Міністерство освіти і науки України
Київський університет імені Бориса Грінченка

ПРИКЛАДНІ АСПЕКТИ
ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Аналіз мережевого трафіку

Навчальний посібник

Львів
Видавництво «Магнолія 2006»
2024

УДК 004.056
Б 82

Рекомендовано до друку Вченою радою Київського університету імені Бориса Грінченка (протокол №4 від 25.04.2019 р.)

Автори:

Борсуковський Юрій Володимирович – кандидат технічних наук, Державний університет інформаційно-комунікаційних технологій;

Борсуковська Вікторія Юріївна – керівник проектів департаменту безпеки ПАТ «Укрсоцбанк»;

Бурячок Володимир Леонідович – доктор технічних наук, професор, Київський університет імені Бориса Грінченка;

Складанний Павло Миколайович – кандидат технічних наук, доцент, Київський університет імені Бориса Грінченка;

Гайдур Галина Іванівна – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій.

Рецензенти:

Самохвалов Ю. Я. – доктор технічних наук, професор;

Казмірчук С. В. – доктор технічних наук, доцент.

Борсуковський Ю. В., Борсуковська В. Ю.,
Бурячок В. Л., Складанний П. М., Гайдур Г. І.

Б 82 **Прикладні аспекти інформаційної та кібернетичної безпеки держави. Аналіз мережевого трафіку** : навч. посіб. / Борсуковський Ю. В., Борсуковська В. Ю., Бурячок В. Л., Складанний П. М., Гайдур Г. І. — Львів – Видавництво «Магнолія 2006», 2024. — 222 с.

ISBN 978-617-574-272-3

У підручнику розкриваються методологічні аспекти щодо дослідження поведінки мережевих додатків і вузлів з метою виявлення і виправлення проблем в роботі мережі для забезпечення інформаційної та кібернетичної безпеки підприємства. Нерідко, для вирішення таких проблем, спеціалісти з інформаційної та кібернетичної безпеки вдаються до використання аналізаторів мережевих пакетів.

Ключовими особливостями використання програмних аналізаторів пакетів є, по-перше, можливості різнобічної аналітики, а по-друге, багатофункціональна фільтрація пакетів, що дозволяє отримати витяги інформації, що потрібні нам для аналізу мережевого трафіку. Саме останньому аспекту і присвячений цей учбовий посібник.

Приводяться приклади практичного використання програмного аналізатора пакетів WireShark для захвату і фільтрації мережевого трафіку. Розглядаються питання щодо вибору фільтрів для аналізу функціонування елементів мережі в найдрібніших деталях.

Підручник орієнтований на широке коло наукових та науково-педагогічних працівників, які займаються питаннями розроблення і застосування систем інформаційної та кібернетичної безпеки, а також фахівців, які працюють у галузях управління, планування та прогнозування ІТ, створюють перспективні або модернізують існуючі АС, ведуть дослідження за напрямками забезпечення безпеки та неперервності функціювання систем ІТ.

Викладений матеріал призначений для аспірантів та магістрантів вищих навчальних закладів, які навчаються за спеціальністю «Безпека інформаційно – комунікаційних систем» в галузі знань «Інформаційна безпека».

УДК 32.973я73 р.

ISBN 978-617-574-272-3

ЗМІСТ

ПЕРЕДМОВА 8
ТЕРМІНИ ТА ВИЗНАЧЕННЯ 10

Еталонна модель OSI 13
Ієрархічні івні моделі OSI 13
Прикладний рівень (Application Layer) 16
Представлення рівень (Presentation Layer) 17
Сеансовий рівень (Session Layer) 18
Транспортний рівень (Transport Layer) 18
Мережевий рівень (Network Layer) 19
Канальний рівень (Data Link Layer) 20
Фізичний рівень (Physical Layer) 21
Відповідність моделі OSI та інших моделей мережевої взаємодії 22
Протокол TCP/IP 23
Модель TCP/IP 25
Графічне пояснення моделей OSI і TCP/IP 28
Огляд програм для аналізу мережевого трафіку 31
SolarWinds Network Bandwidth Analyzer 32
WireShark 33
TCPdump 34
Kismet 35
EtherApe 36
Cain and Abel 37
NetworkMiner 37
KisMAC 38
Висновок 39
Введення в WireShark 40
Завантаження WireShark 40
Інструкції для роботи з WireShark 41
Інструкція користувача 42
Порівняння WireShark та його комерційних аналогів 42
Візуалізація проблем 44

