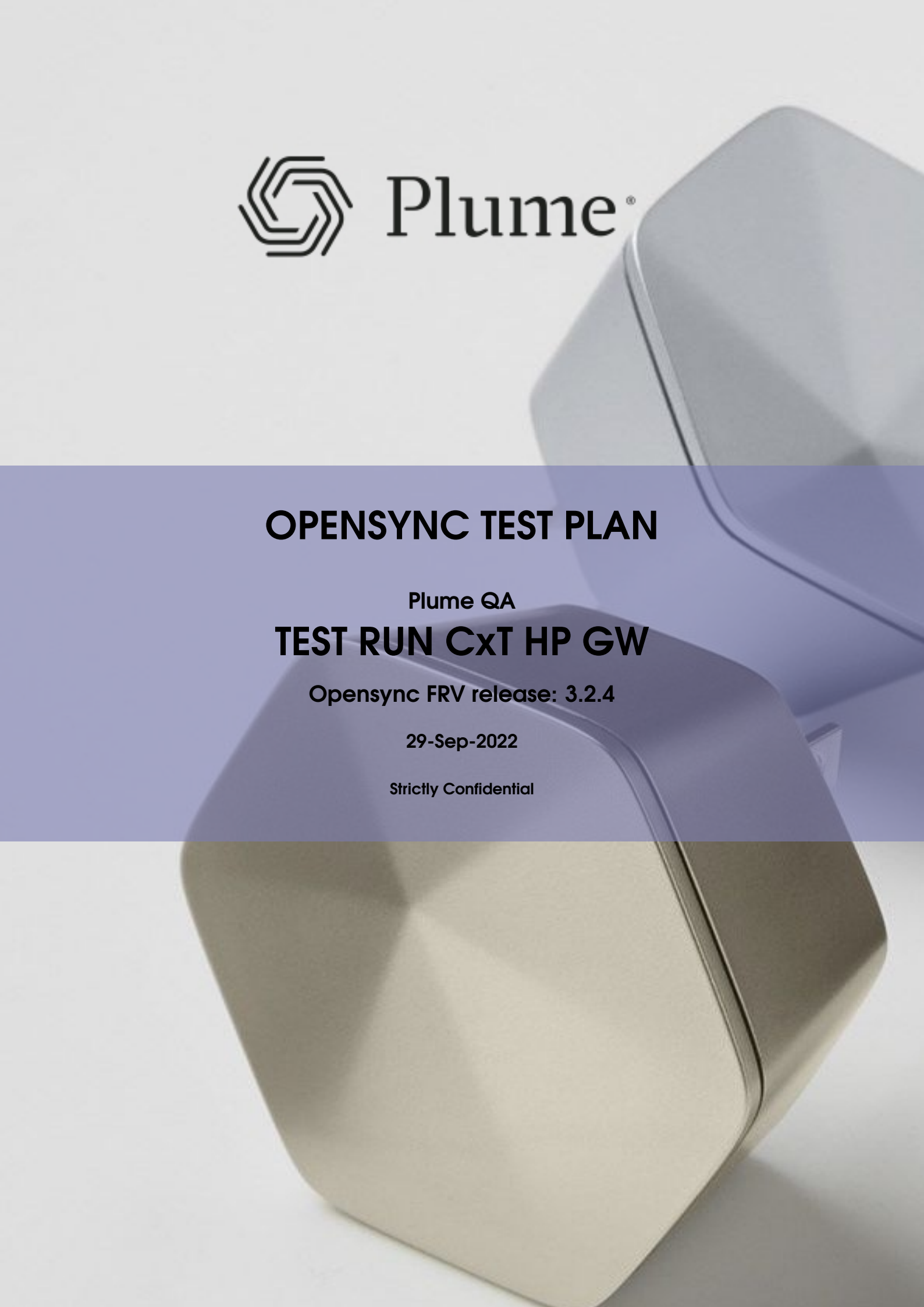

OPENSYNC TEST PLAN

Plume QA

TEST RUN CxT HP GW

Opensync FRV release: 3.2.4

29-Sep-2022

Strictly Confidential

PUBLISHED BY PLUME
PLUME.COM

Contents

1 Onboarding 5

1.1 Onboarding via Frontline 5

1.1.1 Gateway onboarding 5

1.1.2 Extender onboarding 7

1.2 Onboarding via App 8

1.2.1 Android 8

1.2.1.1 Gateway onboarding - Android 8

1.2.1.2 Extender onboarding - Android 9

1.2.1.3 Reclaiming a Node - Android 10

1.2.2 iOS 11

1.2.2.1 Gateway onboarding - iOS 11

1.2.2.2 Extender onboarding - iOS 12

1.2.2.3 Reclaiming a Node - iOS 13

2 Services 15

2.1 Gaming Services 15

2.1.1 Microsoft XBOX 15

2.1.2 Nvidia Shield 17

2.1.3 Sony PlayStation 18

2.1.4 Real Time PC Gaming Experience 19

2.1.5 Nintendo Switch 20

2.1.6 VR - AirLink 21

2.1.7 VR - Streaming 22

3 Frontline 23

3.1 Firmware Upgrading 23

3.1.1 Gateway Firmware Upgrade via Web UI 23

3.1.2 Extender Firmware Upgrade via Frontline . . . 24
3.1.3 Extender Firmware Upgrade via Web UI . . . 25
3.2 VPN Services . . . 26
3.2.1 OpenVPN . . . 26
3.2.2 L2TP/IPSec . . . 27
3.2.3 PPTP . . . 28
3.2.4 Commercial VPN services . . . 29
3.3 VoD Services . . . 30
3.3.1 Netflix . . . 30
3.3.2 Vimeo . . . 31
3.3.3 YouTube . . . 32
3.3.4 Smart TV . . . 33
3.4 IoT Services . . . 34
3.4.1 IoT - Amazon Devices . . . 34
3.4.2 IoT - Light Bulb . . . 35
3.4.3 IoT - Google devices . . . 36
3.4.4 IoT - Apple Devices . . . 37
3.5 Streaming Audio/Video Services . . . 38
3.5.1 Twitch . . . 38
3.5.2 Facebook Live . . . 39
3.5.3 YouTube Live . . . 40
3.5.4 TV to GO . . . 41
3.6 Casting/Discovery/Share services . . . 42
3.6.1 UPNP/DLNA (NAS) . . . 42
3.6.2 Chromecast . . . 44
3.6.3 Sonos . . . 45
3.6.4 Apple Airplay . . . 46
3.6.5 Samba . . . 47
3.6.6 SFTP (FTP over SSH) . . . 48
3.6.7 HTTP Server . . . 49
3.6.8 UPnP Port Forwarding . . . 50
3.6.9 Windows screen mirroring . . . 52
3.7 Multicast IPTV . . . 53
3.7.1 IPTV - Single HD stream with channel switching . . . 53
3.8 Cloud Storage/Backup/Hosting Services . . . 54
3.8.1 iCloud . . . 54
3.8.2 DropBox . . . 55
3.8.3 OneDrive . . . 56
3.8.4 Google Drive . . . 57
4 Technical specifications and reliability . . . 59
4.1 Connectivity . . . 59
4.1.1 Time to acquire a DHCP lease - Wired devices . . . 59
4.1.2 Time to acquire a DHCP lease - Wireless devices . . . 61
4.1.3 WiFi device - Automatic reconnect . . . 62
4.2 Latency . . . 63
4.2.1 Latency per HOP . . . 63

4.3 Stability 64
4.3.1 Five consecutive reboots 64
4.3.2 Five quick power cycles 65
4.3.3 Overnight traffic test on 5 GHz 66
4.3.4 Device inactivity/sleep mode 67
4.3.5 Lost connectivity 68
4.3.5.1 Location status online/offline 68
4.3.5.2 Lost WAN uplink connectivity 69
4.3.5.3 Single node cleaning lady 71
4.4 Client/device management 72
4.4.1 802.11k/v/r 72
4.4.2 Topology 73
4.4.2.1 Wired Daisy Chaining 73
4.5 Performance 74
4.5.1 Ookla 74
4.5.2 Wireless 74
4.5.2.1 Wireless Gateway throughput performance 74
4.5.2.2 Wireless 1st hop throughput performance 75
4.5.2.3 Wireless 2nd hop throughput performance 76
4.5.3 Wired 77
4.5.3.1 Wired Gateway throughput performance 77
4.5.3.2 Wired 1st hop throughput performance 78
4.5.3.3 Wired 2nd hop throughput performance 79
4.5.4 iperf3 80
4.5.5 Wireless 80
4.5.5.1 Wireless gateway throughput performance 80
4.5.5.2 Wireless 1st hop throughput performance 81
4.5.5.3 Wireless 2nd hop throughput performance 82
4.5.6 Wired 83
4.5.6.1 Wired gateway throughput performance 83
4.5.6.2 Wired 1st hop throughput performance 84
4.5.6.3 Wired 2nd hop throughput performance 85
4.6 QoE 86
4.6.1 QoE Node stats in Frontline 86
4.6.2 Live QoE Node stats in Frontline 87
4.6.3 QoE device stats in Frontline 88
4.6.4 Live QoE device stats in Frontline 89
4.7 Utilities 90
4.7.1 Logpull 90
4.7.2 Remote Connection Protocols 91
4.7.2.1 Windows RDP - Video call 91
4.7.2.2 Windows RDP - Drive and clipboard sharing 92
4.7.2.3 Windows RDP - Advanced device forwarding 93

1. Onboarding

1.1 Onboarding via Frontline

1.1.1 Gateway onboarding

Case ID

C1859077

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Completed onboarding via the HomePass app
3) Clients:
– 1x client with access to Frontline

Test Steps

1) Access the onboarded location via Frontline
2) Go to the Pods & Nodes section, click on Add Node/Extender and add the new gateway node via its ID
3) Plug the node into a power socket/strip and connect it to the internet via an Ethernet cable
4) Check if the node comes online in Frontline and shows the gateway icon

