Network Working Group
INTERNET-DRAFT
Category: Informational
<draft-aboba-802-context-02.txt>
6 April 2002

Bernard Aboba
Tim Moore
Microsoft

A Model for Context Transfer in IEEE 802

Abstract

The IEEE 802 Inter-Access Point Protocol (IAPP), under development within the IEEE 802.11 TgF working group, supports the transfer of context between access points implementing IEEE 802 technology. This document describes how IAPP can be used to support transfer of authentication, authorization and accounting (AAA) context between devices supporting IEEE 802.1X network port authentication. This specification is currently being developed within the IEEE 802.11 TgF working group and is being presented to the IETF for informational purposes.

1. Introduction

[IEEE8021X] enables authenticated access to [IEEE802] media, including Ethernet [IEEE8023], Token Ring, and 802.11 wireless LANs [IEEE80211]. Although Authentication, Authorization and Accounting (AAA) support is optional within IEEE 802.1X, it is expected that many IEEE 802.1X Authenticators will function as AAA clients. Behavior of IEEE 802.1X Authenticators acting as RADIUS clients is described in [Congdon].

The IEEE 802 Inter-Access Point Protocol (IAPP), under development within the IEEE 802.11 TgF working group, supports the transfer of context between access points implementing IEEE 802 technology. This document describes how IAPP can be used to support transfer of authentication, authorization and accounting (AAA) context between devices supporting IEEE 802.1X network port authentication [IEEE8021X].

In terms of organization, this document first develops a general model for AAA context transfer. Central to the model is the notion of a "correct" context transfer -- a transfer resulting in the same context on the new access point as would have resulted had a AAA conversation been completed.

The circumstances in which "correct" context transfer can be achieved are analyzed -- demonstrating that this can only be achieved in a limited set of circumstances. As a result, it is suggested that context transfer protocols restrict the domain of applicability to scenarios involving a high degree of homogeneity.

For example, layer 2 context transfer solutions are most likely to be successful transferring context within media families, such as IEEE 802. While the IAPP protocol is expected to be used primarily for transfer of context between IEEE 802.11 access points, it is also possible for it to be used to transfer context between access points supporting other IEEE 802 media, such as IEEE 802.15 or 802.16. Where context transfer between dissimilar media is required, then higher layer homogeneity is needed. This can be achieved, for example, by restricting applicability to access points supporting Mobile IP.

1.1. Terminology

This document uses the following terms:

Authenticator

An Authenticator is an entity that require authentication from the Supplicant. The Authenticator may be connected to the Supplicant at the other end of a point-to-point LAN segment or 802.11 wireless link.

Authentication Server
An Authentication Server is an entity that provides an Authentication Service to an Authenticator. This service verifies from the credentials provided by the Supplicant, the claim of identity made by the Supplicant.

Port Access Entity (PAE)
The protocol entity associated with a physical or virtual (802.11) Port. A given PAE may support the protocol functionality associated with the Authenticator, Supplicant or both.

Supplicant
A Supplicant is an entity that is being authenticated by an Authenticator. The Supplicant may be connected to the Authenticator at one end of a point-to-point LAN segment or 802.11 wireless link.

1.2. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [RFC2119].

2. Context transfer model

In attempting to transfer context between devices, the first task is to understand how "context" is defined, and what the goal of the context transfer is. For the purpose of this document "context" will refer to the set of state defining the service to be provided to the user.

To date, a number of protocols have been proposed for defining and managing services provided on a per-user basis. RADIUS, defined in [RFC2865], [RFC2866], [RFC2867], [RFC2868],[RFC2869], and [RFC3162] is a first-generation protocol for Authentication, Authorization and Accounting (AAA). Diameter and COPS have also been proposed for use in

AAA.

In each of these protocols, exchanges are used to establish, and possibly to remove, state from devices. In thinking about transfer of context initially established through such protocols, we propose the "Equivalency Principle":

> For context established via protocol exchanges, transfer of context to a new device can be accomplished by transferring the protocol exchanges that created the context on the original device, and processing them on the new device. For such a context transfer to be successful, the the state created on the new device by processing

> such an exchange MUST be equivalent to the state that would have been created by having the new device engage in a fresh protocol conversation.

