ЗАСОБИ УПРАВЛІННЯ ПЕРЕВАНТАЖЕННЯМИ І ПОЛІТИКИ ВІДКИДАННЯ ПАКЕТІВ

Вступ

Механізми запобігання перевантаженню і різні політики відкидання пакетів призначені на основі аналізу мережного трафіка відслідковувати вузькі місця в мережі і не допускати виникнення на цих ділянках перевантажень. В умовах перевантаження ці механізми забезпечують тільки пільгову обробку пріоритетного трафіка. Але на практиці часто виникає ситуація, що пакет, який тільки-но надійшов, необхідно поставити у чергу, що вже досягла свого максимального розміру. У результаті деякі пакети слід відкинути. У найпростішому випадку застосовується політика "відкидання хвоста" (tail drop), відповідно до якої відкидаються пакети, які тільки-но надійшли.

Однак політика "відкидання хвоста" призводить до виникнення ефекту глобальної синхронізації – одночасного (синхронного) перезапуску алгоритмів повільного старту множини ТСР-джерел. Крім небажаної зміни розмірів черги, цей ефект здатний також призвести до зростання джитера, затримки пакетів трафіка і зниження продуктивності всієї мережі. Більш ефективними є механізми превентивного управління перевантаженнями, до яких належать алгоритми RED і його модифікації WRED і DWRED.

1. Алгоритм довільного раннього виявлення RED

Алгоритм довільного раннього виявлення (Random Early Detection –RED) є алгоритмом активного управління чергою і має істотні переваги в порівнянні з традиційним механізмом "відкидання хвоста". Механізм RED використовує превентивний підхід до запобігання перевантаженню мережі та замість очікування фактичного переповнення черги, як при "відкиданні хвоста", RED починає відкидати пакети з ненульовою імовірністю, коли середній розмір черги перевищить певне мінімальне граничне значення. Імовірнісний підхід до відкидання пакетів дозволяє бути впевненими в тому, що механізм RED відкине пакети усього лише декількох довільно обраних потоків, тим самим дозволяючи уникнути ефекту глобальної синхронізації.

Механізм раннього довільного виявлення RED націлений на:

• мінімізацію джитера затримки пакетів шляхом контролю за середнім розміром черги;

• запобігання ефекту глобальної синхронізації ТСР-трафіка;

• забезпечення неупередженого обслуговування трафіка, що характеризується короткочасними сплесками;

• строге обмеження максимального середнього розміру черги (шляхом уведення максимального порога).

Головна мета механізму RED полягає в мінімізації середнього розміру черги, а виходить, і результуючої затримки пакетів трафіка.

У рамках механізму RED уводиться ряд параметрів:

* – мінімальне граничне значення розміру черги, при перевищенні якого чергою починається процес відкидання пакетів. Найменше значення, що рекомендується, пакетів;



* – максимальне граничне значення, при перевищенні якого відкидаються всі пакети, які тільки-но надійшли. Значення, що рекомендується, ;



* – це експонентний ваговий коефіцієнт, який бере участь в обчисленні середнього розміру черги і визначає відносний внесок попереднього середнього і поточного розміру черги (миттєвий розмір) у новий середній розмір черги, що обчислюється за формулою



, (1)



де рекомендоване значення =9;



* – знаменник граничної імовірності (mark probability denominator), який визначає імовірність відкидання пакетів при досягненні середнім розміром черги максимального граничного значення . У загальному випадку



, (2)



де рекомендоване значення =10.



При реалізації алгоритму RED у залежності від співвідношень середньої довжини черги і введених граничних значень можливі три ситуації (табл. 1). На рис. 1 наведений характерний для механізму RED графік залежності імовірності відкидання пакетів від середнього розміру черги .



