OFFICIAL RECORD DOCUMENT # 4.B-3 DREYFOUS PROPOSAL_TAB 3 EQUIPMENT & SERVICES
PRDE-OSIATD-2018-003-WIRELESS EQUIPMENT AND SERVICES

Date: january-12-2019

PRDE-OSIATD-2018-003-WIRELESS EQUIPMENT PROPOSAL

EQUIPMENT & SERVICES PROPOSAL – Confidential

Table of Contents:

PMB 641 HC-1 BOX 29030 CAGUAS, PR 00725-8900
P: 787.706.2700 • F: 787.789.2018

I. GENERAL EXPERIENCE:

A New Vision in Educational Services and Materials, Inc. (NEVESEM, Inc. dba Dreyfous and Associates) was established in San Juan, Puerto Rico in 1993, and has been consistently pursuing its mission of providing educational and technological products and services of excellence.

Throughout the years the company has had the opportunity to successfully develop, implement and fulfil significant projects within the public and private school systems. In 2014 we were selected to service RAD #5 (Red de Apoyo Diferenciado) for the Department of Education of Puerto Rico. For the last two years we have been implementing "Proyecto Trei" for three public school districts servicing over 400 schools. For "Proyecto Trei" we developed the tools necessary to help teachers prepare their lesson plans as well as providing quick access to digital curricular content aligned to the Puerto Rico Core Standards for grade levels K-12.

We have 18 years of experience as internet service providers (ISP) through the E-Rate program for private schools and public libraries. Dreyfous and Associates has installed over $25 million dollars in telecommunications equipment such as routers, switches, access points, servers and cabling among others. We currently provide CIPA compliant filtered internet access, voip services, network equipment, on-site technical assistance and managed services to over 300 non-profit organizations in Puerto Rico.

Our centralized Network Operational center (NOC) is home to our Datacenter which stores our array of virtual and physical servers, security equipment, telecommunication services (Firewalls, Content Filters, Routers, Switches, Access Points, Wireless Controllers, Redundant UPS, Electric Generators) and data storage (SAN) interconnected to redundant Fiber Optic connectivity, and point to point antennas to distribute internet that originates from a variety of internet service providers (AT&T, Claro, Liberty, Critical Hub, Blackburn Technologies). We also provide a Help Desk call center that offers technical support and troubleshooting services to all of our customers.

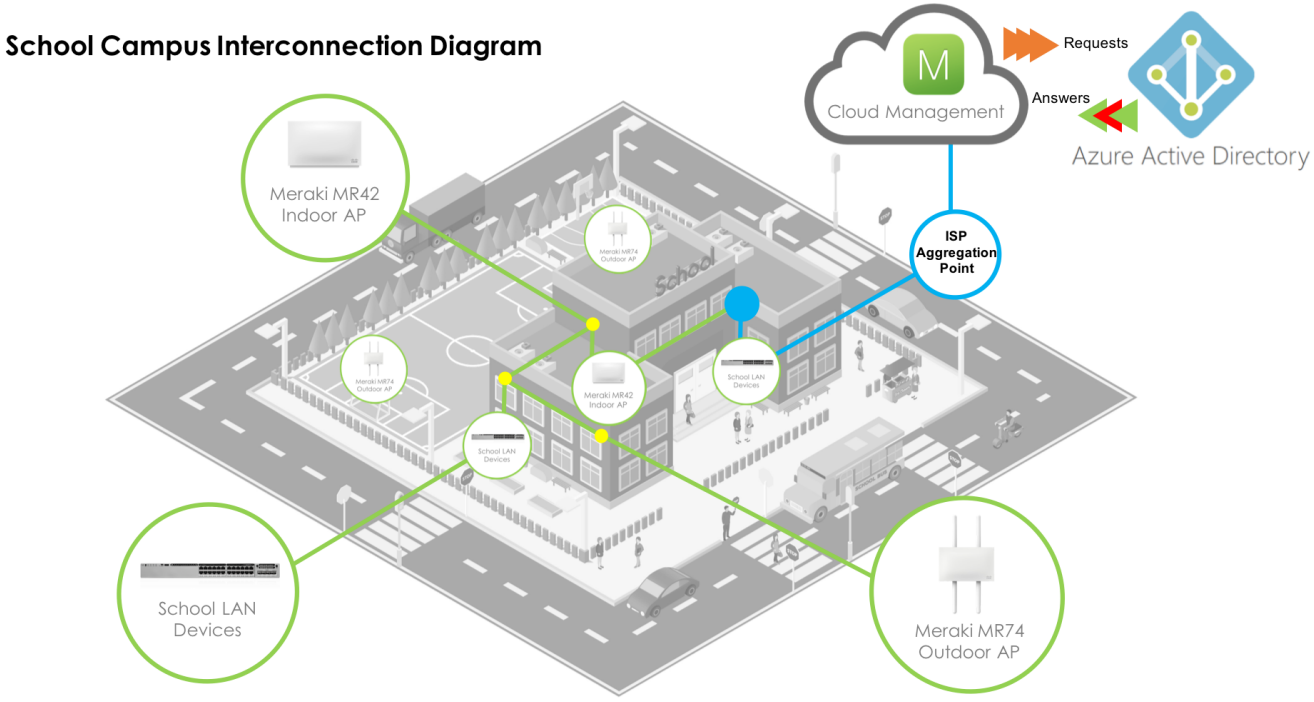
Our IT department is composed of 20 employees with over 18 years of experience providing technical services to all the non-profit educational institutions and public libraries that we service to guarantee a prompt resolution to technical challenges and provide a consistent and continuous service.

Our experienced and qualified personnel have the following qualifications and certifications.

- Microsoft Education Partner - MCTS
- Cisco Systems - CCNA
- Fortinet Partner – NSE-1
- Mikrotik – MTCNA, MTCRE
- Ruckus Wireless – Elite Partner
- Ubiquiti - UBWA
- HP Business Partner
- Iboss Partner
- Grandstream VOIP Certified Partner

II. DESIGN & DOCUMENTATION

- **Network Design:**



SSID 1 – ADMIN
SSID 2 – FACULTY
SSID 3 – TEACHERS

- **Documentation:**
    - **Technical Documentation Document – Attached**

      Includes:

      - Network Diagram
      - Wireless Network Information
        - Wireless Management – Cloud
        - SSID - vlan
        - Access Points – make, model, location, serial, ip address
      - Support Services – client portal user account & website
      - Floor Plan – school map
      - Photos – equipments & installation

III. PRODUCTS & EQUIPMENTS:

- **Access Points:**

Indoor: MR42

Dual-band 802.11ac Wave 2 access point with separate radios dedicated to security, RF management, and Bluetooth.

High performance 802.11ac Wave 2 wireless

The Cisco Meraki MR42 is a four radio, cloud-managed 3x3 MU-MIMO 802.11ac Wave 2 access point. Designed for next-generation deployments in offices, schools, hospitals, shops, and hotels, the MR42 offers performance, security, and simple management.

The MR42 provides a maximum 1.9 Gbps frame rate with concurrent 802.11ac Wave2 and 802.11n 3x3:3 MIMO radios. A dedicated third radio provides real-time WIDS/WIPS with automated RF optimization. In addition, an integrated fourth radio delivers Bluetooth Low Energy (BLE) scanning and Beaconing functionality.

With a combination of cloud management, high perfomance hardware, multiple radios, and advanced software features, the MR42 makes an outstanding platform for the most demanding of uses today and tomorrow. These uses include high-density deployments and support for applications like voice and high-definition video.

MR42 and Meraki cloud management: a powerful combination

Management of the MR42 is handled through the Meraki cloud, enabling rapid deployment across multiple sites without the need for time-consuming training or costly certifications. Since the

MR42 is self-configuring and managed over the web, it can be deployed at a remote location in a matter of minutes, even without on-site IT staff.

24/7 monitoring via the Meraki cloud delivers real-time alerts if the network encounters problems. Remote diagnostic tools enable immediate troubleshooting over the web, meaning multi-site, distributed networks can be easily managed.

The MR42's firmware is automatically kept up to date via the cloud. New features, bug fixes, and enhancements are delivered seamlessly over the web. This means no manual software updates to download or missing security patches to worry about.

Outdoor: MR74

Dual-band 2x2 MIMO 802.11ac Wave 2 access point with separate radios dedicated to security, RF Management, and Bluetooth.

General purpose industrial / outdoor 802.11ac Wave 2 wireless

The Cisco Meraki MR74 is a four-radio, cloud-managed 2x2 MIMO 802.11ac Wave 2 access point. Designed for general purpose, next-generation deployments in harsh outdoor locations and industrial indoor conditions, the MR74 offers performance, enterprise-grade security, and intuitive management.

The MR74 delivers a maximum 1.3 Gbps* aggregate frame rate with concurrent 2.4 GHz and 5 GHz radios. A dedicated third radio provides real-time WIDS/WIPS with automated RF optimization. A fourth radio delivers seamless Bluetooth Low Energy (BLE) scanning and Beaconing.

The combination of cloud management, 802.11ac, full-time RF environment scanning, and an integrated Bluetooth Low Energy radio delivers the high throughput, reliability, and flexibility required by the most demanding business applications like voice and high-definition streaming video, even in the most harsh outdoor environments.

MR74 and Meraki Cloud Management: A Powerful Combination

The MR74 is managed through the Meraki cloud, an intuitive browser-based interface that enables rapid deployment across multiple sites without the need for time-consuming training or costly certifications. Since the MR74 is self configuring and managed over the web, it can be deployed at a remote location in a matter of minutes, even without on-site IT staff.

24x7 monitoring via the Meraki cloud delivers real-time alerts if the network encounters problems. Remote diagnostics tools enable immediate troubleshooting so that distributed networks can be managed with a minimum of hassle.

The MR74's firmware is always kept up to date from the cloud. New features, bug fixes, and enhancements are delivered seamlessly over the web, meaning no manual software updates to download or missing security patches to worry about.

- **Security Enclosure:**

Indoor AP: Wi-Fi AP Cover for Meraki MR Access Points

Ventev's new Wi-Fi AP Cover is designed to accommodate the Meraki MR32, MR34, and MR42 access points. This enclosure is designed for indoor use to protect the MR32, MR34, and MR42 access points from damage caused by tampering or theft. The enclosure, made from polypropylene material, is durable, extremely affordable and is simple to install. The solid cover prevents visual access to the AP in a visually-pleasing and stealthy solution. It is perfect for a variety of applications where a tamper-proof and aesthetically-pleasing design is critical.

Outdoor AP:

14" x 12" x 6" Enclosure w/ Clear Door, Key Lock, 4 N-Style Jack Holes, Universal Backplate

The 14" x 12" x 6" Basic Enclosure is constructed of polycarbonate plastic, making it a durable, extremely affordable solution. The enclosure features a clear door, CAT60 lock, blank backplate, cord grip and 4 pre-drilled N-Style Bulkhead Jack holes. This NEMA 4X enclosure is intended for indoor or outdoor use to protect Wi-Fi access points from corrosion, dust, rain, extreme temperatures and unauthorized access or inadvertent contact with the controls and wiring located inside the enclosure.

- ## Cloud Controller

Cisco Meraki delivers the most robust cloud managed network, enabling massively-scaled deployments with tens of thousands of switches or APs. Support hundreds of thousands of end users in a single network without lengthy provisioning, training, or performance bottlenecks.