For the equivalency principle to be satisfied, it is necessary for the new device to be able to process the protocol exchanges from the old device, and for those exchanges to result in the same state on the new device. This requires that the protocol messages completely describe the context to be created on the device, and that the effect of processing these messages not depend on state that exists uniquely on the old device, but may not exist on the new device.

For example, a protocol message that describes the state to be attained in terms of deltas from a previous state would not be suitable for use in context transfer, since the effect of the protocol message would differ depending on the previous device state. Similarly, if a protocol message were conditionally executed based on dynamic data, such as the number of users on the device, then the message might have a different effect on the new device than on the old device.

To a large extent, AAA protocols meet the criteria, since the desired device state is completely described by the authorizations. Conditional execution, if it occurs, is usually confined to the AAA server.

The messages that establish service context differ, depending on the AAA protocol that is being considered. Within RADIUS, service context is only established via an Access-Accept. Access-Reject messages do not establish context since their purpose is to deny access. Similarly, Access-Challenge messages do not establish context since they represent

an intermediate stage within the authentication conversation. Since only one RADIUS message (Access-Accept) establishes service context, to re-establish context on a new device, to first order it is only necessary to transfer Access-Accept messages to the new device, and process them as if they were sent by the RADIUS server.

Note that since only one RADIUS message type can establish context, the message type need not be included explicitly, since it is implicit. As a result, devices supporting transfer of RADIUS context need only transfer attributes, not the entire RADIUS message.

2.1. "Correct" context transfer

Given this model for context establishment, it is worthwhile to examine when the transfer of context between devices produces a "correct" result.

One way to define correctness in a context transfer is that the transfer establishes on the new device the same context as would have been

created had the new device completed a AAA conversation with the authentication server. Ideally, a context transfer should only succeed if it is "correct" in this way. If a successful context transfer would establish "incorrect" state, it would be preferable for such a transfer to fail.

Not all AAA and access device configurations are capable of meeting this definition of "correctness". Implicit within our context transfer model is trust between devices transferring context. Since the new device acts on the context transfer as though it had been instructed by a trusted AAA server, it is necessary for the new device to trust the old device.

In transfer of context across administrative domains, such a level of trust may not be possible or appropriate. As a result, a context transfer may fail even in situations where the devices are homogeneous, due to lack of trust between administrative domains.

If the deployment is heterogeneous, it also may be difficult to meet this definition of correctness. In these situations, AAA servers often perform conditional evaluation, in which the authorizations returned in an Access-Accept message are contingent on characteristics of the AAA

client or the user. For example, in a heterogeneous deployment, the AAA server might return different authorizations depending on the type of device making the request, in order to make sure that the requested service is consistent with device capabilities.

If differences between the new and old device would result in the AAA server sending a different set of messages to the new device than were sent to the old device, then a context transfer between the devices cannot be carried out correctly.

For example, if some access points within a deployment support dynamic VLANs while others do not, then attributes present in the Access-Request (such as the NAS-IP-Address, NAS-Identifier, Vendor-Identifier, etc.) could be examined to determine when VLAN attributes will be returned, as described in [Condgon]. VLAN support is defined in [IEEE8021Q].

In practice, this limits the situations in which context transfer can be expected to be successful. Where the deployed devices implement the same set of services, it may be possible to transfer context successfully. However, where the supported services differ between devices, the context transfer may not succeed. For example, [RFC2865], section 1.1 states:

> "A NAS that does not implement a given service MUST NOT implement the RADIUS attributes for that service. For example, a NAS that is unable to offer ARAP service MUST NOT implement the RADIUS attributes

> for ARAP. A NAS MUST treat a RADIUS access-accept authorizing an unavailable service as an access-reject instead."

Note that this behavior is only applies to attributes that are known, but not implemented. For attributes that are unknown, section of 5 of [RFC2865] states:

> "A RADIUS server MAY ignore Attributes with an unknown Type. A RADIUS client MAY ignore Attributes with an unknown Type."

Obeying the Equivalency Principle, if a new device is provided with RADIUS context for a known but unavailable service, then it MUST process this context the same way it would handle a RADIUS Access-Accept requesting an unavailable service. This MUST cause the context transfer to fail. However, if a new device is provided with RADIUS context that

indicates an unknown attribute, then this attribute MAY be ignored.

