Тема 8. Багаторівнева структура стеку TCP/IP

Стек протоколів TCP/IP, TCP/IP-модель – набір протоколів мережі Інтернет. Назва походить від назви основних протоколів мережі Інтернет – IP (Internet Protocol – Інтернет протокол) і TCP (Transmission Control Protocol – протокол керування передачею). Фактично це систематизований стек протоколів, що поділяється на чотири рівні, які корелюються з еталонною моделлю OSI.

TCP/IP зародився в результаті досліджень, профінансованих Управлінням перспективних науково-дослідних розробок (Advanced Research Project Agency, ARPA) уряду США в 1970-х роках. Цей протокол був розроблений для того, щоб обчислювальні мережі дослідницьких центрів в усьому світі могли бути об'єднані у формі віртуальної «мережі мереж» (internetwork). Первісна мережа Інтернет була створена в результаті перетворення наявного конгломерату обчислювальних мереж, що носили назву ARPAnet, за допомогою TCP/IP.

Великий внесок у розвиток стеку протоколів TCP/IP вніс університет Берклі, реалізувавши протоколи стеку у своїй версії ОС UNIX. Популярність цієї ОС призвела до поширення протоколів TCP, IP та інших протоколів стеку. Сьогодні цей стек використовують для зв'язку комп'ютерів світової інформаційної мережі Інтернет, а також багатьох корпоративних мереж.

Стек протоколів TCP/IP (модель взаємодії відкритих систем DoD (Department of Defence) міністерства оборони США) ділиться на 4 рівні: прикладний (application), транспортний (transport), міжмережевий (internet) та рівень доступу до середовища передачі (network access layer, link layer). Терміни, що використовуються для позначення блоку переданих даних, різні при використанні різних протоколів транспортного рівня: TCP і UDP.

На прикладному рівні це потік (TCP) і повідомлення (UDP); на транспортному – сегмент і пакет.

8.1. Прикладний рівень

Протоколи прикладного рівня TCP/IP визначають процедури організації взаємодії прикладних процесів (програм) різних мережевих комп'ютерів і форми подання інформації за такої взаємодії. За ознаками взаємодії прикладних процесів виділяють два типи прикладного програмного забезпечення: програма-клієнт та програма-сервер. Протоколи прикладного рівня зорієнтовано на конкретні прикладні завдання. Серед традиційних послуг, котрі забезпечують протоколи прикладного рівня з сімейства TCP/IP, сьогодні найпопулярнішими є електронна пошта – протоколи SMTP та POP3, передача файлів – FTP та TFTP, емуляція віддаленого терміналу – Telnet тощо.

З середини 1990-х років в Інтернеті активно запроваджуються послуги, які базуються на технології WWW, яка ґрунтується на протоколі передачі гіпертексту HTTP.

HTTP (HyperText Transfer Protocol, протокол передачі гіпертекстових документів) – протокол передачі даних, що використовується в комп'ютерних мережах для відображення вебсторінок.

Основним призначенням протоколу HTTP є передача вебсторінок (текстових файлів з розміткою HTML, зображень та застосунків), проте за його допомогою успішно передаються й інші файли (в цьому плані HTTP складає конкуренцію складнішому FTP).

HTTPS (HTTP Secure) – схема URI, що синтаксично ідентична http: схемі, яка зазвичай використовується для доступу до ресурсів Інтернет. Використання https: URL вказує, що протокол HTTP має використовуватися, але з іншим портом за замовчуванням (443) і додатковим шаром шифрування/автентифікації між HTTP і TCP. Ця схема була розроблена у компанії Netscape Communications Corporation для забезпечення автентифікації та шифрування комунікацій і широко використовується в Інтернеті у програмному забезпеченні, в якому важлива безпека комунікацій, наприклад, у платіжних системах та корпоративних логінах.

POP3 (Post Office Protocol, поштовий офісний протокол) – це протокол, що використовується клієнтом для доступу до повідомлень електронної пошти на сервері. Остання версія протоколу – третя. POP3 дозволяє клієнтові мати вибірковий доступ до повідомлень на сервері. За своєю функціональністю POP є набагато простішим за IMAP протокол, не надаючи клієнту інтерфейсу з маніпулювання папками на сервері, вибірковим отриманням частин повідомлення чи можливості завантаження заголовків листів.

POP3 протокол, за замовчуванням працює на 110 порті TCP. Шифрований Secure POP3 (SSL-POP) працює на 995 порті TCP.