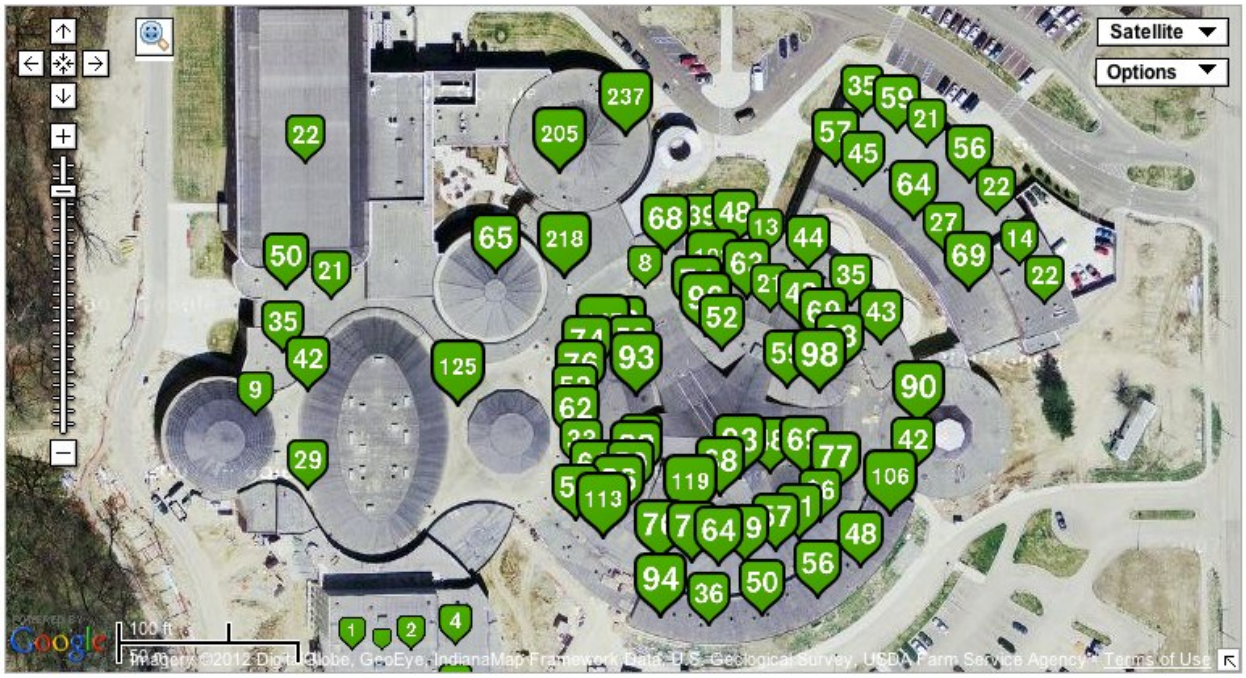
Centrally manage networks of massive scale

Cisco Meraki products come with centralized cloud management right out of the box, enabling administrators to centrally manage networks of all sizes — from small sites with a handful of devices to massive locations with thousands of switches and access points that connect hundreds of thousands of end-user devices to the network.

Deploy thousands of APs

Zero-touch provisioning shortens deployment and configuration time from weeks or days to minutes. Cisco Meraki devices automatically connect to the Cisco Meraki cloud over a secure link, register with their network, and download their configuration. There's no need to manually stage APs or log in to switches for manual configuration and provisioning. Cisco Meraki APs use Auto RF to self-configure and optimize RF settings for maximum performance, even in dense and challenging environments.

Even under dynamic conditions, wireless APs continue to automatically adapt to changing performance and interference conditions, without the need for tedious and manual tuning of wireless parameters.



Benefits

Easy

The Meraki Enterprise Cloud Controller enables administrators to bring up new wireless deployments in minutes, not days. Meraki access points are plug-and-play, auto-configuring, and self-healing. The Cloud Controller's streamlined web interface reduces upfront installation time and eliminates specialized training, while reducing maintenance and troubleshooting over the long run.

Secure

Meraki provides a wide range of standards-based security and access control options, from simple pre-shared key encryption to enterprise- class **802.1x** & **Azure AD** authentication. Different user groups, such as employees and guests, can be placed in distinct virtual networks that isolate traffic according to corporate policy.

Scalable

The Meraki Enterprise Cloud Controller provides true centralized management without any additional hardware. Centrally manage up to 1,000 wireless networks, each with up to 10,000 access points. Whether the networks are on multiple building floors, multiple buildings on a campus, or multiple campuses around the world, an

administrator can push a single configuration to all of the networks instantly, and get aggregated usage and connectivity data in a single view.

Industry-Leading Coverage

Meraki's 802.11a/b/g/n triple-, dual-, and single-radio access points enable administrators to cover large areas with wireless connectivity easily and effectively. With technologies such as mesh routing and dynamic channel optimization, Meraki access points offer excellent coverage in the most challenging RF environments.

Future-Proof Investment

The Meraki Enterprise Cloud Controller never has to be replaced. It is constantly updated with features and enhancements that provide value to a wireless network long after a hardware-based controller has reached its useful lifetime. Administrators can choose Meraki knowing that their investment is protected.

Simple Licensing

The Enterprise Cloud Controller license includes all new feature releases, software updates and support, making budgeting and license management simple.

Lowest Total Cost of Ownership

With no need to purchase expensive WLAN controllers or separate licenses for new features, software maintenance and support, Meraki Enterprise networks offer the lowest TCO of any enterprise-class WLAN. Meraki's Enterprise Cloud Controller has all the features required for a large office deployment out of the box, and enterprise- class phone support and software maintenance are included at no additional cost.

Air Marshal:

Real-Time Wireless Intrusion Prevention System (WIPS) and Forensics

Securing Your Wireless Airspace

Meraki's cloud managed wireless access points (APs) come equipped with Air Marshal, a built-in wireless intrusion detection and prevention system (WIDS/WIPS) for threat detection and attack remediation. APs configured in Air Marshal mode will scan their environment in real-time and take preemptive action based on intuitive user-defined preferences. Air Marshal triggers alarms and automatically contains malicious rogue APs. Intuitive cloud based management with flexible remediation policies makes Air Marshal ideal for security-conscious distributed networks.

Key Benefits:

- Security policy enforcement at the network edge
- Real-time scanning across channels on 2.4GHz and 5GHz bands
- Attack signatures continually updated from cloud
- Granular detection, attack and remediation policies
- Policy-driven real-time alarms via e-mail and SMS
- Works with all Meraki MR-series access points
- Included with the Meraki Enterprise license at no additional cost

Turnkey Setup

With Meraki's Air Marshal, you can deploy a state-of-the-art real-time scanning system without requiring any additional software, hardware or licenses. By default, all APs will opportunistically monitor their surroundings. With a simple click, an AP is marked as an Air Marshal, converting it to a dedicated WIPS scanner.

Centralized Management

Deploy and manage multiple sites from a single-pane of glass, eliminating the need for large IT teams and on-site truck rolls for any security troubleshooting or WIPS-related events. Air Marshal seamlessly scales to thousands of sites.

Event Log

Search by AP, client device, or time

Per AP: Monitor device boots, AutoRF, dropped frames, stuck beacons, authentication status, administrative state, and WIPS events

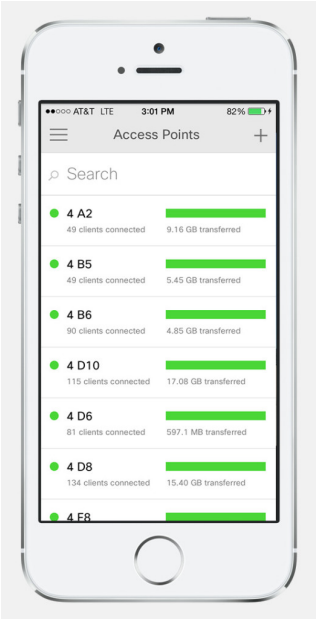
Per client: Monitor 802.11 events, WPA associations, 802.1x authentications, DHCP flows and IP address assignment, authentication states, ARP and DNS info

Historic data stored since inception of network

- **Cloud Mobile App:**

Cloud management in the palm of your hand

Network management using the dashboard app is just as simple as it is on the web. View the status of wireless networks at a glance, quickly identifying healthy or offline access points. See the details of any Meraki access point on the network and verify network connectivity, usage, and settings. Multi-site management is built-in, too.

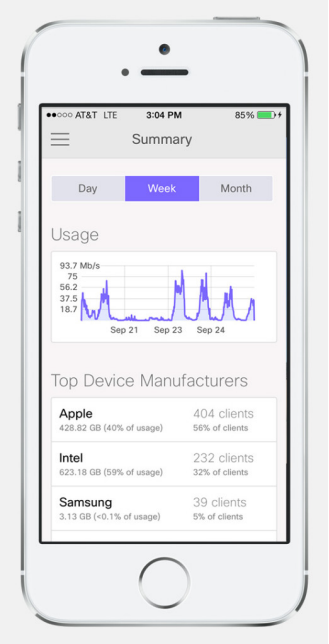


Faster WiFi deployments

To add a new access point, use the app to scan its barcode and add it to the network. The access point will automatically connect to the cloud, provision itself, and become part of the network, appearing in the list of APs. The app takes advantage of a few mobile-specific features: the camera and GPS. When installing the AP, use the phone's camera to take a photo of the mounting location — this makes it easy to visually identify an AP when walking through a deployment. There's no need to hunt around for the AP, since its location can be tagged using built-in GPS.

Network summaries at a glance

The most important data about your network is neatly presented in the summary page. Daily, weekly, and monthly usage graphs show traffic patterns on your network. Top client charts reveal bandwidth-hungry devices and the mix of iOS, Android, and desktop platforms in your environment. To monitor multiple Meraki networks, just select them from the app's menu.



IV. Solution Training (OSIATD Technicians – 8hrs)

- MR Platform Overview

  MR Wireless Access points: indoor models

  MR Wireless Access points: outdoor model

  MR feature: Air Marshal/WIPS (Wireless intrusion prevention)

  MR Feature: Auto RF

  MR Feature: CMX Location Analytics.

  MR Feature: Mesh Routing

  MR Feature: Bluetooth Low Energy

  Demo Lab: AP Setup

  Demo Lab: Basic Troubleshooting

  Demo Lab: Reports

V. IMPLEMENTATION PLAN FOR PROPOSED WIRELESS SOLUTION

In order to provide an orderly implementation of the requested solution and considering the personalized characteristics of the client and the importance and magnitude of the project, it is suggested that the action plan be divided into different stages/phases.

The solution provides different phases that can be simultaneously implemented during the time waiting for the dispatch and arrival of the required equipment (Hardware). The implementation plan is composed of five phases consisting of the following simplified descriptions.

a. **Infrastructure Requirements**
b. **Operational impact analysis (Risk Assessment)**
c. **Responsibilities matrix for vendor & the Department**
d. **Project Implementation Roles & Staffing**
e. **Schedule Plan - Milestones**
    1. **Planning - Kick off meeting**
    2. **Implementation**

a) **Infrastructure Requirements:**
THE DEPARTMENT WILL PROVIDE THE WIRING INFRASTRUCTURE FOR THE ACCESS POINTS INTEGRATED TO THE WLAN (WIRELESS LOCAL AREA NETWORK), AS WELL AS THE SITE SURVEYS AND HEAT MAPS IDENTIFYING THE LOCATION OF THE ACCESS POINTS. THE DEPARTMENT WILL ALSO PROVIDE ALL CABLING RUNS/DROPS, SWITCHES, UPS UNITS, AND CABINETS FOR THIS PROJECT.

b) **Operational impact analysis (Risk assessment):** This deliverable provides a list of project risks. Project risks are circumstances or events that exist outside of the control of the project team and have an adverse effect.

