



## Secure DNS and high DHCP availability better facilitate e-learning

### Challenge

- IP proliferation from BYOD outgrew existing DNS / DHCP solutions
- External DNS resolution slow, insecure
- Internal DNS not always reliable
- DHCP unable to handle IP lease demand
- Time-consuming and repetitive for network admins

### Solution

- 2 x **DNSBOX200** appliances, each deployed in separate DCs
- All running 3 services – Authoritative + Recursive DNS + DHCP with Active-Active Failover

### Benefit

- Core services now reliably facilitate e-learning at the district
- Ultra-secure, lightning-fast DNS resolution
- Increased network availability for thousands of connecting devices
- Easily deployed, fit-for-purpose solution

### About Nickerson-South Hutchinson School District, Kansas, USA

Nickerson–South Hutchinson USD 309 is a unified school district headquartered in South Hutchinson, Kansas, United States. The district is highly committed to ensuring technology is integral to its curriculum and instruction. Every high school student is equipped with a personal Chromebook, and every middle and elementary school student is provided with Chromebooks and iPads while in school.

At any one moment, 1,200 students and several hundred staff each require secure internet access, on and off throughout the school day. That can total around 3,000 active IP addresses and – with the district also supporting BYOD (Bring Your Own Device) mobile phone access – that rises to 4,000 connections.

### DHCP server couldn't handle BYOD

The district previously used a MAC server to connect both school-owned and BYOD devices to the network. When Apple discontinued support for its DHCP service, the district moved to doing this on a Meraki switch.

However, as BYOD was gradually rolled out, the number of IPs connecting to the network grew from hundreds to thousands, drastically changing performance and DHCP configuration requirements. The Meraki switch could no longer handle the large amount of IP leases being requested, causing performance issues for the users.

As a result, Nickerson's IT Director Aaron Bell received complaints about connectivity glitches and – in some cases – students not being able to connect to the internet at all. He now sought a redundant, highly available DHCP solution to replace the old one.

### Need for fast, reliable & secure DNS

The district had also been relying on a Windows Active Directory server to handle thousands of internet (DNS) requests from students and teachers accessing the network. However, as Windows AD is primarily an authentication, authorisation and logging service, using it for DNS services overwhelmed the server, impacting performance.

"This is one of the most common reasons for schools to move away from Microsoft AD for DNS," says **DNSBOX** Technician Callum Key. "It simply isn't built to handle the sheer volume of DNS requests from thousands of devices, each requesting dozens of web pages and websites daily. So, the symptoms you're likely to see in cases like this is slow response times for users, caused by an unreliable DNS service."

Aaron was also worried about network security: as a multi-purpose platform, Microsoft AD is not inherently secure. "DNS servers should be especially protected and secure. In case of an attack on DNS, like a DDoS (Distributed Denial of Service) attack, an MS Active Directory-integrated DNS could have issues; since it would be tasked with the DNS and the critical authentication / logging activities," says Callum. "A DNS-based attack could render all AD services unavailable, preventing users from being able to authenticate or access network services such as fileshares and printers."

In addition to replacing his DHCP solution, Aaron also added a fast, reliable and secure DNS to his spec. With a restrictive school budget, Aaron sought a solution that would deliver best value with the highest impact.



*Windows AD simply isn't built to handle the sheer volume of DNS requests from thousands of devices, each requesting dozens of web pages and websites daily."*



**Callum Key**  
**DNSBOX Technician**



*A DNS-based attack could render all AD services unavailable, preventing users from being able to authenticate or access network services such as fileshares and printers.*

**Callum Key**  
**DNSBOX Technician**



After approaching ApplianSys for information on **DNSBOX**, he was pleased to find that **DNSBOX200**'s modular design could accommodate both services – and include authoritative DNS – on a single physical server – making the solution very affordable.

#### **Fully redundant solution**

Aaron deployed a redundant pair of **DNSBOX200**'s – one at each of the district's separate datacentres. Used as slaves the **DNSBOX200**'s serve authoritative DNS requests – ensuring DNS reliability.

Fully synchronised, they deliver rock solid, high availability active-active DHCP failover, seamlessly handling critical network services for the ~3000 hosted active IP addresses as well as over 1,000 cell phones.

#### **Easy migration**

Compatible with common network equipment like Cisco and Microsoft Active Directory, **DNSBOX** made DHCP migration and zone transfers quick and easy.

Existing zones were transferred directly from the existing Windows DNS server to **DNSBOX200**'s authoritative DNS service.

#### **A premium user experience**

Now Nickerson's network can seamlessly handle thousands of IP leases without issue – ensuring that school devices can always connect successfully to the network.

And the high performance recursive DNS ensures students can always access content quickly and reliably.

No more connectivity glitches, no more delays and no complaints for Aaron - just fast, secure, highly available network services that help deliver the premium learning experience Nickerson needs.