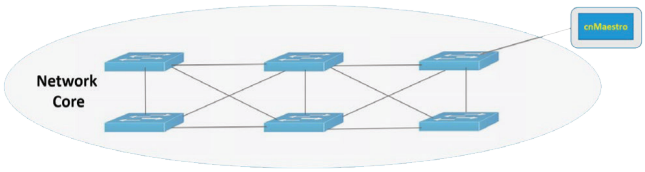
Cambium Networks™

AUTOMATED CONFIGURATION WITH

Policy Based Automation

Zero Touch Configuration and network access policies are important concepts that address the challenges of managing next generation enterprise networks and provide measurable benefits to network administrators. Cambium Networks' Policy Based Automation (PBA) feature fully automates these features to optimize network performance and end user satisfaction. Devices can be added, moved and removed with ease to quickly ensure high user satisfaction as the network evolves.

PBA is a feature that is available today on cnMatrix™, Cambium Networks' portfolio of cloud-managed, enterprise-grade, Layer-2/Layer-3 Ethernet switches. As a fully managed enterprise solution, cnMatrix (deployed with the cnMaestro™ management system) provides network operators with an automation system that is easy to configure, manage and maintain.



Day Zero Core Infrastructure

Automatic Detection Enables "Plug and Play" Operation

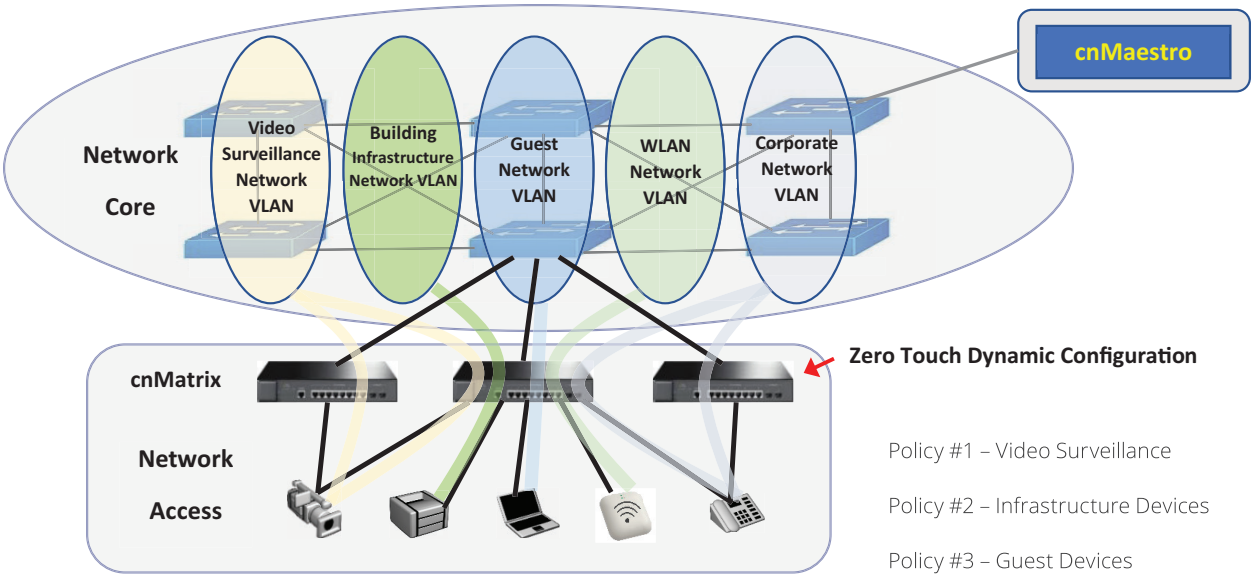
- Saves time
- Reduces errors
- Consistent cleaning
- Leverages IT skill

An overall network architecture is established during the initial deployment phase and remains relatively static. The real action takes place at the network edge where access for devices and users is provided. Additions, moves and changes are a frequent occurrence. Edge connection requirements can be significantly different across devices. Configuring these connections requires specific knowledge about the needs and privileges of the devices being connected. Switch configuration is typically required for each connecting device, such as VLAN assignments, port settings, Quality of Service (QoS) parameters and security settings. Provisioning these settings manually requires network connectivity to the switch, is time-consuming and is-error prone. A significant cause of network outages is due to misconfigurations where one small typing mistake can block an entire team's productivity or open an exploitable security hole. Automating configuration can minimize downtime and simplify troubleshooting.

