EXECUTIVE SUMMARY

Many businesses employ value added resellers (VARs) and MSPs to provide them with networking services because many do not have internal IT resources. Many businesses are structured to have regional offices that oversee activities at many, individual retail locations. These businesses include gas stations, fast food, clothing stores and many others. Regardless of the type of business, they have many common needs. They all want and need feature-rich Wi-Fi and wired networking. And, because few have on-site IT staff, they need systems that are easy to install and are easy to manage remotely.

NETGEAR commissioned Tolly to evaluate its Insight Pro medium business and MSP solution and compare it to offerings from Aruba, Meraki, and Ubiquiti. Tests showed the NETGEAR solution to be demonstrably superior overall to the alternatives for this market offering in part: 1) an architecture designed for multi-customer, multi-location businesses, 2) simple and flexible setup, 3) highly-functional cloud portal, and 4) most extensive management via a mobile app. See Table 1 for a summary.

THE BOTTOM LINE

NETGEAR Insight Pro provides:

1. Solution architecture designed for multi-customer, multi-location businesses
2. Simple and flexible device setup
3. Multi-role management and monitoring
4. Highly functional cloud portal
5. Extensive management via mobile app
6. Controller-free site solution

Table 1

<table>
<thead>
<tr>
<th>Area</th>
<th>Solution</th>
<th>NETGEAR</th>
<th>Aruba</th>
<th>Meraki</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architected for multi-customer (i.e. MSP) business</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌**</td>
<td>✔*</td>
</tr>
<tr>
<td>Architected to provide separate access based on user roles and</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>✔</td>
<td>❌</td>
</tr>
<tr>
<td>responsibilities; e.g., business owner and technical administrators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for remote access to other sites</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Customization of cloud portal via widgets</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Most extensive management via mobile app</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Tech support and case management integrated into mobile app</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Automatic status change emails</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>Automatic weekly summary report emails</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Advanced features</td>
<td></td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
</tr>
</tbody>
</table>

Notes: See report text for further information on "check minus" entries. Generally this indicates support that is not as extensive as NETGEAR. * Two different management approaches available, see report details. ** Not categorized as business owner vs. technical admins.

Source: Tolly, May 2023
Test Results

For this test, Tolly engineers went through the process of defining and building a multi-location business environment to determine the specific capabilities of each solution. See Table 5 for component details.

Business Organization & Solution Architecture

Just as a sturdy house cannot be built on a weak foundation, the underlying architecture of an IT solution - the foundation - has the greatest impact on how a solution can deliver both today and in the future. A solution that is fundamentally deficient can be a nuisance in basic deployments and potentially a major problem in larger deployments.

Business Organization

The most fundamental element for many businesses is the ability to group multiple locations together for the purpose of centralized setup, monitoring, ongoing management and reporting. This capability is a core attribute of NETGEAR Insight Pro.

Aruba Central\(^1\) can define multiple organizations when it is set up in MSP mode. Meraki provides for multiple organizations within an account, however each organization is completely separate.\(^2\) That means that a Meraki Cloud Controller license would need to be purchased for each organization. With Ubiquiti the options available depend upon which Ubiquiti management architecture is used. (See Solution Architecture.)

Within medium businesses, it is evident that the roles of business owner, business manager, and IT technician will generally be separate. The business manager will be interested in confirming the operational status of a given location and being able to access management alert and reports but generally will not want to make any changes to the IT environment. That job would be for an IT specialist.

## Business-Level Organization Support

<table>
<thead>
<tr>
<th>Area</th>
<th>NETGEAR</th>
<th>Aruba</th>
<th>Meraki</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define End-Customer Organization/Account</td>
<td>✔</td>
<td>✔***</td>
<td>✔</td>
<td>✘*</td>
</tr>
<tr>
<td>Define Multiple Locations within each End-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Customer Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define Business Owner</td>
<td>✔</td>
<td>✔-**</td>
<td>✔-**</td>
<td>✘</td>
</tr>
<tr>
<td>Define/Assign Manager</td>
<td>✔</td>
<td>✔-**</td>
<td>✔-**</td>
<td>✘</td>
</tr>
</tbody>
</table>

Note: * The Ubiquiti architecture provides only for defining individual sites and does not provide for any grouping of sites for management purposes. ** None of the other solutions provide for access based on user roles and responsibilities (e.g., business owner or IT manager) although admins can be defined with varying degrees of control. ***When deployed in MSP mode.

