

I know What Your Packet Did Last Hop: Using Packet Histories to Troubleshoot Networks

Normalmente, as pessoas estão sempre por de trás de algum erro que acontece no sistema e cabe aos administradores de sistema fazerem *debug* dos problemas. Antigamente, o nível de complexidade da rede não era tão elevado como hoje em dia, ou seja já não é tão linear, não é possível fazer perguntas à rede de forma a obter respostas sobre o seu estado.

Os autores perante este problema criaram uma solução, o NetSight, através de uma noção chamado de histórico de pacotes (vista geral e onisciente da rede), em que cada pacote tem guardado em si informações sobre a rede (como, onde e o porquê, por exemplo, no caso de uma falha na rede) e que permite que as aplicações consigam facilmente aceder a esse mesmo histórico. Esta investigação visa mostrar a utilidade que a construção deste histórico tem no debugging dos dias de hoje. Para concretizar este estudo, foram contruídas quatro aplicações por cima do NetSight, o *ndb*, *netwatch*, *netshark* e *nprof*, para fazer debug da rede, monitorização, um log do histórico de pacotes e um perfil da rede hierárquico, respetivamente.

Eles tiveram de se preocupar com uma série de desafios, tais como, ter visibilidade de todos os caminhos de cada pacote, ter o estado de todos os *switches* pelos quais cada pacote passou, saber onde e quando cada pacote foi modificado, deve ser armazenado todo o histórico de *queries* e o processamento deve acompanhar o armazenamento. Para resolver a questão da visibilidade, foi introduzido o paradigma das SDN, em que existe um controlador centralizado, que fornece as regras de reencaminhamento e tem perspetiva geral sobre toda a rede, incluindo os caminhos existentes entre *switches*.

Em relação à arquitetura existe um coordenador central, que gere múltiplos servidores NetSight. O coordenador define a transmissão dos *postcards* dos *switches* para os servidores e recebe alterações nos estados de reencaminhamento do *control plane*. Também é responsável por coordenar os pedidos feitos através da API. Esta API é uma interface baseada em expressões regulares, usada pelas aplicações.

Para guardar o histórico, são usados *postcards*. Cada *postcard* contem um *header*, o ID do *switch*, os portos de saída e o número da versão do estado de reencaminhamento. Estes são criados aquando entram num *switch*, marcando-o com um estado relevante de informações, acima mencionadas, e é reencaminhado para um servidor NetSight. Após a geração dos *postcards*, estes são enviados para um servidor, colecionando todos os *postcards* respetivos a um único pacote. Tendo em conta que os *postcards* podem surgir de forma desordenada, em tempos diferentes, estes são guardados numa estrutura, *Path Table*, de forma a agrupar até todos terem sido recebidos. Esta ordem é identificada, através de um campo do *header*.

Dito pelos autores, existe o cPacket Networks, que basicamente não consegue identificar o estado da rede através de um único reencaminhamento. O OFRewind também usa SDNs na sua arquitetura e a utilização de *postcards*. O NetSight foi construído com base nestas ideias, porém com o acrescento da abstração do histórico de pacotes, o PHF(Packet History Filter) API. O NetSight, no geral, difere na motivação pelo qual foi construído, isto é, com o intuito de analisar uma rede, ao contrário das outras investigações que apenas queriam saber o destino dos pacotes ou em debugging por partes do *tenants* e não dos proprietários das infraestruturas.

A base desta investigação é bastante interessante, porque permite ter uma visão do que é que ocorre na rede. Porém, no nosso ponto de vista, poderá gerar mais tráfego, isto é para além dos pacotes que são enviados, são também transmitidos N postcards por cada pacote e caso o que é transmitido seja bastante grande poderá entupir a rede. É necessário que a rede esteja preparada para este tipo de transmissão, que se poderá tornar bastante pesada. As grandes vantagens passam realmente pelo o uso do PHF, que poderá ser bastante útil em clusters ou redes privadas, no sentido de ser possível de inserir os tais servidores NetSight e um coordenador (ou vários), afim de poderem analisar problemas.