

# Samsung WLAN

Day 2



# Day 2 Outline



#### 1. Lab Exercise

• 1.1 Complete Rebuild

#### 2. APC and AP Troubleshooting

- 2.1 System Logs
- 2.2 Station Tracking
- 2.3 Packet Capture
- 2.4 Tech Support

#### 3. Advanced Deployment

- 3.1 Remote AP
- 3.2 Internal Radius Server
- 3.4 Quality of Service
- 3.5 VQM
- 3.6 Root and Repeater AP
- 3.7 SNMP

#### 4. Security

- 4.1 Firewall / ACL
- 4.2 Captive Portal
- 4.3 Web Passthrough
- 4.4 Conditional Web Redirection



- 1. Lab Exercise
- 1.1 Complete Rebuild

Use the WLAN\_day2morning\_LAB to complete Please complete this lab by 12:00pm. The instructor is here to help



# 2. APC and AP Troubleshooting

- 2.1 System Logs
- 2.2 Station Tracking
- 2.4 Tech Support
- 2.5 Interference Devices
- 2.6 Rogue AP's and Stations



# Alarm/Event Debug log/detailed log

### 2.1 System Logs

#### ALARM

WEC8500# show	w alarm info
1 system	MAJ Software Down
2 system	MAJ Cpu Load Alarm
3 system	MAJ Memory Usage Alarm
4 system	MAJ Disk Usage Alarm
5 system	MAJ Fan Rpm Alarm
6 system	CRT System Temperature Alarm
7 system	CRT System Thermal Runaway
8 system	MAJ DHCP Sever Connect Failure
9 system	MAJ DNS Server Connect Failure
10 system	MAJ NTP Server Connect Failure
11 system	CRT Fan Fail alarm
12 system	CRT Temperature Sensor Fail
13 system	MAJ Power Module Fail
14 ap	CRT Duplicated IP
15 ap	CRT No Radio
16 ap	CRT License Expired
17 ap	MAJ BSS INTERFACE DN
18 ap	MAJ AP
19 ap	MAJ AP CPU Load High
20 ap	MAJ AP MEM Usage High
21 ap	MAJ AP Monitor Device Fail
22 ap	MAJ AP RADIO CARD TX FAIL
23 ap	MIN AP CHANNEL BUSY
24 ap	MAJ AP DISK USAGE HIGH
25 wifi	MIN CAC Minor Calls
26 wifi	MAJ CAC Major Calls
27 wifi	MAJ CLUSTER APC Lost Connection
28 security	CRT Radius Servers Failed
29 network	MAJ NET Link dn
30 se	MIN SE VQM Excess Burst
31 se	MIN SE VQM Excess Delay
32 se	MIN SE VQM Low MOS
33 se	CRT SE NFM SE_RESTART

#### WEC8500# show alarm conf

Alarm Log Configuration		1guration
Alarm Group FilterallAlarm Level FilterminorAlarm Log File Size10 MBytesAlarm Log File Count2Alarm Log STD OutOff	p Filter l Filter File Size File Count STD Out	all minor 10 MBytes 2 Off

#### WEC8500# show alarm list all 2013-04-02 10:54:34 MAJ APC Power Module Fail POWER0 1 system 2 network 2013-04-02 10:54:31 MAJ APC ge6 NET Link dn AdminStatus[up] OperStatus[down] 3 network 2013-04-02 10:54:31 MAJ APC ge5 NET Link dn AdminStatus[up] OperStatus[down] 4 network 2013-04-02 10:54:31 MAJ APC ge7 NET Link dn AdminStatus[up] OperStatus[down] 5 network 2013-04-02 10:54:31 MAJ APC xe2 NET Link dn AdminStatus[up] OperStatus[down] 6 network 2013-04-02 10:54:31 MAJ APC ge8 NET Link dn AdminStatus[up] OperStatus[down] 7 network 2013-04-02 10:54:31 MAJ APC xel NET Link dn AdminStatus[up] OperStatus[down] 8 network 2013-04-02 10:54:29 MAJ APC mgmt0 NET Link dn AdminStatus[up] OperStatus[down]

#### WEC8500# show alarm list ?

all	Display the list of active alarms
group	Display the list of active alarms for
	specific group
level	Display the list of active alarms for
	Specific fever

## 2.1 System Logs



#### # Alarm Log Size(Default : 10MBytes) is occupied by event messages

#### # Event messages include Alarm messages

#### Alarm Configuration

#### WEC8500/configure# alarm ?

backupIP	Configure backup AP controller IP address
current-terminal	Configure logging alarms on/off for a current terminal
dump	Convert alarm log DB to dump txt file
group	Configure alarm for specific group
level	Configure alarm for specific level
logcount	Configure the number of backup file for alarm log (Default : 2)
logsize	Configure file size for alarm log
stdout	Configure standard out on/off for all terminals

#### WEC8500# show alarm history all

1 network	2013-04-04 18:41:10 MAJ APC ge4 NET Link dn Clear AdminStatus[up] OperStatus[up]
2 network	2013-04-04 18:41:06 MAJ APC ge4 NET Link dn Declare AdminStatus[up] OperStatus[down]
3 network	2013-04-04 18:40:49 MAJ APC ge1 NET Link dn Clear AdminStatus[up] OperStatus[up]
4 network	2013-04-04 18:40:43 MAJ APC gel NET Link dn Declare AdminStatus[up] OperStatus[down]
5 network	2013-04-04 18:40:29 MAJ APC ge1 NET Link dn Clear AdminStatus[up] OperStatus[up]
6 network	2013-04-04 18:40:16 MAJ APC ge1 NET Link dn Declare AdminStatus[up] OperStatus[down]
7 network	2013-04-04 11:35:05 MAJ APC vlan1.2202 NET Link dn Clear AdminStatus[up] OperStatus[up]
8 network	2013-04-04 11:34:11 MAJ APC vlan1.2201 NET Link dn Clear AdminStatus[up] OperStatus[up]
9 network	2013-04-02 10:54:43 MAJ APC vlan1.1 NET Link dn Clear AdminStatus[up] OperStatus[up]

#### Show Event

WEC8500# show	event
1 network	11:26:13 NOT APC IP Duplication detect IP:1.111.60.63 MAC:94:63:d1:a5:34:63 Interface:vlan1.1217
2 network	11:26:12 NOT APC IP Duplication detect IP:1.111.60.63 MAC:94:63:d1:a5:34:63 Interface:vlan1.1217
3 wifi	11:24:36 NOT RRM DPC RUN Dynamic power control done [2.4GHz]
4 wifi	11:24:35 NOT RRM DPC RUN Dynamic power control done [5GHz]
5 network	11:21:02 NOT APC IP Duplication detect IP:1.110.19.18 MAC:0c:df:a4:2b:6f:97 Interface:vlan1.1212
6 network	11:21:01 NOT APC IP Duplication detect IP:1.110.19.18 MAC:0c:df:a4:2b:6f:97 Interface:vlan1.1212
7 network	11:19:59 NOT APC IP Duplication detect IP:1.111.195.49 MAC:0c:df:a4:2c:7f:67 Interface:vlan1.1202
8 network	11:19:58 NOT APC IP Duplication detect IP:1.111.195.49 MAC:0c:df:a4:2c:7f:67 Interface:vlan1.1202
9 wifi	11:14:37 NOT RRM DPC RUN Dynamic power control done [2.4GHz]
10 wifi	11:14:35 NOT RRM DPC RUN Dynamic power control done [5GHz]

### 2.1 System Logs



#### Debug Log / Log Detail

#### WEC8500# show debug processes

Processes Debug Info.

id	name	pid	runmode	argument
0	swmmon	1719	exec-ever	
1	db	1720	exec-ever	
2	evm	1746	exec-ever	
3	evmlogd	1747	exec-ever	
4	license	1748	exec-ever	
5	pcap	1749	exec-ever	
26	hostapd	2458	exec-ever	
27	wids	2459	exec-ever	
28	guestService	2460	exec-ever	
29	eqm	2461	exec-ever	
30	vqm	2462	exec-ever	
31	irfm	2463	exec-ever	
32	rfsgw	2546	exec-ever	
33	apclt	2581	exec-ever	
34	pm	2582	exec-ever	
35	sipalg	2585	exec-ever	
36	httprd	2591	exec-ever	
37	snmpd	2625	exec-ever	-z
/tr	mp/SNMP/OIDInf	oDataFile	e.CPS	
38	WebAgent	2626	exec-ever	-z
/tr	mp/SNMP/OIDInf	oDataFile	e.CPS	
39	salh	2627	exec-ever	
40	ipwlogd	2628	exec-ever	
41	nfm	2629	exec-ever	
42	cron	1533	monitor-only	
43	syslogd	1521	monitor-only	
44	klogd	1525	monitor-only	
45	ui	2696	exec-ever	

#### WEC8500# show debug log conf

Debug Log Configuration	
Debug Log Mode	On
Debug Log Module Filter	all
Debug Log Level Filter	warning
Debug Log File Size	10 MBytes
Debug Log File Count	2
Module STD Out	Off
Module Filter STD Out	all
Module Level Filter STD Out	debug

#### WEC8500# show debug log detail conf

Debug	Detail Log Configur	ation
Debug Detail	Log Mode	On
Debug Detail	Log Module Filter	all
Debug Detail	Log Level Filter	information
Debug Detail	Log File Size	100 MBytes
Debug Detail	Log File Count	2
Debug Detail	Log STD Out	Off

#### WEC8500# debug log ?

detail	Log debug in detail
dump	Convert legacy DB debug file to txt file
level	Configure debug message for specific level
logcount	Configure the number of backup file for debug log
logsize	Configure file size for debug log
module	Configure debug message for specific module
mstdout	Configure the module Standard Out on/off for debug message
off	Configure debug log off
on	Configure debug log on

```
npi_wec8500# configure terminal
npi_wec8500/configure# alarm stdout on
Alarm Log STDOUT On
npi_wec8500/configure# *2013-11-21 13:05:59 #wifi-NOT: RRM DCS RUN APC Notice
[Normal Run] Dynamic channel selection done [5GHz]
*2013-11-21 13:07:00 #wifi-NOT: RRM DCS RUN APC Notice [Normal Run] Dynamic channel
selection done [2.4GHz]
*2013-11-21 13:07:59 #wifi-NOT: RRM DCS RUN APC Notice [Normal Run] Dynamic channel
selection done [5GHz]
npi_wec8500/configure# alarm stdout off
Alarm Log STDOUT Off
npi_wec8500/configure#
```

# System Logs "Lab 16"



### Lab 16 -

#### Telnet into the APC and look at System logs

- 1. Telnet to the APC "192.168.xx.10"
- 2. Practice with these show commands "Alarms" WEA8500#
  - 1. show alarm info
  - 2. show alarm conf
  - 3. show alarm list all
  - 4. show alarm list ?
  - 5. show alarm history all
  - 6. show event
- 3. Go to configure mode  $\rightarrow$  WEA8500# configure terminal
- 4. WEA8500/configure# alarm ?
- 5. Type exit
- 6. Practice with these commands "Debugs" from WEA8500#
  - 1. show debug processes
  - 2. show debug log conf
  - 3. show debug log detail conf
  - 4. debug log ?



# 2.2.1 Station Tracking History2.2.2 Station Tracking Real-time

Samsung Wireless Enterprise™

### The Flow of Authentication of WLAN Station



Samsung Wíreless Enterprise™

#### **Trace the Station - Association**

WEC8500# show stationtracking station 38:AA:3C:3D:B7:20
38 TR_38AA3C3DB720 [2013-04-08:10:35:43.524] INF <dr_vlan1_1217> Forwarded BOOTREPLY[DHCPACK] for 38:aa:3c:3d:b7:20 to 10.65.182.216</dr_vlan1_1217>
39 TR_38AA3C3DB720 [:10:35:43.523] INF <dsub_dhcpr> DHCP PLD: 38:aa:3c:3d:b7:20 station ip set 10.65.182.216</dsub_dhcpr>
40 TR_38AA3C3DB720 [:10:35:43.523] INF <dr_vlan1_1217> [DHCPACK] received from dhcp server</dr_vlan1_1217>
41 TR_38AA3C3DB720 [:10:35:43.521] INF <dr_vlan1_1217> Forwarded BOOTREQUEST[DHCPREQUEST] for 38:aa:3c:3d:b7:20 to 10.64.2.31</dr_vlan1_1217>
42 TR_38AA3C3DB720 [:10:35:43.520] INF <dr_vlan1_1217> [DHCPREQUEST] received from dhcp client</dr_vlan1_1217>
43 TR_38AA3C3DB720 [:10:35:43.515] INF <dr_vlan1_1217> Forwarded BOOTREPLY[DHCPOFFER] for 38:aa:3c:3d:b7:20 to 10.65.182.216</dr_vlan1_1217>
44 TR_38AA3C3DB720 [:10:35:43.515] INF <dr_vlan1_1217> [DHCPOFFER] received from dhcp server</dr_vlan1_1217>
45 TR_38AA3C3DB720 [:10:35:43.514] INF <dr_vlan1_1217> Forwarded BOOTREQUEST[DHCPDISCOVER] for 38:aa:3c:3d:b7:20</dr_vlan1_1217>
46 TR_38AA3C3DB720 [:10:35:43.513] INF <dr_vlan1_1217> [DHCPDISCOVER] received from dhcp client</dr_vlan1_1217>
47 TR_38AA3C3DB720 [:10:35:43.246] INF <security> STA(38:aa:3c:3d:b7:20) - PMKSA-Add: apc=1 pmkid[89,77,9c,,88,b3,cb]</security>
48 TR_38AA3C3DB720 [:10:35:43.244] INF <security> STA(38:aa:3c:3d:b7:20) - Authenticated. user=nwtest51 vlan=1217 qos=0 acl=setup url=<none></none></security>
49 TR_38AA3C3DB720 [:10:35:43.244] INF <security> STA(38:aa:3c:3d SetFlag[Auth]: wlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=1217 qos=0</security>
ap=61 radio=1 Authentication Completed
50 TR_38AA3C3DB720 [:10:35:43.244] INF <security> SIA(30:aa;3c;3u;D7:20) - CAPWAP Send: SetSessionKey: seq=0x00000000 wlan=1 ap=61 radio=1</security>
51 TR_38AA3C3DB720 [:10:35:43.243] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Recv 4/4 msg of 4-way h/s</security>
52 TR_38AA3C3DB720 [:10:35:43.241] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Send 3/4 msg of 4-way h/s</security>
53 TR_38AA3C3DB720 [:10:35:43.241] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Recv 2/4 msg of 4-way h/s</security>
54 TR_38AA3C3DB720 [:10:35:43.224] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Send 1/4 msg of 4-way h/s</security>
55 TR_38AA3C3DB720 [:10:35:43.224] INF <security> STA(38:aa:3c:3d:b7:20) - RADIUS Recv[Auth]: ACCESS-ACCEPT msg. id=0x12 len=399</security>
56 TR_38AA3C3DB720 [:10:35:42.930] INF <security> STA(38:aa:3c:3d:b7:20) - 802.1x Auth Started. reassoc Process of EAP packet exchange</security>
57 TR_38AA3C3DB720 [:10:35:42.930] INF < security > STA(38:aa:3c:3d:b7:20) - Authentication started (FAP-Request $\rightarrow$ FAP-Success)
58 TR_38AA3C3DB720 1:10:35:42.9291 TNF <security> STA(38:aa:3c:3d:b7:20) - PMK not found for OKC</security>
59 TR_38 - [I:STA]: STA sends Curity> STA (38:aa:3c:3d:b7:20) - (Re)Assoc: PMKID[0][c8, 2a, ee,, 9, 9, 9, 9, 9, 9
60 TR 38 - [O:STA]: APC sends Curity> STA (38:aa:3c:3d:b/:20) - (Re)Assoc: 1 PMKIDs Received
61 TK_381
62 TK_38AA3C3DB/20 [:10:35:42.928] <security> STA(38:aa:3C:30:D/:20) - STA PLD: Created. Wian=1 ap=61 radio=1 1d=1/2</security>
05 IK_50AA5C5DB720 [:10:55:42.925] INF [1:5TA] ASSOCIACION - B55ID(14:09:10:55:6C:C2) STA(36:4d:5C:50:D7:20)

