UOT 004.057.4

Cəfərov Z.Ə.
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
c.zafar@mail.ru

TELEKOMMUNİKASİYA ŞƏBƏKƏLƏRİNDƏ ÜNVANLAŞMA SİSTEMLƏRİNİN ANALİZİ

Məqalə telekommunikasiya şəbəkələrinin ünvanlaşma sistemlərinin analizi məsələsinə həsr olunmuşdur. Tədqiqat prosesində ünvanlaşma sistemlərinin arxitekturu, xarakteristikaları, tətbiq modelləri, IPv6 protokolunun yaranma səbəbləri və üstünlükləri araşdırılmışdır. Mövcud IPv4 ünvanlaşma versiyasında yaranan problemlər təhlil olunmuş və onların həlli üçün IPv6 protokolunun tətbiqinin vacibliyi göstərilmişdir.

Açar sözlər: *İnternet protokolu (IP), ünvanlaşma sistemləri, şəbəkə modelləri, dataqram.*

Giriş

Məlumatı paket kommutasiyalı texnologiya ilə mübadilə etmək üçün telekommunikasiya şəbəkəsinə qoşulmuş hər bir terminal unikal ünvana malik olmalıdır. Bu məqsədlə IP-protokoluna əsaslanan ünvanlaşma sistemi tətbiq edilir [1]. Maksimal çevikliyi təmin etmək və şəbəkə miqyasını nəzərə almaq üçün IPv4 ünvanlaşma sistemində sinifli model istifadə olunur. İnternetin intensiv istifadə olunması trafik xarakteristikalarının dəyişilməsinə, xidmət keyfiyyəti (*Quality of Service*, QoS) üzrə tələblərin sərtləşməsinə, şəbəkənin qovşaq və hostlarının sayının sürətlə artmasına və unikal ünvan ehtiyatlarının tükənməsinə səbəb olmuşdur. Ona görə də təşkilat şəbəkəsi daxilində qeydiyyat olunmayan ünvanların özəl ünvan fəzaları (*Private address*) kimi istifadə edilməsi məsləhət görülmüşdür. Tələb olunan və mümkün ünvan sayları arasında böyük fərq yarandığına və səmərəli istifadə olunmamasına görə ünvan çatışmazlığı problemi daha da kəskinləşdiyi üçün IPv4 ünvanların sinifsiz modelinə keçilmişdir. Tərtib olunan marşrut cədvəli üçün böyük yaddaş tələb edildiyinə görə ünvan axtarışına çox vaxt sərf olunur və nəticədə marşrutlayıcının məhsuldarlığı aşağı düşür. Əksər hallarda məxfilik tələb edilsə də, TCP/IPv4 modelinə görə məlumatlar açıq mətnlə mübadilə olunur. IPv4 protokolunun göstərilən və digər çatışmazlıqlarını aradan qaldırmaq üçün yeni İnternet protokolunun yeni versiyası (IPv6) işlənlənmişdir. Təqdim olunan işdə arxitektur və kəmiyyət parametrləri nəzərə alınmaqla IPv4 və IPv6 prokotolları müqayisəli təhlil olunmuşdur.

IP protokolun şəbəkə modellərində yeri

Telekommunikasiya şəbəkələrinin açıqlığını və çevikliyini təmin etmək məqsədilə OSI (Open Systems Interconnection) modeli təklif olunmuşdur. *Açıqlıq* mövcud texniki və proqram vasitələrini dəyişdirmədən yeni terminalların, terminallar sisteminin, rabitə kanallarının şəbəkəyə əlavə edilməsi imkanının olmasıdır. *Çeviklik* isə terminalların və ya rabitə vasitələrinin sıradan çıxması zamanı şəbəkənin fəaliyyətini davam etdirməsidir.

Şəbəkə arxitekturunu təsvir edən OSI modelinin tələblərinə görə informasiya sistemlərinin qarşılıqlı əlaqəsi 7 səviyyə üzrə təşkil olunur. Yuxarı platformada (*Application Set*) 7-ci (tətbiqi), 6-cı (təsviri) və 5-ci (seans), aşağı platformada (*Transport Set*) isə 4-cü (nəqliyyat), 3-cü (şəbəkə), 2-ci (kanal) və 1-ci (fiziki) səviyyələrin funksiyaları yerinə yetirilir (şəkil 1). OSI modeli telekommunikasiya şəbəkələrinin texniki təchizatından tutmuş proqram təminatına kimi fəaliyyət prinsiplərini izah edir. Ən aşağı üç səviyyə şəbəkədən asılıdır, yəni bu səviyyələrin protokolları kommunikasiya avadanlıqları ilə sıx bağlıdır. Yuxarı üç səviyyə istifadəçilərlə iş üçün nəzərdə tutulub və şəbəkə topologiyası və texnologiyasında baş verən dəyişiklik bu platforma protokollarına heç bir təsir göstərmir. Nəqliyyat səviyyəsi aralıq mövqe tutaraq, aşağı səviyyələrin bütün təfsilatlarını yuxarı platformadan "gizlədir". Hər bir səviyyə informasiya

Adətən, aşağı iki səviyyyənin funksiyaları aparat və proqram, yuxarıda qalan beş səviyyənin funksiyaları isə proqram vasitələri ilə reallaşdırılır [2].

		Mənbə		Ünvan		
Yuxarı platforma	7	*Məlumat* ⇩		⇧ *Məlumat*	7
	6	⇩		⇧	6
	5	⇩		⇧	5
Aşağı platforma	4	*Blok* ⇩		⇧ *Blok*	4
	3	*Paket* ⇩		⇧ *Paket*	3
	2	*Kadr* ⇩		⇧ *Kadr*	2
	1	▫▫▫▫⇨ 0010100010 (*bitlər*) ▫▫▫▫⇨			1

