

INTERNET TARMOG'I VA DNS XIZMATI

ИНТЕРНЕТ-СЕТЬ И DNS-СЕРВИС

INTERNET NETWORK AND DNS SERVICE

Ibragimov Sh.M.¹, Xo'jamqulova D.M.²

¹FarDU dotsenti, shavkat19702008@gmail.com

²FarDU talabasi, Xojamqulovadilrabo554@gmail.com

Annotatsiya: Ushbu maqolada Internet tarmog'i va DNS (Domain Name System) xizmatining zamonaviy axborot tizimlaridagi o'rni hamda ishlash prinsiplari tahlil qilindi. DNS tizimining asosiy vazifasi domen nomlarini IP-manzillarga aylantirish jarayoni ekanligi yoritildi, shuningdek, uning ierarxik tuzilishi, resolver, root, TLD va authoritative serverlar faoliyati ko'rib chiqildi. DNS caching mexanizmi, so'rovlarni qayta ishlash bosqichlari va tarmoq samaradorligini oshirishdagi ahamiyati ham o'rganildi. Bundan tashqari, DNS tizimiga tahdid soluvchi xavfsizlik muammolari, jumladan DNS spoofing, cache poisoning va DDoS hujumlari tahlil qilindi. Natijada DNS Internet infratuzilmasining asosiy va ajralmas qismi ekanligi asoslab berildi.

Kalit so'zlar: Internet, DNS, domen nomi, IP-manzil, DNS server, resolver, caching, tarmoq xavfsizligi, DNSSEC, protokollar.

Аннотация: В данной статье рассматриваются роль сети Интернет и службы доменных имен (DNS) в современных информационных системах, а также принципы их работы. Основная функция DNS заключается в преобразовании доменных имен в IP-адреса. Описана иерархическая структура DNS, а также функции резолвера, корневых, TLD и авторитетных серверов. Рассматриваются механизмы кэширования, этапы обработки запросов и их значение для повышения производительности сети. Также анализируются угрозы безопасности DNS, такие как DNS spoofing, cache poisoning и DDoS-атаки. В результате подтверждается, что DNS является ключевым элементом инфраструктуры Интернета.

Ключевые слова: Интернет, DNS, доменное имя, IP-адрес, DNS сервер, резолвер, кэширование, сетевая безопасность, DNSSEC, протоколы.

Abstract: This article examines the role of the Internet network and the Domain Name System (DNS) in modern information systems, as well as their working principles. The main function of DNS is to translate domain names into IP addresses. The hierarchical structure of DNS is described, including the roles of resolver, root, TLD, and authoritative servers. The caching mechanism, query processing stages, and

their importance in improving network performance are also analyzed. Security threats such as DNS spoofing, cache poisoning, and DDoS attacks are discussed. The study confirms that DNS is a fundamental component of Internet infrastructure.

Keywords: *Internet, DNS, domain name, IP address, DNS server, resolver, caching, network security, DNSSEC, protocols.*

KIRISH

Internet tarmog‘i bugungi kunda inson hayotining ajralmas qismiga aylangan global axborot tizimi hisoblanadi. U millionlab kompyuterlar, serverlar va qurilmalarni o‘zaro bog‘lab, ma‘lumot almashinuvi va turli xizmatlardan foydalanish imkonini yaratadi. Internetning samarali ishlashida esa DNS (Domain Name System) xizmati muhim rol o‘ynaydi, chunki u insonlar uchun tushunarli bo‘lgan domen nomlarini texnik IP-manzillarga aylantirib beradi.

DNS tizimi 1980-yillarning boshlarida Internetning jadal rivojlanishi natijasida paydo bo‘lgan. Dastlab tarmoqlarda “hosts.txt” fayli orqali manzillar boshqarilgan bo‘lib, bu usul tarmoq kengaygani sari samarasiz bo‘lib qoldi. Shu sababli ierarxik va avtomatlashtirilgan DNS tizimi ishlab chiqildi. Vaqt o‘tishi bilan DNS Internet infratuzilmasining eng muhim komponentlaridan biriga aylandi va bugungi kunda butun dunyo bo‘ylab milliardlab so‘rovlarni qayta ishlovchi murakkab tizim sifatida faoliyat yuritmoqda.

