OpenCable™ Specifications
Host Extensions

OpenCable Host Home Networking Extension 2.0

OC-SP-HOST-HN2.0-I07-130418

ISSUED

DISCLAIMER

This document is published by Cable Television Laboratories, Inc. ("CableLabs®").

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various agencies; technological advances; or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein. CableLabs makes no representation or warranty, express or implied, with respect to the completeness, accuracy, or utility of the document or any information or opinion contained in the report. Any use or reliance on the information or opinion is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any cable member to purchase any product whether or not it meets the described characteristics. Nothing contained herein shall be construed to confer any license or right to any intellectual property, whether or not the use of any information herein necessarily utilizes such intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	OC-SP-HOST-HN2.0-I07-130418			
Document Title:	OpenCable Host Home Networking Extension 2.0			
Revision History:	I01 - Released 4/18/08 I02 - Released 5/8/09 I03 - Released 12/11/09 I04 - Released 5/7/10 I05 - Released 5/12/11 I06 - Released 1/12/12 I07 - Released 4/18/13			
Date:	April 18, 2013			
Status:	~~Work in Progress~~	~~Draft~~	**Issued**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Key to Document Status Codes:

Work in Progress	An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Tables

Figures

This page intentionally left blank.

1 SCOPE

1.1 Introduction and Overview

The OpenCable Host specification [HOST] defines bidirectional digital set-top boxes (OCS2) and bidirectional integrated terminal devices (OCT2). This specification defines the requirements for either OCS2 or OCT2 devices to be extended to include IP-based Phase 2 home networking support and enable home networking features to be implemented using the OCAP Home Networking Extension specification [OCAP-HN]. Phase 2 home networking includes support for new physical networks, QoS, and secure transmission of MSO premium content.

Three primary use cases are specifically supported to enable multi-room DVR functionality. The three use cases are:

- Playback of DVR-recorded content from a non-DVR device,
- Scheduling DVR recording from a non-DVR device,
- Trick Modes (Pause/rewind/fwd) from a non-DVR box.

1.2 Purpose of Document

This specification defines minimum technical requirements that must be added to an OpenCable Host device to support OCAP Phase 2 Home Networking Extensions.

1.3 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"SHALL"	This word means that the item is an absolute requirement of this specification.
"SHALL NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific:

- For a specific reference, subsequent revisions do not apply.
- For a non-specific, non-Bundle reference, the latest version applies.
- For non-specific CableLabs references that are part of the [OC-BUNDLE], the versions mandated in a particular Bundle apply.

[47CFR76]	Code of Federal Regulations, Part 76, Subpart W - Encoding rules, §76.1908.
[HN-MIB]	OpenCable Home Networking MIB Specification, OC-SP-MIB-HN, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].
[HNP]	OpenCable Home Networking Protocol 2.0, OC-SP-HNP2.0, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].
[HOST]	OpenCable Host Device 2.1 Core Functional Requirements, OC-SP-HOST2.1, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].
[HOST-DVR]	Host 2.X DVR Extension, OC-SP-HOST2-DVREXT, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].
[IEEE 802.1D]	IEEE 802.1D-2004: IEEE standard for local and metropolitan area networks--Media access control (MAC) Bridges (Incorporates IEEE 802.1t-2001 and IEEE 802.1w).
[IEEE 802.3]	IEEE 802.3-2002: IEEE Standard for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification, March 8, 2002.
[MoCA]	MoCA MAC/PHY v1.0 spec; MoCA-M/P-SPEC-V1.0-08292008.
[MoCA Ext]	MoCA MAC/PHY v1.1 extension spec; MoCA-M/P-SPEC-V1.1-09032008.
[MoCA SMI]	MoCA Enterprise Structure of Management Information, document MOCA-SMI-V1.0-09222008.
[OC-BUNDLE]	OC-SP-BUNDLE, OpenCable Bundle Requirements. See Section 2.3.1 to acquire this specification.
[OCAP]	OpenCable Application Platform (OCAP), OC-SP-OCAP, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].
[OCAP-DVR]	OCAP Digital Video Recorder (DVR), OC-SP-OCAP-DVR, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].
[OCAP-HN]	OCAP Home Networking Extension, OC-SP-OCAP-HNEXT, Cable Television Laboratories, Inc. Referenced in [OC-BUNDLE].

[RFC 2131] IETF RFC 2131, Dynamic Host Configuration Protocol. R. Droms. March 1997.

[RFC 2132] IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997.

[RFC 2863] IETF RFC 2863, The Interfaces Group MIB. K. McCloghrie, F. Kastenholz. June 2000.

[RFC 3203] IETF RFC 3203, DHCP reconfigure extension. Y. T'Joens, C. Hublet, P. De Schrijver. December 2001.

