MARKETING REPORT

MR-363
Home Network Diagnostics Tools and Mechanisms

Issue: 1
Issue Date: March 2017

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	13 March 2017	5 May 2017	Miodrag Djurica, KPN Barbara Stark, AT&T	Original

Comments or questions about this Broadband Forum Marketing Report should be directed to help@broadband-forum.org.

Editor	Miodrag Djurica	KPN
	Barbara Stark	AT&T
Broadband User Services Work Area Director(s)	Jason Walls John Blackford	QA Cafe Arris
Contributors	Miodrag Djurica	KPN
	Barbara Stark	AT&T

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

Home networks are usually installed, operated, and owned by the end user, who in a few cases is an expert, but most likely will have relatively little knowledge of network technologies, and little time or patience to diagnose problems should they occur. However, these end users expect their home networks to reliably support the delivery of a wide variety of Internet services and applications. The user may encounter unacceptable performance of the applications they use due to home network misconfigurations, noise or interference that impacts the behavior of home networking technologies, or other problems. Home network problems often cause Internet services and the users applications to underperform or stop altogether, causing end users to call the Internet Service Provider (ISP) help desk.

While ISPs possess tools to manage their own core and access networks, management of home requires different tools and techniques. Gathering home network specific information may be required and interpreting this information to arrive at a remedy for a problem can require specific expertise. This Marketing Report provides an overview of some of the tools and techniques that can aid an ISP or Network Operator in diagnosing the cause of home network related performance and reliability issues that affect the quality of experience of their customers. The application of these tools is described for specific use cases.

1 Introduction

Home networks can support multiple devices, which may include PCs/laptops, smartphones, tablets, Internet radios, Set-Top-Boxes (STBs), Network-Attached Storage (NAS), game consoles, Internet phones, home automation devices (remote controlled power outlets, light switches), alarm systems, and a variety of other attached devices. These are interconnected by a combination of Ethernet switches, Wi-Fi access points (APs), Power Line Communication (PLC) or other wireless and wired technologies. The number and variety of connected devices in home networks is constantly increasing. The home network is typically connected to the Internet using a Residential Gateway (RG).

When something goes wrong, the end user often calls the Internet Service Provider (ISP) for help. If the ISP has no visibility inside the home network, there is very little the ISP can do. However tools and techniques exist which enable to ISP to gain visibility into the home network and the ISP can use these tools to gain insight into the problems affecting the customer.

This document describes a variety of the available tools and how they can be used by the ISP to help the end user troubleshoot and resolve troubles.

- Section 2 of this document provides an overview of the problems that can be diagnosed by existing tools.
- Section 3 provides a listing of the tools that may be available for the ISP to perform their analysis.
- Sections 4 and 5 provide exemplary guidance on the use of several of these tools to diagnose commonly reported issues, and potential remediation techniques.
- Appendix A provides additional details on the diagnostic tools described in Section 3.

Diagnosis of the problems in the home network, using the tools described in this document as well as other diagnostic methods may be performed by software in APs, or in remote management systems/controllers, or in both. Such systems can monitor QoS and QoE on the home networks, and these systems can assist in remediation by optimizing parameter settings. Additionally these systems can assist with troubleshooting and can report pertinent statistics back to the service provider for further analysis.

Home network diagnostics and optimization techniques and systems should be used in coordination with tools that support diagnosis and troubleshooting of the entire broadband network as reported problems may have multiple and possibly interrelated causes. These systems can be built into customer care tools and may be made available to the user.

1.1 Privacy Implications

The level of visibility diagnostics tools provide into the home network can have serious privacy implications. ISPs should be aware of privacy laws, regulations, and expectations that may apply. These regulations are specific to particular regulatory jurisdictions.

1.2 Protocol Layers

This document uses the following terminology to describe the protocol layers present across an IP-enabled home network.

Physical: Physical media and technologies (such as 100BaseT, Wi-Fi, etc.). Abbreviated as "PHY".

Link: Link layer protocol. The most common is Ethernet Media Access Control (MAC). Abbreviated as "MAC".

Internet: Internet layer protocol. Includes IPv4 and IPv6 protocols. Abbreviated as "IP".

Transport: Supports transport of messages across the Internet. The most common are TCP and UDP, though Neighbor Discovery (ND), ICMPv4, and ICMPv6 are also important for some diagnostics.

Application: All protocols that go between applications on host devices. Includes HTTP, DNS, RTP, CoAP, and many others.

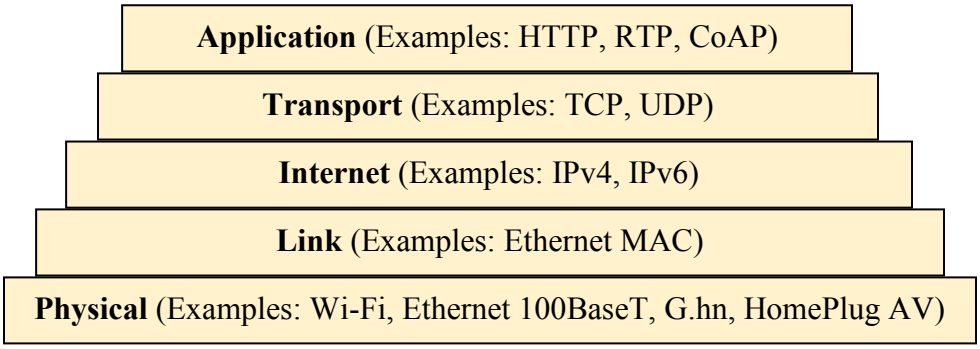

Figure 1: 5-Layer Protocol Stack

2 Diagnostics Uses

Tools can have one or more purposes. Diagnostic tools can assist in device discovery, topology discovery, continuity testing, throughput testing, latency and jitter testing, packet loss testing, and determining the route or path that traffic takes between two devices. These uses are described in more detail in Table 1.

