[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
G09C 1/00 (2006.01)
G06F 12/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 03803955.9

[45] 授权公告日 2009 年 10 月 21 日

[11] 授权公告号 CN 100553190C

[22] 申请日 2003.4.16 [21] 申请号 03803955.9

[30] 优先权

[32] 2002.4.17 [33] JP [31] 114076/2002

[86] 国际申请 PCT/JP2003/004864 2003.4.16

[87] 国际公布 WO2003/088557 日 2003.10.23

[85] 进入国家阶段日期 2004.8.13

[73] 专利权人 松下电器产业株式会社

地址 日本大阪府

[72] 发明人 和田妙美 福冈俊彦

[56] 参考文献

CN1324028A 2001.11.28

JP6-77954A 1994.3.18

JP11-220508A 1999.8.10

审查员 李 燕

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 汪惠民

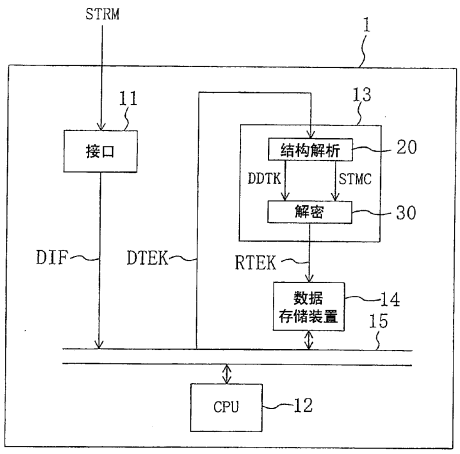
权利要求书 4 页 说明书 21 页 附图 14 页

[54] 发明名称

数字双向通信控制装置及方法

[57] 摘要

本发明涉及数字双向通信控制装置及方法，其中，接口部分(11)对被输入的下行流数据(STRM)进行格式变换。CPU(12)接收被格式变换了的数据(DIF)，实现 MAC 功能的。另外 TEK 处理部分(13)接收从数据(DIF)所得到的 TEK 处理数据(DTEK)，进行该数据结构的解析，根据该解析的结果，进行解密处理。



1．一种数字双向通信控制装置，是在数字双向通信中进行双向控制的装置，其特征在于，包括：

对被输入的下行流数据进行格式变换，生成下行方向数据的接口部分；

接收上述下行方向数据，实现媒体访问控制即MAC功能的CPU；以及

接收从上述下行方向数据中所得到的流量加密密钥处理数据即TEK处理数据，进行该数据结构的解析，并根据该解析的结果，进行解密处理的TEK处理部分，

上述TEK处理部分包括：

构造解析部分，该构造解析部分输入TEK处理数据，解析该TEK处理数据中的MPEG结构、和填充在MPEG结构中的MAC结构，实施用HCS数据的MAC头的错误检测和用HCS数据以外的MAC头信息的错误检测，并输出MAC状态信息数据，其中，上述MAC状态信息数据是表示具有MAC结构的MAC数据的状态以及意义的数据；和

解密部分，该解密部分参照上述MAC状态信息数据，判别TEK处理数据中的被加密了的部分，使用用来解密的TEK数据对被加密了的部分进行解密，并将该解密结果与没有被加密的部分组合起来。

2．如权利要求1所述的数字双向通信控制装置，其特征在于，上述构造解析部分包括：

解析作为TEK处理数据中的MPEG结构的头的MPEG头，输出表示MAC数据的位置的MAC数据位置信号、和表示MAC帧的开头字节位置的MAC数据开头位置信号的MPEG头解析部分；

以上述MAC数据位置信号及MAC数据开头位置信号为输入，对作为MAC结构的头的MAC头中除了扩展头以及MAC管理消息头即MACMM头之外的区域，识别状态信息，同时在TEK处理数据中存在扩展头时，输出表示扩展头的位置的扩展头位置信息数据，并且在TEK处理数据中存在MACMM头时，输出表示MACMM头的位置的MACMM头位置信息数据的MAC头解析部分；

接收上述扩展头位置信息数据，对扩展头的各区进行检查，输出表示扩展头的状态信息的扩展头状态信息数据的扩展头解析部分；以及

接收上述MACMM头位置信息数据，对MACMM头的各区进行检查，输出表示MACMM头的状态信息的MACMM头状态信息数据的MACMM头解析部分，

上述MAC头解析部分，

接收上述扩展头状态信息数据以及MACMM头状态信息数据，根据MAC头中的扩展头以及MACMM头之外的各区的状态信息、和上述扩展头状态信息数据所表示的扩展头的状态信息以及上述MACMM头状态信息数据所表示的MACMM头状态信息，生成上述MAC状态信息数据。

3．如权利要求2所述的数字双向通信控制装置，其特征在于：

上述MPEG头解析部分，检查MPEG头的区域，检测出MAC数据的位置以及MAC帧的开头字节位置，输出上述MAC数据位置信号和MAC数据开头位置信号。

4．如权利要求3所述的数字双向通信控制装置，其特征在于：

上述MAC头解析部分，通过用HCS数据的MAC头的错误检测方法的HCS检查来进行MAC头的错误检测。

5．如权利要求2所述的数字双向通信控制装置，其特征在于：

上述MAC头解析部分，进行对上述MAC头中的表示MAC数据长度的区域的检查，

上述检查是通过参照上述MAC数据开头位置信号统计MAC帧的数据长度，判断该MAC帧长是否和该区域的值以及给定的数据长度的和相一致来进行的。

6．如权利要求2所述的数字双向通信控制装置，其特征在于：

上述MAC头解析部分，除了通过用HCS数据的MAC头的错误检测方法的HCS检查之外，还通过MAC帧长检查以及扩展头长检查来进行MAC头的错误检测，并且，

当上述MAC帧长检查以及扩展头长检查的检查结果中没有错误时，使上述HCS检查的检查结果无效。

7．如权利要求2所述的数字双向通信控制装置，其特征在于：

上述扩展头解析部分，

参照上述扩展头位置信息数据，检查扩展头的区域，判断扩展头的数据长度以及种类，

在扩展头区域的值不当的情况下，识别出扩展头中有错，并将该判断作为上述扩展头状态信息数据而输出。

8．如权利要求2所述的数字双向通信控制装置，其特征在于：

上述MACMM头解析部分，

参照上述MACMM头位置信息数据，检查MACMM头的区域，判断MACMM头的数据长度以及种类，

在MACMM头区域的值不当的情况下，识别出MACMM头中有错，并将该判断作为上述MACMM头状态信息数据而输出。

9．如权利要求1所述的数字双向通信控制装置，其特征在于：

上述解密部分，

参照上述MAC状态信息数据，分出TEK处理数据中的被加密了的部分以及没有被加密的部分，

从TEK处理数据中，抽出用来选择TEK数据的TEK核对数据，

参照被抽出的TEK核对数据，从预先所设有的多个TEK数据中选择用于解密的TEK数据，

将被加密了的部分变换为解密处理单位的位宽，并使用所选的TEK数据进行解密，

将解密后的数据和没有被加密的部分进行组合。

10．一种数字双向通信控制方法，是在数字双向通信中进行双向控制的方法，其特征在于，包括：

对被输入的下行流数据进行格式变换，生成下行方向数据的步骤；

通过CPU接收上述下行方向数据，并实现媒体访问控制即MAC功能的步骤；以及

通过TEK处理部分，接收从上述下行方向数据所得到的流量加密密钥处理数据即TEK处理数据，进行该数据结构的解析，根据该解析的结果，进行解密处理的TEK处理步骤，

上述TEK处理步骤包括：

构造解析步骤，该构造解析步骤解析TEK处理数据中的MPEG结构，以及填充在MPEG结构中的MAC结构，实施用HCS数据的MAC头的错误检测和用HCS数据以外的MAC头信息的错误检测，生成MAC状态信息数据，其中，上述MAC状态信息数据是表示具有MAC结构的MAC数据的状态以及意义的数据；和

解密步骤，该解密步骤参照上述MAC状态信息数据，判别TEK处理数据中的被加密了的部分，使用用来解密的TEK数据对被加密了的部分进行解密，并将该解密结果和没有被加密的部分组合起来。

11．如权利要求10所述的数字双向通信控制方法，其特征在于，上述构造解析步骤包括：

解析作为TEK处理数据中的MPEG结构的头的MPEG头，输出表示MAC数据的位置的MAC数据位置信号，以及表示MAC帧的开头字节位置的MAC数据开头位置信号的MPEG头解析步骤；

使用上述MAC数据位置信号以及MAC数据开头位置信号，对作为MAC结构的头的MAC头中除了扩展头以及MAC管理消息头即MACMM头之外的区域，识别状态信息，同时在TEK处理数据中存在扩展头时，输出表示扩展头的位置的扩展头位置信息数据，并且在TEK处理数据中存在MACMM头时，输出表示MACMM头的位置的MACMM头位置信息数据的MAC头解析步骤；

接收上述扩展头位置信息数据，对扩展头的各区进行检查，生成表示扩展头的状态信息的扩展头状态信息数据的扩展头解析步骤；以及

接收上述MACMM头位置信息数据，对MACMM头的各区进行检查，生成表示MACMM头的状态信息的MACMM头状态信息数据的MACMM头解析步骤，

根据上述MAC头解析步骤中所判断的MAC头中的除扩展头以及MACMM头之外的各区的状态信息、上述扩展头状态信息数据所表示的扩展头的状态信息以及上述MACMM头状态信息数据所表示的MACMM头的状态信息，生成上述MAC状态信息数据。

数字双向通信控制装置及方法

技术领域

本发明涉及一种在数字双向通信中进行双向控制的装置，特别是一种使从中心装置方向终端装置方的下行方向的通信的相关构成最适化的技术。

背景技术

双向CATV所代表的数字双向通信系统中，是通过将多个终端装置与中心装置相连接的双向通信网而构成的。在每个终端装置中，从中心装置向终端装置的下行方向的通信以及从终端装置向中心装置的上行方向的通信的双向控制称作MAC（Media Access Control）功能，通常是通过对通信数据中的作为子层而被填充进来的具有MAC所特有的结构的协议进行解读，而实现处理功能的。