Expected Results

1) The location loads successfully
2) The new gateway node is successfully added and the location now reports more nodes

3) The LED on the gateway node start blinking
4) The node shows up in the topology section in Frontline with the gateway icon and establishes a wireless backhaul with at least one other node

1.1.2 Extender onboarding

Case ID

C1859078

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Completed onboarding via the HomePass app
3) Clients:
– 1x client with access to Frontline

Test Steps

1) Access the onboarded location via Frontline
2) Go to the Pods & Nodes section, click on Add Node/Extender and add the new extender nodes via their ID
3) Plug the nodes into a power socket/strip
4) Check if the nodes comes online in Frontline

Expected Results

1) The location loads successfully
2) The new extender nodes are successfully added and the location now reports more nodes
3) The LED on the extender nodes start blinking
4) The node show up in the topology section in Frontline and establish a wireless backhaul with at least one other node

1.2 Onboarding via App

1.2.1 Android

1.2.1.1 Gateway onboarding - Android

Case ID

C1880294

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Gateway node
3) Clients:
– 1x Android client with the HomePass app
– 1x client with access to Frontline

Test Steps

1) Plug the gateway nodes into a power socket/strip and connect them to the internet via an Ethernet cable
2) In the HomePass app tap on "Set up HomePass" and create a new account
3) Check your email inbox for a verification email
4) Follow the onboarding instructions in the app
5) Check in the app if the gateway nodes have been successfully onboarded
6) Check the location in Frontline

Expected Results

1) The LED on the gateway nodes start blinking
2) The app guides you through the account creation process
3) You get the verification email
4) The app guides you through the onboarding
5) The app shows the gateway nodes you onboarded
6) The customer and the location with the gateway nodes can be found in Frontline

1.2.1.2 Extender onboarding - Android

Case ID

C1880295

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Extender nodes
3) Clients:
– 1x Android client with the HomePass app
– 1x client with access to Frontline

Test Steps

1) Plug the extender nodes into a power socket/strip
2) In the HomePass app tap on "Set up HomePass" to create a new account
3) Check your email inbox for a verification email
4) Follow the onboarding instructions in the app
5) Check in the app if the extender nodes have been successfully onboarded
6) Check the location in Frontline

Alternative:
1) Scroll to the Adapt section of the Home screen
2) Tap on the more options button and tap "Add a pod"
3) Wait until the nodes are found
4) Tap "All done", wait for first time boot–up to complete and tap "Next"

Expected Results

1) The LED on the extender nodes start blinking
2) The app guides you through the account creation process
3) You get the verification email
4) The app guides you through the onboarding
5) The app shows the extender nodes you onboarded
6) The customer and the location with the gateway nodes can be found in Frontline

Alternative:
1) The currently onboarded nodes show in the 2nd panel
2) The Add remaining pods screen opens
3) The new extender nodes are found in under 30 seconds
4) The new extender nodes show up in the panel from step 1

1.2.1.3 Reclaiming a Node - Android

Case ID

C1970698

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup with multiple nodes online (at least 3)
2) Clients:
– 1x Android client with the HomePass app

Test Steps

1) On the home screen scroll down to the SuperPods card
2) Tap on a leaf node and delete it from the location (tap the three dots Delete pod... DELETE POD)
3) Repeat the process for the 2nd leaf node
4) Wait a few minutes, try using the internet
5) On the home page scroll down to the SuperPods card, tap the three dots Add a pod
6) Wait for all unclaimed pods to be discovered again, then click Done

Expected Results

1) You can see all currently claimed nodes
2) The node can be deleted and it disappears from the location
3) The 2nd node can also be deleted and it disappears from the location
4) The internet still works after deleting leaf nodes
5) The Add remaining pods screen opens
6) The previously removed nodes are successfully claimed

1.2.2 iOS

1.2.2.1 Gateway onboarding - iOS

Case ID

C1857894

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Gateway node
3) Clients:
– 1x iOS client with the HomePass app
– 1x client with access to Frontline

Test Steps

1) Plug the gateway nodes into a power socket/strip and connect them to the internet via an Ethernet cable
2) In the HomePass app tap on "New Setup" and create a new account
3) Check your email inbox for a verification email
4) Follow the onboarding instructions in the app
5) Check in the app if the gateway nodes have been successfully onboarded
6) Check the location in Frontline

Expected Results

1) The LED on the gateway nodes start blinking
2) The app guides you through the account creation process
3) You get the verification email
4) The app guides you through the onboarding
5) The app shows the gateway nodes you onboarded
6) The customer and the location with the gateway nodes can be found in Frontline

1.2.2.2 Extender onboarding - iOS

Case ID

C1857895

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Extender nodes
3) Clients:
– 1x iOS client with the HomePass app
– 1x client with access to Frontline

Test Steps

1) Plug the extender nodes into a power socket/strip
2) In the HomePass app tap on "New Setup" to create a new account
3) Check your email inbox for a verification email
4) Follow the onboarding instructions in the app
5) Check in the app if the extender nodes have been successfully onboarded
6) Check the location in Frontline

Alternative:
1) Scroll to the Adapt section of the Home screen
2) Tap on the more options button and tap "Add a pod"
3) Wait until the nodes are found
4) Tap "All done", wait for first time boot–up to complete and tap "Next"

Expected Results

1) The LED on the extender nodes start blinking
2) The app guides you through the account creation process
3) You get the verification email
4) The app guides you through the onboarding
5) The app shows the extender nodes you onboarded
6) The customer and the location with the gateway nodes can be found in Frontline

Alternative:
1) The currently onboarded nodes show in the 2nd panel
2) The Add remaining pods screen opens
3) The new extender nodes are found in under 30 seconds
4) The new extender nodes show up in the panel from step 1

1.2.2.3 Reclaiming a Node - iOS

Case ID

C1970699

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup with multiple nodes online (at least 3)
2) Clients:
– 1x iOS client with the HomePass app

Test Steps

1) On the home screen scroll down to the SuperPods card
2) Tap on a leaf node and delete it from the location (tap the three dots Delete pod... DELETE POD)
3) Repeat the process for the 2nd leaf node
4) Wait a few minutes, try using the internet
5) On the home page scroll down to the SuperPods card, tap the three dots Add a pod
6) Wait for all unclaimed pods to be discovered again, then click Done

Expected Results

1) You can see all currently claimed nodes
2) The node can be deleted and it disappears from the location
3) The 2nd node can also be deleted and it disappears from the location
4) The internet still works after deleting leaf nodes
5) The Add remaining pods screen opens
6) The previously removed nodes are successfully claimed

2. Services

2.1 Gaming Services

2.1.1 Microsoft XBOX

Case ID

C1859163

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x XBOX console
– 1x client with speed test
3) No heavy users on the network

Test Steps

1) Run integrated speed test on your XBOX console
2) Play realtime action multiplayer game that shows network information (Fortnite shows ping) for up to 10 minutes (make sure you are connected to a low latency server, up to 50ms)
3) Occasionally run a speed test on the second client while playing the video game

Expected Results

1) Speed test completes with decent speed (write the speeds down in the test case results)
2) Game works without any latency issues and ping stays low

3) Ping raises when speed test is run (up to 250ms), but does not have a major influence on the gaming experience

2.1.2 Nvidia Shield

Case ID

C1859164

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Nvidia Shield console
– 1x client with speed test
3) No heavy users on the network

Test Steps

1) Play a game that is not turn based for up to 10 minutes (League of Legends, Fortnite, Counter Strike, etc.)
2) Occasionally run a speed test on the second client while playing the video game

Expected Results

1) Game works without any major fluctuations in latency
2) Speed test does not have a major influence on the gaming experience

2.1.3 Sony PlayStation

Case ID

C1859166

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x PlayStation console
– 1x client with speed test
3) No heavy users on the network

Test Steps

1) Run integrated Speed test on your PlayStation console
2) Play realtime action multiplayer game that shows network information (Fortnite shows ping) for up to 10 minutes (make sure you are connected to a low latency server, up to 50ms)
3) Occasionally run a speed test the second device while playing the video game

Expected Results

1) Speed test completes with decent speed (write the speeds down in the test case results)
2) Game works without any latency issues and ping stays low
3) Ping raises when speed test is run (up to 250ms), but game is still playable

2.1.4 Real Time PC Gaming Experience

Case ID

C1859167

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Windows client with Ethernet port and video games installed
– 1x client with speed test
3) No heavy users on the network

Test Steps

1) Play a game that is not turn based for up to 10 minutes (League of Legends, Fortnite, Counter Strike, etc.)
2) Occasionally run a speed test on the second client while playing the video game
3) Connect the client to the internet via Ethernet cable
4) Repeat steps 1 and 2

Expected Results

1) Game works without any major fluctuations in latency
2) Ping raises when speed test is run (up to 250ms), but does not have a major influence on the gaming experience
3) Client connects to the network
4) Ping raises when speed test is run (up to 250ms), but does not have a major influence on the gaming experience

2.1.5 Nintendo Switch

Case ID

C1863518

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Nintendo Switch console
– 1x client with speed test
3) No heavy users on the network

Test Steps

1) Run integrated Speed test on your Nintendo Switch
3) Play realtime action multiplayer game that shows network information (Fortnite shows ping) for up to 10 minutes
3) Occasionally run a speed test on the second client while playing the video game

Expected Results

1) Speed test completes with decent speed (write the speeds down in the test case results)
2) Game works without any latency issues and ping stays low
3) Ping raises when speed test is run (up to 250ms), but does not have a major influence on the gaming experience