Table 1: Diagnostic Uses

Use	Description
Device Discovery	Identify what devices exist in the home network. Device discovery at the MAC layer (Link layer) or IP layer may not provide information at layers above or below. Device discovery at the Application layer will often include device information (e.g., friendly name, manufacturer, model) and IP addresses. How devices are connected to each other is not considered a part of device discovery.
Topology Discovery	Identify what devices exist in the home network and how they are connected. Topology discovery at the IP layer will not provide information about Link layer bridges / switches, and may not provide any information at layers above or below. Topology discovery at the MAC Layer may not provide information at layers above or below. Because so many troubles in home networks are caused by issues with physical layer technologies, understanding physical layer topology is very important.
Continuity	Continuity tests identify whether a path exists between two devices. It is possible for a path to exist at the physical and MAC layers but not at the IP layer. Therefore, it is useful to be able to test for continuity at both MAC and IP layers.
Throughput / Capacity	Throughput tests identify the rate at which a fixed amount of traffic can be transported by a specific protocol between two devices, at the time the test is run. If the home network supports Quality of Service (QoS) settings, these can cause different traffic to experience different throughput. Capacity tests identify maximum possible throughput.
Latency / Jitter	Latency tests identify how long it takes for a packet to travel between two devices. Jitter is a measure of the variation in latency. If the home network supports QoS settings, these can cause different traffic to experience different latency.
Packet Loss	Packet Loss tests identify how many packets are unsuccessful in getting from one device to another. This can be measured either as an absolute number of packets lost or as a percentage against all packets. Since wireless home networking physical layer technologies often treat multicast different than unicast, it can be useful to measure loss of these separately. QoS settings can cause different traffic to experience different loss.
Route / Path	Where multiple paths exist between two devices, it can be useful to identify which path traffic takes. Currently most home network topologies have a single path between any two devices. However, this is expected to change as home networks become more complex and technology evolves.

3 Diagnostic Tools

There exist a variety of tools that can be used to run tests or record information inside a home network, for the diagnostic uses discussed in Table 1. A number of these tools are listed in Table 2, together with their uses. This is not an exhaustive list. More detail on these tools is in Appendix A.

An important aspect of many tools is whether they are active (generate their own traffic on the network) or passive (measure existing traffic on the network). Active tests that generate their own traffic can cause overloaded network links to become even more overloaded and require processing power to be used just for the purpose of testing. However, active tests do not have to wait for traffic to occur, and thus can generate more immediate results. Among the tests listed in Table 2, only the DHCP collection of IP addresses and the frame and packet counts are passive. All others are active. Passive tests use memory and processing capacity on the device collecting the information, but do not place additional load on the network.

Table 2: Tools and their Uses

Tool	How widely deployed?	Can be used for:	Outputs
ARP	All IPv4 devices respond to ARP requests	Device Discovery: at IPv4 (Internet) layer Continuity: at IPv4 (Internet) and below	MAC Address and IPv4 address of all IPv4 devices on the subnet
DHCPv4	All IPv4 devices have DHCPv4 clients	Device Discovery: at IPv4 layer	At the server: MAC Address and IPv4 address of all IPv4 devices on the subnet. At the client: DHCPv4 options sent by the DHCPv4 server to devices.
DNS-SD / mDNS	Various devices advertise services, most notably printers; various devices attempt to discover services they are interested in	Device Discovery: at application layer with device info	IP addresses and application-specific information of DNS-SD advertised services
frame counts	Widely available and enabled	Continuity: at MAC and below Throughput/Capacity: capacity of at least current frames / second	frames/second to/from a Link layer interface or for a specific stream; last/next hop MAC address of counted frames (if counting is specific to this)
ICMPv6	Widely available and enabled both for responding to messages and being able to initiate them	Continuity: at IPv6 and below Latency/Jitter: can be used; TCP and UDP may not behave the same Packet Loss: can be used; TCP and UDP may not behave the same Route/Path: can be used	whether a response was received (or lost), and the round trip time (latency) to receive the response; multiple ICMPv6 messages may see wide variation in latency, indicating jitter. Sequential tests with increasing hop limit can get each hop in path to respond

