D-Link Certified Specialist

[Nuclias Connect Hands-on Tutorial (Beta)]





About This Document

- This document is developed from users' hands-on tutorial perspective to explain the features and functionalities being offered by D-Link Nuclias Connect (Central WiFi Manager (CWM), as previous release).
- Reciting the list of D-Track KM statements presents an unique way of lessons learned from customer service experience.
- Any technology capabilities, being addressed here, are subject to change without further notice.
- The readers should understand that D-Link SHALL NOT be under any legal obligation of any kind whatsoever with respect to the accuracy or completeness of the information contained in this document.

D-Link SMB WLAN Solution (AP / Nuclias Connect)

- Advanced Product Portfolio
  - Indoor single band AP
  - Indoor dual band AP
  - Outdoor AP





- D-Link Nuclias Connect
  - An innovative tool streamline the wireless access point management workflow via a centralized server
  - Wireless AP software controller, up to 1,000 AP management
  - Multi-tenant structure and advanced WLAN configurations
  - Industrial Market Segmentation
    - SMB, Education, Chain store, Factory, and Hospitality
  - Target Market
    - Customers who require cost-effective central wireless management solution (no AP license charge)

Background Of A Story

- D-Link Central WiFi Manager (CWM)
  - Central WiFi Manager (CWM) eliminates the need for more costly hardware controllers and making this solution ideal for users spread across large geographic distances
  - CWM 1.03 supports DAP models: DAP-2230, DAP-2330, DAP-2360, DAP-2610, DAP-2660, DAP-2690, DAP-2695, and etc.
  - CWM 1.03 success story
    - Schools and Education
    - Government
  - In this document, “The legacy CWM” represents “CWM 1.03.”
- D-Link Nuclias Connect Project Management Office (PMO)

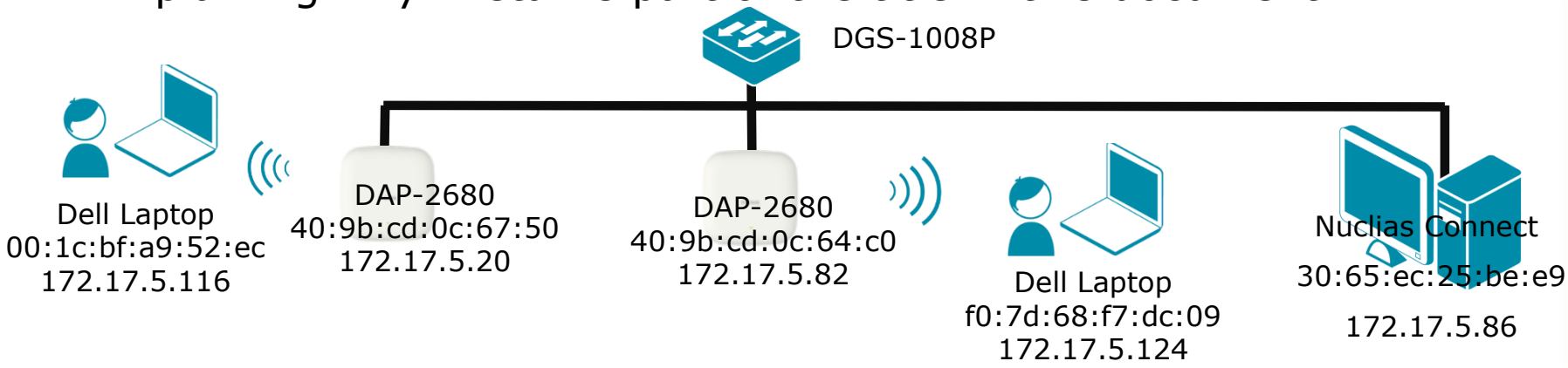
Background Of A Story

- D-Link Central WiFi Manager (CWM)
- D-Link Nuclias Connect Project Management Office (PMO)
  - Wireless characteristics and application behavior are defined by a team of subject-matter experts.
  - Dashboard and Reporting is designed by an industry-recognized proficient in statistics, features of a chart, as well as wireless traffic analytics.
  - Programming team, experience inheritance D-View 7 network management development, excellent information responding and troubleshooting skills.

Background Of A Story

To collect all the gears

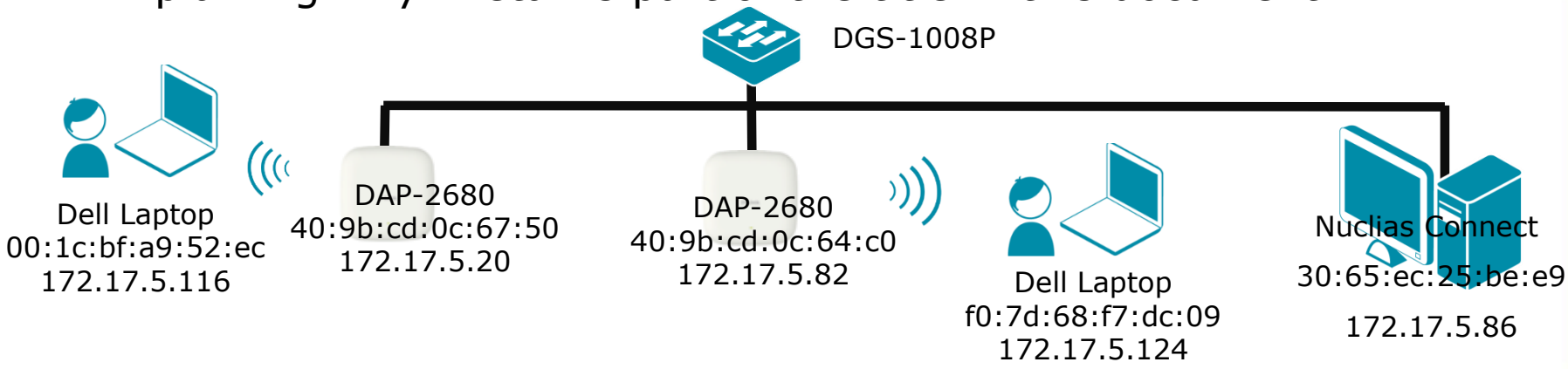
- Nuclias Connect beta firmware (v2.0.0.7 ~ v1.0.0.20)
- DAP-2680 beta firmware (v200rc020 ~ v200rc036)
- Explaining why “Beta” is part of the title in this document



Background Of A Story

To collect all the gears

- Nuclias Connect beta firmware (v2.0.0.7 ~ v1.0.0.20)
- DAP-2680 beta firmware (v200rc020 ~ v200rc036)
- Explaining why “Beta” is part of the title in this document



- One-sentence summary that the writer would like to communicate with the readers.

Proverb

"The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn."

By Alvin Toffler

Proverb

"The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn."

By Alvin Toffler

This page is intentionally left blank.

Nuclias Connect Hands-on Tutorial

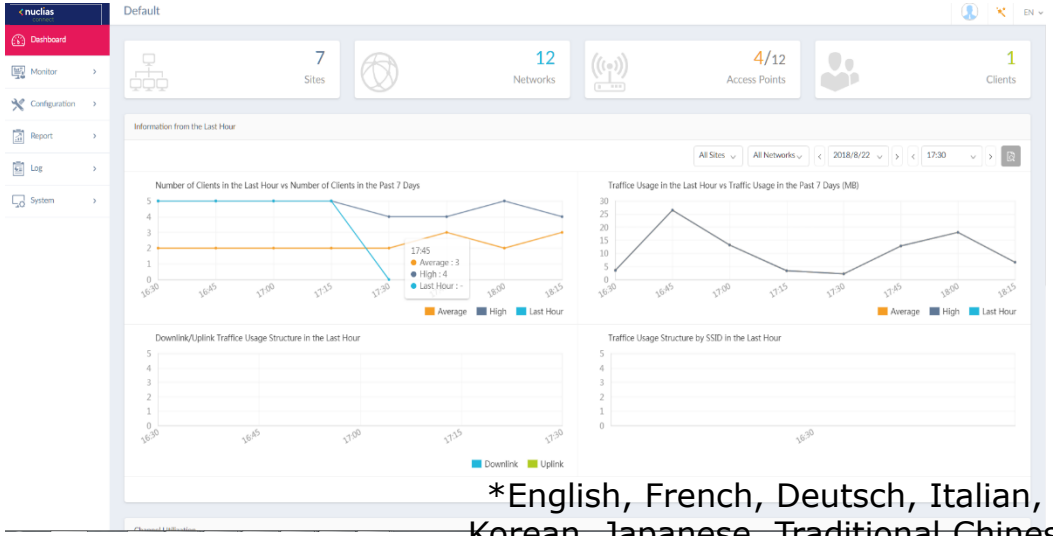
- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

Nuclias Connect Hands-on Tutorial

- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

Nuclias Connect Key Features

- Graphic dashboard GUI offers real-time network status information
- Setup wizard to guide admin easily provisioning and configuration
- L2/L3 Discovery, Captive Portal and Bandwidth Optimization
- Band Steering, IGMP snooping as well as multicast rate control
- Auto RF Management, Dashboard and Reporting System
- 10 languages support*





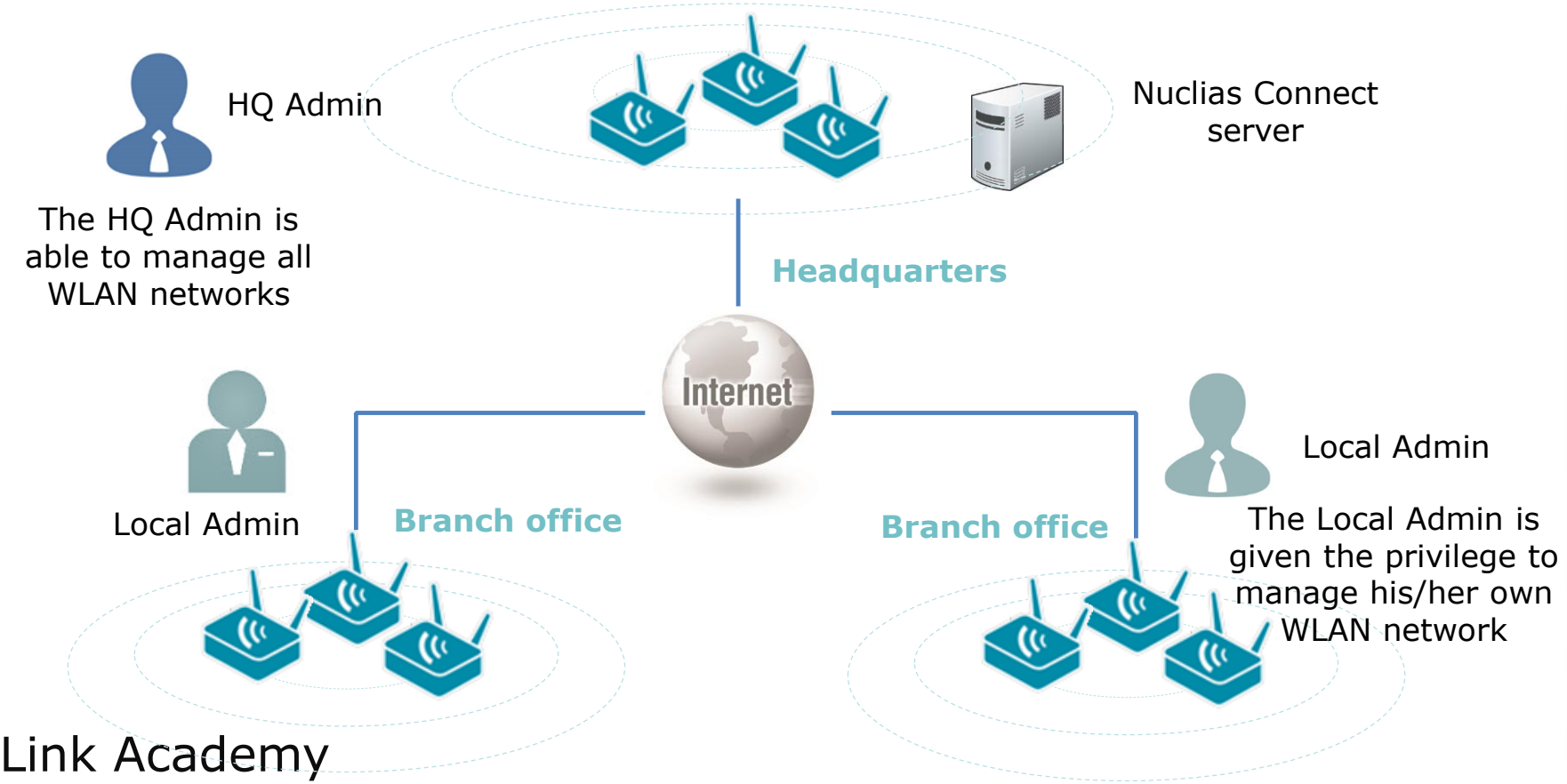




*English, French, Deutsch, Italian, Spanish, Korean, Japanese, Traditional Chinese, Simple Chinese, and Russian

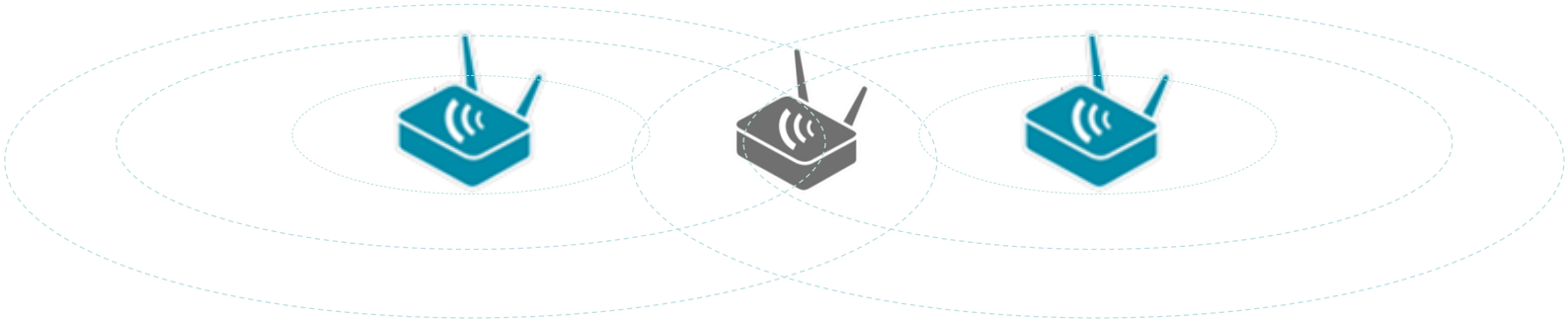
Multi-tenant Architecture In Nuclias Connect

- Offers multi-layer management authority in one controller for multi-site management [Page, 83th]



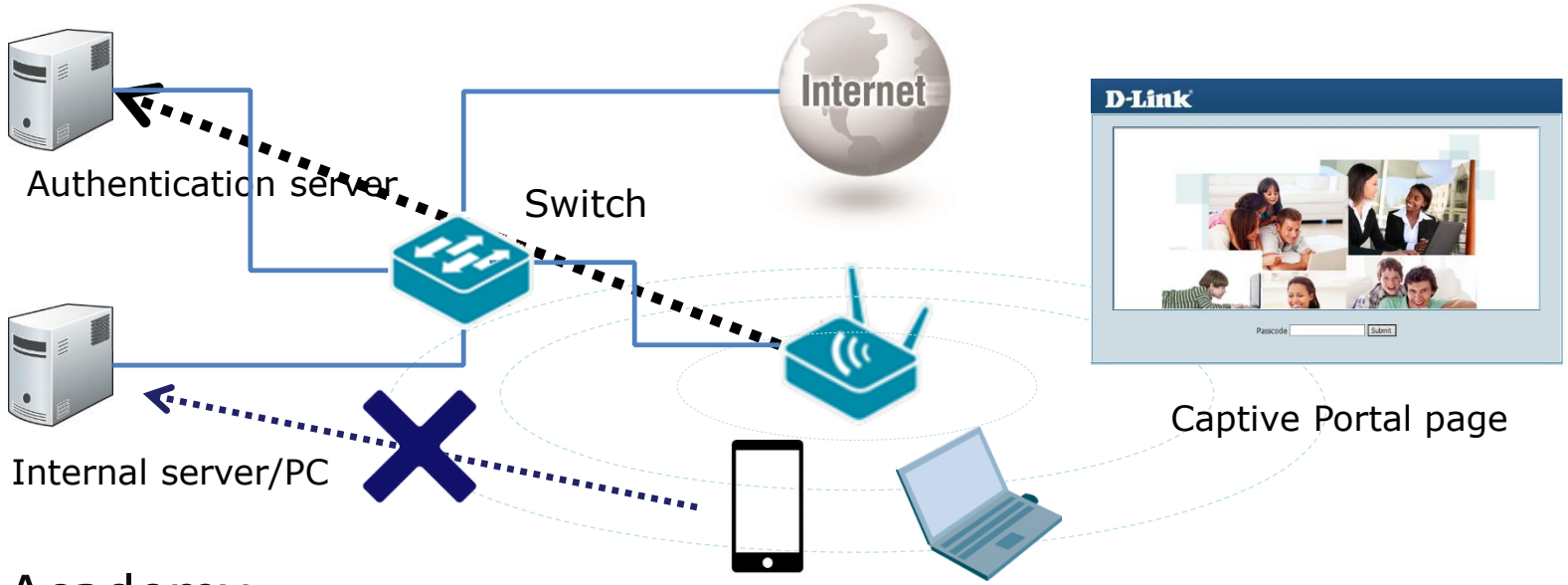
Auto RF Management in Nuclias Connect

- Auto Power and Channel Adjustment [page, 321th ~ 333th]
  - Channel and output power can be automatic adjusted to improve performance and enhance security
- RF self-healing
  - Provides automated RF recover functionality to compensate for RF dead zones and AP failures



Nuclias Connect Captive Portal and Access Control

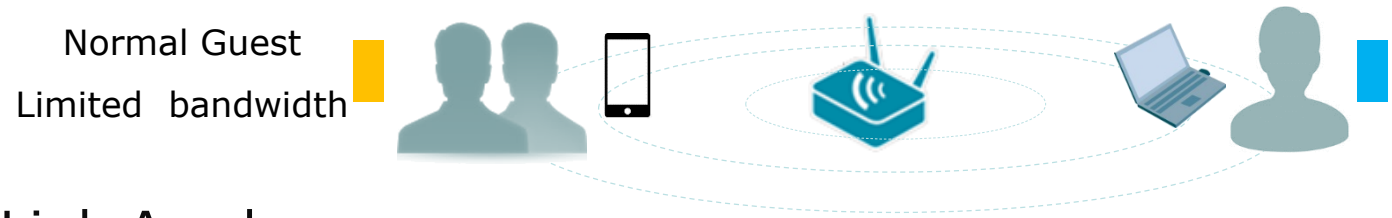
- Multiple authentication methods support
  - Supports local database, passcode authentication [page, 391th ~ 406th] external RADIUS, LDAP, and POP3
- Wireless User Access control
  - Restricted network function, such as MAC ACL [page, 384th ~ 390th], WLAN Partition [page, 441th ~ 445th], User Blocking [page, 446th ~ 455th]



Nuclias Connect Bandwidth Optimization

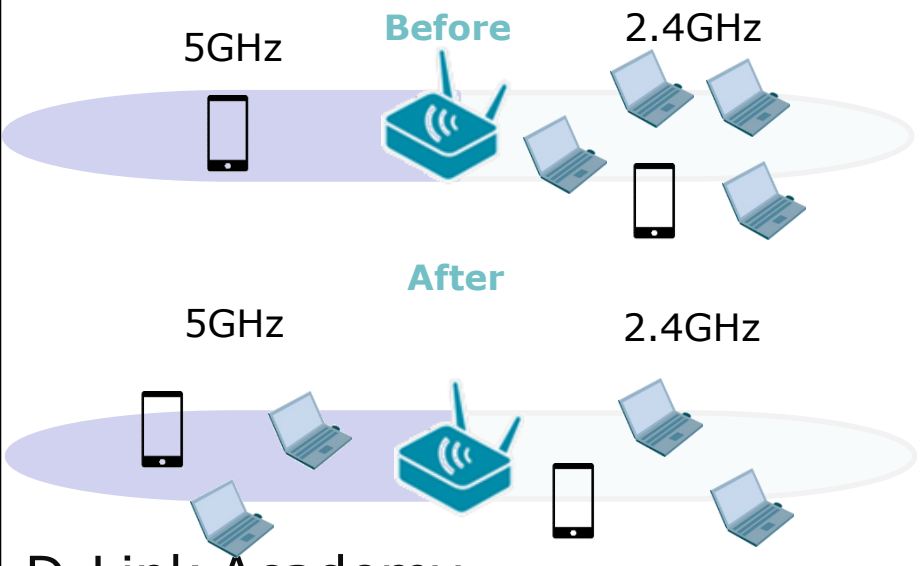
- Supports four type of wireless bandwidth allocation methods
  - Is utilized to optimize the network usage and performance, increase user productivity, satisfaction and performance of all applications

BW evenly allocated by SSID	Allocate specific BW by SSID	Allocate different BW for 11a/b/g/n station	Allocate maximum BW for all station
AP will distribute even bandwidth for each client	All clients share the total bandwidth	AP will distribute different bandwidth for 11a/b/g/n clients	Specify the maximum bandwidth for each connected client

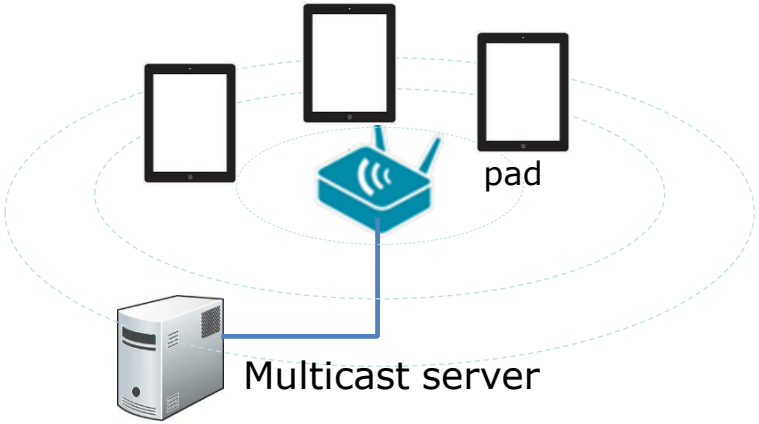


Nuclias Connect Band Steering/Multicast Rate Control

- Band Steering [page, 75th, 270th ~ 276th]
  - It triggers to balance the client loading in AP and establishes a more stable and quicker connection for all wireless clients.
- Multicast rate control and IGMP snooping
  - It provides enhanced multi-media transmitting features in multicast to improve the wireless quality.



Transfer multicast to unicast (IGMP snooping) or control multicast rate to improve performance



Nuclias Connect Product Bulletin

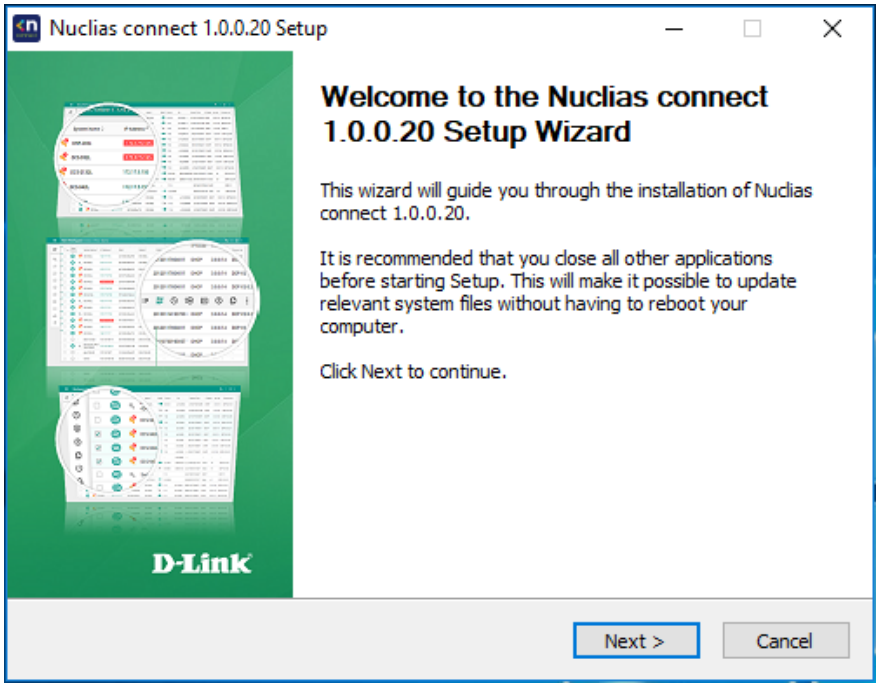
- From The legacy CWM to Nuclias Connect
  - Programming language: node.js (JavaScript runtime built)
  - Database tool, from PostgreSQL to MongoDB (both are advanced open source database).
    - During Nuclias Connect installation, the (MongoDB) database password inter-message process is no longer exist.
    - TCP 27017 is the default port for mongod and mongos instances. [A modification is made in official release: TCP27010.]
  - MongoDB is being adapted in D-Link D-View 7, a web-based network management software that provides an easy and efficient tool to manage wired and wireless devices in multiple locations.
- Any description in this document on "The legacy CWM" refers to CWM 1.03 version 1.03r0098.

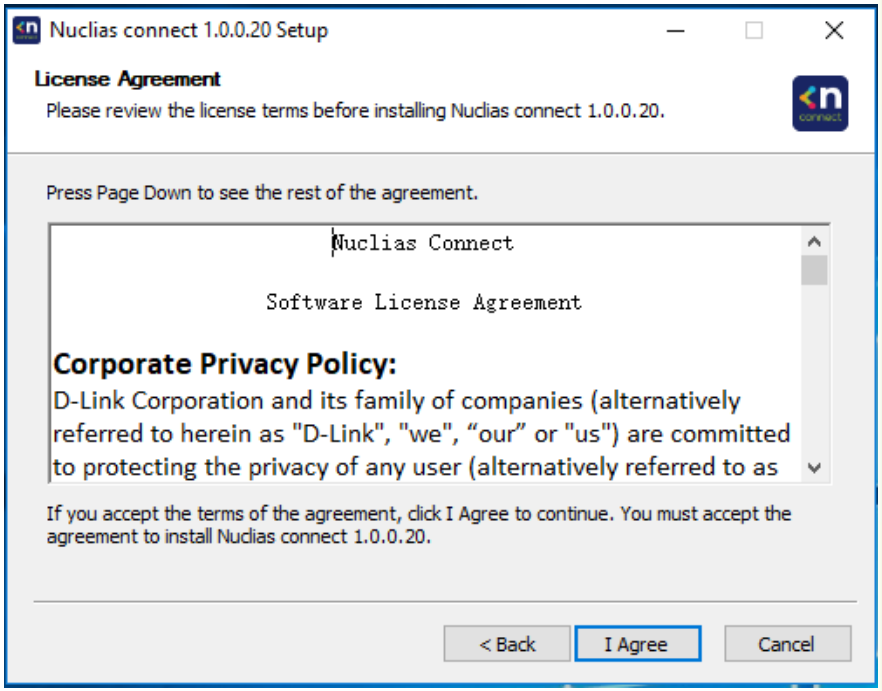
Nuclias Connect Product Bulletin

- System Requirements, the following minimum requirements are recommended on the computer used to run Nuclias Connect application.
- Hardware (Recommended Specs)
  - CPU: Intel Xeon processor E3-1200 v6 product family
  - RAM: 16GB DDR4
  - Minimum hard-drive space: HDD 3TB
  - Display Card: Windows Graphics Card
  - Installed Gigabit Ethernet LAN 10/100/1000 port
- Operating System
  - Supports Windows 7(64bit), Windows 10(64bit), Windows 2016(64bit), Linux system and MAC OS.
  - For Linux/MAC OS system, Docker installation is prerequisite.
  - Working in a virtual machine environment is a proven record.

Nuclias Connect Installation Process (1/6)

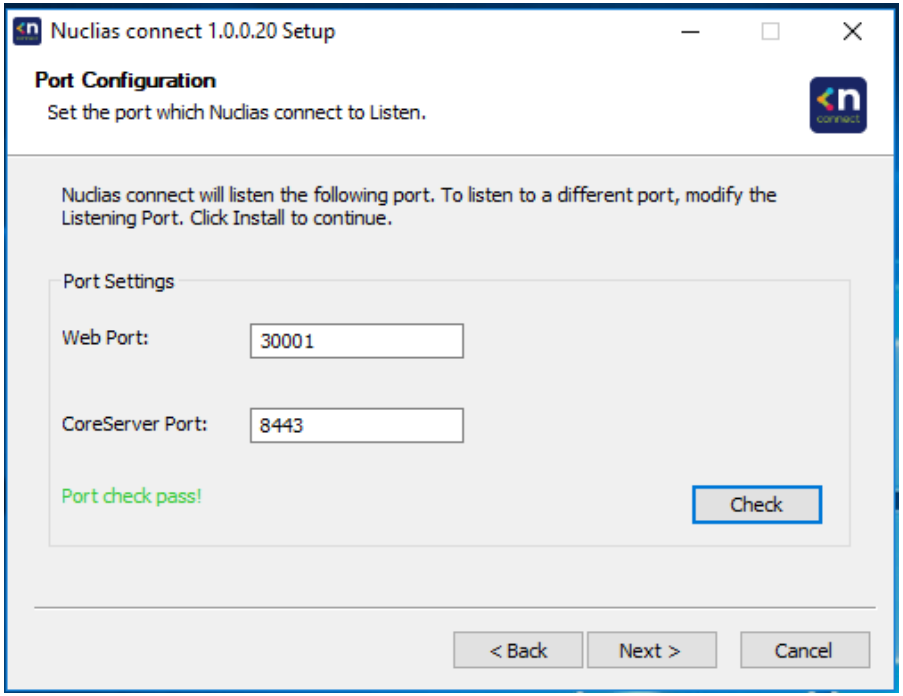
- Nuclias Connect Installation Process (Step by Step guide)

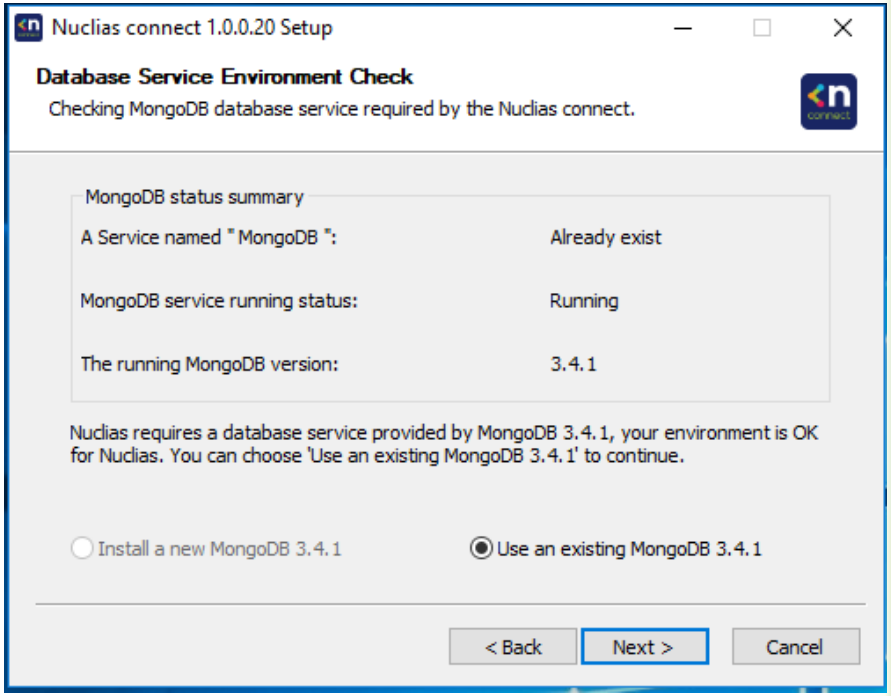




Nuclias Connect Installation Process (2/6)

- Nuclias Connect Installation Process (Step by Step guide)

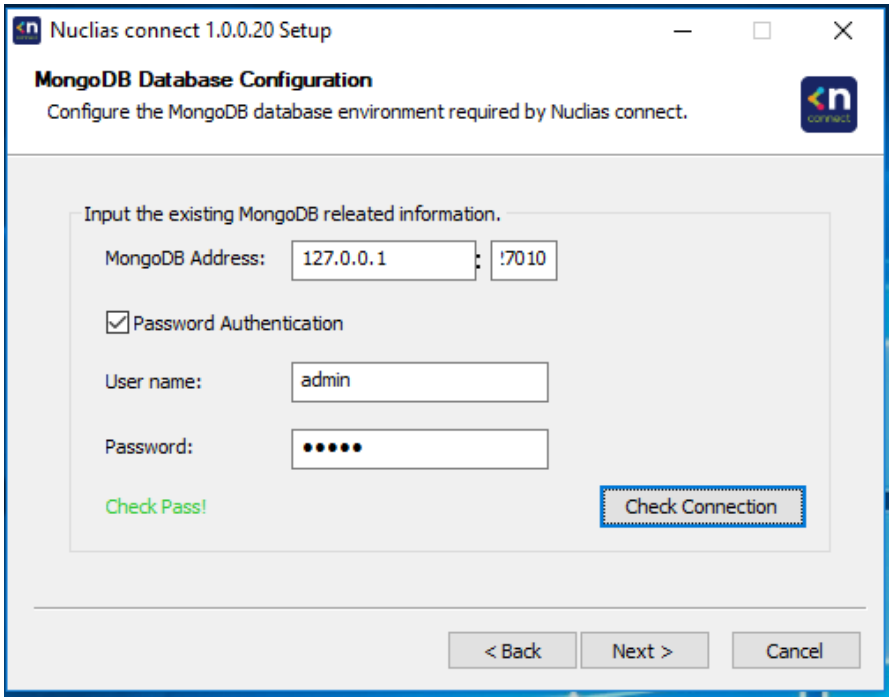


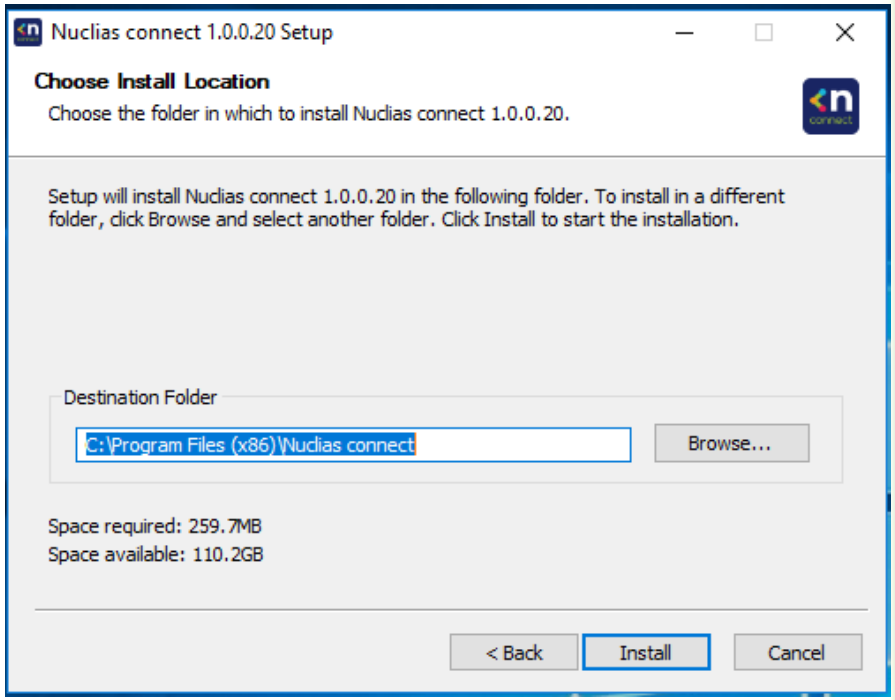


If connecting to pre-installed MongoDB, http://127.0.0.1:27017

Nuclias Connect Installation Process (3/6)

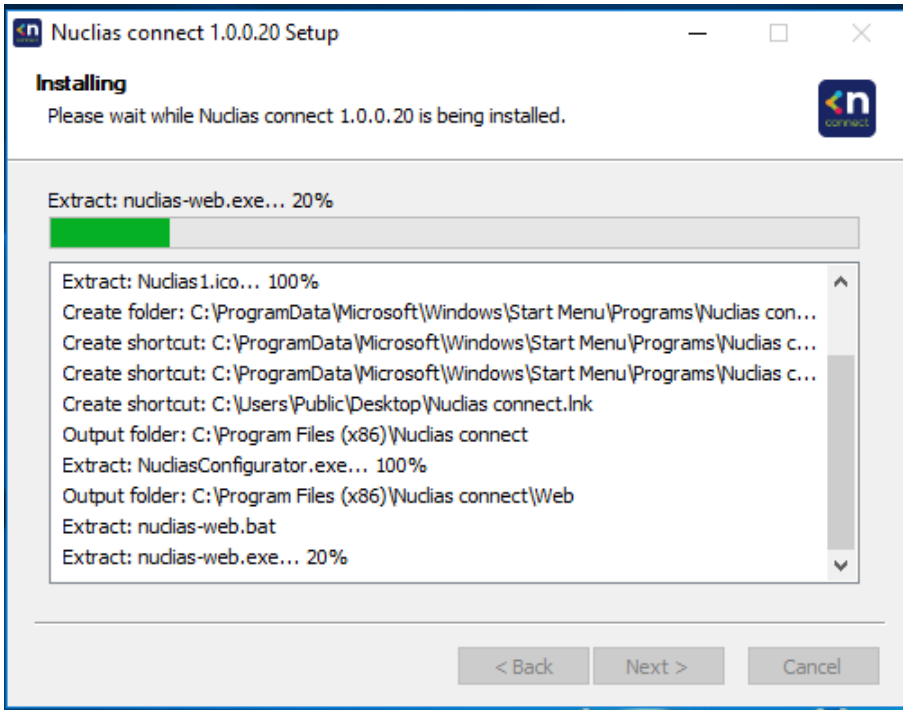
- Nuclias Connect Installation Process (Step by Step guide)

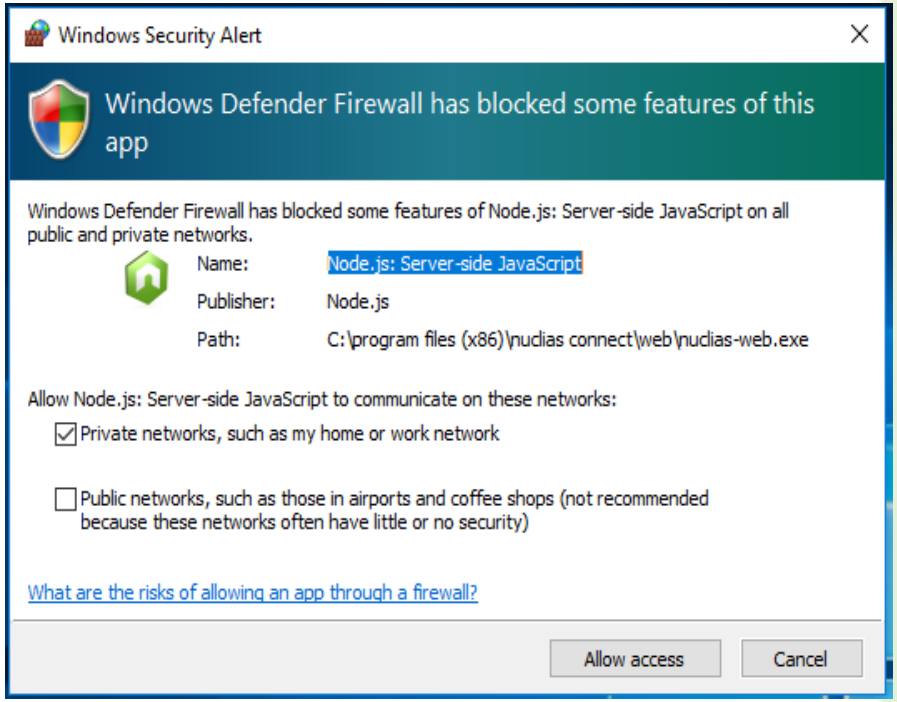




Nuclias Connect Installation Process (4/6)

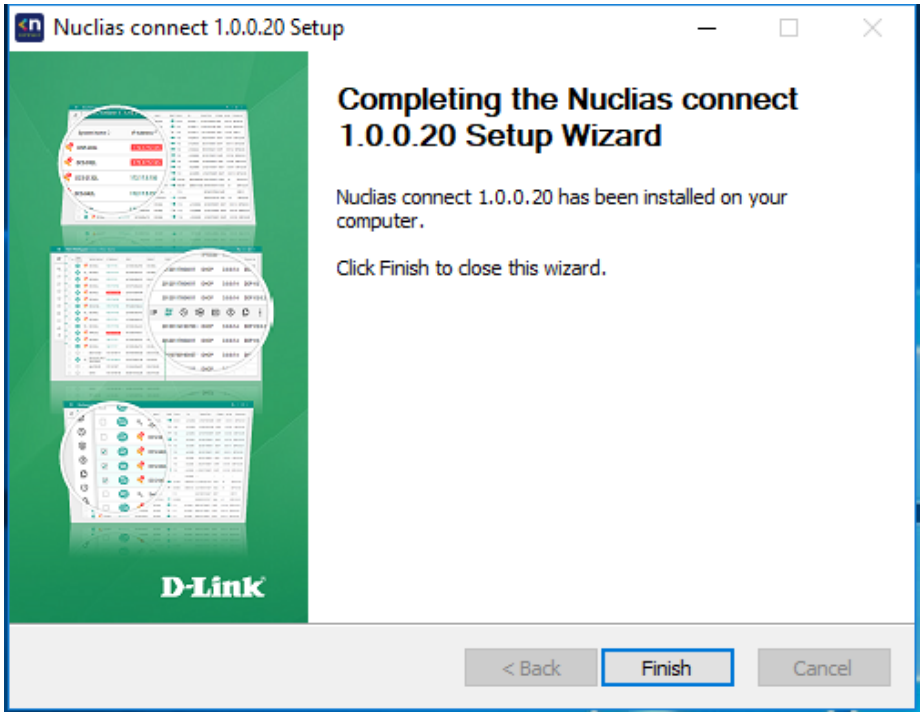
- Nuclias Connect Installation Process (Step by Step guide)





Nuclias Connect Installation Process (5/6)

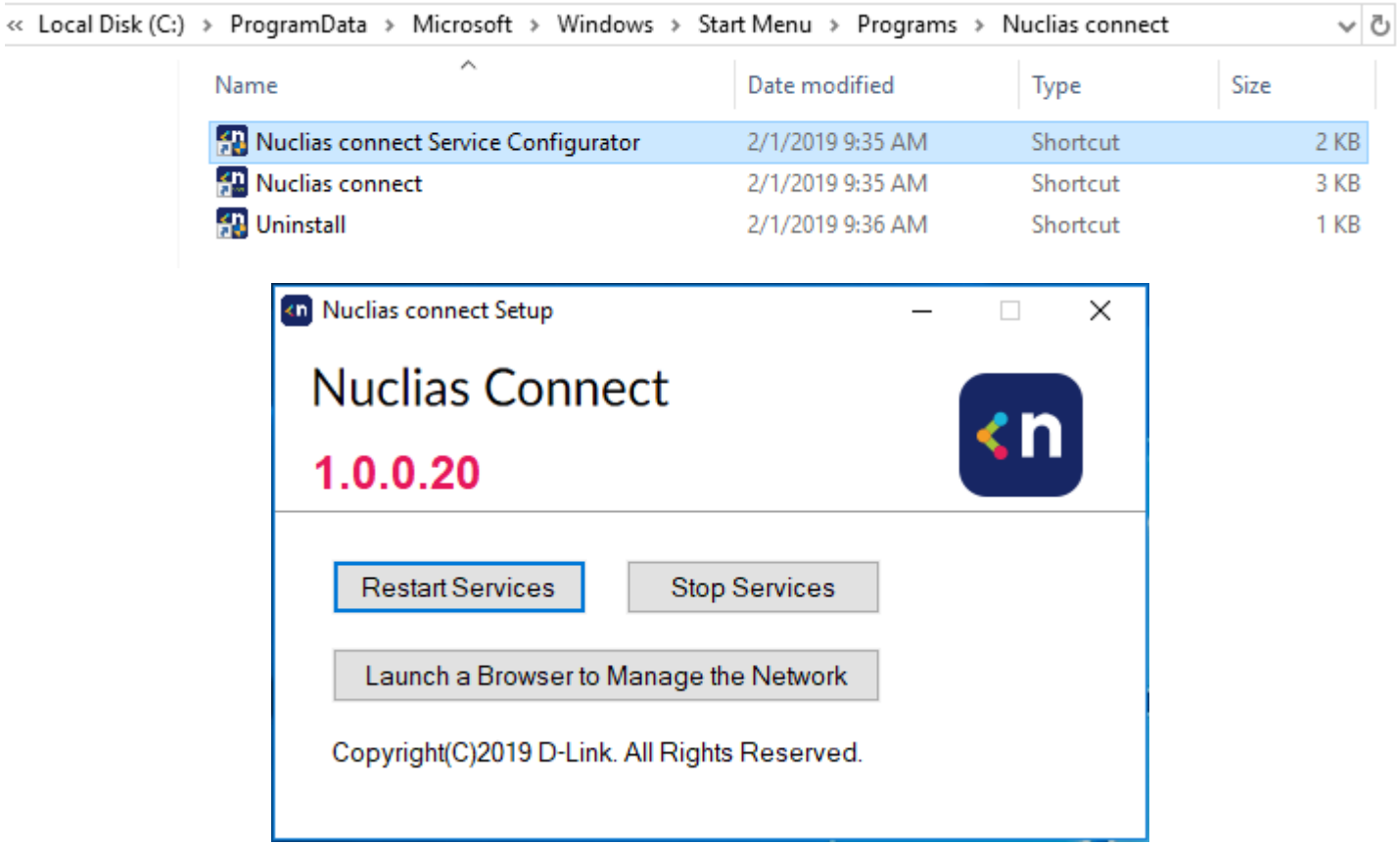
- Nuclias Connect Installation Process (Step by Step guide)



Reboot the server, before launching this application

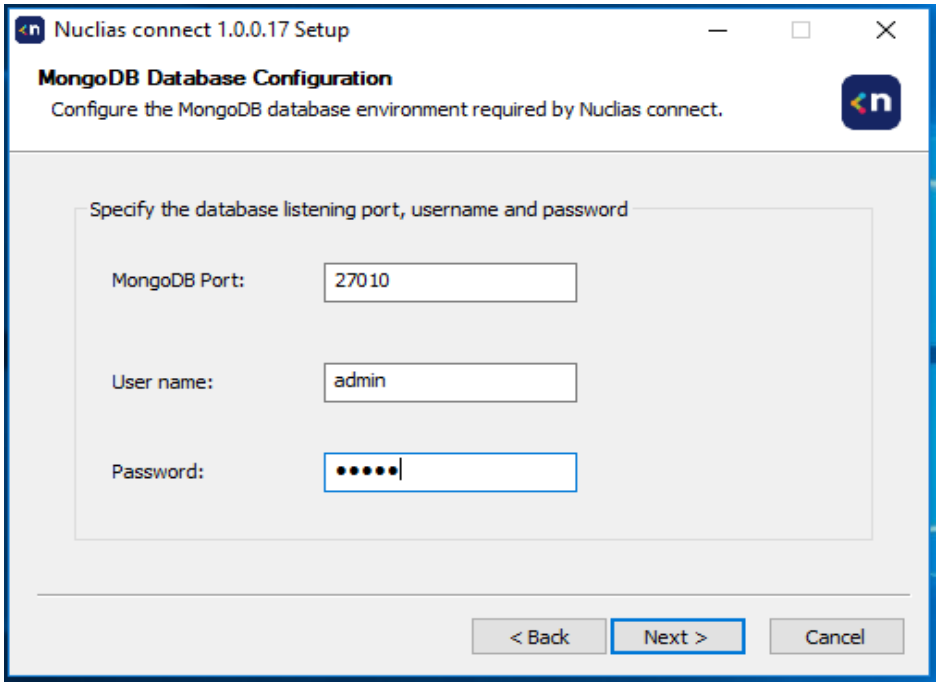
Nuclias Connect Installation Process (6/6)

- Nuclias Connect Installation Process (Step by Step guide)



Nuclias Connect (MongoDB) Installation

- Should you install MongoDB in the first time, you might be approached with the following information

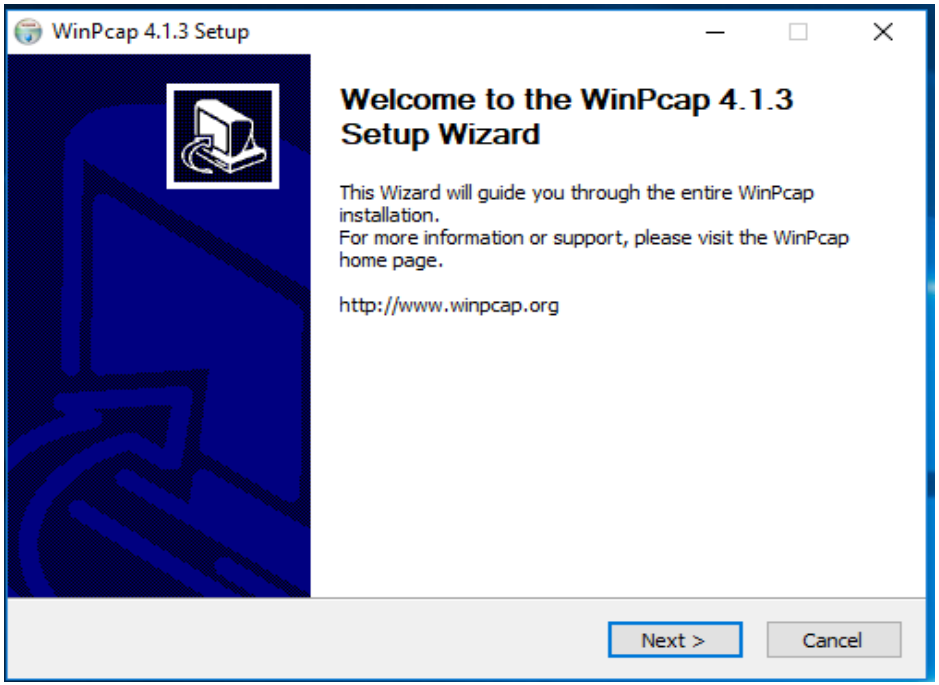


What is the default port being recommended?

User Name/PWD: admin/admin

Nuclias Connect (WinPcap) Installation (1/2)

- The following screen shots show WinPcap 4.1.3 installation process

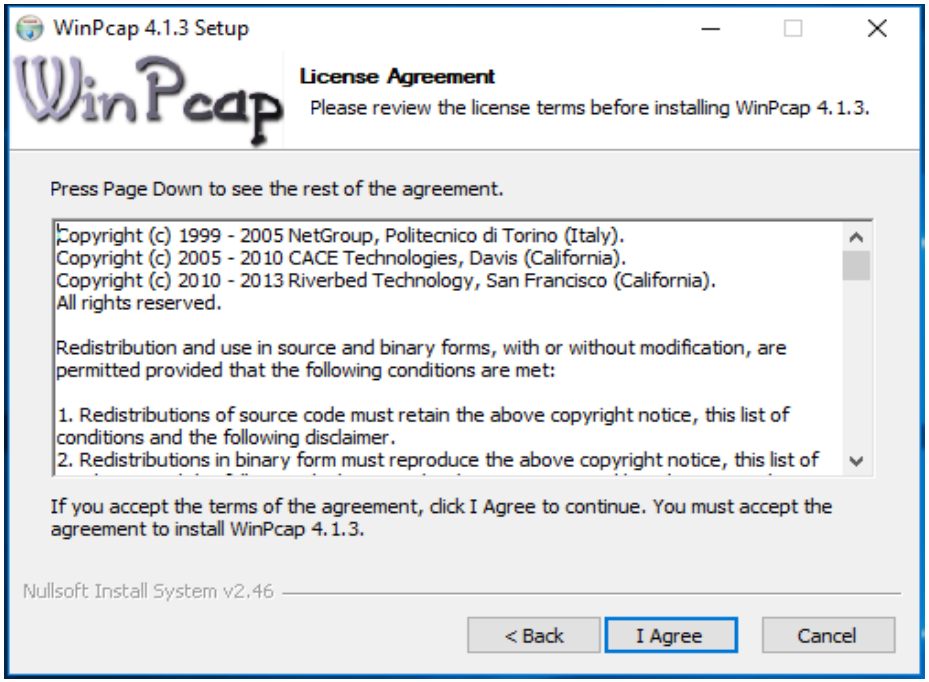


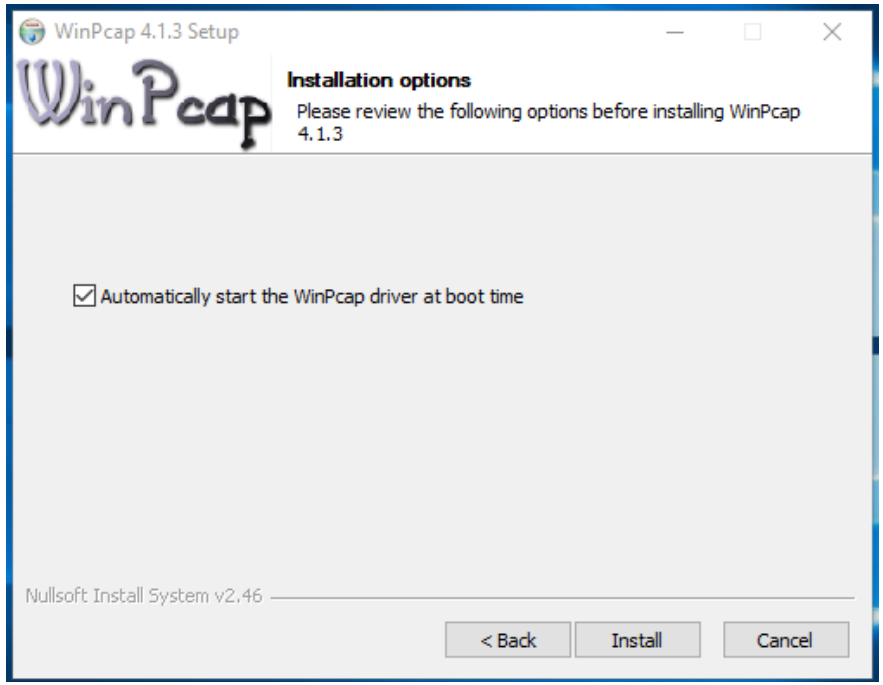
What is the default port being recommended?

User Name/PWD: admin/admin

Nuclias Connect (WinPcap) Installation (2/2)

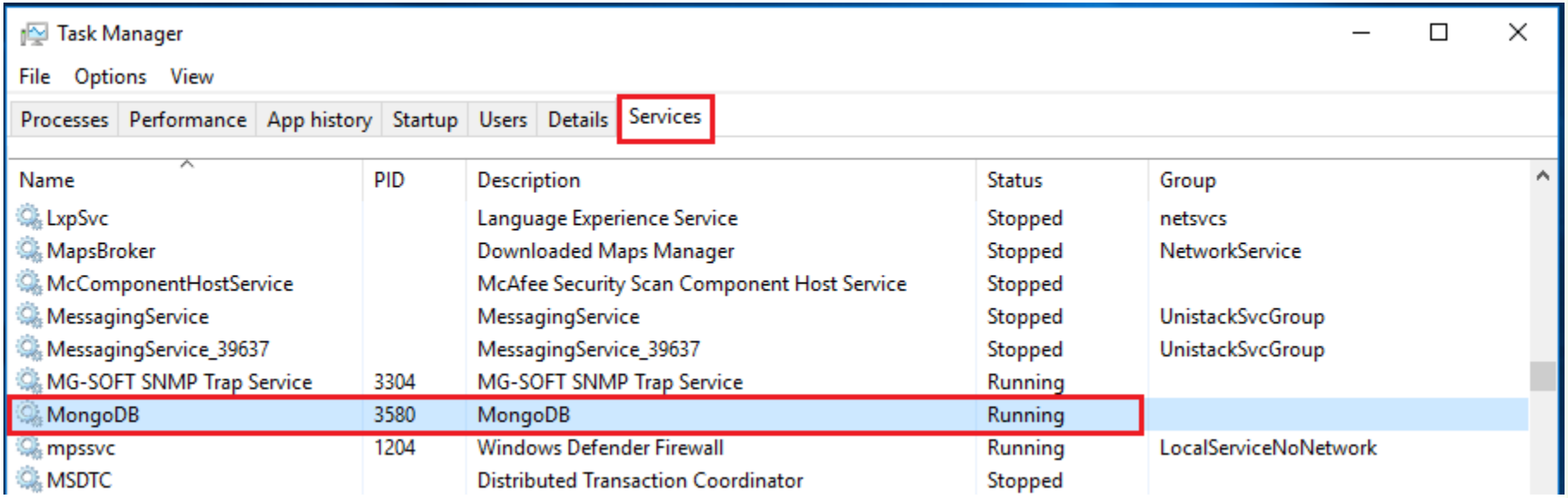
- You may also install WinPcap within Nuclias Connect installation





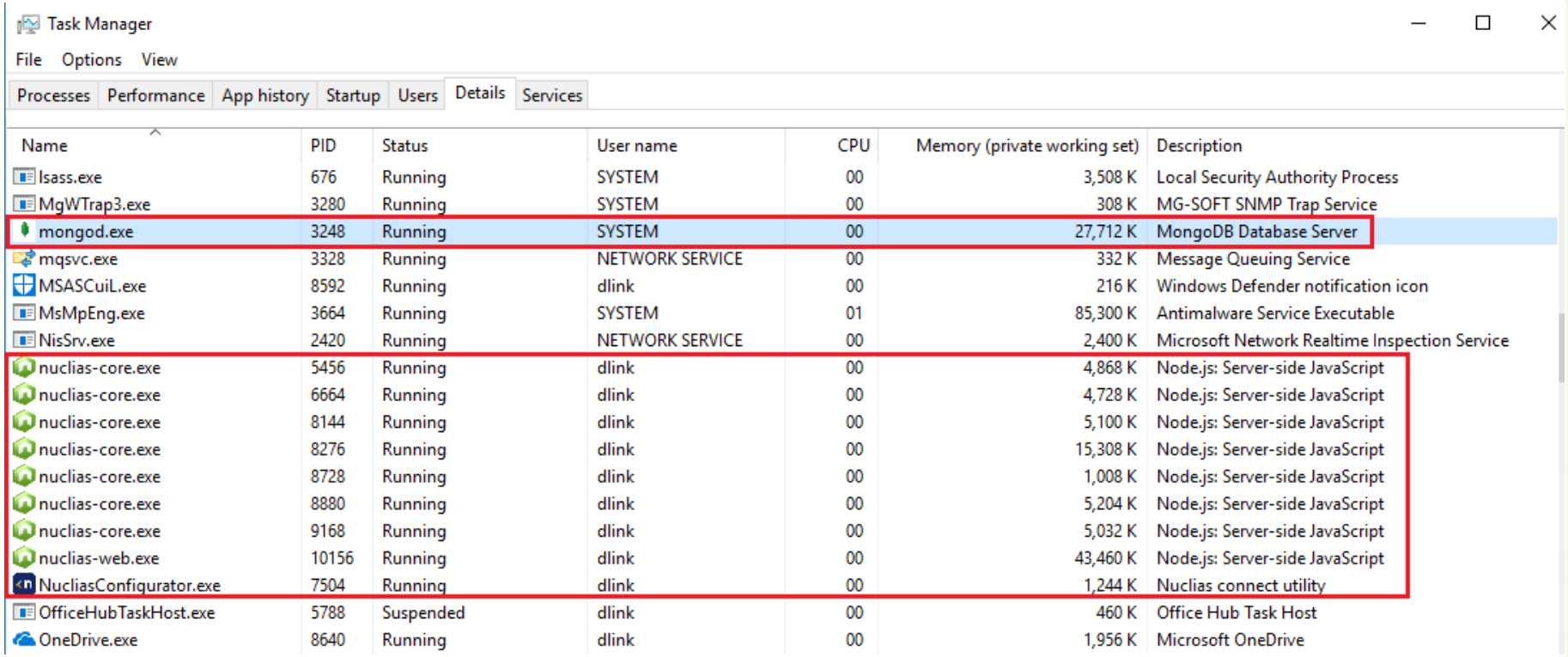
Windows Task Management (Nuclias Connect)

- In Services tab, Mongo DB uses PID (process ID) 3580 in our lab facility and it is in "Running" status. [v.1.0.0.18]



Windows Task Management (Nuclias Connect)

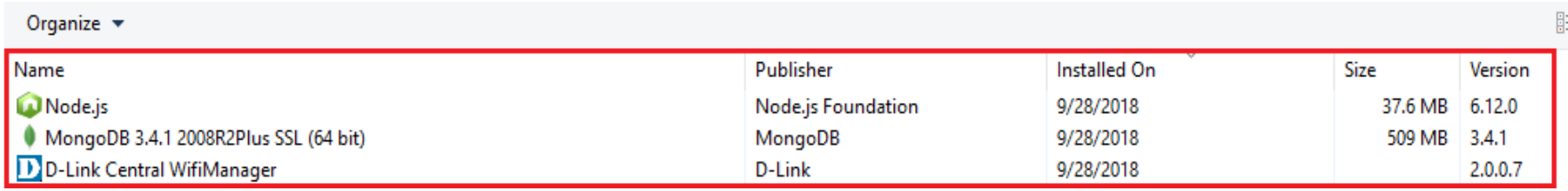
- In Details tab, both "NucliasConfigurator.exe" and "MongoDB" should be in "Running" status. [v.1.0.0.18]

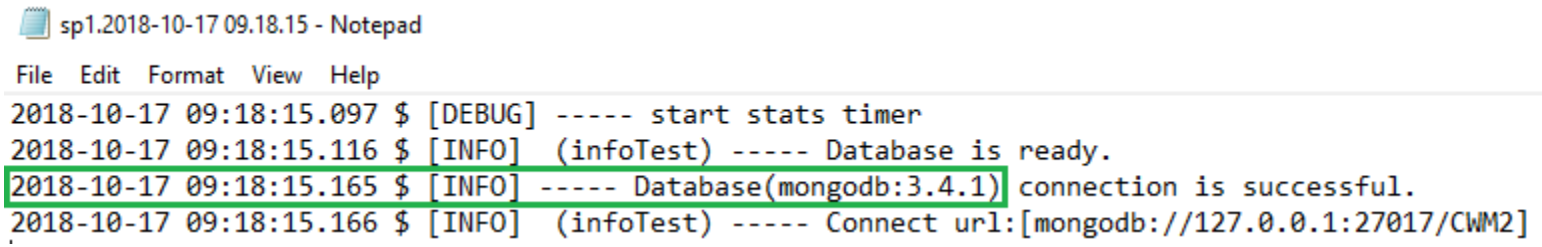


Name	PID	Status	User name	CPU	Memory (private working set)	Description
lsass.exe	676	Running	SYSTEM	00	3,508 K	Local Security Authority Process
MgWTrap3.exe	3280	Running	SYSTEM	00	308 K	MG-SOFT SNMP Trap Service
mongod.exe	3248	Running	SYSTEM	00	27,712 K	MongoDB Database Server
mqsvc.exe	3328	Running	NETWORK SERVICE	00	332 K	Message Queuing Service
MSASCuiL.exe	8592	Running	dlink	00	216 K	Windows Defender notification icon
MsMpEng.exe	3664	Running	SYSTEM	01	85,300 K	Antimalware Service Executable
NisSrv.exe	2420	Running	NETWORK SERVICE	00	2,400 K	Microsoft Network Realtime Inspection Service
nuclias-core.exe	5456	Running	dlink	00	4,868 K	Node.js: Server-side JavaScript
nuclias-core.exe	6664	Running	dlink	00	4,728 K	Node.js: Server-side JavaScript
nuclias-core.exe	8144	Running	dlink	00	5,100 K	Node.js: Server-side JavaScript
nuclias-core.exe	8276	Running	dlink	00	15,308 K	Node.js: Server-side JavaScript
nuclias-core.exe	8728	Running	dlink	00	1,008 K	Node.js: Server-side JavaScript
nuclias-core.exe	8880	Running	dlink	00	5,204 K	Node.js: Server-side JavaScript
nuclias-core.exe	9168	Running	dlink	00	5,032 K	Node.js: Server-side JavaScript
nuclias-web.exe	10156	Running	dlink	00	43,460 K	Node.js: Server-side JavaScript
NucliasConfigurator.exe	7504	Running	dlink	00	1,244 K	Nuclias connect utility
OfficeHubTaskHost.exe	5788	Suspended	dlink	00	460 K	Office Hub Task Host
OneDrive.exe	8640	Running	dlink	00	1,956 K	Microsoft OneDrive

Verification Of Nuclias Connect Installation

- Nuclias Connect server installation verification
  - System Requirements
  - Application Requirements
    - Node.js, v6.12.0 (38 MB)
    - Windows Firewall
    - MongoDB 3.4.1 (2008R2Plus, SSL, 64-bit) v3.4.1 (509 MB)





Installing Nuclias Connect on Linux

- 1. Prepare the OS environment with a recent Linux distribution, such as centos7 or ubuntu
- 2. Install the docker with command "curl -sSL https://get.daocloud.io/docker | sh" or use the Built-in command "yum", "apt-get", then check the version with command "docker -v"
- 3. Install the docker-compose with python-pip and then check the version with command "docker-compose -v"
- 4. Copy the Nuclias Connect installation package to the server, and then Unzip
- 5. Enter the "/cwm-app" directory, exec the script "init.sh"
- 6. Open a browser, and then access "https://localhost:30001"

Installing Docker and Docker-compose on Centos 7 (1/3)

Docker and Docker-compose Installation

- yum update –y
- /etc/sysconfig/selinux [SELINUX=disabled]
- [root@localhost /]# systemctl disable firewalld.service
- Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
- Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
- [root@localhost /]# systemctl stop firewalld.service
- [root@localhost /]# yum install docker
- [root@localhost /]# systemctl enable docker.service
- Created symlink from /etc/systemd/system/multi-user.target.wants/docker.service to /usr/lib/systemd/system/docker.service

Installing Docker and Docker-compose on Centos 7 (2/3)

Docker and Docker-compose Installation

- [root@localhost /]# systemctl start docker.service
- [root@localhost /]# systemctl status docker.service

- $ sudo systemctl restart docker.service ## <-- Restart docker ##
- $ sudo systemctl status docker.service ## <-- Get status of docker ##
- [root@localhost chuck]# yum install epel-release
- [root@localhost chuck]# yum install -y python-pip
- [root@localhost chuck]# pip install docker-compose

Installing Docker and Docker-compose on Centos 7 (3/3)

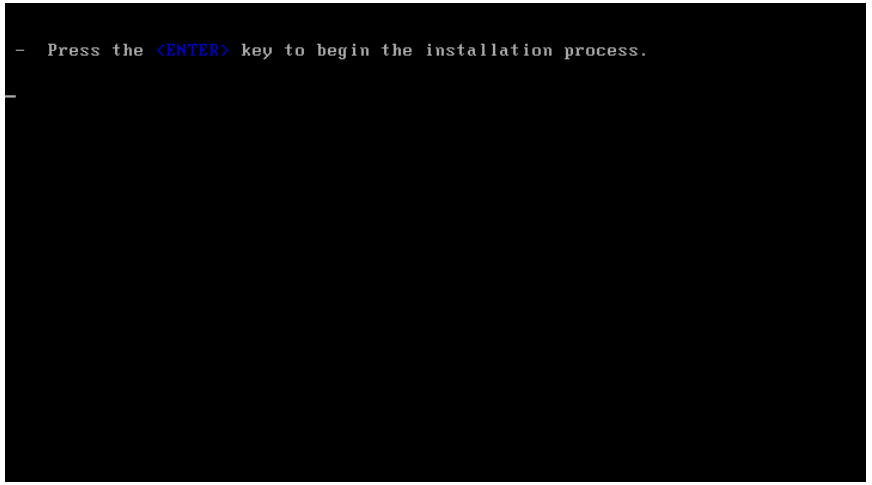
Docker and Docker-compose Installation

- [root@localhost chuck]# yum upgrade python*
- To show your group of Docker containers (both stopped and currently running), use the following command:
- docker-compose ps
- https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-compose-on-centos-7

Installing Nuclias Connect on Centos 7 (1/7)

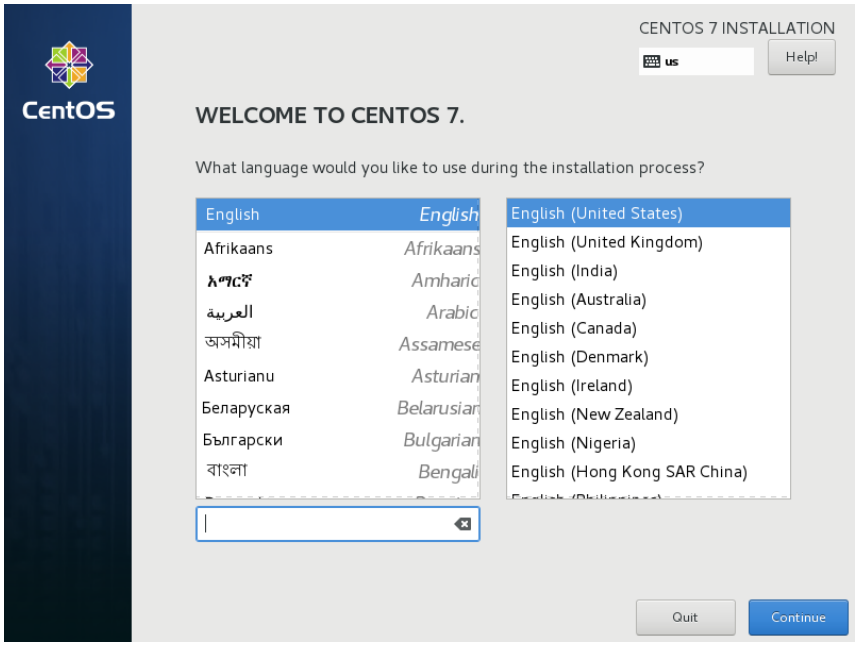
- Installing Nuclias Connect on Centos 7

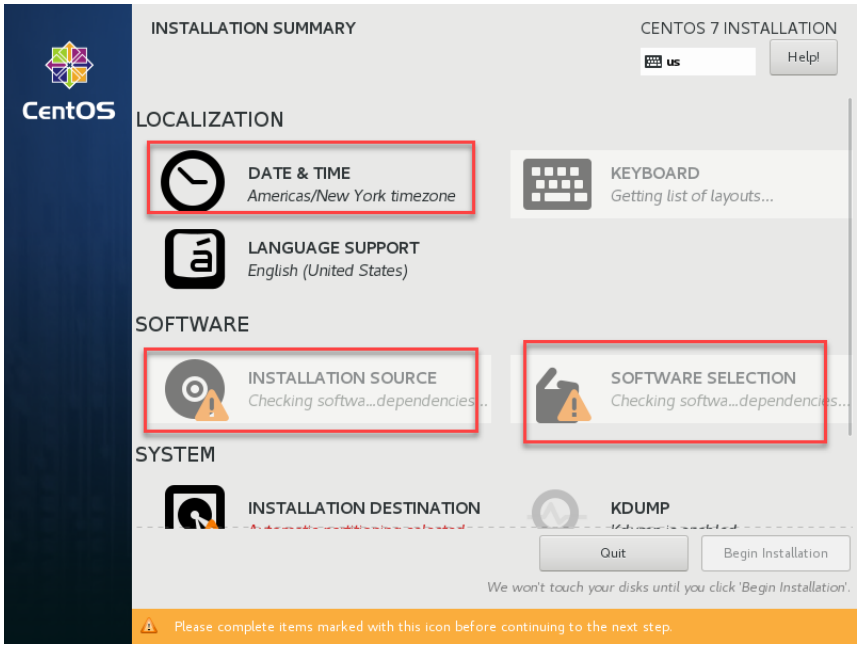




Installing Nuclias Connect on Centos 7 (2/7)

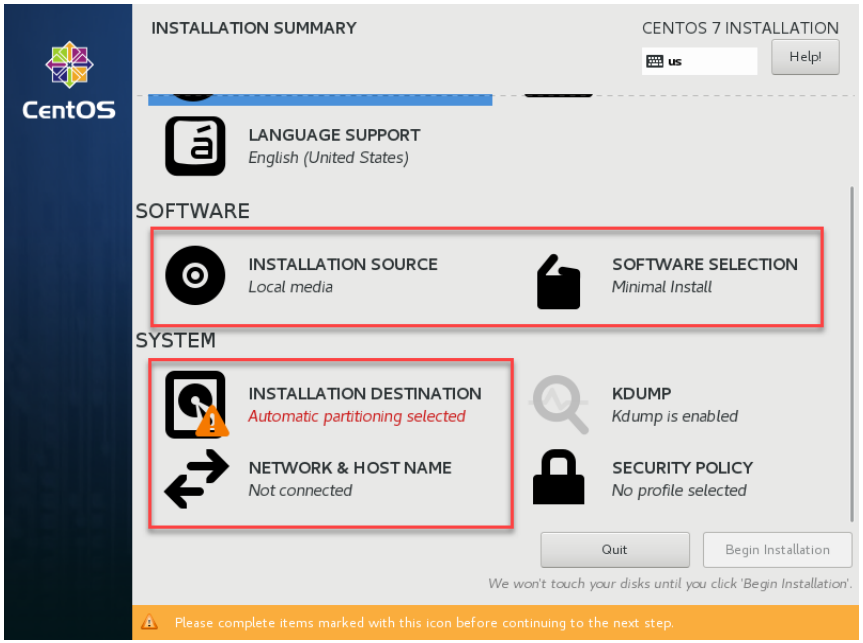
- Installing Nuclias Connect on Centos 7

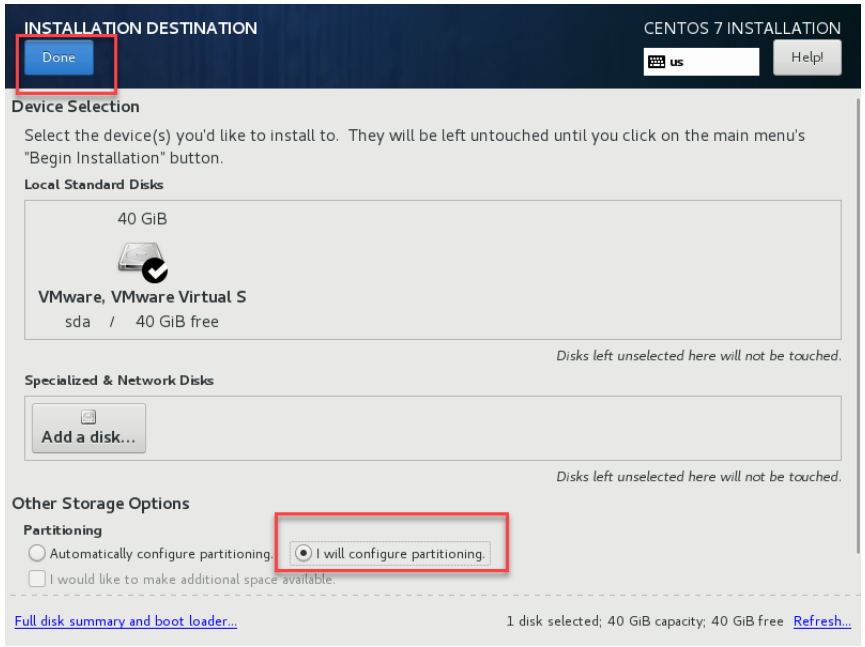




Installing Nuclias Connect on Centos 7 (3/7)

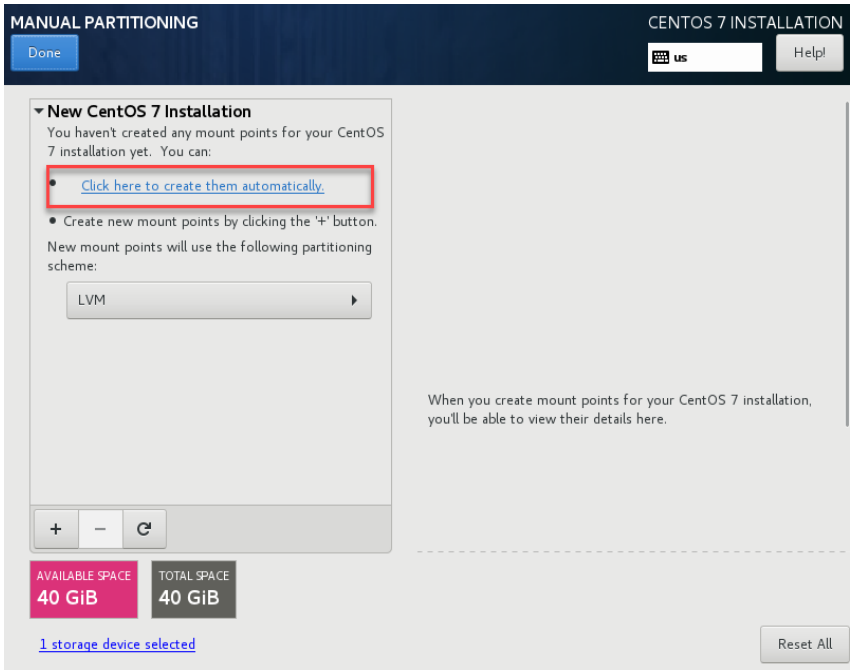
- Installing Nuclias Connect on Centos 7

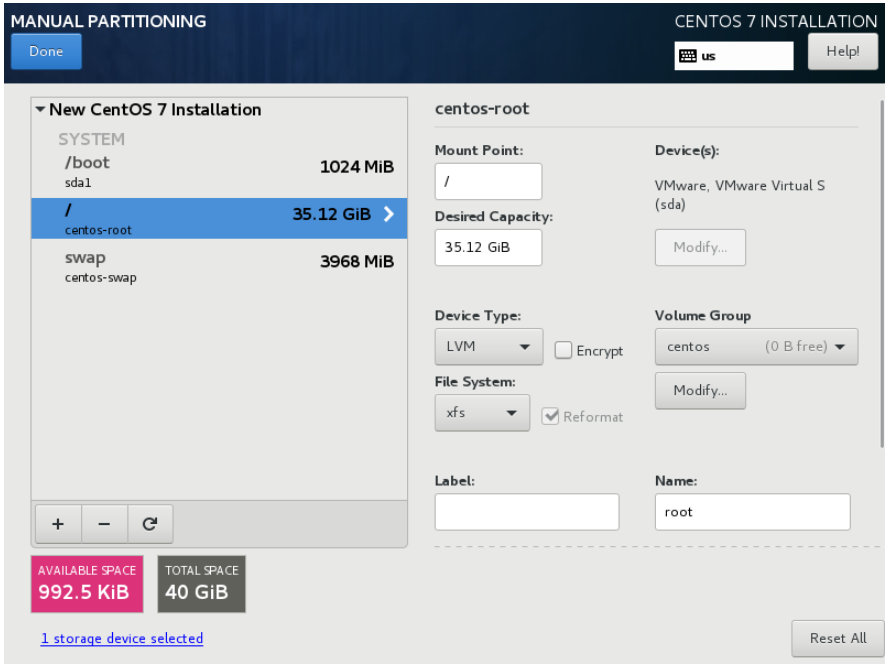




Installing Nuclias Connect on Centos 7 (4/7)

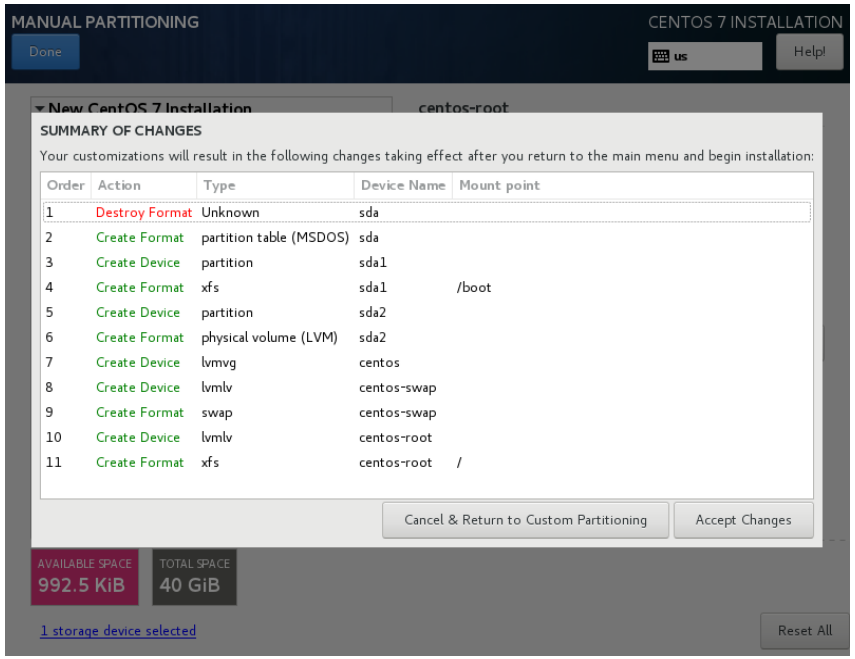
- Installing Nuclias Connect on Centos 7

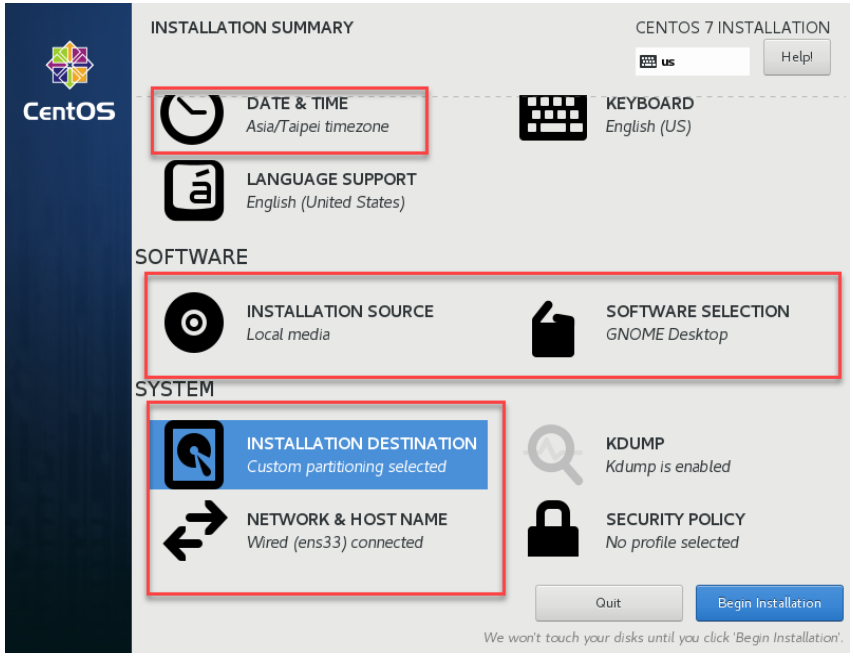




Installing Nuclias Connect on Centos 7 (5/7)

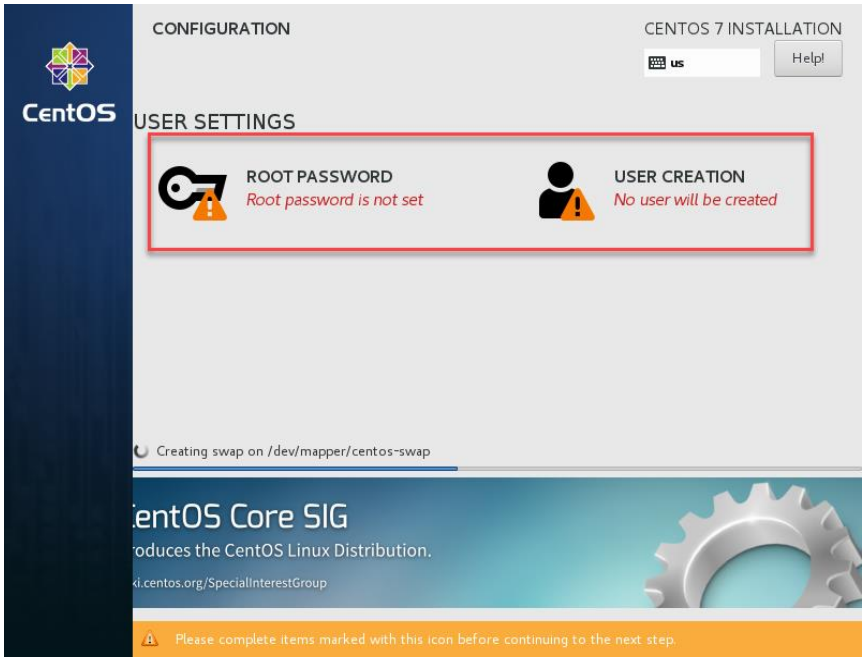
- Installing Nuclias Connect on Centos 7

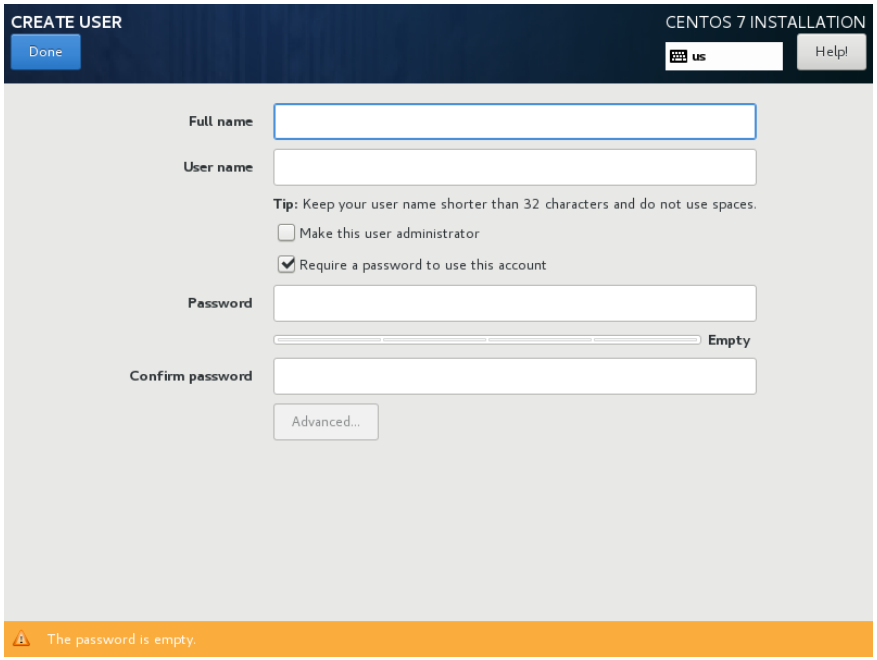




Installing Nuclias Connect on Centos 7 (6/7)

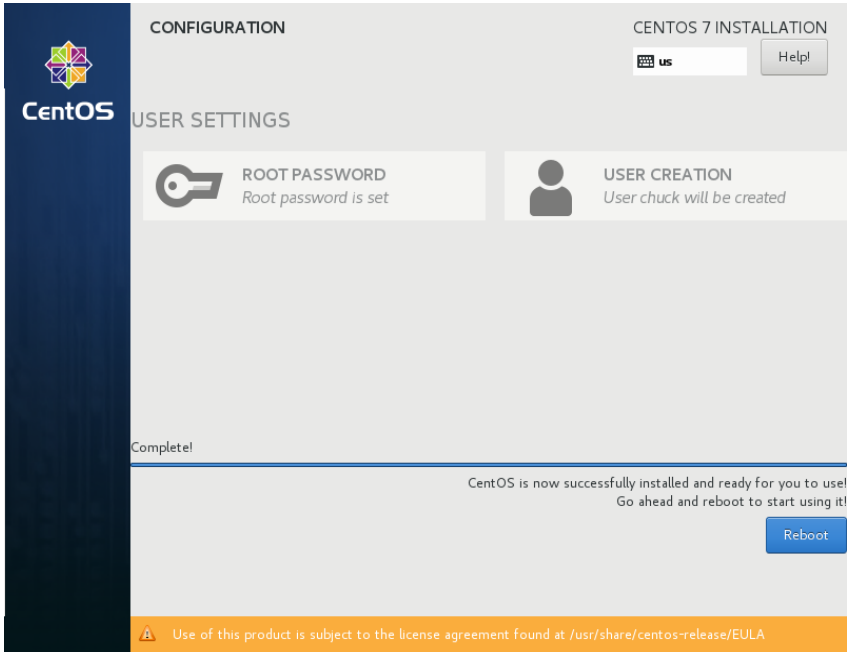
- Installing Nuclias Connect on Centos 7

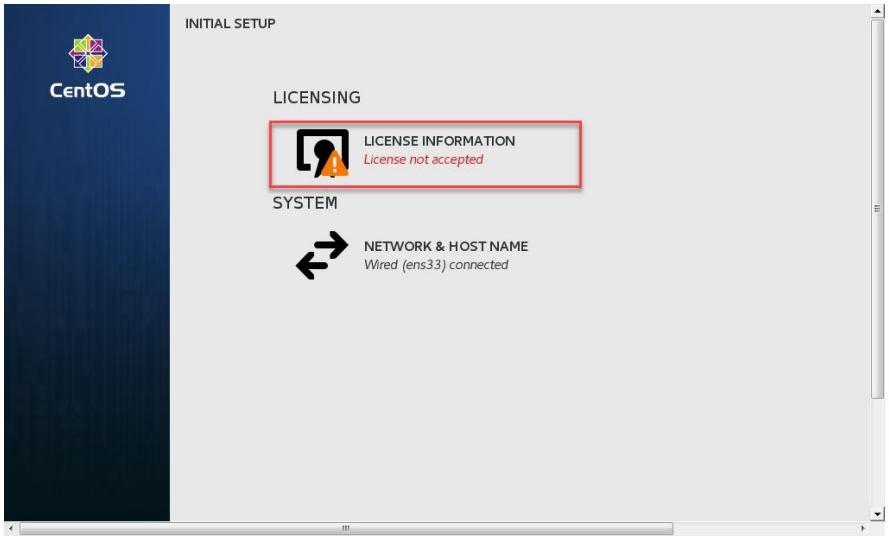




Installing Nuclias Connect on Centos 7 (7/7)

- Installing Nuclias Connect on Centos 7



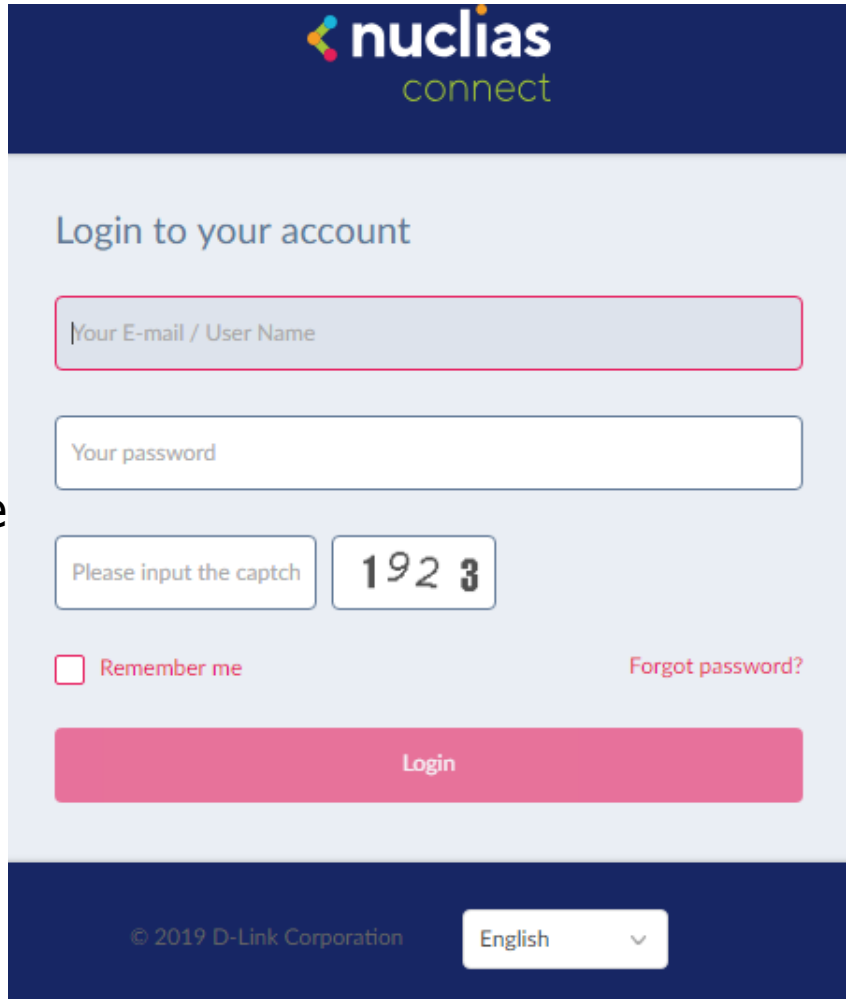


Installing Nuclias Connect on OS X (10.10.3 and above)

- 1. Prepare the OS environment with a recent OS X distribution, at least 10.10.3
- 2. Install the docker by accessing "https://get.daocloud.io/docker-install/mac", then check the version with command "docker -v", "docker-compose -v"(Docker for mac integrated with docker-compose)
- 3. Copy the Nuclias Connect installation package to the server, and then Unzip
- 4. Enter the "/cwm-app" directory, exec the script "init.sh"
- 5. Open a browser, and then access "https://localhost:30001"

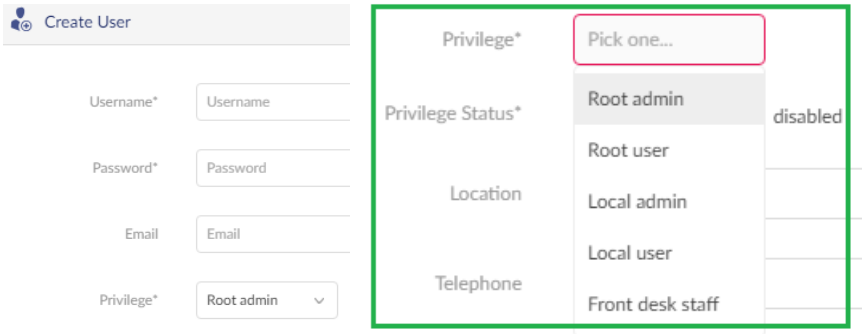
Nuclias Connect Product Bulletin

- Individuals are welcome to download both CWM 1.03/ Nuclias Connect 1.x for free.
- Within our training environment, a valid action code is required to launch this application.
- It is expected that a different workflow will be triggered in the official release.



Nuclias Connect Product Bulletin (User Management)

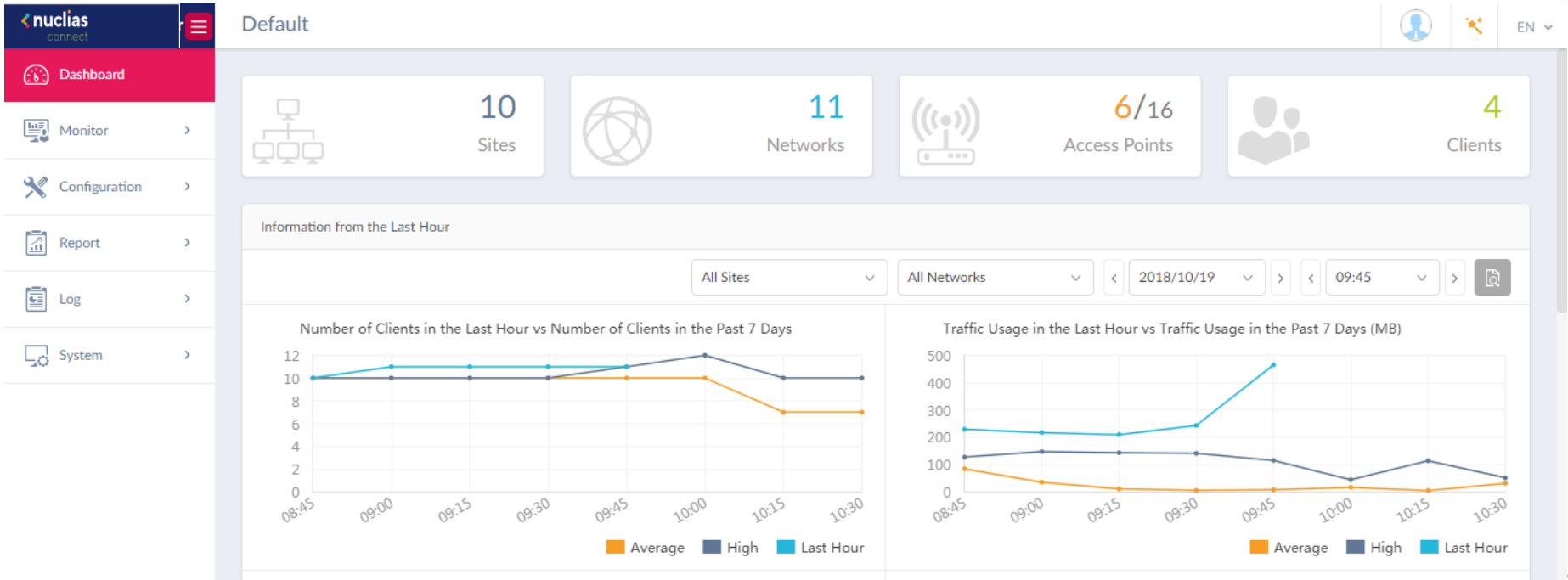
- In Nuclias Connect, user account privileges are listed (DK1500249)
  - Root Admin, is able to view all the settings of groups, system configuration, monitoring, systemlog etc.
  - Root User, can view settings and latest status as "Root Admin" but not able to make configuration changes
  - Local Admin, is given the authority to manage the group specified by "Root Admin"
  - Local User, is assigned the power to view all the info of group specified by "Root Admin" cannot manage
  - Front Desk Staff, is responsible for the passcode management is assigned Sites



Nuclias Connect Product Bulletin (Main Console)

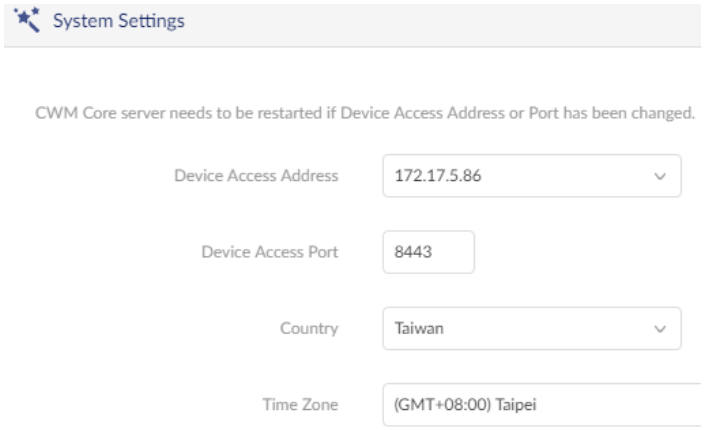
Nuclias Connect Main Console

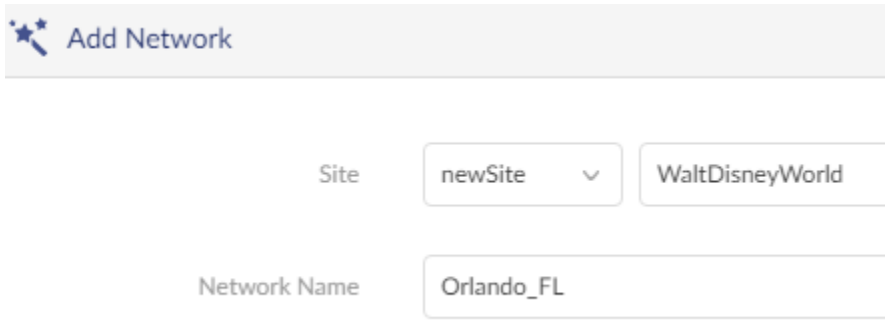
- Tab: Dashboard, Monitor, Configuration, Report, Log, and System
- Wireless Network Overview
- Monitoring The Wireless Network



Nuclias Connect Product Bulletin

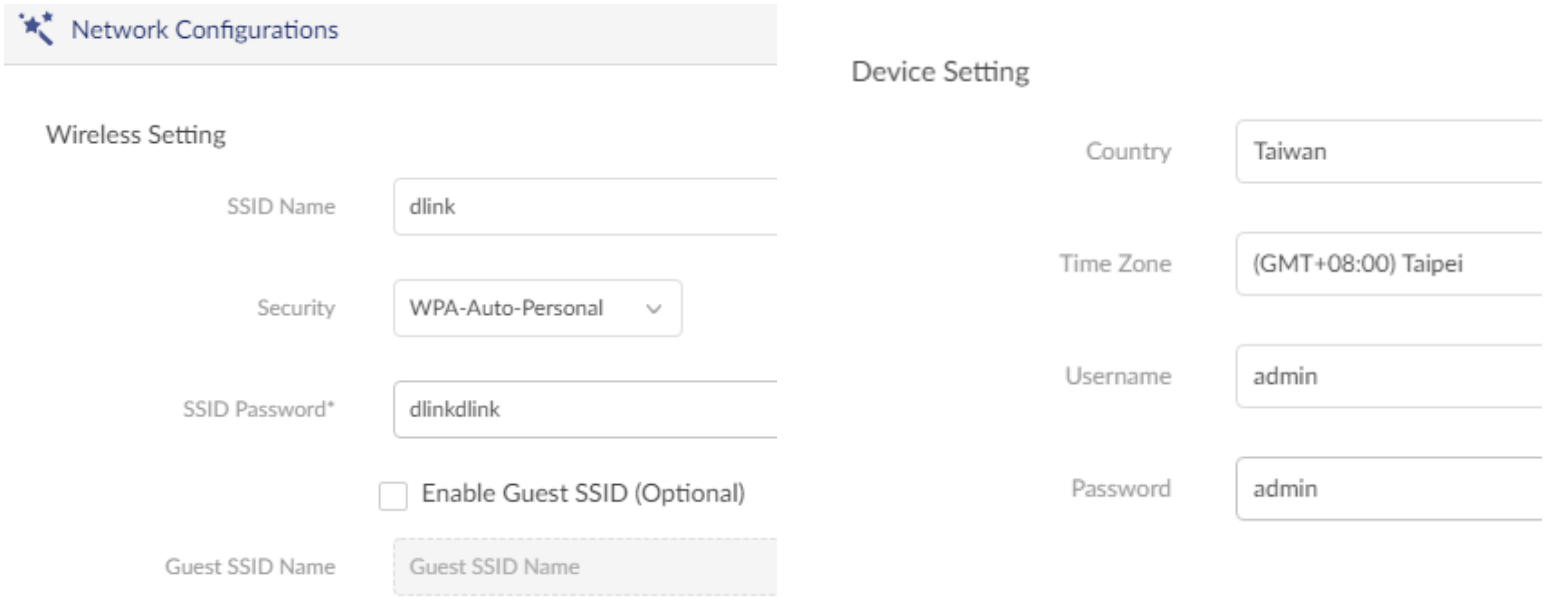
- From The legacy CWM to Nuclias Connect
- In CWM 1.03, lack of "Setup Wizard" made it very difficult and user unfriendly.
- In Nuclias Connect, Setup Wizard creates smooth configuration(1/3)





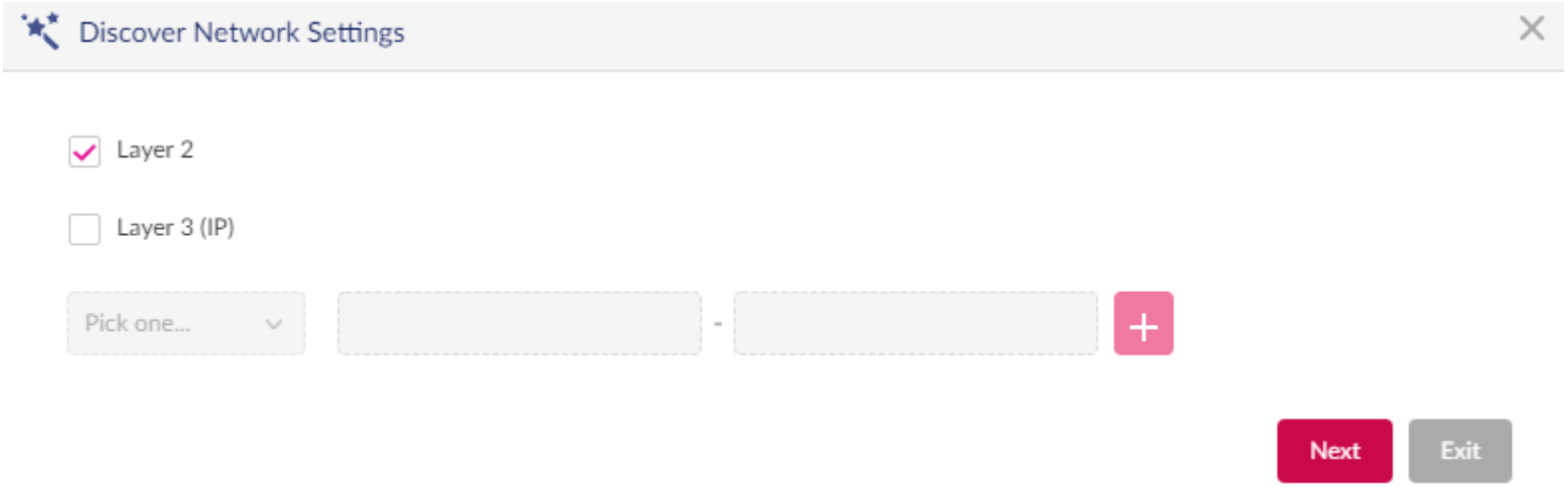
Nuclias Connect Product Bulletin

- From The legacy CWM to Nuclias Connect
- In CWM 1.03, lack of "Setup Wizard" made it very difficult and user unfriendly.
- In Nuclias Connect, Setup Wizard creates smooth configuration(2/3)



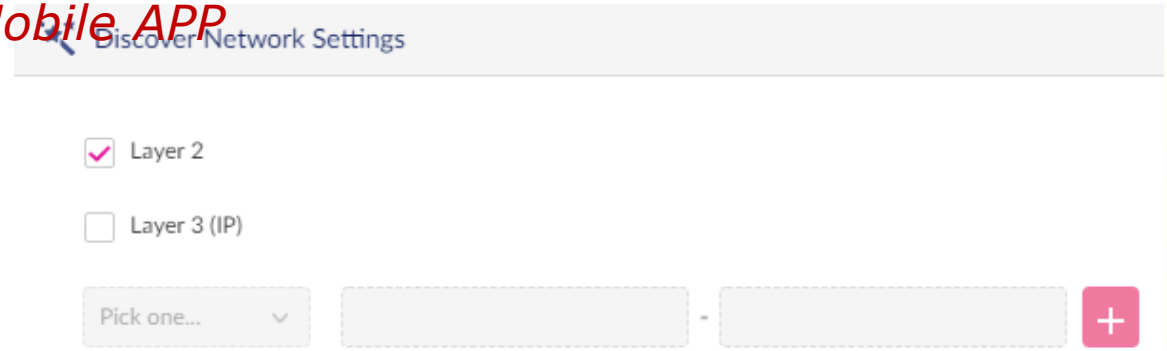
Nuclias Connect Product Bulletin

- From The legacy CWM to Nuclias Connect
- In CWM 1.03, lack of "Setup Wizard" made it very difficult and user unfriendly.
- In Nuclias Connect, Setup Wizard creates smooth configuration(3/3)



Nuclias Connect Product Bulletin

- From The legacy CWM to Nuclias Connect
- In CWM 1.03, the "Access Point Installation Tool" utility is recommended (a) to identify network newly-joined access points, (b) to modify IP address and, (c) to upload Nuclias Connect-related network data file.
- By removing specific task dependencies, Nuclias Connect has improved dramatically with offering both Layer 2 and Layer 3 network discovery, available in Setup Wizard and Profile Configurations.
  - Pushing Profile Config *(a) Nuclias Connect Discover Network Settings, or (b) Mobile APP*

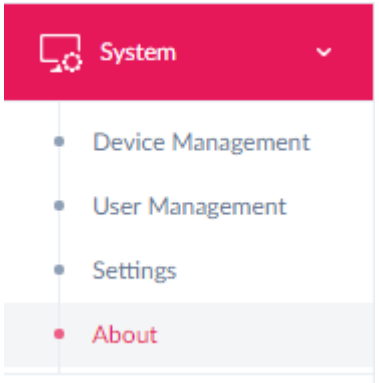


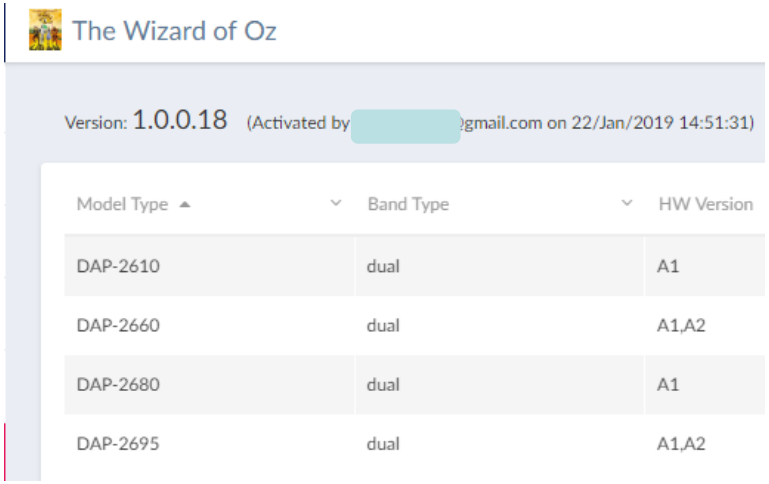
Nuclias Connect Product Bulletin

- From The legacy CWM to Nuclias Connect: Mobile Application
- In CWM 1.03, Mobile Application was not available.
- In Nuclias Connect, [used for training purposes only]
  - Android App (Android version 1.0.4 release: https://www.dropbox.com/s/1uplax0hzkmr5k5/management_app.apk?dl=0
  - iOS App (iOS version 1.0.4 release: https://preview.mydlink.com/preview/ios/issbu/business.html

Nuclias Connect Product Bulletin

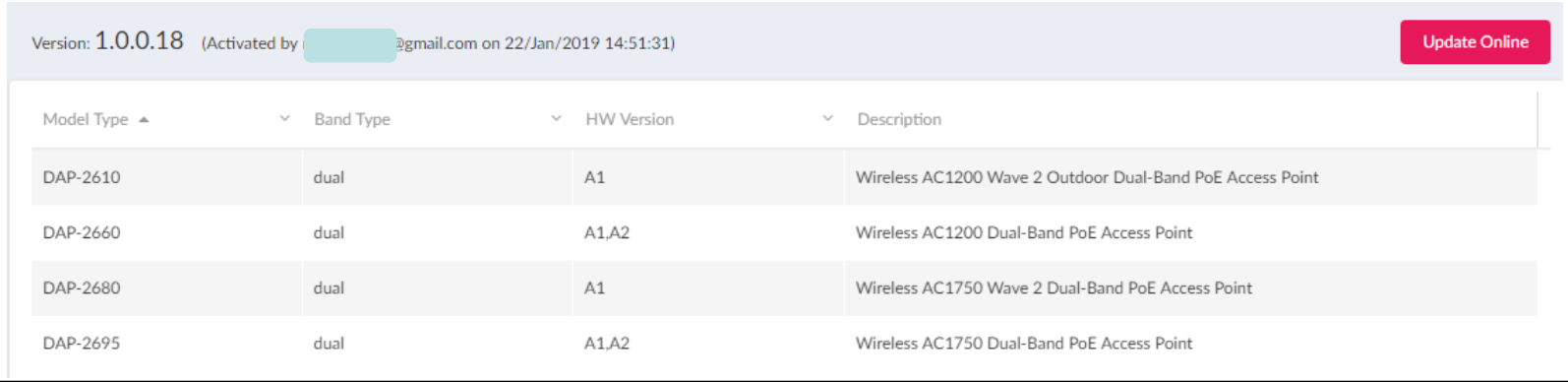
- From The legacy CWM to Nuclias Connect
- In CWM 1.03, "Access Point Module" of each DAP is utilized to seamless communication between the server and the access points.
  - Using the Simple Network Management Protocol (SNMP).
  - D-Track DK1500608 documents "AP Module" summary.
- In Nuclias Connect, "Access Point Module" is NO LONGER required.
  - A way to verify the DAPs being supported in your DNC can be seen from System > About





Nuclias Connect Product Bulletin

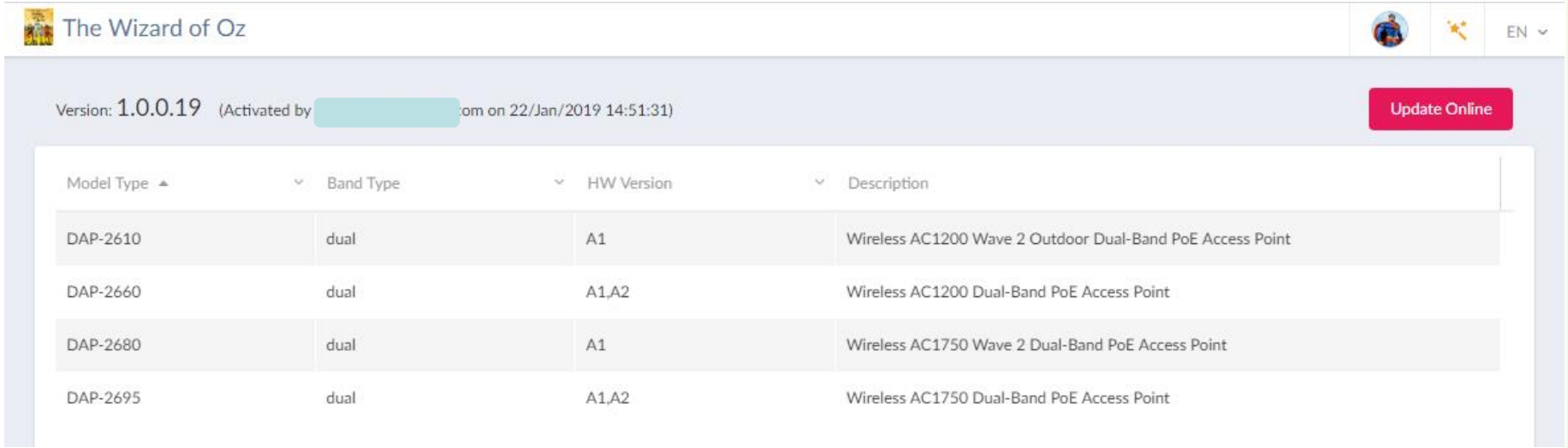
- From The legacy CWM to Nuclias Connect
- In Nuclias Connect, "Access Point Module" is NO LONGER required.
- An example of supported DAPs in Nuclias Connect can be seen in menu: System > About (as of Jan. 2019).
  - List of DAP models are subject to change without prior notice.
  - Supported device list update: (a) DNC core server start and (b) 1:00AM on daily basis
    - To eliminate the problems might be caused should any already supported DAP in which were not listed in our production environment

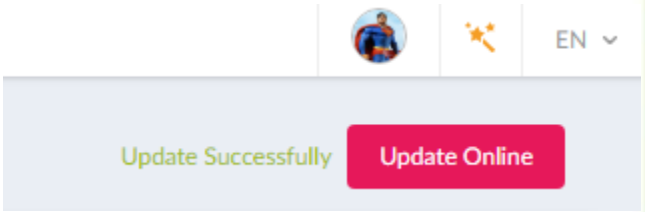


Model Type	Band Type	HW Version	Description
DAP-2610	dual	A1	Wireless AC1200 Wave 2 Outdoor Dual-Band PoE Access Point
DAP-2660	dual	A1,A2	Wireless AC1200 Dual-Band PoE Access Point
DAP-2680	dual	A1	Wireless AC1750 Wave 2 Dual-Band PoE Access Point
DAP-2695	dual	A1,A2	Wireless AC1750 Dual-Band PoE Access Point

Nuclias Connect Product Bulletin

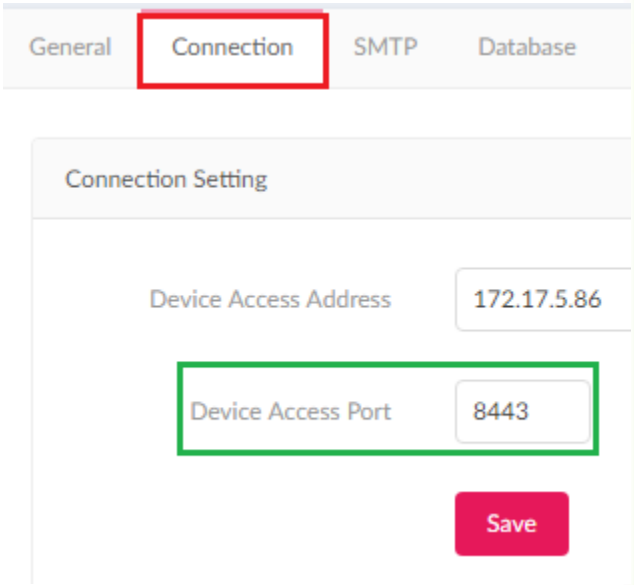
- From The legacy CWM to Nuclias Connect
- An example of supported DAPs in Nuclias Connect can be seen in menu: System > About (as of Jan. 2019).





Nuclias Connect Product Bulletin

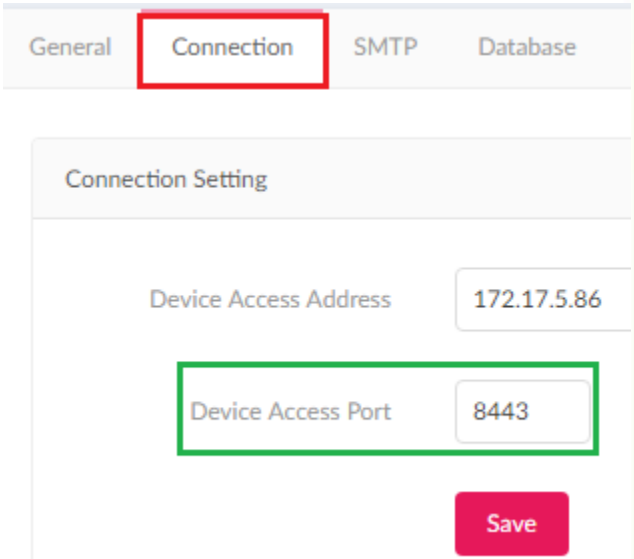
- From The legacy CWM to Nuclias Connect
- In CWM 1.03, the following tcp / udp ports SHALL be reserved for system access
  - UDP 161 (SNMP port), UDP 162 (SNMP trap port), UDP 514 (Syslog port), UDP 8090 (Listen port), as well as UDP 64768 (Service port).
  - TCP 443 (HTTPS, Management port), TCP 9000, Enable ftp-ALG (Manager port), TCP 10000-11000.
- In Nuclias Connect
  - TCP 8443 (Device Access Port), TCP 30001 (Web Access Port).
  - DDP is used to discover DAP.
  - Packet communication with https.



Nuclias Connect	
Connection Status	Connect
Server IP/PORT	172.17.5.86:8443
Group ID	5BC5-BD67BA6B-4F0FD43F-1A5F

Nuclias Connect Product Bulletin

- From The legacy CWM to Nuclias Connect
- In CWM 1.03, the following tcp / udp ports SHALL be reserved for system access
  - UDP 161 (SNMP port), UDP 162 (SNMP trap port), UDP 514 (Syslog port), UDP 8090 (Listen port), as well as UDP 64768 (Service port).
  - TCP 443 (HTTPS, Management port), TCP 9000, Enable ftp-ALG (Manager port), TCP 10000-11000.
- In Nuclias Connect
  - TCP 8443 (Device Access Port), TCP 30001 (Web Access Port).
  - DDP is used to discover DAP.
  - Packet communication with https.



For DAP outbound, TCP 8443 & DNS

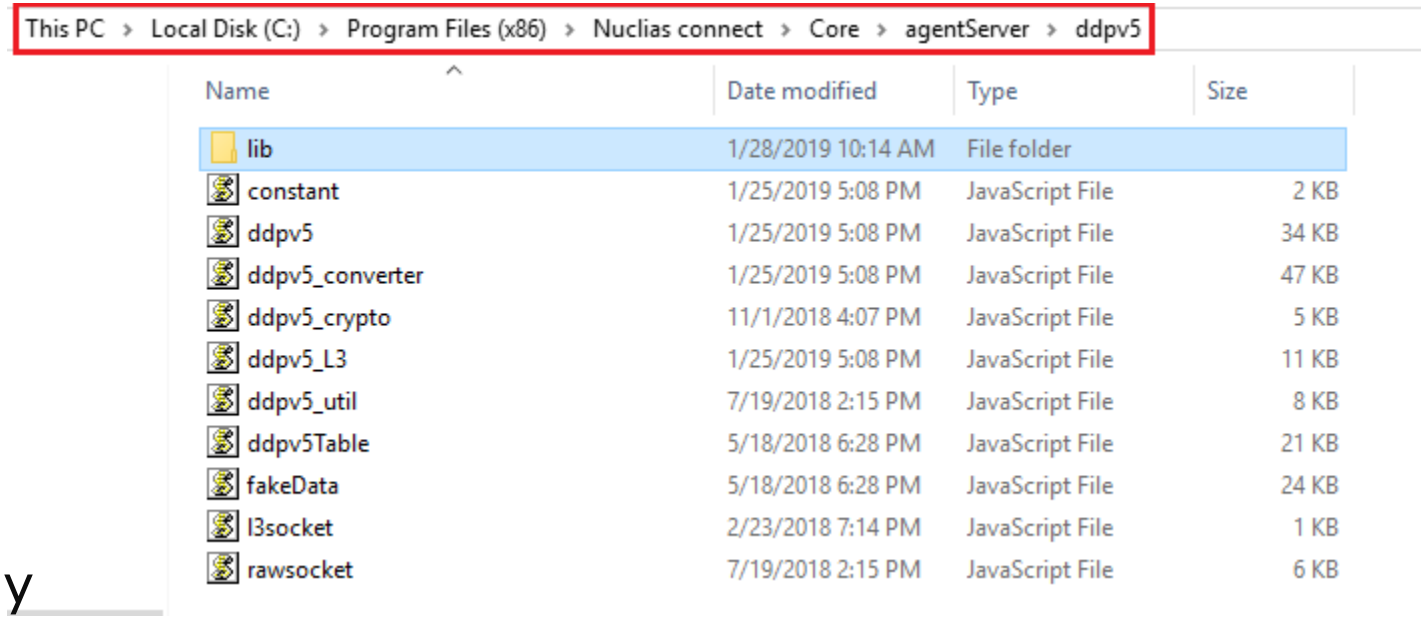
Nuclias Connect	
Connection Status	Connect
Server IP/PORT	172.17.5.86:8443
Group ID	5BC5-BD67BA6B-4F0FD43F-1A5F

Nuclias Connect Product Bulletin

- Protocols in discovering AP
  - DDPv5 (path: C:> Program Files (x86) > Nuclias Connect > Core > agentServer > ddpv5

DDP Version 5

- DDP is a client-server protocol for discovering and configuring network devices, i.e. Ethernet switch, AP, in the LAN.
- The below image sketch presents the folder in a closer way.

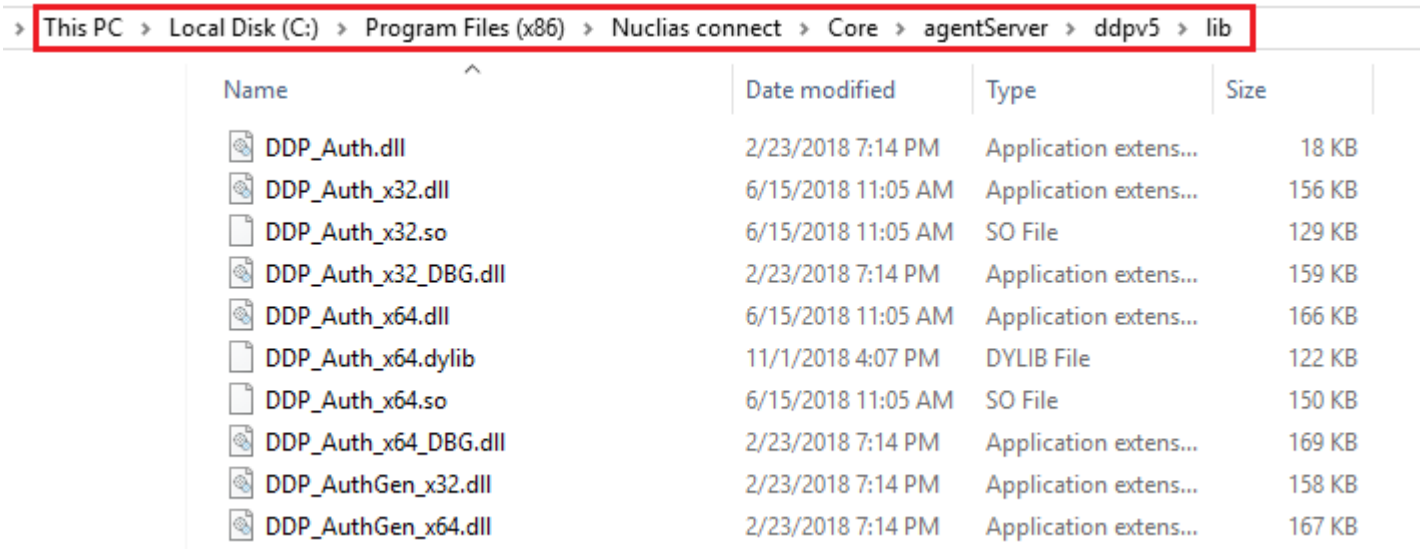


Nuclias Connect Product Bulletin

- Protocols in discovering AP
  - DDPv5 (path: C:> Program Files (x86) > Nuclias Connect > Core > agentServer > ddpv5 > lib

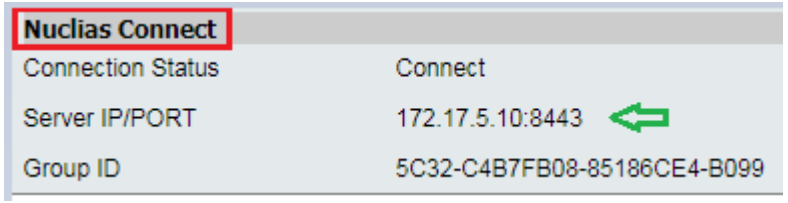
DDP Version 5

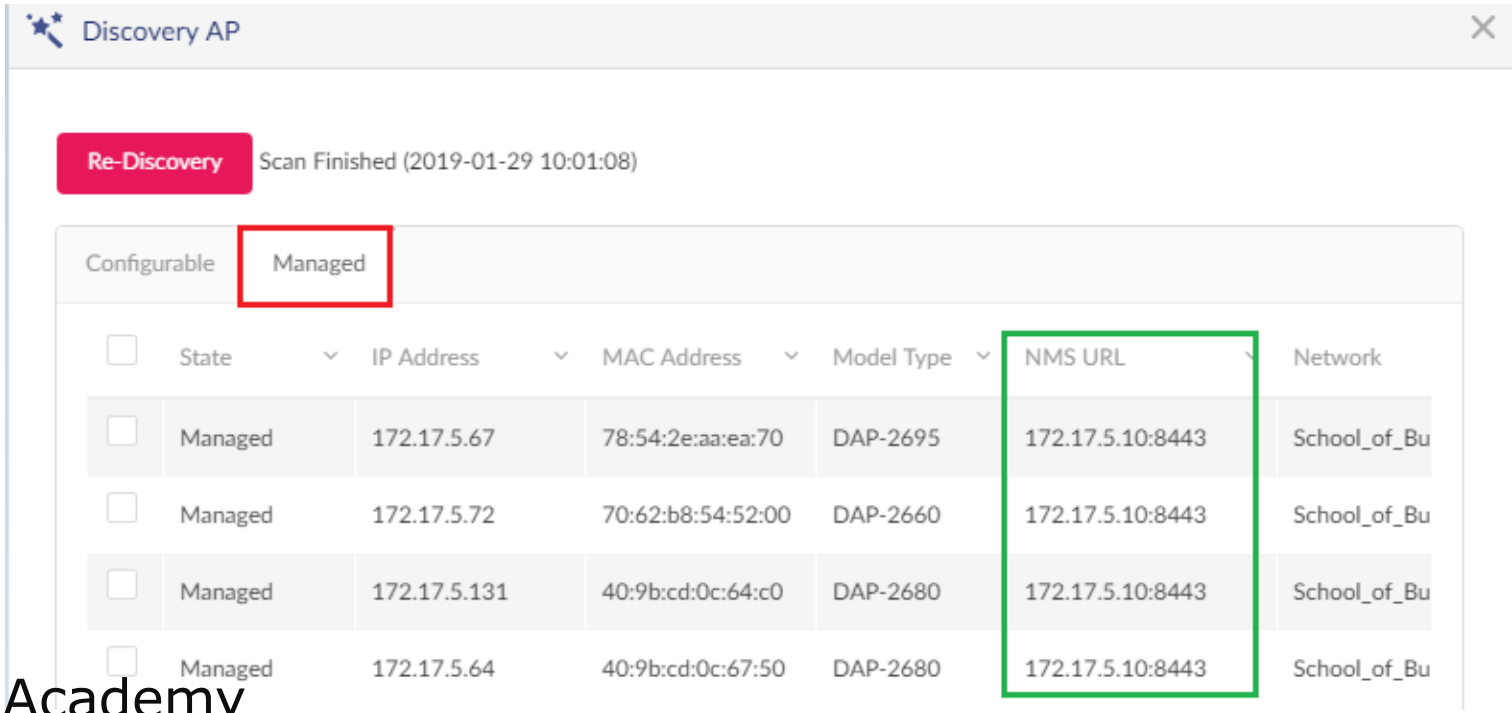
- DDP is a client-server protocol for discovering and configuring network devices, i.e. Ethernet switch, AP, in the LAN.
- The below image sketch presents the folder in a closer way.



Nuclias Connect Product Bulletin

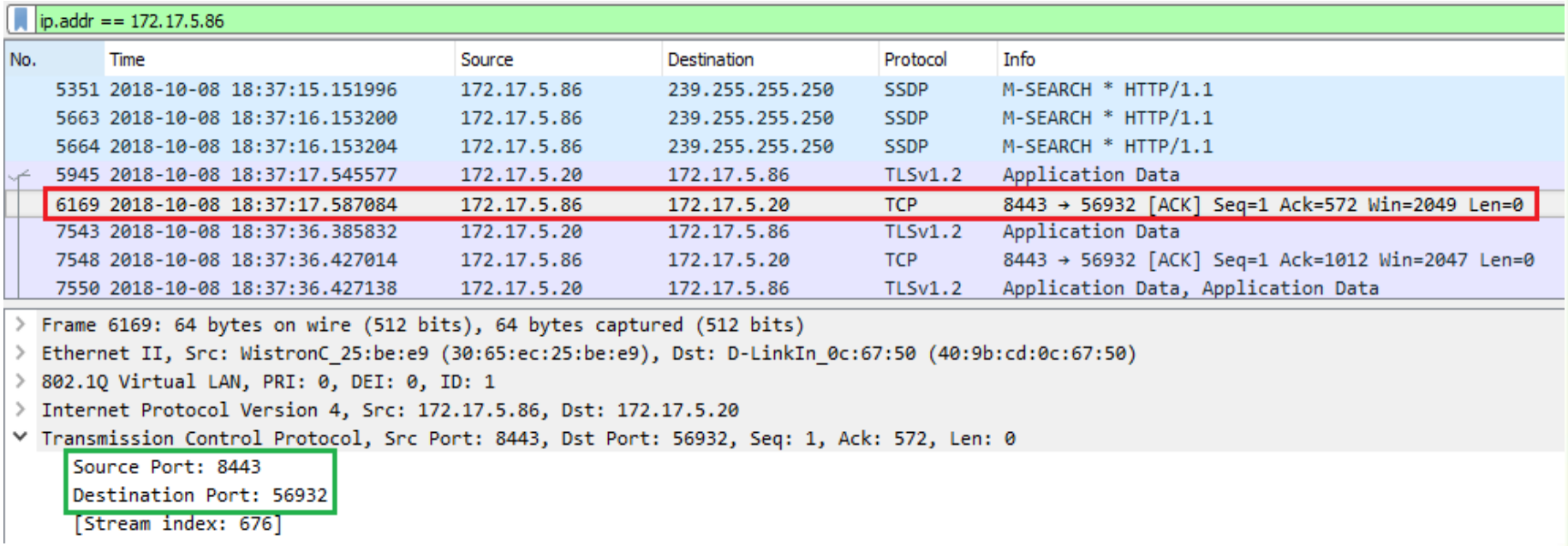
- There are other configuration pages releasing the fact that TCP 8443 port being utilized.
  - DAP Local GUI
  - Nuclias Connect AP Discovery





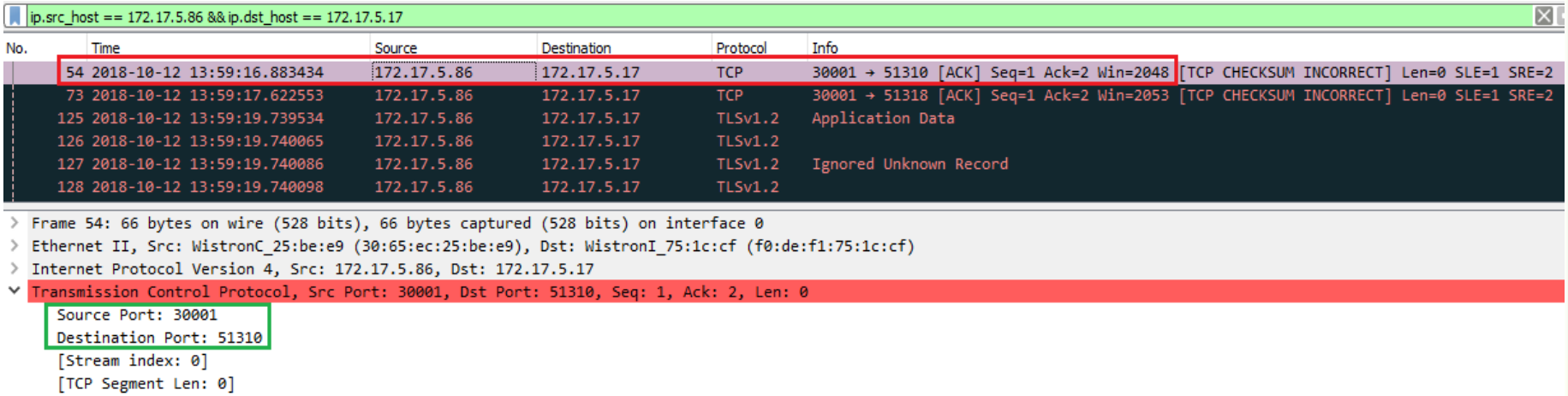
TCP Port Is In Use (Wireshark Capture)

- The below screen shot indicates a Nuclias Connect server (172.17.5.86) communicates with a DAP-2680 (172.17.5.20).
  - TCP Source Port: 8443
  - TCP Destination Port: 56932



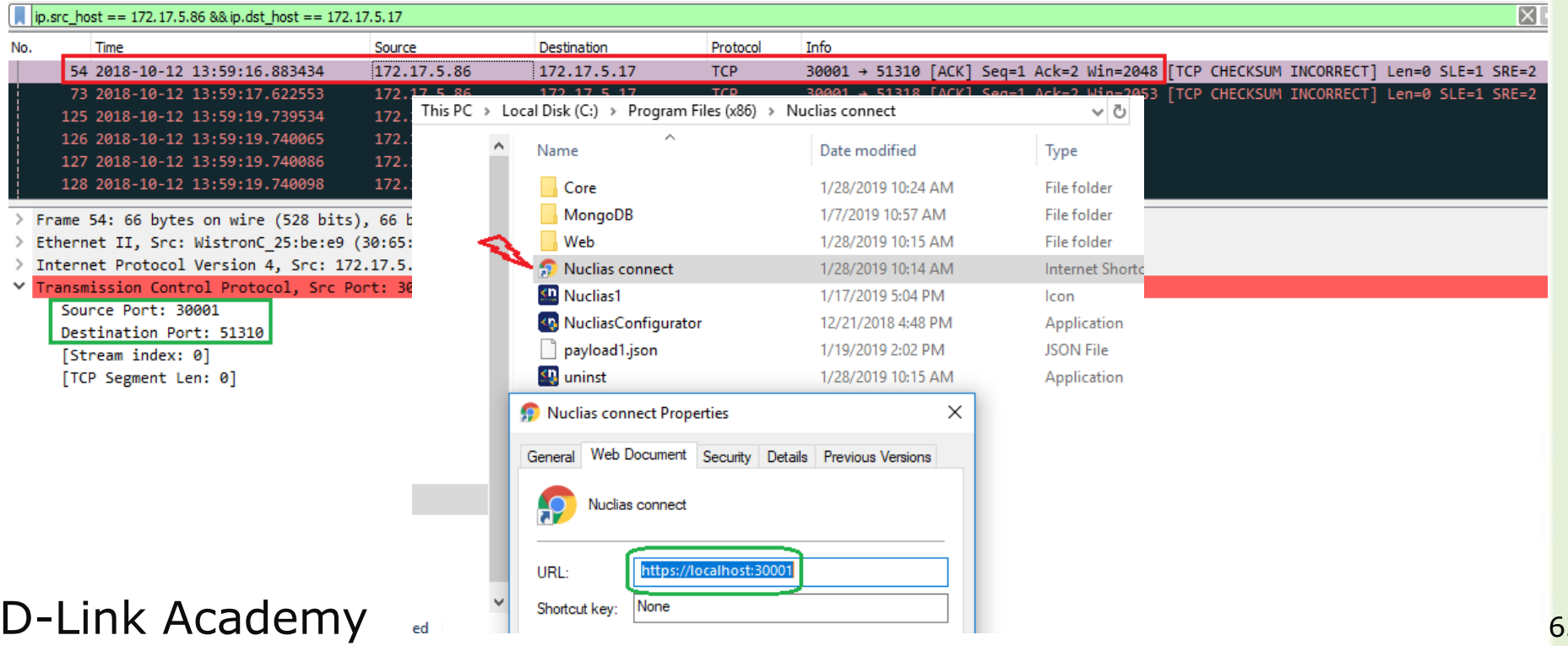
TCP Port Is In Use (Wireshark Capture)

- The below screen shot indicates a Nuclias Connect (172.17.5.86) responds GUI remote access from a workstation (172.17.5.17).
  - TCP Source Port: 30001
  - TCP Destination Port: 51310



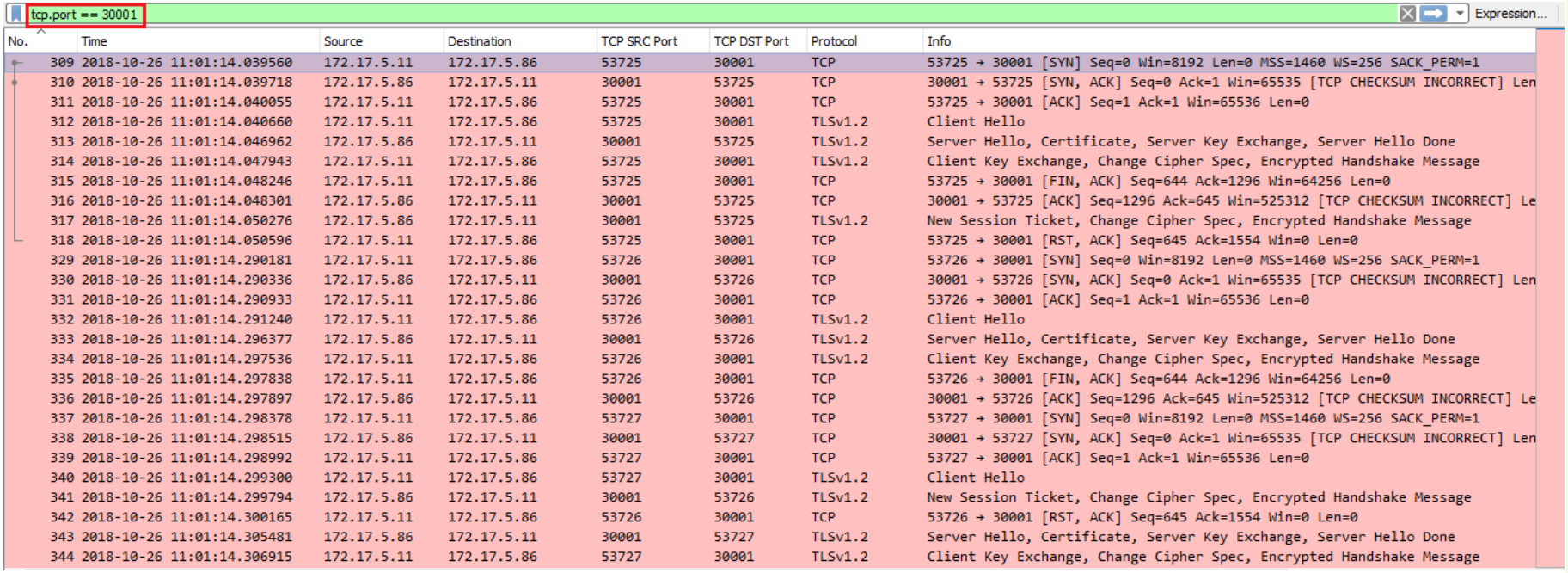
TCP Port Is In Use (Wireshark Capture)

- The below screen shot indicates a Nuclias Connect (172.17.5.86) responds GUI remote access from a workstation (172.17.5.17).
  - TCP Source Port: 30001
  - TCP Destination Port: 51310



TCP Source Port: 30001

- The below diagram is another example where a workstation (172.17.5.11) and Nuclias Connect (172.17.5.86) exchange web content via TCP Port (30001).



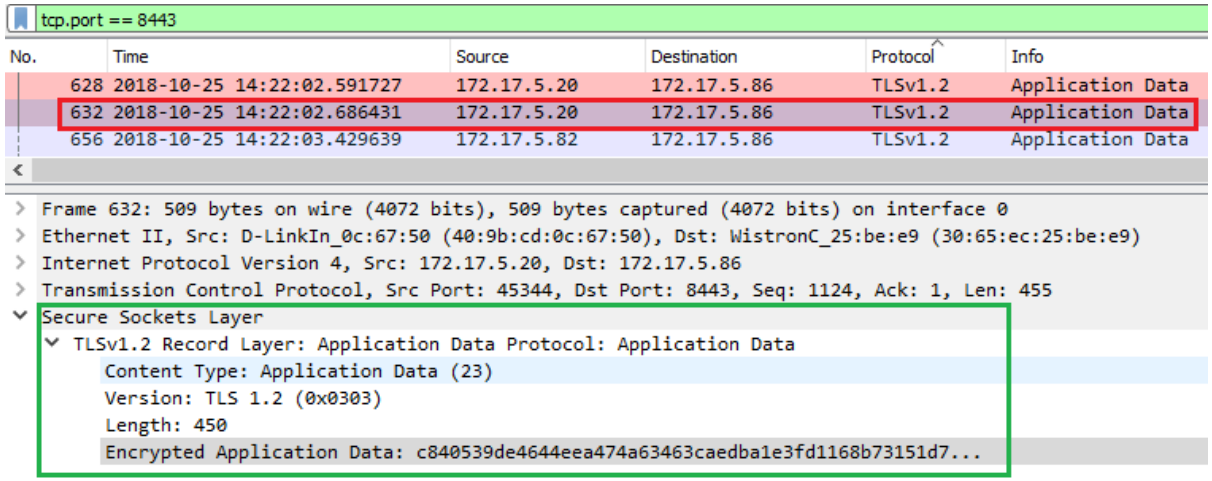
tcp.port == 30001

No.	Time	Source	Destination	TCP SRC Port	TCP DST Port	Protocol	Info
309	2018-10-26 11:01:14.039560	172.17.5.11	172.17.5.86	53725	30001	TCP	53725 → 30001 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
310	2018-10-26 11:01:14.039718	172.17.5.86	172.17.5.11	30001	53725	TCP	30001 → 53725 [SYN, ACK] Seq=0 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len
311	2018-10-26 11:01:14.040055	172.17.5.11	172.17.5.86	53725	30001	TCP	53725 → 30001 [ACK] Seq=1 Ack=1 Win=65536 Len=0
312	2018-10-26 11:01:14.040660	172.17.5.11	172.17.5.86	53725	30001	TLSv1.2	Client Hello
313	2018-10-26 11:01:14.046962	172.17.5.86	172.17.5.11	30001	53725	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Server Hello Done
314	2018-10-26 11:01:14.047943	172.17.5.11	172.17.5.86	53725	30001	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
315	2018-10-26 11:01:14.048246	172.17.5.11	172.17.5.86	53725	30001	TCP	53725 → 30001 [FIN, ACK] Seq=644 Ack=1296 Win=64256 Len=0
316	2018-10-26 11:01:14.048301	172.17.5.86	172.17.5.11	30001	53725	TCP	30001 → 53725 [ACK] Seq=1296 Ack=645 Win=525312 [TCP CHECKSUM INCORRECT] Le
317	2018-10-26 11:01:14.050276	172.17.5.86	172.17.5.11	30001	53725	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
318	2018-10-26 11:01:14.050596	172.17.5.11	172.17.5.86	53725	30001	TCP	53725 → 30001 [RST, ACK] Seq=645 Ack=1554 Win=0 Len=0
329	2018-10-26 11:01:14.290181	172.17.5.11	172.17.5.86	53726	30001	TCP	53726 → 30001 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
330	2018-10-26 11:01:14.290336	172.17.5.86	172.17.5.11	30001	53726	TCP	30001 → 53726 [SYN, ACK] Seq=0 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len
331	2018-10-26 11:01:14.290933	172.17.5.11	172.17.5.86	53726	30001	TCP	53726 → 30001 [ACK] Seq=1 Ack=1 Win=65536 Len=0
332	2018-10-26 11:01:14.291240	172.17.5.11	172.17.5.86	53726	30001	TLSv1.2	Client Hello
333	2018-10-26 11:01:14.296377	172.17.5.86	172.17.5.11	30001	53726	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Server Hello Done
334	2018-10-26 11:01:14.297536	172.17.5.11	172.17.5.86	53726	30001	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
335	2018-10-26 11:01:14.297838	172.17.5.11	172.17.5.86	53726	30001	TCP	53726 → 30001 [FIN, ACK] Seq=644 Ack=1296 Win=64256 Len=0
336	2018-10-26 11:01:14.297897	172.17.5.86	172.17.5.11	30001	53726	TCP	30001 → 53726 [ACK] Seq=1296 Ack=645 Win=525312 [TCP CHECKSUM INCORRECT] Le
337	2018-10-26 11:01:14.298378	172.17.5.11	172.17.5.86	53727	30001	TCP	53727 → 30001 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
338	2018-10-26 11:01:14.298515	172.17.5.86	172.17.5.11	30001	53727	TCP	30001 → 53727 [SYN, ACK] Seq=0 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len
339	2018-10-26 11:01:14.298992	172.17.5.11	172.17.5.86	53727	30001	TCP	53727 → 30001 [ACK] Seq=1 Ack=1 Win=65536 Len=0
340	2018-10-26 11:01:14.299300	172.17.5.11	172.17.5.86	53727	30001	TLSv1.2	Client Hello
341	2018-10-26 11:01:14.299794	172.17.5.86	172.17.5.11	30001	53726	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
342	2018-10-26 11:01:14.300165	172.17.5.11	172.17.5.86	53726	30001	TCP	53726 → 30001 [RST, ACK] Seq=645 Ack=1554 Win=0 Len=0
343	2018-10-26 11:01:14.305481	172.17.5.86	172.17.5.11	30001	53727	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Server Hello Done
344	2018-10-26 11:01:14.306915	172.17.5.11	172.17.5.86	53727	30001	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Nuclias Connect Product Bulletin

- From CWM 1.03 to Nuclias Connect, How a DAP being managed
- In CWM 1.03, when CWM manages a DAP (D-Track DK1500889)
  - SNMP Community was changed from public to pubqfzvq
  - RW SNMP Community was changed from private to priuhcb7
  - SNMPv3 Username was changed to sec27jbd
- In Nuclias Connect, DAP and DNC communication rely on TLSv1.2 (TCP 8443), where application data in the SSL session is encrypted.

"Keep alive" function is also being served

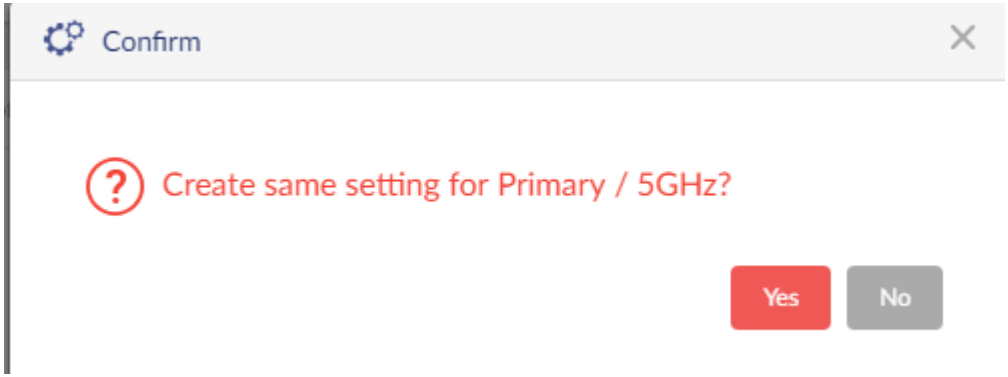


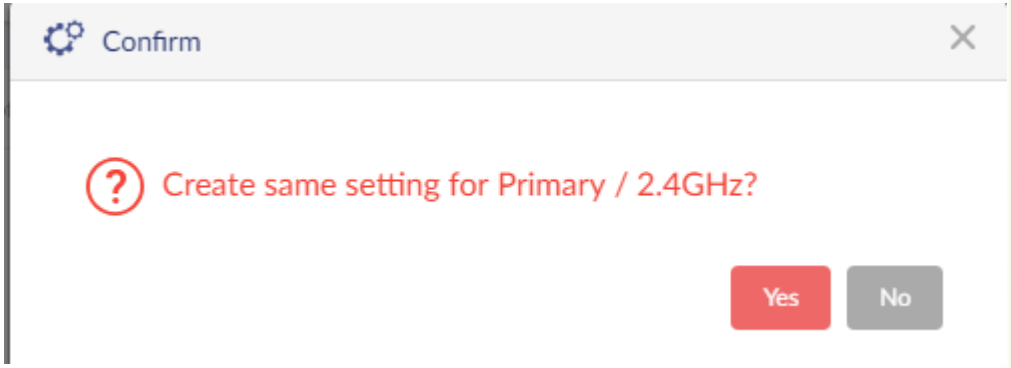
Nuclias Connect Product Bulletin

- In CWM 1.03, UDP 64768 is required for the communication between DAP and CWM on reserved for the Passcode User Authentication (D-Track DK1500579).
- In Nuclias Connect, the reservation of UDP 64768 is NOT necessary.

Nuclias Connect Product Bulletin

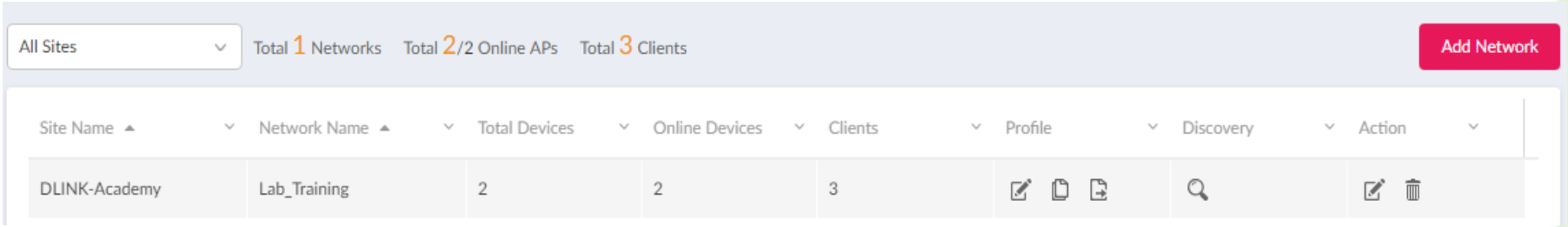
- From The legacy CWM to Nuclias Connect, friendly reminder message is presented should any modification of one wireless band is configured.