作为MAC结构的一例，有称作MCNS（Multimedia Cable Network Systems partners）的由美国电缆运营商以及有线电视的提供商所组成的团体，所提倡的现在事实上已经成为一种标准了的DOCSIS（Data Over Cable Service Interface Specifications）方式。其详细方式已经在美国的CableLabs（Cable Television Laboratories Inc.）所提供的规格书“Data-Over-Cable Service Interface Specifications”中的“Radio Frequency Interface Specification SP-RFIv1.1”中公开了。

下行方向的通信通常是发送视频数据。因此，通信数据中具有MPEG结构，而作为其子层定义了MAC结构。由于下行方向的通信，通信信道频率被分配在较宽的带域上，因此通信控制自身是比较简单的，然而为了发送视频数据就必须要处理庞大的数据量，因此需要按照一定的顺序，实时且准确无误的进行处理。

另外，上行通信中，通常是发送控制数据。该控制数据中，包括来自

终端装置方的命令请求以及用来通知各个终端装置的状态的状态显示数据。接收到了上行方向通信中所发送的控制数据之后，中心装置按照各个终端装置的请求命令，将用来正确控制终端装置的各种信息作为下行通信方向的控制数据发送出去。由于上行方向的通信，多个通信信道频率被分配在较窄的带域上，因此经常会发生多个终端装置间的冲突，或得不到必要的通信信道频率等情况，一般需要复杂的控制，其功能给双向通信中的通信性能带来了很大的影响。

DOCSIS MAC结构，由于和依据以太网的IP通信之间的兼容性很高，基本上具有和以太网通信一样的结构，但是还设置了作为DOCSIS特有区域的各种头区域。其特征是，在其中的称作“扩展头”的可变长区域中，定义了密码以及其他的附加功能。

为实现MAC功能，如上述的规格书中所示的那样，对具有复杂的多层构造的数据结构进行解析之后，必须在适当的时刻进行各种处理。多数处理是实现庞大的数据的组合，因此，验证该组合动作的正确性是一项难度非常高，处理量非常多的工作。

下面来看看各个处理的内容，构成MAC功能的各个处理主要是控制系统中的运算处理，基本上是数据的过滤（分开）、同步处理、重新排序、格式化等单个处理及其组合。这些单个处理本身决不能够说是负荷很大的处理。

然而，MAC功能中，还包括通信系统中的不可缺少的数据的安全功能，关于DOCSIS方式的详细规格，公布在美国的CableLabs所发布的规格书“Data-Over-Cable Service Interface Specifications”的“Baseline Privacy Plus Interface Specifications SP-BPI＋－106-001215”中。

MAC功能的安全功能，叫做Baseline Privacy，使用称作BPKM（Base Line Privacy key Management）的协议。BPKM为了进行安全的键交换，具备对密码键自身进行加密处理的功能，以及用来确认密码键交换消息是正确的对象所发送的，且没有被篡改的消息认证功能。BPKM中，使用作为主键的Authorization Key以及用在实际的数据的加密以及解密中的DES密码键（Traffic Encryption Key，称作TEK）这两级键而进行键的排列。

终端装置以RSA公开键方式接收被加密了的Authorization Key，使用

RSA公开键解密该Authorization Key。接着，通过进行对所获得的Authorization Key的TEK解密以及认证等几个处理，得到TEK数据，最后利用该TEK数据，进行对实际的通信数据的解密。这里，对于进行Authorization Key的解密的RSA密码的解密处理，以及进行TEK数据的解密的DES密码的解密来说，必须同时且反复，进行使用多个64位单位的数据的数值运算，各个单个的处理也都是负荷相当大的处理。

为了实现进行数据双向通信中的双向控制的MAC功能，必须将这样的处理组合起来进行处理。

MAC功能，一般使用通用处理器（CPU）来实现。这是因为，CPU中具有对复杂的处理能够弹性的进行对应这一优点，用来确立系统的可靠性的验证以及功能修正也能够比较容易的实现。

然而，MAC功能，为了实现其庞大的处理，必须使用高性能的CPU。另外，单单有了CPU还是不够的，通过单个的CPU来实现所期望的全部功能是极为困难的。因此，为了构成实现所有的MAC功能的装置，电路规模变得非常之大，成了一种费用已经高到了不现实的程度的装置。

为解决上述问题，本发明的课题是，在数字双向通信控制中，实现CPU处理的负荷的减轻以及装置全体的电路规模的适当化。

发明内容

本发明作为在数字双向通信中进行双向控制的装置，包括：对被输入的下行流数据进行格式变换，生成下行方向数据的接口部分，以及接收上述下行方向数据并实现MAC（Media Access Control）功能的CPU，以及接收从上述下行方向数据所得到的TEK（Traffic Encryption Key）处理数据，进行该数据结构的解析，根据该解析的结果，进行解密处理的TEK处理部分。

这样，用来实现MAC功能的处理中，TEK处理数据的结构解析以及根据该解析结果的解密处理，是通过和CPU分开的TEK处理部分来进行的。因此，减轻的CPU处理的负荷，从而使得装置全体可以通过适当的电路规模来构成。

另外，上述本发明的相关数字双向通信控制装置中的TEK处理部分，

最好还包括输入TEK处理数据，解析该TEK处理数据中的MPEG结构，以及填充在MPEG结构中的MAC（Media Access Control）结构，输出表示作为具有MAC结构的数据的MAC数据的状态以及意义的MAC状态信息数据的构造解析部分；以及参照上述MAC状态信息数据，判别TEK处理数据中的被加密了的部分，使用用来解密的TEK数据对被加密了的部分进行解密，并将该解密结果和没有被加密的部分组合起来的解密部分。

另外，上述本发明的相关数字双向通信控制装置中的构造解析部分，最好还包括解析作为TEK处理数据DTEK中的MPEG结构的头的MPEG头，输出表示MAC数据的位置的MAC数据位置信号，以及表示MAC帧的开头字节位置的MAC数据开头位置信号的MPEG头解析部分；以及输入上述MAC数据位置信号以及MAC数据开头位置信号之后，对作为MAC结构的头的MAC头中除了扩展头以及MACMM（MAC Management Message）头之外的区域，识别状态信息，同时在TEK处理数据DDTK中存在扩展头时，输出表示扩展头的位置的扩展头位置信息数据，并且在TEK处理数据DDTK中存在MACMM头时，输出表示MACMM头的位置的MACMM头位置信息数据的MAC头解析部分；以及接收上述扩展头位置信息数据，对扩展头的各区进行检查，输出表示扩展头的状态信息的扩展头状态信息数据的扩展头解析部分；以及接收上述MACMM头位置信息数据，对MACMM头的各区进行检查，输出表示MACMM头的状态信息的MACMM头状态信息数据的MACMM头解析部分。上述MAC头解析部分，接收上述扩展头状态信息数据以及MACMM头状态信息数据，根据MAC头中的扩展头以及MACMM头之外的各区的状态信息、上述扩展头状态信息数据所表示的扩展头的状态信息以及上述MACMM头状态信息数据所表示的MACMM头状态信息，生成上述MAC状态信息数据。

另外，最好使上述MPEG头解析部分，检查MPEG头的区域，检测出MAC数据的位置以及MAC帧的开头字节位置，输出上述MAC数据位置信号和MAC数据开头位置信号。

另外，上述MAC头解析部分，最好通过HCS检查来进行MAC头的错误检测。或者最好使上述MAC头解析部分，进行对上述MAC头中的表示MAC数据长度的区域的检查，上述检查是通过参照上述MAC数据开头位

置信号统计MAC帧的数据长度，判断该MAC帧长是否和该区域的值以及给定的数据长度的和相一致来进行的。或者最好使上述MAC头解析部分，除了通过HCS检查之外，还通过MAC帧长检查以及扩展头长检查来进行MAC头的错误检测，并且，当上述MAC帧长检查以及扩展头长检查的检查结果中没有错误时，使上述HCS检查的检查结果无效。

另外，最好使上述扩展头解析部分，参照上述扩展头位置信息数据，检查扩展头的区域，判断扩展头的数据长度以及种类，在扩展头区域的值不当的情况下，识别出扩展头中有错，并将该判断作为上述扩展头状态信息数据而输出。

另外，最好使上述MACMM头解析部分，参照上述MACMM头位置信息数据，检查MACMM头的区域，判断MACMM头的数据长度以及种类，在MACMM头区域的值不当的情况下，识别出MACMM头中有错，并将该判断作为上述MACMM头状态信息数据而输出。

另外，最好使上述本发明的相关数字双向通信控制装置中的解密部分，参照上述MAC状态信息数据，分出TEK处理数据中的被加密了的部分以及没有被加密的部分，从TEK处理数据中，抽出用来选择TEK数据的TEK核对数据，参照被抽出的TEK核对数据，从预先所设有的多个TEK数据中选择用于解密的TEK数据，将被加密了的部分变换为解密处理单位的位宽，并使用所选的TEK数据进行解密，将解密后的数据和没有被加密的部分进行组合。

另外，本发明作为在数字双向通信中进行双向控制的方法，包括对被输入的下行流数据进行格式变换，生成下行方向数据的步骤；以及通过CPU接收上述下行方向数据，并实现MAC（Media Access Control）功能的步骤；以及通过TEK处理部分，接收从上述下行方向数据所得到的TEK（Traffic Encryption Key）处理数据，进行该数据结构的解析，根据该解析的结果，进行解密处理的TEK处理步骤。

另外，最好使上述本发明的相关数字双向通信控制方法中的TEK处理步骤包括解析TEK处理数据中的MPEG结构，以及填充在MPEG结构中的MAC（Media Access Control）结构，生成表示作为具有MAC结构的数据的MAC数据的状态以及意义的MAC状态信息数据的构造解析步骤；以及

参照上述MAC状态信息数据，判别TEK处理数据中的被加密了的部分，使用用来解密的TEK数据对被加密了的部分进行解密，并将该解密结果和没有被加密的部分组合起来的解密步骤。

