12 Features That Make Cloud-Managed Networks Easier To Manage

D-Link®

FOR BUSINESS

Introduction

On any given day, a company's network will undergo changes and updates. New employees will come on board and others will leave. Someone will complain that the Wi-Fi is slow. Access points will go offline. People will hog bandwidth. And at least one person will have trouble printing something.

As the manager of a network for an MSP, an enterprise, or an SMB, these are problems that can quickly add up and become issues on your network. Especially the printers. Printers are the stubborn child of an IT network and no matter how much you try, they will always be defiant.

Dealing with them in a timely manner is a fierce race against time, even for managers of small networks. For those turning to the increasingly popular world of cloud-managed networks (CMNs) that can span multiple sites, states, and even regions, having solutions with handy features in place to save time are essential for proactive management.

If you're considering implementing cloud-managed networking solutions for part or all of your the networks you manage, here are 12 features you should consider to help alleviate the everyday problems that can plague them.

1

Zero-Touch Provisioning (ZTP) Reduces Setup and Network Expansion Time and Cost

For all the benefits the command line interface provides, reducing setup time is not one of them. Unless you need an excuse to disappear from the world for a few hours, individually configuring every switch on a network probably isn't what you consider a good use of time in your busy schedule.

CMNs with zero-touch deployment (ZTD), which can also be called zero-touch provisioning (ZTP), can take back some of that time, especially when it comes to setting up the network.

For starters, you don't have to be onsite to handle everything—or anything—with ZTD. It's a rapid-deployment system, and all you need is someone who knows how to place each switch and access point, plug in a few power cords, and connect Ethernet cable at the physical site. It can be someone on site or a third-party contractor if needed.

Once all of the switches and access points are plugged in and installed, you can set up, configure, and manage them from anywhere.

Or you could save even more time by having each switch and access point take care of that work for you. With ZTD, you can configure everything beforehand. Then, once everything's ready to go, each product can download the configuration image, unpack it, and apply the settings automatically.

ZTD/ZTP also eliminates other time-consuming functions of network management including, but not limited to:

- Updating the OS
- Downloading and running patches
- Adding features
- Running basic and advanced configuration files
- Connecting to configuration management platforms
- Expanding networks to accommodate changing business needs

2

Role-Based Access Control Can Relieve Administrative Work, IT Maintenance, and Legal/HR Headaches

Networks would be a lot easier to manage if everyone who worked for a company never retired, quit, or received promotions. That's not how the world works, though. The people needing access to databases, servers, and confidential information is constantly changing. Not only that, but the people who implement the user permissions changes on your network can range from in-house IT administrators to third-party contractors.

With role-based access control, or role-based administration (RBA/C), you can alleviate some of the potential administrative work and legal nightmares by assigning roles, groups, scopes, and assignments through the network. From there, you can place people into specific roles and groups with clearly defined titles and permissions, such as primary, technical, administrative, billing, and more.

Good CMNs will simplify the management of these settings either through an intuitive layout or interface that makes it easy to configure permissions, responsibilities, and privileges on the fly. This system can reduce the amount of paperwork you might need to fill out when someone is hired or moves into a new role, too. Not to mention, this automated feature can also greatly limit any errors that might be made if setting up a new user account manually each time someone was being added to your network.

Other benefits to this feature include:

- Quickly creating broad and detailed user accounts
- Creating clearly defined permissions for administrators, end-users, and specialists
- Separating student, faculty, and administrative access
- Providing Wi-Fi access to campus visitors
- Separating guest and employee access
- Easily granting or revoking privileges during employee transitions
- Granting third-party vendors temporary access to your network
- Maintaining compliance and security

3

Auditable Changelogs Makes Diagnosing Network Problems Easier

Almost every IT manager has had to track down what's causing a problem to a network. Sometimes it's a simple change that was made to a network SSID. Sometimes it was not hitting the "0" key hard enough and mistakenly setting an APs bandwidth limit to 1 Mbps. And sometimes it's an issue you never would have expected to be the cause of the problem.

When that happens, an auditable changelog, or audit trail, can help save time in diagnosing what went wrong and when. Most CMNs provide this feature or capability, but then limit you to the amount of history it keeps, forcing you to build a server that stores the information or manually save what you can before you lose the information. A good audit log feature will include it as part of their service and offer a comprehensive history detailing the last six months, year, or, even all of the events from the moment you set up the network.

Your auditable changelog, or audit trail, should document both administrative- and user-level events, including changes to configurations, debugging, API calls, and more. Beyond diagnosing potential network issues, the audit log should also supply supplemental evidence in proving network compliance or operational integrity. They can also help IT personnel identify any non-compliant issues within their network and proactively address them. This includes potential threats to a network including security breaches, cyber threats, and data corruption.