- **Classroom not ready for installation (ex: roof leaking water)**
- **Reduction in installation time due to limited access to client's locations**
- **Reduction in installation time due to client's personnel availability**

c) **Responsibilities matrix for vendor & the Department:**

Observations:

- All activities/task that are part of the implementation process (Installation, configuration, migration) will be conducted by specialized and trained personnel for each specific task.

- The management of the project will be guided by the tech industry best practices and frame worked by the recommendations of the PMI.

- A project manager will be assigned to manage and supervise all activities. In conjunction with the client all implementation processes will be validated.

Responsibilities:

The proposed solution for this project will be approached with a shared vision where the PRDE participates actively in the implementation of all established objectives.

This will allow:

- Diminish the levels of uncertainty in the structure of the proposed timeline in the implementation of the project. The PRDE will be a participant in the development of said timeline.

- Speed up the transfer of technologies from the beginning of the project as the PRDE will assign adequate personnel to provide support and assistance to our team during the process of gathering of information, action plan structure and overall implementation of the project.

- We will be responsible for the implementation and startup of the new network.

THE PRDE will:

- Explicitly assign the appropriate human resources that will supervise and provide support to each of the areas detailed in this proposal. The selected team must be present during the Kick off meeting.

- Attend all meetings that are requirements for the successful implementation of the project

- Provide all documentation and information requested by our implementation team that is required for the completion of the project. (Lay out plans, heat maps, Frequency analysis, among others)

- Provide adequate access to all environments and facilities during the implementation of the project. In the case that there is confidential information to be shared, a confidentiality agreement can be signed by both parties to ensure the proper management of said confidential information.

- Manage the platform after the implementation is completed, in coordination with the support of all information gathered during said implementation.

- Provide all electrical requirements and database connectivity points necessary for the installation and startup of the new network.

- Report all incidents, situations and optimization requests through the provided communication channels.

Nevesem will:

- Present during the Kick Off meeting all team leaders (Implementation, management, commercial) involved in the project.

- Participate of all required meetings for the successful implementation of the project

- Assign the appropriate specialized human resources for the installation, configuration, network start up and required training for all stages/phases of the project.

- Complete all implementation tasks in accordance to the final details and framework established in the Kick Off meeting.

- Comply with all established timelines and service level agreements.

- Accompany, train and empower the PRDE in the acquisition and management of newly acquired network.

d) Project implementation roles:

The expected roles in the wireless equipment implementation project include:

- **IT manager—IM** - Responsible for the technical vision and overall design.
- **Logistics manager—LM**- Responsible for the procurement, distribution, and return of appropriate equipment.
- **Project manager—PM** - Responsible for the management of the project & team.
- **Installer—INS**- Responsible for access point installation.
- **Technician—TEC** - Responsible for base-level technical configuration of the new environment, turning services up, wifi survey, documentation, testing & certification.

- **Quality assurance—QA** - Responsible for verifying work activity, installation photos (equipment + asset tagging) & quality.

Additional roles include:

- **Operations liaison—**Operations liaison to coordinate between the two organizations. **Site leader—**Each of these teams will need a designated site leader to coordinate local activities.
- **Department of Education Personnel – DEP –** PRDE Project Manager

Estimated project staffing: The staffing of a project will rise and fall during the project lifecycle. It peaks during the wireless LAN implementation phase and tapers off during the final cleanup. Smaller teams can easily execute the project, but it will extend the duration.

	Business planning	**Technical planning**	**Implementation**	**Conclusion**
Project management staff	1	2	10	13
Technical staff	1	2	10	13
Installation staff	1	10	100	111

e) Schedule Plan

Estimated project duration: All IT projects require business planning, technical planning, implementation, and project conclusion.

This wireless LAN implementation project follows the time line projected below:

	Work time	**Elapsed time**
Business planning	1 to 2 weeks	2 to 3 weeks
Technical planning	2 to 3 weeks	3 to 4 weeks
Implementation	3-4 months	4-5 months
Conclusion -Total	**5 months**	**6 months**

Professional Services and Project Management:

This proposal includes installation services, configuration, network start up and management in accordance to the following activities and scope of work.

Inspection:

- Verify and validate hardware equipment availability for each provider/manufacturer

- Perception inventory. This task will be conducted within the Nevesem's facilities prior to the delivery of all equipment for the purpose of creating a registry database of t serial numbers and physical condition of each equipment.

- Evaluate the area of installation provided by the client

- Verify and validate network ports, electric access and existing cabling required for each installation.

- Create the engineering design

Project milestones: *Planning – Project Kick Off*		
Task Name	**Assigned Resource**	**Estimated Time (hrs)**
1. Generate Project documentation & design	IM	80
2. Equipment purchase & lead time confirmation	LM	16
3. Contact customer for introductory project discussion and to schedule Kick Off meeting	PM	2
4. Provide customer with necessary project documentation & design	PM	8
5. Allocate resources and form implementation team	PM	40
6. Conduct Kick Off meeting (on-site or via teleconference)	IM PM DEP	16
a. Meet PRDE implementation team		
b. Review locations list (857 Schools & 37 NIF)		
c. Discuss school access & installation coordination process		
d. Review project scope, design, cloud controller configuration & access point distribution and placement (Surveys & Heat Maps)		
e. Review customer & Nevesem roles and responsibilities		
f. Risks Assessment discussion		
g. Review actions, tasks & ownership		
h. Review & schedule training for PRDE staff based on RFP		
i. Define mechanism and frequency of future project communications		
j. Document any open issues and/or action items		
k. Estimate project timeline (goal)		
7. Publish and distribute Project Plan & project implementation schedule	PM	4

Implementation		
Task Name	**Assigned Resource**	**Estimated Time (hrs)**
1. Confirm receipt of ordered equipment (serial numbers), inventory & classification	LM	40
2. Cloud controller configuration:	IM	80
a. Location Creation (School – 857 & NIF - 37)		
b. Register access point serial numbers per location		
c. SSID creation – 3 per location		
d. Password configuration		
e. Security Policy configuration		
f. Access Point Groups creation		
g. Captive portal configuration – PRDE Logo and colors		
h. Alerts & notifications configuration		
i. Azure AD authentication configuration & testing		
j. Mobile App configuration & testing		
k. Syslog server configuration for 1-year log retention		
3. Schedule installation dates with PRDE staff & implementation group	PM	16
4. Provide install documents & equipment to installers (contractors)	PM	40
5. Equipment installation & asset tagging	INS	4-5 months

II. Closing

Task Name	Assigned Resource	Estimated Time (hrs)
1. Equipment installation photos & asset tagging verification – Quality Assurance	QA	4 per location
2. Service turn up & testing	TEC	4 per location
3. Post deployment verification – wifi survey	TEC DEP	4 per location
4. Tune wifi network as needed	TEC	1 per location
5. Final documentation of network settings and equipment configuration	TEC	2 per location
6. Train PRDE (OSIATD) support staff	TEC	8
7. Project Completion - Installation documents signature (Equipment packing list, Installation certification)	PM DEP	1 per location

VI. USAGE & PERFORMANCE MEASUREMENT & REPORTING – Web Download

- *MR Access Points*

The following types of events will be reported by MR access points:

- 802.11: Wireless association and disassociations
- 802.1X: RADIUS authentication and deauthentications
- Auth: Splash page authentication
- AutoRF: Channel scans and TX power changes
- DFS: Events related to Dynamic Frequency Selection
- DHCP: DHCP leases and related errors
- Events dropped: Too many events were generated too quickly, creating an Events Dropped event
- L3 roaming: Events related to Layer 3 Roaming
- Status: Device status events (UP, Down)
- Meraki VPN: VPN tunnel drops and connectivity events
- Air Marshal: Packet floods and wireless security events
- WPA: WPA authentication and deauthentications

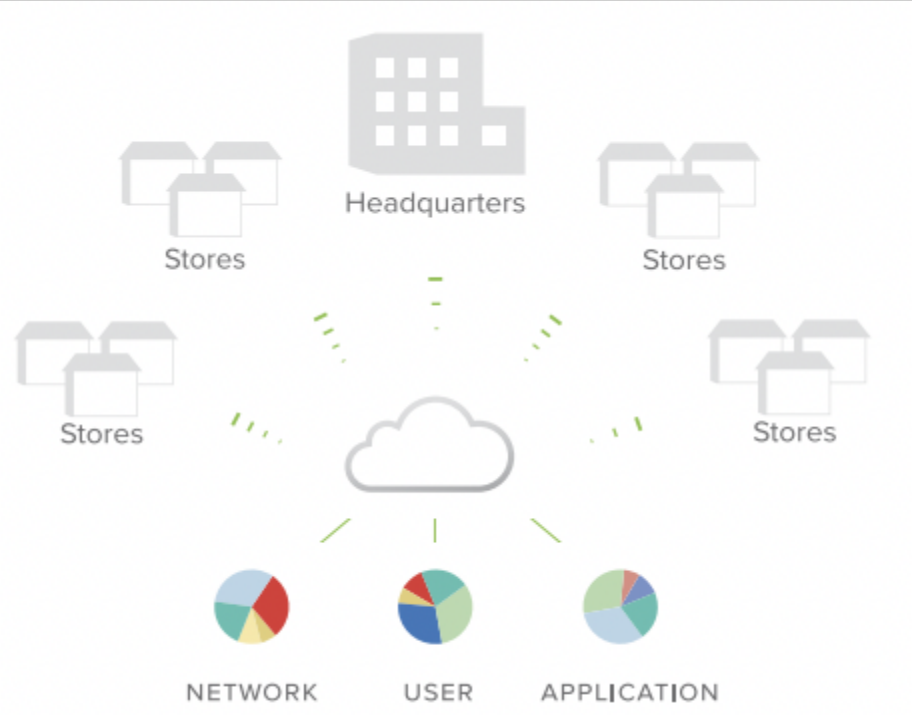
Monitoring the Wireless Network

The Meraki Cloud makes it easy to monitor the status of many Access Points within a network as well as the traffic passing on the wireless network. Larger distributed customers will likely have multiple organizations. Meraki offers a number of organization level monitoring tools in addition to the monitoring tools available at the network level that are discussed in this article.

Wireless Summary Report

A network administrator can obtain rich network analytics from the Summary Report page under the Monitor tab. This report provides information about the Meraki wireless network since its inception, including some of the following statistics:

- Top 10 APs by data consumption and number of client logins
- Top 10 clients by data consumption
- Usage breakdown by SSID and AP model
- Top client device manufacturers and OS types by number of client logins and data consumption



The report can be customized and viewed for statistics over a certain time period to allow for statistical analytics for a specific day, week or month.

