УДК 004.77

В.А. ЧУБАРОВ*, канд. техн. наук, доц., В.В. КОСТЕНКО, аспірант
Криворізький національний університет

ПРОБЛЕМА НЕКОРЕКТНОЇ КОМУТАЦІЇ ETHERNET КАДРІВ У МЕРЕЖЕВИХ КОМУТАТОРАХ РІВНЯ ДОСТУПУ

Метою роботи є мінімізація впливу помилкової комутації Ethernet кадрів мережевих комутаторів на якість обслуговування абонентів та автоматизація процесу виявлення моментів, коли в Ethernet комутаторі виникає hash conflict.

Методи дослідження. В представленій роботі виконано детальний технічний аналіз факторів і умов, які впливають на ефективність комутації Ethernet кадру в комутаційній матриці. На основі експерименту доведено, що у результаті помилкової комутації відбуваються втрати Ethernet кадрів, інформація потрапляє в інший порт абонента, що викликає спрацьовування комерційного обмеження, яке накладається на порт, з урахуванням обраного абонентом тарифного плану, а також зниження якості обслуговування сервісу, який надається абоненту.

Наукова новизна. Наукова новизна полягає в тому, що даний метод дозволить мінімізувати вплив помилкової комутації без фізичної перебудови топології діючої комп'ютерної мережі і заміни частини, або усього мережевого обладнання як рівня доступу, також і рівня агрегації. Додаткові фінансові витрати на придбання обладнання при цьому не передбачені.

Практична значимість. Виключення ймовірності втрати пакетів в комутаторі через помилкове потрапляння не запитаної інформації в порт абонента, в результаті чого могла відбуватись деградація якості обслуговування абонентів.

Результати. На підставі виконаних досліджень та встановлених залежностей запропонована організація поділу, сегментування і логічної ізоляції абонентського трафіку, який може потрапляти в абонентські порти в разі помилкової комутації Ethernet кадрів**.** Одночасно з моніторингом бази даних завантаження портів, було ухвалено рішення включення команди show flood_fdb у базу даних подій. Таким чином, щоразу, коли комутатор сам у себе своїми засобами виявляє конфлікт hash, у базу даних потрапляє й фіксується ця подія. Це дозволяє автоматизувати процес виявлення моментів, коли в комутаторі виникає hash conflict.

Ключові слова. Ethernet кадр, MAC-адреси, hash конфлікт, комутаційна матриця.

doi: 10.31721/2306-5451-2020-1-50-9-15

Проблема та її зв'язок з науковими та практичними завданнями. Сутність проблемі в тому, що відбувається некоректна комутація Ethernet кадру через hash конфлікт у комутаційний матриці. Конфлікт hash виникає тоді, коли через організацію внутрішньої логіки комутатора деякі MAC-адреси вважаються рівними один одному. У результаті такої "помилки" у таблицю комутації попадає тільки перший MAC, а кадри, призначені конфліктуючим MAC, поширюються по всій мережі. Уперше цей конфлікт, і його наслідки були помічені у провайдерських мережевих структурах рівня доступу ще в 2010-2012 роках. Деяким системним адміністраторам проблема вже була відома і вирішувалася вона різними способами. На офіційному форумі технічної підтримки комутаторів D-Link є коментар, який містить технічні подробиці цієї проблеми [1]. В даній статті описано природу та проблематику цього явища і запропонований варіант зменшення впливу цієї проблеми на якість обслуговування рівня доступу.

Аналіз досліджень і публікацій. У роботах [6-9] висвітлюється дана проблема й наводяться деякі варіанти її вирішення. При тому як шляхом зміни алгоритмів хешування, так і шляхом зміни алгоритмів прийняття рішень. Проведено дослідження, що спрямовані на оптимізацію алгоритмів фільтрації кадрів. У статті [11] доводиться, що розвиток методів і алгоритмів фільтрації трафіку в міжмережевих мостах і комутаторах є актуальною як з практичної, так і з теоретичної точки зору. Всі дослідження в вищенаведених матеріалах, звичайно ж, або мінімізують проблему, або повністю її усувають, але при цьому з точки зору практики, жоден з методів не може бути реалізованим. Причини в наступному - при вирішенні проблеми хешування пропонується змінити його алгоритм і при цьому практична частина передбачає розробку принципово нового чіпа ASIC, і в роботі це реалізовано на ПЛІС. Якщо такий метод реально застосувати на практиці, при тому як на проектованій мережі, так і на діючій, то на проектованій доведеться замовляти мережеве обладнання з чіпами, де алгоритм вже реалізований. З урахуванням індивідуальних розробок це є економічно не вигідним, та й не виключено, що в даному алгоритмі відсутні інші, ще більш серйозні помилки. На реально діючій мережі (не в лабораторних умовах) при високих навантаженнях і індивідуальних особливостях, тестування не проводилося. А в разі застосування на діючій мережі, це взагалі не піддається реалізації ніяк, тому, що в цьому

