# Palau Ministry of Education
# Executive Summary

Student Consultant, Andrew Schwartz, Yasuyuki Nishihara
Community Partner, Edwel Ongrung

## I. About the Organization

The Palau Ministry of Education (MOE) is responsible for the development and administration of education throughout the nation's public schools. This includes Finance, Transportation, Facilities and Information Technology. The public school system includes sixteen elementary schools and one high school. Its mission statement is as follows:

> *The mission of the Republic of Palau's Ministry of Education, in partnership with parents and community, is to ensure that our children and youth preserve Palauan culture and become contributing citizens and productive workers in a changing world. This will establish a high quality of life and security for future generations of Palauan.*

The organization receives funding from the Palau government as well as the US Department of Education (US DOE) and other grants. One of the US DOE funding sources, the College Access Challenge Grant, is the financial reason that the consultants are in Palau this year.

## II. Tablet Deployment Business Process Design

The MOE plans to deploy two hundred Apple iPads to 8th grade students in all elementary schools this fall semester, with the total number of tablet devices reaching one thousand in the near future. In order for MOE IT to manage the huge volume of tablets, a clear deployment business process is required. Thus, the consultants designed a business processes and documented it as a business flow diagram. Through this task, the consultants clarified:

- Responsibilities for each role in organization on tablet deployment
- Documents (user guides or procedures) which support smooth tablet deployment
- Attribute information about tablet management which the MOE must maintain
- Requirements for the Mobile Device Management System and other systems

The MOE IT staff was completely involved in the design process so that they could keep the diagram up-to-date on their own. As a recommendation, this process documentation should expand to the other business areas of MOE IT. This expansion will provide more overall capability.

## III. Mobile Device Management Software Implementation

Given the high functionality of an Apple iPad, MOE IT wanted to implement software that would manage the functionality of an iPad to maximize the educational value of the device. The consultants created a software alternative to limit functionality without expending bandwidth on the

MOE, designed setting criteria for incoming devices, and configured servers to support such functionality distribution.

## IV. Extended Access Implementation

It became clear that for incoming tablets, a wireless network would be required. Thus, the consultants designed a wireless network for the school system and implemented access points into Koror Elementary School as a model case. The outcomes consisted of general diagrams for all schools (Network Policies and Design Steps) and specific diagrams for KES (Network Diagrams for KES). The processes can be replicated to the other schools by the MOE IT staff. As a recommendation, implementing a routing protocol will be helpful for expanding network capability.

## V. RADIUS System Implementation

As the wireless infrastructure expands, a non-enterprise security system was becoming less applicable to the environment supported by MOE IT. The consultants configured Open Directory alternatives that were more sustainable and had better user interfaces, and configured an authentication system to be implemented at each of the school networks.

## VI. Additional Recommendations

### MOE IT Management Enhancement

Strengthening IT management is one of the most difficult tasks for managers. MOE IT has faced multiple problems in trying to establish an IT management processes. Through brainstorming sessions with the community partner, the consultants introduced practical steps to implement and enhance the IT management process at MOE IT. By following the given steps, MOE IT can strengthen its IT management and can grow its future capability and capacity.

### Technical Strategy Planning

The MOE should prioritize sustainability in future technical endeavors. As the Ministry continues to undergo technical exercises, it will be important to opt for stable releases instead of feature releases so that future maintenance is minimal.

### Web Content Filtering

To save bandwidth, it will be necessary for the Ministry to start conversations of blocking sites relating to social media, streaming, and piracy for the entire network. Bandwidth is one of the most precious resources within the Ministry, and should be treated as such. While such actions may not be popular, they will be critical in allowing bandwidth to go to more productive purposes.

**Consulting Partner**
**Edwel Ongrung**
*edwel@palaumoe.net*

Computer Service Manager
Palau Ministry of Education
P.O. Box 189
Koror, Palau 96940
*http://www.palaumoe.net/*

**About the Consultants**
**Andrew Schwartz**
*andrewsc@andrew.cmu.edu*
An undergraduate student in Information Systems

**Yasuyuki Nishihara**
*ynishiha@andrew.cmu.edu*
*nishihara.yasuyuki@gmail.com*
A graduate student in Information Systems Management

# Palau Ministry of Education
# Final Consulting Report

Student Consultant, Andrew Schwartz, Yasuyuki Nishihara
Community Partner, Edwel Ongrung

## I. About the Organization

### Organization

The Palau Ministry of Education (MOE) is responsible for the development and administration of education throughout the public schools in its nation. This includes Finance, Transportation, Facilities and Information Technology. The school system includes sixteen elementary schools and one high school. Its mission statement is as follows:

> *The mission of the Republic of Palau's Ministry of Education, in partnership with parents and community, is to ensure that our children and youth preserve Palauan culture and become contributing citizens and productive workers in a changing world. This will establish a high quality of life and security for future generations of Palauan.*

The organization receives funding from the Palau government as well as the US Department of Education (US DOE) and other grants.

### Facilities

The MOE is in charge of 118 buildings both academic and administrative encompassing 340,000 square feet of space. Each academic campus has one computer lab with an average of fifteen machines.

The MOE central office building is housed a mile off the center of Koror, the main state of Palau. The computer services department (MOE IT) has multiple offices and ample space to expand from a technical perspective. All of the MOE's technical spaces have more than adequate climate control for any existing servers and future technology.

### Programs

The MOE supports academic programming through curricular, technological and logistical support. The school system is responsible for the education of 2,000 students and education is mandatory for all students aged six to seventeen. Palau Community College handles all higher education and is unaffiliated with the MOE. Currently they are involved in a grant program through the US DOE called the College Access Challenge Grant (CACG). It is through this program that the consultants are in Palau.

## Staff

The President of Palau, elected every four years for one or two terms, appoints the Minister of Education who is in charge of all activities at the MOE. The MOE is divided into two bureaus, the Bureau of Curriculum Instruction (BCI) and the Bureau of Education Advancement (BEA). Within the BEA are Divisions of School Management, Personnel Management, and Research and Evaluation. In addition to the divisions, there are small departments for Food Service, Transportation, Finance, Materials, Facilities, and Information Technology. The heads of all departments comprise the Management Team, which makes all decisions for the ministry.

The BEA employs sixty people that do not work directly for an individual school. Of those sixty, five work for the IT department. The IT Department is led by Edwel Ongrung, the Computing Services Manager who has been the community partner for several Technology Consulting in the Global Community (TCinGC) endeavors at the MOE.

30% of MOE staff use computers on a daily basis. The staff also has access to computer labs in the neighboring schools after hours for their own work. Based on a 2008 Survey, the IT Department estimates that only 40% of the MOE staff has the computer literacy to use a word processing system like Microsoft Word or Apple Pages.

## Technology Infrastructure

The MOE uses computer systems with ranging platforms from OSX to Windows to Linux, and mobile devices are also supported. The ministry contains a wireless network throughout the central office building with WPA2 security protocols. Current infrastructure supports authentication, mail, and web servers as well as some necessary requirements like DNS and DHCP. Most if not all servers are run with open-source software that allows the MOE to keep costs down while still having relatively reliable programs.

All external connections between MOE central office and each school have a DSL connection at 256Kbps (with the exception of three schools on dial-up). Internally all schools have wired connections with one exception that Palau High School has a wireless network at 20Mbps. All schools go through the MOE to get the Internet access.

## Technology Management

All technology related issued are handled by Edwel and his four staff in the Computer Services Department. The five of them recommend technical expansion plans to the Minister and the Management Team for final decisions and funding. Edwel manages all fiscal and administrative operations of the Computer Services.

## Technology Planning

All technical issues are dealt with on an ad-hoc basis and there is no future IT strategic plan in place.

## Internal and External Communication

Given the size of the ministry, most non-essential information is transferred through peer conversations. Any logistical information is sent by email, which has high reliability as it is sent through the ministry's intranet and does not have to leave the island. Files can be easily shared internally, and are normally done so via email. External Internet access is slow; but stable compared to the standard level in the country.

With bandwidth being as slow as it is, any cloud-based service is not considered reliable to the MOE. When it comes to improving infrastructure, the limiting factor is not the MOE, but the satellite used to transmit data. The Palau Government is attempting to run a cable to Guam, but until they do so (five to ten years) there will be a severe bandwidth restriction on the ministry for the considerable future.

### Information Management

Information is typically stored on paper or flat-file databases on an individual's computer. In 2009, student data was moved to a MySQL database and that has withstood the test of time. With that in mind, other attempts to automate have taken unexpected lengths to complete. This has happened because the staff did not take the time to learn how to effectively use the systems, and as such they are not as willing to move to automation for fear of the duration of such a move. The CMU partnerships have been the focal point behind most successful automation endeavors.

### Business Systems

All business systems are taken care of by the national government. The MOE does not handle any of its own accounting or payroll.

## II. Tablet Deployment Business Process Design

### Motivation

The MOE plans to deploy 200 Apple iPads to all 8th grade students in Palau to enhance their educational experience. They already have 400 tablets (Samsung Galaxy Tablets) and deployed them to schools; but the MOE does not have specific deployment processes to manage the tablets at this time. The MOE plans to purchase an additional 400 iPads, meaning the MOE will have to manage over 1,000 tablets in near future. Without specific deployment processes, tablet management would be difficult due to the large scale of tablets which the MOE has to manage. Therefore, designing clearly the business process will provide the MOE much needed sustainability

### Outcomes

The tablet deployment process has been designed and approved by MOE IT as "Business Flow of Tablet Deployment" (see appendix. B). The document clearly describes the processes in six business areas related to tablet deployment:

1. Purchase: The MOE purchases new tablets
2. Deployment: The MOE deploys tablets to users in each school
3. Regular Update: The MOE/Admin update tablet settings (ex. End of academic year)
4. Urgent Update: The MOE/Admin update tablet settings urgently (ex. Security update)
5. Lost/Stolen: The User loses tablet/tablet is stolen
6. Tech Support: The User needs technical support to use the tablet

Designing a clear tablet deployment process bought the following outcomes:

- Clarified the responsibilities for each role in organization with relation to tablet deployment

- Clarified the documents (user guides or procedures) which support smooth tablet deployment
- Clarified the tablet management attribute information which the MOE must maintain
- Clarified the requirements for the Mobile Device Management System (MDM) (described in Part III) and other systems related to tablet management like an inventory system.

The business process was designed through discussions with the community partners. The consultants put the required tasks for each processes in order (ex. Receive iPads, Set up iPads, Record iPad to inventory sheet, etc.) and clarified who is in charge of those tasks. Also, the consultants created required documentation for some tasks (ex. iPad User guide, Configuration Creation Guide, etc.). Through discussions, the consultants found maintaining the information about tablets on the inventory systems in both the MOE and Ministry of Finance (MOF) was very important. Thus, the consultants listed up the required information for the inventory systems and clarified how to collect and maintain the information based on the iPad deployment. These steps helped to fix the requirements for the Mobile Device Management System.

All the information above was put into a flowchart and shared with the community partners. MOE IT will start deployment this August according to this business process. However, the flowchart is a live document. If the change of a business situation requires amending the business process, the flowchart should reflect the amendment. Community partners were involved the designing of the tablet deployment process, therefore they can maintain the vitality of the flowchart.

As a supplementary outcome of the business process design, methods behind drawing a flowchart using Microsoft Excel was extremely useful for MOE IT. The first time our community partner saw the diagrams, they believed the charts were made with Microsoft Visio or another complicated graphics software. However, the chart was drawn by mix of standard functions in Excel (Narrow width of columns, Insert Shapes, Use Connectors, Snap to Grid, etc.). Student consultants showed the creation process of flowcharts to the MOE IT staff. All techniques were small tips, but they will be helpful for future opportunities to create flowcharts and diagrams.

## Recommendations

MOE should expand the design and documentation process to other business areas in where the staff has responsibility. Currently MOE IT does not have a documentation culture so IT functionalities are not clarified and not shared among the staff and organization. For example, if a member retires or quits the job without documentation, the process and knowledge that the member has will be lost (This situation already appears in other business areas of the MOE). Thus, MOE IT has a certain risk of its business continuity.

Even if the business areas and involved roles are different from the tablet deployment design case, the steps to create business process are basically same, like the following processes:

1. Identify categories and roles involving the business process
2. Check the restrictions or backgrounds of the process
3. Draft the business flow
4. Specify the management factors for each process
5. Discuss the flow with stakeholders
6. Approve the flow

The consultants showed the methods to define and record business process shown as above and the MOE IT Staff learned the creation steps one by one with the consultants. Expansion of the documented area will mitigate business continuity risk and will provide sustainability to MOE IT

# III. Mobile Device Management Software Implementation

## Motivation

Given the high functionality of an Apple iPad, MOE IT wanted to implement software that would manage the functionality of an iPad to maximize the educational value of the device. Low bandwidth throughout the school system required devices controls to be operational offline, and an already overburdened staff required a system that would need very low maintenance. Given that students would hold onto a device for the entire year, devices would need to be secure in maintaining their preferences, as students would have ample time to try to modify restricting settings.

## Outcomes

### *1. Created software alternative to limit functionality without expending bandwidth*

When the consultants decided to implement a Mobile Device Management system, they did not anticipate the long list of requirements that would be set to make the project viable. Requirements often indirectly conflicted with each other, so over time the team and the client met to determine prioritization for each requirement. After considerable vetting, the consultants narrowed the most significant requirements to be as follows:

- System must be based in the Ministry of Education
- Devices must be restricted from accessing high-bandwidth/explicit content
- Devices must be limited even if they cannot connect to the MDM
- System must be free or with low and one-time cost

The consulting team used extensive research, debate, and models to design a business process by which the most significant requirements could be met. Given that the software given to the consultants was fixed, our process became an instance of configuring existing software as opposed to bringing in new software.

### *2. Designed setting criteria for incoming iPads*

The team then met with existing stakeholders within MOE IT and the Division of School Management to design a set of limitations that would be imported into iPads as part of a Configuration Profile. Once criteria were written, a process was designed which would allow administrators, lab attendants or students to apply all software limitations to a single iPad through a web interface or multiple iPads through a desktop application. While an intranet connection would be required for a one-time installation, it would not be required to maintain those limitations.

### *3. Configured OS X Servers to support functionality*

Multiple servers were configured to support different functions of the MDM. Authentication, Configuration Profile and Caching were configured on different systems and each computer was built with additional features to support the overall management of the devices and the entire ministry.

The process behind implementing an MDM kept in mind that if the team chose to implement an Apple system, we would be able to rely on Apple Support given the purchasing plans of the MOE. However, over time it was realized that as the MOE IT purchase did not qualify for the support the consultants were anticipating given the location, the team had to again alter plans of requirements and implementation.

Systems were designed with the user experience of an administrator in mind. While processes were used extensively to integrate the system without relying on consistent Internet, the process was well documented. With that in mind, the MOE IT staff will need to be diligent in making sure steps are not skipped, or they will run into problems down the road dealing with this system and this software will potentially be abandoned.

With respect to Mobile Device Management, no development experience will be necessary to operate this system from a user or administrator perspective.

### Recommendation

In future endeavors relating to an MDM, the consultant team recommends focusing on paid and/or offline systems. Given the uncertainty of future Internet access, it seems that systems are more likely to be sustainable if they focus on internal services.

With that in mind, the team does recommend services that connect schools to the MOE and to other schools. While infrastructure is not reliable in endeavors off of Palau, the infrastructure is reliable when contacting one school from another.

## IV. Extended Network Access Implementation

### Motivation

To use the tablet devices in different areas of the schools, all classrooms with tablet users needed to have a wireless network; but before the student consultants came to Palau, the schools did not have any wireless environment. Therefore, implementation of wireless network became an essential part of the tablet deployment program.

Tablets will be provided into all 16 elementary schools in Palau. However, the student consultants were only in Palau for 10 weeks. Thus, the consultants implemented the extended network into one school, Koror Elementary School (KES), as a model case. MOE IT will eventually deploy the extended network to other 15 elementary schools based on the KES network design.

### Outcomes

Based on the KES's current network, the consultants implemented the following items:

1. Create "Physical Network Diagram" and "Logical Network Diagram" for KES
2. Define "Network Policy" (Basic rules for IP addressing, naming of hosts, and port usage)
3. Define "Network Design Process" (General steps to design new or extended network)
4. Configure and evaluate network devices in the lab environment
5. Implement new access points into KES

### *1. Create Network Diagrams for KES*

As the first step of this task, the consultants created network diagrams after site surveys of KES, because MOE IT did not already have network diagrams. The diagrams consists of a physical diagram and a logical diagram (see Appendix. I ). Each diagram has the information below.

(Physical Diagram)

- Location of device
- Cabling route between devices
- Name and type of device
- Photos of location and device

(Logical Diagram)

- Logical structure of devices
- IP address and network segment information
- Manufacture, Model, Hostname,
- Port information (Port number, Link speed, and Duplex setting)
- Physical location

### *2. Define Network Policies*

MOE IT did not document rules for network design (though they had some rules) so that the consultants defined the rules for the following items and documented them:

- Rule for IP addressing
- List of IP address
- Rule for host names
- Rule for port usage

### *3. Define Network Design Process*

Based on the KES case, the consultants documented the general steps for network design which consist of the following twelve steps (Please see Appendix. N for detailed information):

1. Fix purpose of new network
2. Pre-survey (Off-site, before visiting the site)
3. On-site survey
4. Create network diagram (Current)
5. Design new network (Create future network diagram)
6. Specify requirements for new network
7. Purchase new devices and cables/outlets
8. Configuration of network devices
9. Test new network (Lab environment)
10. Implementation and Test (On-site)

11. Follow up the 1st business day after implementation
12. Update management documents

### 4. Configure and Evaluate Network Devices

After the designing processes described above, the consultants developed a lab environment in the MOE main office. In the environment, they implemented a virtual KES segment and tested whether the network devices and some applications worked correctly.

### 5. Implement the Network Devices into KES

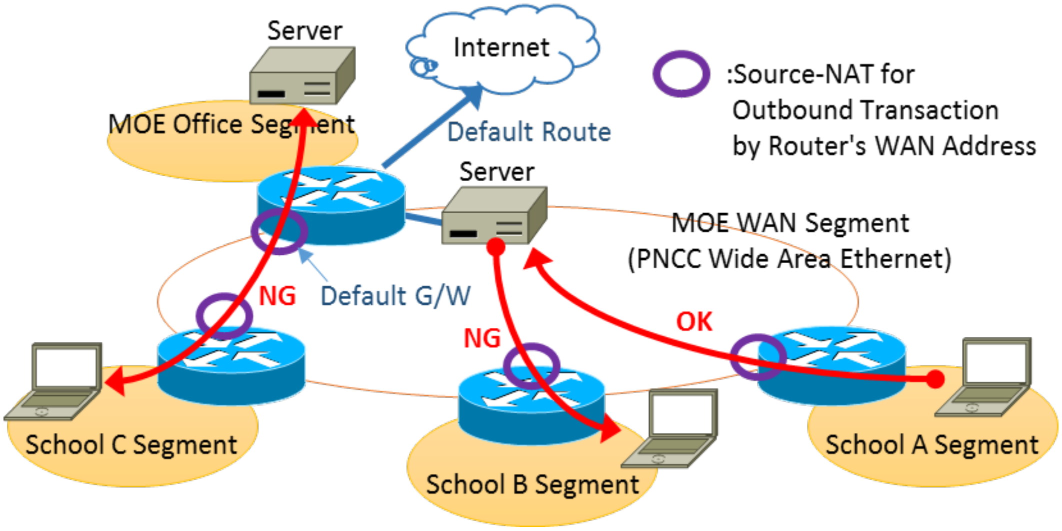
After evaluating the test result, MOE IT staff and consultants implemented the new network devices into KES.

These processes above can be replicated for the other school's network by the MOE IT staff because the consultants clearly showed (and documented) the processes of network design and implementation. Of course the detailed settings should be modified depending on the current environment of each school; but the steps to design and to implement the extended network are common as "the general steps to network designing" shows. Thus, the MOE IT staff can deploy the extended network to the other fifteen schools.

## Recommendation

A Routing protocol should be implemented in order to expand the MOE's network flexibility and use the network in a more dynamic fashion. The consultants had to move this recommendation out of the scope of this project due to time constrains with the TCinGC program. However, the consultants strongly recommend the implementation of the following.

The Current design of MOE's WAN is like the following image.



The routers of each school and MOE's WAN belong to the same network segment (MOE WAN Segment). Currently, the routing protocol is not working in the MOE network which causes each router to only know the segments that it itself has. As a result, the hosts in the network can only communicate with the device in the same network segment and devices directly connected to the router. For example, if the devices under school A router wans to access the server in MOE WAN segment, the transaction can reach to the server; but the return transaction cannot reach the device because the router which the server belongs does not know the school A segment. To avoid this problem, each router in the MOE WAN segment sets the source-NAT (Network Address Translation) on the WAN interface. This configuration translates the source address of the device in the school segment to the router's WAN address so that the return transaction from the server can access to the school router. The school router re-translates the destination address into the original address of the device, and the transaction is completed.

This NAT setting fixes one of the transaction problems (in the chart, "School A Segment" case). However, the server in MOE WAN segment still cannot find the devices under the school routers ("School B Segment" case) and the devices cannot access the servers in the MOE office segment beyond the MOE office router ("School C Segment" case. It is the same as the case nodes communicate between two different school LAN segments). Only Internet requests work beyond the MOE office router because the default route of the router is set towards the Internet (All transactions whose destination is unknown to routers head to the Internet communication line).

Currently, the NAT setting may meet the MOE's network requirement. However, if the MOE wants to manage the nodes on the school's LAN from the MOE office or MOE WAN segment, the NAT setting will need to change. The current NAT setting consumes unnecessary CPU power of the router, and may affect its performance.

To keep the capability of the network, the MOE should implement a routing protocol and make all routers know the neighbor segments. Fortunately, the scale of the MOE network is small (each school has only one or two segments), and the network structure is not changed dynamically (there is no redundant network structure). Based on these conditions, basic routing protocol (like RIPv2 or OSPF) can cover the whole network. The implementation steps of routing protocol are shown as below:

1. Design routing topology based on the future requirement for the network
2. Choose the candidate of routing protocol based on the network design
3. Create configuration of routers and test them in the lab environment
4. Create transition plan for live network
5. Implement routing protocol into the live network

# V. RADIUS System Implementation

## Motivation

As the wireless infrastructure expands, a non-enterprise security system was becoming less applicable to the environment supported by MOE IT. Single passwords for entire networks allow for the high probability of unauthorized users, who will request just as much bandwidth as a regular user. With bandwidth at a premium in Palau, restricting access is pivotal to allowing key users to have a productive time online. As such the implementation of an enterprise authentication system was necessary to prevent unauthorized access.

## Outcomes

### *1. Configure Open Directory service to replace existing MOE LDAP server*

The consulting team worked to build an LDAP - Open Directory system on an Apple OS X Server.

The new OD server was tested against multiple services that are used in the MOE and were currently using the original LDAP server. The consulting team was not able to fully move the MOE over to the new server, but was able to provide the system and documentation to do so when the IT staff is ready. In addition, the services that were set up were configured to authenticate through the OD server. As multiple servers were configured, the devices could be easily set to integrate load balancing and failure recovery.

### *2. Configure FreeRADIUS system to meet MOEIT's needs*

The team configured FreeRADIUS, an open-source authentication system, to allow for future expansion of wireless access points. Given that the team had devised a naming scheme for all devices, it was possible to hard code future names and IP addresses into the RADIUS configuration. The authentication system was also connected to the Open Directory Service created on the same machine, and documentation was provided for future configuration.

# VI. Additional Recommendations

## MOE IT Management Enhancement

MOE IT has the responsibility to manage whole enterprise system in the MOE. The current MOE's IT management, however, is not well defined and is not working in some essential IT management areas (several problems occurred in such management areas due to lack of the management processes).

The student consultants had brainstorming sessions with the community partner about MOE IT management enhancement (Please see discussion materials in Appendix. S). Through the sessions, the consultants created guidelines to strengthen the management. The path is described as the following steps;

1. Know your systems
2. List up current problems for MOE IT and drill down the root causes of the problem
3. Analyze common/significant IT management areas where the causes are covered
4. Define rules/procedures to manage the targets in the IT management areas
5. Implement the rules/procedures into the MOE IT's actual business environment
6. Evaluate the IT management areas regularly

### *1. Know Your Systems*

First of all, MOE IT should clarify what the MOE enterprise systems are. Knowing the systems well is the foundation of all IT management processes. The IT staff cannot manage the systems that the staff does not know well. In order to understand the systems, documenting the list of the systems (called "System Ledger") is quite helpful. The list should have the following attributes:

1. Components of the System
    - Purpose of the System
    - User of the System
    - Hardware, Software, Middleware Information (Manufacture, Model, Version, etc.)
    - Interfaces between relative systems
    - Functionality of the System

- Network Information
- Developer Information

2. Components of the system operation
   - Dairy Operations
   - Operator Information
   - Security Requirement
   - Importance of Business Which the System Supports

All systems that the MOE has should be recorded in the ledger. The relationship between the systems can be described as "System Structure Diagram" (Bird's Eye View).

### *2. List problems for MOE IT and drill down to the root cause*

Problems that have already occurred in MOE IT could come from a wide range of a lack of the essential management process. Each problem has a direct cause and each direct cause may have root causes. By drilling down the direct cause, the root causes may be found.

For example, MOE IT received the report from the principal of Melekeok Elementary School that the uplink transaction to the MOE main office from the school was not working properly. The direct cause was that the router's configuration (about DNS setting) was not correct. However, the direct cause also had some root causes (management issues) like the following questions:

- How to design the network?
- How to store the correct configuration?
- How to check the implementation?
- How to observe the network?
- How to record the failure?

### *3. Analyze common/significant IT management areas where causes surface*

These causes should be mitigated by management activities. To enhance the overall process, the common causes (problems happen frequently) or significant causes (problems have significant impact on MOE business) show IT management areas that are currently weak or missing. These areas could be the target of IT management enhancement.

### *4. Define rules/procedures to manage the targets in the IT management areas*

After fixing the target areas, the actual activities to manage such areas should be defined. To think about activities, a global standard of IT governance will be helpful to get an idea. For example, COBIT5 provides definition of management areas in IT governance and also provides examples of activities for each management area. Implementing COBIT5 would never be recommended because the framework is too huge and complicated to apply to MOE IT; But just looking through the information will be quite useful in defining feasible management processes for MOE IT. Based on the feasible ideas of management process, the actual rules or procedures for IT management will be established.

### *5. Implement the rules/procedures into MOE IT's actual business environment*

The rules or procedures should be implemented into daily operations. Each rule or procedure should be documented and MOE IT staff should understand them before implementation (some training may be required for implementation depending on the staff knowledge level).

### *6. Evaluate the IT management areas regularly*

After implementation, evaluation process on a regular basis is quite important in order to have an effective management process. Evaluation methods and timing are varied in the management areas, but the process is evaluated based on numerical facts, quality of working, the occurring problems, and ideas for improvement. It is also important to report evaluation results to the MOE Management Team on a regular basis. It cannot be stressed enough that without this last step, the overall enhancement will not take full effect.

## Technical Strategy Planning

In future endeavors, the consultants recommend to put sustainability before cost. The consultants were given a system because of its features and its non-cost. Because of this, software was built on a system that may or may not be stable. While opting for the feature release may be more beneficial in terms of showing productivity up the chain, it is more difficult to guarantee that these systems will be as easy to maintain as if a stable release is used

Feature release systems are more applicable to organizations that have the resources to dedicate to solving technical problems. From what our team observed, the MOE IT staff is only able to do its traditional tasks by working extreme hours. With this in mind, we would advocate that sustainability be the number one goal, above any other requirement. When considering options, look to those that have a long-standing history of sustainability as opposed to systems that have new features.

In future endeavors, changes in technological structure should be accompanied by discussion relating to sustainability. If certain software has not been certified by the manufacturer as a “Stable Release”, there should be significant question as to whether or not such a system can be implemented. In addition, if the manufacturer does not have technical support, the IT department should read user manuals and discussions should be had on those user interfaces before sinking significant finances into products. In essence, before new technology is purchased, the IT department and all members who will have to provide technical service should certify that the product will be easy to maintain. Online resources provided by the manufacturer of the software should be used to educate the IT department in making such a certification.

## Web Content Filtering

Consider implementation of Ministry-Wide Content filtering. In the MOE and in other areas of Palauan Government, there has been but one major contributor to the delay of productivity: Facebook. In the US, Facebook has one specific effect on productivity, which is that people are not working as much as they should be. But in Palau, that factor is more than doubled. In other areas of Palauan Government, studies have been conducted which have shown Facebook to be the number one use of bandwidth within an organization. Not only does the usage of Facebook and other forms of social media disrupt the flow of the workday, but it also prevents people who are working from using the network from being productive.

With that in mind, social media is one but many sites that are not used for productivity and still use a consistent level of bandwidth throughout the Palauan public sector. These services can include streaming, messaging and piracy sites. And while the MOE currently does block certain ports, it cannot start blocking sites without policy drafted by the heads of the MOE.

In the coming years, the amount of devices on the MOE network is going to skyrocket. While the team cannot estimate the amount of devices currently using the network, the 1,000 tablets coming into the environment in the next few years is sure to put an entirely new stress on an already slow network system. For individuals who rely on an external connection to do their jobs, this will become an increasingly present issue in the near future.

In every element of the process and software development, the number one concern has been preventing the expenditure of unnecessary bandwidth. In fact, even the consulting team has been denied access to bandwidth at times because of this concern. With high speeds almost a decade away, other changes will need to be made to allow employees who need internet access to be more productive.

Bandwidth changes start with discussion within the Management Team. The Team must figure out which types of services can be taken off the network without disruption to professional or personal endeavors of staff that are considered a priority. Discussion should include whether certain services should only be allowed after school hours. The IT department has numerous ways to prevent or limit services based on time or user. Once criteria have been agreed upon within the Management Team, a policy should be drafted and sent to all staff. Once comments have been received on such a change, the policy can be revised to accommodate the general consensus of MOE staff and faculty. Once the policy has been modified, the MOE IT staff can put such policy into place. The team would recommend those discussions start as soon as possible.

## Collaboration Services

As part of the TCinGC program, the consultants configured Mac OS X Servers to support Jabber (Messaging) and CalDAV (Calendar) services without needing an external connection. With confirmation on delivery of invitations and the ability to accept or deny a request, these systems can save significant time for individuals who need to schedule for large groups. It is the recommendation of the consultants that an effort be made to transition staff to electronic means of communication and scheduling. As scheduling and messaging go digital, it will be easier to collaborate in larger groups and in an organization where members are hours away.

The consultants provided user manuals on configuring and using this service, but the real manpower will come from encouraging staff to step away from paper-based scheduling. While this system is powerful, it is only as powerful as the amount of people consistently using it. In order for the system to be more preferable than a paper-based solution, the system will need to be used daily by the staff.

The consultants trained fifteen individuals before departure. The consultants recommend those individuals be used to train others as soon as possible. The consultants recommend distribution of the given user manuals to assist in implantation across the Ministry.

## List of Appendices

**Tablet Integration Program**

Appendix A. Work Plan

**Project 1: Tablet Deployment Business Process Design**

Appendix B. Tablet Deployment Business Process Diagram

**Project 2: Mobile Device Management Software Implementation**

Appendix C. Specification Document
Appendix D. Test Cases in Lab and Koror Elementary School
Appendix E. Configuration Creation Guide
Appendix F. Configuration Implementation Guide for Device Manager
Appendix G. Configuration Implementation Guide for Configurator
Appendix H. Default Settings for Configuration Profile

**Project 3: Extended Access Implementation**

Appendix I. Network Diagrams
Appendix J. Test Case in Lab
Appendix K. Test Case in Koror Elementary School
Appendix L. Implementation Procedure for Koror Elementary School
Appendix M. Network Design Policy
Appendix N. Network Design Process
Appendix O. Configuration Guide of MicroTik Router
Appendix P. Configuration Guide of Ubiquity Access Point

**Project 4: RADIUS System Implementation**

Appendix Q. Configuration Guide of RADIUS Server

**Side Project: Collaboration Services**

Appendix R. User Guide of Collaboration Services

**Recommendation: IT Management Enhancement**

Appendix S. Discussion Materials for IT Management Enhancement

## About the Consultants

*Andrew Schwartz* is an undergraduate student of Information Systems at Carnegie Mellon University. His industry experience spans Network Configuration, Hardware Installation and Software Development Implementation. Andrew will receive his Bachelor's degree in May 2015 and will begin seeking employment in the fall.

*Yasuyuki Nishihara* is a graduate student of Heinz College (Master of Information Systems Management) at Carnegie Mellon University. He has been working at the IT department of the Bank of Tokyo-Mitsubishi UFJ, Ltd., the largest Japanese commercial bank, for twelve years. After his graduation, he will return to the company and resume working for the IT systems to sustain the banking business.

# Appendix A

Work Plan for "Tablet Integration Program" (as of Fri, Aug 8)

🟧 On Schedule ░ Advance Schedule 🟫 Behind Schedule

| No | | Tasks | Due | Status | Week 1<br>6/3 | Week 2<br>6/9 | Week 3<br>6/16 | Week 4<br>6/23 | Week 5<br>6/30 | Week 6<br>7/7 | Week 7<br>7/14 | Week 8<br>7/21 | Week 9<br>7/28 | Week 10<br>8/4 | Responsi<br>-bility | Outputs |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Scope<br>Planning | Design | Development<br>Implement | | Test<br>(MOE) | Test<br>(Koror Elementary) | | Training &<br>Documentation | | | | (Final Report) |
| ***Project Planning*** | | | | | | | | | | | | | | | | |
| 1 | | Scope of project | | | | | | | | | | | | | | |
| | 1 | Define scope of the project | 6-Jun | Done | 🟧 | | | | | | | | | | Team | Scope Document |
| | 2 | Break down tasks for each project | 6-Jun | Done | 🟧 | | | | | | | | | | Team | Work Plan |
| | 3 | Estimate timeline for each task | 6-Jun | Done | 🟧 | | | | | | | | | | Team | Program Timeline |
| | 4 | Present the scope to stakeholders | 6-Jun | Done | 🟧 | | | | | | | | | | Team | Meeting Agenda |
| ***Project 1: Tablet Deployment Business Process Design*** | | | | | | | | | | | | | | | | |
| 1 | | Check constraints of process building | | | | | | | | | | | | | | |
| | 1 | Identify process categories and roles | 13-Jun | Done | | 🟧 | | | | | | | | | Yuki | |
| | 2 | Check policies about inventory management of MOE | 13-Jun | Done | | 🟧 | | | | | | | | | Yuki | |
| | 3 | Check existing tablets process | 13-Jun | Done | | 🟧 | | | | | | | | | Yuki | |
| 2 | | Create business flows | | | | | | | | | | | | | | |
| | 1 | Draft "Process Flow Diagrams" for each category | 20-Jun | Done | | 🟧 | 🟧 | | | | | | | | Yuki | Flow Diagrams (Draft) |
| | 2 | Specify management factors for each process | 20-Jun | Done | | 🟧 | 🟧 | 🟫 | 🟫 | | | | | | Yuki | |
| | 3 | Discuss the flows with stakeholders | 27-Jun | Done | | | 🟧 | 🟧 | 🟫 | 🟫 | | | | | Yuki | |
| | 4 | Get approval the flows from stakeholders | 27-Jun | Done | | | 🟧 | 🟧 | 🟫 | 🟫 | 🟫 | | | | Yuki | Flow Diagrams |
| 3 | | Documentation | | | | | | | | | | | | | | |
| | 1 | Compile outputs as Business Process Document | 8-Aug | Done | | | | | | | | 🟧 | 🟧 | ░ | Yuki | Business Process Document |
| ***Project 2: Mobile Device Management Software Implementation*** | | | | | | | | | | | | | | | | |
| 1 | | Fix the requirement for MDM | | | | | | | | | | | | | | |
| | 1 | Fix the functions that the MDM should have | 20-Jun | Done | | 🟧 | 🟧 | 🟫 | 🟫 | | | | | | Andrew | |
| | 2 | Fix the management factors that the MDM should have | 20-Jun | Done | | 🟧 | 🟧 | 🟫 | 🟫 | | | | | | Andrew | |
| | 3 | Check that the system environment for the MDM works | 20-Jun | Done | | 🟧 | 🟧 | 🟫 | 🟫 | | | | | | Andrew | |
| 2 | | Check MDM systems (Apple suites) | | | | | | | | | | | | | | |
| | 1 | Research information of Apple Suite | 20-Jun | Done | | 🟧 | 🟧 | 🟫 | | | | | | | Andrew | |
| | 2 | Check Apple Profile manager and make sure it meets the requirements | 20-Jun | Done | | 🟧 | 🟧 | 🟫 | 🟫 | | | | | | Andrew | |
| | 3 | Create "Specification Document" | 20-Jun | Done | | | 🟧 | 🟫 | 🟫 | | | | | | Andrew | Specification Documents |
| 3 | | Install and test MDM system at MOE | | | | | | | | | | | | | | |
| | 1 | Purchase MDM system | 27-Jun | Done | | | | 🟧 | 🟫 | | | | | | Edwel | |
| | 2 | Set up the MDM on Lab at MOE | 27-Jun | Done | | | | 🟧 | 🟫 | 🟫 | | | | | Andrew | |
| | 3 | Create "Test Case" for MOE | 27-Jun | Done | | | | 🟧 | 🟫 | 🟫 | | | | | Andrew | Test Case (MOE) |
| | 4 | Test the MDM with iPad on Lab | 4-Jul | Done | | | | | 🟧 | 🟫 | | | | | Team | |
| | 5 | Evaluate the MDM | 4-Jul | Done | | | | | 🟧 | 🟫 | | | | | Andrew | Test Report |
| 4 | | Test at Koror Elementary School | | | | | | | | | | | | | | |
| | 1 | Set up the MDM on live system environment at MOE | 4-Jul | Done | | | | | 🟧 | 🟫 | | | | | Andrew | |
| | 2 | Create "Test Case" for Koror Elementary | 4-Jul | Done | | | | | 🟧 | 🟫 | 🟫 | | | | Andrew | Test Case (KES) |
| | 3 | Test the each function with tablets | 18-Jul | Done | | | | | | 🟧 | 🟧 | | | | Team | |
| | 4 | Test the each function with tablets (using PicoStation M2) | 1-Aug | Done | | | | | | | | | 🟧 | 🟫 | Team | |
| | 5 | Evaluate the result | 1-Aug | Done | | | | | | | | | 🟧 | 🟫 | Andrew | Test Report |
| 5 | | Training | | | | | | | | | | | | | | |
| | 1 | Create "User guides" - Set dates for staff training | 1-Aug | Done | | | | | | | | | 🟧 | 🟫 | Andrew | User Guides (for Training) |
| | 2 | Train the staff | 8-Aug | Done | | | | | | | | | 🟧 | 🟧 | Team | |

WBS_Revised

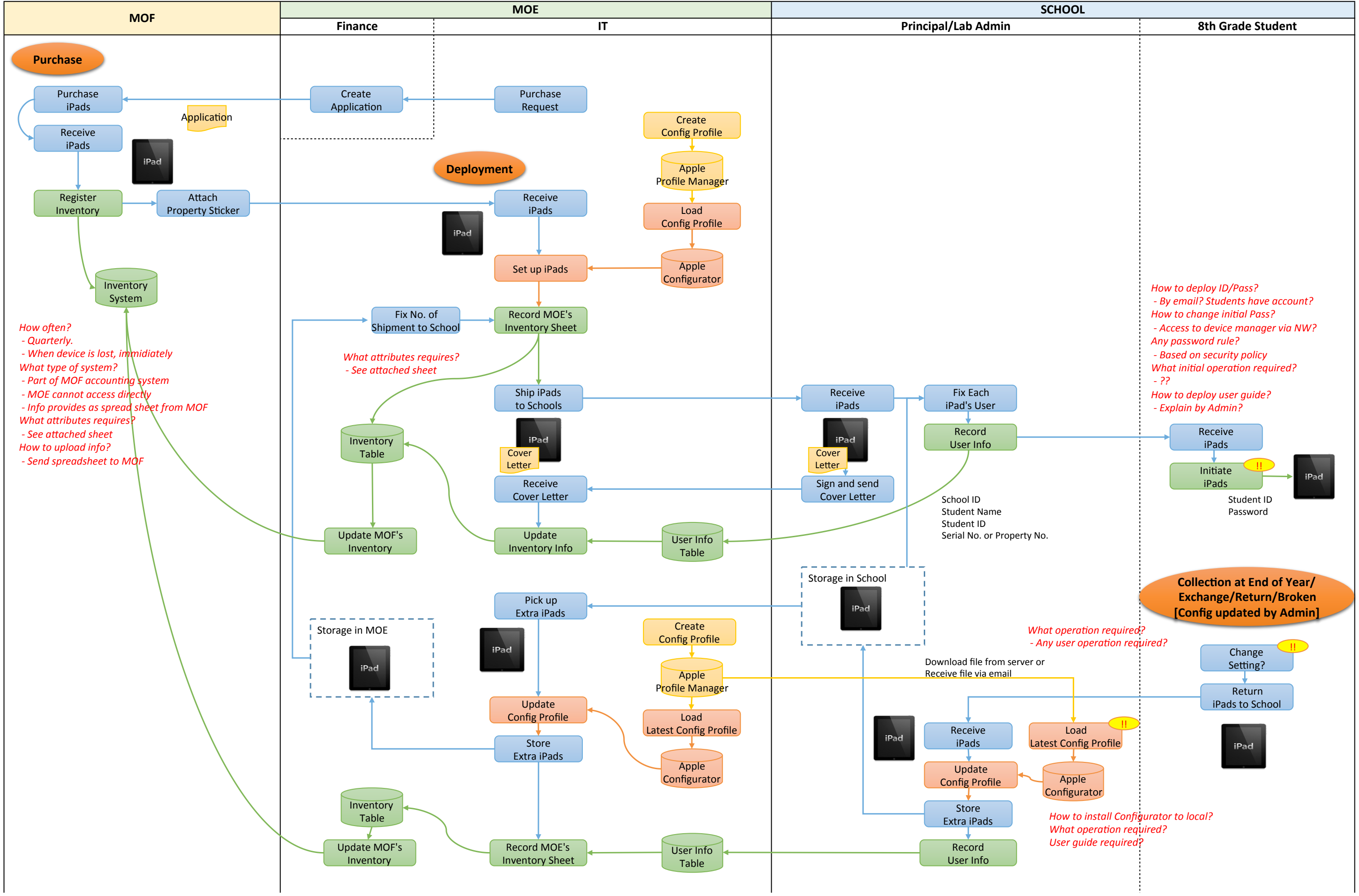
**Work Plan for "Tablet Integration Program" (as of Fri, Aug 8)**

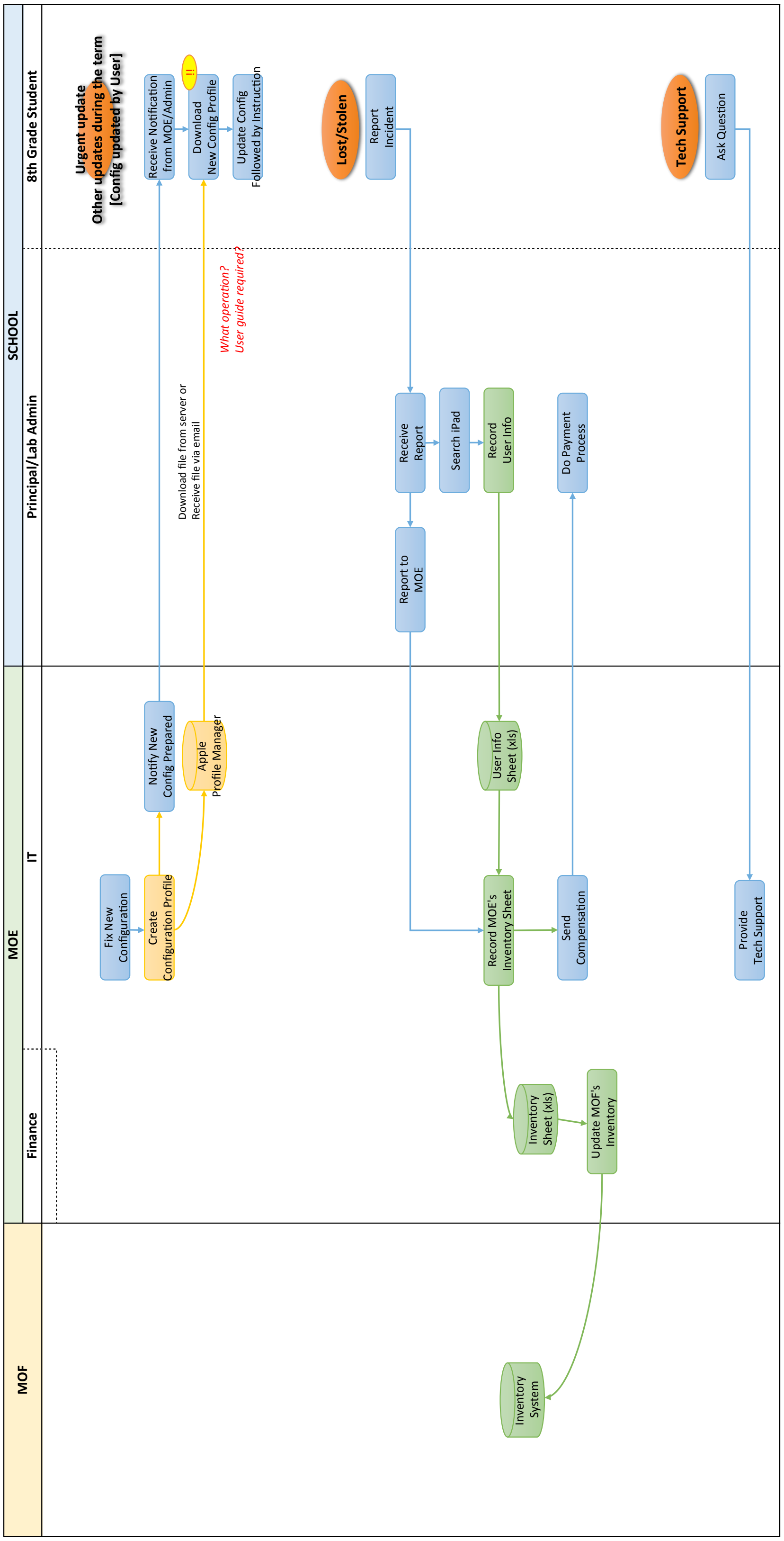
▒ On Schedule ░ Advance Schedule █ Behind Schedule

| No | | Tasks | Due | Status | Week 1 6/3 | Week 2 6/9 | Week 3 6/16 | Week 4 6/23 | Week 5 6/30 | Week 6 7/7 | Week 7 7/14 | Week 8 7/21 | Week 9 7/28 | Week 10 8/4 | Responsi -bility | Outputs |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Scope Planning | Design | Development Implement | | Test (MOE) | Test (Koror Elementary) | | Training & Documentation | | | | (Final Report) |
| *Project 3: Extended Access Implementation* | | | | | | | | | | | | | | | | |
| 1 | | Current Analysis of Koror Elementary School | | | | | | | | | | | | | | |
| | 1 | Collect network information (Logical/Physical) | 13-Jun | Done | | ▒ | | | | | | | | | Team | |
| | 2 | Investigate actual site (Physical) | 13-Jun | Done | | ▒ | | | | | | | | | Team | |
| | 3 | Fix the requirement for new network | 13-Jun | Done | | ▒ | | | | | | | | | Team | |
| 2 | | Network Design | | | | | | | | | | | | | | |
| | 1 | Create "Network Diagram" (Physical/Logical) for Koror Elementary | 13-Jun | Done | | ▒ | | | | | | | | | Yuki | Network Diagram |
| | 2 | Create common design policy for school network | 20-Jun | Done | | ▒ | ▒ | | | | | | | | Yuki | Network Design Policy |
| | 3 | Order new devices | 16-Jun | Done | | ▒ | | | | | | | | | Edwel | |
| | 4 | Order cabling/outlet (if required) | 18-Jun | Done | | ▒ | | | | | | | | | Edwel | |
| 3 | | Server Design | | | | | | | | | | | | | | |
| | 1 | Design servers (DHCP/DNS...) | 20-Jun | Done | | ▒ | ▒ | | | | | | | | Team | |
| | 2 | Fix configuration for servers | 27-Jun | Done | | | ▒ | ░ | | | | | | | Team | |
| 4 | | Test (MOE local) | | | | | | | | | | | | | | |
| | 1 | Develop test network (lab) at MOE | 27-Jun | Done | | | ▒ | ░ | | | | | | | Yuki | |
| | 2 | Create "Test Case" | 27-Jun | Done | | | ▒ | ▒ | | | | | | | Yuki | Test Case for NW (MOE) |
| | 3 | Connect lab network to MOE live network | 4-Jul | Done | | | | | ▒ | | | | | | Yuki | |
| | 4 | Test the devices on Lab environment | 4-Jul | Done | | | | | ▒ | █ | | | | | Yuki | Test Report (MOE) |
| | 5 | Test the APs on Lab environemnt | 25-Jul | Done | | | | | | | | ▒ | █ | | Yuki | Test Report (MOE) |
| 5 | | Implement and test new network devices (Koror Elementary) | | | | | | | | | | | | | | |
| | 1 | Prepare new cabling for Lab 2 building | 27-Jun | Done | | | ▒ | ░ | | | | | | | Warren | |
| | 2 | Remove PCs in Lab 2 at Koror Elementary | 27-Jun | Done | | | ▒ | ▒ | ░ | | | | | | Thomas | |
| | 3 | Check the site before implementation | 4-Jul | Done | | | | | ▒ | | | | | | Yuki | |
| | 4 | Set up the Router/APs (Temporary) for Admin Office | 11-Jul | Done | | | | | | ▒ | | | | | Team | Implementation Procedure |
| | 5 | Create "Test Case" | 11-Jul | Done | | | | | | ▒ | | | | | Yuki | Test Case for NW (MOE) |
| | 6 | Test the devices on Koror Elementary | 11-Jul | Done | | | | | | ▒ | | | | | Team | Test Report (KES) |
| | 7 | Order new devices (PicoStation M2) | 4-Jul | Done | | | | | ▒ | | | | | | Edwel | |
| | 8 | Replace the APs for each room | 25-Jul | Done | | | | | | | | ▒ | █ | █ | Yuki | |
| | 9 | Test the devices (PicoStation M2) on Koror Elementary | 25-Jul | Done | | | | | | | | ▒ | █ | █ | Team | Test Report (KES) |
| 6 | | Documentation | | | | | | | | | | | | | | |
| | 1 | Compile outputs as "Project Documents" | 8-Aug | Done | | | | | | | | ░ | ▒ | ▒ | Yuki | Project Documents |
| *Project 4: RADIUS System Implementation* | | | | | | | | | | | | | | | | |
| 1 | | Research RADIUS Platforms and present best solution | | | | | | | | | | | | | | |
| | 1 | Build information on pros and cons of OSX Server System | 20-Jun | Done | | ▒ | ░ | | | | | | | | Andrew | |
| | 2 | Present Solution | 20-Jun | Done | | ▒ | ░ | | | | | | | | Andrew | |
| 2 | | Install RADUIS System on MOE Server and test with Edwel and Staff | | | | | | | | | | | | | | |
| | 1 | Build RADIUS System on blank server | 27-Jun | Done | | | ▒ | ░ | | | | | | | Andrew | |
| | 2 | Install Mock accounts and test with Andrew & Yuki | 4-Jul | Done | | | ▒ | | ░ | | | | | | Andrew | |
| | 3 | Expand to Airport and test with Test IDs on Lab Network | 4-Jul | Done | | | | | ▒ | █ | | | | | Andrew | Working RADIUS Network |
| 3 | | Import account data and expand server to entire MOE building | | | | | | | | | | | | | | |
| | 1 | Notify MOE Staff of Wi-Fi Change | 11-Jul | - | Shift the task to out of scope | | | | | | | | | | Andrew | Notification |
| | 2 | Manually Assign Usernames and Passwords | 11-Jul | - | Shift the task to out of scope | | | | | | | | | | Andrew | |
| | 3 | Transition to new system over a weekend and test with new accounts | 11-Jul | - | Shift the task to out of scope | | | | | | | | | | Andrew | Test Report (MOE) |
| 4 | | Import account data and expand server to Koror Elementary | | | | | | | | | | | | | | |
| | 1 | Test RADIUS authentication with PicoStation M2 in Lab network | 25-Jul | Done | | | | | | | | ▒ | █ | | Yuki | |
| | 2 | Test RADIUS authentication with PicoStation M2 in KES | 25-Jul | Done | | | | | | | | ▒ | █ | █ | Yuki | |
| | 3 | Notify Koror Elementary Staff of Wi-Fi Change | 1-Aug | | Shift the task to out of scope | | | | | | | | | | Andrew | Notification |
| | 4 | Manually Assign Usernames and Passwords | 1-Aug | | Shift the task to out of scope | | | | | | | | | | Andrew | |
| | 5 | Transition to new system over a weekend and test with random accounts | 1-Aug | | Shift the task to out of scope | | | | | | | | | | Andrew | Test Report (KES) |
| 5 | | Documentation | | | | | | | | | | | | | | |
| | 1 | Compile outputs as "Project Documents" | 8-Aug | Done | | | | | | | | | | ▒ | Andrew | Project Documents |

# Appendix B

**Business Flow of Tablet Deployment**




SCHOOL
8th Grade Student
Principal/Lab Admin
MOE
IT
Finance
MOF
Urgent update
Other updates during the term
[Config updated by User]
Receive Notification from MOE/Admin
!!
Download New Config Profile
Update Config Followed by Instruction
What operation?
User guide required?
Download file from server or
Receive file via email
Fix New Configuration
Create Configuration Profile
Notify New Config Prepared
Apple Profile Manager
Lost/Stolen
Report Incident
Receive Report
Search iPad
Record User Info
Report to MOE
Do Payment Process
User Info Sheet (xls)
Record MOE's Inventory Sheet
Send Compensation
Inventory Sheet (xls)
Update MOF's Inventory
Inventory System
Tech Support
Ask Question
Provide Tech Support

**Approach to fill in MOF's inventory**

1. MOE receives iPads and assigns Property Tag and School which will receive the iPad.
   MOE records all information (Category A-D) into MOE's inventory system.
   (* Normally, info of Category A-C is provided by MOF; but in order for MOE to save a time, MOE do that instead of MOF)
2. School admins assign iPad to students. They record Property No, Student ID and Student Name to School's Spreadsheet.
3. MOE receives school's spreadsheets and copy them into MOE's inventory system.
4. MOE fills in MOF's inventory (provided as spreadsheet) and then, submits inventory information to MOF.

| Cat | Attributes | School's Spreadsheet | MOE's inventory | MOF's inventory |
|---|---|---|---|---|
| A | Info on "Purchase Order"<br>(PO#, Purchase Date..) | | 1<br>Input by MOE* | 4<br>Copy from MOE's submission |
| B | Property Tag<br>(or Property ID) | 2<br>Input by School | Input by MOE* | Copy from MOE's submission |
| C | Info on "Package Box" and "Device"<br>(Model, Description...) | | Input by MOE* | Copy from MOE's submission |
| D | Info from MOE Inventory Staff<br>(Condition, Location...) | Input by School | Input by MOE | Copy from MOE's submission |
| E | Info from MOF<br>(Sub account info...) | | | Input by MOF |
| F | Info from School<br>(Student ID) | Input by School | 3<br>Copy from School's Sheet | Copy from MOE's submission |

| How to verify (by MOE) the information |
|---|
| Check Actual devices When receiving them |
| Check Actual devices When receiving them |
| (Input by MOE) |
| (Input by MOE) |
| Trust information which MOF inputs |
| Trust information which school inputs |

**Approach to fill in MOF's inventory (Detail Attributes)**

| # | MOF Inventory Table | MOE Inventory Table | Description | Cat | Original Data Source | Input |
|---|---|---|---|---|---|---|
| 1 | PO # | po_no | Purchase Order Number | A | Purchase Order | MOE Staff* |
| 2 | PURCH-DT | rcv_date | Purchase Date | A | Purchase Order | MOE Staff* |
| 3 | COST | (N/A) | Purchase Cost | A | Purchase Order | MOF |
| 4 | ACQ-COST | (N/A) | Acquisition Cost (not in PO) | A | MOF | MOF |
| 5 | DESCRIPTION | description | Description | C | Package Box | MOE Staff* |
| 6 | MODEL | model_no | Model Number | C | Package Box | MOE Staff* |
| 7 | SERIAL | serioal_no | Serial Number | C | Package Box | MOE Staff* |
| 8 | (N/A) | wifi_address | Wi-FI MAC Address | C | Device Information | (N/A) |
| 9 | (N/A) | bluetooth_address | Bluetootk MAC Address | C | Device Information | (N/A) |
| 10 | ASSET TAG | asset_tag | Property TAG | B | Assigned by MOF | MOE Staff* |
| 11 | (N/A) | asset_id | Property ID | B | Assigned by MOE | MOE Staff (if required) |
| 12 | MFR | mfr | Manufacturer | C | Package Box | MOE Staff* |
| 13 | MFR-DATE | mfr_date | Manufacture Date | C | Package Box | MOE Staff* |
| 14 | BRAND | brand | Brand | C | Package Box | MOE Staff* |
| 15 | MIN | (N/A) | Ministry | - | Data is always "MOE" | MOE Staff |
| 16 | BUR | (N/A) | Bureau | - | MOE Organization Chart | MOE Staff |
| 17 | DIV | (N/A) | Division | - | MOE Organization Chart | MOE Staff |
| 18 | (N/A) | unit | Accountable Unit for the Item | D | MOE Organization Chart | MOE Staff |
| 19 | ORG | org | Account charged for the purchase | A | Purchase Order | MOE Staff* |
| 20 | C-CTR | cctr | Cost Center charged for the purchase | A | Purchase Order | MOE Staff* |
| 21 | S-ACCT | (N/A) | Sub-account charged for the purchase | E | MOF | MOF |
| 22 | CLASS | (N/A) | Merchandise type | E | MOF | MOF |
| 23 | FUND | (N/A) | Some accounting code used by MOF | E | MOF | MOF |
| 24 | C. CODE | cond | Condition code | D | Inventory Work | MOE Inventory Staff |
| 25 | LST.INV.DT | inv_date | Last Inventory Date | D | Inventory Work | MOE Inventory Staff |
| 26 | LOC. ST. | loc_code | Location Status. | D | Inventory Work | MOE Inventory Staff |
| 27 | CONDITION / LOCATION | remarks | This is a comment area. | D | - | MOE Staff |
| 28 | (N/A) | user_id | Student ID/Personnel ID | F | School's Spreadsheet | School Admins |

*Normally, the attribute is provided by MOF; but in order to save time, MOE does that instead of MOF

# Appendix C

## Specification Document for Tablet Management Systems

### 1. Purpose

- The Ministry of Education (MOE) plans to purchase and deploy iPads for all 8th grade students of 16 elementary schools in Palau. To support the deployment, MOE want to implement software(s) to manage and configure the iPads. This program falls under the College Access Challenge Grant (CACG) under the US Department of Education. The CACG budget must be used by November 14th 2014, so our program must expend its resources by October 30th of this year.

