O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

R.X. Djuraev, Sh.Yu. Djabbarov, B.M. Umirzakov

TARMOQ PROTOKOLLARI

O‘quv qo‘llanma

Toshkent 2017

Mualliflar:

R.X. Djuraev, Sh.Yu. Djabbarov, B.M. Umirzakov

O‘quv qo‘llanmada ma’lumot uzatish tarmoqlarida ishlatiladigan protokollarning vazifalari, qo‘llanilish tamoyillari, tuzilishlari va havfsizlik qoidalari ko‘rib chiqilgan. Ma’lumot uzatish tarmoqlarida kanal pog‘onasining vazifalari, texnologiyalari, tarmoq pog‘onasining protokollari, manzillash tamoyillari, marshrutizatsiya protokollari, boshqarish protokollari, transport protokollarining tuzilishi, vazifalari, QoSni ta’minlash usullari keltirilgan. Tarmoqni sozligini va diagnostikasini amalga oshirish uchun monitoring usullari ko‘rib o‘tilgan.

O‘quv qo‘llanma 5350100 “Telekommunikatsiya texnologiyalari” (Telekommunikatsiyalar) ta’lim yo‘nalishi talabalari uchun mo‘ljallangan.

Muhammad al-Xorazmiy nomidagi

Toshkent axborot texnologiyalari universiteti 2017

MUNDARIJA

KIRISH

Hozirgi kunda dunyo bo‘ylab telekommunikatsiya sohasida fundamental o‘zgarishlar bilan bog‘liq rivojlanishning yangi bosqichi amalga oshirilmoqda. Chuqur ilm talab qiladigan telekommunikatsiya sohasi uchun innovatsion rivojlanish masalalari har doim dolzarb vazifa bo‘lib kelgan. Shu bilan birga sohani innovatsion rivojlantirish, rivojlangan davlatlarning yutuqlarini hisobga olib, mutaxassislarni tayyorlash muhim ahamiyatga ega. Telekommunikatsiya sohasini innovatsion rivojlantirishni amalga oshirish tizimli yondashuv, ya’ni huquqiy, texnologik, tashkiliy va malakali kadrlar bilan ta’minlashni talab qiladi. Zamonaviy sharoitda telekommunikatsiya sohasini innovatsion rivojlantirish masalalarini yechishga qaratilgan kompleks yondashuv bilimli va tajribali mutaxassislarni talab qiladi. Sohani innovatsion rivojlantirish yo‘liga o‘tishda mutaxassislarni tayyorlashda yangicha yondashuvlarga majbur qiladi. Telekommunikatsiya tarmog‘ini innovatsion rivojlantirish uchun ko‘p mutaxassislarni tarmoq texnologiyalari, tarmoq yechimlari va tarmoq integratorlari bo‘yicha tayyorlash kerak. Ma’lumki, telekommunikatsiyaning har bir yangi ko‘rinishi asosan ikkita sababga ko‘ra paydo bo‘ladi;

- unga talabni paydo bo‘lishi;
- mos keluvchi texnik va texnologik asosning mavjudligi.

Halqaro ekspertlarning prognozi bo‘yicha axborotlashtirish masalalari bilan bog‘liq bo‘lgan telekommunikatsiyani innovatsion rivojlantirishning ikkita asosiy yo‘nalishini, ya’ni telekommunikatsiya rivojining asosiy yo‘nalishini va telekommunikatsiya rivojining asosiy kuchini aniqlashga yordam berdi.

Telekommunikatsiya rivojining asosiy yo‘li – bugungi kunda integratsiya jarayonlarini, ya’ni texnologiyalar, tarmoqlar va xizmatlar (turli ko‘rinishdagi axborotlarni uzatishga mo‘ljallangan) kuchaytirish hisoblanadi.

Integratsiya – bu bir maqsadda birlashish va o‘zaro ishlash tushuniladi. Bu bo‘lishi mumkin:

- ko‘plab turli texnologiyalar;

- ko‘plab turli tarmoqlar;
- ko‘plab turli xizmatlar (telekommunikatsiya xizmatlari va axborot xizmatlarining birlashishi, ya’ni multimediya ko‘rinishidagi).

Telekommunikatsiya rivojining asosiy kuchi – bu foydalanuvchilarning muloqot paytida kerakli vaqtda, kerakli joyda, kerakli formada va harakatda maksimum axborotlarni qabul qilish hisoblanadi.

Yuqorida keltirilgan xolat bo‘yicha foydalanuvchilarga yuqori sifatda xizmatlarni taqdim etish telekommunikatsiya operatorlari uchun katta ahamiyatga ega. Bugungi kunda telekommunikatsiya operatorlari tomonidan turli xizmatlar, mobil kompaniyalar tomonidan mobil ilovalar taqdim qilinmoqda. Bu xizmatlar soni kun sayin ortib bormoqda, lekin tarmoqda xizmat ko‘rsatish muammolari ko‘payib bormoqda. Shu sababli tarmoq texnologiyalarini o‘rganishda tarmoq protokollarini ishlatish muhim o‘rinni egallaydi. Tarmoq protokollarini o‘rganishda har xil kompaniyalarning tarmoq qurilmalarini integratsiya qilish muhim ahamiyatga ega.

Ushbu o‘quv qo‘llanmada ma’lumotlar uzatish tarmoqlari va tizimlarini tashkil etish, tarkibiy qismlarning vazifalari, tarmoqlar va ularni ishlash asoslari keltirilgan. O‘quv rejada inobatga olingan “Axborot va kodlash nazariyalari” va “Aloqa tizimlarini modellashtirish va simulyatsiyalash” fanidan ma’ruza, amaliyot va laboratoriya ishlarida asosiy nazariy bilimlarning negizi sifatida qo‘llanilishi nazarda tutilgan.

1. MA’LUMOT UZATISH TARMOQLARINING QURILISH TAMOYILLARI

1.1. Ma’lumot uzatish tarmog‘ining tasnifi

Ma’lumot - bu uzatish va qabul qilib olish uchun mo‘ljallangan axborotning bir ko‘rinishidir. Shu bilan birga axborotning bunday ko‘rinishi yordamida axborotni saqlash va qayta ishlash amallarini bajarish mumkin. Demak, axborot tushunchasi ma’lumot tushunchasiga qaraganda umumiyroq.

Axborot – bu uzatish, tarqatish, o‘zgartirish, saqlash yoki bevosita ishlatish ob’ekti bo‘lgan ma’lumotdir. Axborot deganda qabul qiluvchiga kelib tushadigan har xil ma’lumot tushuniladi. Bu o‘lchash natijalari qandaydir ob’ektni kuzatish haqidagi ma’lumot bo‘lishi mumkin.

Xabar - axborot taqdim qilish shakli hisoblanadi. Bitta xabar bir qancha shaklda taqdim qilinishi mumkin. Masalan, telefon orqali berilayotgan axborot uzluksiz ko‘rinishda yoki telegramma ko‘rinishida, ya’ni diskret ko‘rinishda taqdim qilinishi mumkin. Telegraf orqali ma’lumot uzatilganda, axborot harflar yig‘indisi, ya’ni so‘z ko‘rinishida va sonlarda taqdim qilinadi.

Xizmat - yuqori pog‘ona komponentlari ixtiyoriga beriladigan joriy pog‘onaga tegishli funksional imkoniyatlar to‘plamidir.

Interfeys - ikkita qurilma yoki tizimlar chegarasida ularning to‘liq birga ishlashini ta’minlovchi qurilmalar va protseduralar to‘plami.

Axborot kommunikatsiya sohasida protokol atamasi ma’lumotlarni uzatish, qabul qilish kabi jarayonlarni belgilovchi qoidalar to‘plamiga aytiladi.

Protokollar - bu qoida va texnik protseduralar bo‘lib, bir nechta qurilma yoki dasturlarni ishlash jarayonida ularni bir-biri bilan muloqotda bo‘lishini ta’minlaydi.

Protokollarga taalluqli 3 ta asosiy jihat mavjud:

1. Bir qancha protokollar mavjud bo‘lib, bularning hammasi turli aloqalarni ta’minlashga xizmat qiladi. Har bir protokol maqsadga ko‘ra har xil topshiriqlarni

bajaradi.

2. Protokollar OSI modelining turli pog‘onalarida ishlaydi. Protokolning vazifasi uning ishlash pog‘onasidan kelib chiqib aniqlanadi.

3. Bir qancha protokollar birgalikda ishlashi mumkin. Ular protokollar steki yoki protokollar to‘plami turkumida bo‘ladi.

Protokollar stekining pog‘onalari OSI modelining pog‘onalari bilan mos keladi. Alohida vazifalarni boshqarish uchun har bir pog‘onada har xil protokollar ishlatiladi. Har bir pog‘onaning o‘zida qoidalar to‘plami bo‘ladi.

Protokollar shartli ravishda quyidagicha tasniflanishi mumkin:

- internet tarmog‘ining asosiy protokollari: IP, ICMP, TCP, UDP;
- transport protokollari: RTP, RTCP;
- signal protokollari: SIP, H.323, SIGTRAN, MEGACO/H.248, MGCP, RSVP, SCTP, ISUP, BICC, SCCP, INAP;
- marshrutizatsiya protokollari: RIP, IGRP, OSPF, IS-IS, EGP, BGP;
- axborot xizmatlari va boshqaruv protokollari: SLP, OSP, LDAP;
- xizmat protokollari: FTP, SMTP, HTTP, G.xxx (kodeklar uchun), H.xxx.

Aloqa kanalida ma’lumot uzatish avtomatlashtirilgan tizimdan foydalanib, bu ma’lumotli hujjatlarni xat tashish yo‘li (yoki pochta bilan) va ko‘chirish yo‘li bilan tizim ma’lumotini boshqarib turadi. Ma’lumot uzatishga xizmat qiladigan idora (muassasa) hujjatlarini tarqatishga mexanik va qo‘l yordamida ko‘chirishlardan foydalaniladi. Bunday xizmatlar kichik kapital (mablag‘) yordamida ma’lumotni ohirigacha aniq hujjatlarni uzatishni qayd qiladi va o‘rta pog‘onali punktda ro‘yxatga olib, uni tekshirib (nazorat qilib) turadi. Past operativ (tezlikda) uzatish – foydalanish talablariga javob bera olmaydi. Shuning uchun ham avtomatlashtirilgan ma’lumot uzatish tizimidan foydalanib ma’lumotni operativ yetkazib beradi.

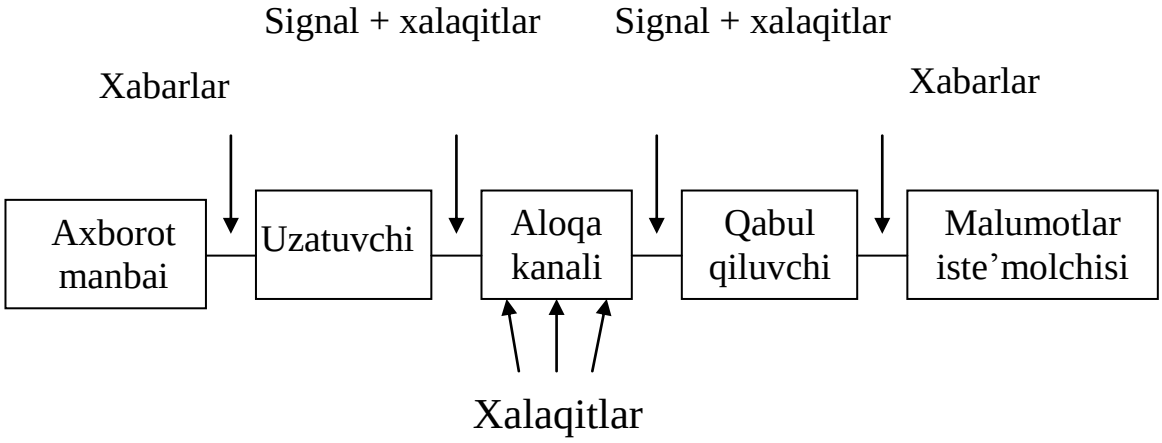
Vositalar to‘plami, ma’lumot uzatishga xizmat qilish uchun ma’lumot uzatish tizimini chaqirib beradi.

Uzatish tizimida ma’lumotni bevosita iste’molga va manba uzatish tizimida abonentlar, kompyuterlar, marshrutizatorlar, ma’lumot saqlash qurilmalari, telefon

apparatlari, peydjerlar, ajratib turuvchi datchiklar, bajaruvchi qurilmalar va odamlar bo‘lishi mumkin.

Uzatish tizimini tarkibiga quyidagilarni kiritishimiz mumkin (1.1-rasm):

1. Uzatish kanali (AK – aloqa kanali);
2. Ma’lumot uzatuvchi qurilmalar;
3. Ma’lumot qabul qiluvchi qurilmalar.



1.1-rasm. Ma’lumot uzatish tizimi

Uzatish abonent xabarini signalga tubdan o‘zgartirib tarqatish va aloqa kanaliga uzatish uchun xizmat qiladi. Qabul qilgich signalni xabarga qayta aylantirib, abonentga yetkazib berish uchun xizmat qiladi.

Ma’lumot uzatishdagi noaniqliklarni kelib chiqishiga sabab, o‘tkazgich aniqligini buzilishi tufayli, gapirganda qabul qilgichlarda yuzaga keladi. Aloqa kanaliga tashqi ta’sir va shovqinlarni ta’siri natijasida ham ma’lumotni aniqligi buziladi.

Ma’lumot uzatish tizimlarini asosiy sifat ko‘rsatkichlari quyidagilar:

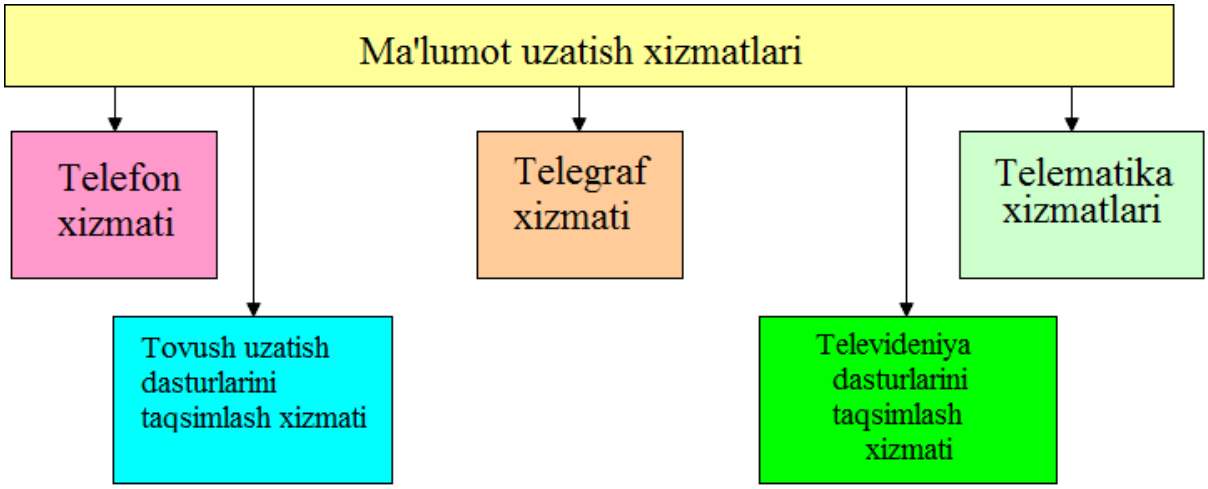
- o‘tkazish qobiliyati;
- ishonchlilik;
- ishlash ishonchligi.

Ma’lumot uzatish tizimidagi o‘tkazish qobiliyati – bir vaqtda tizimni ishlash extimolligi katta bo‘lmagan hajmdagi ma’lumot to‘plamiga ega bo‘lganda

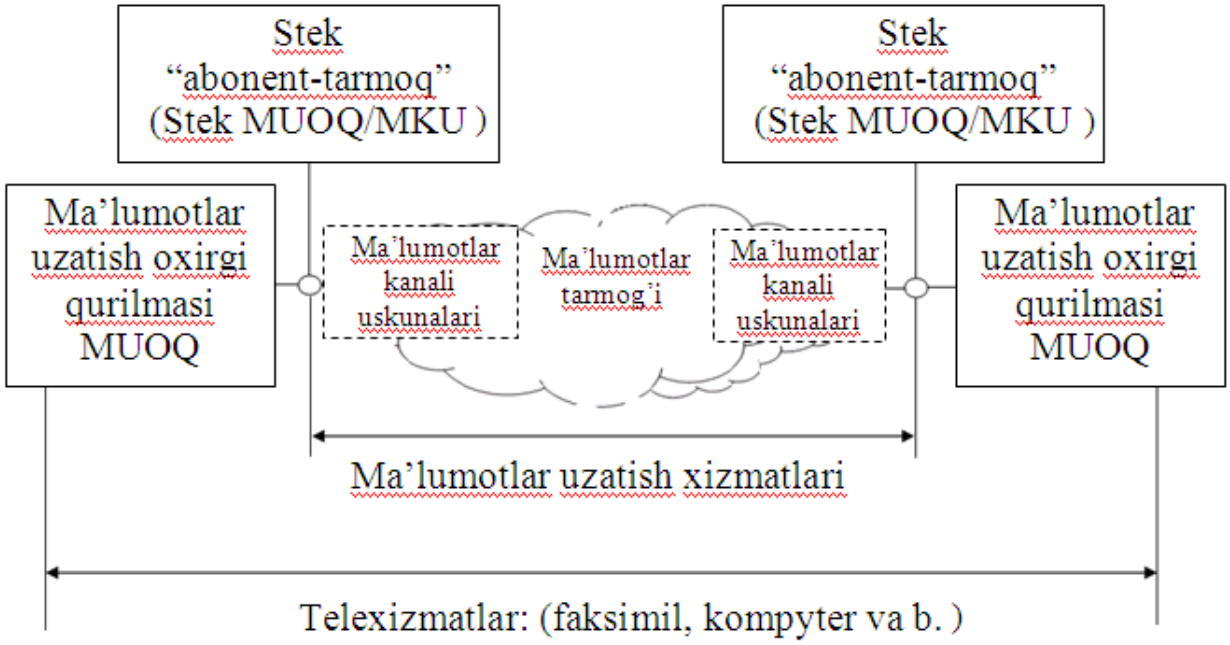
yaxshilanadi. O‘tkazish qobiliyati tizimni aloqa kanali va signalni fizik xususiyatlarini belgilab beradi. Shuningdek bu sifat ko‘rsatkichi kanaldan yuqori tezlikda ma’lumot uzatilishiga bog‘liqdir.

Ma’lumotlar uzatish tizimi 2 guruhga bo‘linadi:

1. Ma’lumot uzatish xizmatlari (1.2a va 1.2b rasm);
2. Ma’lumot uzatish tarmoqlari.



1.2a)



1.2b)

1.2 – rasm. Ma’lumot uzatish xizmatlari

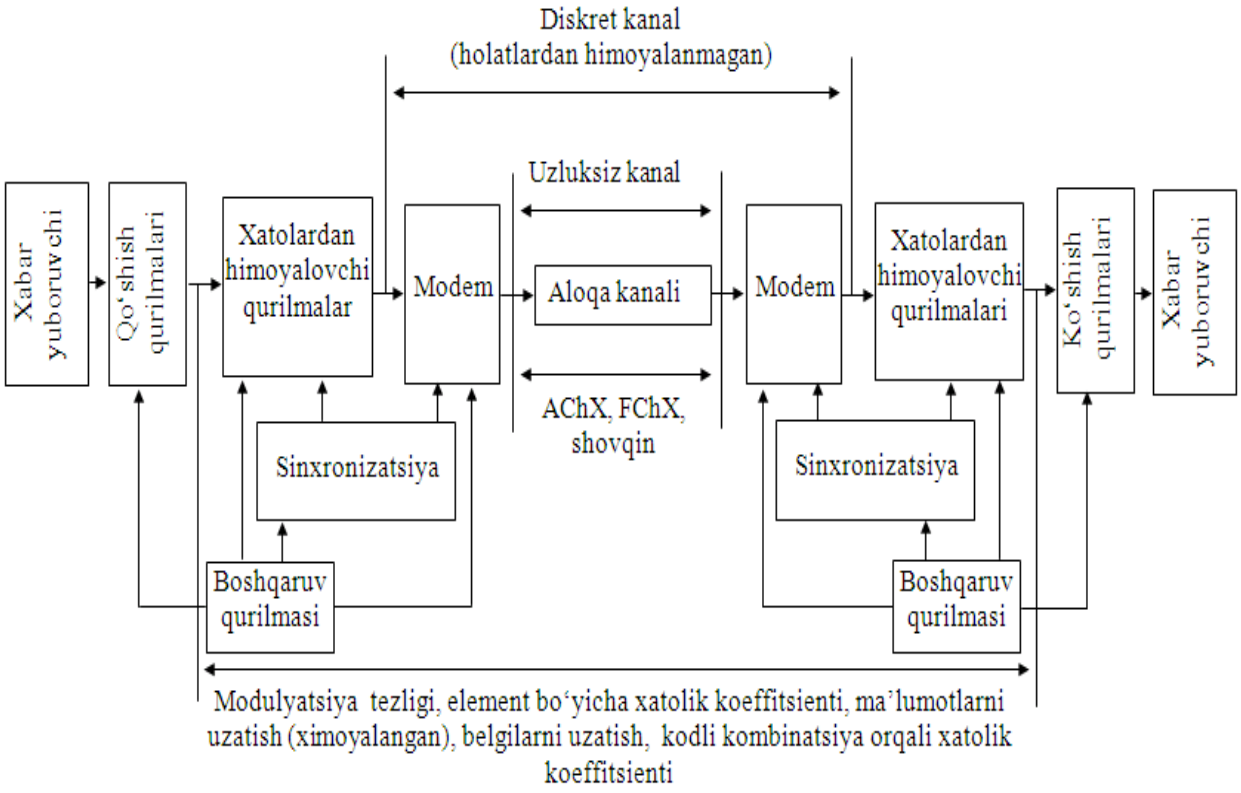
Ma’lumki, har-xil turdagi axborotlarni (ovozli, matn, ma’lumotlar, grafika,

tasvir) uzatish uchun iste'molchilarga taqdim etiladigan xizmatlar to‘plami ma'lumot uzatish xizmati deyiladi.

Ma'lumot uzatish tarmoqlari deb - ma'lumot uzatish xizmatlarini yetkazib berish imkoniyatlarini ta'minlovchi texnik vositalar to‘plamiga aytiladi.

Ma'lumot uzatish tizimlariga quyidagilar kiradi (1.3-rasm):

- terminal qurilmalar;
- kommutatsiya vositalari;
- uzatish tizimlari;
- aloqa kanallari.



1.3 – rasm. Ma'lumot uzatish tizimining tuzulishi

Ma'lumot uzatish tarmoqlari ohirgi qurilmalarni o‘z ichiga olmaydi.

Quyidagi 3 sabab xatolar manbai bo‘lishi mumkin (1.1-jadval):

1.1– jadval.

Asosiy aloqa ko’rsatkichlari

Aloqa xizmati	**Aniqlik**	**Paketlarni yo‘qolish extimolligi**	**Paketlar noto‘g‘ri manzil bo‘yicha yuborilish extimolligi**
Telefoniya	10^{-7}	10^{-3}	10^{-3}
Axborot uzatish	10^{-7}	10^{-6}	10^{-6}
Televideniya	10^{-6}	10^{-8}	10^{-8}

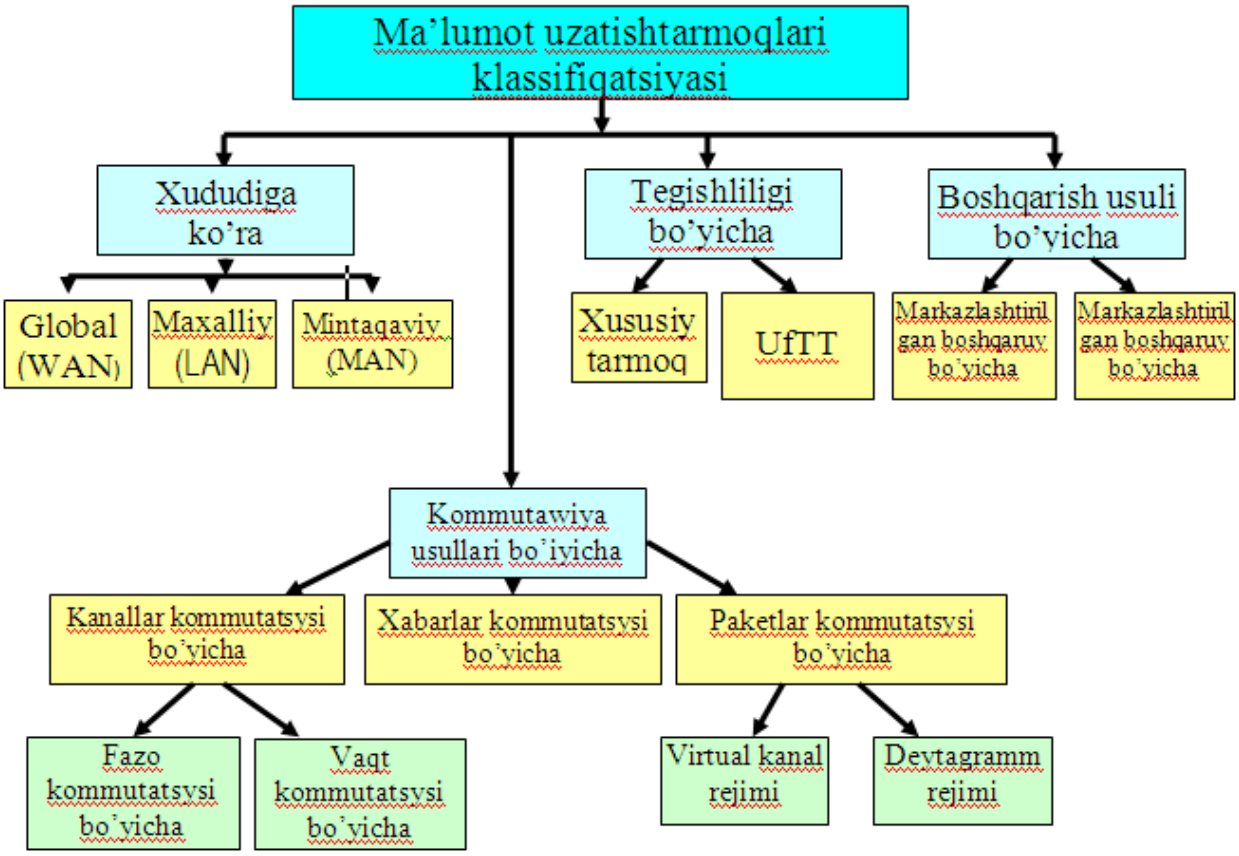
Boshqa telekommunikatsiya tarmoqlari kabi ma’lumot uzatish tarmoqlariga ham ishonchlilik, yashovchanlik, iqtisodiy va keyinchalik takomillashtirish bo‘yicha talablar qo‘yiladi.

Ko‘pchilik umumiy foydalanish tarmoqlari ierarxik tuzilish asosida quriladi. Ma’lumot uzatish tarmog‘ining ierarxik tuzilishdagi afzalligi axborot almashuvida har xil ierarxik satxlarga xizmat ko‘rsatishdir. Tuzilishlardan qaysi birini tanlash foydalanuvchi talabi, yuklama hajmi va boshqa faktlarga bog‘liq.

Ierarxiya tarmog‘i yuqori satxlarida ishonchlilikning yetarlicha yuqori ko‘rsatkichlarini ta’minlash zaruriyatida “To‘liq bog‘lanishli” tuzilishlari ishlatiladi.

Ma’lumot uzatish ishonliligi – bu ma’lumot uzatishda buzilishlarga bardoshliligidir.

Ishlash ishonchliligi – tizim funksiyalarini hammasi to‘g‘ri va to‘liq bajaralishini bildiradi.



1.4 – rasm. Ma’lumot uzatish tarmoqlarining tasniflanishi

Aloqa kanalida ohirgi qurilmaga (manba va ma’lumotni qabul qiluvchi qurilmaga) terminallarni to‘g‘ridan-to‘g‘ri bog‘lanishi – ma’lumot uzatish apparaturasi deyiladi. Ma’lumot uzatish apparaturasiga modem xizmatini, adapter terminallari, tarmoq kartasini misol qilishimiz mumkin. Ma’lumot uzatish qurilmasini ishlashi uzatishlarga javobgarlik, fizik tuzilishi tekislanishi va aloqa liniyasining aniqligini ta’minlab berishiga xizmat qiladi.

Bugungi kunga kelib telekommunikatsiya texnikasi axborotni 5 ta ko‘rinishda uzatib kelmoqda:

– matnli (tekstli);
– ovozli;
– grafikli;
– videoli;
– ma’lumotli.

Masalan, biror bir hodisani tasvirlashda axborotni quyidagi usullaridan foydalanish mumkin:

– rang, xid va ta’m orqali 2% dan 5% gacha ifodalash mumkin;

– matn (harf va raqamlar) orqali 7% gacha ifodalash mumkin;

– ovoz (tovushning past-balandligi, intonatsiya va pauzalar) orqali 38% dan 45% gacha ifodalash mumkin;

– xarakat va mimikalar orqali 35% dan 52% gacha ifodalash mumkin;

– multimediya xizmati (xarakat va ovozning birgalikda mujassamlashgan holda uzatish) orqali 95% dan 98% gacha uzatish mumkin.

Har bir xabar turlari uchun o‘tkazish yo’lagi mavjud (1.2-jadval).

1.2-jadval.

Xizmat turlari

Xizmatlar	
Interaktiv	Taqsimlanishi
Dialogli Xabarlar almashishi Ma’lumot qidirish	Shaxsiy boshqarishsiz foydalanish tomoniga Shaxsiy boshqarishdan foydalanish tomoniga

Ma’lumot uzatish xizmati 5 ta ko‘rinishdagi xabarlarni turli vositalar bilan uzatishni amalga oshiradi. Ma’lumot uzatish xizmati uchun texnik - qurilmalarni tuzilishsini va telekommunikatsiyani asosiy tarmog‘idan operatorni ma’lumot uzatish xizmatidan foydalanishga ruxsat berishi va aloqani qabul qilishi lozimdir.

1.3 – jadval.

O‘tkazish yo’lagining talabi uchun qo‘shimcha yo’laklarni ajratish

Ilova	Uzatish turi	Uzatish formati	Uzatish tuzilishsi	Uzatish tezligi (siqishsiz)	Uzatish tezligi (siqsh bilan)
So‘zlashuv va musiqa	Telefon	611÷6723.1	8 kbit/s*8 bit	64 kbit/s	8÷32 kbit/s
	Telekonferensiya		16 kbit/s*8 bit	128 kbit/s	48 ÷ 64 kbit/s
	CD – audio	MP-3	44.1 kbit/s *16 bit	705.6 kbit/s	128 kbit/s
Tasvir	Odatiy ruxsat etilgan tasvir	SVGA	640 pix/lin* 480 lin/c* 8 bit/pix	2.458 mbit/s	24-245 kbit/s
		JPEG	720 pix/lin* 576 lin/s* 16 bit/pix	6.636 mbit/s	104 - 830 kbit/s
	Yuqori sifatli tasvir		1280 pix/lin* 1024 lin/s* 24 bit/ pix	31,46 mbit/s	0,3 – 3 mbit/s
Video tijorat	Videofon	QSIF (H.261)	176 pix/lin	9,115 Mbit/s	P*64 kbit/s (P=1,2)
		MPEG - 4 (H.320)	176 pix/lin* 144lin/k*12 bit/pix*10 kbit/s	3,04 Mbit/s	64 kbit/s
	Video - konferensiya	GIF (H.261)	352 pix/lin* 288 lin/k* 12 bit/pix * 30 k/s	36,5 Mbit/s	M*368 kbit/s (m=1,2,3,4,5)
		MPEG-1 (PAL)	352 pix/lin* 288 pix/k*12 bit/pix* 25k/s	30,4 Mbit/s	1,15 – 3 Mbit/s
		MPEG-1 (NTFS)	352 pix/lin* 288 pix/k*12 bit/pix* 30k/s	30,4 Mbit/s	1,15 – 3 Mbit/s
Ko‘ngil-ochar video	VCR	CIF (MPEG-2)	720 pix/lin* 576 pix/k*12 bit/pix* 25k/s	30,4 Mbit/s	4 Mbit/s
	Keng yoyiluvchi TV	MPEG-2 (PAL)	720 pix/lin* 576 pix/k*12 bit/pix* 25k/s	124,4 Mbit/s	15 Mbit/s
		MPEG-2 (NTFS)	720 pix/lin* 576 pix/k*12 bit/pix* 25k/s	124,4 Mbit/s	15 Mbit/s
	Yuqori sifatli TV	NDTV	1920 pix/lin* 1080 lin/k * 12 bit/pix * 25 k/s	994,3 Mbit/s	135 Mbit/s
		MPEG-3	1920 pix/lin* 1080 lin/k * 12 bit/pix * 30 k/s	745,8 Mbit/s	20 - 40 Mbit/s

Dialogli xizmat (1.4 - jadval) - shaxsiy kompyuter va foydalanuvchi orasida uzatishdan foydalanish amaliy real masshtab vaqtida aniq xizmatlarni ko‘rsatadi. Bu ma’lumot oqimi simmetrik va simmetrik bo‘lmagan muhitlarda bo‘ladi. Sifatli dialogli xizmatlarga telefon xizmati, ma’lumot uzatish xizmati va videokonferensiyali aloqa xizmatlari misol bo‘la oladi.

1.4-jadval.

Dialogli xizmat tavsifi

Ma’lumot turi	**Xizmatlar na’munasi**	**Yaratilishi**
Ovoz va tasvirlarni xarakatlantirish	Videotelefon	Ikki abonent orasidagi masofada ovozli, xarakatlanuvchi tasvirni, xarakatlanmaydigan tasvirni va hujjatlarni uzatadi
	Keng yo’lakli videokonferensiyali aloqa	Guruhni abonentlar orasidagi masofada ovozli, xarakatlanuvchi tasvirni, xarakatlanmaydigan tasvirlarni videoskanerlarni va hujjatlarni uzatadi
	Video kuzatuv	Bino xavfsizligini ta’minlash uchun xarakatli nazorat
	Video va audio ma’lumotni uzatish xizmati	TV signallarni uzatish dialogli video/audio ma’lumot almashishini yetkazib berish
Ovozli	Ovozli ko‘p dasturlarni uzatish	Sinxron ko‘chirish ko‘plab dasturlar uzatish
Ma’lumotli	Xizmat raqamli ma’lumotni yuqori tezlikda uzatish	Video ma’lumorlarni uzatish ma’lumotni boshqa ko‘rinishda ko‘chirish; xarakatlanmaydigan tasvirni ko‘chirish; taqsimlashni tashkil etishni hisoblash
	Yuqori tezlikli telesignalizatsiya va telenazorat	Real vaqt masshtabida tekshirish. Telemetriya. Trevoga tizimi

1.4-jadval davomi

Hujjatlar	Yuqori tezlikli telefaks	Abonentlar orasida matn (tekst)li, grafikli hujjat va rasmlar almashish
	Yuqori sifatli tasvirlarni almashish	Professional rasmlarni rentgenli rasm va boshqa meditsinaga oid rasmlar, o‘yinlar
	Hujjatlarni almashish	Foydalanishlar orasida turli hujjatlarni almashish

1.5-jadval.

Xabarlarni almashish tavsifi

Ma’lumot turi	**Keng yo’lakli xizmat na’munasi**	**Qo‘llash na’munasi**
Xarakatli tasvir va ovozlar	Video (video pochtasi) uchun pochta qutisi	Elektron pochta qutisi uchun xarakatli tasvirlarni va ovozlarni yetkazishda uzatib boradi
Hujjat	Pochta qutisi uchun hujjatlar	Elektron pochta qutisi uchun turli hujjatlar

Xabarlar almashish xizmatini (1.5-jadval) belgilash uchun to‘g‘ridan to‘g‘ri bo‘lmagan aloqalardan foydalanish orasida, xabarlarni himoyalab ham turadi. Markaziy qurilma oralig‘idagi punktlarni himoyalashda, avtomatik marshrutizator ma’lumotlarni qabul qiluvchiga yo‘naltiradi. Bu vazifa xabarlarni almashish jarayonida uni sifatini oshiradi. Xabarlarni himoya qilishda, elektron pochta qutisi yoki “xabarlarni qayta ishlab chiqish” tizimida muharrirlik funksiyasidan foydalanib xabarni tiklab beradi. Xabarlarni ishlab chiqish funksiyasi yoki elektron pochta qutisidagi matnlar, ma’lumot, rasmlar va boshqa xabarlar almashish xizmatiga misol bo‘la oladi.

1.6 - jadval.

Ma’lumot qidirish xizmati

Ma’lumot turi	**Na’munali keng yo’lakli xizmat**	**Qo‘llanish extimolligi**
Matnli, ma’lumotli, grafikli, ovozli, xarakatlanuvchi va xarakatlanmay-digan tasvirlar	Keng yo’lakli video matn	Video matn, xarakatli tasvir, o‘qitishda, mashqda, tarbiyalashda, reklama, yangiliklar xizmatida
	Videoni qidirish	Xizmatlar qilishda, o‘qitish va mashqda
	Yuqori sifatli tasvirlarni qidirish	Qidirishdan maqsad o‘qitish va mashq. Professional tasvirlarni uzatish, rentgentli va boshqa masalalar
	Hujjatlarni qidirish	Ma’lumot markazidan, arxivdan va boshqa hujjatlarni ochib qidirib olish
	Ma’lumot qidirish	Dasturlardan qidirib olib, undan foydalanish

Ma’lumot qidirish xizmati (1.6 - jadval), ma’lumotni turli zahiralardan foydalanib olishi mumkin.

Zahiralar qismi, ma’lumotni aloqa administratoriga yetkazib berishi yoki ma’lumotni so‘ralgan joyga yetkazib beradi.

1.7 va 1.8 - jadvallarda foydalanuvchiga tegishli xududni boshqarish va taqsimlash xizmatini mavjudlik tavsifi ko‘rsatib o‘tilgan.

1.7 - jadval.

Shaxsiy foydalanishni taqsimlash xizmatisiz xududni (joyini) boshqarish

Ma’lumot turi	**Kengaytirilgan xizmatlarga na’muna**	**Qo‘llanish extimolligi**
Ma’lumot	Raqamli ma’lumotni yuqori tezlikda uzatib taqsimlash xizmati	Ma’lumot uzatishini taqsimlash
Matnli, grafikli, xarakatsiz tasvir	Hujjatlarni uzatish xizmatini taqsimlash	Elektron gazeta, Elektron yangilik
Ovozli va xarakatli tasvir	Video ma’lumot xizmatini taqsimlash	Video va ovozli signallarni taqsimlash
TV	TV xizmatini taqsimlash sifatini muximligi (NTFS, PAL, SECAM)	TV dasturlar
TV	TV xizmatini taqsimlash sifatini oshirish: - TVVI; - TV yuqori ultra sifati	TV dasturlarni taqsimlash
	Pullik TV (pullik TV (ko’rish uchun to’lov, kanal uchun to’lov))	TV dasturlarini taqsimlash

Taqsimlash xizmati ma’lumotni borligini va yo‘qligini tekshirib, ma’lumotni shu xududda to‘g‘ri (aniq) qabul qilib foydalanishni, bitta markaziy manbadan abonentlarga tarqatadi.

Uzatish vaqtida taqsimlash xizmati shaxsiy boshqaruvsiz xabarlar oqimini uzluksiz foydalanuvchi xududida taqsimlanishini, foydalanishi mumkin bo‘lgan va bo‘lmagan tasvirlarni ma’nosiga va o‘zgarishlariga alohida e’tibor qaratadi.

Televideniya ko‘rsatuvlarini va ovozli dasturlar olishda taqsimlash xizmati vakil bo‘lib hisoblanadi.

1.8-jadval.

Xududiy foydalanishda shaxsiy boshqarishni taqsimlash xizmati

Ma’lumot turi	**Keng yo’lakli xizmat na’munasi**	**Qo‘llanish sohasi**
Matnli, grafikli, xarakatlanmaydigan tasvir	Video grafikli kanalni joriy qilish	O‘qitish va shug‘ullanishda, reklamada, yangliklarda, dasturlarda

Telekommunikatsiya kanallarida ma’lumotni uzatishdan maqsad, aloqani tashkil etuvchi nuqtalarni aniqlab, ma’lumotni shu nuqtalardan maxsus tuzilgan qurilmalar majmuasiga uzatishdan iborat. Bu esa ma’lumot uzatish tarmog‘i deyiladi.

1.2. Ma’lumot uzatish tarmoqlariga qo‘yiladigan talablar

Ma’lumot uzatish tarmog‘iga va aloqaning boshqa tarmoqlariga qo‘yiladigan talablar quyidagilar:

1. Ishonchlilikka bo‘lgan talab tarmoqning ma’lum chegarasida oldindan kelishilgan barcha harakteristikalarni qo‘llab quvvatlovchi funksiyani ta’minlash kerakligini bildiradi.

2. Yashovchanlikka talab tarmoqning ma’lum chegarasida barcha oldindan kelishilgan barcha harakteristikalarni qo‘llab quvvatlovchi funksiyasi mavjud bo‘lib, aniq sondagi ichki va tashqi buzilishlar yuz berganida tarmoqning ishlash imkoniyatini saqlab qolishini bildiradi.

3. Iqtisodiyligi. Tarmoqni ta’minlash shartlari bo‘lgan holda bunday tarmoqni yaratish va amalda qo‘llash xarajatlarini optimallash.

4. Kelajakda rivojlana olish imkoniyati. Bu talab tarmoqni doimiy ravishda yuklanishning oshib borishi bilan bog‘liq bo‘lib, ko‘p hollarda tarmoq yuklanishi qay darajada ekanligini aniqlashning iloji yo‘q.

Tarmoq konfiguratsiyalarini amalga oshirish oddiy jarayon bo‘lmasligi va tarmoq faoliyati boshidanoq samarali bo‘lishi kerak. Bu konfiguratsiyalar kelajakka moslashuvchan etib yaratilishi kerak. Shu bilan birga ma’lumot uzatish tarmoqlarining yangi imkoniyatlari paydo bo‘lganda, tarmoq konfiguratsiyalari bu imkoniyatlarni o‘zlashtirish qobiliyatiga ega bo‘lishi kerak.

Umuman olganda ma’lumot uzatish tarmog‘i quyidagi talablarga javob berishi kerak:

1. Integrallik – tarmoq har xil turdagi axborotlarni ularning uzatilish sifatiga mos kelgan holda uzatish imkoniyatini ta’minlashi kerak;

2. Samaralilik – uzatishda tarmoq o‘z zahiralaridan samarali foydalanish imkoniyatini ta’minlashi kerak;

3. Axborotni yetkazib berishning ishonchliligi – tarmoq qurilmalari o‘rtasida aloqa uzilganida ham tarmoq axborotni yetkazib berishni kafolatlashi kerak;

4. Yashovchanlik – tarmoq har qanday ko‘rinishdagi axborot uzatish harakteristikasi bo‘yicha ishlash qobiliyatiga ega bo‘lishi shart. Faoliyatini ma’lum sabablar tufayli to‘xtatgan tarmoq qurilmalari sonining oshishi tarmoqning xizmat ko‘rsatish sifatini tushirib yuboradi, shunday bo‘lsa-da, tarmoqning ikki punkti o‘rtasida biror ko‘rinishdagi axborotni yetkazib berish bajarilishi kerak;

5. Mobillik – tarmoq har xil nuqtalarda joylashgan foydalanuvchilarning tarmoqqa ulanishi va tarmoqdan chiqishi vaqtida boshqa foydalanuvchilarning tarmoqdagi faoliyati buzmasligi va normal ishlashi kerak;

6. Amalda qo‘llashning uzluksizligi – tarmoqda o‘z ishlash xususiyatini yo‘qotmasdan o‘zining ishdan chiqqan qurilmalari va qurilmalararo aloqalarni aniqlash, lokallash va bartaraf etish imkoniyati bo‘lishi kerak;

7. Rivojlanuvchanlik – tarmoq ham alohida guruh doirasida, ham tarmoq orqali birlashtiriladigan guruhlar soni bo‘yicha foydalanuvchilar sonini oshirish imkoniyatini ta’minlashi kerak;

8. Shovqindan himoyalanganlik – tarmoqda aloqa kanalining xatoliklar ehtimoli katta bo‘lganda ham biror ko‘rinishli ma’lumotni yetkazib berish xatolik ehtimoli kichik bo‘lishi ta’minlanishi kerak.

Tarmoqning alohida qismlarida qisqa muddatli shovqinlar, to‘siqlar bo‘lganida ham o‘z faoliyatini davom ettira olishi kerak. Tarmoq shovqinni bartaraf etishda o‘z normal faoliyatini tiklay olishi kerak. Yuqoridagilarni hisobga olib ma’lumot uzatish tarmoqlarini yaratishda quyidagi talablarning qondirilishi hisobga olinishi kerak:

1. Ko‘plab foydalanuvchilar va chiziqli interfeyslarga taqdim etilishi kerak bo‘lgan mavjud aloqa tarmoqlari infratuzilishsidan foydalanish, jumladan har xil jinsli transport tarmoqlari mavjud bo‘lgan tarmoq qurilmalari o‘zaro ishlash imkoniyati nazarda tutilgan;

2. Katta xarajatlar jalb etmasdan tarmoq zahiralarini oldindan taqsimlash imkoniyati, buning uchun tarmoqning o‘zi bir turdagi qurilmalarga asoslangan bo’lishi afzal, qurilmalar esa umumiy modullarning maksimal universalligi bilan modulli tamoyil asosida qurilishi kerak;

3. Tarmoqning kengaya olish imkoniyati;

4. Yangi tarmoq xizmatlarini taqdim etish uchun aniq hajmdagi zahiraning mavjudligi, tarmoqni qurish uchun foydalaniladigan qurilmalar ochiq arxitekturaga ega bo‘lishi kerak, ochiq arxitekturada chiziqli va foydalanuvchi interfeysini doimiy ravishda kengaytirish mumkin;

5. Yangi texnologiyalarga mo‘ljallangan boshqarish tizimini qo‘llash bo‘yicha variantlarning mavjudligi;

7. Tarmoq qurilmalarini amalda qo‘llashda tarmoq faoliyatida uchrashi mumkin bo‘lgan buzilishlar va rad etishlardan ichki va tashqi himoyaning mavjudligi – tarmoqda va tarmoq qurilmalarida bloklarni zahiralash, himoyaviy almashinuvni qo‘llash, oldindan marshrutlash va h.k;

8. Zahirada elektr manbaalarining, manbaaning kafolatlangan tizimlarining mavjudligi va h.k.;

9. Tarmoq narxi va amalda qo‘llash xarajatlarini optimallashtirish bo‘yicha

mexanizmlarining mavjudligi – qurilmaning optimal narxi, qurilmani amalda qo‘llashning osonligi, xizmat ko‘rsatishni soddalashtirish uchun markaziy boshqaruv tizimining mavjudligi, barcha jarayonlarni maksimal avtomatlashtirish (uzatish, kommutatsiya, nazorat va boshqaruv).

Har bir tizimni bir-biri bilan mantiqiy bog‘langan tizimlar majmuasi ko‘rinishida tasvirlash mumkin. O‘z navbatida qism tizim komponentlar majmuasi hisoblanadi. Alohida olingan qism tizimda elektr signallarini uzatish, sinxronlashtirish jarayonini bajarish, fazalash, xatolardan himoya qilish, marshrutlash, kommutatsiya, aloqa o‘rnatish va h.k.larni bajaradi.

Telekommunikatsiya tarmog‘idan bitta ma’lumot uzatish xizmati yoki bir nechta ma’lumot uzatish xizmatlari, ma’lumotni bitta yoki bir nechta telekommunikatsiya tarmog‘iga uzatishi mumkin. Bu turdagi xizmatlarga tarmoqning ma’lumot uzatish xizmati deb yuritiladi.

Ma’lumot uzatish tarmog‘ini o‘zi ma’lumotni jixozlab tugatadi (beradi). Bu telekommunikatsiya tarmog‘ining funksiyalarini himoyalashda va abonentlar orasidagi ma’lumot uzatishni ta’minlash uchun xizmat qiladigan tarmoq hisoblanadi.

Ma’lumot uzatish xizmatini bazasi o‘z ichiga telexizmatlarni, Ma’lumot uzatish xizmatini, tarmoqdagi telekommunikatsiya funksiyalarini himoyalash va abonent terminallarini qamrab oladi. Bu bazada istalgan ma’lumot uzatish xizmatini tashkillashtirishi mumkin. Misol uchun, kompyuter xizmatlari (kompyuterlar orasida ma’lumot almashish), telegraf xizmati va telematika xizmatlari kiradi.

Milliy ma’lumot uzatish tarmog‘i asosida har xil ma’lumot uzatish tarmoqlari va xizmatlari o‘rtasida aloqani tashkil etishning asosiy maqsadi quyidagilardan iborat:

1. Ma’lumot uzatish xizmatlaridan va tarmoqlaridan foydalanishda foydalanuvchilarni va davlatning katta qismini qamrab olishi;

2. Foydalanuvchilar va aloqa operatorlari o‘rtasida ma’lumot almashilganda har xil ma’lumot uzatish xizmatlaridan foydalanish imkoniyatini ta’minlashi;

3. Zamonaviy talab darajasida ma’lumot uzatish xizmatini foydalanuvchiga taqdim etishda sifatli ko‘rsatkichlarga mos kelishini ta’minlashi;

4. Ma’lumot uzatish xizmatiga va tarmog‘iga asoslangan xizmatlarning yashovchanligini va ishonchliligini oshirishni;

5. Davlat organlarini ma’lumot uzatish xizmatlariga bo‘lgan extiyojini, shuningdek favqulodda vaziyatlarda ham ta’minlashi lozim.

Ma’lumot uzatish xizmatini tashkil etish tamoyili bo‘yicha 2 ta guruhga bo‘linadi:

– ma’lumot uzatish xizmatlari kommutatsiyalanadigan va kommutatsiyalanmaydigan elektraloqa tarmog‘ida tashkil etilishi ma’lumot uzatishni (maxsuslashtirilgan ma’lumot tarmog‘i bazasida) ta’minlashi uchun maxsus yaratildi;

– ma’lumot uzatish xizmatlari maxsuslashtirilmagan kommutatsiyalanadigan va kommutatsiyalanmaydigan elektraloqa tarmog‘i asosida tashkil etildi.

Ma’lumot uzatish xizmatiga kirish nuqtasini aloqa operatorlari nuqta deb nomlashadi va aloqa operatorlari foydalanuvchilarga ma’lumot uzatish xizmatlarini ma’lum sifatda taqdim etadi. Kirish nuqtalari hamma operatorlarni jixozlarida joylashgan bo‘ladi. Foydalanuvchining ma’lumotni ohirgi qurilmasiga taqdim qilishiga ko‘ra uzatish qarori kirish nuqtalarida amalga oshiriladi. Boshqa operatorlar xizmati orqali foydalanuvchini ma’lumotlar ohirgi qurilmasi (MOQ) va ma’lumot kanalining ohirgi qurilmasi (MKOQ)ga bog‘lashida, ma’lumot uzatish xizmati operatorini kirish nuqtasida hech qachon bir vaqtda yuz bermaydi. Telekommunikatsiya tarmog’ida ma’lumot uzatish xizmati chegaralari MOQ va MKOQlar orqali ulanishlarda, telekommunikatsiya tarmog’ini maxsuslashmagan baza kanallari ma’lumot kanalini tuzish orqali chegaralanadi. Bu xodisa, qachonki telekommunikatsiya tarmog’iga ulanishida MOQ loyiq yoki maxsus telekommunikatsiya bo‘lmay tarmoqqa ulansa MKOQ o‘zidan-o‘zi tarmoqdan ajraladi.

Bunday ma’lumot uzatish xizmati maxsuslashmagan telekommunikatsiya

tarmog’ida xizmatlarni ko‘chirishdan hosil bo‘ladi. Abonentni texnik vosita guruhi yoki aloqa operatori yoki MKOQlar kirishda texnik vosita bo‘lib hisoblanadi.

Ma’lumot uzatish xizmatini ikki ko‘rinishi mavjud bo‘lib: bazaviy va fakultativdir. Ma’lumotning xarakatini aniqlashda ko‘proq bazaviy xizmatlardan foydalaniladi. Fakultativ xizmat operator xizmatining buyumlaridan foydalanish tushuniladi.

Bazaviy xizmat – ma’lumot uzatishni to‘g‘ridan-to‘g‘ri aniqlaydi, tarmoq orqali o‘zgarishlarni taxlil qilishda qo‘llaniladi.

Fakultativ xizmatda istalgan xizmat ma’lumot uzatish tarmog’iga beriladi, shuningdek kompyuterlarni ishlashini amalga oshirishda, tashqi uzatish protokolida, formatlashda, ma’lumotdan foydalanish mazmunini, ya’ni boshqa qo‘shimcha ma’lumotdan foydalanishni ta’minlaydi yoki ma’lumotning xavfsizligidan o‘zaro foydalanish tushuniladi.

Aksariyat hollarda fakultativ xizmat kompyuterni ishlab turishini amalga oshiradi. Bunday usul aniq chegarani, xizmat sifatini aniqlab javobgarlikni ta’minlovchi foydalanish xizmati va operatorlar orasida qo‘shimcha bitimlarni tuzadi.

Bu xizmatlar vaqt usulida taqdim qilinadi:

– agar bu xizmatga foydalanuvchi a’zo bo‘lsa, har bir so‘rov uchun avtomatik ravishda javob beradi;

– vaqt oraligida belgilangan xizmatga a’zo bo‘lishda har bir so‘rov uchun avtomatik ravishda javob beradi;

– faqat so‘rov bo‘lganda o‘z vaqtida bog‘lanish o‘rnatilganda taqdim etiladi.

Barcha turli tarmoqlarni belgilar guruhi bo‘yicha sinflash mumkin:

- terretorial tarqalganlik;
- idoraga tegishlilik;
- axborotni uzatish tezligi;
- uzatish muhiti turi.

