INTERNATIONAL STANDARD

ISO/IEC 16317

First edition
2011-10-01

Information technology — Telecommunications and information exchange between systems — proxZzzy for sleeping hosts

Technologies de l'information — Téléinformatique — proxZzzy pour hôtes dormants

Reference number
ISO/IEC 16317:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 16317 was prepared by Ecma International (as ECMA-393) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

Large amounts of electricity are used by electronic devices that are on solely for the purpose of maintaining network connectivity while they might otherwise be asleep. The computation required to stay connected is small, but these devices have large power differences between their on and sleep modes; thus, most of this energy use is wasted. Billions of dollars per year of electricity (and consequent carbon emissions) could be saved by widespread use of a “network proxy” for devices like PCs, printers, game consoles and set-top boxes. A low-power proxy handles key network tasks for a high-power device, thus allowing the high-power device to sleep when not in active use.

In 2008, the Energy Star program identified preying in its Computer Specification, version 5.0, as a technology with substantial energy saving potential. The standard designates that a “platform-independent industry standard” will specify the behaviour of a qualifying proxy. It is expected that ISO/IEC 16317 will be that standard.

This International Standard provides an overall architecture for a proxy and key requirements for preying select protocols. Handling of incoming traffic can require generating a reply packet, causing a system wakeup, or ignoring it. Proxies also do some routine packet generation on their own, and data are exchanged between a host and a proxy when the host goes to sleep and when it wakes up.

Existing technologies require other entities on the network to know that the host is asleep and alter their behaviour appropriately. A key goal of a proxy is to save energy, while simultaneously keeping the device accessible to the rest of the network. The operations of the proxy are best-effort, both in attempting to extend sleep time, as well as maintaining network access.

There are many possible ways to implement proxy functionality, and this International Standard seeks to avoid unduly restricting choices in those designs. In particular, it does not specify the location of the proxy, within the host itself or in attached network devices.

Information technology — Telecommunications and information exchange between systems — proxZzzy for sleeping hosts

1 Scope

This International Standard specifies maintenance of network connectivity and presence by proxies to extend the sleep duration of hosts.

This International Standard specifies:

- capabilities that a proxy may expose to a host;
- information that must be exchanged between a host and a proxy;
- proxy behaviour for 802.3 (Ethernet) and 802.11 (WiFi);
- required and optional behaviour of a proxy while it is operating, including responding to packets, generating packets, ignoring packets, and waking the host.

This International Standard does not:

- specify communication mechanisms between hosts and proxies;
- extend or modify the referenced specifications (and for any discrepancies those specifications are authoritative);
- support security and communication protocols such as IPsec, MACSec, SSL, TLS, Mobile IP, etc.

2 Conformance

An “M”, “S” or “O” in the “M/S/O” column in the tables in Clause 6, 7 and 8 qualify the requirements as “M” for Mandatory, “S” for Should and “O” for Option respectively.

Conformant proxies implement at least the mandatory requirements in the “Basic Framework Protocol” in Clause 6 and zero or more Options in Clause 8. Proxies adhere to configuration and management behaviours as specified in Clause 7.

The table below summarises the Requirements and status.

Requirements Implemented	Required/Option
Media (802.3, 802.11)	Requires implementation of 6.1 or 6.2 or both
IPv4 ARP	Mandatory
IPv6 Neighbor Discovery	Mandatory
DNS	Option
DHCP	Option
IGMP	Option
MLD	Option
Remote Access using SIP and IPv4	Option
Remote Access using Teredo for IPv6	Option
SNMP	Option
Service Discovery using mDNS	Option
Name Resolution with LLMNR	Option
Wake Packets	Mandatory

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8802-3:2000, *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 specifications*

ISO/IEC 8802-11:2005, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*

ISO/IEC TR 11802-2:2005, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Technical reports and guidelines — Part 2: Standard Group MAC Addresses*

RFC 826, *An Ethernet Address Resolution Protocol;* David C. Plummer (MIT); November 1982; http://tools.ietf.org/html/rfc826

RFC 1122, *Requirements for Internet Hosts — Communication Layers;* R. Braden; October 1989; http://tools.ietf.org/html/rfc1122

RFC 3261, *SIP: Session Initiation Protocol;* Many Authors; June 2002; http://tools.ietf.org/html/rfc3261

RFC 4380, *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs);* http://tools.ietf.org/html/rfc4380

RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,* http://tools.ietf.org/html/rfc4443

RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification;* http://tools.ietf.org/html/rfc2460

RFC 4861, *Neighbor Discovery for IP Version 6 (IPv6);* http://tools.ietf.org/html/rfc4861

IEEE Std 802.11r-2008, *IEEE Standard for information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 2: Fast Basic Service Set (BSS) Transition"*

http://tools.ietf.org/html/draft-cheshire-dnsext-multicastdns-08 (Multicast DNS)

http://tools.ietf.org/html/draft-cheshire-dnsext-dns-sd-05 (DNS-Based Service Discovery)

[MS-LLMNRP] "Link Local Multicast Name Resolution (LLMNR) Profile", Microsoft Developer Network Open Specifications Developer Center Library, http://msdn.microsoft.com/en-us/library/dd240328%28PROT.10%29.aspx

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1
host
entity that uses a lower-power proxy for maintaining network presence

4.2
proxy
network proxy
entity that maintains network presence for a sleeping higher-power host

4.3
sleep (noun)
mode in which the host uses less energy than it does when fully operational

5 Proxy Usage of Protocols (informative)

5.1 Basic Architecture

For a proxy to function correctly and enable a host to sleep, certain basic functions must be present in the proxy, its host, and in the communications between the proxy and host. This International Standard offers a profile of commonly deployed protocols which can be implemented in a proxy to produce the desired system behaviour.