випадку, виникає необхідність повної заміни обладнання на всіх мережевих рівнях. А це неможливо з багатьох причин. Пропонований метод vlan per user, хоч і не усуває проблему повністю, а тільки зменшує вплив хибних комутацій Ethernet кадрів, за те його впровадження, не передбачає заміну обладнання, а лише передбачає перестроювання логічної топології.

Постановка завдання. Основним показником продуктивності комутаторів є кількість оброблених кадрів в одиницю часу і час затримки кадру. Кадри, які надходять в один порт Ethernet комутатора, повинні передаватися в інший порт тільки в тому випадку, якщо вони призначені для мережі, підключеної до іншого порту. Трафік, тобто Ethernet кадри, призначені для мережі, яка підключена до інших абонентських портів, не повинні туди потрапляти. У разі, коли Ethernet комутатор застосовується на рівні доступу в Інтернет сервіс провайдерів, то обов'язково присутня комерційна складова, а саме: на кожен порт комутатора накладається обмеження за кількістю переданої інформації за одиницю часу. У тому разі, якщо відбулася помилкова комутація Ethernet кадру, інформація потрапляє в інший порт абонента, що може викликати спрацьовування комерційного обмеження, яке накладається на порт, з урахуванням обраного абонентом тарифного плану. Це в свою чергу може викликати втрату пакету тієї корисної інформації, яку абонент отримував на момент помилкової комутації Ethernet кадруЗ метою економії фізичної пам'яті таблиці MAC адрес в мережевих комутаторах, MAC адреса потрапляючи в комутатор в складі ethernet кадру, не записується і не зберігається в пам'яті в тому вигляді як є, а зберігаються тільки деякі hash функції які обчислюються на основі MAC адреси і VLAN. Чіпсети всіх сучасних моделей схильні до цієї проблеми. Оскільки основних виробників присутній всього два: Broadcom і Marvell, то у багатьох вендорів виникає вказана проблема в тій чи іншій мірі на різних серіях комутаторів. І повністю усунути цю проблему можна тільки розробкою по суті нового чіпа, з повною переробкою всього апаратного та схематичного рішення всіх комутаторів. Це призведе до чималого подорожчання отриманого пристрою. Тому завдання в тому, що б не усувати hash конфлікт, а мінімізувати його вплив на продуктивність і якість обслуговування комп'ютерної мережі в цілому, застосувавши розподіл підключених мережевих пристроїв на частини, аж до vlan per user.

Викладення матеріалу та результати. Проблема "конфлікту hash" на мережевих комутаторах D-Link рівня доступу.

Причина "конфлікту MAC". У пам'яті комутатора MAC-адреси не зберігаються у своєму натуральному вигляді. Зберігаються лише деякі значення hash-функції, обчислені на основі MAC і VLAN[3]. Виглядає це приблизно так: val1=hashfunc(mac1+vlan1). Інший запис для іншої пари mac2 і vlan2 буде, відповідно, val2=hashfunc(mac2+vlan2).

На рис 1. наведена схема для більш детального розуміння причини "конфлікту MAC" у пам'яті комутатора.