Table 2

Source: Tolly, May 2023

\(^1\) Aruba Instant On is an alternative to Aruba Central and is outside the scope of this report.

\(^2\) [https://documentation.meraki.com/General_Administration/Organizations_and_Networks/Meraki_Dashboard_Organizational_Structure](https://documentation.meraki.com/General_Administration/Organizations_and_Networks/Meraki_Dashboard_Organizational_Structure)
(Management capabilities will be covered later in this report.) With the others only an “admin” identity is supported. Within the “admin” role, various functions are available. Aruba for various levels of read/write combinations for at the network level but does not appear to allow network-by-network administration. Aruba also provides various read/write levels to its ClearPass Device Insight application. Meraki defines overall “organization" access or access to individual “networks" defined within the organization. Ubiquiti provides for global and site based permissions including a read-only access to all sites. See Table 2, on page 2, for a summary.

Solution Architecture

The NETGEAR solution is architected “top down” with the management solution at both the cloud portal and mobile app levels designed to configure, monitor and manage each location without requiring any additional equipment at each site. NETGEAR Insight Pro provides a clean, easy-to-use GUI that is consistent across web and mobile devices. See Figure 1.

Similarly, Aruba and Meraki network locations can be managed without requiring any additional equipment at each site. Ubiquiti offers two approaches.

Ubiquiti: A Tale of Two Architectures

Ubiquiti implements and offers two different management architectures. They are structured differently and have different cloud management interfaces and different cost structures.

The Ubiquiti legacy architecture requires a local controller computer at each location and each site is managed separately with no per-device management license cost.

Local Controller

In this legacy architecture, which is still offered and supported, all management functionality is site-centric. Ubiquiti requires a separate local controller for every collection of networked devices. For this approach, their “cloud management” consists of making a remote, browser connection to the local controller.

The controller function, known as the “UniFi Network Application” when implemented in software can be installed on a standard computer. The computer running the controller, however, must always be connected to the local network via Ethernet or Wi-Fi and must always be powered on with sleep-mode disabled.

---

**NETGEAR Insight Pro Example Summary Screen - Web GUI**

Source: Tolly, May 2023
Alternatively, Ubiquiti can provide the local controller function via the “UniFi Cloud Key Gen2 Plus” device. This is a member of the UniFi OS Console family and the device is a dedicated management controller (computer), roughly 5”x1”x5” in size, that receives power from a PoE port of the switch and implements the local controller.

Whether implemented in an existing computer or purchased as standalone hardware, the local controller is a hidden, per-site cost for the Ubiquiti solution.

Ubiquiti offers other “Dream” branded hardware, listed as “UniFi OS Consoles,” that include an integrated controller and also provide support for other applications beyond networking. Discussion of those solutions is beyond the scope of this test.

**Cloud Console**

In 2022, Ubiquiti introduced the UniFi Cloud Console. With this solution existing networks/locations can be imported into one or more “sites” and managed from a single console. Migrating to Cloud Console appears to obviate the need for the UniFi Network Application to be present at each site. Users pay $29 per month for a cloud subscription to manage up to 500 devices and $299 per month to manage up to 2,000 devices.

While the UniFi Cloud Console allows for defining and managing multiple sites within one instance, it does not provide for defining multiple, separate customers. The cloud console user would have to track which sites belong to which customer.

**Remote Management Functionality: Mobile & Cloud**

Feature-rich, intuitive remote management is essential to providing the highest uptime and the lowest support costs. NETGEAR provides the most flexibility when adding devices, a consistent and intuitive interface across both its mobile app and cloud portal, and provides for customizing the cloud portal via widgets. NETGEAR provides two-factor authentication, as do the other vendors. NETGEAR offers more than a dozen dashboard widgets. These include: System Health, Wireless Clients, Port Utilization, Topology, Notifications, PoE Power Utilization, and several other utilization widgets.

