Concepts of the LANCOM Management Cloud (LMC)

A fully functional network is the heart of any business. And yet installing it and managing it is deeply complex. The skills shortage makes things worse, as qualified network specialists are hard to find. At the same time, the conventional manual configuration is a time-consuming, error-prone and thus very costly task.

Wouldn't it be great if there were an intelligent, higher instance that automates and controls the entire network from a central location? A kind of intelligence that networks all of the key components, dynamically responds to any new requirements, and which is also secure.

It sounds like a future scenario, but it is not. The LANCOM Management Cloud (LMC) provides a completely integrated solution. In this document we will explore some of the basic concepts of the LMC, although the procedures described here are not an exhaustive guide to the initial configuration of an LMC project. For this, as well as for other topics of interest, it is advisable to visit a corresponding LANCOM training course.

This techpaper deals with the following:

1. The concept – design first, deploy hardware later
2. The organizational levels
   - Organizations
   - Projects
3. The network configuration
   - Networks
   - Security
   - Sites
   - Devices
4. Roles
5. Dashboards
6. Extended functions
7. Support

The concept – design first, deploy hardware later

The LMC brings a change to the workflow when defining and setting up a network. Until now you needed experts to define the network and then manually configure each device. This often has to be done on-site, meaning that experts have to travel to a company's various locations. As a result, well-trained experts spend only a fraction of their time doing the work that they are actually paid for.

With the LMC, an expert carries out the design of the network using a user-friendly web interface and does not actually need to touch a single device. Throughout, the LMC handles a huge amount of details that would otherwise be configured manually for each individual device. For example; do you need to set up VPNs between sites? Which SSIDs are used where? And do you need VLANs? After that, the actual configuration of the devices is performed by the LMC. This is more than just centralized management, it is a view of the entire infrastructure of a business.

With the roll-out, the LMC carries out the complete configuration of each and every device. A technician on location connects the devices that were previously planned by the expert and made known in the project. The devices then contact the LMC and retrieve their configurations, and the expert can now assign the devices within a specific project. The devices at the new location are thus ready for operation a few minutes after connection.

Now let's take a look at the elements of the LMC that are required for this workflow: Organizations, projects, networks, security, sites, and devices.

The organizational levels

Organizations

An organization is the highest level in the LMC architecture and is hierarchically higher than the projects. Since the LMC is addressed at LANCOM partners, only these partners can be created as an organization within the LMC. Each partner can then create a project for each customer to be managed via the LMC.

If an end customer wishes to manage their own network, they can do this after first contacting a LANCOM partner, who then creates a project within their own organization.

Projects

Projects correspond to the customers served by the partner. In other words: You create a project for each customer, and this is where all of the customer data is stored along with global, cross-

site settings. At project level, for example, you can also see the license pool for the managed devices in this project and how long the associated licenses remain valid.

On the subject of license management and other topics relating to the LANCOM Management Cloud, we have a useful series of tutorial videos.

The network configuration

Networks

At the network level, global specifications are defined for certain applications within an IP address range. This allows a developer network to be logically separated from an accounting network, for example, and different access rights can be assigned within these networks. These globally defined networks can then be assigned to all desired locations so that, for example, a hotspot network can be provided at all company locations with the same design and the same access credentials.

First of all the network has a name, e.g. Guests, Sales, or LAN. Next, it has an IP address range, e.g. the class B network 10.0.0.0/16. When the network is assigned to a location, the size of the local subnets (e.g. /24 for class C networks) is specified and it is automatically assigned a class-C network from within the range of the class-B network. Next, you specify whether the locations in this network should be connected via an IPsec VPN. If so, assigning this network to multiple locations causes VPN connections to be automatically created between those locations and the central site. In this way, the LMC always generates a star-shaped VPN topology from the branch locations to the central site.