The report can be e-mailed on a configurable schedule for constant visibility. Administrators can configure one or more e-mail addresses under the 'Schedule monthly e-mails' tab if they

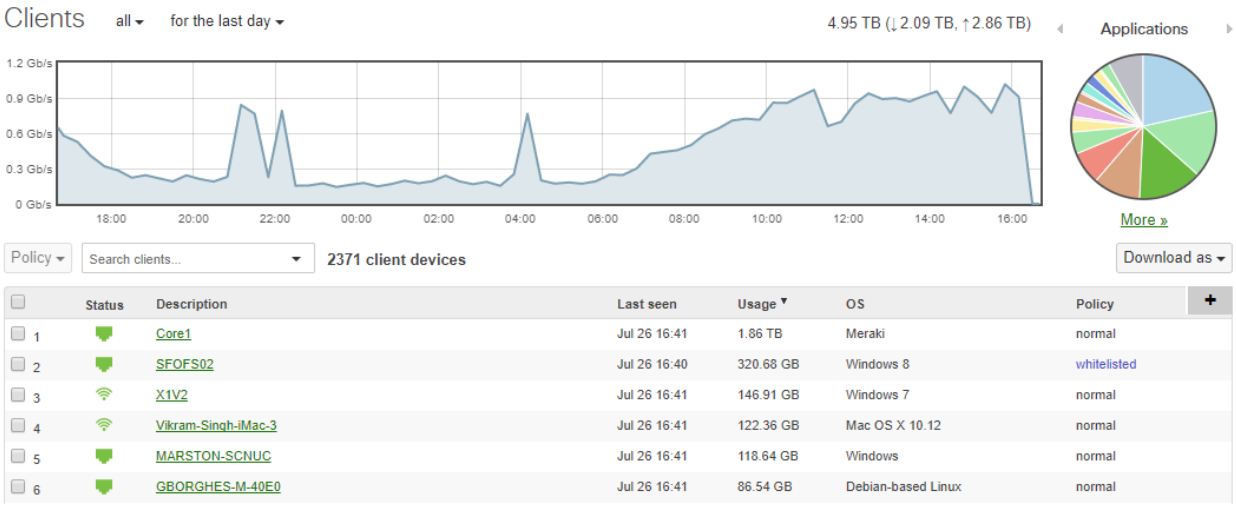
wish to send the summary report to multiple people. They can also add their organization's logo to the report.

Traffic Analytics and Layer 7 Visibility

Meraki Enterprise networks offer powerful application visibility and control tools. Packet inspection engines running custom parsers in each AP provide this information by fingerprinting and identifying applications and application groups. Traffic Shaper then provides the ability to create custom per-user shaping policies based on this application-level visibility. Since Meraki's parsers are designed to run at line rate, there is no performance decrease when enabling Traffic Analysis or Traffic Shaping.

Next to the usage graph at the top of the screen is a pie chart that can display a breakdown of the traffic currently displayed on the page by application, HTTP content type, port number or custom criteria. The gray arrows flip from one chart to the next. Custom pie charts can be configured on the Network-wide Settings page under the Configure tab.

Clicking on either the pie chart itself or the "More" link underneath the pie chart will open up the Traffic Analysis Details page, showing a detailed list of the specific applications and content types that make up the data shown in the pie chart. The applications have been assigned to groups to make classifying applications and creating shaping policies simpler.



Clicking on a particular application or content type within the Traffic Analysis Details page will take you to the Rule Details page, where you will find detailed information about that particular application or content type rule, including which users are contributing to usage of this type and details such as which application group that item belongs to, port number, description of the application or rule and links to additional information.

For broad categories such as 'Miscellaneous secure web', it is now possible to get a more granular breakdown of hostnames and IP addresses that comprise this category. This

functionality can be enabled by enabling the more detailed 'Traffic Analytics' capability under the Network-wide settings page.

Client List

The Clients page shows how the network is being used and by which client devices. The page includes the following features:

- Displays clients that have associated on any SSID advertised by the wireless network, or only those clients that have associated on a given SSID. This can be selected using the SSID drop down menu at the top of the screen.
- Search for clients by MAC, OS, device type or NetBIOS/Bonjour name. (Using Search)
- Zoom control, which enables the administrator to see only those clients that have associated within the specified time span.
- The administrator can also click on the “blocked list” to view only those clients on the MAC blacklist.
- Like the Access Points page, the Clients page has a list that can be customized (adding, removing, and reordering columns) and resorted (by clicking on a column header).
- The “Description” column shows the device name, if it can be determined (i.e., through NetBIOS); otherwise, it simply displays the device’s MAC address.
- The “Operating system” column shows the operating system of the device, which is determined through OS fingerprinting (the unique pattern by which a particular operating system requests an IP address via DHCP).

• An administrator can mouse over a row in the device list to see a new line appear in the usage graph, which depicts the fraction of total bandwidth that the highlighted device used.

Access Point List

The Access Point list is a convenient way to make it easier to find, sort and filter APs in a large network with hundreds or thousands of APs is using AP tagging.

AP Tagging

Alphanumeric tags can be assigned to access points to create groups of APs by location (e.g. Building_1, Floor_4, West_Campus, etc.) or by other criteria. The Access Points page is searchable by tag to make filtering for specific groups of APs fast and easy.

AP's can be tagged individually on the AP details page, or in the AP page by selecting multiple AP's and choosing Action->Add Tags.

Export Access Point Data

List data on the Access Points pages can be exported in XML format for further processing and analysis. An administrator can click on the “Download as XML” link to retrieve the data. Most spreadsheet programs, such as Microsoft Excel, can open an XML file.

Maps and Floor Plans

The aerial map shows the latest information about the APs in the network. The options in the upper-right corner enable an administrator to view the APs on top of a graphical map, a satellite image, or a hybrid view. In the upper-left corner, the arrow controls enable the administrator to pan. Panning can also be achieved by clicking-and-dragging the map. Below the arrow controls, a scale control enables the administrator to adjust the zoom level. The zoom level can also be controlled with the magnifying glass next to the arrow controls, or by double- clicking on a particular region to zoom into.

An administrator can click on an AP to get its name, its mesh mode (mesh gateway or mesh repeater), the number of users that have associated to it in the last 24 hours (also indicated by the number inside the AP), and the amount of data that it has transferred in the last 24 hours. Gray lines between APs represent mesh links.

The “Gear” box in the upper right part of the map lets users select what the numbers in the APs represent (e.g., number of clients connected or mesh hops to gateway), as well as preferences about how to display mesh links.

The “Current clients” link under the network name in the upper left corner, when clicked, will open up a table showing a summary of the distribution of current clients at that moment across the various SSIDs and channels in the network.

Clicking on the link directly above the network name in the upper left corner or selecting the All-network Overview option under the Network drop-down selector at the top of the screen will take the administrator to the All Network Overview page.

AP Color Codes

On the map and in the list the status of the AP is indicated by its color:

- **Green:** The AP is not reporting any problems.
- **Yellow:** The AP is up but experienced a problem recently. In some cases, the administrator may be able to clear this alert on the Access Points page.
- **Red:** The AP is currently down.
- **Gray:** The AP has been down for more than 7 days.

Summary Report Overview

Summary Reports provide a variety of statistics relating to usage on wireless, switch, and security appliance networks. The Summary Report page can be found by navigating to **Organization > Monitor > Summary Report**. This article will provide an overview of what information is available, and how to email or schedule recurring reports

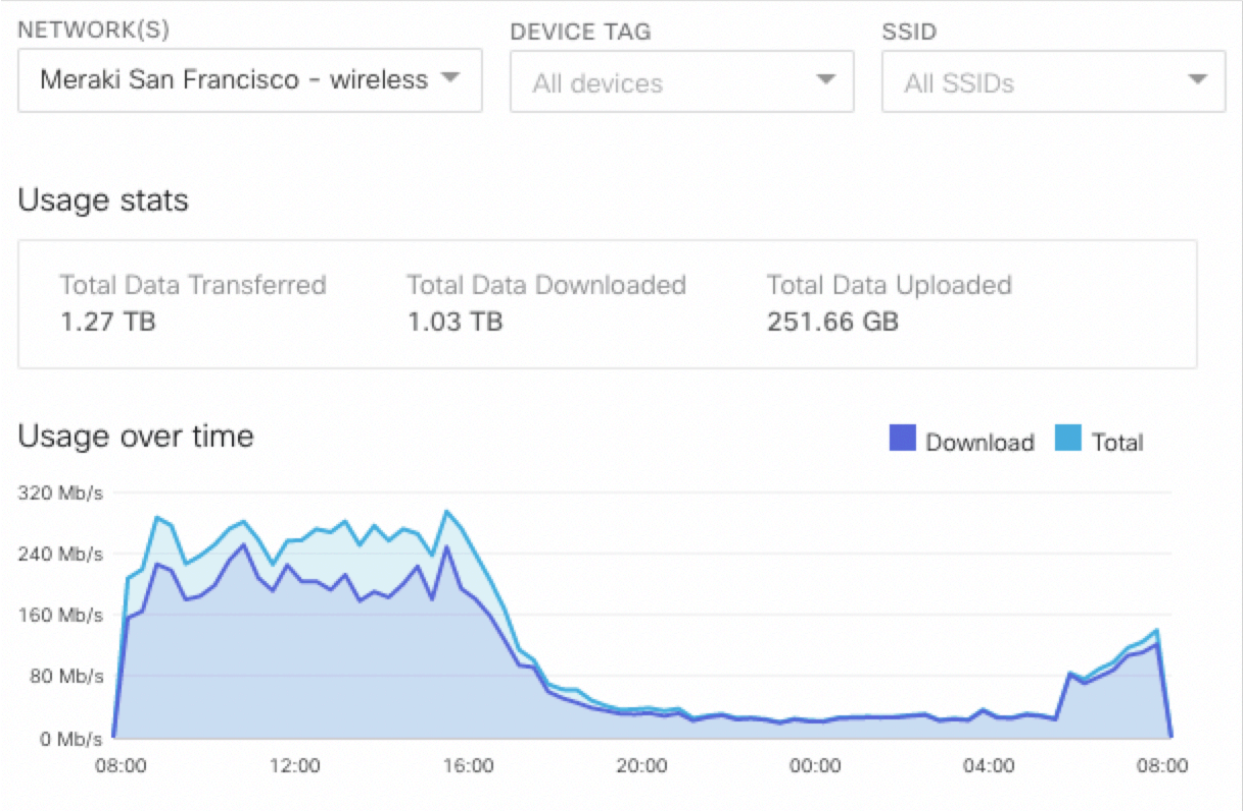
- Common report sections
- Product-specific report sections
- Emailing and scheduling reports

Common report sections

Most Summary Report sections will be available for each network type (wireless, security appliance, and switch). The sections below will provide an example a brief explanation. Example screenshots are from a Wireless network.

Usage

Provides a high-level overview of total traffic across all devices on this network over the time period selected ('last week' in the example below). The quantities next to the section header indicate the total amount of data traffic in each direction (upload/download) over the course of the time period. The graph will show the average total network usage over time.



Top devices by usage

Lists the top 10 Cisco Meraki devices in the network, ranked by total network usage, along with the total number of unique clients that used the device.

