



Troubleshooting

Dashboards, Inferences, Station Logs, and Packet Captures

Skills Learned

You'll be able to:

- > Drill down into specific information using the
 - Station diagnostic dashboard
 - Radio diagnostic dashboard
 - CLI
- > Configure syslog tracking
- > Collect and transmit diagnostic information

Practice Description

Lab will cover

- > Drilling down for information using Dashboards
- > Running and examining station logs
- > Running and examining packet captures

Information Facilities

- > Dashboards
 - Alarms
 - Station Dashboard -> Station Diagnostics
 - Radio Dashboard -> Radio Diagnostics
- > Inferences
- > Syslog

- > Station Logging
- > Station Counters
- > Packet Capture and Analysis
 - From a controller
 - From an AP
 - From a wireless laptop

- > E(z)RF Network Manager

Troubleshooting Triggers

> Proactive

- Alarms
- Inferences
- Trend Dashboards
[E(z)RF Network Manager]

> Reactive

- User complaints

Proactive Troubleshooting: Typical Questions

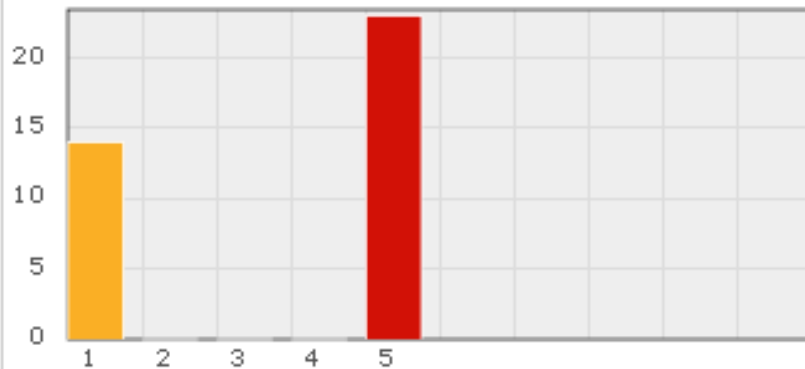
- > Are there throughput bottlenecks?
- > Are my APs functioning properly?
- > Is there something going on that I need to know about?
- > Where can I anticipate problems?

Dashboards - Alarms

Alarms Dashboard [\[Graph Help \]](#)

Alarm Category

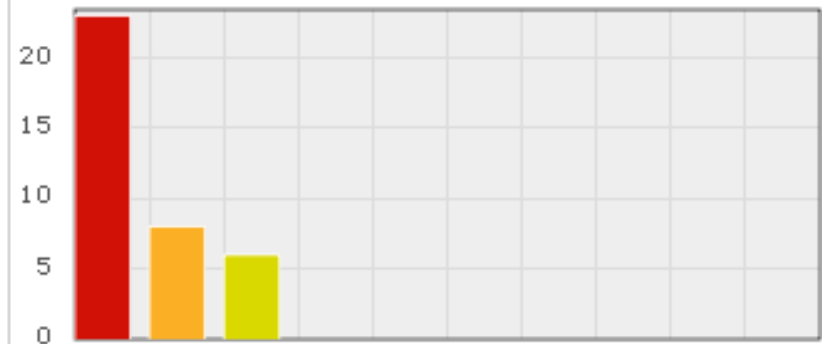
Total Alarms = 37



- 1: Controller Alarms
- 2: AP Alarms
- 3: Server Alarms
- 4: Wireless LAN Alarms
- 5: IDS Alarms

Alarm Severity

Total Alarms = 37



- Critical
- Major
- Minor

☒ Enable Auto Refresh

Alarms in the CLI

What alarms are present?

`show alarm`

What rogues are detected?

`show rogue-ap-list`

Show a summary of syslog messages.

`show syslog-table`

What syslog messages are there?

`show log`



Rogue Alarms

WLAN Management User: admin Controller-192.168.17.15 2:46:58 PM CLI Save Help MCRU

Configuration Maintenance Monitor >>>

Dashboard System Radio Station Voice Alarms Spectrum

Diagnostics Radio Station Inferences

Global Statistics Security Counters QoS Counters

Devices All Stations Phones Associations

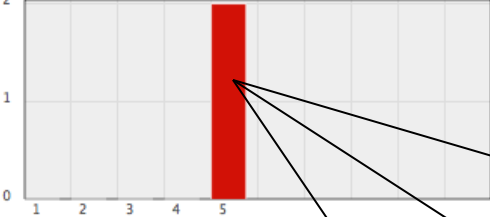
Wireless Radio

Wired [2] [0] [0] [0] [2] [0] [1] [1] [1] [0] [2] [3]

Alarms Dashboard [Graph Help]

Alarm Category

Total Alarms = 2



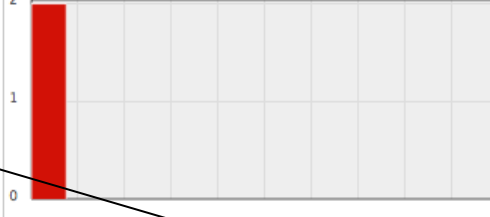
1: Controller Alarms
2: AP Alarms
3: Server Alarms
4: Wireless LAN Alarms
5: IDS Alarms

☒ Enable Auto Refresh

Auto refresh in : 43 secs

Alarm Severity

Total Alarms = 2



■ Critical
■ Major
■ Minor

Alarm Category Details << Prev (1 - 2 of 2) Next >>

Row #	Time	Alarm Type	Alarm Severity	Details
1	02/05/2010 22:45:31	Rogue AP Detected	Critical	CONTROLLER (1:2) ROGUE AP DETECTED. AP mac=00:1d:6a:cb:26:f1 bss=00:1d:6a:cb:26:f1 cch= 6 ess=rogue02 by AP AP-2 (2)
2	02/05/2010 22:45:31	Rogue AP Detected	Critical	CONTROLLER (1:3) ROGUE AP DETECTED. AP mac=00:1d:6a:cb:2d:0d bss=00:1d:6a:cb:2d:0d cch= 6 ess=rogue01 by AP AP-2 (2)

Close

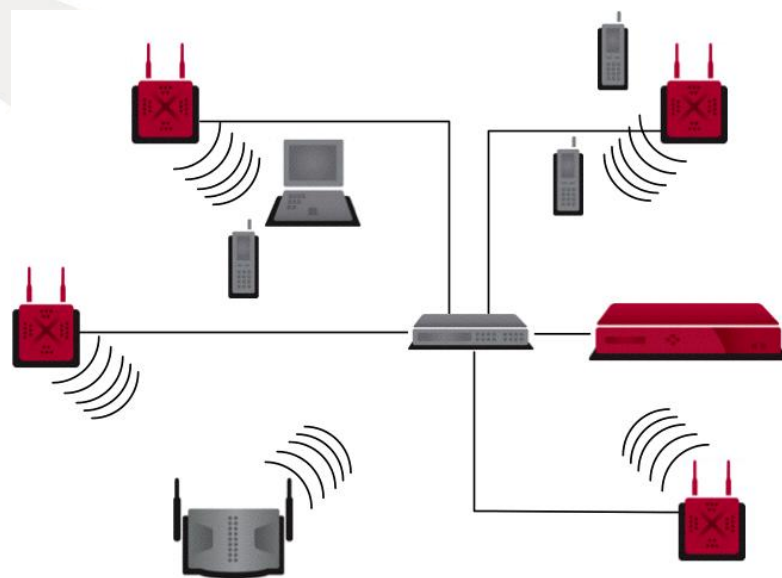
Rogue Detection

Operation

- > Radios with clients scans home channel
- > Radios without clients scan all (configured) channels
- > Radios can be dedicated to scanning
 - All channels, both bands

Detection Settings

- > Allowed APs are listed in an ACL by BSSID address
- > Each created ESSID will have a BSSID added
- > Two ACLs available:
 - Authorized
 - Blocked



Preventing Rogue Notification

WLAN Management User: admin Controller-192.168.17.15 2:49:00 PM CLI Save Help MCRU

