



产品名称Product name	密级Confidentiality level
CAMS	机密
产品版本Product version	Total 19pages 共19页
V100	

## Radius 协议介绍专题

(仅供内部使用)

拟制:

日期:

2003-09-06

审核:

日期:

2003-09-06

审核:

日期:

2003-09-06

批准:

日期:

2003-09-06



华为3Com技术有限公司

版权所有 侵权必究



## 修订记录

日期	修订版本	描述	作者

## 目 录

第 1 章 Radius 协议基本概念.....	3
1.1 Radius 协议应用介绍 .....	3
1.2 Radius 协议结构介绍 .....	3
第 2 章 CAMS 常用 Radius 协议属性 .....	3
2.1 标准 Radius 属性介绍.....	3
2.2 扩展 Radius 属性介绍.....	3
2.3 CAMS 进行 Radius 属性检查的方式 .....	3
2.4 附录.....	3

## 第1章 Radius 协议基本概念

### 1.1 Radius 协议应用介绍

RADIUS ( Remote Authentication Dial In User Service 远程认证拨号用户服务 )是一种在网络接入设备和认证服务器之间承载认证、授权、计费 and 配置信息的协议。RADIUS 协议是在认证、授权、计费方面应用最为广泛的协议之一，具有以下特点：

- 1、客户端/服务器结构；
- 2、采用共享密钥保证网络传输安全性；
- 3、良好的可扩展性；
- 4、认证机制灵活。

RADIUS 协议承载于 UDP 之上，官方指定端口号为：认证授权端口 1812、计费端口 1813。

RADIUS 协议在 RFC2865、RFC2866 中定义。

CAMS 和网络接入服务器之间的通讯采用 Radius。由于 Radius 的良好扩展性，不同的厂家对 Radius 作了扩展。我们公司也对其进行了扩展（华为 Radius+协议），不同公司扩展后的协议不完全兼容，在使用时应该注意不同厂家支持的协议的版本。CAMS 目前支持 Radius 标准协议和 华为 Radius+协议。

