ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПРОЦЕСІВ ВІДМОВОСТІЙКОВСТІ В ПРОГРАМНО-КОНФІГУРОВАНИХ СИСТЕМАХ

Алексін В.В.

Кафедра Інфокомунікаційної інженерії
ім. В.В. Поповського, ХНУРЕ, Україна.

E-mail: vladyslav.aleksin@nure.ua

Abstract

Complications in the field of telecommunications technology lead to the fact that more and more stringent requirements relate to the quality of network services, to the possibility of increasing them, to the quality of traffic processing, the volume of which continues to grow. IP routing has been provided with sufficient capabilities to address fault tolerance issues. Thus, it is possible to restore the data transmission route after virtually any failure of network elements. Possible solutions to failover problems are default gateway availability protocols and failover routing models based on flow models

Відомо, що фундаментом у забезпеченні заданих значень таких важливих показників якості обслуговування (Quality of Service, QoS), як середня затримка, джиттер, рівень втрат пакетів і швидкість їх передачі відводиться протоколам маршрутизації разом з протоколами захисту шлюзу за замовчуванням.

Найважливішими факторами, які є необхідними для успішної роботи відмовостійкої мережі:

- маршрутизація (вибір маршрута пакетів та його зміна вразі виникнення перешкод);
- захист елементів мережі від можливого перевантаження (превентивний та пост-фактум).

В основу IP маршрутизації було положено достатньо можливостей для рішення задач пов'язаних з проблемою відмовостійкості. Таким чином є можливість відновити маршрут передачі даних після, практично, будь-якої відмови мережевих елементів.

Однак на даний момент, немає жодної практичної реалізації маршрутизації, яка б мала змогу це зробити протягом прийнятого інтервалу часу, так як реконфігурація мережі може зайняти більше часу, ніж десяті частки секунди, які зазвичай є прийнятним для користувача інтервалом часу. Затримки викликані тим, що було здійснено недостатня кількість контрольних повідомлень і того факту, що завжди певне число мережевих вузлів повинно бути поінформовано про те, що стався збій в мережі, і ці вузли повинні зробити певні контрзаходи, для чого потрібен час. Незважаючі на те, що розрив з'єднання на кілька секунд є абсолютно прийнятним для з'єднання термінал - термінал, це істотно обмежує використання людиною існуючих IP мереж для зв'язку в режимі реального часу.

Важливо те, що основним джерелом погіршення якості обслуговування є перевантаження елементів мережі. На жаль, більшість протоколів маршрутизації забезпечують перерахунок маршрутів з періодом у десятки секунд та не забезпечують оперативного реагування на перевантаження мережі.

Тому для більш швидкого оперативного реагування на можливі відмови в обслуговуванні пакетів, які викликані перевантаженням каналів і чергами маршрутизаторів, все частіше використовуються засоби відмовостійкої маршрутизації, такі як Fast ReRoute, Fast IGP/BGP Convergence і т.д. При цьому дуже важливо, щоб маршрутний протокол задовольняв ряду важливих вимог: забезпечував реалізацію різних схем резервування ресурсів і елементів мережі: захист каналу,

вузла, маршруту, шлюзу; був адаптований під одно/багато шляхову стратегію маршрутизації, а також наряду з розрахунком самих маршрутів визначав порядок розподілу по них мережевого трафіка.

З точки зору базової архітектури IP-мереж все активне мережеве обладнання працює на канальному і мережевому рівнях моделі OSI, і саме вони визначають надійність і відмовостійкість телекомунікаційних мереж в цілому. На рис.1 приведена класифікаційна схема методів і протоколів забезпечення відмовостійкості телекомунікаційних мереж на різних мережевих рівнях:

