

[MS-NCT]:

Network Cost Transfer Protocol

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation (“this documentation”) for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft [Open Specifications Promise](#) or the [Microsoft Community Promise](#). If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
7/14/2016	1.0	New	Released new document.

Table of Contents

1	Introduction	4
1.1	Glossary	4
1.2	References	4
1.2.1	Normative References	5
1.2.2	Informative References	5
1.3	Overview	5
1.4	Relationship to Other Protocols	5
1.5	Prerequisites/Preconditions	5
1.6	Applicability Statement	5
1.7	Versioning and Capability Negotiation	6
1.8	Vendor-Extensible Fields	6
1.9	Standards Assignments	6
2	Messages	7
2.1	Transport	7
2.2	Message Syntax	7
2.2.1	Network Cost IE	7
2.2.1.1	Cost Flags	7
2.2.1.2	Cost Level	8
2.2.2	Tethering Identifier IE	8
3	Protocol Details	10
3.1	AP Role Details	10
3.1.1	Abstract Data Model	10
3.1.2	Timers	10
3.1.3	Initialization	10
3.1.4	Higher-Layer Triggered Events	10
3.1.5	Message Processing Events and Sequencing Rules	10
3.1.6	Timer Events	10
3.1.7	Other Local Events	10
3.2	Client Role Details	10
3.2.1	Abstract Data Model	10
3.2.2	Timers	10
3.2.3	Initialization	11
3.2.4	Higher-Layer Triggered Events	11
3.2.5	Message Processing Events and Sequencing Rules	11
3.2.6	Timer Events	11
3.2.7	Other Local Events	11
4	Protocol Examples	12
5	Security	14
5.1	Security Considerations for Implementers	14
5.2	Index of Security Parameters	14
6	Appendix A: Product Behavior	15
7	Change Tracking	16
8	Index	17

1 Introduction

The Network Cost Transfer Protocol enables an **IEEE 802.11 access point (AP)** to communicate the **network cost** and information about the AP to **clients**.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

1.1 Glossary

This document uses the following terms:

802.11 Access Point (AP): Any entity that has IEEE 802.11 functionality and provides access to the distribution services, via the wireless medium for associated stations (STAs).

Beacon: A management frame that contains all of the information required to connect to a network. In a WLAN, Beacon frames are periodically transmitted to announce the presence of the network.

client: Synonym for client computer (4).

information element (IE): A unit of information transmitted as part of the management frames in the IEEE 802.11 [\[IEEE802.11-2012\]](#) protocol. Wireless devices, such as access points, communicate descriptive information about themselves in the form of one or more IEs in their management frames.

Media Access Control (MAC) address: A hardware address provided by the network interface vendor that uniquely identifies each interface on a physical network for communication with other interfaces, as specified in [\[IEEE802.3\]](#). It is used by the media access control sublayer of the data link layer of a network connection.

Message Authentication Code (MAC): A message authenticator computed through the use of a symmetric key. A **MAC** algorithm accepts a secret key and a data buffer, and outputs a **MAC**. The data and **MAC** can then be sent to another party, which can verify the integrity and authenticity of the data by using the same secret key and the same **MAC** algorithm.

metered network: A network on which data usage is measured and limited.

network cost: Information about how the Internet service provider bills customers for data usage on the network.

Probe Response: A frame that contains the advertisement IE for a device. The Probe Response is sent in response to a Probe Request. The Probe Response frame is defined in the Wi-Fi Peer-to-Peer (P2P) Specification v1.2 [\[WF-P2P1.2\]](#) section 4.2.3.

tether: Enables a device to gain access to the Internet by establishing a connection with another device that is connected to the Internet.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as defined in [\[RFC2119\]](#). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](#).

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information.

[IEEE-OUI] IEEE Standards Association, "IEEE OUI Registration Authority", February 2007, <http://standards.ieee.org/regauth/oui/oui.txt>

[IEEE802.11-2007] Institute of Electrical and Electronics Engineers, "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", ANSI/IEEE Std 802.11-2007, <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

Note There is a charge to download this document.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/rfc/rfc2119.txt>

1.2.2 Informative References

None.

1.3 Overview

The Network Cost Transfer Protocol enables an IEEE 802.11 access point (AP) to communicate the network cost and information about the AP to clients. It defines two vendor-specific **information elements (IEs)**, Network Cost and Tethering Identifier, within the 802.11 **Beacon** and **Probe Response** to relay this information to the client.

Network Cost IE is used by clients to determine whether data transferred on that particular connection is metered. <1> The Tethering Identifier IE is used to differentiate **tethering** (device-based) networks from stand-alone APs. <2> The difference can then be used to vary the experience in implementation-defined ways.

1.4 Relationship to Other Protocols

The Network Cost Transfer Protocol extends the IEEE802.11 standard, whose conventions are applied as specified in [\[IEEE802.11-2007\]](#). The Network Cost Transfer Protocol introduces a specific use for one of that protocol's reserved information element types, and it defines additional **MAC** layer abstract service primitives for managing the configuration, transmission, and receipt of these new information elements.

