**Q/DKBA**

**华为技术有限公司企业技术标准**

Q/DKBAXXXX-2001

**华为公司宽带产品Portal协议标准**

**第2部分：Portal标准V2.0**

**2001-XX-XX发布 2001-XX-XX实施**

**华 为 技 术 有 限 公 司**发布

目 次

|  |  |
| --- | --- |
| 1 范围 | 4 |
| 2 术语和定义 | 4 |
| 3 概述 | 4 |
| 4协议 | 4 |
| 4.1报文格式 | 4 |
| 4.2报文字段说明 | 4 |
| 4.2.1Ver | 5 |
| 4.2.2Type | 5 |
| 4.2.3Pap/Chap | 5 |
| 4.2.4Rsv | 6 |
| 4.2.5SerialNo | 6 |
| 4.2.6ReqID | 6 |
| 4.2.7UserIP | 6 |
| 4.2.8UserPort | 6 |
| 4.2.9ErrCode | 6 |
| 4.2.10AttrNum | 6 |
| 4.2.11 Authenticator | 6 |
| 4.2.12报文属性字段（Attr）的格式 | 7 |
| 5流程和相关说明 | 9 |
| 5.1信息询问流程（无论成功还是失败） | 9 |
| 5.2下线通知流程（BAS通知Portal Server） | 10 |
| 6其他说明 | 11 |
| 6.1关于TextInfo属性的使用 | 11 |
| 6.2协议的兼容性 | 11 |
| 6.3协议的不完善之处 | 11 |

**前 言**

本标准由宽带联合系统部提出。

本标准主要起草部门：宽带联合系统部，MA5200产品组，ESR产品组，iNet产品组

本标准主要解释部门：宽带总体组

本标准主要起草人：杨宏杰、周和秘、乔明

本标准主要审核人：卢朝晖、胡鹏

本标准批准人：

华为公司宽带产品Portal协议标准V2.0

# 范围

本标准规定了华为公司宽带产品所采用的Portal协议标准。

本标准适用于华为公司具备Portal特性的宽带设备，包括服务器端设备（如：iTellin、iNet IP Hotel系统等）以及BAS端设备（如：ESR、MA5200等）

特别的：对于服务器端设备（如：iTellin、iNet IP Hotel系统等）必须同时支持V1.0与V2.0协议，对于BAS端设备（如：ESR、MA5200等）以V2.0为标准。

# 术语和定义

Portal —— 门户业务

Web认证 —— 通过Web方式进行用户认证

认证Client —— 本文中使用的概念，表示协议中发起认证请求的一方，可以为Portal Server或 任何发起认证的客户机。在不会引起混淆的情况下，简称为Client

认证Server —— 本文中使用的概念，表示协议中接受认证请求的一方，例如BAS设备。 在不 会引起混淆的情况下，简称为Server

BAS ——Broad Access Server 宽带接入设备

# 概述

本文档主要分两部分，一部分描述了PortalServer和BAS设备之间的通信协议，令一部分（附录）提出了对PortalServer 的Web服务器相关配置和网页设计的一些规定。

PortalServer和BAS设备之间的协议规定了采用Portal认证（或Web认证）时PortalServer和BAS设备之间的报文格式和通信流程，协议支持PAP和CHAP两种认证方式，对可能出现的各种情况的认证流程分别做了详细的规定。

Portal V2.0协议是对原有V1.0协议存在的漏洞和不合理之处进行部分完善，增加了用于对协议报文进行验证的字段Authenticator。

对于V1.0与V2.0相互冲突之处，一律以V2.0为准。

# 协议

## 报文格式

协议包采用固定长度头加可变长度的属性字段组成，属性字段采用TLV格式。为了增加对协议报文的校验，扩充报文格式如下（图 4-1）：



图4-1 增加报文校验之后的Portal协议报文格式

## 报文字段说明

### Ver

Ver字段是协议的版本号，长度为 1 字节，Ver = 0x02。之所以对Version进行升级，是因为对Version 1做了如下的扩充：

1. 修改了报文格式，在AttrNum字段之后增加了16个字节的Authenticator字段。
2. 增加对所有协议报文的校验，包括上线流程、下线流程和查询流程。
3. 修改了TextInfo属性，使其完全符合TLV格式（version 1曾经出现过不完全符合TLV格式的软件实现版本），不再区分其内容的语言，并且约定：BAS本地产生的提示信息不上报到Portal Server。

