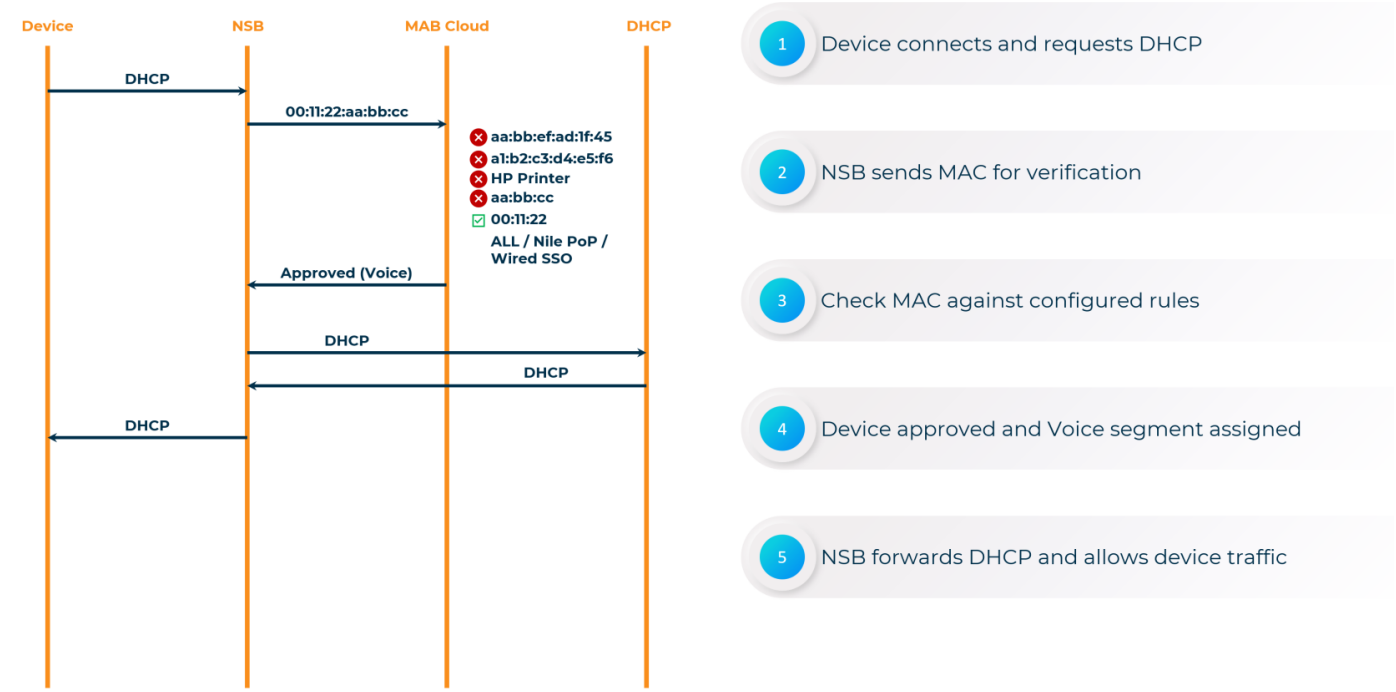
Zero Trust Access: MAC Authentication Bypass (MAB)

MAB and the Zero Trust Campus

The Nile Access Service is built on the principles of a "Zero Trust Campus," ensuring that no user or device is implicitly trusted. As part of this security model, the Nile Access Service supports MAC Authentication Bypass (MAB) as an authentication method for devices that cannot accommodate the 802.1X standard.

While MAB provides network access for non-802.1X capable devices, such as printers and IoT equipment, it is essential to maintain the principles of Zero Trust. Nile's implementation of MAB includes additional security measures to isolate these devices and limit their potential impact on the network.