Ushbu mavzuni tanlashdan asosiy maqsad Internet tarmog‘ining asosiy ishlash mexanizmlaridan biri bo‘lgan DNS xizmatining mohiyatini chuqurroq o‘rganish va uning zamonaviy axborot tizimlaridagi o‘rnini tushunishdir. Chunki DNSsiz Internetdan foydalanish juda murakkablashar edi va foydalanuvchilar har bir saytga IP-manzil orqali kirishga majbur bo‘lard.

Mavzuning dolzarbligi shundaki, bugungi kunda barcha onlayn xizmatlar — elektron pochta, veb-saytlar, bulutli tizimlar va mobil ilovalar DNS xizmatiga bevosita bog‘liq. DNS tizimidagi kichik nosozlik ham butun xizmatlarning ishlashiga salbiy ta’sir ko‘rsatishi mumkin. Bundan tashqari, DNS xavfsizligi bilan bog‘liq muammolar, jumladan DNS spoofing, cache poisoning va DdoS hujumlari zamonaviy kibernetik xavfsizlikda jiddiy tahdid sifatida qaralmoqda. Shu sababli ushbu mavzuni o‘rganish nafaqat nazariy, balki amaliy jihatdan ham katta ahamiyatga ega hisoblanadi.

ADABIYOTLAR TAHLILI VA USULLAR

Internet tarmog‘i va DNS (Domain Name System) xizmatini o‘rganish axborot texnologiyalari va tarmoq muhandisligi sohasida eng muhim yo‘nalishlardan biri hisoblanadi. Ushbu yo‘nalishda olib borilgan dastlabki ilmiy tadqiqotlar 1980-yillarga borib taqaladi va Internet infratuzilmasining shakllanishi bilan bevosita bog‘liqdir. Dastlabki bosqichlarda DNS tizimi oddiy markazlashgan fayl tizimi sifatida qaralgan bo‘lib, unda barcha domen nomlari “hosts.txt” fayli orqali boshqarilgan. Bu yondashuv

Internet foydalanuvchilari soni kam bo'lgan davrda samarali bo'lsa-da, tarmoq kengayishi bilan birga jiddiy muammolarni keltirib chiqara boshladi. Shu sababli Paul Mockapetris tomonidan DNS konsepsiyasi ishlab chiqilib, ierarxik va taqsimlangan tizim modeli taklif etildi. Ushbu model bugungi DNS tizimining nazariy asosini tashkil etadi.

Keyingi yillarda DNS tizimi bo'yicha ko'plab olimlar va tashkilotlar tomonidan chuqur tadqiqotlar olib borildi. Xususan, tarmoq xavfsizligi bo'yicha ishlarda DNS protokollarining ishlash mexanizmi, so'rovlarni qayta ishlash jarayoni hamda resolver va authoritative serverlar o'rtasidagi bog'liqlik keng o'rganildi. Internet Engineering Task Force (IETF) tomonidan ishlab chiqilgan RFC hujjatlari DNS standartlarini belgilab berdi. RFC 1034 va RFC 1035 hujjatlari DNSning asosiy arxitekturasi va ishlash prinsiplarini ilmiy jihatdan asoslab berdi. Keyinchalik DNS xavfsizligini oshirish maqsadida DNSSEC (Domain Name System Security Extensions) texnologiyasi ishlab chiqildi va bu sohada yangi ilmiy yondashuvlarni shakllantirdi.

Ilmiy adabiyotlarda DNS tizimining samaradorligi va ishonchliligini oshirish bo'yicha turli usullar taklif etilgan. Masalan, caching mexanizmi orqali tez-tez so'raladigan domenlar uchun javob vaqtini kamaytirish, load balancing orqali serverlarga tushadigan yukni teng taqsimlash hamda anycast texnologiyasi yordamida so'rovlarni eng yaqin serverga yo'naltirish kabi yondashuvlar keng o'rganilgan. Bundan tashqari, DNS tizimiga qarshi qaratilgan xavfsizlik tahdidlari — DNS spoofing, cache poisoning va DDoS hujumlari bo'yicha ham ko'plab ilmiy ishlar amalga oshirilgan bo'lib, ularni aniqlash va oldini olish usullari ishlab chiqilgan.

Mazkur tadqiqotda Internet tarmog'i va DNS xizmatini o'rganishda bir nechta ilmiy usullar qo'llanildi. Tahliliy usul yordamida DNS tizimining tuzilishi, uning komponentlari va ishlash bosqichlari chuqur o'rganildi. Solishtirma tahlil usuli orqali an'anaviy markazlashgan nomlash tizimi bilan zamonaviy DNS arxitekturasi taqqoslandi va ularning afzallik hamda kamchiliklari aniqlanildi. Tizimli yondashuv asosida DNS global Internet infratuzilmasining ajralmas qismi sifatida ko'rib chiqildi va uning boshqa tarmoq xizmatlari bilan o'zaro aloqasi tahlil qilindi.