2.1.6 VR - AirLink

Case ID

C1905692

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Windows client with Ethernet port and Oculus app installed
– 1x VR client that supports streaming games (eg. Meta Quest 2 with AirLink)
– 1x client with speed test
3) No heavy users on the network
4) For Quest 2 you have to first enable Oculus AirLink, which you can do in Settings Experimental AirLink

Test Steps

1) Open the Oculus app and connect to Wi–Fi network with Windows client
2) Connect VR client to the Wi–Fi network
3) Connect VR client to the Windows client (AirLink with Quest 2)
4) Play a game over AirLink for up to 10 minutes
5) Occasionally run a speed test the second client while playing the video game

Expected Results

2) VR client connects to the Wi–Fi network
3) VR client connects to the Windows client
4) Game works without any major fluctuations in latency
5) Speed test affects the quality (latency, resolution, delay), but does not have a major influence on the gaming experience

2.1.7 VR - Streaming

Case ID

C1905693

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x iOS/Android client with Oculus app
– 1x VR client that supports streaming games (eg. Meta Quest 2 with AirLink)
– 1x client with speed test
3) No heavy users on the network

Test Steps

1) Open the Oculus app and connect to Wi–Fi network with iOS/Android client
2) Connect VR client to the Wi–Fi network
3) Start sharing to iOS/Android client
4) Play a game (Beat Saber, Super Hot, etc.) for up to 10 minutes
5) Occasionally run a speed test on another client connected to your wi–fi network

Expected Results

2) VR client connects to the Wi–Fi network
3) VR client starts sharing to iOS/Android client
4) Game works without any major fluctuations in latency, device roams from node to node without major interruptions
5) Speed test affects the quality (latency, resolution, delay), but does not have a major influence on the gaming experience

3. Frontline

3.1 Firmware Upgrading

3.1.1 Gateway Firmware Upgrade via Web UI

Case ID

C1859115

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Manual for upgrading the gateway node through the WebUI
3) Gateway node
4) Clients:
– 1x PC client with WebUI, Frontline access & access to the firmware release notes
– 1x router/modem client with an accessible WebUI

Test Steps

1) Follow the instructions for upgrading the DUT via the WebUI
2) Check if the DUT is upgraded to the desired version in Frontline

Expected Results

1) Instruction are clear and you can successfully install the new firmware
2) The DUT is on the desired firmware version

3.1.2 Extender Firmware Upgrade via Frontline

Case ID

C1859110

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Extender nodes
3) Clients:
– 1x client with Frontline access

Test Steps

1) Navigate to the test location on Frontline
2) Go to Configuration Location Firmware Upgrade
3) Click on the "Select Version Matrix" button
4) Select the appropriate version
5) Wait until the upgrade finishes
6) Refresh the page

Expected Results

1) The location is available on Frontline and the DUT is shown
2) The Location Firmware Upgrade tab opens
3) The "Select Matrix" window opens
4) The appropriate version is available for the relevant DUT
5) Frontline displays the upgrade progress and reaches the AwaitingReboot/ Rebooting stage
6) The selected Firmware was installed successfully

3.1.3 Extender Firmware Upgrade via Web UI

Case ID

C1962098

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Manual for upgrading extender nodes through the WebUI
3) Extender nodes
4) Clients:
– 1x PC client with WebUI, Frontline access & access to the firmware release notes
– 1x router/modem client with an accessible WebUI

Test Steps

1) Follow the instructions for upgrading the DUT via the WebUI
2) Check if the DUT is upgraded to the desired version in Frontline

Expected Results

1) Instruction are clear and you can successfully install the new firmware
2) The DUT is on the desired firmware version

3.2 VPN Services

3.2.1 OpenVPN

Case ID

C1859117

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) VPN server using an OpenVPN protocol
3) Clients:
– Windows PC client
– Linux PC client
– Smartphone

Test Steps

1) Connect one PC and the smartphone to the Wi–Fi network, and one PC to ethernet (on the test network)
2) Connect all 3 devices to the OpenVPN network
3) Ping the OpenVPN server (check the IP of the VPN interface, the server will usually be X.X.X.1) for 360 seconds
4) In the meantime browse the web or watch a live video stream on devices, while roaming around the house with the smartphone
5) Disconnect from the OpenVPN server

Expected Results

1) All clients connect to network
2) Clients can connect to the VPN server
3) Ping to the VPN server goes through and is tolerable, connection is stable for whole 6 minutes. Check the ping to that same server outside of test network for reference
4) Device stays connected to the VPN server
5) Devices disconnect from the OpenVPN server on demand

3.2.2 L2TP/IPSec

Case ID

C1859118

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) VPN server using a L2TP/IPSec protocol
3) Clients:
– Windows PC client
– Linux PC client
– Smartphone

Test Steps

1) Connect one PC and the smartphone to the Wi–Fi network, and one PC to ethernet (on the test network)
2) Connect all 3 devices to the L2TP/IPSec network
3) Ping the L2TP/IPSec server (check the IP of the VPN interface, the server will usually be X.X.X.1) for 360 seconds
4) In the meantime browse the web or watch a live video stream on devices, while roaming around the house with the smartphone
5) Disconnect from the L2TP server

Expected Results

1) All clients connect to network
2) Clients can connect to the VPN server
3) Ping to the VPN server goes through and is tolerable, connection is stable for whole 6 minutes. Check the ping to that same server outside of test network for reference
4) Device stays connected to the VPN server
5) Devices disconnect from the L2TP server on demand

3.2.3 PPTP

Case ID

C1859120

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) VPN server using a PPTP protocol
3) Clients:
– Windows PC client
– Linux PC client
– Smartphone

Test Steps

1) Connect one PC and the smartphone to the Wi–Fi network, and one PC to ethernet (on the test network)
2) Connect all 3 devices to the PPTP network
3) Ping the PPTP server (check the IP of the VPN interface, the server will usually be X.X.X.1) for 360 seconds
4) In the meantime browse the web or watch a live video stream on devices, while roaming around the house with the smartphone
5) Disconnect from the PPTP server

Expected Results

1) All clients connect to network
2) Clients can connect to the VPN server
3) Ping to the VPN server goes through and is tolerable, connection is stable for whole 6 minutes. Check the ping to that same server outside of test network for reference
4) Device stays connected to the VPN server
5) Devices disconnect from the PPTP server on demand

3.2.4 Commercial VPN services

Case ID

C1859121

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Aommercial VPN service (Nord VPN, Express VPN, TunnelBear) – specify the service you are using in the results
3) Clients:
– Windows PC client
– Linux PC client
– Smartphone

Test Steps

1) Connect one PC and the smartphone to the Wi–Fi network, and one PC via Ethernet (on the test network)
2) Start the VPN app on all clients and connect to the VPN.
3) Ping the VPN server (check the IP of the VPN interface, the server will usually be X.X.X.1) for 360 seconds, in the meantime browse the web or watch a live video stream on devices, while roaming around the house with the smartphone
4) Disconnect from the VPN service

Expected Results

1) All clients connect to the network
2) Clients can connect to the VPN server
3) Ping to the VPN server goes through and is tolerable, connection is stable for whole 6 minutes. Check the ping to that same server outside of test network for reference
4) Devices disconnect from the VPN service on demand

3.3 VoD Services

3.3.1 Netflix

Case ID

C1859124

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smart TV with the Netflix app
– 1x laptop (Windows/macOs)
– 1x smartphone/tablet client (iOS/Android)

Test Steps

1) Connect the TV, laptop, and smartphone to Node Wi–Fi
2) Play a 4K video on Netflix on all 3 devices simultaneously
3) Roam around the house with the phone and seek video so it does not preload
4) Start a speed test on a device connected to Wi–Fi network while the streams are running

Expected Results

1) All devices connect to the network
2) Netflix stream starts on all devices in high quality
3) Seeking works without bigger interruptions (up to 3 seconds)
4) All Netflix streams work without issues even when running a speed test

3.3.2 Vimeo

Case ID

C1859125

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smart TV with the Vimeo app
– 1x laptop (Windows or macOs)
– 1x smartphone/tablet Client (iOS/Android)

Test Steps

1) Connect the TV, laptop, and smartphone to the Wi–Fi network
2) Play a 4K video on Vimeo on all 3 devices simultaneously
3) Roam around the house with the phone and seek video so it does not preload
4) Start a speed test on a device connected to Wi–Fi network while the streams are running

Expected Results

1) All devices connect to the network
2) Vimeo stream starts on all devices in high quality
3) Seeking works without bigger interruptions (up to 3 seconds)
4) All Vimeo streams work without issues even when running a speed test

3.3.3 YouTube

Case ID

C1859126

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smart TV with the YouTube app
– 1x laptop (Windows or macOS)
– 1x smartphone/tablet client (iOS/Android)

Test Steps

1) Connect the TV, laptop, and smartphone to the Wi–Fi network
2) Play a 4K video on YouTube on all 3 devices simultaneously
3) Roam around the house with the phone and seek video so it does not preload
4) Start a speed test on a device connected to Wi–Fi network while the streams are running

Expected Results

1) All devices connect to the network
2) YouTube stream starts on all devices in high quality
3) Seeking works without bigger interruptions (up to 3 seconds)
4) All YouTube streams work without issues even when running a speed test

3.3.4 Smart TV

Case ID

C1859127

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smart TV connected via WiFi

Test Steps

1) Connect the Smart TV to the Wi–Fi network
2) Launch the browser on the TV and initiate a speed test (or launch the Speedtest app on the smart TV)
3) Browse and use various Smart TV features (App store, YouTube, Menus)
4) Download an app and launch it

Expected Results

1) TV connects to the network
2) Speedtest successfully finishes and is able to get 50Mbps both ways (5G connection)
3) Smart TV features work
4) App downloads and launches successfully

3.4 IoT Services

3.4.1 IoT - Amazon Devices

Case ID

C1859132

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– Amazon IoT device (Alexa)
– Smartphone Android/iOS with suitable app for onboarding