You can assign a VLAN ID to a network in the same way. This is then automatically rolled out to all of the sites that use this network. Consequently, all of the data in this network is automatically tagged with its VLAN ID. This separates the networks and is necessary if more than one network is to be operated at any given location.

Practical templates for each switch model (8-port, 10-port, 26-port, etc.) allow the individual networks to be assigned to specific switch ports. This ensures that port assignment is specified uniformly at all locations and technicians performing the on-site cabling can follow a standardized pattern.

All of the settings for this network (VPN, VLAN, ...) are made just once and are then applied automatically at all of your sites.

Finally, you assign an individual color to each network. This helps, for example, to identify which networks are assigned to which ports. This is especially useful if you customize the port assignment to an individual situation, such as when incorporating an existing network.

You can also add a Wi-Fi SSID with various options, such as the encryption type. This is then automatically available at any site that uses this network and has a connected access point.

And a few clicks is all it takes for you to provide a hotspot network at all desired locations. For further information see the “Cloud-managed hotspot” techpaper.

You also set the route that each site uses to access the Internet. You have the choice between a direct local breakout, via the central site, or via the security service provider Zscaler.

The connection to Zscaler is established via the “Internet Security” tab in the respective site. Please note that Zscaler must be licensed and set up separately with the company of the same name.

Security

The “Security” menu entry lets you keep track of your security settings in one place. A security profile is automatically created for each network in your LMC project, or your existing settings and rules are migrated there. There you can create rules such as those for Application Management, Content Filter, and Packet Filter globally for all networks and assign them to the corresponding security profiles. Under Security > Profiles, you can clearly see which security functions take effect in the respective network.

Sites

In the next step you create the sites. This is where you link the network specifications with the site itself. At the same time, you also assign devices to the site. These devices then receive the logical settings for the given location.

Enter the full postal address of each location so that each one appears correctly on the Google Maps-based display.

For each site, you optionally upload the floor plans for the building. You can use these to place the devices later. In the case of access points, the approximate coverage of the radio field is displayed on the dashboard.

However, this cannot replace a coverage analysis for the site as, for example, the materials of the walls are unknown and therefore cannot be modeled.

Devices

The basis of any network is the devices that make it up: Gateways / routers, switches, access points, and firewalls.

Any current LANCOM device—including virtual ones such as vRouter or vFirewall—can be made known to an LMC project by means of its serial number and the cloud PIN shipped with it. Alternatively you can request an activation code in the LMC. Using this code, you can use LANconfig to hand-over one or more devices to the LMC. You can use this procedure for any device that is cloud-ready.

However, devices are not permanently bound to their project. You can hand a device over to another of your projects at any time, or remove it from the LMC completely and operate it as a stand-alone solution.

The registered LANCOM devices can now be assigned to the sites. This information can be supplemented with a photo and a description of the device location (19" rack, suspended ceiling, ...) as a help to remote administrators. This can be useful for communications with technicians on site.

As soon as these devices are connected up at the respective site, they report to the LMC, are immediately provided with a suitable configuration and are included into the 24/7 monitoring.

The devices must have access to the Internet for this. If the router has a dedicated WAN Ethernet port and it finds a DHCP server, it will also be able to find the LMC and immediately obtain the correct configuration, assuming that the device has been made known to the LMC already. Otherwise, the router at this location requires a basic configuration by means of either the LANconfg setup wizard or the WEBconfig setup wizard. The site can also be assigned to the device at this time.

Consequently there is no need to carry out any on-site configuration of the access points, switches and (if applicable) the router, i.e. the administrator performs the commissioning in zero-touch mode.

One option is to prepare the data (serial no. / PIN) for all of the devices and then import everything in one go (bulk import). For further information please refer to the "Rollout" techpaper.

Roles

The roles for users in the LMC determine who is allowed to modify or merely view a project.

There is the role of the **organization administrator**, which essentially corresponds to the LANCOM partner. These users may create projects and other users. They have full control over these projects for as long as they remain registered as project administrator. This right can be withdrawn at any time. The organization administrator therefore does not necessarily have access to the projects assigned to the organization.

