TEST PLAN

IxChariot - IxWLAN Setup Guide

IxChariot

Contents

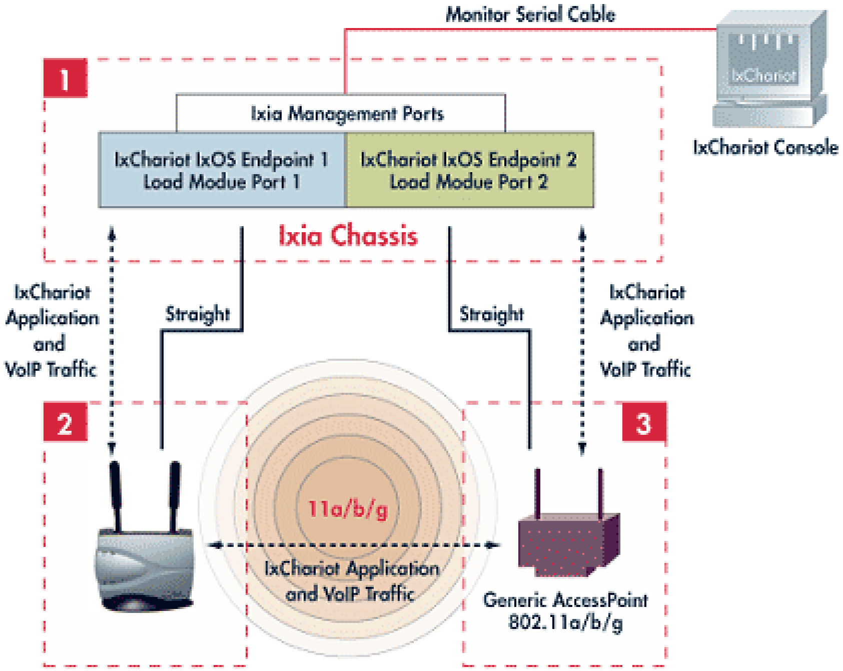
IXIA
26601 West Agoura Road, Calabasas, CA 91302
(877) FOR-IXIA

This Test Plan Primer contains a general outline for testing a particular technology. Not all the capabilities of Ixia technology have been exposed in this document. Please feel free to contact us if additional capabilities are required.

IxChariot–IxWLAN Setup Guide

The following test scenario describes the integration and configuration of IxChariot and the IxWLAN device. In an open air 802.11 environment, there are a large number of factors that may impact your tests, including antenna design, scattering, interference, etc., which need to be kept in mind when benchmarking different devices and networks. In addition, the 802.11 standard defines various physical layer rates that are important when evaluating results. Due to the characteristics of 802.11 (e.g., additional data in packets such as preambles, headers), the maximum performance is always less than link-layer throughput.

Please note that some of these settings may differ in your environment.


Monitor Serial Cable
1
Ixia Management Ports
IxChariot IxOS Endpoint 1
Load Modue Port 1
IxChariot IxOS Endpoint 2
Load Modue Port 2
Ixia Chassis
IxChariot
IxChariot Console
IxChariot Application and VoIP Traffic
Straight
Straight
IxChariot Application and VoIP Traffic
2
3
11a/b/g
IxChariot Application and VoIP Traffic
Generic AccessPoint 802.11a/b/g

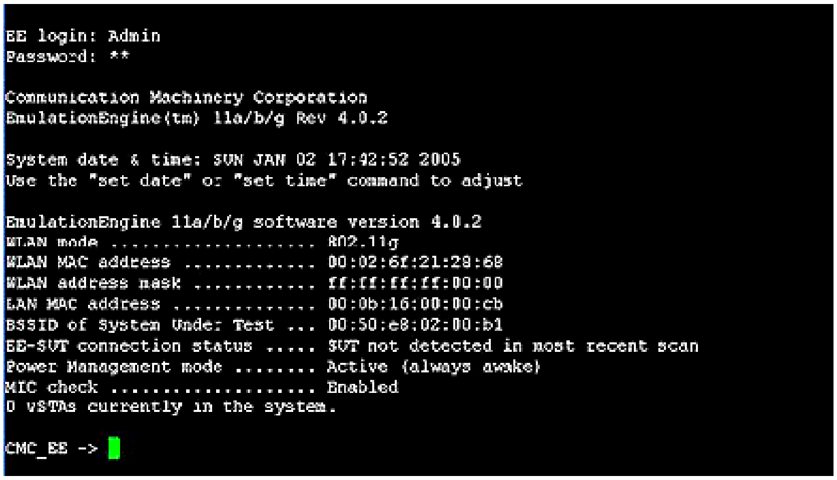
1. IxWLAN Configuration

The basic configuration of an IxWLAN device can be split into three steps:

- Defining the IP addressing of the IxWLAN device
- Creating a Scenario incorporates the definition of the virtual station (vSTA) and traffic source (external, L2)
- Selecting the System Under Test (SUT) and joining it.