IMAP (Internet Message Access Protocol, протокол доступу до інтернет-повідомлень) – мережевий протокол прикладного рівня для доступу до електронної пошти.

IMAP надає користувачеві великі можливості для роботи з поштовими скриньками, розташованими на центральному сервері. Поштовий клієнт, що використовує цей протокол, отримує доступ до сховища кореспонденції на сервері так, начебто ця кореспонденція розташована на комп'ютері одержувача. Електронними листами можна маніпулювати з комп'ютера користувача (клієнта) без постійного пересилання з сервера і назад файлів з повним змістом листів.

SMTP (Simple Mail Transfer Protocol, простий протокол пересилання пошти) – це протокол, який використовується для пересилання електронної пошти до поштового сервера або з клієнта-комп'ютера, або між поштовими серверами. В IANA для SMTP зареєстрований порт 25. SMTP з'єднання де застосовується SSL шифрування використовують порт 465.

SMTP – порівняно простий, текстовий протокол, в якому з'єднання відбувається завжди за ініціативи відправника. SMTP – синхронний протокол і складається із серії команд, що посилаються клієнтом та відповідей сервера. Відправником зазвичай є поштовий клієнт кінцевого користувача або поштовий сервер.

FTP (File Transfer Protocol, протокол передачі файлів) – стандартний мережевий протокол прикладного рівня, призначений для пересилання файлів між клієнтом та сервером в комп'ютерній мережі.

Клієнт та сервер створюють окремі канали для передачі даних та обміну командами. Можлива автентифікація клієнтів із використанням відкритого тексту, зазвичай це ім'я користувача (логін) та пароль. Також сервер може бути налаштований для роботи без автентифікації користувачів (так звані «анонімні сеанси»).

Для захисту даних (а також процесу автентифікації) використовують побудований на основі SSL/TLS варіант FTPS, або розширення протоколу SSH – SSH File Transfer Protocol (SFTP).

DHCP (Dynamic Host Configuration Protocol, протокол динамічної конфігурації вузла) – це стандартний протокол прикладного рівня, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Для цього комп'ютер звертається відповідно – до DHCP-сервера. Мережевий адміністратор може задати діапазон адрес, які будуть розподілені між комп'ютерами. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих мереж TCP/IP.

DNS (Domain Name System, система доменних імен) – ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу.

Кожен комп'ютер в Інтернеті має свою власну унікальну адресу – число, яке складається з чотирьох (у протоколі IPv4) або шістнадцяти (у протоколі IPv6) байт. Оскільки запам'ятати десятки чи навіть сотні номерів – важка процедура, то всі (чи майже всі) машини мають імена, запам'ятати які (особливо якщо знати правила утворення імен) значно легше.

MQTT (Message Queue Telemetry Transport) – спрощений мережевий протокол, що використовується для обміну повідомленнями між пристроями за принципом видавець-підписник.

Протокол MQTT часто використовується для побудови систем на базі Інтернету речей (IoT).

Telnet (TErminaL NETwork) – мережевий протокол для реалізації текстового інтерфейсу по мережі (у сучасній формі – за допомогою транспорту TCP). Назву «telnet» мають також деякі утиліти, що реалізують клієнтську частину протоколу.

Призначення протоколу Telnet у наданні достатньо спільного, двонаправленого, восьмибітового байт-орієнтованого засобу зв'язку. Його основне завдання полягає в тому, щоб дозволити термінальним пристроям і термінальним процесам взаємодіяти один з одним. Передбачається, що цей протокол може бути використаний для зв'язку виду термінал-термінал або для зв'язку процес-процес (розподілені обчислення).

SSH (Secure SHell, безпечна оболонка) – мережевий протокол прикладного рівня, що дозволяє проводити віддалене керування комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколом Telnet, проте шифрує весь трафік, в тому числі і паролі, що передаються.

SSL (Secure Sockets Layer, рівень захищених сокетів) – криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером.

Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, що використовують TCP/IP, причому для шифрування використовується асиметричний алгоритм з відкритим ключем. При шифруванні з відкритим ключем використовується два ключі, причому будь-який з них може використовуватися для шифрування повідомлення. Тим самим, якщо використовується один ключ для шифрування, то відповідно для розшифрування потрібно використовувати інший ключ. У такій ситуації можна отримувати захищені повідомлення, публікуючи відкритий ключ, і зберігаючи в таємниці секретний ключ.