[RFC 3396] IETF RFC 3396, Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4). T. Lemon, S. Cheshire. November 2002.

[RFC 3927] IETF RFC 3927, Dynamic Configuration of IPv4 Link-Local Addresses. S. Cheshire, B. Aboba, E. Guttman. May 2005.

[RFC 4293] IETF RFC 4293, Management Information Base for the Internet Protocol (IP). S. Routhier, Ed., April 2006.

[RSD PROT] Reserved Services Domain Protocols 1.0 Specification, OC-SP-RSD-PROT-I01-080828, August 28, 2008, Cable Television Laboratories, Inc.

[RSD TECH] Reserved Services Domain Technology 1.0 Specification, OC-SP-RSD-TECH-I01-080630, June 30, 2008, Cable Television Laboratories, Inc.

[UPnP ARCH] UPnP Device Architecture 1.1, October 2008.

2.2 Informative References

This specification uses the following informative references.

[OCHN ARCH] OpenCable Home Networking Architecture 2.0 Technical Report, OC-TR-HN-ARCH2.0-D01-080418, April 18, 2008, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

2.3.1 OpenCable Bundle Requirements

The OpenCable Bundle Requirements specification [OC-BUNDLE] indicates the set of CableLabs specifications required for the implementation of the OpenCable Bundle. The version number of [OC-BUNDLE] corresponds to the release number of the OpenCable Bundle that it describes. One or more versions of [OC-BUNDLE] reference this specification. Current and past versions of [OC-BUNDLE] may be obtained from CableLabs at http://www.cablelabs.com/opencable/specifications.

2.3.2 Other References

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: http://www.cablelabs.com /
- IEEE, www.ieee.org
- Code of Federal Regulations, National Archives and Records Administration,
  www.gpoaccess.gov/cfr/index.html

3 TERMS AND DEFINITIONS

This specification contains the following terms and definitions.

IP provisioning data set	The set of parameters from previous DHCPv4 and DHCPv6 messages, and/or Router Advertisements stored for later use.
OpenCable Bundle	The OpenCable Bundle defines a set of specifications required to build a specific version of an OpenCable device. See [OC-BUNDLE].
OpenCable Digital Media Player	An OpenCable Home Networking device capable of playing digital media across an IP-based network. It is a UPnP-compliant Digital Media Player with additional requirements imposed by OpenCable.
OpenCable Digital Media Server	An OpenCable Home Networking device capable of serving digital media across an IP-based network. It is a UPnP-compliant Digital Media Server with additional requirements imposed by OpenCable.
OpenCable Host Device 2.1	A cable receiver that is compliant with one of the hardware profiles defined by this specification. The OCHD2.1 profiles include: • OpenCable Set-top 2.1 (OCS2.1) • OpenCable Terminal 2.1 (OCT2.1)
OpenCable Set-top 2.1	A cable receiver that has no integrated display and is compliant with the OCS2.1 profile defined by this specification.
OpenCable Terminal 2.1	A cable receiver that includes an integrated display and is compliant with the OCT2.1 profile defined by this specification.
Out-Of-Band Messaging	The control and information messages sent from the Network Controller via the Host to the CableCARD requiring a dedicated QPSK channel or DSG channel that may contain the following types of messages: • Conditional Access (CA) messages including entitlements • System Information (SI) messages • Electronic Program Guide (EPG) messages • Emergency Alert System (EAS) messages • Other generic messages
Policy-based Routing	Policy-based routing (PBR) provides a mechanism for forwarding/routing of data packets based on the policies defined by the network administrator. An example of this might be forwarding a packet based on the IP source address.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

AV	Audio/Video
DHCP	Dynamic Host Configuration Protocol
HNHost	Home Networking Host
LAN	Local Area Network
MAC	Media Access Control
OC-DMP	OpenCable Digital Media Player
OC-DMS	OpenCable Digital Media Server
OCAP	OpenCable Application Platform Specification
OCAPHN	OCAP Home Networking Extension
PBR	Policy-Based Routing

5 TECHNICAL REQUIREMENTS

This section contains the technical requirements for this specification.

5.1 General Requirements

5.1.1 OpenCable HOST 2.1 Compliance

The HNHost SHALL comply with all normative requirements in [HOST].

If the HNHost implements Digital Video Recorder (DVR) functionality, the device SHALL comply with all normative requirements in [HOST-DVR].

5.1.2 Middleware

The HNHost SHALL comply with all normative requirements of [OCAP-HN].

The HNHost SHALL support the mapping between the OCAP Home Networking Extension API [OCAP-HN] and LAN protocol messaging as defined in [HNP].

5.2 Network Interface

5.2.1 Physical and MAC Layers

The HNHost MAY implement one or more physical network interfaces that meet the requirements as specified in [RSD TECH]. Such network interfaces are termed the RSD Technology interface.

