Internet-Draft
Category: Experimental
Document: draft-bichot-network-discovery-protocol-02.txt

Guillaume Bichot
THOMSON

April 2003

Network Discovery Protocol (NETDIS)
draft-bichot-network-discovery-protocol-01.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Abstract

This document describes the Network Discovery Protocol (NETDIS), a protocol that provides a way to broadcast information about the network service accessible through the access network where the information is broadcasted. This allows several service providers to share the same access network. The public WLAN access network is particularly targeted by this protocol. As a result a mobile terminal listening NETDIS announcements discovers the list of Service providers (Virtual WLAN operator) supported by the WLAN it is currently attached.

Table of Contents

1. Introduction

The development of public data access network is growing. These networks mainly wireless (WLAN) offer the access to Internet, local services and potentially other core network (3G) services. Since it is impossible, for a customer to subscribe to all possible independent WLAN operators, some service providers provide an aggregation of these WLAN hot spots. They are also called virtual operators. A subscriber of such virtual operator can access to the core network (Internet for instance) through several independent WLANs.

The core network may be Internet or a mobile (3G) network or other private network. The WLAN virtual network operator may be the core network operator.

It is likely that several [virtual] network operators share a public WLAN access network. For instance, in a hot spot like an airport, the WLAN operator has an agreement with two virtual network operators in such a way the customers from both core network operators may access to their respective service (e.g. Internet) through the airport WLAN. There is a need to announce (broadcast) in the access network such information about, basically, the availability of the [virtual]

network operator and the information for accessing the core network (e.g. Internet).

2. Model

The figure 1 illustrates the NETDIS model. A NETDIS controller has in charge to collect NETDIS announcement packets and multicast them within the public access network. The NETDIS announcement packet contains information relative to a [virtual] network operator and the type of core network that can be accessed. The way the NETDIS Announcer delivers the packets to the NETDIS Controller is out of scope of this document. The NETDIS controller may be located within the access network, within a third party operator/aggregator network or anywhere else. The NETDIS Announcer may be located within the access network, the core network, within a third party operator aggregator or anywhere else.

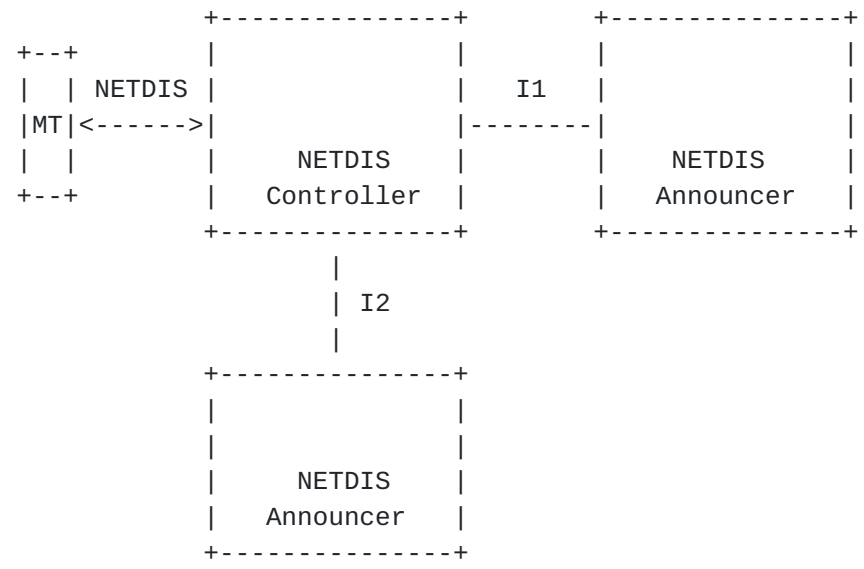

Figure 1: The NDIS model

3. Network announcement

//The SAP protocol (RFC 2974) could be used to carry the announcements. However RFC 2974 stipulates that a SAP listener shall support SDP (RFC 2327). Due to this constraint we have also defined a new announcement protocol based on SAP. Both options are possible.

