WiNOC School Wi-Fi User Access Management Solution Features and Benefits

Author: Frederic Liu

Last update: 2009/03/09

Table of Contents

1. Introduction

WiNOC School Wi-Fi User Access Management System is a total solution designed for school for offering reliable and manageable wireless service in campus. The solution includes school POP3 and RADIUS proxy user account integration, students Internet access authentication, authorization, accounting and auditing, electronic map-based graphical network device management, role-based system administration interfaces, lawful intercept of student Internet access tracking support etc.

The innovative system design integrates “user account management” and “network equipment management” so the system acts as a substitute network administrator that automatically monitors the network’s operation and generates alerts. For wireless users (including students, faculty, staffs and visitors) with various mobile devices, the system provides them with several authentication methods for different kind of mobile application. IEEE802.1x / PEAP method is for the application requires high transmitting security; UAM (Web-redirection) method is the most user-friendly way for the student with limited IT knowledge; MAC address authentication is for the mobile device with limited function to support advanced authentication method; SMS registration method is for the campus visitors require temporary Internet access. By supporting fully automated account management and integration with the existing POP3 or RADIUS servers, the system offers an effective way to reduce a school’s maintenance costs.

1.1. Benefits

The system not only creates values for IT but also all the parties involving school wireless access service. The Fig. 1: WiNOC benefits diagram describes the benefits of the solution to these parties.

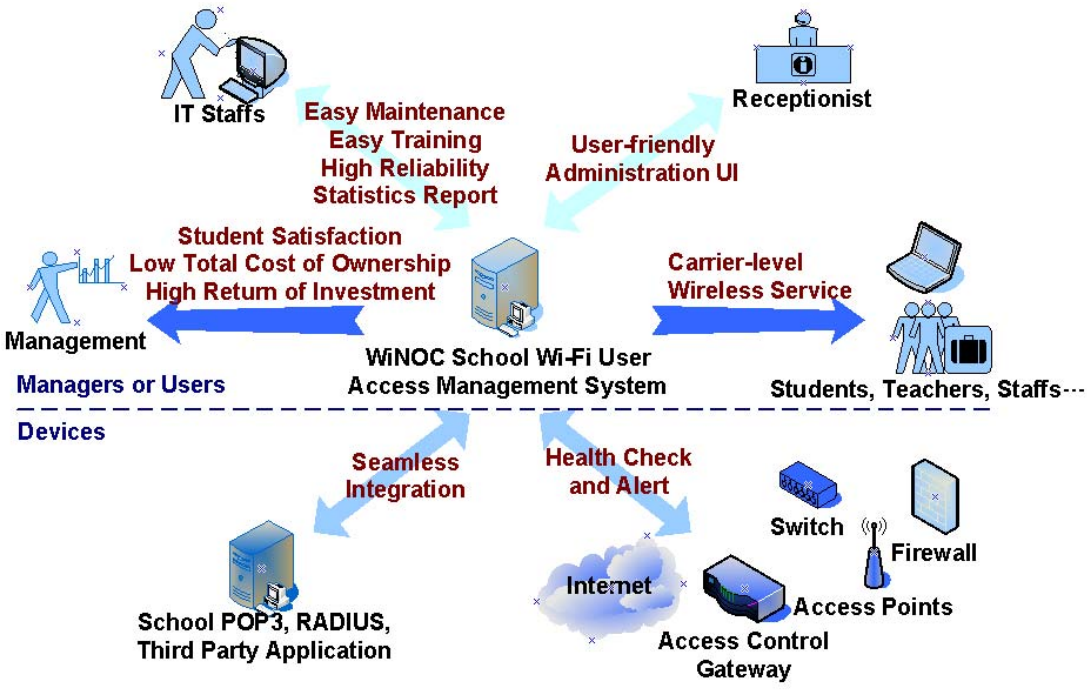


Fig. 1: WiNOC benefits

1.2. Reference Sites

- Management of 750+ Orinoco access points as well as wireless AAA (w/ 2000+ users) in **National Taiwan University of Science and Technology** (http://www.ntust.edu.tw), Taipei City, Taiwan.
- Management of Orinoco and Aruba access points as well as IEEE 802.1x PEAP wireless user access control supporting user roles including teacher, student, employee, visitor and guest, etc, in a military-based hospital and university.
- Management of 35 Cisco access points, 37 InterEpoch access points as well as wireless AAA (w/ 6400+ users) in **Taipei Commercial College** (http://www.slsh.tpc.edu.tw/), Taiwan.
- Billing for Internet access service in **Shangri-la Far Eastern Plaza Hotel Taipei** (http://www.feph.com.tw/) with Fidelio Opera PMS integration.
- Billing for Internet access service in the **Grand Hi-Lai Hotel Kaohsiung** (http://www.grand-hilai.com.tw/) with PMS integration.
- Billing for Internet access service in the **MGM GRAND Macau Hotel** (http://www.mgmgrandmacau.com/) with Fidelio Opera PMS integration.
- More…