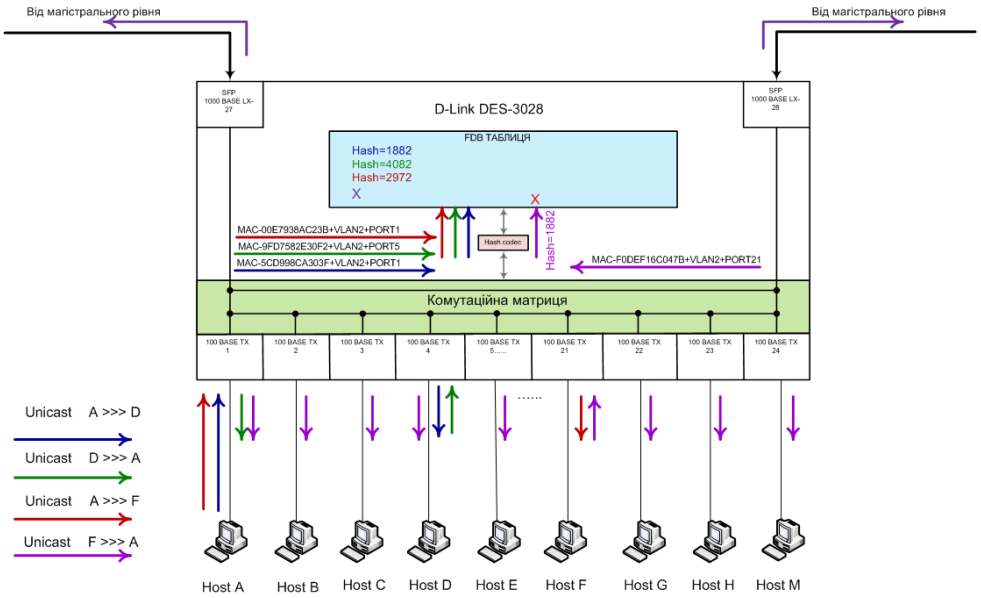

Рис 1. Схема комутатора для більш детального розуміння причини "конфлікту MAC" у пам'яті FDB таблиці

При цьому для зберігання подібних значень пам'ять виділяється в умовах найсуворішої економії. Із цього випливає, що унікальність кожного запису реалізована з деякими допущеннями. Тому ймовірність того, що val2 буде рівно val1 суттєво відрізняється від нуля. Якщо таке відбувається, то mac2 уважається рівним mac1. Із усіх таких MAC-адрес комутатором буде вивчений тільки перший, тому що відмінностей між ними комутатор не бачить.

З модельного ряду D-Link моделі в порядку убування ймовірності конфлікту можна розташувати так:

DES-3028 (чипсет BCM 5347), DES-1228/ME/A1 (чипсет BCM 5347, апаратний аналог 3028);

DES-3200-28/A1/B1 (чипсет BCM 53262), DES-1228/ME/B1 (чипсет BCM 53262), DES-1210-28/ME/B2 (чипсет BCM 53262);

DES-3528, DES-3526;

DES-3200-28/C1.

Можливо, варто було б помістити серію 35xx і 3200-28/C1 в один ряд, але точних описаних даних у літературі знайти не вдалося.

Офіційні коментарі від інженерів D-Link говорять, що чипсети всіх сучасних моделей піддаються даним проблемам. Оскільки основних виробників усього два: Broadcom і Marvell, то в багатьох вендорів спостерігається дана проблема тією чи іншою мірою на різних серіях комутаторів. Чипсети минулих моделей, мали 2-х рівневий хеш, а не однорівневий як нові, тому на них практично відсутня дана проблема, на що вказують тести вендора D-Link. Виробники чипсетів збільшили швидкість роботи FDB(Forward DataBase) таблиці, але як побічний ефект одержали проблему з хешами. Також багато чого залежить від того, як реалізована пам'ять під FDB таблицю й скільки біт відпущене під один хеш запис.

Наявність проблеми хешування MAC зовсім не говорить про те, що дану модель застосовувати неможливо. Кожна модель комутатора має свою маркетингову нішу й припускає її правильне використання. Наприклад моделі DES-3028 і DES- 3200 більшою мірою розраховані на використання з операторською моделлю QinQ. Модель DES-3528 розрахована на корпоративний сегмент, де ціна встаткування має менше значення ніж необхідний функціонал. Модель Des-1210-xx розрахована на використання з операторською моделлю без QinQ.

Як видно із проведених тестів [3] у моделі DES-3028 найнижча стійкість хэш функції до довгих послідовностей (найбільший відсоток колізій утворених хешей), тому при використанні даної конкретної моделі було рекомендовано уникати їх багатокаскадних послідовних з’єднань. В інших моделях дана проблема відсутня.

При експлуатації даних комутаторів, підтверджується, що на моделі DES-3028 проблема виражена гостро, на DES-3200-28/A1/B1 - проблема проявляється менше, а на інших моделях (з перерахованих) може бути помічена тільки при явно помилковому проектуванні мережі.[9]

Діагностика й виявлення проблеми.