Експертний аналіз на рівні додатків 45
Відновлення структури запитів 46
Тимчасова діаграма пакетів 48
Об'єднання потоків даних 49
Висновок 50
Використання WireShark 51
Встановлення і налаштування 52
Кольорове кодування 53
Захоплення пакетів 53
Навігація за списком 55
Управління стовпцями і їх вмістом 56
Упорядкування пакетів 56
Помилка «IP checksum offload» 58
Фільтрація пакетів 60
Фільтри захоплення пакетів 60
Фільтри відображення пакетів 61
Використання експертних опцій 72
Налаштування фільтрів для захоплення трафіку 73
Фільтр по протоколу 75
Фільтр по номеру порту 78
Фільтр по IP адресі і фільтр по MAC 80
Перелік типових фільтрів 83
Пошук конфліктуючих IP-адрес 84
Аналіз мережевого і транспортного рівнів 85
Аналіз HTTP-трафіку 87
Перехоплення SSL-контенту 89
Аналіз трафіку з віддалених хостів 90
Аналіз пакетів 91
Аналіз сеансів і TCP 92
Вилучення даних з трафіку 95
Вилучення VoIP трафіку 98
Сканування портів 100
Варіанти підключення до мережі для захоплення трафіку 101
Захоплення трафіку на стороні клієнта або сервера 101
Захоплення трафіку на комутаторі (SPAN) 103
Переваги SPAN сесії 105
Відгалужувачі мережевого трафіку (TAP) 106

Пошук складних непостійних проблем 111
Налаштування WireShark для аналізу складних проблем 111
Налаштування «dumpcap» для захоплення пакетів 114
Особливості використання «dumpcap» 117
Аналіз SSL/TLS трафіку 123
Використання секретного ключа сервера 126
Використання секретів сесій 130
Розшифровка SSL/TLS трафіку через логування
сесійних ключів браузера 132
Розшифровка TLS трафіку Java додатків 136
Розшифровка WPA2-PSK трафіку 144
Перехоплення паролів 150
Фільтрація захопленого POST трафіку 151
Логін і пароль користувача 151
Визначення типу кодування для розшифровки пароля 153
Розшифровка пароля користувача 153
Розшифровка HTPPS трафіку 153
Процес розриву з'єднання TCP Reset (TCP RST ACK) 155
Локалізація місця TCP Reset 156
Відправка TCP RST (SYN) 157
Відправка TCP RST (ACK) 157
TCP Retransmission 157
Ідентифікація повторних передач 159
Колонка «ACK to» 162
Моніторинг продуктивності сервера і мережі 163
Моніторинг користувача 164
Оцінка часу підключення користувача до сервера 164
Аналіз часу відгуку додатку 166
Локалізація причин 166
Висновки 166
Методика вирішення проблем з додатками 167
Аналіз продуктивності DNS-сервісу 169
Висновок 172

ДОДАТОК 1 174
Просте пояснення моделі OSI 174

ДОДАТОК 2 183
Перелік основних мережевих протоколів 183

ДОДАТОК 3 186
Телекомунікаційна мережа 186
Класифікація за географічним розташуванням 186
Класифікація за структурою взаємозв'язків (топологією) 187
Класифікація за режимом комунікації 188
Класифікація за швидкістю мережі 188
Принципи комунікації 188
Мережеві технології локальних мереж 189
Поняття фрейма 190
Комутація каналів 191
Комутація пакетів 191
Дейтаграма 192
Пакет даних 192
Механізм формування пакетів 192
Протокол визначення адрес (ARP) 193
Опис протоколу 193
ARP-таблиця для перетворення адрес 193
Порядок перетворення адрес 194
Запити та відповіді протоколу ARP 194
MAC-адреса 195
Адресація MAC-рівня 195
Мережа з комутацією каналів 196
Мережа з комутацією пакетів 196
Широкомовна мережа 197

ДОДАТОК 4 199
Поняття маршрутизатора 199
Принцип роботи маршрутизатора 199
Таблиця маршрутизації 200
Застосування 201
Перенаправлення портів і віртуальні сервери 201
Функції безпеки 202
Додаткові можливості 204