### 2. Target Devices

- Apple iPad (250 devices). 50 devices will arrive by August 15, the rest of devices will arrive by October 30.
- 50 iPads will be implemented in two classrooms (25 students for each classroom) at Koror Elementary School as model case. MOE will then wait for the appropriate timing to order the rest, watching for the launch of a new model in October.
- 250 iPads are disseminated between 195 students + 14 principles + 25 teachers + 16 spare stock.
- Existing Samsung Galaxy Tablets (400 devices) are out of scope in this project. MOE will launch a new project to manage these existing devices based on the success of our endeavor.
- The iPads will initially be used within the school. The iPads can connect to each schools' Wi-Fi network, provided in the Admin Offices, Libraries, 8th Grade Classrooms, and Computer Labs. For now the devices cannot connect outside schools like the student's home network. In the future, students may be granted use of networks outside the school.

### 3. Business Requirements

(1) Attributes of each iPad which the MOE wants to manage

I. Inventory Management Perspective

- MOE should know the user/current owner information of each iPad in order to correctly manage the inventory information in Ministry of Finance (MOF).
- MOF assigns a "Property No." for each iPad before sending them to the MOE. MOF will keep the combination of "Serial No." and "Property No." on their inventory system. MOF will export their inventory information to an excel file, and then send that file to the MOE.
- MOE will retrieve "Student ID" and "Property No." from each school, so that they can combine "Serial No.", "Property No." and "Student ID" into one table. MOE will then store the set of information in the MOE's inventory file (also an excel spread sheet).
- MOE should update the inventory information to MOF's inventory system at least once a quarter. If the device is lost or stolen, however, MOE will have to update the information to the MOF's inventory system as soon as possible.

II. Tablet Management Perspective

- MOE wants to know basic information of each tablet for monitoring and security purposes, such as "iOS version", "Installed Applications".
- Some attributes could be changed (Column of "Info" is "Dynamic" on Table 1) after deployment, so that MOE wants to keep current status of these attributes on the system(s) (Column of "Update" is "Yes" on Table 1)
- The frequency of updating depends on the system restriction (there is no specific requirement currently).

**Table 1: List of Candidate Attributes**

| # | Attributes | Type |
|---|---|---|
| 1 | Serial No | Static |
| 2 | Model Name | Static |
| 3 | iOS Version | Dynamic |
| 4 | # Installed Applications | Dynamic |
| 5 | List of installed Applications | Dynamic |
| 6 | Available Memory | Dynamic |
| 7 | Property No | Static |
| 8 | Description | Static |
| 9 | School Name | Dynamic |
| 10 | Student ID | Dynamic |
| 11 | Student Name | Dynamic |

(2) Functions of the systems which MOE wants to operate

- These are the typical functions that a Mobile Device Management (MDM) system could provide (Table 2). MOE wants to implement the functions whose value of "Requirement" is "YES": "Remote Wipe" and "Remote Configuration Profile Change".
- MDM system should provide such functions; but if the system does not support the functions, business operations should provide alternative methods to cover the functions.

**Table 2: List of Functions which MDM system generally supports**

| # | Typical Functions | | Requirement |
|---|---|---|---|
| 1 | Remote Lock | | No |
| 2 | **Remote Wipe** | | **Yes** |
| 3 | Password Reset | Device | No |
| 4 | | User | No |
| 5 | Password Policy Setting | Device | No |
| 6 | | User | No |
| 7 | **Remote Configuration Profile Update** | | **Yes** |
| 8 | Function Limitation | Camera | No |
| 9 | | Bluetooth | No |
| 10 | | Wireless Connection | No |
| 11 | | Tethering | No |
| 12 | URL Filtering | | No |
| 13 | Application Controll | Install | No |
| 14 | | Uninstall | No |
| 15 | | Software Update | No |
| 16 | Screen Capture | | No |
| 17 | GPS Location | | No |

## 4. Selecting MDM system

(1) Considerations

- Most of MDM solutions cannot be selected for the following two reasons:
  - Cloud-based MDM solutions cannot be implemented in Palau because the Internet connection is unstable and its bandwidth is too narrow to work cloud-based solutions in the country.
  - MDM solutions are basically charged depending on the number of devices year by year. MOE does not like this type of payment scheme due to the structure of grant.
- Apple provides software solutions to manage Apple products. They work on the Mac OS server (on MOE intranet) and they are free so that we choose Apple Suites (Apple Configurator and Apple Profile Manager) as the candidates of MDM solution.

(2) Modifying Requirements

- The attributes that the Apple Suite can handle are limited, and the functions that the Apple Suite can provide are also affected by the Internet restriction. Hence, we have to modify the requirements to align with the capability of the software products.
- “Apple Profile Manager” has MDM services to manage Apple devices remotely via network. However, just like all MDM services that interact with apple products, this service is completely based on the Apple Push Notification Service (APNS). After weeks of testing it was determined that APNS could not be relied on given the limited bandwidth accessible at the MOE and its schools. While it is still possible to have the functionality is possible in the system, we were not able to prove a level of success significant enough to feel comfortable using it in our system.
- We decided to develop the MDM system based on “Apple Configurator” by covering lack of the services and functions by business operations or by exclude MOE’s requirements.

- The modified requirements (attributes and functions) are shown as below:

**Table 3: Modified Attributes**

| # | Attributes | Type | Information Strage | Storage Responsibility |
|---|---|---|---|---|
| 1 | Serial No | Static | Spreadsheet in MOE | MOE Staff |
| 2 | Model Name | Static | Spreadsheet in MOE | MOE Staff |
| 3 | iOS Version | Unavailable | - | - |
| 4 | # Installed Applications | Unavailable | - | - |
| 5 | List of installed Applications | Unavailable | - | - |
| 6 | Available Memory | Unavailable | - | - |
| 7 | Property No | Static | Spreadsheet in MOE | MOE Staff |
| 8 | Description | Static | Spreadsheet in MOE | MOE Staff |
| 9 | School Name | Dynamic | Spreadsheet in MOE | School Administrators |
| 10 | Student ID | Dynamic | Spreadsheet in MOE | School Administrators |
| 11 | Student Name | Dynamic | Spreadsheet in MOE | School Administrators |

**Table 4: Modified Functions**

| # | Typical Functions | | Original Requirement | Software/Service | Availability | Conclusion |
|---|---|---|---|---|---|---|
| 1 | Remote Lock | | No | APNS | No | Out of Scope |
| 2 | **Remote Wipe** | | **Yes** | APNS | **No** | **Out of Scope** |
| 3 | Password Reset | Device | No | Configuration Profile | Yes | - |
| 4 | | User | No | Open Directory | Yes | - |
| 5 | Password Policy Setting | Device | No | Configuration Profile | Yes | - |
| 6 | | User | No | Open Directory | Yes | - |
| 7 | **Remote Configuration Profile Update** | | **Yes** | APNS | **No** | **Manually Control** |
| 8 | Function Limitation | Camera | No | Configuration Profile | Yes | - |
| 9 | | Bluetooth | No | Unavailable | No | Out of Scope |
| 10 | | Wireless Connection | No | Configuration Profile | Yes | - |
| 11 | | Tethering | No | Unavailable | No | Out of Scope |
| 12 | URL Filtering | | No | Configuration Profile | Yes | - |
| 13 | Application Controll | Install | No | APNS | No | Out of Scope |
| 14 | | Uninstall | No | APNS | No | Out of Scope |
| 15 | | Software Update | Yes | APNS | No | Out of Scope |
| 16 | Screen Capture | | No | Unavailable | No | Out of Scope |
| 17 | GPS Location | | No | Unavailable | No | Out of Scope |

## 5. System structure

(1) Software

- Apple Configurator
- iPad's User Table (Spreadsheet)

(2) Hardware

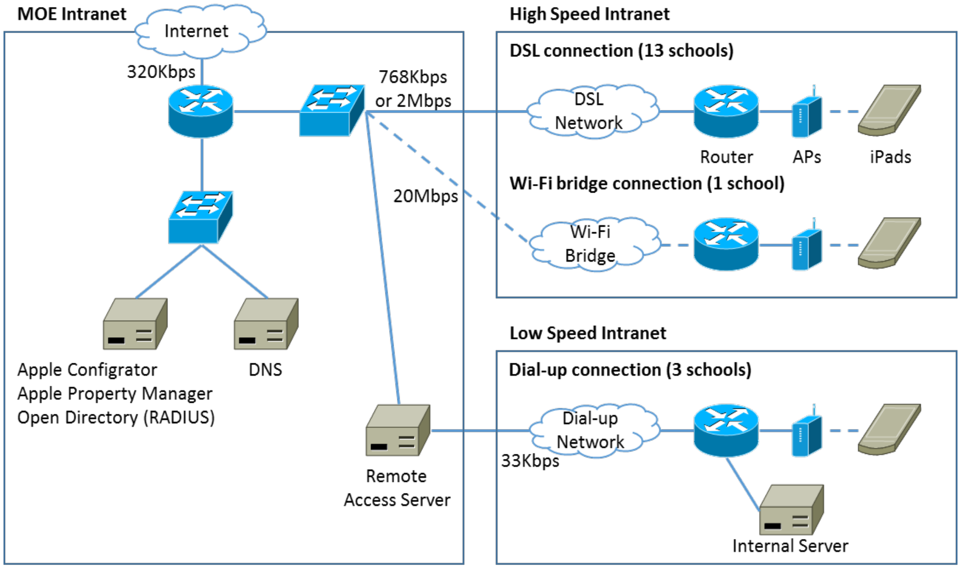
- "Apple Configurator" runs on an Apple Mac mini server at MOE. Detailed specifications show as following. Please also note that both Profile Manager and Apple Configurator can be run and accessed by any new Macintosh Computer.

  Minimum specs needed: core duo i7 2.3GHz, 64GB SSD, 8GB RAM, GB Ethernet, 100MB Ethernet.

- The iPad User Table (Spreadsheet) will be stored on existing file server.

(3) Network Structure

- Network Structure of MOE and each school is shown as below.
- Internet and Intranet connection may be a restriction to use devices via network due to its bandwidth.

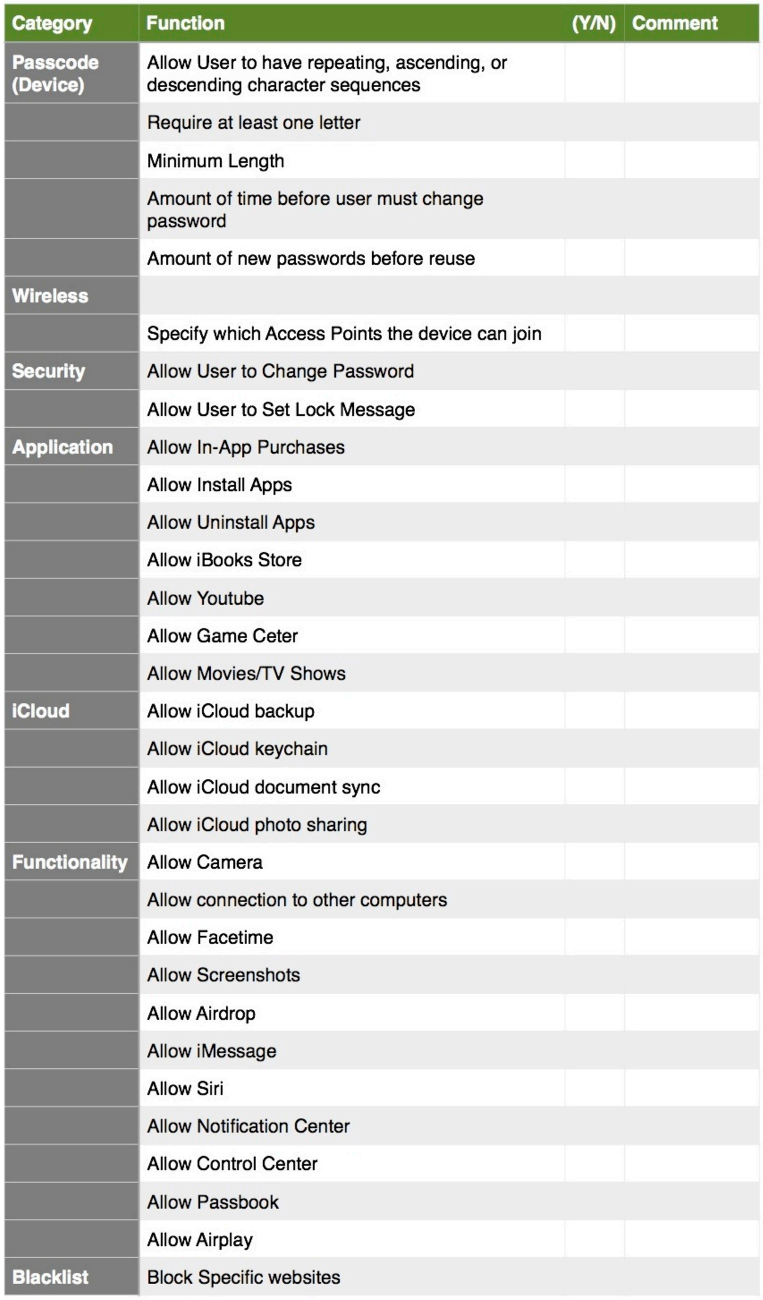


**6. Functions**

(1) Apple Configurator

- Apple Configurator can manage the configuration of iPad's via USB connection:
    - iOS update
    - Configuration Profile
        - Group and User Settings
    - App and Document
    - Wall paper and Lock screen
    - Device name
        - Organization Information – Name, Phone, Email & Address

(2) Configuration Profile



| Category | Function | (Y/N) | Comment |
|---|---|---|---|
| Passcode (Device) | Allow User to have repeating, ascending, or descending character sequences | | |
| | Require at least one letter | | |
| | Minimum Length | | |
| | Amount of time before user must change password | | |
| | Amount of new passwords before reuse | | |
| Wireless | | | |
| | Specify which Access Points the device can join | | |
| Security | Allow User to Change Password | | |
| | Allow User to Set Lock Message | | |
| Application | Allow In-App Purchases | | |
| | Allow Install Apps | | |
| | Allow Uninstall Apps | | |
| | Allow iBooks Store | | |
| | Allow Youtube | | |
| | Allow Game Ceter | | |
| | Allow Movies/TV Shows | | |
| iCloud | Allow iCloud backup | | |
| | Allow iCloud keychain | | |
| | Allow iCloud document sync | | |
| | Allow iCloud photo sharing | | |
| Functionality | Allow Camera | | |
| | Allow connection to other computers | | |
| | Allow Facetime | | |
| | Allow Screenshots | | |
| | Allow Airdrop | | |
| | Allow iMessage | | |
| | Allow Siri | | |
| | Allow Notification Center | | |
| | Allow Control Center | | |
| | Allow Passbook | | |
| | Allow Airplay | | |
| Blacklist | Block Specific websites | | |

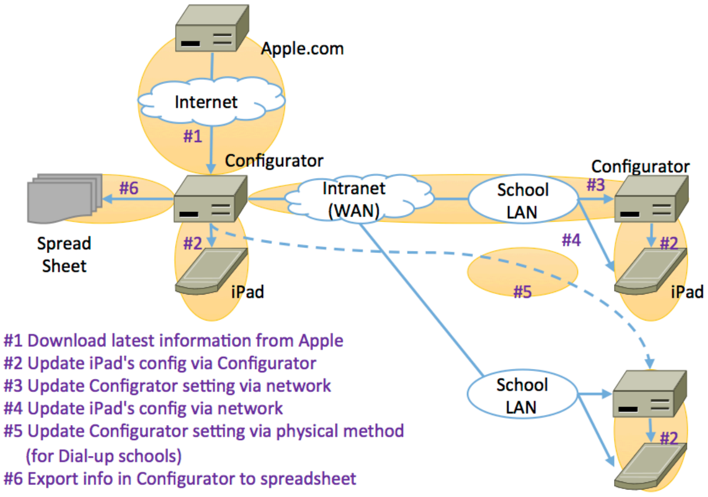
(3) iPad user table (Spreadsheet)

- Edwel has built a website which teachers will enter their student device data into.
- The website will use our Open Directory Server to authenticate

## 7. Interfaces

(1) Apple Configurator

- Create Configuration Profiles and install via Apple Configurator
- Update new Configuration Profiles onto iPad from MOE to iPad's on school LAN via Apple Configurator or via a web interface set up on the Collaboration Server.


Apple.com
Internet
#1
Configurator
Intranet
(WAN)
School
LAN
Configurator
#3
#6
Spread
Sheet
#2
iPad
#4
#2
#5
iPad
School
LAN
#2
#1 Download latest information from Apple
#2 Update iPad's config via Configurator
#3 Update Configrator setting via network
#4 Update iPad's config via network
#5 Update Configurator setting via physical method
(for Dial-up schools)
#6 Export info in Configurator to spreadsheet

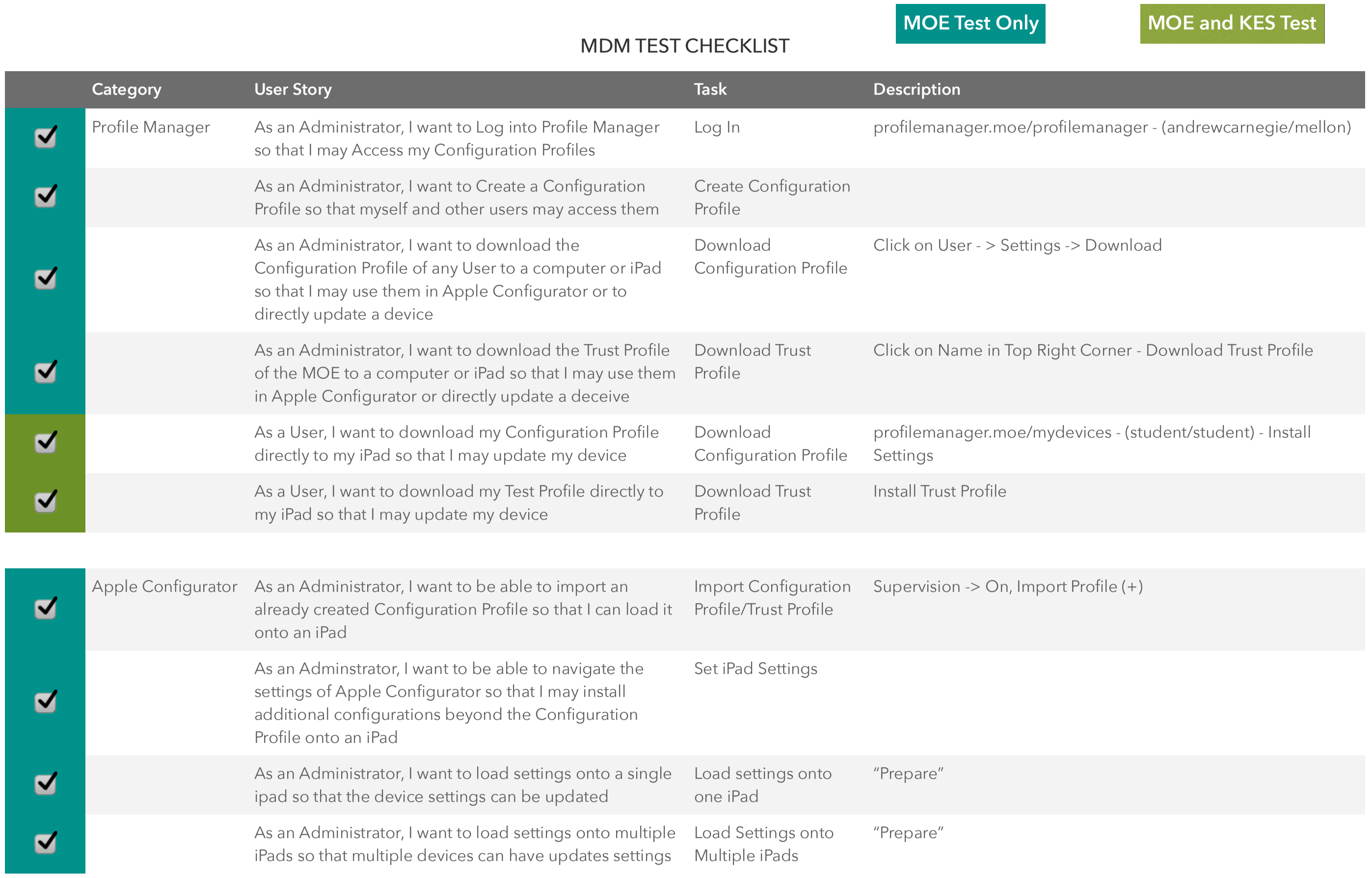
## 8. Security

- Administrator(s) and the MOE IT Department can access Apple Configurator and Apple Profile Manager with a specific ID and password. All configuration profiles will need a password combination to be removed. Network access control on router in MOE prohibits to access from outside MOE network, such as schools.

## 9. Operations

- Please refer to "Business Flow Diagram" to grasp big picture of the new deployment flow

# Appendix D



MOE Test Only

MOE and KES Test

MDM TEST CHECKLIST

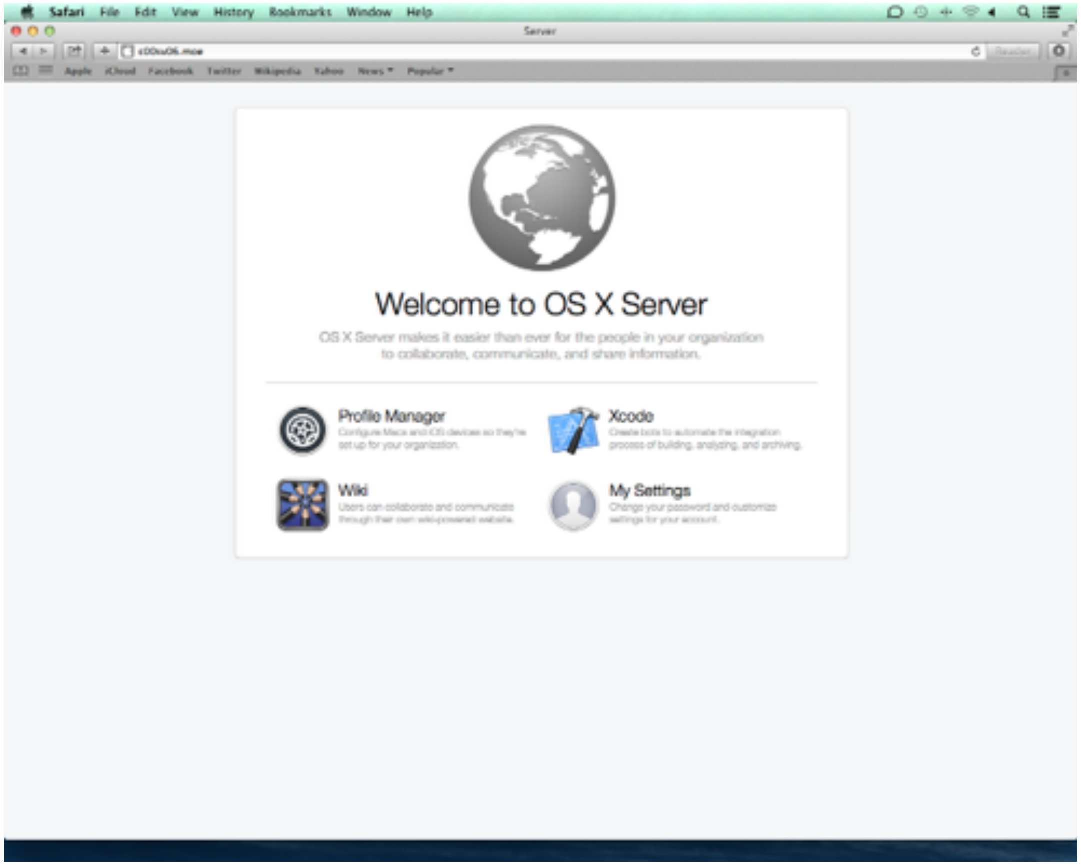
| | Category | User Story | Task | Description |
|---|---|---|---|---|
| ✓ | Profile Manager | As an Administrator, I want to Log into Profile Manager so that I may Access my Configuration Profiles | Log In | profilemanager.moe/profilemanager - (andrewcarnegie/mellon) |
| ✓ | | As an Administrator, I want to Create a Configuration Profile so that myself and other users may access them | Create Configuration Profile | |
| ✓ | | As an Administrator, I want to download the Configuration Profile of any User to a computer or iPad so that I may use them in Apple Configurator or to directly update a device | Download Configuration Profile | Click on User - > Settings -> Download |
| ✓ | | As an Administrator, I want to download the Trust Profile of the MOE to a computer or iPad so that I may use them in Apple Configurator or directly update a deceive | Download Trust Profile | Click on Name in Top Right Corner - Download Trust Profile |
| ✓ | | As a User, I want to download my Configuration Profile directly to my iPad so that I may update my device | Download Configuration Profile | profilemanager.moe/mydevices - (student/student) - Install Settings |
| ✓ | | As a User, I want to download my Test Profile directly to my iPad so that I may update my device | Download Trust Profile | Install Trust Profile |
| ✓ | Apple Configurator | As an Administrator, I want to be able to import an already created Configuration Profile so that I can load it onto an iPad | Import Configuration Profile/Trust Profile | Supervision -> On, Import Profile (+) |
| ✓ | | As an Adminstrator, I want to be able to navigate the settings of Apple Configurator so that I may install additional configurations beyond the Configuration Profile onto an iPad | Set iPad Settings | |
| ✓ | | As an Administrator, I want to load settings onto a single ipad so that the device settings can be updated | Load settings onto one iPad | "Prepare" |
| ✓ | | As an Administrator, I want to load settings onto multiple iPads so that multiple devices can have updates settings | Load Settings onto Multiple iPads | "Prepare" |

# Appendix E

# Palau Ministry of Education

## Configuration Profile Creation Guide

MOE Information Technology - Last Updated August 1, 2014



Welcome to OS X Server

OS X Server makes it easier than ever for the people in your organization to collaborate, communicate, and share information.

Profile Manager
Configure Macs and iOS devices so they're set up for your organization.

Xcode
Create bots to automate the integration process of building, analyzing, and archiving.

Wiki
Users can collaborate and communicate through their own wiki-powered website.

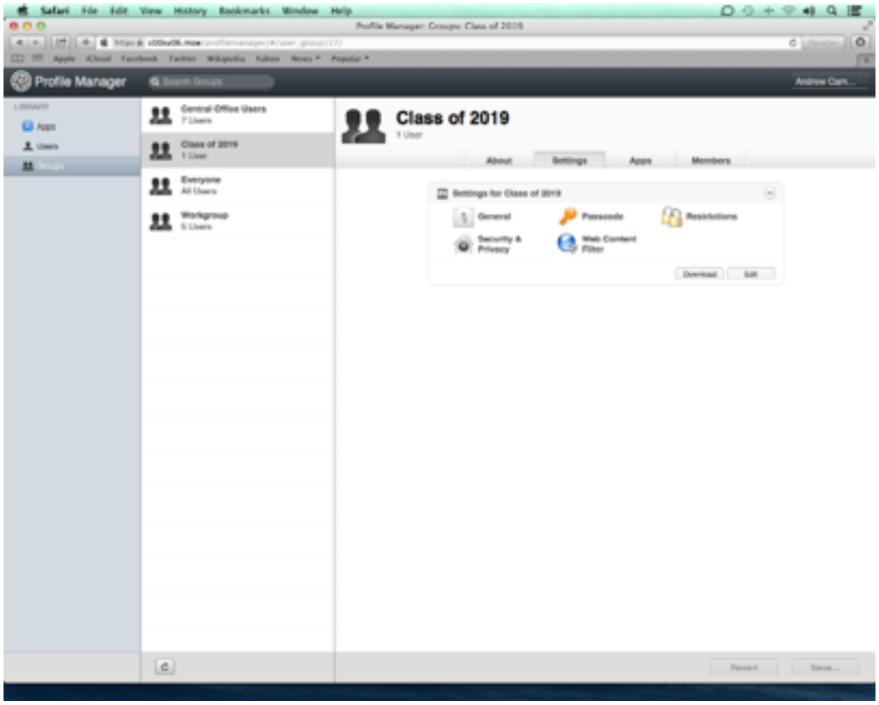
My Settings
Change your password and customize settings for your account.

## Introduction

Welcome to the Configuration Profile Creation Guide!

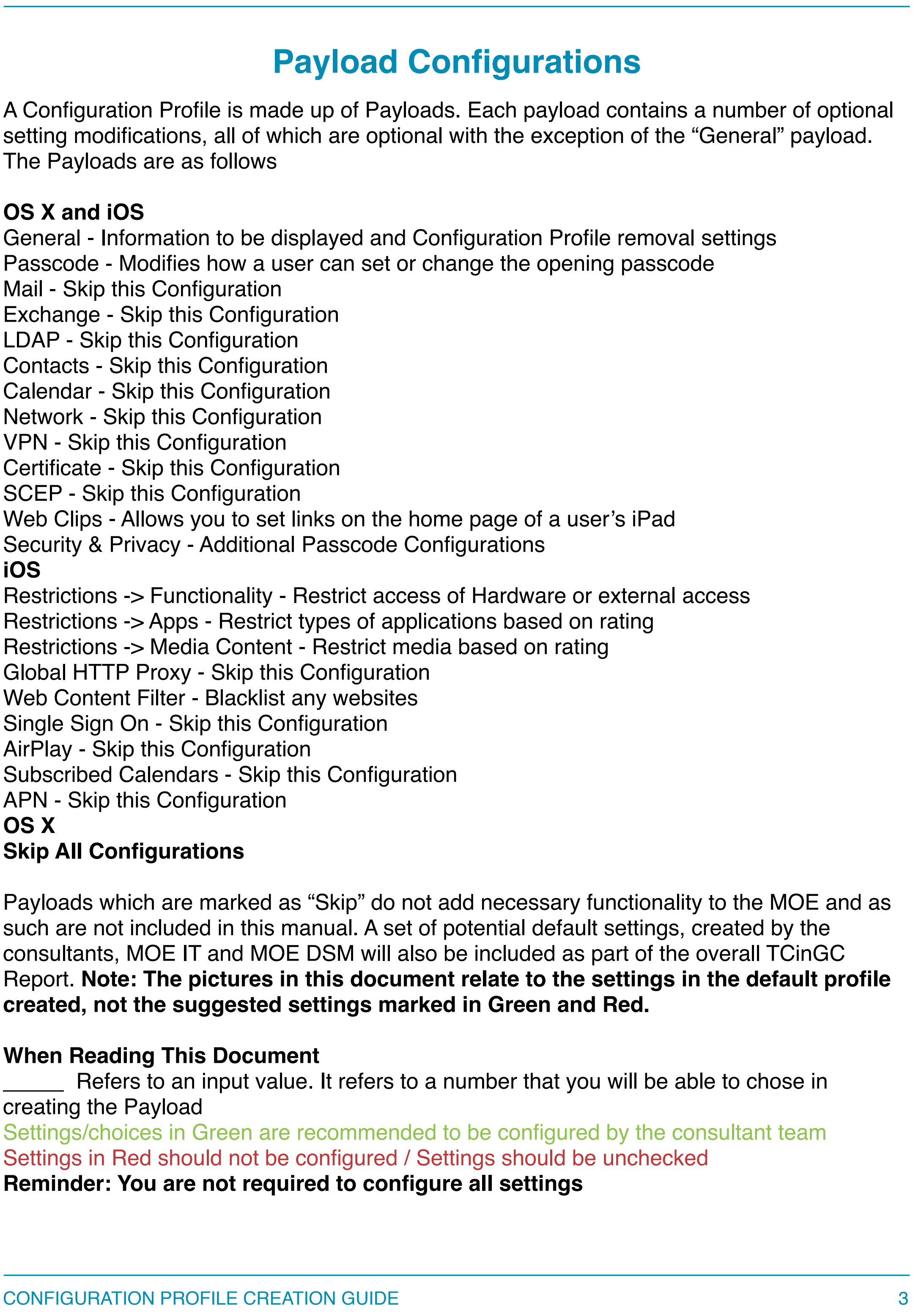
Before we get started, let's make sure that our groups and users and set up on OSX Server. When we create a configuration profile, we do so on a user or group that we have already created in Open Directory.

Now that we have our users and groups configured, let's go to c00sv06.moe/profilemanger
We will have to log in 2 times as an administrator, once to log into the MOE system and once to log into the profile manager itself.



Now that we have logged in, we have to select either the user or group for which we would like to edit settings. NOTE: You can only edit the settings of the users or groups that MOEIT has authorized you for. If you are MOEIT staff, you should be able to edit any user or group.

Once you have selected a user, go to settings and then click edit. The window that pops up will allow you to configure specific payloads for any setting that you would like. To create a payload, click the category and begin. Do not edit payloads in the OSX level. These settings will not apply to the iPad When you are finished, click Save.



# Payload Configurations

A Configuration Profile is made up of Payloads. Each payload contains a number of optional setting modifications, all of which are optional with the exception of the “General” payload. The Payloads are as follows

**OS X and iOS**
General - Information to be displayed and Configuration Profile removal settings
Passcode - Modifies how a user can set or change the opening passcode
Mail - Skip this Configuration
Exchange - Skip this Configuration
LDAP - Skip this Configuration
Contacts - Skip this Configuration
Calendar - Skip this Configuration
Network - Skip this Configuration
VPN - Skip this Configuration
Certificate - Skip this Configuration
SCEP - Skip this Configuration
Web Clips - Allows you to set links on the home page of a user’s iPad
Security & Privacy - Additional Passcode Configurations
**iOS**
Restrictions -> Functionality - Restrict access of Hardware or external access
Restrictions -> Apps - Restrict types of applications based on rating
Restrictions -> Media Content - Restrict media based on rating
Global HTTP Proxy - Skip this Configuration
Web Content Filter - Blacklist any websites
Single Sign On - Skip this Configuration
AirPlay - Skip this Configuration
Subscribed Calendars - Skip this Configuration
APN - Skip this Configuration
**OS X**
**Skip All Configurations**

Payloads which are marked as “Skip” do not add necessary functionality to the MOE and as such are not included in this manual. A set of potential default settings, created by the consultants, MOE IT and MOE DSM will also be included as part of the overall TCinGC Report. **Note: The pictures in this document relate to the settings in the default profile created, not the suggested settings marked in Green and Red.**

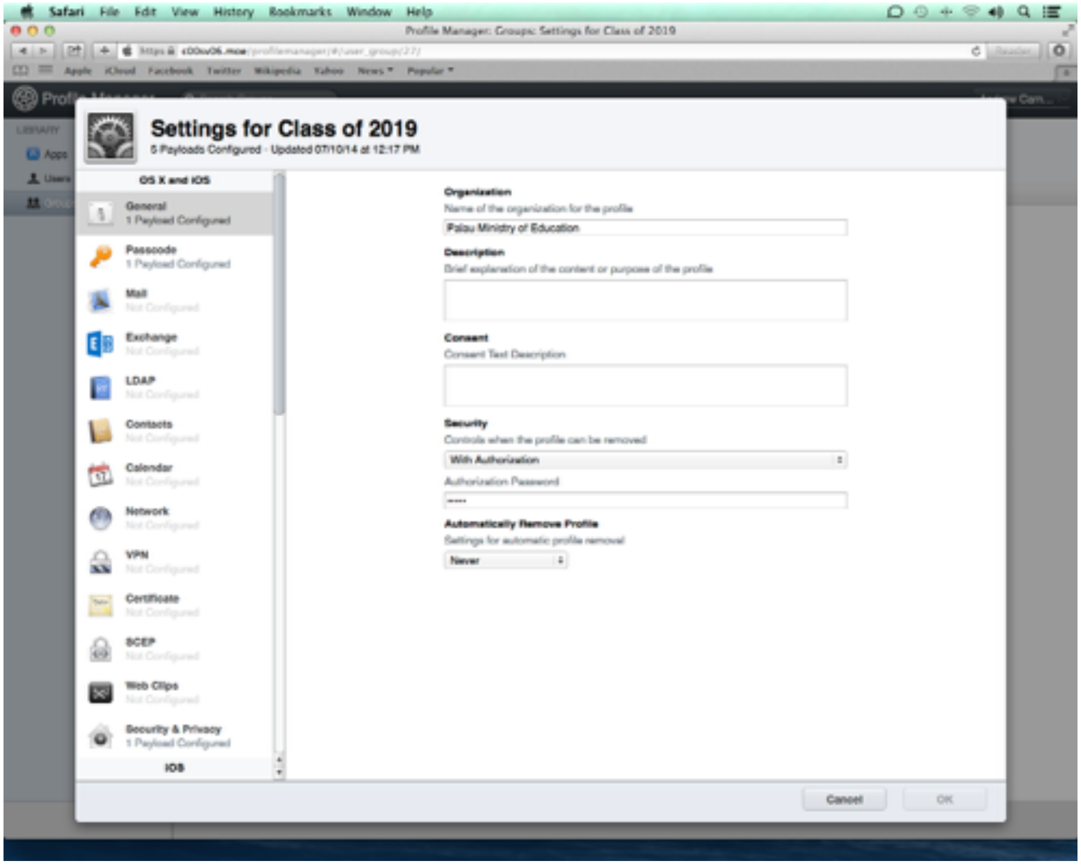
**When Reading This Document**
_____ Refers to an input value. It refers to a number that you will be able to chose in creating the Payload
Settings/choices in Green are recommended to be configured by the consultant team
Settings in Red should not be configured / Settings should be unchecked
**Reminder: You are not required to configure all settings**

**General**

- Organization - Information to be Displayed if User looks up Profile
- Description - Information to be Displayed if User looks up Profile
- Consent - Information to be Displayed if User looks up Profile

- Security - Part of what makes Configuration Profile settings so appropriate for students is that the settings can only be removed if you want them to. There are 3 levels of security
  - Always - Students can remove their profile settings at any time
  - With Authorization - Students can remove the settings with a passcode.However, understand that these passcodes can only be changed by uploading a new configuration profile, so keeping the code secret is very important if this option is chosen
  - Never - Profiles can only be removed by connecting the device back to the computer from which the profile was originally uploaded or by wiping the device and starting from scratch with a Jailbreaking application.

- Automatically Remove Profile - If you are planing on updating profiles on a yearly basis, it may make sense to have profiles remove themselves automatically, making it easier to load new profiles.



Settings for Class of 2019
5 Payloads Configured · Updated 07/10/14 at 12:17 PM

Organization
Name of the organization for the profile
Palau Ministry of Education

Description
Brief explanation of the content or purpose of the profile

Consent
Consent Text Description

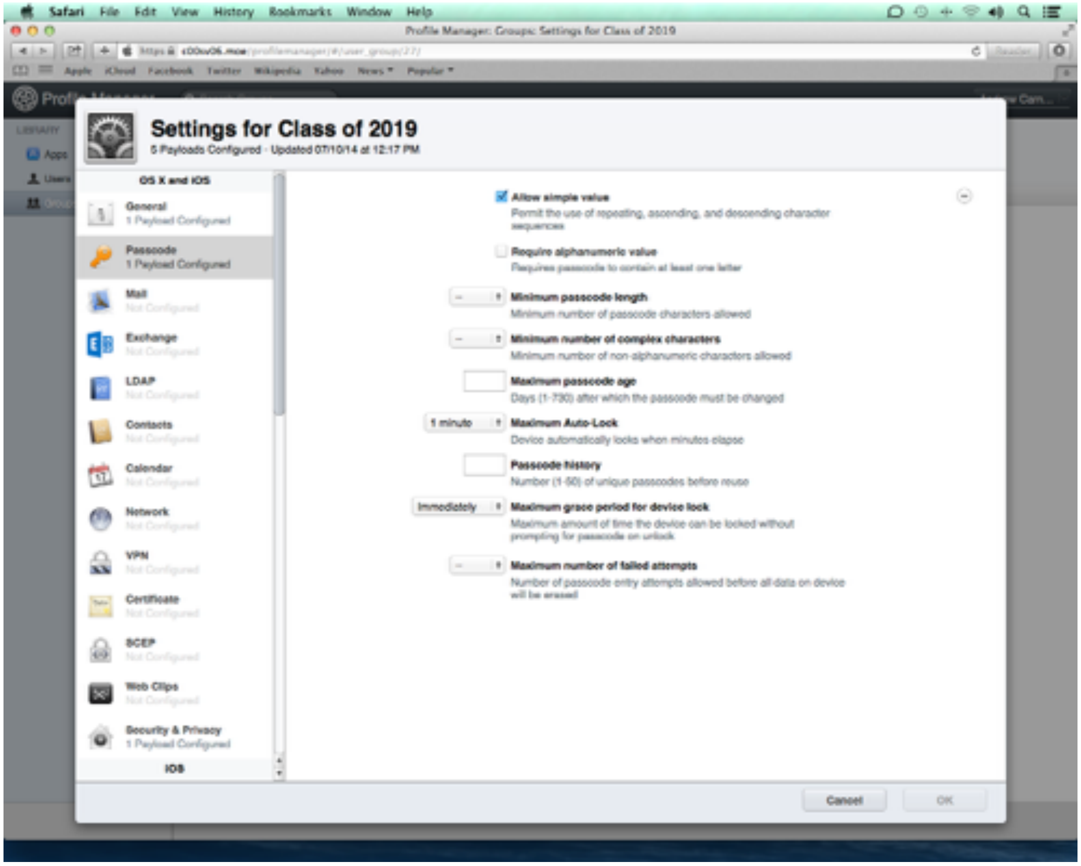
Security
Controls when the profile can be removed
With Authorization

Authorization Password
•••••

Automatically Remove Profile
Settings for automatic profile removal
Never

### Passcode

- Allow Simple Value - Allow the passcode to be extremely easy to remember or guess
  - User could set passcode to 0000, 1234, 2345, etc
- Require alphanumeric value - Prevent user from setting 4 digit code
  - User would be required to put at least one letter in passcode
- Minimum Passcode length
- Minimum number of complex characters
  - User would be required to put at least ___ letters in passcode
- Minimum Passcode age - Require user to change passcode every ____ days
- Maximum Auto-Lock - Require device to lock after ___ minutes of inactivity
- Passcode History - When changing passcode, users can use old passwords after ___ days
- Maximum Grace Period - Device will require password after ____ minutes of device locking
- Maximum number of failed attempts - Device will erase after ___ failed attempts



**Settings for Class of 2019**

5 Payloads Configured · Updated 07/10/14 at 12:17 PM

☑ **Allow simple value**
Permit the use of repeating, ascending, and descending character sequences

□ **Require alphanumeric value**
Requires passcode to contain at least one letter

– **Minimum passcode length**
Minimum number of passcode characters allowed

– **Minimum number of complex characters**
Minimum number of non-alphanumeric characters allowed

**Maximum passcode age**
Days (1-730) after which the passcode must be changed

1 minute **Maximum Auto-Lock**
Device automatically locks when minutes elapse

**Passcode history**
Number (1-50) of unique passcodes before reuse

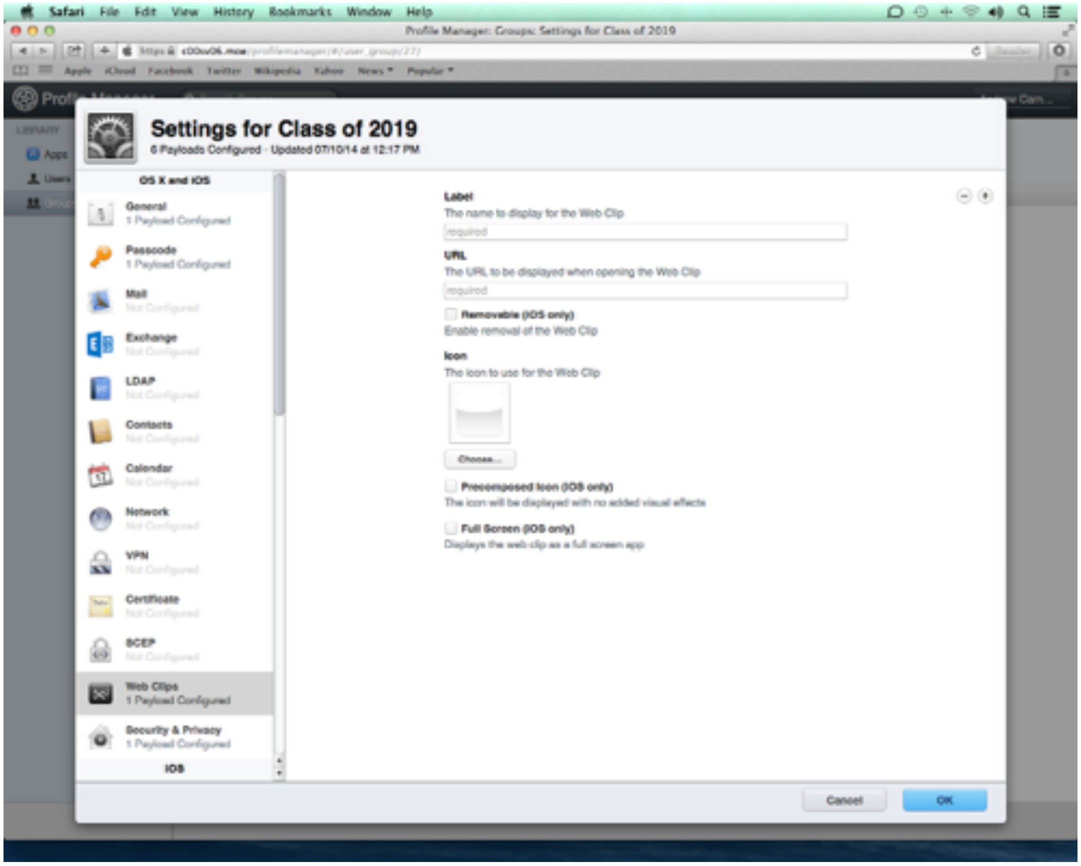
Immediately **Maximum grace period for device lock**
Maximum amount of time the device can be locked without prompting for passcode on unlock

– **Maximum number of failed attempts**
Number of passcode entry attempts allowed before all data on device will be erased

### Web Clips

A web clip looks like an app on the home screen, but is actually a link. When configured, a button will appear on the home screen, and when clicked will bring the user to the link you directed. These can be very helpful if there are links that you would like students to to go often

- Label - The name displayed for the clip
- URL - Where the web clip will take the user (a website link)
- Removable - Whether or not the user can remove the web clip
- Icon - The small picture that will be seen on the home screen (this should be a very simple image)
- Precomposed Icon
- Full Screen - Makes web clip go full screen for the user



Settings for Class of 2019

6 Payloads Configured · Updated 07/10/14 at 12:17 PM

Label

The name to display for the Web Clip

required

URL

The URL to be displayed when opening the Web Clip

required

□ Removable (iOS only)

Enable removal of the Web Clip

Icon

The icon to use for the Web Clip

□ Precomposed Icon (iOS only)

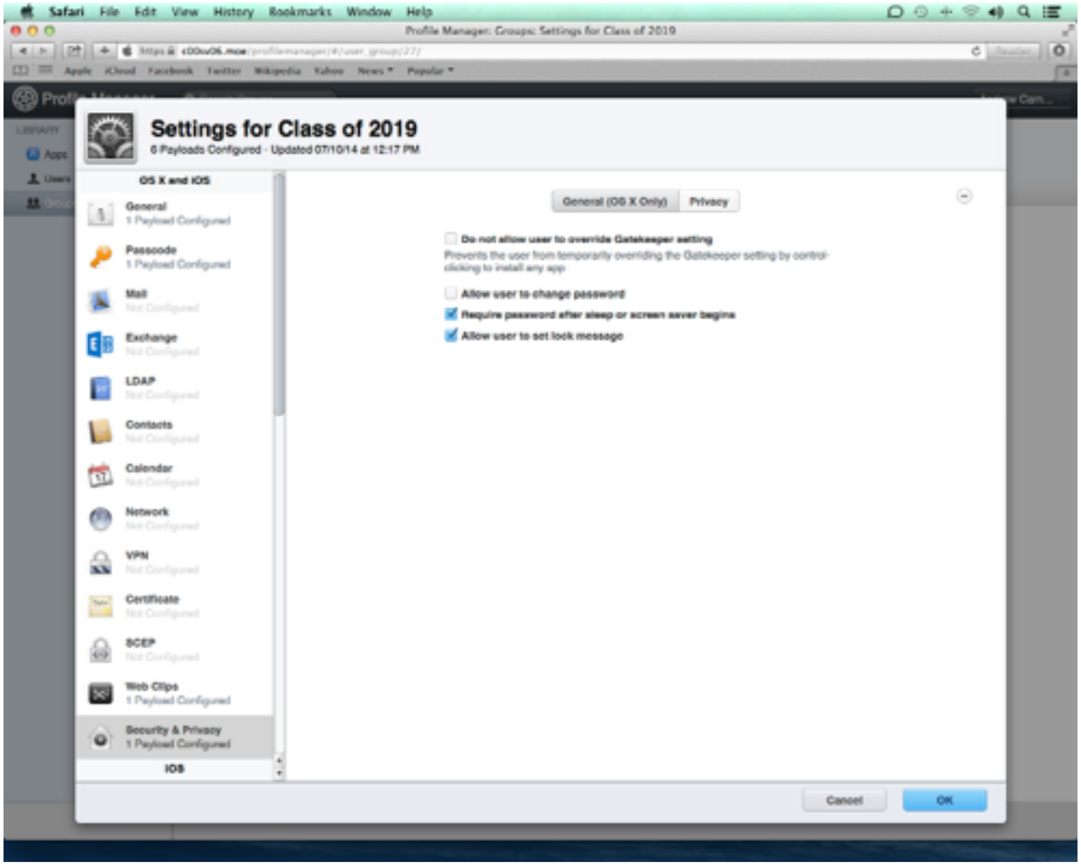
The icon will be displayed with no added visual effects

□ Full Screen (iOS only)

Displays the web clip as a full screen app

### Security & Privacy

- Do Not Allow User to override Gatekeeper Setting
  - Prevents users from installing applications that have been deemed not appropriate
- Allow User to Change Password
- Require password after sleep or screen saver begins
- Allow User to set lock message



Settings for Class of 2019

6 Payloads Configured · Updated 07/10/14 at 12:17 PM

□ Do not allow user to override Gatekeeper setting

Prevents the user from temporarily overriding the Gatekeeper setting by control-clicking to install any app

□ Allow user to change password

☑ Require password after sleep or screen saver begins

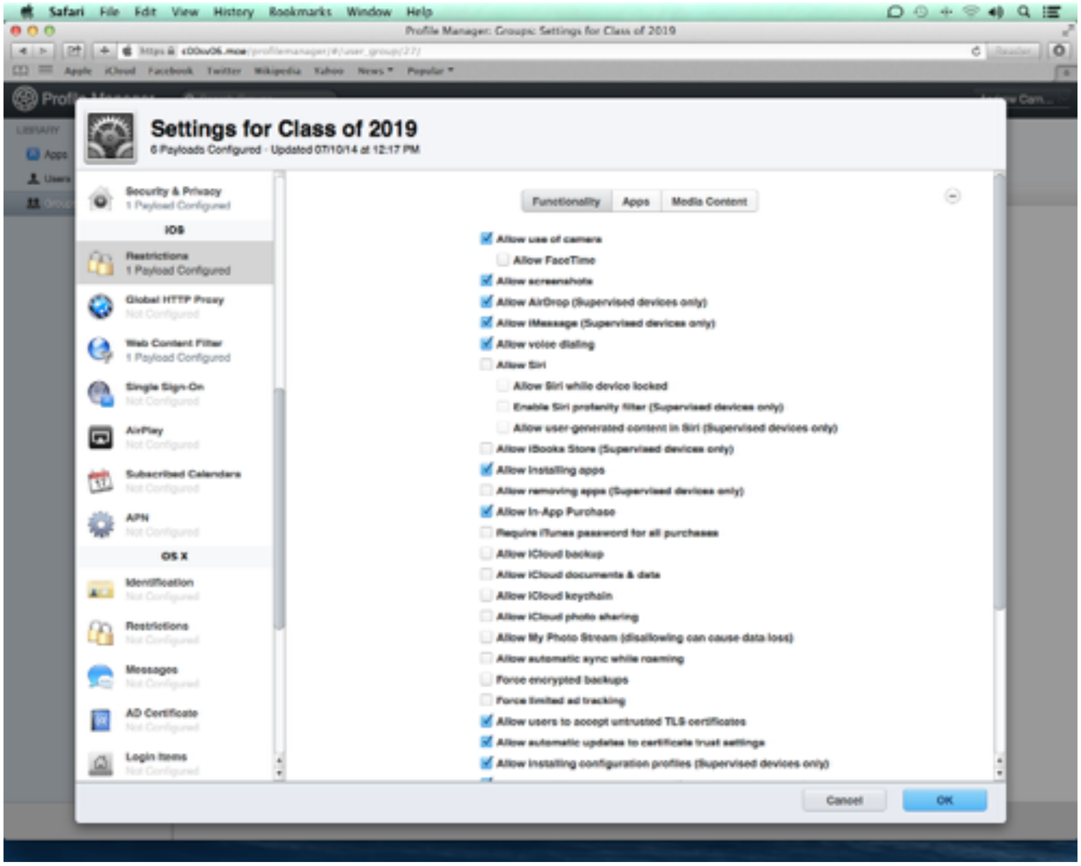
☑ Allow user to set lock message

### Restrictions Part 1 - Functionality

- Allow use of Camera
    - Allow FaceTime
- Allow Screenshots - Allow users to take pictures of their current screen
- Allow Airdrop - Allow users to transfer files to one another using WiFi
- Allow iMessage - allow users to communicate with each other using their devices
- Allow Voice Dialing
- Allow Siri
    - Allow Siri while device locked
    - Enable Siri profanity filter
    - Allow user-generated content in Siri
- Allow iBooks Store
- Allow installing apps
- Allow removing apps
- Allow In-App Purchase
- Require iTunes password for all purchases
- Allow iCloud Backup - iCloud is Apple's Cloud based data storage program
- Allow iCloud documents & data
- Allow My Photo Stream - Sync's photos in the cloud to other devices
- Allow automatic sync while roaming
- Force encrypted backups
- Force limited ad tracking
- Allow users to accept untrusted TLS certificates
- Allow automatic updates to certificate trust settings
- Allow installing configuration profiles
- Allow modifying account settings
- Allow modifying Find My Friends settings
- Allow documents from managed apps in unmanaged apps
- Allow documents from unmanaged apps in managed apps
- Allow Touch ID to unlock device - Allow fingerprint as password in newer apple devices
- Allow Passbook notifications while locked
- Show Control Center in lock screen
- Show Notification Center in lock screen
- Show Today view in lock screen

This is one of the more important payloads, as it relates specifically to what students will or will not be using their devices for. It will be important to have discussions relating to some of these choices.