2. Solution Network Architecture

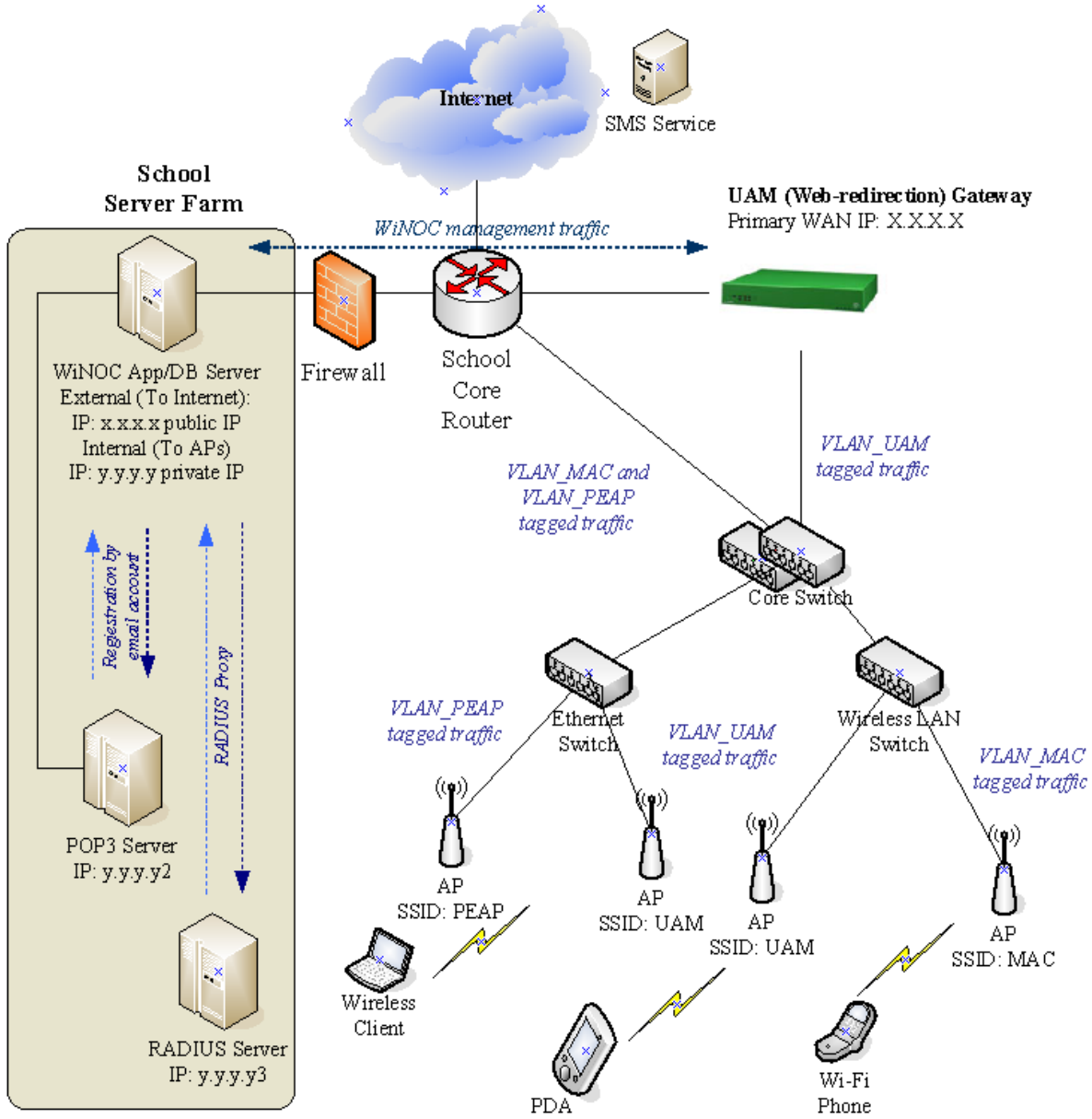


Fig. 2. Solution network architecture

The network architecture of WiNOC School Wi-Fi User Access Management System is composed of the following facilities:

- *POP3 Server:* The Email POP3 server of school students, teachers and staffs, which WiNOC integrates to verify the wireless access credential during the very first log-in of the school students, teachers and staffs.

- *External RADIUS Server:* The RADIUS server of external or other internal user account system, which the accounts of both parties could be roamed for wireless access login at each other's wireless coverage.

- *WiNOC*: The WiNOC School Wi-Fi User Access Management System, which integrates with POP3 server for school user account credential synchronization. Also, WiNOC works with UAM Gateway to redirect school Welcome portal for wireless users to register and log in campus wireless service, control bandwidth utilization, etc. And, WiNOC works with wireless access points and wireless LAN switches to control wireless user access by IEEE802.1x/PEAP or RADIUS MAC authentication.

- *Firewall*: The device that protects wireless network and WiNOC from being hacked by malicious users.