Monitor
Maintenance
Configuration

System Config
Quick Start

Security
Profile
Radius
Captive Portal
Guest Users
Mac Filtering

Wireless IDS/IPS
Rogue APs
Air Shield
IDS

Wired
VLAN
GRE

Wireless
Radio
ESS

QoS
System Settings

Devices

Allowed APs (10 entries)

Global Settings Allowed APs Blocked APs

	BSSID
<input type="checkbox"/>	00:0c:e6:22:eb:bd
<input type="checkbox"/>	00:0c:e6:c1:00:9c
<input type="checkbox"/>	00:0c:e6:99:90:b9
<input type="checkbox"/>	00:0c:e6:55:5b:ec
<input type="checkbox"/>	00:0c:e6:a4:c6:f1
<input type="checkbox"/>	00:0c:e6:32:f5:11
<input type="checkbox"/>	00:0c:e6:41:ae:fb
<input type="checkbox"/>	00:0c:e6:99:a2:2b
<input type="checkbox"/>	00:0c:e6:d9:cc:a2
<input type="checkbox"/>	00:0c:e6:25:a0:ef

Refresh Add Delete

[2] [0] [0] [2] [0] [0] [1] [1] [1] [0] [2] [3] [02d:07h:55m:13s]

Allowed APs - Add

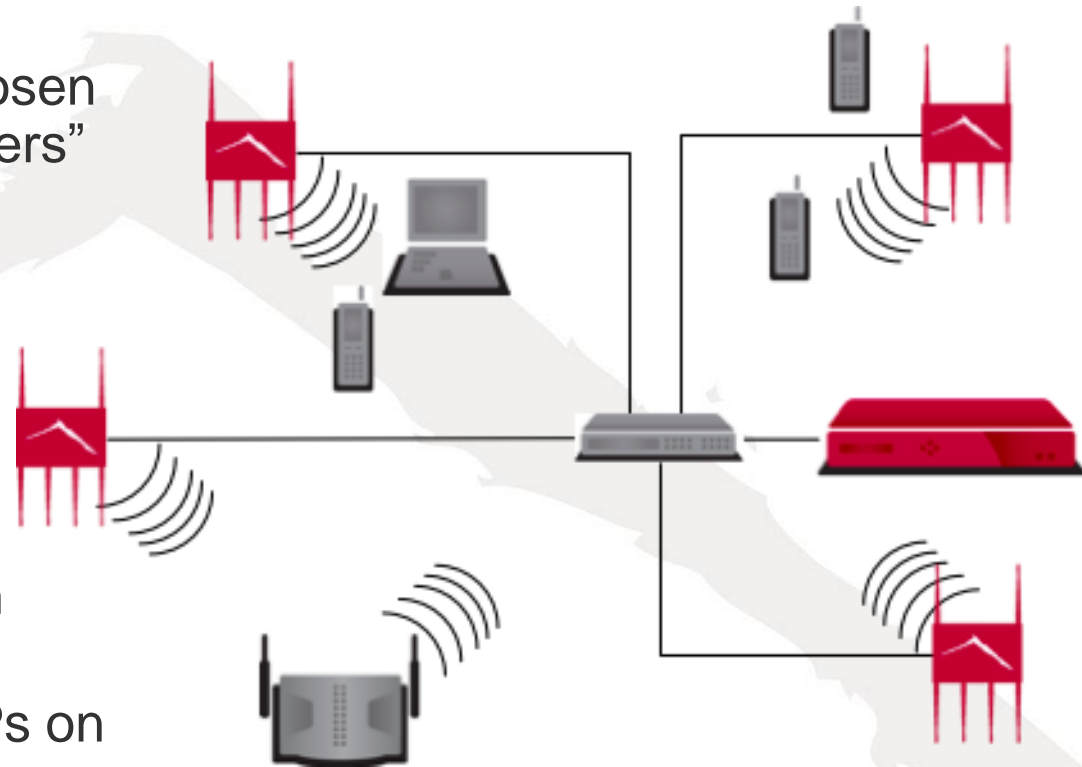
BSSID

Rogue Mitigation

- > Three nearby APs are chosen by controller as “rogue killers”
 - 3.6.1: AP200 only
 - 3.7: AP200 and AP300
 - 4.0: AP200 and AP300

Mitigation Settings

- > Mitigate all (all APs not on authorized list)
- > Mitigate selected (only APs on blocked list)



Inferences

- > Correlates system events to draw conclusions

The screenshot displays the Meru WLAN Management web interface. The top navigation bar includes the title 'WLAN Management', user 'admin', controller IP '192.168.17.15', time '4:41:10 PM', and links for 'CLI', 'Save', 'Help', and the Meru logo. A left sidebar menu lists various system components: Configuration, Maintenance, Monitor (expanded), Dashboard, System, Radio, Station, Voice, Alarms, Spectrum, Diagnostics (expanded), Radio, Station, Inferences (highlighted), Global Statistics, Security Counters, QoS Counters, Devices, All Stations, Phones, Associations, Wireless, Radio, Wired, and Ethernet. The main content area is titled 'Diagnostic Inferences' and shows 'Showing 1 - 2 of 2' events. The events are listed in a table with columns for Timestamp, MAC Address, Source, and Details.

Timestamp	MAC Address	Source	Details
2009-09-08 16:20:51.016	00:90:0b:0c:81:10	Controller	client <192.168.17.76 00:1b:2f:be:cb:37> on AP <00:0c:e6:03:7f:f2> is conflicted with other client <192.168.17.76 00:14:6c:83:ec:45> on AP <00:0c:e6:04:79:d5>.
2009-09-08 16:24:35.768	00:1b:2f:be:cb:37	Station	Inference Rule #8 matched : IP Address Update 17 times within 300 seconds. [IP 0.0.0.0] [unknown] [data] [AP-1 AP-1] [BSSID 00:0c:e6:5c:b0:9a] [ESSID stockholm] [Vlan Tag 0] [L2 State clear] [L3 State clear] [First Seen @ PDT Sep 8 13:20:49]

A 'Refresh' button is located at the bottom right of the interface.

Inference Engine

- > Essentially a bunch of counters that trigger an alert when thresholds are reached
- > Three Areas Tracked
 - Station, Controller, AP (AP300)
 - Turn on at installation (3.6.1)
- > Send to station log and/or syslog
- > Automated reporting available

E(z)RF Network Manager

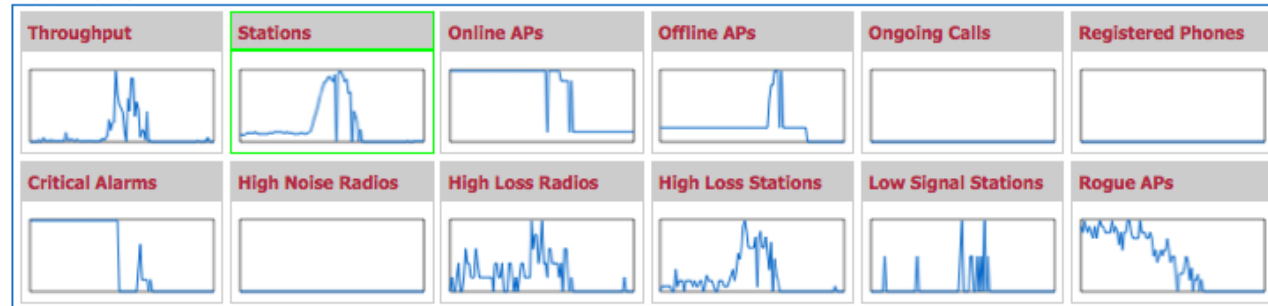
- ▶ Monitor
- ▶ Configuration
- ▶ Inventory
- ▶ Reports & Notify
- ▶ Visualization
- ▶ Administration
- ▼ Monitor
 - Global Dashboard
 - Distribution
 - Trend
 - Long Term Trend
 - Device Dashboard
 - Controller
 - AP
 - Station
 - Fault Dashboard
 - Alarms
 - Event Viewer
 - Tools
 - Search
 - Topology