另外，最好使上述构造解析步骤包括解析作为TEK处理数据DTEK中的MPEG结构的头的MPEG头，输出表示MAC数据的位置的MAC数据位置信号，以及表示MAC帧的开头字节位置的MAC数据开头位置信号的MPEG头解析步骤；以及使用上述MAC数据位置信号以及MAC数据开头位置信号，对作为MAC结构的头的MAC头中除了扩展头以及MACMM（MAC Management Message）头之外的区域，识别状态信息，同时在TEK处理数据DDTK中存在扩展头时，输出表示扩展头的位置的扩展头位置信息数据，并且在TEK处理数据DDTK中存在MACMM头时，输出表示MACMM头的位置的MACMM头位置信息数据的MAC头解析步骤；以及接收上述扩展头位置信息数据，对扩展头的各区进行检查，生成表示扩展头的状态信息的扩展头状态信息数据的扩展头解析步骤；以及接收上述MACMM头位置信息数据，对MACMM头的各区进行检查，生成表示MACMM头的状态信息的MACMM头状态信息数据的MACMM头解析步骤。根据上述MAC头解析步骤中所判断的MAC头中的除扩展头以及MACMM头之外的各区的状态信息、上述扩展头状态信息数据所表示的扩展头的状态信息以及上述MACMM头状态信息数据所表示的MACMM头的状态信息，生成上述MAC状态信息数据。

附图说明

图1为说明本发明的实施方式1的相关数字双向通信控制装置的构成的方框图。

图2为说明图1所示的结构解析部分的内部构成的示意图。

图3为说明本发明的实施方式1的相关MPEG头的解析的状态器的示意图。

图4为说明MPEG头的格式的示意图。

图5为说明包括有指针区的MPEG数据的格式的示意图。

图6为本发明的实施方式1的相关MAC头的解析的状态器。

图7为说明MAC数据的格式的示意图。

图8为用来说明HCS检查之外的MAC头错误检测方法的图。

图9为本发明的实施方式1的相关扩展头解析的状态器。

图10为说明扩展头的格式的示意图。

图11为说明扩展头的一个例子(Downstrem Privacy)的格式的示意图。

图12为本发明的实施方式1的相关MACMM头解析的状态器。

图13为说明MACMM头的格式的示意图。

图14为说明本发明的实施方式1的相关解密部分的动作的流程图。

具体实施方式

下面对照附图说明本发明的具体实施方式。

图1为说明本发明的实施方式1的相关数字双向通信控制装置的构成的方框图。图1中所示的数字双向通信控制装置1是在由中心装置以及多个终端装置所构成的双向通信网中进行双向通信控制的设备，被设置在终端装置的内部。

图1中，11为输入作为由中心装置所发送的视频以及传输控制数据的下行流数据STRM，为了向CPU12发送而进行格式变换，生成作为下行方向数据的CPU接口数据DIF的接口部分，12为经CPU总线接收CPU接口数据DIF，实现MAC（Media Access Control）功能的CPU，14为通过CPU总线15进行和CPU12之间的数据存取的数据存储装置。

13为输入作为视频以及传输控制数据中的TEK处理中所使用的数据的TEK处理数据DTEK，进行数据结构的解析、加密的有无的确认、数据的解密以及数据变换，并将该处理结果作为TEK处理结果数据RTEK而输出的TEK处理部分。TEK处理部分13，包括进行TEK处理数据DTEK的结构解析，输出延迟TEK处理数据DDTK以及MAC状态信息数据STMC的结构解析部分20，以及利用延迟TEK处理数据DDTK以及MAC状态信息数据STMC，判断延迟TEK处理数据DDTK中的加密的有无，进行解密处理以及数据的位变换，并输出TEK处理结果数据RTEK的解密部分30。TEK处理部分13所输出的TEK处理结果数据RTEK被输入到数据存储装置14中。

这里，MAC状态信息数据STMC，表示被嵌入到TEK处理数据DTEK

中的MPEG结构中的，且具有作为网络处理用子层的MAC结构的数据（MAC数据）的状态以及意义。另外，延迟TEK处理数据DDTK是为了与MAC状态信息数据STMC在时间上对应，而使TEK处理数据DTEK延迟0个或一个时钟所得到的。另外，CPU接口数据DIF中，除了对下行流数据STRM进行格式变换所得到的数据之外，还包括CPU总线15的控制信号。

下面对图1中所示的数字双向通信控制装置1的动作进行说明。

终端装置接收到下行流数据STRM之后，将其发送给数字双向通信控制装置1内的接口部分11。接口部分11变换下行流数据STRM的格式，并作为CPU接口数据DIF输出。CPU12通过CPU总线15接收CPU接口数据DIF，并和数据存储装置14一起进行为了实现MAC功能的各种处理。但是，作为用于MAC功能中的TEK处理中所用的数据的TEK处理数据DTEK，经CPU总线15由CPU12发送给TEK处理部分13。

TEK处理部分13中，被输入了TEK处理数据DTEK之后，首先结构解析部分20进行TEK处理数据DTEK中的MPEG结构以及嵌入在MEPG结构中的MAC结构的结构解析。结构解析部分20所输出的延迟TEK处理数据DDTK以及MAC状态信息数据STMC被发送给解密部分30。解密部分30，在延迟TEK处理数据DDTK中，对为了保护数据的机密性而在中心装置侧通过DES（Data Encryption Standard）而被加密了的数据进行解密处理，并向数据存储装置14输出TEK处理结果数据RTEK。构造解析部分20和解密部分30中的处理将在后面详述。

通过这样的构成，用来实现MAC功能的处理当中，TEK处理数据DTEK的结构解析，以及根据该解析结果的解密处理，是通过和CPU12分开的TEK处理部分13来进行的。因此，大幅减轻了CPU处理的负荷。另外，TEK处理部分13中的处理，几乎都是通过将同样的数值运算处理并列且反复的执行来实现的，其分部结构也变得简单。因此，能够通过适当的电路规模来构成装置全体。

另外，通过使将TEK处理数据DTEK从CPU总线15向TEK处理部分13发送的总线为双向的，TEK处理的一部分能够由CPU12来执行。另外，通过使接口部分11向TEK处理部分13直接发送视频以及控制数据，能够降低CPU总线15的占有率，同时能够实现CPU处理的高速化。另外，通过使下

行流数据STRM的输入路径，以及从接口部分11经CPU总线15的CPU接口数据DIF的路径，分别都为双向的，使双向通信控制成为可能。

<结构解析部分>

图2为说明图1中所示的结构解析部分20的内部构成的方框图。图2中，21为解析作为TEK处理数据DTEK中的MPEG结构的头的MPEG头，从MPEG构造中抽出MAC构造，输出表示MAC数据的数据位置的MAC数据位置信号PMC和表示MAC帧的开头字节位置的MAC数据开头位置信号LPMC的MPEG头解析部分。MPEG头解析部分21，输出使TEK处理数据DTEK延迟而得到的延迟TEK处理数据DDTK，同时还输出其相关的MAC数据位置信号PMC以及MAC数据开头位置信号LPMC。

22为被输入了MAC数据位置信号PMC以及MAC数据开头位置信号LPMC之后，对具有MAC结构的MAC数据中的头部分（MAC头）中除了扩展头以及MACMM（MAC Management Message）头之外的部分进行解析，判断各个区域的状态信息也即数据的意义的MAC头解析部分。另外，MAC头解析部分22，在延迟TEK处理数据DDTK中存在扩展头时，输出表示扩展头的位置的扩展头位置信息数据PEH，并且在延迟TEK处理数据DDTK中存在MACMM头时，输出表示MACMM头的位置的MACMM头位置信息数据PMM。

另外，23为接收扩展头位置信息数据PEH，进行对MAC头中的扩展头的解析，输出表示扩展头的状态信息也即状态、意义的扩展头状态信息数据STEH的扩展头解析部分。24为接收MACMM位置信息数据PMM，进行对MACMM头的解析，输出表示MACMM的状态信息也即状态、意义的MACMM头状态信息数据STMM的MACMM头解析部分。

MAC头解析部分22，接收扩展头状态信息数据STEH以及MACMM头状态信息数据STMM，根据MAC头中的除扩展头以及MACMM头之外的区域的状态信息，以及扩展头状态信息数据STEH所示的扩展头的状态信息和MACMM头状态信息数据STMM所示的MACMM头的状态信息，生成MAC状态信息数据STMC。

下面对各个解析部分21～24的动作进行更详细的说明。

<MPEG头解析>

MPEG头解析部分21，通过解析TEK处理数据DTEK中的MPEG头，从MAC结构中抽出MPEG结构。具体的说，逐次检测MPEG头中的各个区域，判断各个区域的数据的意思，给出数据状态。

图3为说明MPEG头解析部分21中的MPEG头解析的状态器的示意图。另外图4为说明MPEG头的格式的示意图。下面对照图3，说明MPEG头解析中的处理的流程。

状态器的状态按照字节时钟发生迁移。状态的初期状态为“IDLE”，在TEK处理数据DTEK中有错误的情况下，使状态为“ERR”。

当状态为“IDEL”时，一直保持该状态直到TEK处理数据DTEK中所包括的包同步表示MPEG帧的开头（S11）。在包同步表示MPEG帧的开头时，当MPEG数据的开头数据，也即图4中所示的MPEG包同步字节数据（sync byte）的值为“Ox47”时，使状态为“S1”（S12），另外，在非上述状态时使状态为“ERR”。

在状态为“S1”的情况下，当图4中所示的TEI（Transport Error Indicator）数据的值为“Ox0”（S13），且图4中所示的PID（Program ID）的前5位上的值位“Ox1F”（S14）时，使状态为“S2”，在非上述状态时使状态为“ERR”。TEI数据为表示MPEG结构中是否有错误的数据，是在错误修正时被附加上的。另外，PID是由传输DOCSIS规格的MAC帧的MPEG数据所设定的。

