

## KEY FACTS



**Mean Time to Repair (MTTR) reduced** by 40% to 80%



**Over 1,300 active network components** across all locations

**Industry:** Public Sector

**Locations:** 6 existing sites + new locations

### Challenges:

- Modernisation of a seven-year-old network without service disruption
- High availability and redundancy for critical IT services
- Introduction of SDN, Wi-Fi 7 and centralised management
- Scalability for new sites and additional services

**Products:** Cisco Catalyst & Nexus switches, Cisco ISR/Catalyst routers, Wi-Fi 7 access points, Cisco Catalyst Centre, Cisco ISE

## NETWORK MODERNISATION FOR A PUBLIC SECTOR AUTHORITY

### OVERVIEW

The authority was tasked with fully modernising a seven-year-old network across six sites, while simultaneously integrating new locations without disrupting ongoing operations.

The objective was to create a high-performance, resilient infrastructure to serve as the technical backbone for all digital services, designed to support the organisation for the next five to seven years.

Damovo was commissioned to redesign and implement the entire network architecture. The solution is based on a Cisco-driven software-defined network (SDN), enabling centralised control, automated management and maximum resilience across all sites.

As a result, the authority benefits from significantly reduced administrative effort, improved network performance and a future-ready infrastructure that can flexibly adapt to new requirements.

## STARTING POINT & OBJECTIVES

The authority's network was over seven years old and had reached its technical limits. Outdated hardware and limited bandwidth, including switches with 1GE uplinks, had significantly constrained performance. Changes or expansions required considerable manual effort due to a lack of automation. Redundancy and resilience were limited, posing a **tangible risk to critical IT services**.

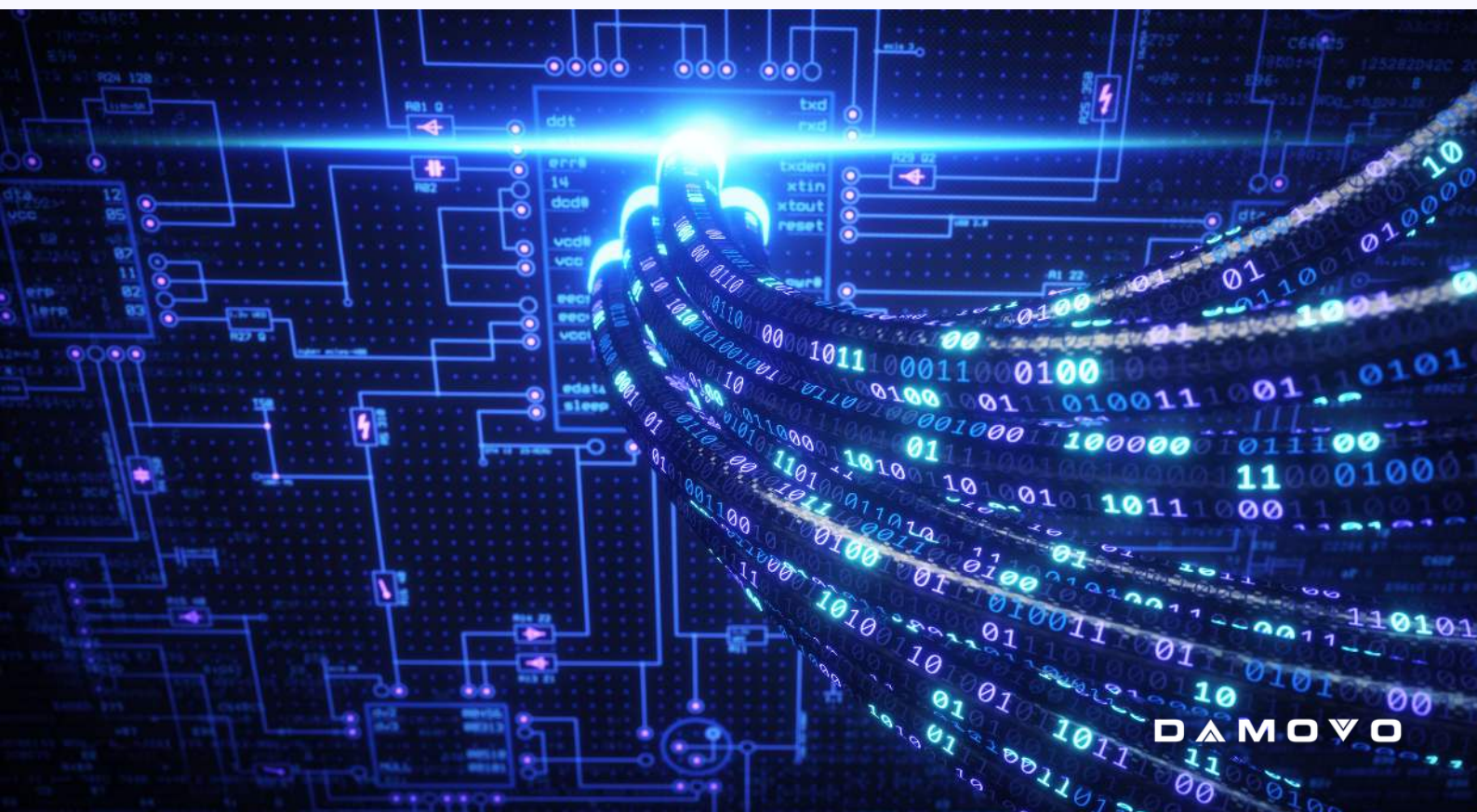
The authority defined clear requirements for the new infrastructure. The network needed to provide **maximum availability and redundancy across all layers**, with downtime to be effectively eliminated.