## Restrictions Part 1 - Functionality



**Settings for Class of 2019**

6 Payloads Configured · Updated 07/10/14 at 12:17 PM

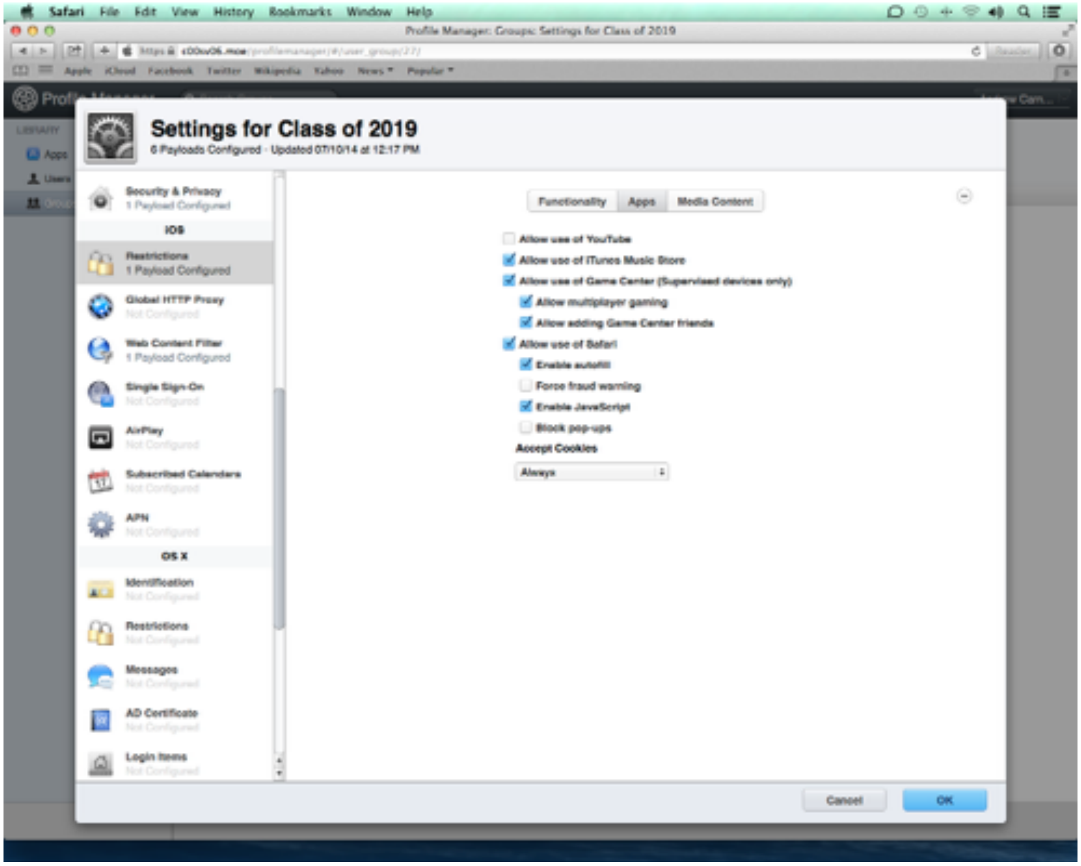
- ☑ Allow use of camera
  - ☐ Allow FaceTime
- ☑ Allow screenshots
- ☑ Allow AirDrop (Supervised devices only)
- ☑ Allow iMessage (Supervised devices only)
- ☑ Allow voice dialing
- ☐ Allow Siri
  - ☐ Allow Siri while device locked
  - ☐ Enable Siri profanity filter (Supervised devices only)
  - ☐ Allow user-generated content in Siri (Supervised devices only)
- ☐ Allow iBooks Store (Supervised devices only)
- ☑ Allow installing apps
- ☐ Allow removing apps (Supervised devices only)
- ☑ Allow In-App Purchase
- ☐ Require iTunes password for all purchases
- ☐ Allow iCloud backup
- ☐ Allow iCloud documents & data
- ☐ Allow iCloud keychain
- ☐ Allow iCloud photo sharing
- ☐ Allow My Photo Stream (disallowing can cause data loss)
- ☐ Allow automatic sync while roaming
- ☐ Force encrypted backups
- ☐ Force limited ad tracking
- ☑ Allow users to accept untrusted TLS certificates
- ☑ Allow automatic updates to certificate trust settings
- ☑ Allow installing configuration profiles (Supervised devices only)

**Note: The pictures in this document and the setting selections shown in them relate to the settings in the default profile created, which were created at a joint meeting between the consultants, MOE IT and MOE DSM. For this profile, you can go to the Profile Manager and download the profile marked “Class of 2019”**

**The suggested settings marked in Green and Red are based solely off of the opinion of the consultant team.**

### Restrictions Part 2 - Apps

- Allow use of Youtube
- Allow use of iTunes Music Store
- Allow Use of Game Center
  - Allow multiplayer gaming
  - Allow adding Game Center Friends
- Allow use of Safari
  - Enable autofil
  - Force fraud warning
  - Enable Javascript
  - Block pop-ups
- Accept Cookies - Allow websites to access information on the device relating to the last time the user visited that specific site, also known as Cookies.



Settings for Class of 2019

6 Payloads Configured · Updated 07/10/14 at 12:17 PM

□ Allow use of YouTube
☑ Allow use of iTunes Music Store
☑ Allow use of Game Center (Supervised devices only)
☑ Allow multiplayer gaming
☑ Allow adding Game Center friends
☑ Allow use of Safari
☑ Enable autofill
□ Force fraud warning
☑ Enable JavaScript
□ Block pop-ups

Accept Cookies

Always

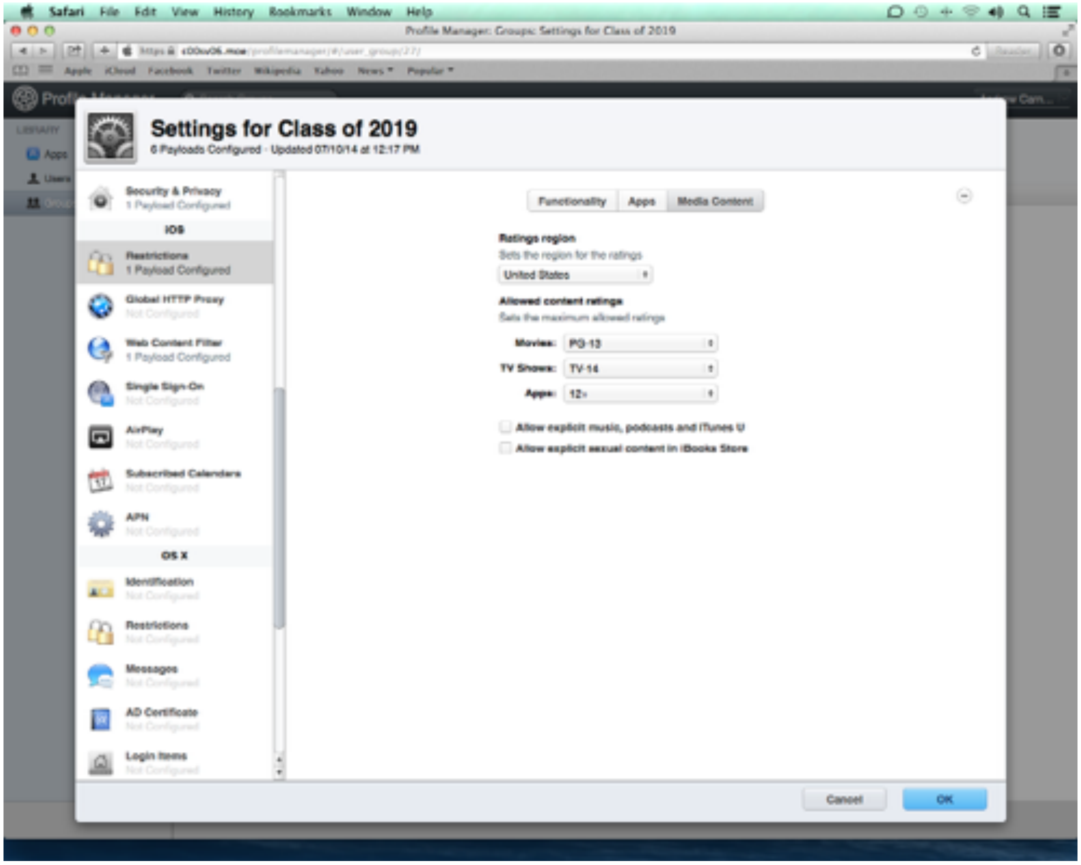
### Restrictions Part 3 -Media Content

- Ratings Region -> Palau or United States

Allowed Content Ratings

- Movies -> PG-13
- TV Shows -> TV-14
- Apps -> 12+

- Allow explicit music, podcasts or iTunes U
- Allow explicit sexual content in iBooks Store



Settings for Class of 2019

6 Payloads Configured · Updated 07/10/14 at 12:17 PM

Ratings region

Sets the region for the ratings

United States

Allowed content ratings

Sets the maximum allowed ratings

Movies: PG-13

TV Shows: TV-14

Apps: 12+

□ Allow explicit music, podcasts and iTunes U

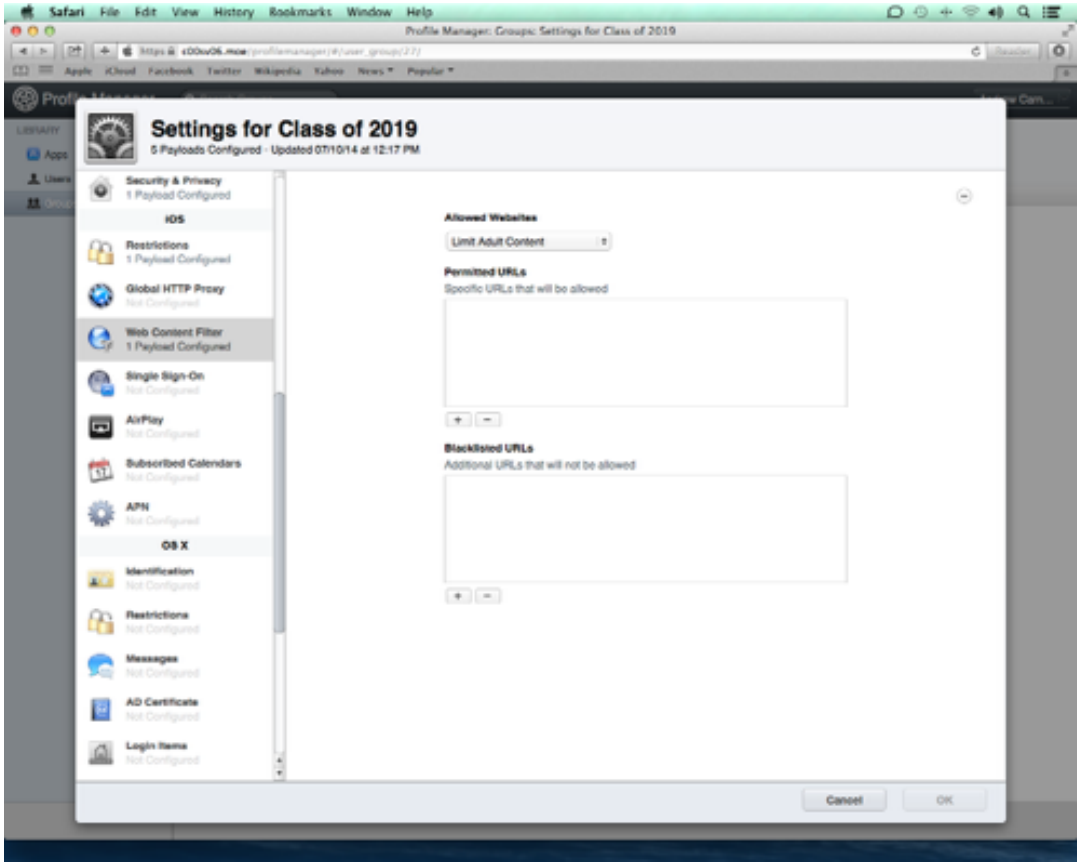
□ Allow explicit sexual content in iBooks Store

### Web Content Filter

The Web Content Filter gives you, the administrator, the ability to restrict what sites a URL can access. There are two ways to restrict content, a Whitelist approach and a Blacklist approach

Permitted URLs
A Whitelist approach blocks all websites except those specified on the list. This is an appropriate option if you have a fully dedicated IT staff who could constantly update this list, but not appropriate for the Ministry of Education

Blacklisted URLs
A Blacklist approach allows you to restrict specific websites like Facebook or twitter, while still giving students the freedom to browse other sites that you may be unfamiliar with. It is the strong recommendation of the consultant team that social media sites be blocked.



Profile Manager: Groups: Settings for Class of 2019

Settings for Class of 2019
5 Payloads Configured · Updated 07/10/14 at 12:17 PM

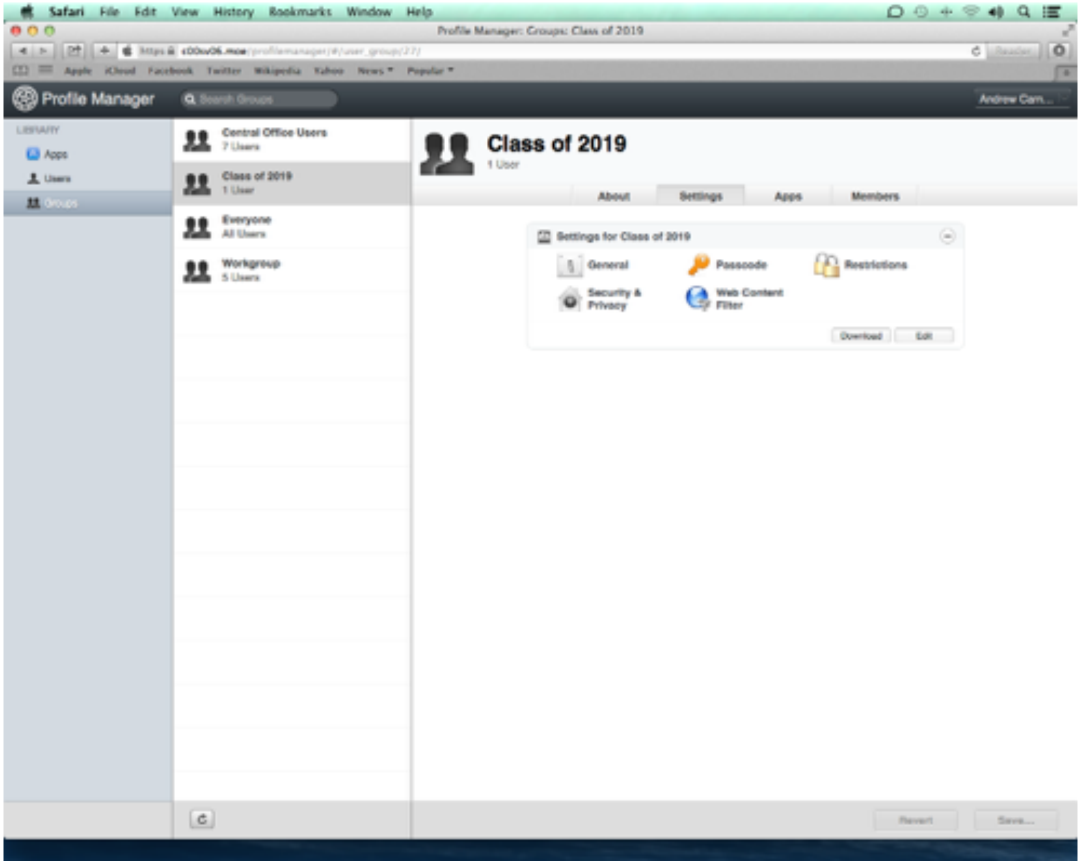
Allowed Websites
Limit Adult Content

Permitted URLs
Specific URLs that will be allowed

Blacklisted URLs
Additional URLs that will not be allowed

Make sure when you have finished setting payloads, you click Save.

Congratulations! You have now created a Configuration Profile.



Once clicking save, you will see next to the “Edit” button there is a “Download” button. In addition to downloading the Configuration Profile through Device Manager (Explained in the Configuration Profile Implementation Guide). You may download this profile by clicking this download button. Remember when clicking this button not to install the Configuration Profile on your own machine. When you download the profile, System Preferences will open up and prompt you. Click “Cancel” at this time. More information on this is available in the Configuration Profile Implementation Guide for Administrators.

If you download the Configuration Profile from this site, You may now use Apple Configurator to install the profile onto multiple devices. In addition, the Configuration Profile will now be available for download on Device Manager.

# Appendix F

# Palau Ministry of Education

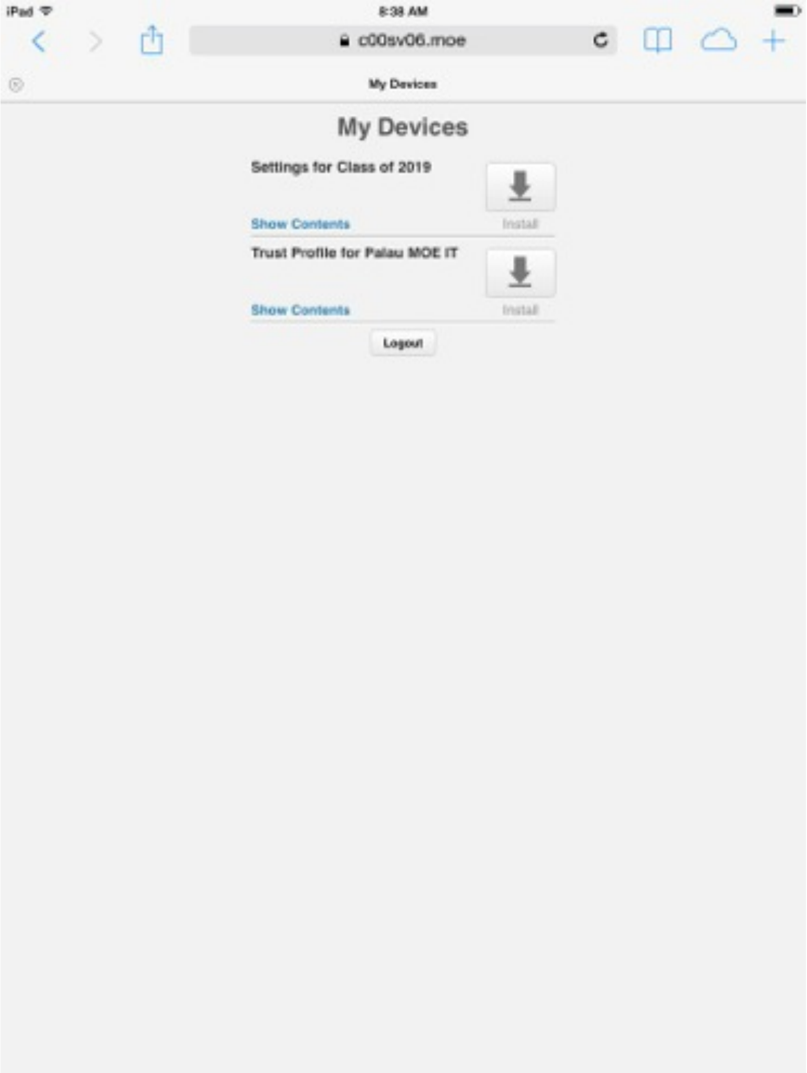
## Configuration Profile Implementation Guide

MOE Information Technology - Last Updated August 1, 2014

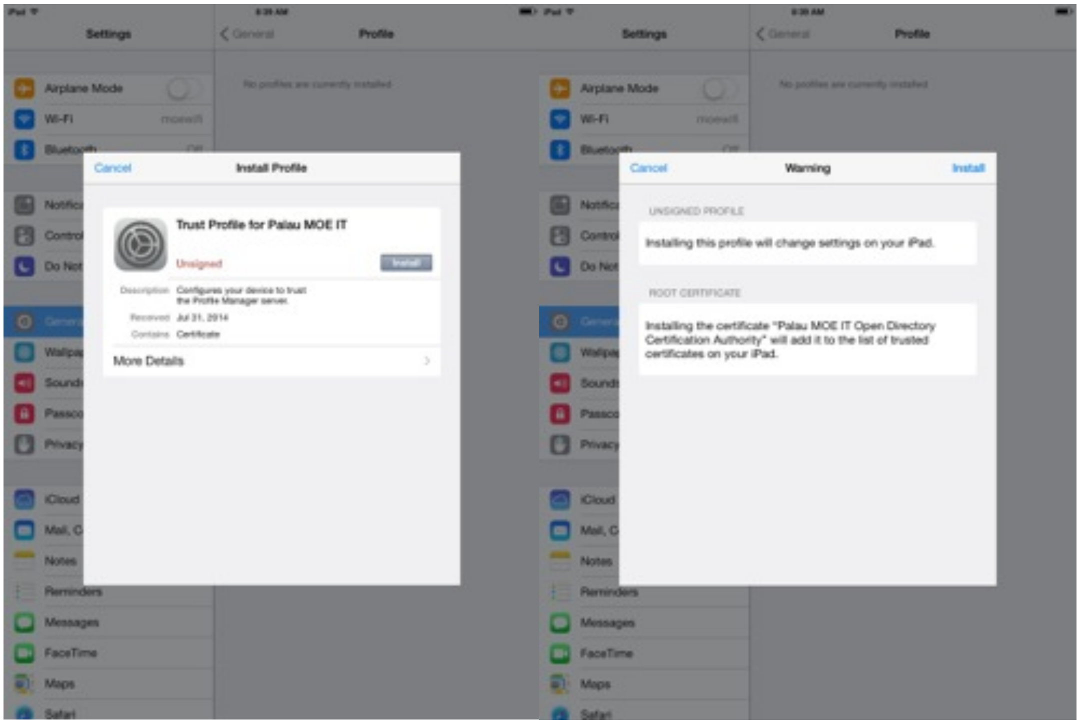
Hello! Welcome to the Configuration Profile Implementation Guide for Users!

We will start by opening up your iPad and going to c00sv06.moe/mydevices (Shown Above)

We may have to log in 2 times, once to log into the MOE system and once to log into the device manager itself. Your username and password are the same as what you use to login to the wireless network



Once we login, we will see multiple download buttons. Start by downloading the trust profile. When you click the download button next to “Trust Profile For MOE IT”, you will be prompted to install it on your device.



Install Profile

Trust Profile for Palau MOE IT

Unsigned

Description Configures your device to trust the Profile Manager server.

Received Jul 31, 2014

Contains Certificate

Warning

UNSIGNED PROFILE

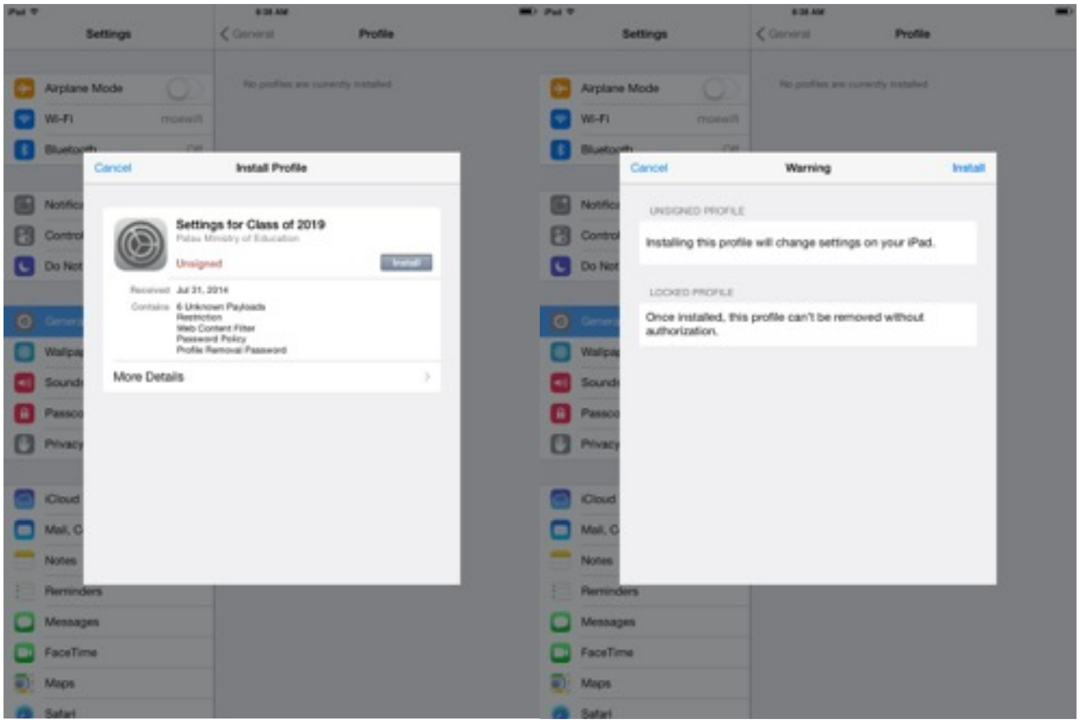
Installing this profile will change settings on your iPad.

ROOT CERTIFICATE

Installing the certificate "Palau MOE IT Open Directory Certification Authority" will add it to the list of trusted certificates on your iPad.

Once you have done so, you will be redirected back to the device manager.

You will then click the configuration profile group which best reflects who you are. In most cases, there will only be one group. You will again be prompted by your device to install the profile, and once you have done so your installation will be complete.



Install Profile

Settings for Class of 2019
Palau Ministry of Education
Unsigned

Received Jul 31, 2014
Contains 6 Unknown Payloads
Restriction
Web Content Filter
Password Policy
Profile Removal Password

Warning

UNSIGNED PROFILE
Installing this profile will change settings on your iPad.

LOCKED PROFILE
Once installed, this profile can't be removed without authorization.

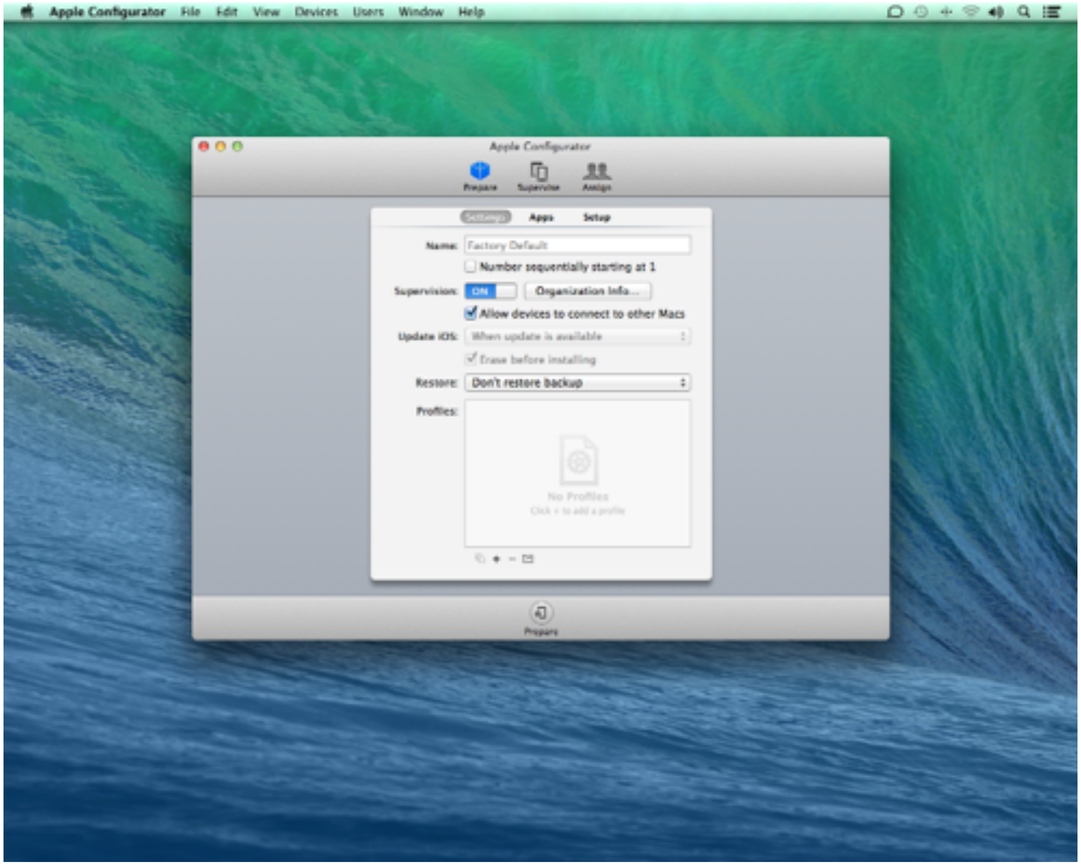
Congratulations! You have now installed a configuration profile on your device!

# Appendix G

# Palau Ministry of Education

## Administrative Configuration Profile Implementation Guide

MOE Information Technology - Last Updated August 1, 2014



Name: Factory Default

□ Number sequentially starting at 1

Supervision: ON

☑ Allow devices to connect to other Macs

Update iOS: When update is available

☑ Erase before installing

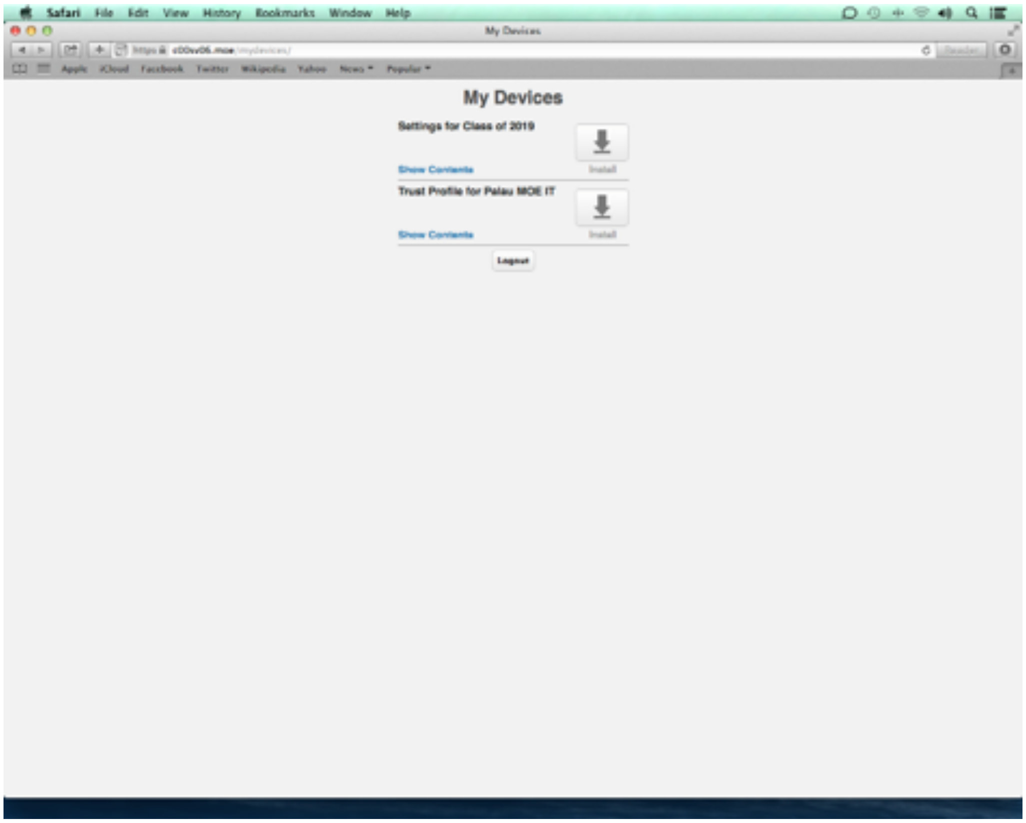
Restore: Don't restore backup

Profiles:

**Hello! Welcome to the Configuration Profile Implementation Guide for Administrators!**

To begin, we must make sure we are using a Mac OSX machine with Apple Configurator Installed. BEFORE YOU OPEN APPLE CONFIGURATOR, UNPLUG ALL DEVICES FROM THE MACHINE WHICH DO NOT NEED TO BE CONFIGURED. In order for apple configurator to work properly, you must have an internet connection and the latest version of iOS downloaded onto your machine. You can download the latest iOS software update through iTunes. Please note that downloading an iOS software update can take days or weeks. If you have already received a Configuration Profile via email or have it on your hard drive, you may skip to page 4.

We will start by opening up your Computer and going to c00sv06.moe/mydevices
We may have to log in 2 times, once to log into the MOE system and once to log into the device manager itself.


Safari File Edit View History Bookmarks Window Help
My Devices
https:// c00sv06.moe/mydevices/
Reader
Apple iCloud Facebook Twitter Wikipedia Yahoo News Popular
Install
Install
Logout

My Devices

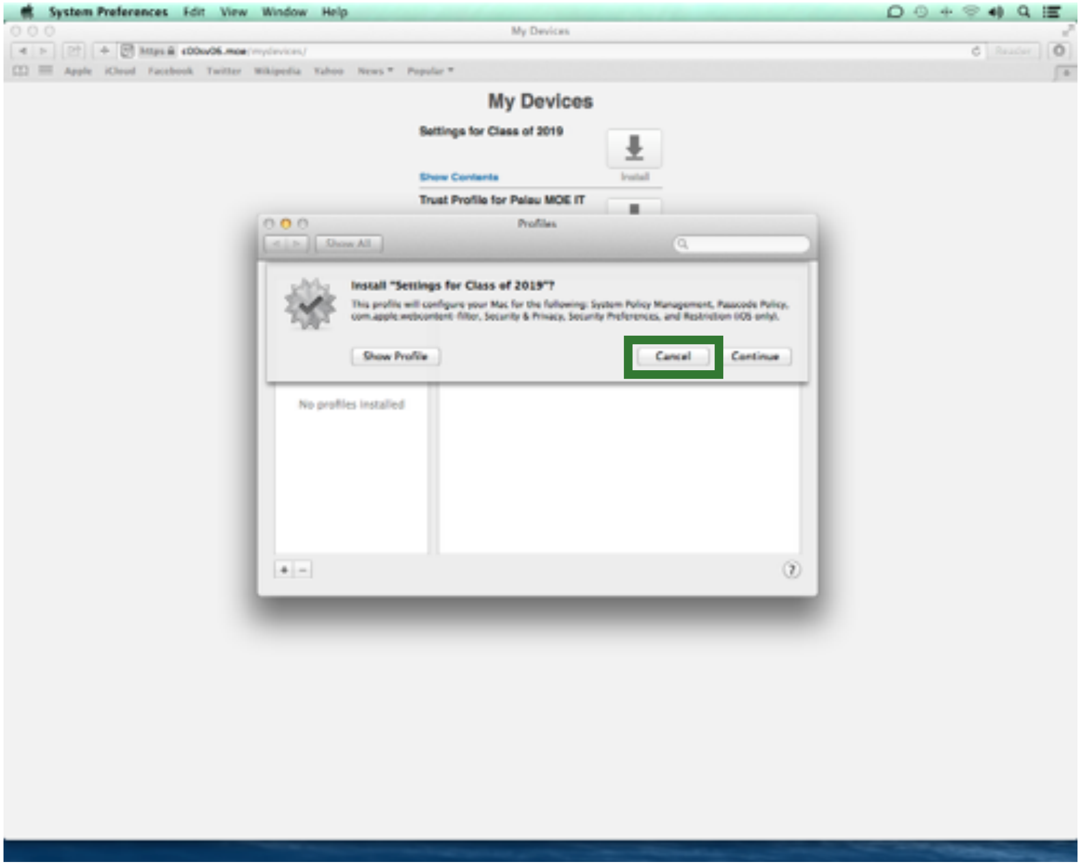
Settings for Class of 2019

Show Contents

Trust Profile for Palau MOE IT

Show Contents

Once we login, we will see multiple download buttons. Start by downloading the trust profile. When you click the download button next to “Trust Profile For MOE IT”, you will be prompted to install it on your device. DO NOT INSTALL THE PROFILE ONTO YOUR DEVICE. Click cancel when prompted.  You will then click the configuration profile group which best reflects who you are. In most cases, there will only be one group. Again, click cancel when prompted to install the profile on your device.



My Devices

Settings for Class of 2019

Show Contents

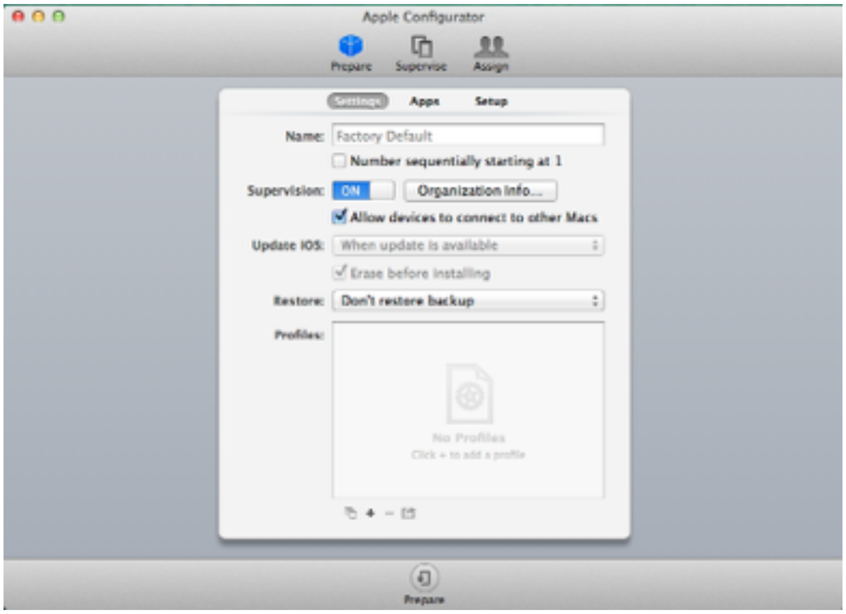
Trust Profile for Palau MOE IT

Install "Settings for Class of 2019"?

This profile will configure your Mac for the following: System Policy Management, Passcode Policy, com.apple.webcontent-filter, Security & Privacy, Security Preferences, and Restriction (iOS only).

No profiles installed

We will now open Apple Configurator. If you do not have an internet connection, the application will not successfully open. Click “Prepare” and turn supervision to the on position. Once that is done, name your iPad and put your organization in “Organization Info”



Name: Factory Default

□ Number sequentially starting at 1

Supervision: ON

☑ Allow devices to connect to other Macs

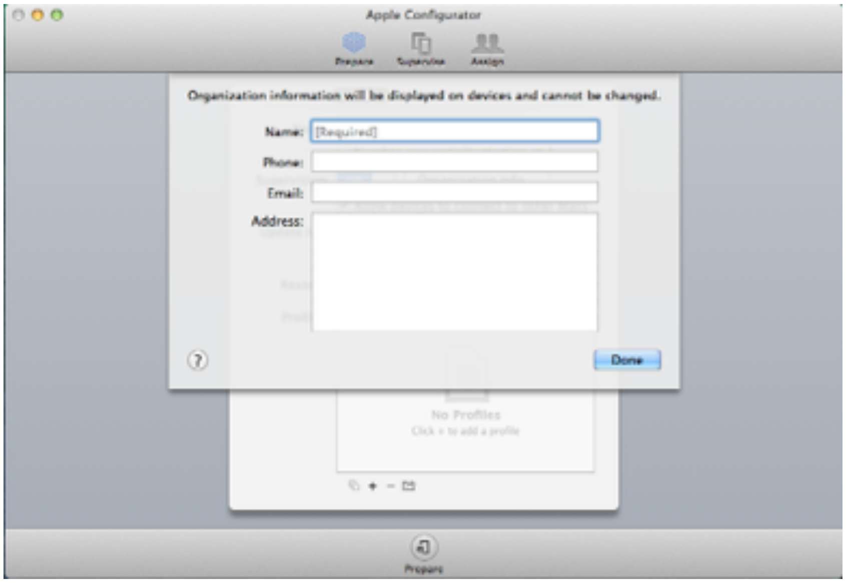
Update iOS: When update is available

☑ Erase before installing

Restore: Don't restore backup

Profiles: No Profiles

Click + to add a profile



Organization information will be displayed on devices and cannot be changed.

Name: [Required]

Phone:

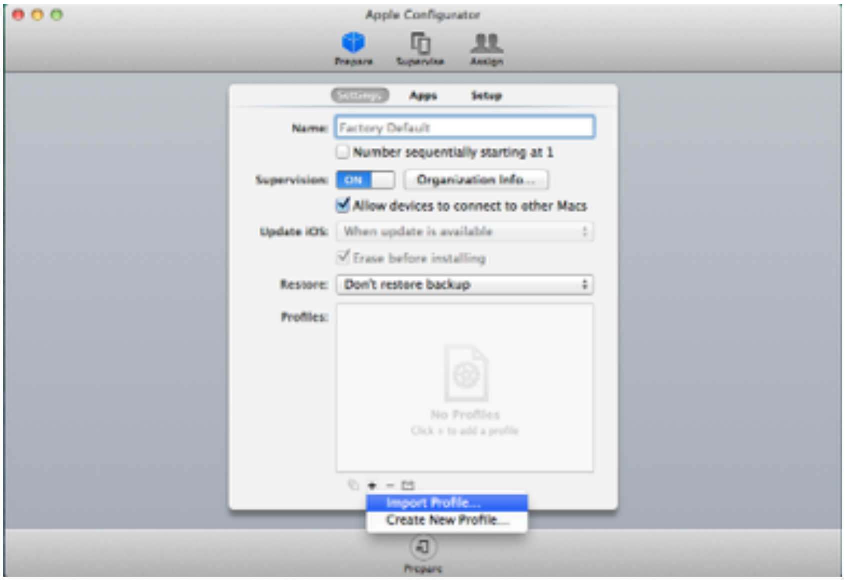
Email:

Address:

No Profiles

Click + to add a profile

Click the + Button at the bottom of the screen. You will then be prompted to select your Configuration profile. If you have just downloaded it, the profile will be in your downloads folder. If not, navigate to where you have stored it. Remember to install both the configuration profile and trust profile.



Name: Factory Default

☐ Number sequentially starting at 1

Supervision: ON  Organization Info...

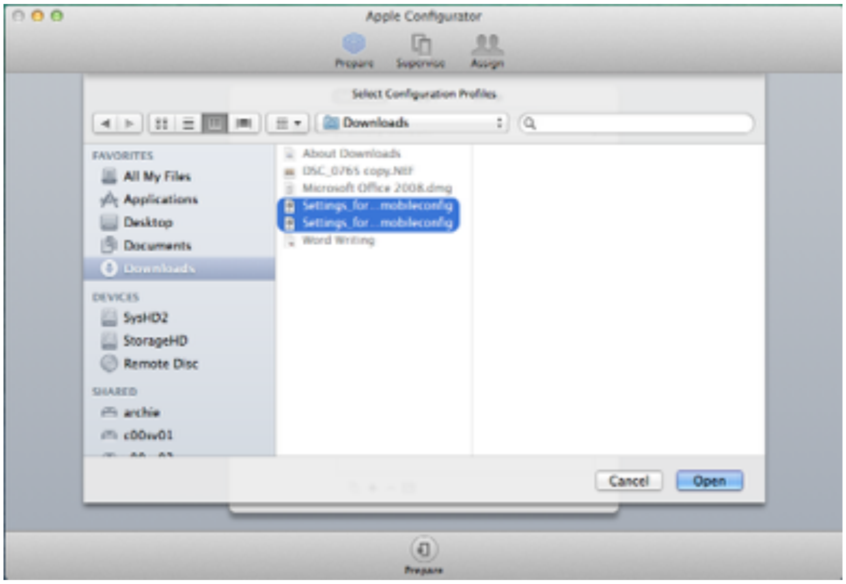
☑ Allow devices to connect to other Macs

Update iOS: When update is available

☑ Erase before installing

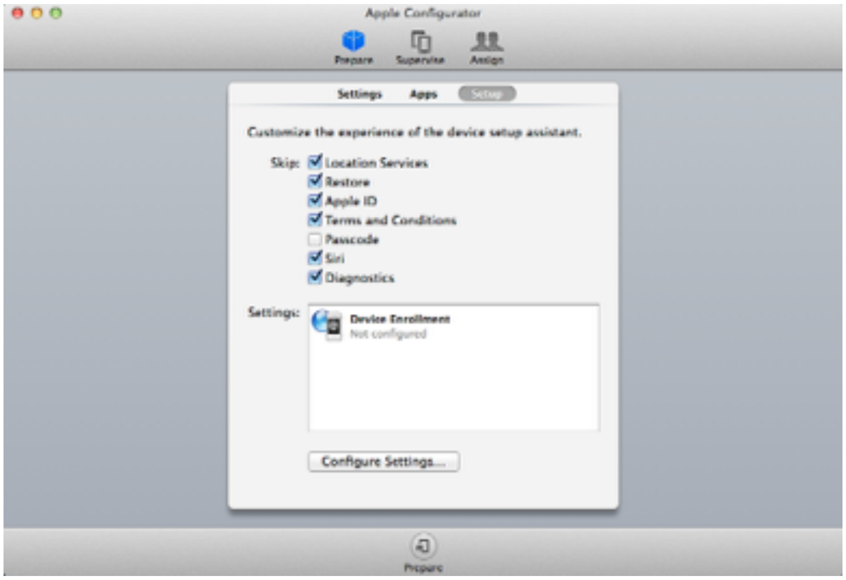
Restore: Don't restore backup

Profiles: No Profiles  Click + to add a profile



About Downloads
DSC_0765 copy.NEF
Microsoft Office 2008.dmg
Settings_for...mobileconfig
Settings_for...mobileconfig
Word Writing

Click “Setup” on the 2nd upper bar. You may skip any installation settings for the user in this page. Then click Prepare at the bottom of the screen.

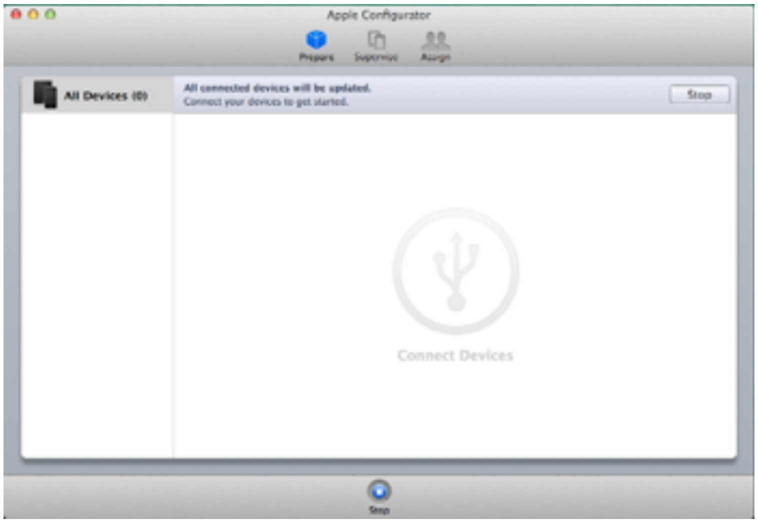


Customize the experience of the device setup assistant.

