Automating the WAN for digital defense modernization

Pairing the power of IP/MPLS and network automation in the era of disruptive innovation

White paper

A confluence of technology shifts is placing immense strain on the defense network infrastructure. Along with the advent of innovative technologies such as 5G, cloud, AI, and drones as well as the adoption of the network-centric warfare doctrine, we are also seeing an end to support for widely deployed low-speed TDM transport technology. Defense forces need to modernize their WAN to move data at speed and scale for competitive advantage and increased efficiency. While IP/MPLS is the obvious choice with its resiliency, multiservice support and rich QoS to provide secure communications, the WAN needs to harness the power of automation for high network agility and efficiency as Defense adopts new innovations. This paper discusses the use cases and benefits of introducing network automation in defense WANs.

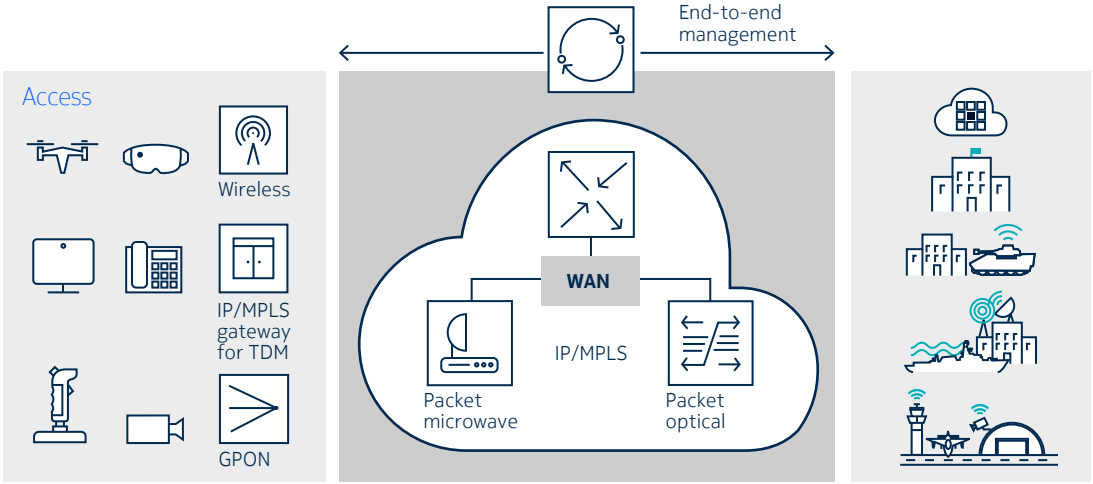
Contents

Today's defense networks

Defense forces are innovating to strengthen their technical capabilities and increase their efficiency. The wide area network (WAN) is the digital cornerstone to carry out these transformative initiatives. It is essential to connect defense personnel, machines, applications and services wherever they are — headquarters, command centers, mobile combat enclaves, and facilities including base, post, camp and station, data centers, as well as federal partners and coalition partners. WAN connectivity enables the right information to be transmitted, analyzed and shared with the right people at the right time.

The WAN is a multi-layer secure network (see figure 1). It comprises IP/MPLS for multiservice, which is carried over optical and microwave packet transport, and connects to various access domains via wireless and fiber access systems. Legacy TDM applications use IP/MPLS gateways to access the multiservice network. The network achieves secure communications using defense-in-depth security capabilities to safeguard network traffic and connected systems.[1]

Figure 1. Defense IP/MPLS WAN reference blueprint



Playing such a critical role, the defense IP/MPLS WAN needs to be built with strong resiliency, multiservice capabilities, deterministic quality of service (QoS) and robust cyber security.

Strong resiliency — Network outages cause communications disruptions that can have grave consequences, including failed missions or even casualties. IP/MPLS offers comprehensive redundancy protection at the nodal level (non-stop routing), link level (FRR and secondary LSP) and end-to-end (pseudowire-redundancy and BGP FRR), which brings the utmost resiliency to the WAN so that the traffic can be restored, even in multi-fault scenarios, as long as there is still a physical connectivity.

