



# What is a Network Access Device (NAD)?

## Table of Contents

- What is a network access device (NAD)?
- What security does a network access device provide?
- How do network access devices enforce access control policies?
- How does an NAD integrate with RADIUS?

## What is a network access device (NAD)?

A network access device (NAD) is a type of hardware device that allows computers or other network devices to connect to a network. These devices are typically located at the edge of a network and provide the interface between the network and the devices connecting to it.

Some common examples of NADs include routers, switches, wireless access points, and modems. Routers are used to connect multiple networks together, while switches are used to connect multiple devices within a network. Wireless access points allow devices to connect to a network wirelessly, and modems are used to connect a network to the Internet.

NADs may also provide additional features such as security, traffic shaping, and Quality of Service (QoS) controls to ensure that network traffic is prioritized and managed effectively. They play a crucial role in the operation and management of modern computer networks.

## What security does a network access device provide?

Network access devices (NADs) provide several security features to protect network infrastructure and devices connected to the network. Here are some common security measures implemented by NADs:

- **Access Control:** NADs enforce access control policies to determine which devices or users are allowed to connect to the network. This is typically achieved through authentication methods such as usernames, passwords, or digital certificates.
- **Firewall Protection:** Many NADs include built-in firewall capabilities to filter network traffic and block unauthorized access attempts. Firewalls examine packets and enforce security policies based on protocols, ports, IP addresses, and other criteria.
- **Virtual Private Network (VPN) Support:** NADs often support VPN technologies, allowing secure remote access to the network over public or untrusted networks. VPNs encrypt network traffic, providing confidentiality and integrity to data transmissions.
- **Intrusion Detection/Prevention System (IDS/IPS):** Some advanced NADs incorporate IDS/IPS functionality to monitor network traffic for malicious activity or suspicious behavior. These systems can detect and alert administrators about potential attacks and may even take proactive measures to prevent them.
- **Network Segmentation:** NADs enable network segmentation, dividing the network into separate subnetworks or VLANs (Virtual Local Area Networks). This helps contain potential security breaches by isolating sensitive data and limiting the spread of threats within the network.
- **Quality of Service (QoS) Controls:** While not strictly a security feature, QoS controls on NADs can help mitigate network-based attacks such as Distributed Denial of Service (DDoS) attacks. QoS mechanisms prioritize network traffic and allocate resources to ensure critical services receive sufficient bandwidth and minimize the impact of malicious traffic.
- **Logging and Auditing:** Many NADs provide logging capabilities to record network events and activities. This data can be analyzed for troubleshooting, monitoring, and forensic purposes to identify security incidents or policy violations.

It's worth noting that the specific security features and capabilities of NADs may vary depending on the device type, vendor, and model. Organizations often implement multiple layers of security, including NADs, firewalls, intrusion detection systems, and other security solutions, to create a comprehensive security posture for their networks.

# How do network access devices enforce access control policies?

Network access devices (NADs) enforce access control policies through various mechanisms. Here are some common methods used by NADs to enforce access control:

- **Authentication:** NADs require users or devices to provide authentication credentials to establish network access. This can involve usernames, passwords, or more secure methods such as digital certificates, smart cards, or biometric authentication. The NAD verifies the credentials provided by the connecting entity before granting access.
- **MAC Address Filtering:** NADs can filter network access based on Media Access Control (MAC) addresses, which are unique identifiers assigned to network interface cards (NICs). By configuring a MAC address whitelist or blacklist, the NAD allows or denies access to specific devices based on their MAC addresses.
- **Port-Based Access Control:** NADs can implement port-based access control, such as IEEE 802.1X, to authenticate and authorize devices before granting network access. This method requires devices to go through an authentication process before they are allowed to communicate on the network.
- **Role-Based Access Control (RBAC):** NADs can integrate with authentication systems that support RBAC. In this approach, users or devices are assigned roles with specific access privileges, and the NAD enforces those privileges based on the authenticated role.
- **Network Segmentation:** NADs enable network segmentation by creating separate subnets or Virtual Local Area Networks (VLANs). Access control policies can be defined at the VLAN or subnet level, allowing administrators to restrict access between different segments of the network.
- **Guest Access and Captive Portals:** NADs often provide guest access features, allowing temporary or limited access for visitors or guest devices. Captive portals can be used to present a login or agreement page before granting network access to guests. These mechanisms ensure that guests comply with network usage policies and prevent unauthorized access.
- **Integration with Authentication Servers:** NADs can integrate with external authentication servers such as RADIUS (Remote Authentication Dial-In User Service) or LDAP (Lightweight Directory Access Protocol). This enables centralized user authentication and allows the NAD to validate user credentials against the server's database.

By combining these access control mechanisms, NADs enforce security policies and ensure that only authorized devices and users are granted access to the network. The specific methods employed may vary depending on the capabilities of the NAD and the organization's security requirements.

# How does an NAD integrate with RADIUS?

Integration between a network access device (NAD) and RADIUS (Remote Authentication Dial-In User Service) typically involves the NAD acting as a client to communicate with a RADIUS server for user authentication and authorization. Here's a high-level overview of how NADs integrate with RADIUS:

- **Configuration:** The NAD is configured with the necessary parameters to establish communication with the RADIUS server. This includes specifying the IP address or hostname of the RADIUS server, shared secrets (a secret key used to authenticate and encrypt communication between the NAD and server), and other relevant settings.
- **Authentication Request:** When a user or device attempts to connect to the network through the NAD, the NAD initiates an authentication request to the RADIUS server. The request includes user credentials, such as a username and password, or other authentication methods supported by the RADIUS server (e.g., digital certificates).
- **RADIUS Server Processing:** The RADIUS server receives the authentication request from the NAD and validates the provided credentials. It verifies the user's identity against its user database, which can be a local database or a remote authentication source like LDAP or Active Directory. The server may also perform additional checks or apply policy-based rules for access control.
- **Authentication Response:** The RADIUS server sends an authentication response back to the NAD. The response indicates whether the authentication was successful or failed. If successful, the response may include additional information such as authorization attributes or session parameters.
- **Access Control and Authorization:** Based on the authentication response received from the RADIUS server, the NAD determines whether to grant or deny network access to the user or device. It applies the access control policies defined by the RADIUS server, such as assigning VLANs, QoS settings, or other specific access privileges based on user roles or attributes.
- **Accounting:** Optionally, the NAD can send accounting information to the RADIUS server to track network usage and session details. This includes data such as the duration of the session, data transfer, and other relevant metrics.