### 1.2 Radius 协议结构介绍

Radius 报文格式如下图所示，各域内容按照从左向右传送。



```
|
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Attributes ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

## 1. Code

Code 域长度为 1 个字节，用于标明 RADIUS 报文的类型，如果 Code 域中的内容是无效值，报文将被丢弃。

RADIUS Code 域的有效值如下：

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server (experimental)
- 13 Status-Client (experimental)
- 65 业务修改请求消息
- 66 业务修改请求回应消息
- 67 业务修改请求回应拒绝消息
- 255 Reserved

其中 12、13、255 为保留的 Code 值，一般不会遇到。1、2、3、4、5、11 比较常见，分别标明报文类型为“认证请求”、“认证接受”、“认证拒绝”、“计费请求”、“计费回应（计费成功）”和“访问质询”。

## 2. Identifier

“标识”域长度为 1 个字节，用于辅助匹配请求和回应报文。如果在短时间内，RADIUS 服务器收到从相同的源 IP、相同源端口收到的报文的标识域的内容也相同，则认为收到的是重复的请求。

Length

“长度”域占两个字节。用于指明报文的有效长度。多出长度域的字节被视为填充的字节，在接收时被忽略；如果报文长度小于长度域中的值，整个报文将被丢弃。长度域的范围在 20 和 4096 之间。

### 3. Authenticator

认证字域长 16 个字节，用于认证 Radius Client 和 Server 之间消息的有效性。

访问请求（Access- Request）认证字

在 Access-Request 包中，认证字的值是 16 字节随机数。认证字的值要不能被预测并且在一个共享密钥的生命期内唯一。

访问回应认证字

Access-Accept、 Access-Reject 和 Access-Challenge 包中的认证字称为访问回应认证字。访问回应认证字的值定义为：

$MD5(\text{Code} + \text{ID} + \text{Length} + \text{RequestAuth} + \text{Attributes} + \text{Secret})$

计费请求（Accounting-Request）认证字

在计费请求包中的认证字域称为计费请求认证字，它是一个 16 字节的 MD5 校验和。计费请求认证字的值定义为：

$MD5(\text{Code} + \text{Identifier} + \text{Length} + 16 \text{ zero octets} + \text{request attributes} + \text{shared secret})$

计费回应（Accounting-Response）认证字

在计费回应报文中的认证字域称为计费回应认证字。它的值定义为：

$MD5(\text{Accounting-Response Code} + \text{Identifier} + \text{Length} + \text{the Request Authenticator field from the Accounting-Request packet being replied to} + \text{the response attributes} + \text{shared secret})$

Attributes

属性

0	1	2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0		
+	+	+
	Type	
	Length	
	Value ...	
+	+	+

属性域的长度是可变的，它是一个由业务类型必需的属性和可选属性组成的属性链。一个属性包含如下三个部分：

#### 4. Type

类型域长度为一个字节。RADIUS 服务器和客户端当遇到不可识别的属性时，可以将其忽略。常用的属性类型请参见 RFC2865、RFC2866。

#### 5. Length

长度域长度为一个字节。指明了一个属性的类型、长度和值域的总长度。如果在认证请求报文中携带有属性长度非法的属性，则必须回应访问拒绝报文。如果在访问回应报文中存在非法的属性长度，这个报文必须被直接丢弃或被认为是访问拒绝报文。

#### 6. Value

值域由零或多个字节组成，包含详细的属性信息。它的格式由属性的长度和类型域决定。注意：RADIUS 中没有一个类型的值域是以 NULL(hex 00)结尾的，也就是说，值域中是没有结束符的。服务器和客户端需要能够处理内嵌的 NULL。

值域的数据类型是下列 5 种类型之一。“text”类型是“string”类型的子集。

