TEST REPORT

Tolly.

#218133

September 2018

Commissioned by
NETGEAR

NETGEAR Insight Pro

Comparison of Deployment Architectures & Solutions for Service Providers and Multi-Location Businesses

EXECUTIVE SUMMARY

SMBs often employ Value Added Resellers 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 manage remotely.

NETGEAR commissioned Tolly to evaluate its Insight Pro small business solution and compare it to offerings from Ubiquiti Networks and Zyxel. Tests showed the NETGEAR solution to be demonstrably superior to the alternatives, offering in part: 1) an architecture designed for multi-customer, multi-location businesses, 2) simple and flexible setup, 3) highly-functional cloud portal, 4) full-fledged management via a mobile app, 5) controller-free site solution, and business-class NAS. 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 Full-fledged management via mobile app

6 Controller-free site solution

Business Deployment Architecture & Solution Overview

Area	Solution		
	NETGEAR	Ubiquiti Networks	Zyxel
Architected for multi-customer, multi-location business	✔	✘	✔-*****
Architected to provide separate access based on User Roles; e.g. Business Owner and technical administrators	✔	✘	✘
Support for remote access to other sites	✔	✔	✔
Controller-free site solution	✔	✔	✔
Highly-Functional cloud portal	✔	✔	✔
Customization of cloud portal via widgets	✔	✔-****	✘
Full-fledged management via mobile app	✔	✔	✘
Tech support and case management integrated in mobile app	✔	✔-**	✘
Consistent UI look and feel between cloud & mobile app	✔	✔-***	✘
Highly-granular setup of switches from cloud portal	✔-*	✔	✔
Automatic status change emails	✔	✘	✘
Automatic weekly summary report emails	✔	✘	✘
Business-class network-attached storage (NAS)	✔	✘	✘

Notes: * NETGEAR Insight Pro provides core device configuration functions with additional deeper functions available at the device-level interface. ** Limited with chat support and send email to tech support. *** Local controller interface differs from cloud portal and mobile app. **** Partially available. ***** Multiple organizations under one account, then multiple locations under organization. Does not have the simplified view available with NETGEAR Insight Pro.

Source: Tolly, August 2018

Table 1

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 4 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 small deployments and potentially a major problem in larger deployments.

Business Organization

The most basic element for many businesses is being able to group multiple locations together for the purpose of centralized setup, monitoring, ongoing management and reporting. NETGEAR and Zyxel provide grouping multiple locations or sites under one organization. With Ubiquiti Networks the options available depend upon which Ubiquiti Networks architecture is used. (See Solution Architecture.)

Within small businesses, it is evident that the roles of business owner, 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 inadvertently make any changes to the IT environment. That job would be for an IT specialist.

For many or most small businesses an IT specialist will not be present on-site but will need to perform all or much of the job remotely.

NETGEAR

Insight Pro

Network Solution for Multi-Location Businesses

Tolly. Certified

Tested August 2018

This reality presents two challenges: 1) the need to separate "business" and "IT" operational identities and, 2) providing for feature-rich remote management via cloud portal and a mobile app.

Only NETGEAR provides the option for defining separate "business owner" and "IT manager" roles. (Management capabilities will be covered later in this report.) With Ubiquiti Networks and Zyxel, only an "admin" identity is supported. Within the "admin" role, various functions are available. Ubiquiti Networks provides for global and site based permissions including a read-only access to all sites. See Table 2 for a summary.

Business-Level Organization Support

Area	Solution		
	NETGEAR	Ubiquiti Networks	Zyxel
Define End-Customer Organization	✔	✘*	✔
Define Multiple Locations within each End-Customer Organization	✔	✘	✔
Define Business Owner	✔	✔-**	✔-**
Define/Assign Manager	✔	✔-**	✔-**

Note: * The Ubiquiti Networks architecture provides only for defining individual sites and does not provide for any grouping of sites for management purposes. ** Neither Ubiquiti Networks nor Zyxel implement the concepts of "business owner" or "IT manager." Admins can be defined with varying degrees of control.

Source: Tolly, August 2018

Table 2

Solution Architecture

The NETGEAR solution is clearly 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. This is also the case with Zyxel.

Ubiquiti Networks: A Tale of Two Architectures

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

The Ubiquiti Networks legacy architecture requires a local controller computer at each location and each site is managed separately with no per-device cost. Its cloud architecture provides controller-free management but at a considerable per-device annual cost. For example, the management cost for a network of 50 devices is $21.94 per device, per annum. See Table 4 for additional pricing information.

