2 Забезпечення комп'ютерної безпеки в інформаційних системах

Ярослав Буригін, Катерина Красовська*, Наталія Тарасова*, Станіслав Боровик*
*Державна служба спеціального зв'язку та захисту інформації України, *Київський національний університет ім. Тараса Шевченка*
УДК 004.057.4:722.4

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАСТОСУВАННЯ МЕРЕЖЕВИХ ПРОТОКОЛІВ ПЕРЕДАЧІ ДАНИХ ДЛЯ ІДЕНТИФІКАЦІЇ, КОНТРОЛЮ ТА АНАЛІЗУ СТАНУ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Анотація: **Проведено аналіз використання мережевих протоколів у сучасних інформаційно-телекомунікаційних системах на підставі якого визначено протоколи, які доцільно використовувати для проведення контролю та аналізу стану телекомунікаційного обладнання та збору даних про нього.**
Summary: **It was analyzed network protocols using in modern information and telecommunication systems. On the basis of results were defined protocols that should be used for monitoring and analysis of telecommunication equipment and data collection about it.**
Ключові слова: **Мережеві протоколи, телекомунікаційне обладнання, інформаційно-телекомунікаційна система, IP-адрес, MAC-адрес.**

I Вступ

Сучасний стан розвитку інформаційного суспільства потребує більш тісної інтеграції повсякденного життя людини з інформаційно-комунікаційними технологіями, пов'язаними як з обробкою даних, так і їх передачею.

Одним з фундаментальних чинників популяризації цих технологій є використання мережевих протоколів, таких як наприклад TCP/IP [1 – 5], який застосовується в Інтернет, і різноманітних інформаційно-телекомунікаційних системах (далі - ІТС).

Зважаючи на сильну розгалуженість сучасних ІТС і велику кількість користувачів і обладнання в них, питання щодо забезпечення гарантованої адресації є найголовнішим.

Водночас слід зауважити, що зазначене питання тісно пов'язано з процесом передавання, обробки та зберігання інформації в ІТС, а також із забезпеченням захисту інформації, а саме її цілісності, доступності та конфіденційності.

Одним із шляхів забезпечення реалізації означеного є використання унікальних ідентифікаторів, таких як:

- мережева адреса або IP-адреса, яка застосовується для адресації (ідентифікації) користувачів (ресурсів) або телекомунікаційного обладнання мереж (систем);
- фізична адреса або MAC-адреса, яка застосовується для ідентифікації мережевих інтерфейсів (активного обладнання).

Для відображення фізичної адреси комп'ютера (телекомунікаційного обладнання) в середовищах мережевих IP-адрес та навпаки застосовують спеціальні мережеві протоколи, яки дозволяють виконувати цей процес достатньо швидко й зручно.

Таким чином, можна дійти висновку, що знаючи IP-адресу та MAC-адресу комп'ютера, можна достатньо чітко ідентифікувати користувача.

Ярослав Буригін, Катерина Красовська, Наталія Тарасова, Станіслав Боровик ©

Разом із тим стрімкий розвиток інформаційно-телекомунікаційні мереж (систем), які розгорнуті та працюють на території України, призвів до появи проблем з їх інтеграцією та взаємодією, які пов'язані з використанням як застарілого обладнання, так і обладнання різних виробників. Такий стан речей призводить до зниження ефективності та надійності роботи інформаційно-телекомунікаційних систем і проблем з адресацією в них.

Тому метою цієї статті є дослідження результатів аналізу використання протоколів інформаційної взаємодії, які застосовуються в сучасних інформаційно-телекомунікаційних системах, і визначення на підставі цього аналізу множини протоколів, які доцільно використовувати для проведення контролю та аналізу стану телекомунікаційного обладнання та збору даних про нього.

Знання вказаних параметрів надасть можливість впливати на ефективність і надійність роботи як телекомунікаційного обладнання, так і ІТС у цілому.

ІІ Основна частина

Основу дослідження складають протоколи, які безпосередньо використовують саме унікальні ідентифікатори телекомунікаційного обладнання в ІТС, тому що саме за допомогою цих індивідуальних параметрів є можливість визначення стану обладнання, його місцезнаходження, виробника та року виробництва.

