



Client Connectivity via IPv4 and IPv6 Protocols

IPv6 Test Plan for Office 365 Component Functionality

Published: 03/2013

Date	Contributor	Version	Description
01/29/13	Eric Beauchesne	0.1	Initial draft, needs SPO inputs
02/03/13	Eri Igawa	1.0	Including SPO requirements
02/28/13	Eri Igawa	1.1	Including BOX and Office requirements
03/04/13	Eri Igawa	1.2	Including RMS requirements Addressing Non-Goals of the doc Including supplemental WAC requirements Update OWA URL

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

©2012 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Internet Explorer, Lync, MSN, Outlook, SharePoint, Windows, Windows Live, Windows Mobile, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

- 1 Overview..... 5**
 - Conventions..... 5
 - Document Non-Goals..... 5
- 2 Environment Requirements..... 6**
 - 2.1 Test Accounts 6
 - 2.2 Client Configuration..... 6
 - 2.3 Network Configuration..... 6
 - 2.3.1 *Proposed Network Design* 6
 - 2.3.2 *IPv6-Capable Network Equipment*..... 7
 - 2.3.3 *IPv6 Only Clients*..... 7
 - 2.3.4 *IPv4 Only Clients*..... 7
- 3 Client Validation..... 8**
 - 3.1 Routable IPv6 Address 8
 - 3.2 Routable IPv4 addresses 8
- 4 DNS Validation 9**
 - 4.1 DNS Records 9
- 5 Exchange Online (EXO) Access and Functionality Validation 10**
 - 5.1 Mail Connection Validation 10
 - 5.1.1 *Outlook Web Access* 10
 - 5.2 Mail Functionality Validation..... 12
 - 5.2.1 *Outlook Web Access* 12
- 6 SharePoint Online (SPO) Access and Functionality Validation..... 13**
 - 6.1 SharePoint Online Access 13
 - 6.1.1 *Accessing the SPO Server*..... 13
 - 6.1.2 *Document Management* 14
- 7 Lync Online Access and Functionality Validation 15**
 - 7.1 Lync Online Access 15
 - 7.1.1 *Accessing the Lync Server* 15
 - 7.1.2 *Lync Functionality*..... 16
- 8 Web Application Companion (WAC) Access and Functionality Validation 18**
 - 8.1 WAC Access..... 18
 - 8.1.1 *Accessing Files with WAC*..... 18
 - 8.1.2 *WAC Functionality* 19
- 9 Self Service Password Reset (SSPR) Functionality Validation..... 20**

9.1	SSPR Functionality	20
9.1.1	<i>Accessing the Password Reset Portal</i>	20
9.1.2	<i>Resetting the Admin Password</i>	21
10	BOX Functionality Validation	22
10.1	BOX Functionality.....	22
10.1.1	<i>Accessing the Office 365 Admin Portal</i>	22
10.1.2	<i>Manage User Provisioning and Password</i>	23
11	Office Functionality Validation	24
11.1	Office Functionality	24
11.1.1	<i>Installing Office 2013 from Office 365 Portal</i>	24
12	Rights Management Services Functionality Validation.....	25
12.1	RMS Functionality Validation	25
12.1.1	<i>Accessing Azure Active Directory Rights Management (AADRM)</i>	25
12.1.2	<i>Office Integration with Rights Management</i>	26
Appendix 1 – Verifying MSODS IPv6 Functionality		27
Appendix 2 – Verifying Exchange Online Protection (EOP) Functionality		28
Appendix 3 – Verifying OrgID Functionality		29
Appendix 4 – Verifying DNS Functionality.....		30

1 Overview

The intent of this document is to provide a step-by-step plan for user-acceptance testing (UAT) and UAT results to ensure that customer network environments can connect with Office 365 production environments utilizing the IPv6 protocol. The tests outlined in this document will validate the capability of a customer environment to connect via IPv6 to Microsoft's Office 365 instances of Exchange Online (EXO), SharePoint Online (SPO), Lync-Online (LYO), Web Access Client (WAC), Self-Serve Password Reset (SSPR) and other Office 365 component services as detailed in the plan.

Each test case should achieve the expected results and provide further information concerning the user scenario, as well as any additional comments or information.

Conventions

1. Text in `Courier New` should be typed without modification
2. Substitute the customer vanity name throughout the document for `contoso.com`.

Document Non-Goals

It is not a goal of this document to describe and test IPv6 future functionality listed below.

1. Purchasing licenses and manage subscriptions.

2 Environment Requirements

2.1 *Test Accounts*

A minimum of three Office 365 test client accounts are required to validate end to end services connectivity over IPv6. Additional accounts can be set up as needed.

2.2 *Client Configuration*

Customers should set up test clients to validate that their currently deployed operating system and browser stack will work as expected. For the purpose of the test, it is expected that the client systems will be using either Windows 7 or Windows 8 and will be configured with Internet Explorer 8 at least.