MAB for Wired connections

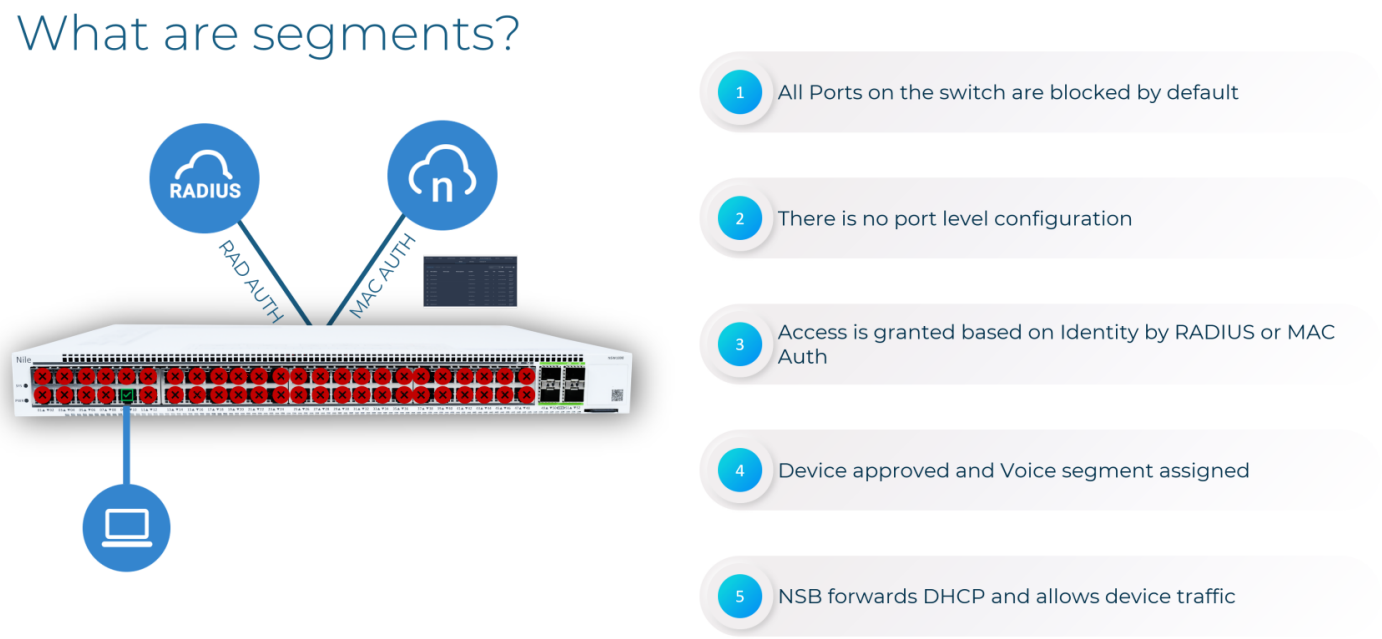


Why Use MAB?

Nile requires all wired access to be authenticated before granting network connectivity. The Nile Access Service supports three different wired authentication methods:

1. Wired 802.1X authentication (requires a RADIUS server)
2. Wired RADIUS MAB authentication (requires a RADIUS server)
3. Nile Portal Wired MAB authentication

MAB is a crucial authentication method for devices that cannot support the 802.1X standard, ensuring comprehensive coverage and secure access to Nile Access Service Segments.



Configuring MAB

Nile provides flexible options for configuring MAB within the Nile Access Service:

Uploading a MAC Address List
You can upload a list of MAC addresses for wired MAB authentication by navigating to the Nile Portal (Settings > Access Management > Wired) and providing the following information:

- MAC address: The device's MAC address (mandatory)
- Segment: The network segment to which the device should be assigned (required for "Allow" status, optional for "Deny")
- Lock to Port: Lock the device to a specific switch port (optional)
- Site, Building, Floor: Restrict the device to a specific geographical location (optional)
- Allow or Deny: Specify whether to allow or deny access for the device (mandatory)

[screenshot required]

Enabling Auto-MAB for Specific Device Types
You can also configure Nile to automatically authenticate devices based on their Organizational Unique Identifier (OUI), the first 24 bits of a MAC address that identify the device manufacturer. This can be done in the Nile Portal (Settings > Access Management > Wired > Add Device > OUI/MAC), where you can select the segment, status (Approved/Denied), and geographical scope for the OUI-based policy.

[screenshot required]

MAB Port Locking and Geographical Scope
Nile offers additional security features for MAB, including the ability to "Lock to Port" and restrict devices to specific geographical locations ("Geo Scope"). These options help mitigate the risks associated with MAB by ensuring that devices can only connect to authorized switch ports and locations.