Зважаючи, що MAC-адреса та IP-адреса є унікальними параметрами телекомунікаційного обладнання, за допомогою яких можна дізнатися характеристики комп'ютера (обладнання), необхідні для розв'язання зазначених проблем, пропонуємо стисло розглянути кожен з протоколів, які використовують ці параметри, та визначити множину протоколів, які доцільно використовувати для проведення аналізу стану телекомунікаційного обладнання мережі.

Для повноти дослідження необхідно провести більш детальний розгляд теоретичних питань та формалізувати поняття унікальних ідентифікаторів, згаданих вище.

Так, розглянемо для початку, що являє собою IP-адреса [6 – 7].

IP-адреса - унікальна мережева адреса вузла в комп'ютерній мережі, побудована за протоколом IP та потрібна для забезпечення глобальної унікальності адреси в мережі Інтернет та в межах мережі у локальному випадку.

У версії протоколу IPv4, яка використовується сьогодні, IP-адреса має довжину 4 байти, являє собою 32-бітове число, представлене чотирма десятковими значеннями 0 – 255, розділених крапками. IP-адреса складається з двох частин: номера мережі і номера вузла. В ізольованих мережах адреса призначається адміністратором із зарезервованих для мережі блоків адрес, а в мережі, яка є складовою частиною мережі Інтернет, адреса видається провайдером або регіональним інтернет-реєстратором. Це зумовлено тим, що провайдери Інтернет мають закріплений за ними діапазон IP-адрес, і при зміні положення комп'ютера, окрім окремих випадків, коли комп'ютер (обладнання) переміщується в межах однієї підмережі, IP-адреса змінюється відповідно до виділеного діапазону для цієї підмережі.

Водночас кожний маршрутизатор за визначенням входить відразу в кілька мереж, тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в кілька IP-мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес відповідно до кількості мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

IP-адреса може бути або статичною (призначатися користувачем у налаштуваннях пристрою або присвоюється автоматично при підключенні до мережі та не може належати іншому обладнанню), або динамічною (призначається автоматично при підключенні до мережі, має обмежений час дії, визначений сервісом, що призначав IP-адресу).

Для отримання IP-адреси користувач може використовувати один з таких протоколів:

• BOOTP (від англ. bootstrap protocol) або його розширена версія DHCP (англ. Dynamic Host Configuration Protocol — протокол динамічного налаштування вузла) – призначений для автоматичного отримання користувачем (комп'ютером) IP-адреси;

• IPCP (Internet Protocol Control Protocol – протокол керування IP) – використовується для налаштування IP-з'єднання в рамках протоколу PPP (від англ. Point-to-Point Protocol – протокол крапка-крапка). PPP – це двокрапковий протокол канального рівня, який використовується для встановлення прямого зв'язку між вузлами мережі з можливістю автентифікації з'єднання та шифрування;

• Zeroconf (від англ. Zero Configuration Networking) – набір технологій, що дозволяє створювати IP-мережу без конфігурації та спеціальних серверів.

Далі розглянемо детальніше, що являє собою MAC-адреса, її властивості та протоколи, які її використовують.

MAC-адреса (далі – MAC, також трапляється Ethernet-адреса, фізична адреса) – це унікальний ідентифікатор, який присвоюється кожній одиниці активного обладнання комп'ютерних мереж. Адреси в кожному з просторів теоретично глобально унікальні і «прошиті» виробником в апаратну частину обладнання. Якщо на комп'ютері користувача замінюється мережевий адаптер, то і MAC комп'ютера теж змінюється, при цьому в комутаторі відбувається відповідна зміна адрес.

Процедура присвоєння MAC-адреси виробниками обладнання регламентована реєстраційною адміністрацією IEEE (підрозділ IEEE Інституту інженерів радіотехніки і електроніки). Кожен виробник комутаційного обладнання отримує свій унікальний ідентифікатор (OUI) після подання заявки та виплати комісійних зборів в IEEE, що є частиною MAC-адреси (24 біти), xx-xx-xx-yy-yy-yy, де xx-xx-xx – унікальний ідентифікатор виробника, і є незмінною складовою MAC всієї лінійки мережевого обладнання виробника.

У широкомовних мережах (таких, як мережі на основі Ethernet) MAC- адреса дозволяє унікально ідентифікувати кожен вузол мережі і доставляти дані тільки цьому вузлу. Таким чином, MAC-адреси формують основу мереж на канальному рівні, яку використовують протоколи більш високого (мережевого) рівня.