在状态为“S2”的情况下，当PID的后8位上的值位“OxFE”时，使状态为“S3”，在非上述状态时使状态为“ERR”（S15）。在状态为“S3”的情况下，当图4中所示的传输加密控制数据（Transport scrambling control）数据的值为“Ox0”，且图4中所示的适配区控制数据（Adaptation field control）的值为“Ox1”时，使状态为“S4”，在非上述状态时使状态为“ERR”（S16）。传输加密控制数据是关于加密控制的控制数据，适配区控制数据为用于DOCSIS的区域分配控制数据。

在状态为“S4”的情况下，当图4中所示的PUSI（payload unit start indicator）数据的值为“Ox1”时，判断存在指针区，使状态为“POINTER”（S17）。在非上述状态时使状态为“MAC_FRM”。PUSI为说明MPEG数据中是否存在MAC数据的开头的数据。这里，指针区是生成MAC数据

开头位置信号LPMC时的重要数据，将在后面对其进行详述。

在状态为“MAC_FRM”的情况下，一直保持该状态直到出现MPEG包同步字节数据（S18），在出现了MPEG包同步字节数据且其值为“Ox47”的情况下（S12），使状态为“S1”，在非上述状态时使状态为“ERR”。

另外，在状态为“ERR”的情况下，一直保持该状态直到包同步表示MPEG数据的开头（S19），在包同步表示MPEG数据的开头时，在MPEG包同步字节数据的值为“Ox47”的情况下，使状态为“S1” （S12），在非上述状态时保持状态不变。

这里，对照图5，对指针区、MAC数据开头位置信号LPMC以及MAC数据位置信号PMC的生成方法进行说明。图5为概念性的说明包含有指针区的MPEG数据的格式的示意图。图5中所示的那样的MPEG数据被包括在TEK处理数据DTEK中。

图5中，MPEG头中的PUSI值为“Ox1”，且存在指针区。也即MPEG头的后面存在指针区，使该指针区的值为M（M：整数）。这说明在指针区的后面，存在一个MAC帧（MAC Frame ＃1）所剩余的M个字节的数据，在其后面开始有一个新的MAC帧（MAC Frame ＃2）。因此，能够从指针区的值M检测出MAC帧的开头字节的位置。

也即，由于状态为“POINTER”的数据为指针区，设置指针区计数器，通过该指针区计数器，从状态为“POINTER”的位置也即从指针区位置开始进行计数，这样，在该指针区计数器的计数值和指针区的值相等时，识别该位置为MAC帧的开头字节的位置。通过这样来生成MAC数据开头位置信号LPMC。

另外，状态为“MAC_FRM”时的数据为MAC结构，按照它来生成MAC数据位置信号PMC。图5中概念性的显示了MPEG数据和MAC数据开头位置信号LPMC以及MAC数据位置信号PMC之间的关系。

另外，这里所求得的各个区域的状态信息被保存在寄存器中。为了使TEK处理数据和状态信息相对应，使TEK处理数据DTEK延迟0个或者一个以上时刻，生成延迟TEK处理数据DDTK。

另外，关于MPEG结构的保护功能，不但设置了对TEI数据的前方保护以及后方保护计数器，还设置了统计MPEG结构数据的长度（188字节）

的MPEG帧长计数器，能够设置即使TEI数据没有显示有错误，在到下一个MPEG结构的开头数据之前的MPEG结构数据长度不是188的情况下，判断该MPEG结构错误的功能。

<MAC头解析>

MAC头解析部分22，进行延迟TEK处理数据DDTK中的MAC头的解析。具体的说，逐次检测MAC头中的各个区域，判断各个区域的数据的意思，给出数据状态。

图6为说明MAC头解析部分22中的MAC头解析的状态器的示意图。该MAC头解析的状态器只在MAC数据位置信号PMC为有效的状态下工作。另外图7为说明MAC数据的格式的示意图。下面对照图6，说明MAC头解析中的处理的流程。

状态器的状态按照字节时钟发生迁移。状态的初期状态为“IDLE”，在MAC结构中有错误的情况下，使状态为“ERR”。

当状态为“IDLE”时，在MAC数据开头位置信号LPMC无效时保持该状态，在其为有效时使状态为“FC”（S21）。这里，状态为“FC”时的MAC头为FC（Field Control）数据，表示MAC数据的种类以及使MAC数据结构能够扩展的扩展头的有无。

当状态为“FC”时，解析FC数据的值（S22）。当FC数据的值显示为SYNC数据时使状态为“PARM_T”（S22A），显示为MACMM时使状态为“PARM_M”（S22B），显示为PacketPDU时使状态为“PARM_D”（S22C）。另外，在FC数据的值为“Oxff”，表示为作为MPEG结构数据的空数据的STUFF字节的情况下，保持状态不变（S22D），在FC数据为以上之外的情况下使状态为“ERR”（S22E）。SYNC数据为由中心装置方发送的用于传输同步处理的必要数据的MAC结构，MACMM为由中心装置方发送的用于传输MAC控制中所用到的带宽分配数据以及同步处理所的必要的数据等的MAC结构，PacketPDU为用来传输通常的视频数据的MAC结构。

另外，通过FC数据中所含有的EHDR_ON的值来判断MAC数据中的扩展头的有无。其为“0”时不存在扩展头，为“1”时存在扩展头。

当状态为“PARM_T”、“PARM_M”、“PARM_D”时，使状态

为“LEN_H”。当状态为“LEN_H”时，使状态为“LEN_L”。当状态为“LEN_L”时，通过EHDR_ON的值来判断MAC数据中的扩展头的有无（S23）。当存在扩展头时使状态为“EHDR”，当不存在扩展头时使状态为“HCS_H”。

由于状态为“EHDR”期间是扩展头的位置，生成扩展头位置信息数据PEH，将其和延迟TEK处理数据DDTK同时发送给扩展头解析部分23。关于扩展头解析部分23的处理内容将在后面叙述。

当状态为“EHDR”时，在扩展头解析部分23进行处理的期间保持状态不变。在通过扩展头解析部分23所输出的扩展头状态信息数据STEH确认到扩展头解析处理正常结束时，使状态为“HCS_H”（S25）。另外，在通过扩展头解析部分23所输出的扩展头状态信息数据STEH确认到扩展头中存在错误，也即确认到MAC结构中有错误时，使状态为“ERR”（S24）。扩展头状态信息数据STEH为说明扩展头的各区域的状态的信息。

当状态为“HCS_H”时，使状态为“HCS_L”。当状态为“HCS_L”时，使状态为“DA_LD”。当状态为“DA_LD”时，使状态为“SA_LD”。

当状态为“SA_LD”时，确认延迟TEK处理数据DDTK的发送目的地址（DA：Destination Address）和终端装置的地址是否一致，当不一致时，由于不是终端装置应当处理的数据，使状态为“ERR”（S26）。在一致时，判断MAC结构是否为SYNC数据或MACMM，也即判断MAC结构中是否存在MACMM头，存在时使状态为“MAC_MNG”，不存在时使状态为“TL_H”（S27）。

由于在状态为“MAC_MNG”期间是MACMM头的位置，生成MACMM头位置信息数据PMM，将其和延迟TEK处理数据DDTK同时发送给MACMM头解析部分24。关于MACMM头解析部分24的处理内容将在后面叙述。

当状态为“MAC_MNG”时，在MACMM头解析部分24进行处理的期间保持状态不变。在通过MACMM头解析部分24所输出的MACMM头状态信息数据STMM确认到MACMM头解析处理正常结束时，使状态为“VALID”（S29）。另外，在通过MACMM头解析部分24所输出的MACMM头状态信息数据STMM确认到MACMM头中存在错误，也即确认

到MAC结构中有错误时，使状态为“ERR”（S28）。MACMM头状态信息数据STMM为表示MACMM头的各区域的状态的信息。

当状态为“TL_H”时，确认延迟TEK处理数据DDTK的发送源地址（SA：Source Address）和终端装置的地址是否一致，当一致时，由于发送目的地和发送源相同判断是不当数据，使状态为“ERR”，在不一致时，使状态为“TL_L”（S2A）。当状态为“TL_L”时，使状态为“VALID”。

当状态为“VALID”时，一直保持状态不变直到MAC结构的最后数据的到来，当MAC数据的最后数据到来时，使状态为“FC”，进行下个MAC结构的结构解析（S2B）。

也即，MAC头解析部分22按照状态而进行工作，在状态为“EHDR”期间由于表示是扩展头，生成扩展头位置信息数据PEH，在状态为“MAC_MNG”期间由于表示是MACMM头，生成MACMM头位置信息数据PMM。并根据扩展头状态信息数据STEH和MACMM头状态信息数据STMM，以及由MAC头解析部分22所解析的MAC头的状态信息，生成MAC状态信息数据STMC。另外，为了和这里所求得的状态相对应，使延迟TEK处理数据DDTK进一步延迟，从结构解析部分20输出。

（MAC头的错误检测）

这里通过HCS检查来进行MAC头的错误检测。所谓HCS检查是指，对图7中所示的MAC数据的构造中的HCS之外的MAC头（FC区、PARM区、LEN区、EHDR区）进行CRC计算，通过比较其和HCS数据的一致性，来检测MAC头中的错误的方法。

图8为用来说明HCS检查之外的MAC头中的错误检测的图。该图中，（a）为LEN区检查（MAC帧长检查），（b）为PARM区的检查（扩展头长检查）。

如图8（a）所示，LEN区的检查中，使用统计LEN区值的LEN计数器。当MAC数据开头位置信号LPMC在表示一个MAC数据（MAC数据1）的开头的位置上变成有效时，LEN计数器开始计数，当在表示下一个MAC数据（MAC数据2）的开头位置上变成有效时，停止该计数器。通过这样使LEN计数器的值表示MAC数据1的数据长度，如果没有错误的话，应当和MAC_LEN的长度（＝LEN区值＋6个字节（FC・PARM・HCS））相一

致。因此，当LEN计数器的值和MAC_LEN的长度相一致时，判断LEN区中没有错误，另外，当LEN计数器的值和MAC_LEN的长度不一致时，判断LEN区中有错误。