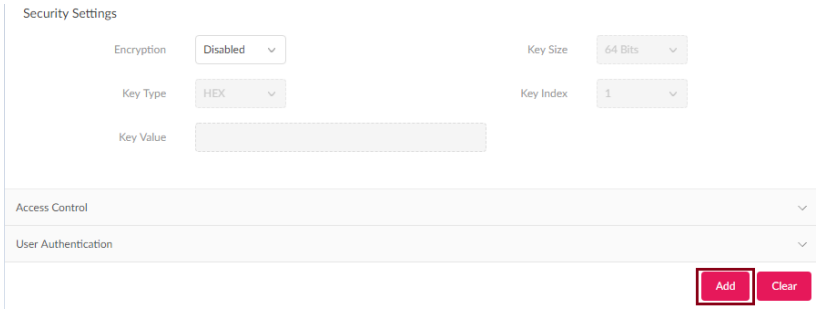




Nuclias Connect Product Bulletin

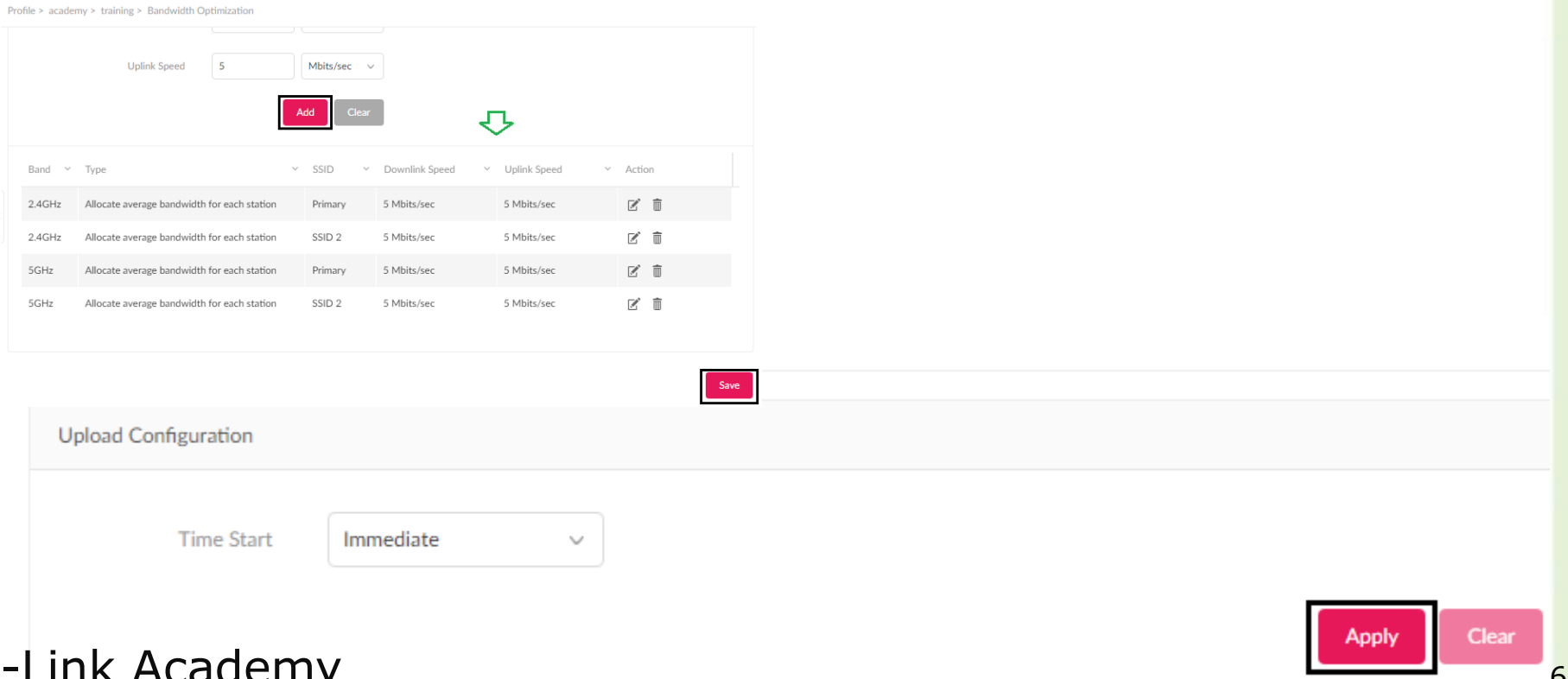
- Using “Add” button to make desired configuration visible and “Save” button written it (configuration) into Nuclias Connect database.





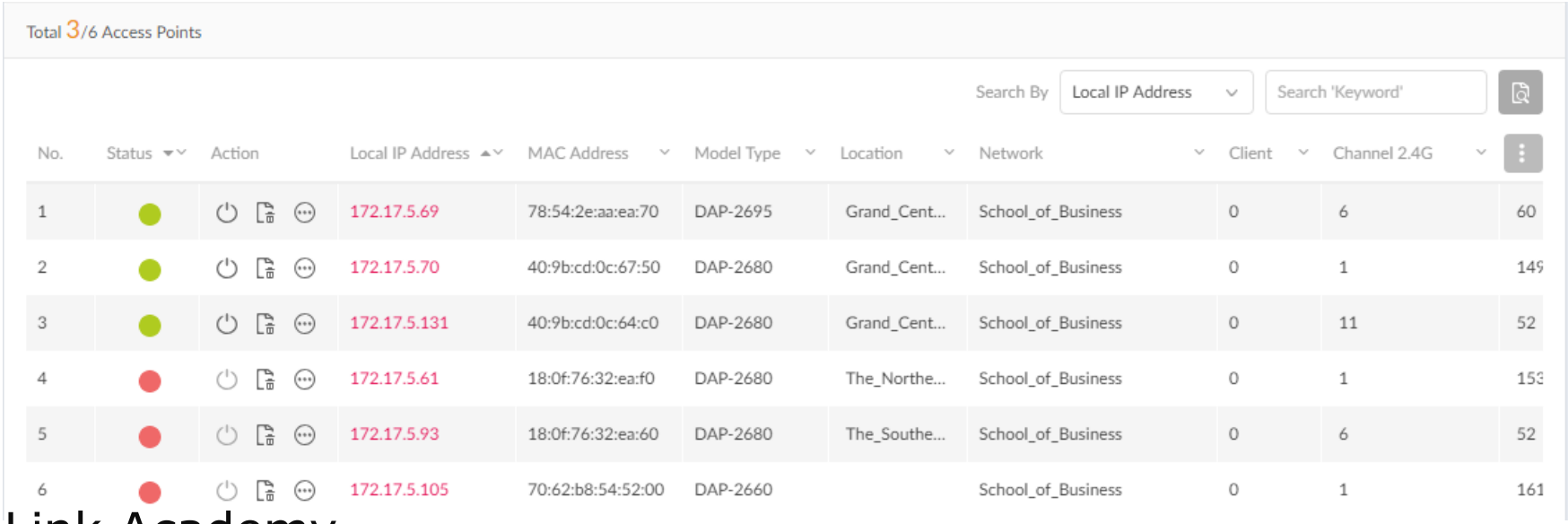
Nuclias Connect Product Bulletin

- Using “Add” button to make desired configuration visible and “Save” button written it (configuration) into Nuclias Connect database.
- “Apply” button forces the configuration update written into DAP.



Nuclias Connect Product Bulletin

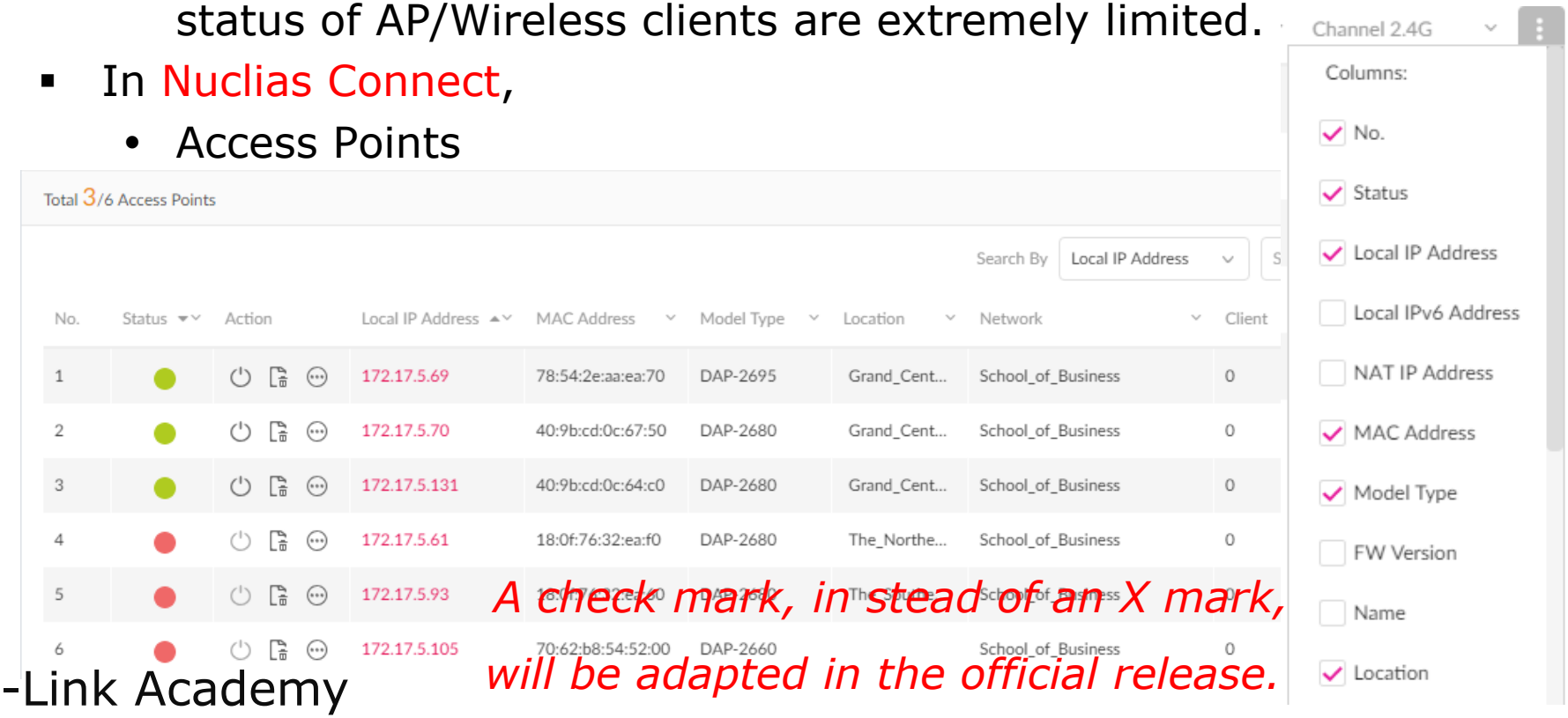
- From CWM 1.03 to DNC, AP/Wireless Client information display
- In CWM 1.03,
  - From the network management perspective, the information and status of AP/Wireless clients are extremely limited.
- In Nuclias Connect,
  - Access Points



No.	Status	Action	Local IP Address	MAC Address	Model Type	Location	Network	Client	Channel 2.4G	
1			172.17.5.69	78:54:2e:aa:ea:70	DAP-2695	Grand_Cent...	School_of_Business	0	6	60
2			172.17.5.70	40:9b:cd:0c:67:50	DAP-2680	Grand_Cent...	School_of_Business	0	1	149
3			172.17.5.131	40:9b:cd:0c:64:c0	DAP-2680	Grand_Cent...	School_of_Business	0	11	52
4			172.17.5.61	18:0f:76:32:ea:f0	DAP-2680	The_Northe...	School_of_Business	0	1	153
5			172.17.5.93	18:0f:76:32:ea:60	DAP-2680	The_Southe...	School_of_Business	0	6	52
6			172.17.5.105	70:62:b8:54:52:00	DAP-2660		School_of_Business	0	1	161

Nuclias Connect Product Bulletin

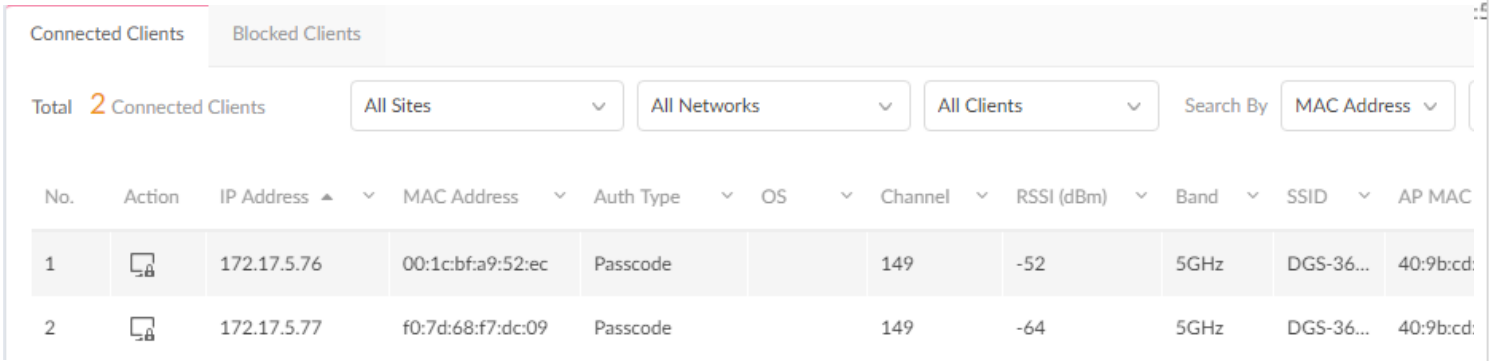
- From CWM 1.03 to DNC, AP/Wireless Client information display
- In CWM 1.03,
  - From the network management perspective, the information and status of AP/Wireless clients are extremely limited.
- In Nuclias Connect,
  - Access Points

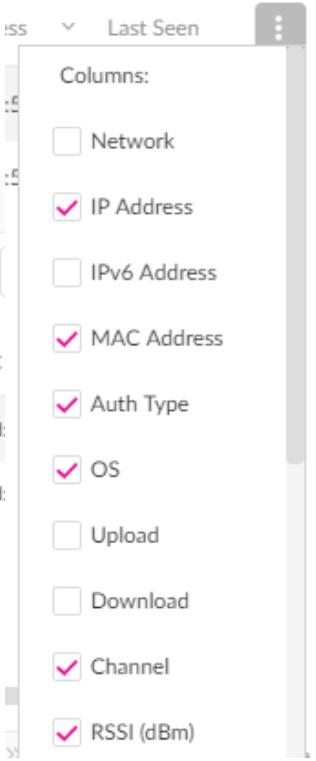


A check mark, in stead of an X mark, will be adapted in the official release.

Nuclias Connect Product Bulletin

- From CWM 1.03 to DNC, AP/Wireless Client information display
- In CWM 1.03,
  - From the network management perspective, the information and status of AP/Wireless clients are extremely limited.
- In Nuclias Connect,
  - Wireless Client(s)





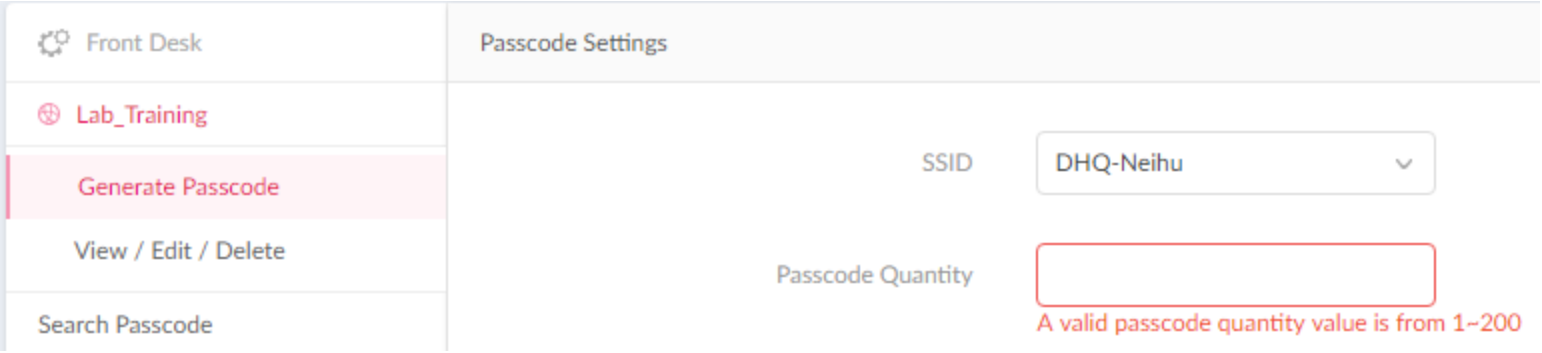
A check mark, in stead of an X mark, will be adapted in the official release.

Nuclias Connect Product Bulletin

- From CWM 1.03 to Nuclias Connect, passcode generation
- In CWM 1.03, (D-Track DK1600436)
  - The maximum number of passcode is 1000 for one group (One group refers to a single network of the site).
  - The maximum number of username/password is 128, per SSID.
- In Nuclias Connect,
  - There is no limit to the number of passcode can be generated in this release (please see next slides for detail explanation).
  - The maximum number of authentication type username/password remains the same (128, per SSID).

Nuclias Connect Product Bulletin

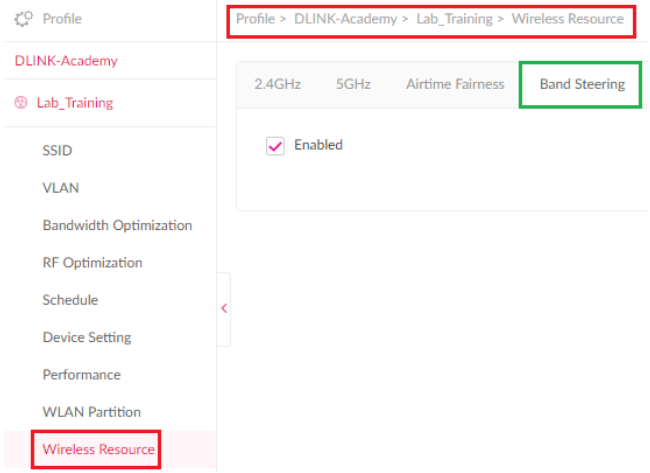
- From CWM 1.03 to Nuclias Connect, passcode generation
- In CWM 1.03, (D-Track DK1600436)
- In Nuclias Connect,
  - Every single attempt in passcode generation for one SSID is limited to 200 passcodes.
  - We are able to make multiple efforts on such actions.
  - Maximum two SSIDs within a network can be set for User Authentication passcode. (Band is counting separately)
  - Number of networks is unrestrained within a Site.



Nuclias Connect Product Bulletin

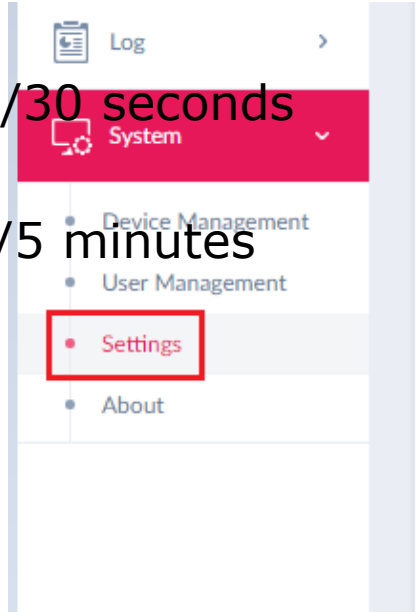
- From CWM 1.03 to Nuclias Connect, the available setting in band steering
- In CWM 1.03,
  - The band steering function is only available in primary SSID (D-Track DK1700050). [bottom left hand screenshot]
- In Nuclias Connect,
  - The band steering function is available in all SSIDs, besides the primary one. [bottom right hand screenshot for details]

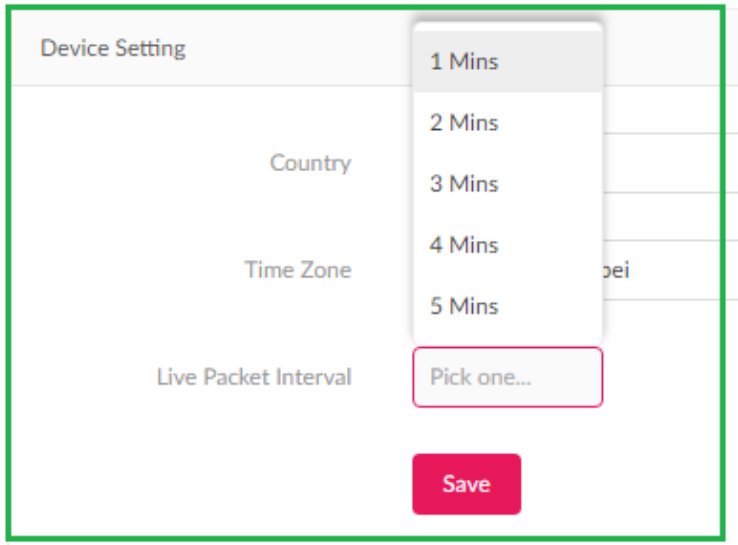




Nuclias Connect Product Bulletin

- From CWM 1.03 to Nuclias Connect, Live Packet Interval
- Live Packet Interval is a parameter to define time periods individual AP responds to CWM on its (DAP) activities
- Should we have mass configuration and (DAP) deployment in our topology, high frequency of these messages may potentially yield undesirable to DNC, leading wireless stations hang issues.
- In CWM 1.03,
  - Options: 5/10/20/30 seconds
- In Nuclias Connect,
  - Options: 1/2/3/4/5 minutes





Nuclias Connect Product Bulletin

- From CWM 1.03 to Nuclias Connect, DAP (Access Points) Topology Maps
- In CWM 1.03,
  - Customized Map View with network Topology and connected wireless clients.
  - The installed memory (RAM) produces greater restraint on the number of devices being displayed. (D-Track DK1700415).
- In Nuclias Connect,
  - The Customized Map View and Google Maps view are expected in phase 2.



Nuclias Connect Product Bulletin

- From CWM 1.03 to Nuclias Connect, The Reporting
- In CWM 1.03, (D-Track DK1600436)
  - Reports being unavailable with the right format.
  - Lack of visibility and a single holistic view of the enterprise performance.
- In Nuclias Connect,
  - Graphic data enhances the visibility of activities.
  - An innovative and creative work brings high value.
  - "The Design Thinking of Dashboard and Report" session is dedicated to details.

Nuclias Connect Product Bulletin, System Upgrade

- The upgrade procedure of CWM server from v1.01 to v1.02 is stated in D-Track DK1500609.

From CWM 1.03 to Nuclias Connect

- Start from scratch
  - Get a fresh system install
- Direct upgrade
  - DAPs device firmware upgrade. IP address of that DAP remains the same, an easy way to be discovered by Nuclias Connect.
    - Under NAT environment, align with mobile app
  - AP profile upgrade tool [cwmMigrationTool-1.0.9.exe, under development]

It is important that a DAP is installed with Nuclias Connect supported firmware.



Nuclias Connect Product Bulletin, System Upgrade

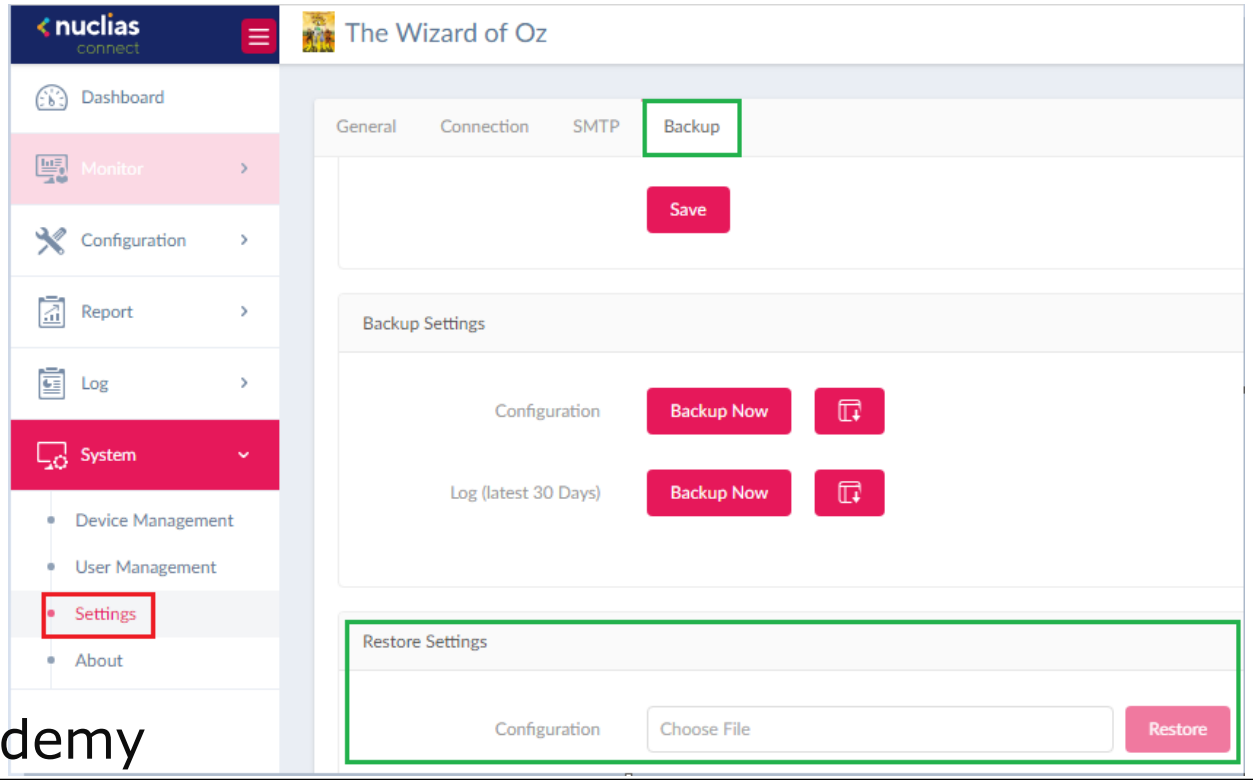
- The upgrade procedure from CWM 1.03 (Windows 7, 8, 10, Server 2012) to Nuclias Connect (Windows & Linux)
- AP profile upgrade tool [cwmMigrationTool-1.0.9.exe, under development]



- Configurations plan to be transferred: Site/Network topology and configuration, SMTP, user account privileges and details
- Creates a file createddbMigration_Configuration_{dateTime}.cfg, and then it is used to restore back to Nuclias Connect.

Nuclias Connect Product Bulletin, System Upgrade

- The upgrade procedure from CWM 1.03 (Windows 7, 8, 10, Server 2012) to Nuclias Connect (Windows & Linux)
- Creates a file createddbMigration_Configuration_{dateTime}.cfg, and then it is used to restore back to Nuclias Connect.

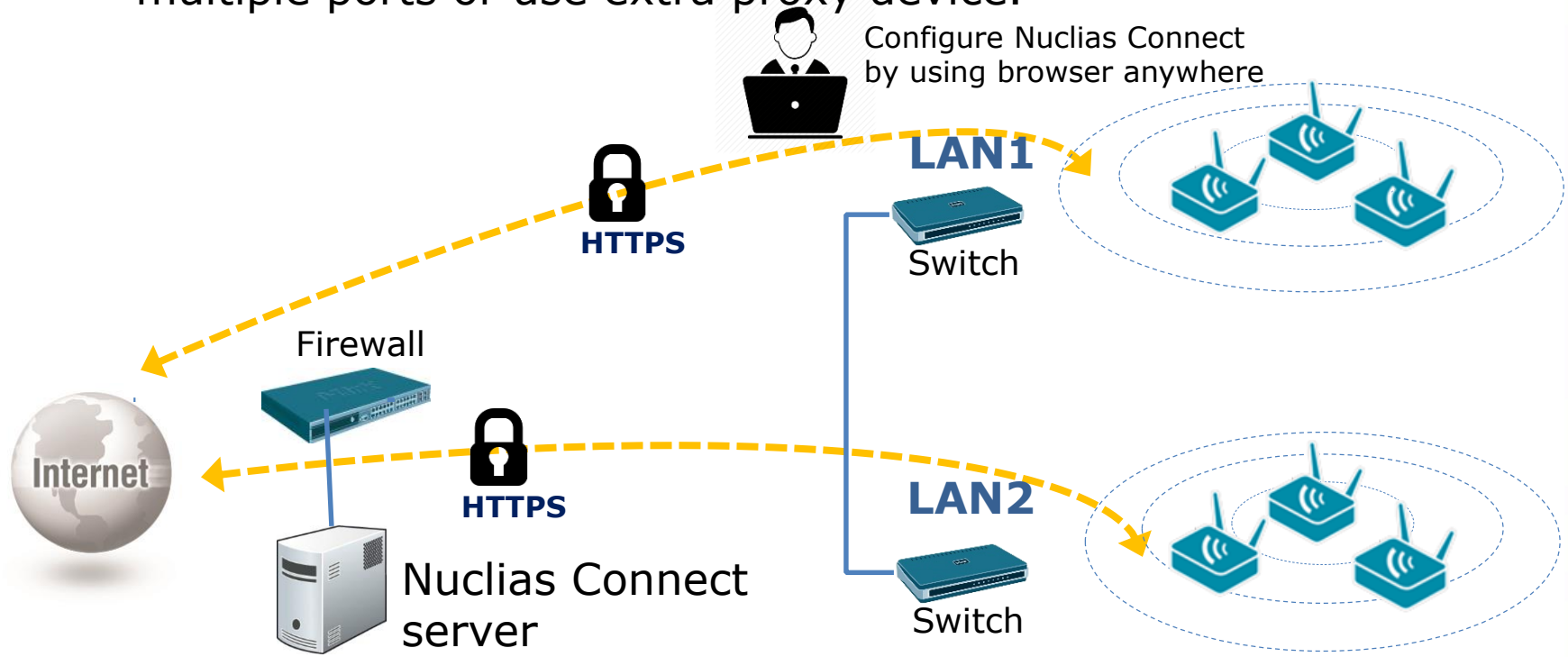


Nuclias Connect Product Bulletin

- Despite the wireless features being provided are not dissimilar between two releases, Nuclias Connect does have better visibility and control tools.
- There is no limit to the number of "Site" and "Network‟ in both releases (D-Track DK1700227). [Site/Network: Multi-tenant authorization structure]
- Remote DNC management can be achieved in a production server, even with multiple Network Interface Cards (NICs) configurations.
- More than 1,000 DAPs in our customer environment can be managed on a project based collaboration. [proven record of success]
- Profile Configuration and DAP firmware update by scheduling [the concept of “AP grouping configuration” stays]
- The active online administrators can be more than 100 [enterprise architecture design]

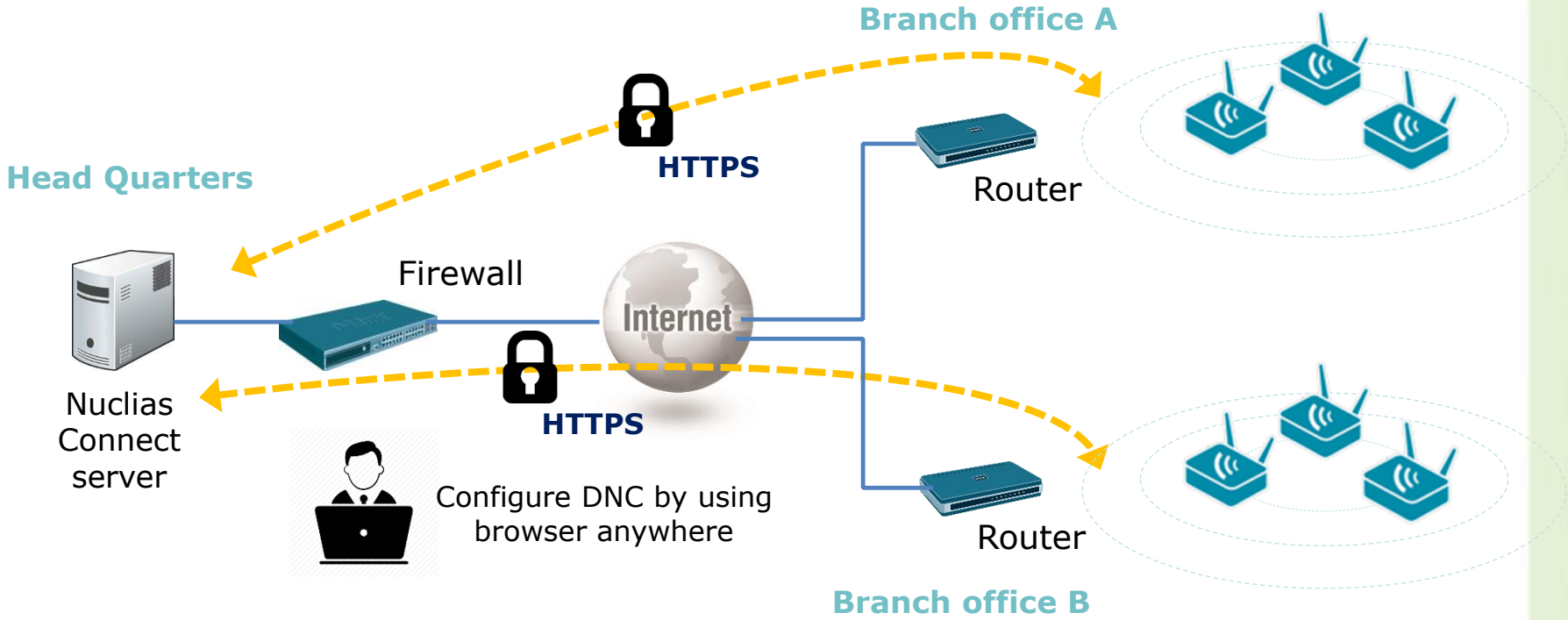
Nuclias Connect Deployment Structure

- Manage APs in local site
  - APs use build in https agent to pass through internet and the directly connect to Nuclias Connect server, no need to reserve multiple ports or use extra proxy device.



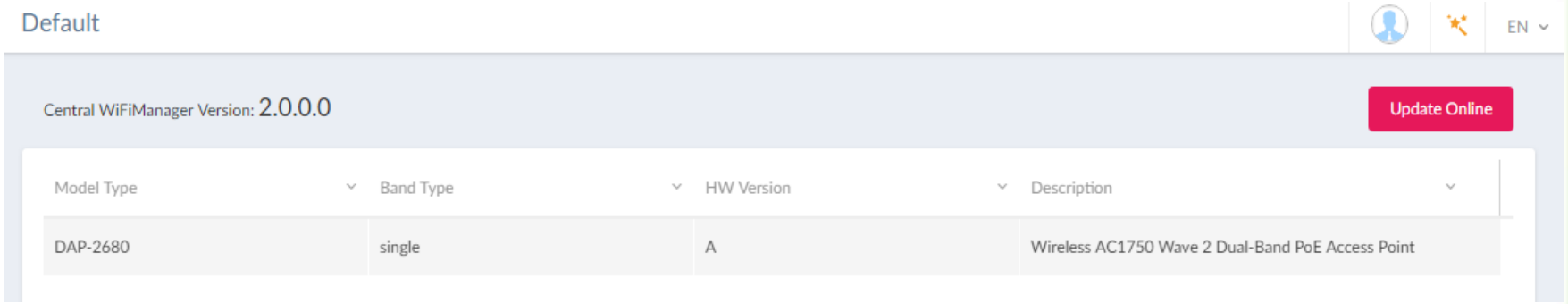
Nuclias Connect Deployment Structure

- Manage APs in multiple sites
  - APs use build in https agent to pass through internet and connect to Nuclias Connect server directly, no need to open multiple ports or use extra proxy device.



Supported Devices And Plan

- DAP-2680 is identified as the FIRST model working with DNC



- The official release will be capable of managing
  - DAP-2695, DAP-3662, DAP-2660, DAP-2610
  - DAP-2310, DAP-2360, DAP-2230, DAP-2662
  - DAP-3666, DAP-2620
  - DAP-2682, DAP-2720
  - DAP-3315
  - Incoming DAP roadmap models (802.11ac WAVE2 and above)

Please contact your D-Link sales representative for details

Supported Devices And Plan

Product Roadmap Plan [Please contact your D-Link sales representative for details]

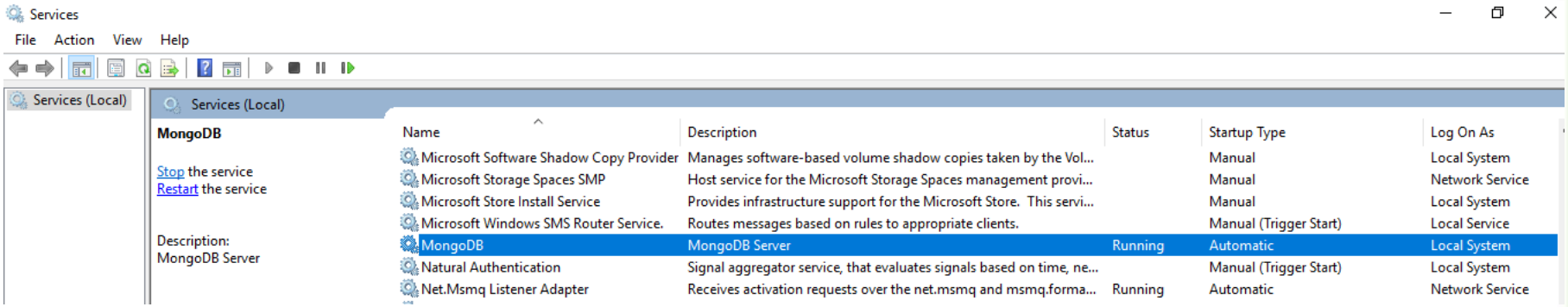
- Nuclias Connect configuration and database backup (CLI, 2.0; GUI, 2.1)
- Google / Custom map view (2.1)
- Wi-Fi Protected Access (WPA3) (2.1)
- FOTA (firmware download) (2.1)
- Fast Roaming (2.1)
- Social Network (Google, Facebook) authentication (2.1)
- DAP online/offline status event (2.1)
- Spectrum Analysis (2.2)
- Load balancing optimization (2.2)

Nuclias Connect Hands-on Tutorial

- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

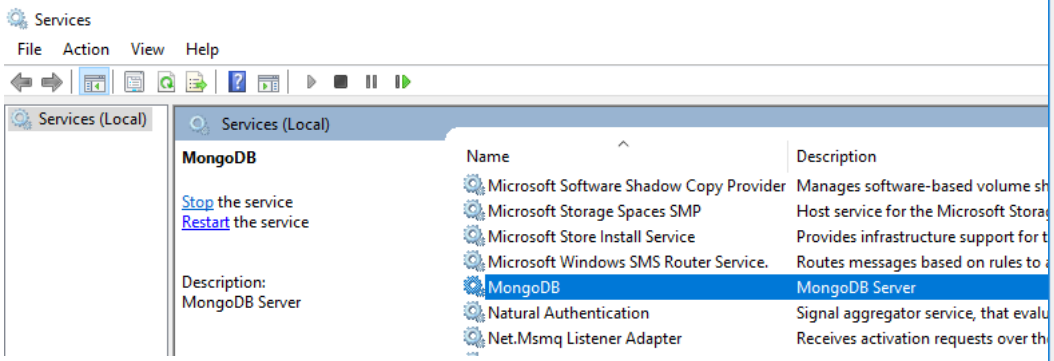
Nuclias Connect System Checkup

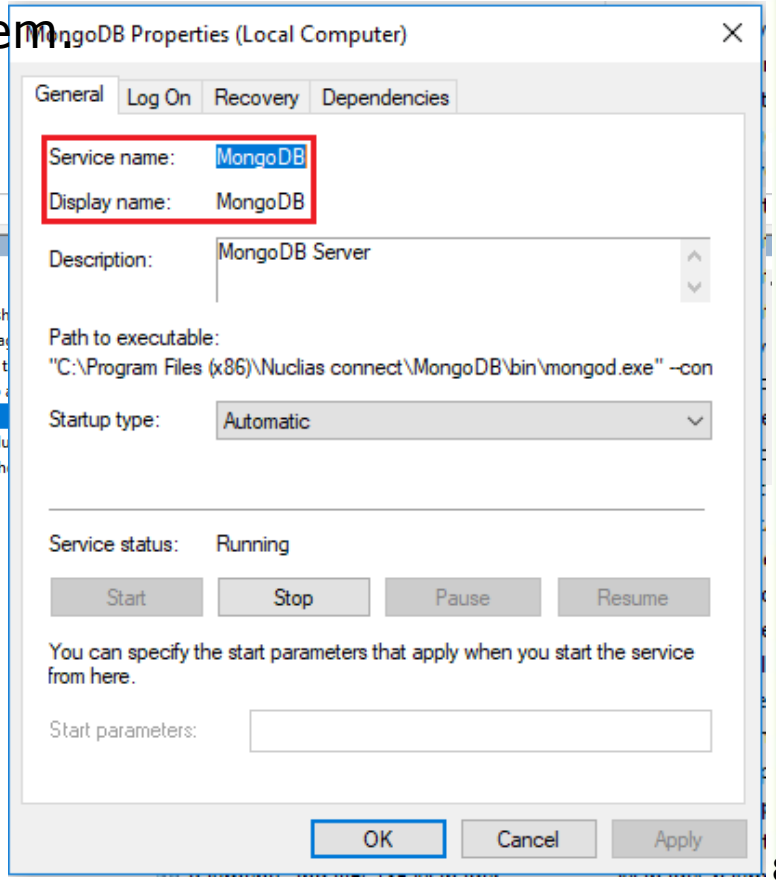
- Nuclias Connect System Checkup [v.1.0.0.19]
- The Services tool displays the services installed on our Windows system and allows you to manage them.
- MongoDB service



Nuclias Connect System Checkup

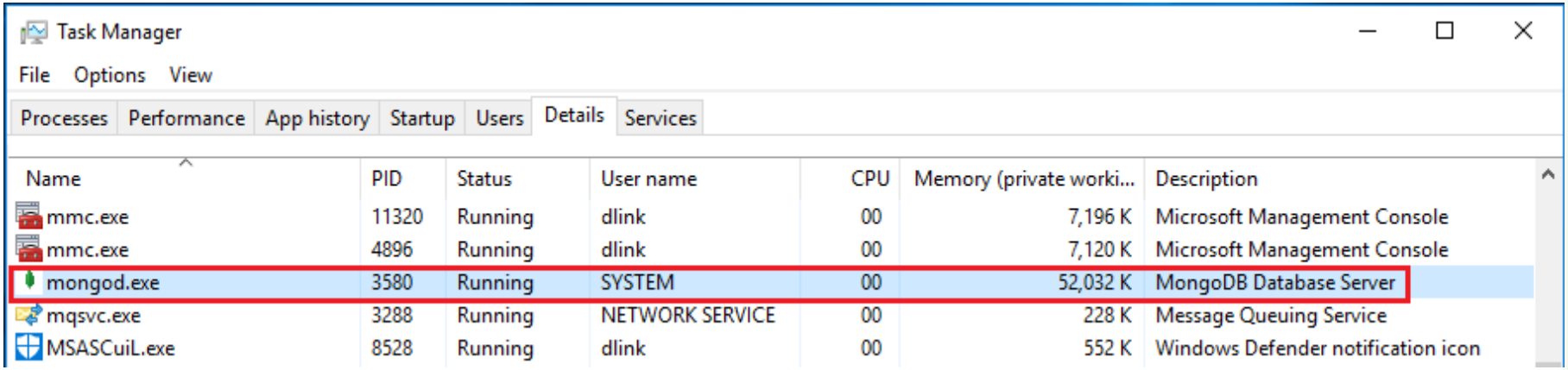
- Nuclias Connect System Checkup [v.1.0.0.19]
- The Services tool displays the services installed on our Windows system and allows you to manage them.
- MongoDB service





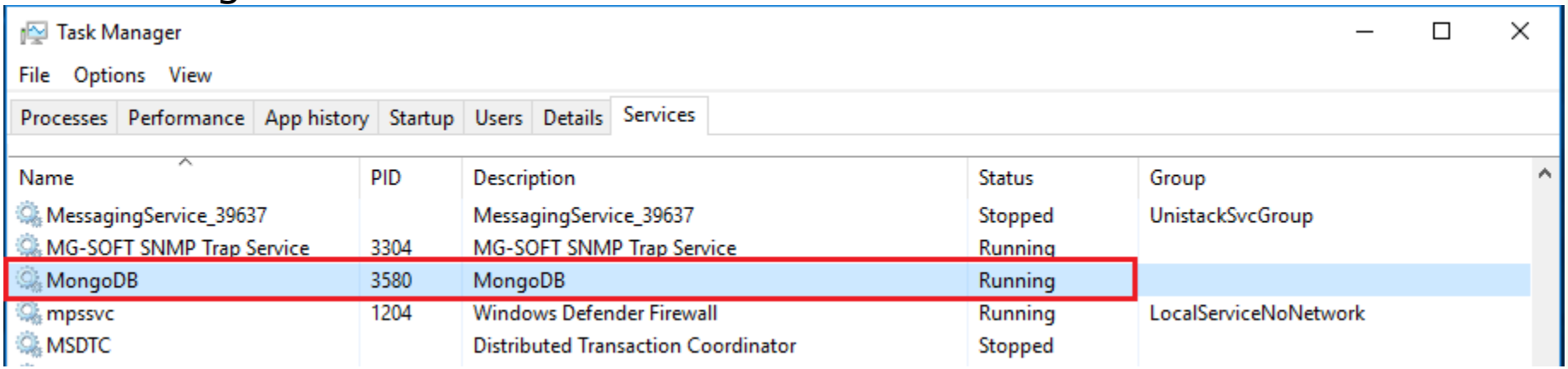
Nuclias Connect System Checkup

- Nuclias Connect System Checkup [v.1.0.0.19]
- Task Manager is a utility included in Windows that shows you what programs are running on your computer.
- The Details tab shows every individual process that's running right now. (finding out an executable's exact location and/or its PID)
- Mongod.exe



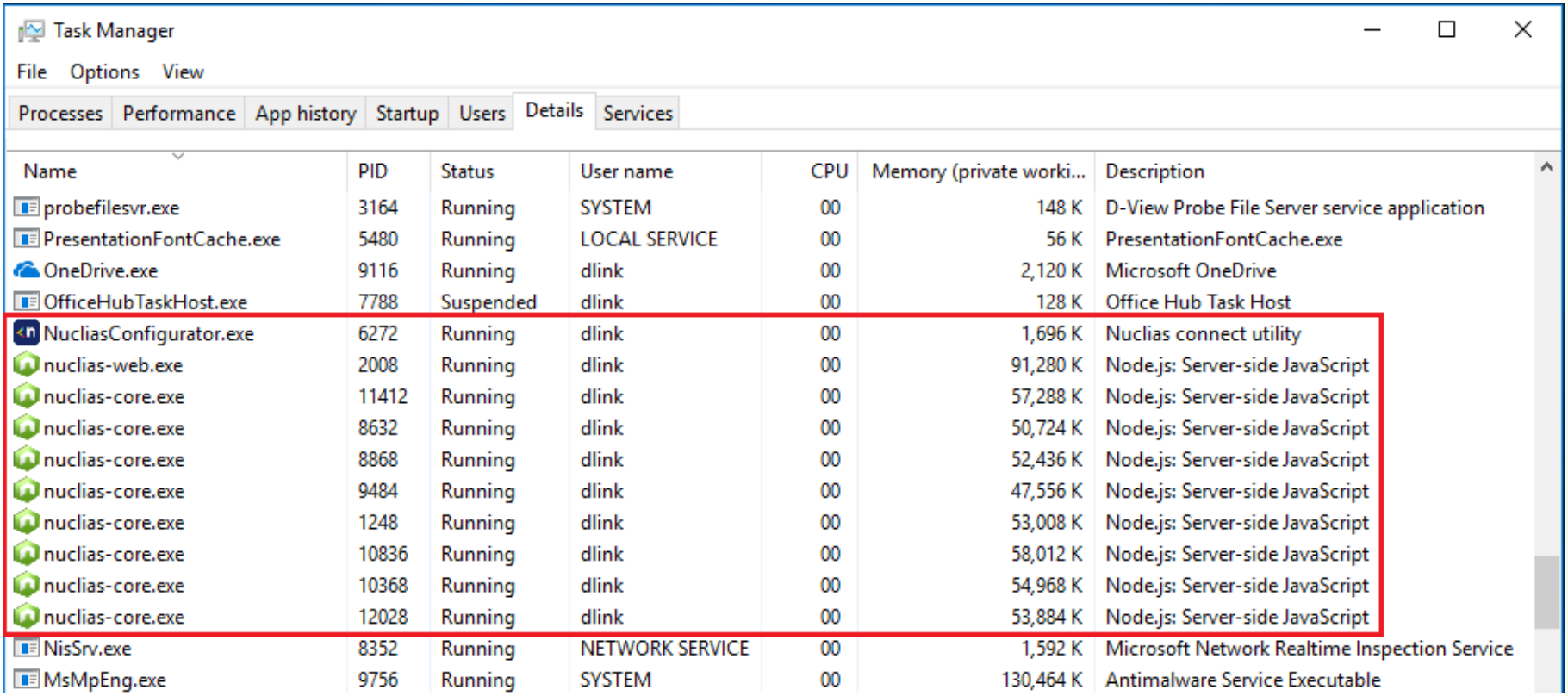
Nuclias Connect System Checkup

- Nuclias Connect System Checkup [v.1.0.0.19]
- Within Task Manager, the Services tab shows at least some of the Windows services installed on your computer. Most services will be Running or Stopped. (a quick and convenient way to start and stop major Windows services.)
- MongoDB



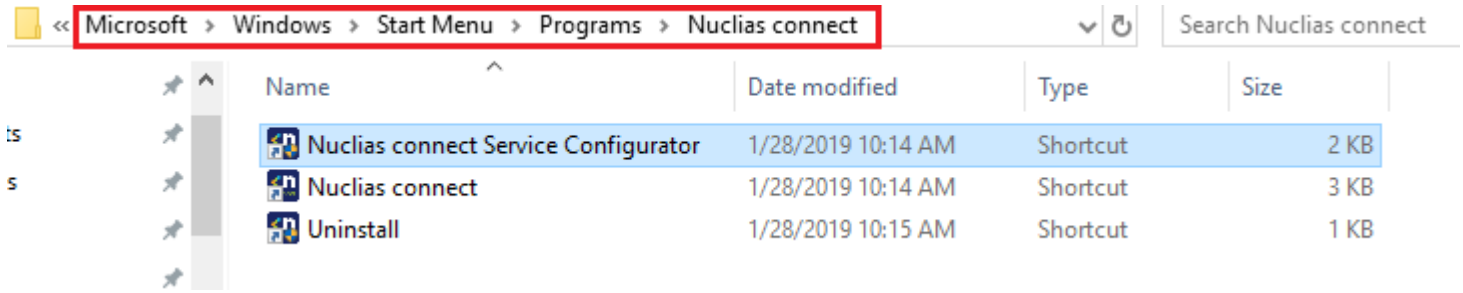
Nuclias Connect System Checkup

- Nuclias Connect System Checkup [v.1.0.0.19]
- The Details tab on NucliasConfigurator.exe and Nuclias-core.exe



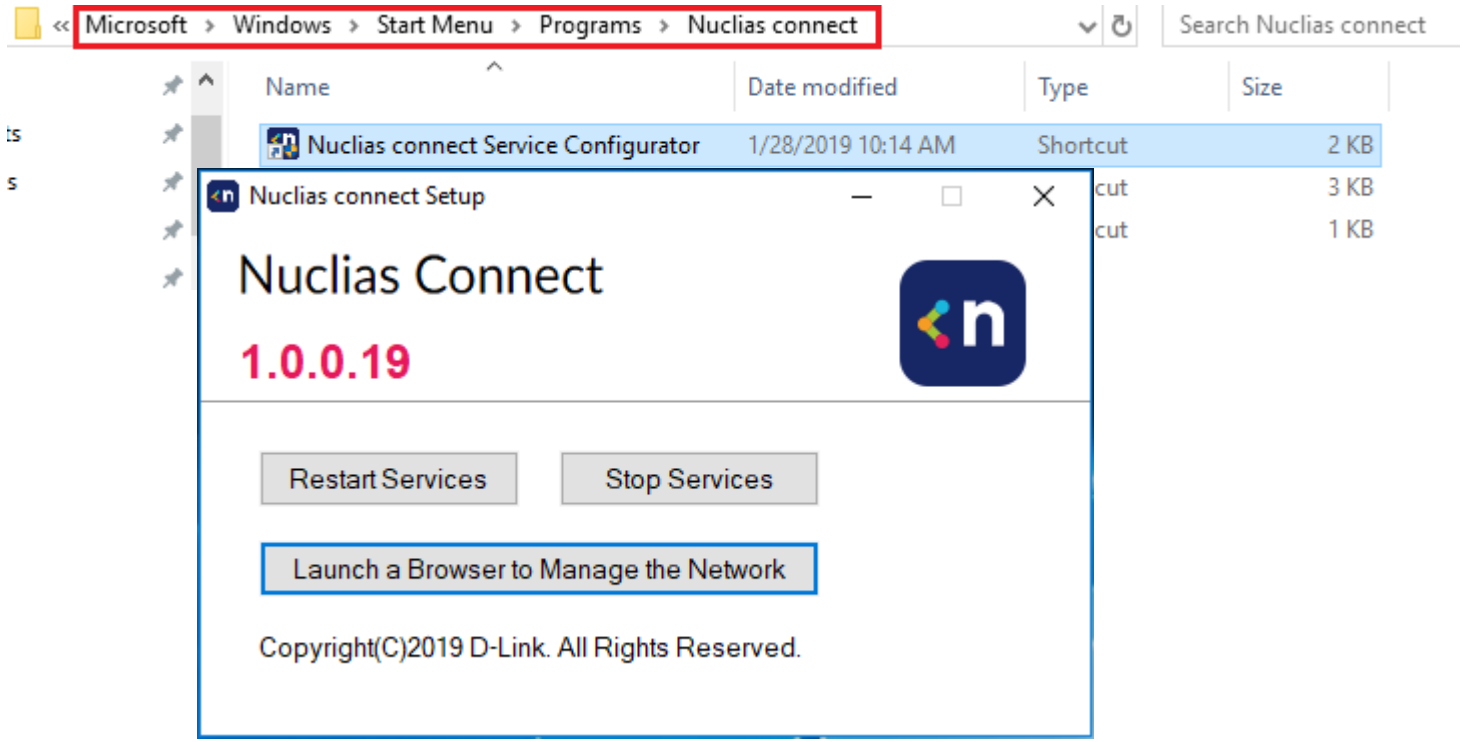
To Launch Nuclias Connect Application

- After the installation, right-click on the "Nuclias Connect" folder from our desktop, we shall be able to see three shortcuts are presented here.



To Launch Nuclias Connect Application

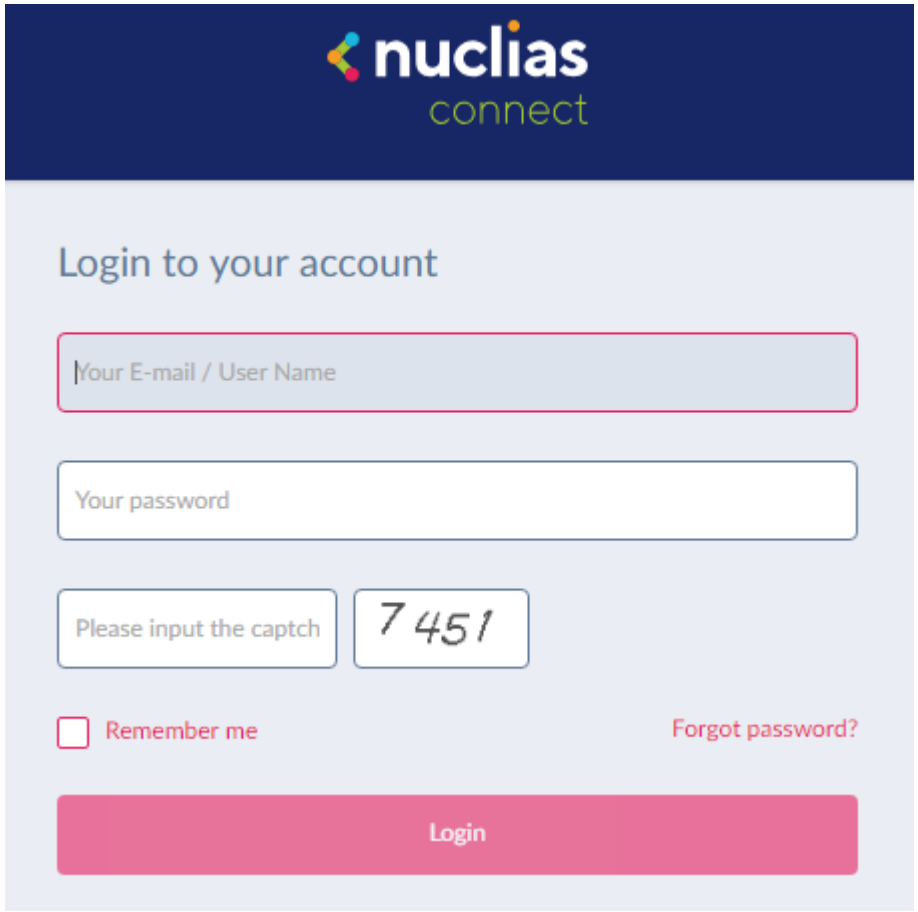
- After the installation, right-click on the "Nuclias Connect" folder from our desktop, we shall be able to see three shortcuts are presented here.



Nuclias Connect Login Page

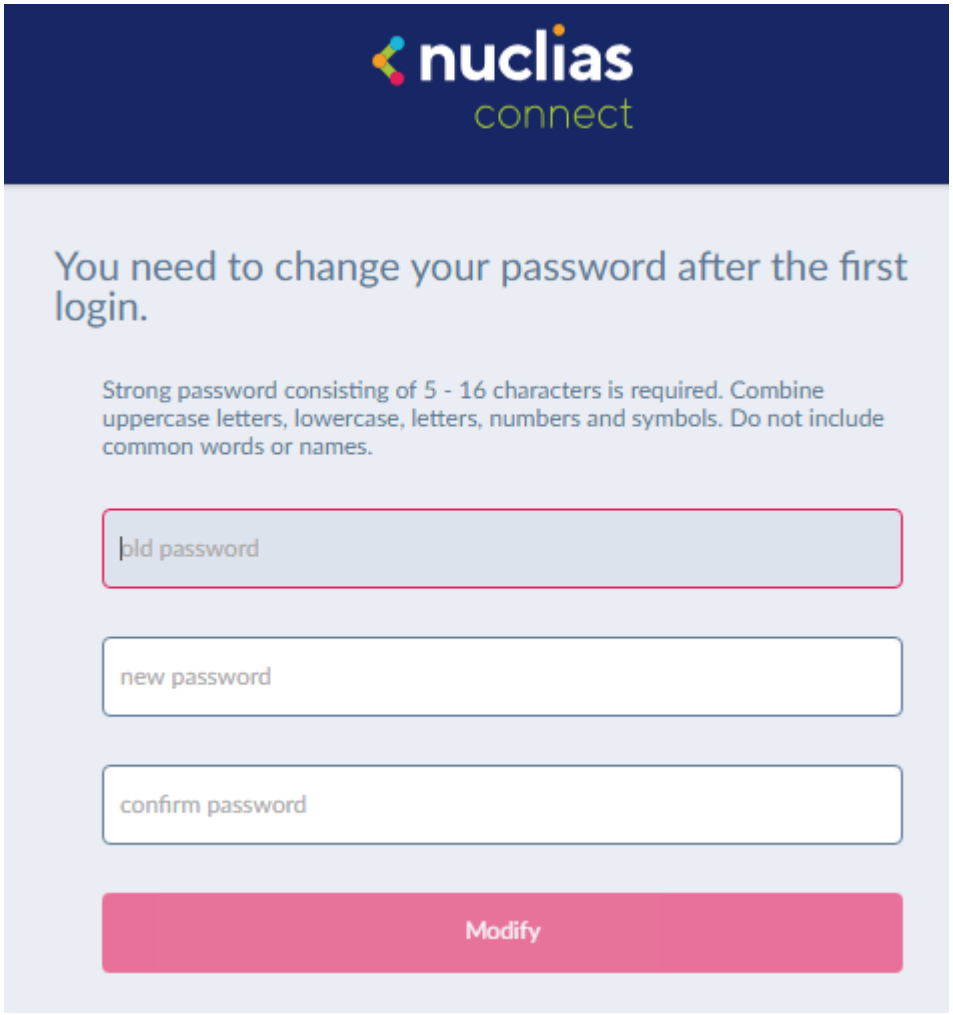
- In DNC Login Page, you need to have your credential ready (default ID/PWD: admin/admin)

User can use browser to login to DNC server by using HTTPS for remote management. (i.e. https://172.17.5.86:30001/)



Nuclias Connect Login Page (Password Change)

- For newly registered users in Nuclias Connect server, the first login will be prompted with password change request.



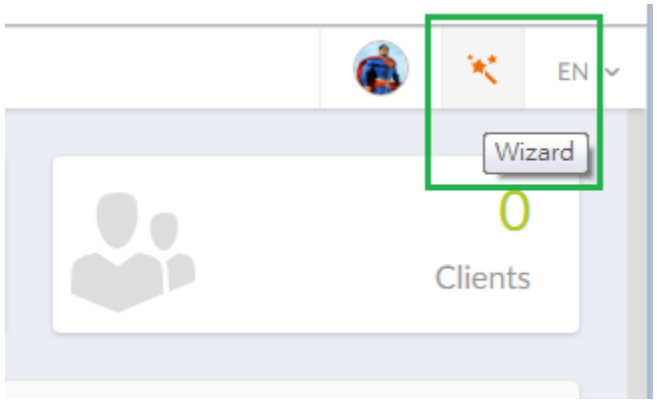
Nuclias Connect User Account Management

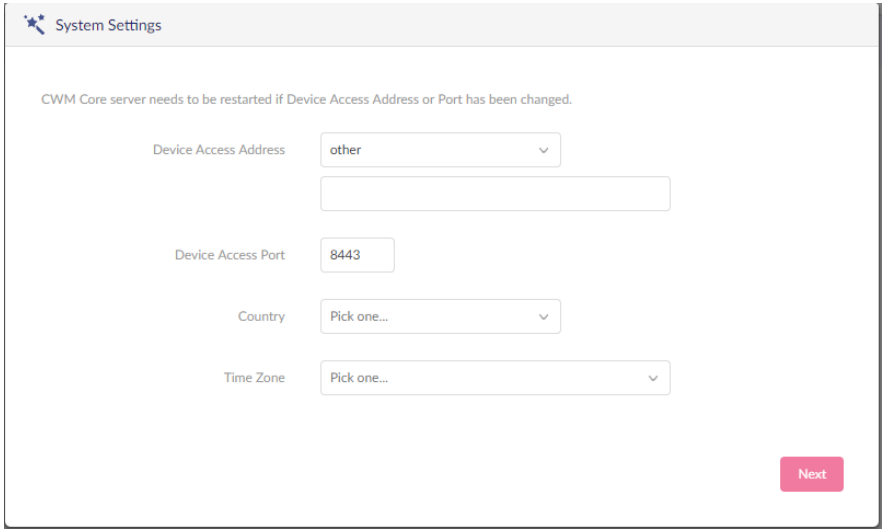
- User account, Administrator is created by default where all of the others accounts are generated by Administrator.
  - Login default/password: admin/admin
- Despite the flexibility of admin user account password changes, D-Track DK1600299 discloses the difficulty to retrieve admin password should it gets misplaced.
- Newly generated user account, first time login and password change process.

Nuclias Connect Setup Wizard (System Setting)

- During Nuclias Connect initial launch, we are requested to provide system settings.

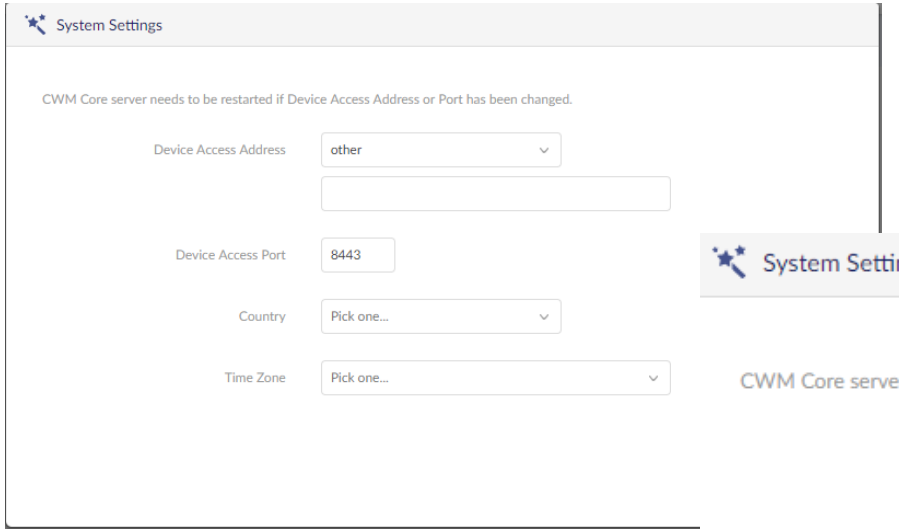
Nuclias Connect Wizard is located on the upper right hand corner of the screen

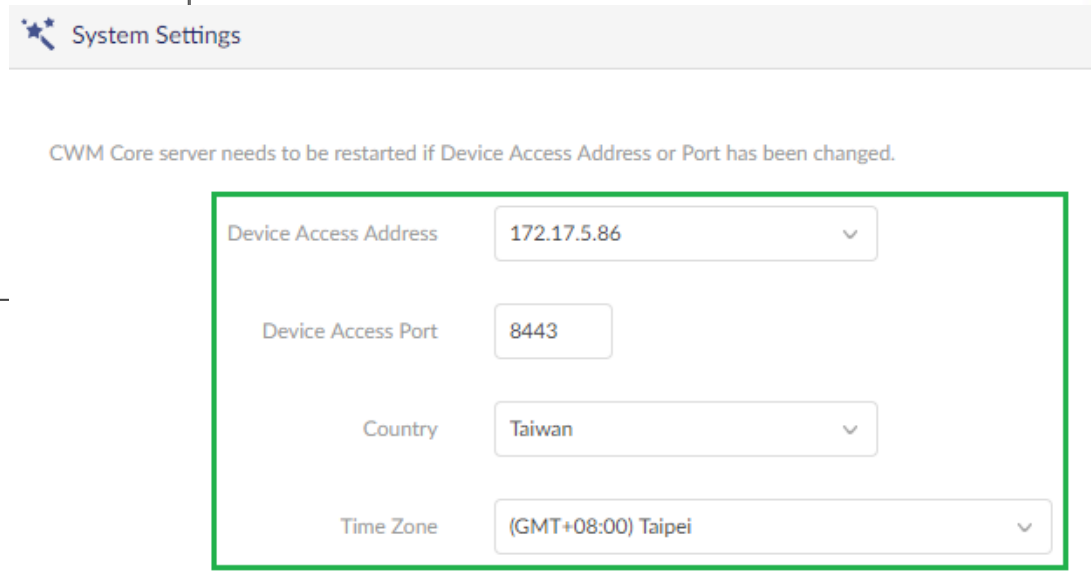




Nuclias Connect Setup Wizard (System Setting)

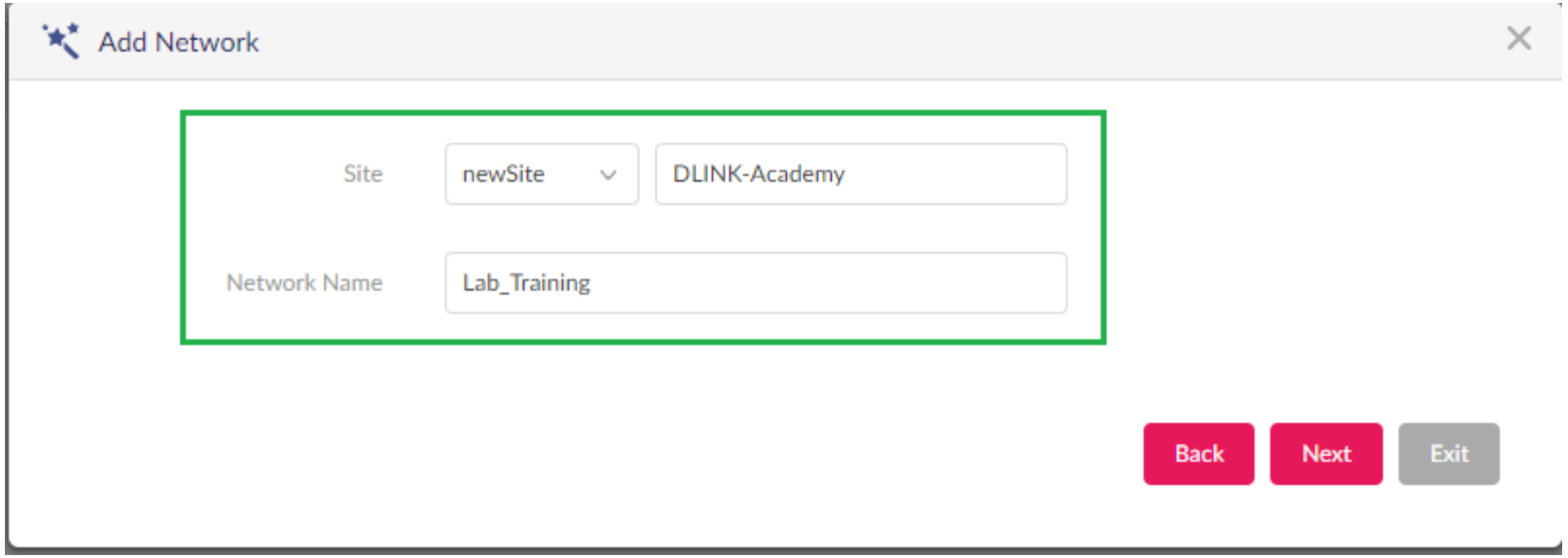
- During Nuclias Connect initial launch, we are requested to provide system settings.





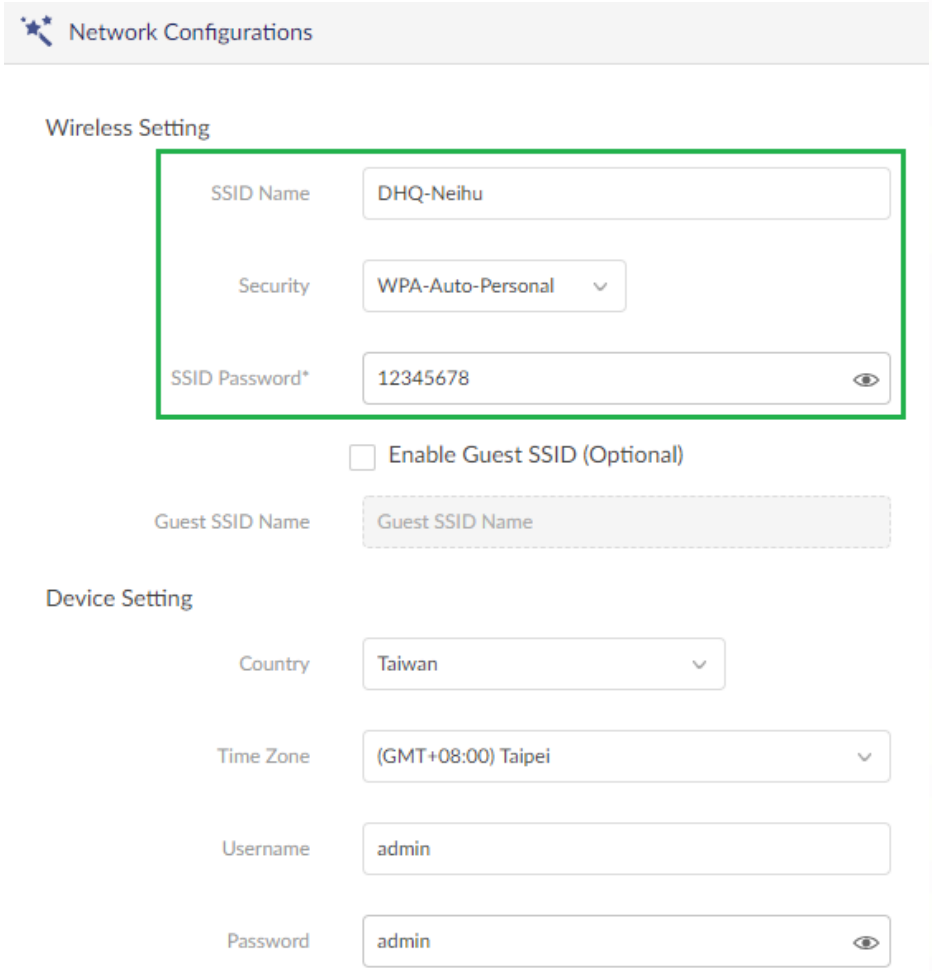
Nuclias Connect Setup Wizard (Network Setting)

- Site and Network is a multi-tenant architecture for business process, please key in meaningful definition.



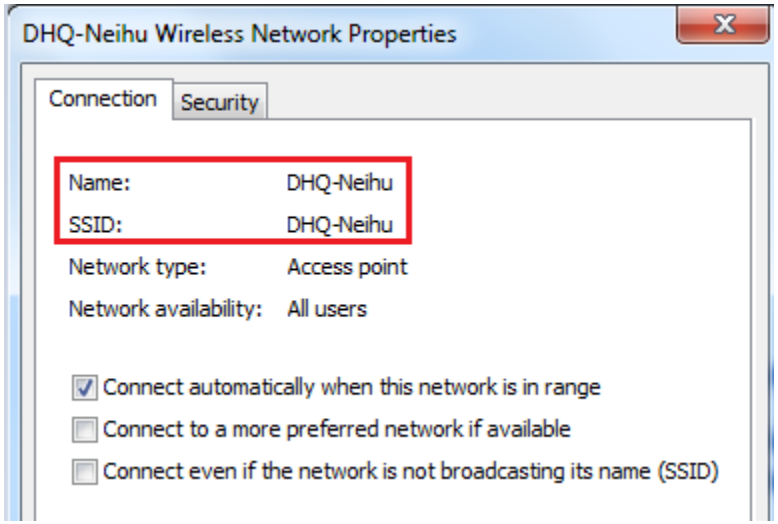
Nuclias Connect Setup Wizard (Network Setting)

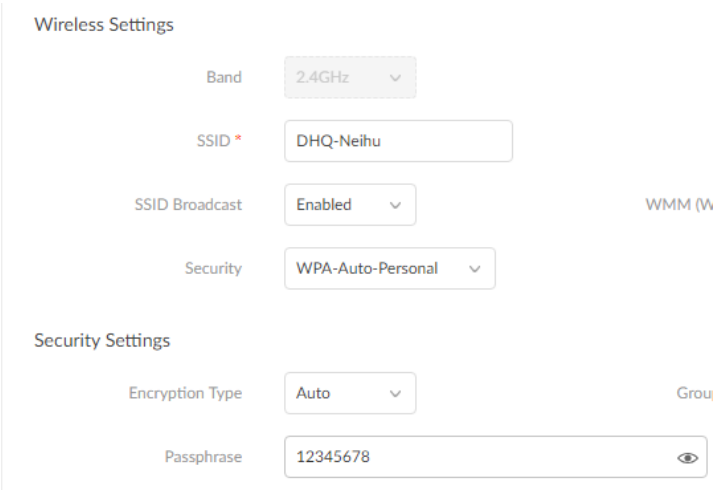
- SSID name is required in this configuration process
  - The default security uses “WPA-Auto-Personal”

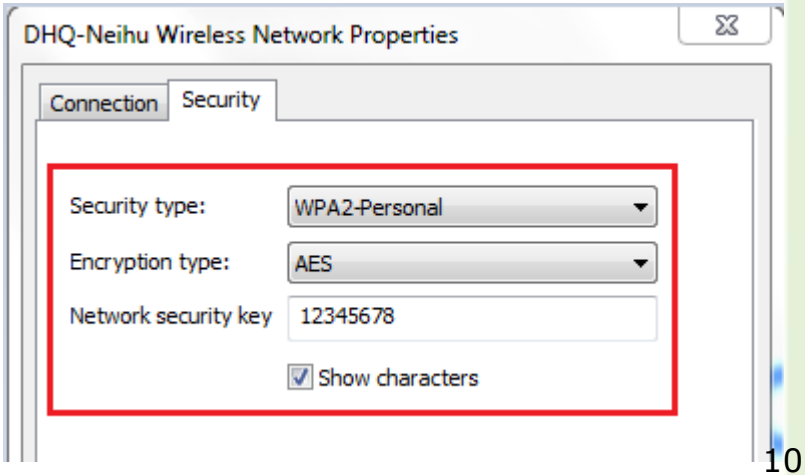


Wireless Client Connection

- With the above "WPA-AUTO-PERSONAL" security settings, when a wireless client attempts to make connection, please ensure proper wireless network properties configuration.







Nuclias Connect Configuration Profile

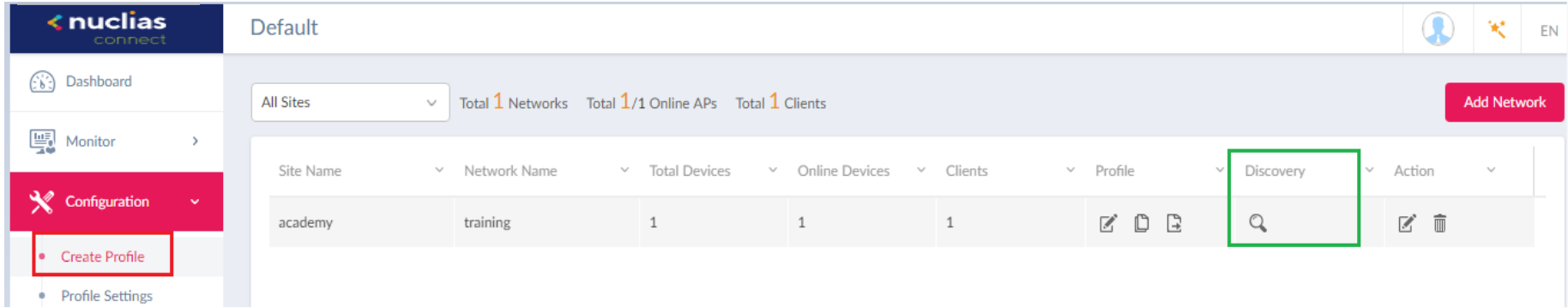
In Nuclias Connect, there are three ways to discover your DAP and push a DNC configuration profile into DAP devices, making it as an manageable device.

- AP Discovery Process and Import Network Profile [page, 104th ~ 109th]
  - Layer 2
  - Layer 3
- Network Profile Export [page, 113th ~ 116th]
- Mobile Application (iOS and Android) [page, 117th ~ 118th]

In a large DAP deployment, it is recommended to use static IPs on Nuclias Connect server and Access Points, instead of DHCP..

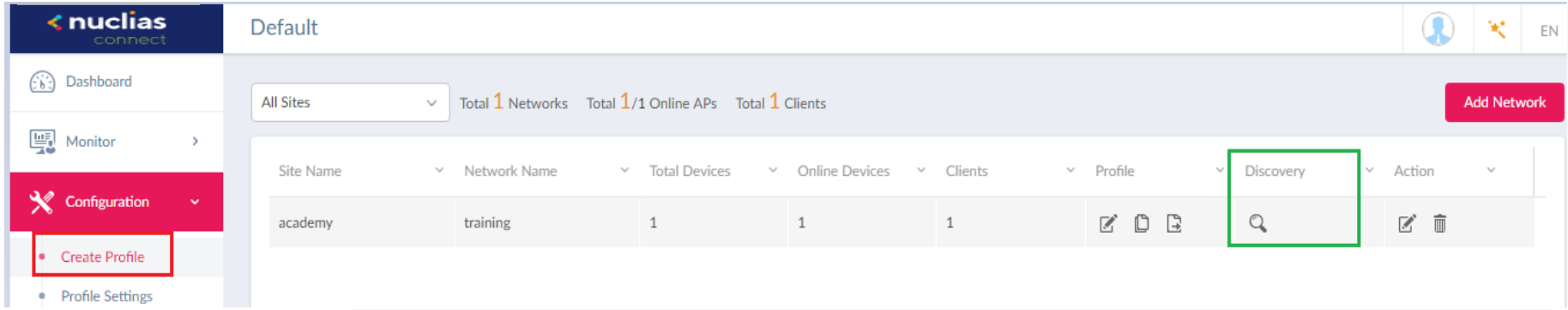
AP Discovery Process and Import Network Profile (1/6)

- Make sure the desired profile is ready to select
- Click “Discovery” icon in a specific profile

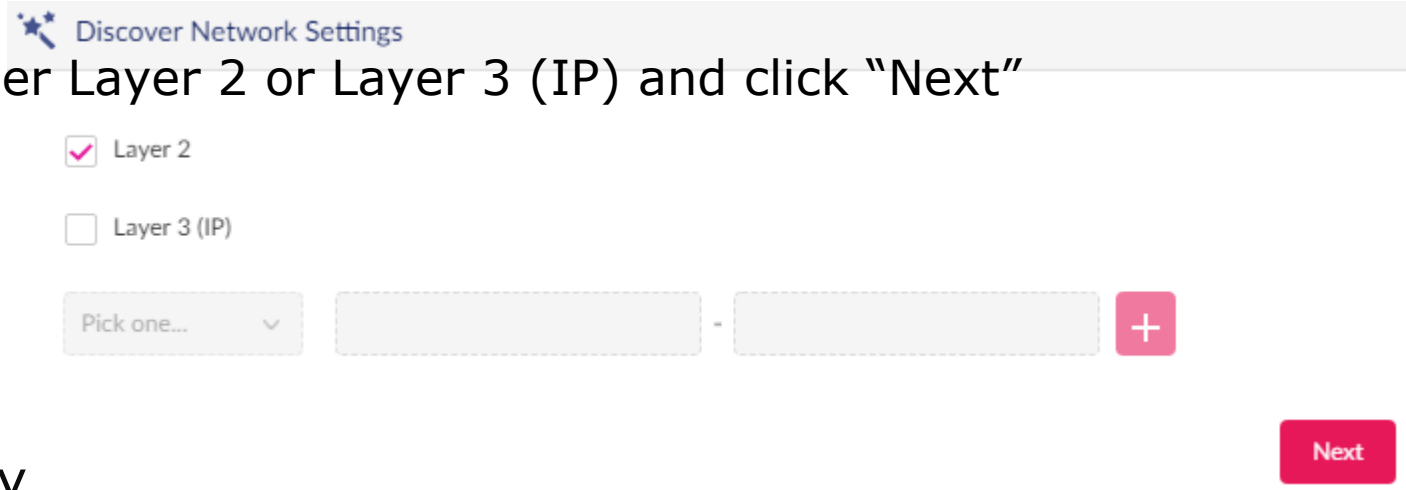


AP Discovery Process and Import Network Profile (2/6)

- Make sure the desired profile is ready to select
- Click “Discovery” icon in a specific profile

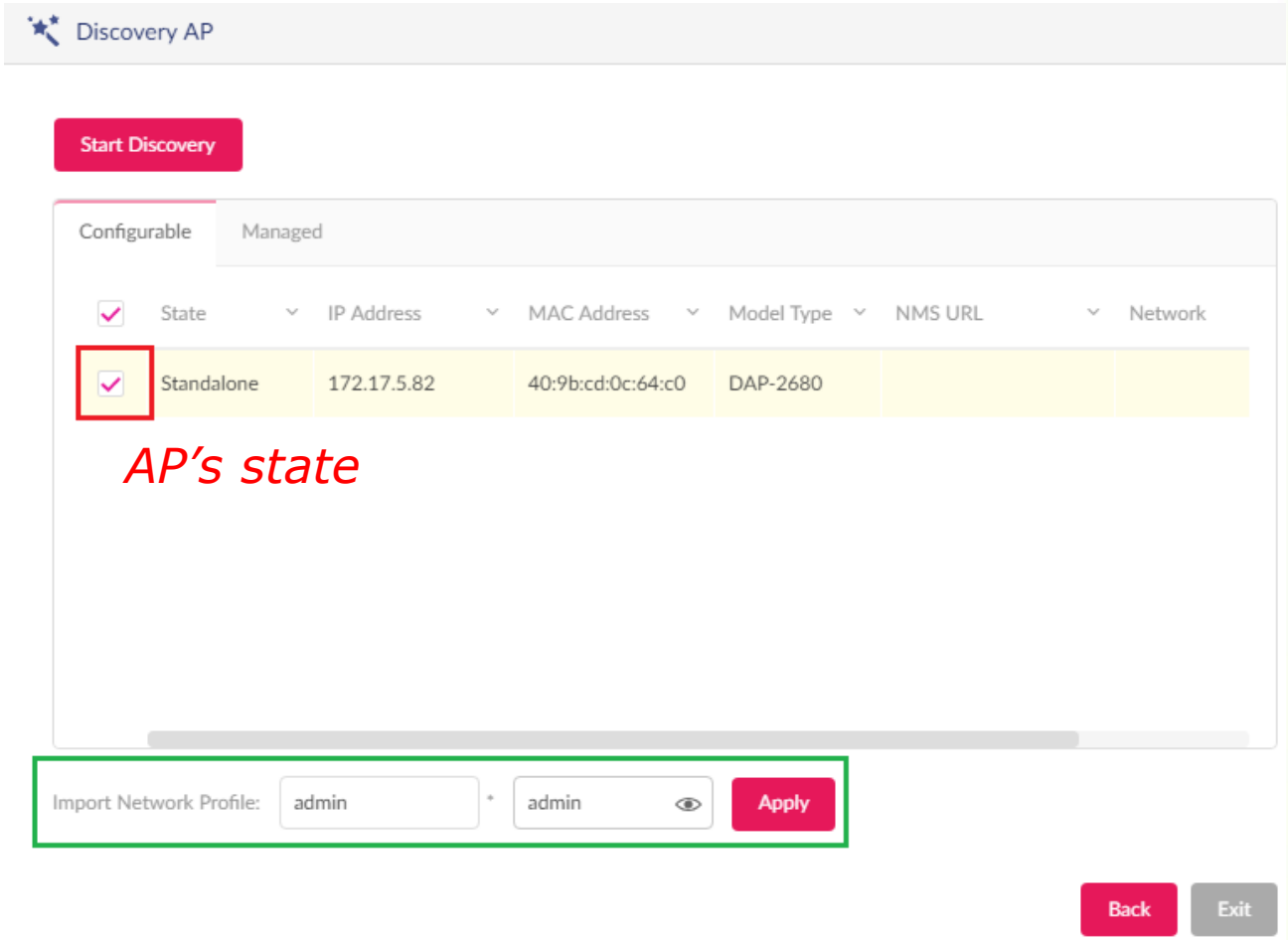


- Select either Layer 2 or Layer 3 (IP) and click “Next”



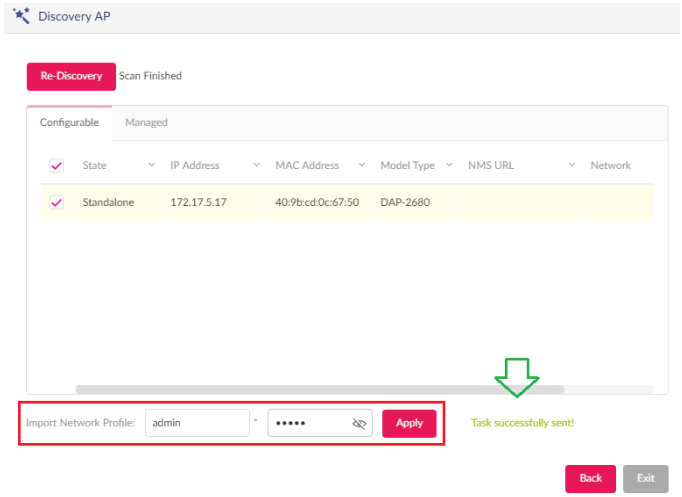
AP Discovery Process and Import Network Profile (3/6)

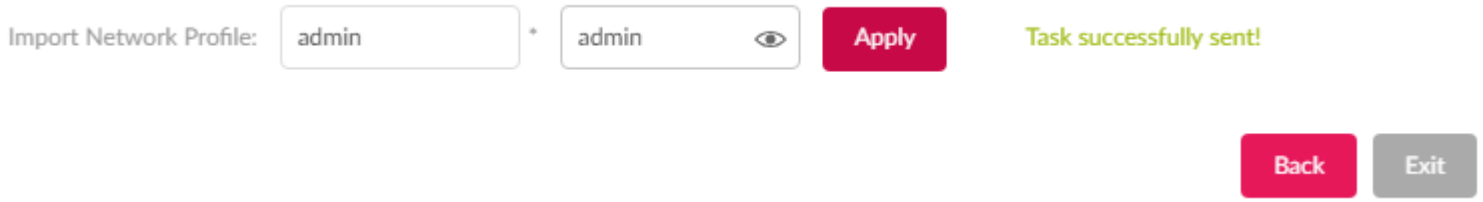
- Click "Start Discovery" button and input user ID/PWD
- Click Apply



AP Discovery Process and Import Network Profile (4/6)

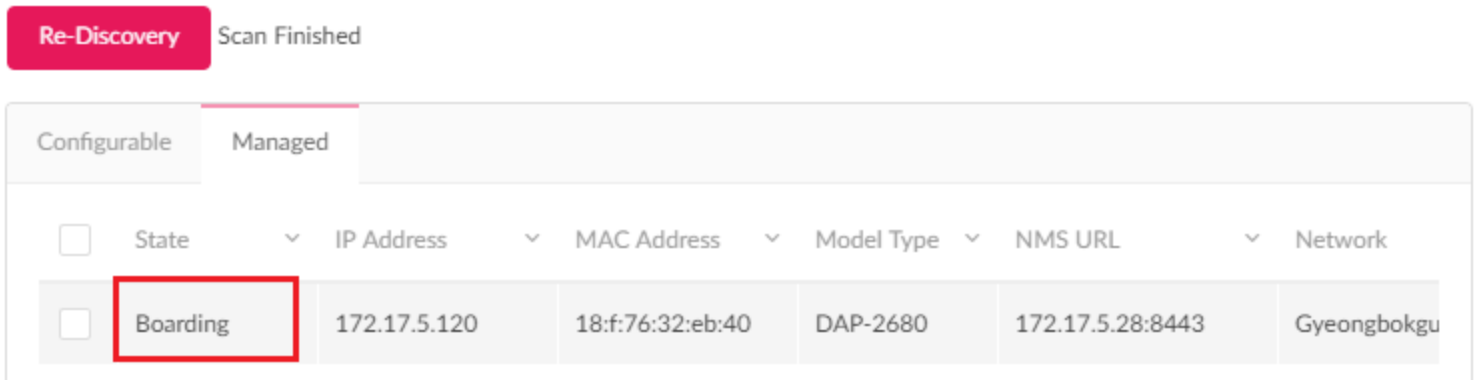
- Should the above task carries proper ID/PWD, then, “Task successfully sent!” message shall be displayed.

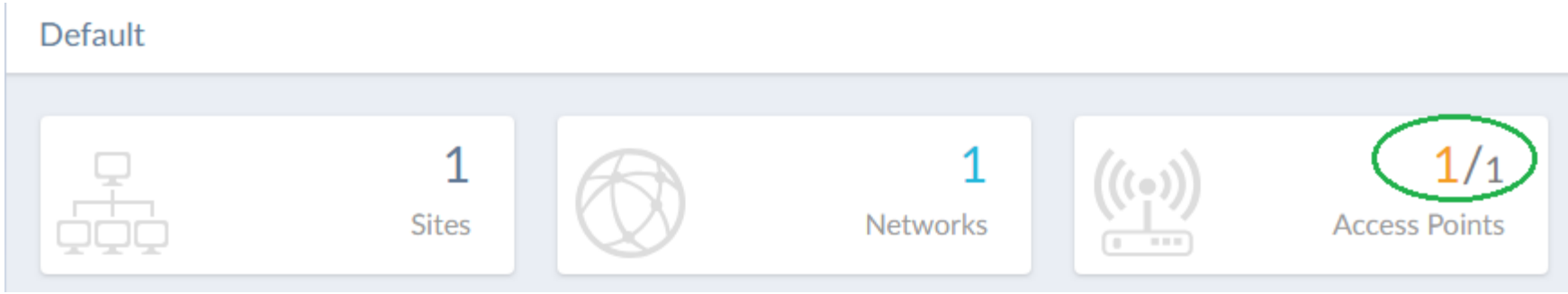




AP Discovery Process and Import Network Profile (5/6)

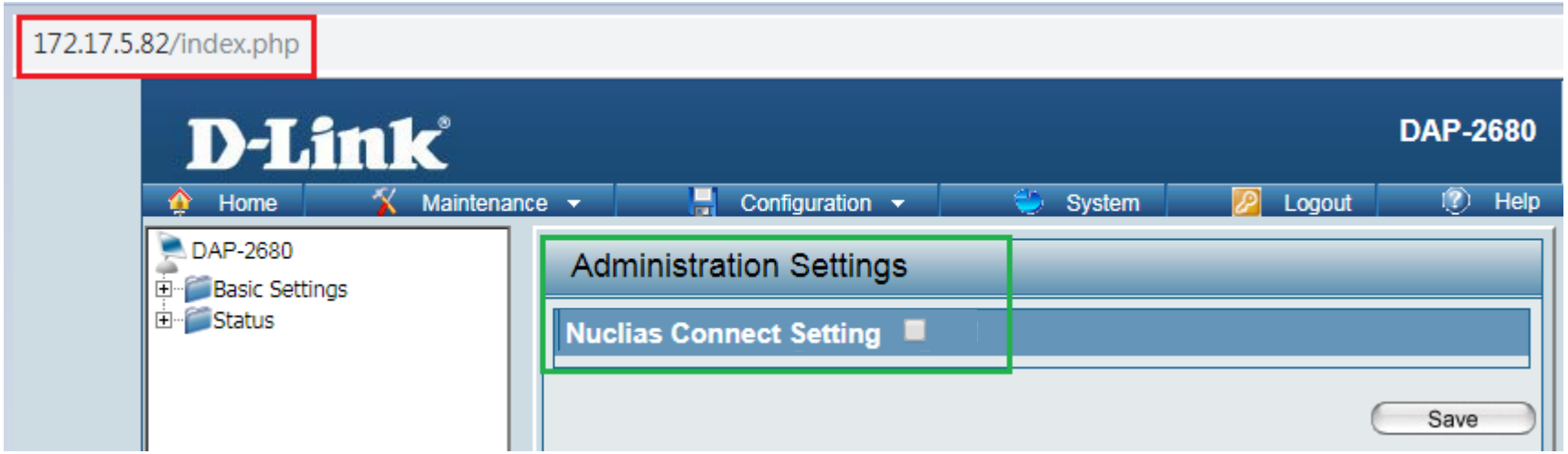
- Nuclias Connect Dashboard should reflect the latest managed AP status.





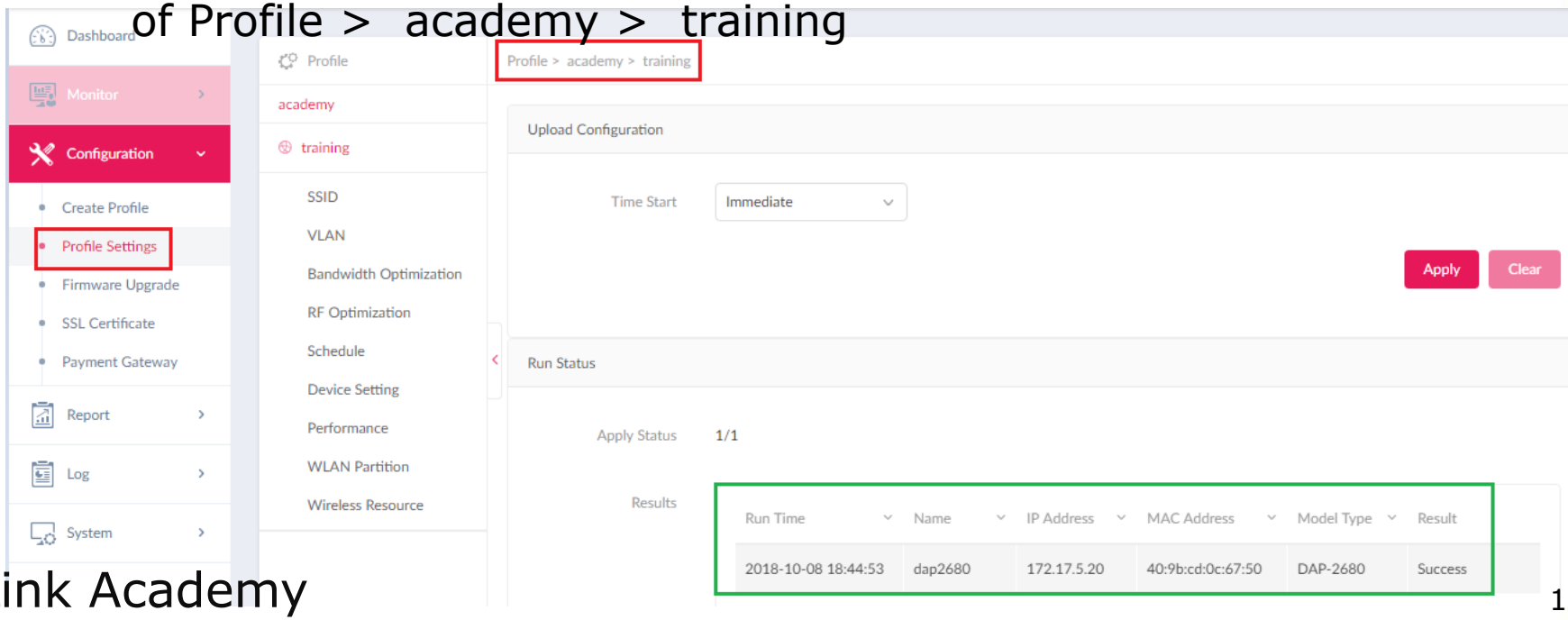
AP Discovery Process and Import Network Profile (6/6)

- DAP's local GUI also responds with a similar message.



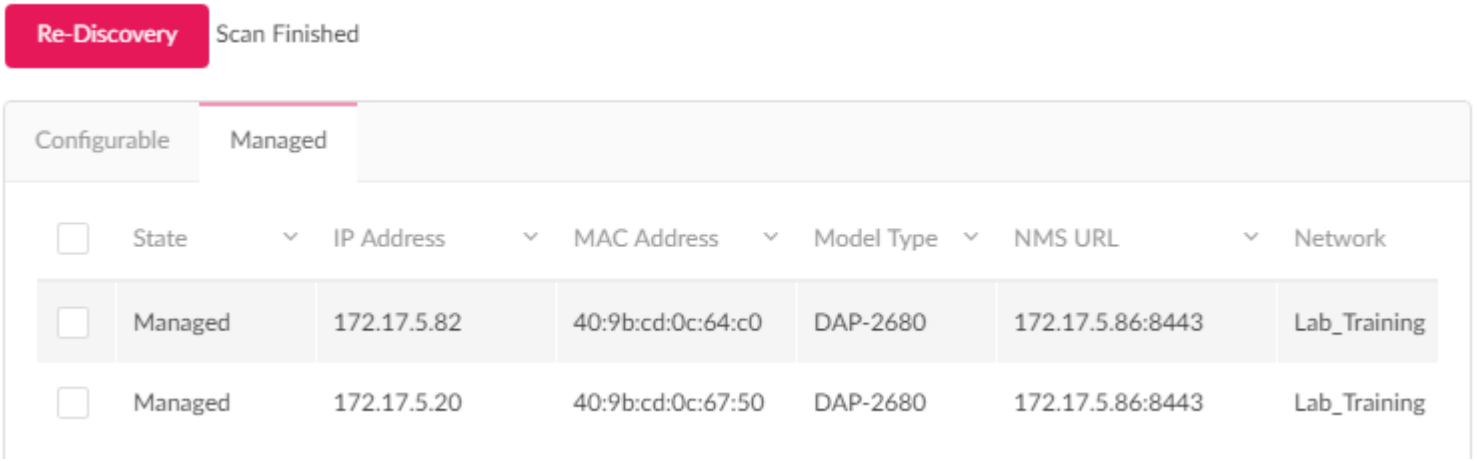
DAP Status Change (From Unregistered to Registered)

- From Unregistered to Registered
- Nuclias Connect Menu: Configuration > Profile Settings > Apply
- During the profile push, we should close look AP device status lighting in DNC, which should be from Orange to YellowGreen
  - To view "Apply Configuration" status, we can browse the menu of Profile > academy > training



Rerun AP Discovery Process

- The below image screen shot is another example of showing AP Discovery task and generated outcome.



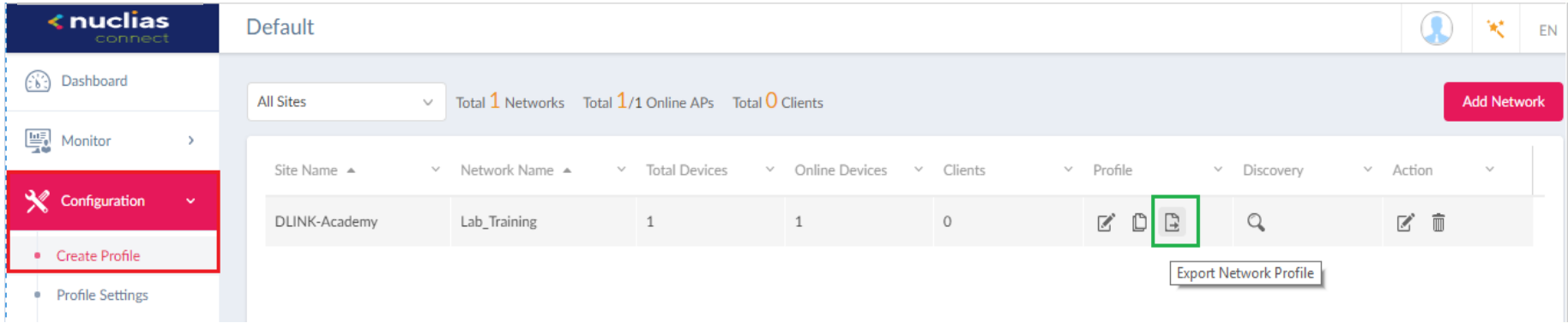
Device(s) are categorized as “Managed”

Type of AP Status, In The Management Process

- Type of AP status whether being managed by Nuclias Connect (DNC Web page)
  - 0: Not Managed (Standalone Mode)
  - 1: Unregistered
  - 2: Boarding
  - 3: Managed
  - 4: Unmanaged
- Type of AP status whether being managed by Nuclias Connect (in DAP GUI) [it is a logic concept, instead of physical connection]
  - 1: Connect
  - 2: Disconnect

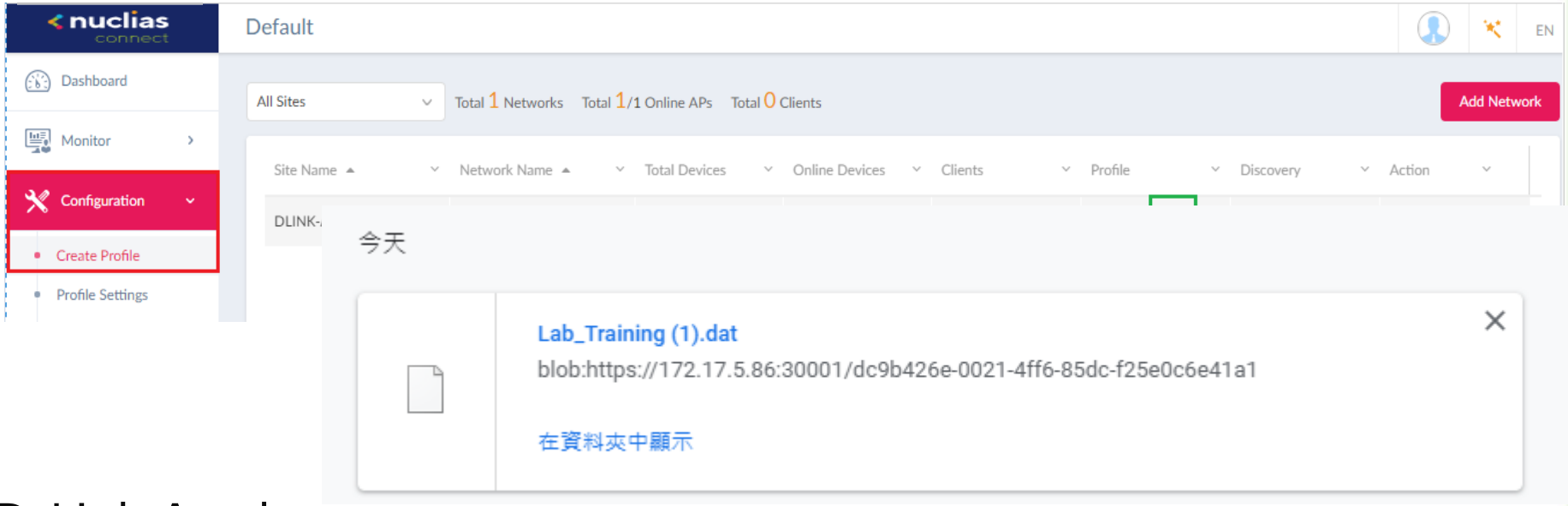
Nuclias Connect Network Profile Export (1/4)

- We could also manage our DAP with the method of "DNC Network Profile Export"
- Step 1: Menu: Configuration > Create Profile, select the "Site Name" we would like to export and then click the "Export Network Profile" button.
  - Our computer will place downloaded files in the default folder



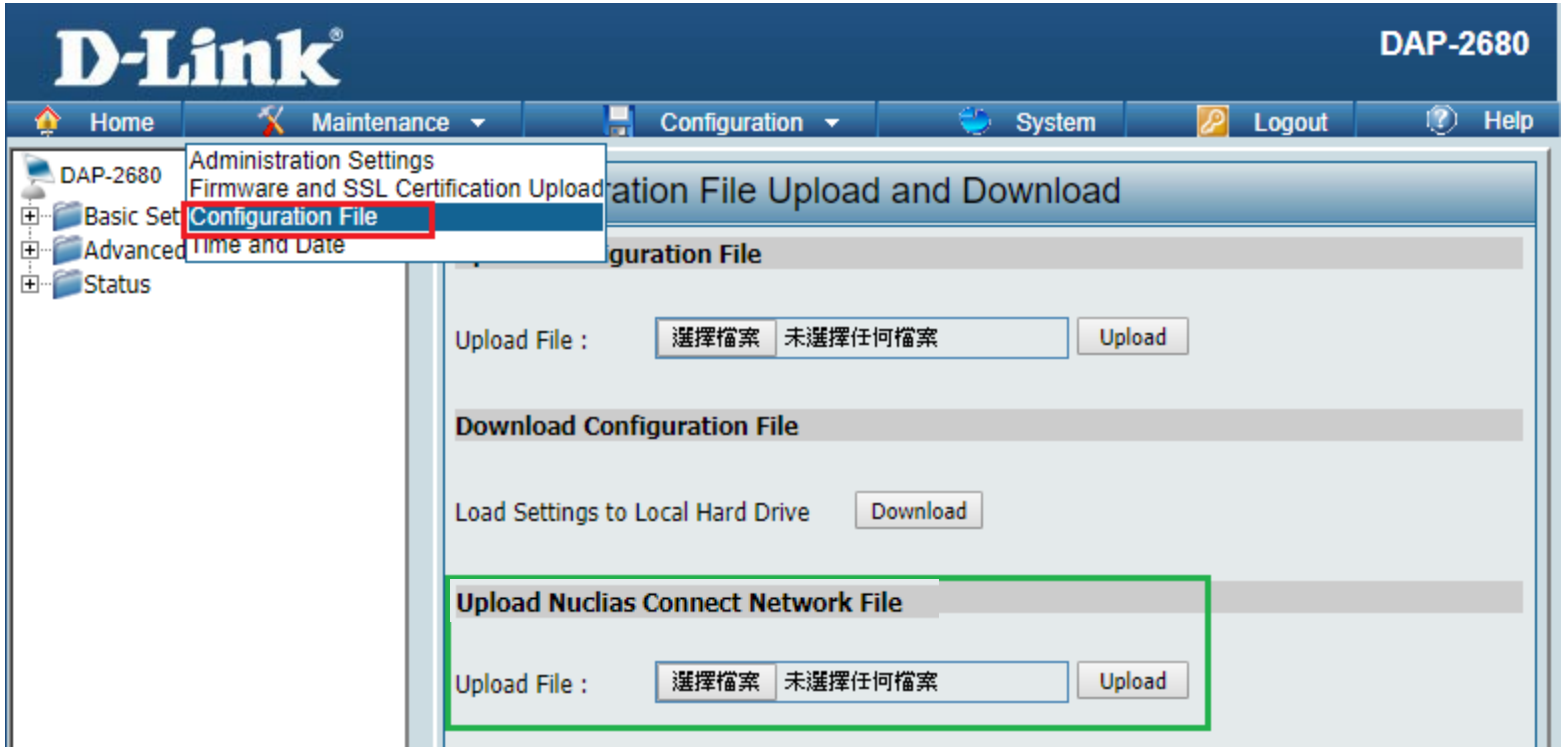
Nuclias Connect Network Profile Export (2/4)

- We could also manage our DAP with the method of "DNC Network Profile Export"
- Step 1: Menu: Configuration > Create Profile, select the "Site Name" we would like to export and then click the "Export Network Profile" button.
  - Our computer will place downloaded files in the default folder



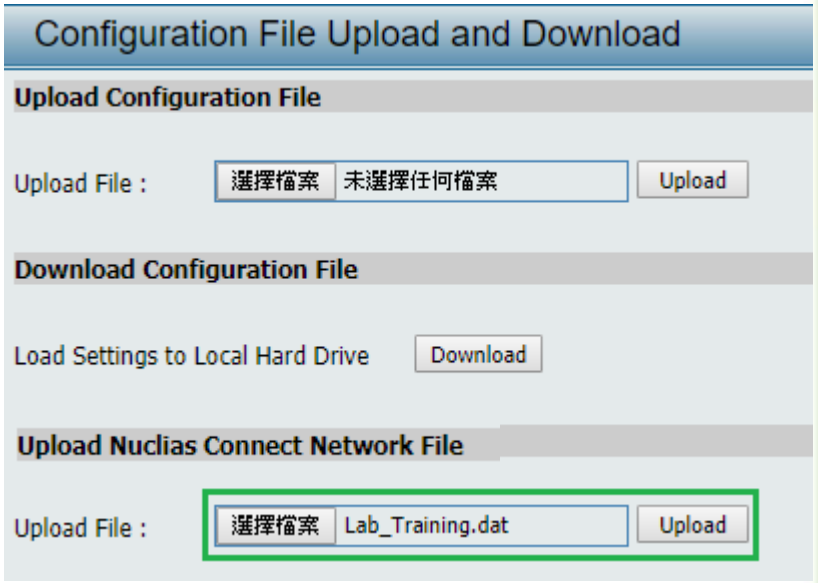
Nuclias Connect Network Profile Export (3/4)

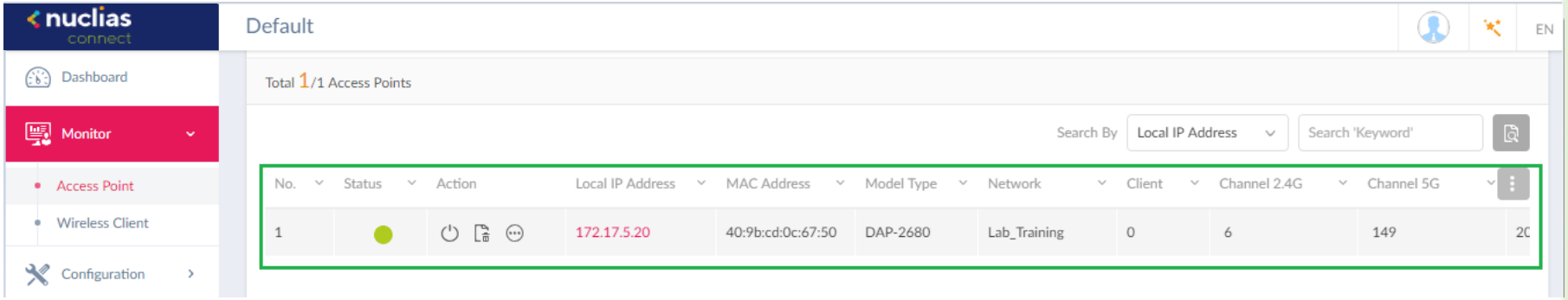
- Login DAP using Web GUI and browse the menu of “Maintenance” “Configuration File”
- Then, click the button of “Upload Nuclias Connect Network File”



Nuclias Connect Network Profile Export (4/4)

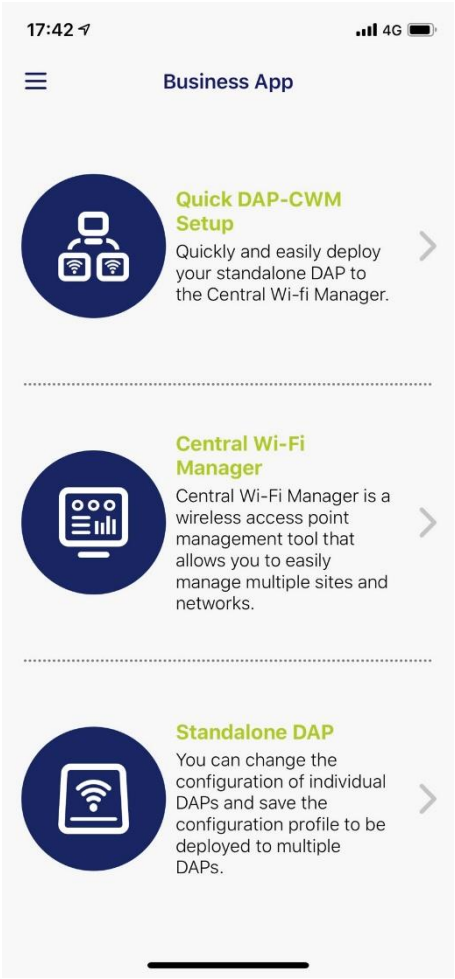
- Once that Network File is in place, then, place “Upload” button
  - Message: Load Setting File
- That DAP device should be displayed in DNC’s menu (Monitor > Access Point)

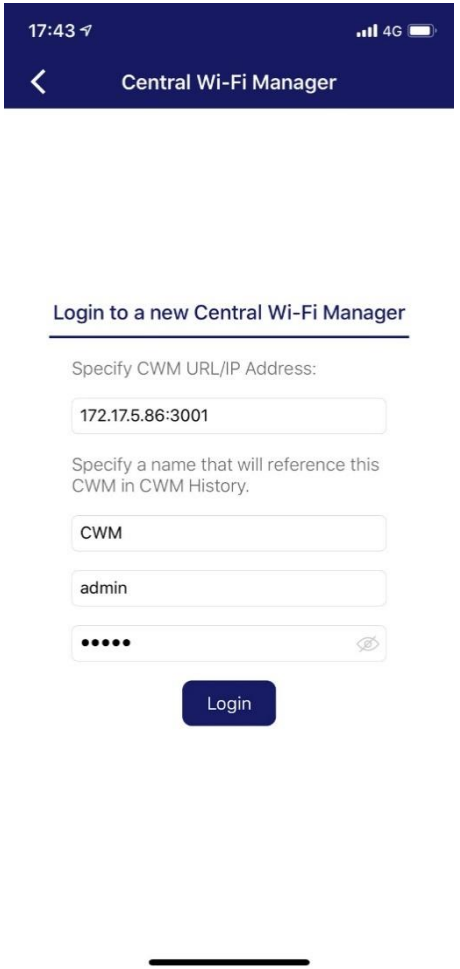




Mobile Application (iOS and Android)

- Mobile Application (iOS)

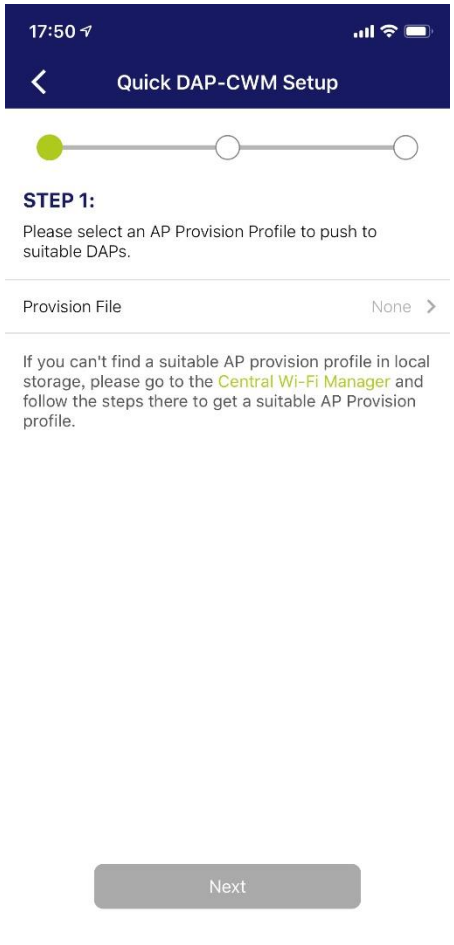




Mobile Application (iOS and Android)

- Mobile Application (iOS)

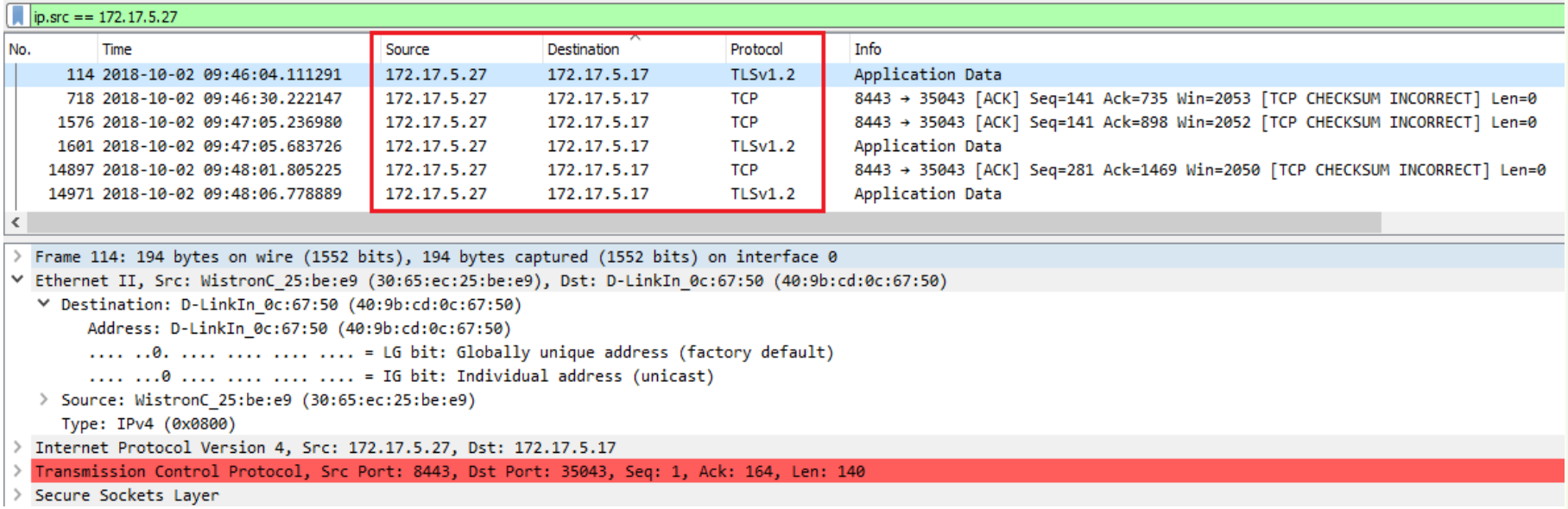
QDCS allows user to find APs and import profile for Nuclias Connect management quickly.





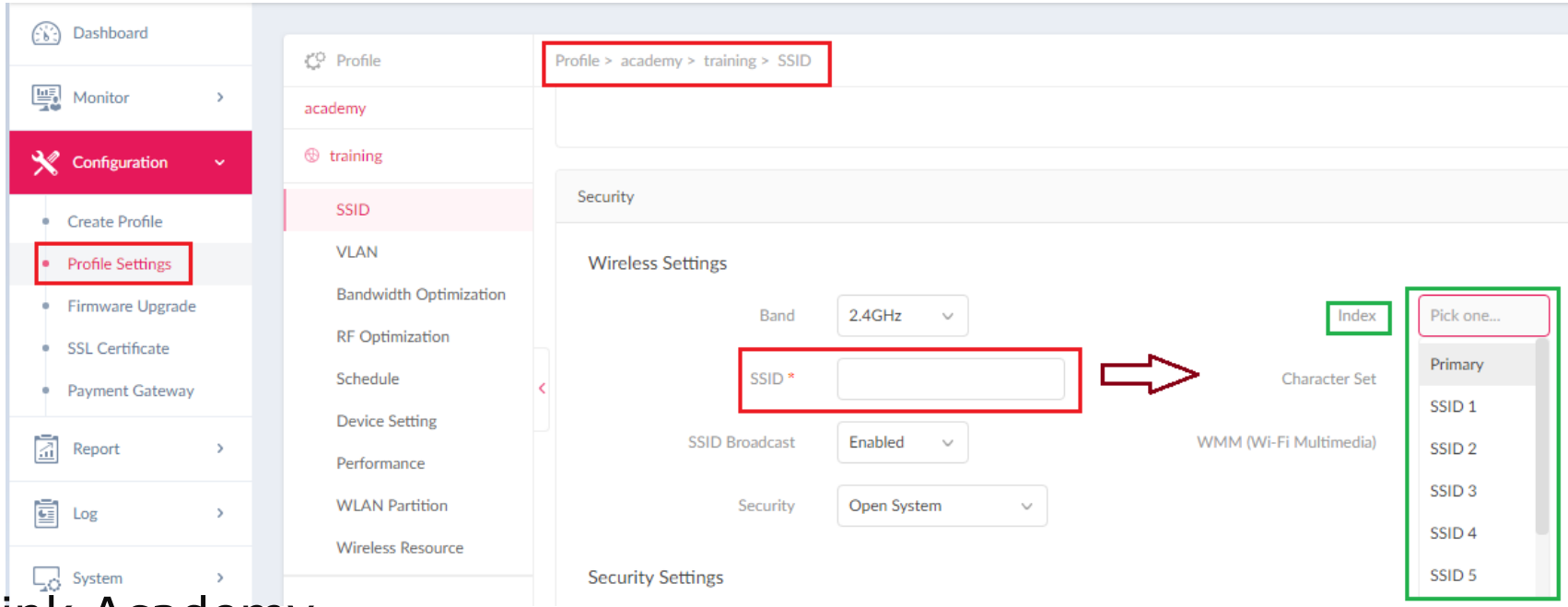
Nuclias Connect and DAP Communication

- Nuclias Connect (IP: 172.17.5.27) to DAP-2680 (IP: 172.17.5.17)
- Protocol: TLSv1.2 (application data)



Configuring SSIDs (1/6)

- We are given the right to configure up to 16 SSIDs on our access point and assign different configuration settings to each SSID.
- To create additional SSID, browse the menu of Configuration > Profile Settings > Profile > academy > training > SSID
- Input the SSID name and bind with proper SSID index



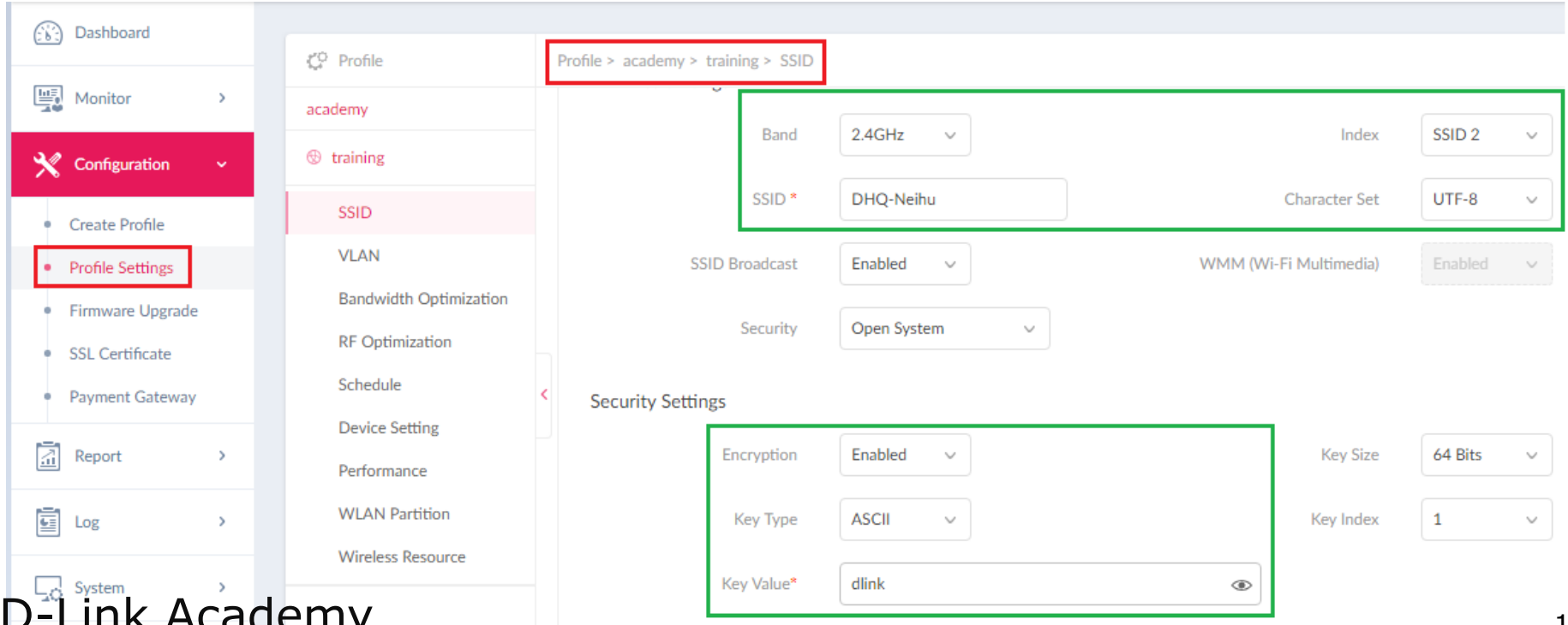
Configuring SSIDs (2/6)

- Configuration parameters
  - SSID: DHQ-Neihu, Index: SSID-2
  - Security Settings, Encryption: enabled; key value: dlink
  - Push Add button and apply a similar setting to 5GHz

- Note: General Deployment Guidelines
  - Make the SSID recognizable, but not enough to reflect identifiable information
  - Define a complex SSID naming convention, non-meaningful strings of characters (letters and numbers)
  - Consider one SSID per frequency band (pointing to the 5 GHz and 2.4 GHz frequency bands respectively)

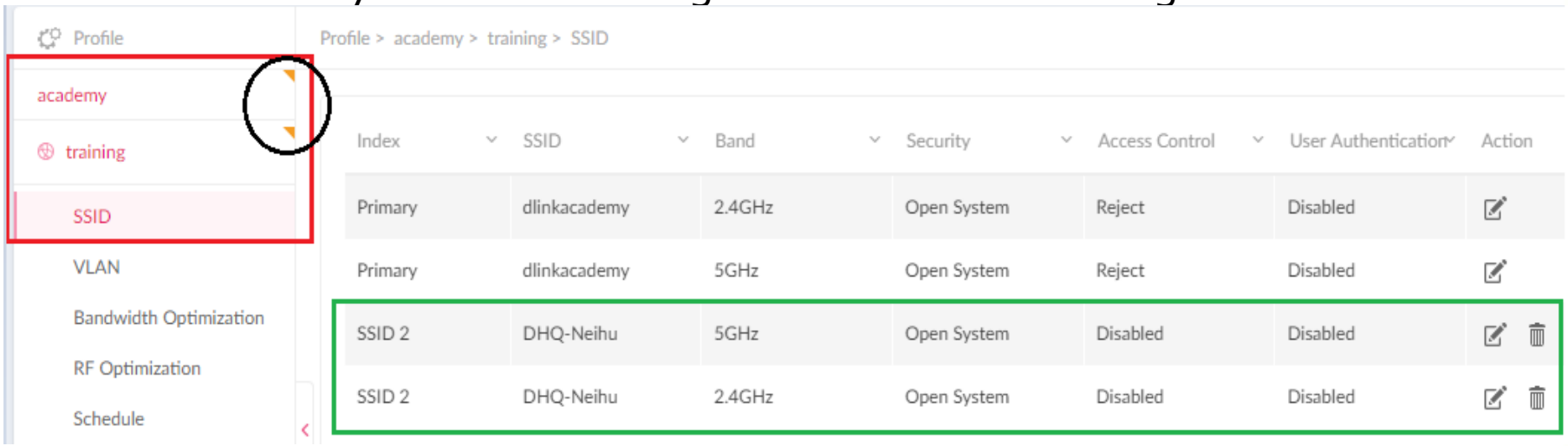
Configuring SSIDs (3/6)

- Configuration parameters
  - SSID: DHQ-Neihu, Index: SSID-2
  - Security Settings, Encryption: enabled; key value: dlink
  - Push Add button and apply a similar setting to 5GHz



Configuring SSIDs (4/6)

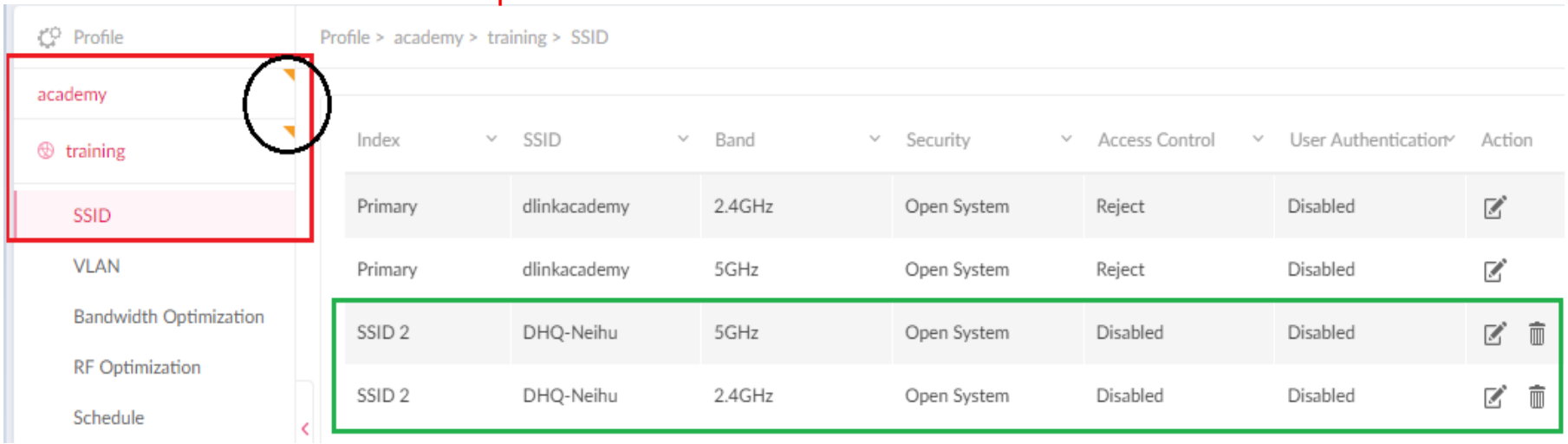
- 2nd SSID configuration verifications
- Menu: Configuration > Profile Setting > Profile > academy > training > SSID
  - Arrow symbols indicating modification of configurations



Configuring SSIDs (4/6)

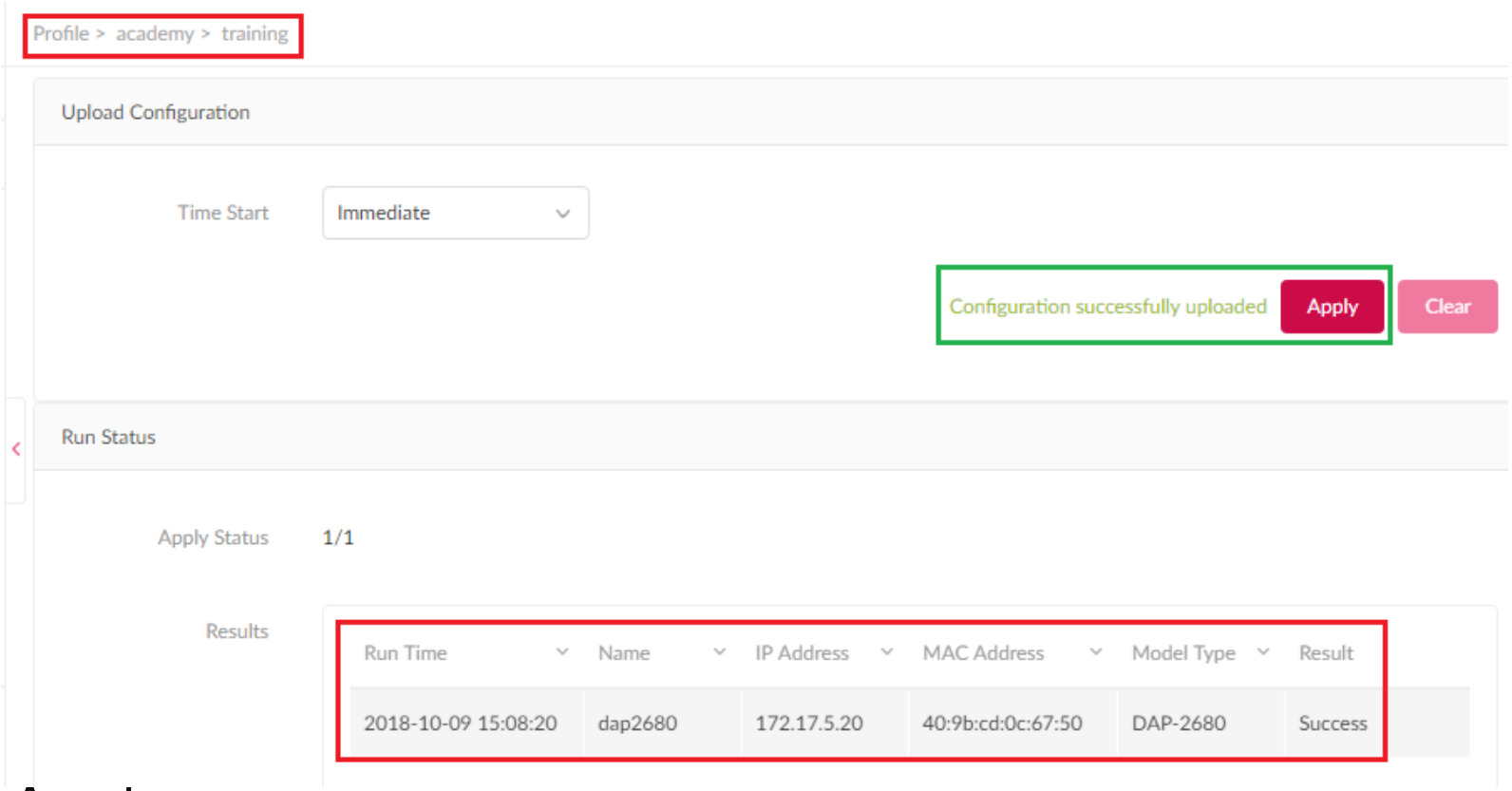
- 2nd SSID configuration verifications
- Menu: Configuration > Profile Setting > Profile > academy > training > SSID
  - Arrow symbols indicating modification of configurations

In DNC official release, a friendly reminder message similar like "configuration needs to upload" will be added.



Configuring SSIDs (5/6)

- 2nd SSID configuration verifications
- DNC message: Configuration successfully uploaded



Configuring SSIDs (6/6)

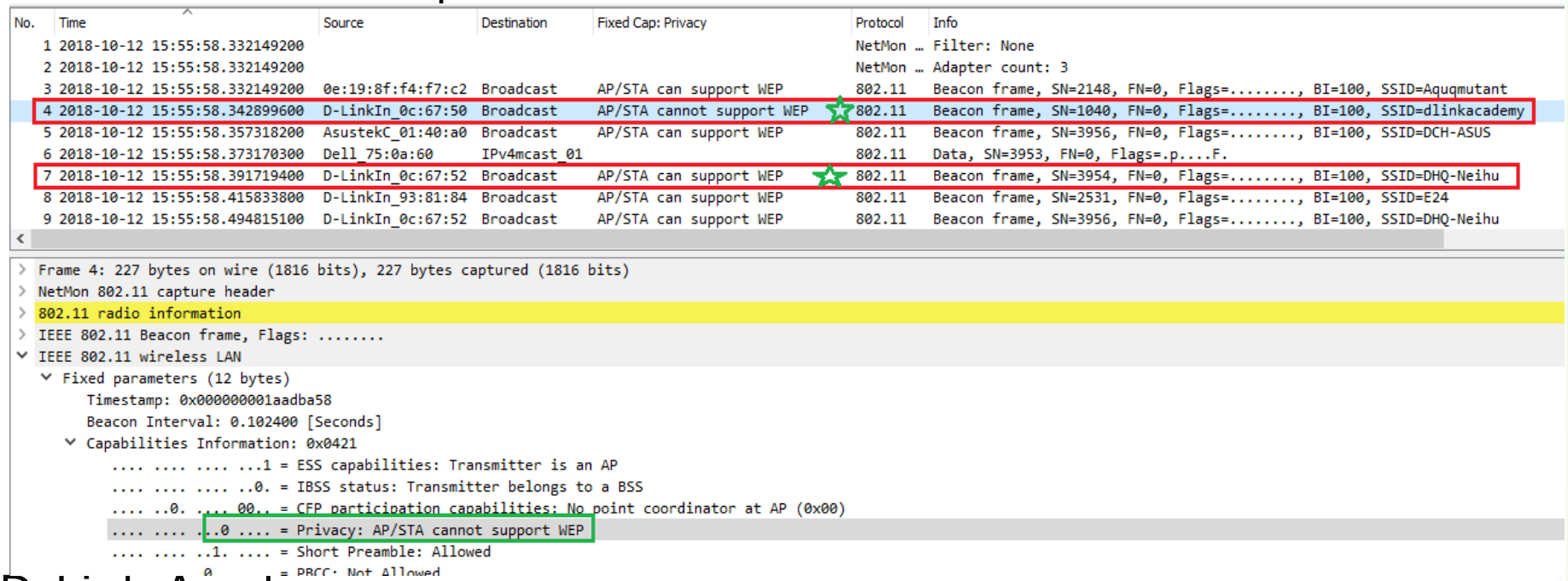
- 2nd SSID configuration verifications
- Wireless client connection

No.	Time	Source	Destination	Protocol	Info
108134	2018-10-09 15:09:36.308780200	D-LinkIn_0c:67:52	Broadcast	802.11	Beacon frame, SN=832, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
108142	2018-10-09 15:09:36.411622300	D-LinkIn_0c:67:52	Broadcast	802.11	Beacon frame, SN=833, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
108161	2018-10-09 15:09:36.590962400	D-LinkIn_0c:67:52	IntelCor_a9:52:ec	802.11	Probe Response, SN=835, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
108162	2018-10-09 15:09:36.592562200	D-LinkIn_0c:67:52	IntelCor_a9:52:ec	802.11	Probe Response, SN=836, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
108164	2018-10-09 15:09:36.616045000	D-LinkIn_0c:67:52	Broadcast	802.11	Beacon frame, SN=837, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
108167	2018-10-09 15:09:36.634785800	D-LinkIn_0c:67:52	IntelCor_a9:52:ec	802.11	Probe Response, SN=838, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
108190	2018-10-09 15:09:36.742852500	D-LinkIn_0c:67:52	IntelCor_a9:52:ec	802.11	Authentication, SN=256, FN=0, Flags=........
108192	2018-10-09 15:09:36.751776700	D-LinkIn_0c:67:52	IntelCor_a9:52:ec	802.11	Association Response, SN=257, FN=0, Flags=....R...
108215	2018-10-09 15:09:36.923219900	D-LinkIn_0c:67:52	Broadcast	802.11	Beacon frame, SN=852, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
108221	2018-10-09 15:09:37.025564000	D-LinkIn_0c:67:52	Broadcast	802.11	Beacon frame, SN=856, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu

No.	Time	Source	Destination	Protocol	Info
108188	2018-10-09 15:09:36.733668400	D-LinkIn_ac:1e:58	Broadcast	802.11	Beacon frame, SN=98, FN=0, Flags=........, BI=100, SSID=dlink-1E56
108189	2018-10-09 15:09:36.737030300	D-LinkIn_77:01:80	Broadcast	802.11	Beacon frame, SN=2196, FN=0, Flags=........, BI=100, SSID=TSD-V12-5G
108190	2018-10-09 15:09:36.742852500	D-LinkIn_0c:67:52	IntelCor_a9:52:ec	802.11	Authentication, SN=256, FN=0, Flags=........
108191	2018-10-09 15:09:36.750296000	D-LinkIn_e4:70:10	Broadcast	802.11	Beacon frame, SN=2465, FN=0, Flags=........, BI=100, SSID=D-Link_2G
108192	2018-10-09 15:09:36.751776700	D-LinkIn_0c:67:52	IntelCor_a9:52:ec	802.11	Association Response, SN=257, FN=0, Flags=....R..
108193	2018-10-09 15:09:36.762589300	D-LinkIn_a8:05:c0	Broadcast	802.11	Beacon frame, SN=987, FN=0, Flags=........, BI=100, SSID=dlink
108194	2018-10-09 15:09:36.766535500	D-LinkIn_5c:6b:f0	Broadcast	802.11	Beacon frame, SN=1534, FN=0, Flags=........, BI=100, SSID=cameratestlabWPS
108195	2018-10-09 15:09:36.772374600	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xa28f84f4
108196	2018-10-09 15:09:36.783429000	D-LinkIn_3c:fb:c6	Broadcast	802.11	Beacon frame, SN=2977, FN=0, Flags=........, BI=100, SSID=895L- testing
108197	2018-10-09 15:09:36.798916400	D-LinkIn_f9:cf:00	Broadcast	802.11	Beacon frame, SN=3910, FN=0, Flags=........, BI=100, SSID=---smtptestspeed

WEP Privacy Displayed in Wireshark Capture

- The privacy field under "Capabilities Information" of "IEEE 802.11 wireless LAN" describes whether encryption type (WEP) being enabled.
  - With the above configuration, the below image diagram making a visible explanation.

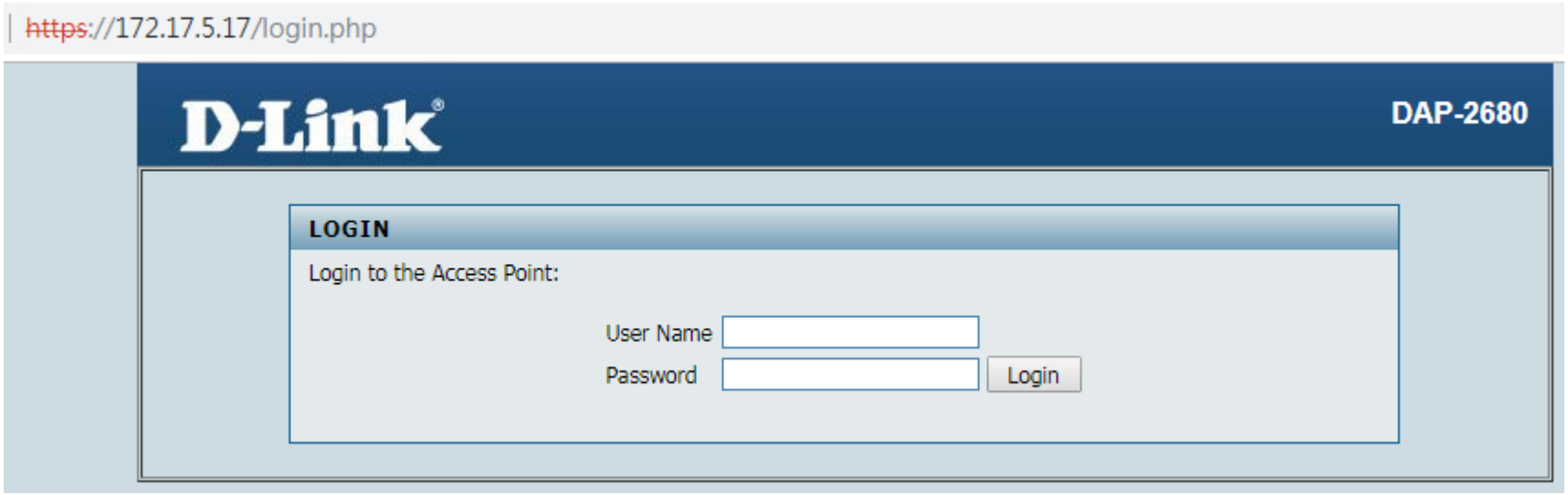


No.	Time	Source	Destination	Fixed Cap: Privacy	Protocol	Info
1	2018-10-12 15:55:58.332149200				NetMon …	Filter: None
2	2018-10-12 15:55:58.332149200				NetMon …	Adapter count: 3
3	2018-10-12 15:55:58.332149200	0e:19:8f:f4:f7:c2	Broadcast	AP/STA can support WEP	802.11	Beacon frame, SN=2148, FN=0, Flags=........, BI=100, SSID=Aquqmutant
4	2018-10-12 15:55:58.342899600	D-LinkIn_0c:67:50	Broadcast	AP/STA cannot support WEP	802.11	Beacon frame, SN=1040, FN=0, Flags=........, BI=100, SSID=dlinkacademy
5	2018-10-12 15:55:58.357318200	AsustekC_01:40:a0	Broadcast	AP/STA can support WEP	802.11	Beacon frame, SN=3956, FN=0, Flags=........, BI=100, SSID=DCH-ASUS
6	2018-10-12 15:55:58.373170300	Dell_75:0a:60	IPv4mcast_01		802.11	Data, SN=3953, FN=0, Flags=.p....F.
7	2018-10-12 15:55:58.391719400	D-LinkIn_0c:67:52	Broadcast	AP/STA can support WEP	802.11	Beacon frame, SN=3954, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu
8	2018-10-12 15:55:58.415833800	D-LinkIn_93:81:84	Broadcast	AP/STA can support WEP	802.11	Beacon frame, SN=2531, FN=0, Flags=........, BI=100, SSID=E24
9	2018-10-12 15:55:58.494815100	D-LinkIn_0c:67:52	Broadcast	AP/STA can support WEP	802.11	Beacon frame, SN=3956, FN=0, Flags=........, BI=100, SSID=DHQ-Neihu

```
> Frame 4: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits)
> NetMon 802.11 capture header
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 wireless LAN
  v Fixed parameters (12 bytes)
      Timestamp: 0x000000001aadba58
      Beacon Interval: 0.102400 [Seconds]
    v Capabilities Information: 0x0421
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..1. .... = Short Preamble: Allowed
        0... .... .... .... = PBCC: Not Allowed
```

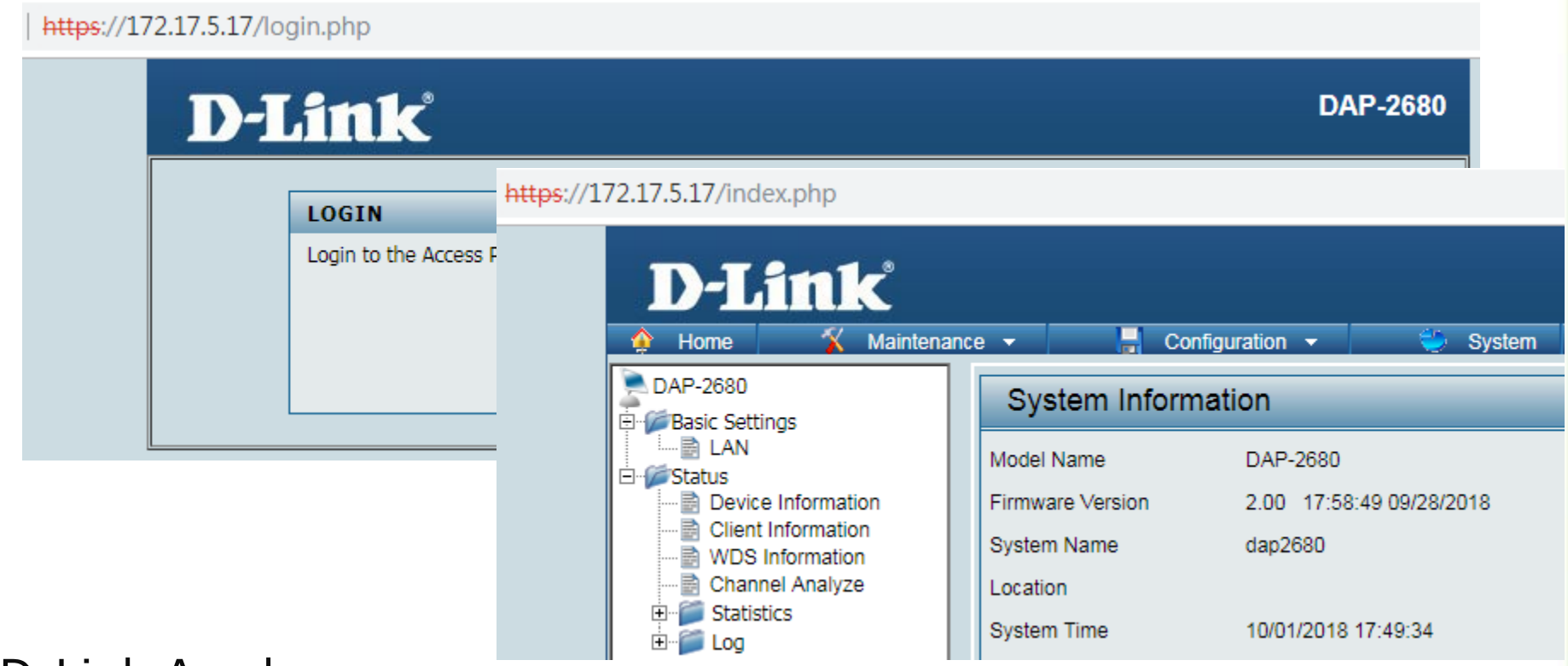
Managed AP, Local GUI Login (1/2)

- Laboratory Network Topology
  - Once an AP being managed by DNC. It is able to be access by GUI, with limited management function



Managed AP, Local GUI Login (2/2)

- Laboratory Network Topology
  - Once an AP being managed by DNC. It is able to be access by GUI, with limited management function

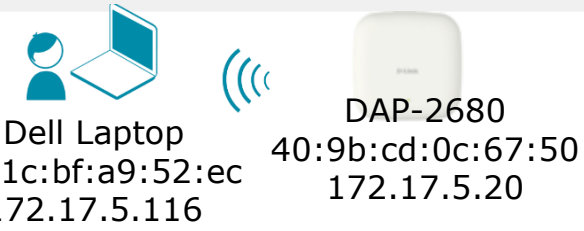


Probe Response Frame

- Probe Response Frame, from DAP-2680 (MAC: 40:9b:cd:0c:67:50) to Wireless Client (MAC: 00:1c:bf:a9:52:ec)

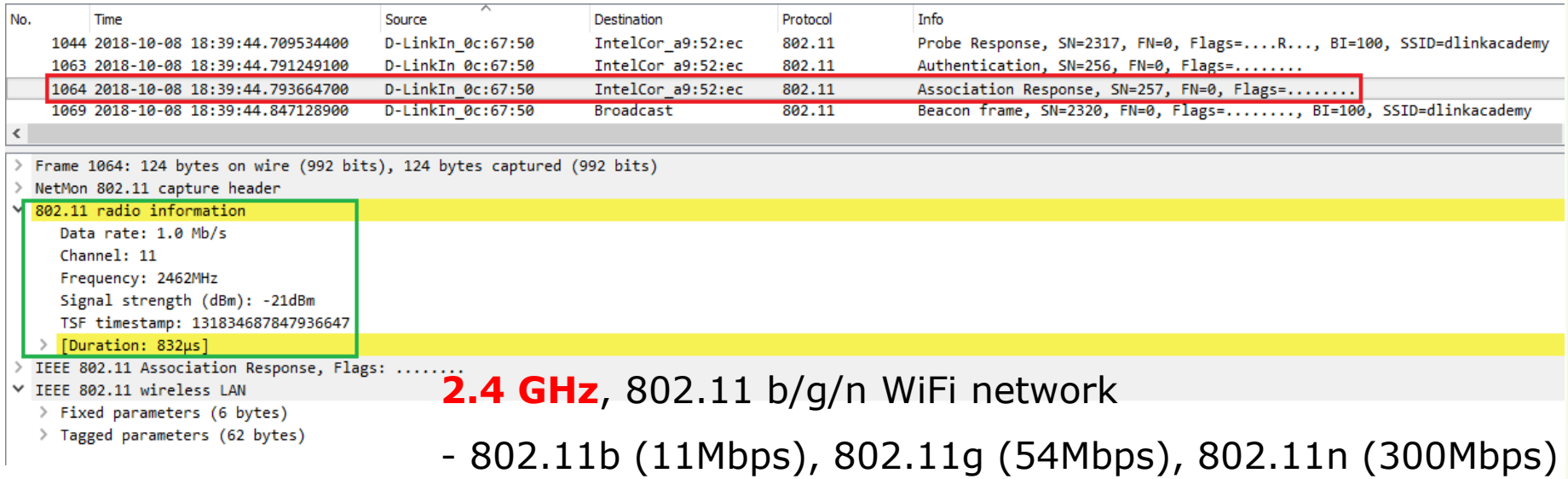
No.	Time	Source	Destination	Protocol	Info
75933	2018-10-02 10:05:31.004809400	D-LinkIn_0c:67:50	IntelCor_a9:52:ec	802.11	Probe Response, SN=933, FN=0, Flags=........, BI=100, SSID=dlinkacademy
75934	2018-10-02 10:05:31.009949800	D-LinkIn_0c:67:50	Broadcast	802.11	Beacon frame, SN=932, FN=0, Flags=........, BI=100, SSID=dlinkacademy
75935	2018-10-02 10:05:31.012004500	D-LinkIn_0c:67:50	IntelCor_a9:52:ec	802.11	Probe Response, SN=934, FN=0, Flags=........, BI=100, SSID=dlinkacademy

```
> Frame 75933: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits)
> NetMon 802.11 capture header
> 802.11 radio information
v IEEE 802.11 Probe Response, Flags: ........
    Type/Subtype: Probe Response (0x0005)
  > Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_a9:52:ec (00:1c:bf:a9:52:ec)
    Destination address: IntelCor_a9:52:ec (00:1c:bf:a9:52:ec)
    Transmitter address: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    Source address: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    BSS Id: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    .... .... .... 0000 = Fragment number: 0
    0011 1010 0101 .... = Sequence number: 933
> IEEE 802.11 wireless LAN
```



Association Response Frame

- IEEE 802.11 Wireless LAN, Management Frame, Association Response
- From Wireless AP (DAP) to wireless station (Dell laptop in our lab)
  - Band, 2.4GHz; channel, 11



2.4 GHz, 802.11 b/g/n WiFi network

- 802.11b (11Mbps), 802.11g (54Mbps), 802.11n (300Mbps)

5 GHz, 802.11 a/n/ac WiFi network

- 802.11a (54Mbps), 802.11ac (1 Gbps)

Wireless Client Getting An IP Address (1/4)

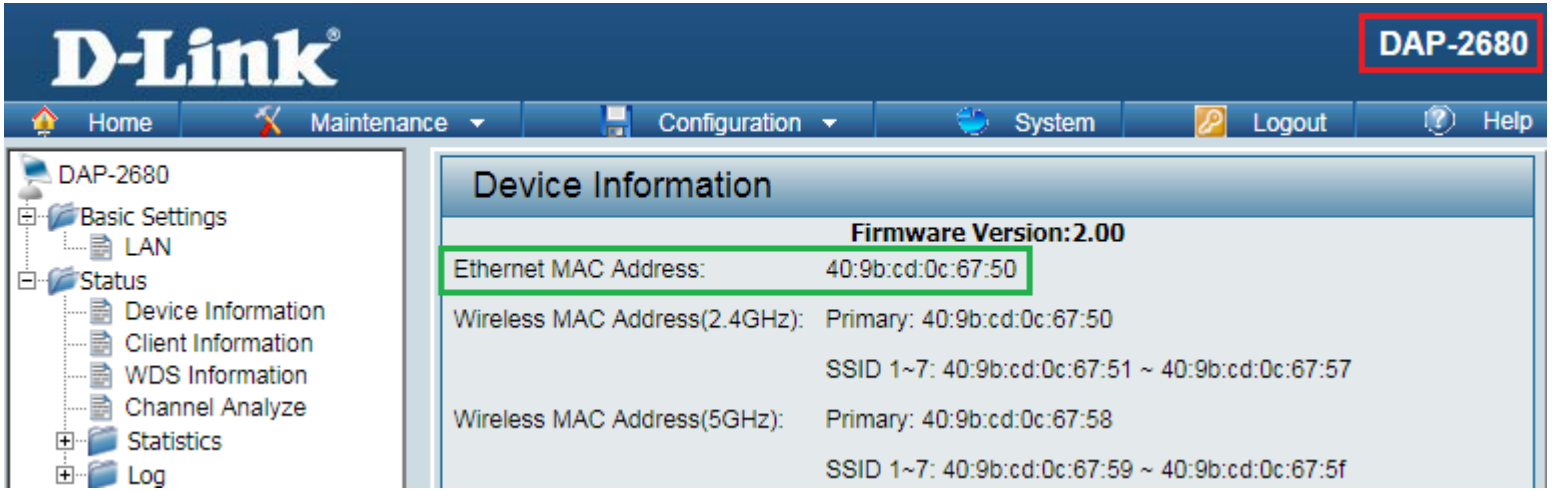
- Wireless station requests for DHCP IP (DHCP Inform)
  - Receiver address: 40:9b:cd:0c:67:50
  - Transmitter address: 00:1c:bf:a9:52:ec

No.	Time	Source	Destination	Protocol	Info
2236	2018-10-08 18:39:50.223252100	D-LinkIn_be:1c:00	Broadcast	802.11	Beacon frame, SN=365, FN=0, Flags=........, BI=100, SSID=potend
2237	2018-10-08 18:39:50.226576400	D-LinkIn_79:71:25	Broadcast	802.11	Beacon frame, SN=2290, FN=0, Flags=........, BI=100, SSID=dlink-7121
2238	2018-10-08 18:39:50.240749700	172.17.5.116	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x25e9730e
2239	2018-10-08 18:39:50.250671400	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e

```
> Frame 2238: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits)
> NetMon 802.11 capture header
> 802.11 radio information
v IEEE 802.11 Data, Flags: .......T
    Type/Subtype: Data (0x0020)
  v Frame Control Field: 0x0801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0000 .... = Subtype: 0
    > Flags: 0x01
    Duration/ID: 32768
    Receiver address: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    Transmitter address: IntelCor_a9:52:ec (00:1c:bf:a9:52:ec)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: IntelCor_a9:52:ec (00:1c:bf:a9:52:ec)
    BSS Id: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    STA address: IntelCor_a9:52:ec (00:1c:bf:a9:52:ec)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0000 .... = Sequence number: 0
> Logical-Link Control
> Internet Protocol Version 4, Src: 172.17.5.116, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Bootstrap Protocol (Inform)
```

Wireless Client Getting An IP Address (2/4)

- Wireless station requests for DHCP IP (DHCP Inform)
  - Receiver address: 40:9b:cd:0c:67:50 (DAP-2680, Ethernet MAC Address).