### Type

Type字段定义报文的类型，长度为 1 字节。该版本兼容原协议的全部命令字，同时新增类型为0x08，0x09，0x0a三个命令字：

| Type | 值 | 方向 | 含义 |
| --- | --- | --- | --- |
| REQ\_CHALLENGE | 0x01 | Client --> Server | Portal Server向BAS发送的Challenge请求报文 |
| ACK\_CHALLENGE | 0x02 | Server --> Client | BAS对Portal Server请求Challenge报文的响应报文 |
| REQ\_AUTH | 0x03 | Client --> Server | Portal Server向BAS发送的认证请求报文 |
| ACK\_AUTH | 0x04 | Server --> Client | BAS对Portal Server认证请求的响应报文 |
| REQ\_LOGOUT | 0x05 | Client --> Server | Portal Server向BAS发送的下线请求报文 |
| ACK\_LOGOUT | 0x06 | Server --> Client | BAS对Portal Server下线请求的响应报文 |
| AFF\_ACK\_AUTH | 0x07 | Client --> Server | Portal Server向BAS发送的 |
| NTF\_LOGOUT | 0x08 | Server --> Client | 用户被强制下线通知报文 |
| REQ\_INFO | 0x09 | Client --> Server | 信息询问报文 |
| ACK\_INFO | 0x0a | Server --> Client | 信息询问的应答报文 |

1. 协议支持的命令字

### Pap/Chap

与原协议一致。

Pap/Chap字段定义此用户的认证方式，长度为 1 字节，只对Type值为 0x03 的认证请求报文有意义：

Chap方式认证－－－值为0x00；

Pap 方式认证－－－值为0x01；

 把Pap/Chap放在协议报文的目前位置，使得整个报文不太协调。但是考虑到现实的原因，目前不对该字段进行任何更改。

### Rsv

与原协议一致。

Rsv目前为保留字段，长度为 1 字节，在所有报文中值为 0；

### SerialNo

与原协议一致。

(1)、SerialNo字段为报文的序列号，长度为 2 字节，由PortalServer随机生成，Portal Server必须尽量保证不同认证流程的SerialNo在一定时间内不得重复，在同一个认证流程中所有报文的SerialNo相同；

(2)、PortalServer发给BAS设备的报文

a、由Portal Server发出的Type值为1、3的请求报文其SerialNo都是随机生成数；

b、由PortalServer向BAS设备发出的Type值为5的报文其SerialNo值分两中情况：当ErrCode为0时，SerialNo值为一个随机生成数；当ErrCode为1时，SerialNo值可能和Type值为1或3的报文相同，具体要看是请求Challenge超时还是请求认证超时；

c、由PortalServer向BAS设备发出的认证成功确认报文（Type值为7的报文）SerialNo和其发出的相应请求报文的SerrialNo相同；比如对于Type值为7的报文其SerialNo值和Type值为3的请求认证报文相同；

(3)、每一个由BAS设备发给PortalServer的响应报文的SerialNo必须和Portal Server发送的相应请求报文的SerialNo一样，否则PortalServer会丢掉从BAS设备发来的响应报文； 比如Type值为2的报文其SerialNo值必须和Type值为1的报文相同，Type值为4的报文其SerialNo值必须和Type值为3的报文相同，Type值为6的报文其SerialNo值必须和Type值为5的报文相同。