TLS (Transport Layer Security, захист на транспортному рівні), як і його попередник SSL – криптографічний протокол, що надає можливості

безпечної передачі даних в Інтернеті для навігації, отримання пошти, спілкування, обміну файлами, тощо. Використовує асиметричне шифрування.

TLS надає можливості автентифікації і безпечної передачі даних через Інтернет із використанням криптографічних засобів. Часто відбувається лише автентифікація сервера, а клієнт залишається неавтентифікованим. Для взаємної автентифікації кожна з сторін мусить підтримувати інфраструктуру відкритих ключів, яка дозволяє захистити клієнт-серверні додатки від перехоплення, редагування повідомлень або ж створення підроблених.

BGP (Border Gateway Protocol, протокол граничного шлюзу) – з 1994 року єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет.

BGP є протоколом міждоменної маршрутизації та належить до класу дистанційно-векторних протоколів. Як протокол міждоменної маршрутизації використовується усіма інтернет-провайдерами, а також великими компаніями та організаціями, які мають власні публічні номери автономних систем (ASN) та користуються послугами більш ніж одного інтернет-провайдера або мають прямі IP-з'єднання з багатьма іншими великими компаніям, що також мають власні публічні номери автономних систем, без використання послуг інтернет-провайдерів.

GTP (GPRS Tunneling Protocol) – це група комунікаційних протоколів на базі IP, які використовують для перенесення GPRS в мережах GSM, UMTS та LTE. GTP описує і здійснює передачу даних між вузлами GSN у пакетній мережі.

LDAP (Lightweight Directory Access Protocol, полегшений протокол доступу до директорій/каталогів) – мережевий протокол прикладного рівня для надсилання запитів та модифікації даних служби каталогів через TCP/IP. LDAP є відкритим, комерційно-нейтральним, промисловим стандартним протоколом.

Серед поширених варіантів використання LDAP – надання єдиного сховища для зберігання імен користувачів та паролів. Це дозволяє різним службам та застосункам надсилати запити до LDAP сервера для валідації користувачів.

MGCP (Media Gateway Control Protocol) – протокол для керування шлюзами між IP-мережею і комутованою телефонною мережею загального користування. MGCP є протоколом сигналізації і керування викликами, який використовується в рамках Voice over IP (VoIP) системи, яка зазвичай взаємодіє з комутованою телефонною мережею загального користування.

NTP (Network Time Protocol, мережевий протокол часу) – мережевий протокол синхронізації внутрішнього годинника комп'ютера з використанням мереж зі змінною затримкою, заснований на комутації пакетів.

RIP (Routing Information Protocol) – один із найрозповсюдженіших протоколів маршрутизації в невеликих комп'ютерних мережах, який дозволяє маршрутизаторам динамічно оновлювати маршрутну інформацію, отримуючи її від сусідніх маршрутизаторів.

VNC (Virtual Network Computing) – протокол надання доступу до віддаленого комп'ютера у мережі TCP/IP з будь-якого іншого комп'ютера або мобільного пристрою з метою відслідковування (моніторингу) та дистанційного керування. Для здійснення такої взаємодії потрібно встановити програмне забезпечення VNC, яке показує у вікні вашого комп'ютера весь екран віддаленого комп'ютера та передає йому коди натиснутих клавіш та команди мишки, таким чином надаючи користувачу повний «ефект присутності».

8.2. Транспортний рівень

Протоколи транспортного рівня TCP/IP-моделі надають транспортні послуги прикладним процесам. Основними протоколами транспортного рівня TCP/IP є протокол керування передавання TCP і протокол користувальницьких дейтаграм UDP. Транспортні послуги цих протоколів

суттєво відрізняються. Протокол UDP доставляє дейтаграми без встановлення з'єднання. При цьому він не гарантує їх доставки. Протокол TCP забезпечує надійну доставку байтових потоків (сегментів) із попереднім встановленням транспортного дуплексного з'єднання (віртуального каналу) між модулями TCP мережевих комп'ютерів. Для розв'язання транспортних завдань протоколи TCP та UDP під час передавання даних формують і додають до даних свої заголовки розміром 20 байт та 8 байт відповідно.