text 1-253 字节长。

string 1-253 字节长。可以包含二进制数据。

address 4 字节，高位在前。

integer 4 字节无符号数，高位在前。

time 4 字节无符号数，高位在前，表示从 1970 年 1 月 1 日零点零时零秒到现在的秒数。

属性可以有多个实例，相同类型的属性实例的顺序不能被改变，不同属性类型的属性实例顺序可以改变。

标准属性具体说明请参考 RFC2865、RFC2866；

同时，各公司在标准属性基础上又扩展了自己的属性，比如我司的 RADIUS+。具体属性定义请参见相应的协议扩展。

## 第2章 CAMS 常用 Radius 协议属性

### 2.1 标准 Radius 属性介绍

Radius 报文所携带的属性以 (Type, Length, Value) 三元组的形式出现，其中，Type 表示该属性的属性号，占一个字节；Length 表示该属性的总长度 (Type、Length、Value 加在一起的长度)，占一个字节；Value 表示该属性的值，长度为 0-253。一个属性的值可以为下面四种类型中的一种：

String 类型， 0-253 个字节；

Address 类型， 4 字节；

Integer 类型， 4 字节；

Time 类型， 4 字节。

全部的属性定义参见附录。下面介绍几个常用的标准属性。

#### 1、User-Name

该属性指定了要进行认证的用户名。

Type	Length	Value
1	>3	String 类型，内容可以是简单的字符，也可以形如 abc@huawei.com 带网络域名。

#### 2、User-Password

该属性指定了要认证的用户的口令。用户口令加密后存放在该属性中。

Type	Length	Value
2	大于 17，并且小于 131	String 类型，加密后的口令存放在这里，长度至少为 16 个字节，至多为 128 个字节。

#### 3、NAS-IP-Address

该属性指明了发起认证请求的设备的 IP 地址。



Type	Length	Value
4	6	Address 类型，4 字节的 IP 地址。

#### 4、Vendor-Specific

该属性用于携带各厂商自己扩展的属性。

Type	Length	Value
26	>=7	各厂商自己扩展的属性。

各厂商自己扩展的属性按照如下的格式填写在 Value 域中。

Value 域的内容：

Vendor-Id	Vendor Type	Vendor Length	Vendor Value
4 字节，指明厂商 Id	1 字节，厂商自己扩展的属性号	1 字节，该扩展属性的长度	该扩展属性的值

每个厂商可以有多个扩展属性按照格式（Vendor Type，Vendor Length，Vendor Value）一起存放在 Vendor-Specific 属性的 Value 域中，但是 Value 域中的总长度不能超过 253 个字节；也可以以多个 Vendor-Specific 属性的形式出现在 Radius 报文中，每个 Vendor-Specific 属性的 Value 域携带一个或多个扩展属性。

#### 5、Session-Timeout

该属性指明允许用户使用的最大时长。

Type	Length	Value
27	6	Integer 类型，4 字节无符号整数，指明用户使用的最大秒数。

#### 6、Acct-Status-Type

该属性指明计费报文的类型。

Type	Length	Value
40	6	Integer 类型，4 字节无符号整数。

该属性出现在计费报文中，不同的取值标志出不同的意义：

- 1 ---表示计费开始报文

- 2 ---表示计费结束报文
- 3 ---表示计费更新报文
- 3 ---表示 Alive 报文
- 7 ---表示 Accounting-On 报文
- .....

## 2.2 扩展 Radius 属性介绍

随着业务的不断发展，大多数厂商都会对 Radius 属性进行扩展以满足自己的需要。华为公司为了统一宽带各产品的协议标准，也对 Radius 属性进行了扩展。

根据标准协议规定，各厂商自己扩展的属性用标准属性 Vendor-Specific（26 号属性）的 Value 域来携带，格式如下面的描述。

属性 Vendor-Specific 以（Type，Length，Value）的形式出现在 Radius 报文中，各厂商自己扩展的属性有两种方式填在上述的 Value 域中：

- （1） Radius 报文中只有一个 Vendor-Specific 属性，所有扩展属性都填在该属性的 Value 域中，扩展属性的格式如下：

Vendor-Id | Vendor Type 1 | Vendor Length 1 | Vendor Value 1 | Vendor Type 2 | Vendor Length 2 | Vendor Value 2 | ...