[screenshot required]

Disabling Nile Wired Authentication

Nile's network is designed with security best practices in mind, and you cannot disable MAB authentication entirely. However, you can create a catch-all "allow all" policy to grant network access to all devices, assigning them to a specific segment. While this approach is not recommended, it can be enabled in the Nile Portal (Settings > Access Management > Wired > Add Device > Allow all MACs).

Remember that the "allow all" policy will automatically create a unique MAC-allowed entry for each device when it first connects to the Nile switch. Deleting the "allow all" policy will not impact connected devices or delete the specific policies that were auto-created.

By understanding the role of MAB within the Nile Access Service and the available configuration options, you can ensure that non-802.1X capable devices are granted secure network access while maintaining the principles of the Zero Trust Campus.

Summary

In summary, the Nile Access Service's implementation of MAC Authentication Bypass (MAB) is a vital component of our comprehensive authentication framework. Nile's flexible MAB configuration options, including MAC address lists, auto-MAB for specific device types, and advanced security controls like port locking and geographical restrictions, empower organizations to extend secure network access to a wide range of devices, including those that cannot support 802.1X.

Furthermore, Nile's innovative approach to network segmentation, which transcends traditional VLAN-based models, enhances the benefits of MAB. The Nile Access Service's Layer 3 segmentation , driven by user identity, device attributes, and application requirements, enables granular access

controls and micro-segmentation. This powerful combination of MAB and Nile's advanced segmentation strategy helps enterprises maintain a robust security posture while accommodating diverse connectivity needs, in alignment with Zero Trust principles.

By leveraging the flexibility and security of MAB within Nile's innovative network architecture, organizations can confidently provide secure access to a wide range of devices, minimizing the attack surface and reducing the risk of lateral movement. As a key part of the Nile Access Service's authentication framework, MAB contributes to the overall effectiveness of this cloud-native network solution in helping enterprises build resilient, agile, and highly secure network environments.

Nile Wired Access Management FAQ

Why do we need Wired Access Management?

Nile requires all wired devices to be authenticated before accessing the network. The Nile Access Service supports three different wired authentication methods:

1. Wired 802.1X authentication (requires a RADIUS server)
2. Wired RADIUS MAB authentication (requires a RADIUS server)
3. Nile Portal Wired Access management authentication

Can I upload a list of Wired pre-approved devices to Access Management?

Yes, you can upload a list of pre-approved devices to the Nile Access Management by uploading a CSV file via the Nile Customer Portal (Settings > Access Management > Wired). The CSV file should include the following information:

- MAC address: The device's MAC address (mandatory)
- Segment: The network segment the device will be assigned to (required for "Allow" status, optional for "Deny")
- Lock to Port: Lock the device to a specific switch port (optional)
- Site, Building, Floor: Restrict the device to a specific geographical location (optional)
- Allow or Deny: Specify whether to allow or deny access for the device (mandatory)

Can I Disable Nile Wired Device Authentication?

No, the Nile network is designed with security best practices, and you cannot disable wired device authentication entirely. However, you can add a catch-all "allow all" policy (not recommended) to grant network access to all devices, assigning them to a specific segment. This policy can be enabled in the Nile Customer Portal (Settings > Access Management > Wired > Add Device > Allow all MACs).

Can I Enable Nile Auto Wired Device Authentication for a Specific Vendor or Device Type?

Yes, you can create a wired device authentication policy for a specific device vendor or type using the Organizational Unique Identifier (OUI). The OUI is the first 24 bits of a MAC address that is used as a globally unique identifier assigned by the IEEE to identify network devices.
You can enable the OUI-based policy in the Nile Customer Portal (Settings > Access Management > Wired > Add Device > OUI/MAC), where you can select the segment, status (Approved/Denied), and geographical scope for the OUI-based policy.

What is Nile Wired Access Management Lock to Port?

The "Lock to Port" feature will lock a device's approval to a specific Nile switch port when the device connects for the first time. If the wired device is moved to a different port or a different switch, the Wired Access Management policy will be changed from "allow" to "deny", and the Nile portal administrator will need to allow the device again.
You can enable the "Lock to Port" feature in the Nile Customer Portal (Settings > Access Management > Wired > Add Device) by entering the OUI (for multiple devices) or MAC (for a single device), selecting a specific segment, and optionally choosing the geographical scope.