Test Steps

1) Factory reset Amazon IoT device
2) Go through onboarding process of Amazon IoT device in the smartphone app
3) Use Amazon IoT device features every day a few times to check if device is connected to network and works as expected

Expected Results

1) Amazon IoT resets and is not associated with Wi–Fi network
2) Amazon IoT device gets successfully associated with Wi–Fi network
3) Amazon IoT device is online and has connectivity at all times

3.4.2 IoT - Light Bulb

Case ID

C1868793

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– Lightbulb IoT device (LifX, Xiaomi, etc.)
– Smartphone Android/iOS with suitable app for onboarding

Test Steps

1) Factory reset Lightbulb IoT device
2) Go through onboarding process of Lightbulb IoT device in the smartphone app
3) Use Lightbulb IoT device features every day a few times to check if device is connected to network and works as expected

Expected Results

1) Lightbulb IoT resets and is not associated with Wi–Fi network
2) Lightbulb IoT device gets successfully associated with Wi–Fi network
3) Lightbulb IoT device is online and has connectivity at all times

3.4.3 IoT - Google devices

Case ID

C1868794

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– Google IoT device (Nest or Google Home device)
– Smartphone Android/iOS with suitable app for onboarding

Test Steps

1) Factory reset Google IoT device
2) Go through onboarding process of Google IoT device in the smartphone app
3) Use Google IoT device features every day a few times to check if device is connected to network and works as expected

Expected Results

1) Google IoT resets and is not associated with Wi–Fi network
2) Google IoT device gets successfully associated with Wi–Fi network
3) Google IoT device is online and has connectivity at all times

3.4.4 IoT - Apple Devices

Case ID

C1868795

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– Apple IoT device (HomePod Mini, Apple Watch, Apple TV)
– Smartphone Android/iOS with suitable app for onboarding

Test Steps

1) Factory reset Apple IoT device
2) Go through onboarding process of Apple IoT device in the smartphone app
3) Use Apple IoT device features every day a few times to check if device is connected to network and works as expected

Expected Results

1) Apple IoT resets and is not associated with Wi–Fi network
2) Apple IoT device gets successfully associated with Wi–Fi network
3) Apple IoT device is online and has connectivity at all times

3.5 Streaming Audio/Video Services

3.5.1 Twitch

Case ID

C1859133

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x laptop (Windows or macOS)
– 1x smartphone/tablet client (iOS/Android)

Test Steps

1) Connect the laptop and smartphone to the Wi–Fi network
2) Start a Twitch stream on both devices
3) Roam around the house with smartphone/laptop and watch the livestream
4) Start a speedtest on a device connected to the Wi–Fi network while the streams are running

Expected Results

1) Both devices connect to the network
2) Twitch livestream starts on both devices in high quality
3) While roaming the stream continues to play with only minor buffering or artefacts
4) While running the speedtest the stream does not get interrupted or drops in quality

3.5.2 Facebook Live

Case ID

C1859134

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Laptop (Windows or macOS)
– 1x Smartphone/Tablet Client (iOS/Android)

Test Steps

1) Connect the laptop and smartphone to the WiFi network
2) Start a Facebook livestream on all devices
3) Roam around the house with the smartphone/laptop and watch the live stream
4) Start a speedtest on a device connected to the Wi–Fi network while the streams are running

Expected Results

1) All devices connect to the network
2) Facebook livestream starts on both devices in high quality
3) While roaming the stream continues to play with only minor buffering or artefacts
4) While running the speedtest the stream does not get interrupted or drops in quality

3.5.3 YouTube Live

Case ID

C1859135

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x laptop (Windows or macOS)
– 1x smartphone/tablet client (iOS/Android)

Test Steps

1) Connect the laptop and smartphone to the WiFi network
2) Start a YouTube livestream on both devices
3) Roam around the house with smartphone/laptop and watch the livestream
4) Start a speedtest on a device connected to the Wi–Fi network while the streams are running

Expected Results

1) Both devices connect to the network
2) YouTube livestream starts on both devices in high quality
3) While roaming the stream continues to play with only minor buffering or artefacts
4) While running the speedtest the stream does not get interrupted or drops in quality

3.5.4 TV to GO

Case ID

C1859136

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x smart TV with a TV to GO app (optional)
– 1x smartphone/tablet client (iOS/Android)
– 1x Wi–Fi laptop

Test Steps

1) Connect all clients to the Wi–Fi network
2) Start the TV to GO app on all devices and play a channel of your choice
3) On all devices switch between available channels
4) Roam around the house with the smartphone/laptop
5) Start a speedtest on a device connected to the network

Expected Results

1) All devices connect to the network
2) TV to GO app starts on all devices and the selected channel plays normally
3) Switching between channels works without any major buffering or interruptions
4) While roaming, the stream continues to play with only minor buffering or artefacts
5) While running the speedtest, the stream does not get interrupted or drops in quality

3.6 Casting/Discovery/Share services

Enabling RDP on the session host

– Go to Settings and search for Remote desktop settings
– Make sure Enable Remote Desktop is set to On
– Check the PC name and connect – UN/PW is the user on the Windows machine

Enabling advanced RDP functions

– Open the group policy editor (gpedit)
– Navigate to Administrative Templates Windows Components Remote Desktop Services Remote Desktop Session Host
– Set Allow audio and video playback redirection and Allow audio recording redirection to enabled. Set Do not allow Clipboard redirection, Do not allow drive redirection, and Do not allow support Plug and Play device redirection to disabled
– Update the profile with the changes using gpupdate /force

Client PC Setup
– Open the Remote Desktop Connection program and navigate to the Local Resources
– Under the Remote audio Settings set Remote audio playback to play on this computer and Record audio recording to Record from this computer
– Under the Local devices and resources More tab tick Drives, Video capture devices, Other supported Plug and Play (PnP) devices. Make sure the Printers and Clipboard options are also ticked in the main window

https://plumedesign.atlassian.net/wiki/spaces/CXT/pages/edit–v2/14285471858

3.6.1 UPNP/DLNA (NAS)

Case ID

C1859137

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1 x Windows PC with Media Server enabled (setup: Setup DLNA Media Server from Control Panel in Windows 10)
– 1x Smartphone/Tablet Client (iOS/Android) with the VLC app
– 1x Android TV with the VLC app

Win10 Media Server setup: Right click on the Start button in the bottom left corner of the screen, choose Control Panel from the menu, then search 'media' at the top right corner of the Control Panel home screen. Click the 'Media streaming options' link in the Network and Sharing Center' section. Follow the on–screen tips to turn

on media streaming, name your media library, allow devices to access your shared media, select media type(s) to share and finally finish the setup.

You should also have some files in the VIDEOS folder (e.g. an episode of Friends)

If the location is in "BRIDGE mode", make sure that "IGMP snooping" and Multicast−to−unicast are enabled

Test Steps

1) Connect all clients to the Wi−Fi network
2) Start sharing media content from the Windows PC Client
3) Discover the UPNP/DLNA server from GW and Leaf nodes of the network on different devices (e.g. Windows PC on the 1st hop, TV on the 2nd hop), via the VLC app or through the Smart TV's built−in input source discovery (usually found under dashboard or somewhere in the menu)
4) Play a video from the server on a Smart TV/Smartphone and seek the video so it doesn't preload
5) Run a Speedtest on a device connected to the network

Expected Results

1) All devices can connect to the network
2) Can enable media streaming on the device
3) The Windows PC server shows up under Local Network in the VLC app (smartphone/Smart TV) or under input sources of the TV (depends on the TV model)
4) Video plays in high quality without any real issues (buffer up to 3 seconds is OK)
5) During the Speedtest the video is not interrupted and the quality of the video does not drop

3.6.2 Chromecast

Case ID

C1859138

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Smartphone/Tablet Client (Android)
– 1x WiFi client
– 1x Smart TV
– 1x Chromecast or Android TV (Nvidia Shield)

Test Steps

1) Connect all DUT to the network (Wi–Fi)
2) Check if Chromecast discovery works from the GW and the Leafs (Ethernet and Wi–Fi)
3) Cast a video from the client (Android – Google photo) to the Smart TV
4) Cast desktop from client to Android TV and play video on Vimeo (Not YT because it opens YT app on Smart TV)
5) Start a Speedtest on a device connected to the network
6) Walk around the house with the casting client to initiate roaming
7) If in BRIDGE mode, test the connection from outside the test network (e.g. try discovery from the switch that the test network is connected to)

Expected Results

1) All DUT connect to the network
2) Chromecast can discover all available devices (Smart TV, Android TV)
3) Video starts playing on Smart TV
4) Desktop casts to Android TV successfully without major buffering or artefacts
5) While running a Speedtest the Chromecast does not stop and there are no major interruptions or artefacts
6) While roaming the Chromecast doesn't stop and there are no major interruptions or artefacts
7) Discovery and stream also works outside of test network (Bridge mode)

3.6.3 Sonos

Case ID

C1859139

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Sonos connected to the GW node over WiFi interface
– 1xSmartphone/Tablet Client (iOS/Android)

Test Steps

1) Connect all devices to the Wi–Fi network
2) Connect the smartphone/tablet to Sonos and play some music (e.g. Sonos App, Spotify, Apple Music), try this from different nodes (GW, Leaf)
3) Move around the house with the phone/tablet and roam between pods and check if you can still skip tracks and change volume
4) Start Speedtest on one Wi–Fi Client

Expected Results

1) All clients can connect to the network
2) The smartphone/tablet can establish a Wi–Fi connection with the Sonos speaker and can play music
3) While roaming controls on Sonos work without issues
4) While running a Speedtest there is no difference in music playback

3.6.4 Apple Airplay

Case ID

C1859140

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x iOS/iPadOS/macOS client that supports Airplay 2
– 1x Smart TV that supports Airplay 2
– 1x Wi–Fi client to run speedtests on