Samsung Wíreless Enterprise™

#### **Trace the Station - Reassociation**

<pre>17 Tm_380A4ECCABA [013-04-18 [6:50:09.600.62] INF (dsub_dhopr&gt; DBCF PLD: 30:04*4eccaBA station ip set 70.31.216.220 18 Tm_380A4ECCABA [013-04-18 [6:50:09.500.62] INF (dsub_dhopr&gt; DBCF PLD: 30:05*4eccaBA station ip set 70.31.216.220 19 Tm_380A4ECCABA [013-04-18 [6:50:09.500.62] INF (dr_vial] 14&gt; [DBCERQUEST[IGCREQUEST] for 30:015*4eccaBa to 70.30.150.30 12 Tm_380A4ECCABA [013-04-18 [6:50:09.550.22] INF (dr_vial] 14&gt; [DBCERQUEST] IGCREQUEST] for 30:015*4eccaBa to 70.30.150.30 12 Tm_380A4ECCABA [013-04-18 [6:50:09.550.22] INF (dr_vial] 14&gt; [DBCERQUEST] IGCREQUEST] for 30:015*4eccaBa to 70.30.150.30 12 Tm_380A4ECCABA [013-04-18 [6:49:16.426.31] INF (dr_vial] 14&gt; [DBCERQUEST] IGCREQUEST] for 30:015*4eccaBa to 70.30.150.30 13 Tm_380A4ECCABA [021-04-18 [6:49:16.426.31] INF (decurity 5TA/380:01*4eccaBa) - BADTUS Acct: Interim Message Sent. Sesion 5167BEC-0000004A 14 Tm_380A4ECCABA [021-04-18 [6:39:36.425.555] INF (decurity 5TA/380:01*4eccaBa) - BADTUS Acct: Interim Message Sent. Sesion 5167BEC-0000004A 15 Tm_380A4ECCABA [021-04-18 [6:39:36.423.40] INF (decurity 5TA/380:01*4eccaBa) - BADTUS Acct: Besion 5167BEC-0000004 A rez1421,463429.0 14 Tm_380A4ECCABA [021-04-18 [6:39:36.424.40] INF (decurity 5TA/380:01*4eccaBa) - STA-Info: Removed(0X556aJCEG). wlan-1 ap=342 radio-2 15 Tm_380A4ECCABA [021-04-18 [6:39:36.424.40] INF (decurity 5TA/380:01*4eccaBa) - STA-Info: Removed(0X556aJCEG). wlan-1 ap=342 radio-2 15 Tm_380A4ECCABA [021-04-18 [6:39:36.902.410] INF (decurity 5TA/380:01*4eccaBa) - STA-Info: Removed(0X556aJCEG). wlan-1 ap=342 radio-2 15 Tm_380A4ECCABA [021-04-18 [6:39:35.902.110] INF (decurity 5TA/380:01*4eccaBa) - STA-Info: Removed(0X556aJCEG). wlan-1 ap=342 radio-2 15 Tm_380A4ECCABA [021-04-18 [6:39:35.902.110] INF (decurity 5TA/380:01*4eccaBa) - SAEVAFWS dot StateStateAB - Advertion StateAB - A</pre>	16 TR_380A94ECCABA [2013-04-18 16:50:09.961.402] INF <dr_vlan1_114> Forwarded BOOTREPLY[DHCPACK] for 38:0a:94:ec:ca:ba to 70.31.216.220</dr_vlan1_114>		
<pre>18 TR_380A4ECCARA [2013-04-18 16:50:09.960.463] INF <dsub_htpp: (ip="461fdddc)" 16:50:09.960.443]="" 19="" <dsub_114="" [2013-04-18="" another="" existed="" inf="" ip="" station="" tr_380a4eccara=""> [DUCERACU received from dhop client 1 TR_380A4ECCARA [2013-04-18 16:50:09.956.423] INF <dsub_114> [DUCERACUEST] received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:49:36.826.133] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:49:36.826.133] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:49:36.826.133] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:49:36.826.133] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:49:36.825.553] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:49:36.825.102] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:36.825.102] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:36.824.104] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:36.824.104] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:36.824.104] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:35.909.115] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:35.909.115] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:35.909.115] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:35.909.115] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:35.909.115] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_380A4ECCARA [2013-04-18 16:39:35.909.115] INF <dsub_114> [DUCERACUEST] INFC received from dhop client 2 TR_</dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_114></dsub_htpp:></pre>	7 TR_380A94ECCABA [2013-04-18 16:50:09.960.853] INF <dsub_dhcpr> DHCP PLD: 38:0a:94:ec:ca:ba station ip set 70.31.216.220</dsub_dhcpr>		
<pre>19 TR_300A4ECCAAM [2013-04-18 16:50:09.960.409] INF <dr (control="" co<="" control="" display="" td="" transmission="" vlan_114=""><td>18 TR_380A94ECCABA [2013-04-18 16:50:09.960.682] INF <dsub_dhcpr> Another Station IP existed.(Ip=461fd8dc)</dsub_dhcpr></td></dr></pre>	18 TR_380A94ECCABA [2013-04-18 16:50:09.960.682] INF <dsub_dhcpr> Another Station IP existed.(Ip=461fd8dc)</dsub_dhcpr>		
<pre>20 TR_380A4ECCABA [2013-04-18 16:50:09.958.42] INF <dryulan_114> FORVERAGEST [NCFREQUEST] for 38:0.834:ecca:ba to 70.30.150.30 21 TR_380A4ECCABA [2013-04-18 16:49:36.422.20] INF <dryulan_114> FORVERAGEST [NCFREQUEST] received from dhcp client 22 TR_380A4ECCABA [2013-04-18 16:49:36.422.13] INF <dryulan_114> FORVERAGEST [NCFREQUEST] received from dhcp client 23 TR_380A4ECCABA [2013-04-18 16:49:36.422.555] INF <dryulan_114> FORVERAGEST [NCFREQUEST] received from dhcp client 24 TR_380A4ECCABA [2013-04-18 16:49:36.422.555] INF <dryulan_114> FORVERAGEST [NCFREQUEST] Received in FADIUS Acct: Interim Message Sent. Session 5167BFEC-0000004A 25 TR_380A4ECCABA [2013-04-18 16:39:36.422.101] INF <dryulan_114> forverity&gt; STA(38:0a:94:ec:ca:ba) = RADIUS Acct: Session 5167BFEC-0000004A Sent 27 TR_380A4ECCABA [2013-04-18 16:39:36.422.101] INF <dryulan_114> forverity&gt; STA(38:0a:94:ec:ca:ba) = RADIUS Acct: Session 5167BFEC-0000004A Sent 27 TR_380A4ECCABA [2013-04-18 16:39:36.424.466] INF <dryulan_114> forverity&gt; STA(38:0a:94:ec:ca:ba) = RADIUS Acct: Session 5167BFEC-0000004A x=23421,4639429,0 tx=23106,4938730,0 28 TR_380A4ECCABA [2013-04-18 16:39:36.924.466] INF <dryulan_114> forverity&gt; STA(38:0a:94:ec:ca:ba) = RADIUS Acct: Session 5167BFEC-0000004A x=23421,4639429,0 tx=23106,4938730,0 28 TR_380A4ECCABA [2013-04-18 16:38:35.900.15] INF <dryulan_114> forverity&gt; STA(38:0a:94:ec:ca:ba) = RADIUS Acct: Mession fifthFEC-0000004A x=23421,4639429,0 tx=23106,4938730,0 30 TR_380A4ECCABA [2013-04-18 16:38:35.900.20] INF <dryulan_12+ 16:38:35.424.70]="" 16:38:35.900.20]="" 30="" <dryulan_12+="" [2013-04-18="" acl="&lt;carbonal" ap="355" i<="" in="" inf="" qos="0" radio="2" security="" send:="" seq0x0400046="" sta(38:0a:94:ec:ca:ba)="CAPWAF" statessionkey:="" td="" the="" tr_380a4eccaba="" transmitter="" user_jinvhan.lee="" vlan="14" wlan="1"><td>19 TR_380A94ECCABA [2013-04-18 16:50:09.960.449] INF <dr_vlan1_114> [DHCPACK] received from dhcp server</dr_vlan1_114></td></dryulan_12+></dryulan_114></dryulan_114></dryulan_114></dryulan_114></dryulan_114></dryulan_114></dryulan_114></dryulan_114></dryulan_114></dryulan_114></pre>	19 TR_380A94ECCABA [2013-04-18 16:50:09.960.449] INF <dr_vlan1_114> [DHCPACK] received from dhcp server</dr_vlan1_114>		
<pre>21 FE_300A4ECCARA [2013-04-18 16:50:09.458.428] INF degruity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Interim Message Sent. Sesion 5167BEC-0000004A 23 FE_300A4ECCARA [2013-04-18 16:49:36.428.420] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS 4 FE_300A4ECCARA [2013-04-18 16:49:36.428.555] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Interim Message Sent. Sesion 5167BEC-0000004A 24 FE_300A4ECCARA [2013-04-18 16:49:36.428.555] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Interim Message Sent. Sesion 5167BEC-0000004A 25 FE_300A4ECCARA [2013-04-18 16:39:36.428.414] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Interim Message Sent. Sesion 5167BEC-0000004A 26 FE_300A4ECCARA [2013-04-18 16:39:36.428.414] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Sesion 5167BEC-0000004A rx=33421.4639429.0 1x=23106.4987030, 28 FE_300A4ECCARA [2013-04-18 16:38:35.908.115] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Sesion 5167BEC-0000004A rx=33421.4639429.0 1x=330044ECCARA [2013-04-18 16:38:35.908.146] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Sesion 5167BEC-0000004A rx=33421.4639429.0 1x=2306.498CCARA [2013-04-18 16:38:35.908.146] INF descurity STA(38:00:44:ec:ca:ha) = RADIUS Acct: Sesion 5167BEC-0000004A rx=33421.4639429.0 1x=330044ECCARA [2013-04-18 16:38:35.908.146] INF descurity STA(38:00:44:ec:ca:ha) = Attenticated.user=jinkhan.lee Valma14 pae-0 28 FE_300A4ECCARA [2013-04-18 16:38:35.908.146] INF descurity STA(38:00:44:ec:ca:ha) = STA-Info: Removed(0x556a2fe10). vlam=1 ap=358 radio=2 28 TE_300A4ECCARA [2013-04-18 16:38:35.908.126] INF descurity STA(38:00:44:ec:ca:ha) = STA-Info: Removed(Valsofe advar h/s 29 TE_300A4ECCARA [2013-04-18 16:38:35.908.126] INF descurity STA(38:00:44:ec:ca:ha) = STA-Info: Removed(Valsofe advar h/s 20 TE_300A4ECCARA [2013-04-18 16:38:35.908.126] INF descurity STA(38:00:44:ec:ca:ha) = STA-Info: Removed(Valsofe, Valsof h/s) 20 TE_300A4ECCARA [2013-04-18 16:38:35.908.126] INF descurity STA(38:00:44:ec:ca:ha) = EAPOL-Rey: Red J/A mag of 4-way h/s 20 TE_300A4EC</pre>	20 TR_380A94ECCABA [2013-04-18 16:50:09.958.923] INF <dr_vlan1_114> Forwarded BOOTREQUEST[DHCPREQUEST] for 38:0a:94:ec:ca:ba to 70.30.150.30</dr_vlan1_114>		
<pre>22 TR_380A4ECCABA [2013-04-18 16:49:56.826.220] NM <security (0x4m="" (0x55633cfe10).="" (0x5563cfe10).="" -="" .cunt="1" 16:38:55.822.557]="" 16:38:55.900.3261)="" 16:38:55.900.426]="" 16:38:55.900.525]="" 16:38:55.900.526]="" 16:38:55.909.115]="" 16:38:55.909.125]="" 16:38:55.920.557]="" 16:38:56.909.115]="" 16:39:56.824.614]="" 16:49:56.826.130]="" 20="" 21="" 24="" 26="" 27="" 28="" 29="" 31="" 32="" 4-way="" 41="" 5167bfec-000004a="" <security="" [2013-04-18="" acci:="" acct:="" ap="358" authenticated.="" h="" interim="" mag="" message="" nm="" of="" qos="0" radio="2" radus="" removed="" s="" sent="" sent.="" session="" sta(38:0a:94:e<="" sta(38:0a:94:ec:ca:ba)="" sta-info:="" td="" tr_380a4eccaba="" user-jinvhan.lee="" vlan="1"><td>21 TR_380A94ECCABA [2013-04-18 16:50:09.958.428] INF <dr_vlan1_114> [DHCPREQUEST] received from dhcp client</dr_vlan1_114></td></security></pre>	21 TR_380A94ECCABA [2013-04-18 16:50:09.958.428] INF <dr_vlan1_114> [DHCPREQUEST] received from dhcp client</dr_vlan1_114>		
<pre>23 TR_380A44CCABA [2013-04-18 16:49:36.825.513] INF (security STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-000004A (2013-04-18 16:39:36.825.515] INF (security STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-000004A (2013-04-18 16:39:36.825.514] INF (security STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-000004A (2013-04-18 16:39:36.825.514] INF (security STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-000004A (2013-04-18 16:39:36.824.614] INF (security STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-000004A (2013-04-18 16:39:36.824.614] INF (security STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-000004A (2014-2016) (</pre>	22 TR_380A94ECCABA [2013-04-18 16:49:36.826.220] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Interim Message Sent. Session 5167BFEC-0000004A</security>		
<pre>24 TR 380A94ECCBAR [2013-04-18 16:49:36.825.555] THF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Control Pressure Press Pressure Pressure Pressure Pressure Press Pressure Pressure</security></pre>	23 TR_380A94ECCABA [2013-04-18 16:49:36.826.133] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS ACCOUNTING Interim message (per 10 min )</security>		
<pre>25 TR_380A4ECCABA [2013-04-18 16:39:36.825.02] INF <security> STA(38:0a:94:ecc:aba) = RADIUS Acct: Interim Message Sent. Session 5167BFEC-0000004A 26 TR_380A4ECCABA [2013-04-18 16:39:36.824.614] INF <security> STA(38:0a:94:ecc:aba) = RADIUS Acct: Session 5167BFEC-0000004A rx=23421,4639429,0 tx=23106,4938730,0 28 TR_380A4ECCABA [2013-04-18 16:39:36.824.466] INF <security> STA(38:0a:94:ecc:aba) = STA-Info: Removed(0x556a3cfe10). vlan=1 ap=342 radio=2 29 TR_380A4ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ecc:aba) = STA-Info: Removed(0x556a3cfe10). vlan=1 ap=342 radio=2 20 TR_380A4ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ecc:aba) = StA-Info: Removed(0x556a3cfe10). vlan=1 ap=342 radio=2 20 TR_380A4ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 602.1x=1 dynVlan=1 aa=1 vlan=114 qos=0 20 TR_380A4ECCABA [2013-04-18 16:38:35.908.400] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 602.1x=1 dynVlan=1 aa=1 vlan=114 qos=0 20 TR_380A4ECCABA [2013-04-18 16:38:35.900.552] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 602.1x=1 dynVlan=1 aa=1 vlan=114 qos=0 20 TR_380A4ECCABA [2013-04-18 16:38:35.900.352] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 602.1x=1 dynVlan=1 aa=1 vlan=114 qos=0 20 TR_380A4ECCABA [2013-04-18 16:38:35.900.352] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 602.1x=1 dynVlan=1 aa=1 vlan=114 qos=0 20 TR_380A4ECCABA [2013-04-18 16:38:35.900.352] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 602.1x=1 dynVlan=1 aa=1 vlan=114 qos=0 20 TR_380A4ECCABA [2013-04-18 16:38:35.900.352] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 4y=14 vlan=1 20 TR_380A4ECCABA [2013-04-18 16:38:35.921.11] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 dynFlag 20 TR_380A4ECCABA [2013-04-18 16:38:35.921.21] INF <security> STA(38:0a:94:ecc:aba) = 802.1x uht Skipped 20 TR_380A4ECCABA [2013-04-18 16:38:35.921.21] INF <security> STA(38:0a:94:ecc:aba) = StFlag: vlan=1 dynFlag, StFlag, StFlag, StF</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	24 TR_380A94ECCABA [2013-04-18 16:49:36.825.555] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS (10105) decounting interim message (per 10 min.) tx=23612,5096397,0</security>		
<pre>26 TE_300A94ECCABA [2013-04-18 16:39:36.825.114] IMF <security> STA(38:0a:94:ec:ca:ba) = PADIUS Acct: Session 5167BEEC-0000004A Sent 27 TE_300A94ECCABA [2013-04-18 16:39:36.824.614] INF <security> STA(38:0a:94:ec:ca:ba) = AADIUS Acct: Session 5167BEEC-0000004A rx=23421,4639429,0 tx=23106,4939730,0 28 TE_300A94ECCABA [2013-04-18 16:38:35.804.466] INF <security> STA(38:0a:94:ec:ca:ba) = STA-Info: Removed(0x556a3cfel), wlan=1 ap=342 radio=2 29 TE_300A94ECCABA [2013-04-18 16:38:35.908.746] INF <security> STA(38:0a:94:ec:ca:ba) = Athenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none> 30 TE_300A94ECCABA [2013-04-18 16:38:35.908.746] INF <security> STA(38:0a:94:ec:ca:ba) = AEHENICATE (user=jinwhan.lee vlan=114 qos=0 31 TE_300A94ECCABA [2013-04-18 16:38:35.908.746] INF <security> STA(38:0a:94:ec:ca:ba) = CAFWAF Sent SetSessionKey: seq=0x04010468 wlan=1 ap=358 radio=2 32 TE_300A94ECCABA [2013-04-18 16:38:35.908.129] INF <security> STA(38:0a:94:ec:ca:ba) = CAFUC-Key: Recv 4/4 msg of 4-way h/s 33 TE_300A94ECCABA [2013-04-18 16:38:35.908.026] INF <security> STA(38:0a:94:ec:ca:ba) = EAFOL-Key: Send 3/4 msg of 4-way h/s 34 TE_300A94ECCABA [2013-04-18 16:38:35.804.711] INF <security> STA(38:0a:94:ec:ca:ba) = EAFOL-Key: Send 3/4 msg of 4-way h/s 35 TE_300A94ECCABA [2013-04-18 16:38:35.824.711] INF <security> STA(38:0a:94:ec:ca:ba) = AEAOL-Key: Send 3/4 msg of 4-way h/s 36 TE_300A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94:ec:ca:ba) = AEAOL-Key: Send 3/4 msg of 4-way h/s 37 TE_300A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94:ec:ca:ba) = AUC-Key: Send 3/4 msg of 4-way h/s 36 TE_300A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94:ec:ca:ba) = AWLAN Skipped 37 TE_300A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94:ec:ca:ba) = AWLANCAKE AME 37 TE_300A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94:ec:ca:ba) = AWLANCAKE AME 37 TE_300A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94</security></security></security></security></security></security></security></security></security></security></security></security></none></none></security></security></security></security></pre>	25 TR 380A94ECCABA [2013-04-18 16:39:36.825.202] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Interim Message Sent. Session 5167BFEC-0000004A</security>		
<pre>27 TE_30A34ECCABA [2013-04-18 16:39:36.824.614] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-0000004A rx=23421,4639429,0 tx=23106,4938730,0 28 TR_300A34ECCABA [2013-04-18 16:38:35.0824.466] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a3cfe10). wlan=1 ap=342 radio=2 29 TR_300A34ECCABA [2013-04-18 16:38:35.090.146] INF <security> STA(38:0a:94:ec:ca:ba) - StHag: wlan=1 802.1x=1 dymVlan=1 aa=1 vlan=114 qos=0 31 TR_300A34ECCABA [2013-04-18 16:38:35.900.146] INF <security> STA(38:0a:94:ec:ca:ba) - SetLag: wlan=1 802.1x=1 dymVlan=1 aa=1 vlan=114 qos=0 31 TR_300A34ECCABA [2013-04-18 16:38:35.900.10MF <security> STA(38:0a:94:ec:ca:ba) - SetLag: wlan=1 802.1x=1 dymVlan=1 aa=1 vlan=114 qos=0 31 TR_300A34ECCABA [2013-04-18 16:38:35.900.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 mag of 4-way h/s 33 TR_300A34ECCABA [2013-04-18 16:38:35.900.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Set 37 (4 mag of 4-way h/s 34 TR_300A34ECCABA [2013-04-18 16:38:35.900.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Set 37 (4 mag of 4-way h/s 35 TR_300A34ECCABA [2013-04-18 16:38:35.900.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Set 37 (4 mag of 4-way h/s 36 TR_300A34ECCABA [2013-04-18 16:38:35.900.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Set 37 (4 mag of 4-way h/s 36 TR_300A34ECCABA [2013-04-18 16:38:35.900.521] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Set 1/4 mag of 4-way h/s 36 TR_300A34ECCABA [2013-04-18 16:38:35.900.521] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_300A34ECCABA [2013-04-18 16:38:35.900.521] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_300A34ECCABA [2013-04-18 16:38:35.900.521] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_300A34ECCABA [2013-04-18 16:38:35.900.521] INF <security> STA(38:0a:94:ec:ca:ba) - Mex foud. okc MMDI[6a, 9b, 87,, 5c, 71, a5] 10 TR_300A34ECCABA [2013-04-18 16:38:35.900.521] INF <security> STA(38:0a:94:ec:c</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	26 TR 380A94ECCABA [2013-04-18 16:39:36.825.114] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-0000004A Sent</security>		
<pre>C TR_300A4ECCABA [2013-04-18 16:38:36.024.486] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a3cfel0). vlan=1 ap=342 radio=2 29 TR_300A4ECCABA [2013-04-18 16:38:35.909.115] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<non> ull=<non> 30 TR_300A4ECCABA [2013-04-18 16:38:35.909.400] INF <security> STA(38:0a:94:ec:ca:ba) - SetFlag: vlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=114 qos=0 31 TR_300A4ECCABA [2013-04-18 16:38:35.909.400] INF <security> STA(38:0a:94:ec:ca:ba) - CAFWAP Send: SetSessionKey: seq=0x04010468 vlan=1 ap=358 radio=2 32 TR_300A4ECCABA [2013-04-18 16:38:35.909.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s 33 TR_300A4ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s 34 TR_300A4ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 3/4 msg of 4-way h/s 35 TR_300A4ECCABA [2013-04-18 16:38:35.802.470] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 36 TR_300A4ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 37 TR_300A4ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - BACL-Key: Send 1/4 msg of 4-way h/s 38 TR_300A4ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A4ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A4ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMKS foud. okc FMKID[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - PMK foud. okc: FMKID[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.621] INF <security> STA(38:0a:94:ec:ca:ba) - Nex STA-Info: Added. vlan=1 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.621] INF <security> STA(38:0a:94:ec:ca:ba) - Nex STA-I</security></security></security></security></security></security></security></security></security></security></security></security></security></security></non></non></security></security></pre>	27 TR 380A94ECCABA [2013-04-18 16:39:36.824.614] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-0000004A rx=23421,4639429,0</security>		
<pre>29 TR 30A94ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated.user=jinwhan.lev lan-114 gos=0 31 TR 380A94ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ec:ca:ba) - SetFlag: wlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=114 gos=0 31 TR 380A94ECCABA [2013-04-18 16:38:35.908.400] INF <security> STA(38:0a:94:ec:ca:ba) - CAFWAP Send: SetSessionKey: seq=0x04010466 wlan=1 ap=358 radio=2 22 TR 380A94ECCABA [2013-04-18 16:38:35.908.400] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Rev 4/4 msg of 4-way h/s 31 TR 380A94ECCABA [2013-04-18 16:38:35.908.129] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Rev 4/4 msg of 4-way h/s 32 TR 380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Rev 2/4 msg of 4-way h/s 34 TR 380A94ECCABA [2013-04-18 16:38:35.824.711] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Rev 2/4 msg of 4-way h/s 35 TR 380A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 4 way-handshake 37 TR 380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started 38 TR 380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 97 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 97 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - FMKSA-Add, CKC: apc=1 pmkid[6a, 9b, 87,, 5c, 71, a5] 40 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - MKIDIOI[06, 9b, 87,, 5c, 71, a5] 41 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - MKSA-Add, CKC: apc=1 pmkid[6a, 9b, 87,, 5c, 71, a5] 42 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - MKSTID CHAEL AND [MKIDIOI [06, 9b, 87,, 5c, 71, a5] 43 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	$28$ TE 380894ECCERE [2013_04_18 16.38.36 824 486] INE security STE(38.0a.94.ec.ca.ba) = STE_Info: Demoved(0x556a3cfe10) wlan=1 an=342 radio=2		
<pre>urlectome&gt; urlectome&gt; 30 TR 300A4ECCABA [2013-04-18 16:38:55.908.748] INF <security> STA(38:0a:94:ec:ca:ba) - SetFlag: wlan=1 802.1x=1 dynVlan=1 aa=1 vlan=114 gos=0 31 TR 300A4ECCABA [2013-04-18 16:38:55.908.708] INF <security> STA(38:0a:94:ec:ca:ba) - CAFWAP Send: SetSessionKey: seq=0x4010466 wlan=1 ap=358 radio=2 32 TR_380A94ECCABA [2013-04-18 16:38:35.900.52] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s 34 TR_380A94ECCABA [2013-04-18 16:38:35.900.52] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s 35 TR_380A94ECCABA [2013-04-18 16:38:35.900.52] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 36 TR_380A94ECCABA [2013-04-18 16:38:35.924.711] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 36 TR_380A94ECCABA [2013-04-18 16:38:35.924.711] INF <security> STA(38:0a:94:ec:ca:ba) - BAPOL-Key: Send 1/4 msg of 4-way h/s 36 TR_380A94ECCABA [2013-04-18 16:38:35.924.711] INF <security> STA(38:0a:94:ec:ca:ba) - BAPOL-Key: Send 1/4 msg of 4-way h/s 36 TR_380A94ECCABA [2013-04-18 16:38:35.924.711] INF <security> STA(38:0a:94:ec:ca:ba) - BAPOL-Key: Send 1/4 msg of 4-way h/s 37 TR_380A94ECCABA [2013-04-18 16:38:35.924.711] INF <security> STA(38:0a:94:ec:ca:ba) - BAPOL-Key: Send 1/4 msg of 4-way h/s 37 TR_380A94ECCABA [2013-04-18 16:38:35.924.731] INF <security> STA(38:0a:94:ec:ca:ba) - DMK found. okc PMKID[6a,9b,67,,5c,71,a5] 37 TR_380A94ECCABA [2013-04-18 16:38:35.922.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[0] (fa,9b,67,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.920.622] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[0] (fa,9b,67,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.920.622] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 41 TR_380A94ECCABA [2013-04-18 16:38:35.920.621] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 41 TR_380A94ECCABA [2013-04-18 16:38:35.910.60] INF [I:STA] STA Moved - BSSS [</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	20 TR_380A94ECCARA [2013-04-18 16:38:35 909 115] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated user=jinwhan lee vlan=114 gos=0 acl=<none></none></security>		
<pre>30 TR 380A94ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ec:ca:ba) - CAFWAP Send: SetSessionKey: seq=0x04010468 wlan=1 ap=358 radio=2 31 TR 380A94ECCABA [2013-04-18 16:38:35.908.129] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s 33 TR 380A94ECCABA [2013-04-18 16:38:35.900.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s 34 TR 380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s 35 TR 380A94ECCABA [2013-04-18 16:38:35.824.587] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s 36 TR 380A94ECCABA [2013-04-18 16:38:35.824.587] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 1/4 msg of 4-way h/s 37 TR 380A94ECCABA [2013-04-18 16:38:35.824.587] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 1/4 msg of 4-way h/s 37 TR 380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped 37 TR 380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR 380A94ECCABA [2013-04-18 16:38:35.822.274] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 30 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 30 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - FMK found. okc FMKID[6a,9b,87,,5c,71,a5] 41 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - MKSA-Add, OKC: apt = mkid[6a,9b,87,,5c,71,a5] 42 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - MKSD Received OKC starts 43 TR 380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - Mex STA-1nfo: Added Nalan=1 44 TR 380A94ECCABA [2013-04-18 16:38:35.81.560] INF <security> STA(38:0a:94:ec:ca:ba) - McK: Started. wlan=1 ap=358 radio=2 45 TR 380A94ECCABA [2013-04-18 16:38:35.81.560] INF <security> STA</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	url= <none></none>		
<pre>31 TR_380A94ECCABA [2013-04-18 16:38:35.908.400] INF <security> STA(38:0a:94:ec:ca:ba) - CAPWAP Send: SetSessionKey: seq=0x04010468 wlan=1 ap=358 radio=2 32 TR_380A94ECCABA [2013-04-18 16:38:35.900.522] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s 34 TR_380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s 35 TR_380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 36 TR_380A94ECCABA [2013-04-18 16:38:35.824.111] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - AUthentication started 38 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.822.622] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[0][6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[0][6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKID8 Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.625] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:3</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	30 TR_380A94ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ec:ca:ba) - SetFlag: wlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=114 qos=0</security>		
<pre>22 TR_380A94ECCABA [2013-04-18 16:38:35.908.129] INF <security> STA(38:0a:94:ecc:a:ba) = EAPOL-Key: Recv 4/4 msg of 4-way h/s 33 TR_380A94ECCABA [2013-04-18 16:38:35.900.352] INF <security> STA(38:0a:94:ecc:a:ba) = EAPOL-Key: Send 3/4 msg of 4-way h/s 45 TR_380A94ECCABA [2013-04-18 16:38:35.900.352] INF <security> STA(38:0a:94:ecc:a:ba) = EAPOL-Key: Send 1/4 msg of 4-way h/s 45 TR_380A94ECCABA [2013-04-18 16:38:35.824.701] INF <security> STA(38:0a:94:ecc:a:ba) = BAPOL-Key: Send 1/4 msg of 4-way h/s 45 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ecc:a:ba) = 802.1x Auth Skipped 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.140] INF <security> STA(38:0a:94:ecc:a:ba) = Authentication started 38 TR_380A94ECCABA [2013-04-18 16:38:35.824.140] INF <security> STA(38:0a:94:ecc:a:ba) = Authentication started 39 TR_380A94ECCABA [2013-04-18 16:38:35.824.140] INF <security> STA(38:0a:94:ecc:a:ba) = Atthentication started 30 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ecc:a:ba) = Atthentication started 31 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ecc:a:ba) = PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.64] INF <security> STA(38:0a:94:ecc:a:ba) = PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ecc:a:ba) = OKC: Started. WIADPI 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ecc:a:ba) = New STA-Info: Added. WIADPI 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ecc:a:ba) = New STA-Info: Added. WIADPI 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ecc:a:ba) = New STA-Info: Added. WIADPI 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ecc:a:ba) = New STA-Info: Added. WIADPI 45 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ecc:a:ba) = OKC: Started. WIADPI ap=358 radio=2 45 TR_</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	31 TR_380A94ECCABA [2013-04-18 16:38:35.908.400] INF <security> STA(38:0a:94:ec:ca:ba) - CAPWAP Send: SetSessionKey: seq=0x04010468 wlan=1 ap=358 radio=2</security>		
<pre>33 TR_380A94ECCABA [2013-04-18 16:38:35.900.552] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 3/4 msg of 4-way h/s 34 TR_380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s 35 TR_380A94ECCABA [2013-04-18 16:38:35.824.171] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s 4 way-handshake 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started 38 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[0[6a,9b,87,,5c,71,a5] 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDS Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.815.600] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 45 TR_380A94ECCABA [2013-04-18 16:38:35.817.600] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.813.600] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.600] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.600] INF <security> STA(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.813.600] INF <security> STA(38:0</security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></security></pre>	32 TR_380A94ECCABA [2013-04-18 16:38:35.908.129] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s</security>		
<pre>34 TR_380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s 35 TR_380A94ECCABA [2013-04-18 16:38:35.824.711] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 36 TR_380A94ECCABA [2013-04-18 16:38:35.824.710] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.170] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started 38 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started 39 TR_380A94ECCABA [2013-04-18 16:38:35.824.2374] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A94ECCABA [2013-04-18 16:38:35.822.241] INF <security> STA(38:0a:94:ec:ca:ba) - FMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.241] INF <security> STA(38:0a:94:ec:ca:ba) - FMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.231] INF <security> STA(38:0a:94:ec:ca:ba) - FMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 FMKIDS Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.815.600] INF (security&gt; STA(38:0a:94:ec:ca:ba) - OKC: Mlan=1 ap=358 radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.600] INF (I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:67:11) 46 TR_380A94ECCABA [2013-04-18 16:38:35.813.501] INF (Security&gt; STA(38:0a:94:ec:ca:ba) - OKC MS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.600] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) + OKC MS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.81.053] INF [STA] Removed station(38:0a:94:ec:ca:ba) + OKC MS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.81.063] INF [I:STA] Removed</security></security></security></security></security></security></security></security></security></security></security></pre>	33 TR_380A94ECCABA [2013-04-18 16:38:35.900.552] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 3/4 msg of 4-way h/s</security>		
<pre>35 TR_30A94ECCABA [2013-04-18 16:38:35.824.711] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 4 way-handshake 36 TR_30A94ECCABA [2013-04-18 16:38:35.824.50] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started 38 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: PMKID[0][6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKID Received OKC Starts 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 45 TR_380A94ECCABA [2013-04-18 16:38:35.817.650] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 46 TR_380A94ECCABA [2013-04-18 16:38:35.817.650] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [I:STA] STA Moved - BSS [342]:f4:d9:fb:37:27:11] 48 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 49 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 40 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 41 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 42 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0</security></security></security></security></security></security></security></security></security></security></security></pre>	R_380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s</security>		
<pre>36 TR_380A94ECCABA [2013-04-18 16:38:35.824.587] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped 37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started 38 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: PMKID[0][6a,9b,87,,5c,71,a5] 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDS Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 45 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.050] INF (security&gt; STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.053] INF [STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.8</security></security></security></security></security></security></security></security></security></security></security></pre>	IR_380A94ECCABA [2013-04-18 16:38:35.824.711] INF < security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s 4 way-handshake		
<pre>37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started 38 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.822.624] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKID Received 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.811.050] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.811.057] INF [STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 49 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 49 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. use=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none> url=<none></none></none></none></security></security></security></security></security></security></security></security></security></security></security></security></pre>	36 TR_380A94ECCABA [2013-04-18 16:38:35.824.587] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped</security>		
<pre>38 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1 39 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: PMKID[0][6a,9b,87,,5c,71,a5] 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.811.55] INF [STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID[f4:d9:fb:37:22:b1] STA(38:0a:94:ec:ca:ba) 47 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID[f4:d9:fb:37:22:b1] STA(38:0a:94:ec:ca:ba) 47 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID[f4:d9:fb:37:22:b1] STA(38:0a:94:ec:ca:</security></security></security></security></security></security></security></security></security></pre>	37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started</security>		
<pre>39 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5] 40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: PMKID[0][6a,9b,87,,5c,71,a5] 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received 44 TR_380A94ECCABA [2013-04-18 16:38:35.801.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a7711f0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. use=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></security></security></security></security></security></security></security></security></pre>	8 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1</security>		
<pre>40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5] 41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: PMKID[0][6a,9b,87,,5c,71,a5] 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></security></security></security></security></security></security></security></pre>	9 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF < security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,,5c,71,a5]		
<pre>41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: PMKID[0][6a,9b,87,5c,71,a5] 42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSs [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></security></security></security></security></security></pre>	40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,,5c,71,a5]</security>		
<pre>42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received 43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSs [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Removed station (38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 49 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></security></security></security></security></pre>	41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: FMKID[0][6a,9b,87,5c,71,a5]</security>		
<pre>43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1 44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></security></security></security></pre>	42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF < security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received OKC starts		
<pre>44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2 45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none> </none></none></security></security></security></security></pre>	43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1</security>		
<pre>45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1 46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></security></pre>	44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2</security>		
<pre>46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2 47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none> </none></none></security></security></security></pre>	45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSS [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1		
<pre>47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11) 48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></pre>	16 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2</security>		
<pre>48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba) 49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></pre>	17 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11)		
<pre>49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2 50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security></security></pre>	48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba)		
50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none></none></security>	49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF < security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2		
	50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none> url=<none></none></none></security>		



#### **Trace the Station – Authentication fails**

- Authentication fails due to the wrong ID/PASSWORD
  - → STA receives REJECT message from RADIUS server
  - → STA sends disassociation message and AP/APC releases the association session

```
41 TR B4629357DC45 [2013-04-29 15:37:21.992.885] INF <security> STA(b4:62:93:57:dc:45) - STA-Info: Removed(0x55662ea950) (ap handle timer). wlan=1 ap=224
  radio=1 auth-progress=0
42 TR B4629357DC45 [2013-04-29 15:37:20.992.821] INF <security> STA(b4:62:93:57:dc:45) - STA PLD Deleted: Done. wlan=1 radio=1 ap=224
43 TR B4629357DC45 [2013-04-29 15:37:20.983.623] INF [STA] Removed station(b4:62:93:57:dc:45) from BSS(f4:d9:fb:38:c9:42)
44 TR B4629357DC45 [2013-04-29 15:37:20.982.799] INF <security> STA(b4:62:93:57:dc:45) - STA PLD: Deleted. id=404
45 TR B4629357DC45 [2013-04-29 15:37:20.982.393] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Update: rx=0 gigawords t
                                                                                                                            STA receives REJECT and
46 TR B4629357DC45 [2013-04-29 15:37:20.982.309] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Update: rx=0,0 bytes tx=
                                                                                                                            sends disassociation
47 TR B4629357DC45 [2013-04-29 15:37:20.982.213] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Msg from AWMB: iface=/
48 TR B4629357DC45 [2013-04-29 15:37:20.982.109] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Msg from AWMB: wla -1 rx=0,0 tx=7,1500
49 TR B4629357DC45 [2013-04-29 15:37:20.981.342] INF [I:STA] Dissassociation - BSSID(f4:d9:fb:38:c9:42) STA(b4:62:93:57:dc:45)
50 TR B4629357DC45 [2013-04-29 15:37:20.915.985] INF <security> STA(b4:62:93:57:dc:45) - EAP FAILURE2: 0 -> 1
51 TR B4629357DC45 [2013-04-29 15:37:20.915.793] INF <security> STA(b4:62:93:57:dc:45) - RADIUS 802.1x Auth: Access Reject Received. id=174 code=3
52 TR B4629357DC45 [2013-04-29 15:37:20.915.404] INF < security> STA(b4:62:93:57:dc:45) - RADIUS Recv[Auth]: ACCESS-REJECT msg. id=0xae len=44
53 TR B4629357DC45 [2013-04-29 15:37:20.543.655] INF <security> STA(b4:62:93:57:dc:45) - 802.1x Recv: EAPOL-Start Received. pae-
  state=AUTH PAE AUTHENTICATING eap-state=EAP IDLE
                                                                                                                                 REJECT is received from
55 TR B4629357DC45 [2013-04-29 15:37:20.523.972] INF <security> STA(b4:62:93:57:dc:45) - 802.1x Auth Started. reassoc=0
                                                                                                                                 Authentication Server
56 TR B4629357DC45 [2013-04-29 15:37:20.523.825] INF <security> STA(b4:62:93:57:dc:45) - Authentication started
57 TR B4629357DC45 [2013-04-29 15:37:20.521.191] INF <security> STA(b4:62:93:57:dc:45) - No PMKID Received from STA
58 TR B4629357DC45 [2013-04-29 15:37:20.521.042] INF <security> STA(b4:62:93:57:dc:45) - New STA-Info: Added(0x55662ea950). wlan=1 ap=224 radio=1 count=1
59 TR B4629357DC45 [2013-04-29 15:37:20.520.529] INF <security> STA(b4:62:93:57:dc:45) - STA PLD: Created. id=404
60 TR B4629357DC45 [2013-04-29 15:37:20.518.621] INF [I:STA] Association - BSSID(f4:d9:fb:38:c9:42) STA(b4:62:93:57:dc:45)
```



#### **Trace the Station – Reassociation fails**

STA does not response in the process of 4 way-handshake
→ Reassociation fails
X These worklasses are smaller as a data the MCD driver (a human of An data) driver to human
$\rightarrow$ These problems are usually caused by the wift driver's bugs of Android smartphone.
154 TE 9462D100EB12 [2012_04_29 16.24.47 271 561] INF security STA (94.62.d1.00.fb.12) _ STA DID Deleted. Done wien-1 radio-2 ap-144
155 TR 94631100FB12 $\left[201504-25\right]$ TR $\left[201504-2$
156 TR 9463p100FB12 APC sends disassociation INF (security) STA(94:63:d1:00:fb:12) - Acctstat Msg from AWMB: iface=287 active=1.0x661128a0
157 TR 9463D100FB12 [2013-04-29 16:24:47.27] /// WE <security> STA(94:63:d1:00:fb:12) - Acctstat Msg from AWMB: wlan=1 rx=2619.486206 tx=3087.1188642</security>
158 TR 9463D100FB12 [2013-04-29 16:24:47.269.693] INF [STA] Removed station(94:63:d1:00:fb:12) from BSS(f4:d9:fb:38:ae:11)
159 TR 9463D100FB12 [2013-04-29 16:24:47.269.220] INF <security> STA(94:63:d1:00:fb:12) - STA PLD: Deleted. id=93</security>
160 T 9463D100FB12 [2013-04-29 16:24:47.268.404] INF [0:STA] Dissasoc Sent - STA(94:63:d1:00:fb:12) reason:4WAY HANDSHAKE TIMEOUT.
161 TR 9463D100FB12 [2013-04-29 16:24:47.267.906] INF <security> STA(94:63:d1:00:fb:12) - STA-Info: Removed(0x5564a4e0f0)(ap handle timer). wlan=1 ap=144</security>
radio=2 auth-progress=0
162 TR_9463D100FB12 [2013-04-29 16:24:47.267.680] INF <security> STA(94:63:d1:00:fb:12) - Deauthenticated. reason=15 user=jw2002.shim wlan=1 ap=144 radio=2</security>
163 TR_9463D100FB12 [2013-04-29 16:24:47.267.416] INF <security> STA(94:63:d1:00:fb:12) - Disconnect[WPA authenticator requests disconnect]:</security>
Deauth (15,4WAY HANDSHAKE TIMEOUT)
Ath EAPOL timeout 500ms
TH LAFOL UNREGAL JOUNTS
166 TR 0452D100TD12 (2011 - 5:24:46.766.754] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key Timeout (WPA PTK PTKSTART, WPA PTK GROUP IDLE)</security>
3th EAPOL timeout 500ms
168 TR_9463D100FB12 [2013-04-29 14 24:46.266.454] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s</security>
<sup>16</sup> 2th EAPOL timeout 500ms 24:46.266.314] INF <security> STA (94:63:d1:00:fb:12) - EAPOL-Key Timeout (WPA_PTK_PTKSTART, WPA_PTK_GROUP_IDLE)</security>
170 TR 9463D100FB12 [2013-04-29 16:24:45 766 017] INF (security) STA (94:63:d1:00:fb:12) - FAPOI-Key: Send 1/4 msg of 4-Way b/s
10 It FADOL timeout 200mc (24:45.765.861) INF security STA(94:63:d1:00:fb:12) = EADOL Key Timeout (WEA DTK PEKSTAPT WEA DTK GROUP THE)
172 TR_9463D100FB12 [2013-04-29 16:24:45.565.611] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s</security>
173 TR_9463D100FB12 [2013-04-29 16:24:45.565.486] INF <security> STA(94:63:d1:00:fb:12) - 802.1x Auth Skipped</security>
174 TR_9463D100FB12 [2013-04-29 16:24:45.565.362] INF <security> STA(94:63:d1:00:fb:12) - Authentication started</security>
175 TR_9463D100FB12 [2013-04-29 16:24:45.563.806] INF <security> STA(94:63:d1:00:fb:12) - STA Removed(prune_account_stop). cour over the pio=2</security>
176 TR_9463D100FB12 [2013-04-29 16:24:45.562.591] INF <security> STA(94:63:d1:00:fb:12) - FMK found. FMKID[71,fa,8c,,b9,4e, OKC Starts</security>
177 TR_9463D100FB12 [2013-04-29 16:24:45.562.447] INF <security> STA(94:63:d1:00:fb:12) - (Re)Assoc: PMKID[0][71,fa,8c,,b2,1e,72]</security>
178 TR_9463D100FB12 [2013-04-29 16:24:45.562.354] INF <security> STA(94:63:d1:00:fb:12) - (Re)Assoc: 1 PMKIDs Received</security>
179 TR_9463D100FB12 [2013-04-29 16:24:45.562.261] INF <security> STA(94:63:d1:00:fb:12) - New STA-Info: Added(0x5564a4e0f0). wlan=1 ap=144 radio=2 count=2</security>
180 TR_9463D100FB12 [2013-04-29 16:24:45.562.034] INF <security> STA(94:63:d1:00:fb:12) - OKC: Started. wlan=1 ap=144 radio=2 prev-ap=158 prev-radio=2</security>
181 TR_9463D100FB12 [2013-04-29 16:24:45.558.379] INF [I:STA] STA Moved - BSSs [158]:f4:d9:fb:3a:65:d1 to [144]:f4:d9:fb:38:ae:11
182 TR_9463D100FB12 [2013-04-29 16:24:45.558.138] INF <security> STA(94:63:d1:00:fb:12) - OKC MDS Recv: wlan=1 ap=144 radio=2</security>
183 TR_9463D100FB12 [2013-04-29 16:24:45.557.459] INF [STA] Removed station(94:63:d1:00:fb:12) from BSS(f4:d9:fb:3a:65:d1)
184 TR_9463D100FB12 [2013-04-29 16:24:45.556.262] INF [I:STA] Reassociation - BSSID(f4:d9:fb:38:ae:11) STA(94:63:d1:00:fb:12)