Кожен прикладний процес взаємодіє з модулем транспортного рівня TCP або UDP через окремий порт, що дозволяє при взаємодії систем однозначно ідентифікувати прикладні процеси. Ці порти нумеруються починаючи з нуля. При передачі запиту прикладної програми клієнта до прикладної програми сервера транспортний модуль, формуючи дейтаграму чи сегмент, вказує номери портів програмних модулів прикладних протоколів сервера й клієнта. З цією метою в заголовку пакета протоколу транспортного рівня виділено два поля – порт одержувача і порт відправника, розміром по 2 байти. Номери портів TCP та UDP до прикладних протоколів сервера стандартизовані IETF. Для цього надано номери в діапазоні від 1 до 1023. Наприклад, програмний модуль TCP сервера зазвичай взаємодіє з модулем протоколу HTTP через порт з номером 80.

DCCP (Datagram Congestion Control Protocol) – мережевий протокол транспортного рівня, розроблений IETF. Він надає механізми для відстеження перевантажень у мережі, уникаючи можливості використання механізмів прикладного рівня. Цей протокол не гарантує доставку інформації в потрібному порядку.

DCCP дуже ефективний для застосунків, в яких дані, що прийшли не вчасно, стають непотрібними. Наприклад: потокове медіа-мовлення, онлайн ігри і інтернет-телефонія. Головна особливість цих застосунків полягає в тому, що старі повідомлення дуже швидко стають непотрібними, тому краще отримати нове повідомлення, ніж намагатися переслати старе.

8.3. Мережевий рівень

Протоколи мережевого рівня TCP/IP забезпечують взаємодію мереж різної архітектури тощо. Основним протоколом мережного рівня технології TCP/IP є міжмережевий протокол IP та його допоміжні протоколи.

Головне завдання міжмережевого протоколу IP – це маршрутизація пакетів даних між різнотипними комп'ютерними мережами. Для розв'язання цього завдання протокол IP підтримує IP-адресацію мереж та вузлів, використовує таблицю маршрутизації пакетів, виконує, за необхідності, фрагментацію та дефрагментацію цих пакетів.

ICMP (Internet Control Message Protocol, міжмережевий протокол керуючих повідомлень) – мережевий протокол, що використовується для передачі повідомлень про помилки та інші виняткові ситуації, що виникли при передачі даних. Також на ICMP покладаються деякі сервісні функції, зокрема на основі цього протоколу заснована дія таких загальновідомих утиліт як *ping* та *traceroute*.

Протокол ICMP не є протоколом орієнтованим на з'єднання (як наприклад TCP), тобто при втраті пакету ICMP не буде робити ніяких спроб по його відновленню. ICMP повідомлення (тип 12) генеруються при знаходженні помилок у заголовку IP пакета (за винятком самих ICMP пакетів, щоб не призвести до нескінченного потоку ICMP повідомлень про ICMP повідомлення).

IGMP (Internet Group Management Protocol, протокол керування групами Інтернету) – протокол керування груповою передачею даних в мережах, базованих на протоколі IP. IGMP використовується маршрутизаторами і IP-точками для об'єднання мережевих пристроїв в групи.

Цей протокол є частиною специфікації групової передачі пакетів в IP-мережах. Він в багато чому аналогічний ICMP для односторонньої передачі. IGMP може використовуватись для підтримки потокового відео і онлайн-ігор, для таких типів програм він дозволяє використовувати ресурси мережі ефективніше.

IGMP використовується лише в мережах IPv4, оскільки в IPv6 групова передача пакетів реалізована інакше.

IPsec (IP Security) – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження справжності та/або шифрування IP-пакетів. IPsec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет.

8.4. Рівень доступу до середовища передачі (Network Access Layer)

Основні функції даного рівня:

- перетворення IP-адрес у фізичні адреси мережі (MAC-адреси);
- інкапсуляція IP-дейтаграм в кадри для передачі по фізичному каналу і передачі кадрів.

ARP (Address Resolution Protocol, протокол визначення адрес) – комунікаційний протокол, призначений для перетворення IP-адрес (адрес мережевого рівня) в MAC-адреси (адреси канального рівня) в мережах TCP/IP.

Перетворення виконується лише для тих IP-пакетів, які відправляються, оскільки лише в момент відправлення створюються заголовки IP та Ethernet.

RARP (Reverse Address Resolution Protocol, зворотний протокол визначення адрес) – протокол, що виконує зворотне перетворення адрес, тобто перетворює фізичну адресу в IP-адресу.

Протокол застосовується під час завантаження вузла (наприклад комп’ютера), коли він посилає групове повідомлення-запит зі своєю фізичною адресою. Сервер приймає це повідомлення і переглядає свої таблиці (або перенаправляє запит будь-куди ще) у пошуках відповідної фізичній, IP-адресі. Після виявлення знайденої адреси відсилається назад на вузол, який її запитав.