Local Controller

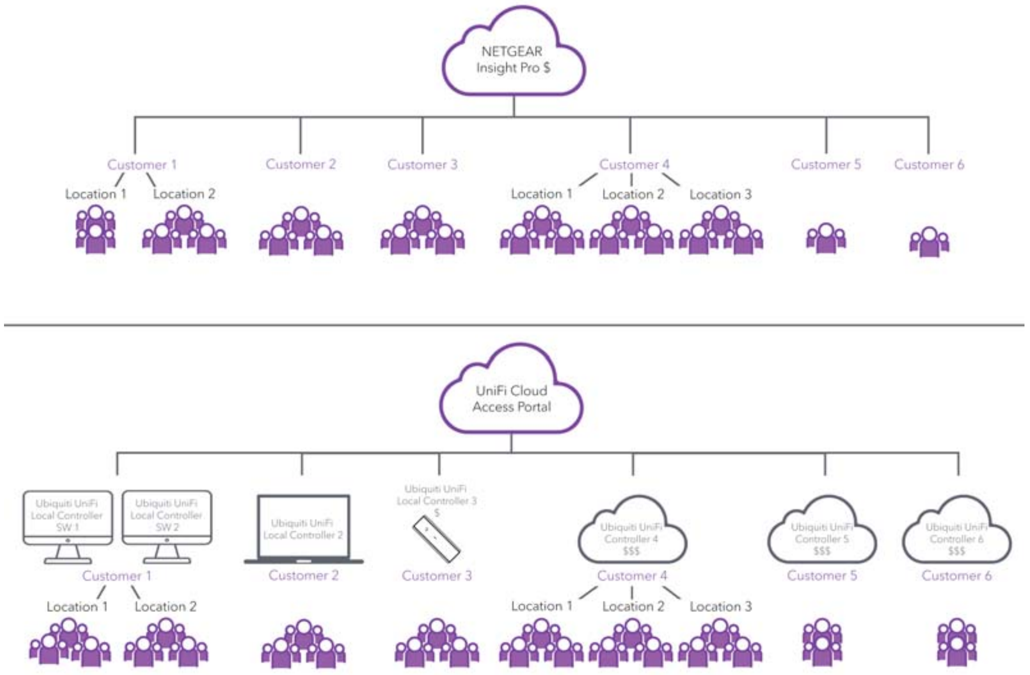
In this legacy architecture, which is still offered and supported, and likely makes up the bulk of deployment, all management functionality is site-centric. That is, even when attempting to manage a multi-site business from the Ubiquiti Networks UniFi cloud portal, the user must "launch" a separate web browser screen to communicate with a specific site. See Figure 1.

Ubiquiti Networks 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. Should the local controller be offline (e.g. "sleeping" computer) or otherwise unavailable, the site cannot be managed.

The local controller is known as the "UniFi SDN Controller." The controller function 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.

Alternatively, can provide the local controller function via the "UniFi Cloud Key Remote Control Device." This device is a dedicated controller (computer), roughly 9"x3"x1" in size, that plugs into a PoE port of the switch and implements the local controller.

Cloud Architecture: NETGEAR vs. Ubiquiti Networks
Consistent vs. Inconsistent, Dual-Architecture Solution


NETGEAR Insight Pro $
Customer 1
Location 1
Location 2
Customer 2
Customer 3
Customer 4
Location 1
Location 2
Location 3
Customer 5
Customer 6
UniFi Cloud Access Portal
Ubiquiti UniFi Local Controller SW 1
Ubiquiti UniFi Local Controller SW 2
Ubiquiti UniFi Local Controller 2
Ubiquiti UniFi Local Controller 3 $
Ubiquiti UniFi Controller 4 $$$
Ubiquiti UniFi Controller 5 $$$
Ubiquiti UniFi Controller 6 $$$
Customer 1
Location 1
Location 2
Customer 2
Customer 3
Customer 4
Location 1
Location 2
Location 3
Customer 5
Customer 6

Source: Tolly, August 2018

Figure 1

From a management perspective, however, nothing changes. In the UniFi cloud portal, the dedicated hardware controller appears the same as a PC-based controller. All configuration still requires the presence of the controller and an active remote session in the controller. In effect, the main UniFi cloud portal provides only the ability to "launch" (to use Ubiquiti Networks' term) into individual controllers. In practice, then, to run or check configurations on, say, 50 sites, 50 separate cloud portal management instances would need to be launched and interacted with individually.