- *Ethernet Switch*: The Ethernet switch should support IEEE 802.1q VLAN tagging feature. Each SSID with different authentication method should map to a specific VLAN ID of the network for controlling.

- *Wireless LAN Switch and Access Point*: The wireless front-end access control device should support multiple SSID with independent VLAN ID. The first SSID (PEAP) provides IEEE802.1x/PEAP authentication is for the application requires high transmitting security; the second SSID (UAM) provides Web portal redirection login method is the most user-friendly way for the student with limited IT knowledge; the third SSID (MAC) provides RADIUS MAC address authentication is for the mobile device with limited function to support advanced authentication method.

- *UAM Gateway*: The UAM AAA access control gateway. It works with WiNOC to authenticate users trying to access the wireless and control bandwidth utilization via web portal redirection technology.

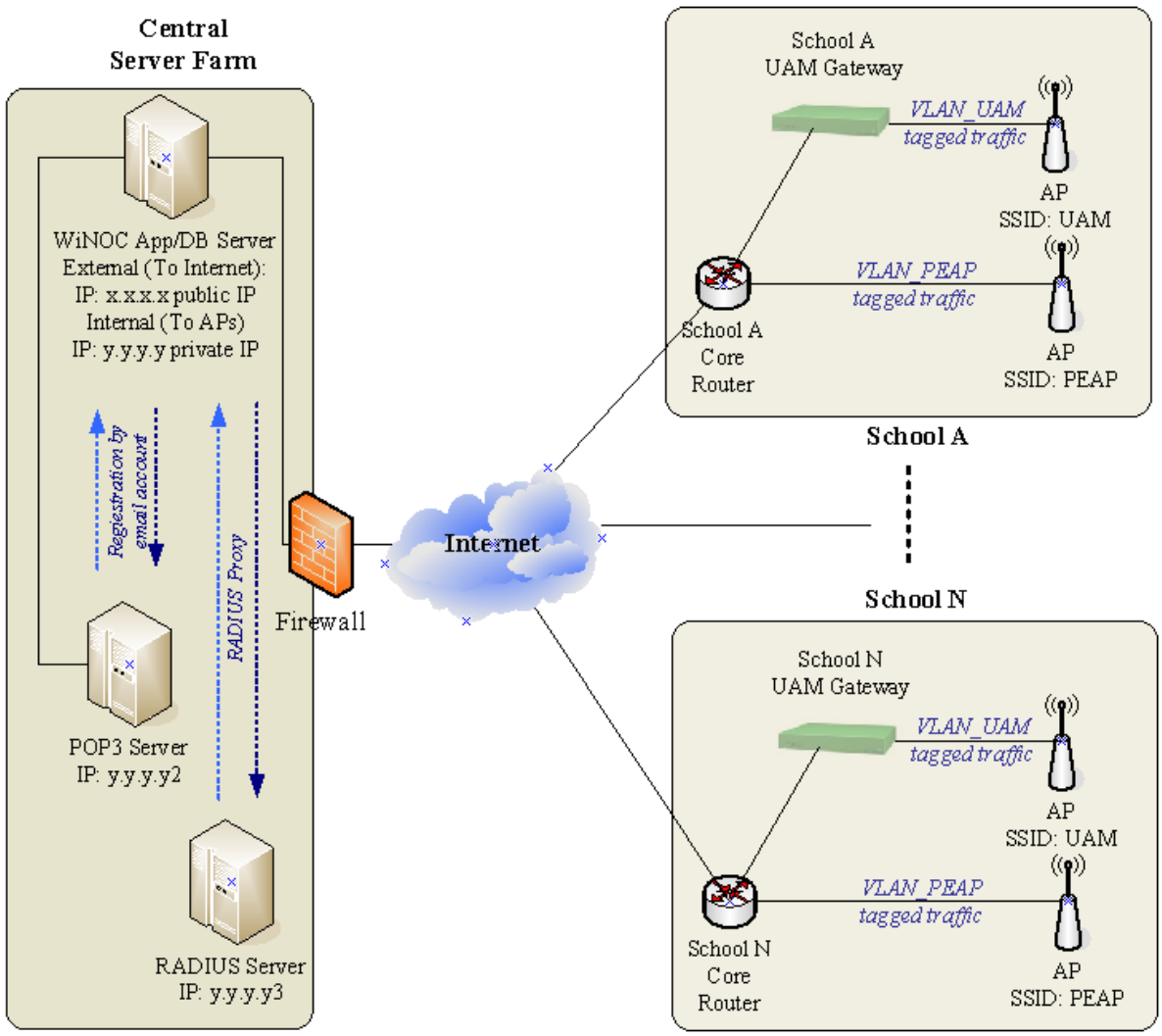


Fig. 3: Central Management Architecture

On the Fig. 3, WiNOC could be the central device and user access management server of multiple schools.

3. Solution Features and Advantages

3.1. For Wireless Users

A. Provide various Wi-Fi access authentication by few-steps registration

The first log-in wireless users could just input his/her mail username and password for verification on web-based registration pages. After the step-by-step registration, the user could log in wireless via various authentication ways according to the user's mobile application.

