



Testing Enterprise Wireless LANs Using IxWLAN and IxChariot

Contents

IPTV – Channel Change Performance Testing.....	3
Test 1 – Optimal Channel Change Performance	8
Test 2 – Single Subscriber Experience.....	14
Test 3 – Triple Play Traffic.....	18

Copyright © 2006 Ixia.
All rights reserved.

The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Ixia. Ixia assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. Ixia and the Ixia logo are trademarks of Ixia. All other companies, product names, and logos are trademarks or registered trademarks of their respective holders.



26601 W. Agoura Road
Calabasas, CA 91302

Phone: (818) 871-1800
Fax: (818) 871-1805
Email: info@ixiacom.com
Internet: www.ixiacom.com

Testing Enterprise Wireless LANs Using IxWLAN and IxChariot

1. Introduction

Wireless 802.11 networks (“wireless LANs” or “WLANs”) are becoming ubiquitous in the corporate networking environment. Because of their widespread use, these networks must be secure, resilient, and meet the high performance requirements of the corporate enterprise. At the same time, the deployment of these wireless networks must be time efficient and cost effective. For these reasons, pre-deployment testing of the WLAN is a necessary step to ensure the seamless integration of the new infrastructure.

The wireless network has a range of important test metrics that it must achieve; however, none is more important than pre-deployment security testing. This is because wireless networks introduce security issues not faced in wired networks since a physical connection is no longer required for a user to access the WLAN. Other important testing issues include network capacity assessment and, of course, a variety of performance measurements since the wireless network must handle the same kinds of traffic as the wired networks

This test plan addresses the testing of wireless deployments by focusing on features generally available in enterprise class access points. The test plan uses Ixia’s IxWLAN as a test tool to test the features. These tests may be conducted during vendor selection or as a part of pre-deployment testing, or as regular maintenance. This emphasis of this test plan is on selected aspects of security, capacity and performance, as well as traffic handling of the Access Point (AP). Depending on the particular features of your network and its deployment requirements, modifications to the tests may be necessary, and additional tests may also be appropriate for more sophisticated networks.

Testing WLAN deployment primarily involves two steps:

- Checking for RF continuity
- Testing the functionality and performance of the WLAN

This test plan focuses on testing the functionality and performance of the WLAN. Because of the requirement to fully test the complex mix of traffic that is typical of enterprise networks, Ixia’s sophisticated IxChariot® traffic generation tool is used to execute the tests presented in this plan.

This plan assumes that the RF continuity requirement has been addressed by a site survey to choose the correct frequencies of operation, and also that there is complete RF coverage necessary to have a fully functional and operational

WLAN. This plan also assumes that the network is fully integrated with the DHCP server and the RADIUS server that has been selected for your specific WLAN deployment.

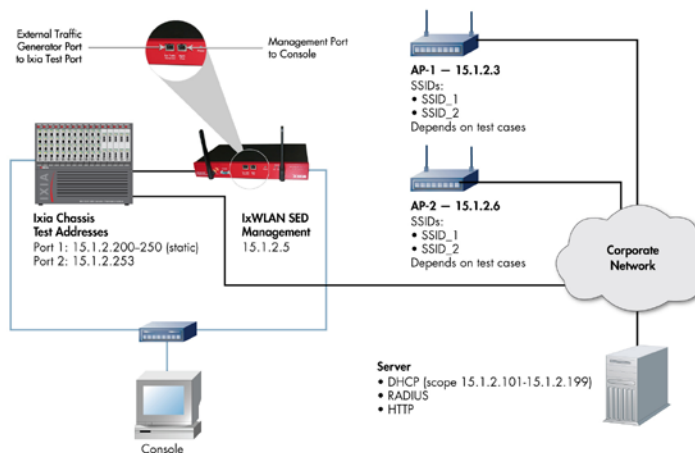
2. Test Objective, Performance Metrics and Setup

The test plan is targeted at three aspects of an enterprise class deployment:

- Security
- Performance and capacity
- New application deployment testing

Each of the tests in this plan first addresses the functional capability of a given feature, and then assesses its performance aspects. Next, each test carefully examines the impact of roaming on the feature, and applies specific test parameters that may be relevant to the particular test case.

The setup of the WLAN network is the same in all the tests that are conducted. The test topology is illustrated in the diagram below:



The IxWLAN scenarios and IxChariot tests for the test cases are available for download and are archived here. The test plan refers to files from this archive and those may be directly used with modifications in your test bed.