### ReqID

与原协议一致。

(1)、ReqID字段长度为 2 个字节，由BAS设备随机生成，尽量使得在一定时间内ReqID不重复。

(2)、在Chap认证方式中：

a、BAS设备在Type为2的请求Challenge响应报文中把该ReqID的值告诉PortalServer；

b、在Type值为3、4、7的报文中ReqID字段的值都和Type值为2的报文中此字段的值相同；

c、在Type值为 5 的报文中，若报文表示请求Challenge超时则此字段值为0 ；若报文表示请求认证超时则此字段值和Type值为2的报文中此字段的值相同；

(3)、在Pap认证方式中，此字段无意义，其值为0；

(4)、在Type值为 5 的报文中，若报文表示请求下线时则此字段值为0 ；

(5)、在Type值为1、6的报文中，该字段均无意义，值都为0；

### UserIP

与原协议一致。

UserIP字段为Portal用户的IP地址，长度为 4 字节，其值由PortalServer根据其获得的IP地址填写，在所有的报文中此字段都要有具体的值；

### UserPort

与原协议一致。

UserPort字段目前没有用到，长度为 2 字节，在所有报文中其值为0；

### ErrCode

ErrCode字段和Type字段一起表示一定的意义，长度为 1字节。

对原协议支持的Type，ErrCode与原协议一致。具体如下：

(1)、对于Type值为1、3、7的报文，ErrCode字段无意义，其值为0；

(2)、当Type值为 2 时：

ErrCode＝0，表示BAS设备告诉PortalServer请求Challenge成功；

ErrCode＝1，表示BAS设备告诉PortalServer请求Challenge被拒绝；

ErrCode＝2，表示BAS设备告诉PortalServer此链接已建立；

ErrCode＝3，表示BAS设备告诉PortalServer有一个用户正在认证过程中，请稍后再试；

ErrCode＝4，则表示BAS设备告诉PortalServer此用户请求Challenge失败（发生错误）；

(3)、当Type值为 4 时：

ErrCode＝0，表示BAS设备告诉PortalServer此用户认证成功；

ErrCode＝1，表示BAS设备告诉PortalServer此用户认证请求被拒绝；

ErrCode＝2，表示BAS设备告诉PortalServer此链接已建立；

ErrCode＝3，表示BAS设备告诉PortalServer有一个用户正在认证过程中，请稍后再试；

ErrCode＝4 ，表示BAS设备告诉PortalServer此用户认证失败（发生错误）；

(4)、当Type值为 5 时：

ErrCode＝0，表示此报文是PortalServer发给BAS设备的请求下线报文；

ErrCode＝1，表示此报文是在PortalServer没有收到BAS设备发来的对各种请求的响应报文，而定时器时间到（即超时）时由PortalServer发给BAS设备的报文；

(5)、当Type值为 6 时：

ErrCode＝0，表示BAS设备告诉PortalServer此用户下线成功；

ErrCode＝1，表示BAS设备告诉PortalServer此用户下线被拒绝；

ErrCode＝2, 表示BAS设备告诉PortalServer此用户下线失败（发生错误）；

对新增命令报文的ErrCode说明如下：

 对Type为REQ\_INFO时，ErrCode无意义，其值为0；

 对Type为NTF\_LOGOUT时，ErrCode含义如下：

| ErrCode | 含义 |
| --- | --- |
| 0 | 下线 |

 对Type为ACK\_INFO时，ErrCode含义如下：

| ErrCode | 含义 |
| --- | --- |
| 0 | 处理成功，但不表示全部消息都被获取了，有多少信息被获得应通过属性来判断，详见下文 |
| 1 | 功能不支持，表示设备不支持这一功能 |
| 2 | 消息处理失败，由于某种不可知原因，使处理失败，例如询问消息格式错误等。 |

### AttrNum

与原协议一致。

AttrNum字段表示其后边可变长度的属性字段属性的个数，长度为 1 字节（表示属性字段最多可有255个属性），其值在所有的报文中都要根据具体情况赋值；

### Authenticator

新增字段。

验证字的长度固定为16字节，网络字节顺序。其内容的计算在请求报文和响应报文中略有区别，并且在验证字的计算时，将类型为7（AFF\_ACK\_AUTH）和类型为8（NTF\_LOGOUT）的报文当作请求报文，尽管这两种报文不是严格意义上的请求报文（严格的说，AFF\_ACK\_AUTH更像是响应报文）。验证字的计算是通过MD5算法实现的，其中报文的各个字段以及BAS和Portal Server之间的共享密钥secret都参与了计算。以下分别介绍请求报文的验证字和响应报文的验证字。

1. 请求报文的验证字（Request Authenticator）：

以字节流Ver + Type + PAP/CHAP + Rsvd + SerialNo + ReqID + UserIP + UserPort + ErrCode + AttrNum + 16个字节的0 + request attributes + secret作为MD5的输入，得到的MD5输出就是请求报文的验证字Request Authenticator的内容。

2. 响应报文的验证字（Response Authenticator）：

以字节流Ver + Type + PAP/CHAP + Rsvd + SerialNo + ReqID + UserIP + UserPort + ErrCode + AttrNum + 本响应报文对应的请求报文的16字节的Request Authenticator + response attributes + secret作为MD5的输入，得到的MD5输出就是响应报文的验证字Response Authenticator的内容。

