

The Evolution of Government Networks

Enabling government digital service delivery

Networks, networks everywhere

The UK Government has built a host of telecom networks—from large national networks like JANET and N3 spine to local networks built by district councils and blue light services. Often, these networks are closed architectures developed for specific applications and around a specific vendor solution. Closed architectures mean networks cannot communicate with one another, and needed data is often stuck behind a wall—creating many islands that require application-specific interconnection to support specific services. Additionally, many networks are designed with proprietary vendor equipment that does not enable a multi-vendor infrastructure. This ‘vendor lock-in’ complicates creating a multi-vendor environment, as it requires specialized adapter development or equipment change-out.

This set of problems has left a legacy of sparsely interconnected and highly duplicated networks—hampering initiatives to digitize and improve government services. This complex system of purpose-based networks makes delivering simple services or cross-departmental project coordination slow and painful. New projects often run over cost and under-deliver functionality due to the complexity of integrating into legacy architectures.

Governments today need to leverage new technologies to implement innovative programs faster, improve service delivery, and ensure data privacy and security. End-users need easier access to information, more self-service capabilities, and faster service delivery. Can a current network built using these fraught models get there from here? Yes, but not by doing what has been done in the past.

Identifying the right problem to solve

The problem is not distance. There are plenty of existing networks covering plenty of UK kilometers—from Aberdeen to Exeter, Swansea to Dover. Protocols—or rather, the standards and hardware with which each network is built—are not the problem, either.

The problem to solve is the interconnectivity of existing networks that enables service orchestration. In the same way an orchestral conductor does not tell the violists where to place their fingers or the pianist when to press the pedals, a network orchestrator asks the individual networks for a connection or for a function, but then leaves the specifics of the work to the network. A network orchestrator allows hierarchy and abstraction—hiding details from the end-to-end service. This enables each network to do what it is good at, and the orchestrator to bring it all together.

Network orchestration in action

Imagine it is mid-January. Several million people have yet to start their tax returns. What if you could spin up some servers in the G-Cloud and reserve bandwidth to the peering points of the ISPs with a single action? Then, in mid-February with another single action, move it all over to DVLA to cope with the flurry of new car registrations when ‘17’ reg comes around?

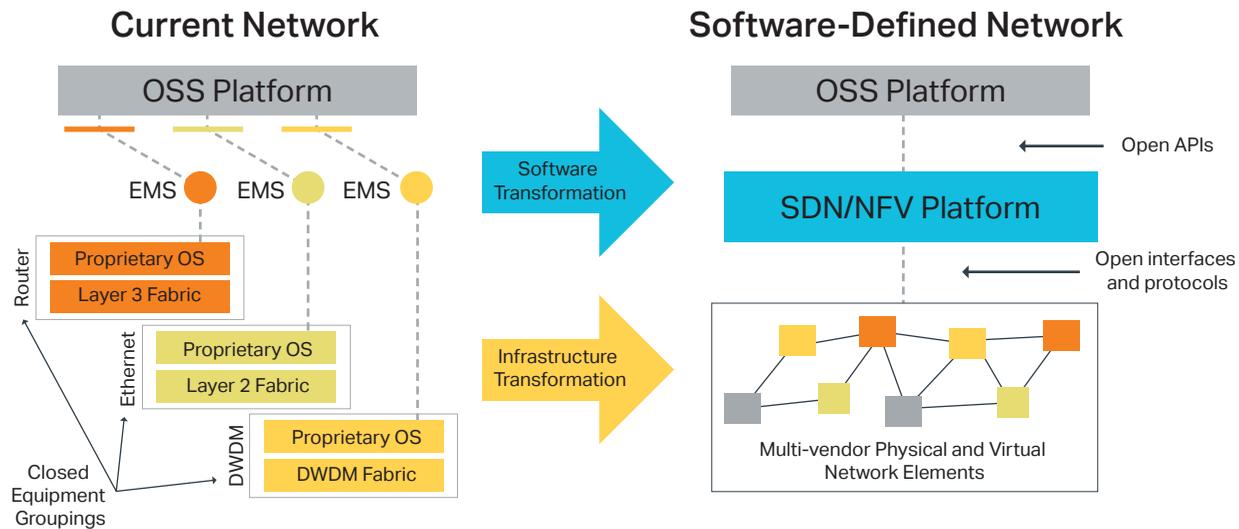


Figure 1. Evolving Government Networks

Government Software-Defined Networking

Software-Defined Networking (SDN) represents the ability to leverage software to control multiple devices as a virtual set of resources—delivering service orchestration.