If an HNHost includes a MoCA interface, it SHALL do so as per the [MoCA] and [MoCA Ext] specifications.

The HNHost SHALL provide a 10BASE-T / 100BASE-TX Ethernet physical interface and MAC layer for the LAN interface as specified in IEEE 802.3i and IEEE 802.3u [IEEE 802.3].

The HNHost MAY provide multiple network interfaces. When two or more interfaces are enabled at the same time, the HNHost SHALL implement a layer 2 bridge to connect the interfaces and implement the Spanning Tree Protocol [IEEE 802.1D] to avoid bridge loops. If an HNHost provides more than one concurrent network interface to the home network, the HNHost SHALL bridge between the home network interfaces.

An HNHOST can implement more than one network interface to the home network, or can enable only one interface at a time. In this case, the HNHost is not required to implement any loop mitigation protocol.

A network interface implemented by an HNHost SHALL be either one of the bridged interfaces or one of the pool of interfaces that can be enabled one at a time on the home network.

When an HNHost bridges a frame, as opposed to the HNHost being the source or the destination of the frame, the HNHost SHALL forward the frame between its interfaces.

Any home network interface implemented by an HNHost SHALL provide a capability to enable or disable the interface using the ifAdminStatus object as defined in [HN-MIB].

5.2.2 Network Layer

The HNHost SHALL provide a network and transport layer for the LAN interface as specified in [HNP].

5.3 Media Types

The HNHost SHALL support rendering of AV media types and formats as specified in [HOST], [OCAP], and [HNP]. This includes both broadcast streaming and monomedia-based content formats.

The HNHost SHALL support serving of AV media types and formats as specified in [HOST], [OCAP], and [HNP] if the device implements [HOST-DVR]. This includes both broadcast streaming and monomedia-based content formats.

5.4 Quality of Service (QoS)

The HNHost MAY implement RSD Manager and RSD Controller functionality as defined in [RSD PROT].

If the HNHost consists of only one RSD Technology interface or multiple non-bridged RSD Technology interfaces, then the HNHost SHALL implement RSD Host functionality as defined in [RSD PROT].

If the HNHost implements multiple bridged RSD Technology interfaces, then the HNHOST SHALL comply with the RSD Bridge functionality as defined in RSD-PROT Specifications [RSD PROT].

If the HNHost implements Ethernet interface that is bridged to the RSD Technology interface, then the HNHost SHALL comply with the PSD Bridge functionality as defined in the [RSD PROT] specifications.

5.5 Content Security

The HNHost SHALL follow encoding and distribution rules for distribution of protected cable-delivered content as specified by [47CFR76].

5.6 Device Interoperability

The HNHost SHALL comply with the requirements specified in [HNP].

5.7 SNMP Requirements

5.7.1 OpenCable Home Networking Extension 2.x SNMP Management Requirements

The HNHost SHALL implement the MIB objects of OC-HOME-NETWORK-MIB as described in Annex A of [HN-MIB].

The HNHost SHALL utilize the same SNMP Access Control method(s) as the OCHD2.1.

The HNHost SHALL NOT allow SNMP access through the Home Network interface(s).

The HNHost SHALL implement the eSTB IF-MIB [RFC 2863] as defined in Table 2 in accordance with the following requirements:

The HNHost SHALL implement the ifAdminStatus object to provide administrative control over the MAC interfaces. This object may be used to reset the interface remotely.

The HNHost SHALL assign ifIndex integer values 3 and above to the HN interface(s).

Note: The OCHD2.1 uses the ifIndex values of "1" and "2" for the eSTB(1) and the Card(2) respectively.

The HNHost SHALL report the interface technology manufacturer, current hardware/software interface version, and the highest hardware/software interface version supported in the ifDescr object described in Table 1.

The HNHost SHALL report each type-value pair in Table 1 separated with a colon and blank space. Each pair is separated by a ";" followed by a blank space. For instance, an ifDescr of an RSD technology from vendor X, current version 1.3.a, highest supported version 1.4 will be as follows:

any text<<MFG: X; CURR_VER: 1.3.A; HIGHEST_VER: 1.4 >>any text

Table 1 - [RFC 2863] ifDescr Format

To report	Format of each field
Technology Mfg Name	MFG: <Manufacturer name>
Current interface version	CURR_VER: <current version of i/f>
Highest interface version	HIGHEST_VER: <highest version of i/f>

The HNHost SHALL report the IANA technology type of the RSD technology implemented by the interface in the ifType object.