Test Steps

1) Connect all devices to the network
2) Start sharing a video clip from the iOS/iPadOS/macOS to the Smart TV, watch it and try seeking; try this from different nodes (GW, Leaf)
3) Move around the house with the casting device to initiate roaming
4) Start Speedtest on one Wifi Client

Expected Results

1) All clients can connect to the network
2) The video plays on the TV without major buffering or artifacts
3) While roaming the video plays without interruptions, buffering. Some artifacts in image could be present while roaming.
4) While running a Speedtest the video plays without issues

3.6.5 Samba

Case ID

C1859141

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– Phone (playing media)
– PC (SMB file transfer)
3) Server:
– Samba server

Test Steps

1) Connect all clients to the network (Wi–Fi)
2) Discover the Samba server from different nodes (GW and Leafs)
3) Transfer a file from the server to the client
4) Start streaming a high bitrate video (20Mbps), watch it, and seek the video
5) Walk around the house to initiate roaming

Expected Results

1) All clients can connect to the network
2) Can discover the Samba server from different nodes
3) The file gets transferred without major issues
4) The video plays in high quality, seeking works without issues (up to 3 seconds)
5) While roaming the video doesn't stop

3.6.6 SFTP (FTP over SSH)

Case ID

C1859142

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– Linux SFTP server
– PC client

Test Steps

1) Connect all devices to the Wi–Fi network
2) Start the FTP server and connect to it with a client (FileZilla/WinSCP/ Linux_native)
3) Upload a 100MB+ file
4) Download the 100MB+ file
5) Start Speedtets during the UL/DL

Expected Results

1) All DUT connect to the network
2) The SFTP server starts and the client can connect to it
3) File successfully uploads
4) File successfully downloads
5) While running a Speedest the file is still uploading/downloading and finishes successfully

3.6.7 HTTP Server

Case ID

C1859143

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x External apache2 server (on the internet) with a 100MB+ file (e.g. Ubuntu download https://ubuntu.com/download/desktop)
– 2x PC client

Test Steps

1) Connect all DUT to the network
2) Open a browser and enter the URL of the file and start the download
3) Open the downloads tab and observe the download status
4) Start a simultaneous HTTP file download on another client
5) Start a Speedtest

Expected Results

1) All DUT connect to the network
2) The download starts successfully
3) The download speed is consistent and reasonably fast
4) The second download does not affect the first one in any major way
5) While running the Spedtest the download continues and finishes

3.6.8 UPnP Port Forwarding

Case ID

C1859144

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Topology / Location: 1 x DUT GW node + 2 x DUT Leaf node
3) Clients:
– client with Transmission app https://transmissionbt.com/ installed (Ubuntu has it by default)
– client connected to the same network as the Node network (WAN)

Test Steps

1) Disable UPnP in the Plume App (Advanced settings)
2) Connect the 1st client to the Wi–Fi network
3) Open Transmission then click Edit –> Preferences –> Network and check that Use UPnP / NAT–PMP port forwarding on router option is enabled, if not enable it
4) Check "Randomize port each time Transmission opens"
5) Close and re–open Transmission. Navigate to the same menu
6) Open terminal on the 2nd client connected to the same subnet. Execute following command: nmap –Pn <IP> –p <port>
<IP> is the WAN IP of the Node network (can be found under Pods & Nodes –> GW Pod –> WAN IP
<port> is the port number shown in the menu in Transmission
7) Enable UPnP in the Plume App (Advanced settings)
8) Reconnect (disconnect and connect again) 1st client to the plume network and reopen Transmission menu
9) Repeat step 6 – note that port is now different
10) Close Transmission
11) Repeat step 6 with port from step 9
12) Disconnect the 1st client and wait for 10 seconds
13) Check the port again on the 2nd client

Expected Results

1) "UPnP is disabled" on Plume location
2) Client connects to Wi–Fi network
3) "UPnP / NAT–PMP port forwarding on router" is enabled
4) "Randomize port each time Transmission opens" is enabled
5) Port used for incoming connection is different
6) Port is filtered/closed
7) "UPnP is enabled" on Plume location
8) Port used for incoming connection is different
9) "Port is opened"
10) Transmission closes

11) "Port is filtered/closed"
12) Client disconnects
13) "Port is filtered/closed"

3.6.9 Windows screen mirroring

Case ID

C1888720

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Windows PC client
– 1x WiFi client
– 1x Smart TV

Test Steps

1) Connect all DUT to the network (Wi–Fi)
2) Check if Wireless display discovery works from the GW and the Leafs (Windows only supports Wi–Fi) – usually you must go into screen mirroring menu in TV for device to be discoverable (Samsung)
3) Cast desktop from Windows client to Smart TV (Casting works with Peer to Peer connection, so we are not testing the image quality, only discovery)
4) Stop mirroring screen after a while

Expected Results

1) All DUT connect to the network
2) TV is discoverable by Windows PC
3) Desktop starts mirroring on Smart TV
4) Screen mirroring stops

3.7 Multicast IPTV

3.7.1 IPTV - Single HD stream with channel switching

Case ID

C1859145

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x IPTV provider (A1) modem/router
– 1x IPTV provider Set–Top Box

Test Steps

1) In Frontline, go to Configuration Multicast, and make sure that IGMP Snooping is enabled
2) Make sure that the backhaul between leaf and GW is established on 5GHz band
3) Connect the IPTV provider's modem/router to the network via Ethernet
4) Connect the Set–Top Box to the extender node via Ethernet
5) Turn the Set–Top Box on and wait for it to boot up
6) Try switching channels, as well as seeking, and observe the speed and possible glitches or freezes
7) Settle down on your favorite HD channel and watch it for 15 minutes

Expected Results

1) You are able to enable IGMP Snooping
2) The backhaul is established on 5GHz
3) The IPTV moded/router is connected to the network
5) The STP is connected to the network
6) You are able to switch channels, seek through the video, and there are no observable glitches or freezes
7) The video and audio quality is stable, there are no noticeable glitches or freezes

3.8 Cloud Storage/Backup/Hosting Services

3.8.1 iCloud

Case ID

C1859151

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x iOS/iPadOS client
– 1x macOS client

Test Steps

1) Connect the two clients to the node WiFi
2) From one of the devices upload a file larger than 100MB to iCloud, while roaming around the house
3) On the other device download that same file from iCloud
4) Delete the file from the first device
5) Upload the file back to iCloud from the second device
6) Download the same file from iCloud back to the first device

Expected Results

1) Devices connect to the network
2) File starts uploading and it finishes without interruptions
3) File can be seen on iCloud on the other device and it can be downloaded without interruptions
4) File can be uploaded from the second device without interruptions
5) File can be downloaded back to the first device without interruptions

3.8.2 DropBox

Case ID

C1859152

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x iOS/Android client with DropBox
– 1x macOS/Windows client with DropBox

Test Steps

1) Connect the two devices to the Node WiFi
2) From one of the devices upload a file larger than 100MB to DropBox, while roaming around the house
3) On the other device download that same file from Dropbox
4) Delete the file on the first device and Dropbox, then upload it back to DropBox
5) Download the same file from Dropbox back to original device

Expected Results

1) Devices connect to test network
2) Files starts uploading and it finishes without interruptions
3) File can be seen on Dropbox on other device and it can be downloaded without interruptions
4) File can be uploaded from the second device without interruptions
5) File can be downloaded back to first device without interruptions

3.8.3 OneDrive

Case ID

C1859153

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x iOS/Android client with OneDrive
– 1x macOS/Windows client with OneDrive

Test Steps

1) Connect two devices to the Node WiFi
2) From one of the devices upload a file larger than 100MB to OneDrive, while roaming around the house
3) On the other device download the same file
4) Delete the file on the first device and OneDrive, then upload it back to OneDrive
5) Download the same file from OneDrive back to original device

Expected Results

1) Devices connect to test network
2) Files starts uploading and it finishes without interruptions
3) File can be seen on OneDrive on other device and it can be downloaded without interruptions
4) File can be uploaded from the second device without interruptions
5) File can be downloaded back to first device without interruptions

3.8.4 Google Drive

Case ID

C1859154

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x iOS/Android client with Google Drive
– 1x macOS/Windows client with Google Drive

Test Steps

1) Connect two devices to the Node Wi–Fi
2) From one of the devices upload a file larger than 100MB to Google Drive, while roaming around the house
3) On the other device download the same file
4) Delete the file on the first device and Google Drive, then upload it back to Google Drive
5) Download the same file from Google Drive back to the original device

Expected Results

1) Devices connect to test network
2) Files starts uploading and it finishes without interruptions
3) File can be seen on Google Drive on other device and it can be downloaded without interruptions
4) File can be uploaded from the second device without interruptions
5) File can be downloaded back to the first device without interruptions

4. Technical specifications and reliability

4.1 Connectivity

4.1.1 Time to acquire a DHCP lease - Wired devices

Case ID

C1859168

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x client with WireShark software & Ethernet port/dongle

Test Steps

1) Open Wireshark, select the appropriate (ethernet) interface and start capturing packets
2) Filter the traffic to "dhcp"
3) Connect laptop to the leaf node using ethernet
4) Wait until the DHCP server sends a DHCPACK message to your laptop
5) Check if the laptop has successfully set the IP address by issuing "ipconfig /all" or similar command
6) Measure the time from first DHCPDISCOVER to DHCPACK message (=T)

Expected Results

4) DHCP server sends DHCPACK message to the laptop
5) IP address is successfully set

6) Time for DHCPDISCOVER is not longer than 15 seconds (T<15), 20 seconds for third party devices

4.1.2 Time to acquire a DHCP lease - Wireless devices

Case ID

C1859169

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– client with WireShark software & 802.11ax OR 802.11ac WiFi connectivity