Trend Dashboard

Trend Interval 48 Hours

☐ Enable Auto Refresh

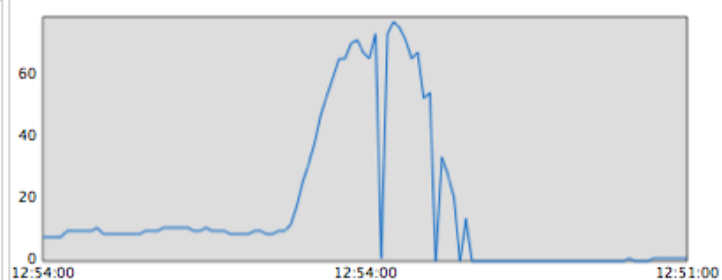
Global Trends



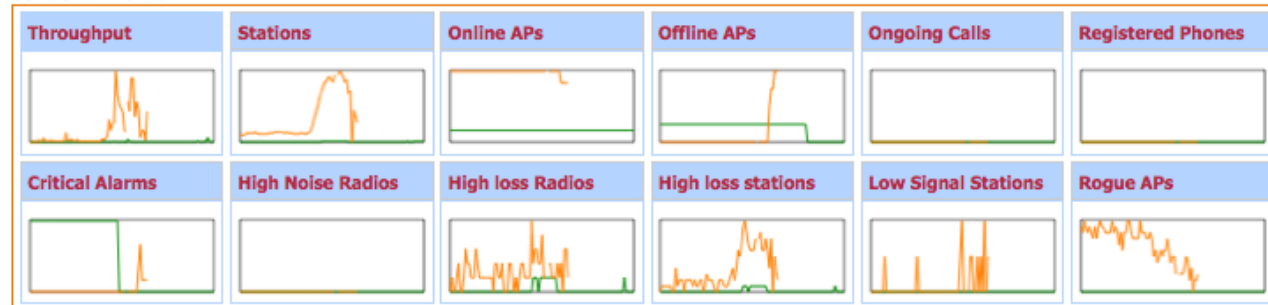
Problem Controllers

Name	IP Address	Summary
------	------------	---------

Stations Trend



Controller Trends



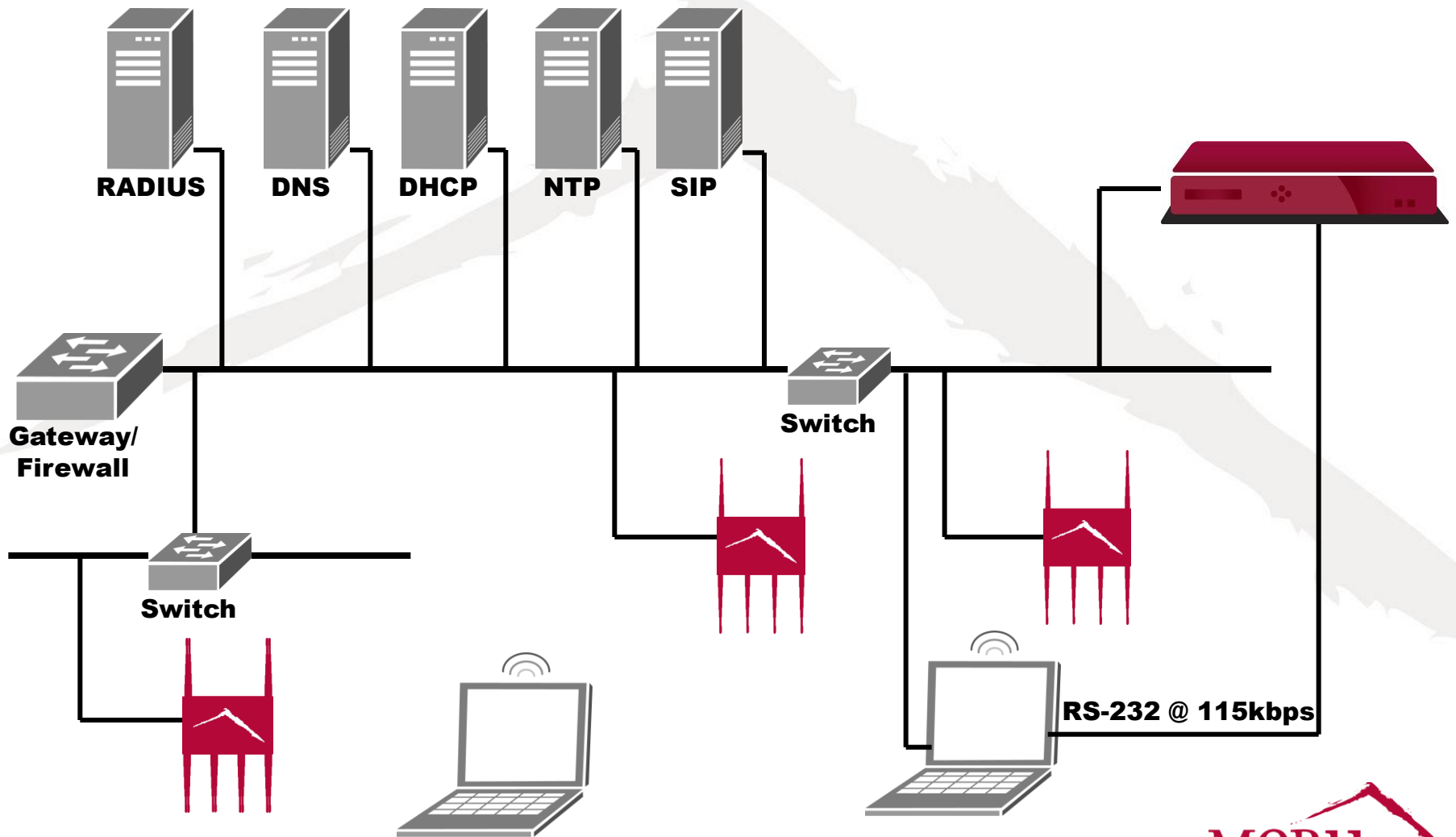
Refresh

- ▶ Network Manager
- ▶ Service Assurance
- ▶ Wireless IPS

Reactive Troubleshooting: Typical Complaints

- > I have a bad phone connection!
- > The network is slow!
 - YouTube looks bad
- > I can't connect!
 - At all
 - Connection drops

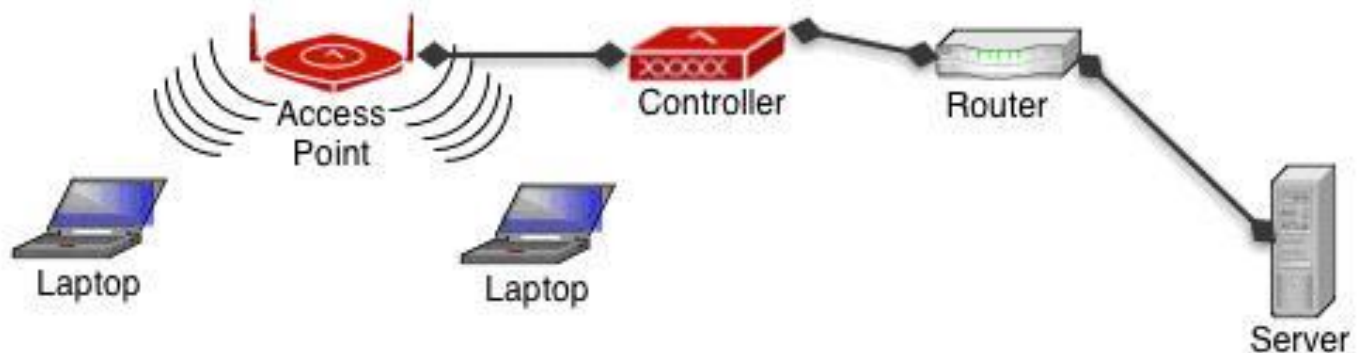
What are We Trying to Do?