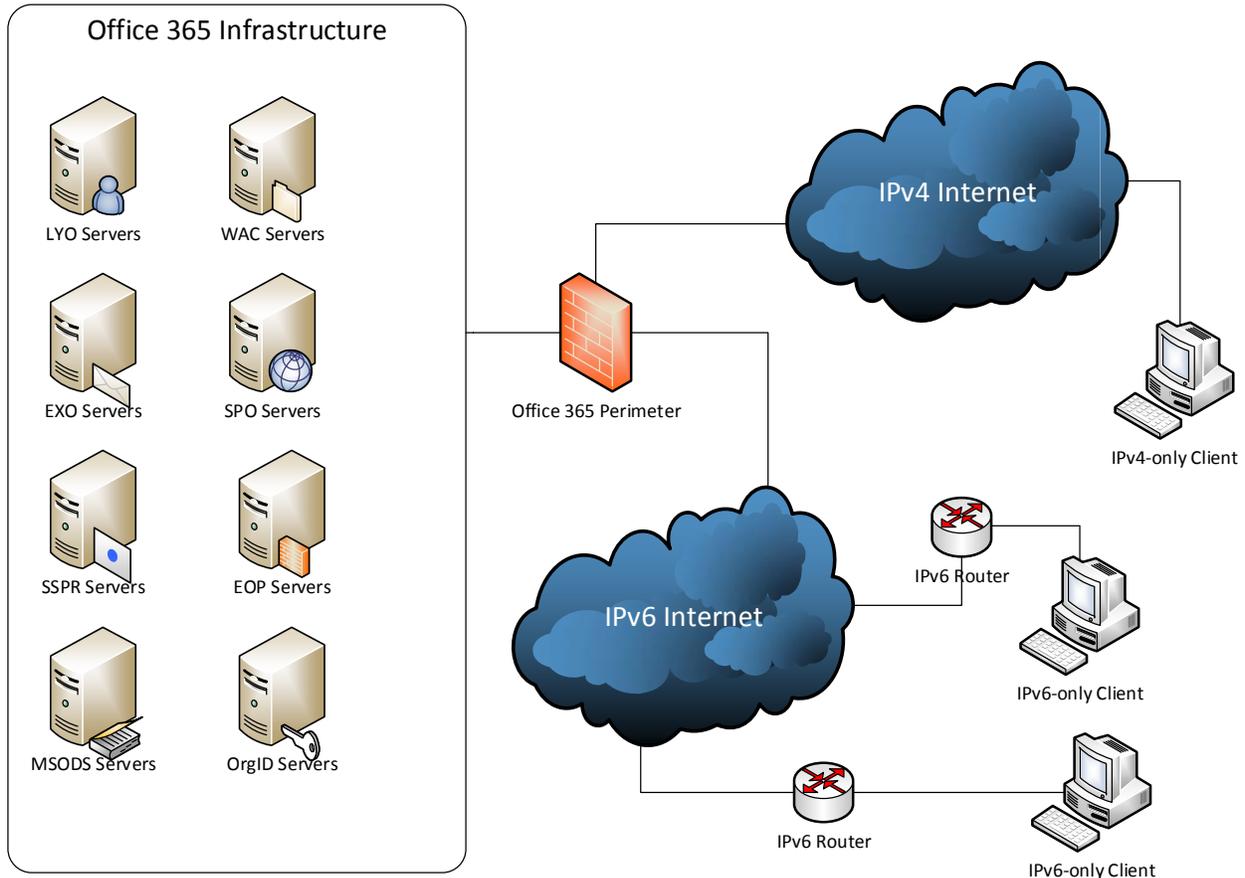
2.3 *Network Configuration*

2.3.1 Proposed Network Design

The following diagram illustrates the proposed design of the test lab network. It is assumed that all testing would be performed within a network simulating the following:

- 1) The IPv4 Internet;
- 2) The IPv6 Internet;
- 3) The Office 365 perimeter infrastructure; and
- 4) The Office 365 internal services infrastructure.

IPv6 Test Lab Configuration



2.3.2 IPv6-Capable Network Equipment

The network must be configured with network equipment that is capable of and configured to support both IPv4 and IPv6. Also, it is assumed that the perimeter will emulate the hardware based communications solution that has been configured to allow IPv6 clients to connect to the Office 365 Exchange Online services.

2.3.3 IPv6 Only Clients

The simulated IPv6 Internet will include at least *two* clients to ensure communications between each other via Office 365 services. Two or more test clients are ideal as they will allow additional client configuration testing and limit the amount of switching between accounts otherwise required with a single client.

2.3.4 IPv4 Only Clients

A minimum of one test client is needed on the simulated IPv4 Internet. Two or more test clients are ideal as they will allow additional client configuration testing and limit the amount of switching between accounts otherwise required with a single client.

3 Client Validation

3.1 *Routable IPv6 Address*

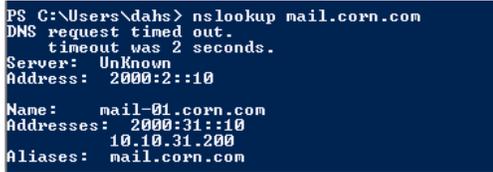
Test case number	
User scenario	Ensure that clients connected to the IPv6 Internet have a routable IPv6 address
Method	<ol style="list-style-type: none"> 1. Open PowerShell 2. Verify client adapter configuration: Type <code>ipconfig -all</code>
Expected results	<ol style="list-style-type: none"> 1. Validate that the client has a preferred routable IPv6 Address on the standard adapter: "IPv6 Address" 2. Validate that the client has a IPv6 default gateway: "Default Gateway"
Pass/fail	
Observed results	
Environment	
Comments or information	

3.2 *Routable IPv4 addresses*

Test case number	
User scenario	Ensure that clients connected to the IPv4 Internet have a routable IPv4 address only
Method	<ol style="list-style-type: none"> 3. Open PowerShell 4. Verify client adapter configuration: Type <code>ipconfig -all</code>
Expected results	<ol style="list-style-type: none"> 1. Validate that the client has a routable IPv4 Address: "IPv4 Address" 2. Validate that the client has a IPv4 default gateway: "Default Gateway" 3. Validate the client has <i>no</i> routable IPv6 address configured.
Pass/fail	
Observed results	
Environment	
Comments or information	

4 DNS Validation

4.1 DNS Records

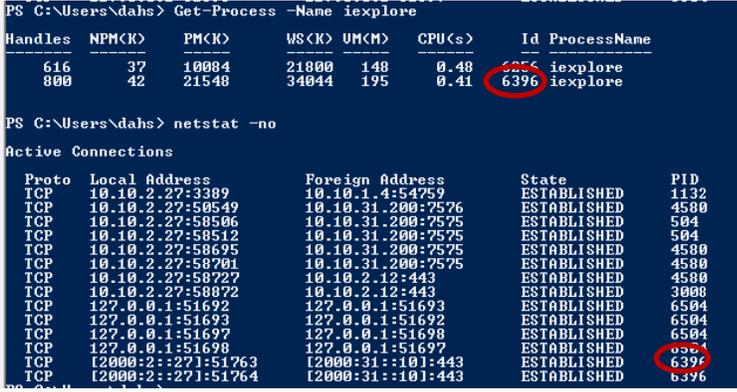
Test case number	
User scenario	Validate user is receiving A and AAAA records
Method	<ol style="list-style-type: none"> 1. Open PowerShell 2. Type: <code>nslookup mail.contoso.com</code> substituting the customer vanity name.  <pre>PS C:\Users\dahs> nslookup mail.corn.com DNS request timed out. timeout was 2 seconds. Server: Unknown Address: 2000:2::10 Name: mail-01.corn.com Addresses: 2000:31::10 10.10.31.200 Aliases: mail.corn.com</pre>
Expected results	<ol style="list-style-type: none"> 1. IPv6-only client(s) receives a routable IPv6 address. 2. IPv4-only client(s) receives a routable IPv4 address.
Pass/fail	
Observed results	
Environment	
Comments or information	