Top devices

Name	Model	# Clients	Usage	Usage %
	MR53	195	127.59 GB	9.78%
	MR42	127	83.23 GB	6.38%
	MR42	224	60.35 GB	4.63%
	MR42	116	57.65 GB	4.42%
	MR52	176	41.61 GB	3.19%
	MR42	86	39.76 GB	3.05%
	MR42	74	38.94 GB	2.99%
	MR34	49	37.67 GB	2.89%
	MR42	167	35.65 GB	2.73%
	MR42	74	28.56 GB	2.19%

Top clients by usage

Lists the top 10 clients on the networked based on total usage (upload and download) during the time period. **% Usage** is the % of total usage on this network that was tied to this client. If individual clients are generating higher than desirable amounts of traffic, consider applying group policies to those clients in order to limit their usage. Alternatively, consider using global traffic shaping rules, on wireless or security appliance networks.

Top client device manufacturers by usage

Similar to **Top clients by usage**, this section lists the top 10 device manufacturers by total usage. In addition to aggregate information from the section above, it also provides a total number of clients with the indicated manufacturer.

Top clients by usage

Description	Usage	Usage %
	125.49 GB	9.62%
	78.19 GB	6.00%
	17.06 GB	1.31%
	14.38 GB	1.10%
	13.06 GB	1.00%
	12.96 GB	0.99%
	11.25 GB	0.86%
	11.08 GB	0.85%
	10.05 GB	0.77%
	8.99 GB	0.69%

Top client device manufacturers by usage

Manufacturer	Usage	# Clients	% Clients
Apple	910.61 GB	925	72.66%
Intel	318.37 GB	269	21.13%
AzureWave Technology	43.29 GB	14	1.10%
VMware	7.43 GB	14	1.10%
Other	7.27 GB	1	0.08%
Microsoft	5.41 GB	2	0.16%
Rivet Networks	3.82 GB	3	0.24%
Samsung(THAILAND)	2.09 GB	16	1.26%
Murata Manufacturing	2.00 GB	8	0.63%
HTC	1.35 GB	11	0.86%

Top device models by per-device usage

Lists the top 10 Cisco Meraki device models in this network based on average usage (upload and download) per device.

Top applications by usage

Lists the top 10 applications on this network based on overall usage (upload and download).These applications should align with those used for Traffic Analytics. If undesirable applications are generating large amounts of traffic, utilize layer 7 firewall rules to block or restrict traffic.

Top device models by usage

Model	# Devices	Usage	Average Usage per Device
MR34	3	45.41 GB	15.14 GB
MR18	1	14.68 GB	14.68 GB
MR42	72	854.35 GB	11.87 GB
MR32	7	80.13 GB	11.45 GB
MR53	17	193.75 GB	11.40 GB
MR52	7	75.91 GB	10.84 GB
MR30H	4	9.55 GB	2.39 GB

Top applications by usage

Application	Usage	Usage %
Miscellaneous secure web	191.61 GB	15.04%
Meraki HTTPS	180.65 GB	14.18%
iTunes	151.82 GB	11.92%
Software updates	139.27 GB	10.93%
UDP	82.69 GB	6.49%
Google HTTPS	61.54 GB	4.83%
YouTube	59.53 GB	4.67%
WebEx	50.04 GB	3.93%
Miscellaneous web	46.02 GB	3.61%
Non-web TCP	40.5 GB	3.18%

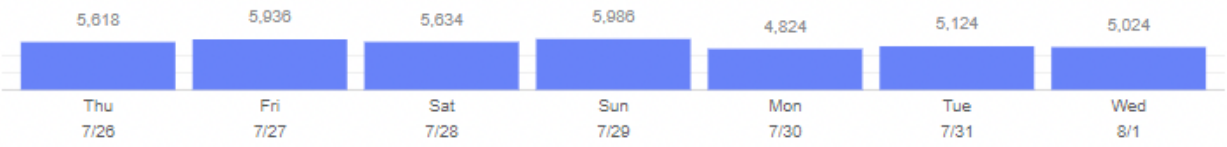
Top operating systems by usage

Lists the top 10 Operating Systems (OS) on the network based on overall usage (upload and download), along with a count of how many clients on the network are using that OS.

Number of sessions over time

Lists the number of wireless device sessions per day. A session is defined as a series of wireless probes from one device, with no more than a 5-minute gap in between adjacent probes. If the "All SSIDs" view of the page is selected, then sessions from unassociated devices will be included, as well as sessions from devices associated to any SSID. If a specific SSID is selected, then only sessions from devices associated with that SSID will be included.

Number of sessions over time



Top operating systems by usage

OS	Usage	# Clients	% Clients
Mac OS X	819.98 GB	591	46.43%
Windows	283.71 GB	241	18.93%
iOS	62.54 GB	324	25.45%
Windows 7	42.59 GB	59	4.63%
Chrome OS	42.18 GB	14	1.10%
Other	14.72 GB	28	2.20%
Android	5.29 GB	39	3.06%
Windows 8	1.37 GB	3	0.24%
Cisco Teleconference	1.20 GB	1	0.08%
Meraki Network OS	120.7 MB	2	0.16%

Wireless Health BETA for the last week

Overview Connections Packet latency

% FAILED CONNECTIONS 9.4%

AVG WIRELESS LATENCY 20ms

Health by AP | Health by client device type

Connection issues by client device type

These client device types have the most trouble connecting to the network

Device type	# client devices w/ problems	% client devices w/ problems
Apple iPhone	0 client devices	0%
Android	0 client devices	0%
Windows 10	1 client device	33.3%
Mac OS X	0 client devices	0%
Windows	0 client devices	0%

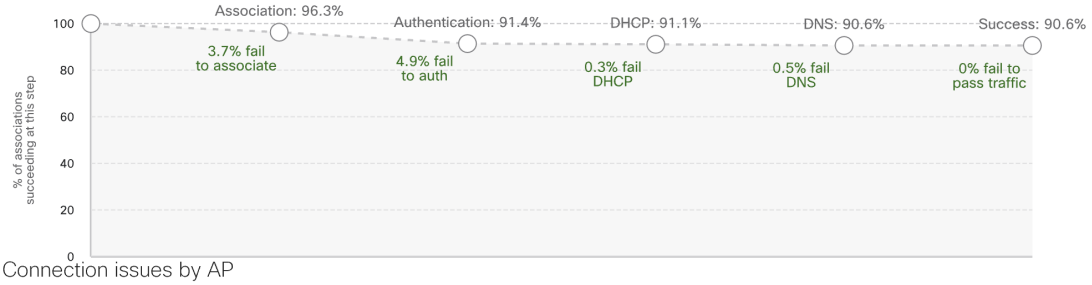
TOTAL CONNECTIONS 6055

FAILED CONNECTIONS 565

CLIENT DEVICES W/ PROBLEMS 61

AVG # FAILED CONNECTIONS PER PROBLEMATIC CLIENT 9

Are there problematic connection steps?



Connection issues by AP

AP	# client devices w/ problems	% client devices w/ problems	Primary failure stage	# failed connections
AP Sala Conferencia	4 client devices	2.3%	Authentication	181 failed connections
AP Sala Pilotos	5 client devices	6.3%	Association	163 failed connections
AP Lobby	5 client devices	3.1%	Authentication	132 failed connections
AP Deli	4 client devices	3.8%	Authentication	89 failed connections

5 results per page 1

Connection issues by client

Client device	% failed connections	# failed connections	Primary failure stage
iPhone	10%	92 connections	Association
iPhone	20.3%	53 connections	Authentication
iPhone	17%	33 connections	Authentication
Android	23.4%	29 connections	Association
34:14:5f:a3:0b:b7	14.2%	25 connections	DNS

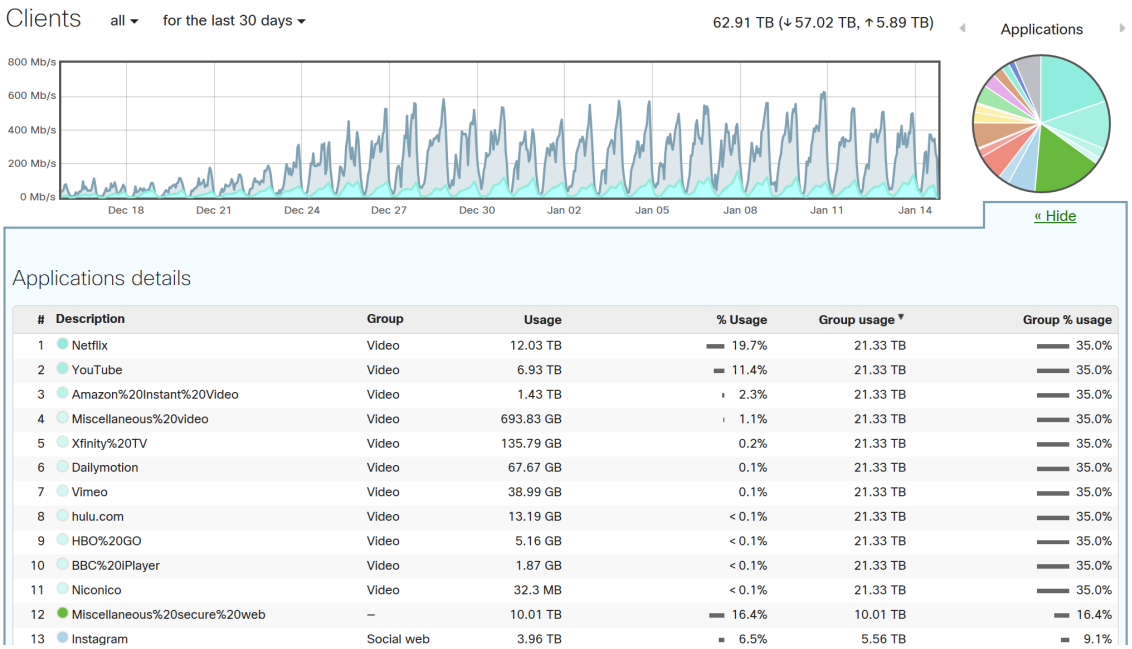
5 results per page 1 2 3 ... 41 42

Access points for the last day

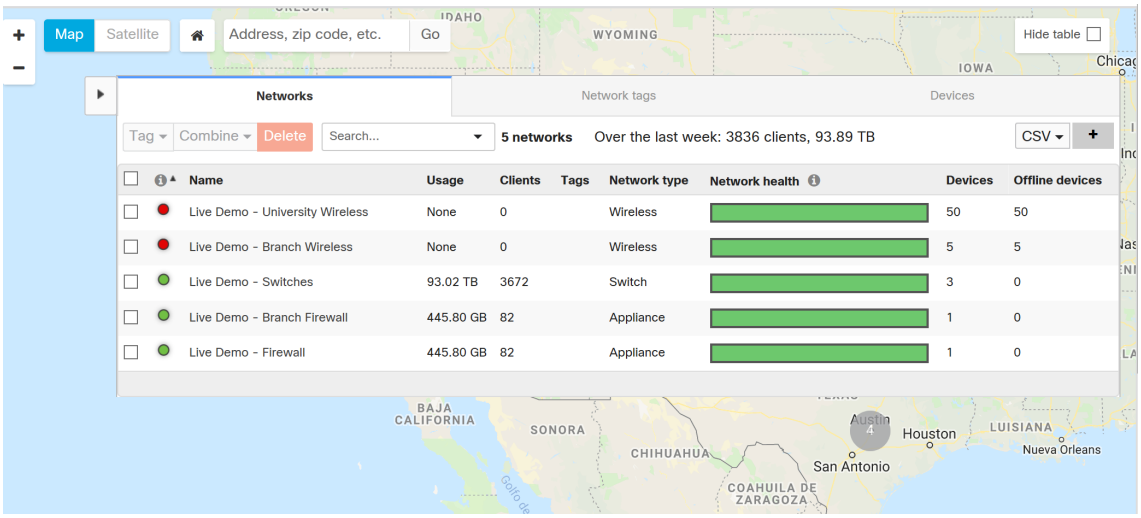
OFFLINE	ALERTING	ONLINE	REPEATERS
0	0	5	0

Edit Search 5 access points Add APs Download As

	Status	Name	MAC address	Model	Connectivity
1		Acme Southwest	02:02:00:59:a9:11	MR16	
2		Acme Southeast	02:02:00:59:a9:12	MR16	
3		Acme Northwest	02:02:00:59:a9:10	MR16	
4		Acme Northeast	02:02:00:59:a9:0f	MR16	
5		Acme North	02:02:00:59:a9:0e	MR16	