For multiple locations to be managed by the same controller, they need to be on the same network. That means setting up a VPN connection between the two locations.

Cloud Controller

The Ubiquiti Networks cloud controller, as noted, provides for management of sites without the presence of a local controller. As with the local controllers, it is "launched" from the Ubiquiti Networks Cloud Access Portal. Thus, it is, confusingly, a "cloud-under-cloud" implementation.

While the cloud controller allows for defining and managing multiple sites within one instance, it does not provide for defining multiple, separate customers - a requirement for managed service providers.

Thus, it appears that MSPs would be required to pay for a separate cloud controller subscription for each of its customers. This is in stark contrast to the NETGEAR model that allows multiple customers to be managed within a single subscription to NETGEAR Insight Pro.

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. Ubiquiti Networks offers limited portal customization. NETGEAR currently offers widgets that can display storage utilization wireless data usage, switch traffic, and PoE power usage. The mobile app integrates support and case management.

Ubiquiti Networks and Zyxel offer more limited capabilities than NETGEAR with their mobile apps. The Zyxel mobile app interface does not have the "look and feel" of its cloud portal. While the other vendors offer more granular device configuration via the cloud portal, this adds to the complexity of the cloud interface. It is Tolly's view that configuration and management via Ubiquiti Networks and Zyxel's portals requires a higher level of technical skill than required to use the NETGEAR cloud/mobile apps effectively.

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 doing initial configuration. For all vendors, it is assumed that the mobile device is on the same network to which the new device will be connected.

NETGEAR provides for three different methods via the Insight mobile app. The simplest method is simply to connect the new device to the network and then use the mobile app to scan for new devices. New devices can easily be selected and added.

The NETGEAR mobile app can also use the phone or tablet's camera to scan the QR code or barcode present on the underside of each NETGEAR device.

Finally, the NETGEAR mobile app can be used to add a new device simply entering its serial number into the app.

By contrast, the Ubiquiti Networks mobile app only supports adding devices via network scan. The Zyxel mobile app only provides for adding a device by scanning the QR code/barcode on the underside of the device.

All three vendors provide for adding devices via the cloud portal.

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. Similarly, should a device go offline, an automatic status message is generated - and again when it is back online. Neither of the other vendors provide these features.

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

Mobile App & Cloud Portal: Remote Management Functionality

Area	Function	NETGEAR		Ubiquiti Networks		Zyxel	
Add & Setup Devices	Via cloud portal	✔		✔*		✔	
	Mobile via network scan	✔		✔		✘	
	Mobile via QR or barcode scan	✔		✘		✔	
	Mobile via serial number	✔		✘		✘	
Notifications & Reports	Automatic status emails	✔		✘		✘	
	Automatic weekly or monthly organization status summary via email	✔		✘		✘	
	Report management in cloud portal	✔		**No report available. Email alerts in beta**		**Support manual generation of site-wide report**	
	Notifications/alerts in mobile app	✔		✔		✘**	
		Mobile	Cloud	Mobile	Cloud	Mobile	Cloud
Power over Ethernet Management	Create PoE schedule	✔	✔	**Function not supported**		✘	✔
Firmware Update Management	Create firmware update schedule	✔	✔	**Function not supported**		✘	✔
Facebook Captive Portal	Create a Wi-Fi portal using FB login	✔	✔	✘	**in beta**	✘	✔
Cable Test	Run cable test on specific ports	✔	✔	**Function not supported**		✘	✔
Network-Attached Storage	Add to network, monitor status	✔	✔	**NAS not offered**		**NAS not offered**	

Note: * The Ubiquiti Networks functionality depends upon whether one is using their legacy local controller approach or their cloud-based management. With the local controller architecture, the cloud access portal simply launches a connection to the local controller
** Only individual device status available when "drilled down" to that device.

Source: Tolly, August 2018

Table 3

notifications and network uptime percentage.

Neither of the other vendors provide automatic reporting or location-specific reports.

Ubiquiti Networks does not offer a reporting function and alerts via email was in beta at the time of the test. Zyxel supports manual generation of reports but the report is site-wide and cannot be generated on a per-location basis.

The NETGEAR mobile app provides automatic notification for events such as a device going offline, back online or firmware update.

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 (and saves 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.