Although it may seem somewhat counter-intuitive, failure is indeed the "correct" result where a known but unsupported service is requested. Presumably a correctly configured AAA server would not request that a device carry out a service that it does not implement. This implies that if the new device were to complete a AAA conversation that it would be likely to receive different service instructions than those present in the context transfer. In such a case, failure of the context transfer is the desired result. This will cause the new device to go back to the AAA server in order to receive the appropriate service definition.

Thus in practice, context transfer is most likely to be successful within a homogeneous device deployment within a single administrative domain. For example, where all the devices support IEEE 802.1X, success is possible, as long as the same set of security services are supported. For example, it would not be advisable to attempt to transfer context between an 802.11 access point implementing WEP to an 802.15 access point without security support. The correct result of such a transfer would be a failure, since if the transfer were blindly carried out, then the user would be moved from a secure to an insecure channel without permission from the AAA server. Thus the definition of a "known but unsupported service" MUST encompass requests for unavailable security services. This includes vendor-specific attributes related to security, such as those described in [RFC2548].

In general, context transfers between media with different service models should not be expected to be successful. For example, attempts to transfer context between cellular devices and 802.11 access points cannot be "correct" within this model, unless the cellular access points implement the same set of services as the 802.11 access points. Where the implemented services differ, the correct behavior would be for such context transfers to fail, and for the 802.11 AP to pick up the correct

service definition by going back to the AAA server. Thus while attempted context transfers between heterogeneous technologies may fail, context transfers between homogeneous devices have a higher probability of success.

2.2. Context handling

AAA is not mandatory to implement for IEEE 802.1X Authenticators. The

IEEE 802.1X [IEEE8021X] specification provides guidelines for usage of RADIUS [RFC2865], a revised version of which can be found in [Congdon]. However, support for other protocols is feasible. Since a IEEE 802.1X Authenticator may support zero or more AAA protocols and implementation of AAA is non-mandatory, an IEEE 802.1X Authenticator cannot be assumed to implement any particular AAA protocol.

Therefore it is important that the context transfer protocol be agnostic with respect to AAA protocols. If two devices share support for a given AAA protocol, then the context transfer mechanism should enable the devices to interoperate. One way to accomplish this is to enable the context transfer mechanism to support multiple AAA protocols within the same message. This allows a device that speaks multiple protocols to interoperate with a device that only supports one of them.

Through addition of a AAA Information Element, and unique sub-elements for each AAA protocol, it is possible to support transfer of context for multiple AAA protocols within the same message. Assigning only one Information Element for AAA ensures against exhaustion of the IAPP element space. Since the number of AAA attributes may be substantial, assignment of Information Elements to individual attributes is to be avoided.

Packaging each AAA protocol message within its own individual sub-element enables compatibility with the definition of correctness described earlier. Within IAPP, a device that receives Information Elements or sub-elements that it does not support will ignore those elements, and process those that it does support.

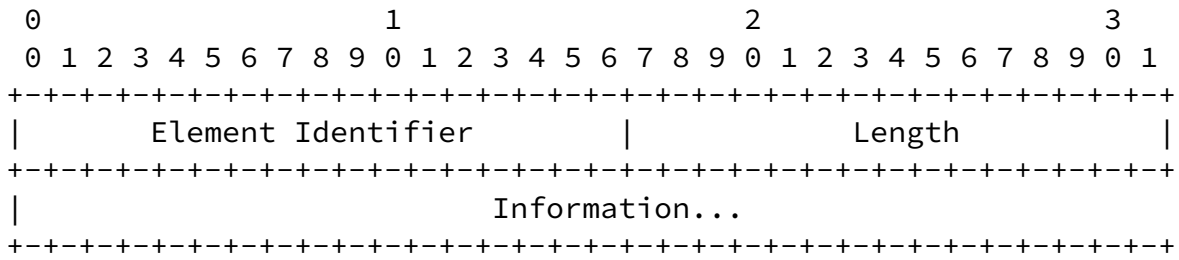
However, as described earlier, our model of context transfer requires that if a device supports a AAA protocol, that transferred AAA messages MUST be processed according to the rules of the protocol. For RADIUS, this implies that the context transfer MUST fail if known but unavailable services are requested, but that unknown attributes MAY be ignored. As a result, individual RADIUS attributes MUST NOT be encoded as Information Elements or sub-elements within IAPP. Rather, RADIUS attribues are encoded as a unit within the RADIUS sub-element. This enables the correct processing to occur. While a device may ignore an entire Information Element or sub-element, once the Information Element or sub-element is recognized it must be processed in its entirety.