Table 2 - [RFC 2863] ifTable, MIB-Object Details for Home Network Interfaces

MIB Object	eSTB (see [HOST])	Card (see [HOST])	RSD Technology
ifIndex:			≥ 3
ifDescr			See requirement above
ifType			IANA assignment
ifMtu			(n)
ifSpeed			(n)
ifPhysAddress			I/F MAC Address
ifAdminStatus			up(1), down(2) *
ifOperStatus			up(1), down(2)
ifLastChange			[RFC 2863]
ifInOctets			(n)
ifInUcastPkts			(n)
ifInDiscards			(n)
ifInErrors			(n)
ifInUnknownProtos			(n)
ifOutOctets			(n)
ifOutUcastPkts			(n)
ifOutDiscards			(n)

MIB Object	eSTB (see [HOST])	Card (see [HOST])	RSD Technology
ifOutErrors			(n)
ifXTable			
ifName			[RFC 2863]
ifInMulticastPkts			(n)
ifInBroadcastPkts			(n)
ifOutMulticastPkts			(n)
ifOutBroadcastPkts			(n)

*All interfaces start with ifAdminStatus in the up(1) state. Changing the ifAdminStatus to down forces a reset of the interface but does not bring the interface to "up" status. This must be done by an SNMP Set command. This allows the operator to control when the interface is enabled.

The HNHost SHALL extend the eSTB ipAddressTable [RFC 4293] for the Home Network interfaces using the ifIndex assignments in the ifTable described in Table 2 above. The ipAddressTable is used to report all IP address assignments for each interface.

5.7.2 MoCA SNMP MIBs

When an HNHost supports a MoCA network interface, it SHALL make the MoCA SNMP MIBs available to applications from the MIBManager API at the OIDs defined by the [MoCA SMI] specification. See the [MoCA] specification for the MoCA MIB definition.

The [OCAP] specification defines how applications are granted read and write access to Host device MIBs.

5.8 Jitter

The HNHost performs the de-jitter operation. The MPEG standard allows only about 4-ms of jitter. Network jitter often may exceed this threshold. The HNHost provides a de-jitter buffer.

When operating as an OC-DMP, the HNHost SHALL support a de-jitter operation and provide a de-jitter buffer of at least 200 ms.

When operating as an OC-DMS, the HNHost SHALL maintain an index file based on PCR chunks and provide a de-jitter buffer of at least 200 ms.

5.9 WAN/LAN Interface IP Address Acquisition

The HNHost contains both WAN and LAN networking interfaces that are provisioned separately although these interfaces share a common IP network stack (i.e., a separate, isolated networking stack for the LAN interface is not required). The HNHost is considered to be a multi-homed IP host (a host connected to multiple networks) but with IP packet forwarding between the WAN and LAN interfaces disabled.

5.9.1 DHCP Requirements

The HNHost SHALL perform IP provisioning independently on the WAN interface and the LAN interface.

The HNHost SHALL only acquire an IPv4 address for the LAN interface.

When multiple LAN network interfaces are enabled at the same time, and bridging is therefore enabled, the HNHost SHALL perform the IP provisioning process on the virtual bridge interface and not the individual network interfaces.

The HNHost SHALL acquire an IPv4 and/or IPv6 IP address for the WAN interface according to the requirements in section 13 of [HOST].

For the LAN network interface with a valid DHCPv4 lease, the HNHost SHALL retain the entire contents of the DHCPv4 OFFER message in its IP provisioning data set.

For the WAN network interface with a valid DHCPv4 lease, the HNHost SHALL retain the entire contents of the DHCPv4 OFFER message in its IP provisioning data set.

For the WAN network interface with a valid DHCPv6 lease, the HNHost SHALL retain the entire contents of the DHCPv6 Advertise message in its IP provisioning data set.

For the WAN network interface with IPv6 enabled, the HNHost SHALL retain the entire contents of the most recent Router Advertisement message in its IP provisioning data set.

If the WAN interface goes down (i.e., has an ifOperStatus other than up), the HNHost SHALL discard all provisioning information in its IP provisioning data set obtained from that interface, including the DHCPv4 ACK, DHCPv6 REPLY, and the IPv6 Router Advertisement.

If the LAN interface goes down (i.e., has an ifOperStatus other than up), the HNHost SHALL discard all provisioning information in its IP provisioning data set obtained from that interface.

Note: When multiple LAN network interfaces are enabled, the LAN interface is only considered down when all component interfaces are simultaneously down.

Upon an IP provisioning change event, the HNHost SHALL update its IP provisioning data set, reset all routing tables, and rebuild the routing tables using the cached information.

The following are considered IP provisioning change events:

- DHCPv4 lease acquisition, renewal, or expiration on any interface
- DHCPv6 lease acquisition, renewal, or expiration on the WAN interface
- Change to IPv6 Router Advertisement
- WAN interface goes down
- LAN interface goes down

Note: When multiple LAN network interfaces are enabled, the bridged LAN interface is only considered down when all component interfaces are simultaneously down.

The HNHost SHALL discard the TTL parameter received from the LAN interface.