Windows XP/Vista build-in IEEE802.1x / PEAP with TKIP and AES (WPA and WPA2) method is for the application requires high transmitting security. Wi-Fi Protected Access (WPA and WPA2) is a certification program administered by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks.

UAM (Web-redirection) method is the most user-friendly way for the wireless users with limited IT knowledge. The users launch a regular web browser to access a login page on the captive portal where user can input in the credentials (typically his username and password) to get access to the network.

Note: *For UAM, it's required the network equipment with UAM functionalities (such as Nomadix™ Access Gateway) in the network to control the access.*

	IEEE 802.1x/PEAP	UAM (Web redirection)
Software requirement	Require IEEE802.1x client utility (Windows XP has build-in utility)	Internet browser
Software configuration	Need more steps to configure at the first usage only.	Easy to configure. But need to input username and password at each log-in.
Wireless data encryption	Dynamic WEP or TKIP key encryption	No encryption protect
Access Control Point	Access Points	Access control gateway

Fig. 4: The Comparison of IEEE802.1x/PEAP and UAM authentication

RADIUS MAC address authentication method is for the mobile device with limited function to support advanced authentication method. For out-of-date mobile devices or limited-function devices which don't support either IEEE802.1x/PEAP or UAM

authentication, the wireless users could register the MAC addresses of the devices into WiNOC for wireless access. The WiNOC will authenticate the access by the registered MAC addresses without inputting username and password during access login.

Note: *For RADIUS MAC authentication, it's required the access point or UAM gateway to support RADIUS MAC authentication function. Normally, there is no wireless data encryption protection support.*

B. Bandwidth Management

The WiNOC policy-based bandwidth management feature enables bandwidth control on a per guest basis such as for normal users 512/512 kbps and for VIP users 1M/1M. The service level could be specified by the user's group. The bandwidth limitation will be applied to AP or UAM gateway after the user is logged in.

Note: *For WiNOC policy-based bandwidth management, it's required the access point or UAM gateway to support RADIUS vendor specific attribute or WISPr RADIUS attribute for user-based bandwidth control.*

3.2. For Operation and Customer Service

A. User-friendly welcome portal provides maximal branding benefits

WiNOC provides welcome portal log-in pages customization service for the wireless users' pleasant experience. The welcome portal could be design to follow the school's standard of artwork and procedures. It is multilingual support according to school's requirement.

B. File-Explorer-Like administration interface

User-friendly and File-Explorer-Like Web-based administration interface for school IT, administration staffs easy to be trained and learned (Multilingual support). Web-based management interface could be accessed by any computer on the Internet or the intranet.

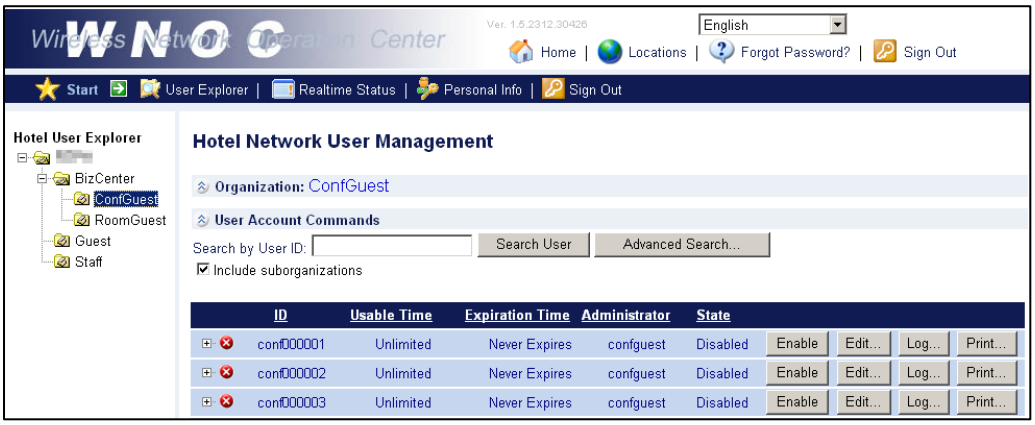


Fig. 5: File-Explorer-Like administration interface

C. Flexible and definable role-based administration authorization control

Support to apply school authorization policy such as IT has full permissions, administration has limited permissions and auditor has read-only permission.