3. Test Cases

3.1. Security

3.1.1. Introduction

Network security is a major concern for any organization and needs to be tested exhaustively. Stations associating to the network wirelessly typically have the same access rights to the resources as wired stations on the LAN. The access depends on the login name and user group to which the login is mapped. The most common authentication used in wireless networks in the enterprise is PEAP/EAP-MS-CHAPv2, which probably is due to the fact that most organizations use Microsoft Windows-based authentication servers. Some organizations may use EAP-TLS, but since this authentication method requires a public key infrastructure (PKI) that increases cost, most opt for the PEAP method.

This test plan uses a PEAP authentication method.

3.1.2. Input Parameters

Parameter	Description
Virtual Stations (vSTA)	Number of Stations (STAs) emulated
vSTA attributes	IP address (DHCP or static), SSID, security settings per Station, traffic type
Traffic type	Internal (Ping) and/or External (IxChariot)
Access Points (APs)	IP addresses
External traffic	HTTP get script (HTTPgif script) for all STAs configured in external traffic mode with a random start time between (0,3) minutes for a 10 minute test
Test Objective	<p>a. Functional Testing – Test functionality of the security feature with 5 internal and 5 external STAs</p> <p>b. Performance/Capacity testing - Find the maximum number of STAs that the AP can support (iteratively using a binary search) or verify the number from data sheet</p>

3.1.3. Functional Testing

Functional security testing assess the implemented authentication methods and ciphers (WPA-PSK with TKIP or RSN (WPA2) with AES-CCMP or Shared Key with WEP etc.).

In this test, you will be testing the network for WPA (PEAP) (WPA-Enterprise) with TKIP as the cipher. Similarly, tests for RSN (PEAP) (WPA2-Enterprise) with AES-CCMP as the cipher can be carried out.

3.1.3.1. Methodology

- a. Set up five (5) virtual stations in external Layer 3 traffic mode with static IP addresses, doing WPA – PEAP and TKIP.
- b. Set up five (5) virtual stations in internal traffic mode with DHCP addresses, a ping count of 30 pings / iteration doing 1,000 iterations, and resetting to “initialized” state after each iteration. Set security settings to WPA – PEAP with TKIP as cipher.
- c. Set up the Access Point to support the security settings to be tested.
- d. Join the SUT
- e. Clear the statistics counters and logs
- f. Run the test and collect data.

3.1.3.1. Results and Reports

The event log produced by IxWLAN enables you to track each step of the 802.1x authentication process. It follows each packet across the air and logs (with a microsecond timestamp and sequence number) the progress of the 802.1x authentication followed by the WPA 4-way handshake and installation of the keys. In this way, you can track any unsuccessful authentication to the exact point of failure.

Please refer to the PEAP-Exchange.html file in the zip file.

The counters showing the details for each vSTA are also available in the vSTA detail reports. A brief sample of the counters for the WPA exchange for a single vSTA is shown below

The IxWLAN scenario file used for this test is the IxWLAN-TP-WPA-Functional.xml

WPA/RSN Counts

Total EAPOL Frames Tx: 56	WPA/RSN Auth Failure Ct: 0
Total EAPOL Frames Rx: 60	WPA/RSN Authentication Ct: 4
EAPOL Key Frames Rx: 12	EAPOL Key Frames Tx: 12
EAPOL Request Frames Rx: 44	Invalid EAPOL Frames Rx: 0
EAPOL Rsp Id Frames Tx: 4	EAPOL Rsp Frames Tx: 44
EAPOL Req Id Frames Rx: 4	EAPOL Len Err Frames Rx: 0

4Way Handshake Msg1 Rx: 4	4Way Handshake Msg2 Tx: 4
4Way Handshake Msg3 Rx: 4	4Way Handshake Msg4 Tx: 4
Group Key Msg1 Rx: 4	Group Key Msg2 Tx: 4
TKIP Local MIC Failures: 0	TKIP Rply Ctr Failures: 0
TKIP ICV Errors: 0	CCMP Rply Ctr Failures: 0
CCMP Decrypt Errors: 0	MIC Failure Reports Tx: 0
Last EAPOL Frame Ver: 1	EAPOL Start Frames Tx: 0

3.1.4.Performance and Capacity Testing

WLAN performance testing is important since it provides a number estimate of the maximum station capacity of the AP. It can be used to test a designed network during pre-deployment or verify information on capacity provided by the Access Point vendor. This estimated number reflects the maximum number of stations that the AP can comfortably support at the thresholds of quality of user experience that is required by the enterprise.

