Network Working Group
Internet-Draft
Expires: April 6, 2004

R. Droms
J. Schnizlein
Cisco Systems
October 7, 2003

RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option

draft-ietf-dhc-agentopt-radius-03.txt

Status of this Memo

Copyright Notice

Abstract

A network access device may choose to authenticate the identity of a device before granting that device access to the network. The IEEE 802.1X protocol is an example of a mechanism for providing authenticated layer 2 network access. A network element using RADIUS as an authentication authority will receive attributes from a RADIUS server that may be used by a DHCP server in the selection of an IP address for assignment to the device through its DHCP client. The RADIUS Attributes sub-option enables a network element to pass along attributes for the user of a device received during RADIUS authentication to a DHCP server.

1. Introduction and Background

The RADIUS Attributes sub-option for the DHCP Relay Agent option provides a way through which network elements can pass information obtained through layer 2 authentication to a DHCP server [2]. IEEE 802.1X [3] is an example of a mechanism through which a network access device such as a switch or a wireless LAN access point can authenticate the identity of the user of a device before providing layer 2 network access using RADIUS [4] as the Authentication Service specified in 802.1X. In 802.1X authenticated access, a device must first exchange some authentication credentials with the network access device. The access device then supplies these credentials to a RADIUS server, which either confirms or denies the identity of the user of the device requesting network access. The access device, based on the reply of the RADIUS server, then allows or denies network access to the requesting device.

Figure 1 summarizes the message exchange among the participants in IEEE 802.1X authentication.

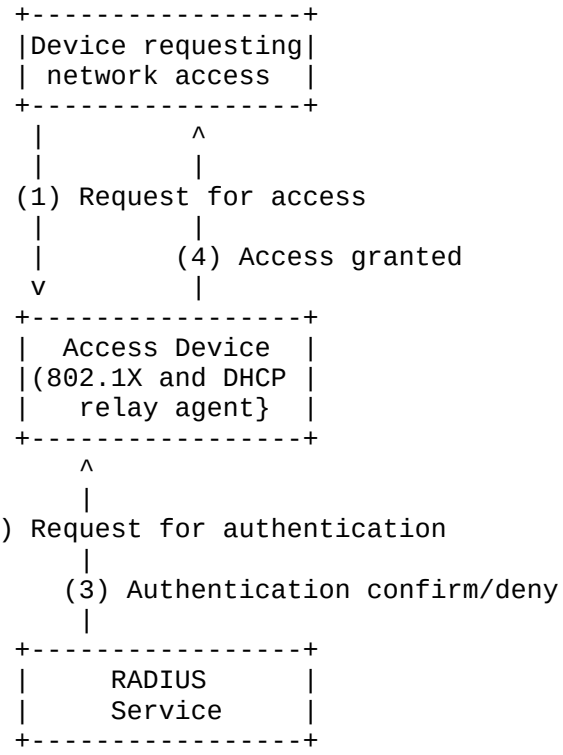


Figure 1

Figure 1

In the application described in this document, the access device acts as an 802.1X authenticator and adds DHCP relay agent options to DHCP messages. During 802.1X authentication, the reply message from the RADIUS server carries additional identification information as attributes to the access device. The access device stores these attributes locally. When the access device subsequently forwards DHCP messages from the network device, the access device adds the identification information in an RADIUS Attributes sub-option. The RADIUS Attributes sub-option is another suboption of the Relay Agent Information option [5].

This document uses IEEE 802.1X as an example to motivate the use of RADIUS by an access device. The RADIUS Attributes sub-option described in this document is not limited to use in conjunction with IEEE 802.1X and can be used to carry RADIUS attributes obtained by the relay agent for any reason.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

2.1 General Terminology

Access device: A network element providing network access to a host

2.2 DHCP Terminology

The following terms are used as defined in RFC2131 and RFC3046: DHCP relay agent, DHCP server, DHCP client.