Terretorial tarqalganlik bo‘yicha tarmoqlar lokal, global va mintaqaviy

bo‘lishi mumkin. Lokal tarmoqlar bitta bino yoki bir nechta binolarni bitta tarmoqqa birlashtirilishi, mintaqaviy tarmoqlar – shaxar va viloyat xududida joylashishi, global tarmoqlar mamlakat va mamlakatlar guruhi xududini qoplashi mumkin, masalan butun dunyo Internet global tarmog‘i.

Xudud bo‘yicha tegishlilik va hukumat tarmoqlari farqlanadi. Tegishlilik tarmoqlar birgina tashkilotga tegishli bo‘lib, shu tashkilot xududidagina joylashadi. Hukumat tarmoqlari – hukumat tuzilishlarida foydalaniladigan tarmoqlardir.

Axborot uzatish tezligi bo‘yicha tarmoqlar past, o‘rtacha va yuqori tezlikli tarmoqlarga bo‘linadi.

Uzatish muhitining turi bo‘yicha koaksial, juft simli, optik tolali, infraqizil diapazonda radiokanallar bo‘yicha tarmoqlarga bo‘linadi.

Ma’lumot uzatishning har xil shartlari orqali xizmatlarni o‘zaro bog‘lashdan asosiy maqsad quyidagilar:

- ko‘plab mamlakatlar va foydalanuvchilar xududini egallash uchun barcha ma’lumot uzatish tarmoqlaridan va xizmatlaridan foydalanish;
- har xil ma’lumot uzatish xizmatlari va har xil aloqa operatorlarining ma’lumot uzatish xizmatlari foydalanuvchilar o‘rtasida ma’lumot almashish imkoniyatini ta’minlash;
- foydalanuvchilarga ko‘rsatiladigan sifat tavsiflarini xalqaro standartlar talabiga mosligini ta’minash;
- ma’lumot uzatish xizmatlariga asoslangan kompyuter va boshqa telexizmatlarning yashovchanligini va ishonchliligini oshirish;
- hukumat organlari, jumladan favqulodda holatlar bo’lganda ma’lumot uzatish xizmatlariga bo‘lgan talabni qondirish.

Ma’lumot uzatish tarmoqlarining barcha asosiy xususiyatlarini jamlagan harakterli, funksional, informatsion va tuzilishviy belgilari bilan sinflanadi. Bunday belgilarga quyidagilar kiradi:

- tarmoq foydalanuvchilarining (abonentlarining) tegishlilik kategoriyasi;
- tashkillashtirish usullari;
- kommutatsiya usuli;

- ma’lumot uzatish kanallari turlari;
- tarmoq o‘lchami;
- tarmoqda axborot uzatish tezligi;
- tarmoq tuzilishsi;
- boshqarish usuli.

Kommutatsiya usullari bo‘yicha ma’lumot uzatish tarmoqlari quyidagilarga bo‘linadi:

Uzoq vaqtli kommutatsiya tarmoqlari. Uzoq vaqtli kommutatsiya deb shunday kommutatsiya usuliga aytiladiki, bunda tarmoqning ikki nuqtasi o‘rtasida doimiy to‘g‘ri ulanish o‘rnatiladi, ulanish soatlar, kecha-kunduz (sutka), umuman katta vaqt oralig’i bilan o‘lchanishi mumkin. Bunday ulanishlarni tashkillashtirishda qatnashadigan kanallar ajratilgan kanallar deb ataladi.

Tezkor kommutatsiyali tarmoqlar. Tezkor kommutatsiya deb kommutatsiyaning shunday usuliga aytiladiki, bunda tarmoqning ikki nuqtasi o‘rtasida vaqtinchalik ulanish o‘rnatiladi.

Kanallar kommutatsiyasiga asoslangan tarmoqlar. Kanallar kommutatsiyasi shunday kommutatsiya usuliki, unda shu tarmoqning chetki ixtiyoriy juft punktlari o‘rtasida vaqtinchalik to‘g‘ri ulanish o‘rnatiladi.

Xabarlar kommutatsiyasiga asoslangan tarmoqlar. Xabarlar kommutatsiyasi deb kommutatsiyaning shunday usuliga aytiladiki, bunda har bir kommutatsiya qurilmasida xabarlarni qabul qilish hisoblab chiqariladi, xabarlarning to‘planishi va oldinga uzatilishi qabul qiluvchining manziliga mos keladi.

Paketlar kommutatsiyasiga asoslangan tarmoqlar. Paketlar kommutatsiyasi deb kommutatsiyaning shunday usuliga aytiladiki, bunda xabarlar tarmoq orqali qabul qilinadigan, buferlanadigan va uzatiladigan aniq qismlarga – paketlarga bo‘linadi. Agar bitta xabarning barcha paketlari qayd qilingan marshrut bo‘yicha uzatilsa, u holda bunday kommutatsiya rejimi virtual deyiladi. Agar har bir paketni uzatish mustaqil marshrut bo‘yicha amalga oshirilsa, bu kommutatsiya rejimi datagramma (deytagramma) deyiladi.

Gibrid kommutatsiyali tarmoqlar. Gibrid kommutatsiya deb shunday usulga

aytiladiki, unda bitta va aynan shu kommutatsiya qurilmasida ikki yoki undan ko‘p yuqorida nomlari keltirilgan kommutatsiya ko‘rinishlaridan foydalangan holda kommutatsiya tarmog‘i ishlab chiqiladi.

Kanallar turlari bo‘yicha ma’lumot uzatishning quyidagi tarmoqlari mavjud:

- simpleks tarmoqlar – axborot faqat bitta yo‘nalish bo‘yicha uzatiladi;
- yarim dupleks tarmoqlar – axborot o‘zgaruvchan qarama-qarshi yo‘nalish bo‘yicha uzatiladi;
- dupleks tarmoqlar – axborot bir vaqtda qarama-qarshi yo‘nalishda uzatiladi.

Ma’lumot uzatish tezligi bo‘yicha ma’lumot uzatish tarmoqlari quyidagilarga bo‘linadi:

- past tezlikli – bunday tarmoqning axborot uzatish tezligi 64 kbit/s;
- o‘rtacha tezlikli – tarmoqning axborot uzatish tezligi 64 kbit/s dan 2048 kbit/s gacha;
- yuqori tezlikli – 2048 kbit/s dan yuqori.

Ma’lumot uzatish tarmog‘i tuzilishi bo‘yicha:

Ierarxik tarmoqlar. Global tarmoqlar ierarxik tuzilishga ega, unda bir necha ierarxiya pog‘onalari mavjud bo‘lib, odatda ular o‘z nomlariga ega bo‘ladi.

Ierarxik tuzilishga ega bo‘lmagan tarmoqlar. Bunday tuzilishga ega tarmoqlardan lokal tarmoqlar qurishda foydalaniladi va bitta ierarxiya pog‘onasiga ega bo‘ladi.

Quyidagilar tarmoqni boshqarish tizimi funksiyasi bo‘lib hisoblanadi: administratoriy boshqaruv, texnik ekspluatatsiya, axborot oqimini nazorat qilish va ularning optimal taqsimoti va h.k. Ma’lumot uzatish tarmog‘iga bog‘langan holda yechilishi kerak bo‘lgan masalada tarmoqqa qo‘yiladigan talablar funksiyasiga shartlar qo‘yilgan holda boshqaruv tizimi markaziy va markaziy bo‘lmagan tamoyil asosida quriladi. Tarmoqni boshqarish usuli bo‘yicha ma’lumot uzatish tarmoqlari quyidagilar:

- markaziy boshqaruvga ega tarmoqlar. Bu tamoyilda hamma uchun yagona markaziy boshqaruv tizimi mavjud deb faraz qilinadi;

- markaziy boshqaruvga ega bo‘lmagan tarmoqlar. Bunday tarmoqlarda boshqaruv tizimi tarqoq tuzilishga ega va ma’lumot uzatish tarmog‘ining barcha pog‘onalari bo‘yicha tarqalgan shunday markazlarni o‘z ichiga oladi;

- aralash boshqaruvga ega bo‘lgan tarmoqlar. Aralash boshqaruvda ma’lum chegarada markaziy va markaziy bo‘lmagan boshqruv tamoyillari qo‘llaniladi.

1.3. Ochiq tizimlarning o‘zaro bog‘lanish etalon modeli

“Ochiq tizimlarning o‘zaro bog‘lanishi” atamasi tizimlar orasidagi ma’lumot uzatish jarayonlariga tegishlidir, ya’ni hamkorlikda foydalaniladigan standartlarni ishlatish tufayli, bir – birlari uchun tizimlar ochiqdir.

Bir qator funksiyalarni bajarib, u yoki bu pog‘ona tarkibiga kiruvchi ochiq tizimning bir qismi **ob’ekt** deb ataladi.

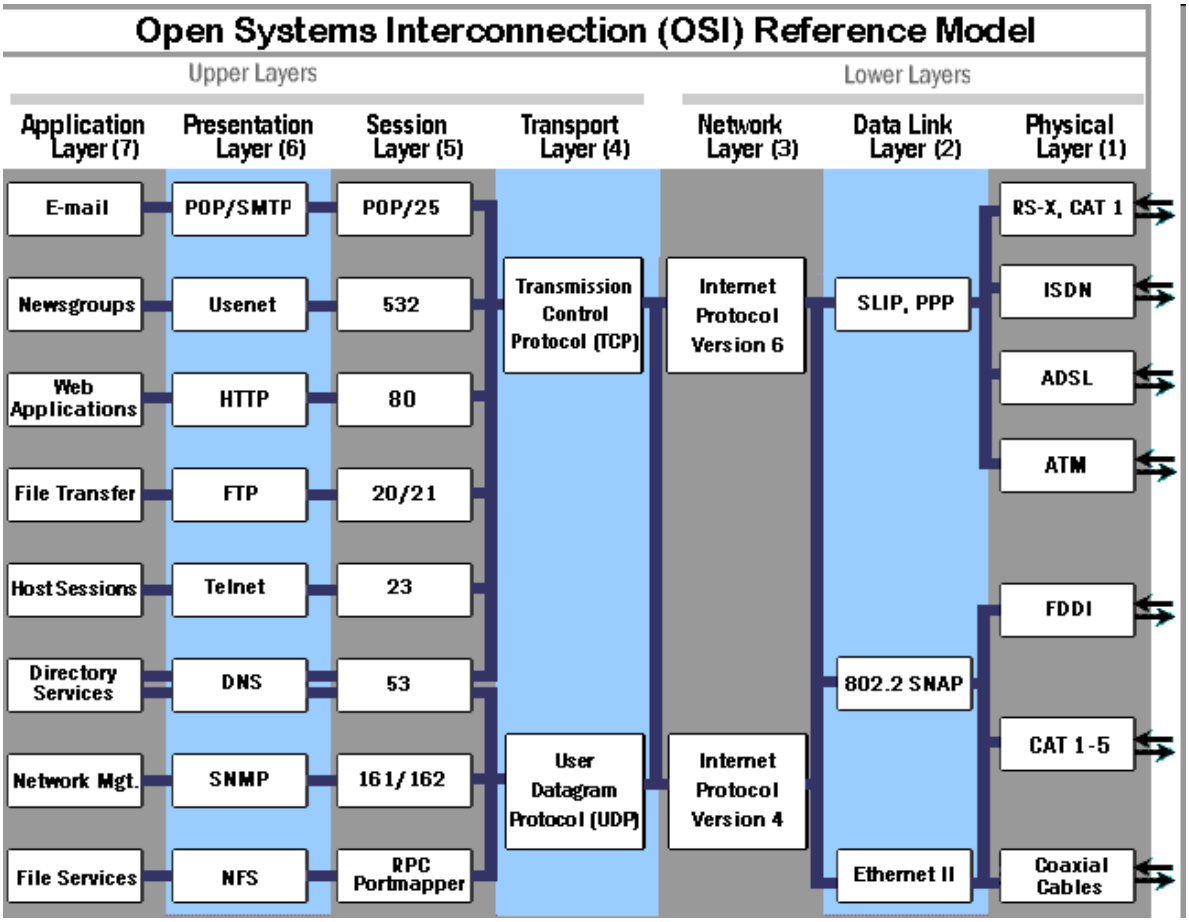
Xalqaro standartlashtirish tashkiloti (ISO) jahonning ko‘p mamlakatlarida axborot tarmog‘i va kompyuter tizimlarini tashkil qilish tajribasini taxlil qilib, hisoblash tarmoqlarini tashkil qilish konsepsiyasini ishlab chiqdi va uni ***ochiq tizimlar arxitekturasi*** deb nomladi.

Bu konsepsiyaga muvofiq *ochiq tizimlarning o‘zaro bog‘lanish etalon modeli* (Open System Interconnection basic reference model,OSI RM) ishlab chiqildi va 1**983** yilda tasdiqlandi (1.5-rasm).

Mazkur model bunday tizim va tarmoqlarni ishlab chiqishni aniqlovchi va tartibga soluvchi halqaro standartlarni kiritishga imkoniyat beradi.

Model xalqaro standartlar tashkiloti (ISO-International Standard Organization) tomonidan ishlab chiqilgan bo‘lib, butun dunyoda axborot tarmoqlari konsepsiyasining asosi sifatida foydalaniladi.

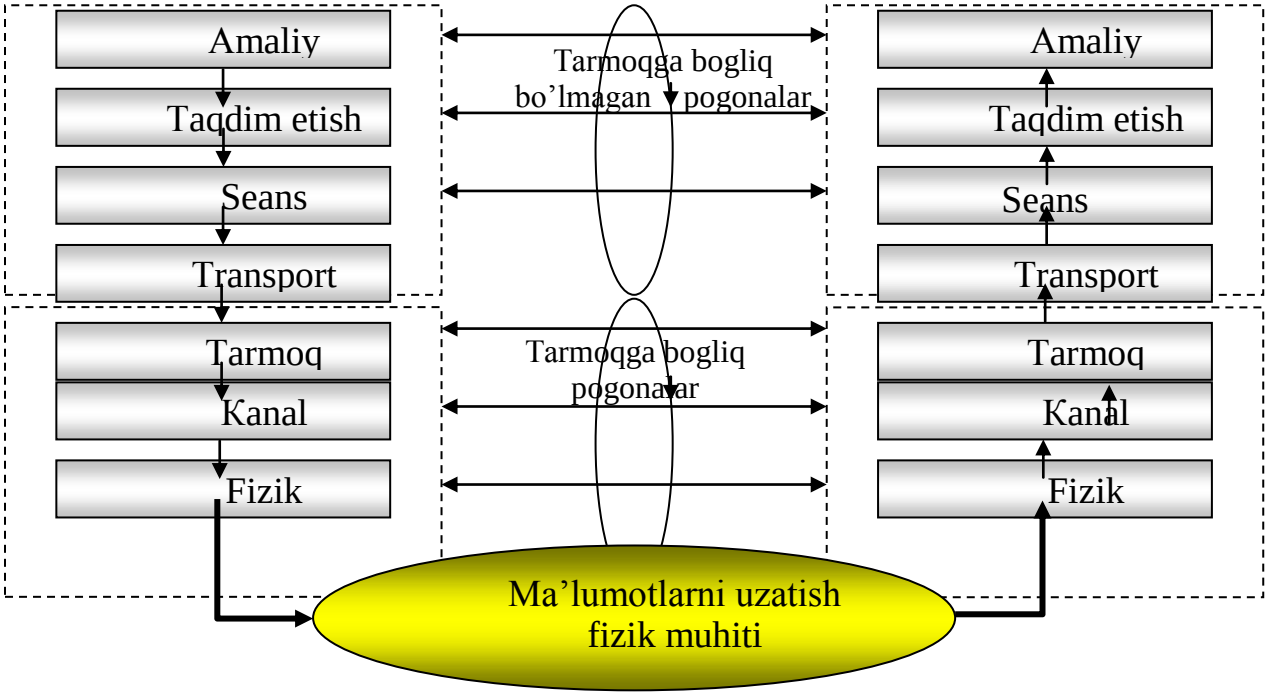
Ochiq tizimlarning tavsiflari va vositalarini aniqlaydigan konseptual asos sifatida OSI etalon modeli ishlatiladi. U ochiq tizimlarning turli ishlab chiqaruvchilar tomonidan tavsiya etilgan tizimlarning bir tarmoqda ishlashini ta’minlovchi o‘zaro bog‘lanishini aniqlaydi va quyidagilarni muvofiqlashtiradi:



1.5 – rasm. OSI- da ishlatiladigan protokollar modeli

- qo‘llanish jarayonlarining o‘zaro bog‘lanishini;
- ma’lumotlarni taqdim etish shakllarini;
- ma’lumotlar saqlanishi bir xilligini;
- tarmoq resurslarini boshqarishni;
- ma’lumotlar xavfsizligi va axborot himoyasini;
- dasturlar va texnik vositalarning diagnostikasini.

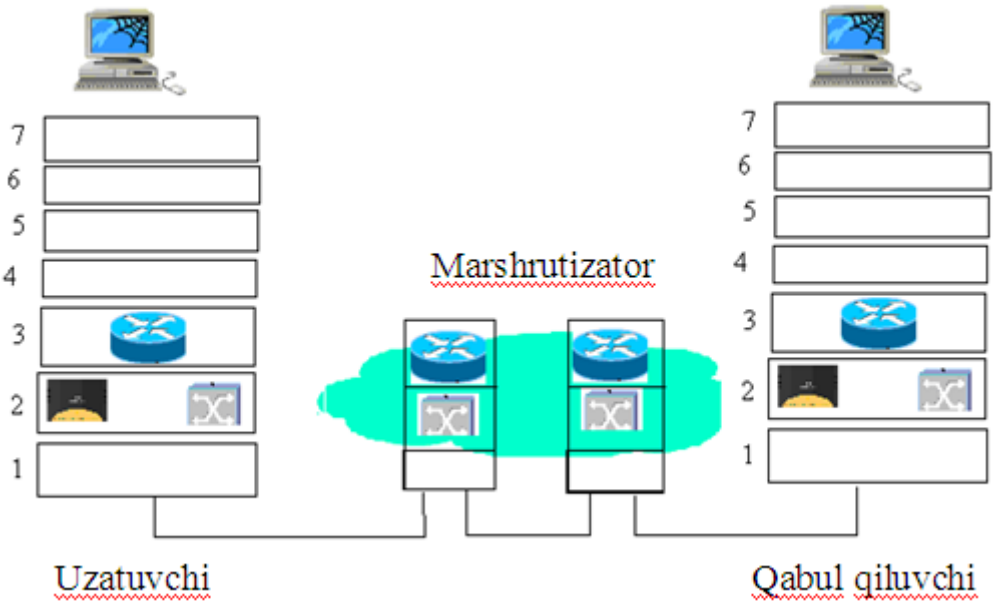
1.6 - rasmda tarmoqning har xil elementlari ishlaydigan pog‘onalari ko‘rsatilgan. Kompyuter va unga o‘rnatilgan operatsion tizim boshqa kompyuter bilan barcha yettita pog‘ona protokollari yordamida o‘zaro aloqa qiladi. Bu aloqalarda har xil kommutatsiya qurilmalari muhim ahamiyat kasb etadi: konsentratorlar, modellar, ko‘priklar, kommutatorlar, marshrutizatorlar, multipleksorlar.



1.6 - rasm. OSI modelining pog‘onalari

Kommunikatsiya qurilmasi uning turiga bog‘liq ravishda fizik, yoki fizik va kanalli, kanalli va tarmoqli pog‘onada ishlashi mumkin, ba’zida transportli pog‘ona (marshrutlovchi) ham qo‘shiladi.

1.7 - rasmda har xil kommunikatsion funksiyalar mosligi ko‘rsatilgan.



1.7 - rasm. Har xil tarmoq qurilmalarini pog’onalarda ishlashi

OSI modeli amalda keng qo‘llanilishi va ahamiyatli bo‘lishiga qaramasdan, ko‘plab kommutatsiya modellaridan biridir. Bu modellar va ularga bog‘liq bo‘lgan protokollar pog‘onalar soni, funksiyalari, xabarlar formati, xizmatlari va boshqa ko’rsatkichlari bilan bir-biridan farq qilishi mumkin.

Ochiq tizimlarning standart xolatdagi o‘zaro bog‘lanishi quyidagicha:

- o‘zaro ochiq tizimning etalon modeli;
- etalon modelini qanoatlantiradigan xizmatlarning aniq to‘plami;
- xizmatlar bajarilishini ta’minlovchi va ularni amalga oshirish uchun ishlab chiqilgan protokollar to‘plami.

Nazorat savollari

1. Ma’lumot uzatish tarmoqlariga tushuncha bering?
2. Ma’lumot uzatish tarmoqlarida protokollarning vazifalari qanday?
3. Protokollarga taalluqli 3 ta asosiy jihat nimalardan iborat, tushuncha bering?
4. Protokollarni qo‘llanish joylarini tushuntiring?

2. MA’LUMOT UZATISH TARMOQLARIDA PAKETLI KOMMUTATSIYA VA KANAL POG‘ONASI PROTOKOLLARI

2.1. Paketli kommutatsiya mexanizmlari va tamoyillari

1960 yillarda paketli kommutatsiya texnologiyasini olimlar britaniyalik Donald Devis va amerikalik Pol Beranlar yaratgan.

60 yillarning birinchi yarmida Devis «paket» terminini kiritdi va yangi kommutatsiya tamoyili asosida kichik tarmoqni qurdi. Beran paketli kommutatsiyaning konsepsiyasini, arxitekturasini buzilishlarga va hujumlarga chidamlilik tomonlarini yaratdi. Keyingi yillarda o‘zining konsepsiyasini bir necha

Devis Alan Tyuring rahbarligida milliy fizika laboratoriyasining a’zosi edi (National Physical Laboratory). Bu laboratoriyada ACE Pilot kompyuteri yaratilgan. British Computer Society Award unvoni bilan taqdirlangan.

Donald Devis

Pol Beran (Paul Baran)

Internetni rivojlanishiga katta xissa qo‘shgan. Paketlar kommutatsiyasi usulini yaratgan. Aleksandr Grem Bell nomidagi oltin medal, texnologiya va innovatsiya sohasida milliy medal bilan taqdirlangan.

2008 yilda Beran texnologiyaning rivojlanishiga qo‘shgan xissasi uchun

AQSH ning medali bilan taqdirlangan.

2.1 - rasm. Mashhur kompaniya rahbarlari

Mashhur 4 ta asosiy boshqaruvchi tarmoq kompaniyalari. Ularning yillik daromadi, qaysidir davlatning budjetidan ko‘p: Cisco Systems (Djon Chambers), Lucent Technologies (Richard Makgin), Nortel Networks (Djon Rot), 3Com (Erik Benamu). 2000 yilda ular yaqin 10 yillikda ularning kompaniyalarining o‘rni to‘g‘risida taxmin qilishadi.

1994 yilda Djon Chambers Cisco Systemsga rahbar bo‘ldi. Cisco Systemsning omadi ko‘p narsalarga bog‘liq bo‘ldi, rahbariyatning ixtiyori, Cisco Systemsni bozorda qanday qabul qilishi, butun jahon qanchalik tez IP protokolga o’tishiga bog’liq bo’ldi.

Cisco Systemsni afzalligi shundaki, butun jahon IP-paket texnologiyasini qo‘llab qo‘vvatlaydi. Bu yerda Cisco nafaqat texnologiyalarni ishlab chiqaradi, balki ularni qo‘llashda boshqarishniyam ko‘zda tutadi. Djon Chambers ishonardiki, o‘zining katta kompaniyasi kichik firmalarni ham o‘z ichiga oladi.

Djon Chambers Cisco Systems ni boshqa hozirgi va o‘tgan gigant tashkilotlar bilan solishtiradi va uni birinchi o‘ringa qo‘yadi.

Djon Chambersni tashabbuskorligi tufayli hammani IP asriga qaratishga, uni eshitishga e’tiborini qaratar edi.

Djon Chambers 2001 yilda butun jahon IP ga o‘tadi deb bashorat qildi. IP tarqalishini chegaralovchi faktorlardan biri, bu QoS - xizmat ko‘rsatish sifatini

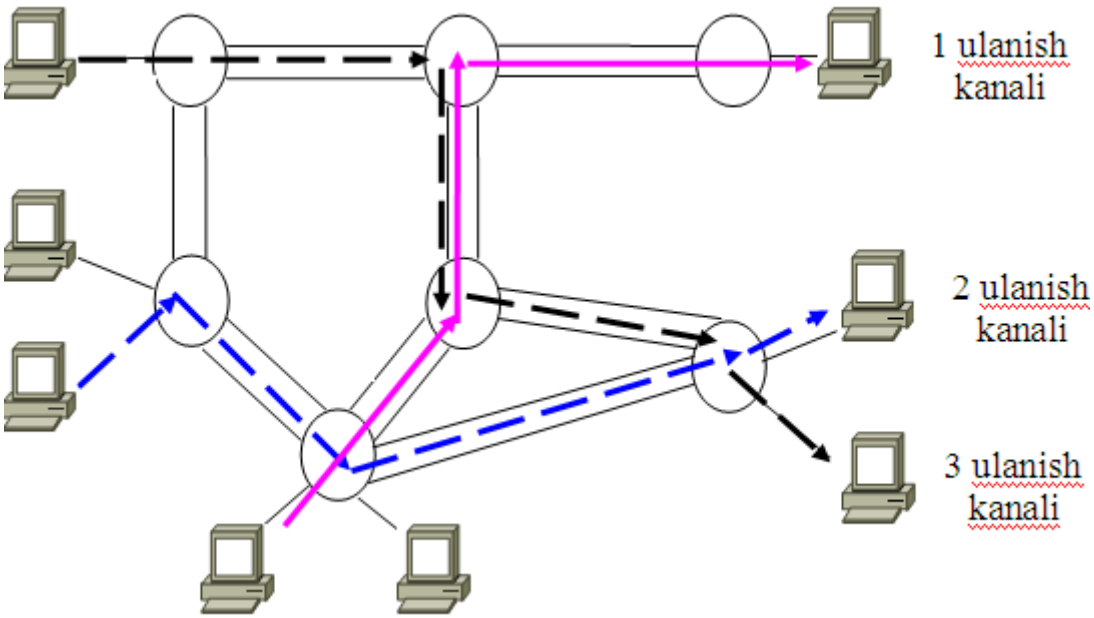
ta’minlash mexanizmini kamchiligi hisoblanadi.

Tarmoqlarda ikki foydalanuvchi bir-biri bilan bog‘lanish jarayonida quyidagi asosiy kommutatsiya usullari orqali amalga oshiriladi (2.1-rasm):

- kanallar kommutatsiyasi;
- haketlar kommutatsiyasi;
- xabarlar kommutatsiyasi.

Signalni uzatish uchun uzatuvchi va qabul qiluvchi o‘rtasida aloqa kanalini o‘rnatish lozim. Bu kanal ikki tomon o‘rtasida butun aloqa seansi davomida fizik bog‘lanish bo‘lib hisoblanadi. Ushbu xolatda biz *kanallar kommutatsiyasi* bilan aloqa o‘rnatgan hisoblanamiz.

Kanallar kommutatsiyasi bir nechta alohida kanallar uchastkasining bog‘lanishidan hosil bo‘lib, ma’lumotlarni qurilmalar orasida to‘g‘ri uzatish uchun hosil qilingan fizik kanal tushuniladi.



2.2 – rasm. Kanallar kommutatsiyasini tuzilishi

Kanallar kommutatsiyasida aloqa seansi quyidagi fazalarga bo‘linadi:

- fazalarni tayyorlash, kanallarni hosil qilish va qo‘llab quvvatlashda tarmoq resurslarini zahiralash;

- o‘rtacha faza, uzatuvchi signallarni ishlab chiqish;

- fazalarni yakunlash, ishlatilib bo‘lingan resurslarni bo‘shatish va uzatishni yakunlash.

Paketlar kommutatsiyasida paket uchta qismdan, ya’ni **sarlovha**, **ma’lumot** va **treyler** qismlarini shakllantiradi.

Sarlovha qismi paketning uzatilish signali, manba manzili, makon manzili, uzatishni sinxronlash kabilarni o‘z ichiga oladi.

Ma’lumot qismi xabar tarkibidagi uzatishga mo‘ljallangan ma’lumotlardan iborat. Tarmoq turiga nisbatan bu qism 0,5— 4 Kb bo‘lishi mumkin.

Treyler qismi ko‘p hollarda xatoliklarni tekshirishga mo‘ljallangan (misol uchun, siklik kod yordamida tekshiruv). Paket shakllanishi OSI modelining amaliy pog‘onasida boshlanadi. Uzatish mo‘ljallangan axborot yuqori (amaliy pog‘onasi)dan quyi pog‘onaga yetkaziladi va har bir pog‘ona ma’lumot qismiga tegishli axborotni qo‘shadi.

Paketlar kommutatsiyasida foydalanuvchilararo uzatilayotgan xabarlar kichik qismlarga — paketlarga bo‘linadi. Ma’lumot uzatish tarmoqlarida paket asosiy uzatish birligi hisoblanadi.

Katta hajmdagi xabarlar kichik paketlarga bo‘linishi tarmoqda ma’lumot uzatish tezligining keskin oshishiga olib keladi.

Xabarlar turli uzunlikga ega bo‘lishi mumkin — bir necha baytdan o‘nlab megabaytgacha, paketlar esa o‘zgaruvchan uzunlikka ega bo‘lishlari mumkin.

Har bir paket kerakli qurilmaga yetib borishi uchun manzil axboroti belgilangan sarlovha qismi bilan boshlanadi. Paket turli qismlardan iborat bo‘lishi mumkin va quyidagilarni o‘z tarkibiga olishi shart:

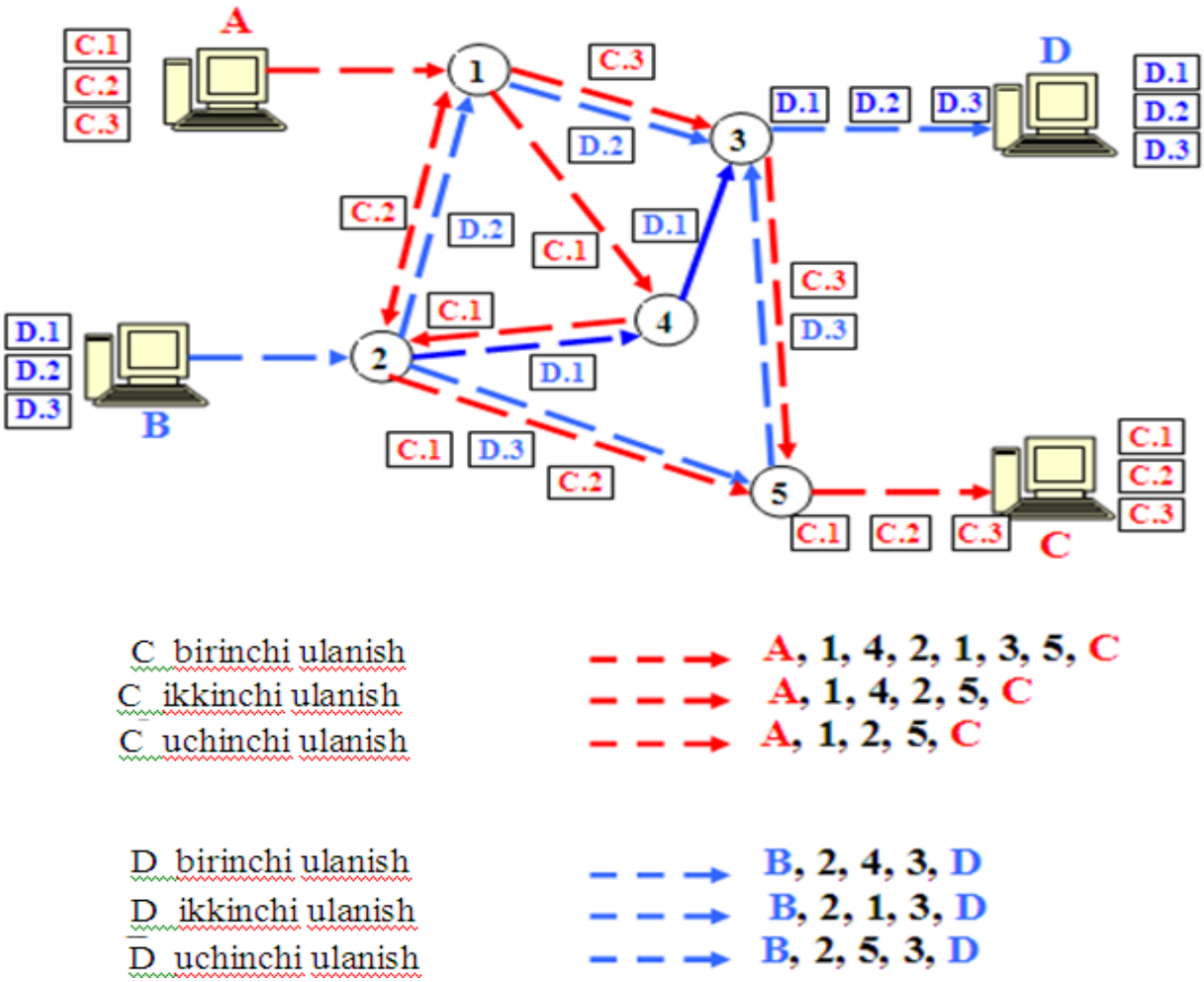
- uzatuvchini ifodalaydigan manba manzili;
- uzatilayotgan ma’lumotlar;
- qabul qiluvchining manzili;
- tarmoq vositalariga ma’lumot uzatilishi lozim bo‘lgan marshrut axboroti;
- xabarni dastlabki ko‘rinishda taqdim etuvchi axborot;
- uzatish aniqligini ta’minlovchi xatoliklarni tekshirish axboroti.

Paketlar kommutatsiyasida uzatilayotgan axborot bir nechta maxsus porsiya-

paketlarga bo‘linadi va bir - biriga bog‘liq bo‘lmagan holda uzatiladi. Shuning uchun paketlar uzatuvchidan qabul qiluvchiga yetib borishida bir necha yo‘llardan uzatilishi mumkin.

Kanallar kommutatsiyasidan farqi “saqla va uzat” uslubi bilan ishlaydi. Ma’lumotlarni uzatishni davom ettirishdan avval uzatilgan paketlarni saqlab oladi. Bu usulda paketlarni uzatish bir qator yutuqlarga olib keladi, tarmoq resurslaridan oqilona foydalanish, paketlarni kechikmasligi (aloqa seansini o‘rnatish bilan bog‘liq), biroq paketlarni tarmoq taklif etayotgan turli yo‘llar orqali marshrutlash uchun ma’lum vaqt talab qilinadi.

Paketlar kommutatsiyasida uzatish vaqtida resurslardan faydalanish uchun raqobat vujudga keladi. O‘z navbatida bu tirbandlikni hosil qiladi. Bunday vaqtda paketlar tarmoqda uzatilishi uchun o‘z navbatini kutadi (2.3 – rasm).



2.3 – rasm. Paketlarni tarmoqda har xil yo‘llar orqali uzatilishi

Paketlar tarmoq orqali mustaqil axborot bloklari sifatida uzatiladi. Paketli kommutatsiya asosidagi tarmoqda kommutatorlar ichki bufer xotirasiga ega bo‘lib, unda paketlar vaqtincha saqlanadi. Kommutatorning chiqish porti band bo‘lganda, paket biror vaqt navbat kutadi va keyingi kommutatorga uzatiladi.

Paketli kommutatsiyaning afzalliklari:

- pulsatsiyali trafikni uzatishda tarmoqning o‘tkazish qobiliyatini oshirish imkoniyatini beradi;
- foydalanuvchilararo trafik xolatini inobatga olgan holda, tarmoq sharoitiga nisbatan fizik kanallarning o‘tkazish qobiliyatini taqsimlash imkoniyatini beradi.

Paketli kommutatsiyaning kamchiliklari:

- kommutatorlarning buferlaridagi xalaqit tarmoq xolatiga bog‘liq bo‘lganligi sababli foydalanuvchilararo uzatish tezligining noaniqligi;
- ma’lumot paketlarining o‘zgaruvchanligi;
- buferlarda navbatlar ortib ketganligi sababli ma’lumotlar (paketlar)ni yo‘qolishi.

Bu kamchiliklarni bartaraf etish maqsadida turli usullar qo‘llaniladi (Quality of Service (QoS) kabi). Bunday usullar qo‘llanilishi sababli paketlar kommutatsiyasi hozirgi kunda yuqori tezlikli tarmoqlarni tashkil etishda eng samarali deb tan olingan.

Paketli kommutatsiya tarmoqlari ikki xil ishlash tartibiga ega: *virtual kanallar tartibi* (ulanish orqali aloqa) va *deytagrammali tartib* (ulanishsiz aloqa).

Paketli kommutatsiya kommutatorining kanallar kommutatsiyasi kommutatoridan farqi kommutatorning chiqish porti paket qabul qilingan vaqtda boshqa paketni uzatish bilan band bo‘lganda paketlarni vaqtinchalik saqlab turish uchun ichki bufer xotirasiga egaligidir.

Ma’lumotlarni uzatishning bunday sxemasi magistral aloqada kommutatorlar orasida trafik pulsatsiyasini kamaytirishga va shu orqali ularni tarmoq o‘tkazish qobiliyatidan yanada samaraliroq foydalanishga imkon beradi.

Tarmoqda birlik vaqt mobaynida paketlar kommutatsiyasi usulini qo‘llab

uzatiladigan kompyuter ma’lumotlarining umumiy hajmi kanallar kommutatsiyasini qo‘llab uzatiladigan ma’lumotlar hajmiga nisbatan ko‘proq bo‘ladi. Buning sababi, katta sonlar qonuniga ko‘ra alohida abonentlar pulsatsiyasi vaqt bo‘yicha shunday taqsimlanadiki, ularning maksimal qiymatlari bir-biriga mos kelmaydi, shuning uchun kommutatorlar, agar xizmat ko‘rsatilayotgan abonentlar soni haqiqatdan ham ko‘p bo‘lsa, doimiy va yetarli pog‘onada bir maromda yuklangan bo‘ladi.

Uzatish manbasidagi to‘xtalishlar:

- sarlovhalarni uzatishga ketadigan vaqt;
- har bir keyingi paketni uzatish jarayonida hosil bo‘ladigan intervallar natijasida yuzaga keladigan to‘xtalishlar.

Har bir kommutatordagi to‘xtalishlar:

- paket buferlanishi vaqti;
- quyidagilar orqali hosil bo‘ladigan kommutatsiya vaqti:

a) paketning navbatda kutadigan vaqti (o‘zgaruvchan qiymat);

b) paketning chiqish portiga ko‘chish vaqti.

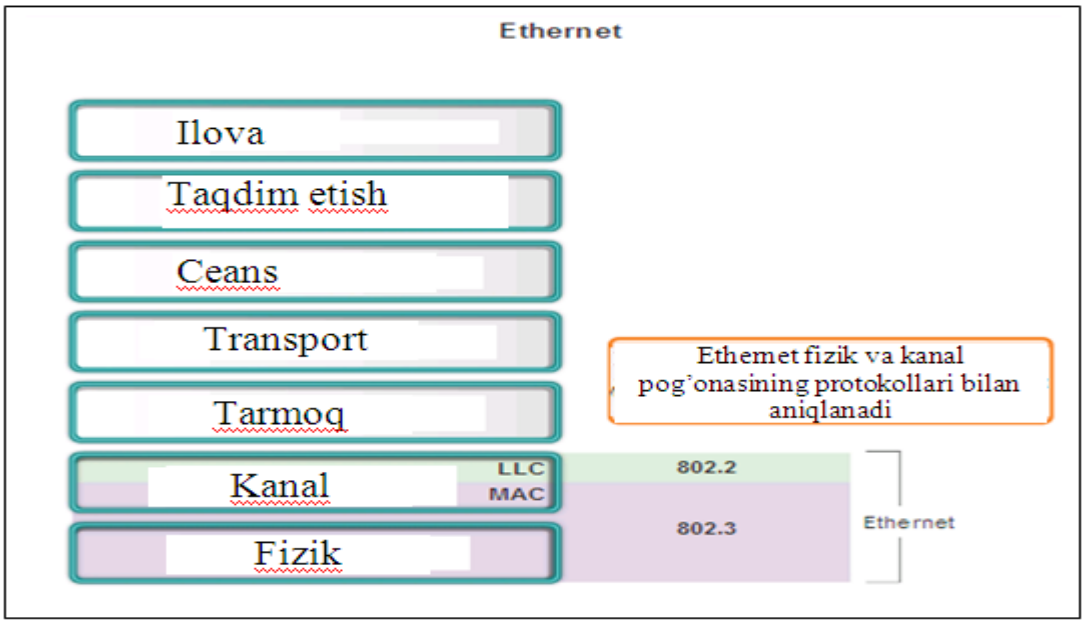
Paketlar kommutatsiyasi amalga oshiriladigan tarmoq ikki abonent o‘rtasidagi o‘zaro aloqa jarayonini sekinlashtiradi, lekin tarmoq o‘tkazish qobiliyatini oshiradi.

2.2. Kanal pog‘onasi protokollari (Ethernet, virtual lokal tarmoq)

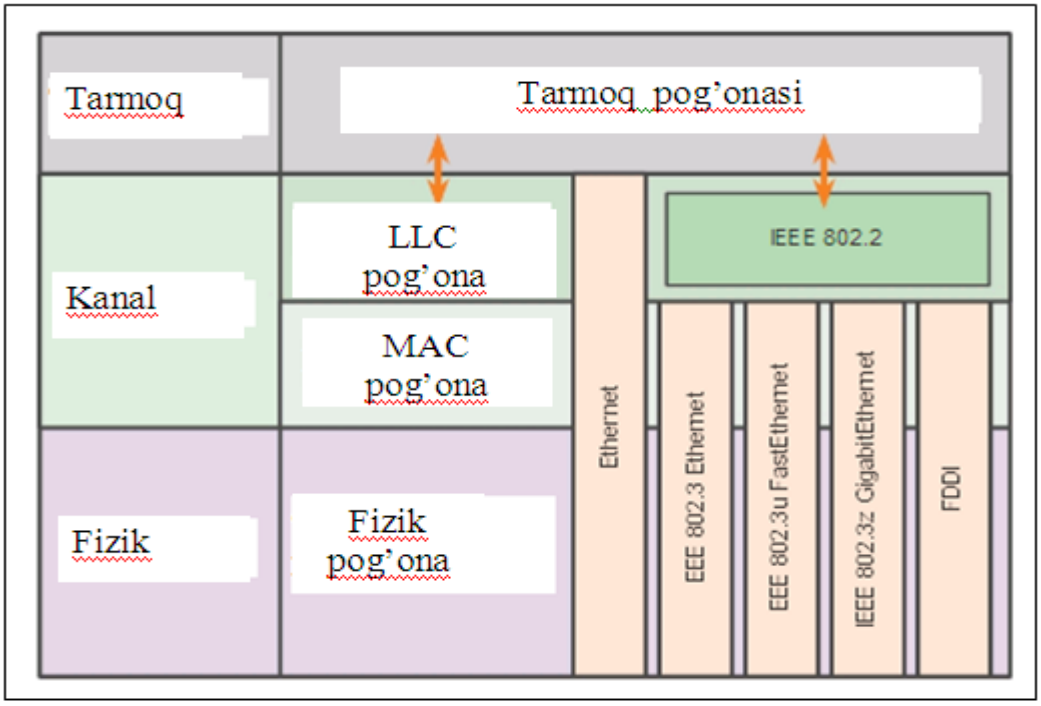
Tarmoqni samaradorligini oshirish va xavfsizligini ta’minlashda lokal tarmoqlarda VLAN lar tashkil etiladi. VLAN tarmog‘i lokal tarmoqda qurilmalarni guruhlaydi. VLAN tarmog‘i doirasidagi qurilmalar guruhi xuddi qurilmalar bitta o‘tkazgich yordamida ulangandek bo‘ladi. VLAN tarmog‘i fizik emas, mantiqiy bog‘lanishga asoslangan.

VLAN tarmog‘i administratorga foydalanuvchilarni yoki qurilmalarni qaerda joylashganligiga bog‘liq bo‘lmagan holda qo‘llanilish sohasi yoki loyihalash guruhi funksiyasi bo‘yicha segmentatsiyani amalga oshirishga yordam beradi.

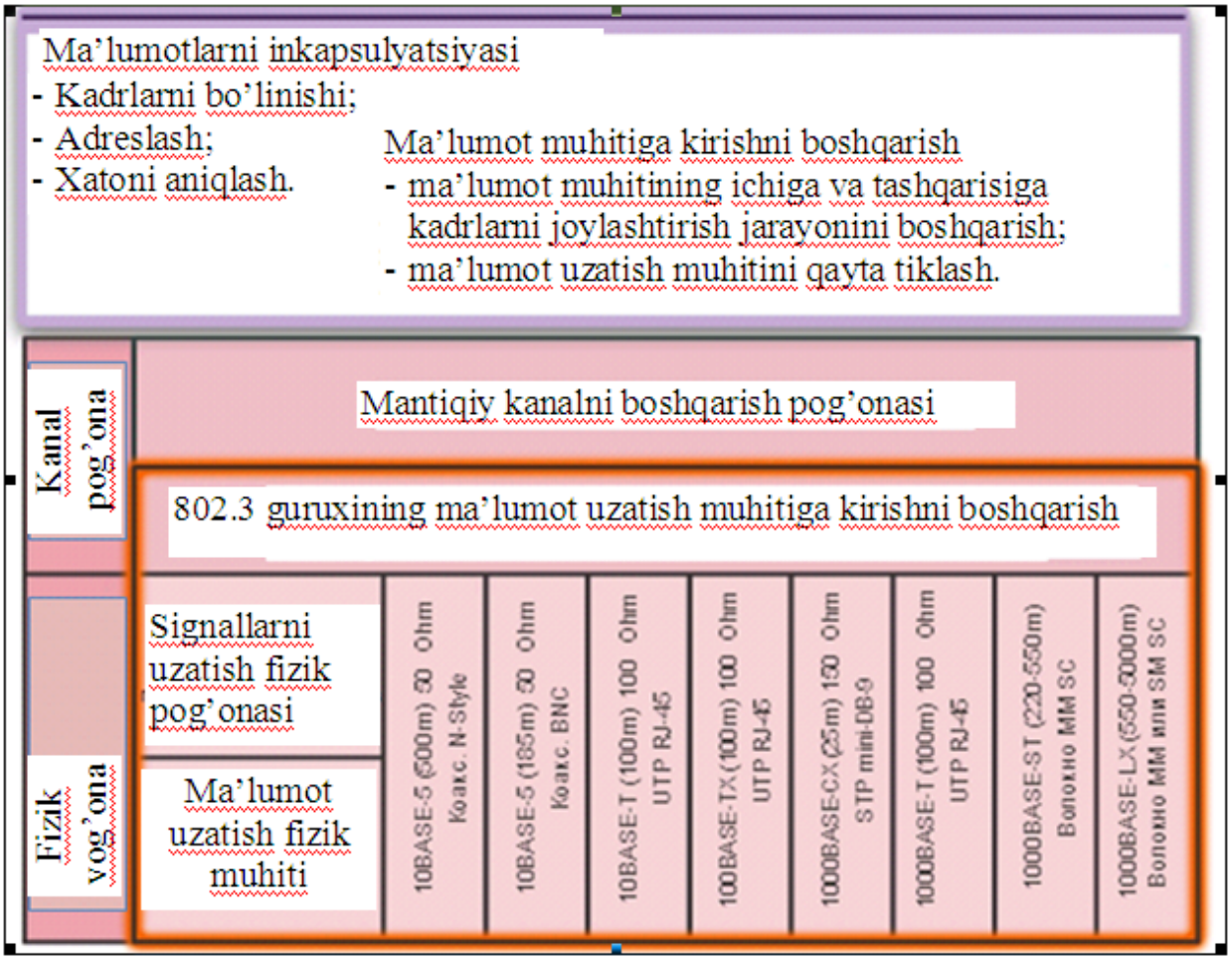
VLAN dagi qurilma xuddi o‘zining shaxsiy tarmog‘iga ega bo‘lgandek bo‘ladi. Kommutatorning ixtiyoriy porti VLAN ga tegishli bo‘lishi mumkin. Bir manzilli (unicast), ko‘p manzilli (multicast) va keng eshittirishli (broadcast) paketlarni uzatish va qabul qilish faqat o‘sha VLAN doirasida bo‘ladi. Har bir VLAN alohida mantiqiy tarmoq hisoblanadi. VLAN ga tegishli bo‘lmagan stansiyalar paketlarni jo‘natish uchun marshrutizatorlar orqali uzatiladi (2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11-rasmlar).



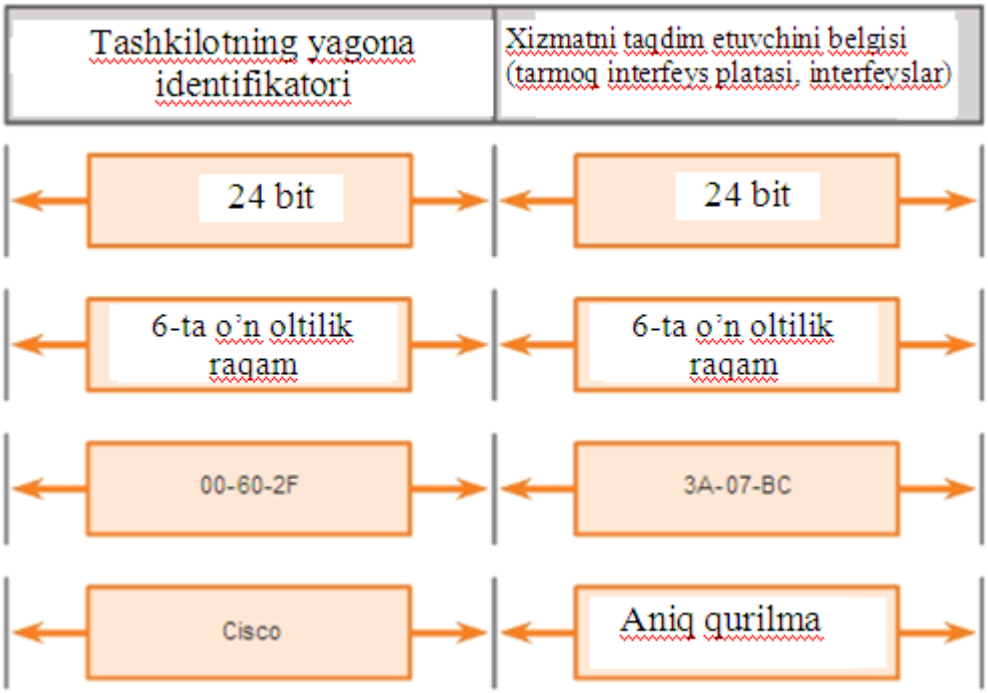
2.4 – rasm. Ethernet kadrining kanal pog‘onasida joylashganligi



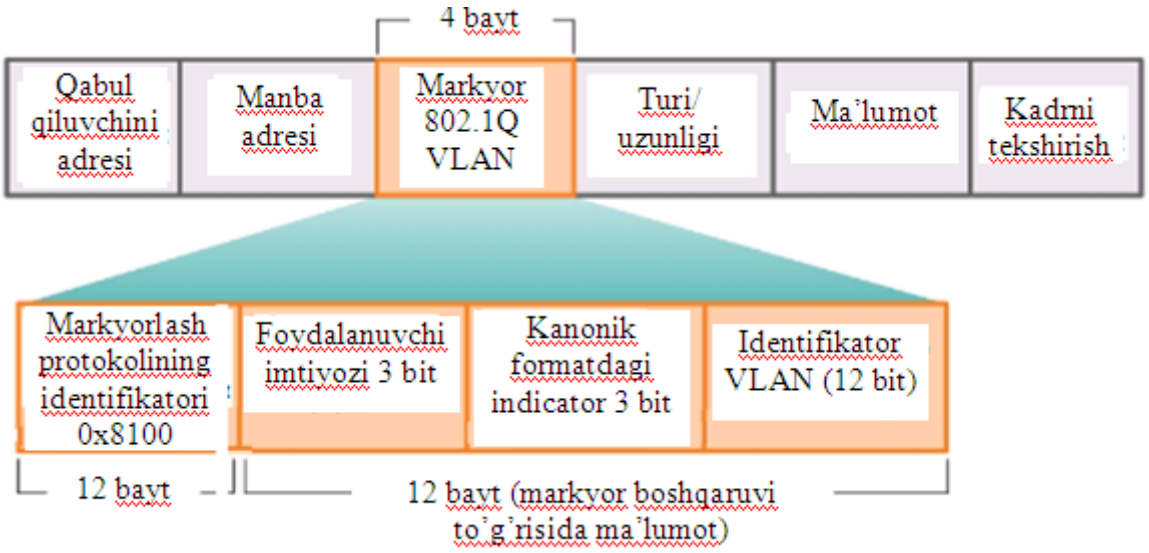
2.5 – rasm. Kanal pog‘onasining qismlarga bo‘linishi



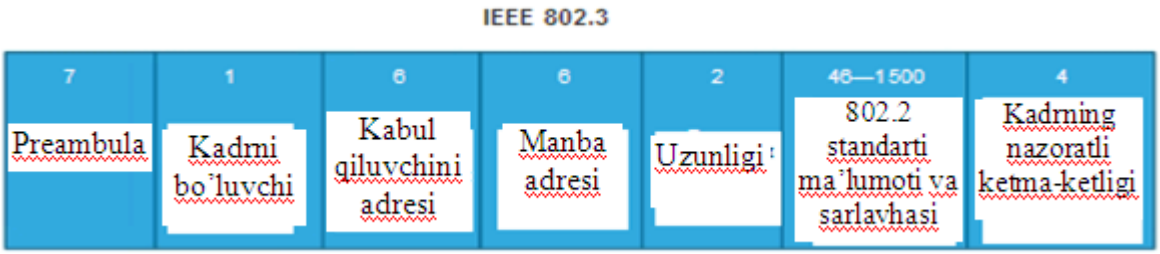
2.6 – rasm. Kanal pog‘onasining vazifasi



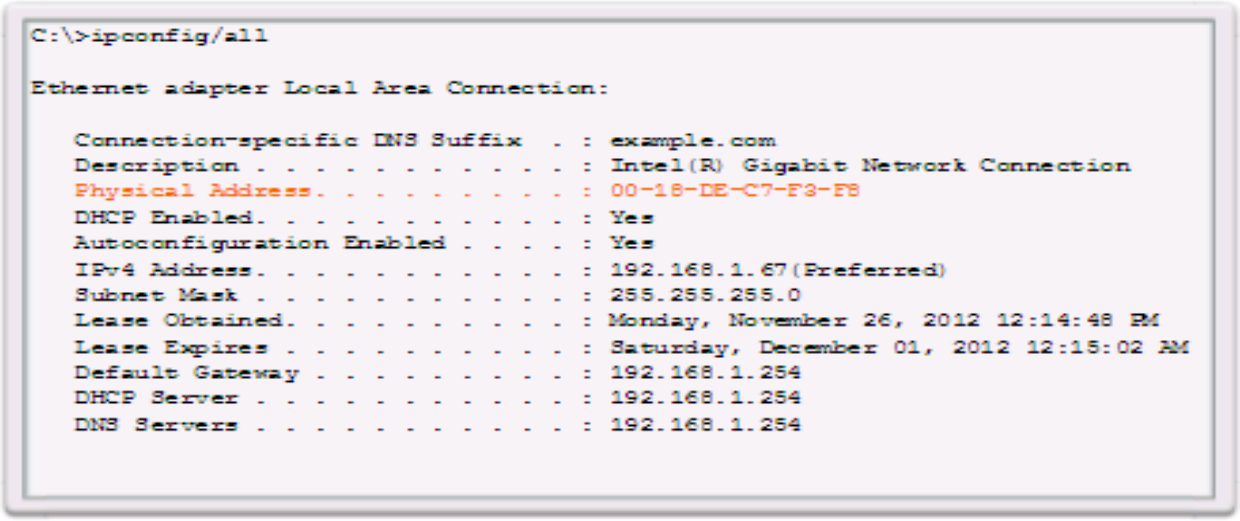
2.7 – rasm. MAC manzilini tuzilishi



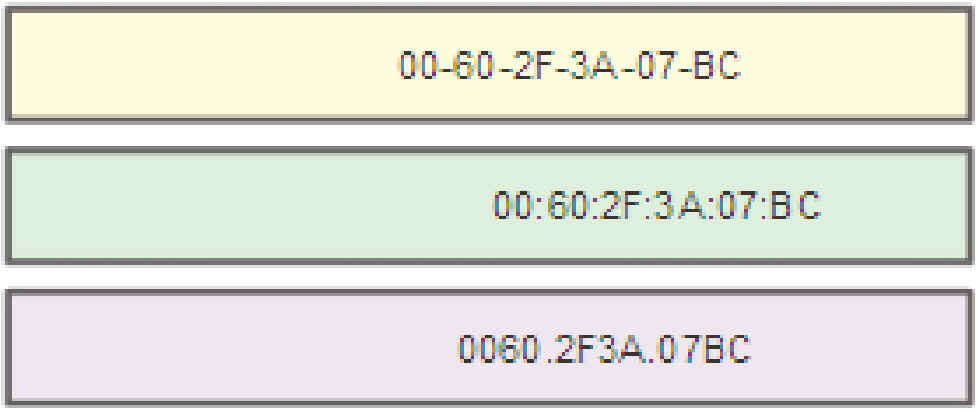
2.8 – rasm. VLAN maydonini tuzilishi



2.9 – rasm. Ethernet kadrining maydoni



2.10 – rasm. MAC manzilini ko‘rinishi



2.11 – rasm. MAC manzilini yozilishi

Qo‘shimcha 4 bayt QoS va VLAN texnologiyalarini qo‘llash imkoniyatini beradi

VLAN tarmog‘i LANning bir nechta segmentlarini qamrab oluvchi mantiqiy keng eshittirishli domenni yaratadi. Katta keng eshittirishli domenni kichik tarmoqlarga bo‘lish mumkin. VLAN tarmoqning samaradorligini oshiradi. Bitta VLAN tarmog‘idagi qurilma keng eshittirishli kadr uzatsa, bu kadrni ushbu VLAN doirasidagi qurilmalarning barchasi qabul qiladi. Boshqa VLAN dagi qurilmalar bu kadrni qabul qilmaydi.

