Тема 6. 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 й 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 (англ. network access layer, link layer, рос. Канальный уровень). 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.

Як і в моделі OSI, дані більш верхніх рівнів інкапсулюються в блоки даних більше нижчих рівнів, наприклад, сегмент (TCP) або пакет (UDP) зі своїми даними і службовими заголовками інкапсулюється всередині поля «Дані» дейтаграми.

6.1. 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.

Сьогодні популярні послуги пакетної IP-телефонії на базі стандартів IETF, до яких відносяться спеціальні протоколи прикладного, транспортного та мережевого рівнів, наприклад, сигналізації SIP, передачі в режимі реального часу RTP та RTCP, резервування ресурсів RSVP, рекомендацій ITU H.323 тощо.

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.

SMTP було розроблено як протокол транспортування і доставки, тому системи, що використовують SMTP, завжди повинні бути у робочому стані. Протокол часто використовується для передачі повідомлень клієнтами електронної пошти, які, проте, не мають можливості діяти як сервер.

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.

IMAP був розроблений для заміни простішого протоколу POP3 і має такі переваги в порівнянні з останнім:

- листи зберігаються на сервері, а не на машині клієнта. Можливий доступ до однієї і тої ж поштової скриньки з різних клієнтів. Підтримується також одночасний доступ декількох клієнтів. У протоколі є механізми, за допомогою яких клієнт може бути проінформований про зміни, зроблені іншими клієнтами.
- підтримка декількох поштових скриньок (або тек). Клієнт може створювати, вилучати і переіменовувати поштові скриньки на сервері, а також переміщати листи з однієї поштової скриньки в інші.
- можливе створення спільних папок, до яких можуть мати доступ декілька користувачів.

- інформація про стан листів зберігається на сервері і доступна всім клієнтам. Листи можуть бути позначені як прочитані, важливі тощо
- підтримка пошуку на сервері. Немає необхідності завантажувати з сервера великої кількості повідомлень для того, щоб знайти одне потрібне.
- підтримка онлайн-роботи. Клієнт може підтримувати з сервером постійне з'єднання, при цьому сервер у реальному часі інформує клієнта про зміни в поштових скриньках, у тому числі про нові листи.
- передбачено механізм розширення можливостей протоколу.

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.

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.

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»).

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

Основним призначенням протоколу HTTP є передача вебсторінок (текстових файлів з розміткою HTML), хоча за допомогою нього успішно передаються як інші файли, які пов'язані з вебсторінками (зображення та додатки), так і не пов'язані з ними.

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).

SSH (Secure SHell – безпечна оболонка) – мережевий протокол рівня додатків, 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.

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).

SSL (Secure Sockets Layer – рівень захищених сокетів) – криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL спочатку був розроблений компанією Netscape Communications. Згодом на підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що отримав ім'я TLS.

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.

6.2. 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.

6.3. 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: адресний протокол ARP; реверсний адресний протокол RARP (Reverse ARP); протокол діагностичних повідомлень ICMP (Internet Control Message Protocol), який надсилає повідомлення вузлам мережі про помилки на маршруті, які виникають при передачі пакетів тощо.

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.

Функціонування мережевого рівня також забезпечує низка протоколів динамічної маршрутизації RIP, OSPF, які динамічно формують маршрути таблиці маршрутизації за алгоритмами вектора VDA (Vector Distance Algorithm) і стану зв'язку LSA (Link State Algorithm) відповідно; протоколів політики зовнішньої маршрутизації EGP (Exterior Gateway Protocol), BGP (Border Gateway Protocol) тощо.

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

Функції:

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