Samsung Wíreless Enterprise™

#### **Trace the Station – EAPOL-logoff**

<ul> <li>Android Smartphone send EAPOL-logoff message right after the successful association</li> <li>Sometimes occurred with Android Smartphone</li> </ul>					
518 TR_FCC734C0D912 [ 11:37:41.849.618] INF [I:STA] Dissassociation - BSSID(f4:d9:fb:37:bd:c2) STA(fc:c7:34:c0:d9:12) STA sends disassociation					
 529 TR_FCC734COD912 [ 11:37:38.192.726] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Stop](EAPOL-Logoff Recv): Stopped. Session 00008401-00000013 wlan=1 ap=33 radio=1</security>					
530 TR FCC734C0D912 [ 11:37:38.192.623] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Stop]: Session 0000840 STA sends EAPOL-logoff suddenly</security>					
531 TR FCC734C0D912 [ 11:37:38.192.189] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Stop]: Session 00008401-000 - x=104,13215,0 tx=89,17784,0</security>					
532 TR_FCC734C0D912 [ 11:37:38.192.008] INF <security> STA(fc:c7:34:c0:d9:12) - 802.1x Recv: EAPOL-Logoff Received</security>					
533 TR_FCC734C0D912 [ 11:37:19.666.134] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Start]: Started. Session 00008401-00000013 wlan=1 ap=33 radio=1 ip=70.31.200.243</security>					
534 TR_FCC734C0D912 [ 11:37:19.657.663] INF <dr_vlan1_110> Forwarded BOOTREPLY[DHCPACK] for fc:c7:34:c0:d9:12 to 70.31.200.243</dr_vlan1_110>					
535 TR_FCC734C0D912 [ 11:37:19.656.992] INF <dsub_dhcpr> DHCP PLD: fc:c7:34:c0:d9:12 station ip set 70.31.200.243</dsub_dhcpr>					
536 TR_FCC734C0D912 [ 11:37:19.656.742] INF <dr_vlan1_110> [DHCPACK] received from dhcp server</dr_vlan1_110>					
537 TR_FCC734C0D912 [ 11:37:19.656.169] INF <dr_vlan1_110> Forwarded BOOTREQUEST[DHCPREQUEST] for fc:c7:34:c0:d9:12 to 70.30.150.30</dr_vlan1_110>					
538 TR_FCC734C0D912 [ 11:37:19.655.749] INF <dr_vlan1_110> [DHCPREQUEST] received from dhcp client</dr_vlan1_110>					
539 TR_FCC734C0D912 [ 11:37:19.653.499] INF <dr_vlan1_110> Forwarded BOOTREPLY[DHCPOFFER] for fc:c7:34:c0:d9:12 to 70.31.200.243</dr_vlan1_110>					
540 TR_FCC734C0D912 [ 11:37:19.653.142] INF <dr_vlan1_110> [DHCPOFFER] received from dhcp server</dr_vlan1_110>					
541 TR_FCC734C0D912 [ 11:37:19.652.523] INF <dr_vlan1_110> Forwarded BOOTREQUEST[DHCPDISCOVER] for fc:c7:34:c0:d9:12 to 70.30.150 20</dr_vlan1_110>					
542 TR_FCC734C0D912 [ 11:37:19.652.019] INF <dr_vlan1_110> [DHCPDISCOVER] received from dhcp client Authentication Completed</dr_vlan1_110>					
543 TR_FCC734C0D912 [ 11:37:19.215.033] INF <security> STA(fc:c7:34:c0:d9:12) - FMKSA-Add: apc=1 pmkid[5f,35,1f,,00,13,d9]</security>					
544 TR_FCC734C0D912 [ 11:37:19.212.616] INF <security> STA(fc:c7:34:c0:d9:12) - Authenticated. user=se13@uready.com vlan=110 qos=0 acl=<none> url=<none></none></none></security>					
545 TR_FCC734C0D912 [ 11:37:19.212.317] INF <security> STA(fc:c7:34:c0:d9:12) - SetFlag[Auth]: wlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=110 qos=0 ap=33 radio=1</security>					
546 TR_FCC734C0D912 [ 11:37:19.211.882] INF <security> STA(fc:c7:34:c0:d9:12) - CAPWAF Send: SetSessionKey: seq=0x02010b90 wlan=1 ap=33 radio=1</security>					
547 TR_FCC734C0D912 [ 11:37:19.211.658] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Recv 4/4 msg of 4-way h/s</security>					
548 TR_FCC734C0D912 [ 11:37:19.209.222] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Send 3/4 msg of 4-way h/s</security>					
549 TR_FCC734C0D912 [ 11:37:19.209.006] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Recv 2/4 msg of 4-way h/s Authentication Succeeded</security>					
550 TR_FCC734C0D912 [ 11:37:19.197.598] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s</security>					
551 TR_FCC734C0D912 [ 11:37:19.196.302] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Recv[Auth]: ACCESS-ACCEPT msg. id=0xe4 len=405</security>					
552 TR_FCC734C0D912 [ 11:37:18.947.503] INF <security> STA(fc:c7:34:c0:d9:12) - 802.1x Recv: EAPOL-Start Received. pae-state=AUTH_PAE_AUTHENTICATING eap- state=EAP_IDLE</security>					
553 TR FCC734C0D912 [ 11:37:18.947.192] INF <security> STA(fc:c7:34:c0:d9:12) - 802.1x Auth Started, reassoc=0</security>					
554 TB FCC734C0D912 [ 11:37:18.947.046] INF <security> STA(fc:c7:34:c0:d9:12) - Authentication started</security>					
555 TR FCC734C0D912 [ 11:37:18.944.506] INF <security> STA(fc:c7:34:c0:d9:12) - No PMKID Received from STA</security>					
556 TR FCC734C0D912 [ 11:37:18.944.400] INF <security> STA(fc:c7:34:c0:d9:12) - New STA-Info: Added(0x1205bbb20), wlan=1 ap=33 radio=1 count=1</security>					
557 TR FCC734C0D912 [ 11:37:18.937.932] INF <security> STA(fc:c7:34:c0:d9:12) - STA PLD: Created. id=135</security>					
558 TR_FCC734C0D912 [ 11:37:18.936.161] INF [I:STA] Association - BSSID(f4:d9:fb:37:bd:c2) STA(fc:c7:34:c0:d9:12)					



#### Station Tracking List

WEC8500# show stationtracking station list
====== Station list =======
1 EC:55:F9:16:2F:17 2 EC:55:F9:99:60:60 3 B4:82:FE:E5:35:26 4 E8:39:DF:08:B1:77 ====== Station list =======

### 2.2.2 Station Tracking Real-time

Samsung Wireless Enterprise™

#### **AP** Association

#### Command: wec8500/configure# stationtracking station D0:22:BE:72:F6:C5 on

WEC8500/configure# stationtracking station D0:22:BE:72:F6:C5 on	
Station Debug On!!!	1 Association starts
WEC8500/configure# *[2014-02-17:15:35:02.987] #TR_D022BE72F6C5-INF: unknown station	1. Association starts
*[2014-02-17:15:35:02.990] #TR_D022BE72F6C5-INF: [I:STA] Association - BSSID(f4:d9:fb:3d:94:62) STA(d0:22:be:72:f6:c5)	
*[2014-02-17:15:35:02.993] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA PLD: Created. wlan=1 ap=1 radio=1 id=1	
*[2014-02-17:15:35:02.999] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - New STA-Info: Added(0x55680010a0). w]an=1 ap	p=1 radio=1 count=1
*[2014-02-17:15:35:02.999] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - No PMKID Received from STA	
*[2014-02-17:15:35:03.000] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - EAPOL-Key: Send 1/4 msg of 4-way h/s. w]an=1	Lap=1 radio=1 2 / way
*[2014-02-17:15:35:03.005] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - EAPOL-Key: Recv 2/4 msg of 4-way h/s. w]an=1	Lap=1 radio=1
*[2014-02-17:15:35:03.005] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - EAPOL-Key: Send 3/4 msg of 4-way h/s. w]an=1	Lap=1 radio=1 handshake
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - EAPOL-Key: Recv 4/4 msg of 4-way h/s. wlan=3	Lap=1 radio=1
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - CAPWAP Send: SetSessionKey: seq=0x00000000 a	apwlan=1 wlan=1 ap=1 radio=1
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - SetFlag[Auth]: wlan=1 802.1x=0 dynvlan=1 aaa	a=0 vlan=0 qos=0 ap=1 radio=1 prev-statu
s=0x802	
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - SetFlag[Auth]: authType=3(PSK) authResult=10	(Success) reauth=0
*[2014-02-17:15:35:03.009] #TR_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - Authenticated	
*[2014-02-17:15:35:03.010] #TR_D022BE72F6C5-INF: [STA_DATA] Auth Done - STA(d0:22:be:72:†6:C5) authType(CACHING Auth) authResult(	Success)
"[2014-02-17:15:35:03.496] #TR_D022BE72F6C5-INF: dr_vlan1_20 [DHCPDISCOVER] received from dhcp client	3 Authentication Complete
"[2014-02-17:15:35:03.496] #TR_D022BE72F6C5-DEB: dsub_dhcpr  ## d0:22:be:72:t6:c5 station PLD info: onOff = 0, server_ip = 0x0	5. Authentication complete
"[2014-02-17:15:35:03.497] #TR_D022BE72F6C5-DEB: dr_v[an1_20 [v]an1.20- fallback]	
"[2014-02-17:15:35:03.497] #TR_D022BE72F6C5-INF: dr_v[an1_20 Forwarded BOOTREQUEST[DHCPDISCOVER] for d0:22:be:72:f6:C5 to 192.1	168.20.1
"[2014-02-17:15:35:03.746] #TR_D022BE72F6C5-INF: dr_v[an1_20 [DHCPOFFER] received from dhcp server	
"[2014-02-1/:15:35:03.746] #TR_D022BE72F6C5-DEB: dr_v[an1_20 DHCP PLD: Found Station.	
"[2014-02-1/:15:35:03.746] #TR_D022BE72F6C5-INF: dr_v[an1_20 Forwarded BOOTREPLY[DHCPOFFER] for d0:22:be:72:t6:c5 to 192.168.20	.38
"[2014-02-17:15:35:03.753] #TR_D022BE72F6C5-INF: dr_vlan1_20 [DHCPREQUEST] received from dhcp_client	4. DHCP process
"[2014-02-17:15:35:03.753] #TR_D022BE72F6C5-DEB: dsub_dhcpr ## d0:22:be:72:T6:C5 station PLD info: onOff = 0, server_ip = 0x0	
"[2014-02-17:15:35:03.754] #TR_D022BE72F6C5-DEB: dr_v[an1_20 [v]an1.20-Tallback]	
"[2014-02-17:15:35:05.754] #TR_DU22BE72F6C5-INF: dr_vlan1_20 Forwarded BootRequest[DHCPREQUEST] for du:22:be:/2:f6:C5 to 192.10	58.20.1
"[2014-02-17:15:35:03.75] #TR_D022BE72F6C5-INF: dr_VIANL20 [DHCPACK] received from ancp server	Station gets an IP address
"[2014-02-17:15:35:05.75] #IR_D0228E72F6C5-INF: dsub_dncpr DHCP PLD: d0:22:06:72:T6:C5 station ip set 192.168.20.38	Station Bets and address
"[2014-02-17:15:35:03,756] #TR_D022BE72F6C5-DEB: dr_Vlan1_20 DHCP PLD: Updated station IP!	
"[2014-02-17:15:55:05.756] #TR_D022BE72F6C5-INF; 07_VIAN_20 FORWarded BOOTREPLY[DHCPACK] TOP 00:22:16:72:16:65 to 192.168.20.3	58 
"[2014-02-17:15:55:05.766] #TR_D022BE72F6C5-INF: Security STA(d0:22:D0:72:T0:C5) - RADIUS ACCT[Start]: Server not configured. S	session 00000401-00000004 wian=1 ap=1 ra
010=L	



### AP Disassociation

WEC8500/configure# \*[2014-02-17:15:07:32.746] #TR\_D022BE72F6C5-INF: [I:STA] Dissassociation Reason(8)- BSSID(f4:d9:fb:3d:94:62) STA(d0:22:be:72:f6:c5)
\*[2014-02-17:15:07:32.748] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA PLD: Deleted. wlan=1 ap=1 radio=1 id=1
\*[2014-02-17:15:07:32.748] #TR\_D022BE72F6C5-INF: [STA] Removed station(d0:22:be:72:f6:c5) from BSS(f4:d9:fb:3d:94:62)
\*[2014-02-17:15:07:32.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA PLD Deleted: Done. wlan=1 radio=1 ap=1
\*[2014-02-17:15:07:32.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA PLD Deleted: Done. wlan=1 radio=1 ap=1
\*[2014-02-17:15:07:32.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA PLD Deleted: Done. wlan=1 radio=1 ap=1
\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA PLD Deleted: Done. wlan=1 radio=1 ap=1
\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA PLD Deleted: Done. wlan=1 radio=1 ap=1
\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA-Info: Removed(0x5568002160)(ap\_handle\_timer). wlan=1 ap=1 radio=1 count=0 auth\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA-Info: Removed(0x5568002160)(ap\_handle\_timer). wlan=1 ap=1 radio=1 count=0 auth\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA-Info: Removed(0x5568002160)(ap\_handle\_timer). wlan=1 ap=1 radio=1 count=0 auth\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA-Info: Removed(0x5568002160)(ap\_handle\_timer). wlan=1 ap=1 radio=1 count=0 auth\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA-Info: Removed(0x5568002160)(ap\_handle\_timer). wlan=1 ap=1 radio=1 count=0 auth\*[2014-02-17:15:07:33.750] #TR\_D022BE72F6C5-INF: security STA(d0:22:be:72:f6:c5) - STA-Info: Removed(0x5568002160)(ap\_handle\_timer). wlan=1 ap=1 radio=1 count=0 auth\*[2014-02-17:1



### Lab 17 -

### **Telnet into the APC and run a station trace**

- 1. Connect your Cell Phone to an AP
- 2. Go to the about phone on your cell and retrieve your mobile phone MAC address
- 3. Telnet to the APC "192.168.xx.10"
- 4. Use this show command WEA8500#
  - 1. show stationtracking station list
  - 2. You should be able to find your mobile MAC address
- 5. Go to configure mode  $\rightarrow$  WEA8500# configure terminal
  - 1. stationtracking station d0:22:be:be:e5:d6 on (Enter your MAC here)
  - 2. Then disconnect and reconnect your mobile device



Packet Capture 2.3.1 APC CLI Configuration 2.3.2 Operation Modes

### 2.3.1 APC CLI Configuration





### 2.3.1 APC CLI Configuration



i.	config-filter					
	1.	(no) ap-mac	: AP MAC			
	2.	(no) enable-ap-mac	: Enable/Disable			
	3.	(no) station-mac	: Station MAC			
	4.	(no) enable-station-mac	: Enable/Disable			
ii.	coi	nfig-ftp: FTP server				
	1.	ipv4-address	: Server IPv4 address			
	2.	login-id	: Login ID & Password			
	3.	remote-file-path	: Remote File Save Location			
	4.	stop-current-forcibly	: FTP stop forcibly			
iii.	(no) enable-capwap-tunneling: include CAPWAP header or not(station-only, not-DTLS mode)					
iv.	filtering-mode [station-only   ap-only]					
	1.	station-only	: Use station MAC			
	2.	ap-only	: Use AP MAC			

## 2.3.1 APC CLI Configuration



- i. operation-mode [active-mode | passive-mode | remote-mode]
  - 1. Operation mode
    - A. active-mode : File create mode, it is saved on system or remote FTP server.
    - B. passive-mode : Voice Enhanced Module triggers specific station's packet capture file automatically.
    - C. remote-mode : Wireshark can receive packet capture information via remote packet capture protocol in real time.

**ii. save-mode** [local | ftp]: operation mode is needed to be active-mode

- 1. local : File will be saved system local disk
- 2. ftp : File will be transported ftp server

#### iii. (no) start-service

- 1. Different action with operation-mode
  - A. active-mode : start/stop packet capture
  - B. remote-mode : start waiting for Wireshark access
  - C. passive-mode : not used



Operation Modes 2.3.2.1 Active Operation Mode 2.3.2.2 Remote Operation Mode

Samsung Wireless Enterprise™

Operation-mode [active-mode | remote-mode]

- active-mode : File create mode, it is saved on the system or on a remote FTP server.
- remote-mode : Wireshark can be setup to receive the packet capture information via remote packet capture protocol in real time.

Samsung

Wireless Enterprise™

### **Active Operation Mode**

- Admin File Save (active mode)
- Save Mode
- Local Disk
- FTP Server Setup
- Trigger Value
- Packet Capturing
- Packet Capture Lab

### 2.3.2.1 Active Operation Mode

Samsung Wíreless Enterprise™

	Default User Name: sams
	Default Password: samsur
ARNING: Urauthorized access to this system is fo will be prosecuted by law. By accessing you agree that your actions may be monit if unauthorized usage is suspected.	erreserves orbidden and \$ this system, \$ tored \$ \$
ERNAME : samsung	not connected - SecureCRT
SWORD : ***********************************	File       Edit       View       Options       Transfer       Script       Tools       Help         10
_WEC8500#	Quick Connect     X       Protocol:     Telnet
	Hostname:         192.168.100.11           Port:         23           Firewall:         None
Logging into the APC via CLI	
	Show quick connect on startup Save session Open in a tab Connect Cancel
	Ready         10, 1         31 Rows, 54 Cols         VT100

# 2.3.2.1 Admin File Save (active mode) Wireless Enterprise

<pre>npi_wEC8500# show pcap current-config detail - Current Status : Idle - Filtering Target : Station - Operation Mode : Admin File Save(active mode) - Save Mode : Local Disk - CAPWAP Option : Disabled - Trigger Values : Period(3600 secs)/File Size(104) - File Save Information(Local save mode) Local Path Disk Usage</pre>							
Saved File List(Last 10)   File Name	Uploaded   Status	Time					
apc_T03-04-10-46-36_RAB.pcap 11:04:10	100	Completed   03-04					
Total File Saved Count							
Filtering Matched Count	Inbound Rate	Outbound Rate					
empty) - Configured Station's MAC List Io. MAC Addr. Filtering Matched Count	Inbound Rate	Outbound Rate					
empty)							
npi WEC8500# show pcap current-config detail							

# 2.3.2.1 Admin File Save (active mode) Wireless Enterprise



# 2.3.2.1 Admin File Save (active mode) Wireless Enterprise

npi_WEC8500# configure terminal npi_WEC8500/configure# pcap npi_WEC8500/configure/pcap# operation-mode active-mode The current operation mode is active-mode. npi_WEC8500/configure/pcap# show pcap current-config detail						
<ul> <li>Current Status : Idle</li> <li>Operation Mode : Admin File Save(active mode)</li> <li>Save Mode : Local Disk</li> <li>CAPWAP Option : Distribution</li> <li>Trigger Values : Per od(3600 secs)/File Size(104857600)</li> <li>File Save Information(Local save mode)</li> <li>Local Path</li></ul>	bytes)/Packet Count(4000000 packets) wser/log/se/pcap/ изокв/204800кв(0.00%)   Uploaded   Status   Time					
apc_T03-04-10-46-36_RAB.pcap Total File Saved Count	This mode can store the pcap file locally on the APC or send the pcap to a FTP Server					
empty) - Configured Station's MAC List No. MAC Addr. Filtering Matched Co empty)	unt Inbound Rate Outbound Rate					



npi\_WEC8500/configure/pcap# save-mode ? local Captured date is saved in local disk ftp Captured date is sent to remote storage using FTP npi\_WEC8500/configure/pcap# save-mode

# npi\_WEC8500/configure/pcap# save-mode ?localCaptured date is saved in local diskftpCaptured date is sent to remote storage using FTPnpi\_WEC8500/configure/pcap# save-mode

### 2.3.2.1 Local Disk

Samsung Wíreless Enterprise™

npi_WEC8500/configure/pcap# start-service Service is started successfully. npi_WEC8500/configure/pcap# show pcap current-config detail - Current Status : Now capturing - Filtering Target : Station - Operation Mode : Admin File Save(active mode) - Save Mode : Local Disk - CAPWAP Option : Disabled				This capture will be saved to the local disk				
<ul> <li>Trigger Values : Period(3600 secs)/File Size(10485/600 bytes)/Packet Count(4000000 packets)</li> <li>Current Info to Save File</li> <li>Seconds to Trigger</li></ul>								
– File Save Infor Local Path Disk Usage	mation(Local s	ave mode)		/user/log/se/pc 8кв/204800кв(0.	ap/			
Saved File   File N   apc_T0   apc_T0   apc_T0	List(Last 10) ame 3-04-10-46-36_ 3-17-14-10-59_ 3-17-14-19-27_	RAB.pcap RAB.pcap RAB.pcap			Uploac   1   1	ed   Status 00   00   00	Completed Completed Completed	Time 03-04 11:04:10 03-17 14:12:11 03-17 14:19:49
Total File Error Coun	Saved Count .			3 0				
- Configured AP's	MAC List ddr. Fi	ltering	Matched	Count	Inbo	und Rate	Outbound	Rate
1 F4:D9:FB: ID	3D:C4:84 Prf.	>ON AP Name		0 IPv4 Addr		0.0 kbps		0.0 kbps
1	ap_1		npi_Lab_AP	192.168.10.100				
- Configured Stat	ion's MAC List ddr. Fi	ltering	Matched	Count	Inbo	und Rate	Outbound	Rate
1 1C:99:4C: AP	AB:29:F8 WN	>ON SSID		282 IPv4 Addr		0.0 kbps		0.0 kbps
1	1		SamsungNPI 1	192.168.100.129				

npi\_WEC8500/configure/pcap# start-service

Service is started successfully.

npi\_WEC8500/configure/pcap# show pcap current-config detail

### 2.3.2.1 Local Disk

Samsung Wireless Enterprise™

hpi_wEC8500/configure/pcap# no start-service									
npi_WEC	8500/configure/pcap# :	show pcap current	After you stop the service, the file						
<ul> <li>Current Status : Idle</li> <li>Filtering Target : Station</li> <li>Operation Mode : Admin File Save(active mode)</li> <li>Save Mode : Local Disk</li> <li>CAPWAP Option : Disabled</li> <li>Trigger Values : Period(3600 secs)/File Size(104857600 bytes)/Pack</li> </ul>			will be saved on the disk. Here is the Saved File List						
- File	Save Information(Loca Local Path	al save mode)	/user/log/se	/pcap/					
	Saved File List(Last   File Name   apc_T03-04-10-46   apc_T03-17-14-10   apc_T03-17-14-19   apc_T03-17-14-19	10) -36_RAB.pcap -59_RAB.pcap -27_RAB.pcap -54_RAB.pcap		Uploaded   Status   100     100     100     100	Time Completed 03–04 11:04:10 Completed 03–17 14:12:11 Completed 03–17 14:19:49 Completed 03–17 14:33:36				
	Total File Saved Count								
- Conf No.	igured AP's MAC List MAC Addr.	Filtering	Matched Count	Inbound Rate	Outbound Rate				
1	F4:D9:FB:3D:C4:84 ID Prf.	>ON AP Name	IPv4 Addr	0 0.0 kbps	0.0 kbps				
	1 ap_1		npi_Lab_AP 192.168.10.1	.00					
- Configured Station's MAC List									
NO.	MAC Addr.	Filtering	Matched Count	Inbound Rate	Outbound Rate				
1	1C:99:4C:AB:29:F8 AP WN	>ON SSID	3,4 IPv4 Addr	82 0.0 kbps	0.0 kbps				
	1 1		SamsungNPI 192.168.100.1	29					

npi\_WEC8500/configure/pcap# no start-service

Service is stopped successfully.

npi\_WEC8500/configure/pcap# show pcap current-config detail

### 2.3.2.1 Local Disk




#### 2.3.2.1 Local Disk





#### 2.3.2.1 FTP Server Setup

Samsung Wíreless Enterprise™

npi_WEC The cur npi_WEC	28500/configure/pcap# rrent save mode is ftp 28500/configure/pcap#	save-mode ftp show pcap current	-config deta	11			
- Curn - Filt - Open - Save - CAPW - Trig	rent Status : Idle ering Target : Statio ration Mode : Admin Mode : FTP MAP Option : Disabl gger Values : Period	n File Save(active ed (3600 secs)/File	mode) size(10 <mark>485760</mark>	00 bytes)/Packet	: Count(4000000 packets	)	
- File	<pre>2 Save Infomation(FTP IPv4 Address Login Name/Password Remote Path Uploaded File List(L   File Name   apc_T03-04-10-46   apc_T03-17-14-10   apc_T03-17-14-19   apc_T03-17-14-19</pre>	save mode) ast 10) -36_RAB.pcap -59_RAB.pcap -27_RAB.pcap -54_RAB.pcap		192.168.0.101 admin/admin ~/pcapFtp/	Uploaded   Status   100     100     100     100	Time Completed   03-04 11: Completed   03-17 14: Completed   03-17 14: Completed   03-17 14:	04:10   12:11   19:49   33:36
	Total Uploaded Count Error Count			4 0			
- Conf No.	igured AP's MAC List MAC Addr.	Filtering	Matched	Count	Inbound Rate	Outbound Rate	
1	F4:D9:FB:3D:C4:84 ID Prf.	>ON AP Name		0 IPv4 Addr	0.0 kbps	0.0 kbps	
	1 ap_1		npi_Lab_AP	192.168.10.100			
- Conf No.	igured Station's MAC MAC Addr.	List Filtering	Matched	Count	Inbound Rate	Outbound Rate	
1	1C:99:4C:AB:29:F8 AP WN	>ON SSID		3,482 IPv4 Addr	0.0 kbps	0.0 kbps	
	1 1		SamsungNPI 1	192.168.100.129			

npi\_WEC8500/configure/pcap# save-mode ftp

The current save mode is ftp.

npi\_WEC8500/configure/pcap# show pcap current-config detail



npi\_wEC8500/configure/pcap# npi\_wEC8500/configure/pcap# npi\_wEC8500/configure/pcap# config-ftp npi\_wEC8500/configure/pcap/config-ftp# ?

forcibly
forcik

npi\_WEC8500/configure/pcap/config-ftp# ipv4-address 192.168.100.99 FTP server IPv4 address is configured(192.168.100.99). npi\_WEC8500/configure/pcap/config-ftp# login-id samsung samsung\*# FTP Login ID(samsung) and Password(samsung) is configured. npi\_WEC8500/configure/pcap/config-ftp# remote-file-path Traces/ FTP Remote Path(Traces/) is configured. npi\_WEC8500/configure/pcap/config-ftp# exit npi\_WEC8500/configure/pcap/config-ftp# exit

#### 2.3.2.1 FTP Server Setup

Samsung Wireless Enterprise™

npi_WEC8500/configure/pcap# start-service Service is started successfully. npi_WEC8500/configure/pcap# show pcap current - Current Status : Now capturing - Filtering Target : Station - Operation Mode : Admin File Save(active - Save Mode : FTP - CAPWAP Option : Disabled - Trigger Values : Period(60 secs)/File Si	config detail mode) ize(1048576 bytes)/Packet C	Once the Trigger Per will be sent to your F You can also force th service	iod expires the pcap TP Server. his by stopping the
- Current Info to Save File Seconds to Trigger Bytes to Trigger Packets to Trigger	9/60 0/1048576 0/50000		
File Save Infomation(FTP save node) IPv4 Address Login Name/Password Remote Path Uploaded File List(Last 10)   File Name apc_T03-19-05-35-17_RTM.pcap apc_T03-19-06-09-49_RTM.pcap apc_T03-19-06-14-56_RTM.pcap apc_T03-19-08-32-08_RTM.pcap apc_T03-19-08-32-08_RTM.pcap apc_T03-19-04-58-22_RTM.pcap apc_T03-19-05-04-37_RTM.pcap apc_T03-19-05-07-21_RTM.pcap apc_T03-19-05-07-21_RTM.pcap apc_T03-19-05-01-41_RTM.pcap apc_T03-19-05-11-41_RTM.pcap Total Uploaded Count	9 	g*# Uploaded   Status 0 Cannot acc 100 C 100 C 100 C 100 C 0 Cannot acc 0 Cannot acc 0 Cannot acc 0 Cannot acc 0 Cannot acc	Time ess file 03-19 05:36:38 ompleted 03-19 06:10:50 ompleted 03-19 06:15:57 ompleted 03-19 08:20:55 ompleted 03-19 08:33:08 ess file 03-19 04:59:43 ompleted 03-19 05:05:38 ess file 03-19 05:08:43 ess file 03-19 05:11:02 ess file 03-19 05:13:02
- Configured AP's MAC List No. MAC Addr. Filtering	Matched Count	Inbound Rate	Outbound Rate
(empty)			
- Configured Station's MAC List No. MAC Addr. Filtering	Matched Count	Inbound Rate	Outbound Rate
1 1C:99:4C:AB:29:F8>ON AP WN SSID	155,420 IPv4 Addr	0.0 kbps	0.0 kbps
1 1	SamsungNPI 192.168.100.129		

#### 2.3.2.1 Trigger Value





 npi\_WEC8500/configure# pcap

 npi\_WEC8500/configure/pcap# trigger-value ?

 60 - 3600
 Period second (60 - 3600)

 npi\_WEC8500/configure/pcap# trigger-value 60 ?

 500 - 102400
 File size (KBytes: 500 - 102400)

 npi\_WEC8500/configure/pcap# trigger-value 60 500 ?

 5000 - 4000000
 Packet count (5000 - 400000)

 npi\_WEC8500/configure/pcap# trigger-value 60 500 ?

 5000 - 4000000
 Packet count (5000 - 400000)

 npi\_WEC8500/configure/pcap# trigger-value 60 500 50000

#### **Packet Capturing**

#### Samsung Wireless Enterprise™

#### Packet Capturing Steps

- MAC of a Station
- MAC of a Access Point
- Configuring Filtering Mode
- Operation Mode
- Save Mode
- Setup Trigger Value
- Start the Service

#### MAC of a Station

Samsung Wireless Enterprise™



#### MAC of a Station



npi_wEC8500/configure/pcap# co npi_wEC8500/configure/pcap/con The MAC value is added success npi_wEC8500/configure/pcap/con	nfig-filter fig-filter# station fully. fig-filter# show pc	-mac 1c:99:4c:ab ap current-confi	:29:f8 g detail		
- Current Status : Idle - Filtering Target : Station - Operation Mode : Remote P	acket Capture(remot	e mode)			
- Configured AP's MAC List No. MAC Addr. ===== ===============================	Filtering	Matched Count		Inbound Rate ====================================	Outbound Rate
- Configured Station's MAC Li	st Filtoning	Matiched Count		Troound Date	Outbound Date
NO. MAC Addr.		Matcheu Count		100unu kate	outbound Rate
1 1C:99:4C:AB:29:F8 0 AP WN	FF< SSID	IPV4	0 Addr	0.0 kbps	0.0 kbps
1 1	Sam:	sungNPI 192.168.	100.129		

npi\_WEC8500/configure/pcap# config-filter npi\_WEC8500/configure/pcap/config-filter# station-mac 1c:99:4c:ab:29:f8 npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail

#### MAC of a Station



immary	Static You can	see st	ations that ar	e con	nectio	on to your AP	C and what A	Р			
tive Alarm	Current Filter :	on is o None	connected to							Char	nae
ANs										_	
ress Points	•									E	port
										Total E	intry : 6
tions	MAC	USER NAME	IP ADDRESS	AP	NAME	SSID	AP MAP LOC.	AUTH.	CYPHER	PROTOCOL	CHANN
uc5	<u>68:94:23:11:74:d0</u>	Eddie	192.168.100.115	AP	303i	npiDesks		WPA2	CCMP	802.11n(5GHz)	161
erference Devices	20:10:7a:56:dd:13		192.168.100.118	npi_l	ab_AP	SamsungNPI		WPA2	CCMP	802.11n(5GHz)	153
tistics	50:ea:d6:67:4b:db		192.168.6.100	npi J	ab_AP	Sales		WPA2	CCMP	802.11n(2.4GHz)	11
	1c:99:4c:ab:29:f8		192.168.100.129	npi_L	.ab_AP	SamsungNPI		WPA2	CCMP	802.11n(5GHz)	153
P Calls	d0:22:be:et:92:a7		192.168.100.119	npi_L	.ab_AP	SamsungNPI		WPA2	CCMP	802.11n(5GHz)	153
0111111	38:aa:3c:93:69:e2		192.168.100.120	npi_L	.ab_AP	SamsungNPI		WPA2	CCMP	802.11n(5GHz)	153

#### MAC of a Access Point



Samsung Wireless Enterprise	M	onitor Configura	tion   Admini	stration   Help						
Summary Active Alarm		Access Points > All AP		Here w station	ve can find i is conned	l the MAC o cted to	f the AP our			
WLANs Access Points	•	Current Filter : Noi	ne						Ex	port
All APs Radios	•	(e) : Edge AP, (r) : Remote AP PROFILE NAME		MAC ADDRESS	IP ADDRESS	UP TIME	CAPWAP UP TIME	ADMIN STATUS	Total E OPER STATUS	ntry : 2 MAP LOCATION
Stations		<u>ap 1</u>	npi_Lab_AP	f4:d9:fb:3d:c4:84	192.168.10.100	17 day, 21 hour, 8 min, 49 sec	5 day, 11 min, 57 sec	Up	Up	
Rogues Interference Devices		<u>ap 3</u>	AP_303i	f4:d9:fb:36:ca:af	192.168.10.102	17 day, 21 hour, 8 min, 51 sec	5 day, 11 min, 51 sec	Up	Up	
Statistics	•				1					
VoIP Calls	Þ									
Resource	_							_	_	

#### MAC of a Access Point



npi_WEC8 The MAC npi_WEC8 - Curre - Filte - Opera - Confi No.	S500/configure/pcap/c value is added succe S500/configure/pcap/c ent Status : Idle ering Target : Static tion Mode : Remote gured AP's MAC List MAC Addr.	config-filter# ap ssfully. config-filter# sh Packet Captured Filtering	o-mac f4:d9:fb: now pcap currer (remote mod <del>e)</del> Matc <mark>n</mark> ed	3d:c4:84 nt-config de Count	AP an addec Next, Filteri	d Station MAC's have b I. you need to activate th ng now	een ne	e
===== = = 5	F4:D9:FB:3D:C4:84	OFF<	<u></u>	IPv4 Addr	0	0.0 kbps	0.0	kbp
_	1 ap_1		npi_Lab_AP	192.168.10.	100			
- Confi No.	gured Station's MAC MAC Addr.	List Filtering	Matched	Count		Inbound Rate	Outbound Rate	e ====
1	1C:99:4C:AB:29:F8	OFF<			0	0.0 kbps	0.0	kbp
,	AP WN	S ID		IPv4 Addr				
	1 1		SamsungNPI 1	92.168.100.	129			

npi\_WEC8500/configure/pcap/config-filter# ap-mac f4:d9:fb:3d:c4:84 npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail

## **Configuring Filtering Mode**



npi_wEC8500/configure/pcap# filtering-mode ? station-only Filtering station mac only ap-only Filtering AP mac only npi_wEC8500/configure/pcap# filtering-mode station-only	(default)
npi_wEC8500/configure/pcap# show pcap current-config detail - Current Status : Idle - Filtering Target : Station - Operation Mode : Admin File Save(active mode)	Select the Filtering mode here
<ul> <li>Save Mode : FTP</li> <li>CAPWAP Option : Disabled</li> <li>Trigger Values : Period(60 secs)/File Size(1048576 bytes</li> </ul>	s)/Packet Count(50000 packets)

npi\_WEC8500/configure/pcap# filtering-mode ?station-onlyFiltering station mac only (default)ap-onlyFiltering AP mac onlynpi\_WEC8500/configure/pcap# filtering-mode station-onlyThe current filtering target is station-only.npi\_WEC8500/configure/pcap# show pcap current-config detail

## **Configuring Filtering Mode**



Samsung

Wireless Enterp

npi\_WEC8500/configure/pcap/config-filter# enable-ap-mac 1

The index of MAC value is applied to capturing rule.

npi\_WEC8500/configure/pcap/config-filter# enable-station-mac 1

The index of MAC value is applied to capturing rule.

npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail





 npi\_WEC8500/configure# pcap

 npi\_WEC8500/configure/pcap# trigger-value ?