Таблиця 1 – Дії механізму RED

|  |  |
| --- | --- |
| Умова | Дія |
| < | Пакети не відкидаються (=0). |
| << | Частина пакетів відкидається. Імовірність відкидання прямо пропорційна збільшенню середнього розміру черги від мінімального до максимального граничного значення ( змінюється від 0 до ). |
| > | Усі нові пакети відкидаються (=1). |



Рисунок 1 – Графік залежності імовірності відкидання пакетів ( ) для механізму RED



Якщо ж середній розмір черги досить невеликий і знаходиться нижче мінімального граничного значення, механізм RED не здатний забезпечити істотних переваги в порівнянні з традиційними механізмами управління чергами. З іншого боку, при затяжному періоді перевантаження мережі поведінка механізму RED, незважаючи на довгу чергу і високе максимальне граничне значення, аналогічна поведінці класичного механізму "відкидання хвоста". Отже, основне призначення механізму RED полягає в згладжуванні сплесків трафіка і попередженні тривалого перевантаження мережі за допомогою повідомлення джерел трафіка про необхідність зниження інтенсивності передачі інформації. Якщо джерела виявлять здатність до взаємодії й одночасно зменшать інтенсивність переданого трафіка, це допоможе запобігти перевантаженню мережі. У іншому випадку середній розмір черги досить скоро досягне максимального граничного значення, що призведе до відкидання всіх пакетів, які надходять.

Фактично механізм довільного раннього виявлення RED базується на обчисленні середнього розміру черги , що визначає припустимий рівень сплеску трафіку в черзі, та обчисленні імовірності відкидання пакетів , яка визначає частоту відкидання пакетів для заданого середнього розміру черги. Зверніть увагу, що при визначенні імовірності відкидання пакетів механізм RED обчислює не поточний, а експонентно зважений середній розмір черги (1). Використання механізмом RED середнього розміру черги обумовлено прагненням реагувати тільки на довготривале перевантаження мережі, а не на короткочасні сплески трафіка.



Під час розрахунку досить важливим є правильний вибір вагового коефіцієнта . Збільшення експонентного вагового коефіцієнта призведе до домінування попереднього середнього розміру черги над її поточним розміром в аспекті обчислення нового середнього розміру черги . Навпаки, зменшення експонентного вагового коефіцієнта приведе до зростання значущості поточного розміру черги при обчисленні її нового середнього розміру.



Нижче наведена формула для розрахунку експонентного вагового коефіцієнта:

, (3)



де В – смуга пропускання вихідного каналу передачі інформації в пакетах розміром MTU байтів.

Оскільки це не впливає на кінцевий результат, краще використовувати значення MTU, яке дорівнює 1500 байт, для всіх каналів передачі інформації навіть у тому випадку, якщо дійсне значення MTU дорівнює 4470 байт.

Наприклад, для каналу DS3 (45 Мбіт/с) В = (45 Мбіт/с / 8) / 1500 = 3750. Отже, експонентний ваговий коефіцієнт .



Мінімальне і максимальне граничні значення можна встановити рівними 0,03В и 0,1В відповідно. Знаменник граничної імовірності при цьому варто установити рівним 1.

У табл. 2 наведено рекомендовані значення параметрів механізму для ліній зв'язку DS1, DS3, ОСЗ і ОС12. При використанні механізму WRED ці значення є рекомендованими значеннями для трафіка IP-пріоритету 0.

Таблиця 2 – Рекомендовані значення параметрів механізму RED для різних ліній зв'язку

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Швидкість передачі в лінії зв'язку | Експонентний ваговий коефіцієнт | Мінімальне граничне значення | Максимальне граничнезначення | Знаменник граничної імовірності |
| DS1 | 4 | 4 | 13 | 1 |
| DS3 | 9 | 112 | 375 | 1 |
| ОСЗ | 10 | 388 | 1292 | 1 |
| ОС12 | 12 | 1550 | 5167 | 1 |

2. Зважений алгоритм довільного раннього виявлення WRED

Зважений алгоритм довільного раннього виявлення (Weighted Random Early Detection, WRED) є модифікацією алгоритму RED і надає різні рівні обслуговування на підставі значення поля IP-пріоритету. Це здійснюється шляхом настроювання окремо для кожного рівня пріоритету таких параметрів механізму RED як , , та, як результат, імовірності відкидання пакетів . Іншими словами, механізм WRED забезпечує більш інтенсивне відкидання низькопріоритетних пакетів і менш інтенсивне відкидання високопріоритетних. Стандартне мінімальне граничне значення для трафіка пріоритету 0 складає половину максимального граничного значення (рис. 2). Для порівняння на рис. 2 наведений також профіль WRED для трафіка з IP пріоритетом 3.



