УДК 004.415.5
Герасимчук М.М. – ст. гр. СІ-41
Тернопільський національний технічний університет імені Івана Пулюя

ПРОТОКОЛ ТУНЕЛЮВАННЯ L2TP

Науковий керівник: асистент кафедри КС, Жаровський Р.О.

Тунелювання в комп'ютерних мережах — процес, в ході якого створюється захищене логічне з'єднання між двома кінцевими точками за допомогою інкапсуляції різних протоколів. Тунелювання являє собою метод побудови мереж, при якому один мережевий протокол інкапсулюється в інший.

Суть тунелювання полягає в тому, щоб "упакувати" передану порцію даних, разом зі службовими полями, в новий "конверт" для забезпечення конфіденційності та цілісності всієї переданої порції, включаючи службові поля. Тунелювання може застосовуватися на мережевому і на прикладному рівнях. Комбінація тунелювання і шифрування дозволяє реалізувати закриті віртуальні приватні мережі (VPN). Тунелювання зазвичай застосовується для узгодження транспортних протоколів або для створення захищеного з'єднання між вузлами мережі.

Тунельний протокол L2TP використовується для підтримки віртуальних приватних мереж. L2TP не забезпечує шифрування та конфіденційність сам по собі, він опирається на інкапсульований протокол для забезпечення конфіденційності. L2TP є протоколом сеансового рівня і використовує зареєстрований UDP-порт 1701.

L2TP використовує два види пакетів: керуючі та інформаційні повідомлення. Керуючі повідомлення використовуються при встановленні, підтримці та анулюванні тунелів і викликів. Інформаційні повідомлення використовуються для інкапсуляції PPP-кадрів, що пересилаються по тунелю. Керуючі повідомлення використовують надійний контрольний канал в межах L2TP, щоб гарантувати доставку. Інформаційні повідомлення при втраті не пересилаються повторно.

Керуюче повідомлення має порядковий номер, який використовується в керуючому каналі для забезпечення надійної доставки. Інформаційні повідомлення можуть використовувати порядкові номери, щоб відновити порядок пакетів і детектувати втрату кадрів. Всі коди надсилаються в порядку, прийнятому для мереж.

L2TP застосовує в якості транспортного протокол UDP і використовує однаковий формат повідомлень як для управління тунелем, так і для пересилання даних. L2TP в реалізації Microsoft використовує в якості контрольних повідомлень пакети UDP, що містять шифровані пакети PPP.

Для забезпечення безпеки L2TP-пакетів звичайно використовується протокол IPsec, який надає конфіденційність, аутентифікацію та цілісність. Комбінація цих двох протоколів відома як L2TP/IPsec.

Кінцеві вузли L2TP тунелю називаються LAC (L2TP концентратора доступу) і LNS (L2TP Server Network). LAC є ініціатором тунелю, тоді LNS - сервер, який очікує нових тунелів. Коли тунель встановлено, мережевий трафік між вузлами є двонаправленим. Потім, протоколи більш високих рівнів запускаються всередині тунелю L2TP. Для цього, L2TP сесія встановлюється всередині тунелю для кожного протоколу вищого рівня. Як LAC, так і LNS можуть ініціювати сесії. Трафік для кожної сесії ізолюється за допомогою L2TP, тому можливо налаштувати кілька віртуальних мереж через один тунель.

Головною перевагою L2TP є те, що цей протокол дозволяє створювати тунель не лише в мережах IP, але і в таких, як ATM, X.25 та Frame Relay.