Test Steps

1) Open Wireshark, select the appropriate (WiFi) interface and start capturing packets
2) Filter the traffic to "dhcp"
3) Move the laptop near the leaf node, turn WiFi ON and try to connect (associate) to the SSID of the test location
4) Wait until the DHCP server sends a DHCPACK message to your laptop
5) Check if the laptop has successfully set the IP address by issuing "ipconfig /all" or similar command
6) Measure the time from first DHCPDISCOVER to DHCPACK message (=T)

Expected Results

4) DHCP server sends DHCPACK message to the laptop
5) IP address is successfully set
6) Time for DHCPDISCOVER is not longer than 1 second (T<1)

4.1.3 WiFi device - Automatic reconnect

Case ID

C1859170

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– client with macOS, iOS, Android, WinOS, Linux

Test Steps

1) Connect a WiFi device to the node WiFi network
2) Enable "Connect automatic" only for the node network (SSID)
3) Manually disconnect the device or go far away so that the connection drops
4) Connect manually to a different WiFi or Internet source
5) Return to the node WiFi location
6) In case of Internet, power outage or reboot, all devices should start to connect back after the location is back online. If any fails to do so, this test automatically FAILS

Expected Results

1) Device connects to the WiFi network
2) Automatic reconnect is ENABLED
3) Connection to WiFi network drops
4) Connected successfully to another network
5, 6) Device automatically reconnects to the node WiFi network

4.2 Latency

4.2.1 Latency per HOP

Case ID

C1859173

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 1x Linux reference client connected to outside WiFi network
– 1x Linux client connected to Wi–Fi via GW node with (from –30dBm to –40dBm)
– 1x Linux client connected to Wi–Fi via first leaf node (from –30dBm to –40dBm)
– 1x Linux client connected to Wi–Fi via second leaf node (from –30dBm to –40 dBm)

Test Steps

1) Connect clients as described in predconditions
2) Connect the reference client to an internet source outside of node WiFi (e.g. directly to the router/switch)
3) Location should not be saturated with performance or speed tests, light internet use is allowed
4) Use next command on Linux to schedule ping on all devices at the same time. On clients write the following command:

```
at 09:00 <<END
ping 172.23.X.1 –c 3600 –i 1 > /tmp/FILENAME
END
```

5) Wait for the test to finish (1 hour) and log pings & noticeable latency
6) Compare the reference device with a LEAF and GW device, and collect them into a spreadsheet (link to spreadsheet: https://docs.google.com/spreadsheets/d/1LUx–rCeI7KB6K7cLkoMHKHABC4GSvYOrKmvhuvKM10c/edit#gid=447246495)

Expected Results

6) There is no major ping loss and no big latency or latency deviations (2nd hop not above 30ms, 1st hop not above 20ms, GW not above 15ms, AVERAGE not bigger than 30ms).

4.3 Stability

4.3.1 Five consecutive reboots

Case ID

C1859179

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– 1x client with Frontline Access

Test Steps

1) Check node status (Topology) and firmware version (Pods & Nodes)
2) Reboot location in Frontline. (Configuration–>Utilities–>Reboot Location–> click "Reboot")
3) Wait for all nodes to reconnect
4) Repeat reboot 5 times
5) Check firmware version again

Expected Results

1) All nodes are connected & on correct firmware version
2) Location starts rebooting
3) All nodes disconnect, then reconnect
4) Rebooting does not cause any problems
5) The firmware version is correct and did not change during reboots, all nodes reconnected

4.3.2 Five quick power cycles

Case ID

C1859180

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– 1x Linux/WinOS client with Frontline account with group admin privileges

Test Steps

1) Plug all pods into a power strip and wait for them to get online
2) Using Frontline, check the firmware version on all pods
3) Turn the power off on the power strip
4) Wait for 5 seconds
5) Turn the power back on
6) Wait for about 17 seconds
7) Repeat steps 2–5 four more times
8) Check the firmware version once again

Expected Results

1) All pods appear in Frontline and are online
7) Pods reconnect within 2 minutes after the last cycle
8) Pods have the same firmware version that they had at the beginning of the test

4.3.3 Overnight traffic test on 5 GHz

Case ID

C1859181

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
– 2x Linux client

Test Steps

1) Establish a line topology by pushing it from the cloud or by manually positioning nodes
2) Make sure the backhaul between nodes is established on 5 GHz band channel
3) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 and −67 dBm)
4) Setup iperf3 server outside of test network, so the traffic goes through the whole test network
To start iperf server use:
iperf3 −s −p 5003
5) On the Wi−Fi client on 2nd hop start iperf3 client and run it at least 16, and up to 24 hours
Command:
iperf3 c <serverIP> p 5003 t 86400 −−bidir
6) Check for Wi−Fi node reboots or disconnects in Frontline
7) Check that Wi−Fi client has not disconnected during the test

Expected Results

1) Location is in line topology
3) Frontline shows EXCELLENT health rating
3) Check for DUT disconnects or reboot
5) iperf test starts and it does not interrupt by itself (it must run at least 16 hours)
6) There are no reboots of Wi−Fi nodes visible in Frontline
7) Wi−Fi client did not disconnect during test

4.3.4 Device inactivity/sleep mode

Case ID

C1859182

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– a few different clients (Android, iOS, WinOS, Linux, macOS)
– client with option to ping/issue commands to the DUT
3) Stable node WiFi Network

Test Steps

1) Connect the device to the Plume WiFi network
2) Leave the device until it goes to sleep mode
3) Check if it still has internet connectivity
4) Do not use the device 2h
5) Check if the device is still connected to the WiFi in Frontline and if the device has internet access
6) Awaken the DUT and check if WiFi access & ping resume

Expected Results

1) Device connects to Plume WiFi network
3) Device keeps/does not keep internet connectivity in sleep mode
5) Device can either be connected or disconnected in Frontline, if it is connected, ping MUST be returning normally
6) Device must connect to WiFi automatically & ping must return replies

4.3.5 Lost connectivity

4.3.5.1 Location status online/offline

Case ID

C1859183

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– client with Frontline account with group admin privileges
3) ACL configuration set as per these instructions: https://plumedesign.atlassian.net/wiki/spaces/CXT/pages/11814295987/HOW+TO+block+control+plane+to+Pods+using+firewall+rules

Test Steps

1) In order to test if Frontline cloud connectivity online/offline status works you need to block control plane SSL/443 between the cloud and the gateway
2) To block cloud connection you need to configure ACL on your ISP router/firewall which will block TCP/443 to the gateway's IP or MAC address, ALSO DISABLE FAST TRACK FIRE WALL RULE DURING THAT TEST (AFTER DISABLING FAST TRACK RULE WAIT 3 MINUTES BEFORE PROCEEDING):
– BRIDGE: Block all nodes on location with the firewall rule
– ROUTER: Block gateway only with firewall rule
3) Enable ACL on the ISP router/firewall
4) Check that the Frontline location appears offline in about 60 seconds (refresh the page if needed)
5) Wait for 30s–60s and disable ACL on the ISP router/firewall to restore cloud connection
6) Location should be back online within 60s

Expected Results

1) Configuration for control plane SSL/443 block is set
3) ACL is enabled
4) Frontline location appears offline
5) ACL is disabled
6) Within 60 seconds location is back online and working

4.3.5.2 Lost WAN uplink connectivity

Case ID

C1859185

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– client with Linux/WinOS and access to Frontline account with a group admin privileges
3) Location in ROUTER mode

Test Steps

1) Location operating in ROUTER mode:
– a) In Frontline "Configuration–>WAN and Ethernet–>Network mode" tab check if the toggle button is in a ROUTER mode or switch to it if it's not already
– b) Wait for the location to reboot and DUTs are back online
2) Connect WiFi client to the 1st leaf node
3) Connect Eth client to the 2nd leaf node
4) Check connectivity between the clients (ping)
5) Disconnect WAN uplink cable from the gateway
6) Check if location is offline in Frontline
7) Check that clients are not seen in Frontline and they cannot ping google.com
8) Check SSID visibility
9) Wait for about 15 minutes
10) Check that nodes will not go to a reboot state
11) Check connectivity again between the clients (ping)
12) Reconnect WAN uplink cable
13) Check Frontline and wait for location to come back online and become fully operational
14) Scan for the SSID visibility
15) Check that clients are seen in the Frontline and in the app and can ping google.com
16) Check connectivity between the clients (ping)

Expected Results

1) Location is in ROUTER mode
2) WiFi client connects
3) Eth client connects
4) Clients can ping each other
6) Location is offline in Frontline
7) Clients are not seen in Frontline and cannot ping google.com
8) No SSID is visible
10) Nodes did not reboot
11) Connectivity between clients still works

13) Frontline shows location back online
14) SSID is visible
15) Clients are visible in Frontline and can ping google.com
16) Connectivity between clients still works

4.3.5.3 Single node cleaning lady

Case ID

C1859186

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– client with open Frontline
– 2x smartphone client (Android/iOS)

Test Steps

1) Make sure that the location is optimized
2) Have one ping running to a leaf that is NOT being tested
3) Connect to a leaf node with one smartphone client and start a video call with another smartphone client that is on LTE
4) Unplug the node that the Wi–Fi client is connected to
5) Wait 15 seconds
6) Plug the node back in

Expected Results

1) Location is optimized
2) Ping is running
3) Wi–Fi client is connected to the node with the best RSSI
4) Node disconnects, interrupting the call
5) Client connects to another node and the video call continues in 10 seconds or less

4.4 Client/device management

4.4.1 802.11k/v/r

Case ID

C1962100

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Access to Frontline
3) Clients:
– 1x client with access to Frontline
– 1x client connected to Node Wi–Fi & with HomePass installed