1.5 Prerequisites/Preconditions

The Network Cost Transfer Protocol requires APs to adhere to 802.11 standard specifications. The AP should have knowledge about the metered state of its network connection. This state may be explicitly configured, inferred from media type, or obtained using any other relevant means.

1.6 Applicability Statement

This protocol is only applicable to APs that support Tethering. The client is required to support connecting to Wi-Fi networks. Lastly, the Tethering Identifier information element (IE) only applies to multi-purpose devices capable of acting as access points, not to dedicated network hardware.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

Parameter	Value	Reference
OUI	00-50-f2	As specified in [IEEE-OUI]

2 Messages

2.1 Transport

The two vendor-specific information elements in the Network Cost Transfer Protocol are transmitted as part of IEEE802.11 Beacons or Probe Responses. There are no requirements for the order of the information elements and it is not necessary that both of them are used at the same time.

The format of information elements is specified in [\[IEEE802.11-2007\]](#) section 7.3.2. The format and processing of Beacon or Probe Response frames are also specified in [\[IEEE802.11-2007\]](#).

2.2 Message Syntax

The following sections specify Network Cost Transfer Protocol Message syntax.

2.2.1 Network Cost IE

The structure of the Network Cost information element (IE) is shown in the following packet.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ATTR										Length						OUI															
...										OUI_Type						Reserved						Cost_Flags									
Reserved										Cost_Level																					

ATTR - Attribute_ID (1 byte): Contains the ID of the element as specified [\[IEEE802.11-2007\]](#) section 7.3.2. It MUST contain a value of 221, identifying a vendor-specific element (as specified in [\[IEEE802.11-2007\]](#) table 26) in which the vendor is identified by an IEEE-issued OUI.

Length (1 byte): The total length of the subsequent fields. This value MUST be 0x08.

OUI - Organizationally Unique Identifier (3 bytes): The IEEE-assigned OUI for Microsoft. The **OUI** field MUST contain a value of (00:50:f2) as specified in [\[IEEE-OUI\]](#).

OUI_Type (1 byte): A packet subtype within the universe specific to a particular OUI value. For the Network Cost IE, the OUI Type MUST contain a value of 0x11.

Reserved (1 byte): MUST be 0.

Cost_Flags (1 byte): Flags that indicate possible states of the network connection, as specified in section 2.2.1.1.

Reserved (1 byte): MUST be 0.

Cost_Level (1 byte): A value indicating the metering type of the network connection, as specified in section 2.2.1.2.

2.2.1.1 Cost Flags

The following table shows the possible **cost flags** that can be represented in the IE:

Value	Name	Description
0x01	Over Data Limit	Usage has exceeded the data limit of the metered network ; different network costs or conditions might apply.
0x02	Congested	The network operator is experiencing or expecting heavy load.
0x04	Roaming	The tethering connection is roaming outside the provider's home network or affiliates.
0x08	Approaching Data Limit	Usage is near the data limit of the metered network; different network costs or conditions might apply once the limit is reached.

If the AP is aware that any of these states applies to its network connection, it SHOULD indicate the corresponding flag in all beacons and probe responses.

2.2.1.2 Cost Level

The following table shows the possible **cost levels** that can be represented in the IE:

Value	Name	Description
0x01	Unrestricted	The connection is unlimited and has unrestricted usage constraints.
0x02	Fixed	Usage counts toward a fixed allotment of data which the user has already paid for (or agreed to pay for).
0x04	Variable	The connection cost is on a per-byte basis.

The AP MUST indicate the cost level that most accurately describes the network's cost and metering type, based on configuration or other information sources [<3>](#).

2.2.2 Tethering Identifier IE

The structure of the Tethering Identifier information element (IE) is shown in the following packet:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
A										Length										OUI											
...										OUI_Type										Type											
Length															MAC_Address																
...																															

A - Attribute_ID (1 byte): Contains the ID of the element as specified [\[IEEE802.11-2007\]](#) section 7.3.2. It MUST contain a value of 221, identifying a vendor-specific element (as specified in [\[IEEE802.11-2007\]](#) table 26) in which the vendor is identified by an IEEE-issued OUI.

Length (1 byte): The length of the subsequent fields. This value MUST be 14 (0x0E).

OUI - Organizationally Unique Identifier (3 bytes): The IEEE-assigned OUI for Microsoft. The **OUI** field MUST contain a value of (00:50:f2) as specified in [\[IEEE-OUI\]](#).

OUI_Type (1 byte): A packet subtype within the universe specific to a particular OUI value. For the Tethering Identifier IE, the OUI Type MUST contain a value of 12.

Type (2 bytes): Used to specify that the network is broadcasted as tethered. The **type** field MUST contain a value of 43 (0x2B).