#	Description	Group	Usage	% Usage	Group usage	Group % usage
1	Netflix	Video	12.03 TB	19.7%	21.33 TB	35.0%
2	YouTube	Video	6.93 TB	11.4%	21.33 TB	35.0%
3	Amazon%20Instant%20Video	Video	1.43 TB	2.3%	21.33 TB	35.0%
4	Miscellaneous%20video	Video	693.83 GB	1.1%	21.33 TB	35.0%
5	Xfinity%20TV	Video	135.79 GB	0.2%	21.33 TB	35.0%
6	Dailymotion	Video	67.67 GB	0.1%	21.33 TB	35.0%
7	Vimeo	Video	38.99 GB	0.1%	21.33 TB	35.0%
8	hulu.com	Video	13.19 GB	< 0.1%	21.33 TB	35.0%
9	HBO%20GO	Video	5.16 GB	< 0.1%	21.33 TB	35.0%
10	BBC%20iPlayer	Video	1.87 GB	< 0.1%	21.33 TB	35.0%
11	Niconico	Video	32.3 MB	< 0.1%	21.33 TB	35.0%
12	Miscellaneous%20secure%20web	–	10.01 TB	16.4%	10.01 TB	16.4%
13	Instagram	Social web	3.96 TB	6.5%	5.56 TB	9.1%



Name	Usage	Clients	Tags	Network type	Network health	Devices	Offline devices
Live Demo - University Wireless	None	0		Wireless		50	50
Live Demo - Branch Wireless	None	0		Wireless		5	5
Live Demo - Switches	93.02 TB	3672		Switch		3	0
Live Demo - Branch Firewall	445.80 GB	82		Appliance		1	0
Live Demo - Firewall	445.80 GB	82		Appliance		1	0

Product-specific report sections

Wireless specific sections

Wireless networks will also provide a section titled **Top SSIDs by usage**. This section will list the top 10 SSIDs configured on the network, based on their overall usage (upload and download), and will provide the total number of unique clients that were seen on the SSID.

Top SSIDs by usage

Name	Encryption	# Clients	Usage	Usage %
Meraki-Corp	802.1x	1010	1.01 TB	81.44%
Office	802.1x	3	5.37 GB	0.42%
Guest	Open	1	1.2 GB	0.09%

Emailing and scheduling reports

Besides viewing the summary report in Dashboard, it is also possible to have the report emailed once or on a recurring basis. Look along the top right of the **Summary Report** page for these options.

Emailing reports

To email a one-time report:

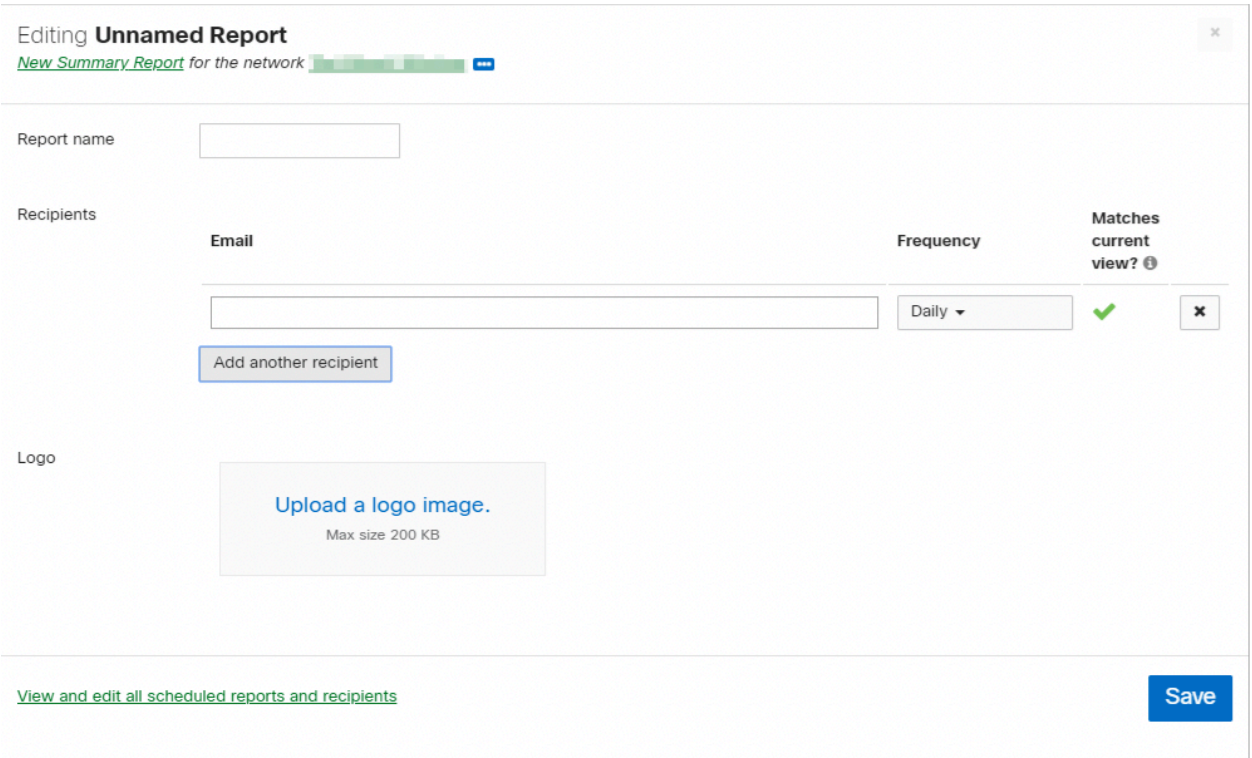
1. Click on the **Mail** icon and select **Email**.
2. Enter an email **Address**.
3. Click **Email Report**.

Scheduling reports

Reports can also be scheduled to occur daily, weekly, or monthly. To schedule a report:

1. Click **Schedule report**.
2. If a logo is desired this can be added in the Logo section. This logo will be applied to ALL new and existing scheduled reports.
3. Name the report in the **Report name** field.
4. Add an email address in the **Recipients** section by clicking **Add another recipient**.
5. Choose the desired **Frequency**.
6. Click **Save**.

To remove an existing scheduled report, just click the **X** at the end of the row. Existing reports can also be modified by simply changing the selections in the row. In both cases, click **Save** to save the changes. To modify multiple scheduled email reports at once, select the **View all scheduled reports and recipients** link.



VII. CONTRACT/SERVICE CHANGES FOR PROPOSED WIFI

The following circumstances are already contemplated in the per location pricing included:

i. If the Department experiences a significant increase or decrease in service requirements because of new construction, closures or consolidations
ii. The Department wishes to modify the type of services utilized by the Department under the contract due to network and technology optimizations or new technology release

VIII. PROBLEM ESCALATION PROCESS

- **Escalation List – Tech Support:**

First Level - Help Desk Specialists

Hours: 24/7
O: (787) 706-2700 Ext. 2740
helpdesk@dreyfous.com

Second Level – Technology Services Manager

Manuel Somohano
O: 787-706-2700 Ext. 2705 | C: 787-469-6041
msomohano@dreyfous.com

Third Level – Network Operations Center

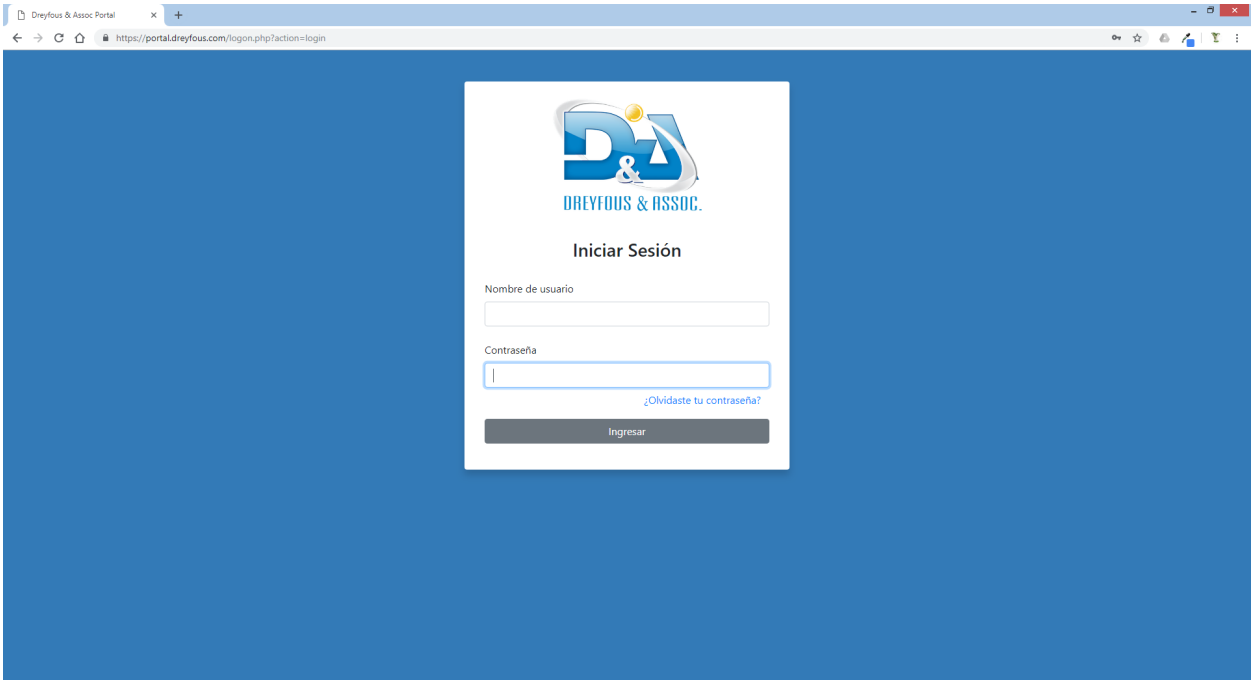
Ricardo Turino
O: (787) 706-2700 Ext. 2722
rturino@dreyfous.com