5.2 Ethernet (IEEE 802.3)

IEEE standard 802.3 specifies Physical and Media Access Control layers of an interoperable protocol, commonly known as Ethernet.

IEEE 802.3 environments have protocols which may affect proxy operation such as updates of network management parameters in response to LLDP exchanges, including possibly waking the host. IEEE 802.3 interfaces are capable of supporting multiple MAC addresses simultaneously. This functionality has been applied to supporting virtual machines – each with one or more unique MAC addresses (each MAC address with one or more IPv4/v6 addresses) on a single physical interface.

Wired deployments differ in nature – Home, Enterprise, and 'Guest' network connections – and, even within each, deployment configuration and network interaction can be significantly different. If link status changes, a

considerable period of time may pass before the proxy will be able to send or receive traffic over the switch port while the Spanning Tree Protocol is executed.

5.3 Wireless LAN (IEEE 802.11)

IEEE standard 802.11 specifies Physical Layer and Media Access Control layers of an interoperable wireless protocol, commonly known as WiFi.

Wireless communication using 802.11 differs from that of wired (IEEE 802.3) LAN operations in the following ways:

- 802.11 wireless communications transpire over unlicensed-band which makes it susceptible to multiple levels of interference and coverage issues. Hence, WiFi connectivity cannot be assured.
- The 802.11 host and the Access Point (AP) are configured to use a common “Profile” —a set of connection parameters such as band, channel, security, etc. The profile is configured out of band and prior to the host going to sleep.

Herein are some wireless-specific deployment considerations for proxy:

- Hosts often disconnect from an AP, and may re-connect to the same AP or another AP within the same SSID, or to an AP in a different SSID. This is based on the Connection Profiles configuration.
- A proxy may be unable to operate in public WiFi hotspots that require explicit user authorization, such as requiring a legal agreement (EULA).
- Some WLAN deployments require a DHCP Renew at association time.

5.4 Dynamic Host Configuration Protocol (DHCP)

DHCP is the primary IP address allocation mechanism for IPv4 and stateless IP address allocation mechanism for IPv6 networks. A DHCP Server allocates IP addresses for systems on the network. The lease time of the IP address may expire while the system is asleep.

The following methods ensure that the proxy can continue using the same IP address that has been allocated to the host by the DHCP Server.

- Host sets an internal timer and wakes itself in time to renew the DHCP lease. There are no requirements for the proxy.
- The proxy wakes the host on a proxy-based timer to renew the DHCP lease.
- The proxy implements DHCP address renewal functionality, without waking the host.

The proxy does not change the IP address of the system while the host is asleep. Doing so would introduce undue implementation complexity, particularly to transfer the new IP address back to the host.

5.5 Internet Protocol v4 Basic Framework (IPv4)

IPv4 protocol suite, defined by IETF, is a set of cooperating protocols that provide network layer interoperability for Internet protocol networks.

5.5.1 ARP – Address Resolution Protocol

ARP (RFCs 826, RFC 1122) provides address mapping of an IPv4 address to a corresponding MAC address.

ARP is important to the proxy because in order for other entities to be able to send an IPv4 packet to a proxy, they must be able to translate the IP address to the corresponding MAC address. The proxy responds to ARP requests for its MAC address(s) to maintain IPv4 connectivity on the IPv4 network.

ARP is an unreliable network protocol and other endpoints on the network do not assume that every ARP request arrives at the destination. Therefore, the short delay (2-10 seconds) on transitions to and from proxy operation should not affect the behaviour of the other endpoints on the network.

5.5.2 Link Local Auto-IP Address Allocation

Link-Local Auto-IP Address allocation uses ARP to allocate an IPv4 address in the absence of a DHCP server (or other allocation methods). A proxy defends a Link-Local Auto-IP Address using algorithms listed in RFC 5227 (except where a new address is required; at that point the proxy must stop supporting the interface and optionally wake the host).

5.5.3 IPv4 Address Conflict Detection

Duplicate address detection (RFC 5227) is required to keep the proxy from using an address that is in use by another node on the network.

5.5.4 IGMP – Internet Group Management Protocol

IGMP (RFC 1112 IGMP version 1, RFC 2236 IGMP version 2, RFC 3376 IGMP version 3) allows network interfaces to participate in multicast groups (these are controlled by the router).

5.5.5 UDP – User Datagram Protocol

A proxy that supports UDP may wake the host on receiving specific UDP datagrams or may respond directly to the datagram.

5.5.6 TCP – Transmission Control Protocol

TCP (RFC 793) provides a stateful and reliable transport layer connection between network endpoints. The proxy may handle accepting connections, originating connections, and waking the host on a connection attempt (TCP SYN) or incoming data.

5.5.7 DNS – Domain Name System

The proxy may need to issue DNS Queries if it provides UDP or TCP connectivity and allows the host to specify Internet compatible host names for the remote endpoint and not direct IPv4 addresses. This International Standard addresses the DNS Client only.

5.6 Internet Protocol v6 Basic Framework (IPv6)

Network presence for IPv6 is maintained by the proxy when the host is asleep by implementing the Neighbor Solicitation function of Neighbor Discovery. The proxy uses IPv6 global addresses, link local addresses, and temporary addresses. Address auto-configuration is handled by the host. ND - Neighbor Discovery.

Neighbor Discovery is a set of five message types implemented on ICMPv6 (RFC 4861), of which the proxy uses four for resolving IPv6 addresses to the MAC address: Router Solicitation, Router Advertisement, Neighbor Solicitation and Neighbor Advertisement.

The proxy should support multiple address sets. Typically, there are three sets in an IPv6 network; the global address, the local address, and possibly a temporary address.