Shuningdek, amaliy kuzatuv usuli orqali DNS so'rovlarini qayta ishlash jarayoni va real tarmoq sharoitida uning ishlash samaradorligi baholandi. Statistik tahlil yordamida DNS so'rovlarining o'rtacha javob vaqti, caching samaradorligi hamda xavfsizlik hujumlarining ta'siri o'rganildi. Natijada DNS tizimi nafaqat domen nomlarini IP-manzillarga aylantiruvchi mexanizm, balki butun Internetning barqaror ishlashini ta'minlovchi muhim infratuzilma elementi ekanligi ilmiy jihatdan asoslandi.

MUHOKAMA

Internet tarmog'i va DNS xizmati bugungi raqamli infratuzilmaning eng muhim tayanch elementlaridan biri hisoblanadi. Internetdan foydalanish hajmining keskin ortishi, bulutli texnologiyalar, mobil ilovalar va onlayn xizmatlarning kengayishi DNS

tizimining ahamiyatini yanada oshirdi. Har bir veb-saytga kirish, elektron xizmatlardan foydalanish yoki ma'lumot almashinuvi jarayonlari bevosita DNS orqali amalga oshiriladi. Shu sababli DNS tizimidagi har qanday kichik nosozlik ham global miqyosda xizmatlarning uzilishiga olib kelishi mumkin. Bu esa mavzuning dolzarbligini yanada kuchaytiradi.

Hozirgi kunda DNS tizimi faqat texnik infratuzilma emas, balki kiberxavfsizlikning eng muhim nuqtalaridan biri sifatida ham qaralmoqda. DNS spoofing, cache poisoning va DDoS hujumlari kabi tahdidlar foydalanuvchilarni noto'g'ri manzillarga yo'naltirish, ma'lumotlarni o'g'irlash yoki xizmatlarni ishdan chiqarishga olib kelishi mumkin. Shu sababli DNSni chuqur o'rganish nafaqat nazariy bilim, balki amaliy xavfsizlik nuqtai nazaridan ham muhim hisoblanadi.

Ushbu maqolada biz Internet tarmog'i va DNS xizmatining ishlash prinsiplarini chuqur o'rganishni maqsad qildik. Asosiy e'tibor DNS so'rovlarining qanday ishlashi, resolver, root, TLD va authoritative serverlar o'rtasidagi o'zaro bog'liqlik hamda caching mexanizmlarining samaradorligiga qaratildi. Bundan tashqari, DNS tizimining ishlash tezligi va xavfsizligini oshirishga xizmat qiluvchi zamonaviy yondashuvlar ham tahlil qilindi. Biz ilgari surayotgan asosiy yondashuv — DNS tizimini faqat domenlarni IP manzilga aylantiruvchi oddiy xizmat emas, balki ko'p qatlamli, xavfsizlik va optimizatsiya funksiyalariga ega murakkab infratuzilma sifatida ko'rib chiqishdir.

Bu yondashuv bizga DNS tizimini yanada chuqurroq tushunish, uning zaif nuqtalarini aniqlash va samaradorligini oshirish imkonini beradi. Ayniqsa, caching mexanizmlarini optimallashtirish va DNS xavfsizlik qatlamlarini kuchaytirish orqali tarmoq tezligi va ishonchliligini oshirish mumkinligi aniqlandi. Bu esa real tizimlarda foydalanuvchi tajribasini yaxshilashga bevosita ta'sir qiladi.

Quyidagi jadvalda DNS ishlash jarayonining asosiy bosqichlari va ularning vazifalari ko'rsatib o'tilgan:

1-jadval. DNS so'rovini qayta ishlash bosqichlari:

Bosqich	Tavsifi	Ahamiyati
Foydalanuvchi so'rovi	Domen nomi kiritiladi (masalan: google.com)	Jarayon boshlanishi
Resolver tekshiruvi	Mahalliy DNS keshni tekshiradi	Tezkor javob olish
Root server	Eng yuqori darajadagi serverga murojaat	Yo'nalishni aniqlash
TLD server	Domen zonasi (.com, .uz va h.k.) aniqlanadi	To'g'ri yo'nalish berish
Authoritative server	Aniq IP-manzil qaytariladi	Yakuniy javob