Wireless Client Getting An IP Address (3/4)

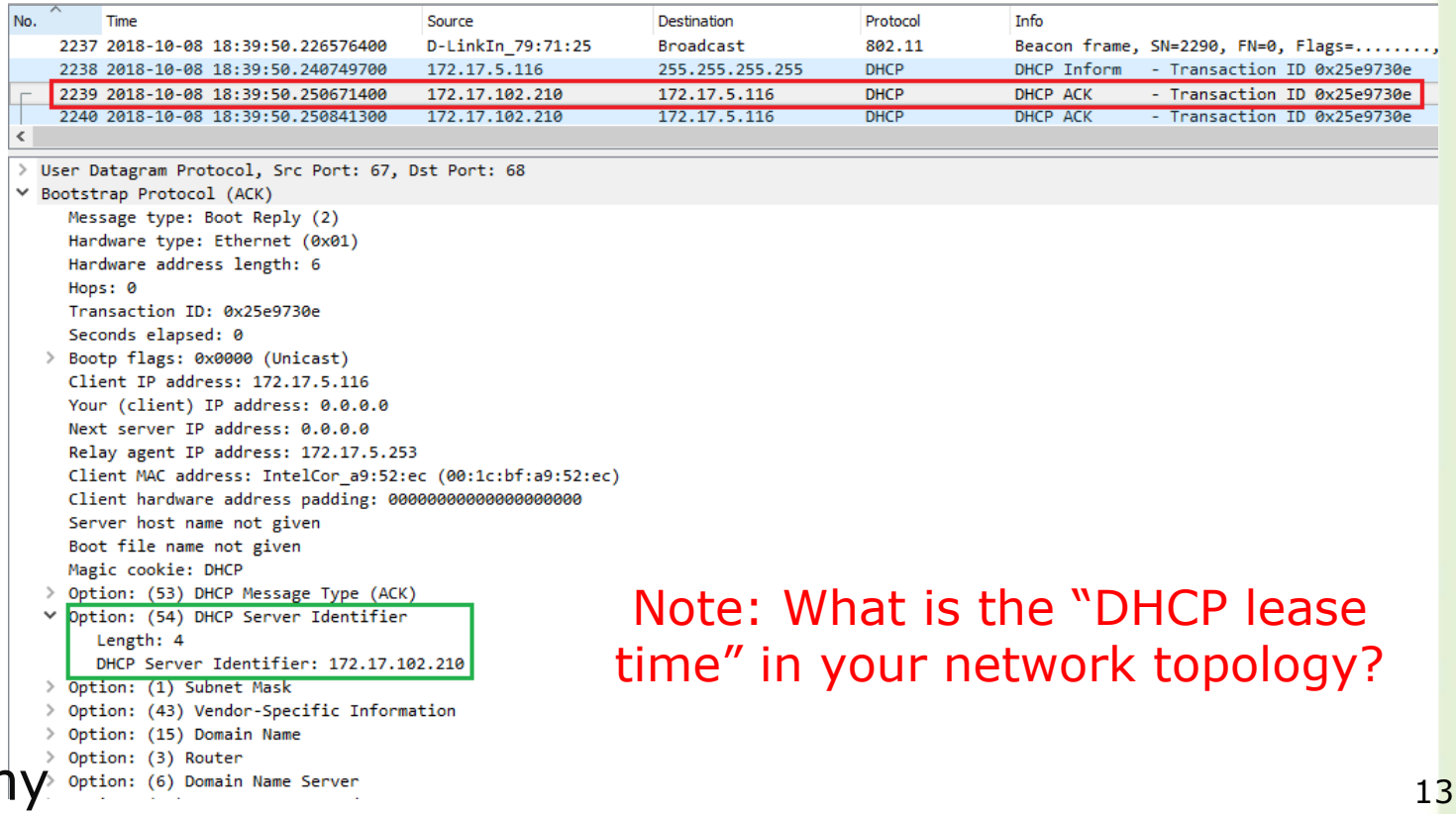
- The Transaction ID in DHCP messages
  - A Transaction ID is used so that the DHCP server can differentiate among wireless clients.
  - The Wireshark capture, from both DAP and wireless station should carry the same Transaction ID.

No.	Time	Source	Destination	Protocol	Info
14142	2018-10-08 18:39:01.330738	172.17.102.210	172.17.5.96	DHCP	DHCP ACK - Transaction ID 0x10cfc447
32200	2018-10-08 18:40:18.054399	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e
32201	2018-10-08 18:40:18.054404	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e
32202	2018-10-08 18:40:18.056139	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e
32203	2018-10-08 18:40:18.057053	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e
1520	2018-10-08 18:36:59.428685	172.17.5.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1

No.	Time	Source	Destination	Protocol	Info
2237	2018-10-08 18:39:50.226576400	D-LinkIn 79:71:25	Broadcast	802.11	Beacon frame, SN=2290, FN=0, Flags=........,
2238	2018-10-08 18:39:50.240749700	172.17.5.116	255.255.255.255	DHCP	DHCP Inform - Transaction ID 0x25e9730e
2239	2018-10-08 18:39:50.250671400	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e
2240	2018-10-08 18:39:50.250841300	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e
2241	2018-10-08 18:39:50.251082600	172.17.102.210	172.17.5.116	DHCP	DHCP ACK - Transaction ID 0x25e9730e

Wireless Client Getting An IP Address (4/4)

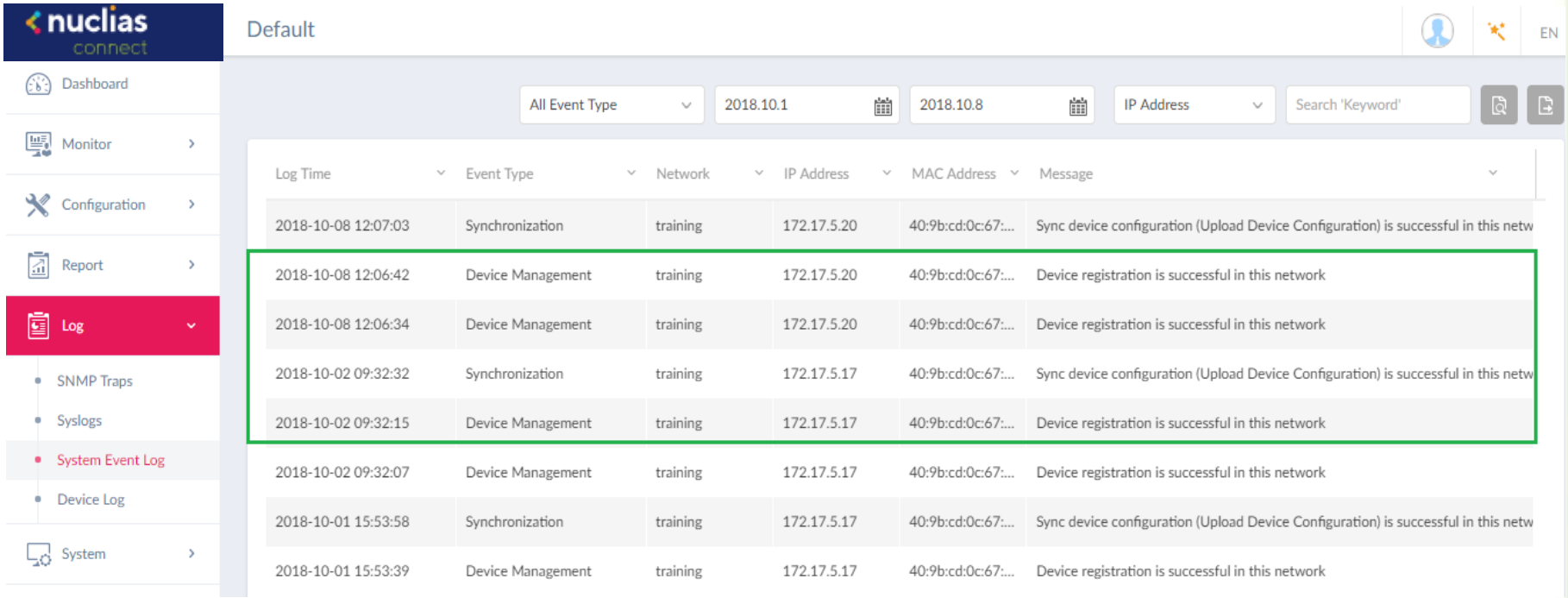
- Wireless station requests for DHCP IP (DHCP Ack)
  - Source: DHCP Server
  - Destination: DHCP Client



Note: What is the "DHCP lease time" in your network topology?

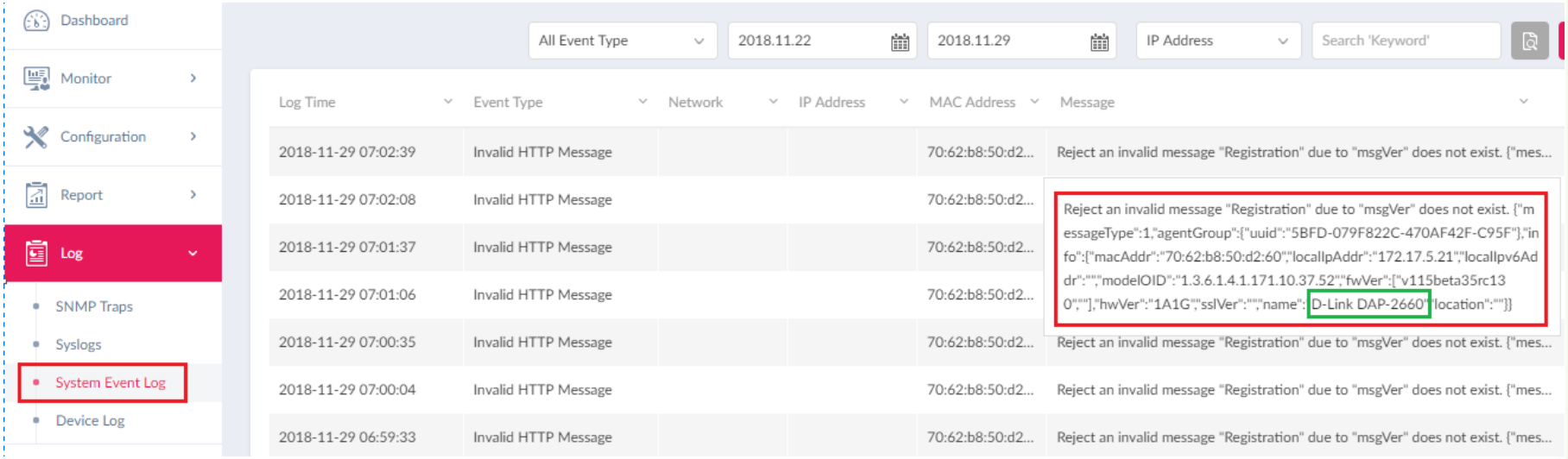
Guidelines for Troubleshooting (DAP Device Registration)

- Once a DAP device being managed by DNC, we should be able to see precise device registration messages, being indicated on the System Event Log under Log tab.



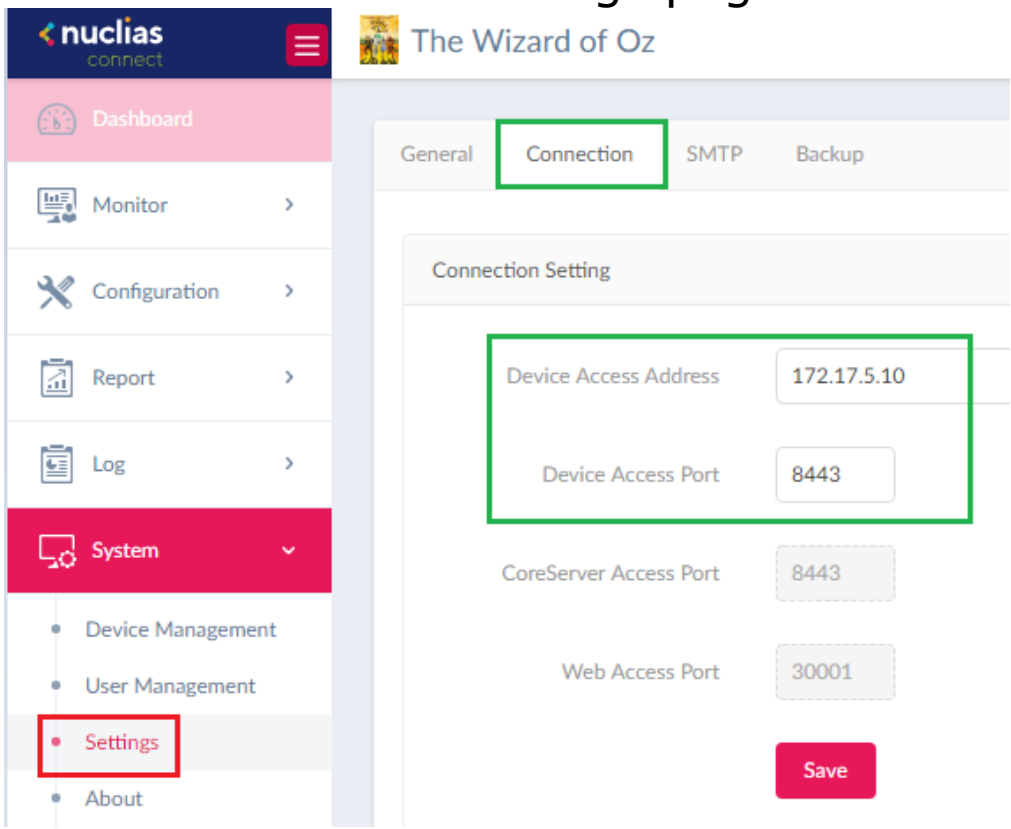
Guidelines for Troubleshooting (DAP Device Registration, Cont'd)

- The below is a sample that a DAP IS NOT installed with proper firmware, in order to be managed by Nuclias Connect.



Guidelines for Troubleshooting (DNC IP Add)

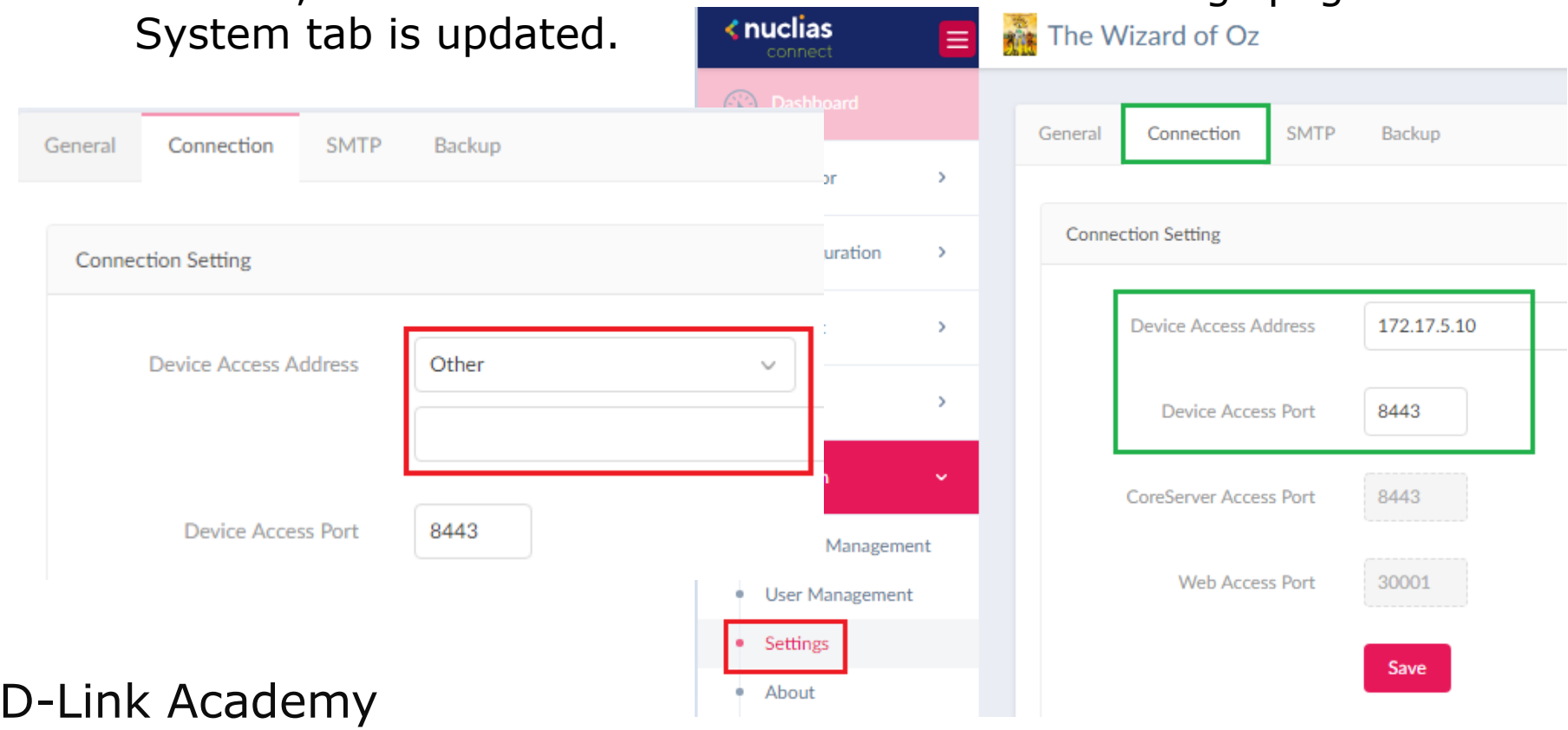
- There is a possibility that the Nuclias Connect server IP address is requested to be modified.
- As such, we need to make sure the IP in the Settings page under System tab is updated.



In official release, the port number is grayed out, preventing any further modifications.

Guidelines for Troubleshooting (DNC IP Add)

- There is a possibility that the Nuclias Connect server IP address is requested to be modified.
- As such, we need to make sure the IP in the Settings page under System tab is updated.

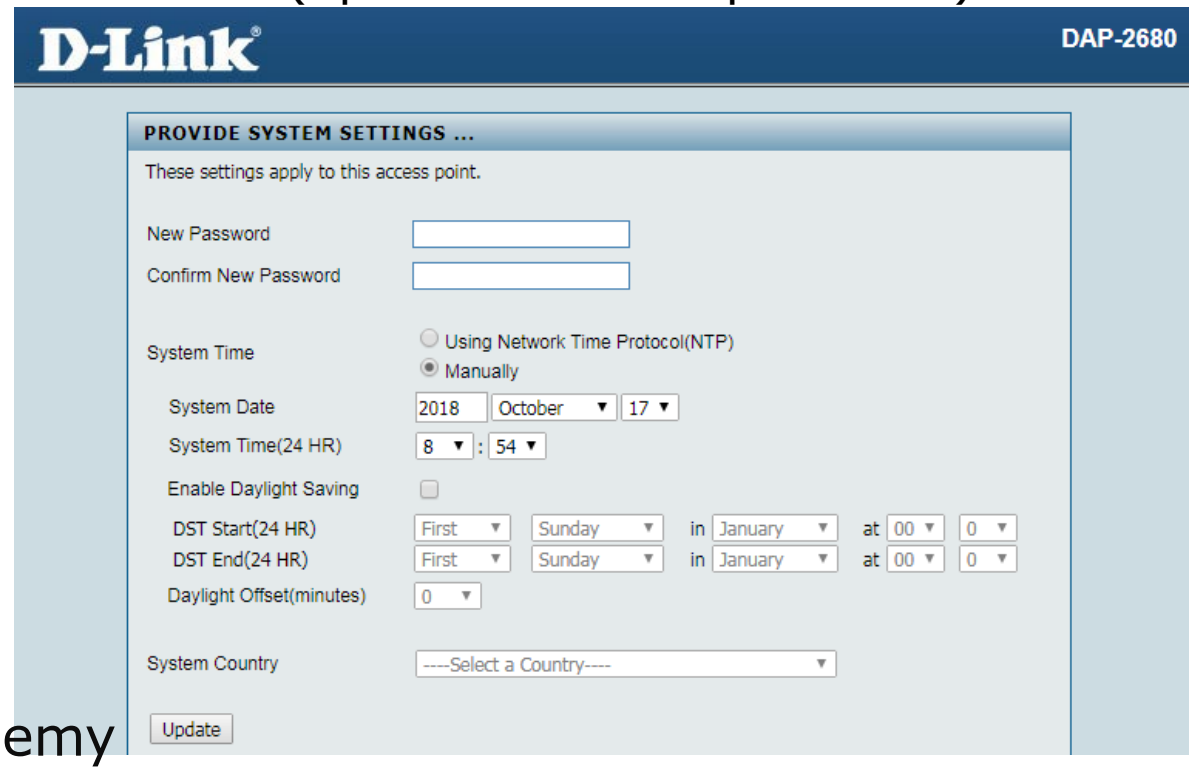


Guidelines for Troubleshooting (DNC IP Add)

- After the DNC IP address being updated, then, we should rebooting that server, and verify below items:
  - System > Settings > Connection (both device access address and web access address need to be updated)
  - Windows Task Manager, Details tab, NucliasConfigurator.exe and Nuclias-core.exe should be in Running status
  - Windows Task Manager, Services tab, mongoDB is in Running status as well

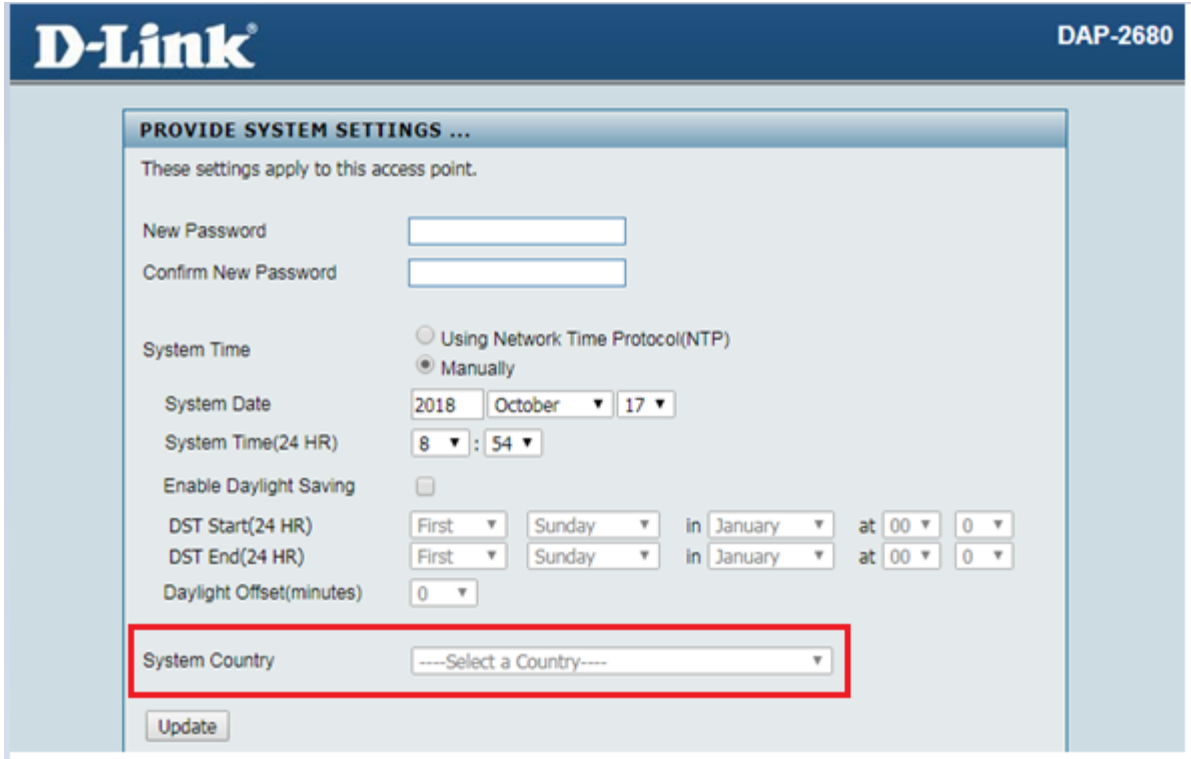
Guidelines for Troubleshooting (Discovering a DAP)

- When there is a difficulty to discover your DAP, make sure
  - (1) DAP firmware has been upgraded
  - (2) make sure DAP reboot and see the password update menu, as shown here (update with new password)



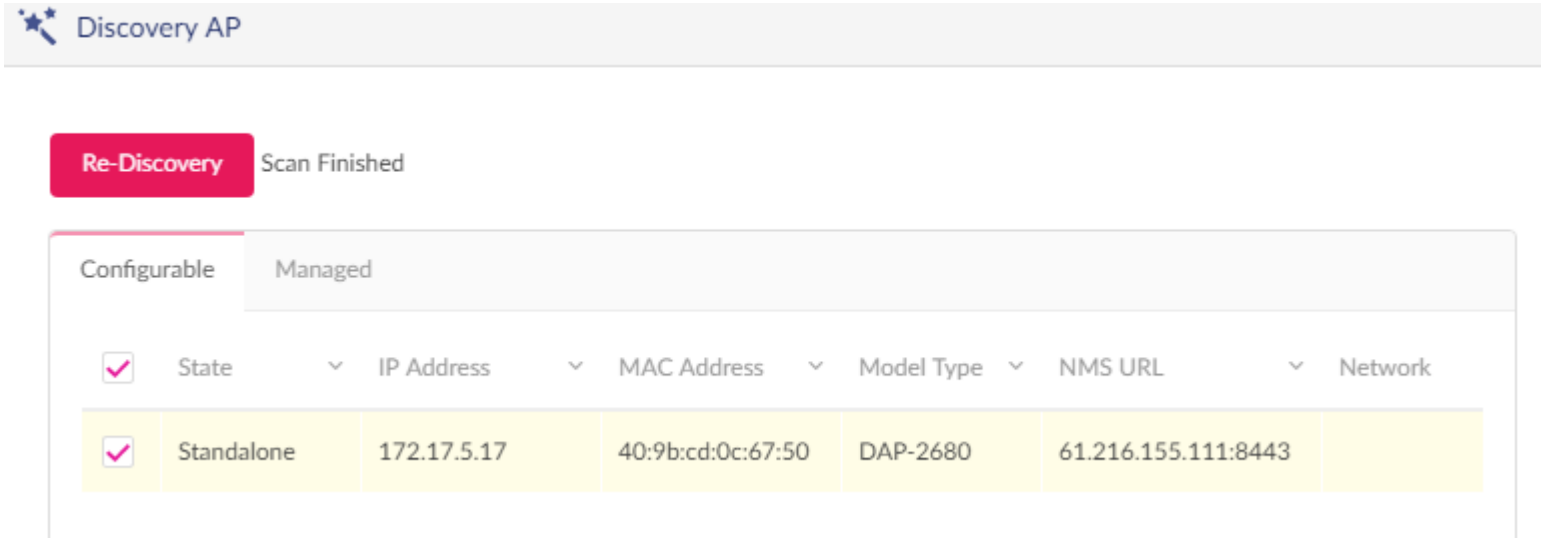
Guidelines for Troubleshooting (Discovering a DAP)

- The available channels and radio powers are in compliance with the regulations in your region. We need to ensure the location (country) settings before beginning wireless networks.



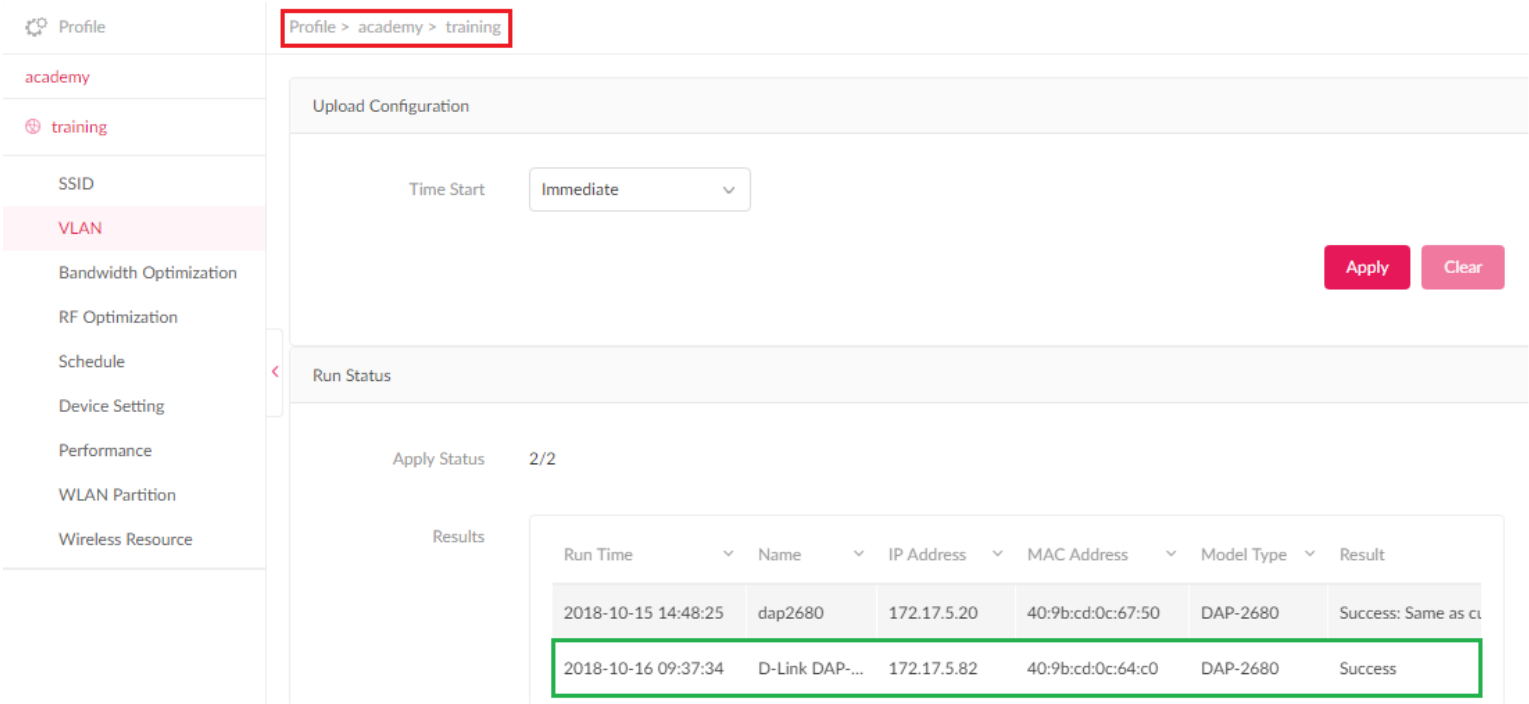
Guidelines for Troubleshooting (Discovering a DAP)

- Scenario: the following device was bonded with RD server (another DNC server), thus, it would not be able to be managed by our lab.



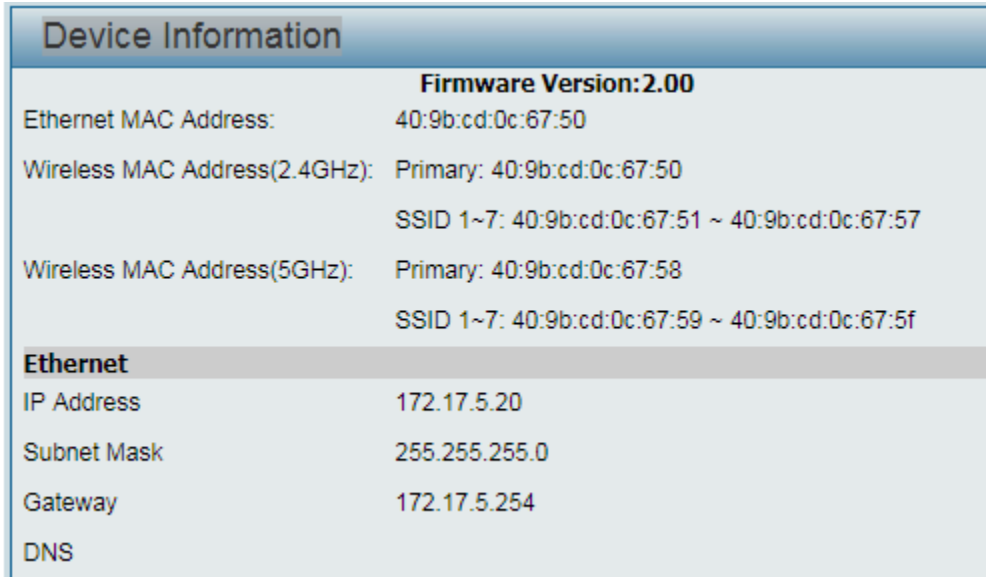
Guidelines for Troubleshooting (Discovering a DAP)

- Should we plan to make any profile changes and apply those changes to managed APs, we could visit “Run Status” to obtain clear understanding of latest standing point.



Guidelines for Troubleshooting (DAP Device Information)

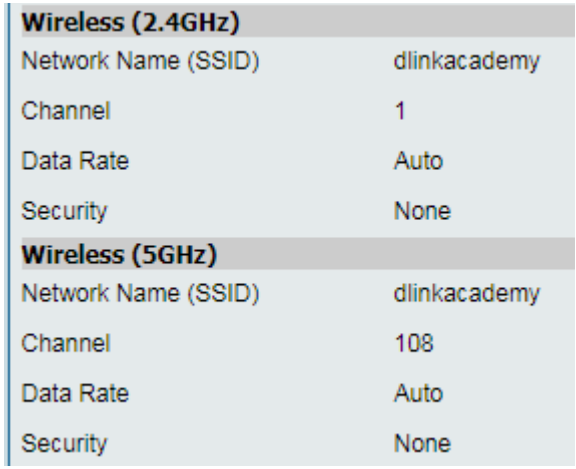
- Once an DAP device being managed by DNC, what type of information would be presented when we login its GUI locally?
  - For example, the managed DAP is using IP of 172.17.5.20



Device Information

Firmware Version:2.00

Ethernet MAC Address:	40:9b:cd:0c:67:50
Wireless MAC Address(2.4GHz):	Primary: 40:9b:cd:0c:67:50
	SSID 1~7: 40:9b:cd:0c:67:51 ~ 40:9b:cd:0c:67:57
Wireless MAC Address(5GHz):	Primary: 40:9b:cd:0c:67:58
	SSID 1~7: 40:9b:cd:0c:67:59 ~ 40:9b:cd:0c:67:5f
Ethernet	
IP Address	172.17.5.20
Subnet Mask	255.255.255.0
Gateway	172.17.5.254
DNS	



Wireless (2.4GHz)	
Network Name (SSID)	dlinkacademy
Channel	1
Data Rate	Auto
Security	None
Wireless (5GHz)	
Network Name (SSID)	dlinkacademy
Channel	108
Data Rate	Auto
Security	None

Guidelines for Troubleshooting (DAP Device Information)

- Once an DAP device being managed by DNC, what type of information would be presented when we login its GUI locally?
  - The DNC server IP, in below screenshot, is 172.17.5.86.
  - Group ID represents the Universally Unique Identifier (UUID).

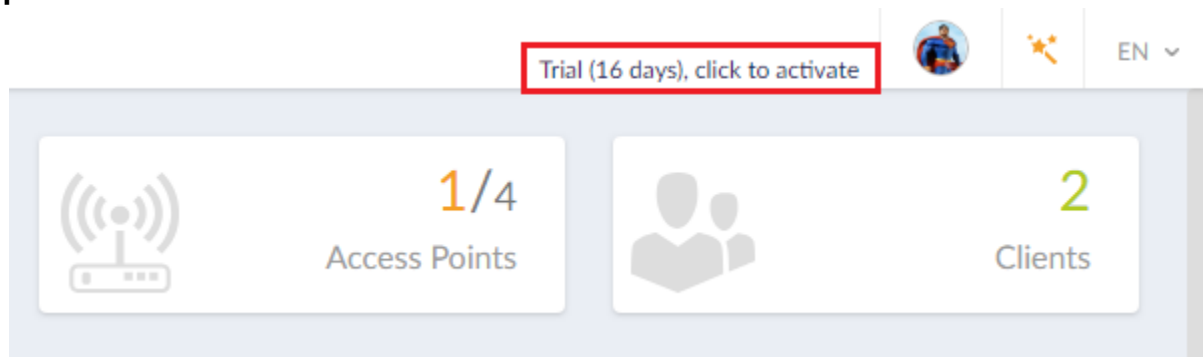
Device Status	
CPU Utilization	19%
Memory Utilization	26%
Nuclias Connect	
Connection Status	Connect
Server IP/PORT	172.17.5.10:8443
Group ID	5C32-C4B7FB08-85186CE4-B099

  - UUID describes the "Network" a specific DAP device belongs to.

- Another way to change "Server IP/Port" is by exporting Network Profile

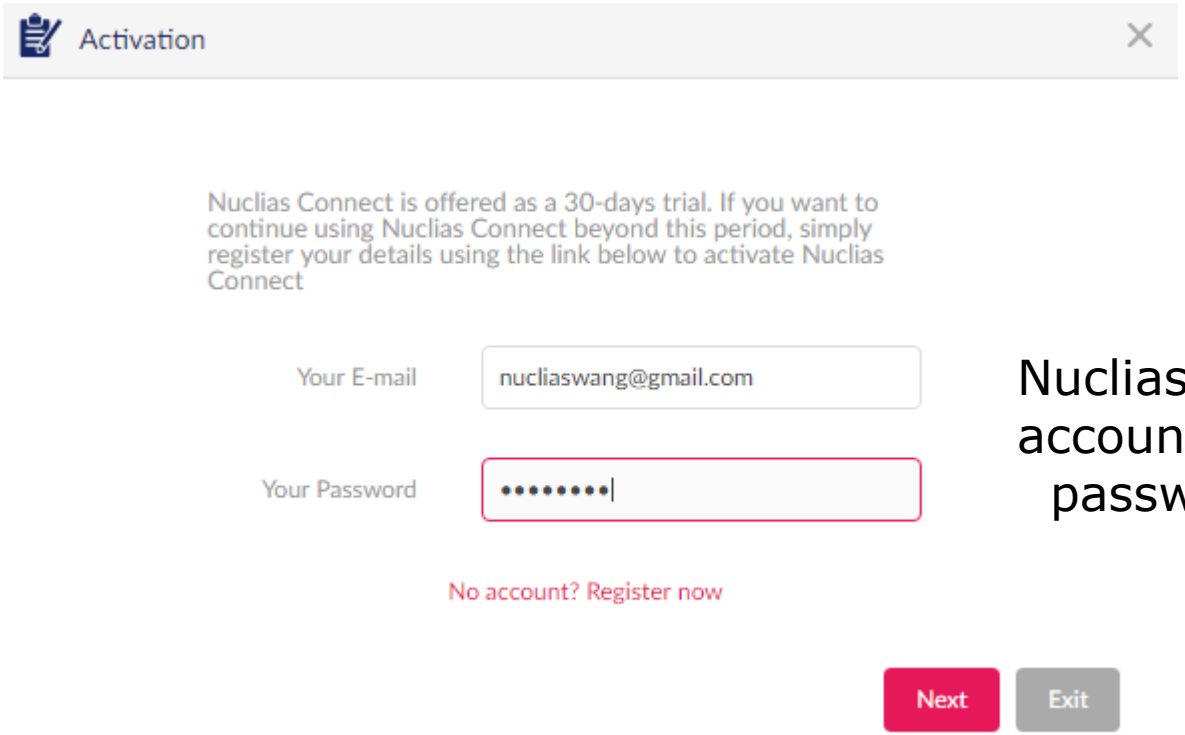
From Trial Application To Official Firmware (1/4)

- Most of the end users download and install Nuclias Connect as a trial application.



From Trial Application To Official Firmware (2/4)

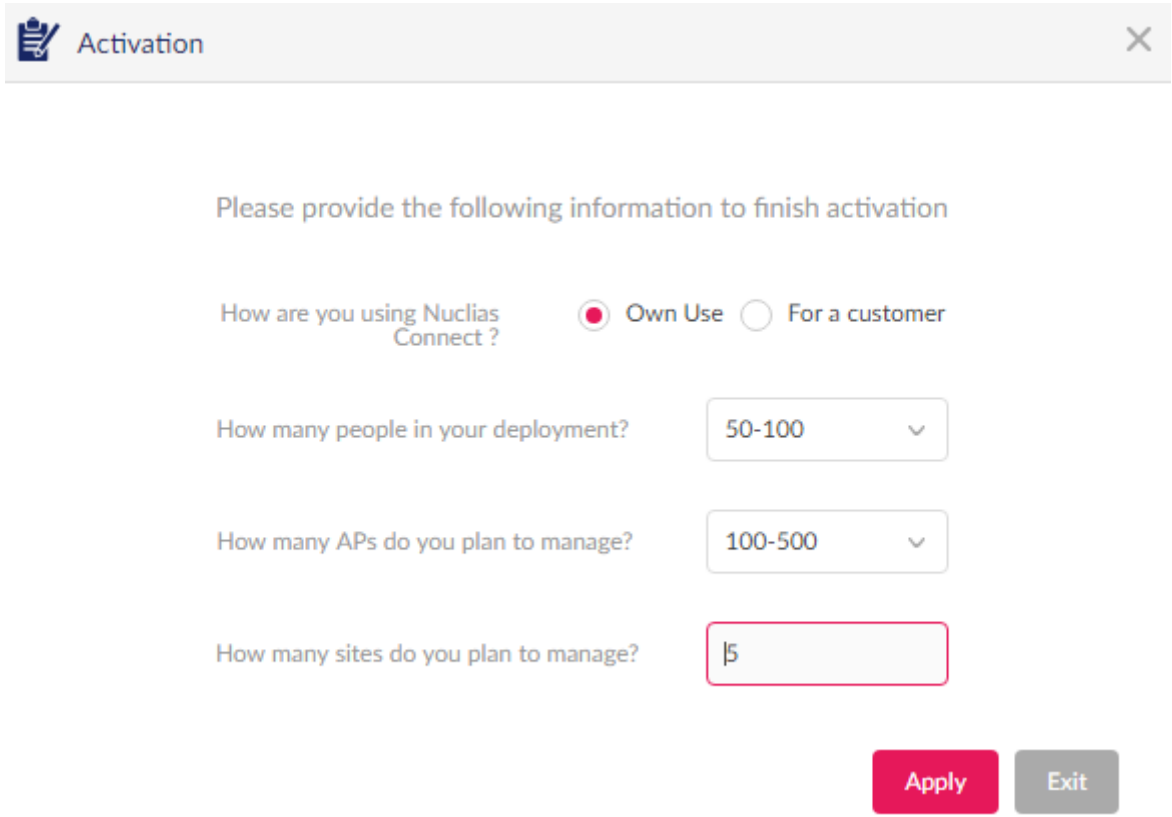
- Should you decide to activate official firmware, a Nuclias user account is required.
  - Double click "click to activate" as displayed in last slide



Nuclias user account and password

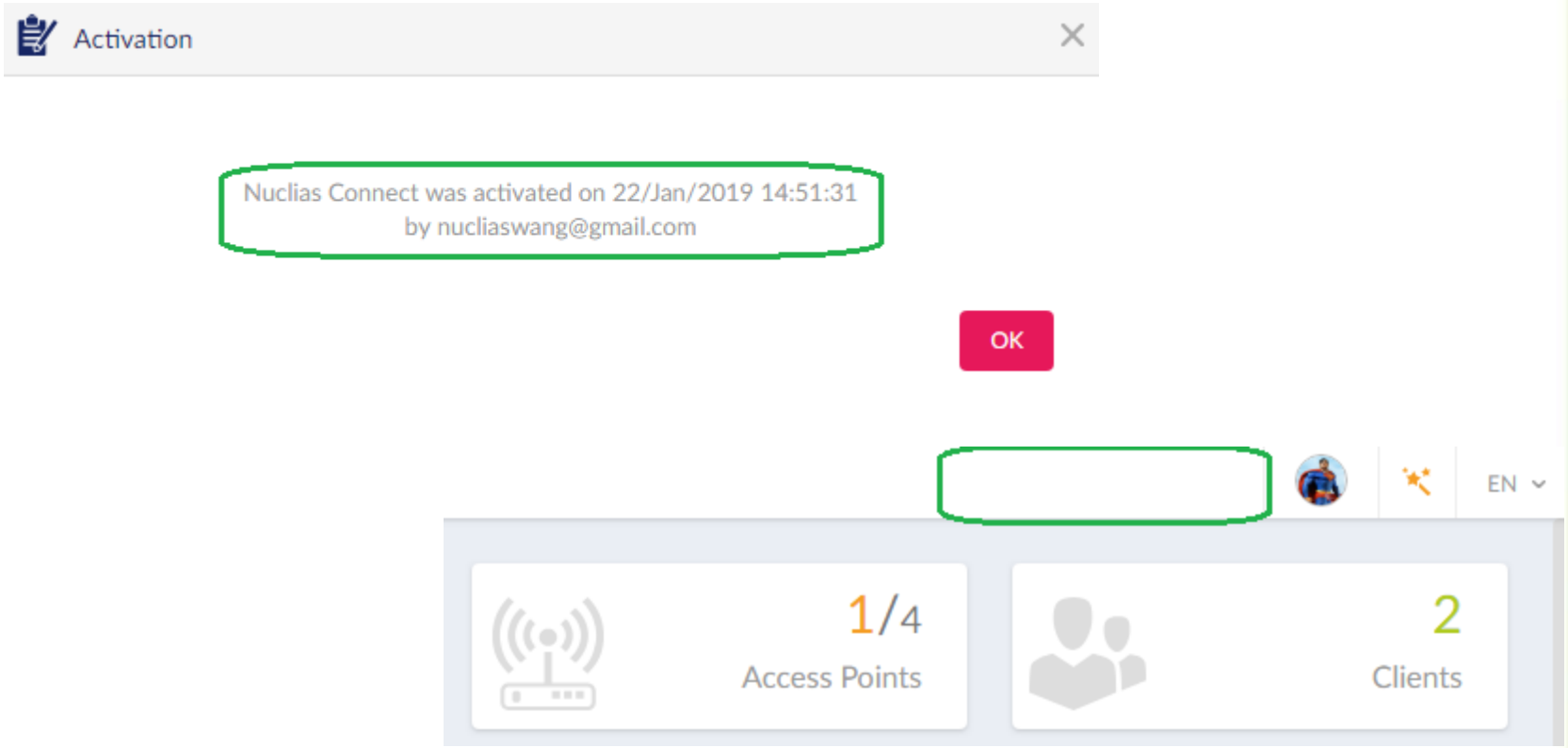
From Trial Application To Official Firmware (3/4)

- Please respond to the following questions



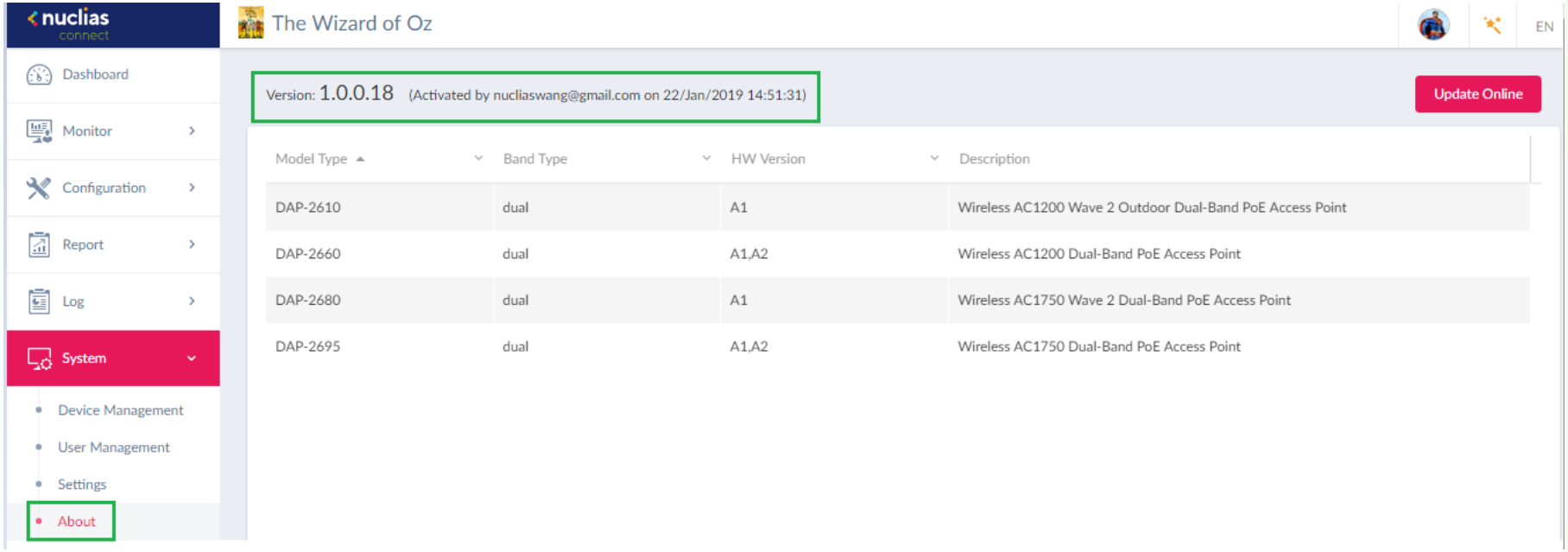
From Trial Application To Official Firmware (4/4)

- Should proper information being verified, Nuclais Connect would present the following message



The Display of Official Firmware

- Navigate to menu (System > About)



Nuclias Connect Hands-on Tutorial

- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

The Design Thinking of Dashboard and Report

- Design Thinking
- Nuclias Connect Dashboard
- Nuclias Connect Management Report

The Design Thinking of Dashboard and Report

- Design Thinking
- Nuclias Connect Dashboard
- Nuclias Connect Management Report

Design Thinking

Thinking critically starts with asking questions. Articulate questions using 6W and 1H.

- WHAT
- WHO
- WHEN
- WHERE
- WHY
- WHAT and WHAT IF
- HOW

Design Thinking

3W and 1H

- WHAT
  - To show users' demand and perspective on wireless service
  - To visualize data and manage the wireless network topology
- WHEN
  - The last seven days
  - The last three months (Ninety days)
  - Fifteen minutes time intervals
- WHAT and WHAT IF
  - Two parameters: traffic usage and number of wireless client(s)
  - Data displayed across the system & Network volatility
  - Threshold & Probability
- HOW

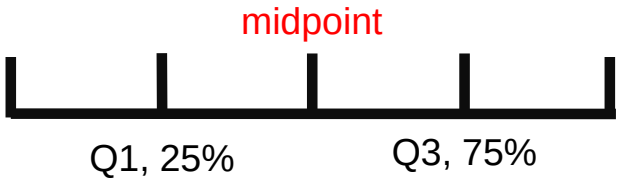
Design Thinking

3W and 1H

- WHAT
  - To show users' demand and perspective on wireless service
  - To visualize data and manage the wireless network topology
- WHEN
  - The last seven days
  - The last three months (Ninety days)
  - Fifteen minutes time intervals
- WHAT and WHAT IF
  - Two parameters: traffic usage and number of wireless client(s)
  - Data displayed across the system & Network volatility
  - Threshold & Probability
- HOW

Design Thinking

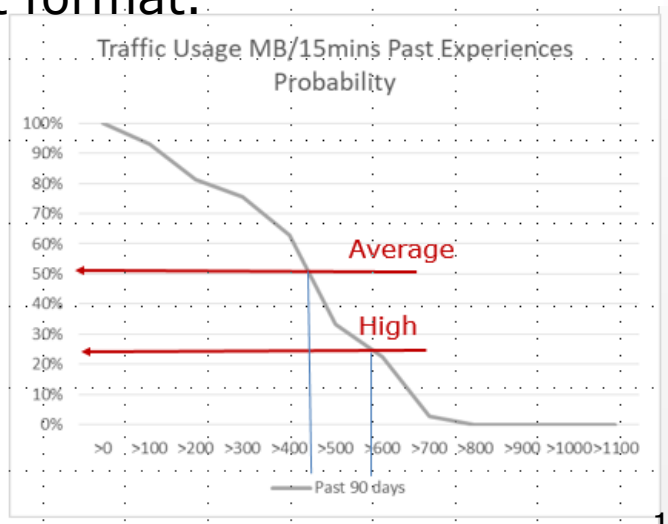
- Fundamental concepts in Statistics
- Quartiles
  - The lower quartile is the value of the middle of the first set, where 25% of the values are smaller than Q1 and 75% are larger. This first quartile takes the notation Q1.
  - The upper quartile is the value of the middle of the second set, where 75% of the values are smaller than Q3 and 25% are larger. This third quartile takes the notation Q3.
- Midpoint vs. Average
  - A midpoint is defined as a point that is exactly in the middle between two other points.
  - Average is a number expressing the central or typical value in a set of data.



Design Thinking

3W and 1H

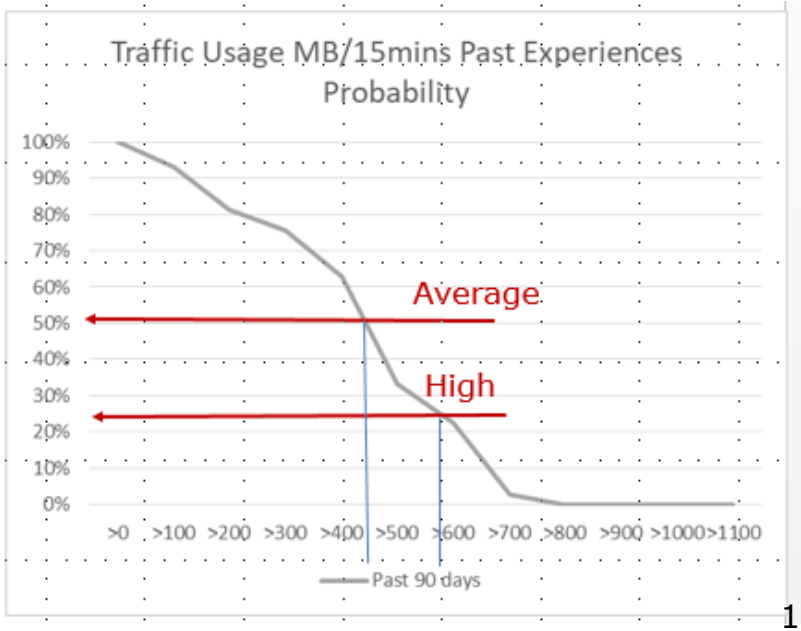
- WHAT
- WHEN
- WHAT and WHAT IF
- HOW
  - Basing upon three months collected data, we are able to generate a probability diagram, which should display Average and High point similar like below chart format.
  - Traffic usage > 0 MB is 100%
  - Traffic usage > 100 MB is close to 0%
  - Average: 50% mark
  - High: 75% mark



Design Thinking

3W and 1H

- HOW
  - Average: over the last three months, 50% probability that traffic usage exceeds 450MB.
  - High: over the last three months, 25% probability that traffic usage exceeds 600MB.



Design Thinking

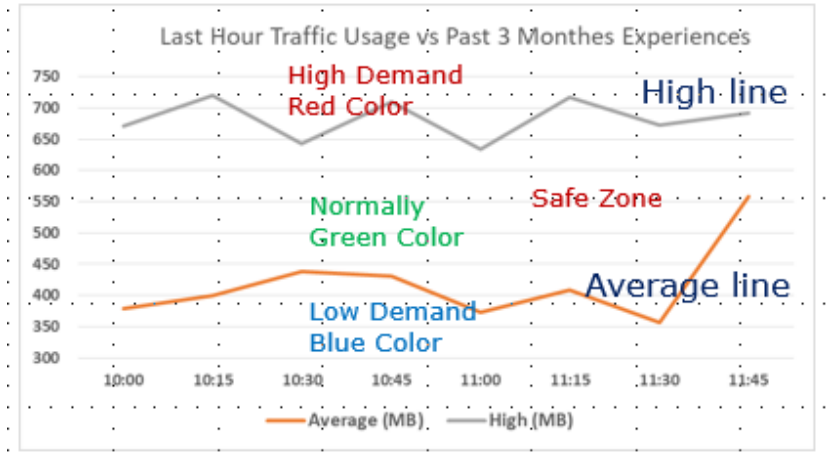
3W and 1H

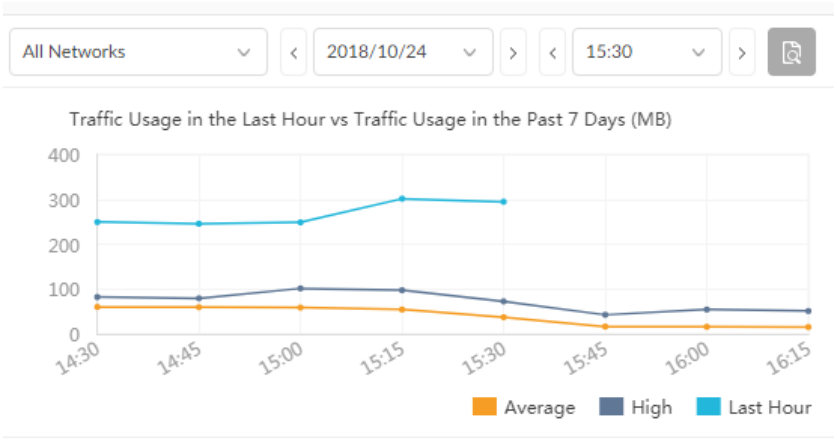
- HOW (a better interpretation from a practical perspective)
  - The most recent Traffic Usage is higher than High line: heavy wireless traffic usage. Close monitoring is recommended.
  - The most recent Traffic Usage is higher than Average line, but lower than High line: a normal behavior requires minor attention.
  - The most recent Traffic Usage is lower than Average line: light traffic on the horizon.

Design Thinking

3W and 1H

- HOW (a better interpretation from a practical perspective)
  - The most recent Traffic Usage is higher than High line: heavy wireless traffic usage. Close monitoring is recommended.
  - The most recent Traffic Usage is higher than Average line, but lower than High line: a normal behavior requires minor attention.
  - The most recent Traffic Usage is lower than Average line: light traffic on the horizon.



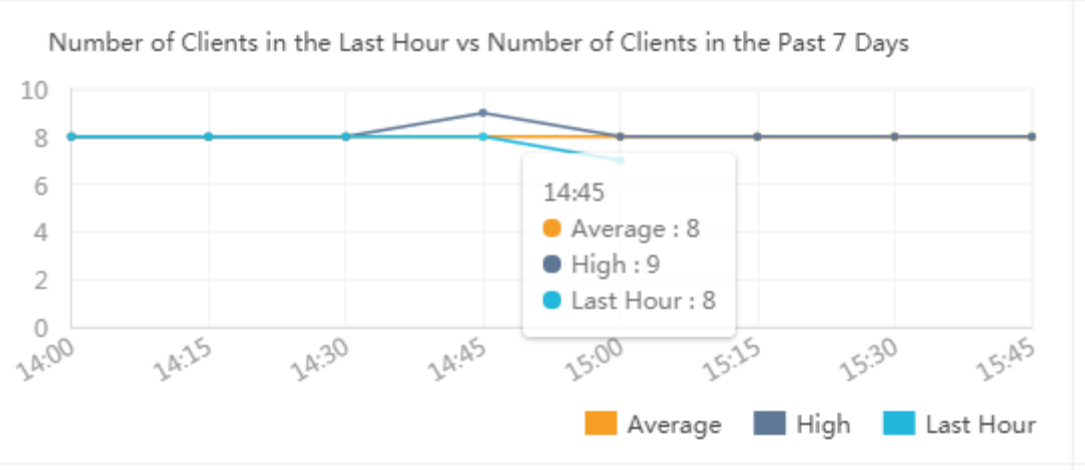


horizontal timelines

Design Thinking

3W and 1H

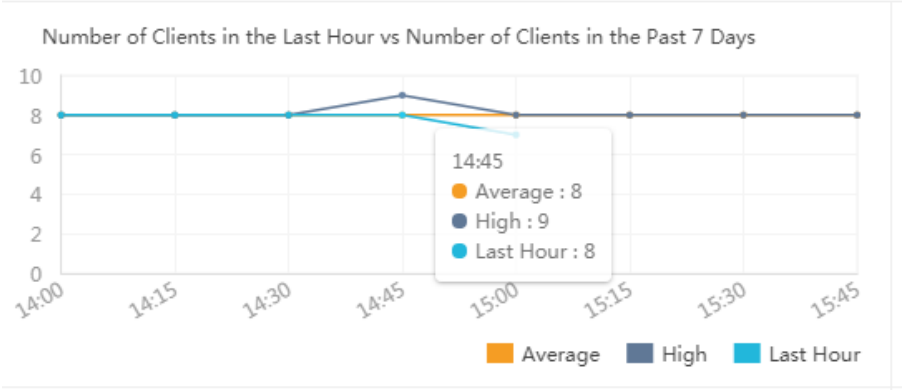
- HOW (Inter-subject swapping, let's go with "wireless client")
  - At 14:45PM, according past 7 days line, 50% probability around 8 unique clients access wireless network in 15 mins.
  - At 14:45PM, according past 7 days line, 25% probability around 9 unique clients access wireless network in 15 mins.



Design Thinking

3W and 1H

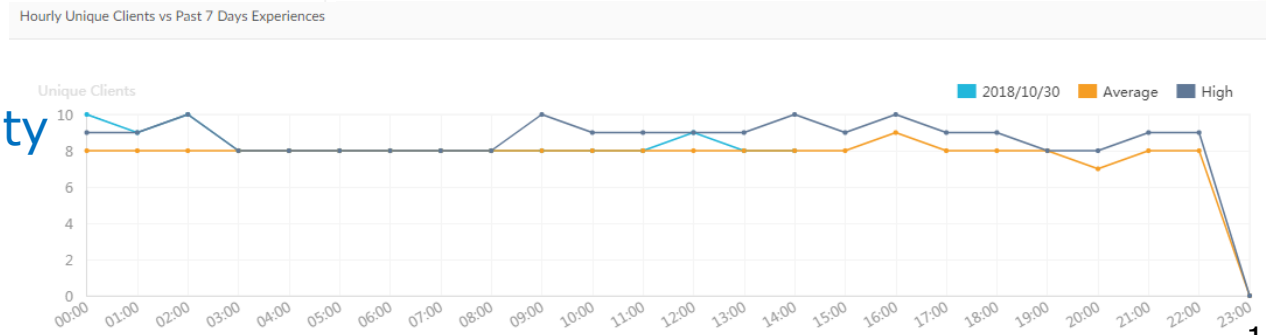
- HOW (Inter-subject swapping, let's go with "wireless client")
  - Despite the subject of "wireless client" remains in both diagrams, the length of time is NOT the same.



Significantly "wireless client" increase is not expected.

Dashboard vs.

Hourly Network Activity



The Design Thinking of Dashboard and Report

- Design Thinking
- Nuclias Connect Dashboard
- Nuclias Connect Management Report

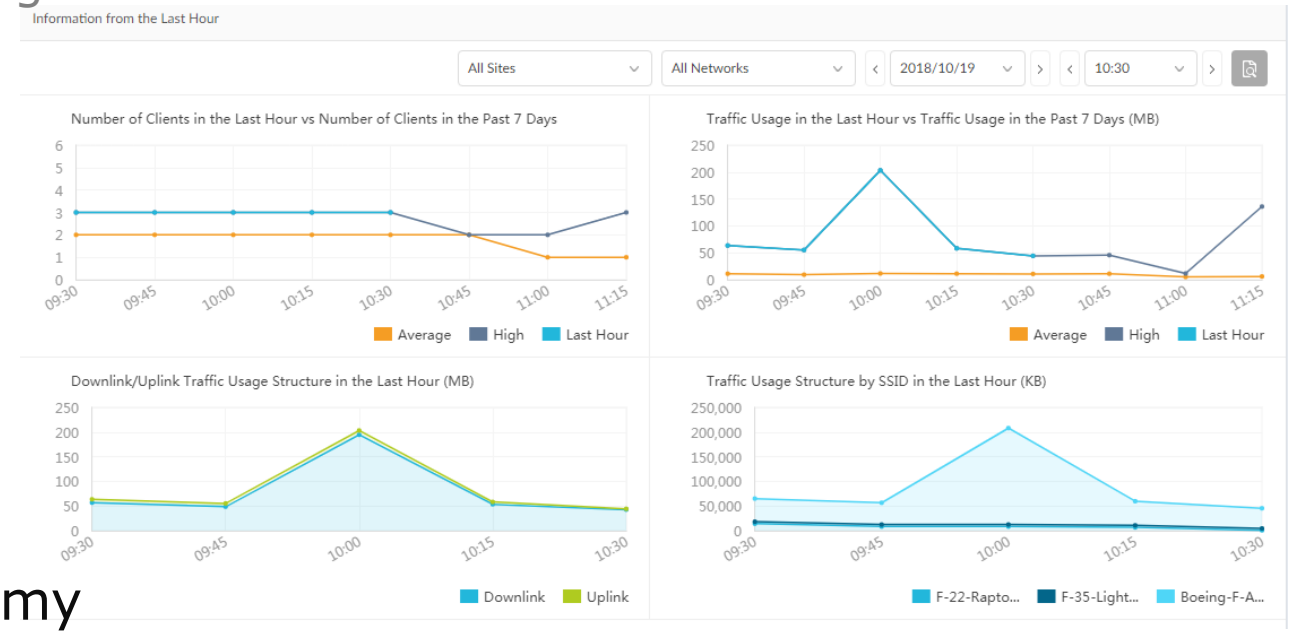
Nuclias Connect Dashboard

- From viewpoint of “Wireless Summary Report”
- This page provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
  - Channel utilization
  - Syslog events

- In DNC official release, the Dashboard may have a sub-item, named “overview”

Nuclias Connect Dashboard

- Nuclias Connect Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
    - Usage breakdown by number of clients, traffic usage, SSID
  - Channel utilization
  - Syslog events

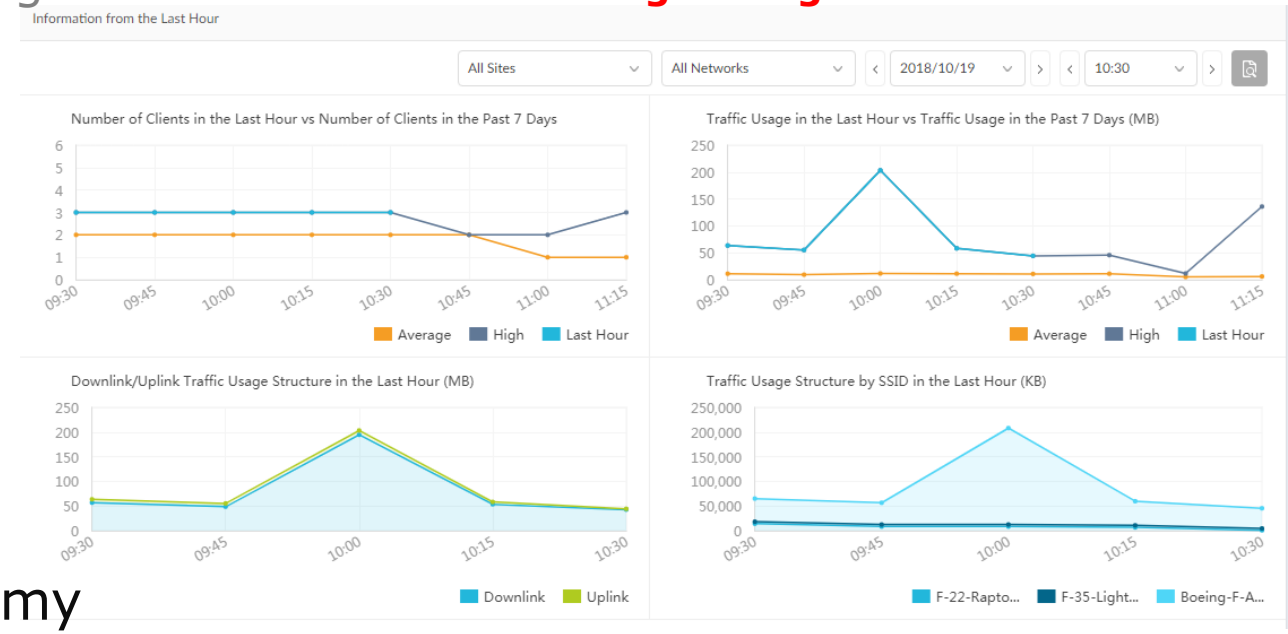


Nuclias Connect Dashboard

- Nuclias Connect Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
    - Usage breakdown by number of clients, traffic usage, SSID
  - Channel utilization
  - Syslog events

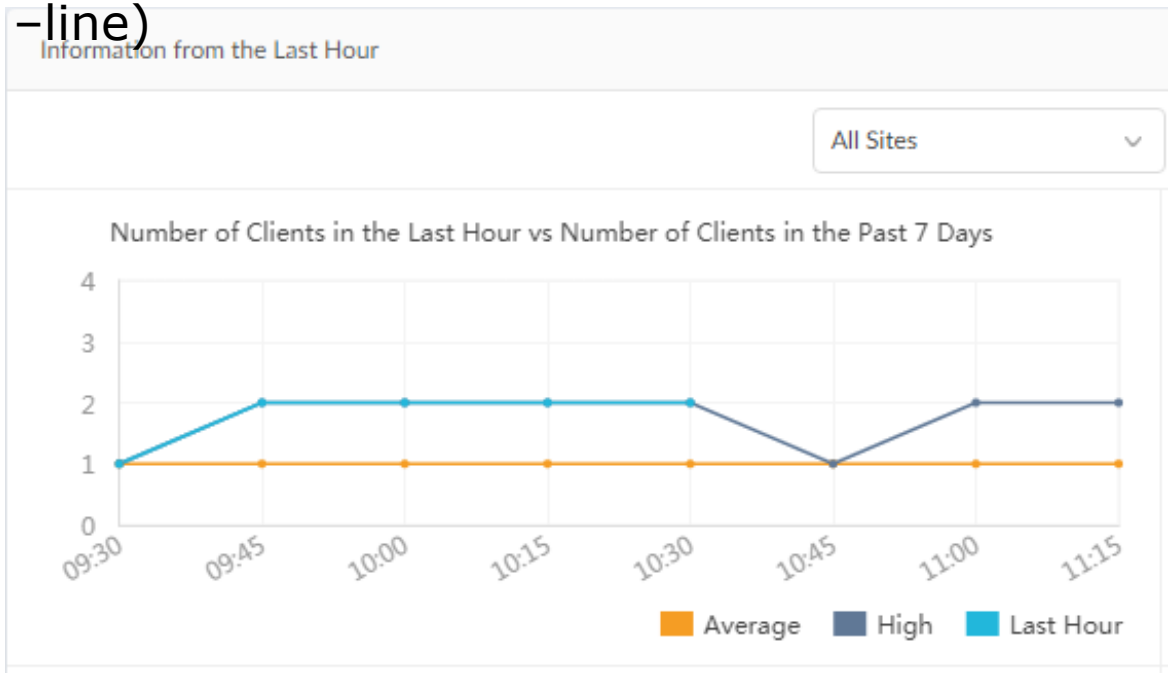
Design Thinking

Average & High



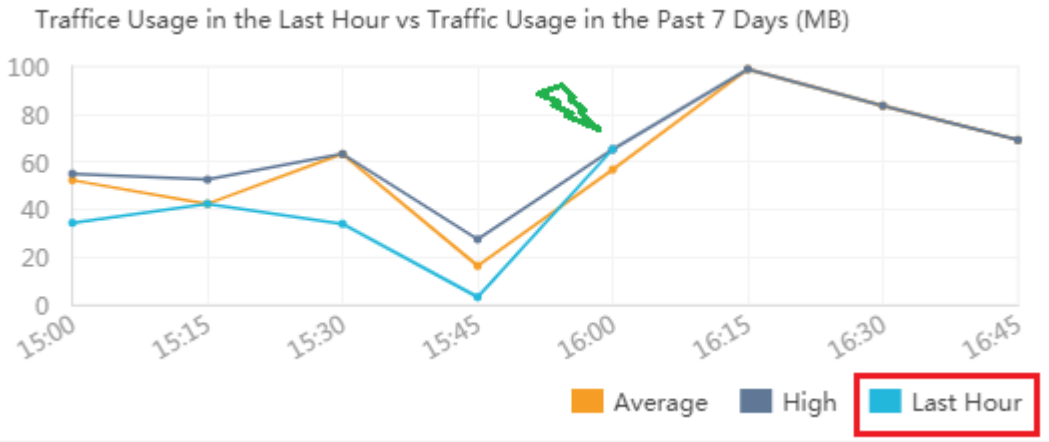
Nuclias Connect Dashboard, Information From The Last Hour

- Dashboard, information from last hour
- Number of clients in the last hour, representing the wireless clients attempting to connecting to our DAPs
  - The number of STA has been connected within last 15-min
  - Menu: Monitor > Wireless Client represents the actual connections (on –line)



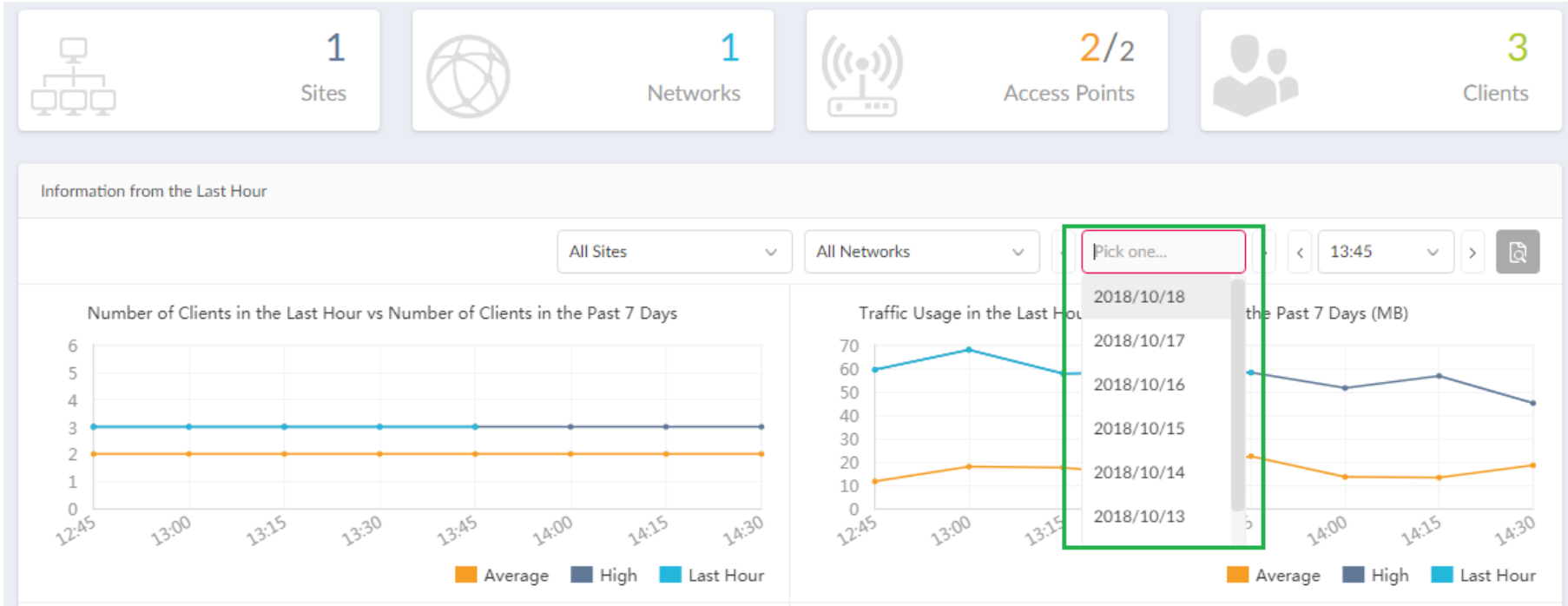
Nuclias Connect Dashboard, Information From The Last Hour

- Traffic Usage (actual network utilization within last hour vs. wireless services forecast for next 60 minutes period of time)
- Major parameters: Traffic Usage and Number of Clients (wireless stations)
- Time Period: Two hours and/or three months
- Time Span represents a period of time. 15-min is a common way to represent.
- Last Hour is about in the middle point of the entire time period



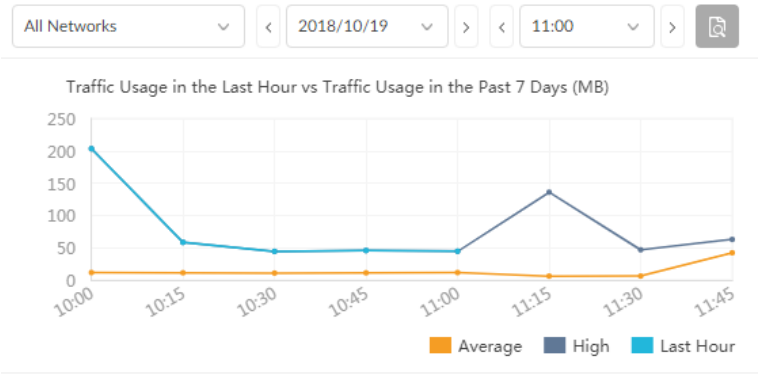
Nuclias Connect Dashboard, Information From The Last Hour

- Traffic Usage, Options to Select Dates



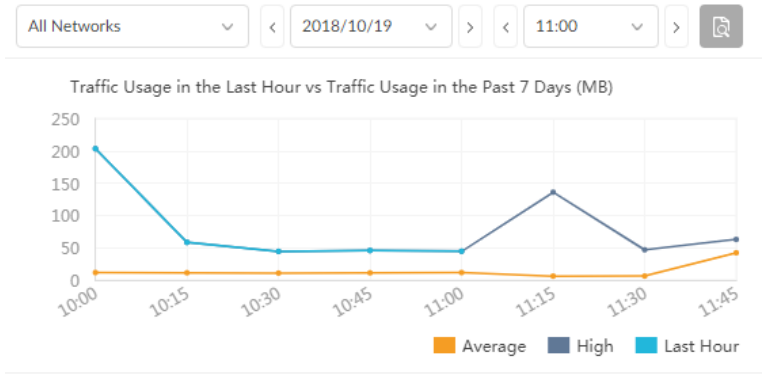
Nuclias Connect Dashboard, Information From The Last Hour

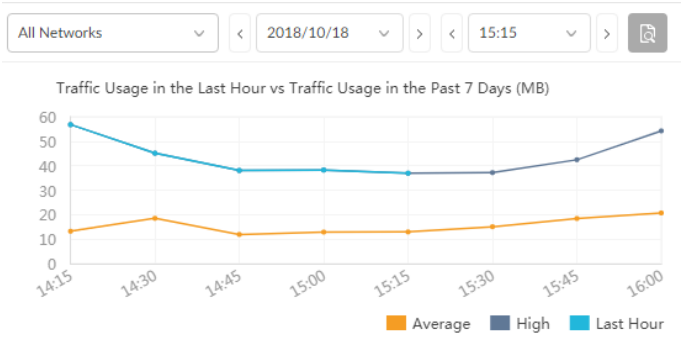
- DNC Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
    - The report can be customized and viewed for statistics over a certain time period to allow for statistical analytics.



Nuclias Connect Dashboard, Information From The Last Hour

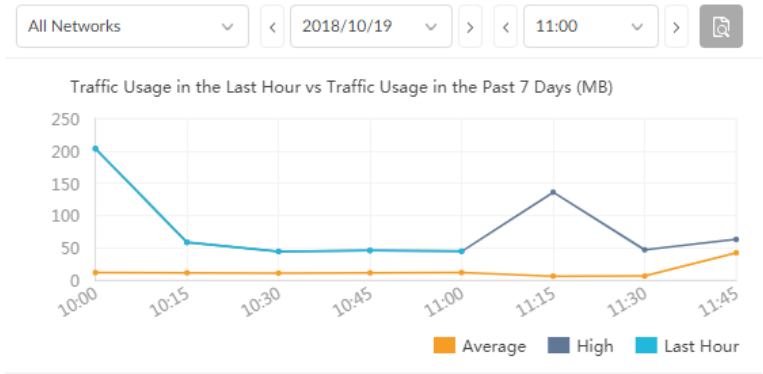
- DNC Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
    - The report can be customized and viewed for statistics over a certain time period to allow for statistical analytics.

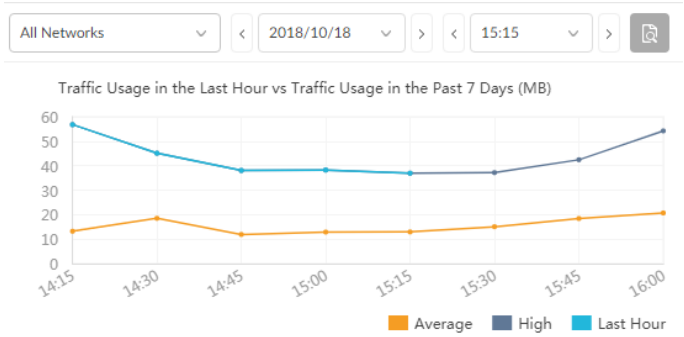


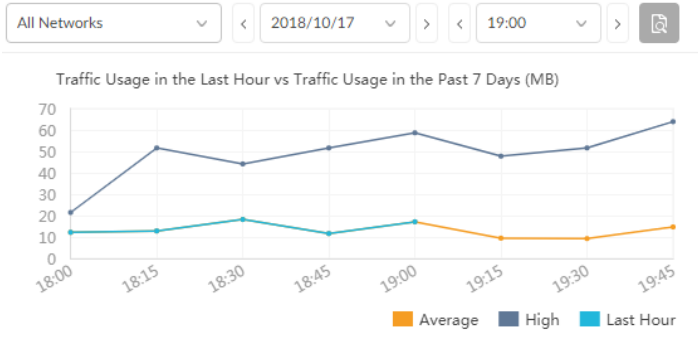


Nuclias Connect Dashboard, Information From The Last Hour

- DNC Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
    - The report can be customized and viewed for statistics over a certain time period to allow for statistical analytics.

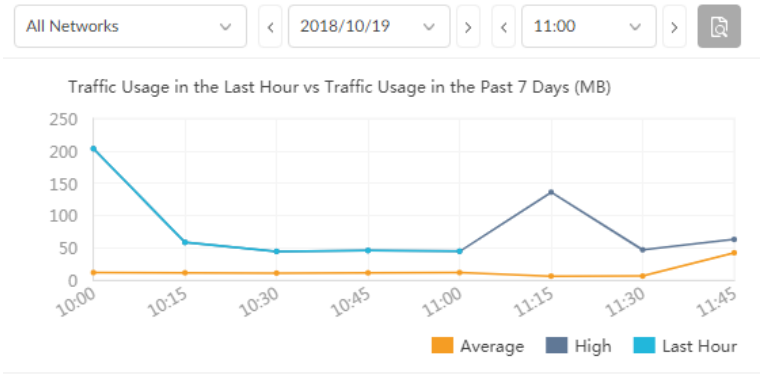


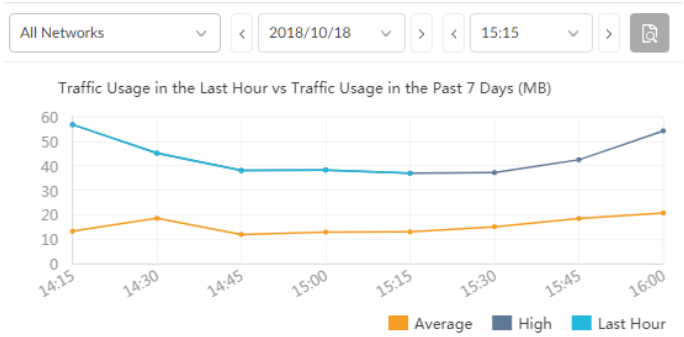


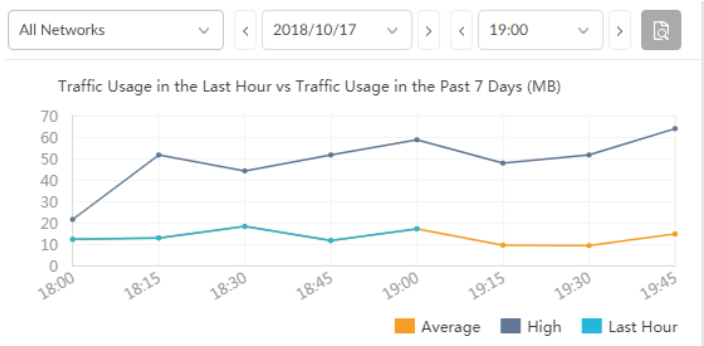


Nuclias Connect Dashboard, Information From The Last Hour

- DNC Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
    - The report can be customized and viewed for statistics over a certain time period to allow for statistical analytics.



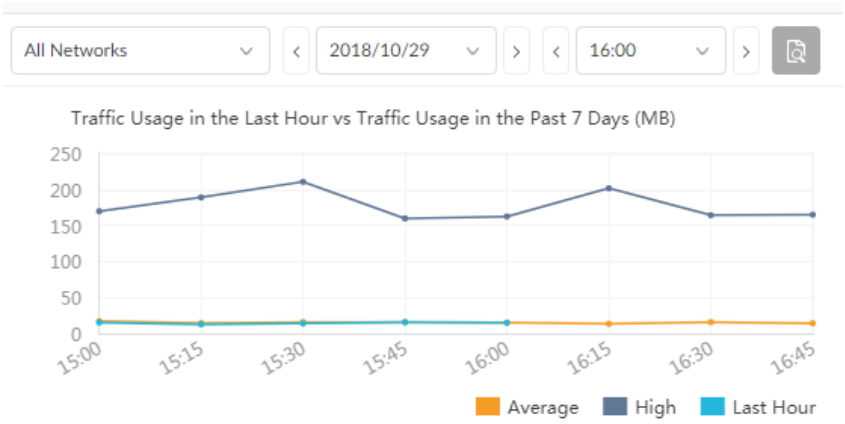


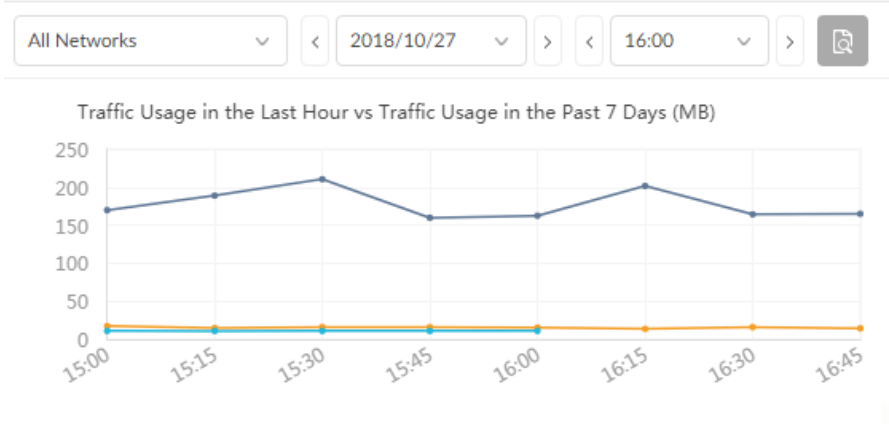


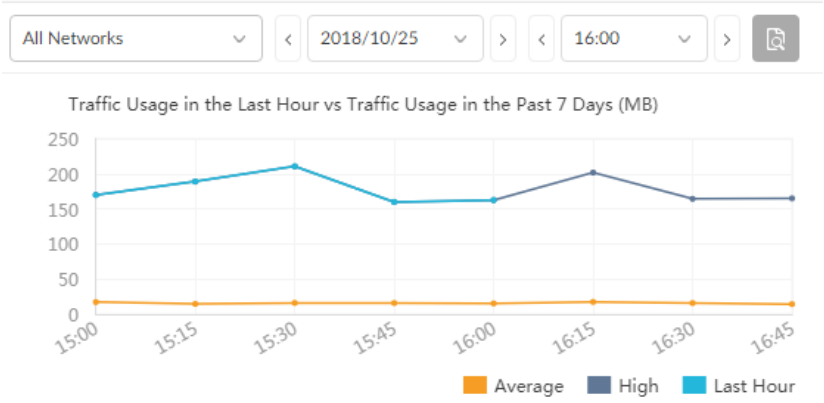
Data will be back-calculated

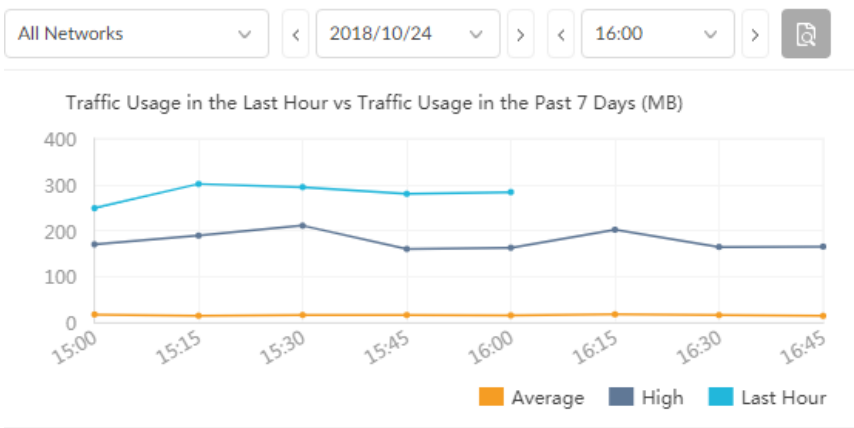
Nuclias Connect Dashboard, Information From The Last Hour

- Traffic Usage, options of dates (another example)



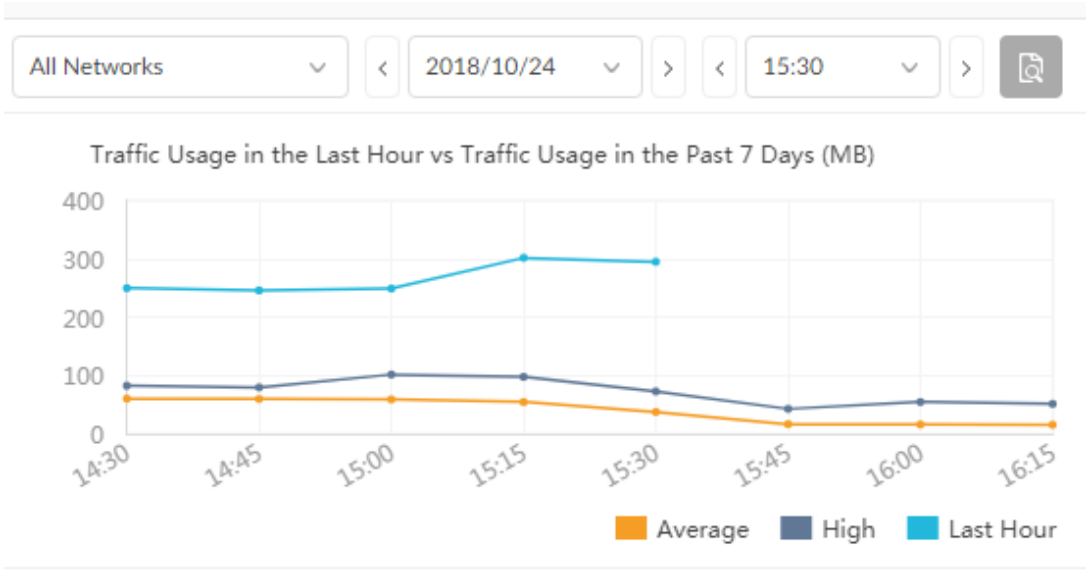






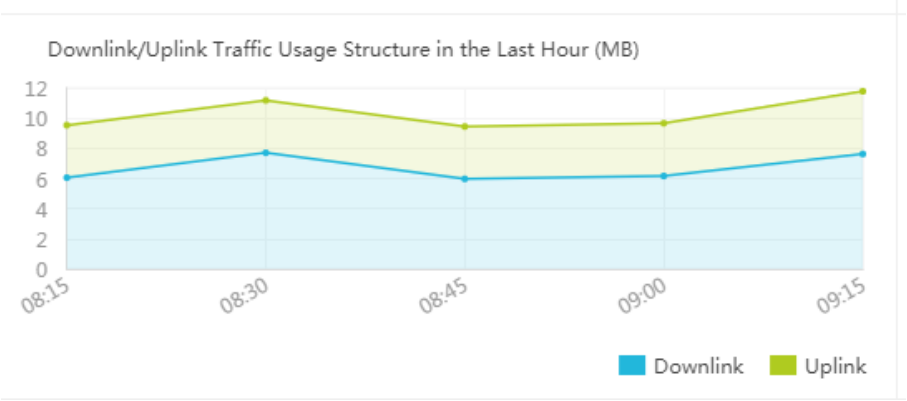
Nuclias Connect Dashboard (Brainstorming Session)

- By default, the blue line, in terms of Traffic Usage, shows the traffic from last hour.
- The below diagram is an indicator showing that "Last Hour" traffic is much (or far) greater than the one from last seven days (both 50% and 25% mark).
- This is an excellent example that the Network Administrator should take a close look whether any parallel events happening at the same time.



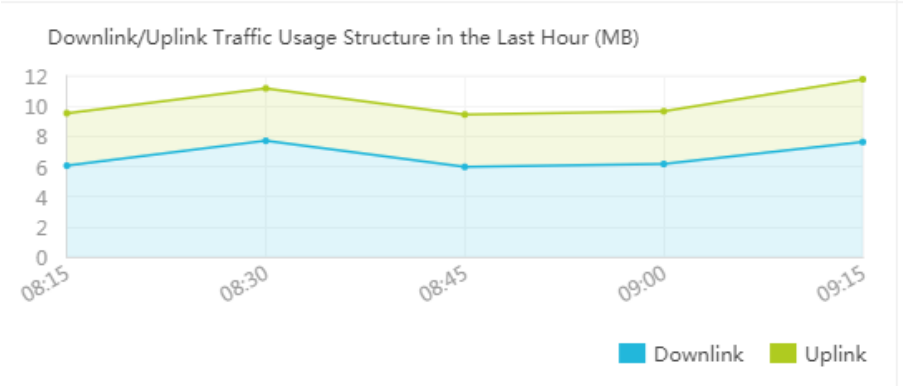
Nuclias Connect Dashboard

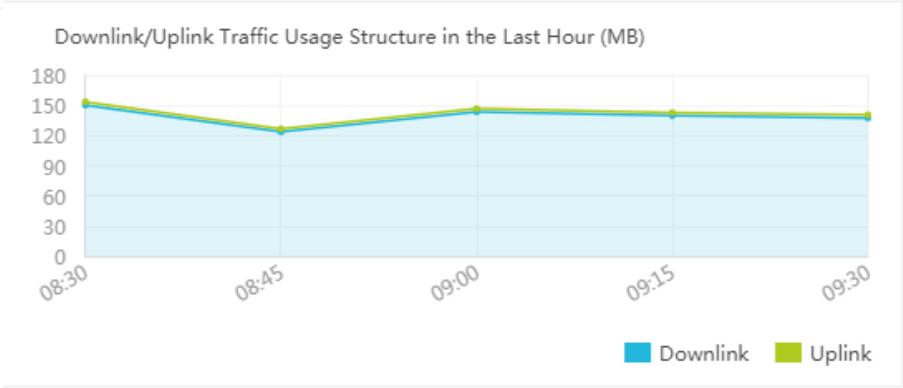
- Accumulated Traffic Usage
  - At 8:15AM, Downlink traffic is around 6 MB where Uplink is about 4 MB (10MB – 6MB) (left hand chart)



Nuclias Connect Dashboard (Brainstorming Session)

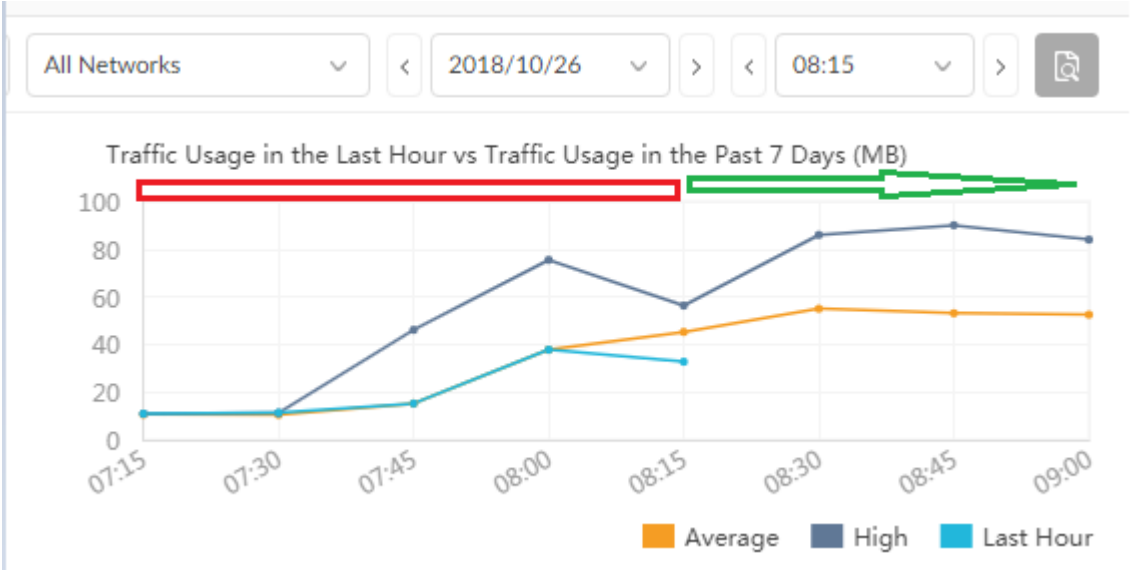
- Accumulated Traffic Usage
  - At 8:15AM, Downlink traffic is around 6 MB where Uplink is about 4 MB (10MB – 6MB) (left hand chart)
  - What would be the proper explanation regarding “Downlink” and “Uplink” traffic displayed in the right hand chart?





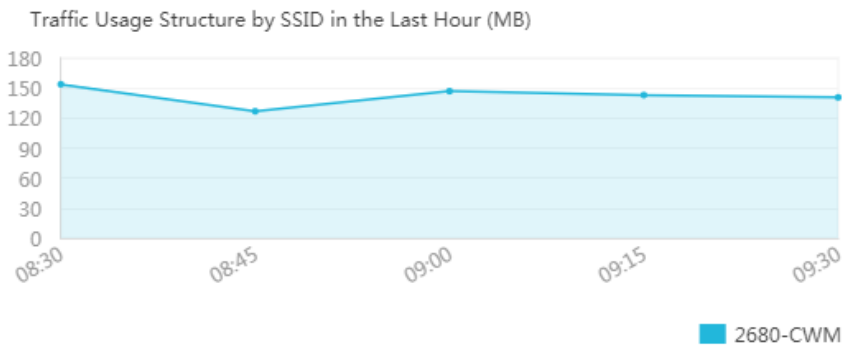
Nuclias Connect Dashboard (Brainstorming Session)

- Traffic Usage
  - Scenario: a Network Admin reports his duty to office around 8:30AM, this is the data shown in Dashboard. What type of expectation he should have in his mind?



Nuclias Connect Dashboard

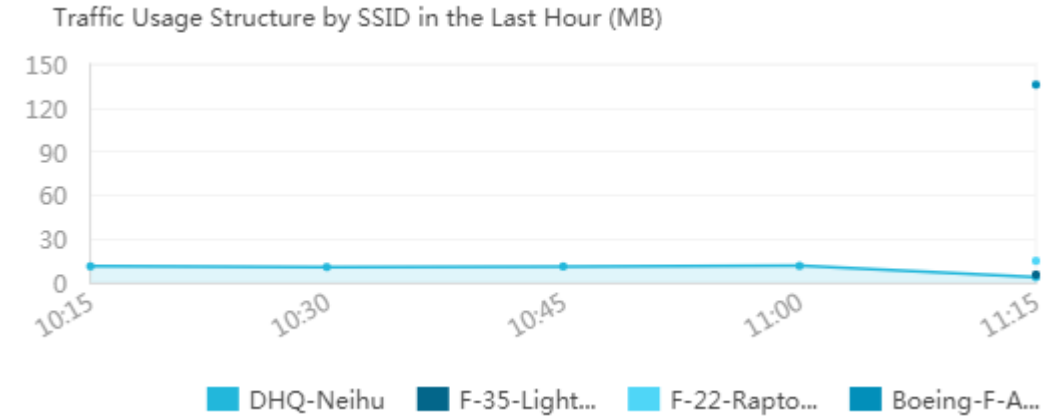
- Traffic Usage Structure by SSID
- The following image screenshot presents the traffic usage where we only have one SSID in our production environment.
  - Name of SSID
  - Coloring Rule
  - Historical Data (Do we see Average / High volume of traffic?)



The objective is to reflect the total wireless traffic sorted by individual SSID

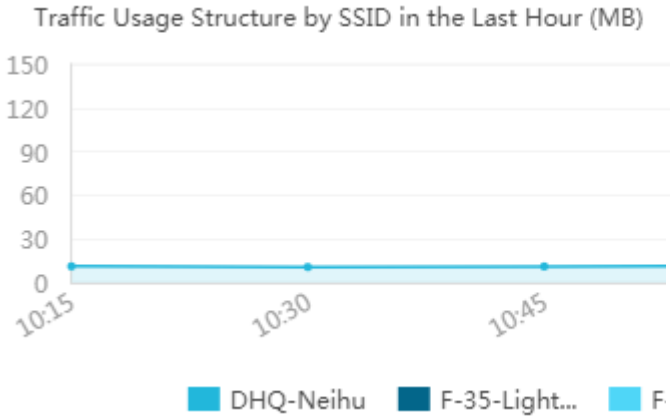
Nuclias Connect Dashboard

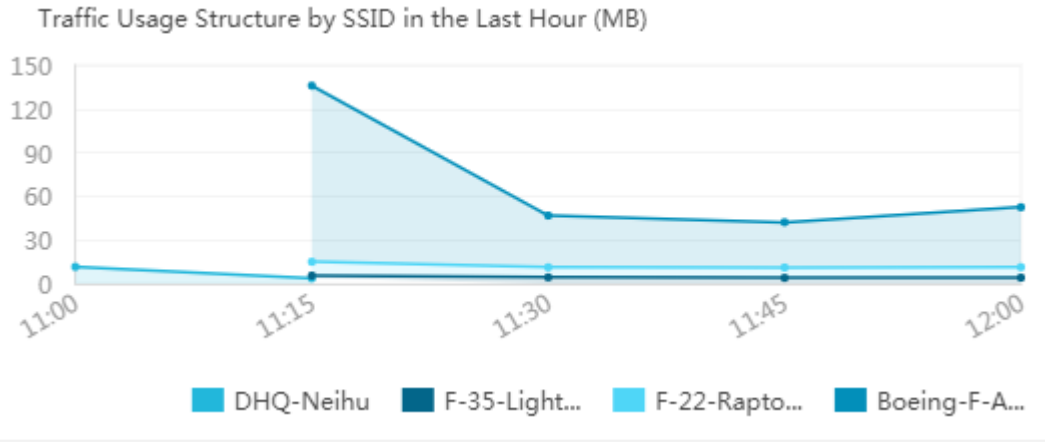
- Implementing multiple SSIDs
- When we have multiple SSIDs in our topology, where we manually assign each wireless client connects to an identical SSID.
- Let’s collect DNC dashboard chart across different times (1/4)



Nuclias Connect Dashboard

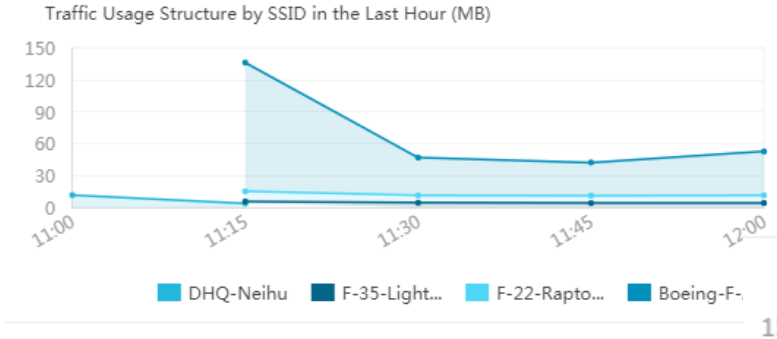
- Implementing multiple SSIDs
- When we have multiple SSIDs in our topology, where we manually assign each wireless client connects to an identical SSID.
- Let’s collect DNC dashboard chart across different times (2/4)

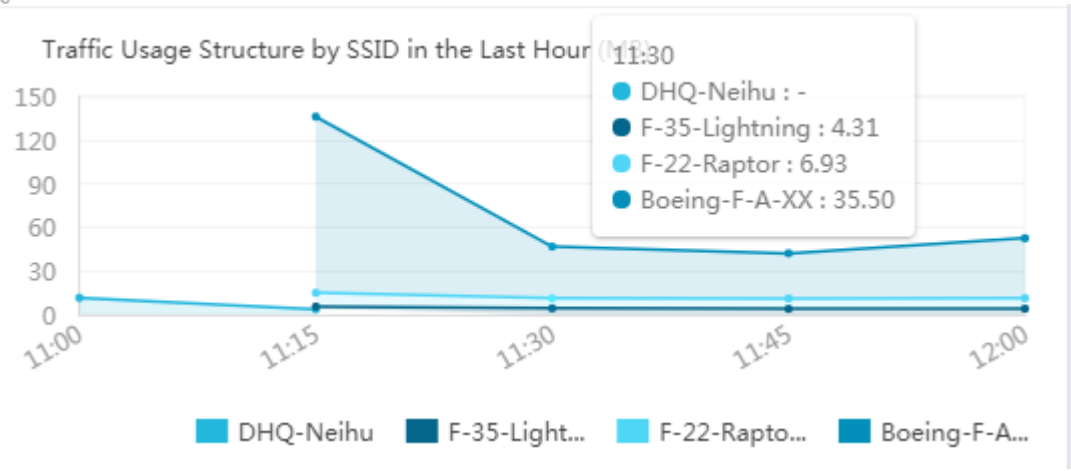




Nuclias Connect Dashboard

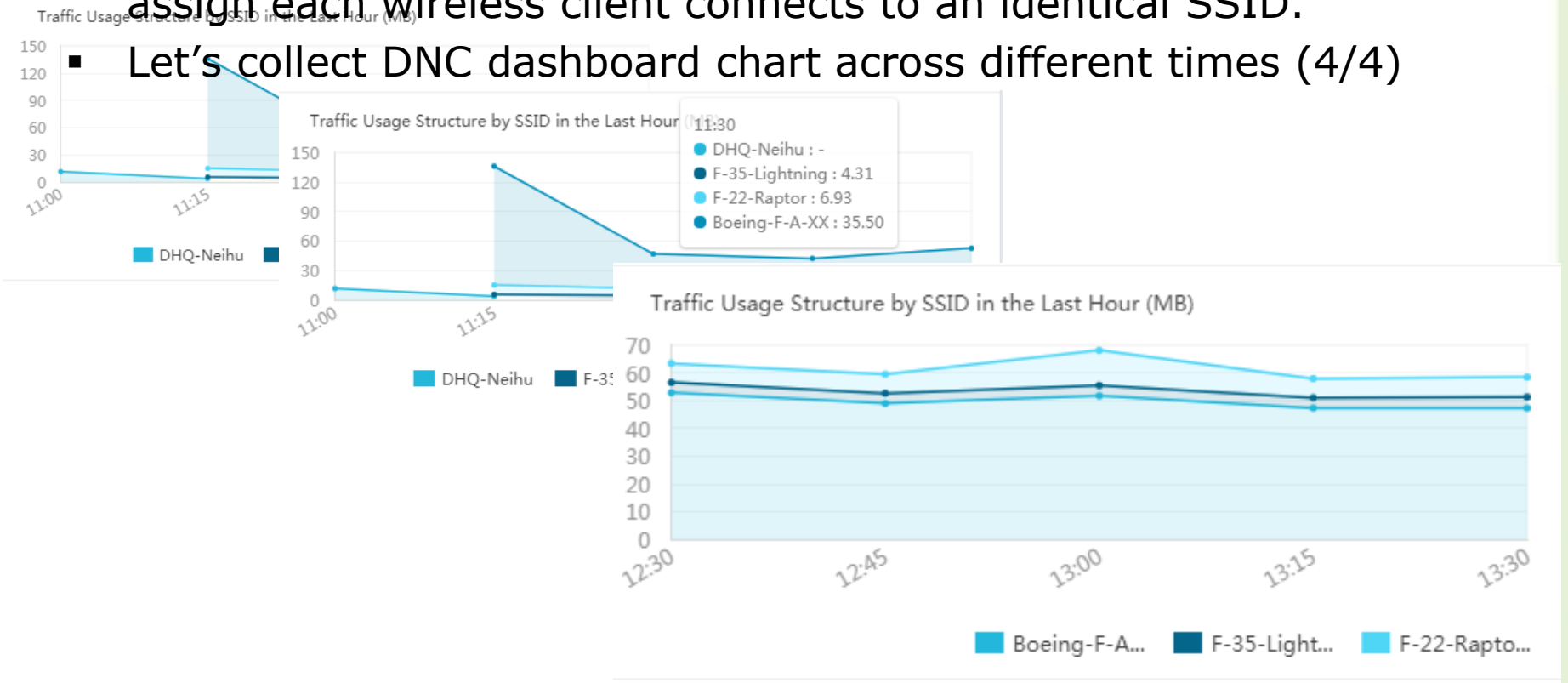
- Implementing multiple SSIDs
- When we have multiple SSIDs in our topology, where we manually assign each wireless client connects to an identical SSID.
- Let’s collect DNC dashboard chart across different times (3/4)





Nuclias Connect Dashboard

- Implementing multiple SSIDs
- When we have multiple SSIDs in our topology, where we manually assign each wireless client connects to an identical SSID.
- Let’s collect DNC dashboard chart across different times (4/4)

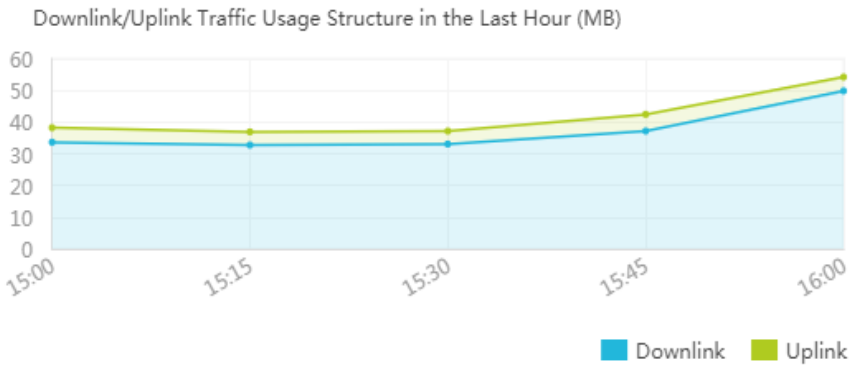


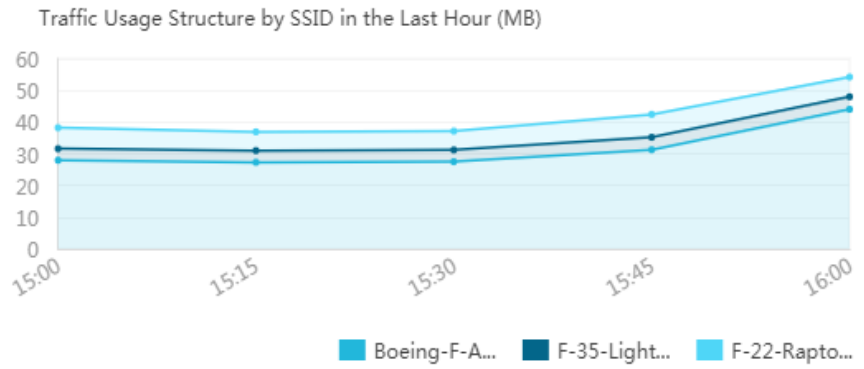
Nuclias Connect Dashboard (Brainstorming Session)

- Implementing multiple SSIDs
- When we have multiple SSIDs in our topology, where we manually assign each wireless client connects to an identical SSID.
  - Is the traffic being presented in an accumulated way?
  - Do we find easy to distinguish one thing from another?

Nuclias Connect Dashboard (Relationship Between Sets Of Data, 1/3)

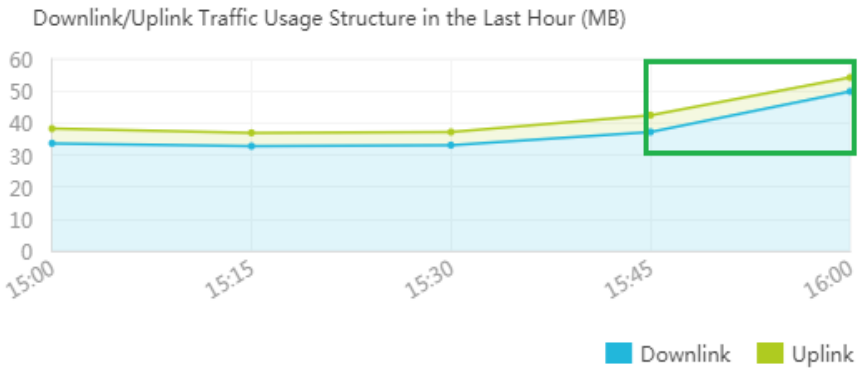
- A correlation between two variables when the effects of one or more related variables are in a direct correlation, positive correlation, or irrelevant conditions.
- Traffic usage, by downlink/uplink and SSID.

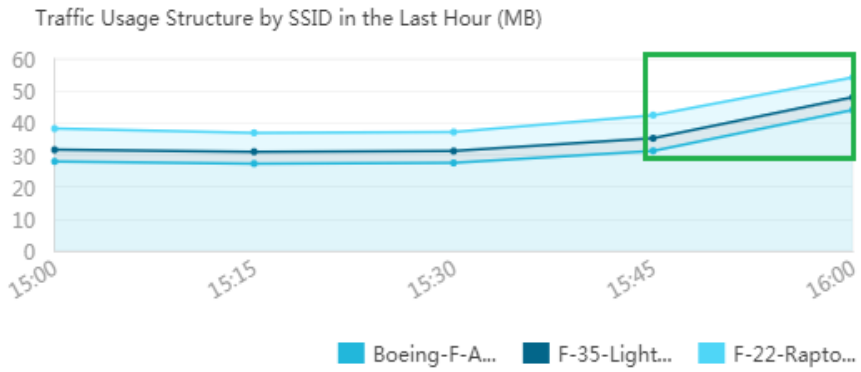




Nuclias Connect Dashboard (Relationship Between Sets Of Data, 2/3)

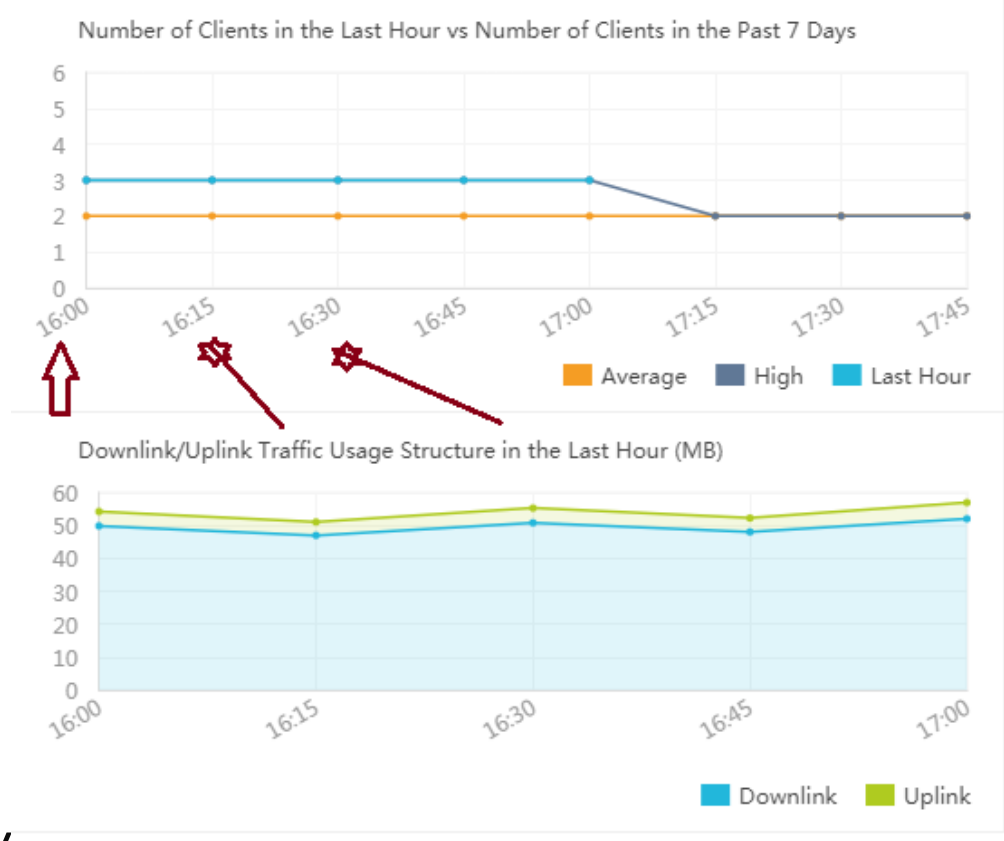
- Traffic usage, by downlink/uplink and SSID
- A stable increase from 15:30PM to 15:45PM, followed by steep speedy from 15:45PM to 16:00PM.
- The symptoms are close to evenly distributed.





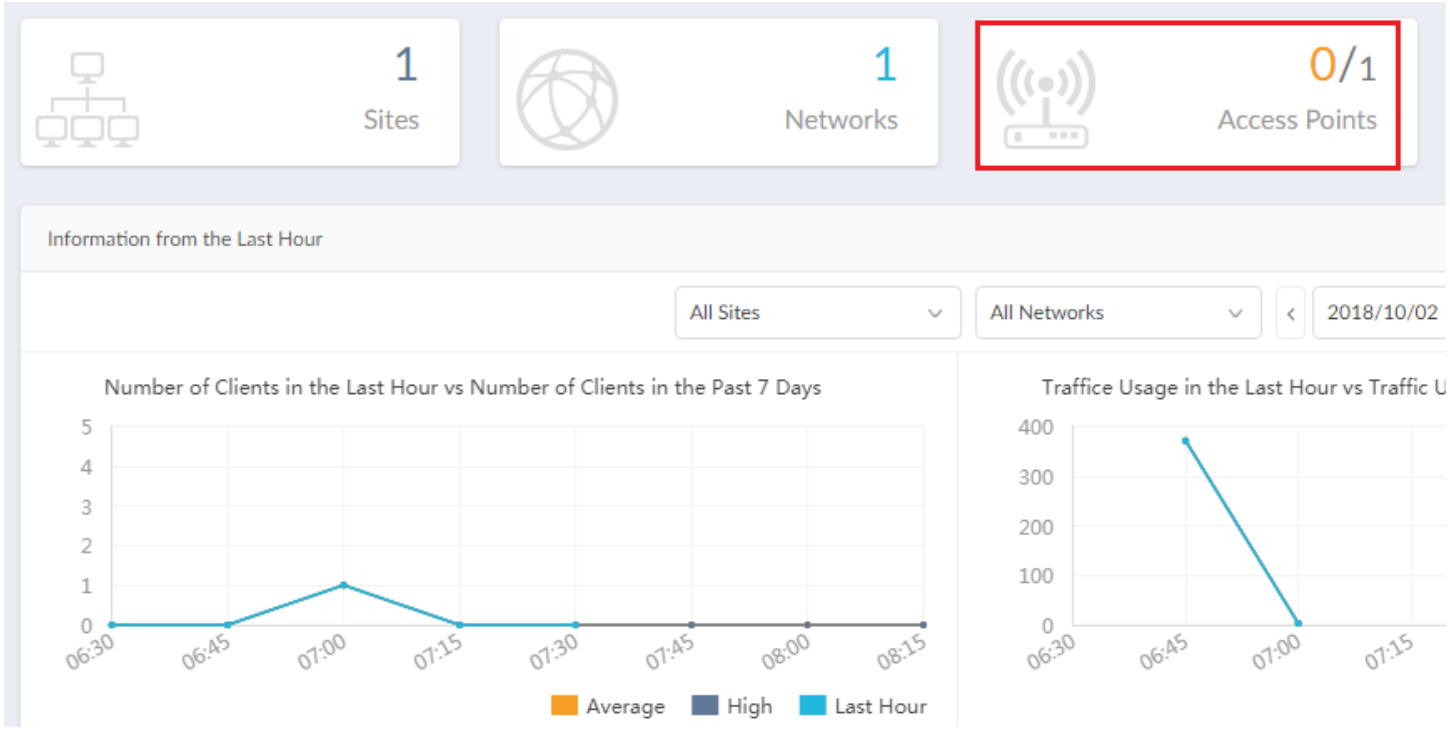
Nuclias Connect Dashboard (Relationship Between Sets Of Data, 3/3)

- Traffic usage by downlink/uplink vs. the number of wireless clients
- Network traffic is occupied by the similar amount of wireless stations.



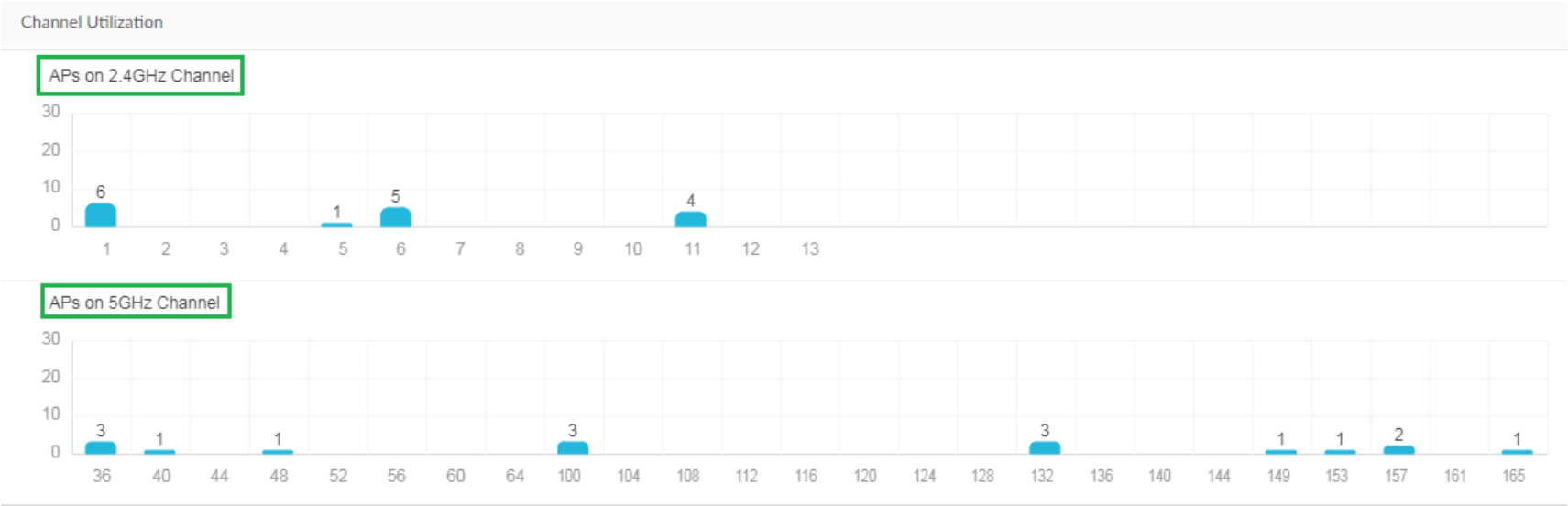
Nuclias Connect Dashboard

- As indicated in below image, since there is no AP connecting to our network, the number of clients should be “Zero”.



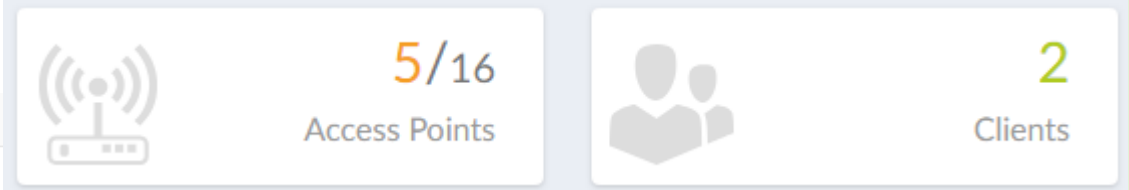
Nuclias Connect Dashboard

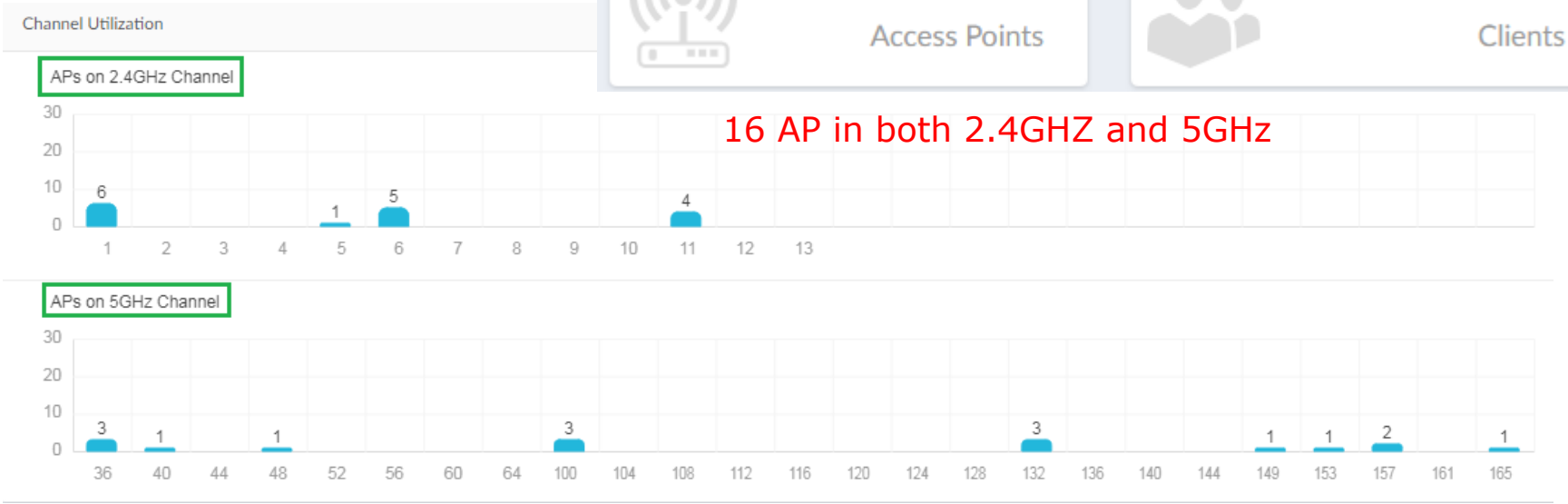
- DNC Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
  - Channel utilization
    - AP on 2.4 / 5 Ghz channel utilization
  - Syslog events



Nuclias Connect Dashboard

- DNC Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
  - Channel utilization
    - AP on 2.4 / 5 Ghz channel utilization
  - Syslog events

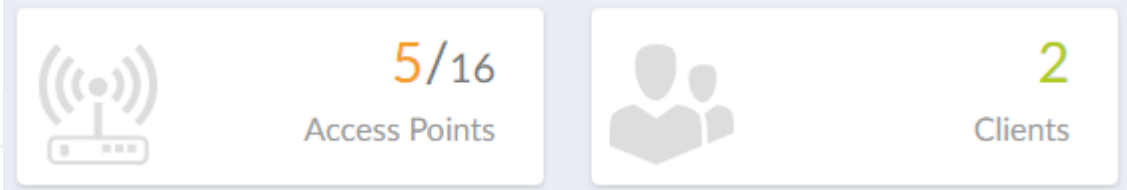


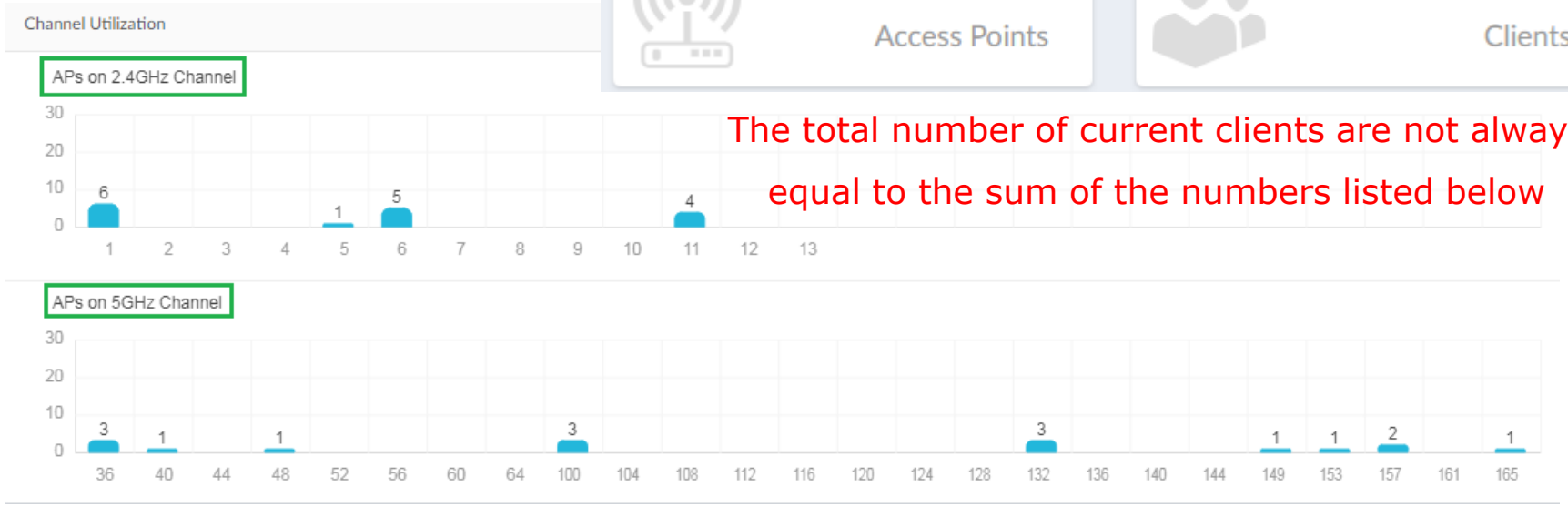


16 AP in both 2.4GHZ and 5GHz

Nuclias Connect Dashboard

- DNC Dashboard provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
  - Channel utilization
    - AP on 2.4 / 5 Ghz channel utilization
  - Syslog events





The total number of current clients are not always equal to the sum of the numbers listed below

Nuclias Connect Dashboard

- From viewpoint of “Wireless Summary Report”
- This page provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
  - Channel utilization
  - Syslog events
    - Device Management
    - Duplicate Task
    - Timeout Task
    - Invalid HTTP Message
    - Initialization

Nuclias Connect Dashboard

- From viewpoint of "Wireless Summary Report"
- This page provides information about the D-Link DAP wireless network, including some of the following statistics
  - Information from the last hour
  - Channel utilization
  - Syslog events
    - Device Management
    - Duplicate Task
    - Timeout Task
    - Invalid HTTP Message
    - Initialization

Nuclias Connect can redirect all syslog (AP and DNC) to another external syslog server

Nuclias Connect Dashboard, Event Management

- "Device Management" event log
- Event Indication: should any un-supported device sends out messages, such as registration, boarding, and/or keep-alive, Nuclias Connect will once again confirm its settings. Should there is any non-supported network / DAP models, Nuclias Connect will break the tie and issue such event
- The content of the log
  - Reject the device's connection due to registration's\ boarding's\ keep alive network does not exist
  - Reject the device's connection due to registration's\ boarding's model is not supported
- Should the end user experiences a situation where DAP already being managed by Nuclias Connect, and then, this Nuclias Connect server is required to update its IP address. (before DNC IP update, Boarding will be the ONLY status during DAP device discovery)

Nuclias Connect Dashboard, Event Management

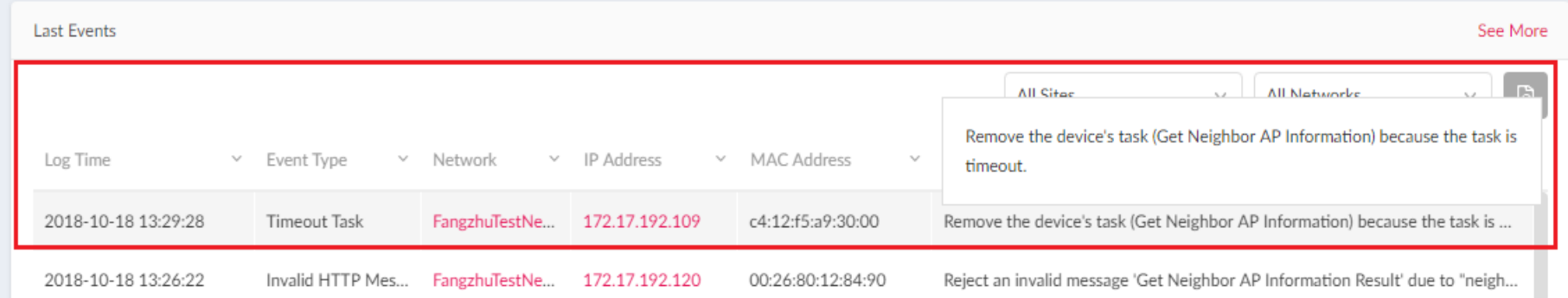
- “Duplicate Task” event log
- Event Indication: When a Nuclias Connect operator intends to deploy the same configurations to managed APs, it (Nuclias Connect) will only take the very last task and then dispatch configuration parameters to managed DAPs. For any intended task occurred in between, DNC would make a note in the system, but not to distribute to managed devices.
- The content of the log
  - Remove the previous task ("<function>") since the same task will be sent out to the device once

Nuclias Connect Dashboard, Event Management

- “Timeout Task” event log
- Event Indication: When a DNC intends to distribute some configurations to devices, where those devices are not able to acknowledge whether those change being taken effect
- The content of the log
  - Remove the device's task ("<Function>") because the task is timeout

Nuclias Connect Dashboard, Event Management

- "Timeout Task" event log



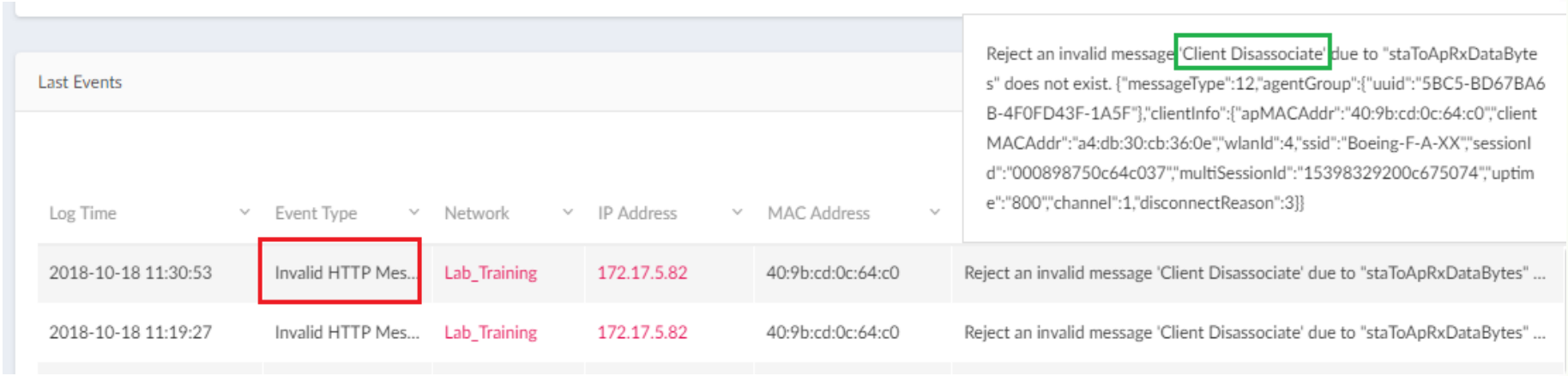
- DNC Dashboard Event Type: Get Neighbor AP Information (SSID or Network Name, IP Address, MAC address) task timeout

Nuclias Connect Dashboard, Event Management

- "Invalid HTTP Message" event log
- Event Indication: When a DAP plans to send messages to DNC, DNC would verify whether those messages are legitimate. The chosen criteria consists of "The sequence of registration process" "Any missing column in transferring message" "Data type error" as well as "Unrecognized message"
- The content of the log
  - Reject device due to receive an invalid message {json}. Current Stage is "None | Reg Init | Reg Done | Boarding Init | Boarding Done | Normal | Unmanaged".
  - Reject an invalid message "<http msg>" due to "<item>" does not exist. {json}
  - Reject an invalid message "<http msg>" due to "<item>" data type is incorrect. {json}
  - Reject an unknown message. {json}

Nuclias Connect Dashboard, Event Management

- "Invalid HTTP Message" event log



- Wireless client disassociation (Note: Are you seeing your wireless clients repeatedly disconnects and reconnects to Wi-Fi Network?)

Nuclias Connect Dashboard, Event Management

- "Initialization" event log
- Event Indication: Once a DNC has started in progress, should there be any issues that need to be clarified, an "Initialization" event log would be recorded.
- The content of the log
  - Fail to get the system data (network list, model list and keep-alive interval)
  - The system data (network list, model list and keep-alive interval) is empty
  - Get the network Configuration, Firmware, SSL Certification data failed
  - The network Configuration, Firmware, SSL Certification data is/are empty

The Design Thinking of Dashboard and Report

- Design Thinking
- Nuclias Connect Dashboard
- Nuclias Connect Management Report

Nuclias Connect Management Report

Nuclias Connect offers the following 4 types of reports

- Peak Network Activity
- Most Active AP
- Hourly Network Activity
- Daily Network Activity

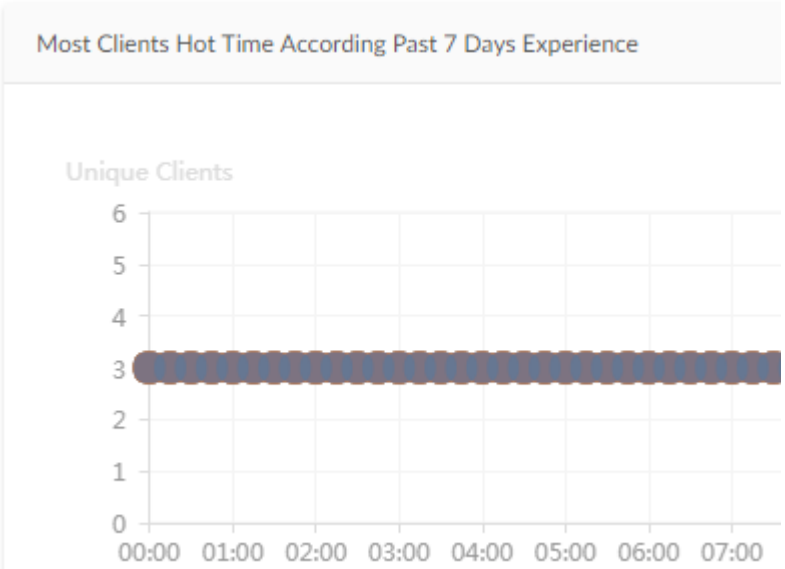
Nuclias Connect Management Report

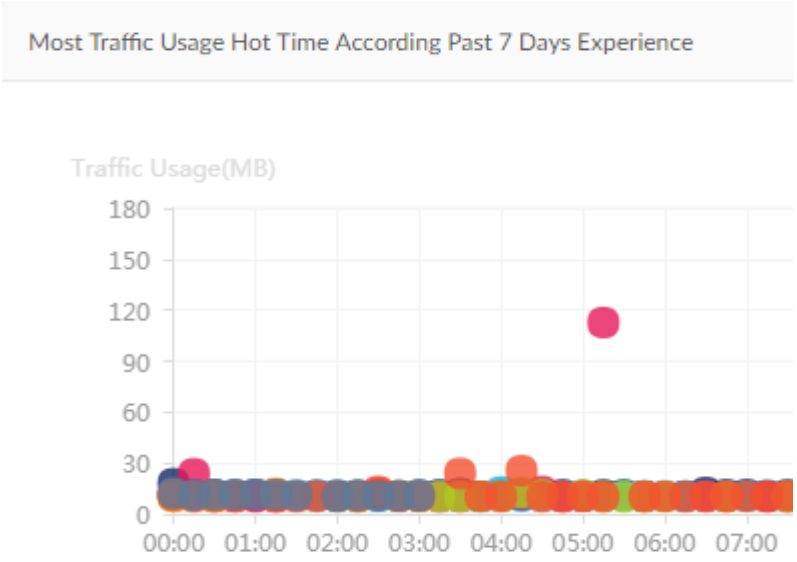
Nuclias Connect offers the following 4 types of reports

- Peak Network Activity
- Most Active AP
- Hourly Network Activity
- Daily Network Activity

Peak Network Activity

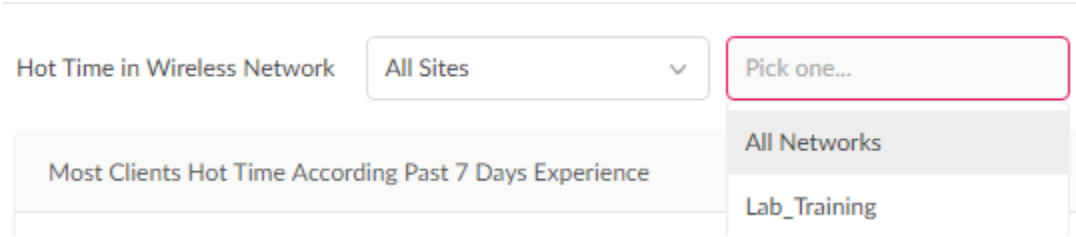
- "Topics to Watch"
  - Number of clients distributed in Wireless Hotspot (Chart Title: Most Clients Hot Time)
  - The wireless network traffic populated in Wireless Hotspot (Chart Title: Most Traffic Usage Hot Time)
  - With 15-min time frame



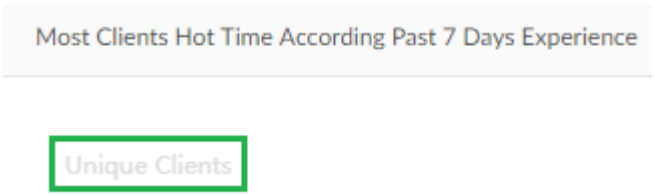


Peak Network Activity

- "Topics to Watch"
- The sum of a complete set of data, with the flexibility to make query either by "Site" or "Network".

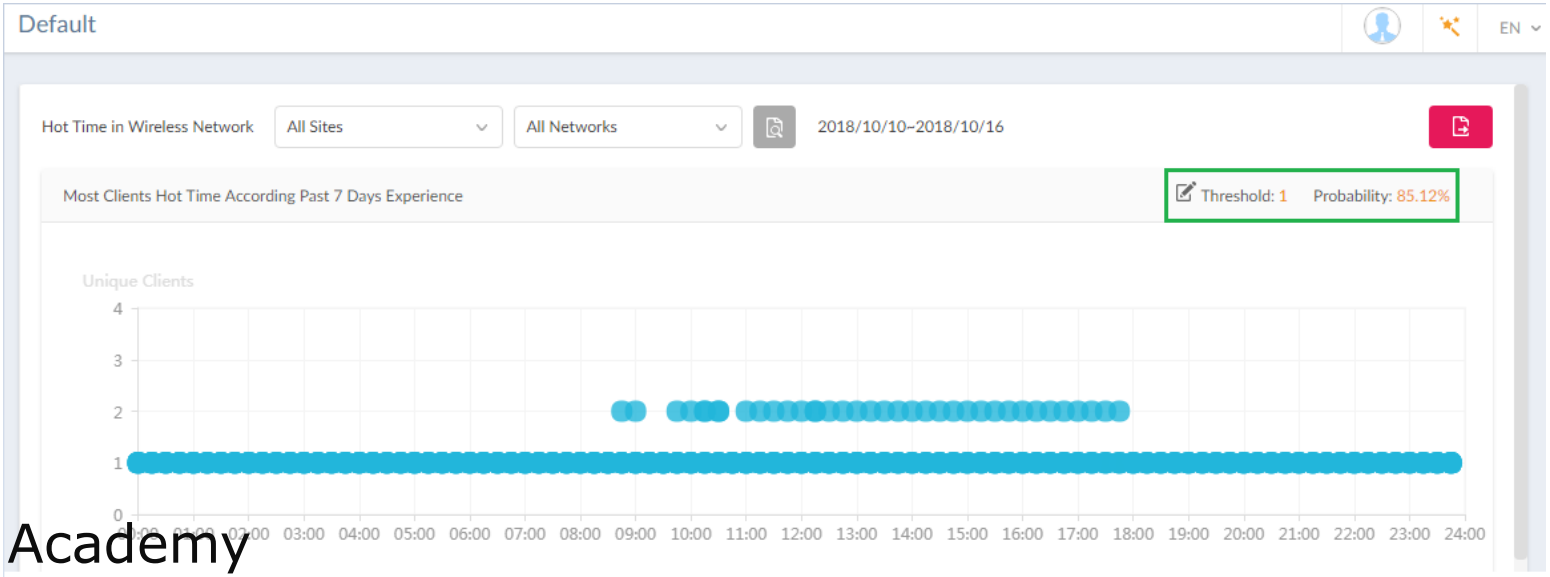


- Time frequency: 7 days for the current version, where 30-days and 90-days data collection are planned in future release.
- Individual wireless station (STA) refers to "unique client".