What to Do When Things Go Wrong

> Ask:

- Has it worked before? What changed?
 - One client, several, or all?
 - One AP, several, or all (locations affected)?
 - Controller and APs contactable?
 - Stations observable?
-
- What is the MAC address of the affected client(s)?



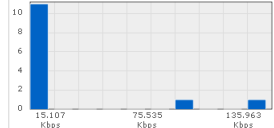
Bad Phone Call Problems

- > Generally, troubleshooting poor quality calls does not require admin access
 - Verify call is handled under QoS
 - QoS Counters
 - QoS Flows
 - Check Station Diagnostics
 - Signal strength
 - Retry
 - Loss

Diagnostics – Station

Stations Dashboard [Graph Help]

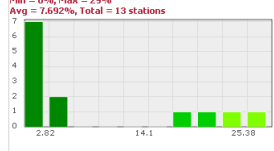
Station Throughput Distribution Advanced...



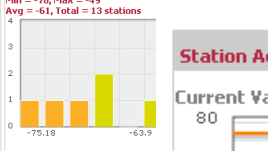
Airtime Utilization Distribution Advanced...



Loss Distribution Advanced...



Signal Strength Distribution Advanced...



☒ Enable Auto Refresh

Station Diagnostics

Stop Diagnostics

Station MAC Address	Station IP Address	SSID	AP ID	AP Name
00:1c:bf:03:e0:00	192.168.1.27	idaho-guest	1	AP-1

Station Activity Time Trend [Graph Help] [Error Log]

Auto refresh in: 25 secs

Current Value: Tx Thruput: 65.013 Kbps, Rx Thruput = 74.855 Kbps



Time (hh:mm:ss) ->

Current Value: Signal Strength = -24



Time (hh:mm:ss) ->

Current Value: Loss % = 24



Time (hh:mm:ss) ->

Current Value: Airtime Utilization % = 0



Time (hh:mm:ss) ->

Station Diagnostics [Events...] [Show Buffered Diagnostics...]

Refreshing. Please wait...

```

22:28:26.285940 | 00:1c:bf:03:e0:00 | DHCP | <msg_type=INFO><server_ip=255.255.255.255><se
22:28:26.286872 | 00:1c:bf:03:e0:00 | DHCP | <msg_type=INFO_ACK><server_ip=192.168.1.7><se
22:28:29.288279 | 00:1c:bf:03:e0:00 | DHCP | <msg_type=INFO><server_ip=255.255.255.255><se
22:28:29.289210 | 00:1c:bf:03:e0:00 | DHCP | <msg_type=INFO_ACK><server_ip=192.168.1.7><se
22:29:38.337590 | 00:1c:bf:03:e0:00 | DHCP | <msg_type=INFO><server_ip=255.255.255.255><se
22:29:38.338106 | 00:1c:bf:03:e0:00 | DHCP | <msg_type=INFO_ACK><server_ip=192.168.1.7><se
    
```

Station Buffered Diagnostics (Station Log)

Station Diagnostics Details

12:54:57.463520	00:14:6c:83:ec:45	Station Assign	<AID=1> assigned to <AP_ID=2><ESSID=stockholm1-guest><BSS
12:54:57.808539	00:14:6c:83:ec:45	802.11 State	state change <old=Unauthenticated><new=Authenticated><AP=
12:54:57.811248	00:14:6c:83:ec:45	802.11 State	state change <old=Authenticated><new=Associated><AP=00:0c
12:55:02.350609	00:14:6c:83:ec:45	DHCP	<msg_type=DISCOVER><server_ip=255.255.255.255><server_mac
12:55:03.101233	00:14:6c:83:ec:45	DHCP	<msg_type=OFFER><server_ip=192.168.20.2><server_mac=00:1b
12:55:03.103773	00:14:6c:83:ec:45	DHCP	<msg_type=REQUEST><server_ip=255.255.255.255><server_mac=
12:55:03.128625	00:14:6c:83:ec:45	IP Address Discovered	<Old IP discovery Method=none><Old IP=0.0.0.0><New IP disc
12:55:03.128630	00:14:6c:83:ec:45	DHCP	<msg_type=ACK><server_ip=192.168.20.2><server_mac=00:1b:2
12:55:22.472851	00:14:6c:83:ec:45	DHCP	<msg_type=INFO><server_ip=255.255.255.255><server_mac=ff:

Close

Station Diagnostics Events

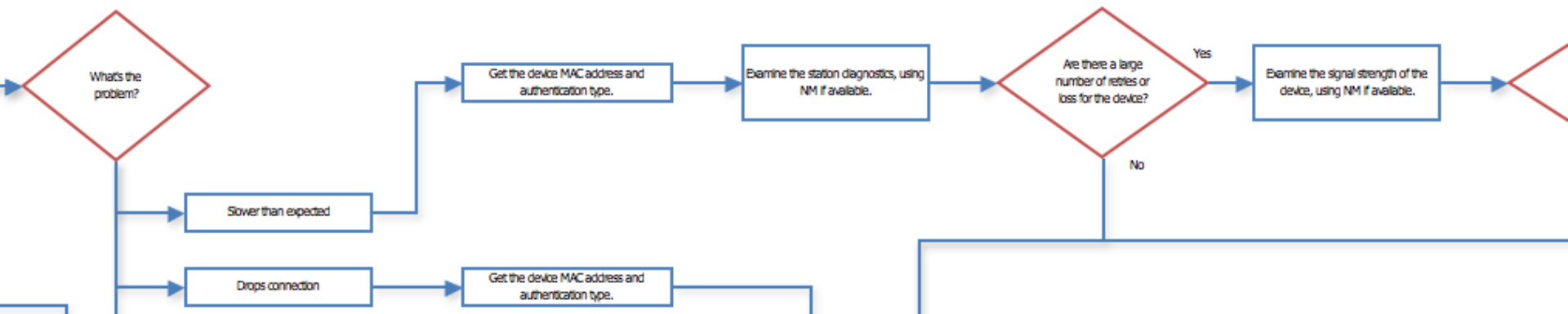
<input checked="" type="checkbox"/> IP Address Discovered	<input checked="" type="checkbox"/> DHCP Ack
<input checked="" type="checkbox"/> Station Assign	<input checked="" type="checkbox"/> 802.11 State
<input checked="" type="checkbox"/> CP User Authentication	<input checked="" type="checkbox"/> 1X Authentication
<input checked="" type="checkbox"/> Encryption	

Close

Slow Network Problems

> Generally, troubleshooting slow networks does not require admin access

- Check Station Dashboard
- Check Station Diagnostics
- Check AP Diagnostics
- Check number of clients

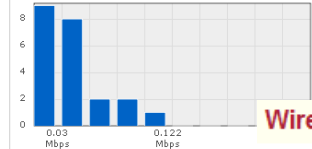


Diagnostics – Radio

Radio Dashboard [\[Graph Help \]](#)

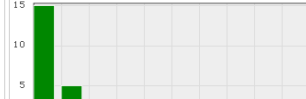
Throughput Distribution [Advanced...](#)

Min = 0.007 Mbps, Max = 0.238 Mbps
Avg = 0.047 Mbps, Total (Wireless Interfaces) = 23



Association Distribution [Advanced...](#)

Min = 0, Max = 3
Avg = 0.522, Total (Wireless Interfaces) = 23

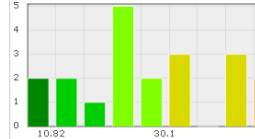


Wireless Interface Diagnostics

[Stop Diagnostics](#)

Loss Distribution

Min = 6%, Max = 55%
Avg = 30.304%, Total (Wireless Interfaces) = 2



☒ Enable Auto Refresh

AP ID	Interface ID	AP Name
2	1	AP-2

Wireless Interface Activity Trend [\[Graph Help \]](#)

