InkBridge Networks

We Authenticate The Internet

AN EDUCATION SECTOR CASE STUDY

Network authentication at scale: Securing campus WiFi for millions of users worldwide

Document	Case Study
Prepared by	Alan DeKok, CEO
Date	2025-07-08

InkBridge Networks

The scale of educational network authentication creates exceptional challenges: providing seamless, secure network access and campus WiFi to a constantly changing population of students, faculty, researchers, and visitors.

The eduroam (education roaming) federation has become the gold standard solution, allowing users from participating educational institutions to access secure campus-wide WiFi networks at any other participating institution worldwide using their home user credentials.

But operating network authentication at this scale introduces unique technical challenges that go beyond typical enterprise deployments, requiring specialized expertise and innovative solutions to manage network traffic and prevent network outages.

The Massive Scale of Campus WiFi

eduroam is one of the largest federated network authentication systems in the world, with:

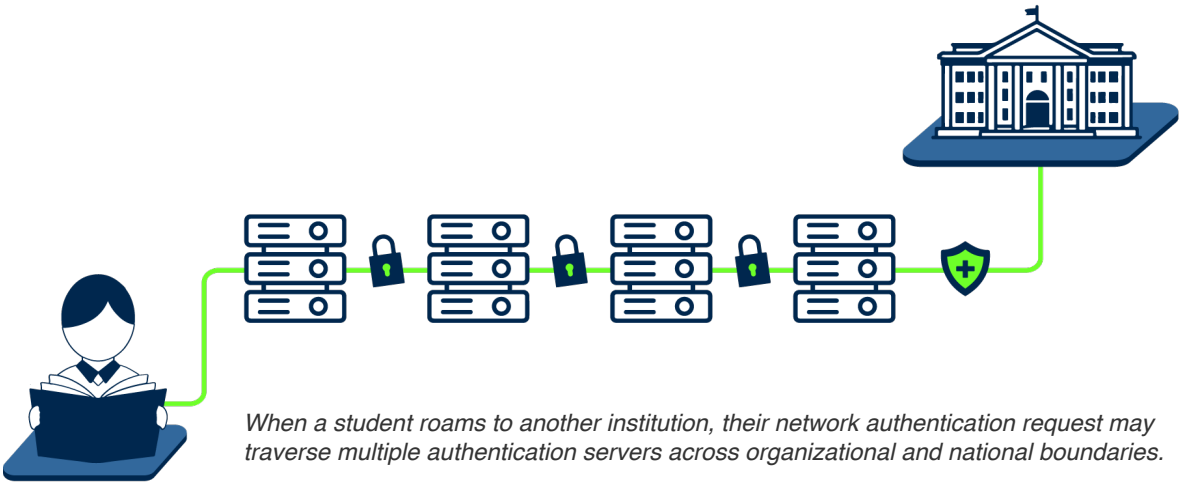
More than 10,000 hotspots across 100+ countries

Over 8.4 billion network authentication requests processed in 2024 alone

Hundreds of millions of end users accessing network services

What makes eduroam particularly challenging is not just the volume of network authentication requests, but the complex, multi-hop routing of these requests across organizational and national boundaries:

- When a student from University of Helsinki visits University of Alberta, their user credentials must be verified through a chain of authentication servers spanning continents.
- Each network authentication request might travel through 4–5 different proxies before reaching its final destination.
- Response times must remain low despite this complexity (under 5 seconds is considered acceptable).
- Network reliability is critical—a failure at any point in the network infrastructure can prevent legitimate users from gaining access.
- At the same time, the system is open to the public and must therefore be kept secure from denial of service (DoS) attacks.
- The system must also be robust in the face of administrator misconfiguration. With thousands of sites connecting to eduroam, there will always be a few that are configured incorrectly or offline for extended periods of time.



When a student roams to another institution, their network authentication request may traverse multiple authentication servers across organizational and national boundaries.