Har xil foydalanuvchi guruhlarning qiziqishlarini hisobga olgan holda VLAN tarmog‘i kirish va xavfsizlikni ta’minlash siyosatini amalga oshiradi.

Xavfsizlik: muhim ma’lumotlarga ega bo‘lgan guruhlarni tarmoqning boshqa qismlaridan ajratiladi. Uning yordamida axborot mahfiyligini buzilish extimolligini kamaytiradi;

Xarajatlarni kamaytirish: o‘tkazish qobiliyatidan samarali foydalanish va qimmat tarmoq infratuzilishlari yangilanishini arzonligi;

Samaradorlikni oshirish: tarmoqni ikkinchi pog‘onada bir nechta mantiqiy guruhlarga bo‘lish (keng eshittirishli domen) ortiqcha tarmoq trafigini sonini kamaytiradi va samaradorlikni oshiradi;

Keng eshittirishli domenlarni kamaytiradi: tarmoqni VLANlarga ajratish keng eshittirishli domendagi qurilmalar sonini kamaytiradi.

Axborot texnologiyalari bo‘limining samaradorligini oshirish: VLAN

tarmog‘i tarmoqni boshqarishni soddalashtiradi. Yangi kommutatorni ekspluatatsiyaga kiritishda ko‘rsatilgan portlarda kerakli qoida va jarayonlarni amalga oshiradi. Axborot texnologiyalari mutaxassislari VLAN ga tegishli nom bilan tarmoq funksiyasini tezda aniqlashadi.

Ilova va loyihalarni boshqarishni soddaligi: VLAN tarmog‘i foydalanuvchilar va tarmoq qurilmalarining tarmoqni geografik talabi yoki ishlashi bo‘yicha moslashtirishi uchun birlashtiradi. Amaliy pog‘onada ishlashni va loyihalashni boshqarish funksiyalarini ajratilganligi hisobiga sodda tuzilgan. Masalan, bunday amaliy topshiriqqa – o‘qituvchilarni elektron ta’lim olish uchun ilovalarni ishlab chiqish platformasi kiradi.

Har bir VLAN tarmoq qaysidir IP tarmoqqa tegishli bo‘ladi. VLAN ni loyihalashda tarmoq manzillashining ierarxik tizimini amalga oshirishni inobatga olish lozim. Ierarxik manzillash deganda tarmoqni to‘liq ishlashida VLAN tarmog‘i yoki IP tarmoqning segmentlarini tartibli berilgan raqamlanishi tushuniladi.

Zamonaviy kommutatsiyalanadigan tarmoqda har xil turdagi hujumlar mavjud. VLAN arxitekturasi tarmoqqa xizmat ko‘rsatishni osonlashtiradi, ammo yomon niyatli odamlarga hujum qilish uchun imkoniyat beradi. Qanday har xil turdagi hujumlarning xarakatlanishini va hujumlarni xavfini kamaytirish usullarini tushunish kerak.

VLAN hopping hujumi begona VLAN hujum qilinayotgan VLAN trafigini ko‘rishga yordam beradi. Kommutator spufinggi – VLAN tarmog‘ining hujum turi bo‘lib, bunda noto‘g‘ri o‘rnatilgan trank porti ishlatiladi. Avtomatik xolatda trank portlar barcha VLAN tarmoqlariga kirishi mumkin va qoidaga ko‘ra kommutatorlar o‘rtasida, ya’ni fizik kanal orqali bir nechta VLAN lar uchun trafikni uzatadi.

2.3. Kanal pog‘onasi protokollari (Frame Relay, ATM)

Frame Relay texnologiyasi

O‘zining taqibchisi bo‘lgan X.25 bilan solishtirilganda Frame Relay (FR) ishlab chiqarish bo‘yicha samaraliroqdir. X.25 texnologiyasini yaratish va global tarmoqqa kirish kamroq ishonchli bo‘lgan analog texnologiyaga asoslangandi. Shuning uchun paketlar qabul qiluvchiga xatosiz va to‘liq etib borishi uchun X.25 texnologiyasi yuboruvchi bilan qabul qiluvchi orasidagi qurilmadan paket butunligi va ushlangan xatoni to‘g‘rilash to‘g‘risidagi xabarni tasdiqlanishini so‘raydi. Oraliqdagi saqlanish paketni uzatishni sekinlashtiradi, ya’ni unda har bir qurilmadan kelgan paket dagi FCS ni tekshirib, undan so‘ng uni keyingisiga yuboradi. Past sifatli tarmoq kanalida ma’lumotni uzatishda qurilmada ushlanib qolish (kechikish) tufayli, doimiy bo‘lmagan tartibsiz xolat yuzaga keladi. Shuning uchun X.25 tarmog‘idan sifatli bo‘lgan sezgir trafikni (masalan, raqamlashtirilgan so‘zlashuv) uzatib bo‘lmaydi.

Keyinchalik yuqori sifatli raqamli kanallar paydo bo‘lgandan so‘ng, bunday tekshirish ortiqcha bo‘lib qoldi. Shuning uchun FR kommutatorlari teshikli kommutatsiya texnologiyasidan foydalanadi, ya’ni manzil axborotini o‘qib bo‘lgandan keyin darhol navbatdagi tranzit qurilmaga uzatib yuboradi. Bu esa hech qancha vaqtni olmaydi. Agar qandaydir xato yuzaga kelsa, FR kommutatorlari kadrni xatoli qismini olib tashlaydi. Xatoni to‘g‘rilash funksiyasi yuqori pog‘onali protokolga yuklatiladi (masalan TCP yoki SPX). Bu xolat kadr hisob kitobi va qayta ishlanishiga ketadigan xarajatni kamaytirib, uning o‘tkazuvchanlik qobiliyatini oshiradi.

FR texnologiyasi oqimni boshqarishda o‘zining maxsus boshqarish mexanizmiga ega bo‘lib, turli xildagi trafikni moslashuvchan multipleksorlanishini ta’minlaydi.

Oqimni boshqarish - bu paketlarni kommutatorga uzatayotganda tezlikni boshqarish jarayonidir. Agar qabul qiluvchi kommutator qandaydir paketni qabul

qila olmasa (o‘ta yuklanish tufayli), berilgan protokol yordamida marshrutizatordan ma’lumot uzatishni to‘xtatsa bo‘ladi va yuksizlanish kamaygandan so‘ng, ishni davom ettirishi mumkin bo‘ladi. Bu jarayon qabul qiluvchi kommutatorga kadrni tashlab yubormaslikni kafolatlaydi. FR bu protokolni to‘liq qo‘llab quvvatlay olmaydi, kadrni qabul qilishda FR kommutatorida buferlar soni yetishmasa u DTE bayroq bilan o‘rnatilgan kadrni tashlab yuborishga imkon beradi.

Marshrutizator ma’lumotlarni qayta tiklashi mumkin, lekin bu kanalda katta tiqilib qolishga, kechikishga olib kelish ehtimoli bor.

Bu muammoni hal qilish yuqori pog‘onali hisoblanuvchi TCP/IP ga xos bo‘lib, boshqarish mexanizmi qaysidir qismini quvvatlab turadi. FECN va BECN bitlarini ishlatganda to‘g‘ri va teskari yo‘nalishda o‘ta yuklanishini xabar beruvchi bayroqlari bo‘ladi.

Axborot bitlari FECN va BECN kadr trafikka tiqilib qolgan zahoti shu kadrga joylashtiriladi. FR interfeys marshrutizatorlari bu bitlar miqdorini shifrlashi mumkin. Masalan TCP/IP ga mos yuqori turuvchi protokol bazasida oqimlarni boshqarishni faollashtirishi mumkin.

Shuni bildirib o‘tish joizki, bu mexanizm tarmoqni tartibli o‘tkazish qobiliyatiga to‘g‘ri kelmaydi va FR qo‘llab quvvatlashi tufayli kelishuvsiz axborot uzatish tezligiga moslashib ketadi.

Committed Information Rate - CIR (CIR) - minimal o‘tkazish qobiliyati har bir PVC yoki SVC ga kafolatlangan. Minimal o‘tkazish qobiliyati (soniyaiga bit bilan o‘lchanadi) tarmoq FR mijozi tomonidan tarmoq orqali yubormoqchi bo‘lgan ma’lumotlar hajmiga qarab tanlanadi va u tarmoq FR operatori yoki administratori tomonidan kafolatlanadi. Bu vaqtda tezlik 16 kbit/s dan 44,8 mbit/s gacha o‘zgarib turishi mumkin. Agar paket jo‘natmalari mijozga yoqilgan port tizimiga ta’sir qilmasa va FR tarmog‘i o‘tkazuvchanlik qobiliyati ma’lum vaqtda bo‘sh resursga ega bo‘lsa, u holda mijoz kelishilgan miqdor CIR ni qabul qilib qo‘yishi mumkin.

Vaqt bo‘yicha tezlikni o‘rtachalashtirish bu yerda kerakli vazifani bajaradi. Misol uchun, ulanish liniyasi orqali o‘tkazish oralig‘i 64 kbit/s ga teng bo‘lgan

foydalanuvchi 32 kbit/s ga teng bo‘lgan CIR virtual bog‘lanishni topmoqchi. Bu degani birinchi yarim soniyada 32 kbit/s qabul qilib, kommutator keyingi yarim soniyada kelgan o‘ng tarafdagi qolgan bitlarni rad etadi. Shuning uchun uzatiladigan axborotga impulsli moslashtirish tushunchasi kiritiladi (Committed Burst Size-Bc) - ma’lumotning maksimal hajmi, ya’ni tarmoq T_s vaqti oralig‘ida uzatishga «majbur» bo‘ladi.

FR texnologiyasi sezgir ma’lumot uzatishda trafikning kechikishi tufayli kanal oralig‘ini zahiralash mexanizmini qo‘llaydi, ya’ni kanalni vaqt bo‘yicha zahiralashda ishlatiladi.

Oddiy ma’lumotlarda multipleksorlash ishlatiladi. Bir qator boshqa mexanizmlar majmuasi nutq paketlarini bir - xil tezlikda uzatishni ta’minlaydi.

Zamonaviy FR nutqni taxminan (10-15 marta) zichlashtirish uchun maxsus algoritmni amalga oshiradi, ya’ni ko‘proq kadr uzatishni qo‘llashga imkon yaratadi.

Mexanizmlardan biri talaffuzni yo‘qotish hisoblanadi. Odatda telefonda so‘zlashayotganlar galma - galdan gapiradilar. Oddiy telefon orqali so‘zlashayotganda «jim» turgan tarafda maxsus shovqin signali uzatiladi. Undan tashqari, gapning va har bir so‘zning orasida tanaffus bo‘ladi. Statistika bo‘yicha telefon orqali gaplashayotganda gapni 60% jim turishni uzatishga ketadi. Kanal oralig‘ida kerakli signaldan tashqari hamma qismini ma’lumot uzatishga ishlatsa bo‘ladi. Qabul qilishda foydalanuvchida «o‘lik» liniya taassurotini uyg‘otmaslik uchun shu vaqtning o‘zida «pushti» shovqin ishlab chiqariladi.

Yana bir ahamiyatli mexanizmlardan biri «raqamlashning o‘zgarish tezligi» hisoblanadi, ya’ni ovoz uzatish minimal qabul qilish sifatini bildiruvchi «kam tezlikdagi (baza) raqamlash» topiladi va «bazali» kadrlar oqimi vujudga keladi. Kanaldagi bo‘sh oraliqlarni esa ovoz sifatini yaxshilovchi qo‘shimcha paketlar tashkil etadi. Bu turdagi telefon trafigini qayta ishlash algoritmi FR tomonidan oson bajariladi.

Ma’lumotlarni uzatish uchun magistral tarmoqda FR mexanizmi bo‘lsa, abonent tarafda qo‘shimcha protokol ishlatiladi.

FR texnologiyasining asosiy kamchiligi shundan kelib chiqadiki, FR kanal pog‘onasi protokoli hisoblanadi. FR yuqori turuvchi protokollarni «ajrata olmaydi». Shu sababli ko‘p muammolar kelib chiqadi. Bu trafikni bir - biridan ajratishning yagona yo‘li har biriga o‘zining virtual bog‘lanishini ta’minlash kerak yoki ikkinchi virtual ulanish uchun qo‘shimcha xarakat talab qilinadi. Muammolar doirasi IP-multikasting deyiladi:

- zichlab uzatilgan signallar yuklamasi tarmoqlarda yo‘qolishi mumkin;
- ovozli qayta uzatish kadri uchun standart to‘lov xizmati bo‘lmaganligi;
- ovozli qayta tarqatilish kadri paketli kommutatsiya tarmog‘ida ushlanishlarga, signallarni buzilishlariga va sifatini pasayishiga olib keladi.

FR texnologiyasi quyidagilarni talab qiladi:

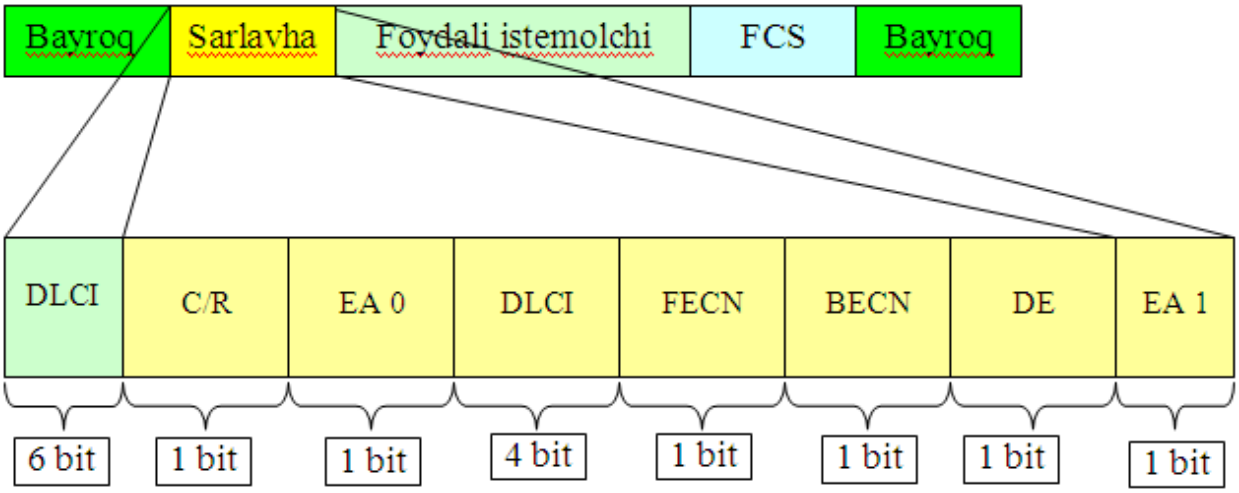
- ohirgi qurilma yuqori pog‘onali intellektual protokol bilan ta’minlangan bo‘lishi kerak;
- aloqa kanali virtual va xatolardan xoli bo‘lmog‘i kerak;
- tadbiq etilgan jihozlar turli - xil uzatishga mo‘ljallangan bo‘lishi kerak.

Bu texnologiya nafaqat lokal tarmoqlarda va xududiy tarmoqni trafik bilan boshqarishga, balki sezgir trafikni, ya’ni ovozni uzatishga moslashadi.

FR tarmoq qurilmasi va foydalanuvchi qurilmasi yordamida interfeys orqali ma’lumotlarni paketli kommutatsiya ko‘rinishida uzatish imkonini beradi. Interfeys vazifasini bajaruvchi tarmoq FR ma’lumot uzatish va tashish uchun ishlatilishi mumkin yoki biror bir korxona uchun xizmat qilishi mumkin.

Tarmoq interfeysi nuqtai nazaridan FR ham X.25 protokoli qatoridan hisoblanadi. Biroq FR texnologiyasi X.25 ga nisbatan funksional imkoniyatlari va formati (hajmi) bo‘yicha farq qiladi. FR asosan liniyadagi katta ma’lumotlar oqimi uchun mo‘ljallangan bo‘lib, yuqori ko‘rsatkichni va foydani ta’minlaydi (2.11-rasm).

FR tarmog‘i orqali uzatish uchun ma’lumotlar kadrga segmentatsiya qilinadi. Bir va bir nechta bir baytli bayroqlar kadrning bo‘linishiga xizmat qiladi. Kadr har xil uzunlikda bo‘lishi mumkin. Kadrning maksimal uzunligi 1600 oktet.



2.11 – rasm. FR kadr formati

Bayroqlar (flags) ma'lumotlar bloki boshi va ohirini cheklab turadi. Boshidagi bayroqdan ikkita bayt axborot manziliga (address) keladi - sarlovha. FCS - ikki baytli kadrni nazorat yig'indisi (Fame control sum).

FR kadrini tashkil etuvchilariga ta'rif beramiz.

- DLCI - ulanish identifikatori;
- C/R - maydonning amaliy qismi, FR protokolidan foydalanmay, tarmoq orqali ochiq uzatiladi;
- EA - manzilning 2, 3 yoki 4 bitli maydonini bildiradi;
- FECN - qurilmada tiqilib qolishlar to'g'risida axborot beradi;
- BECN – manba qurilmasida tiqilib qolishlar to'g'risida axborot beradi;
- DE - kadrni identifikatsiya qiladi, ya'ni tiqilib qolgan vaqtda tashlab yuborilgan bo'lsa.

Xususiy tarmoqni oddiy usulda amalga oshirish axborot qurilmasi uchun FR interfeysiga an'anaviy T1 multipleksorlarini qo'shish hisoblanadi. Undan tashqari boshqa ovoz uzatish va video-telekonferensiyalarni o'tkazish kabi biriktirilgan vazifalarni bajaruvchi interfeyslarga (FR maxsuslashtirilgan interfeyslarni emas) ham o'rnatiladi.

Umumiy ulanishdagi FR tarmog'iga xizmat qilinayotganda telekommunikatsiya liniyasining markaziy ofisida (MO) joylashgan FR

kommutatsiya qurulmasi orqali yo‘naltiriladi.

Tarmoq qurulmasiga ulanuvchi foydalanuvchi qurilmasi axborot uzatish tezligi keng diapozondan tanlangan tezlikda ishlashi mumkin. 36 kbit/s dan 2 mbit/s diapozonidagi tezlik hisoblanadi.

Agar umumiy ulanish va xususiy tarmoqlarda FR protokoli ishlatilsa, har bir foydalanuvchiga FR interfeysini qo‘yish zaruriy shart hisoblanmaydi. Hozirgi kunda FR tarmog‘i ichidagi ulanishlararo qurilmalarning standartlari yo‘q.

ATM texnologiyasining asoslari

Aloqada o‘tkazuvchanlik qobiliyatini o‘sish talabini baholash usuli bu yuqoridagi o‘zgarishlardan kelib chiqqan holda ikkita elektr qonunini o‘zaro hamkorlikda ishlatishdir, ya’ni:

- Djo qonuni, bunda soniyasiga million operatsiyaga ega bo‘lgan hisoblash unumdorligi (MIPS) har ikki yilda 2 barobar oshadi;

- Rudj qonuni, bunda aloqaning o‘tkazuvchanlik qobiliyati, har soniyadagi million operatsiya uchun 0,3 dan 1 Mbit/c ni tashkil etadi.

1990 yilda har bir kompyuterlarni o‘rtacha unumdorligi soniyaiga 100 mln. operatsiyani tashkil qilganini, aloqaning o‘tkazuvchanlik qobiliyati esa keyingi yillar ichida o‘sganini va 300 Mbit/c va 100 Gbit/s oralig‘iga yetganini eslashimiz mumkin.

Agar o‘rtacha talab bu raqamlardan o‘n barobar kichik bo‘lganda ham, baribir ular lokal va katta masshtabli zamonaviy tarmoqlarni unumdorligidan o‘tib ketardi. Bitlarni uzatishda yuqori tezlik va kam to‘htalishlar asosiy tavsiflar bo‘lib hisoblanadi. Bularga yana uchinchi ta’minlovchi texnologiyani bir xillik tavsifini qo‘shishimiz mumkin. Bu tavsiflar 1980 - yillar boshlarida boshlangan izlanishlarni dastlabki zamini qilib olindi. Bu izlanishlarni o‘tkazishda oqimlarni boshqarish va xatoliklarni qayta ishlash funksiyalari birgalikda bajarilishi taxmin qilingan edi. Bu taxmin raqamli traktlarni yuqori sifatiga, tarmoq zveno xududida ishlovchi o‘zaro bog‘lik bo‘lmagan uzatishni yuqori tezlikga va protokoliga

asoslangan edi.

Bundan tashqari, uzatish oqimiga bog‘lik bo‘lmagan yagona kommutatsiya usulini qo‘llashni topish haqida ma’lum bir to‘xtamga kelingan edi. Bu tamoyillarni qoniqtiruvchi protokol bo‘lib, kadrlarni retranslyatsiya protokoli (FR) hisoblanadi. Xuddi o‘sha vaqtda MAC (Medium Access Control) muhitiga imkoniyat bo‘lgan, boshqariluvchi pog‘ona paketlarini yuboruvchi lokal tarmoq ko‘priklarini o‘zaro hamkorlikda ishlatish g‘oyasi paydo bo‘ldi.

ATM rejimlari haqida so‘zlashdan oldin, biz ikki xil asosiy kommutatsiya rejimlari to‘g‘risida to‘htalib o‘tamiz:

- kanallar kommutatsiyasi, bu ma’lumotlar uchun to‘liq shaffoflikka ega. Bundan tashqari u real vaqt mobaynida so‘zlashuv va videoni uzatish talablariga to‘liq javob beradi va uni yuqori tezliklarga moslashishi ko‘riladi. Ammo bu usul kamchilikka ega. U kanallarni ma’lum uzatish tezligida namoyon etadi. Masalan, 64 Kbit/c uzatish tezligiga ega xizmatlarning raqamli oqimi. Shuning uchun turli xil loyihalanuvchi xizmatlar uchun munosib belgilangan uzatish tezligidagi kanallarni tanlash va rejalashtirilishi kerak edi. Bu rejalashtirish qiyin va noma’qul edi, ya’ni aniq xizmat ma’lum uzatish tezligiga mos kelishi shart emas. Bu yo‘nalishdagi qidiruvlardan samaradorlik kamligi tufayli vos kechishga to‘g‘ri keldi.

Virtual kanal tushunchasiga asoslangan paketli kommutatsiya moslashtirishni tashkil qilib bera oladi va aloqa kanallarini samarali ishlatishni ta’minlaydi.

Zamonaviy texnologik tarmoqlarni rivojlanishi, optik tolali aloqa liniyalarini yaratishdagi yutuqlar, katta xotirali va yuqori pog‘onada tez ishlaydigan integral sxemalarni paydo bo‘lishi ko‘chirishni asinxron rejimi (ATM) deb ataladigan yangi transportlash usulini yaratishga olib keldi. ATM texnologiyasini yaratilishi va rivojlanishi tashabbuskorlari sifatida yirik telekommunikatsiya kompaniyalari namoyon bo‘ldi. Ularni birgalikdagi xarakatlari ATM texnologiyasi yordamida ma’lumotlarni uzatish usulini ishlab chiqish va bunda axborotni tez, arzon va sifatli yetkazishga qaratilgan edi. ATM texnologiyasi bu talablarni to‘la qondirgandan

so‘ng, unga keng yo’lakli texnologiya B-ISDNni transport mexanizmi asos qilib olindi. Bu ma’lumotlarni uzatishni raqamli standarti bo‘lishi bilan birga, telefon tarmoq abonentlari uchun global tarmoq orqali ma’lumotlar oqimini uzatish imkonini beruvchi kommunikatsiya protokollarini topishga sabab bo‘ldi. ATM texnologiyasi shunday yagona bo‘ldiki, bunda uni ham lokal, ham global tarmoqlarda ishlatish imkoniyati paydo bo‘ldi. U yuqori o‘tkazuvchanlik qobiliyatini namoyon qiladi va uzatish uchun axborot yo‘q bo‘lsa, tarmoq resurslarini ishlatmaydi. Agar axborot paydo bo‘lsa, u yacheykalarga joylashtiriladi. So‘ngra bu ma’lum iste’molchi kanali orqali uzatiladi. Agar ATM tarmog‘idagi qurilma hech narsa yubormasa, unda tarmoq bo‘sh resurslarning boshqa qurilmalarni ishlatadi.

ATM texnologiyasi quyidagilarni ta’minlaydi:

- belgilangan uzunlikdagi paket (yacheyka) ko‘rinishida ma’lumotlarni barcha turlarini transportlash (so‘zlashuv, musiqa, xarakatsiz va xarakatli tasvirlar, ma’lumotlar);

- foydalanuvchi uchun unga kerak bo‘lgan tarmoq o‘tkazuvchanlik qobiliyati resurslariga kerakli paytda vaqt ajratish;

- interaktiv xizmat va axborotlarni taqsimlash xizmatlarini, shu bilan birga aloqa o‘rnatiladigan va aloqa o‘rnatilmaydigan xizmatlarni ham ta’minlaydi.

ATM texnologiyasi tarmoq operatorlari uchun quyidagi noyob imkoniyatlarni yaratadi:

- tarmoqning yuqori moslashuvchanligini ta’minlaydi. Bunda foydalanuvchilarni sifatli xizmatga bo‘ladigan talablarini o‘zgarishi tushuniladi;

- tarmoqning qurilish loyihasiga va ekspluatatsiyasiga ketgan sarf - xarajatlarni kamaytiradi va shu bilan birga tarmoq qurulmasini ishlab chiqish, ya’ni ko‘plab ikkilamchi tarmoq o‘rniga bitta tarmoq yaratilishi va ekspluatatsiya qilinishi tushuniladi.

Aloqa tarmoqlarini dunyo tajribasidagi tahlili analog tarmoqlardan, raqamli tarmoqlarga o‘tish bosqichlari quyidagilar ekanligini ko‘rsatadi:

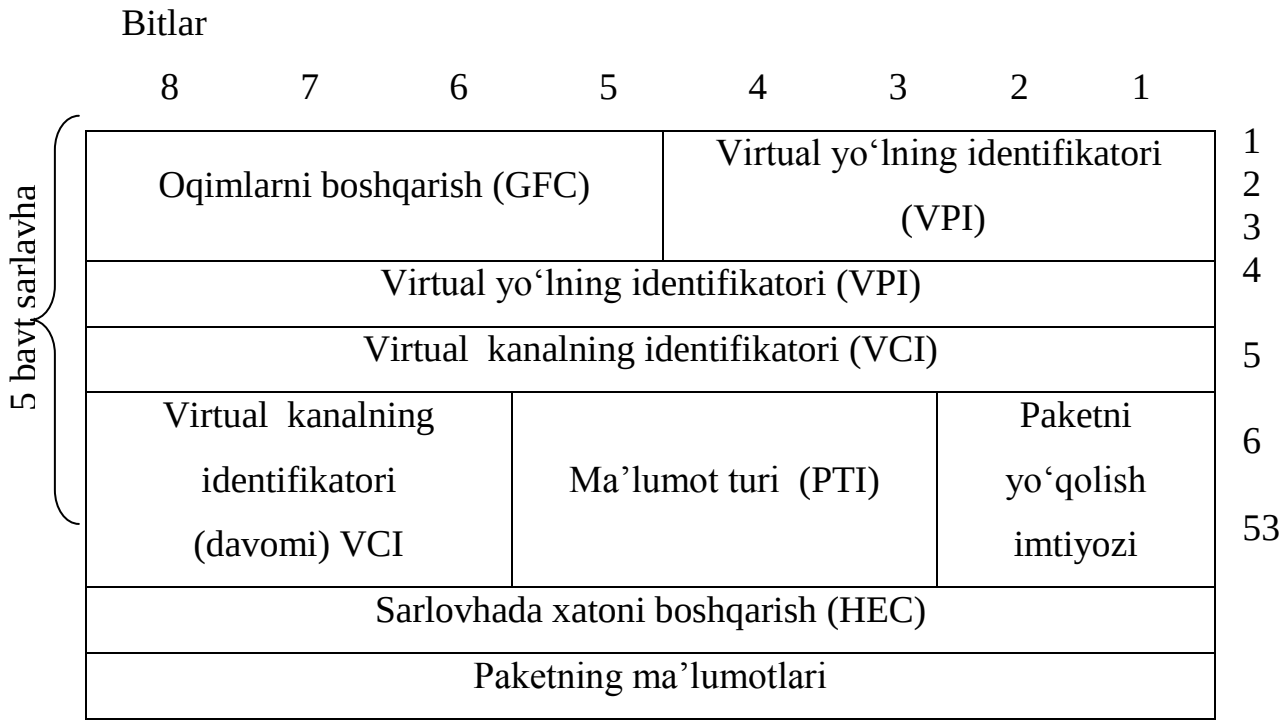
- raqamli tarmoqlarni rivojlanishi;

- tor yo’lakli integral xizmat ko‘rsatishning raqamli tarmoqlarini yaratilishi. Bunda telefon xizmatlari uchun kanal kommutatsiyasi va 64 Kbit/s tezlikli raqamli tarmoq bazasidagi telematik xizmatlar uchun paketli kommutatsiya ishlatilishi;

- keng yo’lakli integral xizmat ko‘rsatishni raqamli tarmoqlarini qurilishi.

ATM texnologiyasi umumiy foydalanish tarmoqlarida ovoz, video va ma’lumotlarni uzatishda zarur hisoblanadi. Yuqori o‘tkazuvchanlik qobiliyati va sifatli xizmat ko‘rsatishni ta’minlashi, uni magistral va lokal tarmoqlarda ham qo‘llanilishiga imkoniyat yaratib beradi.

ATM texnologiyasida ixtiyoriy kanal orqali, ya’ni kompyuter, telefon, videokanallardan kelayotgan ma’lumotlar oqimini 53 baytga teng uzunlikdagi va 5 baytga teng sarlovhaga ega bo‘lgan, belgilangan uzunlikdagi paketlar orqali uzatish ko‘zda tutiladi. ATM paketlari yacheyka (cell) deb ataladi. Paketlarning kichik uzunlikda bo‘lganligi, ularni uzatishdagi vaqtni qisqarishiga olib keladi va bu paketlarni uzatishda kam to‘xtalishlarga olib keladi. Bu uzatishni doimiy pog‘onada bo‘lishini talab qiladigan multimediyali axborotlarga xosdir (2.12-rasm).



2.12 - rasm. ATM yacheykasining tuzilishi

Multimediyali trafikka tarmoq kommutatorlari birinchi marta xizmat ko‘rsatganda, uning paketlari 155 Mbit/s tezlikdagi va 53 baytga teng uzunlikdagi paketlarni uzatish vaqtida ham, kamida 3 mks kutish vaqtini talab qiladi.

Paketlarning ishlatilish manzili qurilmasiga ega bo‘lishi va axborot hajmining foizi paketning ma’lumot maydonidan oshib ketmasligi uchun, ATM texnologiyasida barcha global tarmoqlar uchun usul qo‘llaniladi, ya’ni bu tarmoqlar har doim aloqa o‘rnatiladigan protokol yordamida ishlaydi va ohirgi qurilmalarning manzili faqatgina aloqa o‘rnatish bosqichida ishlatiladi.

ATM pog‘onasini bazali elementi bo‘lib yacheyka hisoblanadi. ITU-Tni ATM uchun taklif qilingan ATM paketining umumiy ko‘rinishi quyidagicha: yacheyka sarlovhasi 5 oktetni tashkil etsa, axborot maydoni 48 oktetga tengdir. ITU.361 rekomendatsiyasiga binoan yacheykani uzatish (2.12 – rasm) quyidagi ketma-ketlikda amalga oshiriladi:

- oktetlar birinchisidan boshlab o‘sish navbatida uzatiladi, oktet ichidagi bitlar 8-chisidan boshlab kamayish tartibida uzatiladi;

- yacheykani hamma maydonlari uchun birinchi bit asosiy hisoblanadi (MSB-Most Sighificant Bit).

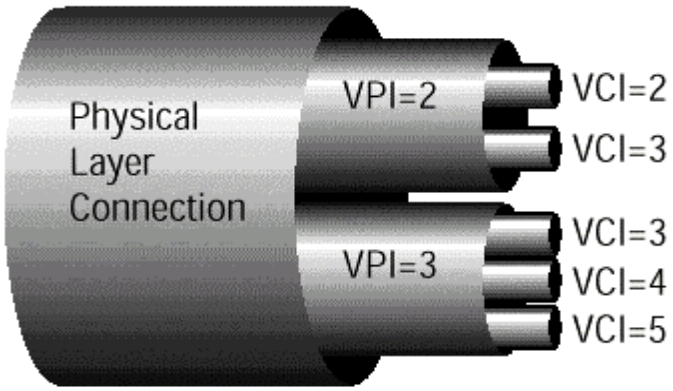
“Foydalanuvchi-tarmoq” interfeysidagi yacheykani sarlovhasi quyidagi ko‘rinishga ega:

- oqimni umumiy boshqarish (OUB) (GFC-Generic Flow Control) 4 bit;
- virtual yo‘l identifikatori (VYI) (VPI-Virtual Puth Identifier) - 8 bit;
- virtual kanal identifikatori (VKI) (VCI-Virtual Channel Identifier) -16 bit;
- foydali yuklama turi (FYuT) (PT - Payload Type) - 4 bit;
- yacheykani yo‘qotish imtiyozi (YaYP) (CLP - Cell Lass Priority) 1 bit;
- sarlovhadagi xatoliklarni nazorati (SXN) (HEC-Heder Error Control)-8 bitga teng.

Virtual kanallar va virtual yo‘llar

Yacheyka sarlovhasida ATMni har bir yacheykasi ikki qismli manzilga ega, ya’ni VPI (virtual path identifier, VPI) va VCI (vitual channel identifier, VCI)dan iborat. Bu manzil fizik interfeys pog‘onasida ATMni virtual ulanishini noyob identifikatsiyasini ta’minlaydi. Uzatishni fizik marshruti (masalan, DS1 yoki DS3) bir yoki undan ko‘proq marshrutlarga ega va bundan tashqari har bir virtual marshrut bir yoki undan ko‘proq virtual kanallarga ega bo‘lishi mumkin.

Quyidagi 2.13 - rasmda fizik pog‘onadagi ulanish ko‘rsatilgan.

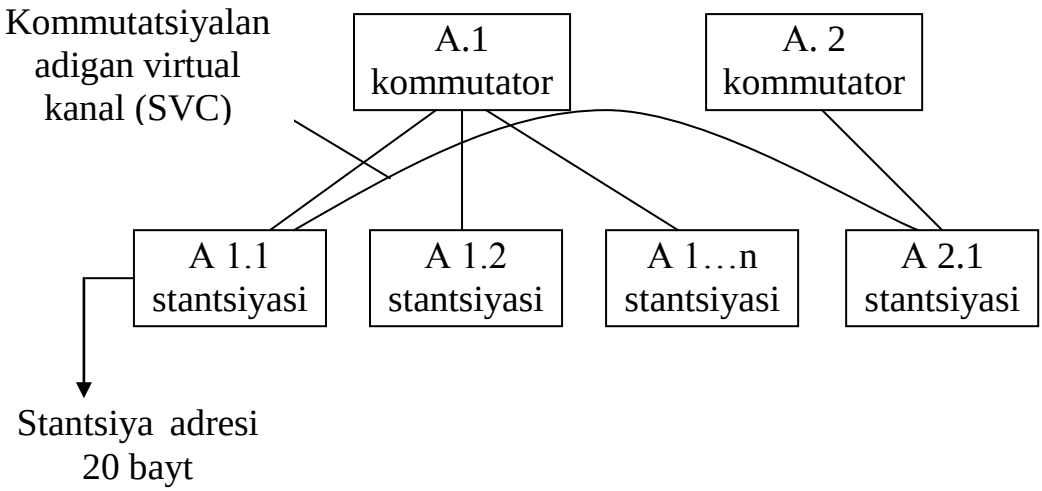


2.13-rasm. Fizik pog‘onadagi ulanish

Uzatishni ma’lum marshrutida VPI va VCI alohida kanalga biriktirilgan va faqat berilgan kommutator uchun ma’lum qiymatlarga ega hisoblanadi. VPI va VCI manzillari tarmoq ulanish marshrutida ATMni har bir kommutatorlarida o‘zgarib turadi, ya’ni har bir kommutator kiruvchi VPI va VCIni, chiquvchi VPI va VCIga o‘zgartirib turadi. Ziddiyatli holatlar sodir bo‘lmagan vaqtda, manzil tarmoq boshqa joylarida ishlatilishi mumkin. ATM uzatish marshrutiga, virtual marshrut yoki virtual kanalga kommutatsiyani ta’minlab beradi.

Aloqa o‘rnatilayotganda, unga ulanishni oraliq raqami beriladi va bu ulanish paytida keyingi paketlarni uzatishda (ya’ni aloqa uzilish vaqtigacha) paketlarni xizmat maydonida, ishlatilish manzilining qurilmasi o‘rniga ancha qisqa bo‘lgan ulanish raqami ishlatiladi. Paketda 5 baytga teng kichik sarlovha bor. Bulardan 3 bayti, ATM tarmog‘i doirasida noyob bo‘lgan virtual ulanish raqamiga beriladi.

Qolgan 48 bayt esa, raqamli ovozni 6 razryadiga yoki hisoblash tarmog‘ini 6 baytli ma’lumotiga ega bo‘lishi mumkin. Katta bo‘lmagan belgilangan uzunlikdagi paketlar, sinxron trafikni uzatishda uzilishlar kam bo‘lishini kafolatlaydi. Shu narsa ayonki, har bir kanal uchun qat’iy belgilangan kanalli intervallarni rad etish natijasida, ideal bir - xillikga ega bo‘lish mumkin bo‘lmay qoladi. Biroq turli trafik paketlariga turli xizmatlar ko‘rsatilganda, birinchi paketni maksimal kutish vaqti, bitta paketni qayta ishlash uchun ketgan vaqtga teng bo‘ladi. Trafik turini kiritish va birinchi xizmat ko‘rsatish, ATM texnologiyasini o‘ziga xos tarafi hisoblanadi va bu unga bitta kanalda sinxron va asinxron paketlarni joylashtirish imkonini beradi. ATM tarmoqlarida ohirgi qurilma va tarmoq orasida ulanish aloqani individual liniyasi orqali amalga oshiriladi. Kommutatorlari esa, o‘zaro bir - birlari bilan zichlashtirilgan kanal orqali ulanadi va ular kerakli kommutatorga ulangan barcha qurilmalarning paketlarini uzatadi (2.13-rasm).



2.13 - rasm ATM tarmog‘ining tuzilishi

ATM tarmog‘i telefon tarmog‘i tuzilishsiga o‘xshash tuzilishga ega. Bunda ohirgi stansiyalar quyi pog‘onali kommutatorlar bilan ulanadi. Bu esa o‘z navbatida yuqori pog‘onali kommutatorlar bilan ulanadi.

ATM kommutatorlari, kommutatorlar tarmog‘ida trafikni marshrutizatsiya qilish uchun ohirgi qurilmalar manzilini ishlatadi. Paketli kommutatsiya virtual kanal identifikatori (VCI) asosida sodir bo‘ladi. U o‘rnatilganda aloqa o‘rnatishga tayinlanadi va aloqa uzilganda u yo‘q qilib tashlanadi. Virtual ulanish ohirgi

stansiyani 20 baytli manzillari asosida o‘rnatiladi. Manzilni bunday uzunligi katta tarmoqlar uchun mo‘ljallangan. Manzil ierarxiyali tuzilishga ega. U telefon tarmog‘idagi raqamga o‘hshashdir va shahar, davlat kodlariga moslarini ishlatadi. Virtual ulanishlar doimiy (Permanent Virtual Circuit, PVC) va kommutatsiyalanadigan (Switched Virtual Circuit, SVC) bo‘lishi mumkin. Doimiy virtual ulanishlar ikkita belgilangan abonentlarni ulaydi va tarmoq administratori tomonidan o‘rnatiladi. Kommutatsiyalanadigan virtual ulanishlar ixtiyoriy ohirgi abonentlar orasida aloqani o‘rnatish boshlanganda o‘rnatiladi. ATMni ohirgi stansiyasini quyi pog‘ona kommutatorlari bilan ulash UNI (User Network Interface) standarti orqali amalga oshiriladi. UNI paket tuzilishini, stansiya manzilini, boshqariladigan axborotni almashishni, ATM protokoli pog‘onasini va trafikni boshqarish usullarini aniqlaydi.

Nazorat savollari

1. Ethernet kadri nimalardan tashkil topgan?
2. VLAN ni ishlashini tushuntiring?
3. L2, L3 kommutatorlarning farqi nimada?
4. Kommutatorlarni ishlashi nimaga asoslangan?
5. Paketli kommutatsiyadan foydalangan holda virtual kanal turlari va virtual kanal ish tartibi, deytagramm rejimi va ish tartibi qanday?
6. X.25 stek protokoliga tavsif bering?
7. Frame Relay texnologiyasining talabi qanday?
8. Frame Relay kadrini tuzilishini tushuntirib bering?
9. Tarmoqda ishlatiladigan qurilmalarga tavsif bering?
10. ATM tarmog‘ini qurish tamoyillari nimalardan iborat?
11. ATM yacheykasini tuzilishini tushuntirib bering?

3. MA’LUMOT UZATISH TARMOQLARIDA TARMOQ POG‘ONASI PROTOKOLLARI

3.1. Tarmoq pog‘onasi protokollari. IPv4 va IPv6 manzillash

Tarmoq pog‘onasi quyidagilarni ta’minlaydi:

- foydalanayotgan tarmoq va fizik muhitlarni kommutatsiyalash;
- marshrutizatsiyalashga bog‘liq bo‘lmagan transport tarmoq pog‘onasi uchun axborotlarni uzatishni ta’minlovchi tarmoq ulanishlarini o‘rnatish;
- faol holda tutish va uzish vositalarini yetkazib berish;
- ma’lumot oqimlarini boshqarilishini ta’minlash;
- paketlar jo‘natilishi ketma – ketligini tartibga solish;
- shoshilinch ma’lumot uzatilishini ta’minlash;
- xatolarni topish va tuzatilishini ta’minlash.

Tarmoq pog‘onasining ma’lumotlarini paketlar deb atash qabul qilingan. Tarmoq pog‘onasida 2 xil protokol ishlaydi.

1. **Tarmoq protokollari** – tarmoq orqali paketlarni xarakatini yo‘lga qo‘yadi;

2. **Marshrutlash protokollari** – marshrutizator tarmoqlararo bog‘lanishlar topologiyasi to‘g‘risida axborot to‘playdi.

Tarmoq pog‘onasi vazifalariga quyidagilar kiradi:

- murakkab tarmoqlarning qurilmalari o‘rtasidagi paketlar uzatilishi;
- biron bir me’zon asosida paketlarni uzatish uchun eng muqobil marshrutni aniqlash;
- kanal pog‘onasi protokollarini moslashtirish (murakkab tarmoq miqyosida).

Uchinchi pog‘onada bajariladigan tarmoq protokoli ma’lumot paketlari marshrutini tanlashda qo‘llaniladi

1980-yillarning birinchi yarmida yaratilgan va keyinchalik TCP/IP nomini olgan axborot uzatish modelining protokoli yaratilgan. TCP/IP stek protokoli to‘rt

pog‘onali tuzilishga ega bo‘lib, har bir pog‘onada o‘zining protokollari mavjuddir. Bu protokol orqali manzillashdan nafaqat internet tarmog‘i elementlarini manzillashni amalga oshirish mumkin, balki lokal tarmoqda ham foydalanuvchilarga yagona manzillar berish mumkin. Manzillash orqali tarmoq foydalanuvchilari bir-biridan farqlanadi va paketlar aniq belgilangan foydalanuvchiga yetib borishi kafolatlanadi. Oldin shaxsiy kompyuterlar soni kam bo‘lgan va ularni manzillashda muammo bo‘lmagan, ammo shaxsiy kompyuterlarning va boshqa tarmoq qurilmalarining sonini keskin ortishi manzillashda muammolarni vujudga keltirdi. IP protokollarining to‘rtinchi IPv4 va oltinchi IPv6 versiyalari mavjud bo‘lib, ular turli xususiyatlarga ko‘ra bir-biridan farqlanadi. Barcha tarmoqning asosiy tuzilishi IPv4 ga asoslangan, ammo ushbu protokol taqdim etayotgan manzillar soni hozirgi ehtiyojlarni qondira olmaydi. Internet tarmog‘i shu darajada rivojlanmoqdaki, u taqdim etayotgan xizmat turlari ham ko‘payib bormoqda. Internet buyumlari, ya’ni masofadan boshqaruv tizimlari, “aqlli uy” kabi zamonaviy imkoniyatlarni ta’minlash uchun IPv6ni qo‘llashdan boshqa iloj qolmadi. “Xalqaro simsiz tadqiqot” forumi a’zolarining baholashicha 2017-2020 yillarda internet buyumlarining soni 7 trln.ni tashkil etadi va bir foydalanuvchiga to‘g‘ri keladigan o‘rtacha miqdorda Internet buyumlarining soni 3000-5000 tani tashkil qilar ekan [1]. Hozirda IPv4 manzillari yakunlangani uchun IPv6 protokolini tarmoqda qo‘llash ustida global miqyosda ish boshlangan.

IP protokoli

Internetda ko‘plab turli xil paketlardan foydalaniladi, lekin asosiylaridan biri bu - IP-paketdir (RFC-791). IP-protokol ishonchli bo‘lmagan transport muhitini taklif etadi. Mazkur protokolning ma’lumotlarni uzatish algoritmi juda ham oddiy: xato hollarda deytagramma tashlab yuboriladi, jo‘natuvchiga esa tegishli ICMP-xabar yuboriladi (yoki hech narsa yuborilmaydi).

IP-protokolida tarmoqlararo xizmatlarni ta’minlash uchun to‘rtta asosiy mexanizm qo‘llaniladi: xizmat ko‘rsatish turi, paket yashash vaqti, sarlovhaning nazorat yig‘indisi, qo‘shimcha imkoniyatlar.

Xizmat ko‘rsatish turi tarmoqlararo deytagrammaning uzatilishida talab etiladigan sifatni ko‘rsatishi uchun foydalaniladi.

Paketning yashash vaqti tarmoqdagi paketning mavjud bo‘lish vaqtining yuqori chegarasini ko‘rsatadi. Ushbu ko‘rsatkich jo‘natuvchi tomonidan beriladi va paketning marshrut nuqtalari bo‘ylab xarakatlanishiga ko‘ra kamayib boradi. Paketning vaqti qabul qilib oluvchiga yetib borguniga qadar nol bo‘lsa, u holda ushbu paket yo‘q qilinadi.

Sarlovhaning nazorat yig‘indisi undagi ma’lumotlarning himoyasini ta’minlaydi. Agarda modul sarlovhada xatolikni aniqlasa, ushbu paket uni aniqlagan modul tomonidan yo‘q qilinadi.

Qo‘shimcha imkoniyatlar ayrim qo‘shimcha xizmatlar bajarilishini ta’minlaydi. Masalan, ma’lumotlarni himoyalash va maxsus marshrutlashtirish usullari.

IPv4 protokoli

IPv4 protokoli o‘tgan asrning 70-yillarida ishlab chiqilgan. 2^{32} ta manzillarini taqdim eta olish imkoniga ega bo‘lgan ushbu protokol bir qancha kamchiliklarga ega. Eng asosiysi, manzillar soni barcha ehtiyojlarni qondirish uchun kamlik qiladi. Bundan tashqari xavfsizlik masalalari ushbu protokolda ko‘rib chiqilmagan.

IPv4 paket formati

IPv4 paketlar formati 3.1-rasmda ko‘rsatilgan.

Sarlovha maydonlarining funksional vazifasi quyidagilardan tashkil topgan:

Versiya maydoni (Version) mazkur protokol versiyasini ko‘rsatadi. Hozirgi vaqtda protokolning 4-versiyasi bilan birgalikda (ya’ni 0100 maydonida) protokolning 6-versiyasidan foydalanish boshlanadi (ya’ni 0110 maydonida).

Sarlovha uzunligi maydoni (Header Length) tarmoqlararo diagramma sarlovhasining 32 razryadli so‘zlardagi uzunligini ko‘rsatadi. Eng kam (minimal)

uzunlik – beshta so‘z, eng katta (maksimal) uzunlik –32-razryadli so‘zlardan o‘n beshtasi.

Servis turi maydoni (Type of Service) xizmat ko‘rsatishning talab etiladigan sifat ko’rsatkichlarini ko‘rsatadi. Imtiyoz esa, har bir deytagrammaga imtiyoz kodini berish orqali paketlarni uzatilishida unga ustunliklar beradi.

<table>
<tr><td>Versiya
(Version)</td><td>4
Sarlovha uzunligi
(Header Length)</td><td>8
Servis (xizmat) turi
(Type of Service)</td><td colspan="2">16
Paketning to‘liq uzunligi
(Total Length)</td></tr>
<tr><td colspan="3">16
Umumiy identifikator
(Identification)</td><td>3
Bayroq
(Flag)</td><td>13
Fragmentli siljitish
(Fragment Offset)</td></tr>
<tr><td>8
Yashash vaqti
(TTL - Time To Live)</td><td>8
Protokol turi (Protocol)</td><td colspan="3">16
Sarlovhaning nazorat yig‘indisi
(Header Checksum)</td></tr>
<tr><td colspan="5">32 Jo‘natuvchining IP-manzili (manzili) (Source Address)</td></tr>
<tr><td colspan="5">32 Qabul qilib oluvchining IP-manzili (manzili)(Destination Address)</td></tr>
<tr><td colspan="4">IP ning yordamchi ko‘rsatkichlari
(IP opsiyalari) (Options)</td><td>To‘ldiruvchi (Padding)
(qo‘shimcha 32 bitgacha)</td></tr>
<tr><td colspan="5">Ma’lumotlar (Data) ...</td></tr>
</table>

3.1-rasm. IPv4 paket formati

Bitlar: 12 - D (delay) — kechikish, 13 - T (throughput) — samaradorlik (o‘tkazish qobiliyati), 14 - R (reliability) — ishonchlilik, S (cost) — narhi.