 60 - 3600
 Period second (60 - 3600)

 npi\_WEC8500/configure/pcap# trigger-value 60 ?

 500 - 102400
 File size (KBytes: 500 - 102400)

 npi\_WEC8500/configure/pcap# trigger-value 60 500 ?

 5000 - 4000000
 Packet count (5000 - 400000)

 npi\_WEC8500/configure/pcap# trigger-value 60 500 ?

 5000 - 4000000
 Packet count (5000 - 400000)

 npi\_WEC8500/configure/pcap# trigger-value 60 500 50000



npi_wEC8500/configure/pcap# trigger-value 60 1024 50000 Trigger values are configured(60/1024/50000). npi_wEC8500/configure/pcap# show pcap current-config detail		
<ul> <li>Current Status : Idle</li> <li>Filtering Target : Station</li> <li>Operation Mode : Admin File Save(active mode)</li> <li>Save Mode : Local Disk</li> <li>CAPWAP Option : Disabled</li> <li>Trigger Values : Period(60 secs)/File Size(1048576 bytes)/Packet Compared to the second seco</li></ul>	ount(50000 packets)	
<ul> <li>File Save Information(Local save mode) Local Path</li> <li>Disk Usage</li> <li>Local Path</li> </ul>	рсар/ кв(0.00%)	
	Trigger Value has been set	

#### Start the Service

Samsung Wireless Enterprise™



npi\_WEC8500/configure/pcap/config-filter# exit
npi\_WEC8500/configure/pcap# start-service
Service is started successfully.
npi\_WEC8500/configure/pcap# show pcap current-config detail



## Lab 18 – (1/2)

Telnet into the APC and get a pcap of a connected device.

The pcap should be stored locally and retrieved to the computer desktop

Connect a station to a WLAN Find the MAC address of that device Add the station here npi\_WEC8500# configure terminal npi\_WEC8500/configure# pcap npi\_WEC8500/configure/pcap# config-filter npi\_WEC8500/configure/pcap/config-filter# station-mac D0:22:BE:BE:E5:D6 Set Filtering to ON npi\_WEC8500/configure/pcap/config-filter# enable-station-mac 1 npi\_WEC8500/configure/pcap/config-filter# exit Select Operation Mode npi WEC8500/configure/pcap# operation-mode active-mode Select Save Mode npi\_WEC8500/configure/pcap# save-mode local Set Trigger Value npi WEC8500/configure/pcap# trigger-value 60 1024 50000



### Lab 18 – (1/2)

#### Telnet into the APC and get a pcap of a connected device. The pcap should be stored locally and retrieved to the computer desktop

Check the current config npi\_WEC8500/configure/pcap# show pcap current-config detail

Samsung

Wireless Enterpi

#### Remote Operation Mode

- Remote Packet Capture
- Select Operation Mode
- Configuring the MAC of a station
- Configuring AP MAC address
- Configuring Filtering Mode
- Starting the Service
- Computer Setup
- Stopping the Service



## Remote Packet Capture w/Wire-Shark

• The APC can capture a packet exchanged between the wireless terminals on a remote PC in real-time by using the remote packet capture protocol.



#### PLEASE NOTE!

- You will need to have Wireshark installed on your PC
- Downloadable URL: <u>http://www.wireshark.org/download.html.</u>
- Wireshark: <u>1.10.2</u> Stable & Latest version
- WinPcap: 4.1.3 Stable & Latest version
   Included in Wireshark installation image

#### 2.3.2.2 Remote Packet Capture



1	not	connec	ted - Se	cureCRT							23
	File	Edit	View	Options	Transfer	Script	Tools	Help			
	23		I X	h	#	58 🖨		X 1	0		Ŧ
l											<u> </u>
l	Qui	ick Con	nect							×	
	PI	rotocol:	(	Telnet	•	•]					
	н	ostname	e:	192.168.1	00.11	4					
	P	ort:	[	23	Firewall:	None			•		
1											
l											
۱											=
		Show	quick cor	nnect on sta	rtup	V Save	e sessio	n			
						Ope	n in a t	ab		_	
						Cor	nnect		Cancel		
							-				-
L	Ready	_	_			10, 1	31 Ro	ws, 54	Cols	V1100	H.

#### First we will need to setup the APC

#### Steps to setup

- 1. Start by telneting into the APC
- 2. Select the Operation Mode
- 3. Setup the pcap config for the station
- 4. Setup the pcap config for the AP
- 5. Enable the Filtering
- 6. Start the service
- Setup our PC that has the Wireshark installed to capture the traffic

#### 2.3.2.2 Remote Packet Capture

Samsung Wireless Enterprise™

Logging into the APC via CLI	Default User Name: samsung
	Default Password: samsung
<pre>\$ \$ SwARNING: Ur authorized access to this system is forbidden a     will be prosecuted by law. By accessing this system     you agree that your actions may be monitored     if unauthorized usage is suspected. </pre>	=====\$ nd \$ em, \$ \$ =====\$
USERNAME : samsung PASSWORD : ******	
LAST LOGIN TIME : 2014-03-05 16:09:03 LOGIN FAIL COUNT : 1	
npi_wEC8500#	

#### 2.3.2.2 Select Operation Mode

npi\_wEC8500# show pcap current-config detail Using the show command we can view the - Current Status : Idle 💳 current pcap config detail Filtering Target : Station Operation Mode : Admin File Save(active mode) Save Mode : Local Disk - CAPWAP Option : Disabled - Trigger Values : Period(3600 secs)/File Size(104857600 bytes)/Packet Count(4000000 packets) File Save Information(Local save mode) File Name | Uploaded | Status | Time apc\_T03-04-10-46-36\_RAB.pcap 100 Completed 03-04 11:04:10 Total File Saved Count ..... 1 Error Count ..... 0 Configured AP's MAC List Filtering Inbound Rate Matched Count Outbound Rate \_\_\_\_\_ \_\_\_\_ \_\_\_\_\_\_ \_\_\_\_ (empty) Configured Station's MAC List Inbound Rate Matched Count Outbound Rate - terinc (empty)

Samsung

Wireless Enterprise

WE-WLAN - Day 2 - Jan. 2015

#### 2.3.2.2 Select Operation Mode



Samsung

Wireless Enterprise

#### 2.3.2.2 Select Operation Mode

EC8500# configure terminal wec8500/configure#\_pcap Change the Operation Mode to Remote WEC8500/configure/pcap# operation-mode remote-mode current operation mode is remote-mode. WEC8500/configure/pcap# show pcap current-config detail : Idle - Current Status : Remote Packet Capture(remote mode) Operation Mode - Configured AP's MAC List Filterind NO. Matched Count Inbound Rate Outbound Addr. (empty) - Configured Station's MAC List Matched Count NO. MAC Addr. Inbound Rate Outbound Rate (empty)

Samsung

Wireless Enterpr

npi\_WEC8500# configure terminal npi\_WEC8500/configure# pcap npi\_WEC8500/configure/pcap# operation-mode remote-mode

#### 2.3.2.2 Configuring MAC of a station



Samsung Wireless Enterprise™

#### 2.3.2.2 Configuring MAC of a station

npi_wec85 npi_wec85 The MAC v npi_wec85	00/configure/pcap# 00/configure/pcap/c alue is added succe 00/configure/pcap/c	config-filter config-filter# sta csfully. config-filter# sho	tion-mac 1c:99:4c:ab:29:fi w pcap current-config deta	B ail	
- Curren - Filter - Operat	t Status : Idle ing Target : Statio ion Mode : Remote	n : Packet Capture(r	emote mode)		
- Config No.	ured AP's MAC List MAC Addr.	Filtering	Matched Count	Inbound Rate	Outbound Rate
(empty)					
- Config No.	ured Station's MAC MAC Addr.	List Filtering	Matched Count	Inbound Rate	Outbound Rate
1	1C:99:4C:AB:29:F8 AP WN	OFF< SSID	IPv4 Addr	0 0.0 kbps	0.0 kbps
	1 1		SamsungNPI 192.168.100.13	29	

Samsung Wireless Enterpr

npi\_WEC8500/configure/pcap# config-filter npi\_WEC8500/configure/pcap/config-filter# station-mac 1c:99:4c:ab:29:f8 npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail

#### 2.3.2.2 Configuring MAC of a station



Samsung Wireless Enterprise™

## 2.3.2.2 Configuring AP MAC address Wireless Enterprise

Samsung Wireless Enterprise	Monitor Configura	ation   Admir	nistration   Help						
Summary	Access Points > All AP	5	Here	we can	find the	MAC of t	he		
Active Alarm	Current Filter : No	one	ΑΡοι	ur static	on is conr	nected to		Char	nge
WLANs									
Access Points								Đ	cport
All APs	(e) : Edge AP, (r) : Remote	₽ AP						Total E	intry : 2
Radios >	AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	UP TIME	CAPWAP UP TIME	ADMIN STATUS	STATUS	MAP LOCATION
Stations	<u>ap 1</u>	npi_Lab_AP	f4:d9:fb:3d:c4:84	192.168.10.100	17 day, 21 hour, 8 min, 49 sec	5 day, 11 min, 57 sec	Up	Up	
Rogues	<u>ap 3</u>	AP_303i	f4:d9:fb:36:ca:af	192.168.10.102	17 day, 21 hour, 8 min, 51 sec	5 day, 11 min, 51 sec	Up	Up	
Interference Devices									
Statistics >	_			1					
VoIP Calls →									
Resource									
-									

#### 2.3.2.2 Configuring AP MAC address

npi\_wEC8500/configure/pcap/config-filter# ap-mac f4:d9:fb:3d:c4:84 The MAC value is added successfully. npi\_wEC8500/configure/pcap/config-filter# show pcap current-config detail Current Status : Idle Filtering Target Station AP and Station MAC's have Remote Packet Capture(remote mode) Operation Mode been added. Configured AP's MAC List ٧O. Filterina Matched Count ound Rate You need to activate the F4:D9:FB:3D:C4:84 0.0 kbp OFE<--Filtering now ID Prf. AP TPVA ame npi\_Lab\_AP 192.168.10.100 ap\_1 1 Configured Station's MAC List Matched Count Inbound Rate outbound Rate 1C:99:4C:AB:29:F8 0.0 kbps 0.0 kbp OFF<---0 SSID IPv4 Addr SamsungNPI 192.168.100.129 1

Samsung

Wireless Enterp

npi\_WEC8500/configure/pcap/config-filter# ap-mac f4:d9:fb:3d:c4:84 npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail

#### 2.3.2.2 Configuring Filtering Mode



<pre>npi_WEC8500/configure/pcap# filtering-mode ?    station-only</pre>	ault)
<ul> <li>Current Status : Idle</li> <li>Filtering Target : Station</li> <li>Operation Mode : Admin File Save(active mode)</li> </ul>	Select the Filtering mode here
<ul> <li>Save Mode : FTP</li> <li>CAPWAP Option : Disabled</li> <li>Trigger Values : Period(60 secs)/File Size(1048576 bytes)/F</li> </ul>	Packet Count(50000 packets)

npi_WEC8500/configu	re/pcap# filtering-mode ?
station-only	Filtering station mac only (default)
ap-only	Filtering AP mac only
npi_WEC8500/configu	re/pcap# filtering-mode station-only
The current filtering ta	rget is station-only.
npi_WEC8500/configu	re/pcap# show pcap current-config detail

## 2.3.2.2 Configuring Filtering Mode

Samsung Wireless Enterprise™



npi\_WEC8500/configure/pcap/config-filter# enable-ap-mac 1 The index of MAC value is applied to capturing rule. npi\_WEC8500/configure/pcap/config-filter# enable-station-mac 1 The index of MAC value is applied to capturing rule. npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail

#### 2.3.2.2 Starting the Service

Samsung Wireless Enterprise™

npi_wEC8 npi_wEC8 service npi_wEC8 - Curre rilte - Opera	3500/configure/p 3500/configure/p is started succ 3500/configure/p ent Status : W ation Mode : F	pcap/config-filter# pcap# start-service cessfully. pcap# show pcap cur wating for client's Station Remote Packet Captu	exit rent-config deta access re(remote mode)	il	The Wire con	APC is now waitineshark to make the the section	ng for ne remote
- Conf <sup>*</sup> No.	igured AP's MAC MAC Addr.	List Filtering	Matched	Count		Inbound Rate	Outbound Rate
1	F4:D9:FB:3D:C4 ID Prf.	4:84>ON AP N	ame	IPv4 Addr	0	0.0 kbps	0.0 kbps
-	1 a	ap_1	npi_Lab_AP	192.168.10.	100		
- Conf <sup>*</sup> No.	igured Station's MAC Addr.	s MAC List Filtering	Matched	Count		Inbound Rate	Outbound Rate
1	1C:99:4C:AB:29 AP WN	9:F8>ON SSI	D	IPv4 Addr	0	0.0 kbps	0.0 kbps
	1 1	 1	SamsungNPI :	192.168.100.	129		

npi\_WEC8500/configure/pcap/config-filter# exit npi\_WEC8500/configure/pcap# start-service Service is started successfully. npi\_WEC8500/configure/pcap# show pcap current-config detail



# The configuration for the capture of packets is finished, now we need to setup our Wireshark on our computer

#### 2.3.2.2 Computer Setup



#### Capture $\rightarrow$ Options... 'Manage Interfaces' click

pture									
Capture		Interface		Link-layer he	ader Pr	om. Mode	Snaplen [B	8] Buffer [MB]	Capture Filter
	Wireless Net fe80:8fa:96aa:41 192:168:100:110	work Connect 34:52c6	ion	Ethernet		enabled	default	2	E
	Local Area Co fe80::e444:1564:2 10.26:206.151	e77:8ce9		Ethernet		enabled	default	2	
	Local Area Co	onnection* 11		Ethernet		enabled	default	2	
	Local Area Co	onnection* 9						-	<b>.</b>
Capt	ture on all inter promiscuous r	faces node on all int	erface	s				<b>v</b>	Compile selected BPFs
nture F	iles							Display Options	· · · · · · · · · · · · · · · · · · ·
pearer									
File:						Brow	/se	Update list of	f packets in real time
Use	<u>m</u> ultiple files			Use pcap-ng f	ormat			Automaticall	y scroll during live capture
✓ Next	file every	1	÷ n	nebibyte(s)	-			TR. I. Cala another	info dialogo
Next	file every	1	÷ n	ninute(s)	~			Inde capture	into dialog
Ring	buffer with	2	fi	les				Name Resolution	
Stop	capture after	1	÷ fi	le(s)				Resolve MAC	addresses
op Capt	ure Automatic	ally After						Resolve <u>n</u> etw	ork-layer names
	* *	packet(s)						Resolve trans	port-laver name
1	* *	mebibyte(s)	-					<u>_</u>	
1       1	A.	minute(s)	-					Use <u>e</u> xternal	network name resolver
	¥								


#### 'Remote Interfaces' tab click and 'Add' Click







Host: 192.168.100.11		📕 Wireshark: Remote In 💷 💷 💌
Port: 2002   Authentication   Interface IP on   the network   that your PC is     On     Port:   2002   Authentication   Interface IP on   the network   that your PC is		Host: 192.168.100.11
This address should be the Interface IP on the network that your PC is On		Port: 2002 Authentication
	This address should be the Interface IP on the network that your PC is on	<ul> <li>Null authentication</li> <li>Password authentication</li> <li>Username:</li> <li>Password:</li> <li><u>OK</u> <u>Cancel</u></li> </ul>



#### Check the registration of AP Controller, 'Close' click

Interface Management	te Interfaces	
Remote Interfaces		
Host	▲ Name	<ul> <li>Hide</li> </ul>
□ 192.168.100.11	rpcap://[192.168.100.11]:2002/wec8500remotePCAP	
<u>A</u> dd <u>D</u> elete		Apply <u>C</u> lose



#### Select AP Controller Interface, 'Start' click

Wiresha	rk: Capture Opt	tions					
Capture							
Captur	e	Interface	Link-layer hea	der Prom. Mode	Snaplen [B]	Buffer [MB]	Capture Filter
	Local Area Co fe80:cc5f:8ca5:64	onnection* 9 468:415f	Ethernet	enabled	default	2	
	Local Area Co fe80::b1fc:c6a4:3 192.168.100.97	onnection 2 7d3:541f	Ethernet	enabled	default	2	
	Wireless Net fe80::bcf9:34cd:9 0.0.0.0	work Connection 2 935:8f29	2 Ethernet	enabled	default	2	=
	rpcap://[192.	168.100.11]:2002/	Ethernet	enabled	default	2	-
<							4
Cap	oure on all inter	faces					Manage Interfaces
Use	promiscuous n	node on all interfac	es				
<u>C</u> aptur	re Filter:					<u> </u>	Compile selected BPFs
Capture F	Files				D	isplay Options	
File:				Brow	se	☑ Update list of	f packets in real time
Use	<u>m</u> ultiple files		🖉 Use pcap-ng fo	rmat		Automaticall	y scroll during live capture
✓ Nex	t file every t file every		mebibyte(s) minute(s)			✓ <u>H</u> ide capture	info dialog
Ring	g buffer with	2	files		м	lame Resolution	
Sto	p capture after	1	file(s)			Resolve MAC	addresses
Stop Cap	ture Automatic	ally After				Resolve <u>n</u> etw	ork-layer names
<b>1</b>	×	packet(s)				Resolve <u>t</u> rans	port-layer name
		mebibyte(s) 🔻					network name resolver
	v	minute(s) 👻				Se external	network hame resolver
Help							Start Close

Samsung Wireless Enterprise™

#### **Display Capturing packets**

🔏 Ca	pturing from r	ocap://[192.16	58.100.11]:2	002/wec85	00remotePCA	P [Wire	eshark 1.10.2	(SVN I	Rev 51934	from /tru	unk-1.	10)]						x
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture	<u>A</u> nalyze	Statistics	Telephony	<u>T</u> ools	Internals H	<u>H</u> elp										
0	ا 👗 🖲	2   🖹 🖁	X2	0	• 🕸 💫 रै	F 🕹		⊕ (		T   M	( 🗹	<b>1</b>	%   <b>(</b>	ġ				
Filter	ip.addr == 1	92.168.100.12	5				<ul> <li>Expressi</li> </ul>	ion (	<b>Clear</b> Ap	ply Sav	e							
No.	Time	Source		0	estination		Protoco	ol	Le	ength In	lfo							~
	1 0.0000	0000 192.1	.68.100.1	L25 1	173.194.77	7.188	тср			162 5	9489	> h	pvroo	m [PSH	I, ACK	] Seq=	1 AC	k=
	2 0.0230	5400 173.1	.94.77.18	38 1	192.168.10	0.125	TCP			66 h	pvro	om >	5948	9 [ACK	[] Seq	=1 Ack	=97	Wile
	3 5.2399	9700 192.1	.68.100.1	L25 8	8.8.8.8		DNS			79 S	tand	ard	query	0xa9c	:1 A	api.cr	itte	rc
	4 5.2420	3400 192.1	68.100.1	L25 8	8.8.8.8		DNS			83 S	tand	ard	query	0x269	A 80	b.scor	ecar	dr
	5 5.2614	9700 8.8.8	.8	1	192.168.10	0.125	DNS			157 S	tand	ard	query	respo	nse 0	xa9c1	CNA	ME
	6 5.2635	3600 8.8.8		]	192.168.10	0.125	DNS			277 S	tand	ard	query	respo	nse 0	x2698	CNA	ME
	/ 5.2646	0600 192.1	.68.100.1	125 1	184.169.18	\$9.156	ТСР			/4 3	4210	> h	ttps	[SYN]	Seq=0	Win=1	4600	
	8 5.266/0	0000 192.1	.68.100.1	125 1	165.254.29	9.195	ТСР			74 4	6608	> n	ττρ [	SYNJ S	eq=0	W1n=14	600	Lei
	9 5.2839	0200165.2	54.29.19	95 1	192.168.10	0.125	ТСР			/4 n	ttp	> 46	608 L	SYN, A	CK] S	eq=0 A	CK=1	W
	10 5.2855	3100 192.1	.68.100.1	125 1	165.254.29	9.195	ТСР			66.4	6608	> n	ττρ [/	ACK] S	eq=1	ACK=1	win=	14
	12 5.2808	5800 192.1	.08.100.1	120 1	103.234.2	9.195	HITP			1081 G	EI /	pz:c.	COS [		82024	oris_ap	_an=	FFI I
	12 5.30384	1000 165.2	54.29.1	90 J	192.108.10	0.125				275 0	iccp ittp:/	> 40	200 0	ACKJ 5 V (CT	req=1	ACK=10	10 W	
	14 5 2066	100 103.2	69 100 1	105 1	165 254 20	10.125	тср			57 J H	6609	1.1. . bi	200 0		F09d)	16 Ack	-210	14
	15 5 2172	400 192.1	68 100.1	125 1	165 254 20	105	тср			66.4	6608	> 11 > hr	ttp [/	ACKJ 3 ETN A	CV] C	10 ACK	6 40	w k
_	16 5 2210	000 184 1	60 180 1	156 1	107 168 10	0 125	тср		_	74 h	ttns	~ 2	4210	ELN, A	ACK] 5	Eq=101	Ack-	1
	17 5 3226	100 192 1	68 100 1	25 1	184 169 18	156	TCP			66.3	4210	> h	ttns	[ACK]	Sed=1	Ack=1	Win	=1
	18 5 3247	8000 192 1	68 100 1	25 1	184 169 18	156	TLSV	1		250 C	lien	t He	110	[ACK]	JUG-1	ACK-1		-1.
	19 5, 3332	5800 165.2	54, 29, 10	95 1	192.168.10	0.125	TCP	-		66 h	ttp	> 46	608 F	FTN. A	CK] 5	ea=310	Ack	=1
	20 5.3347	3400 192.1	68,100.1	125 1	165.254.29	.195	ТСР			66 4	6608	> h	ttp [	ACK] S	eq=10	17 Ack	=311	W
	21 5.3801	7000 184.1	69.189.1	156 1	192.168.10	0.125	TCP			66 h	ttps	> 34	4210	[ACK]	Seq=1	Ack=1	85 W	/in:
	22 5.3832	7600 184.1	69.189.1	156 1	192.168.10	0.125	TLSV	1		1514 s	erve	r He	110					
	23 5.3833	0600 184.1	69.189.1	156 1	192.168.10	0.125	ТСР			1514 [	тср	segm	ent o	fare	assem	bled P	DU]	-
•												-					-	F
0 💆	rpcap://[192.1	.68.100.11]:20	02/wec8500	remot F	Packets: 145 · I	Displayed	l: 145 (100.0%	6)	Prof	ile: Defau	lt							





### 2.3.2.2 Stopping the Capture



npi_WEC8 Service npi_WEC8	500/configure/pcap# r is stopped successfu 500/configure/pcap# s	no start-service Hy. show pcap current	-config detai	1				
- Curre - Filte - Opera	nt Status : Idle ring Target : Station tion Mode : Remote	n Packet Capture(re	emote mode)					
- Confi No.	gured AP's MAC List MAC Addr.	Filtering	Matched	Count	Inbound	Rate	Outbound	Rate =======
1	F4:D9:FB:3D:C4:84 ID Prf.	>ON AP Name		IPV4 Addr	0 	0.0 kbps		0.0 kbps
	1 ap_1		npi_Lab_AP	192.168.10.10	00			
- Conti No.	gured Station's MAC L MAC Addr.	_ist Filtering	Matched	Count	Inbound	Rate	Outbound	Rate
1	1C:99:4C:AB:29:F8 AP WN	>ON SSID		96 IPV4 Addr	59	0.0 kbps		0.0 kbps
	1 1		SamsungNPI 1	92.168.100.12	9			

npi\_WEC8500/configure/pcap# no start-service

Service is stopped successfully.

npi\_WEC8500/configure/pcap# show pcap current-config detail

### 2.3.2.2 Stopping the Capture

\_wEC8500/configure/pcap/config-filter# no ap-mac f4:d9:fb:3d:c4:84 MAC value is deleted successfully. \_wEC8500/configure/pcap/config-filter# no station-mac 1c:99:4c:ab:29:f8 The MAC value is deleted successfully. There is no available MAC filtering value(station and AP), so the service will be stopped. npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail - Current Status : Idle Filtering Target : Station : Remote Packet Capture(remote mode) Operation Mode - Configured AP's MAC List Filtering Matched Count Inbound Rate NO. Outbound (empty) - Configured Station's MAC List Inbound Rate NO. Matched Count Outhound \_\_\_\_\_ \_\_\_\_ \_\_\_\_\_\_\_ (empty)

Samsung

Wireless Enter

npi\_WEC8500/configure/pcap/config-filter# no ap-mac f4:d9:fb:3d:c4:84 npi\_WEC8500/configure/pcap/config-filter# no station-mac 1c:99:4c:ab:29:f8 There is no available MAC filtering value(station and AP), so the service will be stopped.

npi\_WEC8500/configure/pcap/config-filter# show pcap current-config detail



# **Tech Support**

WE-WLAN - Day 2 - Jan. 2015

# 2.4 Tech Support

Samsung Wíreless Enterprise™

#### **APC Reboot History**

SNMP	Tech Support > APC Reboot History
HTTP-HTTPS	
Telnet-SSH	Downloa
Local Management Users	APC Reboot History
Logs	Array
DB backup/restore	[REBOOT SUMMARY]====================================
Reboot	Your APC reboot history may be
Factory Reset	EVENT NAME: SYS_RESTART EVENT DESC: UPC[/usr/log//bin/swm] restart system
File Management	<ul> <li>REBOOT TIME: 14:30:23, Oct 08 2013</li> <li>If so, simply download the file</li> </ul>
Package Upgrade	KERNEL LOG]====== here and send to tech-support
FTP-SFTP	[ 23.630802] console [cdr-1] enabled
Time	<pre>[ 23.635332] Creating 1 MTD partitions on "nor0": [ 23.639950] 0x000000dc00000-0x000000fc0000 : "crash_raw"</pre>
License	[ 23.646146] CDR connector initialized (ID = {8.1}) [ 23.963868] ata1: SATA link up 3.0 Gbps (SStatus 123 SControl 320)
Tech Support	[ 23.970364] ata1.00: ATA-9: SanDisk SSD U100 16GB, 10.56.00, max UDMA/133 [ 23.977179] ata1.00: 31277232 sectors, multi 1: LBA48 NCQ (depth 31/32)
APC Reboot History	[ 23.984104] ata1.00: configured for UDMA/133
APC Coredump	[ 23.988612] scsi 0:0:0:0: Direct-Access ATA SanDisk SSD U100 10.5 PQ: 0 ANSI: 5
AP Crash	[ 23.997209] Su 0:0:0:0: [Sda] 31277232 512-byte logical blocks: (16.0 Gb/14.9 Gb) [ 24.005022] sd 0:0:0:0: [sda] Write Protect is off

# 2.4 Tech Support

Samsung Wíreless Enterprise™

### APC Coredump

HTTP-HTTPS   Telnet-SSH   Local Management Users   Logs   DB backup/restore   Reboot   Reboot   Factory Reset   File Management   File Management   Package Upgrade   Package Upgrade   File Management   License   License   Time   License   Tense   APC Creedumy	SNMP >	Tech Support > APC Coredump
Telnet-SSH   Local Management Users   Logs   DB backup/restore   Reboot   Factory Reset   File Management   Package Upgrade   FTP-SFTP   Time   License   License   Tech Support   APC Credung   APC Credung	HTTP-HTTPS	ABC Coredumn
Local Management Users Logs  DB backup/restore Reboot  Factory Reset File Management  Package Upgrade  FTP-SFTP Time  File Send file to tech support if requested by downloading here APC Reboot History APC Coredump APC Coredump	Telnet-SSH	
Logs   DB backup/restore  Reboot  Factory Reset  File Management  Package Upgrade  FTP-SFTP  Time  License  Tech Support  APC Reboot History  APC Cresh	Local Management Users	
DB backup/restore Reboot Reboot Factory Reset File Management Package Upgrade FTP-SFTP Time Package License Tech Support APC Reboot History APC Coredump AP Crash	Logs >	
Reboot   Factory Reset   File Management   Package Upgrade   Package Upgrade   FTP-SFTP   Time   License   Tech Support   APC Reboot History   APC Coredump   AP Crash	DB backup/restore	
Factory Reset   File Management   Package Upgrade   Package Upgrade   FTP-SFTP   Time   License   License   Tech Support   APC Reboot History   APC Coredump   AP Crash	Reboot >	
File Management   Package Upgrade   FTP-SFTP   Time   License   Tech Support   APC Reboot History   APC Coredump   AP Crash	Factory Reset	
Package Upgrade   FTP-SFTP   Time   License   Tech Support   APC Reboot History   APC Coredump   AP Crash	File Management	
FTP-SFTP   Time   License   Tech Support   APC Reboot History   APC Coredump   AP Crash	Package Upgrade	
Time   License   Tech Support   APC Reboot History   APC Coredump   AP Crash	FTP-SFTP	Send file to tech support if
License Tech Support APC Reboot History APC Coredump AP Crash	Time >	
Tech Support       APC Reboot History       APC Coredump       AP Crash	License	requested by downloading here
APC Reboot History APC Coredump AP Crash	Tech Support 🔹	
APC Coredump	APC Reboot History	
AP Crash	APC Coredump	
	AP Crash	

