IS YOUR NETWORK INFRASTRUCTURE 5G-READY?

Will 5G bring scalability challenges along with changes to networking architectures?

5G technology, with its speed 10 times faster than 4G LTE, can help businesses realise many long-held ambitions like real-time augmented reality (AR), virtual reality (VR), distributed machine learning within the Internet of Things (IoT), autonomous vehicles, smart cities, edge computing, etc. While 5G technology is imminent and likely to transform the pace of business operations, it will bring scalability challenges along with changes to networking architectures.

CHALLENGES THAT THIS CHANGE WILL INTRODUCE

Growth in technology leads to an increase in the number of transmitters and receivers required for effective connectivity, meaning a problem in any of these devices would not only affect connectivity, but also all other dependent processes.

SOFTWARE-DEFINED NETWORKING

Software-defined networking (SDN) controllers, which manage flow control for improved network management and application performance, will kick in to control network traffic as network dependency will be more software oriented than hardware oriented.

Many software-defined networks can track when and who makes changes, but businesses must carefully monitor who has access to the controller and keep access to it secure. Also, any configuration or programming error can result in the failure of SDN controllers, which will

> “The monitoring tool should ensure that the performance metrics of individual virtual network function (VNF) entities that relate to a service are associated correctly.”

lead to chaos in controlling traffic in networks and sub networks.

NETWORK FUNCTIONS VIRTUALISATION

With network functions virtualisation (NFV), common functions like routing, load balancing, and securing firewalls will be replaced on traditional network devices with virtual machines performing the same function.

As NFV environments are more dynamic than traditional ones, they require a complete overhaul of the existing processes, and both the traditional and virtual infrastructures should be managed simultaneously. Any down device, be it traditional or virtual, could inadvertently cripple the stability and functionality of a network.

SOLUTIONS FOR BUSINESSES TO EMBRACE

Major industries and business organisations follow the simple policy of monitoring everything in order to prevent any mishaps in their networks. To obtain a complete picture of what's happening in a network, an effective monitoring solution is indispensable.

In addition to monitoring key parameters like status, performance metrics, and traffic, the monitoring tool should also be equipped with new capabilities that can cope with 5G technology. With 5G, wireless wide area networks (WANs) could serve as a primary connectivity method, so measuring performance across these connections will become critical for enterprises to ensure effective integration of 5G networks. The tool should be capable of handling any bandwidth speed without compromising on performance.

NEED FOR A NETWORK MAP

The monitoring solution should also provide a network map of basic information that displays an overview of the whole network at a glance.

It should show the status of a network device and the actual traffic that flows through each device. Additionally, it should provide various performance metrics that will help track the overall performance of all devices in the network and should be quick enough to detect changes.

TACKLING SOFTWARE-DEFINED NETWORKING

The tool should have a tightly monitored security system so that access to the SDN controller is restricted. It should be able to efficiently back up the configuration and restore it when there is a failure in the SDN controllers.

> “Many software-defined networks can track when and who makes changes, but businesses must carefully monitor who has access to the controller and keep access to it secure.”

↑ Sivaramakrishnan M R, product consultant at Site24x7.

THE SOLUTION FOR NFV

The monitoring tool should also ensure that the performance metrics of individual virtual network function (VNF) entities that relate to a service are associated correctly.

For instance, the tool should be able to capture if a virtual domain name system (vDNS) is performing its functions correctly, and measure the request and response time taken by the vDNS.

NEED FOR AN ALERTING SYSTEM

Above all, the solution should send alerts when devices go down, when configured thresholds are breached, and when the configuration of any device changes along with the details of the network administrator who made the change.

Alerts should also be generated when the VNF association breaks, when there's a breach in the SDN controllers' security, or when the controllers fail. Last but not the least, the tool you choose should offer all these solutions in one place.

To sum up, a cloud-based, scalable monitoring solution that provides access to data from any location is imperative for businesses to manage any growing network successfully.