Meraki’s dashboard provides overall system health information, client utilization, application data usage, and individual client statistics. The Meraki dashboard does not appear to be configurable.

Aruba’s dashboard has multiple options for displaying various elements of network information. The “Global” view provides overall network health, WAN health, and AI insights via different tabs. Most screens can be viewed either in summary or list mode. The sidebar provides groups of management, analysis, and maintenance sub-tasks. The Aruba dashboard content elements do not appear to be configurable.

Ubiquiti offers two different consoles, the local network application and the Cloud Console. Both console environments are much more basic than the other solutions primarily offering device and traffic information. The network application appears to provide more information than the Cloud Console. Neither management interface appears to be configurable.

The NETGEAR Insight mobile app provides for configuring locations, adding and setting up devices, setting up VLANs, and scheduling updates for firmware upgrades.

The Aruba Central mobile app presents a clear summary of APs, switches, and gateways on its main screen. It provides detailed information about clients and provides troubleshooting tools and an alert log.

The Meraki mobile app main screen provides a summary of network devices, and clients for the past day, week, month, or last two hours. The app also shows useful information such as top applications, wireless health (e.g. failed connection %), and a list of SSIDs along with a client count.

When one starts the Ubiquiti mobile app no information is available until the user selects either a local controller or a “Cloud Console” with which to connect. As testers had the devices under the control of the local controller, that option was evaluated in detail at the device level.

The UniFi app provides a count of devices and clients along with a Wi-Fi experience chart that moves with time during the day, and a list of most active clients. The app allows the user to modify switch and AP settings. It also allows customers that use Ubiquiti gateways/firewalls to modify the configurations of those devices.

These and other features are detailed below and results summarized in Table 3.

**Add & Setup Devices**

Tolly evaluated the options available for adding new devices and performing initial device configuration.

NETGEAR provides for three different methods for adding devices via the Insight mobile app. The simplest method is to
The NETGEAR mobile app can be used to add a new device simply entering its serial number into the app.

NETGEAR also provides for bulk addition of devices. This provides an efficient method for MSPs to deploy new sites.

With Aruba Central, preconfigured switches will automatically connect to Aruba Central. For switches in factory default configuration, one must manually add either the serial number or the Ethernet MAC address via the Aruba Central console.

### Mobile App & Cloud Portal: Remote Management Functionality

<table>
<thead>
<tr>
<th>Area</th>
<th>Function</th>
<th>NETGEAR</th>
<th>Aruba</th>
<th>Meraki</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add &amp; Setup Devices</td>
<td>Via cloud portal</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Mobile via network scan</td>
<td>✔️</td>
<td>✘</td>
<td>✘</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Mobile via QR or barcode scan</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✘</td>
</tr>
<tr>
<td></td>
<td>Mobile via serial number</td>
<td>✔️</td>
<td>✘</td>
<td>✔️</td>
<td>✘</td>
</tr>
<tr>
<td>Notifications &amp; Reports</td>
<td>Automatic status emails</td>
<td>✔️</td>
<td>✘</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Report Customization</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✘</td>
</tr>
<tr>
<td></td>
<td>Report management in cloud portal</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✘</td>
</tr>
<tr>
<td></td>
<td>Notifications/alerts in mobile app</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✘</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>Custom login option</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

### Power over Ethernet Management

<table>
<thead>
<tr>
<th>Function</th>
<th>NETGEAR</th>
<th>Aruba</th>
<th>Meraki</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create PoE schedule</td>
<td>✔️</td>
<td>✘</td>
<td>✘</td>
<td>✔️</td>
</tr>
</tbody>
</table>

### Firmware Update Management

<table>
<thead>
<tr>
<th>Function</th>
<th>NETGEAR</th>
<th>Aruba</th>
<th>Meraki</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create firmware update schedule</td>
<td>✔️</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
</tr>
</tbody>
</table>

### Cable Test

<table>
<thead>
<tr>
<th>Function</th>
<th>NETGEAR</th>
<th>Aruba</th>
<th>Meraki</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run cable test on specific ports</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Note:** See report text for details. Some specifics of functions vary across vendors with “check” marks.