This maximum station number may be arrived at directly from the AP manufacturer’s claim or from the related design document. In this test case, for example, you can verify that the AP can handle at least 30 stations rather than finding a breaking point for the AP.

3.1.4.1.Methodology

First test:

- a. Set up twenty (20) virtual stations in external layer-3 traffic mode with static IP addresses, doing WPA – PEAP and TKIP.
- b. Set up ten (10) virtual stations in internal traffic mode with DHCP-acquired addresses, a ping count of 30 pings / iteration, and perform 100 iterations, resetting to “initialized” state after each iteration.
- c. Set security settings to WPA – PEAP and use TKIP as the cipher.
- d. Set up the Access Point to support the security settings to be tested.
- e. Configure a test in IxChariot, where each vSTA (in external layer 3 mode) IP corresponds to a pair transmitting to another endpoint on the distribution side of the network.
- f. Join the SUT
- g. Clear the statistics counters and logs
- h. Run the test and collect data.

Second test:

- a. Set up twenty (20) virtual stations in external layer-3 traffic mode with

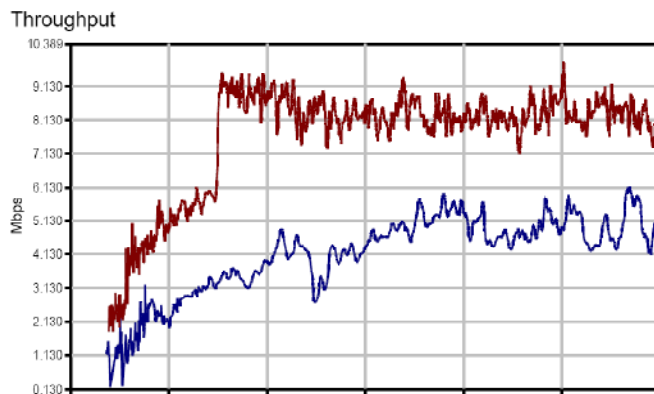
- static IP addresses, doing WPA – PEAP and TKIP.
- b. Set up ten (10) virtual stations in internal traffic mode with DHCP-acquired addresses, a ping count of 30 pings / iteration, and perform 100 iterations, resetting to “Ready” state after each iteration. Set security settings to WPA – PEAP and use TKIP as the cipher.
- c. Set up the Access Point to support the security settings to be tested.
- d. Configure a test in IxChariot where each vSTA (in external layer 3 mode) IP corresponds to a pair transmitting to another endpoint on the distribution side of the network.
- e. Join the SUT
- f. Clear the statistics counters and logs
- g. Run the test and collect data.

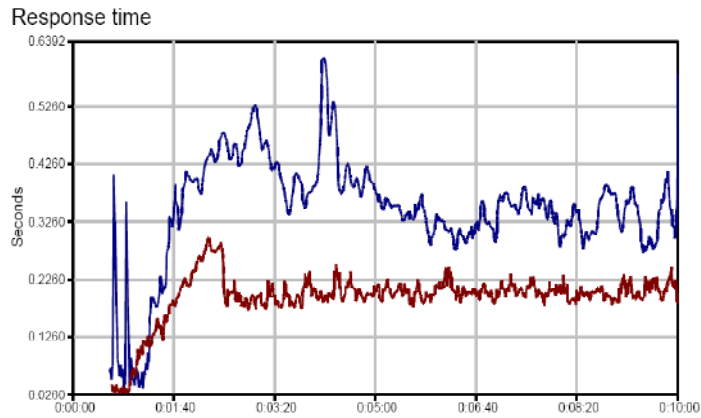
Once you have completed both tests, compare IxChariot performance measurements using the IxChariot test comparison tool.

3.1.4.1. Results and Reports

As shown in the graph below, these two test demonstrate that the throughput for the external traffic changes (~7Mbps against ~4Mbps). What is also interesting to note in this test is that the response times across this simple network are about twice as high with only 10 stations cycling through the authentication process and stressing the state machine of the AP. This is a critical metric since an AP that is incapable of handling such a load may actually fail not from a network point of view, but from a usability point of view. In this situation, a network user may be able to ping the AP, but may not be able to get traffic through the AP.