ДОДАТОК 5 206
TCP-порти для SSL трафіку 206
Додаток 6 208
Перелік навчальних прикладів трафіку WireShark 208
ЗМІСТ 208

ДОДАТОК 6 212
Протокол Transport Layer Security (TLS) 212
Опис протоколу 212
Відкриття сеансу (рукостискання) 212
Алгоритми обміну/узгодження спільного ключа 214
Цифрові сертифікати 214
Відкликання сертифікатів 216

ЛІТЕРАТУРА 218

Навчальне видання

БОРСУКОВСЬКИЙ Юрій Володимирович
БОРСУКОВСЬКА Вікторія Юріївна
БУРЯЧОК Володимир Леонідович
СКЛАДАННИЙ Павло Миколайович
ГАЙДУР Галина Іванівна

ПРИКЛАДНІ АСПЕКТИ

ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Аналіз мережевого трафіку

Навчальний посібник

Підп. до друку 14.11.2023 р.
Формат 70x100/16. Папір друк. №2. Гарнітура PT Serif.
Умовн. друк. арк. 18,04.

Видавництво «Магнолія 2006»
м. Львів-53, 79053, Україна, тел.: +38 (050) 370-19-57

e-mail: magnol06@ukr.net
https://magnolia.lviv.ua

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників і розповсюджувачів
видавничої продукції: серія ДК № 2534 від 21.06.2006 року,
видане Державним комітетом інформаційної політики,
телебачення та радіомовлення України

Надруковано у друкарні видавця Марченко Т. В.

Протокол TCP/IP

Протокол TCP/IP – це засіб для обміну інформацією між комп'ютерами, об'єднаними в мережу. Не має значення, чи складають вони частина однієї і тієї ж мережі або підключені до окремих мереж. Не грає ролі і те, що один з них може бути комп'ютером Cray, а інший Macintosh. TCP/IP – це стандарт, що не залежить від платформи і який перекидає мости, яка лежить між різнорідними комп'ютерами, операційними системами та мережами. Сьогодні цей протокол використовується для глобального управління мережею Internet [52].

Під терміном «розуміння протоколу TCP/IP» ми будемо мати на увазі нашу здатність розбиратися в наборах протоколів, які використовуються комп'ютерами TCP/IP для обміну інформацією. Далі ми розглянемо деякі із цих протоколів і з'ясуємо, що собою становить стек TCP/IP.

Зрозуміло, що програмне забезпечення TCP/IP на нашому комп'ютері представляє собою специфічну для даної платформи реалізацію протоколів TCP, IP і інших членів сімейства TCP/IP.

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 із метою, щоб обчислювальні мережі дослідницьких центрів у всьому світі могли бути об'єднані для обміну даними у формі віртуальної «мережі мереж» (internetwork). Первісна Internet була створена в результаті перетворення існуючого конгломерату обчислювальних мереж, що носили на той час назву ARPAnet, за допомогою TCP/IP.

Причина, по якій TCP/IP настільки важливий сьогодні, полягає в тому, що він дозволяє самостійним мережам підключатися до мережі Internet або об'єднуватися для створення приватних інтрамереж. Обчислювальні мережі, складові інтрамереж фізично підключаються через пристрої, які називаються маршрутизаторами або IP-маршрутизаторами. Фактично маршрутизатор – це комп'ютер, який передає пакети даних з однієї мережі в іншу. В інтрамережі, що працює на основі TCP/IP, інформація передається у вигляді дискретних блоків, що називаються IP-пакетами (IP packets) або IP-дейтаграмами (IP datagrams).

Завдяки програмному забезпеченню TCP/IP всі комп'ютери, підключені до обчислювальної мережі, стають «близькими родичами». По суті це програмне забезпечення «приховує» маршрутизатори та базову архітектуру мереж і робить так, що все це виглядає як одна велика мережа.

Точно так же, як підключення до мережі Ethernet розпізнаються по 48-розрядним ідентифікаторам Ethernet, підключення до локальної мережі

ідентифікуються 32-розрядними IP-адресами, які ми представляємо у формі десяткових чисел, розділених крапками (наприклад, 128.10.2.3). Таким чином, взявши IP-адресу віддаленого комп'ютера, комп'ютера в інтрамережі або в мережі Internet ми можемо відправити на нього дані, так як нібито вони складали частину однієї і тієї ж фізичної мережі.