如图8（b）所示，PARM区的检查中，使用统计PARM区值的PARM计数器。在当MAC数据开头位置信号LPMC在表示一个MAC数据（MAC数据3）的开头的位置上变成有效时之后的6个字节（相当于FC·PARM·LEN区的长度）的位置上，LEN计数器开始计数，在统计到PARM区的值的位置上，停止该计数器。通过这样使得PARM计数器停止计数的位置相当于扩展头的末端位置，之后按照图6继续进行状态解析。如果PARM计数器所显示的扩展头的末端位置错误的话，后继的状态解析结果就会显示出错。因此，在MAC数据3的状态解析结束时，当状态解析的结果不为“ERR”时，判断PARM区中没有错误，另外，当状态解析的结果为“ERR”时，忽略PARM区检查的结果。

FC区的检查，确认FC区的值的检查处理以及后继的按照图6所进行的状态解析处理，是否适应于根据FC区的值所判断出的数据的种类，当状态解析的结果不为“ERR”时，判断FC区中没有错误，另外，当状态解析的结果为“ERR”时，忽略FC区检查的结果。

EHDR区的检查，当后述的扩展头解析部分23的状态解析结果不为“ERR”时，判断EHDR区中没有错误，另外，当状态解析的结果为“ERR”时，判断EHDR区中有错误。

如上所述的MAC头的各区的检查结果，可以设置在所有的区中都没有错误的情况下，即使HCS检查结果为错误时也判断该MAC头中没有错误的功能。例如，当MAC帧长检查以及扩展头长检查的检查结果中没有错误时，可以使HCS检查的检查结果无效。另外，还可以不使用这样的MAC头的错误检查方法，而仅仅通过HCS检查来进行MAC头的错误检测。

<扩展头解析>

扩展头解析部分23，在延迟TEK处理数据DDTK中存在扩展头的情况下，进行该扩展头的解析。具体的说，逐次检测扩展头中的各个区域，判断各个区域的数据的意思，给出数据状态。

图9为说明扩展头解析部分23中的扩展头解析的状态器的示意图。另

外图10为说明扩展头的格式的示意图。如图10所示，扩展头由表示扩展头的种类的EH TYPE区、表示扩展头的数据部分的EH VALUE区以及表示EH VALUE区的长度的EH LEN区构成，后面将EH TYPE、EH VALUE和EH LEN各区作为一组而进行重复操作。

下面对照图9，说明扩展头解析中的处理的流程。状态器的状态按照字节时钟发生迁移。

在状态为初始状态“IDEL”的情况下，当MAC头解析部分22所发送的扩展头位置信息数据PEH为有效时，使状态为“EH_TL”，在非上述情况下保持该状态不变（S31）。

状态为“EH_TL”时的MAC数据表示扩展头的种类以及数据长度。扩展头中包括下面三种类型，也即，作为MAC数据的加密的相关数据的“Downstream Privacy”，在连续发送MAC数据，且这些MAC数据具有相同的头的情况下，被实施了压缩该重复的头使带宽节约成为可能的功能的PHS（Payload Header Suppression）的数据“Downstream PHS”，以及用来填充扩展头的“Null”。图11为说明作为“Downstream Privacy”的扩展头的格式的示意图。

当状态为“EH_TL”，MAC数据表示上述3种类型中的任何一种时，使状态为“EH_VAL”，在非上述情况下，判断延迟TEK处理数据DDTK中有错误，使状态为“ERR”（S32）。

当状态为“EH_VAL”时，在扩展头为“Downstream Privacy”的情况下（S33），当表示协议的版本的Version数据（Protocol Version Number）的值不为Ox01时，或者作为EH VALUE区的最后的数据的Reserved数据的值不为Ox00的情况下，判断延迟TEK处理数据DDTK中有错误，使状态为“ERR”（S34、S35）。

在非上述状态下，确认是否到了EH VALUE区的末尾（S36）。这里的确认是通过统计EH LEN区的值的EH LEN计数器来进行的。也即，当EH LEN计数器的值和EH LEN区的值不一致的情况下，保持状态不变。另外，当一致时，确认是否到了扩展头区的末尾（S37）。这里的确认是参照扩展头位置信息数据PEH而进行的。当到了扩展头区的末尾时，判断扩展头解析正常终止，使状态为“IDLE”，当没有到扩展头区的末尾时，

使状态为“EH_TL”。

其结果是，扩展头解析部分23，将扩展头各区的状态信息、判断延迟TEK处理数据DDTK中是否有错的情况下的错误信息以及判断扩展头的解析正常终止时的正常终止状态信息，作为扩展头状态信息数据STEH输出给MAC头解析部分22。

<MACMM头检测>

MACMM头解析部分24，当延迟TEK处理数据DDTK中存在MACMM头的情况下，进行该MACMM头的解析。具体的说，逐次检测MACMM头中的各个区域，判断各个区域的数据的意思，给出数据状态。

图12为说明MACMM头解析部分23中的MACMM头解析的状态器的示意图。另外图13为说明MACMM头的格式的示意图。图13中，DA为延迟TEK处理数据DDTK的发送目的地址区，SA为延迟TEK处理数据DDTK的发送源地址区，MsgLEN为MACMM的数据长度区，DSAP为表示以ISO8802－2为标准的LLC发送目的地址指针的区，SSAP为表示以ISO8802－2为标准的LLC发送源地址指针的区，Control为表示以ISO8802－2为标准的Unnumbered信息帧区，Version为表示MACMM的版本的区，Type为表示MACMM的种类的区，RSVD为用来将MAC Management Payload配置在32位的环境上的保留数据区，MAC Management Payload为MACMM的实际数据区，CRC为用来对从DA到MAC Management Payload之间进行CRC计算的检查序列数据区。

下面对照图12，说明MACMM头解析中的处理的流程。状态器的状态按照字节时钟发生迁移。

在状态为初始状态“IDEL”的情况下，当MAC头解析部分22所发送的MACMM头位置信息数据PMM为有效时，使状态为“MSGL_H”，在非上述情况下保持该状态不变（S41）。

当状态为“MSGL_H”时，比较所接收到的延迟TEK处理数据DDTK的发送源地址（SA）和终端装置的地址，在二者一致的情况下，判断延迟TEK处理数据DDTK为不当数据，使状态为“ERR”，另外，在不一致的情况下，使状态为“MSGL_L”（S42）。

当状态为“MSGL_L”时，使状态为“DSAP”。当状态为“DSAP”

时，在延迟TEK处理数据DDTK为Ox00的情况下，使状态为“SSAP”，在非上述情况下，判断延迟TEK处理数据DDTK为不当数据，使状态为“ERR”（S43）。

当状态为“SSAP”时，在延迟TEK处理数据DDTK为Ox00的情况下，使状态为“CONTROL”，在非上述情况下，判断延迟TEK处理数据DDTK为不当数据，使状态为“ERR”（S44）。

当状态为“CONTROL”时，在延迟TEK处理数据DDTK为Ox03的情况下，使状态为“VERSION”，在非上述情况下，判断延迟TEK处理数据DDTK为不当数据，使状态为“ERR”（S45）。

当状态为“VERSION”时，在延迟TEK处理数据DDTK为Ox01或Ox02的情况下，使状态为“TYPE”，在非上述情况下，判断延迟TEK处理数据DDTK为不当数据，使状态为“ERR”（S46）。

当状态为“TYPE”时，使状态为“RSVD”。当状态为“RSVD”时，判断MACMM头解析正常结束，使状态为“IDLE”。

其结果是，MACMM头解析部分24，将MACMM头各区的状态信息、判断延迟TEK处理数据DDTK中是否有错的情况下的错误信息以及判断MACMM头的解析正常结束时的正常结束状态信息，作为MACMM头状态信息数据STMM输出给MAC头解析部分22。

通过MAC头解析部分22、扩展头解析部分23以及MACMM头解析部分24的处理，结构解析部分20的处理结束。处理结束之后，将MAC状态信息数据STMC以及和它相对应的延迟TEK处理数据DDTK发送给解密部分30。

<解密部分30>

解密部分30，被输入结构解析部分20所输出的延迟TEK处理数据DDTK以及MAC状态信息数据STMC，在延迟TEK处理数据DDTK中，对为了保护数据的机密性而被中心装置方通过DES（Data Encryption Standard）加密了的部分的数据进行解密处理，将该处理结果作为TEK处理结果数据RTEK输出给数据存储装置14。

图14为说明解密部分30的动作的流程图。图14中，31为被输入了延迟TEK处理数据DDTK以及MAC状态信息数据STMC，判断延迟TEK处理数

据DDTK中的加密的有无，输出第1解密处理对象数据DD1以及解密处理对象外数据DDX的加密有无检测部分，32为将第1解密处理对象数据DD1变换为适合于解密处理的64位数据，并作为第2解密处理对象数据DD2而输出的第1位变换部分。33位从延迟TEK处理数据DDTK中，抽出用来选择TEK数据的TEK核对数据ITEK的TEK核对数据抽出部分，34为使用TEK核对数据ITEK抽出TEK数据TEK的TEK数据抽出部分。35为对第2解密处理对象数据DD2进行解密，输出第1解密处理结果数据RD1的解密处理部分，36为将第1解密处理结果数据RD1变换为和解密处理对象外数据DDX一样的位宽的8位数据，作为第2解密处理结果数据RD2输出的第2位变换部分，37为将第2解密处理结果数据RD2和解密处理对象外数据DDX结合并作为结合数据CBD输出的数据结合部分，38为将结合数据CBD变换成适合于数据存储装置14的位宽，并作为TEK处理结果数据RTEK输出的第3位变换部分。

这里，第1解密处理对象数据DD1为延迟TEK处理数据DDTK中的被DES加密了的部分的数据，解密处理对象外数据DDX为延迟TEK处理数据DDTK中的没有被DES加密的部分的数据。另外，TEK数据TEK为用来解密的数据，这里实际上就是使用在数据的加密以及解密中的DES密码键。TEK核对数据ITEK，是为了从预先所设有的多个TEK数据中选择出用于解密的TEK数据TEK而进行核对的序列数据。这里，TEK数据TEK包含有解密处理的初期值数据。