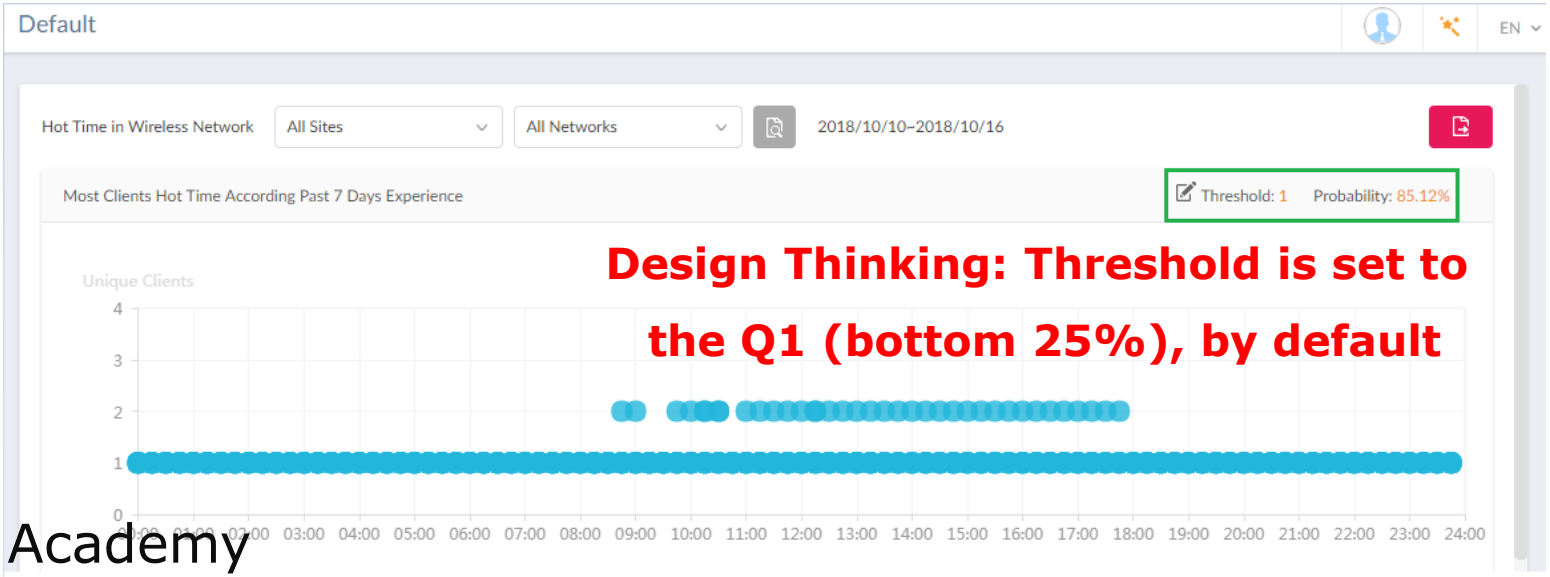
Peak Network Activity

- In Reporting, Threshold represents
  - The boundary beyond which a radically different state of affairs exists.
  - The minimum value which serves as a benchmark for comparison.
- In Reporting, Probability is a quantifiable likelihood (chance) of the occurrence of an event is equal to or more than Threshold value.



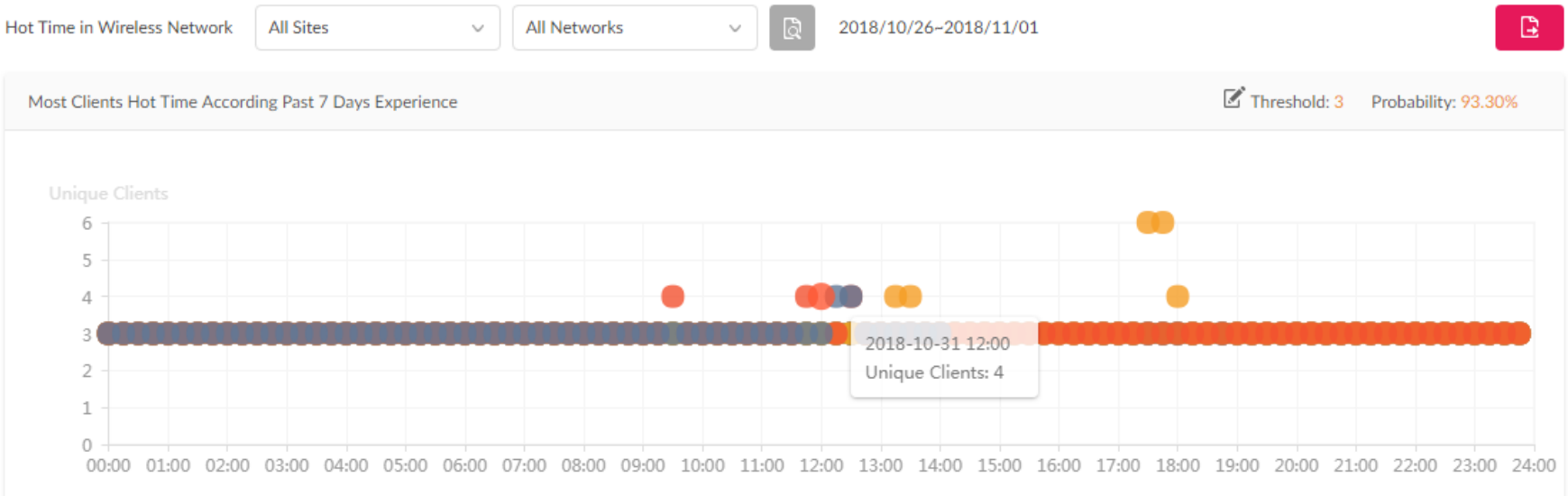
Peak Network Activity

- In Reporting, Threshold represents
  - The boundary beyond which a radically different state of affairs exists.
  - The minimum value which serves as a benchmark for comparison.
- In Reporting, Probability is a quantifiable likelihood (chance) of the occurrence of an event is equal to or more than Threshold value.



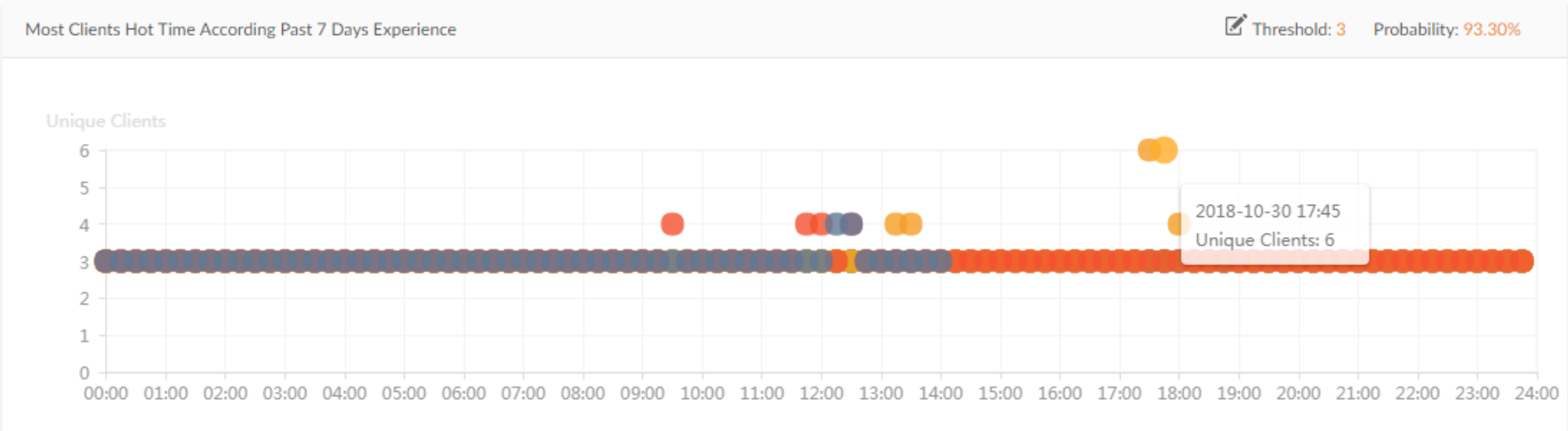
Peak Network Activity (Live Example I, 1/4)

- Most Clients Hot Time According Past 7 Days Experience
- By taking the last 7 days collected data, we have realized that
  - 3 unique wireless station (STA) are the most common instance
  - There are occasions that from 09:00AM to 14:00PM, we may experience 4 unique wireless station, which is 33% increase [(4-3)/3 = 33%]



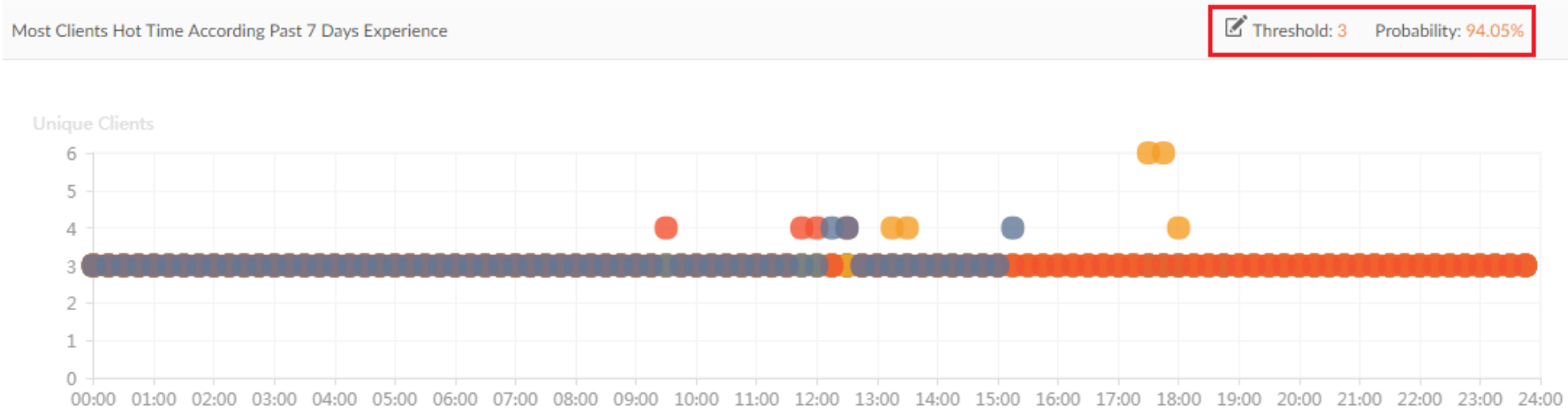
Peak Network Activity (Live Example I, 2/4)

- Most Clients Hot Time According Past 7 Days Experience
- By taking the last 7 days collected data, we have realized that
  - 3 unique wireless station (STA) are the most common instance
  - On Oct. 30, around 17:45PM, we do see 6 unique wireless station in communication exchange. [(6-3)/3 = 100% increase]
    - Two iPHONEs and One Android phone were working on Nuclias Connect mobile app then



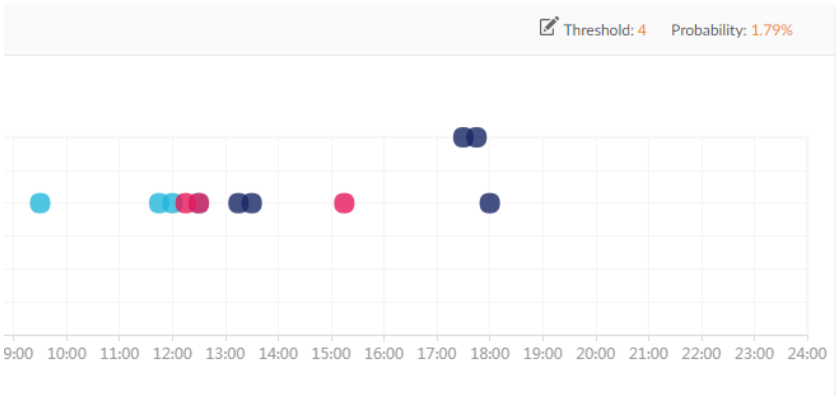
Peak Network Activity (Live Example I, 3/4)

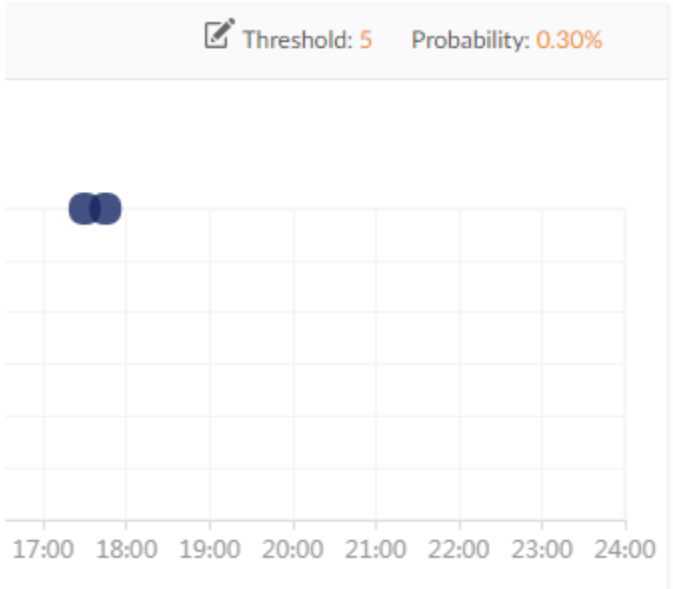
- Most Clients Hot Time According Past 7 Days Experience
- By taking the last 7 days collected data, we have realized that
  - The possibility of greater than or equal to 3 unique wireless station is around 94%.



Peak Network Activity (Live Example I, 4/4)

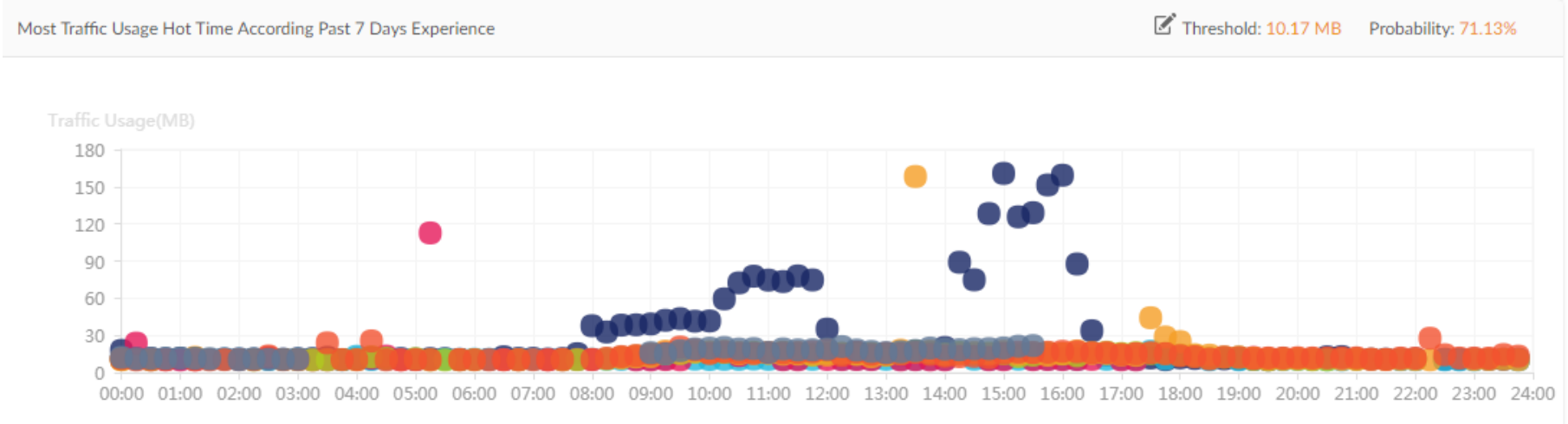
- Most Clients Hot Time According Past 7 Days Experience
- By taking the last 7 days collected data, we have realized that
  - Greater than or equal to 4 unique wireless station: 1.79%
  - Greater than or equal to 5 unique wireless station: 0.3%





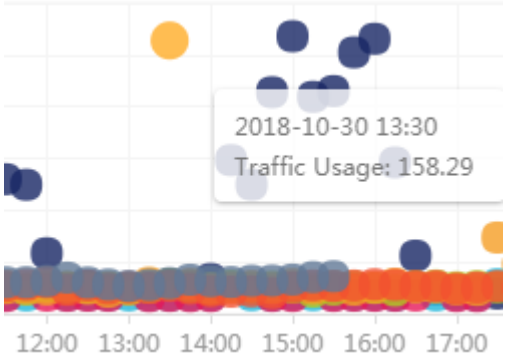
Peak Network Activity (Live Example II, 1/4)

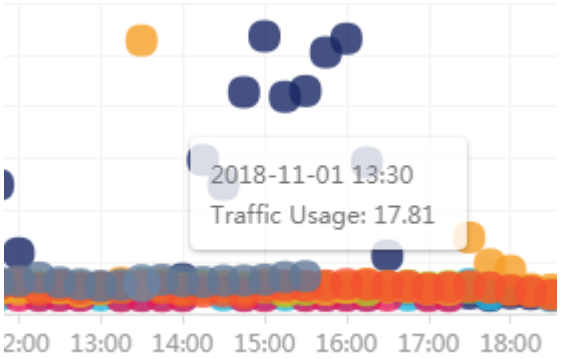
- Most Traffic Usage Hot Time According Past 7 Days Experience
- Let’s capture a few screen shots here and make an explanation



Peak Network Activity (Live Example II, 2/4)

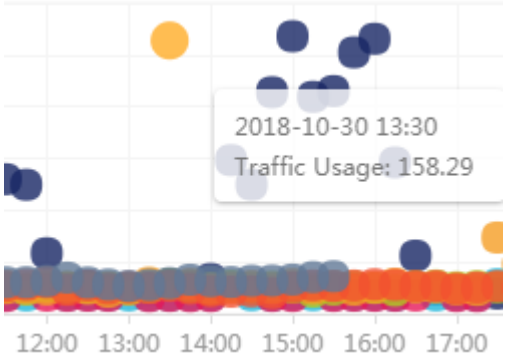
- Most Traffic Usage Hot Time According Past 7 Days Experience
- Let’s capture a few screen shots here and make an explanation

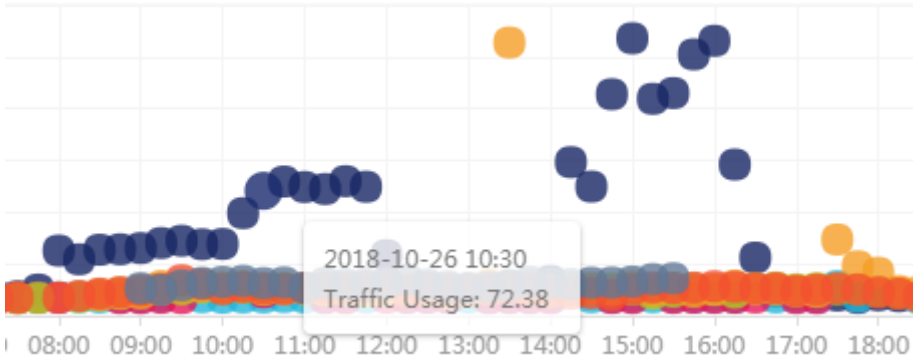


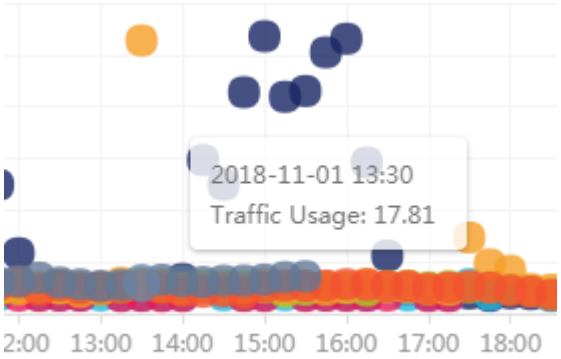


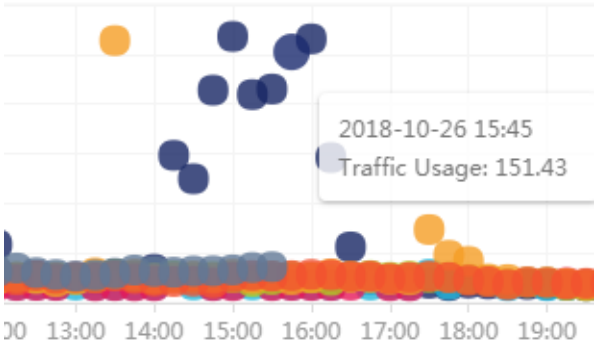
Peak Network Activity (Live Example II, 3/4)

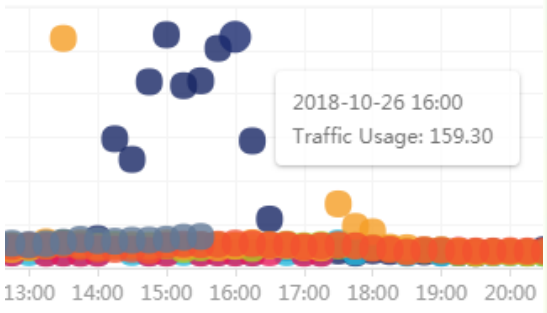
- Most Traffic Usage Hot Time According Past 7 Days Experience
- Let’s capture a few screen shots here and make an explanation





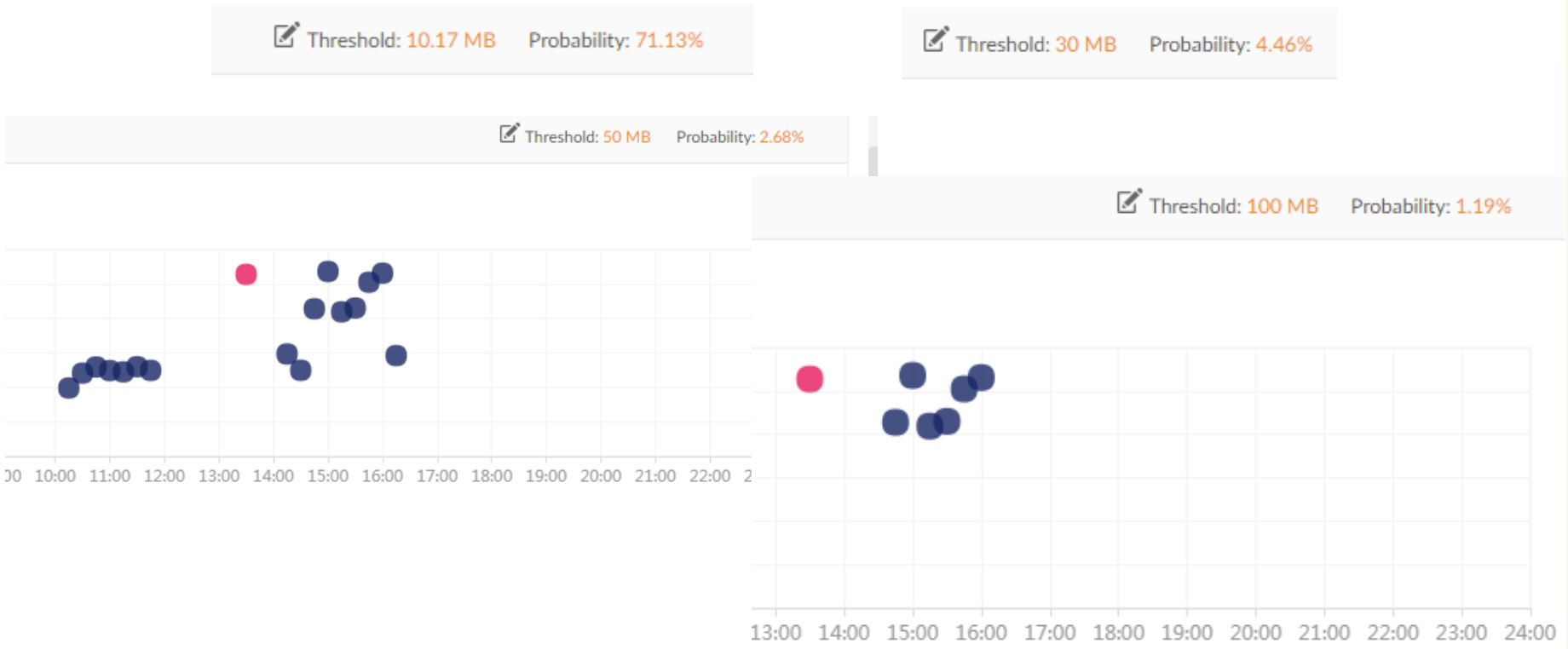






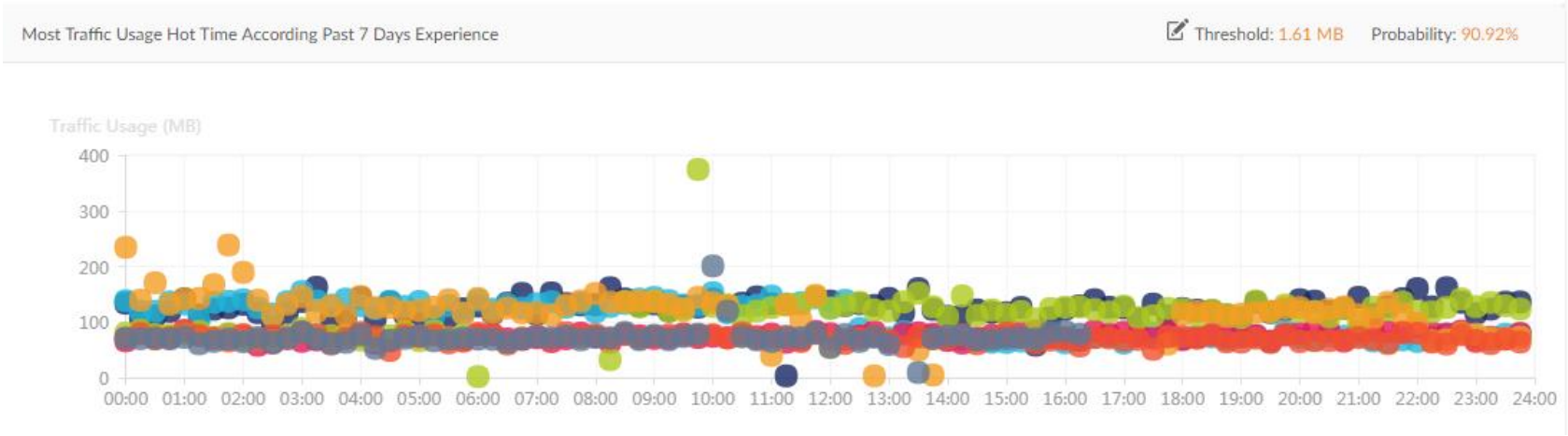
Peak Network Activity (Live Example II, 4/4)

- Most Traffic Usage Hot Time According Past 7 Days Experience
- Let’s capture a few screen shots here and make an explanation



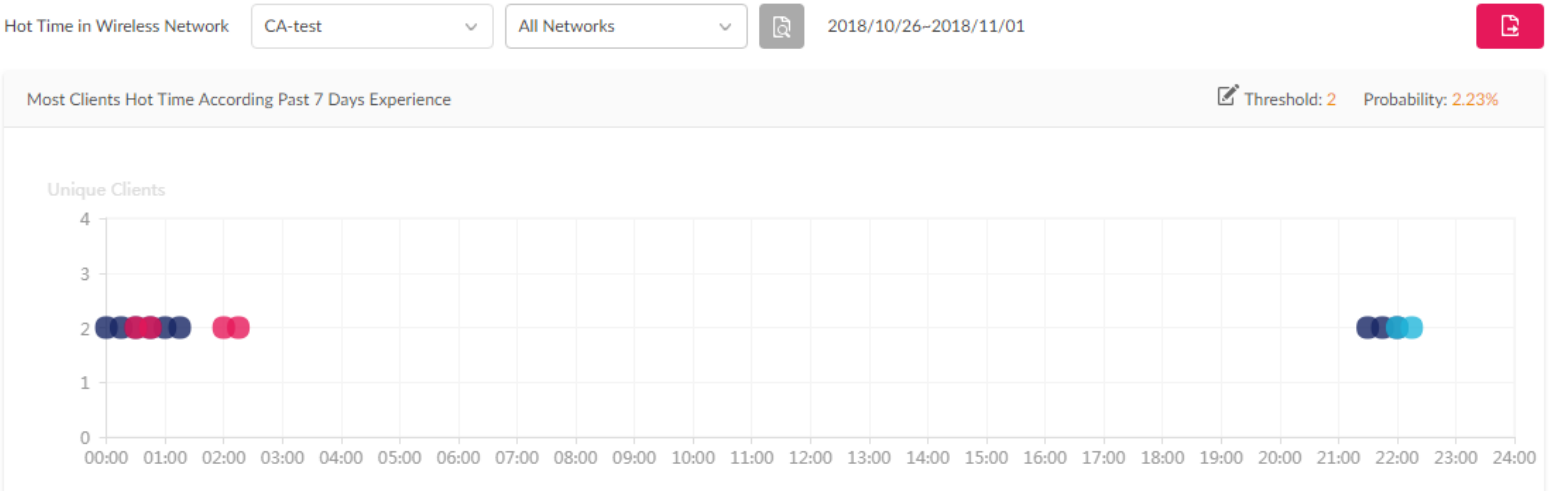
Peak Network Activity (From WLAN Network Management Perspective)

- With the latest 7-day (for current Nuclias Connect release) historical data and real-time utilization, DNC makes a clear disclosure whether additional Wireless AP (D-Link DAP) should come up the stage to deliver services.
- What is the network traffic load during the busiest hours?



Peak Network Activity (From WLAN Network Management Perspective)

- With the latest 7-day (for current Nuclias Connect release) historical data and real-time utilization, DNC makes a clear disclosure whether additional Wireless AP (D-Link DAP) should come up the stage to deliver services.
- What is the network traffic load during the busiest hours?
- Are we seeing more or less wireless stations outside normal business hours?

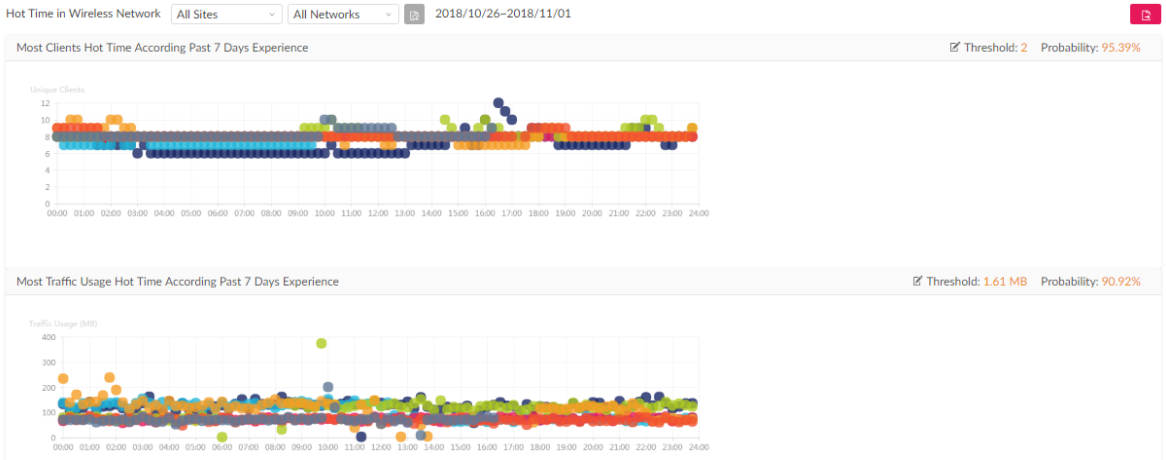


Peak Network Activity (From WLAN Network Management Perspective)

- With the latest 7-day (for current Nuclias Connect release) historical data and real-time utilization, DNC makes a clear disclosure whether additional Wireless AP (D-Link DAP) should come up the stage to deliver services.
- What is the network traffic load during the busiest hours?
- Are we seeing more or less wireless stations outside normal business hours?
- What is the period of peak congestion that may last for more than one hour?
- With the concept of "Relationship Between Sets Of Data" as stated earlier, are we seeing two variables (number of clients & wireless traffic usage) have a positive association / correlation?

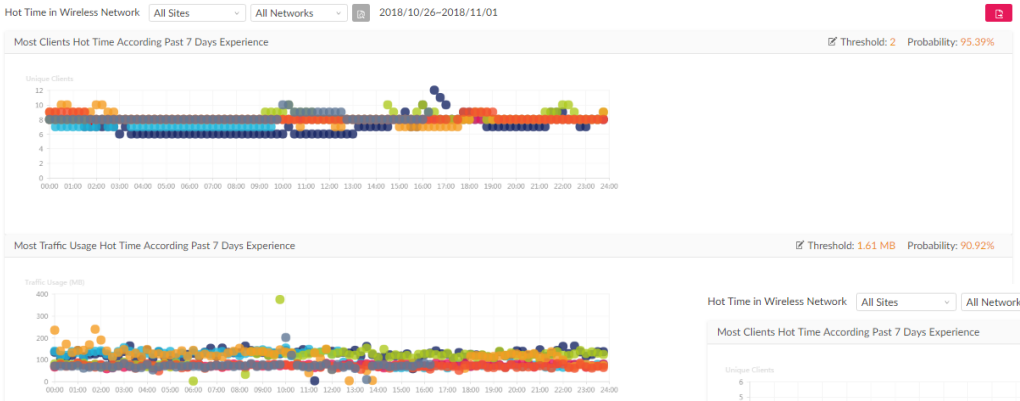
Peak Network Activity (From WLAN Network Management Perspective)

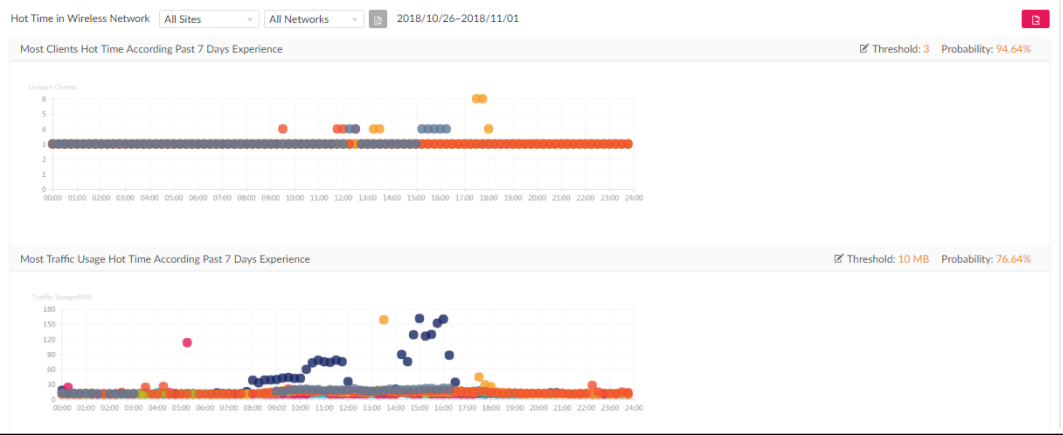
- With the latest 7-day (for current Nuclias Connect release)…..
- With the concept of "Relationship Between Sets Of Data" as stated earlier, are we seeing two variables (number of clients & wireless traffic usage) have a positive association / correlation?
  - 2 clients/1.6 MB vs. 3 clients/10 MB



Peak Network Activity (From WLAN Network Management Perspective)

- With the latest 7-day (for current Nuclias Connect release)…..
- With the concept of "Relationship Between Sets Of Data" as stated earlier, are we seeing two variables (number of clients & wireless traffic usage) have a positive association / correlation?
  - 2 clients/1.6 MB vs. 3 clients/10 MB





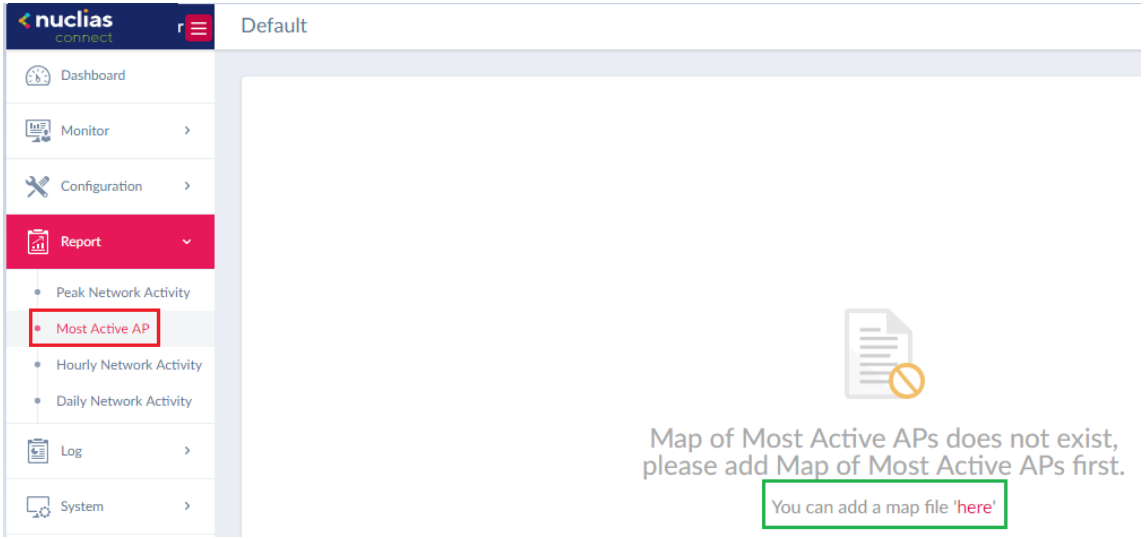
Nuclias Connect Management Report

Nuclias Connect offers the following 4 types of reports

- Peak Network Activity
- Most Active AP
- Hourly Network Activity
- Daily Network Activity

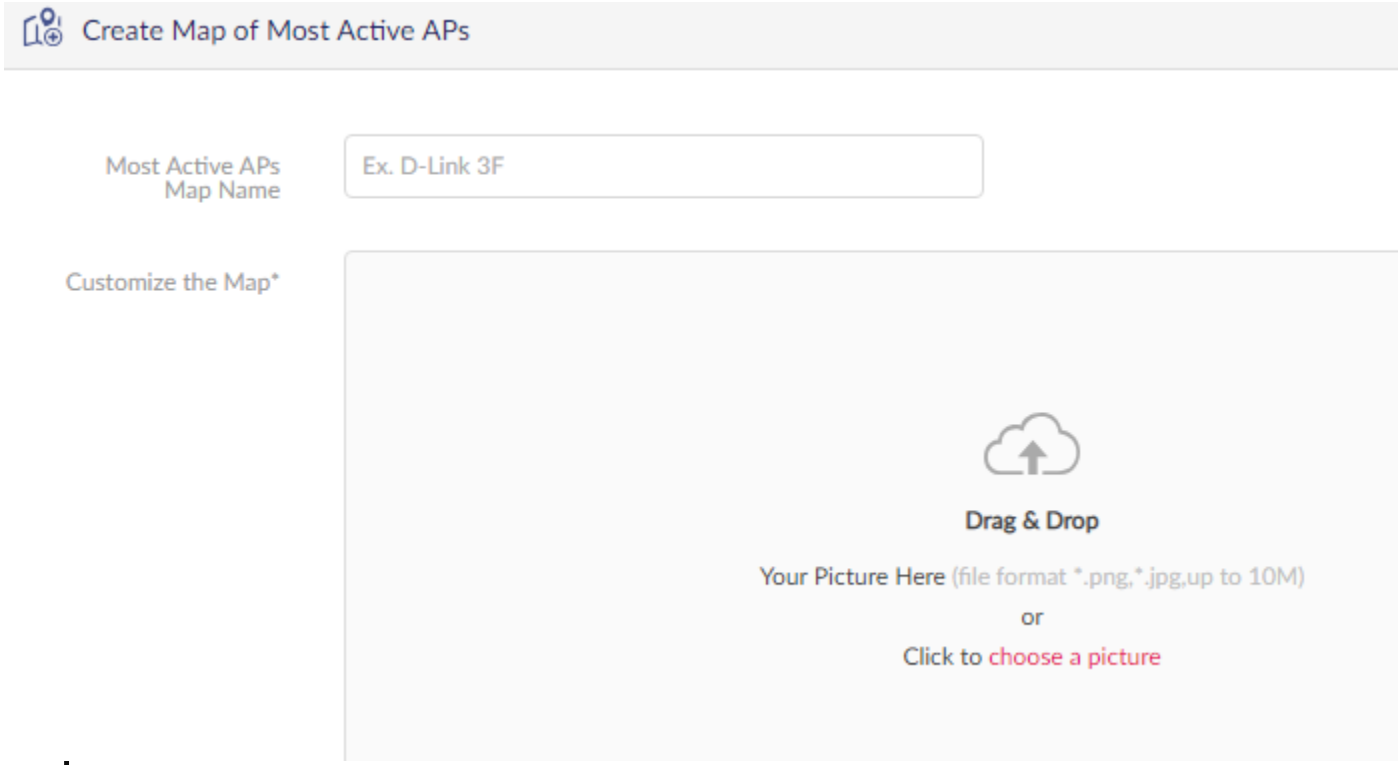
Most Active AP, Wireless Site Maps (1/7)

- Objective: to place APs in Wireless Site Maps for better visualization
- Menu: Report > Most Active AP



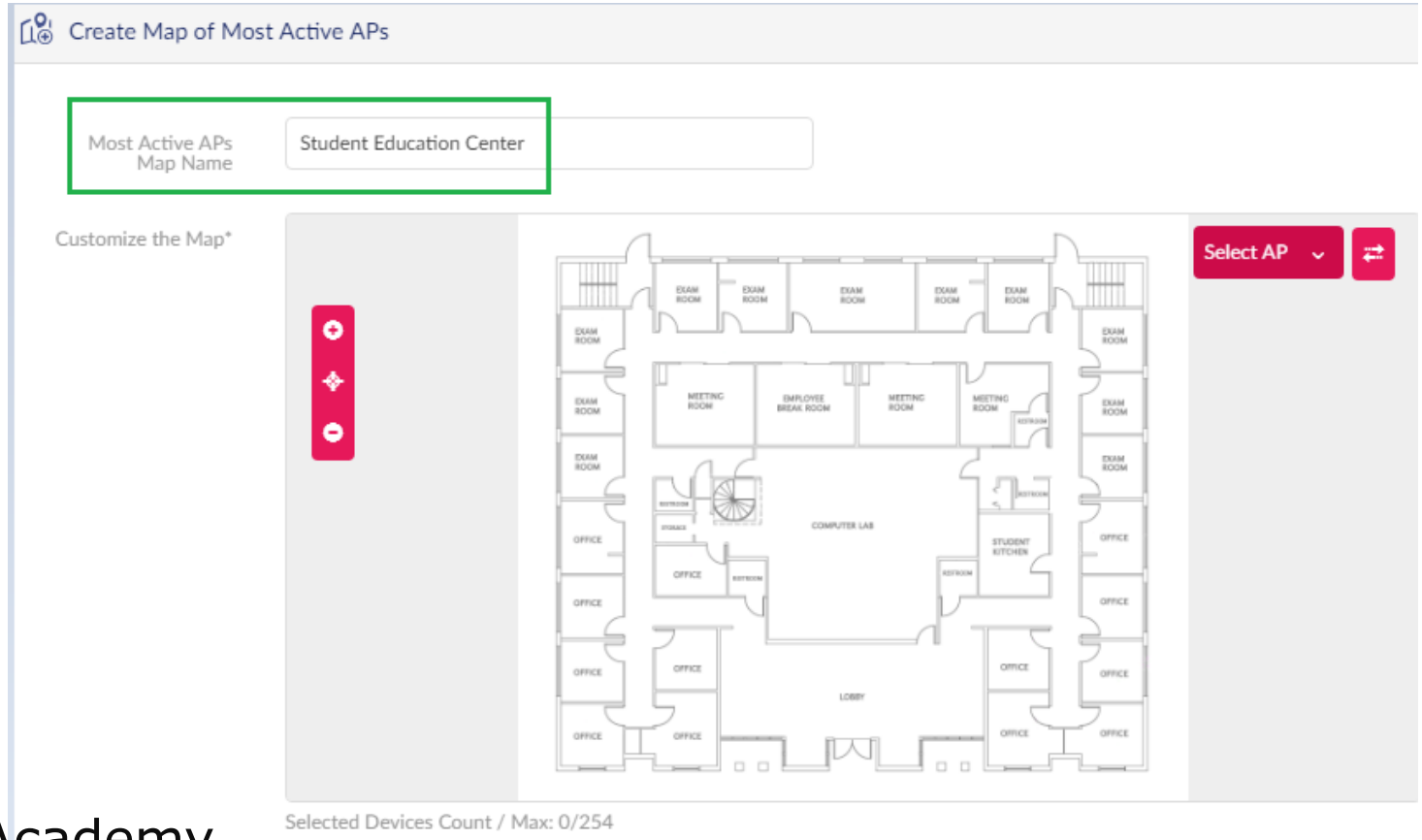
Most Active AP, Wireless Site Maps (2/7)

- Wireless Site Maps configurations
- Menu: Report > Most Active AP
  - Choose an image diagram from the folder



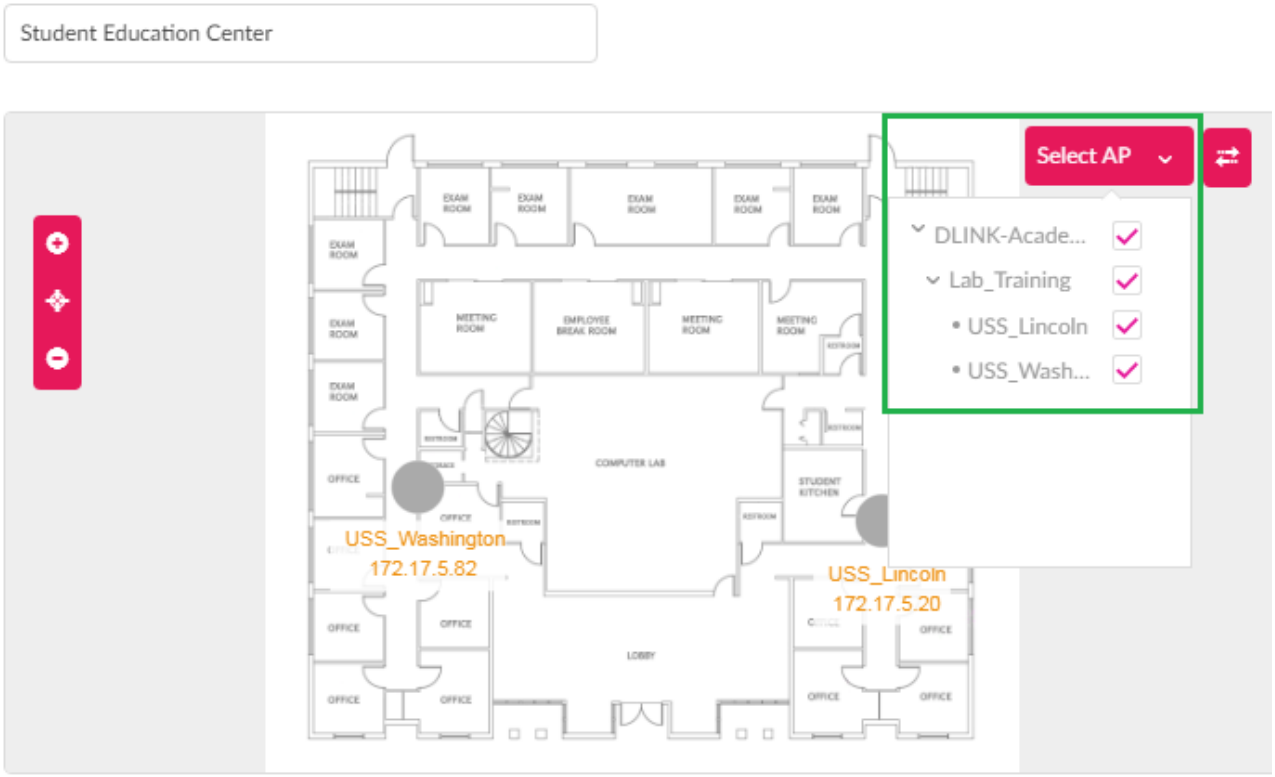
Most Active AP, Wireless Site Maps (3/7)

- Configure name description in the column of “Most Active APs Map Name” (in this example, we use “Student Education Center”)



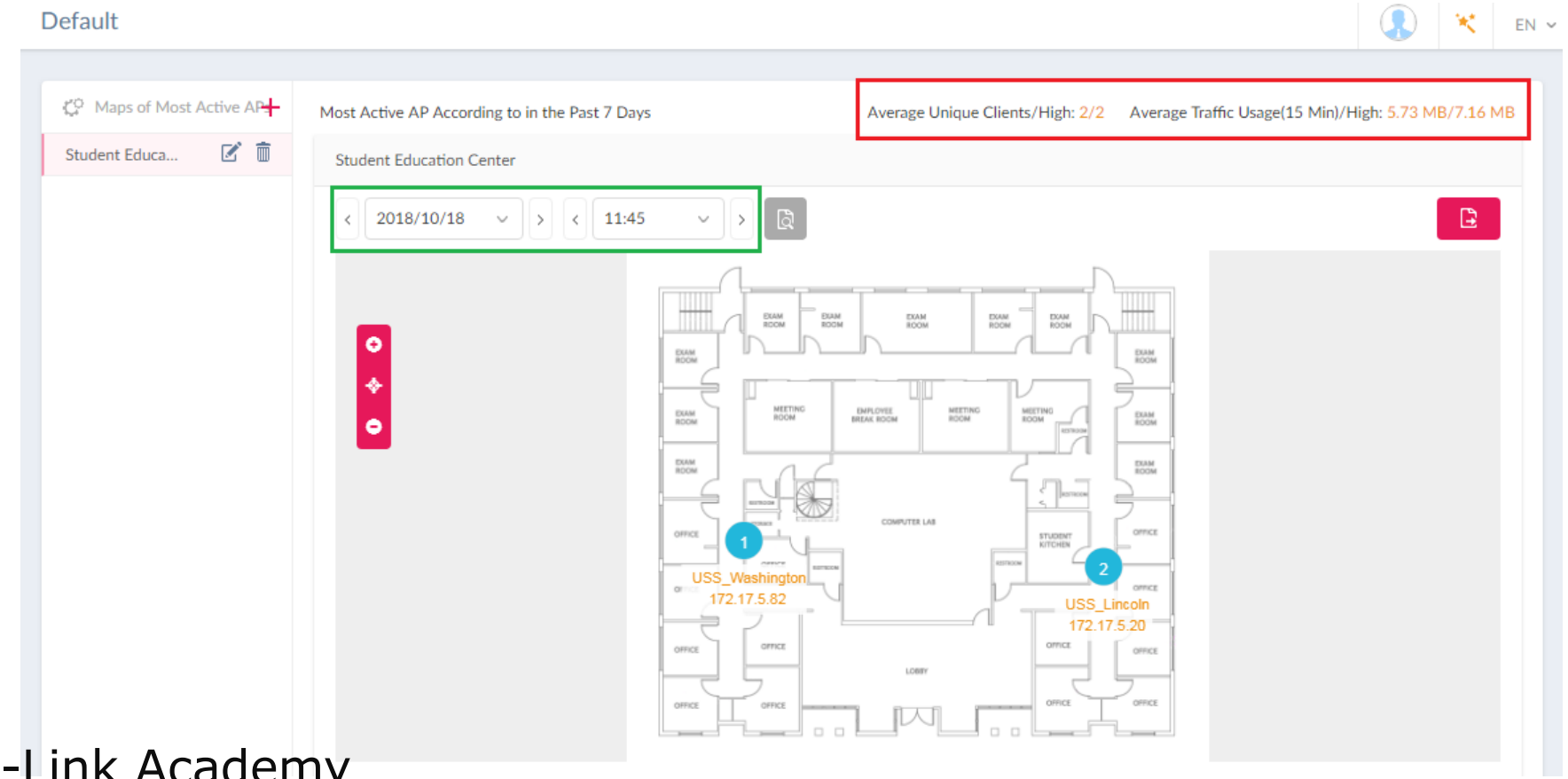
Most Active AP, Wireless Site Maps (4/7)

- Select AP to be inserted into this diagram
  - Two AP (DAP-2680) being selected and click “Save”



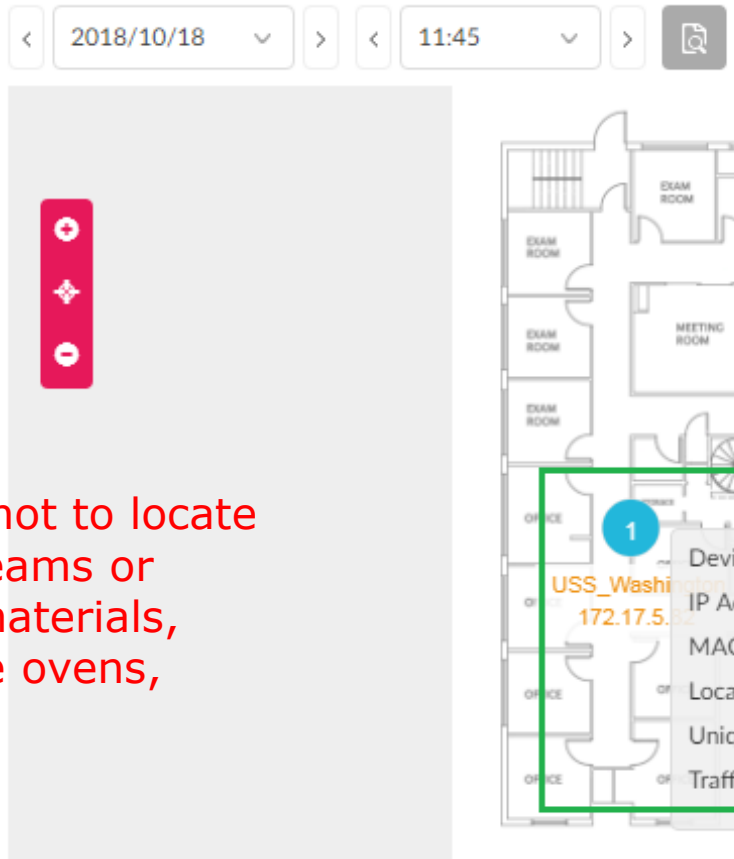
Most Active AP, Wireless Site Maps (5/7)

- Return to main menu (Report > Most Active AP) to review latest output



Most Active AP, Wireless Site Maps (6/7)

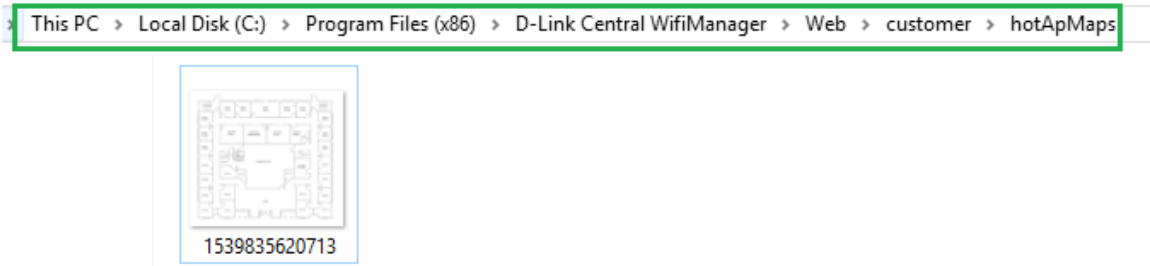
- By simply moving the mouse close the AP icon, then we should be able to view more information on specific AP.



It is best practice not to locate DAPs near steel beams or other interfering materials, such as microwave ovens, electrical conduits.

Most Active AP, Wireless Site Maps (7/7)

- Should we plan to view where this image file is located in DNC server, the following sketch could offers assistance.



Wireless Site Maps (another example)

- After inputting “Neihu-Taipei” in its column, apply the profile. Then, in Report > Most Active AP, the information shall be carried out.



Most Active AP

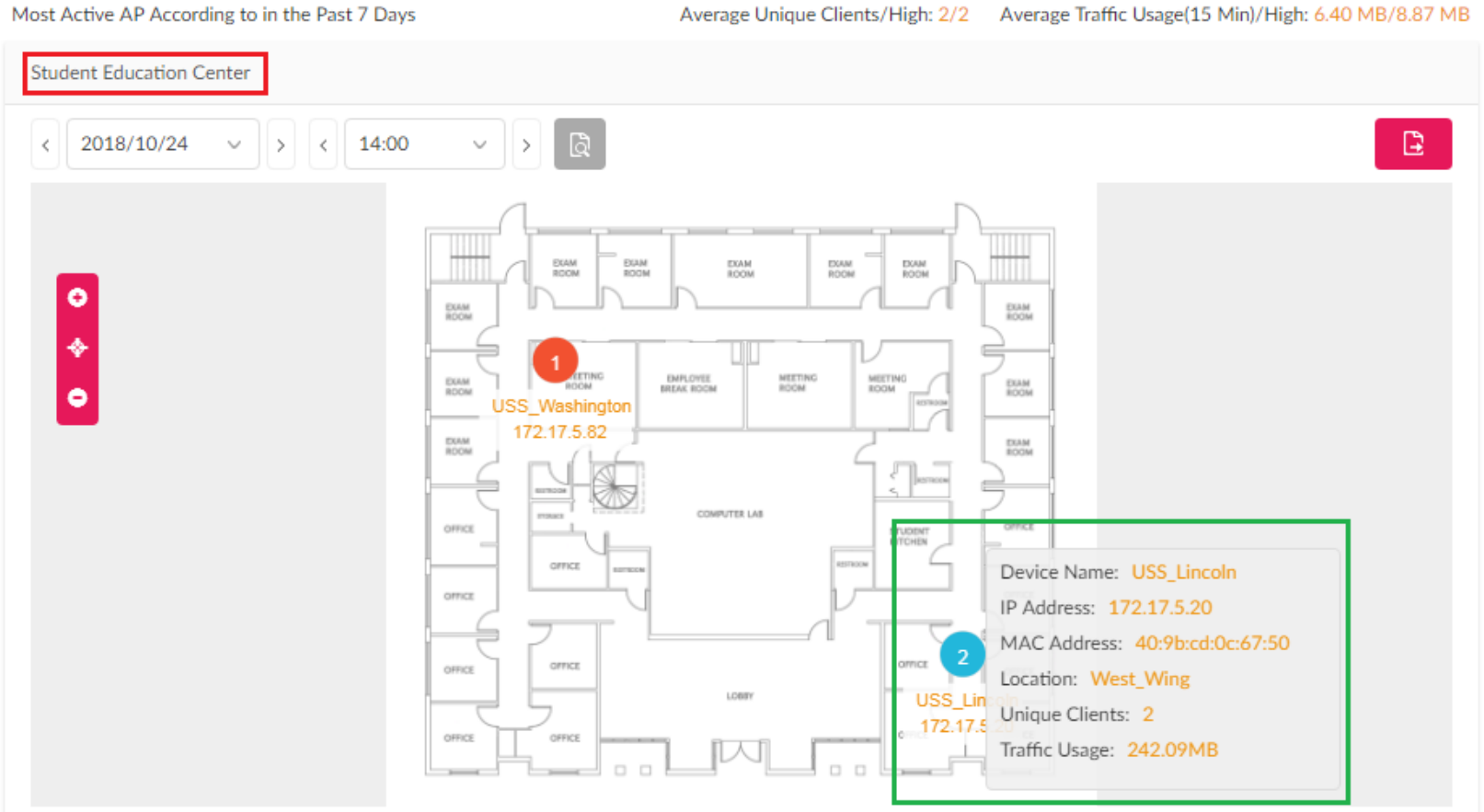
- Show individual AP in different color according traffic usage.
  - APs traffic usage exceed High threshold, then show it in Red color.
  - APs traffic usage exceed Average threshold and lower than High threshold. Then shows it in Green color.
  - APs traffic is lower than Average threshold than shows in Blue color.

3-month data, the "Average & High" from Design Thinking



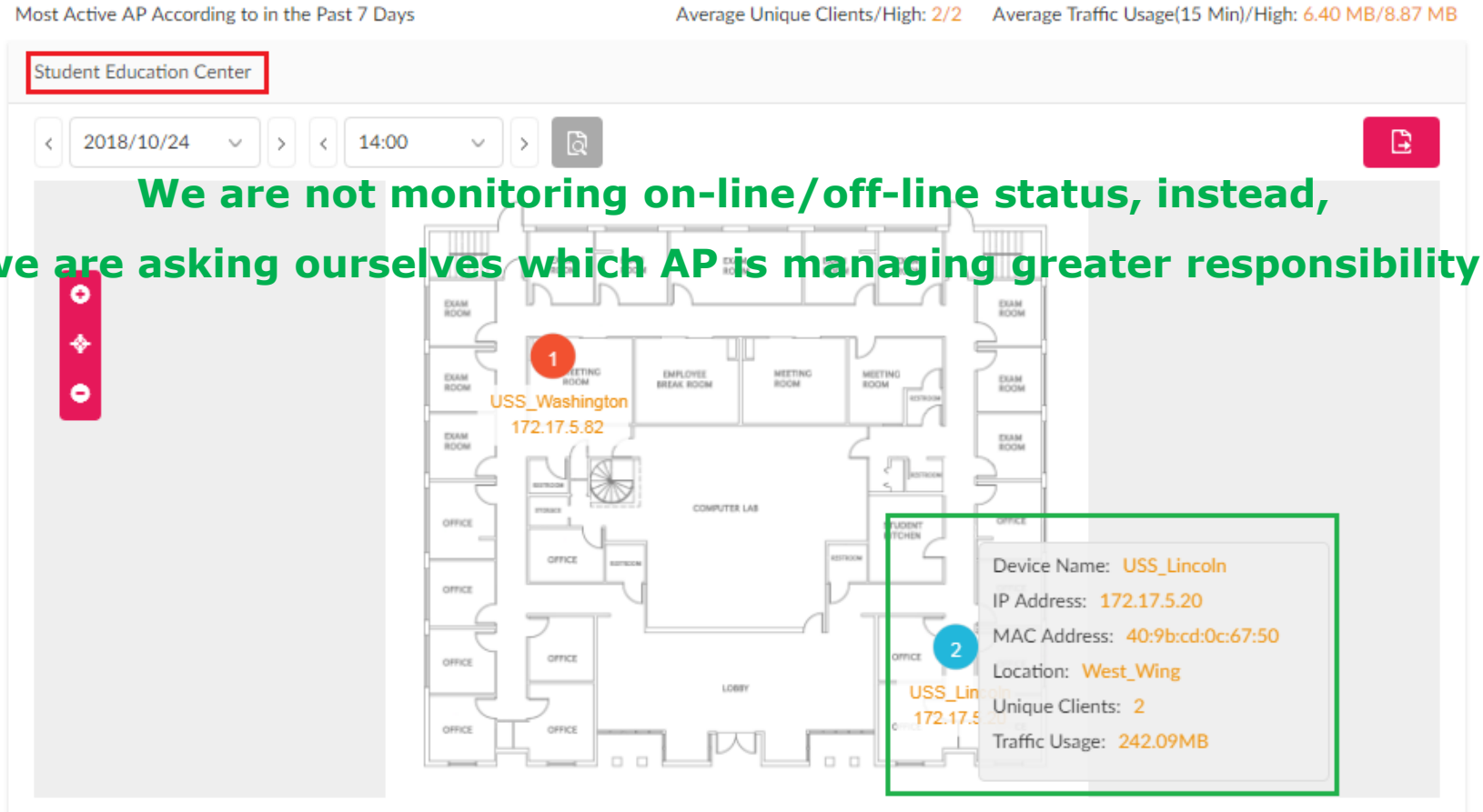
Wireless Site Maps (Coloring)

- Actual network utilization produces different color display in maps.



Wireless Site Maps (Coloring)

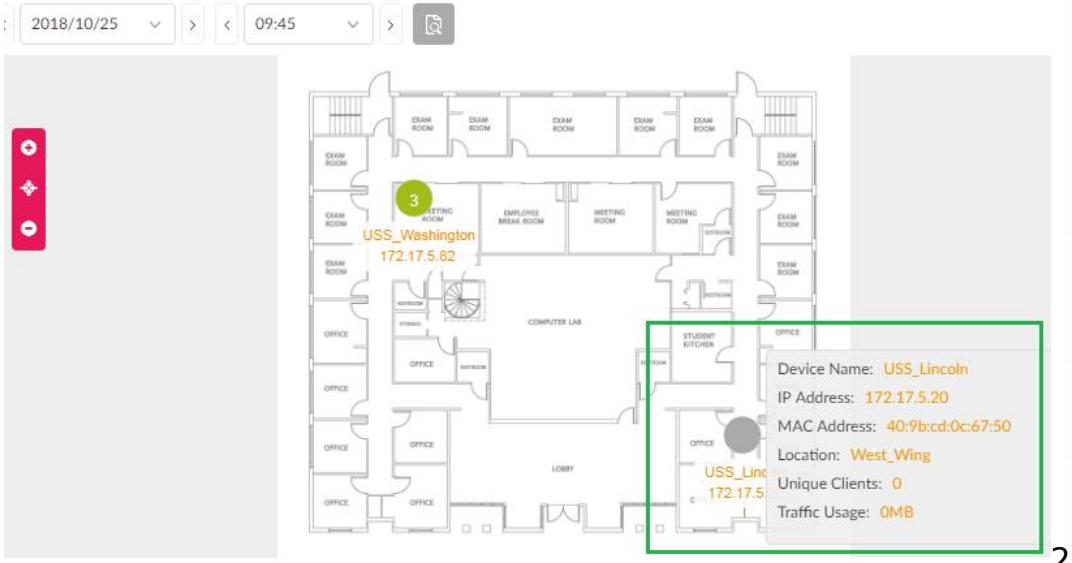
- Actual network utilization produces different color display in maps.



Wireless Site Maps (Coloring)

- Despite two Access Points are on-line and shown in our map; however, lack of network connections in a single AP is leading gray color icon being displayed in the map.

No.	Status	Action	Local IP Address	MAC Address	Model Type	Name	Location	Network	Client	
1			172.17.5.20	40:9b:cd:0c:67:50	DAP-2680	USS_Lincoln	West_Wing	Lab_Training	0	6
2			172.17.5.82	40:9b:cd:0c:64:c0	DAP-2680	USS_Washington	West_Wing	Lab_Training	3	1



Most Active AP (From A Business Development Perspective)

- We are not monitoring on-line/off-line status, instead, we are asking ourselves which AP is managing greater responsibility?

- At the same time, for those always heavy weight wireless traffic carrying APs, should we make (a) wireless configuration tuning or (b) additional DAP purchase on a timely basis?
- Are we able to select APs from different Site/Network profile and locate them in the same floor for administrative object visibility?
- Should there is an AP constantly experiencing light duty, do we re-locate it to a different location?

- Any other helpful advise?

Nuclias Connect Management Report

Nuclias Connect offers the following 4 types of reports

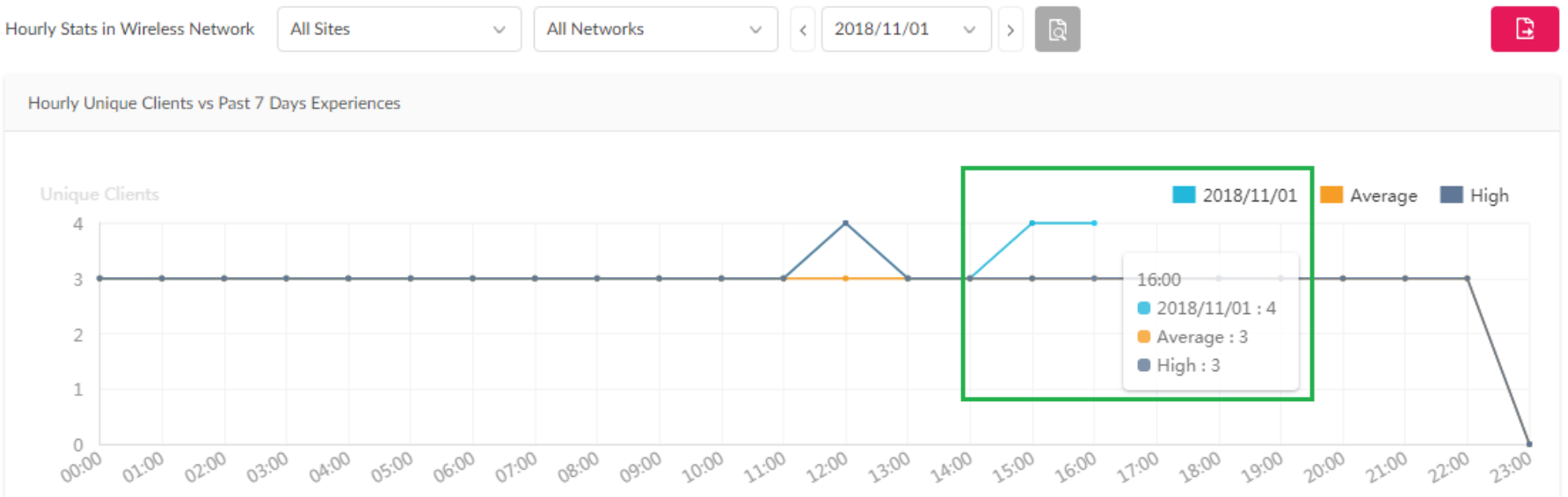
- Peak Network Activity
- Most Active AP
- Hourly Network Activity
- Daily Network Activity

Hourly Network Activity

- The wireless administrator is interested in seeing “number of users” and “wireless traffic usage” on a hourly basis, by day within last seven days.
  - Admins want to see specific date the demand from user to wireless service, and comparing with past experiences.
- This design concept of “average” and “high” remains the same.

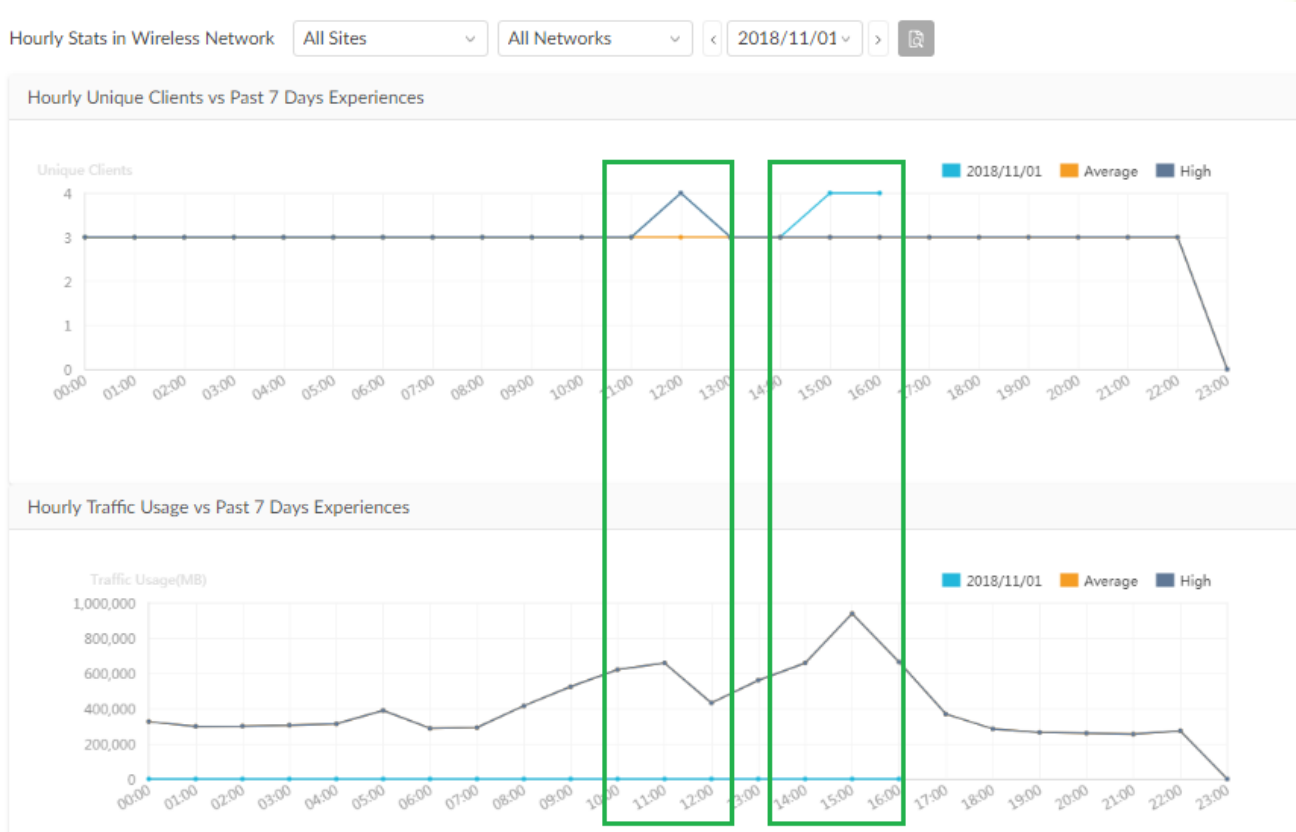
Hourly Network Activity

- From the following chart, we are aware that
  - 3 wireless stations is of common
  - 4 wireless stations during 11:00AM ~ 13:00PM and after 15:00PM



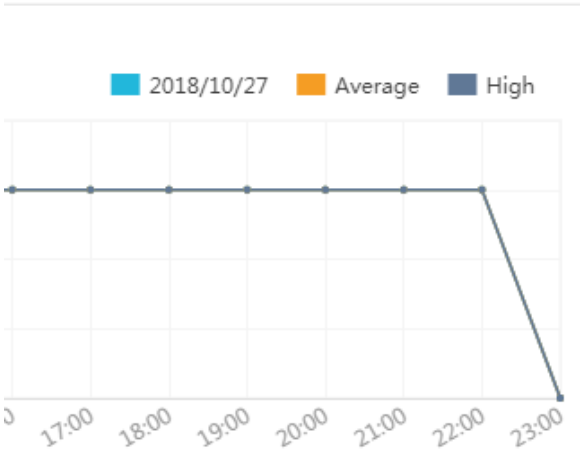
Hourly Network Activity

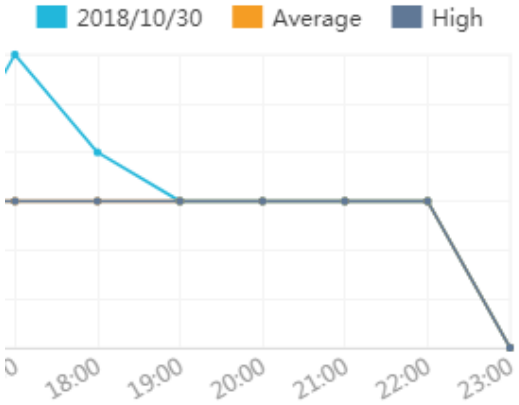
- From the following chart, we are aware that
  - Network traffic is in high demand, as the number of user increases.

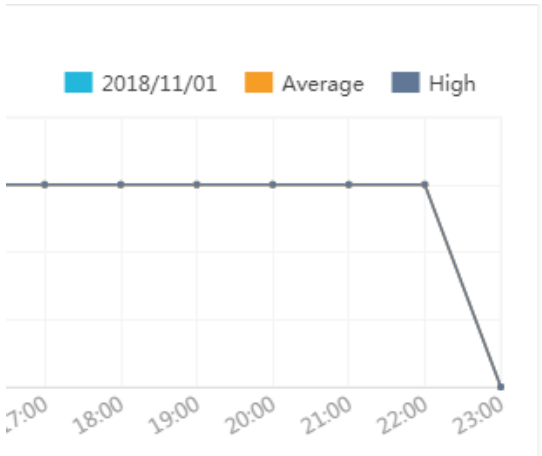


Hourly Network Activity

- With the following charts on different dates, what would be a possible cause that a significant network traffic drop, after 10:00PM?





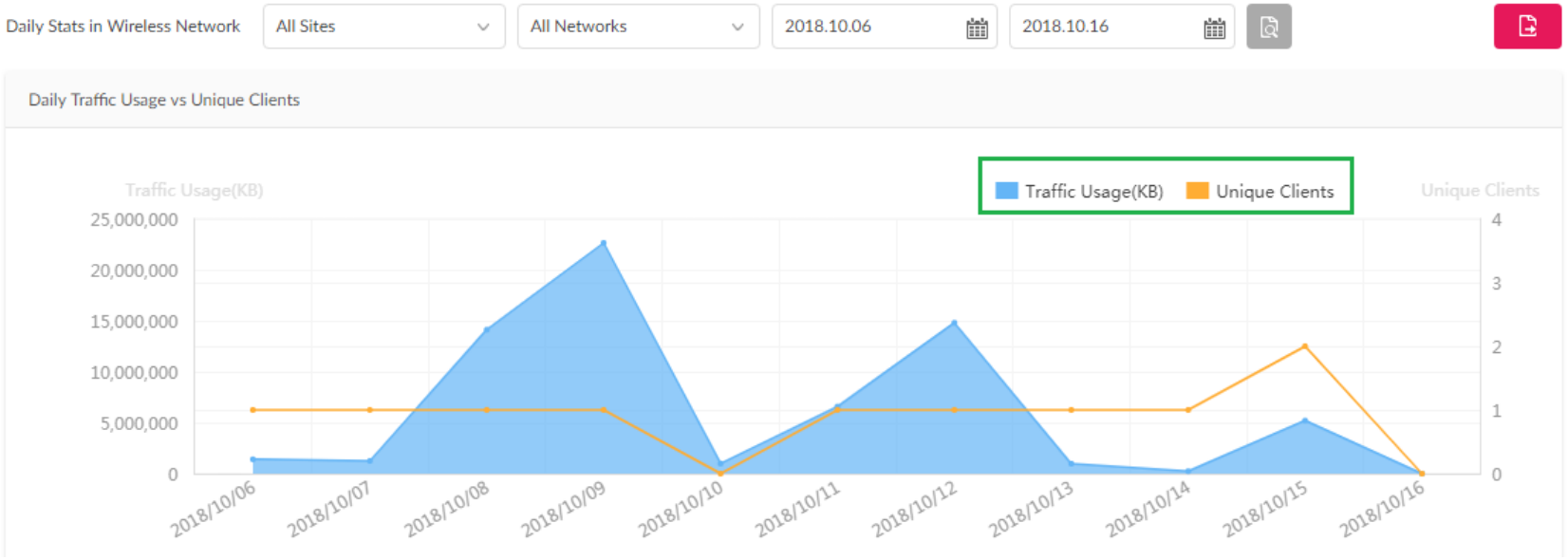


Daily Network Activity

- Menu: Report > Daily Traffic Usage vs Unique Clients.
- Presents the wireless traffic demand from user to network volume usage in wireless network

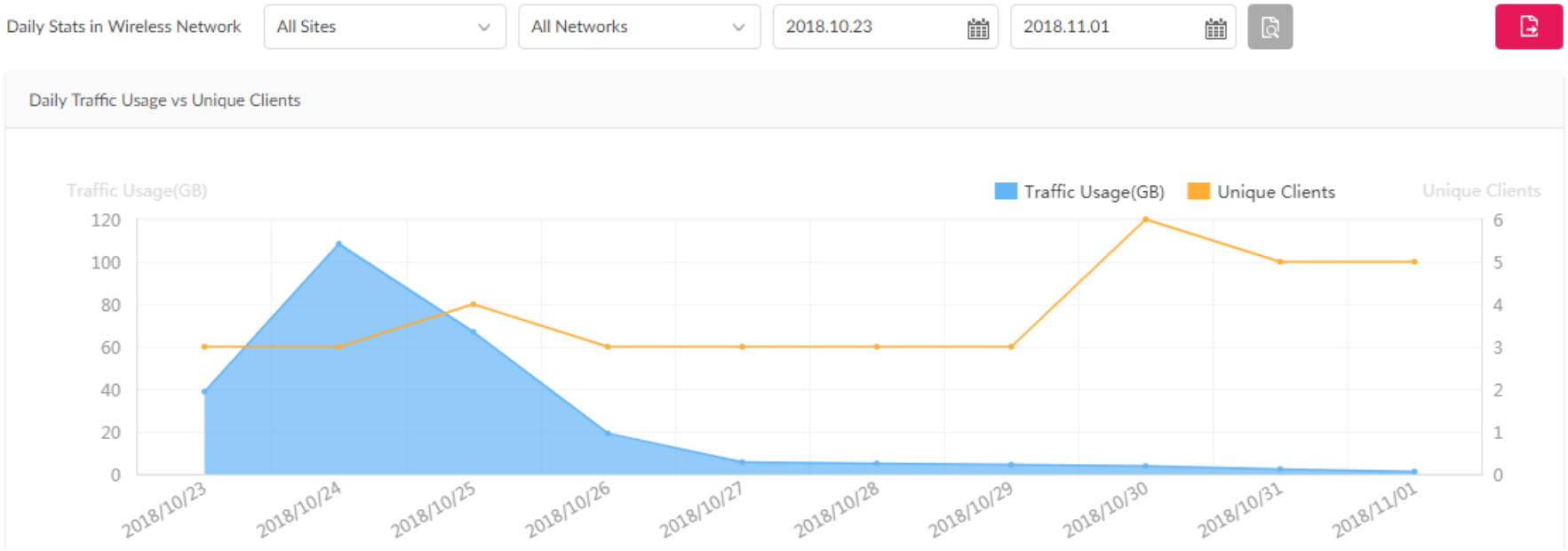
Daily Network Activity

- Menu: Report > Daily Traffic Usage vs Unique Clients.
- Presents the wireless traffic demand from user to network volume usage in wireless network
- Network traffic movement for selected period of time, where default range is the 10-day moving average.



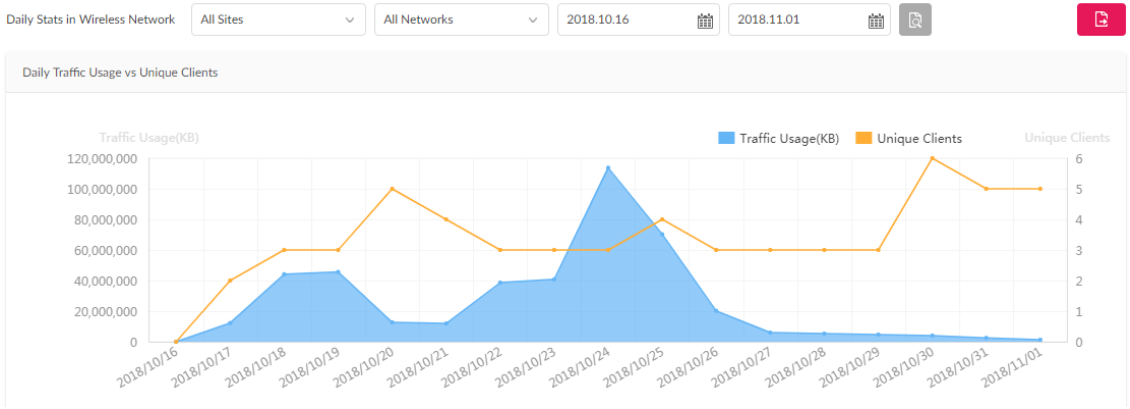
Daily Network Activity

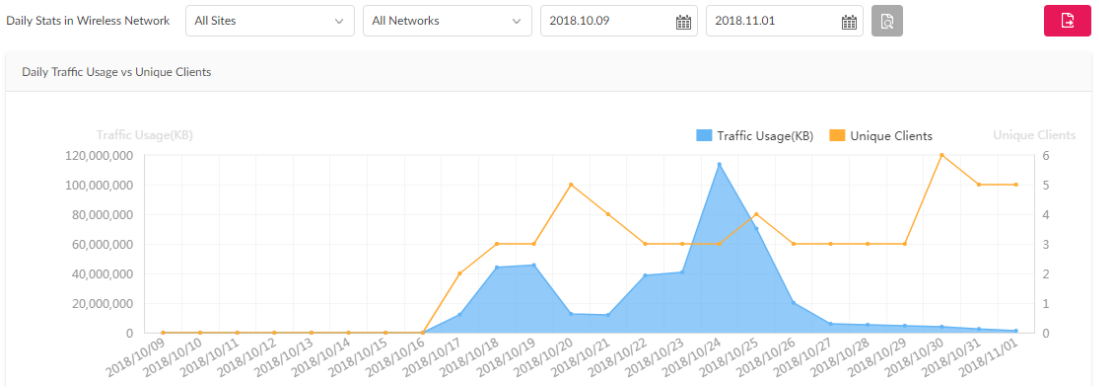
- Menu: Report > Daily Traffic Usage vs Unique Clients.
- The accumulated value is being calculated on a daily basis, at the end of the day, and will be display in the days that followed.



Daily Network Activity

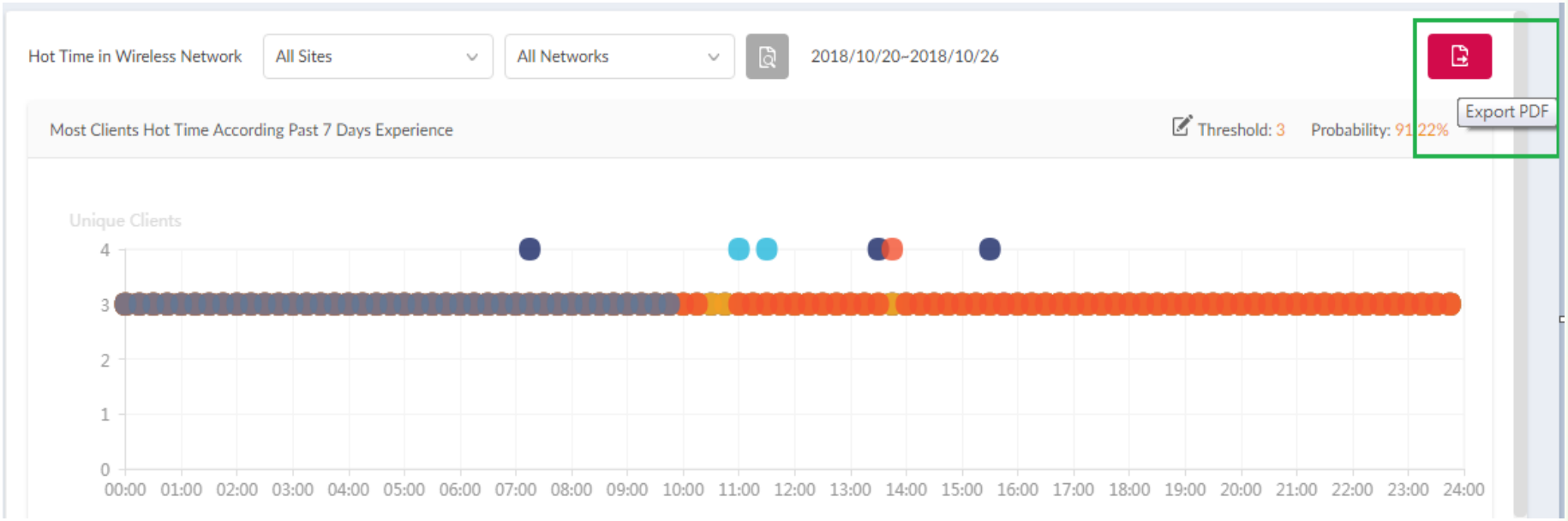
- Daily Network Activity also provides the flexibility to select diffrent dates.





Nuclias Connect Management Report

- Export Report
  - To export report, Nuclias Connect offers the PDF format.
  - There are minor differences between different releases (Please see D-Track DK1600429 for details)



The Design Thinking of Dashboard and Report

- Network Management System
  - A framework of policies, processes and procedures used by an organization to ensure that it can fulfill all the tasks required to achieve its objectives.
- Decision Support System
  - A decision support system (DSS) is an information system that supports business or organizational decision-making activities.
  - The amount of time staying on a wireless network (by STA)
  - STA using the legacy standards (802.11a, 802.11b, or 802.11g)
  - Use for short period of time (by APs)

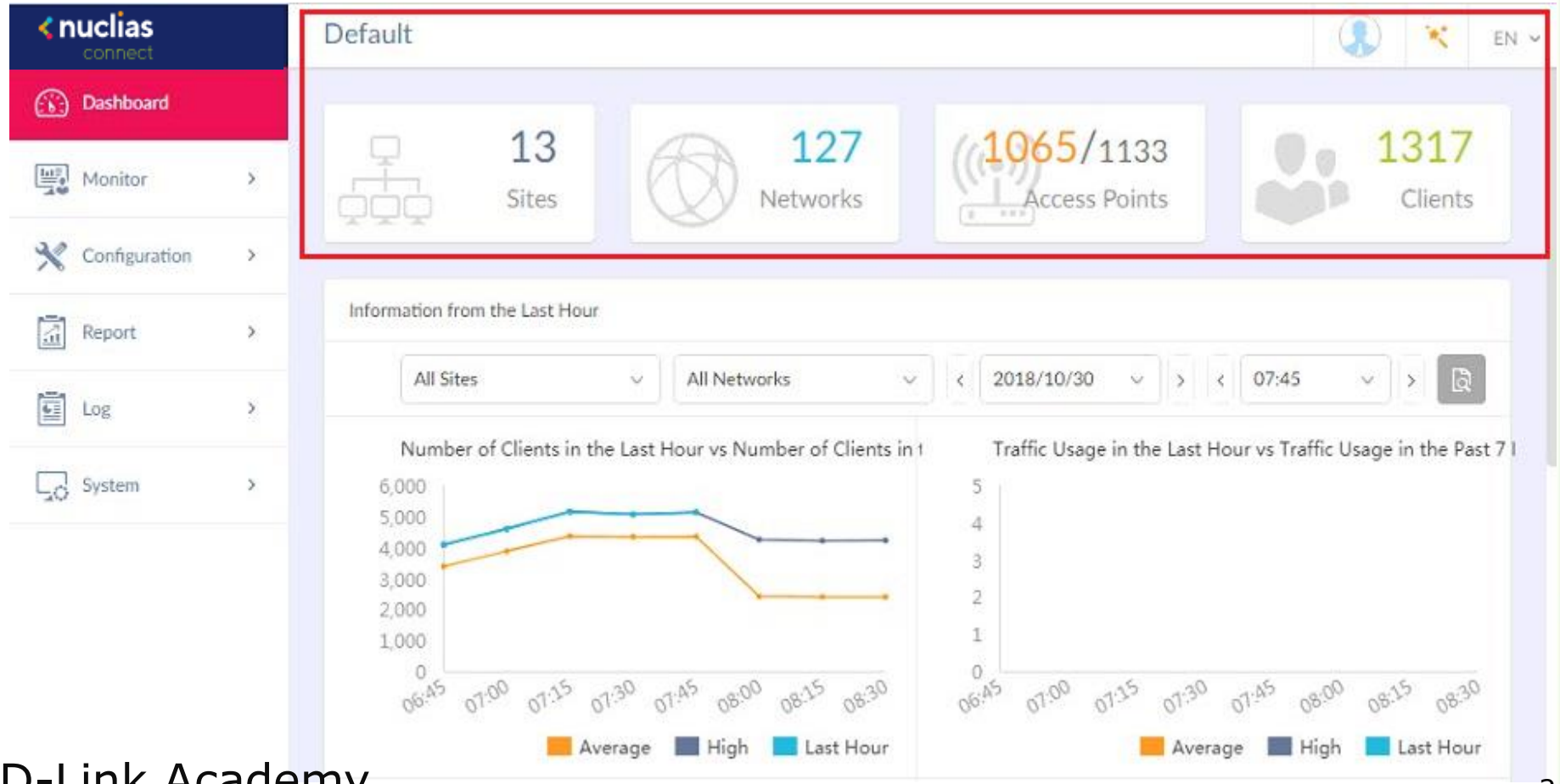
- Do we understand and meet customer needs?

Nuclias Connect Hands-on Tutorial

- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

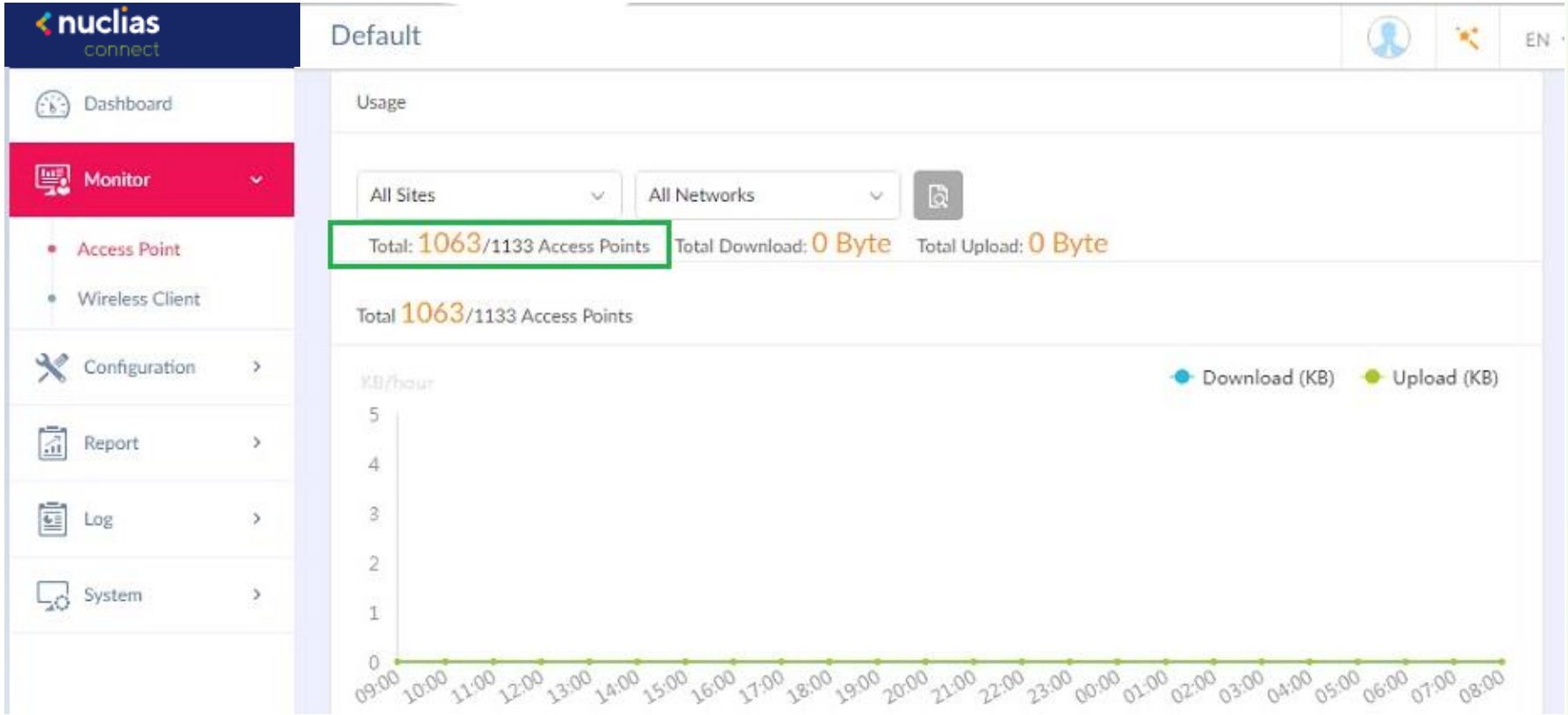
Case Studies

- Customer in education industry. DNC mighty force in “Dashboard”



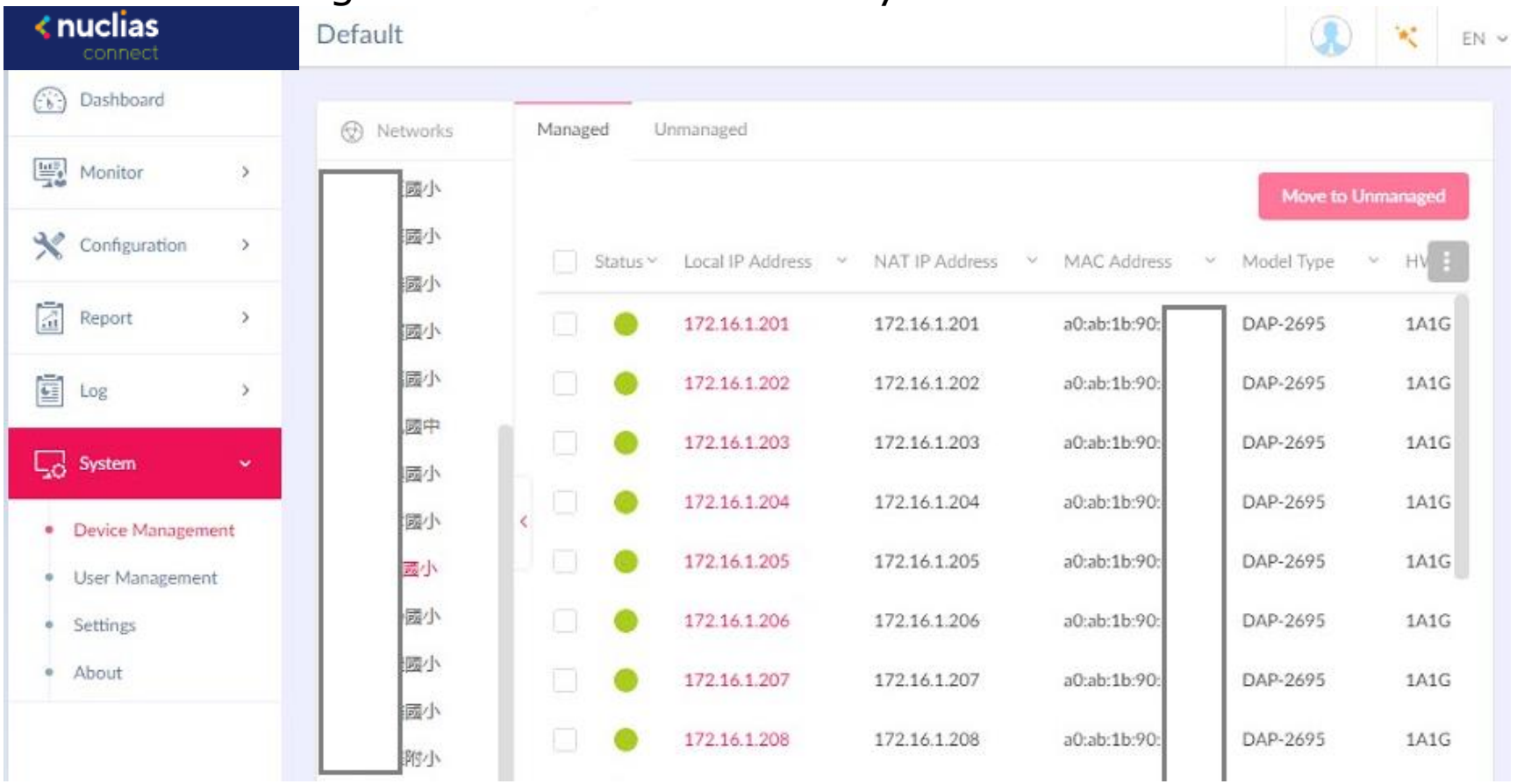
Case Studies

- Number of Access Points in Monitor tab



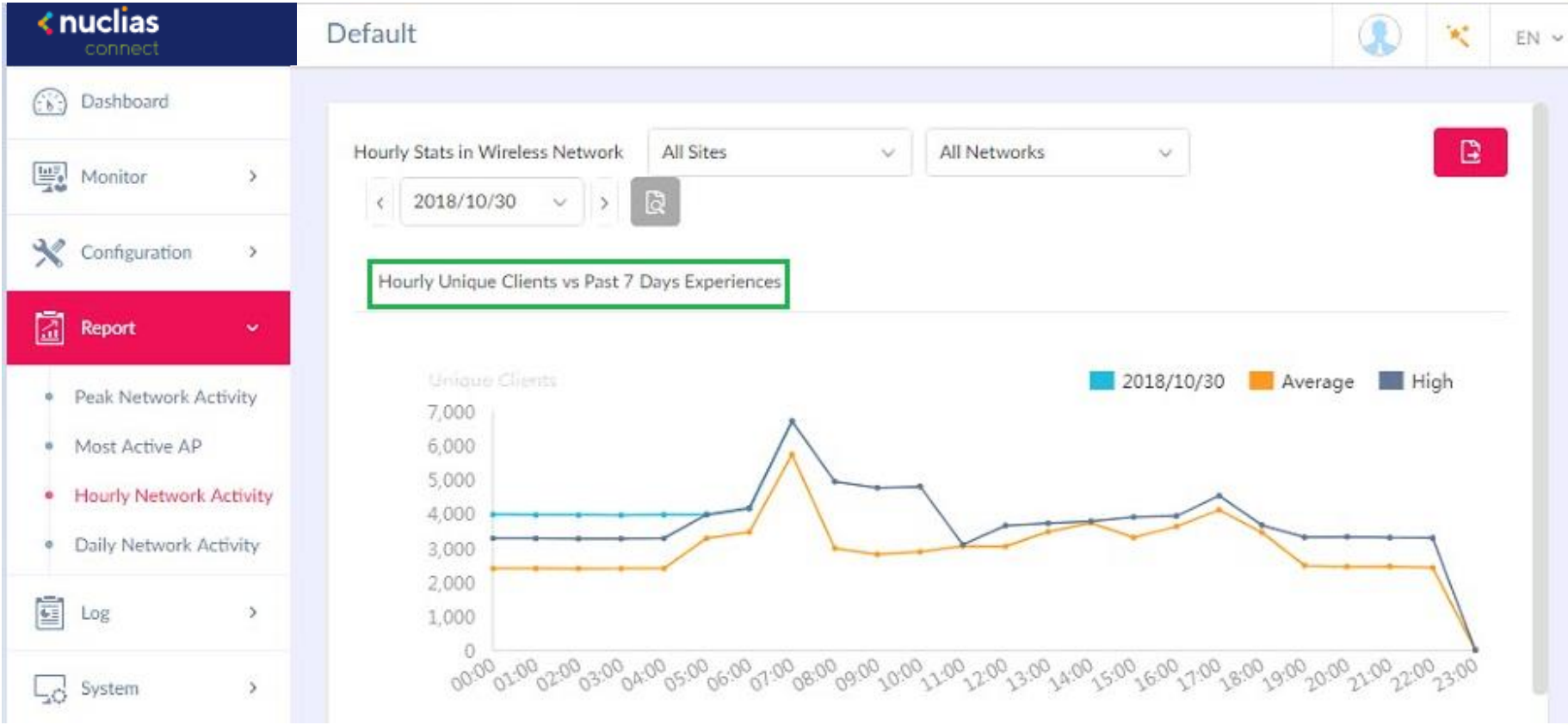
Case Studies

- Device Management overview under System tab



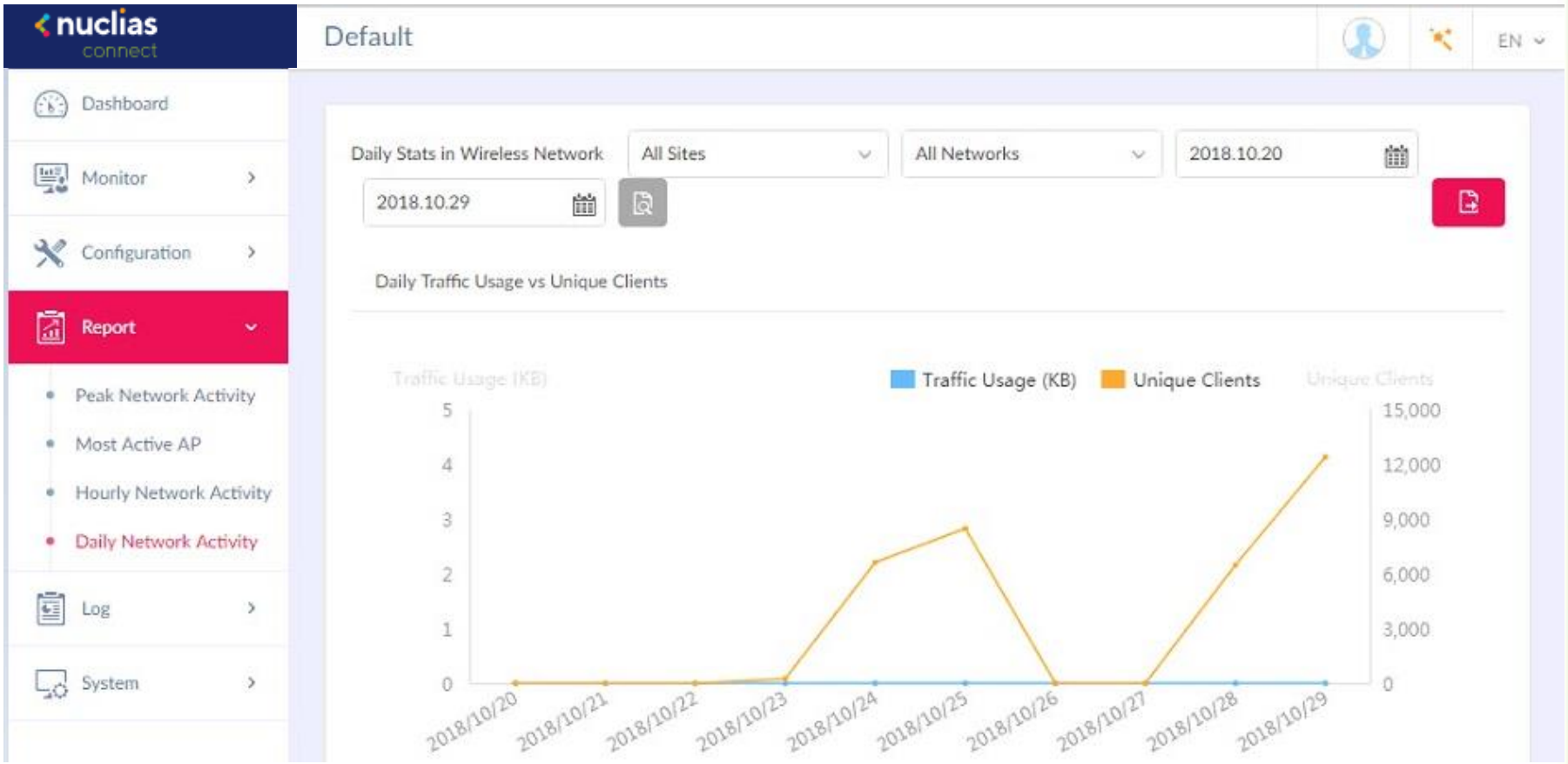
Case Studies

- Report > Hourly Network Activity



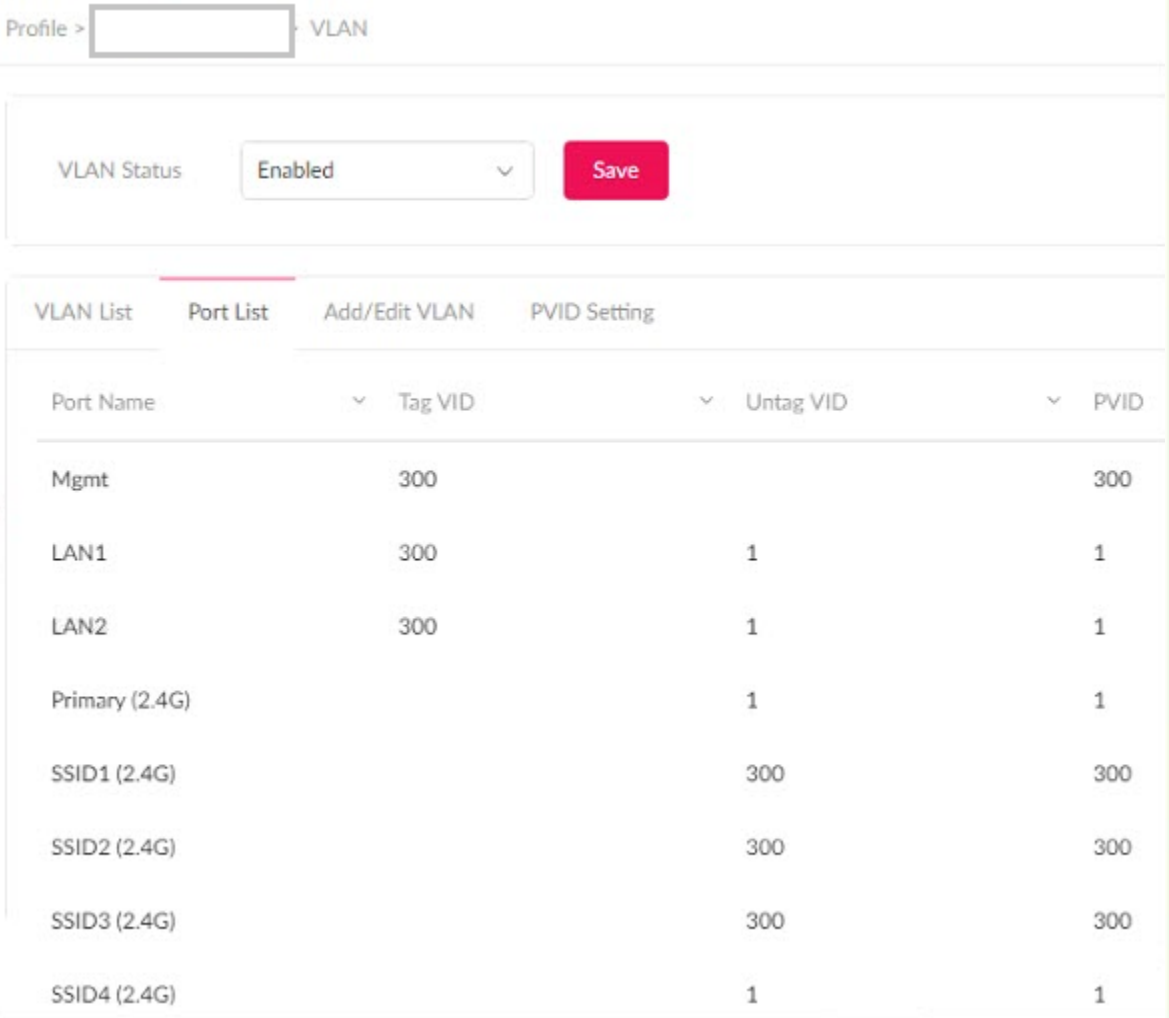
Case Studies

- Report > Daily Network Activity



Case Studies

- Profile > VLAN

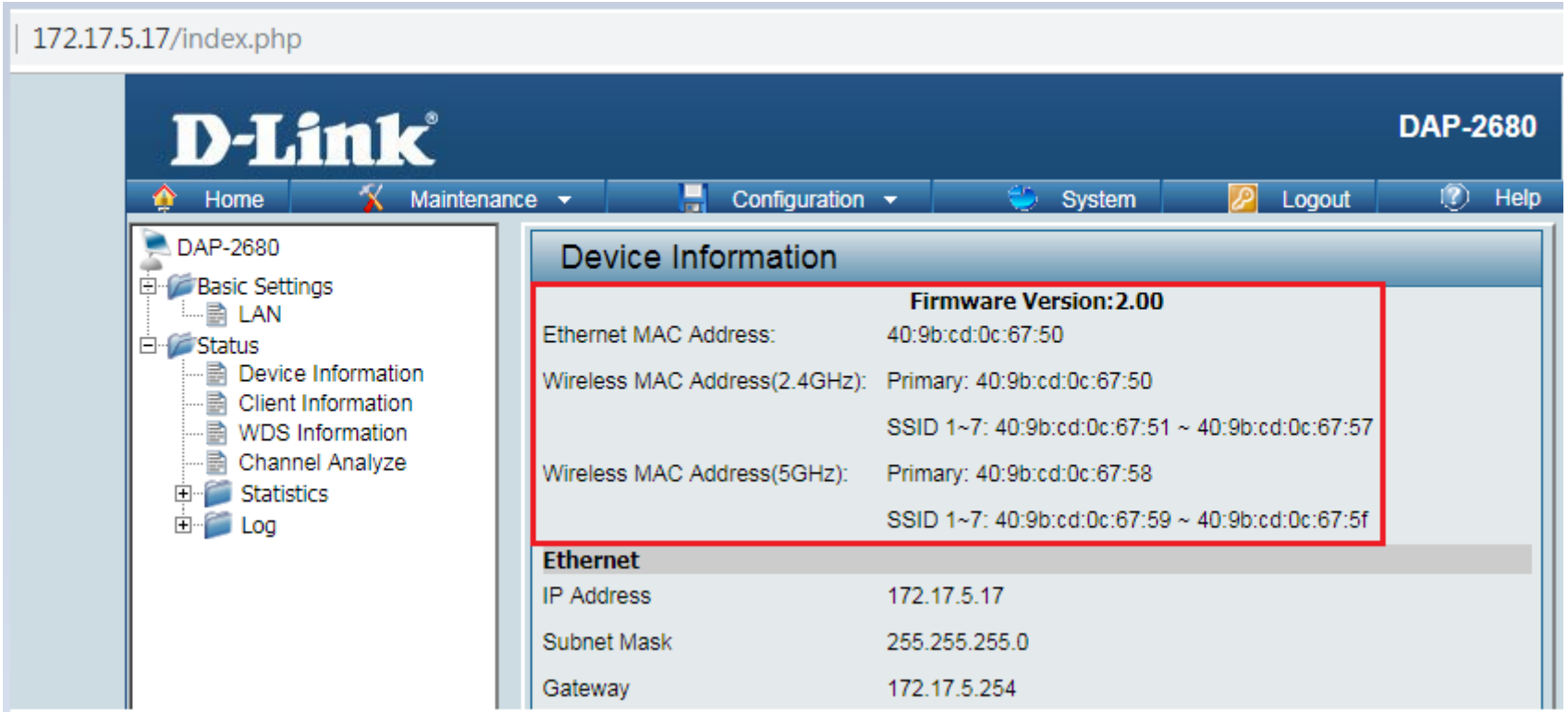


Nuclias Connect Hands-on Tutorial

- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

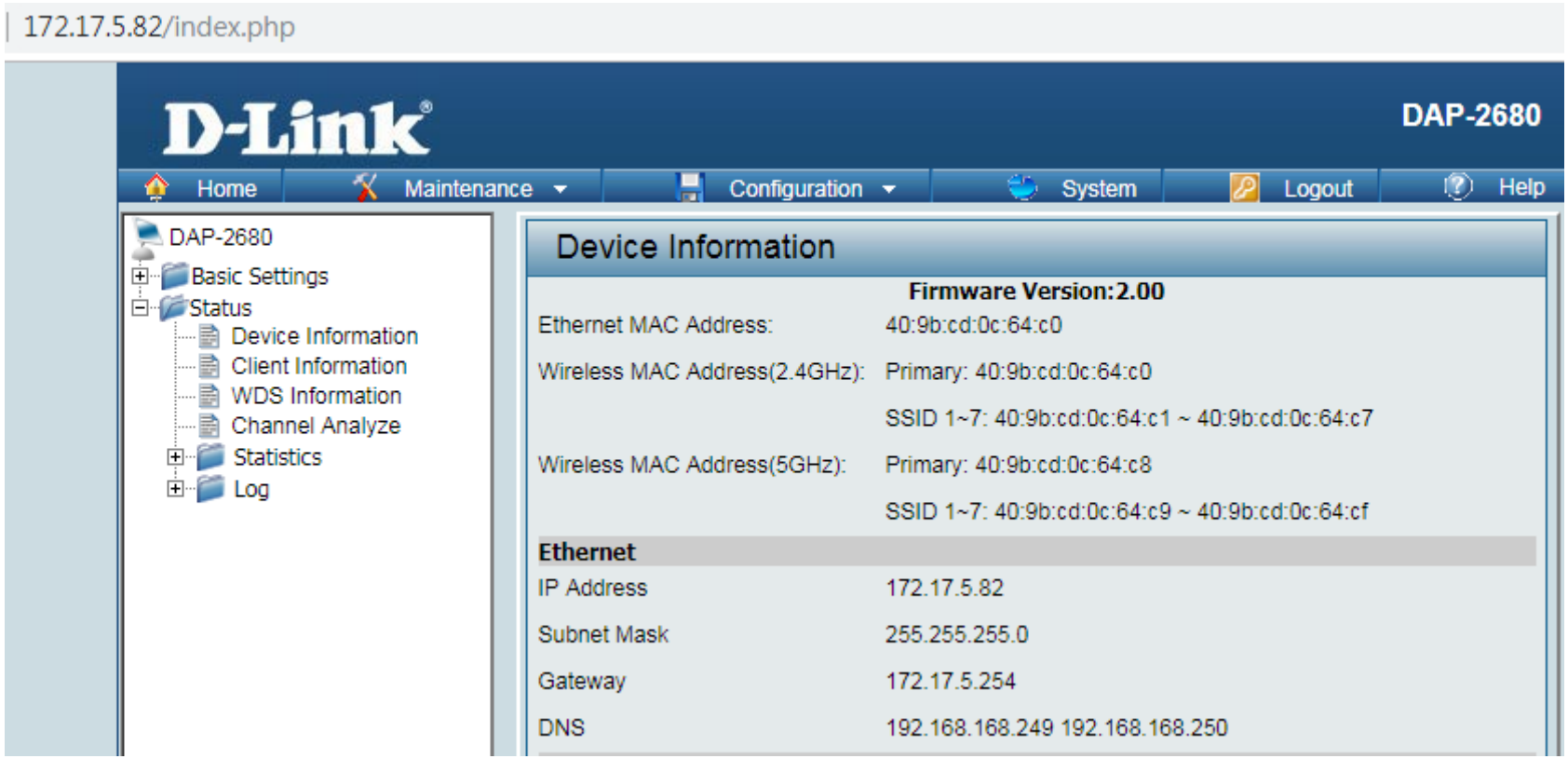
DAP-2680 Device Information (1/2)

- DAP-2680 testing device information
  - MAC address may be referred in later slides



DAP-2680 Device Information (2/2)

- DAP-2680 testing device information
  - MAC address may be referred in later slides



Wireless Profile Settings and Verifications

Wireless Profile Settings and Verifications

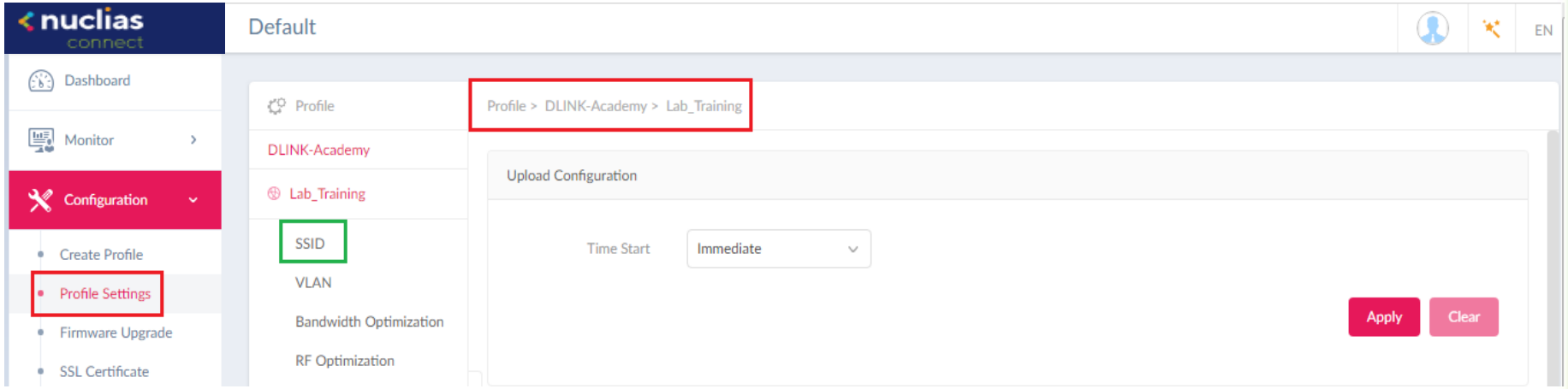
- Multiple SSIDs in One Profile
- List of the SSIDs
- Band Steering
- Channel Width
- Channel Width Modification
- Short Slot Time
- ACK TimeOut
- Beacon Interval
- Wi-Fi Multimedia (WMM)
- Traffic Indication Map (TIM)
- HT (High Throughput) Capabilities

Multiple SSIDs in One Profile (1/9)

- Multiple SSIDs implementations
- Name of SSID:
  - Boeing-F-A-XX [SSID 2]
  - F-22-Raptor [SSID 3]
  - F-35-Lightning [SSID 4]
- Band: both 2.4GHz and 5GHz
- SSID Broadcast: enabled
- Security: Open System

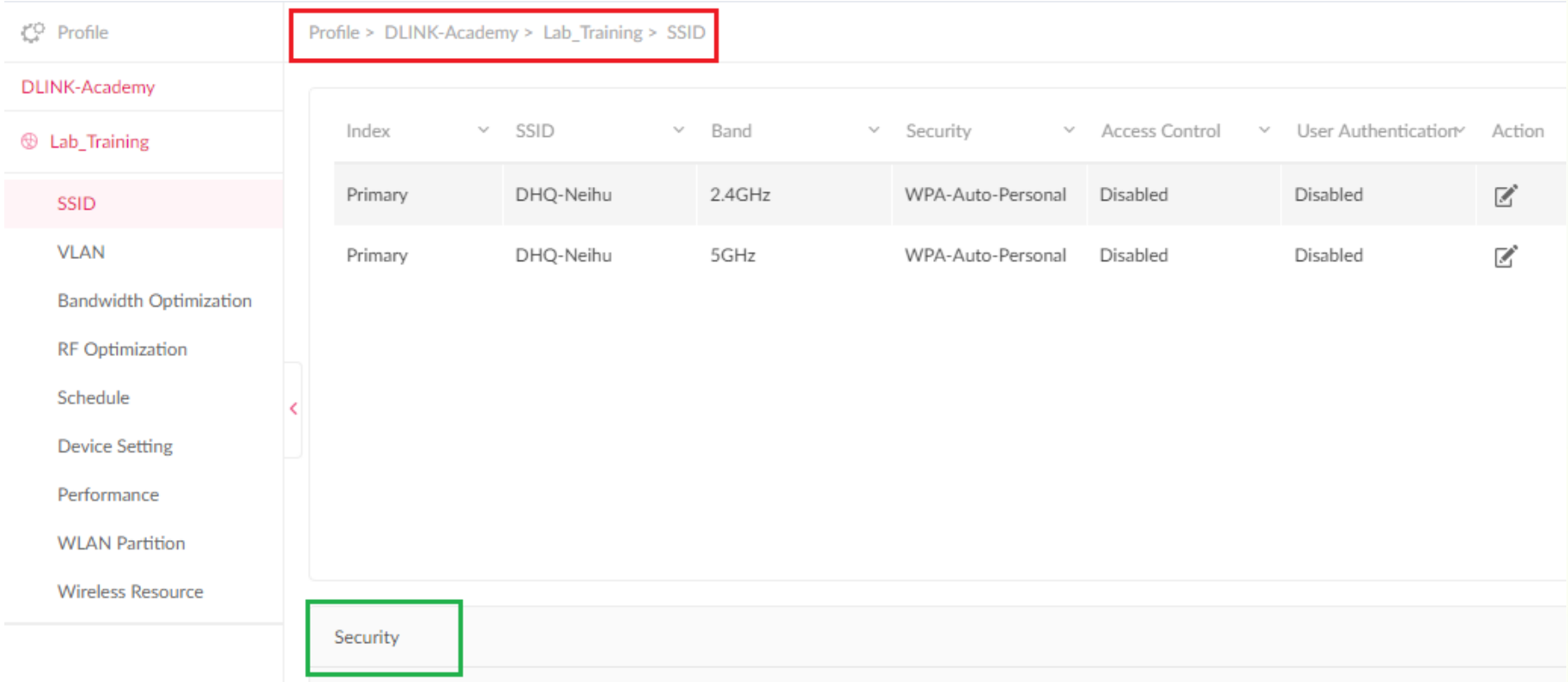
Multiple SSIDs in One Profile (2/9)

- Multiple SSIDs implementations
- Menu: Configuration > Profile Settings > Profile > DLINK-Academy > Lab_Training
  - Click the session of SSID



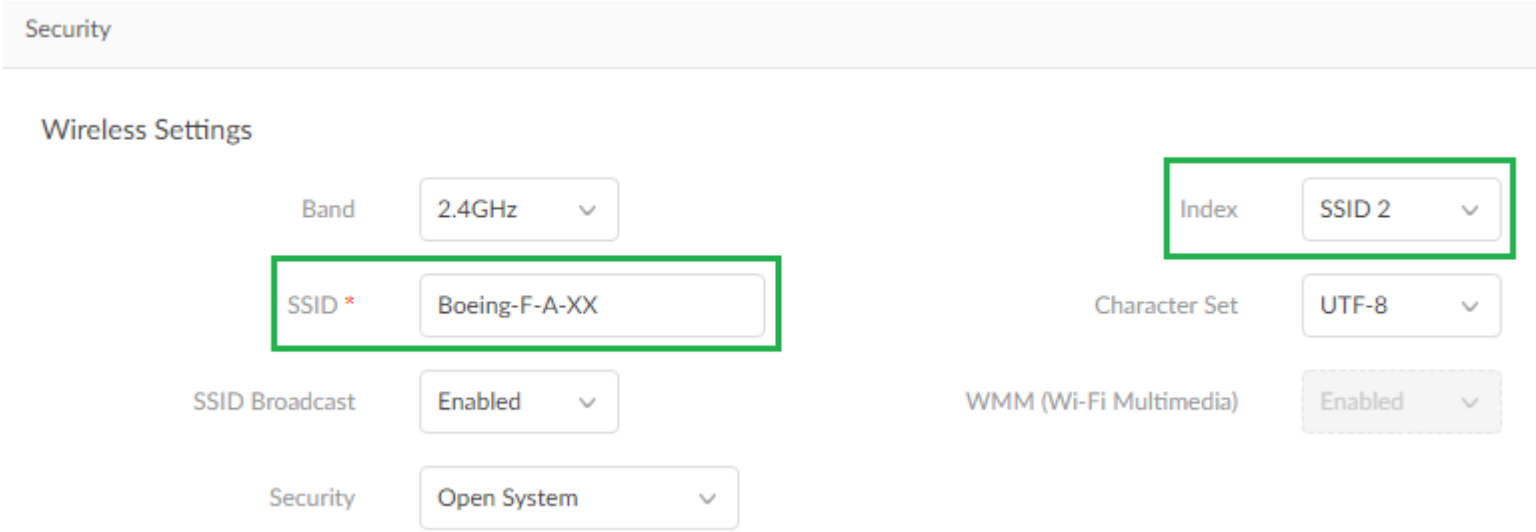
Multiple SSIDs in One Profile (3/9)

- Multiple SSIDs implementations
- Menu: Click “Security” to make configuration modifications



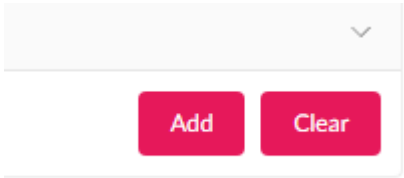
Multiple SSIDs in One Profile (4/9)

- Multiple SSIDs implementations
- Input parameters in the "Wireless Settings" under the segment of Security



Multiple SSIDs in One Profile (5/9)

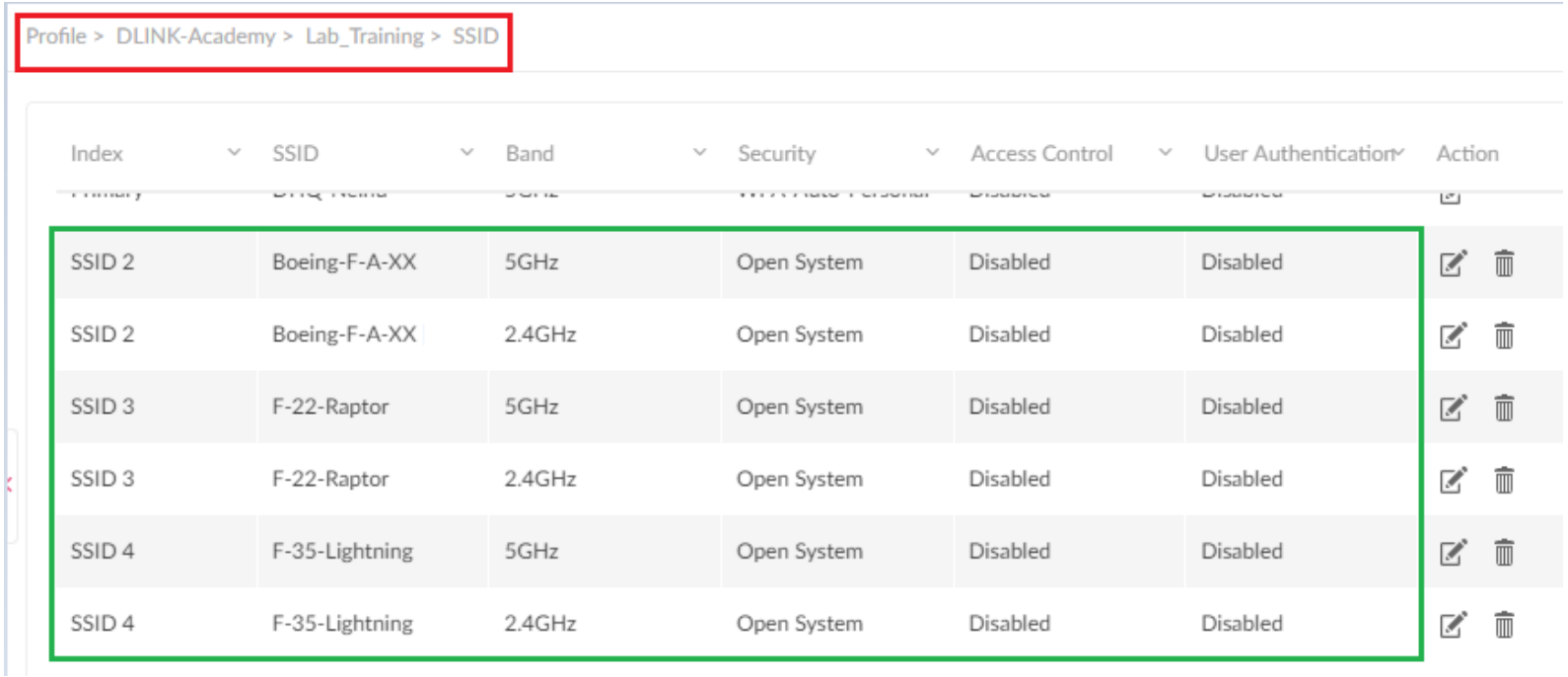
- Multiple SSIDs implementations
- Click “Add” and then click “Yes” button to respond the message of “Create same settings for SSID 2 / 5 GHz”





Multiple SSIDs in One Profile (6/9)

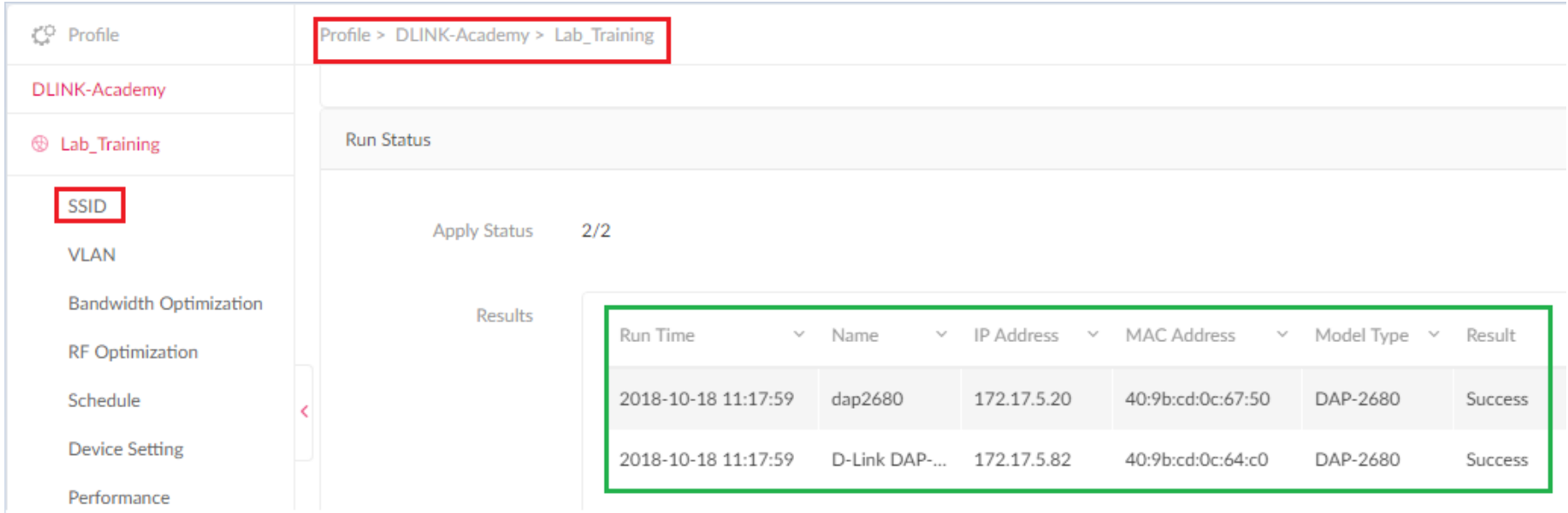
- Multiple SSIDs implementations
- Continue the configuration task for another 2 SSIDs
- Configuration verification. Menu: Profile > DLINK-Academy > Lab_Training > SSID



Index	SSID	Band	Security	Access Control	User Authentication	Action
SSID 2	Boeing-F-A-XX	5GHz	Open System	Disabled	Disabled	
SSID 2	Boeing-F-A-XX	2.4GHz	Open System	Disabled	Disabled	
SSID 3	F-22-Raptor	5GHz	Open System	Disabled	Disabled	
SSID 3	F-22-Raptor	2.4GHz	Open System	Disabled	Disabled	
SSID 4	F-35-Lightning	5GHz	Open System	Disabled	Disabled	
SSID 4	F-35-Lightning	2.4GHz	Open System	Disabled	Disabled	

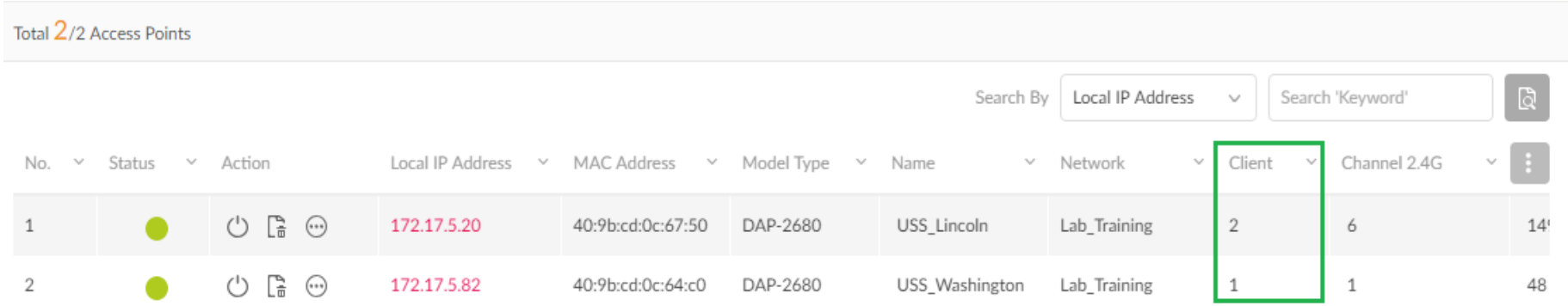
Multiple SSIDs in One Profile (7/9)

- Multiple SSIDs implementations
- Apply the latest configuration to Profile by clicking "Apply" button in the menu of Profile > DLINK-Academy > Lab_Training
  - Time Start parameter: immediately
- Run Status verification (within the same page)



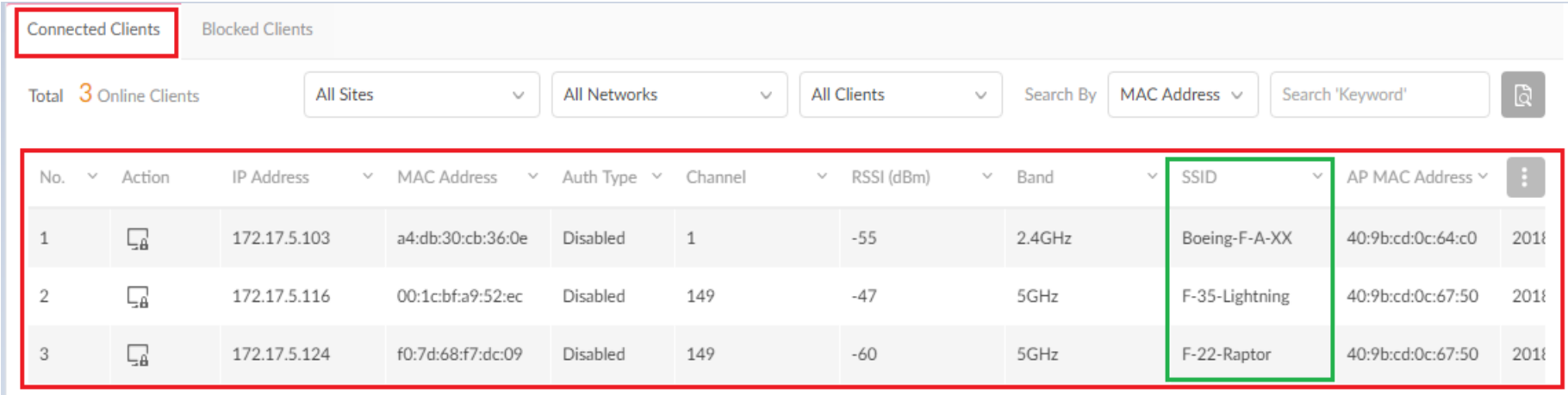
Multiple SSIDs in One Profile (8/9)

- Multiple SSIDs implementations
- Obtain three laptops and make wireless connections, one for each SSID (Menu: Monitor > Access Point)



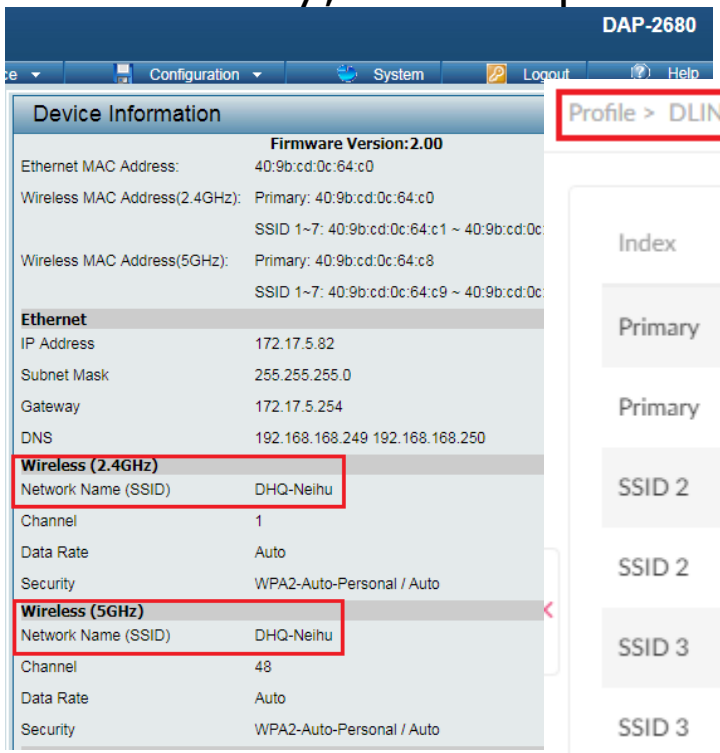
Multiple SSIDs in One Profile (9/9)

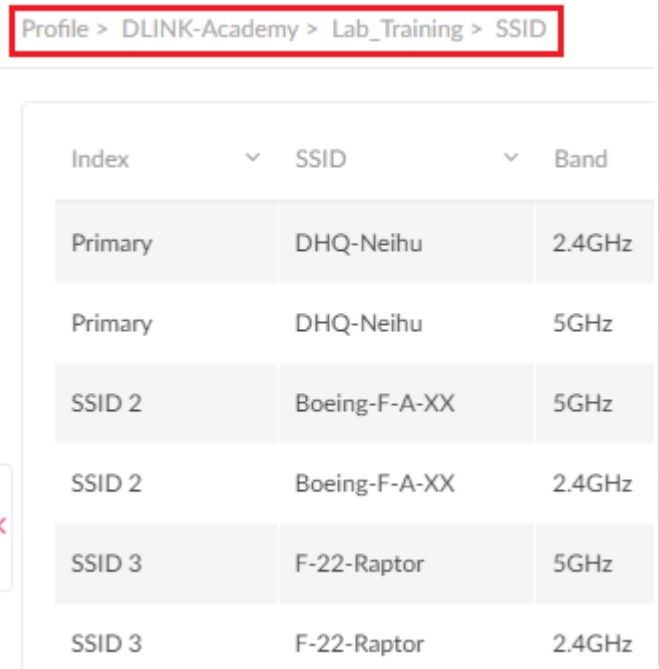
- Multiple SSIDs implementations
- Obtain three laptops and make wireless connections, one for each SSID (Menu: Monitor > Wireless Client)

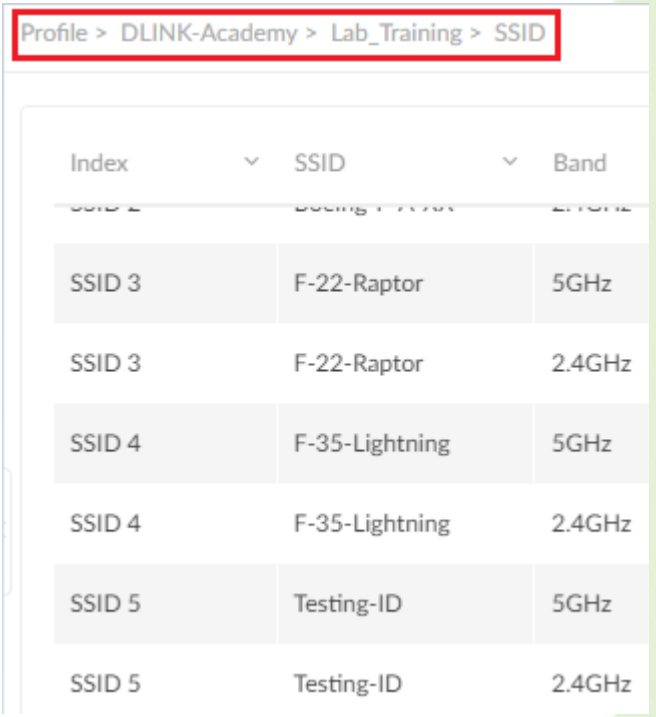


List of the SSIDs

- In DAP GUI, it presents the primary SSID configurations.
- In Nuclias Connect, the SSID index shows configured SSID, from Primary, SSID1 up-to SSID7.







Working In a Dual-Band Network

- 2.4 GHz usually covers greater range (~300 feet) and 5 GHz with lower indoor range (~90 feet)
- 2.4 GHz has three non-overlapping channels, and 5 GHZ carry twenty-four three non-overlapping channels (a lot more space).
- Working in a dual-band network, we can
  - maintain 802.11b/g/n compatibility for older 2.4 GHz devices as well as
  - provide better performance for newer 802.11a/n/ac compatible devices
- An objective is to provide both capacity and coverage.

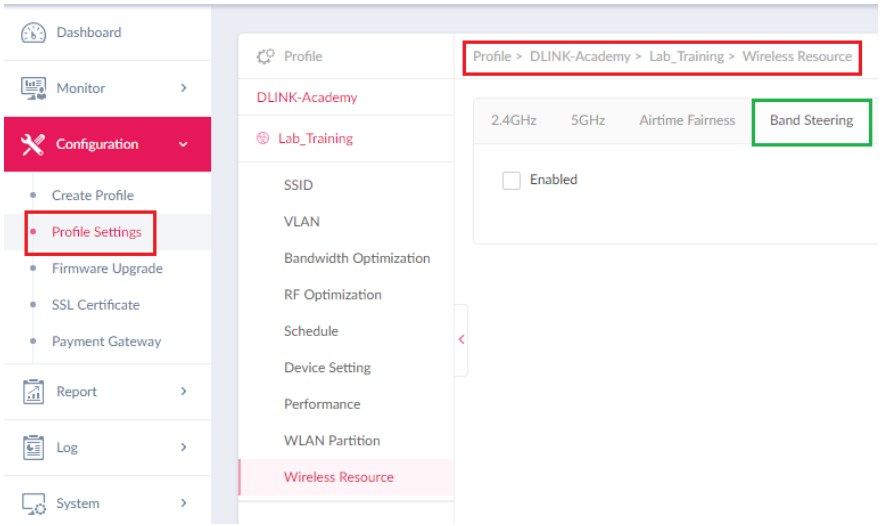
Band Steering Configuration in Profile Settings (1/5)

- Band Steering is a key feature to encourage dual-band capable wireless clients to connect to the less crowded 5GHz network, and leave the 2.4GHz network available for those clients who support 2.4GHz only.
- The benefits of such function yields improved Wi-Fi performance for all clients [by moving to a preferred frequency band].
- In Nuclias Connect, Band Steering is located on the Wireless Resources session of Profile Settings page under the Configure tab.

Band Steering Configuration in Profile Settings (2/5)

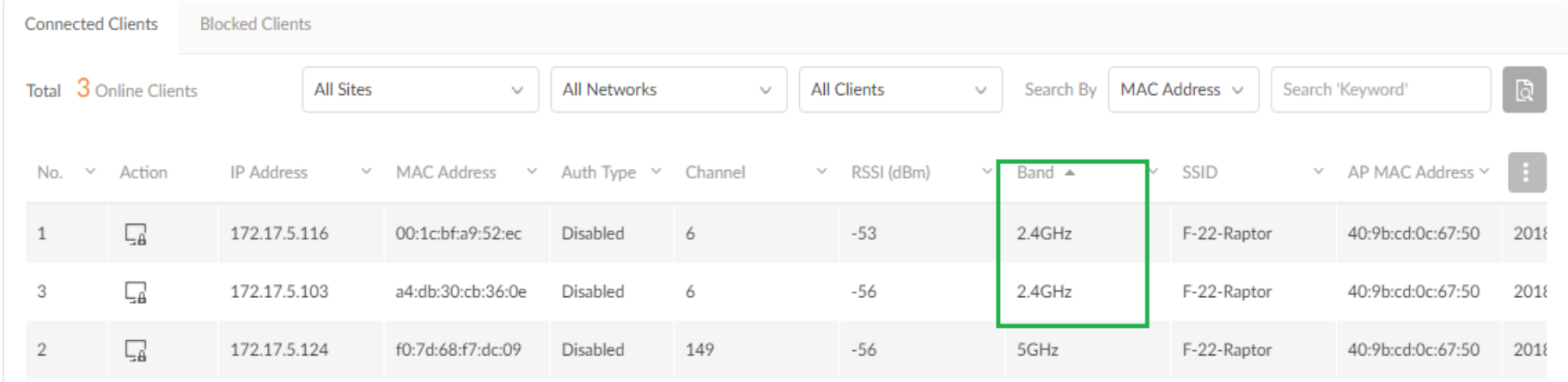
Band Steering in Nuclias Connect

- 5 GHz wireless shall be in “On” status. (menu: Profile > Performance > 5GHz tab)
- It is NOT enabled by default. (menu: Profile > Wireless Resource > Band Steering)
- Name of SSID and other parameters are recommended match identically, both 2.4 GHz and 5 GHz.

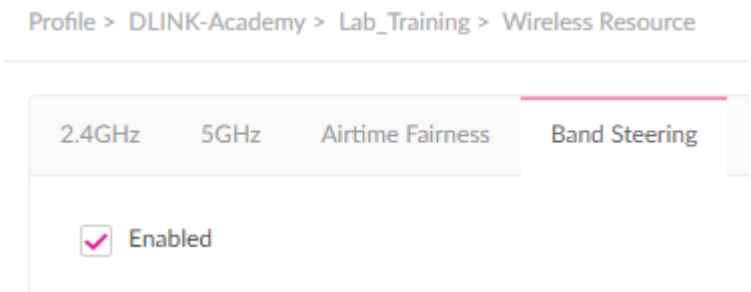


Band Steering Configuration in Profile Settings (3/5)

- Band Steering lab practice
- Two of the three wireless stations are using 2.4GHz band.

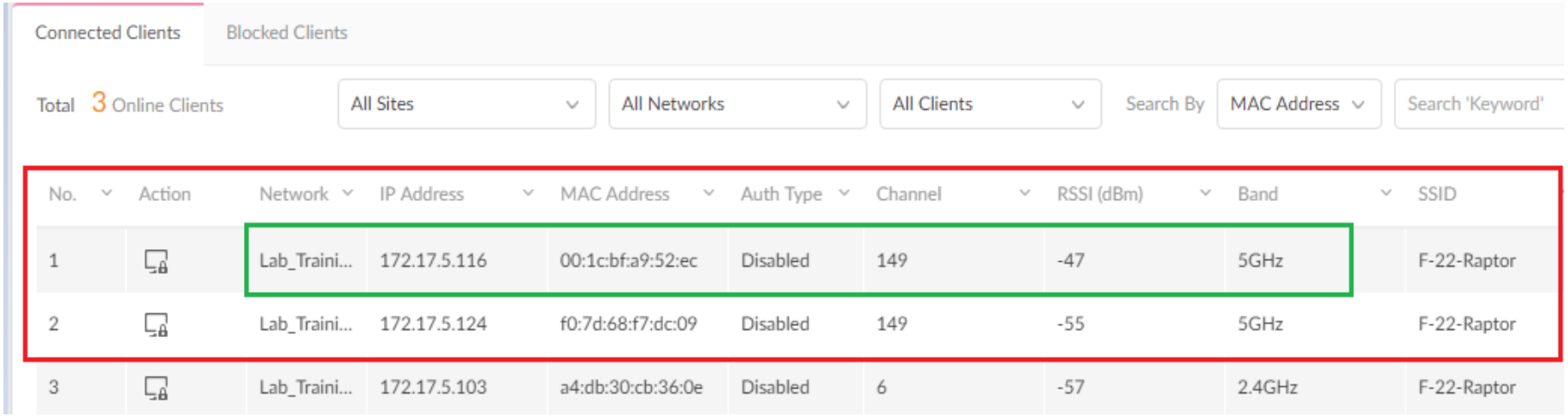


- We are going to enable Band Steering function



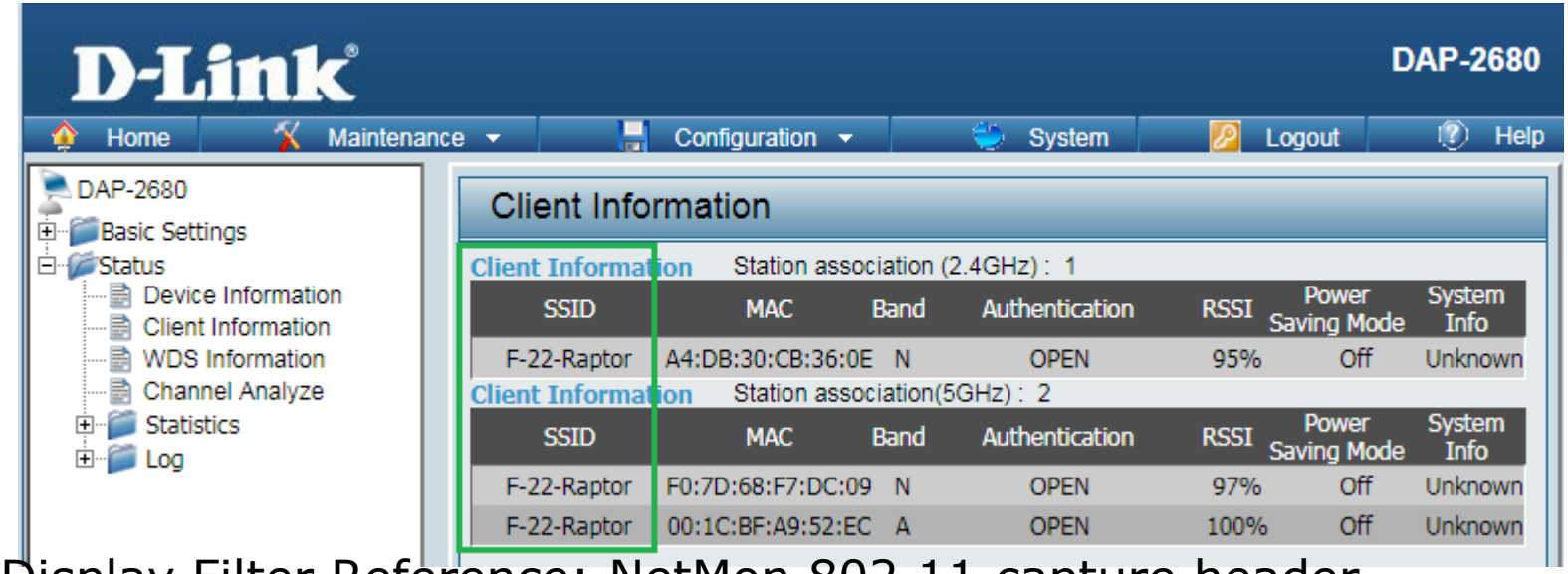
Band Steering Configuration in Profile Settings (4/5)

- Band Steering lab practice
- After activating Band Steering function, then, we apply this configuration to related devices.
- Within a reasonable timeframe, by viewing Wireless Client page under the Monitor tab, we should be able to see two devices are in 5GHz.
  - The laptop (172.17.5.116) was in 2.4GHz according to last slide



Band Steering Configuration in Profile Settings (5/5)

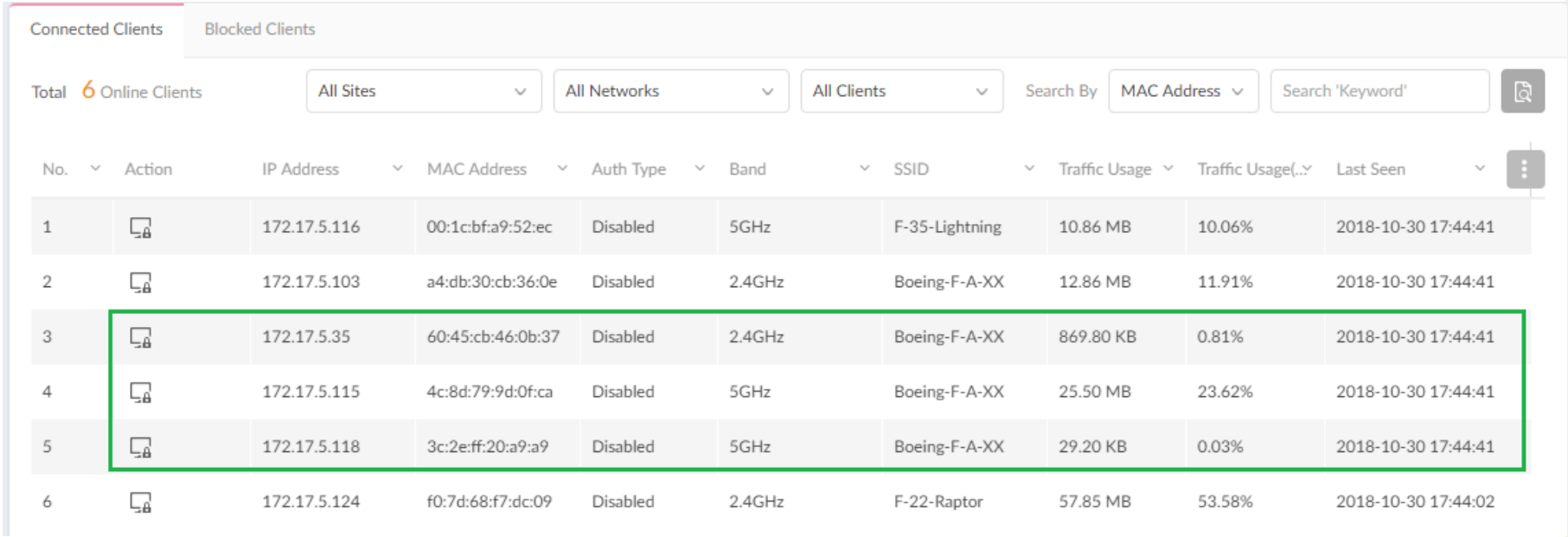
- Band Steering lab practice
- The connected DAP (DAP-2680) local GUI also reflects a similar information, as shown here.