Source: Tolly, May 2023
APs and switches can also be added via the Aruba Central mobile app by scanning the barcode found on the device.

The Meraki mobile app allows new devices to be added via scanning the barcode, entering the serial number, or adding “from inventory” if devices have been entered into the company “inventory.”

With the Ubiquiti UniFi mobile app, a device can be added via scanning for new devices when physically near the new devices.

All vendors provide for adding devices via the cloud portal. With Ubiquiti, the process is called device “adoption.”

Notifications & Reports

Clear, concise and easy management reporting is also an essential element of keeping a business running.

NETGEAR provides automatic, proactive email confirmation of new devices being added to environments. An automatic status message is generated should a device go offline and again when the device goes back online.

NETGEAR provides concise reports for each business organization with the option of weekly or monthly timeframe. The report contains summary information including: number of APs and switches, power usage, upload/download data consumption, client count, system health, recent critical notifications and network uptime percentage.

Tolly could not find similar detailed email status functionality in the Aruba solution though Meraki does provide an option for email subscription to overall system outage alerts. Ubiquiti Cloud Console provides “Push Notification Settings” for a dozen different events within the areas of updates, admin activity, and backups.

All vendors except Ubiquiti provide for report management from their respective web portals.

Aruba Central mobile app and the Meraki mobile app also provide an “alert” notifications tab.

Captive Portal

Many business want guests to register before using, for example, an in-store Wi-Fi network. NETGEAR offers “Instant Captive Portal” that is licensed separately and provides custom login options including support for social media logins.

Aruba provides a captive portal that can be used to register guests or authenticate business users against an external server or the internal database of the managed device. Meraki notes that a captive portal, i.e., “splash page,” can be set up for switches or wireless access points. Ubiquiti provides this function with their “Hotspot Portal.”

Power over Ethernet Management: PoE Schedule

Businesses may wish to restrict availability of Wi-Fi access to certain hours of the day and/or days of the week. For example, a store may not want its Wi-Fi and Internet connection to be available to passersby when the store is closed.

Creating a PoE schedule allows this granular level of control over WLAN APs (that can save power). NETGEAR provides for granular PoE scheduling that allows custom start and end times along with an “all day” option that would be useful for easy configuration of businesses that might be closed on weekends.

Schedules can be set as one time or recurring and are on a port-by-port basis. NETGEAR PoE schedules can be set equally easily in both the mobile app and cloud portal.

Aruba and Ubiquiti do not offer any PoE scheduling function. While Meraki does offer this function, via the “port schedules” functionality, it can only be configured via their cloud portal and not via their mobile app.

Firmware Update Management: Scheduled Updates

It is important that device firmware be kept up to date but equally important that the updates be scheduled so as not to disrupt business activities.

NETGEAR provides for scheduling firmware updates where the administrator can specify both the start date/time and the end date/time of the update window. The user can optionally choose to open the update window again automatically on a daily, weekly or monthly basis.

Ubiquiti also allows firmware updates via the mobile app. Aruba and Meraki only allow firmware updates to be managed via their cloud portals.

Cable Test

The network infrastructure vendor cannot control the cabling used to connect devices to the network. Frequently, for a variety of reasons, the physical cable is the faulty component that can be the source of trouble - and user downtime. Thus, being able to run a per-port cable test remotely is an important problem isolation and management tool.

NETGEAR provides per-port cable test capability from both its mobile app and its
cloud portal. Meraki provides cable test capability only from its cloud portal. Aruba and Ubiquiti do not provide any cable test functionality from either mobile apps or web portals.

**Additional Diagnostics & Troubleshooting**

While beyond the scope of the comparative evaluation, Tolly noted that NETGEAR provides an impressive set of diagnostic and troubleshooting features, all of which are available on the mobile app and intuitive to use.

In addition to the aforementioned cable test function, the mobile diagnostics screen provides multiple functions for troubleshooting directly as well as for working with NETGEAR to diagnose and/or replace a device.

**Port Mirroring.** Allows network technicians to send a copy of traffic from one port to another available port to capture, for example, network traffic for additional analysis.

**Share Diagnostics.** This feature allows a user to email diagnostics information for a given device directly to a specified email address which would, presumably, be a contact at NETGEAR support.