# 2.4 Tech Support

Samsung Wíreless Enterprise™

#### **AP Crash**

SNMP >	Tech Support > AP Cra	sh								
HTTP-HTTPS	AD Crash		If usin	g a lo	ot of AP's	you car	า			
Telnet-SSH	Current Filter : No	00	use th	e filte	er here to	, o show				bango
Local Management Users	Current Hiter . Wo	ile .	less re	sults	or only o	down Al	P's			Linange
Logs >	(r) : Remote AP								То	tal Entry : 2
DB backup/restore	AP PROFILE NAME	AP NAME	MODEL	VERSION	MAC ADDRESS	IP ADDRESS	MODE	ADMIN STATUS	OPERATIONAL STATUS	MAP LOCATION
Reboot >	<u>ap 1</u>	npi_AP1	WEA302i	1.4.5.R	f4:d9:fb:3d:e1:44	192.168.10.100	General AP	Up	Up	
Factory Reset	<u>ap 2</u>	npi_AP2			f4:d9:fb:3d:c4:84	0.0.0.0	General	Up	Down	
File Management							AP			
Package Upgrade					1					
FTP-SFTP										
Time >	Foot Notes :									
License	1. HTTP/ FTP/ SFTP should	be run, before AF	PC received AP C	Crash file fron	n AP.					
Tech Support 🔹		1								
APC Reboot History	_			_ Н	TTP/FTP/	STFP sh	ould			
APC Coredump				be	e turned	on				
AP Crash										

WE-WLAN - Day 2 - Jan. 2015



#### Lab 18 -

#### **Download the APC Reboot and Coredump Files**

- 1. Go to Administration  $\rightarrow$  Tech Support
- 2. Go to APC Reboot History  $\rightarrow$  Download file
- 3. Go to APC Coredump  $\rightarrow$  Download file



Summary		Interference Devices			Here we c causing in	an view d terferenc	evic e wi	es that m th our AF	iay be Ys
active Alarm		Current Filter : N	lone						Change
NLANs									
Access Points	•								Total Entry :
		AP PROFILE NAME	AP NAME	NO	EVOKE TIME	INTERFERER TYPE	RSSI	MIN FREQUENCY	MAX FREQUENCY
Stations		ap_1	npi_AP1	1	2013-11-21 12:22:29	bluetooth	-60	2434	2434
loques	•	ap_2	Warehouse_Root	1	2013-11-21 12:58:47	zigbee	-55	2417	2417
		ap_3	eddie_home	1	2013-11-21 13:00:26	bluetooth	-80	2453	2453
Interference Devices									
Statistics	•				1				



# 2.6 Rogue AP's and Stations

- 2.6.1 Monitoring Rogue
- 2.6.2 Setup White/Black List

# 2.6.1 Monitoring Rogue



Summary	Wire	less Intrusions > AP						
Active Alarm	Cu	urrent Filter : None			-			Change
WLANs			Here we d	can monitor	Rogue AP's			
Access Points	Þ					Cont	ainment	Remove Export
Stations		MAC ADDRESS	SSID	CHANNEL NUMBER	NUMBER OF CLIENTS	CLASS TYPE	STATUS	Total Entry : 49 DETECTING AP
Wireless Intrusions		f4:d9:fb:6a:01:20	SamsungNPI	161	1	Unmanaged	Alert	f4:d9:fb:3d:e1:44
ΔΡ		f4:d9:fb:6a:01:21	SamsungGuestWifi	161	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
Station		f4:d9:fb:6a:01:22	npiDesks	161	1	Unmanaged	Alert	f4:d9:fb:3d:e1:44
Adhoc		f4:d9:fb:6a:01:2e	SamsungGuestWifi	11	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		f4:d9:fb:6a:01:2f		11	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
Interference Devices		6c:f3:7f:95:f2:30	arrow-employee	11	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
Statistics	•	6c:f3:7f:95:f2:31	arrow-guest	11	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
VotD Calle	、	6c:f3:7f:95:f2:32	STIAP	11	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
VOIP Calls		6c:f3:7f:95:f2:33	STI-Mobile	11	1	Unmanaged	Alert	f4:d9:fb:3d:e1:44
Resource		6c:f3:7f:95:f2:38	arrow-employee	44	1	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:f2:39	arrow-guest	44	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:f2:3a	STIAP	44	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:f2:3b	STI-Mobile	44	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:e0:40		6	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:e0:41	arrow-guest	6	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:e0:42	STIAP	6	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:e0:43	STI-Mobile	6	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:e0:48	arrow-employee	48	1	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:e0:49	arrow-guest	48	0	Unmanaged	Alert	f4:d9:fb:3d:e1:44
		6c:f3:7f:95:e0:4a		48	1	Unmanaged	Alert	f4:d9:fb:3d:e1:44

# 2.6.1 Monitoring Rogue



Samsung Wireless Enterprise

Monitor

Wireless Intrusions > Station

Configuration | Administration

Help

Active Alarm
WLANs
Access Points
Stations
Wireless Intrusions
AP
Station
Station Adhoc
Station Adhoc Interference Devices
Station         Adhoc         Interference Devices         Statistics
Station         Adhoc         Interference Devices         Statistics         VoIP Calls

Curre	ent Filter: None	Horowo	can monitor	Roque statio	nc	Change
				Nogue static		ontainment Expor
						Total Entry :
	MAC ADDRESS	BSSID	SSID	CHANNEL NUMBER	STATUS	DETECTING AP
	b4:b6:76:4b:64:05	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
	58:94:6b:63:f5:08	6c:f3:7f:95:e0:48	arrow-employee	48	Alert	f4:d9:fb:3d:e1:44
	20:10:7a:03:70:0f	6c:f3:7f:95:e0:98	arrow-employee	149	Alert	f4:d9:fb:3d:e1:44
	<u>18:3d:a2:4a:6c:10</u>	f4:d9:fb:3d:c0:e3	SamsungBCS	157	Alert	f4:d9:fb:3d:e1:44
	20:10:7a:56:dd:13	f4:d9:fb:6a:01:20	SamsungNPI	161	Removed	f4:d9:fb:3d:e1:44
	04:54:53:a8:44:1b	6c:f3:7f:95:e0:9b	STI-Mobile	149	Removed	f4:d9:fb:3d:e1:44
	<u>c8:d7:19:34:c7:1b</u>	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
	88:53:2e:8f:a4:21	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
	<u>c8:f7:33:d2:fa:23</u>	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
	18:3d:a2:53:5f:30	f4:d9:fb:6a:01:20	SamsungNPI	161	Removed	f4:d9:fb:3d:e1:44
	78:a3:e4:a6:c3:3f	6c:f3:7f:95:f2:33	STI-Mobile	11	Removed	f4:d9:fb:3d:e1:44
	f4:b7:e2:3f:72:53	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
	08:3e:8e:87:fc:55	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
	64:a3:cb:43:1a:59	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
	40:0e:85:05:c3:5b	00:00:00:00:00:00		0	Removed	f4:d9:fb:3d:e1:44
	d0:22:be:ba:b2:5d	f4:d9:fb:3d:c0:f0	SamsungBCS	11	Alert	f4:d9:fb:3d:e1:44
	00:27:10:ce:1b:6c	f4:d9:fb:3d:c9:e2		161	Alert	f4:d9:fb:3d:e1:44
	68:94:23:11:6f:6f	6c:f3:7f:95:e0:48	arrow-employee	48	Alert	f4:d9:fb:3d:e1:44
	00:24:d2:14:16:82	f4:d9:fb:3d:c9:f1		1	Alert	f4:d9:fb:3d:e1:44
	58:94:6b:f0:23:8c	6c:f3:7f:95:e0:98	arrow-employee	149	Removed	f4:d9:fb:3d:e1:44



Samsung Wireless Enterprise	Monitor Configuration Administration Help
Controller >	Wireless Intrusions > General
Access Points	
AP Groups	Enable the Rogue Service here
Remote AP Groups	General
Security >	SERVICE STATE 1 © Enable O Disable
Wireless Intrusions -	EXPIRATION TIMEOUT <sup>2</sup> 1200
General	
Channel Validation	Foot Notes :
Classification	1. Activate or deactivate WIDS
Policy >	2. It determines the maintainance time for monitored data. If a rogue is detected but the rogue then disappears then the information maintained will expire once the
Station Allow Limit	timeout is reached.
Containment	

### 2.6.2 Setup Black List



		AP Blacklist	Managed AP	Station Blacklist	Managed Statior	Managed OUI	Managed SSID	Managed/Neighbor AP
Controller	×	Wireless Intrusion	s > Classification >	AP Blacklist	1			
Access Points		Current Filter :	None					Change
AP Groups								Add Doloto
Remote AP Groups			the the s	Dissels lists			00 : 00 : 00	Add Delete
Security	•	-	In the	BIACK IIST, I	we nave u	Infriendly De	evices to	Total Entry : 0
			be rep	ported to tr	ne monito	oring screen		
Wireless Intrusions	•				No data			
General								
Channel Validation								
Classification								
Policy	•							
Station Allow Limit								
Containment								

#### Samsung Wíreless Enterpríse™

# 3. Advanced Deployment

- 3.1 <u>Remote AP</u>
- 3.2 Internal Radius Server
- 3.4 <u>Quality of Service</u>
- 3.5 <u>VQM</u>
- 3.6 Root and Repeater AP
- 3.7 <u>SNMP</u>



### 3.1 Remote AP

- 3.1.1 Firewall Ports
- 3.1.2 Public IP added
- 3.1.3 FTP Port
- 3.1.4 Remote AP Group
- 3.1.5 WLAN for Remote AP
- 3.1.6 CAPWAP Tunnel Mode
- 3.1.7 Remote AP "Scenario 1 and 2"



# Please note the following must be configured on your firewall to allow the AP to connect to the CAPWAP IP address

- Port mapping must be setup on the following ports
  - 5246 udp
  - 5247 udp
- Example 192.168.10.10 represents my CAPWAP IP
  - policy 20 in address any any 12.13.14.15 32 protocol udp port any 5246 nat-ip 192.168.10.10
  - policy 21 in address any any 12.13.14.15 32 protocol udp port any 5247 nat-ip 192.168.10.10

ontroller	Controller	- Network > Stat	ic Route	You must l	have a st	atic rout	e setup	
General							coccap	
orts							Ac	ld Delet
iterfaces						•	_	
	Ctatic Dec	ite						
iterface Groups	Static Rol							
nterface Groups etwork		DEST	MASK	NEXT HOP	DISTANCE	GW INTERFACE	GW INTERFACE	STATUS
terface Groups twork MSTP		DEST	MASK	NEXT HOP	DISTANCE	GW INTERFACE INDEX	GW INTERFACE TYPE	STATUS
nterface Groups etwork MSTP Static MAC		DEST	MASK 0.0.0.0	NEXT HOP	DISTANCE 1	GW INTERFACE INDEX 10010	GW INTERFACE TYPE other	<b>STATUS</b> active

# 3.1.2 Public IP added

Samsung Wireless Enterprise™

Samsung Wireless Enterprise	Monitor Configuration	Administration   H	el We need to our AP	to add C	our public IP	address
Controller -	Controller > Redundancy					
General						
Ports						Apply
Interfaces	(1)					
Interface Groups	Fall Back					
Network +	FALCBACK	🔘 Enable 🔘 Disable				
Multicast >	ТҮРЕ	Now OAt Time				
Country	TIME	00 - : 00 - ~ 00	- : 00 -			
APC Lists	INTERVAL (SEC)	120				
Redundancy						
Statistics >						
Access Points	CIIC	k on the hai	me of the A	PC		Add Delete
AP Groups	Backup APC List		2			
Remote AP Groups			_			Total Entry : 1
Security	APC NAME	MAC ADDRESS	IP ADDRESS	PORT	PUBLIC IP ADDRESS	PUBLIC PORT
security ,	npi WEC8500 🗲	f4:d0:fb:40:2c:0e	192.168.10.10	5246	12.204.186.57	5246
Rogues						

WE-WLAN - Day 2 - Jan. 2015



Samsung Wireless Enterprise	Monitor   Configuration	Administration Help	
Controller •	Controller > Redundancy >	Edit	4
General			
Ports			Back Apply
Interfaces	APC NAME	npi_WEC8500	
Interface Groups	MAC ADDRESS	f4:d9:fb:40:2c:0e	
Network >	IP ADDRESS	192.168.10.10	
Multicast >	PORT	5246	
Country	PUBLIC IP ADDRESS	12 . 204 . 186 . 5	
APC Lists	PUBLIC PORT	5246	
Redundancy			Add your public ID addross
Statistics >			Aud your public ip address

# 3.1.3 FTP Port



Samsung Wireless Enterprise Monitor Configuration Administration Help								
SNMP >	FTP-SFTP	You will n	You will need to open this					
The FTP is used for Upgrades port on your firewall to upgrade a remote AP								
Local Management Users	FTP		SFTP					
Logs →	FTP	● Enable	SFTP	● Enable				
DB backup/restore	PORT	21	USER	samsung				
Dahaat A	USER	samsung	PASSWORD 2					
KeDool /	PASSWORD 2		CONFIRM PASSWORD					
Factory Reset	CONFIRM PASSWORD		This will be	changed on				
File Management								
Package Upgrade →	Foot Notes :		Stay tuned					
FTP-SFTP	1. Even if you change account-name of connection	or password, services that are already	established will be maintained. Changed configur	ation can be affected on the next				

# 3.1.4 Remote AP Group

Samsung Wireless Enterprise™

Wireless Enterpris	e	Monitor   Confi	guration   Administratio	n   Help				
					Lets create a Ren add our Remote	note AP Grou AP to this Rer	p and note	
Controller	•	AP Groups			AP Group			
WLANs	÷	Current Filter :	None			2	Change	
Radio	പ						<b>&gt;</b>	
Access Points		(R) Remote AP Group					Add Delete	6
AP Groups			AP GROUP NAME		AP GROUP DESCRIPTION	AP COUNT	WLAN COUNT <sup>1</sup>	
Security	•		<u>default</u>		not_used	0	1	
Wireless Intrusion	Þ		<u>RemoteAP</u> (R)		0	0	1	
			403i testing		403i_testing	1	1	
User QoS			<u>302i testing</u>		302i_testing	2	2	
Mobility Management	•		<u>NPI Default WLANS</u>		Always On SSID	2	3	

#### 3.1.4 Remote AP Group



		3	Enter name of remote group and	
Controller	AP Groups > Add	/	, check on Remote AP Group, Hit Apply,	
WLANs >				
Radio 🔸		<u>k</u>	_	Back Apply
Access Points	GROUP NAME	RemoteAP	Remote AP Group	
AP Groups				
Security >				
Wireless Intrusion				



#### **AP Groups**

Current Filter : (R) Remote AP Group	None       Click on the Remote         Click on the Remote       created for further         also see that the R       tagged with "(R)" set	e AP Group you just configuration. You can emote AP Group is symbol for identification.		Change Add Delete Total Entry : 6
	AP GROUP NAME	AP GROUP DESCRIPTION	AP COUNT	WLAN COUNT <sup>1</sup>
	default K	not_used	0	1
	<u>RemoteAP</u> (R)	0	0	0
	403i testing	403i_testing	1	1
	<u>302i testing</u>	302i_testing	2	2
	NPI Default WLANS	Always On SSID	2	3
	<u>303i testing</u>	303i_testing	1	1

1

# 3.1.4 Remote AP Group

Samsung Wireless Enterprise™

Ξ

 $\overline{\nabla}$ 

G	eneral	APs	WLANs	802.11a/n	802.11b/g/n	Remote AP Group	Advanced
AP Grou	ps > APs						
							Back
AP GROU	JP NAME	Remote/	\P				
Currer	nt Filter	None					Change
	- (4)						
Selected	APs						Total Entry : 0
	AP PROF	ILE NAME	AP NAME		MAC ADDRESS	IP ADDRESS	LOCAL AUTH. LIST STATUS
				No data			
Here y be in t	ou can se his Remo	lect which AP w	vill H				
then h	it the Up	Arrow button.					Change
All APs							Total Entry : 6
	AP PROF	ILE NAME	AP NAME	MAC ADDRESS	IP ADD	RESS AP	GROUP NAME
	ар	1	npi Lab AP	f4:d9:fb:3d:c4:84	0.0.0.0	302i	testing 🔺

	ap_2	npi_302i_AP2	f4:d9:fb:3d:e1:44	0.0.0	302i_testing
$\Box$	ap_3	npi_403i_AP	f4:d9:fb:6a:01:03	0.0.0.0	403i_testing
	ap_4	npi_303i_AP	f4:d9:fb:69:d5:61	192.168.10.117	303i_testing
	ap_7	npi_412i_AP	f4:d9:fb:69:eb:c3	0.0.0	NPI_Default_WLANS

WE-WLAN - Day 2 - Jan. 2015

# 3.1.4 Remote AP Group



General	APs	s WL	ANs	802.11a/n	802.11b/g/n	Remote AP Group	Advanced
AP Groups > Re	emote AP Group	> User Authentica	tion				
User Authentication	ACL Profile						
	-						
							Back Apply
AP GROUP NAME		RemoteAP					
BACKUP RADIUS	SERVER 1 <sup>1</sup>	💌		If using a	a radius serve	er for this rer	note AP
BACKUP RADIUS	SERVER 2 <sup>1</sup>	💌		group	au would col	oct that have	
BACKUP RADIUS	SERVER 3 <sup>1</sup>	💌		group, y	Ju would sel		•
				Set to En	able and hit	apply	
Foot Notes :							
1. At least one Radi	us server should be	configured in 'Security	> AAA > Ra	dius'			
							Send To APs
Current Filter :	None						Change
Remote AP User	List						Total Entry : 0
	ID	NAME		DEPAR	TMENT	E-MAI	L
				No data			
		d fau tha luta wa		Comun			
Local Net User	s are created	a for the intern	al Radius	sserver			
This will be dis	scussed later	on					
Current Filter :	None						Change
Local Net User L	ist						Total Entry : 4
	ID	NAME		DEPAR	TMENT	E-MAI	L
	Eddie	Eddie Weak	еу			eweakley@ar	row.com
	John	John Hann	n			j.hannon@ar	row.com
	akathin	Akshay Kat	1in			akathin@arro	ws3.com

WE-WLAN - Day 2 - Jan. 2015



Wireless Enterprise	MO	onitor		Why remo	Create a W te office?	LAN for	your hom	ie or
Controller	→ W	/LANs >	WLANs					
This is helpfu	ul so	_	ilter : None					Change
that all data not sent back controller	traffi k to t	c is he	) DROFTLE NAME	SSID	INTERFACE GROUP	RADIO AREA	Enable Disable	Add Delete
ogues	F		1 npi_lab	npi_wlan	npi_lab	2.4GHz/5GHz	Enable	WPA + WPA2
LANs	•		2 Wlan 3 quest	Cowboys_Wlan	test_20	2.4GHz/5GHz	Disabled Disabled	WPA + WPA2
WLANs	•	<u>1</u>	0 Eddie_Home	Work_Connection	npi_lab	2.4GHz/5GHz	Enable	WPA + WPA2

# 3.1.6 CAPWAP Tunnel Mode

Samsung Configuration Administration Monitor Help Wireless Enterprise Advanced General Security Controller WLANs > WLANs > General For the CAPWAP Tunnel you have 2 options Apply Back **AP Groups** 10 ID **Remote AP Groups** PROFILE N/ ME Eddie Home Work Connection Security SSID default, eddie home AP GROUP LISTS *Local Bridging* will dump off all Rogues • npi\_lab INTERFACE GROUP station traffic to the local network WLANs All • RADIO AREA<sup>1</sup> WLANs Local Bridging 🝷 CAPWAP TUNNEL MODE 2 Local Bridging Radio SUPPRESS SSID 802.3 Tunnel User QoS AAA UVEKKIDE 🔍 Enable 🛛 🔘 Disable 127 MAX. ALLOWED STATIONS **Mobility Management**  Enable
 O Disable 802.3 Tunnel sends all traffic Enable Disable
 Dis back through the APC

Samsung Wireless Enterprise™

# 3.1.6 CAPWAP Tunnel Mode

Samsung Wíreless Enterprise™

	General 802.	1a/n 802.11b/g/n	Remote AP Advanced							
Controller >	Access Points > Remote AP									
WLANs -	This option will only appear if you have									
WLANs	added the AP to a Remote AP Group.									
Radio >	AP PROFILE NAME	ap_4								
Access Points	AP NAME	npi_303i_AP								
AP Groups	AP GROUP NAME	RemoteAP	Here we can sp	CAPWAP Tunnel and Local Bridging.						
	ACL PROFILE		CAPWAP Tunn							
Security >	SCOPE	All O ACL Profile Only								
Wireless Intrusion										
User QoS	Tunnel Forwarding									
Mobility Management	_		WLAN 💌	Split Tunnel ACL 🖌 Add Delete						
DNS	NO.	VLAN SPLIT TUNNE	LACL	EDIT						
010			No data							
NTP	Local Bridging Forwarding									
DHCP		WLAN 💌	VLAN ID 0 ACL	Pre-Auth. ACL 🔽 Add Delete						
	☐ NO.	VLAN VLAN ID	ACL P	RE-AUTH. ACL EDIT						
			No data							
	If you need to tag the data traffic, you can tag the traffic with a VLAN ID here. You can also add an ACL to this AP									

#### 3.1.7 Remote AP "Scenario 1"

Samsung Wireless Enterprise™

#### You have a remote office with multiple AP's at the remote office



WE-WLAN - Day 2 - Jan. 2015



Samsung

Wireless Enterp

### 3.1.7 Remote AP "Scenario 2"

Samsung Wíreless Enterpríse™

You have a remote employee that uses an AP while out of office from many different location


#### 3.1.7 Remote AP "Scenario 2"



#### Hard Setting the CAPWAP IP Address -Statically assign the CAPWAP IP to an AP

- 1. Connect the Samsung Rollover cable to the console port of the AP
- 2. Login Name = root
- 3. Password = samsung
- 4. Warehouse\_Root# config capwap apcIP 12.204.186.56
- 5. Warehouse\_Root # config save

You must perform a save command after making this change

Quic	ck Connect			×	Ŋ
Pro Po Ba Da Pa Str	otocol: ort: aud rate: ata bits: arity: op bits:	Serial       COM1       115200       8       None       1	Flow Control DTR/DSR RTS/CTS XON/XOFF		
	] Sho <u>w</u> quick co	nnect on startup	Sa <u>v</u> e session	Cancel	



# Samsung recommends that you turn this on for Security in the event that the AP is not behind a corporate firewall

Samsung Wireless Enterprise Monitor Configuration Administration Help							
	General 8	302.11a/n	802.11b/g/n	Remote AP	Advanced		
Controller >	Access Points > Advanced						
Access Points							
AP Groups						Back Apply	
Remote AP Groups	AP PROFILE NAME AP NAME	ap_3 eddie	_home				
Security >	ECHO INTERVAL (SEC) <sup>1</sup>	30	D	<b>FLS</b> allows	datagra	im-based	
Rogues 👻	MAX DISCOVERY INTERVAL (S	SEC) <sup>2</sup> 20	ap	plications	s to com	municate in a way	
WIDS Setting	REPORT INTERVAL (SEC) <sup>3</sup>	120	th	at is desig	ned to p	prevent	
Channel Validation	STATISTICS TIMER (SEC) 4	120	62	eavesdronning tampering or			
Black/White List	RETRANSMIT INTERVAL (100M	15) <sup>5</sup> 5					
Policy •	MAX RETRANSMIT <sup>6</sup>	5	m	essage to	rgery.		
Station Allow Limit	ECHO RETRANSMIT INTERVAL	(SEC) 7 3					
WLANs >	MAX ECHO RETRANSMIT <sup>8</sup>	5					
Radio >	TELNET 9	() Er	able 🔘 Disable 🛛 50	023			
User QoS	ssh <sup>10</sup>	Er	able 🔘 Disable 🏾 50	022			
Mobility Management	DTLS <sup>11</sup>	Ena	ble 💌				
DNS	LED	Off	▼ 00 ▼ : 00	· · · 00 · : 00 ·			
	EDGE AP	) Er	iable 🔘 Disable				



# Lab 19 – (1/3)

### Setup an Remote AP

- 1. Go to Configuration  $\rightarrow$  Controller  $\rightarrow$  Redundancy
  - Click on the name of your APC
  - Update the public IP address =  $12.204.186.56 \rightarrow$  Hit Apply
- 2. Go to Configuration  $\rightarrow$  Controller  $\rightarrow$  Network  $\rightarrow$  Static Route
  - Verify that a Static route has been added
- 3. Go to Configuration  $\rightarrow$  AP Groups
  - Create a Remote Group called "home\_group"
  - Click on name of Group
  - Add one of your AP's to this group  $\rightarrow$  Hit Apply
- 4. Go to Configuration  $\rightarrow$  Access Points  $\rightarrow$  Click on the AP you placed in the Remote Group
  - Click on the Advanced Tab  $\rightarrow$  Set Telnet to Enable and hit Apply



#### Lab 19 – (2/3)

#### Setup an Remote AP

- 1. Next, Telnet to the Access Point you wish to make a Remote AP
  - Telnet to the APC First 192.168.xx.10
  - Enter login and password
  - WEC8500#show ap summary

WEC8500# show	WEC8500# show ap summary								
AP Mgmt inte	face IP : 192.168.10.10	(vlan1.10)		_					
AP_ID Prof	ile AP_NAME	MAC_Address	IPv4Addr	State	Speed	Duplex	Location	Country(Model Type)	
1 2 3 4 5 WEC8500#	ap_1 npi_Lab_A ap_2 Eddie_Hom ap_3 AP_303 ap_4 Student4_AP ap_5 Student4_AP	f4:d9:fb:3d:c4:84 f4:d9:fb:3d:e1:44 f4:d9:fb:36:ca:af f4:d9:fb:3d:a5:96 f4:d9:fb:3d:94:96	192.168.10.100 192.168.0.114 192.168.10.102 192.168.10.105 192.168.10.104	1/1/5 1/1/5 1/1/5 1/1/5 1/1/5	100 100 100 100 100	Full Full Full Full Full	npi_lab Carrollton EddieDeskTop Anywhere Root	US (Unknown) US (Unknown) US (Unknown) US (Unknown) US (Unknown)	

#### 2. Telnet to the AP you added to the remote AP Group

- Example = WEC8500#telnet 192.168.10.100 50023
- Login = root
- Password = samsung

#### Remote AP "Lab 19"



#### Lab 19 – (3/3)

#### Setup an Remote AP

#### Statically set your CAPWAP IP



- 1. Configure a static capwap IP
  - Student4\_AP5# config capwap apcIP 192.168.xx.10
  - Student4\_AP5# config Connection closed by foreign host.
- 2. Next, unplug the AP and plug in the remote Network
  - In classroom, plug your AP into neighbors port 1-16
- 3. Go to Configuration  $\rightarrow$  Access Points  $\rightarrow$  See that your AP has registered.
- 4. Lastly, default the AP and set back to normal
  - First, unplug from the AP from the remote network and plug back into your local network. (port 17-24)
  - You must connect via console to Default an AP
  - Go to Configuration → Access Points → Click on the AP you placed in the Remote Group
  - Click on the Advanced Tab → Set Console to Enable and hit Apply
- 5. Connect to the AP via Console Cable
  - Login = root
  - Password = samsung
  - Student4\_AP1# system factory reset ip aft
  - Factory Set ..
  - · System was reset without network informations
- 6. After the AP comes back to the login screen,



3.2 Internal Radius Server

- 3.2.1 Local Net Users
- 3.2.2 Creating a LN Users
- 3.2.3 Assigning to a WLAN
- 3.2.4 Windows Settings



#### Internal RADIUS Server

The Samsung wireless LAN system provides the security and authentication function by interoperating with an internal RADIUS server.

The internal RADIUS server is supported on the WEC8050 and the WEC8500.

To use the internal RADIUS server, operator can add, delete, or edit a user (maximum 512 users).

### 3.2 Internal Radius Server

Samsung Wíreless Enterprise™

Samsung Wireless Enterprise	Monitor Configuration	Administratio	on Help		
			As you can see	e the internal radius	
			server is alread	dy setup.	
Controller >	Security > AAA > RADIUS			/	
Access Points					
AP Groups					Add Delete
Demote AD Course	(*): Internal Radius Server				Total Entry : 1
Remote AP Groups		INDEX	ТҮРЕ	IP ADDRESS	PORT
Security -		0 (*)	Auth	127.0.0.1	1812
AAA 👻					
RADIUS			1		
TACACS+					
Local Net Users	East Nation				
Management User	Foot Notes :	E	MAN - Constitute Dedical		
Captive Portal	1. Can't be deleted if the server con	riguration is used in "V	vLANS > Security > Radius'.		

WE-WLAN - Day 2 - Jan. 2015

### 3.2.1 Local Net Users

Samsung Wireless Enterprise™

Samsung Wireless Enterprise	1	Monitor	Configur	ation   Administ	ration Help
Controller	•	Security	> AAA > Lo	ocal Net Users	
Acce Here is whe	ere	you v	vill cre	ate	Change
<sup>AP G</sup> your Local	Net	User	S		Add Delete Import Local Net User List Export Local Net User List
Remote AP Groups					Total Entry: 3
Security	•		NO.	USER ID	E-MAIL
AAA	•		1	Eddie	eweakley@arrow.com
RADIUS			2	<u>John</u>	j.hannon@arrow.com
Local Net Users			3	<u>Mai</u>	mai@arrows3.com
Captive Portal	•				You can also Import or Export
MAC Filter					
Access Control Lists	•				a Local Net User List
Firewall	•				
NAT	•	Foot Note	IS :		I
Role Based Access Control		Use "Impo	rt" command w	ith caution. It replaces th	he existing users with user entries from the imported file.

#### 3.2.2 Creating a LN Users

Samsung Wíreless Enterprise™

Samsung Wireless Enterpris	se	Monitor   Configurati	ion   Administration	Help
Controller	×	Security > AAA > Loca	l Net Users	
Access Points		Current Filter : Non	e	Change
AP Groups				
Remote AP Groups				Add Delete Import Local Net User List Export Local Net User List
Security	•	NO.	USER ID	Total Entry : 3 E-MAIL
AAA	•		Eddie	eweakley@arrow.com
RADIUS		2	<u>John</u>	j.hannon@arrow.com
Local Net Users		3	Mai	mai@arrows3.com
Captive Portal	÷			
MAC Filter		Let's creat	te a user	1
Access Control Lists	÷			-
Firewall	Þ			
NAT	÷	Foot Notes :		
Role Based Access Contro		Use "Import" command with	caution. It replaces the existin	g users with user entries from the imported file.