Протокол TCP/IP дає вирішення проблеми обміну даними між двома комп'ютерами, підключеними до однієї і тієї ж локальної мережі, але які можуть належати до різних фізичних мереж.

У цьому випадку, рішення складається з декількох частин, причому кожен член сімейства протоколів TCP/IP вносить свою складову в спільну справу.

IP – самий фундаментальний протокол з комплекту TCP/IP – передає IP-дейтаграми по інтрамережі і виконує важливу функцію, що має назву маршрутизація. По суті це вибір маршруту, за яким дейтаграма буде слідувати із пункту А в пункт В, і використання маршрутизаторів для «стрибків» між мережами.

TCP – це протокол більш високого рівня, який дозволяє прикладним програмам, що запущені на різних комп'ютерах мережі, обмінюватися потоками даних. TCP поділяє потоки даних на ланцюжки, які називаються TCP-сегментами, і передає їх за допомогою IP. У більшості випадків кожен TCP-сегмент пересилається в одній IP-дейтаграмі. Однак, при необхідності, TCP має можливість розщеплювати сегменти на кілька IP-дейтаграм, що вміщаються в фізичні кадри даних і які використовуються для передачі інформації між комп'ютерами у мережі.

Оскільки IP не гарантує, що дейтаграми будуть отримані в тій же самій послідовності, в якій вони були послані, TCP здійснює повторну «збірку» TCP-сегментів на іншому кінці маршруту, щоб утворити безперервний потік даних.

Інший важливий член комплекту TCP/IP – User Datagram Protocol (UDP, протокол користувацьких дейтаграм), який схожий на TCP, але більш примітивний. TCP – «надійний» протокол, тому що він забезпечує перевірку на наявність помилок і обмін підтверджуючими повідомленнями щоб дані досягали свого місця призначення завідомо без спотворень. UDP – "ненадійний" протокол, бо не гарантує, що дейтаграми будуть приходити в тому порядку, в якому були послані, і навіть того, що вони прийдуть взагалі.

Інші TCP/IP протоколи грають менш помітні ролі, але не в меншій мірі є важливими у роботі мереж TCP/IP. Наприклад, протокол визначення адрес *(Address Resolution Protocol, ARP)* перетворює IP-адреси у фізичні мережеві адреси, такі, як ідентифікатори Ethernet. Споріднений протокол – протокол зворотного перетворення адрес *(Reverse Address Resolution Protocol,*

RARP) – забезпечує виконання зворотної дії, перетворення фізичних мережевих адрес у IP-адреси.

Порівнюючи ієрархічну побудову моделі OSI і модель TCP/IP ми можемо бачити взаємозв'язок між основними протоколами (Рис. 4). При перенесенні блоку даних із мережевої прикладної програми у плату мережевого адаптера він послідовно проходить через ряд модулів TCP/IP. При цьому, на кожному кроці він доповнюється інформацією, необхідною для еквівалентного модуля TCP/IP на іншому кінці ланцюжка. До того моменту, коли дані потрапляють в мережеву плату, вони представляють собою стандартний кадр Ethernet, якщо припустити, що мережа заснована саме на цьому інтерфейсі. Програмне забезпечення TCP/IP на приймальному кінці відтворює вихідні дані для приймаючої програми шляхом захоплення кадру Ethernet і проходження його в зворотному порядку по набору модулів TCP/IP.

Таким чином, відносно протоколу TCP/IP можна назвати три ключових моменти:

- TCP/IP – це набір протоколів, які дозволяють фізичним мережам об'єднуватися разом для утворення Internet. TCP/IP з'єднує індивідуальні мережі із метою утворення єдиної віртуальної обчислювальної мережі, у якій окремі комп'ютери ідентифікуються не фізичними адресами мереж, а IP-адресами.
- В TCP/IP використовується багаторівнева архітектура, яка чітко описує, за що відповідає кожен протокол. TCP і UDP забезпечують високорівневі службові функції передачі даних для мережевих програм, і обидва спираються на IP при передачі пакетів даних. А IP уже відповідає за маршрутизацію пакетів до їх пункту призначення.
- Дані, що переміщаються між двома прикладними програмами, що працюють на комп'ютерах мережі Internet, «подорожують» вгору і вниз по стекам TCP/IP на цих комп'ютерах. Інформація, додана модулями TCP/IP на стороні відправника, «розрізається» відповідними TCP/IP-модулями на приймаючому кінці і використовується для відтворення вихідних даних.