Test Steps

1) Go to Frontline under Configuration –> WiFi Radios, and disable Fast Transition (FT) 802.11r if it's not already
2) Connect the Windows/macOS client to the DUT node
3) Ping the default gateway –i 0.1 (100ms) from the client
4) In Frontline, go to Devices –> click on the three dots next to the client –> Manual Steer
5) Initiate manual steering of the client to the neighboring DUT node
6) Count lost pings
7) Steer the client back to the source DUT node
9) In Frontline, go to Configuration –> WiFi Radios –> enable Fast Transition 802.11r
9) Repeat the steps 3, 4, 5, and 6
10) Compare the results

Expected Results

1) Fast Transition can be disabled
2) Client connects to the DUT node
3) Client can be pinged
4) Client is listed in Frontline
5) Manual steering happens (sometimes it can take a few tries)
6) There are not many lost pings
7) Client steers back to DUT node
8) Fast Transition can be enabled
10) Steering is faster & better when Fast Transition is enabled

4.4.2 Topology

4.4.2.1 Wired Daisy Chaining

Case ID

C1962099

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Ethernet cables to connect network nodes
3) 2x Ethernet PC client with iPerf3

Test Steps

1) Connect Wi−Fi nodes with cable (Node to Node, RGW to another node, you can cable them only from GW node)
2) Check in FrontLine if new topology is working as expected
3) Connect one Ethernet client to last daisychained node and other Ethernet client to same subnet on testbed
4) Start iPerf3 server on the testbed client
5) Run iPerf3 test on the client that is connected with Ethernet to last daisychained node with next command: iPerf3 −c "iPerf server IP" −P 5 −t 60

Expected Results

2) Bridge mode: More than one Wi−Fi node shows up in FrontLine with globe picture
2) Router mode: More than one Wi−Fi node shows up in FrontLine online without wireless backhaul (no globe picture)
5) iPerf3 results are in range of 940Mbps +/− 20Mbps

4.5 Performance

4.5.1 Ookla

4.5.2 Wireless

4.5.2.1 Wireless Gateway throughput performance

Case ID

C1962107

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable WiFi client supporting 802.11a/b/g/n/ac/ax

Test Steps

1) Push a topology from the cloud or manually position nodes to establish a line topology
2) Make sure the backhaul between nodes is established on 5 GHz band channel
3) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
4) Connect your client to gateway node via Wi−Fi (−(30−40) RSSI)
5) Measure wireless upload and download speed on gateway node with Ookla Speedtest, also log client RSSI and Channel

Expected Results

1) Nodes are in line topology
2) Backhaul is on 5GHz
3) Backhaul RSSI between nodes is excellent
4) Client is connected to gateway node via Wi−Fi
5) UL and DL speeds are sufficent for Wi−Fi radio (Mind that speeds are capped by access link from ISP)
800+ Mbps (4x4 160MHz)
500+ Mbps (4x4 80MHz AX)
400+ Mbps (4x4 80MHz AC)
if 3x3 or 2x2 radio it can also be less

4.5.2.2 Wireless 1st hop throughput performance

Case ID

C1962108

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wireless client supporting 802.11a/b/g/n/ac/ax

Test Steps

1) Push a topology from the cloud or manually position nodes to establish a line topology
2) Make sure the backhaul between nodes is established on 5 GHz band channel
3) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
4) Connect your client to 1st hop node via Wi−Fi (−(30−40) RSSI)
5) Measure wireless upload and download speed on 1st hop node with Ookla speedtest, also log client RSSI and Channel

Expected Results

1) Nodes are in line topology
2) Backhaul is on 5GHz
3) Backhaul RSSI between nodes is excellent
4) Client is connected to 1st hop node via WiFi
5) UL and DL speeds are sufficent for Wi−Fi radio (Mind that speeds are capped by access link from ISP)
350+ Mbps (4x4 160/80MHz backhaul)

4.5.2.3 Wireless 2nd hop throughput performance

Case ID

C1962109

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wireless client supporting 802.11a/b/g/n/ac/ax

Test Steps

1) Push a topology from the cloud or manually position nodes to establish a line topology
2) Make sure the backhaul between nodes is established on 5 GHz band channel
3) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
4) Connect your client to gateway node via Wi−Fi (−(30−40) RSSI)
5) Measure wireless upload and download speed on 2nd hop node with Ookla speedtest, also log client RSSI and Channel

Expected Results

1) Nodes are in line topology
2) Backhaul is on 5GHz
3) Backhaul RSSI between nodes is excellent
4) Client is connected to 2nd hop node via WiFi
5) UL and DL speeds are sufficent for Wi−Fi radio (Mind that speeds are capped by access link from ISP)
150+ Mbps (If only dual band device, it can be less)

4.5.3 Wired

4.5.3.1 Wired Gateway throughput performance

Case ID

C1962110

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wired client with Eth port or dongle supporting 802.11a/b/g/n/ac/ax

Test Steps

1) Push a topology from the cloud or manually position nodes to establish a line topology
2) Make sure the backhaul between nodes is established on 5 GHz band channel
3) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
4) Connect your client to gateway node via Eth port or dongle
5) Measure wired upload and download speed on gateway node with Ookla speedtest

Expected Results

1) Nodes are in line topology
2) Backhaul is on 5GHz
3) Backhaul RSSI between nodes is excellent
4) Client is connected to gateway node via Eth cable
5) UL and DL speeds reach the following KPIs: 900Mbps UL and DL (Mind that speeds are capped by access link from ISP)

4.5.3.2 Wired 1st hop throughput performance

Case ID

C1962111

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wired client with Eth port or dongle supporting 802.11a/b/g/n/ac/ax

Test Steps

1) Push a topology from the cloud or manually position nodes to establish a line topology
2) Make sure the backhaul between nodes is established on 5 GHz band channel
3) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
4) Connect your client to 1st hop node via Eth port or dongle
5) Measure wired upload and download speed on 1nd hop node with Ookla speedtest, log topology RSSI and channels

Expected Results

1) Nodes are in line topology
2) Backhaul is on 5GHz
3) Backhaul RSSI between nodes is excellent
4) Client is connected to 1st hop node via Eth cable
5) UL and DL speeds reach the following KPIs: 400Mbps UL and DL (4x4 80MHz)
(Mind that speeds are capped by access link from ISP)

4.5.3.3 Wired 2nd hop throughput performance

Case ID

C1962112

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wired client with Eth port or dongle supporting 802.11a/b/g/n/ac/ax

Test Steps

1) Push a topology from the cloud or manually position nodes to establish a line topology
2) Make sure the backhaul between nodes is established on 5 GHz band channel
3) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
4) Connect your client to 2nd hop node via Eth port or dongle
5) Measure wired upload and download speed on 2nd hop node with Ookla speedtest, log topology RSSI and channels

Expected Results

1) Nodes are in line topology
2) Backhaul is on 5GHz
3) Backhaul RSSI between nodes is excellent
4) Client is connected to 2nd hop node via Eth cable
5) UL and DL speeds reach the following KPIs: 150Mbps UL and DL (Mind that speeds are capped by access link from ISP)

4.5.4 iperf3

4.5.5 Wireless

4.5.5.1 Wireless gateway throughput performance

Case ID

C1962113

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable WiFi client supporting 802.11a/b/g/n/ac/ax
3) iperf3 server connected via wired connection to a dedicated Ethernet port on MultiGigaEthernet (1, 2.5, 5, 10 GE), iPerf server must be outside of test network – traffic goes over WAN of test network

Test Steps

1) Make a reference iperf3 measurment directly on the switch to make sure that iperf server is wokring correctly
2) Push a topology from the cloud or manually position nodes to establish a line topology
3) Make sure the backhaul between nodes is established on 5 GHz band channel
4) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
5) Connect your client to gateway node via Wi−Fi (−(30−40) RSSI)
6) Measure wireless upload and download speeds on gateway node using iperf3, also log client RSSI and Channel
All tests should be performed with an iperf3 utility by issuing:
server: iperf3 −s
a) UPLINK (UL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10
b) DOWNLINK (DL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10 −R

Expected Results

1) Results on iperf server are in range of 2.3G if operating on 2.5G network
2) Nodes are in line topology
3) Backhaul is on 5GHz
4) Backhaul RSSI between nodes is excellent
5) Client is connected to gateway node via Wi−Fi
6) UL and DL speeds reach the following KPIs:
800+ Mbps (4x4 160MHz)
500+ Mbps (4x4 80MHz)
if 3x3 or 2x2 radio it can also be less

4.5.5.2 Wireless 1st hop throughput performance

Case ID

C1962114

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable WiFi client supporting 802.11a/b/g/n/ac/ax
3) iperf3 server connected via wired connection to a dedicated Ethernet port on MultiGigaEthernet (1, 2.5, 5, 10 GE), iPerf server must be outside of test network – traffic goes over WAN of test network

Test Steps

1) Make a reference iperf3 measurment directly on the switch to make sure that iperf server is wokring correctly
2) Push a topology from the cloud or manually position nodes to establish a line topology
3) Make sure the backhaul between nodes is established on 5 GHz band channel
4) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
5) Connect your client to 1st hop node via Wi−Fi (−(30−40) RSSI)
6) Measure wireless upload and download speeds on 1st hop node using iperf3, also log client RSSI and Channel
All tests should be performed with an iperf3 utility by issuing:
server: iperf3 −s
a) UPLINK (UL): iperf3 −c ipaddriperf3_server −i 1 −t 300 −P 10
b) DOWNLINK (DL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10 −R

Expected Results

1) Results on iperf server are in range of 2.3G if operating on 2.5G network
2) Nodes are in line topology
3) Backhaul is on 5GHz
4) Backhaul RSSI between nodes is excellent
5) Client is connected to 2nd hop node via WiFi
6) UL and DL speeds reach the following KPIs:
350+ Mbps (4x4 160/80MHz backhaul)