5.9.2 IP Routing Table Construction

The HNHost constructs multiple IP routing tables with separate tables for the WAN and LAN side network interfaces. This allows an application to have IP access to both interfaces.

If the HNHost has WAN access only (WAN ifOperStatus up, LAN ifOperStatus down on all LAN interfaces), it obtains DHCP parameters from the WAN interface to form the MAIN and DOCSIS routing tables (HN table is empty).

If the HNHost has LAN access only (WAN ifOperStatus down, LAN ifOperStatus up on 1 or more interfaces) and is using dynamic IP address acquisition, it obtains DHCP parameters from the LAN-side server to form the MAIN and HN routing tables (DOCSIS table is empty).

If the HNHost has both WAN and LAN access (WAN ifOperStatus up, LAN ifOperStatus up on 1 or more interfaces) and is using dynamic IP address acquisition on the LAN interface, it obtains DHCP parameters from both networks to form the MAIN, DOCSIS, and HN routing tables.

After obtaining the WAN and LAN-side IP addresses, Subnet Masks and Default Gateway address, the steps that must be performed are:

- Create the WAN-side, LAN-side and Main routing tables
- Create the Routing Policy Database with the following entries
    - WAN-side rule with highest priority
    - LAN-side rule with next highest priority
    - MAIN table rule with lowest priority
- Create a new socket and bind it to the local LAN IP address
- Create a new socket and bind it to the local WAN IP address, if necessary

An application obtains a LAN IP address using the classes and methods described in section 6.8 of [OCAP-HN].

An application can also obtain a WAN IP address using the classes and methods described in section 6.8 of [OCAP-HN] if it needs to send and receive traffic using the WAN interface.

An application can use the approach described in section 6.8 of [OCAP-HN] to associate (bind) a socket with a particular global IP address belonging to the HNHost device. A socket associated with a public IP address belonging to the WAN interface is referred to as a DOCSIS socket. A socket associated with a public IP address belonging to the LAN interface is referred to as an HN socket. All other sockets will be referred to as unbound sockets or simply sockets.

The HNHost SHALL support multiple routing tables using a policy-based routing mechanism along with socket binding to direct IP traffic to the proper interface.

The HNHost SHALL implement the following independent routing tables in its network stack:

- a DOCSIS routing table (WAN-side)
- an HN routing table (LAN-side)
- a Main routing table

Note: The DOCSIS routing table does not refer to the eCM routing table.

The HNHost SHALL construct the DOCSIS routing table entirely from the cached DHCPv4, DHCPv6, and Router Advertisement messages received on the WAN interface.

The HNHost SHALL construct the HN routing table from the cached DHCPv4 messages received on the LAN interface if the HNHost has obtained a valid DHCPv4 lease.

The HNHost SHALL install the route for Auto-IP devices (169.254.0.0/16) on the LAN interface in the HN routing table.

When the LAN interface does not have a valid DHCPv4 lease, the HNHost SHALL install a default route without a gateway for the LAN interface in the HN routing table. In this case there is no default gateway present and hosts are directly reachable on the LAN interface.

Note: This default route without a gateway is referred to as the default Auto-IP route.

The HNHost SHALL construct the Main routing table as follows:

- The DHCPv4, DHCPv6, and Router Advertisements received from the WAN interface will be used to create routes.
- The DHCPv4 messages received from the LAN interface if it has obtained a valid DHCPv4 lease.
- Install the route for Auto-IP devices (169.254.0.0/16) on the LAN interface in the MAIN routing tables.
- The default route created from DHCPv4 messages received from the LAN interface will be assigned a lower priority than the default route created with WAN provisioning information.

The HNHost SHALL use all DNS Server IP addresses obtained from any DHCPv4 or DHCPv6 messages received on the WAN interface.

The HNHost SHALL use all DNS Server IP addresses obtained from any DHCPv4 messages received on the LAN interface.

When performing a DNS lookup, the HNHost SHALL query all DNS server addresses obtained from the WAN interface before querying any DNS server addresses obtained from the LAN interface.

The HNHost SHALL associate the Hostname assigned from the WAN interface to the addresses assigned to the WAN interface.

The HNHost SHALL associate the Hostname assigned from the LAN interface to the addresses assigned to the LAN interface.

When making routing decisions for DOCSIS sockets, the HNHost SHALL use the DOCSIS routing table.

When making routing decisions for HN sockets, the HNHost SHALL use the HN routing table.

When making routing decisions for unbound sockets, the HNHost SHALL use the Main routing table.

5.9.3 LAN Interface DHCP Requirements

The following requirements are applicable only when the HNHost acquires a dynamic LAN IP address via DHCPv4.

The HNHOST DHCP client behavior during all phases of operation, including initial IP address lease acquisition and lease renewal, SHALL be in accordance with the Client requirements of [RFC 2131] and the DHCP option requirements of [RFC 2132].