Multiservice capability — In addition to legacy TDM applications, the defense WAN needs to support new IP-based applications (voice, video and big data) with segregated VPN services

Deterministic QoS — With a large number of applications contending for bandwidth, the network needs strong and flexible traffic management capabilities to constantly deliver data with stringent QoS for each application, including TDM-based applications that have stringent delay and jitter requirements.

1 For more details on network security capabilities, please download http://resources.nokia.com/asset/194791

Robust cyber security — As the level and sophistication of malicious cyber activities continue to rise, cyber security is a top priority, even for unclassified day-to-day business operations. The WAN security capabilities can be integrated into the security framework as the first line of defense for system confidentiality, integrity and availability.

Evolving challenges for defense WAN

Defense operations are embracing ICT innovations like 5G, cloud and AI with full force. This requires high network agility and cross-layer (IP/MPLS and transport) management to meet daily operational requirements.

Moreover, defense missions still depend on applications using low speed TDM transport technology. With TDM equipment moving from end-of-life to end-of-support, it becomes more pressing to gracefully migrate these TDM circuits to IP/MPLS WANs, which can provide the same service availability as previously but on a fully supported platform.

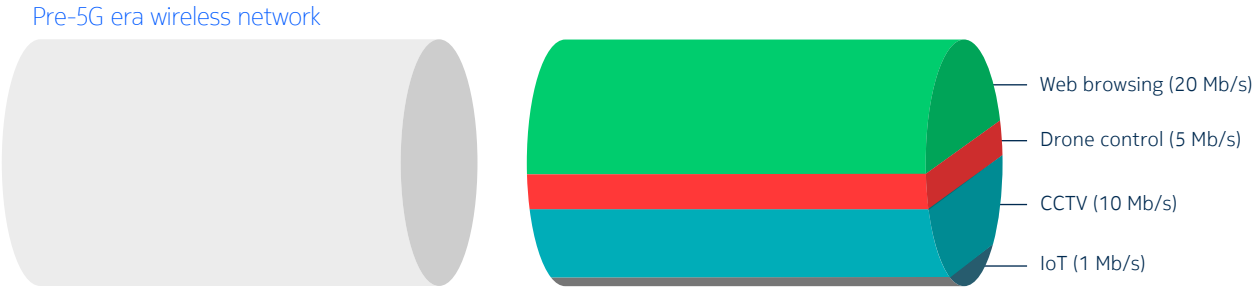
5G adoption requires unprecedented WAN network agility

5G is a game-changing technology[2] with the capacity to fully replace wired systems. Its innovative network slicing capability makes it possible for a shared wireless network to offer multiple services while meeting stringent quality of service requirements such as bandwidth and deterministic delay depending on the service.

A 5G network slice (see figure 2) is a virtual network partition that contains dedicated resources to support a specified set of services, applications or users with different QoS or security levels. For example, drone control requires stringent latency parameters while web browsing is very delay tolerant.

The 5G network slicing capability opens up the possibility of a new service paradigm where, as missions are launched and completed, it is possible to dynamically connect and disconnect users and devices. For example, a new 5G slice might be needed on short notice for a drone mission exercise. Ideally, it could be made available on demand, however, provisioning an IP/MPLS VPN today that could support the end-to-end 5G slice takes hours or even days. It also requires deep network expertise.

Figure 2. 5G brings in network slicing capability



2 For more 5G information, please download the e-book resource

Cross-layer management

The IP/MPLS WAN runs on a packet transport layer that typically uses microwave transmission at the edge and optical transport in the core. The traditional approach has been to manage them as separate layers.

However, with each layer treated as a separate domain, any network activities require intensive manual co-ordination efforts between them. This takes time, hampering operations speed, and is prone to manual errors. As the WAN network expands and scales out to meet user demands, the co-ordination efforts required continue to increase.

Newer IP/MPLS routers integrate the packet microwave functionality, thus eliminating the packet microwave network element. This means that they are managed as one node (or single network element in networking terms), making cross-layer management with microwave transport less of a challenge. However, operators today still traditionally manage IP/MPLS and optical layers as two siloes.

With the adoption of cloud computing, AI, 5G, IoT and big data, the challenges are only increasing as more nodes with larger capacity are deployed to move data between data centers. Some of the common operations challenges include multi-layer topology discovery and path diversity analysis. These hinder network operations and affect service velocity and reliability.