3.1 SAP potential usage

In case of the usage of SAP, the following constraints apply.

- Session deletion is not supported
- Encryption is not supported
- The SAP announcer is located in the NDP controller.
- The originating source field shall be empty
- A new payload type is defined: 'application/NETDIS'

3.2 NETDIS announcement protocol

This is the protocol to be used instead of SAP.

NETDIS uses UDP/IP multicast in order to broadcast the information relative to the different network services. For each network service provider, announcements [packets] are sent regularly and continuously within the well-known multicast channel.

IPv4 global scope network announcements use multicast addresses in the range 224.2.128.0 - 224.2.255.255 with NETDIS announcements being sent to <TBD>

IPv6 are announced on the address FF0X:0:0:0:0:0:2:7FFE where X is the 4-bit scope value. For example, an announcement for a link-local session assigned the address FF02:0:0:0:0:0:1234:5678, should be advertised on NETDIS address FF02:0:0:0:0:0:2:7FFE.

NETDIS announcements MUST be sent on port <TBD> and SHOULD be sent with an IP time-to-live of 255.

The announcement contains the identity of the [virtual] network operator as well as some information regarding the network. The header MAY be signed.

3.3 Transport protocol

NETDIS (or SAP) packets are carried over UDP / IP.

3.4 Announcement interval

The time period between repetitions of an announcement is chosen such that the total bandwidth used by all announcements on a single NETDIS group remains below a preconfigured limit. Each announcement should have an equal announcement interval that will be fixed by the NETDIS controller.

4. Packet format

The figure 2 represents an NETDIS announcement packet carried by the SAP packet. The SAP header as well as the payload type field is described in [1].