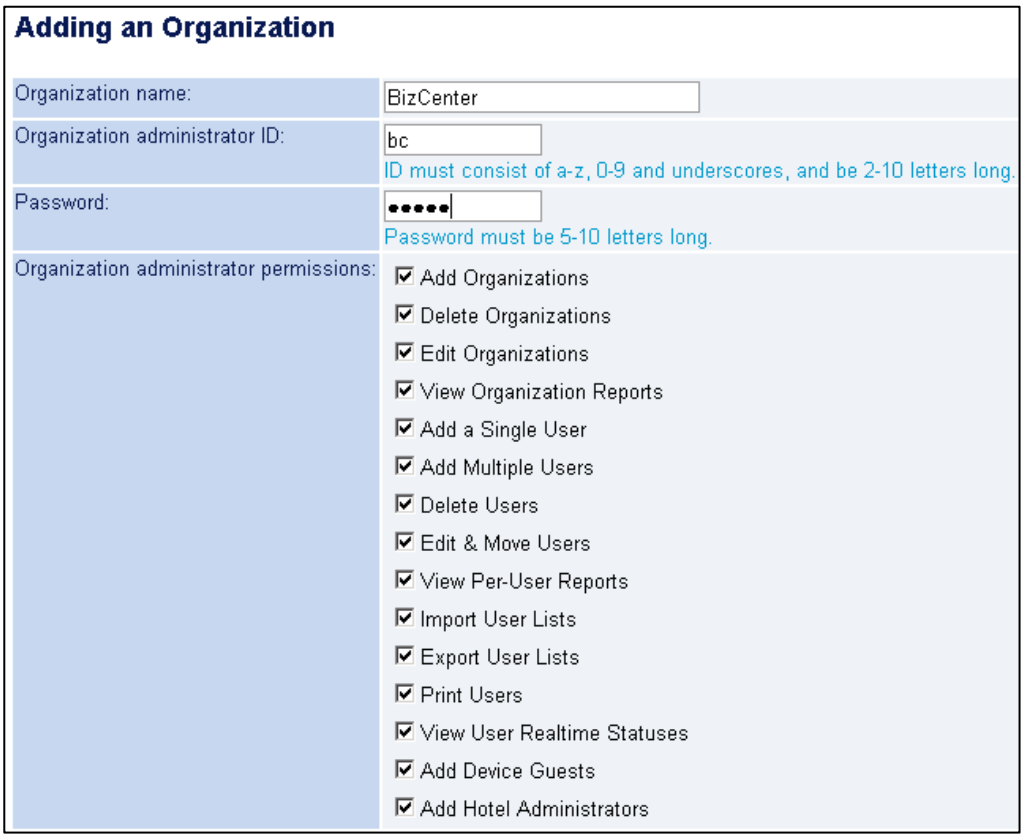
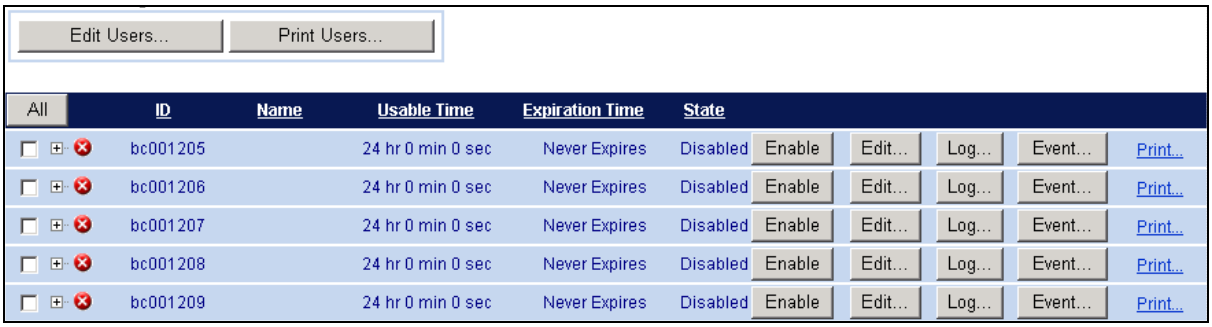
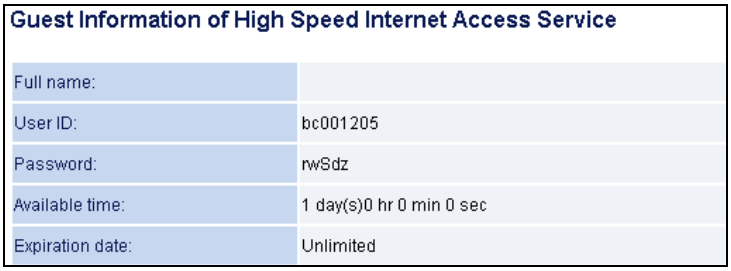


Fig. 6: Role-based administration authorization control

D. Definable temporary accounts for school visitors

The school IT or administrators could enable and print a temporary account via the Web-based Interface to give away to allow school visitors who don't have school mail account for registration to access wireless Internet using the credentials on the print-out sheet.





Guest Information of High Speed Internet Access Service

Full name:	
User ID:	bc001205
Password:	rwSdz
Available time:	1 day(s)0 hr 0 min 0 sec
Expiration date:	Unlimited

Fig. 7: Temporary accounts for visitors

For conference event, also support batch account properties editing (account enable/disable state, password and access plan) and batch account information printing (account ID, password, usable minutes and expiration time etc) via web-based administration user interface.