Tool	How widely deployed?	Can be used for:	Outputs
IEEE 1905.1a Topology Discovery	Emerging	Device Discovery: at PHY, MAC, and IP layer with device info Topology Discovery: at MAC and physical layer Continuity: at MAC and below	PHY, MAC, and IP layer map of the network. Some indication of link throughput between two MAC layer interfaces.
iperf	Available for all major OSs but rarely deployed; requires both sides be configured	Continuity: at IP and below Throughput/Capacity: various tests for throughput Packet Loss: can be used	throughput statistics
IPv6 ND	All IPv6-capable devices	Device Discovery: at IPv6 layer Continuity: at IPv6 and below	MAC address and IPv6 address(es) of other devices on the local link
LLDP	Widely deployed in devices that forward at the link layer	Device Discovery: at MAC layer Topology Discovery: at MAC layer Continuity: at MAC and below	MAC address of link local devices
LLTD	Deployed in MS PCs, available for Linux, but rarely enabled anywhere	Device Discovery: at MAC layer Topology Discovery: at MAC layer Continuity: at MAC and below	MAC address of link local devices
packet counts	Widely available and enabled	Continuity: at IP and below Throughput/Capacity: capacity of at least current packets / second	number of packets received and sent over some time period (often since last reboot) on an IP interface; may also include other counts
physical technology metrics	Widely available and enabled	Continuity: at physical layer Throughput/Capacity: provides info on physical link capacity Topology: provides info on directly-connected devices	Varies per physical layer technology. For example, Wi-Fi Access Points (APs) can provide list of associated devices and other APs, and other statistics; Wi-Fi Stations can provide list of APs and other statistics.

Tool	How widely deployed?	Can be used for:	Outputs
ping (ICMPv4)	Widely available and enabled in IPv4 devices	Continuity: at IPv4 and below Latency/Jitter: can be used; TCP and UDP may not behave the same Packet Loss: can be used; TCP and UDP may not behave the same	round trip response time and lost packets
spanning tree protocol	Rare in consumer-grade	Topology Discovery: at MAC layer; no discovery of hosts Route/Path: can be used	list of device IP addresses
traceroute (ICMPv4)	Widely available and enabled in IPv4 devices	Continuity: at IPv4 and below Latency/Jitter: can be used; TCP and UDP may not behave the same Route/Path: can be used	round trip response time and lost packets for all points in the path
UPnP SSDP	Widely available and enabled in PCs, routers, media servers / renderers	Device Discovery: at UPnP Application layer with device info Continuity: at UPnP Application layer and below	discovered UPnP devices and services

4 Using Tools

4.1 From a Managed Residential Gateway (RG)

The following tools (from Table 2) are commonly found on RGs, and can be very helpful in troubleshooting problems inside the home network:

- ARP
- DHCPv4 (server)
- IPv6 ND
- ping (ICMPv4)
- traceroute (ICMPv4)
- ICMPv6
- frame counts
- packet counts
- physical technology metrics

The following tools (from Table 2) are not commonly found in RGs at this time, but may provide value in troubleshooting problems that cannot be identified using the above methods.

- mDNS / DNS-SD -- recommended due to ever-increasing number of devices (especially printers) using these for service discovery; an RG that supports these could also become a DNS-SD server, to add more value to the user
- LLDP -- simple and lightweight, and useful in determining whether the problem is at the MAC or IP layer.
- IEEE 1905.1a -- not widely deployed or available, but is lightweight and shows great promise
- UPnP SSDP -- recommended due to large number of devices that make use of UPnP services

4.2 From an ISP Application or a Managed Device

The ISP can make available applications for download (or from a CD or DVD) to assist in troubleshooting. These can be loaded on PCs, smartphones, tablets, and any other device that supports loading of such applications.

Managed devices includes set-top boxes (STBs), Home Automation / Security Gateways, and any other device which the ISP provides to a user for delivery of an ISP service.

Following are some tools (from Table 2) where implementations are readily available that can be included in such applications and managed devices.

- ARP
- IPv6 ND
- UPnP SSDP
- mDNS / DNS-SD
- ping (ICMPv4)

- traceroute (ICMPv4)
- ICMPv6
- frame counts
- packet counts
- physical technology metrics
- iperf

The following tools (from Table 2) could be useful, if it is possible to provide them in an application (they may require capabilities to exist inside the network interface cards or chips):

- LLDP -- simple and lightweight, and useful in determining whether the problem is at the MAC or IP layer.
- IEEE 1905.1a -- not widely deployed or available, but is lightweight and shows great promise

Where the device is supplied by the ISP, the ISP can specify use of network interface chips or cards that support these tools.

5 Examples of Use

This section provides examples of how various tools can be used (and combined together) to analyze the home network for some commonly reported troubles. Note that there are multiple ways to diagnose these troubles, and these examples are merely provided to demonstrate one possible way.

Note: As the focus of this document is related to tools that can be used to resolve troubles within the home network, troubles with the service provider network and equipment are assumed to have been ruled out through means not described in these usage examples.

5.1 Non-computer device cannot connect to the Internet

Many customers have devices, besides their PCs and Laptops, within their homes that had been connected to the Internet (e.g., DVR/DVD player or Set-top-box, game console, picture frame) but for some reason can no longer connect.

Exemplary actions available for resolving the customer reported trouble:

1. Check if the device has a presence on the home network: Many devices announce their presence to other devices within the home network in order to communicate with each other. The RG or modem is a natural choice to perform this test, as the RG is gateway to the Internet. Checking if a device is present or has been present on the RG or modem's devices or host table will indicate if the device has recently been discovered by the RG. This action will validate that the device at one time was "seen" by the RG or modem. The RG or modem fills its devices or hosts table using tools for **Device discovery** (e.g., ARP, DHCP, IPv6 ND) listed in Table 2.
2. Check if the device is actively receiving data between the device and the RG and Modem. The RG or modem may have collected statistics related to the device and listed them in its devices or hosts table. In situations where the RG or modem doesn't have statistics related to a discovered device, the RG and modem may have collected statistics for specific interfaces. These statistics can be used if the device (e.g., STB) is the only device that uses an interface (e.g., is directly connected to the Ethernet port). The determination of whether a device is the only device to use an interface can be discovered using the tools for **Device Discovery** and **Topology** listed in Table 2. The RG or modem can detect if it is actively receiving data from the device using the tools for **Throughput/Capacity** (e.g., packet counts) listed in Table 2.
3. Check if the device is still reachable from the RG or Modem: RG and Modems have diagnostics that can be executed against devices in the home network using the tools for **Continuity** (e.g., ping, traceroute) listed in Table 2.
4. If the device is reachable or the RG or modem is actively receiving data but is not transmitting data, the issue most likely is within the RG or modem. At this point the trouble resolution procedure for that type of equipment is invoked. These procedures check for items like ensuring the RG is able to connect to Internet and if the firewall/NAT functions are appropriately configured.
5. If the device is not reachable from the RG or modem, the typical next step is to clear the device from the RG or modem's device or host table and reboot or re-power the affected device to see if the device can be detected and the RG or modem can receive data from the