Рисунок 2 – Профілі WRED для трафіка з IP-пріоритетами 0 і 3

Значення параметрів WRED, що використовуються за замовчуванням у продуктах Cisco, наведені в табл. 3, 4. Зверніть увагу, що мінімальне граничне значення для високопріоритетного трафіка має бути більше, ніж мінімальне граничне значення для низькопріоритетного трафіка. Це необхідно для забезпечення строгої черговості відкидання пакетів, відповідно до якої першими відкидаються низькопріоритетні пакети.

Таблиця 3 – Профілі Cisco для WRED на основі пріоритетів, які використовуються за замовчуванням

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP-пріоритет | Мінімальне граничне  значення, | Максимальне граничне  значення, | Знаменник граничної імовірності, | Максимальний відсоток відкинутих пакетів, |
| 0 | 20 | 40 | 10 | 10% |
| 1 | 22 | 40 | 10 | 10% |
| 2 | 24 | 40 | 10 | 10% |
| 3 | 26 | 40 | 10 | 10% |
| 4 | 28 | 40 | 10 | 10% |
| 5 | 31 | 40 | 10 | 10% |
| 6 | 33 | 40 | 10 | 10% |
| 7 | 35 | 40 | 10 | 10% |
| RSVP | 37 | 40 | 10 | 10% |

Таблиця 4 – Профілі Cisco для WRED на основі DSCP, які використовуються за замовчуванням

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DSCP | Мінімальне граничне значення, | Максимальне граничне значення, | Знаменник граничної імовірності, | Максимальний відсоток відкинутих пакетів, |
| AF11, AF21, AF31, AF41 | 33 | 40 | 10 | 10% |
| AF12, AF22, AF32, AF42 | 28 | 40 | 10 | 10% |
| AF13, AF23, AF33, AF43 | 24 | 40 | 10 | 10% |
| EF | 37 | 40 | 10 | 10% |

Алгоритм WRED можна реалізувати як на центральному процесорі маршрутизатора, так і в розподіленому режимі. Коли алгоритм WRED виконується на центральному процесорі маршрутизатора, то він застосовується до вихідної черги інтерфейса, а граничні значення визначаються в так:

, ,



де – розмір вихідної черги утримання.



3. Алгоритм WRED на основі потоку (flow WRED)

Алгоритм WRED на основі потоку (flow WRED) є модифікацією алгоритму WRED, що передбачає штрафування потоків, які займають надмірну частку ресурсів. Це зв'язано з тим, що під час перевантаження мережі неадаптивні потоки (UDP-трафік) передають дані з набагато більшою інтенсивністю, ніж потоки, що володіють здатністю до адаптації (TCP-трафік). З метою забезпечення рівномірного обслуговування активних потоків трафіка механізм WRED класифікує усі пакети в черзі в залежності від їхнього пріоритету і потоку трафіка, до якого вони належать. Крім цього, WRED підтримує інформацію про стан всіх активних потоків (active flows), тобто потоків, хоча б один пакет яких поставлений на обробку в яку-небудь з черг. Інформація про стан активних потоків використовується для визначення справедливої частки виділених потокові ресурсів черги, а також для виявлення і штрафування потоків, що віднімають надмірно великий обсяг ресурсів. Щоб механізм WRED адекватніше реагував на сплески потоків трафіка, необхідно збільшити справедливу частку ресурсів для кожного потоку шляхом застосування так званого коефіцієнта масштабування. Справедлива частка ресурсів черги, яка виділяється активному -му потоку – без урахування коефіцієнта масштабування обчислюється як



, (4)



з урахуванням коефіцієнта масштабування



. (5)



Тут – розмір черги потоку ; – кількість активних потоків.



Потік, вимоги якого перевищують справедливу частку ресурсів з урахуванням коефіцієнта масштабування, штрафується шляхом збільшення ненульової імовірності відкидання для всіх нових пакетів цього потоку.