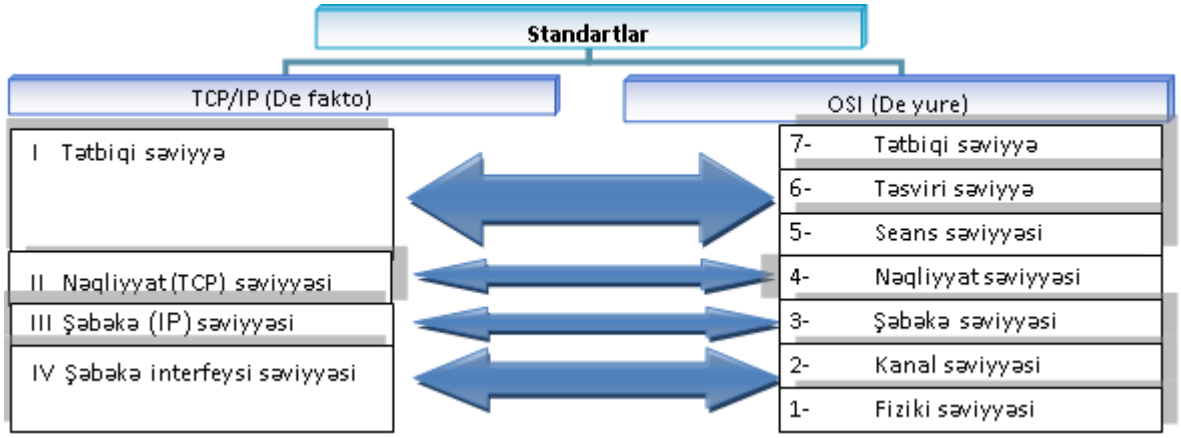
Şəkil 1. OSI modelinə görə informasiya sistemlərinin qarşılıqlı əlaqəsi

Lakin İnternetin təməli TCP/IP standartı əsasında qoyulmuşdur. İnternet şəbəkəsinin fəaliyyəti, məlumatların marşrutlaşması və ötürülməsindən başlayaraq şəbəkə avadanlıqlarının konfiqurasiyasına qədər funksiyaların yerinə yetirilməsi TCP/IP protokollar bazasında təşkil edilir [3]. Bu modelə malik şəbəkə arxitekturasında 4 səviyyə istifadə olunur (şəkil 2).

		Mənbə		Ünvan	
Application	*I*	*Məlumat* ⇩		⇧ *Məlumat*	*I*
TCP	*II*	*Blok* ⇩		⇧ *Blok*	*II*
IP	*III*	*Paket* ⇩		⇧ *Paket*	*III*
Link	*IV*	*Kadr* ⇩ ⇨		⇧ *Kadr* ⇨	*IV*

Şəkil 2. TCP/IP modelinə görə kompüterlərin qarşılıqlı əlaqəsi

Hər halda OSI və TCP/IP arxitekturları arasında aşkar uyğunluqlar var (şəkil 3).



Şəkil 3. Şəbəkə arxitekturu üzrə standart modellərin səviyyə uyğunluqları

TCP/IP modelinin ən aşağı səviyyəsi (IV səviyyə) şəbəkə qurğuları arasında fiziki mühit üzrə verilənlərin mübadiləsini təmin edərək, OSI modelinin 1-ci (fiziki) və 2-ci (kanal) səviyyələrinə birgə uyğun gəlir. Şəbəkə interfeysi (*Network İnterface Layer*) adlanan bu səviyyədə lokal şəbəkələr üzrə fiziki və kanal səviyyələrin məlum protokolları istifadə olunur.

Bu protokollar TCP/IP stekində reqlamentləşdirilmir. Növbəti, III səviyyə (*Network Layer*) şəbəkələrarası əlaqə səviyyəsi adlanır. II, nəqliyyat səviyyəsi (*Transport Layer*) məlumat mübadiləsinə nəzarət funksiyalarını yerinə yetirməklə TCP/IP modelinin əsas səviyyəsi hesab olunur. TCP/IP modelinin ən yuxarı, I səviyyəsi tətbiqi səviyyə (*Application Layer*) adlanır. Bu səviyyə aşağı platformanın protokolları bazasında kommunikasiya proqramlarını fəallaşdırır [2].

Cədvəl 1-də şəbəkə arxitekturunun standart (TCP/IP və OSI) modelləri üzrə səviyyələr haqqında məlumat göstərilmişdir.

Cədvəl 1

Şəbəkə arxitekturunun standart modelləri üzrə səviyyələr

Şəbəkə modellərinin səviyyələri					
Plat-forma	TCP/IP modeli	OSI modeli	Səviyyə funksiyaları	Şəbəkədən asıllığı	İcra vasitələri
Yuxarı plat-forma *(Appli--cation Set)*	I-Tətbiqi səviyyə (Application Layer)	7-Tətbiqi səviyyə (Application Layer)	Kommunikasiya proqram-larının tətbiq olunması		
		6-Təsviri səviyyə (Presentation Layer)	Sıxılma, kodlama, şifrələmə standartlarının, multimedia formatlarının istifadə edilməsi	Asılı olmayan	Proqram (SoftWare)
		5-Seans səviyyəsi (Session Layer)	Rabitə seanslarının təşkili		
Aşağı plat-forma *(Trans-port Set)*	II-Nəqliyyat səviyyəsi (Transport Layer)	4-Nəqliyyat səviyyəsi (Transport Layer)	Məlumat mübadiləsinin idarə olunması	Aralı q səviyyə	
	III-Şəbəkə səviyyəsi (Net-work Layer)	3-Şəbəkə səviyyəsi (Network Layer)	Paketlərin göstərilən ünvana çatdırılması üçün optimal marşrutun seçilməsi		
	IV -Şəbəkə interfeysi səviyyəsi (Network İnterface Layer)	2-Kanal səviyyəsi (Data-Link Layer)	Kadrın hazırlanması, rabitə xəttinə giriş/çıxışının təşkili və düzgünlüyün yoxlanması;	Şəbəkə-dən asılı	Proqram-aparat
		1-Fiziki səviyyə (Physical Layer)	Bitlər ardıcıllığı ilə təsvir olunmuş informasiyanın ötü-rülməsi mühitinin yaradılması.		Aparat (HardWare)

IP protokolun əsas funksiyası

İP protokolu TCP/IP və OSI modelləri üzrə 3-cü səviyyənin şəbəkələrarası əlaqə funksiyalarını reallaşdırır. Ümumi halda şəbəkə səviyyəsinin profili daha genişdir (cədvəl 2). Müxtəlif texnologiyaların uzlaşdırılması, iri şəbəkələrdə ünvanlaşmanın sadələşdirilməsi, şəbəkələr arasında parazit trafiklərin mübadiləsinin qarşısının çevik və etibarlı alınması və s. məsələlər də bu səviyyədə həll olunur. Şəbəkə səviyyəsi məlumat mübadiləsini *dataqram* vasitəsilə yerinə yetirir.