5 Exchange Online (EXO) Access and Functionality Validation

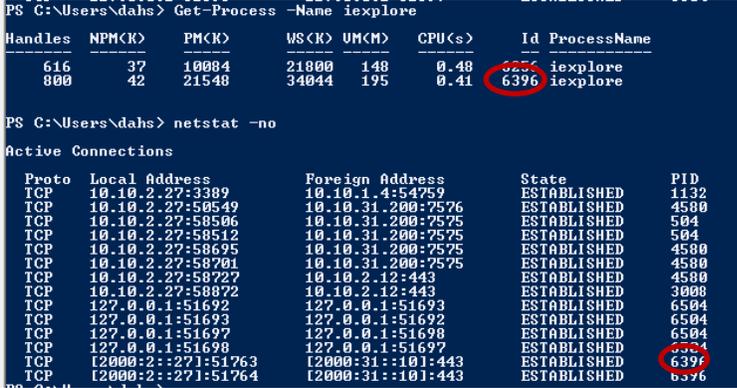
5.1 Mail Connection Validation

5.1.1 Outlook Web Access

5.1.1.1 Single Factor Authentication

Test case number	
User scenario	Validate user is able to connect to Outlook Web Access over IPv6
Method	<ol style="list-style-type: none"> From the IPv6-only client, open PowerShell Open Internet Browser to a blank page Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> Open Task Manager and identify the process Open PowerShell Enter: <code>Get-Process -Name iexplore</code> In the Internet Browser type: <code>https://outlook.office365.com/owa/contoso.com</code> In PowerShell type: <code>netstat -no</code> Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6  <pre> PS C:\Users\dahs> Get-Process -Name iexplore Handles NPM(K) PM(K) WS(K) UM(K) CPU(s) Id ProcessName ----- 616 37 10084 21800 148 0.48 6396 iexplore 800 42 21548 34044 195 0.41 6397 iexplore PS C:\Users\dahs> netstat -no Active Connections Proto Local Address Foreign Address State PID TCP 10.10.2.27:3389 10.10.1.4:54759 ESTABLISHED 1132 TCP 10.10.2.27:50549 10.10.31.200:7576 ESTABLISHED 4500 TCP 10.10.2.27:58506 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58512 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58695 10.10.31.200:7575 ESTABLISHED 4500 TCP 10.10.2.27:58701 10.10.31.200:7575 ESTABLISHED 4500 TCP 10.10.2.27:58727 10.10.2.12:443 ESTABLISHED 4500 TCP 10.10.2.27:58872 10.10.2.12:443 ESTABLISHED 3008 TCP 127.0.0.1:51692 127.0.0.1:51693 ESTABLISHED 6504 TCP 127.0.0.1:51693 127.0.0.1:51692 ESTABLISHED 6504 TCP 127.0.0.1:51697 127.0.0.1:51698 ESTABLISHED 6504 TCP 127.0.0.1:51698 127.0.0.1:51697 ESTABLISHED 6396 TCP [2000:2::27]:51763 [2000:31::101]:443 ESTABLISHED 6397 TCP [2000:2::27]:51764 [2000:31::101]:443 ESTABLISHED 6396 </pre>
Expected results	Internet Browser accesses OWA over IPv6
Pass/fail	
Observed results	
Environment	
Comments or information	

5.1.1.2 Two Factor Authentication

Test case number	
User scenario	Log-in using 2FA
Method	<ol style="list-style-type: none"> 1. From the IPv6-only client, open PowerShell 2. Open Internet Browser to a blank page 3. Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> a. Open Task Manager and identify the process b. Open PowerShell c. Depending on which browser is used d. Enter: <code>Get-Process -Name iexplore</code> 4. In Internet Browser type in the secure mail URL: <code>https://outlook.office365.com/owa/contoso.com</code> 5. Ensure that the 2FA Authentication page is displayed 6. In PowerShell type: <code>netstat -no</code> 7. Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6  <pre> PS C:\Users\dahs> Get-Process -Name iexplore Handles NPM(K) PM(K) WS(K) UM(M) CPU(s) Id ProcessName ----- 616 37 10084 21800 148 0.48 6256 iexplore 800 42 21548 34044 195 0.41 6396 iexplore PS C:\Users\dahs> netstat -no Active Connections Proto Local Address Foreign Address State PID ---- TCP 10.10.2.27:3389 10.10.1.4:54759 ESTABLISHED 1132 TCP 10.10.2.27:50549 10.10.31.200:7576 ESTABLISHED 4500 TCP 10.10.2.27:58506 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58512 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58695 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58701 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58727 10.10.2.12:443 ESTABLISHED 4580 TCP 10.10.2.27:58872 10.10.2.12:443 ESTABLISHED 3008 TCP 127.0.0.1:51692 127.0.0.1:51693 ESTABLISHED 6504 TCP 127.0.0.1:51693 127.0.0.1:51692 ESTABLISHED 6504 TCP 127.0.0.1:51697 127.0.0.1:51698 ESTABLISHED 6504 TCP 127.0.0.1:51698 127.0.0.1:51697 ESTABLISHED 6396 TCP [2000:2::27]:51763 [2000:31::10]:443 ESTABLISHED 6396 TCP [2000:2::27]:51764 [2000:31::10]:443 ESTABLISHED 6396 </pre> <ol style="list-style-type: none"> 8. Log-in to Account using an account that is enabled for 2FA
Expected results	User is able to log-in using 2FA to OWA
Pass/fail	
Observed results	
Environment	
Comments or information	

5.2 Mail Functionality Validation

5.2.1 Outlook Web Access

Test case number	
User scenario	Validate mail flow in OWA
Method	<p>Single Factor Authentication (Dual Stack or IPv6 Only Clients)</p> <ol style="list-style-type: none"> 1. Ensure that all protocol validation tests are completed and OWA is working over IPv6 for both client machines. 2. Log-In to OWA with "Test User 1 (TU1)" on "Client1" 3. Log-in to OWA with "Test user 2 (TU2)" on "Client2" 4. Send email from TU1 to TU2 and validate receipt. 5. Send a calendar invite from TU2 to TU1 and validate receipt <p>Two Factor Authentication (Dual Stack or IPv6 Only Clients)</p> <ol style="list-style-type: none"> 1. Ensure that all protocol validation tests are completed and OWA is working over IPv6 for both client machines. 2. Log-In to OWA with "Test User 3 (TU3)" on "Client1". Ensure that TU3 is set up for 2FA. 3. Log-in to OWA with "Test user 4 (TU4)" on "Client2". Ensure that TU4 is set up for 2FA. 4. Send email from TU3 to TU4 and validate receipt. 5. Send a calendar invite from TU4 to TU3 and validate receipt
Expected results	<ol style="list-style-type: none"> 1. User is able to log-in using single factor authentication and send/receive mail 2. User is able to log-in using two factor authentication and send/receive mail
Pass/fail	
Observed results	
Environment	
Comments or information	

6 SharePoint Online (SPO) Access and Functionality Validation

6.1 SharePoint Online Access

6.1.1 Accessing the SPO Server

Test case number	
User scenario	Validate user is able to connect to SPO over IPv6
Method	<ol style="list-style-type: none"> 1. From the IPv6-only client, open PowerShell 2. Open Internet Browser to a blank page 3. Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> a. Open Task Manager and identify the process b. Open PowerShell c. Enter: <code>Get-Process -Name iexplore</code> 4. In the Internet Browser type: <code>https://contoso.sharepoint.com/</code> 5. In PowerShell type: <code>netstat -no</code> 6. Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6
Expected results	User accesses SPO over IPv6
Pass/fail	
Observed results	
Environment	
Comments or information	

```

PS C:\Users\dahs> Get-Process -Name iexplore
Handles  NPM(K)  PM(K)  WS(K)  UM(M)  CPU(s)  Id  ProcessName
-----  -
616     37     10004  21800  148    0.48    6236 iexplore
800     42     21548  34044  195    0.41    6396 iexplore

PS C:\Users\dahs> netstat -no
Active Connections
Proto Local Address           Foreign Address         State           PID
----  -
TCP    10.10.2.27:3389         10.10.1.4:54259         ESTABLISHED    1132
TCP    10.10.2.27:50549        10.10.31.200:7575       ESTABLISHED    4580
TCP    10.10.2.27:58506        10.10.31.200:7575       ESTABLISHED    504
TCP    10.10.2.27:58512        10.10.31.200:7575       ESTABLISHED    504
TCP    10.10.2.27:58695        10.10.31.200:7575       ESTABLISHED    4580
TCP    10.10.2.27:58701        10.10.31.200:7575       ESTABLISHED    4580
TCP    10.10.2.27:58727        10.10.2.12:443          ESTABLISHED    4580
TCP    10.10.2.27:58872        10.10.2.12:443          ESTABLISHED    3000
TCP    127.0.0.1:51692         127.0.0.1:51693         ESTABLISHED    6504
TCP    127.0.0.1:51693         127.0.0.1:51692         ESTABLISHED    6504
TCP    127.0.0.1:51697         127.0.0.1:51698         ESTABLISHED    6504
TCP    127.0.0.1:51698         127.0.0.1:51697         ESTABLISHED    6504
TCP    [2000:2::27]:51763      [2000:31::101]:443      ESTABLISHED    6396
TCP    [2000:2::27]:51764      [2000:31::101]:443      ESTABLISHED    6396
    
```