Along with this, a good auditable changelog should keep track of useful information, including:

- The date and time the changes took place
- User information associated with each change
- The configuration settings that were modified
- Product and security updates and/or patches
- Compliance integrations

4

Authentication via Customizable Captive Portal, 802.1x, and a RADIUS Server Can Help Limit Network Security Risks

In a perfect world, no one would steal laptops and cellphones and employees wouldn't lose their devices. It isn't a perfect world, though, and these things happen, risking the exposure of confidential, personal, and private information.

Requiring authentication via a customizable captive portal can help limit the security risk of stolen devices. Through the use of 802.1x, you can require that any person on a network must pass two data encryption tests before joining a network no matter which device they use.

Since 802.1x operates on the RADIUS service, it nearly eliminates the issue of scalability, helping you maintain security measures even as your network expands to accommodate more people and devices. Additionally, with authenticated networks, you can easily restrict the access of anyone on the network if their devices become compromised or they're trying to sneak into networks themselves.

It also helps you:

- Deploy a large-scale, authenticated network
- Monitor network access
- Limit open network access
- Increase network security measures

5

Advanced Traffic Reports and Data Analysis Helps You Improve Network Speed

The rapid growth of IoT devices and the number of personal devices available today have shifted the role and scope of a business network. Along with managing the bandwidth available for critical business operations, including voice, video, and data connections, your network also needs to handle the thousands of tasks that may require small amounts of bandwidth but depend more on low latency. This is especially true for networks that serve critical services depending on split-second decisions, such as hospitals and healthcare facilities.

This is where advanced traffic reports and data analysis make it easier to manage your network, as this feature can remove the need to examine each individual switch and access point individually. Instead, it can filter the data by input criteria and quickly analyze large swaths of data to help you find what you need.

Given this, it's important to implement a CMN with the capability to handle the enormous amounts of data flowing through networks—especially one that scales alongside network growth. This includes accommodating for the potential addition of IoT and personal, switches, access points, IP surveillance cameras, servers, video conferencing equipment, data, and more.

Advanced Traffic Reports and Data Analysis can especially help you determine where any latency is occurring, whether that be at the client, server or application level.

6

Automatic Monitoring and Alerts Encourage Proactive Network Management

Monitoring and managing a network comes with a host of responsibilities, daily tasks, and short- and long-term projects. Because of that, it's nearly impossible for you to check every device on a network to make sure it's up and running. As much as you don't want to be blindsided by a preventable network problem, you also don't want to be alerted every five minutes by issues that might resolve themselves.

CMNs with automatic monitoring can help take on some of those tasks and provide you with the resources to proactively manage a network. Through the feature, you should be able to select the specific alerts you want to receive and receive them on a tablet or computer. These can include alerts regarding firmware upgrades, patches, added devices, and offline access points. Additionally, your monitoring system should provide an option to receive a notification based on the amount of downtime experienced by an access point.

For example, maybe you know that when an access point goes offline, it usually comes back on in a few minutes. Because of that, there's no need to receive an alert that might otherwise distract you from a current project. However, if that same access point is down for 15 minutes, you might want to know so you can address it before it leads to larger network problems.

Network downtime costs money, and the more you can do to prevent that, the happier you'll keep everyone and the more time you'll save by getting ahead of problems.

A good automatic monitoring and alert system should also notify you if/when:

- Firmware changes are made to one or multiple network switches and/or access points
- Security updates have been applied
- SSIDs and passwords have been changed
- Network issues, such as downtime, are affecting connectivity

7

Over-the-Web Firmware Upgrades Decrease Server Down Time

Over-the-web firmware upgrades are nearly a standard feature now, especially for CMNs that oversee hundreds, and sometimes thousands, of switches, access points, and cameras.

However, the better systems will provide scheduling features that allow you to pick the best time and date to apply upgrades. It should also provide you with several options when it comes to upgrading firmware, including picking the date and time you want to apply either a partial or complete upgrade.

After all, the last thing you want to do is bring down the all or part of the network you manage for a business, school, hospital, or another client. This is particularly true if a recent firmware upgrade has caused compatibility issues with other devices on the network and you're hesitant to apply a full network firmware upgrade.

8

Searchable Network-Wide Event Logs Help IT Managers Focus on Important Tasks

On a multi-site cloud network, the number of events that occur each day can quickly climb into the range of tens of thousands, and having to manually comb through the log looking for specific events will eat up a valuable chunk of time that an IT manager could be devoting to other projects.

In a similar fashion to the auditable changelogs that help IT managers diagnose network problems, network-wide event logs keep track of every event that happens on a network. This includes device logins, failed password attempts, any accounts there were locked out, and application errors and other events that might have caused problems.

A CMN with a searchable network-wide event log can shorten the time it takes to find specific events by providing the ability to filter by the date, event type, device type, and more.

