



Network modernization

Unlocking the full value of software-defined networking

Why make the change?

Grant Donald
Networking Technology Director, NTT

Digital transformation has and continues to dramatically change how IT services across all industries are being delivered to clients.

This transformation has added new technology, new types of endpoints, increased network traffic and driven more applications to the cloud. Increased performance and availability requirements, which are needed to remain competitive, continue to increase, while what is demanded of the network due to the proliferation of devices, increased traffic and cloud-based application growth continues to climb exponentially.

Increasingly, operations management faces pressure to reduce costs, while it struggles to keep up with business to:

- Accelerate innovation and extend CD/CI initiatives.
- Deliver an exceptional end-to-end user experience.
- Ensure consistency in meeting policy and security standards.

'Infrastructure-led disruption leads to business value. The days of risk-averse cultures are being swept away as I&O leaders recognize the value of speed and agility in managing new technology, new ways of working and cultural changes.'

Gartner Says Infrastructure-Led Disruption Will Drive Business Innovation

End-to-end software-defined network fabric, software-defined networking (SDN) and centralized network management

Software-defined networking (SDN) uses software to configure device-to-device networking. End-to-end software-defined network fabric adds artificial intelligence (AI) and machine learning (ML) capabilities that provide the automation to achieve greater efficiency and predictability in network operations administration and management. This creates optimal and automatic performance network configurations based on business intent and then develops customized networking baselines to define the optimal network state. These baselines are then used to monitor the network to identify network performance issues faster, provide continuous verification and automate corrective action where feasible.

By reducing the complexity of managing and enforcing network policies, the end-to-end software-defined network fabric provides a vendor-agnostic method to understand, monitor, configure and administer all devices and network interactions.

Is it worth the effort to change?

IT operations leaders must always consider the cost of any change in their operation against the value the change will deliver. The level of effort in changing procedures, modifying the operational environment and reskilling staff is always concerning and not without its own set of challenges.

Centralization of network management delivers immediate benefits that quickly justify any efforts to change and enable you to be ready for a future demanding ever-increasing agility, greater scale and higher performance. Many industry analysts believe that end-to-end software-defined network fabric will be a future necessity to manage and administer the network complexity associated with multiple public clouds, multiple campus environments and connectivity to an even broader array of IoT and edge devices.

The value of end-to-end software-defined network fabric with centralized network management

What is the value of an end-to-end software-defined network fabric with centralized network management? The implementation of this capability delivers improved quality of service, lowers operating costs and can take some of the complexity out of network management.

Lowers cost by improving operational efficiency

The end-to-end software-defined network fabric translates a business-aligned policy into a desired network state by using centralized network orchestration software to automatically implement policy-based configurations consistently across the network.

With this ability to monitor, identify and react in real-time to changing network conditions you gain enhanced agility and the ability to react more quickly without compromising risk exposure. Business aligned policies can be based on job roles, device function and application requirements. Intent-based policies are stated in terms of what the network should do rather than how it should be done. Intent-based policies can also include performance requirements such as availability and latency.

Manual methods to onboard devices, configure ports set-up and implement access control lists are no longer feasible. 70% of policy violations are due to human error. Policy violation introduces security risk and creates service issues. A recent industry survey reported that 80% of all service incidents are caused by planned and unplanned changes.

Network management simply can't keep up with the volume of change by continuing to add additional networking staff. Legacy centralized change management processes can't adequately respond to maintain the quality of service and respond to new users and network additions. Automating the deployment, monitoring, verification and remediation of policy configuration lowers costs by:

- Accelerating the policy activation and verification processes by automating network changes for thousands of devices.
- Reducing the human error associated with the traditional change and configuration deployment practices.
- Simplifying the process of adding and refreshing network resources.
- Capping or reducing the number of skilled staff required for network management.
- Improving the quality of service.

Network telemetry and end-to-end software-defined network fabric provide detailed visibility into the real-time user experience. Using machine learning and artificial intelligence, intent-based networking (IBN) systems can also determine the best way to implement the desired network state and can take automated corrective action to maintain it.

These advances:

- Improve optimization of network traffic flow.
- Lessen time to react to changes needed to deliver the LOS required to achieve the customer experiences expected.
- Reduce network noise and enable faster issue identification and resolution.

The end result is higher availability and improved network performance.

Reduced business risk through improved policy compliance

Security attacks are both more numerous and more sophisticated. Network weak points represent prime territory for infiltration. Endpoint devices including laptops, smartphones, cameras, sensors, machines, robots, meters and IoT devices continue unabated proliferation. Each of these devices presents a potential security threat if policies are not effectively and consistently applied and maintained.

Automation of policy deployment and continuous verification of compliance improves security from the edge to the cloud. Policy compliance helps to secure application traffic over the internet. End-to-end software-defined network fabric with centralized access control lowers the risk of unsecured elements or unauthorized users accessing the network.

Simplifies the complexity of network management

You are now able to treat the network as an integrated and consistent infrastructure. Growing demands can increase network complexity which together with the rapidity of change means it's essential to adopt a more dynamic approach to building, deploying and managing the entire environment.

With an end-to-end software-defined network fabric all users, devices and connected things are recognized automatically. The best network path to improve performance is automatically defined. Network availability is improved by lowering unplanned downtime.

Deployment and verification of policies across the network and all access points are assured and compliance maintained. Managing performance, achieving business SLAs and optimizing costs all become less challenging.

Realize the advantages

Overcome your network challenges today and prepare for an even more challenging future by adding end-to-end software-defined network fabric and centralized access to your software-defined network. Lower your operating costs, improve the efficiency of network administration and deliver higher levels of availability and performance.

‘Software-defined infrastructure is growing at 13% year-on-year. **Software provides commercial and operational flexibility,** while allowing for orchestrated and automated approaches to managing these environments.’

NTT Network Insights Report

Take the next step

When you need a partner to enable you to capitalize on your planned investments, we can help you accelerate your journey to software-defined. We have the experience and global resources to support your transition to a new operational model designed to maximize the performance of your new and existing assets.

We can help you implement a roadmap to a software-defined network designed to deliver the full value of your investment. Technology transformation calls for operational change – you can now enhance your support model with services designed specifically to realize the benefits of your new technology. Our SDI Lifecycle Services provide the visibility and control you need to ensure your software is as consistently managed as your legacy hardware.