Auto refresh in: 59 secs

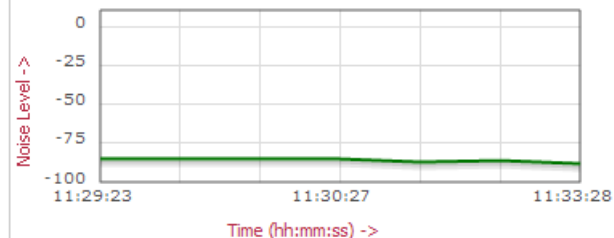
Current Value: **Throughput: 0.016 Mbps**



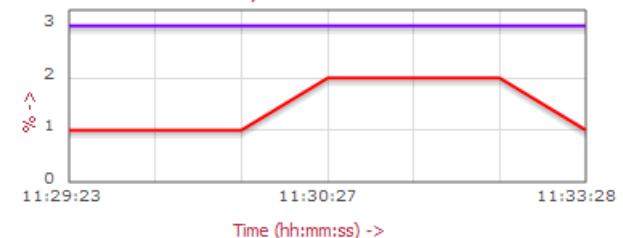
Current Value: **Associated Stations = 1**



Current Value: **Noise Level = -88**



Current Value: **Loss % = 1, Channel Utilization % = 3**



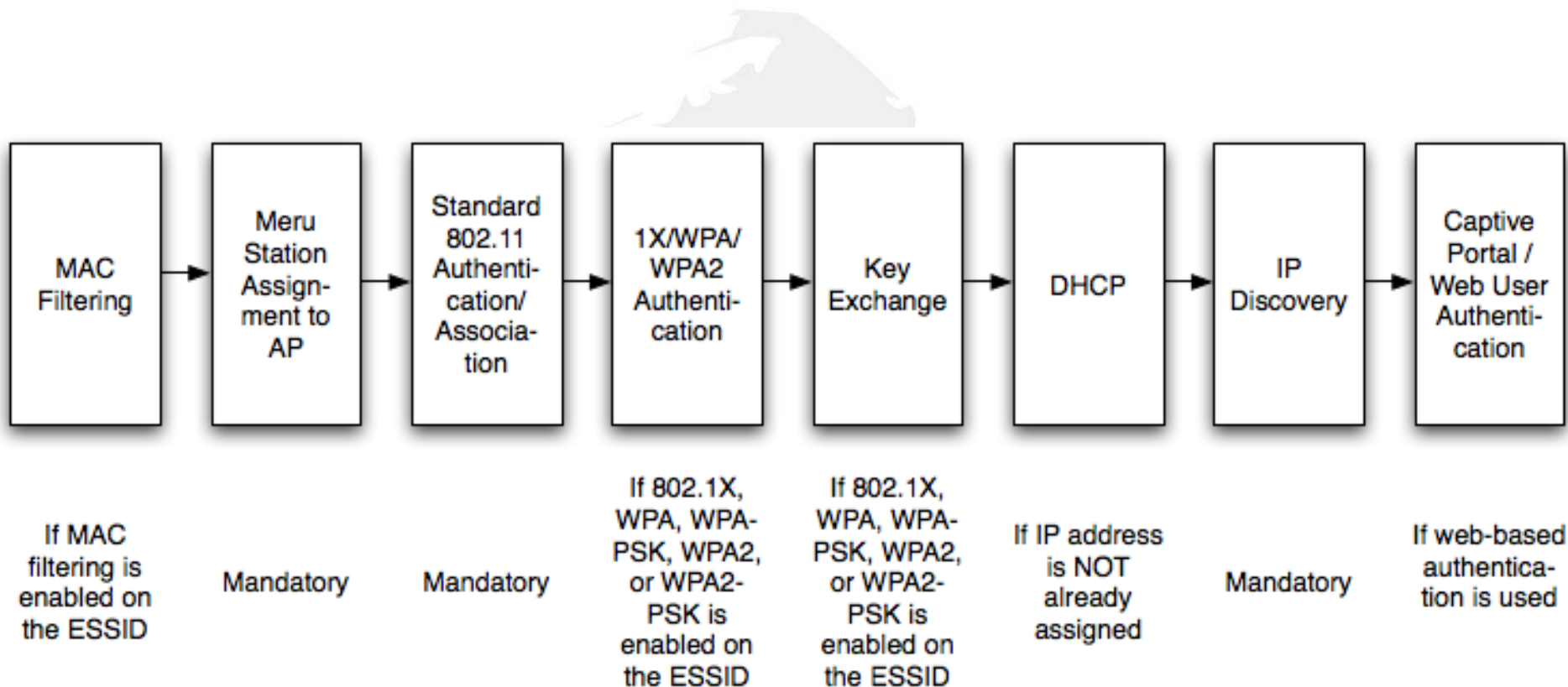
Connectivity Problems

> Generally, troubleshooting connectivity requires admin access

- Check Station Diagnostics*
 - Station Buffered Diagnostics
- Check Station Logs
 - Interactive
 - Historical
- Check Station Events* [E(z)RF Network Manager]
 - Historical
- Check Syslog* (for captive portal problems)
- Check Station Counters*
- Capture packets

* Does not require admin access

Stages of Connection



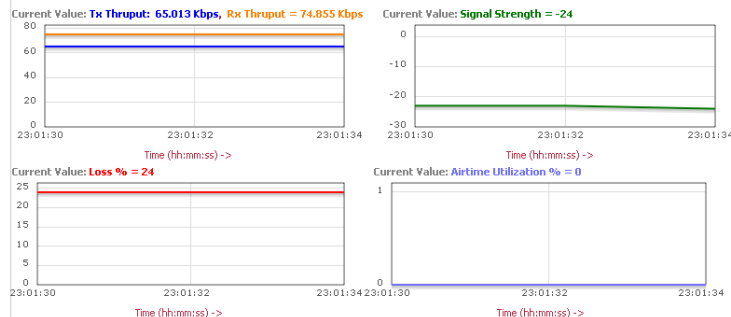
Station Logging

Station Diagnostics

Stop Diagnostics

Station MAC Address	Station IP Address	SSID	AP ID	AP Name
00:1c:bf:03:e0:00	192.168.1.27	idaho-guest	1	AP-1

Station Activity Time Trend [Graph Help] [Error Log] Auto refresh in: 25 secs



Station Diagnostics [Events...] [Show Buffered Diagnostics...] Retrefreshing, Please wait...

22:28:26.285940	00:1c:bf:03:e0:00	DHCP	<msg_type=INFO><server_ip=255.255.255.255><se
22:28:26.286872	00:1c:bf:03:e0:00	DHCP	<msg_type=INFO_ACK><server_ip=192.168.1.7><se
22:28:29.288279	00:1c:bf:03:e0:00	DHCP	<msg_type=INFO><server_ip=255.255.255.255><se
22:28:29.289210	00:1c:bf:03:e0:00	DHCP	<msg_type=INFO_ACK><server_ip=192.168.1.7><se
22:29:38.337590	00:1c:bf:03:e0:00	DHCP	<msg_type=INFO><server_ip=255.255.255.255><se
22:29:38.338100	00:1c:bf:03:e0:00	DHCP	<msg_type=INFO><server_ip=192.168.1.7><se

Station Diagnostics Details

```
12:54:57.463520 | 00:14:6c:83:ec:45 | Station Assign | <AID=1> assigned to <AP_ID=2><ESSID=stockholm1-guest><BSS
12:54:57.808539 | 00:14:6c:83:ec:45 | 802.11 State | state change <old=Unauthenticated><new=Authenticated><AP=
12:54:57.811248 | 00:14:6c:83:ec:45 | 802.11 State | state change <old=Authenticated><new=Associated><AP=00:0c
12:55:02.350609 | 00:14:6c:83:ec:45 | DHCP | <msg_type=DISCOVER><server_ip=255.255.255.255><server_mac
12:55:03.101233 | 00:14:6c:83:ec:45 | DHCP | <msg_type=OFFER><server_ip=192.168.20.2><server_mac=00:1b
12:55:03.103773 | 00:14:6c:83:ec:45 | DHCP | <msg_type=REQUEST><server_ip=255.255.255.255><server_mac=
12:55:03.128625 | 00:14:6c:83:ec:45 | IP Address Discovered | <Old IP discovery Method=none><Old IP=0.0.0.0><New IP disc
12:55:03.128630 | 00:14:6c:83:ec:45 | DHCP | <msg_type=ACK><server_ip=192.168.20.2><server_mac=00:1b:2
12:55:22.472851 | 00:14:6c:83:ec:45 | DHCP | <msg_type=INFO><server_ip=255.255.255.255><server_mac=ff:
```