TDM migration and operations

While TDM network equipment has passed end-of-life and is entering into end-of-support, a significant number of critical applications and end devices still require low speed TDM technology such as RS-232 serial interfaces. Although new generation IP/MPLS service routers support TDM interfaces, the pool of TDM experts is dwindling. It is becoming more challenging to carry out TDM circuit migration to IP/MPLS and operate those TDM circuits afterwards.

Automate the network

Network automation capitalizes on network programmability to do more with the network and resources. It can deliver services faster with higher resource utilization, and at the same time improve operational simplicity with greater network visualization.[3] The rest of this paper will discuss common use cases in more detail and how network automation can help operators meet the three evolving challenges discussed in the previous section.

Automated transport slicing for maximal 5G operational flexibility

A 5G network comprises three domains (figure 3):

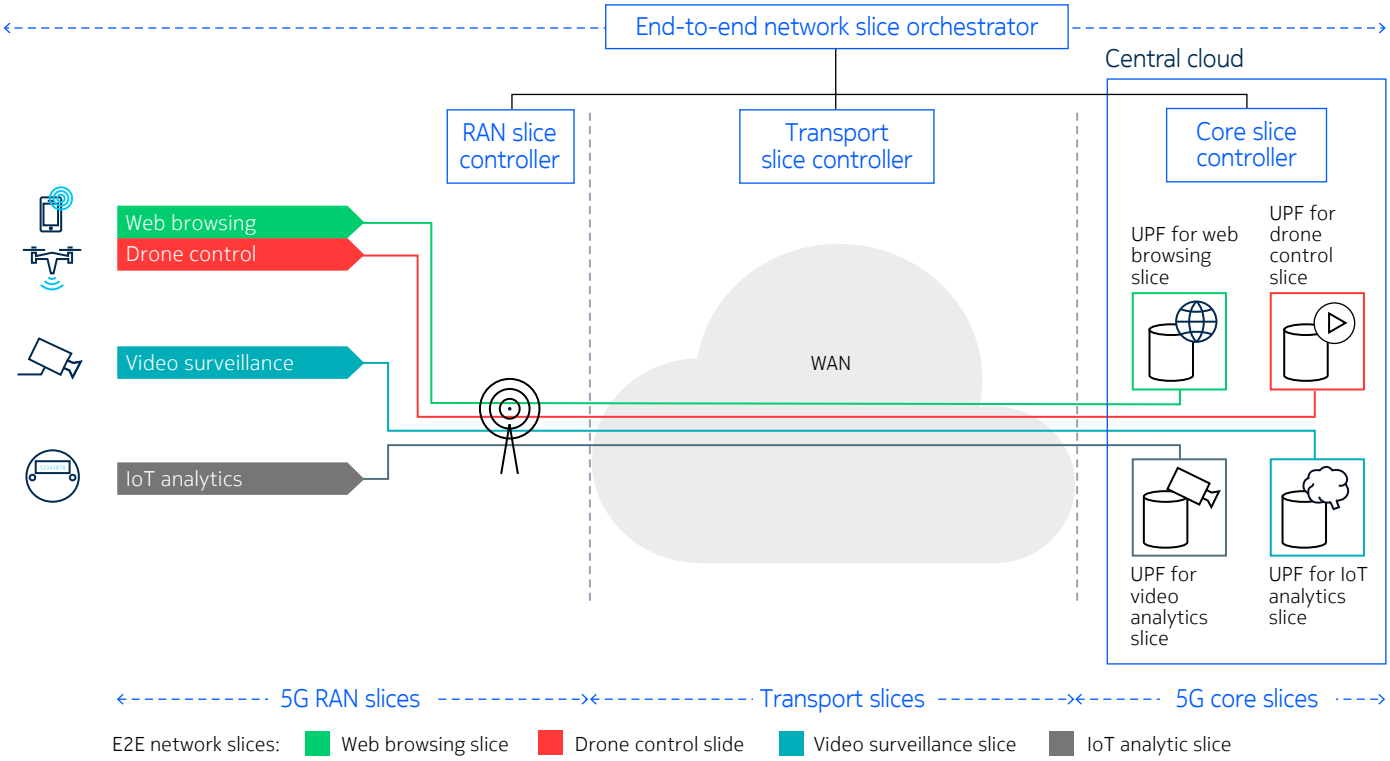
1. A 5G radio access network (RAN) slice connecting to wireless users and devices
2. A 5G core connecting RAN traffic to applications in data centers or the internet
3. A transport network connecting the RAN and the core.