For the school with the policy to provide free wireless Internet to public, the public user could register a new account by the mobile phone number. The pass code of the new account will be sent via SMS to the mobile phone for the registration confirmation. Then, the school could trace the public user by mobile phone number.

E. Detailed event logs of wireless users' status for troubleshooting

WiNOC provides several event logs for tracking "wireless user account registration", "wireless user login/logout", etc. Information recorded in these logs is extremely useful when troubleshooting.

S/N	Type	Time	Source	Category	Account ID	Event	User	Computer	Description
688800		4/13/2007 9:08:55 PM	WNOC	ServicePurchase	3510	1	(User)	HSIA_WNOC	Hotel guest purchase Internet service succeeded. Access plan ID: 2; Bandwidth: 768Kbps/768Kbps; Duration: 1440 min; Charge: NTD$600 Login password: kreiling; IP Up-Sell: False
688799		4/13/2007 9:08:22 PM	IAS	AccessReject	3510	1	N/A	hsia_wnoc	User "3510 (00-18-DE-83-E7-FC)" rejected by IAS
688798		4/13/2007 9:08:22 PM	IasExAuth	AccessRequest	3510	1	N/A	hsia_wnoc	User "3510 (00-18-DE-83-E7-FC)" rejected because nonstopped accounting account expired

Fig. 8: WiNOC detailed event log for troubleshooting

3.3. For School IT Support

A. Lawful Intercept of wireless client Internet access tracking

The UAM gateway may provide tracking IP logs, which can be enabled to track all the TCP/IP sessions of the users accessing a public network. These tracking logs enable IT to trace-back to a particular MAC address and username based on port and IP address information of the external site that has been attacked, hacked or used in an illegal way.

WiNOC build-in Syslog server enables the IT to store and manage the lawful intercept tracking logs in the database server. WiNOC build-in RADIUS server also keeps wireless

user's log-in/log-out time, MAC address, IP address, port number, transmitted bytes and usage time in database for tracking, statistics and analysis.

Login Time	Logout Time	Used Time (sec)	In Data (KB)	Out Data (KB)	Location	Region	MAC Address
11/17/2008 5:55:05 PM					MachineRoom	FEPH	00-17-42-85-34-47
11/17/2008 9:30:43 AM	11/17/2008 2:30:48 PM	18005	2228	8719	MachineRoom	FEPH	00-17-42-85-34-47
11/16/2008 12:22:46 AM	11/17/2008 9:30:23 AM	119257	24024	527307	MachineRoom	FEPH	00-1A-80-D7-27-5E
11/14/2008 9:49:41 PM	11/16/2008 12:22:46 AM	95585	12072	45324	MachineRoom	FEPH	00-17-42-85-34-47
11/13/2008 4:51:51 PM	11/14/2008 8:43:52 AM	57121	6436	11441	MachineRoom	FEPH	00-17-42-85-34-47

Fig. 9: Lawful Intercept of guest Internet access tracking

B. Manage multiple UAM gateways, WLAN switches and access points

According to the schools network planning and policy, WiNOC enables the school to manage multiple wireless access control devices which might be located within the same campus or different campuses. The wireless user account roaming between the multiple wireless access control devices could be supported. The wireless users could access wireless network with the same username and password across these wireless coverage areas.

C. Network devices monitoring and management

WiNOC device health monitoring function supports background network devices (such as UAM gateway, Firewall, Ethernet switch and AP) health monitoring and anomaly alerting by Email. WiNOC device status monitoring feature enables SNMP-based device status and performance statistics reporting and analysis.

School IT specialists can scan floor plans as JPG, GIF, or PNG files and upload them to WiNOC. Then, the positions of the wireless access points can be marked on the floor plans, so that these devices can be managed graphically and easily. The Google map integration is also supported for large-scale outdoor devices management.