Among other things, this approach enables the context transfer operation

to be independent of the supported AAA protocol. For example, a device supporting both Diameter and RADIUS could include sub-elements for both protocols. This would enable transfer of context to a new device supporting either protocol.

2.3. Information Element format

Within IAPP, Information Elements have the following structure:



Element Identifier

The Element Identifier field is two octets. It identifies the enclosed Information Element.

TBD - Element Identifier for AAA

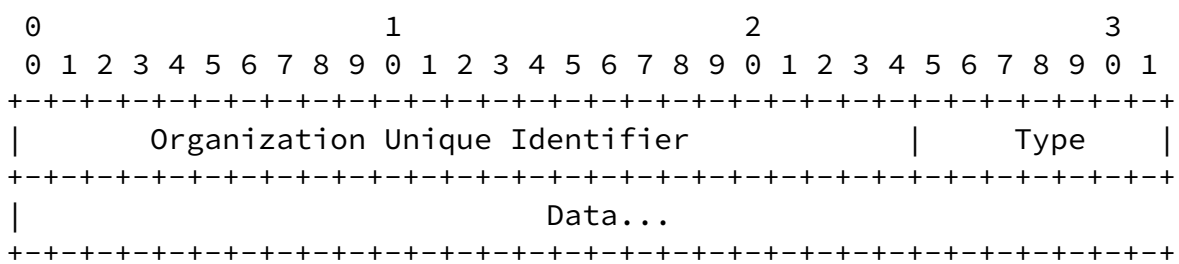
Length

The Length field is two octets. It encodes the length of the Information Element, including the Element Identifier, Length and Information fields.

Information

The Information field is variable length. It encodes the Information Element.

AAA sub-elements are encoded within the Information field as follows:



Organization Unique Identifier (OUI)

The OUI is a three octet field, encoding the Organization Unique Identifier. An OUI of zero is used for standardized sub-elements. Non-zero OUIs can be used to support vendor-specific sub-elements.

Type

The type field is one octet, and represents the AAA protocol type:

1 = RADIUS
2 = Diameter

Data

The Data field is of variable length, and contains the context to be transferred. For RADIUS this consists of a list of attributes.

2.4. Usage guidelines for the RADIUS sub-element

RADIUS context is established solely by Access-Accept messages, and therefore the bulk of RADIUS attributes within the RADIUS sub-element are those that may be included within an Access-Accept.

There are three classes of exception:

[1] Authentication attributes not relevant to IEEE 802 or to IEEE 802.1X context transfer.

[2] Accounting attributes such as the Acct-Authentic and Acct-Multi-SessionId accounting attributes.

[3] Attributes included within an Access Request that provide additional information relating to the previous session on the old AP. This includes NAS-IP-Address, NAS-IPv6-Address, NAS-Port,NAS-Identifier, Called-Station-Id, Calling-Station-Id, and NAS-Port-Id.

The attributes allowable for use with transfers of IEEE 802.1X context are described in Appendix A.

As noted in [Congdon], some attributes are not relevant to IEEE 802, while others that are relevant are not useful for context transfer. For example, where an IAPP protocol provides support for integrity protection, transfer of an additional integrity check (Message-Authenticator attribute) is not necessary. Similarly, since the IEEE 802.1X backend state machine is driven purely by the authentication outcome, not by the contents of the EAP-Message attribute, transferring this attribute is not necessary.

Acct-Authentic encodes the authentication technique utilized on the old access point: RADIUS, Local or Remote. A value of RADIUS denotes authentication against a backend RADIUS server; Local means that the user authenticated against the local database on the old device; Remote means that a AAA protocol other than RADIUS was used.

Typically, it does not make sense to transfer context of sessions established by local authentication. This violates the Equivalency Principle because context established via local authentication will not in general be the same as the context that would be established by carrying out a conversation with the AAA server. In order to guard against inappropriate context transfers, the new device MUST examine the authentication status prior to deciding to accept the context transfer.

Acct-Multi-SessionId enables linkage of accounting records from related sessions. As described in [Congdon], it is possible to maintain the same Acct-Multi-SessionId as a user moves between devices. To enable this, it is necessary to include the Acct-Multi-SessionId in the context transfer.