#### 3.2.2 Creating a LN Users

Samsung Wireless Enterprise™

Samsung Wireless Enterpris	se <sup>I</sup>	Monitor   Configuration   /	Administration   I	Help Save cr Saving yo	curity edentials pur credentials allows your computer to connect to the n	etwork
				when you	of the rest of the	
Controller	Þ	Security > AAA > Local Net Use	rs > Add		Vser name Password	
Access Points					ОК	Cancel
AP Groups						Back Apply
Remote AP Groups		USER ID	tom			
Security	•	PASSWORD 🕑 1	samsung	$\backslash$		
		CONFIRM PASSWORD	samsung			
	•	FULL NAME	Tom Hanks		When you the i	Jser
RADIUS		DEPARTMENT	Warner		connects they	
Local Net Users			0705551024			
Captive Portal	•		5725551254		need to use this	s info
MAC Filter		CELL PHONE	9725554321			
Access Control Lists	•	HOME PHONE				
Firewall	•	E-MAIL	thanks@arrow.com			
NAT	•					
Role Based Access Control						

#### 3.2.3 Assigning to a WLAN

Samsung Configuration Administration Monitor Help Wireless Enterprise General Security Advanced Controller WLANs > WLANs > Security > L2 ⊩ Access Points L3 Radius **AP Groups** Apply Back Remote AP Groups NPI\_Desk303i **PROFILE NAME** Security L2 SECURITY TYPE <sup>1</sup> WPA + WPA2 ۲ Make sure to change the Rogues WPA WPA POLICY Auth Key MGMT to CCMP V WLANs ENCRYPTION TYPE 802.1x WPA2 POLICY WPA2 CCMP • ENCRYPTION TYPE Radio AUTH KEY MGMT User QoS PSK FORMAT ASCII 🔻 **Mobility Management** PSK KEY 3 ..... DNS 43200 PMK LIFETIME (SECONDS) NTP 0 EAPOL REAUTHENTICATION PERIOD DHCP MAC FILTER 

Samsung Wíreless Enterprise™

#### 3.2.3 Assigning to a WLAN

Samsung Monitor Configuration | Administration Help Wireless Enterprise General Security Advanced Controller Þ WLANs > WLANs > Security > Radius L2 | L3 | Radius Access Points AP Groups Apply Back Remote AP Groups **PROFILE NAME** NPI\_Desk303i Enable Disable Security Þ AUTHENTICATION SERVER Internal 🔹 **RADIUS SERVER 1** ₽ Rogues **RADIUS SERVER 2** WLANs ÷ RADIUS SERVER 3 WLANs Radio Enable
 Oisable ACCOUNTING SERVER User QoS **RADIUS SERVER 1** ٧ 1. Set to Enable **RADIUS SERVER 2** ۲ **Mobility Management** ь 2. Select Internal Radius server **RADIUS SERVER 3** ٧ DNS NTP 0 FALLBACK TEST INTERVAL (SECONDS) DHCP Þ ACCOUNTING INTERVAL (SECONDS) 600

Samsung Wireless Enterprise™





Select "Manually create a network profile"

Enter SSID and select WPA-2 Enterprise/AES Optional: Connect even if the network is not broadcasting



RADIUS Wireless Netw	ork Properties					
Connection Security						
Name:	RADIUS					
SSID:	RADIUS					
Network type:	Access point					
Network availability:	All users					
Connect automa	tically when this network is in range					
Connect to a more	re preferred network if available					
Connect even if	the network is not broadcasting its name (S	SID)				
Enable Intel connection settings						
Configure						

Edit connection settings

RADIUS Wireless Network Properties						
Connection Security						
Security type: Encryption type:	WPA2-Enterprise   AES					
Choose a network authentication method: Microsoft: Protected EAP (PEAP) ▼ Settings Remember my credentials for this connection each time I'm logged on						
	OK Cancel					

Select Security Settings





Uncheck windows logon credentials

#### Samsung Wíreless Enterprise™

	Advanced settings
DIUS Wireless Network Properties	802.1X settings 802.11 settings
Connection Security	Specify authentication mode:
	User authentication
Security type:	
cryption type:	
	Enable single sign on for this network
	Perform immediately before user logon
oose a network authentication method:	Perform immediately after user logon
licrosoft: Protected EAP (PEAP)	Maximum delay (seconds):
Remember my credentials for this connection each	Allow additional dialogs to be displayed during single sign on
time I'm logged on	This network uses separate virtual LANs for machine and user authentication
Advanced settings	
	OK Cano
OK Cancel	
	Select "Specify Auth Mode"
Select Security Advanced Settings	Select User Auth
	Select Save Credentials
	Country of the C
Windows Security	Currently connected to:
	Internet access
Save credentials	Wireless Network Connection
Saving your credentials allows your computer to connect to the network	RADIUS
when you're not logged on (for example, to download updates).	9133
	WE Advice Name: RADIUS call
	WE-Admin Name: RADIUS Signal Strength: Good
	WE-Admin Name: RADIUS Signal Strength: Good Sta Security Type: WPA2 Radio Type: 802.11n
User name	WE-Admin sta Signal Strength: Good Security Type: WPA2 Radio Type: 802.11n WIFI-L1
User name Password	WE-Admin sta WIFI-L1 WE_VOIP_Demo Name: RADIUS Signal Strength: Good Security Type: WPA2 Radio Type: 802.11n SSID: RADIUS SID: RADIUS
User name Password	WE-Admin Name: RADIUS Signal Strength: Good Security Type: WPA2 WIFI-L1 SID: RADIUS WE_VOIP_Demo
User name Password	WE-Admin Name: RADIUS Signal Strength: Good Security Type: WPA2 RADIUS WE_VOIP_Demo CP-TEST BCS-Lab
User name Password OK Cancel	WE-Admin sta Signal Strength: Good Security Type: WPA2 Sadio Type: 802.11n SID: RADIUS WE_VOIP_Demo CP-TEST BCS-Lab GALAXY NOTE3 3905
User name Password OK Cancel	WE-Admin sta Signal Strength: Good Security Type: WPA2 Radio Type: 802.11n SID: RADIUS WE_VOIP_Demo CP-TEST BCS-Lab GALAXY_NOTE3_3905 -

WE-WLAN - Day 2 - Jan. 2015

Connect to Network



# Quality of Service (DSCP)

#### 3.4 Quality of Service



Samsung Wireless Enterprise	Monitor   Configuration	Administration   Help		
	Wired Wirele	255		
Controller >	Radio > 802.11a/n/ac > QoS	> Wired		
Access Points				
AP Groups				Apply
Remote AP Groups	STATION EDCA PROFILE	WMM Default		
Security >	Tagging Policy			
Wireless Intrusions	802.1P POLICY	None		
WLANs >	OUTER DSCP	Enable C Disable  Inner Packet		
Radio 👻	INNER DSCP	Default Value 💌		
802.11a/n/ac 🗸	PROTOCOL <sup>1</sup>	DSCP -		
General				
QoS	QoS Default Values			
802.11h	ACCESS CATEGROY	PROTOCOL	VALUE	
802.11n/ac		802.1p	6	
RRM	VOICE	DSCP	46	
Admission Control		802.1p	4	
802.11b/g/n 👻	VIDEO	DSCP	26	
General		802.1p	0	
QoS	BEST EFFORT	DSCP	0	
802.11n		802.1p	1	
RRM	BACKGROUND	DSCP	8	
Admission Control				
Advanced	L			



## 3.5 VQM

- 3.5.1 Voice Quality Monitoring
- 3.5.2 Features of VQM
- 3.5.3 Configuration for VQM
- 3.5.4 Monitoring Voice Traffic



The WEC8500 provides the Voice Quality Monitoring (VQM) function as an additional service.

As a function that monitors a voice packet in real-time, the VQM checks and manages the voice quality of a voice call being service by using the current wireless LAN section and also provides the status information by monitoring the quality of a voice traffic.



#### Features

- Voice Call Signal Tracing and Troubleshooting
- Voice Quality Check
- Statistics related to Voice traffic

### 3.5.3 Configuration for VQM

Samsung Wíreless Enterprise™

SNMP >	License					
HTTP-HTTPS	Service Status and Current Lim	ite	1	Liconco Podundancy Status		
Telnet-SSH	Service Status and Current Lin	115		License Redundancy Status		
Tellite borr	NUMBER OF AP	25		LICENSE TYPE	Unknown	
Local Management Users	VQM	Enable		PEER MAC ADDRESS	N/A	
Loas	FIREWALL	Enable		PEER LICENSE STATUS	N/A	
3-				PEER LICENSE INSTALLATION FAIL	N/A	
DB Backup/Restore			romindor VON	I must be allowed	via liconco	
Reboot >		AS a	in order to use t	this feature		
Factory Reset	License Key Status <sup>1</sup>					
File Management	OFFICIAL KEY	Valid				
The Hundgement	TEMPORARY KEY	Not valid				
Package Upgrade						
FTP-SFTP	SLM License Key Status					
	SLM LICENSE KEY 1	None				
Time	SLM LICENSE KEY 2	None				
License						
Tech Support >	NEW ACTIVATION KEY FILE				Browse Ac	tivation

## 3.5.3 Configuration for VQM

Samsung Wireless Enterprise™

Samsung Wireless Enterprise	2	Monitor   Configuration	Administration   Help		
Controller	Þ	Controller > General			
Access Points					
AP Groups			Apply		Apply
Remote AP Groups	~			SIP ALG	
Security	GO	to Controller > Ge	neral and make	SIP ALG (VOIP AWARE)	€ Enable C Disable
Wireless Intrusions	sur	re SIP ALG is enable	ed.	SIP EKKUK RESPUNSE	e Enable C Disable
WIFEIESS INCLUSIONS				SIP DETECT LONG DURATION CALL	Enable C Disable
WLANs	+		Apple	SIP NO ANSWER TIMEOUT (SEC)	600
Padio			Арріу	SIP CONNECT TIMEOUT (SEC)	7200
Kaulo	r	AP Registration		SIP MONITORING PORT 1	5060
User QoS				SIP MONITORING PORT 2	0
Mobility Management	•	AUTO	Enable C Disable	SIP MONITORING PORT 3	0
inobility indiagenetic				SIP MONITORING PORT 4	0
DNS			Apply	SIP MONITORING PORT 5	0
NTP	Þ				
DHCP	Þ	Repeater Service			Apply
		SERVICE	C Enable		
				Voice Monitoring	
			Apply	VOICE QUALITY MONITORING	⊙ Enable O Disable
				VOICE ENHANCED MONITORING	Enable C Disable

### 3.5.3 Configuration for VQM

Samsung Wireless Enterprise™

	-				
Controller	•	Radio > 802.11b/g/n > Admis	sion Control		
WLANs	•				
Radio	•				Apply
802.11a/n/ac	•	Voice Call Admission Control <sup>1</sup>		Video Call Admission Control <sup>1</sup>	
General		ADMISSION CONTROL 2	O Enable O Disable	ADMISSION CONTROL	O Enable O Disable
QoS		ADMISSION CONTROL		NETHOD	C chatter C channel Utilization
802.11h		MAX CALLS 3	24	METHOD	Static Channel Utilization
000.11-/		HANDOVER CALLS	2	MAX CALLS	6
802.11N/ac	_			HANDOVER CALLS	0
RRM			to Radio > $802.11a/r$	N(%)	10
Admission Control		MAJOR ALARM THRESHOLD	10 1100 / 002.110/1		
802.11b/g/n	•	802	2.11b/g/n > Admissic	on Control	0
General		and	d enable Voice and V	ideo Call	
QoS		0 -1			
802.11n	E	AC Multicast Stream Admissi	mission Control.	lo <mark>r</mark> ol	
RRM				STATION KICKOUT CONTROL	O Enable O Disable
Admission Control		ADMISSION CONTROL	O Enable (	ASSOC BETRY COUNT TURESHOLD	
Advanced		METHOD	Static Channel Utilization	ASSUC RETRY COUNT THRESHOLD	0
Auvanceu	<u> </u>	MAX STREAMS	20		
Preferred Calls		HANDOVER STREAMS	0		
Sub Channel Groups		MAY CHANNEL LITTLIZATION (%)	75		
Sleeping Cell Detection			10		
Energy Saving	•	(%)	0		



## 3.5.4 Monitoring Voice Traffic

- 3.5.4.1 VoIP Calls
- 3.5.4.2 Statistics

#### 3.5.4.1 VoIP Calls



MAC ADDRESS       USER NAME       IP ADDRESS       TEL       CALL       SOLUTION       CALL       REG.         gues       •		
Current Filter:       None       Current Filter:       None         LANS       Current Filter:       None       Non		
MANS       VOIP Stations       Nate       Nate </th <th>ge</th> <th></th>	ge	
Attons       MAC ADDRESS       USER NAME       IP ADDRESS       TEL       CALL       CALL       REC.       CALL SERVER       SSID       RADI         terference Devices       40/07/12/11/61/70       10.65.178.150       4477       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         00/16/57/21/161/70       10.65.181.101       32.17       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         00/16/57/21/183/f9       10.65.181.101       32.17       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         00/16/57/21/183/f9       10.65.181.102       2854       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         00/16/57/21/16/74       10.65.179.134       4257       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         00/16/57/21/16/74       10.65.179.134       4257       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         00/16/57/21/16/74       10.65.179.134       4257       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         00/16/57/21/16/78/15       bw		
Autom         Number         CALL         CALL         REG. STATUS         CALL SERVER         SSID         RAC           ogues         • </th <th>bort</th> <th></th>	bort	
AttonsguesMAC ADDRESSUSER NAMEIP ADDRESSTELCALLCALLREG.CALL SERVERSSIDRADIbc:72:b1:d1:fe:7bleehr10.65.178.1504717UDPIdleRegistered123.34.1.20ureadymobile5Gatisticsd0:dfi:r7:be:1b:33laplace.lee10.65.186.1333188UDPIdleRegistered10.25.1193.177smart25G00:16:b7:21:b1:r310.65.186.1133188UDPIdleRegistered10.25.1193.177smart25G00:16:b7:21:b1:r3jihyeya.choi10.65.148.1130448UDPIdleRegistered123.34.1.20ureadymobile5Gfo:6b:ca:44:5b:33jihyeya.choi10.65.148.1310448UDPIdleRegistered123.34.1.20ureadymobile5Gfo:6b:ca:44:5b:33jihyeya.choi10.65.148.1310448UDPIdleRegistered123.34.1.20ureadymobile5Gfo:6b:ca:44:5b:33jihyeya.choi10.65.148.1310448UDPIdleRegistered123.34.1.20ureadymobile5Gcompleted Calls38:0a:94:ee:a6:30leeyb10.65.158.1344257UDPIdleRegistered123.34.1.20ureadymobile5Gfo:6b:ca:42:65:55kunmin.ahn10.65.151.1144171UDPIdleRegistered123.34.1.20ureadymobile5Gfo:6b:ca:42:65:56kunmin.ahn10.65.131.1744431UDPIdleRegistered123.34.1.20uread	try : 96	
ogges         NUMBER         PROTOCOL         STATUS         STATUS         CALL SERVER         SSLD         RADI           terference Devices         bc:72:b1:d1:f6:7b         leehr         10.65.178.150         4717         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           atistics         00:16:b7:21:b1:7a         10.65.181.119         3217         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           01P Calls         00:16:b7:21:b1:7a         10.65.181.119         3217         UDP         Ide         Registered         10.251.193.177         smart.2         5G           01P Calls         00:16:b7:21:a3:19         10.65.145.213         0348         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           01P Stations         00:16:b7:21:a3:19         10.65.181.192         2854         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           Completed Calls         00:16:b7:21:b6:ca:42:86:50         voongkonlee         10.65.179.13         4870         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           Completed Calls         00:1	AP	00010
bc:72:b1:d1:f6:7b         leehr         10.65.172.150         4717         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           tatistics         d0:df:7:be:1b:33         laplace.lee         10.65.181.119         3217         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           oiP Calls         00:16:b7:21:b7:7a         10.65.181.119         3217         UDP         Ide         Registered         10.3.34.1.20         ureadymobile         5G           oiP Calls         00:16:b7:21:b7:7a         10.65.181.119         3217         UDP         Ide         Registered         10.3.34.1.20         ureadymobile         5G           oiP Calls         00:16:b7:21:b3:7         10.65.181.119         218         UDP         Ide         Registered         10.3.34.1.20         ureadymobile         5G           volP Stations         00:16:b7:21:b3:3         jihyeya.cho         10.65.181.192         2854         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G           do:df:r2:1b1:d5:f81:d         yoongkwan.cho         10.65.179.89         3991         UDP         Ide         Registered         123.34.1.20         ureadymobile         5G	NAME	BSSID
terrerence Devicesdi0:df:c7:be:1b:33laplace.lee10.65.181.1193217UDPIdleRegistered123.34.1.20ureadymobile5Gatistics0116:b7:21:bf:7a10.65.186.1333188UDPIdleRegistered10.251.193.177smart25G0117 Calls01:61:b7:21:a3:f910.65.191.1175186UDPIdleRegistered10.251.193.177smart25G0117 Calls01:61:b7:21:a3:f910.65.185.1310348UDPIdleRegistered123.34.1.20ureadymobile5G0116 Calls01:01:61:7:21:b1:7a0.65.181.1922854UDPIdleRegistered123.34.1.20ureadymobile5G0117 Calls01:01:61:7:11:f1:84:b1youngkona.cho10.65.181.1922854UDPIdleRegistered123.34.1.20ureadymobile5G0116 Calls01:01:61:7:11:61:84:b1youngkona.cho10.65.179.893991UDPIdleRegistered123.34.1.20ureadymobile24G01:16:b7:21:b1:c710.65.159.1344257UDPIdleRegistered123.34.1.20ureadymobile5G38:0ar:94:ee:a6:30leeyb10.65.151.1144171UDPIdleRegistered123.34.1.20ureadymobile5G39:15:b1:6a:08:b9hs67.kim10.65.135.122824UDPIdleRegistered123.34.1.20ureadymobile5G99:55:b1:6a:08:b9hs67.kim10.65.135.122824UDPIdleRegistered123.34.1.2	AP-9F18	f4:d9:fb:35:b6
atistics       00:16:b7:21:bf:7a       10.65.186.133       3188       UDP       Ide       Registered       10.251.193.177       smart2       5G         IP Calls       00:16:b7:21:a3:f9       10.65.191.117       5186       UDP       Ide       Registered       10.251.193.177       smart2       5G         foi:6b:ca:48:5b:33       jihyeya.choi       10.65.145.213       0348       UDP       Ide       Registered       12.3.34.1.20       ureadymobile       5G         couve Caus       b0:d0:9c:81:f4:d8       yoongkwan.cho       10.65.180.94       4870       UDP       Ide       Registered       12.3.34.1.20       ureadymobile       5G         source       38:0a:94:ee:a6:30       leeyb       10.65.179.89       3991       UDP       Ide       Registered       12.3.34.1.20       ureadymobile       2.4G         source       38:0a:94:ee:a6:30       leeyb       10.65.179.89       3991       UDP       Ide       Registered       12.3.34.1.20       ureadymobile       5G         source       78:f7:be:7b:dc:a5       oktae78.kim       10.65.179.18       3519       UDP       Ide       Registered       12.3.34.1.20       ureadymobile       5G         source       60:6b:ca:42:86:5b       kunmi.ahn       10.65	AP-9F21	f4:d9:fb:35:e7
IP Calls         00:16:b7:21:a3:f9         10.65.191.117         5186         UDP         Ide         Registered         10.251.193.177         smart2         5G           oIP Stations         00:00:00:00:00:00:00:00:00:00:00:00:00:	AP-9F27	f4:d9:fb:35:c8
f0:bb:ca:48:5b:33       jihyeya.choi       10.65.145.213       0348       UDP       Ide       Registered       123.34.1.20       ureadymobile       5G         /oIP Stations       b0:d0:9c:81:f4:d8       youngkonlee       10.65.181.192       2854       UDP       Ide       Registered       123.34.1.20       ureadymobile       5G         cuve cairs       94:d7:71:ef:84:b1       youngkonlee       10.65.179.89       3991       UDP       Idle       Registered       123.34.1.20       ureadymobile       24.63         source       38:0a:94:ee:a6:30       leeyb       10.65.179.89       3991       UDP       Idle       Registered       123.34.1.20       ureadymobile       24.63         source       00:16:b7:21:bd:c7       10.65.179.18       3519       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         f0:6b:ca:42:8e:5b       kunmin.ahn       10.65.179.18       3519       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         f0:6b:ca:42:8e:5b       kunmin.ahn       10.65.179.18       3519       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         f0:6b:ca:42:8e:5b       kunmin.ahn       10.65.131.174       4	AP-9F29	f4:d9:fb:35:53
NoIP Stations         b0:d0:9c:81:f4:d8         yoongkwan.cho         10.65.181.192         2854         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           completed Calls         94:d7:71:ef:84:b1         youngkonlee         10.65.180.94         4870         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           source         38:0a:94:ee:a6:30         leeyb         10.65.179.89         3991         UDP         Idle         Registered         10.251.193.177         smart2         5G           source         00:16:b7:21:bd:c7         10.65.159.134         4257         UDP         Idle         Registered         10.251.193.177         smart2         5G           78:f7:be:7b:dc:a5         oktae78.kim         10.65.151.114         4171         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           bc:72:b1:d5:f8:c5         bw.bae         10.65.131.174         4431         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           98:52:b1:6a:08:b9         hs67.kim         10.65.136.19         5912         UDP         Idle         Registered         123.34.1.20         ureadymobile <t< td=""><td>AP-9F13</td><td>f4:d9:fb:35:c7</td></t<>	AP-9F13	f4:d9:fb:35:c7
Marke Cans         94:d7:71:ef:84:b1         youngkonlee         10.65.180.94         4870         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           source         38:0a:94:ee:a6:30         leeyb         10.65.179.89         3991         UDP         Idle         Registered         123.34.1.20         ureadymobile         2.4G           source         00:16:b7:21:bd:c7         10.65.159.134         4257         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           f0:6b:ca:42:8e:5b         kunmin.ahn         10.65.151.114         4171         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           bc:72:b1:d5:f8:c5         bw.bae         10.65.131.174         4431         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           98:52:b1:6a:08:b9         hs67.kim         10.65.135.122         8224         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           98:52:b1:6a:08:b9         hs67.kim         10.65.135.122         8224         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G	AP-9F27	f4:d9:fb:35:c8
Completed Calls38:0a:94:ee:a6:30leeyb10.65.179.893991UDPIdleRegistered123.34.1.20ureadymobile2.4GsourceSource00:16:b7:21:bd:c710.65.159.1344257UDPIdleRegistered10.251.193.177smart25G78:f7:be:7b:dc:a50ktae78.kim10.65.179.183519UDPIdleRegistered123.34.1.20ureadymobile5G60:6b:ca:42:8e:5bkunmin.ahn10.65.151.1144171UDPIdleRegistered123.34.1.20ureadymobile5G98:52:b1:6a:08:b9hs67.kim10.65.135.1228224UDPIdleRegistered123.34.1.20ureadymobile5G94:63:d1:00:75:a6bko.park10.65.135.1228224UDPIdleRegistered123.34.1.20ureadymobile5G94:63:d1:00:75:a6bko.park10.65.186.1683107UDPIdleRegistered123.34.1.20ureadymobile5G94:63:d1:00:75:a6bko.park10.65.186.1683107UDPIdleRegistered123.34.1.20ureadymobile5G94:63:d1:00:75:a6bko.park10.65.186.1683107UDPIdleRegistered123.34.1.20ureadymobile5G94:63:d1:00:75:a6bko.park10.65.186.1683107UDPIdleRegistered123.34.1.20ureadymobile5G94:63:d1:00:75:a6bko.park10.65.186.1683107UDPIdleRegistered123.34.1.20urea	AP-9F12	f4:d9:fb:35:8d
Descurce         00:16:b7:21:bd:c7         10.65.159.134         4257         UDP         Idle         Registered         10.251.193.177         smart2         5G           78:77:be:7b:dc:a5         oktae78.kim         10.65.179.18         3519         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           f0:6b:ca:42:8e:5b         kunmin.ahn         10.65.179.18         3519         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           bc:72:b1:d5:f8:c5         bw.bae         10.65.131.174         4431         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           98:52:b1:6a:08:b9         hs67.kim         10.65.135.122         8224         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           94:63:d1:00:75:a6         bkon.park         10.65.135.122         8224         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           94:63:d1:00:75:a6         bkon.park         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           b4:62:93:56:72:bd         goodsen	AP-9F07	f4:d9:fb:35:b0
78:f7:be:7b:dc:a5         oktae78.kim         10.65.179.18         3519         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           f0:6b:ca:42:8e:5b         kunmin.ahn         10.65.151.114         4171         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           bc:72:b1:d5:f8:c5         bw.bae         10.65.151.114         4171         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           98:52:b1:6a:08:b9         hs67.kim         10.65.135.174         4431         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           94:63:d1:00:75:a6         bkon.park         10.65.135.122         8224         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           04:63:d1:00:75:a6         bkon.park         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           cc:f9:e8:0c:78:13         jaeseung.hwang         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           b4:62:93:56:72:bd         <	AP-9F29	f4:d9:fb:35:53
f0:6b:ca:42:8e:5b       kunmin.ahn       10.65.151.114       4171       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         bc:72:b1:d5:f8:c5       bw.bae       10.65.131.174       4431       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         98:52:b1:6a:08:b9       hs67.kim       10.65.186.59       5912       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         94:63:d1:00:75:a6       bkon.park       10.65.185.122       8224       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         cc:f9:e8:0c:78:13       jaeseung.hwang       10.65.186.168       3107       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         b4:62:93:56:72:bd       goodsense       10.65.180.48       4843       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         b4:62:93:56:72:bd       goodsense       10.65.180.48       4843       UDP       Idle       Registered       123.34.1.20       ureadymobile       5G         b6:cf3:73:3c:66:d6       huhmoo       10.65.127.142       2774       UDP       Idle       Registered <t< td=""><td>AP-9F05</td><td>f4:d9:fb:35:a6</td></t<>	AP-9F05	f4:d9:fb:35:a6
bc:72:b1:d5:f8:c5         bw.bae         10.65.131.174         4431         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           98:52:b1:6a:08:b9         hs67.kim         10.65.186.59         5912         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           94:63:d1:00:75:a6         bkon.park         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           cc:f9:e8:0c:78:13         jaeseung.hwang         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           b4:62:93:56:72:bd         goodsense         10.65.180.48         4843         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           6c:f3:73:3c:66:d5         huhmoo         10.65.127.142         2774         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G	AP-9F31	f4:d9:fb:35:92
98:52:b1:6a:08:b9         hs67.kim         10.65.186.59         5912         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           94:63:d1:00:75:a6         bkon.park         10.65.135.122         8224         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           cc:f9:e8:0c:78:13         jaeseung.hwang         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           b4:62:93:56:72:bd         goodsense         10.65.180.48         4843         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           6c:f3:73:3c:66:d5         huhmoo         10.65.127.142         2774         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G	AP-9F27	f4:d9:fb:35:c8
94:63:d1:00:75:a6         bkon.park         10.65.135.122         8224         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           cc:f9:e8:0c:78:13         jaeseung.hwang         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           b4:62:93:56:72:bd         goodsense         10.65.180.48         4843         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           cc:f3:73:3c:66:d6         huhmoo         10.65.127.142         2774         UDP         Idle         Registered         123.34.1.20         ureadymobile         2.4G	AP-9F06	f4:d9:fb:35:c8
cc:f9:e8:0c:78:13         jaeseung.hwang         10.65.186.168         3107         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           b4:62:93:56:72:bd         goodsense         10.65.180.48         4843         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           6c:f3:73:3c:66:d6         huhmoo         10.65.127.142         2774         UDP         Idle         Registered         123.34.1.20         ureadymobile         2.4G	AP-9F25	f4:d9:fb:35:a7
b4:62:93:56:72:bd         goodsense         10.65.180.48         4843         UDP         Idle         Registered         123.34.1.20         ureadymobile         5G           6c:f3:73:3c:66:d6         huhmoo         10.65.127.142         2774         UDP         Idle         Registered         123.34.1.20         ureadymobile         2.4G	AP-9F26	f4:d9:fb:35:3e
6c:f3:73:3c:66:d6 huhmoo 10.65.127.142 2774 UDP Idle Registered 123.34.1.20 ureadymobile 2.4G	AP-9F07	f4:d9:fb:35:b0
	AP-9F28	f4:d9:fb:35:8f:
88:9b:39:f8:6e:61 jh0508.lee 10.65.138.135 0604 UDP Idle Registered 123.34.1.20 ureadymobile 2.4G	AP-9F03	f4:d9:fb:35:8d
78:59:5e:45:5e:3f yklee1 10.65.132.35 3921 UDP Established Registered 123.34.1.20 ureadymobile 2.4G	AP-9F01	f4:d9:fb:35:56

#### 3.5.4.1 VoIP Calls



Samsung	Monitor Configur	ation	Administratio	n   Heln						
wireless Enterprise			Administration	n ncip	,					
Immary	VoIP Calls > Active Ca	alls								
tive Alarm	Current Filter : N	one	_							Change
LANs			A	ctiv	le Ca	lls				
cess Points	Þ									Export
										Total Entry
ations	MAC ADDRESS	USER NAME	IP ADDRESS	CALLER	CALLEE	AP NAME	START TIME	DIRECTION	MOS(UP) <sup>1</sup>	MOS(DOWN) <sup>1</sup>
gues	bc:72:b1:d0:9d:41	elly	10.65.142.204	3968	#01044992879	AP-9F07	19:50:54	Outbound	4.18	4.18
erference Devices	<u>bc:72:b1:d5:f8:c5</u>	bw.bae	10.65.131.174	4431	#01093972798	AP-9F27	19:51:23	Outbound	4.18	4.18
tistics	•	VoIP Calls	> Active Calls >	Detail						
DIP Calls		De	tail Inforn	nation						Bac
VoIP Stations										
Active Calls	Foot Notes :	Client Info	ormation			Call Informa	tion			
	1. MOS is updated in 30 se	eco MAC ADD	RESS	bc:72:b	1:d0:9d:41	CALLER NUM	BER	3968		
completed Calls		IP ADDRE	ESS	10.65.14	42.204	CALLEE NUM	BER	#01044992	879	1710-66
		USER NAM	16	ureadyn	nobile	REST		-60	0401/08030/0898	1/1806
		RADIO		5G	nobile	SNR		39 dB		
		BSSID		f4:d9:fb	:35:b0:42	DATA RATE		72.2 Mbps		
		ESTABLIS	HED AP	AP-9F07	7	START TIME		01-06 19:5	):54	
		CURRENT	AP	AP-9F07	7	DIRECTION		Outbound		
			oc.	Digital C	City/R3/9?	CALLER MED	IA PORT	27072		
						CODEC		G711u		
						UPSTREAM N	105	4.18		
						DOWNSTRE/	AM MOS	4.18		
						UPSTREAM J	ITTER	0 msec		
						DOWNSTRE	M JITTER	0 msec		
						UPSTREAM D	ELAY	54 msec		