Creating a 5G network slice requires orchestrating the provisioning of a slice in each of these three domains and seamlessly interconnecting them. This is an immense task if left to be done manually. Therefore, it is necessary to automate orchestration across all three domains to rapidly deliver, optimize and assure 5G services with rapid turn up of 5G slices. This can be accomplished with an end-to-end network slice orchestrator (abbreviated as the orchestrator hereafter), orchestrating the controller in each of these three domains.[4]

3 To learn more about network automation, read paper Network Automation and Programmability

4 For more details on transport slicing, please read paper Transport slicing in private 5G networks

Figure 3. End-to-end 5G network slicing

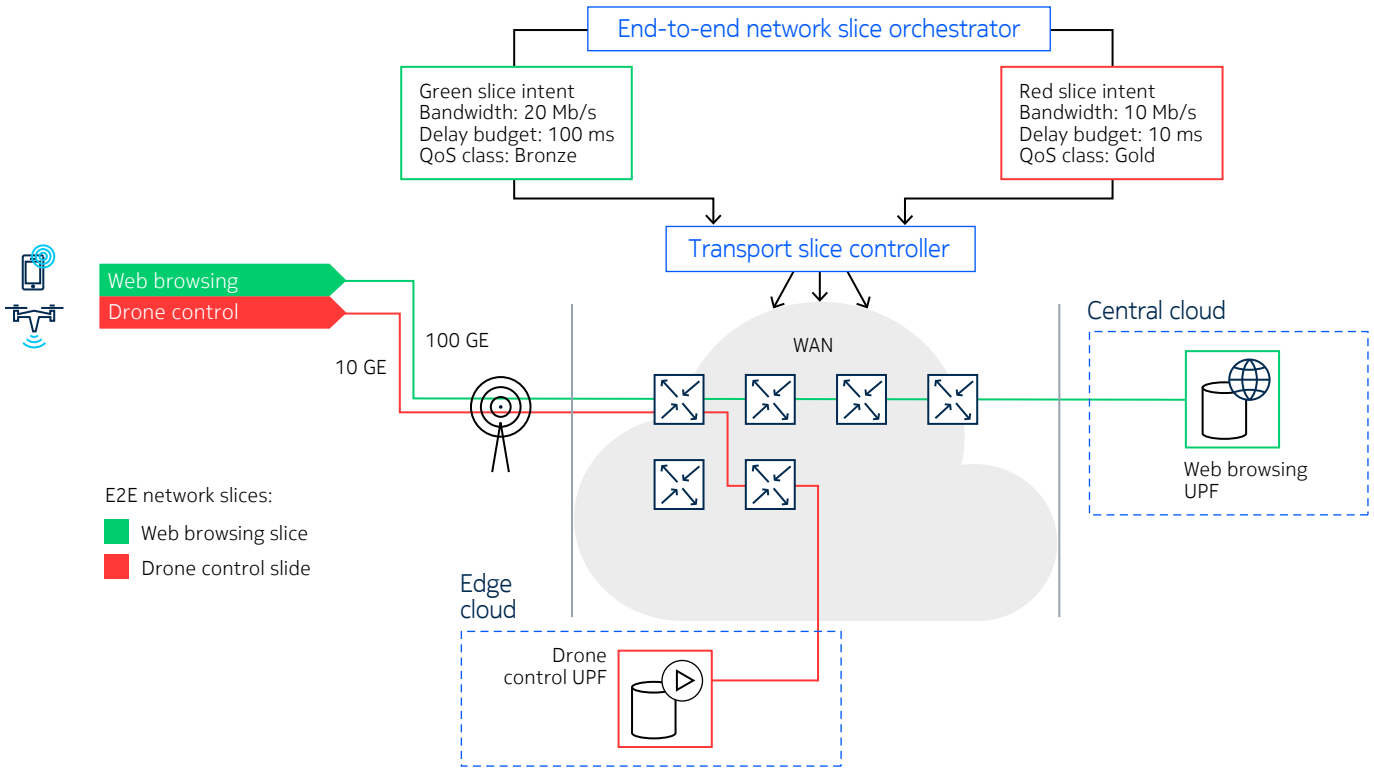


The IP/MPLS WAN is an integral component of the 5G system, playing the foundational role of 5G transport. Therefore, the IP/MPLS WAN network needs to support transport slicing with the WAN network manager playing the role of transport slice controller. Taking advantage of software-defined networking (SDN) technology and network automation, the WAN becomes programmable by the network manager. The network manager has a northbound API enabling the orchestrator to order the provisioning of a transport slice. The orchestrator provides the service requirements (also