5.6.1 MLD – Multicast Listener Discovery

MLD (RFC 2710) allows endpoint nodes to report their membership in IPv6 multicast groups. MLD is updated for source-address selection by RFC 3590 and for source-specific multicast by RFC 3810.

A proxy maintains a table of IPv6 multicast addresses to which the host is subscribed, and the proxy maintains its membership in each multicast group by responding to MLD Query messages with MLD Report messages. The proxy need not send unsolicited MLD Report or MLD Done messages. Because the host is not a multicast router, the proxy does not send MLD Query messages or process MLD Report or MLD Done messages.

5.7 Remote Access using SIP and IPv4

In this International Standard, SIP (RFC 3261) is used by a remote entity to wake a host. SIP proxies along the path can facilitate the traversal of NATs and firewalls. The reason for waking the host (i.e., the particular host application that needs to be used) is outside the scope of this International Standard. SIP methods and responses used in the remote wake functionality are REGISTER, INVITE, ACK, and SIP Status Codes.

The following diagram shows a sample SIP implementation that may be used by the proxy to wake the host. Only the messages into and out of the Device Network Proxy are included in this specification. All other messages and entities are a possible implementation and not covered by this specification.

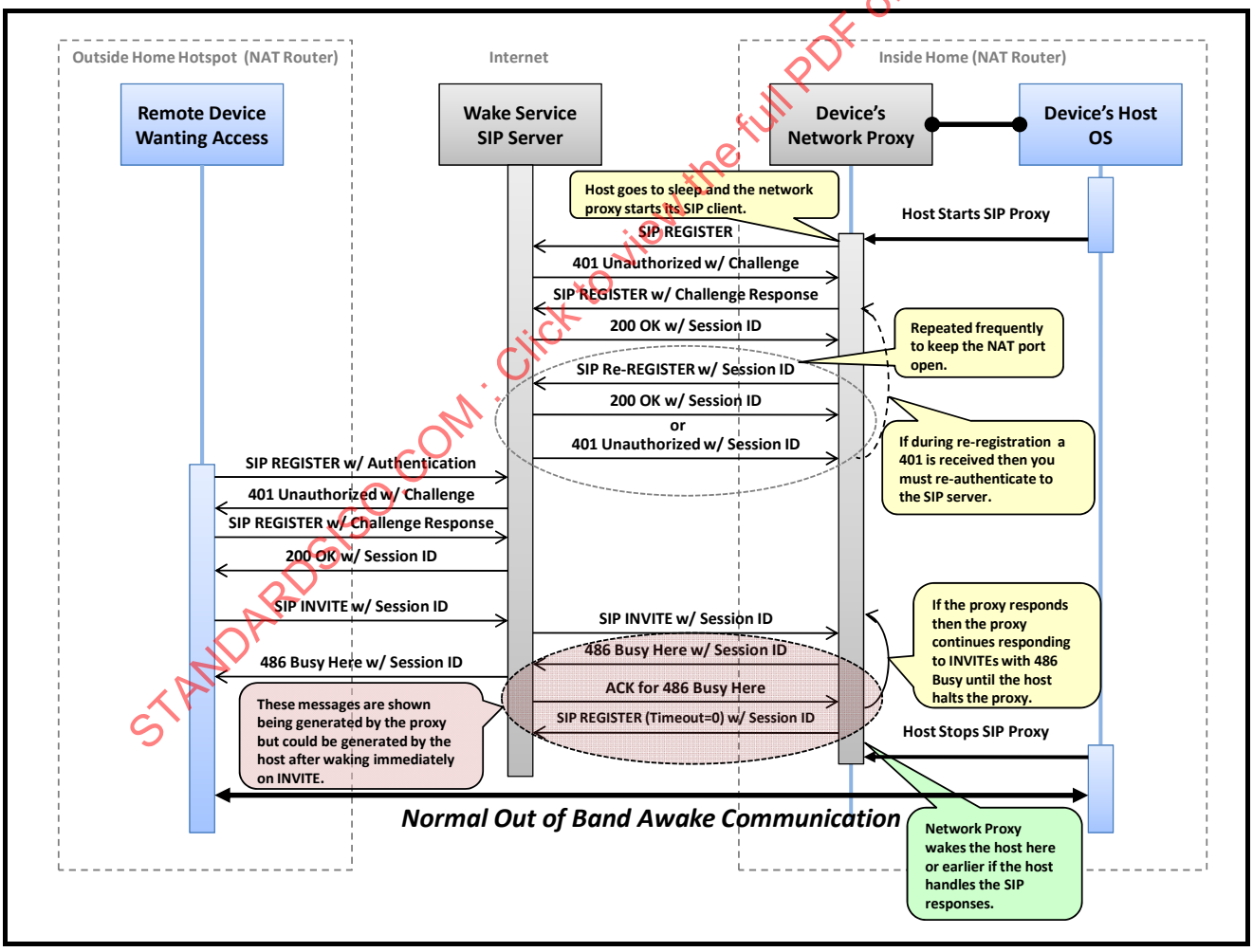

Figure 1 — SIP Remote Wake

The above example shows the host wake processing using SIP as "INVITE/486 Busy Here/..." however this is not a requirement. The requirements in this International Standard are written in a general way that includes allowing a "200 Ok" response and establishing a SIP session.

5.8 Remote Access using Teredo for IPv6

Teredo (RFC 4380) is an IPv6 transition technology that allows peer to peer connectivity between peers behind a NAT. The Teredo protocol encapsulates IPv6 packets inside UDP IPv4 packets. One of the tunnels a Teredo client maintains is with the Teredo server in the cloud. The proxy maintains this tunnel by sending Router Solicitation (RS) messages at regular intervals. The proxy ignores any responses from the server to the RS packet.