DOWNSTREAM DELAY

54 msec

#### 3.5.4.1 VoIP Calls



Samsung Wireless Enterpris	Monitor   Config	juration   A	dministration	Help							
Summary	VoIP Calls > Comp	leted Calls									
Active Alarm											
/LANs	Search Condition										
coss Doints	MAC ADDRESS	00:00:	00:00:00:00	USER	IAME			TEL NUM	BER		
cess points	START TIME		00 💌 : 00 💌	END TI	ME		00 💌 : 0	0 💌			
ations										App	v Cancel
gues	•										
terference Devices			story of	Com	nlata						Export
			SLUTY OF	COM	piete	u Cal	12			_	
ITISTICS	MAC ADDRESS	USER NAME	IP ADDRESS	CALLER	CALLEE	AP NAME	START TIME	EN		MOS(UP)	MOS(DOWN)
P Calls	▼ <u>d0:22:be:ef:92:a7</u>		192.168.100.159	701006	701077	npi_AP1	01-14 03:38:10	01-14	03:38:11	1	4.18
oIP Stations	d0:22:be:ef:92:a7		192.168.100.159	701006	701077	npi_AP1	01-14 03:38:36	01-14	03:39:37	1.07	4.18
ctive Calls	<u>d0:22:be:ef:92:a7</u>		192.168.100.159	701006	701077	npi_AP1	01-14 03:43:42	01-14	03:43:43	1.66	4.18
omploted Calls	d0:22:be:be:e5:d6		192.168.100.167	701173	701073	npi_AP1	01-14 03:49:58	01-14	03:50:38	3.98	4.18
ompleted Calls	<u>38:aa:3c:93:69:e2</u>		192.168.100.121	701106	701010	npi_AP1	01-14 03:58:37	01-14	03:58:37	1	4.18
ource	38:aa:3c:93:69:e2		192.168.100.121	701010	701106	npi_AP1	01-14 03:58:51	01-14	03:59:24	4.09	4.18
	d0:22:be:ef:92:a7		102 100 100 150	701077	701010	: AD1	01-14-04-00-09	01-14	04:00:09	1.5	4.18
	d0:22:be:be:e5:d6	ΝЛ	oon Oni	nion	Scoro		C) A 12	01-14	04:00:51	3.98	4.18
	<u>38:aa:3c:93:69:e2</u>		ean Opi		SCULE		<b>J</b> - A <sub>33</sub>	01-14	04:03:05	3.53	4.18
	d0:22:be:ef:92:a7		Moncur	$\sim Of$	Voico	Oual	<b>11+1</b>	01-14	04:14:06	1.21	0
	<u>d0:22:be:ef:92:a7</u>		weasur	eOI	voice	Qua	11LY 27	01-14	04:15:28	1.09	4.18
	<u>d0:22:be:ef:92:a7</u>		192.168.100.159	701006	701077	npi_AP1	01-14 04:15:35	01-14	04:15:36	1.62	4.18
	<u>d0:22:be:be:e5:d6</u>		192.168.100.167	701173	701073	npi_AP1	01-14 05:03:34	01-14	05:03:37	3.81	4.18
	d0:22:be:ef:92:a7		192.168.100.159	701010	701077	npi_AP1	01-14 05:05:03	01-14	05:05:03	0	0
	<u>d0:22:be:ef</u> :92:a7		192.168.100.159	701010	701077	npi_AP1	01-14 05:05:21	01-14	05:05:46	1.39	4.18
	<u>38:aa:3c:93</u> :69:e2		192.168.100.121	701010	701106	npi_AP1	01-14 05:18:42	01-14	05:18:43	1.3	3.53
	38:aa:3c:93:69:e2		192.168.100.121	701010	701106	npi AP1	01-14 05:18:49	01-14	05:18:53	3.88	4.18
	38:aa:3c:93:69:e2		192.168.100.121	701010	701106	npi AP1	01-14 05:19:10	01-14	05:19:10	1.62	4.18
	20.00.00.00.00.00		192 168 100 121	701010	701106	npi AP1	01-14 05:19:17	01-14	05:19:20	3.77	4.18
	30:88:3C:93:09:62		195110011001151			1 1 per 1 1 1 1 1 1 1 1		100 Mar 100 Mar 1			

#### 3.5.4.2 Statistics



Samsung Wireless Enterpris	e	Monitor   Configuration	Administrati	on   Help		User [	<u>akshay</u> ]   Logou	t   Save Configuration
		Assoc/Ho Data T	raffic	VoIP				
Wireless Intrusion	•	Statistics > Network Quality >	Radios > 802	.11a/n/ac > VoIP	)			
Interference Devices								
Statistics	•			Netwo	ork Quality	(Radios)		Radio Switch
APC Ports		Last updated : Thu Sep 25 13:48:05 20	014					
AP Ports		Call count statistics 1						
AP Join								
RADIUS Servers		Current calls : 0						
Mobility			5 MIN	15 MIN	1 HOUR	12 HOUR	1 DAY	TOTAL
Load Balancing		TOTAL <sup>2</sup>	0	0	0	0	0	0
Network Quality	•	SETUP SUCCESS <sup>3</sup>	0	0	0	0	0	0
General	_	SUCCESS <sup>4</sup>	0	0	0	0	0	0
Alert List	-	FAILURE <sup>5</sup>	0	0	0	0	0	0
System	•	CANCEL	0	0	0	0	0	0
Radios	•	CALLED NUMBER BUSY	0	0	0	0	0	0
802.11a/n/ac		REQUEST TIMEOUT	0	0	0	0	0	0
802.11b/g/n		NOT FOUND	0	0	0	0	0	0
WLANs		FORBIDDEN	0	0	0	0	0	0
APs	•	SIGNAL TIMEOUT	0	0	0	0	0	0
Device Types		ETC	0	0	0	0	0	0
		DROP, RATE	0(-%)	0(-%)	0(-%)	0(-%)	0(-%)	0(-%)

#### 3.5.4.2 Statistics



Samsung Wireless Enterprise		Monitor   Configuration	Administrat	on   Help	)		User [ <u>akshay</u> ]   Log	out   Save Configuration
		Assoc/Ho	oIP					
Wireless Intrusion	*	Statistics > Network Quality	> WLANs > Vo	[P				
Interference Devices								
Statistics -				Ne	etwork Qua	lity (WLAN	<b>S)</b>	Back
APC Ports		Last updated : Thu Sep 25 13:49:54	2014					
AP Ports		PROFILE NAME	npi_network					
AP Join		SSID	SamsungNPI					
RADIUS Servers		collocated at the 1						
Mobility		Call count statistics *						
Load Balancing		Current calls : 0						
Network Quality 🗸 🗸			5 MIN	15 M	IN 1 HOUR	12 HOU	R 1 DAY	TOTAL
General	_	TOTAL <sup>2</sup>	0	0	0	0	0	0
Alert List	-	SETUP SUCCESS <sup>3</sup>	0	0	0	0	0	0
System +		SUCCESS <sup>4</sup>	0	0	0	0	0	0
Radios 🗸		FAILURE 5	0	0	0	0	0	0
802.11a/n/ac		CANCEL	0	0	0	0	0	0
802.11b/g/n		CALLED NUMBER BUSY	0	0	0	0	0	0
WLANs		REQUEST TIMEOUT	0	0	0	0	0	0
APs >		NOT FOUND	0	0	0	0	0	0
Device Types		FORBIDDEN	0	0	0	0	0	0
V-TD C-II-	Ŧ	SIGNAL TIMEOUT	0	0	0	0	0	0

WE-WLAN - Day 2 - Jan. 2015

#### 3.5.4.2 Statistics



Samsung Wireless Enterpr	User [ <u>akshay</u> ]   Logout   Save Configuration   Help											
		Assoc/Ho	Data Rates	Data Traffic	RF	VoIP						
APC Ports	*	Statistics > Network	Quality > APs > (	802.11a/n/ac > Vo	[P							
AP Ports												
AP Join							Dadi	a Cuultab				
RADIUS Servers				Ne	twork Qua	lity (APS)	Kaul	o Switch Back				
Mobility		Last updated : Thu Sep 25	13:50:52 2014									
Load Balancing		PROFILE NAME	ap_9									
Network Quality	•	AP NAME	npi_412	i_AP2								
General												
Alert List		Call count statistics <sup>1</sup>										
System	•	Current calls : 0										
Radios	•		5 M	4IN 15 MIN	1 HOUR	12 HOUR	1 DAY	TOTAL				
802.11a/n/ac		TOTAL <sup>2</sup>	0	0	0	0	0	0				
802.11b/g/n		SETUP SUCCESS <sup>3</sup>	0	0	0	0	0	0				
WLANs	E	SUCCESS 4	0	0	0	0	0	0				
APs	•	FAILURE <sup>5</sup>	0	0	0	0	0	0				
802.11a/n/ac		CANCEL	0	0	0	0	0	0				
802.11b/g/n		CALLED NUMBER BUSY	0	0	0	0	0	0				
Device Types		REQUEST TIMEOUT	0	0	0	0	0	0				
INTP Calls	•	NOT FOUND	0	0	0	0	0	0				
		FORBIDDEN	0	0	0	0	0	0				



- To provide a wireless LAN service where cable installation is difficult, a Samsung AP can be configured as a repeater mode to relay wireless LAN traffics.
- To configure this kind of network, the Repeater AP and Root AP are required.
- The Repeater AP is working as a wireless terminal and the Root AP connects a Repeater AP to a wireless terminal for connection to the WEC8500.
- The Root AP and Repeater AP will use radio 5GHz to connect to one another.
- Due to this, the Root and Repeater will only be able to broadcast its SSID on the 2.4Ghz radio

#### 3.6 Root and Repeater AP

Samsung Wireless Enterprise™



WE-WLAN - Day 2 - Jan. 2015

Samsung Wíreless Enterprise™

Samsung Wireless Enterprise		Monitor	Configuration	Administration	n   Help							
Controller	+	Access	Points		First,	plug in	the	AP's	that you	l are	goin	g to
Access Points	Curre	ent Filter : None	L have	use for Root and the Repeater AP								
AP Groups				n						<b></b>		
Remote AP Groups						Multi Set	Ena	Dis	alle Add	Delete	Export	
Security	•	(e) : Edg	e AP, (r) : Remote AP							To	otal Entry : 4	
Rogues	+		AP PROFILE NAME	AP NAME	MAC	IP ADDRESS	ADMIN STATUS	OPER STATUS	MAP LOCATION	MODE	MODEL	VERSION
WLANs	•		<u>ap 1</u>	npi_AP1	f4:d9:fb:3d:e1:44	192.168.10.50	Up	Up		General AP	WEA302i	1.4.8.R
Radio	÷		<u>ap 2</u>	Warehouse_Root	4:d9:fb:3d:c4:84	192.168.10.52	Up	Up		General AP	WEA302i	1.4.8.R
User QoS			<u>ap 3</u>	eddie_home	f4:d9:fb:3d:e2:c4	192.168.70.28	Up	Down		General AP(r)	WEA302i	1.4.8.R
Mobility Management	Þ		<u>ap 4</u>	Warehouse_Repeat	4:d9:fb:3c:23:2c	192.168.10.55	Up	Up		General AP	WEA302i	1.3.14.R
DNS	_											

#### 3.6 Root and Repeater AP

Samsung Wíreless Enterprise™

The Root and Repeater AP's must be setup in the same AP Group.



 Back

 AP GROUP NAME
 npi\_AP1

 Current Filter : None
 Change

#### Selected APs

AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	AP GROUP NAME
ap_1	npi_AP1	f4:d9:fb:3d:e1:44	192.168.10.50	npi_AP1
ap_2	Warehouse_Root	f4:d9:fb:3d:c4:84	192.168.10.52	npi_AP1
ap_4	Warehouse_Repeat	f4:d9:fb:3c:23:2c	192.168.10.56	npi_AP1


Samsung Wireless Enterprise Monitor Configuration Administration Help												
Controller	•	Access	Points Now,	lets click	on our l	Root Al	Ρ					
Access Points		Curr	ent Filter : None								Change	
AP Groups					(3)	Multi Set	Ena	hle Disa	ble Add	Delete	Export	
Remote AP Groups		(e) : Edg	ge AP, (r) : Remote AP							To	otal Entry : 4	
Security	•		AP PROFILE NAME	AP NAME	MAC	IP ADDRESS	ADMIN	OPER	MAP LOCATION	MODE	MODEL	VERSION
Rogues	•						STATUS	STATUS		General		
WLANs	×.		<u>ap 1</u>	npi_AP1	f4:d9:fb:3d:e1:44	192.168.10.50	Up	Up		AP	WEA302i	1.4.8.R
Radio	•		ap 2	Warehouse_Root	f4:d9:fb:3d:c4:84	192.168.10.52	Up	Up		General AP	WEA302i	1.4.8.R
User QoS			<u>ap 3</u>	eddie_home	f4:d9:fb:3d:e2:c4	192.168.70.28	Up	Down		General AP(r)	WEA302i	1.4.8.R
Mobility Management	•		<u>ap 4</u>	Warehouse_Repeat	f4:d9:fb:3c:23:2c	192.168.10.55	Up	Up		General AP	WEA302i	1.3.14.R
DNS												



Change the AP M	lode to Root AP	istration   Help	
	General 802.11	a/n 802.11b/g/n Advanced	
Controller >	Access Points > General		
Access Points			
AP Groups	<b>`</b>		Back Apply
Remote AP Groups	AP PROFILE NAME	ap_2	
Coqueity		Warehouse_Root	(5)
security ,		Poot AP	<b>—</b> /
Rogues >	AP MODE -		The AP will now report
WLANs >	MAP LOCATION		
Radio >	LOCATION	MDF	after hitting Apply
User QoS	IP ADDRESS	192.168.10.52	
Mobility Management	IP ADDRESS POLICY	O DHCP     O AP Priority (AP Followed)     O Static IP	
Mobility Management	IP ADDRESS	0.0.0.0	
DNS	NETMASK	0.0.0.0	
NTP	GATEWAY	0.0.0.	
DHCP	DISCOVERY TYPE 2	AP Followed Current Discovery Type : DHCP	
	ADMIN STATUS	Up	
	OPER STATUS	Up	
	PRIMARY CONTROLLER NAME 3		
	SECONDARY CONTROLLER NAME 3		
	TERTIARY CONTROLLER NAME 3		

Samsung Wireless Enterprise	Monitor	Configuration	Administratio	n   Help							
Controller 🗸	Access	Points									
General Ports	Curre	Current Filter : None Change									
Interfaces		The mode is now changed									
Lets change	(e) : Edg	(e) : Edge AP, (r) : Remote AP									
this AP		AP PROFILE NAME	AP NAME	MAC	IP ADDRESS	ADMIN STATUS	OPER STATUS	MAP LOCATION	MODE	MODEL	VERSION
Mode to Repeater		<u>ap 1</u>	npi_AP1	f4:d9:fb:3d:e1:44	192.168.10.50	Up	Up		General AP	WEA302i	1.4.8.R
		<u>ap 2</u>	Warehouse_Root	f4:d9:fb:3d:c4:84	192.168.10.52	Up	Up		Root AP	WEA302i	1.4.8.R
Statistics		<u>ap 3</u>	eddie_home	f4:d9:fb:3d:e2:c4	192.168.70.28	Up	Down		General AP(r)	WEA302i	1.4.8.R
Access Points		<b>a</b> p 4	Warehouse_Repeat	f4:d9:fb:3c:23:2c	192.168.10.55	Up	Up		General AP	WEA302i	1.3.14.R
Remote AP Groups	6				1						
Security >											

Change the AP N	/lode to Root AP	istration   Help	
	General 802.11	a/n 802.11b/g/n Advanced	
Controller	Access Points > General		
Access Points		7)	
AP Groups		~	Back Apply
Remote AP Groups	AP PROFILE NAME	ap_4 Warehouse Repeat	
Security >	¥		
Rogues >	AP MODE <sup>1</sup>	Repeater AP 💌	The AP will now reboot
WLANs >	MAC ADDRESS	f4:d9:fb:3c:23:2c	ofter bitting Apply
Radio +	LOCATION	Warehouse	arter nitting Apply
User QoS	IP ADDRESS	192.168.10.55	
Mobility Management	IP ADDRESS POLICY	OHCP      AP Priority (AP Followed)     Static IP	
DNS	NETMASK		
NTP	GATEWAY	0.0.0.0	
DHCP	DISCOVERY TYPE 2	AP Followed Current Discovery Type : DHCP	
	ADMIN STATUS	Up	
	OPER STATUS	Up	
	PRIMARY CONTROLLER NAME 3		
	SECONDARY CONTROLLER NAME 3		
	TERTIARY CONTROLLER NAME 3		
-			

Samsung Wireless Enterprise	Monitor Configuration	Administration   Help			
Controller >	Controller > General				
Access Points					
AP Groups		Apply			Apply
Remote AP Groups	AP Management		SIP ALG		
Security	IP ADDRESS	192 . 168 . 50 . 11	SIP ALG (VOIP AWARE)	€ Enable C Disable	
boomry	INTERFACE	vlan1.50	SIP ERROR RESPONSE	● Enable O Disable	
Wireless Intrusions			SIP DETECT LONG DURATION CALL	€ Enable C Disable	
WLANs			SIP NO ANSWER TIMEOUT (SEC)	600	
		Apply	SIP CONNECT TIMEOUT (SEC)	7200	
Radio			SIP MONITORING PORT 1	5060	
User QoS	You will need to a	ctivate the Repeater S	Service	0	
Mobility Management		•		0	
DNC			SIP MONITORING PORT 4	0	
DNS		Apply	SIP MONITORING PORT 5	0	
NTP					
DHCP	Repeater Service				Apply
	SERVICE	C Enable C Disable			
	<u> </u>		Voice Monitoring		
		Apply	VOICE QUALITY MONITORING	€ Enable C Disable	
		Арріу	VOICE ENHANCED MONITORING	Enable C Disable	



- Now unplug the Repeater AP
- Install the Repeater AP with an external power supply
- The AP should now connect to the Root AP
- Once an AP has been changed to Root or Repeater type, it cannot be apart of the default AP Group.
- You must change the AP back to General or move the APs to another AP Group.

Samsung Wíreless Enterprise™

Access Points											
Curr	Current Filter : None Change										
Wor	Working Setup "Access Points"										
	AP PROFILE NAME	AP NAME	MAC	IP ADDRESS	ADMIN	OPER	MAP LOCATION	Tot	al Entry : 4	VERSION	
					STATUS	STATUS		General			
	<u>ap 1</u>	npi_AP1	f4:d9:fb:3d:e1:44	192.168.10.50	Up	Up		AP	WEA302i	1.4.8.R	
	<u>ap 2</u>	Warehouse_Root	f4:d9:fb:3d:c4:84	192.168.10.52	Up	Up		Root AP	WEA302i	1.4.8.R	
	<u>ap 3</u>	eddie_home	f4:d9:fb:3d:e2:c4	192.168.70.28	Up	Down		General AP(r)	WEA302i	1.4.8.R	
	<u>ap 4</u>	Warehouse_Repeat	f4:d9:fb:3c:23:2c	192.168.10.56	Up	Up		Repeater AP	WEA302i	1.4.8.R	

#### You can see here that I have connected my phone to the repeater AP and using the 2.4GHz protocol

							_					
Active Alarm		Current Filter :	None									Change
WLANs												
Access Points	F											Export
Stations			LICED				_				To	tal Entry : 4
Rogues	•	MAC	NAME	IP ADDRESS	AP NAME	SSID		AP MAP LOC.	AUTH.	CYPHER	PROTOCOL	CHANNEL
	_	5c:0a:5b:1a:cc:79		192.168.100.113	npi_AP1	npi_wlan			WPA2	CCMP	802.11n(5GHz)	161
Interference Devices		38:aa:3c:93:69:e2		192.168.100.121	npi_AP1	npi_wlan			WPA2	CCMP	802.11n(5GHz)	161
Statistics	•	20:10:7a:56:dd:13		192 168 100 111	npi_AP1	ppi_wlyo			WPA2	CCMP	802.11n(5GHz)	161
		cc:3a:61:0e:21:55		192.168.100.143	Warehouse_Repeat	npi_wlan			WPA2	CCMP	802.11n(2.4GHz)	11
VOIP Calls	P 1											
Resource												
						-						
	-	045										
WE-WLAN - Day 2 - Ja	n. 2	015										



# 3.7 Simple Network Management Protocol (SNMP)

- 3.7.1 SNMP Supported
- 3.7.2 Enabling SNMP
- 3.7.3 Trap Control

# 3.7.1 SNMP Supported



#### **SNMP** versions supported by Samsung APC

- SNMPv1/v2c : Community-based Simple Network Management Protocol Version 2
- SNMPv3 : Security model including authentication, encryption

#### Security Features in SNMPv2c/v3

Version	Level	Authentication	Encryption	How to work
v1/v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication
v3	noAuthNoPirv	Username	No	Uses a Username match for authentication
v3	authNoPriv	MD5 or SHA	No	Authentication based on the HMAC-MD5 or HMAC-SHA
v3	authPriv	MD5 or SHA	DES or AES	Encryption in addition to authentication based on the DES or AES

#### Trap

• SNMP Trap can be configured on the both WEC and CLI.

#### Notice

- SNMPv1/v2c and v3 can be configured on the both WEC and CLI modes
- Each AP does not support SNMP agent.
- Typically, SNMP set/get packet use port 161, SNMP Trap/inform packet use port 162.
- Port number of SNMP Trap/inform is configurable.



# 3.7.2 Enabling SNMP

- 3.7.2.1 SNMP v1/v2c
- 3.7.2.2 SNMPv3

# 3.7.2.1 SNMP v1/v2c



Samsung Wireless Ente	erprise	Monitor   Conf	guration	Administration	НеІр					
SNMP	-	SNMP > APC > 1	1/v2c Commun	ity						
APC	<b>.</b>		In SNMPv1/v2c, Community name is used for authentication.							
System Info	→ SNMP manager must have a same Community name as AP(							Add Delete		
v1/v2c Communi	ity					, , , , , , , , , , , , , , , , , , , ,		Total Entry : 0		
v3 User Trap Receiver		Сом	COMMUNITY NAME IPV4 ADDRESS IPV6 ADDRESS NETMASK					ACCESS TYPE		
Trap Control	Þ					No data				
AP	) - F									
	SNMP > Co	mmunity > Add	If IP a then /	ddress is 0.0 APC permits	.0.0 and N all SNMP r	etmask is 0, nanagers access throug	gh SNMP	Apply		
	NAME		samsungrw							
	IP VERSION		🖲 v4 🔘 v6							
	IPV4 ADDRE	ESS	10.240.	128. 100						

IPV4 ADDRESS	10 . 240 . 128 . 100
IPV6 ADDRESS	0000: 0000: 0000: 0000: 0000; 00000: 0000
NETMASK	32 Access Type : RO (Read Only) and RW (Read-Write)
ACCESS TYPE	RW -
	RO RW

# 3.7.2.1 SNMP v1/v2c



Samsung Wireless Enterprise		Monitor   Co	nfiguration   A	Administration	Неір			
SNMP	-	SNMP > APC	> Trap Receiver					
APC	•							
System Info								Add Delete
v1/v2c Community								Total Entry : 0
v3 User		□ NO.	IPV4 ADDRESS	PORT NUMBER	TRAP VERSION		COMMUNITY NAME	-
Trap Receiver					No da	ata		
Trap Control	Þ							
AP	Þ							

SNMP > APC > Trap Receiver >	Address = SNMP Manager	
		Back Apply
IPV4 ADDRESS	192. 168. 100. 99	
PORT NUMBER	162	
TRAP VERSION	v1 •	
COMMUNITY NAME	samsungwlan	

### 3.7.2.2 SNMPv3



AUTH PROTOCOL No data	PRIV PROTOCOL	Add D Total
AUTH PROTOCOL No data	PRIV PROTOCOL	Add C Total
AUTH PROTOCOL No data	PRIV PROTOCOL	Add Total
AUTH PROTOCOL No data	PRIV PROTOCOL	Add []
AUTH PROTOCOL No data	PRIV PROTOCOL	Total
AUTH PROTOCOL No data	PRIV PROTOCOL	
No data		ACCESS TYPE
	E	Back Apply
Entor in the l	ogin info from	
	U	

WE-WLAN - Day 2 - Jan. 2015

# 3.7.3 Trap Control



#### Here you can set the alarm thresholds

Samsung Wireless Enterprise	Monitor Configuration	Administration   Help		
SNMP -	SNMP > APC > Trap Control >	Alarm Threshold		
APC 🗸				
System Info				Apply
v1/v2c Community				
v3 User	CPU Load		Memory Usage	
Trap Receiver	MONITOR		MONITOR	
Trap Control 🔹 👻	THRESHOLD(%)	90	THRESHOLD(%)	90
Alarm Threshold				
Alarm Information				
Event Information	Disk Usage		Fan Alarm	
AP ►	MONITOR	🖲 Enable 🖉 Disable	MONITOR	
HTTP-HTTPS	THRESHOLD(%)	90	THRESHOLD(LEVEL)	3
Telnet-SSH				



# 4. Security

- 4.1 Firewall / ACL
- 4.2 Captive Portal
- 4.3 Web Pass-Through
- 4.4 Conditional Web Redirection

# 4.1 Firewall / ACL

Samsung Wireless Enterprise	Monitor Configuration Administration Monitor Configuration Administration The APC is not a complex firewall
Controller >	Security > Firewall > General
Access Points	
AP Groups	Apply
Remote AP Groups	FIREWALL © Enable © Disable
Security -	
AAA >>	
Captive Portal 🔹	The WEA8500 has a built in Firewall, in order to use
Guest Users	you must onable it here
Web Authentication	you must enable it here
MAC Filter	
Access Control Lists	
Firewall 🔹	
General	
Policy	
Interface	

WE-WLAN - Day 2 - Jan. 2015

# 4.1 Firewall / ACL

Samsung Wireless Enterpris	e	Monitor   Configuration   /	Administration Help Here you can create polices for the Firewall
Controller	•	Security > Firewall > Policy >	Add
Access Points			
AP Groups			Back Apply
Remote AP Groups		PROTOCOL	Any 🔽
Security	•	SOURCE IP	Any 🔻 0.0.0/0.0.0
ААА	•	SOURCE PORT	Any 🗸
Captive Portal	•	DESTINATION IP	Any 🔽 0, 0, 0, 0 / 0, 0, 0, 0
Guest Users		DESTINATION PORT	
Web Authentication			Natilsad
MAC HITER			
Firewall	<i>P</i>	ACTION	Feinin V
General	•		
Policy			
Interface			

# 4.1 Firewall / ACL

Samsung Wireless Enterpr	ise	Monitor   Configuratio	on Administration Help
Controller	÷	Security > Firewall > In	nterface > Add
Access Points			
AP Groups			Back Apply
Remote AP Groups		INTERFACE	Select Interface
Security	•	DIRECTION	Ingress Egress Forward
^^^		POLICY RULE	
Cantive Portal	-		
Guest Users	•		
Web Authentication			
MAC Filter		c	Solact the Interface to Apply the Policy to and the
Access Control Lists	•		diversions
Firewall	•	C	airection
General			
Policy			
Interface			



# 4.2 Captive Portal

- 4.2.1 Introduction
- 4.2.2 Access Control List
- 4.2.3 Guest Access WLAN
- 4.2.4 Web Authentication
- 4.2.4 Guest Users
- 4.2.5 Lobby Ambassador
- 4.2.6 Enable WLAN



- Samsung's wireless LAN system provides a built-in Guest Access function.
- A guest will be granted limited service after connecting to a specific WLAN (SSID).
- The Guest will be redirected to a login page, where at the time they must enter the ID and Password provided by the WLAN administrator or the Lobby Ambassador.
- This will gain the Guest access to the network

Samsung Wireless Enterpri	se	Monito	or   C ity > A	configura	ation   Ad	dministra Our Gues 1. Redir 2. Allow and F	l to cre st user ect th v them PW	eate an ACL that s em to the inter n access after lo	t will redi nal web p gging in v	rect bage with ID
AP Groups		_							Ва	ck Apply
Remote AP Groups	_		192	2.168	3.xx.1(	) = the interfac	e IP of	the network		
ΔΔΔ			yu		COIIII				Ad	d Delete
Captive Portal	•		SEQ	ACTION	PROTOCOL	SOURCE IP/MASK	SOURCE	DESTINATION IP/MASK	DESTINATION	MATCH
MAC Filter			1	Permit	UDP	Any	Any	Any	=53	0
Access Control Lists	•		<u>2</u>	Permit	Any	Any	Any	192.168.11.10/255.255.255.255	Any	0
Time Profile	_		<u>3</u>	Permit	Any	192.168.11.10/255.255.255.255	Any	Any	Any	0
IP ACL			<u>4</u>	Permit	ICMP	Any	=0	Any	=0	0
Access Group(Interface	)									
Access Group(System)										



Samsung Wireless Enterpri	se	User [ eddie ]   Logout   Save Co	nfiguration
Controller Access Points	· ^	Security > Access Control Lists > IP ACL	Delete
AP Groups Remote AP Groups Security		NAME No data	
AAA Captive Portal MAC Filter	+	Foot Notes : 1. Can't be deleted if the access list is used in Access Group.	
Access Control Lists Time Profile IP ACL	•	We need to create an access control list that will redirect users to the internal captive portal	
Access Group(Interface Access Group(System)	2)		_

Here are the create to set	actio up o	ons we need to ur Captive Portal	User [ eddie ]   Logout   Save Configuration
			the other 3 sequences needed
Controller	· •	Security > Access Control Lists	> IP ACL > Add
Access Points		0	This name will match for all entries
AP Groups		<u> </u>	Back Apply
Remote AP Groups		NAME	CaptivePortal 1
Security	•	PROTOCOL	
AAA	•	SOURCE IP	Any 🗸 0.0.0.0/0.0.0.0
Captive Portal	•	SOURCE PORT	Any 🗸
MAC Filter		DESTINATION IP	Any 🗸 0.0.0.0.0.0.0.0.0.0
Access Control Lists	•	DESTINATION PORT	
Time Profile		TOS	▼
IP ACL		OS-AWARE	Any V
Access Group(Interface)	)	ACTION	Permit V
Access Group(System)			



Samsung Wireless Enterpris	se Ma	onitor Configuration Administration Help	User [ eddie ]   Logout   Save Configuration
Controller	→ <mark>∧</mark> S	ecurity > Access Control Lists > IP ACL	
Access Points AP Groups			Add Delete
Remote AP Groups		CaptivePortal	
Security	•		
AAA Captive Portal	) C	lick the Named ACL and add the other	
MAC Filter		lies	
Access Control Lists Time Profile	•		
IP ACL			
Access Group(Interface	)		
Access Group(System)			



Samsung Wireless Enterpris	se	Monitor   Configuratio	n Administration Help	User [ eddie ]   Logout   Save Configuration
Controller Access Points	· ^	Security > Access Control	Lists > Add	
AP Groups				Back Apply
Remote AP Groups		NAME	CaptivePortal	
Security	•	PROTOCOL	Any 🗸	
AAA	→ I	SOURCE IP	Any V 0, 0, 0, 0, 0, 0, 0, 0, 0	Hit Apply,
Captive Portal	• •	SOURCE PORT	Any 🗸	then add the
MAC Filter		DESTINATION IP	Address V 192 . 168 . 11 . 10 / 255 . 255 . 255 . 255	other 2 rules
Access Control Lists	•	DESTINATION PORT	Any V	
Time Profile		TOS		
IP ACL		OS-AWARE	Any V	
Access Group(Interface	)	ACTION	Permit V	
Access Group(System)				



Wireless Enterpr	ise	Monitor   Configuration	n Administration Help	User [ eddle ]   Logout   Save Configuration
Controller Access Points	<u> </u>	Security > Access Control	Lists > Add	Pack
P Groups			Out which is	
emote AP Groups		SEOUENCE		/
ecurity	•	PROTOCOL	Any V	
۵۵۵		SQURCE IP	Address V 192, 168, 11, 10 / 255, 255, 255, 255	Hit Apply,
Captive Portal		SOURCE PORT	Any 🗸	then add the
MAC Filter		DESTINATION IP	Any V 0. 0. 0. 0 / 0. 0. 0. 0	last rule
Access Control Lists	<b>_</b>	DESTINATION PORT	Any 🗸	
Time Profile		TOS	V	
ΤΡΑΟΙ		OS-AWARE	Any 🗸	
Access Group(Interface	e)	ACTION	Permit V	
Access Group(System)				





ontroller	× 🗸 - 5	Security	> Access Co	ntrol Lists		ACL Lis	t complete		
ccess Points						Now le	t's assign it to		
D. Caravan						our WL	AN	Ва	ck Apply
P Groups	- 1			NAME			TIME PROFILE		
emote AP Groups				CaptivePort	al		٧		
ecurity	•		L						
AAA	•							Ad	d Delete
Captive Portal	•	S	EQ ACTION	PROTOCOL	SOURCE IP/MASK	SOURCE	DESTINATION IP/MASK	DESTINATION	MATCH
			-			PORT		PORT	COUNT
MAC Filter									_
MAC Filter Access Control Lists	-		<u>1</u> Permit	UDP	Any	Any	Any	=53	0
MAC Filter Access Control Lists	•		<u>1</u> Permit <u>2</u> Permit	UDP Any	Any Any	Any Any	Any 192.168.11.10/255.255.255.255	=53 Any	0 0
MAC Filter Access Control Lists Time Profile	•		<u>1</u> Permit <u>2</u> Permit <u>3</u> Permit	UDP Any Any	Any Any 192.168.11.10/255.255.255.255	Any Any Any	Any 192.168.11.10/255.255.255.255 Any	=53 Any Any	0 0 0