Skip: ☑ Location Services
☑ Restore
☑ Apple ID
☑ Terms and Conditions
□ Passcode
☑ Siri
☑ Diagnostics

Settings: Device Enrollment
Not configured

Once you click “Prepare” the computer will install the configuration profile on any device which is connected to the computer. You may install these profiles on as many devices as you would like. Remember that if a device does not have the most current iOS, apple configurator will need to update the software before it installs profiles. This makes it very important to have the latest software update for iOS already installed on the machine.



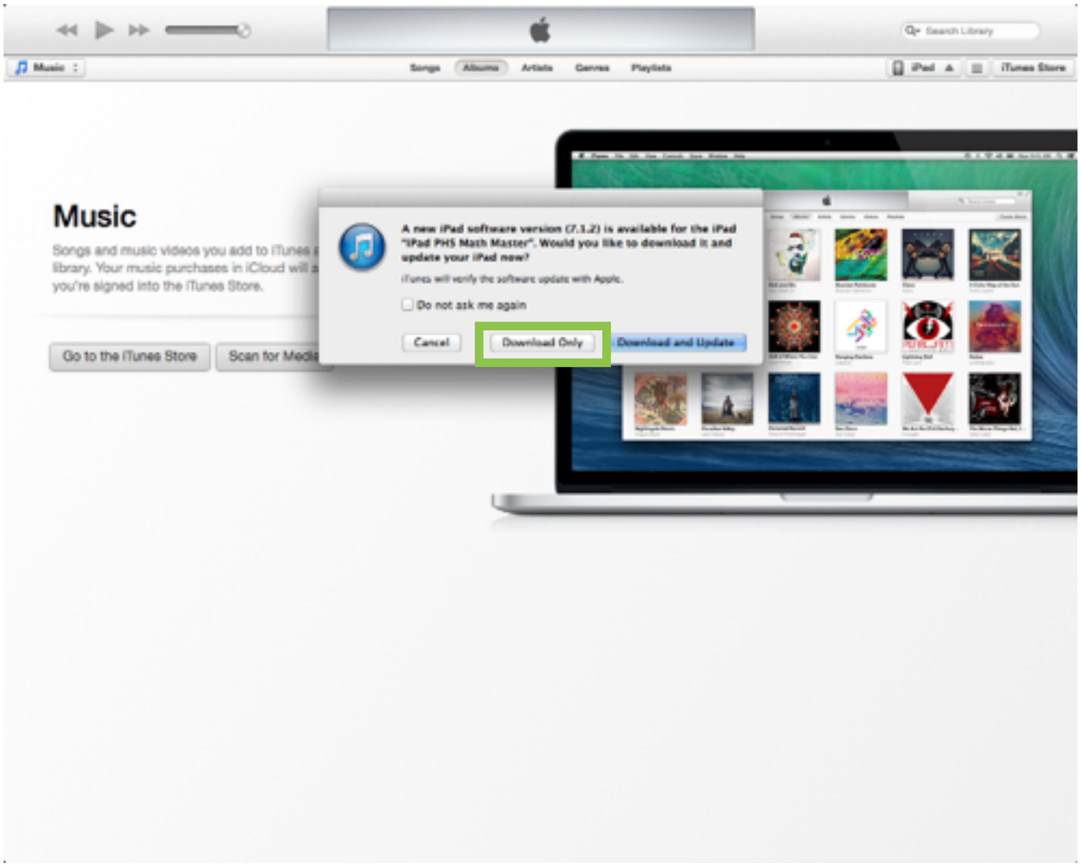
All connected devices will be updated.
Connect your devices to get started.

## iOS Software Update

If Apple Configurator attempts to download a new software update, it will be a long process taking days or even weeks. As Apple Configurator was not built to download a file for that long, it will be more appropriate to download the file with iTunes. If the file is stored within iTunes, Apple Configurator will still be able to find it. To download this file with iTunes, close Apple Configurator and unplug all devices. Then plug one device into iTunes that does not have updates software and open iTunes.

iTunes will prompt you to download and install the update. Click “Download Only” and wait for the download to complete. iOS update files are typically sized at 1 Gigabyte.

Once the download has completed, you will be ready to reopen Apple Configurator and continue.



Music

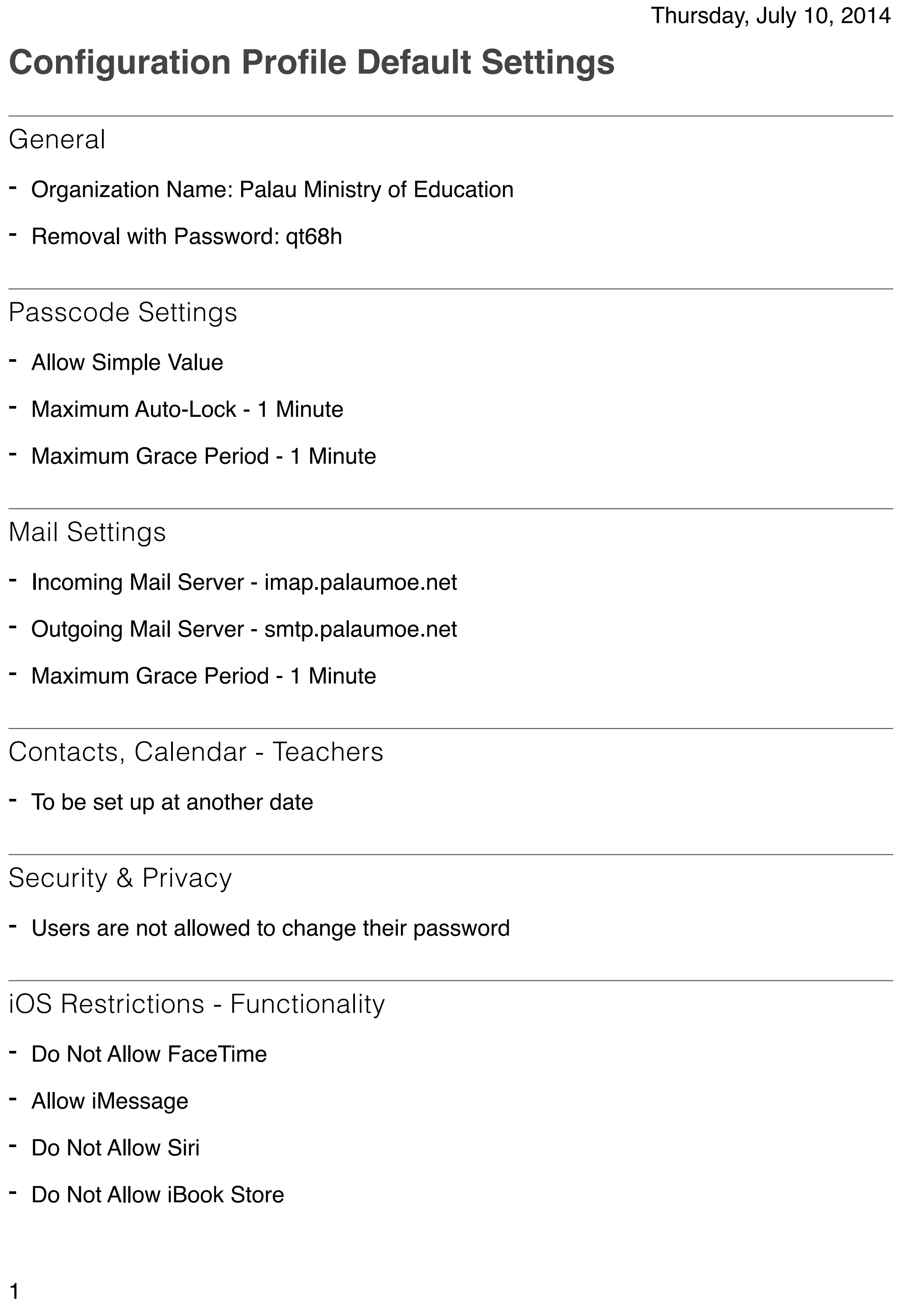
Songs and music videos you add to iTunes
library. Your music purchases in iCloud will a
you're signed into the iTunes Store.

A new iPad software version (7.1.2) is available for the iPad "iPad PHS Math Master". Would you like to download it and update your iPad now?

iTunes will verify the software update with Apple.

□ Do not ask me again

# Appendix H



Thursday, July 10, 2014

## Configuration Profile Default Settings

### General

- Organization Name: Palau Ministry of Education
- Removal with Password: qt68h

### Passcode Settings

- Allow Simple Value
- Maximum Auto-Lock - 1 Minute
- Maximum Grace Period - 1 Minute

### Mail Settings

- Incoming Mail Server - imap.palaumoe.net
- Outgoing Mail Server - smtp.palaumoe.net
- Maximum Grace Period - 1 Minute

### Contacts, Calendar - Teachers

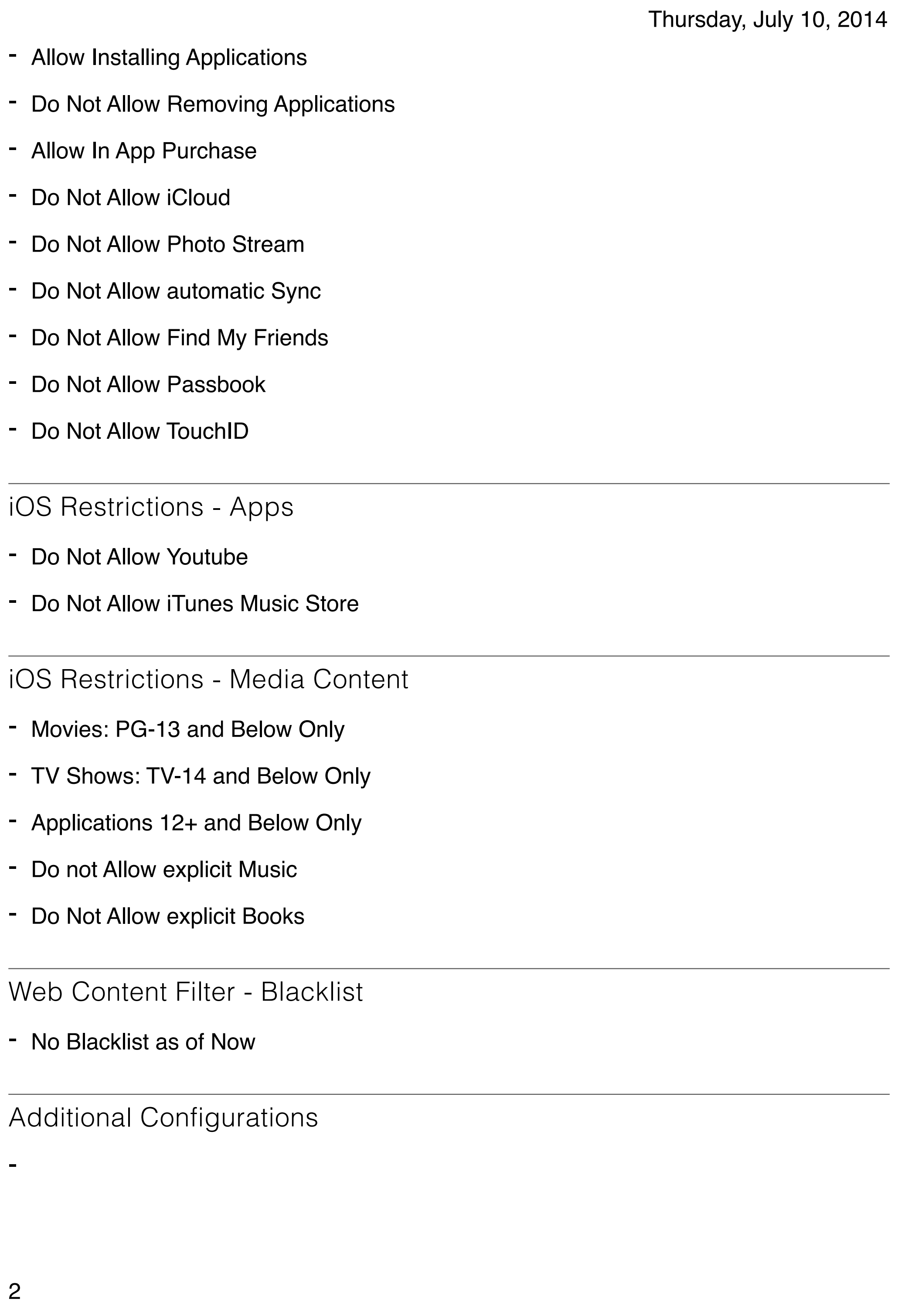
- To be set up at another date

### Security & Privacy

- Users are not allowed to change their password

### iOS Restrictions - Functionality

- Do Not Allow FaceTime
- Allow iMessage
- Do Not Allow Siri
- Do Not Allow iBook Store



Thursday, July 10, 2014

- Allow Installing Applications
- Do Not Allow Removing Applications
- Allow In App Purchase
- Do Not Allow iCloud
- Do Not Allow Photo Stream
- Do Not Allow automatic Sync
- Do Not Allow Find My Friends
- Do Not Allow Passbook
- Do Not Allow TouchID

## iOS Restrictions - Apps

- Do Not Allow Youtube
- Do Not Allow iTunes Music Store

## iOS Restrictions - Media Content

- Movies: PG-13 and Below Only
- TV Shows: TV-14 and Below Only
- Applications 12+ and Below Only
- Do not Allow explicit Music
- Do Not Allow explicit Books

## Web Content Filter - Blacklist

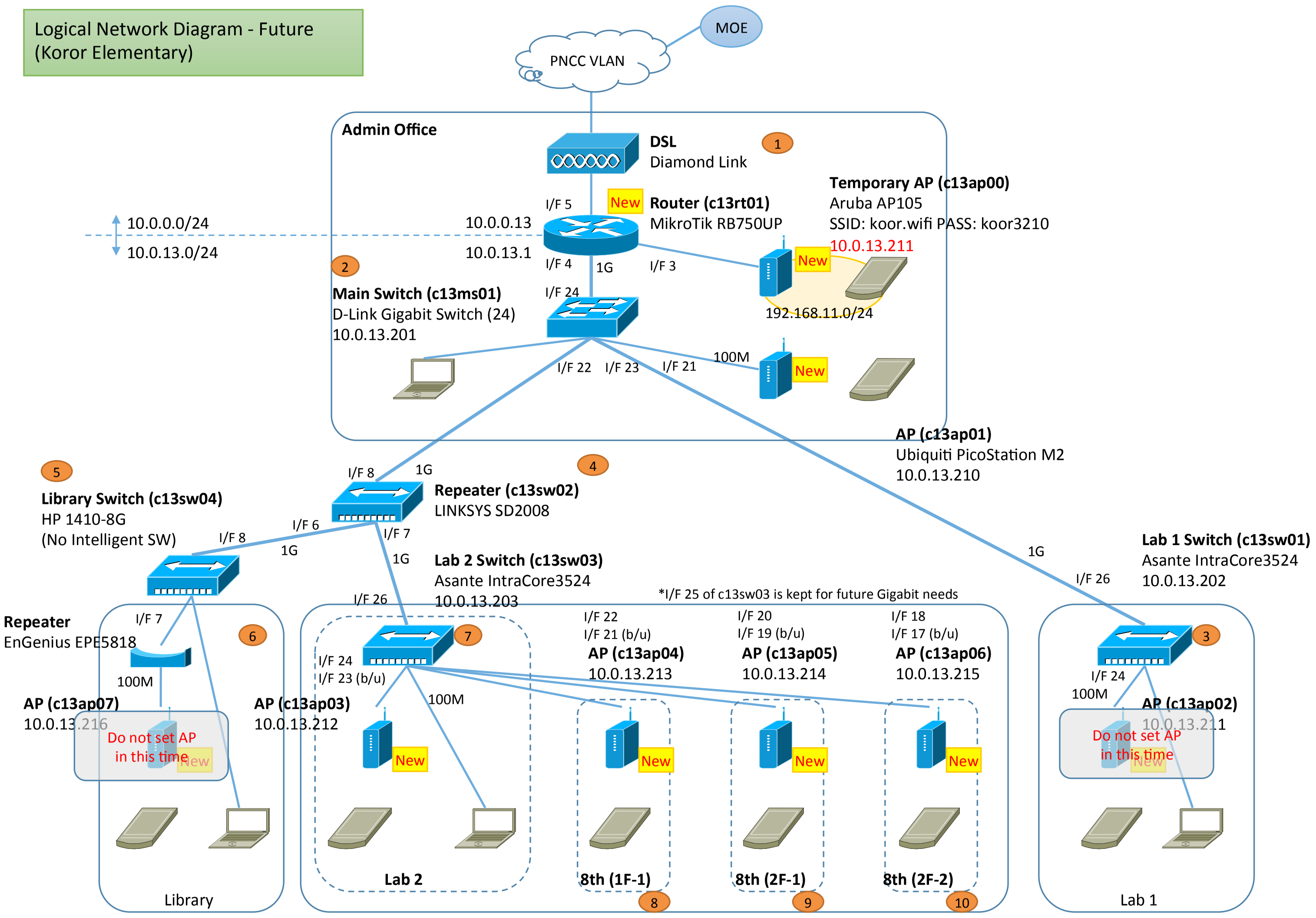
- No Blacklist as of Now

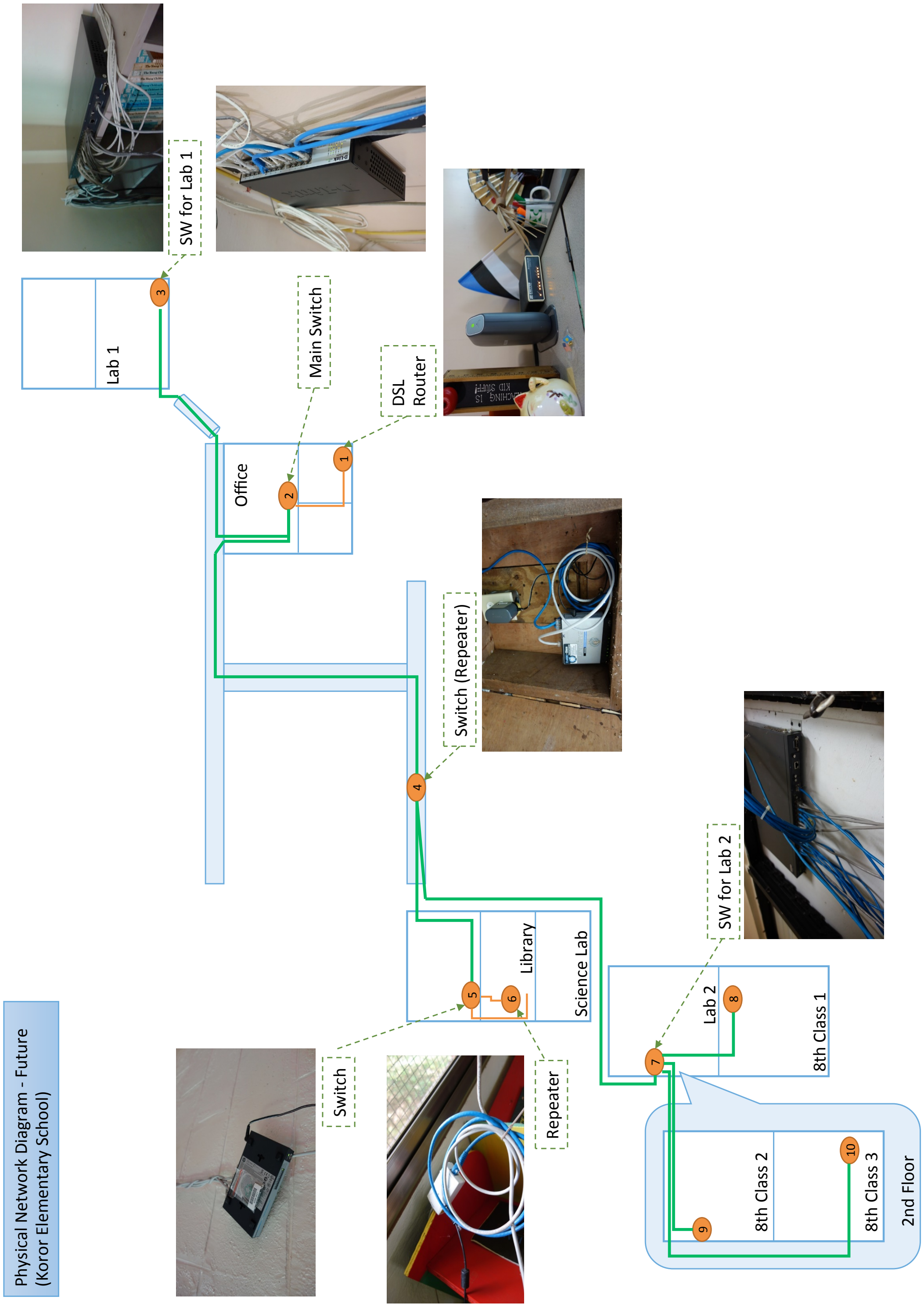
## Additional Configurations

-

2

# Appendix I


Logical Network Diagram - Future
(Koror Elementary)
MOE
PNCC VLAN
Admin Office
DSL
Diamond Link
1
New
Router (c13rt01)
MikroTik RB750UP
I/F 5
10.0.0.13
10.0.13.1
I/F 4
1G
I/F 3
10.0.0.0/24
10.0.13.0/24
Temporary AP (c13ap00)
Aruba AP105
SSID: koor.wifi PASS: koor3210
10.0.13.211
New
192.168.11.0/24
2
Main Switch (c13ms01)
D-Link Gigabit Switch (24)
10.0.13.201
I/F 24
I/F 22
I/F 23
I/F 21
100M
New
AP (c13ap01)
Ubiquiti PicoStation M2
10.0.13.210
5
Library Switch (c13sw04)
HP 1410-8G
(No Intelligent SW)
I/F 8
1G
4
Repeater (c13sw02)
LINKSYS SD2008
I/F 8
I/F 6
1G
I/F 7
1G
Lab 2 Switch (c13sw03)
Asante IntraCore3524
10.0.13.203
I/F 26
*I/F 25 of c13sw03 is kept for future Gigabit needs
1G
I/F 26
Lab 1 Switch (c13sw01)
Asante IntraCore3524
10.0.13.202
Repeater
EnGenius EPE5818
I/F 7
6
100M
AP (c13ap07)
10.0.13.216
Do not set AP
in this time
New
Library
7
I/F 24
I/F 23 (b/u)
100M
AP (c13ap03)
10.0.13.212
New
Lab 2
I/F 22
I/F 21 (b/u)
AP (c13ap04)
10.0.13.213
New
8th (1F-1)
8
I/F 20
I/F 19 (b/u)
AP (c13ap05)
10.0.13.214
New
8th (2F-1)
9
I/F 18
I/F 17 (b/u)
AP (c13ap06)
10.0.13.215
New
8th (2F-2)
10
3
I/F 24
100M
AP (c13ap02)
10.0.13.211
Do not set AP
in this time
New
Lab 1



Physical Network Diagram - Future
(Koror Elementary School)

# Appendix J

**Test Case for New Wi-Fi Network in Lab Environment**

(OK/NG)

| # | Category | Item | Criteria | Method | Result |
|---|---|---|---|---|---|
| 1 | Cabling | Label | Each cable has correct labels | Check labels by comparing with NW diagram | - |
| 2 |  | Port | Each cable connect correct port | Check port number by comparing with NW diagram | OK |
| 3 | NW Connection | Link up | NW device's LED indicates "link up" | Check whether LED of each ports turns on | OK |
| 4 |  | Auto Negotiation | Speed/Duplex has negotiated correctly | Check management tool of each NW devices by comparing with NW Diagram | OK |
| 5 |  | Ping | Ping response is "OK" between two devices | Do Ping based on the ping table | OK |
| 6 | DHCP (c13rt01) | Windows PC | Device receives correct DHCP address from router | Connect device to c13ms01 and check IP address whether it is within 10.100.13.2-200 |  |
| 7 | DHCP (c13ap01: UAP) | iPad | Device receives correct DHCP address from Access Point | Connect device to c13ap01 and check IP address whether it is 192.168.11.x |  |
| 8 |  | Windows PC | Device receives correct DHCP address from Access Point | Connect device to c13ap01 and check IP address whether it is 192.168.11.x |  |
| 9 |  | Mac PC | Device receives correct DHCP address from Access Point | Connect device to c13ap01 and check IP address whether it is 192.168.11.x |  |
| 10 |  | Android Phone | Device receives correct DHCP address from Access Point | Connect device to c13ap01 and check IP address whether it is 192.168.11.x |  |
| 11 | Route | Routing Table | Routing table has only appropriate routes | Login router (c13rt01) and check the routing table which has the following two segments:<br>10.100.13.0/24<br>10.0.0.0/24 |  |
| 12 | RADIUS Authentication (via Airport) | iPad | RADIUS authentication is success from the device | Pass the authentication using test ID/Password:<br>ID: student<br>Password: student | OK |
| 13 |  | Windows PC | RADIUS authentication is success from the device | Pass the authentication using test ID/Password:<br>ID: student<br>Password: student | OK |
| 14 |  | Android Phone | RADIUS authentication is success from the device | Pass the authentication using test ID/Password:<br>ID: student<br>Password: student | OK |
| 15 | Capacity Performance | Connection of AP | AP accept connection from many iPads | Connect 25 wireless devices to AP at one time and check the connectivity of each devices | - |
| 16 |  | Throughput | AP provides appropriate throughput to iPads | Download huge file from intranet and check the downloading time comparing with estimation | - |

**Test Case for New Wi-Fi Network in Lab Environment**

(OK/NG)

| # | Category | Item | Criteria | Method | Result |
|---|---|---|---|---|---|
| 17 | Application Performance | iPad | Application which requires MOE'S intranet connection works correctly | Safari connects to /c00sv06.moe/ | OK |
| 18 | | iPad | Application which requires the Internet connection works correctly | Safari shows the top page of Google (www.google.com) | OK |
| 19 | System Log | Router | System log shows router works correctly | Check system log in c13rt01 and confirm the log does not contain suspicious log | OK |
| 20 | | Switch | System log shows switch works correctly | Check system log in c13ms01 and confirm the log does not contain suspicious log | OK |
| 21 | | AP | System log shows AP works correctly | Check system log in c13ap01 and confirm the log does not contain suspicious log | OK |

**Ping Table (for KES Lab)**

| | From | | | To | | Result |
|---|---|---|---|---|---|---|
| | Device | IP Address | | Device | IP Address | (OK/NG) |
| 1 | c13rt01 (Lab) | 10.0.0.100 | --> | c00rtr01 (Live) | 10.0.0.254 | |
| 2 | | | --> | c13rt01 (Live) | 10.0.0.13 | |
| 3 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | |
| 4 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | |
| 5 | | | --> | c13ms01 | 10.100.13.201 | |
| 6 | | | --> | c13ap01 (UAP) | 10.100.13.211 | OK |
| 7 | | | --> | c13ap02 (Airport) | 10.100.13.212 | |
| 8 | PC under C13ms01 | 10.100.13.198 (DHCP) | --> | c13ms01 | 10.100.13.201 | |
| 9 | | | --> | c13ap01 (UAP) | 10.100.13.211 | OK |
| 10 | | | --> | c13ap02 (Airport) | 10.100.13.212 | |
| 11 | | | --> | c00rtr01 (Live) | 10.0.0.254 | |
| 12 | | | --> | c13rt01 (Live) | 10.0.0.13 | |
| 13 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | |
| 14 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | |
| 15 | Device under c13ap01 | 192.168.11.xxx (DHCP) | --> | c13ap01 (UAP) | 10.100.13.211 | OK |
| 16 | | (Src-NAT at AP) | --> | c13ms01 | 10.100.13.201 | OK |
| 17 | | | --> | c13ap02 (Airport) | 10.100.13.212 | |
| 18 | | | --> | PC under C13ms01 | 10.100.13.200 (DHCP) | |
| 19 | | | --> | c00rtr01 (Live) | 10.0.0.254 | OK |
| 20 | | | --> | c13rt01 (Live) | 10.0.0.13 | OK |
| 21 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | OK |
| 22 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | OK |
| 23 | Device under c13ap02 | 10.100.13.xxx (DHCP) | --> | c13ap02 (Airport) | 10.100.13.212 | |
| 24 | | | --> | c13ms01 | 10.100.13.201 | |
| 25 | | | --> | c13ap01 (Aruba) | 10.100.13.211 | |
| 26 | | | --> | PC under C13ms01 | 10.100.13.198 (DHCP) | |
| 27 | | | --> | c00rtr01 (Live) | 10.0.0.254 | |
| 28 | | | --> | c13rt01 (Live) | 10.0.0.13 | |
| 29 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | |
| 30 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | |

# Appendix K

**Testcase for New Wi-Fi Network in Koror Elementary School**

| # | Category | Item | Criteria | Method | Result |
|---|---|---|---|---|---|
| 1 | Cabling | Label | Each cable has correct labels | Check labels by comparing with NW diagram | |
| 2 | | Port | Each cable connect correct port | Check port number by comparing with "Cabel Connection List" | OK |
| 3 | NW Connection | Link up | NW device's LED indicates "link up" | Check whether LED of each ports turns on | OK |
| 4 | | Auto Negotiation | Speed/Duplex has negotiated correctly | Check management tool of each NW devices by comparing with NW Diagram | OK |
| 5 | | Ping | Ping response is "OK" between two devices | Do Ping based on the ping table | OK |
| 6 | DHCP (from Router) | Windows PC | Device receives correct DHCP address from router | Connect device to c13ms01 and check IP address whether it is within 10.100.13.2-200 | |
| 7 | DHCP (from Aruba AP) | Windows PC | Device receives correct DHCP address from Access Point | Connect device to c13ap01 and check IP address whether it is 192.168.11.x | |
| 8 | | iPad | Device receives correct DHCP address from Access Point | Connect device to c13ap01 and check IP address whether it is 192.168.11.x | |
| 9 | Routing | Routing Table | Routing table has only appropriate routes | Login router and check the routing table which has the following two segments:<br>10.0.13.0/24 (KES LAN segment)<br>10.0.0.0/24 (MOE WAN segment)<br>0.0.0.0/0 (default route) | |
| 10 | RADIUS Authentication | iPad | RADIUS Authentication is success from iPad | Pass the authentication using test ID/Password:<br>ID: student<br>Password: student | OK |
| 11 | | Windows PC | RADIUS Authentication is success from PC | Pass the authentication using test ID/Password:<br>ID: student<br>Password: student | OK |
| 12 | | Android Phone | RADIUS Authentication is success from PC | Pass the authentication using test ID/Password:<br>ID: student<br>Password: student | OK |
| 13 | Capacity Performance | Connection of AP | AP accept connection from many iPads | Connect 25 wireless devices to AP at one time and check the connectivity of each devices | |
| 14 | | Throughput | AP provides appropriate throughput to iPads | Download huge file(?) from intranet and check the downloading time comparing with estimation | |
| 15 | Application Performance | iPad | Application which requires MOE'S intranet connection works correctly | Safari connects to /c00sv06.moe/ | OK |
| 16 | | iPad | Application which requires the Internet connection works correctly | Safari shows the top page of Google (www.google.com) | OK |

**Testcase for New Wi-Fi Network in Koror Elementary School**

| # | Category | Item | Criteria | Method | Result |
|---|---|---|---|---|---|
| 17 | System Log | Router | System log shows router works correctly | Check system log in c13rt01 and confirm the log does not contain suspicious log | **OK** |
| 18 | | Switch | System log shows switch works correctly | Check system log in c13ms01 and confirm the log does not contain suspicious log | **OK** |
| 19 | | AP | System log shows AP works correctly | Check system log in c13ap01 and confirm the log does not contain suspicious log | **OK** |

**Ping Table (for KES)**

| | From | | | To | | Result |
|---|---|---|---|---|---|---|
| | Device | IP Address | | Device | IP Address | (OK/NG) |
| 1 | c13rt01 | 10.0.0.13 | --> | c00rt01 (Live) | 10.0.0.254 | |
| 2 | | | --> | c13rt01 (Lab) | 10.0.0.100 | |
| 3 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | |
| 4 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | |
| 5 | | | --> | c13ap01 (UAP) | 10.0.13.210 | OK |
| 6 | | | --> | c13ap03 (UAP) | 10.0.13.212 | OK |
| 7 | | | --> | c13ap04 (UAP) | 10.0.13.213 | OK |
| 8 | | | --> | c13ap05 (UAP) | 10.0.13.214 | OK |
| 9 | | | --> | c13ap06 (UAP) | 10.0.13.215 | OK |
| 10 | PC under C13ms01 | 10.100.13.100 | --> | c13ap01 (UAP) | 10.0.13.210 | OK |
| 11 | | | --> | c13ap03 (UAP) | 10.0.13.212 | OK |
| 12 | | | --> | c13ap04 (UAP) | 10.0.13.213 | OK |
| 13 | | | --> | c13ap05 (UAP) | 10.0.13.214 | OK |
| 14 | | | --> | c13ap06 (UAP) | 10.0.13.215 | OK |
| 15 | | | --> | c00rt01 (Live) | 10.0.0.254 | |
| 16 | | | --> | c13rt01 (Lab) | 10.0.0.100 | |
| 17 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | |
| 18 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | |
| 19 | Device under c13ap01 | 10.0.13.xxx (DHCP) | --> | c13ap01 (UAP) | 10.0.13.210 | OK |
| 20 | | | --> | PC under C13ms01 | 10.0.13.200 (DHCP) | OK |
| 21 | | | --> | c00rt01 (Live) | 10.0.0.254 | OK |
| 22 | | | --> | c13rt01 (Lab) | 10.0.0.100 | OK |
| 23 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | OK |
| 24 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | OK |
| 25 | Device under c13ap03 | 10.0.13.xxx (DHCP) | --> | c13ap03 (UAP) | 10.0.13.212 | OK |
| 26 | | | --> | PC under C13ms01 | 10.0.13.200 (DHCP) | OK |
| 27 | | | --> | c00rt01 (Live) | 10.0.0.254 | OK |
| 28 | | | --> | c13rt01 (Lab) | 10.0.0.100 | OK |
| 29 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | OK |
| 30 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | OK |
| 31 | Device under c13ap04 | 10.0.13.xxx (DHCP) | --> | c13ap04 (UAP) | 10.0.13.213 | OK |
| 32 | | | --> | PC under C13ms01 | 10.0.13.200 (DHCP) | OK |
| 33 | | | --> | c00rt01 (Live) | 10.0.0.254 | OK |
| 34 | | | --> | c13rt01 (Lab) | 10.0.0.100 | OK |
| 35 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | OK |
| 36 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | OK |
| 37 | Device under c13ap05 | 10.0.13.xxx (DHCP) | --> | c13ap05 (UAP) | 10.0.13.214 | OK |
| 38 | | | --> | PC under C13ms01 | 10.0.13.200 (DHCP) | OK |
| 39 | | | --> | c00rt01 (Live) | 10.0.0.254 | OK |
| 40 | | | --> | c13rt01 (Lab) | 10.0.0.100 | OK |
| 41 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | OK |
| 42 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | OK |
| 43 | Device under c13ap06 | 10.0.13.xxx (DHCP) | --> | c13ap06 (UAP) | 10.0.13.215 | OK |
| 44 | | | --> | PC under C13ms01 | 10.0.13.200 (DHCP) | OK |
| 45 | | | --> | c00rt01 (Live) | 10.0.0.254 | OK |
| 46 | | | --> | c13rt01 (Lab) | 10.0.0.100 | OK |
| 47 | | | --> | f00sv01 (RADIUS) | 10.0.0.236 | OK |
| 48 | | | --> | f00sv06 (ProfileMGR) | 10.0.0.241 | OK |

# Appendix L

## Network Implementation Procedure for Koror Elementary School

| | |
|---|---|
| **Date/Time:** | **3:00pm - 5:00pm, Tuesday, July 8, 2014** |
| **Place:** | **Koror Elementary School (KES)** |
| Attached: | Network Diagram (Logical, Physical)<br>Cable Connection List (KES)<br>Network Test Case (KES) |

### 1. Check and Notification

(1) Check cabling and outlets before implementation.

- Check the cabling status based on "Cable Connection List (KES)"

(2) Check the status of network and other devices before implementation

(3) Keep current router (Belkin) settings, especially:

- Wi-Fi setting (SSID, Security, Channel, Password…)
- DHCP addresses which the router (Belkin) provides currently.

(4) Check that IP addresses used for new network devices do not exist on current network.

(5) Notify the network change (and disconnection) to the staff in KES

### 2. Place Access Points for Admin Office

(1) *c13ap01* (in Admin Office)

*Until "PicoStation M2" arrives, "Aruba AP 105" is used as *c13ap01*.

- Connect *c13ap01* (already configured before implementation) to *c13rt01.*
- Turn on *c13ap01* and test network connection from Console PC (= ping to *c13ap01*)
- Connect a wireless device to c13ap01 and test network connection from the device. (Use Ping Table No.13 - No.19)

### 3. Replace Router (*c13rt01*) in Admin Office (Principal's room) [[Network Disconnection Occurs!]]

- Unplug all cables from current Router (Belkin).
- Replace current router (Belkin) to *c13rt01* (MikroTik RB750UP) and connect **ONLY DOWNLINK cable (for *c13ms01*)** to *c13rt01*. (ATTENTION: Do NOT CONNECT UPLINK cable to *c13rtr01* until completion of the test for KES segment for avoiding to affect MOE WAN network.)
- Test network connection from *c13rt01* to each network device in KES segment. (use Ping

Table No.5 - No.6)

- Connect UPLINK cable to *c13rt01.*
- Test network connection to MOE segment. (use Ping Table No.1 - No.4)

**4. Check Network After Implementation**

- Test rest of items based on “Network Test Case (KES)”.

**5. Keep Backup of Configuration**

- Keep the backup files of *c13rt01* and *c13ap01*.

[END OF THE PROCEDURE]

## Network Implementation Procedure for Koror Elementary School

| | |
|---|---|
| **Date/Time:** | **10:00am - 12:00am, Monday, Aug 4, 2014** |
| **Place:** | **Koror Elementary School (KES)** |
| Attached: | Network Diagram (Logical, Physical) |
| | Cable Connection List (KES) |
| | Network Test Case (KES) |
| | MDM Test Case (KES) |

---

**1. Place access points for each room**

(2) *C13ap01* (in Admin Office)

- Connect *c13ap01* to *c13ms01.*
- Turn on *c13ap01* and test network connection from Console PC connected to *c13ms01*.
- Connect a wireless device to c13ap01 and test network connection from the device.

(3) *C13ap03* (in Lab 2)

- Connect *c13ap03* to *c13sw03*.
- Turn on *c13ap03* and test network connection from Console PC connected to *c13sw03*.
- Connect a wireless device to *c13ap03* and test network connection from the device.

(4) *C13ap04* (in 8th Grade Classroom 1F-1)

- Connect *c13ap04* to *c13sw03*.
- Turn on *c13ap04* and test network connection from Console PC connected to *c13sw03*.
- Connect a wireless device to *c13ap04* and test network connection from the device.

(5) *C13ap05* (in 8th Grade Classroom 2F-1)

- Connect *c13ap05* to *c13sw03.*
- Turn on *c13ap05* and test network connection from Console PC connected to *c13sw03*.
- Connect a wireless device to *c13ap05* and test network connection from the device.

(6) *C13ap06* (in 8th Grade Classroom 2F-2)

- Connect *c13ap06* to *c13sw03.*
- Turn on *c13ap06* and test network connection from Console PC connected to *c13sw03*.
- Connect a wireless device to *c13ap05* and test network connection from the device.

**2. Check Network After Implementation**

- Test rest of items based on “Network Test Case (KES)”.

**3. Test Applications Using New Network**

- Proceed test based on “MDM System Test Case (KES)”.

[END OF THE PROCEDURE]

# Appendix M

**List of IP Address for 10.0.0.x [SAMPLE]**

| IP Address | | | | Usage | Hostname | Date |
|---|---|---|---|---|---|---|
| 10 | 0 | 0 | 1 | JFK | c01rt01 | 06/30/14 |
| | | | 2 | Ngarchelong | c02rt01 | 06/30/14 |
| | | | 3 | Ngaraard | c03rt01 | 06/30/14 |
| | | | 4 | Ngiwal | | |
| | | | 5 | Melekeok | c05rt01 | 06/30/14 |
| | | | 6 | Ngchesar | | |
| | | | 7 | Airai | c07rt01 | 06/30/14 |
| | | | 8 | Ngardmau | c08rt01 | 06/30/14 |
| | | | 9 | Ngeremlengui | c09rt01 | 06/30/14 |
| | | | 10 | Ibobang | c10rt01 | 06/30/14 |
| | | | 11 | Aimeliik | c11rt01 | 06/30/14 |
| | | | 12 | GBH | c12rt01 | 06/30/14 |
| | | | 13 | Koror | c13rt01 | 06/30/14 |
| | | | 14 | PHS | c14rt01 | 06/30/14 |
| | | | 15 | Meyuns | c15rt01 | 06/30/14 |
| | | | 16 | Peleliu | c16rt01 | 06/30/14 |
| | | | 17 | Angaur | c17rt01 | 06/30/14 |
| | | | 18 | Sonsorol | | |
| | | | 19 | Pulo-Ana | | |
| | | | 20 | Tobi | | |
| | | | 21 | Maris Stella | | |
| | | | 22 | Mindszenty | | |
| | | | 23 | SDA | | |
| | | | 24 | PMA | | |
| | | | 25 | MOE | c25rt01 | 06/30/14 |
| | | | 26 | Food Service | | |
| | | | 27 | Special Education | c27rt01 | 06/30/14 |
| | | | 28 | Public Library | c28rt01 | 06/30/14 |
| | | | … | | | |
| | | | 100 | Koror (for Lab) | cA1rt01 | 08/04/14 |
| | | | 101 | DHCP Range | | 06/30/14 |
| | | | … | (50 Nodes) | | 06/30/14 |
| | | | 150 | DHCP Range | | 06/30/14 |
| | | | 151 | | | |
| | | | | | | |

**Host/Network Device Naming Policy**

| Location | | School No. | | Device | | Device No. | |
|---|---|---|---|---|---|---|---|
| 1 Char | | 2 Digit | | 2 Char | | 2 Digit | |
| **c** | Compus | **00** | MOE | **rt** | Router | **01** | 1st device |
| **f** | Office | **01** | JFK | **ms** | Main Switch | **02** | 2nd device |
| | | **02** | Ngarchelong | **sw** | Switch | **03** | 3rd device |
| | | **03** | Ngaraard | **ap** | Access Point | | ... |
| | | **05** | Melekeok | **sv** | Server | | |
| | | **07** | Airai | **pr** | Printer | | |
| | | **08** | Ngardmau | | | | |
| | | **09** | Ngeremlengui | | | | |
| | | **10** | Ibobang | | | | |
| | | **11** | Aimeliik | | | | |
| | | **12** | GBH | | | | |
| | | **13** | Koror | | | | |
| | | **14** | PHS | | | | |
| | | **15** | Meyuns | | | | |
| | | **17** | Peleliu | | | | |
| | | **18** | Angaur | | | | |
| | | **27** | Sped | | | | |
| | | **29** | Mood | | | | |

**Examples**

| Hostname | Meaning |
|---|---|
| 7 Char | |
| **c01rt01** | JFK's router No.1 |
| **c13ms01** | Koror's main switch No.1 |
| **c14ap10** | PHS's access point No.10 |
| **f14sw01** | PHS(Office)'s switch No.1 |
| **f00sv01** | MOE's server No.1 |

**Assigning Policy for School LAN**

| | | | | |
|---|---|---|---|---|
| 10 | 0 | x | 1 | Default Gateway |
| | | | 2 | Users on Ethernet |
| | | | … | (199 nodes) |
| | | | 200 | |
| | | | 201 | Network Devices |
| | | | … | (30 nodes) |
| | | | 230 | |
| | | | 231 | Printers |
| | | | … | (20 nodes) |
| | | | 250 | |
| | | | 251 | Servers |
| | | | … | (4 nodes) |
| | | | 254 | |

**Assigning Policy for MOE WAN**

| | | | | |
|---|---|---|---|---|
| 10 | 0 | 0 | 1 | Campus LANs (Router Public Address) |
| | | | … | (100 Nodes) |
| | | | 100 | |
| | | | 101 | DHCP range |
| | | | … | (100 Nodes) |
| | | | 150 | |
| | | | 151 | Not Assigned |
| | | | … | (100 Nodes) |
| | | | 200 | |
| | | | 201 | Network Devices |
| | | | … | (30 nodes) |
| | | | 230 | |
| | | | 231 | Printers, Special Devices |
| | | | … | (5 nodes) |
| | | | 235 | |
| | | | 236 | Servers |
| | | | … | (10 nodes) |
| | | | 245 | |
| | | | 246 | Gateways |
| | | | … | (9 nodes) |
| | | | 254 | Default Gateway |

**Port Usage Policy**

| | |
|---|---|
| Hostname: | **c013sw01** |
| IP address: | **10.0.13.202** |
| Device: | **Asante IntraCore 3524** |
| Location: | **Lab 1** |

| Port | Speed | Duplex | Hostname | Comments |
|---|---|---|---|---|
| 1 | 1G | Auto | | |
| 2 | 1G | Auto | | |
| 3 | 1G | Auto | | |
| 4 | 1G | Auto | | |
| 5 | 1G | Auto | | |
| 6 | 1G | Auto | | |
| 7 | 1G | Auto | | |
| 8 | 1G | Auto | | |
| 9 | 1G | Auto | | |
| 10 | 1G | Auto | | |
| 11 | 1G | Auto | | |
| 12 | 1G | Auto | | |
| 13 | 1G | Auto | | |
| 14 | 1G | Auto | | |
| 15 | 1G | Auto | | |
| 16 | 1G | Auto | | |
| 17 | 1G | Auto | | |
| 18 | 1G | Auto | | |
| 19 | 1G | Auto | | |
| 20 | 1G | Auto | | |
| 21 | 1G | Auto | | |
| 22 | 1G | Auto | | |
| 23 | 1G | Auto | c013ap01 | Access Point for Lab1 |
| 24 | 1G | Auto | c013msw01 | Uplink to main switch |

Other Devices

Network Devices

# Appendix N

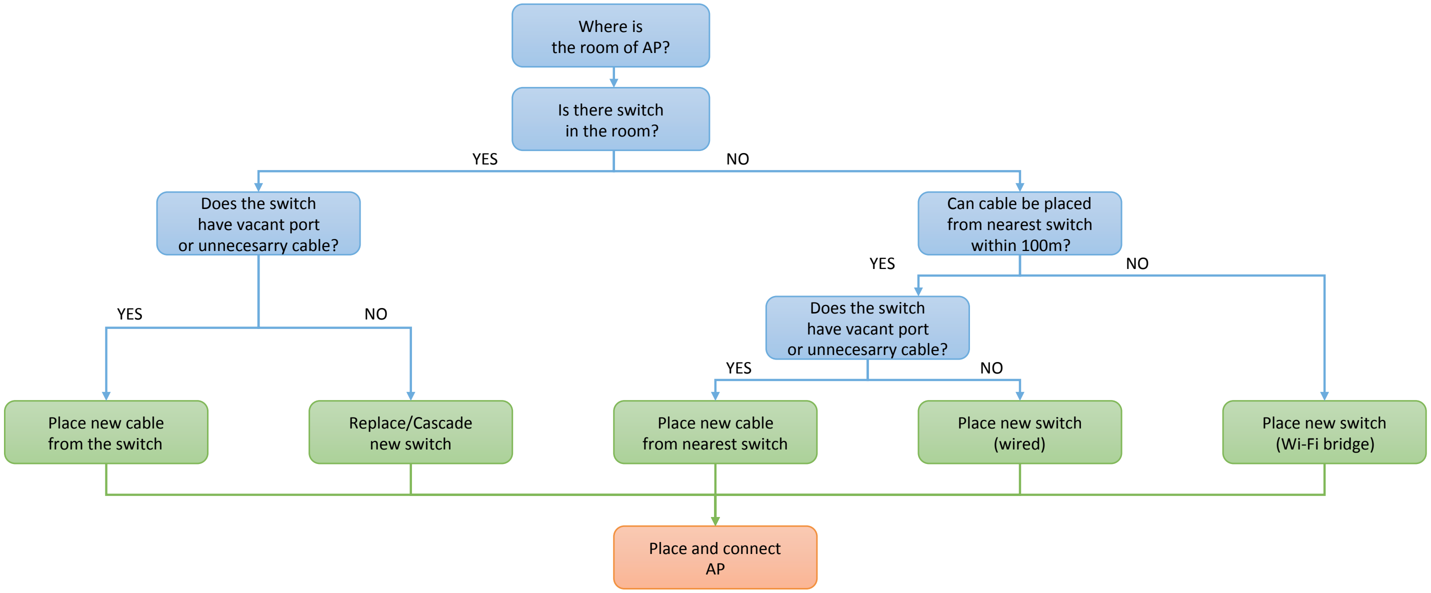
## General Steps of Network Design and Implementation

| Items | | | Actions |
|---|---|---|---|
| **1. Fix Purpose of New Network** | | | |
| 1) | | Answer basic questions for new network requirements | What is the goal of new network (or extended network)? If you want to provide Wi-Fi network, you should able to answer these questions: Who is the users? How many? Where? By when? … Through these steps, you can fix the purpose of new network and get clear requirements. |
| **2. Pre-survey (Before Visiting Site)** | | | |
| 2) | | Collect existing information (map, NW structure…) | Before visiting the site, you should collect existing information, such as NW diagrams of the site, maps, and photos. Based on the information you can figure out what information is missing and need to survey. |
| 3) | | Login network devices remotely (configuration, log…) | If you can login the device remotely, it will be helpful to understand current network situation. From configuration and log, you can figure out logical structure and potential problems of the network. |
| 4) | | List up items which will be checked in site survey | Through pre-survey, you can list up the items which you will check in site survey. The list may prevent to forget survey items and provide working efficiency at survey. |
| **3. Site Survey** | | | |
| 5) | | 1st Survey (Overall) | The main purpose of first survey is to understand overview of the network and confirm actual situation. And then, on 2nd survey, verify the detail points. [You do not need to separate survey two times. If you can finish the all survey in one time, it would be better] |
| | a. | Follow from WAN to LAN (top to bottom) | Follow network devices and cables from WAN (DSL or telecom lines) to LAN (Router, Main switch, Switches, Hubs, Cables, RJ-45, and End-user devices). And record them. |
| | b. | Check model of devices | What is maker/model of the network device?<br>Where is the location placed? |
| | c. | Check connections b/w devices | What devices are connected with the device?<br>Where are cables placed? |
| | d. | Take Pictures | Taking pictures is a good way to keep and share information more correctly. Also, you can check the port usage and other information based on the pictures. |
| | e. | Check something wrong/bad | Through the survey, you should check something wrong or bad about network (damaged cables, strange fan noise, dirty place, and so on) and record them. |
| 6) | | 2nd Survey (Detail) | In 2nd survey, you should check the points which you have not checked in 1st survey. It is better to do 2nd survey after creating network diagrams. If you have the diagrams, they will be great help for the survey (to verify the info of the diagram and to clarify the info still missing). |
| | a. | Check ports (availability, usage, I/F number) | How many ports (interfaces) are vacant? What device are mainly connected to the device?<br>Which ports are used for uplink (downlink) cable? |
| | b. | Check outlets (availability) | How many outlets are vacant near the network device (if add more devices)? |
| | c. | Check cabling (availability, route, quality, length) | How many cables are available (unused) for new devices? Where cable can be placed? |
| | d. | Check configuration (if available) | Connecting console device to the network device, and check its configuration to get logical network information (IP address, Access Control, and any other special settings). |
| **4. Create Network Diagram** | | | |
| 7) | | Physical Network Diagram (Current) | Based on the survey, create physical network diagram (current).<br>Basically, it is a map which contains location of network devices, cable route, and photos. Reader can grasp overview of current network. |
| 8) | | Logical Network Diagram (Current) | Based on the survey, create logical network diagram (current).<br>It provides logical information of each devices and connections with each other. It contains type of device, model, I/F, Vlan (if applicable), and IP address. |
| **5. Design New Network** | | | |
| 9) | | Logical Network Diagram (Future) | Modify the current logical diagram based on requirements of new network. Add new device (eliminate old ones), fix connections, and specify logical setting (hostname, port usage, speed, duplex, IP address, network segment and so on). |

### General Steps of Network Design and Implementation

| Items | | Actions |
|---|---|---|
| 10) | Physical Network Diagram (Future) | Modify the current physical diagram based on requirements of new network. Fix location of new devices, new cabling (route) and placed new outlets (if required) |
| **6. Specify Requirements** | | |
| 11) | Specify Requirements | Through designing process, you can fix the requirements for new network. Clarifying  the requirement will prevent to |
| **7. Purchase/Order new devices and cables/outlets** | | |
| 12) | Purchase new devices | Based on the requirements, order new devices, cabling, and outlets. |
| **8. Configuration** | | |
| 13) | Create configuration | Based on the requirements, create configuration for new devices (including change current network devices). |
| **9. Test New Network (Lab and On-site)** | | |
| 14) | Create test case | Create test criteria before starting test. Test items vary depending on the new requirements; but, the following items commonly contain: Connection Test (b/w NW devices and other user devices), Function Test (new function works correctly), Log (system log/counter do not contain unreasonable data) |
| 15) | Test network devices and record/report the results | Based on test cases, check the test criteria in Lab environment and Onsite. If the result is not correct, fix the problem. All result record as "test result" and report to appropriate person. |
| **10. Implementation** | | |
| 16) | Implementation new network | After verifying the network working with testing in Lab, implement the new network on-site based on the network diagrams. And then, test the network based on the test case for on-site. |
| **11. Follow Up 1st Business Day** | | |
| 17) | Be on-site on 1st business day | Even if the test results are perfect, some trouble could show up when the system works. So, network engineers should be in the site on 1st business day and support the users when system failures happen. |
| **12. Update Management Documents** | | |
| 18) | Keep diagrams as management tools | Logical/Physical network diagrams are useful as management tools of network. However, it is more important to keep them up-to-date (when network change happens). |

Logic Tree for Network Design in Tablet Deployment Project


Where is the room of AP?
Is there switch in the room?
YES
NO
Does the switch have vacant port or unnecesarry cable?
Can cable be placed from nearest switch within 100m?
YES
NO
YES
NO
Does the switch have vacant port or unnecesarry cable?
YES
NO
Place new cable from the switch
Replace/Cascade new switch
Place new cable from nearest switch
Place new switch (wired)
Place new switch (Wi-Fi bridge)
Place and connect AP

# Appendix O

## Configuration Guide of MikroTik Router (Webfig on Router OS v5.24)

This document is a Configuration Guide of MikroTik Router (routerboard 750 series) for WAN routers at elementary schools. The settings and instructions are based on the router for Koror Elementary School as of Aug 8, 2014. Thus, if you apply the configuration into the other routers, you should check whether the setting is based on up-to-date network design and configuration which MOE IT requires.