5.9 SNMP

The proxy stands in for an SNMP v1 and v2 (RFC 1156, 1157, 1141) agent, and avoids unnecessary wakes for some SNMP requests. The SNMP proxy responds to SNMP GET requests with values provided to it from the host. The host can specify the action to be taken on receiving a SNMP SET.

5.10 Service Discovery using mDNS

When clients browse for services on the network using DNS-Based Service Discovery (DNS-SD) over Multicast DNS (mDNS), the proxy handles advertising services to clients, and should only wake the host when a client initiates an application session with a service.

The proxy advertises services as an mDNS responder initialized with a static set of DNS-SD service registrations. The proxy must meet the requirements for multicast DNS responders. The proxy responds to multicast queries with multicast responses, and periodically sends unsolicited announcements. When clients initiate application sessions with advertised transport endpoints, e.g. TCP/UDP ports referenced in DNS SRV records, the proxy wakes the host.

5.11 Name Resolution with LLMNR

The proxy answers Link-Layer Multicast Name Resolution (LLMNR) queries on behalf of the host by listening for UDP LLMNR queries on the relevant port and multicast addresses, so that the host doesn't need to. The proxy wakes the host if it detects an LLMNR conflict in addition to connection requests. Behaviour is based on RFC 4795 with differences as noted in [MS-LLMNR].

5.12 Wake Packets

While the proxy's function is to increase the time a host remains in sleep by interceding on behalf of the host during periods in sleep, waking is equally important for proper operation of the host on the network. Any host using a proxy must have one or more mechanisms for waking on network traffic. While many mechanisms can be conceived, four possible mechanisms are as follows.

1. Magic Packet™ (a trademark of Advanced Micro Devices, Inc.)
2. Wake on TCP SYN
3. Wake on UDP datagram
4. Wake on TCP DATA.

For numbers 2-4, these could optionally be further narrowed as port filtered, address filtered, port/address filtered and not filtered. This list is not exhaustive.

6 Basic Framework Protocols

6.1 Ethernet 802.3 (Option)

6.1.1 Configuration Data

ID	Configuration Data	Observation
C1	MAC Address	MAC address of the interface(s) to be proxied.

6.1.2 Behavioural Requirements

The proxy expects that the host has established a network connection. This may be via static or dynamically assigned addresses to a given physical port. If security is enabled, the host has established port authentication (802.1X) and encryption parameters (802.1AE).

During host to proxy transitions, the host should avoid changing the network interface link status for such actions as reducing link speed to reduce power consumption. The host may be required to reduce link speed to meet platform power requirements in sleep states.

ID	Requirement	M/S/O	Rationale
R1	The proxy SHALL ignore frames containing unrecognized and unhandled L2 frame headers.	M	Sending QoS tagged packets to the proxy must not cause the proxy to fail for the given protocol. This does not mean special handling is required; the tags can be ignored (IEEE 802.1p).
R2	The proxy SHOULD detect if 802.3 Ethernet media is disconnected and cease functioning on the disconnected interface.	S	
R3	If the host has established an 802.3az LLDP session with the link peer, the proxy SHOULD support LLDP for 802.3az.	S	Proxy LLDP replies MAY include positive or negative acknowledgements of any attempted EEE parameter changes.
R4	On receipt of an 802.1X EAPOL “Request Identity” packet, the proxy MAY wake the host.	O	The main security credentials are in the host.

6.2 WiFi 802.11 (Option)

6.2.1 Configuration Data

ID	Configuration Data	Observation
C2	MAC Address	MAC address of the interface being proxied.
C3	Current Profile	The profile used by the host for its current association; it MAY contain Connection Parameters such as SSID, BSSID, band/channel.
C4	Pre-Master Key	The Pre-Master Key (802.11i PMK, 802.11r PMK-R1) SHOULD be transmitted securely to the proxy.

6.2.2 Behavioural Requirements

The proxy expects that the host has a current and valid 802.11 association with an AP. If security is enabled, host has established the security state with the Wireless infrastructure, and the host is able to send 802.11 data frames to the network.

ID	Requirement	M/S/O	Rationale
R5	The proxy SHALL act as a non-AP STA in Infrastructure BSS mode.	M	The proxy is applicable only to Infrastructure mode non-AP STAs, and does not support other modes like IBSS, DLS, PAN, etc. (EEE 802.11-EEE 802.11-2007).2007
R6	The proxy SHALL maintain or re-establish an 802.11 association with the AP belonging to the SSID, as per the profile.	M	Per IEEE 802.11-2007
R7	If wireless security is enabled in the profile, the proxy SHALL maintain or re-establish a secure association (802.11i 4-way, 802.11r FT) as part of the association procedures.	M	Per IEEE 802.11-2007
R8	In the absence of periodic 802.11 traffic, the proxy SHALL maintain the current (secure) connection with the AP by sending keep-alive messages.	M	A keep-alive is desirable because some APs clean up their state for inactive clients as part of maintenance procedures. 802.11 keep-alive mechanisms include NULL data frames, 11w, vendor specific methods, ARP, and SIP. Suggested frequency is 3 seconds between keep-alives.
R9	The proxy SHALL detect disconnection of the wireless communication link to the AP infrastructure.	M	Disconnection MAY be detected by a vendor specific algorithm (e.g. using missed beacons from AP, lower RSSI Threshold level, etc.), NULL data frames, or a method defined in 802.11w.
R10	If the proxy is disconnected, the proxy SHALL attempt Re-Association or wake the host.	M	Per IEEE 802.11-2007
R11	In response to the AP Group Key update, the proxy SHALL perform the Group Transient Key (GTK) update procedure.	M	Per IEEE 802.11-2007
R12	If supported by the AP, the proxy MAY utilize 802.11 power saving mechanisms (e.g. PS Poll, U-APSD, etc.).	O	
R13	The proxy MAY implement 802.11r (secure fast roaming).	O	802.11r allows secure re-associations without full EAP 802.1X Authentication and reduces roaming latency (IEEE 802.11r-2008)