Таким чином, IP-адреса являє собою потужний засіб ідентифікації обладнання або користувачів (комп'ютерів) у мережах, але більш надійним засобом ідентифікації служить MAC-адреса пристрою у мережі, тому що вона «прошита» виробником у саме обладнання, що ускладнює вплив на неї сторонніх чинників (хакерів, іншого обладнання у мережі, адміністратора мережі тошо).

Для перетворення MAC-адрес в адреси мережевого рівня і назад застосовуються спеціальні протоколи: ARP, RARP, InARP в мережах IPv4 та NDP в мережах на основі IPv6 [6-7].

Розглянемо згадані протоколи більш детально.

ARP (від англ. Address Resolution Protocol - адресний протокол) – мережевий протокол, призначений для визначення MAC-адреси за відомою IP-адресою.

Адреси перетворюються шляхом пошуку відповідності в ARP-таблиці. Ця таблиця зберігається в пам'яті і містить у двох колонках відповідні пари зі ставлення IP та MAC-адрес для кожного вузла мережі.

Алгоритм роботи протоколу в широкомовних мережах такий: IP запитує у ARP: «Яку MAC-адресу має інтерфейс з адресою IP1?» ARP дивиться таблицю: якщо запису немає, то записуємо вихідний пакет у буфер. ARP формує ARP запит і надсилає широкомовним кадром Ethernet. Усі хости отримують кадр і передають IP1 з кадру своєму ARP. Той порівнює IP1 з IP інтерфейсу, на який прийшов кадр, і якщо є збіг, генерує ARP-відповідь.

Записи в кеші ARP можуть бути статичними і динамічними. Час зберігання записів у ARP таблиці і метод зберігання вибирається програмно (наприклад, операційною системою), але його можна змінити. Не можна обійти увагою той факт, що новий запис в ARP-таблиці з'являється автоматично, через кілька мілісекунд після того, як вона була потрібна. В операційній системі Windows час оновлення таблиці ARP становить 2 хвилини, але може бути змінений адміністратором мережі.

RARP (від англ. Reverse Address Resolution Protocol — зворотний протокол перетворення адрес) – протокол використовує зворотну логіку (з апаратної адреси - в логічну) протоколу ARP для отримання своєї IP-адреси за своєю MAC-адресою.

Так, під час завантаження вузла мережі або комп'ютера він розсилає групове повідомлення-запит зі своєю MAC-адресою (фізичною адресою). Сервер опрацьовує це повідомлення та переглядає свої таблиці з метою пошуку необхідної IP-адреси або в разі відсутності відповідних даних направляє до іншого сервера. У разі знаходження IP-адреси вона надсилається назад до вузла запиту. Також зазначений діалог можуть зчитувати й інші вузли мережі та зберігати ці відомості у своїх ARP-таблицях.

Крім того, RARP дозволяє розподіляти IP-адресу між хост-вузлами, що застосовуються нечасто. За рахунок цього IP-адресу, що використовувалась якимось вузлом (комп'ютером), може бути звільнено та передано іншому вузлу.

Таким чином, RARP є аналогом DHCP/BOOTP для Ethernet мереж.

Необхідно зазначити, що RARP є застарілим протоколом, а отже не всі реалізації протоколу TCP/IP надають можливість застосовувати RARP.

InARP (Inverse Address Resolution Protocol – інверсивний протокол перетворення адрес) - протокол використовує зворотну логіку (з апаратної адреси - в логічну) протоколу ARP для отримання IP-адреси необхідного вузла (комп'ютера) мережі за відомою MAC-адресою.

InARP є доповненням до протоколу ARP та використовується для зворотнього пошуку.

NDP (Neighbor Discovery Protocol – протокол виявлення сусідів) – протокол, відповідальний за автоналаштування адреси кінцевих точок мережі, виявлення інших вузлів на лінії, виявлення адреси інших вузлів на рівні каналу зв'язку, виявлення конфлікту адрес, пошук доступних шляхів і DNS-серверів, виявлення підмереж і підтримку доступності інформації про шляхи до інших активних сусідніх вузлів.

Цей протокол встановлює п'ять різних типів пакета ICMPv6 для виконання функцій IPv6, схожих з ARP та іншими протоколами взаємодії для IPv4. Порівняно з функціоналом IPv4, цей протокол є більш надійним за наявності в мережі проблемних роутерів і непостійних вузлів.