**Index**

**1. Login**

✓ You can access the router via web browser on your PC. When the router has a factory setting, you can access the router by the following steps:

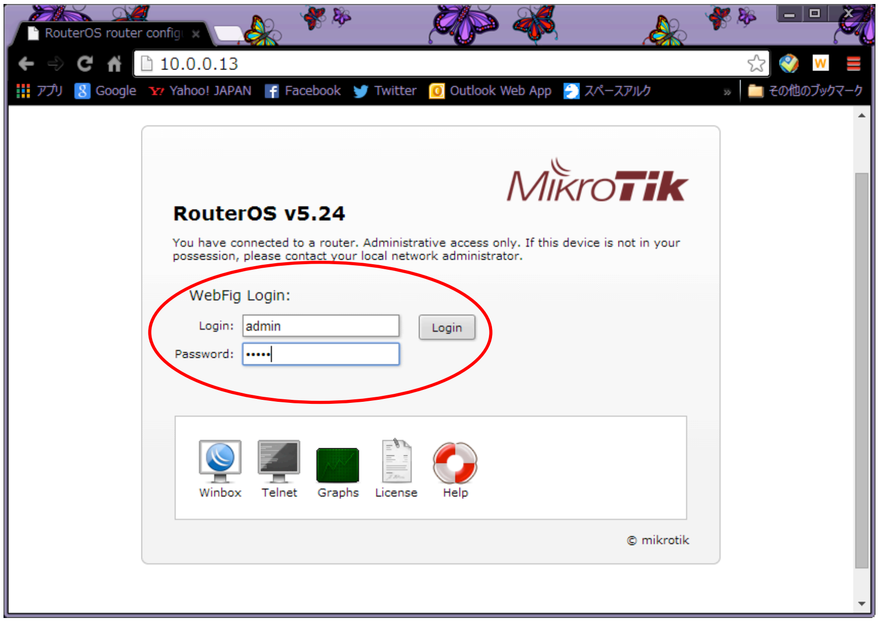
(1) Set your computer IP configuration to automatic

(2) Connect your computer to interface 2-5 of the router

(3) Power on the router (you will receive DHCP address from the router)

(4) Enter “192.168.88.1” in your web browser

✓ The default username is “admin” and there is no-password. Enter them into the windows and click “Login” button. You can login the router.



RouterOS v5.24

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

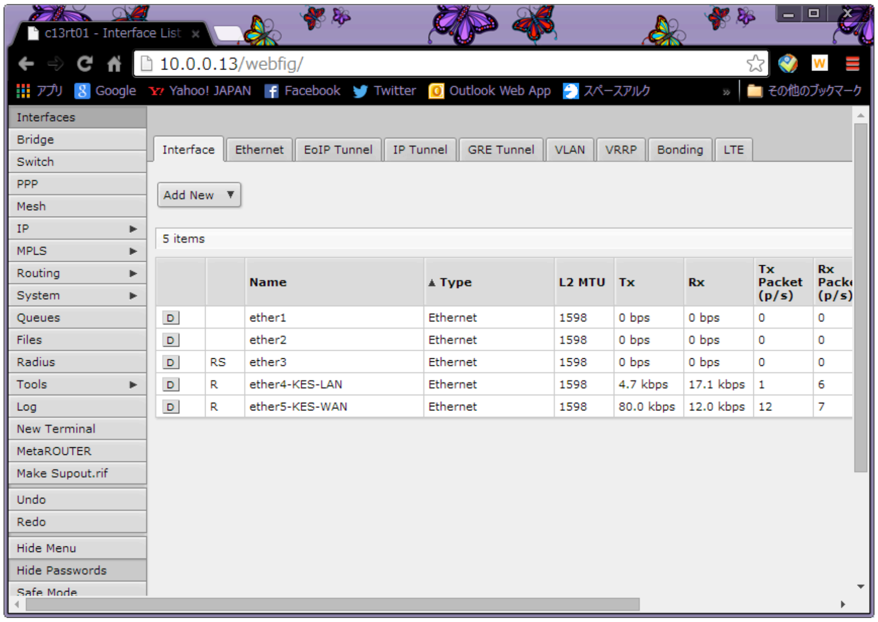
WebFig Login:

Login: admin

Password: •••••

## 2. Interfaces

- ✓ Here is the top screen after login.



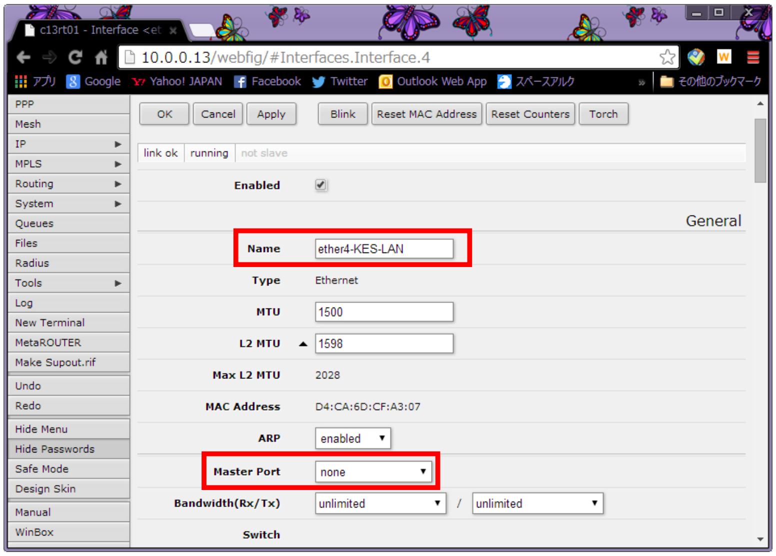
5 items

| | | Name | ▲ Type | L2 MTU | Tx | Rx | Tx Packet (p/s) | Rx Packe (p/s) |
|---|---|---|---|---|---|---|---|---|
| D | | ether1 | Ethernet | 1598 | 0 bps | 0 bps | 0 | 0 |
| D | | ether2 | Ethernet | 1598 | 0 bps | 0 bps | 0 | 0 |
| D | RS | ether3 | Ethernet | 1598 | 0 bps | 0 bps | 0 | 0 |
| D | R | ether4-KES-LAN | Ethernet | 1598 | 4.7 kbps | 17.1 kbps | 1 | 6 |
| D | R | ether5-KES-WAN | Ethernet | 1598 | 80.0 kbps | 12.0 kbps | 12 | 7 |

- ✓ Firstly, you should configure the interfaces. After clearing default setting, you assign the interfaces based on the network design. (When you clear the setting, you may be disconnected from the router. So please keep in mind to match your PC's addressing to router's addressing)
- ✓ In the KES case, "ether 4" is for LAN segment (Name: ether4-KES-LAN) and "ether 5" is for WAN segment (Name: ether5-KES-WAN).

- ✓ When clicking the name of each interface, you can see the configuration for the interface.
- ✓ In the KES case, you will set the following three items (the other settings are default):

| | | |
|---|---|---|
| (1) | Name | interface#-location-purpose (like ether4-KES-LAN) |
| (2) | Master port | none |
| (3) | Speed | 100Mbps (RB750 does not have 1Gbps port) |



link ok | running | not slave

Enabled ☑

General

Name: ether4-KES-LAN

Type: Ethernet

MTU: 1500

L2 MTU: 1598

Max L2 MTU: 2028

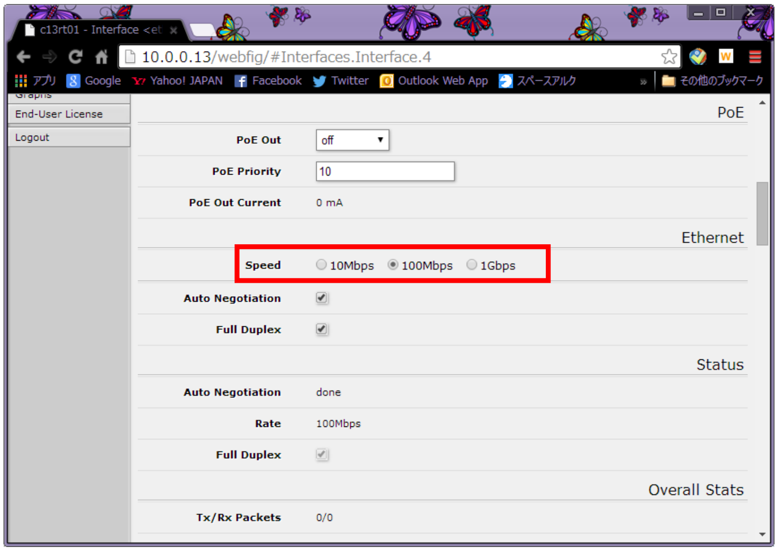
MAC Address: D4:CA:6D:CF:A3:07

ARP: enabled

Master Port: none

Bandwidth(Rx/Tx): unlimited / unlimited

Switch



PoE

PoE Out: off

PoE Priority: 10

PoE Out Current: 0 mA

Ethernet

Speed: ○ 10Mbps ● 100Mbps ○ 1Gbps

Auto Negotiation ☑

Full Duplex ☑

Status

Auto Negotiation: done

Rate: 100Mbps

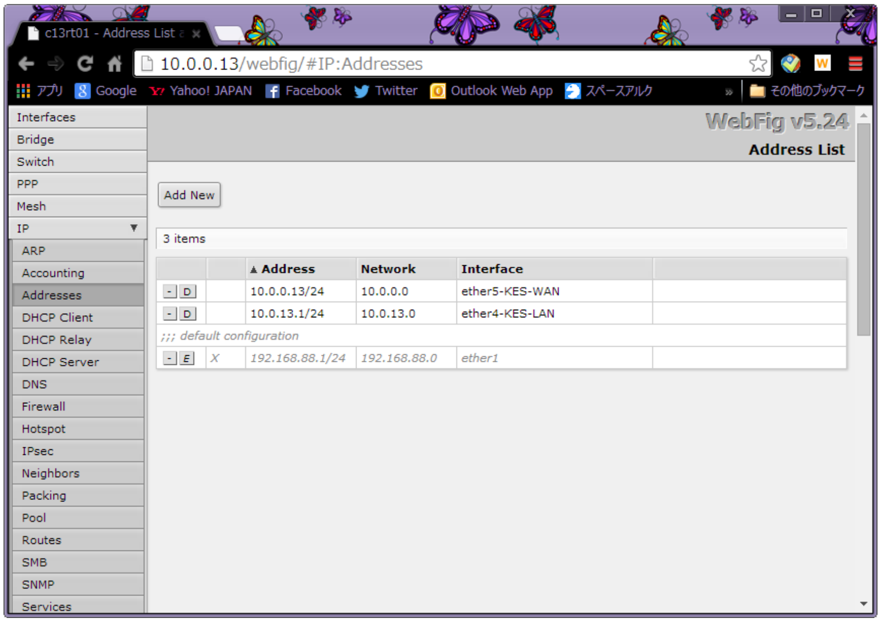
Full Duplex ☑

Overall Stats

Tx/Rx Packets: 0/0

### 3. IP Addressing

- ✓ Next step is to assign IP address and segment for each interface. When you go to “IP > Addresses”, you can see the screen like the following.

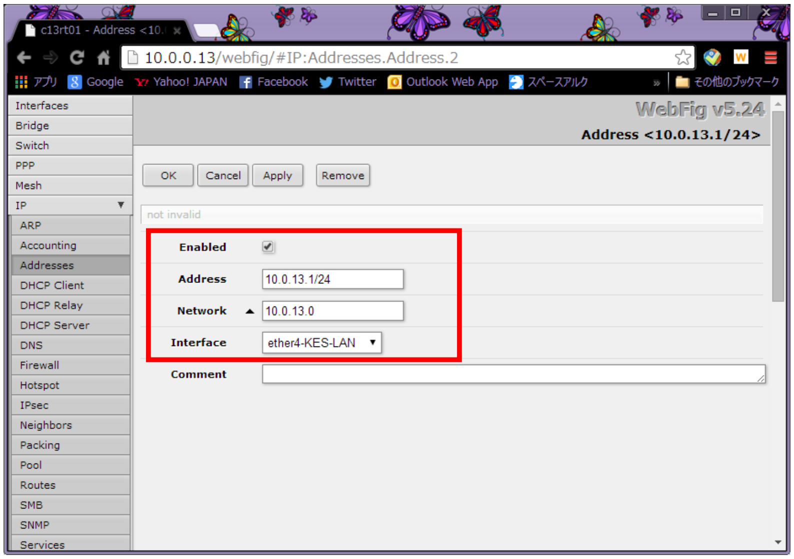


3 items

| | | | ▲ Address | Network | Interface |
|---|---|---|---|---|---|
| - | D | | 10.0.0.13/24 | 10.0.0.0 | ether5-KES-WAN |
| - | D | | 10.0.13.1/24 | 10.0.13.0 | ether4-KES-LAN |
| ;;; default configuration | | | | | |
| - | E | X | *192.168.88.1/24* | *192.168.88.0* | *ether1* |

- ✓ If you want to add new IP address, click "Add New" button. Input the following information, and then click "OK" to apply the address setting:

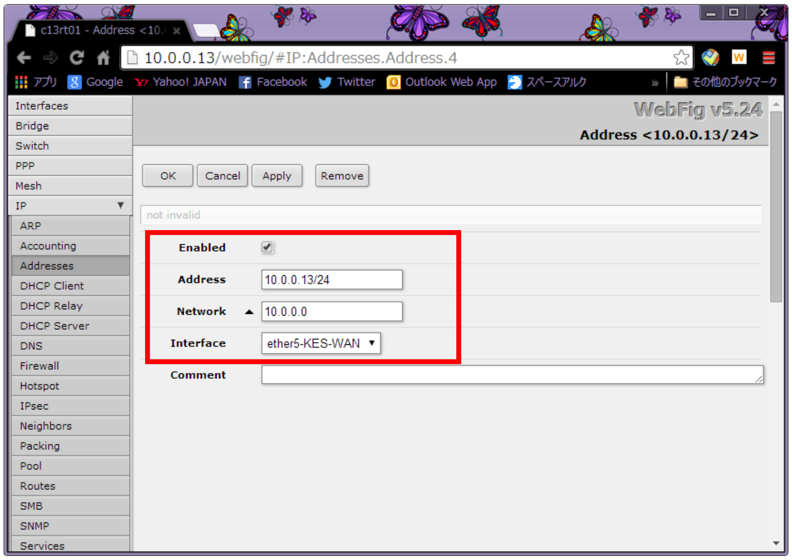
|  |  |  |
|---|---|---|
| (1) | Enabled | checked |
| (2) | Address | Interface Address/Subnet (like 10.0.13.1/24) |
| (3) | Network | Network Address (like 10.0.13.0) |
| (4) | Interface | Assigned Interface (select from pull-down menu) |



10.0.0.13/webfig/#IP:Addresses.Address.2

Address <10.0.13.1/24>

Enabled ☑
Address 10.0.13.1/24
Network ▲ 10.0.13.0
Interface ether4-KES-LAN ▾
Comment



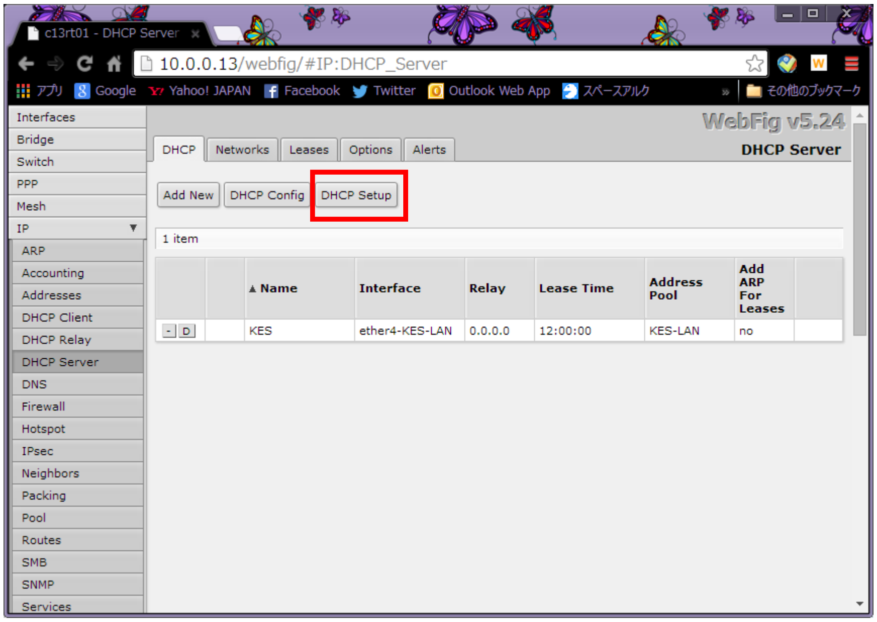
10.0.0.13/webfig/#IP:Addresses.Address.4

Address <10.0.0.13/24>

Enabled ☑
Address 10.0.0.13/24
Network ▲ 10.0.0.0
Interface ether5-KES-WAN ▾
Comment

### 4. DHCP

- ✓ When you go to “IP > DHCP Server”, you can see the DHCP configuration.
- ✓ By clicking “DHCP Setup” button, the setup wizard shows up.

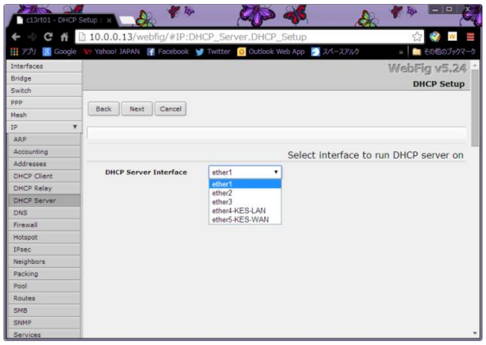


1 item

| | | ▲ Name | Interface | Relay | Lease Time | Address Pool | Add ARP For Leases |
|---|---|---|---|---|---|---|---|
| - D | | KES | ether4-KES-LAN | 0.0.0.0 | 12:00:00 | KES-LAN | no |

- ✓ Setup Wizard has 6 steps.

(1) Assign the interface (and click next)

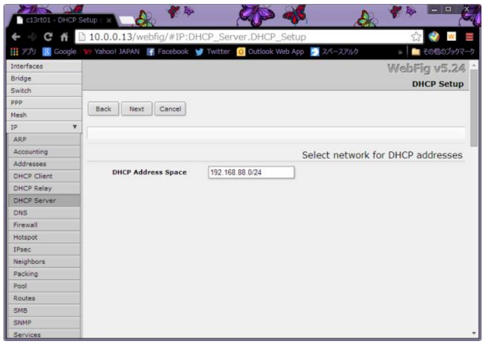


DHCP Setup

Select interface to run DHCP server on

DHCP Server Interface: ether1 (ether1, ether2, ether3, ether4-KES-LAN, ether5-KES-WAN)

(2) Set address space (and click next)

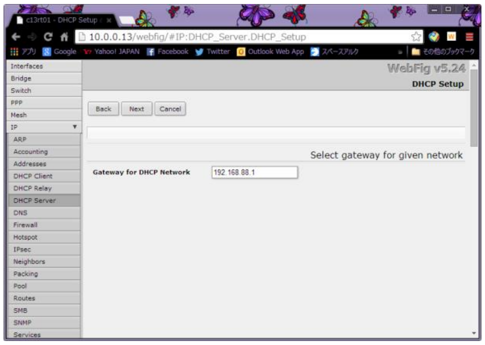


DHCP Setup

Select network for DHCP addresses

DHCP Address Space: 192.168.88.0/24

(3) Assign default gateway (and click next)

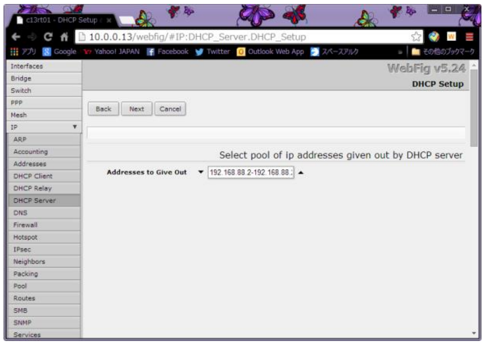


DHCP Setup

Select gateway for given network

Gateway for DHCP Network: 192.168.88.1

(4) Set Address range for DHCP (and click next)

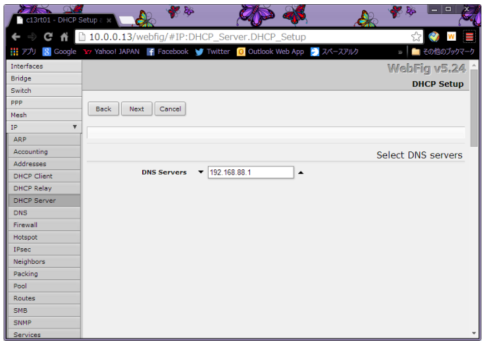


DHCP Setup

Select pool of ip addresses given out by DHCP server

Addresses to Give Out: 192.168.88.2-192.168.88.:

(5) Set DNS address (and click next)

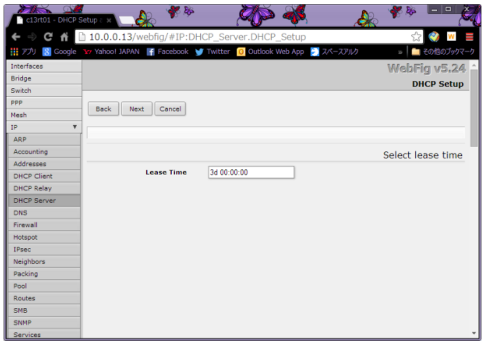


DHCP Setup

Select DNS servers

DNS Servers: 192.168.88.1

(6) Set lease time (and click next: finish)



DHCP Setup

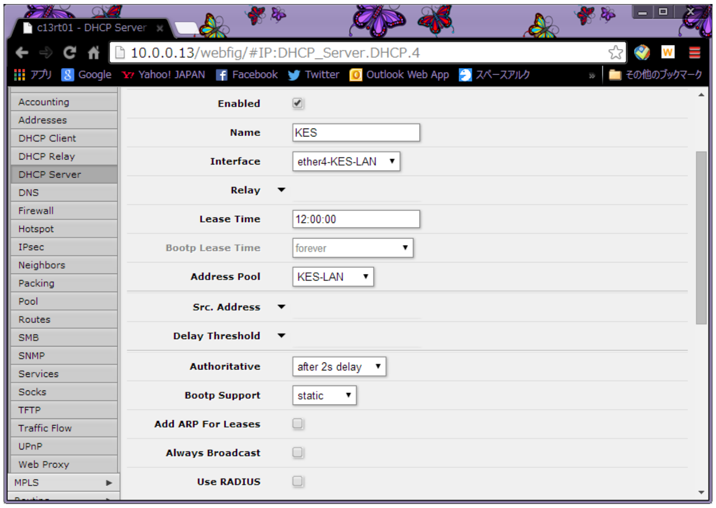
Select lease time

Lease Time: 3d 00:00:00

Last modified: Aug 8, 2014

✓ Sample setting for KES LAN is the following (you can see that on “DHCP” and “Network” tab):

| | | |
|---|---|---|
| (1) | Name | KES |
| (2) | Interface | ether4-KES-LAN (Interface for LAN segment) |
| (3) | Lease Time | Half a day (12:00:00) |
| (4) | Address Pool | KES-LAN (named in “IP > Pool”) |
| (5) | Address | 10.0.13.0/24 |
| (6) | Gateway | 10.0.13.1 |
| (7) | DNS Server | 10.0.0.254 |



c13rt01 - DHCP Server

10.0.0.13/webfig/#IP:DHCP_Server.DHCP.4

Enabled ☑

Name: KES

Interface: ether4-KES-LAN

Relay

Lease Time: 12:00:00

Bootp Lease Time: forever

Address Pool: KES-LAN

Src. Address

Delay Threshold

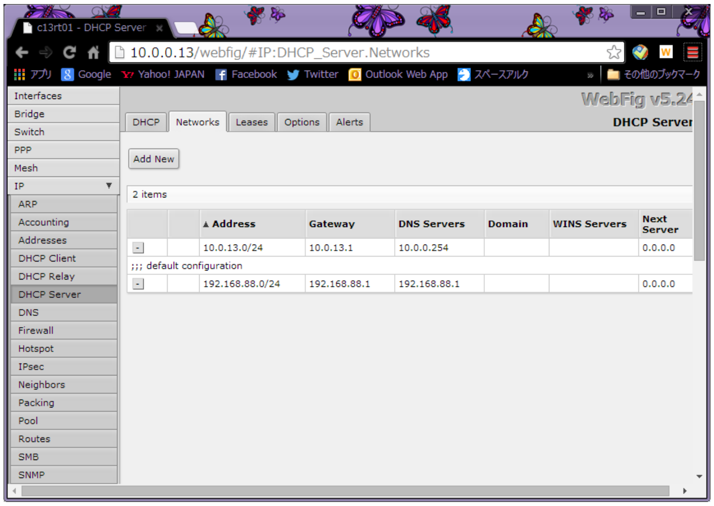
Authoritative: after 2s delay

Bootp Support: static

Add ARP For Leases ☐

Always Broadcast ☐

Use RADIUS ☐



c13rt01 - DHCP Server

10.0.0.13/webfig/#IP:DHCP_Server.Networks

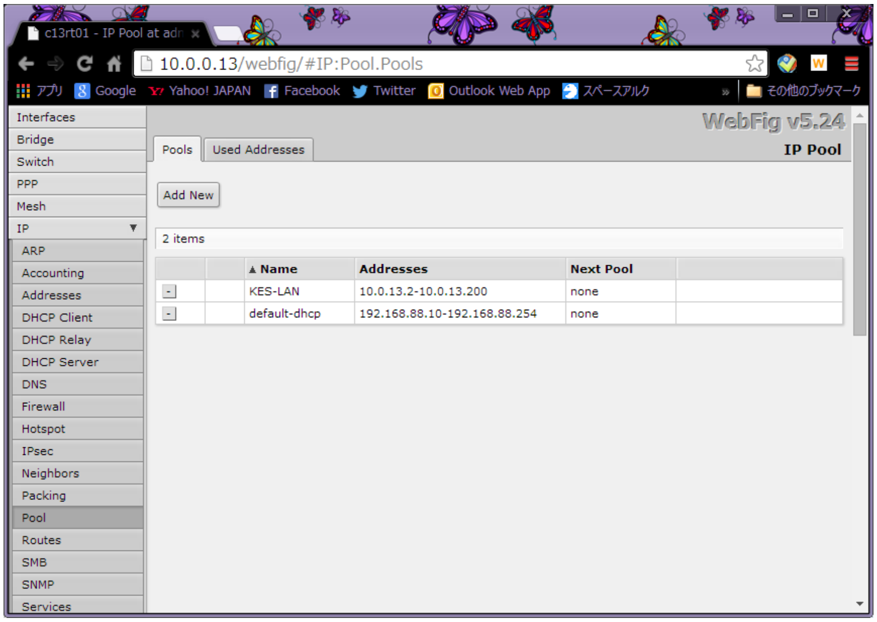
WebFig v5.24

DHCP Server

2 items

| | | ▲ Address | Gateway | DNS Servers | Domain | WINS Servers | Next Server |
|---|---|---|---|---|---|---|---|
| - | | 10.0.13.0/24 | 10.0.13.1 | 10.0.0.254 | | | 0.0.0.0 |
| ;;; default configuration | | | | | | | |
| - | | 192.168.88.0/24 | 192.168.88.1 | 192.168.88.1 | | | 0.0.0.0 |

- ✓ DHCP range can be modified at Pool setting (you can see that when going to “IP > Pool”)
- ✓ In the KES case, the range is 10.0.13.2 - 10.0.13.200 (which is based on the IP addressing policy)

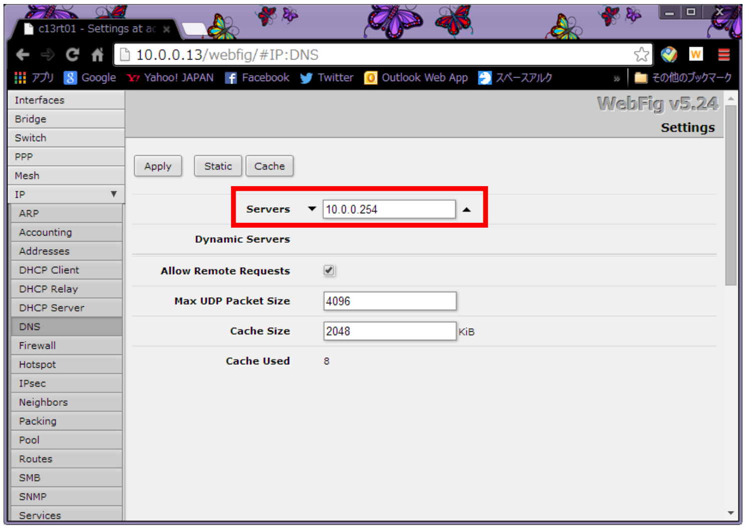


2 items

| | ▲ Name | Addresses | Next Pool |
|---|---|---|---|
| - | KES-LAN | 10.0.13.2-10.0.13.200 | none |
| - | default-dhcp | 192.168.88.10-192.168.88.254 | none |

## 5. DNS

- ✓ When you go to “IP > DNS”, you can apply DNS setting (10.0.0.254. other settings are default).



Servers: 10.0.0.254

Dynamic Servers

Allow Remote Requests: ☑

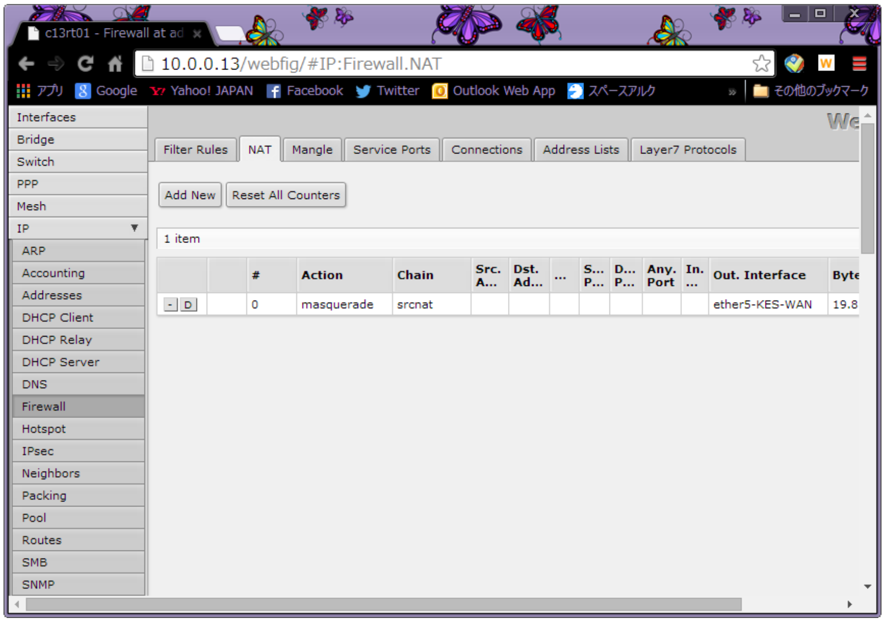
Max UDP Packet Size: 4096

Cache Size: 2048 KiB

Cache Used: 8

**6. NAT**

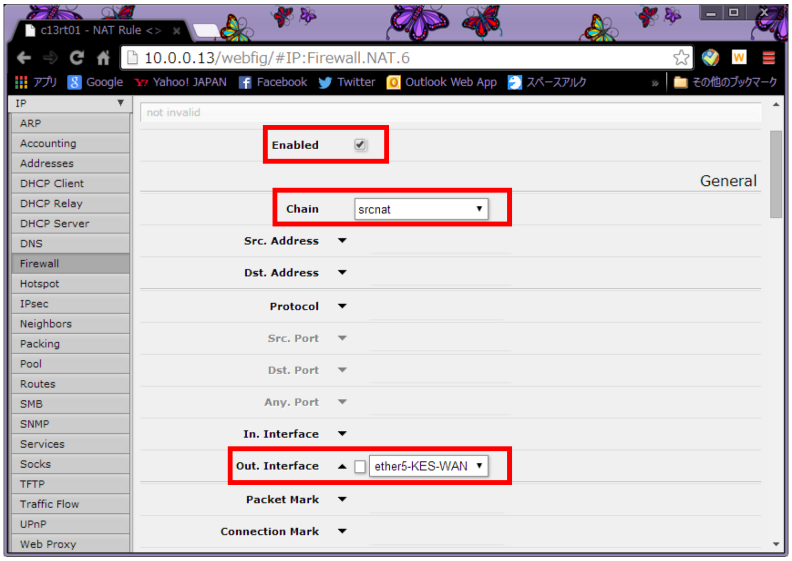
- ✓ We need to apply source-NAT (masquerade) setting for outbound transaction on WAN interface in order to communicate the hosts in MOE WAN segment from the hosts under the router.
- ✓ When you go to “IP > Firewall > NAT (tab)”, you can see the current status of NAT setting.



| | | # | Action | Chain | Src. A... | Dst. Ad... | ... | S... P... | D... P... | Any. Port | In. ... | Out. Interface | Byte |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - D | | 0 | masquerade | srcnat | | | | | | | | ether5-KES-WAN | 19.8 |

✓ The rule is simple so that you only set 4 items for NAT setting:

| | | |
|---|---|---|
| (1) | Enabled | Checked |
| (2) | Chain | srcnat (source address NAT) |
| (3) | Out. Interface | ether5-KES-WAN |
| (4) | Action | masquerade |



Enabled ☑

General

Chain srcnat

Src. Address

Dst. Address

Protocol

Src. Port

Dst. Port

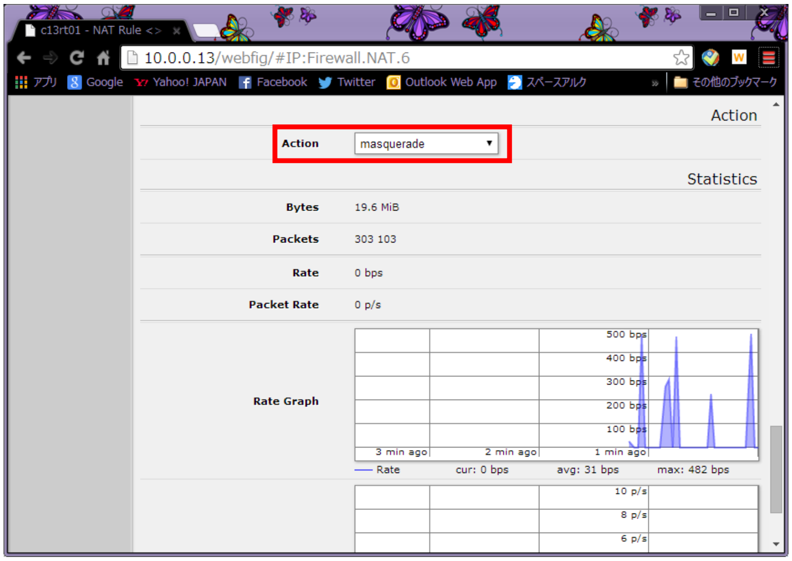
Any. Port

In. Interface

Out. Interface □ ether5-KES-WAN

Packet Mark

Connection Mark



Action

Action masquerade

Statistics

Bytes 19.6 MiB

Packets 303 103

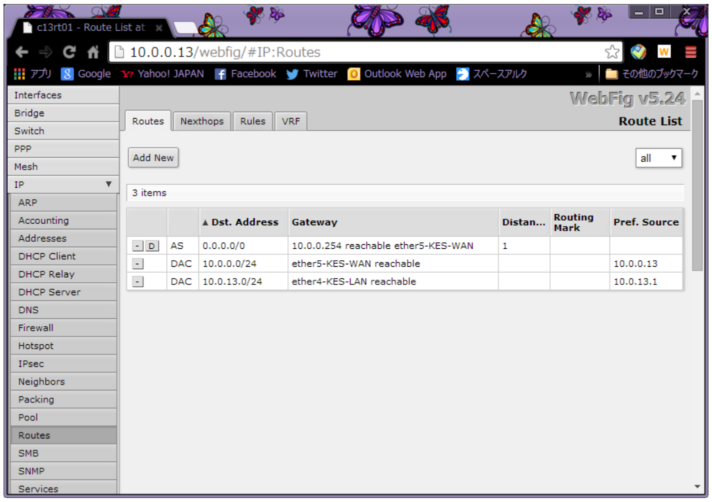
Rate 0 bps

Packet Rate 0 p/s

Rate Graph

## 7. Default Route

- ✓ All transactions (except for the segments under the route) should go to the default gateway of MOE WAN segment (10.0.0.254). Thus, the static default route setting is required.
- ✓ When you go to "IP > Routes", you can see the current route information. By clicking "Add New", you can add new static route setting.



Route List

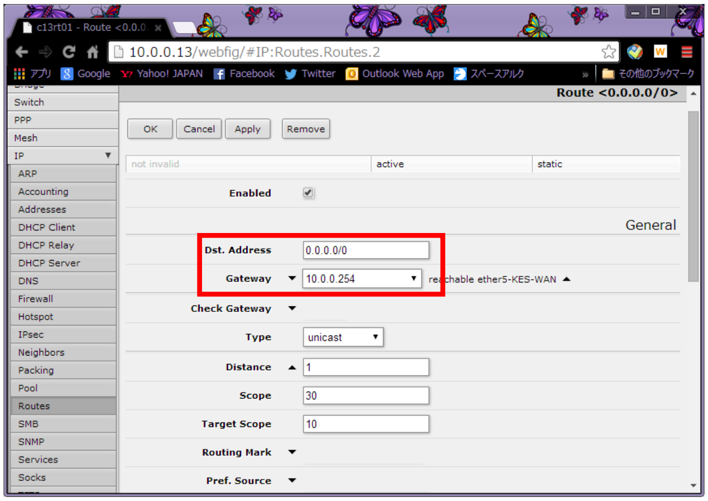
3 items

| | | ▲ Dst. Address | Gateway | Distan... | Routing Mark | Pref. Source |
|---|---|---|---|---|---|---|
| - D | AS | 0.0.0.0/0 | 10.0.0.254 reachable ether5-KES-WAN | 1 | | |
| - | DAC | 10.0.0.0/24 | ether5-KES-WAN reachable | | | 10.0.0.13 |
| - | DAC | 10.0.13.0/24 | ether4-KES-LAN reachable | | | 10.0.13.1 |

- ✓ You input the two following information:

(1) Dst. Address 0.0.0.0/0 (default route)

(2) Gateway 10.0.0.254 (default gateway address of MOE WAN segment)



Route <0.0.0.0/0>

not invalid | active | static

Enabled ☑

Dst. Address: 0.0.0.0/0

Gateway: 10.0.0.254 reachable ether5-KES-WAN

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

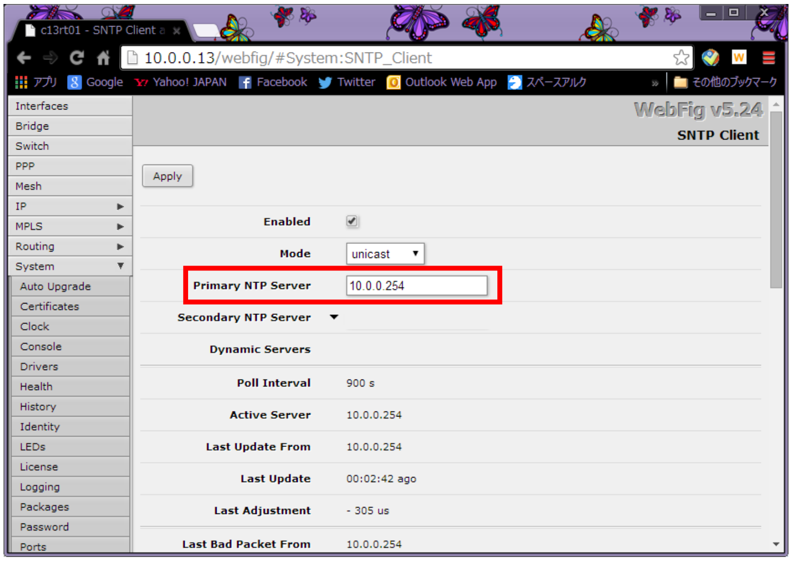
Target Scope: 10

Routing Mark:

Pref. Source:

### 8. Clock

- ✓ After going to "System > SNTP Client", you can see the NTP client setting.
- ✓ Just input the NTP address (10.0.0.254) in MOE network and click "Apply".



Enabled ☑

Mode unicast

Primary NTP Server 10.0.0.254

Secondary NTP Server

Dynamic Servers

Poll Interval 900 s

Active Server 10.0.0.254

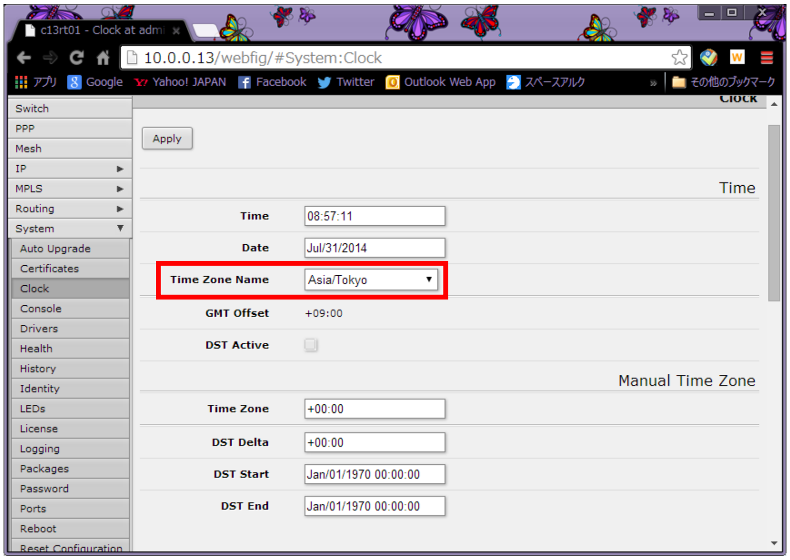
Last Update From 10.0.0.254

Last Update 00:02:42 ago

Last Adjustment - 305 us

Last Bad Packet From 10.0.0.254

- ✓ You also need to set a right time zone. After going to "System > Clock", you select the time zone name from pull-down menu ("Asia/Tokyo" is a same time zone as Palau).
- ✓ Check whether the router can receive the correct time from NTP server via network.



Time

Time 08:57:11

Date Jul/31/2014

Time Zone Name Asia/Tokyo

GMT Offset +09:00

DST Active □

Manual Time Zone

Time Zone +00:00

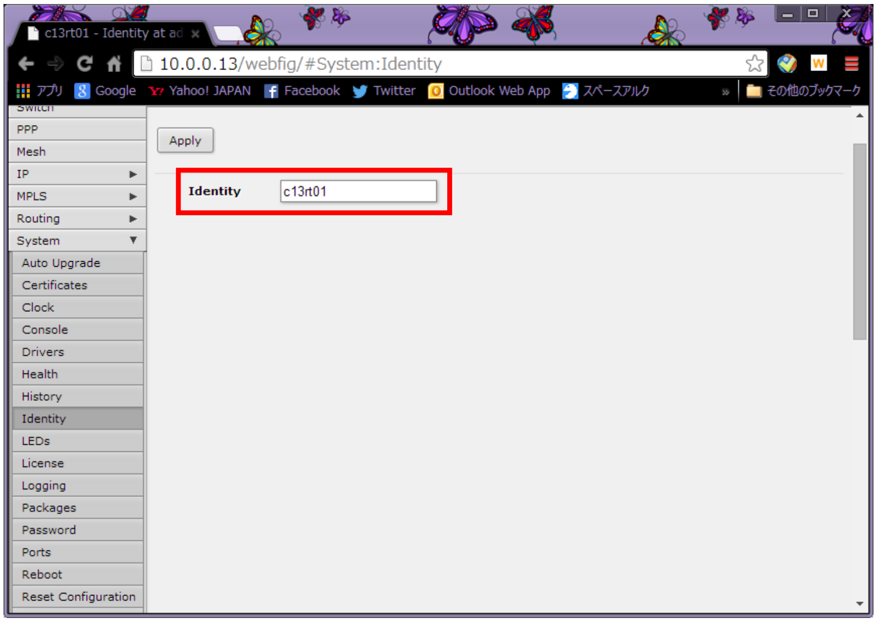
DST Delta +00:00

DST Start Jan/01/1970 00:00:00

DST End Jan/01/1970 00:00:00

### 9. Hostname

✓ After going to “System > Identity”, you can input the hostname (in KES case, “c13rt01”).

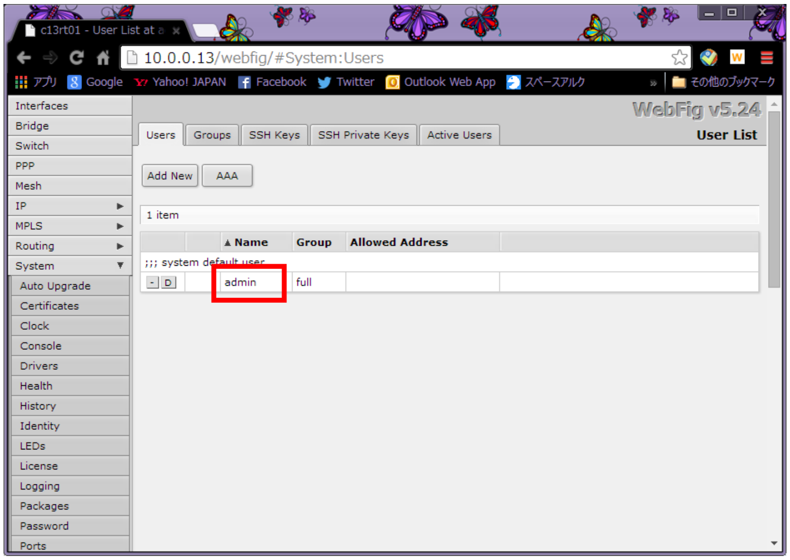


10.0.0.13/webfig/#System:Identity

Identity c13rt01

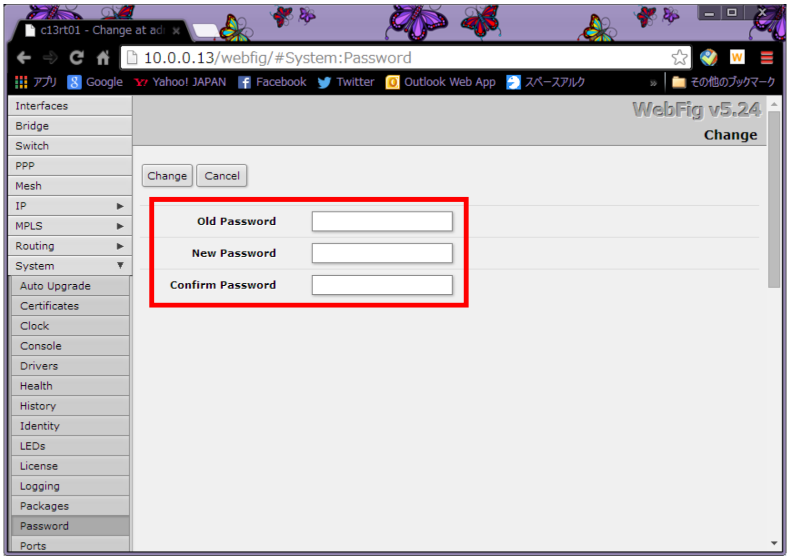
### 10. User and Password

- ✓ User ID (and role) is defined on "User List" (go to "System > Users"). The setting of Admin is default so that you do not need to change the setting.



|  | ▲ Name | Group | Allowed Address |
|---|---|---|---|
| ;;; system default user |  |  |  |
| - D | admin | full |  |

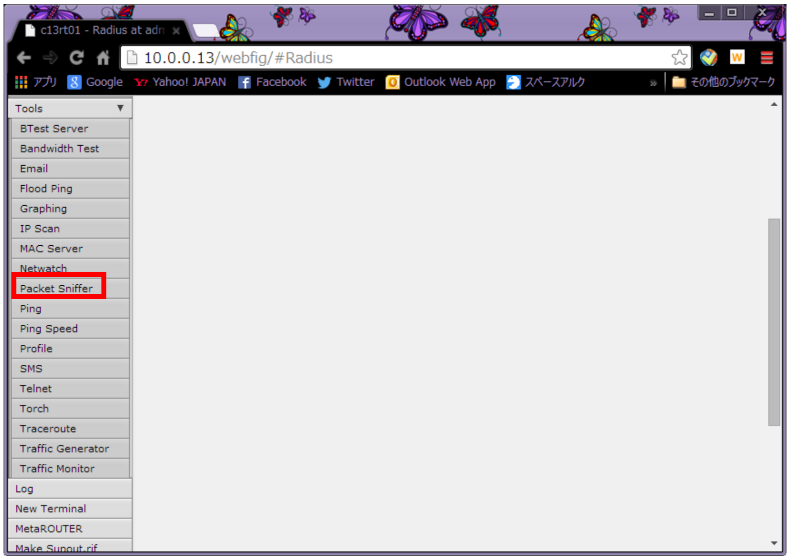
- ✓ When you logged in the router as Admin, you can change the password setting of the user via "System > Password". You input old and new passwords into the box, and click "Change". (there is no-password as default setting)



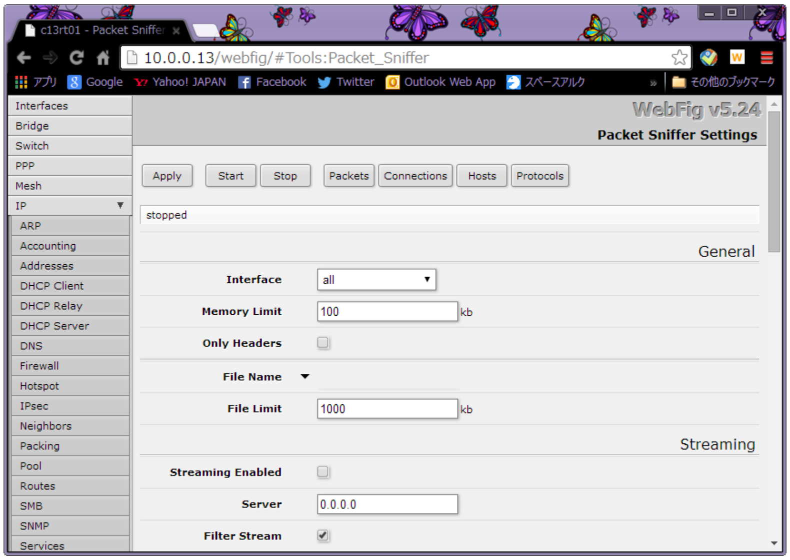
Old Password
New Password
Confirm Password

### 11. Tools

- ✓ RouterOS provides some network tools. When you go to “Tools”, you can find the lineup of tools.
- ✓ In addition to some basic tools like “Ping” and “Traceroute”, “Packet Sniffer” is a powerful tool when troubleshooting.



- ✓ You can capture the packets as you like (by filtering) and analyze the transactions in detail.



Packet Sniffer Settings

stopped

General

Interface: all

Memory Limit: 100 kb

Only Headers: □

File Name

File Limit: 1000 kb

Streaming

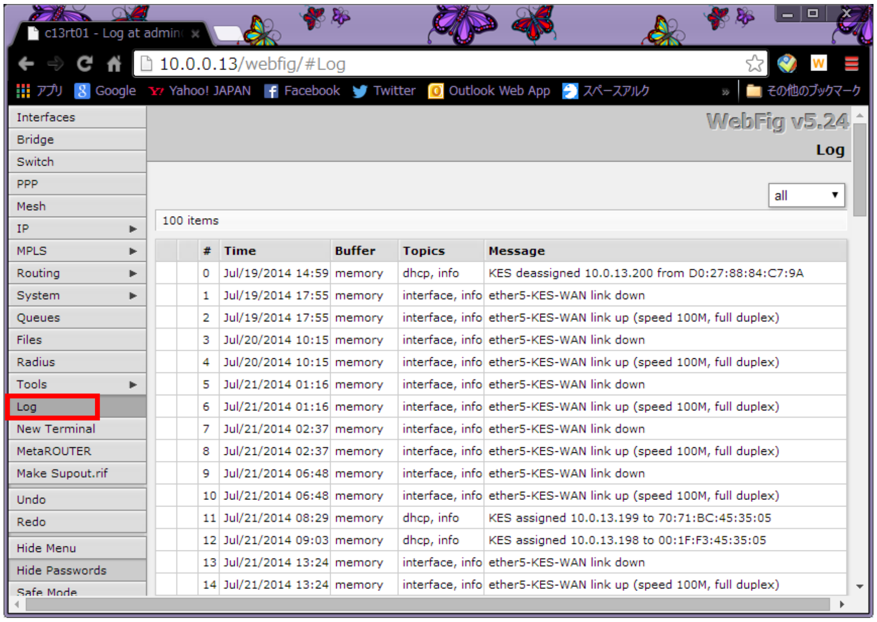
Streaming Enabled: □

Server: 0.0.0.0

Filter Stream: ☑

### 12. Log

✓ System log is also important information for IT operation. You can see the log information when going to “Log”.