If you know the day that a problem first occurred, you can use the list to help track down potential causes. You can also use it to:

- Identify potential security vulnerability
- Improve system performance by diagnosing potential bottlenecks and applying fixes
- Save time by identifying minor network issues before they cause system-wide problems
- Gain detailed insight into the network's system metrics
- Automatically correct network issues through the use of monitoring software

9

Intuitive VLAN Configuration Can Automatically Balance Network Bandwidth Needs and Channels

One of the more time-consuming processes in managing a network is reconfiguring the settings on access points and switches to help balance bandwidth needs across multiple sites. As businesses expand, add employees and devices, change locations, and relocate departments, keeping the network configured to handle the changing bandwidth needs for voice, video, and data can become a challenging balancing act.

An intuitive VLAN configuration can take some of the time out of that process by automatically filtering traffic to the appropriate VLANs across your network, whether it's centered in one location or spread out across multiple sites. So, as your business expands and adds cubicles, desk phones, computers, video conference centers, and even new office buildings/sites, the intuitive VLAN automatically identifies the traffic and assigns it to the corresponding data channels you have set up on your network.

Additionally, if you want to go in and adjust or fine-tune your network manually, you could use the intuitive VLAN to help streamline the setup process while minimizing any potential network hiccups that may occur.

10

Cloud-Based RF Optimization Delegates Traffic and Signal Strength as Needed

Wireless devices can place tremendous strain on a network, especially on APs that are constantly balancing bandwidth requirements and signal strength. Classrooms, meeting rooms, and more can go from needing very little bandwidth for a presentation to using large amounts of bandwidth during a webinar where many people are logged in and simultaneously streaming. All of this becomes more problematic when an AP decides it's tired and goes offline to take a quick nap.

Cloud-based RF optimization lets you manage and monitor the network from afar, including giving you the option to enable/disable autoconfiguration settings, such as the channel. A more elaborate system will open up the ability to select which channels an AP can use to help you customize the network even further and limit the slowdowns that packed networks and bandwidth hogs can have. Furthermore, it can even help adjust the signal strength of those APs for you in case one does do down. All of this goes a long way in keeping the network flowing smoothly even as the bandwidth needs shift and change throughout a network and all the location it serves.

More importantly, it can help you ensure that networks serving critical services, such as the ones healthcare professionals depend on in hospitals and clinics, have the bandwidth required to access vital and time-sensitive information.

11

Social Login Wi-Fi Access Support Can Increase and Simplify Account Signups

Whether you're managing your own network or implementing one for a business, at some point you may want to have customers sign up and create accounts so you can send them marketing materials and other relevant information. The problem is that up to 86 percent of people hate having to create an entirely new account to access content or Wi-Fi,[1] and 92 percent of people say they would rather leave a site if they forget their password than try to reset or recover it. [2]

One of the easiest ways for businesses and schools to encourage customers to create accounts with their business—and keep them returning—is through social media logins. Along with this simple social integration comes the potential for a wealth of information, including any demographic information that might be harder to gather through a custom, site-specific registration process. However, this is heavily dependent on how you choose to integrate this feature within your network.

The other benefits of using a CMN with social login access for Wi-Fi include the ability to:

- Gather demographics that provide more detail about your customers' interests
- Deliver information that can help you or your clients with retargeting campaigns
- Convert leads into customers/ acquisitions
- Market upcoming events and products
- Increase awareness of services and new policies affecting customers and/or citizens

12

Intuitive Web-Based Interface with Multilingual Support Makes It Easier to Support Multiple Regions

In a global economy, localized and national CMN solutions need to serve the needs of IT professionals from varying backgrounds. Without a web-based interface that has multilingual support, you limit the areas you can deploy it and the people you can hire to help manage it.

While multilingual support might not be a necessity for networks that include only a few buildings or local sites within a city or a state, it could be a lifesaver for multinational corporations that want to unify their network on one CMN.

One Final Note on Cloud-Managed Networks

An IT network is only as strong as its weakest link, and as businesses, schools, hospitals, governments, and more turn to CMNs for either some or all of their networking needs, they'll need solutions with onboard features that help them effectively and efficiently manage them. Maybe that's the exact position you find yourself in today.

Implementing CMN solutions into your network can be a nerve-wracking experience, especially when you're the one who's responsible. Knowing the network will be reliable, deliver the performance you need, and meet the budgetary and compliance demands of your network is crucial to you and all the people it serves.

If you have questions, please reach out to us at D-Link and ask away. We've been in the networking business for over 30 years and have designed, developed, and implemented networks for the world's largest casinos, automobile companies, restaurants, security services, and more.

Test Before You Invest

Give Nuclias a FREE 30-Day Trial

📞 **(888) 331-8686**   ✉ **solutions@dlink.com**

References

1. Soni R, Walker T, Freidlin S, Goldberg J, Centenaro L, Salman A. 9 Things You Should Know About Social Login & CRO [Internet]. CXL. 2019 [cited 2019Mar25]. Available from: https://conversionxl.com/blog/social-login/

2. The Value of Social Login Solving the Engagement Gap. Available from: http://www1.janrain.com/rs/janrain/images/Industry-Research-Value-of-Social-Login-2013.pdf