Close

Interactive Station Logging

> Used to track stations

```
riga# station-log
Interactive Per-Station Event Logging Shell (enter "help" for help)
station-log> ?
```

Interactive Event Logging Shell Usage:

```
help, ?
exit, quit
```

This help message
Exit/Quit

```
station show
station add <AA:BB:CC:DD:EE:FF>
station del <AA:BB:CC:DD:EE:FF>
station del <#>
station del all
```

Show stations in the filter list
Add a station to the filter list by MAC
Delete a station from the filter list by MAC
Delete a station from the filter list by index
Delete all stations from the filter list

```
event show
event <event> <dispcnd>
```

Show the event filter list
Set the display condition for event <event>
<event> may be: #ID of event, or "all"
<dispcnd> may be: "all" (!), "none" (x) or "list" (?)

```
station-log>
```

Historical Station Logging

- > Used to track stations in the past
- > Same as buffered diagnostics

station-log show

-mac=rr:ss:tt:uu:vv:yy
-since=xxx

```
riga# station-log show -mac=00:14:6c:83:ec:45
2009-11-12 12:22:04.241 | 00:14:6c:83:ec:45 | Station Assign | <AID=1> assigned to <AP_ID=2>
2009-11-12 12:22:05.817 | 00:14:6c:83:ec:45 | 802.11 State | state change <old=Unauthentic
2009-11-12 12:22:05.821 | 00:14:6c:83:ec:45 | 802.11 State | state change <old=Authenticat
2009-11-12 12:22:07.549 | 00:14:6c:83:ec:45 | DHCP | <msg_type=DISCOVER><server_ip=
2009-11-12 12:22:08.041 | 00:14:6c:83:ec:45 | DHCP | <msg_type=OFFER><server_ip=19
2009-11-12 12:22:08.045 | 00:14:6c:83:ec:45 | DHCP | <msg_type=REQUEST><server_ip=
2009-11-12 12:22:08.050 | 00:14:6c:83:ec:45 | IP Address Discovered | <Old IP discovery Method=none
2009-11-12 12:22:08.051 | 00:14:6c:83:ec:45 | DHCP | <msg_type=ACK><server_ip=192.
```

Syslog Diagnostics

- > Enable Security logging on the Security Profile of interest
 - Syslog shows Captive Portal messages not seen elsewhere

SysLog Files Table (8 entries)

	Facility Name	Last Accessed	Size(KB)	#Lines	Last Record
<input type="checkbox"/>	Security	10/17/2010 04:00:46	37	208	Controller Access User philippe@192.168.0.171 login to controller at time Sun Oct 17 04:00:46 2010 is OK
<input type="checkbox"/>	QoS	10/17/2010 02:46:31	1	0	
<input type="checkbox"/>	System WNC	10/17/2010 03:42:26	4	9	Station Info Update : MacAddress : 00:14:6c:88:c2:b9, UserName : , AP-Id : 1, AP-Name : AP-1, BSSID : 00:0c:e6:a5:9d:64, ESSID : helsinki-voice, Ip-Type : dynamic dhcp, Ip-Address : 192.168.12.99, L2mode : wep, L3-mode : clear, Vlan-Name : vln-voice, Vlan-Tag : 12
<input type="checkbox"/>	NMS	10/17/2010 02:46:31	1	0	
<input type="checkbox"/>	Mobility	10/17/2010 02:46:31	1	0	
<input type="checkbox"/>	Bulk Update	10/17/2010 02:46:31	1	0	
<input checked="" type="checkbox"/>	Upgrade	10/17/2010 02:41:46	5	40	Upgrade complete Meru rpms installed:
<input type="checkbox"/>	Per User Firewall	10/17/2010 02:46:31	1	0	

Syslog facility: Upgrade (40 entries)

Line	Priority	Mnemonic	Time	Record
	debug			
1	info	UPG	10/17/2010 02:36:02	Upgrade AP(s) to 4.0-105
2	info	UPG	10/17/2010 02:36:02	Upgrade AP 1 START
3	info	UPG	10/17/2010 02:36:02	Upgrade AP 2 START
4	info	UPG	10/17/2010 02:36:02	Upgrade AP 1 Upgrade Requested
5	info	UPG	10/17/2010 02:36:02	Upgrade AP 2 Upgrade Requested
6	info	UPG	10/17/2010 02:36:03	Upgrade AP 1 Reading File
7	info	UPG	10/17/2010 02:36:03	Upgrade AP 2 Reading File
8	info	UPG	10/17/2010 02:36:33	Upgrade AP 1 Erasing Flash
9	info	UPG	10/17/2010 02:36:33	Upgrade AP 2 Erasing Flash

Refresh Seek/Refresh Stop

Refresh View SysLog

Syslog access is also available in the CLI

Station Counters

> show station

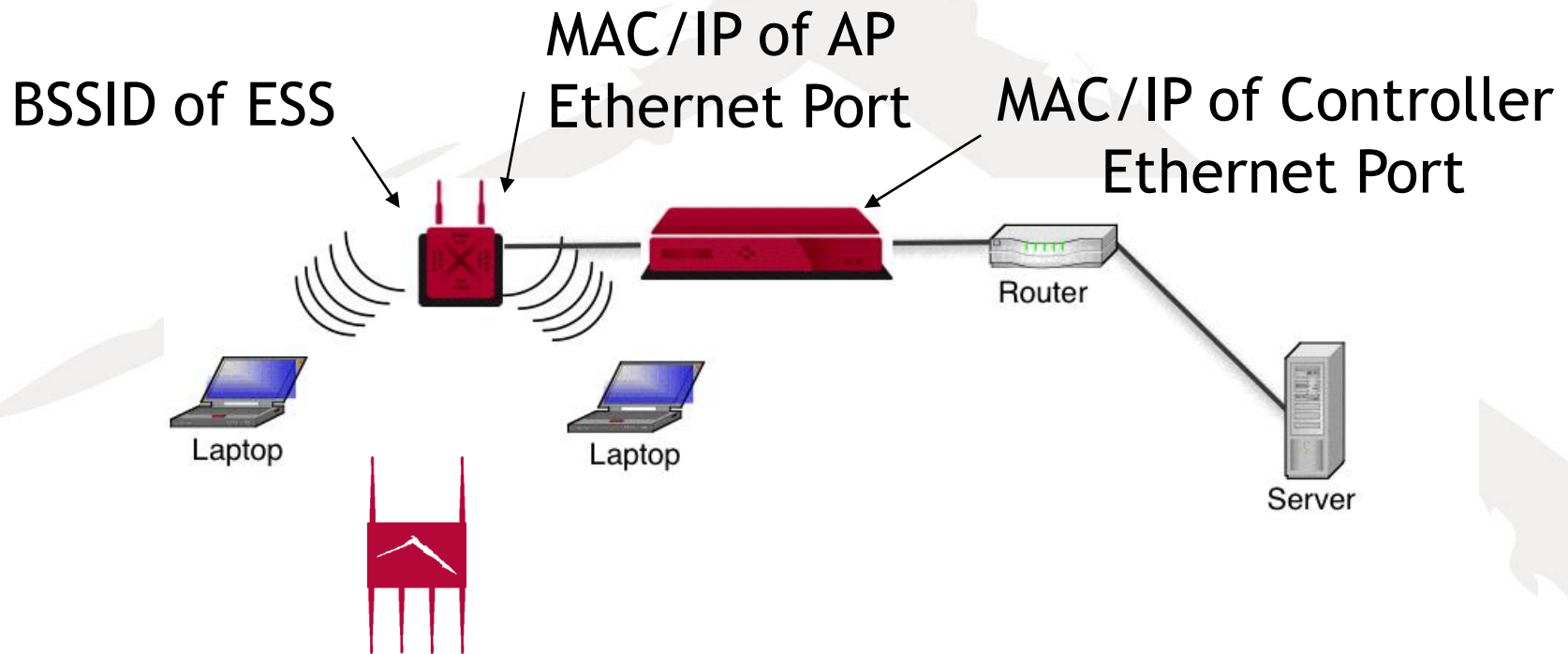
- **general** [mac-address XX:XX:XX:XX:XX:XX]
- **all** [mac-address XX:XX:XX:XX:XX:XX]
- **details** mac-address XX:XX:XX:XX:XX:XX
- **details** ip-address XXX.XXX.XXX.XXX
- **802.11** [mac-address XX:XX:XX:XX:XX:XX]
- **counter** [mac-address XX:XX:XX:XX:XX:XX]
- **network** [mac-address XX:XX:XX:XX:XX:XX]
- **security** [mac-address XX:XX:XX:XX:XX:XX]

```
riga# show station counter
```

