keltiruvchi xatcho‘plarga ta’rif bering.
13. Tahdid manbai nima?
14. Xavf ehtimoli nima?

# QISQARTMALAR RO‘YXATI

| | | |
|---|---|---|
| ADM | - add/drop multiplexer | - kiritish/chiqarish multipleksori |
| ADSL | - Asymmetric Digital Subscriber Line | - Assimmetrik raqamli abonent liniyasi |
| ANSI | - American National Standards Institute | - Amerika xalqaro standartlashtirish instituti |
| ATM | - Asynchronous Transfer Mode | - Asinxron uzatish rejimi |
| ARQ | - Automatic repeat request | - Paketlarni uzatishda avtomatik takrorlash |
| BER | - Bit Error Rate | - Xatoliklarni yuzaga kelishi |
| CDMA | - Code-Division Multiple Access | - Kanallari kod bo‘yicha ajratilgan ko‘p marotaba ulanish |
| DoS | - Differentiated optical Services | - Differensial optik xizmatlar |
| DOD | - Department of Defense | - Axborotni himoyalash tashkiloti |
| DNS | - Domain Name System | - Domen nomlar tizimi |
| ETSI | - European Telecommunication Standards Institute | - Evropa Telekommunikatsiya standartlashtirish instituti |
| FDL | - Fiber Delay Line | - Ma’lum bir vaqt oralig‘ida optik signalni ushlab turush uchun qo‘llaniladigan uzun tolali-optik liniya |
| FTP | - File Transfer Protocol | - Fayllarni qayta uzatish protokoli |
| GII | - Global Information Infrastruc-ture | - Global axborot infratuzilmasi |
| GSM | - Global System For Mobile | - Mobil aloqaning xalqaro standarti |
| HTTP | - Hyper Text Transfer Protocol | - Gipermatnni uzatish protokoli |
| HTML | - Hyper Text Markup Lahguage | - Gipermatn tili |
| IEEE | - Institute of Electrical and | - Elektrotexnika va elektronika sohasidagi |

| | | |
|---|---|---|
| | Electronics Engineers | injinerlar instituti |
| IETF | - Internet Engineering Task Force | - Internet muammolari bo‘yicha shug‘ullanadigan injinerlar guruhi |
| IEC | - International Electrotechnical Commission | - Xalqaro Elektrotexnik Komissiyasi |
| IP | - Internet protocol | - Internet protokol |
| IPv4 | - Internet protocol Version 4 | - Internet protokolning 4-versiyasi |
| IPv6 | - Internet protocol Version 6 | - Internet protokolning 6-versiyasi |
| ISDN | - Integrated Services Digital Network | - Integral xizmatli raqamli tarmoq |
| ISO | - International Organization for Standardization | - Xalqaro standartlashtirish tashkiloti |
| ITU-T | - International Telecommunication Union | - Telekommunikatsiya sohasidagi Xalqaro Telekommunikatsiya ittifoqining standartlashtirish sektori |
| ITU-R | - International Telecommunication Union-Radio Sector | - Xalqaro Telekommunikatsiya ittifoqining radioaloqa sektori |
| IMS | - IP Multimedia Subsystem | - IP multimedia tizimosti |
| LAN | - Local Area Network | - Lokal tarmoq |
| LLC | - Logical Link Control | - Logik kanal bilan boshqarish |
| MAN | - Metropolitan Area Network | - Umumshahar tarmog‘i |
| MAC | - Media Access Control | - Muhitga ulanish bilan boshqarish |
| MPLS | - Multiprotocol Label Switching | - Belgilar bo‘yicha ko‘p protokolli kommutatsiyalash |
| MGCF | - Media gateway controller function | - Transport shlyuzini boshqaruvchi vosita |
| NGN | - Next Generation Network | - Keyingi avlod tarmog‘i |