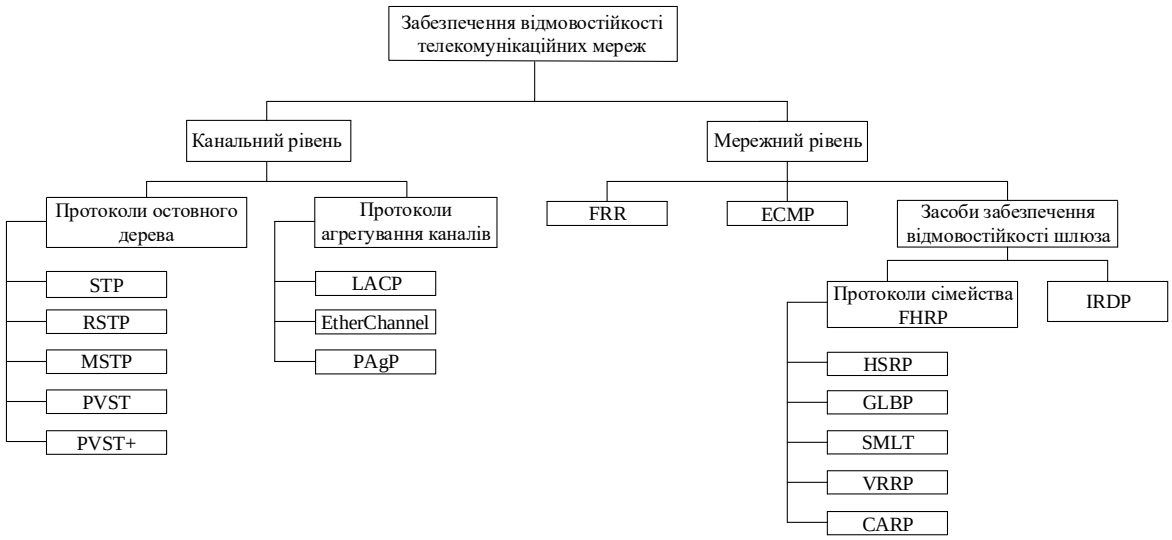

Рис. 1 – Класифікація протоколів, що забезпечують відмовостійкість телекомунікаційних мереж

Як видно з Рис.1, протоколи забезпечення відмовостійкості на канальному рівні діляться на дві великі групи - протоколи остовного дерева і протоколи агрегування каналів. Протоколи мережевого рівня в свою чергу діляться на протоколи, що забезпечують відмовостійкість шлюзу, ECMP і FRR. В рамках даної роботи необхідно детально розглянути протоколи сімейства FHRP та схеми захисту FRR, так як саме ці засоби підвищення відмовостійкості краще інших дають можливість найбільш якісно реалізувати та дослідити явище відмовостійкої маршрутизації разом з балансуванням навантаження та захистом шлюзу.

Протокол IRDP описаний в стандарті RFC 1256. Даний протокол реалізує алгоритм оповіщення клієнтів про присутність маршрутизатора в мережі самостійно або за запитом клієнтів. Таким чином, IRDP дозволяє клієнтам знаходити і призначати шлюзи, задані за замовчуванням. Мінус даного протоколу випливає з необхідності клієнтам самим призначати адреси шлюзів, отримані за допомогою даного протоколу, а також можливість їх динамічного перемикання, що передбачає необхідність його підтримки з боку клієнтів.

Протокол ECMP описаний в стандарті RFC 2992. Даний протокол працює з протоколами динамічної маршрутизації як внутрішнього (IGP), так і зовнішнього (EGP) шлюзу. Він дозволяє призначати в системі кілька рівнозначних маршрутів для передачі трафіку. Таким чином, ECMP дозволяє рівномірно розподілити потік даних через кілька мережевих з'єднань, а в разі відмови провести перемикання з непрацюючого маршруту на працюючий, забезпечуючи тим самим відмовостійкість на мережевому рівні. Швидка перемаршрутізація (Fast Re-Route, FRR) забезпечує відмовостійкість в MPLS-мережах шляхом побудови обхідного маршруту для трафіку, якщо виявляється проблема на робочому маршруті. Перемикання займає близько 50 мс. FRR використовує заздалегідь розраховані маршрути, тобто, маршрутизатора потрібно всього лише використовувати нову мітку і направити трафік на інший порт.