Scaling Challenges That Push the RADIUS Protocol to its Limits

The core challenge eduroam operators face is managing significant network traffic across a distributed infrastructure where network disruptions, packet loss, attacks, and server failures can have cascading effects on network authentication.

For example, if an eduroam operator wanted to expand from regional to national coverage, their network authentication traffic would be projected to increase 10–20 times. Existing network infrastructure is often not designed for this scale.

These challenges stem from fundamental limitations in the RADIUS protocol itself:

1. Silent failures create troubleshooting nightmares

The RADIUS protocol was originally designed to perform retransmissions in the event of packet loss. This approach works well enough in most cases, but the RADIUS protocol was also designed to deliberately drop packets in many cases. That is, a RADIUS server can simply drop a packet without notifying the client that it has done so—a design choice that creates enormous problems in federated environments:

- When network authentication fails, servers have no way to distinguish between network outages, server failures, or slow networks.
- IT administrators often receive support calls from users unable to connect, but the protocol provides very little diagnostic information to determine where in the proxy chain the failure has occurred.
- Interconnected authentication servers can make incorrect failover decisions due to having insufficient information about the status of other servers (due to the above issues). The result is that there can be cascading network issues.

2. Network congestion leads to denied access

Internet infrastructure is designed to handle network congestion by discarding data packets when overwhelmed. While this approach works acceptably for video streaming or web browsing (causing momentary glitches), with network authentication using the RADIUS protocol it results in authentication failures:

- During peak usage periods (such as the start of academic terms), network authentication failures spike due to network congestion.
- Each authentication server in the federated chain adds another point where packets can be dropped.
- Dropping one packet in the middle of WiFi authentication (EAP) usually means that the entire authentication session will fail.
- Server failover usually helps with service availability, but for EAP, server failover can cause hundreds or thousands of EAP sessions to fail all at the same time. These failures cause users to retry, further increasing system load.
- A substantial percentage of eduroam traffic is, in fact, useless! Internal investigations show that 30% of traffic is for users whose accounts were deleted years ago—if not decades. In some extreme cases, up to 90% of authentication sessions result in rejects.

The result of all these problems is that users experience seemingly random connection failures that are difficult for network administrators to reproduce or diagnose.

3. Cross-border authentication complexities

When network authentication requests cross international boundaries:

- Varying network qualities and routing paths affect reliability of secure network access.
- Regulatory requirements can impact how authentication data and user location are handled.
- Maintenance windows and technical support hours rarely align across global time zones, complicating network outages.

The InkBridge Networks Solution: **Protocol Enhancements for Next-Generation Network Authentication**

Based on extensive collaboration with global eduroam operators and network authentication experts, InkBridge Networks has developed a series of RADIUS protocol enhancements that address these challenges without requiring a complete rebuild of existing network infrastructure.

Some of these enhancements are available now in our RADIUS server products. Others require the standards to change. We are writing new RADIUS documents (RFCs) at the Internet Engineering Task Force (IETF) to fully describe and standardize these changes.

Explicit response signaling

Rather than silently dropping packets when uncertain how to proceed, enhanced authentication servers can provide explicit signals about why network authentication failed:

- Authentication servers can indicate when they're unable to contact the next hop in the chain.
- Authentication failures can include reason codes that simplify troubleshooting network issues.
- Network administrators gain visibility into where exactly in the chain problems occur.
- Authentication servers can perform failover more quickly than they could before and can make better decisions about when to fail over (or not).

Better Access-Rejects

Access-Reject packets are being enhanced to provide the originating server (i.e., the visited network) with better information, so that they can reduce the amount of traffic they send to the proxy network.

- Home servers can indicate that this user account does not exist or is being abusive. They can indicate that this account should be prevented from accessing the network for a period of time. This time period is long enough to cut down on bad traffic by 99% or more, but it is also short enough that it does not affect typical users.
- Home servers can better deal with the conflicting requirements to reject users quickly (to free up resources in the proxy chain), while at the same time delaying rejects for a short period to prevent dictionary attacks on the user account. Protocol changes allow the home server to reply immediately, but also to indicate to the visited network that the reject should be delayed before sending it to the access point.