known as service intent) including RAN and core endpoints, as well as transport QoS requirements to the WAN manager. It uses its intent-based network automation capability to build a custom transport slice that can meet the QoS requirements. Since this process requires neither human planning nor intervention, it significantly accelerates the provisioning speed and eliminates human errors.

For example, users need two 5G slices to be provisioned to support a military drone exercise: one for regular web browsing to access data and another for drone control. Web browsing can be bandwidth intensive but is insensitive to latency, while drone control only needs moderate bandwidth but is sensitive to delay. Therefore, the service intent for the web browsing slice is to optimize for bandwidth while, for drone control, it is to minimize delay.

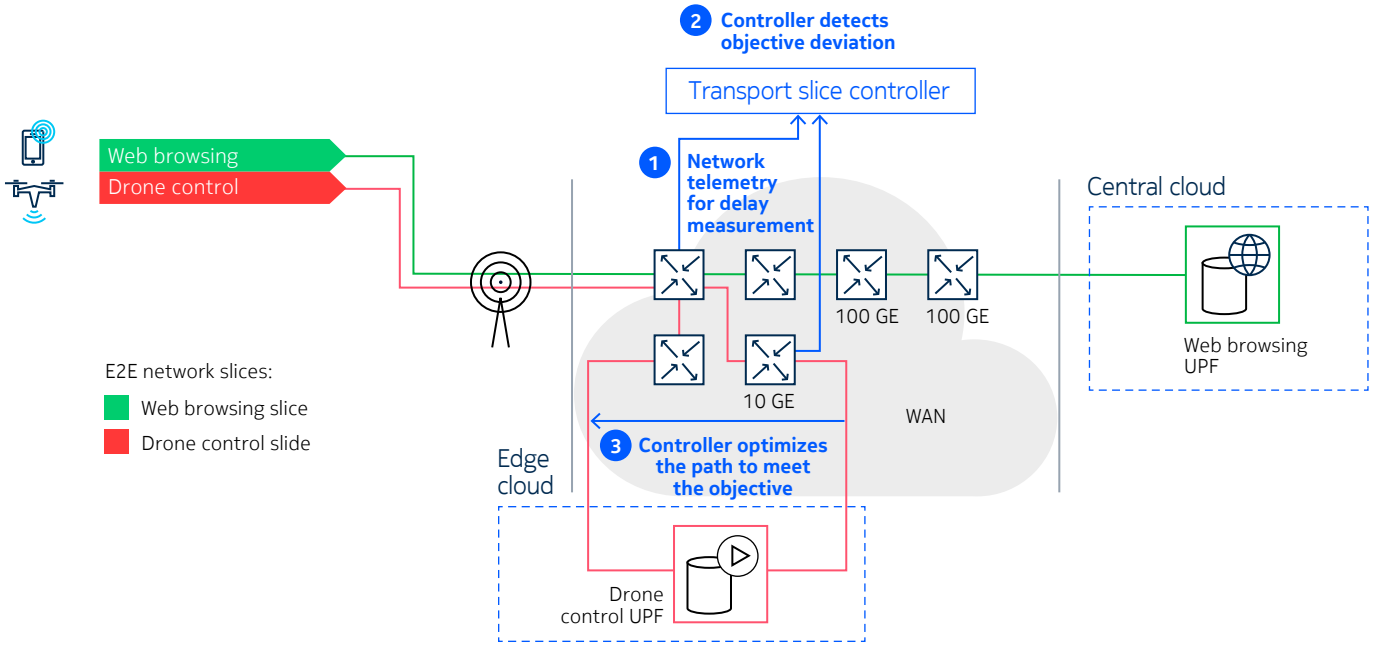
Based on this intent information, the WAN manager will allocate the necessary network resources to build two separate slices (green and red) in the WAN (figure 4). The green slice uses a multi-hop 100 Gbps trunk connecting the RAN and the core to establish a path dedicated for web browsing during the drill. The red slice has only one hop for minimal delay while meeting the required bandwidth for drone control. Note that the drone control UPF is located nearer to the drone exercise to minimize delay.