ID	Requirement	M/S/O	Rationale
R14	In response to the AP triggered re-authentication i.e. EAP identity, the proxy SHALL wake the host	M	Per IEEE 802.11-2007
R15	The proxy SHALL either execute re-association procedures, or wake the host.	M	If the host is woken, it is expected to execute the 802.11 association and security procedures. Per IEEE 802.11-2007
R16	If the proxy is unable to connect to the AP, it SHALL wake the host.	O	
R17	The proxy MAY wake the host on a key lifetime expiration (PMK, PMK-R0, PTK)	O	

The wireless connection may be terminated during the wake transition. The proxy may deliver the existing wireless connection parameters to the host, to reduce the wake transition time.

6.3 ARP

6.3.1 Configuration Data

ID	Configuration Data	Observation
C5	IP Address	IP addresses of interfaces to be proxied

6.3.2 Behavioural Requirements

ID	Requirement	M/S/O	Rationale
R18	The proxy SHALL properly respond to ARP requests received on the MAC layer broadcast address.	M	ARP operations require that the proxy be capable of receiving ARP requests (RFC 826, 1122).
R19	The proxy SHALL properly respond to ARP requests received on proxied MAC unicast addresses.	M	ARP operations require that the proxy be capable of receiving ARP requests (RFC 826 and RFC 1122).
R20	The proxy SHALL reply to ARP Requests where the target protocol address is a proxied IP address with ARP Responses.	M	RFC 5227
R21	The proxy SHALL reply to ARP Requests containing source protocol address as zero, with an ARP Response.	M	This is to support ARP probes for Address Conflict Detection. RFC 5227
R22	ARP Responses generated by the proxy SHALL have the same MAC and IPv4 address provided in the configuration data	M	Source Physical and Logical addresses are fields in the ARP Response packet, and the proxy must insert the same values as what the host would have added.

ID	Requirement	M/S/O	Rationale
R23	If the proxy supports the QoS Option, the proxy SHALL tag outgoing IPv4 packets with the default QoS value of 0, or any QoS value configured by the host.	O	There MAY be cases where an application wants to increase or decrease the packet priority for that protocol (IEEE 802.1p and IEEE 802.1D).
R24	The proxy MAY wake the host on duplicate address detection.	O	

6.4 Neighbour Discovery

6.4.1 Configuration Data

ID	Configuration Data	Observation
C6	MAC Address	MAC address of the interface being proxied
C7	IPv6 Solicitation Addresses	Solicitation addresses for link-local and global IPv6 addresses of the interface being proxied
C8	IPv6 Temporary Addresses	IPv6 Temporary Addresses of the interfaces being proxied
C9	IPv6 Target Addresses	IPv6 target addresses
C10	Target MAC Address	

6.4.2 Behavioural Requirements

The proxy expects that the link-local and global addresses have the same solicitation address and that the temporary addresses have the same solicitation address.

ID	Requirement	M//S/O	Rationale
R25	The proxy SHALL respond to an ND Neighbor Solicitation by responding with an ND Neighbor Advertisement	M	See RFC 4861.
R26	The proxy SHALL respond to Global Address Neighbor Solicitation requests	M	
R27	The proxy SHALL respond to Link-local Neighbor Solicitation requests	M	
R28	The proxy SHALL respond to Temporary Address Solicitation requests	M	
R29	The proxy SHALL respond to ND Neighbor Solicitation messages that include recognized extended headers	M	IPv6 headers for Neighbor Solicitation messages can include extension headers (RFC 2460).

6.5 Wake Packets

6.5.1 Configuration Data

There is no configuration data.

6.5.2 Behavioural Requirements

ID	Requirement	M/S/O	Rationale
R30	The proxy SHALL wake the host on an incoming TCP connection attempt (TCP SYN).	M	The proxy must support a standardized method to wake the host from remote accesses. The proxy MAY implement additional filtering criteria – such as on protocol ports and addresses - to prevent spurious wake events.
R31	The proxy SHALL wake the host on an incoming Magic Packet.	M	

7 Proxy Configuration and Management

The host directs the proxy to become operational. The proxy may take time to initialize, and the host may take time to wake. Thus, there may be times when neither the host nor the proxy is operational. The operational control change between host and proxy should be done in timely manner to avoid functional loss.

Multiple interfaces may be connected to the same network. A proxy may support more than one interface.

7.1 Configuration Data

ID	Configuration Data	Observation
C11	Proxy capabilities	The set of capabilities that a proxy exposes
C12	Proxy configuration	Host enables specific capabilities and provides data for those capabilities

7.2 Behavioural Requirements

The proxy exposes its capabilities to the host. The host configures, initiates, and terminates proxy operation.

ID	Requirement	M/S/O	Rationale
R32	The proxy SHALL follow host directives to initiate and terminate operation.	M	Any capability of a proxy MAY be left disabled; the proxy is not expected to enable those capabilities. The host MAY wake itself so MAY terminate proxy operation before the proxy itself encounters any wake condition.
R33	Following cessation of a capability, the proxy MAY continue operation of other enabled capabilities.	O	

ID	Requirement	M/S/O	Rationale
R34	The proxy SHOULD NOT wake the host when media connection are lost	S	Otherwise when a switch reboots, all hosts would wake. There are valid reasons to wake the host.
R35	The proxy SHALL be capable of waking the host.	M	
R36	The proxy SHALL ignore ill-formed packets.	M	IPv4 packet processing must conform to RFC 791.
R37	The proxy SHALL ignore fragmented IPv4 packets.	M	Fragmented packets enable potential security exploits.
R38	The proxy SHALL ignore IPv4 packets with Sender-specified source routed packets.	M	Prevents the packet from circumventing firewalls using Source Address Routing.