- Display Filter Reference: NetMon 802.11 capture header
  - netmon_802_11.phy_type, PHY type

Band Steering Configuration in Profile Settings (another example)

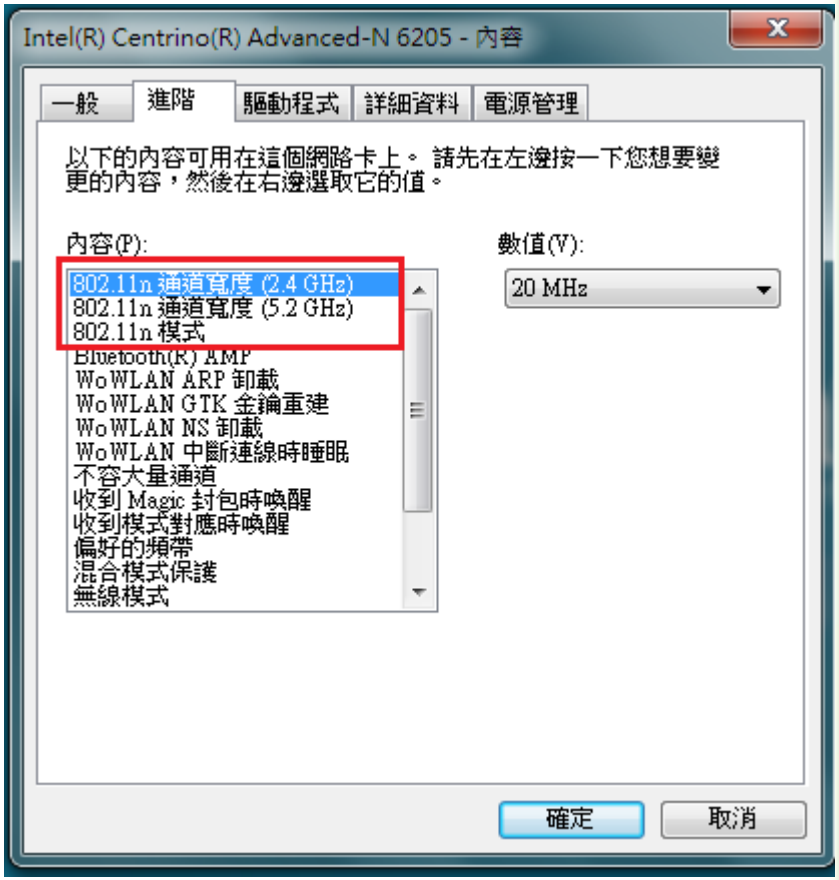
- Three mobile devices, one Android phone and two iPhone just joined our lab network. Some of them are immediately assigned to 5GHz. (iPHONE5, 2.4GHz)



No.	Action	IP Address	MAC Address	Auth Type	Band	SSID	Traffic Usage	Traffic Usage(..)	Last Seen
1		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	5GHz	F-35-Lightning	10.86 MB	10.06%	2018-10-30 17:44:41
2		172.17.5.103	a4:db:30:cb:36:0e	Disabled	2.4GHz	Boeing-F-A-XX	12.86 MB	11.91%	2018-10-30 17:44:41
3		172.17.5.35	60:45:cb:46:0b:37	Disabled	2.4GHz	Boeing-F-A-XX	869.80 KB	0.81%	2018-10-30 17:44:41
4		172.17.5.115	4c:8d:79:9d:0f:ca	Disabled	5GHz	Boeing-F-A-XX	25.50 MB	23.62%	2018-10-30 17:44:41
5		172.17.5.118	3c:2e:ff:20:a9:a9	Disabled	5GHz	Boeing-F-A-XX	29.20 KB	0.03%	2018-10-30 17:44:41
6		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	2.4GHz	F-22-Raptor	57.85 MB	53.58%	2018-10-30 17:44:02

Enabling Band Steering

- Experience interference from Bluetooth devices, microwave ovens, cordless phones, and/or co-channel interference from other AP
- The objective is to encourage dual-band capable clients to stay on the 5GHz band on dual-band Aps. Thus, making sure the NIC card of your wireless clients support 5 GHz. (Control Panel > Network and Internet > Network Connections > Properties of Wireless Network Connection



RTS/CTS (Request To Send/Clear To Send)

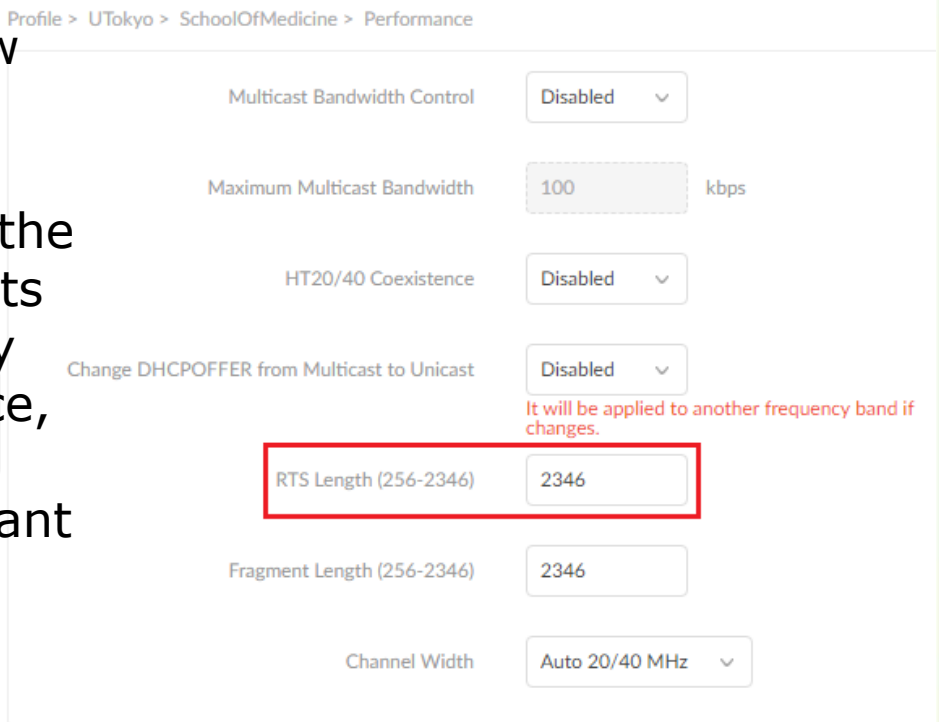
Request To Send/Clear To Send

- The function of RTS is to ask laptops and smartphones for permission to send the next data packet.
- The lower the threshold, the more stable your Wi-Fi network, since Access Point asks to send packets more frequently.
- The maximum of a wireless frame is 2304 bytes + 8 WEP bytes, close to 2312. Thus, if RTS length is set between 2312 and 2346, meaning it (RTS) is not being activated.

RTS/CTS (Request To Send/Clear To Send)

Request To Send/Clear To Send configuration guideline

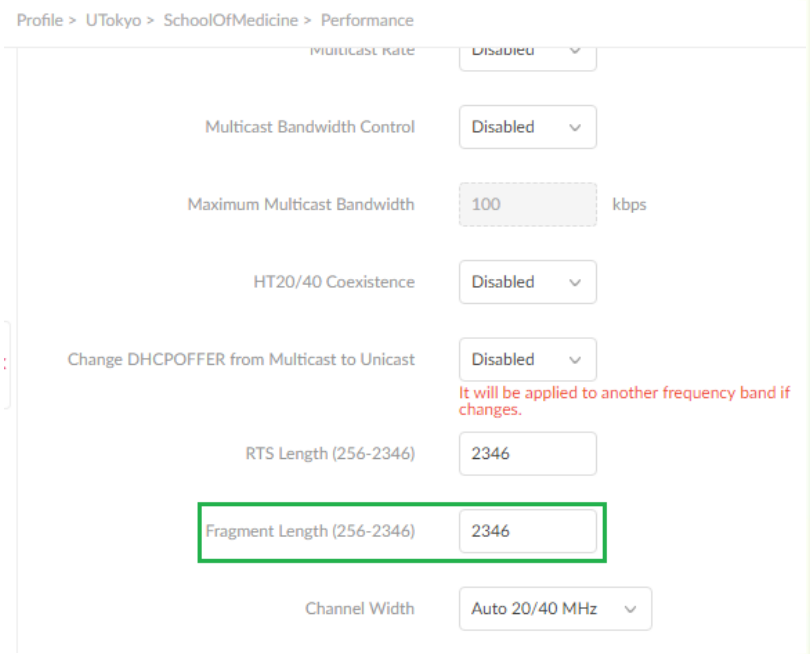
- RTS length (2312 ~ 2346): low wireless interference, fewer wireless clients
- RTS length (256 ~ 2312): (a) the larger amount of wireless clients with the active wireless activity and strong wireless interference, the smaller this number is recommended to be. (b) constant dropouts, re-connect (Menu: Configuration > Profile > Performance)



Fragment Length

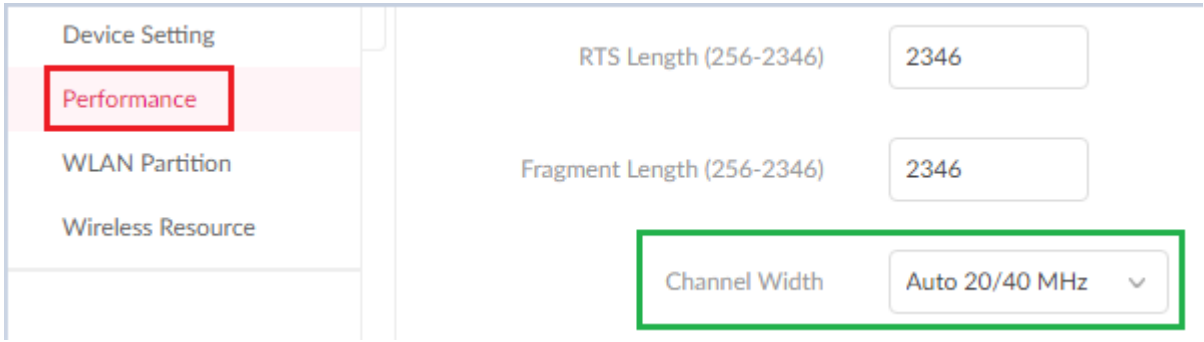
Fragment Length

- It (Fragment Length) is used to set the maximum size of a packet can be sent out.
- The smaller the packet is, the better the reliability it brings where suffering inferior performance.
- It is recommended to maintain in 2346, its default values. Reduce this settings where (a) communication is poor, (b) severe radio interference. (menu: Profile > Performance)



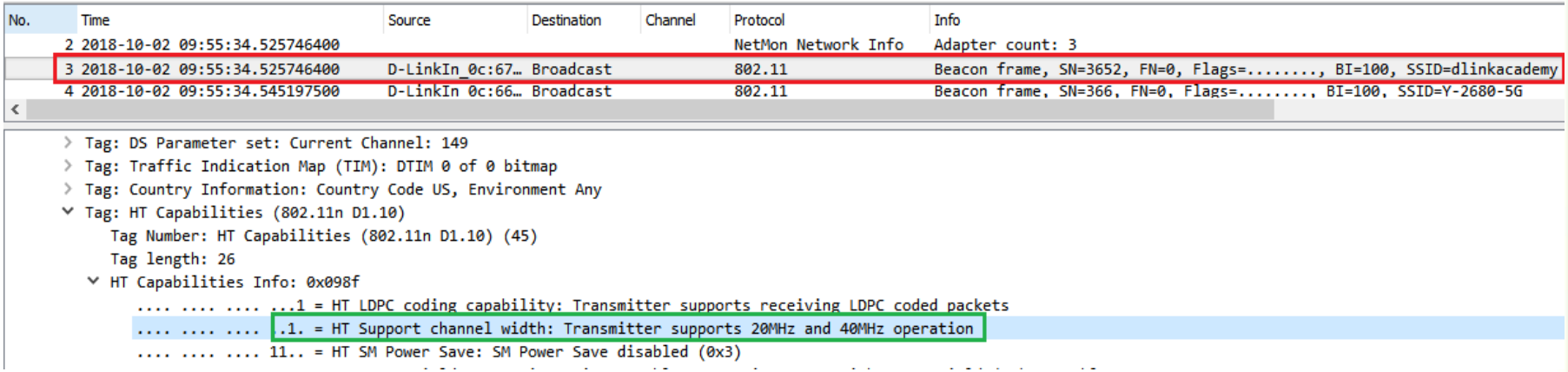
Channel Width

- Channel Width
- Menu: Profile > academy > training > Performance



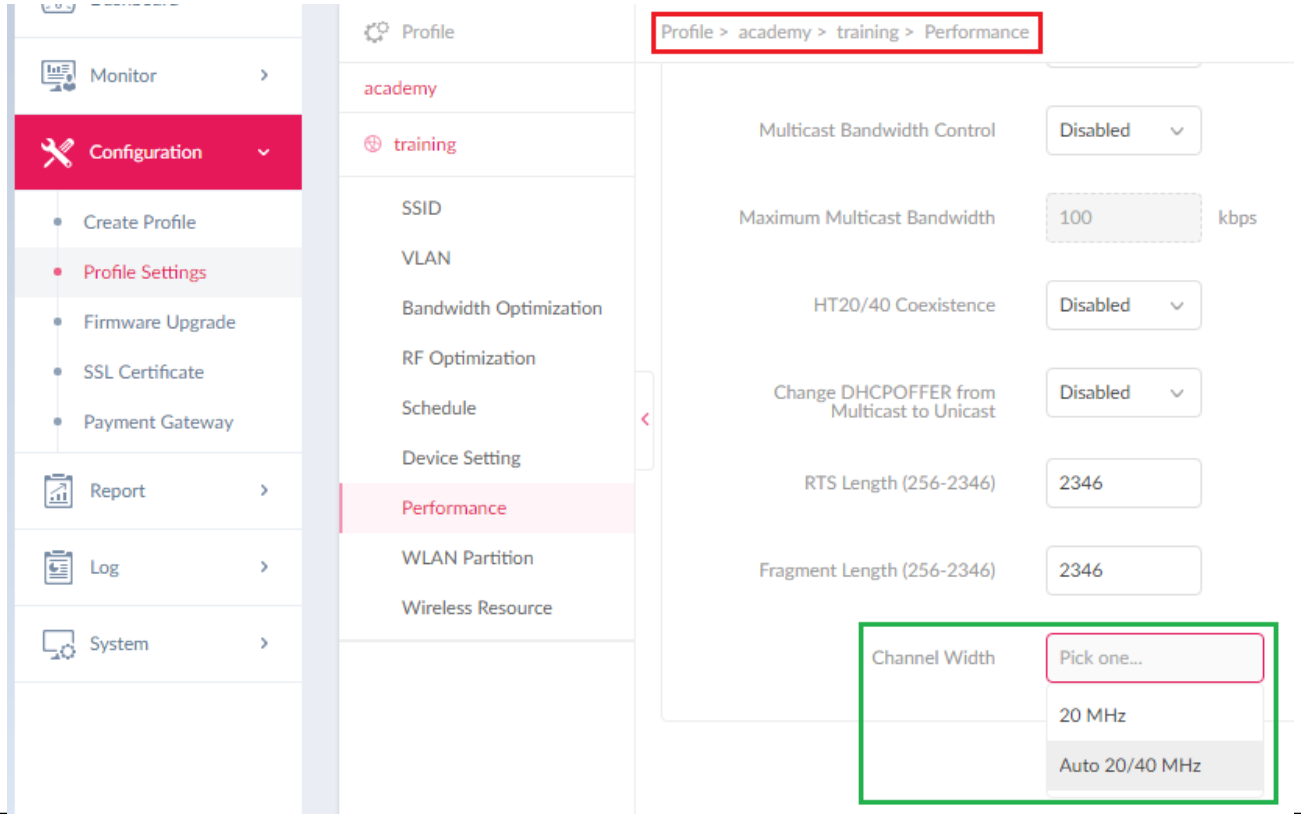
802.11a/b/g: 20-Mhz channel (48 carrier signals); 40-Mhz channel (96)

802.11n: 20-Mhz (52 carrier signals); 40-Mhz (108)



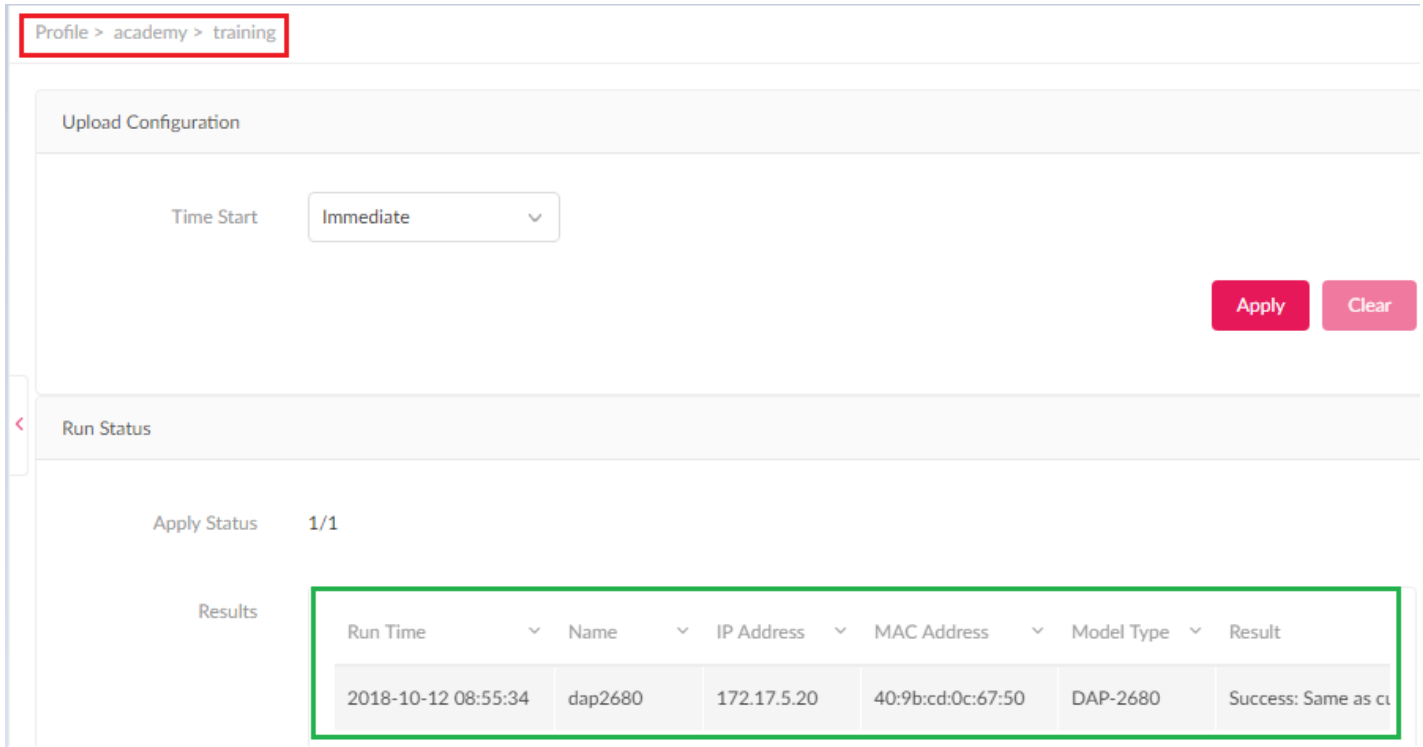
Channel Width Modification (1/3)

- Lab Scenario: Channel Width modification
- Menu: Profile > academy > training > Performance
- Channel Width, from Auto 20/40 MHz to 20 MHz



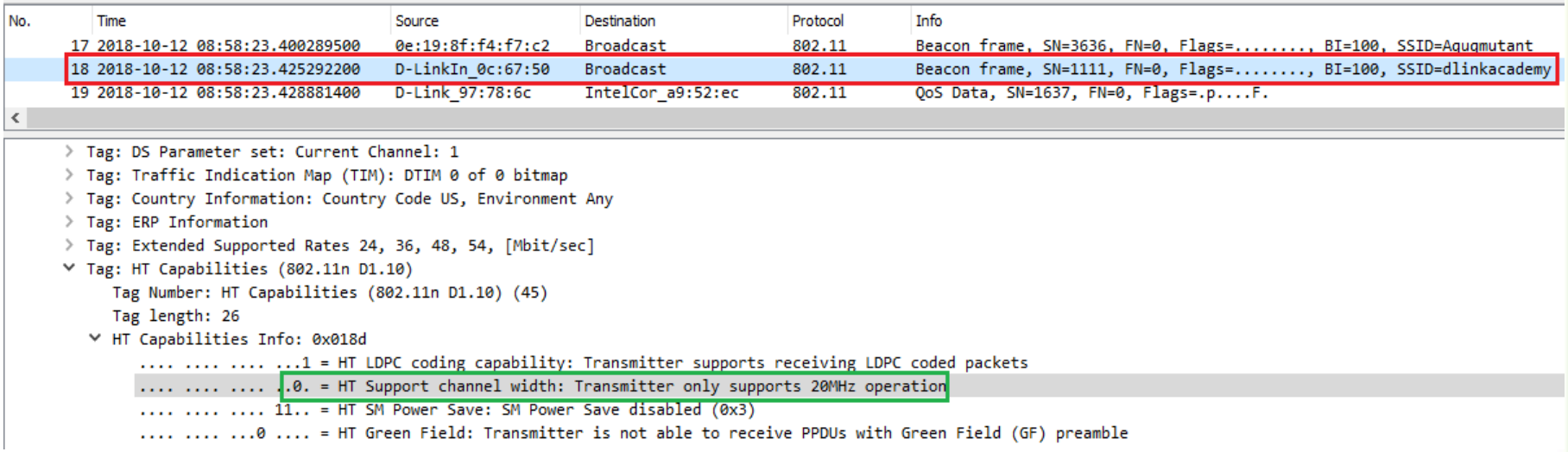
Channel Width Modification (2/3)

- Lab Scenario: Channel Width modification
- Menu: Profile > academy > training > Performance
- Channel Width, from Auto 20/40 MHz to 20 MHz



Channel Width Modification (3/3)

- Lab Scenario: Channel Width modification
- Wireshark capture shows the latest Channel Width: 20 MHz



No.	Time	Source	Destination	Protocol	Info
17	2018-10-12 08:58:23.400289500	0e:19:8f:f4:f7:c2	Broadcast	802.11	Beacon frame, SN=3636, FN=0, Flags=........, BI=100, SSID=Aquqmutant
18	2018-10-12 08:58:23.425292200	D-LinkIn_0c:67:50	Broadcast	802.11	Beacon frame, SN=1111, FN=0, Flags=........, BI=100, SSID=dlinkacademy
19	2018-10-12 08:58:23.428881400	D-Link_97:78:6c	IntelCor_a9:52:ec	802.11	QoS Data, SN=1637, FN=0, Flags=.p....F.

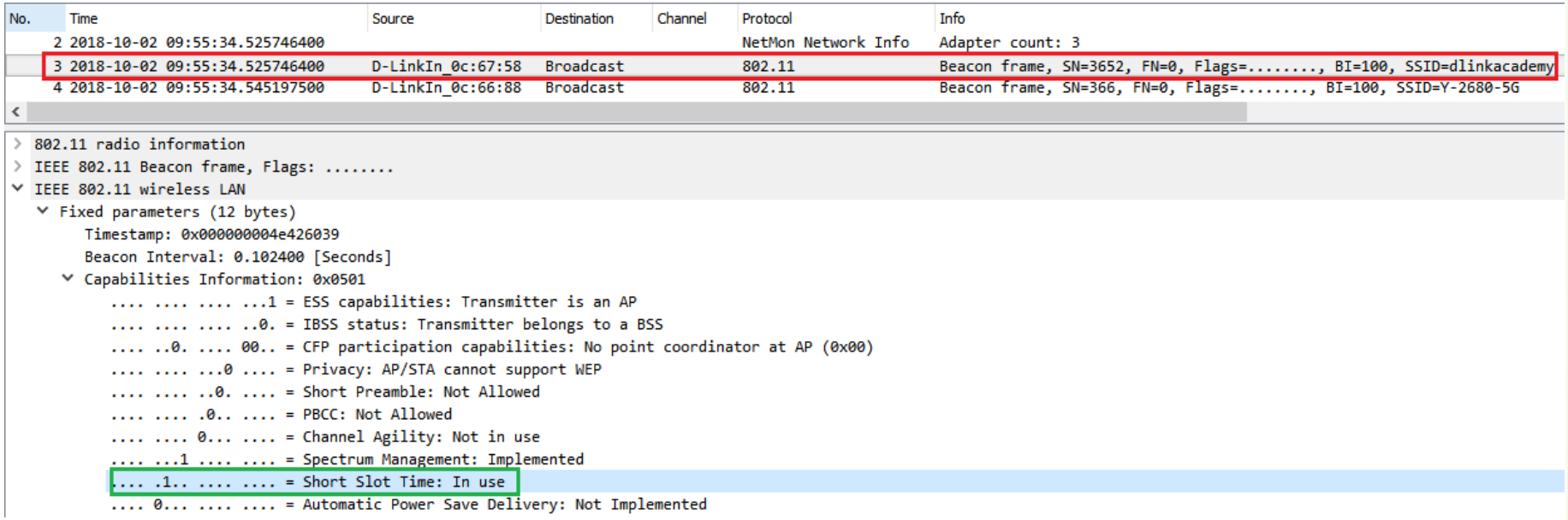
```
> Tag: DS Parameter set: Current Channel: 1
> Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
> Tag: Country Information: Country Code US, Environment Any
> Tag: ERP Information
> Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
v Tag: HT Capabilities (802.11n D1.10)
    Tag Number: HT Capabilities (802.11n D1.10) (45)
    Tag length: 26
  v HT Capabilities Info: 0x018d
      .... .... .... ...1 = HT LDPC coding capability: Transmitter supports receiving LDPC coded packets
      .... .... .... ..0. = HT Support channel width: Transmitter only supports 20MHz operation
      .... .... .... 11.. = HT SM Power Save: SM Power Save disabled (0x3)
      .... .... ...0 .... = HT Green Field: Transmitter is not able to receive PPDUs with Green Field (GF) preamble
```

Short Slot Time

- Short slot time represents the amount of time a device waits after a collision before retransmitting a packet. (an 802.11g-only feature)
- By enabling short slot time, the throughput on 802.11g, 2.4GHz radios can be increased.
- Once short slot time is activated, the wireless device uses the short slot time only when all clients associated to the 802.11g, 2.4GHz radio support short slot time.

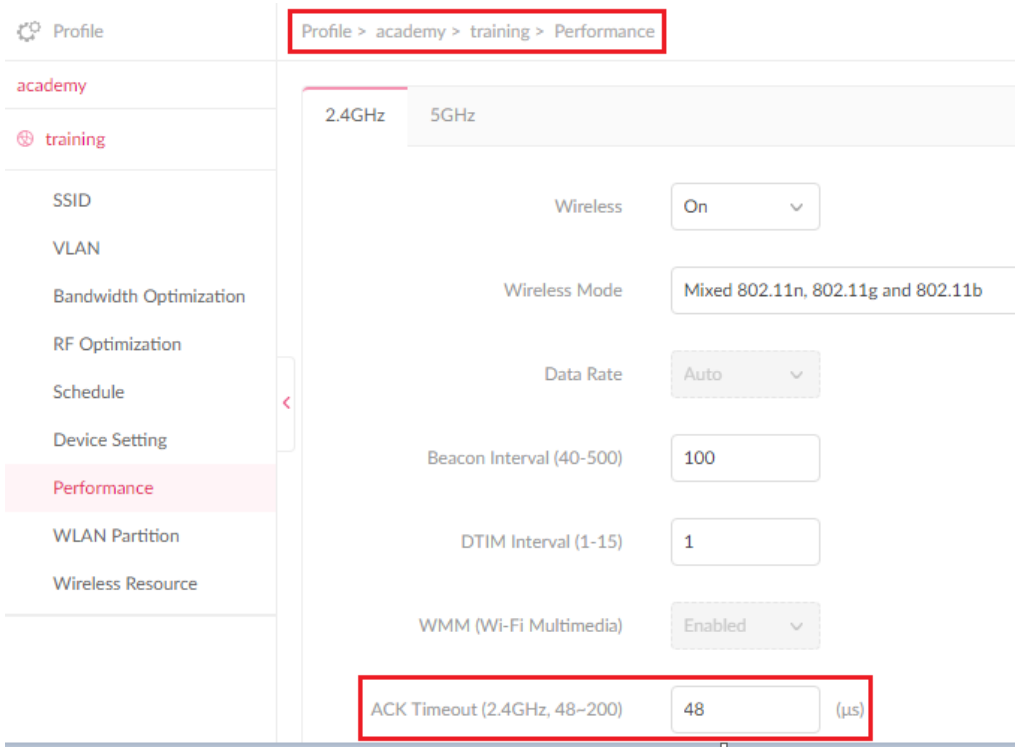
IEEE 802.11 Wireless LAN Capabilities Information

- IEEE 802.11 Wireless LAN, Fixed Parameters
- Short Slot Time
  - Only the wireless devices with clients associated to the 802.11g, 2.4GHz radio support slot time.
  - To improve WiFi performance on the 802.11g, 2.4GHz radio.



ACK TimeOut

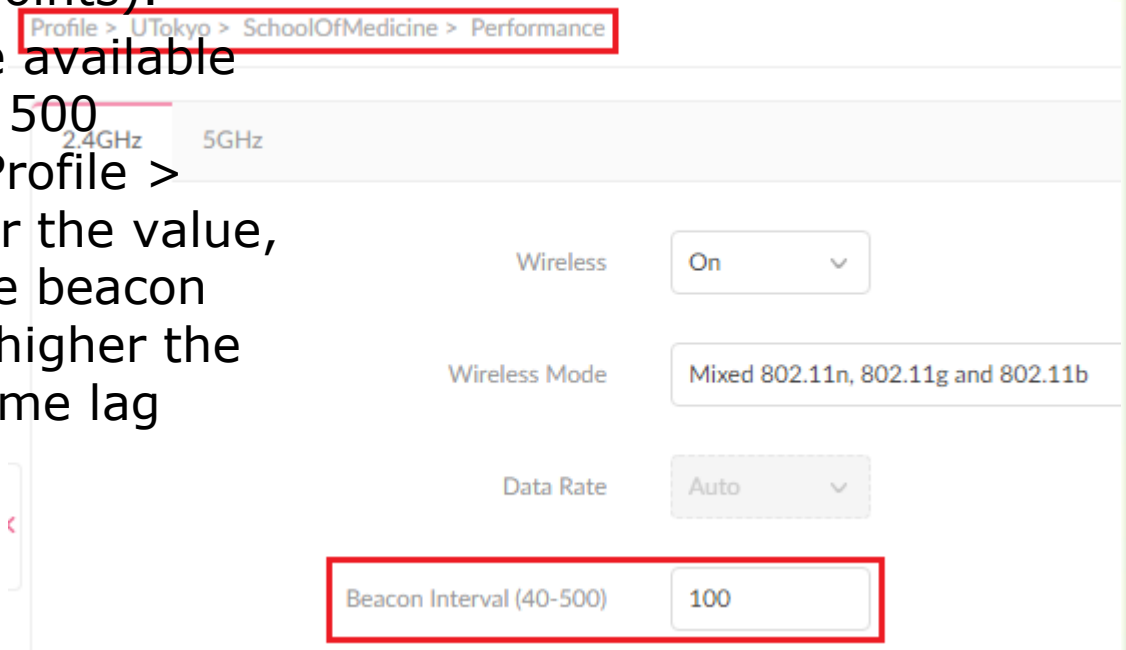
- The Ack TimeOut (2.4GHz, 64-200) indicates a value to optimize throughput over long distance links.
- Menu: Profile > Profile Settings > Site > Network > Performance > ACK Timeout (2.4GHz, 48~200)



Beacon Interval

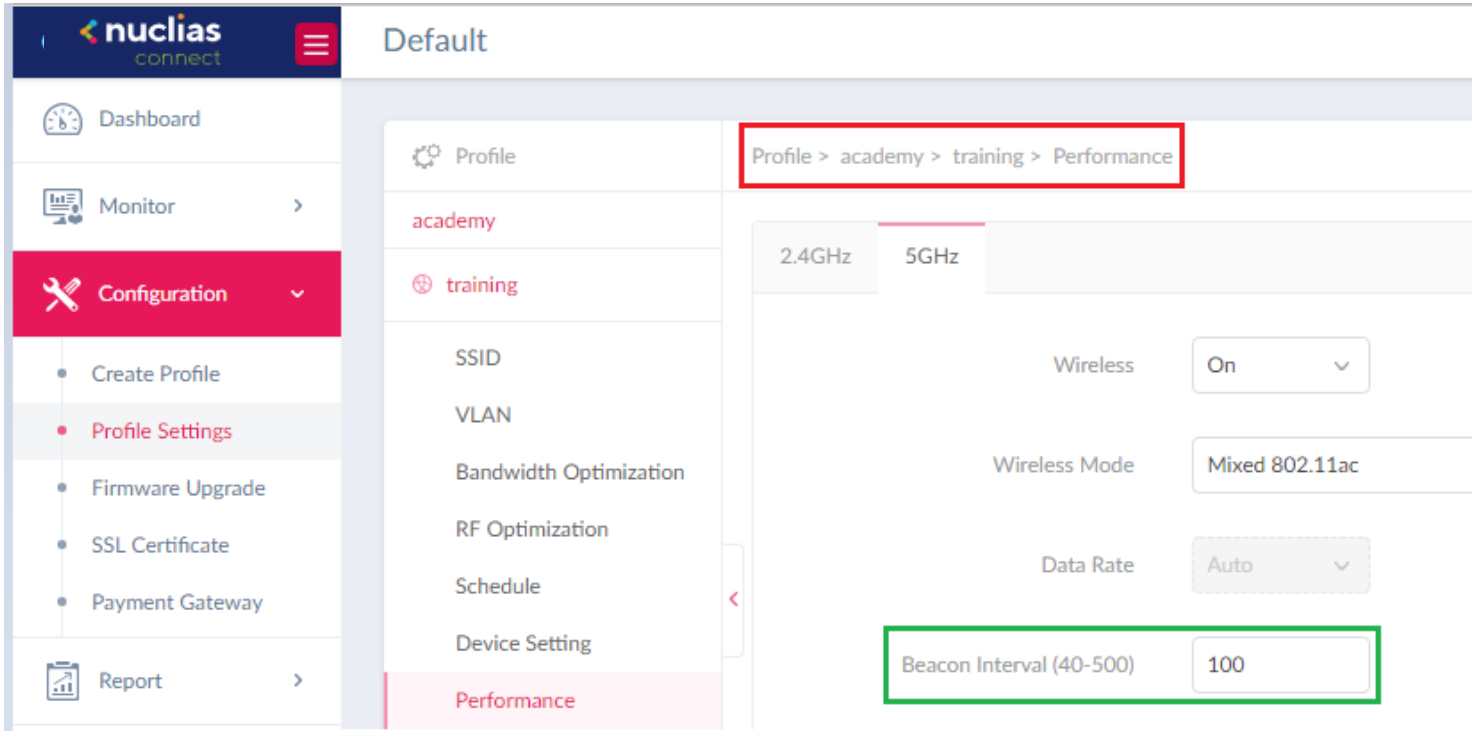
Beacon Interval

- Beacon Broadcast interval is the time lag between each of the beacons sent by DAPs (access points).
- In Nuclias Connect, the available range is between 40 ~ 500 nanoseconds. (Menu: Profile > Performance) The lower the value, the more frequently the beacon frame is sent out. The higher the value, the bigger the time lag between beacons.



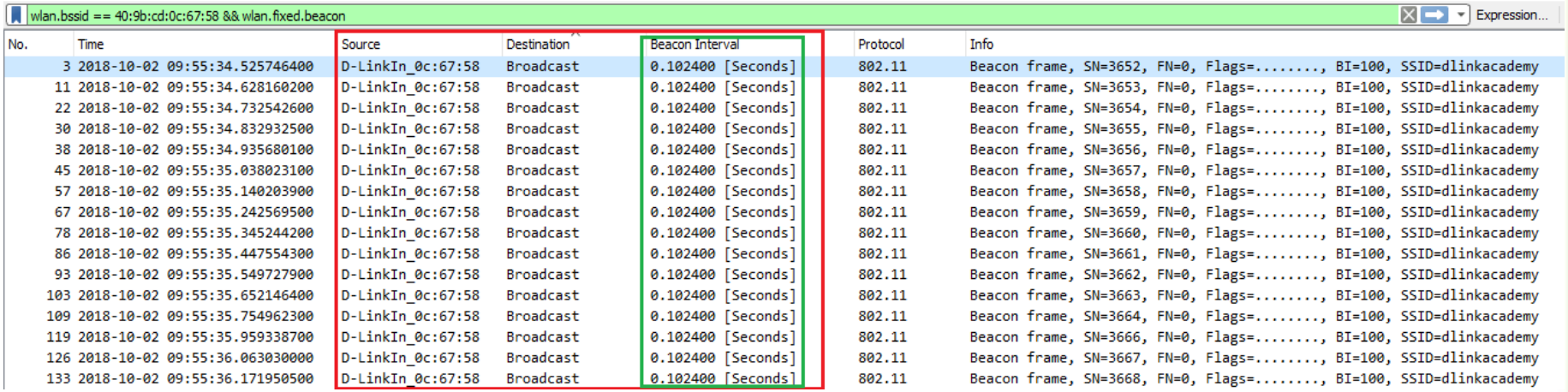
Beacon Interval (1/2)

- IEEE 802.11 Wireless LAN, Fixed Parameters
- Beacon Interval, the default Beacon Interval in DNC is 100 ms (by default) (menu: Profile > academy > training > Performance)



Beacon Interval (2/2)

- IEEE 802.11 Wireless LAN, Fixed Parameters
- Beacon Interval, the default Beacon Interval in DNC is 100 ms
- The collected Wireshark capture reflects such settings

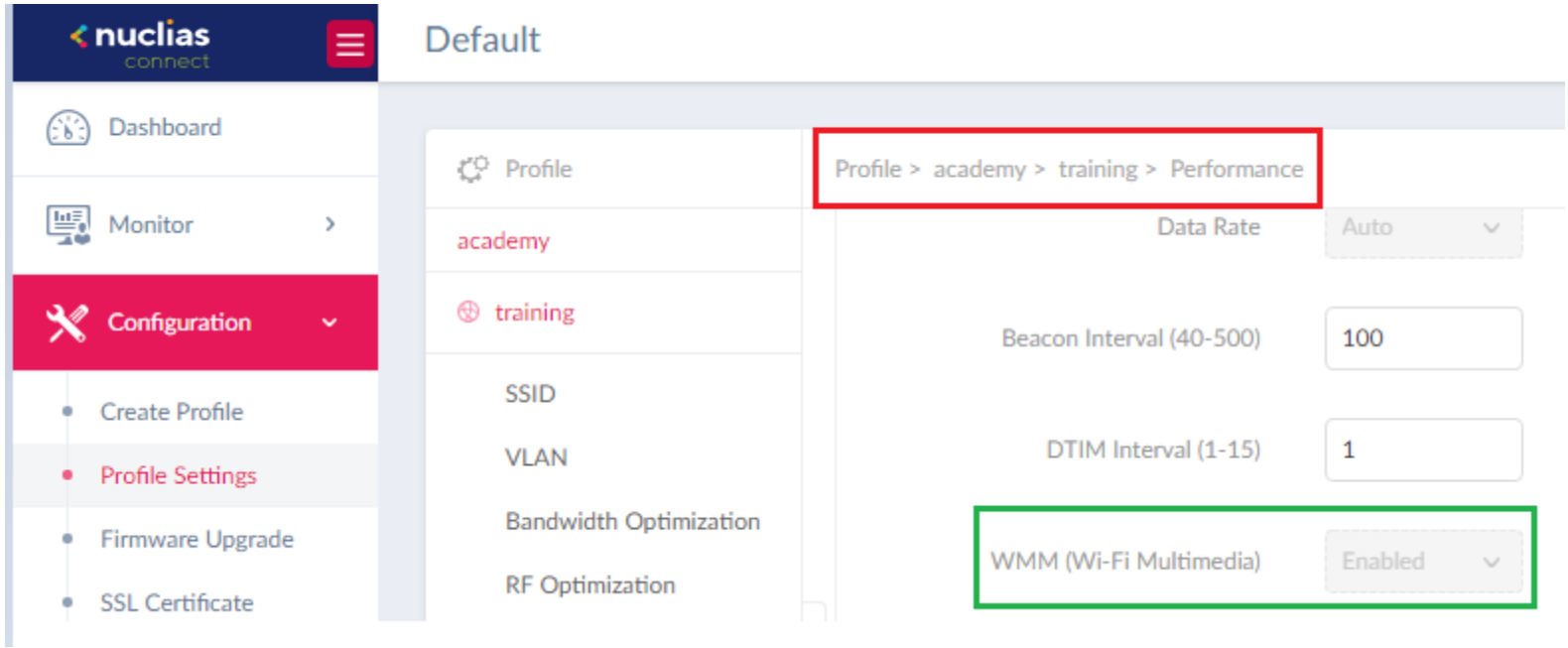


wlan.bssid == 40:9b:cd:0c:67:58 && wlan.fixed.beacon

No.	Time	Source	Destination	Beacon Interval	Protocol	Info
3	2018-10-02 09:55:34.525746400	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3652, FN=0, Flags=........, BI=100, SSID=dlinkacademy
11	2018-10-02 09:55:34.628160200	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3653, FN=0, Flags=........, BI=100, SSID=dlinkacademy
22	2018-10-02 09:55:34.732542600	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3654, FN=0, Flags=........, BI=100, SSID=dlinkacademy
30	2018-10-02 09:55:34.832932500	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3655, FN=0, Flags=........, BI=100, SSID=dlinkacademy
38	2018-10-02 09:55:34.935680100	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3656, FN=0, Flags=........, BI=100, SSID=dlinkacademy
45	2018-10-02 09:55:35.038023100	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3657, FN=0, Flags=........, BI=100, SSID=dlinkacademy
57	2018-10-02 09:55:35.140203900	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3658, FN=0, Flags=........, BI=100, SSID=dlinkacademy
67	2018-10-02 09:55:35.242569500	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3659, FN=0, Flags=........, BI=100, SSID=dlinkacademy
78	2018-10-02 09:55:35.345244200	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3660, FN=0, Flags=........, BI=100, SSID=dlinkacademy
86	2018-10-02 09:55:35.447554300	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3661, FN=0, Flags=........, BI=100, SSID=dlinkacademy
93	2018-10-02 09:55:35.549727900	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3662, FN=0, Flags=........, BI=100, SSID=dlinkacademy
103	2018-10-02 09:55:35.652146400	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3663, FN=0, Flags=........, BI=100, SSID=dlinkacademy
109	2018-10-02 09:55:35.754962300	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3664, FN=0, Flags=........, BI=100, SSID=dlinkacademy
119	2018-10-02 09:55:35.959338700	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3666, FN=0, Flags=........, BI=100, SSID=dlinkacademy
126	2018-10-02 09:55:36.063030000	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3667, FN=0, Flags=........, BI=100, SSID=dlinkacademy
133	2018-10-02 09:55:36.171950500	D-LinkIn_0c:67:58	Broadcast	0.102400 [Seconds]	802.11	Beacon frame, SN=3668, FN=0, Flags=........, BI=100, SSID=dlinkacademy

Wi-Fi Multimedia (WMM) (1/2)

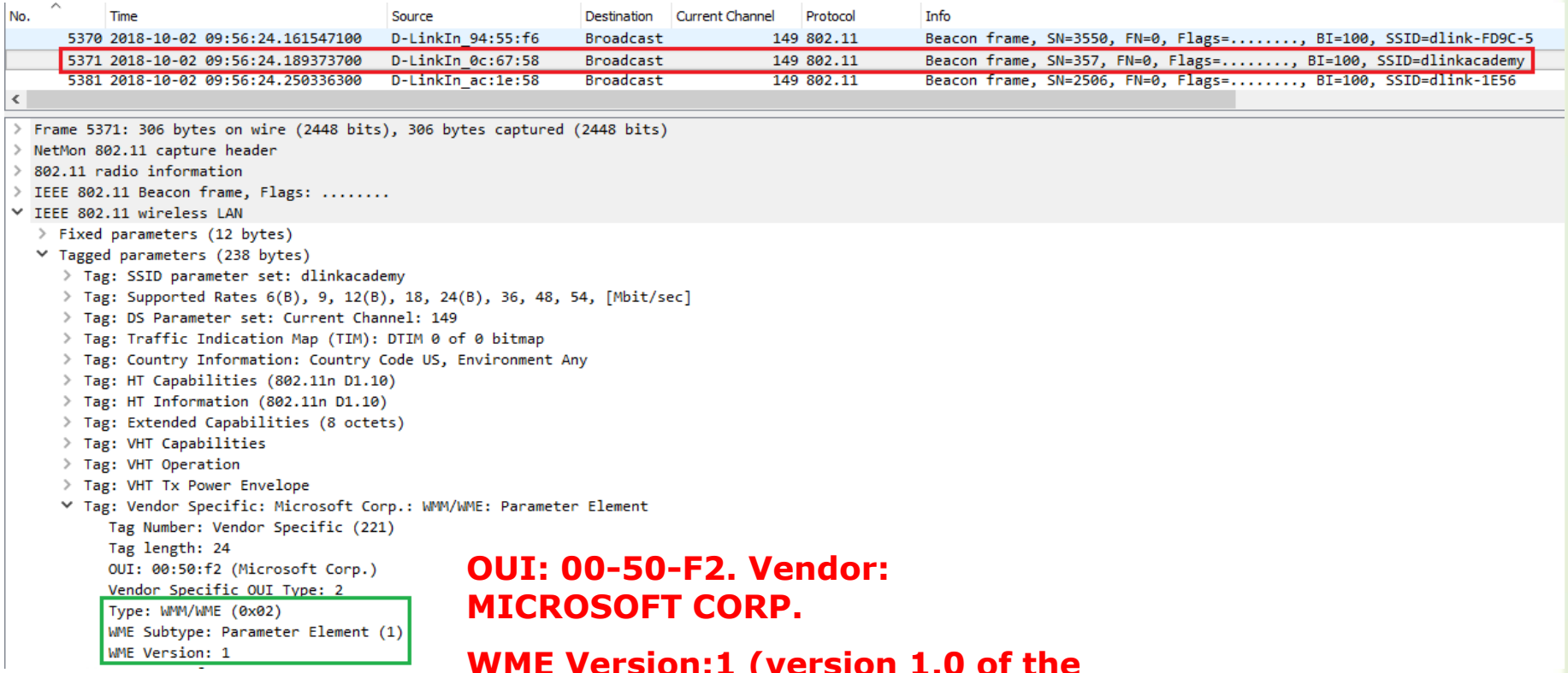
- Wi-Fi Multimedia (WMM) is a subset of the 802.11e wireless LAN (WLAN) specification that enhances quality of service (QoS) on a network by prioritizing data packets according to four categories.
- WMM is also known as Wireless Multimedia Extensions (WME).



Enabled by default

Wi-Fi Multimedia (WMM) (2/2)

- Wi-Fi Multimedia (WMM) is shown in a Wireshark capture.

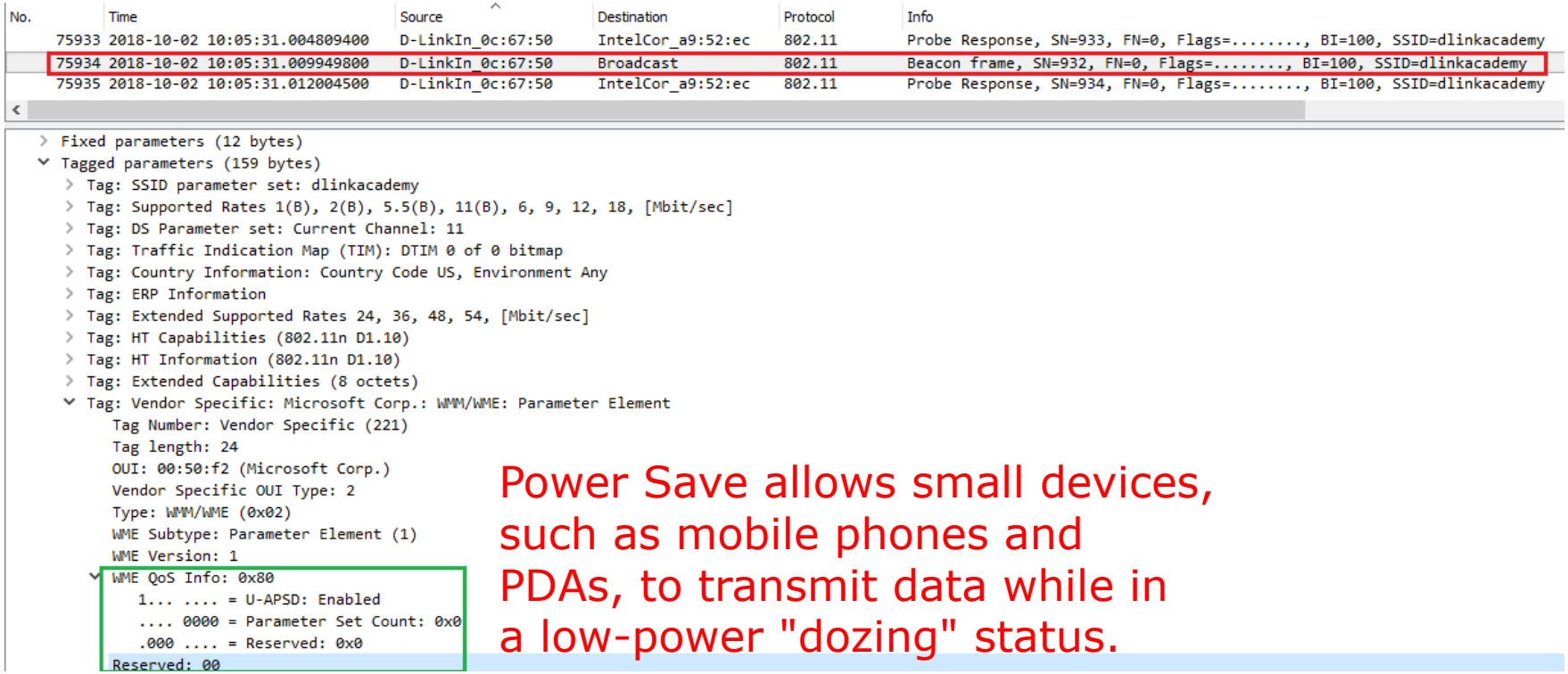


OUI: 00-50-F2. Vendor: MICROSOFT CORP.

WME Version:1 (version 1.0 of the WME specification)

Wireless Multimedia Extensions (WME) QoS

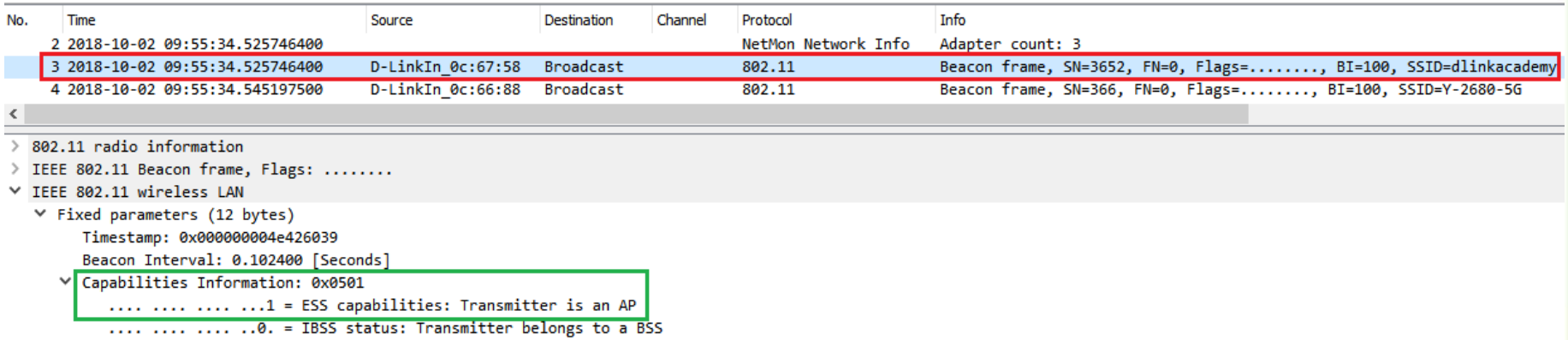
- U-APSD, an optional part of the IEEE amendment 802.11e QoS, is a power-save mechanism.
- U-APSD is also known as WMM Power Save.



Power Save allows small devices, such as mobile phones and PDAs, to transmit data while in a low-power "dozing" status.

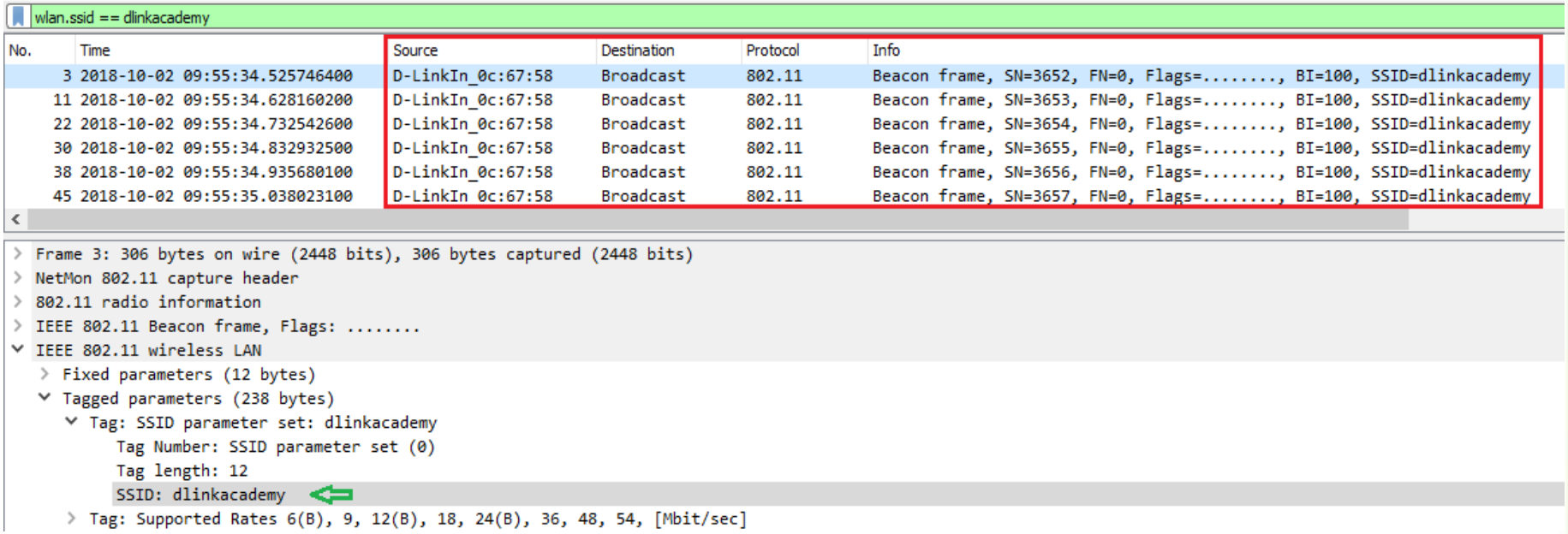
IEEE 802.11 Wireless LAN Capabilities Information

- IEEE 802.11 Wireless LAN, Fixed Parameters
- Extended Service Set (ESS) capabilities
  - Each BSS consists of a single access point (AP) together with all wireless client devices (stations, also called STAs) creating a local or enterprise 802.11 wireless LAN (WLAN).



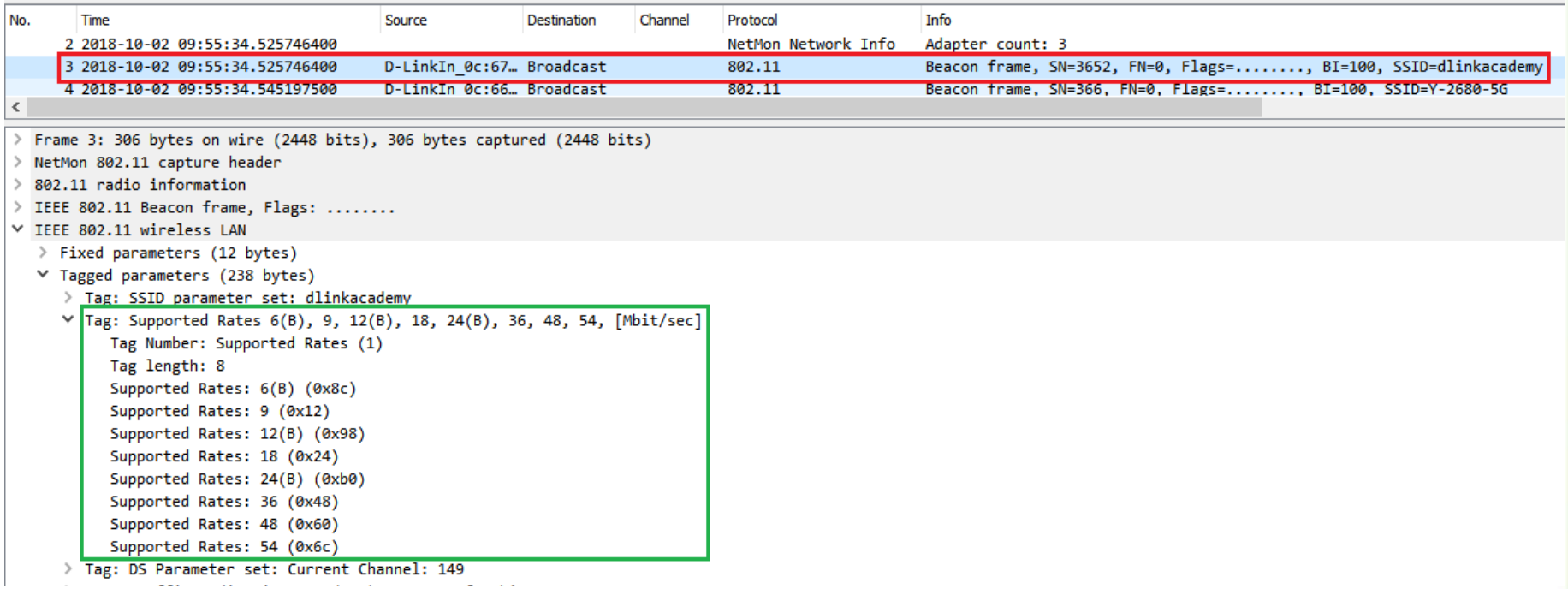
Service Set Identifier (SSID)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- Service Set Identifier (SSID) parameter set
- A beacon frame is sent from DAP-2680 (MAC: 409b:cd0c:6758) with SSID of "dlinkacademy"



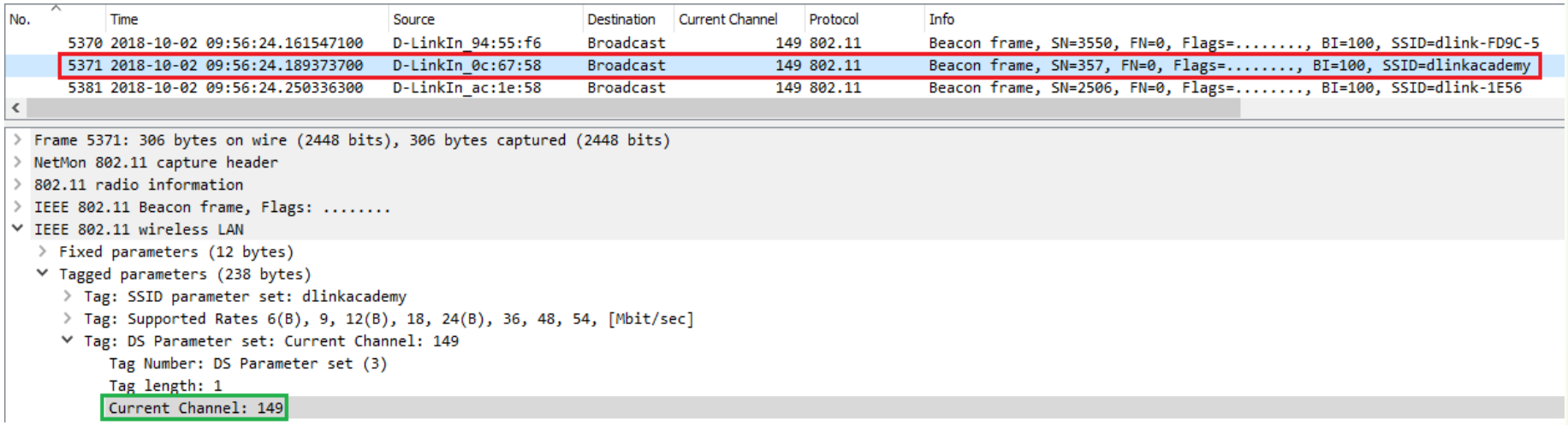
Supported Rates

- IEEE 802.11 Wireless LAN, Tagged Parameters
- Supported Rates
- DAP-2680 802.11 supported rates include
  - 6 (B), 9, 12 (B), 18, 24 (B), 36, 48, 54 [Mbit/sec]



DS (Direct Sequence) Parameter Set

- IEEE 802.11 Wireless LAN, Tagged Parameters
- DS Parameter set, current channel
- This wireless client (Dell laptop, IP: 172.17.5.116) is connected to wireless channel 149.



No.	Time	Source	Destination	Current Channel	Protocol	Info
5370	2018-10-02 09:56:24.161547100	D-LinkIn_94:55:f6	Broadcast	149	802.11	Beacon frame, SN=3550, FN=0, Flags=........, BI=100, SSID=dlink-FD9C-5
5371	2018-10-02 09:56:24.189373700	D-LinkIn_0c:67:58	Broadcast	149	802.11	Beacon frame, SN=357, FN=0, Flags=........, BI=100, SSID=dlinkacademy
5381	2018-10-02 09:56:24.250336300	D-LinkIn_ac:1e:58	Broadcast	149	802.11	Beacon frame, SN=2506, FN=0, Flags=........, BI=100, SSID=dlink-1E56

```
> Frame 5371: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits)
> NetMon 802.11 capture header
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 wireless LAN
    > Fixed parameters (12 bytes)
    v Tagged parameters (238 bytes)
        > Tag: SSID parameter set: dlinkacademy
        > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
        v Tag: DS Parameter set: Current Channel: 149
            Tag Number: DS Parameter set (3)
            Tag length: 1
            Current Channel: 149
```

Traffic Indication Map (TIM)

- Traffic indication map (TIM) is a structure used in 802.11 wireless network management frames.
- The Traffic indication map information element is stated under section 7.3.2.6 of 802.11-1999 standard.
- A bitmap is used to indicate any sleeping listening stations if the Access Point (AP) has any buffered frames present for it.
  - The bit mask is called the Traffic Indication Map and consists of 2008 bits.
- Bitmap Control (1 byte), is used to indicate multicast/broadcast are buffered at the AP and use as space save (bitmap offset)
  - If 1st bit=1, buffered multicast/broadcast data at AP, if 1st bit=0, no multicast/broadcast data at AP.

Traffic Indication Map (TIM)

- Partial Virtual Bitmap (1-251 byte), is a series of flags showing whether each associated STAT has unicast frames buffered at the AP.
  - Represent stations in low power mode for which AP has traffic buffered.
- Each bit in this Partial Virtual Bitmap filed corresponds to an Association Id (AID) of a STA.

Delivery Traffic Indication Message (DTIM)

Delivery Traffic Indication Message

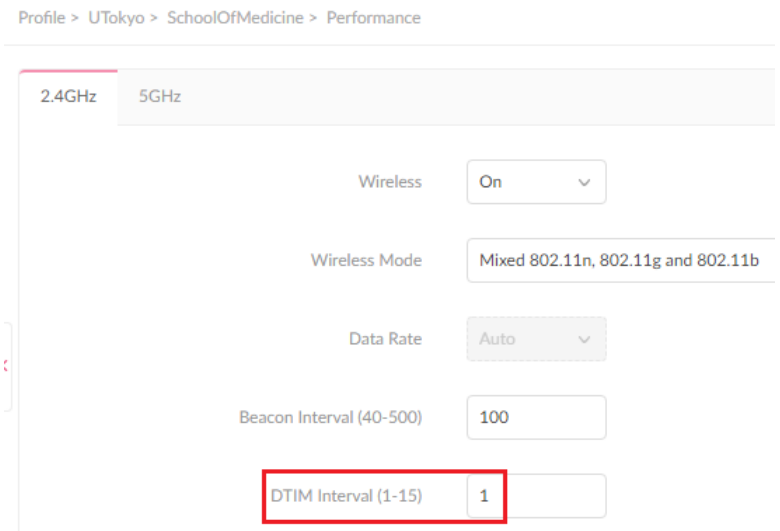
- Power saving is a key consideration when designing wireless network. While a STA in sleep mode, the AP temporary keeps those (buffer) frames.
- DTIM, high number: the longer time a wireless client is being a Power Saving mode (sleep mode), the more power (battery life) being saved. However, it brings inferior throughput (or high latency) [large DTIM numbers might yield a buffer overflow]
- DTIM, low number: it decreases AP's load in saving those buffer frame, at the same time, the wireless client experiences better throughput, but not able to save power
- Nuclias Connect offers the range "DTIM Interval (1-15)" and it applies for all configured SSIDs (menu: Profile > Performance)



Delivery Traffic Indication Message (DTIM)

Delivery Traffic Indication Message

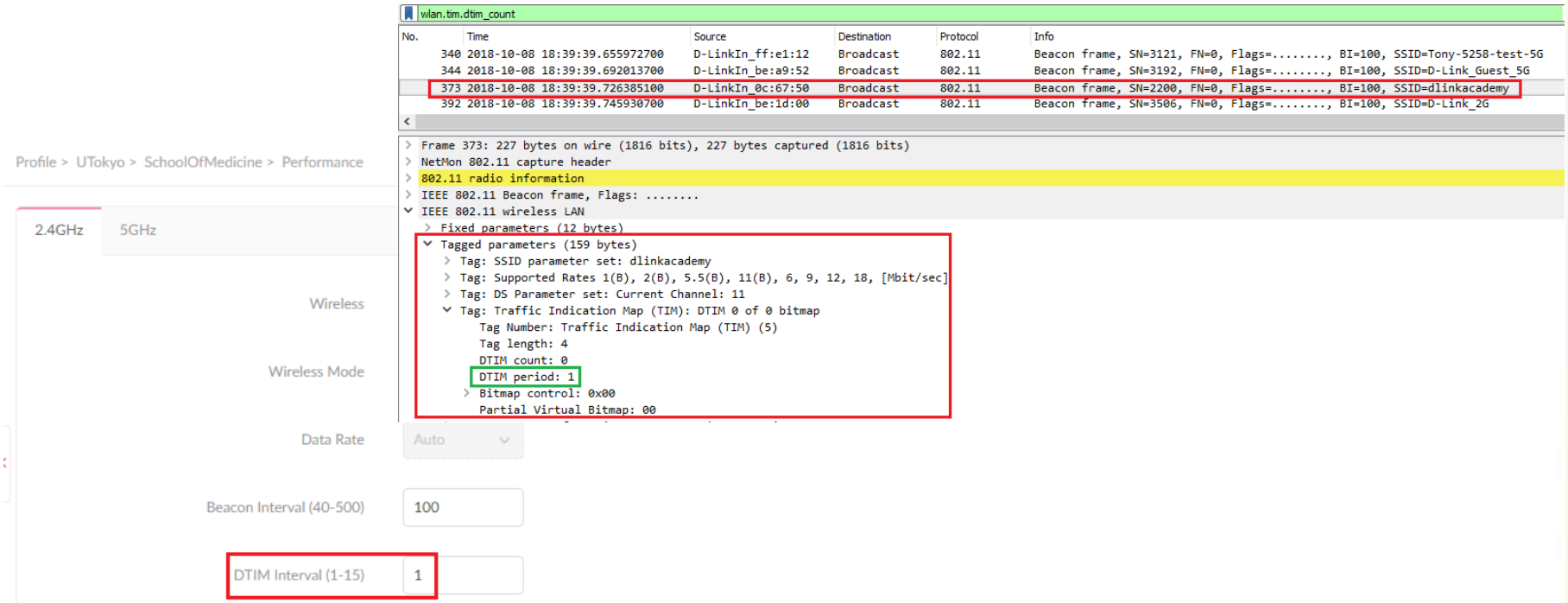
- When the STA wakes up, it reviews the DTIM parameter to see the number of beacon frames this STA needs to wait, to be able to receive the buffer frame.



Delivery Traffic Indication Message (DTIM)

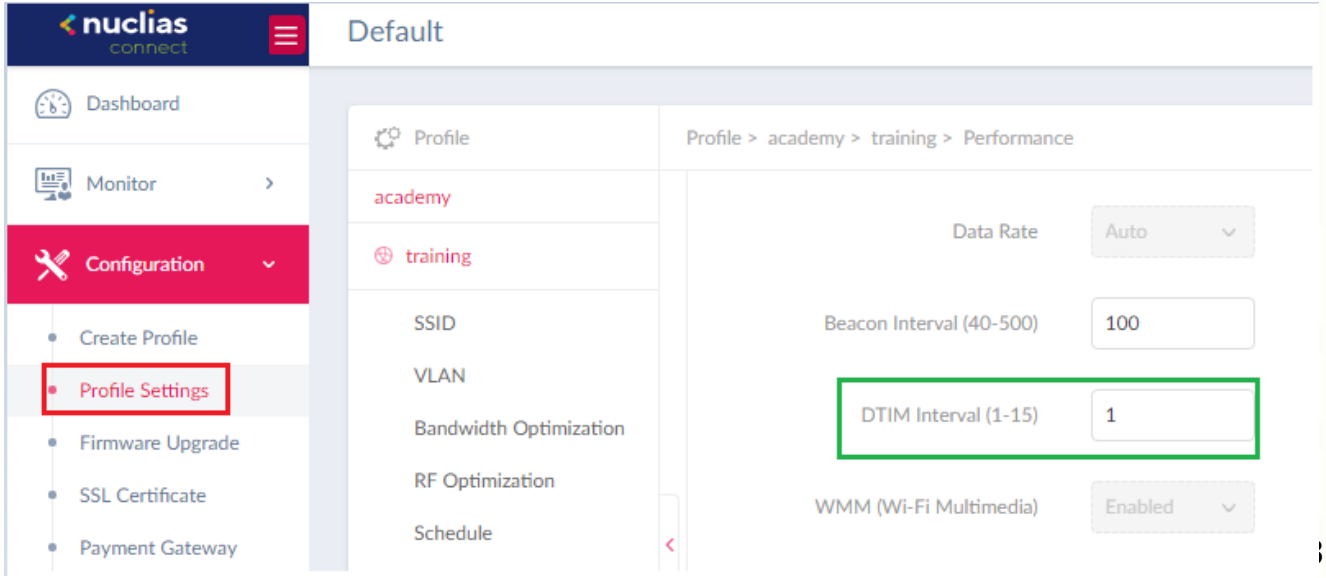
Delivery Traffic Indication Message

- When the STA wakes up, it reviews the DTIM parameter to see the number of beacon frames this STA needs to wait, to be able to receive the buffer frame.



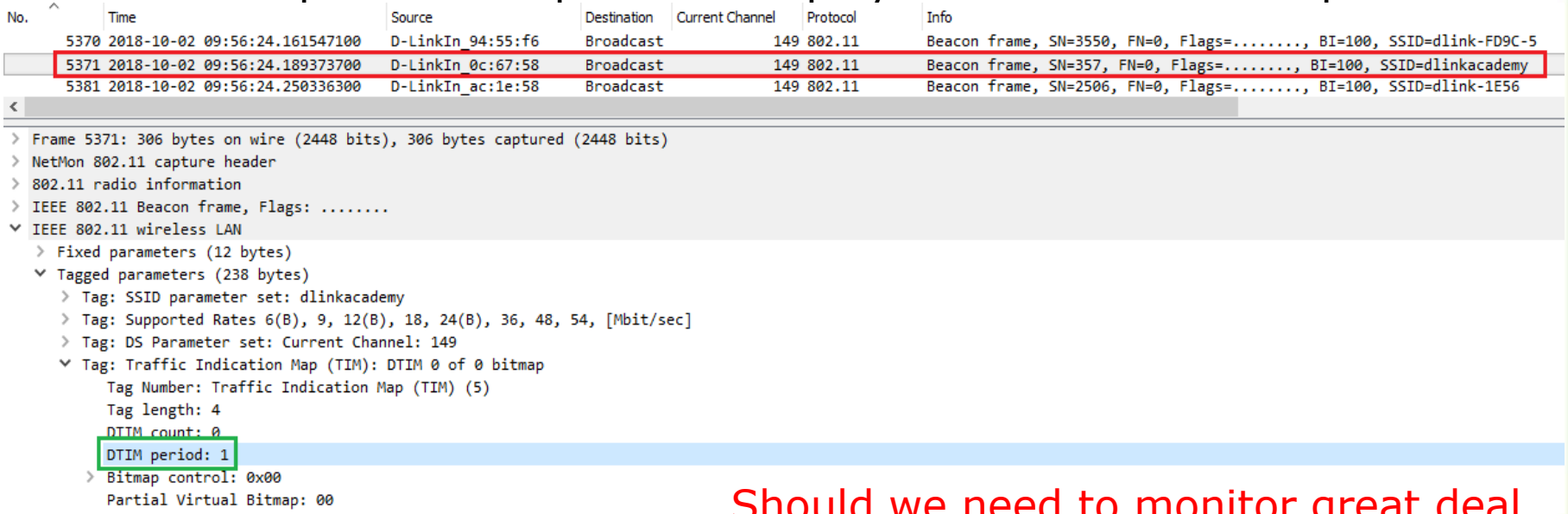
DTIM (Delivery Traffic Indication Map) (1/2)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- DTIM (Delivery traffic indication map or message) is an additional message added after the normal beacon broadcast by an access point.
- DTIM Interval goes hand in hand with the Beacon interval setting, by buffering broadcast and multicast data, letting your mobile devices or clients know when to "wake up" to receive those data.



DTIM (Delivery Traffic Indication Map) (2/2)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- An example of DTIM period is displayed in a Wireshark capture.

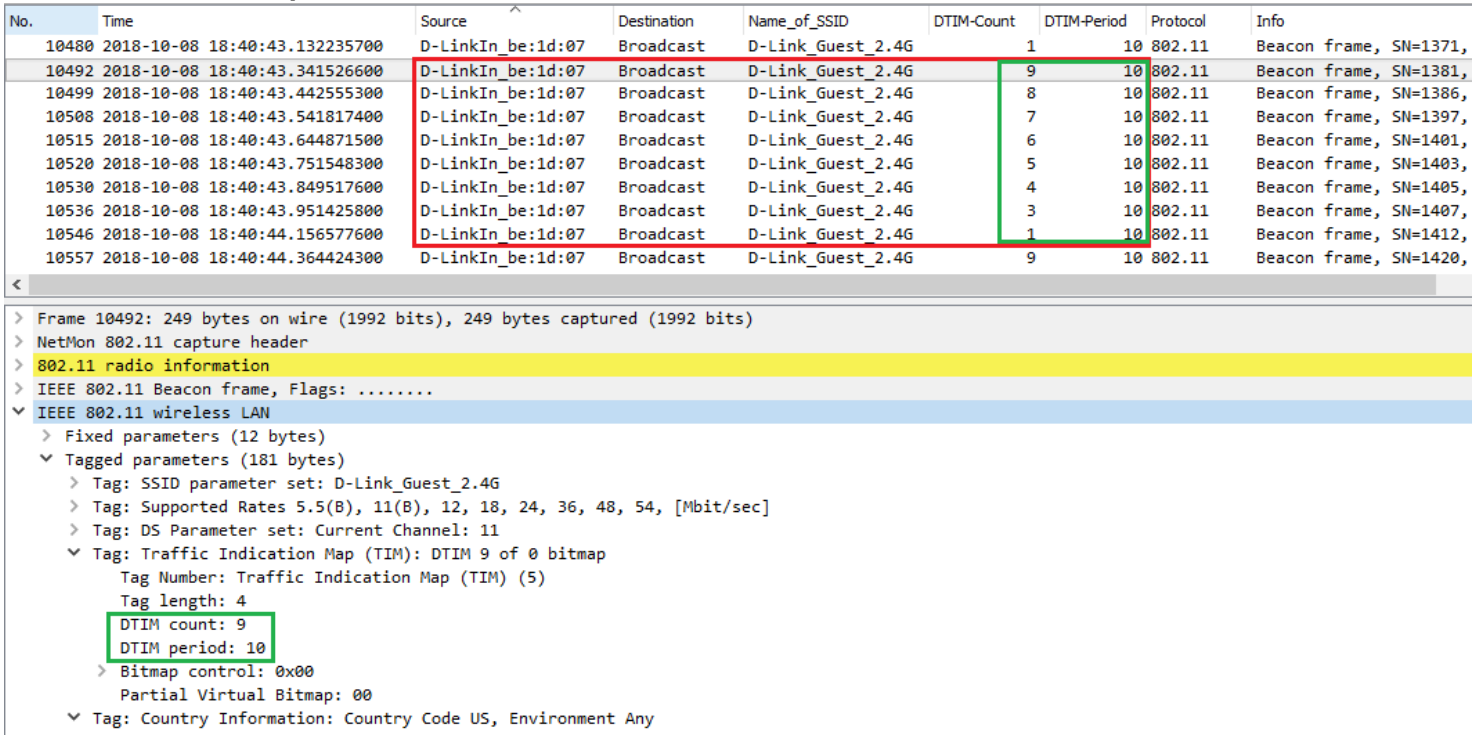


Should we need to monitor great deal of DAPs under DNC, then, it is best practice to reduce DTIM interval in order to reduce RF interference.

Delivery Traffic Indication Message (DTIM)

Delivery Traffic Indication Message

- The below collected Wirehsark capture screenshot is for reference, NOT from DAP/Nuclias Connect.

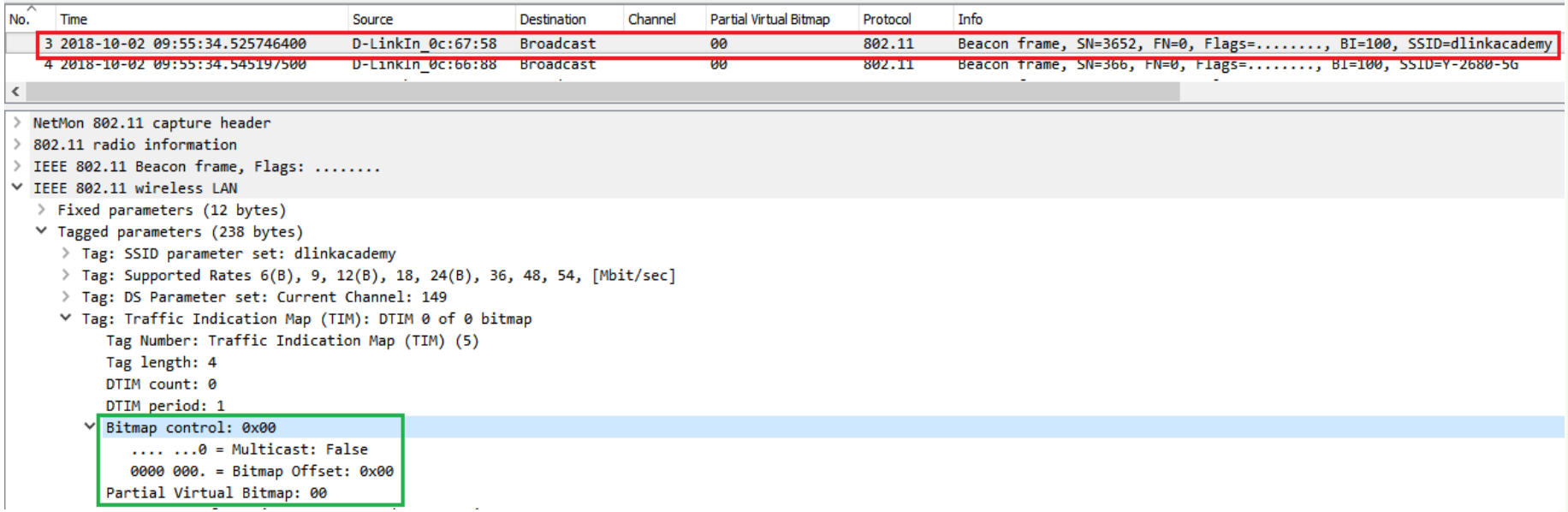


No.	Time	Source	Destination	Name_of_SSID	DTIM-Count	DTIM-Period	Protocol	Info
10480	2018-10-08 18:40:43.132235700	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	1	10	802.11	Beacon frame, SN=1371,
10492	2018-10-08 18:40:43.341526600	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	9	10	802.11	Beacon frame, SN=1381,
10499	2018-10-08 18:40:43.442555300	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	8	10	802.11	Beacon frame, SN=1386,
10508	2018-10-08 18:40:43.541817400	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	7	10	802.11	Beacon frame, SN=1397,
10515	2018-10-08 18:40:43.644871500	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	6	10	802.11	Beacon frame, SN=1401,
10520	2018-10-08 18:40:43.751548300	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	5	10	802.11	Beacon frame, SN=1403,
10530	2018-10-08 18:40:43.849517600	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	4	10	802.11	Beacon frame, SN=1405,
10536	2018-10-08 18:40:43.951425800	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	3	10	802.11	Beacon frame, SN=1407,
10546	2018-10-08 18:40:44.156577600	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	1	10	802.11	Beacon frame, SN=1412,
10557	2018-10-08 18:40:44.364424300	D-LinkIn_be:1d:07	Broadcast	D-Link_Guest_2.4G	9	10	802.11	Beacon frame, SN=1420,

```
> Frame 10492: 249 bytes on wire (1992 bits), 249 bytes captured (1992 bits)
> NetMon 802.11 capture header
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 wireless LAN
  > Fixed parameters (12 bytes)
  v Tagged parameters (181 bytes)
    > Tag: SSID parameter set: D-Link_Guest_2.4G
    > Tag: Supported Rates 5.5(B), 11(B), 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 11
    v Tag: Traffic Indication Map (TIM): DTIM 9 of 0 bitmap
        Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 4
        DTIM count: 9
        DTIM period: 10
      > Bitmap control: 0x00
        Partial Virtual Bitmap: 00
    v Tag: Country Information: Country Code US, Environment Any
```

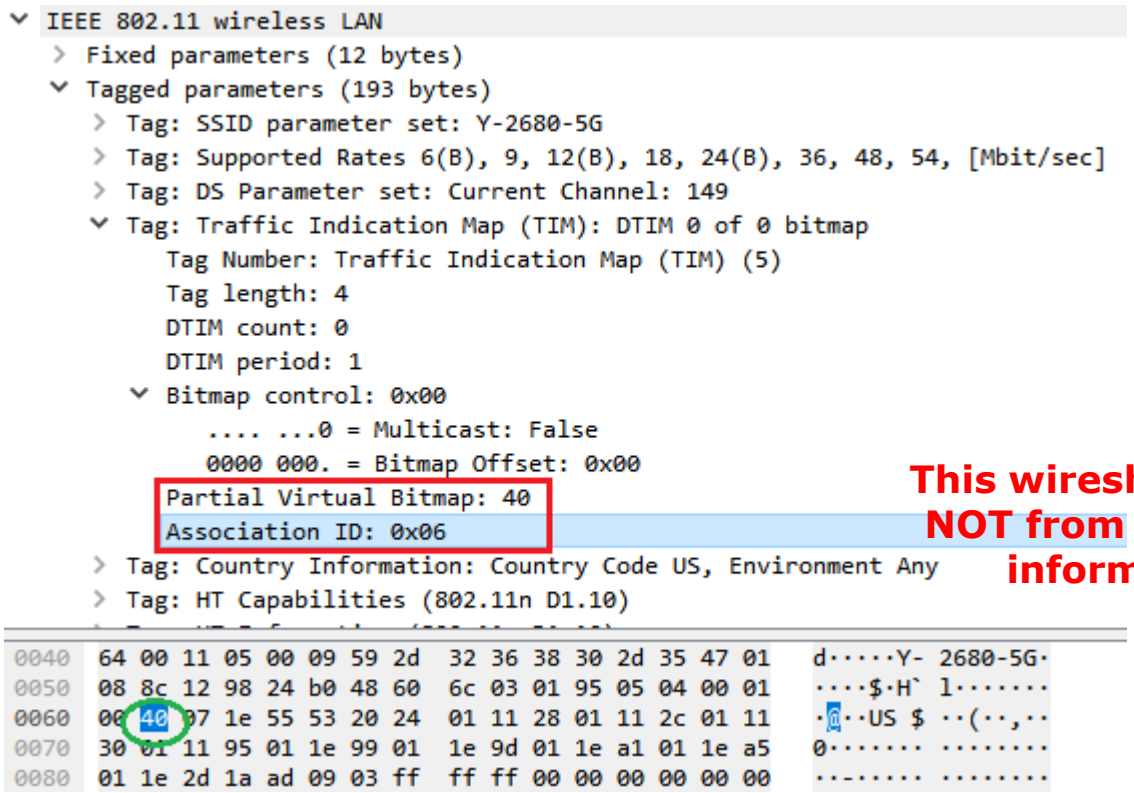
Bitmap Control

- IEEE 802.11 Wireless LAN, Tagged Parameters
- According to below capture, since the 1st bit of Bitmap Control is set to 0, there is no multicast/broadcast data at AP.



Partial Virtual Bitmap

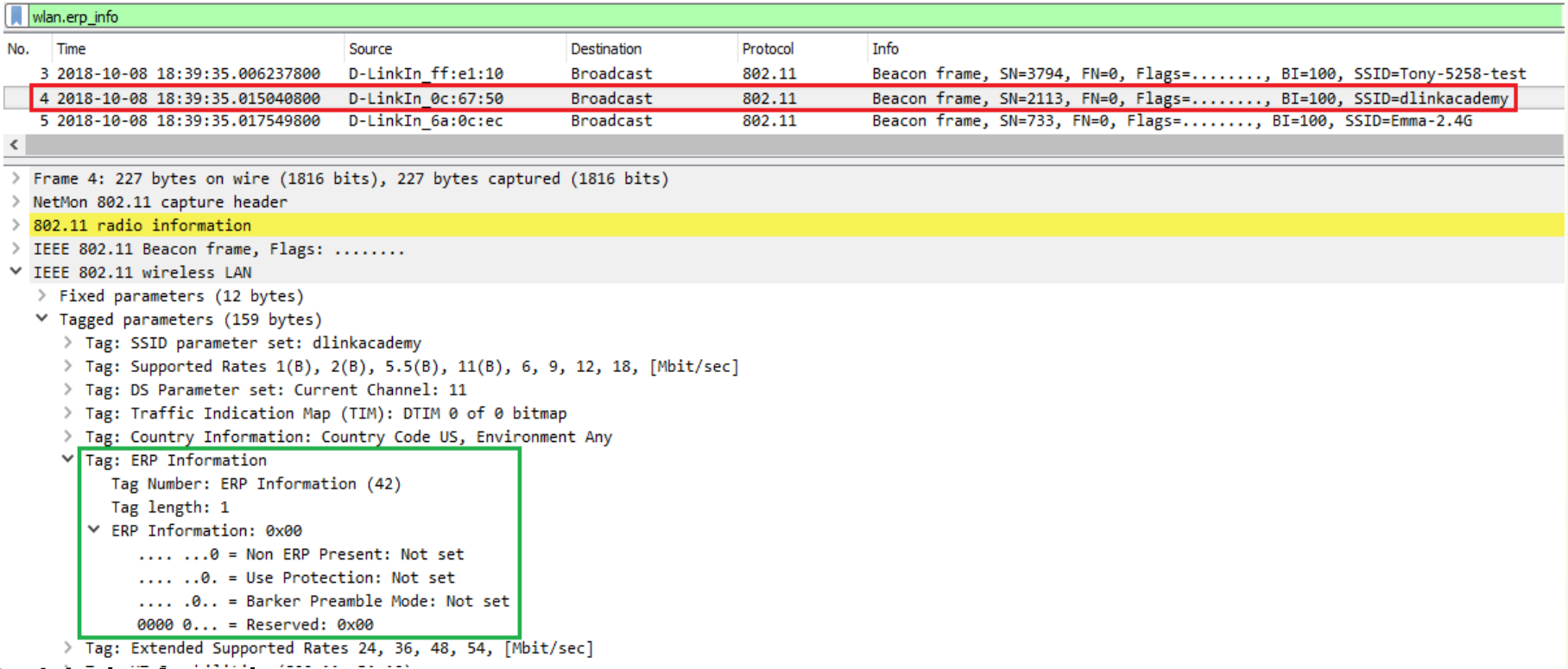
- IEEE 802.11 Wireless LAN, Tagged Parameters
- A Wireshark capture with Partial Virtual Bitmap & Association ID (AID)



This wireshark capture IS NOT from DAP-2680, for information only

Extended-Rate PHY (ERP)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- ERP Information, the extended rate PHY (ERP) is defined by 802.11g.

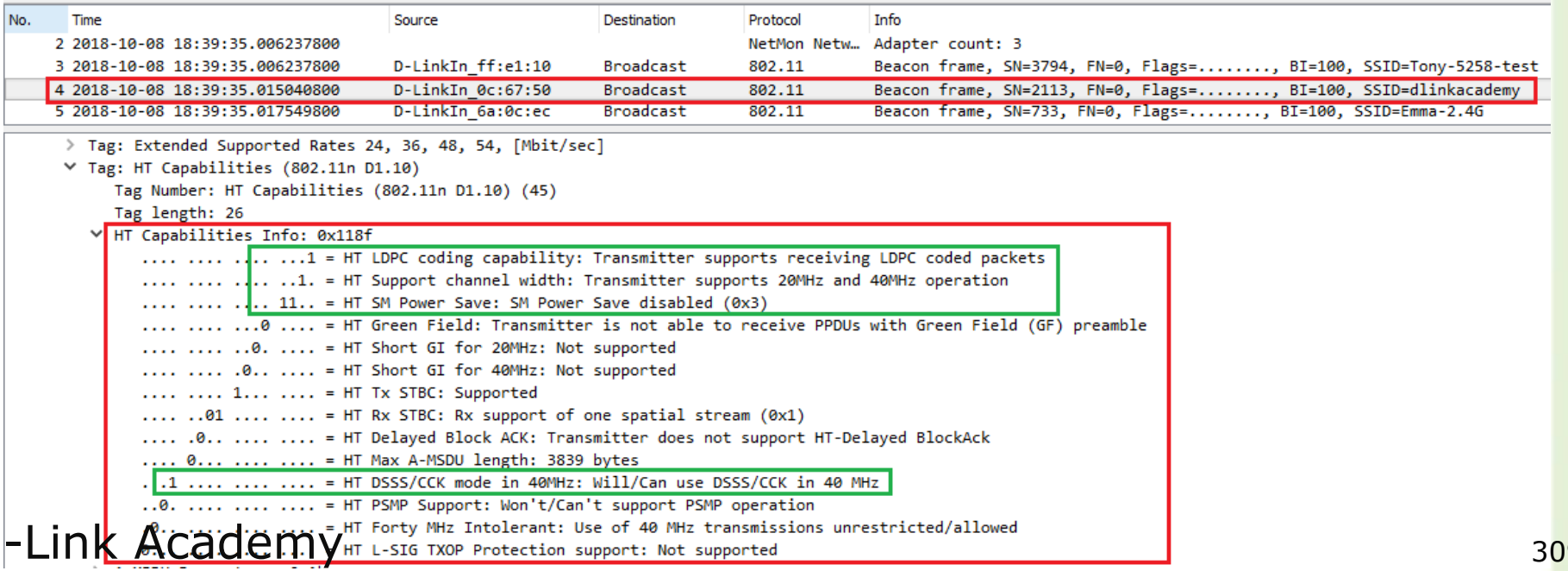


HT (High Throughput) Capabilities (1/3)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- HT Capabilities
  - LDPC Coding Capability: Indicating Low Density Parity Check usage
  - Supported Channel Width: 0 for only 20MHz, 1 for both 20MHz & 40MHz support
  - SM Power Save: to indicate STA SM Power Save capability
  - DSSS/CCK Mode in 40MHz – 1 for Client STA does use DaSS/CCK in 40 MHz

HT (High Throughput) Capabilities (2/3)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- HT Capabilities
  - LDPC Coding Capability
  - Supported Channel Width
  - DSSS/CCK Mode in 40MHz



HT (High Throughput) Capabilities (3/3)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- HT Capabilities
  - Tx Beamforming Capabilities-TxBF (4 bytes) [wlan.txbf.txbf]

No.	Time	Source	Destination	Protocol	Info
2	2018-10-08 18:39:35.006237800			NetMon Netw…	Adapter count: 3
3	2018-10-08 18:39:35.006237800	D-LinkIn_ff:e1:10	Broadcast	802.11	Beacon frame, SN=3794, FN=0, Flags=........, BI=100, SSID=Tony-5258-test
4	2018-10-08 18:39:35.015040800	D-LinkIn_0c:67:50	Broadcast	802.11	Beacon frame, SN=2113, FN=0, Flags=........, BI=100, SSID=dlinkacademy
5	2018-10-08 18:39:35.017549800	D-LinkIn_6a:0c:ec	Broadcast	802.11	Beacon frame, SN=733, FN=0, Flags=........, BI=100, SSID=Emma-2.4G

```
> Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
v Tag: HT Capabilities (802.11n D1.10)
    Tag Number: HT Capabilities (802.11n D1.10) (45)
    Tag length: 26
  > HT Capabilities Info: 0x118f
  > A-MPDU Parameters: 0x1b
  > Rx Supported Modulation and Coding Scheme Set: MCS Set
  > HT Extended Capabilities: 0x0400
  v Transmit Beam Forming (TxBF) Capabilities: 0x0d47e606
      .... .... .... .... .... .... .... ...0 = Transmit Beamforming: Not supported
      .... .... .... .... .... .... .... ..1. = Receive Staggered Sounding: Supported
      .... .... .... .... .... .... .... .1.. = Transmit Staggered Sounding: Supported
      .... .... .... .... .... .... .... 0... = Receive Null Data packet (NDP): Not supported
      .... .... .... .... .... .... ...0 .... = Transmit Null Data packet (NDP): Not supported
      .... .... .... .... .... .... ..0. .... = Implicit TxBF capable: Not supported
      .... .... .... .... .... .... 00.. .... = Calibration: incapable (0x0)
      .... .... .... .... .... ...0 .... .... = STA can apply TxBF using CSI explicit feedback: Not supported
      .... .... .... .... .... ..1. .... .... = STA can apply TxBF using uncompressed beamforming feedback matrix: Supported
      .... .... .... .... .... .1.. .... .... = STA can apply TxBF using compressed beamforming feedback matrix: Supported
      .... .... .... .... ...0 0... .... .... = Receiver can return explicit CSI feedback: not supported (0x0)
      .... .... .... .... .11. .... .... .... = Receiver can return explicit uncompressed Beamforming Feedback Matrix: delayed and immediate feedback capable (0x3)
      .... .... .... ...1 1... .... .... .... = STA can compress and use compressed Beamforming Feedback Matrix: delayed and immediate feedback capable (0x3)
      .... .... .... .11. .... .... .... .... = Minimal grouping used for explicit feedback reports: Groups of 1, 2, 4 supported (0x3)
```

High Throughput Capabilities, HT Short GI (1/3)

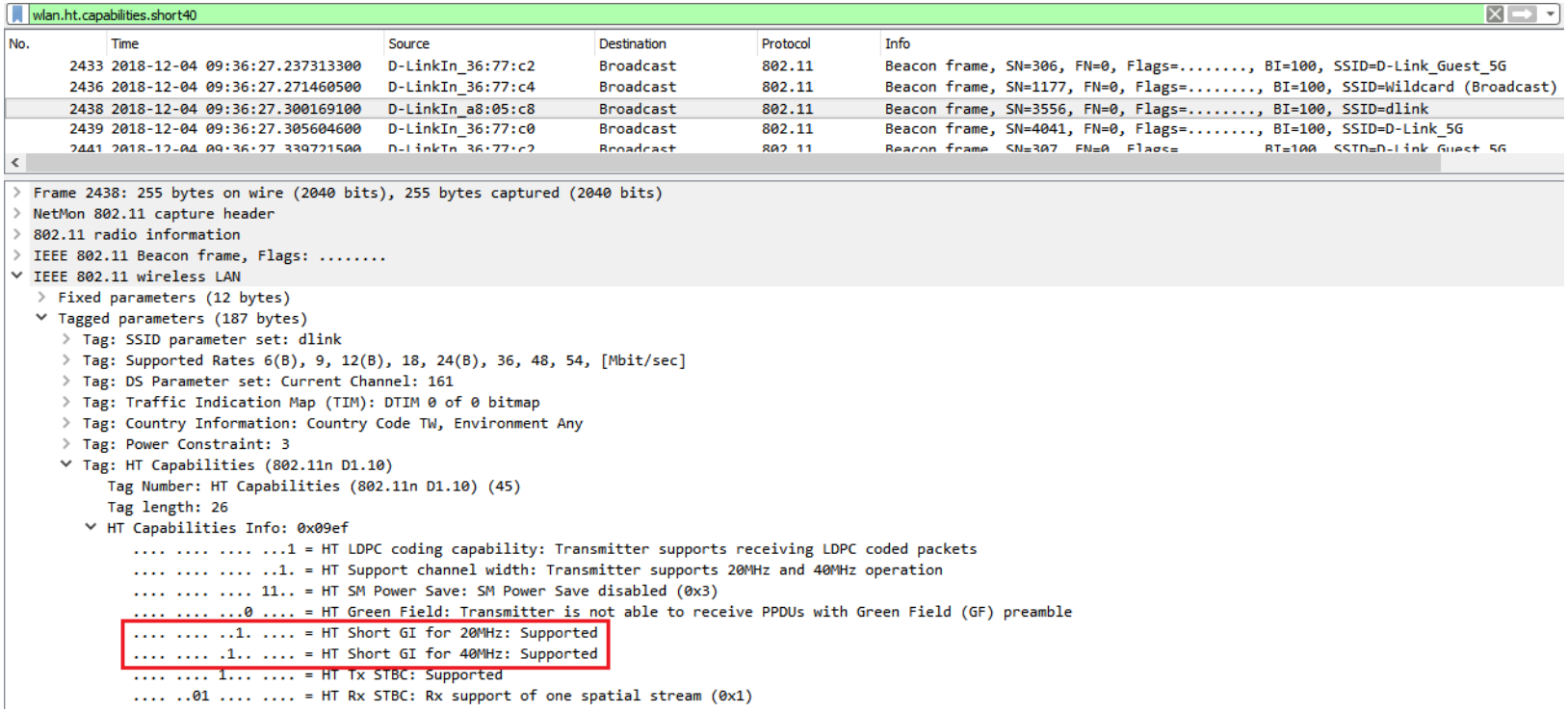
High Throughput Short Guard Interval (GI)

- Guard Interval is intended to avoid signal loss from multipath effect
- It is possible that RF signals arrives the receiving antenna by two or more paths. Should the latter message reaches the antenna too fast, signal may interfere with the earlier symbol. That is what is called "signal degradation"
- Short GI is utilized to improve the throughput, enable short GI can improve the data rate throughput about 10% (exp.)*
  - 802.11 a/b/g requires guard interval (GI) to be 800 ns (nanosecond)
  - 802.11n and the next 802.11ac, Short Guard Interval (400 ns)
  - Enable short GI: having only 802.11n or 802.11ac
  - Disable short GI: mixed mode in our environment
- Data rate (wlan_radio.data_rate), to view what data rate the frame was sent at by the transmitter.

High Throughput Capabilities, HT Short GI (2/3)

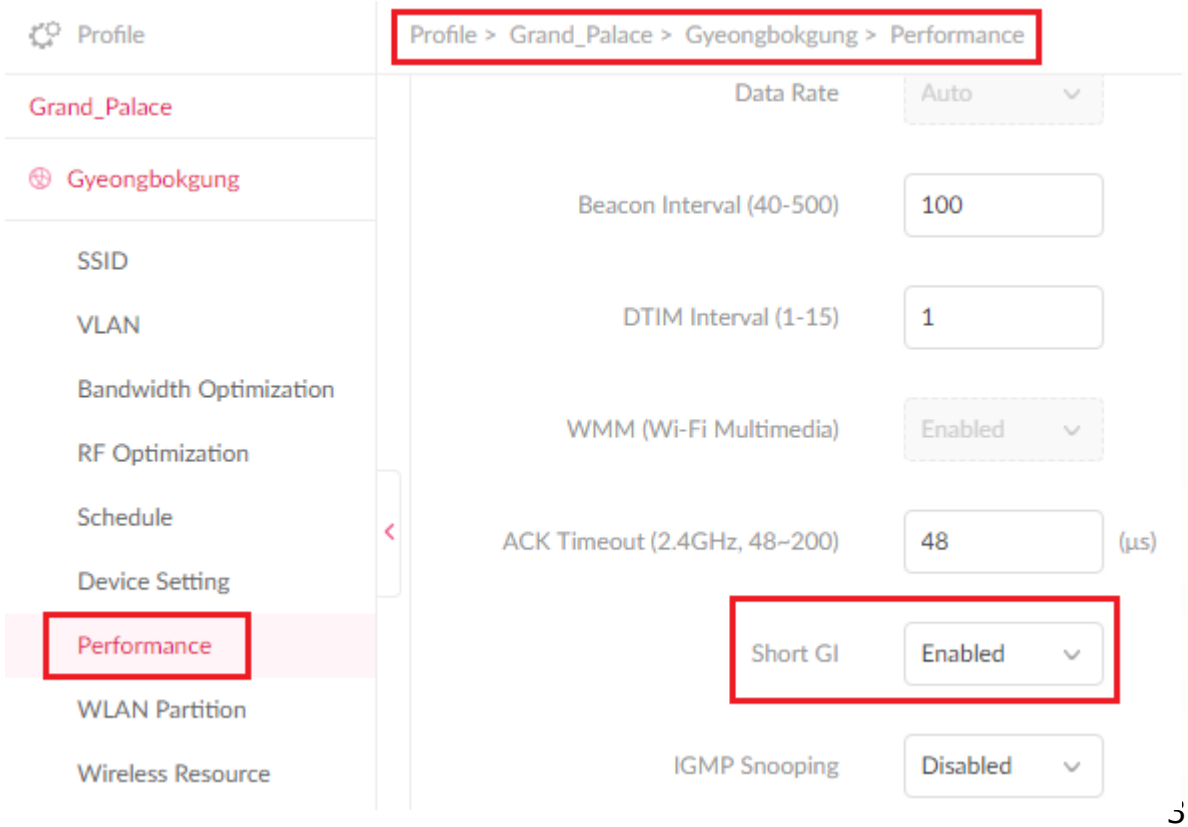
Wireshark Display Filter Reference: IEEE 802.11 wireless LAN

- wlan.ht.capabilities.short20, HT Short GI for 20MHz
- wlan.ht.capabilities.short40, HT Short GI for 40MHz



High Throughput Capabilities, HT Short GI (3/3)

- In Nuclias Connect, the Short GI setting is located in the (Profile, performance) under Configuration tab
  - Setting by default: disabled



IEEE 802.11 Authentication

- IEEE 802.11 Wireless LAN, Management Frame, Authentication
- From Wireless AP (DAP) to Wireless station (Dell laptop)

No.	Time	Source	Destination	Protocol	Info
1044	2018-10-08 18:39:44.709534400	D-LinkIn_0c:67:50	IntelCor_a9:52:ec	802.11	Probe Response, SN=2317, FN=0, Flags=....R..., BI=100, SSID=dlinkacademy
1063	2018-10-08 18:39:44.791249100	D-LinkIn_0c:67:50	IntelCor_a9:52:ec	802.11	Authentication, SN=256, FN=0, Flags=.....
1064	2018-10-08 18:39:44.793664700	D-LinkIn_0c:67:50	IntelCor_a9:52:ec	802.11	Association Response, SN=257, FN=0, Flags=.....

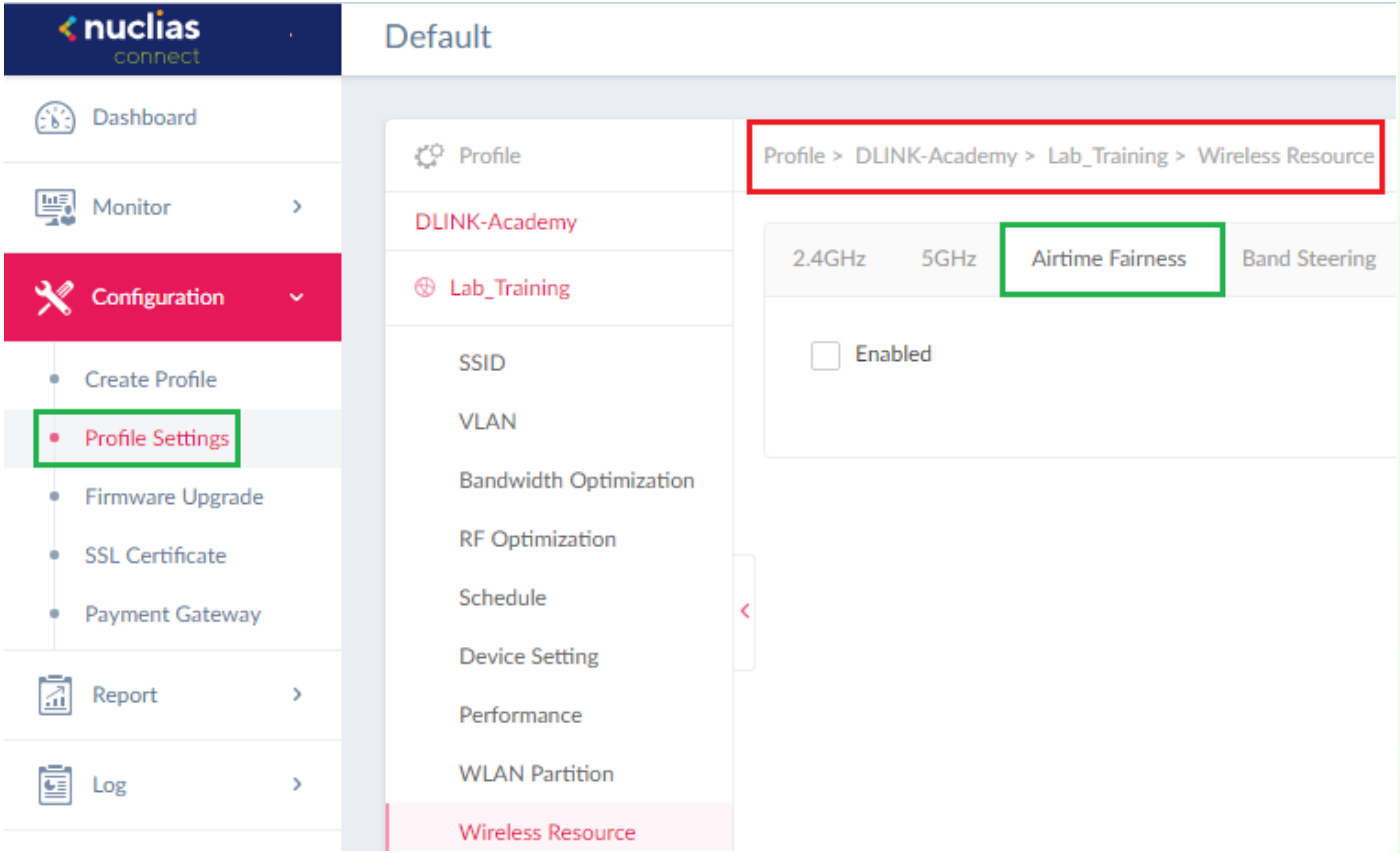
```
> Frame 1063: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> NetMon 802.11 capture header
> 802.11 radio information
v IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x000b)
  v Frame Control Field: 0xb000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1011 .... = Subtype: 11
    > Flags: 0x00
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_a9:52:ec (00:1c:bf:a9:52:ec)
    Destination address: IntelCor_a9:52:ec (00:1c:bf:a9:52:ec)
    Transmitter address: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    Source address: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    BSS Id: D-LinkIn_0c:67:50 (40:9b:cd:0c:67:50)
    .... .... .... 0000 = Fragment number: 0
    0001 0000 0000 .... = Sequence number: 256
v IEEE 802.11 wireless LAN
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
```

Airtime Fairness

- Popularity of wireless LANs has grown rapidly, bringing a situation where identical 802.11 standard devices being utilized in the same place and at the same time. (D-Track DK1500414)
  - Conference room is a clear example on that
- By the laws of Physics, slower device (i.e. 802.11g) requires longer time-frame to receive and transmit data, comparing to newer device (i.e. 802.11n or 802.11ac).
  - That leads to a situation which slowness of higher data rated clients in the presence of slow clients
- Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate.
- The character of this feature is to ensure higher download speed to latest devices when slower devices are connected to the same AP.

Airtime Fairness Configuration in Profile Settings (1/3)

- Airtime Fairness setting is located on the Wireless Resources session of Profile Settings page under the Configure tab.



Airtime Fairness Configuration in Profile Settings (2/3)

- Before Airtime Fairness setting being activated

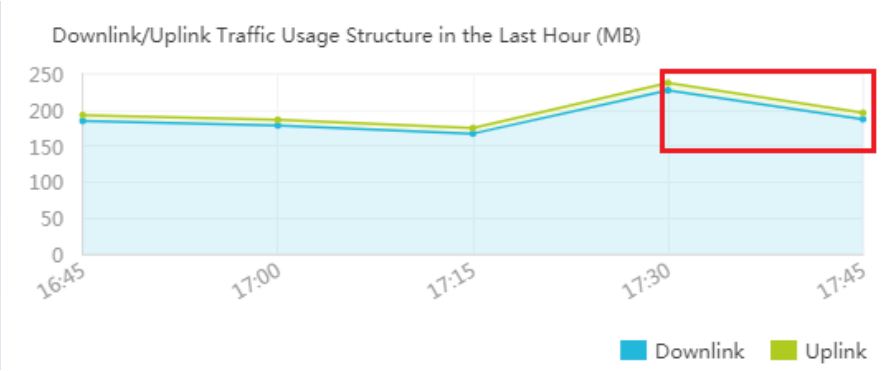
No.	Action	IP Address	MAC Address	Auth Type	Band	SSID	Traffic Usage	Traffic Usage(..)	Last Seen
2		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	5GHz	F-22-Raptor	10.62 MB	3.89%	2018-10-24 17:23:57
3		172.17.5.103	a4:db:30:cb:36:0e	Disabled	2.4GHz	F-22-Raptor	123.01 MB	45.08%	2018-10-24 17:23:57
1		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	5GHz	F-22-Raptor	139.21 MB	51.02%	2018-10-24 17:23:57

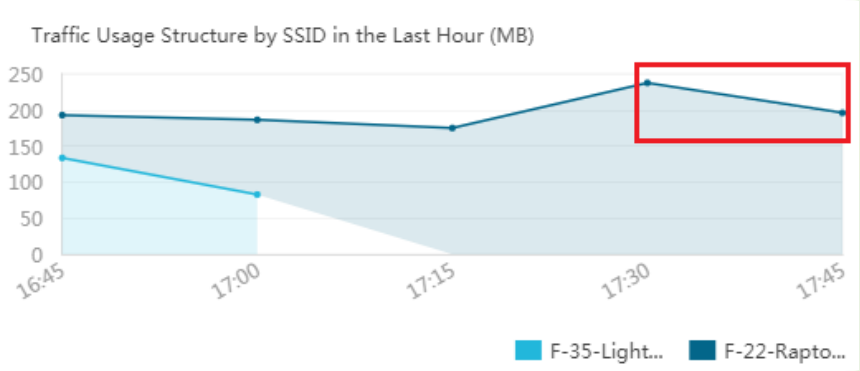
- After the settings

No.	Action	IP Address	MAC Address	Auth Type	Band	SSID	Traffic Usage	Traffic Usage(..)	Last Seen
2		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	5GHz	F-22-Raptor	1.86 MB	1.34%	2018-10-24 17:33:04
1		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	5GHz	F-22-Raptor	39.44 MB	28.43%	2018-10-24 17:32:17
3		172.17.5.103	a4:db:30:cb:36:0e	Disabled	2.4GHz	F-22-Raptor	97.44 MB	70.23%	2018-10-24 17:33:04

Airtime Fairness Configuration in Profile Settings (3/3)

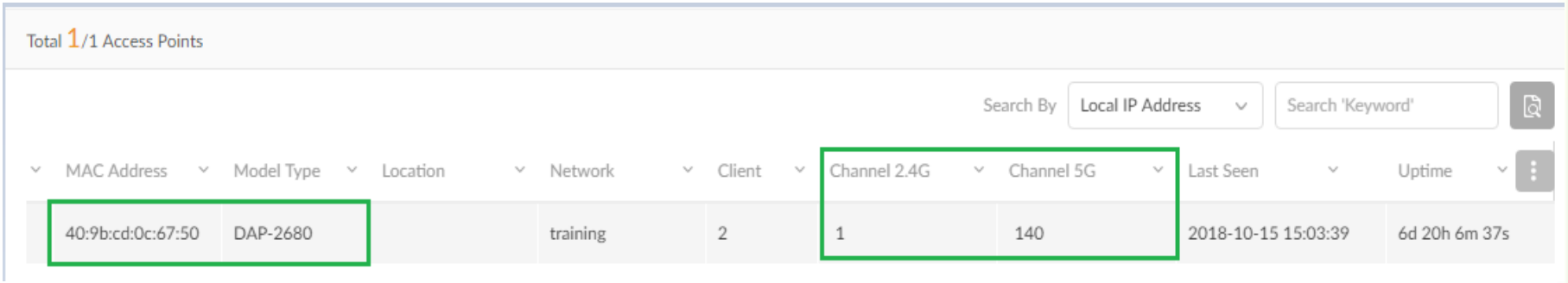
- Traffic usage decrease, after Airtime Fairness being activated.





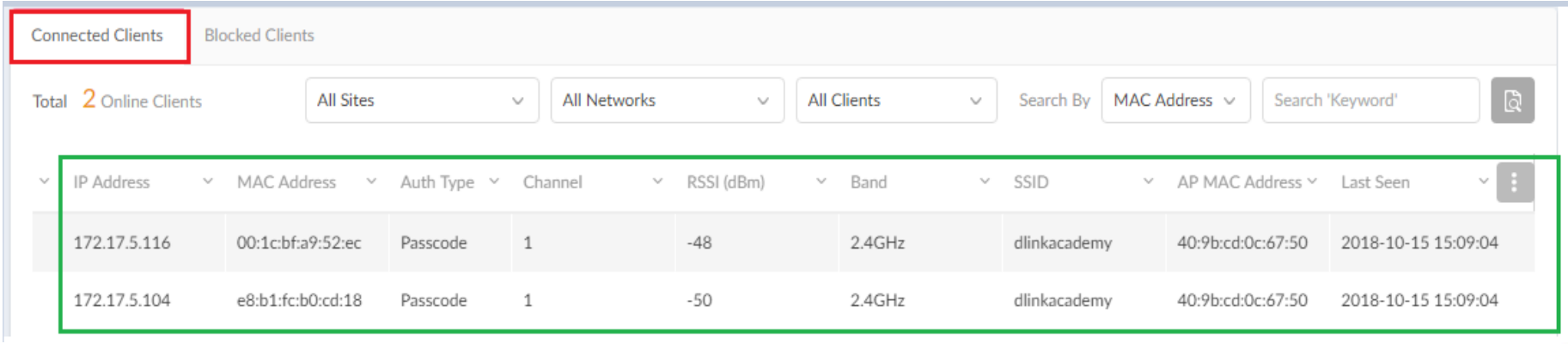
WLAN Channels in Use

- WLAN Channels in use can be viewed from Monitor > Access Point
  - Channel 2.4GHz (1) & Channel 5GHz (140)



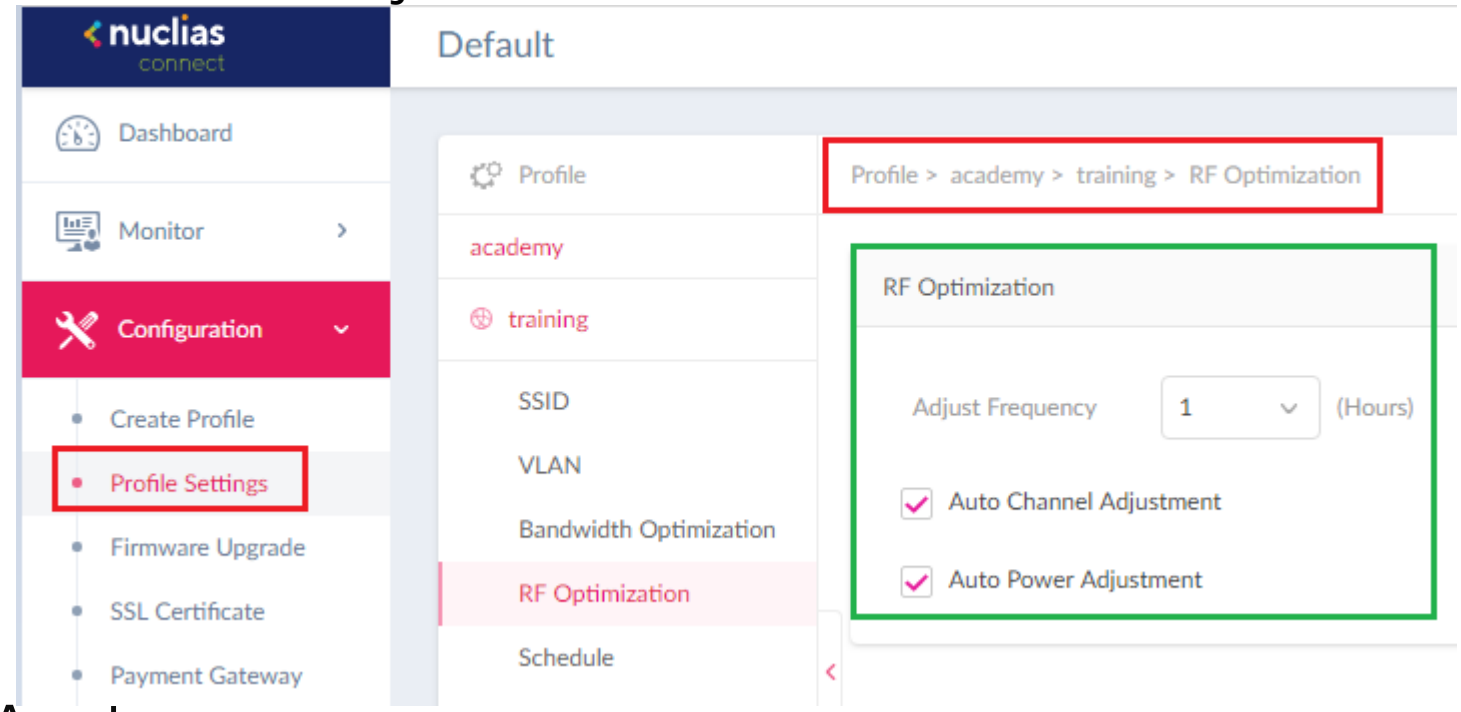
WLAN Channels in Use

- WLAN Channels in use can be viewed from Monitor > Wireless Client
  - 172.17.5.116 (00:1c:bf:a9:52:ec)
  - 172.17.5.104 (e8:b1:fc:b0:cd:18)



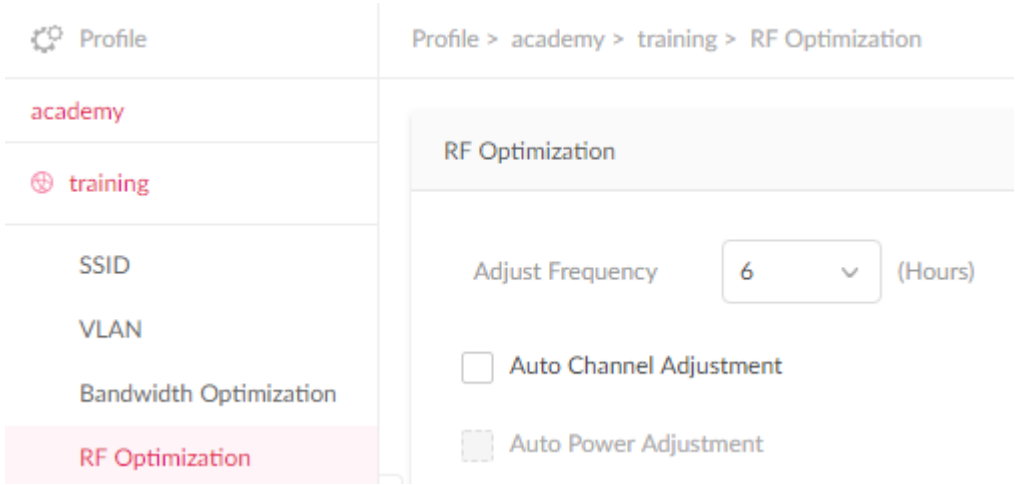
RF Optimization

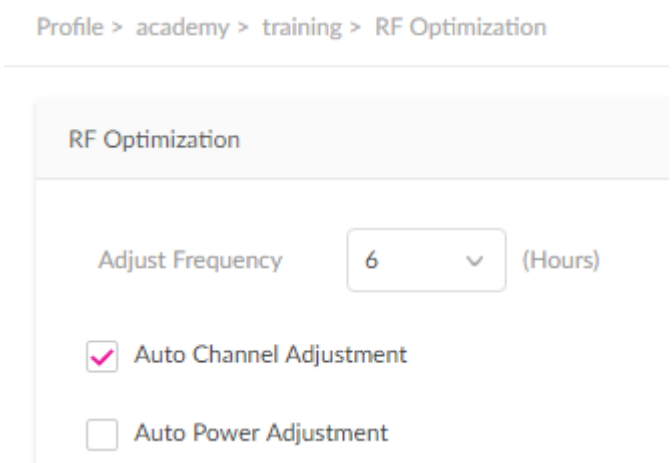
- RF Optimization settings under Configuration tab
  - Adjust Frequency: 1 ~ 12 hours, within a one-hour time slot
  - Auto Channel Adjustment
  - Auto Power Adjustment



Profile Settings, Auto Channel Adjustment and Auto Power Adjustment

- In the RF Optimization page under the configuration tab, we are able to see two options: Auto Channel Adjustment and Auto Power.
- Power Adjustment is only available until the activation of "Channel Adjustment."

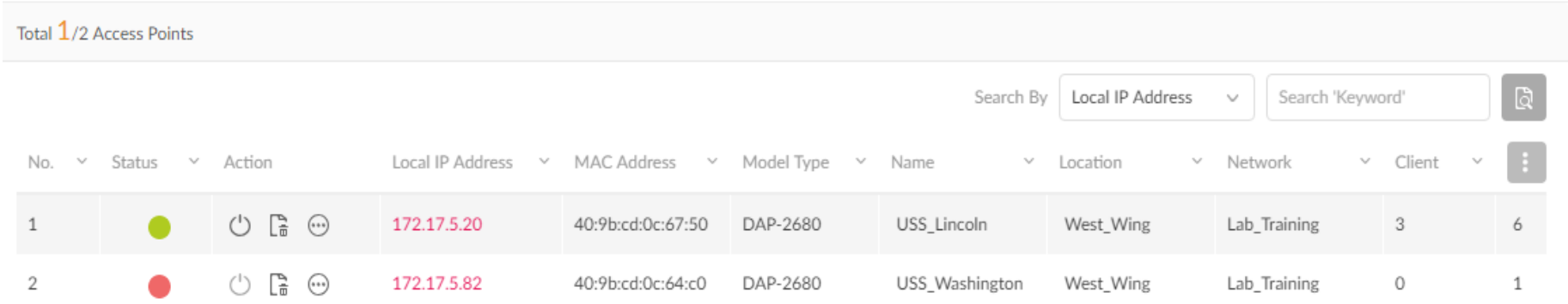




Automatic power adjustment shall minimize the occurrence of RF interference.

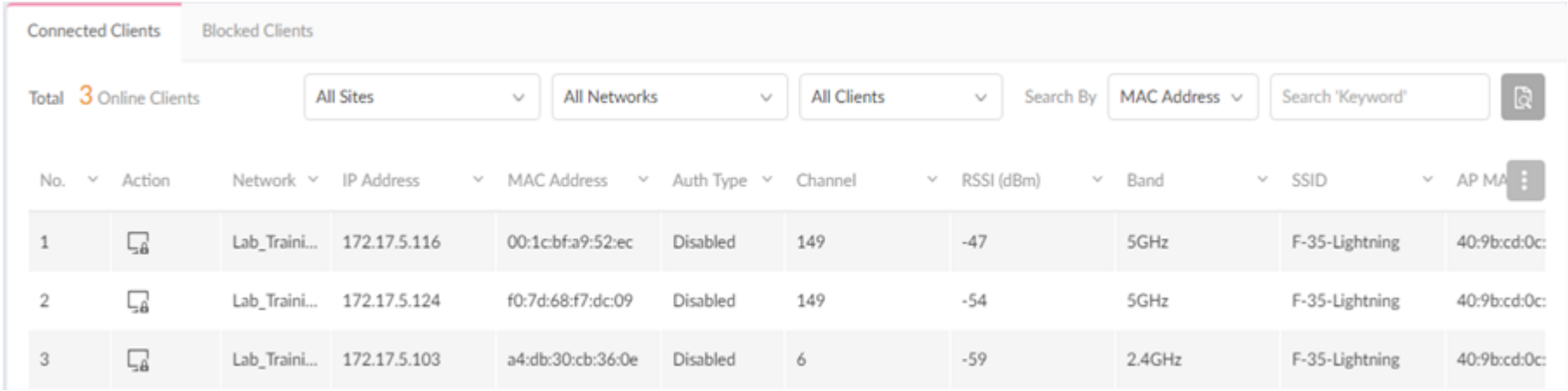
Auto Channel Adjustment, One AP (1/3)

- Auto Channel Adjustment Hands-On Lab
- Assuming we only have 1 DAP-2680 (IP: 172.17.5.20), and all three laptops are connecting to “F-35-Lightning” SSID, where Auto Channel Adjustment is going to be activated.



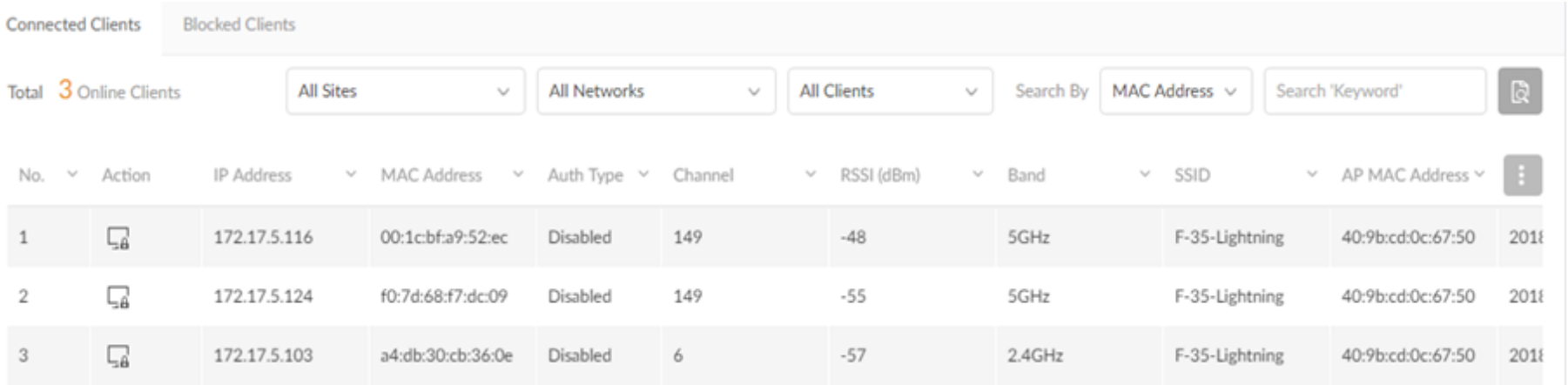
Auto Channel Adjustment, One AP (2/3)

- Auto Channel Adjustment algorithm
- One AP in our lab and activate “Auto Channel Adjustment”. No change in channel would be made.
  - Time of data collection: 11:30AM



Auto Channel Adjustment, One AP (3/3)

- Auto Channel Adjustment algorithm
- One AP in our lab and activate “Auto Channel Adjustment”. No change in channel would be made.
  - Time of data collection: 14:30PM (same wireless channel)



Automatic Channel Selection Process

- D-Track DK1500239 states that CWM is developed to deploy the most general configurations to each Access Point.
- As such, it (DNC) allows DAP automatically making the channel selection and power maximization.
- In last two slides, we are able to see that in a “One AP” environment, there is no channel changes
- But, if we have two APs, what would be a possible result?

Auto Channel Adjustment Hands-On Lab (1/7)

- Auto Channel Adjustment Hands-On Lab
- Assuming we only have two DAP-2680, and all three laptops are connecting to “F-22-Raptor” SSID, as shown below.

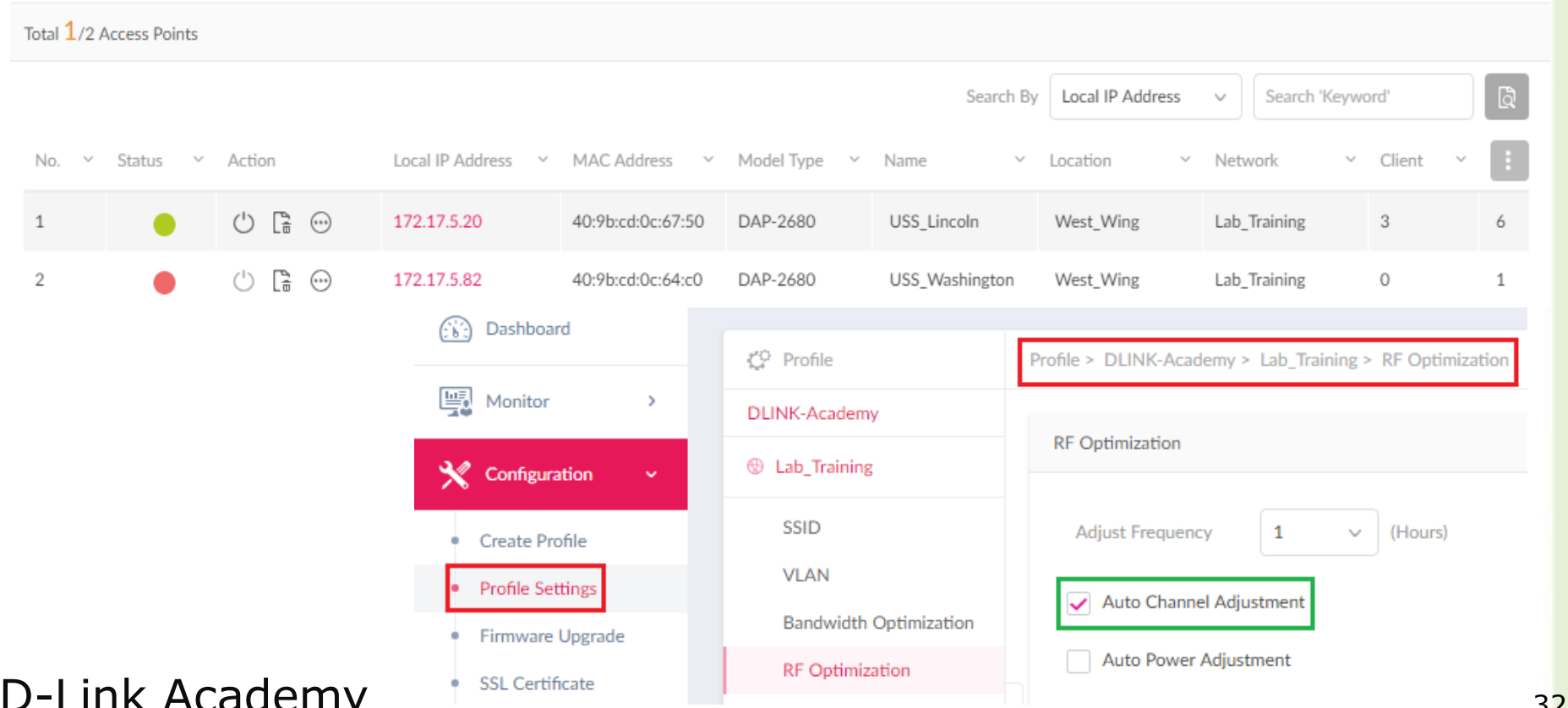
Connected Clients | Blocked Clients

Total 3 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

No.	Action	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address
1		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	6	-60	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50
2		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	149	-53	5GHz	F-22-Raptor	40:9b:cd:0c:67:50
3		172.17.5.103	a4:db:30:cb:36:0e	Disabled	6	-57	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50

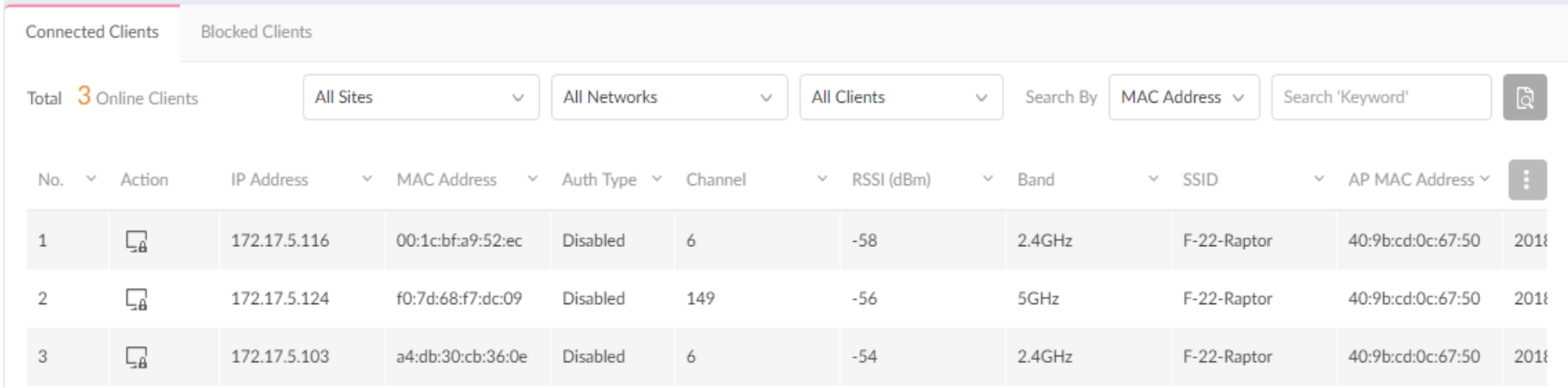
Auto Channel Adjustment Hands-On Lab (2/7)

- Auto Channel Adjustment Hands-On Lab
- We are going to activate “Auto Channel Adjustment” function



Auto Channel Adjustment Hands-On Lab (3/7)

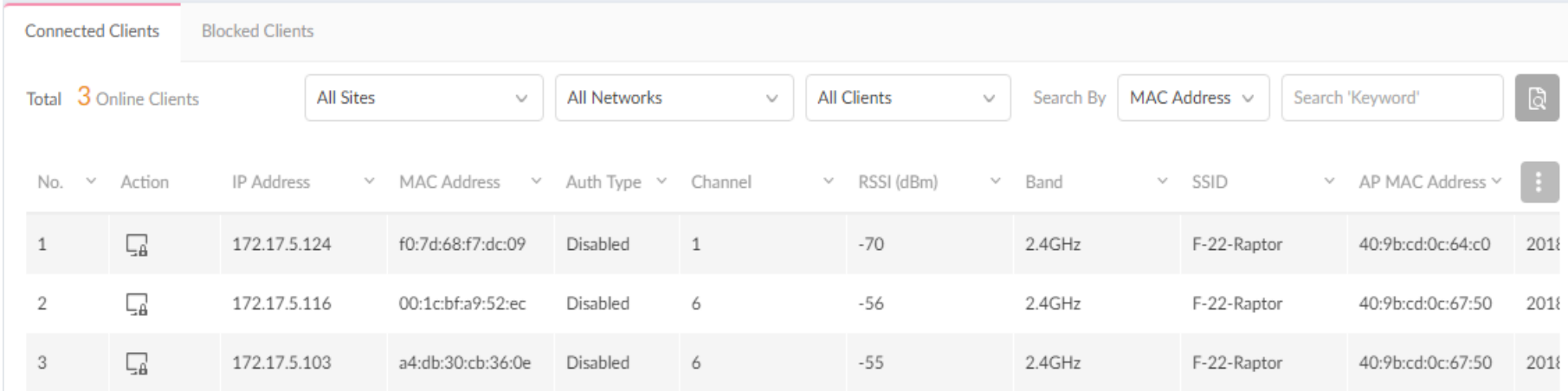
- Auto Channel Adjustment Hands-On Lab
- The following collected diagrams would show the changes of channel. (Data collected, 12:25PM)
  - Two in channel 6 and one in channel 149



No.	Action	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address
1		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	6	-58	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50
2		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	149	-56	5GHz	F-22-Raptor	40:9b:cd:0c:67:50
3		172.17.5.103	a4:db:30:cb:36:0e	Disabled	6	-54	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50

Auto Channel Adjustment Hands-On Lab (4/7)

- Auto Channel Adjustment Hands-On Lab
- The following collected diagrams would show the changes of channel. (Data collected, 1:25PM) [one hour later]
  - Two in channel 6 and one in channel 1



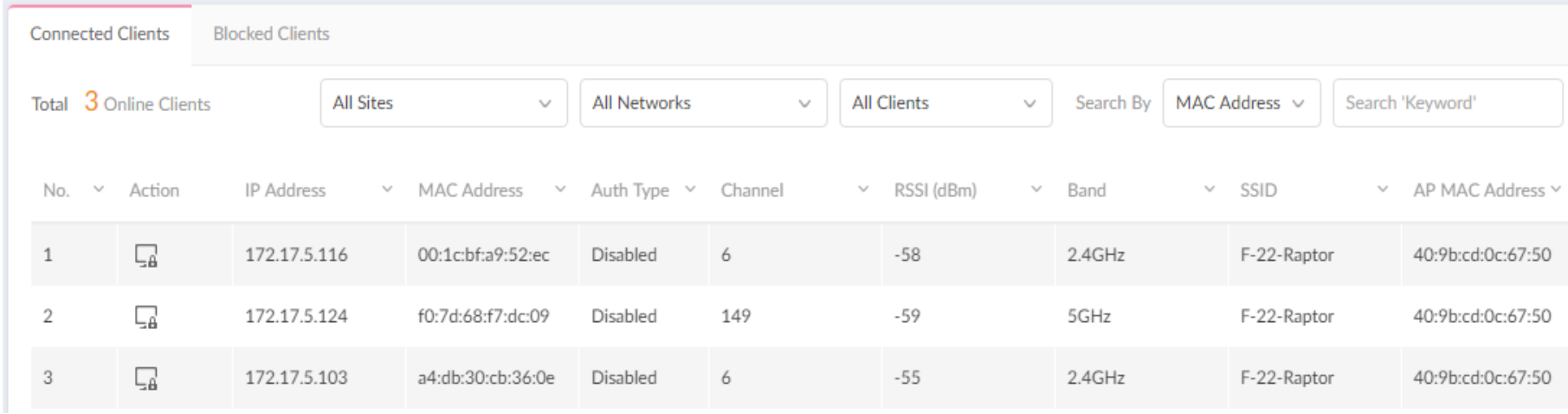
Connected Clients | Blocked Clients

Total 3 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

No.	Action	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address
1		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	1	-70	2.4GHz	F-22-Raptor	40:9b:cd:0c:64:c0
2		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	6	-56	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50
3		172.17.5.103	a4:db:30:cb:36:0e	Disabled	6	-55	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50

Auto Channel Adjustment Hands-On Lab (5/7)

- Auto Channel Adjustment Hands-On Lab
- The following collected diagrams would show the changes of channel. (Data collected, 14:30PM) [one hour later]
  - Two in channel 6 and one in channel 149



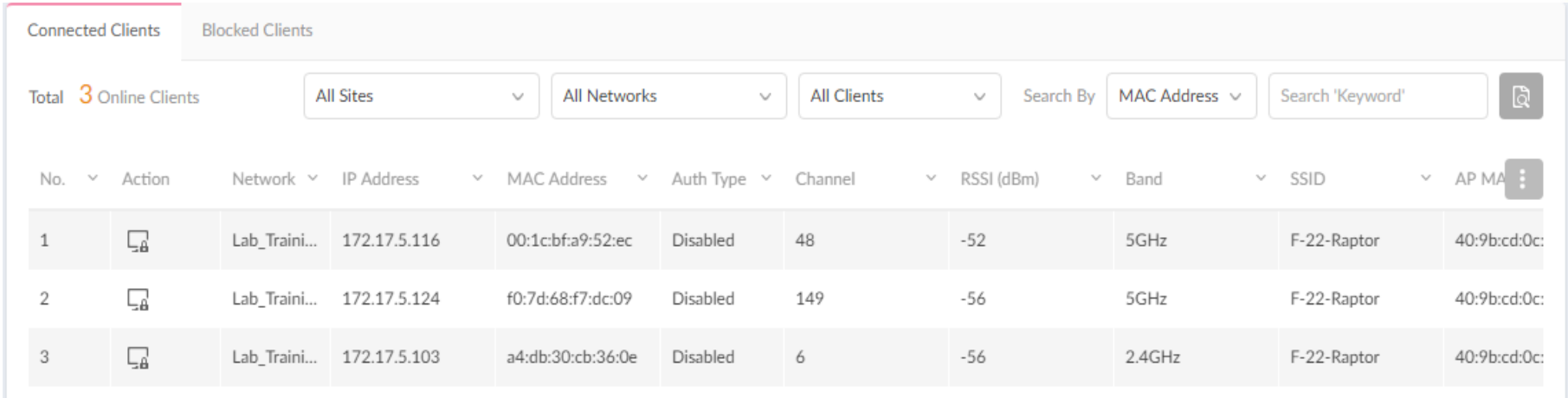
Connected Clients | Blocked Clients

Total 3 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

No.	Action	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address
1		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	6	-58	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50
2		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	149	-59	5GHz	F-22-Raptor	40:9b:cd:0c:67:50
3		172.17.5.103	a4:db:30:cb:36:0e	Disabled	6	-55	2.4GHz	F-22-Raptor	40:9b:cd:0c:67:50

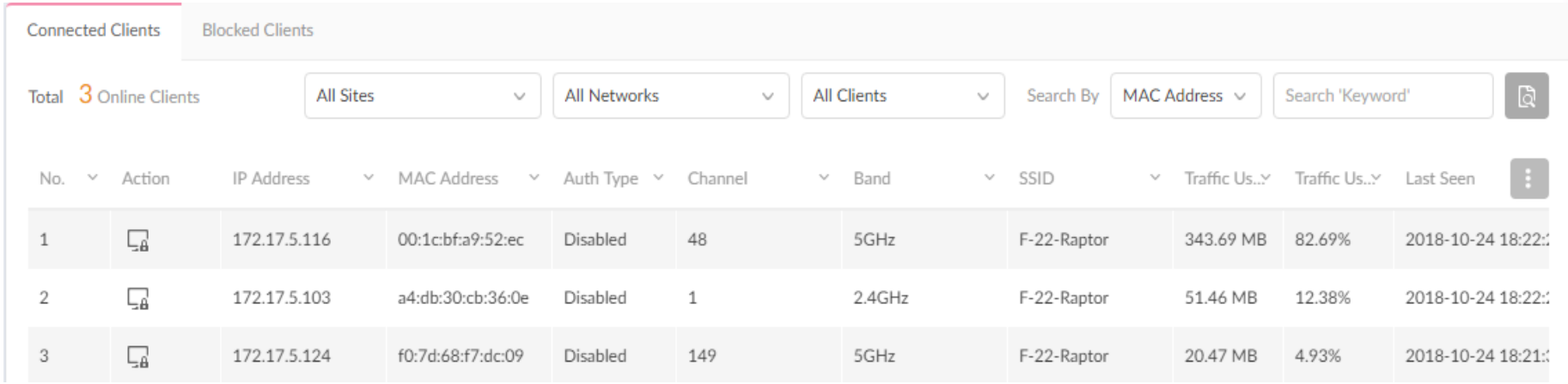
Auto Channel Adjustment Hands-On Lab (6/7)

- Auto Channel Adjustment Hands-On Lab
- The following collected diagrams would show the changes of channel. (Data collected, 17:30PM) [three hours later]
  - One in channel 6, one, channel 48, and last one 149



Auto Channel Adjustment Hands-On Lab (7/7)

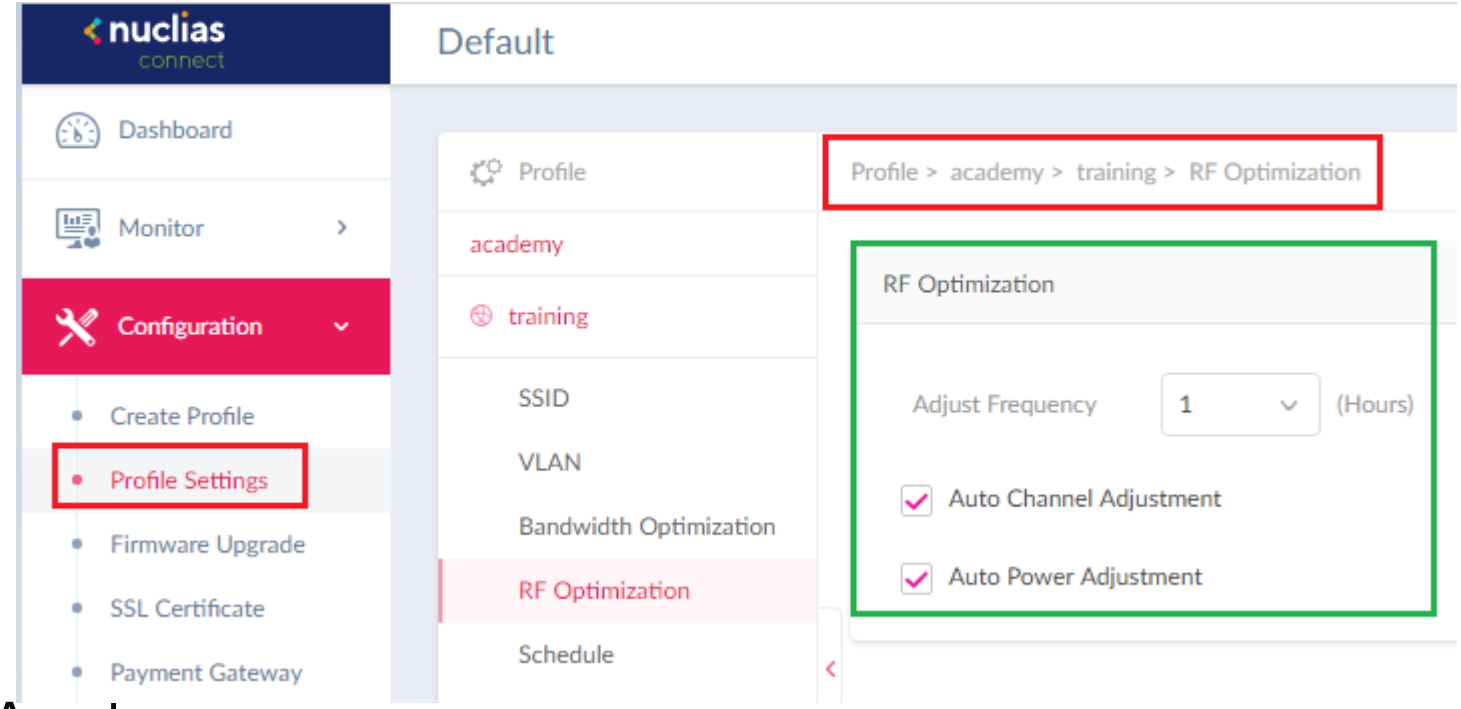
- Auto Channel Adjustment Hands-On Lab
- The following collected diagrams would show the changes of channel. (Data collected, 18:23PM) [one hour later]
  - One in channel 1, one, channel 48, and last one 149



RF Optimization

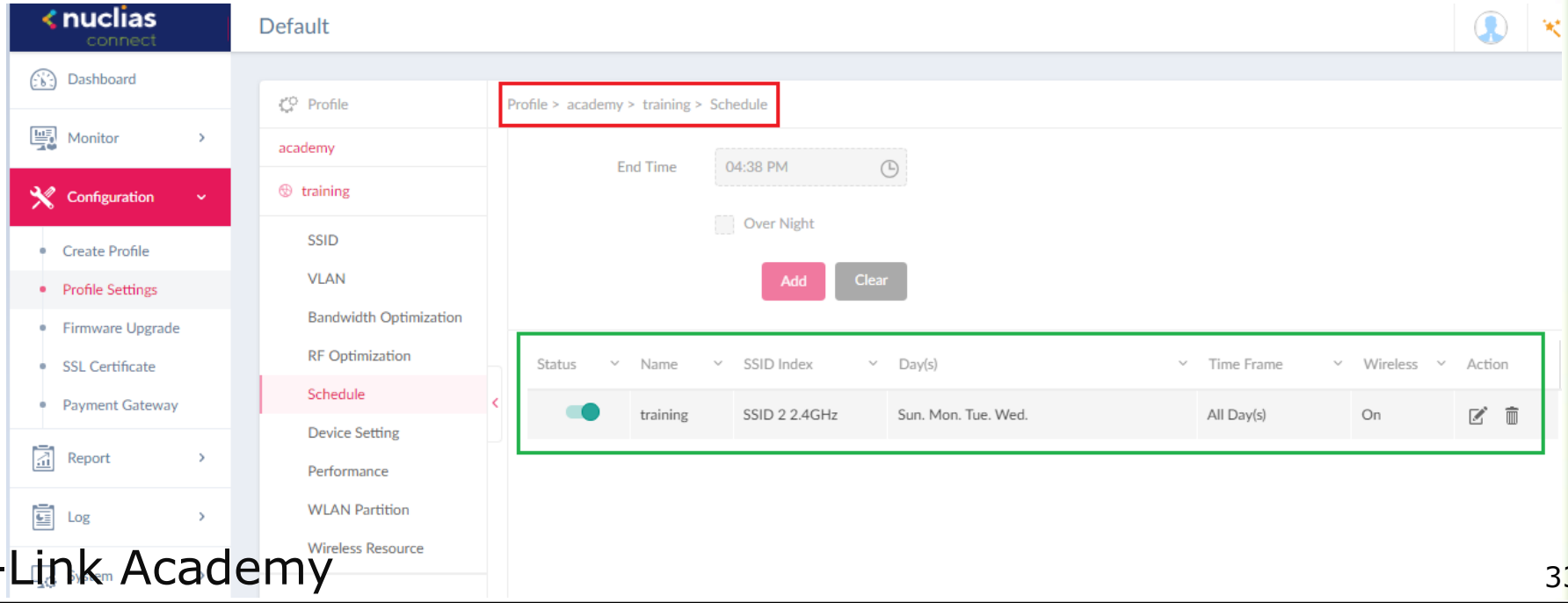
- RF Optimization settings under Configuration tab

In Nuclias Connect official release, this page might carry different outlook with more functions.