Модель TCP/IP

Серед основних мережевих моделей існують дві загальноприйняті моделі: модель OSI і модель TCP/IP. Іноді їх називають як теоретичну і практичну моделі.

Модель TCP/IP також називають моделлю DARPA (скорочення від Defense Advanced Research Projects Agency, організація, в якій свого часу розроблялися мережеві проекти, в тому числі протокол TCP/IP, і яка стояла біля витоків мережі Інтернет) або моделлю Міністерства оборони США (модель *DoD, Department of Defense*, проект DARPA працював на замовлення цього відомства).

Модель TCP/IP була розроблена для опису стека протоколів TCP/IP *(Transmission Control Protocol/Internet Protocol)*. Вона була розроблена значно раніше, ніж модель OSI – у 1970 році було розроблено необхідний набір стандартів, а до 1978 року було остаточно сформовано те, що сьогодні ми називаємо TCP/IP. Пізніше стек адаптували для використання в локальних мережах. На початку 1980 протокол став складовою частиною ОС UNIX. У тому ж році з'явилася об'єднана мережа Internet.

Стек протоколів TCP/IP – набір мережевих протоколів, на яких базується інтернет. Зазвичай в стеці TCP/IP верхні 3 рівня (прикладний, представницький і сеансовий) моделі OSI об'єднують в один – прикладний. Оскільки в такому стеку не передбачено уніфікований протокол передачі даних, функції із визначення типу даних передаються додатку.

У моделі TCP/IP визначено чотири рівні. Як видно із рисунка (Рис. 4) – один рівень TCP/IP може описуватися декілька рівнями моделі OSI.

На відміну від еталонної моделі OSI, модель TCP/IP більшою мірою орієнтується на забезпечення мережевих взаємодій, ніж на жорстке розділення функціональних рівнів. Для цієї мети вона визнає важливість ієрархічної структури функцій, але надає проектувальникам протоколів достатню гнучкість в реалізації. Відповідно, еталонна модель набагато краще підходить для пояснення механіки міжкомп'ютерних взаємодій, але протокол TCP/IP, відповідно, став основним міжмережевим протоколом обміну даними.

Розглянем детально рівні моделі TCP/IP і їх відповідність моделі OSI (Рис. 4):

- **Рівень мережевих інтерфейсів (Link Layer).** Відповідає двом нижнім рівням моделі OSI: канальному і фізичному. Виходячи з цього, зрозуміло, що даний рівень визначає характеристики середовища передачі (кручена пара, оптичне волокно, радіоефір), вид сигналу, спосіб кодування, доступ до середовища передачі, виправлення помилок, фізичну адресацію (MAC-адреси). У моделі TCP/IP на цьому рівні працює протокол Ethernet і його похідні (Fast Ethernet, Gigabit Ethernet).
- **Рівень міжмережевої взаємодії (Internet Layer).** Відповідає мережному рівню моделі OSI. Бере на себе всі його функції:

маршрутизацію, логічну адресація (IP-адреси). На даному рівні працює протокол IP.

- **Транспортний рівень (Transport Layer).** Відповідає транспортному рівню моделі OSI. Відповідає за доставку пакетів від джерела до одержувача. На даному рівні задіються два протоколи: TCP і UDP. TCP є більш надійним, ніж UDP за рахунок створення попереднього з'єднання, запитів на повторну передачу при виникненні помилок. Однак, в той же час, TCP повільніший, ніж UDP.
- **Прикладний рівень (Application Layer).** Його головне завдання – взаємодія з додатками і процесами на хостах. Приклади протоколів: HTTP, FTP, POP3, SNMP, NTP, DNS, DHCP.

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Рис. 4. Співставлення рівнів моделі OSI із рівнями моделі TCP/IP

Далі розглянемо ще одне важливе поняття – інкапсуляція, яке дозволяє зрозуміти яким чином відбувається підготовка пакету даних для передачі.