а) Пристрій у мережі доступний, MAC-адреса коректна (див. біт для групового розсилання), але на порту не виявляється.

б) За допомогою спеціального функціонала enable flood_fdb. Комутатор почне стежити за MAC-адресами й вести в пам'яті копію (тобто цей функціонал - винятково моніторинг) конфліктів. Переглянути таблицю конфліктів можна командою show flood_fdb, приклад виконання якої наведений у таблиці 1.

Таблиця 1

Приклад show flood_fdb - конфлікт FDB

Value	VLAN ID	MAC Address	Time Stamp
3865	24	00-22-B0-04-6A-17*	9978796
3865	1511	00-1A-79-11-85-E4	9978796
2438	115	00-D0-5C-78-2D-70	2716954

Однакове value указує на конфлікт. Зірочка говорить про те, що MAC- адреса присутня у таблиці комутації. Таким чином, "проблемним" у даному прикладі є MAC 00-1A-79-11-85-E4.

В DES-3200-28/C1 такого механізму немає, тому що вважається, що дана модель не піддана проблемі "конфлікт hash".

Наслідки й варіант розв'язку конфлікту MAC-адреси. Самою очевидною проблемою, звичайно ж, буде відсутність усіх "пересічних" MAC-адрес у таблиці комутації. При одержані кадра, адресованого такому MAC-у, комутатор не зможе визначити порт призначення DLF (Destination Lookup Failure) і кадр буде відправлений в усі порти, які є учасниками даного VLAN, крім того у порт, звідки даний кадр був отриманий. Тим самим комутатор (світч) перетворюється в концентратор (хаб), тобто не справляється зі своїм основним завданням - комутацією трафіка. Чим більше пересічних MAC-адрес у мережі, тим більше зайвого трафіка по ній переміщається. Якщо трафік поширюється на абонентів, які оплачують різні тарифні плани, то у випадку "конфлікту hash" трафік абонента з більшою смугою, потрапить у порт абонента з меншою смугою. Частина кадрів при такій ситуації може втрачатися й кінцевий споживач не одержує небхідну якість надаваного сервісу.

Це й було виявлено засобами моніторингу навантаження на абонентські порти рівня доступу. Скрін навантаження абонентського комутатора, де зіставлені графіки завантаження портів у момент проблеми, надано на рис 2.

З рис 2. видно, що в моменти часу з 4 до 6 ранку, з 12:00 по 12:15 а так само з 14:00 по 14:15 трафік у всіх графіках ідентичний по своїй структурі. Отже, природа виникнення цього трафіка є саме конфлікт hash MAC-адрес на комутаторі рівня доступу.