Figure 4. Intent-based automated transport slice provisioning



As 5G user traffic is dynamic and changes in real time, the transport network needs to be responsive to constantly meet the QoS objectives. The WAN manager continually collects telemetry data for network statistics and OAM results such as delay. It then proactively monitors the delay performance and optimizes the path in the WAN if the performance falls short of the objective (figure 5). This closed-loop mechanism of service assurance and optimization ensures constant high application performance, particularly for delay-sensitive application such as drone control.

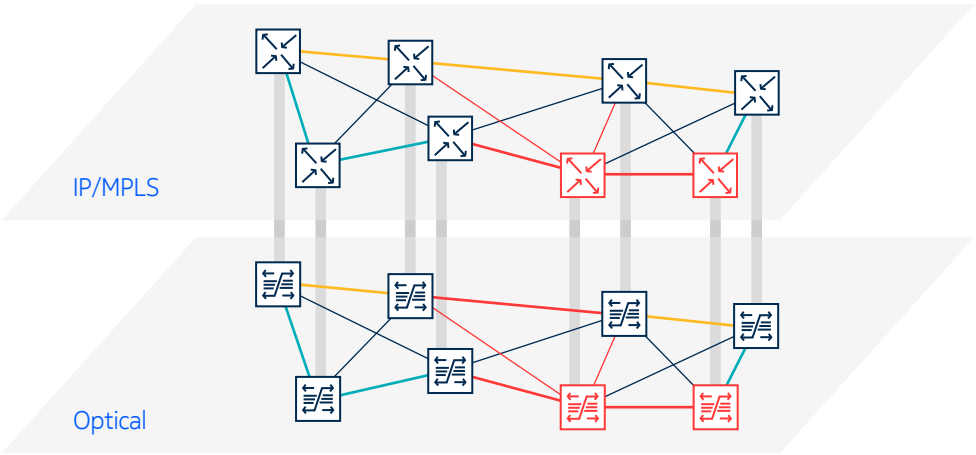
Figure 5. Automated assurance and optimization in 5G transport network



Automated IP/optical multi-layer management for resilient services

Managing a multi-layer IP/optical WAN (figure 6) using disjoint network managers and ad-hoc tools is a daunting challenge since information about each layer is stored and managed in its own silo with no coordination.

Figure 6. A multi-layer IP/optical WAN blueprint



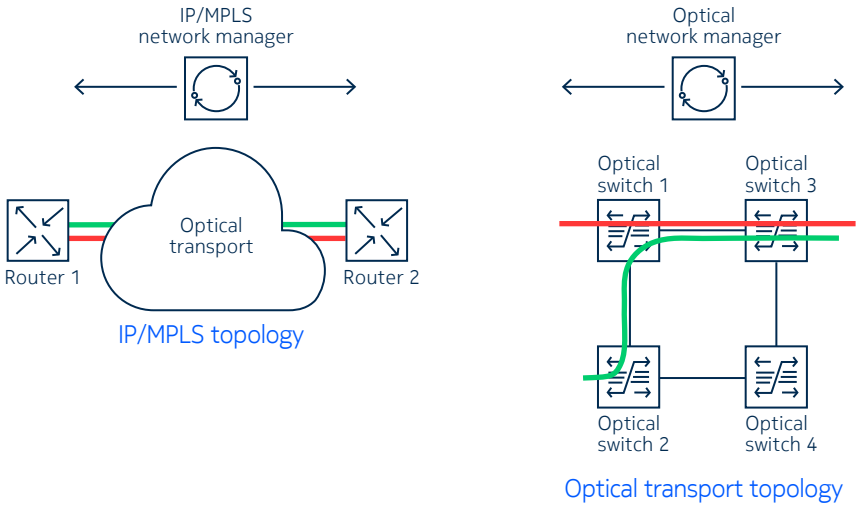
Leveraging the network automation capabilities of a unified network manager to exercise cross-domain control with cross-layer coordination, we can remove these barriers and significantly improve network operation efficiency and service reliability.[5]