2.3 RADIUS Terminology

The following terms are used in conjunction with RADIUS:

RADIUS server: An entity that provides RADIUS service through the exchange of RADIUS protocol messages

Attribute: Data value carried in a RADIUS protocol message

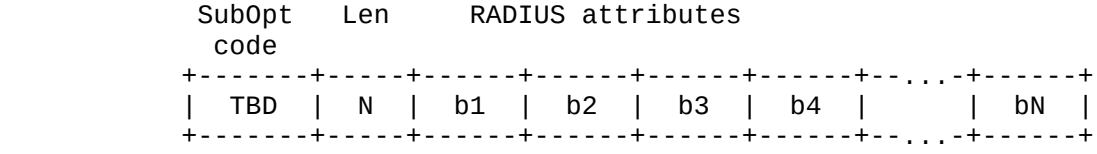
2.4 802.1X Terminology

The following terms are used as defined in the IEEE 802.1X protocol: Authenticator, Supplicant.

3. RADIUS Attributes sub-option format

The RADIUS Attributes Sub-option is a new sub-option for the DHCP Relay Agent option.

The format of the RADIUS Attributes sub-option is:



The RADIUS attributes are encoded according to the encoding rules in RFC 2865, in bytes b1...bN.

4. DHCP Relay Agent Behavior

When the DHCP relay agent receives a DHCP message from the client, it MAY append a DHCP Relay Agent Information option containing the RADIUS Attributes sub-option, along with any other sub-options it is configured to supply. The RADIUS Attributes sub-option MUST contain the attributes received in response to the client's authentication with the RADIUS service. The DHCP relay agent MUST NOT add more than one RADIUS Attributes sub-option in a message.

The relay agent SHOULD include the User-Name and Class attributes in the RADIUS Attributes sub-option, and MAY include other attributes.

5. DHCP Server Behavior

When the DHCP server receives a message from an relay agent containing a RADIUS Attributes sub-option, it extracts the contents of the of the sub-option and uses that information in selecting configuration parameters for the client.

6. DHCP Client Behavior

The host need not make any special provision for the use of the RADIUS Attributes sub-option.

7. RADIUS Server Behavior

The RADIUS server MUST return the User-Name and Class attributes to the access device, and MAY return other attributes.

8. Security Considerations

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in RFC 3118 [6]. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in RFC 2131.

The DHCP Relay Agent option depends on a trusted relationship between the DHCP relay agent and the server, as described in section 5 of RFC 3046. While the introduction of fraudulent relay-agent options can be prevented by a perimeter defense that blocks these options unless the relay agent is trusted, a deeper defense using the authentication option for relay agent options [7] or IPsec [8] SHOULD be deployed as well.

9. IANA Considerations

IANA has assigned the value of TBD for the DHCP Relay Agent Information option sub-option code for this sub-option. This document does not define any new namespaces or other constants for which IANA must maintain a registry.

10. Terms of Use

Cisco has a pending patent which relates to the subject matter of this Internet Draft. If a standard relating to this subject matter is adopted by IETF and any claims of any issued Cisco patents are necessary for practicing this standard, any party will be able to obtain a license from Cisco to use any such patent claims under openly specified, reasonable, non-discriminatory terms to implement and fully comply with the standard.

Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[3] Institute of Electrical and Electronics Engineers, "Port based Network Access Control", IEEE Standard 802.1X, March 2001.

[4] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June

2000.

[5] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

Informative References

[6] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[7] Stapp, M., Lemon, T. and R. Droms, "The Authentication Suboption for the DHCP Relay Agent Option", draft-ietf-dhc-auth-suboption-01 (work in progress), November 2002.

[8] Droms, R., "Authentication of DHCP Relay Agent Options Using IPsec", draft-ietf-dhc-relay-agent-ipsec-00 (work in progress), September 2003.

Authors' Addresses

Ralph Droms
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
USA

EMail: rdroms@cisco.com

John Schnizlein
Cisco Systems
9123 Loughran Road
Fort Washington, MD 20744
USA

EMail: jschnizl@cisco.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.