**Factory Reset & Remove.** This provides a one-click method to both reset the device to factory settings and remove it from the NETGEAR Insight Pro management system. Once reset, the device can be re-added.

**Configuration Backup.** Create time-stamped backups of system configuration with customer-defined names and descriptions.

**RMA.** With this feature one can either restore an existing backup of a device configuration or replace an existing device with a new device while keeping the existing device configuration.

**Troubleshoot.** This option brings up another menu of useful IP network tools: 1) Ping test, 2) DNS Lookup, and 3) Traceroute.

These tools help network technicians to debug connectivity issues.

**Secure Diagnostics Mode.** Enabled at the device level, this mode, according to NETGEAR, “connects your Insight device to NETGEAR’S diagnostic server, allowing support personnel to remotely diagnose your system”.

**Cloud Portal Troubleshooting.** From the Insight cloud portal, there are additional troubleshooting options. As in the mobile app, the admin can initiate a “ping” from a selected device to any other Internet address to determine end-to-end latency. The DNS Lookup, and Traceroute functions are also provided.

The admin can also run an “Ookla Speedtest” that measures Internet connection upload speed, download speed, and latency from the device under test to the Ookla web server.

---

### Advanced Features

<table>
<thead>
<tr>
<th>Area</th>
<th>NETGEAR</th>
<th>Aruba</th>
<th>Meraki</th>
<th>Ubiquiti</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Energy Efficient Mode*</td>
<td>✔</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>mDNS (Multicast DNS) Gateway</td>
<td>✔</td>
<td>✔</td>
<td>✘</td>
<td>✔</td>
</tr>
<tr>
<td>MPSK (Multi Pre-Shared Key for Wi-Fi)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✘</td>
</tr>
<tr>
<td>Location Device Groups**</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✘</td>
</tr>
</tbody>
</table>

Note: *NETGEAR EEM is a proprietary technology. Tolly could not find any similar offering from the other vendors.

**Location Device Groups** is NETGEAR’s name for being able to group devices at a location that would have common (i.e., the same) configurations. Meraki “group policies” allow for policies, such as firewall rules or traffic shaping policies, to be applied to multiple devices.

Source: Tolly, May 2023
Advanced Features

This section compares some advanced features that simplify management and provide additional energy efficiency. See Table 4.

AP Energy Efficient Mode (EEM)

NETGEAR has implemented what it terms “energy efficient mode” and notes that it can reduce the energy use of APs by 20%. Once enabled via the portal, EEM is activated when an AP has no client connections over a three-minute period. When active, EEM reduces the number of Wi-Fi streams to 1x1 on each band. When a wireless device connects, EEM deactivates.

Tolly did not find any similar function in the other solutions.

mDNS (Multicast DNS) Gateways

mDNS is a protocol that resolves .local hostnames without the need to query a DNS server. Also known as the “Bonjour” protocol, it is a “zero configuration” feature that allows communications between stations on the same LAN without prior configuration.

All solutions evaluated support mDNS.

Multi Pre-Shared Key (MPSK) for Wi-Fi

MPSK allows for a single SSID to be accessed using multiple, different, pre-shared keys. This allows for easier management and maintenance, for example, for IoT devices as these can be assigned to use a different pre-shared key than end users. That way if, for example, the end user shared key is compromised and must be changed, the IoT devices remain unaffected.

NETGEAR, Aruba, and Meraki support MPSK. No reference to this feature could be found for Ubiquiti.

Insight Device Groups

Insight Pro Admins can set up location-level Device Groups for Insight managed access points, routers and switches that share common configurations.³

Aruba provides a similar function with its configuration groups. Meraki provides for policies to be applied across multiple devices. Tolly did not find any similar function for Ubiquiti.

Test Setup & Methodology

Tolly engineers built out a multi-location environment for each vendor using new hardware “out of the box” and each vendor’s cloud portal and mobile application. The details of the components used in the evaluation are found in Table 4.

For the mobile app, the version for Apple iOS was used for all testing. The latest versions of software available were used as of early May 2023.

Tolly went through each step of the setup and management test list and documented feature availability on both the cloud portal and the mobile app. The list of test areas can be found in Tables 2 through 4.