Length (2 bytes): Contains the length of the **MAC_Address** field in octets. This value MUST be 6 (0x06).

MAC_Address (6 bytes): Contains the **MAC address** of the AP.

3 Protocol Details

3.1 AP Role Details

To compensate for an unreliable transmission over the wireless medium, the information elements SHOULD be contained in each Beacon frame and probe response.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

The 802.11 Access Point (AP) MUST have initial information about the cost state of the upstream flow of data and convey the appropriate flag in the IE. This information may be administratively configured, inferred from media type, or acquired by other means.

3.1.4 Higher-Layer Triggered Events

If the metering state of the network changes, the AP should immediately reflect the new value in all future beacons and probe responses.

3.1.5 Message Processing Events and Sequencing Rules

None.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Client Role Details

The client acquires information about the network during network discovery and connection. The client role is triggered when in range of an 802.11 Access Point (AP) and finding the relevant information element in the beacon or probe response frame.

3.2.1 Abstract Data Model

For each AP to which the client is currently connected, the client should maintain the current estimated cost state and network type.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

When in range of an 802.11 Access Point (AP), the client should inspect the beacon and probe response frames for the information elements defined by this protocol. If they are present, they should inform the client's data about the network. If not, the client may infer value using implementation-specific defaults.

3.2.5 Message Processing Events and Sequencing Rules

If these information elements are found, the local knowledge of the current network should be updated with the information they contain. Use of this information is implementation-dependent and handled by higher-layer protocols.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

The following table shows some sample cost attribute values:

Name	Cost Flag	Cost Level	Description
Default WLAN	0x00	0x01	Unrestricted connection; standard WLAN backed by fixed broadband.
Portable Hotspot Default	0x00	0x02	Metered network; limit unknown or not yet reached; reasonable default for mobile broadband connections without other information.
Over Limit / Throttled	0x01	0x01	User has exceeded data limit; speed is reduced, but no further usage limitation applies.
Over Limit / Charges	0x01	0x04	User has exceeded data limit; additional usage incurs incremental charges.
Portable Hotspot / Roaming	0x04	0x04	Connection is roaming; incremental charges apply due to network state.

The following is an example of the Network Cost IE conveyed in a Beacon or Probe Response frame for the over data limit cost flag.

Offset (hex)	Value (hex)	Field
0000	DD	Element ID
0001	08	Length
0002	00	OUI (Microsoft)
0003	50	
0004	F2	
0005	11	OUI Type
0006	00	Reserved
0007	01	Cost Flag (Over Data Limit)
0008	00	Reserved
0009	02	Cost Level (Fixed)

Figure 1: Example of the Network Cost IE

The following is an example of the Tethering Identifier IE conveyed in a Beacon or Probe Response frame.

Offset (hex)	Value (hex)	Field
0000	DD	Element ID
0001	08	Length
0002	00	OUI (Microsoft)
0003	50	
0004	F2	
0005	11	OUI Type
0006	00	Type
0007	2B	
0008	00	Length
0009	06	
0010	68	MAC Address
0011	5D	
0012	43	
0013	0B	
0014	66	
0015	12	

Figure 2: Example of the Tethering Identifier IE

5 Security

5.1 Security Considerations for Implementers

The information transferred by this protocol is transmitted unencrypted, even for a secured AP. Do not include sensitive information.

5.2 Index of Security Parameters

None.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs.

- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 R2 operating system
- Windows 10 operating system
- Windows Server 2016 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

[<1> Section 1.3](#): Windows 8 and Windows Server 2012 could consume but not generate the IE. They implemented only the client role.

[<2> Section 1.3](#): Windows 8 and Windows Server 2012 did not implement this IE.

[<3> Section 2.2.1.2](#): Windows implementations acting as APs always set the cost to Fixed with no flags set, regardless of the actual state.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index

A

[Applicability](#) 5

C

[Capability negotiation](#) 6

[Change tracking](#) 16

F

[Fields - vendor-extensible](#) 6

G

[Glossary](#) 4

I

[Implementer - security considerations](#) 14

[Index of security parameters](#) 14

[Informative references](#) 5

[Introduction](#) 4

M

Messages

[Network Cost IE](#) 7

[Tethering Identifier IE](#) 8

[transport](#) 7

N

[Network Cost IE message](#) 7

[Normative references](#) 5

O

[Overview \(synopsis\)](#) 5

P

[Parameters - security index](#) 14

[Preconditions](#) 5

[Prerequisites](#) 5

[Product behavior](#) 15

R

[References](#) 4

[informative](#) 5

[normative](#) 5

[Relationship to other protocols](#) 5

S

Security

[implementer considerations](#) 14

[parameter index](#) 14

[Standards assignments](#) 6

T

[Tethering Identifier IE message](#) 8

[Tracking changes](#) 16

[Transport](#) 7

V

[Vendor-extensible fields](#) 6

[Versioning](#) 6