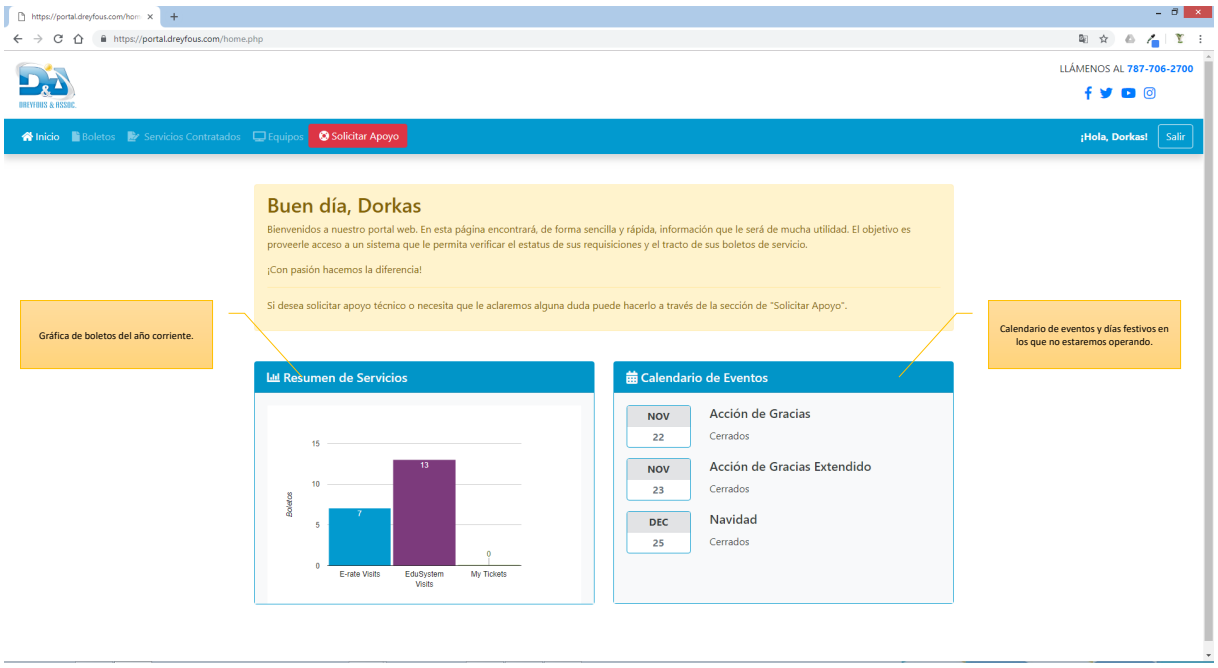
Alexander López
O: (787) 706-2700 Ext. 2707 | C: (787) 375-4182
alopez@dreyfous.com

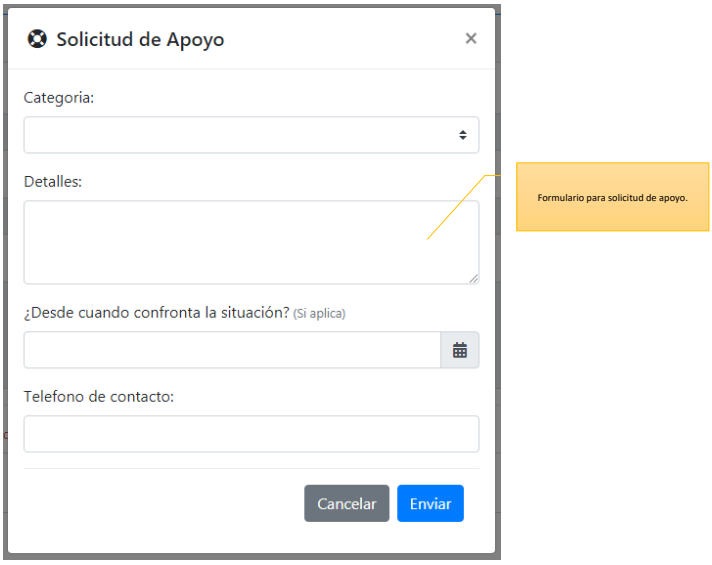
Fourth Level – CEO / FOUNDER

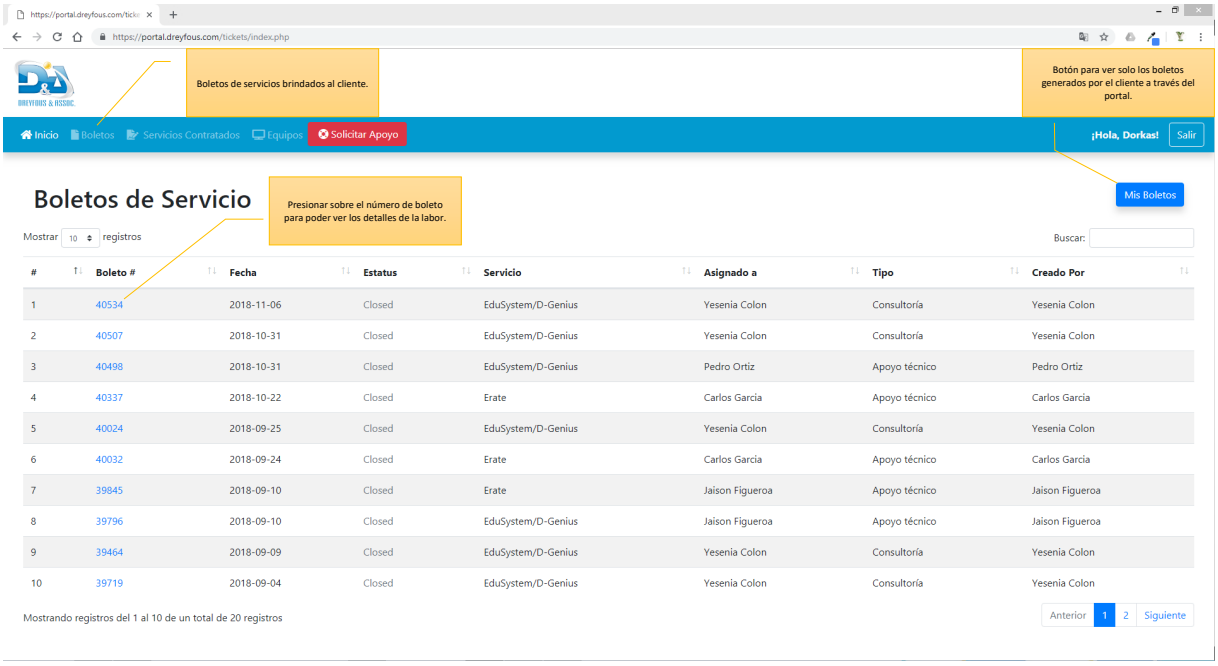
Dr. Ricardo Dreyfous
O: (787) 706-2700 Ext. 2701 | C: (787) 506-1006
rdreyfous@dreyfous.com

- **Client Support Portal:**
  - **Ticket Creation**









#	Boleto #	Fecha	Estatus	Servicio	Asignado a	Tipo	Creado Por
1	40534	2018-11-06	Closed	EduSystem/D-Genius	Yesenia Colon	Consultoría	Yesenia Colon
2	40507	2018-10-31	Closed	EduSystem/D-Genius	Yesenia Colon	Consultoría	Yesenia Colon
3	40498	2018-10-31	Closed	EduSystem/D-Genius	Pedro Ortiz	Apoyo técnico	Pedro Ortiz
4	40337	2018-10-22	Closed	Erate	Carlos Garcia	Apoyo técnico	Carlos Garcia
5	40024	2018-09-25	Closed	EduSystem/D-Genius	Yesenia Colon	Consultoría	Yesenia Colon
6	40032	2018-09-24	Closed	Erate	Carlos Garcia	Apoyo técnico	Carlos Garcia
7	39845	2018-09-10	Closed	Erate	Jaison Figueroa	Apoyo técnico	Jaison Figueroa
8	39796	2018-09-10	Closed	EduSystem/D-Genius	Jaison Figueroa	Apoyo técnico	Jaison Figueroa
9	39464	2018-09-09	Closed	EduSystem/D-Genius	Yesenia Colon	Consultoría	Yesenia Colon
10	39719	2018-09-04	Closed	EduSystem/D-Genius	Yesenia Colon	Consultoría	Yesenia Colon

Dreyfous & Associates
EduSystem Service Ticket

PMB 641 HC-01 Box 29030
Caguas, PR 00725-9900
Tel. 787-706-2700
Fax: 787-789-2018

Ticket #: 40534 **WSR #**

Institution: Academia Cristiana Yarah **City:** Toa Baja

Date: 2018-11-06 **Arrival time:** 01:00PM **Visit duration:** 02:20

Technician: Yesenia Colon **Departure time:** 03:20PM

Project: EduSystem, D-Genius **Students attended:**

Administrators attended: 2 **Teachers attended:** 8

Level:

Course:

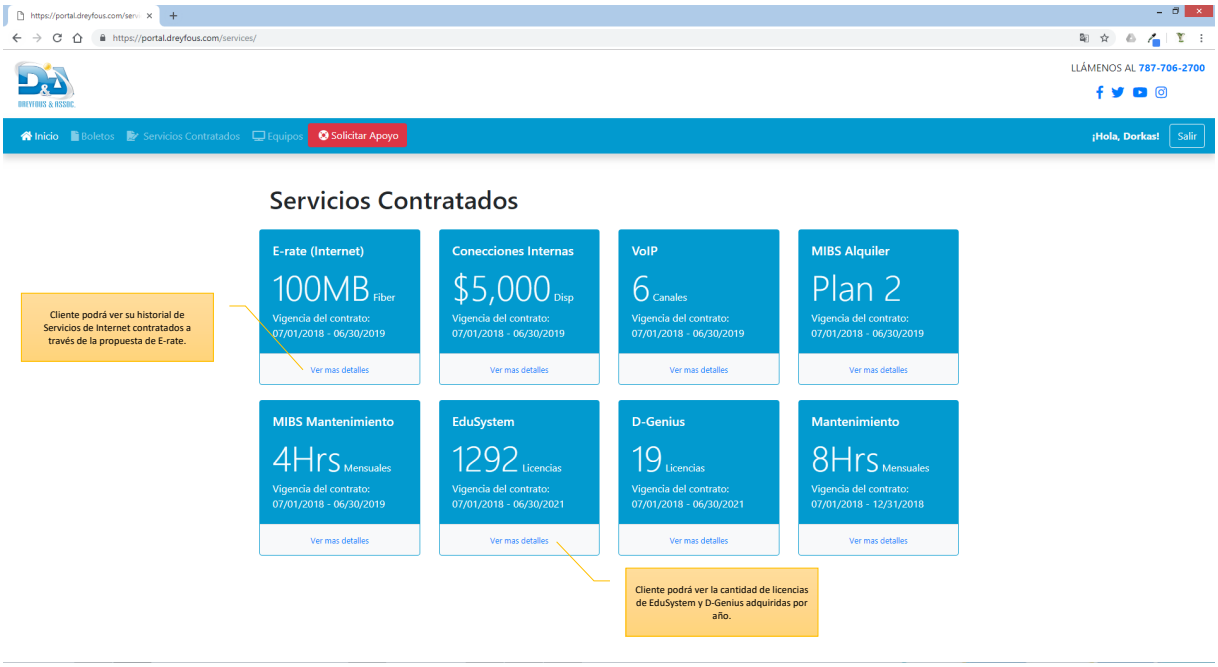
Services provided:
Administrative, , Project Orientation