Принцип MPLS FRR заснований на тому, що якась проміжна топологія використовується як засіб резервування мережі. Недолік використання MPLS FRR полягає в тому, що алгоритм, що дозволяє обмежити тривалість операцій відновлення 50 мс, не є детерминистским: така операція відновлення має локальний характер, і, як тільки відбувається відмова, всій мережі може заново знадобитися перерахунок маршрутів, крім того для забезпечення додаткової відмовостійкості мережі будуть потрібні додаткові вельми дорогі порти маршрутизаторів IP / MPLS.

Розглянемо протоколи сімейства FHRP більш детально, саме ці протоколи забезпечують захист шлюза за замовчуванням.

Протоколи динамічної маршрутизації (RIP, OSPF, IS-IS, BGP і т.д.) по факту є протоколами, що забезпечують відмовостійкість на мережевому рівні, так як ці протоколи збільшують доступність мережі. Основне їхнє завдання – це передача пакетів по оптимальним маршрутом, а в разі відмови перейти на інший маршрут. Також для оптимізації роботи мережі на мережевому рівні можливе використання таких протоколів як Equal Cost Multi-Path (ECMP) і протоколів сімейства Frist Hop Redundancy Protocol (FHRP), які забезпечують балансування навантаження між декількома маршрутами в мережі і високу доступність шлюзів, заданих за замовчуванням, шляхом їх дублювання і спільної роботи, а також гарантують дуже швидке час відновлення в разі аварій.

Одним з найбільш ефективних способів підвищення надійності мережі є створення структур з дублюванням. На практиці використовується кілька різновидів схем дублювання: організація паралельних з'єднань, установка двох або більше центральних маршрутизаторів/комутаторів, побудова розподіленої магістралі.

На даний момент більшість великих ЛВС будуються за схемою з маршрутизаторами/L3-комутаторами в центрі, які виконують роль шлюзів, заданих за замовчуванням. У таких ЛВС зазвичай організовуються віртуальні мережі з маршрутизацією, передбачені надлишкові зв'язку між пристроями, встановлений резервний центральний комутатор.

В такому випадку на канальному рівні комп'ютерної мережі слабким місцем буде саме маршрутизатор / L3-комутатор. У разі виходу його з ладу можливо кілька варіантів розвитку подій, що вимагають втручання системного адміністратора: налаштування робочих станцій на роботу з іншим маршрутизатором в якості шлюзу за замовчуванням або установка додаткового маршрутизатора. Для збільшення відмовостійкості такої мережі використовують два шлюзу. Протоколи сімейства FHRP дозволяють забезпечувати клієнтів відмовостійким шлюзом.

Сенс роботи даних протоколів полягає в тому, щоб дозволити кільком мережевим пристроям використовувати один адрес (в загальному випадку - адрес шлюзу), забезпечуючи тим самим відмовостійкість для клієнтів.

Сімейство протоколів FHRP направлені на збільшення доступності шлюзу за замовчуванням і включає в себе такі протоколи:

1. Протокол маршрутизації «гарячого» резерву HSRP (Hot Standby Router Protocol) був розроблений компанією Cisco Systems. Протокол HSRP вирішує завдання доступності та відмовостійкості шлюзу, заданого за замовчуванням. Досягається це за рахунок використання у двох і більше маршрутизаторів або комутаторів третього рівня одної IP-адреси і MAC-адреси так званого віртуального маршрутизатора. Така група маршрутизаторів / L3-комутаторів називається HSRP-групою.

2. Протокол VRRP (Virtual Router Redundancy Protocol), як і решта протоколів сімейства FHRP призначений для збільшення доступності маршрутизаторів виконуючих роль шлюзу. Це досягається шляхом об'єднання групи маршрутизаторів в один віртуальний маршрутизатор та призначення їм загальної IP-адреси, яка і буде використовуватися як шлюз за замовчуванням для комп'ютерів в мережі.