7.2.1 Returned Data (Option)

ID	Configuration Data	Observation
C13	Status indication including any error information (optional)	
C14	Packet that triggered a host wake-up (optional)	

8 Options

8.1 IGMP Multicast (Option)

8.1.1 Configuration Data

ID	Configuration Data	Observation
C15	Subscribed Multicast Addresses	Multicast IP addresses to be proxied.

8.1.2 Behavioural Requirements

ID	Requirement	M/S/O	Rationale
R39	On host to proxy transitions the proxy SHALL register all configured multicast addresses.	M	This mitigates the possibility of a missed report query during the transition to proxy operation.
R40	The proxy SHALL implement version 2 of IGMP.	M	Version 3 extends version 2 to include/exclude other hosts, and this is not necessary for the proxy (RFC 2236).

8.2 DHCP Address Allocation (Option)

8.2.1 Configuration Data

ID	Configuration Data	Observation
C16	Host IP address	
C17	Subnet Mask for the Unicast IP Address	
C18	IP Address of the Gateway	
C19	DHCP Lease Time Left	
C20	DHCP Server IP Address	This MAY be the same as the gateway address above.

8.2.2 Behavioural Requirements

ID	Requirement	M/S/O	Rationale
R41	The proxy MAY wake the host prior to address lease expiration.	O	On wake, the host is expected to renew the lease.
R42	The proxy MAY perform DHCP RENEW.	O	The proxy MAY perform address operations, such as lease renewal. This is defined as implementing DHCP within the proxy.
R43	If DHCP RENEW is implemented in the proxy, the proxy MAY wake the host if the address lease is lost or critical (defined in the application specific technical requirements) DHCP parameters have changed.	O	If the IP address state is lost or changes to something other than what the host had before proxying began then the proxy is no longer proxying for the host.

8.3 Remote Access using SIP and IPv4 (Option)

Configuration DataID	Configuration Data	Observation
C21	SIP Server (IP Address or its Domain Name)	
C22	SIP Authentication Method and SIP Credentials	
C23	DNS Server IP Address	

8.3.1 Behavioural Requirements

ID	Requirement	M/S/O	Rationale
	IP Basic Framework Requirements		
R44	SIP SHALL be implemented over UDP.	M	As required in SIP RFCs.
R45	SIP MAY be implemented over TCP.	O	Deviates from RFC 3261 which requires TCP.
R46	If the proxy accepts a server by name, it SHALL implement name resolution.	O	The DNS server MAY implement load balancing and a single IP address SHOULD not be used.
	SIP – Session Initiation Protocol for Remote Wake		
R47	The proxy SHALL maintain its SIP registration to the SIP server as per RFC 3261.	M	Required for the wake usage to work.
R48	The proxy SHALL ensure that an INVITE message can be received from the SIP server even through multiple layers of NAT.	M	The server has to be able to send the wake message to the proxy. The SIP outbound section of the SIP RFC describes methods for keeping NAT open. One common method is to send the SIP re-REGISTER message every 29 seconds.
R49	When a SIP authentication challenge is issued by the server upon receiving a re-REGISTER message from the proxy, the proxy SHALL re-authenticate with the SIP server.	M	Failing to re-authenticate will make your proxy “not available” or “logged out” to the server.
R50	When a valid SIP INVITE message is received by the proxy and the SIP transport is TCP, the proxy SHALL complete the state processing per RFC 3261 sending a SIP response message and receiving an ACK SIP message.	M	If the proxy can wake early during state processing and continue functioning then the wake can occur at any time. If the proxy cannot continue functioning after the wake signal the proxy will need to wait to finish processing before it can send the wake signal.
R51	When a valid SIP INVITE message is received by the proxy and the SIP transport is UDP, the proxy SHALL send the required SIP RESPONSE message as per RFC 3261.and wake the host.	M	The host is expected to terminate the SIP registration once awake.

8.4 Remote Access using Teredo for IPv6

The proxy expects that the host has previously established a Teredo connection to the Teredo Server in the cloud. The proxy is only responsible for sending a periodic keep-alive. There may be one or more instances of this capability.

8.4.1 Data Configuration

ID	Configuration Data	Rationale
C24	Min and Max time interval	Min and Max can be set to the same value. The periodic time interval (in seconds) defines the maximum time between packets being sent out.
C25	Complete packet	Router Solicitation packets are constructed by the host per RFC 4380. The proxy relies on the host to provide it a well-formed, integrity checked packet.

8.4.2 Behavioural Requirements

ID	Requirement	M/S/O	Rationale
R52	The proxy SHALL send the packet periodically within the range of Min and Max intervals.	M	A Router Solicitation (RS) message is sent to a Teredo server. RS messages refresh NAT mappings (RFC 4380, Section 5.2). The proxy ignores all responses to RS.
R53	The proxy SHALL wake the host on receiving an indirect bubble packet	M	See RFC 4380 for indirect bubble packet.

8.5 Simple Network Management Protocol (SNMP)

This option defines proxy operation for SNMPv1 and SNMP v2.