At the same time, **high-performance connectivity** was required, including multi-gig links, Wi-Fi 7 and optimised core and distribution upgrades. Administration was to be significantly simplified through automation and centralised control.

On the security level, consistent policies were defined as standards across all sites.

The network also needed to **support data, voice and video services simultaneously**, without impacting performance.

Another key focus was **scalability**: new sites needed to be integrated seamlessly without requiring changes to the overall architecture. The solution also had to be cost-efficient and ensure **investment protection** for the next five to seven years.



## IMPLEMENTATION

Damovo implemented a **software-defined network (SDN) architecture**, combining flexibility, performance and security. The solution is based on a **centrally managed infrastructure**, with core, distribution and access layers intelligently orchestrated using Cisco Catalyst and Nexus switches.

The **core and distribution layers** are built on Cisco Catalyst 9500 and 9300 switches, centrally managed via Cisco Catalyst Centre. This enables automated zero-touch provisioning, dynamic routing and consistent network segmentation.

In the data centres, a **spine-leaf architecture** orchestrated via Cisco ACI ensures high scalability, low latency and efficient load balancing, supported by Cisco Nexus 9300 switches.

At the **access layer**, Catalyst C9300X and C9200CX switches provide high-performance connectivity for Wi-Fi 7 access points.

For **WAN and routing**, Cisco ISR 1100, Catalyst 8300 and Catalyst 8500 routers were deployed, supporting MPLS and IPsec encryption, as well as VPN, firewall capabilities and LTE backup to ensure resilience.

In the **wireless LAN** environment, Cisco Catalyst 9800 WLAN controllers are used alongside indoor access points such as Cisco CW9176I and outdoor models like CW9163E. These components are fully integrated into the SDN environment and centrally managed via Catalyst Centre, including dynamic channel allocation, user-based policies and centralised policy management.

For **security and identity management**, Cisco Identity Services Engine (ISE) was implemented to enforce access control, microsegmentation and policy management across all network devices in a context-aware manner.

In addition, **management and orchestration platforms** were integrated, including Cisco Catalyst Centre for centralised SDA control of core, distribution and access switches, and Cisco Nexus Dashboard for server fabric management.