6.1.2 Document Management

Test case number	
User scenario	User can create and manage documents over IPv6 (i.e. open/edit/save Word/Excel/PPT/OneNote)
Method	<ol style="list-style-type: none"> 1. Ensure that all protocol validation tests are completed and SPO is working over IPv6 client machines. 2. Log-In to SPO, and open any Document Library. <code>https://contoso.sharepoint.com/Shared Documents</code> 3. Create the New Document in the Document tab of the SharePoint Ribbon. 4. Save it in the Document Library, and validate the document has been saved successfully.
Expected results	User can create and manage documents on SPO over IPv6
Pass/fail	
Observed results	
Environment	
Comments or information	

7 Lync Online Access and Functionality Validation

7.1 Lync Online Access

7.1.1 Accessing the Lync Server

Test case number	
User scenario	User on IPv6 client signs into Lync Online
Method	<ol style="list-style-type: none"> 1. From the IPv6-only client, open PowerShell 2. Log-In to Lync using Lync 15 desktop client 3. Identify the Process ID that the Lync Client is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> a. Open Task Manager and identify the process b. Open PowerShell c. Enter: <code>Get-Process -Name Lync</code> 4. In PowerShell type: <code>netstat -no</code> 5. Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6
Expected results	User can successfully log into Lync on an IPv6 client.
Pass/fail	
Observed results	
Environment	
Comments or information	Clients need to be configured with an IPv6-capable web proxy (NOTE: SQUID has this capability)

7.1.2 Lync Functionality

Test case number	
User scenario	Users on the IPV6 clients add each other to their contact list
Method	<ol style="list-style-type: none"> 1. Ensure that all protocol validation tests are completed and Lync is working over IPv6 client machines. 2. Log-In to Lync using Lync 15 desktop client with "Test User 1 (TU1)" on "Client1" 3. Log-In to Lync using Lync 15 desktop client with "Test user 2 (TU2)" on "Client2" 4. Search and Add TU2 into a contact list on TU1 and validate the contact list. 5. Search and Add TU1 into a contact list on TU2 and validate the contact list.
Expected results	Both users successfully add a user located on an IPv6 client
Pass/fail	
Observed results	
Environment	
Comments or information	<ul style="list-style-type: none"> • User 1 and 2 must be on separate IPv6 subnets with an IPv6 capable router between them to eliminate any factors being in the same subnet may introduce.

Test case number	
User scenario	A user on the IPV6 client creates and manages a meeting with users on IPv4- and IPv6-only clients
Method	<ol style="list-style-type: none"> 1. Ensure that the protocol validation tests are completed and Lync is working over IPv6 on "Test user 1 (TU1)" on "Client1" machines. 2. Ensure that the protocol validation tests are completed and Lync is working over IPv6 on "Test user 2 (TU2)" on "Client2" machines. 3. Ensure that the protocol validation tests are completed and Lync is working over IPv4 on "Test user 3 (TU3)" on "Client3" machines. 3. Log-In to Lync using Lync 15 desktop client with "Test User 1 (TU1)" on "Client1" 4. Log-In to Lync using Lync 15 desktop client with "Test user 2 (TU2)" on "Client2" 5. In the TU1 Lync main window, press Alt, and then click "Meet Now" and start AV conference. 6. In the TU1 conversation window, invite TU2 to join the AV conference. 7. In the TU2 conversation window, click Share and desktop, and validate TU1 is able to see the shared desktop. 8. In the TU1 conversation window, click Share and click PowerPoint Presentation, and validate TU2 is able to see the PPT. 9. Log-In to Lync using Lync 14 desktop client with "Test user 3 (TU3)" on "Client3" 10. In the TU1 conversation window, invite TU3 to join the AV conference. 11. Validate TU3 is able to join and see the current AV conference including the shared desktop and PPT. 12. Validate TU1 and TU2 are able to see all 3 participants in the conference.

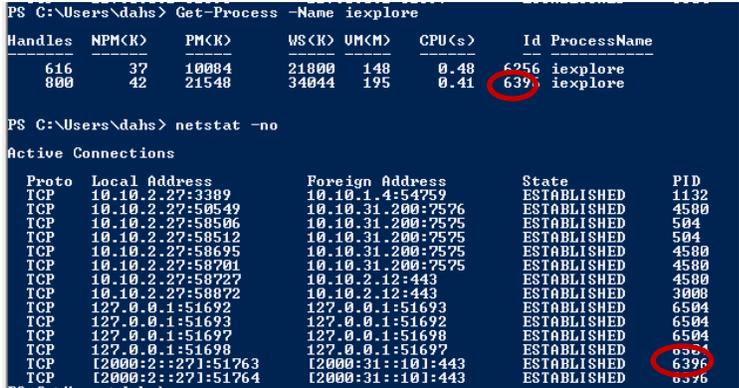
Expected results	Users on IPv6 clients can fully interact with other users on IPv4- and IPv6-only clients using Lync.
Pass/fail	
Observed results	
Environment	
Comments or information	<ul style="list-style-type: none"> All Internet-emulating subnets have direct connectivity to each other as well as via the Lync Online infrastructure.

Test case number	
User scenario	A user on the IPV6 client uses Outlook to schedule a Lync meeting with users on IPv4- and IPv6-only clients
Method	<ol style="list-style-type: none"> 1. Ensure that the protocol validation tests are completed and Lync and Outlook are working over IPv6 on "Test user 1 (TU1)" on "Client1" machines. 2. Ensure that the protocol validation tests are completed and Lync and Outlook are working over IPv6 on "Test user 2 (TU2)" on "Client2" machines. 3. Ensure that the protocol validation tests are completed and Lync and Outlook are working over IPv4 on "Test user 3 (TU3)" on "Client3" machines. 13. Log-In to Lync using Lync 15 desktop client with "Test User 1 (TU1)" on "Client1", and launch Outlook 2013. 14. Log-In to Lync using Lync 15 desktop client with "Test user 2 (TU2)" on "Client2" 15. Log-In to Lync using Lync 14 desktop client with "Test user 3 (TU3)" on "Client3" 16. In the TU1 Outlook Calendar, on the Home tab, click New Online Meeting, and send the meeting invitation to TU2 and TU3. 17. Validate TU1, TU2, and TU3 are able to join the conference from the meeting invitation.
Expected results	User on an IPv6 client can successfully schedule a Lync meeting using their Outlook application.
Pass/fail	
Observed results	
Environment	
Comments or information	<ul style="list-style-type: none"> All clients must be running Outlook 2013 and connected to an O365 infrastructure The O365 infrastructure must be in place and configured to connect to the Lync Online infrastructure for the lab environment and each user has a mailbox. It is not necessary for the users to have mailboxes on separate systems.