为了完成校验功能，需要注意如下几点：

 在Server和Client两端需要配置相同的共享密钥Secret，否则无法通过接收方的校验；

 双方都使用RFC1321中描述的MD5加密算法；

 接收方为了校验所接收到报文的正确性，必须采用和发送方完全一样的计算过程。如果计算出来的验证字和接收到的报文中的验证字一致，则认为报文合法；否则任务报文错误，可以简单丢弃，但是建议对丢弃报文进行统计。

 请求验证字和响应验证字的计算参照了RADIUS计费报文的验证字的计算方法。

 目前支持的报文类型存在如下的请求和响应关系：

请求响应

REQ\_CHALLENGE <——> ACK\_CHALLENGE

REQ\_AUTH <——> ACK\_AUTH

REQ\_LOGOUT <——> ACK\_LOGOUT

REQ\_INFO <——> ACK\_INFO

NTF\_LOGOUT 无

AFF\_ACK\_AUTH 无

### 报文属性字段（Attr）的格式

Attr字段（属性字段）是一个可变长字段，由多个属性依次链接而成，每个属性的格式为TLV格式，具体如下（图4-2）：



图 4-2 报文属性字段格式

报文属性字段说明如下：

(1)、属性类型(AttrType)

表 4-2 属 性字 段 的定义

|  |  |  |  |
| --- | --- | --- | --- |
| Attr(属性字段) | AttrType | AttrValue自身的长度（属性值长 度） | 属性含义 |
| UserName | 0x01 | <=32 （可变） | 用 户 名，具体为：  “用户名”＋“@”+“域名” |
| PassWord | 0x02 | <=16（可变） | 用户提交的明文密 码 |
| Challenge | 0x03 | 16（固定） | Chap方式加密的魔 术 字 |
| ChapPassWord | 0x04 | 16（固定） | 经过Chap方式加密后的密码 |

(2)、属性长度(AttrLen)

AttrLen字段表示属性的长度，长度为1字节，其值是整个属性三个字段AttrType、AttrLen、AttrValue的长度之和：也就是AttrValue的长度加上2；

(3)、属性值(AttrValue)

AttrValue的值为具体的属性值，比如用户名、口令等，长度有些可变，有些固定（具体见表4-2），但最长不能超过253(255-2)字节；

 支持原协议中的全部属性字，并且对部分属性说明如下：

1. TextInfo

格式为：类型+长度+内容

类型为5，长度大于等于3，小于等于255，该属性用于将RADIUS等第三方鉴权设备的提示信息透传到Portal Server。该属性所携带的内容为字符串，但是不包括字符串结束符‘\0’。该属性在同一个报文中允许多个，建议只携带1个该属性。该属性可以存在于从BAS到Portal Server的任何报文中。

2. UpLinkFlux(暂不支持)

格式为：类型+长度（在REQ\_INFO报文中）或者类型+长度+内容（在ACK\_INFO报文）

类型为6，长度为2或者10：在REQ\_INFO报文中，长度为2；在ACK\_INFO报文中，长度为10。在ACK\_INFO报文中其内容是一个表示从该用户终端上行（输出）流量的8字节（64位）无符号整数（网络顺序），单位为kbytes。

3. DownLinkFlux(暂不支持)

格式为：类型+长度（在REQ\_INFO报文中）或者类型+长度+内容（在ACK\_INFO报文）

类型为7，长度为2或者10：在REQ\_INFO报文中，长度为2；在ACK\_INFO报文中，长度为10。在ACK\_INFO报文中，其内容是一个表示该用户终端下行（输入）流量的8字节（64位）无符号整数（网络顺序），单位为kbytes。

4. Port

格式为：类型+长度（在REQ\_INFO报文中）或者类型+长度+内容（在ACK\_INFO报文）

类型为8，长度可以大于等于2，小于等于37：

"主机名"+"-"+"2位槽号"+"1位子槽号"+“2位端口号”+("4位VPI"+"5位VCI")或

("4位外层VLAN"+"0"+"4位内层VLAN")