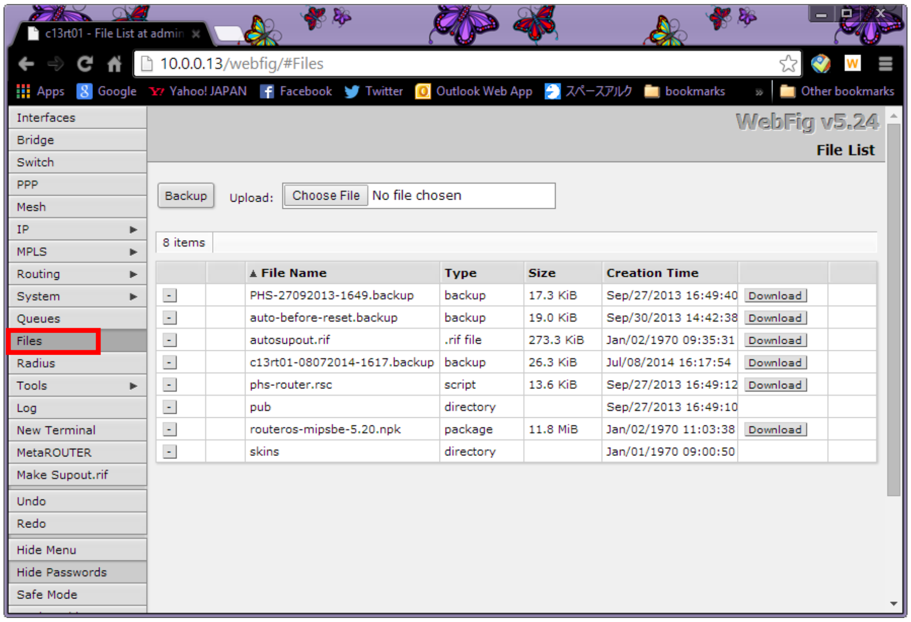


100 items

| # | Time | Buffer | Topics | Message |
|---|---|---|---|---|
| 0 | Jul/19/2014 14:59 | memory | dhcp, info | KES deassigned 10.0.13.200 from D0:27:88:84:C7:9A |
| 1 | Jul/19/2014 17:55 | memory | interface, info | ether5-KES-WAN link down |
| 2 | Jul/19/2014 17:55 | memory | interface, info | ether5-KES-WAN link up (speed 100M, full duplex) |
| 3 | Jul/20/2014 10:15 | memory | interface, info | ether5-KES-WAN link down |
| 4 | Jul/20/2014 10:15 | memory | interface, info | ether5-KES-WAN link up (speed 100M, full duplex) |
| 5 | Jul/21/2014 01:16 | memory | interface, info | ether5-KES-WAN link down |
| 6 | Jul/21/2014 01:16 | memory | interface, info | ether5-KES-WAN link up (speed 100M, full duplex) |
| 7 | Jul/21/2014 02:37 | memory | interface, info | ether5-KES-WAN link down |
| 8 | Jul/21/2014 02:37 | memory | interface, info | ether5-KES-WAN link up (speed 100M, full duplex) |
| 9 | Jul/21/2014 06:48 | memory | interface, info | ether5-KES-WAN link down |
| 10 | Jul/21/2014 06:48 | memory | interface, info | ether5-KES-WAN link up (speed 100M, full duplex) |
| 11 | Jul/21/2014 08:29 | memory | dhcp, info | KES assigned 10.0.13.199 to 70:71:BC:45:35:05 |
| 12 | Jul/21/2014 09:03 | memory | dhcp, info | KES assigned 10.0.13.198 to 00:1F:F3:45:35:05 |
| 13 | Jul/21/2014 13:24 | memory | interface, info | ether5-KES-WAN link down |
| 14 | Jul/21/2014 13:24 | memory | interface, info | ether5-KES-WAN link up (speed 100M, full duplex) |

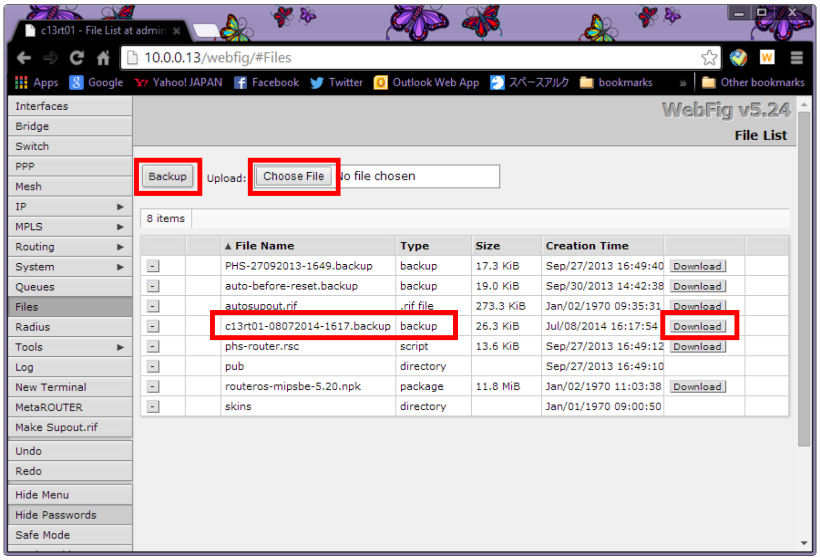
### 13. Configuration File (Backup and Restore)

- ✓ RouterOS provides a file explorer function. You can store the backup of configuration file and download it onto your computer. Also you can upload the other configuration files from your computer and restore the route from the configuration file.
- ✓ When you go to “File” menu, you can see the list of files which the router has.



|  |  | ▲ File Name | Type | Size | Creation Time |  |  |
|---|---|---|---|---|---|---|---|
| - |  | PHS-27092013-1649.backup | backup | 17.3 KiB | Sep/27/2013 16:49:40 | Download |  |
| - |  | auto-before-reset.backup | backup | 19.0 KiB | Sep/30/2013 14:42:38 | Download |  |
| - |  | autosupout.rif | .rif file | 273.3 KiB | Jan/02/1970 09:35:31 | Download |  |
| - |  | c13rt01-08072014-1617.backup | backup | 26.3 KiB | Jul/08/2014 16:17:54 | Download |  |
| - |  | phs-router.rsc | script | 13.6 KiB | Sep/27/2013 16:49:12 | Download |  |
| - |  | pub | directory |  | Sep/27/2013 16:49:10 |  |  |
| - |  | routeros-mipsbe-5.20.npk | package | 11.8 MiB | Jan/02/1970 11:03:38 | Download |  |
| - |  | skins | directory |  | Jan/01/1970 09:00:50 |  |  |

- ✓ In order to keep a backup file of configuration, just click “Backup” button on the top. The backup file named “hostname-date-time.backup” is automatically stored on the router.
- ✓ When clicking “Download”, you can download the file into your computer.



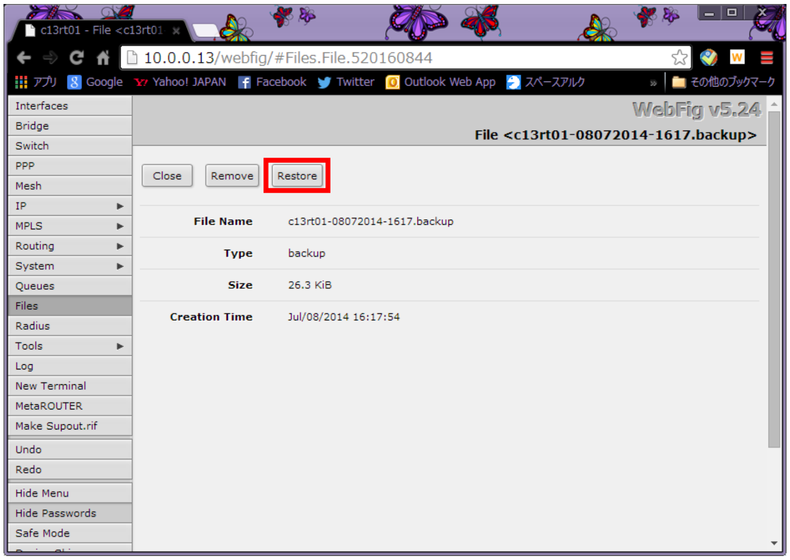
File List

No file chosen

8 items

| | | ▲ File Name | Type | Size | Creation Time | | |
|---|---|---|---|---|---|---|---|
| - | | PHS-27092013-1649.backup | backup | 17.3 KiB | Sep/27/2013 16:49:40 | Download | |
| - | | auto-before-reset.backup | backup | 19.0 KiB | Sep/30/2013 14:42:38 | Download | |
| - | | autosupout.rif | .rif file | 273.3 KiB | Jan/02/1970 09:35:31 | Download | |
| - | | c13rt01-08072014-1617.backup | backup | 26.3 KiB | Jul/08/2014 16:17:54 | Download | |
| - | | phs-router.rsc | script | 13.6 KiB | Sep/27/2013 16:49:12 | Download | |
| - | | pub | directory | | Sep/27/2013 16:49:10 | | |
| - | | routeros-mipsbe-5.20.npk | package | 11.8 MiB | Jan/02/1970 11:03:38 | Download | |
| - | | skins | directory | | Jan/01/1970 09:00:50 | | |

- ✓ By clicking the “Choose File” button, you can upload a file from your computer onto the router.
- ✓ After uploading the file, by clicking the filename on the list, you can see profile of the file.
- ✓ Finally, clicking “Restore” button on the top, you can restore the router from the backup file.



File <c13rt01-08072014-1617.backup>

File Name c13rt01-08072014-1617.backup

Type backup

Size 26.3 KiB

Creation Time Jul/08/2014 16:17:54

# Appendix P

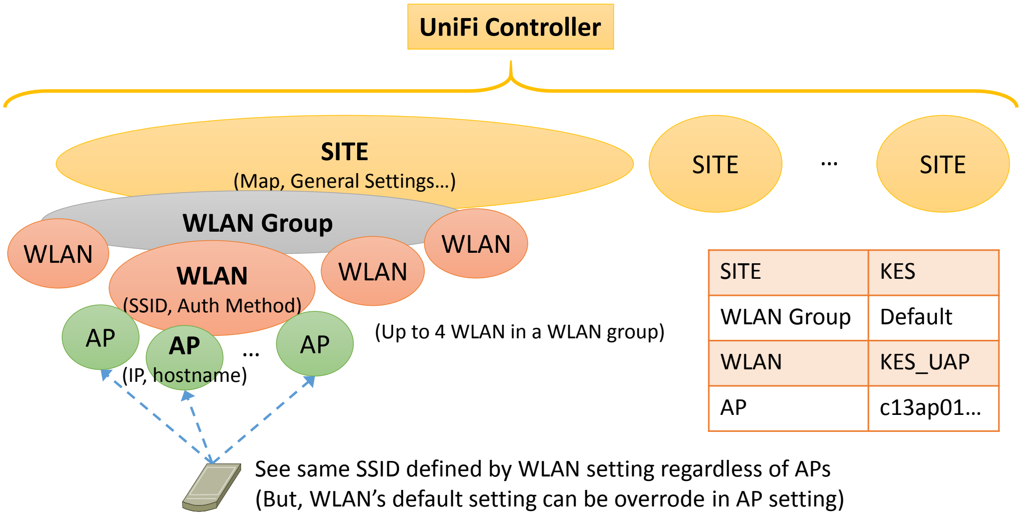
## Configuration Guide for UAP-AP (by UniFi Controller)

This is a configuration guide for "Ubiquiti UAP-AP" access points by using "UniFi Controller (v3.2.1)". The settings and instructions are based on the setting for Koror Elementary School as of Aug 8, 2014. Thus, if you apply the configuration into the other site's access points, you should check whether the setting is based on up-to-date network design and configuration which MOE IT requires.

**INDEX**

**[Managing Structure of UniFi Controller]**

Unifi Controller manage its wireless network setting as the following image.



| | |
|---|---|
| SITE | KES |
| WLAN Group | Default |
| WLAN | KES_UAP |
| AP | c13ap01… |

See same SSID defined by WLAN setting regardless of APs
(But, WLAN's default setting can be overrode in AP setting)

**[Attention]**

For initial setup of access point, the AP should belong to DHCP enabled network, and PC with UniFi Controller should be in the same L2 network of the AP. Thus, when you set up the APs in different network from target network (like Lab environment), you should follow the steps below.

(1) Connect new AP to DHCP enabled network (AP receives new IP address from DHCP server)
(2) Connect PC with UniFi to the same network and find the AP [Guide #5]
(3) Disconnect “switch” from router (AP and PC are still in same L2 network)
(4) Change IP address of the AP to new (correct) address [Guide #6]
(After this change, UniFi cannot see the AP once)
(5) Change IP address of PC to same segment of new IP address of the AP
(6) Find the AP on UniFi [Guide #5]
(7) Move to the AP to designated “site” on UniFi [Guide #7]

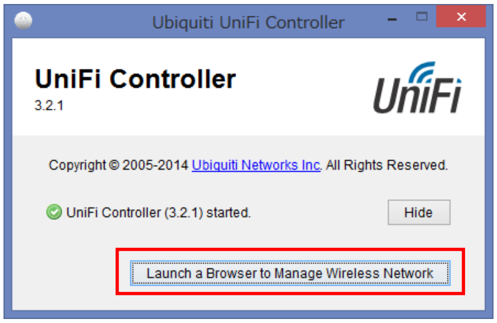
*Fining new APs and transition of status (like Adopting, Provisioning, and Connected) on UniFi Controller sometimes take a time (over a few minutes). So you should assume time for such transition and keep refresh the screen of UniFi.

**[Reset the device]**

Push the reset button next to LAN port more than 5 seconds.
*When push and release quickly, the device will restart (not reset).

## 1. Set up UniFi Controller (only first time to login UniFi)

- When you start the application, the following window shows up. Click "Launch a Browse…" button.



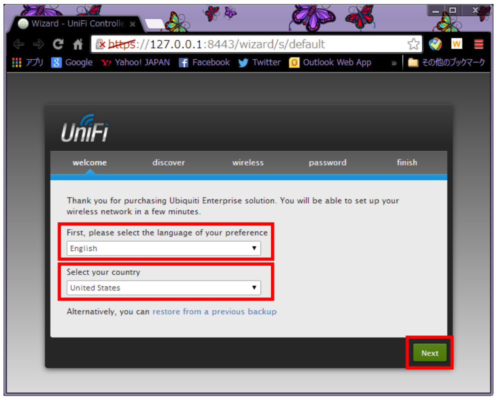
Ubiquiti UniFi Controller
UniFi Controller
3.2.1
UniFi

Copyright © 2005-2014 Ubiquiti Networks Inc. All Rights Reserved.

UniFi Controller (3.2.1) started.

Hide
Launch a Browser to Manage Wireless Network

- Your browser has automatically launched. And ask your language and country. Unfortunately, "Palau" does not show up so that choose "United States" to proceed.



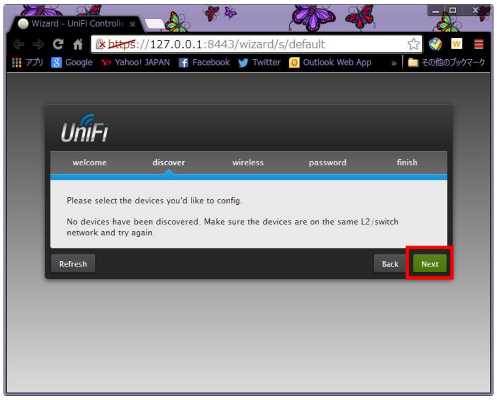
Thank you for purchasing Ubiquiti Enterprise solution. You will be able to set up your wireless network in a few minutes.

First, please select the language of your preference: English

Select your country: United States

Alternatively, you can restore from a previous backup

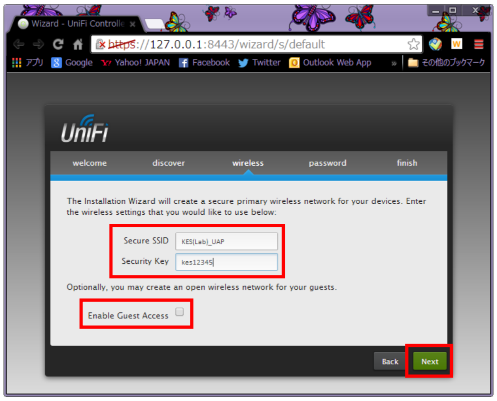
- After connecting access point (AP) to the same Layer 2 network as your computer, UniFi discover the AP from the network and shows the information on the window. If not the following screen shows up. This time, you don't need to care about AP's existence. Just select "Next".



Please select the devices you'd like to config.

No devices have been discovered. Make sure the devices are on the same L2/switch network and try again.

- Enter the SSID and Secure Key of the network (this setting could be changed later so currently do not so much care about the values). Then, click “Next”.



The Installation Wizard will create a secure primary wireless network for your devices. Enter the wireless settings that you would like to use below:

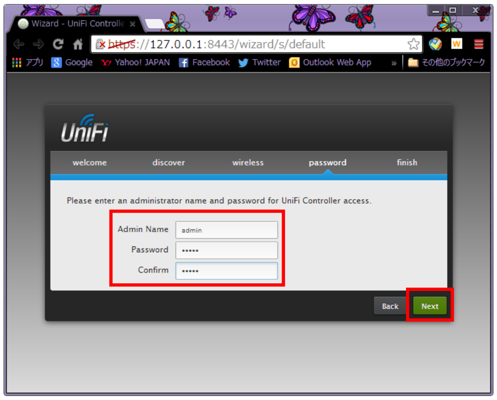
Secure SSID KES(Lab)_UAP

Security Key kes12345

Optionally, you may create an open wireless network for your guests.

Enable Guest Access □

- Set ID and Password for your UniFi Application (it will be used when you login to UniFi, not configure APs). Then, click “Next”.



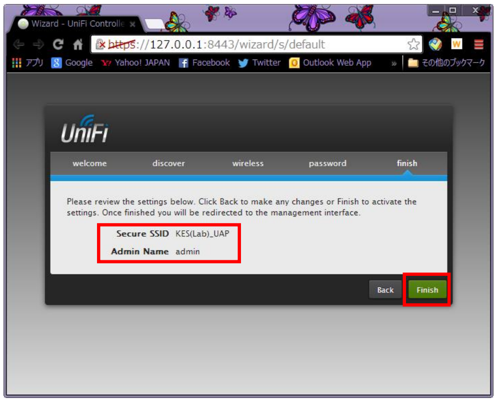
Please enter an administrator name and password for UniFi Controller access.

Admin Name admin

Password •••••

Confirm •••••

- Finally, confirm the setting which UniFi shows, and then, click “Finish”.



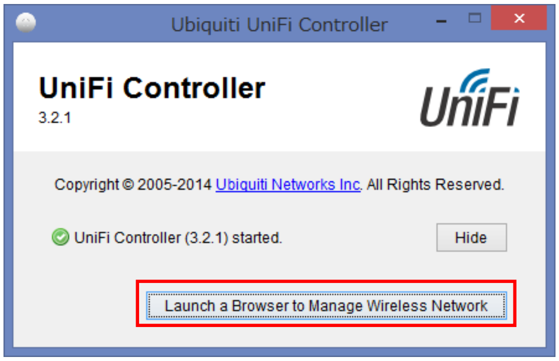
Please review the settings below. Click Back to make any changes or Finish to activate the settings. Once finished you will be redirected to the management interface.

**Secure SSID** KES(Lab)_UAP

**Admin Name** admin

**2. Login to UniFi Controller**

- When you start UniFi Controller, the following window shows up. Click "Launch a Browser…"



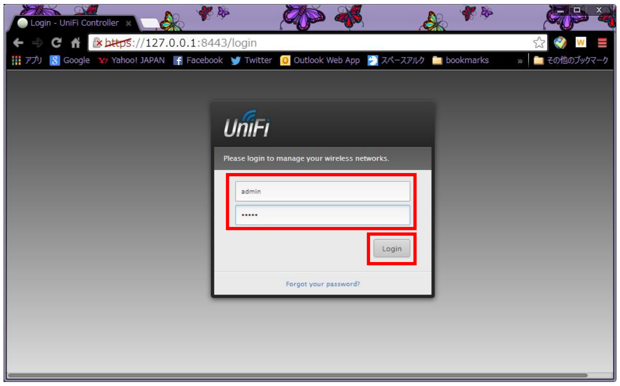
Ubiquiti UniFi Controller

UniFi Controller
3.2.1

Copyright © 2005-2014 Ubiquiti Networks Inc. All Rights Reserved.

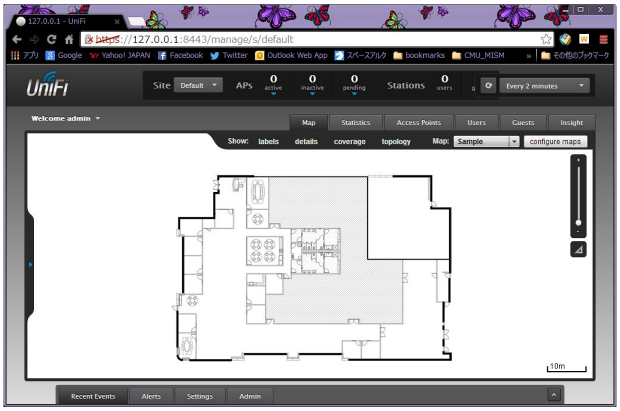
UniFi Controller (3.2.1) started.

- On your browser, the login window appears. Enter ID and Password you set, and click "Login".



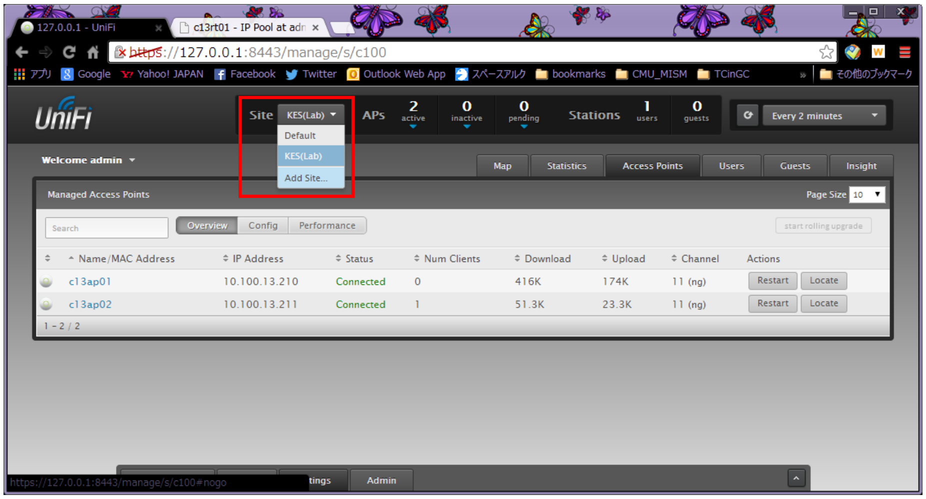
Please login to manage your wireless networks.

- Now, you logged in UniFi Controller.



### 3. Create new “Site”

- UniFi can manage multiple set of configuration for each location which AP placed. In MOE case, it is better to create “Site” setting for each school.
- First, click the pull-down menu of “Site”, choose “Add site…”

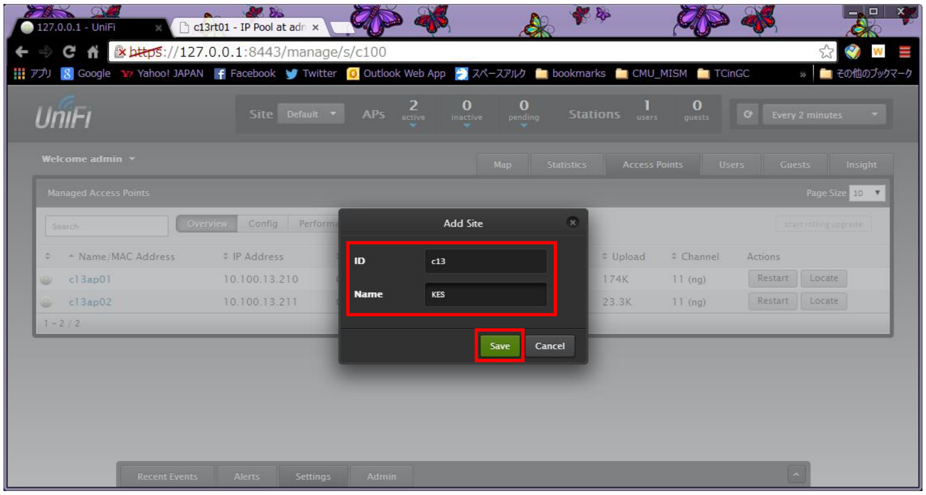


Managed Access Points

| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| c13ap01 | 10.100.13.210 | Connected | 0 | 416K | 174K | 11 (ng) | Restart Locate |
| c13ap02 | 10.100.13.211 | Connected | 1 | 51.3K | 23.3K | 11 (ng) | Restart Locate |

1 - 2 / 2

- Then, enter ID and Name of new site. ID is a location code of the school (cnn) and Name is a shorten name of the school in this case. Then, click “Save”.

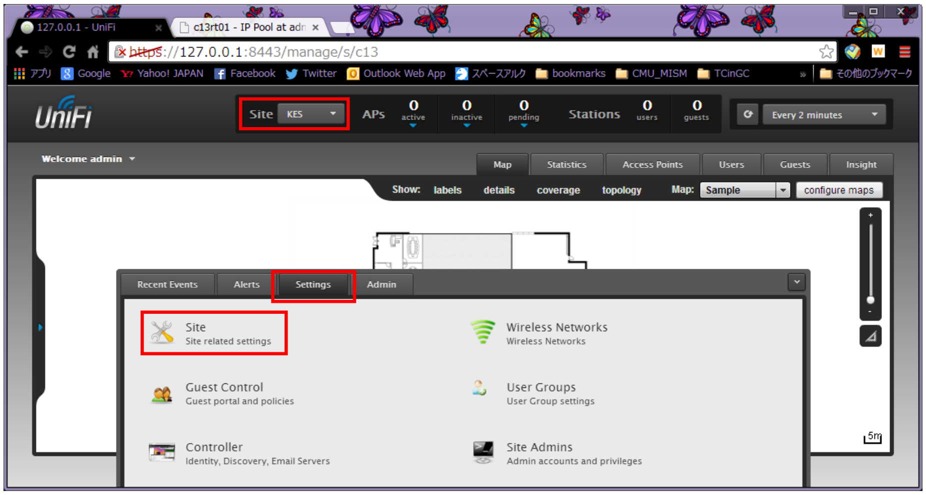


Add Site

ID: c13

Name: KES

- To go to the site setting, choose the site name which you want to configure from Site menu at top of the window. And click the “Settings” at bottom of the window.
- Setting menu shows up. Click “Site” to enter site settings.


127.0.0.1 - UniFi
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c13
アプリ Google Yahoo! JAPAN Facebook Twitter Outlook Web App スペースアルク bookmarks CMU_MISM TCinGC その他のブックマーク
UniFi
Site KES
APs 0 active 0 inactive 0 pending
Stations 0 users 0 guests
Every 2 minutes
Welcome admin
Map
Statistics
Access Points
Users
Guests
Insight
Show: labels details coverage topology
Map: Sample
configure maps
Recent Events
Alerts
Settings
Admin
5m

Site
Site related settings

Wireless Networks
Wireless Networks

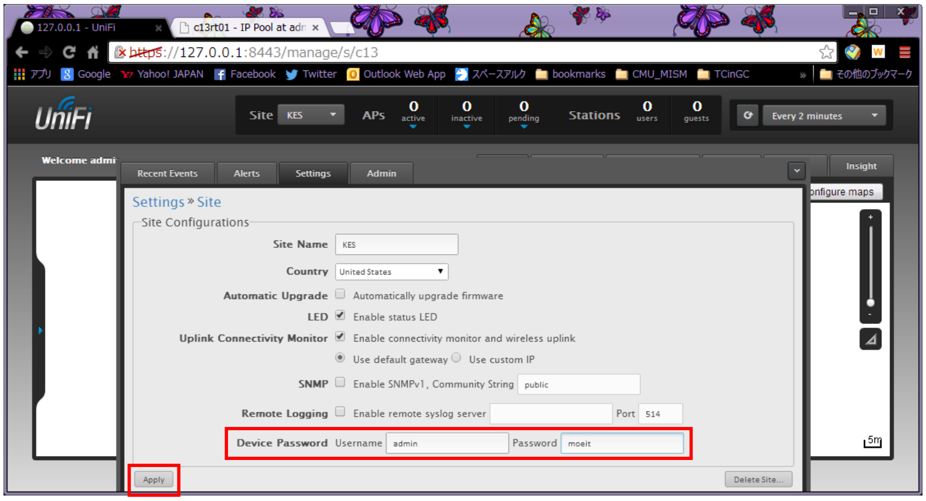
Guest Control
Guest portal and policies

User Groups
User Group settings

Controller
Identity, Discovery, Email Servers

Site Admins
Admin accounts and privileges

- Enter the password for device. Username is “admin and set the designated password (moeit). The other settings are default. Then, click “Apply” to finish the settings.


127.0.0.1 - UniFi
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c13
アプリ Google Yahoo! JAPAN Facebook Twitter Outlook Web App スペースアルク bookmarks CMU_MISM TCinGC その他のブックマーク
UniFi
Site KES
APs 0 active 0 inactive 0 pending
Stations 0 users 0 guests
Every 2 minutes
Welcome admi
Recent Events
Alerts
Settings
Admin
Insight
onfigure maps
5m

Settings » Site

Site Configurations

Site Name: KES

Country: United States

Automatic Upgrade: □ Automatically upgrade firmware

LED: ☑ Enable status LED

Uplink Connectivity Monitor: ☑ Enable connectivity monitor and wireless uplink

● Use default gateway ○ Use custom IP

SNMP: □ Enable SNMPv1, Community String: public

Remote Logging: □ Enable remote syslog server Port: 514

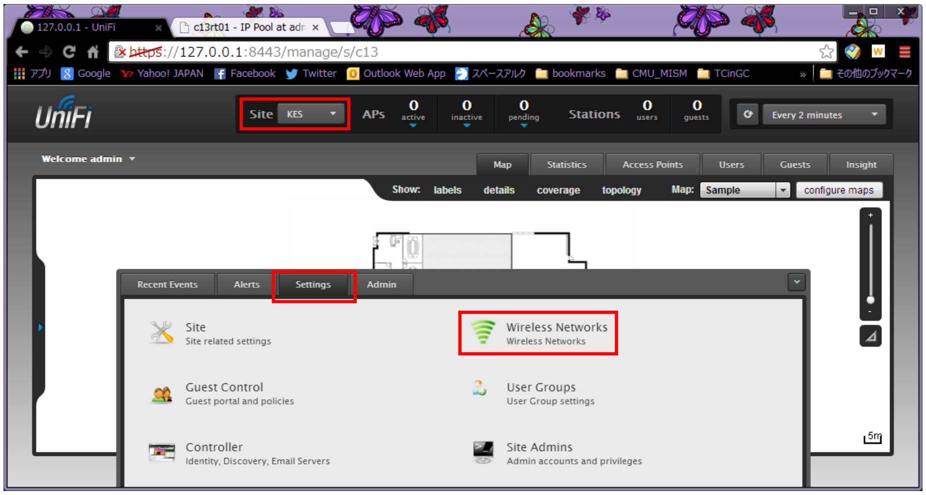
Device Password: Username: admin Password: moeit

Apply

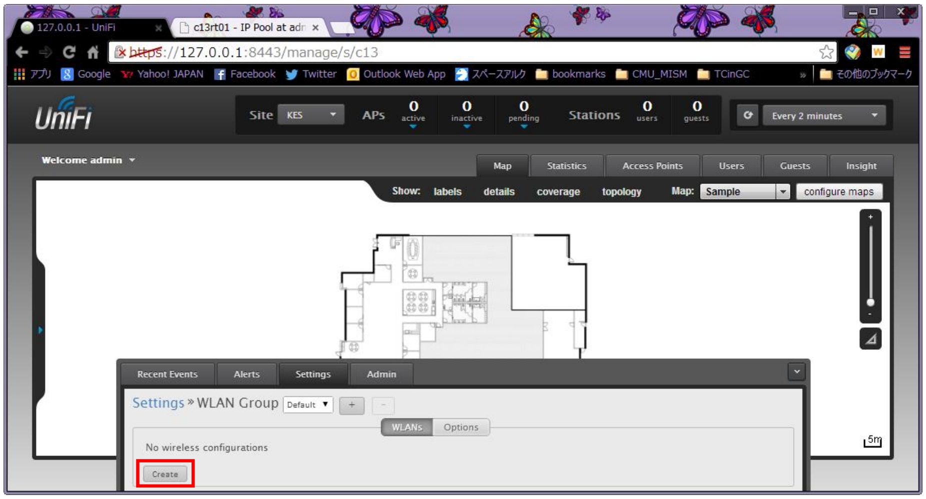
Delete Site...

### 4. Set up wireless LAN (WLAN)

- Make sure the proper site name shows, click settings and “Wireless Networks”.



- Currently, there is no wireless network setting. So, click “Create” button to set up the network.



- Enter the detail settings of the wireless LAN.

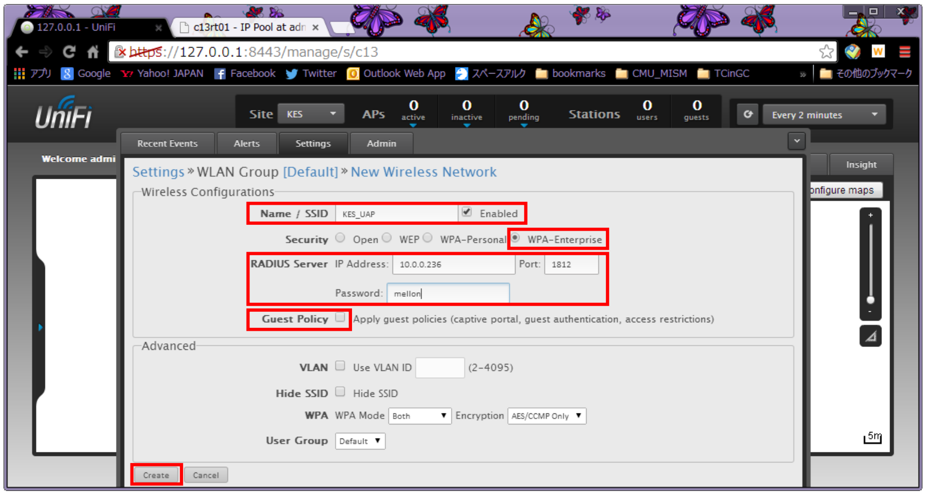
(1) Name / SSID XXX_UAP (XXX is shorten school name, like KES_UAP)
check ON for “Enabled”

(2) Security WPA-Enterprise

(3) RADIUS Server IP address 10.0.0.236
Port 1812 (default)
Password mellon

(4) Guest Policy check OFF

- Then click OK to finish the setting.


127.0.0.1 - UniFi
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c13
アプリ Google Yahoo! JAPAN Facebook Twitter Outlook Web App スペースアルク bookmarks CMU_MISM TCinGC その他のブックマーク
UniFi
Site KES
APs 0 active 0 inactive 0 pending
Stations 0 users 0 guests
Every 2 minutes
Welcome admi
Recent Events
Alerts
Settings
Admin
Insight
onfigure maps
5m
Create
Cancel

Settings » WLAN Group [Default] » New Wireless Network

Wireless Configurations

Name / SSID KES_UAP ☑ Enabled

Security ○ Open ○ WEP ○ WPA-Personal ● WPA-Enterprise

RADIUS Server IP Address: 10.0.0.236 Port: 1812

Password: mellon

Guest Policy □ Apply guest policies (captive portal, guest authentication, access restrictions)

Advanced

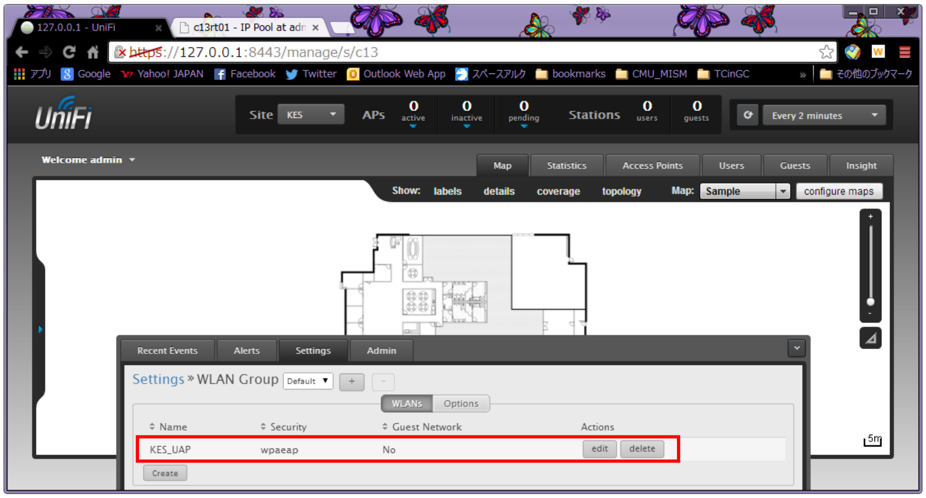
VLAN □ Use VLAN ID (2-4095)

Hide SSID □ Hide SSID

WPA WPA Mode Both Encryption AES/CCMP Only

User Group Default

- The new wireless network shows up the settings window.

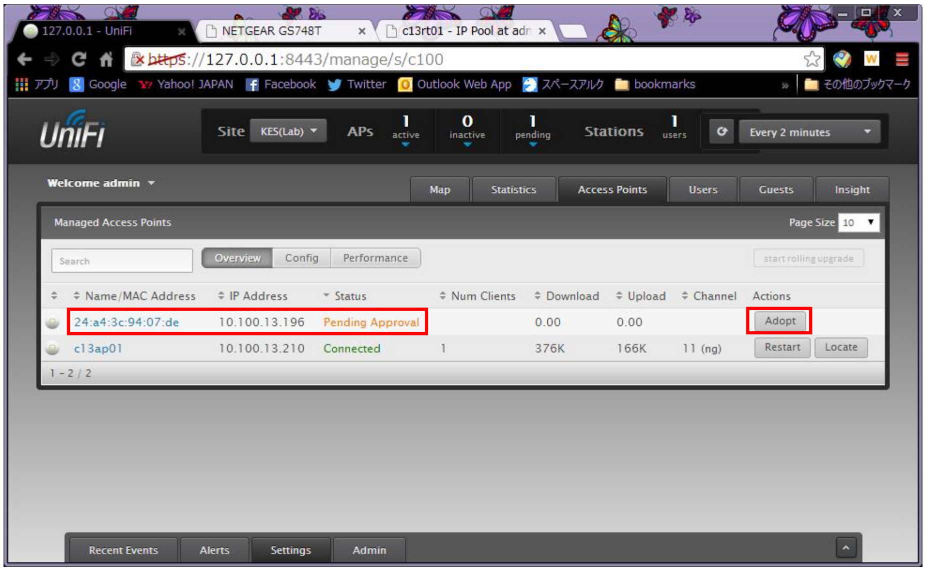

127.0.0.1 - UniFi
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c13
アプリ Google Yahoo! JAPAN Facebook Twitter Outlook Web App スペースアルク bookmarks CMU_MISM TCinGC その他のブックマーク
UniFi
Site KES
APs 0 active 0 inactive 0 pending
Stations 0 users 0 guests
Every 2 minutes
Welcome admin
Map
Statistics
Access Points
Users
Guests
Insight
Show: labels details coverage topology
Map: Sample
configure maps
5m
Recent Events
Alerts
Settings
Admin
WLANs
Options
Create

Settings » WLAN Group Default

| Name | Security | Guest Network | Actions |
|---|---|---|---|
| KES_UAP | wpaeap | No | edit delete |

**5. Register new access point**

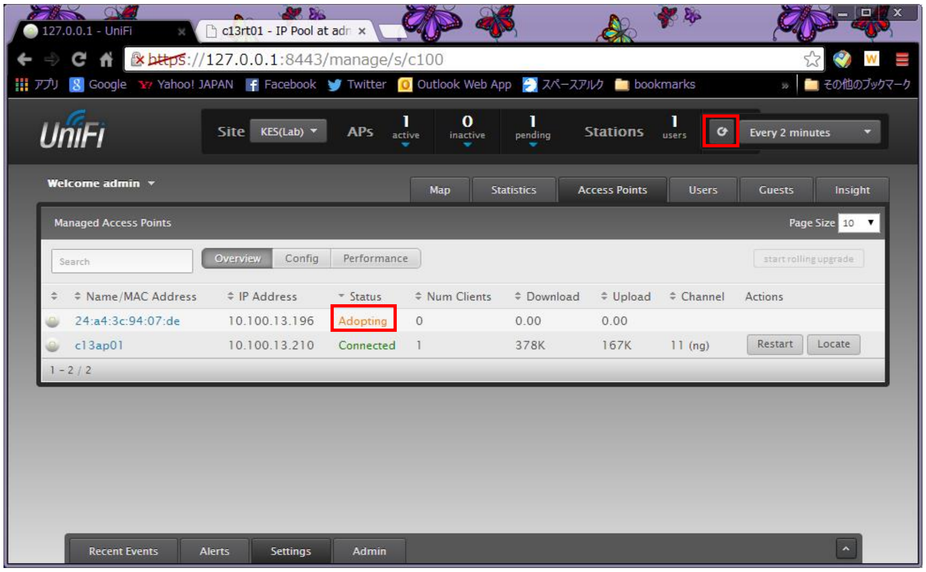
- When new access point connects to the same L2 network under DHCP enabled L3 network, UniFi automatically find the AP and shows the AP on “Access Points” tab. At this time, “Status” of the AP is “Pending Approval”. Click “Adopt” in order for the AP to be under the control of UniFi.


127.0.0.1 - UniFi
NETGEAR GS748T
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c100
アプリ Google Yahoo! JAPAN Facebook Twitter Outlook Web App スペースアルク bookmarks その他のブックマーク
UniFi
Site KES(Lab)
APs 1 active 0 inactive 1 pending
Stations 1 users
Every 2 minutes
Welcome admin
Map Statistics Access Points Users Guests Insight
Managed Access Points
Page Size 10
Search
Overview Config Performance
start rolling upgrade
Recent Events Alerts Settings Admin

| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| 24:a4:3c:94:07:de | 10.100.13.196 | Pending Approval | | 0.00 | 0.00 | | Adopt |
| c13ap01 | 10.100.13.210 | Connected | 1 | 376K | 166K | 11 (ng) | Restart Locate |

1 - 2 / 2

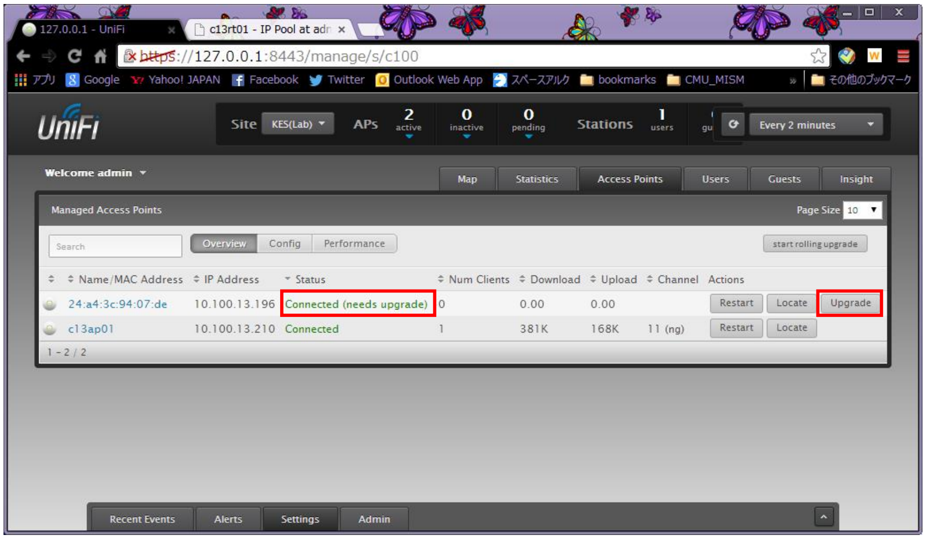
- Automatically start adopting process. It takes a little time. Click the refresh button on the top, you can update the current status.


127.0.0.1 - UniFi
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c100
アプリ Google Yahoo! JAPAN Facebook Twitter Outlook Web App スペースアルク bookmarks その他のブックマーク
UniFi
Site KES(Lab)
APs 1 active 0 inactive 1 pending
Stations 1 users
Every 2 minutes
Welcome admin
Map Statistics Access Points Users Guests Insight
Managed Access Points
Page Size 10
Search
Overview Config Performance
start rolling upgrade
Recent Events Alerts Settings Admin

| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| 24:a4:3c:94:07:de | 10.100.13.196 | Adopting | 0 | 0.00 | 0.00 | | |
| c13ap01 | 10.100.13.210 | Connected | 1 | 378K | 167K | 11 (ng) | Restart Locate |

1 - 2 / 2

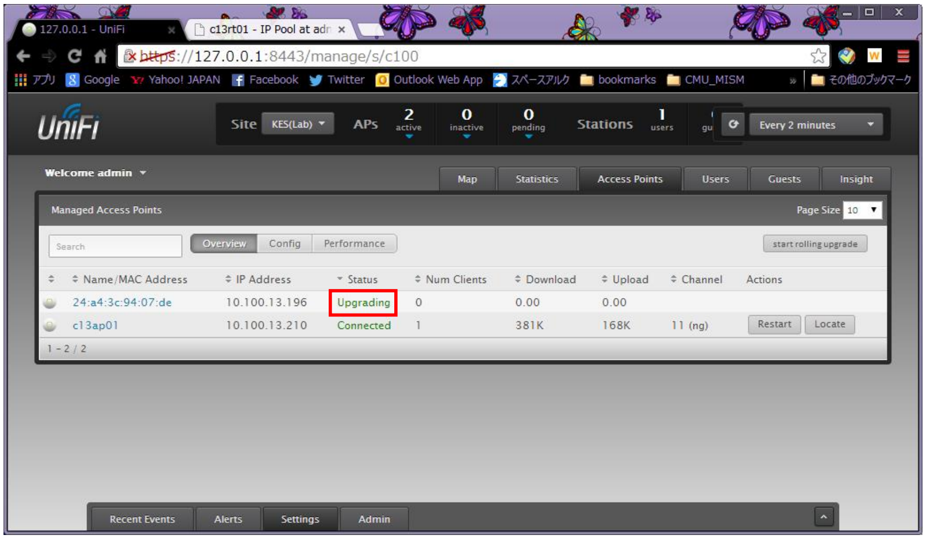
- The new access point was successfully adopted. The status changes to “Connected” or “Connected (needs upgrade)”. If UniFi requires upgrade, you click the “Upgrade” button at left of the line of AP.



| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| 24:a4:3c:94:07:de | 10.100.13.196 | Connected (needs upgrade) | 0 | 0.00 | 0.00 | | Restart Locate Upgrade |
| c13ap01 | 10.100.13.210 | Connected | 1 | 381K | 168K | 11 (ng) | Restart Locate |

1 - 2 / 2

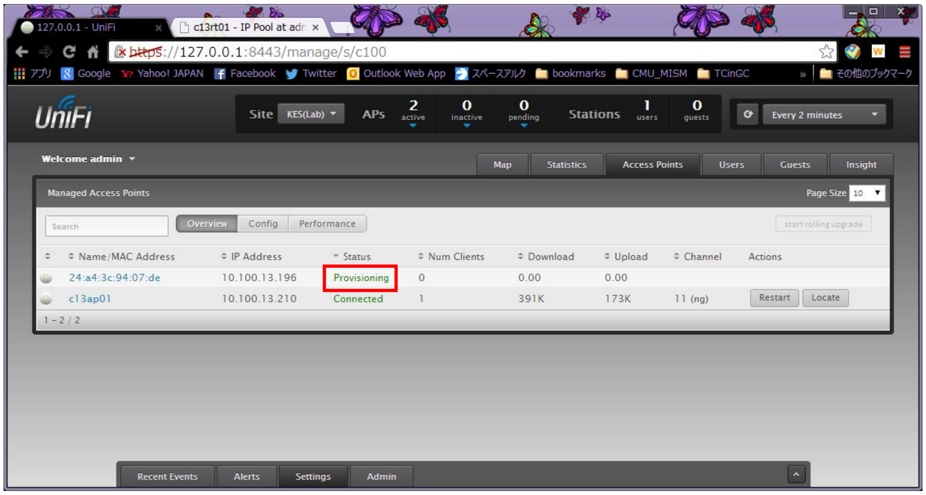
- UniFi tries to upgrade the AP via network. AP may reboot during upgrading process. Check the current status of AP by refreshing the screen from refresh button on the top.



| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| 24:a4:3c:94:07:de | 10.100.13.196 | Upgrading | 0 | 0.00 | 0.00 | | |
| c13ap01 | 10.100.13.210 | Connected | 1 | 381K | 168K | 11 (ng) | Restart Locate |

1 - 2 / 2

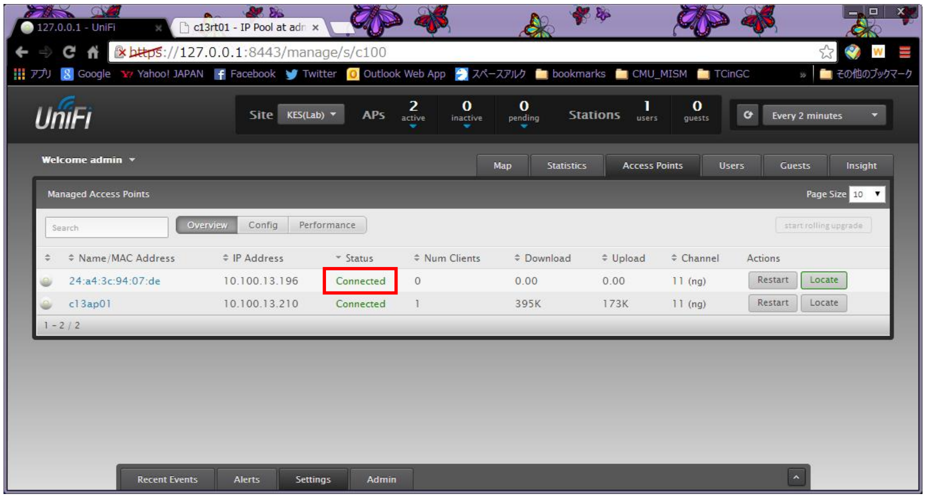
- Upgrading process continue…


127.0.0.1 - UniFi
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c100
UniFi
Site KES(Lab)
APs 2 active 0 inactive 0 pending
Stations 1 users 0 guests
Every 2 minutes
Welcome admin
Map Statistics Access Points Users Guests Insight
Managed Access Points
Page Size 10
Search
Overview Config Performance
start rolling upgrade
Recent Events Alerts Settings Admin

| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| 24:a4:3c:94:07:de | 10.100.13.196 | Provisioning | 0 | 0.00 | 0.00 | | |
| c13ap01 | 10.100.13.210 | Connected | 1 | 391K | 173K | 11 (ng) | Restart Locate |

1 - 2 / 2

- Now, upgrading process has finished. The AP's status come back to "Connected".