Як приклад розглянемо дії, що застосовуються механізмом WRED на основі потоку по відношенню до тільки-но поставленого в чергу пакета. При визначенні імовірності відкидання пакета механізм WRED на основі потоку враховує як значення поля IP-пріоритету пакета, так і інформацію про стан активних потоків. Від IP-пріоритету пакета залежать сконфігуровані (або стандартні) мінімальне і максимальне граничні значення. Якщо середній розмір черги нижче мінімального граничного значення , то імовірність відкидання пакета встановлюється рівною нулю (цей пакет не буде відкинутий). Якщо ж < <, то враховується інформація про стан активних потоків трафіка. Так, якщо пакет належить потокові, що перевищив справедливу частку ресурсів з урахуванням коефіцієнта масштабування, механізм WRED збільшує імовірність відкидання цього пакета шляхом зменшення відповідного максимального граничного значення:



. (6)



Ненульова імовірність відкидання пакета розраховується на підставі мінімального і нового максимального граничного значення. Оскільки результатом зниження максимального граничного значення є істотне збільшення кута нахилу кривої імовірності відкидання (рис. 3), шанси пакета бути відкинутим різко зростають.



Рисунок 3 – Графік імовірності відкидання пакета при використанні механізму WRED

Якщо ж потік трафіка не перевищує справедливої частки ресурсів з урахуванням коефіцієнта масштабування, то ненульова імовірність відкидання пакета розраховується за стандартним методом (2).

Коли середній розмір черги перевищує максимальне граничне значення >, механізм WRED на основі потоку відкидає всі пакети, призначені для постановки в чергу.



4. Механізм явного повідомлення про перевантаження ECN

Механізм явного повідомлення про перевантаження (Explicit Congestion Notification, ECN) замість відкидання пакета використовує відповідне маркування заголовка пакета. Для реалізації механізму явного повідомлення про перевантаження в заголовку IP-пакета виділяється спеціальне ECN-поле довжиною два біта (рис. 4).



Рисунок 4 – Заголовок IP-пакета (RFC 3168)

Установка джерелом ТСР-з'єднання біта ЕСТ (ECN-Capable Transport, транспортування даних з підтримкою поля ECN) вказує на здатність кінцевих пристроїв транспортного протоколу до інтерпретації поля ECN. Біт СЕ (Congestion Experienced – виявлена помилка) установлюється маршрутизатором з метою повідомлення кінцевих вузлів з'єднання про перевантаження мережі.

Приклад використання механізму ECN наведений на рис. 5. Для успішної роботи механізму ECN TCP-джерело і TCP-одержувач мають повідомити один одного про підтримку поля ECN. З цією метою TCP-джерело встановлює в заголовку пакета біти ECN у 01 (або 10) і передає пакет (крок 1 на рис. 5). Якщо TCP-джерело не підтримує механізм ECN, то відповідні біти будуть встановлені в нулі (ECN=00). Припустимо, на маршрутизаторі R1 з метою запобігання перевантажень використовується механізм WRED, і він випадково обрав саме цей переданий пакет для відкидання. Однак, знайшовши значення ECN=01, маршрутизатор не відкине пакет, а замінить значення поля ECN на 11 – сигнал про перевантаження – і передасть пакет далі (крок 2).

Пакет досягає TCP-одержувача (крок 3), де аналізується значення поля ECN. Значення ECN=11 сигналізує про наявність у мережі перевантаження в напрямку від TCP-джерела до TCP-одержувача, а значить про необхідність звуження TCP-джерелом розміру вікна перевантаження. TCP-одержувач повідомляє отриману інформацію про стан мережі шляхом установки в TCP-заголовку нового пакета спеціального прапорця явного виявлення перевантаження (Explicit Congestion Experienced, ECE) (крок 4). Відзначимо, що зміст бітів ECN на кроці 4 неважливий, тому що цей пакет використовується для повідомлення TCP-джерела про перевантаження і необхідність звуження розміру TCP-вікна. Даний пакет проходить через маршрутизатор (крок 5) і досягає TCP-джерела (крок 6), який у відповідь на прапорець ECE зменшує розмір вікна перевантаження (congestion window, CWND) у два рази. Для повідомлення TCP-одержувача про зміни розміру вікна в новому пакеті, що направляється до TCP-одержувача, встановлюється прапорець CWR (Congestion Window Reduced – розмір вікна зменшений) (крок 7).