说明：只有一层VLAN时，外层VLAN填"0"。共35个字符。

| Attr（属性字段） | AttrType | AttrLen | 属性含义 |
| --- | --- | --- | --- |
| TextInfo | 0x05 | 大于等于3，小于等于255 | 本属性只能在BAS到Portal Server的报文中存在，同时，协议规定：BAS只是透传从RADIUS来的错误信息，属性的内容可以为任意字符串，不带'\0'结束符 |
| UpLinkFlux | 0x06 | 2或者10 | (暂不支持)本属性只能在REQ\_INFO和ACK\_INFO报文中存在。数量不能超过1。  当Type=REQ\_INFO时，长度为2。  当Type=ACK\_INFO时，长度为10，内容是一个表示该用户的流量的8字节无符号整数（网络顺序），单位为kbytes |
| DownLinkFlux | 0x07 | 2或者10 | (暂不支持)同上 |
| Port | 0x08 | 大于等于2，小于等于37 | 本属性只能在REQ\_INFO和ACK\_INFO报文中存在。数量不能超过1。  当Type=REQ\_INFO时，长度为2。"主机名"+"-"+"2位槽号"+"1位子槽号"+“2位端口号”+("4位VPI"+"5位VCI")或 ("4位外层VLAN"+"0"+"4位内层VLAN") 说明：只有一层VLAN时，外层VLAN填"0"  共35个字符 |

表 4-3新增属性的定义

# 流程和相关说明

Version 2的协议流程除了完全包含Version 1的协议流程之外，还增加了信息查询和BAS主动通知Portal Server下线的流程。旧版本协议的流程说明如下：

## Chap认证方式上线流程

### Chap认证流程（每一步都正确的情况下）（图 5-1）

### 

图 5-1 Chap方式认证正常流程

### Chap认证流程（请求Challenge失败或被拒绝的情况下）（图 5-2 ）

### 

图 5-2 Chap认证方式请求魔术字失败流程

### Chap认证流程（请求Challenge没有响应的情况下）（图 5-3）

### 

图 5-3 Chap认证方式，请求魔术字无响应流程

### Chap认证流程（认证结果为失败或被拒绝的情况下）（图 5-4）

### 

图 5-4 Chap认证方式，认证失败流程

### Chap认证流程（请求认证没有响应的情况下）（图5-5）

### 

图 5-5 Chap认证方式，请求认证无响应流程

## Pap认证方式上线流程

### Pap认证流程（每一步都正确的情况下）（图 5-6）

### 

图：5-6 Pap认证方式正常流程

### 

### Pap认证流程（认证失败或被拒绝的情况下）（图 5-7）

图 5-7 Pap 认证方式，认证失败流程

### Pap认证流程（请求认证没有响应的情况下）（图 5-8）



图 5-8 Pap认证方式，请求认证无响应流程

## 下线流程

（说明：下线流程不分Chap和Pap）

### 下线成功的流程（图 5-9）

### 

图 5-9 正常下线流程

### 下线失败或被拒绝的流程（图5-10）



图 5-10 下线失败流程

### 

### 下线没有响应流程（图 5-11）

图 5-11 下线报文无响应流程

 新增流程的说明如下：

## 信息询问流程（无论成功还是失败，参见图5-12）



图5-12 信息询问流程

根据协议，REQ\_INFO消息的定义如下：

|  |  |
| --- | --- |
| Ver | 1 |
| Type | REQ\_INFO |
| Pap/Chap | 无意义，填0 |
| Rsv | 无意义，填0 |
| SerialNo | 任意，建议使用一个能用于区分当前不同会话的一个数值。Server将在应答消息中使用相同的SerialNo |
| ReqID | 无意义，填0 |
| UserIP | 被询问的用户IP |
| UserPort | 无意义，填0 |
| ErrCode | 无意义，填0 |
| AttrNum | 根据实际情况填写 |
| Authenticator | 根据Request Authenticator的计算方法进行计算的结果 |
| <Attribution> | 这个消息可以带属性UpLinkFlux, DownLinkFlux, 和Port中的一个或多个，取决于Client需要询问何种信息。在发询问时，根据需要询问的内容，带一个长度为2的相应属性即可。 |

ACK\_INFO的消息的定义如下：

|  |  |
| --- | --- |
| Ver | 1 |
| Type | ACK\_INFO |
| Pap/Chap | 无意义，填0 |
| Rsv | 无意义，填0 |
| SerialNo | 与相应询问消息的SerialNo一致 |
| ReqID | 无意义，填0 |
| UserIP | 被询问的用户IP |
| UserPort | 无意义，填0 |
| ErrCode | 见上文的对ErrCode的定义 |
| AttrNum | 根据实际情况填写 |
| Authenticator | 根据Response Authenticator的计算方法进行计算的结果 |
| <Attribution> | 这个消息可以带属性UpLinkFlux, DownLinkFlux, 和Port中的一个或多个，取决于相应的REQ\_INFO消息带了哪些询问属性。如果某属性取不到，则不返回该属性。所以一个属性在本消息中存在的必要条件是：  i. 询问消息中存在  ii. 能被取得 |