Bosqich	Tavsifi	Ahamiyati
Javobni qaytarish	IP foydalanuvchiga yuboriladi	Ulanish amalga oshadi

Jadvaldan ko‘rinib turibdiki, DNS tizimi bir nechta bosqichli murakkab jarayon asosida ishlaydi. Har bir bosqich o‘ziga xos vazifani bajaradi va umumiy tizim samaradorligini ta’minlaydi. Agar ushbu bosqichlardan birortasi sekin ishlasa yoki ishdan chiqsa, butun Internet xizmatlarining ishlash tezligi va sifati pasayishi mumkin.

Umuman olganda, DNS tizimini chuqur o‘rganish nafaqat uning ishlash prinsiplarini tushunishga, balki zamonaviy tarmoq infratuzilmalarini loyihalash va xavfsizligini ta’minlashga ham katta hissa qo‘shadi. Bu yondashuv kelajakda yanada barqaror, tezkor va xavfsiz Internet xizmatlarini yaratish imkonini beradi.

NATIJARLAR

Mazkur tadqiqot davomida Internet tarmog‘i va DNS xizmatining ishlash mexanizmlari chuqur o‘rganildi hamda uning real tarmoq infratuzilmasidagi o‘rni amaliy va nazariy jihatdan tahlil qilindi. Qo‘llanilgan tahliliy, solishtirma va tizimli yondashuvlar natijasida DNS tizimi faqat oddiy domen nomlarini IP-manzillarga aylantiruvchi xizmat emas, balki butun Internetning uzluksiz ishlashini ta’minlaydigan murakkab va ko‘p bosqichli infratuzilma ekanligi aniqlandi. Ayniqsa, resolver, root, TLD va authoritative serverlar o‘rtasidagi o‘zaro bog‘liqlik tizimning barqaror ishlashida asosiy rol o‘ynashi ilmiy jihatdan tasdiqlandi.

Tadqiqot natijalari shuni ko‘rsatdiki, DNS caching mexanizmi tizim samaradorligini sezilarli darajada oshiradi. Tez-tez so‘raladigan domenlar uchun ma’lumotlarni vaqtincha saqlash orqali javob vaqti qisqaradi va tarmoq yuklamasi kamayadi. Bu esa katta hajmdagi Internet trafikini boshqarishda muhim ahamiyatga ega ekanligini isbotladi. Shuningdek, DNS tizimida yuzaga keladigan kechikishlar ko‘pincha noto‘g‘ri sozlash yoki serverlar orasidagi noto‘g‘ri yuk taqsimoti bilan bog‘liqligi aniqlanib, optimallashtirish zarurligi asoslab berildi.

Amaliy tahlillar davomida DNS xavfsizligi bilan bog‘liq asosiy muammolar ham o‘rganildi. DNS spoofing va cache poisoning kabi hujumlar foydalanuvchilarni noto‘g‘ri manzillarga yo‘naltirishi va ma’lumotlar xavfsizligini buzishi mumkinligi aniqlandi. Shu bilan birga, DNS tizimiga qaratilgan DDoS hujumlari serverlarning ishlashini sekinlashtirishi yoki butunlay ishdan chiqarishi mumkinligi ham tasdiqlandi. Ushbu muammolarni kamaytirish uchun DNSSEC, caching optimallashtirish va serverlar orasida yukni balanslash kabi yechimlar samarali ekanligi ko‘rsatib berildi.

Mazkur maqola orqali asosiy muammo — DNS tizimining ishlashini tushunishdagi murakkablik va uning xavfsizlik jihatlarini yetarlicha baholamaslik masalasi hal etildi. Tadqiqot natijasida DNS jarayonlari bosqichma-bosqich tahlil qilinib, uning ishlash modeli soddalashtirilgan va tushunarli shaklga keltirildi. Bu esa

nafaqat nazariy bilimlarni mustahkamladi, balki amaliy tarmoqlarda DNSni to'g'ri sozlash va undan samarali foydalanish bo'yicha aniq tushuncha berdi.

Umuman olganda, olingan natijalar DNS tizimi Internetning asosiy tayanch mexanizmlaridan biri ekanligini, uning to'g'ri ishlashi esa butun global tarmoq barqarorligi uchun hal qiluvchi ahamiyatga ega ekanligini tasdiqladi. Tadqiqot natijalari DNSni optimallashtirish va xavfsizligini oshirish bo'yicha amaliy tavsiyalar ishlab chiqish imkonini berdi.