```

+++++-----+
| Vendor-Id | Vendor Type 1 | Vendor Length 1 | Vendor Value 1 |
+++++-----+
+++++-----+
| Vendor Type 2 | Vendor Length 2 | Vendor Value 2 | .....
+++++-----+

```

其中，Vendor-Id 为该厂商的唯一标志（华为公司为 2011），（Vendor Type n，Vendor Length n，Vendor Value n）表示扩展属性 n。但是，Value 域的总长度不能超过 253 字节。

- （2） Radius 报文中有多多个 Vendor-Specific 属性，每个属性的 Value 域中携带一个或多个扩展属性。格式同 1 所述。

```

+++++-----+

```

[illegible]

华为公司扩展的属性的完整定义参见附录。下面介绍几种常用的扩展属性。

### 1、Input-Peak-Rate

该属性表示用户接入到 NAS 的峰值速率。

Vendor Type	Vendor Length	Vendor Value
1	6	Integer 类型，4 字节无符号整数，单位为 bps。

## 2、 Output-Peak-Rate

该属性表示从 NAS 到用户的峰值速率。

Vendor Type	Vendor Length	Vendor Value
4	6	Integer 类型，4 字节无符号整数，单位为 bps。

### 3、 In\_Kb\_Before\_T\_Switch

该属性表示费率切换前接收的千字节数。

Vendor Type	Vendor Length	Vendor Value
7	6	Integer 类型，4 字节无符号整数，单位为 KB。

#### 4. Out Kb Before T Switch

该属性表示费率切换前发送的千字节数。

Vendor Type	Vendor Length	Vendor Value
8	6	Integer 类型，4 字节无符号整数，单位为 KB。

## 5、PortalURL

该属性表示强制用户进入的门户网站的 URL。

Vendor Type	Vendor Length	Vendor Value
27	最大为 255	String 类型，最长为 253 个字符。

## 2.3 CAMS 进行 Radius 属性检查的方式

CAMS 接收到 Radius 报文后，要对报文中携带的属性进行检查，并根据一定的策略对非法属性进行处理。

CAMS 把协议定义的标准属性和厂商自己扩展的属性分别定义成不同的字典文件，例如，定义标准属性的字典文件为 dictionary，定义华为扩展属性的字典文件为 dictionary.huawei。

字典文件定义了标准属性和扩展属性，同时对于多值的属性，也定义了其取值范围。

(1) 标准属性的字典文件 dictionary 的内容格式如下：