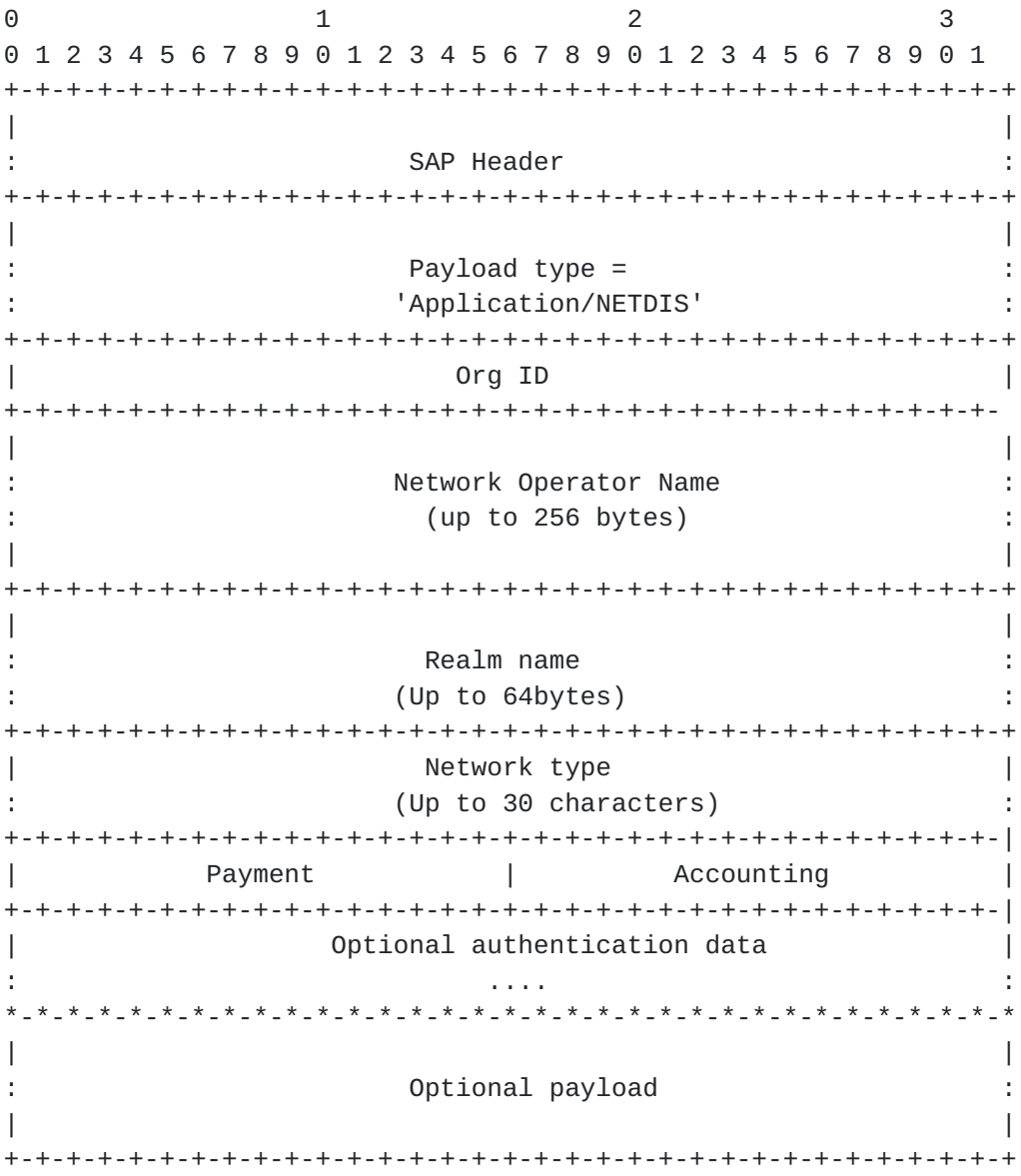

Figure 2: SAP carries NETDIS packet

The figure 3 represents a NETDIS announcement packet carried by the NETDIS announcement protocol.