8 Web Application Companion (WAC) Access and Functionality Validation

8.1 WAC Access

8.1.1 Accessing Files with WAC

Test case number	
User scenario	Validate user is able to connect to Office Web Apps over IPv6
Method	<ol style="list-style-type: none"> From the IPv6-only client, open PowerShell Open Internet Browser to a blank page Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> Open Task Manager and identify the process Open PowerShell Enter: <code>Get-Process -Name iexplore</code> In the Internet Browser type: <code>https://contoso.sharepoint.com/</code> In PowerShell type: <code>netstat -no</code> Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6  <pre> PS C:\Users\dahs> Get-Process -Name iexplore Handles NPM(K) PM(K) WS(K) VM(M) CPU(s) Id ProcessName ----- 616 37 10004 21000 148 0.48 6256 iexplore 800 42 21548 34044 195 0.41 6396 iexplore PS C:\Users\dahs> netstat -no Active Connections Proto Local Address Foreign Address State PID TCP 10.10.2.27:3389 10.10.1.4:54259 ESTABLISHED 1132 TCP 10.10.2.27:50549 10.10.31.200:7576 ESTABLISHED 4500 TCP 10.10.2.27:58506 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58512 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58695 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58701 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58727 10.10.2.12:443 ESTABLISHED 4580 TCP 10.10.2.27:58872 10.10.2.12:443 ESTABLISHED 3000 TCP 127.0.0.1:51692 127.0.0.1:51693 ESTABLISHED 6504 TCP 127.0.0.1:51693 127.0.0.1:51692 ESTABLISHED 6504 TCP 127.0.0.1:51697 127.0.0.1:51698 ESTABLISHED 6504 TCP 127.0.0.1:51698 127.0.0.1:51697 ESTABLISHED 6504 TCP [2000:2::27]:51763 [2000:31::101]:443 ESTABLISHED 6396 TCP [2000:2::27]:51764 [2000:31::101]:443 ESTABLISHED 6396 </pre>
Expected results	User accesses Office Web Apps over IPv6
Pass/fail	
Observed results	
Environment	
Comments or information	

8.1.2 WAC Functionality

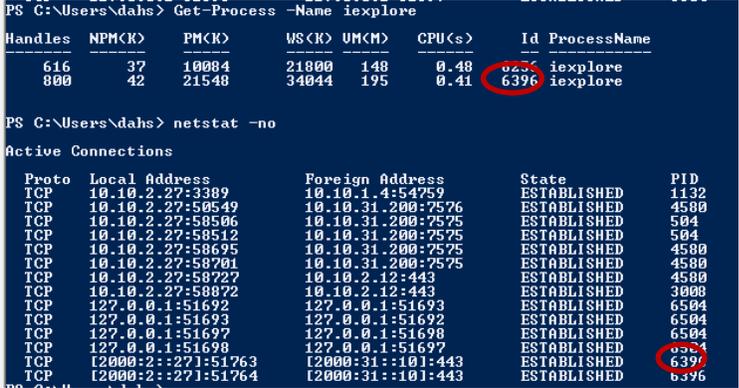
Test case number	
User scenario	User accesses the range of available Office files, is able to make changes and save them through SPO.
Method	<ol style="list-style-type: none"> 1. Ensure that all protocol validation tests are completed and Office Web Apps is working over IPv6 client machines. 2. Log-In to SPO, and open any Document Library. https://contoso.sharepoint.com/Shared Documents 3. Load a WORD document, and validate that you are able to scroll to the end, edit, and save the document. 4. Load an EXCEL document, and validate that you are able to fully interact with the spreadsheet. 5. Load a PowerPoint presentation, and validate that you are able to view, edit, and save the presentation. 6. Load an OneNote notebook, and validate that you are able to view, edit, save, and sync changes between more than one clients.
Expected results	Users on an IPv6 client can successfully work with the entire range of Office files and save them through SPO.
Pass/fail	
Observed results	
Environment	
Comments or information	.

Test case number	
User scenario	User accesses the range of available Office files, is able to fully interact through EXO.
Method	<ol style="list-style-type: none"> 7. Ensure that all protocol validation tests are completed and Office Web Apps is working over IPv6 client machines. 8. Log-In to EXO, and open any email with Office Document attached. https://outlook.office365.com/owa/contoso.com 9. Click "Preview" and load a WORD document, and validate that you are able to fully interact with the document. 10. Click "Preview" and load an EXCEL document, and validate that you are able to fully interact with the spreadsheet. 11. Click "Preview" and load PowerPoint presentation, and validate that you are able to fully interact with the presentation. 12. Load an OneNote notebook, and validate that you are able to view, edit, save, and sync changes between more than one clients.
Expected results	Users on an IPv6 client can successfully work with the entire range of Office files and save them through EXO.
Pass/fail	
Observed results	
Environment	
Comments or information	.

9 Self Service Password Reset (SSPR) Functionality Validation

9.1 SSPR Functionality

9.1.1 Accessing the Password Reset Portal

Test case number	
User scenario	Validate user is able to connect to Reset Password Portal over IPv6
Method	<ol style="list-style-type: none"> 1. From the IPv6-only client, open PowerShell 2. Open Internet Browser to a blank page 3. Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> a. Open Task Manager and identify the process b. Open PowerShell c. Enter: <code>Get-Process -Name iexplore</code> 4. In the Internet Browser type: <code>https://passwordreset.microsoftonline.com/</code> 5. In PowerShell type: <code>netstat -no</code> 6. Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6  <pre> PS C:\Users\dahs> Get-Process -Name iexplore Handles NPM(K) PM(K) WS(K) UM(M) CPU(s) Id ProcessName ----- 616 37 10004 21800 148 0.48 6236 iexplore 800 42 21548 34044 195 0.41 6396 iexplore PS C:\Users\dahs> netstat -no Active Connections Proto Local Address Foreign Address State PID TCP 10.10.2.27:3389 10.10.1.4:54259 ESTABLISHED 1132 TCP 10.10.2.27:50549 10.10.31.200:7576 ESTABLISHED 4580 TCP 10.10.2.27:58506 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58512 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58695 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58701 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58727 10.10.2.12:443 ESTABLISHED 4580 TCP 10.10.2.27:58872 10.10.2.12:443 ESTABLISHED 3000 TCP 127.0.0.1:51692 127.0.0.1:51693 ESTABLISHED 6504 TCP 127.0.0.1:51693 127.0.0.1:51692 ESTABLISHED 6504 TCP 127.0.0.1:51697 127.0.0.1:51698 ESTABLISHED 6504 TCP 127.0.0.1:51698 127.0.0.1:51697 ESTABLISHED 6504 TCP [2000:2::27]:51763 [2000:31::101:443 ESTABLISHED 6396 TCP [2000:2::27]:51764 [2000:31::101:443 ESTABLISHED 6396 </pre>
Expected results	Validate user is able to connect to Password Reset Portal over IPv6.
Pass/fail	
Observed results	
Environment	
Comments or information	