4.5.5.3 Wireless 2nd hop throughput performance

Case ID

C1962115

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable WiFi client supporting 802.11a/b/g/n/ac/ax
3) iperf3 server connected via wired connection to a dedicated Ethernet port on MultiGigaEthernet (1, 2.5, 5, 10 GE), iPerf server must be outside of test network – traffic goes over WAN of test network

Test Steps

1) Make a reference iperf3 measurment directly on the switch to make sure that iperf server is wokring correctly
2) Push a topology from the cloud or manually position nodes to establish a line topology
3) Make sure the backhaul between nodes is established on 5 GHz band channel
4) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
5) Connect your client to 2nd hop via Wi−Fi (−(30−40) RSSI)
6) Measure wireless upload and download speeds on 2nd hop node using iperf3, also log client RSSI and Channel
All tests should be performed with an iperf3 utility by issuing:
server: iperf3 −s
a) UPLINK (UL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10
b) DOWNLINK (DL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10 −R

Expected Results

1) Results on iperf server are in range of 2.3G if operating on 2.5G network
2) Nodes are in line topology
3) Backhaul is on 5GHz
4) Backhaul RSSI between nodes is excellent
5) Client is connected to 2nd hop node via WiFi
6) UL and DL speeds reach the following KPIs:
150Mbps UL and DL

4.5.6 Wired

4.5.6.1 Wired gateway throughput performance

Case ID

C1962116

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wired client with Ethernet port or Ethernet dongle
3) iperf3 server connected via wired connection to a dedicated Ethernet port on MultiGigaEthernet (1, 2.5, 5, 10 GE), iPerf server must be outside of test network – traffic goes over WAN of test network

Test Steps

1) Make a reference iperf3 measurment directly on the switch to make sure that iperf server is wokring correctly
2) Push a topology from the cloud or manually position nodes to establish a line topology
3) Make sure the backhaul between nodes is established on 5 GHz band channel
4) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
5) Connect your client to gateway node via Ethernet
6) Measure upload and download speeds on gateway using iperf3, also log client RSSI and Channel
All tests should be performed with an iperf3 utility by issuing:
server: iperf3 –s
a) UPLINK (UL): iperf3 –c ip_addr_iperf3_server –i 1 –t 300 –P 10
b) DOWNLINK (DL): iperf3 –c ip_addr_iperf3_server –i 1 –t 300 –P 10 –R

Expected Results

1) Results on iperf server are in range of 2.3G if operating on 2.5G network
2) Nodes are in line topology
3) Backhaul is on 5GHz
4) Backhaul RSSI between nodes is excellent
5) Client is connected to gateway via Ethernet
6) UL and DL speeds reach the following KPIs:
900Mbps UL and DL

4.5.6.2 Wired 1st hop throughput performance

Case ID

C1962117

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wired client with Ethernet port or Ethernet dongle
3) iperf3 server connected via wired connection to a dedicated Ethernet port on MultiGigaEthernet (1, 2.5, 5, 10 GE), iPerf server must be outside of test network – traffic goes over WAN of test network

Test Steps

1) Make a reference iperf3 measurment directly on the switch to make sure that iperf server is wokring correctly
2) Push a topology from the cloud or manually position nodes to establish a line topology
3) Make sure the backhaul between nodes is established on 5 GHz band channel
4) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
5) Connect your client to 1st hop node via Ethernet
6) Measure upload and download speeds on gateway using iperf3, log topology RSSI and channels
All tests should be performed with an iperf3 utility by issuing:
server: iperf3 −s
a) UPLINK (UL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10
b) DOWNLINK (DL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10 −R

Expected Results

1) Results on iperf server are in range of 2.3G if operating on 2.5G network
2) Nodes are in line topology
3) Backhaul is on 5GHz
4) Backhaul RSSI between nodes is excellent
5) Client is connected to 1st hop node via Ethernet
6) UL and DL speeds reach the following KPIs:
400Mbps UL and DL

4.5.6.3 Wired 2nd hop throughput performance

Case ID

C1962118

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Device / Client:
– portable wired client with Ethernet port or Ethernet dongle
3) iperf3 server connected via wired connection to a dedicated Ethernet port on MultiGigaEthernet (1, 2.5, 5, 10 GE), iPerf server must be outside of test network – traffic goes over WAN of test network

Test Steps

1) Make a reference iperf3 measurment directly on the switch to make sure that iperf server is wokring correctly
2) Push a topology from the cloud or manually position nodes to establish a line topology
3) Make sure the backhaul between nodes is established on 5 GHz band channel
4) Make sure the established backhaul connection have a strong (EXCELLENT) channel gain (RSSI between −60 to −67 dBm)
5) Connect your client to 2nd hop node via Ethernet
6) Measure wired upload and download speeds on 2nd hop node using iperf3, log topology RSSI and channels
All tests should be performed with an iperf3 utility by issuing:
server: iperf3 −s
a) UPLINK (UL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10
b) DOWNLINK (DL): iperf3 −c ip_addr_iperf3_server −i 1 −t 300 −P 10 −R

Expected Results

1) Results on iperf server are in range of 2.3G if operating on 2.5G network
2) Nodes are in line topology
3) Backhaul is on 5GHz
4) Backhaul RSSI between nodes is excellent
5) Client is connected to 2nd hop node via Eth cable
6) UL and DL speeds reach the following KPIs:
150Mbps UL and DL

4.6 QoE

4.6.1 QoE Node stats in Frontline

Case ID

C1870198

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– 1x client with Frontline access

Test Steps

1) Check the location QoE stats in Frontline after the location is set up
2) Ensure multiple devices are connected to the location and that the location is stable
3) Check the QoE node stats after one day (QoE –> Nodes)

Expected Results

1) The QoE stats start updating soon after the location is set up
2) Multiple devices are connected and the location is stable
3) The QoE node stats bar is continuous for all nodes, excepting disconnects

4.6.2 Live QoE Node stats in Frontline

Case ID

C1870199

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– 1x client with Frontline access

Test Steps

1) Turn on live QoE stats for 1 day (QoE –> Enable Live Mode –> More options –> +1 day)
2) Ensure multiple devices are connected to the location and that the location is stable
3) Check the QoE node stats after one day

Expected Results

1) The QoE Live stats turn on and the timer shows > 24 hours
2) Multiple devices are connected and the location is stable
3) The QoE node stats bar is continuous for all nodes, excepting disconnects, for the duration of the timer

4.6.3 QoE device stats in Frontline

Case ID

C1870200

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– 1x client with Frontline access

Test Steps

1) Check the location QoE stats in Frontline after the location is set up
2) Ensure multiple devices are connected to the location and that the location is stable
3) Check the QoE device stats after one day (QoE –> Devices)

Expected Results

1) The QoE stats start updating soon after the location is set up
2) Multiple devices are connected and the location is stable
3) The QoE device stats bar is continuous for all nodes, excepting disconnects

4.6.4 Live QoE device stats in Frontline

Case ID

C1870201

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– 1x client with Frontline access

Test Steps

1) Turn on live QoE stats for 1 day (QoE –> Enable Live Mode –> More options –> +1 day)
2) Ensure multiple devices are connected to the location and that the location is stable
3) Check the QoE device stats after one day

Expected Results

1) The QoE Live stats turn on and the timer shows > 24 hours
2) Multiple devices are connected and the location is stable
3) The QoE device stats bar is continuous for all nodes, excepting disconnects, for the duration of the timer

4.7 Utilities

4.7.1 Logpull

Case ID

C1900421

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Client:
– 1x client with Frontline access

Test Steps

1) Start a logpull under Configuration –> Utilites –> Generate logpull
2) Wait 5 minutes (the location must be stable during this time)
3) Download the logpull

Expected Results

1) The logpull process starts
2) The location is stable and does not reboot/go offline during this time
3) The logpull downloads a .tgz file for each node

4.7.2 Remote Connection Protocols

4.7.2.1 Windows RDP - Video call

Case ID

C2039696

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
–2x Windows PC (one session host, one client)
3) Set up both the session host and the client according to the instructions

Test Steps

1) Connect to the session host via the computer name
2) Use the internet. Watch at least one YouTube video
3) Disconnect and reconnect to the session host via its IP
4) Join a zoom call and test the video and audio functionalities

Expected Results

1) The remote connection is established successfully
2) The internet works and you can watch the YouTube video with sound and video coming through on the client
3) The remote connection reestablishes successfully
4) The video call works as it would if you ran it from your own PC (uses the client speakers, microphone, and webcam)

4.7.2.2 Windows RDP - Drive and clipboard sharing

Case ID

C2039697

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
–2x Windows PC (one session host, one client)
3) Set up both the session host and the client according to the instructions

Test Steps

1) Connect to the session host via IP/the computer name
2) Minimize the remote session
3) Copy a website address (e. g. youtube.com) from the client PC into the remote session using copy and paste (notepad, web browser, etc.)
4) Copy a file from the remote session to the client PC desktop using copy and paste (minimize the remote session)
5) In the remote session, open the client drive via the file explorer and find, then delete the file from step 4

Expected Results

1) The remote connection is established successfully
2) The session minimizes to the client PC desktop
3) The address is successfully pasted
4) The file is successfully copied and appears on the client PC desktop
5) The file shows in the remote session and can be deleted successfully

4.7.2.3 Windows RDP - Advanced device forwarding

Case ID

C2039698

Test type

None

Test case coverage

None

Preconditions

1) Initial test environment setup
2) Clients:
–2x Windows PC (one session host, one client)
3) Set up both the session host and the client according to the instructions
4) An USB HID (mouse, tablet, etc.)

Test Steps

1) Connect to the session host via the computer name
2) Plug in a USB thumbdrive
3) Plug in a phone
4) Plug in an HID device

Expected Results

1) The remote connection is established successfully
2) The USB thumbdrive is recognized in the remote session and you can copy/paste files to/from it
3) The phone detects being plugged in and when allowing access to files, shows up in the remote session
4) The mouse/tablet/joystick/... works in the remote session

Plume