另外，由于为了防止被破解而要定期的变更TEK数据，为了使更新TEK数据时的中心装置和终端装置之间的通信不被中断，在TEK抽出部分34中，预先设置有用来保存前后的TEK数据、解密处理的初期值数据、延迟TEK处理数据DDTK中的扩展头中所设定的TEK数据的索引·序列编号的数据存储缓存。

下面对照图14，对解密部分30的处理进行说明。另外，MAC状态信息数据STMC至少包括：被包括在扩展头中的表示MAC数据是否被加密了的Encrypt位所生成的MAC数据Encrypt信号，表示MAC头以及地址数据（SA、DA）的位置的激活信号，表示存在于扩展头中的TEK核对数据的位置的TEK核对数据激活信号。

首先在加密有无检测部分31中，参照MAC状态信息数据STMC，判别延迟TEK处理数据DDTK中的被加密了的部分以及没有被加密的部分，输出第1解密处理对象数据DD1以及解密处理对象外数据DDX。也即，在MAC数据Encrypt信号表示MAC数据被加密了的情况下，将MAC数据中的MAC头以及地址数据作为解密处理对象外数据DDX输出，同时将除此之外的MAC数据作为第1解密处理对象数据DD1输出。另外，在MAC数据Encrypt信号表示MAC数据没有被加密的情况下，将MAC数据全体作为解密处理对象外数据DDX输出。

之后，第1解密处理对象数据DD1在第1位变换部分32中，被变换成作为解密处理单位的位宽的64位，并作为第2解密处理对象数据DD2而被输出。

另外，在TEK核对数据抽出部分33中，从延迟TEK处理数据DDTK中抽出用来选择TEK数据的TEK核对数据ITEK。也即，将TEK核对数据激活信号所表示的数据作为TEK核对数据ITEK而抽出并输出。在TEK核对数据抽出部分33中，利用TEK核对数据ITEK从数据存储缓存中抽出TEK数据TEK。

之后，在解密处理部分35中，使用第2解密处理对象数据DD2以及TEK数据TEK进行解密处理，将该处理的结果作为第1解密处理结果数据RD1。

接下来在第2位变换部分36中，将第1解密处理结果数据RD1变换为和解密处理对象外数据DDX相同的位宽的8位，将该变换结果作为第2解密处理结果数据RD2输出。在数据结合部分37中，将第2解密处理结果数据RD2和解密处理对象外数据DDX结合并作为结合数据CBD而输出之后，在第3位变换部分38中，将结合数据CBD变换成适合于数据存储装置14的位宽，并将该处理结果作为TEK处理结果数据RTEK输出给数据存储装置14。

另外，作为解密处理单位的64位，以及作为第2解密处理结果数据RD2的位宽的8位，并不仅限于该值，例如还可以在8×n（n：整数）位中自由的选择。

根据如上所构成的本发明，在由中心装置以及多个终端装置所构成的双向通信网中的数字双向通信扩展装置中，由CPU以及其他的TEK处理部分来实现MAC功能中的运算处理量很大的TEK功能的专用处理。这样，