The detailed steps to setup the IxWLAN device for a no encryption/open system test can be found below:

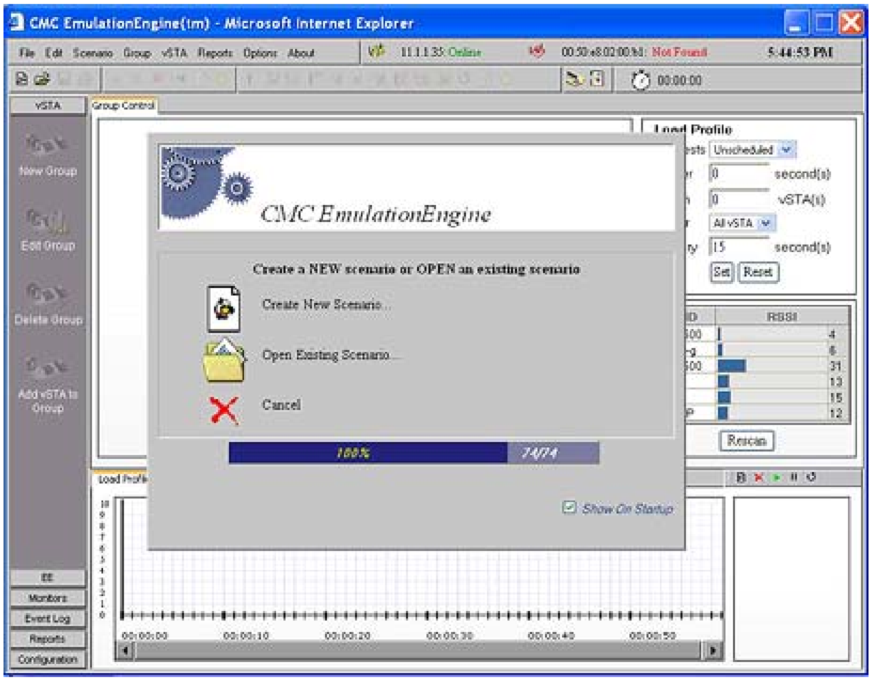
1. Open a Serial Connection to the IxWLAN device (9600, 8, N, 1, no). Alternatively, you can also telnet into the device using the default IP address (192.168.0.50).



```
EE login: Admin
Password: **

Communication Machinery Corporation
EmulationEngine(tm) 11a/b/g Rev 4.0.2

System date & time: SUN JAN 02 17:42:52 2005
Use the "set date" or "set time" command to adjust

EmulationEngine 11a/b/g software version 4.0.2
WLAN mode ..................... 802.11g
WLAN MAC address .............. 00:02:6f:21:28:68
WLAN address mask ............. ff:ff:ff:ff:00:00
LAN MAC address ............... 00:0b:16:00:00:cb
BSSID of System Under Test ... 00:50:e8:02:00:b1
EE-SUT connection status ..... SUT not detected in most recent scan
Power Management mode ........ Active (always awake)
MIC check .................... Enabled
0 vSTAs currently in the system.

CMC_EE -> 
```

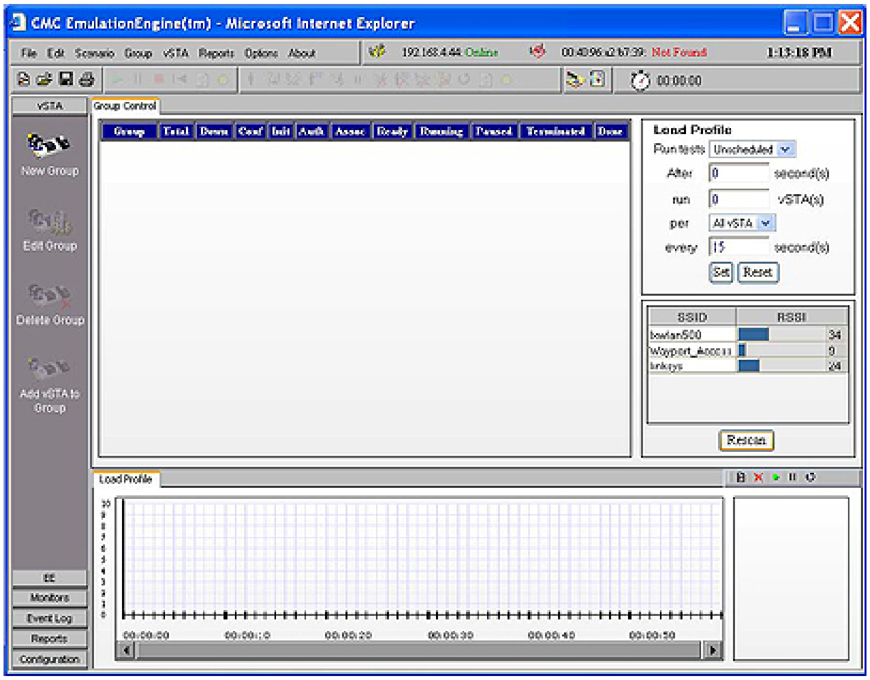
2. Login using "Admin" and "EE" as password (case sensitive). Please change your password to "IxWLAN" if you are running release 5.0 and above.
3. Set the IP address of the wired Ethernet port to the one you want to use. For example: set ippaddr 11.1.1.35.
4. Reboot the device by entering the Reboot command.