Розглянемо принцип інкапсуляції на конкретному прикладі (Рис. 5). Нехай ми хочемо потрапити з комп'ютера на сайт. Для цього наш комп'ютер повинен підготувати http-запит на отримання ресурсів веб-сервера, на якому зберігається потрібна нам сторінка сайту.

1. На прикладному рівні до даних (Data) браузера додається HTTP-заголовок.
2. Далі на транспортному рівні до нашого пакету додається TCP-заголовок, що містить номери портів відправника і одержувача (80 порт – для HTTP).
3. На мережевому рівні формується IP-заголовок, що містить IP-адреси відправника і одержувача.

4. Безпосередньо перед передачею, на канальному рівні додається Ethernet-заголовок, який містить фізичні (MAC-адреси) відправника і одержувача.

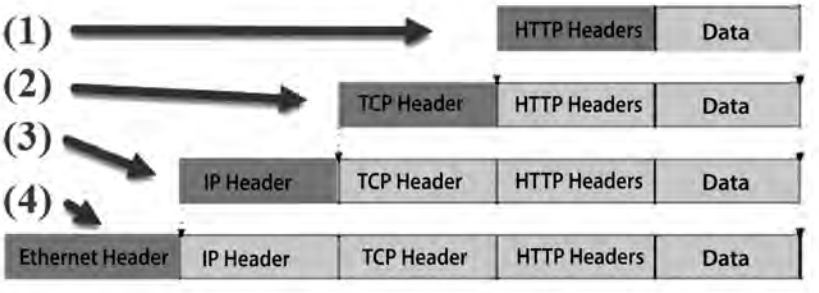

Рис. 5. Пояснення принципу інкапсуляції даних

Після всіх цих процедур пакет у вигляді бітів інформації передається по мережі. На прийомі відбувається зворотна процедура. Web-сервер на кожному рівні буде перевіряти відповідний заголовок. Якщо перевірка пройшла вдало, то заголовок відкидається і пакет переходить на верхній рівень. В іншому випадку весь пакет відкидається.

Графічне пояснення моделей OSI і TCP/IP

Далі наведено кілька зображень, які наочно демонструють функціональні рівні мережевих моделей і їх взаємодію в процесі передачі даних [24].

Layer		Protocol data unit (PDU)
Host layers	7. Application	Data
	6. Presentation	
	5. Session	
	4. Transport	Segment (TCP) / Datagram (UDP)
Media layers	3. Network	Packet
	2. Data link	Frame
	1. Physical	Bit