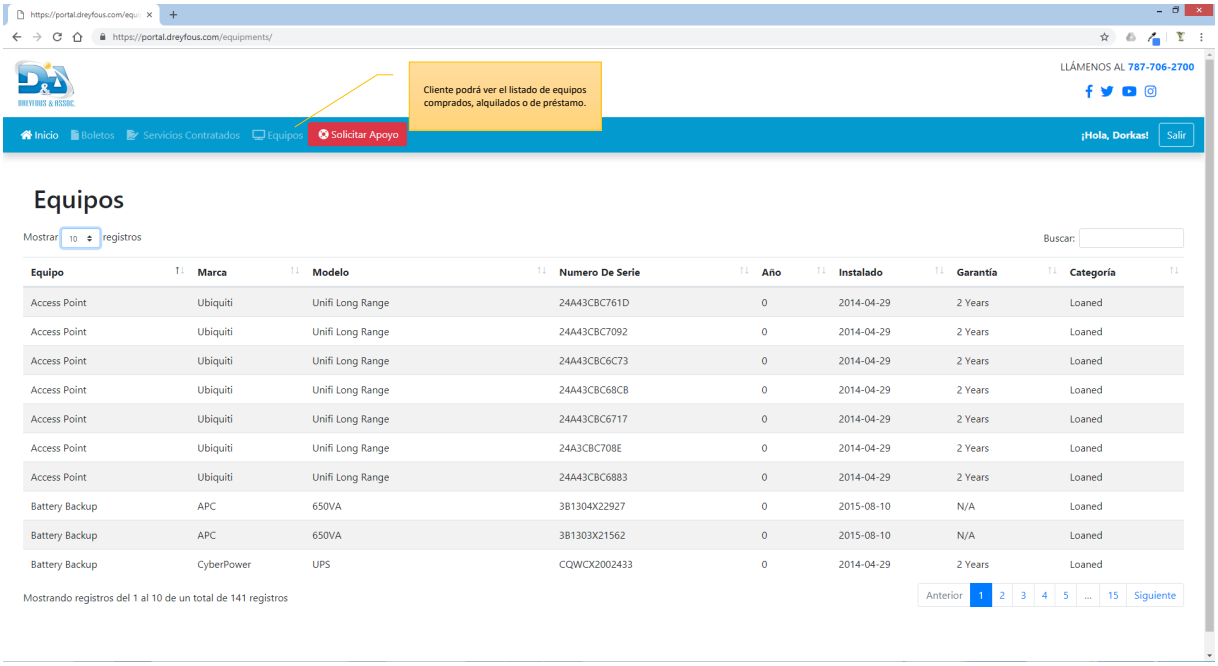
Visit details:
Visita de seguimiento a la institución me reuní con maestra Quiles (4to a 6to) indica que una de las hojas de trabajo (Reto matemático) tiene la equivocada de una lección anterior y solicita material adicional de geometría. Fui dónde los 2 maestros nuevos (inglés y matemáticas) y ambos me mostraron que lo están trabajando, calendarizando bien. La maestra de historia indica que todo bien al momento. En elemental Villegas y Bonilla bien al momento. Se coordinó visita para el miércoles 14 Nov con maestra nueva de D-Genius. Hablé con el principal y con Dorkas de lo acontecido.

Client name: Sra. Dorkas Felicie **Signature:**

Tue Nov 06 2018 @ 03:20PM

Ejemplo de boleto generado por empleado y firmado por cliente.



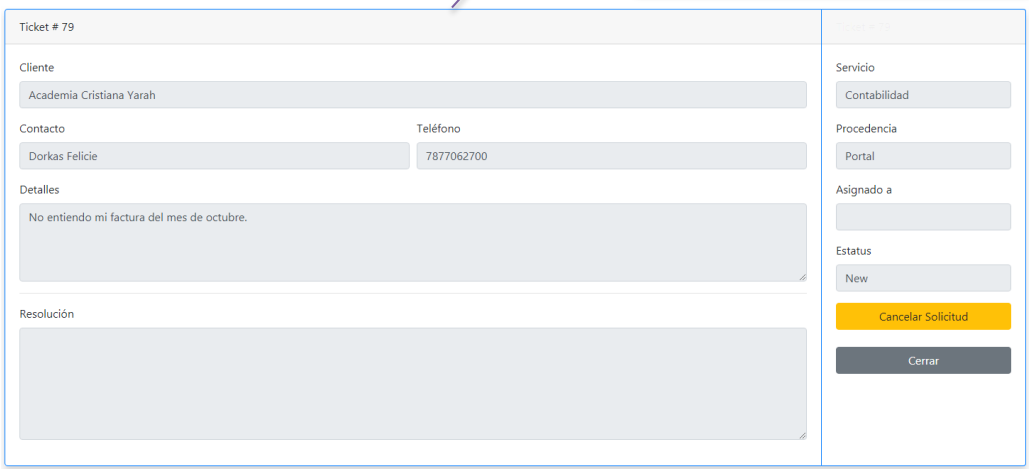


Equipo	Marca	Modelo	Numero De Serie	Año	Instalado	Garantía	Categoría
Access Point	Ubiquiti	Unifi Long Range	24A43CBC761D	0	2014-04-29	2 Years	Loaned
Access Point	Ubiquiti	Unifi Long Range	24A43CBC7092	0	2014-04-29	2 Years	Loaned
Access Point	Ubiquiti	Unifi Long Range	24A43CBC6C73	0	2014-04-29	2 Years	Loaned
Access Point	Ubiquiti	Unifi Long Range	24A43CBC68CB	0	2014-04-29	2 Years	Loaned
Access Point	Ubiquiti	Unifi Long Range	24A43CBC6717	0	2014-04-29	2 Years	Loaned
Access Point	Ubiquiti	Unifi Long Range	24A3CBC708E	0	2014-04-29	2 Years	Loaned
Access Point	Ubiquiti	Unifi Long Range	24A43CBC6883	0	2014-04-29	2 Years	Loaned
Battery Backup	APC	650VA	3B1304X22927	0	2015-08-10	N/A	Loaned
Battery Backup	APC	650VA	3B1303X21562	0	2015-08-10	N/A	Loaned
Battery Backup	CyberPower	UPS	CQWCX2002433	0	2014-04-29	2 Years	Loaned

IX. BILLING DISPUTE RESOLUTION FOR ALL PROPOSED SERVICES

Shall our Company be awarded this contract; the Department of Education will have access to our web-based Client Service Portal. The Department of Education would identify one or more employees, who will be granted access to manage billing dispute issues. Our Portal would provide a dashboard option to request support, selecting Accounting/Billing on the Category box, then detailing the issue below, and a phone number to contact. After sending the support request, our company will process the request, on a time frame of 48 hours, subject to working days. Our Accounting Department would process these requests directly by our Accounting Assistants, and monitored by the Accounting Supervisor, who shall intervene for an escalation process. On our Client Service Portal, authorized employees from the Department of Education would be able to track their requests; to validate whether the request is in process of evaluation, or if the evaluation process has ended.

Example: Billing dispute ticket using our client portal.



- **Escalation List - Accounting:**

First Level - Accounting Assistant

Zamilka Figueroa
O: 787-706-2700 Ext. 2730
zfigueroa@dreyfous.com

Second Level – Accounting Manager

Naomi Ojeda
O: 787-706-2700 Ext. 2708
nojeda@dreyfous.com

X. Case Study:

Colegio San Ignacio

Highlights

- **Colegio en Puerto Rico instala red inalámbrica para estudiantes y colaboradores**
- **Más de 700 estudiantes distribuidos en 7 edificios, además de 150 colaboradores**
- **47 puntos de acceso internos y externos MR62/MR72**

El Colegio San Ignacio de Loyola de Puerto Rico fue fundado hace más de sesenta años por un grupo de españoles Jesuitas motivados a ofrecer educación católica en la capital de esta cálida isla del caribe.

Este colegio privado ubicado en San Juan de Puerto Rico ofrece educación secundaria a más de 700 estudiantes distribuidos en 7 edificios, además de 115 colaboradores entre profesores y personal administrativo. Andrés Torres es el encargado de que todo lo relacionado a la tecnología funcione de manera eficiente, entre sus responsabilidades esta ofrecer una red inalámbrica que fomente el aprendizaje y la colaboración entre profesores y estudiantes.

Retos que tenía del departamento de tecnología:

Tenían una solución de compleja administración que no soportaba las exigencias del colegio en cuanto a velocidad y seguridad.

Contaban con una solución obsoleta que les dificultaba analizar el comportamiento de los usuarios y adaptar la red según las necesidades específicas.

Necesitaban una red de fácil administración que les enviara alertas y les permitiera hacer troubleshooting.

Querían encontrar una solución que no necesitara un equipo de TI numeroso.

Por qué Cisco Meraki

Andrés Torres, gerente de tecnología, escuchó en una reunión anual de colegios jesuitas en Estados Unidos sobre las ventajas de una solución de administración de redes en la nube llamada Meraki. Tras escuchar esto Andrés investigó y participó en el webinar *Introducción a la Nube* que le permitió probar el punto de acceso MR32 y entender lo sencillo que era administrar redes con Meraki.

“Al volver del viaje, me uní al webinar para optar por el punto de acceso gratis. Cuando me llegó lo conecté rápidamente y sin problema. Comencé a ver cómo funcionaba y hacer cosas que antes no podía hacer como segregar varios SSID’s al mismo tiempo y manejar el ancho de banda entre otras cosas” Andrés Torres.

Andrés también nos comentó que en un principio también probó el equipo de seguridad MX400 durante un mes lo que le permitió hacer todo el análisis de lo que necesitaba instalar en el colegio, sorprendiéndole la relación precio valor.

La implementación y administración

- Instalación por fases según las necesidades específicas del Colegio.
- Implementación de 47 puntos de acceso internos MR32/MR34 y externos MR66/MR72.
- Implementación de equipos de seguridad y firewall MX400

· Configuración de 3 SSID's: personal administrativo, estudiantes y equipos de tecnología.

· Cisco Meraki les permite hacer filtrado de contenidos y bloquear páginas de juegos, descargas y aquellas que congestionan la red, incluyendo catalogación de tráfico (traffic shaping).

· Los estudiantes y el personal se conecta a la red mediante la autenticación RADIUS Meraki, mientras que los huéspedes se proporcionan conexiones temporales con las restricciones de ancho de banda por SSID y por cliente.

"Al ser el único que administra la red en el Colegio, Cisco Meraki ha hecho del manejo de la red una labor más sencilla y eficiente" comentó Andrés

Resultados

· Todas las áreas de aprendizaje tienen WiFi

· El equipo de TI puede establecer restricciones basadas en el tiempo en cada SSID, asegurando uso de la red adecuada y la prevención de los huéspedes tengan acceso a la red durante las horas libres.

· Mientras que los estudiantes y profesores se benefician de la velocidad máxima de la red por primera vez, los huéspedes también están reportando una mejor experiencia del usuario con capacidades de login simples.

· El Dashboard de Cisco Meraki le ha facilitado la administración al equipo de TI ya que les permite tener visibilidad de usuarios, dispositivos y aplicaciones compatibles en los diferentes lugares, y también proporcionan un ambiente seguro para los estudiantes.

· Andrés es capaz de monitorear y solucionar problemas de su panel de control de forma remota y puede incluso añadir nuevos dispositivos a la red en cuestión de minutos y asignarle políticas.