5. Access the browser interface of the IXWLAN device by connecting to the IP address of the wired Ethernet interface. Please note that your host needs to be on the same subnet as the IxWLAN. You must use Internet Explorer and change the settings to access temporary pages (Tools->Internet options->Temporary Internet Files-> Settings->Check for newer version of stored pages->Every time you visit the page)

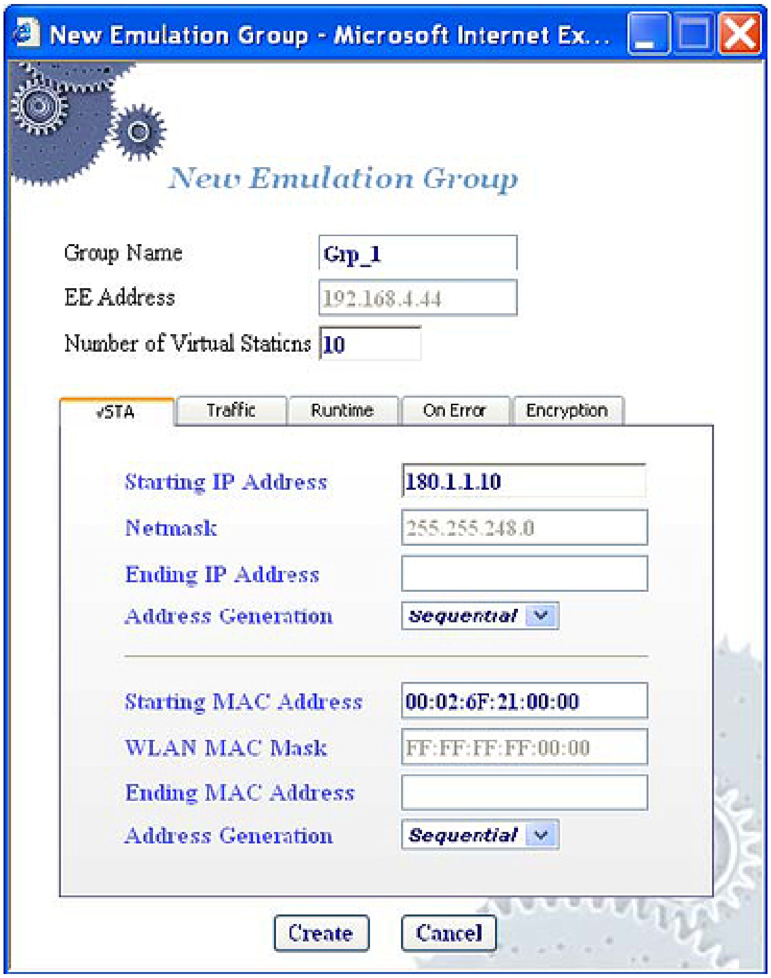


Create a NEW scenario or OPEN an existing scenario

6. Press the Create New Scenario icon.



7. Press the New Group icon and define the number and IP range for the vSTAs in the vSTA tab. Do not change the MAC address.

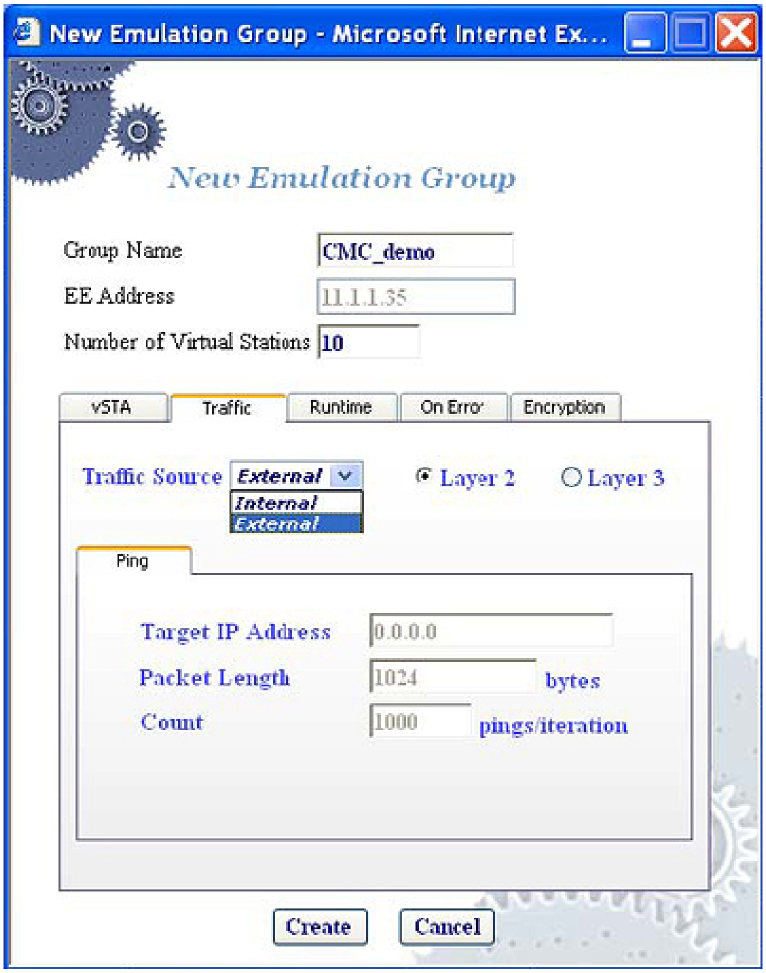


Group Name: Grp_1
EE Address: 192.168.4.44
Number of Virtual Stations: 10

Starting IP Address: 180.1.1.10
Netmask: 255.255.248.0
Ending IP Address:
Address Generation: Sequential

Starting MAC Address: 00:02:6F:21:00:00
WLAN MAC Mask: FF:FF:FF:FF:00:00
Ending MAC Address:
Address Generation: Sequential