Paketning to‘liq uzunligi maydoni (Total Length) deytagrammaning sarlovha va foydali ish yuki bilan birga, oktet (bayt)lardagi umumiy uzunligini

belgilaydi. Paketning to‘liq uzunligi 65535 bayt (2^{16}-1=65 535)gacha yetishi mumkin.

Umumiy identifikator maydoni (Identification) - tarmoqlararo deytagrammalarning fragmentlarini yig‘ish uchun mo‘ljallangan.

Bayroq (Flag) maydoni deytagrammalarni fragmentatsiyalash imkoniyatini ta’minlaydi hamda fragmentatsiyadan foydalanishda deytagrammaning so‘nggi fragmentini identifikatsiyalash imkonini beradi. “Flaglar” maydonining 0 biti zahirada bo‘lib, 1 esa paketlarni fragmentatsiyasini boshqarish uchun xizmat qiladi (0 – fragmentatsiyalash ruxsat etiladi; 1 - ta’qiqlanadi), 2 biti mazkur fragment so‘nggisi yoki so‘nggisi emasligini aniqlaydi (0- so‘nggi fragment; 1 – davomini kutmoq lozim).

Fragmentli siljitish maydoni mazkur fragmentning deytagrammadagi o‘rnini ko‘rsatadi. Birinchi fragment nolga teng siljishga ega.

Qandaydir sabablar natijasida ushlab (kechiktirib) qolingan paketlarni tarmoqdan bartaraf etish uchun sarlovhadagi yashash vaqti maydonida paket tarmoqda mavjud bo‘lishi lozim bo‘lgan vaqt ko‘rsatiladi. Ushbu vaqt qiymati paketning tarmoq bo‘ylab qurilmalardan o‘tishi sayin kamayib boradi. U tamom bo‘lganida, jo‘natuvchi tegishli ICMP-xabar bilan xabardor qilingan holda, paket yo‘q qilinadi. Bunday chora tarmoqni siklik marshrutlardan va haddan tashqari ish bilan yuklashdan himoya qiladi.

Protokol turi (Protocol) maydoni foydalaniladigan yuqori sath (ICMP - 1, IGMP - 2, TCP - 6, UDP - 17) protokolini aniqlaydi.

Sarlovhaning nazorat yig‘indisi maydoni (Header Checksum). Paketning manzil qismi buzib ko‘rsatilish ehtimolini kamaytirish va uning natijasi – uning aynan manzilga yuborilmasligi (va yo‘qolishi)ni oldini olish uchun, sarlovha paketi 2 bayt o‘rin egallaydigan va butun sarlovha bo‘ylab hisoblanadigan tekshirish ketma-ketligi – nazorat yig‘indisi bilan yuboriladi.

Sarlovhada bo‘lgan IP-manzillar (jo‘natuvchining IP-manzili (Source Address) qabul qilib oluvchining IP-manzili (Destination Address)) tarmoq

ob’ektlari – so‘nggi ko‘rsatma va marshrutlashtiruvchilarning 32-bitlik identifikatorlari bo‘lib xizmat qiladi.

IPning yordamchi ko‘rsatkichlari maydoni (IP opsiyalari) (Options) – qo‘shimcha xizmatlar bor yoki yo‘qligini aniqlaydi. O‘zgaruvchan uzunlikka ega deytagrammada bo‘lishi yoki bo‘lmasligi mumkin.

To‘ldiruvchi maydon (Padding) sarlovhani 32-razryadli chegaraga moslashtirish (to‘g‘rilash) uchun qo‘llaniladi.

IP-manzillash asoslari. IP-manzil o‘nlik sonlarda ifoda etilgan, W.X.Y.Z shaklida nuqtalar bilan ajratilgan. Unda nuqtalar oktetlarni ajratish uchun foydalaniladigan (masalan, 10.0.0.1) noyob 4 oktetlik (32-bitlik) kattalikni o‘zida ifoda etadi. Manzilning 32 biti ikki qismdan iborat: tarmoq yoki aloqa manzili (o‘zida manzilning tarmoq qismini ifoda etuvchi) va xost manzili (tarmoq segmentida xostni identifikatsiyalovchi). Tarmoqlarni ulardagi xostlar soni bo‘yicha ajratish IP-manzillarni sinflarga ajratish asosida amalga oshiriladi.

IP-manzillarning 5 ta: A, B, C, D va E sinflari mavjud. Faqatgina A, B va C sinf manzillari noyob sinf sifatida foydalanilishi mumkin. D sinfiga oid manzillar qurilmalar to‘plamiga murojaat qilish uchun qo‘llanilad. “E” sinfiga oid manzillar esa tadqiqot olib borish maqsadida zahiralashtirilgan va hozirgi vaqtda ulardan foydalanilmaydi. Bundan tashqari barcha sinflardagi bir necha manzillar maxsus maqsadlar uchun zahiralashtirilgan.

“A” sinf manzillari. “A” sinf tarmoqlari manzildagi eng katta (chap) bitning 0 qiymati bilan aniqlanadi. Birinchi oktet (0 dan 7 gacha bitlar) manzildagi chap bitdan boshlanadi. Ushbu oktet tarmoqdagi tarmoqosti (tarmoqning ichidagi kichik tarmoq)lar sonini belgilaydi, ayni vaqtda qolgan uchta oktet (8 dan 31 ga qadar bitlar) tarmoqdagi xostlar sonini ifoda etadi. Misol uchun, tarmoqdagi A 124.0.0.1 sinfi manzilini olaylik. Bunda 124. - tarmoq manzilini ifoda etadi, manzil ohiridagi 0.0.1 esa, ushbu tarmoqdagi birinchi xostni anglatadi. “A” sinf manzillari yordamida, har bir tarmoqda faqatgina 16 777 214 (2^{24}-2) ta xostlarni ifoda etish mumkin.

“B” sinf manzillari. “B” sinf tarmoqlari manzilning katta bitlarida 10 qiymatlar bilan belgilanadi. Manzildagi birinchi ikkita oktet (0 dan 15 ga qadar bitlar) tarmoq manzillarini ifoda etish uchun xizmat qiladi, qolgan ikkita oktet esa, ushbu tarmoqlardagi xost raqamlarini ifoda etadi. 16384 ta tarmoqning har birida 65534 ta xostga ega bo’lamiz. Misol uchun, “B” sinfi manzilidagi 172.16.0.1, tarmoq manzili - 172.16, xost raqami - 0.1.

“*C” sinf manzillari.* “C” sinf tarmoqlari manzildagi katta bitlar 110 qiymatlari bilan aniqlanadi. Birinchi uchta oktet (bitlar 0 dan 23 ga qadar) tarmoq raqamlarini ifoda etish uchun foydalaniladi, so‘nggi oktet esa (bitlar 24 dan 31 ga qadar) tarmoqdagi xostlar raqamini o‘zida ifoda etadi. Shunday qilib, 2 097 152 ta tarmoqqa ega bo‘lamiz. Ularning har birida 254 ta xost bo‘ladi. Misol uchun C sinfi tarmog‘idagi 192.11.2.1 manzilni olaylik. Undagi 192.11.2 tarmoq manzilini o‘zida ifoda etadi. Tarmoqdagi xostning raqami esa – 1.

“D” sinf manzillari. “D” sinf tarmoqlari IP – manzilning birinchi to‘rtta bitlarida 1110 qiymatlari bilan belgilanadi. “D” sinfining manzil kengligi qurilmalar to‘plamini manzillash uchun foydalanuvchi, guruhli IP – manzillarni ifoda etish uchun zahiralashtirilgan. Bu mazkur paketning manzil maydonida ko‘rsatilgan raqam bilan guruhni tashkil etuvchi bir nechta qurilmalarga darhol yetkazilish lozimligini anglatadi.

“E” sinf manzillari. “E” sinf tarmoqlari IP – manzilning katta to‘rtta bitlarida 1111 qiymatlari bilan belgilanadi. Hozirgi vaqtda ushbu diapazon manzillaridan foydalanilmaydi. Ular tajriba maqsadlari uchun zahiralashtirilgan.

Kichik tarmoq (Tarmoqosti)larni manzillash. “A” sinfi, “B” sinfi va “C” sinfi tarmoqlaridagi xost raqamlari singari, tarmoqosti manzillari lokal ravishda beriladi. Boshqa IP – manzillari singari, kichik tarmoqlarning har bir manzili noyobdir.

IPv6 protokoli

IPv6 4-versiyaning vorisi bo‘lgan Internet protokolining yangi versiyasini ifoda etadi. IPv4 ga nisbatan IPv6 dagi o‘zgarishlarni quyidagi guruhlarga ajratish mumkin:

- *manzillashning kengayishi*. IPv6 da manzil uzunligi 128 bitgacha kengaytirilgan (IPv4 da 32 bit). Bu esa manzillash ierarxiyasining ko‘proq pog‘onalarini ta’minlash, manzillashtiriladigan qurilmalar sonini oshirish, avto-konfiguratsiyani soddalashtirish imkonini beradi. Multikasting-marshrutlashtirish imkoniyatlarini kengaytirish uchun manzil maydoniga “scope” (manzillar guruhi) kiritilgan. Manzilning yangi “anycast address” turi aniqlangan. U mijoz so‘rovlarini serverning istalgan guruhiga yuborish uchun foydalaniladi. Anycast manzillash o‘zaro xarakat qiluvchi serverlar to‘plamidan foydalanish uchun mo‘ljallangan bo‘lib, ularning manzillari mijozga oldindan ma’lum bo‘lmaydi;

- *qo‘shimcha opsiyalar*. IP-sarlovhalarning opsiyalari kodlashtirilishining o‘zgartirilishi paketlarni qayta manzillashtirilishini yengillashtirish imkonini beradi. Opsiyalar uzunligiga bo‘lgan cheklovlarni kamaytiradi va kelajakda qo‘shimcha opsiyalar kiritilishini yanada ochiqroq qiladi;

- *ma’lumot oqimlariga belgilar qo‘yish imkoniyati*. Muayyan transport oqimlariga tegishli bo‘lgan, ular uchun jo‘natuvchi qayta ishlashning muayyan tartibini so‘ragan paketlarga belgi qo‘yish imkoniyati. Masalan TOS (xizmatlar turi)ning nostandart turi yoki ma’lumotlarga vaqtning real tizimida qayta ishlash joriy qilindi;

- xususiy almashishlarni identifikatsiyalash va himoyalash. IPv6 da ma’lumotlarning yaxlitligini va istalganda xususiy ma’lumotni himoyalash uchun tarmoq ob’ektlarida yoki sub’ektlarida identifikatsiyalash tasnifi joriy qilingan.

IPv6 paket formati

Quyidagi 3.2-rasmda IPv6 sarlovhasining formati aks ettirilgan.

<table>
<tr><td>4
Versiyalar</td><td>4
Imtiyoz</td><td colspan="2">24
Oqim belgisi</td></tr>
<tr><td colspan="2">16
Ma’lumotlar o‘lchami</td><td>8
Keyingi
sarlovha</td><td>8
Qadamlarning
cheklangan soni</td></tr>
<tr><td colspan="4">128
Jo‘natuvchining manzili</td></tr>
<tr><td colspan="4">128
Qabul qiluvchining manzili</td></tr>
<tr><td colspan="4">Ma’lumotlar (Data)
...</td></tr>
</table>

3.2-rasm. IPv6 paketining formati

“Versiya” maydoni Internet protokoli versiyasining 4 bitlik kod raqami. Imtiyozning 4 bitlik “Imtiyoz” maydoni IPv6 sarlovhasida jo‘natuvchiga paketlarni yetkazishning nisbiy ustuvorligini identifikatsiyalash imkonini beradi. Imtiyozlarning qiymatlari ikki diapazonga bo‘linadi. 0 dan 7 gacha kodlar trafik ustuvorligini berish uchun foydalaniladi. U uchun jo‘natuvchi ortiqcha yuklanish ustidan nazoratii amalga oshiradi (misol uchun, ortiqcha yuklanish signaliga javoban TCP oqimini pasaytiradi). 8 dan 15 gacha bo‘lgan qiymatlar trafik ustuvorligini aniqlash uchun foydalaniladi. U uchun ortiqcha yuklanish signaliga javoban oqimni pasaytirish amalga oshirilmaydi. Misol uchun, doimiy (turg‘un) chastota bilan yuboriladigan “real vaqt” paketlari ko’rinishida.

“Oqim belgisi” – oqim belgisining 24 bitlik kod maydoni IPv6 sarlovhasida jo‘natuvchi tomonidan paketlarni ajratish uchun foydalanilishi mumkin. Ular uchun marshrutlashtiruvchida maxsus qayta ishlash talab etilmaydi. Misol uchun, nostandart QoS yoki “real-time” xizmati kabi.

Ma’lumotlar o‘lchami - belgisiz 16 bitlik son. O‘zida ma’lumotlar

maydonining oktetlardagi uzunlik kodini tashiydi va u paket sarlovhasidan so‘ng keladi. Agar kod 0 ga teng bo‘lsa, u holda ma’lumotlar maydoni uzunligi jumboq ma’lumotlar maydonida yozilgan bo‘ladi va u o‘z navbatida opsiyalar zonasida saqlanadi.

Keyingi sarlovha – 2 bitlik ajratuvchi. IPv6 sarlovhadan keyin bevosita keluvchi sarlovha turini identifikatsiyalaydi. IPv4 protokoli ishlatadigan qiymatlardan foydalanadi.

Qadamlarning chegaralangan soni (paketning maksimal yashash vaqti) – 8 bitlik belgisiz butun son. Paket o‘tuvchi har bir qurilmada bittaga kamayadi. Qadamlar nolga teng bo‘lganda paket yo‘q qilinadi.

IPv4 dan farqli o‘laroq, IPv6 qurilmalari paketlarning maksimal yashash vaqtini belgilanishini talab etmaydi. Shu sababli IPv4 “time to live” (TTL) maydoni IPv6 uchun “hop limit” – qadamlarning chegaralangan soni deb nomlangan. Amaliyotda unchalik ko‘p bo‘lmagan IPv4 ilovalar TTL bo‘yicha cheklovlardan foydalanadilar.

“Jo‘natuvchi manzili” va “Qabul qiluvchining manzili” maydonlariga manzil uzunligi IPv4 ga nisbatan uzun bo‘lganligi uchun 128 bit ajratilgan.

IPv6 versiyasida manzillash va manzillar yozuvlarini taqdim etish arxitekturasi

Manzillarning uchta turi mavjud:

Unicast: Birlik interfeys identifikatori. Unicast manzildan yuborilgan paket manzilda ko‘rsatilgan interfeysga yetkaziladi.

Anycast: turli qurilmalarga tegishli bo‘lgan interfeyslar to‘plamini identifikatsiyalovchi. Anycast manzildan yuborilgan paket manzilda ko‘rsatilgan interfeyslardan biriga yetkaziladi (marshrutlashtirish protokolida belgilanganlardan eng yaqini).

Multicast: Turli qurilmalarga tegishli bo‘lgan interfeyslar to‘plamini identifikatsiyalovchi. Multicast manzil bo‘yicha yuborilgan paket ushbu manzil

tomonidan berilgan barcha interfeyslarga yetkaziladi.

IPv6 da keng ravishda oldindan xabar beruvchi manzillar mavjud emas. Ularning funksiyalari multikast manzillarga o‘tkazilgan.

IPv6 manzillarini matn satrlari ko‘rinishida ifoda etishning uchta standart shakllari mavjud:

1. Asosiy shakli x: x: x: x: x: x: x: x ko‘rinishiga ega. Bunda “x” – 16 bitlik – o‘n oltilik sonlar.

Misollar:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200S:417A

E’tibor qiling, har bir muayyan maydonlarda boshlang‘ich nollarni yozishga hojat yo‘q, biroq har bir maydonda hech bo‘lmaganda bitta raqam bo‘lishi lozim (2-bandda bayon etilgan xolatdan tashqari).

2. IPv6 manzillari ayrim turlarida ko‘pincha o‘zlarida nolli bitlarning uzun ketma-ketligini mujassamlashtiradi. Nol bitlik manzillar yozuvini qulayroq qilish uchun, ortiqcha nollarni olib tashlash uchun maxsus sintaksis nazarda tutilgan. « :: » yozuvidan foydalanish 16 ta nollik bitlardan iborat guruhlar borligiga ishora qiladi. « :: » kombinatsiyasi faqatgina manzil yozilishida paydo bo‘lishi mumkin. «::» ketma-ketligi shuningdek yozuvdan manzildagi boshlang‘ich va yakunlovchi nollarni olib tashlash uchun foydalanilishi mumkin. Masalan:

1080:0:0:0:8:800:200S:417A	unicast manzil
FF01:0:0:0:0:0:0:43	multicast manzil
0:0:0:0:0:0:0:1	teskari aloqa manzili

quyidagi ko‘rinishda ifoda etilishi mumkin:

1080::8:800:200S:417A	unicast manzil
FF01::43	multicast manzil
:: 1	teskari aloqa manzili

3. IPv4 va IPv6 larda ishlash uchun qulayroq bo‘lgan yozuvning muqobil shakli bo‘lib x:x:x:x:x:x:d.d.d.d xizmat qiladi, bunda “x” – manzilning o‘n oltinchilik 16 bitlik kodlari, “d” esa – manzilning kichik qismini tashkil etuvchi

o‘nlik 8 bitlik kodlari (standart IPv4 ifodasi), Misol uchun:

0:0:0:0:0:0:13.1.68.3 (siqilgan ko‘rinishda ::13.1.68.3)

0:0:0:0:0:FFFF:129.144.52.38 (siqilgan ko‘rinishda ::FFFF:129.144.52.38)

Jadvaldan ko‘rinib turibdiki bu ikki protokol bir-biri bilan solishtirilganda ustunlik va kamchiliklari bor. IPv6 protokolida xavfsizlik choralari ko‘rilgani, ya’ni IPSec protokolini ishini osonlashtirish uchun qo‘shimcha maydon qo‘shilganligi, ma’lumotlarni yetib borishi sifati va ishonchliligi, IPv6 asosidagi qurilgan tarmoqning sodda arxitekturaga ega bo‘lishi, ya’ni NAT – tarmoq manzillarini ishlatmagan holda end-to-end asosida ishlashni tashkil etgani uchun ham bu protokolga o‘tish eng to‘g‘ri yechimdek ko‘rinishi mumkin. Ammo, hozirdagi ko‘plab tarmoq qurilmalarining IPv6 protokolini qo‘llab quvvatlamasligi, ko‘plab kontent ma’lumotlardan IPv6 orqali foydalanish ilojsiz bo‘lgani, qurilmalarni yangilash uchun esa katta xarajat va vaqt talab etilishi bu protokolni qo‘llashda ko‘plab qiyinchiliklarni keltirib chiqarmoqda.

Hozirda IPv4 manzillari qolmagani va keyingi ulanayotgan yangi foydalanuvchilarni faqat IPv6 orqali manzillash mumkin bo‘lganligi, IPv6 protokoliga o‘tish muqarrarligini anglatadi.

3.2. Marshrutizatsiya protokollari

TCP/IP stekining yo‘nalish axborotlari bilan almashishning hamma protokollari adaptiv protokollar sinfiga kiradi. Ular o‘z navbatida ikki guruhga bo‘lingan, ularning har biri quyidagi algoritmlar turi bilan bog‘langan:

- *masofa-vektor algoritmi* (Distance Vector Algorithms, DVA);
- *aloqa xolati algoritmi* (Link State Algorithms, LSA).

Masofa-vektor turidagi algoritmlarda marshrutizator vaqti-vaqti bilan va keng ogox qilingan holda tarmoq bo‘yicha o‘zidan to unga ma’lum bo‘lgan tarmoqlarga masofa vektorini yuboradi. Masofa deganda odatda paket muvofiq tarmoqqa tushishdan oldin nechta oraliq marshrutizatorlar orqali o‘tishi tushiniladi. Nafaqat paket o‘tgan oraliq nuqtalar, u qo‘shni marshrutizatorlar orasida aloqa

bo‘yicha o‘tgan vaqtini ham hisobga oluvchi boshqa metrika ham ishlatiladi. Qo‘shni marshrutizatordan vektorni qabul qilib har bir marshrutizator o‘zi bevosita (agar tarmoqlar uning portiga ulangan bo‘lsa) yoki qo‘shni marshrutizatorlarning o‘xshash elementlaridan bilib olgan unga ma’lum boshqa tarmoqlar to‘g‘risida axborotni vektorga qo‘shadi va tarmoq bo‘yicha vektorning yangi mazmunini jo‘natadi, oxir oqibat har bir marshrutizator inter tarmoqdagi tarmoqlar va qo‘shni marshrutizatorlar orqali ularga bo‘lgan masofa to‘g‘risida axborotni bilib oladi.

Masofa-vektor algoritmlari uncha katta bo‘lmagan tarmoqlardagina yaxshi ishlaydi. Katta tarmoqlarda ular intensiv keng ogoxlantirish trafigi bilan aloqa liniyalarini sifatsiz qiladilar. Bundan tashqari bu algoritm konfiguratsiyaning o‘zgarishi har doim ham to‘g‘ri bajarilmaydi, chunki marshrutizatorlar tarmoqdagi aloqalar topologiyasi aniq tushunchaga ega emaslar, ular faqat vositachilar orqali olingan, umumlashgan axborotga – masofa-vektoriga egalar. Masofa-vektori protokoliga muvofiq marshrutizator ishi ko‘prik ishini eslatadi, chunki bunday marshrutizator tarmoqning aniq topologik sur’atiga ega emas.

Masofa – vektori algoritmi asosidagi eng ko‘p tarqalgan protokol bo‘lib, RIP protokoli hisoblanadi.

Aloqa xolatining algoritmi, har bir marshrutizatorni tarmoq aloqalarining aniq grafasini qurish uchun yetarli axborot bilan ta’minlaydi. Hamma marshrutizatorlar bir xil graflar asosida ishlaydi, bu marshrutlash jarayonini konfiguratsiyasi o‘zgarishiga mustaxkamliroq qiladi. Keng ogoxlantirishli jo‘natmalar faqat aloqalar xolatining o‘zgarishidagina ishlatiladi, bunday xolat ishonchli tarmoqlarda kam uchraydi. Aloqa liniyalar xolatini qandayligini tushunish uchun uning portlariga ulangan marshrutizator o‘zining yaqin qo‘shnilari bilan kalta paketlarni vaqti-vaqti bilan almashib turadi. Ushbu grafik ham keng ogohlantiruvchi, lekin u qo‘shnilar orasida bo‘lganligi sababli tarmoqni kamroq sifatsizlantiradi.

TCP/IP stekida aloqalar xolatining algoritmi asosidagi protokol bo‘lib, OSPF protokoli hisoblanadi.

RIP masofa-vektor protokoli

RIP (Routing Information Protocol) protokolida hamma tarmoqlar raqamga ega (raqam tashkil bo‘lish usuli, tarmoqda tarmoq pog‘onasining protokolini ishlatilishiga bog‘liq), marshrutizatorlar esa, identifikatorlarga ega. RIP protokoli keng “Masofa vektori” tushunchasini ishlatadi. Masofa vektori, bu tarmoq raqamlari va uchastkalarida qadam (xop)larga bo‘lgan masofani hisoblovchi ikki juft son.

Masofa vektori marshrutizatorlar tomonidan tarmoq bo‘yicha tarqatiladi va bir necha qadamdan keyin har bir marshrutizator yetishadigan tarmoq va unga bo‘lgan masofa to‘g‘risidagi ma’lumotlarga ega bo‘ladi. Agar qaysidir tarmoq bilan aloqa uzilsa, marshrutizator bu xolatni belgilab, vektor elementiga ushbu tarmoqqacha bo‘lgan masofaga, “Aloqa yo‘q” maxsus ya’ni, maksimal belgi qo‘yadi. RIP protokolida bu belgi 16 son hisoblanadi.

Aloqaning xolatiga va qurulmalarni o‘zgarishiga moslashish uchun marshrutlash jadvalining har bir yozuviga taymer ulanadi. Agar taym-out davrida ushbu yo‘nalishni tasdiqlovchi xabar kelmasa, unda u yo‘nalish jadvalidan olib tashlanadi. RIP protokolidan foydalanilganda Bellman-Ford dinamik dasturlashining evristik algoritmi ishlaydi va uning yordamida topilgan yechim optimalga yaqin hisoblanadi.

RIP protokolining ustunligi, uning hisoblashdagi oddiyligi, kamchiligi esa keng ogohlantiruvchi paketlarni vaqti-vaqti bilan jo‘natadi va topilgan yo‘nalish optimal ekanligi hisoblanadi.

OSPF aloqa xolati protokoli

OSPF protokoli quyidagi xususiyatlarga ega:

- sinfsizlik-protokol sinfsiz ishlab chiqilgan. Shuningdek u VLSM ni ishlatish va CIDR marshrutizatsiyasida ishlaydi;

- samaradorlik-marshrutda o‘zgarish bo‘lsa marshrutizatsiyani yangilash (doimiy bo‘lmagan yangilanish)ni ishga tushiradi. Protokol optimal yo‘lni to‘plash uchun SPF qisqa yo‘lni izlash algaritmini ishlatadi;

- tez bir xillikka erishish-tarmoq o‘zgarganligini tez translyatsiya qilish;

- masshtablik – kichik va katta tarmoqqa ishlatishga mo‘ljallangan. Ierarxik tuzilishni qo‘llab quvvatlash uchun marshrutizatorni bitta maydon (area)ga guruhlash mumkin;

- xavfsizlik - MD5 Message Digest autentifikatsiyasini qo‘llab quvvatlaydi. Agar bu funksiya yoqilgan bo‘lsa, OSPF marshrutizatorlar oldindan berilgan bir xil parolli teng huquqli qurilmadan marshrutizatsiyaning faqat shifrlangan xabarlarini qabul qiladi.

Administratoriy masofa (Administrative distance (AD)) (MM)- marshrut manbasining ishonchlilik qiymatini ko‘rsatadi. OSPF protokolining MMsi 110 ga teng.

Hamma marshrutizatsiya protokollari o‘xshash komponentlarni ishlatadi. Hamma protokollar marshrutizatsiyaning ma’lumotlarini almashish uchun marshrutizatsiya protokolining xabarini ishlatadi. Xabar marshrutizatsiya algoritmi yordamida qayta ishlashini ta’minlovchi ma’lumotlar tuzilishini qurishga yordam beradi.

OSPF marshrutizatsiya protokolining 3 ta (3.1 - jadval) asosiy komponenti mavjud.

1) Ma’lumotlarning tuzilishi.

OSPF protokoli 3 ta ma’lumotlar bazasini yaratadi va xizmat ko‘rsatadi:

- qo‘shni qurilmalar to‘g‘risida ma’lumotlar bazasi-qo‘shni qurilmalarning jadvalini yaratadi;

- kanal xolati to‘g‘risida ma’lumotlar bazasi (LSDB) - topologiya to‘g‘risida jadval yaratadi;

- jo‘natmalarning ma’lumotlar bazasi- marshrutizatsiya jadvalini yaratadi.

Bu jadvallar marshrutizatorlar o‘rtasida ma’lumotlar almashishini bajaruvchi qo‘shni murshrutizatorlar ro‘yxatidan iborat.

2) Marshrutizatsiya protokolining xabari.

OSPF protokoli marshrutizatsiya ma’lumotlarini uzatish uchun xabarlarni almashishda 5 ta turdagi paketni ishlatadi.

- salomlashish paketi (hello);
- ma’lumotlar bazasini tavsiflovchi paket;
- kanal xolati paketi;
- kanal xolatini yangilash paketi;
- kanal xolatini tasdiqlash paketi.

Bu paketlar qo‘shni marshrutizatorlarni aniqlash uchun va tarmoq to‘g‘risida aniq ma’lumotga ega bo‘lish maqsadida marshrutizatsiya ma’lumotlarini almashish uchun ishlatiladi.

3) Algoritm.

Markaziy protsessor Deykstra qisqa yo‘lni izlash algoritmini ishlatgan holda topologiya jadvali va qo‘shni qurilmalar jadvalini qayta ishlaydi. Qisqa yo‘lni izlash algoritmi ko‘rsatilgan joyga barcha kirishlarni narhi to‘g‘risidagi ma’lumotga asoslanadi.

Qisqa yo‘lni izlash algoritmi SPF qisqa yo‘llar daraxtini har bir marshurtizatorni daraxtning ildiziga joylashtirish orqali yaratadi va har bir qurilmaga qisqa yo‘llarni hisoblaydi. Shundan keyin SPF qisqa yo‘llar daraxti optimal marshurtni hisoblash uchun ishlatiladi. OSPF protokoli marshrutizatsiya jadvalini yaratish uchun qo‘llaniluvchi jo‘natmalarni ma’lumotlar bazasiga optimal marshrutni tanlash uchun kiritadi.

OSPF protokolini ishlatuvchi marshrutizatorlar marshrutizatsiya ma’lumotlarini taqdim etishda marshrutizatorlar bir xil marshrutizatsiya jadvaliga ega bo‘lish uchun kanal xolati bo‘yicha marshrutizatsiya jarayonining quyidagi 5 ta qadamini bajaradi:

3.1 – jadval.

OSPF ma’lumotlarni tuzilishi

Ma’lumotlar bazasi	**Jadval**	**Tavsifi**
Qo‘shnilar bo‘yicha ma’lumotlar bazasi	Qo‘shni qurilmalar jadvali	- 2 tomonlama ma’lumot almashish o‘rnatilgan barcha qo‘shni marshrutizatorlar ro‘yxati; - har bir marshrutizator uchun alohida jadval mavjud; - jadvalni **show ip ospf neighbor** buyrug‘i yordamida ko‘rish mumkin.
Kanalni xolati bo‘yicha ma’lumotlar bazasi	Topologiya jadvali	-tarmoqdagi barcha marshrutizatorlar to‘g‘risida ma’lumotlarni yig‘adi; -bu ma’lumotlar bazasi tarmoqning topologiyasini ko‘rsatadi; - bir maydonda bo‘lgan barcha marshrutizatorlar bir xil kanalni xolati bo‘yicha ma’lumotlar bazasini ishlatadi; -jadvalni **show ip ospf database** buyrug‘i yordamida ko‘rish mumkin.
Jo‘natmalarning ma’lumotlar bazasi	Marshrutizatsiya jadvali	-kanalni xolati bo‘yicha ma’lumotlar bazasidagi algoritmni ishga tushishi orqali yaratilgan marshrutlar to‘g‘risida ma’lumotlarni yig‘adi;

3.1 – jadval davomi

		-har bir marshrutizator boshqa marshrutizatorlarga paketlarni jo‘natish joyi va usuli to‘g‘risidagi ma’lumotlarga ega bo‘lgan marshrutizatsiya jadvalini ishlatadi; -bu ma’lumotlarni **show ip route bo‘yrug‘i** yordamida ko‘rish mumkin.

1. Qo‘shni qurilmalar bilan qo‘shnichilik munosabatlarini o‘rnatish OSPFni ishlatuvchi marshrutizator ma’lumotlarni almashish uchun tarmoqdan bir-birini aniqlashni bajarishi kerak. OSPFni ishlatuvchi marshrutizator OSPF yoqilgan barcha interfeyslaridan salomlashish paketini ushbu interfeyslar chegarasida qo‘shni qurilmalarni aniqlash uchun jo‘natadi. Qo‘shni qurilma mavjud bo‘lganda OSPFni ishlatuvchi marshrutizator u bilan bir xillik munosabatini o‘rnatishga harakat qiladi.

2. Kanal xolati to‘g‘risida xabarlarni almashish. Bir xillik munosabati o‘rnatilgandan keyin marshrutizatorlar kanal xolati to‘g‘risidagi (LSA) xabarlarni almashadi. LSA har bir to‘g‘ridan - to‘g‘ri ulangan kanalning xolati va narhi to‘g‘risidagi ma’lumotga ega. Marshrutizatorlar o‘zining LSA xabarlarini qo‘shni qurilmalarga jo‘natadi. Qo‘shni qurilmalar LSA xabarlarini olishi bilan o‘zining LSA xabarini to‘g‘ridan to‘g‘ri ulangan qo‘shnilarga jo‘natadi va bu jarayon bir maydondagi barcha marshrutizatorlar barcha LSA xabarlarni qabul qilib olguncha davom etadi.

3. Topologiya jadvalini yaratish. OSPFni ishlatuvchi marshurtizatorlar kanal xolati to‘g‘risidagi xabarni olgandan keyin qabul qilingan paketlar asosida topologiya to‘g‘risidagi ma’lumotlar bazasini yaratadi. Bu ma’lumotlar bazasida ohir oqibat tarmoqning topologiyasi to‘g‘risida barcha axborotlar yig‘iladi.

4. SPF qisqa yo‘lni izlash algoritmini bajarilishi. Shundan keyin marshrutizatorlar qisqa yo‘lni izlash algoritmini bajarishga tushishadi.

Katta samaradorlikni va masshtablikni ta’minlash uchun OSPF protokoli maydonlarga bo‘lingan ierarxik marshrutizatsiyani quvvatlaydi. OSPF maydoni kanal xolati bo‘yicha tuzilgan ma’lumotlar bazasidagi kanal xolati to‘g‘risidagi bir xil ma’lumotlarni ishlatuvchi marshrutizatorlar guruhidan iborat.

OSPF protokolini quyidagi usullardan birida ishlatish mumkin:

- bitta maydon uchun OSPF. Magistral yoki nol maydon deb nomlanuvchi bitta maydonda joylashgan (0 maydon).
- bir nechta maydonlar uchun OSPF. OSPF protokoli ierarxik tartibda bir nechta maydonlar yordamida ishlatiladi. Barcha maydonlar magistral maydonga (0 maydon) ulanishi shart. Maydonlar orasida ulanishni amalga oshiruvchi marshrutizatorlar chegaraviy marshrutizatorlar deyiladi (AVR).

OSPFda bir nechta maydonlar uchun ierarxik marshrutizatsiyani ta’minlash maqsadida bitta katta avtanom tizimi (AT)ni bir nechta kichik maydonlarga bo‘lish mumkin. Ierarxik marshrutizatsiyani ishlatishda maydonlar o‘rtasida (maydonlararo marshrutizatsiya) marshrutizatsiya bajariladi. Protsessorning resurslari (M: ma’lumotlar bazasi takroriy hisoblash)ni talab qiluvchi marshrutizatsiya jarayonlarining ko‘pchiligi bitta maydon doirasida bajariladi.

Har doim marshrutizator bitta maydon doirasida topologiyada o‘zgarish to‘g‘risida yangi ma’lumotni qabul qilsa, marshrutizator qisqa yo‘lni izlash algoritmini bajarishi, yangi SPF qisqa yo‘l daraxtini yaratishi va marshrutizatsiya jadvalini yangilashi kerak. Qisqa yo‘lni izlash algoritmi mikroprotsessorning katta hajmdagi resursni talab qiladi, ya’ni resurs bu hisoblashga ketadigan vaqt maydonini o‘lchamiga bog‘liq bo‘ladi.

Izoh: topologiyaning o‘zgarishi boshqa maydondagi marshrutizatorlar

o‘rtasida masofa vektor formatida qayta taqsimlanadi. Boshqacha aytganda bu marshrutizatorlar faqat marshrutizatsiya jadvalini yangilaydi va qaytadan qisqa yo‘lni izlash algoritmini bajarmasligi kerak.

Bitta maydondan juda ko‘p marshrutizatorlar bo‘lsa kanal xolati to‘g‘risidagi ma’lumotlar bazasi juda katta hajmga ega bo‘ladi va mikroprotsessorning yuklanishi ortadi. Shuning uchun mashrutizatorlarni maydonlarga taqsimlashdan katta ma’lumotlar bazasini kichik ma’lumotlar bazasiga samarali taqsimlash kerak. Bunda samarali boshqarish imkoniyatini ta’minlashga e’tibor qilish lozim.

3.3. ICMP boshqarish xabarlari bilan almashish protokoli

Marshrutizator qurilmadan kelgan bironta IP paketini uzatishda duch kelgan xatolar to‘g‘risida xabar berishga imkon beradi. Shuni aytish kerakki, ICMP (Internet Control Message Protocol) protokoli – bu xatolar to‘g‘risida xabar beruvchi, lekin xatolarni tuzatuvchi protokol emas. ICMP protokolining har bir xabari tarmoq bo‘ylab, IP paket ichida uzatiladi. ICMP xabarlari imtiyozsiz marshrutlanadi. Shuning uchun ular ham yo‘qolishi mumkin. Bundan tashqari, yuklangan tarmoqda, ular marshrutizatorlarning qo‘shimcha yuklanishini keltirib chiqarishi mumkin. Xatolar to‘g‘risida juda ko‘p xabarlar keltirib chiqarmasligi uchun xatolar to‘g‘risidagi ICMP xabarlarni tashuvchi IP paketlarning yo‘qolishi, ICMPning yangi xabarlarini paydo qilmasligi kerak.

ICMP xabarlarining bir nechta turi mavjud (3.2 - jadval). Xabarning har bir turi o‘z formatiga ega va ularning hammasi uchta umumiy maydondan boshlanadi: xabar turini (TYPE), u xabarni belgilanishini aniqlab beradi, belgilovchi 8 bitli to‘la son, 8 bitli kod maydoni (CODE), u xabarning belgilanishini aniqlab beradi, nazorat yig‘indisini 16 bitli maydoni (CHECKSUM). Bundan tashqari ICMP xabari har doim sarlovha va xatoni keltirib chiqargan IP paketning birinchi 64 biti ma’lumotlarga ega. Bu qurilma-yuboruvchi xato sababini aniqroq taxlil qilishi uchun bajariladi, chunki TCP/IP steki – qo‘shma pog‘onasidagi hamma protokollar

o‘z xabarlarining birinchi 64 bitini taxlil qilish uchun eng muhim axborotga egalar. Maydon turi quyidagi belgilanishga ega (3.2 – jadval):

3.2 – jadval.

Maydon turi

Belgilanishi	Xabarlar turi
0	Aks-sado-javob (Echo Replay)
3	Yetib bo‘lmaydigan belgilangan qurilma (Destination Unreachable)
4	Manbani yo‘qotish (Source Quench)
5	Yo‘nalishni o‘zgartirish (Redirect)
8	Aks-so‘rov (Echo Request)
11	Deytagramma vaqtining tugashi (Time Exceeded for a Datagram)
12	Paket ko’rsatkichining muammosi. (Parameter Problem on a datagram)
13	Vaqt belgisini talab qilish (Timestamp request)
14	Vaqt belgisining javobi (Timestamp Replay)
17	Manzilni talab qilish (Address Mask Request)
18	Manzil javobi (Address Mask Replay)

Ko‘rinib turibdiki, ishlatilayotgan xabar turlaridan ICMP protokoli tor masalalarini xal qiluvchi protokollar birlashmasi bo‘lib hisoblanadi.

Xabar turlarini taxlil qilib chiqamiz (3.3-jadval).

Aks sado – protokoli. ICMP protokoli tarmoq qurilmalariga erishishni nazoratlash uchun tarmoq administratorlariga vositalar taqdim etadi. Bu vositalarni xabarning ikki turi bilan almashishni kirituvchi aks-protokol: aks - so‘rov va aks - javob shaklida tasavvur etish mumkin. Kompyuter yoki marshrutizator inter tarmoq bo‘yicha aks - so‘rov yuboradi, unda qurilmaning IP manzili ko‘rsatiladi. AKS - SO‘ROV olgan qurilma aks - javobni tashkil qiladi va talab yuboruvchiga-qurilmaga xabarni qaytaradi. Talabda bo‘lgan ayrim ma’lumotlar, javobda

qaytarilishi kerak. Chunki aks - so‘rov va aks - javob tarmoq bo‘yicha IP paketlar ichida uzatiladi va ularni muvoffaqiyatli yetkazib berish, inter tarmoqni butun transport tizimining normal ishlashini bildiradi.

Belgilangan qurilmaga yetib bora olmaslik to‘g‘risida ma’lumotlar. Marshrutizator IP paketni yubormasa yoki yetkazib bera olmasa, u paketni yuboruvchi qurilmaga “Yetib bo‘lmaydigan belgilangan qurilma” (3-xabar turi) xabarini yuboradi. Bu xabar kod maydonida, paket nima uchun yetkazib berilmaslik sababini aniqlovchi mazmunga ega. Sabab quyidagicha kodlanadi.

3.3 – jadval.

ICMP protokolining xabarlari

Kod	Sabab
0	Tarmoqqa yetishib bo‘lmaydi
1	Qurilmaga yetishib bo‘lmaydi
2	Protokolga yetishib bo‘lmaydi
3	Portga yetishib bo‘lmaydi
4	Fragmentatsiya talab etiladi, 2F bit esa o‘rnatilgan
5	Manba bergan yo‘nalishda xato
6	Tayinlash tarmog‘i noma’lum
7	Tayinlash qurilmasi noma’lum
8	Qurilma-manbaga ajratish
9	Tayinlangan tarmoq bilan o‘zaro ishlash administratoriy ta’qiqlangan
10	Tayinlangan qurilma bilan o‘zaro ishlash administratoriy taqiqlangan
11	Servisning berilgan sinfi uchun tarmoqqa erishib bo‘lmaydi
12	Servisning berilgan sinfi uchun qurilmaga erishib bo‘lmaydi

Marshrutizator qandaydir sabab bilan tarmoq bo‘yicha 10- paketni uzata olmasligini aniqlasa, qurilma manbaga ICMP xabarini yuboradi va keyin paketni olib tashlaydi. Xato sababidan tashqari ICMP xabari yetkazib berilmagan paket

sarlovhasini va ma’lumotlar maydonining birinchi 64 bitini ham kiritadi. Tayinlash tarmog‘i yoki qurilmaga apparaturaning vaqtincha ishdan chiqishi, yuboruvchi belgilangan manzil noto‘g‘ri ko‘rsatkichga hamda marshrutizator belgilangan tarmoqqa yo‘nalishi to‘g‘risida ma’lumotga ega bo‘lmaganda erishilmasligi mumkin. Protokol va portga erishilmaslik tayinlash qurilmasidagi qo‘shma pog‘onaning qaysi bir protokolida amalga oshishishi UDP yoki TCP protokollarining ochiq porti yo‘qligi orqali bildiradi.

Yo‘nalishni boshqa tomonga yo‘naltirish. Kompyuterlarda yo‘nalish jadvallari odatda statik hisoblanadi, chunki tarmoq administratori tomonidan konfiguratsiyalanadi, marshrutizatorlarda esa dinamik hisoblanadi, chunki yo‘nalish axborotlari bilan almashish protokollari yordamida avtomatik tarzda shakllanadi. Shuning uchun vaqt o‘tishi bilan, tarmoq topologiyasi o‘zgarganda kompyuterlarning yo‘nalish jadvallari eskirishi mumkin. Bundan tashqari bu jadvallar odatda kam axborotga ega, masalan, faqat bir nechta marshrutizatorlarning manzili.

Kompyuterlar xatti-xarakatini tuzatish uchun marshrutizator “yo‘nalishni boshqa tomonga yo‘naltirish” (Redirect) deb nomlanuvchi ICMP protokolining xabarini ishlatishi mumkin.

ICMP protokolini boshqa tomonga yo‘naltirish mexanizmi, kompyuterlarga uning lokal marshrutizatorlarining faqat IP-manzillarini konfiguratsiya fayllarida asrashga imkon beradi. Boshqa tomonga yo‘naltirish xabarlari yordamida marshrutizatorlar kompyuterga, qaysi marshrutizatorga u yoki bu tayinlangan tarmoq uchun paketlarni jo‘natish zarurligi to‘g‘risida unga kerakli axborotni xabar qilib turadi, ya’ni marshrutizatorlar kompyuterga, yo‘nalish jadvallarining ularga kerakli qismini uzatishadi.

Marshrutizator “yo‘nalishni boshqa tomonga yo‘naltirish” xabariga keyinchalik foydalaniladigan IP manzil va o‘z ma’lumotlar maydonining birinchi 64 bitli dastlabki paket sarlovhasini joylashtiradi.

Paket sarlovhasidan qurilma qaysi tarmoq uchun ko‘rsatilgan marshrutizatordan foydalanish kerakligini bilib oladi.

3.4. IP – telefoniyada qo’llaniluvchi standartlar va protokollar

Ma’lumot uzatish tarmoqlari orqali telefon so‘zlashuvlarini tashkil etishning samarali usuli, IP texnologiyasining ilovalaridan biri - IP telefoniya hisoblanadi. U eng iqtisodiy - foydali usul bo‘lib, uning asosida foydalanuvchiga telefon so‘zlashuvlar uchun kam bo‘lgan xarajatlarni talab etuvchi telefon xizmatlari taklif etiladi.

IP ga asoslangan tarmoqlarda barcha ma’lumotlar: ovoz, matn, video, kompyuter dasturlari yoki boshqa turdagi barcha axborotlar paketlar ko‘rinishida uzatiladi. Ushbu tarmoqdagi barcha kompyuter va terminallar o‘zining noyob manziliga ega. Uzatiladigan paketlar mazkur sarlovhada ko‘rsatilgan manzil asosida qabul qiluvchiga jo‘natiladi. Ma’lumotlar bir vaqtning o‘zida ko‘pgina foydalanuvchilar va jarayonlar orasida bitta shu tarmoq orqali uzatilishi mumkin. IP tarmoqda muammolar yuzaga kelsa, shikastlangan joyni ma’lumotlar aylanib o‘tishi mumkin. Bu vaziyatda IP protokol signali uchun kanal ajratilishini talab etmaydi.

IP tarmoq orqali ovozlarni uzatish jarayoni bir necha bosqichdan iborat: Dastlab ovoz raqamlanadi. Keyin raqamlangan ma’lumotlar fizik hajmni kamaytirish maqsadida taxlil etiladi va ko‘rib chiqiladi. Odatda shu bosqichda ortiqcha tanaffuslar va fon shovqinlari yo‘qotiladi hamda jipslashtiriladi. Navbatdagi bosqichda qabul qilingan ma’lumotlar ketma-ketligi paketlarga bulinadi va unga qabul qiluvchining manzil-axborot protokoli hamda xatolarni tuzatishga doir qo‘shimcha ma’lumotlar qo‘shiladi. Shu vaqtda paketni bevosita tarmoqqa uzatilishidan avval, uning tashkil topishi uchun kerakli miqdordagi ma’lumotlarni vaqtincha to‘planishi yuz beradi.

Qabul qilingan paketlardan axborotlarni ajratib olish ham bir necha bosqichlardan iborat: Ovoz paketlari qabul qiluvchi terminaliga yetib kelgach, avval uning ketma-ketlik tartibi tekshiriladi. IP-tarmoq yetkazish muddatini kafolatlamaydi, tartib raqami yuqori bo‘lgan paketlar avvalroq borishi va ular orasidagi intervallar ham o‘zgarib turishi mumkin. Dastlabki ketma-ketlikni va

sinxronlashtirishni tiklash uchun paketlarni vaqtincha to‘planishi yuz beradi. Lekin ba’zi paketlar uzatish davrida yo‘qotilishi yoki jo‘natilishga ajratilgan vaqtdan o‘tishi mumkin. Odatda qabul qiluvchi terminal yo‘qolgan yoki kechikkan paketlarni qayta so‘rashi mumkin. Ovozlarni uzatish usuli ushlanishlarga tanqidiy qaraydi. Olingan paketlar asosida yo‘qolganlarni taxminan tiklaydigan approksimatsiya algoritmi yoqiladi yoki bu yo‘qolishlar e’tiborga olinmay, bo‘shliqlar ma’lumotlar bilan tasodifiy to‘ldiriladi.

Bunday shakldagi ma’lumotlar ketma-ket dekompressiyalanadi va qabul qiluvchiga ovoz axborotlarini tashuvchi audio-signalga bevosita aylantiradi. Shunga asoslanib, qabul qilingan axborot dastlabki vaziyatdagi axborotga mos kelmasligi mumkinligini ta’kidlash lozim.

IP telefoniyaning tuzilishi paketli kommutatsiya tarmog‘ida multimediani amalga oshirishga mo‘ljallangan terminal qurilma, jihozlar va tarmoq xizmatlari tasvirini o‘z ichiga olgan. Telekommunikatsiya sohasini standartlashtirish tomonidan ishlab chiqilgan H.323 standartidan foydalanish asosida tashkil topgan. H.323 standartidagi terminal qurilma va tarmoq jihozlari mavjud vaqt ko‘lamida ma’lumotlarni, so‘zlarni va video axborotlarni uzatishi mumkin. H.323 terminallari orasida aloqani ta’minlaydigan tarmoq murakkab topologiyali segment va ko‘p segment xususiyatiga ega bo‘lishi mumkin. H.323 terminali shaxsiy kompyuterlar bilan ulanishi yoki avtanom qurilma sifatida amalga oshirilishi mumkin. So‘z almashish ta’minoti – H.323 standartidagi qurilma uchun majburiy vazifadir.

H.323 tavsiyasida 4 ta birikma keltirilgan:

- terminal;
- makon nazoratchisi (Gatekeeper);
- yo’lak;
- ko‘p nuqtali konferensiyalarni boshqarish qurilmasi.

Sanab o‘tilgan barcha birikmalar H.323 deb nomlanuvchi makonni tashkil etgan. Bitta makon nazoratchisi bir necha yakuniy qurilmalardan iborat bo‘lib, nazoratchi makondagi barcha yakuniy qurilmalarni boshqaradi. H.323 terminali boshqa H.323 terminallar bilan yoki ko‘p nuqtali konferensiyalarni qurilmasi bilan

birga harakat qilib, mavjud vaqt koʻlamida joʻnatmalarni uzatishi va qabul qilishi mumkin boʻlgan tarmoqdagi yakuniy nuqtalar sifatida gavdalanadi. Yuqoridagi vazifalarni taʼminlash uchun terminal oʻz ichiga quyidagilarni qamrab oladi.

- audio qurilmalar (mikrofon, akustika tizimi, telefon miksheri, akustik exolarni pasaytirish tizimi);
- video qurilmalar (monitor, videokamera);
- tarmoq interfeys qurilmasi;
- foydalanuvchining interfeysi.

H.323 terminali H.245, Q.931, RAS, RTP va H.450 protokollar oilasini taʼminlashi hamda G.711 audio kodlashni qoʻllash lozim. Ovozlarni anʼanaviy kommutatsiya kanallari oʻrniga IP tarmogʻi orqali uzatish texnologiyasi, yulaklar oʻrnatish orqali konfiguratsiyani inobatga oladi. Yulak (полоса) axborotni jipslaydi va IP paketga aylantiradi. IP tarmoqqa yuboradi, qarama-qarshi tomondagi yulak aks xarakatlarni amalga oshiradi, yaʼni chaqiriq paketlarini oʻqiydi va taqsimlaydi. Natijada oddiy telefon apparati chaqirishni hech bir muammosiz qabul qiladi. Axborotlarni bunday oʻzga tus olishi, dastlabki ovoz signalini ortiqcha koʻpaytirmasligi kerak. Uzatish rejimi mavjud vaqt koʻlamida abonentlar oʻrtasidagi axborot almashinuvini saqlab qolishi kerak. Yulaklarning asosiy vazifalari:

- IP va telefon tarmoqlari oʻrtasida fizik interfeysni amalga oshirish;
- abonent signalini shakllantirish va oʻrnatish;
- abonentlarni bogʻlash;
- abonent signallarini maʼlumotlar paketiga aylantirish va yana qaytarish;
- signal va ovoz paketlarini tarmoq orqali uzatish;
- aloqani uzish.

TCP/ IP tuzilmasida yulak vazifalarining asosiy qismi qoʻllanish jarayonida amalga oshadi. Chaqiriqlarni boshqarish vazifasini makon nazoratchisi boshqaradi.

Makon nazoratchisining vazifalari:

- taxallus (psivdonim) manzillarni transport manzillariga aylantiradi;
- ishlab chiqaruvchi tomonidan belgilab berilgan aloqa uchun yetarli

bo‘lgan chastota yulaklari miqdori va boshqa qirralariga ega avtorizatsiyali chaqiriq asosida tarmoqqa kirishni nazorat etish:

- o‘tkazish palasalarini nazorat qiladi;
- makonlarni boshqaradi.

Makon nazoratchisi yuqorida sanab o‘tilgan barcha vazifalarni faqat o‘zida ro‘yxatga olingan terminal, yulak va boshqaruv qurilmalariga nisbatan amalga oshiradi.

IP manzil, telefon raqami yoki belgilar qatoriga qo‘yilgan nom (elektron pochta manziliga xos) asosida amalga oshirilishi mumkin. Makon nazoratchisi oson esda qoladigan, qo‘yilgan nomlardan foydalanish imkonini berib, chaqiruvni soddalashtiradi. Makon nazoratchisi vazifalari yulaklarga kiritilishi mumkin.

Konferensiyalarni boshqarish serveri (MCU – Multipoint Control Unit) uch va undan ortiq H.323 terminallari aloqasini ta’minlaydi. Konferensiyada ishtirok etayotgan barcha terminallar MCU bilan bog‘lanishni o‘rnatadi. Server ko‘pgina manzillarga yo‘llanilishi kerak bo‘lgan konferensiya zahiralarini boshqaradi, ovoz, videoni ko‘rib chiqadi, audio va video oqimni aniqlaydi. H.323 tuzilmasi doirasida ko‘p nuqtali konferensiyalarni boshqarish tizimi o‘rnatilishi bo‘yicha ikkita yondashuv bor:

1. Ko‘p nuqtali konferensiyani markazlashgan holda boshqarish;
2. Ko‘p nuqtali konferensiyalarni markazlashmagan holda boshqarish.