What is Wired Access Management Geo Scope?

The Wired Access Management Geo Scope is a feature that limits wired device authentication pre-approval to a specific location (site, building, or floor). If a wired device is moved to a different location, the Wired Access Management policy will be changed from "allow" to "deny", and the Nile portal administrator will need to allow the device again.
You can enable the Geo Scope in the Nile Customer Portal (Settings > Access Management > Wired > Add Device) by entering the OUI (for multiple devices) or MAC (for a single device), selecting a specific segment, and choosing the geographical scope (site, building, or floor).

Can Administrators Pre-Approve Devices Based on Device Make, Model, or Software?

Yes, the Nile Access Service can fingerprint devices and allows administrators to create fingerprint-based rules to pre-approve devices. You can navigate to "Settings > Access Management > Wired > Add Devices" in the Nile Customer Portal. Nile has an extensive database of device models, makes, and operating systems that can be used to create these rules. When you start typing the name of your device, the system will auto-populate and display the matching entries in our database.

What If My Device is Not in Nile's Database?

If your device is not in the Nile database, the administrator will need to use the MAC address or Organizational Unique Identifier (OUI) for pre-approval. You can reach out to Nile support and provide the details of your device, so it can be reviewed and added to the database at a later date.

How Does Fingerprint-Based Approval Work?

Nile's device fingerprinting works as follows:

1. The exact MAC address rule match always takes precedence.
2. If there is no exact MAC address match, the device will be matched against a fingerprint rule.
3. If there is no fingerprint rule match, the device will be matched against an OUI rule.
4. If there are no other matching rules, the device will be assigned to the "All" rule.

When a new device connects to the network and does not have an IP address, Nile will use limited information like the MAC address to attempt a fingerprint match. To get the device a temporary IP address, you need to create an "All" rule with a quarantine or Internet-only segment. Nile's fingerprinting uses parameters like MAC address, DHCP, DNS transactions, and User-Agent data to accurately match the device.

If the device does not match the fingerprint rule, it will be placed in the segment defined by the "All" rule. Once the device gets a temporary IP and starts communicating, Nile will fingerprint it and automatically move it to the correct fingerprint-based segment, updating the device's IP address accordingly. Nile will learn the device's fingerprint and create a specific entry for it going forward.

What Happens If I Create an Exact MAC Address Entry for a Device?

If you create an exact MAC address entry for a device with a specific segment assignment, Nile will not automatically move that device to a different segment based on fingerprinting. Devices matching an exact address or OUI rule will not be moved automatically. It is recommended not to create exact MAC address or OUI entries for devices you want to onboard using fingerprinting.

What If Nile Fingerprints a Device Incorrectly?

If a device is fingerprinted incorrectly, Nile recommends removing the device from the cache and adding the exact MAC address. You can then contact Nile support to provide the device details, so we can evaluate and add it to our database.

What Happens If a Device Matches Multiple Fingerprint Rules?

When a device matches multiple fingerprint rules, the most specific rule will take precedence. For example, a rule for "Avaya IP Phone 250" will win over a more general "Avaya" rule.

What If I Create New Rules After Devices Are Already Connected?

Rules need to be created before connecting the devices. When a device connects, Wired Access Management will match it against the existing rules. If there are no matching rules, a device entry will be created with a "waiting for approval" status. To have a new rule applied to an existing

device, you will need to delete the device entry and disconnect/reconnect the device to apply the new rule.

Nile is adding an enhancement to automatically verify all existing entries with a "waiting for approval" status after a new rule is created. If the device matches the new rule, its status will automatically change to "allow" or "deny" based on the new rule.

What Happens If We Delete an Existing Rule?

Deleting an existing rule will not impact any existing device Wired Access Management entries. It will only affect the addition of new devices. When a new device is added, if it matches a rule, a specific entry will be created for that device. The only impact would be if both the rule and the device entry were deleted - in this case, the device status will change to "waiting for approval" and require manual approval.

Read Next

Revision #7
Created 20 March 2024 18:21:59 by JR
Updated 28 March 2024 21:53:20 by JR