8. Press the Traffic tab and set it to External and Layer 2.



Group Name: CMC_demo

EE Address: 11.1.1.35

Number of Virtual Stations: 10

Traffic Source: External

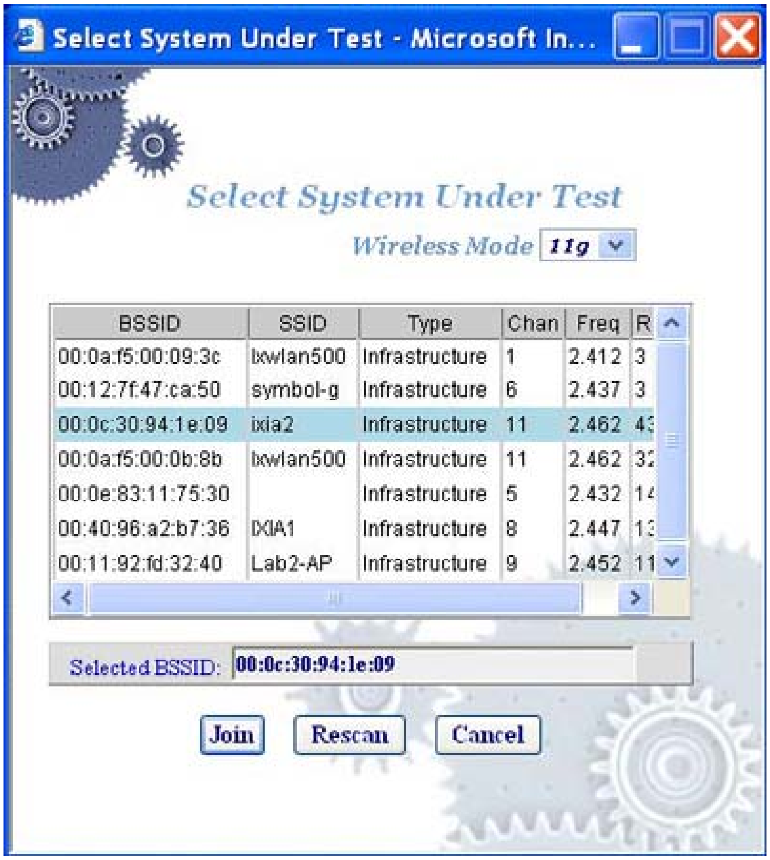
● Layer 2 ○ Layer 3

Target IP Address: 0.0.0.0

Packet Length: 1024 bytes

Count: 1000 pings/iteration

9. Press the SUT icon in the top toolbar to select the Access Point to be tested. Select the Access Point by BSSID and press the **Join** button. Press **Rescan** if you do not see your Access Point.



Select System Under Test - Microsoft In...

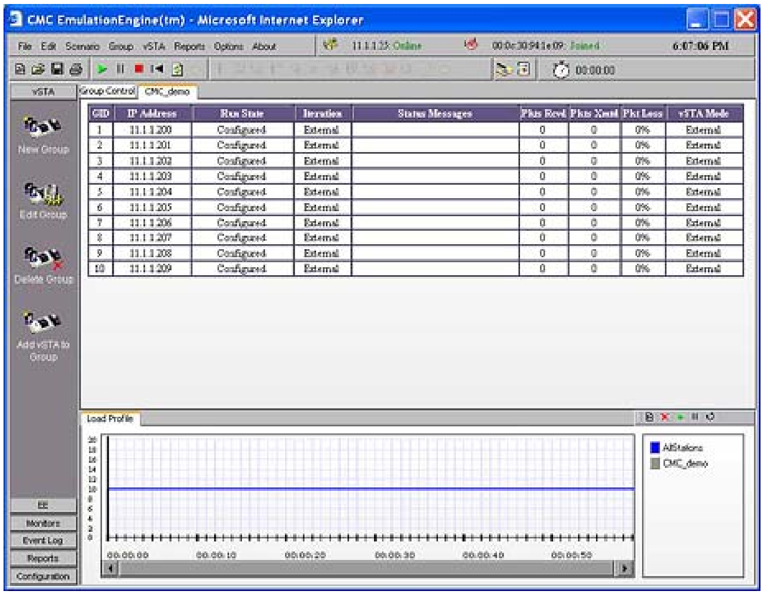
Select System Under Test

Wireless Mode 11g

BSSID	SSID	Type	Chan	Freq	R
00:0a:f5:00:09:3c	lxwlan500	Infrastructure	1	2.412	3
00:12:7f:47:ca:50	symbol-g	Infrastructure	6	2.437	3
00:0c:30:94:1e:09	ixia2	Infrastructure	11	2.462	43
00:0a:f5:00:0b:8b	lxwlan500	Infrastructure	11	2.462	32
00:0e:83:11:75:30		Infrastructure	5	2.432	14
00:40:96:a2:b7:36	IXIA1	Infrastructure	8	2.447	13
00:11:92:fd:32:40	Lab2-AP	Infrastructure	9	2.452	11

Selected BSSID: 00:0c:30:94:1e:09

The main GUI of the IxWLAN device will display the Join status.