³ https://kb.netgear.com/000065639/What-are-Insight-Device-Groups
## Systems Evaluated

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Device Type</th>
<th>Device Name</th>
<th>Model</th>
<th>Advertised Price (USD)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETGEAR</td>
<td>PoE LAN Switch</td>
<td>NETGEAR 8-Port Multi-Gigabit/10G Ethernet Ultra60 PoE++ Smart Switch with 2 SFP+ Ports</td>
<td>MS510TXUP</td>
<td>$749.99</td>
<td>10-ports. Cloud managed. 8 PoE++ ports.</td>
</tr>
<tr>
<td></td>
<td>WLAN Access</td>
<td>NETGEAR Cloud Managed WiFi 6 (WAX625) AX5400 Dual-Band PoE Multi-Gig Insight Managed WiFi 6 Access Point</td>
<td>WAX625</td>
<td>$269.99</td>
<td>802.11ax 4x4. Cloud Managed. Power adapter extra.</td>
</tr>
<tr>
<td></td>
<td>Management Software</td>
<td>Insight Pro Web Portal, Cloud Version 6.10.6.9, Mobile App 6.10.5. Insight Pro &lt;$22 per year per device sold via distribution channel. NPR1SNG1-10000S. First year free for each device.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aruba</td>
<td>PoE LAN Switch</td>
<td>Aruba 2930M 24G Smart Rate POE Class 6 1-slot Switch</td>
<td>2930M (ROM668)</td>
<td>$10,140.00</td>
<td>24 Autosensing 1/2.5/5GBaseT ports PoE Class 6</td>
</tr>
<tr>
<td></td>
<td>WLAN Access</td>
<td>Aruba AP 555</td>
<td>JZ356A</td>
<td>$1,990.00</td>
<td>4x4 (2.4GHZ), 8x8 (5GHZ)</td>
</tr>
<tr>
<td></td>
<td>Management Software</td>
<td>Aruba Central Foundation - Q9Y60AAE - $505 for 5-year license.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meraki</td>
<td>PoE LAN Switch</td>
<td>Meraki MS350-24X</td>
<td>MS350-24X-HW</td>
<td>$6,623.52</td>
<td>24-port Layer 3 switch with optional mGig with UPoE (plus enterprise license).</td>
</tr>
<tr>
<td></td>
<td>WLAN Access</td>
<td>Meraki MR44</td>
<td>MR44-HW</td>
<td>1,537.75</td>
<td>4x4 (2.4GHZ), 4x4 (5GHZ)</td>
</tr>
<tr>
<td></td>
<td>Management Software</td>
<td>Cisco Meraki Enterprise Cloud Controller - LIC-ENT-5YR. $752.63 for 5-year license.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ubiquiti</td>
<td>PoE LAN Switch</td>
<td>UniFi Switch 8 60W</td>
<td>US-8-60W</td>
<td>$109.00</td>
<td>8-ports. Cloud managed. (4 ports of PoE.)</td>
</tr>
<tr>
<td></td>
<td>WLAN Access</td>
<td>UniFi U6 Professional</td>
<td>U6-Pro-US</td>
<td>$159.00</td>
<td>802.11AC 2x2:2. 1GbE uplink. Cloud Managed.</td>
</tr>
<tr>
<td></td>
<td>Local Controller (Hardware)</td>
<td>UniFi Cloud Key Gen2 Plus</td>
<td>UCK-G2-PLUS</td>
<td>$199.00</td>
<td>PoE-powered, computer “brick” used as local controller.</td>
</tr>
<tr>
<td></td>
<td>Local Controller (Software)</td>
<td>UniFi Network Application v7.3.82 (Windows 10). No licensing or subscription cost.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Software Cloud Portal</td>
<td>UniFi Cloud Console v2.5.53</td>
<td></td>
<td>$29 per month for up to 500 devices. $299 per month from 501 to 2,000 devices.</td>
<td></td>
</tr>
</tbody>
</table>


Source: Tolly, May 2023

Table 5
About Tolly

The Tolly Group companies have been delivering world-class IT services for nearly 30 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at: http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided “as is,” and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.