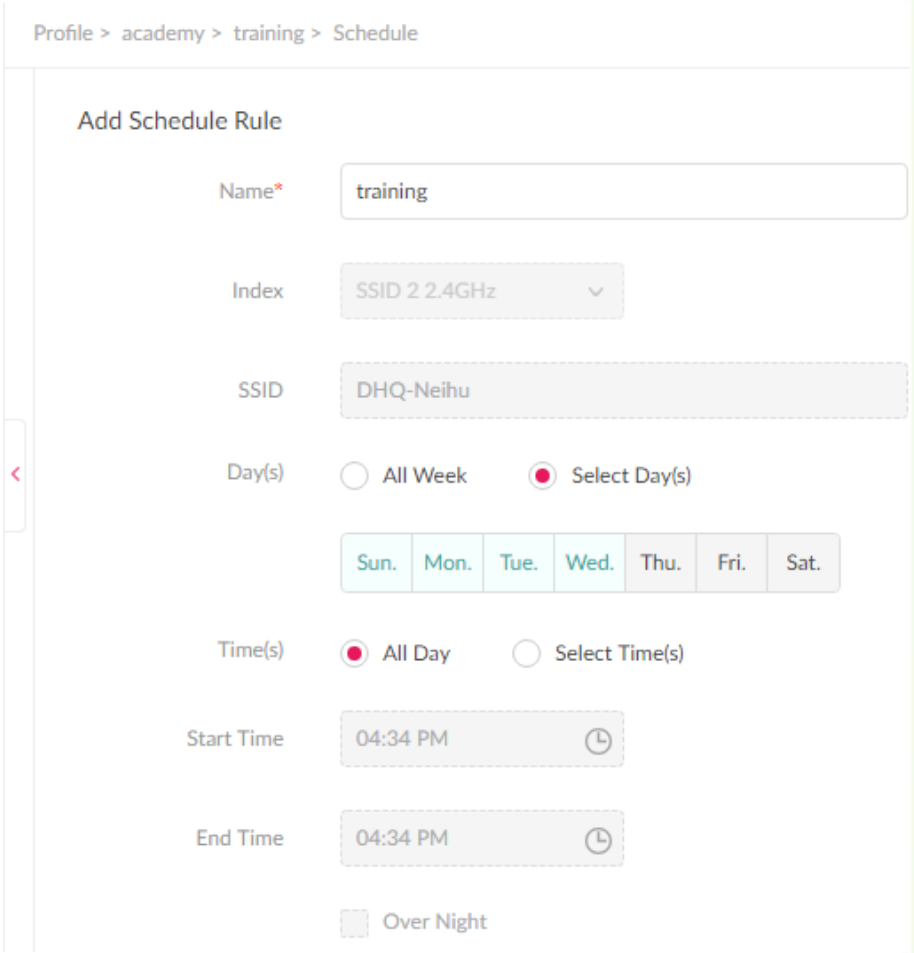
Wireless Schedule Configuration (1/3)

- Wireless Schedule configuration
- Menu: Configuration > Profile configuration > Profile > academy > training > Schedule
  - The below diagram is an example that SSID of DHQ-Neihu is only available from Sunday to Wednesday



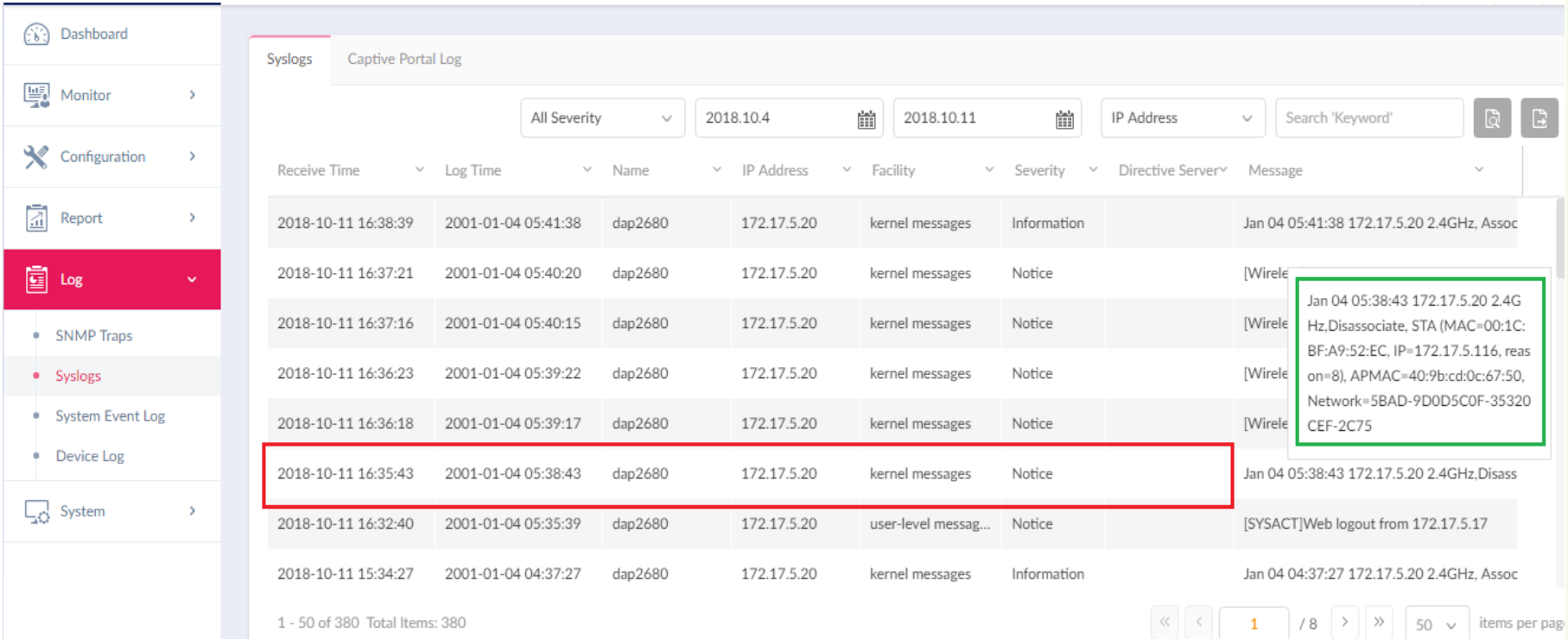
Wireless Schedule Configuration (2/3)

- Wireless Schedule configuration
- Menu: Configuration > Profile configuration > Profile > academy > training > Schedule
  - The below diagram is an example that SSID of DHQ-Neihu is only available from Sunday to Wednesday



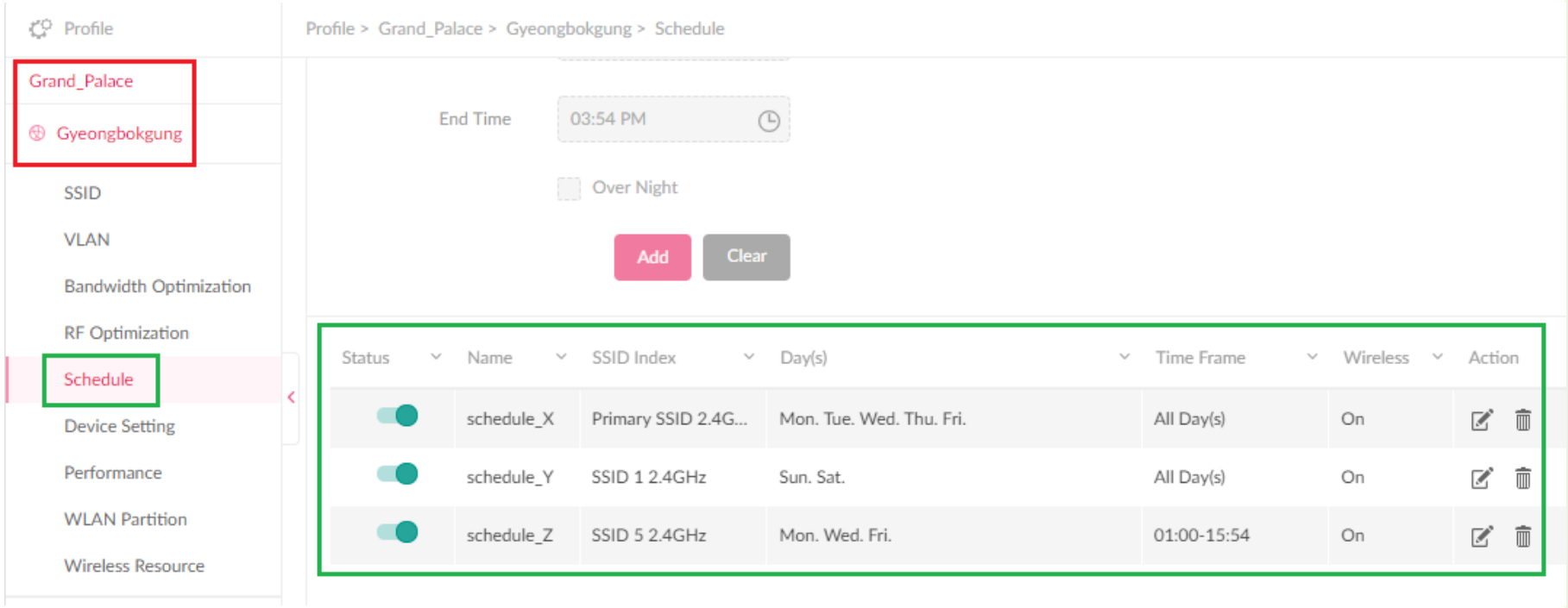
Wireless Schedule Configuration (3/3)

- Wireless Schedule configuration
- Connected wireless stations got disassociated



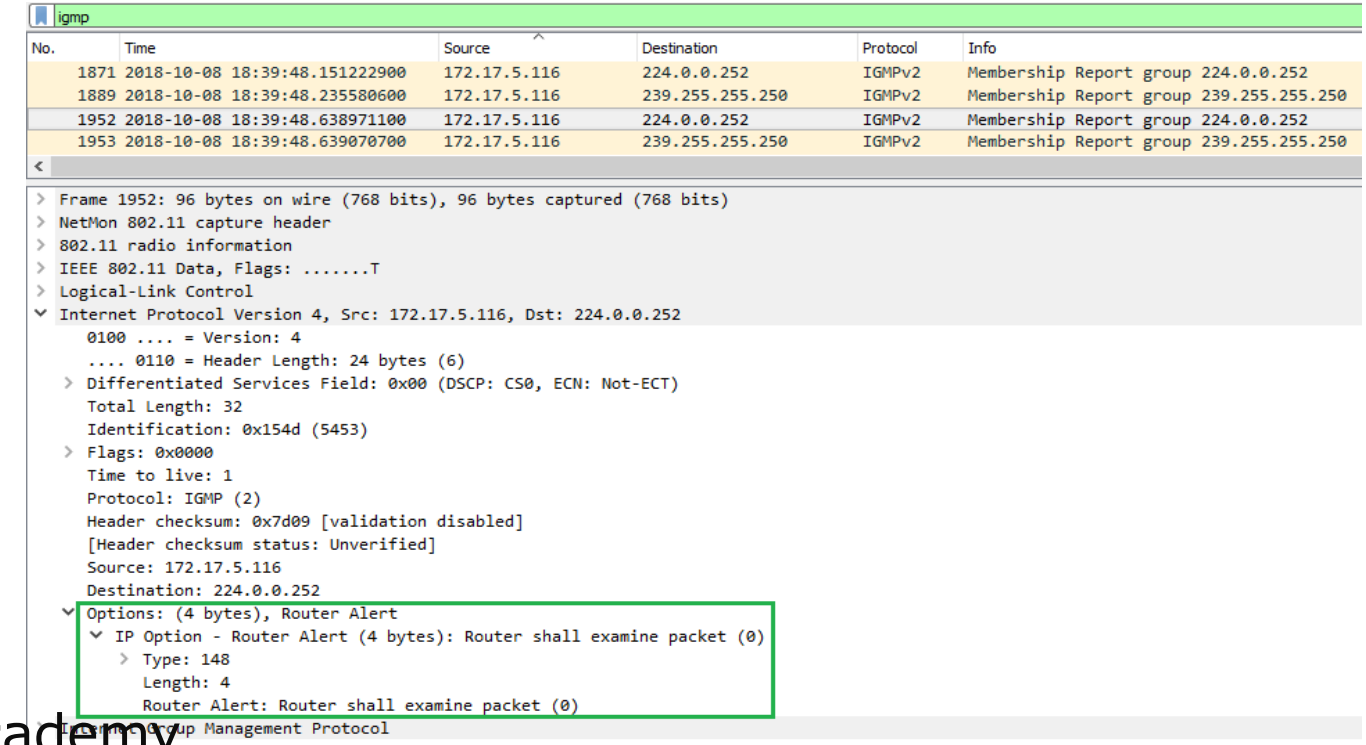
Selection By Different Schedules

- In DNC official release, a profile is able to be linked to multiple schedules.



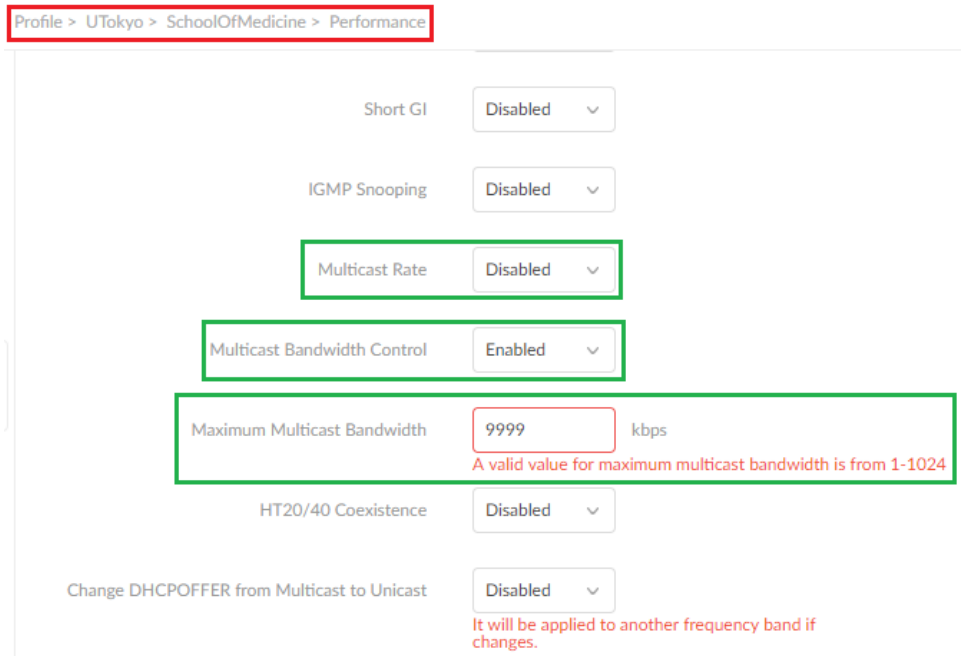
IGMP Snooping

- In Nuclias Connect, Administrators are able to disable or enable IGMP Snooping settings.
  - An example Nuclias Connect is in Disabled mode. (packets collected from a wireless client]



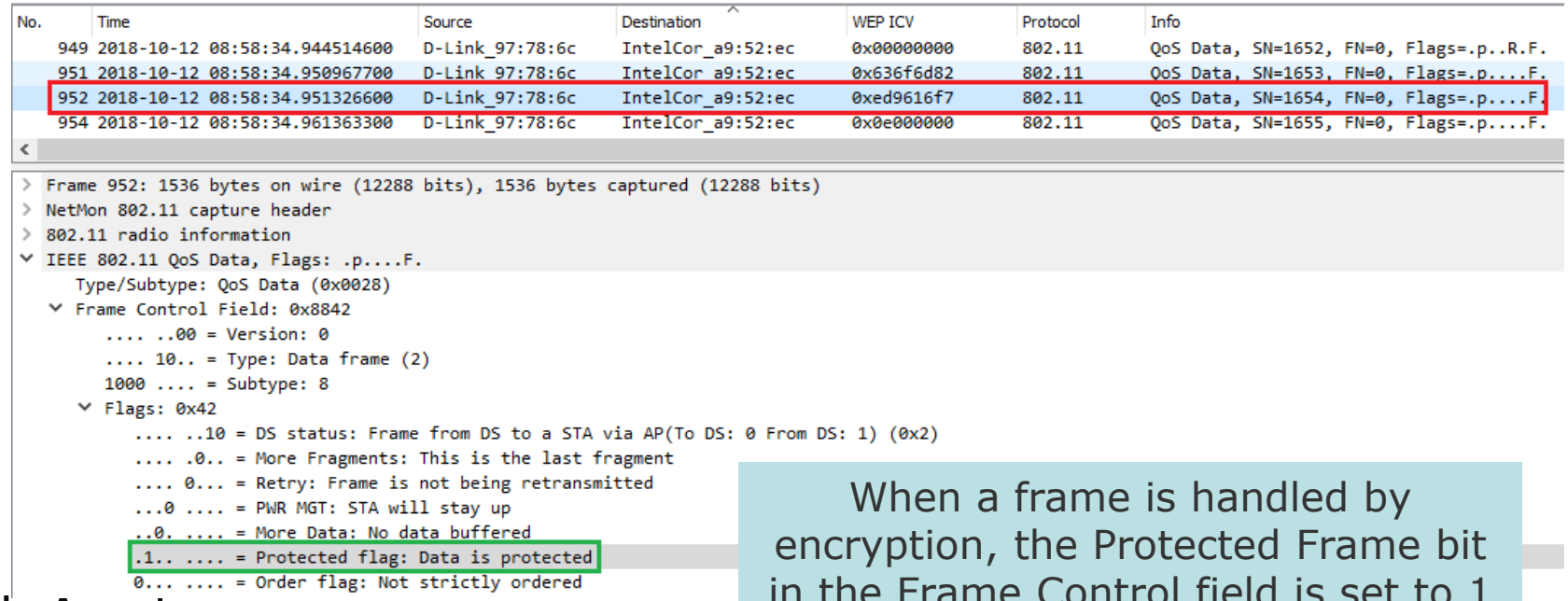
Multicast Bandwidth Management

- In Nuclias Connect, there are a few ways to manage multicast bandwidth. For example, (menu: Profile > Performance)
  - Multicast Rate
  - Multicast Bandwidth Control
  - Maximum Multicast Bandwidth



IEEE 802.11 QoS Data (1/5)

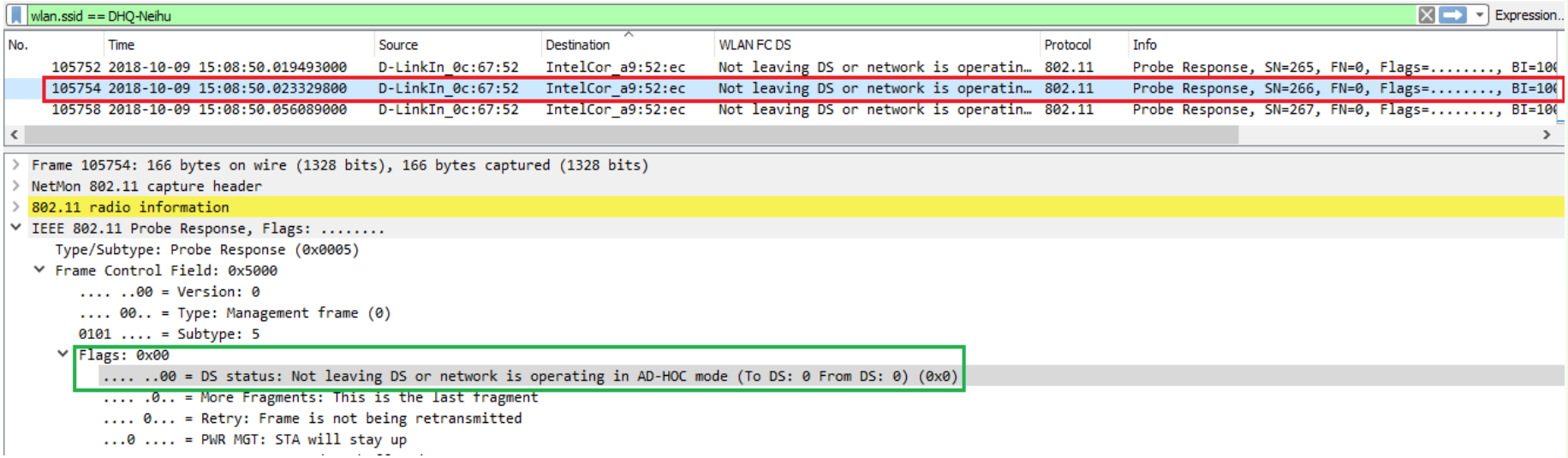
- Frame checksum (C)
  - wlan.fc.protected is a frame checksum example that
  - wlan.fc.protected==0 MAC Service Data Unit (MSDU) payload not encrypted
  - wlan.fc.protected==1 MSDU payload encrypted



When a frame is handled by encryption, the Protected Frame bit in the Frame Control field is set to 1

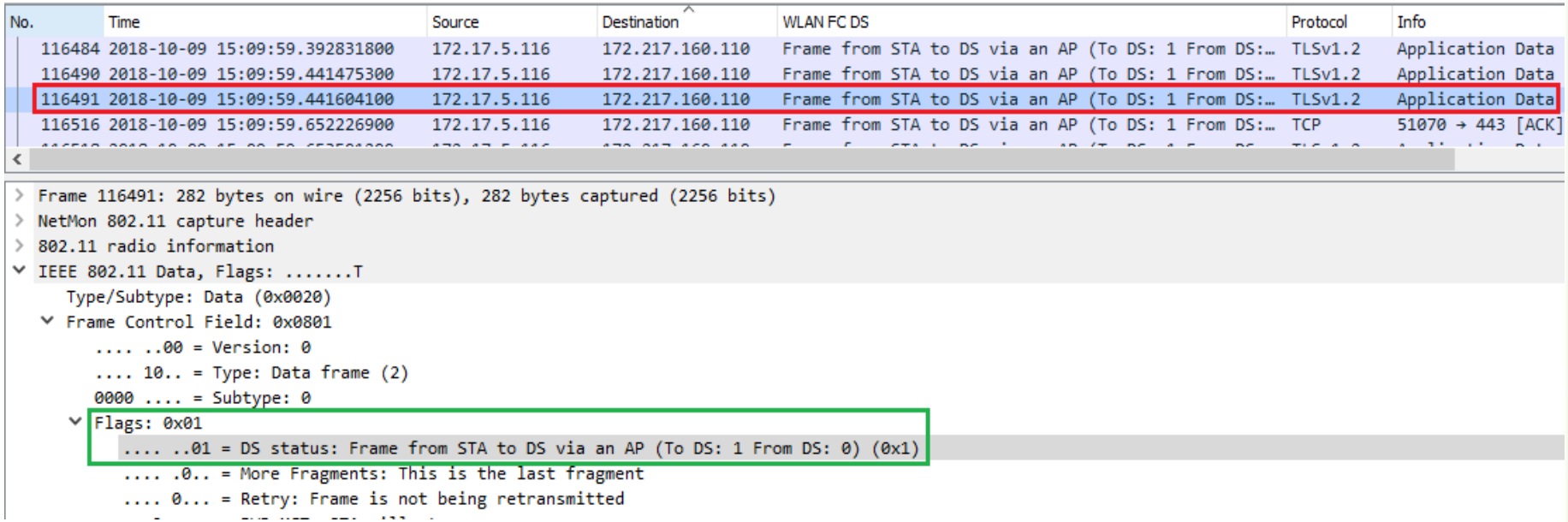
IEEE 802.11 QoS Data (2/5)

- Frame checksum (C)
  - wlan.fc.ds==0 control or management frame (mostly)
  - wlan.fc.ds==1 to DS (distribution system)
  - wlan.fc.ds==2 from DS (distribution system)
  - wlan.fc.ds==3 WDS or mesh network



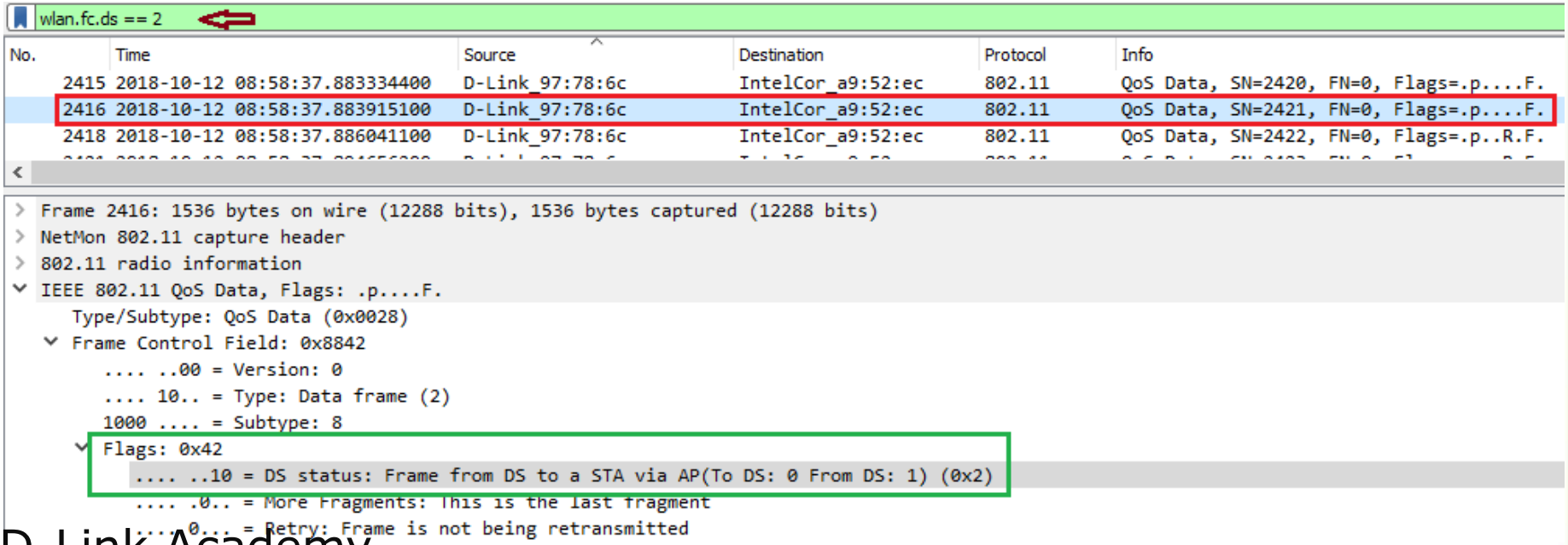
IEEE 802.11 QoS Data (3/5)

- Frame checksum (C)
  - wlan.fc.ds==0 control or management frame (mostly)
  - wlan.fc.ds==1 to DS (distribution system)
  - wlan.fc.ds==2 from DS (distribution system)
  - wlan.fc.ds==3 WDS or mesh network



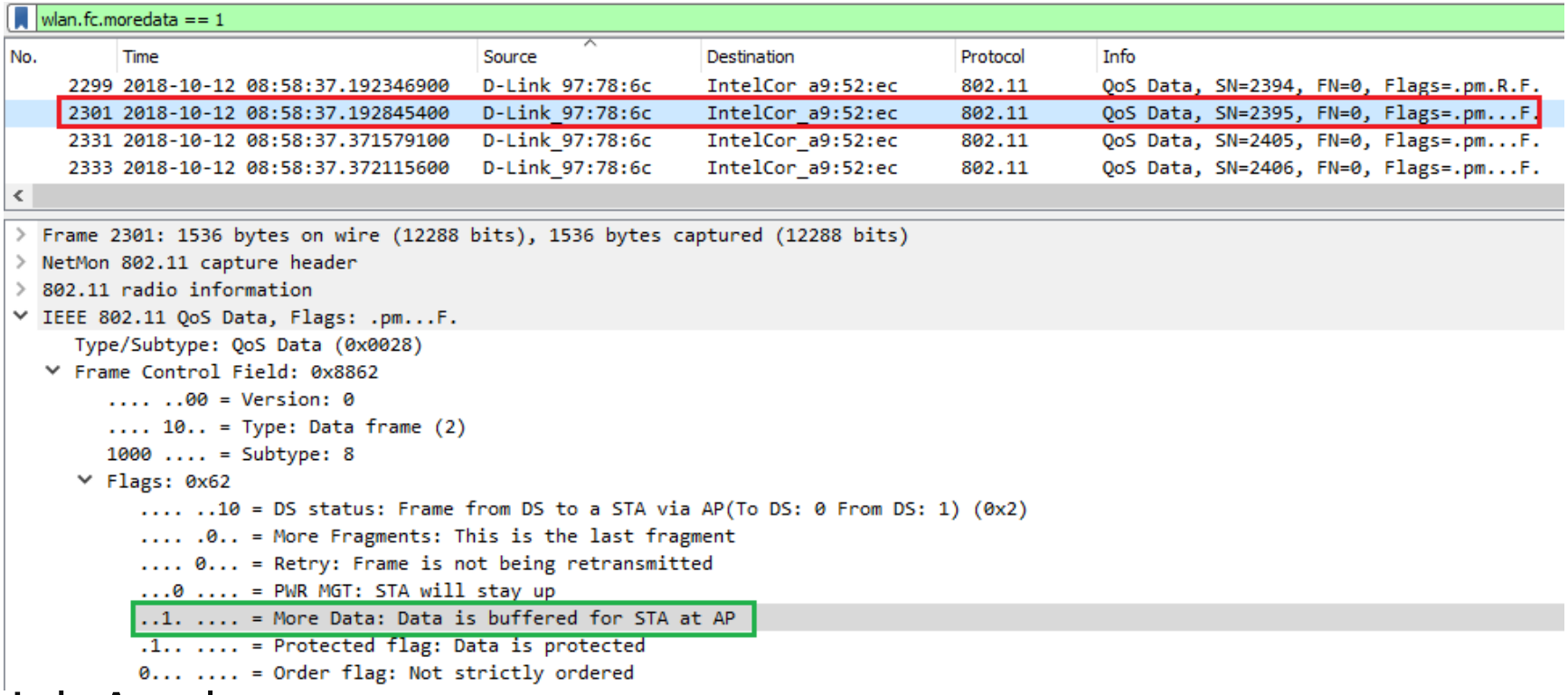
IEEE 802.11 QoS Data (4/5)

- Frame checksum (C)
  - wlan.fc.ds==0 control or management frame (mostly)
  - wlan.fc.ds==1 to DS (distribution system)
  - wlan.fc.ds==2 from DS (distribution system)
  - wlan.fc.ds==3 WDS or mesh network



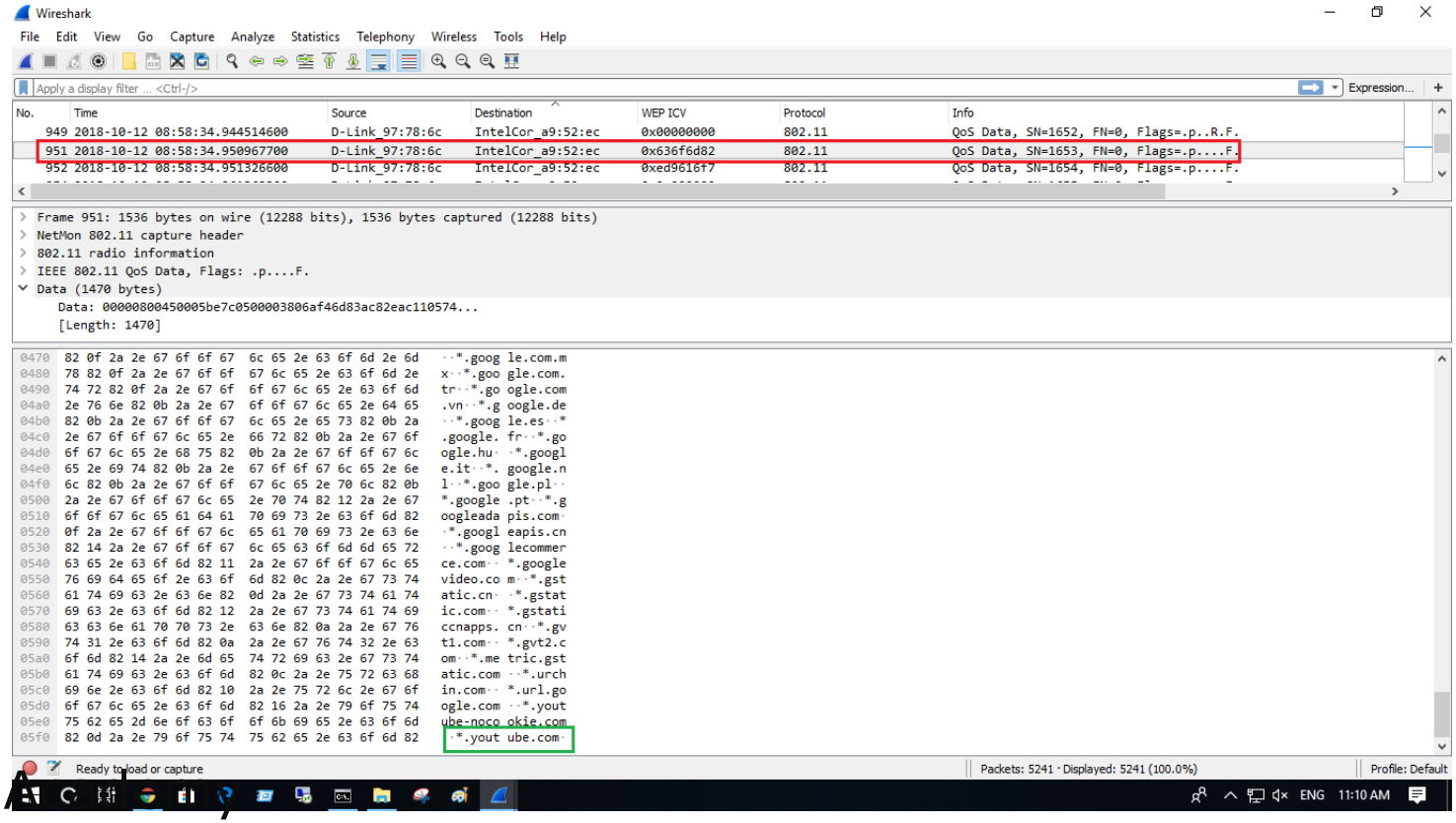
IEEE 802.11 QoS Data (5/5)

- Frame checksum (C)
  - wlan.fc.moredata==0 more data not buffered
  - wlan.fc.moredata==1 more data buffered



IEEE 802.11 QoS Data (Website Browsing)

- The below wireshark capture indicates wireless station's "website browsing activities" in our hands-on lab
  - For example, google.com, youtube.com

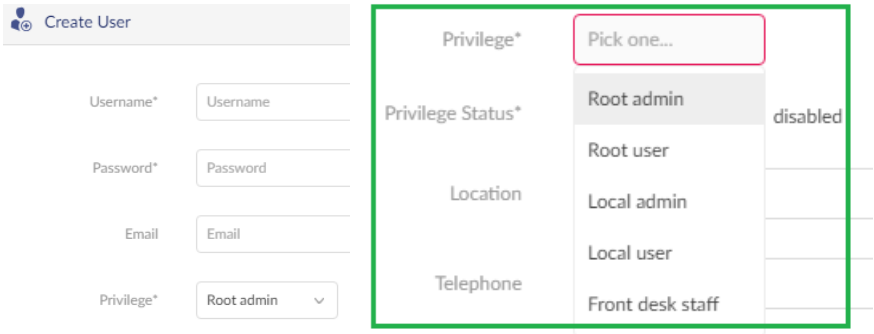


Nuclias Connect Hands-on Tutorial

- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

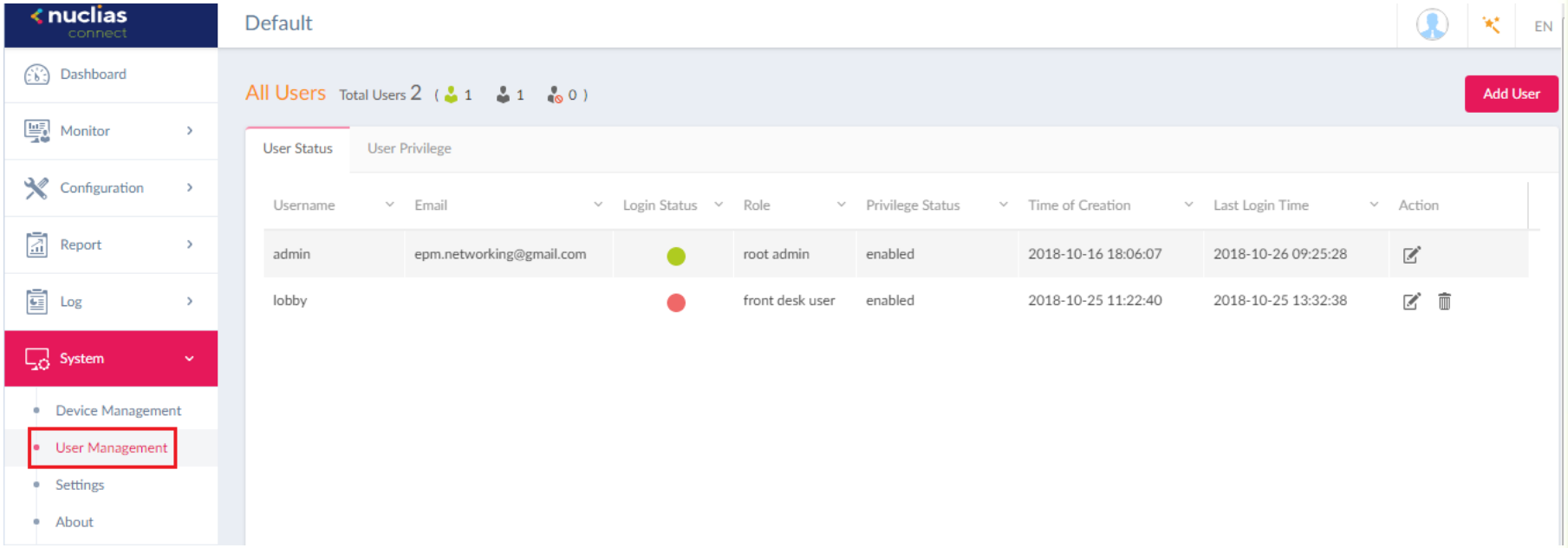
User Management, Access Control and System Administration

- In CWM 1.0, user account privileges are known as (DK1500249)
  - Root Admin, is able to view all the settings of groups, system configuration, monitoring, systemlog etc. [v.1.03rc0098, Root User]
  - Root User, can view settings and latest status as "Root Admin" but not able to make configuration changes
  - Local Admin, is given the authority to manage the group specified by "Root Admin"
  - Local User, is assigned the power to view all the info of group specified by "Root Admin" cannot manage
  - Front Desk Staff, is responsible for the passcode management is assigned Sites



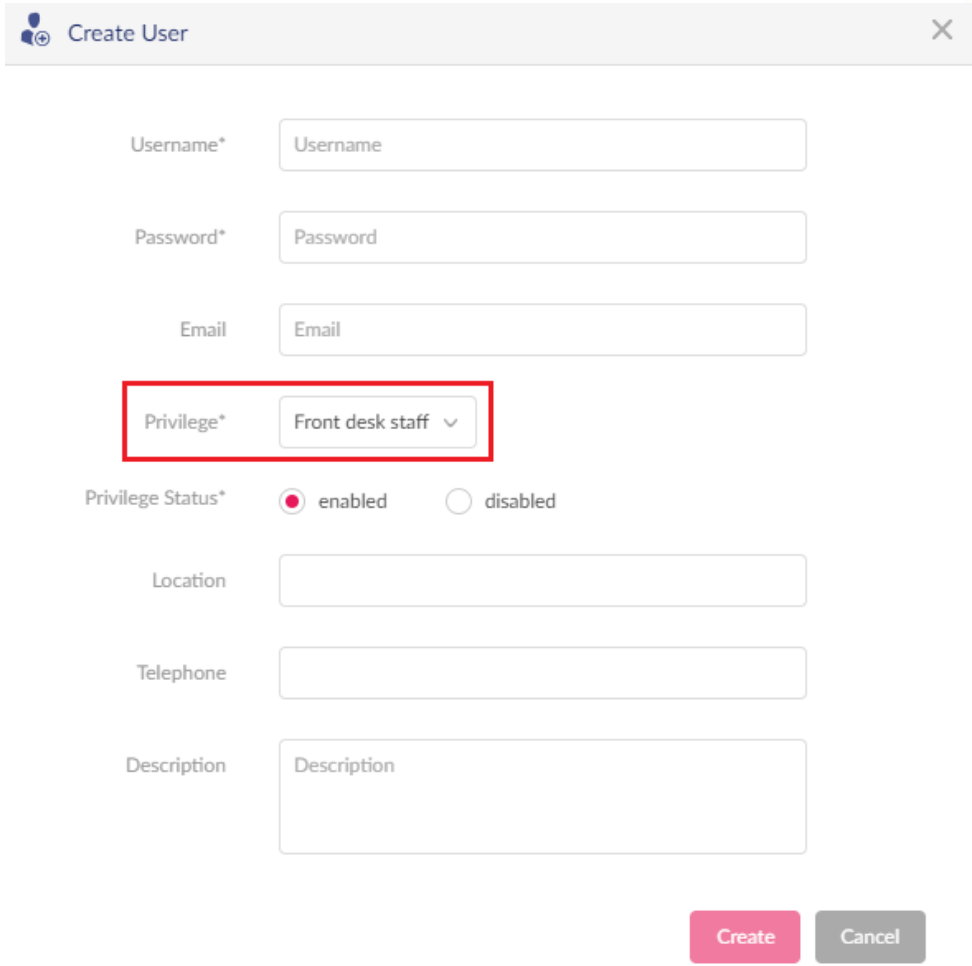
User Management, Access Control and System Administration

- User Account Creation
- User Account Creation on the User Management page under the System tab



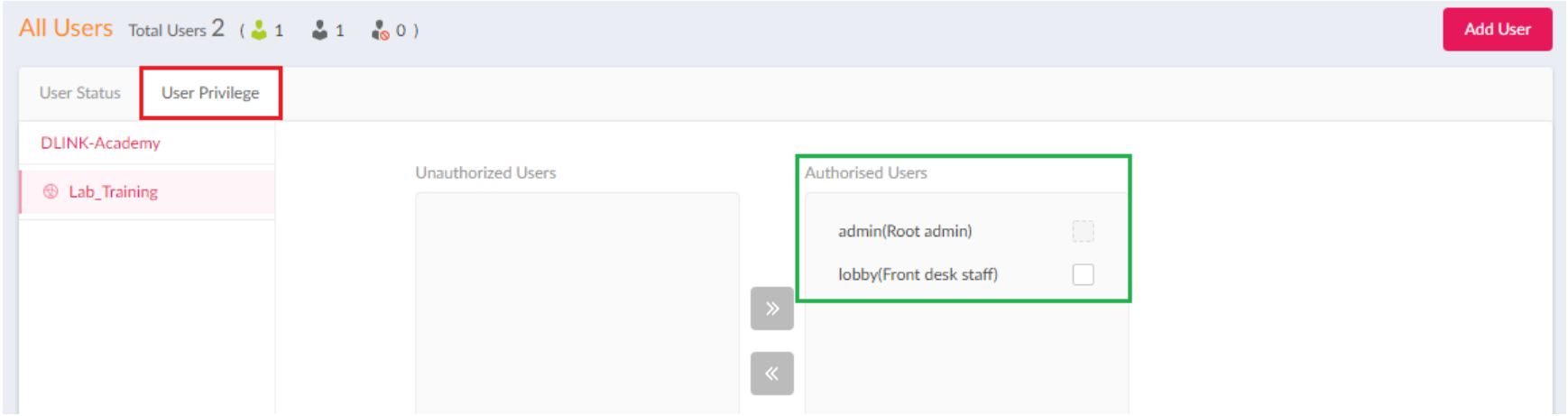
User Management, Access Control and System Administration

- Passcode setup privilege
- A “frontdesk” user account needs to be set up
  - Menu: System > User Management > Add User”
  - Privilege: Front Desk Staff



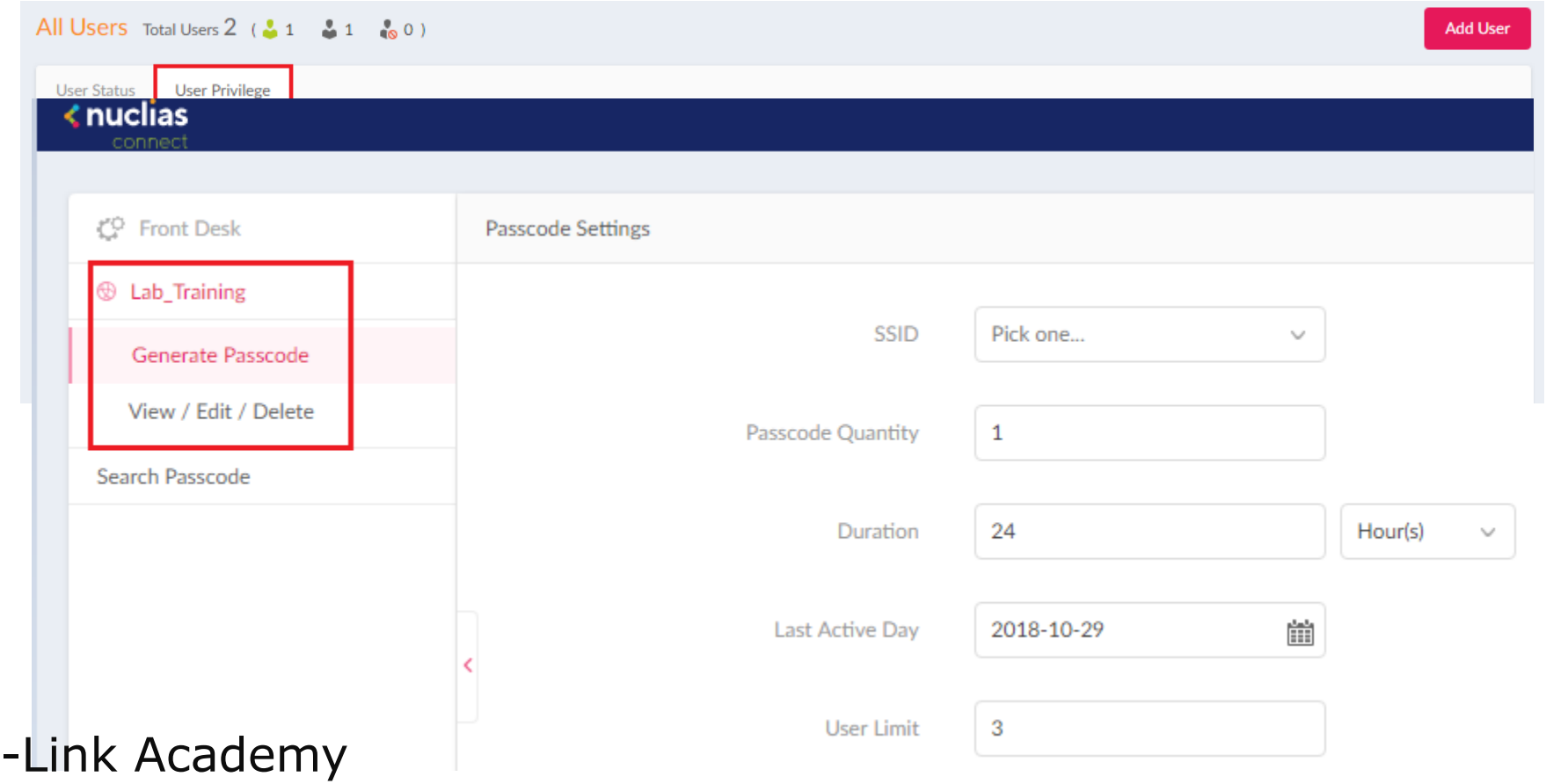
User Management, Access Control and System Administration

- User privilege should be provided to that user, in order to exercise required duties.



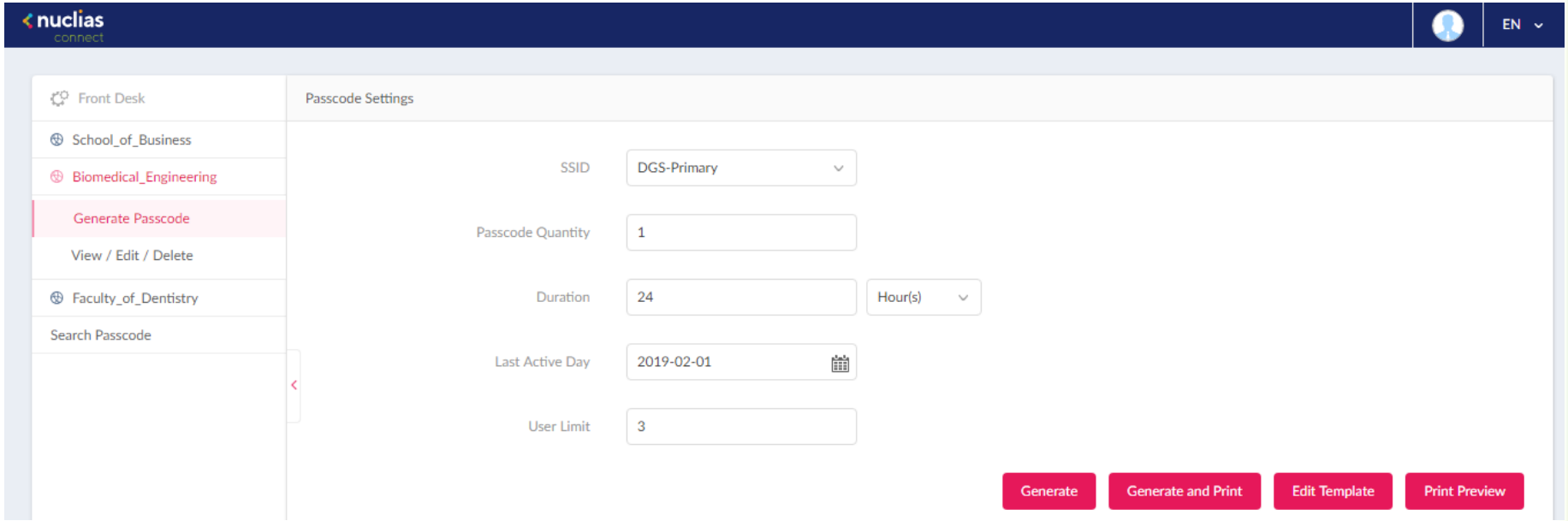
User Management, Access Control and System Administration

- User privilege should be provided to that user, in order to exercise required duties.



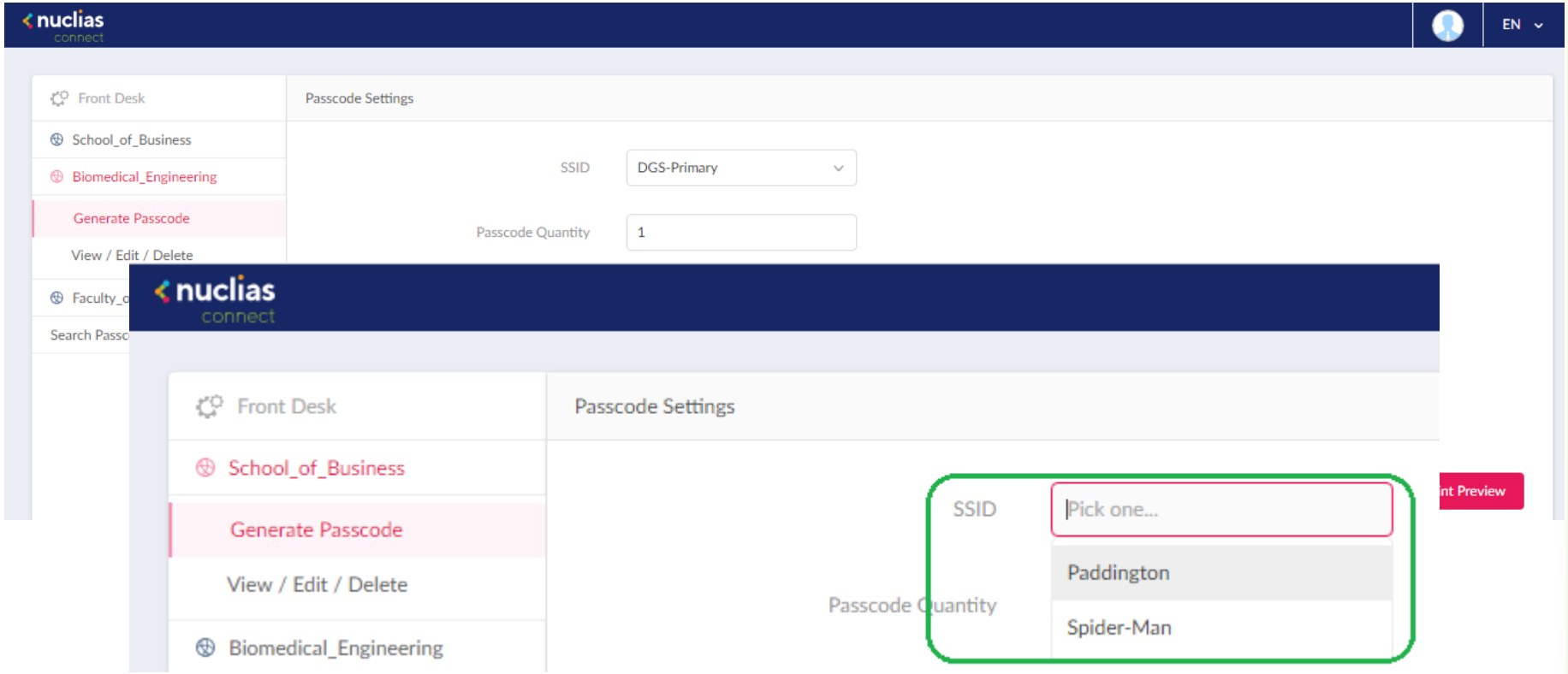
User Management, Access Control and System Administration

- Another example regarding "Front Desk Staff" privilege (multiple Site / Network associations).



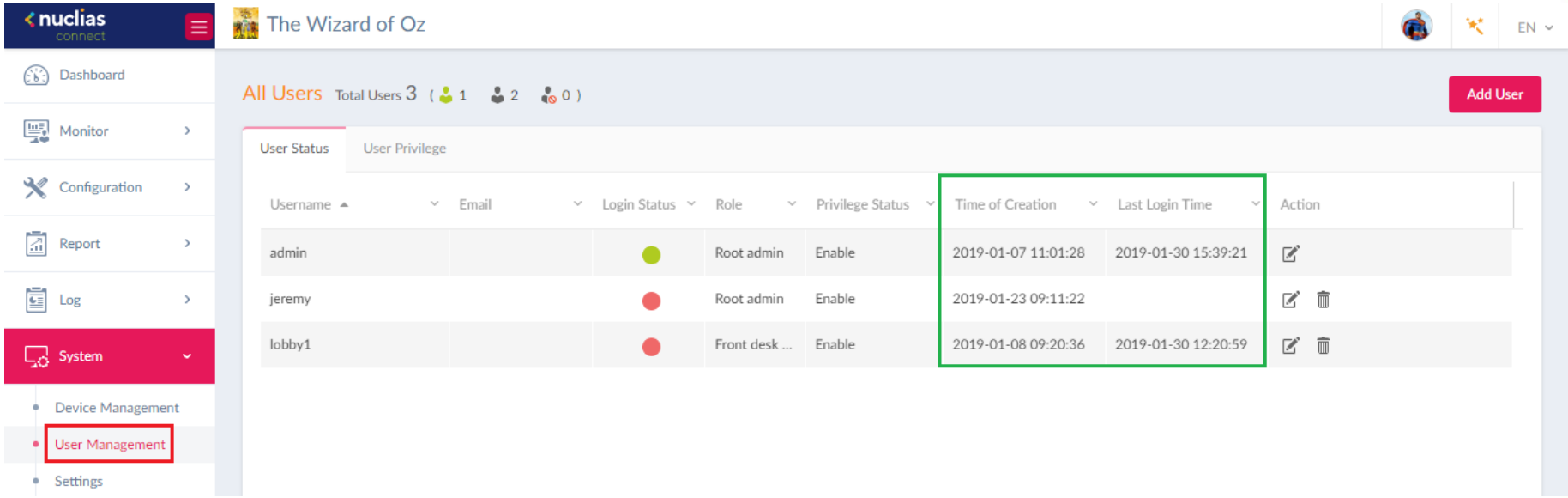
User Management, Access Control and System Administration

- Another example regarding "Front Desk Staff" privilege (multiple Site / Network associations).



User Management, Access Control and System Administration

- User Account Management, Last Login Time
- The "last login" attribute is the most accurate way to check active users last logon time.
  - It could be used to identify stale user and computer accounts.



User Management, Access Control and System Administration

- SSID Broadcast
- Wireless Client List
- Wireless Client Polling Interval
- Wireless Client Connection (Wireshark Capture)
- Connected Clients Search
- MAC Access Control List (ACL)
- Passcode User Authentication
- Captive Portal Login Page Customization
- Wireless Network Connections Limitations
- RSSI Threshold
- WLAN Partition
- Blocking Access To Our Network

Configuring Multiple SSIDs

Service Set Identifier (SSID) Configuration Guide

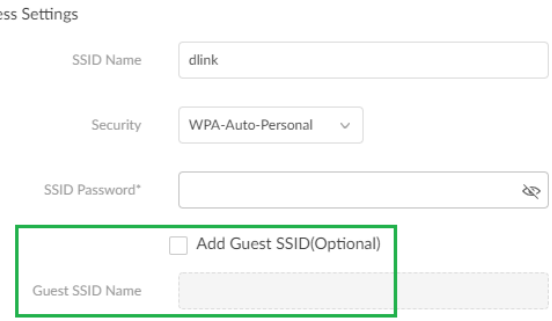
- SSIDs are case sensitive and can contain up to 32 alphanumeric characters
- There are settings we can apply to individual SSID
  - VLAN (IP Interference Settings)
  - Wireless Client Authentication method (Username/Password, Remote RADIUS, LDAP, POP3, and etc..)
  - Redirection of packets
- Do not include spaces in your SSIDs



Configuring Multiple SSIDs

Service Set Identifier (SSID) Configuration Guide

- Guest Mode SSID
  - Guest Mode SSID is used to response to probe request with a wildcard SSID.
  - When enabled, it assists wireless clients passively scan to associate the AP, but do not transmit probe requests.

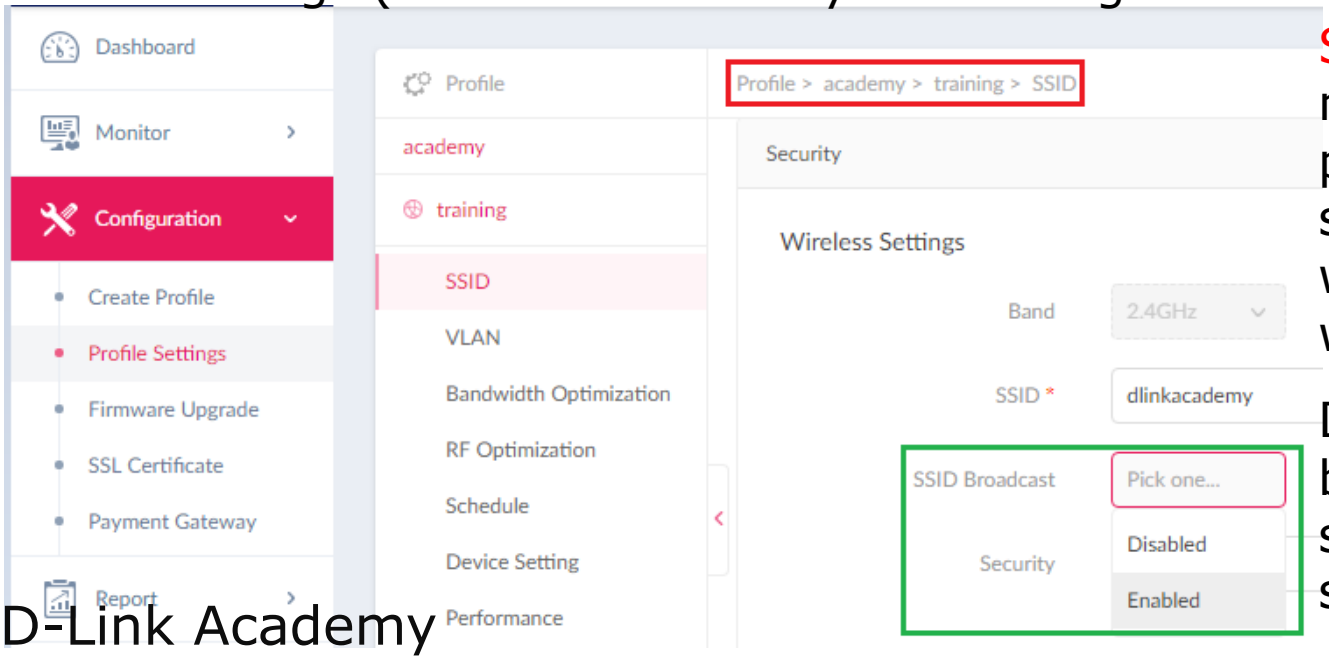


No.	Time	Source	Destination	Protocol	Info
9887	2018-10-08 18:40:40.621267900	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1190, FN=0, Flags=........, SSID=Wildcard (Broadcast)
9925	2018-10-08 18:40:40.965567200	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1195, FN=0, Flags=........, SSID=Wildcard (Broadcast)
9931	2018-10-08 18:40:41.079922600	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1197, FN=0, Flags=........, SSID=Wildcard (Broadcast)
9932	2018-10-08 18:40:41.080810800	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1198, FN=0, Flags=........, SSID=Wildcard (Broadcast)
9956	2018-10-08 18:40:41.429166000	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1204, FN=0, Flags=........, SSID=Wildcard (Broadcast)
10723	2018-10-08 18:40:45.859927100	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1222, FN=0, Flags=........, SSID=Wildcard (Broadcast)
10850	2018-10-08 18:40:46.204095000	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1227, FN=0, Flags=........, SSID=Wildcard (Broadcast)
10851	2018-10-08 18:40:46.205005200	D-LinkIn_03:58:b6	Broadcast	802.11	Probe Request, SN=1228, FN=0, Flags=........, SSID=Wildcard (Broadcast)
7163	2018-10-08 18:40:20.815164600	be:45:ad:34:1c:e4	Broadcast	802.11	Probe Request, SN=1234, FN=0, Flags=........, SSID=Wildcard (Broadcast)
79	2018-10-08 18:39:36.102008700	Apple_d1:1c:37	Broadcast	802.11	Probe Request, SN=1235, FN=0, Flags=........, SSID=Wildcard (Broadcast)

  - When disabled, client devices do not specify SSID is not accepted (more secure)

SSID Broadcast Lab Practice (1/7)

- SSID Broadcast (Enable and Disable Mode)
- By default, wireless access points (APs) automatically transmit their network name (SSID) into the open air.
- Disable this feature on your Wi-Fi network with Nuclias Connect can be achieved by using the function of Configuration > Profile Settings (Profile > academy > training > SSID).

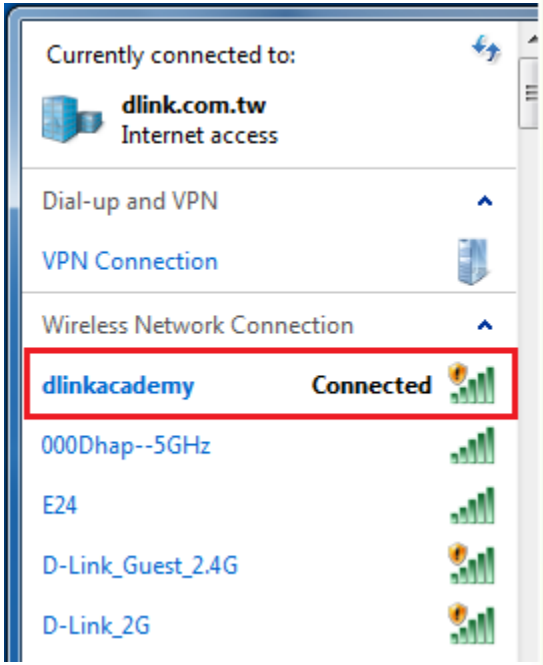


SSID Broadcast makes it easier for potential hackers to see that you have a wireless network within range.

Disable SSID broadcast could be seen as a simple security solution.

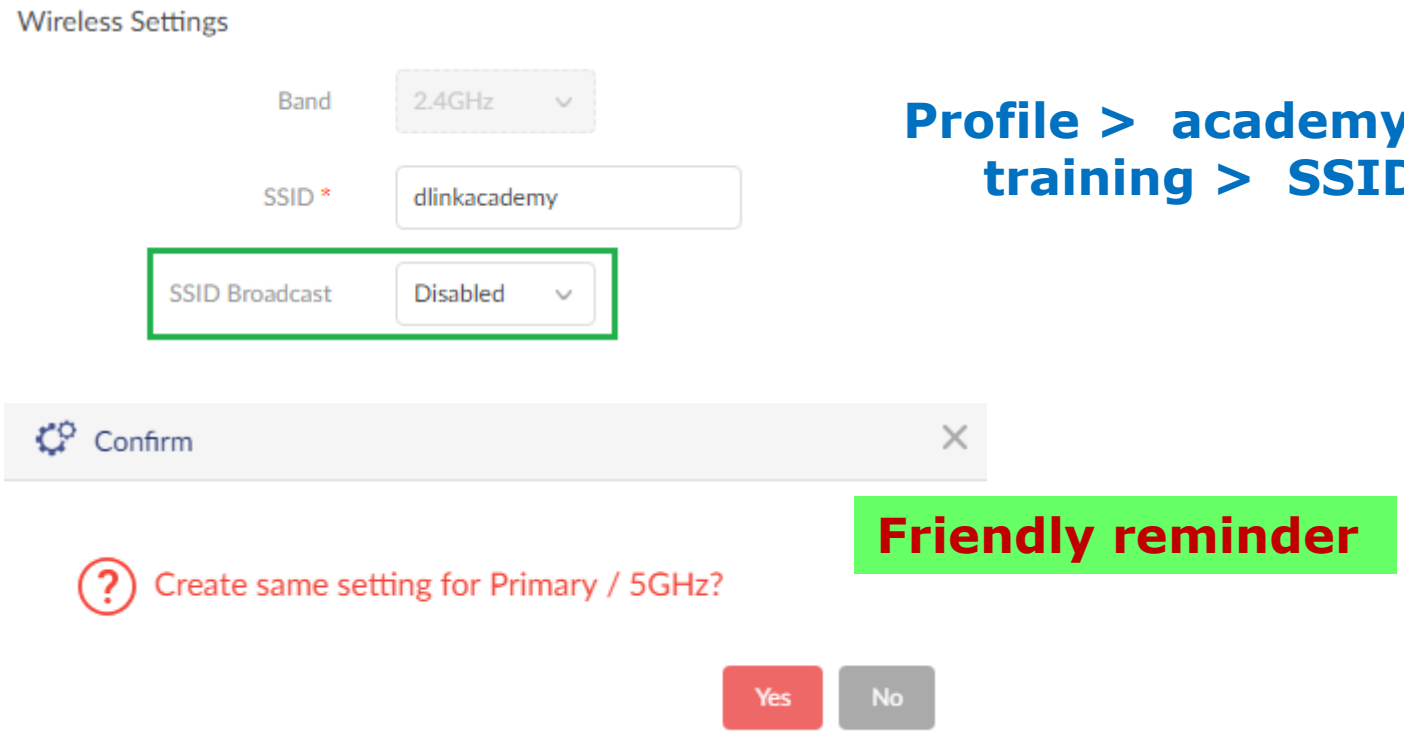
SSID Broadcast Lab Practice (2/7)

- SSID Broadcast (Enable and Disable Mode)
- SSID Broadcast (it is in enabled mode)
- Wireless station is able to see that SSID



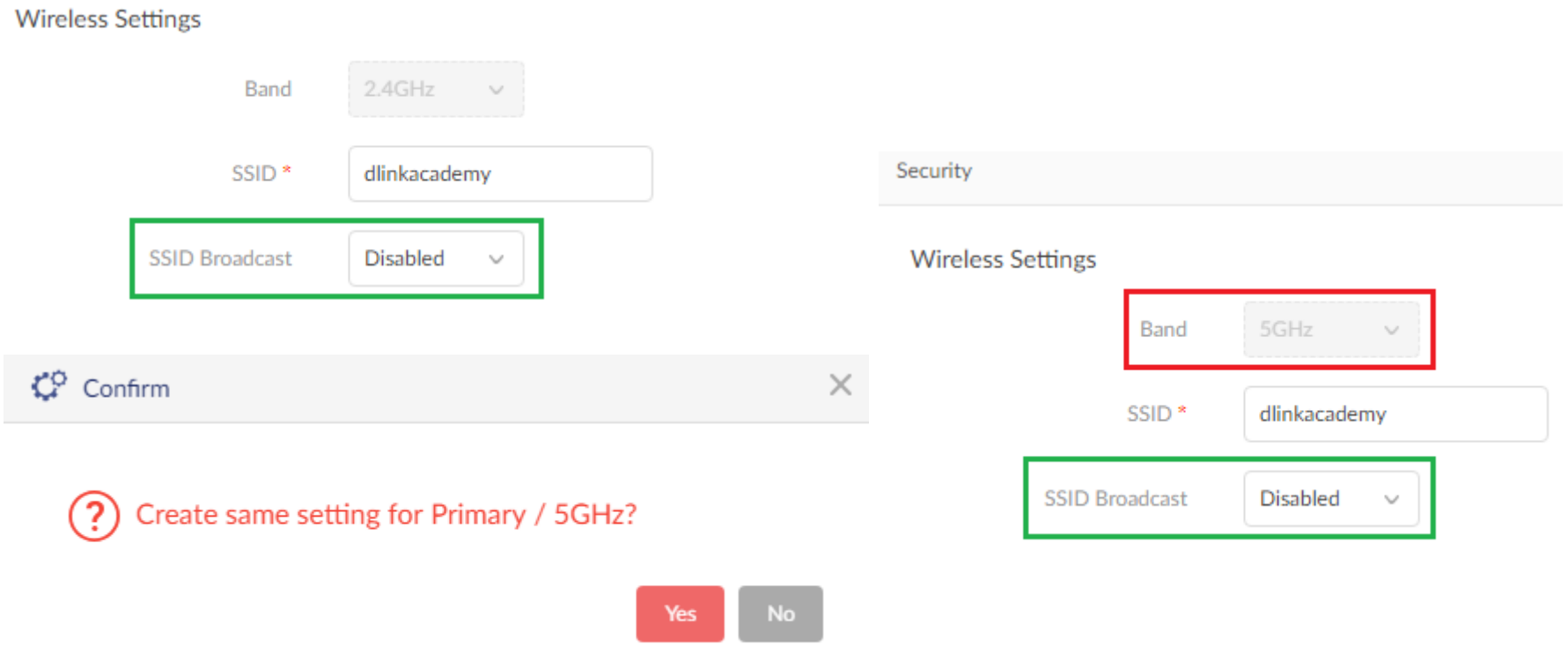
SSID Broadcast Lab Practice (3/7)

- SSID Broadcast (Enable and Disable Mode)
- Disable SSID Broadcast (Nuclias Connect configurations)



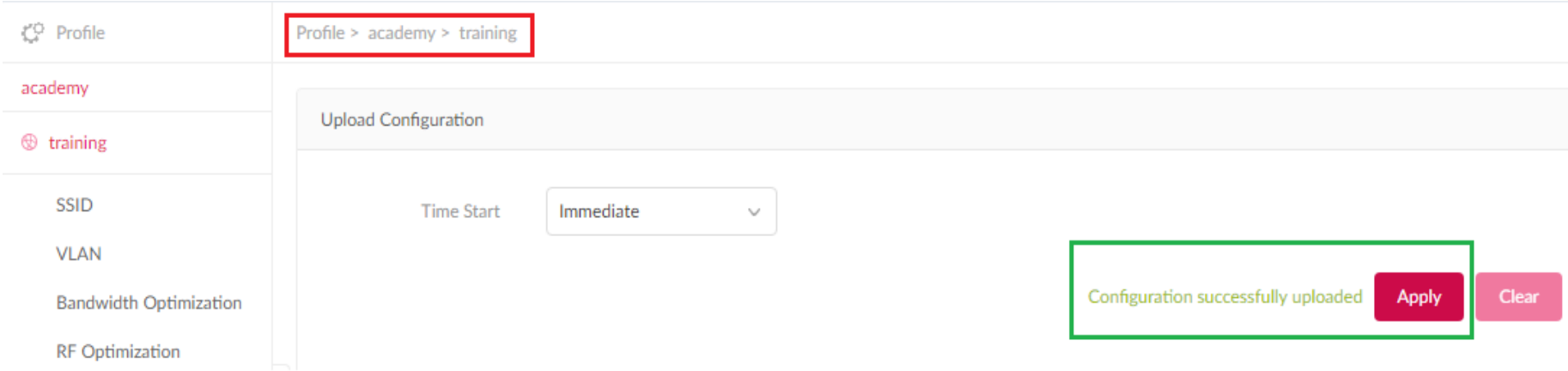
SSID Broadcast Lab Practice (4/7)

- SSID Broadcast (Enable and Disable Mode)
- Disable SSID Broadcast (Nuclias Connect configurations)



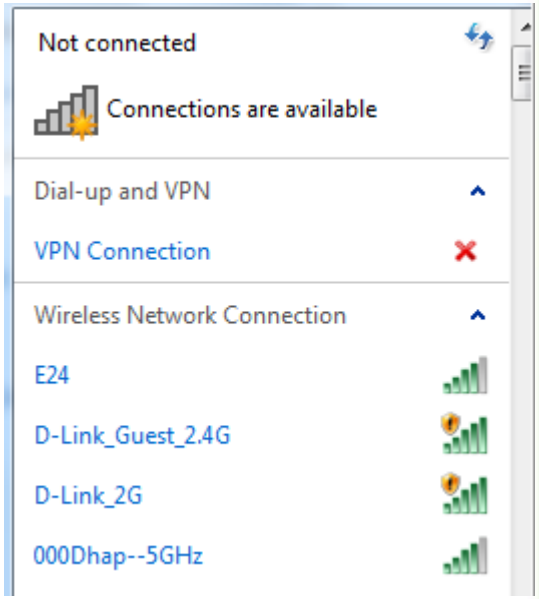
SSID Broadcast Lab Practice (5/7)

- SSID Broadcast (Enable and Disable Mode)
- Disable SSID Broadcast (Apply the latest configurations to AP)



SSID Broadcast Lab Practice (6/7)

- SSID Broadcast (Enable and Disable Mode)
- SSID Broadcast (it is in disabled mode)
- Wireless station CAN NOT see that SSID



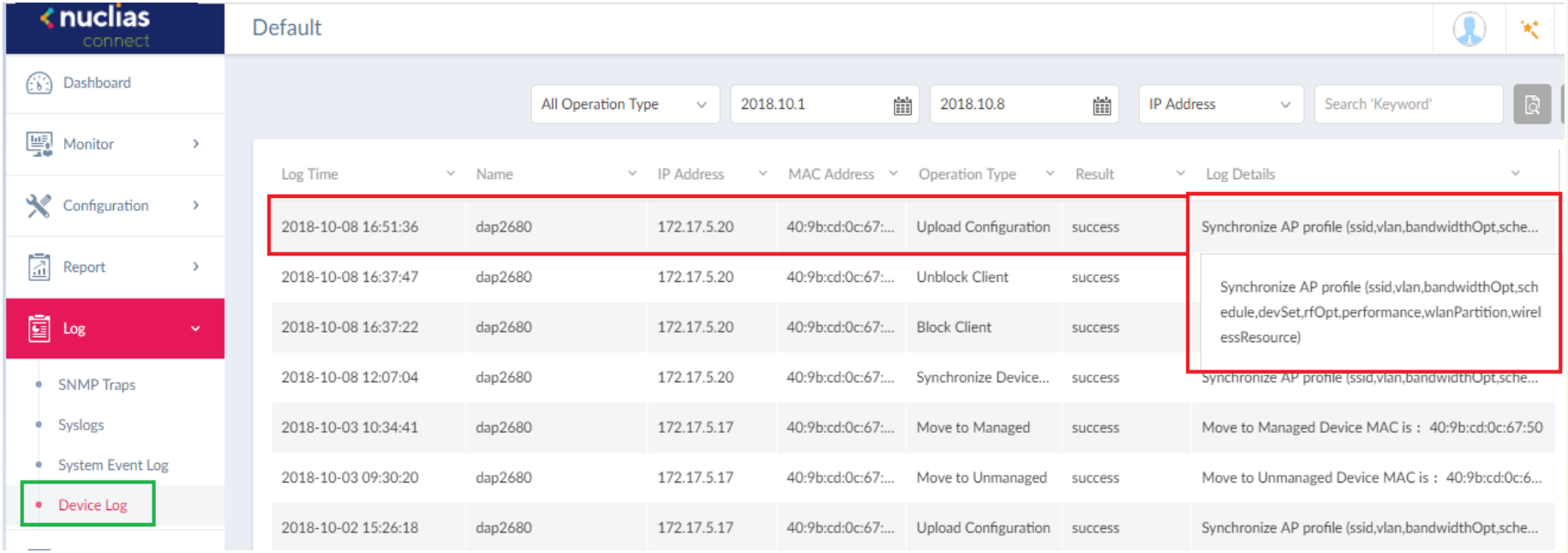
- Please revert to "enabled mode" for the remaining exercises

SSID Broadcast Lab Practice (7/7)

- SSID Broadcast (Enable and Disable Mode)
- Brain Storming
  - (a) What kind of message in “Log > Device Log” describing the activity we were just experienced?

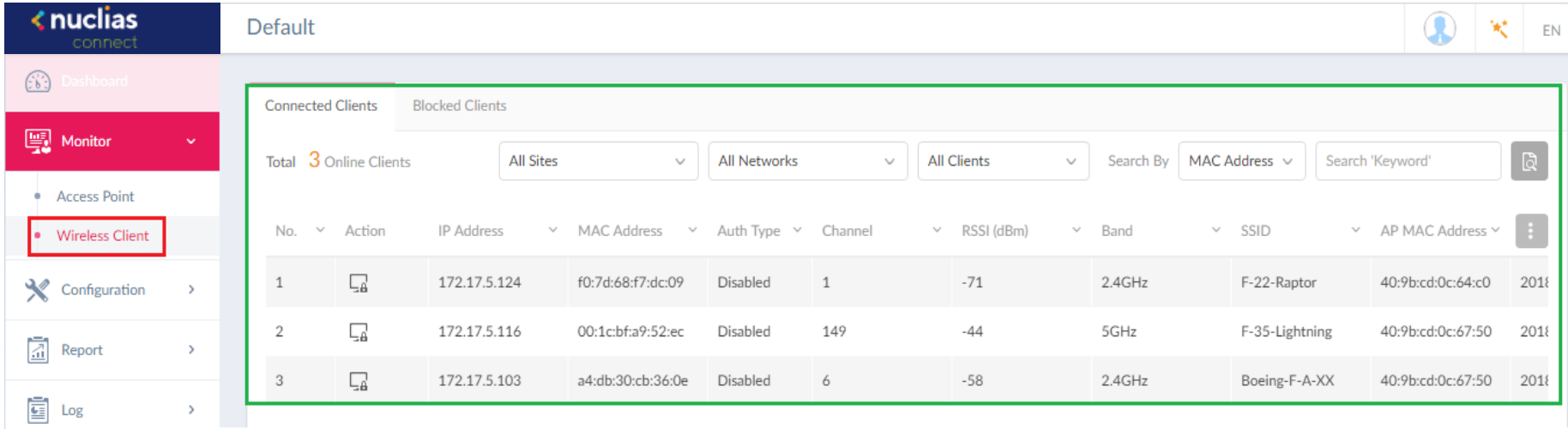
SSID Broadcast Lab Practice (7/7)

- SSID Broadcast (Enable and Disable Mode)
- Brain Storming
  - (a) What kind of message in "Log > Device Log" describing the activity we were just experienced?



Wireless Client List

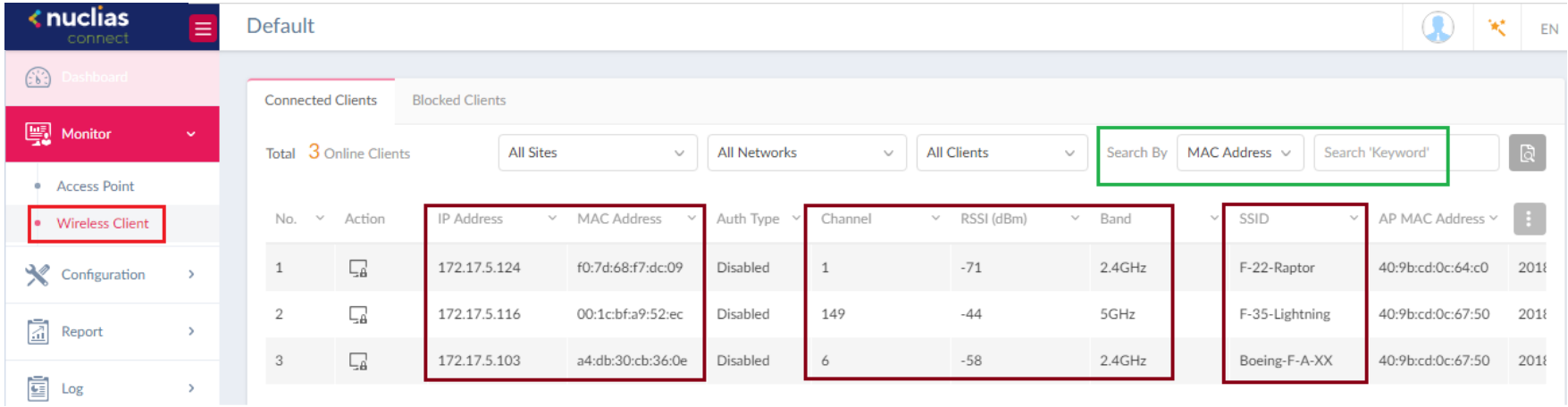
- The list of Wireless Clients are on the “Wireless Client” page under the Monitor tab.
- It is used to display how the network is being used and by which client devices.



Wireless Client List

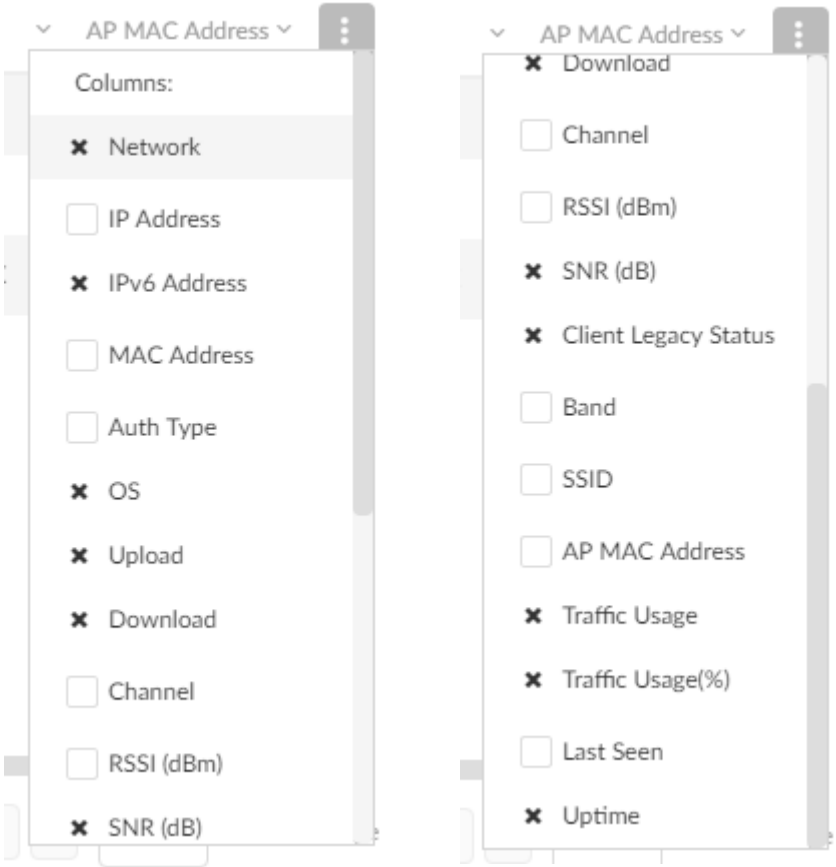
Wireless Client List consists the following information

- The MAC, IP address of each wireless client.
- The 802.11 channels, their channel frequencies, and the measurement of the power present in a received radio signal.
- The association with any SSID which being advertised by our DNC managed wireless topology.
- The wireless client search criteria, by IP or MAC address.



Wireless Client List

- The Wireless Client List also offers the flexibility to add more column in releasing Wireless Client information.
  - An X mark next to the checkbox makes information invisible.



Wireless Client List

- Usage stats for Individual upload / download links

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.124	f0:7d:68:f7:dc:09	Disabled	1	-67	2.4GHz	F-22-Raptor	40:9b:cd:0c:64:c	
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-44	5GHz	F-35-Lightning	40:9b:cd:0c:67:5	
172.17.5.103	a4:db:30:cb:36:0e	Disabled	6	-60	2.4GHz	Boeing-F-A-XX	40:9b:cd:0c:67:5	

OS
Upload
Download
Channel

Connected Clients | Blocked Clients

Total 3 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

IP Address	MAC Address	Auth Type	Upload	Download	Channel	RSSI (dBm)	Band	SSID	AP MAC Addr
172.17.5.124	f0:7d:68:f7:dc:09	Disabled	71.78 MB	2.74 MB	1	-70	2.4GHz	F-22-Rap	
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	22.04 MB	35.26 MB	149	-44	5GHz	F-35-Ligh	
172.17.5.103	a4:db:30:cb:36:0e	Disabled	100.61 MB	2.25 GB	6	-58	2.4GHz	Boeing-F	

OS
Upload
Download
Channel

for Individual upload

Wireless Client List

- Usage stats for Individual upload / download links

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.124	f0:7d:68:f7:dc:09	Disabled	1	-67	2.4GHz	F-22-Raptor	40:9b:cd:0c:64:c	
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-44	5GHz	F-35-Lightning	40:9b:cd:0c:67:5	
172.17.5.103	a4:db:30:cb:36:0e	Disabled	6	-60	2.4GHz	Boeing-F-A-XX	40:9b:cd:0c:67:5	

OS
Upload
Download
Channel

Connected Clients | Blocked Clients

Total 3 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

IP Address	MAC Address	Auth Type	Upload	Download	Channel	RSSI (dBm)	Band	SSID	AP MAC Addr
172.17.5.124	f0:7d:68:f7:dc:09	Disabled	71.78 MB	2.74 MB	1	-70	2.4GHz	F-22-Rap	
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	22.04 MB	35.26 MB	149	-44	5GHz	F-35-Ligh	
172.17.5.103	a4:db:30:cb:36:0e	Disabled	100.61 MB	2.25 GB	6	-58	2.4GHz	Boeing-F	

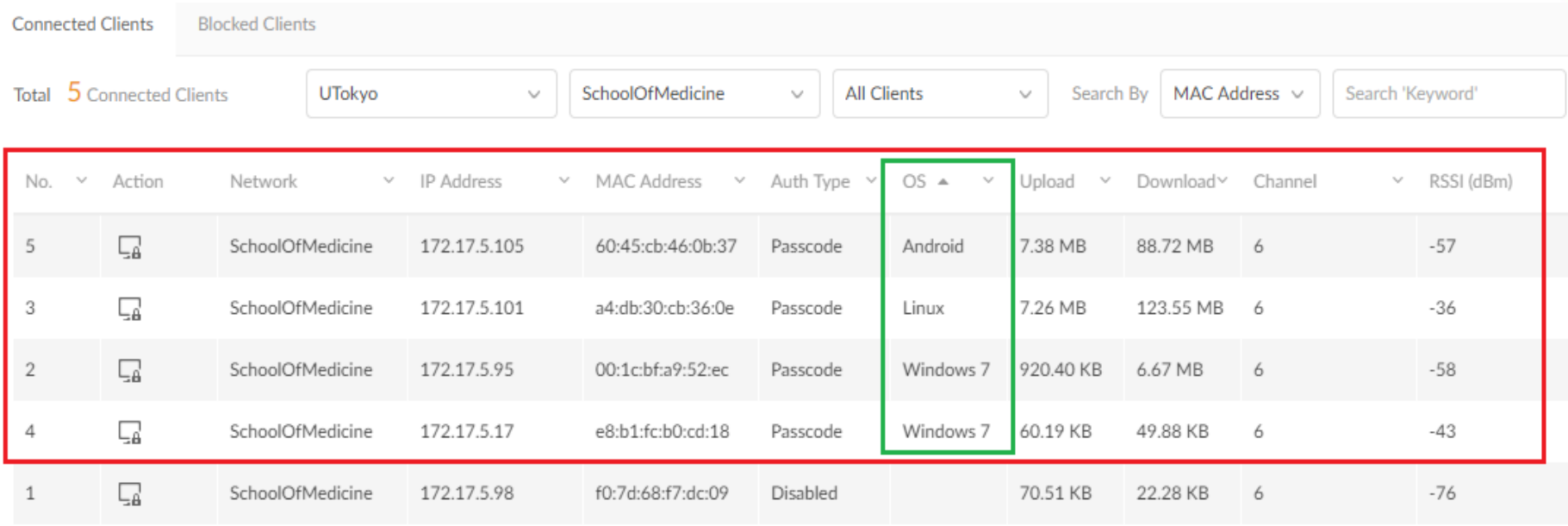
OS
Upload
Download
Channel

Whom is our Top 1 client on data consumption?

Wireless Client List, Operating System Information

The OS field in Wireless Client List

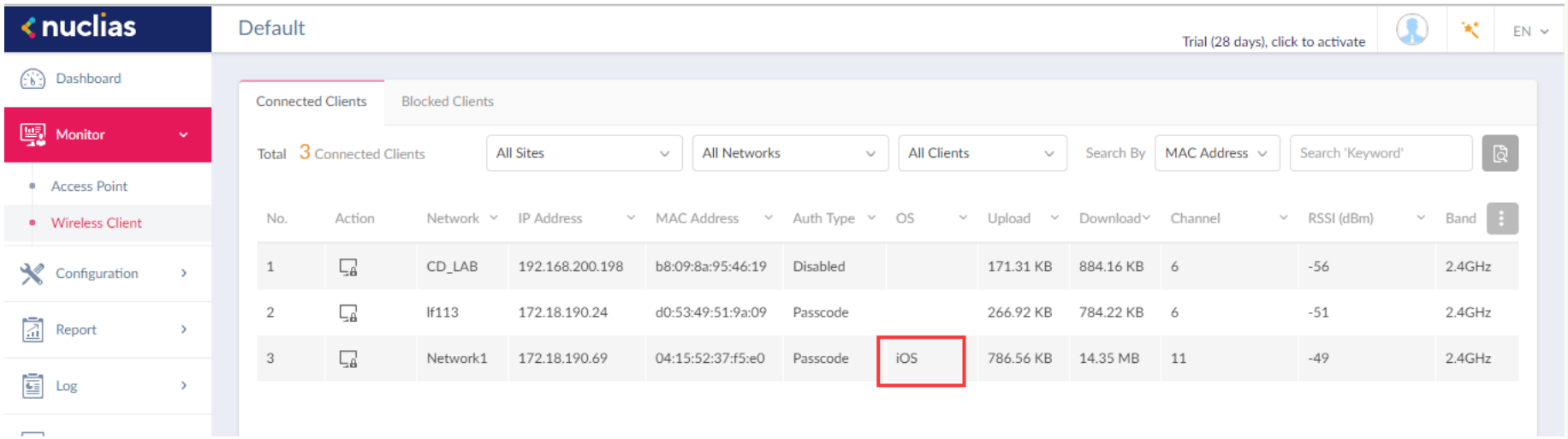
- Ubuntu 16.04 SNMP
  - Enabling Ubuntu 16.04 SNMP (sudo apt-get install snmp snmp-mibs-downloader; sudo apt-get install snmpd)



Wireless Client List, Operating System Information

The OS field in Wireless Client List

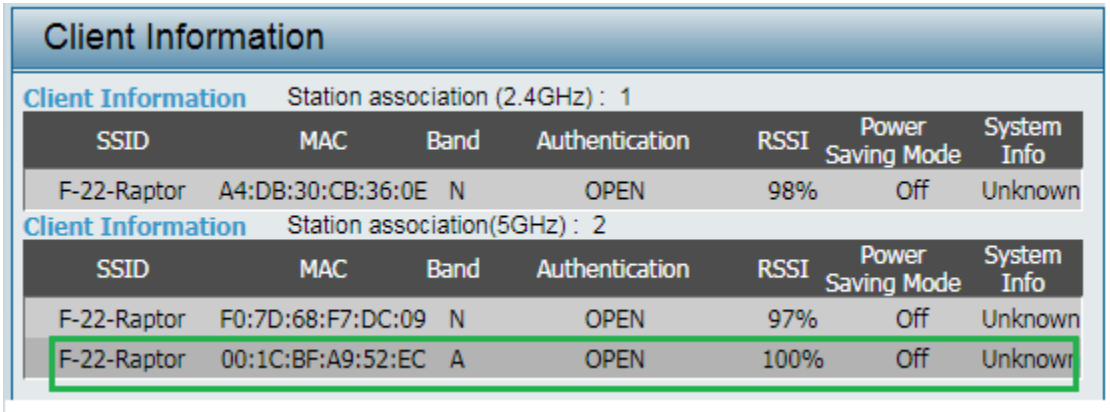
- Another example where a wireless client uses iPhone



Wireless Client List

- The column of "Client Legacy Status"

No.	Action	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	SNR (dB)	Client Legacy Status
1		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-48	47	YES
2		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	149	-56	39	NO
3		172.17.5.103	a4:db:30:cb:36:0e	Disabled	6	-56	39	NO



Wireless Client Polling Interval

- Wireless Client (Time frequency to pull wireless station information in, around 90 seconds).

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-52	5GHz	dlinkacademy	40:9b:cd:0c:67:50	2018-10-04 08:37:30

Wireless Client Polling Interval

- Wireless Client (Time frequency to pull wireless station information in, around 90 seconds).

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-52	5GHz	dlinkacademy	40:9b:cd:0c:67:50	2018-10-04 08:37:30

Total 1 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-51	5GHz	dlinkacademy	40:9b:cd:0c:67:50	2018-10-04 08:39:01

Wireless Client Polling Interval

- Wireless Client (Time frequency to pull wireless station information in, around 90 seconds).

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-52	5GHz	dlinkacademy	40:9b:cd:0c:67:50	2018-10-04 08:37:30

Total 1 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-51	5GHz	dlinkacademy	40:9b:cd:0c:67:50	2018-10-04 08:39:01

Total 1 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-52	5GHz	dlinkacademy	40:9b:cd:0c:67:50	2018-10-04 08:40:32

Wireless Client Polling Interval

- Another live example regarding Wireless Client Polling Interval, which shall be 90 seconds as well.

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.192.115	00:21:6a:65:e0:a2	Disabled	48	-43	5GHz	2680-CWM	40:9b:cd:0c:66:b0	2018-10-04 08:56:39
172.17.192.116	00:21:5d:27:32:4e	Disabled	48	-43	5GHz	2680-CWM	40:9b:cd:0c:66:b0	2018-10-04 08:56:39

Total 2 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

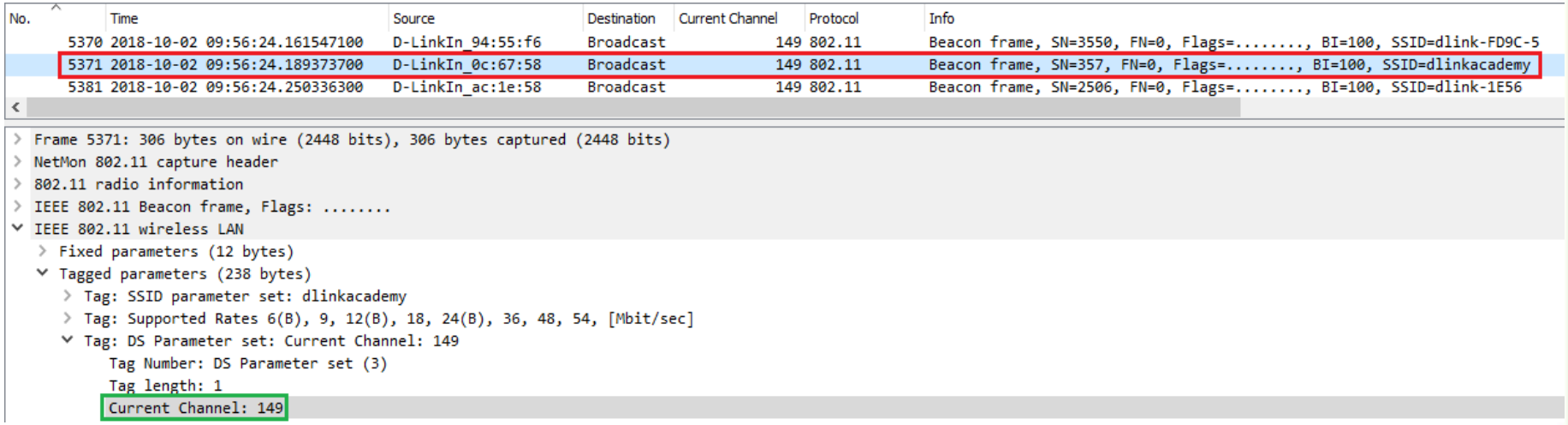
IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.192.115	00:21:6a:65:e0:a2	Disabled	48	-43	5GHz	2680-CWM	40:9b:cd:0c:66:b0	2018-10-04 08:58:11
172.17.192.116	00:21:5d:27:32:4e	Disabled	48	-48	5GHz	2680-CWM	40:9b:cd:0c:66:b0	2018-10-04 08:58:11

Total 2 Online Clients | All Sites | All Networks | All Clients | Search By MAC Address | Search 'Keyword'

IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address	Last Seen
172.17.192.115	00:21:6a:65:e0:a2	Disabled	48	-44	5GHz	2680-CWM	40:9b:cd:0c:66:b0	2018-10-04 08:59:41
172.17.192.116	00:21:5d:27:32:4e	Disabled	48	-43	5GHz	2680-CWM	40:9b:cd:0c:66:b0	2018-10-04 08:59:41

Wireless Client Connection (Wireshark Capture)

- This wireless client (Dell laptop, IP: 172.17.5.116) is connected to wireless channel 149.

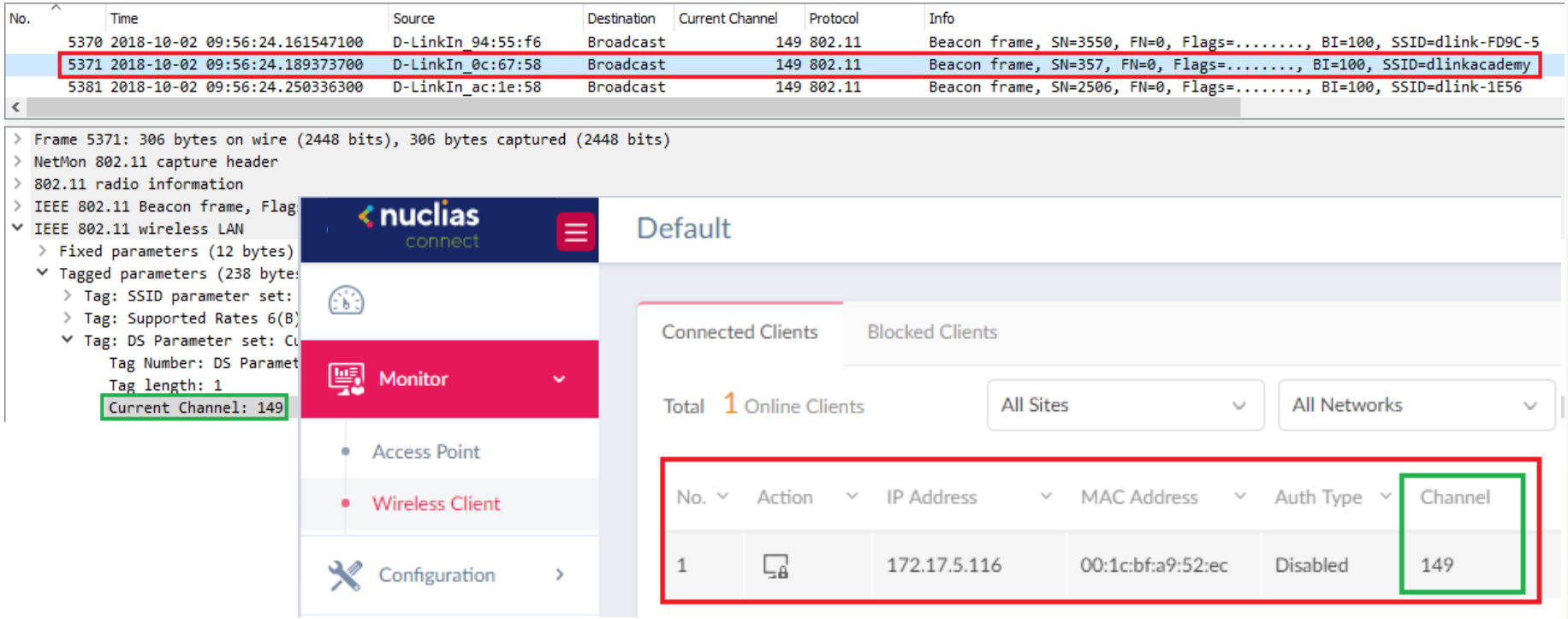


No.	Time	Source	Destination	Current Channel	Protocol	Info
5370	2018-10-02 09:56:24.161547100	D-LinkIn_94:55:f6	Broadcast	149	802.11	Beacon frame, SN=3550, FN=0, Flags=........, BI=100, SSID=dlink-FD9C-5
5371	2018-10-02 09:56:24.189373700	D-LinkIn_0c:67:58	Broadcast	149	802.11	Beacon frame, SN=357, FN=0, Flags=........, BI=100, SSID=dlinkacademy
5381	2018-10-02 09:56:24.250336300	D-LinkIn_ac:1e:58	Broadcast	149	802.11	Beacon frame, SN=2506, FN=0, Flags=........, BI=100, SSID=dlink-1E56

```
> Frame 5371: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits)
> NetMon 802.11 capture header
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 wireless LAN
  > Fixed parameters (12 bytes)
  v Tagged parameters (238 bytes)
    > Tag: SSID parameter set: dlinkacademy
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    v Tag: DS Parameter set: Current Channel: 149
        Tag Number: DS Parameter set (3)
        Tag length: 1
        Current Channel: 149
```

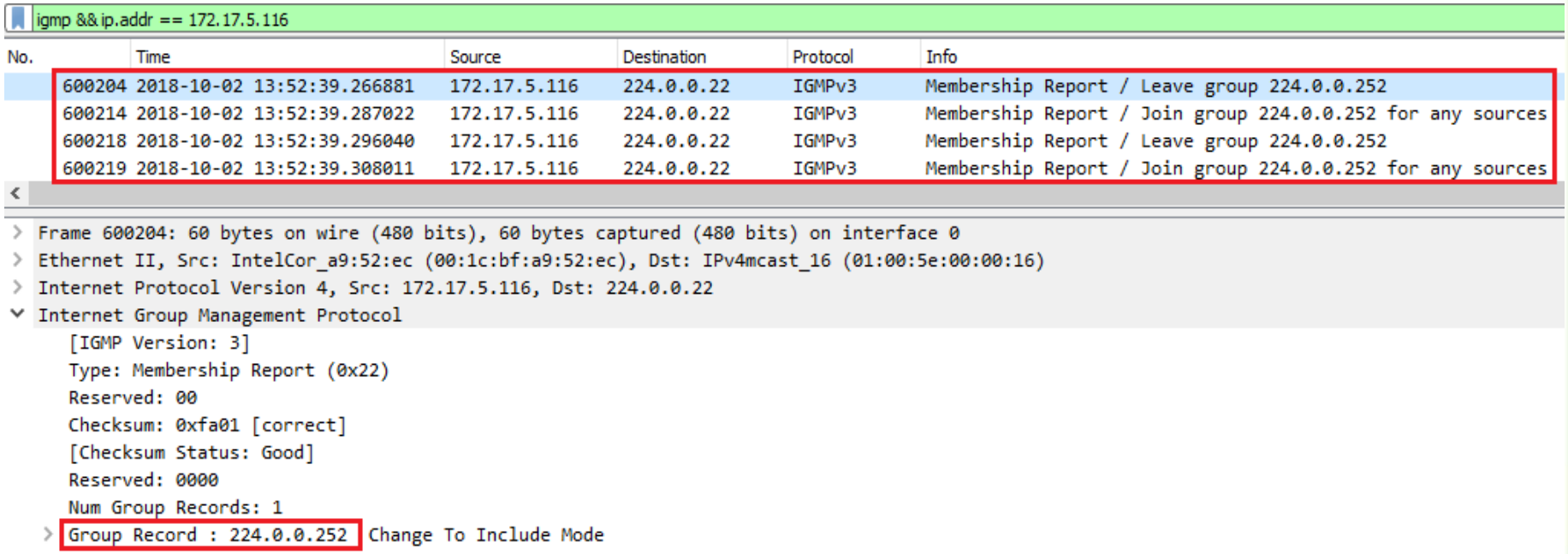
Wireless Client Connection (Wireshark Capture)

- This wireless client (Dell laptop, IP: 172.17.5.116, channel 149) information is corresponding to Nuclias Connect GUI.



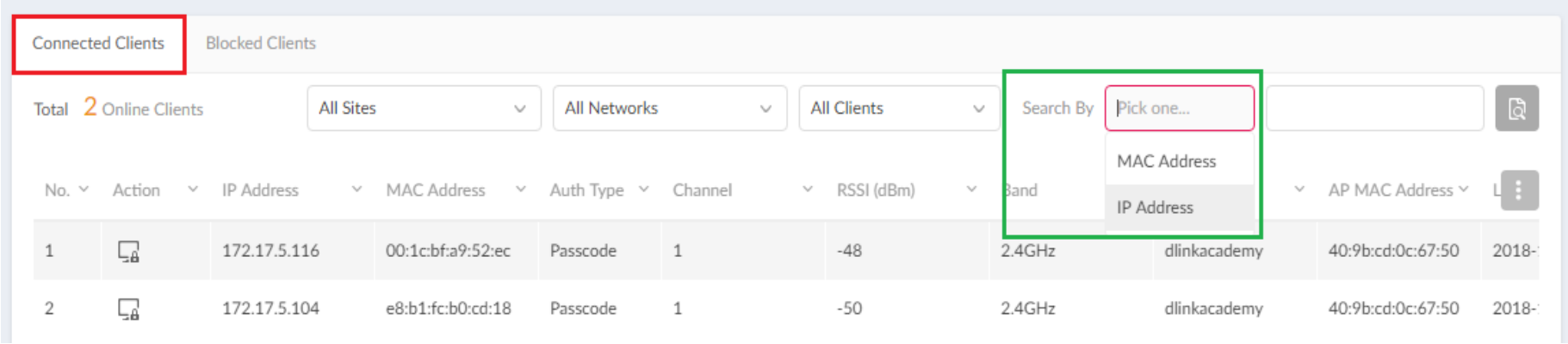
Wireless Client Connection (Wireshark Capture)

- This wireless client (Dell laptop, IP: 172.17.5.116) is browsing Internet on YouTube training materials. [ONOS SDN Controller]



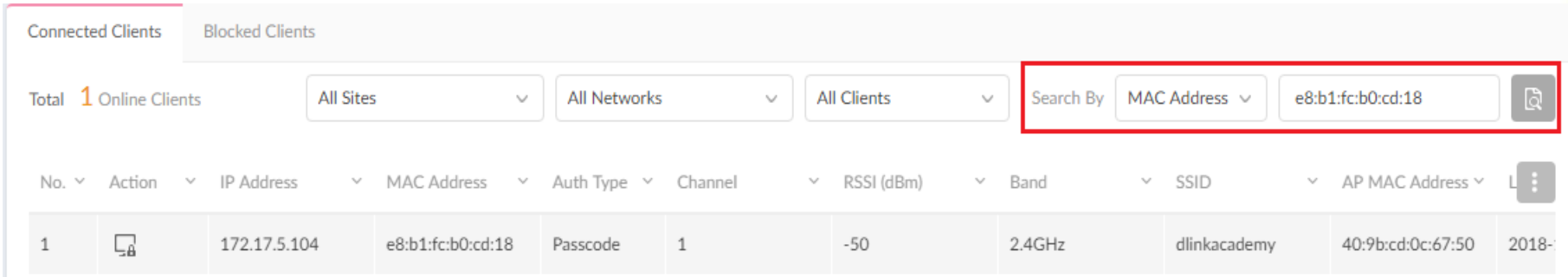
Connected Clients Search (1/2)

- Connected Clients Search Criteria
- Nuclias Connect offers many different types of searching algorithms regarding connected clients
  - MAC address and IP address

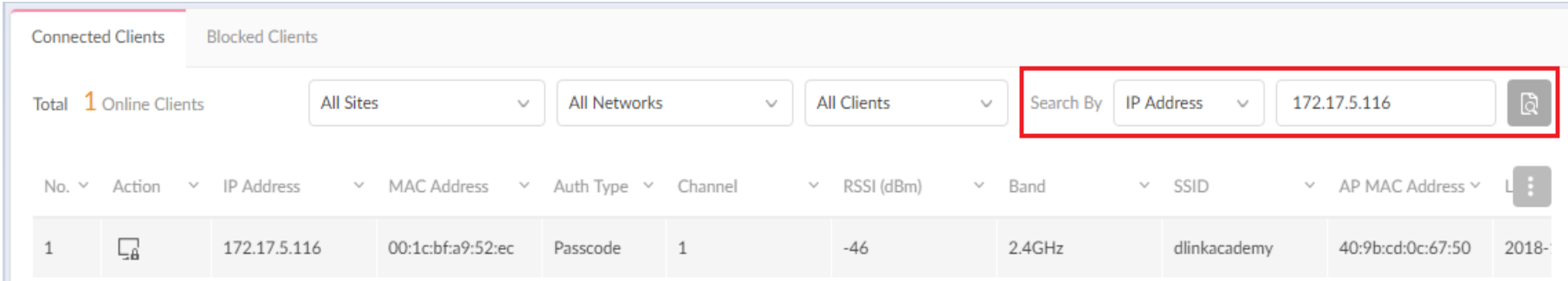


Connected Clients Search (2/2)

- Connected Clients Search Criteria
- By MAC address

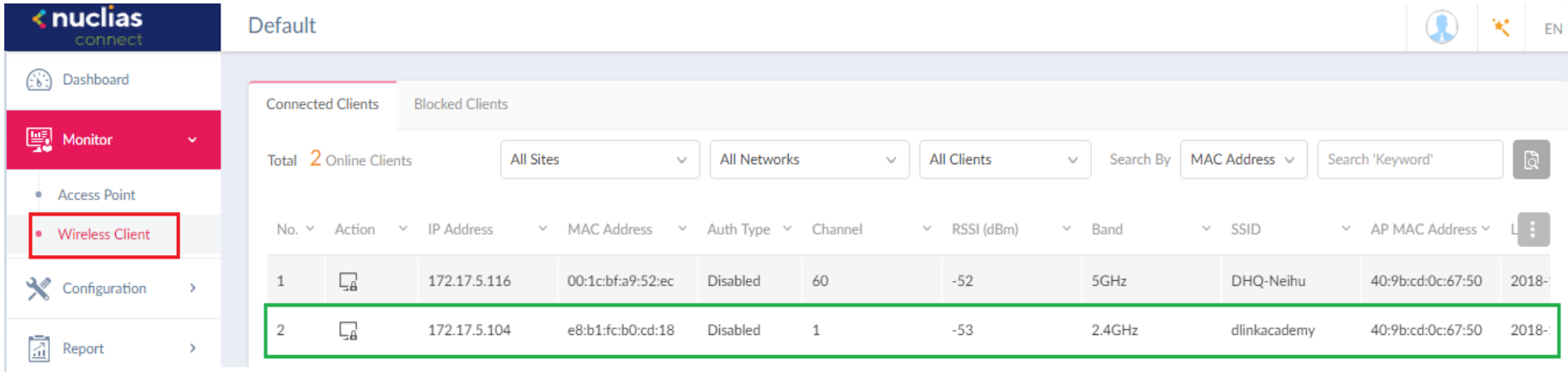


- By IP address



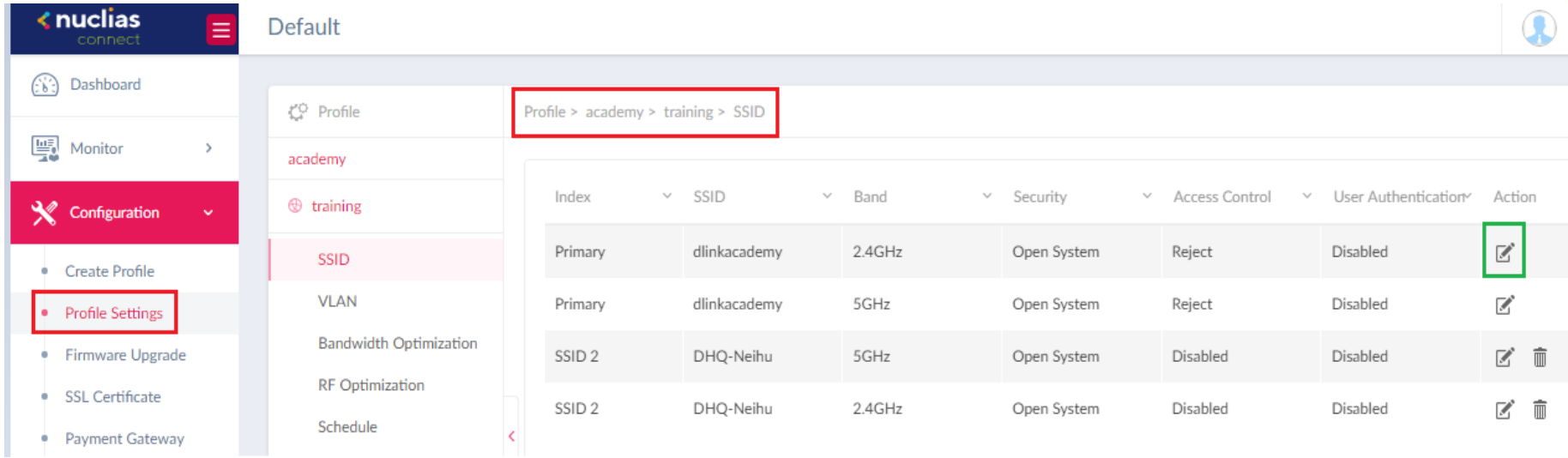
MAC Access Control List (ACL) (1/7)

- MAC Access Control List (ACL) scenario
- A MAC access control list (ACL) lets you permit or deny WiFi access to individual devices based on their MAC addresses. [preventing malicious network activity]
- From DNC menu, Monitor > Wireless Client, we have identified a user with MAC of e8:b1:fc:b0:cd:18 in our network
  - We would like to set up a MAC access control list (ACL) to disallow its access to our wireless network



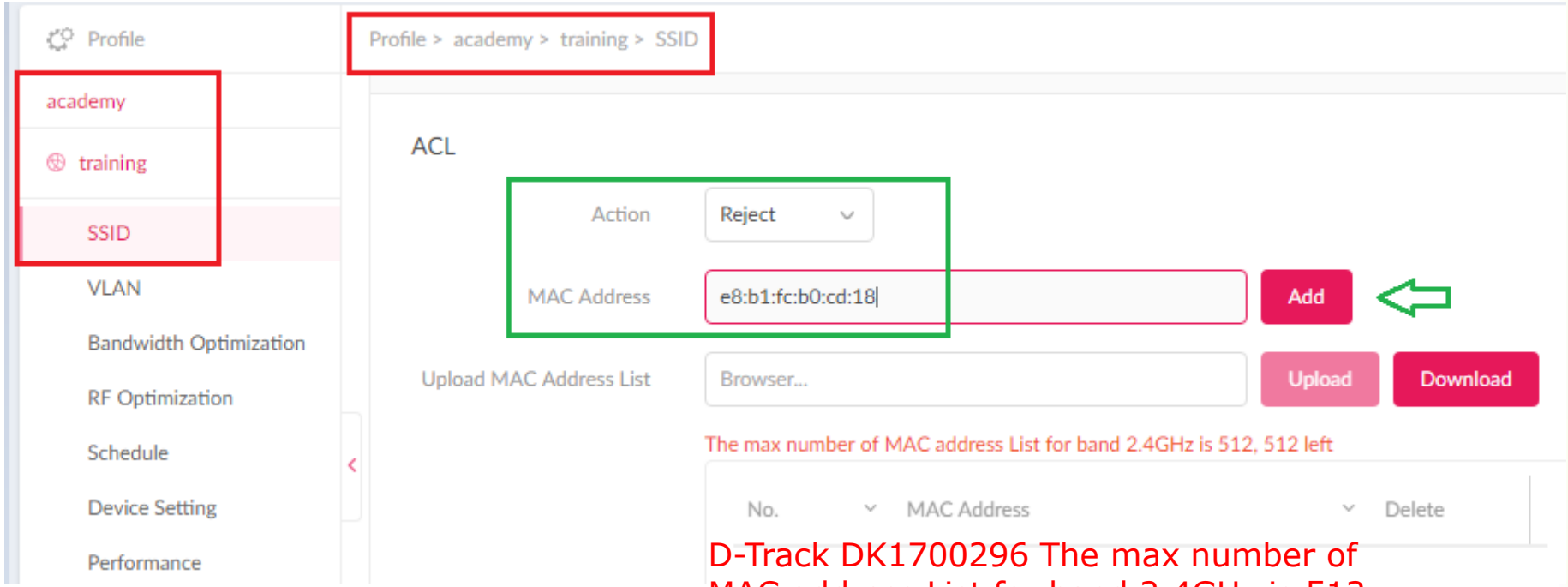
MAC Access Control List (ACL) (2/7)

- MAC Access Control List (ACL) scenario
- Browse the menu of “Profile > academy > training > SSID” click the Edit icon next within the column of “Action” in “dlinkacademy” SSID



MAC Access Control List (ACL) (3/7)

- MAC Access Control List (ACL) scenario
- Input the value of "e8:b1:fc:b0:cd:18" (colon sets) into the MAC Address column and click "Add" button

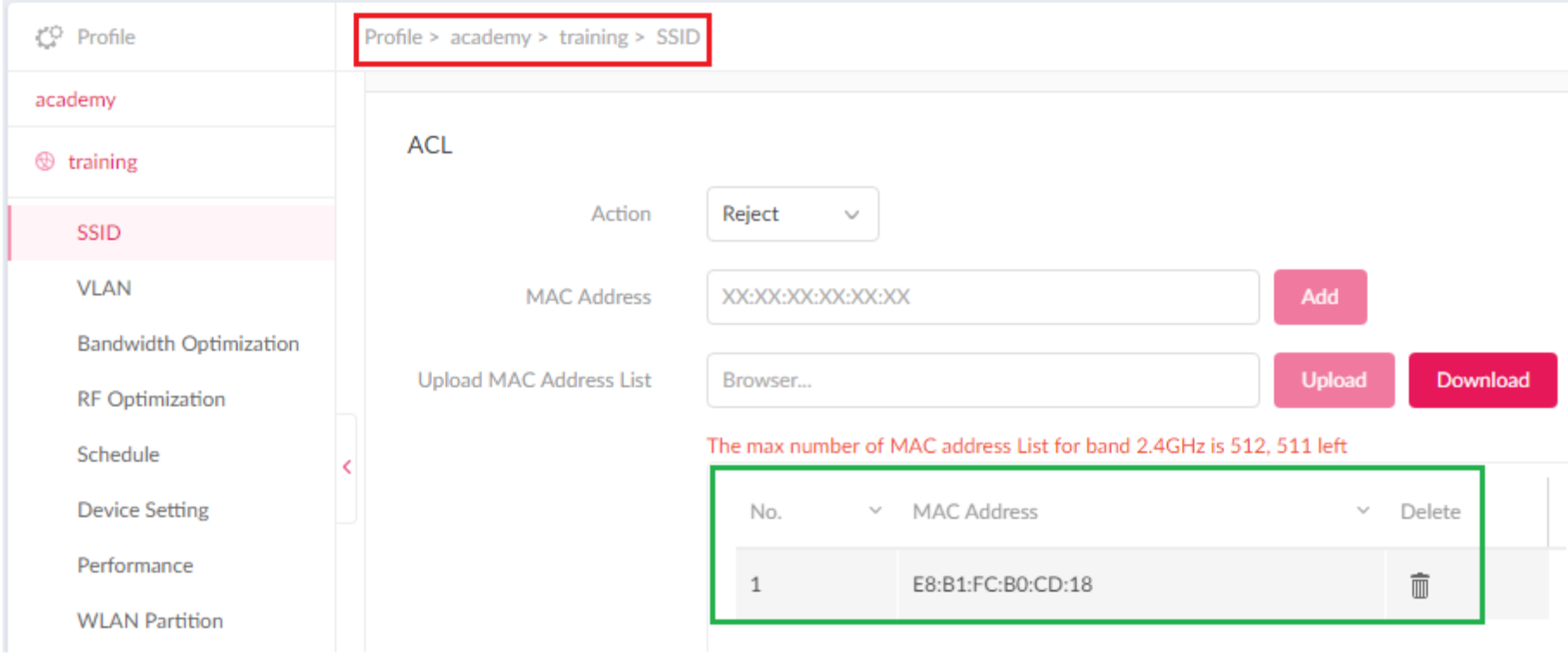


D-Track DK1700296 The max number of MAC address List for band 2.4GHz is 512

D-Track DK1500338 states the MAC filter file format accepted by CWM-100

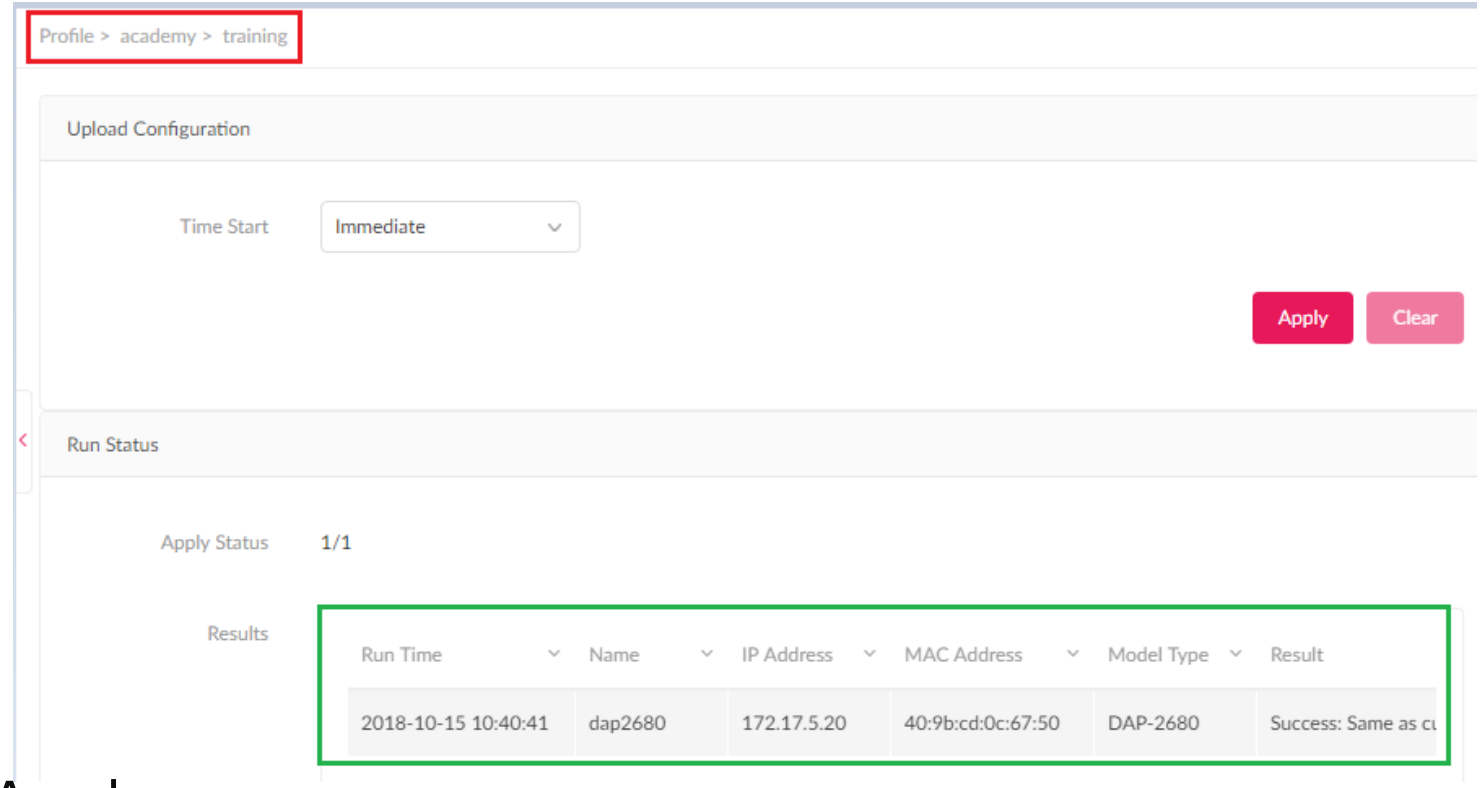
MAC Access Control List (ACL) (4/7)

- MAC Access Control List (ACL) scenario
- The "e8:b1:fc:b0:cd:18" should be in the MAC address list, as shown below



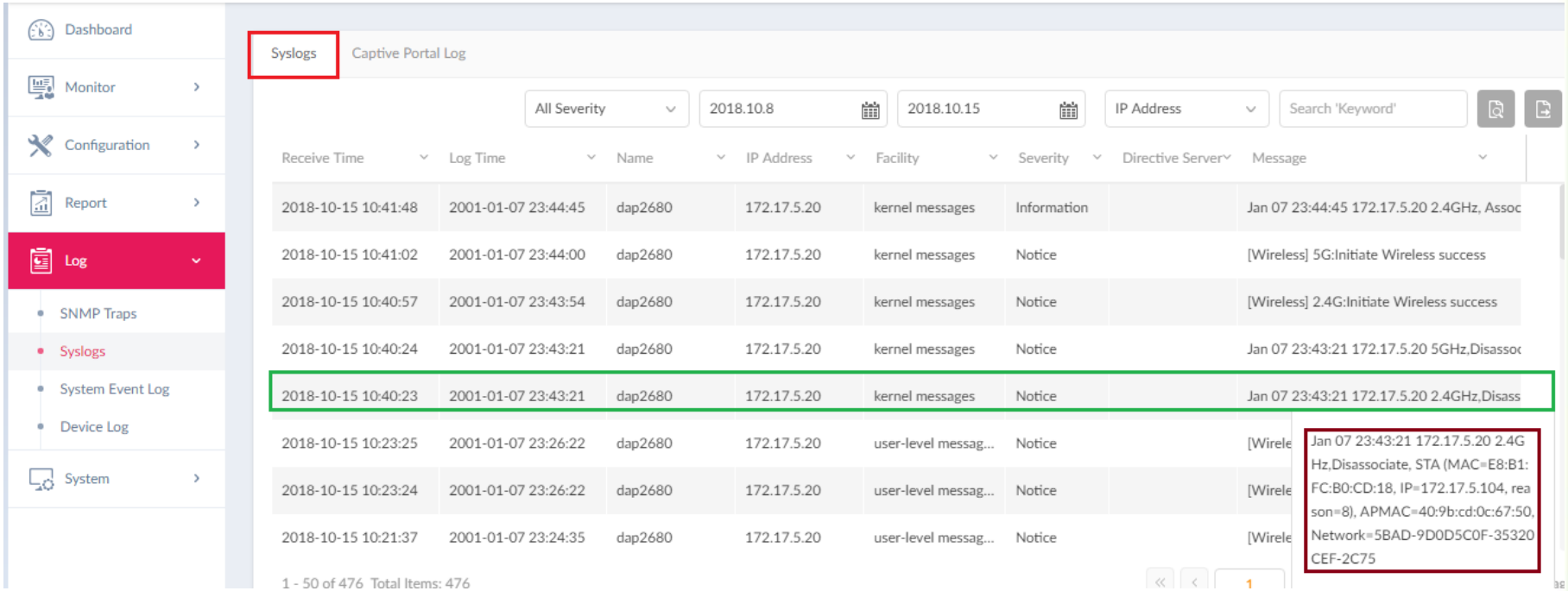
MAC Access Control List (ACL) (5/7)

- MAC Access Control List (ACL) scenario
- Below image screen shot shows configuration successfully being applied



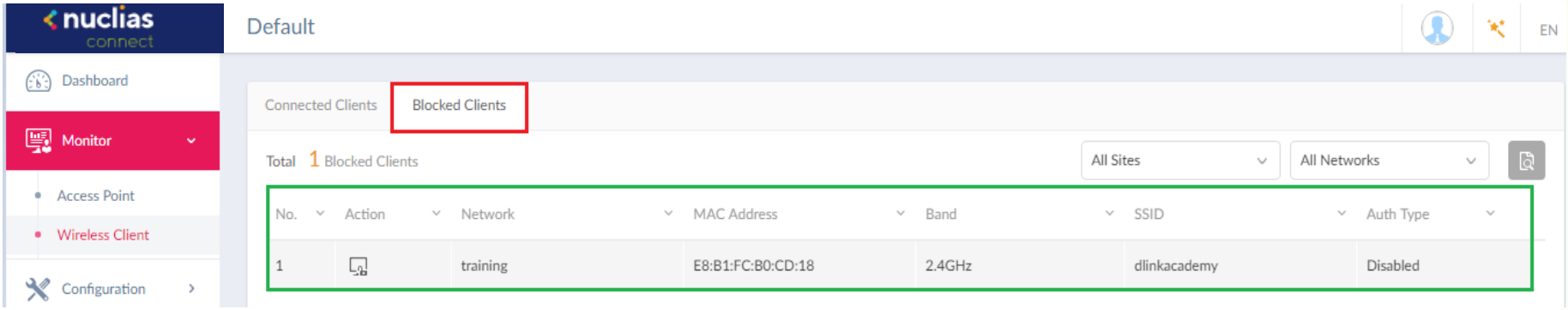
MAC Access Control List (ACL) (6/7)

- MAC Access Control List (ACL) scenario
- Below the menu "Log > Syslogs" we should be able to see the disassociation message regarding that specific wireless station



MAC Access Control List (ACL) (7/7)

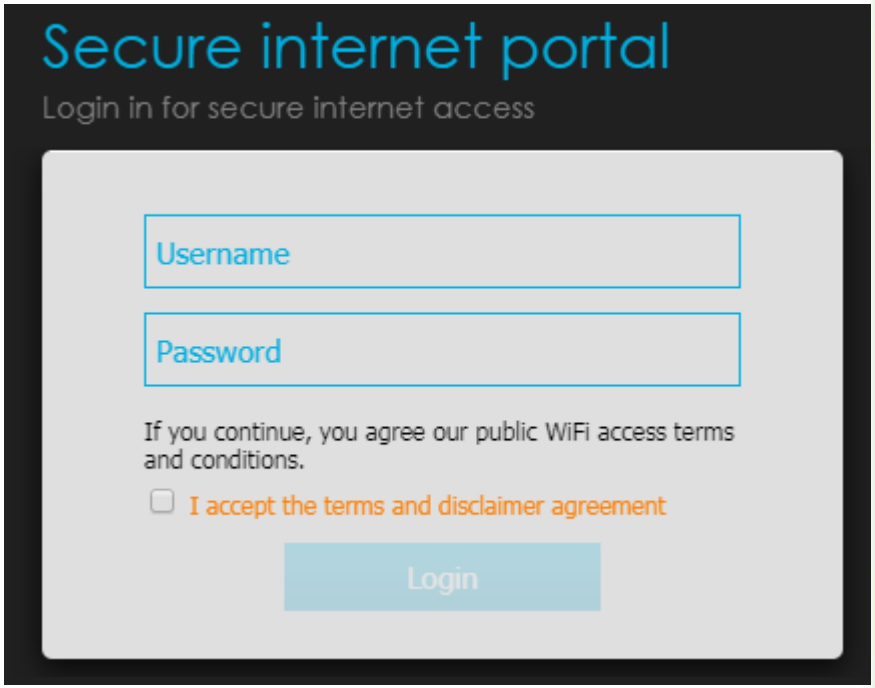
- MAC Access Control List (ACL) scenario
- The wireless station with MAC of "E8:B1:FC:B0:CD:18" is also shown in the "Blocked Client" list



- Note: When we are adding and/or removing AP devices on a frequent basis, what would be a better way to maintain long MAC address list?

Captive Portal

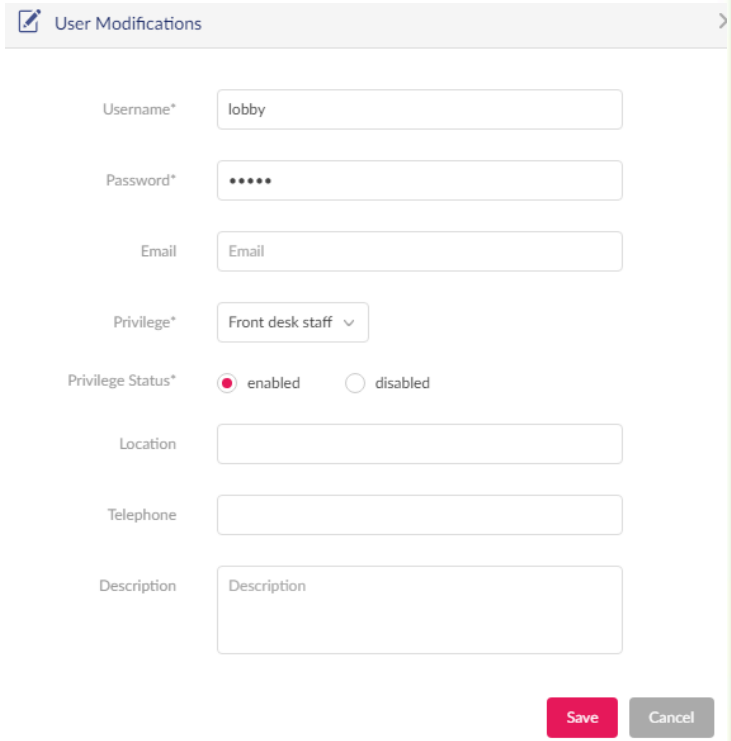
- A captive portal is a web page that is presented to newly connected users before these users are granted to connect to the network as well as access to permitted resources.
  - DK1600065, 256 DAPs for a single Captive Portal login
- A captive portal is also known as a "splash page" where the DNC default splash page is like diagram indicated in the right hand side.
- Passcode (Pre-created passcode or Buy passcode through PayPal)



Passcode User Authentication IS available in Primary SSID

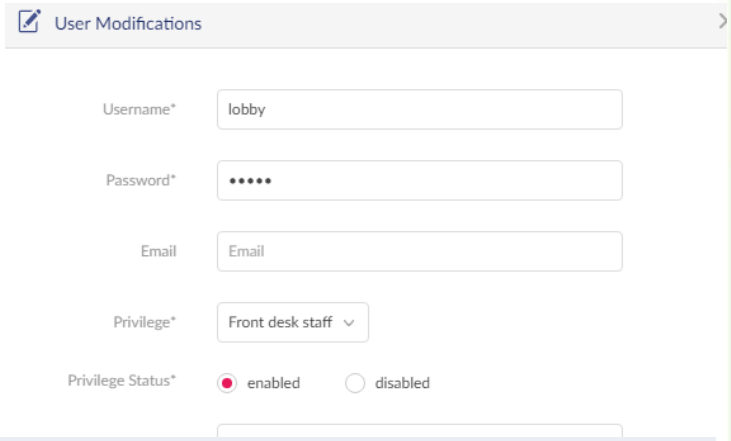
Passcode User Authentication Scenario (1/9)

- Passcode User Authentication scenario
- Users with “front desk user” privilege have the option to create passcode for users.
- Lab Scenario
  - Username: lobby (with “front desk staff” privilege)



Passcode User Authentication Scenario (1/9)

- Passcode User Authentication scenario
- Users with "front desk user" privilege have the option to create passcode for users.
- Lab Scenario
  - Username: lobby (with "front desk staff" privilege)



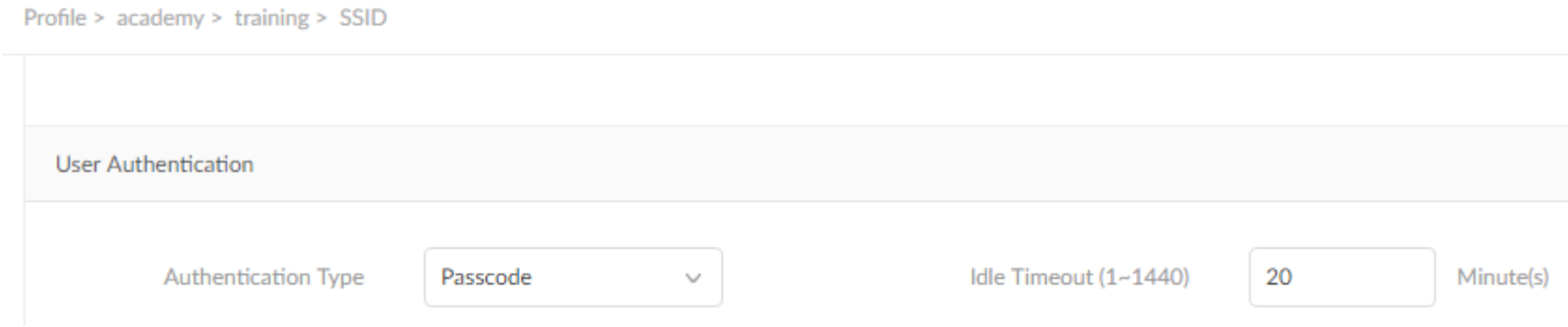
All Users Total Users 2 (1 1 0)

User Status | User Privilege

Username	Email	Login Status	Role	Privilege Status	Time of Creation	Last Login Time
admin			root admin	enabled	2018-09-28 11:09:29	2018-10-15 11:28:20
lobby			front desk user	enabled	2018-10-01 09:24:43	2018-10-15 11:56:16

Passcode User Authentication Scenario (2/9)

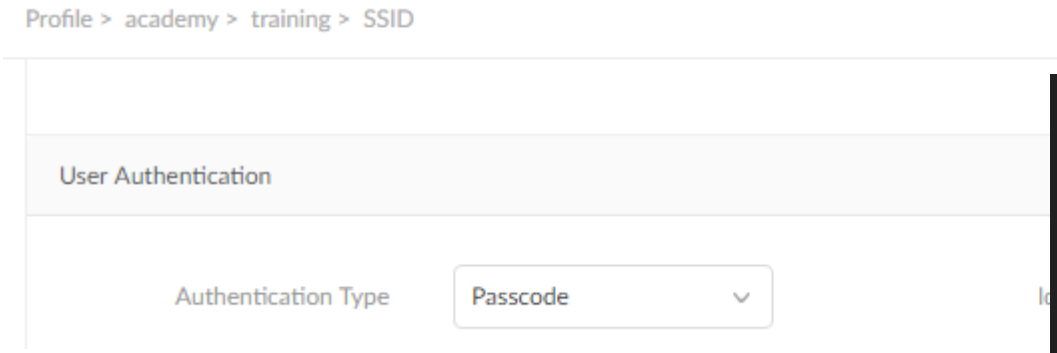
- Passcode User Authentication scenario
- Lab Scenario
  - SSID: dlinkacademy
  - Idle Timeout: 20 (minutes)
  - Splash Page Customization: default

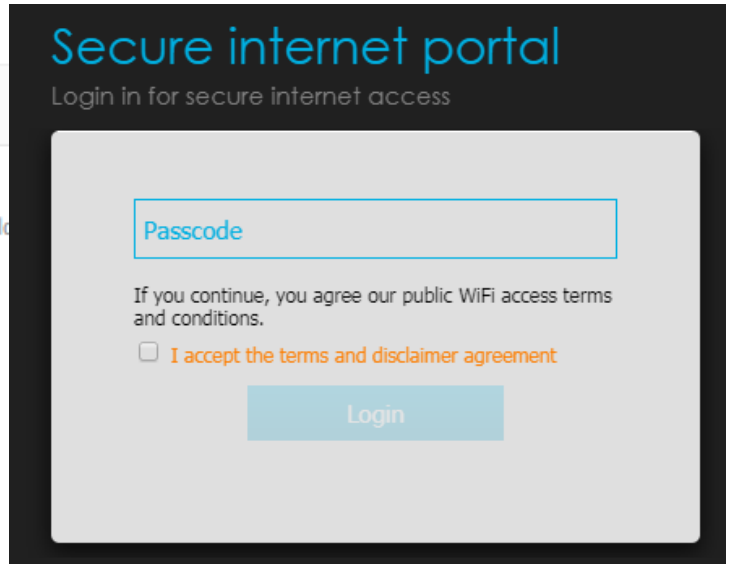


This Idle Timeout value is the maximum period after which a client is considered idle if there is no wireless traffic from the client.