127.0.0.1 - UniFi
c13rt01 - IP Pool at adr
https://127.0.0.1:8443/manage/s/c100
UniFi
Site KES(Lab)
APs 2 active 0 inactive 0 pending
Stations 1 users 0 guests
Every 2 minutes
Welcome admin
Map Statistics Access Points Users Guests Insight
Managed Access Points
Page Size 10
Search
Overview Config Performance
start rolling upgrade
Recent Events Alerts Settings Admin

| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| 24:a4:3c:94:07:de | 10.100.13.196 | Connected | 0 | 0.00 | 0.00 | 11 (ng) | Restart Locate |
| c13ap01 | 10.100.13.210 | Connected | 1 | 395K | 173K | 11 (ng) | Restart Locate |

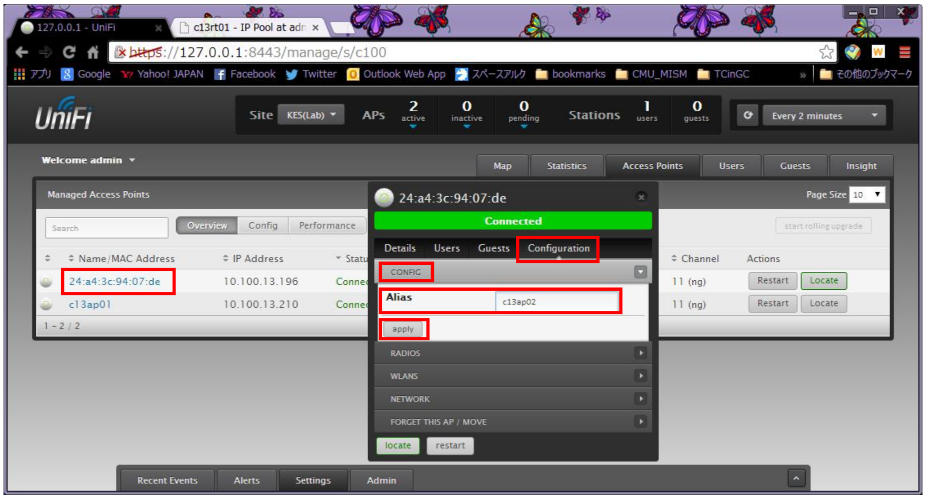
1 - 2 / 2

12

Last Modified: Aug 8, 2014

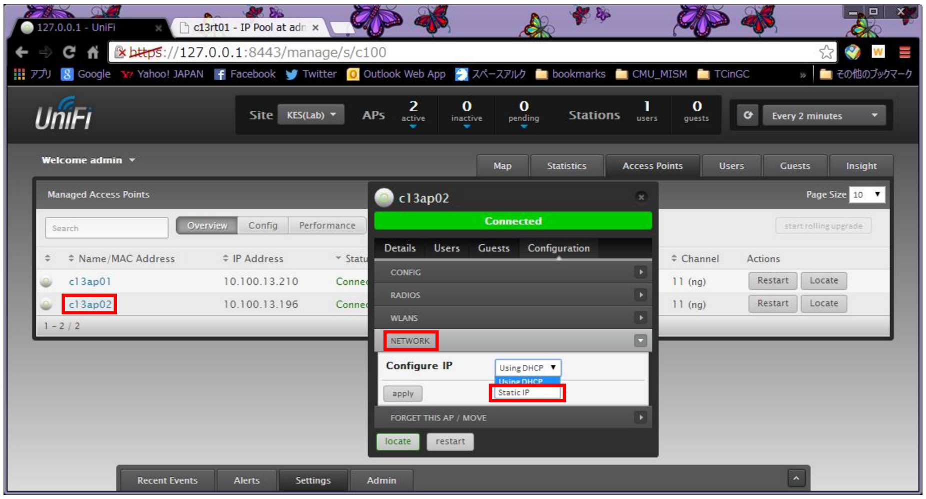
**6. Configure new access point**

- After joining the AP under UniFi Controller, you need to set up the access point.
- When clicking the AP's name on "Access Points" tab, detail information window shows up.
- Go to "Configuration" tab of the window and click "CONFIG" bar. Then, enter the hostname of the AP (in this case, "c13ap02"). Click "Apply" button.



Alias c13ap02

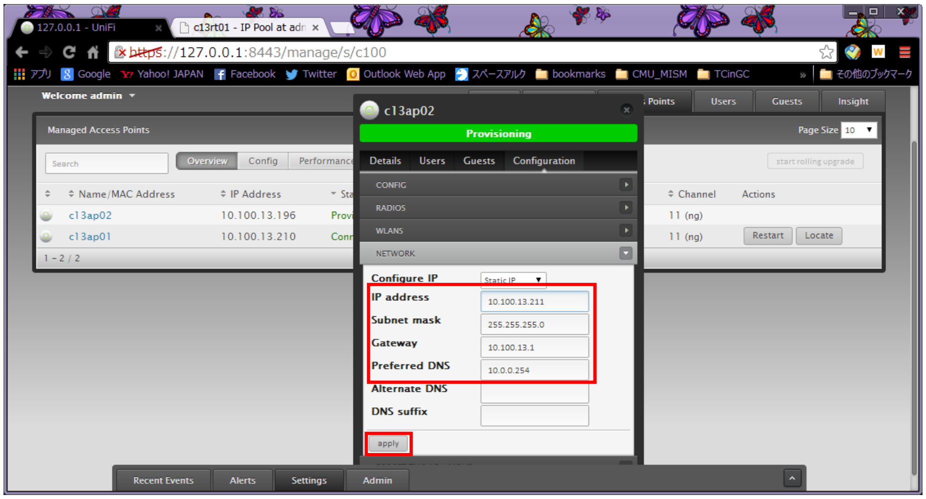
- After changing the alias, name of the AP will be changed.
- Then, go to "NETWORK" bar, and select "Static IP" from the drop-down box.



Configure IP: Using DHCP ▾ (Using DHCP / Static IP)

- Enter the IP address information of AP. Then, click “Apply” button.

| | | |
|---|---|---|
| (1) | IP Address | Designated IP address (ex. 10.100.13.211) |
| (2) | Subnet mask | 255.255.255.0 (24 bit subnet) |
| (3) | Gateway | Router’s address of the network (ex. 10.100.13.1) |
| (4) | Preferred DNS | 10.0.0.254 |



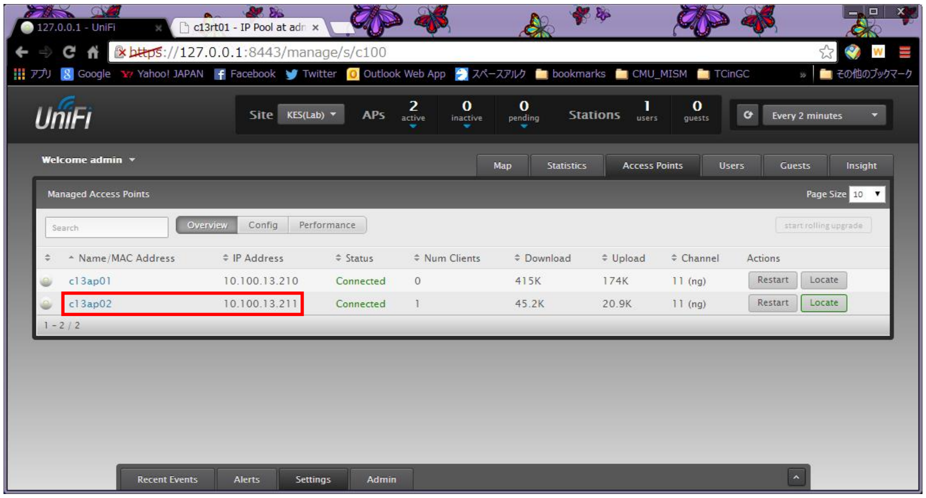
https://127.0.0.1:8443/manage/s/c100

c13ap02 — Provisioning — Configuration — NETWORK

Configure IP: Static IP
IP address: 10.100.13.211
Subnet mask: 255.255.255.0
Gateway: 10.100.13.1
Preferred DNS: 10.0.0.254
Alternate DNS:
DNS suffix:

apply

- The hostname and IP address of the AP have successfully changed.



https://127.0.0.1:8443/manage/s/c100

Site KES(Lab) — APs 2 active, 0 inactive, 0 pending — Stations 1 users, 0 guests

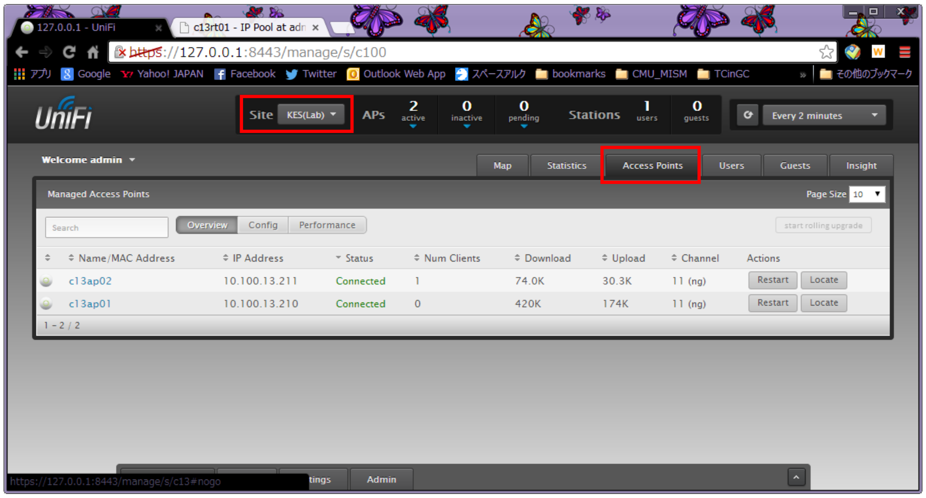
Managed Access Points

| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| c13ap01 | 10.100.13.210 | Connected | 0 | 415K | 174K | 11 (ng) | Restart Locate |
| c13ap02 | 10.100.13.211 | Connected | 1 | 45.2K | 20.9K | 11 (ng) | Restart Locate |

1 - 2 / 2

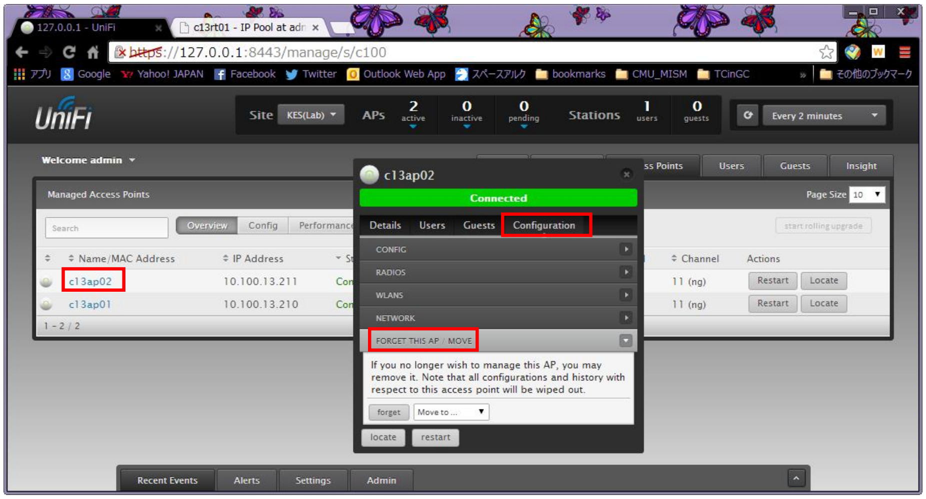
### 7. Move AP to another site

- If you want to move AP to other site setting, first, you choose the “Site” where the AP currently belongs and the, show “Access Points” tab.



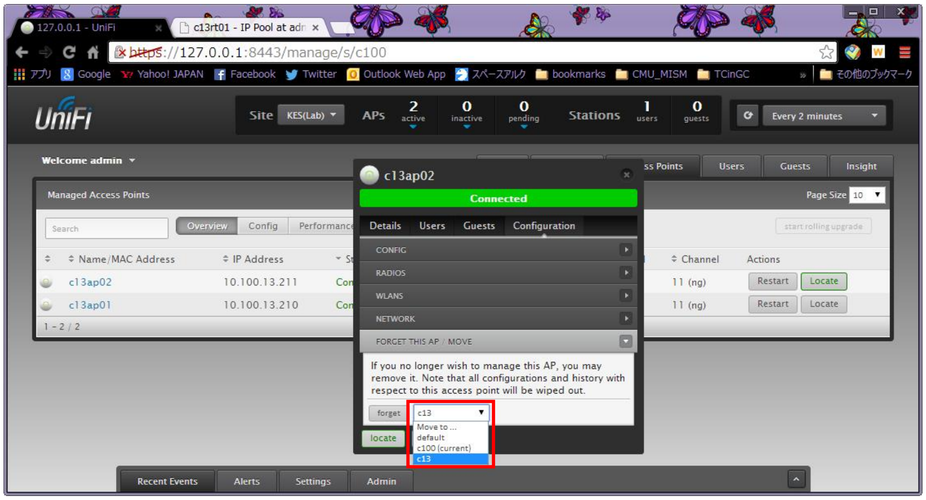
| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| c13ap02 | 10.100.13.211 | Connected | 1 | 74.0K | 30.3K | 11 (ng) | Restart Locate |
| c13ap01 | 10.100.13.210 | Connected | 0 | 420K | 174K | 11 (ng) | Restart Locate |

- Click the AP name which you want to move in order to show the detail information window.
- Click “Configuration” tab, and then show “FORGET THIS AP / MOVE” tab.



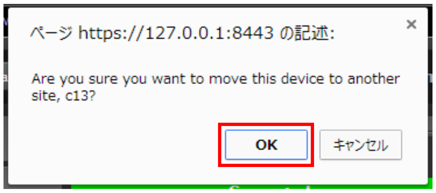
If you no longer wish to manage this AP, you may remove it. Note that all configurations and history with respect to this access point will be wiped out.

- Choose the site to which you want to move the AP, from the drop-down box (ex. “c13” in this case).


https://127.0.0.1:8443/manage/s/c100
UniFi
Site KES(Lab)
APs 2 active 0 inactive 0 pending
Stations 1 users 0 guests
Every 2 minutes
Welcome admin
Managed Access Points
Page Size 10
Overview Config Performance
Name/MAC Address IP Address Channel Actions
c13ap02 10.100.13.211 11 (ng) Restart Locate
c13ap01 10.100.13.210 11 (ng) Restart Locate
c13ap02
Connected
Details Users Guests Configuration
CONFIG
RADIOS
WLANS
NETWORK
FORGET THIS AP / MOVE
forget
locate
c13
Move to ...
default
c100 (current)
c13
Recent Events Alerts Settings Admin

If you no longer wish to manage this AP, you may remove it. Note that all configurations and history with respect to this access point will be wiped out.

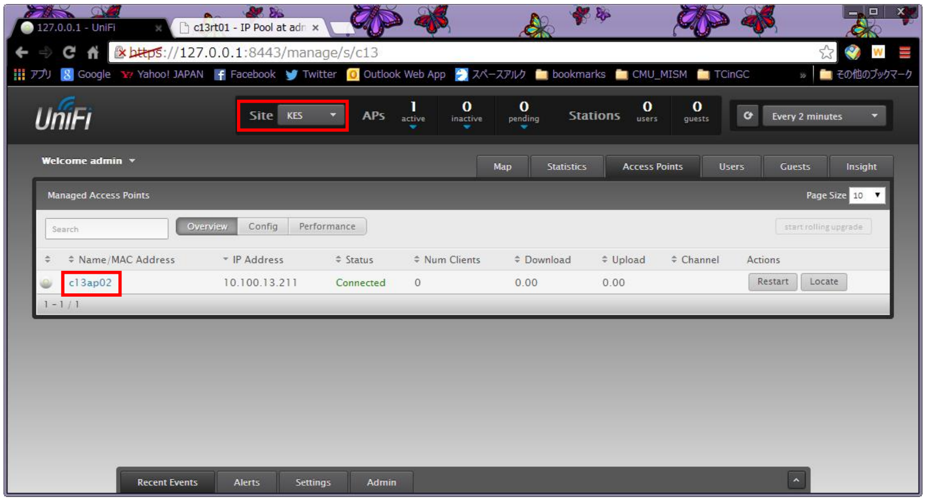
- Attention message shows up. Make sure the information (the site name) and Click “OK”



ページ https://127.0.0.1:8443 の記述:

Are you sure you want to move this device to another site, c13?

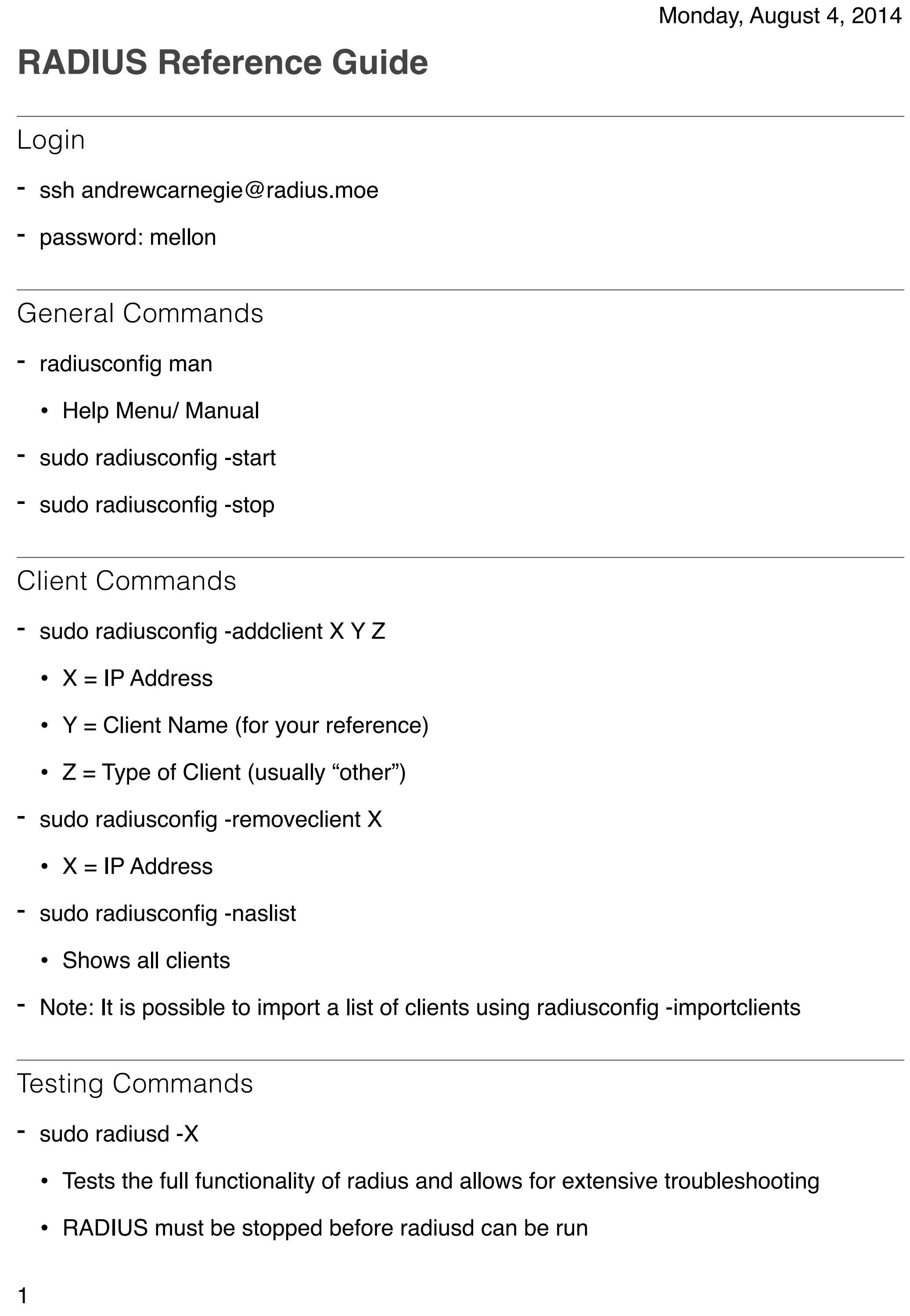
- Now, the AP successfully moves to new site.


https://127.0.0.1:8443/manage/s/c13
UniFi
Site KES
APs 1 active 0 inactive 0 pending
Stations 0 users 0 guests
Every 2 minutes
Welcome admin
Map Statistics Access Points Users Guests Insight
Managed Access Points
Page Size 10
Overview Config Performance
start rolling upgrade
Recent Events Alerts Settings Admin

| Name/MAC Address | IP Address | Status | Num Clients | Download | Upload | Channel | Actions |
|---|---|---|---|---|---|---|---|
| c13ap02 | 10.100.13.211 | Connected | 0 | 0.00 | 0.00 | | Restart Locate |

1 - 1 / 1

# Appendix Q



Monday, August 4, 2014

## RADIUS Reference Guide

### Login

- ssh andrewcarnegie@radius.moe
- password: mellon

### General Commands

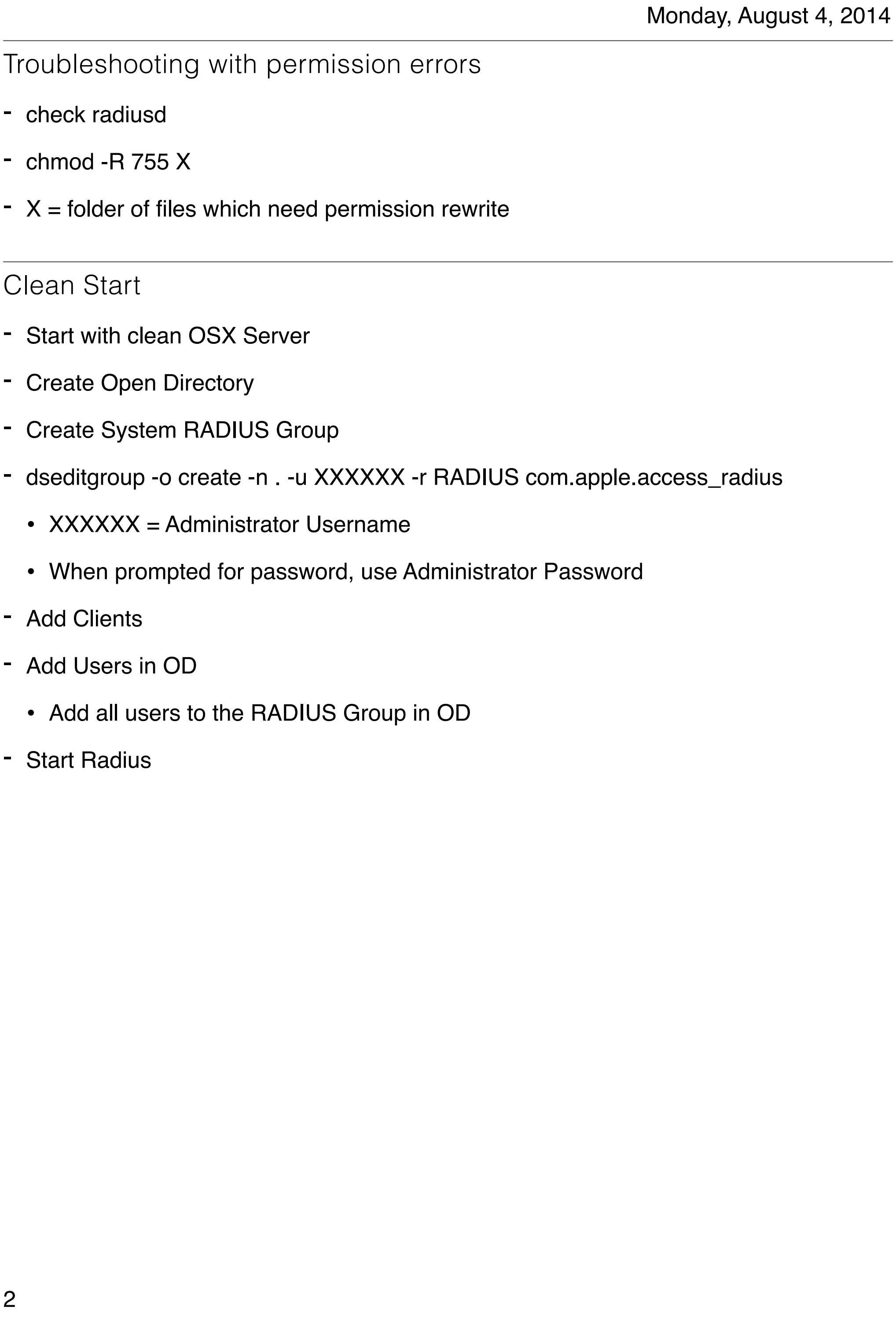
- radiusconfig man
  - Help Menu/ Manual
- sudo radiusconfig -start
- sudo radiusconfig -stop

### Client Commands

- sudo radiusconfig -addclient X Y Z
  - X = IP Address
  - Y = Client Name (for your reference)
  - Z = Type of Client (usually “other”)
- sudo radiusconfig -removeclient X
  - X = IP Address
- sudo radiusconfig -naslist
  - Shows all clients
- Note: It is possible to import a list of clients using radiusconfig -importclients

### Testing Commands

- sudo radiusd -X
  - Tests the full functionality of radius and allows for extensive troubleshooting
  - RADIUS must be stopped before radiusd can be run



Monday, August 4, 2014

## Troubleshooting with permission errors

- check radiusd
- chmod -R 755 X
- X = folder of files which need permission rewrite

## Clean Start

- Start with clean OSX Server
- Create Open Directory
- Create System RADIUS Group
- dseditgroup -o create -n . -u XXXXXX -r RADIUS com.apple.access_radius
  - XXXXXX = Administrator Username
  - When prompted for password, use Administrator Password
- Add Clients
- Add Users in OD
  - Add all users to the RADIUS Group in OD
- Start Radius

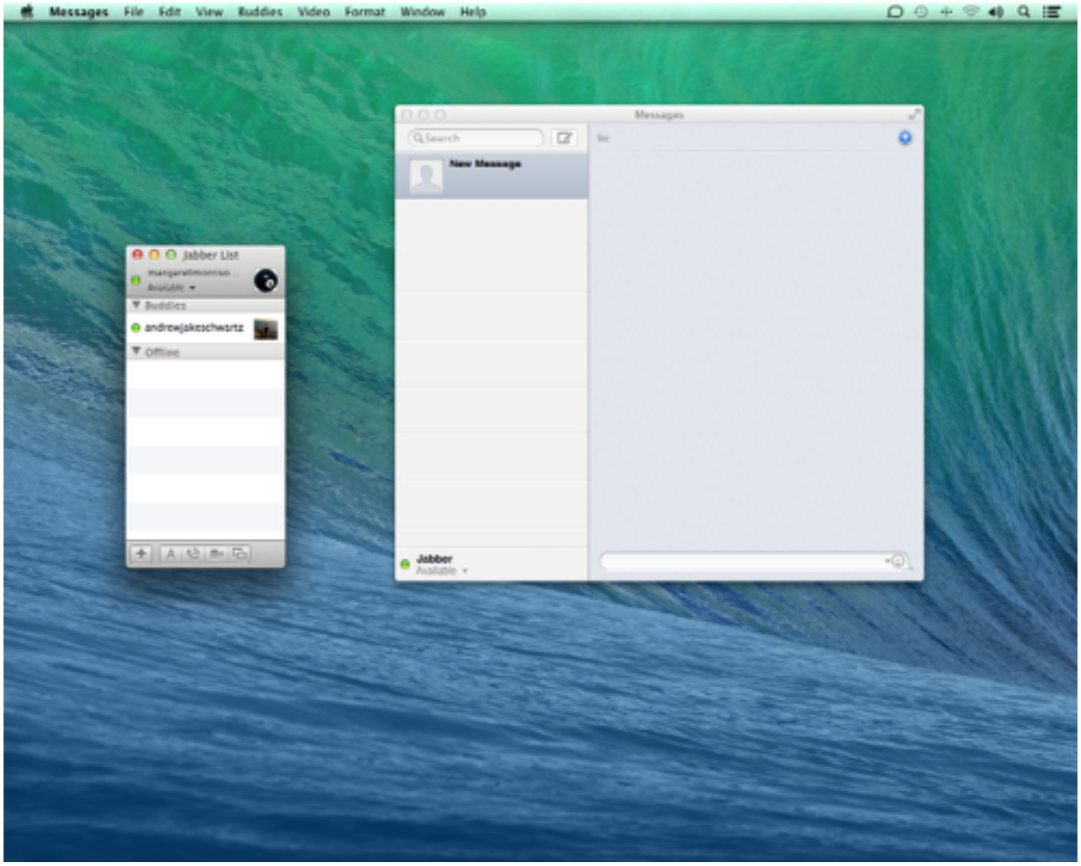
2

# Appendix R

# Palau Ministry of Education

## Collaboration Services User Guide

MOE Information Technology - Last Updated August 1, 2014

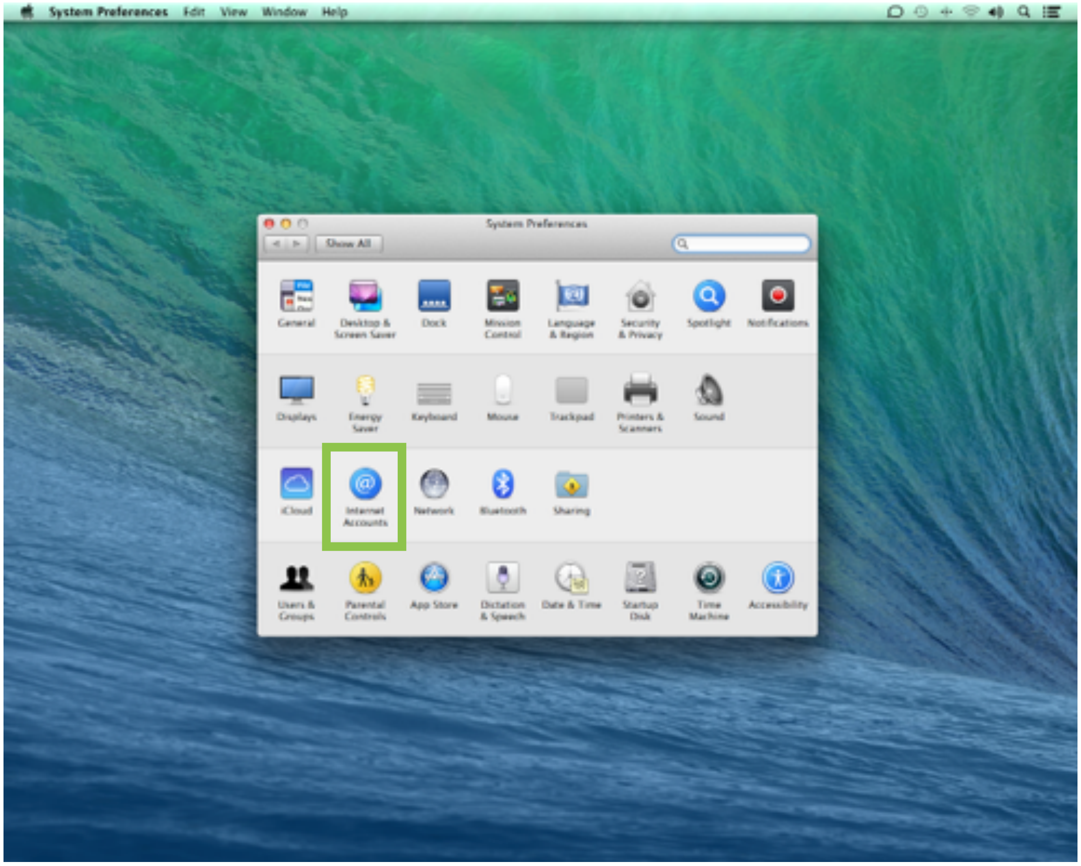


# Setup

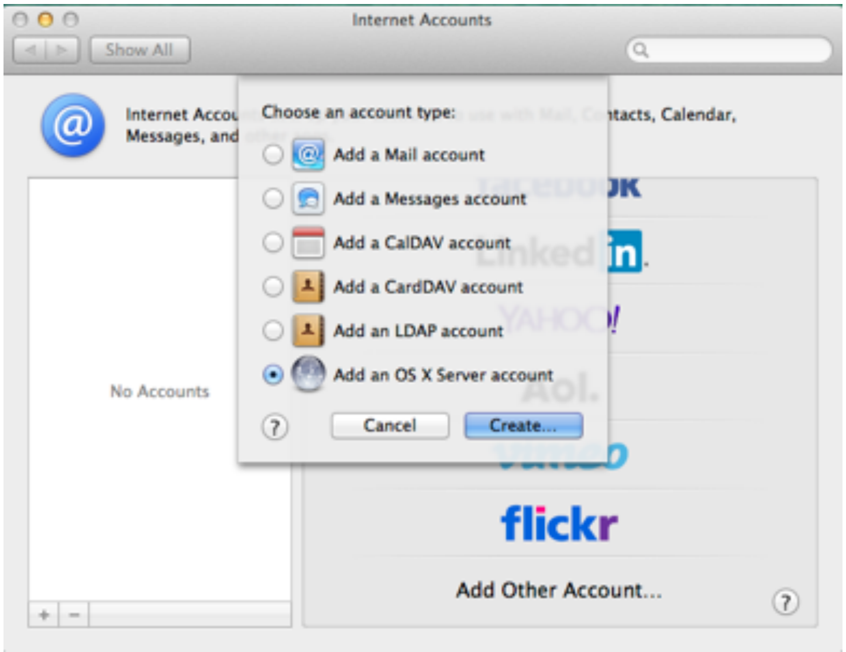
Hello! Welcome to Collaboration Services Configuration for Users!

The MOE Collaboration Service is meant to give you access to internal messaging and calendars to be used by any staff within the Ministry of Education. By this time, you should have been notified of your username and password by MOEIT. If you have not, you will not be able to proceed.

Begin by Opening up System Preferences and clicking the “Internet Accounts” Tab



Click “Add Other Account” and select “Add OS X Server Account”


Choose an account type:

○ Add a Mail account

○ Add a Messages account

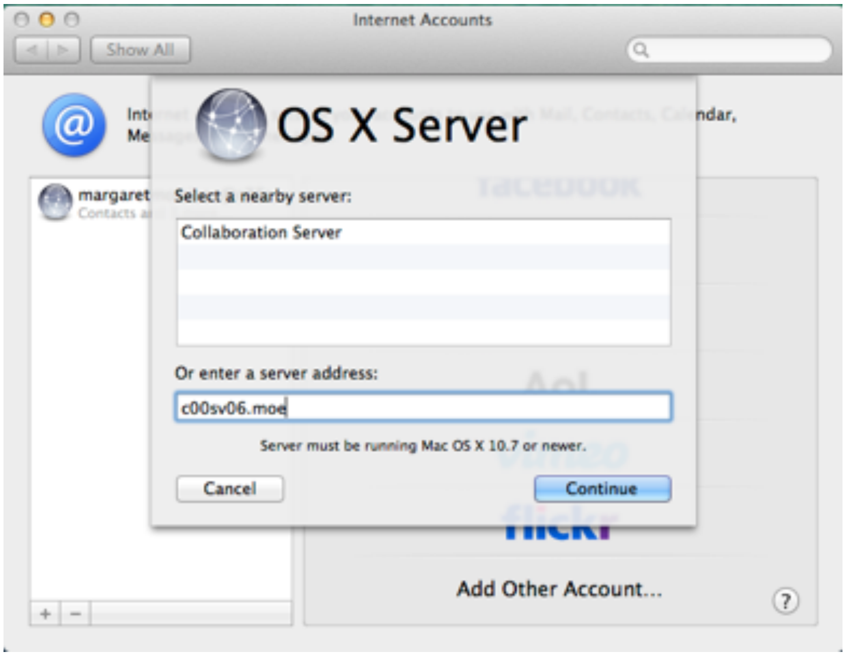
○ Add a CalDAV account

○ Add a CardDAV account

○ Add an LDAP account

● Add an OS X Server account

The Server address is c00sv06.moe


OS X Server

Select a nearby server:

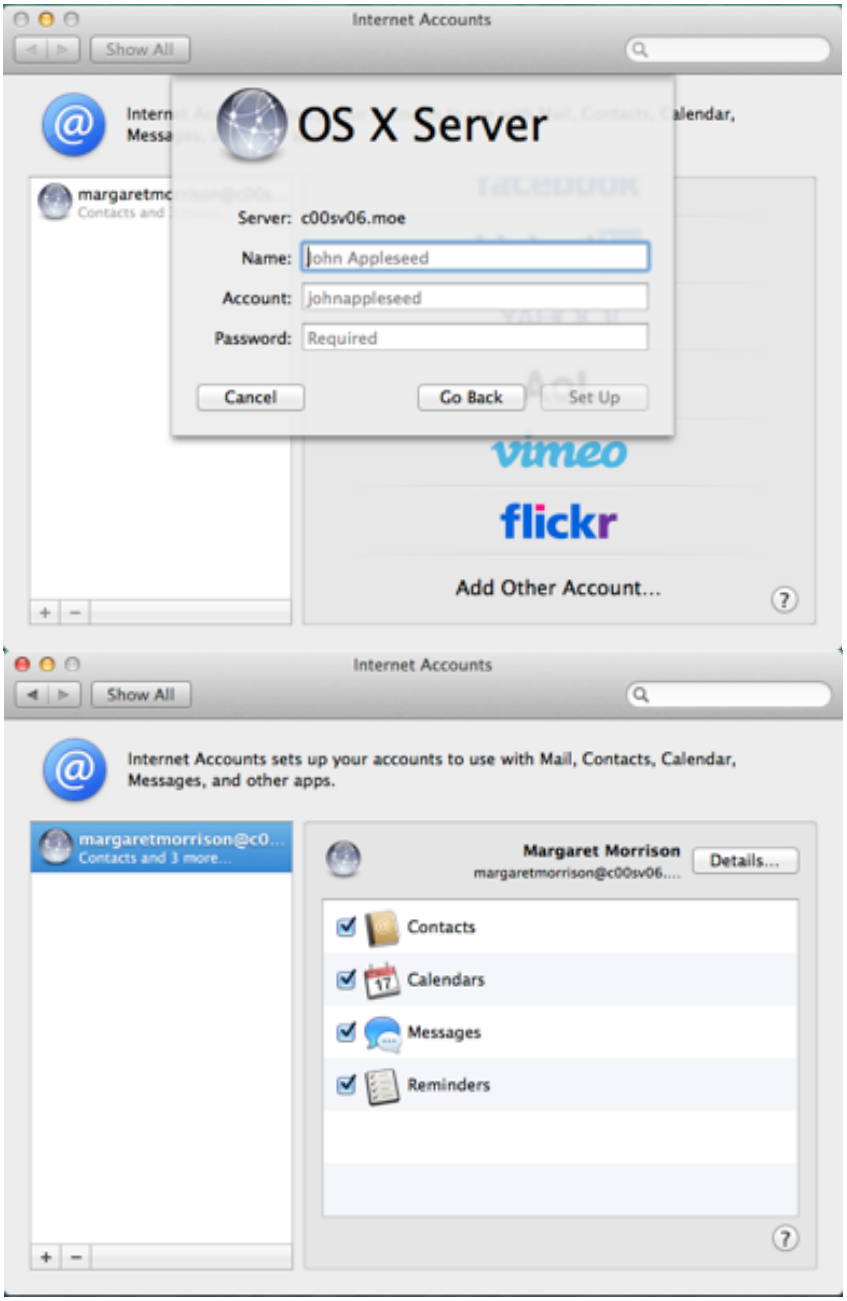
Collaboration Server

Or enter a server address:

c00sv06.moe

Server must be running Mac OS X 10.7 or newer.

Your name, account and password will be provided to you by MOE IT.



OS X Server

Server: c00sv06.moe

Name: John Appleseed

Account: johnappleseed

Password: Required

Internet Accounts sets up your accounts to use with Mail, Contacts, Calendar, Messages, and other apps.

Margaret Morrison
margaretmorrison@c00sv06....

☑ Contacts

☑ Calendars

☑ Messages

☑ Reminders

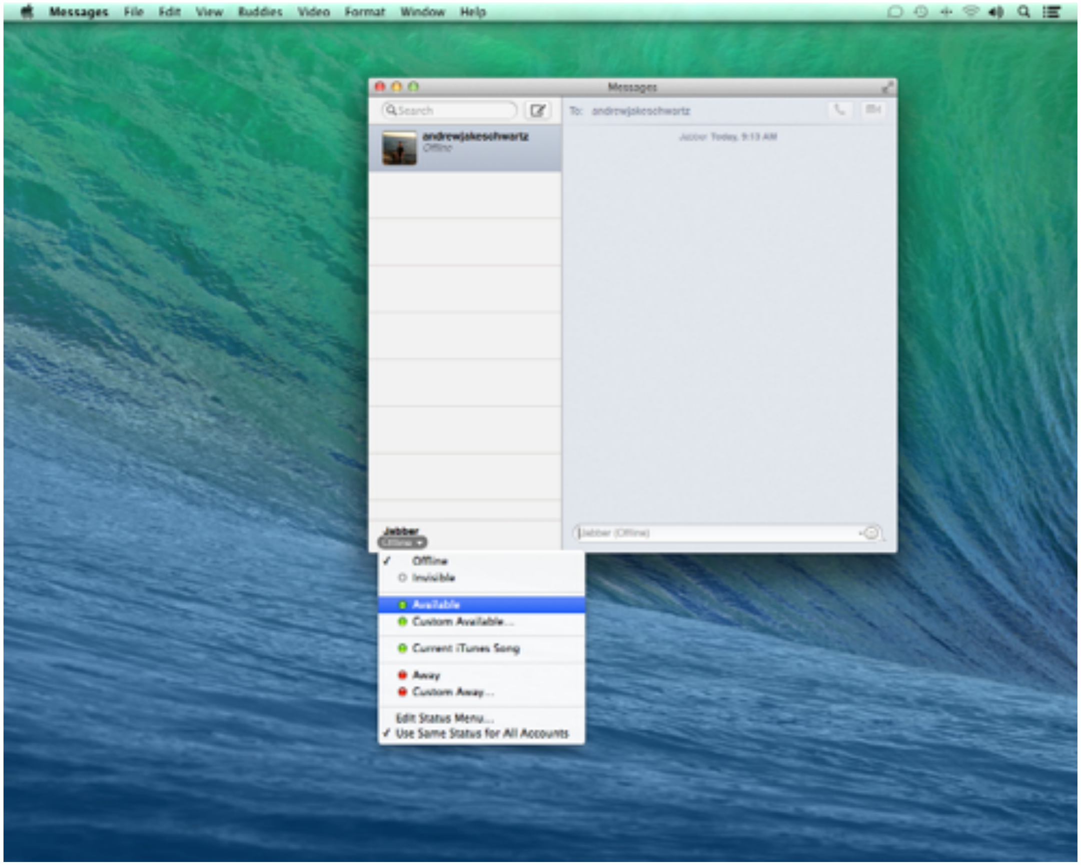
If your screen looks like shown below, your account has been configured.

## Messages

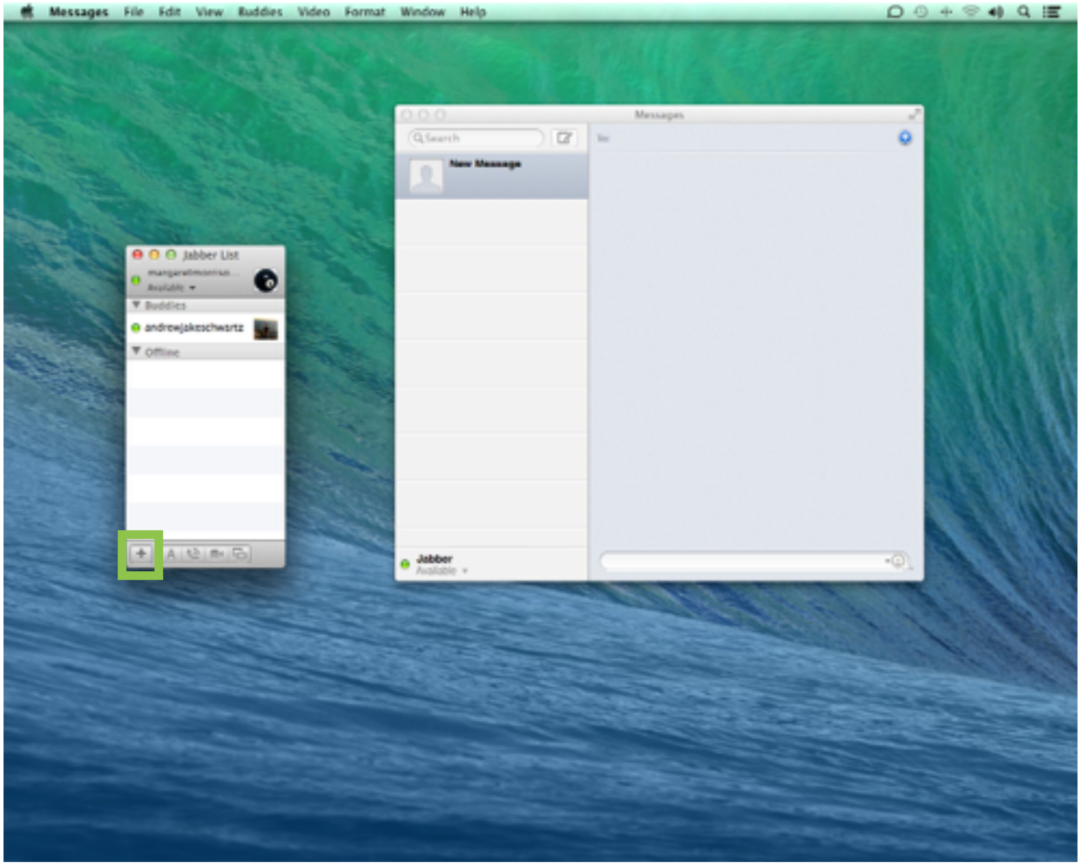
The first application we will use as part of collaboration services is called Messages. This application can be used to send text or files to other individuals in the MOE with more speed and convenience than a mail server. In addition, there is no limit on file transfers with this application.

Messages is typically used to connect to other people through the cloud, but we will be using it to only communicate with people within the MOE through a service called "Jabber". You will see Jabber in the bottom left hand corner of the window that opens up (you may have to skip the setup window)

Let's Open up Messages. You can do this through your dock or through the search bar. If a setup window appears, click "Skip".To Login, click "Offline" and a drop down menu will appear. Then Click "Available" to Login to the server.



Go to View -> Buddy List to bring up your Collaboration Services list. In the bottom left of the window, click the + button.

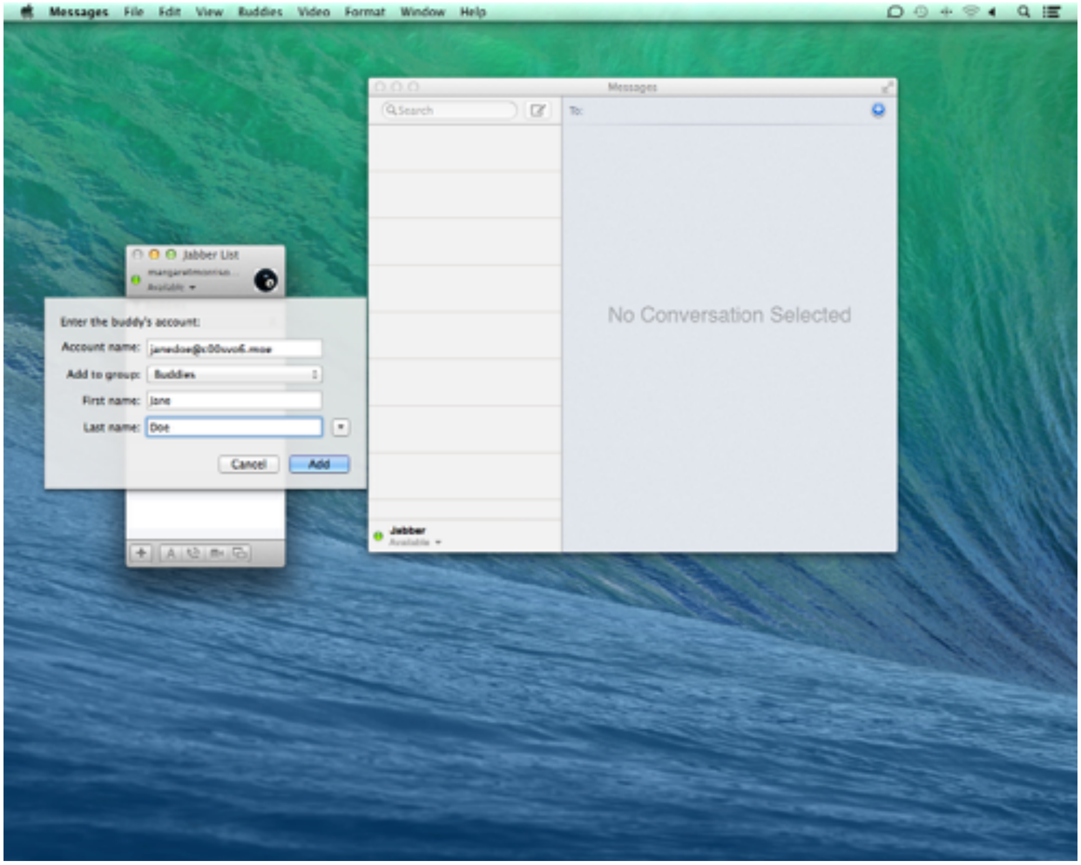


From this screen you can add any of your fellow MOE employees.

In order to be able to communicate with another individual, both people must confirm “Friendship” in the system. The first user will click the + button and enter the following information. Your friends account will then be asked to accept, and then both individuals can contact each other using messages.

Account name - FirstnameLastname@c00sv06.moe

This process will only need to occur once per friendship. This process confirms that only you and your specified colleagues can access this system.



Enter the buddy's account:

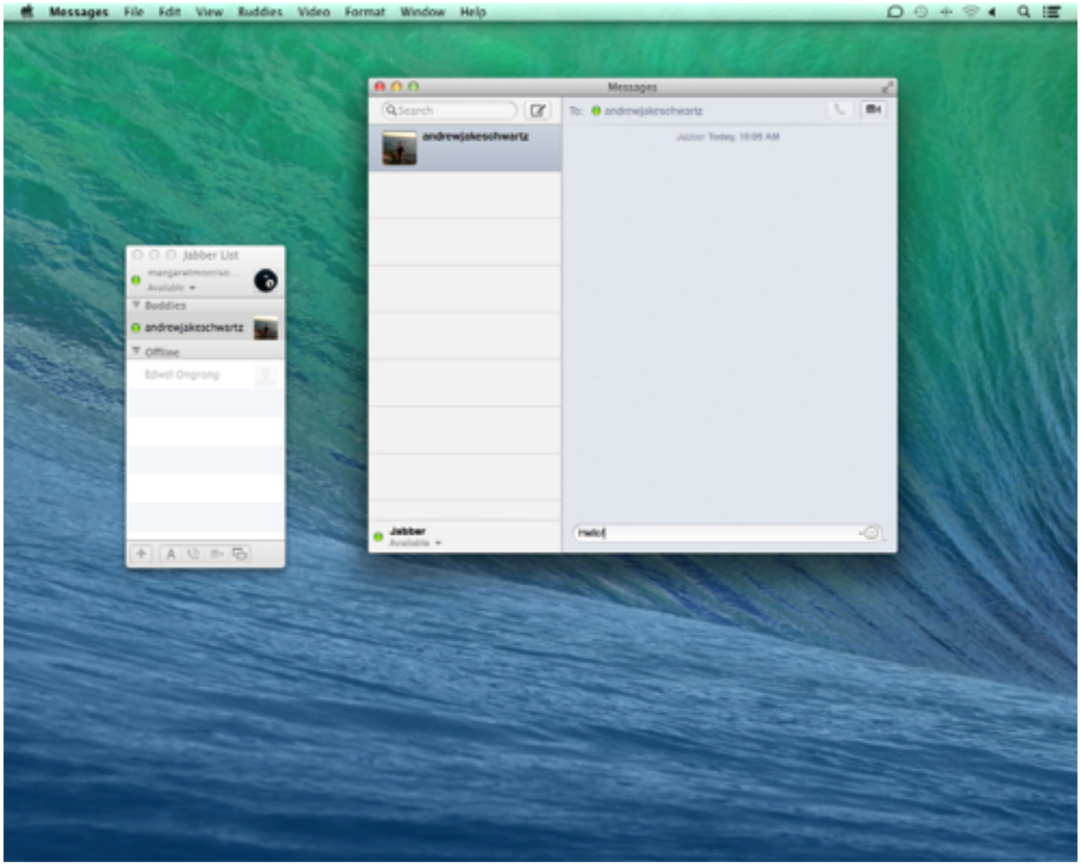
Account name: janedoe@c00sv06.moe

Add to group: Buddies

First name: Jane

Last name: Doe

To send a message to a buddy, click their name on the buddy list and begin typing.



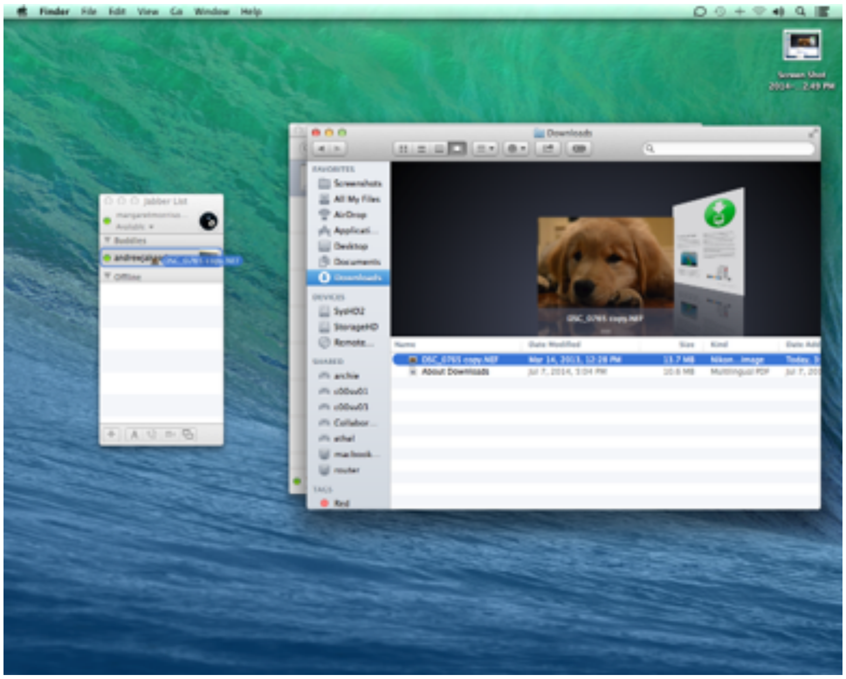
Hello!