	Test run with “internal traffic” stations in steady “Ready” state.
	Test run with “internal traffic” stations with changing state starting from “Initialized” state.





From the zip file with the plan, the following are the IxChariot and IxWLAN test files used for the first test:

IxWLAN-TP-WPA-Performance-20e-10i-initialized.tst
 IxWLAN-TP-WPA-Performance-20e-10i-initialized.xml

From the zip file with the plan, the following are the IxChariot and IxWLAN test files used for the second test:

IxWLAN-TP-WPA-Performance-20e-10i-ready.tst
 IxWLAN-TP-WPA-Performance-20e-10i-ready.xml

3.1.5. Roaming Testing – Pre-authentication, Fast Reconnect (Fast RADIUS) and PMKSA

The features tested in this test are optional features that may not be available in all APs and RADIUS servers. However, these features do help in minimizing the roam times for a secure network and should be tested if available and implemented.

The pre-authentication feature is specified for WPA2 (RSN) networks only. It provides a means for the station to authenticate with other APs in the network over the distribution network. This means that a station roaming to an AP with which it has already authenticated does not need to go through the complete RSN handshake. The required key generation is already completed, and the AP and the station have a cache of keys that is referenced to expedite the roam.

Fast Reconnect (fast RADIUS) is a feature that provides a session_id based means to speed up the 802.1x authentication for a particular station. In

this method, the client station caches session information from a previously established TLS session, and then provides the session_id from that session in the TLS "client_hello" message, near the start of the new 802.1X authentication exchange. If the Authentication Server has a matching cached session with the same session_id, the session and the station can use the master_secret from that session, skipping the certificate exchange and lengthy public/private key encryption operations in the TLS exchange.

The fast RADIUS reconnection technique can also be used in pre-authentication to speed up the exchange. Fast RADIUS reconnection and/or PMKSA caching can be used as well in re-establishing an association with a single AP after having disassociated.

You can measure the difference in roam times with the options mentioned above turned on and turned off. The tests are run in internal mode with APs and RADIUS servers that are capable of supporting the feature and the security settings set to RSN (PEAP) / AES-CCMP.

The difference in roam times can be measured with the options mentioned above turned on and turned off.

3.1.5.1. Methodology

- a. Set up group "SlowRoam" with 5 vSTAs in internal traffic mode with DHCP addresses, a Ping count of 20 Pings / iteration, doing 30 iterations and resetting to "Ready" state after each iteration. Keep the iteration delay to 10ms. Set security settings to WPA with PEAP and TKIP as cipher. Disable PMKSA and Fast RADIUS option on the vSTAs.
- b. Set up another group as "FastRoam" with 5 vSTAs in internal traffic mode with DHCP addresses, a Ping count of 20 Pings / iteration, doing 30 iterations and resetting to "Ready" state after each iteration. Keep the iteration delay to 10ms. Set security settings to WPA with PEAP and TKIP as cipher. Enable PMKSA and Fast RADIUS option on the vSTAs.
- c. Set up the AP to support the security settings with pre-authentication turned off.
- d. Turn on the fast RADIUS feature on the authentication server.
- e. Join the SUT.
- f. Clear the statistics counters and logs.
- g. Run the test and collect data.
- h. Repeat the test with pre-authentication turned on the APs and the vSTAs.

3.1.5.1. Results and Reports

The PMKSA and Fast Reconnect (Fast RADIUS) features in a WLAN environment have two interconnected advantages. First, they minimize the roam times; and second, due to lower roam times, key caching, and faster authentication, the loss of data in a continuous stream of data traffic (such as streaming media or VoIP calls) is minimized. IxWLAN lets you measure both the status and the roam times. It also indicates the data frame to data frame times and hang time, i.e., management frame to management frame time, for the roams.

As shown below, the roam times are much lower for the group with the PMKSA and Fast Reconnect enabled as expected. This group also shows fewer losses on the pings.