8.5.1 Configuration Data

ID	Configuration Data	Observation
C26	UDP ports used, SNMP community names (with access properties), getall_flag (on OID set, on GET/SET with unknown OID)	
C27	List of OID-Value pairs	Fully qualified OID-Value pairs and per OID access properties to be cached.

8.5.2 Behavioural Requirements

ID	Requirement	M/S/O	Rationale
R54	The proxy SHALL support SNMP v1 and v2	M	See RFC 1156, RFC 1157, and RFC 1441.
R55	The proxy SHALL reply with the value specified in the table of OID-Value pairs to an SNMP GET REQUEST to a cached OID.	M	The returned value is supplied from the table of OID-Values.
R56	The proxy SHALL support the SNMP GET NEXT Request.	M	Needed for SNMP walks. The table of OID-value pairs has other sequences than the original MIB, and thus other NEXT's.
R57	If the getall_flag is not enabled, the proxy SHALL respond to an SNMP GET REQUEST for an uncached OID as prescribed in RFC 1157 (return noSuchName).	M	The proxy cannot differentiate between an OID that the host does not support or that is missing from the MIB.
R58	If the getall_flag is enabled, the proxy SHALL wake the host on an SNMP GET REQUEST to an uncached OID.	M	
R59	If any writable community is defined by the host, the proxy SHALL wake the host on any SNMP SET REQUEST	M	Arbitrary SETs to cached or uncached OIDs SHOULD NOT wake the host if the community was not writeable.

8.6 Service Discovery using mDNS

8.6.1 Configuration Data

ID	Configuration Data	Observation
C28	Interface Addresses	Interface addresses of the host as advertised as A and AAAA records.
C29	Host Name Domain	The name of the host in the ".local." as advertised in the PTR records (Reverse DNS).
C30	Service Records	As advertised in SRV records.
C31	Shared Resource Record sets	If the proxy is capable of participating in the shared resource record sets, then the host provides this data to the proxy.
C32	Service names	As advertised in PTR records referring SRV records.
C33	Ancillary data	As advertised in TXT records associated with SRV records in the same resource record set.
C34	Multicast Addresses	If the proxy maintains membership in mDNS multicast groups with wider than link local.

8.6.2 Behavioural Requirements

The proxy expects that one or more valid IP addresses (IPv4 and/or IPv6) are being defended, as per the basic framework with at least one corresponding fully-qualified domain name in the <local.> top-level domain. The host completes all mDNS probing and announcing operations before commencing sleep (see section 9 of mDNS draft).

ID	Requirement	M/S/O	Rationale
R60	The proxy SHALL maintain membership in the link-local mDNS group associated with its Internet protocol basic frameworks – 224.0.0.251 for IPv4 and ff02::fb for IPv6.	M	This entails sending IGMP and MLD packets and the proxy needs to receive and process link-local mDNS messages.
R61	The proxy MAY additionally maintain membership in mDNS groups with wider scope than link-local.	O	In future, mDNS MAY not be limited to link-local scope.
R62	The proxy SHALL process all mDNS messages received on UDP port 5353 with a link-local IP multicast destination for the mDNS groups in which the host is a member.	M	
R63	The proxy SHALL process, per mDNS ID, mDNS queries received on UDP port 5353 at all of the interface IP addresses.	M	
R64	The proxy SHALL check the source address of received mDNS messages and ignore messages transmitted from addresses outside the scope of the mDNS multicast group.	M	Failure to meet this requirement MAY have negative security consequences.
R65	When transmitting over IPv4, the proxy SHALL send mDNS responses with the TTL in the IP header set to 255.	M	This is a requirement for mDNS responders using IPv4 to coexist with older mDNS clients.
R66	The proxy SHOULD honour the "unicast response" bit in the multicast DNS class field and send answers by unicast accordingly	S	I.e. if the responder has multicast that record recently (within ¼ of the TTL for the record). The recommendation applies equally to the proxy as well as the host.
R67	The proxy SHALL suppress known answer responses. It SHALL not send responses to questions that already include the answer with a TTL of at least half the correct value.	M	Section 7.1 of mDNS draft 07.
R68	The proxy SHALL suppress multi-packet known answer responses. It SHALL wait a random interval between 400 and 500 ms after receiving a query with the "truncated" (TC) bit set before sending its response, and it SHALL not send answers in that response which appear in subsequent queries received while it waits.	M	Section 7.2 and 7.4 of mDNS draft 07.
R69	Except when suppressing known answers, the proxy SHALL respond when it possesses authoritative negative, or non-null positive answers to a query.	M	Section 8 of mDNS draft.

ID	Requirement	M/S/O	Rationale
R70	The proxy SHALL respond immediately to queries for A and AAAA records for one of the fully-qualified domain names of the host.	M	Section 8 of mDNS draft.
R71	The proxy SHALL respond immediately with a positive answer to queries for PTR records in the 254.169.in-addr.arpa domain corresponding to any IPv4 link-local interface address.	M	Sections 5 and 8 of mDNS draft.
R72	The proxy SHOULD respond to queries for A and AAAA records by placing all the other interface addresses configured by the host into the Additional Answers section.	S	Section 8.2 of mDNS draft.
R73	The proxy SHALL NOT respond with a null response.	M	
R74	The proxy SHALL wait a random interval of time, no more than 500 ms, before responding to queries for PTR records with fully qualified domain names ending with ".local.".	M	Regarding wait: Section 8 of mDNS draft, in the passage discussing collision avoidance. Elevated from SHOULD in IETF draft because the expectation is that on a large network, a substantial fraction of the population SHOULD be sleeping at any given time.
R75	The proxy SHALL immediately respond to queries for SRV and TXT records with fully qualified domain names ending with ".local." and for which it is the unique responder.	M	Section 8 of mDNS draft.
R76	If the proxy participates in shared resource records, it SHALL wait a random interval of time, no more than 500 ms, before responding to queries for SRV and TXT records with fully qualified domain names ending with ".local.".	M	Section 8 of mDNS draft.
R77	The proxy SHALL process mDNS query messages composed of more than one question.	M	Section 8.3 of mDNS draft.
R78	The proxy SHOULD aggregate responses whenever possible.	S	Section 8.4 of mDNS draft.
R79	The proxy SHALL properly respond to legacy (see 8.5 of mDNS) multicast DNS queries with directed unicast responses in the format of conventional unicast DNS.	M	Section 8.5 of mDNS draft.
R80	The proxy SHALL wake the host when conflict resolution is required.	M	Conflict resolution detection is described in section 10 of mDNS draft.
R81	If the proxy has advance knowledge that the host's energy consumption requirements cannot be met when an event arises that requires its awakening, it MAY send a goodbye packet to indicate that the service is no longer available.	O	Section 11.2 of mDNS draft.