| | | |
|---|---|---|
| NP | - Network Performance | - Tarmoq xarakteristikasi |
| NMS | - Network Management System | - Tarmoqni boshqarish tizimi |
| OBS | - Optical Burst Switching | - Bloklarni optik kommutatsiyalash |
| OSI | - Open System Interconnection | - Ko‘p sathli ochiq tizim |
| OSSF | - Operation Support Sustem Functions | - Operatsiyalarni ta’minlash tizimining vazifalari |
| OPS | - Optical Packet Switching | - Paketlarni optik kommutatsiyalash |
| PON | - Passive Optical Network | - Passiv optik tarmoq |
| QoS | - Quality of Service | - Xizmat ko‘rsatish sifati |
| RIP | - Routing Information Protocol | - Ma’lumotni marshrutizatsiyalash protokoli |
| RTCP | - Real-time Transport Control Protocol | - Real vaqtdagi transport nazorat protokoli |
| RTP | - Real-time Transport Protocol | - Real vaqtdagi transport protokoli |
| SCS | - Structured Cabling System | - Strukturalashgan kabelli tizimlar |
| SDH | - Synchronous Digital Hierarchy | - Sinxron raqamli ierarxiya |
| STM | - Synchronous Transport Module | - Sinxron transport moduli |
| SMTP | - Simple Mail Transfer Protocol | - Pochta xabarlarini yetkazish protokoli |
| STP | - Shielded Twisted Pair | - Ekranlashgan juftik |
| SLA | - Service Level Agreements | - Xizmat ko‘rsatish sathi haqida kelishuv |
| TCP | - Transmission Control Protocol | - Uzatishni boshqaruvchi transport protokol |
| TMN | -Telecommunications Management Network | - Telekommunikatsiya tarmog‘ini boshqarish |
| TOS | - Type of Service | - Xizmat ko‘rsatish turi |
| UDP | - User Datagram Protocol | - Foydalanuvchi datagrammasi protokoli |
| UTP | - Unshielded Twisted Pair | - Ekranlashtirilmagan juftlik kabel |
| VoIP | - Voice over Internet Protocol | - IP tarmoq bo‘ylab so‘zlashuv trafigini |

| | | |
|---|---|---|
| | | uzatish texnologiyasi |
| VoD | - Video on Demand | - Talab bo‘yicha video |
| VPN | - Virtual Private Network | - Virtual shaxsiy tarmoq |
| WDM | -Wavelength Division Multiplexing | - To‘lqin uzunligi bo‘yicha multipleksorlash |
| WWW | - World Wide Web | - Butun dunyo to‘ri |

## FOYDALANILGAN ADABIYOTLAR RO‘YXATI


1. O‘zbekiston Respublikasi Prezidenti Sh. Mirziyoyevning “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi PF-4947-sonli farmoni.
2. R.I.Isayev, R.K.Atametov, R.N.Radjapova, Telekommunikatsiya uzatish tizimlari. -«Fan va texnologiya», 2011. — 520 bet.
3. N.Yu.Yunusov, R.I.Isayev, G.X.Mirazimova, Optik aloqa asoslari. O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi. – T.: Cho‘lpon nomidagi NMIU, 2014, 368 bet.
4. R.I.Isayev, U.N.Karimova, Metrologiya, standartlashtirish va sertifikatlashtirish. – T., «Fan va texnologiya», 2011, 496, bet.
5. Е.Е.Маликова, Ц.Ц.Михайлова, А.П.Пшеничников. Расчет оборудования мультисервисных сетей связи. Методические указание по курсовому проектированию. 2-ое изд., -М.: Горячая линия – Телеком, 2014.-76 с.
6. Е.С.Чердынцев, Мультимедийные сети: учебное пособие / Томский политехнический университет. – Томск. 2012, - 97 с.
7. О.К.Скляров, Волоконно – оптическиесети и системы связи: Учебное пособие. 2-ое издание. стер. СПБ.: Изд-во «Лань», 2010, 272 с.
8. В.И.Битнер, Ц.Ц. Михайлова, Сети нового поколения – НГН. Учебное пособие для вузов. – М.: Горячая линия – телеком, 2011, - 226 с.
9. Д.С.Гулевич. Сети связи следующего поколения: Учебное пособие / Д.Гулевич – М: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007. -183 с.
10. В.А.Ершов, Н.А.Кузнецов. Мультисервисные телекоммуникационные сети. –М.: Изд-во МГТУ им. Баумана Н.Э., 2003. -432 с.