Dataqram TCP/IP sisteminin əməliyyat apardığı protokol vahididir. Bu anlayışın şəbəkə xarakteristikaları ilə hec cür əlaqəli olmaması TCP/IP protokollarının avadanlıqlardan qeyri-asılılığını təmin edir. Dataqramın tərkibinə onun əlaqəli şəbəkələr üzrə nəqli üçün ünvan məlumatları daxil edilir. Şəbəkə səviyyəsi marşrut cədvəllərini hazırlayan protokolları da özündə cəmləşdirir. IP protokolu şəbəkə interfeysi səviyyəsinin protokolları bazasında fəaliyyət göstərərək dataqramın marşrutlaşması, fraqmentləşməsi və yığılıb toplanması funksiyalarını yerinə yetirir. Burada dataqram lokal şəbəkənin kadrına çevrilərək fiziki mübadilə səviyyəsinə təqdim edilir [4].

Cədvəl 2

Şəbəkə səviyyəsinin xarakteristikaları

Şəbəkə səviyyəsinin xarakteristikaları	
Funksiyalar	Məlumatın ötürülməsi yolunun təyin edilməsi (marşrutlaşdırma)
	Məntiqi ünvanların fiziki (aparat) ünvana translyasiyası
	Kommutasiya
	Fraqmentasiya
	Şəbəkədəki pozuntu və həddən artıq yüklənmə hallarının izlənməsi
Məsələlər	Qeyri-standart strukturlu əlaqələr üzrə məlumatların ötürülməsi
	Müxtəlif texnologiyaların uzlaşdırılması
	İri şəbəkələrdə ünvanlaşmanın sadələşdirilməsi
	Parazit trafiklərin mübadiləsinin qarşısının alınması
Protokollar	Şəbəkə protokolları (dataqramın şəbəkə üzrə ötüülməsi): IP, IPX, IPSec
	Marşrutlaşdırma protokolları: RIP, OSPF, IS-IS, BGP
	İdarəetmə protokolları: ICMP, IGMP, ARP, RARP, DHCP
Üstünlüklər	Lokal şəbəkələrlə sıx əlaqə
	Daxilolma səviyyəsində müxtəlif şəbəkə texnologiyalarının istifadə olunması
	Təkamüllü inkişaf
	Yeni tələblərə cəld adaptasiya
	Kütləvi yayılma
	Xidmət dəyərlərinin aşağı olması
Çətinliklər	Əlavə məsariflər
	Təhlükəsizlik
	Xidmət keyfiyyəti

IP-şəbəkəsinə qoşulmuş hər bir hostda IP-dataqramları eyni ünvanlaşma, fraqmentləşmə və marşrutlaşma qaydası ilə emal olunur. IP protokolu məntiqi seans və ya virtual kanalların digər identifikasiya vasitələrini istifadə etmədiyinə görə hostlar dataqramları ayrıca bir protokol vahidi kimi qəbul edirlər. IP protokolu TCP/IP modelli şəbəkə üzrə mübadilə olunan məlumatın dəqiq formatını göstərməklə şəbəkədə verilənlərin ötürülməsinin baza vahidini - "*IP dataqramı*"nı müəyyən edir (şəkil 4).

Versiya (IP v4 və ya IP v6)	Başlığın uzunluğu (*Header length*)	Xidmət növü *(Type of Service*)	Dataqramın uzunluğu (Total Length)
Fraqment identifikatoru	Bayraq (paket üzərində DF – fraqmentləşməmiş, MF- fraqmentləşmiş)	Fraqmentin uzunluğu *(Fragment Offset)*	
Paketin şəbəkədə mövcudluq müddəti *(TTL-Time to Live)*	Transport Layer Protocol (TCP və ya UDP)	Başlığın nəzarət cəmi (*Header Checksum*)	
Paketi göndərənin (Source) IP- ünvanı			
Paketi alanın (Destination) IP- ünvanı			
Opsiya (boş ola bilər) - *məxfilik, mühafizə və keyfiyyəti təmin etmək üçün məlumat*			Tamamlayıcı
Verilənlər (istifadəçi məlumatı)			

Şəkil 4. IP dataqramı

IP paketi iki hissədən ibarət olur: başlıq və faydalı informasiya (istifadəçi məlumatı) (şəkil 5).

Başlıq			*İstifadəçi məlumatı*
S	D		00001..01010.....11100101010

S = Source Address ("Göndərənin ünvanı"); D = Destination Address ("Alanın ünvanı")

Şəkil 5. IP paketin strukturu

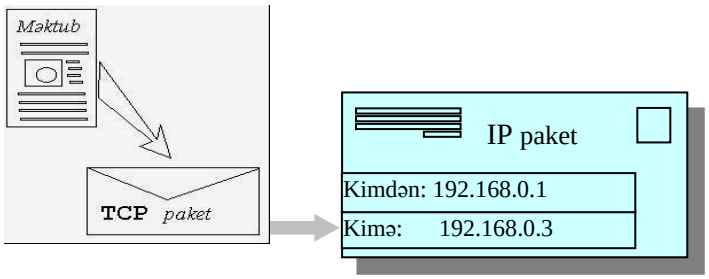
IP başlığının birinci hissəsində məlumat mübadiləsində iştirak edən kompüterin hansı şəbəkəyə mənsub olduğunu marşrutlayıcıya bildirən informasiya saxlanılır. Başlığın ikinci hissəsində paketin hansı kompüterə çatdırılmasını təyin edən informasiya əks olunur.

TCP/IP arxitekturalı şəbəkələrdə məlumat paketlərlə göndərilir. Şəbəkə səviyyəsində IP protokolu sistemlərarası seans yaratmadan paketlərin təyin edilmiş ünvana çatdırılması xidmətini göstərir. IP protokolu hər bir paket üzrə ayrılıqda marşrut təyin etdiyi üçün dataqramların tələb olunan ardıcıllıqda etibarlı catdırılmasına zəmanət verilmir. Hostlar arasında təsdiqləmə mexanizmi mövcud deyildir. Paketlər itə, korlana, tirajlana bilər və s. Məlumatın həcmi paketin standart uzunluğundan böyük ola bilər. Paketin başlığı üçün nəzarət cəmi hesablansa da, istifadəçi məlumatının düzgün ötürülməsinə nəzarət edilmir. Paket mübadiləsi idarə olunmur, təkrar göndəriş dəstəklənmir.