5 To learn the full coordination capability, read solution sheet IP Optical Multi-layer and Cross-Domain Coordination

Automated multi-layer typology detection

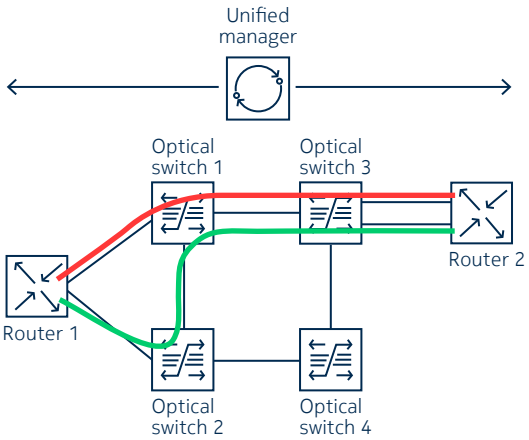
One of the highlights of this approach is that the present mode of operation only provides network operators an isolated view of the IP/MPLS and optical topologies (figure 7). Typically, IP/MPLS routers are connected to each other via the optical transport layer. As a result, operators need a lot of manual effort to identify and visualize the end-to-end paths between two peering routers that traverse the optical layer.

Figure 7. Disjoint IP and optical layer topologies



Network automation with a cross-domain network manager provides an intuitive visualization of the multi-layer topology by leveraging protocols such as LLDP snooping. It can also compare traffic counts to gather cross-layer connection information to build out a full multi-layer topology (figure 8). This provides full visualization of both IP and optical topologies in a fully correlated way.

Figure 8. Auto-discovered multi-layer topology with a unified network manager

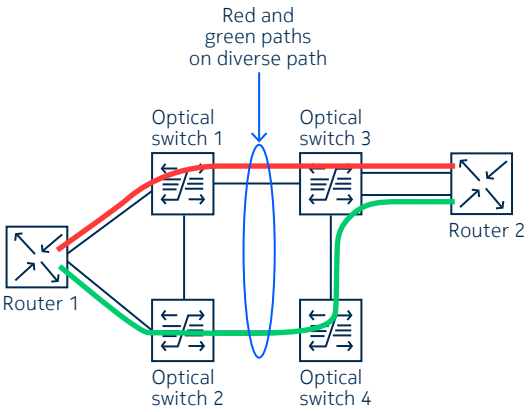


Analysis of multi-layer path diversity

Another highlight of this approach is the ability to analyze IP/MPLS path diversity, which is pivotal to reliable service delivery. In the example in figure 6, Router 1 appears to have diverse routes to reaching Router 2 through the red and green paths. However, the two paths are not really diverse as they share the same fiber trunk between Optical Switch 1 and 3. Should a fiber cut occur there, both paths will be affected. Router 1 would lose connectivity to Router 2 despite the dual-homing network architecture. With disjoint IP/MPLS and optical topology information in a disjoint management paradigm (figure 5), the operator is challenged to evaluate the shared risk of what appears to be diverse paths in the network.

Network automation can perform path diversity analysis to detect the shared risk. The multi-layer network manager can re-reroute the green path through Optical Switch 4 to offer true path diversity, thereby improving service reliability (figure 9).