The following fields SHALL be present in the DHCPDISCOVER and DHCPREQUEST message from the HNHOST and set as described below.

The hardware type (htype) SHALL be set to 1 (Ethernet).

The hardware length (hlen) SHALL be set to 6.

The client hardware address (chaddr) SHALL be set to one of the 48-bit MAC addresses associated with the LAN interface of the HNHOST if the interface is bridged; otherwise it is set to the single 48-bit MAC address of the interface. This MAC address is distinct from the MAC address assigned to the DOCSIS WAN interface.

The Client-identifier option (61) SHALL be included with the hardware type set to 1 and the value set to the same 48-bit MAC address as the chaddr field.

The "parameter request list" option (55) SHALL be included with the following option codes present in the list:

Option code 1 (Subnet Mask)

Option code 3 (Router Option)

Option code 6 (Domain Name Server)

Option code 15 (Domain Name)

Option code 51 (IP address lease time)

Option code 54 (Server Identifier)

To enable class identification, DHCP option 60 SHALL be included, containing the character string "OpenCable2.1" using characters from the NVT ASCII character set with no terminating NULL.

The following requirements pertain to the DHCPOFFER/DHCPACK message.

The HNHOST SHALL ignore any DHCP options delivered by the DHCP server in the DHCP message that the HNHost does not require or cannot interpret.

The HNHOST SHALL verify the existence of the following DHCP fields within the DHCPOFFER/DHCPACK message it receives from the DHCP server during initial IP address lease acquisition:

The IP address to be used by the HNHost (yiaddr)

The subnet mask to be used by the HNHost (Subnet Mask, Option 1)

A list of IP addresses of one or more routers to be used for forwarding HNHost-originated IP traffic (Router, Option 3); the HNHost is not required to use more than one router IP address for forwarding but SHALL use at least one.

The IP Address Lease Time (Lease Time, Option 51)

The Server Identifier of the DHCP server (Server Identifier, Option 54)

If any of the following DHCP fields is absent from the DHCPACK message, the HNHOST SHALL reject the offered lease and restart its DHCP IP address acquisition process from the INIT state as defined in [RFC 2131].

- Yiaddr
- Subnet Mask, Option 1
- Router, Option 3
- Lease time, Option 51
- Server Identifier, Option 54

The HNHOST SHALL disregard any TFTP Server Name (either option 66 or 'siaddr' field of header) and Bootfile Name (either option 67 or 'file' field of header) parameters defined in a DHCPOFFER/DHCPACK message.

The HNHOST SHALL verify the existence of the following DHCP fields within the DHCPACK message it receives from the DHCP server during a DHCP Renew or Rebind.

- Yiaddr
- Subnet Mask, Option 1
- Router, Option 3
- Lease time, Option 51
- Server Identifier, Option 54

If the DHCPACK message does not contain the *yiaddr* field, the HNHOST SHALL restart its DHCP IP acquisition process from the INIT state as defined in [RFC 2131].

If any DHCP field required within the DHCPOFFER/DHCPACK message it receives from the DHCP server during initial IP address lease acquisition is missing or is invalid in the DHCPACK message during a DHCP Renew or Rebind, the HNHOST SHALL ignore the message and continue DHCP operation.

If any required DHCP field is missing or is invalid in the DHCPACK message during a DHCP Renew or Rebind, the HNHOST SHALL ignore the message and continue with DHCP operation.

Note: An example of an invalid field would be an option that is syntactically malformed (e.g., with an incorrect option length).

The HNHost SHOULD also implement a different retransmission strategy for the RENEWING and REBINDING states, as recommended in [RFC 2131], which is based on one-half of the remaining lease time.

The HNHost SHALL limit the number of retransmissions to five or fewer for the DHCPDISCOVER and DHCPREQUEST messages.

[RFC 3203] describes an extension to DHCPv4 that allows a DHCP server to send a FORCERENEW message that forces a client to renew its lease.

The HNHost SHALL ignore all received FORCERENEW messages.

The backoff values for retransmission of DHCPDISCOVER messages SHOULD be chosen according to a uniform distribution between the minimum and maximum values in the rows of Table 3.

Table 3 - DHCP Backoff Distribution Values

Backoff Number	Minimum (sec.)	Maximum (sec.)
1	3	5
2	7	9
3	15	17
4	31	33
5	63	65

Table 4 - HNHost DHCP Request

DHCP Request Options	Value	Description
CPE Option 60	"OpenCable2.1"	OpenCable Version

5.9.4 Multiple Routing Table Examples (Informative)

The Linux operating system supports multiple routing tables using an implementation called Policy Routing. This section provides an example of how to use Linux Policy Routing to fulfill the requirements in the IP Routing Table Construction section. The examples in this section assume Ubuntu 10.04 LTS is being used.