3. Security considerations

3.1. Trust issues

Implicit within our context transfer model is trust between devices engaging in a context transfer. Since the new device will act on the context transfer as though it had been given the service instructions by a trusted AAA server, it is necessary for the new device to trust the old device, at least sufficiently to allow transfer of AAA context.

In transfer of context across administrative domains, such a level of trust may not be possible or appropriate. Therefore it is possible for context transfer to fail even in situations where the devices are homogeneous, due to lack of trust between administrative domains.

Note however, that even where the required trust exists, it SHOULD NOT extend to enabling the new Access Point to obtain the keys used for encrypting traffic on the old Access Point. This would enable a rogue new Access Point to decrypt traffic previously captured on the old

Access Point. A variety of mechanisms can be used to prevent this and a specific mechanism is not mandated in this specification. For example, it is possible for the old Access Point to transfer to the new Access Point a "transfer key" derived via a one-way function from the old key, so that the old key cannot be easily obtained from the "transfer key". Alternatively, where perfect forward secrecy (PFS) is desired, a new key can be derived that does not depend on the old key.

Another implication of the "Equivalency Principle" is that the context transfer protocol SHOULD provide the same level of security as the AAA protocol whose context is being transferred. For example, AAA protocol messages may include attributes requiring confidentiality. This includes user passwords, encryption keys, or tunnel passwords. In order to transfer these attributes securely, confidentiality is required. Similarly, where the AAA protocol is using IPsec [RFC2401] to provide confidentiality, it does not make sense for the context transfer protocol to use a less secure mechanism, such as the shared secret-based hiding described in [RFC2865].

4. IANA Considerations

This specification does not create any RADIUS attributes nor any new number spaces for IANA administration.

5. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

[RFC2401] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2548] Zorn, G., "Microsoft Vendor-specific RADIUS attributes", RFC 2548, March 1999.

[RFC2865] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2867] Zorn, G., Mitton, D., Aboba, B., "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., Goyret, I., "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC2869] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, June 2000.

[RFC3162] Aboba, B., Zorn, G., Mitton, D.,"RADIUS and IPv6", RFC 3162, August 2001.

[Congdon] Congdon, P., Et al. "IEEE 802.1X Usage Guidelines", Internet draft (work in progress), draft-congdon-radius-8021x-17.txt, November 2001.

[IEEE802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[IEEE8021Q] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q/D8, January 1998.

[IEEE8021X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

[IEEE8023] ISO/IEC 8802-3 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, (also ANSI/IEEE Std 802.3- 1996), 1996.

[IEEE80211]

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, IEEE Std. 802.11-1997, 1997.

Appendix A - Table of Attributes

The following table provides a guide to which attributes are sent and received as part of IEEE 802.1X authentication, and which attributes are considered part of the "context" to be transferred during roaming. L3 denotes attributes that will be understood only by switches or access points implementing Layer 3 capabilities.

802.1X	Context	#	Attribute
X	X	1	User-Name [RFC2865]
		2	User-Password [RFC2865]
		3	CHAP-Password [RFC2865]
X	R	4	NAS-IP-Address [RFC2865]
X	R	5	NAS-Port [RFC2865]
X	X	6	Service-Type [RFC2865]
		7	Framed-Protocol [RFC2865]
		8	Framed-IP-Address [RFC2865]

		9	Framed-IP-Netmask [RFC2865]
L3	X	10	Framed-Routing [RFC2865]
X	X	11	Filter-Id [RFC2865]
X	X	12	Framed-MTU [RFC2865]
		13	Framed-Compression [RFC2865]
L3	X	14	Login-IP-Host [RFC2865]
L3	X	15	Login-Service [RFC2865]
L3	X	16	Login-TCP-Port [RFC2865]
X	X	18	Reply-Message [RFC2865]
		19	Callback-Number [RFC2865]
		20	Callback-Id [RFC2865]
L3	X	22	Framed-Route [RFC2865]
L3	X	23	Framed-IPX-Network [RFC2865]
X	X	24	State [RFC2865]
X	X	25	Class [RFC2865]
X	X	26	Vendor-Specific [RFC2865]
X	X	27	Session-Timeout [RFC2865]
X	X	28	Idle-Timeout [RFC2865]
X	X	29	Termination-Action [RFC2865]
X	R	30	Called-Station-Id [RFC2865]
X	R	31	Calling-Station-Id [RFC2865]
X	R	32	NAS-Identifier [RFC2865]
X		33	Proxy-State [RFC2865]
		34	Login-LAT-Service [RFC2865]
		35	Login-LAT-Node [RFC2865]
		36	Login-LAT-Group [RFC2865]