Birinchi guruh konferensiyaning barcha ishtirokchilari boshqalariga ko‘p manzilli (guruhli) axborotlarni uzatadilar. Bu tarmoqning ba’zi sigmentlarida jo‘natmalar to‘planib qolishini oldini olish imkonini beradi. Lekin bunday konferensiyani boshqarish noqulaylik yaratadi. Markazlashgan usul qo‘llanilgan yakuniy qurilmalarda signallar MCU tizimida uzatadi. Bu esa uni uzatilishini ta’minlaydi.

IP telefoniyani joriy etilishidagi eng muhim muammolardan biri - xizmatlarni yuqori sifatda ta’minlashdir.

IP tarmoqlarda belgilangan QoS xizmatlari sifatini ta’minlash masalalari bilan telekommunikatsiya sohasini standartlashtiruvchi xalqaro tashkilotlar

shug‘ullanadilar.

Tarmoq zahiralariga maxsus talablar bilan so‘z jo‘natmalarini uzatish zarurati xizmatlar sifatini ta’minlovchi ko‘plab texnologiya va protokollarni ishlab chiqilishiga sabab bo‘ldi.

QoS mexanizmlari quyidagi vazifalarni amalga oshirilishini ta’minlashlari lozim.

- tarmoq zahiralarini boshqarish (o‘tkazish yulaklari, tarmoq qurilmalarini boshqarish amalga oshiriladi, global tarmoqda ishlash imkoniyatidan foydalaniladi va boshqalar);

- tarmoq zahiralaridan samaralari foydalanish (iqtisodiy samaradorlikni oshirish maqsadida jo‘natmalarni nazorat etish imkonini beruvchi menejment va tarifikatsiya);

- o‘ziga xos xizmatlar (QoS)ning ko‘rsatkichlarini boshqarish va nazorat qilish, xizmat operatorlari uchun o‘z mijozlariga turli pog‘onadagi xizmatlarni ta’minlash imkonini beradi;

- to‘liq integrallashgan tarmoq uchun asos yaratish (tarmoqda QoS mexanizmlaridan foydalanish kelajakda integral multimedia tarmog‘ini yuzaga kelishiga olib keladi).

Tayinlanish xususiyatiga muvofiq paketli kommutatsiya tarmoqlaridagi so‘z xizmati sifatini yaratuvchi mexanizmlarni uch guruhga bo‘lish mumkin:

- har bir tarmoq elementidagi QoS mexanizmi (masalan, navbatlarni tashkil etish vazifasi, jo‘natmalarni yo‘naltirish kabilar);

- QoS mexanizatsiya signalizatsiyalari tarmoqdagi tarmoq elementlari orasida ochiq sifatni ta’minlaydi;

- tarmoq jo‘natmalarini boshqarish va administratorlash uchun QoSni ta’minlaydigan hisob, boshqaruvi va usul vazifalari.

An’anaviy kommutatsiya tarmoqlari ovoz spektrlarining signallarini uzatish uchun yetarlicha eliment signallarini kafolatlangan o‘tkazish yo’lagi bilan uzatadi.

Paketli kommutatsiya tarmog‘i kafolatlangan o‘tkazuvchanlik xususiyatini ta’minlamaydi, chunki aloqa nuqtalari orasida kafolatlangan yo‘lni ta’minlamaydi.

E-mail singari paketlarni kelish tartibi va oraliq vaqtining ahamiyati bo‘lmagan ilovalarda ma’lum bir paketlar orasidagi ushlanish vaqti muhim ahamiyat kasb etmaydi. IP telefoniya ma’lumot uzatishning sohalaridan biri bo‘lib, unda zamonaviy kodlash usullari va axborotlarni uzatish hamda kanallarni o‘tkazuvchanlik xususiyatlarini o‘sishi asosida ta’minlanadigan signallarni uzatish dinamikasi muhim bo‘lib, bu IP telefoniyani an’anaviy telefon tarmoqlari bilan samarali raqobat qilish imkoniyatini beradi.

Quyidagilar IP telefoniyaning asosiy sifatlarini tashkil etuvchilari hisoblanadi:

- tushunarlilik – so‘zlarni sofligi va aniqligi;
- exo - o‘zining so‘zlarini eshitish;
- daraja - so‘zning balandligi.

Signallashuv sifatlariga:

- chaqiruvni o‘rnatilishi - samarali ulanish tezligi va bog‘lanish vaqtini o‘rnatilishi;
- chaqiruvni yakunlanishi - yakun vaqti va uzilish tezligi;
- DTMF- ko‘p chastotali raqamlarni terish signallarini aniqlash va belgilash.

IP telefoniya sifatiga ta’sir ko‘rsatuvchi omillarni ikki guruhga bo‘lish mumkin:

1. IP tarmoqning sifat omillari:

- yuqori o‘tkazuvchanlik xususiyati - u o‘tkazayotgan kerakli va ortiqcha ma’lumotlarning eng yuqori soni;
- ushlanish - tarmoq orqali paket uzatilishi uchun kerak bo‘ladigan vaqt oralig‘i;
- djitter - ikki ketma-ket paketlar orasidagi ushlanish;
- paketlarni yo‘qotish - tarmoq orqali uzatishda yo‘qolgan paket va ma’lumotlar.

2. Yo’lak sifatining omillari:

- kerakli o‘tkazish yo’lagi – turli vokoderlar turli yulakni talab qiladi. Masalan, G.723 vokoderi har bir so‘z kanali uchun 16.3 kbit/s li yulakni talab qiladi;

- ushlanish - raqamli signal protsessori yoki boshqa qayta ishlash qurilmalari uchun so‘z signallarini kodlash va koddan chiqarishga ketadigan vaqt;

- djitter buferi - barcha paketlar olinmagunga qadar ma’lumot paketlarini saqlash va djitterni kamaytirish uchun kerakli ketma-ketlikda uzatish imkoni;

- paketlarni yo‘qotish - paketlarni zichlash yoki IP telefoniya jihozlariga uzatishda paketni yo‘qotilishi;

- exoni yuqotish - tarmoq orqali uzatish davrida yuz beradigan exoni yuqotish mexanizmi;

- o‘lchamni boshqarish - so‘zlar balandligini nazorat etish imkoniyligi.

Yakunlovchi jihozlar va turli ishlab chiqaruvchilarning yulaklar bilan IP-telefoniyani standartlashtirish (3.4 - jadval) muammolarining mosligini ta’minlash bo‘yicha bir nechta xalqaro tashkilotlar shug‘ullanmoqda.

- Xalqaro Elektr Aloqa Ittifoqi (XEAI)ning telekommunikatsiya sohasini standartlashtirish (International Telecommunication Union-Telecommunication, ITU-T);

- Telekommunikatsiyalar bo‘yicha standartlashtirish Yevropa Instituti (ETSI, European Telecommunication Standart Institute);

- Internetning muxandislik muommolari bo‘yicha ishchi guruhi (Internet Engineering Task Force, IETF);

- Amerika Standartlar Milliy Instituti (American National Standart Institute, ANSI);

- VoIP forumi (Voice over IP) va boshqalar.

IP - telefoniya Xalqaro Elektr Aloqa Ittifoqi ko‘rsatmalariga asosan ishlaydi. Birinchi navbatdagi ko‘rsatmalar sifatida G.729, G.723.1 bo‘lib, soniyaiga 8 kbit va soniyaiga 6,3 - 5,3 kbit tezlikdagi jipslangan so‘zlar uchun standartlarni o‘rnatgan. So‘zlarni IP tarmoqdan uzatish uchun H.323 standarti majburiy standart hisoblanadi.

H.323 ko‘rsatmalar guruhini paketli tarmoqda multimediya aloqasini o‘rnatilishini ta’minlovchi tarmoq birikmalari, protokollari va jarayonlari belgilab beradi. Ular QoS xizmat sifatini kafolatlamaydigan, zahiralari taqsimlanadigan

tarmoqlarda abonent terminallarining faoliyat tartibini belgilaydi. H.323 - moslama jihozi telefon (IP-telefoniya) aloqasi, ovoz va videouzatish (videotelefoniya) hamda ovoz, video, ma'lumotlar uzatilishi (multimediya konferensiyasi)da qo'llanilishi mumkin.

3.4 - jadval.

IP – telefoniya bilan bog'liq standartlar

Nomlanishi	**Vazifasi**
T.120	Mavjud vaqtda konferensiyalarni uzatish
H.320	ISDN Videokonferensiyasi
H.323	Paketli kommutatsiya tarmoqlarida multimediya aloqalari.
H.324	Past tezlikdagi ma'lumotlarni uzatish kanallari orqali video, audio aloqa, masalan: kommutatsiyaviy modem bog'lanishlari orqali.
OSP	XML tili asosida IP jo'natmani ta'minlaydigan, ochiq xatti xarakatlar protokoli.
SIP	VoIP yulaklari va foydalanuvchining yakuniy jihozlar uchun aloqa seanslarini ko'zdan kechirish protokoli
RSVP	Foydalanuvchining paketli jo'natmalar ustivorligini ta'minlovchi zahiralarni saqlash protokoli
RTP	Mavjud vaqtda audio va videolarni uzatilishini ta'minlovchi mavjud vaqt protokoli
MGCP	Media yulaklarni boshqarish protokoli, turli xizmatlardagi ma'lumotlar paketini boshqarishni olib borilishini aniqlaydi
LDAP	Kataloglarga kirishning soddalashgan protokoli, u tarmoqda ma'lumotlarsiz universal manzillashni ta'minlaydi.

Hozirgi kunda standartning yangi nushasi tayyorlanmoqda. Bunda H.323 – yulaklararo aloqani tashkil etish va faksimil aloqa tarmog‘i paketlarini yaratilishi tasvirlanadi. Zamonaviy telefon aloqasida keng tarqalgan, ikkinchi chaqiruv haqidagi ogohlantirish va ma’lumot rejimi vazifalari haqida ham gap bormoqda. Yangi standart nushasi telefon bilan bog‘liq vazifalardan tashqari, tarifikatsiya maqsadida seans ko‘rsatkichlarini inobatga olish imkonini beradigan usullar, IP-manzillar o‘rniga abonent ismlaridan foydalanish uchun sharoit yaratadigan kataloglar qo‘shiladi.

H.323 standarti turli xildagi tarmoqlarda multimediya-aloqalarini tashkil etadigan H.32x ko‘rsatmalar oilasiga mansub, bular:

- H.320 - qisqa yo’lakli raqamli kommutatsiya tarmoqlari;
- H.321 – keng yo’lakli ISDN va ATM tarmoqlari;
- H.322 – o‘tkazish yo’lagi kafolatlangan paketli tarmoqlar;
- H.324 – umumiy foydalanishdagi telefon tarmoqlari.

H.323 standartini ishlab chiqilishining asosiy maqsadlaridan biri, boshqa turdagi tarmoqlar bilan multimediya aloqalarini ta’minlash hisoblanadi. Bu vazifa ma’lumotlarni to’plash va signallarni uzatishni ta’minlovchi yulaklar yordamida bajariladi. Standartga moslik sharti bilan turli imkoniyatdagi qurilmalar bir - biri bilan birga xarakatlanishi mumkin. Masalan, video ma’lumotli terminallar audio konferensiyalarda ishtirok etishi mumkin.

Boshqa standartlar majmui multimediali aloqa uchun H.323 tavsifi istalgan ko‘rinishdagi ko‘p nuqtali bog‘lanishdan «nuqta-nuqta» bog‘lanishgacha ishlatiladi. Bu standartlarning asosiy komponentlari 3.5 - jadvalda keltirilgan.

H.323 standarti ohirgi qurilmalarni boshqa standart bilan bog‘liqligini aniqlaydi. Telefon tarmoqlarida kommutatsiya kanallari va kommutatsiya paketlari kesishmasida paydo bo‘ladi. H.323 tarmoq standarti boshqa turdagi H.32x tarmoq bilan bog‘liqdir.

3.5 - jadval

Tavsiya	Tavsif
H.225	Xabarni chaqiruvlar boshqaruviga qarab signalizatsiya va ro'yxatlashni, shuning bilan multimedia ma'lumotlarini sinxronlashgan va paketli oqim bo'yicha aniqlaydi.
H.245	Multimedia ma'lumotlarini uzatish oqimida ochiq va yopiq kanal uchun xabarni aniqlaydi va boshqa buyruq, so'rovlarni ham.

IP-telefoniyaning takomillashuvida keyingi bosqich H.323ning tasnifi pastki pog'onaning etalon modeli va ochiq tizim bilan o'zaro ishlashidir. U kanalli va tarmoq pog'onalari xizmat sifati, qulaylikni ta'minlash uchun tegishli imkoniyatni inobatga oladi.

IETF ishchi guruhi tomonidan zahiralashgan protokol (RSVP) ishlab chiqilgan. Multimedia dasturlari RSVP yordamida mavjud bo'lgan tarmoq protokollarining istalgan biror biri orqali (asosan IP bundan tashqari ma'lumotni sifatli uzatishni ta'minlash uchun UDPdan ham foydalanishi mumkin) maxsus xizmatlarini talab qilishi mumkin. RSVP protokoli telefon so'zlashuvlarni bir-biri bilan, har bir qurilma bilan bog'lab turishi tufayli QoSga katta e'tibor beradi va bundan tashqari aniq ma'lumotlarni uzatishi mumkin.

RSVP QoS muammolarini hal etishni nazarda tutgan. Bunda multimediya dasturlariga xos bo'lgan internet protokollaridagi kamchiliklar, xususan ma'lumotlarni sinxronlash vositalarini yetarli rivojlanmaganligi mavjuddir.

TCP/IP ga o'xshash ishonchli protokollar ma'lumotlar yo'qolishini qaytara oladigan ko'p pog'onali vositalar orqali uzatiladi. Birgina ko'p tenglamali arxitektura audio va video signallarni dekoderlash jarayonlari vaqti tartiblangan sezgirligiga xalaqit beradi. Shu vaqt mezoni IPni shakllantirmaydi. Bundan sinxronizatsiya juda qiyin masala ekanligi kelib chiqadi.

Har bir ma’lumotlar paketida axborotlar tartibli raqamlashtiriladi. Bunday qo‘shimcha axborotlar tufayli amaliy dasturlar audio va video ma’lumotlar oqimida qiyin bo‘lmagan nisbiy aralashma bo‘ladi. Axborotni vaqtida yuborish uchun qabul qilingan har bir paketda sinxronizatsiyani qiyinchiliklarsiz amalga oshiradi. Dastur kadrni tartiblangan raqam bo‘yicha oson qabul qiladi. RSVPni sinxronli uzatishida va multimedia axborotlarini sifatli uzatishda RTP protokoli asosan qo‘llaniladi.

IP-telefoniyani tez sur’atdagi rivojlanishi IP tarmoqqa kanal kommutatsiyali tarmoq bilan ulanishga qaratilgan yulaklarning mos kelish muammosini keltirib chiqardi. Ko‘p nuqtali multimedia aloqalarini boshqaruvchi guruh IETF tashkiloti aloqa seanslarini umumlashtirishga qaratilgan protokol (SIP)ni ishlab chiqdi. H.323 standartlariga hozircha kiritilmagan SIP protokoli IP telefoniyani keng tarqalishiga turtki bo‘ldi, chunki u IP telefoniya va oddiy telefon orasidagi mavjud to‘siqlarni yo‘qotadi.

IP telefoniyada ovoz signallarini uzatilish sifatini ta’minlanishida ularni quyidagicha o‘rganib chiqish lozim:

1. Audiosignallar kirishidagi barcha kerak bo‘lmagan tarkibiy qismlarni bekor qilish. So‘zlarni raqamlardan chiqarish jarayonidan so‘ng dinamikdagi exoni mikrofonda yo‘qotish. IP turkumidagi va an’naviy telefon turkumidagi telefon tarmoqlaridagi shaxsiy kompyuterlar asosidagi barcha «Ochiq mikrofon» va boshqa ovozlar uchun exolarni va shovqinlarni samarali pasaytirish o‘ta zarur. Ushbu vazifalarni shaxsiy kompyuterning audiokomponentlari amalga oshiradi. Shuning uchun IP telefoniya tizimi bunday xususiyatga ega bo‘lmasligi mumkin. IP telefoniyaning yulaklari uchun kamroq ishni ko‘rib chiqish yuklatiladi.

2. So‘zlarda «tanaffus»larni so‘ndirish: qoldiq fon shovqinlarini tanish va yakuniy nuqtada tiklash hamda signallarni tanish uchun kodlashtirish. Tanaffuslarni yaqin nuqtada to‘liq so‘ndirgan afzal. Atrofdagi tovushlarni saqlab qolish uchun fon shovqiniga aylantirish lozim. Bu esa tizimda bu tovushlarni yakuniy nuqtada eshituvchi uchun tiklash imkonini beradi. Ko‘p chastotali raqamli terish signallarini va boshqa signallarni yakuniy nuqtada tiklash uchun qisqa kodlar

bilan almashtirish mumkin.

3. Ovoz ma’lumotlarini siqish. Raqamlangan ovozni turli usulda siqish mumkin. IP telefoniya uchun to‘g‘ri qaror tez, so‘z sifatini saqlaydigan va chiqishda ma’lumotlarning kichik xususiyatlarini uzatishdan iborat bo‘lishi kerak.

4. Siqilgan ovoz ma’lumotlarni qisqa sigmentlarga «bulish» va ketma-ketlikda raqamlash, uzatish va paketlarga sarlovhani qo‘shish. TCP/IP protokoli o‘zgaruvchan bo‘lgan paketlarni boshqarsada, ulardan foydalanishda ovoz ilovalarini tarmoqlararo yo‘naltirishdagi barqarorlikni, oldindan ko‘ra bilishlikni ta’minlashga to‘siq bo‘ladi. Marshrutizatorlar kichik paketlarni ko‘rib chiqadi va IP manzili orqali bir xil hajmdagi va bir xil usulda uzatiladigan paketlarni asosan ko‘rib chiqadi. Natijada paketlar bitta yo‘nalishda keladi va ularni qayta tartibga solish lozim.

5. Paketlarni yo‘qolishini va ushlanishini taxliliy o‘rganib chiqishni taminlash uchun paketlarni moslashish «qayta sinxronizatsiya buferi» da qabul qilish va qayta tartibga solish. Bu yerda asosiy maqsad paketlar orasidagi o‘zgaruvchan ushlanishlarning ta’sirini yengib o‘tishdan iborat.

IP kanalning o‘tkazuvchanlik xususiyatining muhim omillaridan biri so‘z axborotlarini kodlash va koddan chiqarishning eng maqbul algoritmlarini tanlashdan iborat.

Bugungi kunda mavjud bo‘lgan barcha turdagi so‘z kodeklarini ishlash tamoyilini uch guruhga bo‘lish mumkin:

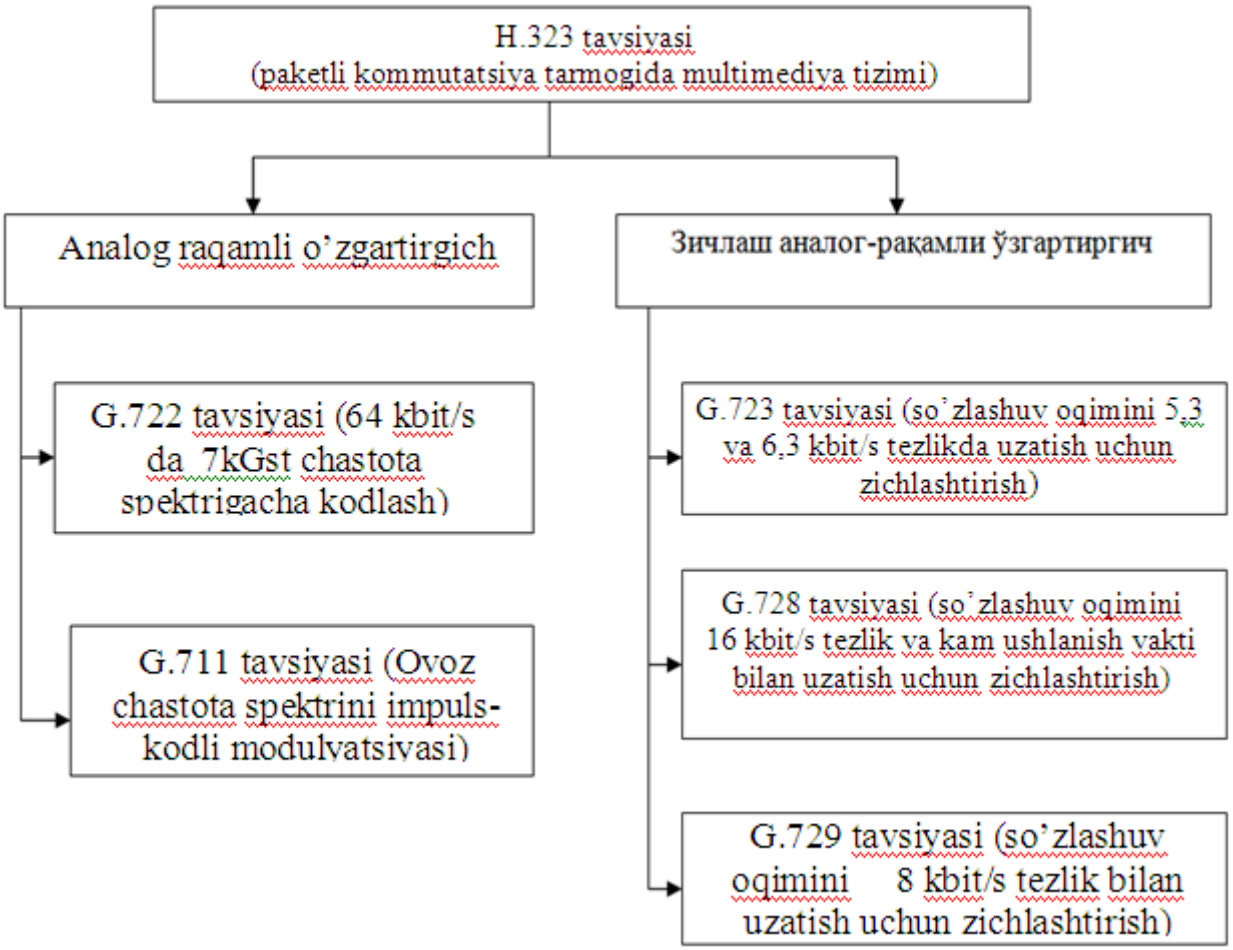
1. Kodlangan impulsli modulyatsiya va moslashgan differinsial kodlangan impulsli modulyatsiya kodeklari an’anaviy telefon tizimlarida qo‘llaniladi va ko‘p hollarda ARO‘/RAO‘larning uyg‘unligini aks ettiradi.

2. Vokoderli so‘z signallarini o‘zgaruvchan kodeklari uyali aloqa tizimlarida radiotraktning o‘tkazuvchanlik xususiyatiga talablarni tushurish uchun yuzaga kelgan. Ko‘p hollarda bu kodeklar analog jihozlarda qo‘llaniladi.

3. Umumlashgan kodeklarda so‘zlarni o‘zgartirish va sintezlash texnologiyasini jamlagan. Ular raqamli signallar bilan ish olib boradi. Bu turdagi kodeklar o‘zida raqamli vokoder asosida amalga oshadigan IKM yoki ADIKM

kodeklarni jamlagan.

IP telefoniyaning ovoz yulaklarida kodek tushunchasi faqat kodlash va koddan chiqarish algoritmlarini anglatmasdan va apparatura tadbig‘ini ham anglatadi. IP telefoniyada qo‘llaniladigan ko‘pgina kodeklar 3.3-rasmda ko‘rsatilgan G oilasining standarti H.323 tavsiyalarida belgilangan.



3.3-rasm. So‘z signallarini kodlash uchun standartlar

Signallar ko‘rinishidagi ma’lum ilovalar asosida kodlashning barcha usullarida signal uzatish vaqtida amplituda sezilarli sakrash bilan kelmaydi.

So‘zlarni uzatishdagi ushlanish raqamli signallarni ko‘rib chiqish muhimligi bilan bog‘liq bo‘lmay, balki bevosita siqish usulining xususiyatiga ham bog‘liq bo‘ladi. LPC bashorat liniyasi bilan kodlash orqali 2.4 yoki 4.8 Kbit/s li uzatish yulaklari mos bo‘ladigan juda katta pog‘onada siqishga ega bo‘lishi mumkin, lekin ovoz sifati sezilarli pog‘onada kamayadi. Signal kodlangach protsessor uning

shaklini tiklashga harakat qiladi va natijani dastlabki signal bilan taqqoslaydi, so‘ngra o‘ta moslikka erishish uchun kodlash ko‘rsatkichlarini belgilashni boshlaydi. Bunday moslikka erishgach apparatura olingan kodni aloqa liniyasi orqali uzatadi va qarama-qarshi tomonda esa ovoz tiklanishi yuz beradi. Bunday usuldan foydalanishda o‘ta yuqori hisoblash quvvati sodir bo‘ladi. Eng ko‘p tarqalgan, ta’riflangan kodlash usullaridan biri LD-CELP hisoblanadi. U 16 Kbit/s o‘tkazuvchanlik xususiyati asosida qoniqarli tiklash sifatiga erishish imkonini beradi. Algoritm 16 razryadli ovoz signallarini analog-raqamli o‘zgarish natijasida olingan raqamlar ketma-ketligiga qo‘llaniladi. Bu usulni qo‘llanishida ham o‘ta yuqori hisoblash quvvati talab etiladi. 1995 yil mart oyida yangi G.723 standarti qabul qilindi. Bu telefon tarmoqlari orqali videokonferensiyalarni tashkil etish uchun so‘zlarni zichlashda foydalanish ko‘zda tutilgan va G.723 ni asosini MP-MLQ usulida so‘zlarni zichlash tashkil etiladi. U yuqori eshittirishning yetarli sifatlarini saqlagan holda so‘zlarni o‘ta yuqori zichlash imkonini beradi. Bu usul asosida optimallashuv jarayoni yotadi. Unda turli xildagi takomillashuvlar yordamida so‘zni 4.8, 6.4, 7.2 va 8.0 Kbit/s pog‘onasigacha zichlash mumkin. Algoritmning tuzulishi uzatish vaqtida dasturiy ta’minot asosida ovozni zichlash pog‘onasini o‘zgartirish imkonini beradi. Kodlash natijasida ushlanish 20ms dan oshmaydi. O‘tkazish kengligidan foydalanish samaradorligi oshirilsa, so‘zlarni zichlash mexanizmi o‘z navbatida ushlanishlarni o‘sishiga va sifatni yomonlashuviga olib keladi.

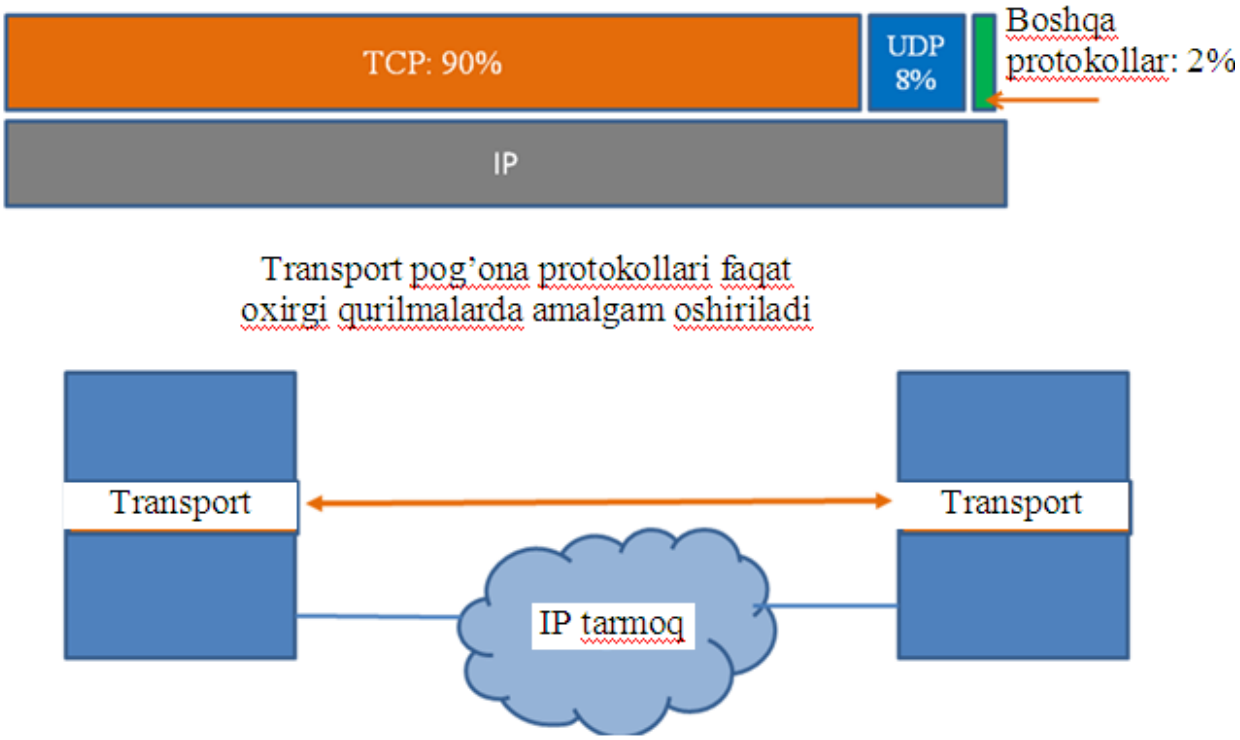
Nazorat savollari

1. Ovoz kodeklari qaerda ishlatiladi?
2. Ovozni paketga aylanishi qanday amalga oshiriladi?
3. Xizmat ko‘rsatish sifati nima?
4. IP kanalning o‘tkazuvchanlik xususiyati nima?

4. MA’LUMOT UZATISH TARMOQLARIDA TRANSPORT POG‘ONASI PROTOKOLLARI

4.1. Transport pog‘onasi protokollari: UDP, TCP va SCTP

Transport pog‘onasining asosiy maqsadi – o‘zining foydalanuvchilariga ishonchli, tejamli (resurs va kanallardan foydalanish rejasi asosida) va foydali xizmatlarni taqdim etishdan iborat (amaliy pog‘onada, 4.1-rasm).



4.1 – rasm. Transport pog‘onasi protokolini qo‘llanilishi

Transport pog‘onasining funksiyasi:

- foydalanuvchiga ma’lumotlarni to‘g‘ri yetkazib berilishini tekshirish;
- ulash, o‘rnatish;
- qabul qilganligi haqida hisobot;
- yo‘qotilgan yoki noto‘g‘ri yuborilgan ma’lumotlarni qayta jo‘natish;
- oqimlarni boshqarish.

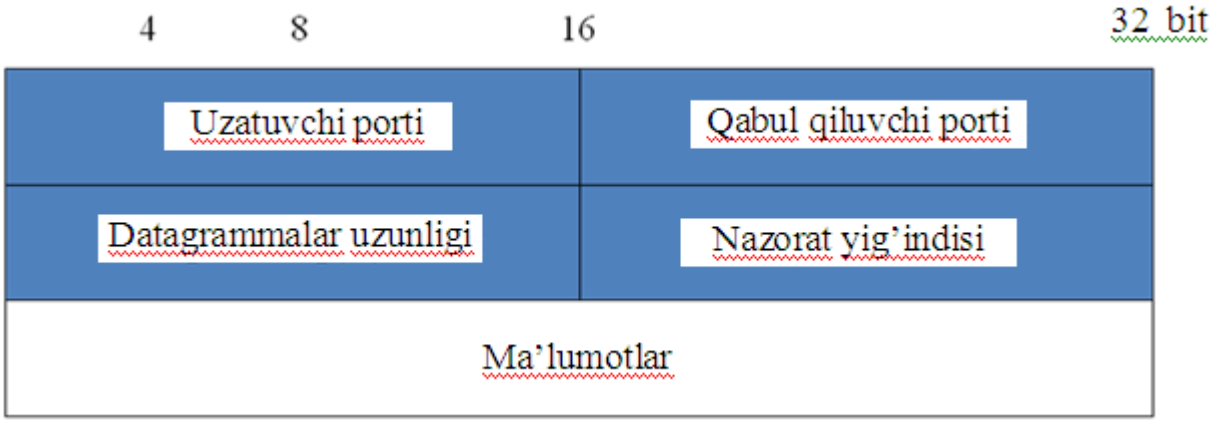
Qabul qiluvchining manzilini to‘g‘riligini tekshirish uchun psevdosarlovha

tuzilishi (UDP va TCP uchun)dan foydalanadi.

Transport pog‘ona protokollaridan ommaboplari TCP va UDP protokollari hisoblanadi:

- TCP protokoli – bu ishonchli protokol, ma’lumotlarni tartibli uzatish ketma-ketligini kafolatlaydi va tarmoq yuklamasini boshqarishni ta’minlaydi.
- UDP protokoli, xabarlar bilan ishlashga mo‘ljallangan, ma’lumotlarni uzatish ketma-ketligini kafolatlamaydi, tarmoq yuklamalarini nazorat qilmaydi (4.2-rasm).

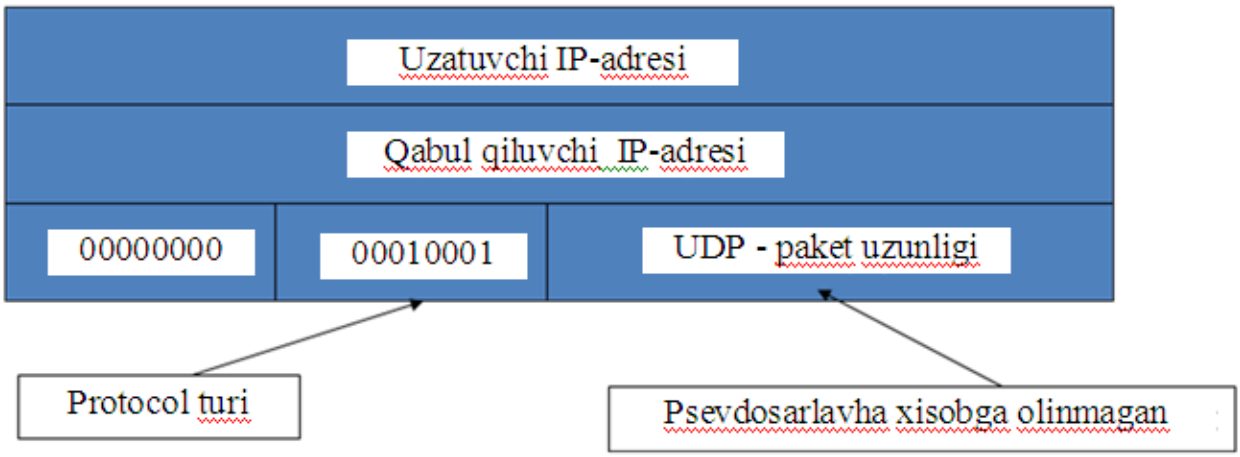
Lekin UDP protokoli tez ishlaydigan protokol hisoblanadi va xabarlar chegarasini ta’minlaydi.



4.2 – rasm. UDP sarlovha tuzulishi

UDP psevdosarlovha

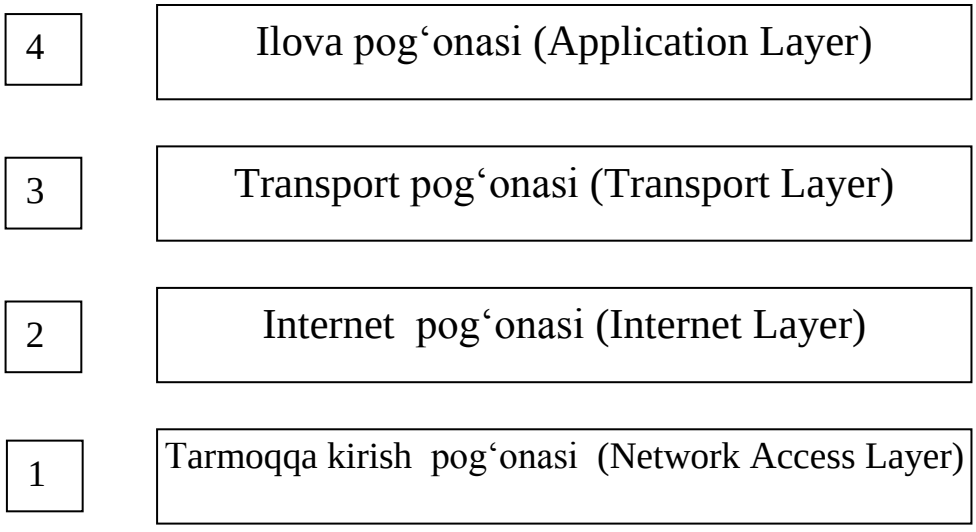
- nazorat yig‘indilarini hisoblashdan oldin UDP-paketiga qo‘shiladi. (psevdosarlovha va ma’lumotlar, nazorat yig‘indisi sarlovhaga asoslangan xolatda hisoblanadi) Yetkazib berishni to‘g‘riligini tekshirish uchun kerak. Qabul qiluvchiga uzatilmaydi (4.3-rasm);
- UDP-paketi noldan 16 bitgacha to‘ldiriladi;
- qabul qiluvchi nazorat yig‘indisini hisoblashda ma’lumotning psevdosarlovhasi asosida qabul qilingan IP – sarlovha, UDP sarlovha va ma’lumotlar maydonidan foydalanadi.



4.3 –rasm. UDP sarlovhasini tuzulishi

Umumun olganda, TCP protokollari to‘plami yuqorida ko‘rib chiqilgan OSI modeli to‘plamidan farq qiladi. TCPni quyidagi jadval asosida ko‘rish mumkin (4.4 - rasm):

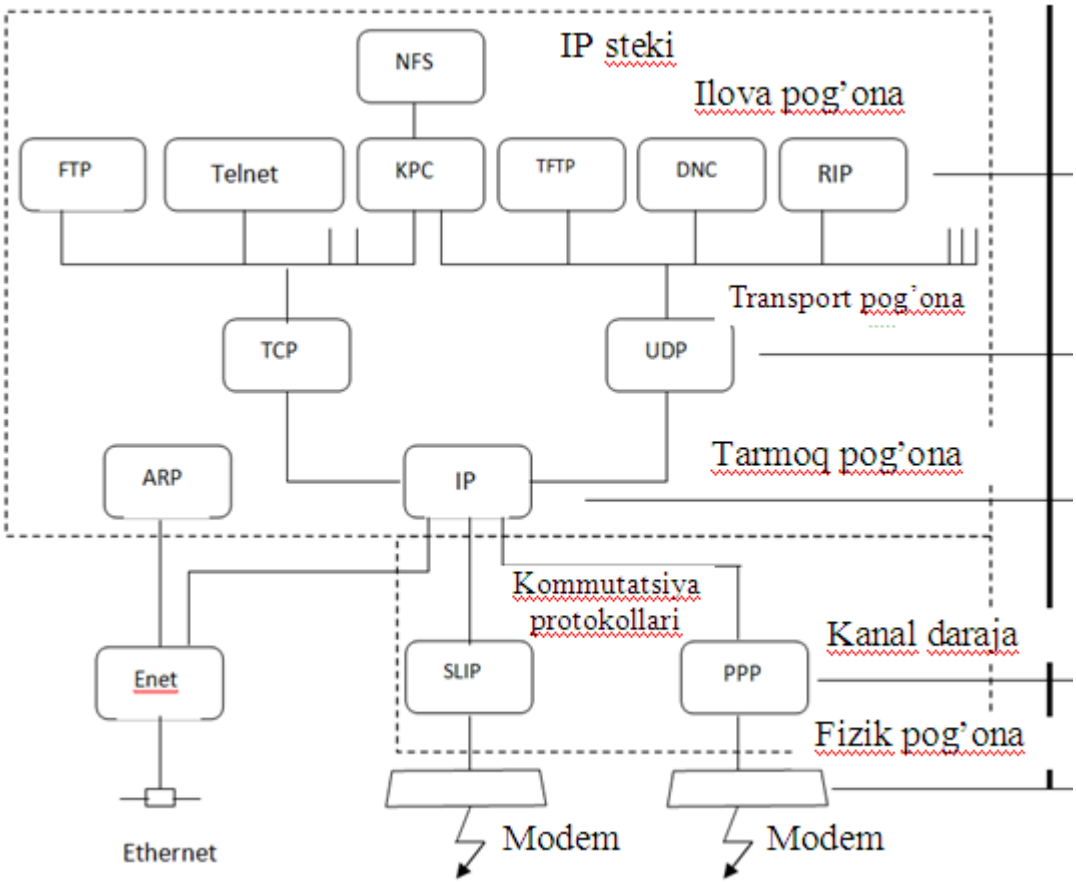
- ilova pog‘onasi (Application Layer);
- transport pog‘onasi (Transport Layer);
- Internet pog‘onasi (Internet Layer);
- tarmoqqa kirish pog‘onasi (Network Access Layer).



4.4 – rasm. TCP/IP protokollari to‘plamining tuzulishi

Ushbu rasmda tarmoqqa kirish pog‘onasida barcha fizikaviy qurilmalarga kirish protokollari joylashgan. Yuqorida tarmoqlararo almashinuv protokollari IP, ARP, ICMP mavjud. Yanada yuqoriroqda esa asosiy transport protokollari hisoblangan TCP va UDP, ular ma’lumotlarni paketlarga to‘plashdan tashqari, qaysi ilovaga ma’lumotlarni jo‘natish va qaysi ilovadan ma’lumotlarni olish lozimligini aniqlaydi. Eng yuqorida ilova pog‘onasidagi protokollar joylashib, ular ilovalardan ma’lumotlarni almashtirishda foydalanadilar.

OSI (Open Sustem Interconnection) tasnifiga asoslanib, TCP/IP protokollari tuzulishini etalon modeli (4.5 - rasm) bilan solishtirib ko‘ramiz.



4.5 – rasm. Tarmoq qurilmasida TCP/IP oilasiga mansub protokolarni qo‘llovchi modullar

Rasmdagi to‘g‘ri to‘rtburchak bilan belgilangan modullar ma’lumotlarni uzatish yo‘li-“chiziqlar”da paketlarni o‘rganib chiqadi. Bu chizmani taxlil etishdan avval ba’zi atamalarni keltirib o‘tamiz.

Drayver - tarmoq adapteri bilan bevosita birga harakat qiluvchi dastur;

Modul - drayver, tarmoqdagi qo‘llanish dasturlari va boshqa modullar bilan bilan birga xarakat qiladigan dastur;

Tarmoq interfeysi - kompyuterni tarmoqqa ulovchi fizik qurilma – Ethernet kartasi;

Kadr - tarmoq interfeysidan uzatadigan va qabul qiladigan ma’lumotlar bloki;

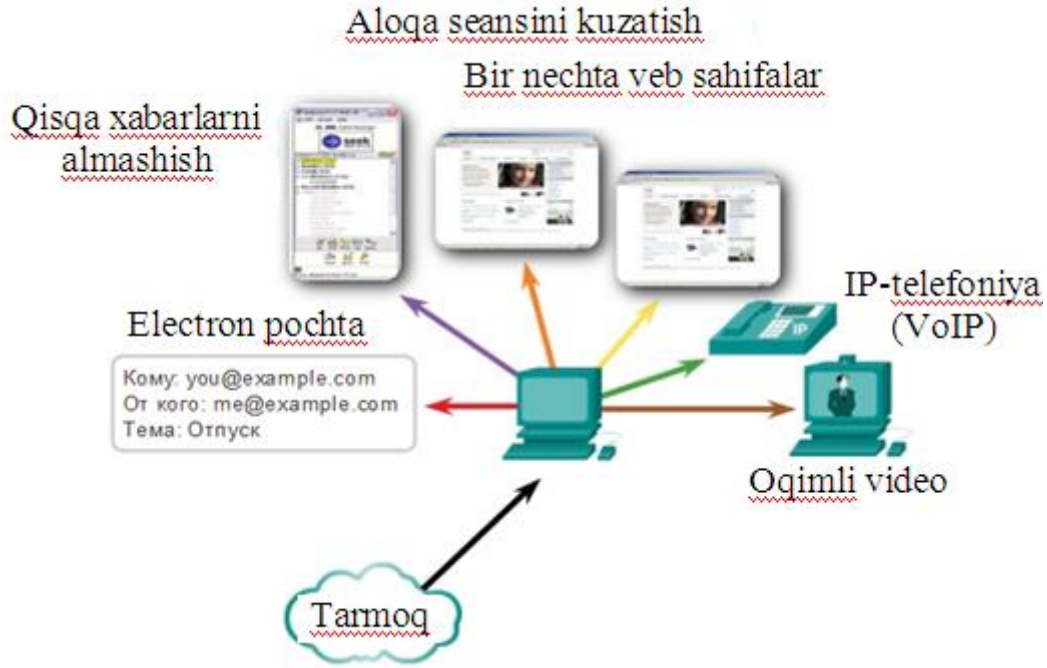
IP – paket - IP modulini tarmoq interfeysi bilan almashadigan ma’lumotlar bloki;

UDP – deytagramma - IP moduli UDP moduli bilan almashinadigan ma’lumotlar bloki;

TCP - IP moduli bilan TCP moduli almashinadigan ma’lumotlar bloki;

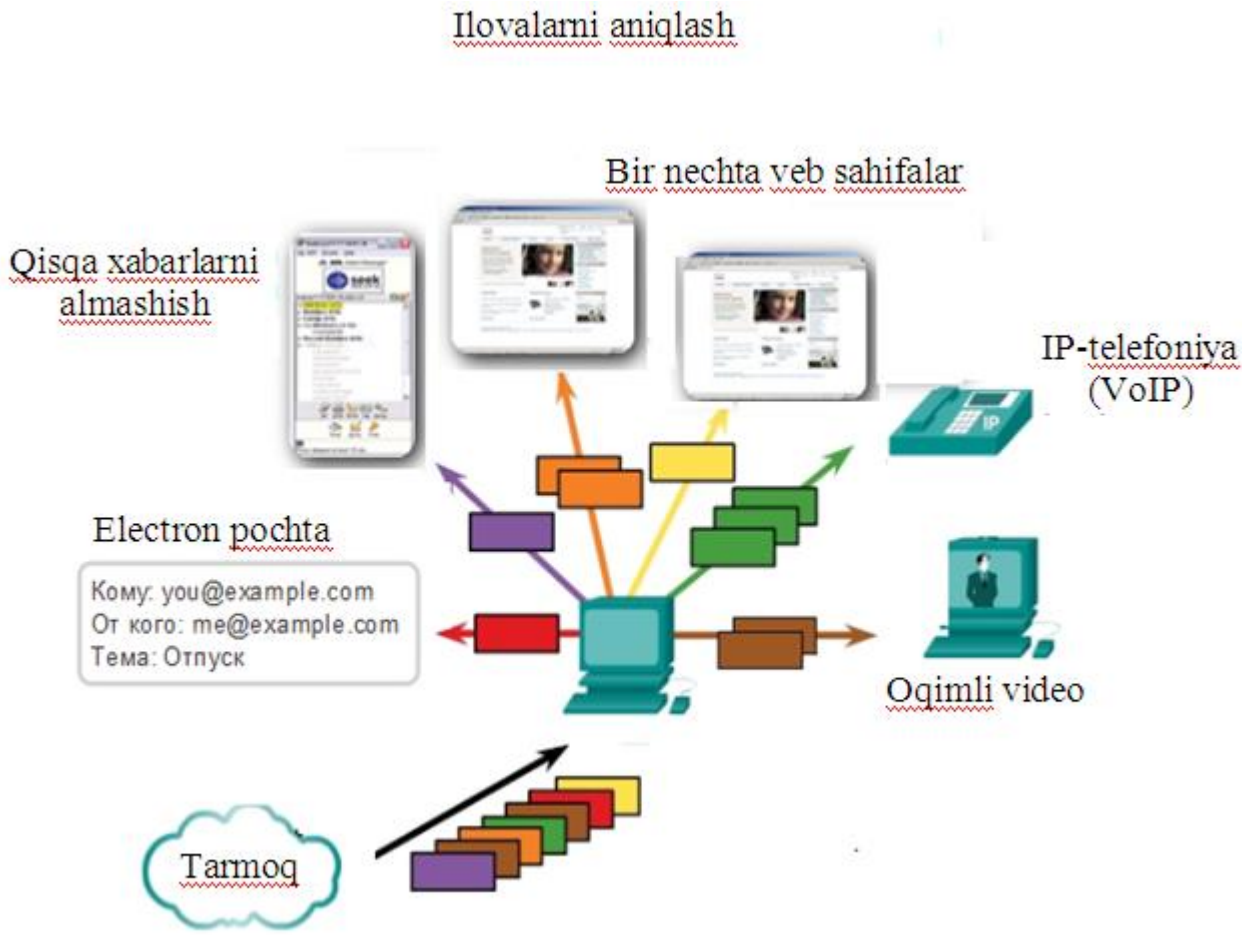
Qo‘llanish ma’lumotlari - Transport pog‘onasida tarmoq qo‘llanish dasturlari bilan protokollar almashinadigan ma’lumotlar bloki;

Inkapsulyatsiya (kapsula-«idish»ni yot organizmlardan xoli etish uchun tashkil etish ma’nosini bildiradi) - bir protokol hajmidagi ma’lumotlarni ikkinchi protokol hajmiga joylashtirish usuli. Masalan IP paketini Ethernetga yoki TCPni IP paketiga joylashuvi (4.6-rasm).



4.6 - rasm. Transport pog‘onasida aloqa seanslarini uzatilishi

Transport pog‘onasi qabul qiluvchi va uzatuvchining ilovalari o‘rtasida har bir aloqa seanslarini alohida kuzatadi (4.7-rasm).



4.7 – rasm. Transport pog‘onasida ilovalarni ajratilishi

Transport pog‘onasi qurilmada bir nechta ilovalar ochilgan bo‘lsa, ularning to‘g‘ri qabul qilinishiga kafolat beradi.

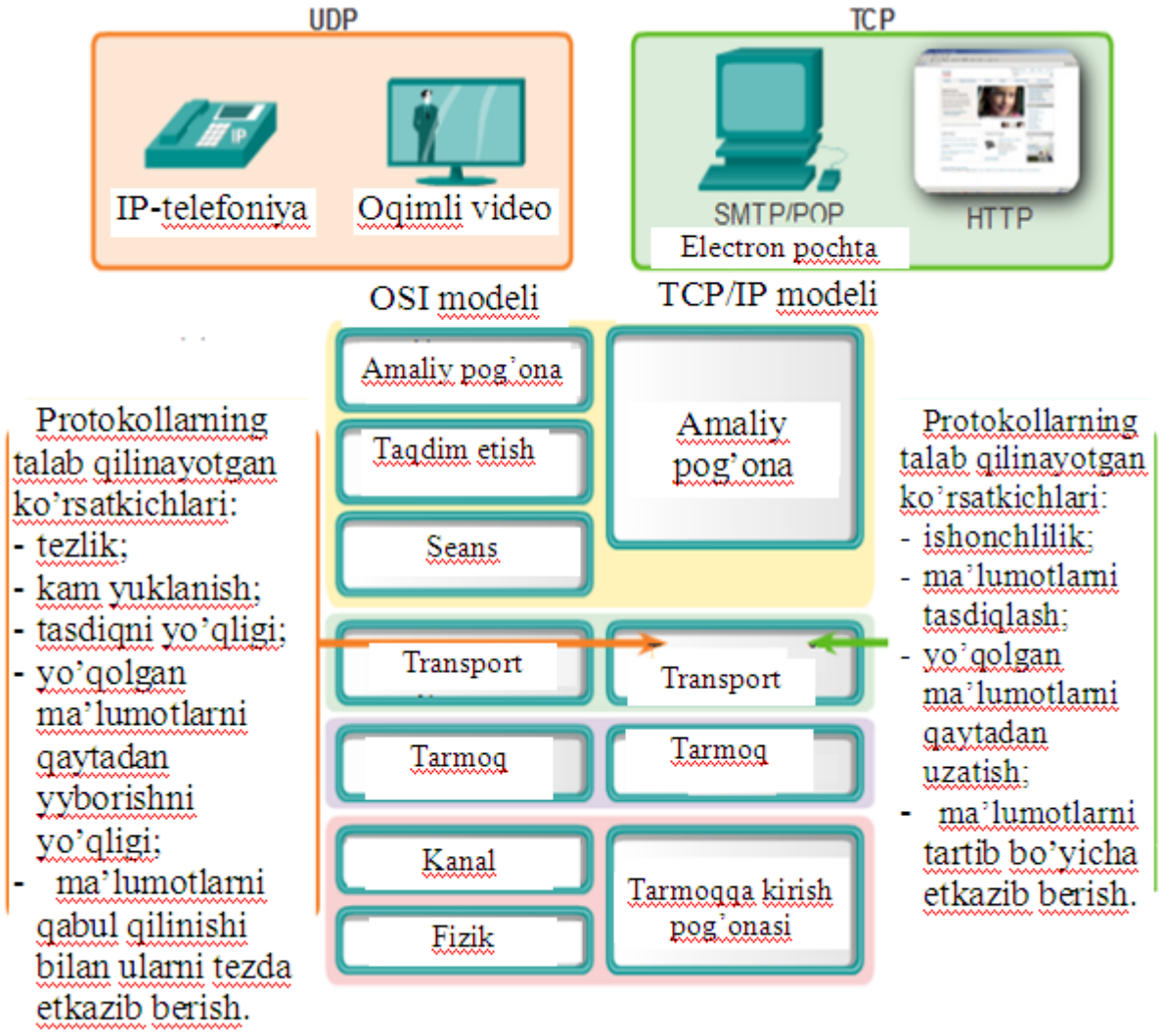
TCP ishonchli transport protokoli hisoblanadi. Bu esa ilovalar o‘rtasida ishonchli ma’lumot uzatishni yetkazib berilganligini tasdiqlash orqali ta’minlab beradi. Paketlarni TCP protokoli orqali uzatishda manbadan qabul qiluvchigacha bo‘lgan jarayon kuzatiladi.

TCP ishonchlilikni ta’minlash uchun quyidagi 3 ta asosiy vazifani bajaradi:

- ma’lumot segmentlarini uzatishni kuzatish;
- qabul qilingan ma’lumotlarni tasdiqlash;
- tasdiqlanmagan barcha ma’lumotlarni qaytadan uzatish.