The network switch needs to dynamically recognize devices and automatically apply predefined policies that perform the required switch configuration. Policies can be customized on a per-switch basis or centrally managed and distributed depending on the needs of the organization. These policies can be developed and validated prior to deployment, eliminating potential issues and ensuring uniform configuration throughout the network. Policies can be simple, acting as a general catch-all; they can also be complex, identifying and satisfying the special access needs of devices as determined by the network administrator. Lastly, since policy-based switch configuration is dynamic, it is automatically cleared once a device is disconnected. This rapidly closes potential security holes and returns edge access to a known consistent state.

Each of these individual capabilities is provided by the cnMatrix PBA feature. As a core cnMatrix component, PBA is engineered to exceed both the basic and advanced needs of a network administrator. Simplified device configuration and eliminated issues lead to saved time, conserved resources and reduced cost of ownership. Key PBA advantages include:

- Automation of 'Adds,' 'Moves,' and 'Changes' of edge devices
- Elimination of error-prone manual configuration data entry
- Simplified and reduced troubleshooting
- Each port is treated equally
- Enhanced security by auto-segmenting devices
- Better leverage of skilled IT resources
- Reduced expenses required for deployment and operation



PBA USE CASES

PBA can be used to automate the configuration that is necessary when adding, moving or changing network connections. For example, policies can be created for all Wi-Fi access points, all video surveillance cameras or any other type/class of device. You can have a different policy for your indoor access points versus your outdoor access points. If preferred, policies targeting devices from a specific manufacturer can be used as well. There are no limits to the types of devices for which PBA policies can be used.

PBA OPERATION

The operating principles behind PBA are straightforward. PBA policies are defined by the network administrator. Each policy contains device detection criteria and associated actions that are initiated when a matching device is detected. When the match is no longer valid, all PBA-based configuration changes are automatically removed.

PBA device detection capabilities are easy-to-use and flexible. The switch leverages several mechanisms to learn about connecting devices, including Link Layer Discovery Protocol (802.1ab LLDP) data and MAC addresses. If this information matches the device identification criteria specified by a policy, the policy's actions are applied. Applied actions include switch and/or port-related configuration. Device detection is entirely port independent. All ports are treated equal. Preconfiguring a port for specific devices is no longer required, and administrators can now connect and reconnect any device to any port.

A wide array of actions are available to be initiated. The most common operation performed is port segmentation. This entails dynamically creating VLANs and updating port membership for those VLANs. VLAN membership may also be updated on switch uplink ports, automating the configuration of a complete virtual data path through the switch. The resulting device auto-segmentation ensures that a secure environment is maintained. Devices will only have access to the permissible network segments and are blocked from accessing all others. Port security settings can automatically be updated as well to correctly mark and prioritize flows for appropriate upstream handling.

All configuration as a result of policy actions are dynamic in nature. Dynamic configuration is cleared once the associated PBA policy is no longer being applied to a port. When a device connection is terminated or the administrator decides a PBA policy is no longer needed, all related settings revert to their previous state.

All of these operations occur transparently without IT intervention. Devices are detected, suitable configuration updates are applied and the configuration is cleared when no longer necessary, all with zero-touch.

PBA is fully managed through the full complement of network management interfaces: CLI, Web-GUI, SNMP and cnMaestro™ (Cambium Networks' on-premises and cloud-based management system). All of these management interfaces offer full control over PBA functionality. When creating policies with cnMaestro, the policies will be pushed to all switches in the network. In this case, every port of every switch will be capable of applying the same policies. The administrator can plug his devices into any port of any switch for a complete zero-touch experience.

Every network operator seeks methods that optimize performance and minimize intervention. PBA provides a proven automated tool set that enables network operators to meet this goal.

Cambium Networks™

Cambium Networks, Ltd.
3800 Golf Road, Suite 360,
Rolling Meadows, IL 60008