CMC EmulationEngine(tm) - Microsoft Internet Explorer

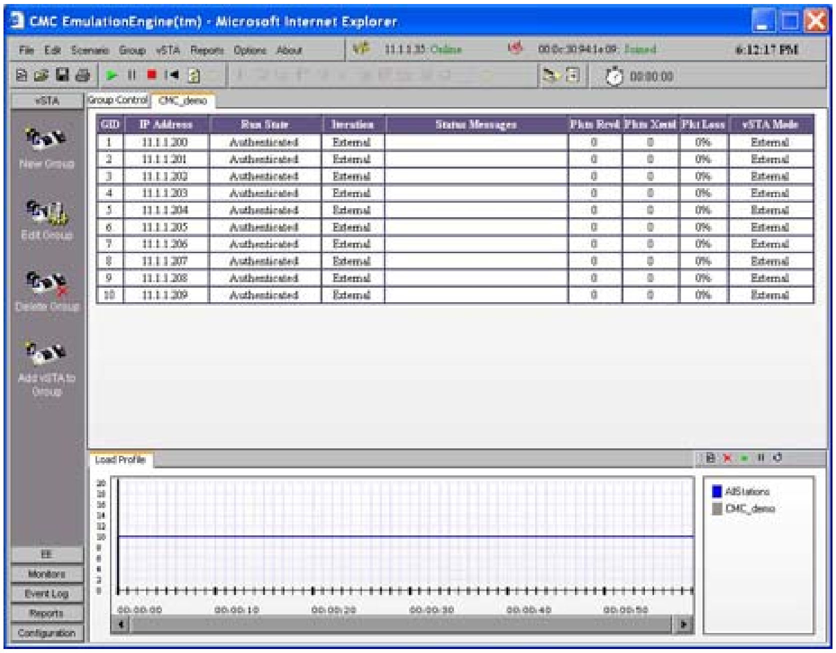
11.1.1.25 Online 00:0c:30:94:1e:09 Joined 6:07:06 PM

00:00:00

GID	IP Address	Run State	Iteration	Status Messages	Pkts Rcvd	Pkts Xmtd	Pkt Loss	vSTA Mode
1	11.1.1.200	Configured	External		0	0	0%	External
2	11.1.1.201	Configured	External		0	0	0%	External
3	11.1.1.202	Configured	External		0	0	0%	External
4	11.1.1.203	Configured	External		0	0	0%	External
5	11.1.1.204	Configured	External		0	0	0%	External
6	11.1.1.205	Configured	External		0	0	0%	External
7	11.1.1.206	Configured	External		0	0	0%	External
8	11.1.1.207	Configured	External		0	0	0%	External
9	11.1.1.208	Configured	External		0	0	0%	External
10	11.1.1.209	Configured	External		0	0	0%	External

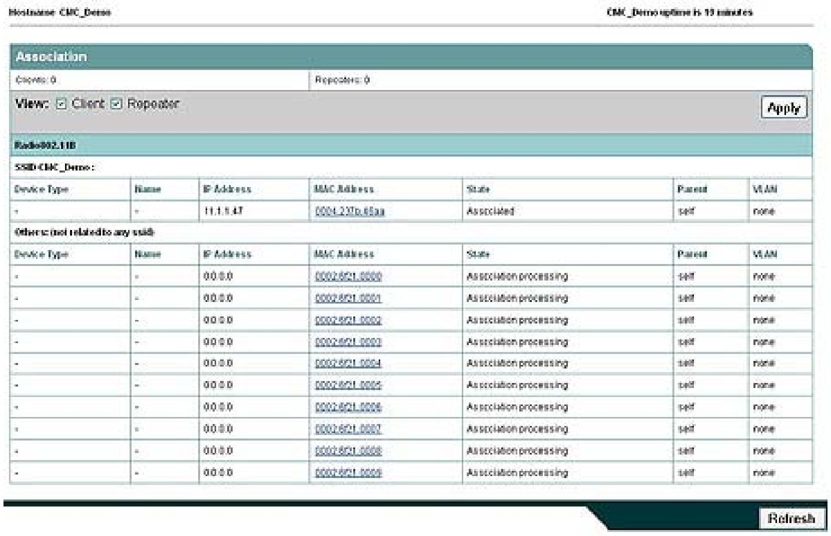
10. Go to **Scenario** and select the **Authenticate** option

    This starts the 802.11 Authentication process. Authentication is the process a station uses to announce its identity to an Access Point (AP) or to a RADIUS server for 802.1x Authentication. There is open and shared key. Since this is an open network, we had 10 stations sending authentication request frames to the AP and receiving authentication responses. Some Access Points will show the state of the vSTA in their association table.



CMC EmulationEngine(tm) - Microsoft Internet Explorer

GID	IP Address	Run State	Iteration	Status Messages	Pkts Rcvd	Pkts Xmtd	Pkt Loss	vSTA Mode
1	11.1.1.200	Authenticated	External		0	0	0%	External
2	11.1.1.201	Authenticated	External		0	0	0%	External
3	11.1.1.202	Authenticated	External		0	0	0%	External
4	11.1.1.203	Authenticated	External		0	0	0%	External
5	11.1.1.204	Authenticated	External		0	0	0%	External
6	11.1.1.205	Authenticated	External		0	0	0%	External
7	11.1.1.206	Authenticated	External		0	0	0%	External
8	11.1.1.207	Authenticated	External		0	0	0%	External
9	11.1.1.208	Authenticated	External		0	0	0%	External
10	11.1.1.209	Authenticated	External		0	0	0%	External



Hostname CMC_Demo

CMC_Demo uptime is 19 minutes

Association

Clients: 0 | Repeaters: 0

View: ☑ Client ☑ Repeater

Radio802.11B

SSID CMC_Demo :