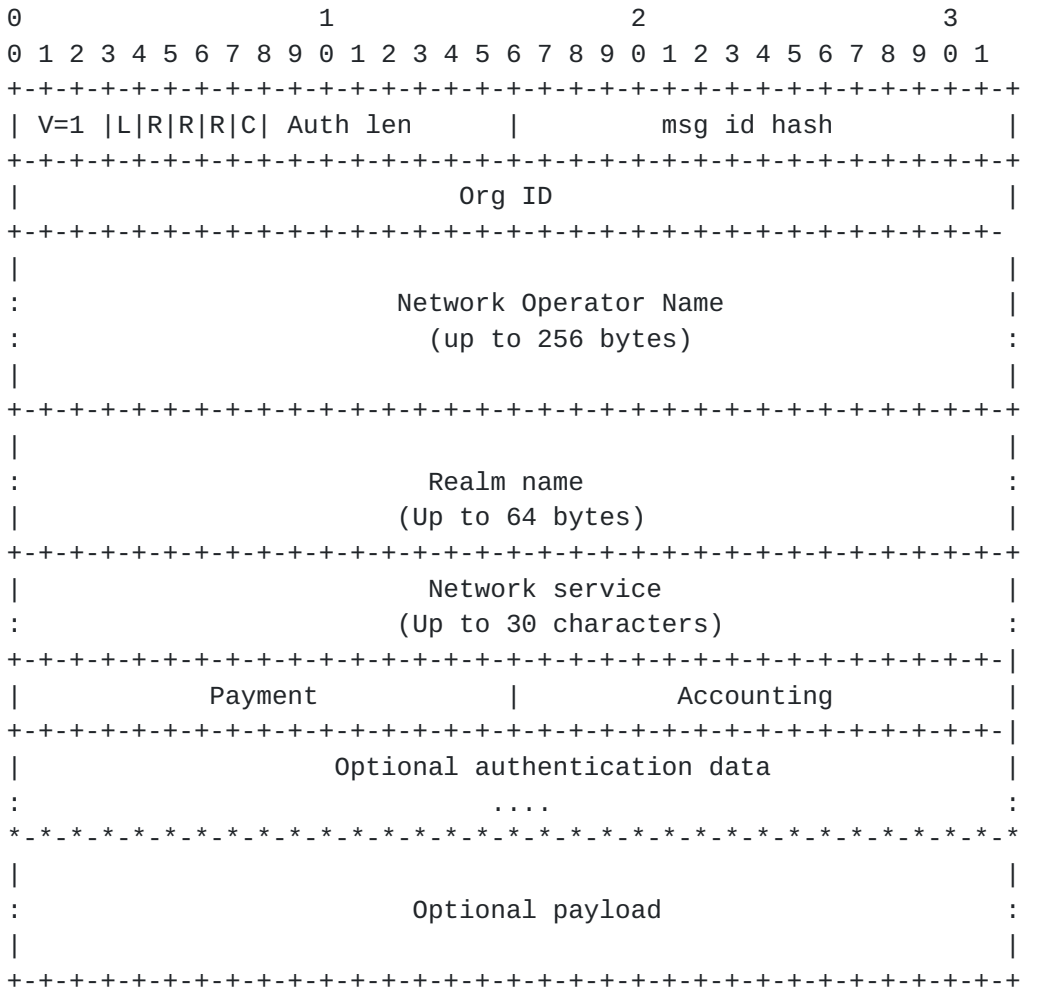

Figure 2 NETDIS announcement protocol carries NETDIS packet

V: Version Number. The version number field MUST be set to 1.

L: Indicates whether the announcement relies to the access (local) network. If yes L is set to 1. Otherwise L is set to 0

R: Reserved. NETDIS announcers MUST set this to 0, NETDIS listeners MUST ignore the contents of this field.

C: Compressed bit. If the compressed bit is set to 1, the payload is compressed using the zlib compression algorithm [3]. If the payload is to be compressed and encrypted, the compression MUST be performed first.

Auth len: An 8 bit unsigned quantity giving the number of 32 bit words following the main NETDIS header that contain authentication data. If it is zero, no authentication header is present.

Authentication data: containing a digital signature of the packet, with length as specified by the authentication length header field. See [1] for details. Alternatively, an organization (see Organization ID) may specify its own authentication mechanism. If it is the case the Authorization Length MUST be set to zero.

Msg id hash: A 16 bits quantity that used in combination with the real name and the network service provides a globally unique identifier indicating the precise version of this announcement. The choice of value for this field is not specified here, except that it MUST be unique for each Network announcement by a particular NETDIS announcer and it MUST be changed if the announcement description is modified.

Org ID: an organization identifier. Identify the organization (e.g. standardization body) that has characterized this announcement. Extra value is defined and registered through IANA.

Ox00000000: default value meaning no organization specified.
0x10xxxxxx: IETF: the remaining 24 bits point out the RFC that this announcement relies on.

Network operator name: this is the name of the [virtual] operator of the network. The network operator is a well-identified interlocutor for the customer, the client. The name is a bytes string that may contain any byte with the exceptions of 0x00 that is used to terminate the string. By default the byte string contains US-ASCII characters. The format of this field may however depend on the Organization ID (see above). The value may for instance correspond to the so-called PLMN-ID as defined in [4].

Realm name: This gives the domain name the announcement relies on. This is a character string formatted according to [3]. The NETDIS listener may use the realm name to form the Network Access Identifier (NAI) as specified in [3]. One announcement relies on one real name. This means that an operator that wants to propose several different network accesses will use different real names and thus will generate several announcements: one per network access.

Network service: this identifies the type of service the operator offers the access. The field is a bytes string that may contain any byte with the exceptions of 0x00 that is used to terminate the string. By default the byte string contains US-ASCII characters. This document defines a few services. New network services may be defined

according to the organization ID. One announcement relies on one network service. This means that an operator that wants to propose several network services generates several announcements: one per network service.

0x00: Null byte string: Not identified: the network type is unknown.

"IN" - Internet access: The [virtual] network operator offers the access to the Internet. After being authenticated by the service provider, the client can access to the Internet. There is no recommended format for the Network Operator Name. There is no extra information linked with this network type.

The following values are examples. It is up to each organization body to defines new network service values.