device. If the device is not detected, if possible the device can be either reset to factory defaults or reconfigured.

6. If the previous action (5) does not resolve the issue, there is most likely a topology issue within the home network. These can sometimes be resolved by checking if the device is reachable as in actions (3-5) using another device that is connected through the same type of interface (e.g., MoCA, Wireless) and segment.

5.2 Computer device cannot access the Internet

Customers may have PCs, Laptops, tablets and smartphones within their homes that had been connected to the Internet, but for some reason can no longer connect.

Exemplary actions available for resolving the customer reported trouble:

1. Employ steps from Section 5.1 to make sure there is general IP connectivity. If IP connectivity exists, then specific tests that are applicable to computers are needed.
2. If the previous actions do not resolve the issue, it may be possible to use diagnostics tools provided in the computer operation system, such as a Troubleshoot tool. These tools will sometimes disable/enable or reset network interfaces as part of their processes.

5.3 Cannot Discover UPnP / DLNA device

Commonly implemented UPnP services include UPnP IGD (used to create temporary port forwarding rules in home routers) and UPnP AV (used to share content among devices. Devices with support for UPnP services or with the ability to control devices with UPnP services are prevalent in many home networks. They include many home routers, computers with Microsoft Windows operating systems and Windows Media Player, many Blu-ray players, DVRs, and Smart TVs. A key element of the UPnP device architecture is the use of IP multicast messages for advertisement and discovery. Sometimes devices that should be able to see UPnP messages from each other do not see these messages. Problems with UPnP communication are often device-specific (e.g., UPnP is not running), and such causes should be ruled out during any holistic troubleshooting effort. The following steps provide examples for diagnosing troubles that are caused by home networking issues.

Note that issues related to multicast will also impact other multicast-based service discovery mechanisms, such as mDNS.

Exemplary actions available for resolving the customer reported trouble:

1. Employ steps from Section 5.1 to make sure there is general IP connectivity. If IP connectivity exists, then specific tests related to UPnP messages are needed.
2. Check if the RG can see UPnP SSDP messages from the device in question to determine **Device Discovery** and **Continuity** at the UPnP Application layer. If the RG implements the Device.UPnP.Discovery.Device.{i}. object (TR-181 [2]), it can report all UPnP devices it discovers.
3. Determine through **Topology** testing (traceroute, IEEE 1905.1a Topology Discovery, ICMPv6) what sort of home network topology exists in the home network. If possible, determine from the topology whether there is a direct connection (i.e., the connection does

not go through other routers or across multiple physical layer technologies) between the RG and the device in question. Topology testing that only provides IP layer information (e.g., traceroute, ICMPv6) will only provide information on other routers, but not on physical layer technologies. IEEE1905.1a Topology Discovery does provide physical layer topology.

4. If the RG does not see the UPnP device (SSDP messages), and has a direct connection to the device, then the device should be considered suspect (e.g., the UPnP stack may not be enabled). The customer must ensure the UPnP stack is enabled. Other device-specific actions may be taken, such as reboot, disconnecting and reconnecting to the network, etc.
5. If the RG does not see a device that does not have a direct connection, then either the device is suspect or there are problems with transmission of multicast in the home network. If the RG sees the device, but the device is not seen elsewhere on the home network, multicast issues are likely to be the cause. A laptop running a UPnP Controller for the UPnP device in question can be connected to the home network at various points for additional troubleshooting. For example, the laptop can be directly connected by Ethernet to the RG, connected by the Wi-Fi 2.4 GHz radio, connected by the 5 GHz radio, and taken to any other point in the home network that uses a different physical layer home networking technology. If there are other routers in the home network topology, the laptop can be connected to the various links supplied by the other routers.
6. If the UPnP device can be seen by the laptop when they are on the same link, this indicates a suspect device. To resolve the issue ensure UPnP is enabled, try reboot, network disconnect/reconnect, or other commonly employed actions.
7. If the laptop sees the UPnP device when they are on the same link but not from other links, then there is a link that has multicast problems (most likely, multicast forwarding is not enabled on the link). By moving the laptop (and the device, if possible) to various links in the network, it is possible to determine exactly which link is causing the trouble. Whatever device is responsible for forwarding packets onto that link needs to be configured to enable multicast forwarding. Wireless links are the most suspect, since router vendors have been known to disable multicast capabilities on some wireless links.