To use Linux Policy Routing, the Linux kernel should be built with both the CONFIG_IP_ADVANCED_ROUTER and CONFIG_IP_MULTIPLE_TABLES flags enabled.

5.9.4.1 Example 1: DHCPv4 on LAN

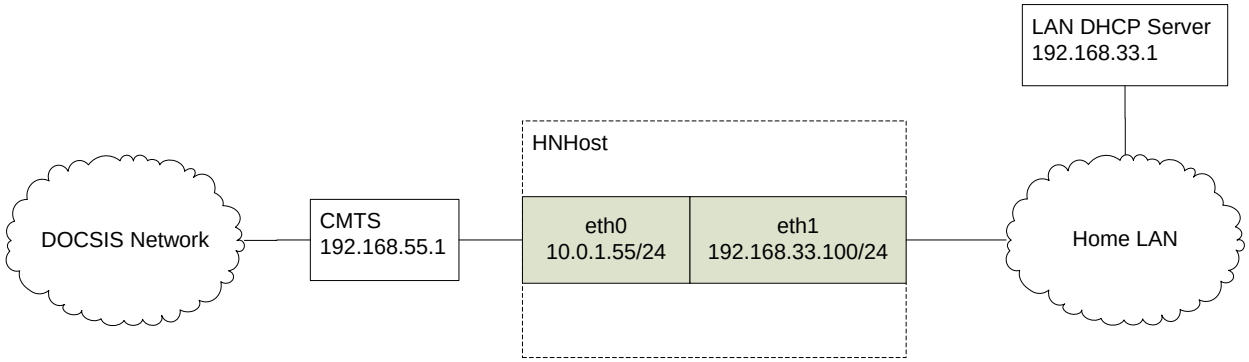

Figure 1 - DHCPv4 on LAN Reference Network

The HNHost will be provisioned by the LAN and WAN DHCP servers as follows:

	WAN DHCP Provisioning	LAN DHCP Provisioning
IPv4 Address	10.0.1.55	192.168.33.100
IPv4 Subnet Mask	255.255.255.0	255.255.255.0
IPv4 Default Gateway	10.0.1.1	192.168.33.1

Construct the Routing Tables

Linux routing tables are identified using numbers from 0 to 255. Tables `local` and `main` have the numbers 255 and 254 associated with them. The /etc/iproute2/rt tables file can be customized to assign names to each table.

```
#
# Reserved by Linux
#
255   local
254   main
253   default
```

```
0     unspec

#

# Added for Policy Routing example

#

1     hn

2     docsis
```

The DOCSIS table is constructed using information from the WAN DHCP server only.

```
ip route add 10.0.1.0/24 dev eth0 src 10.0.1.55 table docsis

ip route add default via 10.0.1.1 dev eth0 src 10.0.1.55 table docsis
```

The HN table is constructed using information from the LAN DHCP server only.

```
ip route add 192.168.33.0/24 dev eth1 src 192.168.33.100 table hn

ip route add default via 192.168.33.1 dev eth1 src 192.168.33.100 table hn

ip route add 169.254.0.0/16 dev eth1 src 192.168.33.100 table hn
```

The Main table is constructed by combining the information from the WAN and LAN DHCP servers. Note that the WAN information is assigned a lower metric and therefore has a higher priority. Therefore, the WAN-assigned default gateway will take precedence in most situations.

```
ip route add 10.0.1.0/24 dev eth0 src 10.0.1.55 metric 10 table main

ip route add default dev eth0 via 10.0.1.1 src 10.0.1.55 metric 10 table main

ip route add 192.168.33.0/24 dev eth1 src 192.168.33.100 metric 20 table main

ip route add default dev eth1 via 192.168.33.1 src 192.168.33.100 metric 20 table main
```

Construct the Rule Table

The Rule table is used by the Linux operating system to select the appropriate routing table for each packet.

```
# This rule applies to sockets that bind to WAN IP address

ip rule add priority 10 from 10.0.1.0/24 table docsis

# This rule applies to sockets that bind to LAN IP address

ip rule add priority 20 from 192.168.33.0/24 table hn

# Unbound sockets and non-IP packets (e.g. ARP) use the Main table

ip rule add priority 30 table main
```

5.9.4.2 Example 2: Auto-IP on LAN

Note that a default gateway is only necessary on the LAN side if the HNHost needs to communicate with devices that have a global IPv4 address rather than an Auto-IP address. These devices might have been assigned an address before the LAN DHCP server went offline.

Auto-IP will be used on the LAN when a DHCP server is not available. Policy Routing can still be used to fulfill the requirements of this specification.