TCP xabarlarni segmentlarga bo‘ladi. Bu segmentlarga tartib raqamlari

qo‘yiladi. Shundan so‘ng ularni paketga yig‘ish uchun IP protokol bo‘yicha uzatiladi. TCP uzatilgan segmentlarni u yoki bu tugunga borganligini kuzatadi. Agar jo‘natuvchi belgilangan vaqt ichida tasdiqlashni qabul qilmasa, u holda TCP bu segmentlarni yo‘qolgan deb ko‘radi va ularni qaytadan jo‘natadi. Qaytadan uzatish faqat xabarning yo’qolgan qismi uchun bajariladi. Qabul qiluvchi tomonidagi TCP protokol xabarning segmentlarini qaytadan yig‘ish va ularni mos keluvchi ilovalarga uzatish uchun javob beradi (4.8-rasm).

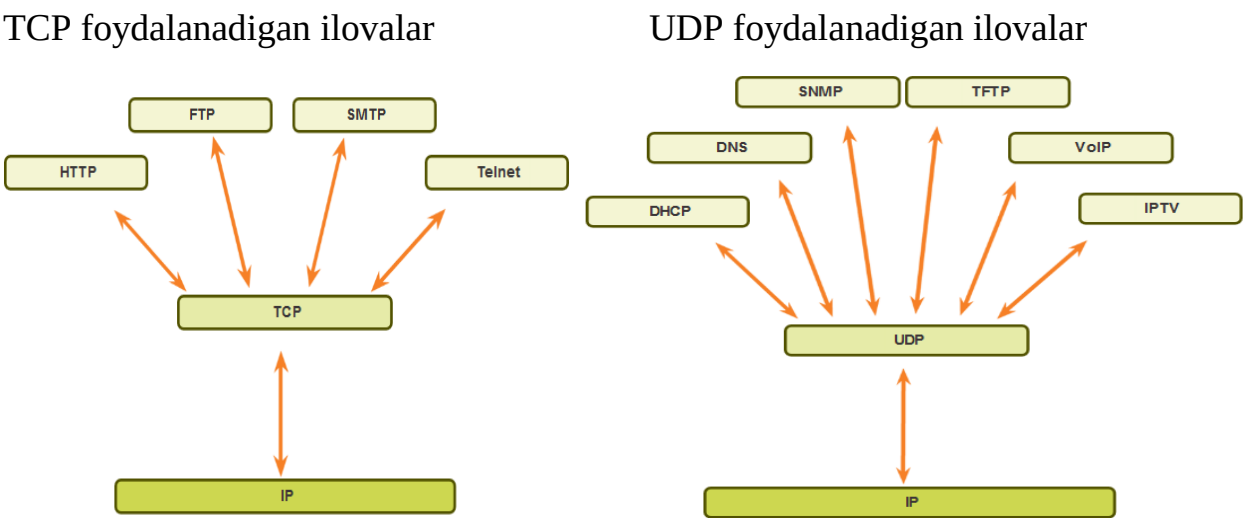


4.8 – rasm. Transport pog‘onasining ko‘rsatkichlari

Ishonchlilikni ta’minlashning bunday jarayonlari tarmoq resurslarini yuklanishiga olib keladi. Jo‘natuvchi va qabul qiluvchi o‘rtasida yuqoridagi jarayonlarni bajarish uchun qo‘shimcha boshqaruvchi ma’lumotlar uzatiladi. Bu nazorat axboroti TCPning sarlovhasida bo‘ladi (4.9-rasm).

Qo‘shimcha yuklanish ishonchlilikni ta’minlash uchun qaysidir ilovalar uchun foydaliligini kamaytiradi va uning samaradorligini yomon deyish mumkin.

UDP ilovalar o‘rtasida ma’lumot segmentlarini uzatish uchun faqat asosiy funksiyalarni ta’minlaydi. Buning uchun u katta bo‘lmagan resurslarni ishlatish va ma’lumotlarni tekshirish orqali ta’minlaydi. UDP ma’lumotlarni kafolatsiz yetkazish protokoli hisoblanadi. Kompyuter tarmoqlarida kafolatsiz yetkazish ishonchsiz hisoblanadi. UDP jo‘natuvchiga ma’lumotlarni muvofaqqiyatli yetib kelganligini tasdiqlovchi transport pog‘onasining jarayonlarini ishga tushirmaydi. UDP protokoli oddiy pochtadan ro’yxatdan o‘tkazilmagan xatni yuborishga o‘xshaydi. Jo‘natuvchi qabul qiluvchini olganligini bilmaydi, pochta bo‘limlari esa xatni nazoratga olishga, jo‘natuvchini xabardor qilishga va manzilga yetib borganligiga javobgarlikni o‘z zimmalariga olmaydi.



4.9 – rasm. TCP va UDP protokollar foydalanadigan ilovalari

Oqimni boshqarish axborotini uzatish protokoli (SCTP)

Oqimni boshqarish axborotini uzatish protokoli (SCTP) axborotni yetkazib berish ortiqchaligi va ishonchlilikning yuqori pog‘onasi bilan ikkita ohirgi punktlar o‘rtasida IP tarmoq orqali signalizatsiya xabarlarini uzatishni ta’minlaydi. Buning uchun real vaqtda axborotni ayrim axborot oqimlari bo‘yicha bir qancha

manbalardan yetkazib berishning yuqori ishonchliligini imkoniyatlar protokoliga o‘rnatilishi bilan farqlanadigan standartlashtirilgan usul qo‘llaniladi. Shuningdek ushbu protokol bo‘yicha ishlaydigan Internet bog‘lanishning o‘ta yuklanganlik holatida o‘z-o‘zini o‘chirish funksiyasi amalga oshiriladi.

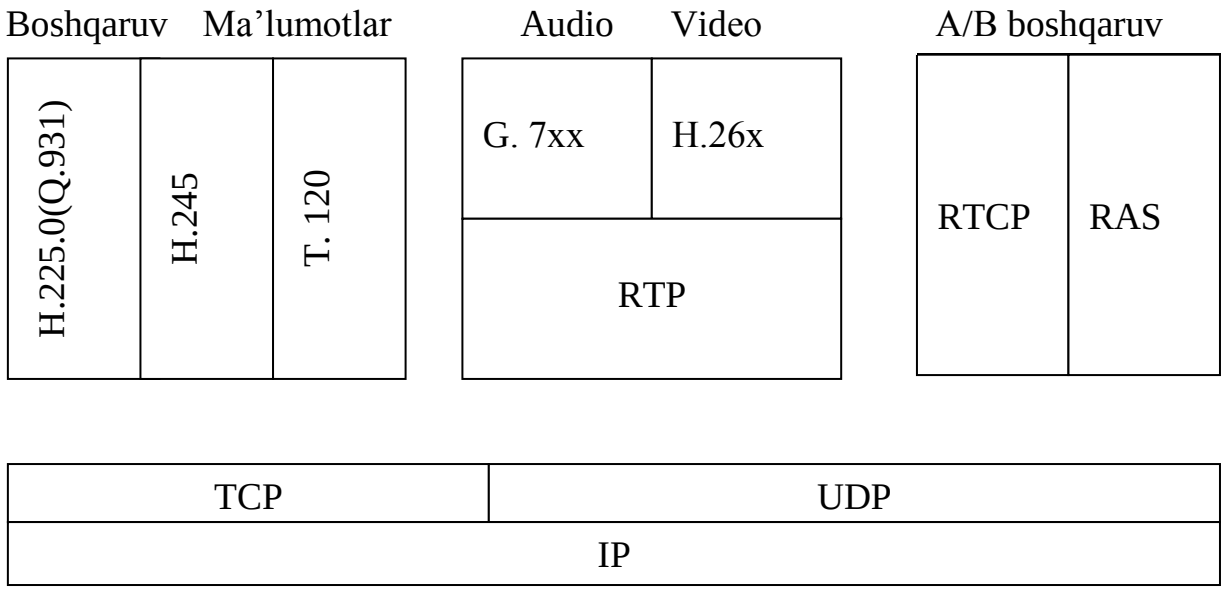
SCTP va signalli ilovalar o‘rtasidagi interfeys adaptiv pog‘ona orqali boshqariladi. Adaptiv pog‘ona oraliq pog‘onani shunday hosil qiladiki, unda protokollar stekining yuqori pog‘onasidagi muayyan arxitektruaning signalli protokollari transport muhiti bilan o‘z interfeyslarini va SCTP protokolidan boshqa transport protokoli o‘rniga foydalanilgan holatda ichki funksional imkoniyatlarini o‘zgartirmasligi kerak. Boshqa jihatdan, protokollar stekining ta’minlab turadigan arxitekturasi o‘z qoidalarini buzmasdan Internet arxitekturasiga mos kelishi kerak.

SCTP protokoli turli maqsadlarda turli xil ilovalardan – fayllarni HTTP vositalar yordamida uzatishdan signalli axborotni tashishgacha, MTP ishlash imkoniyatlarini o‘zgartirishdan SCCP signalizatsiya axborotini transportirovka qilishni o‘zgartirishgacha foydalanish mumkin.

4.2. Transport pog‘onasi protokollari: RTP va RTCP

RTP protokoli bir manzilli va guruhli jo‘natmalarning tarmoq xizmatini qo‘llagan holda ushlanishlarga seziluvchan axborotlarni yetkazishga ixtisoslashgan. U o‘z vaqtida yetkazilishini kafolatlovchi o‘z mexanizmlariga yoki boshqa xizmat sifati ko‘rsatkichlariga ega emas. Bu ishlarni quyida keltirilgan protokollar bajaradi. Odatda RTP UDP dan ustun ishlab, uning xizmatlaridan foydalanadi, lekin ba’zida boshqa transport protokollaridan ustun ishlashi ham mumkin (4.10-rasm).

RTP xizmati oqimda paketning ketma-ket raqamini va kerakli yuk turini ko‘rsatishni taqozo etadi hamda vaqtincha belgilash qo‘llaniladi. Junatuvchi har bir RTP paketni vaqtincha belgi bilan belgilaydi. Qabul qiluvchi esa uni ajratib oladi va ushlanish yig‘indisini hisoblaydi.



4.10-rasm. H.323 protokollar to‘plami

Paketlar orasidagi ushlanish farqi djitterni belgilash imkonini beradi va uning ta’sirini kamaytiradi, ya’ni barcha paketlar ilovaga bir xildagi ushlanish bilan beriladi.

Shunday qilib, RTPning asosiy xususiyati – qabul qilingan paketlarning ba’zi to‘plamining o‘rtacha ushlanishini hisoblash va ushbu o‘rtacha ko‘rsatkichga teng ushlanish asosida foydalanuvchining ilovasiga ularni doimiy yetkazib turish kabilar kiradi. RTPning yana bir ustunligi RSVP bilan uni belgilangan xizmat bosqichida sinxronlashgan multimediya axborotlarini uzatishda qo‘llash mumkin.

Mavjud vaqtda uzatishlarni boshqarish protokollari bilan birga RTP qo‘shilsa, uning imkoniyatlari oshishi mumkin.

RTCP yordamida RTP paketlarini yetkazilishi nazorat qilinadi hamda uzatilayotgan seansning boshqa ishtirokchilari bilan aks aloqani ta’minlaydi. RTCP doimiy ravishda o‘zining boshqarish protokollarini tarqatib turadi. Bunday tarqatish mexanizmi foydalanish axborotiga ega bo’lgan RTP paketlari uchun ham qo‘llaniladi.

RTCP ning asosiy vazifasi olinayotgan axborot sifatida hisobot uchun ilovadan foydalanib, aks aloqani tashkil etishdir. RTCP uzatilgan va yo‘qotilgan paketlar soni, djitter ahamiyati va boshqalar haqida ma’lumot uzatadi. Bu axborot

uzatuvchi tomonidan uzatish koʻrsatkichlarini oʻzgartirish uchun ishlatilishi mumkin.

Nazorat savollari

1. Tarmoqlararo almashinuv protokollari nima?
2. TCP va UDP protokollarining farqi nimada?
3. ICMP protokoli nima uchun ishlatiladi?
4. Paketlarni qabul qilinishi qanday amalga oshiriladi?
5. Real vaqtda qanday protokollar ishlatiladi?
6. QoS sinflari nimaga javob beradi?
7. Xizmat koʻrsatish sifat koʻrsatkichlari qanday tekshiriladi?
8. IP - telefoniya qaysi protokollar bilan ishlaydi?
9. RTP protokoli qachon ishlatiladi?
10. RTCP protokolining asosiy vazifasi nimadan iborat?
11. RSVP protokolining ishlatilishini tushuntirib bering?

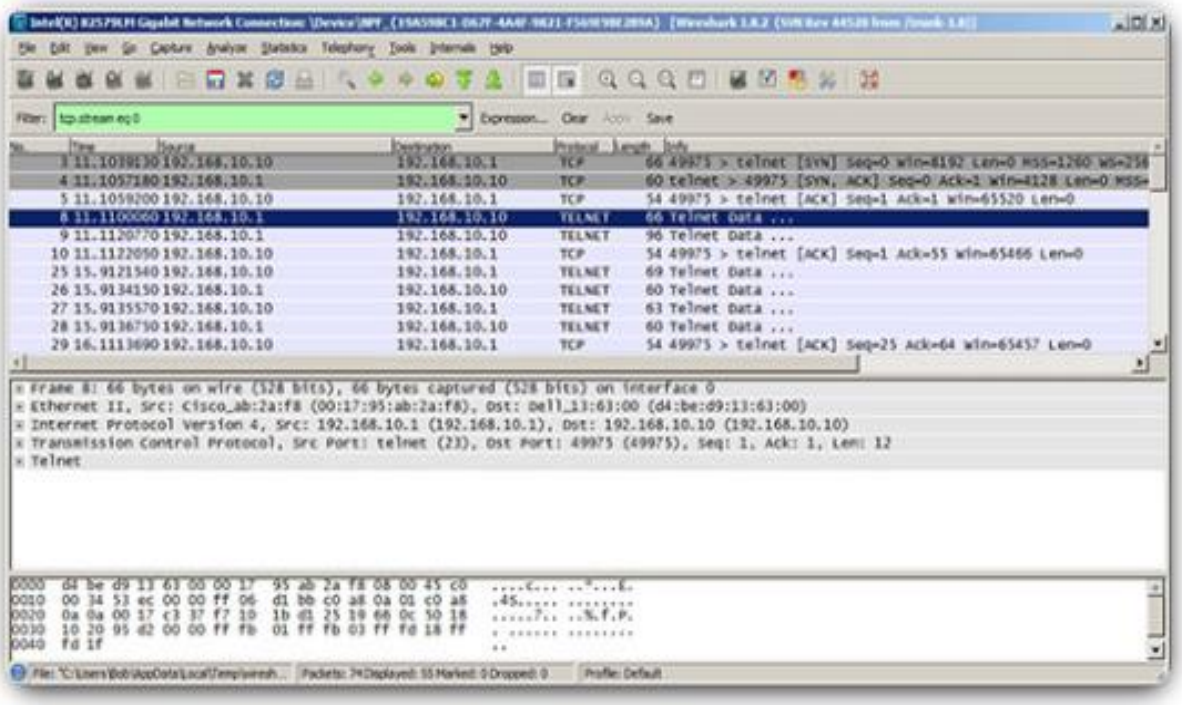
5. MA’LUMOT UZATISH TARMOQLARIDA AMALIY VA HIMOYALANGAN TARMOQ PROTOKOLLARI

5.1. Amaliy pog‘ona protokollari: Telnet, FTP va TFTP, NTP

Amaliy pog‘ona protokollari - bu ilova dasturlari bo‘lib, qo‘llanilishi jihatdan turli vazifalarni bajaradi. Masalan: Telnet qurilmalarga uzoqdan ulanishni ta’minlaydi. FTP va TFTP protokollari esa serverga ma’lumotlarni uzatish va qabul qilish uchun ishlatiladi.

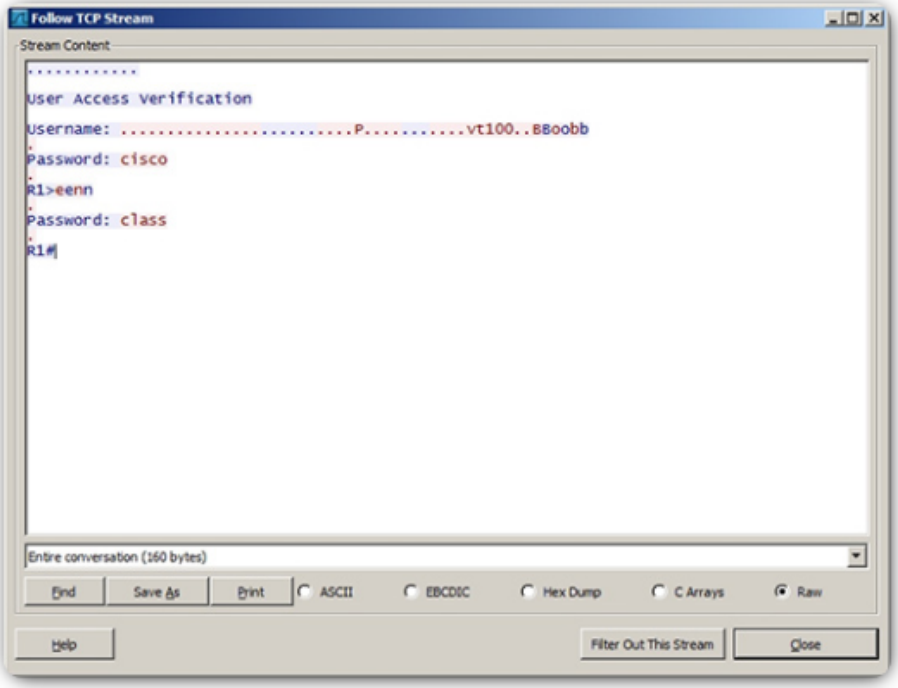
Lokal tarmoqlarda telnetni qisqa vaqt uchun ishlatish mumkin. Telnet eskirgan protokol hisoblanib, qurilmalar o‘rtasida ishlashda shifrlanmagan xavfsiz ma’lumot ko‘rinishiga o‘xshaganday identifikatsiya axborotlari (foydalanuvchi nomi va paroli) ochiq uzatiladi. SSH uzoqdagi qurilmalar bilan bog‘lanishda himoyani ta’minlaydi. Qurilmalarni autentifikatsiya (foydalanuvchi nomi va paroli) ma’lumotlarini ishonchli shifrlaydi. Shuningdek qurilmalar o‘rtasida uzatilayotgan ma’lumotlarni ham himoyalaydi. SSH TCP-port 22 ni,Telnet TCP-port 23 ni ishlatadi.

5.1 – rasmda begona shaxs Wireshark dasturi yordamida paketlarni ko‘rishi mumkinligi keltirilgan. Telnet oqimida foydalanuvchi nomi va parolini ushlashi mumkin.



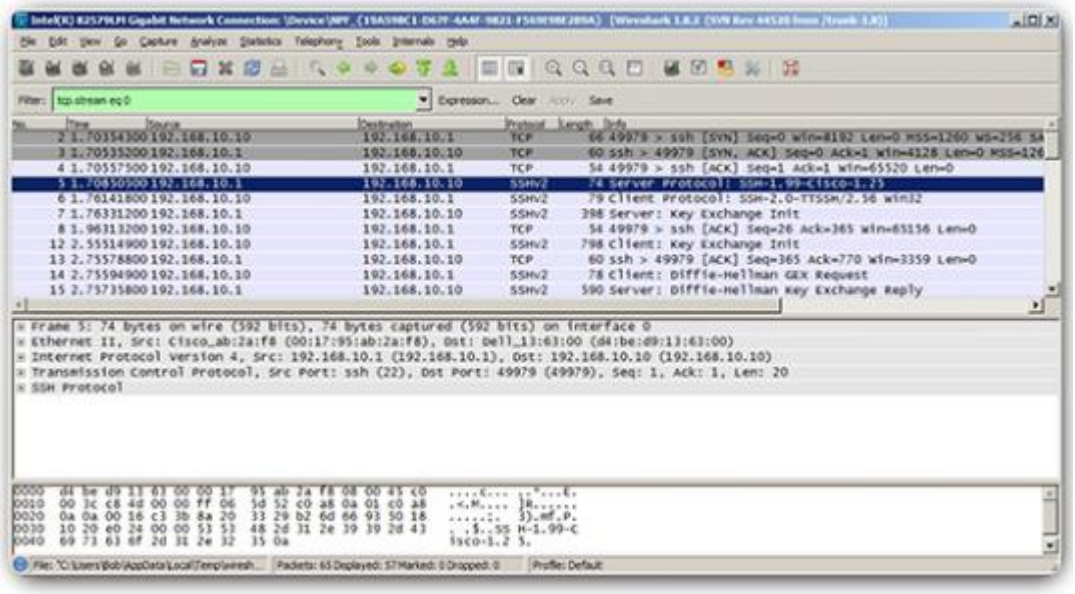
5.1 - rasm. Telnetni Wireshark dasturi yordamida ushlash

5.2 – rasmda begona shaxs himoyalanmagan telnet seansida administratorning nomini va parolini ushlashi mumkinligi keltirilgan.



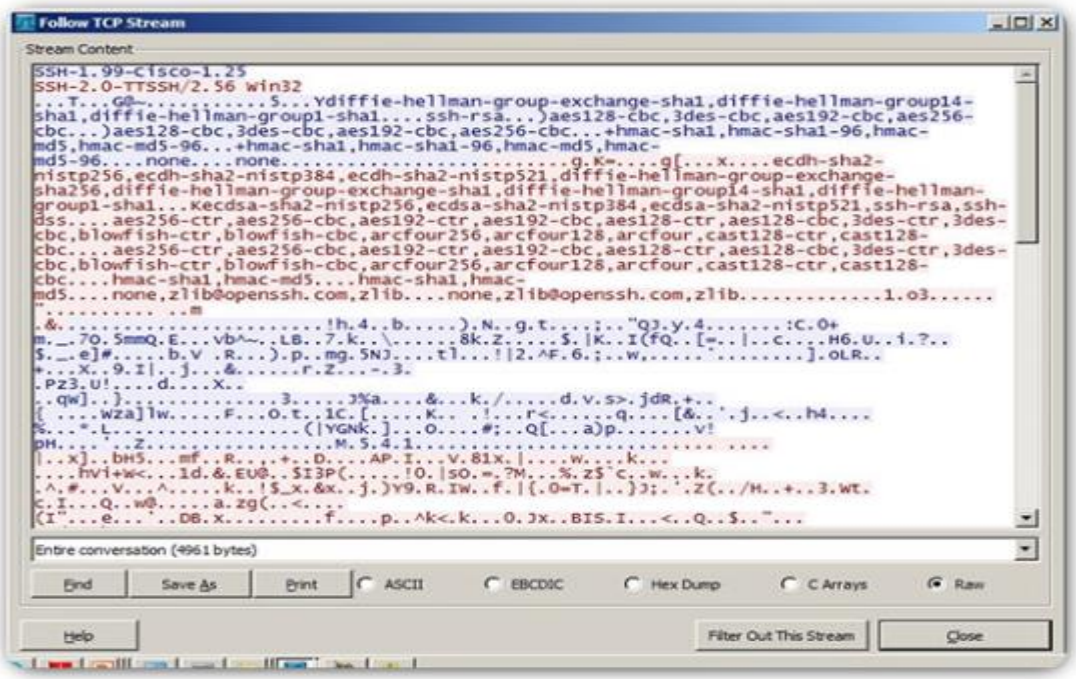
5.2 – rasm. Himoyalanmagan telnet seansida administratorning nomini va parolini ushlash

5.3 – rasmda SSH seansini Wireshark dasturi yordamida ko‘rish ko‘rsatilgan. Begona shaxs administratorning qurilmasini IP manzili yordamida seansni kuzatishi mumkinligi keltirilgan.



5.3 – rasm. SSH seansini Wireshark dasturi yordamida ko‘rish

5.4 – rasmda SSH protokoli yordamida foydalanuvchi nomi va paroli shifrlangan ko‘rinishi keltirilgan.



5.4 – rasm. SSH protokoli yordamida foydalanuvchi nomi va paroli shifrlangan ko‘rinishi

SSH protokolini ishlashi uchun kriptografik funksiyalarga va imkoniyatlarga (shifrlash) ega bo‘lgan IOS dasturiy ta’minotli kommutatorlar kerak bo‘ladi. Kommutatorda **show version** buyrug‘ini berib, kommutator qaysi IOS versiyasida ishlayotganligini ko‘rish mumkin (5.5 - rasm). Agar operatsion tizimning nomida K9 so‘zi ishlatilsa, bu kriptografik funksiyaga va imkoniyatlarga (shifrlash) egaligini ko‘rsatadi.

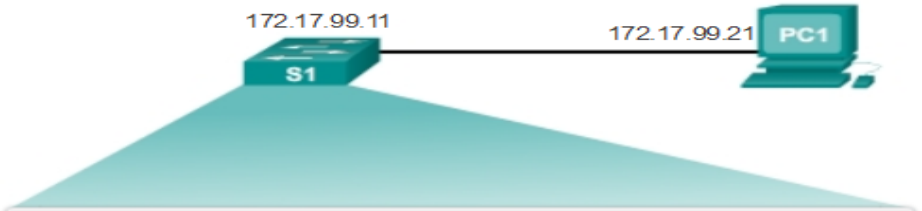
```
S1> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE, RELEASE SOFTWARE (fc1)

<выходные данные опущены>
```

5.5 – rasm. Operatsion tizimning nomida k9 so‘zi mavjudligi

SSH protokolini sozlashdan oldin kommutatorda tugunning maxsus nomini va tarmoq ulanishining mos keluvchi ko’rsatkichlarini ko‘rsatish lozim.

SSH protokoli borligini bilish uchun **show ip ssh** buyrug‘i beriladi. Agar kommutatorda kriptografik funksiyani qo‘llab quvvatlovchi IOS bo‘lmasa, bu buyruq ishlamaydi.