A Government SDN (GSDN) leverages SDN to create a virtual network across several existing, unconnected physical networks. GSDN does for networks what the UK Government Digital Services did for website services—makes network services and interconnection simpler, faster, and more secure.

A GSDN addresses several constraints of today's networks:

- 1) Consolidates the underlying infrastructure into a single 'pane-of-glass' management view
- 2) Encourages the migration towards an open, vendor-agnostic architecture—removing the constraints forcing agencies into vendor lock-in
- 3) Optimizes connectivity across networks to improve interoperability

Software has changed the paradigm on the communication network, from rigid and inflexible to dynamic and agile. In this approach, end-users have simplified access to government services—anytime, anywhere. Governments can leverage the cloud to consolidate applications, increase collaboration, and support mobility of the workforce, accelerating service velocity and improving cyber resiliency.

Four key steps to network transformation

The transformation to a GSDN should be based on an organization's specific needs. Here are four key steps in the transformation process:

Step 1: Implementing SDN management and control software

Software makes taking the first step possible without massive infrastructure changes. Government IT leaders often do not have the ability to make the revolutionary network architecture changes needed to support their needs. SDN management and control software can abstract the network infrastructure and provide a 'single-pane-of-glass' view into single or multiple networks.

Step 2: Optimize existing networks

Once there is SDN management across networks, it is easier to interconnect segmented networks to enable new applications. If these interconnects will carry sensitive data, transport layer encryption can ensure wire-speed encryption to minimize latency impact to the applications.

Step 3: Leverage Virtual Network Functions (VNF)

Network Functions Virtualization (NFV) removes the need for application-specific hardware at the end points. Rather than individual, special purpose boxes such as firewalls, routers, and switches at every agency location, NFV can deliver software-based 'virtual' appliances to each location. This leverages a standard server for multiple virtual appliances and provides a key component of the 'retire, replace, reform' strategy.

Step 4: Multi-Domain Service Orchestration

A Multi-Domain Service Orchestrator (MDSO) enables end-to-end service automation and orchestration across multiple technology (physical or virtual) and vendor domains. MDSO eliminates silos by abstracting the complexity of underlying domains and enabling network operators to support end-to-end, lifecycle service orchestration.

Choosing the right SDN solution

SDN comes in many shapes, sizes, and restrictions. It can be challenging to compare the variety of SDN solutions. A GSDN network that enables a single network as well as cross-network orchestration should include the following capabilities:

- ✓ Vendor-agnostic support of any network vendor hardware manufacturer
- ✓ Multi-vendor inventory reporting
- ✓ Open, programmable capability to enable unique customization as needed
- ✓ Ability to support automation of service delivery across multi-layer, multi-vendor networks

Ciena: Hardware + software solutions

Ciena's Blue Planet software enables vendor-agnostic network virtualization, automation, and multi-vendor, multi-layer and multi-domain abstraction and control. Ciena's management services group provides various levels of engineering and design, install and implementation, and professional consulting and management support. Ciena's managed services group is CAS(T)-certified, as defined by CESG as part of the OSEA product for Openreach.

Ciena's expertise in industry-leading packet-optical infrastructure and intelligent software enables a fully agile network that meets growing capacity demands, automates operations, and reduces costs. Ciena is a trusted partner to the majority of global Tier 1 service providers and governments across the globe.



Ciena may make changes at any time to the products or specifications contained herein without notice. Ciena and the Ciena Logo are trademarks or registered trademarks of Ciena Corporation in the U.S. and other countries. Third-party trademarks are the property of their respective owners and do not imply a partnership between Ciena and any other company. Copyright © 2016 Ciena® Corporation. All rights reserved. PS146 9.2016