## 下线通知流程（BAS通知Portal Server）

对于从Portal Server向BAS请求用户下线的流程此处不进行描述。用于Server首先检测到用户已经下线；或者BAS主动切断连接时，用来通知Portal Server（参见图5-13）：



图5-13 下线通知流程

通知消息固定向UDP端口50100发送。

NTF\_LOGOUT的定义如下：

|  |  |
| --- | --- |
| Ver | 1 |
| Type | NTF\_LOGOUT |
| Pap/Chap | 无意义，填0 |
| Rsv | 无意义，填0 |
| SerialNo | 无意义，填0 |
| ReqID | 无意义，填0 |
| UserIP | 被下线的用户IP |
| UserPort | 无意义，填0 |
| ErrCode | 见上文的对ErrCode的定义 |
| AttrNum | 根据实际情况填写 |
| Authenticator | 根据Request Authenticator的计算方法进行计算的结果 |
| <Attribution> | 无，或者Server设备需要通过文字信息描述下线原因，可以带一个或多个TextInfo属性 |

# 其他说明

## 关于TextInfo属性的使用

TextInfo用于传递文字信息。建议使用如下惯用法：

 正常情况下，任何消息都不带该属性。

 如果Server通过第三方设备实现鉴权，例如Radius Server，而该设备又包含文字信息，应使用该信息作为文字信息。

 BAS本身产生的错误信息不传送到Portal server。

 建议BAS能通过调试命令关闭/打开消息透传的功能。

## 协议的兼容性

显然，引入了报文验证字之后，版本Version 2与Version 1完全不兼容。如果严格按照扩充后的协议，旧版本的下线流程和查询流程报文将因为没有携带Authenticator字段而被认为是非法的报文。为了实现与旧版本的兼容，建议在实现新协议的软件中增加版本切换的控制开关：如果对端使用旧版本协议，则通过兼容开关确保能与之对接。

## 协议的不完善之处

尽管对每个报文都增加了校验，但是依然可能被BAS和Portal Server之外的第三者利用。本文不对此进行详细的描述。

## 协议其他说明

1、此协议规定承载报文的是UDP协议，也即报文为UDP报文，BAS设备在固定端口2000上等待接收PortalServer发来的各种请求报文和确认报文；

2、 在PortalServer端目前不采用超时重传和出错重传，对于PortalServer发出的各种请求报文，若在一定的时间内没有收到BAS设备发来的响应报文或着收到的响应报文出错，对于超时没有响应则PortalServer向BAS设备发送一个表示等待响应超时的报文，同时PortalServer认为相应的请求失败，直接告诉用户失败；

3、Chap认证的相关说明：

(1)、challenge的生成：challenge由BAS设备在收到请求Challenge报文的时候随机生成，长度为16个字节，跟随Challenge应答报文下发到Portal Server。

(2)、Chap\_Password的生成：Chap\_Password的生成遵循标准的Radious协议中的Chap\_Password 生成方法（参见RFC2865）。密码加密使用MD5算法，MD5函数的输入为

ChapID ＋ Password ＋Challenge

其中，ChapID取ReqID的低 8 位，Password的长度不够协议规定的最大长度，其后不需要补零。

4、无论采用Chap认证还是Pap认证，都允许用户口令为空；

5、当用户向PortalServer提交的连接请求里用户名为空时，PortalServer在向BAS设备发送认证请求时应用一个缺省的用户名代替（比如\*\*\*）；

6、认证流程中各种报文所带属性的个数（建议）：

(1)、请求Challenge 报文：0个属性；

(2)、对请求Challenge响应的报文：若请求Challenge成功则为1个属性—Challenge属性，若请求Challenge失败则属性个数为0个；

(3)、请求认证报文：2个属性，分别为用户名、PassWord 或ChapPassWord ；

(4)、对请求认证的响应报文：0个属性；

(5)、请求下线报文或表示超时的报文：0个属性；

(6)、对请求下线的响应报文：0个属性；

(7)、PortalServer对收到从BAS设备发来的认证成功报文的确认：0个属性；

7、报文的长度限制是最小32字节，最大1024（1K）字节；