8.7 Name Resolution with LLMNR

8.7.1 Configuration Data

ID	Configuration Data	Requirement
C35	Interface Addresses	The interface addresses of the host as advertised as A and AAAA records.
C36	Host Name	The name of the host as advertised in the PTR records (Reverse DNS)

8.7.2 Behavioural Requirements

These requirements assume that one or more valid IP address (IPv4 and/or IPv6) is being defended, as per the basic framework with at least one corresponding single-label name.

ID	Requirement	M/S/O	Rationale
R82	The proxy SHALL support reception and sending of queries over UDP.	M	[MS-LLMNRP] Section 2.1.
R83	The proxy SHALL accept and send responses as large as the maximum UDP payload that can be carried over IPv4 or IPv6.	M	This is a requirement of the LLMNR profile, described in [MS-LLMNRP] sections 3.1.5 and 3.2.5.
R84	The proxy SHALL maintain membership in the link-local LLMNR groups associated with its Internet protocol basic frameworks, i.e. 224.0.0.252 for IPv4 and ff02::1:3 for IPv6.	M	This entails sending IGMP and MLD packets and it is required of the proxy to permit reception and processing of link-local LLMNR messages.
R85	The proxy SHALL process valid LLMNR queries received on UDP port 5355 with a link-local IP multicast address as the destination.	M	This is a basic requirement of any LLMNR responder.
R86	The proxy SHALL ignore received UDP LLMNR queries sent to a unicast address.	M	This is a basic requirement of any LLMNR responder. Failure to meet this requirement MAY have negative security consequences.
R87	The proxy SHALL respond to queries for A, AAAA, PTR and ANY.	M	This is a basic requirement for LLMNR implementations conformant with the LLMNR profile described in [MS-LLMNRP] Section 3.2.5.
R88	When transmitting over IPv4, the proxy SHALL send all LLMNR responses with the TTL in the IP header set to 255.	M	This is a requirement for LLMNR responders using IPv4 to coexist with older LLMNR clients.
R89	The proxy SHALL wake the host whenever conflict resolution is required.	M	Conflict resolution detection is described in section 4 of RFC 4795.
R90	The proxy SHALL respond to LLMNR queries utilizing UTF-8 encoding (U-Labels).	M	Internationalization support is described in [LLMNRP] Section 3.2.5.

Annex A
(informative)

System Considerations

A.1 AC and DC Power Mode

Network proxies and power management policies would benefit if the proxy could detect and take action on the operating status of the host (e.g. laptop lid) or current power source. Specifically, below are some system enhancements that would prolong battery life and give users a better mobile experience. We recommend that OEM help solve these hardware issues. The following may be configured by the user to execute the following scenarios:

- A sleeping proxy could turn off/On WoL/proxy if the power source changed from AC to battery while it was asleep. For example, when a user undocks a sleeping laptop to take it with them.

- A sleeping proxy could disable WoL/proxy if it could detect that the user had closed the laptop lid. This functionality should be configurable by the user as part of their power management options or policy. For example, a user enables WoL/proxy while the laptop lid is up, but off when the lid is closed and the laptop is potentially stored in a laptop bag.

- A sleeping proxy could detect a change in power source (say, DC to AC) and activate proxy on its preconfigured network.

- A proxy could continue operation when the system transitions from AC to DC mode.

The ability to detect these events when in low power (D3) is not currently possible in today's hardware. Implementing a solution for these events will help save energy and enhance the user experience.

A.2 Security Considerations

This International Standard does not specifically address Security concerns arising out of the proposed proxy protocol design. However, a number of potential threat scenarios have been identified and potential mitigation is suggested below.

- Denial of Sleep Attack – It is possible that an adversary may send periodic unauthenticated end-to-end packets to the proxy, denying the system from entering or staying in the Sleep state. This can be partially mitigated by using defense mechanisms (Firewalls, Intrusion Detection and Prevention systems), either externally and/or as part of the system.

- Compromised Proxy – It is possible that an adversary may assume control of the proxy and use the Proxy to launch attacks on the system, on the network, or on other Internet connected machines. This can be partially mitigated by using System measurement techniques for ensuring the integrity and robustness of the software/firmware/hardware that executes within the proxy.

- Subversion Attacks – It is possible that an adversary may take control of the proxy and use it to generate IP packets with Option headers that circumvent external defense mechanisms. This can be partially prevented by disallowing the proxy to generate IP packets with Options in its header.

- IPsec - IPsec can be deployed in one of two modes – tunnel and transport modes. Tunnel mode is used for IPsec-encapsulation of VPN traffic where a remote client accesses one or more nodes in a trusted network via a VPN gateway. Traffic to the nodes in the trusted network is typically in-the-clear.