9.1.2 Resetting the Admin Password

Test case number	
User scenario	Client resets Office 365 Admin Password
Method	<ol style="list-style-type: none"> 1. Ensure that all protocol validation tests are completed and the portal is working over IPv6 client machines. 2. Access to Password Reset Portal. https://passwordreset.microsoftonline.com 3. Confirm "Yes, I am an administrator" and click "Next". 4. Validate that Captcha shows symbols properly. 5. Click reload button on the right side of Captcha, and validate Captcha symbols are regenerated properly. 6. Click audio button on the right side of Captcha, and validate the media file plays. 7. Click "abc" button to switch back to text Captcha, and enter an administrator's email address and Captcha text. Click "Next". An email containing instructions is sent to the alternate email address. 8. After receiving email to Alternate email address, click URL to reset password. 9. If the organization has a custom domain, or is using directory synchronization, a security code is sent to your mobile phone thru SMS. Otherwise, skip to Step 11. 10. In the wizard, on the Mobile phone verification page, type the Security code you received on your mobile phone, and click "Next". 11. On the Create a new password page, type a new password, confirm the new password, and click "Finish". 12. When the password has been reset, click the link in the wizard to return to Office 365 and validate log-in with new password.
Expected results	Administrator can successfully reset their password over IPv6.
Pass/fail	
Observed results	
Environment	
Comments or information	

10 BOX Functionality Validation

10.1 BOX Functionality

10.1.1 Accessing the Office 365 Admin Portal

Test case number	
User scenario	Validate user is able to connect to Office 365 Admin Portal over IPv6
Method	<ol style="list-style-type: none"> 1. From the IPv6-only client, open PowerShell 2. Open Internet Browser to a blank page 3. Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> a. Open Task Manager and identify the process b. Open PowerShell c. Enter: Get-Process -Name iexplore 4. In the Internet Browser type: https://portal.microsoftonline.com/ 5. In PowerShell type: netstat -no 6. Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6
Expected results	Validate user is able to connect to Office 365 Admin Portal over IPv6.
Pass/fail	
Observed results	
Environment	
Comments or information	

```
PS C:\Users\dahs> Get-Process -Name iexplore
```