Metric	SlowRoam	FastRoam
Total Roams	45	45
Successful Roams	45	45
Failed Roams	0	0
Aborted Roams	0	0
Roam start-to-stop time min (msec)	690.557	553.824
Roam start-to-stop time max (msec)	883.407	644.860
Roam start-to-stop time avg (msec)	756.641	594.407
Data-frame-to-data-frame min (msec)	990.724	731.556
Data-frame-to-data-frame max (msec)	1253.247	993.503
Data-frame-to-data-frame avg (msec)	1107.069	866.627
Transmit frames dropped min	2	2
Transmit frames dropped max	3	2
Transmit frames dropped avg	2	2
% frames lost	5%	3%

From the TP repository, this refers to IxWLAN-TP-Roaming.xml. The results for the test are published for both each group and on a per vSTA basis - IxWLAN-TP-Roaming-group-results.pdf and IxWLAN-TP-Roaming-results.pdf

3.2. Multiple SSID and Access control

3.2.1. Introduction and network details

Most enterprise class APs are now equipped with the capability to support multiple SSIDs (Service Set Identifiers). Each SSID typically maps to a different

VLAN on the wired side of the AP so that users connecting to the wireless network with different SSIDs are mapped to different roles and have different access rights to the network. Typical examples include a guest network for visitors to an office, as well as an employee network that offers more privileges – for example, access to corporate servers and the email system.

These SSIDs typically also have different security settings (e.g., the guest network may be an open network; whereas, the employee network may be a secured WPA/TKIP network). Testing the deployment of these networks, and characterizing the performance is essential to ensure that the access rights are correctly set and that the access points can handle the load that is expected on all available SSIDs without disruption of service.

IxWLAN allows you to test multiple SSIDs by setting an SSID per virtual station (vSTA). To test this feature, in the example test network, you will be using two SSIDs:

- “Employee” – WPA/TKIP
- “Administrator” – RSN(WPA2) / AES-CCMP

Both SSIDs are DHCP-enabled and obtain addresses from the same DHCP pool, but are tagged with different VLANs on the distribution side of the AP. Access may be defined differently in a real network, but in this test network the access rights are the same.

3.2.2. Multiple SSID Functionality testing

The suggested way to test the multiple SSID feature for functionality is to create two groups on the IxWLAN and configure them with the security settings for the SSIDs. In the current test case, the two groups are identified with the SSID as the title. The IP address settings are set to DHCP and the traffic is set to internal mode. The target IP address is set to the gateway address of the network. You may want to use an IP address that is specifically reachable only from a particular VLAN.

Some negative testing is also possible by trying to reach an IP address that cannot be reached from a certain SSID. To do this, join the SUT and associate the vSTA. Once the test is completed, it can be extended to run with external traffic. This test is discussed in the next section where the WLAN is tested for its capability to handle the number of stations it was designed to handle (capacity testing), and the impact on the end-user experience.

3.2.2.1. Methodology

- a. Set up ten (10) vSTAs in internal traffic mode with DHCP addresses, doing WPA – PEAP and TKIP and SSID “Employee”

- b. Set up ten (10) vSTAs in internal traffic mode with DHCP addresses, doing RSN – PEAP and AES-CCMP and SSID “Administrator”
- c. Set up the access point to support the SSID and corresponding security settings to be tested.
- d. Join the SUT.
- e. Clear the statistics counters and logs.
- f. Run the test and collect data.

3.2.2.2.Results

The RSN (WPA2) and WPA authentications are different in the way they are handled even though the basic premise of using the 802.1x authentication keys and the 4 way handshake remains the same.

The event log in the for the WPA exchange is located in the file WPA-Eventlog.htm, and the RSN exchange is detailed in the RSN-Eventlog.htm

The scenario file for this test case is named IxWLAN-TP-MSSID-Functional.xml

3.2.3.Multiple SSID performance and capacity testing

Due to the variety of WLAN solutions available, it must be clarified that the current SUT is presumed to be a fully functional AP (fat-AP) based WLAN.

The basic objective of this test is to load the AP not only from a point of view of passing traffic, but also from a point of view of stressing the AP’s state machine by emulating a group of users coming online and disconnecting while some users constantly pass traffic. The design documents or specifications from the manufacturer should provide you with the number of stations that the AP is able to support. This may be dependent on the location of the AP (e.g., in the lobby of the office) and the design of the WLAN.

With this use case, you will be loading the AP with 30 external traffic generating stations and 20 internal stations. The total stations are divided amongst the 2 SSIDs equally.

With the test WLAN, create two groups

- Admin_Ext – For external traffic using the “Administrator” SSID
- Employee_Ext – For external traffic using the “Employee” SSID

The traffic mix used in this test is only used as an example, and you should adjust it to meet your own particular testing needs.