Project administrators have full control over the projects assigned to them, i.e. they can also add additional users to projects.

For example, a **technical administrator** has no access to the user administration.

Then there are **project members** who can edit the configuration of the devices, networks, and sites, but who cannot add new users or adjust global project information.

Members of the **Rollout Wizard** role are (mostly non-technical) colleagues on-site who add devices to the site using the LMC Rollout Wizard web application.

The **hotspot operator** role is also suitable for non-technical employees and is used to create cloud-managed hotspot vouchers.

Finally, there are the **project viewers** who can merely see the data of one project. You can use this role, for example, to allow customers to monitor their networks.

Further information on roles and permissions can be found in the infopaper “User roles and rights”.

Dashboards

Dashboards provide a visualization of all of the information for a project or individual sites, and they offer a variety of different focuses. In the following we consider some of these dashboards and the information they present.

WAN / VPN

This displays all of the project sites on a map and immediately shows you all of the VPN tunnels between the sites along with their current status by means of the signal colors green and red.

Historical data about the WAN links gives you a quick overview of router throughput and the number of VPN connections.

Wi-Fi / LAN

Once the floor plans of your buildings have been uploaded, you can use them to show the positions of your access points. Although the coverage display cannot take the walls and other factors into account, it at least provides a first indication. The main advantage of this presentation is to show the current load on each access point, so that overloads can be detected in good time.

The dashboard presents statistics that give you an overview of the deployed devices, the number of users, the load and the top applications, among others. If you detect a bottleneck, for example, you can easily switch from the dashboard to the relevant devices at the location and inspect the details more closely.

Security / Compliance

By means of the widgets you can immediately see if there are devices without a set password or in need of a firmware update. Open ports are also displayed with an appropriate warning.

LANCOM Trusted Access

Monitor connections, logs, licenses, and managed blocklists for users and endpoints in your LTA environment.

My Dashboards

With “My Dashboards,” you can tailor your monitoring views to your personal needs. Customizable dashboards and practical monitoring tools help you maintain full visibility of network events, identify errors more quickly, and optimize workflows. Create up to 11 personalized dashboards per project, with configurable layouts, widgets, and filters for monitoring tailored to your requirements.

A detailed overview of your options and instructions for creating your personal dashboards can be found directly in the LMC in the dashboard’s information section, as well as in this techpaper.

Extended functions

Add-ins / scripting

The add-ins that LANCOM Systems can activate for a project allow specially trained users to make individual extensions to the LMC. These extensions allow a Javascript sandbox to be used for generating command-line scripts and configuration extensions based on the OID structure (LCOS or LCOS SX). These can be used to roll out any configuration to the devices. Scripts work with variables that can be set on any level of the LMC (networks, security, sites, devices), which is useful for further script customization. A variable with a selection type could, for example, control which part of the script becomes active and thus write the definition for different SIP providers. For more information, see the Add-in manual.

Efficient, automated workflows with webhooks

From monitoring and troubleshooting to deployment and upgrades: As an administrator, you rely on a holistic view of all network activities to respond quickly. Using webhooks in the LMC saves you valuable time by flexibly communicating alerts and notifications to messaging services and automation tools when an event occurs. Learn more in the Webhooks techpaper.

Application Programming Interface (API)

Many functions within the services in LMC can also be accessed programmatically via an API. The documentation of the REST API of the LMC services, along with the http calls, can be found in the system information for the LMC. More on this in the related documentation.

Support

For questions relating to the LMC, Support team members are available for a live chat during office hours to answer queries immediately.

Alternatives are the LMC Help Portal and also the LANCOM Knowledge Base with articles on the LANCOM Management Cloud, further information and helpful instructions. A look at the FAQs on the LMC provides you with answers to frequently asked questions on the topics of security, migration, features, WLAN, switches, routers / VPN, operations, and licensing.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com