"3GPP" - 3GPP access: the [virtual] network operator offers the access to a 3GPP network services. Authentication and all 3GPP services are managed through the 3GPP network according to a well-known method (e.g. 3GPP).

"3GPP2" - 3GPP2 access: the [virtual] network operator offers the access to a 3GPP2 network. Authentication and all 3GPP services are managed through the 3GPP network according to a well-known method (e.g. 3GPP2).

Payment: this 16 bits field identifies the method of payment that is accepted by the service provider. Each bit indicates whether the corresponding method is available (1) or not (0). The following values are defined.

All 00: not identified: the payment method is not identified
0x0001 - pre-paid card: a pre-paid card from the provider may be used
0x0002 - subscription: The services from that service provider are available only on subscription.
0x0004 - credit card: the service may be paid online with a credit card.
0x0008 - Free: the service(s) from that service provider is (are) free

Accounting: defines the way the [virtual] network operator debits your account. Each bit indicates whether the corresponding method is available (1) or not (0). For each valid method an associated string located in the payload field indicates the price. The price is a bytes string that may contain any byte with the exceptions of 0x00 that is used to terminate the string. By default the byte string contains US-ASCII characters. The format of this price string may however depend on the Organization ID (see above).

The following values are defined.

All 00: not identified: the accounting method is not identified
0x0001 - Divers: The method and the fees are explicitly mentioned in the associated string located in the payload part.
0x02 - day: the fee is for a 24 hours period
0x03 - minute: each minute of the session is counted.
0x04 - Size: the fee depends on the total amount of data exchanged during the session
0x05 - Connection: each successful connection implies a well-defined fee.

The header is followed by the optional payload data. If the C bit is set in the header the payload is compressed. The payload gathers optional accounting information and extra information according to a specification identified by the organization ID.

5. Implementation

One context this protocol makes sense is the public WLAN.

A mobile terminal (the NETDIS listener) discovers a set of access points and associates with one according to the WLAN specification (best signal strength for instance). No particular ESSID (or equivalent WLAN ID) is targeted. Once the terminal is associated it listens the NETDIS announcements. The user (or the terminal if only one choice is possible) chooses the network operator he wants to deal with and triggers the authentication process.
If no announcement is present, the terminal may try to associate with another access point belonging to another network (different ESSID or equivalent WLAN ID). If there is no other WLAN (ESSID) or no announcement are present then NETDIS fails.

The mobile terminal can even listens the NETDIS announcement before being associated with whatever access point. The terminal needs only to join/synchronize with an access point and it should be able to listen the multicast/broadcast packets). In case of several access points in range, the terminal listen the different announcement from the different access points. There may be several WLANs. The user (or the terminal if only one choice is possible) chooses the network operator he wants to deal with and triggers the association between the mobile terminal and the corresponding access point.

The mobile terminal may use the realm name (found in the announcement) as part of the NAI [3] in order to establish the AAA connection (EAP) with the host associated with the chosen [virtual] network operator.

6. Security Considerations

NETDIS (as SAP) contains mechanisms for ensuring integrity of session announcements, for authenticating the origin of an announcement.

In case of non-usage of the integrity protection mechanism some denial of service attacks are possible.

- A Rogue NETDIS controller can floods the medium with wrong announcements.
- A rogue NETDIS controller can spoof announcements by catching real announcements, modify them and forward them. Although in a wireless environment this type of attack is unlikely it may appear when the rogue controller (an access point in that case) has a better signal strength than the regular Controller (access point). The NETDIS listener would then prefer to listen the Rogue controller. A way to solve that problem is for the listener to listen several controllers (access points), one after the other, in order to compare the announcements.

7. References

1 Session Announcement Protocol, RFC 2974, October 2000.
2 Session Description Protocol, RFC 2327, April 1998.
3 Network Access Identifier, RFC 2486
4 Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification

8. Acknowledgments

9. Author's Addresses

Guillaume Bichot
THOMSON
2 independence way
Princeton, NJ 08540 - USA
Email: guillaume.bichot@thomson.net

10. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

11. Full Copyright Statement