Samsung Wireless Enterprise	Monitor	Con	figuration   Ad	Iministration	Неір		User [ eddie ]	Logout   Save Configuration
<ol> <li>In this case we will edit the current WLAN</li> <li>First Disable the Guest11 WLAN that already exists.</li> <li>Next click on the ID number and lets change the Security Policy</li> </ol>					Enable Disat	Change De Add Delete		
Security >		ID	PROFILE NAME	SSID	INTERFACE GROUP	RADIO AREA	ADMIN STATUS	SECURITY POLICIES
Rogues		1	Company10	Company10	CompanyGroup10	2.4GHz/5GHz	Enable	WPA + WPA2
WLANs 🗸		<b>₩</b> <sub>2</sub>	Guest11	Guest11	GuestGroup11	2.4GHz/5GHz	Enable	WPA + WPA2
WLANs Radio >					1			
Hear Oas		-	_	_		_	_	

Samsung Wireless Enterprise	Monitor Configuration	Administration   Help	User [ eddie ]   Logout   Save Configuration
	General Secu	rity Advanced	
Controller >	WLANs > WLANs > General		
Access Points		Go to the secu	urity Tab to setup
AP Groups		access for this	WLAN Back Apply
Remote AP Groups	ID PROFILE NAME	2 Guest11	
Security >	SSID	Guest11	
Rogues >	AP GROUP LISTS	default, Main_AP_Group	
WLANs -	RADIO AREA <sup>1</sup>	All V	
WLANs	CAPWAP TUNNEL MODE 2	802.3 Tunnel 🗸	Make sure to check Enable
Radio >	SUPPRESS SSID	O Enable 💿 Disable	for Guest Service
User QoS	AAA OVERRIDE	○ Enable	
Mobility Management	GUEST SERVICE	● Enable ○ Disable	
DNS	ADMIN STATUS	⊖Enable	

# 4.2.3 Guest Access WLAN



# 4.2.3 Guest Access WLAN

General     Security       WLANs > WLANs > Security > L3       L2		L3 is used for Guest Access Security		Hit Apply
			•	Back Apply
	PROFILE NAME	Guest71		
	WEB POLICY	Enable O Disable		
	Web Authentication			
	C Web PassThrough			
	C Conditional Web Redirection			
C One Time Redirection				
	PRE-AUTHENTICATION ACL	CP 💌	1.	Here we will enable the web
	OVERRIDING REDIRECT URL	C Enable C Disable		policy
	URL		2.	Select the Authentication
			3.	Select the Pre-Authentication ACL



Samsung Wireless Enterpris	e	Monitor Configuration Administration Help	User [ samsung ]
Controller	F	Security > Captive Portal > Web Authentication	
Access Points			
AP Groups		Select the Web Authentication Type	
Remote AP Groups		Web Login Page	
Security	•	WEB AUTHENTICATION TYPE Internal	
AAA	Þ	Redirect to the requested URL.     C Redirect URL	
Captive Portal	•		
Guest User			
Web Authentication		Foot Notes :	
MAC Filter		1. If the Redirect URL is empty, redirect to default authentication success page.	
Access Control Lists	•	2. Logo file should be PNG or JPG format.	
Firewall	•	3. Terms and Conditions file should be TXT format (UTF-8 encoding only).	
NAT	•	Apply	
Role Based Access Control		Input the interface IP of the network	
Rogues	•	Web Service Address vou are connecting to.	
WLANs		IP ADDRESS 192. 168. 71. 10	
			_



Samsung Wireless Enterprise	Monitor Configuration Administration Help
We have 4 differ	ent WEB Auth types
Controller >	Security > Captive Portal > Web Authentication
Access Points AP Groups	Preview Apply
Remote AP Groups	Web Login Page
Security     ▼       AAA     ▶       Captive Portal     ▼       Guest Users	WEB AUTHENTICATION TYPE       Internal         Internal       Internal         Internal       Soriginal of External         Downloaded       Customized
Web Authentication	e where the user should go after they have authenticated
AFTER AUTHENTICATION	<ul> <li>Redirect user's original opening web page.</li> <li>Redirect URL</li> </ul>

File Edit View Favorites Tools Hel	hp $\mathcal{P} \cdot \mathcal{O} \times$ 🥔 Wireless Enterprise Manager $\times$	http://192.168.72.10/content/configura       Image: State	Ĩ
Samsung Wireless Enterprise	Monitor Configuration Administration Help	Guest Service	tion
Controller Se Access Points AP Groups	elect Internal for Classroom	Enter your user name      Preview Apply	
Remote AP Groups Security	WEB AUTHENTICATION TYPE Internal  C Dedirect to the one quested URL.	LOGIN	-
Captive Portal  Guest Users Web Authentication MAC Filter Access Control Lists Firewall NAT	<ul> <li>AFTER AUTHENTICATION <sup>1</sup></li> <li>Using Internal,</li> <li>the users will see</li> <li>a login screen</li> <li>appear like this</li> </ul>	WELCOME         In order to use the wireless network, Please login         your assigned/registered account         If you do not know or have forgotten your account         and/or password, Contact to Help Desk for         assistance.         Copyright © 1995-2014 SAMSUNG All rights reserved	
Role Based Access Control  Rogues  WLANs	Web Service Address IP ADDRESS 192, 168, 71, 10		_
Radio >	Web Service Port		


## 4.2.4 Web Authentication

Samsung Wireless Enterprise™

	Using Customized we can editing the fields below	Preview
Web Login Page		
WEB AUTHENTICATION TYPE	Customized	
LOGO	Hide O Show	
SELECT FILE 2		Browse
HEADER	WELCOME	
BODY	In order to use the wireless network, Please login your assigned/registered account. If you do not know or have forgotten your account and/or password, Contact to Help I stance.	Desk for assi
FOOTER	Copyright ** 1995-2014 SAMSUNG All rights reserved	
TERMS AND CONDITIONS	Hide O Show	
SELECT FILE <sup>3</sup>		Browse
COLOR	#0	

Samsung Wireless Enterprise™

Samsung Wireless Enterprise	Monitor	Configuration	Administration	Help				
You can choose the form	your G	uest Auth	Type her	9				
Access Points AP Groups Remote AP Groups Security AAA Captive Portal Guest Users Web Authentication	GUEST A PRIMAR SECOND CACHE D	UTH TYPE Y RADIUS SERVER <sup>1</sup> ARY RADIUS SERVER <sup>1</sup> DURATION (SEC.) ES :	Local	- V - V	Local RADIUS Local/RADIU RADIUS/Loo	JS cal		Apply
Access Control Lists → Firewall → NAT → Role Based Access Control	1. GL •	Here we When Au or custor	can create ithenticati nized it wi	e Guest U ion is set ill use this	sers to interna s list			Change
Rogues	_						Add Delete	Import Export Total Entry : 1
User QoS		USER ID <u>quest</u>	START TIME	END TIME	FULL NAME	Enable	SPONSOR -	GRANTOR System

Samsung Wíreless Enterprise™

Samsung Wireless Enterprise	1	Monitor   Configuration   Admin	istration   Help		
					Local Net Users from your Internal Radius Server can
Controller	÷	Security > Captive Portal > Cuest User	rs		be used as well.
Access Points					
AP Groups		· · · ·			Арріу
Remote AP Groups		GUEST AUTH TYPE	RADIUS   Internal		
Security	•	SECONDARY RADIUS SERVER <sup>1</sup>	T		
AAA	•	CACHE DURATION (SEC.)	60		
Captive Portal	•	/			
Guest Users					
Web Authentication		Foot Notes :			
MAC Filter		1. In case of using RADIUS authentication, RAI	DIUS server should be confi	igured.	
Access Control Lists	)				
Firewall	•	Cuest licers			
NAT	•	00001 05015			
Role Based Access Control		Current Filter : None			Change

Samsung Wíreless Enterprise™

Samsung		Monitor	Configuration	Administratio	n Help				
wireless Enterpris	52		*						
Controller	×.	Security	> Captive Portal >	Guest Users					
Access Points									
AP Groups									Apply
Remote AP Groups		GUEST AU	ЈТН ТҮРЕ	Local	T				
Security	•	PRIMARY	( RADIUS SERVER <sup>1</sup>		▼				
ΔΔΔ		SECOND	ARY RADIUS SERVER <sup>1</sup>		▼				
Captive Portal	• •	CACHE D	URATION (SEC.)	60					
Guest Users									
Web Authentication		Foot Note	s :						
MAC Filter		1. In case	of using RADIUS authe	ntication, RADIUS serv	er should be configured	ł.			
Access Control Lists	•								
Firewall	•	Guest Use	ers	Crea	te a Gues	t User			
NAT Role Based Access Control	•	Curren	t Filter : None						Change
Roques	•								
Nogues							A	dd Delete	Import Export
WLANS	•								Total Entry : 1
Radio	F		USER ID	START TIME	END TIME	FULL NAME	STATUS	SPONSOR	GRANTOR
User QoS			<u>quest</u>	-	-	-	Enable	-	System

Samsung Wíreless Enterprise™

Security > Captive Portal > Gue	est Users > Add	
		Back Apply Apply & Print
Guest Users		
USER ID	guest868003	Senerator
PASSWORD 1	G	Generator
CONFIRM PASSWORD		
START TIME	2014-03-06 00 ▼ : 00 ▼ : 00 ▼	
END TIME	2014-03-06 23 ▼ : 59 ▼ : 59 ▼ Unlimited	
FULL NAME		The Generator will auto
COMPANY		select the User ID and
EMAIL		Select the Oser iD and
PHONE		Password
MAX SESSION		
STATUS	Enable Oisable	
COMMENTS		
Here you can detern Time and End Time.	nine the Start	
The Guest User Acco	unt will be	
deleted after End Tir	ne	
COMMENTS		
1.00		

Samsung Wíreless Enterprise™

Security > Captive Portal > Gue	est Users > Add
How many sessions for this account	Back Apply Apply & Print
allowed?	Juest868003 Generator
PASSWORD 1 CONFIRM PASSWORD START TIME	You have the option to print the login information here or just apply
END TIME	2014-03-06 23 ▼ : 59 ▼ : 59 ▼
FULL NAME COMPANY EMAIL PHONE	
MAX SESSION STATUS	1 ● Enable
COMMENTS	This information will appear on the print out
Sponsor	
SPONSOR	
DEPARTMENT	
EMAIL	
COMMENTS	







Samsung Wireless Enterprise	Monitor   Configuration	Administration   Help
SNMP >	Local Management Users	<ol> <li>Create an account for the front desk</li> <li>With an (Lobby Ambassador) account, the user will be able to create guest users.</li> </ol>
HTTP-HTTPS Telnet-SSH	1	Go to Administration>Local Management Users> APC and hit Add Back Apply
Local Management Users	ID PASSWORD	frontdesk       Image: samsung
Logs >	CONFIRM PASSWORD	samsung
DB backup/restore	LEVEL	4 (Lobby Ambassador)
Reboot >		

## 4.2.5 Lobby Ambassador





## 4.2.5 Lobby Ambassador



uest Users	Guest U	lsers T	ne only fu has is to c	nction this acc reate Guest U	count sers			
	Guest Us	ers						
	Currer	nt Filter : None						Change
							4	Add Delete
							_	Total Entry : 2
		USER ID	START TIME	END TIME	FULL NAME	STATUS	SPONSOR	GRANTOR
		quest	-	-	-	Enable	-	System
		<u>quest868003</u>	-	2014-03-06 23:59:59	-	Enable	-	eddie

## 4.2.6 Enable WLAN



Controller	• WLANs	> WLAI	۱s					
ccess Points	Curr	ent Filter :	None			<b>\</b>		Change
P Groups							•	
mote AP Groups							Enable Disa	ble Add Delete
curity	•							Total Entry :
		ID	PROFILE NAME	SSID	INTERFACE GROUP	RADIO AREA	ADMIN STATUS	SECURITY POLICIES
gues		<u>1</u>	Company10	Company10	CompanyGroup10	2.4GHz/5GHz	Enable	WPA + WPA2
ANs	• · · · · · · · · · · · · · · · · · · ·	2	Guest11	Guest11	GuestGroup11	2.4GHz/5GHz	Disabled	Web Authentication
/LANs					🦉 Wireless Enterp	orise Manager - N	Windows Internet	E 🗆 🗉 🗙
				_	@ http://192.168	.10.10/confirm_p	assword.php?frm:	=form&fn_name=chl



### Setup a WLAN that uses Captive Portal with Internal Web Authentication

### First create the ACL for Captive Portal (1/4)

- 1. Go to Configuration  $\rightarrow$  Security $\rightarrow$  Access Control Lists  $\rightarrow$  IP ACL  $\rightarrow$  Add
  - a. Name = CaptivePortal
  - b. Sequence = 1
  - c. Protocol = udp
  - d. Source IP = Any
  - e. Source Port = Any
  - f. Destination IP = Any
  - g. Destination Port = 53
  - h. Action = Permit
  - i. Apply



### Setup a WLAN that uses Captive Portal with Internal Web Authentication

### First create the ACL for Captive Portal (2/4)

- 1. Security → Access Control Lists → IP ACL → CaptivePortal
  - a. Sequence = 2
  - b. Protocol = Any
  - c. Source IP = Any
  - d. Source Port = Any
  - e. Destination IP = 192.168.xx.10/255.255.255.255
  - f. Destination Port = Any
  - g. Action = Permit
  - h. Apply



### Setup a WLAN that uses Captive Portal with Internal Web Authentication

### First create the ACL for Captive Portal (3/4)

- 1. Security → Access Control Lists → IP ACL → CaptivePortal
  - a. Sequence = 3
  - b. Protocol = Any
  - c. Source IP = 192.168.xx.10/255.255.255.255
  - d. Source Port = Any
  - e. Destination IP = Any
  - f. Destination Port = Any
  - g. Action = Permit
  - h. Apply



### Setup a WLAN that uses Captive Portal with Internal Web Authentication

### First create the ACL for Captive Portal (4/4)

- 1. Security  $\rightarrow$  Access Control Lists  $\rightarrow$  IP ACL  $\rightarrow$  CaptivePortal
  - a. Sequence = 4
  - b. Protocol = ICMP
  - c. Action = Permit
  - d. Apply



### Setup a WLAN that uses Captive Portal with Internal Web Authentication

- 1. Go to Configuration  $\rightarrow$  WLANs  $\rightarrow$  WLANs  $\rightarrow$  Hit Change
  - a. ID = 2
  - b. Profile Name = GuestXX
  - c. SSID = GuestXX
  - d. Interface Group = GuestGroupXX
  - e. Radio Area = All
  - f. Guest Service = Enable
  - g. Click on the ID #3  $\rightarrow$  Security  $\rightarrow$  L3
  - h. WEB Policy = Enable with Web Authentication
  - i. Pre-Authentication ACL = CaptivePortal  $\rightarrow$  Apply
  - j. Enable the WLAN
- 2. Go to Configuration  $\rightarrow$  Security  $\rightarrow$  Captive Portal  $\rightarrow$  Web Auth
  - a. Web Auth Type = Internal
  - b. After Auth = optional setup
  - c. Input the Web service address
  - d. Hit Apply



#### Setup a WLAN that uses Captive Portal with Internal Web Authentication

- 1. Go to Configuration  $\rightarrow$  Security  $\rightarrow$  Captive Portal  $\rightarrow$  Guest Users
  - a. Guest Auth Type = Local
  - b. Click Add = Create a user ID to be able use this service
- 2. Test
  - a. Connect your PC or Phone to the SSID and login using the created guest ID



## 4.3 Web Passthrough

- 4.3.1 Introduction
- 4.3.2 ACL Rules
- 4.3.3 Setup Web Passthrough



### Introduction

- When the wireless users try to access Internet at the first time, Users are redirected to the web page specified by Web Passthrough.
- Web Passthrough is a useful feature that is used for guest access.
- The process of web passthrough is similar to that of web authentication except that authentication credentials are required for web authentication.

### **Process of Web Passthrough**

- User associate a WLAN with no security and get DHCP IP address.
- When user open a web browser, user sends a specific HTTP get message and APC returns HTTP Redirect message to the user.
- User's web page is redirected to the redirected web page.

### Limitations

• If WLAN is configured as local bridging mode, Web Passthrough does not work (PKG ver. 1.4.12)

## 4.3.2 ACL Rules



#### Applying ACL to WLAN

- Web passthrough is applied to the WLAN with no security.
- ACL is applied to prevent users from accessing unauthorized destinations but a part of packets from/to user must be allowed to establish a basic communication.

#### ACL Rules for Web Passthrough

- Allowed Rules
  - DNS flow
  - DHCP flow
  - Redirected Web server defined by administrator
  - (Optional) HTTP Proxy Server's IP Address
  - (Optional) The IP address of Server to download some applications
  - → All the above flows are from/to wireless users

#### Denied Rules

Traffic Flows that Administrator does not intend to allow on the WLAN

APC makes a redirection for HTTP get message only when the packet is matched by ACL denied rule.

#### (Internal implementation!)



## 4.3.3 Setup Web Passthrough

Controller		Security :	Access Con	trol Lists						
Access Points								_		
AP Groups									Back App	ly
Remote AP Groups			V	NAME /ebPassthrogh			TIME PROFILE	<b>▼</b>		
Security	-									
AAA	•							A	Add Delet	te
Captive Portal		<b>S</b>		PROTOCOL	SOURCE ID/MASK	SOURCE PORT	DESTINATION ID/MASK	DESTINATION PORT	матсн сои	NT
MAC Filter			Permit	UDP	10.10.100.0/255.255.255.0	Any	120.30.10.21/255.255.255.255	=53		DNS
Access Control Lists	-		Permit	UDP	10.10.100.0/255.255.255.0	Any	30.50.10.22/255.255.255.255	67~68		DHCP
Time Profile			Permit	Any	10.10.100.0/255.255.255.0	Any	10.20.30.40/255.255.255.255	Any		<b>Redirected Web Seve</b>
			Permit	Any	10.10.100.0/255.255.255.0	Any	10.40.40.40/255.255.255.255	Any		<b>HTTP Proxy Server</b>
I ACE			Permit	Any	10.10.100.0/255.255.255.0	Any	50.50.50/255.255.255.255	Any		Download Server
Access Group(Interfac										
Access Group(Interface	e)									
Access Group(Interface Access Group(System)				ACL inclu	des a implicit-deny	rule. So yo	u don't need to add a "c	deny any any	" rule.	
Access Group(Interfac Access Group(System) Firewall	e) ▶			ACL inclu	des a implicit-deny	rule. So yo	u don't need to add a "c	deny any any	" rule.	
Access Group(Interfac Access Group(System) Firewall NAT	≥) ▶ ▶			ACL inclu	des a implicit-deny	rule. So yo	u don't need to add a "c	deny any any	" rule.	
Access Group(Interfac Access Group(System) Firewall NAT	≥)	_		ACL inclu	des a implicit-deny	rule. So you	u don't need to add a "c	deny any any	" rule.	
Access Group(Interfac Access Group(System) Firewall NAT	≥) ▶	Gei	eral	ACL inclu Security	des a implicit-deny	rule. So you	u don't need to add a "c	deny any any	" rule.	
Access Group(Interfact Access Group(System) Firewall NAT Controller	> > >	Ger WLANS >	eral WLANs > /	ACL inclu Security	des a implicit-deny	rule. So you	u don't need to add a "c	deny any any	" rule.	1
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points	>> >> >>	Ger WLANS >	eral WLANS > /	ACL inclu Security	des a implicit-deny	rule. So you	u don't need to add a "c	deny any any	" rule.	
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points	> > >	Gei WLANs >	eral WLANs > /	ACL inclu Security Advanced	des a implicit-deny	rule. So you	u don't need to add a "c	deny any any	<b>" rule.</b> Back Αρμ	bly
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points AP Groups	> > >	Get WLANS >	eral VLANS > /	ACL inclu Security Advanced	des a implicit-deny	rule. So you	u don't need to add a "c	deny any any	<b>" rule.</b> Back App	oly r
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points AP Groups Remote AP Groups	>	Ger WLANS > PROETLE ACL RULE	eral WLANS > A	ACL inclu Security Advanced	des a implicit-deny Advanced	rule. So yo	u don't need to add a "c	deny any any	" rule. Back App	JV 4
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points AP Groups Remote AP Groups Security	E)	Gen WLANS > PROFILE ACL RULE STATIC A	eral WLANS > A	ACL inclu Security Advanced	des a implicit-deny Advanced	rule. So you	u don't need to add a "c	deny any any	" rule. Back App	
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points AP Groups Remote AP Groups Security Poques	E)	Get WLANS > PROFILE ACL RULE STATIC A DHCP OVI	eral WLANS > /	ACL inclu Security Advanced	Advanced          wlas1         WebPassthrogh         Enable       Disable         Enable       Disable		u don't need to add a "c	deny any any	" rule. Back Αρρ	
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points AP Groups Remote AP Groups Security Rogues	E	Gen WLANS > PROFILE ACL RULE STATIC A DHCP OV DHCP SER	eral WLANS > / AME DDRESS DISAL RRIDE VER <sup>1</sup>	ACL inclu Security Advanced	des a implicit-deny Advanced wlan1 WebPassthrogh • Enable @ Disable © Enable @ Disable	rule. So you	u don't need to add a "c	deny any any	" rule.	
Access Group(Interfact Access Group(System) Firewall NAT Controller Access Points AP Groups Remote AP Groups Security Rogues WLANS	E)	Get WLANS > PROFILE ACL RULE STATIC A DHCP OVI DHCP SER	eral WLANS > / IAME IDRESS DISAL RRIDE VER <sup>1</sup>	ACL inclu Security Advanced	des a implicit-deny Advanced	rule. So you	u don't need to add a "c	deny any any	" rule.	

Samsung Wireless Enterprise™

## 4.3.3 Setup Web Passthrough

General     Security     Advanced       Controller     WLANS > WLANS > Security > L3       Access Points     L2       AP Groups     Back       Renote AP Groups     PROFILE NAME       VLANS     WEB POLICY       Web PassThrough     Web PassThrough       OVERRIDING REDIRECT URL     Enable       Disable     OVERRIDING REDIRECT URL       VLANS     URL       PROFILE NAME     Image: Security       VIANS     OVERRIDING REDIRECT URL       PROFILE NAME     Enable       Disable     Overset on the security       VIANS     OVERRIDING REDIRECT URL       PROFILE NAME     Enable       Disable     URL       Image: Security     OVERRIDING REDIRECT URL       OVERRIDING REDIRECT URL     Enable       Disable     URL       Image: Security     ONS       Access Points     Approx       AP Groups     Enable       Security     ONS       Access Points     ONS       Access Points     ONS       Approx     Imable       Image: Security     Image: Security       Security     Image: Security       Image: Security     Image: Security       Image: Security     Image: Security					
Controller WLANs > WLANs > Security > L3   Access Points L2 IS Radius   AP Groups Back Ap   Remote AP Groups PROFILE NAME Wan1   Security Image: Controller Co			General	Security	Advanced
Access Points       12 13 Radus         AP Groups       Back       Back       Back       Back       Back       Apple         Security       •	Controller	•	WLANs > WLANs	> Security > L3	}
AP Groups   Renote AP Groups   Security   Rogues   VLANs   VLANs   VLNs   Radio   VLNs   PRE-AUTHENTICATION ACL   PRE-AUTHENTICATION ACL   VVERRIDING REGIRECTORI   DNS   Controller   AD Groups   Renote AP Groups   Renote AP Groups   Security   Image: Security	Access Points		L2 L3 Radius		
Renote AP Groups   Security   Rogues   WLANs   WLANs   WLANs   Radio   OverRationa Web Redirection   PRE-Authentication Act   OverRationa Redirect unit   Enable   Disable   UR   Intp://10.20.30.40/index.html     Access Points   AP Groups   Renote AP Groups   Security   Renote AP Groups   Security   Renote AP Groups   Security   Renote AP Groups   Security   Image: Sec	AP Groups				Back
Security   Rogues   WLANs   WLANs   WLANs   Radio   OConditional Web Redirection   PRE-AUTHENTICATION ACL   OVERRIDING REDIRECT URL   OVERRIDING REDIRECT URL   Inttp://10.20.30.40/index.html	Remote AP Groups		PROFILE NAME	W	lan1
Rogues   WLANs   WLANs   WLANs   WLANs   Radio   PRE-AUTHENTICATION ACL   OVERRIDING REDIRECT URL   Enable   Disable   URL   Intp://10.20.30.40/index.html     Access Points   Access Points   Security   Security <td>Security</td> <td> (</td> <td>WEB POLICY</td> <td>۲</td> <td>) Enable 🔘 Disable</td>	Security	(	WEB POLICY	۲	) Enable 🔘 Disable
WLANs     WLANs     PRE-AUTHENTICATION ACL     PRE-AUTHENTICATION ACL     OVERRIDING REDIRECT URL     Enable     DNS     Access Points     AP Groups     DNS Client 1     Security     Security     DNS Client 1     Security     Security     At Drops     DNS SERVER     120, 20, 10, 12     200, 0, 0, 0     VLANs     Security     Access Points     Apply     DNS SERVER     120, 20, 10, 21     200, 0, 0, 0     VLANs     Security     Access Points     Apply     Security     Securit	Rogues	•	Web Auther	ntication	
WLANS     PRE-AUTHENTICATION ACL       OVERRIDING REDIRECT URL     © Enable       Disable       URL       http://10.20.30.40/index.html	WLANs	•	Web PassTr Conditional	Web Redirection	
Access Points   Access Points   Apply   Renote AP Groups   Security   Kagues   VLANs	WLANs		PRE-AUTHENTICAT	ION ACL	v
URL     http://10.20.30.40/index.html     Controller     DNS     Access Points     AP Groups     Apply     NS Client 1     Security   Rogues   WLANs     UNANE	Radio		OVERRIDING REDI	RECT URL	) Enable 🔘 Disable
Controller DNS   Access Points Apply   AP Groups DNS Client 1   Security SERVICE @Enable @Disable   Ist DNS SERVER 120, 30, 10, 21   2ND DNS SERVER 0, 0, 0   3RD DNS SERVER 0, 0, 0					
Access Points   AP Groups   Remote AP Groups   Security   Rogues   WLANs   WLANs	Controller >	DNS			
AP Groups Apply   Remote AP Groups DNS Client 1   Security SERVICE   SERVICE © Enable © Disable   1ST DNS SERVER 120, 30, 10, 21   2ND DNS SERVER 0, 0, 0, 0   3RD DNS SERVER 0, 0, 0, 0	Access Points				
Remote AP Groups     DNS Client <sup>1</sup> Security     >       Rogues     >       WLANs     >       NO DNS SERVER     0,0,0,0       3RD DNS SERVER     0,0,0,0	AP Groups		<b>↓</b>		Apply
Security         SERVICE         © Enable         Disable           Rogues         1ST DNS SERVER         120, 30, 10, 21         120, 30, 10, 21           VLANS         3RD DNS SERVER         0, 0, 0, 0         0	Remote AP Groups	DNS Clien	nt <sup>1</sup>		
IST DNS SERVER         120, 30, 10, 21           2ND DNS SERVER         0, 0, 0, 0           WLANS         3RD DNS SERVER         0, 0, 0	Security >	SERVICE		● Enable ● Disable	
WLANS - BRD DNS SERVER 0, 0, 0, 0	Rogues +	1ST DNS S	SERVER		
	WLANs 🗸	3RD DNS	SERVER		
If LIPL is not IP address format but domain name APC must	WLANs				If LIRL is not IP address format but domain name APC must
Radio DNS Relay DNS Relay	Radio + I	DNS Rela	У		activate DNS client and to receive LIPL into ID address because
User QoS SERVICE © Enable © Disable Di	User QoS	SERVICE	2	○ Enable	Bedirection measure returned toward the wireless because
Mobility Management	Mobility Management	CACHING	SIZE <sup>4</sup>	10000	Redirection message returned toward the wireless user is sent with
IP address of redirected Web page	DNS				IP address of redirected Web page

Samsung Wireless Enterprise™



## 4.4 Conditional Web Redirection

- 4.4.1 Introduction
- 4.4.2 ACL Rules
- 4.4.3 Setup Conditional Web Redirect

## 4.4.1 Introduction



#### Introduction

- With Conditional Web Redirection, User is redirected to a particular web page when user reaches the expiration date or when the user needs to pay a bill for continued wireless service.
- When user's authentication period is expired and user try to authenticate, Radius server returns Samsung-Url-Redirect information and APC redirects to user's specified URL when they open a browser.

#### **Process of Conditional Web Redirection**

- 1. Radius server detects that user reaches the expiration date or needs to pay a bill for wireless service.
- 2. When user (re)authenticates after Step2, Radius server returns {Samsung-Url-Redirect} or {Samsung-Url-Redirect, Samsung-Url-Redirect-Acl} message.
- 3. When user open a browser, user is redirected to Redirected web page. Conditional Web Redirection is similar to the Web Passthrough but ACL rule for Conditional Web redirection is provided by Samsung-Url-Redirect-Acl message from Radius server or Pre-auth-ACL on WLAN L3 security can be applied.

#### Preconditions

• To use Conditional Web Redirection, Radius server must have Samsung dictionaries related to Conditional Web redirection

#### Limitations

- If WLAN is configured as local bridging mode, Conditional Web Redirection does not work (PKG ver. 1.4.12)
- Pre-auth-ACL feature on the WLAN does not work at PKG version 1.4.x (Available after 1.5.0)

## 4.4.2 ACL Rules



#### Applying ACL to WLAN

- Conditional Web Redirection can be applied to the WLAN with 802.1x.
- ACL is applied to prevent users from accessing unauthorized destinations but a part of packets must be allowed to establish a basic communication. This ACL has been used only until authentication is successful

#### ACL Rules for Conditional Web Redirection

- Allowed Rules
  - DNS flow
  - DHCP flow
  - Redirected Web server defined by administrator
  - (Optional) HTTP Proxy Server's IP Address
  - (Optional) The IP address of Server to download some applications
  - $\rightarrow$  All the above flows are from/to wireless users

#### **Denied Rules**

- Traffic Flows that Administrator does not intend to allow on the WLAN
- APC makes a redirection for HTTP get message only when the packet is matched by ACL denied rule.

#### (Internal implementation!)



# 4.4.3 Setup Conditional Web Redirect Wireless Enterprise

#### Case 1 : ACL rule is referred by Samsung-Url-Redirect-Acl

	General	Security	Advanced
Controller >	WLANs > WLANs > 9	Security > L3	
Access Points	L2   L3   Radius		
AP Groups			Back Apply
Remote AP Groups	PROFILE NAME	wlan1	
Security >	WEB POLICY	Enab	able 🔘 Disable
	Web Authenticat	tion	
Rogues	Meh PassThroug	ab	
WLANs 👻	Conditional Web	Redirection	
WLANs	PRE-AUTHENTICATION A	ACL	<b>v</b>
Radio >>	OVERRIDING REDIRECT	URL 🔘 Enab	able 💿 Disable
	URL		

#### Case 2 : Pre-auth-ACL is applied (Available after v1.5.0)

	General Secur	rity Advanced
Controller >	WLANs > WLANs > Security > L3	
Access Points	L2 L3 Radius	
AP Groups		Back Apply
Remote AP Groups	PROFILE NAME	wlan1
Security >	WEB POLICY	
	Web Authentication	
Rogues	🖉 Web PassThrough	
WLANs 👻	Conditional Web Redirection	
WLANs	PRE-AUTHENTICATION ACL	WebRedirect -
Radio >	OVERRIDING REDIRECT URL	🔘 Enable 💿 Disable
	URL	



# End of Day 2