Improved failover intelligence

Enhanced RADIUS protocol behavior allows authentication servers to make more informed decisions when network issues arise:

- Authentication servers can distinguish between temporary network congestion and server failures.
- Dynamic routing adjustments can bypass problematic nodes in the authentication chain.
- Recovery happens automatically when network services are restored.

Defining best practices for proxy networks

The only reference to proxy networks in the RADIUS standards is a short line from 25+ years ago saying that “this issue is the subject of ongoing research”.

We are collating 25 years of experience running RADIUS proxies into a best practices document:

- Define practices for proxy retransmissions
- Define best practices for load balancing and failover
- Define best practices for rate-limiting proxied packets
- Describe other best practices that have been proven to be useful in production networks

Real-World Results: Enhanced Network Authentication Reliability, Reduced Support Burden

Educational institutions implementing these enhanced network authentication features have reported significant improvements:

- Network authentication failure rates dropped by up to 65% during peak registration periods.
- Mean time to resolution for network authentication issues decreased from hours to minutes.
- IT support ticket volume related to network access went down by approximately 40%.

SUPPORTING YOUR EDUCATIONAL INSTITUTION'S NETWORK

InkBridge Networks brings decades of RADIUS expertise alongside extensive eduroam implementation experience to educational institutions worldwide. Our team includes engineers who helped develop the protocol standards and have spent 25+ years solving authentication challenges unique to academic environments.

Through our Education support tier, IT teams gain direct access to specialists who understand the complexities of campus networks, eduroam federation requirements, and peak-load scenarios. This includes same-business-day responses and targeted configuration reviews to ensure optimal performance during critical periods like registration and exam seasons.

Future-Proofing Network Authentication for Educational Institutions

Looking ahead, InkBridge Networks is working with the broader network authentication community to formalize these enhancements through the IETF standardization process:

- Real-world operational validation ensures standards reflect practical needs for secure network access.
- Multiple vendors have committed to implementing these RADIUS protocol enhancements.
- Interoperability testing ensures smooth transitions for participating institutions.

As Alan DeKok, CEO of InkBridge Networks, explains:

"Rather than starting with theoretical standards that may never be implemented, we're taking a pragmatic approach—validating these network authentication improvements in production environments first, then documenting them as standards. This ensures what we standardize actually solves real-world problems for network administrators."

LEARN MORE
about InkBridge Networks' solutions for educational institutions.

REQUEST A QUOTE
to discover how we can enhance your network authentication infrastructure.

The InkBridge Networks Advantage for Managing Network Authentication

Educational institutions working with InkBridge Networks gain:

- Access to cutting-edge network authentication protocol enhancements before they become widely available
- Access to proprietary software enhancements that have been proven in large-scale networking environments
- Expert guidance on optimizing network authentication infrastructure for peak performance
- Support from the same team that maintains FreeRADIUS, the world's most widely deployed RADIUS server
- A scalable solution that grows with your institution and federation

As educational networks continue to grow in complexity and scale, the importance of reliable, high-performance campus WiFi infrastructure will only increase. By addressing the fundamental limitations of traditional RADIUS protocol implementations, InkBridge Networks is ensuring that educational institutions can provide seamless, secure network access to their communities—no matter how large they grow or how complex their network infrastructure becomes.

InkBridge Networks

26 rue Colonel Dumont
38000 Grenoble
France

T +33 4 85 88 22 67
F +33 4 56 80 95 75
W https://inkbridgenetworks.com
E sales@inkbridge.io

InkBridge Networks (Canada)

100 Centrepointe Drive, Suite 200
Ottawa, ON, K2G 6B1
Canada

T +1 613 454 5037
F +1 613 280 1542

InkBridge Networks

We authenticate the Internet