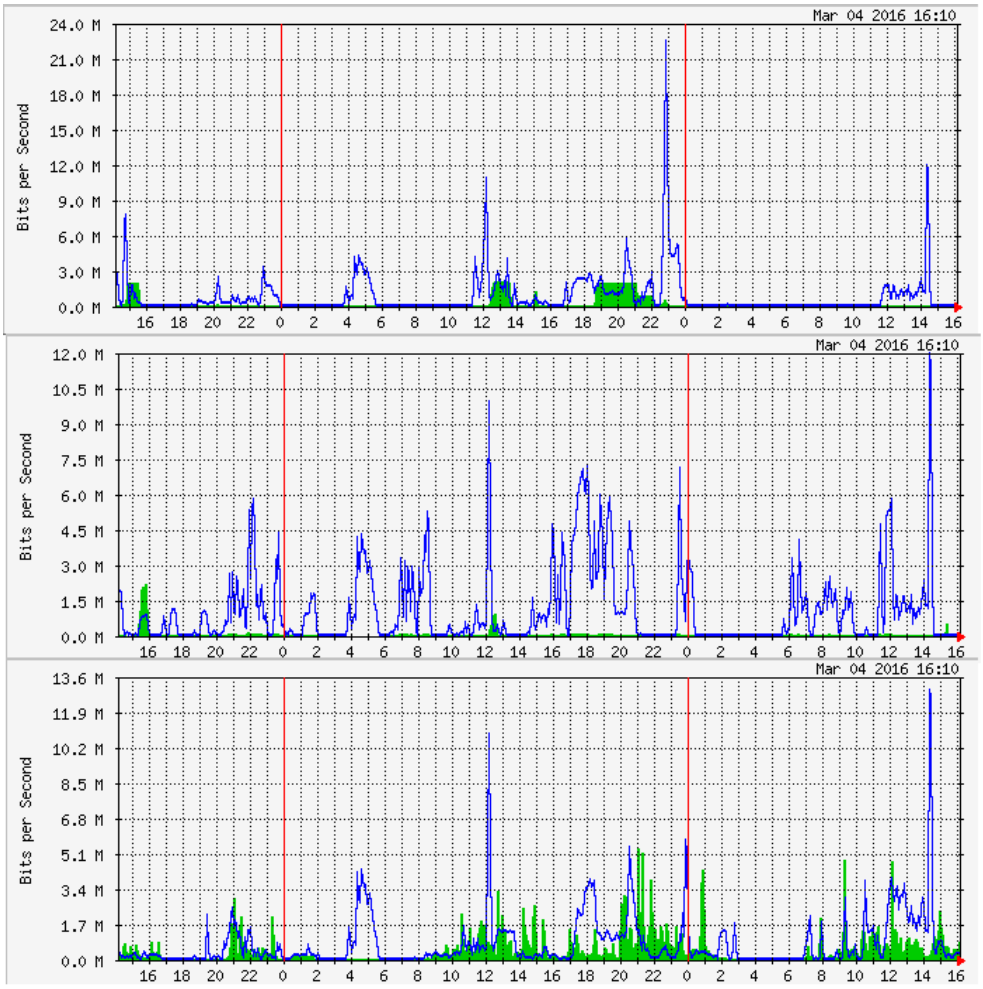

Рис 2. Графіки завантаження портів у момент проблеми конфлікту hash

Одночасно з моніторингом бази даних завантаження портів, було ухвалене рішення включення команди show flood_fdb у базу даних подій.

Таким чином, щоразу коли комутатор сам у себе своїми засобами виявляє конфлікт hash, у базу даних попадає й фіксується ця подія. На рис 3. зображений фрагмент інформації з фіксації конфлікту hash засобами самого комутатора і поява запису про цей конфлікт в базі даних подій комутатора.

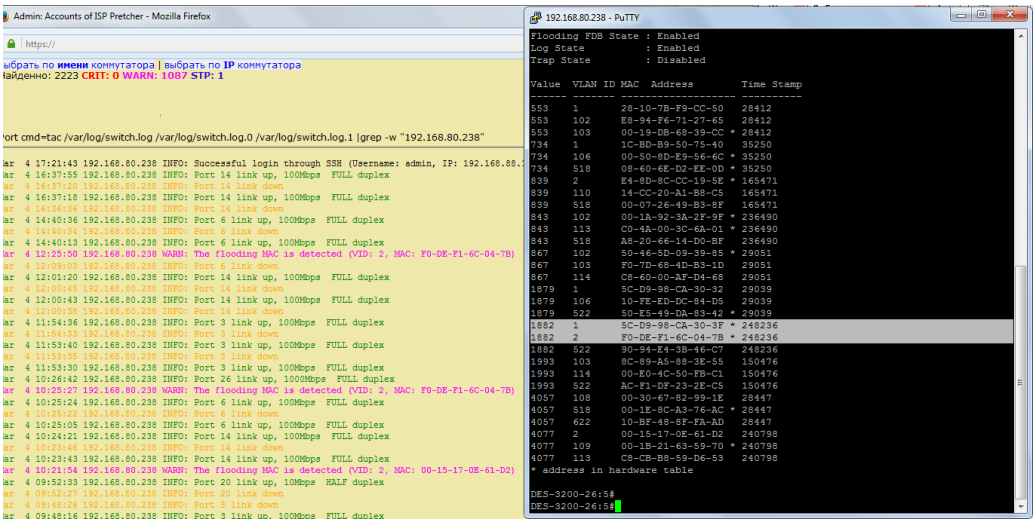

Рис 3. Фрагмент інформації з фіксації конфлікту hash засобами самого комутатора і поява його в базі даних подій

При детальному аналізі й зіставлення отриманих фактів, удалося з'ясувати, що час на графіках завантаження портів у момент проблеми збігається із часом у таблиці подій. У такий спосіб вдається знаходити мережні пристрої, яких з’являються конфлікти hash.