Рис. 6. Назви фрагментів даних на різних рівнях моделі OSI

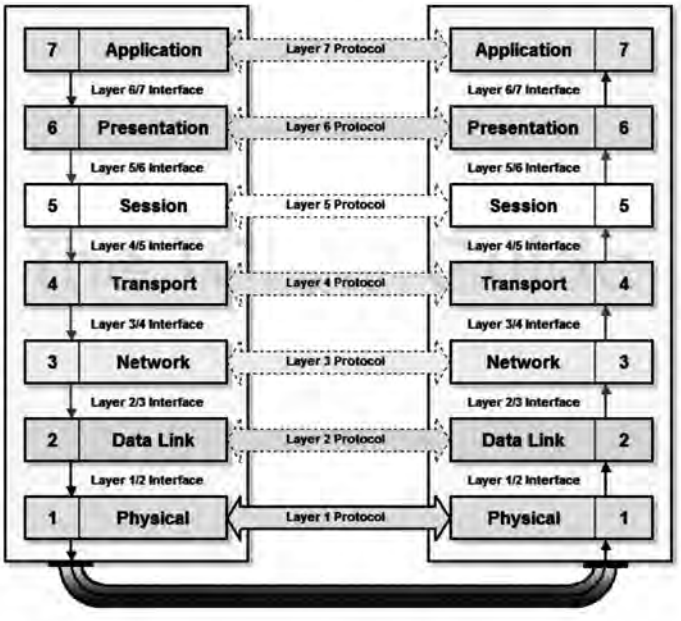

Рис. 7. Всі рівні моделі OSI

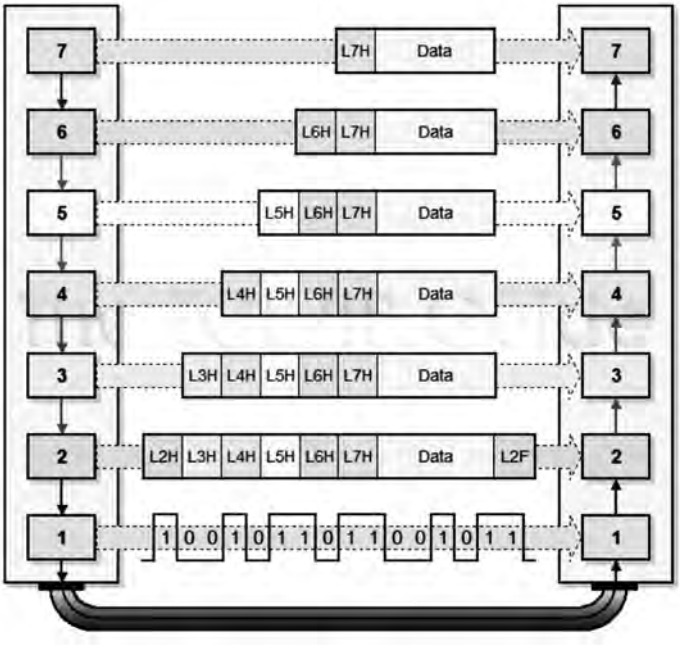

Рис. 8. Інкапсуляція заголовків (L – Layer, H – Header)