Bu problemlər OSI və TCP/IP modellərinin eyniadlı, nəqliyyat səviyyəsində həll olunaraq kompüterlər arasında məlumatın etibarlı mübadiləsi təmin edilir. Bu səviyyədə məlumat mübadiləsini idarə edən TCP (*Transmission Control Protocol*) və ya qısa məlumatların rabitə seansı yaratmadan mübadiləsini idarə edən UDP (*User Dataqram Protocol*) protokolu istifadə olunur. Məlumatı TCP protokolu paketlərə bölür. Verilənləri düzgün ardıcıllıqla yerləşdirmək və məlumatın tamlığını yoxlamaq üçün hər bir porsiya nömrələnir. Qəbul edən tərəfdə, TCP protokolu paketləri yığır, düzgün ardıcıllıqda yerləşdirir, hər hansı bir porsiya çatmırsa, onun təkrar göndərilməsi tələb ediilir, bundan sonra məlumat TCP xidmətindən istifadə edən tətbiqi proqrama ötürülür. TCP protokolunun paketləri IP-dataqramın «Verilənlər» sahəsinə yerləşdirilir. TCP paketinin başlığı dataqramın başlığına əlavə edilir.

Ünvanlaşma sistemlərinin modelləri

İnternet şəbəkəsinin müxtəlif qovşaqlarını əlaqələndirmək üçün marşrutlayıcılardan (*router*) istifadə edilir [5]. TCP/IP=(TCP+IP) modelində IP protokolu məlumatın hara, TCP isə necə mübadilə olunmasını təyin edir (şəkil 6).



Şəkil 6. IP paketi

IPv4 protokolunun arxitekturuna görə ünvanlar 32 bit uzunluğa malik olub, "." (nöqtə) ilə ayırılan 4 oktetdən (*octets*) ibarətdir. Hər oktetin aldığı qiymət [0÷255] intervalına düşür. Asanlıqla hesablamaq olar ki, müxtəlif IP-ünvanların sayı 4 milyarddan artıqdır: $K=2^{32}=4\ 294\ 967\ 296$. IP-ünvan anlayışı host termini ilə sıx bağlıdır. Yalnız şəbəkəyə qoşulmuş kompüterlər deyil, həmçinin şəbəkənin marşrutlayıcısı, kommutatoru və s. kommunikasiya avadanlıqları da host hesab olunur. IP ünvanlaşma sistemi Internet şəbəkəsinin xüsusiyyətini nəzərə alır. Belə ki, İnternet ayr-ayrı kompüterlərin birləşməsi deyil, şəbəkələr şəbəkəsi olduğuna görə hər bir IP-ünvan iki hissədən təşkil olunur: 1) şəbəkənin ünvanı (şəbəkənin identifikatoru, Network_ID); 2) host ünvanı (hostun identifikatoru, Host_ID). Network İD (Net_ID) - IP ünvanda kompüterin mənsub olduğu şəbəkənin nömrəsini göstərən hissədir. Net_ID **(**şəbəkənin nömrəsi) administrator tərəfindən InterNIC *(The Internet's Network Information Center*) təşkilatının məsləhəti ilə təyin ediilir. Host_ID şəbəkə daxilində kompüterlərin bir-birindən fərqlənməsini təmin edir.

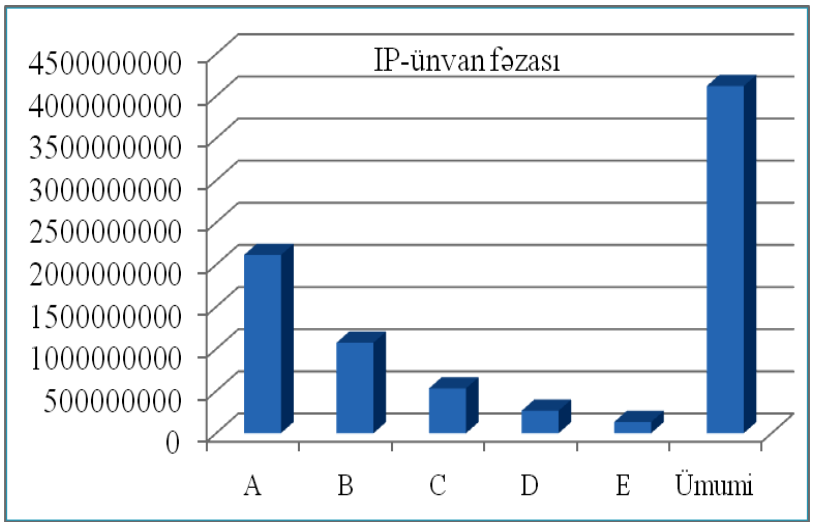
Bütün kompüterlər üçün eyni qiymətə malik olduğuna görə, IP ünvanın şəbəkənin nömrəsini (Net_ID) göstərən hissəsini dəyişmək olmaz. Host_ID-dəki bitləri iki hissəyə bölərək hər bir seqment üçün unikal nömrə (Subnet_ID) yaradılır. Birinci hissə seqmenti unikal bir altşəbəkə kimi qəbul edilməsi, ikinci hissə isə hostu fərqləndirmək üçün istifadə olunur. Buna "*subnetting"* və ya "*subnetworking"* deyilir.

IP-ünvanlaşma prosesində şəbəkənin miqyasını nəzərə almaq üçün üç əsas sinif - A, B və C tətbiq edilir. D və E siniflər isə xüsusi məqsədlə istifadə olunur [6]. Şəbəkənin sinfindən asılı olaraq IP-ünvanın oktetləri şəbəkə və host ünvanlarına ayrılır. Şəbəkə siniflərini fərqləndirmək üçün IP-ünvanın birinci oktetinin ikilik təsviri üzrə yuxarı bitləri və onluq qiyməti istifadə edilir. Şəbəkələrin sinifli modeli üzrə IPv4 ünvanın struktur və kəmiyyət xarakteristkaları aşağıda (cədvəl 3 və şəkil 7) əks etdirilir.