Як варіант розв'язку, пропонується зменшити вплив конфлікту на якість надаваного сервісу. Пропонується фізичне виключення проблемних комутаторів з кільцевої топології й включення їх по окремому фізично незалежному оптичному лінку. А у випадку неможливості такого розв'язку або відсутності вільних волокон, пропонується сегментація мережі на Vlan-и меншого розміру, аж до vlan-per-user. Широкомовний домен при цьому поменшається, кількість переданого по мережі трафіка теж. На рисунку 4 наведена схема зміненої фізичної топології мережі рівня доступу з метою мінімізації конфлікту hash на якість надаваного сервісу.

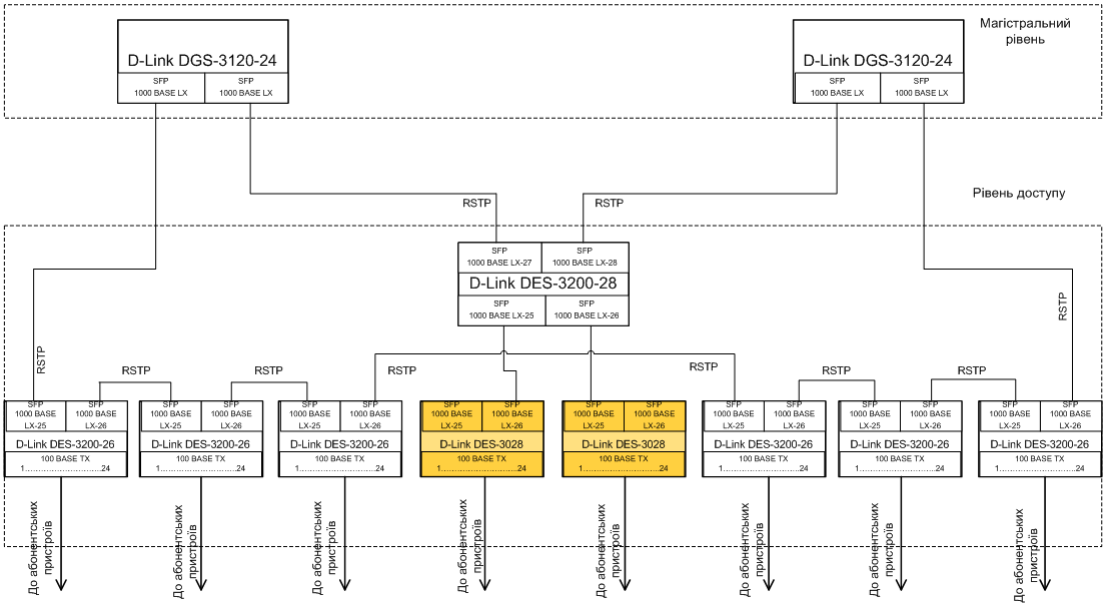

Рис 4. Схема зміненої фізичної топології мережі рівня доступу з метою мінімізації конфлікту hash

У випадку vlan-per-user проблема буде зведена до мінімуму, але не виключена повністю. І причина тому є присутність ще двох VLAN, які не можуть бути зменшені до мінімальної кількості VLAN-ів. Це виникає у зв’язку з присутністю керуючого (management) і мультикаст (mvr) VLAN-ів. Оскільки конфлікти запросто відбуваються між різними VLAN, то перетинання з абонентським MAC може викликати "флуд трафіку" керуючого VLAN-у або погіршення роботи IPTV.

На рис. 5 наведений приклад конфлікту hash між різними VLAN.

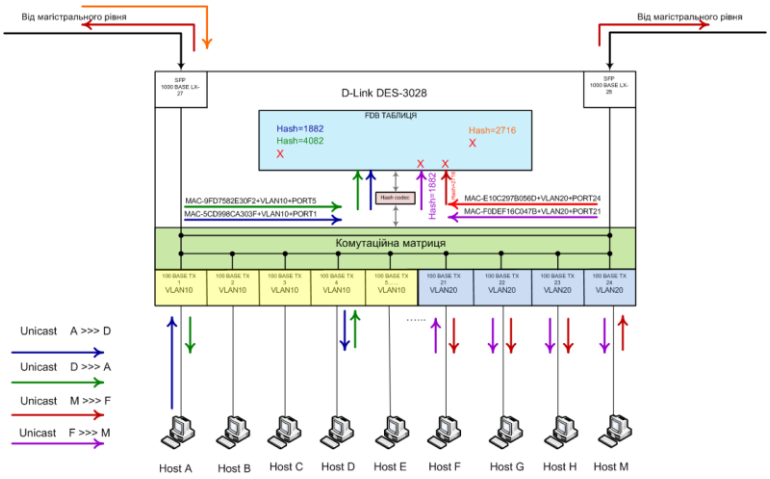

Рис 5. Приклад конфлікту hash між різними VLAN.