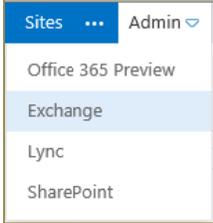
Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName
616	37	10084	21800	148	0.48	6396	iexplore
800	42	21548	34044	195	0.41	6396	iexplore

```
PS C:\Users\dahs> netstat -no
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	10.10.2.27:3389	10.10.1.4:54759	ESTABLISHED	1132
TCP	10.10.2.27:50549	10.10.31.200:7576	ESTABLISHED	4580
TCP	10.10.2.27:58506	10.10.31.200:7575	ESTABLISHED	504
TCP	10.10.2.27:58512	10.10.31.200:7575	ESTABLISHED	504
TCP	10.10.2.27:58695	10.10.31.200:7575	ESTABLISHED	4580
TCP	10.10.2.27:58701	10.10.31.200:7575	ESTABLISHED	4580
TCP	10.10.2.27:58727	10.10.2.12:443	ESTABLISHED	4580
TCP	10.10.2.27:58872	10.10.2.12:443	ESTABLISHED	3000
TCP	127.0.0.1:51692	127.0.0.1:51693	ESTABLISHED	6504
TCP	127.0.0.1:51693	127.0.0.1:51692	ESTABLISHED	6504
TCP	127.0.0.1:51697	127.0.0.1:51698	ESTABLISHED	6504
TCP	127.0.0.1:51698	127.0.0.1:51697	ESTABLISHED	6504
TCP	[2000:2::27]:51763	[2000:31::101]:443	ESTABLISHED	6396
TCP	[2000:2::27]:51764	[2000:31::101]:443	ESTABLISHED	6396

10.1.2 Manage User Provisioning and Password

Test case number	
User scenario	Manage user provisioning and password in Office 365 Admin Portal
Method	<ol style="list-style-type: none"> 1. Ensure that all protocol validation tests are completed and the portal is working over IPv6 client machines. 2. Access the Office 365 Admin Portal, and log-in using administrator account. https://portal.microsoftonline.com/ 3. Validate admin is able to see "Service Overview" and click each tab "service health", "service requests", "inactive email users", and "mail protection". 4. Click "user and groups" on the left, and validate that admin is able to create new user and edit the properties. 5. Select a user and click "Reset Password" on the right "quick steps", and validate admin is able to reset password. 6. Click "domain" on the left, and validate admin is able to add and verify custom domain which hosts AAAA records in the DNS. 7. Click "Admin" in the right corner, and validate admin is able to launch console for each service; "Exchange", "Lync", and "SharePoint".  <ol style="list-style-type: none"> 8. Click your account name on the right corner and click sign out, and validate admin is able to sign out.
Expected results	Administrator can successfully manage Office 365 Admin Portal over IPv6.
Pass/fail	
Observed results	
Environment	
Comments or information	

11 Office Functionality Validation

11.1 Office Functionality

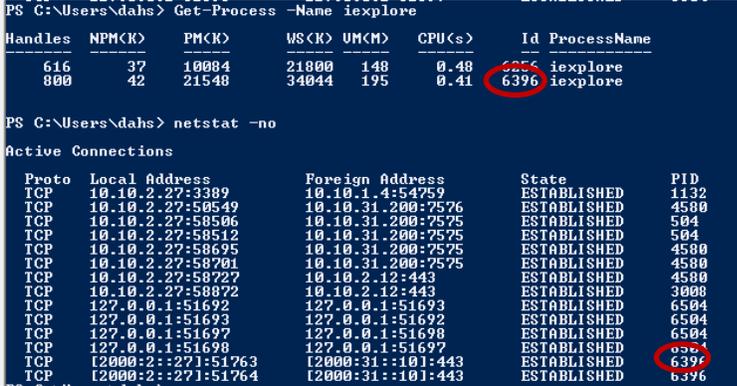
11.1.1 Installing Office 2013 from Office 365 Portal

Test case number																																																																																																				
User scenario	Validate user is able to install Office 2013 over IPv6																																																																																																			
Method	<ol style="list-style-type: none"> 1. From the IPv6-only client, open PowerShell 2. Open Internet Browser to a blank page 3. Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> a. Open Task Manager and identify the process b. Open PowerShell c. Enter: Get-Process -Name iexplore 4. In the Internet Browser type: <code>https://portal.microsoftonline.com/</code> 5. In PowerShell type: <code>netstat -no</code> 6. Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6 <div data-bbox="581 961 1323 1354" data-label="Code-Block"> <pre>PS C:\Users\dahs> Get-Process -Name iexplore</pre> <table border="1"> <thead> <tr> <th>Handles</th> <th>NPM(K)</th> <th>PM(K)</th> <th>WS(K)</th> <th>UM(M)</th> <th>CPU(s)</th> <th>Id</th> <th>ProcessName</th> </tr> </thead> <tbody> <tr> <td>616</td> <td>37</td> <td>10084</td> <td>21800</td> <td>148</td> <td>0.48</td> <td>6396</td> <td>iexplore</td> </tr> <tr> <td>800</td> <td>42</td> <td>21548</td> <td>34044</td> <td>195</td> <td>0.41</td> <td>6396</td> <td>iexplore</td> </tr> </tbody> </table> <pre>PS C:\Users\dahs> netstat -no</pre> <p>Active Connections</p> <table border="1"> <thead> <tr> <th>Proto</th> <th>Local Address</th> <th>Foreign Address</th> <th>State</th> <th>PID</th> </tr> </thead> <tbody> <tr> <td>TCP</td> <td>10.10.2.27:3389</td> <td>10.10.1.4:54759</td> <td>ESTABLISHED</td> <td>1132</td> </tr> <tr> <td>TCP</td> <td>10.10.2.27:50549</td> <td>10.10.31.200:7576</td> <td>ESTABLISHED</td> <td>4580</td> </tr> <tr> <td>TCP</td> <td>10.10.2.27:58506</td> <td>10.10.31.200:7575</td> <td>ESTABLISHED</td> <td>504</td> </tr> <tr> <td>TCP</td> <td>10.10.2.27:58512</td> <td>10.10.31.200:7575</td> <td>ESTABLISHED</td> <td>504</td> </tr> <tr> <td>TCP</td> <td>10.10.2.27:58695</td> <td>10.10.31.200:7575</td> <td>ESTABLISHED</td> <td>4580</td> </tr> <tr> <td>TCP</td> <td>10.10.2.27:58701</td> <td>10.10.31.200:7575</td> <td>ESTABLISHED</td> <td>4580</td> </tr> <tr> <td>TCP</td> <td>10.10.2.27:58727</td> <td>10.10.2.12:443</td> <td>ESTABLISHED</td> <td>4580</td> </tr> <tr> <td>TCP</td> <td>10.10.2.27:58872</td> <td>10.10.2.12:443</td> <td>ESTABLISHED</td> <td>3000</td> </tr> <tr> <td>TCP</td> <td>127.0.0.1:51692</td> <td>127.0.0.1:51693</td> <td>ESTABLISHED</td> <td>6504</td> </tr> <tr> <td>TCP</td> <td>127.0.0.1:51693</td> <td>127.0.0.1:51692</td> <td>ESTABLISHED</td> <td>6504</td> </tr> <tr> <td>TCP</td> <td>127.0.0.1:51697</td> <td>127.0.0.1:51698</td> <td>ESTABLISHED</td> <td>6504</td> </tr> <tr> <td>TCP</td> <td>127.0.0.1:51698</td> <td>127.0.0.1:51697</td> <td>ESTABLISHED</td> <td>6504</td> </tr> <tr> <td>TCP</td> <td>[2000:2::27]:51763</td> <td>[2000:31::101]:443</td> <td>ESTABLISHED</td> <td>6396</td> </tr> <tr> <td>TCP</td> <td>[2000:2::27]:51764</td> <td>[2000:31::101]:443</td> <td>ESTABLISHED</td> <td>6396</td> </tr> </tbody> </table> </div> 7. Click "Office 365 Settings" in the right corner, and select "Software" tab. 8. Select Language and version, and click "install" to validate user is able to install Office programs. 	Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName	616	37	10084	21800	148	0.48	6396	iexplore	800	42	21548	34044	195	0.41	6396	iexplore	Proto	Local Address	Foreign Address	State	PID	TCP	10.10.2.27:3389	10.10.1.4:54759	ESTABLISHED	1132	TCP	10.10.2.27:50549	10.10.31.200:7576	ESTABLISHED	4580	TCP	10.10.2.27:58506	10.10.31.200:7575	ESTABLISHED	504	TCP	10.10.2.27:58512	10.10.31.200:7575	ESTABLISHED	504	TCP	10.10.2.27:58695	10.10.31.200:7575	ESTABLISHED	4580	TCP	10.10.2.27:58701	10.10.31.200:7575	ESTABLISHED	4580	TCP	10.10.2.27:58727	10.10.2.12:443	ESTABLISHED	4580	TCP	10.10.2.27:58872	10.10.2.12:443	ESTABLISHED	3000	TCP	127.0.0.1:51692	127.0.0.1:51693	ESTABLISHED	6504	TCP	127.0.0.1:51693	127.0.0.1:51692	ESTABLISHED	6504	TCP	127.0.0.1:51697	127.0.0.1:51698	ESTABLISHED	6504	TCP	127.0.0.1:51698	127.0.0.1:51697	ESTABLISHED	6504	TCP	[2000:2::27]:51763	[2000:31::101]:443	ESTABLISHED	6396	TCP	[2000:2::27]:51764	[2000:31::101]:443	ESTABLISHED	6396
Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName																																																																																													
616	37	10084	21800	148	0.48	6396	iexplore																																																																																													
800	42	21548	34044	195	0.41	6396	iexplore																																																																																													
Proto	Local Address	Foreign Address	State	PID																																																																																																
TCP	10.10.2.27:3389	10.10.1.4:54759	ESTABLISHED	1132																																																																																																
TCP	10.10.2.27:50549	10.10.31.200:7576	ESTABLISHED	4580																																																																																																
TCP	10.10.2.27:58506	10.10.31.200:7575	ESTABLISHED	504																																																																																																
TCP	10.10.2.27:58512	10.10.31.200:7575	ESTABLISHED	504																																																																																																
TCP	10.10.2.27:58695	10.10.31.200:7575	ESTABLISHED	4580																																																																																																
TCP	10.10.2.27:58701	10.10.31.200:7575	ESTABLISHED	4580																																																																																																
TCP	10.10.2.27:58727	10.10.2.12:443	ESTABLISHED	4580																																																																																																
TCP	10.10.2.27:58872	10.10.2.12:443	ESTABLISHED	3000																																																																																																
TCP	127.0.0.1:51692	127.0.0.1:51693	ESTABLISHED	6504																																																																																																
TCP	127.0.0.1:51693	127.0.0.1:51692	ESTABLISHED	6504																																																																																																
TCP	127.0.0.1:51697	127.0.0.1:51698	ESTABLISHED	6504																																																																																																
TCP	127.0.0.1:51698	127.0.0.1:51697	ESTABLISHED	6504																																																																																																
TCP	[2000:2::27]:51763	[2000:31::101]:443	ESTABLISHED	6396																																																																																																