MAC Address	MACFilterCnt	IPDiscCnt	Asso.Cnt	SoftHOCnt	PwrSavingTrCnt	KeyExCnt	RadiusAuthCnt	CPGuestUserCnt	Pkts Tx	Pkts Rx	TxByteCnt	RxByteCnt
00:14:6c:83:ec:45 0	23	5	1	0	0	0	0	0	8927	633	538301	101775

Station Database Counter Table(1 entry)

Where to Capture Packets



Capturing Packets on the Controller

> From the Controller

- Use the `capture-packets` command
`name# capture-packets`
- Use `-w` to save a capture (must be last option)
`name# capture-packets -w filename`

> From APs (AP200/300/1000i only)

- Use the `-i` option of the `capture-packets` command.
`name# capture-packets -i ap_num`

> To stop real-time packet capture, press Ctrl-C

> Move captured files to laptop and use Wireshark to filter

```
name# cd capture
name# copy filename ftp://user@ip_address/
name# cd images
```


Filtering Packets

- > The built-in Ethereal sniffer lets you filter packets.
- > Syntax:
 - `-R primitive[[equivalence value]`
 - No spaces are allowed in filter specification
 - Equivalences are: `==` (equal to), `!=` (not equal to)
- > Capture only SIP packets from AP 1:
 - `name# capture-packets -i 1 -R sip`
- > Capture traffic from an IP address:
 - `name# capture-packets -R ip.addr==192.168.10.50`
- > For more complex filtering, capture files to laptop and use Wireshark
 - ◆ `name# capture-packets -i 47 -R wlan.addr==00:1e:52:72:67:95`

Wireshark

AirPcap USB wireless capture adapter nr. 00 - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

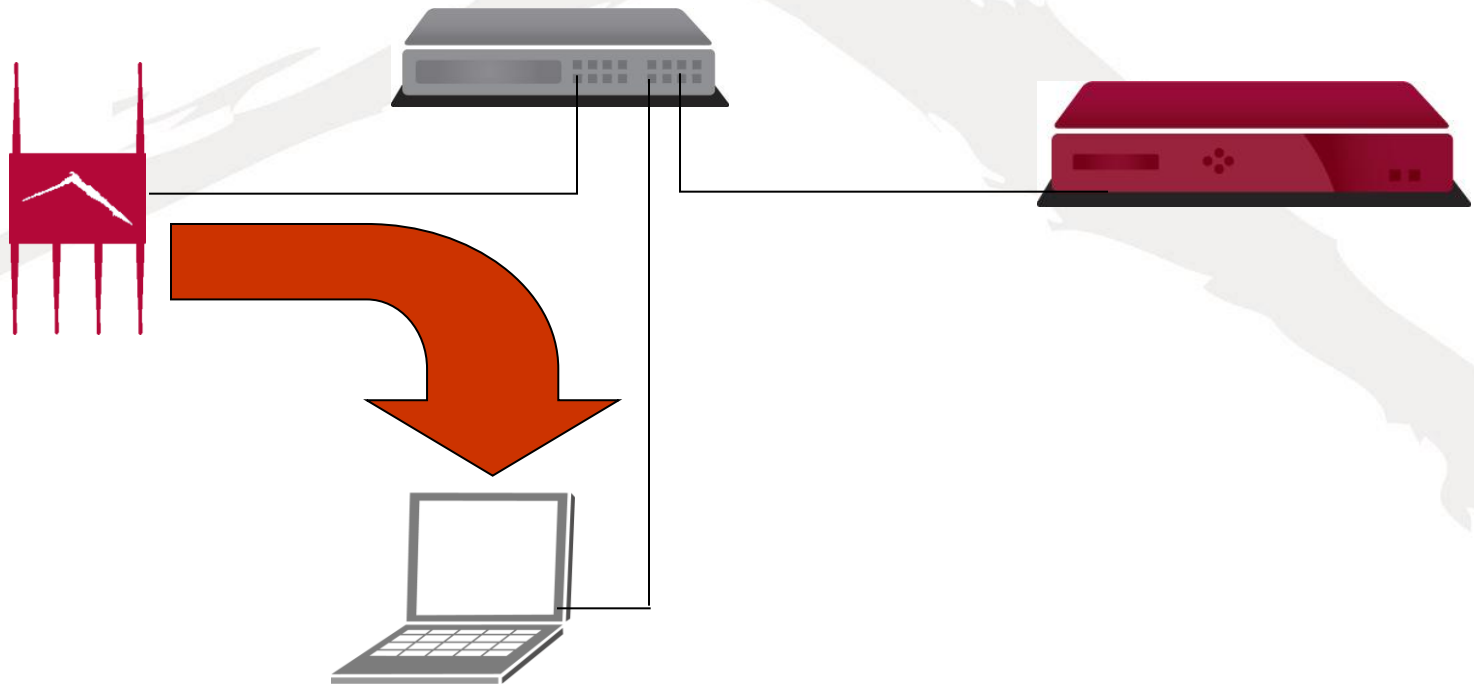
No.	Time	Source	Destination	Protocol	Info
550	4.680666	AlphaNet_cb:26:f1	Intel_80:3a:f3	IEEE 802	Probe Response, SN=415, FN=0, Flags=..
551	4.681290	06:06:10:b5:31:99	Netgear_b5:31:99	IEEE 802	Probe Response, SN=3249, FN=0, Flags=
552	4.681427	06:06:10:b5:31:99	06:06:10:b5:31:99 (RA	IEEE 802	Acknowledgement, Flags=.....C
553	4.681664	0a:06:03:be:cb:37	Broadcast	IEEE 802	Beacon frame, SN=3696, FN=0, Flags=..
554	4.681915	06:06:10:b5:31:99	Netgear_b5:31:99	IEEE 802	Probe Response, SN=3250, FN=0, Flags=
555	4.682165	06:06:10:b5:31:99	06:06:10:b5:31:99 (RA	IEEE 802	Acknowledgement, Flags=.....C
556	4.683915	AlphaNet_cb:26:f1	Broadcast	IEEE 802	Beacon frame, SN=416, FN=0, Flags=...
557	4.684291	06:06:10:b5:31:99	Netgear_b5:31:99	IEEE 802	Probe Response, SN=3251, FN=0, Flags=
558	4.684541	06:06:10:b5:31:99	06:06:10:b5:31:99 (RA	IEEE 802	Acknowledgement, Flags=.....C
559	4.710793	AlphaNet_cb:2d:0d	Broadcast	IEEE 802	Beacon frame, SN=1841, FN=0, Flags=..
560	4.736916	06:06:10:b5:31:99	Broadcast	IEEE 802	Beacon frame, SN=1560, FN=0, Flags=..
561	4.772169	Netgear_b5:31:99	Broadcast	IEEE 802	Probe Request, SN=2263, FN=0, Flags=.
562	4.775288	AlphaNet_cb:2d:0d	Netgear_b5:31:99	IEEE 802	Probe Response, SN=1842, FN=0, Flags=
563	4.777320	AlphaNet_cb:2d:0d	Netgear_b5:31:99	IEEE 802	Probe Response, SN=1842, FN=0, Flags=
564	4.777540	AlphaNet_cb:a5:29	AlphaNet_cb:a5:29 (RA	IEEE 802	Acknowledgement, Flags=.....
565	4.778318	Netgear_be:cb:37	Broadcast	IEEE 802	Probe Request, SN=2328, FN=0, Flags=.
566	4.780291	AlphaNet_cb:26:f1	Netgear_b5:31:99	IEEE 802	Probe Response, SN=417, FN=0, Flags=.