5.4 Slow Internet Connection Caused by Problems in the Wi-Fi LAN

When a customer is connected to their home Wi-Fi network a report of a slow Internet connection will typically refer to the quality of their experience with either their Internet browsing activities or one or more applications. If the user reports, ‘slow Internet’, the user will probably be unable to distinguish those problems caused by a malfunctioning broadband access, the broadband WAN network itself, a problem at the application layer, or the performance their own system from those performance issues actually caused by problems with their Home Network. Internet speed tests (such as the online tests provided by Ookla, Xfinity, etc.) are generally used by customers to determine if they have a problem, but do not indicate the location of the problem in the network. The TR-143 [1] file transfer tests (if provided in the RG), and other speed tests implemented in the RG made to a point inside the access network can determine whether there are performance issues within the home or within the service provider's network. Additionally, the underlying cause of the user’s poor experience could be an issue such as high latency, transmission errors, or poor connectivity occurring anywhere on the end-to-end network connection rather than simply poor throughput on the Wi-Fi portion of the connection.

The fact that the customer is reporting 'slow performance' rather than a total failure is itself diagnostic. Connectivity has been established, and thus the procedures discussed in Sections 5.1 and 5.2 have either been successful or are probably not required.

This use case only considers the testing of the home network. For Wi-Fi networks, performance issues can have a number of root causes, however two of the most prevalent are problems related to interference or those caused by signal coverage problems. Wi-Fi interference can be occur from other Wi-Fi networks either those in the premises or those located in nearly premises, while non-Wi-Fi interference occurs from exogenous interference from non-Wi-Fi sources. Coverage issues are related to received signal strength that is not sufficient to provide coverage to the entire premises. Additional causes of degraded Wi-Fi performance include equipment failure, and misconfiguration of access points or the customer's end point equipment.

The following exemplary actions may assist in diagnosing the cause of the slow performance and point to a remedy when the problems are due to coverage, or Wi-Fi interference issues:

1. The tools for **Device Discovery** and **Topology Discovery** as described in Sections 3 and 4 of this document enable an understanding of which elements exist in the Wi-Fi network and how they are associated (**Connectivity**).
2. Requesting the Access Point to return information and statistics from itself and related to observed Neighboring Access Points provides information regarding performance (**Throughput**, **Latency/Jitter**, **Packet Loss**) and potential sources of interference impacting performance. Performance may be due to poor coverage (see Step 4), interference from other Wi-Fi networks (see Step 5), or interference from non-Wi-Fi sources (see Step 7).
3. Performing speed tests (such as those based on iperf), or using physical technology metrics as described in Section 3, can evaluate the **Throughput** of the Wi-Fi connections.
4. Using the collected information check for Wi-Fi coverage problems (experienced as poor performance or lack of connectivity) in the home (see Section 5.4.1 for a description on Poor Wi-Fi coverage). These may show up as a low Wi-Fi received signal strength at a station placed in a particular location. Instrumentation of received signal strength is widely available on Wi-Fi AP's and stations. Coverage problems may be resolved by moving either the Wi-Fi access point or the end user's equipment to a different location in the home or by installing a Wi-Fi extender or an additional Access Point.
5. If it appears that interference from other Wi-Fi networks (see Section 5.4.2 for a description of Wi-Fi Interference) significantly degrades performance, then reconfiguring the home Wi-Fi to use a different channel or band, or to change other Wi-Fi configuration parameters, could resolve interference problems. Many physical layer metrics can help analyze interference. In some cases the analysis of the network requires historical data. This may require a long-term collection of physical layer metrics in order to obtain the appropriate history of the Wi-Fi network.
6. Although detecting cases of non-Wi-Fi produced interference can be difficult using currently available tools, performance problems introduced by non-Wi-Fi sources may be both diagnosed and resolved by reconfiguring the Wi-Fi to use a different channel or band, or changing other Wi-Fi configuration parameters. If non-Wi-Fi interference is suspected

removing or moving the location of a possible source of non-Wi-Fi interference may also resolve the issue.

7. Wi-Fi equipment faults may be detected by running "self-test" diagnostic tools provided on the Wi-Fi access nodes, or by using tools on the customer's equipment to diagnose such issues.

5.4.1 Poor Wi-Fi Coverage

Placement of Wi-Fi access points can lead to poor Wi-Fi coverage due to low signal strength of transmissions between devices. Either a device within the home network cannot connect to the access point or transmission between the two devices suffers from performance problems due to the low received signal strength. In Figure 2, the problem occurs where devices in Room 4 cannot connect or has poor performance in Room 4 because the Wi-Fi access point is located in the living room.

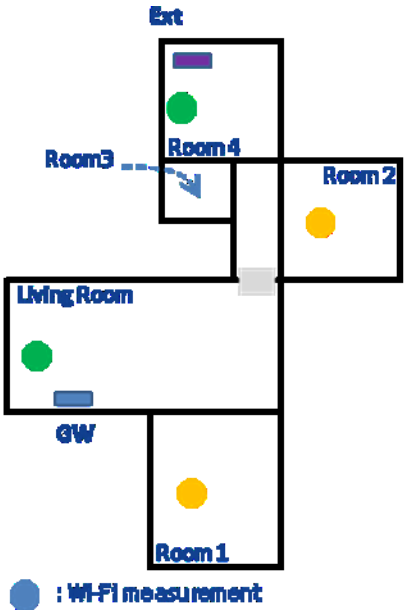

Figure 2: Wi-Fi Coverage

5.4.2 Wi-Fi Interference

Wi-Fi interference occurs when Wi-Fi channels and bands overlap with neighbor networks where activity of devices, access points and extenders in these networks interfere with transmissions leading to lower throughput throughout the home. In Figure 3 the contention occurs in networks where the neighboring Wi-Fi networks (shaded) overlap with the Wi-Fi networks in the home. Usually the neighboring networks are not in the same residence of the subscriber.