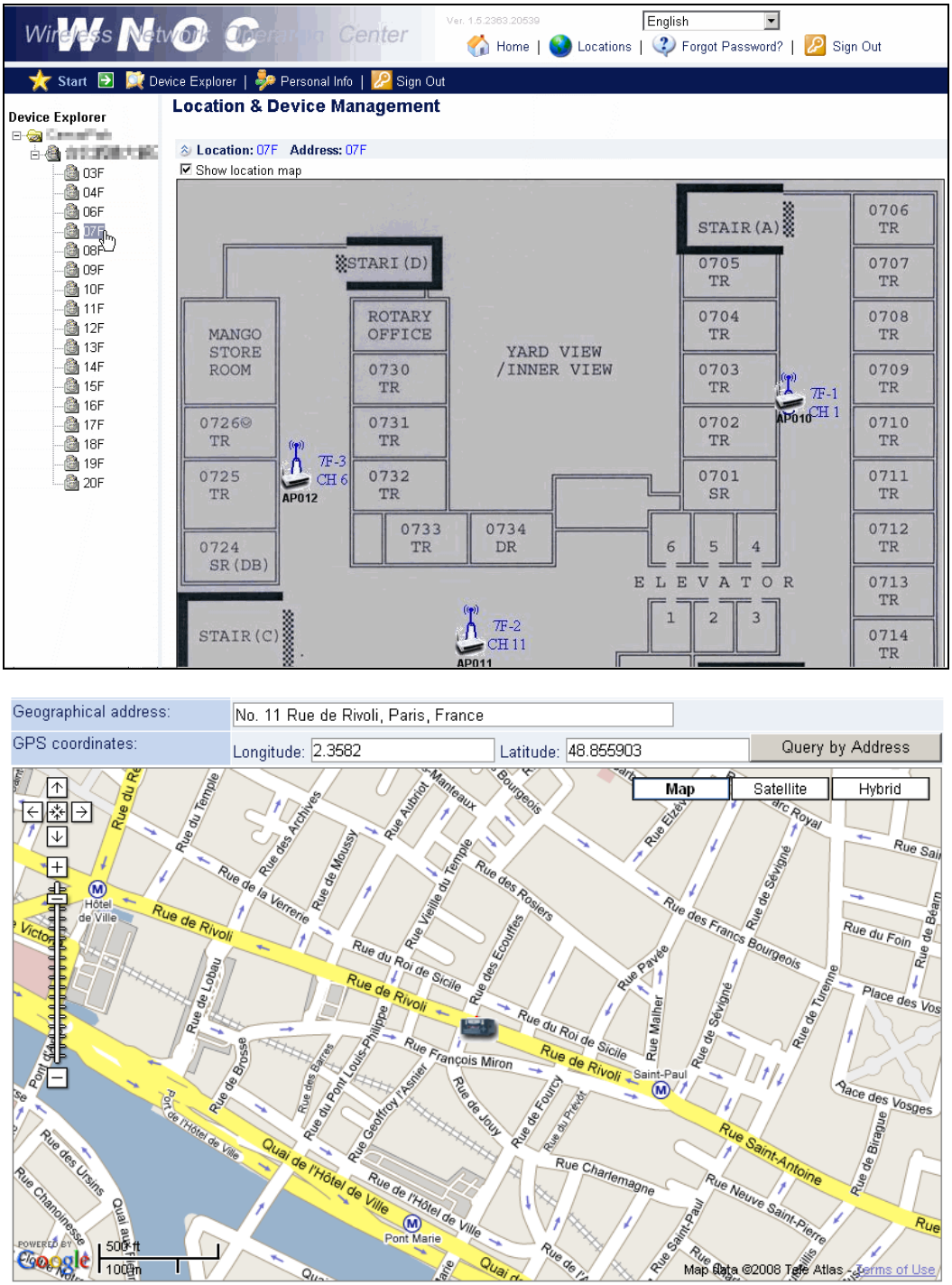


Fig. 10. Managing network devices graphically

D. Assign specific authorization and service level according to the user group

Besides assigning the session timeout, idle timeout and bandwidth limitation, the VLAN ID could be assigned to individual user account according to the user group or the authentication method. The user would be authorized the privilege of campus network access by the assigned VLAN ID. For example, the visitor account could only be allowed to access Internet (No campus Intranet) with 256K/256K bandwidth.

Note: *For WiNOC VLAN assignment, it's required the access point, WLAN switch or UAM*

gateway to support RADIUS standard or vendor specific attribute for user-based VLAN assignment.

	SSID	SSID Broadcast	Authentication method	Authorization
Staff	staff	Public	802.1x/PEAP	VLAN11_Staff, Internet, Intranet....
External roaming user	roam	Public	802.1x/PEAP	VLAN12_External, Internet
Guest	guest	Public	UAM/PAP	VLAN13_Guest, Internet
VoIP device	VOIP	Hidden	MAC address	VLAN14_VoIP, Intranet
RFID device	RFID	Hidden	MAC address	VLAN15_RFID, Intranet

Fig. 11: The authorization table for different user group or authentication method

E. Various Statistics Reports

WiNOC's "Report Wizard" provides various types of reports on how the system performs during a specified period of time. These reports can be used as a basis for correcting operational strategy of the Internet access service. The Report Wizard can generate the following reports:

- **Per user, by-Interval distribution graph** for the number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-location top *n* billboard graph** for the number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-hour top *n* billboard graph** for the number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-week top *n* billboard graph** for the number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-month top *n* billboard graph** for the number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-year top *n* billboard** for the number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-location text report** for the total/average number of user online sessions, used time, uploaded bytes, or downloaded bytes

- **By-hour text report** for the total/average number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-week text report** for the total/average number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-date text report** for the total/average number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-month text report** for the total/average number of user online sessions, used time, uploaded bytes, or downloaded bytes
- **By-year text report** for the total/average number of user online sessions, used time, uploaded bytes, or downloaded bytes