11. В.Н.Иванов, В.Н.Гордиенко, Г.Н.Поков, Р.И.Исаев и др. Цифровые и аналоговые системы передачи: Учебник для вузов / – М.: Радио и связь, 1995.
12. Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. Сети связи: Учебник для ВУЗов. СПб.: БХВ – Петербург, 2010. 400 с.
13. Б.И.Крук, В.Н.Попантонопуло, В.Н.Шувалов, Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии / под ред. профессора В.П. Шувалова – Изд. 3-е, испр. и доп. – М.: Горячая линия – Телеком, 2003. – 647 с.
14. В.В.Величко, Е.А.Субботин, В.П.Шувалов, А.Ф.Ярославцев. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети. - Москва, Горячая линия – Телеком. 2005. 592 с.
15. А.В.Засецкий, А.В.Иванов, С.Д.Постников, И.В.Соколов, Контроль качества в телекоммуникациях и связи. Часть II, под. редакцией А.Б.Иванова – М.: Компания САЙРУС СИСТЕМС, 2001. 335 с.
16. А.Б.Иванов, Контроль соответствия в телекоммуникациях и связи. Измерения, анализ, тестирование, мониторинг. 4. I. М.: Компания Сайрус Системс. 2001. – 375 с.
17. Л.Е.Варакин, Глобальное информационное общество: Критерии развития и социально – экономические аспекты. – М.: МАС, 2001.
18. Б.С.Гольдштейн, И.М.Ехриель, Р.Д.Рерле, Интеллектуальные сети. – М.: Радио и связь, 2000. 500 с.
19. А.В. Росляков, Общеканальная система сигнализации № 7. –М.: Эко – Трендз, 1999. – 176 с.
20. Khanvilkar S. et al. Multimedia Networks and Communication // Electrical Engineering Handbook / edited by W.K. Chen. – [S. l.]: Academic Press, 2004. – P. 401–425.

21. Perkins C. RTP: Audio and Video for the Internet. – [S. l.]: Addison Wesley, 2003. – 432 p.
22. ITU-T Recommendation 6.803. Architecture of transport networks based on the SDH (06/97).
23. ITU-T Recommendation 1.326. Function architecture of transport networks based on ATM. (11/95).
24. ITU-T Recommendation 6.872. Architecture of optical transport networks. (12/98).
25. ITU-T Recommendation M. 3000 – Overview of TMN Recommendations.
26. ITU-T Recommendation M. 3010 – Principles for a telecommunication management network (TMN).
27. ITU-T Recommendation M. 3020 – TMN interface specification methodology.
28. ITU-T Recommendation M. 3100 – Generic network information model.
29. ITU-T Recommendation M. 3200 – TMN management service: overview.
30. ITU-T Recommendation M. 3300 – TMN management capabilities presented at the F – interface.
31. ITU-T Recommendation M. 3400 – TMN management functions.
32. ITU-T, “Security Architecture for Open Systems Interconnection for CCITT Applications”, Recommendation X.800, 1991.
33. ITU-T, “Information technology – Security techniques – Guidelines for the use and management of trusted third party services”, Recommendation X.842, 2000.
34. ISO, “Information Processing Systems – Open Systems Interconnection Reference Model – Part 1: Basic Reference Model”, ISO/IEC 7498 – 1.
35. ISO, “Information Processing Systems – Open Systems Interconnection Reference Model – Part 2: Security Architecture”, ISO/IEC 7499 – 2.

## MUNDARIJA

“Multimedia li aloqa tarmoqlari”
Fanidan darslik.

5350100-“Telekommunikatsiya texnologiyalari” yo‘nalishi bo‘yicha ta’lim oluvchi talabalar uchun.

“Telekommunikatsiya injiniringi” kafedrasi yig‘ilishida ko‘rib chiqilgan va nashrga tavsiya etilgan (27.03.2018 y.34-sonli bayonnoma).

“Telekommunikatsiya texnologiyalari” fakulteti ilmiy-uslubiy kengashi yig‘ilishida ko‘rib chiqilgan va nashrga tavsiya etilgan
( 2018 y. - sonli bayonnoma).

Muhammad al-Xorazmiy nomidagi TATU ilmiy-uslubiy kengashi yig‘ilishida ko‘rib chiqilgan va nashrga tavsiya etilgan
( 2018 y. - sonli bayonnoma).

Mualliflar: R.I. Isayev

D.X. Ibatova

Mas’ul muharrir: R.I. Isayev

Musahhih: N.D. Yulanova