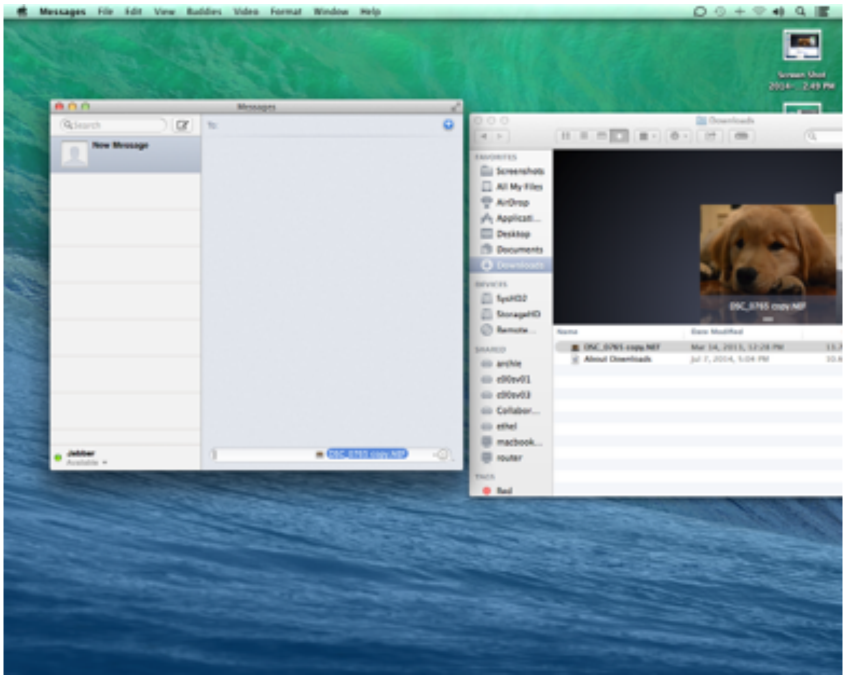
The second major feature deals with file transfers. File transfers can be done using this service with no limitation on the size of the file. This makes the service much easier than email.

To transfer a file between individuals, you may drag the file onto

- The individuals name on your buddy list
- The text input in the messaging window

The two ways to complete file transfers are shown below





Messages should be used for:

- Quick messages
- Informal Messages
- Messages to 1-5 People
- File Transfers bigger than one document
- Messages that do not need to be later referenced

Messages is meant for informal communication. While it is possible to search archives of your Messages, it is not as easy or convenient as email.

File transfers, while faster and more efficient than email, can only be downloaded once

Messages should not be used for:

- Formal Messages
- Messages to large groups of people
- Messages that need to refereed to on a constant basis

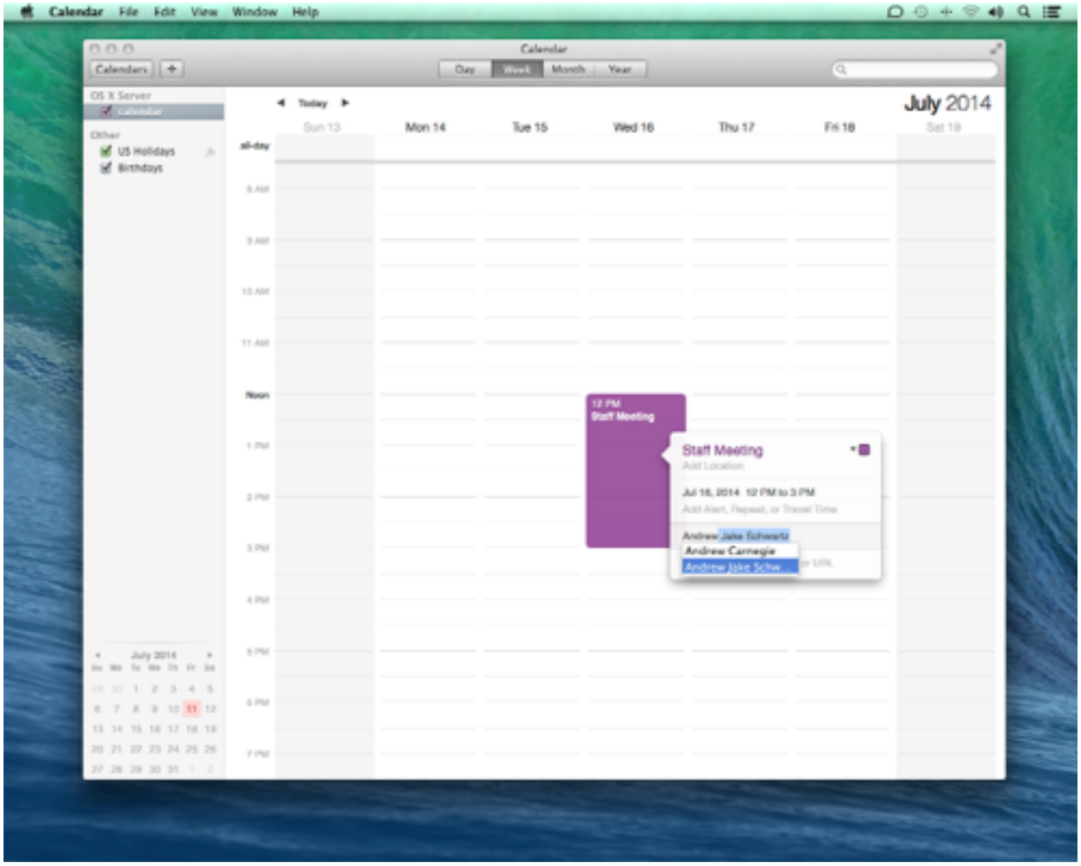
Note: As your software upgrades year to year, features and operations within Messages will change slightly. Like any other piece of software, the ability to successfully use this software will depend on daily or weekly usage of the product.

# Calendars

Now let's open up Calendars. This application is meant to completely replace the way that you schedule events and collaborate with others at the MOE.

To begin, double click the day / time to start an event. From this window you can add a title, location, alert time or notes.

With this application you can make events and send them to other individuals within the MOE. When you go to create an event, go to the Invite section. From here you can enter a colleagues name and it should autofill with their account information.

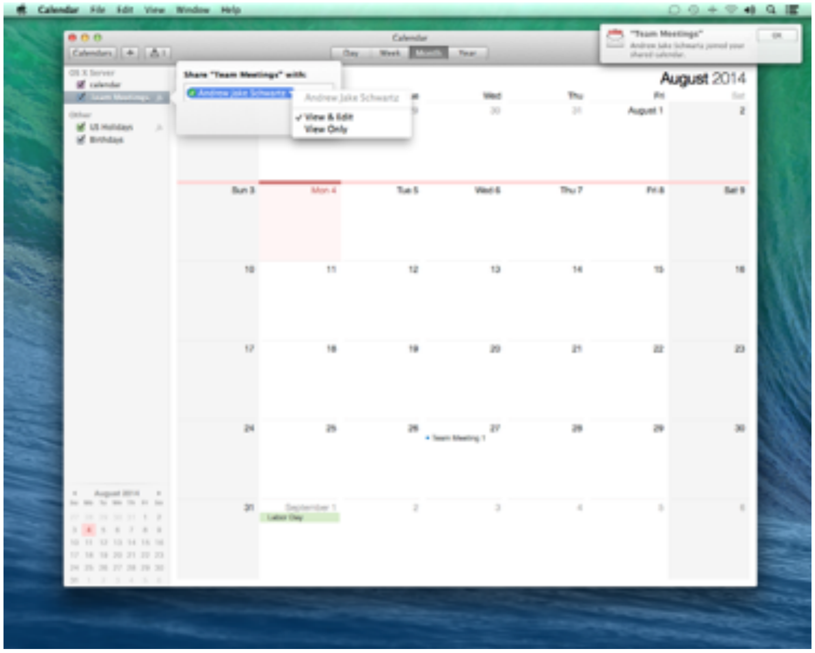


Staff Meeting
Add Location
Jul 16, 2014 12 PM to 3 PM
Add Alert, Repeat, or Travel Time
Andrew Jake Schwartz
Andrew Carnegie
Andrew Jake Schw...

There are two ways to collaborate with others using the calendar service. The first is the way described above, where you invite each individual and they have the ability to accept or reject your invitation. The second method does not involve confirmation, but also does not need user action to invite or accept a calendar event.

The process for a team calendar is as follows. Create a new calendar under File - > New Calendar. Once you have created a calendar on the server, you can Right Click (Option + Click) the calendar and start sharing it with members of your team.

Once you enter a team member's name, you can set there ability to View & Edit or just View. The team members will have to confirm the calendar join, but then all events will synchronize.



Share "Team Meetings" with:

Andrew Jake Schwartz

✓ View & Edit
View Only

"Team Meetings"
Andrew Jake Schwartz joined your shared calendar.

To make the most out of this application, you should transfer all of your events from your current calendar. The calendar can be printed out if you prefer a hard-copy.

With the integration of Calendar and Messages into the Ministry, you will allow for a significant level of efficiency to arise throughout your team.

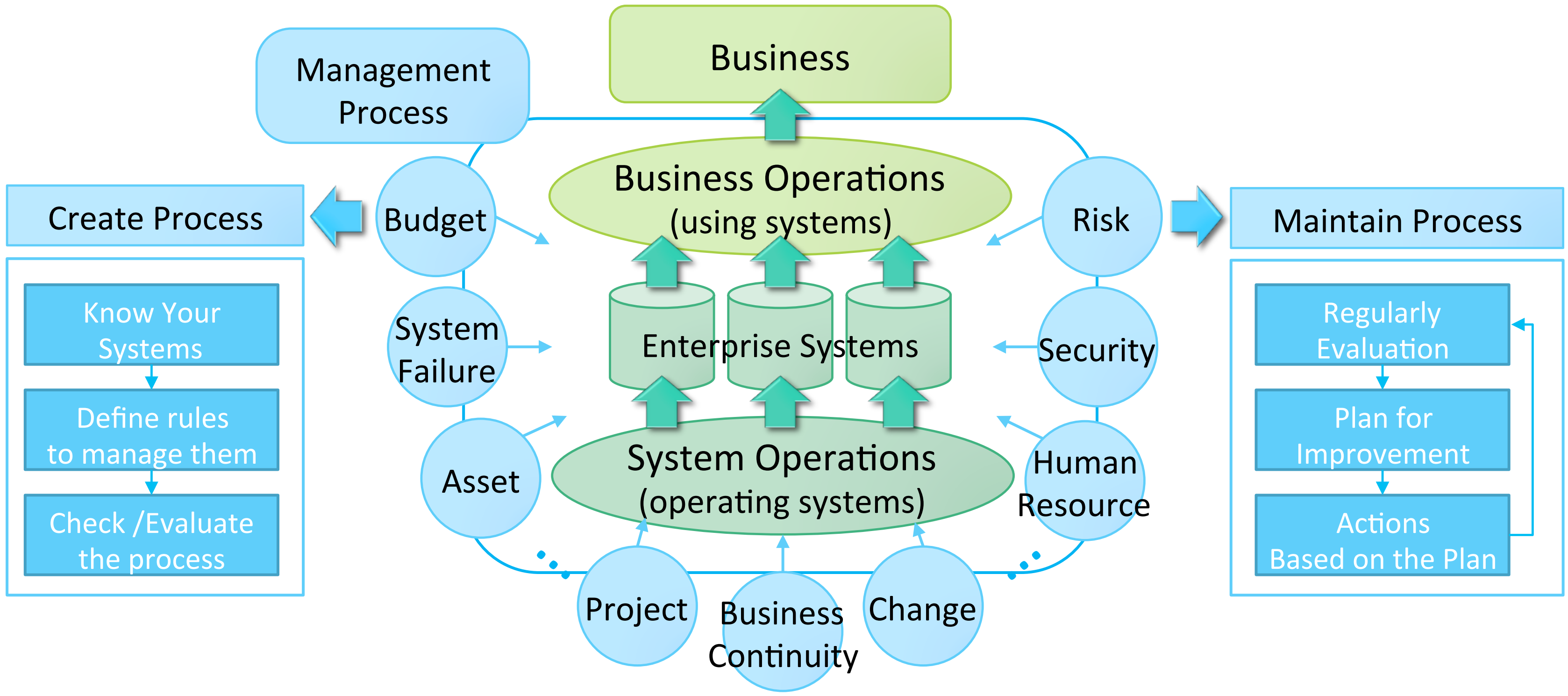
## Appendix S

Discussion on 7/23

# MOE IT Operation Improvement Project

- Before starting discussions…
  - What is your image (scope, range, or definition…) of “IT Operation”?
  - What are current problems of “IT Operation” (which you want to solve)?
  - What is the purpose (or main target) of this project?

- My Image of “Enterprise System Structure” is shown as below.



1

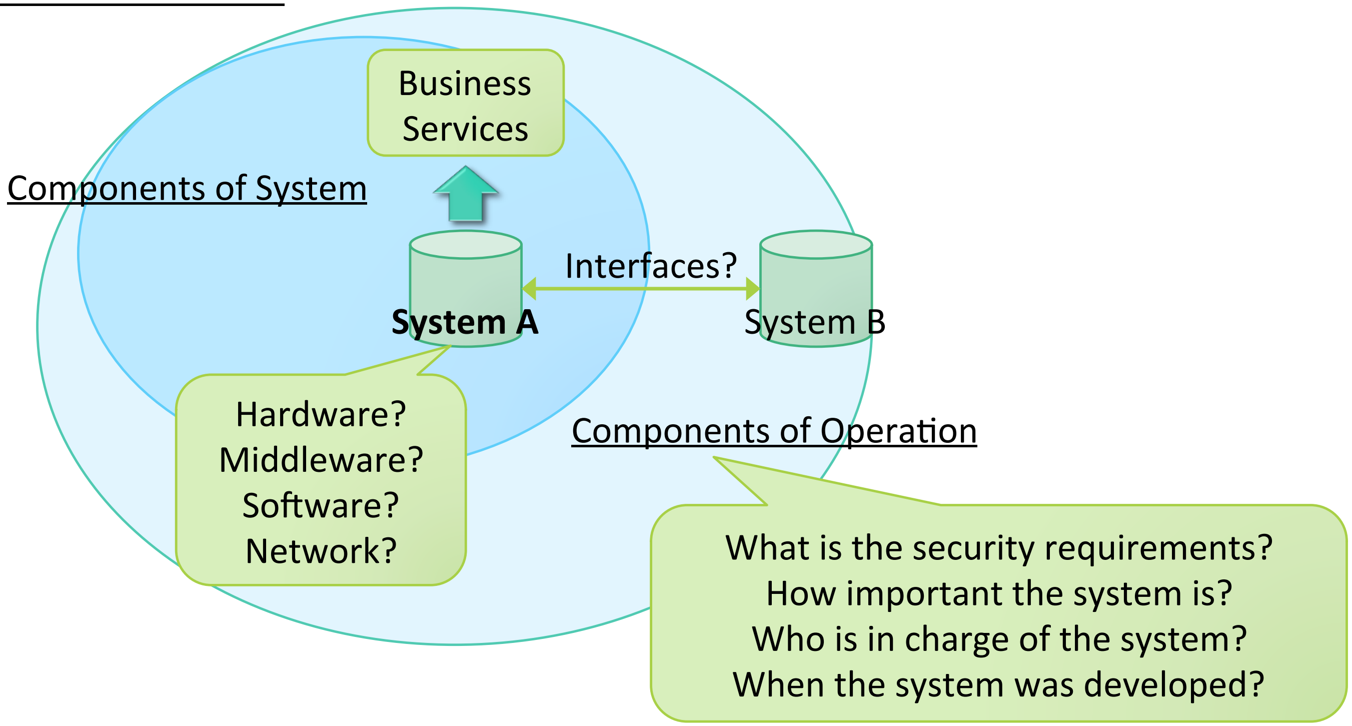
Yuki Nishihara - Jul 23, 2014

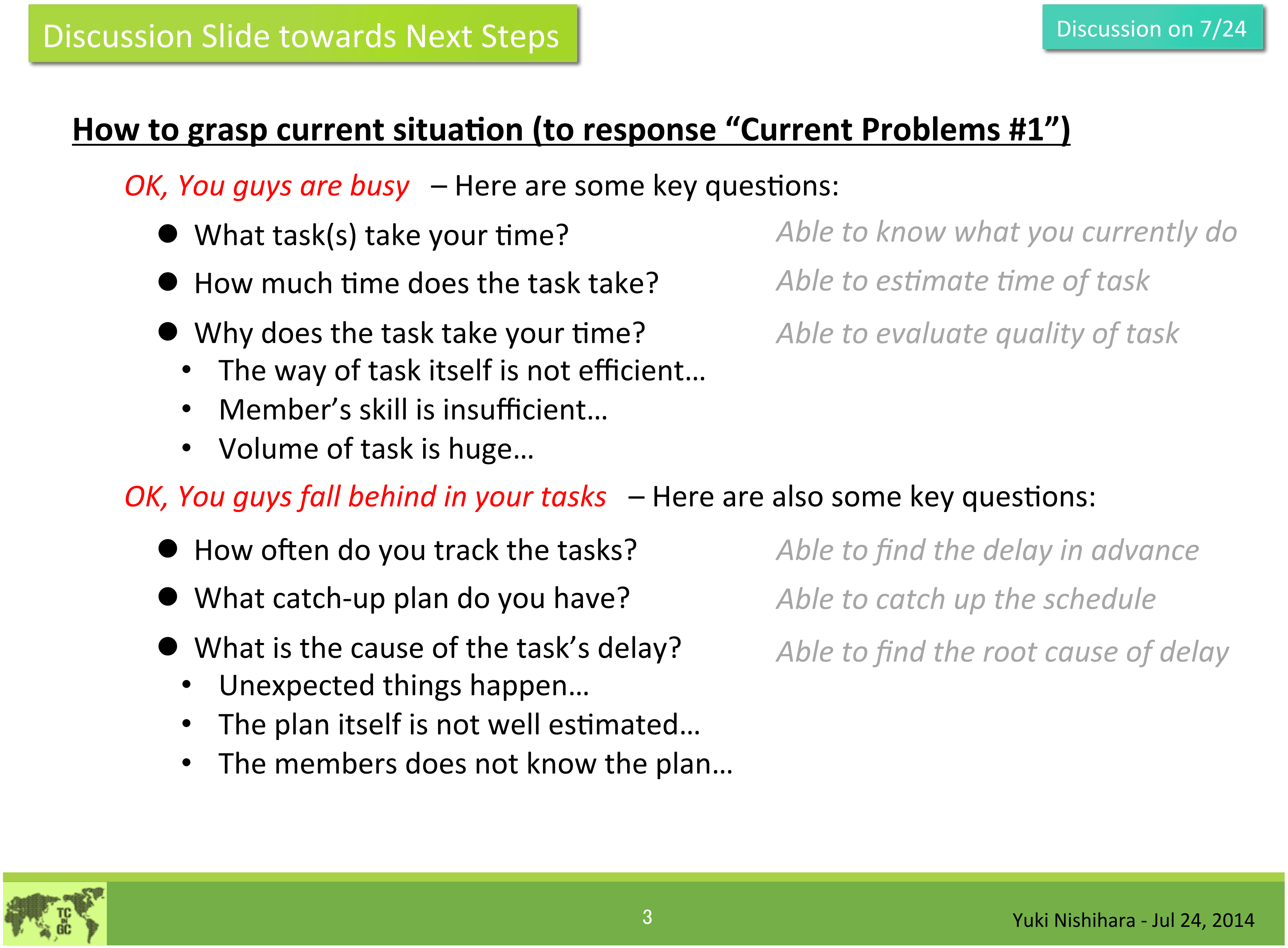
# Know Your Systems

Discussion on 7/23

- "Know MOE systems" is a starting point for all IT management.
  (we cannot manage the system if we don't know what we want to manage)
- How to know MOE systems?
  – one way is to create **"list of system"** (called **"System Ledger"** in my company) and maintain it.
- Put the information about all systems in MOE into the same table.

## The Attributes of the table





Discussion Slide towards Next Steps

Discussion on 7/24

## How to grasp current situation (to response "Current Problems #1")

*OK, You guys are busy* – Here are some key questions:

- ● What task(s) take your time? — *Able to know what you currently do*
- ● How much time does the task take? — *Able to estimate time of task*
- ● Why does the task take your time? — *Able to evaluate quality of task*
  - The way of task itself is not efficient…
  - Member's skill is insufficient…
  - Volume of task is huge…

*OK, You guys fall behind in your tasks* – Here are also some key questions:

- ● How often do you track the tasks? — *Able to find the delay in advance*
- ● What catch-up plan do you have? — *Able to catch up the schedule*
- ● What is the cause of the task's delay? — *Able to find the root cause of delay*
  - Unexpected things happen…
  - The plan itself is not well estimated…
  - The members does not know the plan…

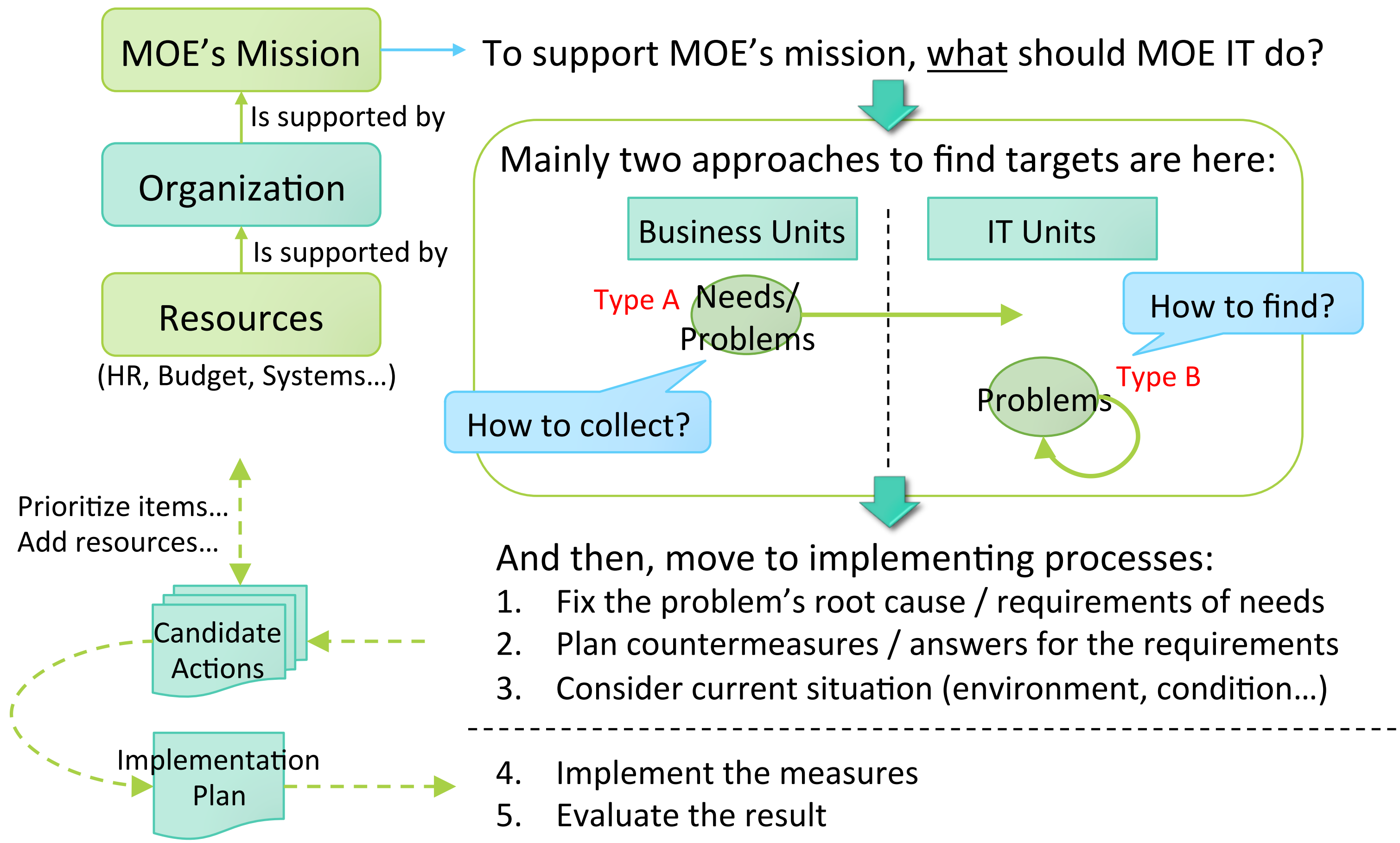
3

Yuki Nishihara - Jul 24, 2014

## Discussion Slide towards Next Steps

Discussion on 7/24

### How to plan MOE IT's next action (to response "Current Problems #2")



MOE's Mission

Is supported by

Organization

Is supported by

Resources

(HR, Budget, Systems…)

To support MOE's mission, what should MOE IT do?

Mainly two approaches to find targets are here:

Business Units

IT Units

Type A Needs/ Problems

How to collect?

How to find?

Problems

Type B

Prioritize items…
Add resources…

Candidate Actions

Implementation Plan

And then, move to implementing processes:

1. Fix the problem's root cause / requirements of needs
2. Plan countermeasures / answers for the requirements
3. Consider current situation (environment, condition…)

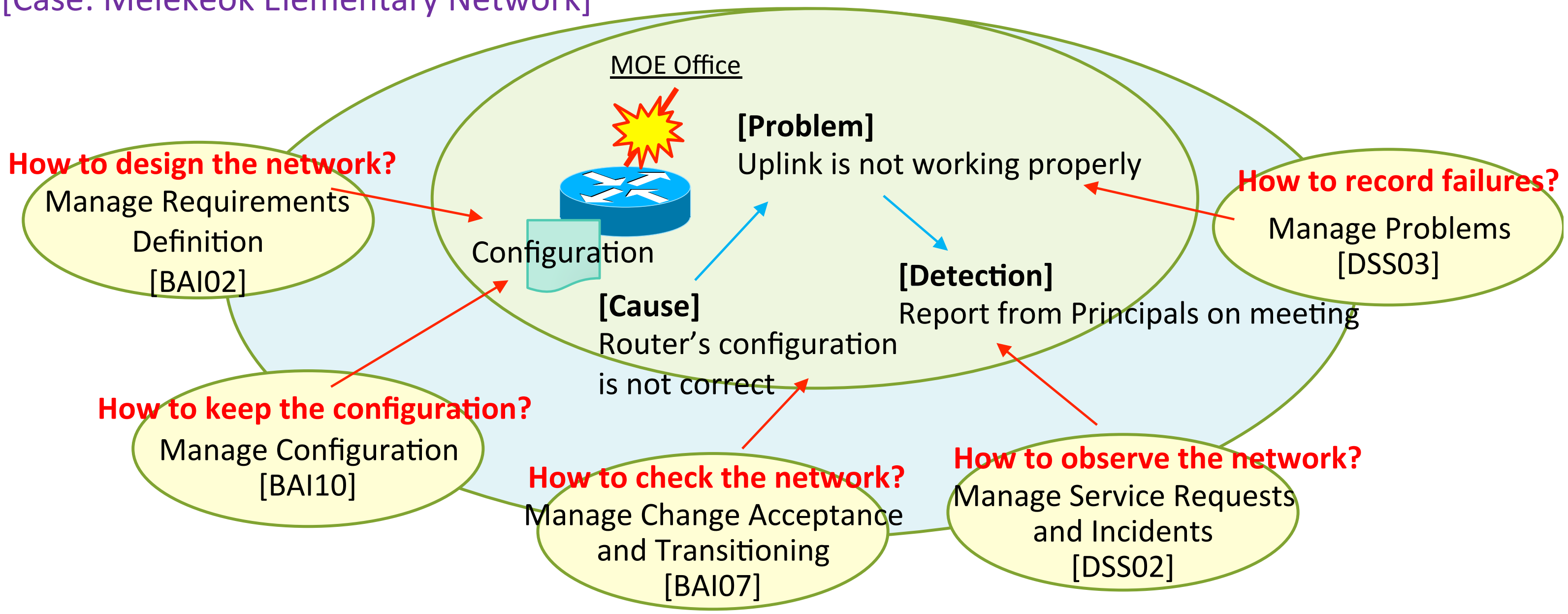
4. Implement the measures
5. Evaluate the result

## General Steps to IT Management Enhancement

Discussion on 8/5

1. **Know your systems**
   - A) Create “System Ledger” (described on P.2)
   - B) Create “System Structure Diagram”
     - ● Like a “bird’s eye view”.
     - ● Big structure of MOE IT systems can be grasped by looking the diagram.
2. **List up current problems for MOE IT and drill down the root causes of the problem**
3. **Analyze common/significant IT management areas where the causes are covered**

[Case: Melekeok Elementary Network]



MOE Office

Configuration

**[Problem]**
Uplink is not working properly

**[Detection]**
Report from Principals on meeting

**[Cause]**
Router’s configuration
is not correct

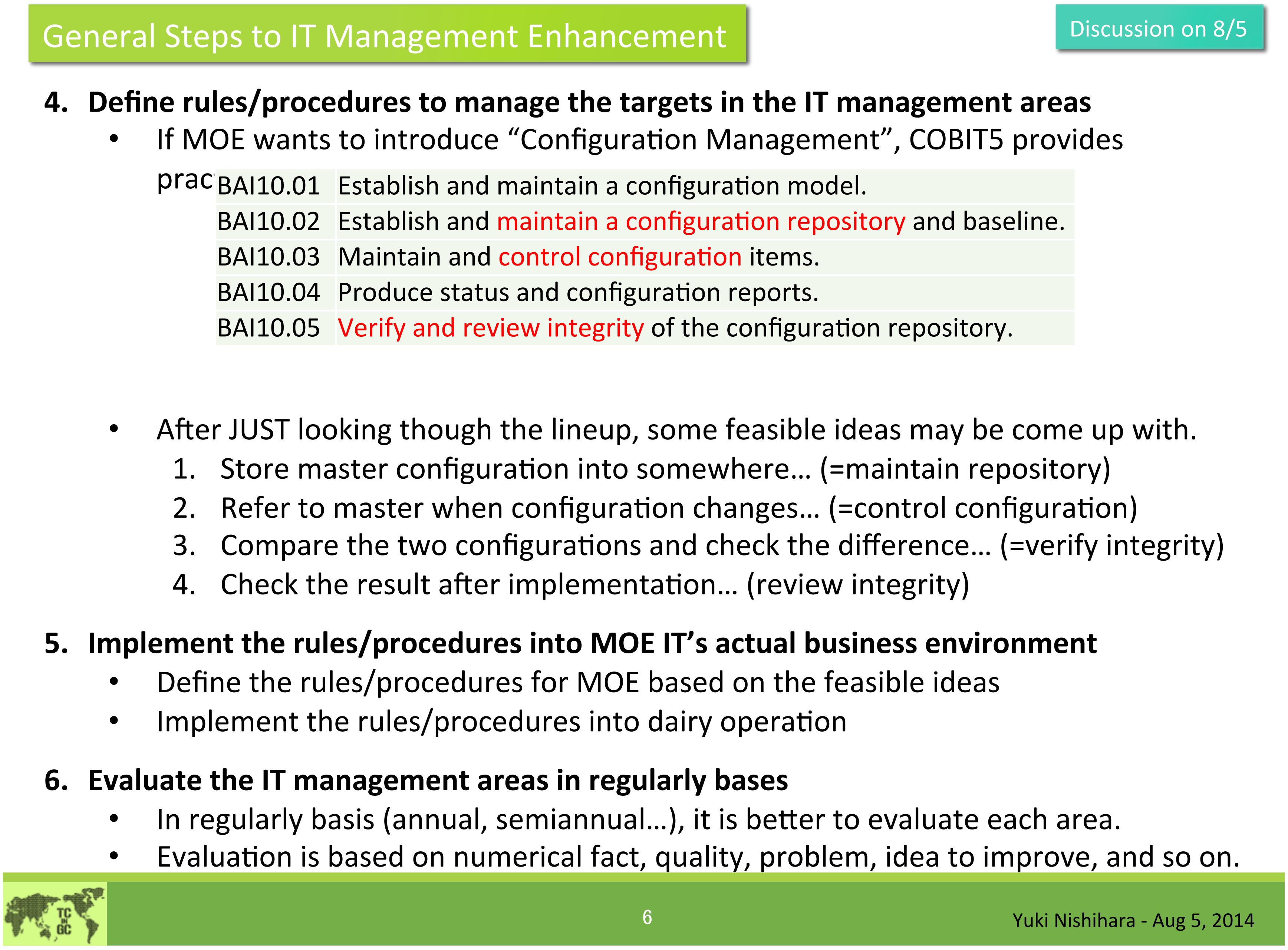
How to design the network?
Manage Requirements Definition [BAI02]

How to keep the configuration?
Manage Configuration [BAI10]

How to check the network?
Manage Change Acceptance and Transitioning [BAI07]

How to observe the network?
Manage Service Requests and Incidents [DSS02]

How to record failures?
Manage Problems [DSS03]



## General Steps to IT Management Enhancement

Discussion on 8/5

4. **Define rules/procedures to manage the targets in the IT management areas**
   - If MOE wants to introduce “Configuration Management”, COBIT5 provides prac

| | |
|---|---|
| BAI10.01 | Establish and maintain a configuration model. |
| BAI10.02 | Establish and maintain a configuration repository and baseline. |
| BAI10.03 | Maintain and control configuration items. |
| BAI10.04 | Produce status and configuration reports. |
| BAI10.05 | Verify and review integrity of the configuration repository. |

   - After JUST looking though the lineup, some feasible ideas may be come up with.
     1. Store master configuration into somewhere… (=maintain repository)
     2. Refer to master when configuration changes… (=control configuration)
     3. Compare the two configurations and check the difference… (=verify integrity)
     4. Check the result after implementation… (review integrity)

5. **Implement the rules/procedures into MOE IT’s actual business environment**
   - Define the rules/procedures for MOE based on the feasible ideas
   - Implement the rules/procedures into dairy operation

6. **Evaluate the IT management areas in regularly bases**
   - In regularly basis (annual, semiannual…), it is better to evaluate each area.
   - Evaluation is based on numerical fact, quality, problem, idea to improve, and so on.

# An Example of Regularly Reporting Format

Discussion on 8/5

## 1. Results of Past Half Year

Future plan should be based on the past result

| | |
|---|---|
| Budget | • Planned Budget / Actual Expenditure<br>• Causes of Differences… |
| Project Results | • # of Projects<br>• Progress / Quality of Projects… |
| System Failures | • # of Failures / $ of Business Impact<br>• Tendency of System Failures… |
| Human Resource | • # o time the staff used<br>• Result of training (evaluation) |

To track the results,
IT management process is required

(Extend to Action)

**(ex) # of system failures**
**Two questions will be solved…**

1. How to detect the failures?
   - Reporting from users?
   - Detection system implement? (Like, “ping server”)
   - Collect system logs? …
2. How to record the failures?
   - Prepare the “list”?
   - Keep info w/o missing? …

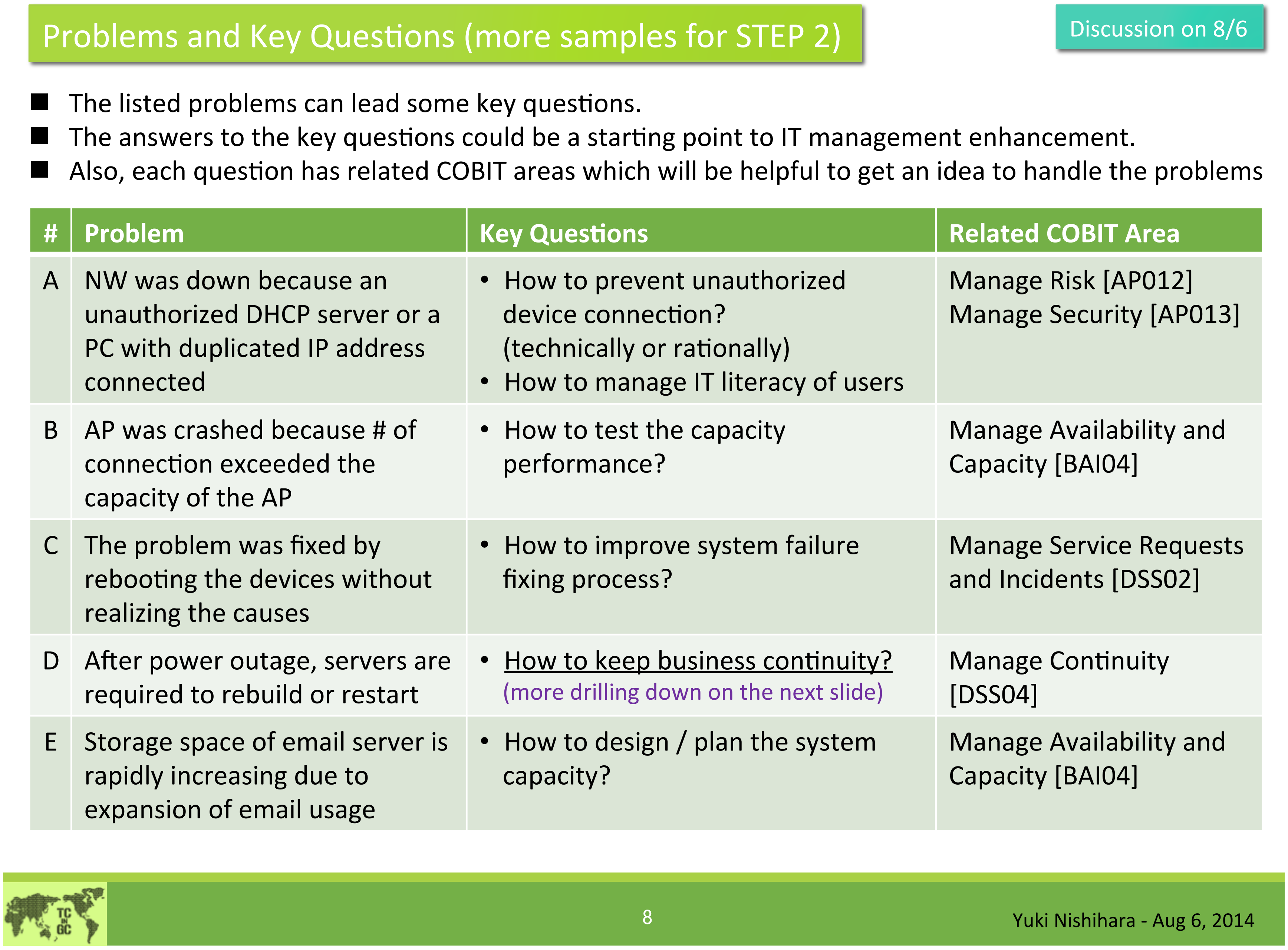
## 2. Plans for Next Half Year

Some initiatives take a time to finish

| | |
|---|---|
| Budget | • Planned Budget… |
| Project Results | • Planned Project / Schedule… |
| System Failures | • Countermeasures against Failures… |
| Human Resource | • Plan for Training… |

## 3. Plans for Mid-term / Long-term

Report (share) these items to managing team regularly will make the future investment easier.



## Problems and Key Questions (more samples for STEP 2)

Discussion on 8/6

- The listed problems can lead some key questions.
- The answers to the key questions could be a starting point to IT management enhancement.
- Also, each question has related COBIT areas which will be helpful to get an idea to handle the problems

| # | Problem | Key Questions | Related COBIT Area |
|---|---|---|---|
| A | NW was down because an unauthorized DHCP server or a PC with duplicated IP address connected | • How to prevent unauthorized device connection? (technically or rationally)<br>• How to manage IT literacy of users | Manage Risk [AP012]<br>Manage Security [AP013] |
| B | AP was crashed because # of connection exceeded the capacity of the AP | • How to test the capacity performance? | Manage Availability and Capacity [BAI04] |
| C | The problem was fixed by rebooting the devices without realizing the causes | • How to improve system failure fixing process? | Manage Service Requests and Incidents [DSS02] |
| D | After power outage, servers are required to rebuild or restart | • <u>How to keep business continuity?</u> (more drilling down on the next slide) | Manage Continuity [DSS04] |
| E | Storage space of email server is rapidly increasing due to expansion of email usage | • How to design / plan the system capacity? | Manage Availability and Capacity [BAI04] |

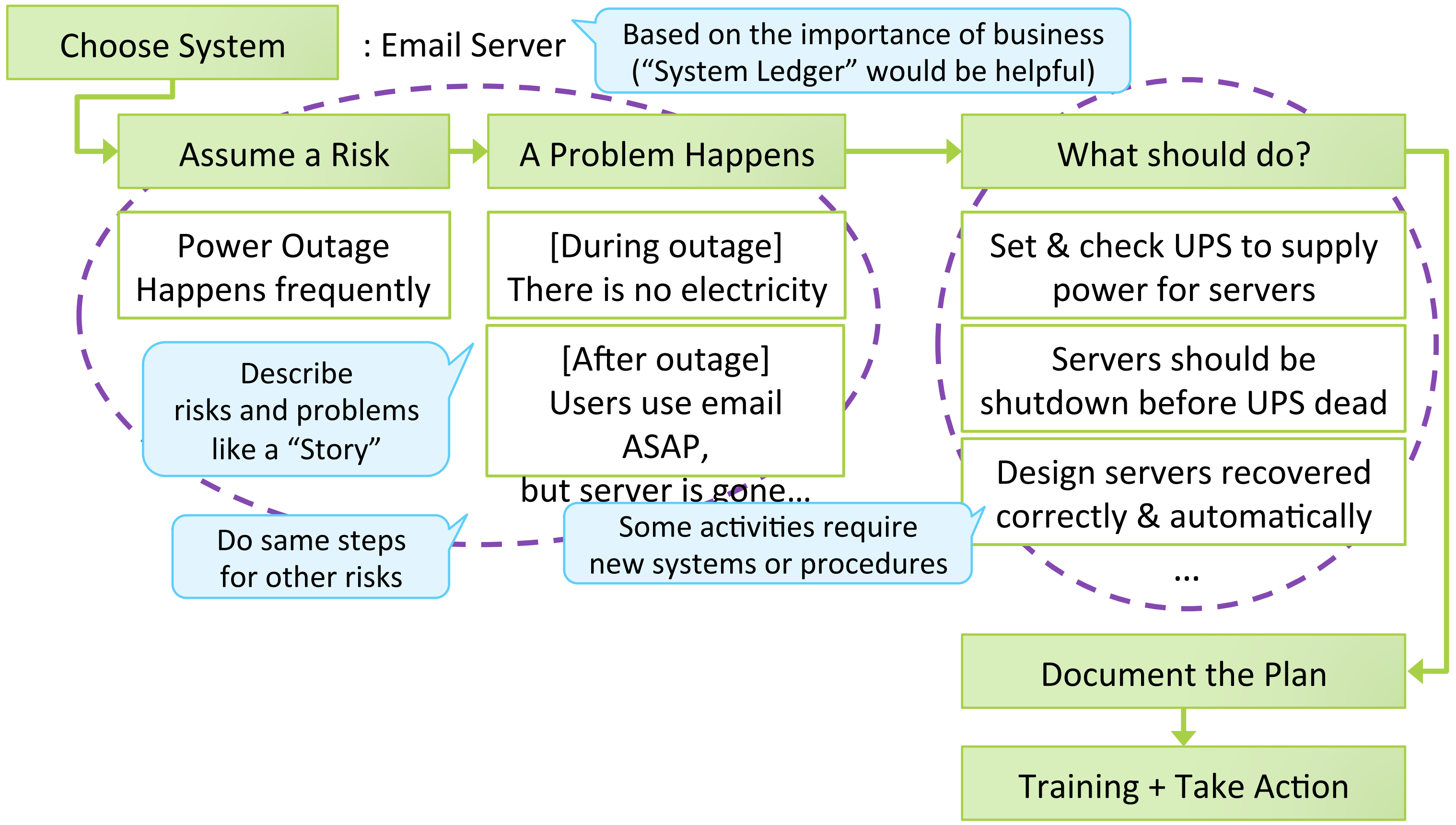
Yuki Nishihara - Aug 6, 2014

# More drilling down the problem (Example)

Discussion on 8/6

## How to keep business continuity?

- Creating a business continuity plan (BCP) or thinking about business continuity will be a good chance to clarify activities in order to strengthen IT services



Choose System : Email Server

Based on the importance of business (“System Ledger” would be helpful)

Assume a Risk

Power Outage Happens frequently

Describe risks and problems like a “Story”

Do same steps for other risks

A Problem Happens

[During outage] There is no electricity

[After outage] Users use email ASAP, but server is gone…

Some activities require new systems or procedures

What should do?

Set & check UPS to supply power for servers

Servers should be shutdown before UPS dead

Design servers recovered correctly & automatically

…

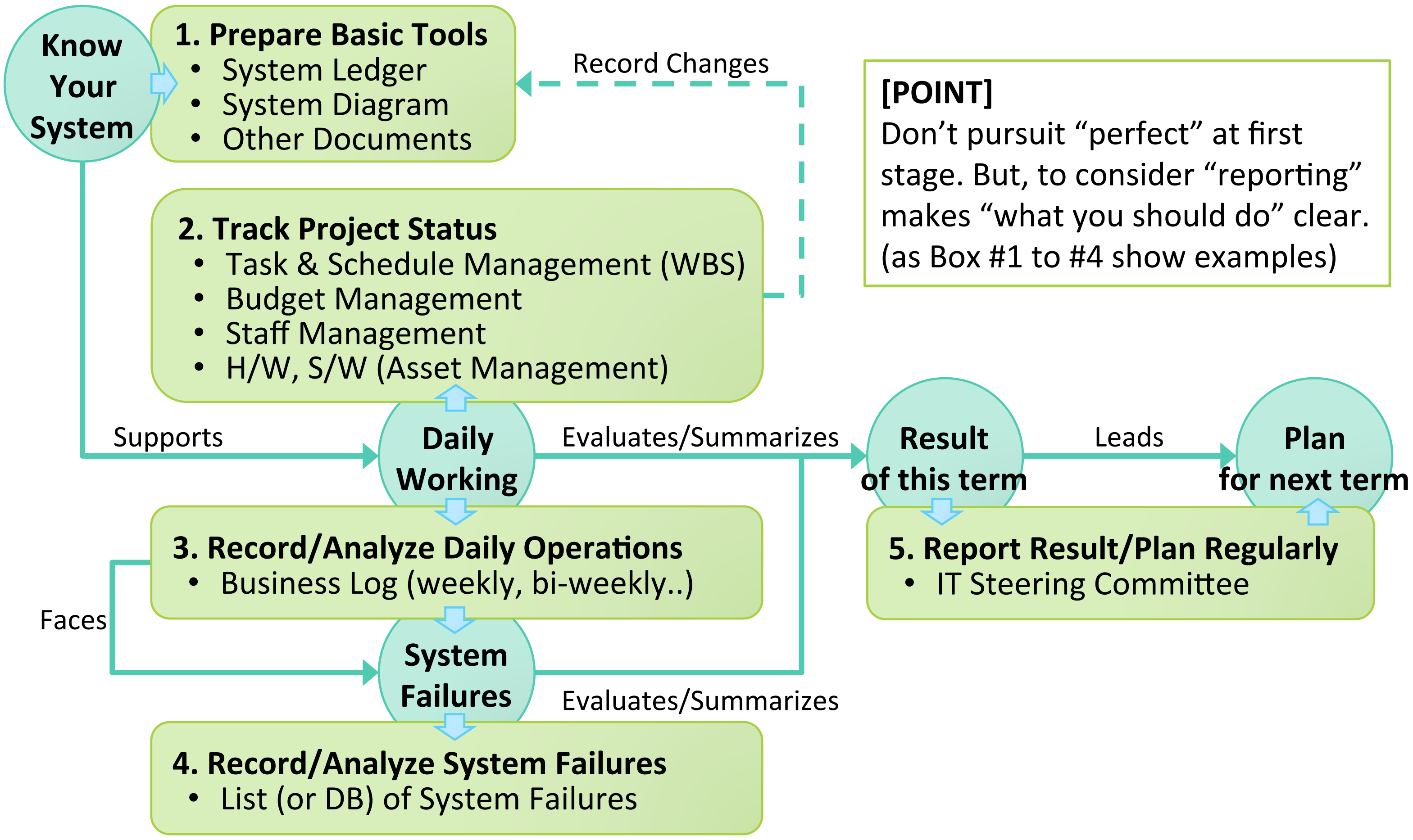
Document the Plan

Training + Take Action

## Starting Point of IT Management Enhancement

Recommendations

- As the first goal, try to **define and store the information** which will be required to **report the result** of “this term” toward the management team of MOE at the end of the term.



**1. Prepare Basic Tools**
- System Ledger
- System Diagram
- Other Documents

**2. Track Project Status**
- Task & Schedule Management (WBS)
- Budget Management
- Staff Management
- H/W, S/W (Asset Management)

**3. Record/Analyze Daily Operations**
- Business Log (weekly, bi-weekly..)

**4. Record/Analyze System Failures**
- List (or DB) of System Failures

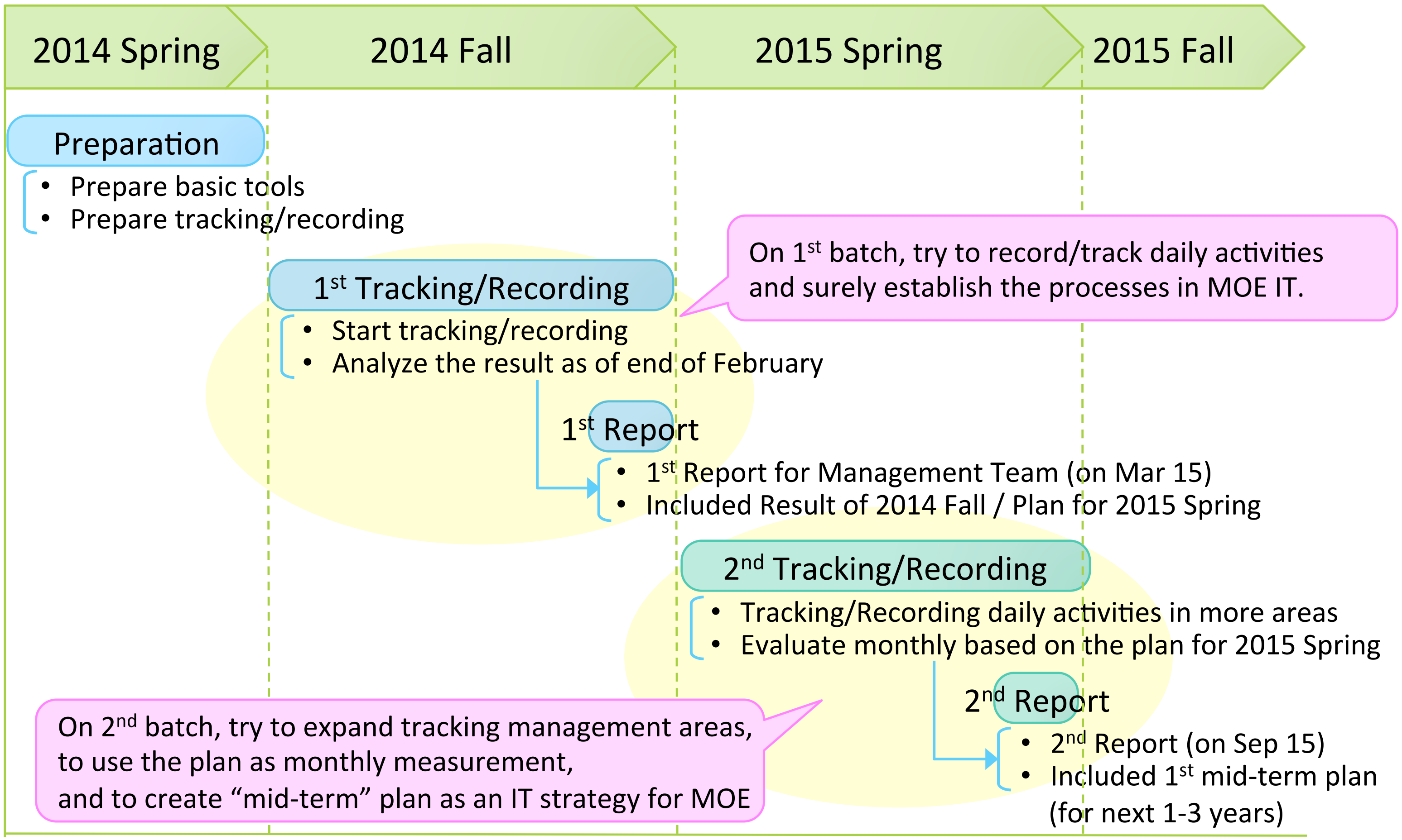
**5. Report Result/Plan Regularly**
- IT Steering Committee

**[POINT]**
Don’t pursuit “perfect” at first stage. But, to consider “reporting” makes “what you should do” clear. (as Box #1 to #4 show examples)

## Starting Point of IT Management Enhancement (Cont.)

Recommendations

- A model schedule could be the following. “Small start” (recording daily activities in the limited area) is recommended; but the result should be reported before end of 2014 Fall.



2014 Spring | 2014 Fall | 2015 Spring | 2015 Fall

Preparation
- Prepare basic tools
- Prepare tracking/recording

1st Tracking/Recording
- Start tracking/recording
- Analyze the result as of end of February

On 1st batch, try to record/track daily activities and surely establish the processes in MOE IT.

1st Report
- 1st Report for Management Team (on Mar 15)
- Included Result of 2014 Fall / Plan for 2015 Spring

2nd Tracking/Recording
- Tracking/Recording daily activities in more areas
- Evaluate monthly based on the plan for 2015 Spring

2nd Report
- 2nd Report (on Sep 15)
- Included 1st mid-term plan (for next 1-3 years)

On 2nd batch, try to expand tracking management areas, to use the plan as monthly measurement, and to create “mid-term” plan as an IT strategy for MOE