Department for Education

Title:	**Network Switching Standards**
Published:	23 March 2022
Updated:	-

Find out what standards your school or college should meet on switch performance, management, security and resilience.

Prepared from information from the DfE by the Association of Network Managers in Education.
www.anme.co.uk

Standard 1

The network switches should provide fast, reliable and secure connections to all users both wired and wireless

The importance of meeting the standard

You will have a high number of users accessing the network at the same time. A high-performance solution will make sure that the speed and management of data transferred around the network is efficient, secure and doesn't slow down as more devices use it.

How to meet the standard

You should ask your supplier or in-house support team to make sure that switches provide a minimum of 1Gbps connectivity to the user device deployed to the desktop.

You should also make sure that higher speed (multi-gigabit) ports support devices and infrastructure equipment that needs high bandwidth such as servers, media devices and wireless access points. See dependencies on this standard.

Switches that connect to wireless access points, CCTV and telephones must comply with the correct POE requirements outlined by the device manufacturer.

Technical requirements to meet the standard

Where switches are stacked, they should support 40Gbps interconnects between switches in a stack, dedicated stacking ports should be used to enable high speed communication between each switch in the stack.

Connections linking switches or switch stacks in hub rooms must connect back to the core server room using a minimum of 2x10Gbps with links taking different routes where possible. See dependencies on this standard.

Switches providing POE should adhere to IEEE 802.3af.at or bt as required by the connecting device and have LLDP-Med enabled.

Switches should:

- have a minimum of 512MB of core memory
- support a minimum of 16000 MAC addresses
- support spanning tree protocols such as MST or RST
- use non-blocking switch fabric

Switches should be Energy Efficient Ethernet compliant to a minimum of 802.3az standard or equivalent.

Dependencies to the standard

The performance of your network switches may be affected by the specification and quality of your network cabling.

When to meet the standard

You should meet the standard when you need to replace your current solution that is underperforming or unsupported.

Standard 2

Have a platform that can centrally manage the network switching infrastructure

The importance of meeting the standard

A computer network will have many users accessing and transferring data. A central management console will allow the control and monitoring of the network efficiently and securely to ensure effective performance.

How to meet the standard

Your supplier or in-house support team should provide a central management tool that can be used to configure the switching (core and edge), monitor performance and provide alerts in the event of a failure.

Technical requirements to meet the standard

Switches should include a manufacturer warranty and support arrangement (telephone, email and web) including licences, software enhancements and firmware updates, providing 5 years of cover as a minimum.

They should also include a system administrator training package on your school or college site that is:

- approved by your manufacturer
- appropriate to the scale of the solution
- covering all security elements for the solution

When to meet the standard

You should meet the standard when you need to replace your current solution that is underperforming or unsupported.

Standard 3

The network switches should have security features to protect users and data from unauthorised access

The importance of meeting the standard

School and college IT networks should prevent access by unauthorised users while giving access to regular and guest users.

Network switching infrastructure without adequate security may allow unauthorised users access to secure information stored by the school or college, such as student records.

How to meet the standard

You should ask your supplier or in-house support team to ensure that switches are configured to support network segregation, security and quality of service. This should not impact the network's deployment or performance and should be aligned with the environment.

Any administrative accounts that have access to make configuration changes, must be secure and fully documented.

The delivery of software updates should be set to automatically update as soon as they are available and manual checks should also be undertaken.

Technical requirements to meet the standard

You should ensure that you have implemented NACs and Policy Management that ensures authorised mobile user devices or guest user roles are securely authenticated onto the network. Network traffic should be protected from external and unauthorised internal interception.

Have central management tools that can be used to configure the network switches, monitor performance and provide alerts in the event of a failure.

When to meet the standard

You should meet the standard when you need to replace your current solution that is underperforming, unsupported or following a scheduled maintenance or configuration review.

Standard 4

Core network switches should be connected to at least one UPS to reduce the impact of outages

The importance of meeting the standard

Your school or college will have a high number of users accessing the network at the same time. An outage of part or all of the network would cause disruption to teaching and admin operations.

How to meet the standard

Ask your supplier or in-house support team to make sure that critical switches and their connections have been identified to ensure any failure of any single element will not cause a major outage.

These will include items such as multiple power supplies, UPS solutions and dual connections between switches.

Technical requirements to meet the standard

Critical core switches should have at least:

- 2 power supplies
- 2 management modules
- 2 connections to other critical infrastructure such as routers, servers and other core switches

The critical core switches should be connected to at least 1 UPS.

When to meet the standard

You should meet the standard when you need to replace your current solution that is underperforming, unsupported, or following a scheduled maintenance or configuration review.