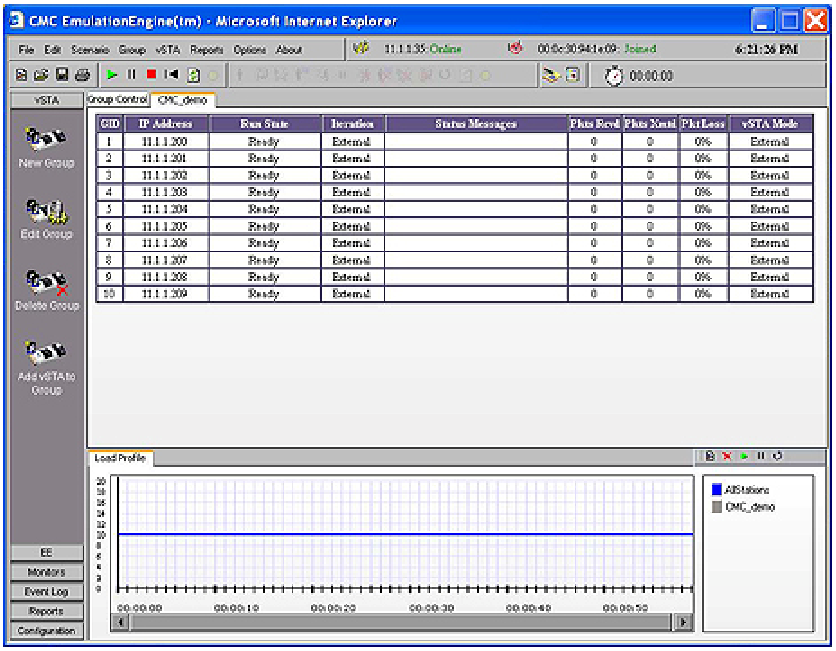
Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
-	-	11.1.1.47	0004.237b.65aa	Associated	self	none

Others: (not related to any ssid)

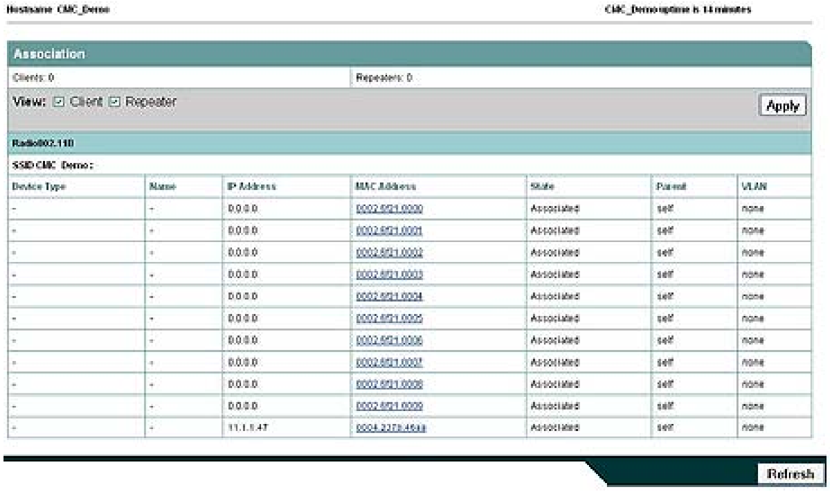
Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
-	-	0.0.0.0	0002.6f21.0000	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0001	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0002	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0003	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0004	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0005	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0006	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0007	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0008	Association processing	self	none
-	-	0.0.0.0	0002.6f21.0009	Association processing	self	none

11. Go to Scenario and select the Associate option.

    Association is the state at which the client is allowed to pass data to the AP. In this case, we have 10 vSTAs send association requests to the AP and receiving a positive association response. The Access Point's association table will display the changed state.



GID	IP Address	Run State	Iteration	Status Messages	Pkts Rcvd	Pkts Xmtd	Pkt Loss	vSTA Mode
1	11.1.1.200	Ready	External		0	0	0%	External
2	11.1.1.201	Ready	External		0	0	0%	External
3	11.1.1.202	Ready	External		0	0	0%	External
4	11.1.1.203	Ready	External		0	0	0%	External
5	11.1.1.204	Ready	External		0	0	0%	External
6	11.1.1.205	Ready	External		0	0	0%	External
7	11.1.1.206	Ready	External		0	0	0%	External
8	11.1.1.207	Ready	External		0	0	0%	External
9	11.1.1.208	Ready	External		0	0	0%	External
10	11.1.1.209	Ready	External		0	0	0%	External



Hostname CMC_Demo

CMC_Demo uptime is 14 minutes

Association

Clients: 0

Repeaters: 0

View: ☑ Client ☑ Repeater

Radio802.11B

SSID CMC_Demo :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
-	-	0.0.0.0	0002.6f21.0000	Associated	self	none
-	-	0.0.0.0	0002.6f21.0001	Associated	self	none
-	-	0.0.0.0	0002.6f21.0002	Associated	self	none
-	-	0.0.0.0	0002.6f21.0003	Associated	self	none
-	-	0.0.0.0	0002.6f21.0004	Associated	self	none
-	-	0.0.0.0	0002.6f21.0005	Associated	self	none
-	-	0.0.0.0	0002.6f21.0006	Associated	self	none
-	-	0.0.0.0	0002.6f21.0007	Associated	self	none
-	-	0.0.0.0	0002.6f21.0008	Associated	self	none
-	-	0.0.0.0	0002.6f21.0009	Associated	self	none
-	-	11.1.1.47	0004.2378.46a8	Associated	self	none

In a standard 802.11 authentication and association sequence, there are three states and the IxWLAN device takes you through each one of them:

- unauthenticated and unassociated
- authenticated and unassociated
- authenticated and associated

12. Go to Scenario and select the Run option. This will set the IxWLAN device in the proper state to integrate with IxChariot and forward traffic streams.