Passcode User Authentication Scenario (3/9)

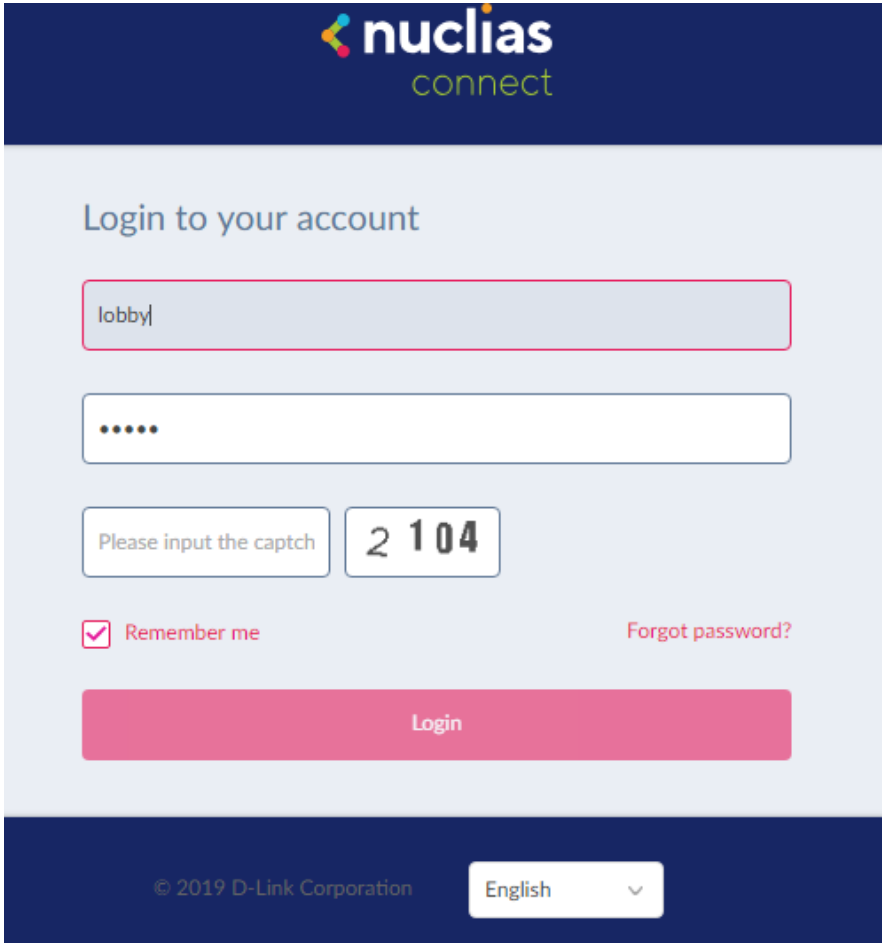
- Passcode User Authentication scenario
- Lab Scenario
  - SSID: dlinkacademy
  - Idle Timeout: 20 (minutes)
  - Splash Page Customization: default





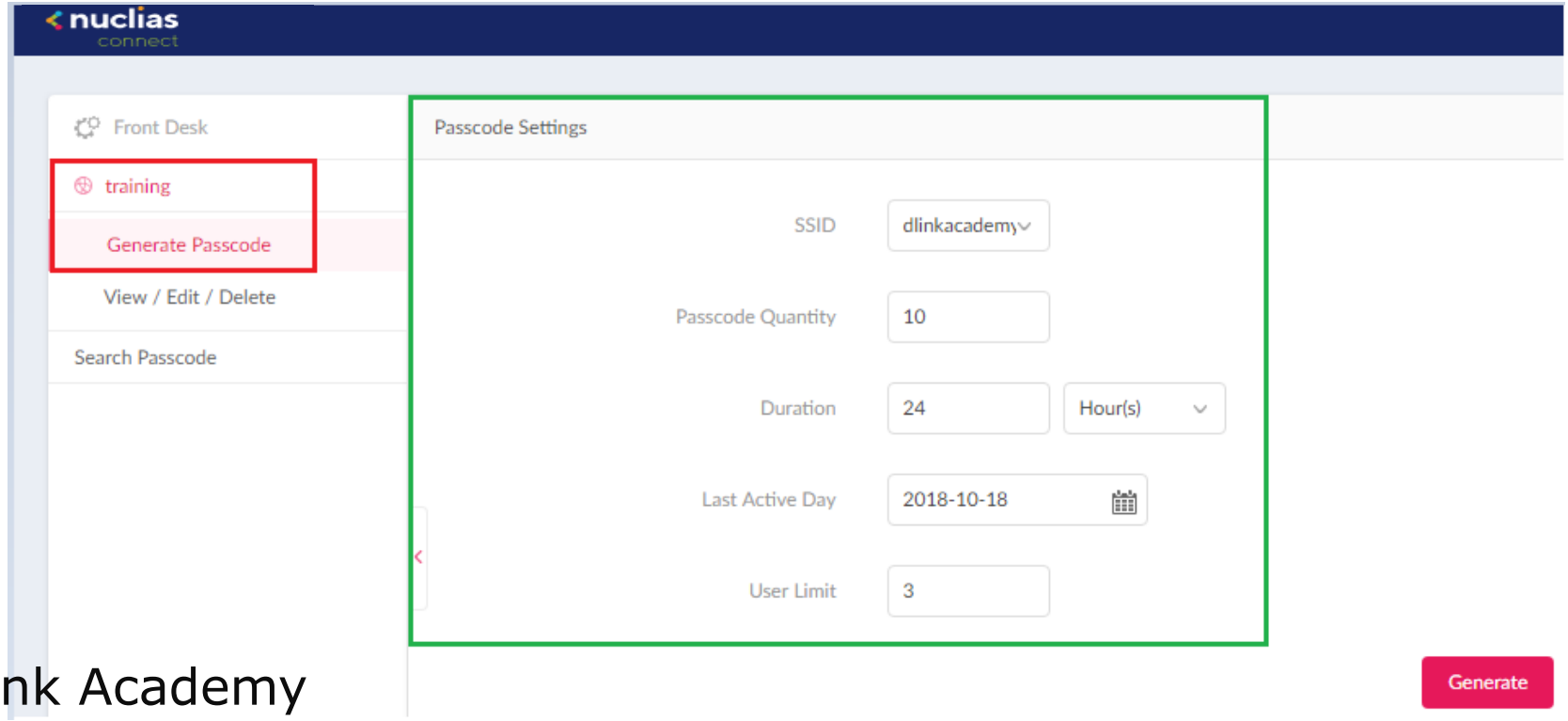
Passcode User Authentication Scenario (4/9)

- Passcode User Authentication scenario
- Lab Scenario
  - Login using “lobby” user account



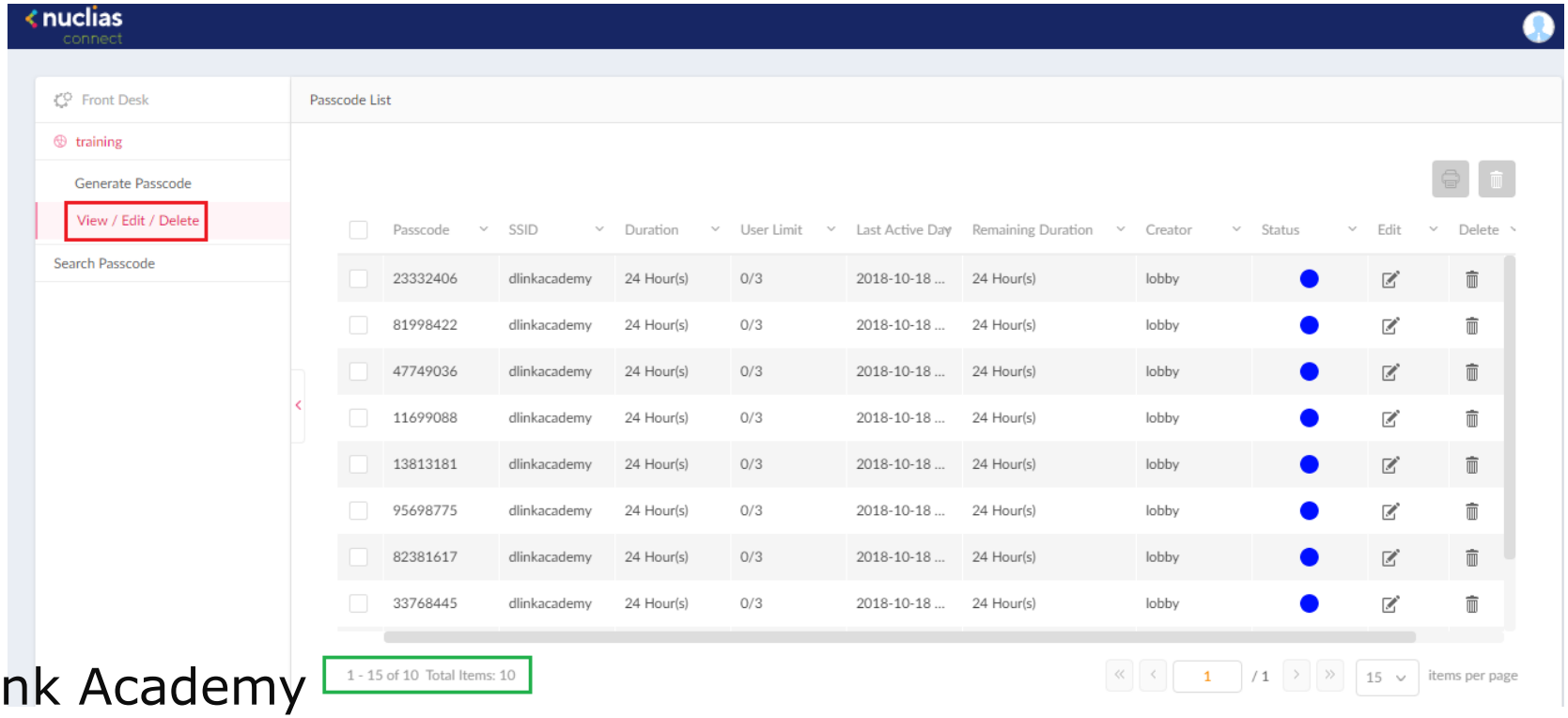
Passcode User Authentication Scenario (5/9)

- Passcode User Authentication scenario
- Lab Scenario
  - Passcode Generation, setup the parameters of “Passcode Quantity” “Duration” “User Limit (per code)”



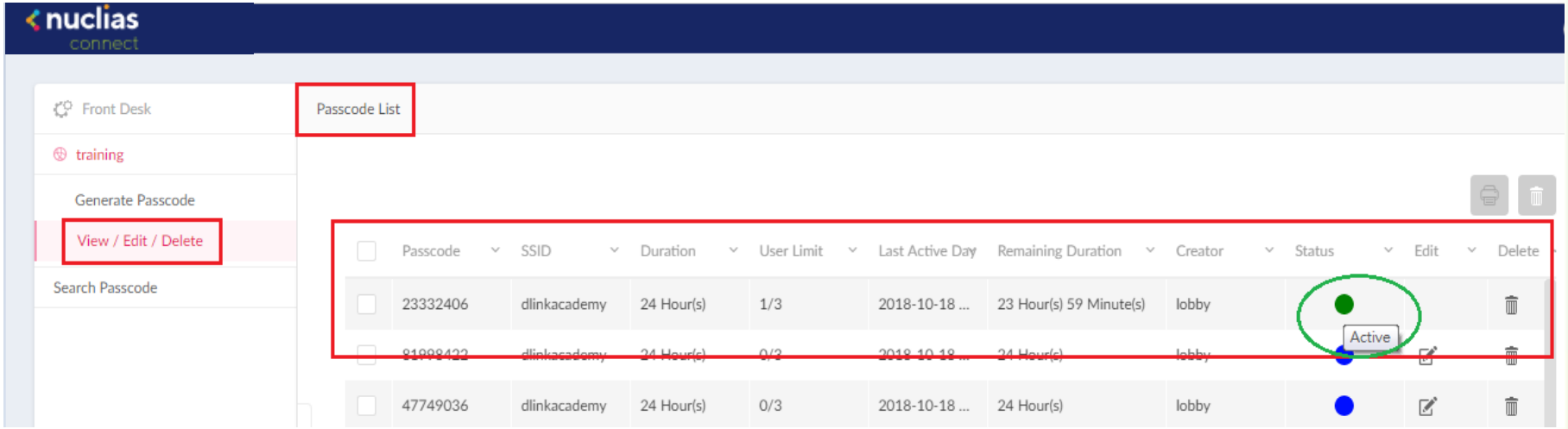
Passcode User Authentication Scenario (6/9)

- Passcode User Authentication scenario
- Lab Scenario
  - By clicking the "Generate" button, then, a list of passcode would be presented



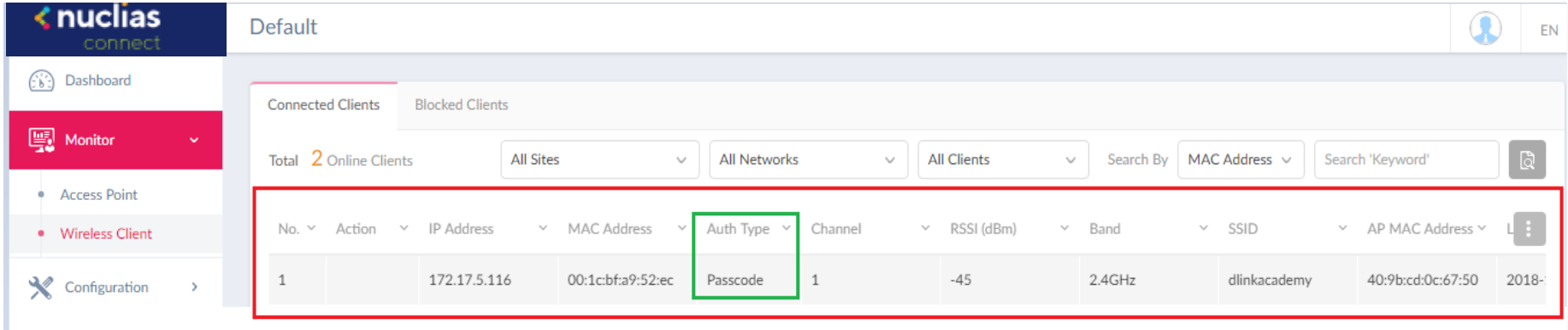
Passcode User Authentication Scenario (7/9)

- Passcode User Authentication scenario
- Lab Scenario
  - By sharing the passcode of "23332406" with user to login our network



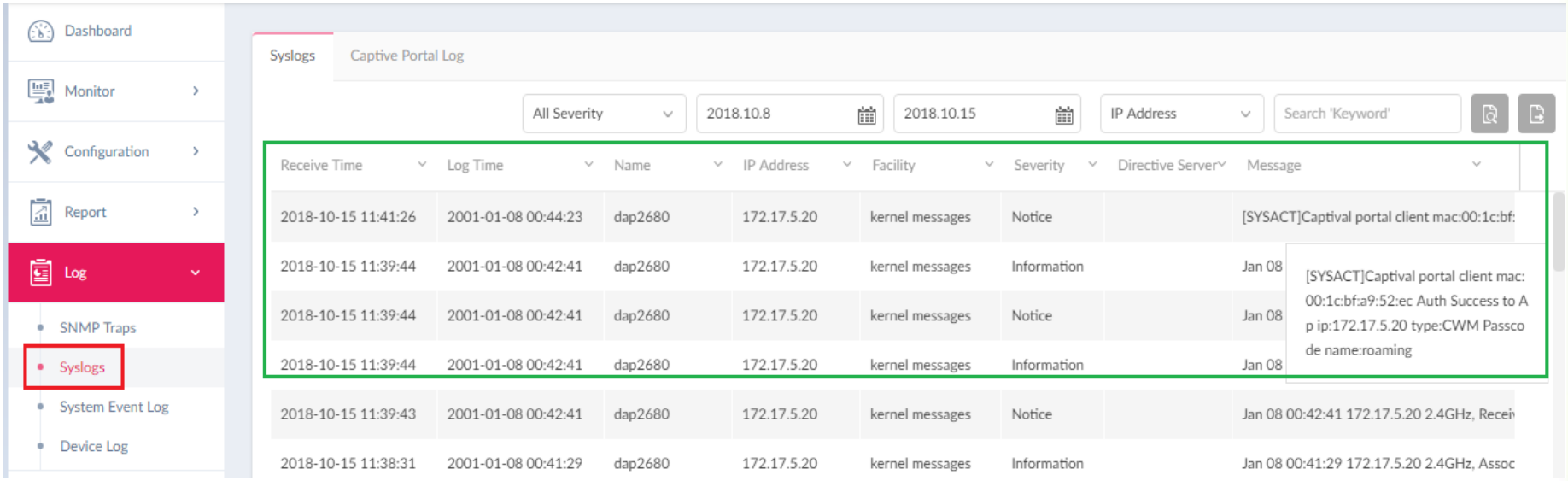
Passcode User Authentication Scenario (8/9)

- Passcode User Authentication scenario
- Lab Scenario
  - Return to DNC main console with Admin user account



Passcode User Authentication Scenario (9/9)

- Passcode User Authentication scenario
- Lab Scenario
  - DNC, Log > Syslog



SSID in collaboration with Passcode Configuration

- The same SSID index / name with passcode in two bands

Index	Band	SSID	Security	Access Control	User Authentication	Action
Primary	2.4GHz	dlink	WPA-Auto-Personal	Disabled	Passcode	
Primary	5GHz	dlink	WPA-Auto-Personal	Disabled	Passcode	

- Different SSID index / name with passcode in two bands

Profile > djntest > test > SSID

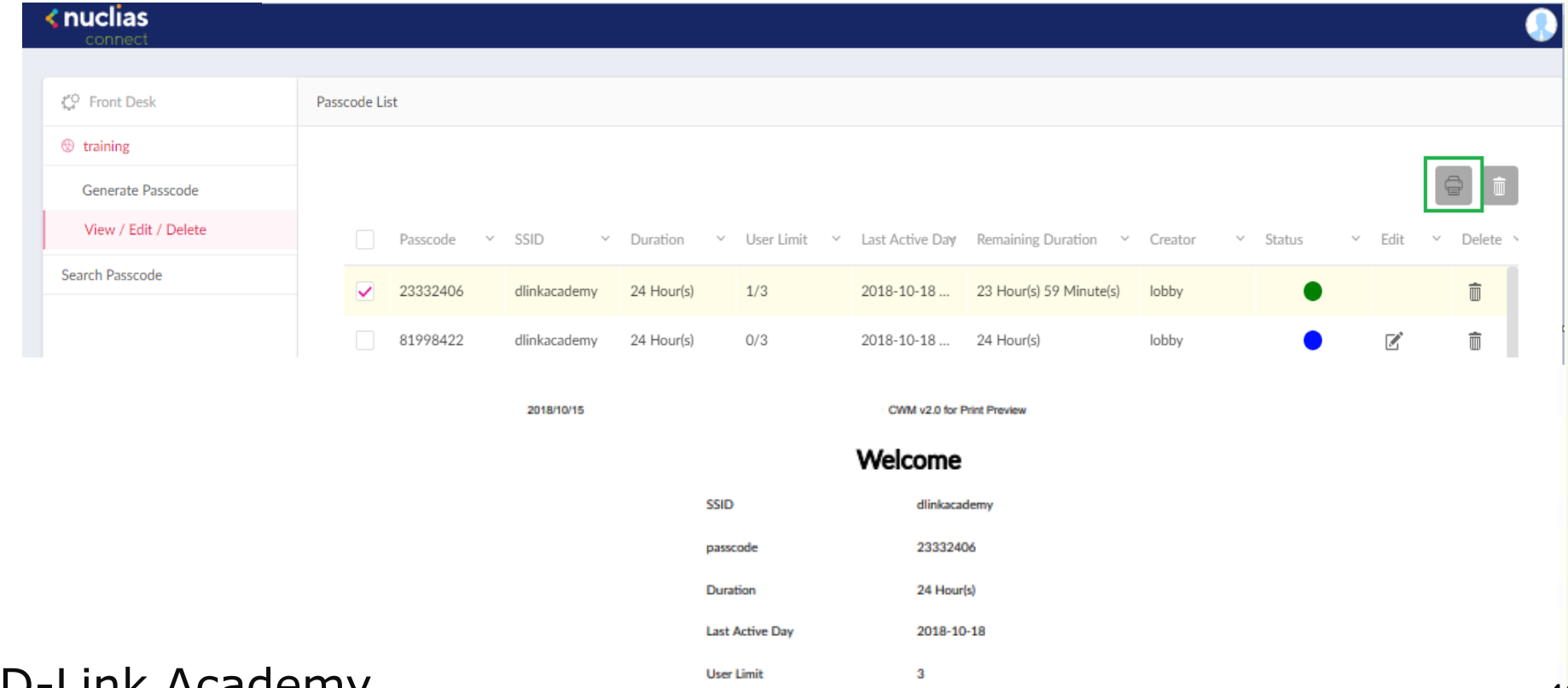
Index	Band	SSID	Security	Access Control	User Authentication	Action
Primary	2.4GHz	dlink00	WPA-Auto-Personal	Disabled	Disabled	
Primary	5GHz	dlink	WPA-Auto-Personal	Disabled	Passcode	
SSID 1	2.4GHz	SSID1	Open System	Disabled	Passcode	

Passcode User Authentication

- Passcode User Authentication discussion
- What if we would like to print out passcode, how does the print-put look like?

Passcode User Authentication

- Passcode User Authentication discussion
- What if we would like to print out passcode, how does the print-put look like?

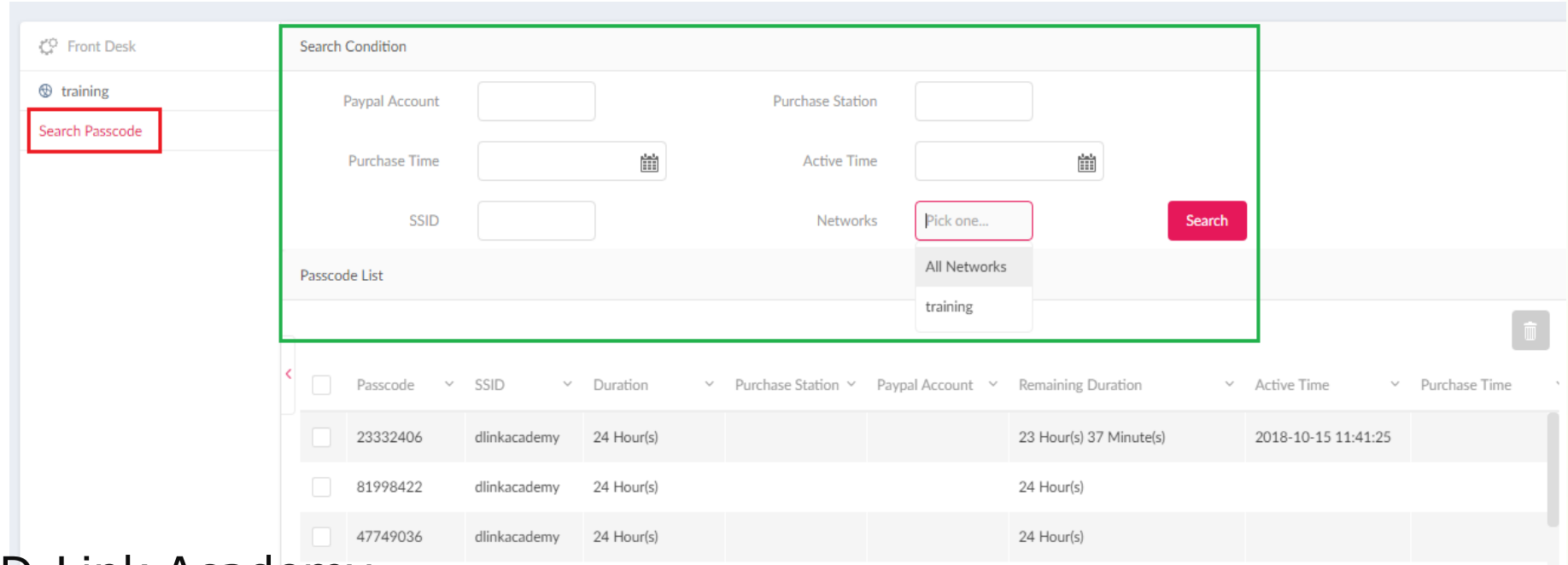


Passcode User Authentication Discussion

- Passcode User Authentication discussion
- Passcode Search Criteria, what type of searching criteria is available in Passcode search function?

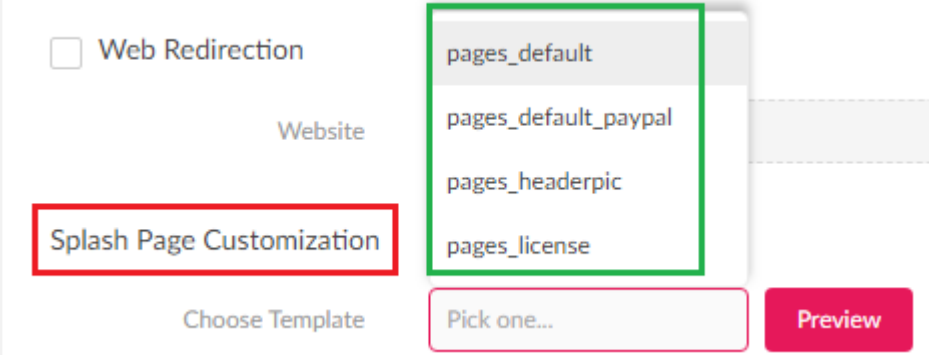
Passcode User Authentication Discussion

- Passcode User Authentication discussion
- Passcode Search Criteria, what type of searching criteria is available in Passcode search function?
  - Paypal Account, Purchase Station, Purchase Time, Active Time, SSID, and Networks



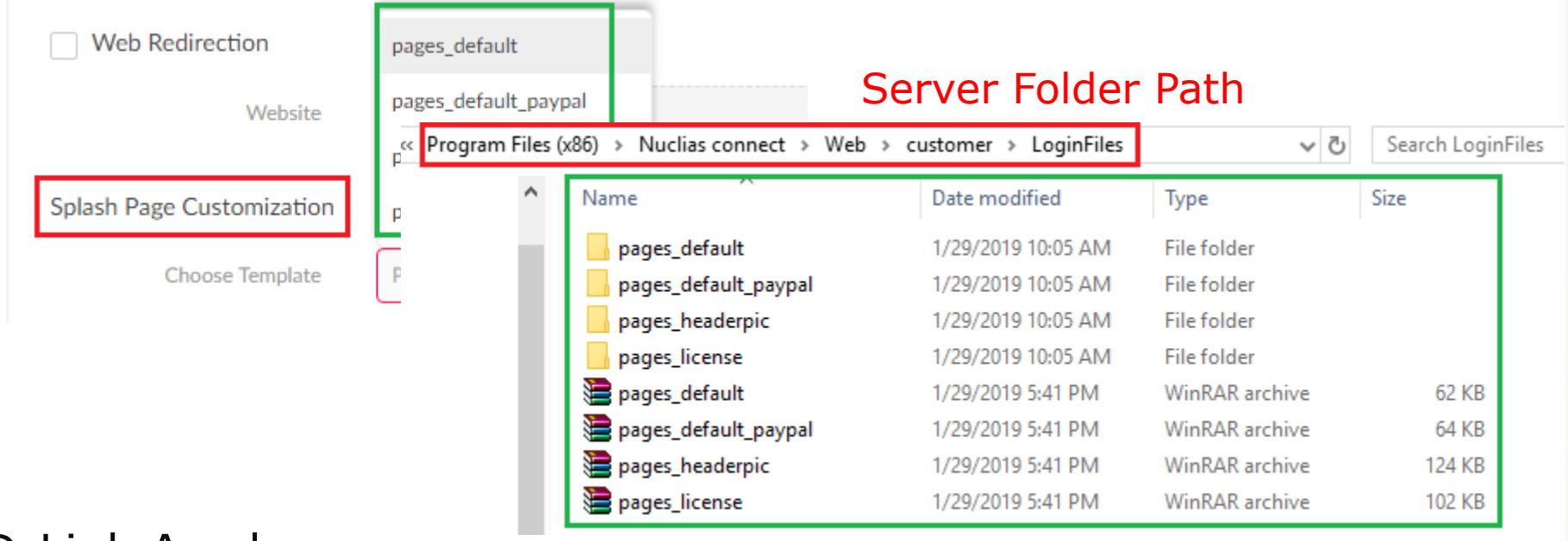
Captive Portal Login Page Customization

- Nuclias Connect offers a flexible way to customize the look and feel of the captive portal login page.
- There are four options being provided: pages_default, pages_default_paypal, pages_headerpic, and pages_license.
- Each one of them brings an unique web page source file.



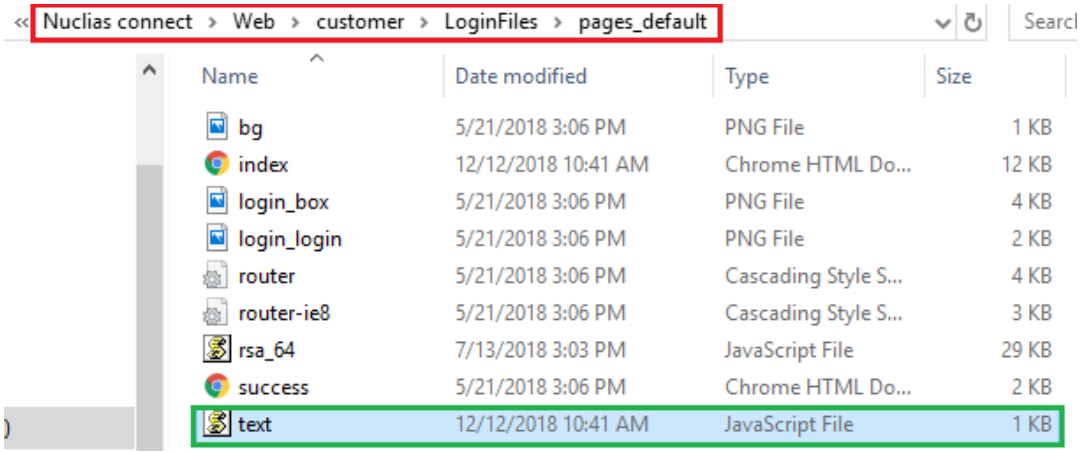
Captive Portal Login Page Customization

- Nuclias Connect offers a flexible way to customize the look and feel of the captive portal login page.
- There are four options being provided: pages_default, pages_default_paypal, pages_headerpic, and pages_license.
- Each one of them brings an unique web page source file.



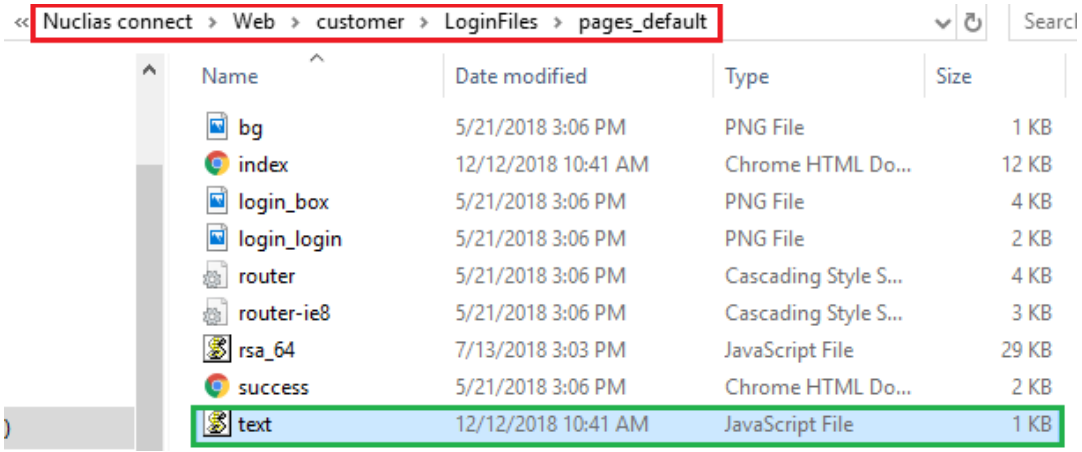
Captive Portal Login Page Customization

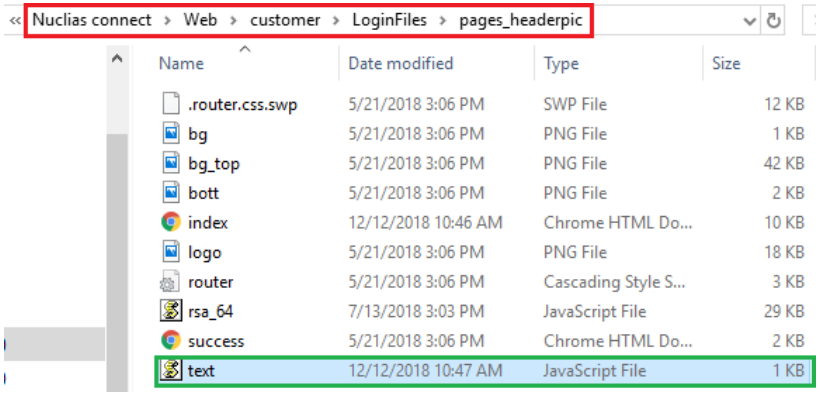
- The “text.js” file within each of the option is used in parameter modifications.



Captive Portal Login Page Customization

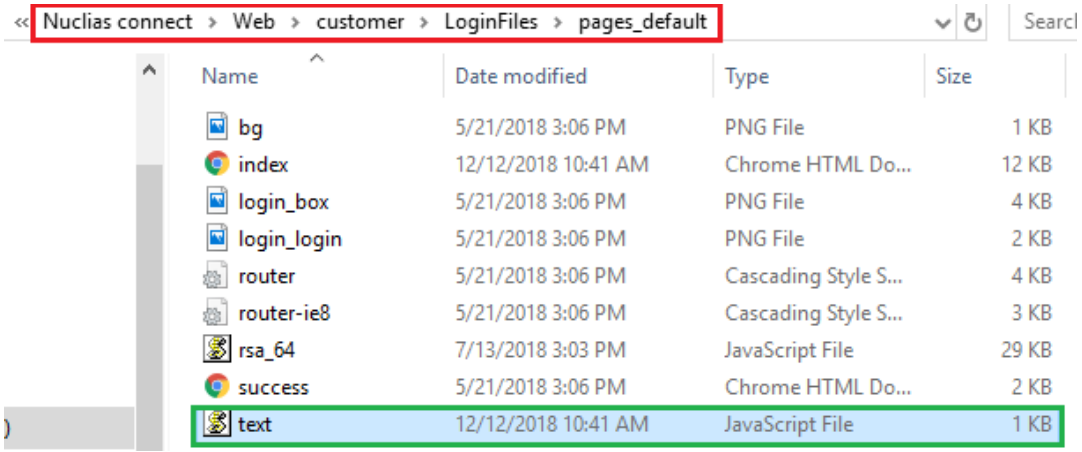
- The "text.js" file within each of the option is used in parameter modifications.

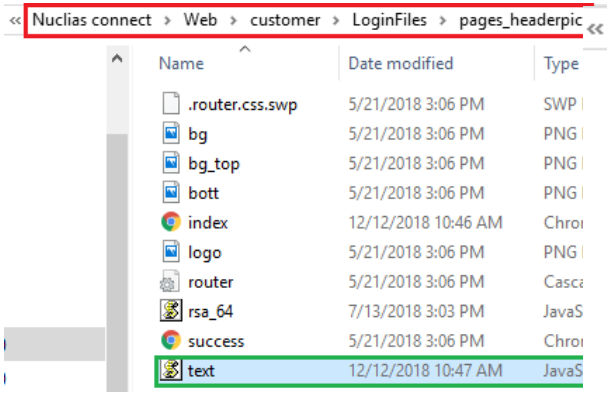


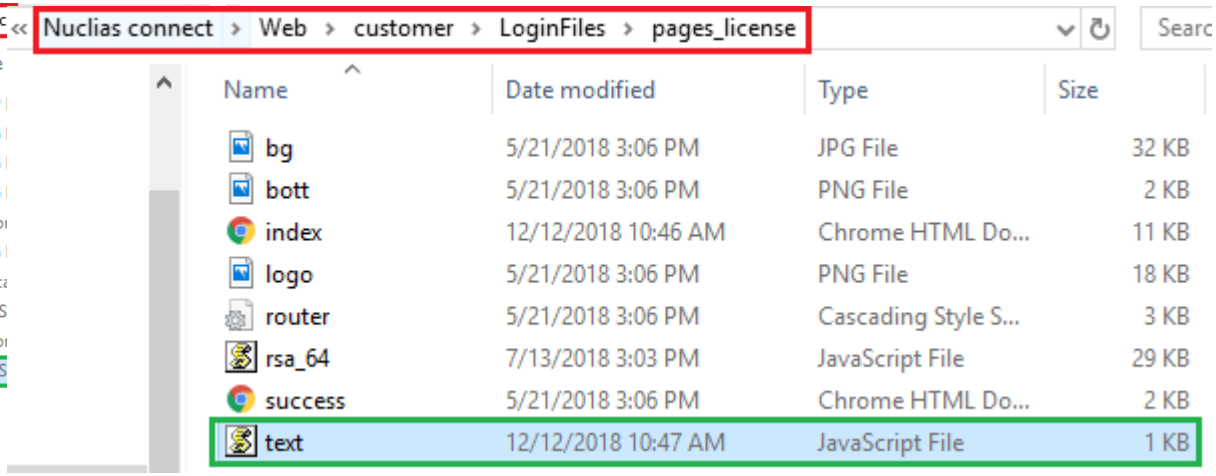


Captive Portal Login Page Customization

- The "text.js" file within each of the option is used in parameter modifications.







Captive Portal Login Page Customization

- The “text.js” file shall include, but not limited to, the following statements
  - var main_title="Secure internet portal";
  - var sub_title="Login in for secure internet access";
  - var username="Username";
  - var password="Password";
  - var login="Login";
  - var license_notice="Logging in indicates you have read and accepted the license";
  - var license_link="Use Policy";
  - var license_content="If you continue, you agree our public WiFi access terms and conditions.";
  - var fail="Captive Portal Login Fail";
  - var passcode="Passcode";
  - var success="Success";
  - var process="Processing...";

Captive Portal Login Page Customization (1/5)

- Page header modification lab
- The default page header image file (file name: bg_top) under the "pages_headerpic" folder is similar as below diagram

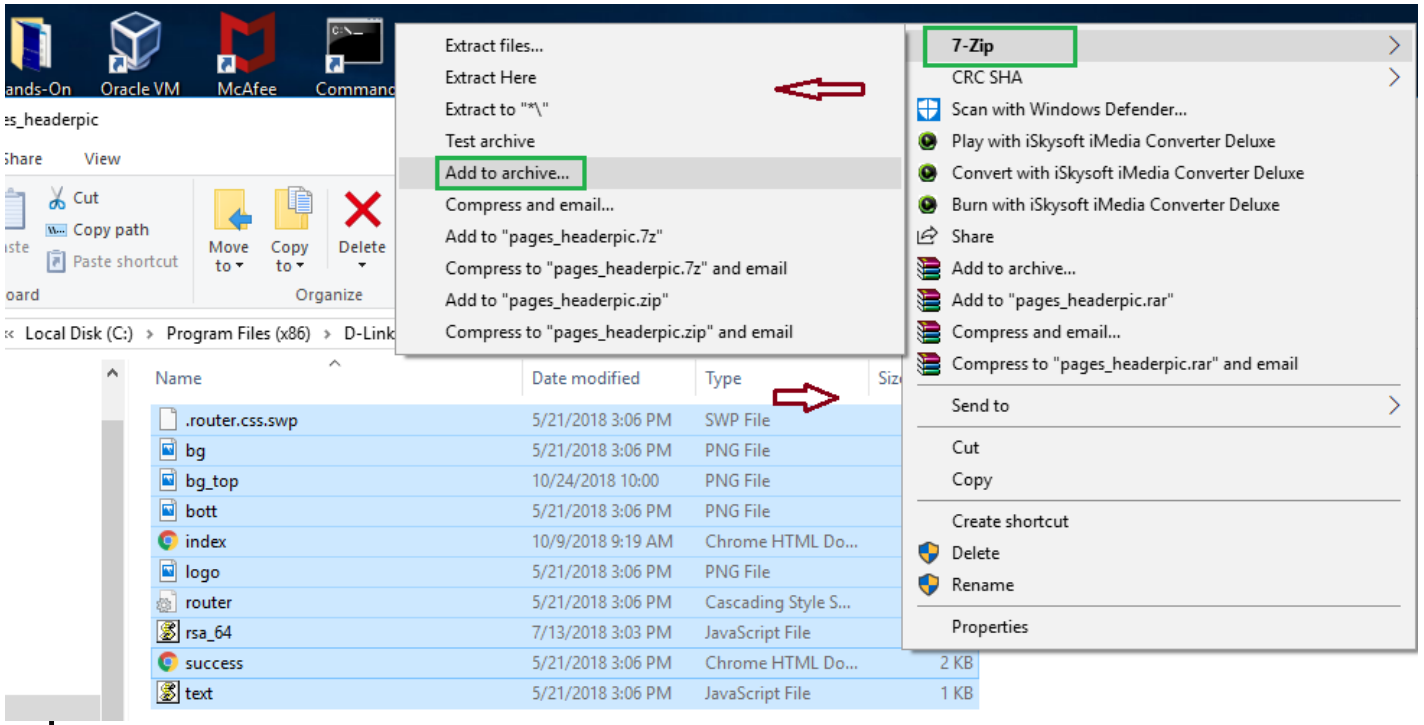


- We are going to use another image file and put the same file name over there

- D-Track DK1500473 is another documented case study for reference.

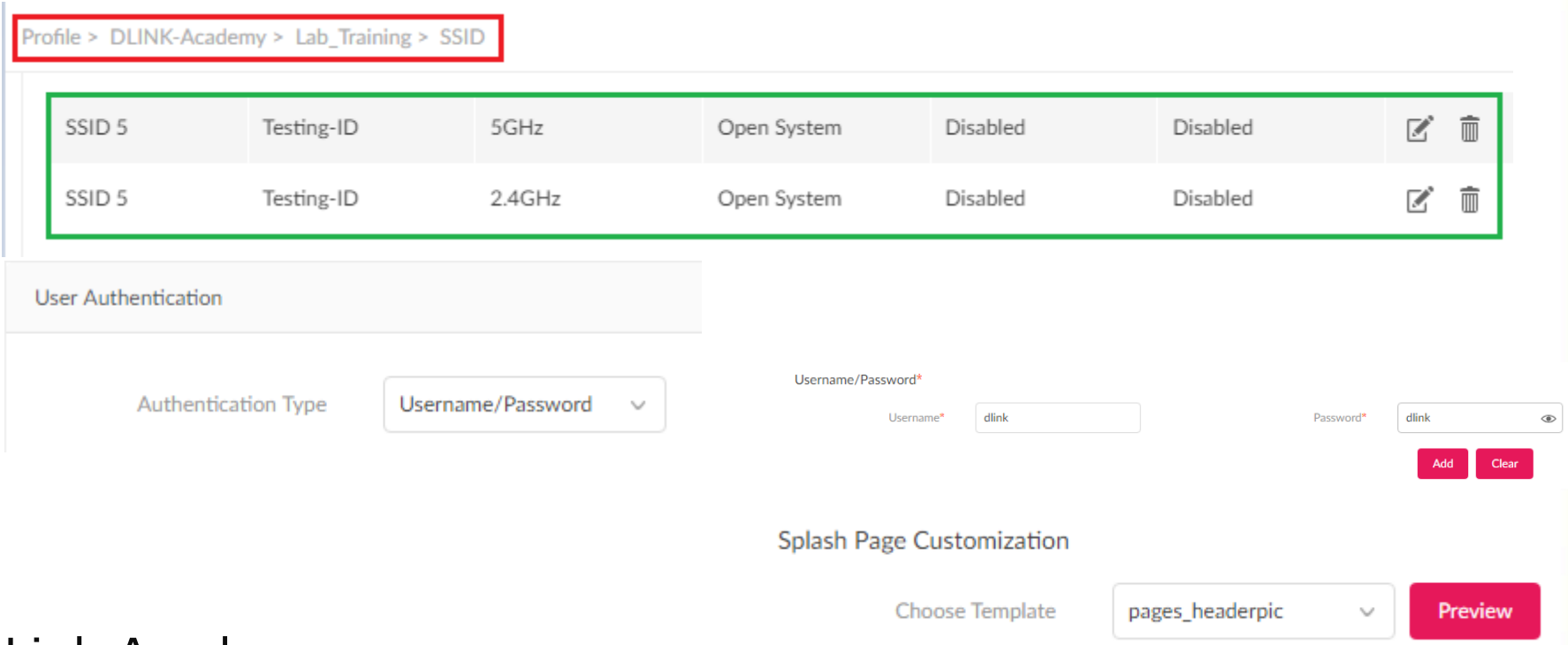
Captive Portal Login Page Customization (2/5)

- Page header modification lab
- After you are done editing the extracted source files, you would need to compress the files back to a ".tar" file before uploading it back the DNC WEB GUI.



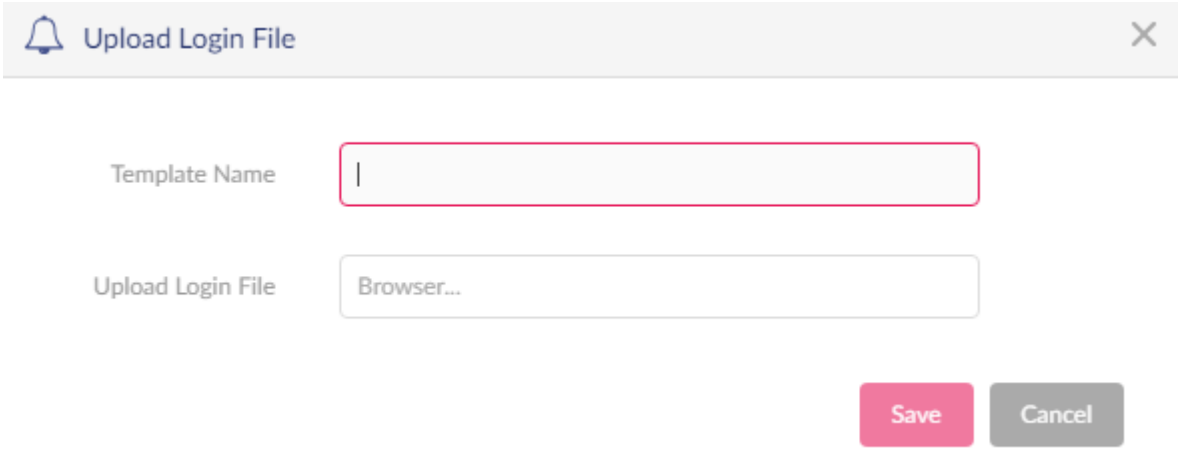
Captive Portal Login Page Customization (3/5)

- Page header modification lab
- We are going to apply just configured Splash Page Customization, with the User Authentication of "username/password" (dlink/dlink) under the SSID of "Testing-ID".



Captive Portal Login Page Customization (4/5)

- Page header modification lab
- We also need to upload the login file (make sure no file name conflict).



Captive Portal Login Page Customization (5/5)

- Page header modification lab
- We also need to upload the login file (make sure no file name conflict).



Captive Portal Login Page Customization Discussion

- D-Track DK1600281 documents configuration guide on "Customized captive portal login page to for multiple SSID"
  - The default template can't be removed or deleted.
  - A single captive portal login page can be shared by all of the SSIDs.
  - Identical captive portal login page for individual SSID is also feasible, where maximum 400KB file size is the limitation (file compression technique is a durable approach).

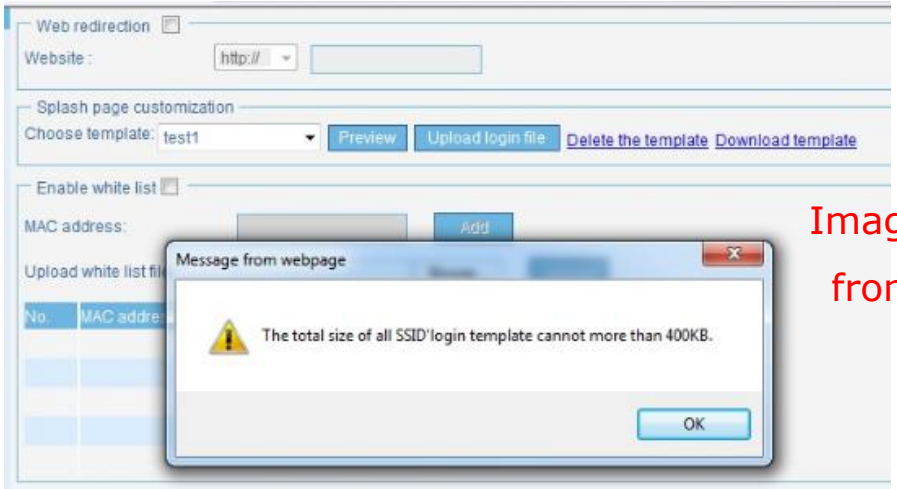
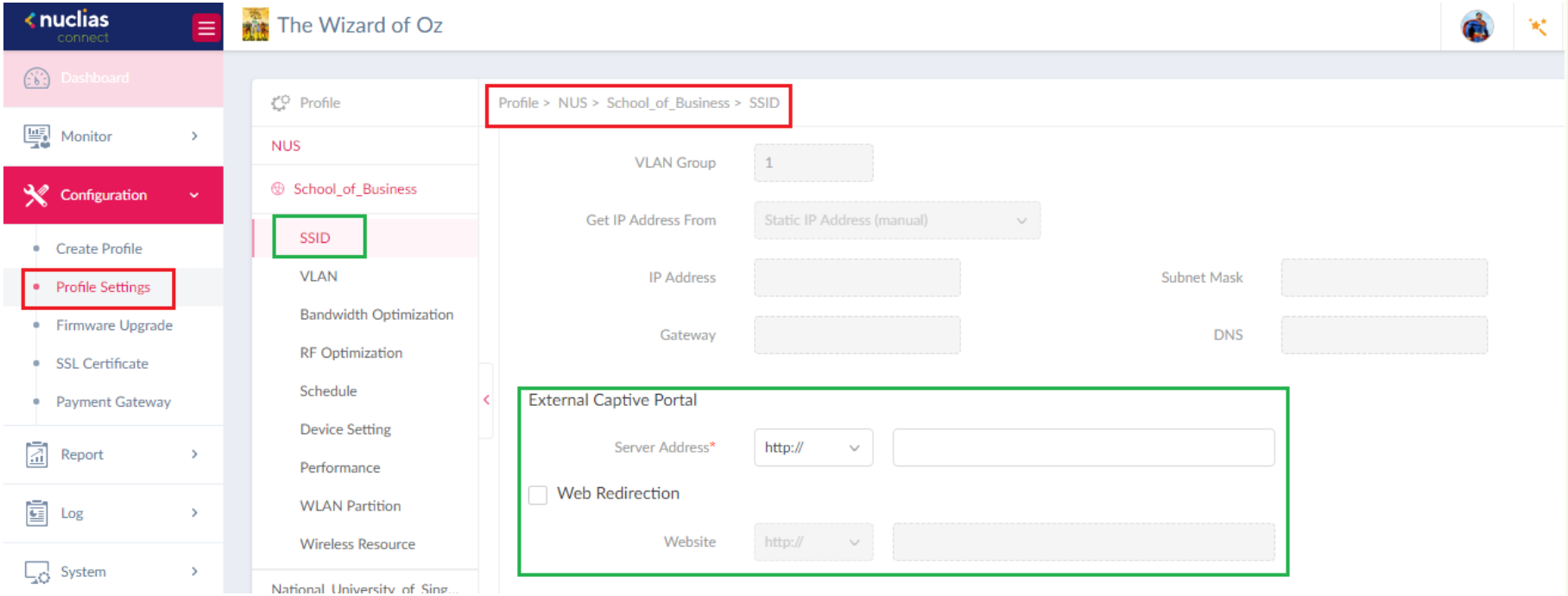


Image screenshot from CWM 1.03

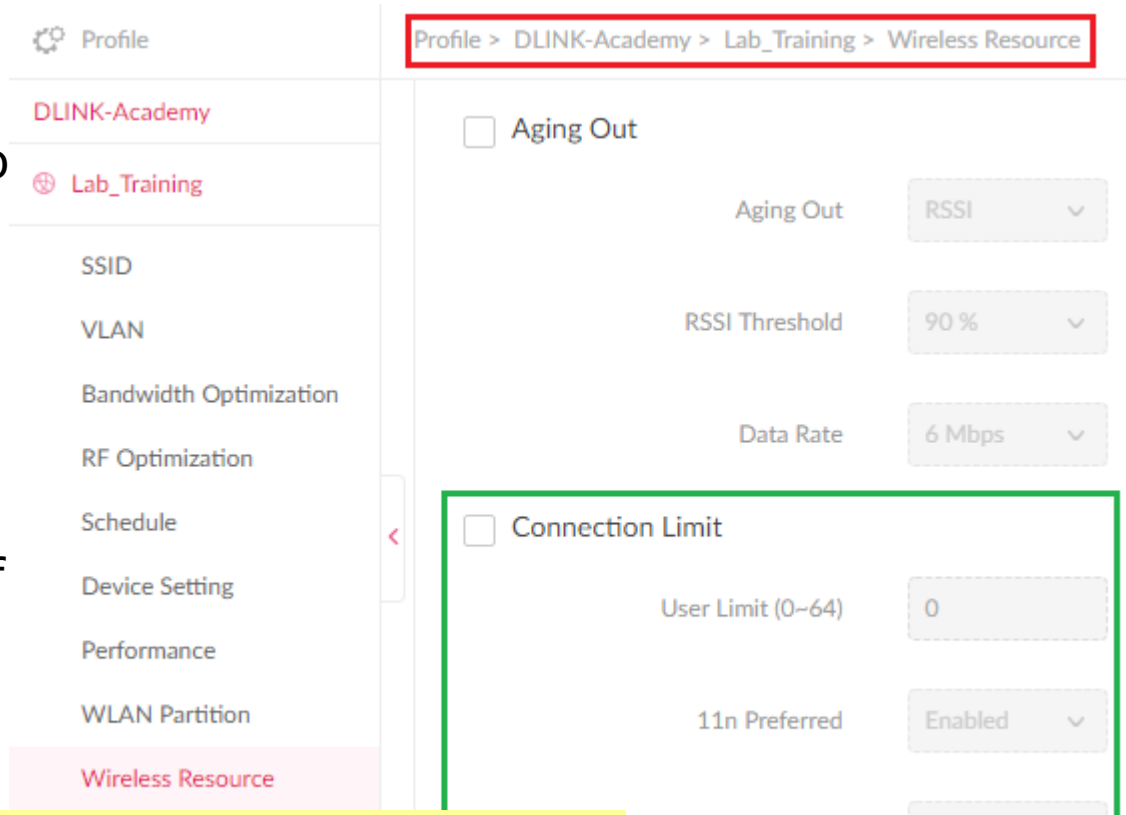
External Captive Portal

- External Captive Portal
- The External Captive Portal configuration is on SSID/Profile Settings page under the Configure tab.



Wireless Network Connections Limitations

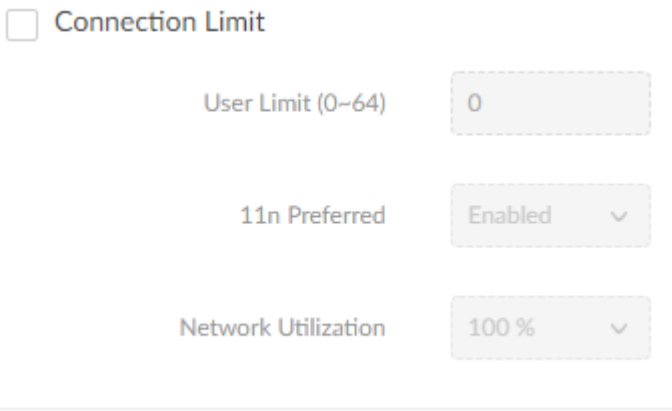
- Wireless Connection Limit is a mechanism to ensure the number of users are allowed to connect as well as the network utilization being permitted.
- Wireless Connection Limit setting is viewable from "Wireless Resource" of Profile Settings page under the Configure tab.



Should fewer devices are allowed to connect to a specific network, co-channel interface would be reduced and capacity would be enlarged.

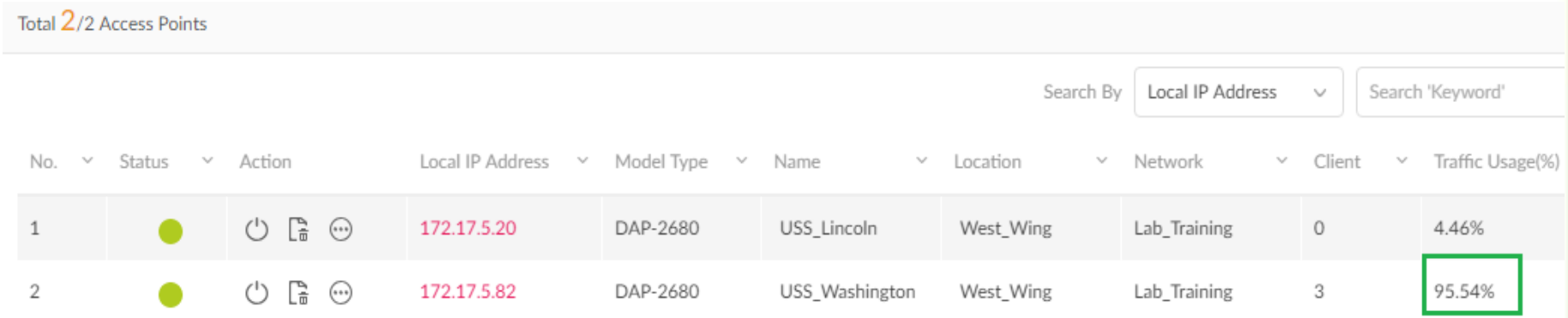
Wireless Network Connections Limitations

- Configuration parameters within "Wireless Connection Limit" session (D-Track DK1500843)
  - User Limit (0~64), it (User Limit) is set put limitations on the number of client connecting to a specific AP.
  - 11n Preferred, it (11n Preferred) gives preference to 802.11n users and denies non-802.11n clients access to the AP when the maximum limit is reached.
  - The already connected non-802.11n client will be dispatched.



Wireless Connection Limit Lab Practice I (1/3)

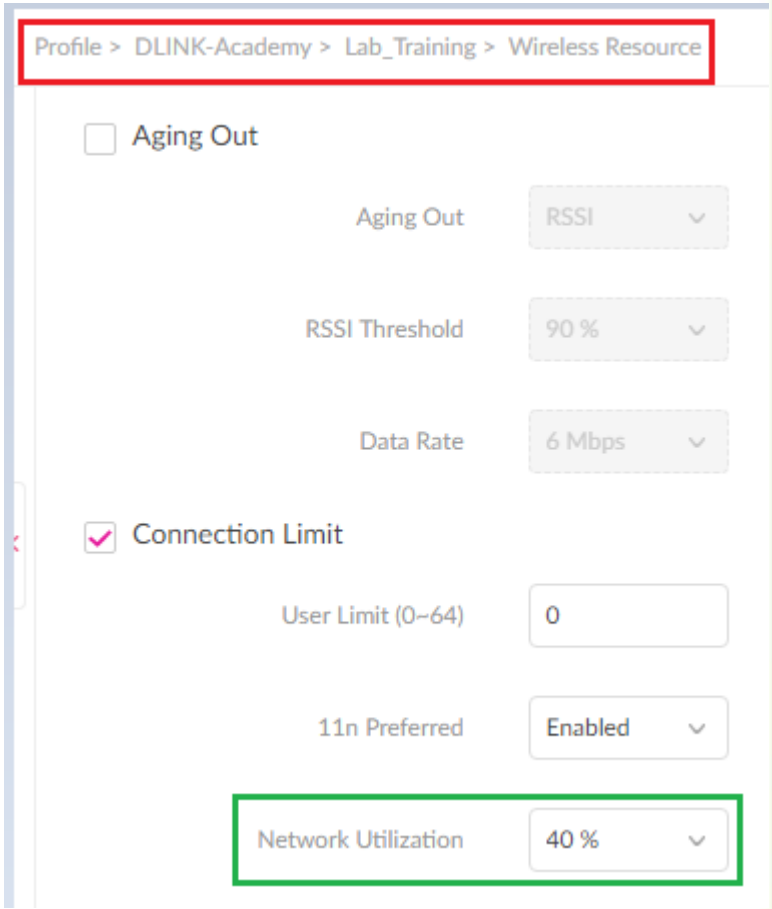
- Wireless Connection Limit Lab Practice
- Heavy network usage in our network



- We would like to rely on Wireless Connection Limit settings to see whether we can make any difference.

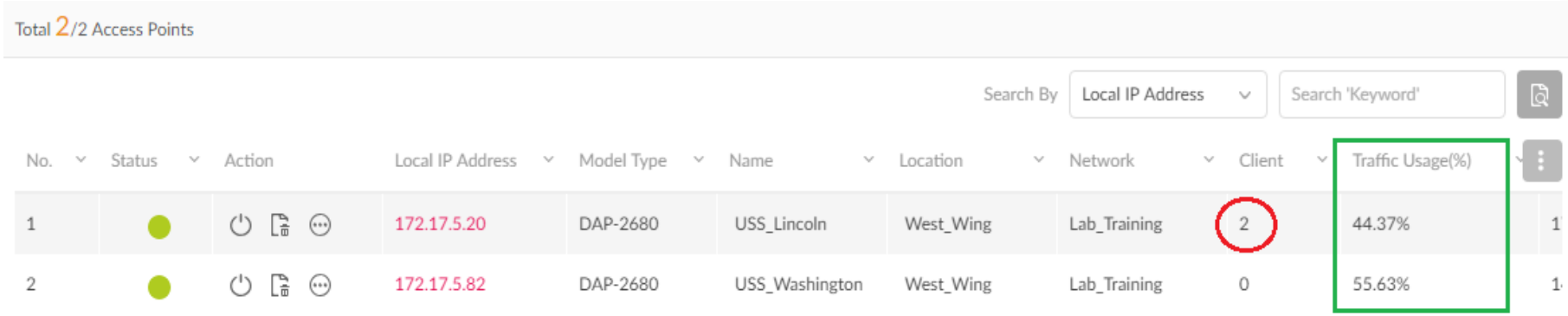
Wireless Connection Limit Lab Practice I (2/3)

- Wireless Connection Limit Lab Practice
- Make the "Network Utilization" to 40%, in stead of unlimited use



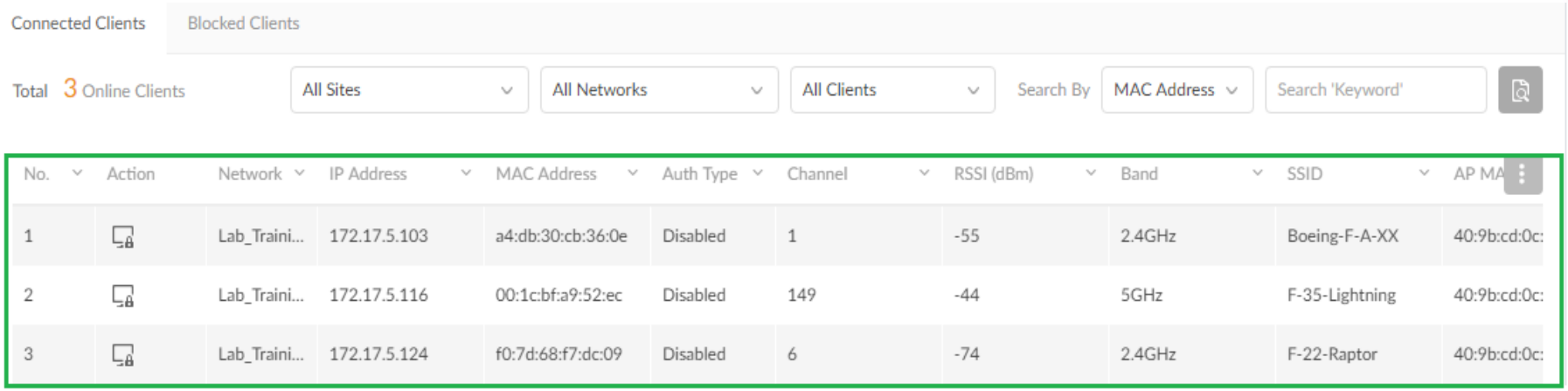
Wireless Connection Limit Lab Practice I (3/3)

- Wireless Connection Limit Lab Practice
- We have observed the network utilization where it shows
  - Only two wireless clients are able to connect to network
  - Network utilization is around 45%



Wireless Connection Limit Lab Practice II (1/4)

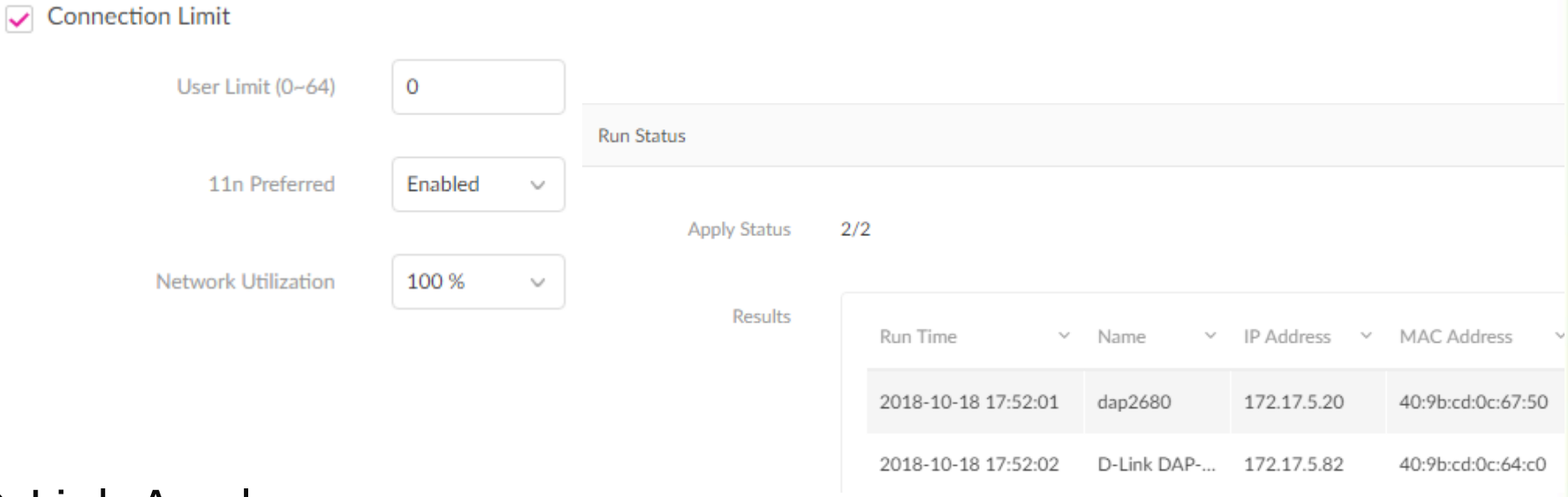
- Access Control, Connection Limit on Wireless Network Connection
- The range is from 0 to 64
- Wireless Network Connections Limitations Lab practice
- There are three wireless stations within the profile of “DLINK-Academy”



No.	Action	Network	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MA
1		Lab_Traini...	172.17.5.103	a4:db:30:cb:36:0e	Disabled	1	-55	2.4GHz	Boeing-F-A-XX	40:9b:cd:0c:
2		Lab_Traini...	172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-44	5GHz	F-35-Lightning	40:9b:cd:0c:
3		Lab_Traini...	172.17.5.124	f0:7d:68:f7:dc:09	Disabled	6	-74	2.4GHz	F-22-Raptor	40:9b:cd:0c:

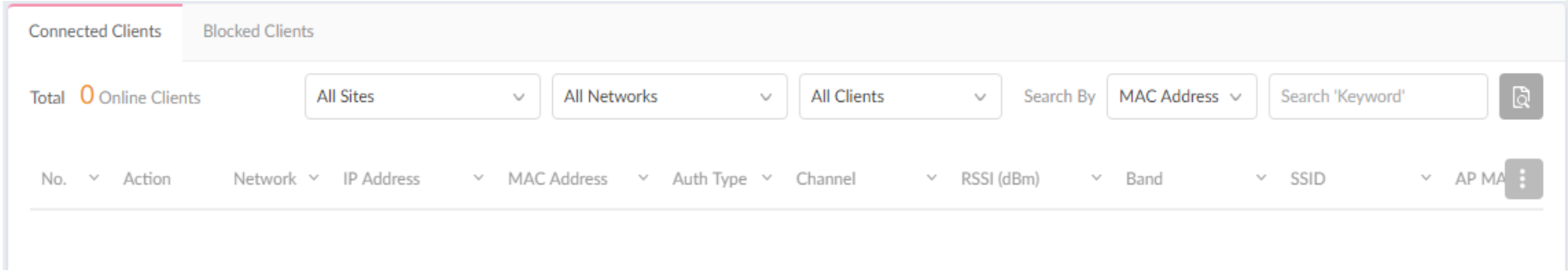
Wireless Connection Limit Lab Practice II (2/4)

- Wireless Network Connections Limitations Lab practice
- A sudden urgent request from high level executives asks to put temporary shutdown in our wireless topology
- Menu: Profile > DLINK-Academy > Lab_Training > Wireless Resource
- Click "Connection Limit" and put to 0 (zero)



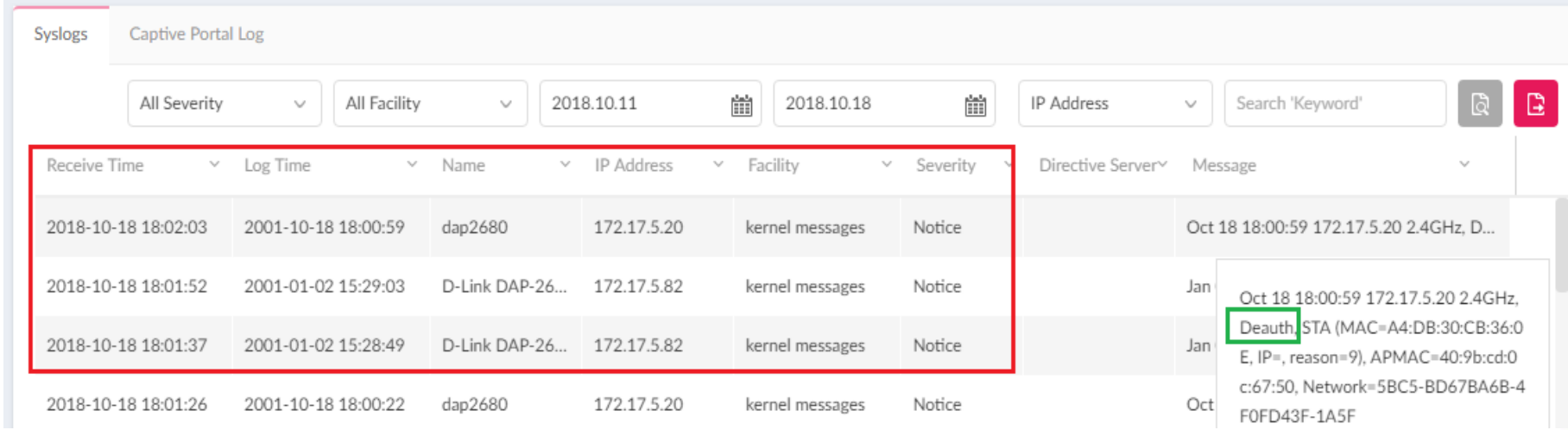
Wireless Connection Limit Lab Practice II (3/4)

- Wireless Network Connections Limitations Lab practice
- Wireless client connection status
  - There is no connection under the “connection clients” in the menu: Monitor > Wireless Client



Wireless Connection Limit Lab Practice II (4/4)

- Wireless Network Connections Limitations Lab practice
- Wireless Client Deauth message(s) via the Menu: Log > Syslog



Reason 9: Station requesting (re)association is not authenticated with responding station



RSSI Threshold

- RSSI Threshold
- Received signal strength indicator (RSSI) is a measurement of the power present in a received radio signal.
- RSSI Threshold allows the AP to kick a wireless client once this wireless client goes below the set RSSI (Received Signal Strength Indicator) value.

RSSI Threshold

- D-Track DK1500843, the attached chart should address dBm value comparing with ACL RSSI Threshold (in percentage).



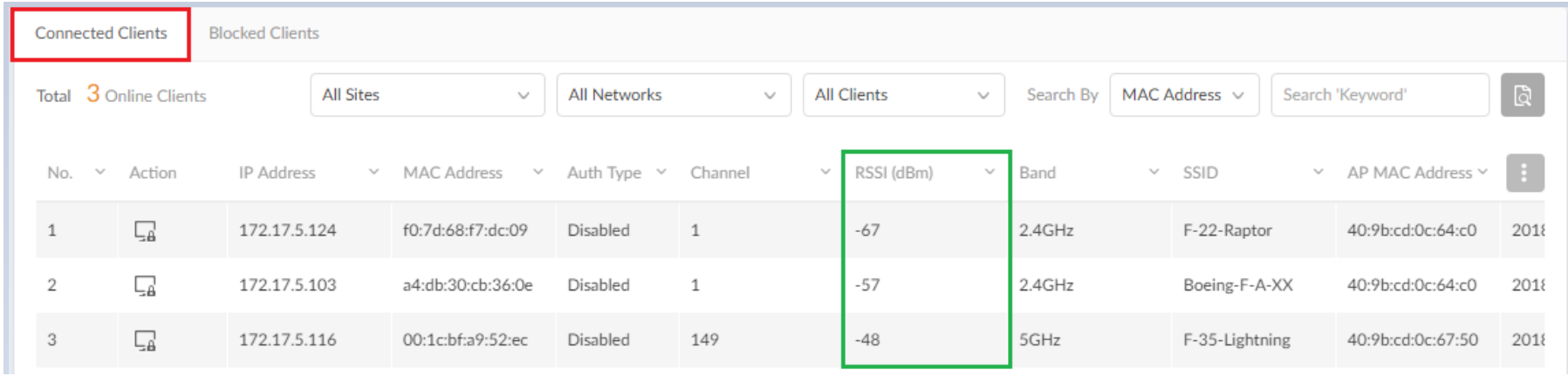

```
from percent to dbm######
  0%  -> 0
  2%  -> 1
  4%  -> 1
  6%  -> 4
  8%  -> 4
 10%  -> 6
 12%  -> 6
 14%  -> 6
 16%  -> 6
 18%  -> 6
 20%  -> 9
 22%  -> 9
 24%  -> 9
 26%  -> 9
 28%  -> 9
 30%  -> 12
 32%  -> 12
 34%  -> 12
 36%  -> 12
 38%  -> 12
 40%  -> 15
 42%  -> 15
 44%  -> 15
 46%  -> 15
 48%  -> 15
 50%  -> 18
```

```
 52%  -> 18
 54%  -> 18
 56%  -> 18
 58%  -> 18
 60%  -> 21
 62%  -> 21
 64%  -> 21
 66%  -> 21
 68%  -> 21
 70%  -> 24
 72%  -> 24
 74%  -> 24
 76%  -> 24
 78%  -> 24
 80%  -> 27
 82%  -> 27
 84%  -> 27
 86%  -> 27
 88%  -> 27
 90%  -> 36
 92%  -> 36
 94%  -> 36
 96%  -> 36
 98%  -> 36
100%  -> 42
```

54Mbps is believed a more reasonable data rate value

RSSI Threshold Lab Practice (1/3)

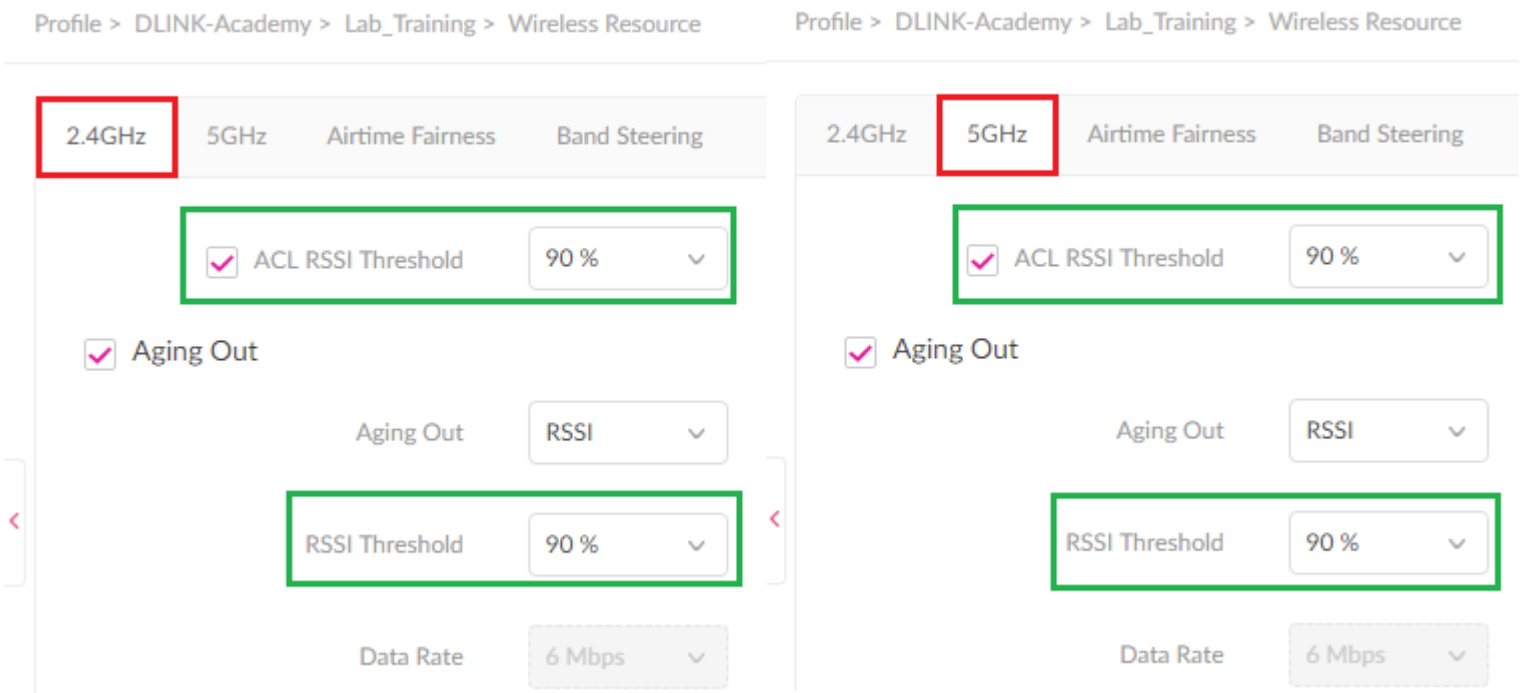
- RSSI Threshold Lab Practice
- There are three wireless clients in our lab facility, where the RSSI information for each station is displayed here as well.



No.	Action	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID	AP MAC Address
1		172.17.5.124	f0:7d:68:f7:dc:09	Disabled	1	-67	2.4GHz	F-22-Raptor	40:9b:cd:0c:64:c0
2		172.17.5.103	a4:db:30:cb:36:0e	Disabled	1	-57	2.4GHz	Boeing-F-A-XX	40:9b:cd:0c:64:c0
3		172.17.5.116	00:1c:bf:a9:52:ec	Disabled	149	-48	5GHz	F-35-Lightning	40:9b:cd:0c:67:50

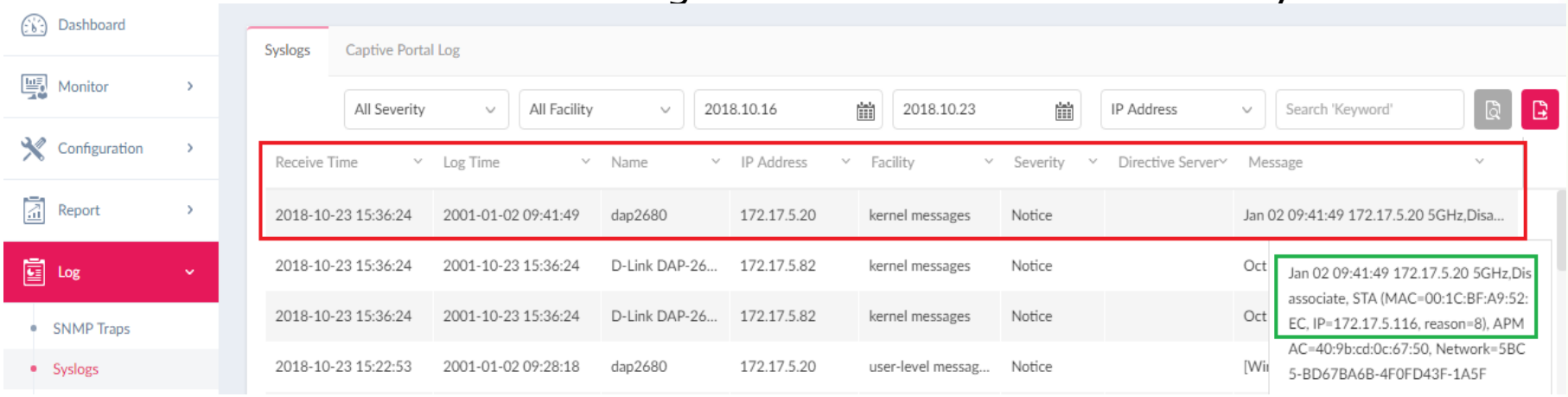
RSSI Threshold Lab Practice (2/3)

- RSSI Threshold Lab Practice
- We are going to make "RSSI Threshold" to an extreme number and then to see the outcome of such configurations.



RSSI Threshold Lab Practice (3/3)

- RSSI Threshold Lab Practice
- All three wireless stations got disassociated immediately.

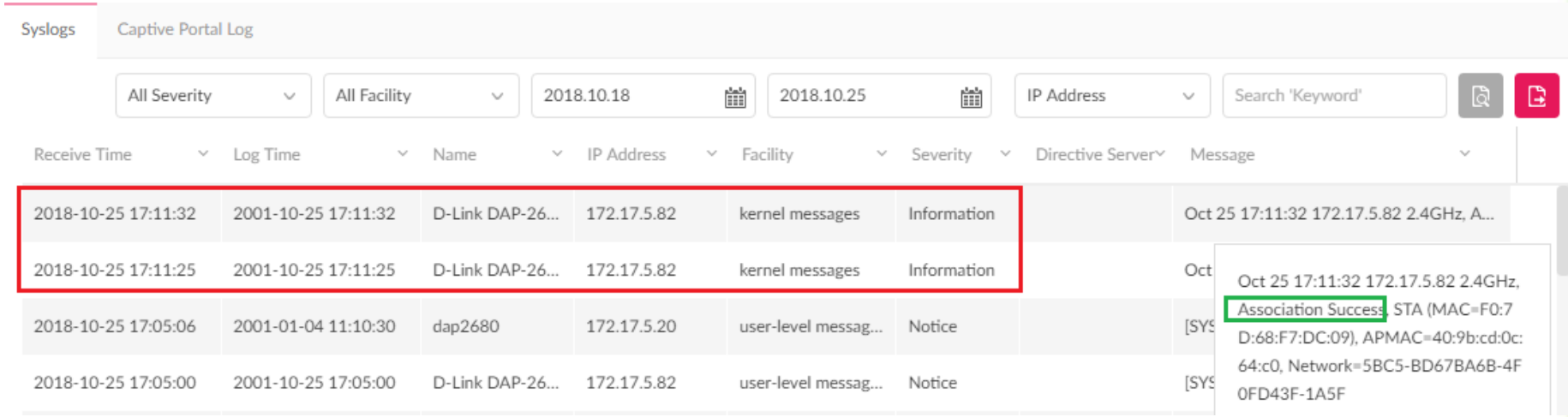


Wireless Roaming

- Wireless roaming is when a wireless client(station) moves around in an area with multiple access point(AP), it may automatically switch to another AP which has better signal strength.
- As stated in D-Track DK1600285, the CWM 1.0 server saves wireless client information, including the one from CP authentication procedure, then client would roam to another AP under the same profile settings.

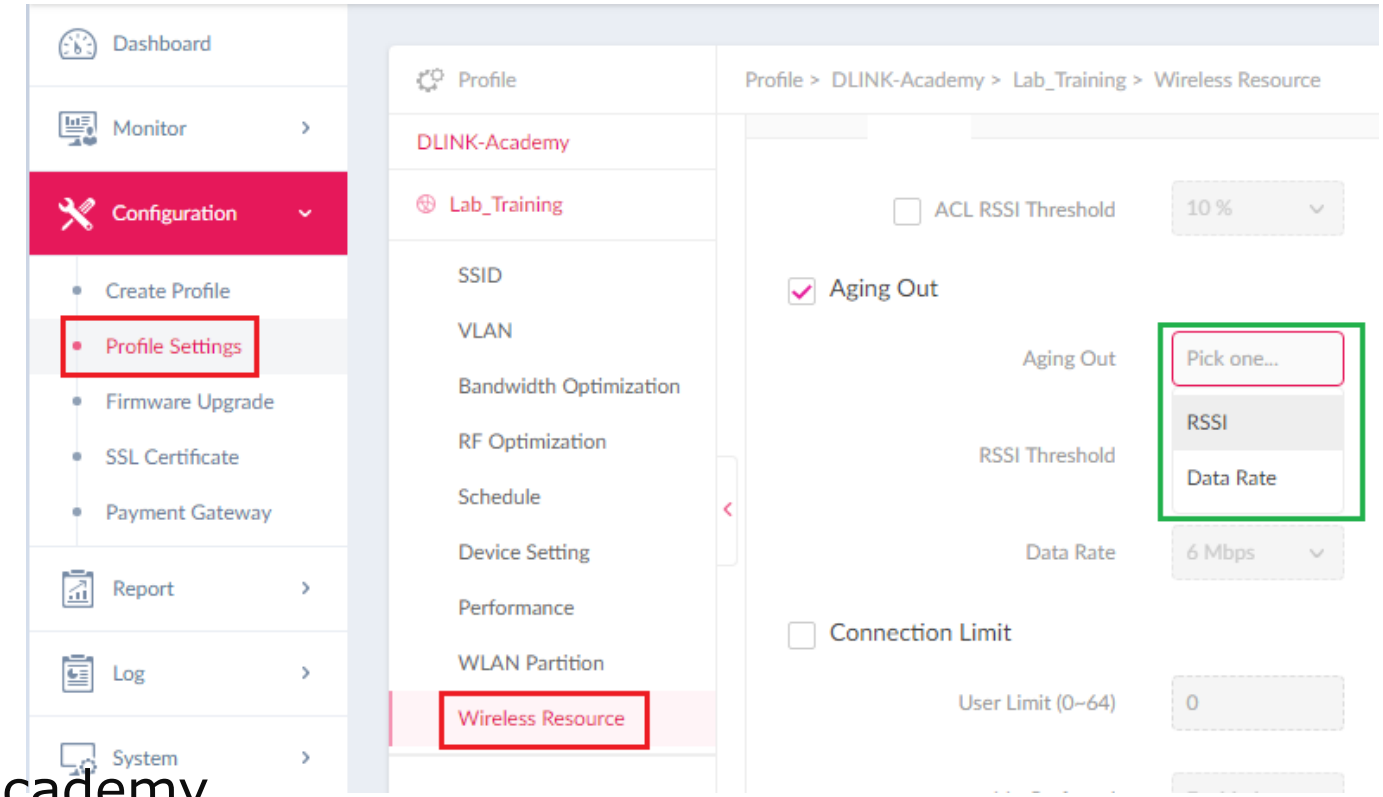
User Management, Access Control and System Administration

- In our lab facility, there are two DAP on-line, where two wireless clients connect to one DAP (A) and one wireless client connect another DAP (B). We unplugged the power of one DAP (A).
- The following messages show two wireless stations got connected to the alive AP on a timely fashion.



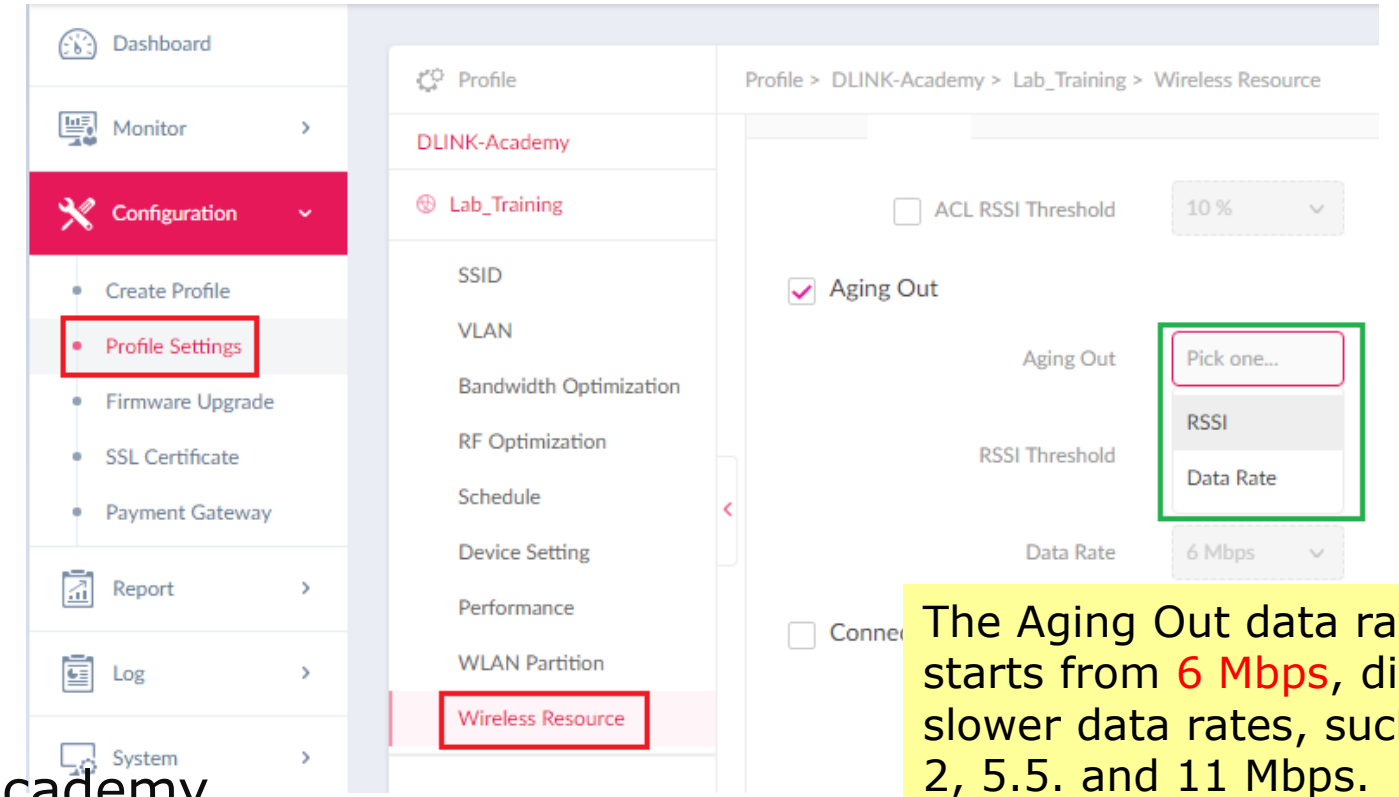
User Management, Access Control and System Administration

- Explanation of terms
- Aging Out (Kick-out). Various criteria being specified where DNC should age out a wireless client: RSSI / Data Rate



User Management, Access Control and System Administration

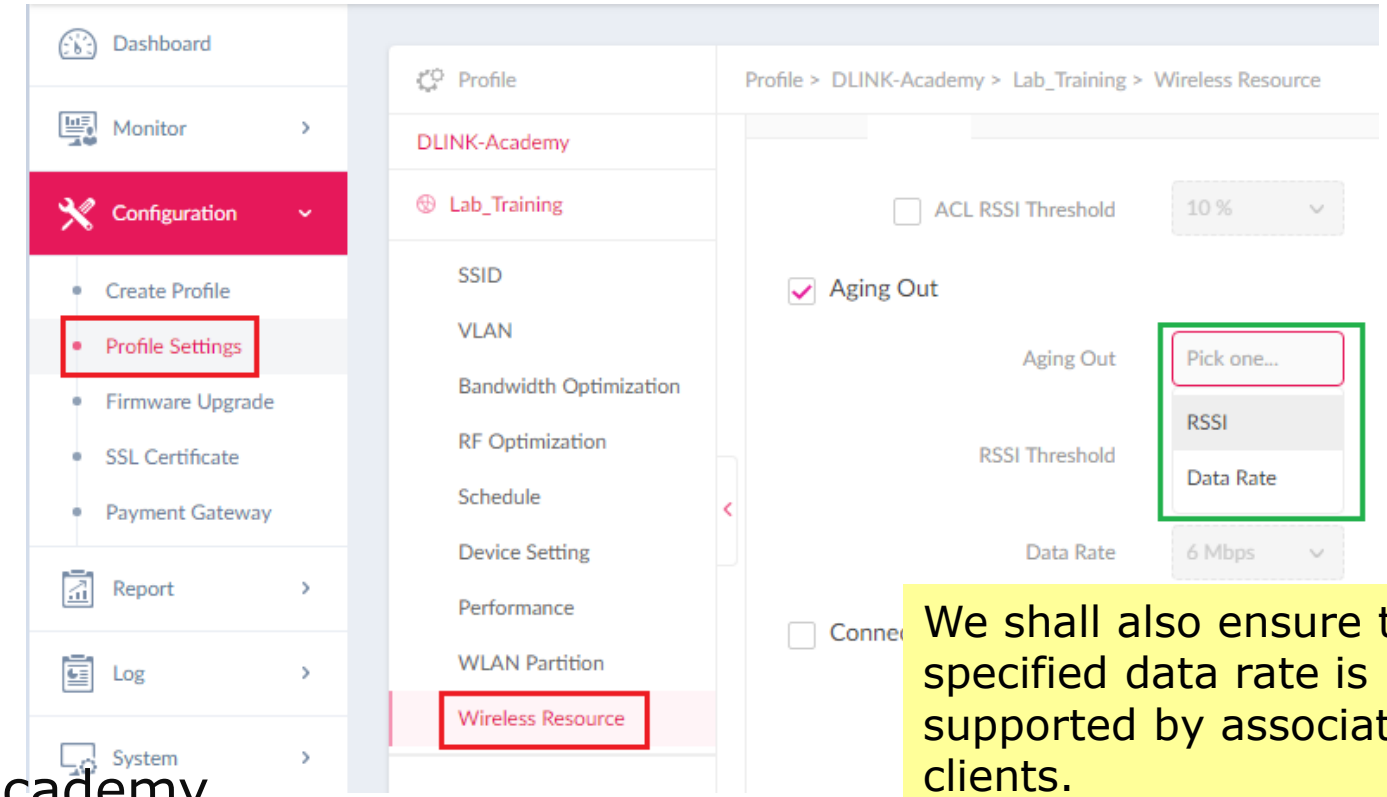
- Explanation of terms
- Aging Out (Kick-out). Various criteria being specified where DNC should age out a wireless client: RSSI / Data Rate



The Aging Out data rate starts from 6 Mbps, disabling slower data rates, such as 1, 2, 5.5. and 11 Mbps.

User Management, Access Control and System Administration

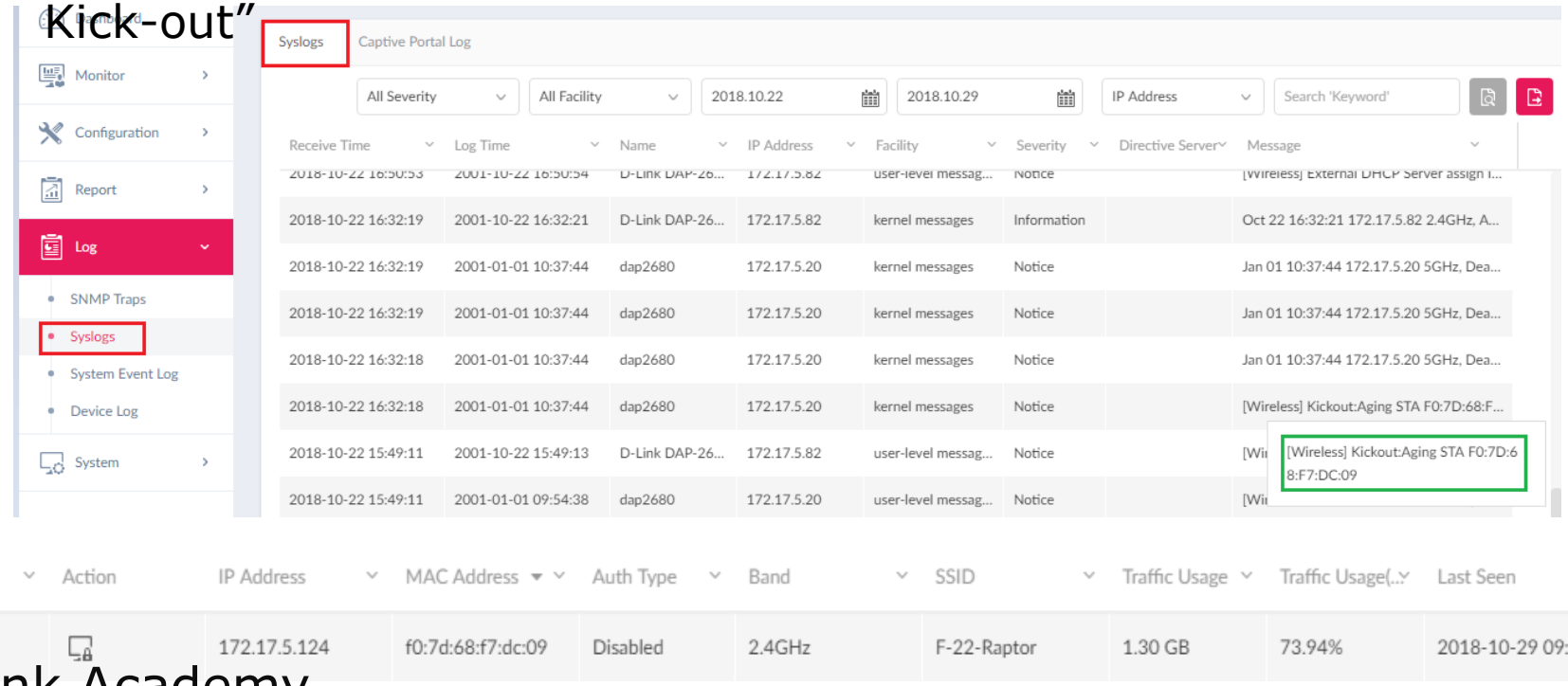
- Explanation of terms
- Aging Out (Kick-out). Various criteria being specified where DNC should age out a wireless client: RSSI / Data Rate



We shall also ensure the specified data rate is supported by associated clients.

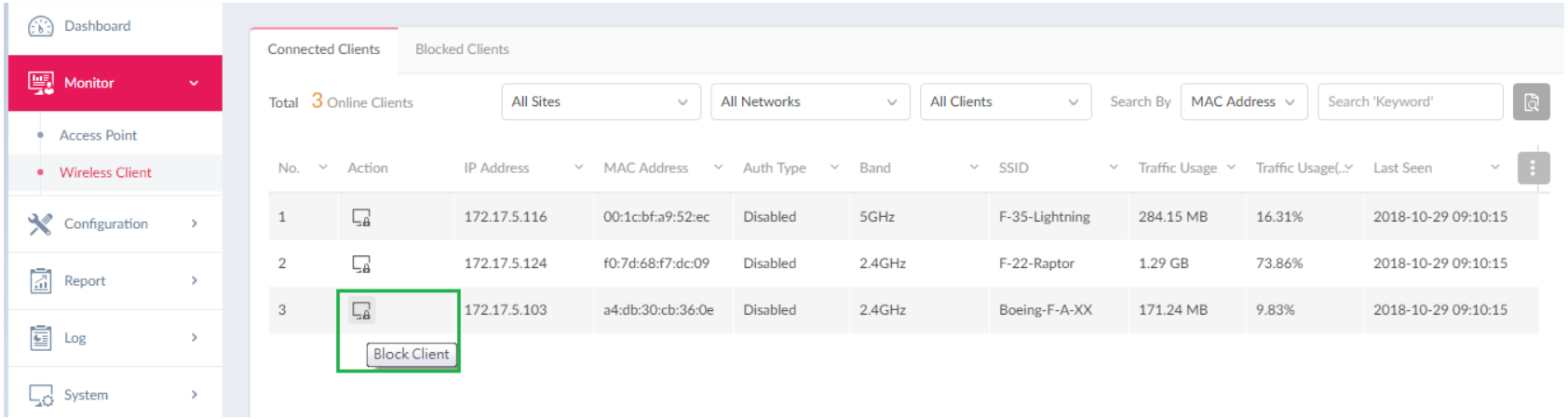
User Management, Access Control and System Administration

- Explanation of terms
- Aging Out (Kick-out). Various criteria being specified where DNC should age out a wireless client: RSSI / Data Rate
- The following image shows an example of "Wireless Client Aging Kick-out"



User Management, Access Control and System Administration

- Explanation of terms
- Kick-off function serves the purpose to force a wireless client being disconnected from the AP managed by CWM (D-Track DK1700291)
  - CWM 1.0 / Nuclias Connect will automatically add this wireless client's mac address to the reject-access list and apply this settings to all managed APs without any further notification.
- "Blocking Wireless Client" is on Wireless Client page under the Monitor tab.

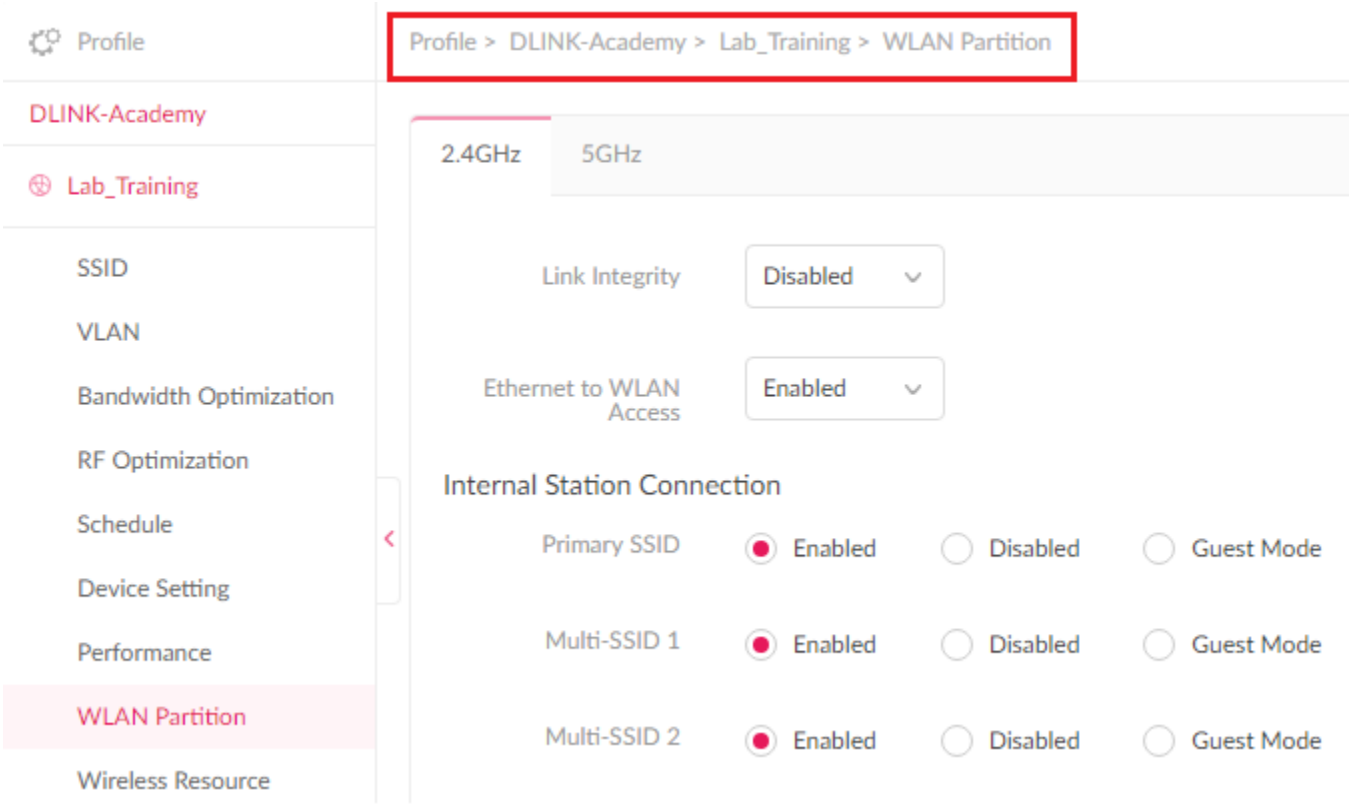


WLAN Partition

- WLAN Partition configuration parameters (DK1700228)
  - Link Integrity: If enable, STA will be disconnected if AP detect LAN port down.
  - Internal Station Connection:
    - ✓ Enable: Select this option to allow communication between wireless clients connected to the same SSID and between wireless clients connected to different SSIDs configured on this access point.
    - ✓ Disable: Select this option to disallow communication between wireless clients connected to the same SSID, but to allow communication between wireless clients connected to different SSIDs configured on this access point.
    - ✓ Guest: Select this option to disallow communication between wireless clients connected to the same SSID and between wireless clients connected to different SSIDs configured on the access point

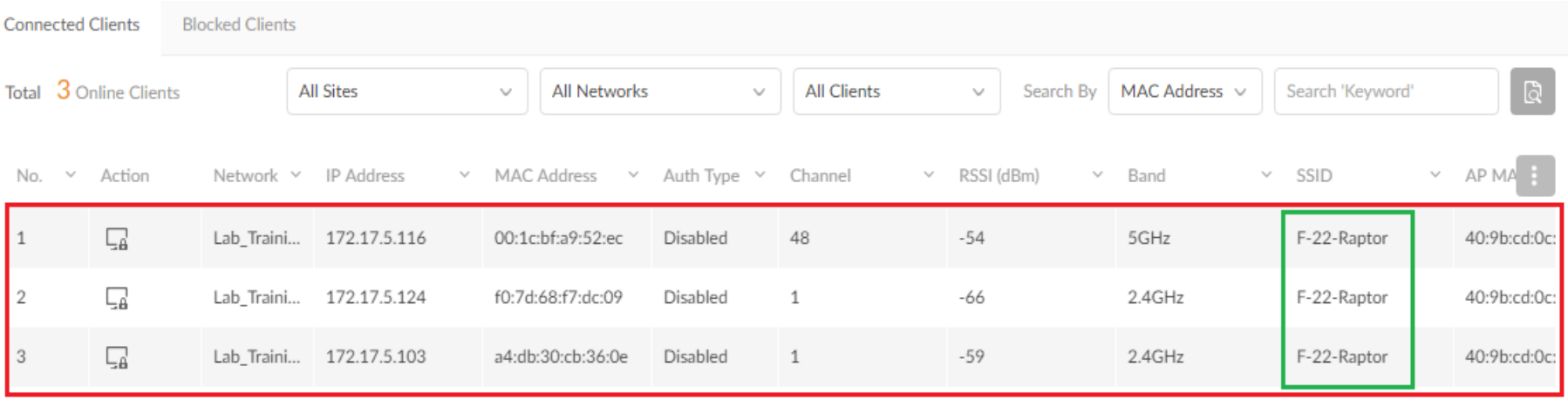
Nuclias Connect WLAN Partition Settings

- WLAN Partition configuration is located on the Profile Settings page under the Configure tab



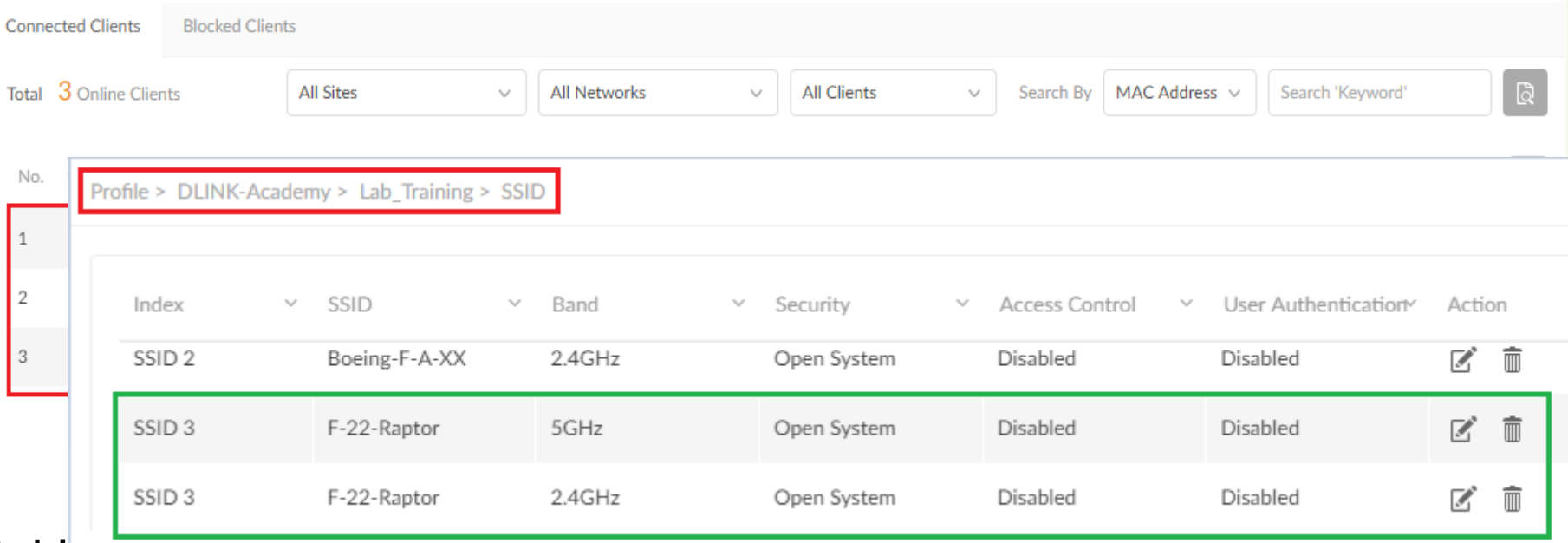
WLAN Partition Practice Lab (1/3)

- WLAN Partition configuration is located on the Profile Settings page under the Configure tab
  - Our lab indicates three wireless stations connected to SSID F-22-Raptor, which is SSID 3, in our Profile (DLINK-Academy, Lab_Training)



WLAN Partition Practice Lab (2/3)

- WLAN Partition configuration is located on the Profile Settings page under the Configure tab
  - Our lab indicates three wireless stations connected to SSID F-22-Raptor, which is SSID 3, in our Profile (DLINK-Academy, Lab_Training)

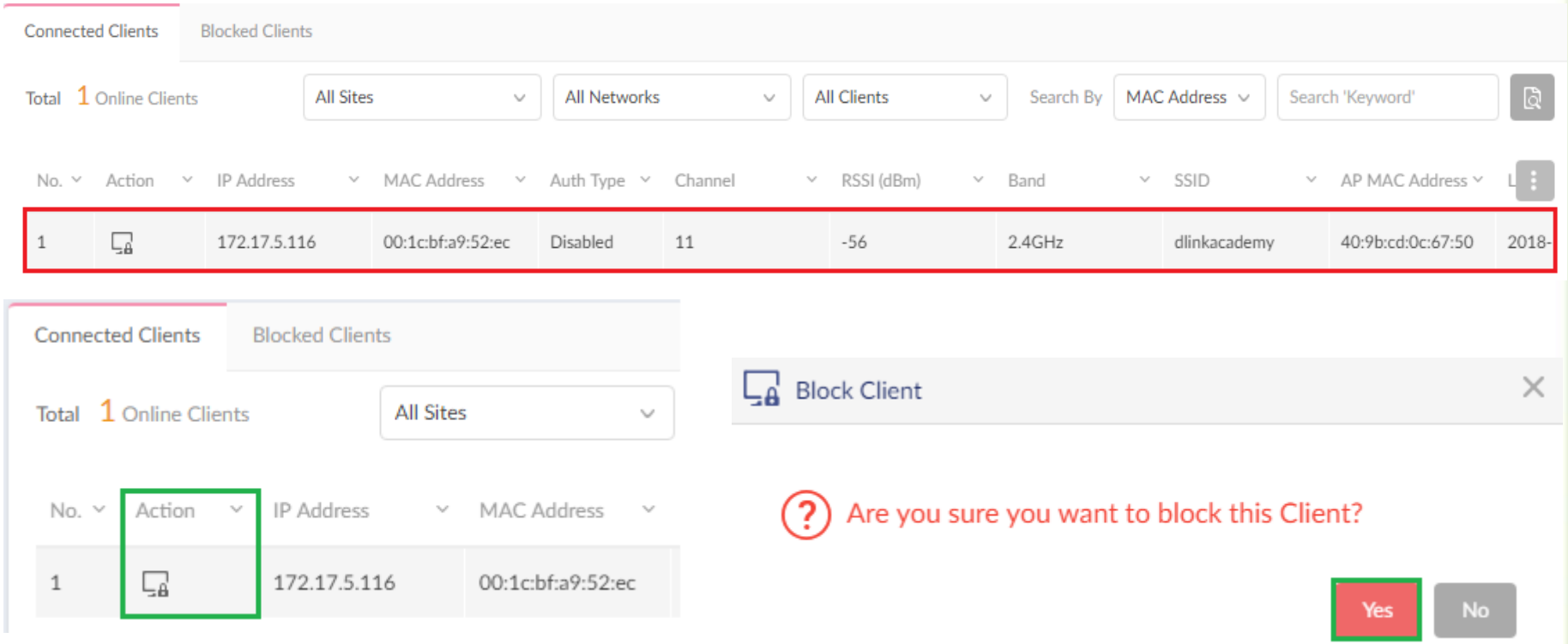


WLAN Partition Practice Lab (3/3)

- WLAN Partition configuration is located on the Profile Settings page under the Configure tab
  - Our lab indicates three wireless stations connected to SSID F-22-Raptor, which is SSID 3, in our Profile (DLINK-Academy, Lab_Training)
  - Activate the “Internal Station Connection” in guest mode and verify the communication between wireless clients within the same SSID

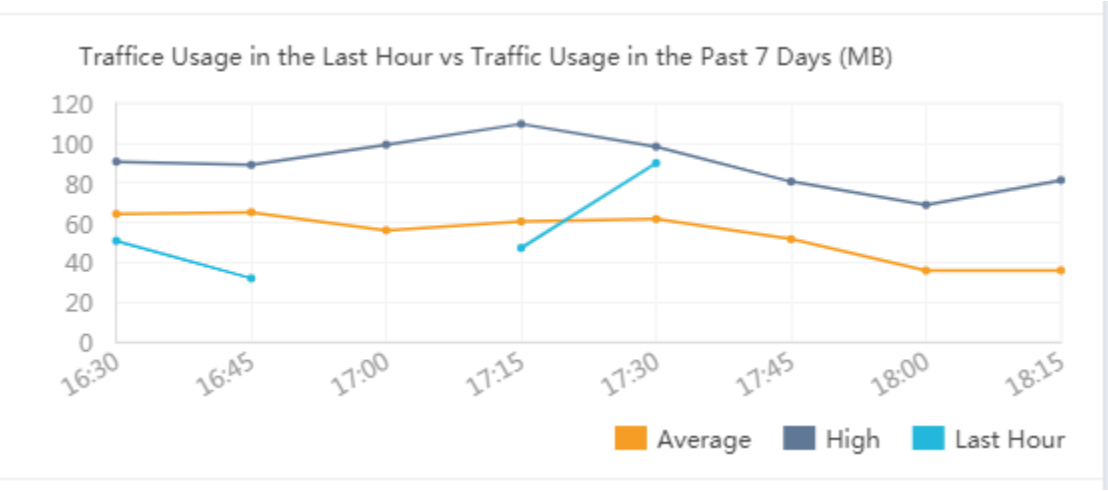
Blocking Access To Our Network

- Client access limitations
  - Network administrator is able to block individual user account access using Nuclias Connect “Block Clinet” option



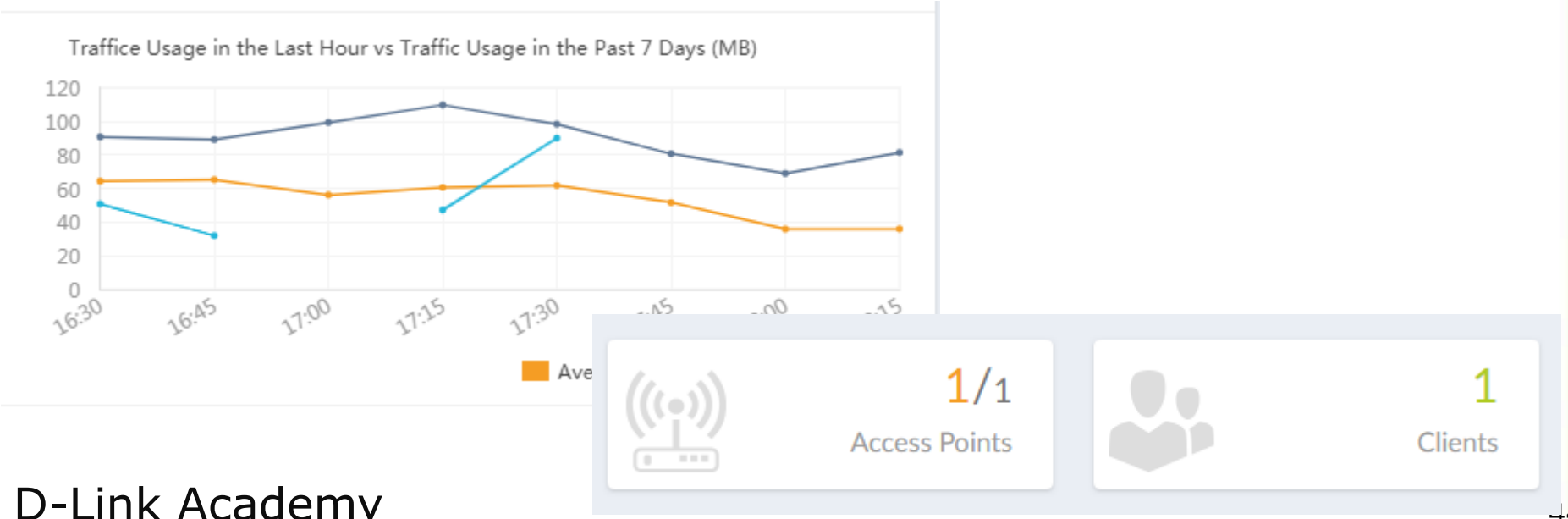
Blocking Access To Our Network (1/8)

- To block a wireless client
- In the traffic usage chart from Dashboard, we identify wireless stations have created more than commonly used wireless traffic.
  - Per below diagram, the "last hour traffic" is close to the "High" traffic utilization, basing upon the analytical data during last 7 days, where only ONE wireless station is in our topology



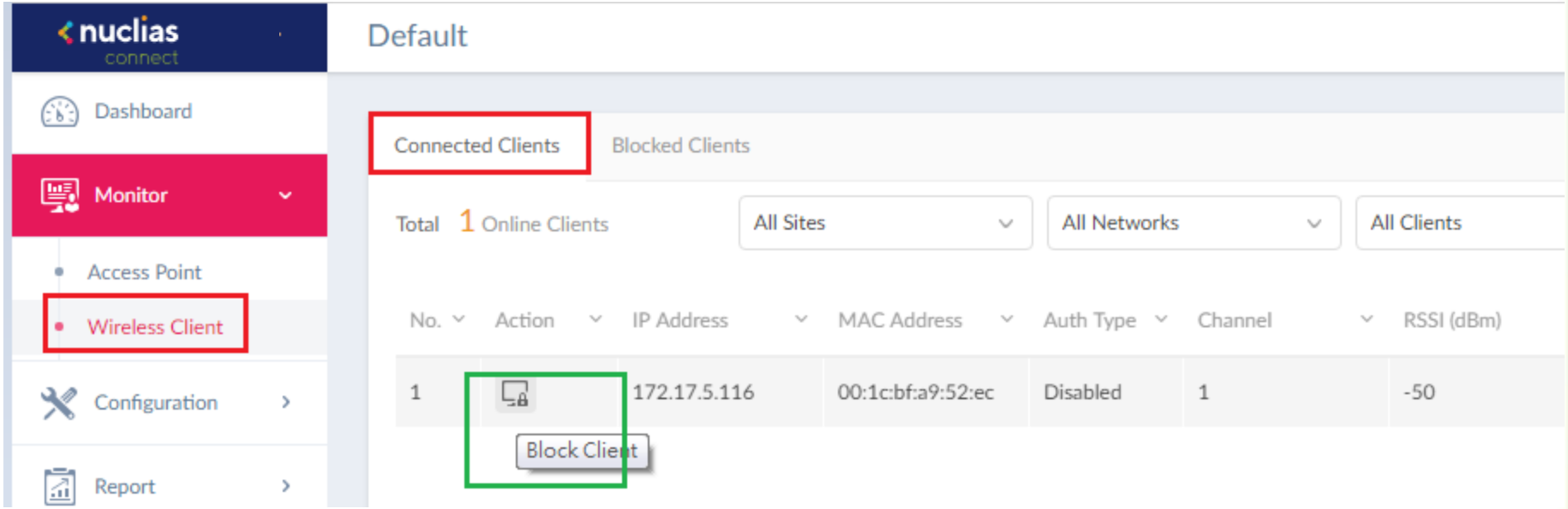
Blocking Access To Our Network (2/8)

- To block a wireless client
- In the traffic usage chart from Dashboard, we identify wireless stations have created more than commonly used wireless traffic.
  - Per below diagram, the "last hour traffic" is close to the "High" traffic utilization, basing upon the analytical data during last 7 days, where only ONE wireless station is in our topology



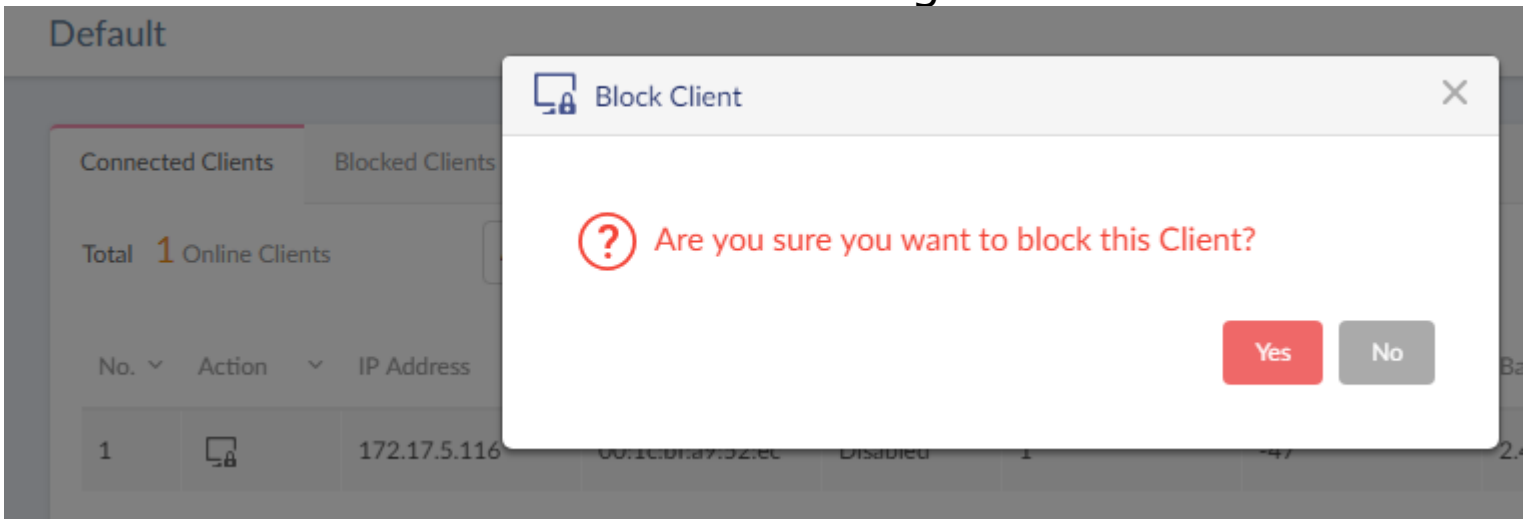
Blocking Access To Our Network (3/8)

- To block a wireless client
- Assuming this is on weekends and no device was supposed to occupy warless traffic, as such, the wireless administrator decides to block wireless communication on that
- Menu: Monitor > Wireless Client (clicking the “Block Client” button)



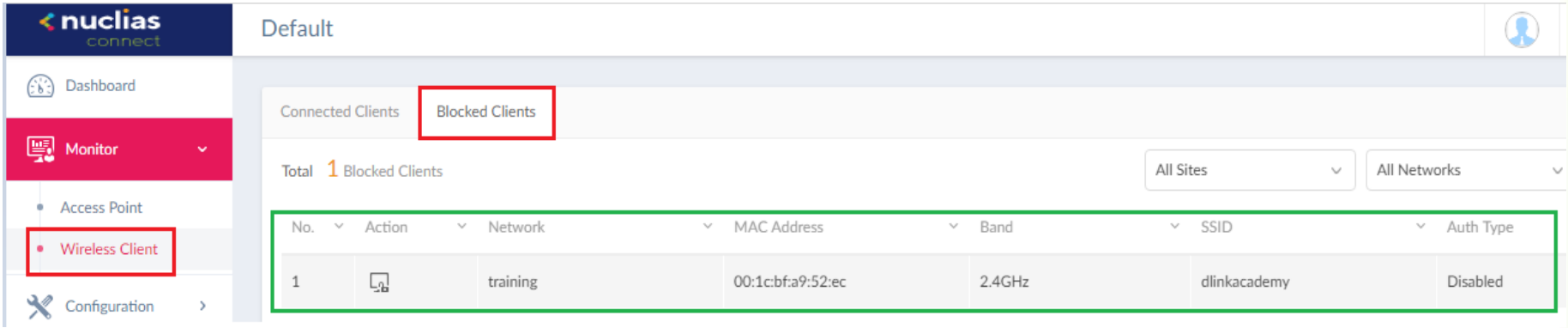
Blocking Access To Our Network (4/8)

- To block a wireless client
- Click “Yes” to confirm this setting

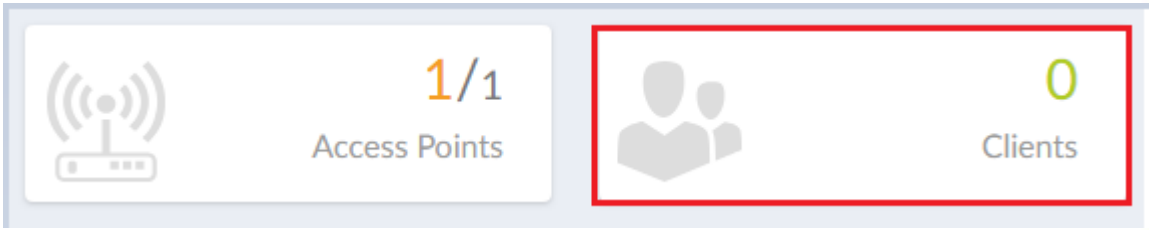


Blocking Access To Our Network (5/8)

- To block a wireless client
- Then, we should be able to view this client in “Blocked Client” tab

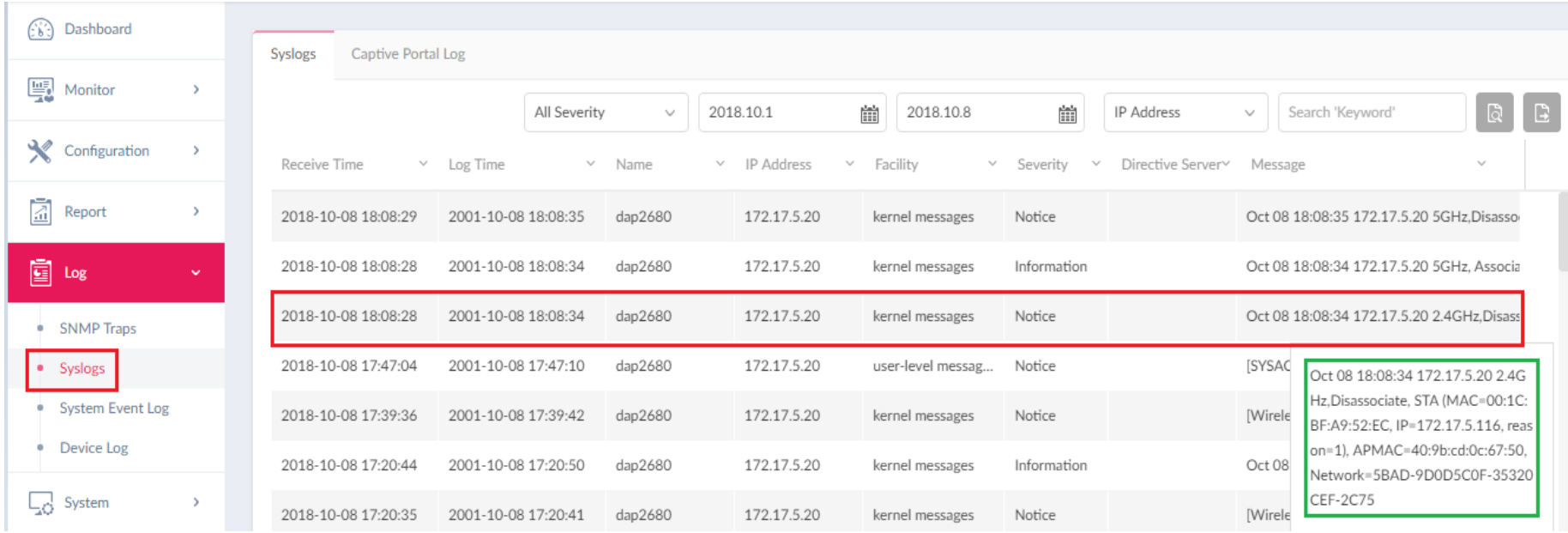


- Nuclias Connect Dashboard also makes a timely update



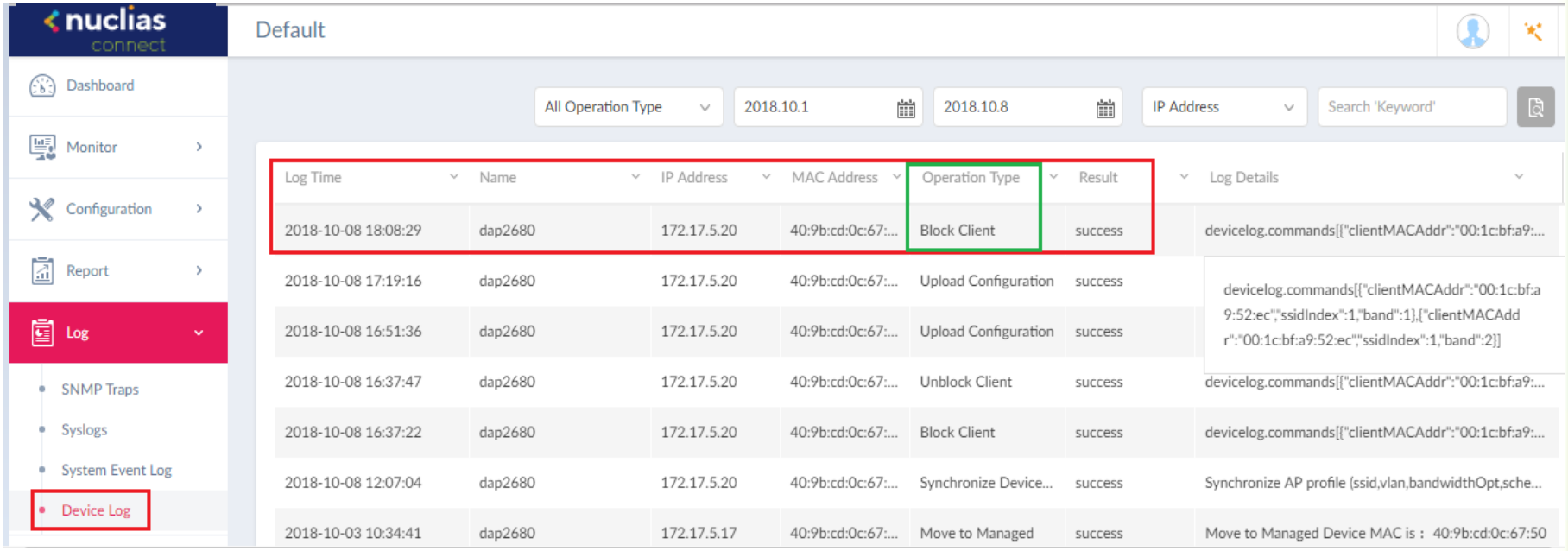
Blocking Access To Our Network (6/8)

- To block a wireless client
- In Log > Syslog, where we shall see a disassociation message record



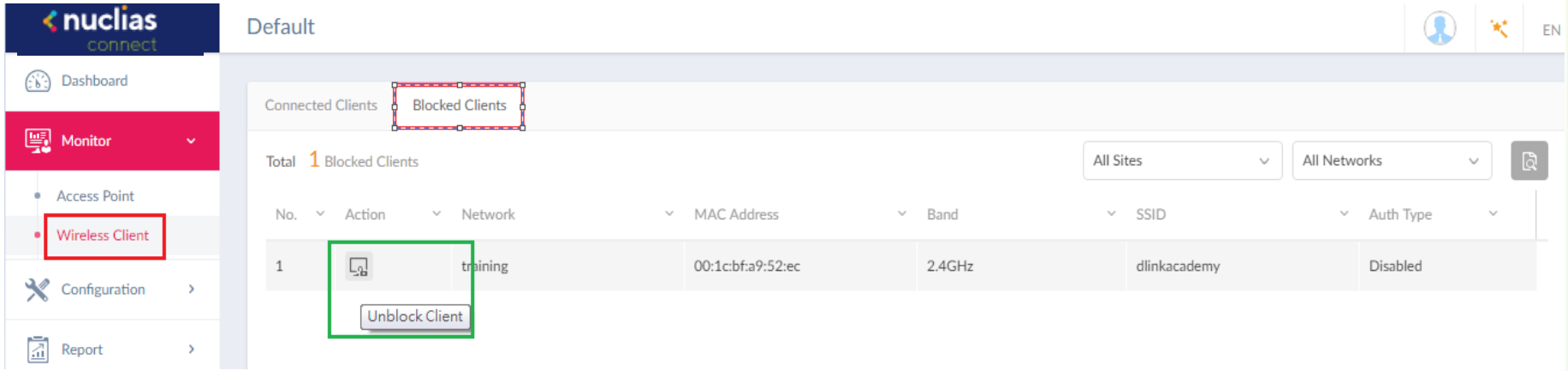
Blocking Access To Our Network (7/8)

- To block a wireless client
- In Log > Device Log, we shall also verify message regarding such activity



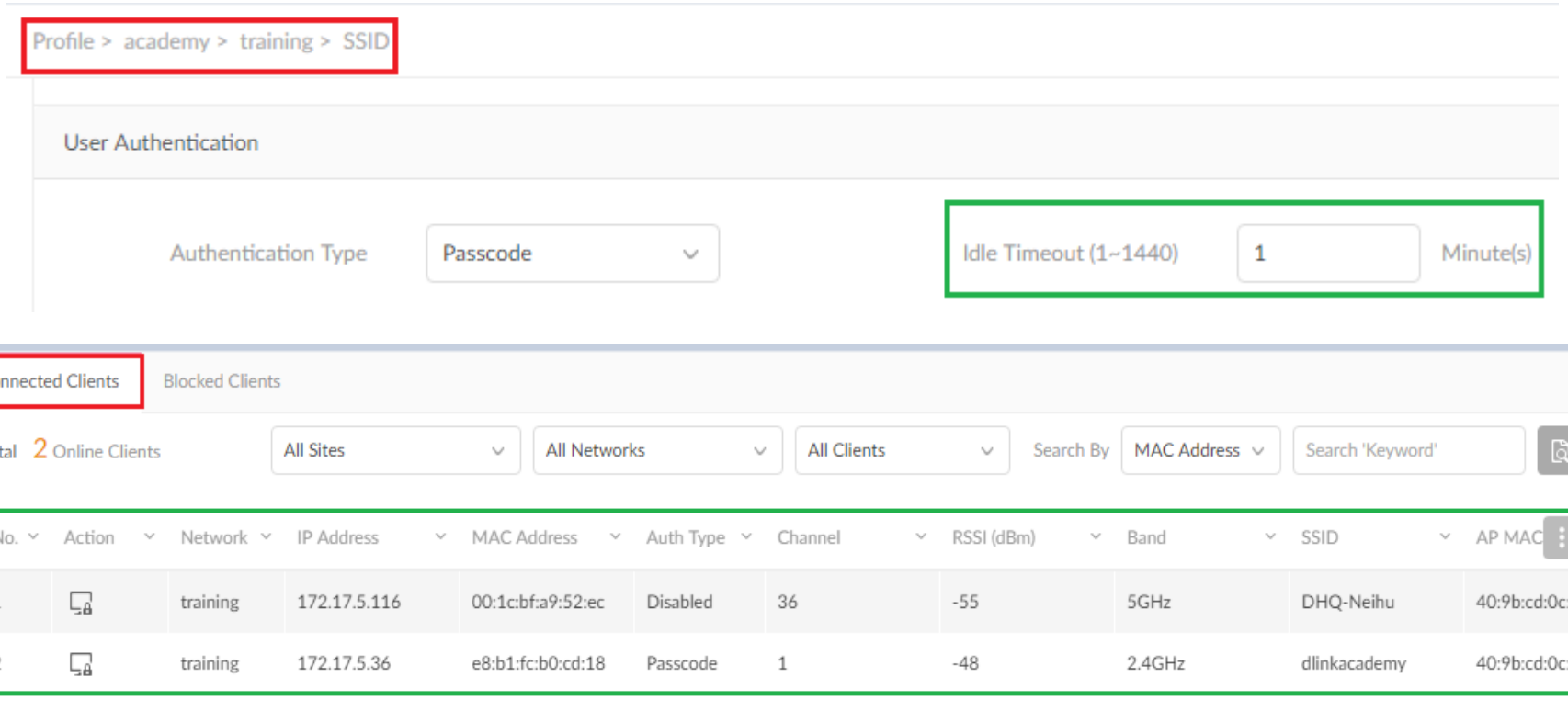
Blocking Access To Our Network (8/8)

- To block a wireless client
- Should you latest on decide to let this wireless station resume connection, just double click the “Unblock Client” icon



User Authentication Idle Timeout

- Idle Timeout is set to 1 minute for SSID “dlinkacademy”
- Client connected status



User Management, Access Control and System Administration

System Administration

- SMTP Settings for Sending Mail
- System Redundancy
- Log Backup
- Uninstall Nuclias Connect Server System

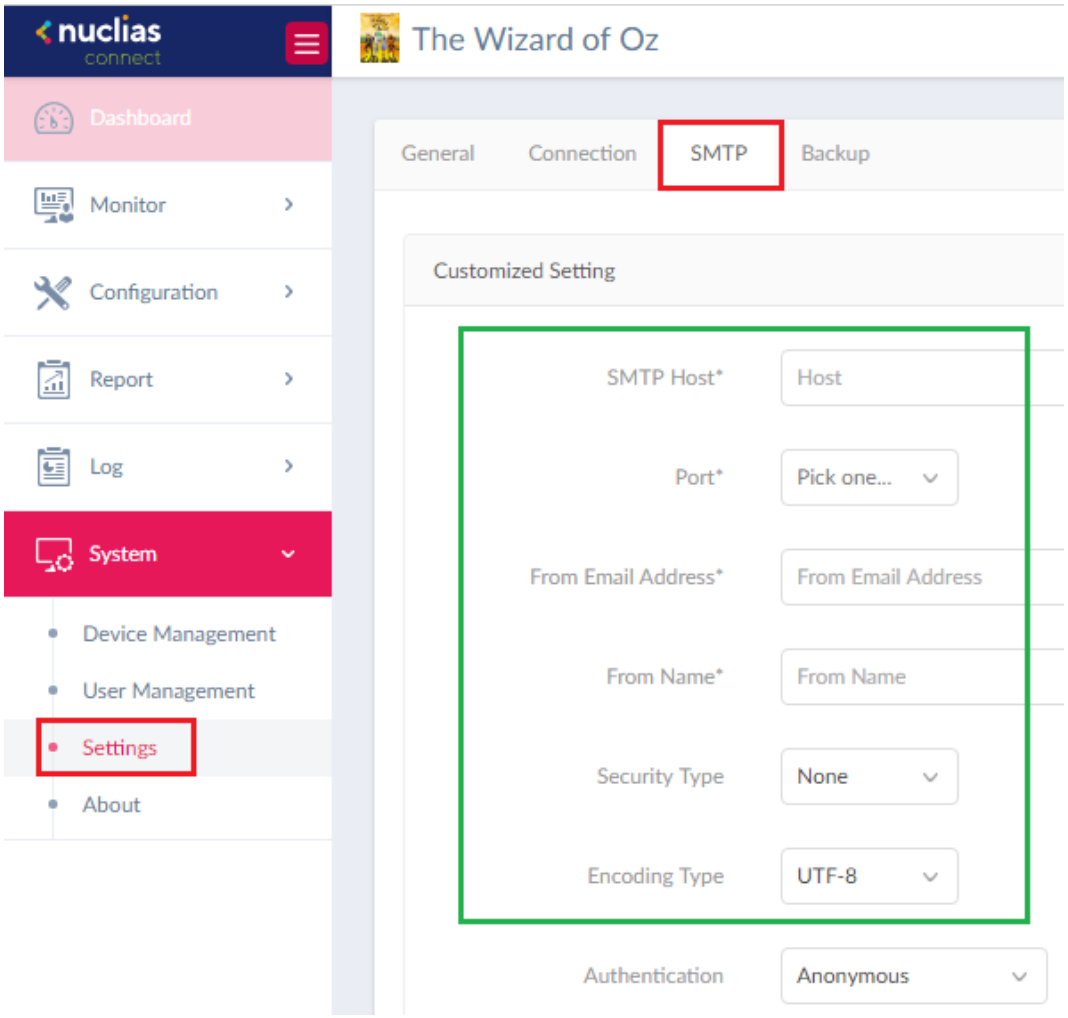
User Management, Access Control and System Administration

System Administration

- SMTP Settings for Sending Mail
- System Redundancy
- Log Backup
- Uninstall Nuclias Connect Server System

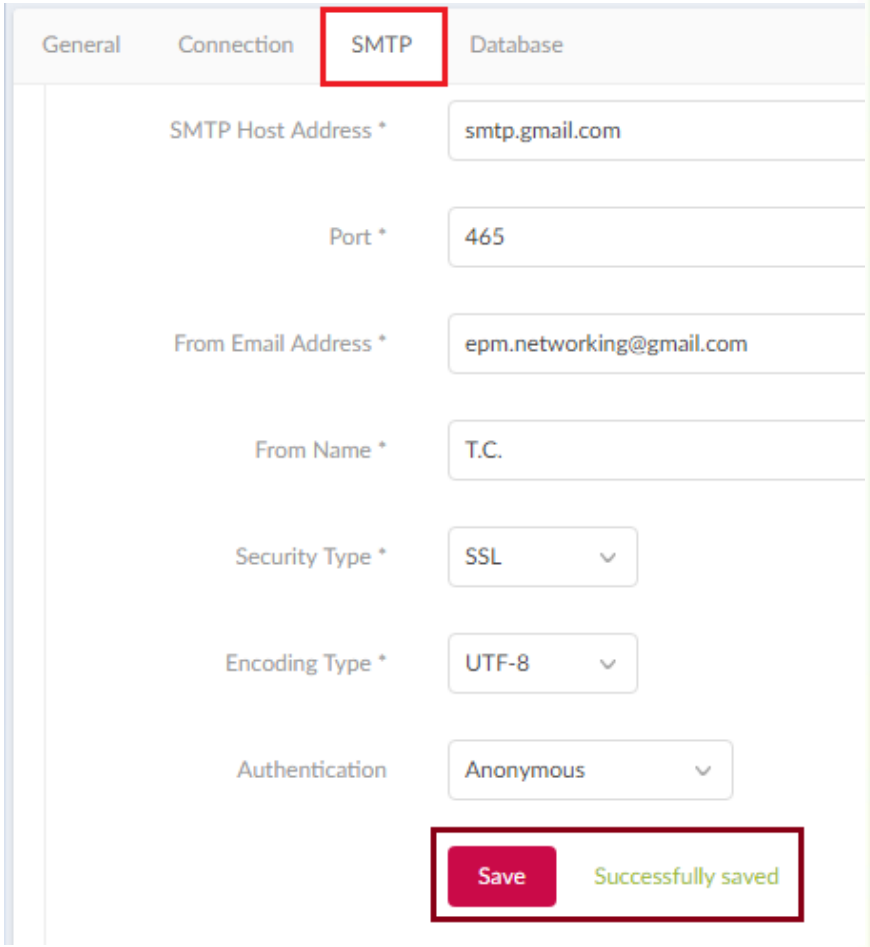
SMTP Settings for Sending Mail

- Nuclias Connect offers the capability to send out e-mail
- The SMTP Settings is located on the Settings page under the System tab.



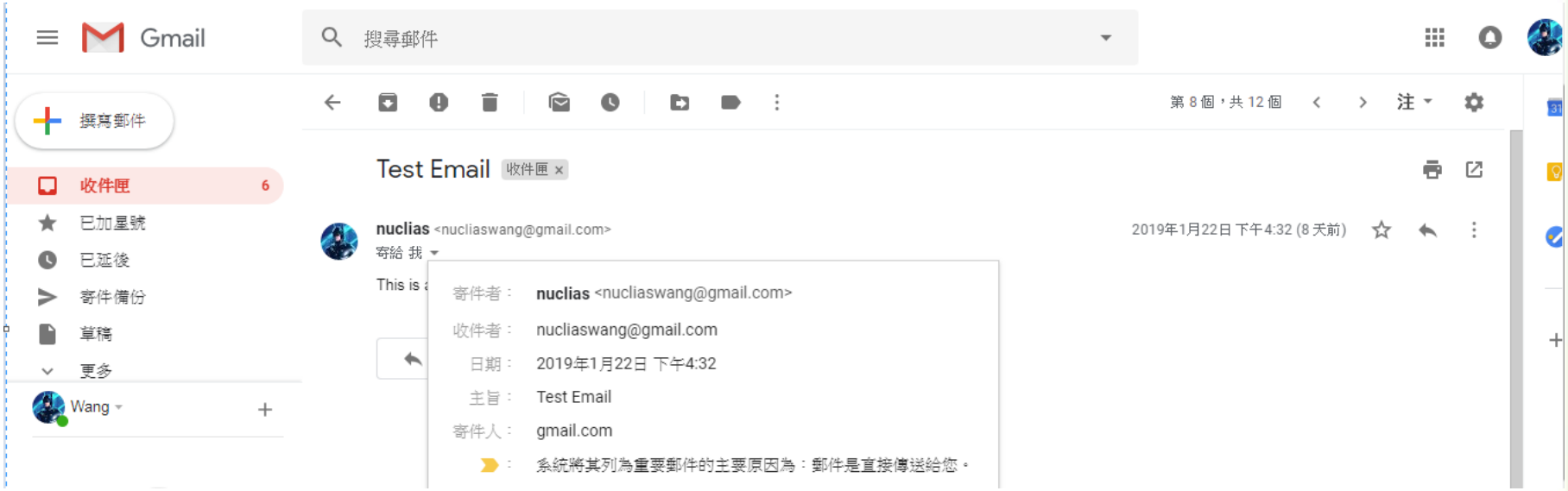
SMTP Settings for Sending Mail

- Configuration settings
  - smtp.gmail.com
  - port 25
- Change account access for less secure apps (GMAIL)
  - Go to your Google Account.
  - On the left navigation panel, click Security.
  - On the bottom of the page, in the Less secure app access panel, click Turn on access.



SMTP Settings for Sending Mail

- Configuration settings
  - smtp.gmail.com
  - port 25
- A testing e-mail is attached, showing DNC sent an e-mail to GMAIL



- SNMP Traps messages are the components being distributed. (D-Track DK1800023)

User Management, Access Control and System Administration

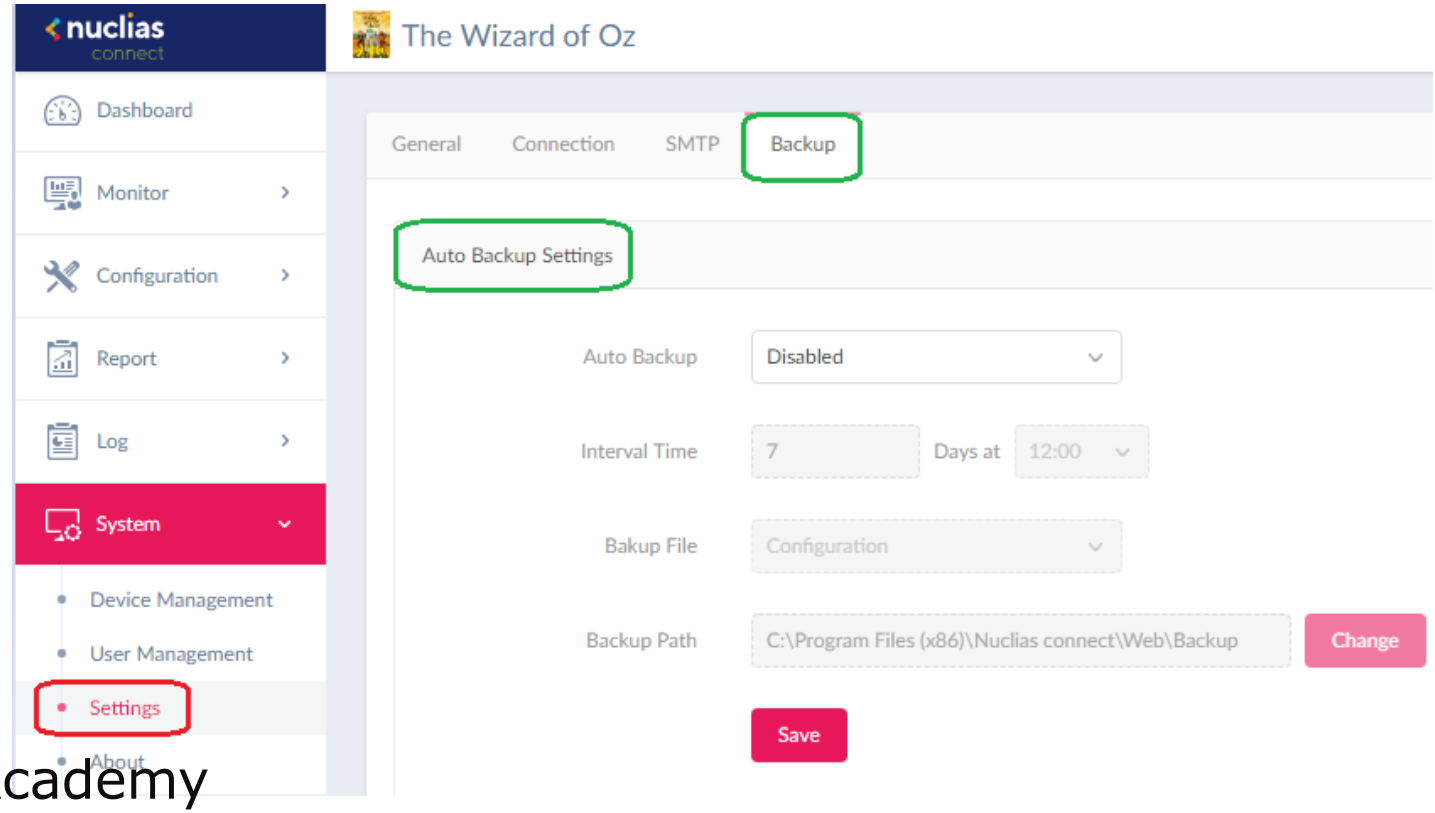
System Administration

- SMTP Settings for Sending Mail
- System Redundancy
- Log Backup
- Uninstall Nuclias Connect Server System

User Management, Access Control and System Administration

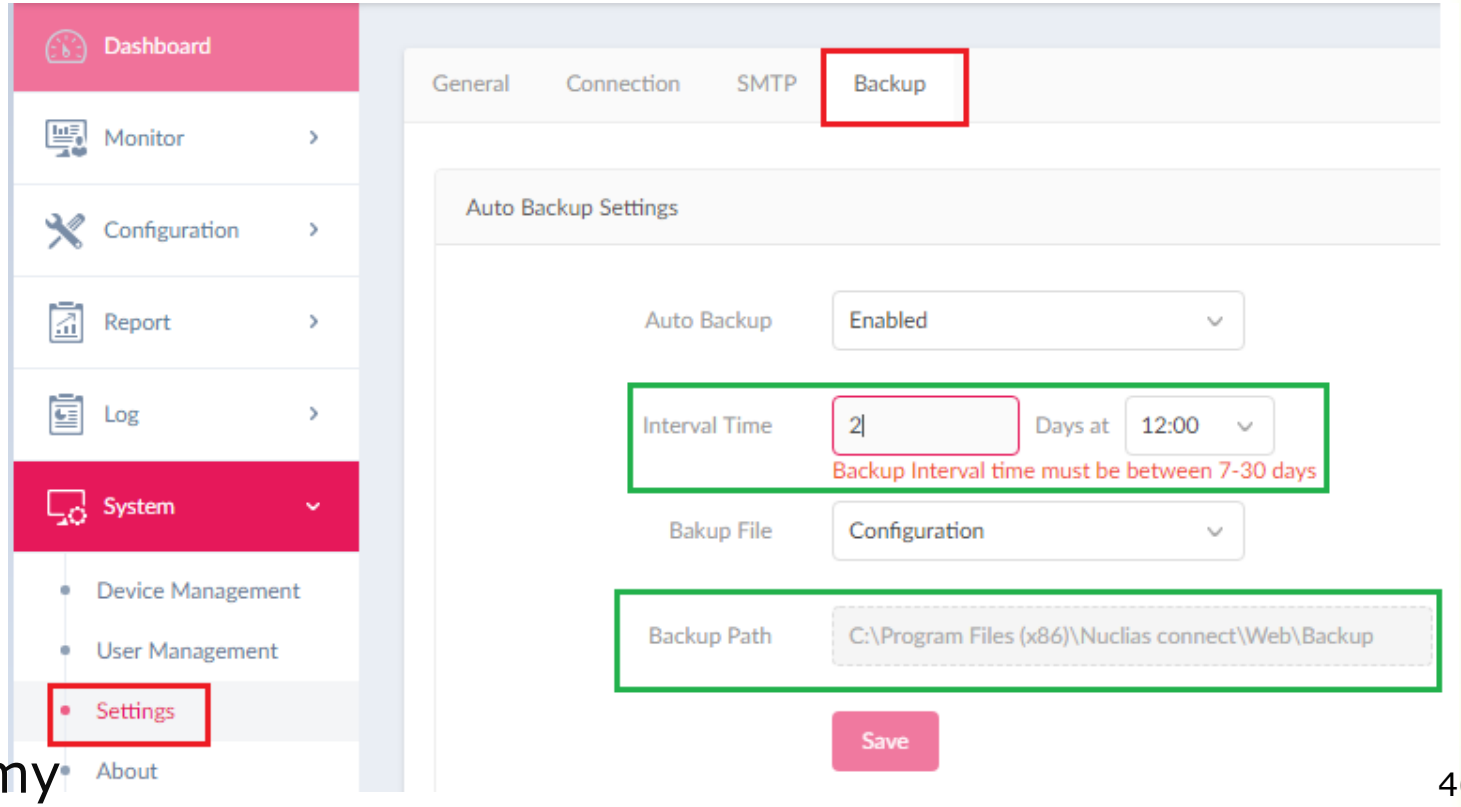
System Administration

- System Redundancy
  - Windows OS



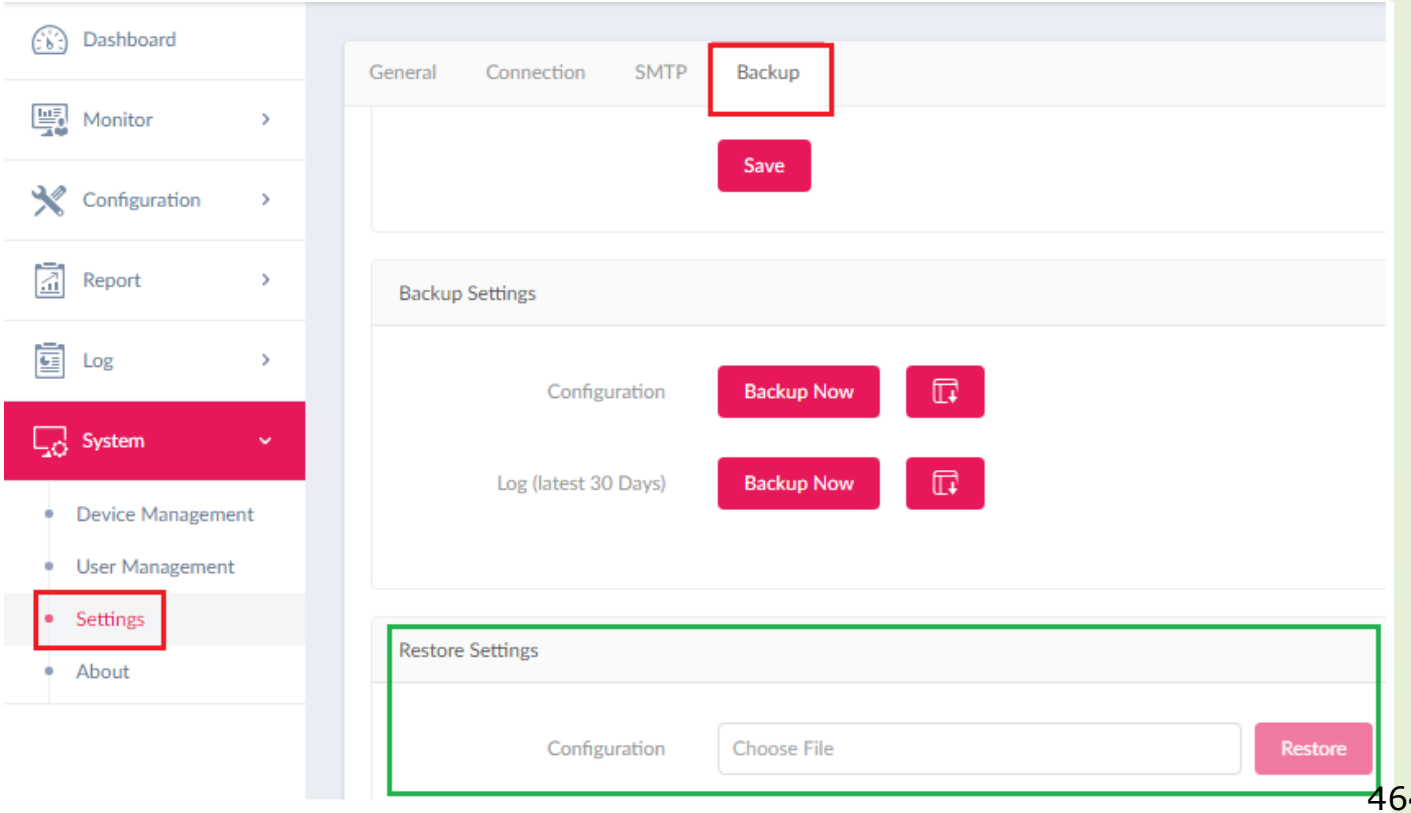
Nuclias Connect Configuration Backup and Restore

- Nuclias Connect Configuration Backup and Restore
- Navigate the menu of System > Settings > Backup
- Auto Backup Settings (setting the frequency for full backups and file location)



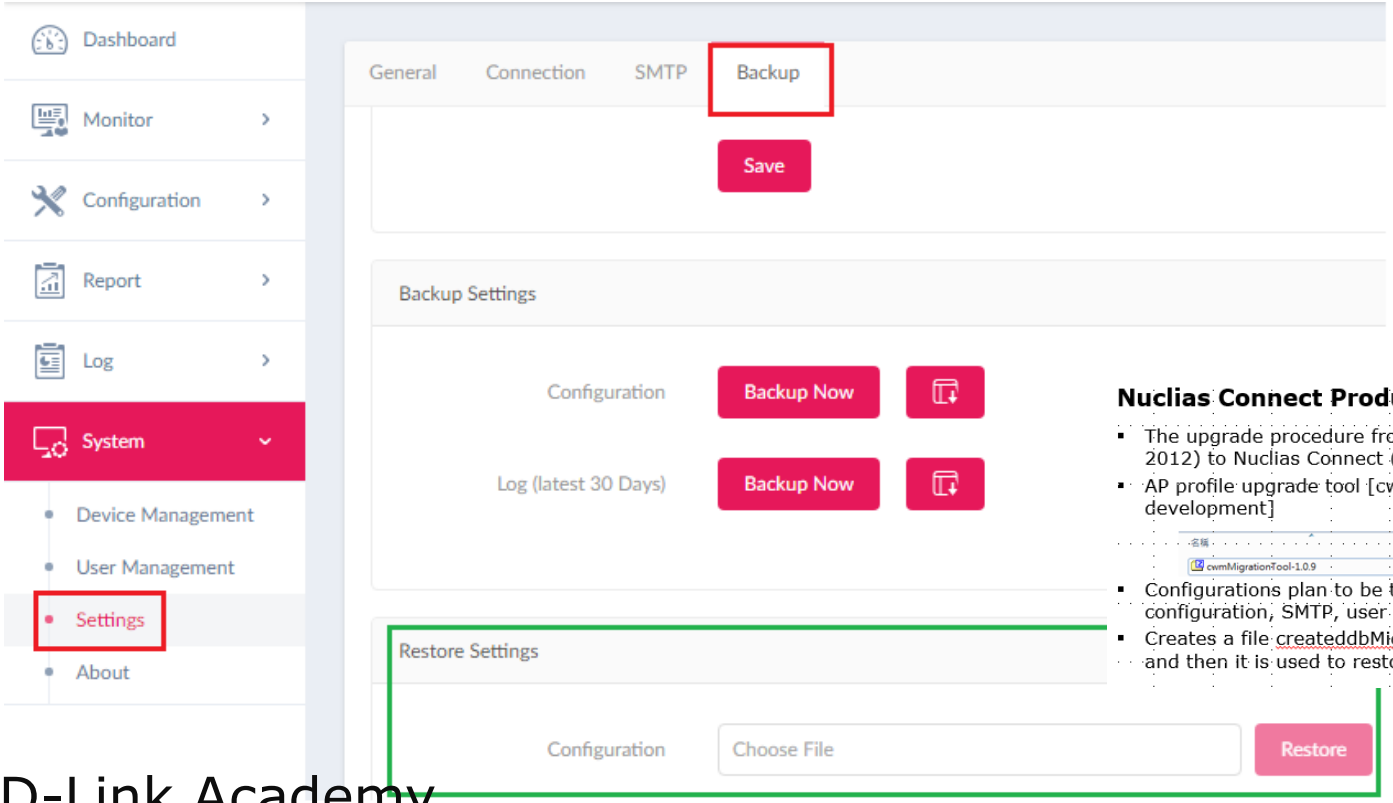
Nuclias Connect Configuration Backup and Restore

- Nuclias Connect Configuration Backup and Restore
- Navigate the menu of System > Settings > Backup
- Configuration Restore



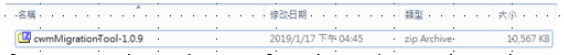
Nuclias Connect Configuration Backup and Restore

- Nuclias Connect Configuration Backup and Restore
- "Restore Settings" field also serves CWM 1.03 direct upgrade to Nuclias Connect platform



Nuclias Connect Product Bulletin, System Upgrade

- The upgrade procedure from CWM 1.03 (Windows 7, 8, 10, Server 2012) to Nuclias Connect (Windows & Linux)
- AP profile upgrade tool [cwmMigrationTool-1.0.9.exe, under development]



- Configurations plan to be transferred: Site/Network topology and configuration, SMTP, user account privileges and details
- Creates a file createddbMigration_Configuration_{dateTime}.cfg, and then it is used to restore back to Nuclias Connect.