Frame 1 (150 bytes on wire, 150 bytes captured)
Radiotap Header v0, Length 28
IEEE 802.11 Beacon frame, Flags:C
IEEE 802.11 wireless LAN management frame

0000 00 00 1c 00 ef 18 00 00 ad 28 b4 01 93 01 00 00C.....
0010 10 02 85 09 a0 00 ae 97 66 00 00 17 80 00 00 00f.....
0020 ff ff ff ff ff ff 00 1d 6a cb 2d 0d 00 01 d6 cbj.....j.
0030 2d 0d e0 6e 81 61 4d 98 74 09 00 00 64 00 31 04 ...n.am. t...d.i.
0040 00 07 72 6f 67 75 65 30 31 01 08 82 84 8b 96 0c ...rogue0 1.....
0050 12 18 24 02 01 06 05 04 00 01 00 00 23 01 00 20w..o

File: "C:\DOCUMENTS~1\User01\LOCALS~1\Temp\... Packets: 1876 Displayed: 1876 Marked: 0 Dropped: 0 Profile: Default

Capturing Packets Directly from APs



Capturing 802.11 Frames Directly from APs

- > Synchronize clocks with Controller and Wireshark PC
- > Create a `sniff` profile
 - Point to Wireshark PC's IP address
 - Specify index number(s) of L3-connected APs
 - L2 mode also available
 - Set truncation length to 0
 - Enable `sniff`
- > Set up and activate Wireshark
 - Set up Capture Options...
 - Filter on incoming port
- > When you're done, disable `sniff` profile

If You Need to Call Support

Have a problem description ready:

- > Devices affected
- > To which specific devices it happens
 - MAC address of devices for connectivity problems
- > When / under what conditions it happens
- > If it worked previously, what recent changes occurred
- > What you've tried up to this point

diagnostics-controller **Command**

- > “diagnostics-controller” command captures *controller* state into file
- > When you need to capture the *entire* system state, use the command “diagnostics”
 - Takes snapshot of system state
 - Essential for reporting problems
 - Does not affect operation
 - Need to copy off the controller

Lab Preview

- > Create and examine alarms
 - > Trigger and examine inferences
 - > Examine the syslog
 - > Examine station logs
 - > Examine station counters
-
- > Capture and examine packets
 - SIP
 - RADIUS

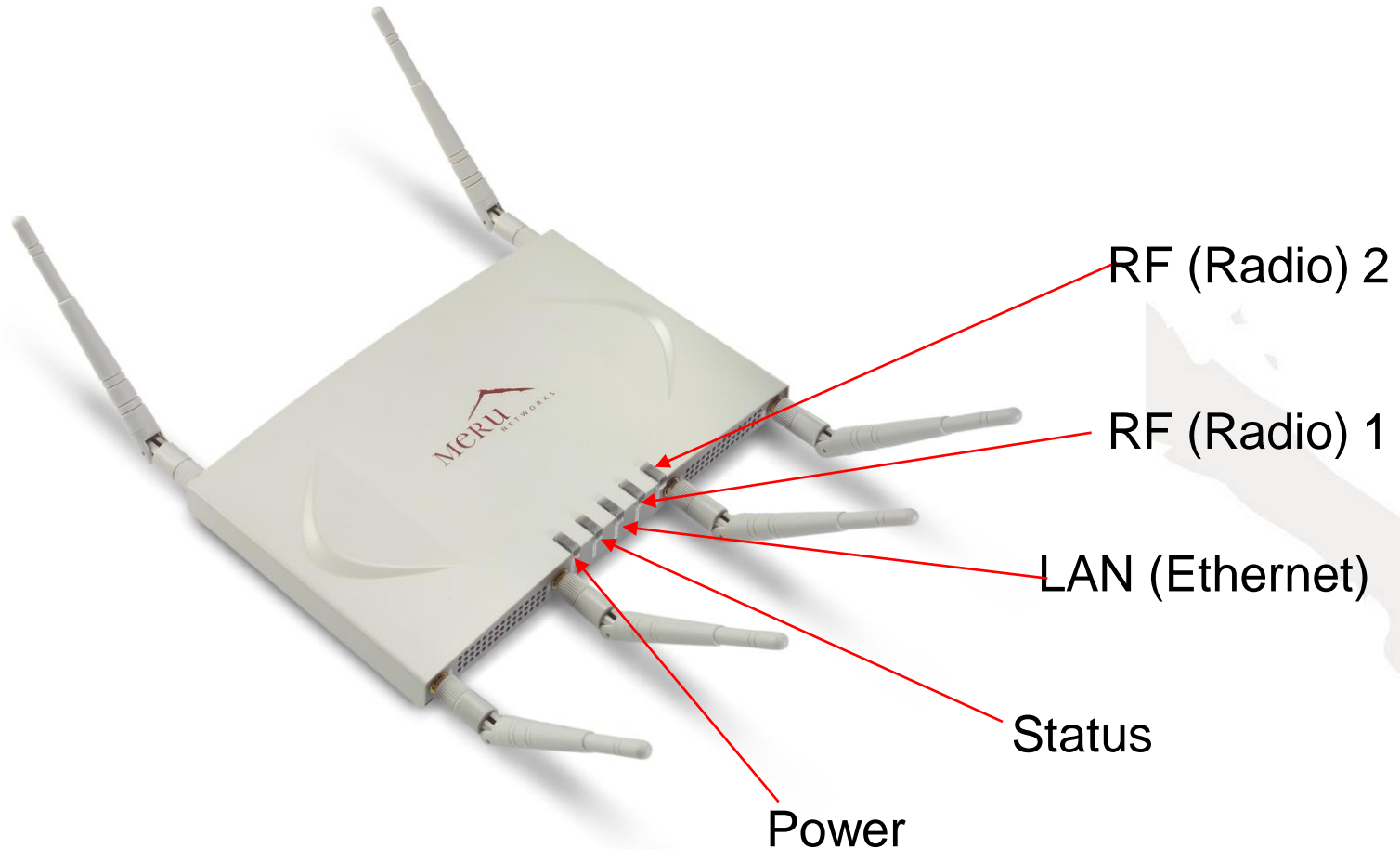
Sample Symptom List:

Captive Portal Clients Cannot Authenticate

- > Local vs. Remote setting for auth incorrect
 - > Controller IP not added to RADIUS client list
 - > User was not given remote access permissions in dial-in settings, or secret is mismatched
 - > Max connections per username has been exceeded (either on server or in captive portal settings on controller)
 - > Incorrect binding of radius profile to ssl server
-
- ◆ Ping RADIUS server from controller
 - ◆ Examine 802.1x events on controller, see if RADIUS request/response is happening correctly
 - ◆ If there are multiple logins under same name/passwd, try using a different username/passwd to validate either connection bound exceeded or leakage

Sample Hardware Reference: Access Point

300 LEDs



Sample Hardware Reference:

AP 300 LEDs

LED	Interpretation
Power	off—no power green—presence of power
Status	off—no power green—booting stage 1 blinking green and off—booting stage 2 blinking green and white—discovering the controller blinking green and blue—downloading a configuration from the controller blinking blue and off—AP is online and enabled, working state blinking red and yellow—failure; consult controller for alarm state
LAN	off—no power, or no link green—link status OK (at any speed) green/blinking—activity (at any speed) red—auto negotiation failure
Radio 1 Radio 2	off—no radio present green—radio enabled green blinking—data activity yellow—disabled or in scanning mode red—failure