```

ATTRIBUTE  User-Name           1  string
ATTRIBUTE  Password            2  string
ATTRIBUTE  NAS-IP-Address      4  ipaddr
ATTRIBUTE  NAS-Port            5  integer
ATTRIBUTE  Framed-Routing      10 integer

.....

VALUE      Framed-Routing      None           0
VALUE      Framed-Routing      Broadcast       1
VALUE      Framed-Routing      Listen          2
VALUE      Framed-Routing      Broadcast-Listen 3

```

以 ATTRIBUTE 开头的行定义了一个属性，依次为属性名、属性号、值类型；  
以 VALUE 开头的行定义了某个属性的可能的取值和说明，依次为属性名、文字说明、取值。

(2) 扩展属性的字典文件的内容格式如下（以华为公司为例）：

```
VENDOR    HUAWEI    2011

ATTRIBUTE  hw_Input_Peak_Rate        1  integer  HUAWEI
ATTRIBUTE  hw_Input_Average_Rate     2  integer  HUAWEI
ATTRIBUTE  hw_Input_Basic_Rate       3  integer  HUAWEI
```

以 Vendor 开头的行指明了厂商名和厂商 Id，依次为厂商名、厂商 Id；

以 ATTRIBUTE 开头的行定义了该厂商的一个扩展属性，依次为扩展属性名、属性号、值类型、厂商。

CAMS 在收到 Radius 报文后，就是根据字典文件的定义进行属性检查的。

(1) 如果某个属性不是 Vendor-Specific（26 号属性），那么就用定义标准属性的字典文件 dictionary 来检查其合法性。

属性检查方式：

- a) 属性不完整，如果某个属性的 Length 域缺少，或 Length 域指明带有 Value 域但 Value 域缺少，或两者都缺少，则报此错误；
  - b) 属性号不存在，如果在字典文件中找不到某个属性，则报此错误。
- (2) 如果某个属性是 Vendor-Specific(26 号属性)，则知道该属性的 Value 域携带有某个厂商自己定义的扩展属性，于是先解析出 Value 中携带的厂商信息 Vendor-Id，然后用该厂商的字典文件 dictionary.Vendor 来解析 Value 域中携带的扩展属性，例如 dictionary.huawei。属性的合法性检查同 1。

如果把 CAMS 的日志级别设为调试级别，则可以通过日志来察看 CAMS 对 Radius 报文检查的具体信息。

## 2.4 附录

表2-1 Radius 协议标准属性列表

Attribute	Type	Length	类型	说明
User-Name	1	>=3	String	用户名
User-Password	2	18~130	String	用户密码
CHAP-Password	3	19	String	CHAP 认证密码
NAS-IP-Address	4	6	Address	NAS 的 IP 地址
NAS-Port	5	6	Integer	NAS 的端口号
Service-Type	6	6	Integer	服务类型
Framed-Protocol	7	6	Integer	用户接入协议
Framed-IP-Address	8	6	Address	用户 IP 地址
Framed-IP-Netmask	9	6	Address	用户 IP 掩码
Framed-Routing	10	6	Integer	用户路由
Filter-Id	11	>=3	String	过滤列表名称
Framed-MTU	12	6	Integer	用户最大传输单元
Framed-Compression	13	6	Integer	压缩协议
Login-IP-Host	14	6	Address	登陆主机地址
Login-Service	15	6	Integer	登陆的服务类型
Login-TCP-Port	16	6	Integer	登陆使用的 TCP 端口
Reply-Message	18	>=3	String	回应消息
Callback-Number	19	>=3	String	回呼号码
Callback-Id	20	>=3	String	回呼 ID
Framed-Route	22	>=3	String	用户路由信息
Framed-IPX-Network	23	6	Integer	IPX 网络号码
State	24	>=3	String	
Class	25	>=3	String	
Vendor-Specific	26	>=7	String	携带厂商扩展属性
Session-Timeout	27	6	Integer	服务的最大使用时长

Attribute	Type	Length	类型	说明
Idle-Timeout	28	6	Integer	连接空闲时长
Termination-Action	29	6	Integer	服务结束时 NAS 采取的动作
Called-Station-Id	30	>=3	String	被叫号码
Calling-Station-Id	31	>=3	String	主叫号码
NAS-Identifier	32	>=3	String	设备 ID
Proxy-State	33	>=3	String	代理服务器状态
Login-LAT-Service	34	>=3	String	
Login-LAT-Node	35	>=3	String	
Login-LAT-Group	36	34	String	
Framed-AppleTalk-Link	37	6	Integer	
Framed-AppleTalk-Network	38	6	Integer	
Framed-AppleTalk-Zone	39	>=3	String	
Acct-Status-Type	40	6	Integer	计费状态类型
Acct-Delay-Time	41	6	Integer	计费延时
Acct-Input-Octets	42	6	Integer	流入字节数
Acct-Output-Octets	43	6	Integer	流出字节数
Acct-Session-Id	44	>=3	String	计费 ID
Acct-Authentic	45	6	Integer	计费认证方式
Acct-Session-Time	46	6	Integer	用户使用服务的时长
Acct-Input-Packets	47	6	Integer	流入的包数
Acct-Output-Packets	48	6	Integer	流出的包数
Acct-Terminate-Cause	49	6	Integer	回话结束原因
Acct-Multi-Session-Id	50	>=3	String	连接多个相关会话的计费 ID
Acct-Link-Count	51	6	Integer	链接数
CHAP-Challenge	60	>=7	String	发给 CHAP 认证用户的 Challenge
NAS-Port-Type	61	6	Integer	设备的端口类型
Port-Limit	62	6	Integer	设备可以提供给用户使用的端口数

Attribute	Type	Length	类型	说明
