Байлюк Є.М., асистент,
Поліщук О.А., асистент,
Житомирський державний технологічний університет

ПІДСИСТЕМА ДЗЕРКАЛЮВАННЯ ТРАФІКУ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Дзеркалювання трафіку (Traffic Mirroring) – це функція комунікаційного пристрою, яка забезпечує пересилку копій повідомлень з одного інтерфейсу пристрою на інший інтерфейс цього ж пристрою. Ця функція застосовується з метою моніторингу та аналізу трафіку при виконанні пошуку несправностей у мережі або з метою копіювання трафіку для аналізу системою виявлення вторгнень.

Дзеркалювання трафіку може здійснюватися на різних пристроях мережі – комутаторах, маршрутизаторах, пристроях захисту тощо. Дзеркалювання трафіку також може здійснюватися для повідомлень різних рівнів моделі OSI і для його виконання можуть застосовуватися різні засоби. Необхідно зазначити, що існує два варіанти забезпечення дзеркалювання трафіку:

– локальне дзеркалювання трафіку (Local Traffic Mirroring);
– віддалене дзеркалювання трафіку (Remote Traffic Mirroring).

Локальне дзеркалювання передбачає, що отримувач копій повідомлень підключений локально, до одного з інтерфейсів пристрою. Віддалене дзеркалювання передбачає, що отримувач копій повідомлень не має безпосереднього підключення до пристрою, а розміщений у мережі у межах досяжності[1].

Досить широко технології дзеркалювання трафіку застосовуються у мережах, що побудовані на основі комутаторів Ethernet. У цьому випадку застосовується загальна назва – дзеркалювання портів (Port Mirroring). Виробники обладнання застосовують як згадану загальну назву технології, так і вводять свої власні позначення. Наприклад, відомі виробники комутаторів Huawei, Juniper, D-Link, Brocade застосовують загальну назву – Port Mirroring, а фірма Cisco застосовує власну назву – Switched Port Analyzer (SPAN). Фірма 3Com (нині підрозділ Hewlett-Packard) свого часу також застосовувала власну назву технології – Roving Analysis Port (RAP).

Дзеркалювання портів у комутованих мережах може здійснюватися як локально, так і віддалено. Відповідно застосовуються такі позначення згаданих варіантів дзеркалювання:

– локальне дзеркалювання портів (Local Port Mirroring);
– віддалене дзеркалювання портів (Remote Port Mirroring).

На комутаторах Ethernet та деяких інших пристроях Cisco застосовується три різновиди технології дзеркалювання портів, а саме:

– локальне дзеркалювання портів (Local Switched Port Analyzer, Local SPAN або SPAN);
– віддалене дзеркалювання портів (Remote Switched Port Analyzer, Remote SPAN або RSPAN);
– інкапсульоване віддалене дзеркалювання портів (Encapsulated Remote Switched Port Analyzer, Encapsulated RSPAN або ERSPAN).

Для всіх зазначених вище технологій дзеркалювання введено загальні поняття:

– вхідний трафік (RX, Received/Ingress Traffic);
– вихідний трафік (TX, Transmitted/Egress Traffic);
– порт джерела трафіку (Source SPAN Port);
– порт призначення трафіку (Destination SPAN port).

Вхідний трафік – це сукупність кадрів, які поступають на вхідний блок порта комутатора Ethernet від підключеного до порта пристрою. Вихідний трафік– це сукупність кадрів, що передаються з вихідного блоку порта комутатора Ethernet до підключеного до порта пристрою. Порт джерела – порт комутатора, трафік якого буде дзеркалюватися. Для порта джерела може здійснюватися дзеркалювання тільки вхідного чи тільки вихідного трафіку та вхідного і вихідного трафіку одночасно. Порт призначення – порт комутатора, на який буде пересилатися трафік для дзеркалювання. Як правило, що цього порта підключається робоча станція, на якій встановлено додаток – аналізатор трафіку.

У кожної технології дзеркалювання портів є свої особливості та обмеження щодо застосування. Технологія SPAN передбачає, що порти джерела і призначення знаходяться на одному і тому ж комутаторі (або стеці комутаторів) і тегування (чи інкапсуляція) не застосовуються. Технологія RSPAN передбачає, що порти джерела і призначення можуть знаходиться на віддалених комутатора (або стеках комутаторів). Для функціонування цієї технології обов'язково створюється окрема VLAN (Remote SPAN VLAN), що застосовується для транспортування повідомлень. Виконується тегування трафіку і його передача здійснюється через транкові канали.

Технологія ERSPAN реалізовується лише на окремих, високопродуктивних моделях пристроїв Cisco. У цій технології передача трафіку здійснюється через наявну мережну L3-інфраструктуру. З цією метою передбачено застосування засобів не лише канального, а й мережного рівнів моделі OSI, зокрема, протоколу GRE (Generic Routing Encapsulation)[2].

Таким чином, організація дзеркалювання трафіку на комутаторах Ethernet фірми Cisco має свої особливості, пов'язані як з обмеженнями обладнання, так із необхідністю забезпечення функціонування комплексу взаємопов'язаних мережних протоколів.

Література

1. Barker, Keith. CCNA Security 640-554. Official Cert Guide / Keith Barker, Scott Morris.– Cisco Press, 2013. – 740 p.
2. Santos, Omar. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. – Cisco Press, 2015. – 658 p.