Tarmoqning IP domenini global konfiguratsiya rejimida **ip domain-name** *domen nomi* yordamida ko‘rsatiladi. 5.6 – rasmda domen nomi **cisco.com** qilib olingan.




```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

5.6 – rasm. Uzoqdagi qurilmani boshqarish uchun SSH protokolini sozlash

IOSning hamma versiyalarida ham SSHning 2 versiyasi ishlatilmaydi. SSHning 1 versiyasida ma’lum zaifliklar mavjud. SSHni sozlash uchun global konfiguratsiya rejimida **ip ssh version 2** buyrug‘i beriladi. Juft RSA kalitlari yaratilganda SSH protokoli avtomatik ishga tushadi. Kommutatorda SSH serverini ishlatish va juft RSA kalitlarini generatsiya qilish uchun global konfiguratsiya rejimida **crypto key generate rsa** buyrug‘i kiritiladi. RSA kalitlarini yaratishda administratordan modulni uzunligini kiritish talab etiladi. Modulning uzunligi 1024 bit bo‘lishi tavsiya etiladi (5.6 – rasm). Uzun modul ishlatilsa xavfsiz bo‘ladi, lekin uni yaratishda va ishlatishda ko‘p vaqt ketadi.

Izoh: juft RSA kalitlarini o‘chirish uchun global konfiguratsiya rejimida crypto key zeroize rsa buyrug‘idan foydalaniladi. Juft RSA kalitlarini o‘chirilgandan keyin SSH server avtomatik o‘chadi.

SSH-server foydalanuvchilarni lokal yoki autentifikatsiya serveri yordamida himoyalashi mumkin. Autentifikatsiyaning lokal usulini ishlatish uchun global konfiguratsiya rejimida **username** *imya_polzovatelya* **secret** *password* buyrug‘i beriladi. Foydalanuvchi uchun **admin** parol uchun **ccna** olindi.

Tinch holatda SSH ikkala versiya (1 va 2)ni qo‘llab quvvatlaydi. Agar ikkala versiya ishlasa, u holda **show ip ssh** buyrug‘ining natijasi 1.99 versiya deb xabar beradi. 1 versiyada ko‘p zaifliklar mavjud. Shu sababli faqat 2 versiyani ishlatish tavsiya qilinadi. Uni ishlatish uchun global konfiguratsiya rejimida **ip ssh version 2** buyrug‘i beriladi.

5.2. Himoyalangan tarmoq protokollari

VPN – shaxsiy virtual tarmoq (SHVT) deganda, u albatta shaxsiy tarmoq ko‘rsatkichlariga ega. Hech qanday “gap - so‘zsiz” tarmoqni shaxsiy deb atash uchun biror - bir korxona butun tarmoqning infratuzilmasiga, ya’ni kabel, kross qurilmasi, kanal hosil qiluvchi qurilma, kommutator, marshrutizator va boshqa kommutatsiya qurilmalariga egalik qilganda aytish mumkin.

VPNning boshqa tarmoqlardan asosiy farqi, bu uning boshqa tarmoqlardan ajralganligidadir. Ajralganligini ko‘rsatuvchi ko‘rsatkichlar quyidagilardan iborat:

- *istalgan mustaqil tarmoq texnologiyasini tanlay olish*: tanlash imkoniyati faqat ishlab - chiqaruvchining qurilmalarini imkoniyati bilan chegaralanishi mumkin;

- *mustaqil manzillash tizimi.* VPN da manzil tanlashda cheklanish yo‘q, u istalgancha bo‘lishi mumkin;

- *ishlab - chiqaruvchanligini oldindan aytish mumkin*. Shaxsiy aloqa kanallari avvaldan ma’lum kafolatlangan o‘tkazuvchanlik qobiliyatini korxona qurilmalari (global ulanishlar uchun) yoki kommutatsiya qurilmalar (lokal ulanishlar uchun) o‘rtasida ta’minlaydi;

- *maksimal pog‘onadagi xavfsizlik*. “Tashqi dunyo” bilan aloqa yo‘qligi butun tarmoq bo‘yicha axborotni “o‘g‘irlanishi” ehtimolligini kamaytiradi.

Lekin VPN - judayam “arzonga” aylanmaydi. Bunday tarmoqlarni milliy yoki xalqaro doirada ishlaydigan, moliyaviy barqaror va yirik kompaniyalar o‘zlariga ep ko‘radi. Shaxsiy tarmoqni yaratish - shaxsiy tarmoq infratuzilmasiga ega zarur, ish jarayoni uchun muhim.

VPN tarmoqdan o‘tayotgan axborot turini aniqlay olishi lozim (tovush, SNA, video oqim yoki elektron pochta). U juda tez bir trafikni boshqasidan ajrata olishi kerak. Yana tarmoq VPN - ogoh bo‘lishi kerak, chunki servis - provayder internet va ekstranet tarmoqlari uchun foydalanuvchi va xizmatlarni osongina guruhlay olishi lozim. MPLS texnologiyasi kommutatsiyalanadigan va marshrutizatsiyalanadigan tarmoq uchun VPN xabardorlikni beradi. Bu narsa yagona infratuzilmada servis-provayderga tez va tejamkor, himoyalangan, istalgan hajmdagi VPN tarmog‘ini hosil qilish imkonini beradi.

Turli boshqa yo‘llarni ishlatmagan holda MPLS tarmog‘i trafikni kodlamay, tunellashtirmay uni himoyasini ta’minlay oladi. MPLS texnologiyasi har bir alohida tarmoqda xuddi FR va ATM ulanishdagi kabi xavfsizlikni ta’minlay oladi. Agarda an’anaviy VPN tarmog‘i tarmoqdagi harakatni, bazali qiymatlarini amalga oshirsa, MPLS texnologiyasi bilan jihozlangan tarmoq, keng doiradagi

VPN xizmatlaridan VPN tarmog‘ining harakatini bazali xizmatlariga IPni qo‘shgan holda amalga oshiradi. Bu reja servis provayderlarning mo‘ljallangan usulda xizmatlarini mo‘ljallangan modelga o‘tishini bildiradi. VPN uzatish jadvallari asosida 3-sathdagi trafikni bemalol taqsimlay oladi. MPLS VPN birinchi buyurtmachi trafigini boshqa buyurtmachi trafigidan bemalol ajratadi, chunki har bir VPN tarmog‘idagi hamma buyurtmachilar o‘zining noyob identifikatoriga ega. Bu narsa huddi ATM va FRdagi kabi xavfsizlikni ta’minlaydi, chunki VPN tarmog‘ining foydalanuvchisi tarmoqdan tashqarida uzatilayotgan trafikni ko‘rmaydi.

Yana bir marta MPLS - VPN tarmog‘ining tavsifsini ko‘rib chiqamiz. Buyurtmachining istalgan marshrutiga MPLS belgisi uzviy bog‘lanadi. Uni marshrut boshida joylashgan RE - marshrutizator qo‘shadi. Ushbu belgi ma’lumotlar paketini ohirgi nuqtadagi RE marshrutizatorga uzatishga yo‘naltirilgan:

- ma’lumotlar paketini magistral bo‘ylab uzatganda 2 ta belgidan foydalanadi. Ustki belgi paketni kerakli ohirgi RE -marshrutizatoriga yo‘naltiradi. Keyingi belgi ushbu RE - marshrutizatoriga paketni keyingi yo‘nalishni tanlash uchun qo‘shiladi;
- RE va SE - marshrutizatorlari o‘rtasidagi aloqa kanalida standart uzatish sxemalari (IP for war doing) ishlatiladi. RE har bir SEni uzatish jadvali bilan bog‘laydi (for warding table), ushbu jadvallarga faqatgina shu SE larga tegishli marshrutlar saqlanadi.

VPNni to‘g‘rilash uchun, provayderning magistral tarmog‘i orqali o‘tadigan marshrutlar haqidagi axborot uning chegarasidan chiqishi kerak emas. Mijozlarning saytidagi marshrutlash haqidagi axborot esa ayrim VPNlarning chegarasidan chiqmasligi talab etiladi.

Yo‘nalish haqidagi axborotni tarqalishiga to‘siq bo‘lishi mumkin bo‘lgan narsa, bu mos shakllangan marshrutizatordir. Marshrutizatsiyalash protokoli qaysi interfeys va kimdan yo‘nalganligi to‘g‘risidagi axborotni olish va kimga uzatish kerakligi haqida xabardor bo‘lishi kerak.

MPLS VPN tarmog‘ida bunday to‘siqlar rolini chegaraviy RE marshrutizatorlari bajaradi. Tasavvur qiling, RE marshrutizator orqali mijoz sayti va provayder tarmog‘i o‘rtasida ko‘rinmas chegara o‘rnatiladi. Bir tomonga RE marshrutizatorlari R marshrutizatorlari bilan bog‘lanishi uchun zarur interfeyslar o‘rnatiladi. Yana bir tomonga mijozlarning sayti ulanishi uchun kerak bo‘lgan interfeyslar o‘rnatiladi. Bir tomondan RE marshrutizatorlari magistral tarmoqning marshrutlari haqidagi axborot kelsa, bir tomondan mijozlarning saytidagi marshrutlar haqidagi axborot keladi.

RE marshrutizatorlariga bir necha IGP turidagi protokollar joylashtirilgan. Ulardan biri RE ni R bilan ulash uchun, marshrutlarni ketma-ket va uzatish uchun uchta ichki interfeys bilan bog‘langan. Qolgan ikkita IGP protokoli mijozlarning saytidan tushgan axborotlarni qayta ishlaydi.

Qolgan RElar ham xuddi shu tarzda shakllangan. R marshrutizatorlari barcha interfeyslardan kelayotgan IGP axborotini qabul qiladi va qayta ishlaydi. Natijada barcha RE va R marshrutizatorlari marshrut jadvallariga ega bo‘lishadi. Ularda provayder tarmog‘ining ichidagi barcha marshrutlar mavjud bo‘ladi. Shuni ta’kidlash kerakki, mijozlarning saytlaridagi marshrutlar haqidagi axborot bu yerda yo‘q. Shunga mos ravishda mijozlar provayder tarmog‘idagi marshrutlar haqida hech narsa bilmaydilar. Chegaraviy RE marshrutizatorlari tomonidan jadval, o‘zida marshrutlash haqida axborot bor, maxsus «marshrutlashning global jadvali» degan nom olgan. Bu jadvaldan holi holda RE mijozlarning saytidagi marshrutlar asosida VRF (VPN Roting and forwarding) jadvalini tuzgan, bunda RE mijozlarning saytidan tushgan e’lon asosida jadval tuzadi.

Mijozlarning sayti oddiy IP tarmog‘idan iborat, marshrutlash axboroti istalgan IGP protokoli yordamida uzatilishi va qayta ishlanishi mumkin. Ko‘rinib turibdiki, bu jarayon provayder tomonidan rejalashtirilmaydi. Marshrutlash haqidagi e’lonlar bemalol qurilmalar orasida tarqaladi. Bu narsa chegaraviy RE marshrutizatoriga yetib borguncha sodir bo‘ladi, chunki u ularning keyingi tarqalishida chegara bo‘lib xizmat qiladi.

Turli mijozlarning marshrutlarini cheklash uchun RE marshrutizatorlariga

o‘rnatilgan interfeyslarga, mijoz saytlari ulangan alohida marshrutlash protokollari o‘rnatilgan. Ushbu protokol mijozning marshrut e’lonlarini faqat bitta interfeys orqali uzatadi va qabul qiladi, ularni na ichki RE va R marshrutizatorlar bog‘lanadigan inrefeys orqali na boshqa mijozlarning sayti ulangan interfeyslar orqali uzatmaydi. Natijada RE marshrutizatorlarida bir nechta VRF jadvallari hosil bo‘ladi.

Soddalashtirib shuni aytish mumkinki, REda unga nechta ulangan sayt bo‘lsa shuncha VRF hosil bo‘ladi. Umuman olganda, RE marshrutizatorlarida bir nechta virtual marshrutizatorlar hosil bo‘ladi, ularning har biri o‘zining VRF jadvallari bilan ishlaydi. Saytlar va VRF jadvallari o‘rtasida yana boshqa aloqa mavjud bo‘lishi mumkin. Misol uchun bitta RE ga bitta VPN ning bir nechta sayti ulangan bo‘lsa, unda ularga bitta umumiy VRF jadval hosil qilish mumkin. Har bir shunday jadvalga faqat shu VPNga tegishli saytga murojaat qila oladi.

IPSec protokoli (Internet Protocol Security) asosan IP tarmoqlarda ma’lumotlarni xavfsiz uzatishni ta’minlaydi. IPSecning ishlatilishi quyidagilarni kafolatlaydi:

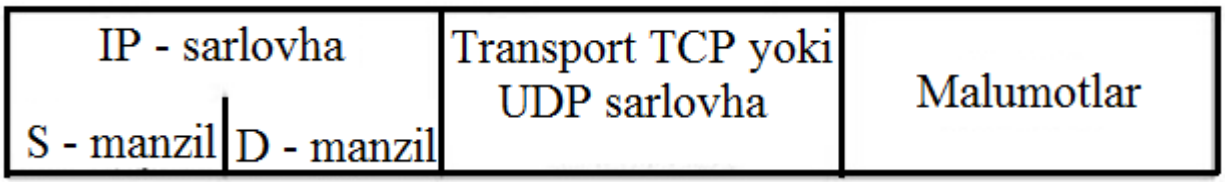
- uzatilayotgan ma’lumotlarning yaxlitligini, ya’ni ma’lumotlar uzatilishida buzilmaydi, yo‘qolmaydi va takrorlanmaydi;

- jo‘natuvchining autentligini, ya’ni ma’lumotlar haqiqiy jo‘natuvchi tomonidan uzatilgan;

- uzatiladigan ma’lumotlarning mahfiyligini, ya’ni ma’lumotlar shunday shaklda uzatiladiki, ularni ruxsatsiz ko‘zdan kechirishning oldi olinadi.

Ta’kidlash lozimki, axborot xavfsizligi tushunchasiga odatda, yana bir talab-ma’lumotlarning foydalanuvchanligi kiritiladi. Ma’lumotlarning foydalanuvchanligi deganda ma’lumotlar yetkazilishining kafolati tushuniladi. IPSec protokollari bu masalani hal etmaydi va uni transport satxda ISP ga qoldiradi. IPSec protokollar steki tarmoq satxida axborot himoyasini ta’minlaydi. Bu himoya ishlovchi ilovalarga ko‘rinmasligiga olib keladi. IP-paket IP tarmoqlarda kommunikatsiyaning fundamental birligi hisoblanadi. Uning

tuzilmasi 5.7-rasmda keltirilgan.



5.7 – rasm. IP-paket tuzulishi

IP-paket tarkibida manba manzili S va axborot qabul qiluvchining manzili D, transport sarlovhasi, bu paketda tashiluvchi ma’lumotlar xili xususidagi axborot va ma’lumotlarning o‘zi bo‘ladi.

Autentifikatsiyalashni, uzatiluvchi ma’lumotlarning mahfiyligi va yaxlitligini ta’minlash maqsadida, IPSec protokollarining steki qator standartlashtirilgan kriptografik texnologiyalar asosida qurilgan:

- kalitlarni almashtirish ochiq tarmoqdan foydalanuvchilar orasida mahfiy kalitlarni taqsimlashning Diffi-Xellman algoritmi bo‘yicha amalga oshiriladi;

- ikkala tomonning haqiqiyligini kafolatlash va main-in-the-midle xilidagi hujumlarni oldini olish maqsadida Diffi-Xellman algoritmi bo‘yicha almashishlarni imzolashda ochiq kalitlar kriptografiyasidan foydalaniladi;

- ochiq kalitlarning haqiqiyligini tasdiqlashda raqamli sertifikatlar ishlatiladi;

- ma’lumotlarni shifrlashda blokli simmetrik algoritmlardan foydalaniladi;

- xeshlash funksiyalari asosida axborotlarni autentifikatsiyalash algoritmlari ishlatiladi.

Himoyalangan kanalni o‘rnatish va madadlashdagi asosiy masalalar quyidagilar:

- foydalanuvchilar yoki kompyuterlarni autentifikatsiyalash;

- himoyalangan kanalning ohirgi nuqtalari orasida uzatiluvchi ma’lumotlarni shifrlash va autentifikatsiyalash;

- kanalning ohirgi nuqtalarini ma’lumotlarni autentifikatsiyalashda va

shifrlashda kerak bo'ladigan mahfiy kalitlar bilan ta'minlash.

Yuqorida sanab o'tilgan masalalarni hal etishda IPSec tizimi axborot almashish xavfsizligi vositalarining kompleksidan foydalanadi.

IPSec protokolining amalga oshirilishida quyidagi komponentlardan foydalaniladi:

- IPSecning asosiy protokoli. Ushbu komponent himoyani inkapsulyatsiyalovchi protokol ESP (Encapsulation Security Rau1oad)ni va sarlovhani autentifikatsiyalovchi protokoli AH (Authentication Header)ni amalga oshiradi. U sarlovhalarni ishlaydi; paketga qo'llaniladigan xavfsizlik siyosatini aniqlash uchun SPD va SAD ma'lumotlar bazasi bilan o'zaro aloqa qiladi;

- kalit axborotlarini almashishni boshqarish protokoli IKE. IKE odatda foydalanish satxida qo'llaniladi (operatsion tizimga o'rnatilgani bundan istisno);

- xavfsizlik siyosatlarining ma'lumotlar bazasi SAD (Security Association Database). Bu eng muhim komponentlardan biri bo'lib, paketga qo'llaniladigan xavfsizlik siyosatini belgilaydi. SAD dan asosiy protokol IPSec tomonidan kiruvchi va chiquvchi paketlarni ishlashda foydalaniladi;

- xavfsiz assotsiatsiyalarning ma'lumotlar bazasi SPD. Bu ma'lumotlar bazasi kiruvchi va chiquvchi axborotni ishlash uchun xavfsiz assotsiatsiyalar SA(Security Association) ro'yxatini saqlaydi. Chiquvchi SAlardan chiquvchi paketlarni himoyalashda, kiruvchi SAlardan esa IPSec sarlovhali paketlarni ishlashda foydalaniladi. SAD ma'lumotlar bazasi SA bilan qo'lda yoki kalitlarni boshqarish protokollari IKE yordamida to'ldiriladi;

- xavfsizlik siyosatini va xavfsiz assotsiyatsiyalarni boshqarish. Bu SAni va xavfsizlik siyosatini boshqaruvchi ilovalardir.

Asosiy protokol IPSec (ESP va AHni amalga oshiruvchi) TCP/IP protokollarining transport va tarmoq steklari bilan o'zaro uzviy aloqada bo'ladi. IPSecni tarmoq sathining qismi deyish mumkin. IPSecning asosiy moduli ikkita interfeysni - kirish yo'li va chiqish yo'li interfeyslarni ta'minlaydi. Kirish yo'li

interfeysi kiruvchi paketlar tomonidan, chiqish yo‘li interfeysi esa chiquvchi paketlar tomonidan foydalaniladi. IPSecning amalga oshirilishi TCP/IP protokollar stekining transport va tarmoq sathlari orasidagi interfeysga bog‘liq bo‘lmasligi lozim.

SPD va SAD ma’lumotlar bazasi IPSec ishlashiga jiddiy ta’sir ko‘rsatadi. Ulardagi ma’lumotlar tuzilmasini tanlash IPsec ishlashining unumdorligiga ta’sir etadi.

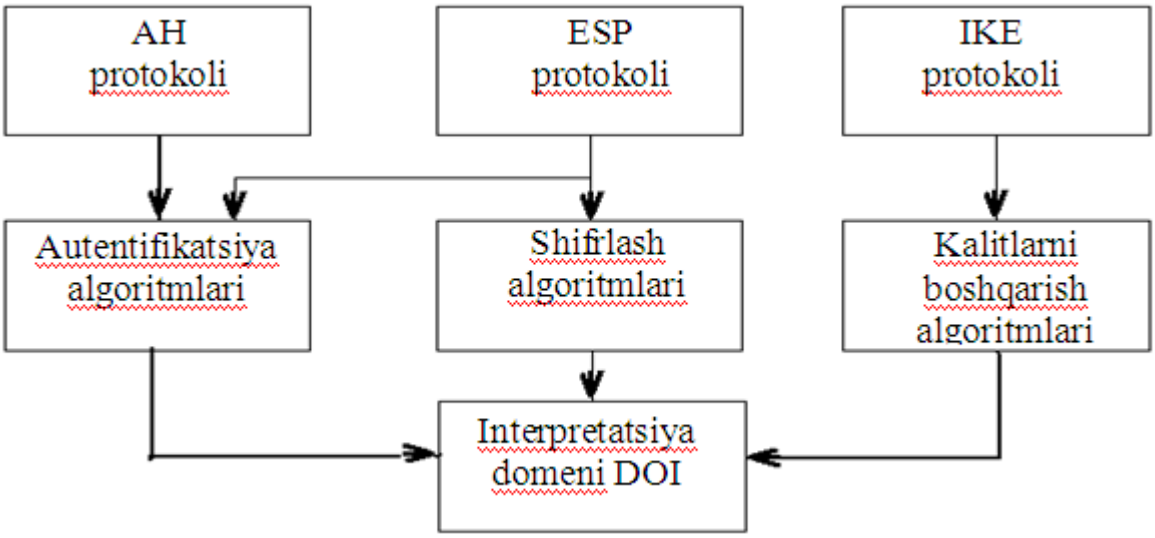
IPSec dagi barcha protokollarni ikkita guruhga ajratish mumkin:

- uzatiluvchi ma’lumotlarni bevosita ishlovchi (ularning xavfsizligini ta’minlash uchun) protokollar;

- birinchi guruh, protokollariga kerakli himoyalangan ulanishlar ko’rsatkichlarini avtomatik tarzda muvofiqlashtirishga imkon beruvchi proto-kollar.

IPSec yadrosini uchta AH, ESP virtual kanal va kalitlarni boshqarish IKE ko’rsatkichlarini muvofiqlashtiruvchi protokollar tashkil etadi.

IPSec xavfsizlik vositalarining arxitekturasi 5.8-rasmda keltirilgan.



5.8-rasm. IPSec protokollari stekining arxitekturasi

Arxitekturaning yuqori sathida quyidagi protokollar joylashgan:

- virtual kanal ko’rsatkichlarini muvofiqlashtiruvchi va kalitlarni boshqarish protokoli IKE. Bu protokol himoyalangan kanalni initsializatsiyalash

usulini, jumladan ishlatiluvchi kriptohimoyalash algoritmlarini muvofiqlashtirishni, hamda himoyalangan ulanish doirasida mahfiy kalitlarni almashish va boshqarish muolajalarini belgilaydi;

- sarlovhani autentifikatsiyalovchi protokol AH. Bu protokol ma'lumotlar manbaini autentifikatsiyalashni, ularning, qabul qilinganidan so'ng, yaxlitligini va xaqiqiyligini tekshirish, takroriy axborotlarning tiqishtirilishidan himoyani ta'minlaydi;

- himoyani inkapsulyatsiyalovchi protokol ESP. Bu protokol uzatiluvchi ma'lumotlarni kriptografik berkitishni, autentifikatsiyalashni va yaxlitligini ta'minlaydi, hamda takroriy axborotlarning tiqishtirilishidan himoyalaydi.

AH va ESP protokollarining har biri alohida va birgalikda ishlatilishi mumkin. Bu protokollarning vazifalari qisqacha bayonidan ko'rinib turibdiki, ularning imkoniyatlari qisman bir xil.

AH protokoli faqat ma'lumotlarni yaxlitligini va autentifikatsiyalashni ta'minlashga javob beradi. ESP protokoli kuchliroq hisoblanadi, chunki u ma'lumotlarni shifrlashi mumkin, undan tashqari AH protokoli vazifasini ham bajarishi mumkin.

IKE, AH va ESP protokollarining o'zaro aloqalari quyidagicha kechadi. Avval IKE protokoli bo'yicha ikkita nuqta orasida mantiqiy ulanish o'rnatiladi. Bu ulanish IPSec standartlarida "xavfsiz assotsiatsiya"-Security Association, SA nomini olgan. Ushbu mantiqiy kanal o'rnatilishida kanalning ohirgi nuqtalarini autentifikatsiyalash bajariladi, hamda ma'lumotlarni himoyalash ko'rsatkichlari, masalan, shifrlash algoritmi, sessiya mahfiy kaliti va x,. tanlanadi. So'ngra xavfsiz assotsiatsiya SA tomonidan o'rnatilgan doirada AH va ESP protokoli ishlay boshlaydi. Bu protokollar yordamida uzatiluvchi ma'lumotlarning istalgan himoyasi, tanlangan ko'rsatkichlardan foydalanilgan holda bajariladi.

IPSec arxitekturasining o'rta sathini IKE protokolida qo'llaniluvchi ko'rsatkichlarni muvofiqlashtirish va kalitlarni boshqarish algoritmlari hamda AH va ESP protokollarida ishlatiluvchi autentifikatsiyalash va shifrlash algoritmlari

tashkil etadi.

Ta’kidlash lozimki, IPSec arxitekturasining yuqori sathidagi virtual kanalni himoyalash protokollari (AH va ESP) muayyan kriptografik algoritmlarga bog‘liq emas. Autentifikatsiyalash va shifrlashning ko‘p sonli turli-tuman algoritmlaridan foydalanish imkoniyati tufayli IPSec tarmoqni himoyalashni tashkil etishning yuqori pog‘onada moslashuvchanligini ta’minlaydi. IPSecning moslashuvchanligi deganda har bir masala uchun uning yechilishini turli usullari tavsiya etilishi tushuniladi. Bir masala uchun tanlangan usul, odatda, boshqa masalalarni amalga oshirish usullariga bog‘liq emas. Masalan, shifrlash uchun DES algoritmining tanlanishi ma’lumotlarni autentifikatsiyalashda ishlatiluvchi daydjestni hisoblash funksiyasini tanlashga ta’sir qilmaydi.

IPSec arxitekturasining pastki sath interpretatsiyalash domeni DOI (Domain of Interpretation) dan iborat. Interpretatsiyalash domenining qo‘llanish zaruriyatiga quyidagilar sabab bo‘ldi. AH va ESP protokollari modulli tuzilmaga ega, ya’ni foydalanuvchilar o‘zaro kelishgan holda shifrlash va autentifikatsiyalashning turli kriptografik algoritmlaridan foydalanishlari mumkin. Shu sababli, barcha ishlatiluvchi va yangi kiritiluvchi protokol va algoritmlarning birgalikda ishlashini ta’minlovchi modul zarur. Aynan shu vazifalar interpretatsiyalash domeniga yuklatilgan.

Interpretatsiyalash domeni ma’lumotlar bazasi sifatida IPSecda ishlatiladigan protokollar va algoritmlar, ularning ko’rsatkichlari, protokol identifikatorlari va b. xususidagi axborotlarni saqlaydi. Mohiyati bo‘yicha interpretatsiyalash domeni IPSec arxitekturasida fundament rolini bajaradi. AH va ESP protokollarida autentifikatsiyalash va shifrlash algoritmlari sifatida milliy standartlarga mos keluvchi algoritmlardan foydalanish uchun bu algoritmlarni interpretatsiyalash domenida ro‘yxatdan o‘tkazish lozim.

AH yoki ESP protokollari uzatiluvchi ma’lumotlarni quyidagi ikkita rejimda himoyalashi mumkin:

- tunnel rejimda: IP paketlar butunlay, ularning sarlovhasi bilan birga himoyalanadi;

- transport rejimida: IP paketlarning faqat ichidagilari himoyalanadi.

Tunnel rejimi asosiy rejim hisoblanadi. Bu rejimda dastlabki paket yangi IP paketga joylanadi va ma’lumotlarni tarmoq bo‘yicha uzatish yangi IP-paket sarlovhasi asosida amalga oshiriladi. Tunnel rejimida ishlashda har bir oddiy IP-paket kriptohimoyalangan ko‘rinishda butunligicha IPSec konvertiga joylanadi. IPSec konverti, o‘z navbatida boshqa himoyalangan IP-paketga inkapsulyatsiyalanadi. Tunnel rejimi odatda maxsus ajratilgan xavfsizlik shlyuzlarida - marshrutizatorlar yoki tarmoqlararo ekranlarda amalga oshiriladi. Bunday shlyuzlar orasida himoyalangan tunnellar shakllantiriladi.

Tunnelning boshqa tomonida qabul qilingan himoyalangan IP-paketlar "ochiladi" va olingan dastlabki IP-paketlar qabul qiluvchi lokal tarmoq kompyuterlariga standart qoidalar bo‘yicha uzatiladi. IP-paketlarni tunnellash tunnellarni egasi bo‘lmish lokal tarmoqdagi oddiy kompyuterlar uchun shaffof hisoblanadi. Ohirgi tizimlarda tunnel rejimi masofadagi va mobil foydalanuvchilarni madadlash uchun ishlatilishi mumkin. Bu holda foydalanuvchilar kompyuterida IPSecning tunnel rejimini amalga oshiruvchi dasturiy ta’minot o’rnatilishi lozim.

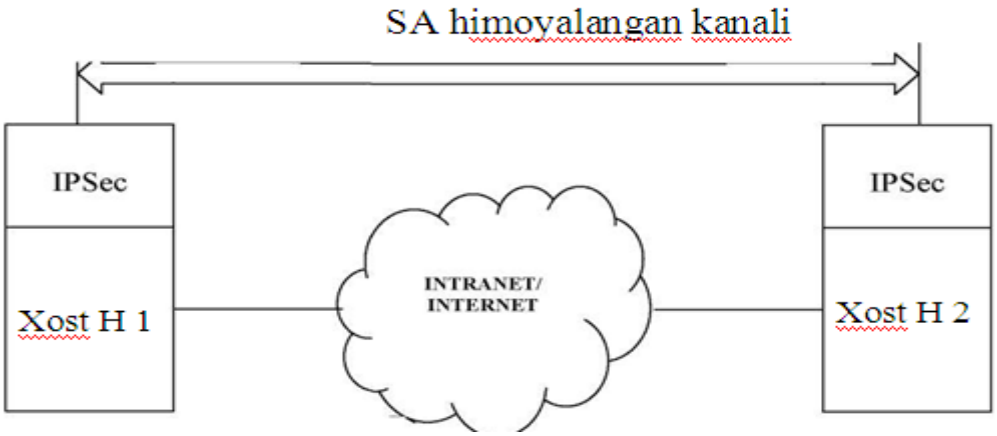
Transport rejimida tarmoq orqali IP-paketni uzatish bu paketning dastlabki sarlovhasi yordamida amalga oshiriladi. IPSec konvertiga kriptohimoyalangan ko’rinishda faqat IP-paket ichiga joylanadi va olingan konvertga dastlabki IP-sarlovha qo‘shiladi. Transport rejimi tunnel rejimiga nisbatan tezkor va ohirgi tizimlarda qo‘llanish uchun ishlab chiqilgan. Ushbu rejim masofadagi va mobil foydalanuvchilarni, hamda lokal tarmoq ichidagi axborot oqimini himoyalashni madadlashda ishlatilishi mumkin. Ta’kidlash lozimki, transport rejimida ishlash himoyalangan o’zaro aloqa guruhiga kiruvchi barcha tizimlarda o’z aksini topadi va aksariyat hollarda tarmoq ilovalarini qayta dasturlash talab etiladi.

Tunnel yoki transport rejimidan foydalanish ma’lumotlarni himoyalashga qo’yiladigan talablarga, hamda IPSes ishlovchi tugun roliga bog‘liq. Himoyalanuvchi kanalni tugallovchi tugun-xost(ohirgi tugun) yoki shlyuz

(oraliqdagi tugun) bo'lishi mumkin. Mos holda, IPSecni qo'llashning quyidagi uchta asosiy sxemasi farqlanadi:

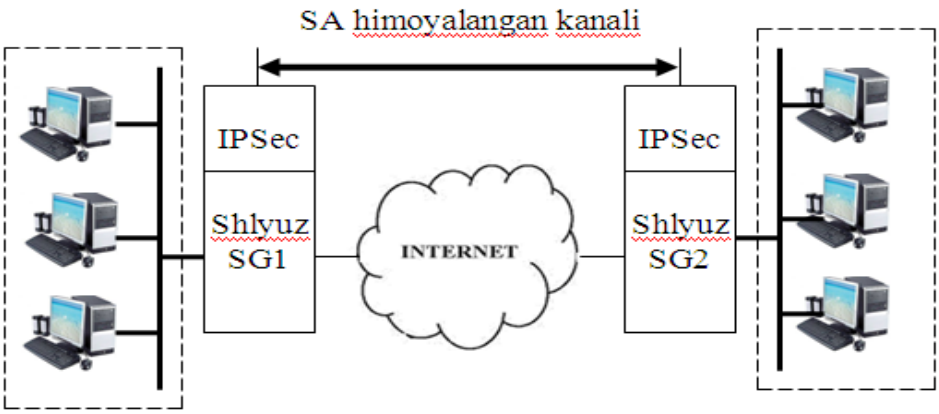
- "xost - xost";
- "shlyuz - shlyuz";
- "xost - shlyuz";

Birinchi sxemada himoyalangan kanal tarmoqning ohirgi ikkita tuguni, ya'ni HI va H2 xostlar orasida o'rnatiladi (5.9 - rasm), IPSecni madadlovchi xostlar uchun transport hamda tunnel rejimlaridan foydalanishga ruxsat beriladi.



5.9 - rasm. "Xost-xost " sxemasi

Ikkinchi sxemaga binoan, himoyalangan kanal har birida IPSec protokoli ishlovchi, xavfsizlik shlyuzlari SG1 va SG2 (Security Gateway) deb ataluvchi oraliqdagi ikkita tugunlar orasida o'rnatiladi (5.10 - rasm).

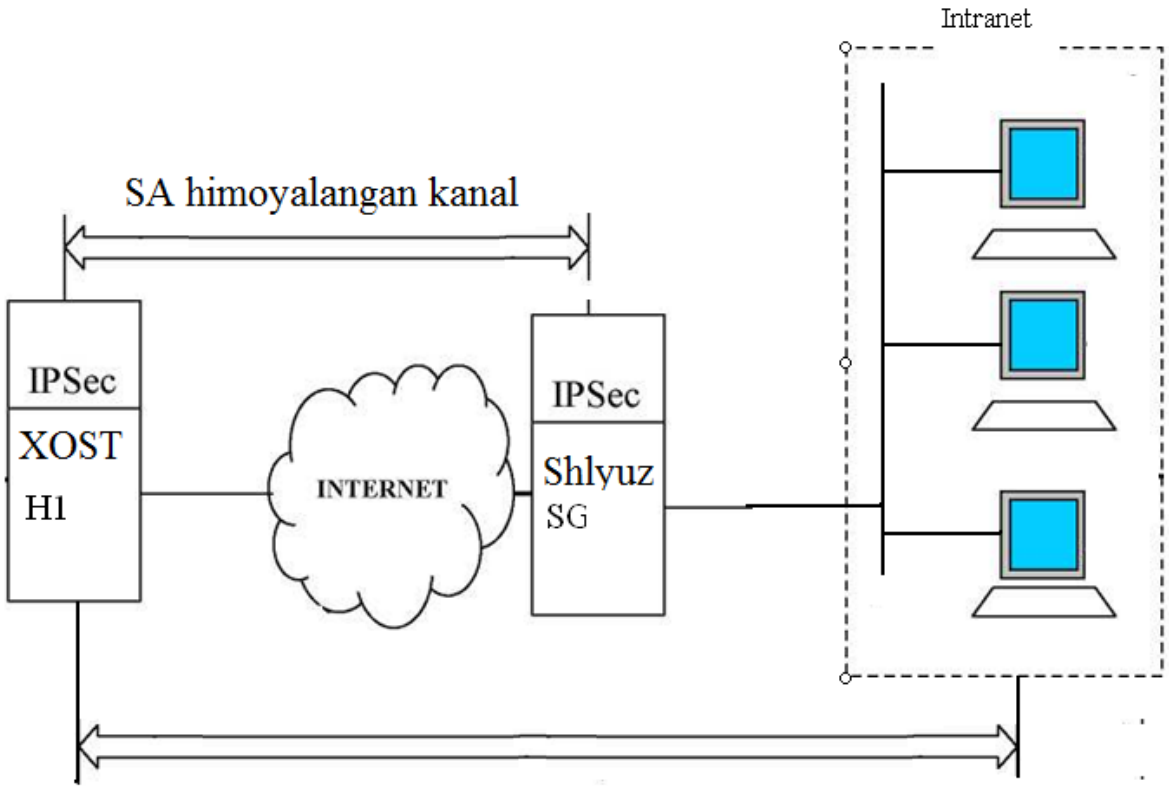


5.10 - rasm. "Shlyuz-shlyuz" sxemasi

Xavfsizlik shlyuzi ikkita tarmoqqa ulanuvchi tarmoq qurilmasi bo’lib, o’zidan keyin joylashgan xostlar uchun shifrlash va autentifikatsiyalash funksiyalarini bajaradi. VPNning xavfsizlik shlyuzi alohida dasturiy mahsulot, alohida apparat qurilma hamda VPN funksiyalari bilan to‘ldirilgan marshrutizator yoki tarmoqlararo ekran ko‘rinishida amalga oshirilishi mumkin.

Ma’lumotlarni himoyalangan almashish tarmoqlarga ulangan, xavfsizlik shlyuzlaridan keyin joylashgan har qanday ikkita ohirgi tugunlar orasida ro’y berishi mumkin. Ohirgi tugunlardan IPSec protokolni madadlash talab qilinmaydi, ular o’zlarining trafigini himoyalanmagan holda korxonaning ishonchli tarmog‘i Intranet orqali uzatadi. Umumfoydalanuvchi tarmoqqa yuboriluvchi trafik xavfsizlik shlyuzi orqali o’tadi va bu shlyuz o’zining nomidan IPSec yordamida trafikni himoyalashni ta’minlaydi. Shlyuzlarga faqat tunnel rejimida ishlashga ruxsat beriladi, garchi ular transport rejimini ham madadlashlari mumkin (bu holda samara kam bo‘ladi).

"Xost - shlyuz" sxemasi ko’pincha himoyalangan masofadan foydalanishda ishlatiladi (5.11-rasm).



5.11-rasm. "Xost-xost"kanali bilan to‘ldirilgan "xost-shlyuz" sxemasi

Bu yerda himoyalangan kanal IPSec ishlovchi masofadagi H1 xost va korxona Intranet tarmog‘iga kiruvchi barcha xostlar uchun trafikni himoyalovchi SG shlyuz orasida tashkil etiladi. Masofadagi xost shlyuzga paketlarni junatishda ham transport va ham tunnel rejimlaridan foydalanishi mumkin, shlyuz esa xostga paketlarni faqat tunnel rejimida junatadi.

Bu sxemani masofadagi H1 xost va shlyuz tomonidan himoyalanuvchi ichki tarmoqqa tegishli biror H2 xost orasida parallel yana bir himoyalangan kanalni yaratib modifikatsiyalash mumkin. Ikkita SAdan bunday kombinatsiyadan foydalanish ichki tarmoqdagi trafikni ham ishonchli himoyalashga imkon beradi.

Ko’rilgan IPSec asosida himoyalangan kanalni qurish sxemalari turli-tuman VPNlarni yaratishda keng qo‘llaniladi. IPSec asosida turli arxitekturaga ega bo‘lgan VPN, jumladan masofadan foydalanuvchi VPN (Remote Access VPN), korporatsiya ichidagi VPN (Intranet VPN) va korporatsiyalararo VPN (Extranet VPN) quriladi.

IPSec asosidagi VPN-texnologiyalarining jozibaliligini quyidagi sabablar orqali izohlash mumkin:

- tarmoq satxining himoyasi tarmoqda ishlovchi barcha tadbiq etish tizimlari uchun shaffof, ya’ni barcha ilovalar himoyalangan tarmoqda hech qanday tuzatishsiz va o’zgarishsiz xuddi ochiq tarmoqda ishlaganidek ishlayveradi;

- himoyalash tizimining masshtablanuvchanligi ta’minlanadi, ya’ni murakkabligi va unumdorligi turli bo‘lgan ob’ektlarni himoyalash uchun murakkabligi, unumdorligi, narhi, pog‘onasi bo‘yicha adekvat bo‘lgan himoyalashning dasturiy yoki dasturiy-apparat vositalaridan foydalanish mumkin;

- masshtablanuvchi qatordagi axborotni himoyalash mahsulotlari birga ularni turli sathdagi ob’ektlarda (masofadagi yagona terminallardan to ixtiyoriy masshtabli lokal tarmoqlargacha) resurslaridan va trafigidan barcha begonalar foydalana olmaydigan yagona korporativ tarmoqqa birlashtirish mumkin.

PPTP protokoli

Kanal sathidagi VPN. OSI modelining kanal sathida ishlatiluvchi VPN vositalari uchinchi (va yuqoriroq) sathning turli xil trafigini inkapsulatsiyalashni ta’minlashga va «nuqta-nuqta»lidagi virtual tunnellarni (marshrutizatordan marshrutizatorga yoki shaxsiy kompyuterdan lokal hisoblash tarmog‘ining shlyuzigacha) qurishga imkon beradi. Bu guruhga L2F (Layer 2 Forwarding) va PPTP (Point-to-Point Tunneling Protocol) protokollari hamda Cisco Systems va Microsoft firmalarining birga ishlab chiqqan L2TP (Layer 2 Tunneling Protocol) standartidan foydalanuvchi VPN-mahsulotlar taalluqli.

Himoyalangan kanalning protokoli PPTP «nuqta-nuqta» ulanishlarida, masalan, ajratilgan liniyalarda ishlaganda qo‘llaniluvchi PPP protokoliga asoslangan. PPTP protokoli ilovalari va tadbiqiy sath xizmatlari uchun himoya vositalarining shaffofligini ta’minlaydi va tarmoq sathida ishlatiluvchi protokolga bog‘liq emas. Xususan, PPTP protokoli ham IP tarmoqlarida, ham IPX, DECnet yoki NetBEUL protokollari asosida ishlovchi tarmoqlarda paketlarni tashishi mumkin. Ammo, PPP protokoli hamma tarmoqlarda ham ishlatilmasligi sababli (aksariyat lokal tarmoqlarida kanal sathida Ethernet protokoli ishlasa, global tarmoqlarda IP/MPLS protokollari ishlaydi), uni universal vosita deb bo‘lmaydi. Yirik tarmoqlarning turli qismlarida, umuman aytganda, turli kanal protokollari ishlatiladi. Shu sababli bu geterogen muhit orqali kanal sathining yagona protokoli yordamida himoyalangan kanalni o‘tkazishi mumkin emas.

PPTP protokolining ma’lumotlarni IP, IPX va NetBEUL protokollari bo‘yicha almashish uchun himoyalangan kanallarni yaratishga imkon beradi. Ushbu protokollarning ma’lumotlari PPP kadrlariga joylanadi va PPTP protokoli vositasida IP protokolining paketlariga inkapsulyatsiyalanadi va shu protokol yordamida shifrlangan ko‘rinishda har qanday TCP/IP tarmog‘i orqali tashiladi (5.12 - rasm).

Uzatilaligan kadr sarlavhasi	IP sarlavhasi	GRE sarlavha	PPP sarlavha	Shifrlangan ma’lumot	Uzatilaligan kadr oxiri

5.12 – rasm. PPTP tunneli bo‘yicha jo‘natiluvchi paket tuzilishi

- Internet ichida ishlatiluvchi kanal sathining sarlovhasi, masalan, Ethernet kadrining sarlovhasi;

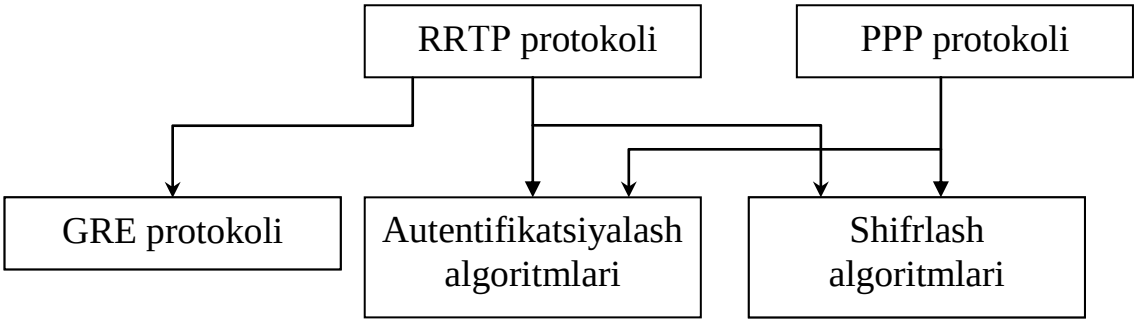
- tarkibida paketni jo‘natuvchi va qabul qiluvchi manzillari bo‘lgan IP sarlovhasi;

- marshrutlash uchun inkapsulyatsiyalashning umumiy usulining sarlovhasi GRE (Generic Routing Encapsulation);

- tarkibida, IPX yoki NetBEUL paketlari bo‘lgan dastlabki paket PPP.

Tarmoqning qabul qiluvchi tuguni IP paketlardan PPP kadrlarni chiqarib oladi, so‘ngra PPP kadrdan dastlabki paket IP, IPX yoki NetBEUL paketini chiqarib olib uni lokal tarmoq bo‘yicha muayyan manzilga jo‘natadi. Kanal sathining inkapsulyatsiyalovchi protokollarining ko‘p protokolliligi (unga PPTP protokol ham taalluqli), ularning yanada yuqoriroq sathning himoyalangan kanal protokollaridan afzalligidir. Masalan, agar korporativ tarmoqda IPX yoki NetBEUL ishlatilsa, IPSec yoki SSL protokollarini ishlatib bo‘lmaydi, chunki ular IP tarmoq sathining faqat bitta protokoliga mo‘ljallangan.

Inkapsulyatsiyalashning mazkur usuli OSI modelining tarmoq sathi protokollariga bog‘liq bo‘lmaslikni ta’minlaydi va ochiq IP-tarmoqlar orqali har qanday lokal tarmoqlardan (IP, IPX yoki NetBEUL) himoyalangan masofadan foydalanishni amalga oshirishga imkon beradi. PPTP protokoliga muvofiq himoyalangan virtual kanal yaratishda masofadagi foydalanuvchini autentifikatsiyalash va uzatiluvchi ma’lumotlarni shifrlash amalga oshiriladi (5.13-rasm).



5.13-rasm. PPTP protokolining arxitekturasi

Masofadagi foydalanuvchini autentifikatsiyalashda PPP uchun qo‘llaniladigan turli protokollardan foydalanish mumkin. Microsoft kompaniyasi tomonidan Windows 98/XP/NT/2000ga kiritilgan PPTPning amalga oshirilishida autentifikatsiyalashning quyidagi protokollari madadlanadi: parol bo‘yicha aniqlash protokoli PAP (Pasword Athentication Protocol), qo‘l berishishda aniqlash protokoli MSCHAP (Microsoft Challenge - Handshaking Authentication Protocols) va aniqlash protokoli EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). PAP protokolidan foydalanilganda identifikatorlar va parollar aloqa liniyalari orqali shifrlanmagan ko‘rinishda uzatiladi, bunda autentifikatsiyalashni faqat server o‘tkazadi. MSCHAP va EAP-TLS protokollaridan foydalanilganda niyati buzuq odamning ushlab qolingan shifrlangan parolli paketdan qayta foydalanishidan himoyalash mijoz va VPN-serverni augentifikatsiyalash ta’minlanadi.

PPTP yordamida shifrlash Internet orqali jo‘natishda ma’lumotlardan hech kim foydalana olmasligini kafolatlaydi. Shifrlash protokoli MPPE (Microsoft Point-to-Point Encryption) faqat MSCHAP(1 va 2 versiyalari) va EAP-TLS bilan birga ishlay oladi. Mijoz va server orasida ko’rsatkichlarni muvofiqlashtirilishida shifrlash kalitining uzunligini avtomatik tarzda tanlay oladi. MPPE protokoli uzunligi 40, 56 yoki 128 bit bo‘lgan kalitlar bilan ishlashni amalga oshiradi.

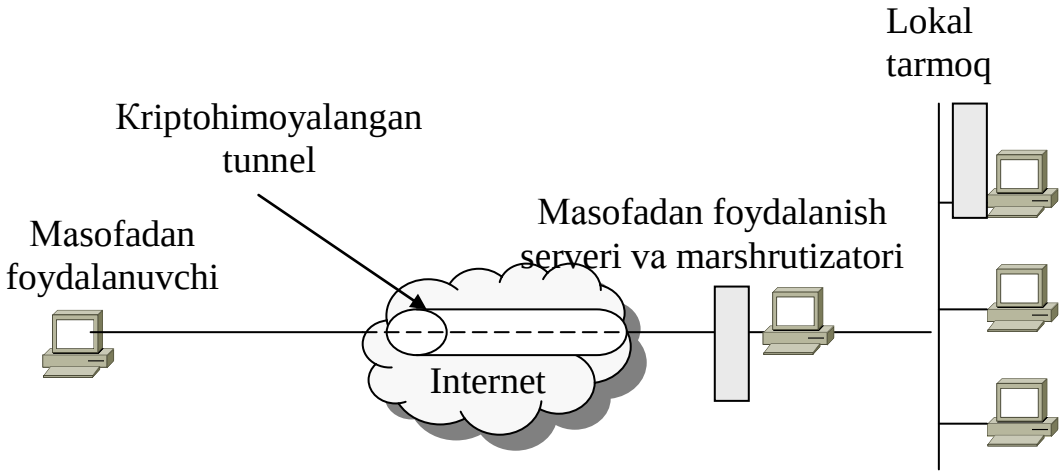
PPTP protokoli har bir olingan paketdan so‘ng shifrlash kalitining qiymatini o‘zgartiradi.

PPTP protokolini qo‘llashning quyidagi ikkita asosiy sxemasi aniqlangan:

- masofadan foydalanuvchining Internet bilan to‘g‘ridan-to‘g‘ri ulanishidagi tunnellash sxemasi;

- masofadan foydalanuvchining Internet bilan provayder orqali telefon liniyasi bo‘yicha ulanishidagi tunnellash sxemasi.

Tunnellashning birinchi sxemasi amalga oshirilganida (5.14-rasm) masofadan foydalanuvchi Windows 98/XP/NT tarkibidagi masofadan foydalanish servisi RAS (Remote Access Service)ning mijoz qismi yordamida lokal tarmoq bilan masofaviy bog‘lanishni o‘rnatadi. So‘ngra foydalanuvchi lokal tarmoqdan masofadan foydalanish serveriga, uning IP manzilini ko‘rsatib murojaat etadi va u bilan PPTP protokoli bo‘yicha aloqa o‘rnatadi.



5.14-rasm. Masofadan foydalanuvchi kompyuterini Internetga to‘g‘ridan to‘g‘ri ulanishidagi tunnellash sxemasi

Ta’kidlash lozimki, L2F texnologiyasidan foydalanilganda provayderning masofadan foydalanish serveri foydalanuvchini autentifikatsiyalashni faqat virtual kanal yaratilishi zarurligini aniqlash va istalgan lokal tarmoqning masofadan foydalanish serveri manzilini topishda ishlatadi. Haqiqiylikni yakuniy tekshirish lokal tarmoqning masofadan foydalanish serveri tomonidan u bilan provayder serveri ulanganidan so‘ng bajariladi.

L2F protokolining quyidagi kamchiliklarini ko‘rsatish mumkin:

- unda IP protokolining joriy versiyasi uchun axborot almashinuvining ohirgi nuqtalari orasida kriptohimoyalangan tunnel yaratish ko‘zda tutilmagan;

- virtual himoyalangan kanal faqat provayderning masofadan foydalanish serveri va lokal tarmoqning chegara marshrutizatori orasida yaratilishi mumkin. Bunda masofadagi foydalanuvchi kompyuteri bilan provayder serveri orasidagi joy ochiq qoladi.

L2TP protokoli

Hozirda L2F protokoli Internet standarti loyihasi maqomiga ega bo‘lgan L2TP protokoliga singdirilgan.

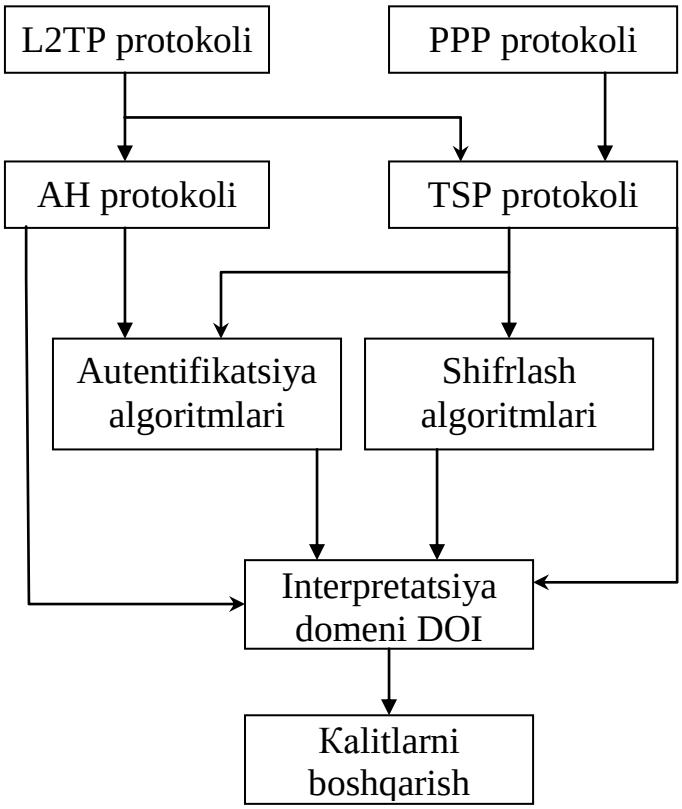
L2TP protokoli IETF tashkilotida Microsoft va Cisco Systems kompaniyalarining yordamida ishlab chiqilgan. L2TP protokoli ixtiyoriy muhitli tarmoq orqali PPP-trafikni uzatishda himoyalangan tunnellash protokoli sifatida ishlab chiqilgan.

PPTPdan farqli holda L2TP protokoli IP protokoliga bog‘langan emas, shu sababli undan paketlarni kommutatsiyalovchi tarmoqlarda, masalan, ATM yoki FR tarmoqlarda foydalanish mumkin.

L2TP protokolida PPTP va L2F protokollarining nafaqat yaxshi xususiyatlari birlashtirilgan, balki yangi funksiyalar, jumladan, IPSec protokollari stekining AN va ESP protokollari bilan ishlash imkoniyati qo‘shilgan. L2TP protokolining arxitekturasi 5.15 - rasmda keltirilgan.

AH va ESP protokollari foydalanuvchilarning, kelishilgan holda, shifrlash va autentifikatsiyalashning turli kriptografik algoritmlarini ishlatishlariga yo‘l qo‘yadi. Interpretatsiya domeni DOT (Domain of Interpretation) ishlatiluvchi protokollar va algoritmlarning birga ishlashini ta’minlaydi.

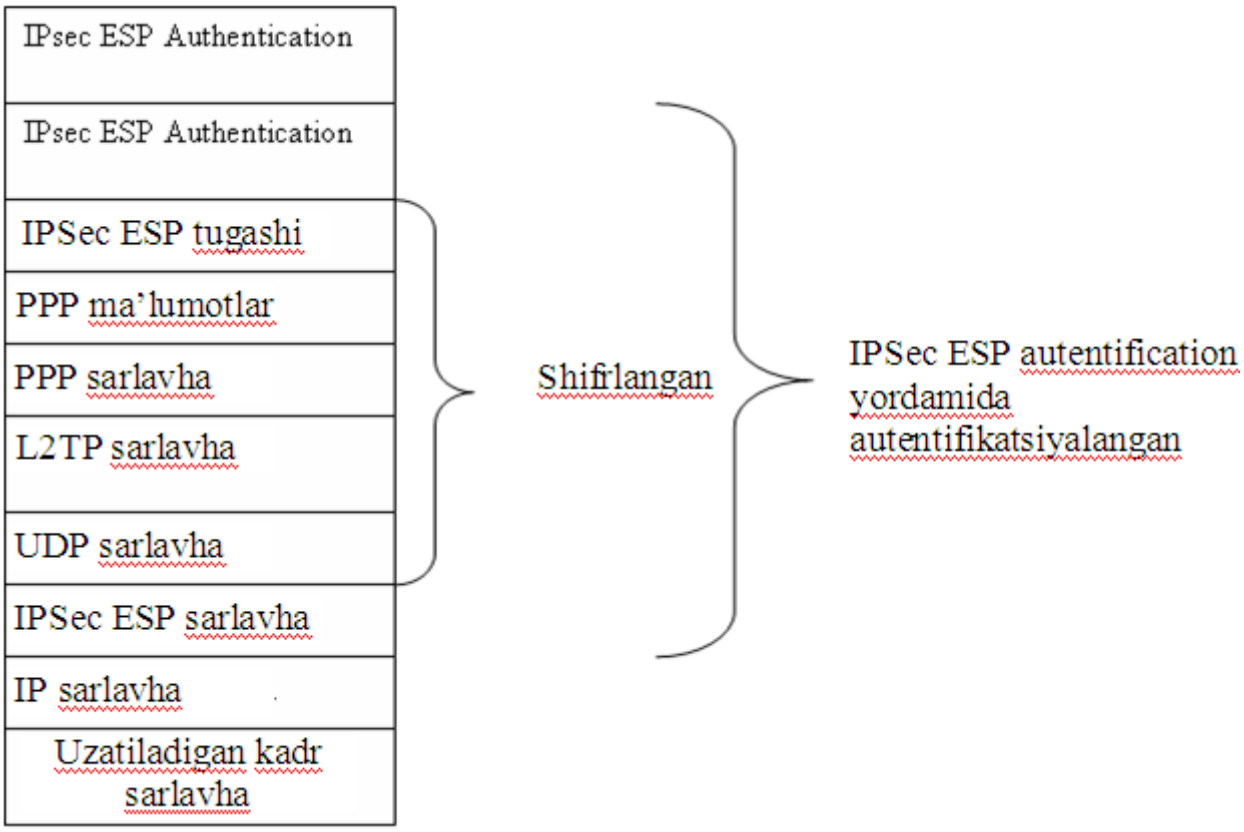
Mohiyati bo‘yicha, gibrid protokol L2TP masofadagi foydalanuvchilarni autentifikatsiyalash, himoyalangan virtual ulanishni yaratish va ma’lumotlar oqimlarini boshqarish funksiyalari bilan L2TP protokoli transport sifatida UDP protokolini ishlatadi, tunnelni boshqarishda va ma’lumotlarni tashishda xabarlarning bir xil formatidan foydalanadi.



5.15 – rasm. L2TP protokolining tuzilishi

PPTP protokolidagidek, L2TP protokoli tunnelga uzatish uchun paketni yig‘ishda avval PPP axborot ma’lumotlari maydoniga PPP sarlovhasini, so‘ngra L2TP sarlovhasini qo‘shadi. Shu tariqa olingan paket UDP protokol tomonidan inkapsulyatsiyalanadi. L2TP protokol jo‘natuvchi va qabul qiluvchi porti sifatida UDP-portidan foydalanadi.

5.16-rasmda L2TP tunneli bo‘yicha jo‘natiluvchi paket tuzilmasi keltirilgan.



5.16– rasm. L2TP tunneli bo‘ylab jo‘natiladigan paket tuzilishi

IPSec protokollar steki xavfsizlik siyosatining tanlangan xiliga bog‘liq holda L2TP protokoli UDP-xabarni shifrlashi va unga ESPning sarlovhasini va ohirini, hamda IPSec ESP Authenticationning ohirini qo‘shishi mumkin. So‘ngra inkapsulyatsiyalash bajariladi. Tarkibida jo‘natuvchi va qabul qiluvchi manzillari bo‘lgan IP-sarlovha qo‘shiladi. Ohirida L2TP ma’lumotlarni uzatishga tayyorlash uchun ikkinchi PPP-inkapsulyatsiyalashni bajaradi.

Kompyuter - qabul qiluvchi ma’lumotlarni qabul qiladi. PPPning sarlovhasi va ohirini ishlaydi. IP sarlovhani olib tashlaydi. IPSec ESP Authentication yordamida IPning axborot maydoni autentifikatsiyalanadi. IPSec ESP protokoli esa paketning shifrlashni ochishda yordam beradi. Keyin kompyuter UDP sarlovhasini ishlaydi va tunnelni identifikatsiyalash uchun L2TP sarlovhasidan foydalanadi. Endi PPP paketning tarkibida faqat foydali ma’lumotlar bo‘ladi, ular ishlanadi va ko‘rsatilgan qabul qiluvchiga yuboriladi.

L2TP protokoli «foydalanuvchi» va «kompyuter» sathlarda autentifikatsiyalashni ta’minlaydi hamda ma’lumotlarni autentifikatsiyalaydi va shifrlaydi. Mijozlarni va VPN serverlarini autentifikatsiyalashning birinchi bosqichida L2TP sertifikatsiya xizmatidan olingan lokal sertifikatlardan foydalanadi.

L2TP kompyuterni autentifikatsiyalashni tugatganidan so‘ng, foydalanuvchi sathda autentifikatsiyalashda foydalanuvchi ismini va parolni ochiq ko‘rinishda uzatuvchi har qanday protokol, xatto PAP ishlatilishi mumkin. Bu tamomila xavfsiz, chunki L2TP butun sessiyani shifrlaydi. Ammo foydalanuvchini autentifikatsiyalashni, kompyuter va foydalanuvchini autentifikatsiyalashda turli kalitlardan foydalanuvchi MSCHAP yordamida o‘tkazish xavfsizlikni oshirishi mumkin.

L2TP protokolining taxmini bo‘yicha provayderning masofadan foydalanish serveri va korporativ tarmoq marshrutizatori orasida tunnel hosil qiluvchi sxemalardan foydalaniladi.

IPSec protokoli asosan IP tarmoqlarda ma’lumotlarni xavfsiz uzatishni ta’minlaydi. IPSecning ishlatilishi quyidagilarni kafolatlaydi:

- uzatilayotgan ma’lumotlarning yaxlitligini, ya’ni ma’lumotlar uzatilishida buzilmaydi, yo‘qolmaydi va takrorlanmaydi;

- uzatiladigan ma’lumotlarning mahfiyligini, ya’ni ma’lumotlar shunday shaklda uzatiladiki, ularni ruxsatsiz ko‘zdan kechirishning oldi olinadi.

5.3. QoSni ta’minlash usullari

Paketli kommutatsiya tarmog‘ida ovoz va video xabarlarini uzatishda katta texnik muamolardan biri ovoz va tasvirlarni buzilishsiz va shovqinsiz olishga yordam beruvchi kafolatli xizmat ko‘rsatish sifati (QoS)ni ta’minlash hisoblanadi. Aksariyat paketli kommutatsiya tarmoqlarida signalni kechikishiga sezgir bo‘lmagan ilova va vazifalarni bajarish qurilgan. Ovoz va video xabarlar ma’lumot uzatish tezlgiga nisbatan juda talabchandir. Paketni kechikishi 200 ms dan ortsa,

bu degani paketni vaqti o‘tdi, kerak emas, ma’lumotlar eskirib bo‘lganlgini bldiradi. Ovoz va video xabarlarini uzatish uchun tarmoq qurilgan, ishlab chiqilgan bo‘lishi kerak. Shu bilan birga ekspluatatsiya qilishda real vaqtda paketlarni o‘tish samaradorligini maksimal oshirish keak.

Shak shubhasiz o‘tkazish yo‘lagini katta yuklanishini videotrafik tashkil qiladi. Ma’lumki, bugungi kunda televideniya xabarlarini uzatish va so‘rov bo‘yiicha videoning bitta kanalini uzatish 4 Mbit/s da uzatishni talab qiladi. Vaziyat sezilarli pog‘onada o‘zgaradi, qachonki MPEG – 4 standartida o‘tish amalga oshirilganda. Lekin har qanday holatda videotrafik uchun sifatli tasvirni olish uchun qo‘shimcha 2 Mbit/s ni zahiralash kerak bo‘ladi.

Muammolar qachonki, global tarmoq (WAN) orqali uzatilayotgan signalni sifatini qo‘llab quvvatlashi kerak bo‘lganda ko‘payadi. Lokal tarmoq 10, 100 Mbit/s va 1 Gbit/s oddiy tezligi WANga kirishda yuqori narhda bo‘lganligi uchun ishlatilmaydi, chunki global tarmoqqa murojaat qilish tezligi 1,45 Mbit/s va undan past bo‘lgan tezlikni tashkil qiladi. Elektron pochta va boshqa turdagi ma’lumotlarni almashish bu qandaydir kechikishga ega, ammo bu muhim ahamiyatga ega emas. Ovoz va video xabarlarni uzatish uchun o‘tkazish yo‘lagining bir qismini zahiralash kerak, aks holda xizmatni olish fikri to‘laliligicha yo‘qotiladi.

Multimedali xabarlarni uzatishda QoS asosiy talab hisoblanadi. Qanday qilib paketlarni tashlab yubormasdan yoki kechikishsiz har xil turdagi trafikning paketlarini kafolatli uzatish muhim vazifa hisoblanadi.

QoS uchun asosiy tavsiflar quyidagilar:

- paketlarni yetkazishning kechikishi. Bu ko‘rsatkich asosan video va ovoz xabarlarini uzatishda asosiy ahamiyatga ega;
- djitter – paketlarni yetkazishda kechikishni o‘zgarishi. Djitterni bir nechta usullar bilan hisoblash mumkin. Djitterni hisoblash quyidagi tavsiyanomalarda aniqlangan:

- IETF RFC 3550 RTP: A Transport Protocol for Real-Time Applications;
- IETF RFC 3611 RTP: Control Protocol Extended Reports (RTCP XR);

- paketlarni yo‘qolishi – tarmoqni o‘ta yuklanishi natijasida alohida paketlar tashlab yuboriladi. Ovoz va video xabarlarni uzatishda asosiy ko‘rsatkich hisoblanadi.

Ovoz, video va ma’lumotlarni uzatish uchun xizmat ko‘rsatish sifati

Ovoz xabarlarini uzatish uchun QoS talabi video xabarlarni uzatish talabiga nisbatan osonroq.

XEAI va IETF (XEAI G.711, G.726, G.728, G.729, G.114, H.264, H.261; RFC 3261 The Internet Assigned Number Authority Header Field Parameter Registry for the Session Initiation Protocol) tavsiyanomalarini taxlil qilish ovoz xabarlarini uzatishni amalga oshirishda QoS tavsiflariga talablarni umumlashtirishga yordam beradi.

1. Ovoz trafigi RFC 3246 tavsiyanomasiga muvofiq DSCP EF ko‘rinishida belgilanishi kerak.

2. Signalizatsiya CS 3 ko‘rinishida belgilanishi (rivojlantirish vaqtida AF31 ni ishilatishi mumkin)

3. Yuqori sifatli VoIP xizmatini taqdim etish uchun magistrallarda paketlarni yo‘qolishi 0.25 % dan oshmasligi kerak.

4. Bir tomonlama kechikish XEAIning G.114 tavsiyanomasiga muvofiq 150 ms dan oshmasligi kerak.

5. Kechikishni o‘zgarishi (djitter) 10 ms dan ko‘p bo‘lmasligi kerak. Maksimal djitter belgilangan kechikishdan kam bo‘lishi kerak. Bu kechikishning tebranish qiymati minimal tarmoq kechikishini ayirmasiga teng. VoIP uchun bu qiymat 10 ms deb qabul qilingan. Bu G.114 tavsiyanomasida ko‘rsatilgan 150 ms ga nisbatan yetarli hisoblanadi. Bu qiymatdan biz magistral bo‘yicha tarqalish vaqti (30 ms) va kodekning kechikishi (35 ms) bizga 35 ms li djitter uchun beradi. Bu 35 ms dan 30 ms kirish (15 ms) uchun va 5 ms magistral uchun sarflanadi,

ya’ni moslashgan djitter – buferlar uchun kechikishni tebranishi 10 ms dan kam bo‘lishi kerak.

6. Har bir so‘zlashuv uchun ikkinchi pog‘onaning sarlovhasi va kodekning (kvantlash chastotasiga bog‘liq) 20 – 106 Kbit/s kafolatli imtiyozli o‘tkazish yo‘lagini talab qiladi.

7. Signalizatsiya trafigi uchun 150 bit/s (ikkinchi pog‘onaning sarlovhasini qo‘shganda) kafolatli o‘tkazish yo‘lagini talab qiladi.

Kanalning o‘tkazish yo‘lagini samarali ishlatishning muhim faktorlaridan biri ovoz xabarlarini optimal kodlash/dekodlash – kodekini tanlash hisoblanadi.

8. Impuls kodli modulyatsiya (IKM) va adaptiv differensial impuls kodli modulyatsiya (ADIKM) kodeklari bugungi kunda an’anaviy telefon tizimlarida qo‘llanilmoqda. Aksariyat hollarda raqamli analog o‘zgartirgich (RAO‘) / analog raqamli o‘zgartirgich (ARO‘)ni o‘zida mujassamlashtirgan.

9. Radio traktni o‘tkazish yo‘lagiga talabni so‘ndirish ovoz signallarini vokoderli o‘zgartirish kodeklari uchun mobil aloqa tizimlarida vujudga keldi. Bu guruhdagi kodeklar axborot asosida signalning garmonik sintezini ishlatadi. Uning vokal tashkil etuvchisi fonemlar hisoblanadi. Bu kodeklar ko‘pincha analog qurilmalarda qo‘llaniladi.

10. Kombinatsiyalashgan (gibridli) kodeklar vokoderli o‘zgartirishlar ovozni sintez qilish texnologiyasini o‘zida qamrab olgan, lekin maxsus DCP vositalar yordamida raqamli qurilmalarda qo‘llanilmoqda. Bunday turdagi kodeklar IKM yoki ADIKM kodekini o‘zida mujassamlashtirgan.

5.1 – jadvalda turli kodeklarni ishlatishda ovoz sifatini baholash to‘g‘risida ma’lumot keltirilgan.

5.1 – jadval.

Har xil kodeklarni qo‘llash orqali ovoz sifatini baholash

Ovoz kodeki	**Tezlik, Kbit/c**	**MOS – bahosi**
G.711	64	4.10
G.726	32	3.85
G.728	16	3.61

5.1 – jadval davomi

G.729	8	3.92
G.729a	8	3.70
G.729.1	6.3	3.9

IP telefoniyada qo‘llaniladigan aksariyat kodeklar H.323 standartida yozilgan (5.2 – jadval). Me’yoriy xujjatlar asosida ovoz xabarlari xizmatlarining qurilmalarida kodlash / dekodlashda minimal kechikish va qabul qilsa bo‘ladigan xabarlarni sifatini ta’minlash maqsadida 32 Kbit/s li ADIKM usulini qo‘llash tavsiya qilinadi. Ushbu kodlash usuli asosiy deb hisoblanishi kerak.

5.2 – jadval.

H.323 oilasiga mansub kodeklarning tavsifi

Kodek	**Kodek tipi**	**Kodlashtirish tezligi, Kbit/c**	**Kodlashtirish vaqtida kechikish**
G.711	IKM	64	0.75
G.726	ADIKM	32	3.85
G.728	LD-CELP	16	3.61
G.729	CS-ACELP	8	3.92
G.726a	CS-ACELP	8	3.70
G.723.1	MP-MLQ	6.3	3.9
G.723.1	ACELP	5.3	

Internet tarmog‘ida ma’lumot uzatish uchun xizmat ko‘rsatish sifatiga talab

Ma’lumotlarni uzatish uchun tarmoqdagi dasturiy ta’minotning talabini inobatga olish kerak.