Login-LAT-Port	63	>=3	string	
Tunnel-Type	64	6	Integer	隧道类型
Tunnel-Medium-Type	65	6	Integer	隧道介质类型
Tunnel-Client-Endpoint	66	6	Integer	隧道客户端
Tunnel-Server-Endpoint	67	6	Integer	隧道服务端
Acct-Tunnel-Connection	68	6	Integer	
Tunnel-Password	69	6	Integer	隧道密码
EAP-Message	79	>=3	String	
Tunnel-Private-Group-id	81	6	Integer	
Tunnel-Assignment-id	82	6	Integer	
Tunnel-Preference	83	6	Integer	
Acct-Interim-Interval	85	6	Integer	
Acct-Tunnel-Packets-Lost	86	6	Integer	
NAS-Port-Id	87	6	String	
Framed-Pool	88	6	String	
Tunnel-Client-Auth-id	90	6	Integer	
Tunnel-Server-Auth-id	91	6	Integer	

表2-2 Radius 协议华为扩展属性列表

Attribute	Type	Length	类型	说明
Input-Peak-Rate	1	6	Integer	用户接入到 NAS 的峰值速率
Input-Average-Rate	2	6	Integer	用户接入到 NAS 的平均速率
Input-Basic-Rate	3	6	Integer	用户接入到 NAS 的基本速率
Output-Peak-Rate	4	6	Integer	从 NAS 到用户的峰值速率
Output-Average-Rate	5	6	Integer	从 NAS 到用户的平均速率
Output-Basic-Rate	6	6	Integer	从 NAS 到用户的基本速率
In_Kb_Before_T_Switch	7	6	Integer	费率切换前接收的千字节数
Out_Kb_Before_T_Switch	8	6	Integer	费率切换前发送的千字节数



Attribute	Type	Length	类型	说明
In_Pkt_Before_T_Switch	9	6	Integer	费率切换前接收的包的个数
Out_Pkt_Before_T_Switch	10	6	Integer	费率切换前发送的包的个数
In_Kb_After_T_Switch	11	6	Integer	费率切换后接收的千字节数
Out_Kb_After_T_Switch	12	6	Integer	费率切换后发送的千字节数
In_Pkt_After_T_Switch	13	6	Integer	费率切换后接收的包的总个数
Out_Pkt_After_T_Switch	14	6	Integer	费率切换后发送的包的总个数
Remanent_Volume	15	6	Integer	该连接的剩余可用总流量
Tariff_Switch_Interval	16	6	Integer	最近的费率切换时刻与当前时刻的时间间隔
ISP-ID	17	>=3	String	
Max-Users-Per-Logic-Port	19	6	Integer	一个逻辑端口的最大用户数
Command	20	6	Integer	
Priority	22	6	Integer	服务的优先级
Control_Identifier	24	6	Integer	区分是否重复报文
Result_Code	25	6	Integer	表示 Trigger-Request或 SetPolicy的结果
Connect_ID	26	6	Integer	用户连接索引
PortalURL	27	>=3	String	强制用户进入门户网站的门户网站 URL
Ftp-Directory	28	3~64	String	FTP 用户工作目录
Exec-Privilege	29	6	Integer	EXEC 用户优先级
Group-IP-Address	30	6	Integer	
Group-IP-Mask	31	6	Integer	
Acct-Destination-IP-Addr	39	>=3	String	免费目的 IP 地址类别
Acct-Destination-Volume	40	>=3	String	收费目的 IP 地址类别
NAS-Startup-Timestamp	59	6	Integer	NAS 系统启动时刻
Ip-Host-Addr	60	25~33	String	NAS 在认证和计费请求报文中携带用户 IP 地址和 MAC 地址
Multicast_Source_Group	97	>=36	String	用户作为组播源加入的组播组地址和

Attribute	Type	Length	类型	说明
				组播 CAR 属性
Multicast_Recieve_Group	98	6	Integer	用户作为组播接收者加入的组播组地址
User_Multicast_Type IGMP-Flag IGMP-Session-Time	99	6	Integer	单播/组播权限
HW_Service_Chg_Cmd	105	6	Integer	增值业务使用
HW_Acct_Packet_Type	106	6	Integer	标识计费包的性质
HW_Call_Reference	107	6	Integer	呼叫参考，从摘机到挂机的全过程中唯一
HW_PSTN_Port	108	6	Integer	PSTN 端口
HW_Voip_Service_Type	109	6	Integer	VoIP 服务类型
HW_Acct_Connection_Time	110	6	Integer	中继链路占用时长
HW_Error_Reason	112	6	Integer	错误原因
HW_Remain_Monney	113	6	Integer	剩余钱，以“分”为单位
HW_Org_GK_Address	123	6	Address	源 GK 地址
HW_Org_GW_Address	124	6	Address	源 GW 地址
HW_Dst_GK_Address	125	6	Address	目的 GK 地址
HW_Dst_GW_Address	126	6	Address	目的 GW 地址
HW_Access_Num	127	>=3	String	接入码
HW_Remain_Time	128	6	Integer	剩余时间，以“秒”为单位
HW_Codec_Type	131	6	Integer	语音编码方式
HW_Transfer_Num	132	>=3	String	指示网关实际需要接通的被叫号码
HW_New_User_Name	133	>=3	String	转帐业务中表示目的卡号
HW_Transfer_Station_Id	134	>=3	String	ONLY 系统使用：呼转后的真实被叫号码
Client-Primary-DNS	135	6	Address	第一 DNS 服务器地址
Client-Secondary-DNS	136	6	Address	第二 DNS 服务器地址



Attribute	Type	Length	类型	说明
HW_ONLY_Account_Type	137	6	Integer	ONLY 系统业务计费类型
Version	254	>=3	String	宽带产品的版本号
Product-ID	255	>=3	String	宽带产品名称