在能够降低CPU的负荷的同时，还能够使电路规模适当化，进一步还提高了总处理能力，从而能够提高作为装置全体的性价比。

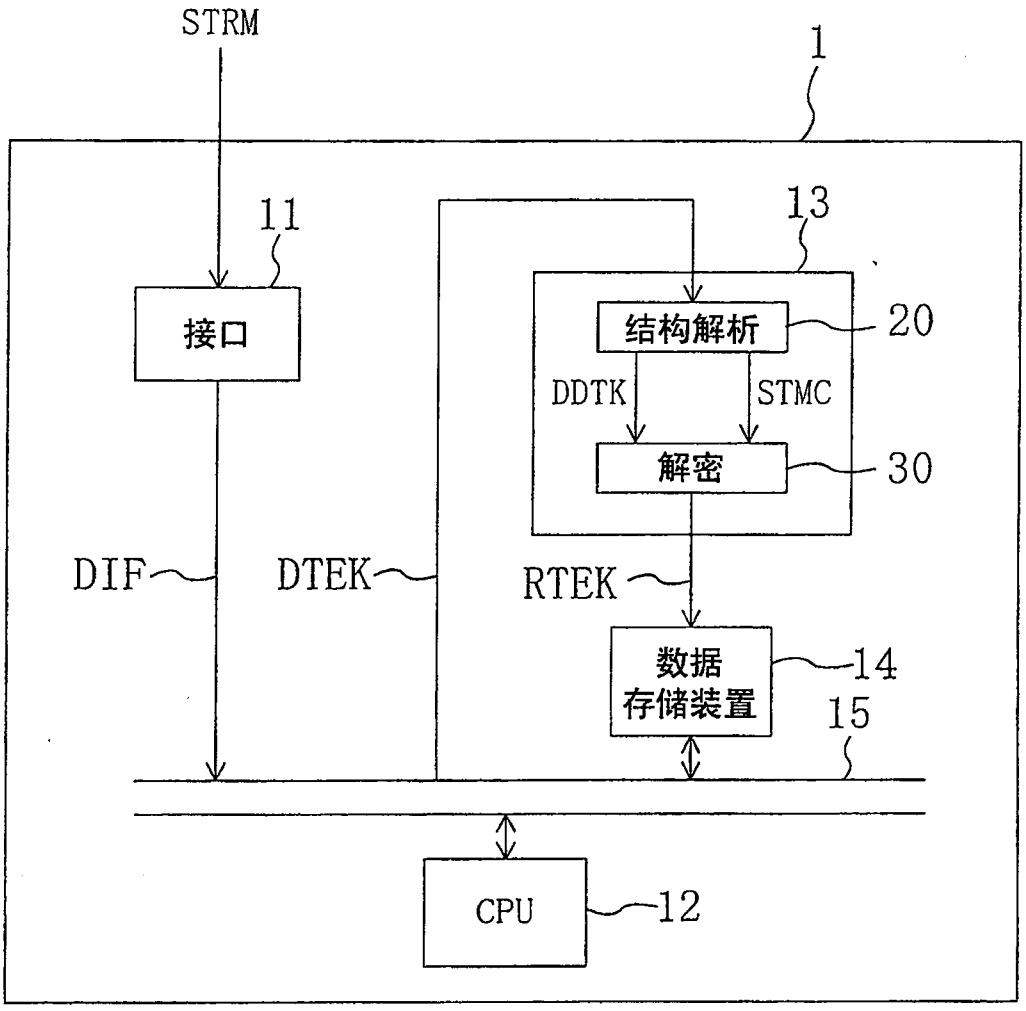

STRM
1
11
13
接口
结构解析
20
DDTK
STMC
解密
30
DIF
DTEK
RTEK
数据
存储装置
14
15
CPU
12

图 1

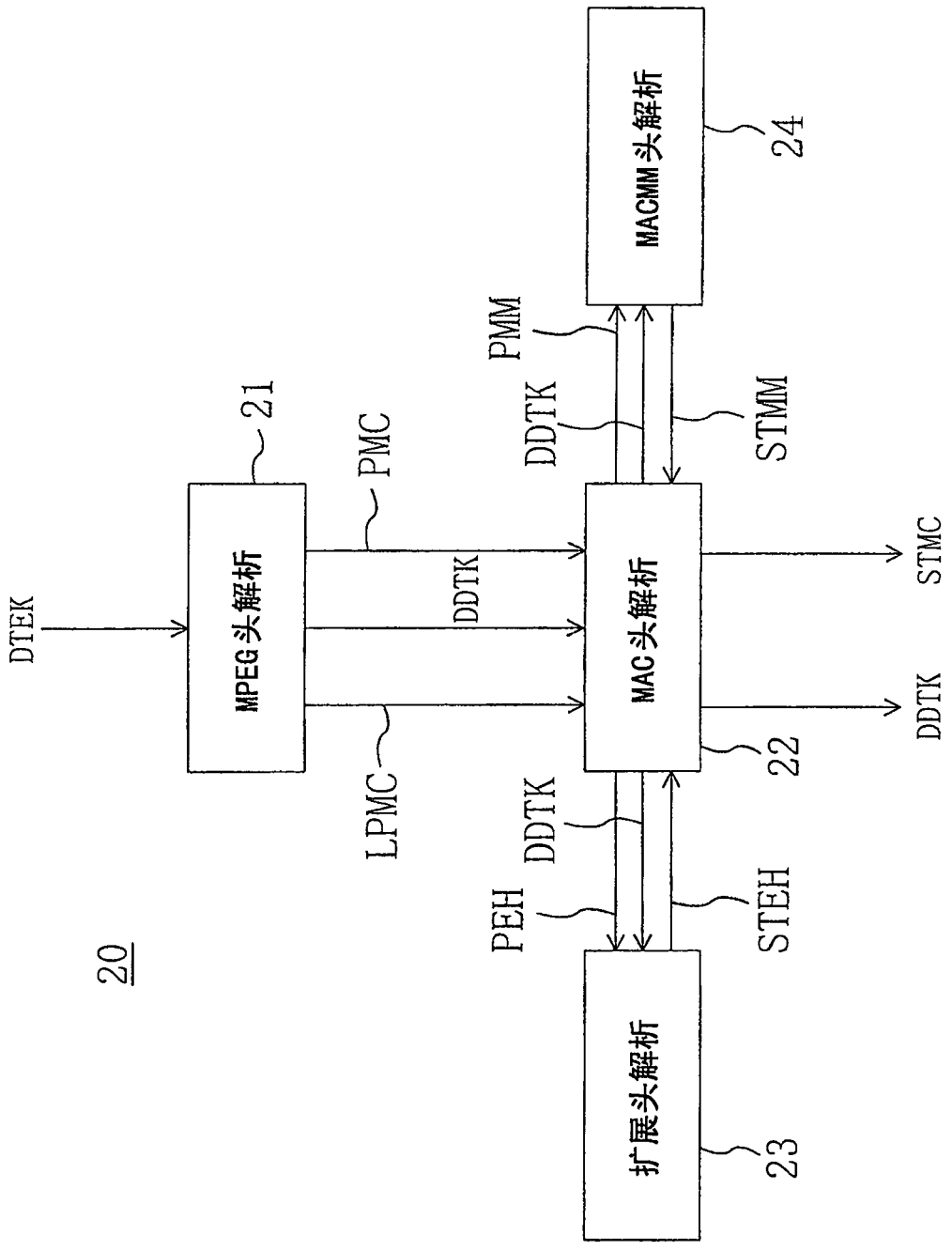

20
DTEK
MPEG头解析
21
PMC
LPMC
DDTK
MAC头解析
22
PMM
DDTK
STMM
MACMM头解析
24
STMC
DDTK
PEH
DDTK
STEH
扩展头解析
23

图 2

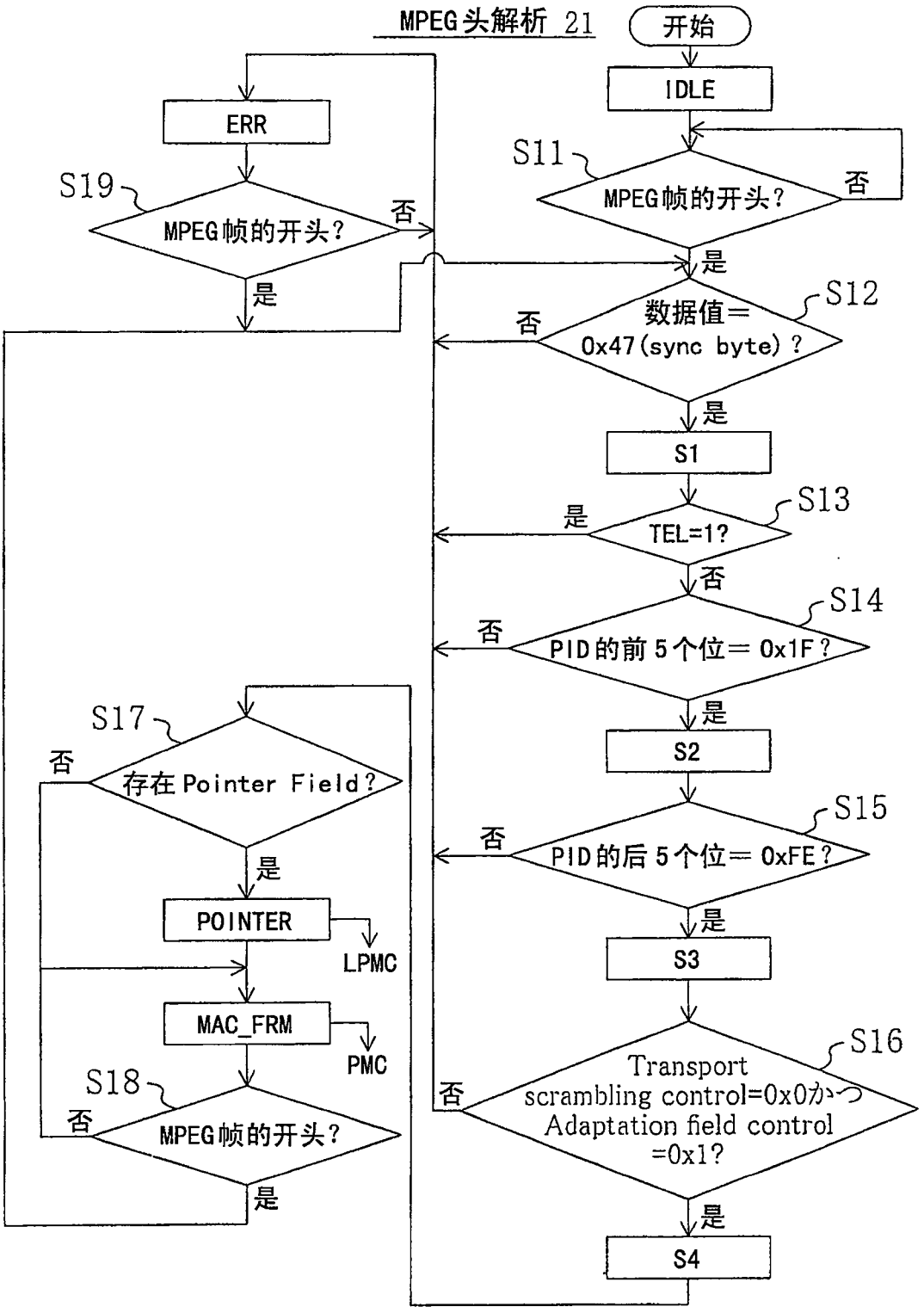

MPEG头解析 21
开始
IDLE
S11
MPEG帧的开头?
否
是
S12
数据值=
0x47(sync byte)?
否
是
S1
S13
TEL=1?
是
否
S14
PID的前5个位= 0x1F?
否
是
S2
S15
PID的后5个位= 0xFE?
否
是
S3
S16
Transport
scrambling control=0x0かつ
Adaptation field control
=0x1?
否
是
S4
ERR
S19
MPEG帧的开头?
否
是
S17
存在 Pointer Field?
否
是
POINTER
LPMC
MAC_FRM
PMC
S18
MPEG帧的开头?
否
是

图 3

Field	Length (bit)	Description
sync byte	8	0x47:MPEG Packet Sync Byte
transport error indicator (TEI)	1	0… 包中没有错误的情况 1… 包中有错误的情况
payload unit start indicator (PUSI)	1	0…没有pointer field区的情况 1…没有pointer field区的情况 *pointer field是MPEG帧的第 5byte PUSI是在其包中存在 payload 的开始时建立
transport priority	1	0(预约)
PID	13	DOCSIS Data-Over-Cable的情况下为0x1FFE
transport scrambling control	2	0(预约)
adaptation field control	2	1(在DOCSIS PID中不能使用该区)
continuity counter	4	PID的循环计数器

图 4

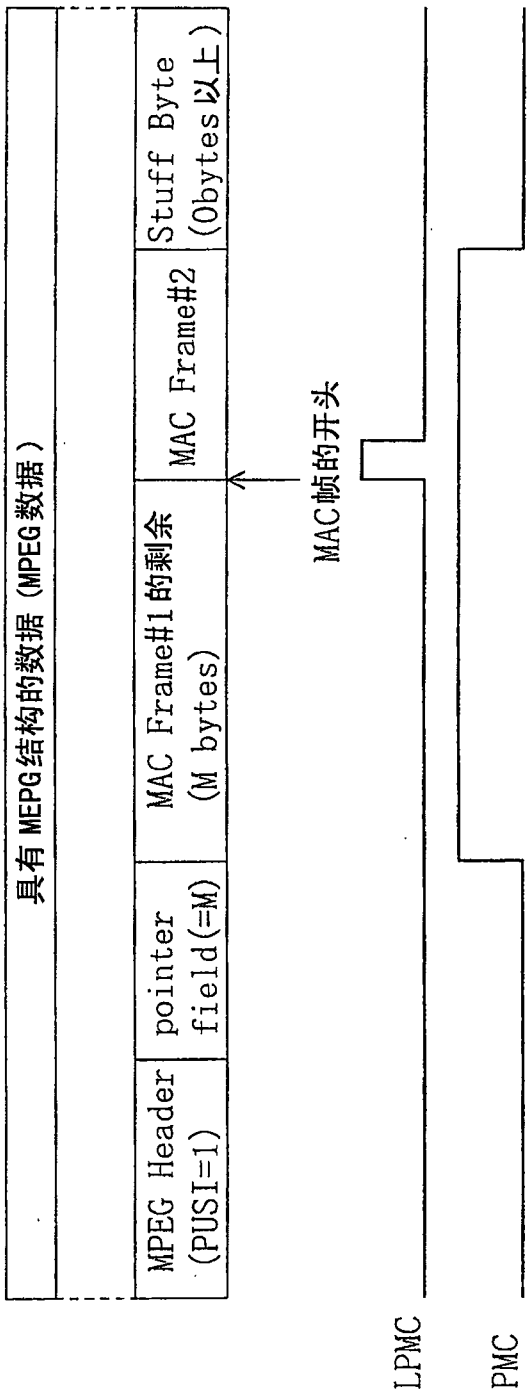

具有 MEPG结构的数据（MPEG数据）
MPEG Header (PUSI=1)
pointer field(=M)
MAC Frame#1的剩余 (M bytes)
MAC Frame#2
Stuff Byte (Obytes以上)
MAC帧的开头
LPMC
PMC