Figure 9. Diverse path restoration



Service automation for graceful TDM migration

TDM-based legacy applications still play a pivotal role in the success of many missions. However, even with the extensive TDM support present in new IP/MPLS routers,[6] as the pool of TDM expertise is dwindling, it becomes challenging to gracefully carry out TDM migration and proficiently operate TDM services afterwards.[7]

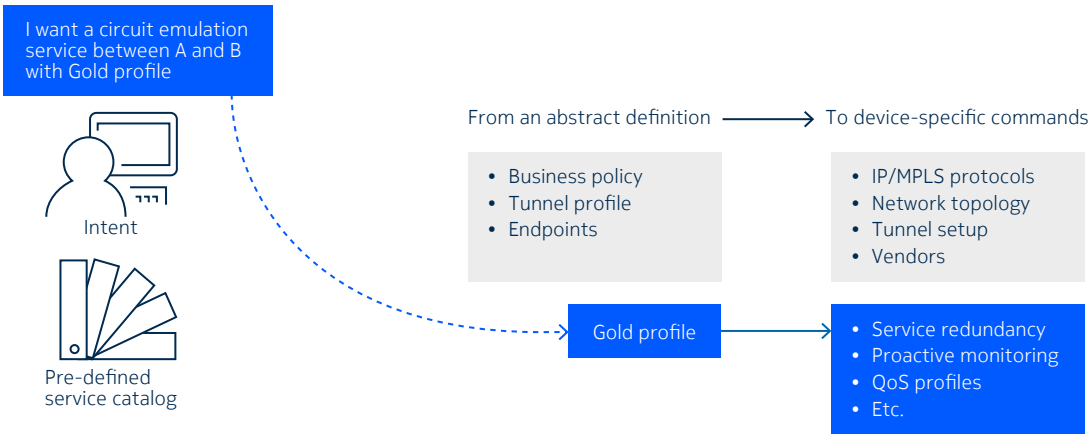
Network automation offers an opportunity to deliver network services in an abstracted manner, hiding the technology complexities from operators. Service requirements are expressed in simple terms as the "intent" or input from the users. Service automation then fulfills the service by translating the intent into network configurations, essentially, router-specific commands that comply with both the business policy and service intents (see figure 10).

The network manager also computes and establishes, if necessary, a network path connecting the two service endpoints. This paradigm, also known as intent-based networking, hides the TDM technology complexities as well as eliminating network and traffic engineering efforts and allowing operators to confidently carry out the TDM migration.

6 For details of legacy interface support on IP/MPLS routers, please download 7705 SAR Adapter Cards datasheet

7 For discussion of TDM migration, please read paper Migrating from SDH/SONET Networks to IP/MPLS Networks

Figure10. Service automation with intent-based networking



After successful migration, circuit emulation services require continuous circuit monitoring to ensure that TDM packets are reliably delivered. Packet loss and network jitter result in performance degradation. Network analytics can automate the monitoring of key TDM circuit parameters such as network delay and jitter buffer depth at TDM endpoints. Alarms can be raised when the measurement crosses a pre-configured threshold. This allows operators to take remedial measures, either in automated or manual manner, before the TDM circuits experience service degradation.

Conclusion

As defense forces modernize to strengthen C3 and embrace cloud and AI for data-informed, data-driven decisions, the WAN is critical for the transport of data at speed and scale. It is imperative, therefore, that the WAN continues to transform, harnessing the power of network automation to build an agile and adaptive network.

A successful network transformation rests not only on adopting technology. Network design expertise and professional services are equally important. With its comprehensive and innovative product portfolio that spans IP/MPLS, packet optical and microwave transport, data center fabric, network automation and 5G, Nokia can assist defense organizations to build networks that help protect national security and defend allies and partners.

Click here to find out more about Nokia solutions for defense.

Abbreviations

API	Application programming interface
C3	Command, control and communications
IBN	Intent-based Networking
ICT	Information and communications technology
LSP	Label-switched path
MAC	Media access control
MPLS	Multiprotocol label switching
NGE	Network group encryption
OAM	Operations, administration and maintenance
PPP	Point-to-point protocol
QoS	Quality of service
R-VPLS	Routed VPLS
SDH	Synchronous digital hierarchy
SONET	Synchronous optical network
STP	Spanning tree protocol
TDM	Time-division multiplexing
TWAMP	Two-way active measurement protocol
VCCV	Virtual circuit connectivity verification
VLAN	Virtual LAN
VLL	Virtual leased line
VPLS	Virtual private LAN service
VPN	Virtual private network
VPRN	Virtual private routed network
VPWS	Virtual private wire service
VRF	Virtual routing and forwarding
WDM	Wavelength division multiplexing

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2023 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID210211 (February)