З рис 5. варто зробити висновок, що MAC E1-0C-29-7B-05-6D і F0-DE-F1-6C-04-7B із-за конфлікту hash не можуть потрапити до FDB таблиці.

Отже, конкретно для цих MAC-адрес комутатор буде працювати в режимі HUB і отже трафік усередині сегмента конкретно цього VLAN (у наведеному випадку VLAN20) буде поширюватися на всі порти.

Наступна проблема - сам механізм виявлення таких конфліктів (enable flood_fdb), де проводяться обчислення, аналогічні тим, що виконуються в ASIC (Application-Specific Integrated Circuit) [3]. Тобто це не добування проблемної адреси з комірок пам'яті, а обчислення, що проводиться паралельно роботі чипа. Тільки в цьому випадку витрачаються вже ресурси CPU. Звідси випливає, що великий потік трафіка може привести до непотрібного навантаження на CPU комутатору. На практиці, на жаль, так і виходить. У моделі DES-3028 навантаження на CPU може доходити до 100% тим самим роблячи пристрій недоступним. При тому, якщо комутатор виступає в ролі релей-агента, то абоненти перестають одержувати адреси від DHCP. На DES-3200-28/A1/B1 ситуація трохи відрізняється - комутатор з деякою ймовірністю не може відповісти на ARP-запит. Коли час життя ARP (Address Resolution Protocol) на маршрутизаторі минає, комутатор на якийсь час стає недоступний. А оскільки моніторинг за працездатністю всіх комутаторів рівня доступу виконаний за принципом перевірки їх доступності, то результатом може стати періодично повторювана "аварія" на карті моніторингу мережі. Це у свою чергу може ввести в оману службу моніторингу, в обов'язки якої входить контроль над працездатністю комп'ютерної мережі в цілому.

Висновки та напрямок подальших досліджень. Визначені наслідки впливу конфлікту hash на якість обслуговування кінцевих мережевих пристроїв абонентів повністю усунути неможливо. Але є можливість максимально зменшити їх вплив, а саме використовувати сегментацію мережі аж до vlan-per-user. Параллельно з цим треба виконати фізичне виключення проблемних комутаторів з кільцевої топології й включення їх по окремому фізично незалежному оптичному лінку. А при проектуванні нових сегментів комп'ютерної мережі, використовувати комутатори де застосовується метод дворівневого hash. Виробник таких комутаторів в більшості випадків заявляє, що проблема hash-conflict зведена до мінімуму. Напрямком подальших досліджень є необхідність автоматизувати процесс виявлення hash conflict та забезпечити інформацією службу моніторингу.

Список літератури

1. des-3200 ХЭШ [Електронний ресурс] Режим доступу до статті: http://forum.dlink.ru/viewtopic.php?p=653278#p653278

2. Memory management unit architecture for switch fabric EP 1168727 A2 [Електронний ресурс] Режим доступу до статті: http://nag.ru/upload/images/15587/img_EP1168727A2.pdf

3. Проблема хеш коллизий [Електронний ресурс] Режим доступу до статті: http://nag.ru/articles/reviews/15587/raz-tablitsa-dva-tablitsa.html

4. **Брюс Шнайер** (Bruce Schneier), «Прикладная криптография», 2е издание, ISBN 0-471-11709-9, гл.18, Однонаправленные хэш-функции

5. **Росс Андерсон** (Ross Anderson), «Security Engineering» (англ.), Wiley, ISBN 0-471-38922-6

6. **Маков С.В., Шрайфель И.С., Литюк В.И.** Метод фильтрации трафика в Ethemetмостах и условия его применения // Электротехнические и информационные комплексы и системы, научно-технический и теоретический журнал. - М.: Изд-во РГУТиС - №4, т. 6.- 2010. - С. 22-27

7. **Маков С.В., Шрайфель И.С.** Оценка эффективности фильтрации трафика в межсетевых мостах и коммутаторах [Электронний ресурс] // Сервис в России и за рубежом. - Вып.5(24). - 2011г. URL; http:// www.mgus.ru/ files/ electronicjoumal/ number24/ 5.doc