Cədvəl 3

IPv4 ünvanın struktur və kəmiyyət xarakteristikaları

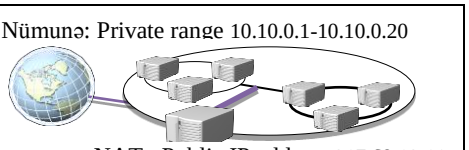
Sinif	IP ünvanin oktetləri		Şəbəkə və kompüter identifikatoru üçün ayrılmış bitlərin sayı		Şəbəkə identifikatorunun birinci oktetinin yuxarı mərtəbə bitləri və aldığı qiymətlərin intervalı		Şəbəkələrin və şəbəkədəki kompüterlərin (hostların) sayı		Ünvan fəzası
	NET-WORK	HOST							
A	1	3	7	24	0	1 -126	126	16 777 214	2113928964
B	2	2	14	16	1 0 · · ·	128-191	16384	65 534	1073709056
C	3	1	21	8	1 1 0 · ·	192-223	2 097 152	254	532676608
D	Geniş yayım		20	8	1 1 1 0 ·	224-239	1048576	254	266338304
E	Ehtiyat nömrə		19	8	1 1 1 1 0	240-247	524288	254	133169152
								Cəmi:	4119822084



Şəkil 7. IPv4 ünvan fəzasının siniflər üzrə paylanması

Diaqramdan göründüyü kimi, IPv4 protokolu üzrə ünvan fəzasının yarısını A sinfə mənsub kodlar təsvir edir. İnternet şəbəkəsinin unikal ünvan ehtiyatları demək olar ki, tükənmişdir. Ona görə də, təşkilat şəbəkəsi daxilində özəl (*Private address*) ünvanlardan istifadə edə bilər. RFC1918 sənədlərində bu məqsədlə aşağıdakı siniflər üzrə ünvan fəzalarından istifadə olunması məsləhət görülür (şəkil 8):

Şəbəkə sinifləri	Sayı	Diapazon
A	1 ədəd	[10.0.0.0 ÷ 10.255.255.255]
B	16 ədəd	[172.16.0.0 ÷ 172.31.255.255]
C	256 ədəd	[192.168.0.0 ÷ 192.168.255.255]



Şəkil 8. Özəl ünvanlar və NAT sxemi

Özəl ünvana malik hostların İnternetlə əlaqə zərurəti yarandıqda *şəbəkə ünvanlarının translyasiya*sı (*Network Address Translation*, NAT) texnologiyası tətbiq olunur.

Sinifsiz ünvanlaşma modeli

Fərz edək ki, İnternetə qoşulmuş lokal şəbəkə 2000 kompüterdən təşkil olunmalıdır. Ünvan məkanı əldə etmək üçün bir *B* ya da səkkiz *C* sinif şəbəkə seçilə bilər. *B* sinif şəbəkənin hər biri 65534 ünvan tutur ki, bu da tələb ediləndən dəfələrlə artiq olur. 8 ədəd *C* sinif şəbəkə (2032 ünvan kodu) seçildikdə isə aşağıdakı problem yaranır: onların hər biri marşrut cədvəlində ayrıca bir sətirlə təsvir edilir, marşrutlayıcıya nəzərən öz aralarında mütləq əlaqəyə malik olmayan 8 fiziki şəbəkə bir lokal şəbəkədə yerləşir, eyni marşruta malik olduqlarına baxmayaraq, dataqramlar bir-birindən asılı olmayaraq marşrutlaşdırılır. Ünvan məkanına bu cür qənaət etməklə xidməti (idarəetmə) trafik və marşrut cədvəli ilə işin təmini və emalı üzrə məxaricər də dəfələrlə artırılmış olur. Bu səbəbdən və həm də tələb olunan və ayrıla bilən ünvan sayları arasında yaranan böyük say fərqinə görə sinifli model üzrə IP-ünvanlarından səmərəli istifadə edilmir.

Qeyd olunanlardan əlavə şəbəkə və host nömrələri arasında oktetlər ilə sədd çəkilməsinin heç bir formal səbəbi mövcud deyil və münasib təqdim olunması üçün IP-ünvanlar siniflərə ayrılmışdır. Sinifdən kənar ünvanlaşma sistemində isə IP-ünvan daxilində şəbəkə və host bitləri ixtiyari qaydada hissələrə ayrılır və IP-ünvana 32 mərtəbəli şəbəkə maskası (*netmask)* əlavə edilir. Bu maska şəbəkə identifikatorunu göstərən mərtəbələrə "1", hostun nömrəsini göstərən mərtəbələrə isə "0" yazılmaqla tərtib olunur. Sinifsiz modelə görə IP ünvanı *a.b.c.d*/*N* formatda təsvir olunur, burada *a.b.c.d* -ünvan, *N* isə şəbəkə identifikatorunu əks etdirən bitlərin sayını göstərir [7]. Məsələn, 138.158.128.0/17 ünvanlı şəbəkə üçün maskada ardıcıl olaraq 17 ədəd "1", 15 ədəd isə "0" əks olunur: 11111111.11111111.10000000.00000000.

IP-ünvanda şəbəkə və host nömrələri üçün ayrılmış ikilik mərtəbələrin sayını bilərək, şəbəkələrin və onlara mənsub hostların maksimal saylarını təyin etmək olur:

$$Q_{Net}^{\max} = 2^N - 2,\ Q_{host}^{\max} = 2^H - 2$$

burada *N* və *H=(32-N)* şəbəkə və kompüter nömrələri üçün ayrılmış ikilik mərtəbələrin uyğun sayıdır. Cədvəl 4-də sinifsiz model üzrə bütün (*N* =[1÷32]) qiymətləri üçün şəbəkə maskasının onluq təsviri əks olunmuşdur.

Cədvəl 4

Sinifsiz model üzrə şəbəkə maskaları

/N	ŞƏBƏKƏ MASKALARI	/N	ŞƏBƏKƏ MASKALARI	/N	ŞƏBƏKƏ MASKALARI	/N	ŞƏBƏKƏ MASKALARI
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

Sinifsiz model üzrə IP-ünvanın *Netmaska* təsviri ilə bit-bit hasilinə görə şəbəkə identifikatorunu (*Network_İD*), maskanın inkarı (*No_netmask*) ilə bit-bit hasilinə görə host identifikatorunu (*Host_İD*) təyin etmək olar. Məsələn, IP = 205.38.193.134/26 ünvanı 205.38.193.128 koda malik şəbəkədə 6 nömrəli hostu təsvir edir:

IP =	11001101 00100101 11000111 10000110	= 205.38.193.134
Netmask =	11111111 11111111 11111111 11000000	= 255.255.255.192
No_netmask =	00000000 00000000 00000000 00111111	= 0.0.0.63
Network_İD=	11001101 00100101 11000111 10000000	= 205.38.193.128
Host _İD =	00000000 00000000 00000000 00000110	= 6

Göründüyü kimi, tələb edilən və ayrıla bilən ünvan sayları arasında fərqi minimuma endirməklə sinifsiz model üzrə IPv4 protokolunun ünvan fəzalarından qismən səmərəli istifadə olunur. Sinifsiz ünvanlaşma modeli *İnternetdə birbaşa sinifsiz marşrutlama* (*Classless Internet Direct Routing*, CIDR) adlanır.