Internet tarmog‘ida ma’lumot uzatishni xizmat ko‘rsatish sifati bo‘yicha

talabini bajarish uchun quyidagilarni amalga oshirish kerak:

- tarmoqda dasturiy ta’minotning talabini hisobga olish;
- ishlab chiqarilgan quvvatni yuklanishini asosiy o‘tkazish qobiliyatiga mos kelishini rejalashtirishni bajarish;
- to‘rttadan ko‘p bo‘lmagan trafikning ajratilgan sinfini qo‘llash;
- lokal – aniqlangan muhim sinf (juda muhim ilovalar uchun), yuqori imtiyozli tranzaksiyali va interaktiv ilova;
- tranzaksiyali / interaktiv sinf – mijoz – xizmat ilovasi, xabarni uzatish bo‘yicha ilova;
- hajmli sinf (Bulk) – elektron pochta (E-mail), sinxronizatsiya, katta hajmdagi fayllarni uzatish;
- imkoniyat bo‘yiicha sinf (Best Effort) – tinchlik bo’yicha barcha belgilanmagan trafiklar uchun sinf.

Lokal – aniqlangan termini – har bir mijoz uchun katta bo‘lmagan biznes – imtiyozga ega bo‘lgan tranzaksiyali va interaktiv ilovalar uchun xizmatning yuqori sinfi. Bu sinf kam sondagi ilovalarga tayinlanadi.

Tranzaksiyali / interaktivli – bu ikkita o‘hshash ilovalarning kombinatsiyasi: mijoz – server tranzaksiya ilovalari va interaktiv ilovalarni tranzaksiyasi. Interaktiv bo‘lmagan ilovalar uchun mo‘ljallangan. Bu ilovalar foydalanuvchi bajarilgan jarayonni natijasini kutmaydigan FTP, sinxronizatsiya, video ma’lumotlarni tarqalish yoki boshqa turdagi ilovalarni o‘z ichiga oladi.

Imkoniyat bo‘yicha so‘rov (Best Effort) – internet tarmog‘ining barcha turdagi ma’lumotlar trafigi uchun mo‘ljallangan. Faqat agar ilova alohida qayta ishlash uchun olingan bo‘lsa, bu sinfdan chiqib ketadi. Ko‘plab korporativ tashkilotlarning mijozlari yuzlab ilovalarni o‘zlarining tarmoqlarida avtomatik holatdagi sinf uchun o‘tkazish yo‘lagini talab qiladi (aksariyat hollarda ular shu sinfda qoladi). Bu sinfga tushgan ilovalarga xizmat ko‘rsatish kengroq bo‘ladi. O‘tkazish qobiliyatining 25% ini imkoniyat bo‘yicha trafikni sinfini qo‘llab quvvatlashga ajratish tavsiya etiladi.

Video xabarlarni uzatish uchun xizmat ko‘rsatish sifati

Multiservis tarmoqlarida televideniya eshittiruvlarini va xizmatlarini integratsiyalashuvi servis provayderlar uchun qator muammolarni yuzaga keltirdi. Video (xususan, so‘rov bo‘yicha video), ko‘p kanalli televideniya eshittiruvi va HDTV tarmoqni ovoz va videoga qaraganda katta resurslarni talab qiladi.

Video ma’lumotlarga nisbatan QoS ning turli xildagi talablariga ega. Xatto internet tarmog’ida eng yaxshi talab qilingan ilovalar ham mavjud kechikishlar (djitter)ni qandaydir paketlarni yo‘qotish bilan yengishi mumkin. Faqat IP ustidan video (ATM) 10^{-9} diapazonda minimal paketlarni yo‘qolishi uchun aniq talabga ega. Amaliyotda paketlar faqat tarmoqning o‘ta yuklanishi sharitida tashlab yuborilishi mumkin.

Video ilovalarining ikki asosiy turi mavjud: interaktiv video (masalan: videokonferensiya) va oqimli video (masalan: IPTV, bir manzil yoki ko‘p manzil bo‘yicha uzatilishi mumkin).

XEAI va IETF tavsiyanomalarini taxlili asosida video xabarlarni uzatish uchun QoS tavsiflarini asosiy talablarini umumlashtiramiz.

5.3 – jadvalda har xil standartli video xabarlarni uzatish tezligiga talablar keltirilgan.

5.3 –jadval.

Har xil standartli video xabarlarni uzatish tezligiga talablar

Sifat	**Usul yoki standart**	**Uzatish tezligi, Mbit/s**	**Siqish**
Sifat videokonferensiyasi	H.261	0.1	Ha
VCR sifat	MPEG-1	1.2	Ha
Teleuzatish sifati	MPEG-2	2 dan 4 gacha	Ha
Raqamli televideniya sifati			
Siqishsiz	ITU-R601	166	
Siqish bilan	MPEG-2	3 dan 6 gacha	Ha

5.3 –jadval davomi

Siqish bilan	H.264/MPEG-4	2 dan 4 gacha	Ha
HDTV			
siqishsiz	CD-DA	2000	
Siqish bilan	MPEG-2	25-34	Ha
Siqish bilan	H.264/MPEG-4	15-30	Ha

Interaktiv videoni sozlashda quyidagilar tavsiya qilinadi.

- interaktiv video trafik AF41 deb belgilanishi kerak;
- yo‘qolishlar 1 % dan kam bo‘lishi kerak;
- bir tomonlama kechikish 150 ms dan ko‘p bo‘lmasligi kerak;
- kechikishni tebranishi 30 ms dan ko‘p bo‘lmasligi kerak;
- minimal kafolatli o‘tkazish yo‘lagi (LLQ) videokonferensiya sessiyasining hajmiga 20 % ko‘pi bilan teng bo‘lishi kerak.

Videokonferensiya G.711 audio kodekiga ega. Unda mos keluvchi ovoz trafigini yo‘qolishiga, kechikishga, kechikishlarni tebranishiga talab mavjud. Video trafik ovoz trafigidan katta farq qiladi. Masalan, videokonferensiya trafigi o‘zgaruvchan hajmdagi paketlarni va o‘zgaruvchan tezlikli paketlarni uzatadi.

Videokonferensiya tezligi – video oqimlarni kadrga solish tezligi.

Oqimli video trafigi uchun talablar:

- oqimli video (bir manzilli yoki ko‘p manzilli jo‘natmalar) SS 4 deb belgilanishi kerak;
- yo‘qolishlar 2 % dan ko‘p bo‘lmasligi kerak;
- kechikish 4 – 5 soniyadan ko‘p bo‘lmasligi kerak (video ilovalarni buferga olish imkoniyatiga bog‘liq holda);
- kechikishni tebranishiga muhim talab mavjud emas;
- o‘tkazish yo‘lagini kafolati bo‘yicha talab vieo oqimni kodlashtirish tezligining formatiga bog‘liq;
- oqimli video odatda bir tomonlama bo‘ladi. Shu sababli uzoqdagi filiallarni filialdan markazga yo‘naltirishda marshrutlarni sozlash shart emas;

- video oqimning ko‘ngil ochar turi uchun DSCP CS 1 deb belgilash mumkin va ular uchun CBWFQ (Internet/scavenger sinfi ishlatiladi) navbatida o‘tkazish yo‘lagining minimum kafolati talab etiladi.

Keyingi yillarda multimeda trafiklarining jadallik bilan o‘sishi ma’lumot uzatish tarmoqlarini ishlatishida jiddiy muammolarni yuzaga keltirdi.

Ovoz, video va ma’lumotlarni uzatish trafikda ularga xizmat ko‘rsatishda har xil talablarni qo‘yadi. Shu sababli ma’lumot uzatish tarmoqlarini rivojlantirish va ularda muammolarni yuzaga kelishi xizmat ko‘rsatish sifatini ta’minlash masalasi dolzarb hisoblanadi.

5.4 – jadval.

QoSni ta’minlash tavsifi

Ko‘rsatkich	**IntServ**	**DiffServ**	**IntServ**
QoSni ta’minlash usuli	Zahiralash	Imtiyozlash	Zahiralash, imtiyozlash
Qo‘shimcha protokollarni ishlatish lozimligi	RSVP	Yo‘q	RSVP
Marshrutizorlarni unumdorligiga talab	Yuqori	Past	O‘rta
Tarmoqni kengaytirish samaradorligi	Yuqori emas	Yuqori	Yuqori
Turli ishlab chiqaruvchilarning qurilmalarini moslashuvchanligi	O‘rta	Yuqori	O‘rta
Sifatni ta’minlashni kafolatligi	Yuqori	O‘rta	Yuqori
Realizatsiya xarajatlari	Yuqori	Past	O‘rta

Hozirgi kunda ma’lumot uzatish tarmoqlarida xizmat ko‘rsatish sifatini ta’minlashning turli usullari mavjud. U yoki bu texnologiyani tanlash xizmat

ko‘rsatish sifatining talabiga bog‘liq. Taqdim etilayotgan xizmatning sifati foydalanuvchilarning talabini qondira olishi kerak.

Integrated Service (IntServ, RFC 1633) bu – xizmat ko‘rsatishning integratsiyalangan modeli. Kerakli o‘tkazish qobiliyatini kafolatlagan holda to‘liq (End-to-End) xizmat ko‘rsatish sifatini ta’minlashi mumkin. IntServ o‘zining maqsadi uchun RSVP signalizatsiya protokolidan foydalanadi. Bu esa ilovalarni resurslarga to‘g‘ridan – to‘g‘ri talab qo‘yishini ifodalashga yordam beradi va o‘zida shu talablarni ta’minlash mexanizmlarini qamrab oladi. IntServ qisqacha resurslarni zahirlash deb atash mumkin (Resource reservation).

RSVP pratokoli. Bu protokol har bir oqimi uchun o‘zlarining QoS – talablari to‘g‘risidagi signallar uzatishga yordam beradi. Kirishni boshqarish maqsadida bu talablarning sonli tavsiflarini aniqlash uchun ishchi ko‘rsatkichlar ishlatiladi.

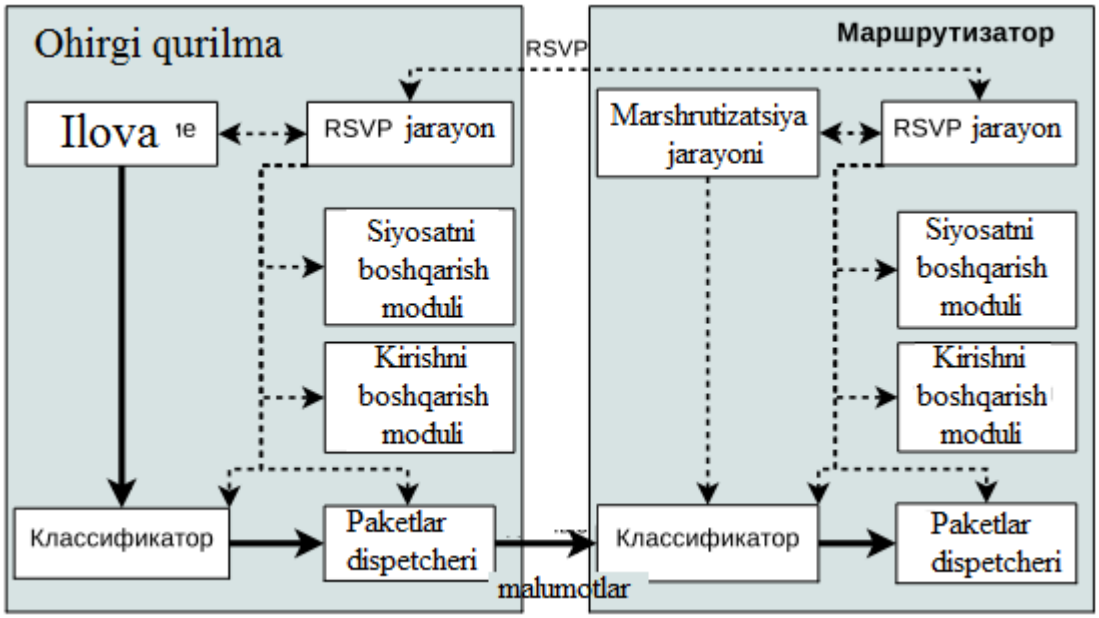
RSVP protokoli audio va videokonferensiya ilovalariga o‘hshash guruhli jo‘natishlarda qo‘llaniladi. RSVP protokoli multimedia trafigiga mo‘ljallangan bo‘lib, uning yordamida bir tomonlama trafik uchun o‘tkazish yo‘lagini oson zahiralash mumkin. Masalan tarmoq fayl tizimining trafigi uchun (Network File System - NFS) va VPN trafigini boshqarishida ishlatiladi.

RSVP protokoli tarmoqdagi kira olishli marshrutlangan yo‘l bo‘ylab resurslarning zahiralash to‘g‘risidagi so‘rovlarini signalizatsiyalab beradi (5.18 – rasm). Shu asnoda RSVP o‘zining shaxsiy marshrutini ishlab chiqmaydi, yani teskarisi bo’ladi.

Bu protokol boshqa yanada quvvatli marshrutlash protokollaridan foydalanish uchun ishlab chiqilgan. Har qanday boshqa IP – trafikda, ma’lumotlar va boshqaruv trafigi uchun yo‘lni aniqlashda RSVP tarmoqda qo‘llaniladigan marshrutlash protokoli bo‘lishi kerak.

RSVP protokolining ishlashi. Ilovalarning ma’lumotlar oqimi nomidan tegishli QoS pog‘onasini tarmoqlardan so‘rash uchun oxirgi tizimlar RSVP protokolidan foydalanishadi. Oqimni uzatish uchun qo‘llanadigan RSVP - so‘rovlar har bir tugundan o‘tganda tarmoq bo‘ylab uzatiladi. RSVP protokoli har

bir shu tugunlarda ma’lumotlar oqimi uchun resurslarni zahiralashga harakat qiladi.



5.18 - rasm. IntServ ning asosiy komponentlari

RSVP – moslashgan marshrutizatorlar kerakli tayinlangan nuqtaga kerakli ma’lumotlar oqimini yetkazib berishga yordam beradi. 5.18 - rasmda RSVP protokolni qo‘llaydigan asosiy modullar, ma’lumotlar oqimi to‘g‘risidagi axborot va klient hamda marshrutizatorni oqimlarini boshqarishi to‘g‘risidagi axborotni tasviri keltirilgan.

Resurslarni zahiralashdan avval, marshrutizatorning RSVP – demoni qarorni qabul qiluvchi ikkita kanal modullar bilan ulanadi – kira olishni boshqarish moduli (policy cantrol) va siyosatni boshqarish moduli (policy cantrol).

Kira olishini boshqarish moduli - QoS pog‘onaning so‘rovini ta’minlash uchun tugun ozod resurslarga ega ekanligini aniqlaydi.

Siyosatni boshqarish tuguni - foydalanuvchida zahiralashni olib borishga xuquq bormi yoki yo‘q ekanligini aniqlaydi. Agar birorta tekshiruvchi o‘tmasa, RSVP – demon, so‘rovni yaratgan ilovaning jarayoniga xato to‘g‘risida xabarni jo‘natadi. Agar ikkala tekshiruv ham normal holatda o‘tsa, RSVP – demon paketlarni tasniflash ko’rsatkichlarini va kerakli QoS pog‘onasini olish uchun

paketlarni rejalashtiruvchini o‘rnatadi. Paketlarni tasniflovchi har bir paket uchun QoS sinifini aniqlaydi, paketlarni rejalashtiruvchi esa QoS sinfiga asoslanib paketlarni uzatishni boshqaradi. Navbatlarda vaznli adolatli navbat algaritmi (Weighted Fair Queing - WFQ) va ixtiyoriy oldindan aniqlangan og’irlik algaritmi (Weighted Random Farly Detection - WRFD) rejalashtirish pog‘onasida QoSni qo‘llashni ta’minlaydi. WFQ va WRFD algoritmlarini quyida ko‘rib chiqamiz.

Kira olishni boshqarish moduli tomonidan qarorni qabul qilish jarayonida talab etilgan o‘tkazish yo’lagini zahiralashni faqat shunday holda bo‘ladiki, unda agar qolgan qismning talab etilgan trafik sinfi uchun yetarli bo‘lsa zahiralanadi, aks holda kira olishga so‘rov rad etiladi, lekin trafikning shu sinfi uchun jim turishi bo‘yicha aniqlangan xizmat ko‘rsatish sifati bilan baribir trafik uzatiladi. Ko‘p hollarda, bitta yoki bir nechta marshrutizatorlarda kira olishga agar so‘rov rad etilsa ham yuklama ortib ketgan marshrutizatorlarda zahiralashni o‘rnatib, ma’qul bo‘lgan xizmat ko‘rsatish sifatini yana modul amalga oshirib boraveradi. Shuning uchun boshqa ma’lumotlar oqimi, ular tomonidan buyurtirilgan o‘tkazish yo’lagidan to‘liq foydalana olishlari mumkin.

Zahiralash har doim bitta va faqat shu bitta manzilli yo‘l yoki ko‘p manzilli daraxt bo‘yicha davom ettirilishi kerak. Aloqa liniyasining ishdan chiqish holatida marshrutizator shu to‘g‘risida RSVP – demonga, u generatsiyalayotgan RSVP – xabarlar yangi yo‘l bo‘ylab uzatilishi uchun xabar berishi kerak.

Zahiralashni o‘rnatish jarayonini beshta alohida qadamlarga bo‘lishi mumkin:

1) Ma’lumotlarni jo‘natadiganlar RSVP boshqaruv xabarlarini, odatdagi trafikni ma’lumotlar bilan jo‘natadigan yo‘l bo‘ylab yuboriladi. Shu xabarlarda, jo‘natilgan yoki faqat hozirda jo‘natiladigan ma’lumotlar ta’riflanadi.

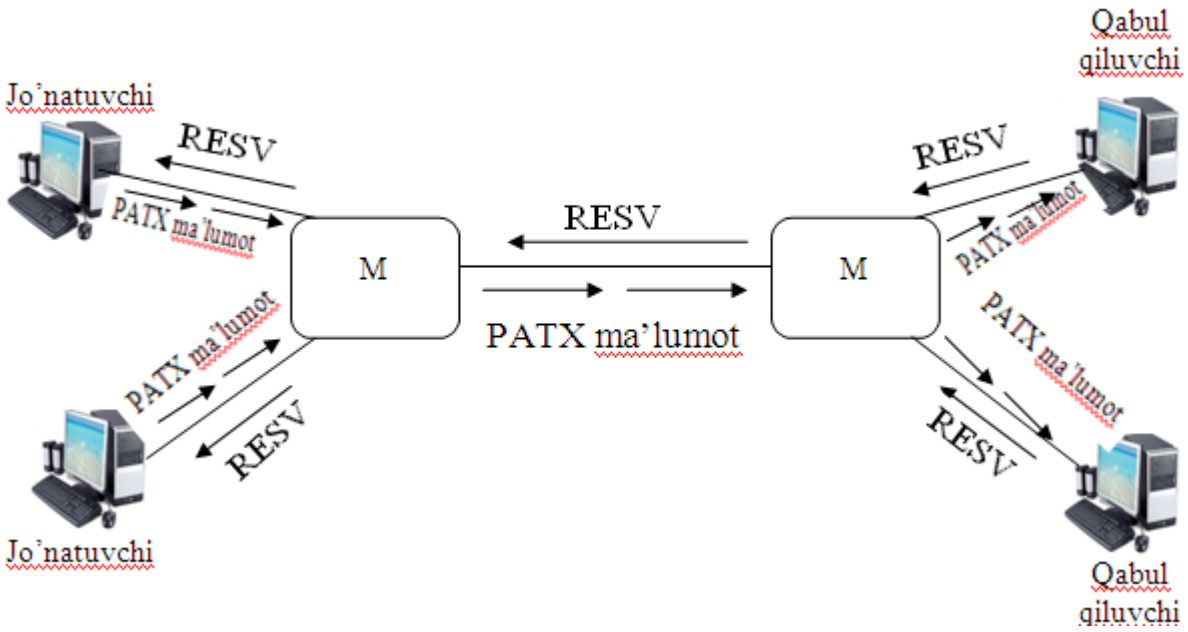
2) Har bir RSVP – marshrutizator PATH – xabarlarni tutib oladi, avvalgi tayinlash nuqtasining IP – manzilini saqlaydi, uni o‘rniga shaxsiy manzilini yozdiradi va ilovalarning ma’lumotlari uzatiladi, yo‘l bo‘yicha yangilangan xabarni jo‘natiladi.

3) Qabul qiluvchi – stansiyalar uchun PATH – xabarni ular qabul qilgan seanslar ko‘pligini tanlaydi va RSVP va RESV – xabarlar yordamida avvalgi marshrutizatorlardan resurslarni RSVP - zahiralashni so‘rab oladi. RSVP RESV – xabar qabul qiluvchidan RSVP PATH – xabarlar o‘tgan marshrut bo‘ylab teskari tomondagi yo‘nalishda yuboruvchiga ketadi.

4) RSVP – marshrutizatorlar mana shu RESV – so‘rovlarni xotirada ushlashi mumkinmi yo‘qligini aniqlaydi. Agar ha degan javob bo‘lsa, u holda ular zahiralashga olingan so‘rovlarni yig‘adi va avvalgi marshrutizatorga so‘rovni jo‘natadi.

5) Tegishli marshrutizatorlardan resurslarni zahiralashga so‘rovlarni qabul qilib, jo‘natuvchilar resurslarni zahiralash yakunlandi degan xulosaga keladi, ya’ni xaqiqiy resurslarni RSVP xabarlar tomonidan amalga oshirilgani tasdiqlanadi.

RSVP – zahiralash mexanizmi sxematik ravishda 5.19 - rasmda ko‘rsatilgan.



5.19 - rasm. Resurslarni zahiralashning RSVP mexanizmi

RSVP – komponentlari. RSVP – komponentlari quyidagi funksiyalarni bajaradi:

- RSVP – jo‘natuvchi (RSVP sender) bu – RSVP – seansida trafikni jo‘natishni aniqlashtiruvchi (initsialovchi) ilova. Quyida RSVP – tarmoq bo‘ylab RSVP – jo‘natuvchi uzatishi mumkin bo‘lgan oqimlarni tasnifi keltirilgan:

a) ma’lumotlarni uzatish tezligining o‘rtachasi;

b) tez (otilib) chiqishning maksimal hajmi.

Anjumanlar vaqtida yoki IP - protokol bo‘ylab (VoIP) ovozni uzatishda ilova RSVP – jo‘natgich va RSVP – qabul qilgich rolini ham bajarishi mumkin. Quyida RSVP – tarmoq bo‘ylab RSVP – qabul qilgichlar uzatishi mumkin bo‘lgan oqimlar tavsifi sanab o‘tiladi:

a) ma’lumotlarni uzatish tezligining o‘rtachasi;

b) tez chiqishning maksimal hajmi;

c) QoS, unga qo‘shiladigan:

- kafolatli xizmat ko‘rsatishi – PATH – xabarlarida, shuningdek tarmoqda bo‘lishi mumkin bo‘lgan maksimal kechikish uzatiladi;

- boshqariladigan yuklanish bilan xizmat ko‘rsatish - marshrutizatorlar faqat tarmoqdagi kechikishlar minimal bo‘lgandagina kafolat beradi.

RSVP protokolida 7 xil xabarlar ishlatiladi; ikkitasi shartli PATH, RESV va beshta opsional – PATH ERROR, PATH TEARDOWN, RESV ERROR, RESV CONFIRM va RESV TEARDOWN. RSVP marshrutizatorlar va mijozlar bu xabarlarni zahiralash holatini qo‘llab quvvatlash va yaratish uchun ishlatadi.

Odatda IP protokolining ustidan bevosita RSVP protokoli ishlaydi. Demak, RSVP protokoli ishonchsiz datagramma hisoblanadi. Ular marshrutizatorlarda davriy ravishda yangilanishi kerak bo‘lgan moslashuvchan holatni yaratishga yordam beradi.

RSVP protokoli RSVP, RESV xabarlari yordamida so‘rashi mumkin bo‘lgan integrallashgan xizmatni ikkita turini ko‘rsatadi: yuklanishni boshqarish xizmati va kafolatlangan bitli tezlik xizmati.

Boshqariladigan yuklanish – yuklanishni boshqarish xizmat (controlled load service) zahiralangan oqimni belgilangan joyiga kafolatsiz yetkazib beradigan trafik tomonidan minimal ta’sir ko‘rsatilsa, yetkazib berishni kafolatlaydi. Bundan

tashqari bu xizmatlarni ishlatishda Cisco kompaniyasi alohida zahiralangan oqimlarni izolyatsiyasini inobatga olgan. Oqimlarni izolyatsiya qilish resurslarni zahiralashda tarmoqda mavjud boshqa zahiralangan rusurslarni ta’sir qilmasligini ta’minlaydi.

Qoida bo‘yicha yuklanishni boshqarish xizmati tarmoqni o‘ta yuklanishga sezgir bo‘lgan internet ilovalarining trafigini uzatishda qo‘llaniladi. Shuningdek, ilova yuklanishsiz tarmoqda juda yaxshi ishlaydi, lekin o‘ta yuklanish bo‘lganda tezda “yaroqsiz” holga keladi. Masalan: FTP protokolida ishlovchi ilova.

Zahiralashning stillari. Resurslarni RSVP – zahiralash o‘qim uchun ikkita turga bo‘linishi mumkin: individual va umumiy.

Individual zahiralash. Bu distinct reservations shunday ilovalarda qo‘llaniladiki, ularda ma’lumotlarning bir nechta manbalari bir vaqtda axborotni jo‘natishi mumkin. Video ilovalarda har bir jo‘natuvchi ma’lumotlarning individualli oqimini generatsiyalaydi, u uchun kira olishni alohida boshqarishni amalga oshirish va qabul qiluvchigacha butun yo‘l bo‘ylab navbatni rejalashtirishi kerak. Demak, shunday oqimga, har bir jo‘natuvchi uchun va qo‘ldagi har bir kanal uchun resurslarni alohida zahiralashtirishni amalga oshirishi kerak.

Eng oddiy holda resurslarni individualli zahiralash bitta manzilli trafik bilan ilova masalasi kuzatiladi, bunda faqat bitta jo‘natuvchi va bitta qabul qiluvchi bor xolos.

Umumiy zahiralash. Bu “Shared reservations” shunday ilovalarda qo‘llaniladiki, ularda ma’lumot manbalarining bir nechtasi axborotni bir vaqtda uzata olmaydi. Masalan raqamli audio ilovalar, yoki VoIP ilovalar. Har qanday alohida olingan vaqt oralig‘idaga qarasak ko‘p bo‘lmagan odamlarni gaplashishini ko’rish mumkin. Bynda axborotni kam sonli jo‘natuvchilargina uzatadi. Bunday oqim har bir jo‘natuvchi uchun resurslarni alohida zahiralashga muhtoj emas, u uchun bitta zahiralash kerak bo‘lib, u guruhdagi har bir qanday jo‘natuvchiga kerak bo‘lganda qo‘llash mumkin. U guruhdagi ixtiyoriy junatuvchiga kerak bo’lgandagina qo’llaniladi.

RSVP protokolining atamalarida bunday oqim umumiy oqim (shared flow)

deb ataladi; u umumiy aniqlangan yoki guruhli zahiralashlar yordamida o‘rnatiladi.

Zahiralash usuli quyida ko‘rib chiqiladi.

- umumiy aniqlangan (Shared Explicit-SE) oqimlarni zahiralashda tarmoq resurslari alohida ko‘rsatiladi.

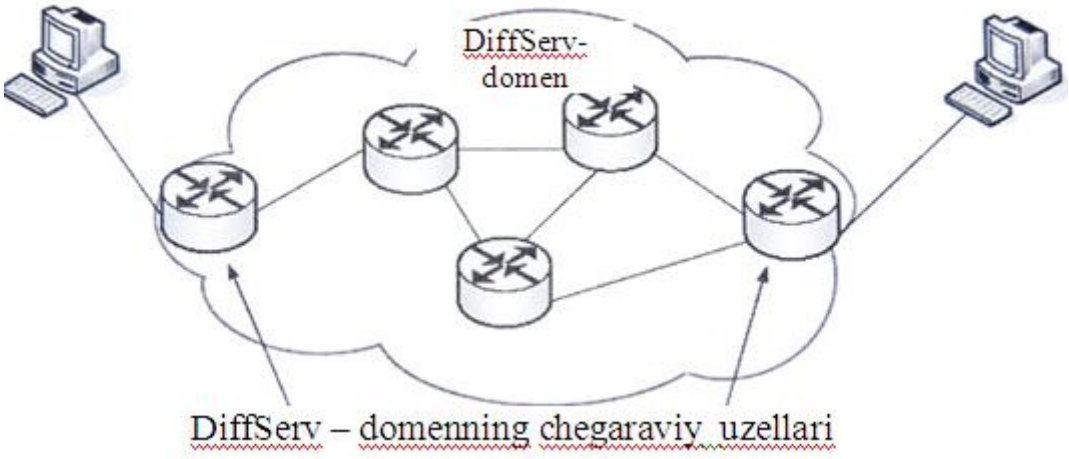
- guruhli filtr (Wildcard Filter-WF) yordamida o‘tkazishi yo’laksi va kechikishning harakteristikalari har qanday jo‘natuvchi uchun zahiralangan bo‘lishi mumkin. Bunday filtr jo‘natuvchilarni alohida berilishiga imkon bermaydi. U barcha jo‘natuvchilarni qabul qiladi, bunga manbaning manzilini va portdagi nolni o‘rnatishni ko‘rsatib turadi.

Differensiallashgan xizmatlar (Diffserv) arxitekturasi

1998 yili IETF tashkiloti differensiallashgan xizmatlarni (diffserv Working Group) yaratish bo‘yicha ishchi guruhni shakllantirdi. Diffserv arxitekturaviy modelini intserv modelining trafikni kafolatli xizmat ko’rsatish sifati mexanizmi bilan trafikni kafolatsiz etkazish mexanizmini bog‘lab turuvchi ko‘prik bilan solishtirishi mumkin. DiffiServ mo‘deli differensialashgan trafikni har xil imtiyozli sinflarga bo‘lish yo‘li bilan ta’minlaydi.

DiffServ (5.20 – rasm) yondoshuvining asosiy vazifasi IPv4 paket sarlovhasidan differensial xizmat (DS)ning xizmat ko’rsatish turini bayti (Type of Service-ToS)ni va IPv6 paketning trafik sinfi (Traffic Class) baytini aniqlash hisoblanadi. Mana shu belgilash har o‘tishda ma’lumotlar paketining xarakati to‘g‘risida qaror qabul qilishga bog‘liq, ya’ni har bir oraliq tugunda.

Differensiallashgan xizmatlar arxitekturasi u xizmat ko‘rsatish sifatiga qo‘yilgan talablarga bog‘liq holda katta diapazondagi har xil takliflarni o‘zining mijozlariga berishi uchun xizmatlarni yetkazib berayotganlar foydalanishi mumkin bo’lgan boshlang’ich asosni ta’minlaydi.



5.20 - расм. DiffServ - domenning chegaraviy tugunlari tuzilishi

Mijoz xizmatlarni talab qilingan darajasini aniq bir ilovaning paketi uchun differensial xizmatning (DSCP) kod maydoning mos keluvchi qiymatini o'rnatish orqali tanlash mumkin. Differensial xizmatning kodi xizmatni etkazib beruvchi (PHB)ning tarmoqda har bir oraliq tugunida paketning xarakati to'g'risidagi echimlarning zanjirini aniqlaydi.

PHB– siyosat bu - qadamma-qadam xizmat ko'rsatishi siyosati bo'lib, u differensiyal xizmatlarning kod maydon (DSCP)ini tegishli qiymati bilan paketlarga nisbatan tarmoq tugunining xolatini aniqlaydi. Trafik oqimining barcha paketlariga xizmat ko'rsatish uchun o'ziga xos talablari bilan o'zida har doim DSCP maydonidagi bitta qiymatni olib yuradi.

Diffeserv – domenni ichidagi barcha tugunlar differensiallashga xizmatlarlarning kod maydonida saqlanayotgan qiymatga asosan paketga qo'llanilishi kerak bo'lgan PHB – siyosatni aniqladi. Diffeserv domenining chegaraviy tugunlari diffeserv – domeniga tushayotgan trafikni shakllantirish muhim funksiyasini bajaradi. Trafikni shakllantirish quyidagi funksiyalarni bajarilishini o'z ichiga oladi:

- paketlarni tasniflash (DSCP maydoniga qiymat o'rnatish);
- trafikni cheklash.

Trafikni shakillanishi diffserv – domenining kirish interfeysiga bajariladi.

Shakillanish diffserv – domeniga tushayotgan trafikni boshqarishida muhim axamiyatga ega. Bunday xolat har bir paket uchun tarmoq unga mos bo’lgan PHB – siyosatni aniqlashi mumkin.

5.4 - rasmda differensional xizmatlarning arxitekturasi keltirilgan.

5.4 - jadval.

Differensiallashgan xizmatlarning arxitekturasini funksional bloklari

Funksianal blok	**Joylashishi**	**Funksiyasi**	**Harakati**
Trafikni shakillantiruvchi	Diffserv-demonining chegaraviy marshrutizatorini kiruvchi interfeysi	Paketlarni tasniflash, trafikini tenglashtirish va chegaralash	Kirish trafigini chegaralash va trafikni profili asosida DSCP maydonining qiymatini o‘rnatish
PHB-siyosatni amalga oshiruvchi qurilma	Diffserv-domenining barcha marshrutizatorlari	Resurslarni taqsimlash va paketlarni tashlab yuborish siyosati	DSCP maydonida berilgan qiymatga mos ravishda xizmat ko’rsatish sifatining tavsifiga asosan paketlarni qayta ishlash PHB – siyosati aniqlanadi

Trafikni shakllantiruvchilar – bular tarmoqning chegaraviy qurilmalarida amalga oshiriluvchi xizmat ko’rsatish sifatining har xil funksiyalaridir. Chegaraviy funksiyalar DSCP maydoniga mos keluvchi qiymatni qo’yish yo’li bilan trafikni belgilaydi. Yoki tasniflaydi. Shuningdek tarmoqqa kiruvchi trafikni uning o’rnatilgan profiliga mos kelishini tekshirish maqsadida monitoringini olib boradi.

Differensial xizmatning kodi diffserv domenidagi paketni qayta ishlash usulini aniqlovchi qiymatga asoslangan maydonni o’z ichiga oladi.

Trafikning tegishli sinfiga to‘g‘ri keladigan PHB-siyosati qator omillarga bog‘liq:

- kirish oqimining jadalligi yoki trafikning berilgan sinfi uchun yuklama. Bu ko’rsatkich trafikning chegaraviy shakllantiruvchisi orqali nazorat qilinadi;

- trafikni berilgan sinfi uchun resurslarni taqsimlash. Bu ko’rsatkich diffeserv-domenning tugunlarida amalga oshiriluvchi resurslarning taqsimlash funksiyalari orqali nazorat qilinadi.

- trafikni yo‘qotish darajasi. Bu ko’rsatkich diffeserv-domenining tugunlarida olib boriladigan paketlarni tashlab yuborish siyosatiga bog’liq.

Ikkita standartli PHB – siyosat mavjud – zudlik bilan uzatish PHB- siyosat (EF PHB) va kafolatli yetkazib berishi PHB – siyosat (AF PHB).

Paketlarni zudlik bilan uzatish PHB – siyosati. U diffserv-domenining tugunlarida paketlarga to‘g‘ridan-to‘g‘ri xizmat ko‘rsatishni ta’minlash uchun foydalaniladi. Uning asosiy yutug’i kam darajada paketlarni yo‘qotish, kam kechikish, trafikni sezilarsiz titrashi hamda kafolatlangan o‘tkazish yo’lagi hisoblanadi. EF PHB siyosati trafikning shunday ilovalariga xizmat ko‘rsatishda qo‘llaniladiki, masalan, IP-tarmoqda ovozni uzatish (VoIP), videoanjumanlarning ilovalari hisoblanadi hamda virtual ijarali kanallar bo‘ylab axborotni uzatish ham kiradi, chunki bu xizmat diffserv-domenining oxirigi tugunlarida ikki nuqtali ulanishdan iboratdir. Bunday xizmat ko‘rsatish turi ko‘pincha yuqori (premium service) sinfli xizmatlar deb atashadi.

Paketlarni kafolatli yetkazib berish PHB-siyosati. Bu Assured Forwarding PHB – AF PHB xizmatlarni yetkazib beruvchi diffserv domenidagi mijozdan olingan IP paketlarni bir nechtasini turlidarajada etkazib berish ishonchliligini ta’minlashi mumkin. Ohirgi tugunlarida AF PHB siyosati TCP-ilovalari uchun ma’qul hisoblanadi.

Paketlarni kafolatli yetkazib berishi PHB – siyosati AF-trafikning to‘rtta sinfidan har biri uchun xizmat ko‘rsatishning har xil darajalari mavjudligini ko‘zda tutadi. AF-trafikning har bir sinifiga paketlarning shaxsiy navbati to‘g‘ri keladi, bu esa o‘tkazish yo’lagini samarali boshqarishni olib borishiga imkon beradi. AF-

trafikning har bir sinifi paketlarni tashlab yuborishni uchta imtiyozli daraja bilan xarakterlanadi (pastki, o‘rtadagi va yuqori). Bu ixtiyoriy avvaldan aniqlanadigan mexanizm (Random Early Detection-RED) turi bo‘yicha navbatlarni boshqarish mexanizmini amalga oshirish imkonini beradi.

AF- PHB siyosatida shunday vosita borki, uning yordamida xizmatlarni etkazib beruvchi DSCP maydonidagi qiymatga qarab IP-paketlarni bir nechta har xil daraajalarda ishonchli utkazib berishni ta’minlashi mumkin.

PHB siyosatini shakllanishini uchta yechimi mavjud:

- tarmoqni initsializatsiyasi (aniqlashi);
- xizmat ko‘rsatish sifati to‘g‘risida signalizatsiyasi;
- siyosat dispetcheri.

Tarmoqni initsializatsiyasi. Resurslarni taqsimlashning usullaridan biri evristik usullar yoki tizimli modellash texnikasidan foydalanib tarmoqning resurslarini initsializatsiyalashdan iborat. Shuni ta’kidlash joizki, bu usul QoS siyosati va trafikning profili yetarlicha ko‘p vaqt mobaynida o’zgarmagan. Katta bo‘lmagan tarmoqlarda faqat qo‘llanilishi mumkin.

Xizmat ko‘rsatish sifati to‘g‘risida signalizatsiya. Shu usulga binoan PHB – siyosatini amalga oshirishda ilovalar tarmoqqa RSVP signalli protokol yordamida xizmat ko‘rsatish sifatiga talablar to‘g‘risida xabar beradi. RSVP protokoli diffserv – domen kira olishni boshqarishni talab etuvchi tarmoqning yana bir zvenosi sifatida qaraladi.

QoS siyosat dispetcheri. Siyosatni aniqlash trafikning oqimiga qo‘llaniladigan QoS darajalarini tanlashni taqozo etadi. Siyosatlar esa siyosatlarni tarqatish protokoli COPS (Com mon Open Policy Service)yordamida tayinlanadi. Bu IETF guruhi tomonidan ishlab chiqilgan.

Navbatlarni qayta ishlash mexanizmi FIFO - paketlarni ketma-ket “birinchi kelgan – birinchi bo‘lib ketadi” (first-in first-out-FIFO) tamoyilida ishlovchi oddiy navbat. Aslida, bu yerda hech qanday imtiyozlash yo‘q.

Imtiyozli navbatlar: Priority Queuing (PQ) ayrim paketlarni boshqalardan shart qo’yilgan imtiyozlashni ta’minlaydi. Hammasi bo‘lib 4 ta navbat: high,

medium, normal va low. Qayta ishlash yuqori imtiyozli navbatdan boshlab ketma-ket olib boriladi, va uni to‘liq tozalanishigacha imtiyozi past navbatlarga o‘tilmaydi. Shunday qilib, kanalning yuqori imtiyozli navbatlar bilan monopoliyasi yaratilishi mumkin. Imtiyozi aniq ko‘rsatilmagan trafik avtomatik ravishda (default) navbatga tushadi.

Ixtiyoriy navbatlar: Custom Queuing (CQ) sozlanadigan navbatlarni ta’minlaydi. Har bir navbat ucun kanalini o‘tkazish yo’lagi boshqarishni ko‘zda tutadi. 17 ta navbatlar qo‘llab quvvatlanadi. Tizimli “0” navbat boshqaruvchi yuqori imtiyozli paketlar uchun zahiralab qo‘yilgan va foydalanuvchilarga bu paytda yo’l qo’yilmaydi.

Navbatlar, birinchisidan boshlab ketma-ketlikda aylanib o’tadi. Har bir navbat “hisoblagich”ga ega. Baytlar navbatda aylanib o’tishidan oldin berilgan qiymat bo’lib,qachonki navbatdan chiqib ketsa u paketning xajmiga ko’ra kamayadi. Agar hisoblagich 0 ga teng bo’lmasa navbatdagi paket to’liq o’tadi.

Tortilgan adolatli navbat (WFQ): Weighted Fair Queing (WFQ) trafikni avtomatik ravishda oqimlarga (flows) bo‘lib yuboradi. Jimlik bo‘yicha ularning soni 256 ga teng, ammo o‘zgarishi mumkin. Agar oqimlar, navbatlarga nasbatan ko‘p bo‘lsa, bitta navbatga bir nechta oqimlar joylashtiriladi. Paketni oqimga (tasniflash) tegishligi ToS asosida manbaning manzili, qabul qiluvchining IP-manzili, manbaning porti va qabul qiluvchining porti (IP protokol) asosida aniqlanadi. Har bir oqim alohida navbatni ishlatadi.

WFQ ni (Scheduler) qayta ishlovchi mavjud oqimlar orasidagi yulakni teng (fair - adolati) bo‘lishni ta’minlaydi. Buning uchun foydalanadigan yo’lak oqimlar soniga bo‘linadi va har biri teng qismni oladi. Undan tashqari, har bir oqim o‘z vazniga (weight) ega. Oqimning vazni qayta ishlovchi tomonidan shunday hisobga olinadi.

Demak WFQ qo‘shimcha ravishda ToS ni hisobga olib, foydalanish mumkin bo‘lgan o‘tkazuvchanlik qobiliyatini avtomatik ravishda adolatli taqsimlaydi. IP imtiyozlari katta oqimlar – katta o’tkazish yulagini oladi. IP imtiyozlari bir xil bo’lgan oqimlarda ToS teng o’tkazish yo’lagini oladi. Yuklama oshgan taqdirda

yuklanmagan yuqori imtiyozli oqimlar o‘zgarishsiz faoliyat ko‘rsatadi, past imtiyozli yuqori yuklanganlari esa – cheklanadi.

WFQ bilan RSVP birga ishlaydi. Jimlikda WFQ past tezlikli interfeyslarda yoqilgan bo’ladi.

Ixtiyoriy avvaldan aniqlangan tortilgan algoritm (WRED): Weighted Randam Early Detection (WRED) paketlarga har xil darajada xizmat ko‘rsatish ularni tashlab yuborish ehtimoliga bog‘liq holda taqdim etadi va IP – imtiyoz maydonidagi qiymatga asosan RED mexanizmini ko’rsatkichlarini tanlab o‘rnatishni ta’minlaydi. Boshqacha aytganda, WRED algoritmi bir tipga tegishli bo’lgan paketlarni tezroq tashlab yuborishni va qolgan barcha paketlarni kamroq tashlab yuborishni ko’zda tutadi.

CBWFQ-Class Based Welghted Sair Queuing sinflar asosidagi navbatlarga xizmat ko‘rsatish mexanizmiga to‘g‘ri keladi. Quyidagi ko’rsatkichlar asosida barcha trafik 64 ta sinfga bo‘linadi: kirish interfeysi, kira olish listi (aceess list), protokol, DSCP ni qiymati, QoS MPLS belgisi.

Chiqish interfeysining umumiy o‘tkazuvchanlik qobiliyati sinflar bo‘yicha taqsimlanadi. Har bir sinfga ajratiladigan o‘tkazish yo’lagi absolyut qiymad (bandwith kb/s)da yoki foiz (bandwith percent)da interfeysda nisbiy o‘rnatilgan qiymatda aniqlanishi mumkin.

Konfiguratsiyalangan sinflarga tushmagan paketlar default sinfiga tushadi. Uni qo‘shimcha sozlash mumkin va kanalning bo‘sh o‘tkazish yo’lagini oladi. Har qanday sinfning navbatini to‘lishida shu sinfning paketlari yo’q qilinadi.

Low Latency Queuing (LLQ) - past kechikishli navbat. LLQ ni imtiyozli navbatli PQ (LLQ=PQ + CBWFQ)li CBWFQ mexanizmi sifatida qarash mumkin.

LLQ da PQ LLQ ovoz (VoIP) trafigi mavjud bo’lganda tavsiya qilinadi. Videoanjumanda yaxshi ishlaydi.

5.4. Monitoringda qo‘llaniladigan tarmoq protokollari

Ishlab turgan tarmoqni monitoring qilish tarmoq administratoriga tarmoqni samarali boshqarish va boshqa mutaxassislar uchun tarmoqdan foydalanish to‘g‘risida statistik hisob yaratish uchun axborotni taqdim etadi. Kanallarni holati va xatolarni paydo bo‘lish chastotasini va aktiv ulanishlarni ko‘rinib turishi, tarmoq administratori uchun tarmoqdan foydalanish holatini baholashni osonlashtiradi. Qandaydir vaqt oralig‘ida bu axborotlarni yig‘ish va ko‘rish tarmoqni taxlil qilishga va loyihani o‘sishini bashorat qilishga, shuningdek nosoz qurilmani batamom ishdan chiqquncha uni aniqlab, almashtirish imkoniyatini beradi.

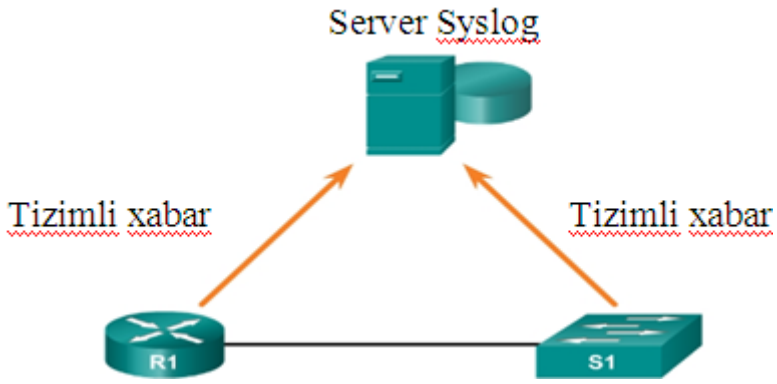
Administrator tarmoqni monitoring qilishda 3 ta protokoldan foydalanishi mumkin. Syslog, SNMP va NetFlow eng ko‘p qo‘llaniladigan protokollar bo‘lib, har biri o‘z kamchiligiga ega. Ularni birgalikda ishlashi tarmoqni holatini taxlil qilishda samarali usul hisoblanadi. NTP (Network Time Protocol — «tarmoqning vaqt protokoli»)protokoli barcha qurilmalardagi vaqtlarni sinxronizatsiyasini ta’minlash uchun ishlatiladi. Bu esa har xil qurilmada jurnallar faylini solishtirishda muhim hisoblanadi.

Tarmoqdagi qurilmada qandaydir hodisani sodir bo‘lishida ishonchli mexanizmlarni ishlatish orqali administratorni tizimli xabar orqali ogohlantiradi. Bu xabarlar juda muhim bo‘lishi mumkin. Administratorlarni ishlarida bunday xabarlarni saqlash va ko‘rsatishni har xil usullari bo‘lishi mumkin. Xabar to‘g‘risida ogohlantirishni jo‘natish usullari tarmoq infratuzilishsiga kam ta’sir qilishi kerak.

Tarmoq qurilmalari beradigan eng keng tarqalgan tizimli xabarni olish usuli bu syslog protokoli hisoblandi.

Syslog termini standartni tavsiflash uchun ishlatiladi. Syslog protokoli UNIX tizimi uchun 80 yillarda ishlab chiqilgan, lekin IETF jamiyati tomonidan RFC 3164 nomi bilan birinchi marta 2001 yilda xujjatlashtirilgan. Syslog IP tarmoq bo‘yicha hodisalar to‘g‘risidagi ogohlantirishli xabarni jo‘natish uchun

UDP 514 portini ishlatadi (5.22 - rasm).



5.22 – rasm. Tarmoq tuzilishi

Syslog protokolini tarmoqning ko‘p qurilmalari tushunadi, ya’ni marshrutizatorlar, kommutatorlar, ilovalar serverlari, tarmoqlararo ekranlar va boshqalar. Syslog protokoli tarmoq qurilmalari uchun tizimli xabarlarni tarmoq bo‘yicha Syslog serveriga jo‘natishni ta’minlaydi. Shu maqsadda maxsus ajratilgan tarmoq (out-of-band, OOB)ni yaratish mumkin.

Windows va UNIX operatsion tizimlar uchun Syslog serverining dasturiy ta’minotida har xil paketlar mavjud. Ularning ko‘plari bepul.

Syslogni jurnallashtirish xizmati 3 ta asosiy imkoniyatlarga ega:

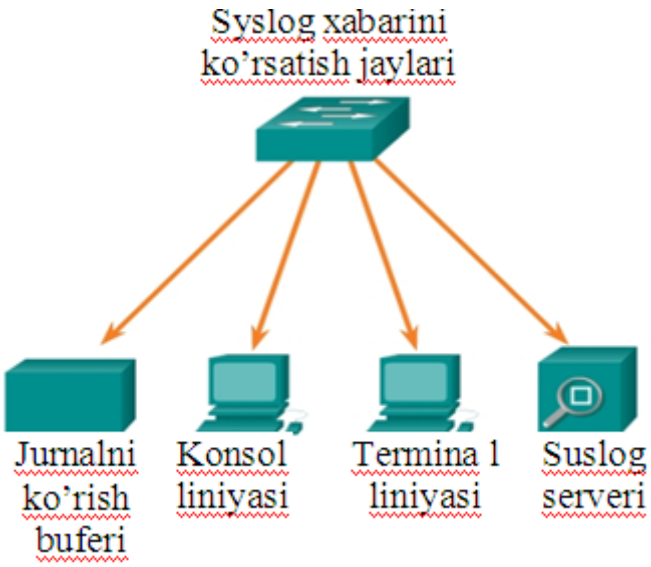
- monitoring va qayta tiklash uchun jurnalga axborotlarni yig‘ish;
- yig‘ish kerak bo‘lgan axborot turini tanlash;
- yig‘ilgan Syslog xabarini qabul qiluvchilarini aniqlash .

Cisco qurilmalarida syslog protokoli tizimli xabarlarni jo‘natishni boshlaydi va debug jarayonida kerakli qurilmaning jurnalini ko‘rish mumkin. Jurnallarni ko‘rish jarayoni bu xabarlarni boshqaradi va bu qurilmani sozlanishiga bog‘liq. Masalan, syslog xabari tarmoq bo‘yicha tashqi syslog serveriga jo‘natishi mumkin.

Syslog xabari uchun eng keng tarqalgan usullar quyidagilar (5.23-rasm):

- jurnallarni ko‘rish buferi (marshrutizatorni yoki kommutatorni tezkor xotira qurilmasidagi);
- konsol liniyasi;
- terminal liniyasi;

- syslog serveri.



5.23 – rasm. Syslog xabarini ko‘rsatish joylari

Syslog serverida jurnallarni ko‘rish orqali tizimli xabarlarni uzoqdan yoki telnet, SSH yoki konsol port yordamida qurilmaga ulanish orqali kuzatish mumkin.

Syslogning har bir pog‘onasi ahamiyatga ega:

- ogohlantirish pog‘onasi **(warning) –** kritik holatning pog‘onasi **(emergency) –** bu xabar dasturiy ta’minotning yoki qurilmaning buzilishi to‘g‘risida; bu turdagi xabar qurilmaning ishlamay qolganligini bildiradi. Syslogni bu pog‘onasi jiddiy muammoga bog‘liq;

- tekshrish pog‘onasi **(debugging) –** bu pog‘onadagi xabar **debug** ning turli buyrug‘ini bajarish natijasida olingan chiqish ma’lumotlaridan iborat;

- ogohlantirish pog‘onasi **(notification) –** ogohlantirish pog‘onasidagi xabar ma’lumotnoma ko‘rinishidagi harakterga ega. Qurilmani ishlash qobiliyatiga ta’sir ko‘rsatmaydi. Ogohlantirish pog‘onasida xabar interfeysni holati aktiv yoki aktiv emasligini yoki tizimni qayta ishga tushganligini ko‘rsatadi.

Nazorat savollari

1. Nima sababdan monitoring tashkil etiladi?
2. Monitoring protokollari vazifalari nimadan iborat?
3. Syslog va SNMP protokoli qanday ishlaydi?
4. Monitoringda xavfsizlik masalalari ko‘riladimi?
5. Qurilmalarga kirishda nechta usuldan foydalanish mumkin?
6. Qurilmalarga kirishda qanday xavfsizlik choralari ko‘riladi?
7. FTP va TFTP protokollarining farqi nimada?
8. Amaliy pog‘onada qanday protokollar ishlatiladi?

QISQARTMALAR RO‘YHATI

ADIKM	- adaptiv differensial impuls kodli modulyatsiya
ARO‘	- analog raqamli o‘zgartirgich
AT	- avtanom tizimi
IKM	- Impuls kodli modulyatsiya
MKOQ	- ma’lumot kanalining ohirgi qurilmasi
MO	- markaziy ofis
MOQ	- ma’lumotlar ohirgi qurilmasi
RAO‘	- raqamli analog o‘zgartirgich
XEAI	- Xalqaro Elektr Aloqa Ittifoqi

INGLIZCHA QISQARTMALAR

AH	- Authentication Header	- autentifikatsiyalovchi protokoli
ANSI	- American National Standart Institute	- Amerika Standartlar Milliy Instituti
ARP	- Address Resolution Protocol	- manzilni aniqlash protokoli
ATM	- Asynchronous Transfer Mode	- Uzatishning asinxron rejimi
BECN	- backward explicit congestion notification	- manba qurilmasida tiqilib qolishlar to‘g‘risida axborot berish
CBWFQ	- Class Based Welghted Sair Queuing	- Sinflarga asoslangan boshqa navbat
CIDR	- Classless Inter-Domain Routing	- Sinfsiz Inter-Domain Yonaltiruvchi (marshrutizator)
CIR	- Committed Information Rate	- Qabul qilingan ma'lumot darajasi
COPS	- Com mon Open Policy Service	- Siyosatlar esa siyosatlarni tarqatish protokoli
CQ	- Custom Queuing	- Ixtiyoriy navbatlar
DCP	- Digital Cinema Package	- Raqamli kino paket

DECnet	- Digital Equipment Corporation network	- Raqamli qurilmalar korporatsiyasi tarmog'i
DES	- Data Encryption Standard	– simmetrik shifrlash algoritmi
DLCI	- Data link connection identifier	- ma'lumot uzatish kanali identifikatori;
DOI	- Domain of Interpretation	- interpretatsiyalash domeni
DSCP	- Differentiated Services Code Point	- Turli xizmatlarning kod nuqtasi
DTE	- Data Terminal Equipment	- ma'lumotlar ohirgi qurilmasi
DVA	- Distance Vector Algorithms	- masofa-vektor algoritmi
EAP-TLS	- Extensible Authentication Protocol-Transport Layer Security	- Yagona haqiqiyligini tekshirish protokoli - Transport daraja xavfsizligi
ESP	- Encapsulation Security Rau1oad	- himoyani inkapsulyatsiyalovchi protokol
ETSI	- European Telecommunication Standart Institute	- Telekommunikatsiyalar bo'yicha standartlashtirish Yevropa Instituti
FECN	- forward explicit congestion notification	- oldindan aniq tiqilinch haqida xabarnoma
FIFO	- first-in first-out	-"birinchi kelgan – birinchi bo'lib ketadi"
FR	- Frame Relay	- kadrlarni retranslyatsiya protokoli
FTP	- File Transfer Protocol	- fayllarni uzatish protokoli
HDTV	-High Definition Television	- Oliy belgilangan televizor
HTTP	-HyperText Transfer Protocol	- gipermatnlarni uzatish protokoli
ICMP	- Internet Control Message Protocol	- Internet Boshqarish Xabar Protokoli
IETF	- Internet Engineering Task Force	- Internetning muxandislik muommolari bo'yicha ishchi guruhi
IGMP	- Internet Group Management	- Internet protokolini guruhli

	Protocol	boshqarish
IGP	- Interior Gateway Protocol	- Ichki shlyz protokoli
IKE	- Internet Key Exchange	- Internet kaliti almashinuvi
IntServ	- Integrated Service	- Telefonga o'rnatilgan xizmat
IPSec	- Internet Protocol Security	- Internet protokoli xavfsizligi
ISDN	- Integrated Services Digital Network	- Integratsiyalangan xizmat ko‘rsatish raqamli tarmog‘i
ITU	- International Telecommunication Union	- Xalqaro elektraloqa ittifoqi
ITU-T	- International Telecommunication Union-Telecommunication	- Telekommunikatsiya bo’yicha Xalqaro elektraloqa ittifoqi
LLQ	- Low Latency Queuing	- Kichkina vaqtinchalik kutish
LSA	- Latent semantic analysis	- Yashirin semantik tahlil
LSA	- Link State Algorithms	- aloqa xolati algoritmi
MAC	- Medium Access Control	- O'rta kirish nazorati
MCU	- Multipoint Control Unit	- Ko'p nuqtali boshqaruv bo'limi
MPEG	- Moving Picture Experts Group	- video bo’yicha ekspertlar guruxi
MPPE	- Microsoft Point-to-Point Encryption	- Microsoft nuqtadan - nuqtagacha shifrlash
MSCHAP	- Microsoft Challenge - Handshaking Authentication Protocols	- qo‘l berishishda aniqlash protokoli
NAT	- Network Address Translation	- tarmoq manzillarini moslashtirish
NTP	- Network Time Protocol	- tarmoqning vaqt protokoli
OSPF	- Open Shortest Path First	- dinamik marshrutizatsiya protokoli
PAP	- Pasword Athentication Protocol	- parol bo‘yicha aniqlash protokoli
PPP	- Point-to-Point Protocol	- Point-to-Point protokoli

PPTP	- Point-to-Point Tunneling Protocol	- Point-to-Point tunnellash protokoli
PQ	- Priority Queuing	- Imtiyozli navbatlar
PVC	- Permanent Virtual Circuit	- Doimiy Virtual O'chirish
QoS	- Quality of Service	- kafolatli xizmat ko‘rsatish sifati
RAS	- remote access services	- masofaviy erkin foydalanish xizmatlari
RFC	- Request for Comments	- Fikr uchun so'rov
RIP	- Routing Information Protocol	- Yonaltiruvchi (marshrutizator) ma'lumot protokoli
RSA	- Rivest, Shamir, Adleman	- ochiq kalitli kriptografik algoritm
RSVP	- Resource ReSerVation Protocol	- tarmoq resurslarini zaxiralash protokoli
RTP	- Real-time Transport Protocol	- real vaqt transport protokoli
SA	- Security Association	- xavfsiz assotsiatsiyalar
SAD	- Security Association Database	- xavfsizlik siyosatlarining ma’lumotlar bazasi
SCTP	- Stream Control Transmission Protocol	- Oqimni boshqarish axborotini uzatish protokoli
SNMP	- Simple Network Management Protocol	- Tarmoqni boshqaruvchi oddiy protokol
SSH	- Secure Shell	- xavfsiz qobiq
TCP/IP	- Transmission Control Protocol / Internet protocol	- Uzatishni boshqarish protokoli / Internet protokol
TFTP	- Trivial File Transfer Protocol	- fayllarni uzatuvch oddiy protokol
TTL	- time to live	- yashash vaqti
UDP	- User Datagram Protocol	- Foydalanuvchi datagramm protokoli
UNI	- User Network Interface	- Foydalanuvchi Tarmoq interfeysi
VCI	- vitual channel identifier	- virtual kanal identifikatori

VLAN	- Virtual Local Area Network	- Lokal kommyuter tarmog’i
VPI	- virtual path identifier	- virtual yo‘l identifikatori
VPN	- Virtual Private Network	- shaxsiy virtual tarmoq
WAN	- Wide Area Network	- global kompyuter tarmoq
WF	- Wildcard Filter	- guruhli filtr
WFQ	- Weighted Fair Queing	- Tortilgan adolatli navbat

Foydalanilgan adabiyotlar ro’xati

1. W. Stallings. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Copyright © 2016 by Pearson Education, Inc.
2. W. Stallings Data and computer communications. Pearson Education, Inc. Pearson Prentice Hall, 2007.
3. O’zbekiston Respublikasini yanada rivojlantirish bo’yicha harakatlar strategiyasi to’g’risida. O’zbekiston Respublikasi Prezidentining PF-4947-son farmoni. Toshkent, 2017 yil 7 fevral.
4. Semenov Yu.A. Algoritmi telekommunikatsionnix setey. Chast 1. Moskva 2014
5. Algoritmi telekommunikatsionnix setey: uchebnoe posobie 1-2 ch. / Yu.A. Semenov, —M.: Internet-Universitet Informatsionnix Texnologiy; BINOM. Laboratoriya znaniy, 2014.
6. R.X. Djuraev, Sh.Yu. Djabbarov, Umirzakov B.M. Texnologii peredachi dannix. Uchebnoe posobie. Tashkent 2008

Қўшимча адабиётлар

1. А. Б. Гольдштейн, Б. С. Гольдштейн. Технология и протоколы MPLS. СПб.: БХВ-Петербург, 2014. — 304 с.
2. Чердынцев Е.С. Ч-45. Мультимедийные сети: учебное пособие / Е.С. Чердынцев; Томский политехнический университет. – Томск: изд-во Томского политехнического университета, 2012. – 97 с.
3. Khanvilkar S. ET AL. Multimedia networks and communication // ELECTRICAL ENGINEERING HANDBOOK / edited by w.k. chen. – [s. l.]: Academic Press, 2004. –p. 401–425.
4. Xeld G. Texnologii peredachi dannix. 7-ye izd. -SPb Piter, K.: Izd. Gruppa BHV, 2003
5. Semenov Yu. V. «Proektirovanie setey svyazi sleduyushego pokoleniya» -

Spb.: Nauka i Texnika, 2005.

6. Kucheryaviy A.Ye., Gilchenok A.Z., Ivanov A.Yu., Paketnaya set svyazi obshego polzovaniya. –SPb.: Nauka i texnika, 2001

Elektron qo‘llanma

1 *P. B. Xramsov* Administrirovanie seti i servisov internet uchebnoe posobie. http://172.20.1.14/knigi_stat/internet/services/index. html © Sentr Informatsionnых Texnologiy, 1997

2 Maksim KULGIN SETI «Optimizatsiya raboty protokola TSR v raspredelennых setyax» http://172.20.1.14/knigi_stat/internet/tifamily/optimize01.html

3 *Vladimir Pleshakov* CISCO Internetworking Technology Overview *Server* http://172.20.1.14/knigi_stat/nets/ito/index.html *Mark-ITT*

4 D. Komer Protokoly TCP/IP Tom 1. Tamoyily, protokoly i arxitektura http://172.20.1.14/knigi_stat/internet/comer/contents.html

5 Radik Usmanov Protokol TCP. http://172.20.1.14/knigi_stat/internet/tifamily/tcpspec.html

6 Nikolay Malix Chto eto takoe - kommutator ili marshrutizator? http://172.20.1.14/knigi_stat/nets/ethernet/com_rout.html

Tarmoq protokollari

5350100 “Telekommunikatsiya texnologiyalari” (Telekommunikatsiyalar) ta’lim yo‘nalishi talabalari uchun o‘quv qo‘llanma

“MUT va T” kafedrasi majlisiida ko’rib chiqildi va chop etishga tavsiya etildi. 2017 yil “11” 04 № 32-son bayonnoma

“Telekommunikatsiya texnologiyalari” fakultetining ilmiy-uslubiy kengashida ko’rib chiqildi va chop etishga tavsiya etildi. 2017 yil “18” 04 № 8 - sonli bayonnoma.

Muhammad al-Xorazmiy nomidagi TATU ilmiy-uslubiy kengashida ko’rib chiqildi va chop etishga tavsiya etildi.
2018 yil “4” 05 № 8(99)- sonli bayonnoma

Tuzuvchilar: R.X. Djurayev
Sh.Yu. Djabbarov
Umirzakov B.M.

Taqrizchi: Sultonov I.
Amirsaidov U.

Ma’sul muxarrir: J.B. Baltayev

Musahhih: N.D. Yulanova