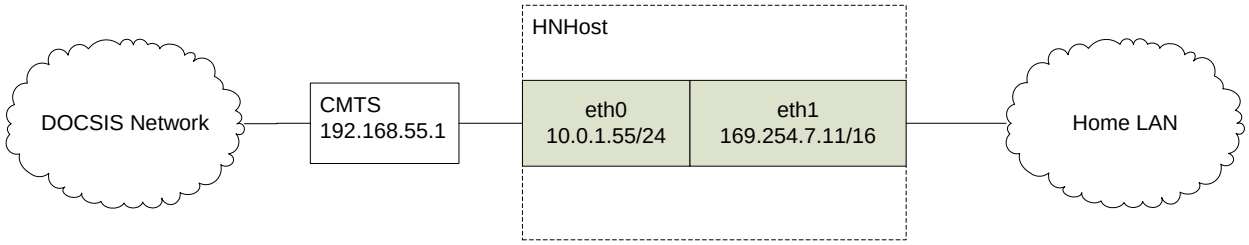

Figure 2 - Auto-IP on LAN Reference Network

The HNHost will be provisioned by the WAN DHCP server and Auto-IPs for the LAN-side as follows:

	WAN DHCP Provisioning	**LAN Auto-IP Provisioning**
IPv4 Address	10.0.1.55	169.254.7.11
IPv4 Subnet Mask	255.255.255.0	255.255.0.0
IPv4 Default Gateway	10.0.1.1	n/a

Construct the Routing Tables

Linux routing tables are identified using numbers from 0 to 255. Tables `local` and `main` have the numbers 255 and 254 associated with them. The /etc/iproute2/rt tables file can be customized to assign names to each table.

```
#
# Reserved by Linux
#
255    local
254    main
253    default
0      unspec
#
# Added for Policy Routing example
#
1      hn
2      docsis
```

The DOCSIS table is constructed using information from the WAN DHCP server only.

```
ip route add 10.0.1.0/24 dev eth0 src 10.0.1.55 table docsis
ip route add default via 10.0.1.1 dev eth0 src 10.0.1.55 table docsis
```

The HN table is constructed as follows:

```
ip route add 169.254.0.0/16 dev eth1 src 169.254.7.11 table hn
ip route add default via 169.254.7.11 dev eth1 src 169.254.7.11 table hn
```

The Main table is constructed by combining the information from the WAN DHCP server and the Auto-IP address. Note that the WAN information is assigned a lower metric and therefore has a higher priority. Therefore, the WAN-assigned default gateway will take precedence in most situations.

```
ip route add 10.0.1.0/24 dev eth0 src 10.0.1.55 metric 10 table main
ip route add default dev eth0 via 10.0.1.1 src 10.0.1.55 metric 10 table main
ip route add 169.254.0.0/16 dev eth1 src 169.254.7.11 metric 20 table main
ip route add default dev eth1 via 169.254.7.11 src 169.254.7.11 metric 20 table main
```

Construct the Rule Table

The Rule table is used by the Linux operating system to select the appropriate routing table for each packet.

```
# This rule applies to sockets that bind to WAN IP address
ip rule add priority 10 from 10.0.1.0/24 table docsis
# This rule applies to sockets that bind to HN IP address
ip rule add priority 20 from 169.254.0.0/16 table hn
# Unbound sockets and non-IP packets (e.g. ARP) use the Main table
ip rule add priority 30 table main
```

Appendix I Revision History

The following ECN was incorporated into OC-SP-HOST-HN2.0-I02-090508:

ECN	Accepted Date	Title
HOST-HN2.0-N-09.1383-1	4/17/09	Inclusion of MoCA, MoCA MIBs, and mandatory RSD support

The following ECN was incorporated into OC-SP-HOST-HN2.0-I03-091211:

ECN	Accepted Date	Title
HOST-HN2.0-N-09.1430-3	11/6/09	SNMP requirements update

The following ECN was incorporated into OC-SP-HOST-HN2.0-I04-100507:

ECN	Accepted Date	Title
HOST-HN2.0-N-10.1541-1	4/30/10	Network Interface requirement updates

The following ECN was incorporated into OC-SP-HOST-HN2.0-I05-110512:

ECN	Accepted Date	Title
HOST-HN2.0-N-11.1661.2	5/9/11	Host HN: Reference edits for OpenCable bundle inclusions

The following ECNs were incorporated into OC-SP-HOST-HN2.0-I06-120112:

ECN	Accepted Date	Title
HOST-HN2.0-N-10.1619-2	5/9/11	Multiple HN Interfaces
HOST-HN2.0-N-11.1683-1	8/26/11	Add HN ipAddressTable Support

The following ECN was incorporated into OC-SP-HOST-HN2.0-I07-130418:

ECN	Author	Accepted Date	Title
HOST-HN2.0-N-12.1800-1	Overcash	9/21/12	HN Host IP Stack Requirements