Overall, the solution represents a **fully integrated Cisco ecosystem** of switches, routers, wireless controllers, access points and management platforms, seamlessly orchestrated via SDN and covering all network layers from the data centre to branch locations.

## END-TO-END: DESIGN, IMPLEMENTATION AND HANDOVER

Damovo took the lead role in the project, supporting the authority from initial concept design through to final rollout. This included detailed solution design, defined migration strategies, configuration planning and the phased implementation of all project stages.

The go-live was prepared through precise wireless site planning, structured testing procedures and close coordination with the customer. A systems engineer was on site during critical phases to ensure a smooth transition.

In parallel, Damovo provided training for the IT team and documented all processes, enabling the authority to operate and further develop the new infrastructure independently.

## PROJECT PHASES

Damovo delivered the project in clearly defined phases. Following the **kick-off**, where project governance, communication channels and timelines were established, the design and configuration phase began.

During workshops, all requirements were captured, dependencies analysed and the **target architecture documented** in a **detailed implementation design**. In parallel, a **migration plan** was developed, including transition scenarios to minimise downtime.

The **implementation began with a pilot** across two floors at the main site. Wireless surveys and heatmap simulations ensured optimal placement of the access points.

Following a successful pilot phase, additional floors and sites were migrated step by step. Server, core and WAN components, as well as the wireless controllers, were implemented in parallel and integrated into the SDN architecture. A systems engineer was on site during go-live.

During the **testing and pilot phase**, network functions and security policies were validated, network performance was fine-tuned and the internal IT team was prepared for independent operation through **targeted training in SDN and SD-Access**. Damovo also provided comprehensive documentation of all processes.

Several sites are already live, with the remaining locations being migrated step by step. Damovo continuously adapts the rollout plan to evolving requirements.

## CHALLENGES

Two factors required particular attention during the course of the project. Global supply chain constraints and geopolitical influences made hardware procurement more complex. Damovo continuously adapted the rollout plan to mitigate delays and keep the project on schedule.

The second factor was technical in nature. Wireless site planning across multiple locations required a high level of precision. Heatmap simulations and on-site surveys ensured that Wi-Fi 7 coverage met the defined standards at all sites.

At the same time, the transition to SDN and SD-Access introduced a new operating model for the authority's internal IT team. As network control and management differ significantly from traditional environments, Damovo involved the IT team from the outset and provided targeted training to prepare them for independent operation.

In both cases, operations for end users continued without interruption throughout the migration.



## RESULTS

Since the go-live of the first sites, significant improvements have been achieved. With the introduction of SD-Access and Cisco Catalyst Centre, configuration changes can now be deployed centrally and dynamically. Manual administrative effort has been significantly reduced.

- Manual configuration effort reduced by 30–70%
- Provisioning of new sites is fully automated, without requiring changes to the overall architecture
- Network changes implemented in minutes rather than hours
- Mean Time to Repair (MTTR) reduced by 40–80% due to centralised telemetry and end-to-end visibility
- Significantly improved network performance through multi-gig switches and a spine-leaf architecture
- Reliable, high-performance Wi-Fi 7 coverage across all sites
- Consistent security policies automatically enforced across all sites and devices
- IT team fully enabled to operate independently following SDN and SD-Access training

The authority can now respond more flexibly to new requirements. The infrastructure is not only more stable than before but it also provides a solid foundation for the organisation's digital development in the years ahead.

## ABOUT DAMOVO

Damovo is a global technology service provider that supports businesses worldwide on their path to digitalisation. Our comprehensive portfolio includes solutions in the areas of cybersecurity, enterprise networks, unified communications & collaboration, contact centres, and global managed services.

With over 600 dedicated employees, we operate in Europe, the Americas and the Asia-Pacific region and offer global support in more than 150 countries.

## LET'S CONNECT

Visit our website to learn more about how Damovo can transform your business.

 [www.damovo.com](https://www.damovo.com)

Contact us now.

 [connect@damovo.com](mailto:connect@damovo.com)