TCP	[2000:2::27]:51764	[2000:31::101]:443	ESTABLISHED	6396																																																																																																
Expected results	User is able to install Office 2013 over IPv6																																																																																																			
Pass/fail																																																																																																				
Observed results																																																																																																				
Environment																																																																																																				
Comments or information	System requirements for Office 2013 and Office 365																																																																																																			

12 Rights Management Services Functionality Validation

12.1 RMS Functionality Validation

12.1.1 Accessing Azure Active Directory Rights Management (AADRM)

Test case number	
User scenario	Validate Admin is able to connect and enable RMS over IPv6
Method	<ol style="list-style-type: none"> From the IPv6-only client, open PowerShell Open Internet Browser to a blank page Identify the Process ID that the browser is running under. This can be accomplished in the following ways <ol style="list-style-type: none"> Open Task Manager and identify the process Open PowerShell Enter: <code>Get-Process -Name iexplore</code> In the Internet Browser type: <code>https://activedirectory.windowsazure.com/</code> In PowerShell type: <code>netstat -no</code> Identify the process(es) running under the Internet Browser PID and ensure that the "Local Address" and "Foreign Address" are IPv6  <pre> PS C:\Users\dahs> Get-Process -Name iexplore Handles NPM(K) PM(K) WS(K) UM(M) CPU(s) Id ProcessName ----- 616 37 10084 21800 148 0.48 6256 iexplore 800 42 21548 34044 195 0.41 6396 iexplore PS C:\Users\dahs> netstat -no Active Connections Proto Local Address Foreign Address State PID ---- TCP 10.10.2.27:3389 10.10.1.4:54759 ESTABLISHED 1132 TCP 10.10.2.27:50549 10.10.31.200:7576 ESTABLISHED 4580 TCP 10.10.2.27:58506 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58512 10.10.31.200:7575 ESTABLISHED 504 TCP 10.10.2.27:58695 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58701 10.10.31.200:7575 ESTABLISHED 4580 TCP 10.10.2.27:58727 10.10.2.12:443 ESTABLISHED 4580 TCP 10.10.2.27:58872 10.10.2.12:443 ESTABLISHED 3088 TCP 127.0.0.1:51692 127.0.0.1:51693 ESTABLISHED 6504 TCP 127.0.0.1:51693 127.0.0.1:51692 ESTABLISHED 6504 TCP 127.0.0.1:51697 127.0.0.1:51698 ESTABLISHED 6504 TCP 127.0.0.1:51698 127.0.0.1:51697 ESTABLISHED 6396 TCP [2000:2::27]:51763 [2000:31::10]:443 ESTABLISHED 6396 TCP [2000:2::27]:51764 [2000:31::10]:443 ESTABLISHED 6396 </pre> Log-in to AADRM with Admin account. Select "Manage" from "Rights management", and click "activate" to enable Rights Management.
Expected results	Internet Browser accesses AADRM and enable RMS over IPv6
Pass/fail	
Observed results	
Environment	
Comments or information	

12.1.2 Office Integration with Rights Management

Test case number	
User scenario	Validate User is able to create/consume rights management protected content over IPv6
Method	<ol style="list-style-type: none"> 1. Ensure that all validation tests are completed and Office application is working over IPv6 client machines. 2. Launch Office 2013 application with "Test User 1 (TU1)" on "Client1" 3. Click the file tab, and on the "Info" tab do one of the following: <ol style="list-style-type: none"> a. In Word, on the "Info" tab, click "Protect Document", point to "Restrict Permission" and assign the access level b. In Excel, on the "Info" tab, click "Protect Excel", point to "Restrict Permission" and assign the access level c. In Word, on the "Info" tab, click "Protect Presentation", point to "Restrict Permission" and assign the access level <p>Ensure you chose to allow Test user 2 to access the contents.</p> <ol style="list-style-type: none"> 4. Validate TU1 is able to protect and save Office contents. 5. Launch Office application with "Test user 2 (TU2)" on "Client2" 6. Open the contents TU1 has created, and validate TU2 is able to access protected contents with assigned access level.
Expected results	User is able to create/consume rights management protected content over IPv6
Pass/fail	
Observed results	
Environment	
Comments or information	Installing and configure certain version of Microsoft Office is required

Appendix 1 – Verifying MSODS IPv6 Functionality

MSODS has already undergone its own independent IPv6 testing and has confirmed it is IPv6-capable. Also, MSODS is a back-end service with limited client interaction. Due to these factors, testing this service is not deemed necessary and is out of scope of the test plan.

In the event testing is desired, however, the following scenarios can be validated:

1. Customer tenant admin opens PowerShell and connects to provisioning API to handle administrative tasks.
2. Customer tenant admin sets up directory sync from their on-premise Active Directory to MSODS via AdminWebService.
3. Customer tenant admin accesses RESTAPI via IE and application to handle administrative tasks.
4. External partner accesses BecWebService to manage its customer accounts.

Appendix 2 – Verifying Exchange Online Protection (EOP) Functionality

EOP is a back-end service with limited client interaction. The full functionality of the Exchange Online Service will depend on this function being available *within* the infrastructure and should be considered part of the EXO service availability. Due to this factor, testing this service may be deemed out of scope of the test plan.

In the event testing is desired, however, the following scenarios can be validated:

1. Delivery from customer's on-premise IPv6 endpoint to EOP (ipv6.contoso-com.*.com).
2. Delivery from EOP to the customer's IPv6 on-premise IPv4/IPv6 endpoints.
3. Delivery from EOP to non-tenant IPv4/IPv6 endpoints across the Internet.

IMPORTANT NOTE: The IPv6 address space renders a few of the current strategies unusable (e.g. IP address blocking) so there are some limitations as to what the service will support – by design due to practical limitations. EOP can offer very limited protection based on the sender address with IPv6. SPAMMING rules will still be applied to content but *not* IP address.

Appendix 3 – Verifying OrgID Functionality

OrgID is a back-end service with limited client interaction. The full functionality of the Office 365 Services will depend on this function being available *within* the infrastructure and should be considered a fundamental prerequisite for Office 365 service availability. Due to this factor, testing this service may be deemed out of scope of the test plan.

In the event testing is desired, however, the following scenarios can be validated:

1. Managed users with IPv4 only can login and logout from OrgID.
2. IPv4 machine can access all login/logout related UI on the Internet Explorer 8.
NOTE: The old UI <https://portal.microsoftonline.com> is due to be replaced with a modern UI. This is a direct connection to O365 and is operated by OrgID. For managed users, user ID and password is managed by OrgID.
3. Managed users with IPv6 only can login and logout from OrgID.
IMPORTANT NOTE: Use of the portal (i.e. <https://portal.microsoftonline.com>) will be the most impactful proof of IPv6 capability.
4. IPv6 machine can access all login/logout related UI on Internet Explorer 8.
5. Cross Instance Functionality with IPv6 (i.e. use of multiple services simultaneously) - expect the same behavior as with IPv4.
6. User with IPv4 only can use guest feature by logging in to LiveID
7. User with IPv6 only can use guest feature by logging in to LiveID
IMPORTANT NOTE: Currently LiveID does not support IPv6 access for Guests.
8. Non-Login related functionality (ex. SAPI) has no regression with IPv4
IMPORTANT NOTE: This is not a concern for direct client communications with O365 services.

Appendix 4 – Verifying DNS Functionality

Office 365 DNS is a back-end service with limited client interaction. The full functionality of the Office 365 Services will depend on this function being available *within* the infrastructure and should be considered a fundamental prerequisite for Office 365 BOX service availability. Due to these factors, testing this service may be deemed out of scope of the test plan. There is a related scenario in the “10. BOX Functionality Validation” section.

In the event testing is desired, however, the following scenarios can be validated:

1. Customer via Admin UI being able to add and verify custom domain which hosts AAAA records in the DNS.
2. Customer is able to send DNS resolution queries for AAAA records, and DNS resolver confirms that queries came for AAAA records with subsequent IPv6 address responses going back out.
3. Internal Office 365 DNS Resolver queries for AAAA records, and DNS resolver confirms that the queries came for AAAA records with subsequent IPv6 address response going back out.

IMPORTANT NOTE: The customer must have registered 128-bit addresses on DNS to create the necessary AAAA records and subsequently have them resolved.