Hal-hazırda sinifli ünvanlaşma modeli köhnəlmiş hesab edilərək IP-ünvan blokları CIDR model ilə təqdim edilir.

IPv6 ünvanlaşma sisteminin üstünlükləri

Qovşaq və hostların sayının sürətlə artması IPv4 protokollu şəbəkələrdə ünvan böhranı yaratmışdır. Bundan əlavə, yüz minlərlə sətirə malik cədvəllərlə iş, paketlərin fraqmentləşdirilməsi və s. prosedurlar marşrutlayıcıların həddindən artiq yüklənməsinə səbəb olur və şəbəkənin məhsuldarlığı aşağı düşür. Açıq mətnlə ötürüldüyü üçün məlumatların məxfiliyi təmin edilmir [8]. IETF (*Internet Engineering Task Force*) komitəsi mövcud problemləri IPv6 kimi məhşurlaşan IPng (*Internet Protocol next generation*) – yeni nəsil şəbəkələrarası protokolun vasitəsilə həll edir.

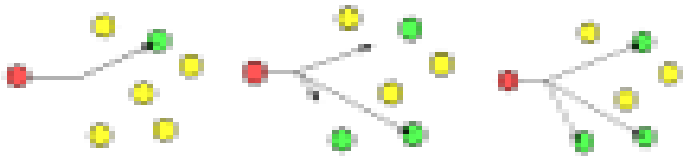
IPv6 protokolunun əsas fərqli cəhəti daha uzun (128 bit) strukturlu ünvandan istifadə olunmasıdır. Ünvandakı mərtəbələrin sayının bu qədər artırılması ünvan çatışmazlığı problemini həll edir və şəbəkənin fəaliyyətinin daha səmərəli təşkil edilməsi məqsədi daşıyır [9].

IPv4 ünvanın ikisəviyyəli iyerarxiyası (şəbəkə və host nömrələri) əvəzinə IPv6 protokolunda 4 səviyyə istifadə olunur ki, onlardan üçü şəbəkənin, biri isə qovşağın identifikasiyası üçün nəzərdə tutulur. Yeni strukturda iyerarxiya səviyyələrinin artması ünvanların aqreqasiyası texnologiyasının (CIDR) fəaliyyətini təmin edir və marşrutlama üzrə resurs itkilərini aradan qaldırır.

IP protokolunun 6-cı versiyasında ünvanın yeni təsvir qaydası qəbul olunmuşdur, belə ki, şəbəkə ünvanını təyin edərkən əksər hallarda maskanın sərhədləri baytın ala biləcəyi qiymətlərlə üst-üstə düşmədiyinə görə onaltılıq təsvir münasib hesab edilmişdir. IPv6 protokolunda ünvanlar 128 *bit* və ya 16 *bayt* uzunluğa, 16 bitli (65536 kombinasiyalı, 0÷FFFF) 8 oktetə malikdir. IPv6-da ünvanların sayı 2^{128} -ə ($3.4x10^{38}$, yer kürəsinin hər kvadrat metrinə düşən ünvan sayı $6.6x10^{23}$-ə bərabərdir) bərabərdir. IPv6 sistemində ünvan onaltılıq say sistemində dörd rəqəmli ədədləri ":" (qoşa nöqtə) ilə ayırmaqla təsvir olunur, məsələn: FEDC:OA96:0:0:0:0:7733:567A. IP protokolunun hər iki (IPv4 və IPv6) versiyasını dəstəkləyən şəbəkələr üçün 4 ədəd aşağı mərtəbəli baytın ənənəvi onluq təsvirlə istifadə olunması imkanı vardır, məsələn: 0:0:0:0:0:FFFR 194.135.75.104.

IPv6 ünvanlaşma sistemində 4-cü versiya üzrə tətbiq edilən xüsusi ünvanlar ümumiləşdirilmiş və əsasən aşağıdakı növ ünvanlar təyin olunmuşdur: *unicast, anycast, multicast* (şəkil 9).

Müxtəlif marşrut sxemlərinə malik ünvan növləri *prefiks formatı* adı almış ən yuxarı mərtəbə bitlərinin qiymətinə görə təyin edilir. IPv4 modelindən fərqi olaraq IPv6 sistemində *broadcast* (geniş məntiqi əlaqə) ünvanı movcud deyil.



Şəkil 9. Marşrut sxemləri

Unicast növ ünvan ayrıca bir qovşağı – kompüteri və ya marşrutlayıcı portunu təyin edir. Paket həmin ünvana ən qisa yol üzrə çatdırılır. *Cluster* (*anycast*) – klaster növ ünvan ümumi ünvan prefiksinə malik multicast kimi qovşaqlar qrupunu təyin edir. Lakin burada paket həmin qovşaqlar qrupuna ən qisa yol üzrə marşrutlandırılır, sonra «ən yaxında» yerləşən qovşaqlarından birinə çatdırılır. *Multicast* – çoxəlaqəli ünvan müxtəlif fiziki şəbəkələrə mənsub olsa belə, qovşaqlar çoxluğunun ünvanını təyin edir.

IPv6 protokolunda identifikasiya, şifrələmə və s. digər prosedurları asanlaşdırmaq üçün paketin başlığına yeni sahələr əlavə edilmişdir. Paket başlığının yeni sxemi onu minimum informasiya daşiyan *əsas* və iştirakı məcburi olmayan *əlavə* hissələrə ayırmağa imkan verir. Bu yanaşma opsional (dəyişkən) başlığın təyin olunması yolu ilə IPv6 protokolunun imkanlarını genişləndirir və onu həm də açıq edir [10].