8. **Маков С.В.** Быстрая фильтрация кадров в мостах Ethernet с адаптивным вычислением хеш-функции // Современные проблемы радиоэлектроники: Сборник научных трудов. - Росж)в-на-Дону.: РШСТ ГОУ ВПО «ЮРГУЭС». - 2010. - С. 80-82

9. **Ткачев В.Н.** Современные проблемы в развитии кампусных информационных сетей общежитий ХНУРЭ / В.Н. Ткачев, С.Р. Полчаников. - Сборник тезисов Международной научно-технической конференции, посвященной 75-летию В.В. Свиридова "Информационные системы и технологии" (ИСТ-2012). - Морское-Харьков: 2012. - 152 с.

10. **О.Г. Король Л.Т. Пархуць, С.П. Евсеев**. Метод каскадного формирования мас-кодов с использованием модулярных преобразований Научные ведомости 2013. №15 (158). Выпуск 27/1

11. **Маков, Сергей Владимирович** Разработка и исследование эффективности методов построения таблиц фильтрации кадров в мостах и коммутаторах вычислительной техники [Электронний ресурс] https://www.dissercat.com/content/razrabotka-i-issledovanie-effektivnosti-metodov-postroeniya-tablits-filtratsii-kadrov-v-most

Рукопис подано до редакції 18.03.2020

УДК 622.235

О.О. ФРОЛОВ*, д-р техн. наук, проф., В.М. ПИКАЛО, студ.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

УДОСКОНАЛЕННЯ МЕТОДИКИ ВИЗНАЧЕННЯ РАЦІОНАЛЬНОГО ДІАМЕТРУ СВЕРДЛОВИН ДЛЯ БУРОПІДРИВНИХ РОБІТ

Мета. Метою роботи є встановлення найбільш раціонального діаметра свердловинного заряду вибухової речовини для конкретних гірничо-геологічних умов відпрацювання родовища.

Методи дослідження. Для досягнення поставленої мети в представлених дослідженнях використано: метод комплексного аналізу – для аналізу та узагальнення попередніх наукових досліджень щодо вибору та встановлення найбільш раціональних діаметрів свердловинних зарядів на кар'єрах; аналітичний та графоаналітичний методи – для удосконалення методики визначення діаметра свердловинного заряду при проведенні буропідривних робіт на кар'єрах в гірських масивах з різним ступенем тріщинуватості.

Наукова новизна. Наукова новизна результатів досліджень полягає в тому, що, на підставі представленої аналітичної залежності, отримано графічні залежності зміни вартості буропідривних робіт для різних діаметрів свердловинного заряду вибухової речовини. Вони дозволяють встановити найбільш раціональні діаметри свердловин в кар'єрі при заданих умовах з урахуванням різного ступеня тріщинуватості гірського масиву.

Практична значимість. Результати досліджень дозволяють для встановлених гірничо-геологічних та технологічних умов розробки родовища корисних копалин визначити раціональний діаметр вибухових свердловин на основі врахування техніко-економічних показників роботи підприємства.

Результати. За результатами виконаних досліджень встановлено, що діаметр свердловинного заряду є одним з найбільш важливих параметрів регулювання ступеня дроблення, а його вибір залежить від міцності та тріщинуватості порід. Запропоновано удосконалену методику визначення раціонального діаметру свердловин для буропідривних робіт на кар'єрах. Отримано вираз, який пов'язує вартісні показники буріння і підривання з основними технологічними показниками буропідривних робіт, в тому числі з діаметром свердловинного заряду. Для гірничо-геологічних умов кар'єру побудовані залежності між діаметром свердловинного заряду ВР та вартістю буропідривних робіт для різних гірських порід з різним ступенем тріщинуватості. Встановлені раціональні діаметри свердловинного заряду при виконанні бурових робіт станками СБШ-250 для порід різної категорії тріщинуватості

Ключові слова: буропідривні роботи, діаметр свердловини, питомі витрати, гірський масив, вибухова речовина, тріщинуватість, кар'єр.

doi: 10.31721/2306-5451-2020-1-50-15-20

Проблема та її зв'язок з науковими та практичними задачами. Ефективне керування процесом вибухового руйнування скельних гірських масивів є однією з найважливіших науково-технічних задач гірництва. Вирішення її забезпечує зменшення витрат як на проведення буропідривних робіт (БПР) в кар'єрі зокрема, так і на видобуток корисних копалин в цілому.