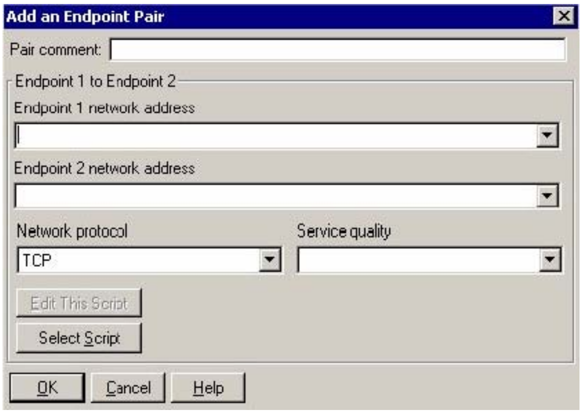
2. Ixia–IxApplifier/IxChariot Configuration

The basic configuration of IxChariot to work in tandem with the IxWLAN device can be split into three steps:

- Defining the MAC/IP addresses (using IxApplifier if the Performance Endpoint for IxOS is used) and ensuring that Performance Endpoints are running on the hosts
- Creating an IxChariot test using the source IP addresses defined in step 1)
- Running the test once all vSTAs are in Ready state

1. First, launch the IxApplifier application.
2. Expand the Chassis Chain, Loopback, Card1 (In this example, we have a LM100TXS8 residing on slot 1 of a 400T chassis. You may need to choose the appropriate card that you want to use).
3. In the Chassis and Port Configuration, Click on Port 1.
4. On the right hand side, in the Application Download tab, change the Package Name field from "undefined" to "@ixChariot Performance Endpoint".
5. Click on "Apply to port x.x.1".
6. On the right hand side, under the interfaces tab, click on the "add interfaces button".
7. Once in the Add Interfaces window, change the "create interfaces" according to the number of streams you may want to configure. For the purposes of this document, we will leave the "create interfaces" to default 1.
8. In the "MAC Address Block" of the "Add Interfaces" windows, configure the MAC address and IPv4 source addresses for the test. Please note that the MAC and IPv4 addresses must the same as the one configured for IxWLAN vSTAs™. In this case, we configure 00:02:6F:21:00:00 as the initial MAC and 180.1.1.10 as the initial IPv4 Source Address and increment it sequentially to create ten MAC/IP address pairs.
9. Click on the "Add new interfaces to port x.x.1".
10. Go to a second port in the chassis chain and define it with a random MAC address and an IPv4 address that is in the same subnet as the vSTAs, the IxWLAN device and the SUT (e.g. 180.1.1.20).
11. On the Post Download Tab, ensure that the "Run Program" radio button is selected and that the correct path to the "chariot.exe" file is entered in the Program field.
    NOTE: This will ensure that the IxChariot console will come up after the "Run a test folder" button has been pressed.
12. Once the IxApplifier has been configured, you are now ready to click on the "Run a test" folder positioned at the top left of the IxApplifier application.
13. This will trigger the IxChariot to run.
14. Click on the "New" button.

15. Pull down "Edit" and select "Add pair".



Add an Endpoint Pair

Pair comment:

Endpoint 1 to Endpoint 2

Endpoint 1 network address

Endpoint 2 network address

Network protocol: TCP

Service quality

16. For "Endpoint 1 network address", enter 180.1.1.10

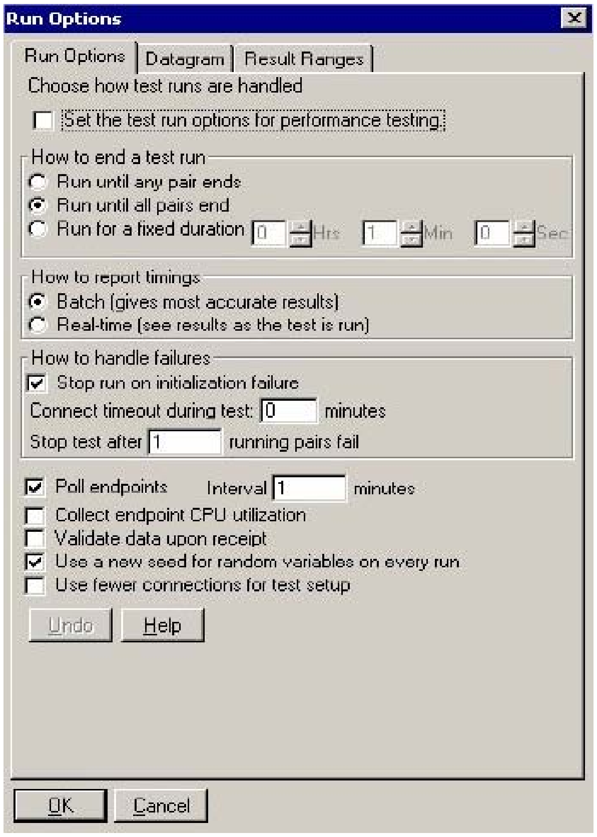
17. For "Endpoint 2 network address", enter 180.1.1.20

18. The Network protocol may be changed from "TCP" to "UDP" depending on the protocol that is being tested.

19. Click on "Select Script" and select "Response_time.scr".

20. Click "OK".

21. Click on the "Run" pull down option and select "Set Run Options".



Run Options

Choose how test runs are handled

□ Set the test run options for performance testing.