IPv6 dataqramının uzunluğu 40 bayt təşkil edən əsas başlığı aşağıdakı formata malikdir (şəkil 10):

Versiya (4 *bit*)	Trafik sinfi (8 *bit*)	Trafikin nişanı (20 *bit*)	
Başlığın uzunluğu (16 *bit*)		Növbəti başlıq (8 *bit*)	Keçid limiti (8 *bit*)
Paketi göndərənin (Source) IP- ünvanı			
Paket göndərilənin (Destination) IP- ünvanı			

Şəkil 10. IPv6 dataqramının əsas başlığının formatı

Trafik sinfi (Traffic Class) sahəsi təyinatına görə IPv4 protokolunda *Xidmət növü* (*Type of Service*) sahəsinə, *Keçid limiti* (Hop Limit) isə paketin şəbəkədə mövcudluq müddətini göstərən TTL (*Time to Live*) sahəsinə ekvivalentdir. *Trafikin nişanı* (*Flow Label*) onun seçilməsi və ayrıca emal olunmasına imkan verir. Bu isə marşrutlayıcıların yükünün azalması baxımından çox vacibdir. *Növbəti başlıq* (*Next Header*) sahəsi IPv4 versiyası üzrə protokol (*Protocol*) sahəsinə analojidir və əsas başlığın davamı olan əlavə başlığın növünü göstərir. Hər bir əlavə başlıq Next Header sahəsinə malikdir. Dataqram əlavə başlığa malik deyilsə, *növbəti başlıq* sahəsində faydalı yükün nəqlinin təşkili üçün istifadə edilən protokollardan (TCP, UDP) biri qeyd olunur. IPv6 standartına görə təyin olunmuş başlıq növləri cədvəl 5-də göstərilir.

Cədvəl 5

IPv6 standartına üzrə başlıq növləri

Başlıqlar	İzahı
Routing	Dataqramı göndərənin seçdiyi marşrut haqqında informasiya
Fragmentation	Dataqramın fraqmentləri haqqında məlumat
Authentication	Göndərənin əsilliyinin yoxlanması üçün zəruri olan parametrlər
Encapsulation	Məxfiliyin təmin edilməsi üçün zəruri olan məlumat
Hop-by-Hop Options	Paketin emalı üçün xüsusi parametrlər
Destination Options	Təyinat qovşağı üçün əlavə parametrlər

IPv6 protokoluna keçid zamanı marşrutlayıcıların yükü azalır. Buna yeni İnternet protokolunun malik olduğu aşağıdakı xüsusiyyətlər imkan verir. IPv6 dataqramının əlavə başlıqları son qovşaq və sərhəd marşrutlayıcılarında emal olunur. Bu isə marşrutlayıcıların iş alqoritmini sadələşdirir və vacib funksiyaların aparat səviyyəsində asanlıqla reallaşdırılmasına imkan yaradır. IPv6 dataqramının fraqmentləşməsi üzrə funksiyalar da son qovşaq və sərhəd marşrutlayıcılarında yerinə yetirilir. Son qovşaqlar marşrut üzrə paketin minimal uzunluğunu təyin edir və paket bu qiyməti aşmayan ölçü ilə ötürülür. Paketin marşrut üzrə ölçüsünün təyin edilməsi *Path* MTU (*Maximum Transfer Unit*) *discover* texnologiyası adlanır. IPv6 protokolunu dəstəkləyən marşrutlayıcılar şəbəkənin nüvəsində fraqmentləşmə aparmır, yalnız ICMP protokolunun «çox uzun paket» xəbərdarlığını son qovşağa çatdırır.

Marşrutlaşmanın göndərən (məsələn, sərhəd marşrutlayıcıları) tərəfdən idarə olunması şəbəkənin nüvəsindəki marşrutlayıcıları növbəti marşrutu seçmək üçün ünvan cədvəlində axtarışdan azad edir. Əlavə altbaşlıq ən optimal yola istiqamətləndirərək paketin marşrutuna tam nəzarət olunmasına imkan verir. Lokal şəbəkədə qovşaq ünvanı kimi şəbəkə interfeysi üzrə MAC (*Media Access Control*) ünvanın istifadə olunması ARP (*Address Resolution Protocol*) protokolunun tətbiqi zərurətini aradan qaldırır.

Təhlükəsizlik (seans iştirakçılarının identifikasiya, autentifikasiya və avtorizasiyası, məlumatların şifrələnməsi) prosedurları IPv6 standartının tərkib hissəsi olan IPSec protokolu ilə yerinə yetirilir [11].

IPv6 protokolu öz funksiyalarının hərəkət edən obyektlər üzrə istifadə olunmasına imkan verən mexanizmlərə də malikdir [12].

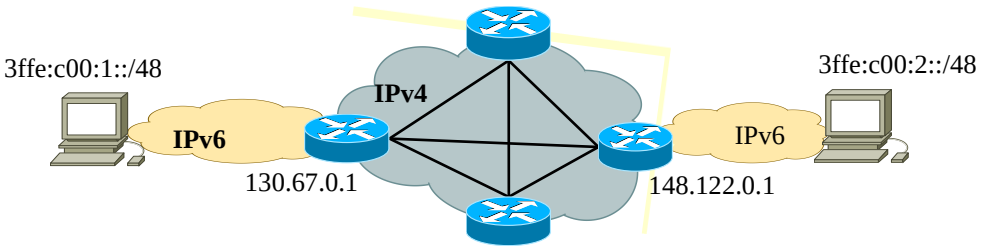
IPv4 və IPv6 protokollarının bəzi xarakteristikaları cədvəl 6-da əks olunur.

Cədvəl 6

IPv4 və IPv6 protokollarının müqayisəli xarakteristikaları

Xarakteristikalar	**IPv4**	**IPv6**
Ünvanın uzunluğu	32-bit (4-bayt)	128-bit (16-bayt)
Mümkün ünvanların sayı	2^{32}	2^{128}
Oktetlərin sayı	4	8
Oktetin uzunluğu	8 bit (256 kombinasiya 0÷255)	16 bit (65 536 kombinasiya 0÷FFFF)
İdentifikasiya səviyyəsi	*a.b.c.d* identifikasiyası səviyyəsi-3: • *a.b* – şəbəkənin ünvanı • *c* – altşəbəkənin ünvanı • *d* – altşəbəkədə host- ünvanı	*a.b.c.d.e* identifikasiyası səviyyəsi-5: • *a* – provayder • *b* – provayderin klasteri • *c* – abunəçinin identifikatoru • *d* –şəbəkə identifikatoru • *e* –hostun identifikatoru
Ünvan sinfləri	*A,B,C,D,E*	*Tətbiq olunmur*
Ünvan fəzası	Public/ Private	Global/ Site-local ünvan (FEC0::/10)
Multicast ünvan	(224.0.0.0 /4)	(FF00::/8)
Broadcast	*Tətbiq olunur*	*Tətbiq olunmur*
Susma marşrutu	127.0.0.1	::
Loopback ünvan	127.0.0.1	::1

IPv6 protokolu, istifadəsinə mərhələlərlə keçid nəzərə alınmaqla layihələndirilmişdir ki, müxtəlif versiyalar üzrə fəaliyyət göstərən qovşaqların qarşılıqlı əlaqələri təmin edilsin. Bunun üçün qovşaqlarda iki protokol steki yerləşdirilir və protokolun müxtəlif versiyası ilə dəstəklənən işçi stansiyalarla qarşılıqlı əlaqələri yaradan zaman uyğun TCP/IP steki istifadə olunur. Bu halda marşrutlayıcılar hər iki protokolu ayrı-ayrılıqda emal edir. IPv4 və IPv6 paketləri bir-birinə xüsusi şlüz vasitəsilə çevirilir (şəkil 11).