3. Протокол GLBP (Gateway Load Balancing Protocol) працює аналогічно, але не ідентично іншим протоколам резервування шлюзу, таким як HSRP і VRRP. Ці протоколи дозволяють декільком маршрутизаторам брати участь у сконфігурованій віртуальній групі маршрутизаторів із загальною віртуальною IP-адресою. Один член групи вибирається активним маршрутизатором, в той час як інші залишаються неактивними доти, поки не відбудеться збій з активним маршрутизатором. При цьому ці резервні маршрутизатори володіють ресурсами, які майже не використовуються протягом усього часу експлуатації цієї системи. GLBP забезпечує розподіл навантаження на кілька маршрутизаторів використовуючи одну віртуальну IP-адресу та кілька віртуальних MAC-адресів. Кожний хост налаштований з однаковою віртуальною IP-адресою і всі маршрутизатори у віртуальній групі беруть участь у передачі пакетів. Маршрутизатори відправляють один одному повідомлення hello кожні 3 секунди.

4. Потокол CARP створювався командою OpenBSD як вільна альтернатива протоколам HSRP і VRRP. Протокол CARP (Common Address Redundancy Protocol) мережевий протокол, основним завданням якого є використання однієї IP-адреси кількома хостами в межах сегмента мережі. CARP є вільною, безпечною (в тій мірі, в якій взагалі можна говорити про безпеку протоколу ARP) альтернативою протоколам VRRP і HSRP. CARP дозволяє виділити групу хостів у тій частині мережі і призначити їй один IP-адреса. Така група називається «redundancy group» (група надмірності). В межах цієї групи один з вузлів стає «головним», а решта позначаються як «резервні». У кожен момент часу майстер-хост відповідає на ARP-запити до призначеного IP-адресою і обробляє трафік, що йде до цією адресою. Кожен хост одночасно може належати до декількох груп.

З усіх перерахованих протоколів особливої уваги слід надати протоколам GLBP та CARP, так як незважаючи на їх недоліки, саме вони мають найбільш можливостей рішення проблем пов' язаних з відмовостійкістю. Наприклад протокол GLBP, незваючи на те, що це пропрієтарни протокол компанії Cisco, саме цей протокол має можливість балансування навантаження без використання додаткових засобів. А протокол CARP в свою чергу є вільною альтернативою протоколам HSRP і VRRP і використовується UNIX-подібних системах. Зокрема на операційних системах Linux. А оскільки на даний момент адміністрування інтернет-мереж у великій мірі реалізується на операційних системах Linux, це найкращий варіант рішення проблем з відмовостійкістю для мережного обладнання будь-якого виробника, у різниці з пропрієтарними протоколами Cisco, але має слабкий рівень безпеки і не є сумісним з іншими існуючими стандартами.

Висновки

Таким чином на основі проведеного аналізу засобів забезпечення відмовостійкості можна зробити висновок про те, що найкращим рішенням проблем відмовостійкості в телекомунікаційних системах це використання протоколів збільшення доступності шлюзу за замовчуванням, які дають можливість разом зі схемами захисту FRR реалізувати відмовостійку маршрутизацію з балансуванням навантаження.

Література:

1. Лемешко А.В. Модель отказоустойчивой маршрутизации многоадресных и широковещательных потоков в MPLS-сети / А.В. Лемешко, К.М. Арус // Системи обробки інформації. – №9 (116). – 2013.

2. Лемешко А.В., Еременко А.С., Тарики Н., Арус К.М. Підвищення масштабованості і продуктивності рішень щодо відмовостійкої маршрутизації в телекомунікаційних мережах.// Системи обробки інформації. 2016. № 1(138). С. 152–156.

3. Гольдштейн А. Б. Технология и протоколы MPLS / А. Б. Гольдштейн, Б. С. Гольдштейн. – Санкт Петербург: БХВ, 2005. – 304 с.