How to end a test run
○ Run until any pair ends
● Run until all pairs end
○ Run for a fixed duration 0 Hrs 1 Min 0 Sec

How to report timings
● Batch (gives most accurate results)
○ Real-time (see results as the test is run)

How to handle failures
☑ Stop run on initialization failure
Connect timeout during test: 0 minutes
Stop test after 1 running pairs fail

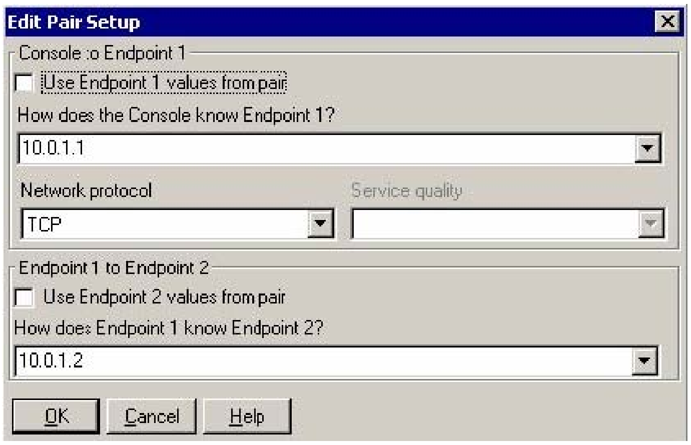
☑ Poll endpoints Interval 1 minutes
□ Collect endpoint CPU utilization
□ Validate data upon receipt
☑ Use a new seed for random variables on every run
□ Use fewer connections for test setup

22. Select the "Run until all pairs end" radio button.

23. Select the "Batch" radio button.

24. Click "OK".

25. Click on the "Edit" pull down menu and select "Edit Pair Setup".

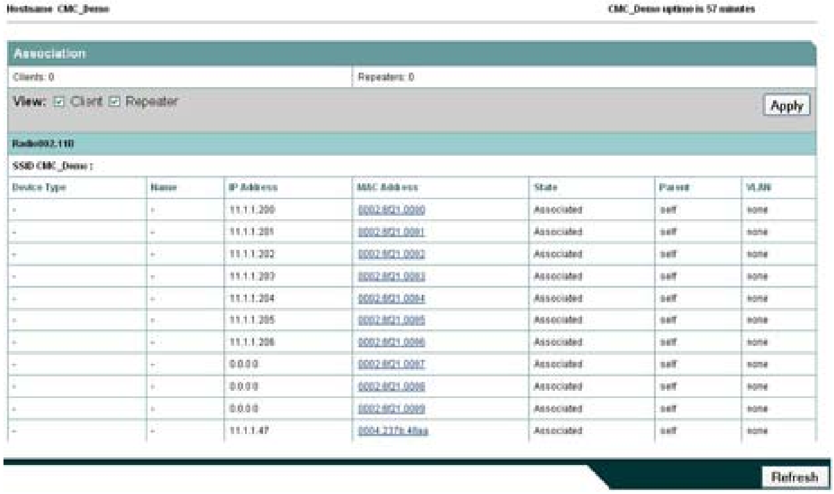


Edit Pair Setup
Console :o Endpoint 1
☐ Use Endpoint 1 values from pair
How does the Console know Endpoint 1?
10.0.1.1
Network protocol
TCP
Service quality
Endpoint 1 to Endpoint 2
☐ Use Endpoint 2 values from pair
How does Endpoint 1 know Endpoint 2?
10.0.1.2
OK
Cancel
Help

26. Ensure that the "How does the Console know Endpoint 1?" IP address is the Mgmt IP address of the Port.

27. Click "OK".

28. Providing that the IxWLAN device is configured, you may now click on the "Run" button. The Association table in the SUT will now show the source IP addresses for each vSTA that has an associated IxChariot pair generating traffic.



Hostname CMC_Demo

CMC_Demo uptime is 57 minutes

Association

Clients: 0 Repeaters: 0

View: ☑ Client ☑ Repeater

Radio802.11B

SSID CMC_Demo :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
-	-	11.1.1.200	0002.8f21.0080	Associated	self	none
-	-	11.1.1.201	0002.8f21.0081	Associated	self	none
-	-	11.1.1.202	0002.8f21.0082	Associated	self	none
-	-	11.1.1.203	0002.8f21.0083	Associated	self	none
-	-	11.1.1.204	0002.8f21.0084	Associated	self	none
-	-	11.1.1.205	0002.8f21.0085	Associated	self	none
-	-	11.1.1.206	0002.8f21.0086	Associated	self	none
-	-	0.0.0.0	0002.8f21.0087	Associated	self	none
-	-	0.0.0.0	0002.8f21.0088	Associated	self	none
-	-	0.0.0.0	0002.8f21.0089	Associated	self	none
-	-	11.1.1.47	0004.237b.48aa	Associated	self	none