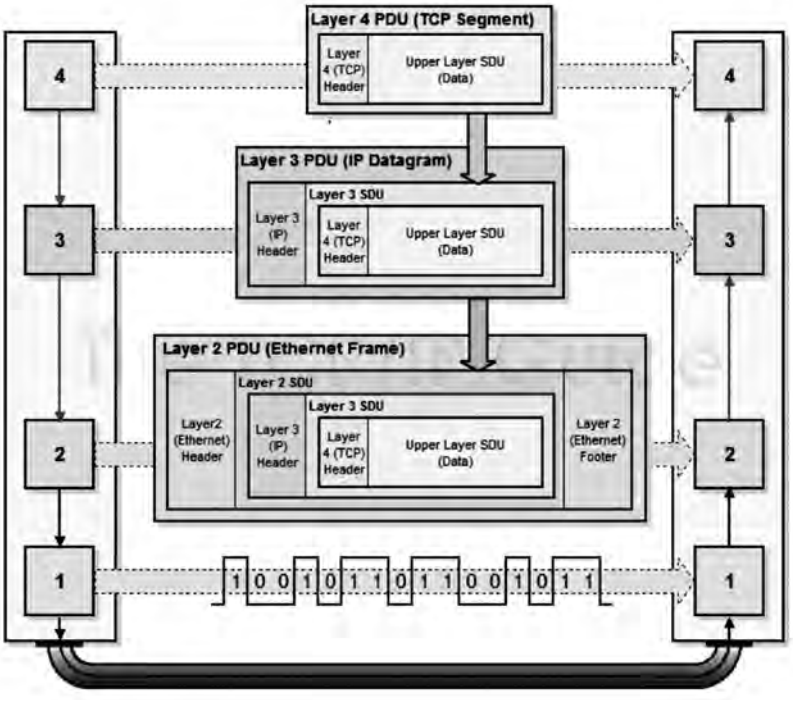

Рис. 9. Інкапсуляція заголовків і даних в 4-х нижніх рівнях

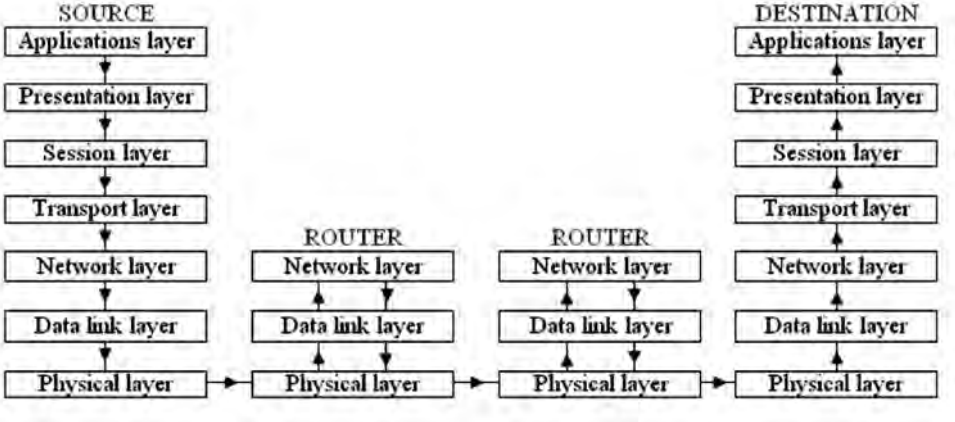

Рис. 10. Потік даних між хостами у розподіленій мережі

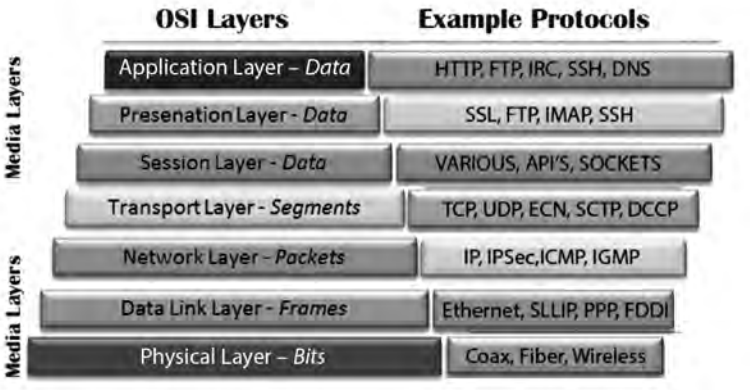

Рис. 11. Приклади протоколів кожного рівня

Огляд програм для аналізу мережевого трафіку

Для дослідження поведінки мережевих додатків і вузлів, а також щоб виявити неполадки в роботі мережі спеціалісти часто вдаються до використання аналізаторів мережевих пакетів. Ключові особливості подібного ПО – це, по-перше, можливості різнобічної аналітики, а по-друге, багатофункціональна фільтрація пакетів, що дозволяє виловити крупиці інформації, що цікавить в безмежному потоці мережевого трафіку.

Аналіз трафіку є процесом і важливість правильної інтерпретації цього процесу відома будь-якому IT-професіоналу.

Зараз на ринку представлена велика кількість варіацій програмного забезпечення для аналізу мережевого трафіку. Ціновий діапазон цих програмних аналізаторів вельми широкий – від безкоштовних рішень до рішень з дорогою корпоративною ліцензією.

Розглянем список з найбільш доступних програмних продуктів для аналізу трафіку, а також зробимо короткий огляд вбудованої в них функціональності для захоплення, обробки і візуального надання різної мережевої інформації [44].

Частина функцій у всіх наведених рішеннях для аналізу мережевого трафіку схожа – вони дозволяють з тим чи іншим рівнем деталізації проглянути відправлені і отримані мережеві пакети, – але практично всі з них мають характерні особливості, які роблять їх унікальними при використанні в певних ситуаціях або мережних середовищах.

Зрозуміло, що до аналізу мережевого трафіку ми вдаємося тоді, коли у нас з'являється мережева проблема, але ми не можемо швидко її локалізувати, звести до певного комп'ютера, налаштування або протоколу, і нам потрібно

проводити більш глибокий аналіз цієї проблеми та пошук причин її виникнення.

SolarWinds Network Bandwidth Analyzer

Рис. 12. SolarWinds Network Bandwidth Analyzer

Дане рішення позиціонується виробником як програмний пакет з двох продуктів – *Network Performance Monitor* (базове рішення) і *NetFlow Traffic Analyzer* (модульне розширення). Як заявляється, вони мають схожі, але все ж відмінні функціональні можливості для аналізу мережевого трафіку, що доповнюють один одного при спільному використанні відразу двох продуктів.

Network Performance Monitor здійснює моніторинг продуктивності мережі і дає загальне уявлення про те, що відбувається у мережі.

Це рішення дозволяє контролювати загальну працездатність мережі, спираючись на величезну кількість статистичних даних, таких як швидкість і надійність передавання даних та пакетів, а також, в більшості випадків, дозволяє швидко ідентифікувати несправність в роботі мережі. Наявність інтелектуальних можливостей програми по виявленню потенційних проблем і широкі можливості по візуальному представленню результатів у вигляді таблиць і графіків з чіткими попередженнями про можливі проблеми, значно полегшує цю роботу.