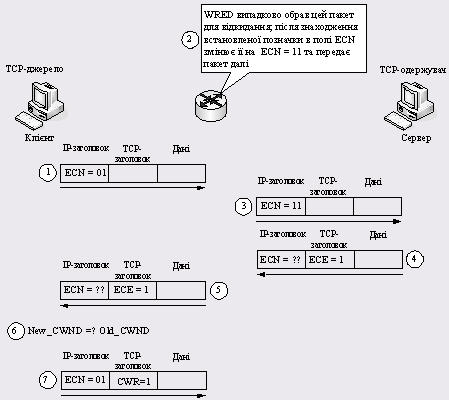


Рисунок 5 – Приклад використання механізму ECN для зменшення вікна перевантаження CWND

5. Механізм вибіркового відкидання пакетів SPD

трафік перевантаження синхронізація мережа

Механізм вибіркового відкидання пакетів (Selective Packet Discard, SPD) потрібний для відділення важливого управляючого трафіка мережі (наприклад, пакетів з відновленням інформації про маршрути) від іншого трафіка на рівні маршрутизатора. Механізм SPD допомагає маршрутизаторові підтримувати цілісність інформації про маршрути протоколів IGP і BGP під час перевантаження мережі шляхом пріоритетної обробки пакетів протоколів маршрутизації відносно пакетів іншого мережного трафіка.

Відповідно до механізму SPD до черги IP-процесу маршрутизатора застосовується вибіркова політика відкидання пакетів. Пакети трафіка, які потребують обробки у вхідній черзі IP-процесу, розділені на три групи:

• важливий управляючий трафік IP (пакети протоколу маршрутизації), який часто називається пріоритетним трафіком (priority traffic;

• звичайний IP-трафік (наприклад, пакети аплікацій telnet або ping), IP-пакети з альтернативами, а також будь-яке розширення або інкапсуляція IP, які не підтримуються механізмом прискореної комутації CEF;

• пакети, що необхідно відкинути.

До останньої групи належать IP-пакети, які за тих або інших обставин не пройшли тест на коректність, – пакети з невірною контрольною сумою, неправильною версією, з "часом життя" (Time-to-Live, TTL), що минув, невірним номером порту UDP/TCP, невірним значенням поля протоколу IP і т.д. При одержанні більшості з цих пакетів автоматично генерується ICMP-пакет (Internet Control Message Protocol – протокол управляючих повідомлень Internet) з метою повідомлення джерела про помилку. Невелика кількість ICMP-пакетів генерується деякими службовими програмами, такими, як traceroute. Слід зазначити, що великий обсяг ICMP-трафіку може бути частиною атаки зловмисників, що намагаються вивести з ладу маршрутизатор шляхом переповнення черги IP-процесу. Отже, стає очевидною необхідність вибіркового відкидання цих пакетів без утрати важливої управляючої інформації.

У рамках механізму SPD, аналогічно RED, уводяться параметри і – мінімальне і максимальне граничні значення завантаження черг відповідно. Від співвідношення величини поточної довжини вхідної черги і введених граничних значень залежить режим функціонування механізму SPD. У цілому механізм SPD може функціонувати в таких режимах:



• відключений (Disabled);

• нормальний режим функціонування (Normal): <, в якому пакети не відкидаються;



• режим випадкового відкидання пакетів (Random drop): < <, відкидаються всі IP-пакети, що належать звичайним потокам трафіку. Імовірність відкидання пакетів розраховується за формулою . Випадкові відкидання пакетів одержали назву SPD-скидань (SPD flush). Слід зазначити, що важливий управляючий трафік мережі як і раніше ставиться в чергу для обробки;



• режим тотального відкидання пакетів (Full drop): >, в якому механізм SPD відкидає всі пакети, що належать звичайним потокам трафіка. Важливий управляючий трафік усе ще ставиться на обробку в спеціальну пріоритетну чергу (priority queue), що обробляється перед усіма звичайними чергами IP-процесу;



• режим активного відкидання пакетів (Aggressive drop). Спеціальний режим, за якого відкидаються всі IP-пакети, що не пройшли перевірку на коректність. Відкидання некоректних пакетів відбувається, коли розмір вхідної черги перевищує мінімальне граничне значення ( >).



Усі режими функціонування механізму виборчого відкидання пакетів SPD схематично подані на рис. 6.



Рисунок 6 – Режими функціонування механізму SPD