NDP встановлює такі п'ять типів пакета ICMPv6:

1. запит на доступність маршрутизаторів.
2. відповідь маршрутизатора.
3. запит доступних сусідів.
4. відповідь сусіда.
5. перенаправлення.

Ці повідомлення використовуються для забезпечення наступної функціональності:

- виявлення маршрутизатора: вузол може розмістити маршрутизатор, що знаходиться на підключеній лінії;
- виявлення підмережі: вузли можуть виявляти працюючі підмережі для підключених ліній;
- виявлення параметрів: вузли можуть запитувати параметри лінії;
- автоматична настройка адреси: конфігурування адрес мережевих інтерфейсів;
- дозвіл адреси: робота між IP-адресою та адресами рівня каналу зв'язку;
- виявлення наступного переходу: вузли можуть знаходити наступний на шляху пакета маршрутизатор;
- виявлення недоступності сусіда (NUD): визначення того, що сусід більш недоступний на лінії;
- виявлення конфлікту адрес (DAD): вузли самі можуть визначати, чи зайнята адреса;
- перенаправлення: маршрутизатор може інформувати вузол про інші оптимальні маршрутизатори для початку шляху пакета;
- рекурсивний DNS-сервер (RDNSS) і список пошуку DNS (DNSSL) призначається через параметри відгуку маршрутизатора (RA) – нова функція і підтримується не всім програмним забезпеченням.

Отже, завдяки своїй більш сучасній побудові, протокол NDP може бути надійним інструментом для роботи з MAC та IP-адресами телекомунікаційного обладнання в мережі, але не є універсальним, тому що перехід на стандарт IPv6 на сьогодні відбувається дуже повільно і складно через проблеми узгодження з технологіями, які використовуються у стандарті IPv4.

III Висновок

Виходячи з вищевикладеного, можна дійти попереднього висновку, що MAC-адреса є більш потужним інструментом для роботи з обладнанням у мережі. Цей ідентифікатор використовують мережеві протоколи, які шляхом одночасного застосування IP та MAC-адрес в одній таблиці надають змогу зіставляти та об’єднувати ці два унікальні параметри телекомунікаційного обладнання, що забезпечує більш ефективну роботу як самої ІТС, так і її надійну інтеграцію до мережі Інтернет.

Крім того, за результатами проведеного в статті аналізу необхідно зазначити, що на цей час серед мережевих протоколів, що використовують MAC та IP-адреси, особливої уваги заслуговує протокол ARP: простий, але такий, що має достатній функціонал для об'єднання двох найважливіших унікальних параметрів обладнання в єдину динамічно оновлювану таблицю, що забезпечує більш надійну ідентифікацію телекомунікаційного обладнання.

Водночас, вважається за необхідне провести окреме наукове дослідження для побудови математичного та інформаційного апарату для здійснення аналізу існуючих інформаційно-телекомунікаційних систем, побудови їх віртуальних моделей і проведення математичних розрахунків надійності та відмовостійкості інформаційно-телекомунікаційних систем.

Крім того, зважаючи, що адміністратор мережі або користувач, застосовуючи певну техніку, програмні засоби і алгоритми має можливість замість «прошитої» MAC-адреси, призначити телекомунікаційному обладнанню будь-яку іншу MAC-адресу, з метою однозначної ідентифікації користувачів та недопущення їх підміни, пропонуємо дослідити можливість додаткового застосування інших унікальних ідентифікаторів, а саме реєстраційних номерів апаратної частини обладнання або його програмного забезпечення.

*Список використаної літератури: **1**. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. СПб.. Питер, 2006. - 958 с, **2.** Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. - 960 с., **3.** Палмер М., Синклер Р. Б. Проектирование и внедрение компьютерных сетей. Учебный курс. 2-е изд., перераб. и доп.: Пер. с англ. - СПб.: БХВ-Петербург, 2004. - 752 с. **4.** Одом, Уэнделл. Компьютерные сети. Первый шаг.: Пер. с англ. - М.: Издательский дом «Вильямс», 2006. 432 с. **5.** Современные компьютерные сети. 2-е изд./ В. Столлингс. СПб.: Питер, 2003. 783 с.: ил. -(Серия «Классика computer science»). **6.** Network Protocols Handbook - Javvin Technologies (January 2005) - 360 pages. **7.** Семенов Ю. А. Протоколы Интернет – М.: Горячяя линия-Телеком, 2001 – 1100 с.*