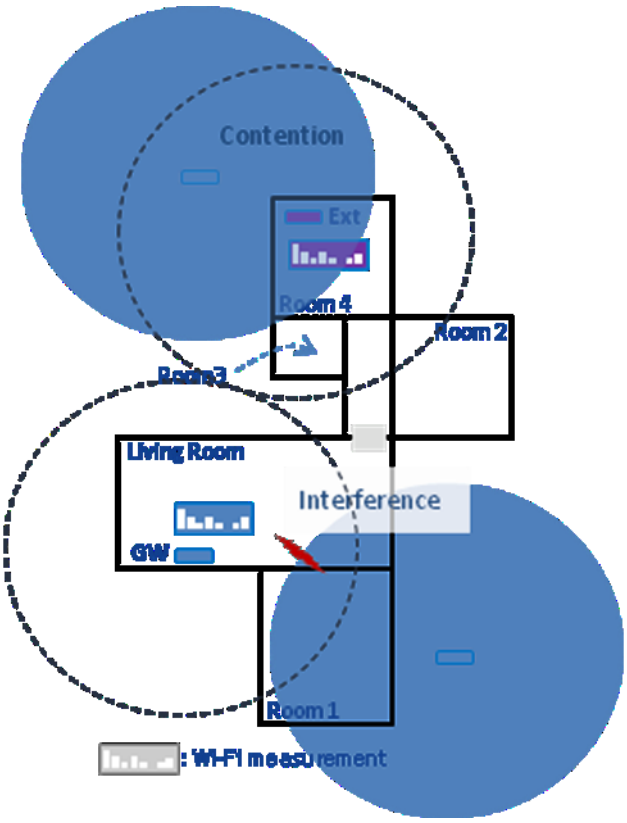

Figure 3: Wi-Fi Interference

6 Terminology

6.1 References

The following references are of relevance to this Marketing Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Marketing Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-143	*Enabling Network Throughput Performance Tests and Statistical Monitoring*	Broadband Forum	2015
[2] TR-181	*Device Data Model for TR-069*	Broadband Forum	2016
[3] RFC 792	*Internet Control Message Protocol*	IETF	1981
[4] RFC 826	*An Ethernet Address Resolution Protocol*	IETF	1982
[5] RFC 2131	*Dynamic Host Configuration Protocol*	IETF	1997
[6] RFC 4443	*Internet Control Message Protocol v6*	IETF	2006
[7] RFC 4861	*Neighbor Discovery for IP version 6 (IPv6)*	IETF	2007
[8] RFC 5227	*IPv4 Address Conflict Detection*	IETF	2008
[9] RFC 6762	*Multicast DNS*	IETF	2013
[10] RFC 6763	*DNS-Based Service Discovery*	IETF	2013
[11] 802.1Q	*Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks*	IEEE	2011
[12] 802.1AB	*Station and Media Access Control Connectivity Discovery*	IEEE	2005
[13] 1905.1a	*Standard for Convergent Digital Home Network for Heterogeneous Technologies*	IEEE	2014
[14] LLTD	*Link Layer Topology Discovery Protocol Specification*	Microsoft	2010
[15] UDA 1.1	*UPnP Device Architecture 1.1*	UPnP Forum	2008

6.2 Abbreviations

This Marketing Report uses the following abbreviations:

AP	Access Point
AFT	Address Forwarding Table
ARP	Address Resolution Protocol
BDPU	Bridge Protocol Data Units
CoAP	Constrained Application Protocol
CPE	Customer Premises Equipment.
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNS-SD	Domain Name System - Service Discovery
DVD	Digital Versatile Disc
DVR	Digital Video Recorder
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LLDP	Link Layer Discover Protocol
LLTD	Link Layer Topology Discovery
MAC	Media Access Control
mDNS	Multicast Domain Name System (protocol)
NAS	Network-Attached Storage
ND	Neighbor Discovery
PC	Personal Computer
PHY	Physical layer technology
PLC	Power Line Communication
QoE	Quality of Experience
QoS	Quality of Service
RG	Residential Gateway
RTP	Real-time Transport Protocol
RTT	Round Trip Time
SSDP	Simple Service Discovery Protocol
STB	Set-Top Box
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network.

Appendix A Diagnostic Tool Descriptions

This appendix provides additional detail and references for the tools listed in Table 2.

A.1 Address Resolution Protocol (ARP) cache

- **Defined in:** RFC 826 [4], RFC 5227 [8]
- **Implemented in:** all IPv4 capable devices
- **Output:** All devices maintain an ARP cache with IPv4 address and MAC address of responses to the ARP messages they sent.
- **How it works:** All IPv4-capable hosts and routers send an ARP message to discover the MAC address of IP addresses they want to send an IPv4 message to on the local subnet. This information is maintained in an ARP cache. It is also possible for devices to send ARP messages to discover all devices on the subnet (some routers periodically send an ARP to all IPv4 addresses on the subnet) or to ensure continued connectivity to a particular device (some devices send frequent periodic ARP messages to the IPv4 gateway address). The ARP cache is periodically flushed, but the frequency of flushing is implementation-dependent.
- **Limitations:** If devices enter and leave the home network or enter sleep modes, the ARP cache can become stale and not representative of whether an IPv4 address still maps to the same MAC address or is still present on the subnet.