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking “Accept”, you consent to the use of ALL the cookies. [Do not sell my personal information.](#)

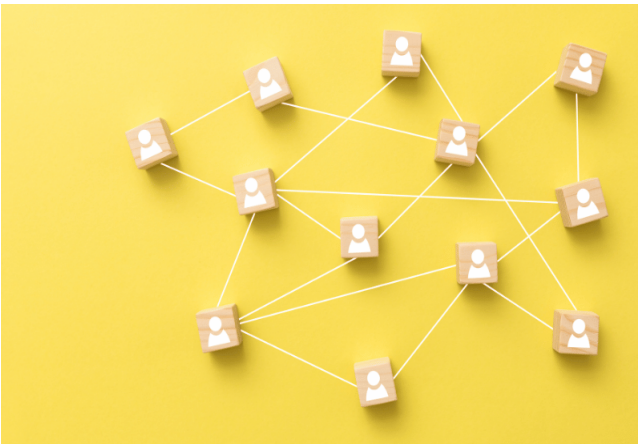
The integration between the NAD and RADIUS allows for centralized authentication and authorization management, simplifying the administration and enforcement of access control policies across the network. It enables organizations to maintain a single authentication infrastructure while leveraging the security features provided by RADIUS servers.

Related Reading



(<https://www.portnox.com/cybersecurity-101/access-control-list-acl/>)

**What is an Access Control List (ACL)?**  
(<https://www.portnox.com/cybersecurity-101/access-control-list-acl/>)



(<https://www.portnox.com/cybersecurity-101/network-microsegmentation/>)

**What is Network Microsegmentation?**  
(<https://www.portnox.com/cybersecurity-101/network-microsegmentation/>)



(<https://www.portnox.com/cybersecurity-101/network-access-server-nas/>)

**What is a Network Access Server (NAS)?**  
(<https://www.portnox.com/cybersecurity-101/network-access-server-nas/>)

- 
- BLOG**  
(<https://www.portnox.com/blog/>)

**SUPPORT**  
(<https://www.portnox.com/support/>)

**LEGAL**  
(<https://www.portnox.com/legal/>)

**PRIVACY**  
(<https://www.portnox.com/privacy-policy/>)

- PRODUCTS**  
(</products/>)
- ZTNA (</Portnox-Cloud/>)

RADIUS  
(<https://www.portnox.com/Portnox-Cloud/Radius/>)

TACACS+  
(<https://www.portnox.com/Portnox-Cloud/Tacacs/>)

Pricing (</Pricing/>)

- SOLUTIONS**  
(<https://www.portnox.com/solutions/>)
- Passwordless  
(</Solutions/Passwordless-Authentication/>)

ZTNA (</Solutions/Zero-Trust-Network-Access/>)

802.1X (</Solutions/8021x-Authentication/>)

IoT Security (</Solutions/IoT-Security/>)

Guest Access (</Solutions/Guest-Access-Management/>)

- RESOURCES**  
(</resources/>)
- Blog  
(<https://www.portnox.com/blog/>)

Case Studies (</Resources/Case-Study/>)

Products Briefs  
(</Resources/Product-Brief/>)

White Papers (</Resources/White-Paper/>)

Webinars (</Resources/Webinar/>)

Cloud Documentation  
([https://docs.portnox.com/?utm\\_medium=Website&utm\\_source=Home](https://docs.portnox.com/?utm_medium=Website&utm_source=Home))

- PARTNERS**  
(</partners/>)
- Reseller Program  
(</Partners/Program/>)

Managed Services  
(</Partners/Managed-Services/>)

Become A Partner (</Partners/>)

Partner Portal  
(<https://portnox.force.com/>)

- ABOUT**  
(<https://www.portnox.com/about-us/>)
- Why Portnox  
(<https://www.portnox.com/Why-Portnox/>)

News  
(<https://www.portnox.com/Press-Releases/>)

Logi Careers  
(<https://portnox.pinpointhq.com/>)

Contact Us  
(<https://www.portnox.com/contact-us/>)

Security Statement  
(<https://www.portnox.com/Security-Statement/>)

(<https://www.facebook.com/portnox>) 

(<https://twitter.com/portnox>) 

©2023 Portnox. All Rights Reserved.

(<https://www.linkedin.com/company/portnox/>) 



(<https://www.youtube.com/user/portnox1>) 

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept", you consent to the use of ALL the cookies.  
[Do not sell my personal information.](#)

[Cookie settings](#)    [ACCEPT](#)

([https://www.instagram.com/portnox\\_security/](https://www.instagram.com/portnox_security/)) 



(/press-  
releases/portnox-  
clear-achieves-  
soc-2-type-ii-  
certification/)  
  
(/news/portnox-  
receives-iso-  
27001-security-  
certification-  
for-network-  
access-  
control/)

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking “Accept”, you consent to the use of ALL the cookies.  
[Do not sell my personal information.](#)

[Cookie settings](#)    ACCEPT