802.1X # Attribute

802.1X # Attribute

L3	X	37	Framed-AppleTalk-Link [RFC2865]
L3	X	38	Framed-AppleTalk-Network [RFC2865]
L3	X	39	Framed-AppleTalk-Zone [RFC2865]
X		40	Acct-Status-Type [RFC2866]
X		41	Acct-Delay-Time [RFC2866]
X		42	Acct-Input-Octets [RFC2866]
X		43	Acct-Output-Octets [RFC2866]
X		44	Acct-Session-Id [RFC2866]
X	X	45	Acct-Authentic [RFC2866]
X		46	Acct-Session-Time [RFC2866]

X		47	Acct-Input-Packets [RFC2866]
X		48	Acct-Output-Packets [RFC2866]
X		49	Acct-Terminate-Cause [RFC2866]
X	X	50	Acct-Multi-Session-Id [RFC2866]
		51	Acct-Link-Count [RFC2866]
X		52	Acct-Input-Gigawords [RFC2869]
X		53	Acct-Output-Gigawords [RFC2869]
X		55	Event-Timestamp [RFC2869]
		60	CHAP-Challenge [RFC2865]
X	X	61	NAS-Port-Type [RFC2865]
		62	Port-Limit [RFC2865]
		63	Login-LAT-Port [RFC2865]
X	X	64	Tunnel-Type [RFC2868]
X	X	65	Tunnel-Medium-Type [RFC2868]
L3	X	66	Tunnel-Client-Endpoint [RFC2868]
L3	X	67	Tunnel-Server-Endpoint [RFC2868]
L3	X	68	Acct-Tunnel-Connection [RFC2867]
L3	X	69	Tunnel-Password [RFC2868]
		70	ARAP-Password [RFC2869]
		71	ARAP-Features [RFC2869]
		72	ARAP-Zone-Access [RFC2869]
		73	ARAP-Security [RFC2869]
		74	ARAP-Security-Data [RFC2869]
		75	Password-Retry [RFC2869]
		76	Prompt [RFC2869]
X		77	Connect-Info [RFC2869]
X		78	Configuration-Token [RFC2869]
X		79	EAP-Message [RFC2869]
X		80	Message-Authenticator [RFC2869]
X	X	81	Tunnel-Private-Group-ID [RFC2868]
L3	X	82	Tunnel-Assignment-ID [RFC2868]
X	X	83	Tunnel-Preference [RFC2868]
		84	ARAP-Challenge-Response [RFC2869]

802.1X	#	Attribute

802.1X	#	Attribute
X		85 Acct-Interim-Interval [RFC2869]
X		86 Acct-Tunnel-Packets-Lost [RFC2867]
X	R	87 NAS-Port-Id [RFC2869]

802.1X	Context	#	Attribute
		88	Framed-Pool [RFC2869]
L3	X	90	Tunnel-Client-Auth-ID [RFC2868]
L3	X	91	Tunnel-Server-Auth-ID [RFC2868]
X	R	95	NAS-IPv6-Address [RFC3162]
		96	Framed-Interface-Id [RFC3162]
L3	X	97	Framed-IPv6-Prefix [RFC3162]
L3	X	98	Login-IPv6-Host [RFC3162]
L3	X	99	Framed-IPv6-Route [RFC3162]
L3	X	100	Framed-IPv6-Pool [RFC3162]

Key
===

802.1X = Allowed for use with IEEE 802.1X
Context = Transferred during roaming if available
L3 = implemented only on switches/access points with Layer 3 capabilities
R = Attributes acceptable for context transfer that are included only within an Access-Request

Acknowledgments

The authors would like to acknowledge Bob O'Hara of Informed Technology and Dave Bagby of 3Com for contributions to this document.

Authors' Addresses

Bernard Aboba
Tim Moore
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: {bernarda, timmoore}@microsoft.com
Phone: +1 425 882 8080
Fax: +1 425 936 7329

Intellectual Property Statement

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.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Expiration Date

This memo is filed as <draft-aboba-802-context-03.txt>, and expires November 22, 2002.