A.2 DHCPv4

- **Defined in:** RFC 2131 [5]
- **Implemented in:** all IPv4 capable devices
- **Output:** The RG and other routers can provide a list of all IPv4 addresses they have provided and the associated MAC address.
- **How it works:** All IPv4-capable devices must obtain IPv4 address in order to communicate with other devices. After joining, device sends out broadcast for any available reachable DHCP server. IP address is given out by DHCPv4 server, and there can be more than one such server available in home network. DHCPv4 server keeps track of given IP addresses. Each IP address is given out to particular device with lease time (typically 24 hours), after which period it will expire, unless renewed by DHCPv4 server upon request from the device.
- **Limitations:** If devices enter and leave the home network without explicitly releasing own IP address, it will take some time before DHCPv4 server becomes aware that device has left the network.

A.3 Domain Name System - Service Discovery (DNS-SD) / Multicast DNS (mDNS)

- **Defined in**: DNS-SD defined in RFC 6763 [10]; mDNS defined in RFC 6762 [9]
- **Implemented in**: discovery of DNS-SD-advertised services using mDNS queries is implemented in PCs (all operating systems), smart phone operating systems, tablet operating systems; advertisement of DNS-SD service records (included in responses to mDNS queries) is implemented by printers and also some other devices
- **Output**: DNS resource records related to DNS-SD and for providing the relevant IPv4 and IPv6 addresses
- **How it works**: Devices that advertise services using DNS-SD will send DNS resource records in unsolicited mDNS responses. They will also provide these records when queried for them from either mDNS or unicast DNS. Devices that discover DNS-SD-advertised services can passively listen for the advertisements or actively discover by sending mDNS queries.
- **Limitations**: Used widely for discovering and advertising printers, but not as extensively for discovering and advertising other services.

A.4 Frame Counts

- **Defined in:** N/A
- **Implemented in:** many devices that keep track of interface statistics – such as RGs and Wi-Fi APs
- **Output:** Number of successfully transmitted frames, number of retransmissions, number of failed transmissions, total number of transmitted frames.
- **How it works:** transmitting device keeps track of total number of Ethernet (MAC layer) or Wi-Fi frames that have been transmitted on the link layer.
- **Limitations:** Not supported on all devices. Provides no direct higher layer information.

A.5 ICMPv6

- **Defined in**: RFC 4443 [6]
- **Implemented in**: all IPv6-capable devices
- **Output**: Provides similar to ping (see A.13) and traceroute (see A.15) capabilities, but done over IPv6
- **How it works**: See descriptions of ping (A.13) and traceroute (A.15). ICMPv6 is very analogous to ICMPv4, and provides similar functionality.
- **Limitations**: Requires IPv6

A.6 IEEE 1905.1

- **Defined in:** IEEE 1905.1 and IEEE 1905.1a [13] (1905.1 is used here to refer collectively to both 1905.1 and 1905.1a)
- **Implemented in:** currently only implemented in a small number of devices
- **Output:** Each 1905.1 device creates and maintains its own list of other 1905.1 devices, based on their responses to periodically sent messages.

- **How it works:** IEEE 1905.1 messages are defined for a variety of physical layer technologies. The protocol uses a Control Message Data Unit (CMDU) to send Type-Length-Value encoded information among 1905.1-enabled devices on the local link. The CMDUs are communicated directly over the Link layer of the different supported technologies and without the use of an IP stack. Every 1905.1-enabled device receives 1905.1 messages from all other 1905.1-enabled devices on the local link, which allows each device to have information on the physical layer network topology. IEEE 1905.1 makes use of LLDP (see A.9) to discover bridging devices that do not support IEEE 1905.1.
- **Limitations:** Only works among 1905.1-enabled devices, of which there are few.

A.7 Iperf

- **Defined in**: based on *ttcp* application developed by National Center for Supercomputing Application of University of Illinois.
- **Implemented in**: Can be downloaded as an application for all common computer operating systems.
- **Output**: time-stamped report of the amount of data transferred between originating node and end-device and the throughput measured.
- **How it works**: it creates TCP and UDP data streams from originating device to end-device and measures the throughput of the path between them. It allows the user to set various parameters that can be used for testing a network, or alternatively for optimizing or tuning a network.
- **Limitations**: Both originating device and end-device must have Iperf installed.

A.8 IPv6 Neighbor Discovery (ND)

- **Defined in**: RFC 4861 [7]
- **Implemented in**: all IPv6 capable devices.
- **Output**: similar to ARP in IPv4, IPv6 ND results in list of IPv6 addresses and corresponding MAC addresses of devices on the same network segment.
- **How it works**: the IPv6 neighbor discovery process uses Internet Control Message Protocol version 6 (ICMPv6) messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices..
- **Limitations**: Requires IPv6.

A.9 Link Layer Discovery Protocol (LLDP)

- **Defined in:** IEEE 802.1AB [12]
- **Implemented in:** all LLDP capable devices.