Considering that the network will handle only data traffic, the following metrics are considered important from a network deployment point of view:

- Capacity – number of STAs an AP can support
- Performance – throughput and response time per STA as an indicator of the end user experience

3.2.3.1. Methodology

- a. Set up twenty (20) vSTAs in external Layer-3 traffic mode with static IP addresses, doing WPA – PEAP and TKIP with SSID “Employee”. This is the “Employee_Ext” group
- b. Set up twenty (20) vSTAs in external Layer-3 traffic mode with static IP addresses, doing RSN – PEAP and AES-CCMP with SSID “Administrator”. This is the “Admin_Ext” group.
- c. Set up the access point to support the security settings to be tested.
- d. Configure a test in IxChariot where each vSTA (in external Layer 3 mode) IP corresponds to a pair transmitting to another endpoint on the distributions side of the network. The application traffic is determined by the use case.
- e. Join the SUT.
- f. Clear the statistics counters and logs.
- g. Run the test and collect data.

3.2.3.1. Results and Reports

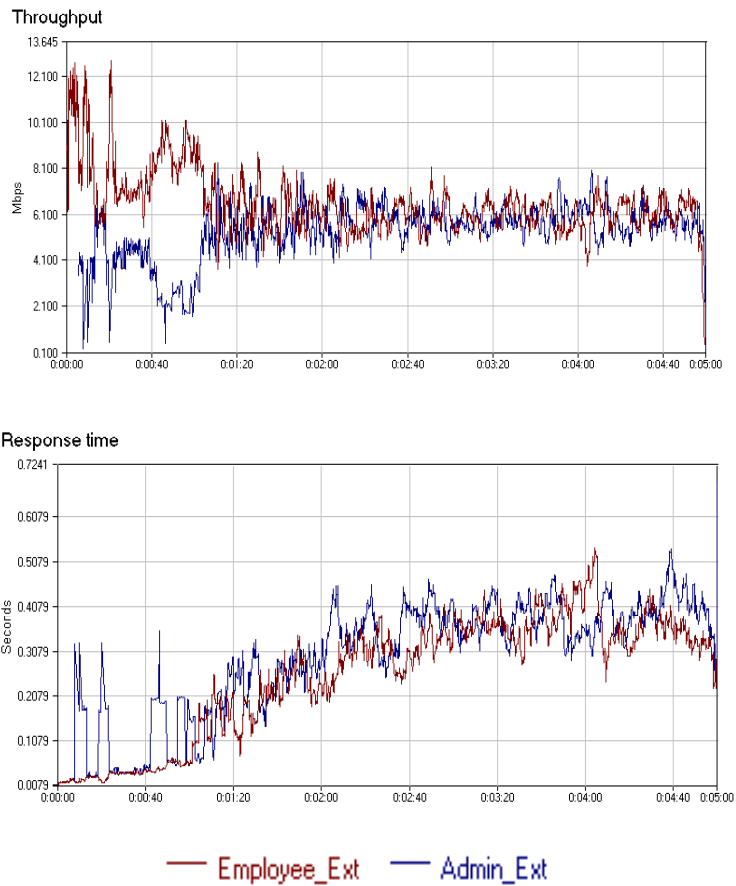
A couple of points should be clarified before you review test results:

1. The number of stations and the traffic be run depends on the network.
2. A variety of other tests, including roaming testing, may be needed and conducted using the IxWLAN and IxChariot testing software to provide a complete picture of the end-user. Throughput, one-way delay (or response time), MOS scores, and jitter key parameters to review

The tests for an unencrypted (SSID – Guest) to an encrypted network (SSID – Administrator or Employee) may actually prove that there may be a need for the Guest SSID to have a lower bandwidth compared to the Employee or the Administrator SSID. In the test scenarios presented here, no such restrictions have been introduced. This test is important especially from a point of view of the Guest and Employee or Administrator bandwidth allocations.

Please keep in mind, that the tests presented here are samples only, and the results may differ from network to network depending on the traffic type and the number of users per SSID.

The graphs presented here are generic items that you may want to compare using the IxChariot compare test feature. This allows us the capability of comparing performance on separate runs of the test for different network metrics.



The IxChariot and IxWLAN test files from the zip file are IxWLAN-TP-MSSID-Performance.tst and IxWLAN-TP-MSSID-Performance.xml