Şəkil 11. IP dataqramların konversiyası

Bu prosesin ən vacib tərkib hissəsi ünvanların çevrilməsidir. Həmin proseduru sadələşdirmək üçün «birgə IPv6 və IPv4 ünvanları» adlanan mexanizm tətbiq olunur ki, burada 4 ədəd aşağı mərtəbəli baytlar IPv4 protokoluna analoji istifadə edilir. Bir protokol başqa protokol bazasında qurulmuş şəbəkədə tunelləşdirilərək inkapsulyasiya olunur. Bu zaman paket digər protokolun paketinə yerləşdirilir. Hal-hazırda IPv6 paketlərinin İnternetin bu protokolu dəstəkləməyən şəbəkə sahələrində tranziti zamanı inkapsulyasiya texnologiyası üzrə təcrübi zonalar yaradılmışdır [13]. IP protokolunun modernləşdirilməsini təyin edən standartlar RFC 2373 («IP Version 6 Addressing Architecture») sənədlərində əks olunur.

Nəticə

Yeni nəsil İnternet protokolu (IPv6) şəbəkədə xidmət keyfiyyəti, informasiya təhlükəsizliyi, ünvan böhranı və s. məsələlərin həlli ilə əlaqadar olaraq IPv4 prokolununun çatışmazlıqlarını aradan qaldırmaq üçün işlənib-hazırlanmışdır. IPv6 modelində ünvanlaşmanın yeni genişlənmiş sxemi yaradılmışdır. Ünvan uzunluğunun artırılmasında başlıca məqsəd ünvanlaşma sisteminin funksional imkanlarının genişləndirilməsi və şəbəkənin fəaliyyətinin daha səmərəli təşkili olmuşdur. IPv6 protokolu marşrutlama funksiyalarının optimallaşdırılmasına imkan verir. Ünvanların aqreqasiyalaşdırılması marşrutlayıcılarda ünvan cədvəlinin ölçüsünü və uyğun olaraq növbəti marşrutlayıcını seçmək üçün axtarış vaxtını qısaldır. Marşrutlama üçün əlavə altbaşlıq ən optimal yola istiqamətlənərək paketin marşrutuna tam nəzarət olunmasına imkan verir. Marşrutlama funksiyalarının ixtisarı hesabına şəbəkənin miqyaslaşma imkanı artır. ARP protokolunun tətbiqi zərurətinin aradan qaldırılması şəbəkənin məhsuldarlığını yüksəldir. IPv6 standartı məlumatların mühafizəsini təmin edir. Bunlardan əlavə, IPv6 protokolu öz funksiyalarının hərəkət edən obyektlər üzrə istifadə olunmasına da imkan verən mexanizmlərə malikdir. Bu xüsusiyyətlər IPv6 protokoluna keçidin vacibliyini göstərir.

Ədəbiyyat

1. Ситанов С.В., Алаева С.С. Компьютерные сети, Иваново: ИГТУ, 2010, 134 с.
2. И.Шапошников. Компьютерные сети. Принципы, технологии, протоколы, СПб., 2006 с. 304.
3. Семенов Ю.А. Алгоритмы телекоммуникационных сетей. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных, БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий, ИНТУИТ.ру, 2007, 334 с.
4. Семенов Ю.А. Алгоритмы телекоммуникационных сетей. Часть 2. Протоколы и алгоритмы маршрутизации в INTERNET, БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий – ИНТУИТ.ру, 2007, 305 с.
5. Максимов Н.В., Попов И.И. Компьютерные сети, М.: Форум, 2010, 464 с.
6. Масленников Р. Хаос и порядок в Интернете, М.: СамИздат, 2009, 134 с.
7. Леинванд А. Конфигурирование маршрутизаторов, М.: «Вильямс», 2001, 147 с.
8. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы, СПб: «Питер», 2001, 405 с.

9. Фейт С. TCP/IP: архитектура, протоколы, реализация, М.: «Вильямс», 2003, 424 с.
10. Tatipamula M., Grossetete P., Esaki H. Ipv6 Integration and Coexistence Strategies for Next-Generation Networks// IEEE Commmun. Mag., 2004, №1, с.88–96.
11. Мамаев М., Петренко С. Технологии защиты информации в Интернете, СПб: Питер, 2002, 309 с.
12. Michael Palmer. Hands-On Networking Fundamentals, 2nd edition, Cengage Learning, 2012, 90 p.
13. Vinod Joseph, Srinivas Mulugu, Network Convergence: Ethernet Applications and Next Generation Packet Transport Architectures, London: Morgan Kaufmann, 2013, 620 p.

УДК 004.057.4
Джафаров Зафар А.
Азербайджанский Технический Университет, Баку, Азербайджан
c.zafar@mail.ru
Анализ системы адресации в сетях телекоммуникации
Статья посвящена анализу системы адресации в телекоммуникационных сетях. В ходе исследований были изучены архитектура, модели применения, характеристики системы адресации, причины проявления и преимущества протокола IPv6. Проанализированы проблемы текущей версии систем адресации IPv4, для их решения отмечена необходимость применения IPv6.
Ключевые слова: *интернет-протокол (IP), системы адресации, сетевые модели, дейтаграмма.*

Zafar A. Jafarov
Azerbaijan Technical University, Baku, Azerbaijan
c.zafar@mail.ru
Analysis of the system in addressing telecommunications networks
This article analyzes the addressing system in telecommunication networks. Our researches have studied architecture, model application, the system features addressing the cause of manifestation and its advantages protocol IPv6. The problems of the current version of addressing systems IPv4 are analysed, the need for IPv6 for their decision has been noted.
Keywords: *Internet protocol (IP), addressing system, network models, datagram.*