- **Output:** Information that may be sent using LLDP includes system name and description, link layer port name and description, system capabilities (switching, routing, etc.), and MAC/PHY information.
- **How it works:** Link Layer Discovery Protocol (LLDP) is discovery protocol standardized by IEEE as 802.1AB. It runs over the Link layer and it allows locally attached devices in a network, such as switches and routers, to advertise information about themselves to listening devices. Devices in network continuously broadcast and listen for LLDP messages, so they can discover when a new device is added or one removed. In this way, they maintain an accurate picture of a dynamic network. It works with routers and switches, and thus does not provide overall picture of connectivity which includes end-devices.
- **Limitations:** device must support LLDP.

A.10 Link Layer Topology Discovery (LLTD)

- **Defined in:** LLTD specification [14] (proprietary protocol developed by Microsoft).
- **Implemented in:** all LLTD capable devices (typically Windows based).
- **Output:** Link Layer Network Map.
- **How it works:** Being a Link Layer implementation, LLTD operates strictly on a given local network segment. It cannot discover devices across routers, an operation which would require Internet Protocol level routing. The LLTD Mapper I/O component is the master module which controls the discovery process and generates the Network Map.
- **Limitations:** supported on Windows devices.

A.11 Packet Counts

- **Defined in: N/A**
- **Implemented in:** many devices which keep track of statistics – such as RGs and Wi-Fi APs
- **Output:** Number of successfully transmitted packets, number of retransmissions, number of failed transmissions, total number of transmitted packets.
- **How it works:** transmitting device keeps track of total number of packets that have been transmitted. If packets are sent using transfer control protocol like TCP, which includes acknowledgement of successful reception of packet(s), transmitting device can keep track of success/failure rate. If retransmissions are supported by transfer control protocol, transmitting device can keep track of that too.
- **Limitations:** Transfer control protocol must support return information on successfully received packets.

A.12 Physical technology metrics

- **Defined in:** standards documents of PHY technologies
- **Implemented in:** many devices which keep track of PHY interface statistics – such as RGs and Wi-Fi APs

- **Output:** it can be detecting presence of interference, received signal power, received and transmitted bits, physical layer beacon information, and other physical layer statistics
- **How it works:** transceivers collect statistics
- **Limitations:** Many statistics are unavailable in some devices. Provides no direct higher layer information.

A.13 Ping (ICMPv4)

- **Defined in:** RFC 792 [3].
- **Implemented in:** all IPv4 devices.
- **Output:** Round trip time and packet loss to specific device (given by hostname or IPv4 address).
- **How it works:** Ping is the simplest and most widely used part of ICMPv4 which is used to test the connectivity and Round Trip Time (RTT) of simple packets. Single packet is transmitted to probed device. Upon received response from probed device, and assuming that there are no processing delays and waiting in queues, time difference between sending and receiving response indicates latency on the link.
- **Limitations:** Ping is prone to delays in the queues on the way from originator to destination and back. Due to presence of other data sources in home network which might be using the same link, there is variation in obtained result. Does not test UDP or TCP.

A.14 Spanning Tree Protocol

- **Defined in:** IEEE 802.1Q [11]
- **Implemented in:** most Ethernet bridges and switches
- **Output:** list of all IP addresses of devices on path from originating device (RG) to end-device, their domain names and 3 RTT (per device) from originating device to each of devices on path.
- **How it works:** The most straightforward approach to network topology discovery is to read out the Address Resolution Protocol (ARP) or Address Forwarding Tables (AFTs) stored in the switches in the network, and using the Spanning Tree Protocol (STP) for further topology discovery. STP creates a spanning tree within a network of connected bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. The bridges use special data frames called Bridge Protocol Data Units (BPDUs) identify themselves to other switches.
- **Limitations:** discovers MAC layer bridges and switches.

A.15 Traceroute (ICMPv4)

- **Defined in:** RFC 792 [3]
- **Implemented in:** supported by all devices supporting ICMP [6].

- **Output:** list of all IP addresses of devices on path from originating device to end-device, their domain names. and corresponding round trip times
- **How it works:** The route is recorded as the round-trip times of the packets received from each successive host on the route from originating device to end-device. Times are averaged (in 3 iterations) by sending probing packets from the originating device to each device on the path to end-device. Averaged list of times from the originating device to each device on the path is recorded by the originating device.
- **Limitations:** Does not measure UDP or TCP, and does not indicate how much of the round trip time was in each direction.

A.16 UPnP SSDP

- **Defined in:** UPnP Device Architecture (UDA) 1.1 [15]
- **Implemented in:** UPnP Devices implement advertisement and notification elements, while UPnP Control Points implement discovery.
- **Output:** UPnP Control Point can provide a list of discovered UPnP Devices and their UPnP Services.
- **How it works:** UPnP SSDP is an Application layer solution for device discovery in networks. It allows UPnP Devices to send advertisements that can be seen by Control Points, and for Control Points to send discovery messages. Control Points can perform actions on discovered Services.
- **Limitations:** Devices must support UPnP. For the RG to provide a list of UPnP Services, it must implement

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Marketing Report has been approved by members of the Forum. This Marketing Report is subject to change. This Marketing Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Marketing Report may be copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Marketing Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Marketing Report, or use of any software code normatively referenced in this Marketing Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Marketing Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Marketing Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Marketing Report except to the extent this Marketing Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Marketing Report are not deemed to be derivative works of the Marketing Report.

2. NO WARRANTIES

THIS MARKETING REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS MARKETING REPORT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS MARKETING REPORT.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE MARKETING REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY

SUCH RIGHTS ARE DESCRIBED ON THE MARKETING REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

The text of this notice must be included in all copies of this Marketing Report.

End of Broadband Forum Marketing Report MR-363