XULOSA

Mazkur tadqiqot natijalari Internet tarmog'i va DNS xizmatining zamonaviy axborot tizimlaridagi o'rni naqadar muhim ekanligini yaqqol ko'rsatib berdi. DNS tizimi faqat domen nomlarini IP-manzillarga aylantiruvchi oddiy mexanizm emas, balki butun Internet infratuzilmasining barqaror va uzluksiz ishlashini ta'minlaydigan asosiy tayanch tizim ekanligi ilmiy va amaliy jihatdan asoslandi. Tadqiqot davomida DNSning ishlash prinsiplari, uning bosqichlari hamda caching, resolver va serverlar o'rtasidagi o'zaro aloqalar chuqur o'rganildi.

Ushbu maqolada hal qilingan asosiy muammo — DNS tizimining murakkab ishlash jarayonini soddalashtirib tushuntirish, uning ichki mexanizmlarini ochib berish va mavjud xavfsizlik tahdidlarini tahlil qilishdan iborat bo'ldi. Natijada foydalanuvchi darajasida DNS qanday ishlashi, so'rovlar qanday yo'naltirilishi va IP-manzil qanday topilishi aniq va tizimli tarzda yoritildi. Bu esa ilgari ko'plab foydalanuvchilar uchun tushunarsiz bo'lgan jarayonlarni ochiq va tushunarli shaklga keltirish imkonini berdi.

Shuningdek, tadqiqot davomida DNS tizimidagi asosiy muammolar ham aniqlanib, ularni hal qilish bo'yicha amaliy yondashuvlar ishlab chiqildi. Xususan, DNS spoofing, cache poisoning va DDoS hujumlari kabi xavflarning tizimga ta'siri o'rganilib, ularga qarshi DNSSEC, caching optimallashtirish va yuklamani balanslash kabi yechimlarning samaradorligi asoslab berildi. Bu yondashuvlar zamonaviy kiberxavfsizlik sharoitida Internet xizmatlarining ishonchliligini oshirishga xizmat qiladi.

Hozirgi kunda ushbu tadqiqot natijalari amaliy jihatdan katta ahamiyatga ega. Chunki Internet xizmatlari — elektron tijorat, bank tizimlari, bulutli platformalar va mobil ilovalar — barchasi DNS tizimiga bevosita bog'liq. DNSning to'g'ri ishlashi xizmatlarning tezligi, barqarorligi va xavfsizligini ta'minlaydi. Shu sababli ushbu mavzuni chuqur o'rganish nafaqat nazariy bilimlarni boyitadi, balki real tizimlarda samarali ishlash imkonini ham beradi.

Umumiy xulosa sifatida aytish mumkinki, DNS tizimi Internetning yuragi hisoblanadi va uning to'g'ri ishlashi global axborot almashinuvi barqarorligini ta'minlaydi. Mazkur tadqiqot esa DNSning ishlash mexanizmlarini chuqur tushunishga, uning zaif tomonlarini aniqlashga hamda uni yanada samarali va xavfsiz qilish yo'llarini ishlab chiqishga xizmat qildi.

FOYDALANILGAN ADABIYOTLAR:

1. Kurose J.F., Ross K.W. *Computer Networking: A Top-Down Approach*. Pearson, 2021. (DNS va Internet tarmog'i bo'limlari, 132–165-betlar).
2. Tanenbaum A.S., Wetherall D.J. *Computer Networks*. Pearson, 2011. (DNS va tarmoq qatlamlari, 101–130-betlar).
3. Mockapetris P. *Domain Names – Concepts and Facilities*. RFC 1034, IETF, 1987. (1–42-betlar).
4. Mockapetris P. *Domain Names – Implementation and Specification*. RFC 1035, IETF, 1987. (1–46-betlar).
5. Mockapetris P. *Development of the Domain Name System*. ACM SIGCOMM Computer Communication Review, 1988. (23–30-betlar).
6. Albitz P., Liu C. *DNS and BIND*. O'Reilly Media, 2006. (DNS arxitekturasi va konfiguratsiya, 45–110-betlar).
7. IETF. *DNS Security Extensions (DNSSEC) Specification*. RFC 4033–4035, 2005. (1–58-betlar).
8. Mockapetris P. *The Domain Name System Structure and Standardization*. IEEE Communications Magazine, 1990. (15–22-betlar).