Ubiquiti Networks does not offer any PoE scheduling function. While Zyxel does offer this function, it can only be configured via their Nebula 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 can 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 Networks does not offer any scheduled firmware update function. While Zyxel does offer this function, it can only be configured via their Nebula cloud portal and not via their mobile app.

Facebook Captive Portal

Many business want guests to register before using the in-store Wi-Fi network. Given the vast user base of Facebook, a captive portal requiring Facebook login to authenticate is a popular choice for allowing Wi-Fi access.

NETGEAR provides an intuitive "Facebook WiFi" configuration option for its wireless environment. This option is available both in its cloud portal and via the Insight mobile app.

Ubiquiti Networks' support of a Facebook captive portal is in beta in its cloud portal. Similarly, Zyxel supports setting up a Facebook captive portal only via its cloud portal and not via its mobile app.

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. Zyxel provides cable test capability only from its cloud portal. Ubiquiti Networks does not provide any cable test functionality.

Network-Attached Storage (NAS)

It is the rare business that doesn't require on-site disk storage. Thus, having a business-class, network-attached storage system available can bring significant value.

Of the vendors evaluated, only NETGEAR offers business-class NAS. This shared resource can provide multiple terabytes of storage that can be shared in a controlled manner across site users. With built-in RAID, the NETGEAR ReadyNAS solution provides protection against a disk failure in the unit. The device status can also be viewed in both the cloud portal and mobile app. Currently, share-level configuration of the NAS must be done by logging into the NAS via separate web browser.

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. Some of the features for Ubiquiti Networks were only available in beta at the time of testing in August 2018. Beta status was noted in the results. Some additional feature testing was performed in September 2018.

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 and 3.

Systems Evaluated

Vendor	Device Type	Device Name	Model	Advertised Price	Notes
NETGEAR	PoE LAN Switch	NETGEAR 8-port Insight Managed Smart Cloud Switch 62W/PoE (GC110P)	GC110P-100NAS	$179.83	8-ports. Cloud managed. PoE all ports.
	WLAN Access Point	NETGEAR Insight Managed Smart Cloud Wireless Access Point	WAC505-100NAS	$79.99	802.11AC 2x2:2. Cloud Managed. Power adapter extra.
	Network Attached Storage	NETGEAR ReadyNAS 422 2-bay NAS Diskless	RN42200-100NES	$320.88	Price does not include disks
	Management Software	Insight Pro Web Portal 5.0.11.5, Cloud Version 5.0.10.11, Mobile App 5.0.11. Insight Pro <$15 per year per device sold via distribution channel.			
Ubiquiti Networks	PoE LAN Switch	UniFi Switch 8 60W	US-8-60W	$112	8-ports. Cloud managed. (4 ports of PoE.)
	WLAN Access Point	UniFi AP-AC Lite	UAP-AC-LITE	$84.10	802.11AC 2x2:2. Cloud Managed
	Local Controller (Remote Control Device)	UniFi Cloud Key	UC-CK	$78.58	PoE-powered, computer "brick" used as local controller
	Management Software Local Controller	Software and "Cloud Key": UniFi SDN v5.8.24. No charge for local controller software and no per-device management fee. Mobile app version 4.0 (40002).			
	Management Software Cloud Portal	UniFi Cloud v5.8.24. Annual pricing (Cost/devices): $299/10, $498/20, $697/30. $199 for every 10 devices over 30. Custom pricing for 500 devices or more. Mobile app same as above.			
Zyxel	PoE LAN Switch	ZyXEL NT NSW100-10P Nebula Cloud SWT 8PT GbE Nebula Cloud Managed PoE SWT 1Yr	MAP102	$204.99	10-ports. Cloud managed (8 ports of PoE)
	WLAN Access Point	Nebula Cloud Managed Access Point	NAP102	$129.99	802.11AC 2x2:2. Cloud Managed
	Management Software	Nebula Cloud v.20180814-125508, Mobile app version 1.6. 0. Nebula annual $55 per switch, $45 per AP. Multi-year and perpetual subscriptions available.			

Note: Prices gathered from Amazon. Advertised price used. Price information current as of September 2018. Support as bundled with product. Ubiquiti Networks does not offer network attached storage. Zyxel does not offer a NAS for business customers. Switch and AP firmware current as of August.

Source: Tolly, September 2018

Table 4

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

NETGEAR Business

NETGEAR Insight provides full-fledged business IT infrastructure management from your phone and from a cloud portal.

NETGEAR® BUSINESS

For more information on
NETGEAR Business solutions visit:

https://www.netgear.com/insight

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.