User Management, Access Control and System Administration

System Administration

- System Redundancy
  - Windows OS (please see last slide)
  - Docker container in Ubuntu Linux / MAC environment
  - Web UI components in Docker application, where Nuclias Connect database located in a different folder path

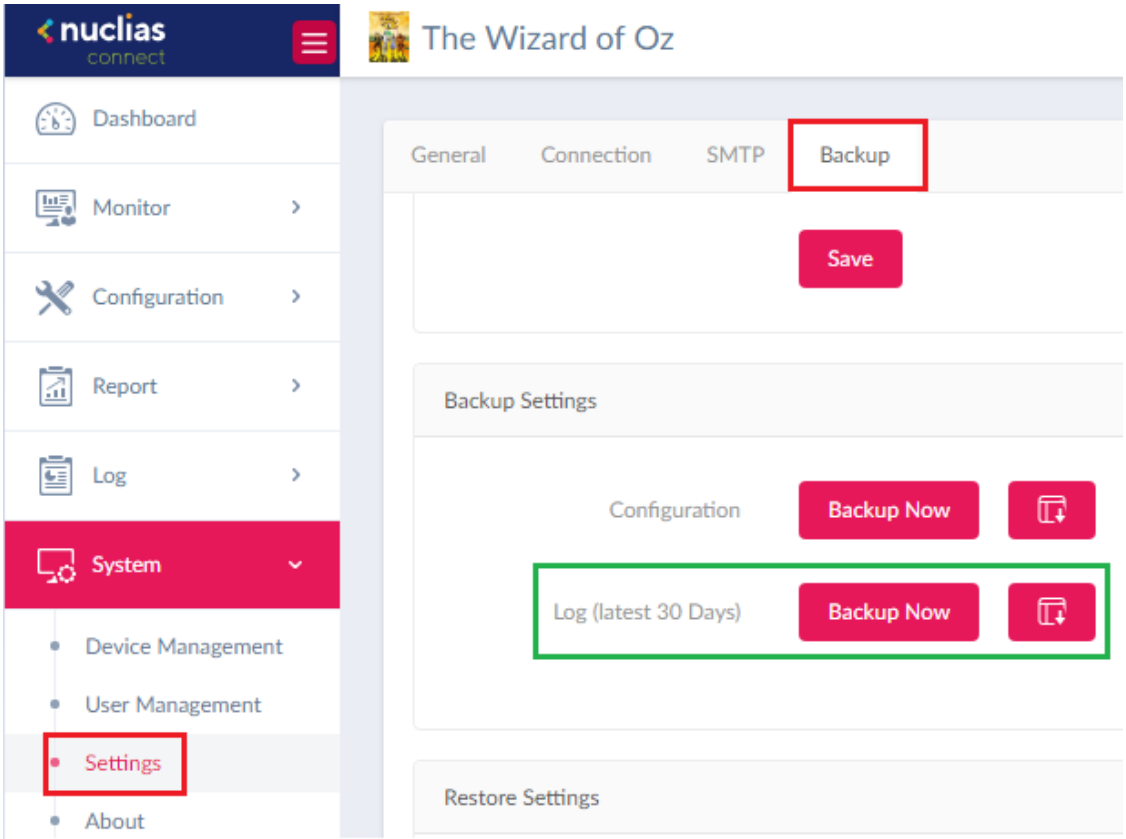
User Management, Access Control and System Administration

System Administration

- SMTP Settings for Sending Mail
- System Redundancy
- Log Backup
- Uninstall Nuclias Connect Server System

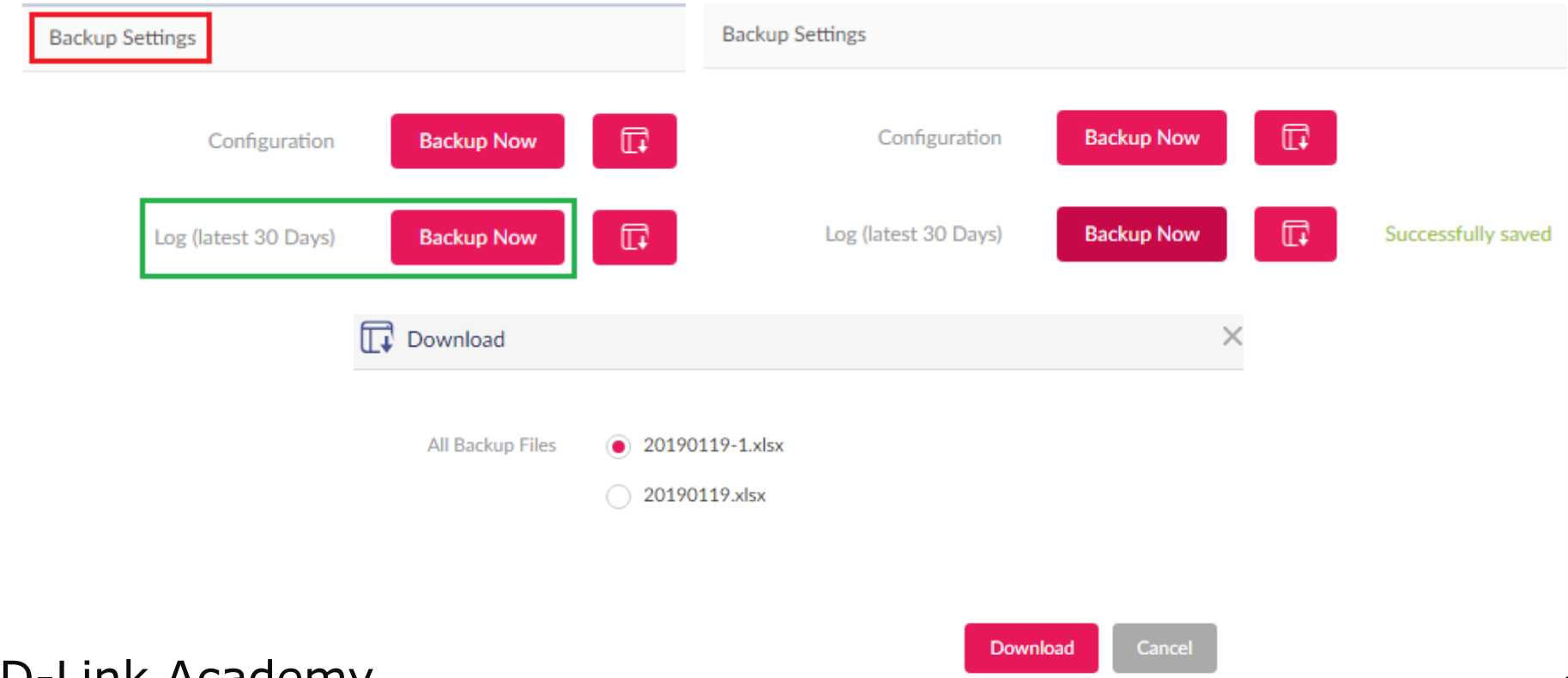
Nuclias Connect Log Backup

- Nuclias Connect Log Backup
- Navigate the menu of System > Settings > Backup > Backup Settings



Nuclias Connect Log Download

- Nuclias Connect Log Download
- Navigate the menu of System > Settings > Backup > Backup Settings



Nuclias Connect Log File Download Review

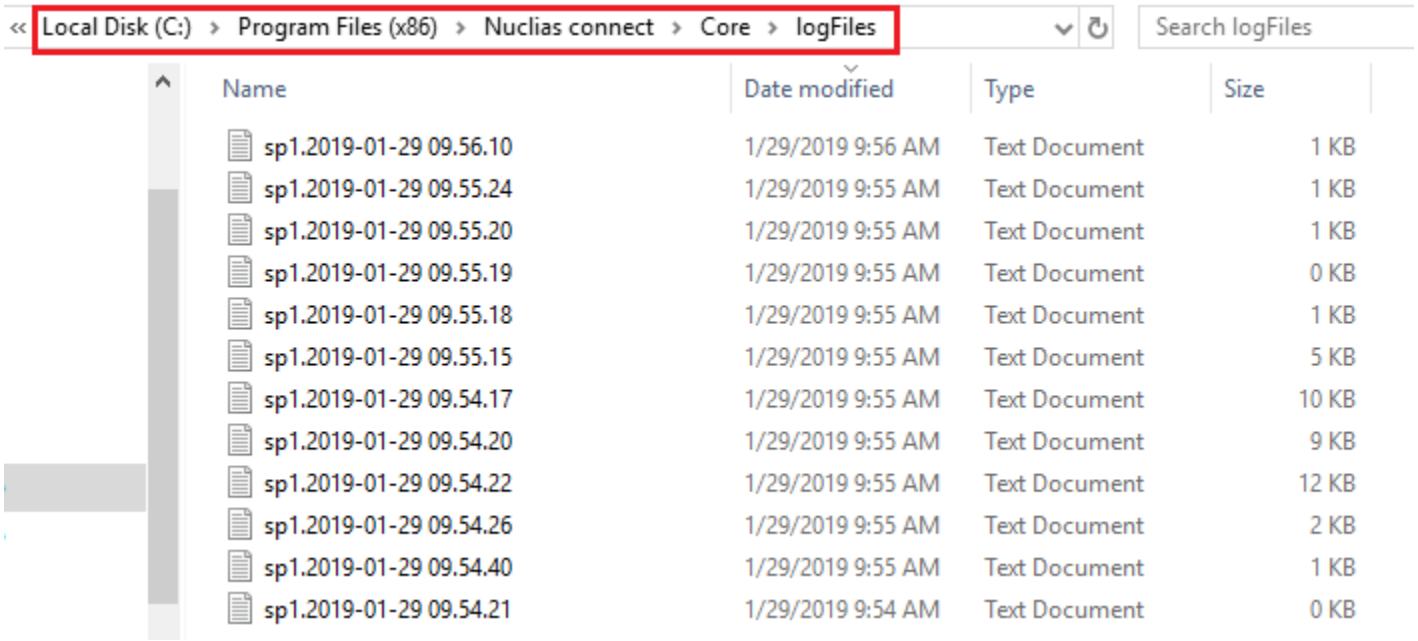
- Nuclias Connect Log download review
- Open the log file

	A	B	C	D	E	F	G	H	I	J
1	Log Time	Name	IP Address	MAC Add	Operation	Result	Log Details			
2	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Register D	Success	School_of_Business			
3	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Register D	Success	School_of_Business			
4	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Register D	Success	School_of_Business			
5	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Register D	Success	School_of_Business			
6	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Synchroniz	Success	Configuration			
7	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Synchroniz	Success	Configuration			
8	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Channel or		Channel. 2.4 GHz: 6, Channel. 5 GHz: 36			
9	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Channel or		Channel. 2.4 GHz: 6, Channel. 5 GHz: 60			
10	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Channel or		Channel. 2.4 GHz: 6, Channel. 5 GHz: 64			
11	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Channel or		Channel. 2.4 GHz: 1, Channel. 5 GHz: 36			
12	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Channel or		Channel. 2.4 GHz: 6, Channel. 5 GHz: 52			
13	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Channel or		Channel. 2.4 GHz: 1, Channel. 5 GHz: 64			
14	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Channel or		Channel. 2.4 GHz: 1, Channel. 5 GHz: 153			
15	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Set AP Ch	Success	2.4 GHz: 6, 5 GHz: 52			
16	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Set AP Po	Success	2.4 GHz: 100%, 5 GHz: 100%			
17	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Set Device	Success	DHQ			
18	2019-01-0	DAP_2680	172.17.5.9	18:0f:76:3	Set Device	Success	DAP_2680_ea_60			
19	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Set AP Ch	Success	2.4 GHz: 1, 5 GHz: 153			
20	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Set AP Po	Success	2.4 GHz: 100%, 5 GHz: 100%			
21	2019-01-0	D-Link DA	172.17.5.9	18:0f:76:3	Set Device	Success	DHQ			

Device-Log | System-Event-Log | Syslog | Trap-Log

Nuclias Connect Core Server Log

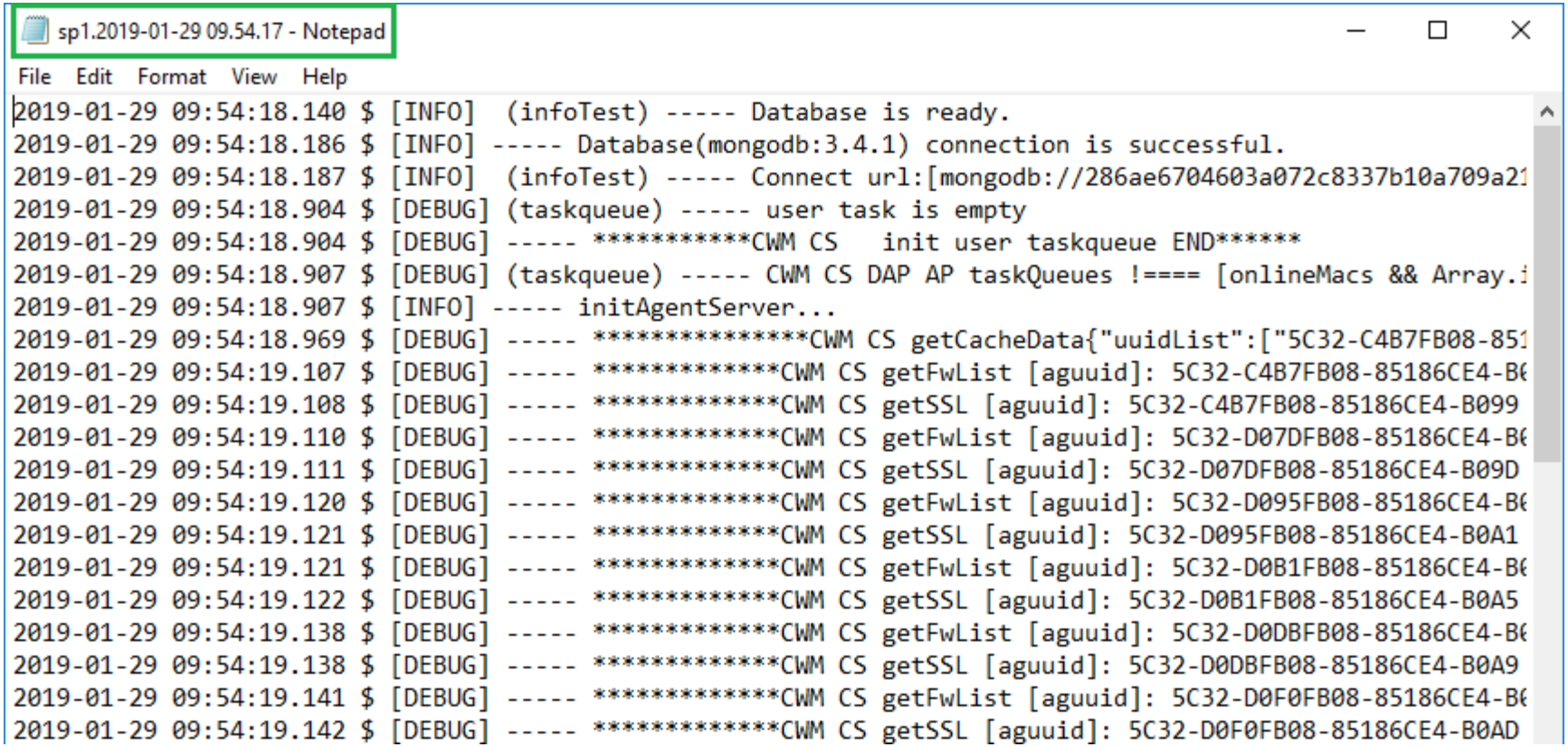
- Nuclias Connect Core Server Log Backup folder path



- D-Track DK1800023: In CWM 1.03 r0098, the log file naming convention is "stdout_xxxx-x-xx xx-xx-xx.txt"

Nuclias Connect Core Server Log

- Nuclias Connect Core Server Log content (an example from our lab practice)



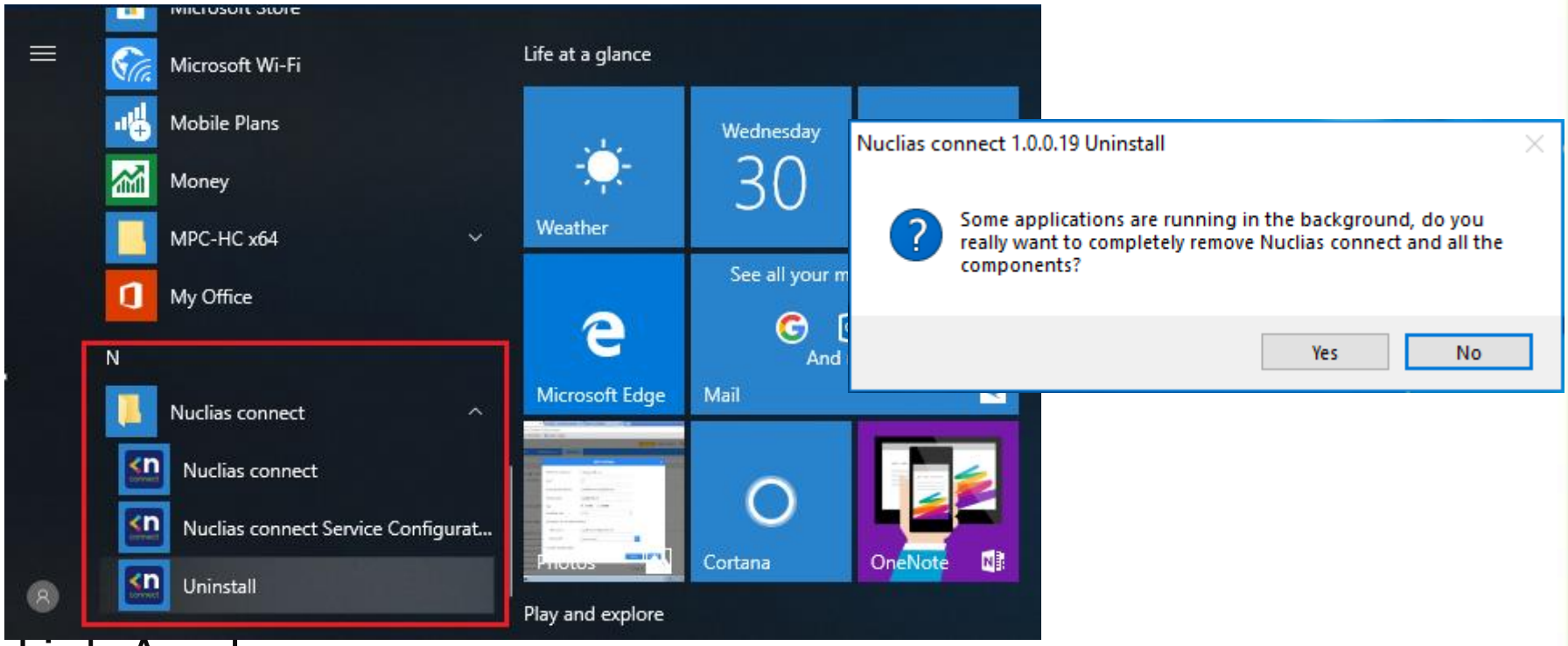
User Management, Access Control and System Administration

System Administration

- SMTP Settings for Sending Mail
- System Redundancy
- Log Backup
- Uninstall Nuclias Connect Server System

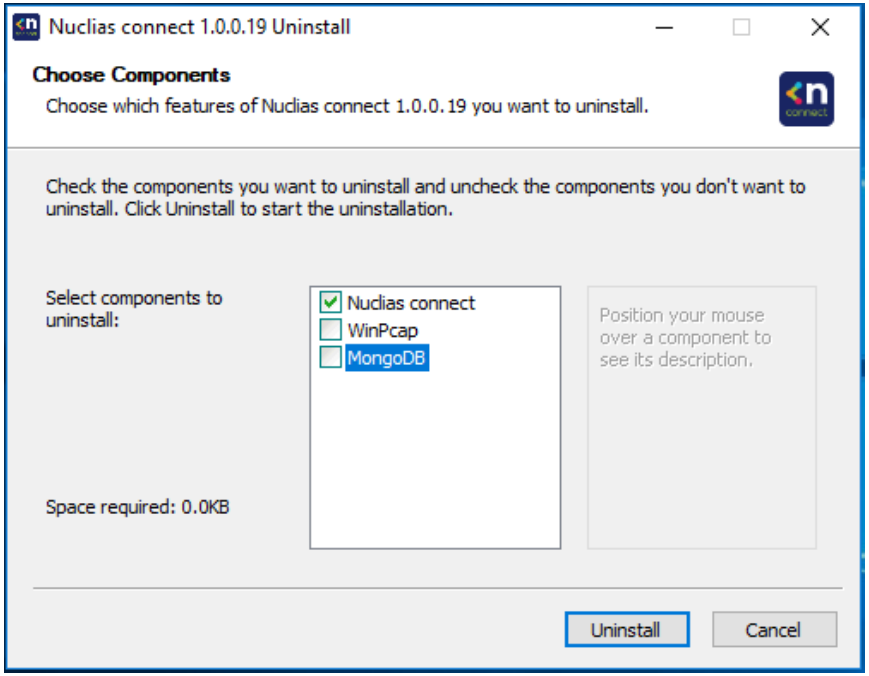
Uninstall Nuclias Connect Server System

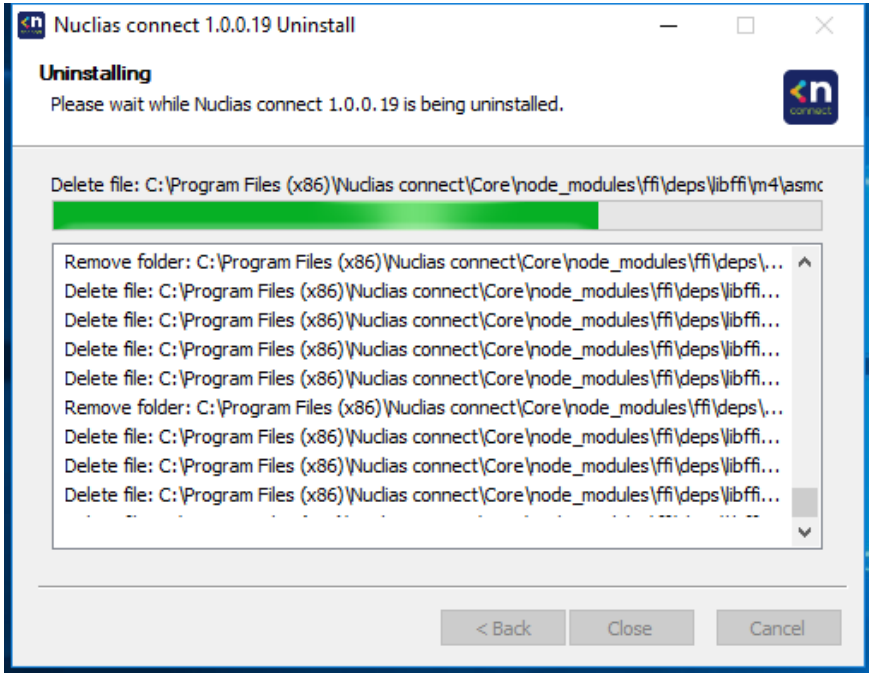
- Should we have reason to decide to uninstall an existing DNC server systems, we could use the Uninstall shortcut, as pointed below.
  - Uninst.exe file is going to be launched.



Uninstall Nuclias Connect Server System

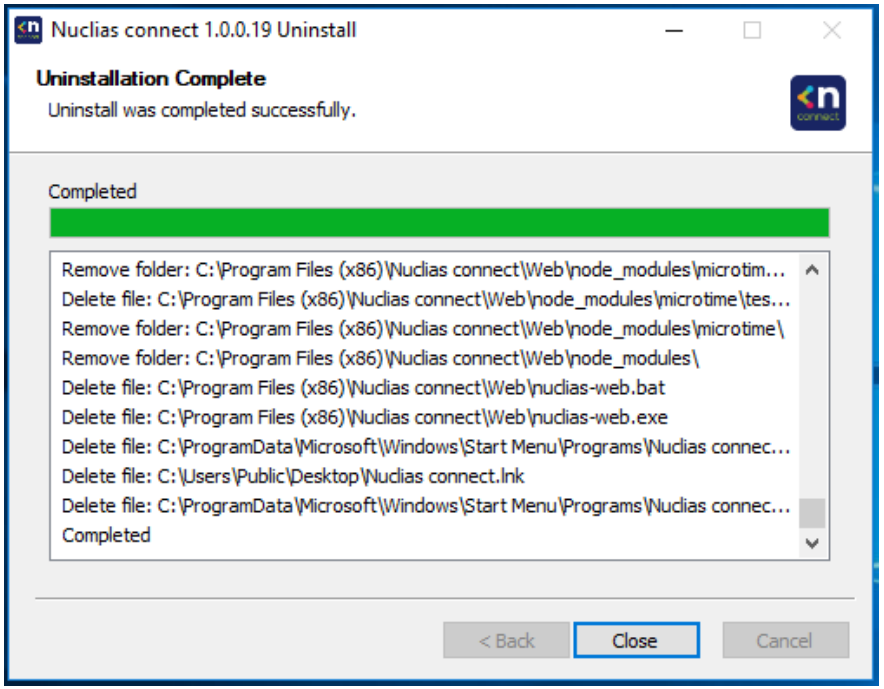
- Should we have reason to decide to uninstall an existing DNC server systems, we could use the Uninstall shortcut, as pointed below.
  - Uninst.exe file is going to be launched.

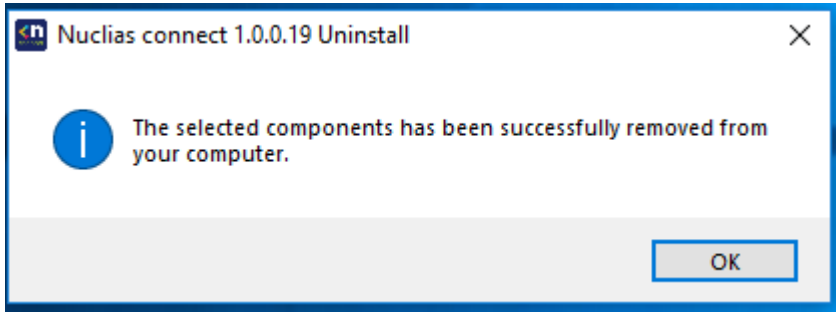




Uninstall Nuclias Connect Server System

- Full Uninstall complete



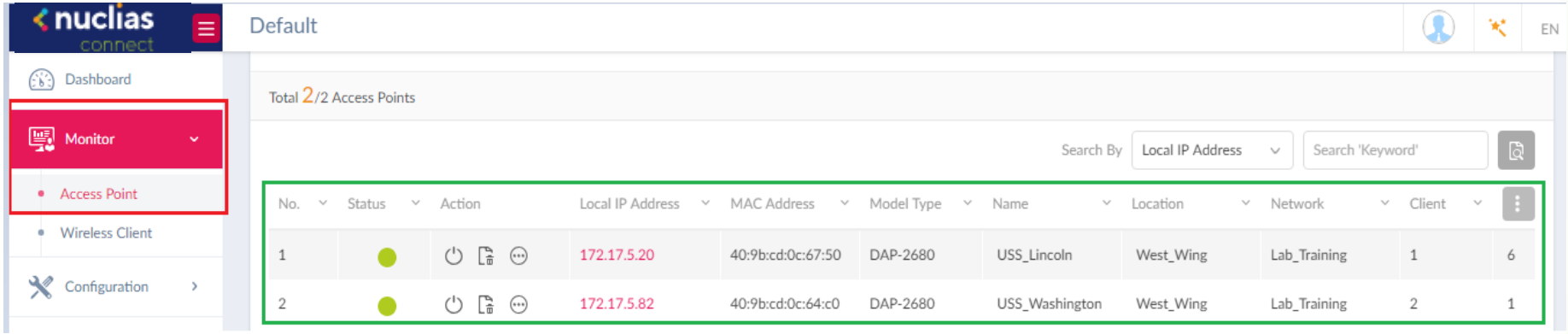


Nuclias Connect Hands-on Tutorial

- Nuclias Connect Product Bulletin
  - What's New In The Latest Release
  - The Installation Process
  - Supported Devices and Plan
- Setup Wizard and Basic Connection
  - Nuclias Connect Setup Wizard and AP Discovery
  - Basic WLAN Connection Settings and Verifications
- The Design Thinking of Dashboard and Report
- Case Studies
- Hands-on Laboratory Scenarios and Troubleshooting
  - Wireless Profile Settings and Verifications
  - User Management, Access Control, and System Administration
  - Access Points Device Management

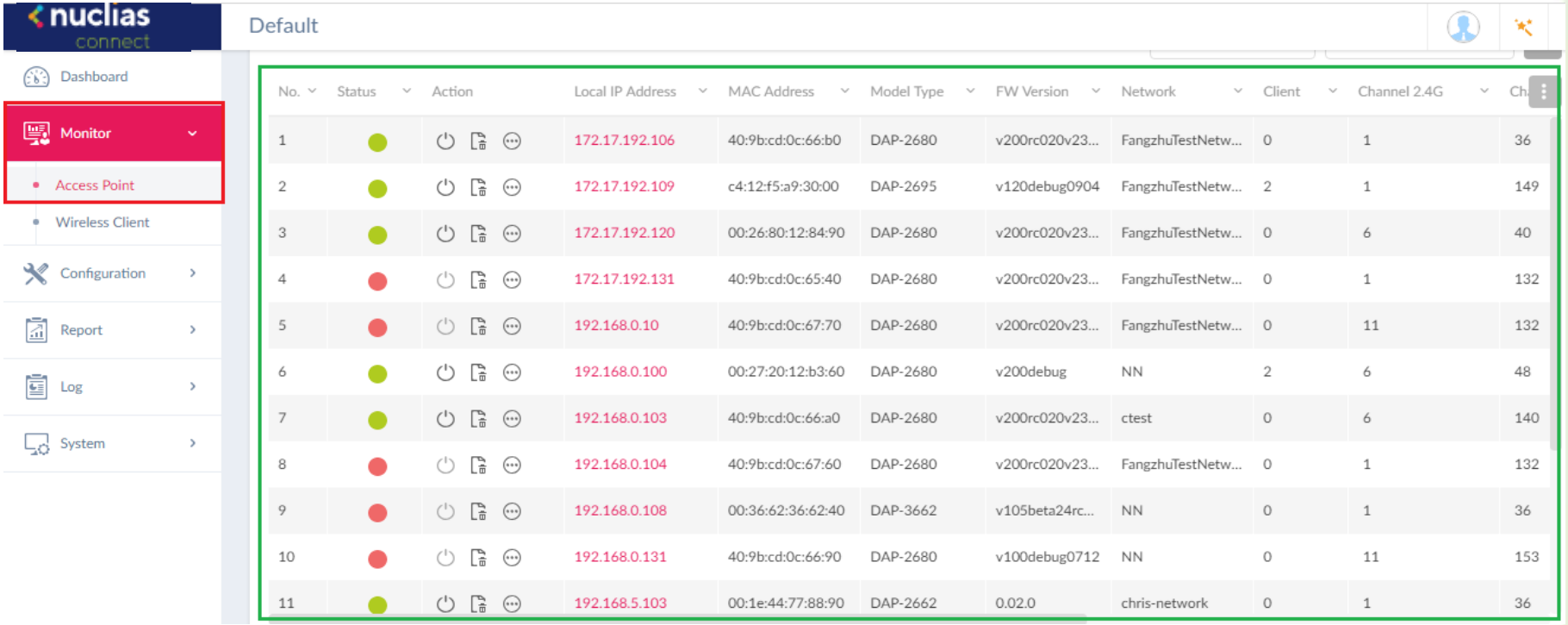
A List of Access Points

- The Access Point List page is under the Monitor tab.
- The objective is to monitor the status of DAP Access Points within our network topology.
  - We are able to check the lighting device status in real time.
  - Nuclias Connect offers an easy way to find, sort and filter APs in a large network.



A List of Access Points

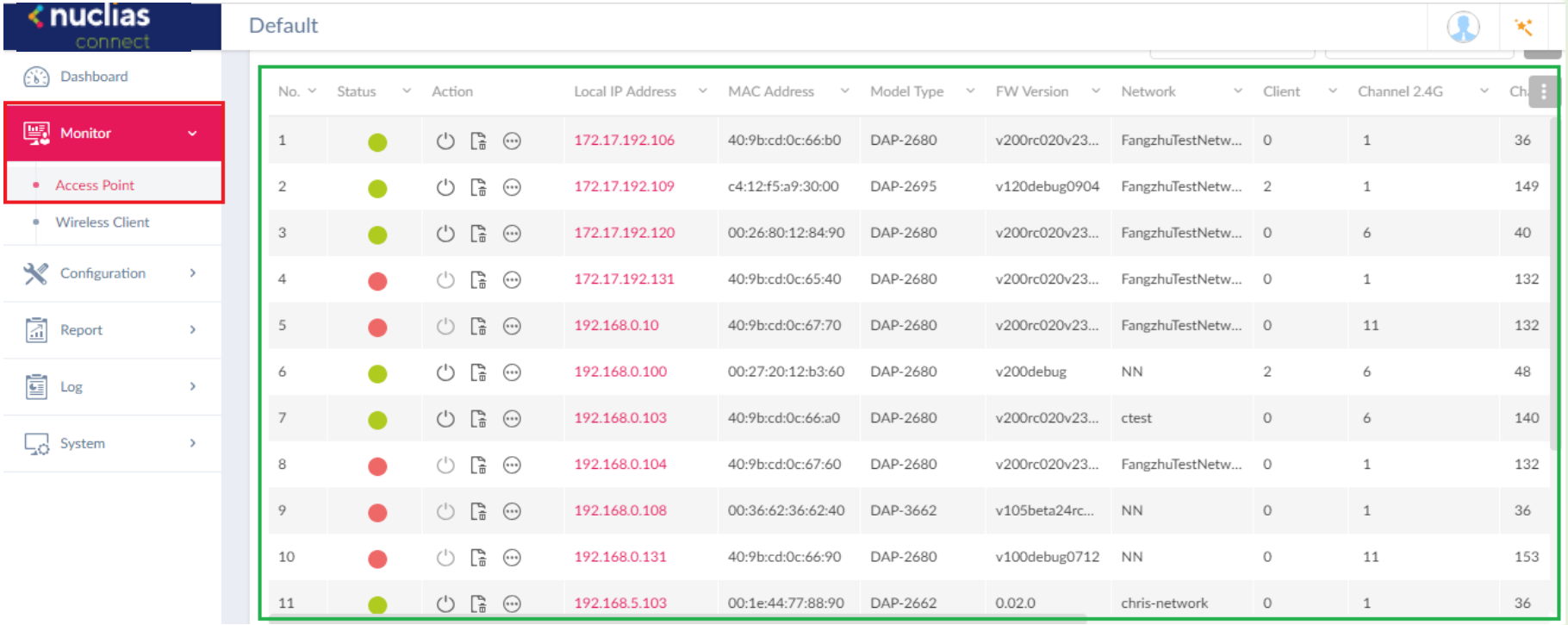
- Access Point List (live example in production environment).



No.	Status	Action	Local IP Address	MAC Address	Model Type	FW Version	Network	Client	Channel 2.4G	Ch
1			172.17.192.106	40:9b:cd:0c:66:b0	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	1	36
2			172.17.192.109	c4:12:f5:a9:30:00	DAP-2695	v120debug0904	FangzhuTestNetw...	2	1	149
3			172.17.192.120	00:26:80:12:84:90	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	6	40
4			172.17.192.131	40:9b:cd:0c:65:40	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	1	132
5			192.168.0.10	40:9b:cd:0c:67:70	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	11	132
6			192.168.0.100	00:27:20:12:b3:60	DAP-2680	v200debug	NN	2	6	48
7			192.168.0.103	40:9b:cd:0c:66:a0	DAP-2680	v200rc020v23...	ctest	0	6	140
8			192.168.0.104	40:9b:cd:0c:67:60	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	1	132
9			192.168.0.108	00:36:62:36:62:40	DAP-3662	v105beta24rc...	NN	0	1	36
10			192.168.0.131	40:9b:cd:0c:66:90	DAP-2680	v100debug0712	NN	0	11	153
11			192.168.5.103	00:1e:44:77:88:90	DAP-2662	0.02.0	chris-network	0	1	36

A List of Access Points

- Access Point List (live example in production environment).



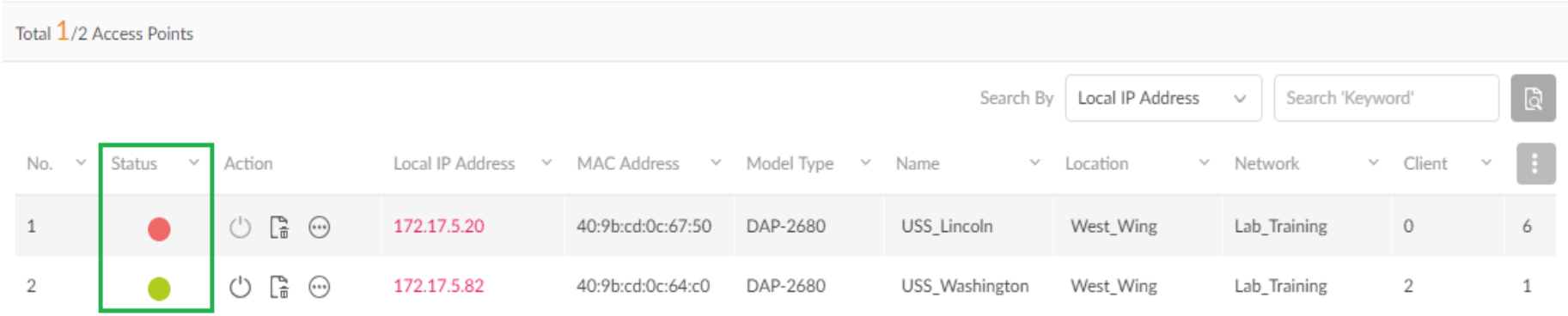
No.	Status	Action	Local IP Address	MAC Address	Model Type	FW Version	Network	Client	Channel 2.4G	Ch
1			172.17.192.106	40:9b:cd:0c:66:b0	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	1	36
2			172.17.192.109	c4:12:f5:a9:30:00	DAP-2695	v120debug0904	FangzhuTestNetw...	2	1	149
3			172.17.192.120	00:26:80:12:84:90	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	6	40
4			172.17.192.131	40:9b:cd:0c:65:40	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	1	132
5			192.168.0.10	40:9b:cd:0c:67:70	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	11	132
6			192.168.0.100	00:27:20:12:b3:60	DAP-2680	v200debug	NN	2	6	48
7			192.168.0.103	40:9b:cd:0c:66:a0	DAP-2680	v200rc020v23...	ctest	0	6	140
8			192.168.0.104	40:9b:cd:0c:67:60	DAP-2680	v200rc020v23...	FangzhuTestNetw...	0	1	132
9			192.168.0.108	00:36:62:36:62:40	DAP-3662	v105beta24rc...	NN	0	1	36
10			192.168.0.131	40:9b:cd:0c:66:90	DAP-2680	v100debug0712	NN	0	11	153
11			192.168.5.103	00:1e:44:77:88:90	DAP-2662	0.02.0	chris-network	0	1	36

To avoid poor wireless performance as a result of co-channel interference, adjacent Wi-Fi APs shall be use non-overlapping channels.

A List of Access Points

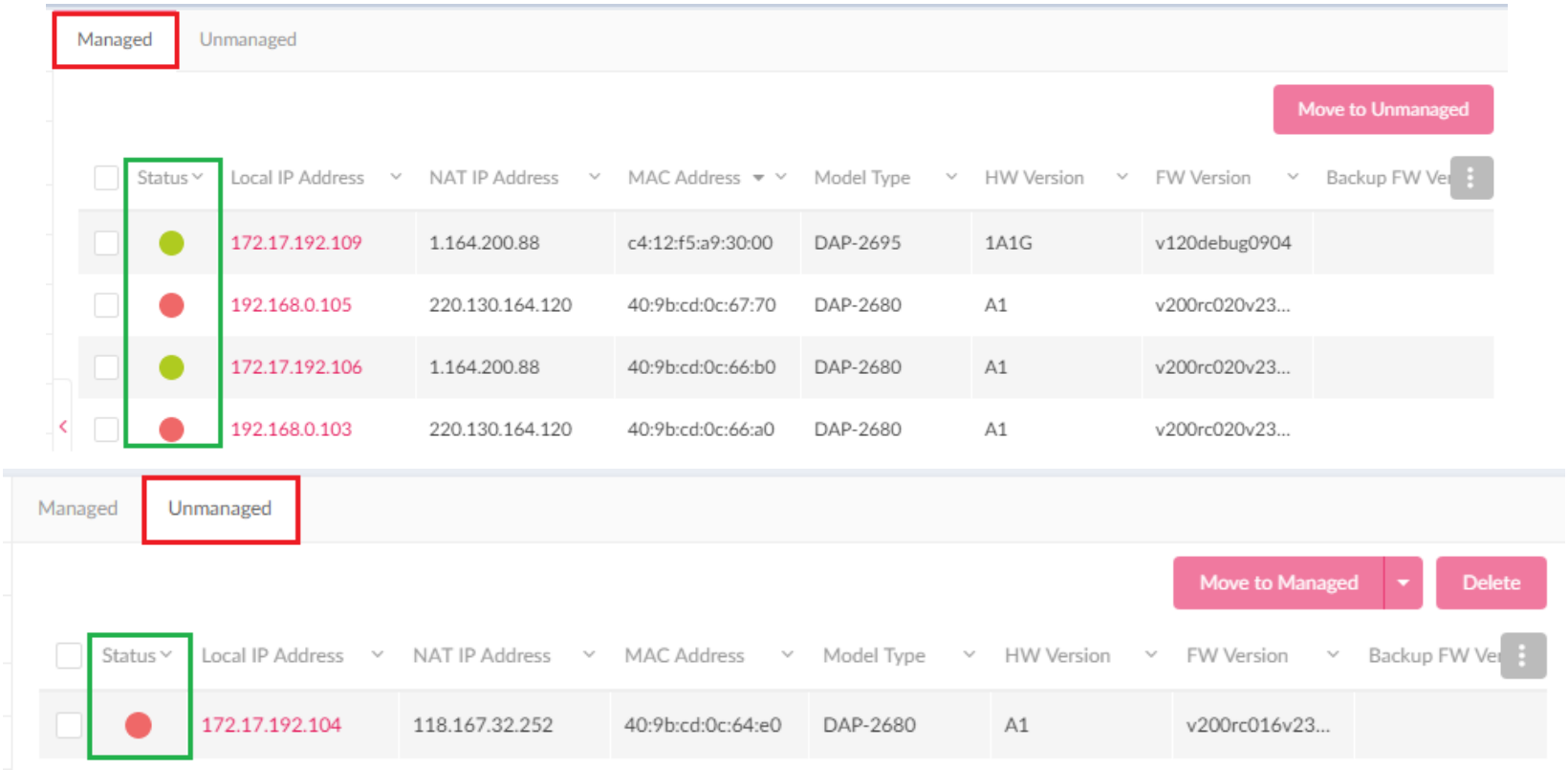
The status of the AP is indicated by its color, for example

- YellowGreen: The AP is connected to network, but not reporting any problems.
- IndianRed: The AP is currently offline (down status)



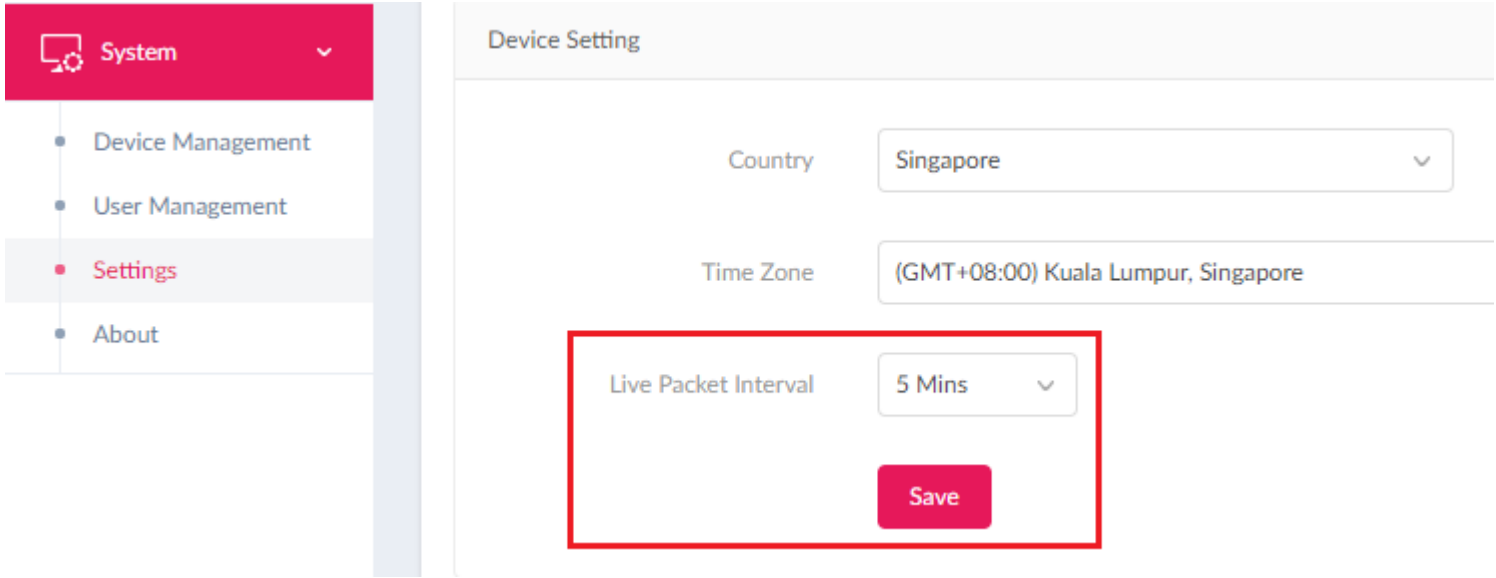
A List of Access Points

- The same Access Point Color Codes apply to Device Management page under the System tab.



Live Packet Interval (1/2)

- Live Packet Interval is a parameter to define time periods individual AP responds to Nuclias Connect on its (DAP) activities.
- The following diagram indicates 5-min Live Packet Interval settings, collaborating with Wireshark capture.



Live Packet Interval (2/2)

- Live Packet Interval is a parameter to define time periods individual AP responds to Nuclias Connect on its (DAP) activities.
- The following diagram indicates 5-min Live Packet Interval settings, collaborating with Wireshark capture.
  - Nuclias Connect: 172.17.5.10
  - DAP-2680: 172.17.5.93

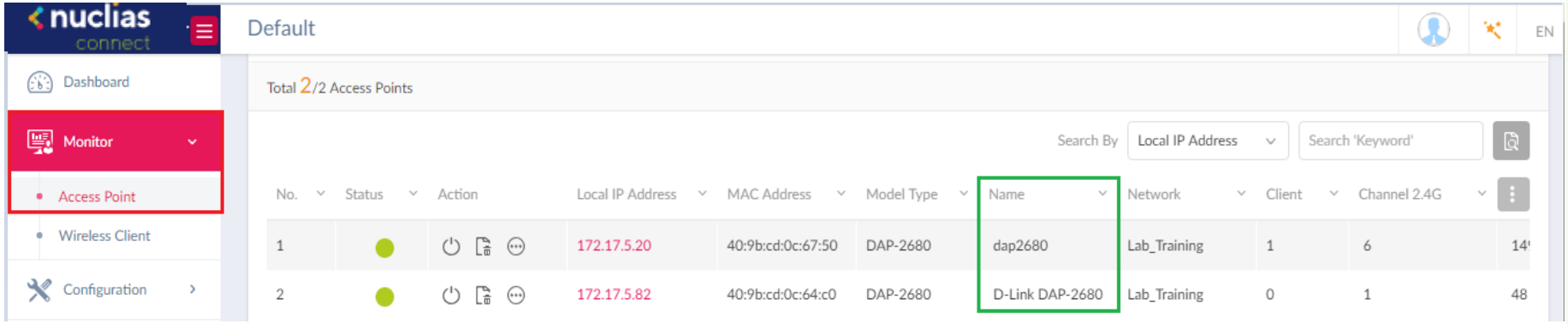
Watch out the column of "Time"

ip.src == 172.17.5.10 && ip.dst == 172.17.5.93

No.	Time	Source	Destination	Protocol	Info
3322	2019-01-07 13:53:08.603083	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=1 Ack=1466 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
5378	2019-01-07 13:54:39.722461	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=1 Ack=2933 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
6306	2019-01-07 13:55:25.789587	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=1 Ack=3113 Win=2052 [TCP CHECKSUM INCORRECT] Len=0
6307	2019-01-07 13:55:25.802054	172.17.5.10	172.17.5.93	TLSv1.2	Application Data
7463	2019-01-07 13:56:09.901413	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=141 Ack=4585 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
9627	2019-01-07 13:57:41.008310	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=141 Ack=6059 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
11650	2019-01-07 13:59:12.121662	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=141 Ack=7536 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
12998	2019-01-07 14:00:27.196025	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=141 Ack=7716 Win=2052 [TCP CHECKSUM INCORRECT] Len=0
12999	2019-01-07 14:00:27.212129	172.17.5.10	172.17.5.93	TLSv1.2	Application Data
13357	2019-01-07 14:00:43.292223	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=281 Ack=9195 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
15403	2019-01-07 14:02:14.408205	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=281 Ack=10675 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
21537	2019-01-07 14:03:45.518538	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=281 Ack=12154 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
23407	2019-01-07 14:05:16.627526	172.17.5.10	172.17.5.93	TCP	8443 → 35079 [ACK] Seq=281 Ack=13633 Win=2053 [TCP CHECKSUM INCORRECT] Len=0
23665	2019-01-07 14:05:28.649169	172.17.5.10	172.17.5.93	TLSv1.2	Application Data

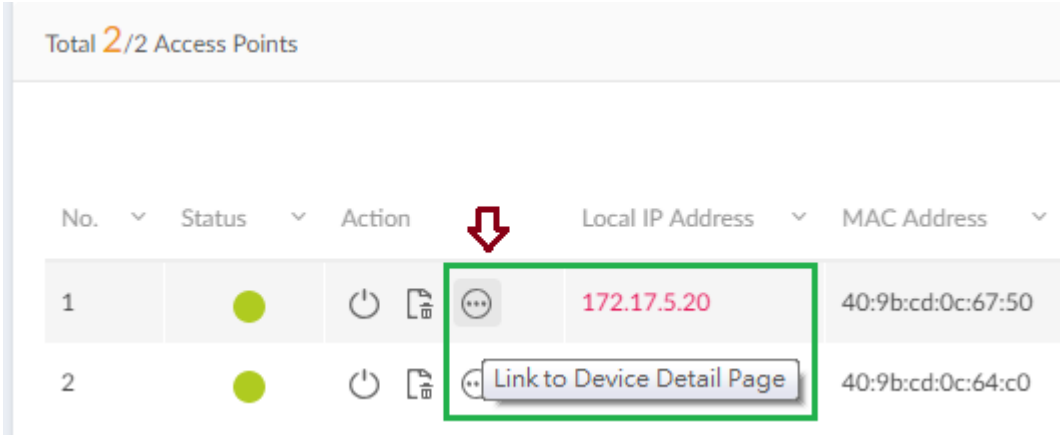
DAP Device Name Lab Practice (1/4)

- DAP Device Name lab practice
- Menu: Monitor > Access Point, we have seen the list of managed devices and have reason to believe “device name” update necessary



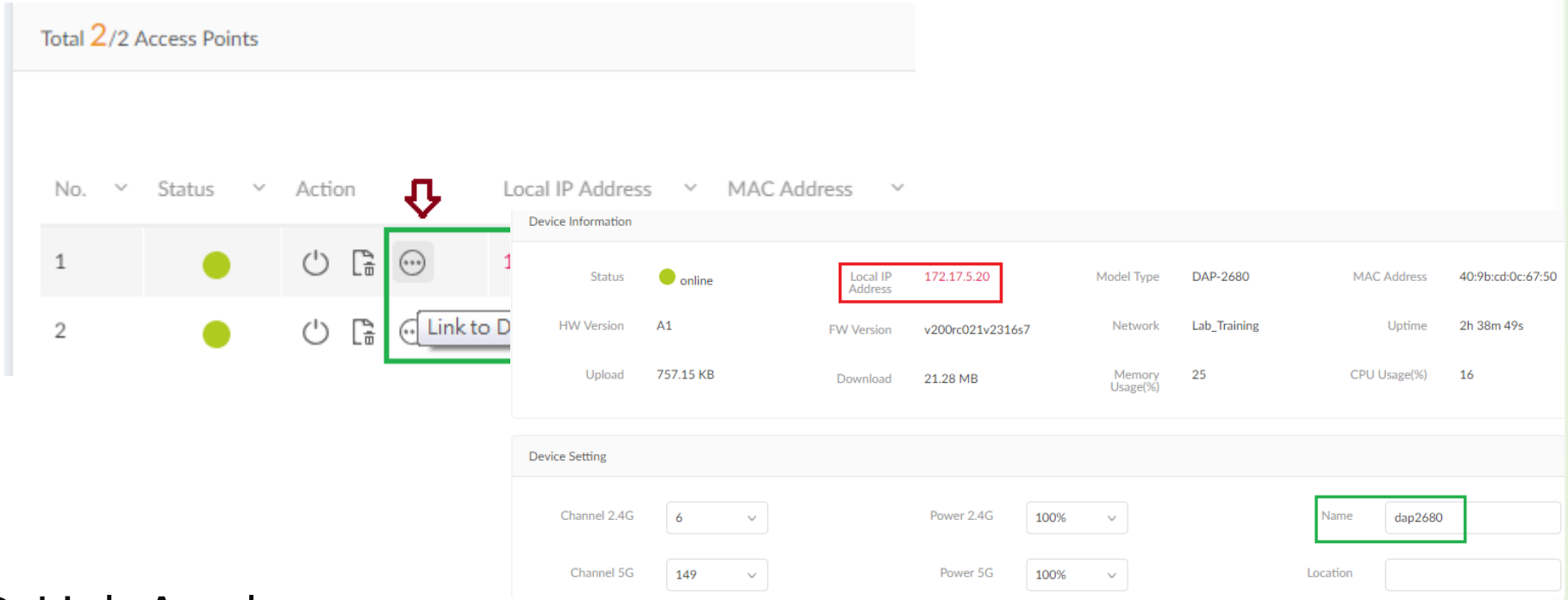
DAP Device Name Lab Practice (2/4)

- DAP Device Name lab practice
- We have decided using the following parameters
  - DAP-2680, IP: 172.17.5.20, device name: USS_Lincoln
  - DAP-2680, IP: 172.17.5.82, device name: USS_Washington



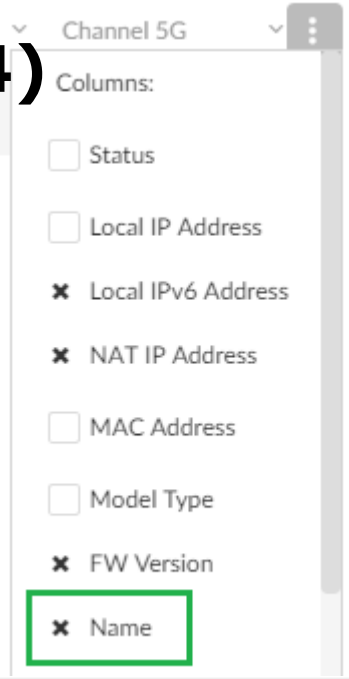
DAP Device Name Lab Practice (3/4)

- DAP Device Name lab practice
- We have decided using the following parameters
  - DAP-2680, IP: 172.17.5.20, device name: USS_Lincoln
  - DAP-2680, IP: 172.17.5.82, device name: USS_Washington



DAP Device Name Lab Practice (4/4)

- DAP Device Name lab practice
- Device name configuration verifications
  - Select the Name column, if necessary



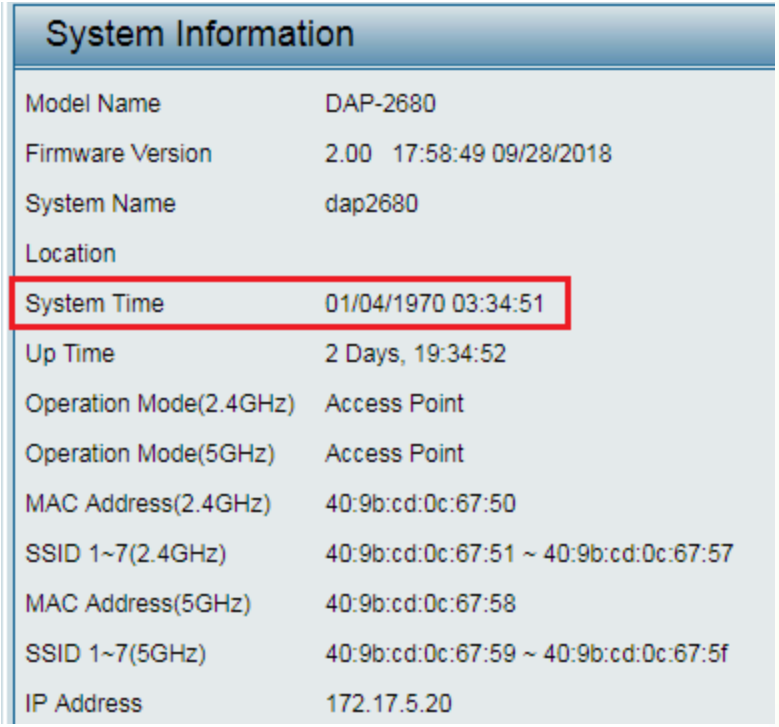
Total 2/2 Access Points

Search By Local IP Address Search 'Keyword'

No.	Status	Action	Local IP Address	MAC Address	Model Type	Name	Network	Client	Channel 2.4G
1			172.17.5.20	40:9b:cd:0c:67:50	DAP-2680	USS_Lincoln	Lab_Training	1	6
2			172.17.5.82	40:9b:cd:0c:64:c0	DAP-2680	USS_Washington	Lab_Training	0	1

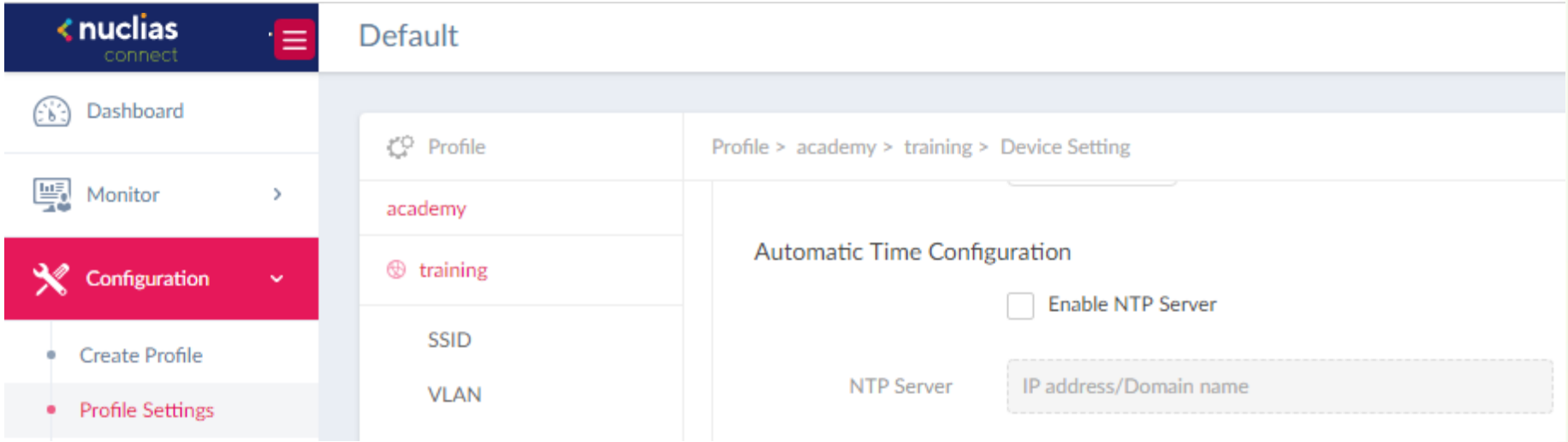
DAP System Time Lab Practice (1/5)

- DAP System Time lab practice
- Within our lab facility, the DAP System Time is shown as "01/04/1970 03:34:51," which of course is not a proper display



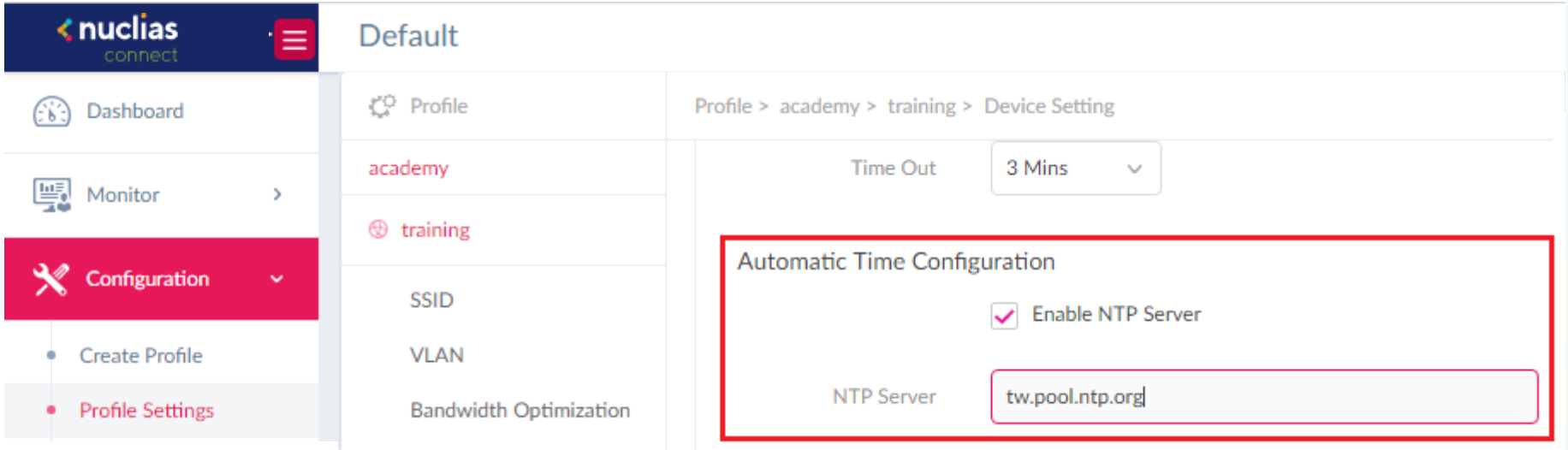
DAP System Time Lab Practice (2/5)

- DAP System Time lab practice
- We have decided to utilize DNC's feature to set up System Time (Menu: Configuration, Profile Setting, Profile > academy > training > Device Setting)



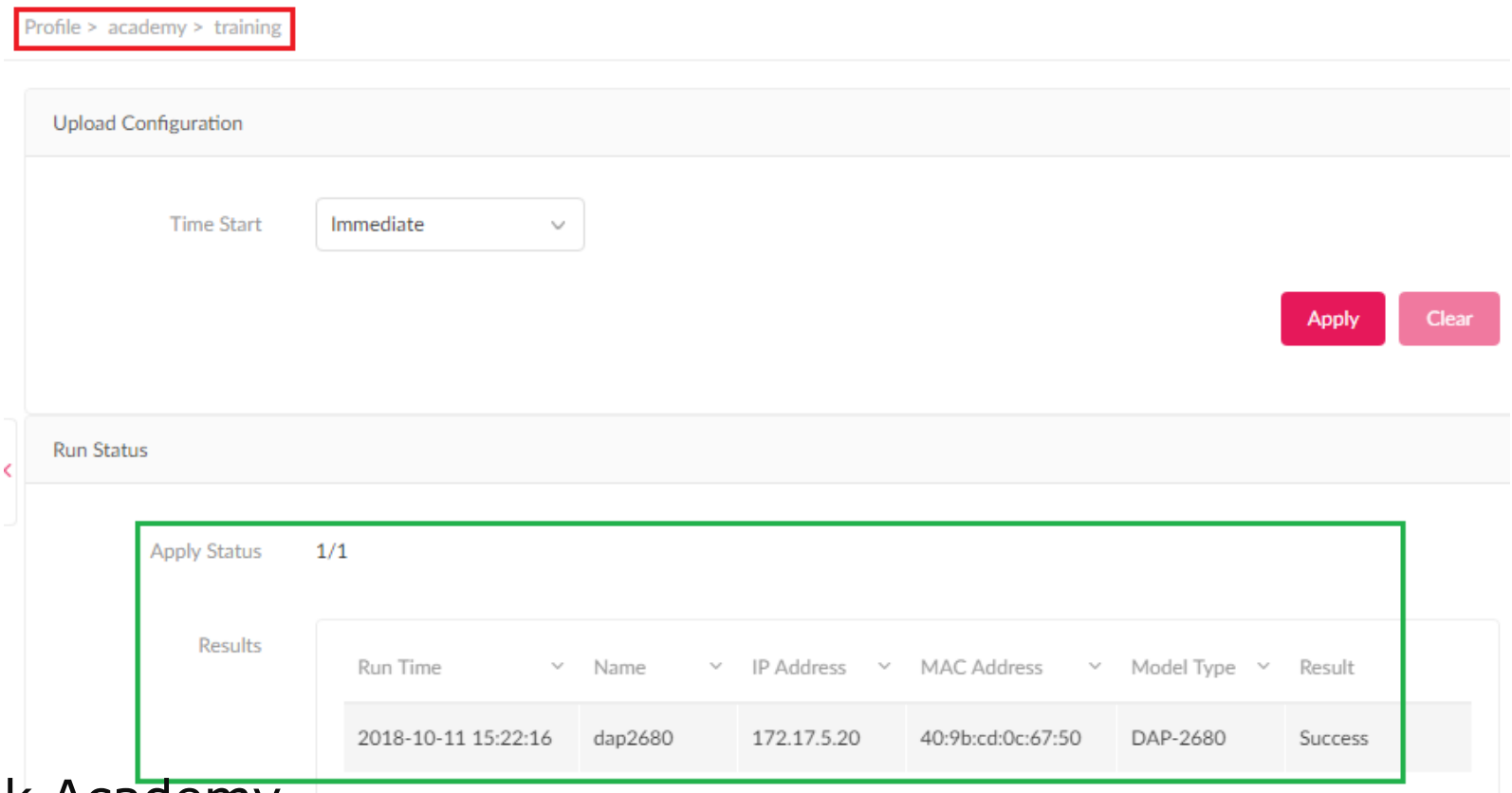
DAP System Time Lab Practice (3/5)

- DAP System Time lab practice
- We have decided to utilize DNC's feature to set up System Time (Menu: Configuration, Profile Setting, Profile > academy > training > Device Setting)
  - tw.pool.ntp.org



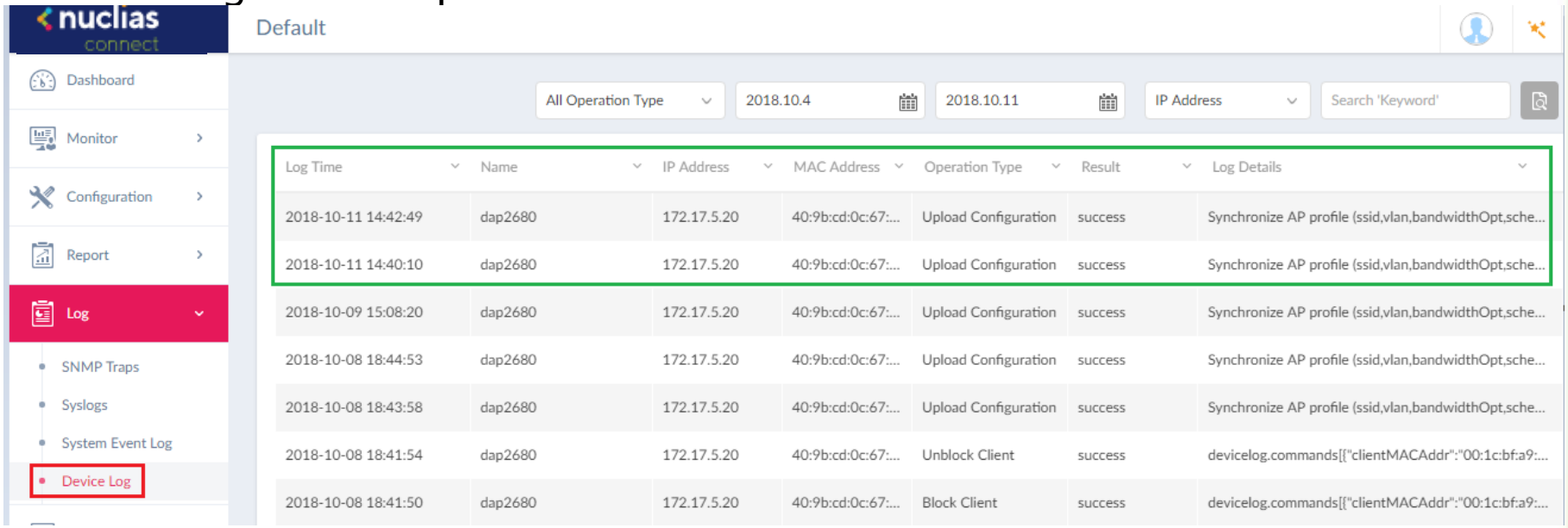
DAP System Time Lab Practice (4/5)

- DAP System Time lab practice
- Configuration upload status verification



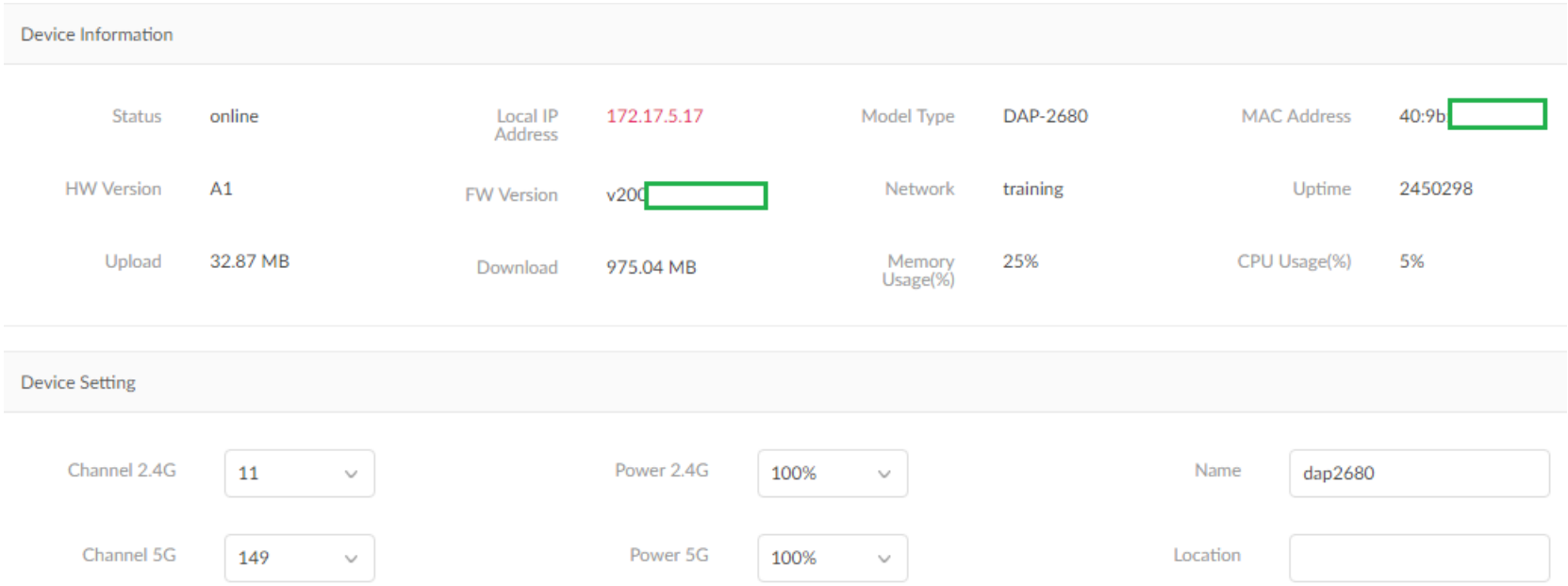
DAP System Time Lab Practice (5/5)

- DAP System Time lab practice
- Configuration upload status verification



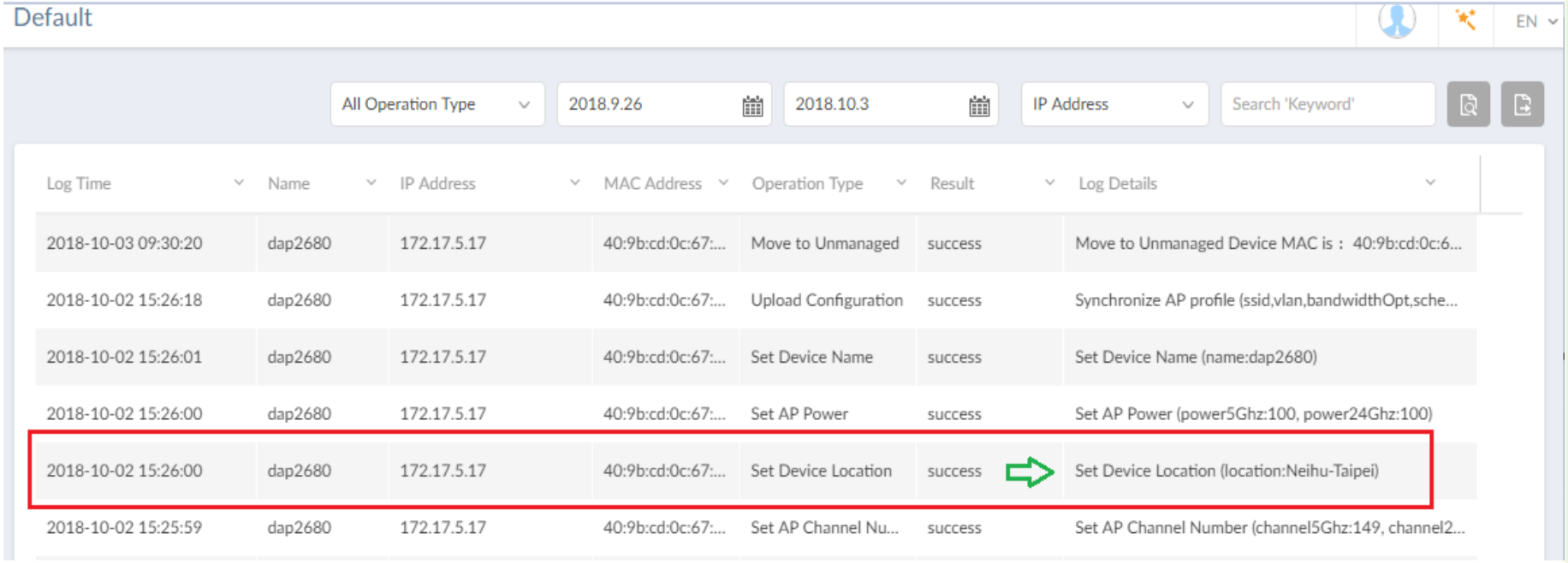
Access Points Device Management

- Under the menu of Report, Most active AP, we will see “device location” information.
- The place to update its message is in Monitor > Access Point > Link to Device Detail Page.



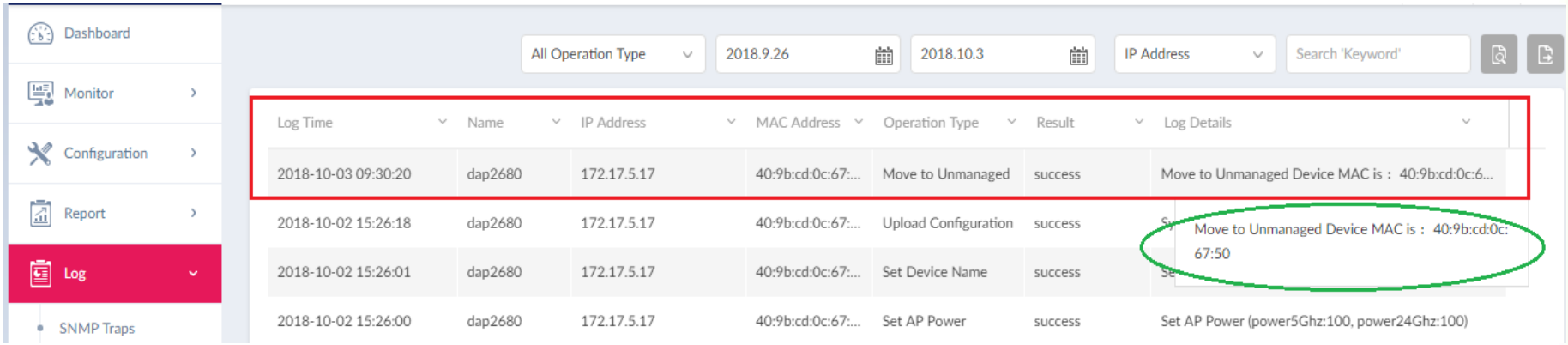
Access Points Device Management

- Device Log
- Under the menu of Log > Device Log, we are able to view the record shown the update of device location.



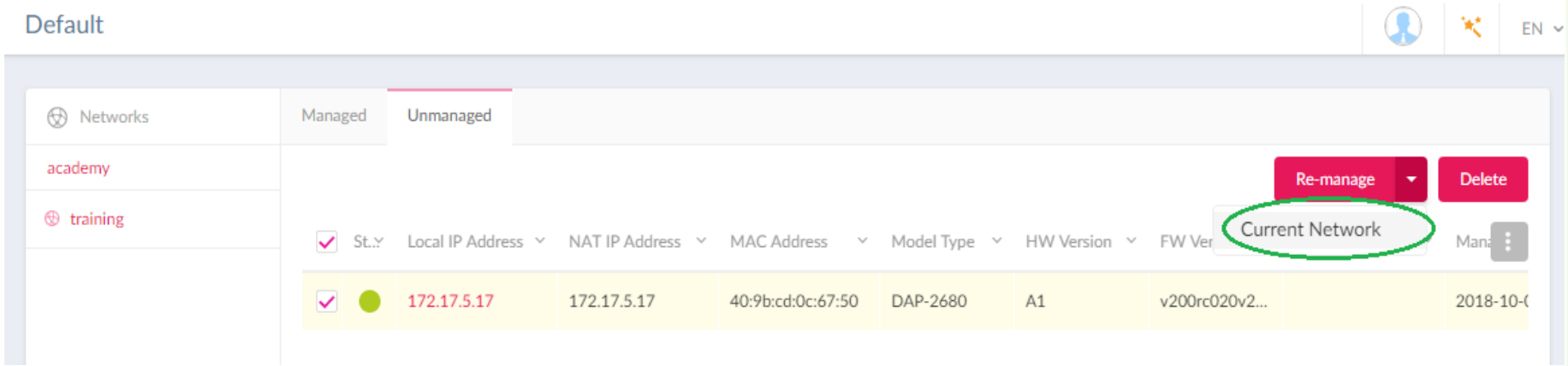
Access Points Device Management

- The AP management mode is modified from Managed to Unmanaged mode.



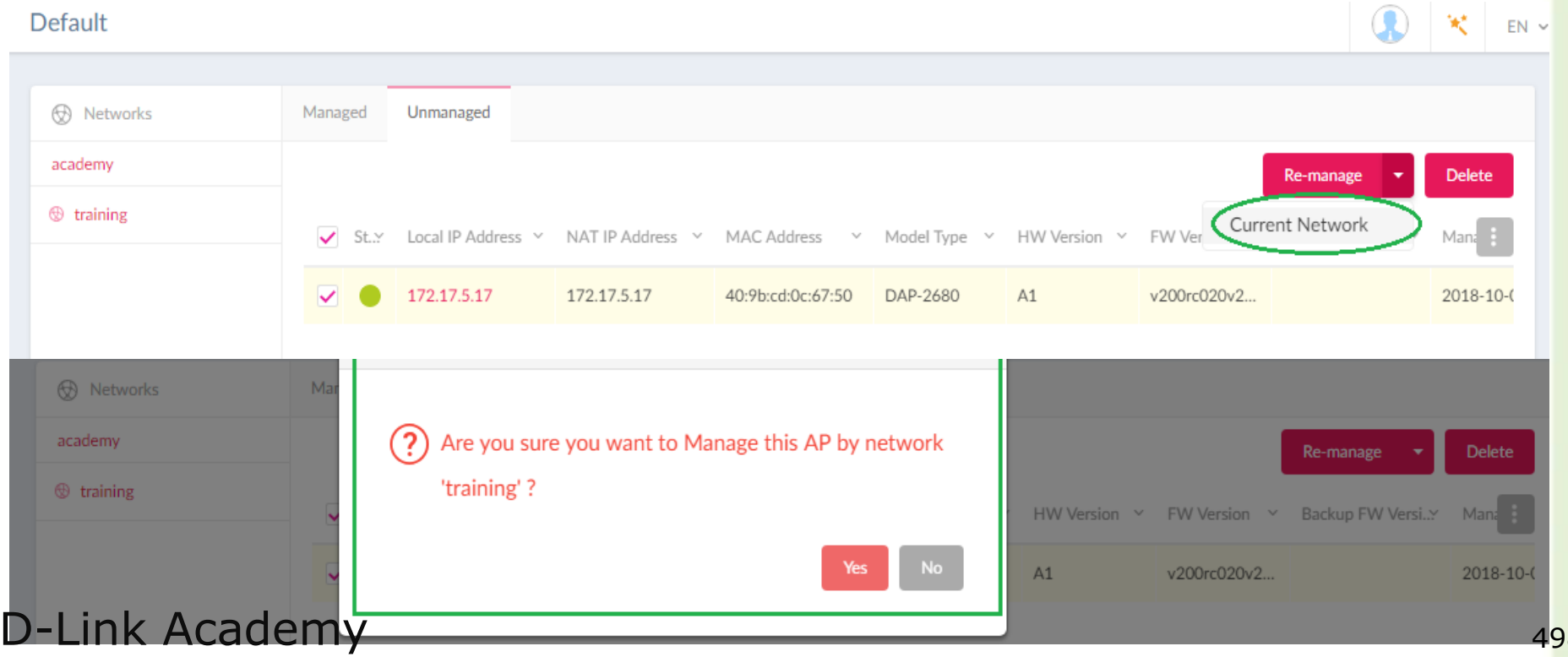
Access Points Device Management

- Should you desire to make an unmanaged device back to managed mode, what you should do is go to the menu of System > Device Management > Unmanaged tab, select the device and then click on the "Re-Manage" button.



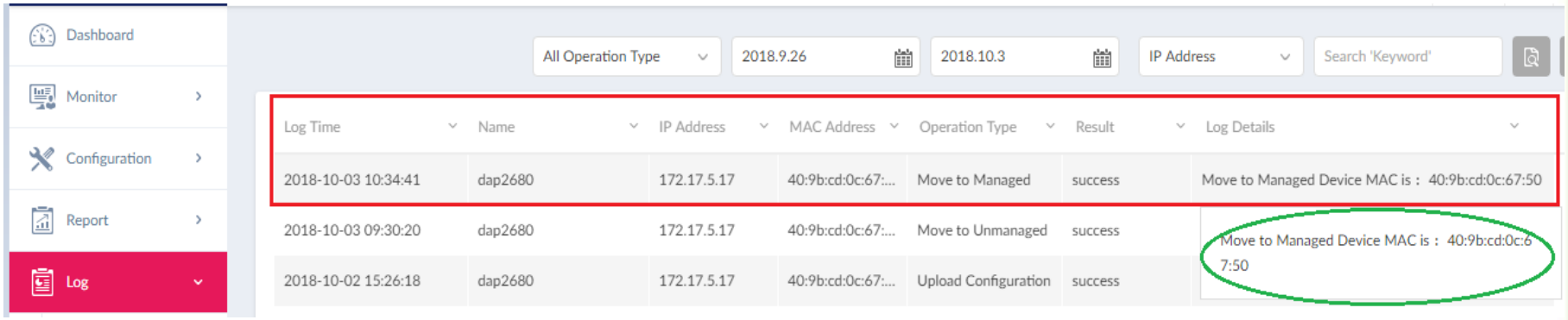
Access Points Device Management

- Should you desire to make an unmanaged device back to managed mode, what you should do is go to the menu of System > Device Management > Unmanaged tab, select the device and then click on the "Re-Manage" button.



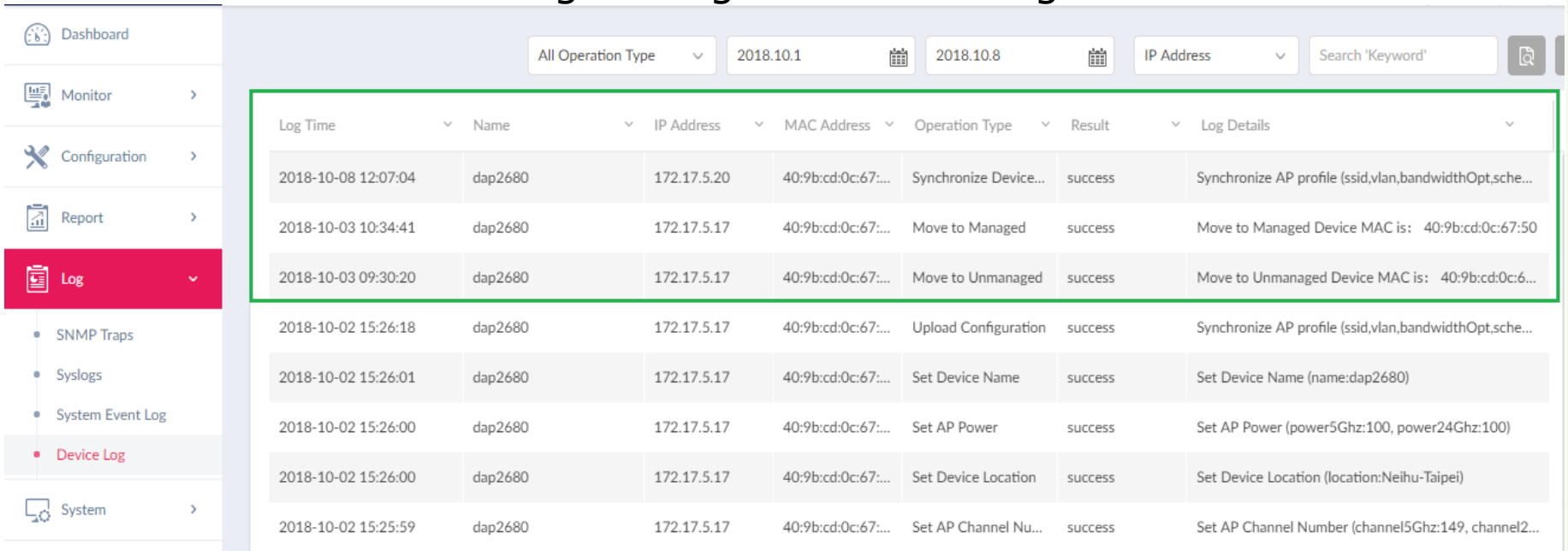
Access Points Device Management

- The Device Log in Nuclias Connect system also reflects the latest configuration status.



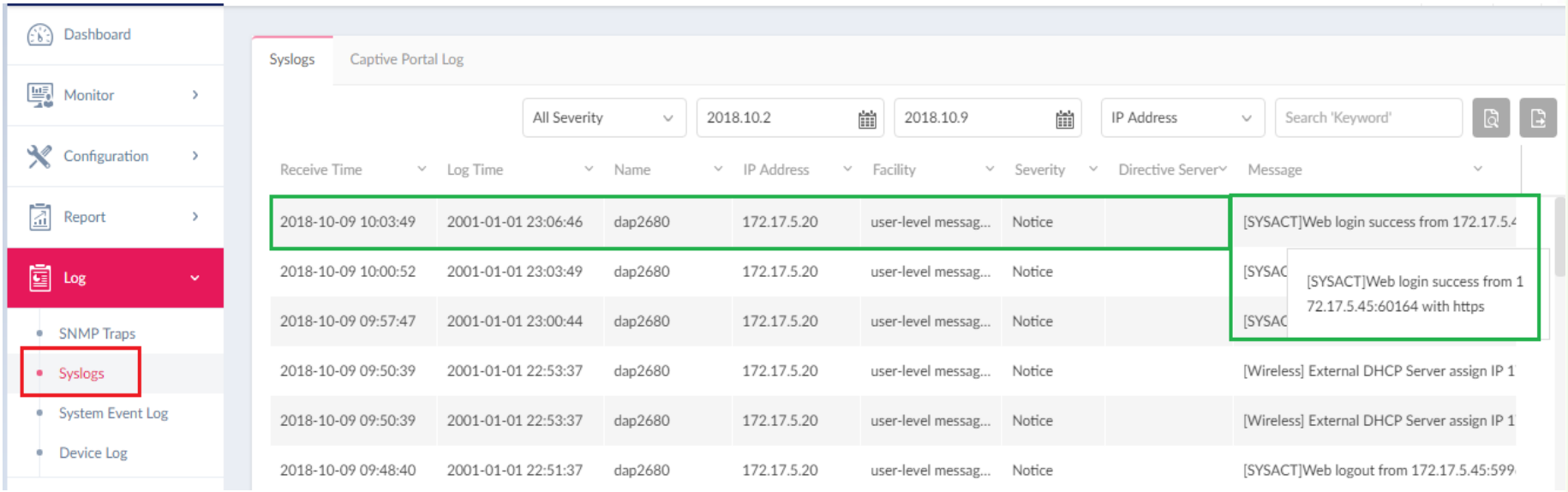
Access Points Device Management

- The below image screen shot is another example of DAP's status (from unmanaged to be managed)
  - On the Device Log settings under the Log tab



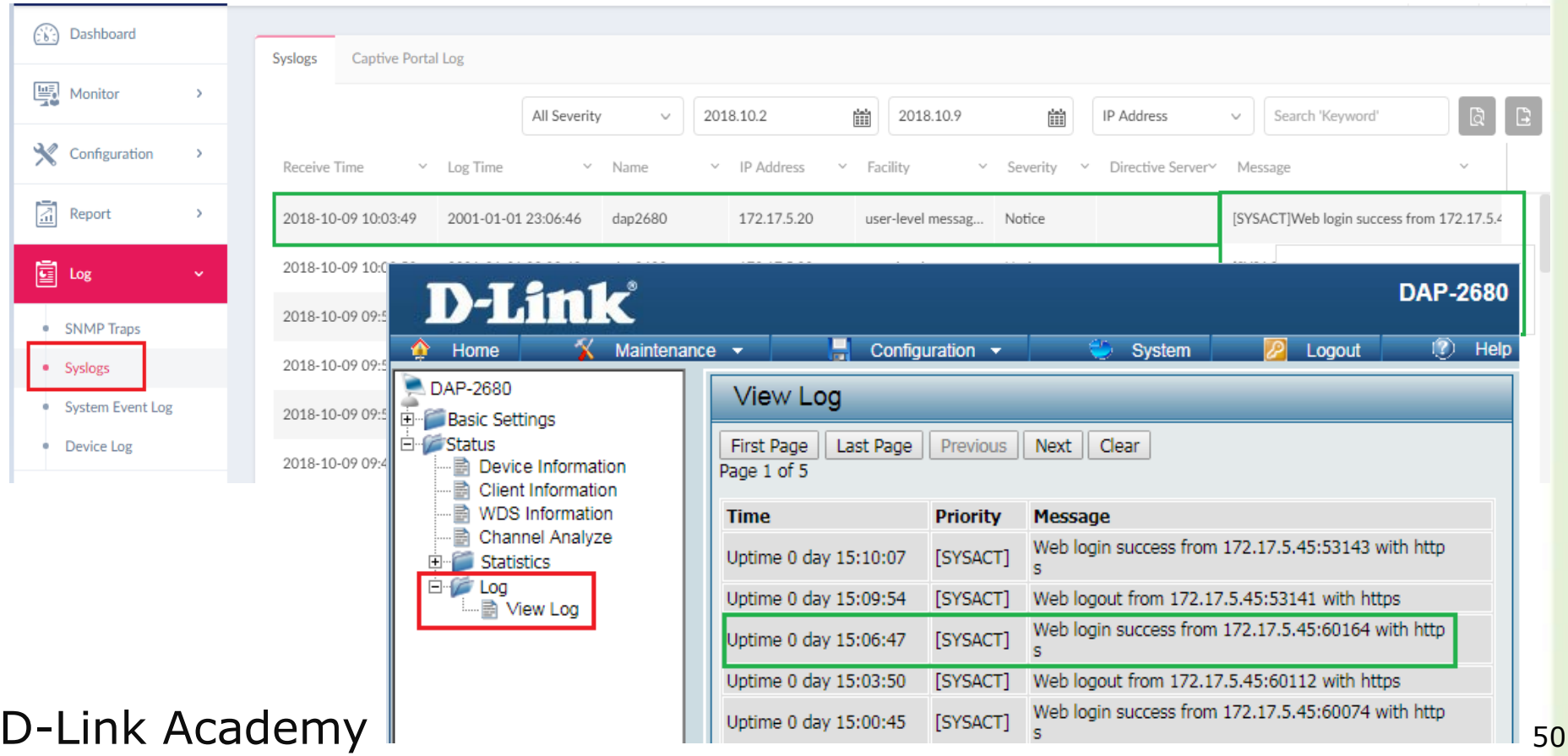
Access Points Device Management

- The SysLogs information (under menu of Log) in Nuclias Connect directly retrieves from DAP GUI View Log.



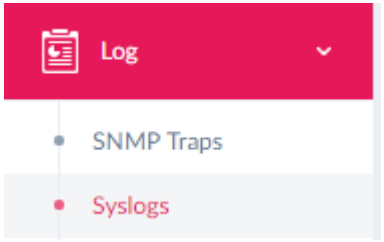
Access Points Device Management

- The SysLogs information (under menu of Log) in Nuclias Connect directly retrieves from DAP GUI View Log.



Log, 5G Group Key Update Discussion (1/2)

- In Nuclias Connect, we have seen constant 5GHz Group key update on the Syslog page under the Log tab.
- What kind of configuration parameter(s) would possibly bringing such situation?

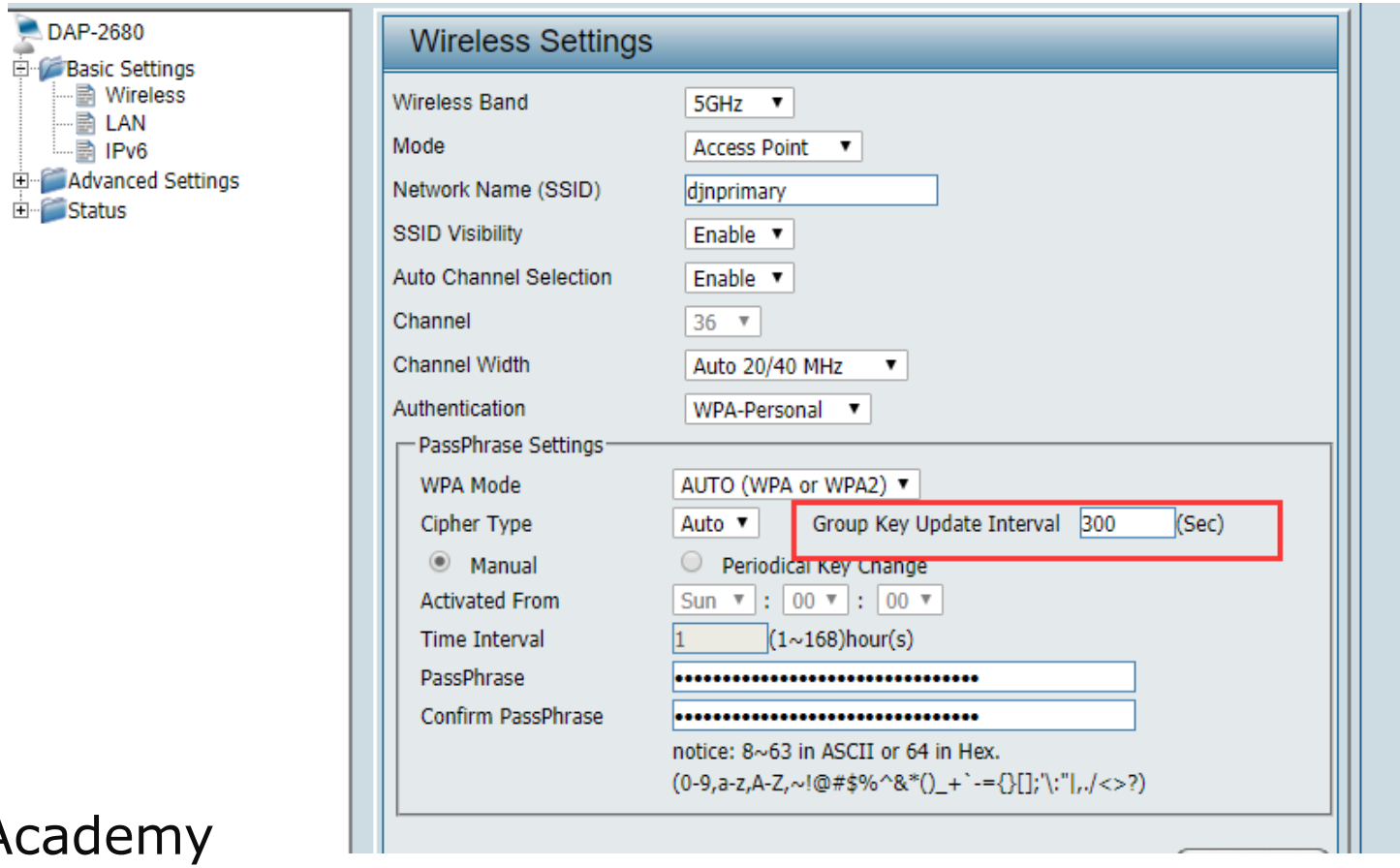


2018-10-29 03:00:21	2001-01-01 15:26:54	dap2680	172.17.192.140	kernel messages	Information		[Wireless] 5G:Group key update start:ST...
2018-10-29 02:55:22	2001-01-01 15:21:54	dap2680	172.17.192.140	kernel messages	Notice		[Wi
2018-10-29 02:55:22	2001-01-01 15:21:54	dap2680	172.17.192.140	kernel messages	Information		[Wi

[Wireless] 5G:Group key update start:S
TA 00:21:6a:65:e0:a2

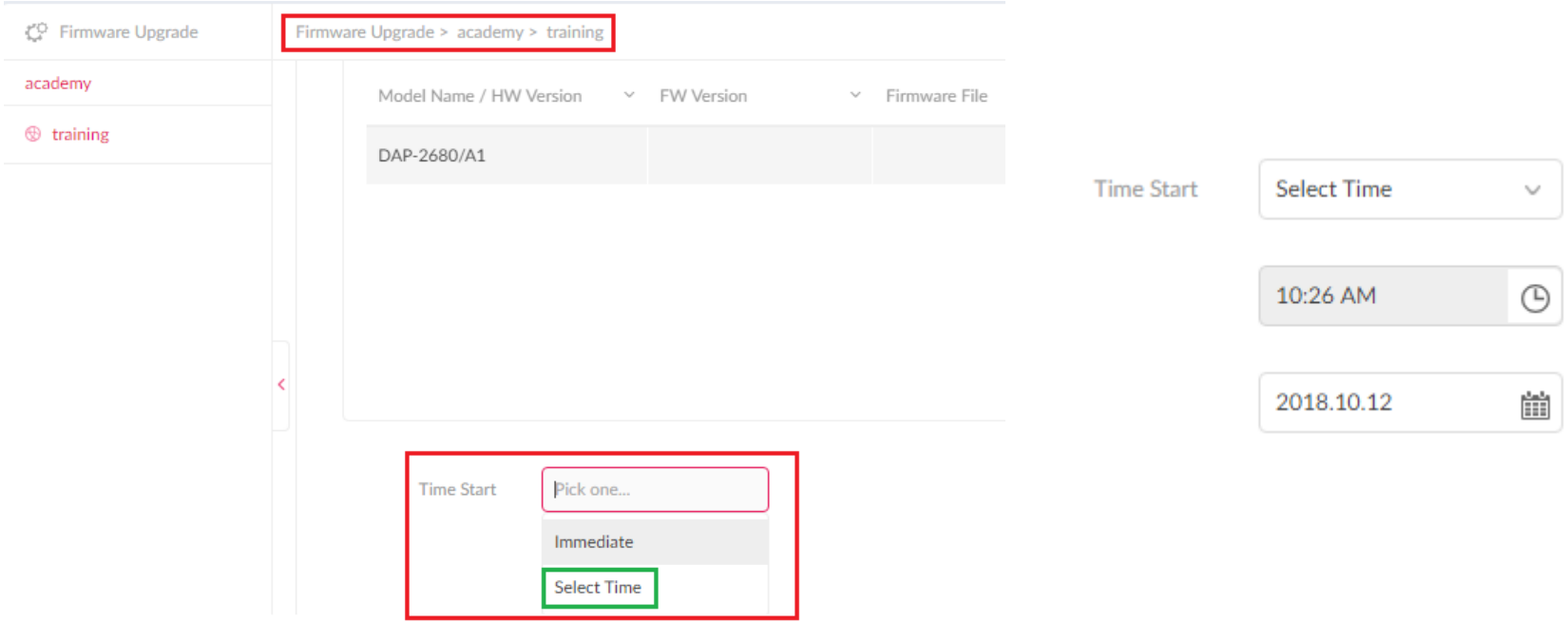
Log, 5G Group Key Update Discussion (2/2)

- The "Group Key Update Interval" inside the DAP is configured as 300 seconds, meaning every 5 minutes, we would have an update.



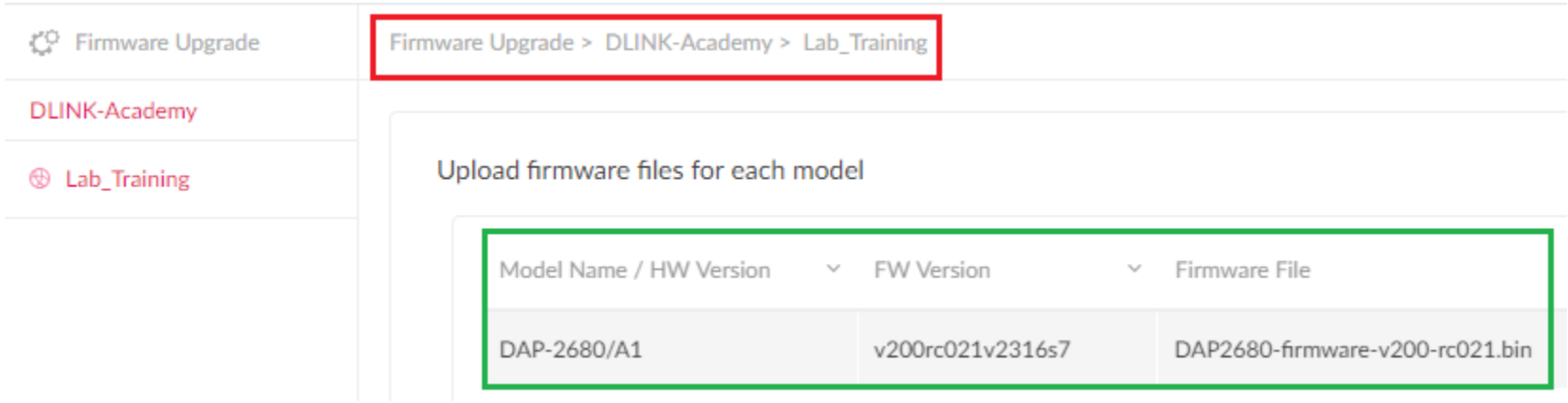
Access Points Device Management

- DAP Firmware Upgrade
- Nuclias Connect allows admins to easily schedule and reschedule firmware upgrades on their networks.
- Menu: Firmware Upgrade > academy > training



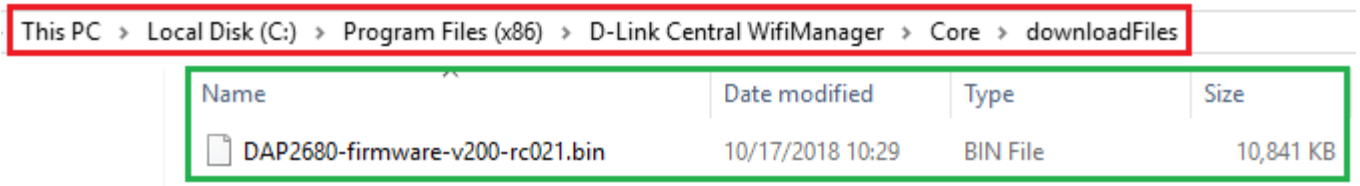
Access Points Device Management

- For Menu: System > Device List, we have identified two DAP-2680s are in our device list, where once occupies with "v200rc021v2316s7" firmware and another "v200rc020v2316s7"
- We have reached our decision to make embedded firmware universal.
  - DAP firmware: DAP2680-firmware-v200-rc021.bin



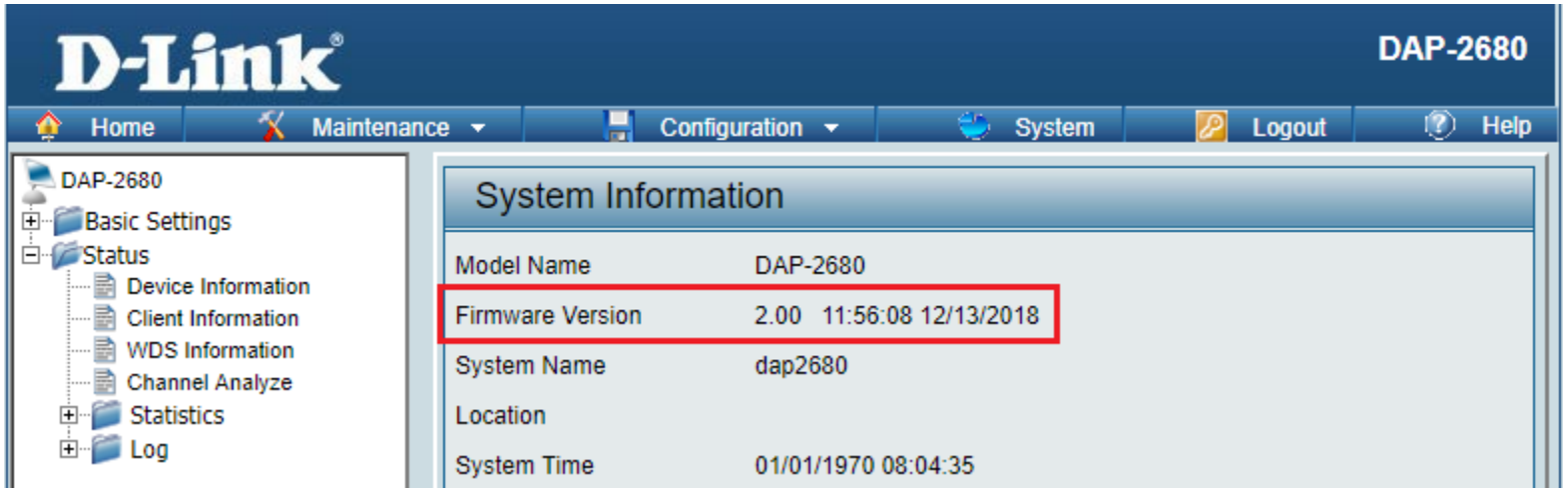
Access Points Device Management

- The folder path of DAP firmware: “DAP2680-firmware-v200-rc021.bin”



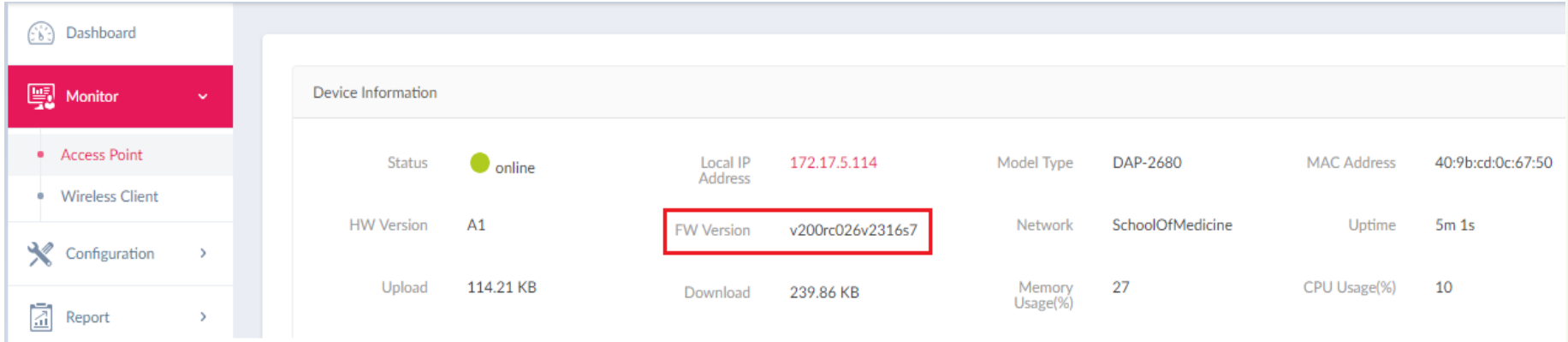
DAP Firmware Upgrade Practice (1/6)

- DAP Firmware Upgrade Practice
- We are planning to upgrade DAP firmware, from rc026 to rc029, via Nuclias Connect
- The following screen shot shows installed version (DAP GUI)



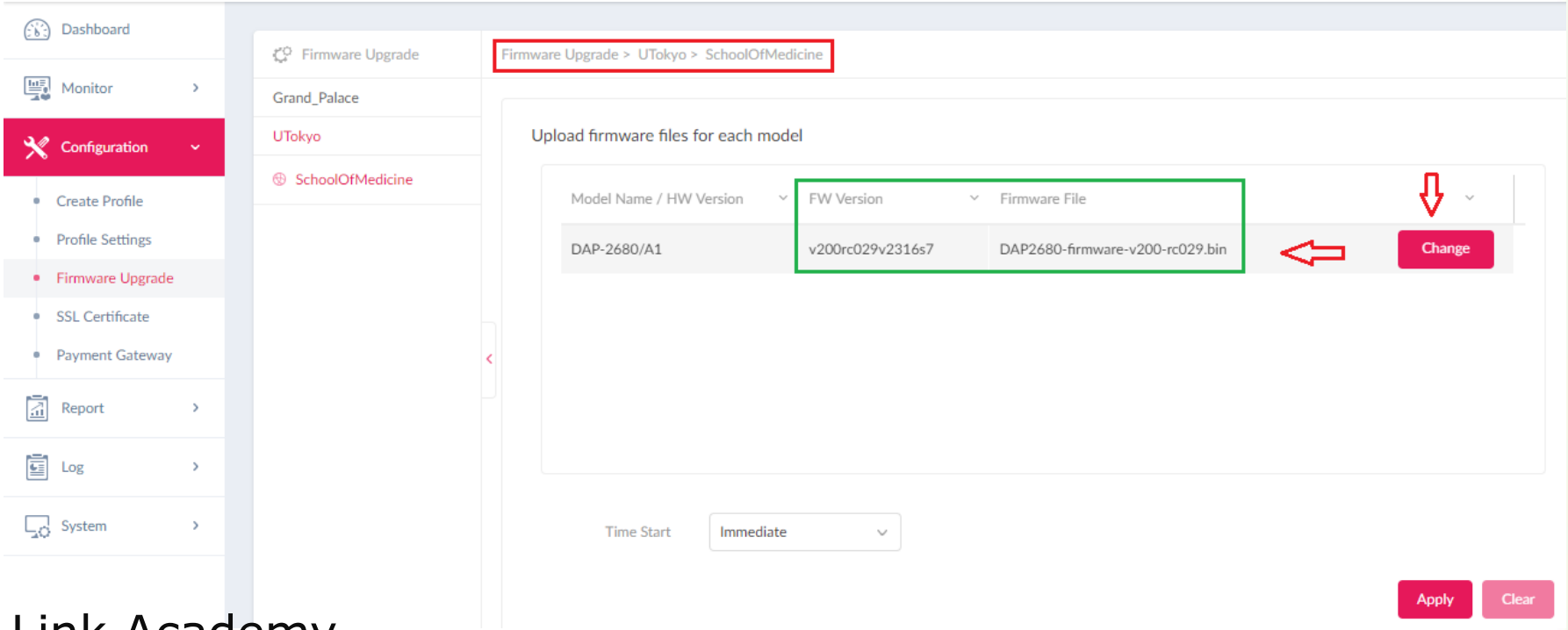
DAP Firmware Upgrade Practice (2/6)

- DAP Firmware Upgrade Practice
- We are planning to upgrade DAP firmware, from rc026 to rc029, via Nuclias Connect
- The following screen shot shows installed version (Nuclias Connect)



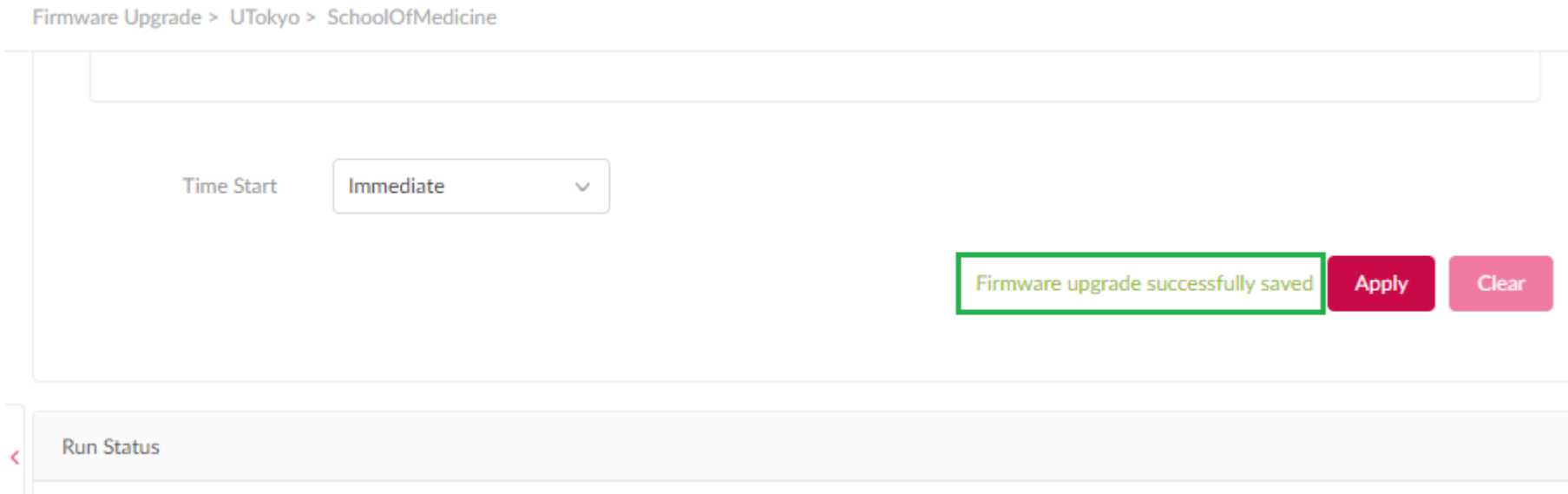
DAP Firmware Upgrade Practice (3/6)

- DAP Firmware Upgrade Practice
- Menu: Configuration > Firmware Upgrade > UTokyo > SchoolOfMedicine
  - Upload firmware files; Time Start: immediate



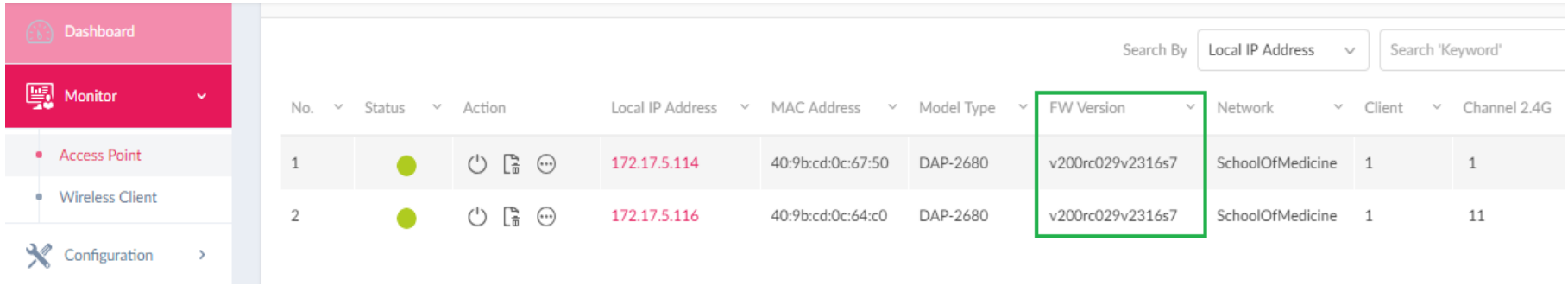
DAP Firmware Upgrade Practice (4/6)

- DAP Firmware Upgrade Practice
- Click the Apply button and verify the status



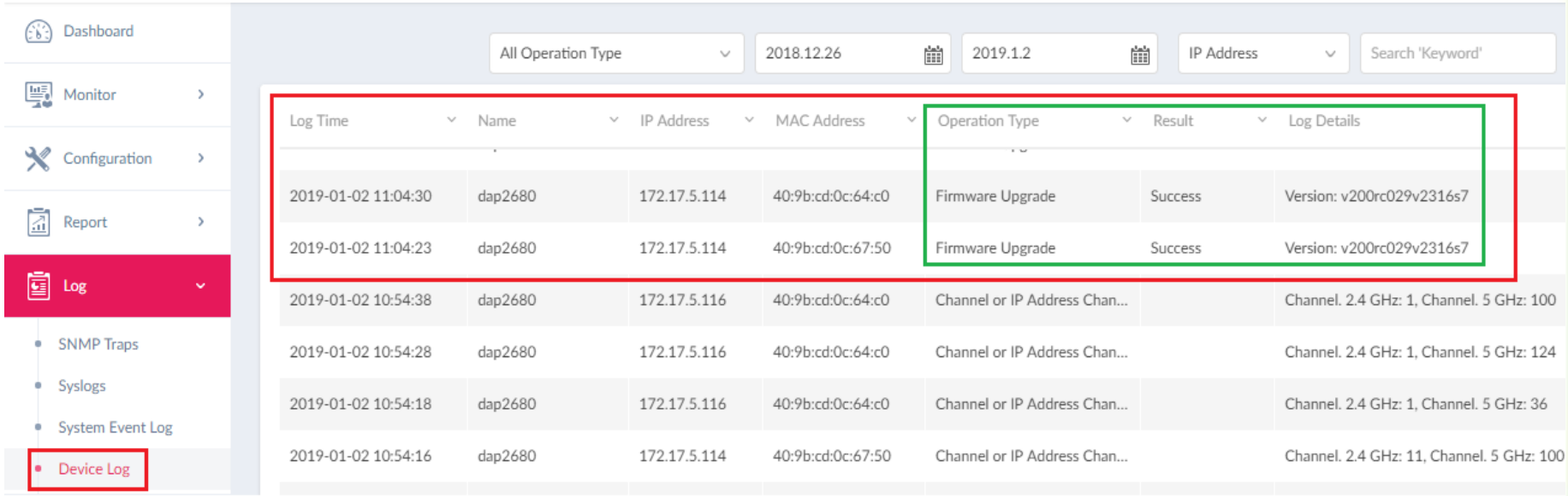
DAP Firmware Upgrade Practice (5/6)

- DAP Firmware Upgrade Practice
- Menu: Monitor > Access Points, where the managed DAPs shall carry latest firmware



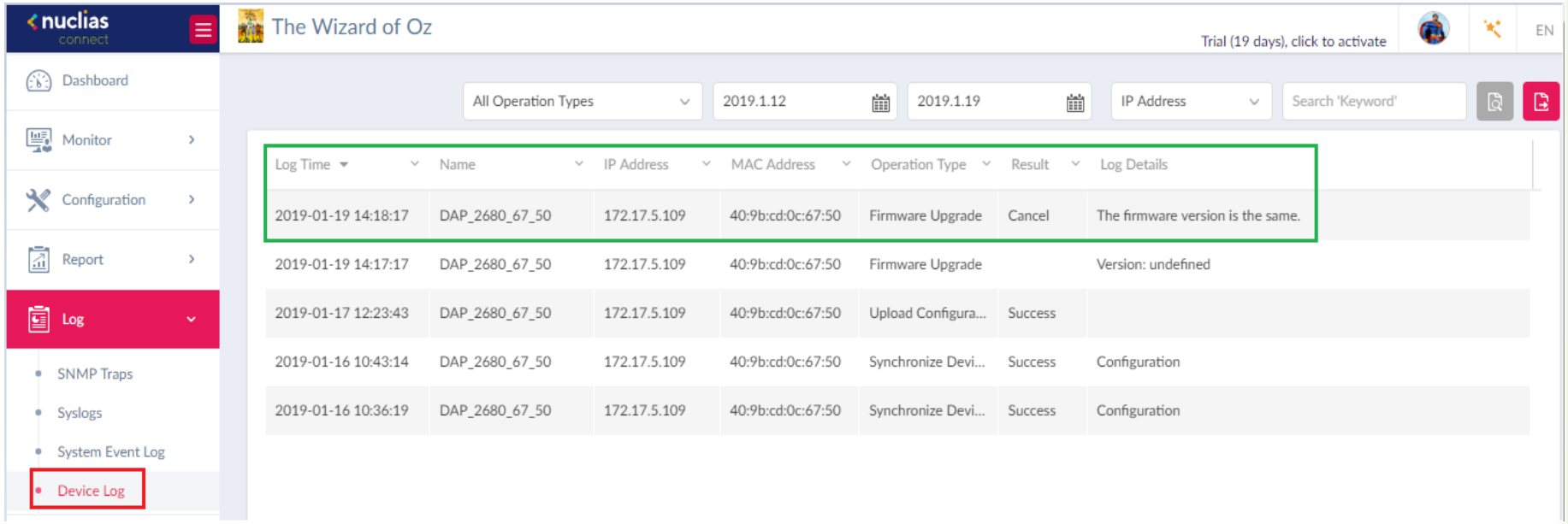
DAP Firmware Upgrade Practice (6/6)

- DAP Firmware Upgrade Practice
- Menu: Log > Device Log, where firmware upgrade messages should be displayed as well



Device Log regarding DAP Firmware Upgrade

- We had a situation where the Network Administrator attempts to upgrade the same firmware twice.
- By verifying the existing and going-to-be DAP firmware, Nuclias Connect produces the following log message (Log > Device Log).



Country Information (1/5)

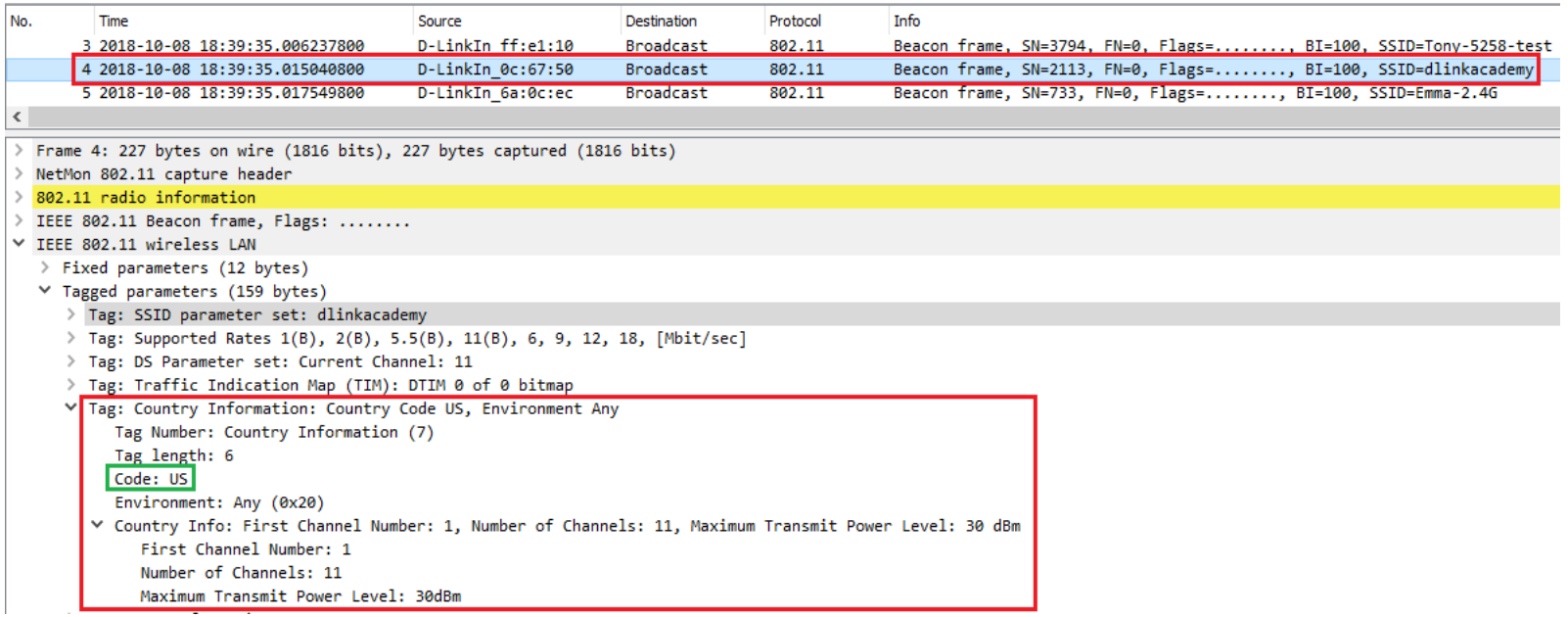
- IEEE 802.11 Wireless LAN, Tagged Parameters
- Country Information, a way for networks to describe regulatory constraints to new stations

No.	Time	Source	Destination	Protocol	Info
3	2018-10-08 18:39:35.006237800	D-LinkIn_ff:e1:10	Broadcast	802.11	Beacon frame, SN=3794, FN=0, Flags=........, BI=100, SSID=Tony-5258-test
4	2018-10-08 18:39:35.015040800	D-LinkIn_0c:67:50	Broadcast	802.11	Beacon frame, SN=2113, FN=0, Flags=........, BI=100, SSID=dlinkacademy
5	2018-10-08 18:39:35.017549800	D-LinkIn_6a:0c:ec	Broadcast	802.11	Beacon frame, SN=733, FN=0, Flags=........, BI=100, SSID=Emma-2.4G

```
> Frame 4: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits)
> NetMon 802.11 capture header
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 wireless LAN
  > Fixed parameters (12 bytes)
  v Tagged parameters (159 bytes)
    > Tag: SSID parameter set: dlinkacademy
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 11
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    v Tag: Country Information: Country Code US, Environment Any
        Tag Number: Country Information (7)
        Tag length: 6
        Code: US
        Environment: Any (0x20)
      v Country Info: First Channel Number: 1, Number of Channels: 11, Maximum Transmit Power Level: 30 dBm
          First Channel Number: 1
          Number of Channels: 11
          Maximum Transmit Power Level: 30dBm
```

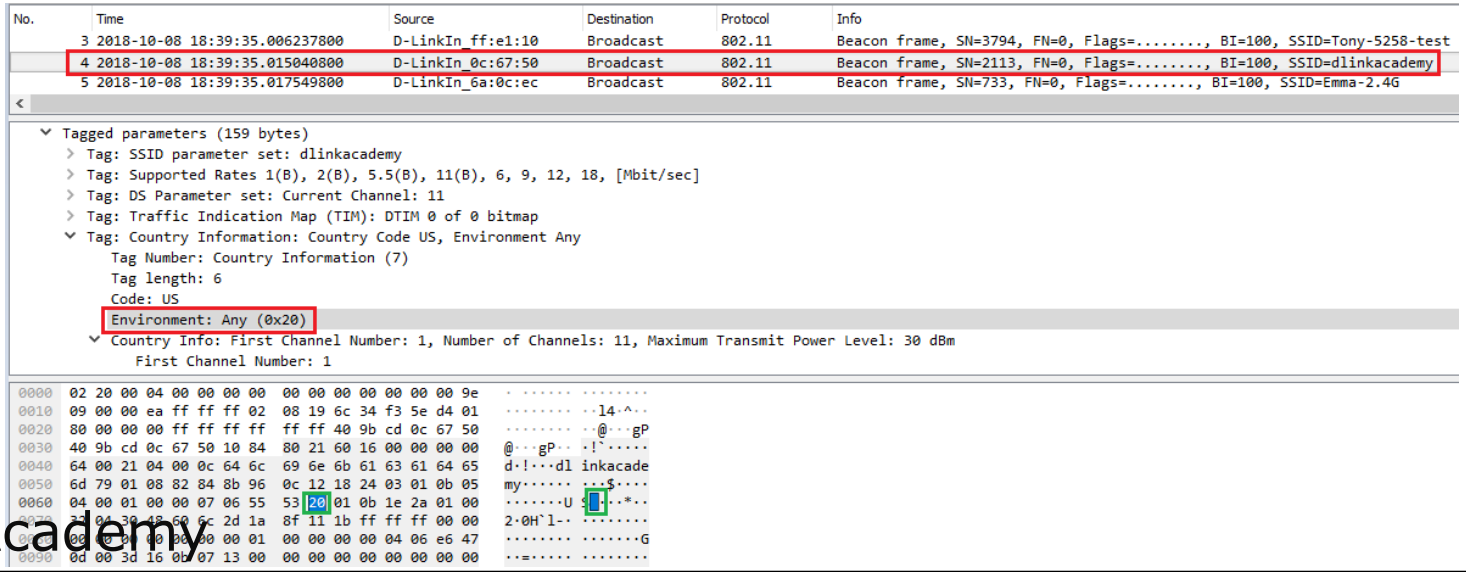
Country Information (2/5)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- Country Information, a way for networks to describe regulatory constraints to new stations
  - The first two letters of a three-character ASCII string are the ISO country code ("US" stands for the United States)



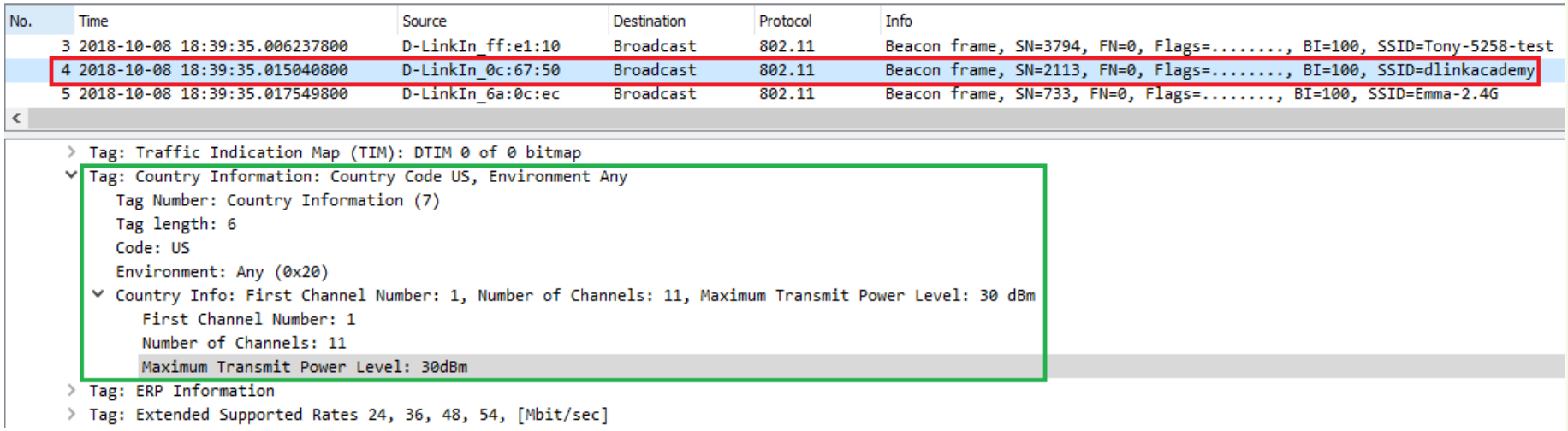
Country Information (3/5)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- Country Information, the third letter of a three-character ASCII string describes "environments," where
  - "I" indoor
  - "O" outdoor
  - Space, meaning a single set of omnibus regulations covers all environments



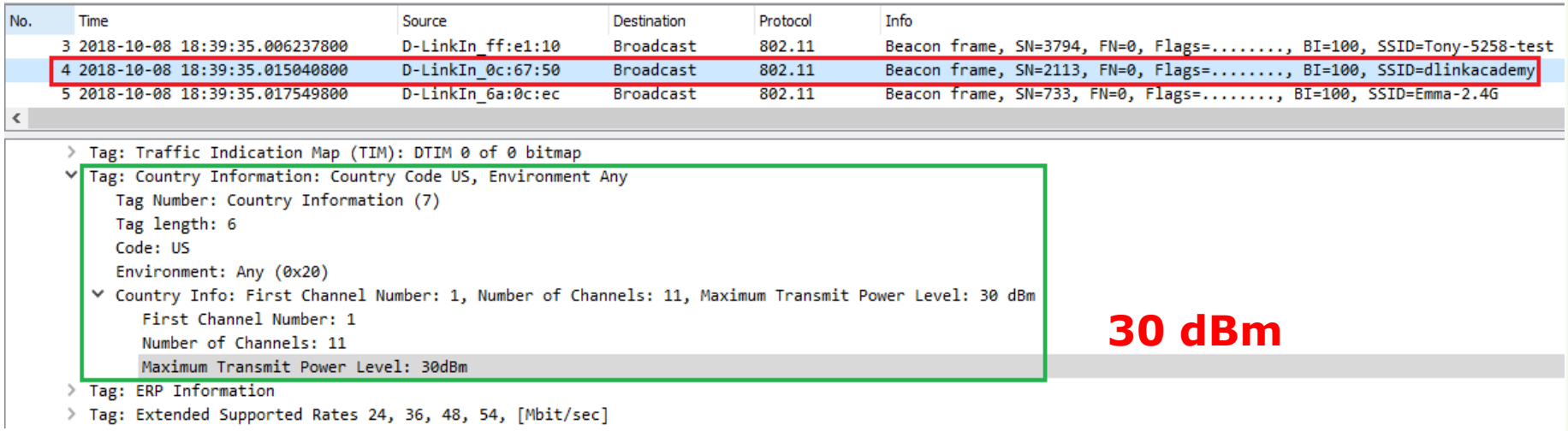
Country Information (4/5)

- IEEE 802.11 Wireless LAN, Tagged Parameters
- Country Information, per below diagram, what is the Maximum Transmit Power being set in this DAP-2680?



Country Information (5/5)

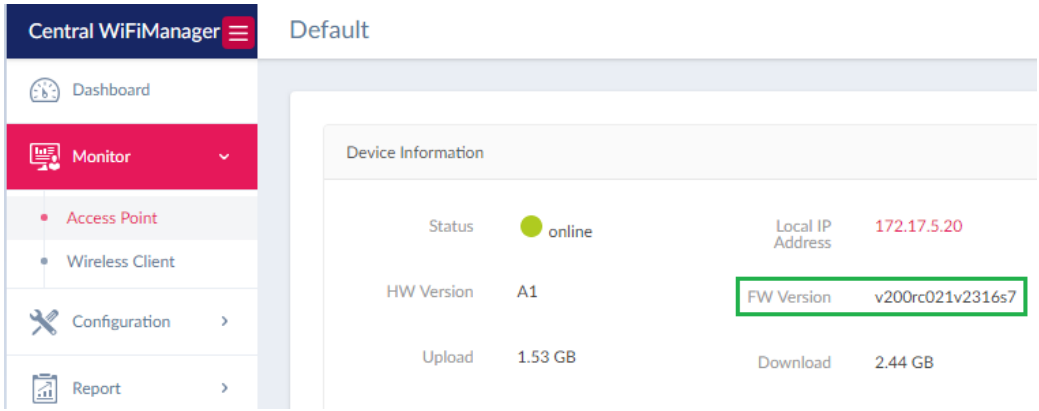
- IEEE 802.11 Wireless LAN, Tagged Parameters
- Country Information, per below diagram, what is the Maximum Transmit Power being set in this DAP-2680?



Access Points Device Management

Troubleshooting Guideline

- DAP just hangs (program freezes or stops responding)
  - Are we able to connect to DAP GUI?
  - Any wireless stations still able to connect to the SSID being broadcast by this AP?
  - The "managed relationship" between Nuclias Connect and non-responding AP remain the same or not at all?
- DAP Firmware version in-use (D-Track DRU20180417000003)
  - The below screenshot indicates FW Version v200rc021v2316s7



802.11 – Reason Codes and Status Codes

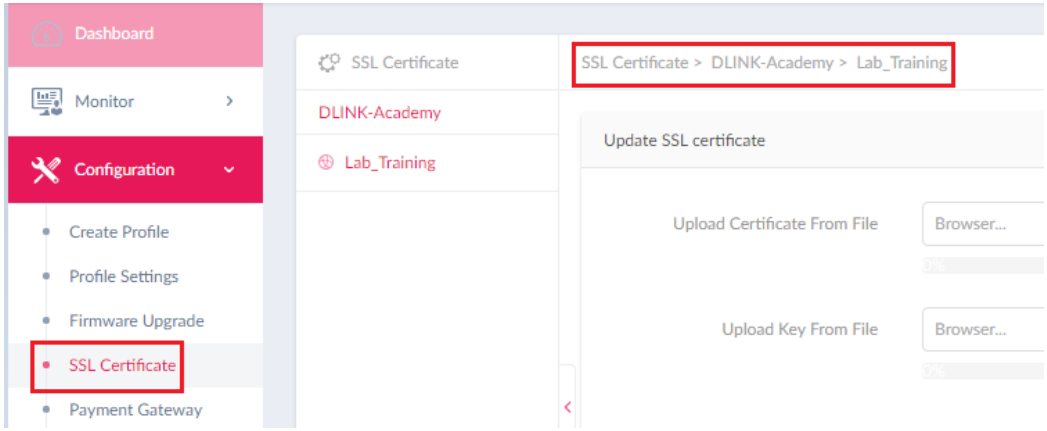
- During our lab practice, we have seen the below 802.11 reason code scenario from DAP-2680 GUI, what kind of implication it is meant to be?
  - 2.4G:Disassociate:STA F0:7D:68:F7:DC:09 (reason 8): Disassociated because sending STA is leaving BSS
  - 2.4G:Deauth:STA F0:7D:68:F7:DC:09(reason 6): class 2 frame received from non-authenticated STA

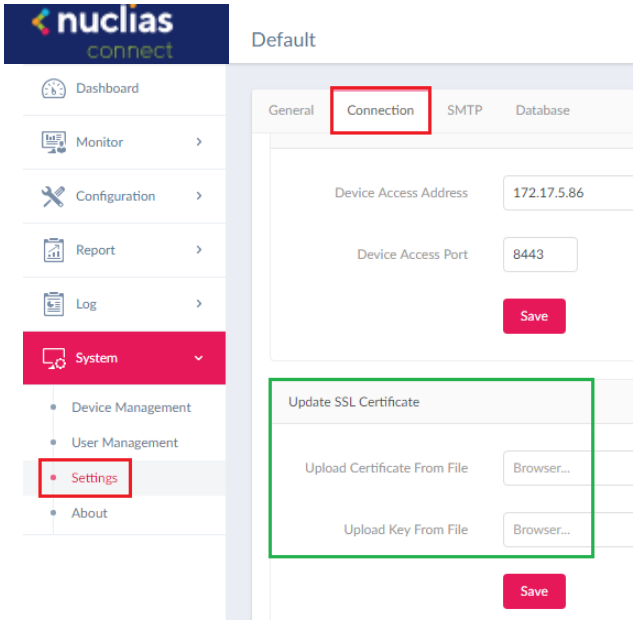
Time	Priority	Message
Dec 5 15:40:32	[SYSACT]	Web login success from 172.17.5.8
Dec 5 15:39:00	[SYSACT]	Web logout from 172.17.5.8
Dec 5 15:35:57	[SYSACT]	Web login success from 172.17.5.8
Dec 5 15:31:03	[Wireless]	2.4G:Association Success:STA F0:7D:68:F7:DC:09
Dec 5 15:30:32	[Wireless]	2.4G:Association Success:STA F0:7D:68:F7:DC:09
Dec 5 15:30:18	[Wireless]	2.4G:Disassociate:STA F0:7D:68:F7:DC:09 (reason 8)
Dec 5 15:30:16	[SYSACT]	Web login success from 172.17.5.28
Dec 5 15:30:07	[Wireless]	2.4G:Association Success:STA F0:7D:68:F7:DC:09
Dec 5 15:30:06	[Wireless]	2.4G:Received disassociate:STA F0:7D:68:F7:DC:09 (reason 8)
Dec 5 15:30:05	[Wireless]	2.4G:Association Success:STA F0:7D:68:F7:DC:09
Dec 5 15:30:04	[Wireless]	5G:Initiate Wireless success
Dec 5 15:30:04	[Wireless]	2.4G:Initiate Wireless success
Dec 5 15:30:03	[Wireless]	2.4G:Deauth:STA F0:7D:68:F7:DC:09(reason 6)
Dec 5 15:30:03	[Wireless]	2.4G:Deauth:STA F0:7D:68:F7:DC:09(reason 6)
Dec 5 15:30:03	[Wireless]	2.4G:Received disassociate:STA F0:7D:68:F7:DC:09 (reason 8)

Reject an invalid message 'Client Disassociate' due to "staToApRxDataBytes" does not exist. {"messageType":12,"agentGroup":{"uuid":"5BFD-079F822C-470AF42F-C95F"},"msgVer":"1.5.3","clientInfo":{"apMACAddr":"40:9b:cd:0c:64:c0","clientMACAddr":"f0:7d:68:f7:dc:09","wlanId":6,"ssid":"DSR250","sessionId":"15439950020c64c007","multiSessionId":"15439950020c64c007","channel":6,"disconnectReason":6}}

Privacy Enhanced Mail (PEM)

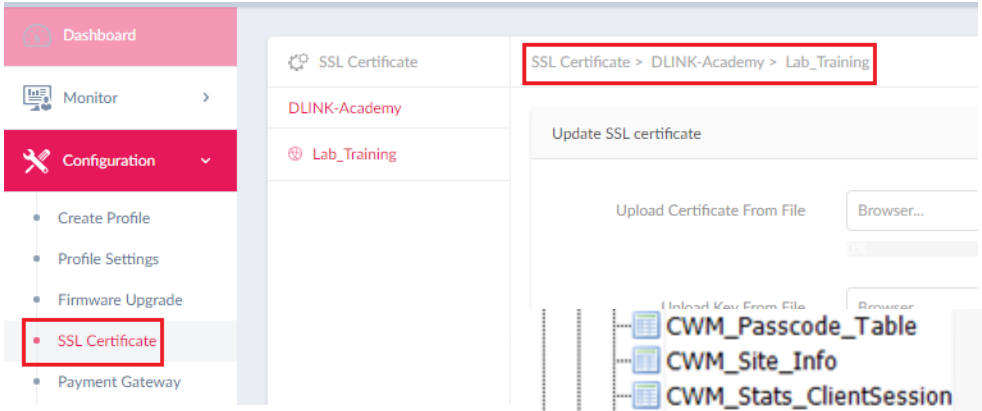
- Privacy Enhanced Mail (PEM) is a Base64 encoded DER certificate.
- These PEM certificates are usually used for web servers as they can easily be translated into readable data using a simple text editor.
- There are two locations where we are able to upload SSL Certificate
  - Configuration > SSL Certificate: it is for DAP certificate
  - System > Setting: it is for DNC server certificate

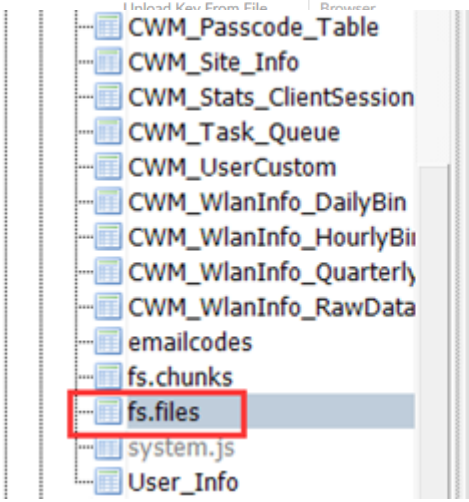


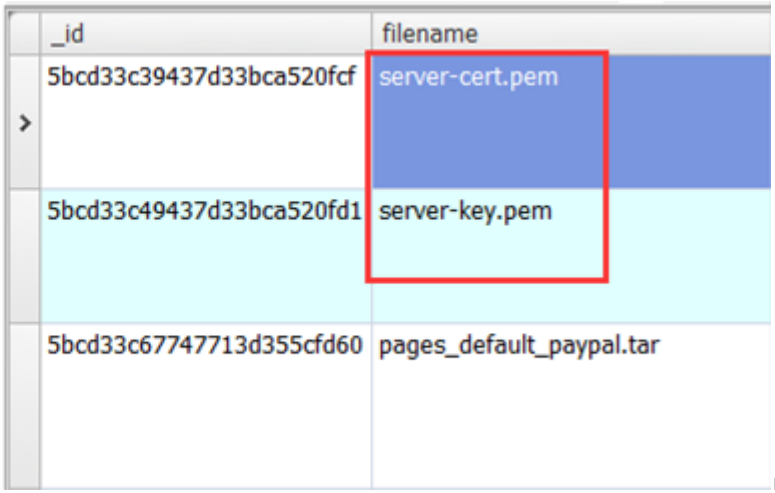


Nuclias Connect Privacy Enhanced Mail (PEM)

- The SSL certificate of Access Points (DAP) upload is on the SSL Certificate page under the Configure tab.
- Those certificates would go to database directly.

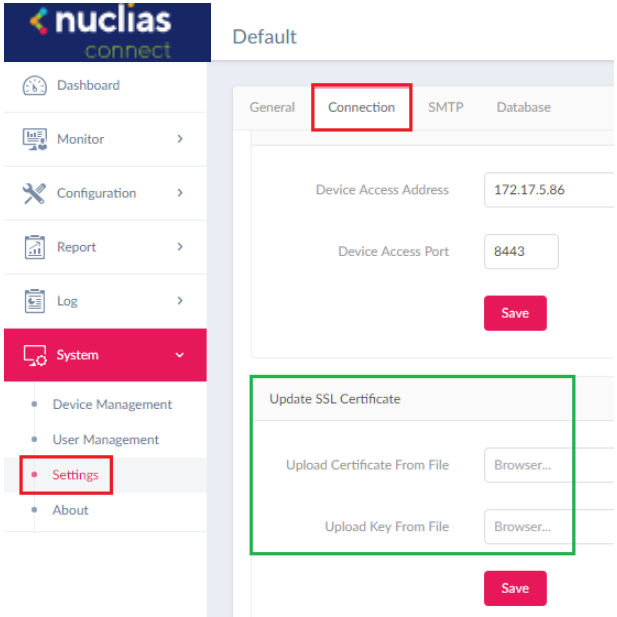






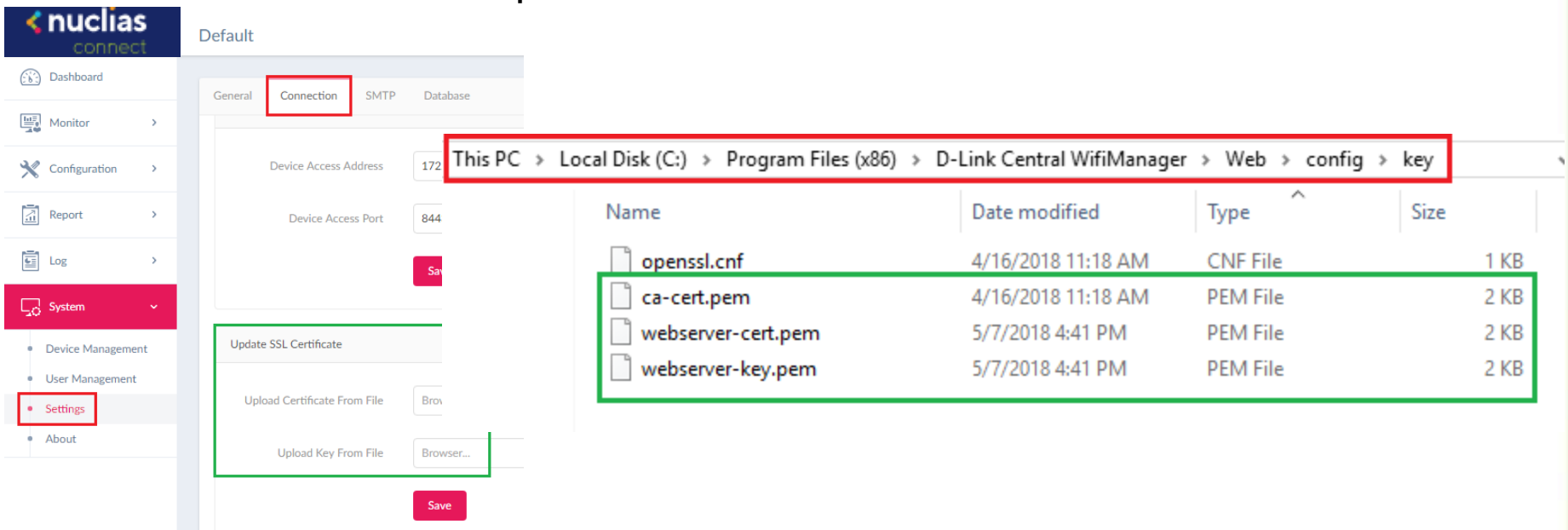
Nuclias Connect Privacy Enhanced Mail (PEM)

- The below sketches indicate the folder path of SSL certificates and keys being used in Nuclias Connect.
  - The –key.pem format for the certificate key file
  - The following items are SLL certificates for “web https” and “coreserver https”



Nuclias Connect Privacy Enhanced Mail (PEM)

- The below sketches indicate the folder path of SSL certificates and keys being used in Nuclias Connect.
  - The –key.pem format for the certificate key file
  - The following items are SLL certificates for “web https” and “coreserver https”



This page is intentionally left blank.

Conclusion

- Take home message

Proverb

"Talent wins games, but teamwork and intelligence wins championships."

By Michael Jordan

Proverb

"Talent wins games, but teamwork and intelligence wins championships."

By Michael Jordan



Copyright © 2015 D-Link Corporation. All Rights Reserved. D-Link, D-Link logo, D-Link sub brand logos, D-Link Certification Logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries. All other trademarks are trademarks of their respective manufacturers and owners.