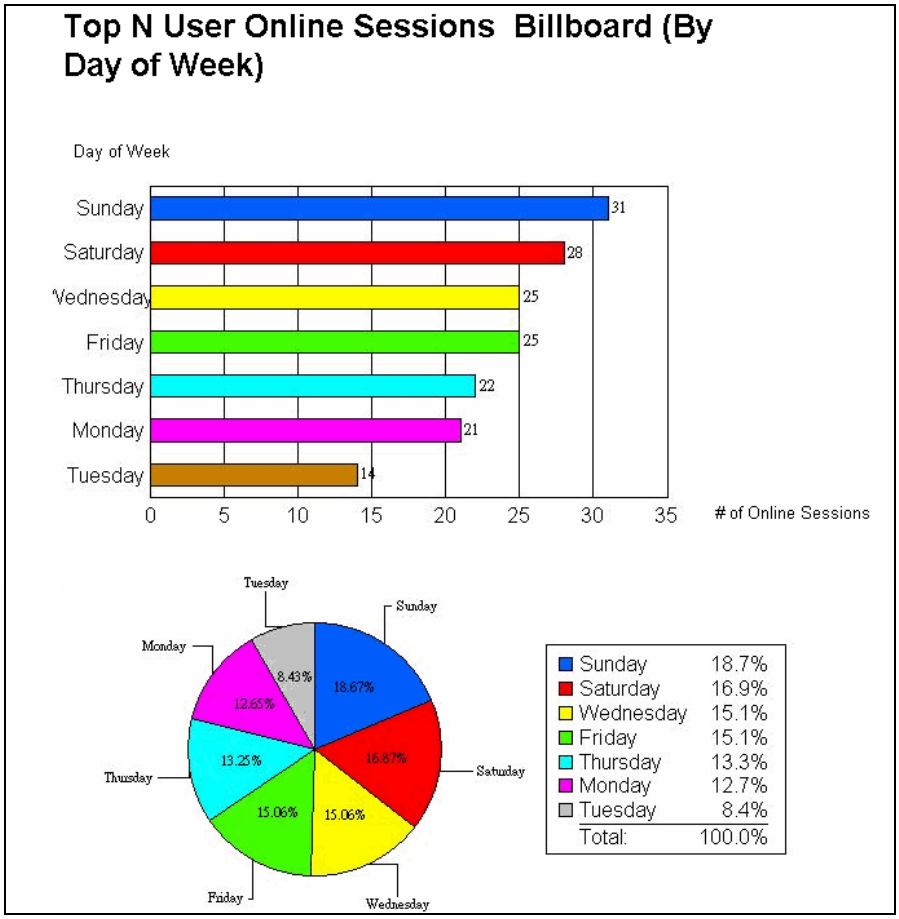


Fig. 12. Graphical statistics report

F. Hierarchically grouping administration accounts, user accounts and devices

WiNOC File-Explorer-like administration interface supports hierarchically grouping administration accounts, user accounts and devices by organization and location for flexible role-based authorization of different deployments. For example, headquarter could manage all user accounts and devices of all branches. The branch A could only manage the user accounts and devices under the branch A's organization folder.

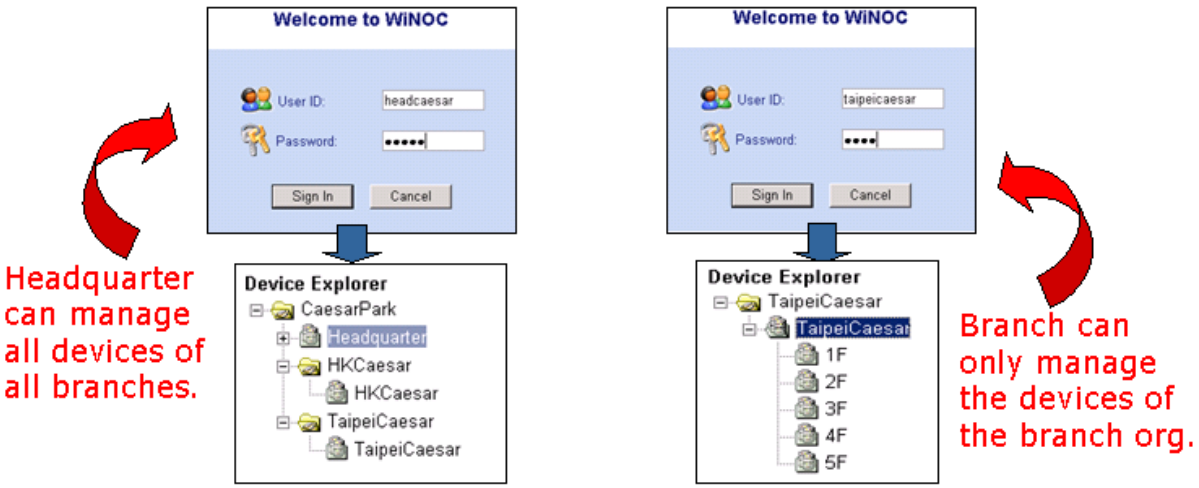


Fig. 13: Hierarchically grouping administration

G. Support for high availability

By using WiNOC's Server Clustering functionality, multiple WiNOC servers can be used to provide nonstop service.