DonRiver

Industry Insight

Network Analysis – Finding the Needle in the Haystack

Finding network anomalies is one of the biggest frustrations for CSPs – it can be like trying to find a needle in a haystack. Yet, provide the right tools, in this case a magnet, and the solution becomes more obvious. For CSPs, proactively monitoring the network with the right tools can reduce customer dissatisfaction, increase reputation and provide financial protection.

When the network deviates from normal patterns it causes anomalies in the network due to either a performance or a security issue. These are two of the main struggles for the CSP – service assurance and protection of both the network and the customer.

Customer service assurance

Around 80% of customer churn occurs because of CSP inability to quickly and effectively deal with issues. Customers do not always inform operators that they are experiencing network issues, which can be challenging, so CSPs must proactively analyze and tackle network problems.

Networks are becoming more complex as new technologies and services are introduced and the volume of traffic increases. With this level of complexity, identifying an anomaly in user or network patterns becomes challenging. Yet, it is expected the CSP offers service assurance even when faced with unexpected heavy flows of traffic.

Pre-emptive controls

Specific events such as sports or politics can see network traffic soar. CSPs need to account for this heavy flow and ensure network capacity and distribution is sufficient to serve the demand. Proactive management of network performance can enable CSPs to pre-empt issues where the network might stumble. Also, using historical network and performance data can assist with predicting the level of traffic required.

However, some unexpected events, such as terror threats, have seen unprecedented levels of traffic flooding networks that have suspended services. This is when the CSP must be quick to respond and identify changing patterns as they occur.

Faults need to also be quickly identified and fixed. With increasing competition, customers no longer wait to give operators a second chance – there are too many other temping offers out there and loyalty is low. Applications that constantly monitor network usage and performance are operationally critical, this is especially the case to spot security breaches.

Network security

In this digital world, we see many reports of hackers targeting companies to either steal personal / customer data or halt operations through attack or virus. Whatever the motive, CSPs must protect their systems and customer data to limit the financial threat.

Real-time monitoring of anomalies and service quality levels can enable CSPs to quickly identify issues and resolve them efficiently. Quick reaction is essential to limit the impact on both the CSP and the customer. Innovative OSS solutions can further generate in-depth analysis and informative reports, to visualize trends. This enables CSPs to take steps to learn from past events and plan for any future challenges.

With so much competition in the market, CSPs must ensure that service assurance underpins all operations (this includes SDN/NFV). The threat from both security and system complexity has never been so high. CSPs need to be constantly monitoring – analyzing and automatically pinpointing issues, as they happen to ensure financial stability.

Professional Insight: John McVey