图 5

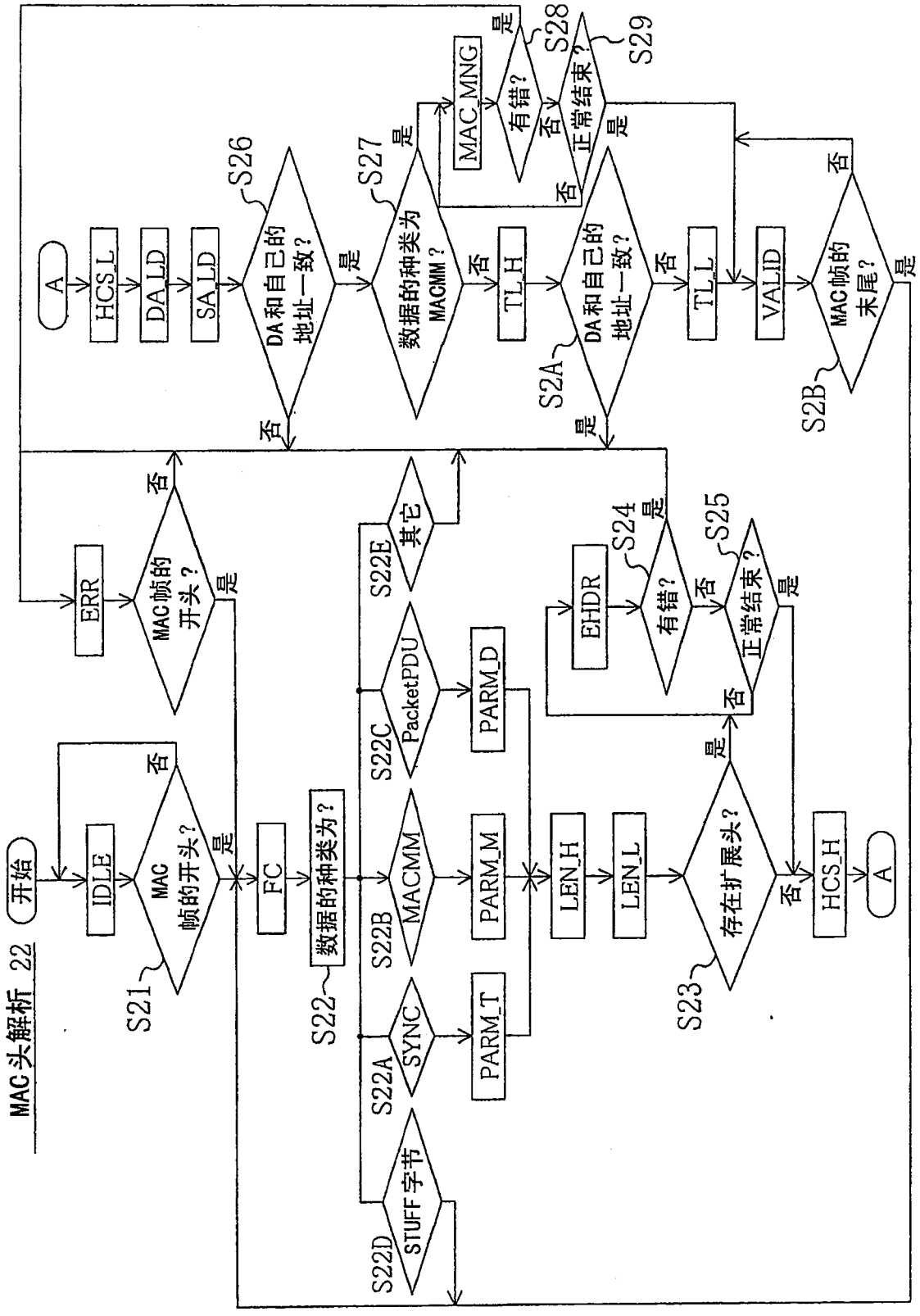

MAC头解析 22
开始
IDLE
MAC帧的开头？
否
是
S21
ERR
MAC帧的开头？
否
是
FC
数据的种类为？
S22
S22A
SYNC
PARM_T
S22B
MACMM
PARM_M
S22C
PacketPDU
PARM_D
S22D
STUFF字节
S22E
其它
LEN_H
LEN_L
存在扩展头？
是
否
S23
EHDR
有错？
是
否
S24
正常结束？
是
否
S25
HCS_H
A
A
HCS_L
DA_LD
SA_LD
DA和自己的地址一致？
否
是
S26
数据的种类为MACMM？
是
否
S27
MAC_MNG
有错？
是
否
S28
正常结束？
是
否
S29
TL_H
DA和自己的地址一致？
否
是
S2A
TL_L
VALID
MAC帧的末尾？
否
是
S2B

图 6

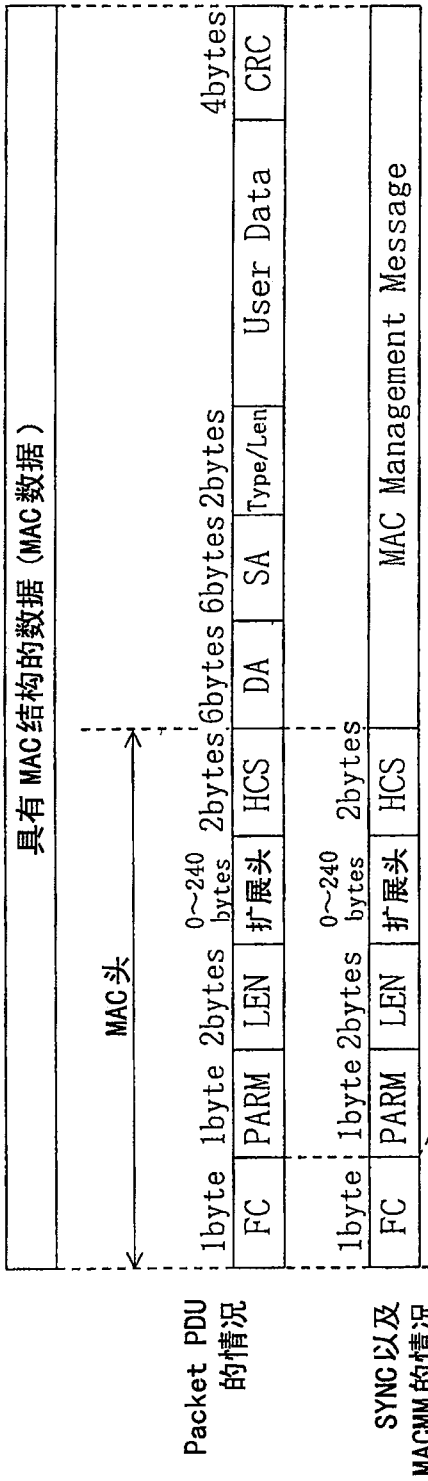

具有 MAC结构的数据（MAC数据）
MAC头
Packet PDU 的情况
SYNC以及 MACMM的情况
1byte
1byte
2bytes
0~240 bytes
2bytes
6bytes
6bytes
2bytes
4bytes
FC
PARM
LEN
扩展头
HCS
DA
SA
Type/Len
User Data
CRC
1byte
1byte
2bytes
0~240 bytes
2bytes
FC
PARM
LEN
扩展头
HCS
MAC Management Message
2bits
5bits
1bits
FC TYPE
FC PARM
EHDR_ON

图 7

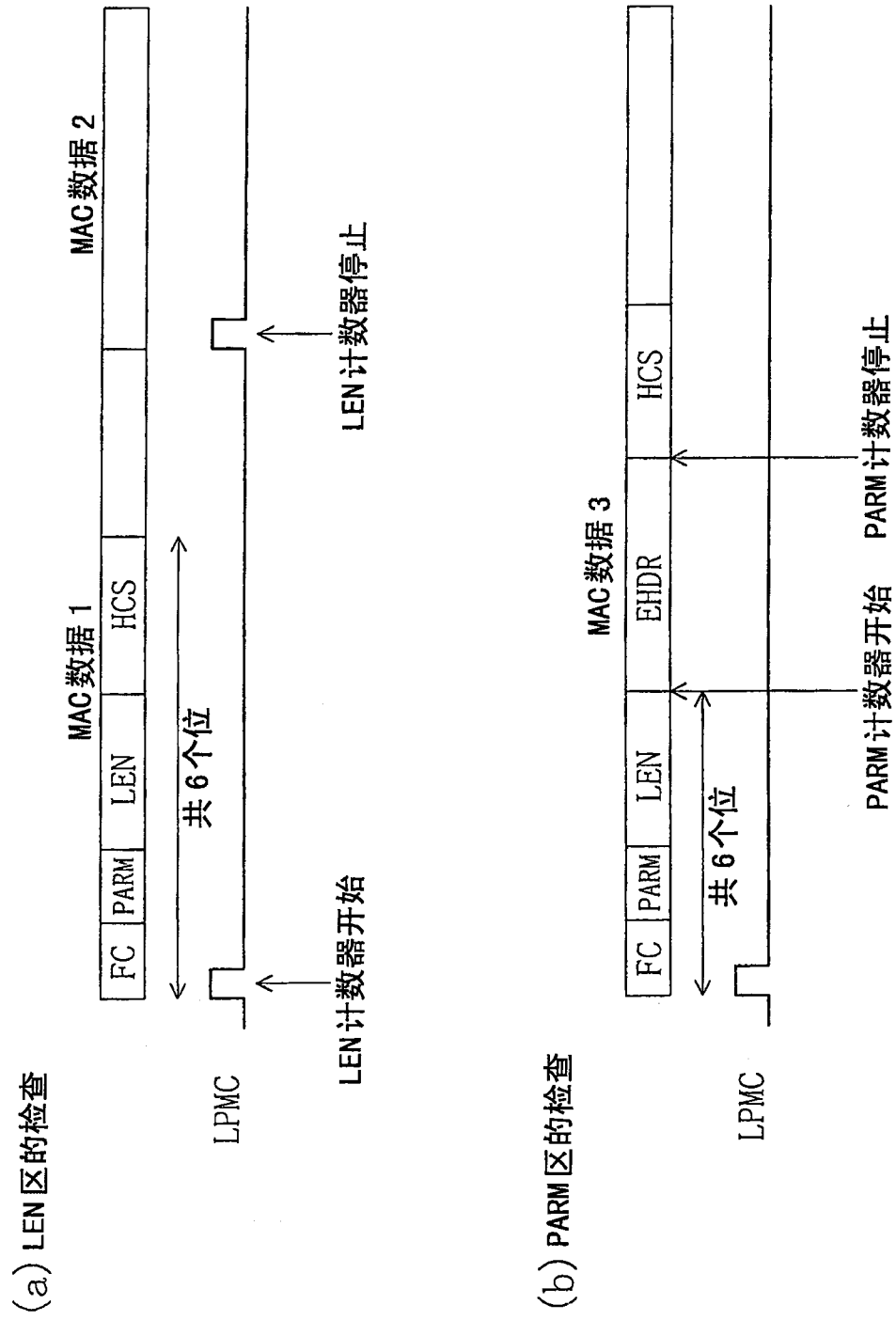

(a) LEN区的检查
MAC数据 1
MAC数据 2
FC
PARM
LEN
HCS
共6个位
LPMC
LEN计数器开始
LEN计数器停止
(b) PARM区的检查
MAC数据 3
FC
PARM
LEN
EHDR
HCS
共6个位
LPMC
PARM计数器开始
PARM计数器停止

图 8

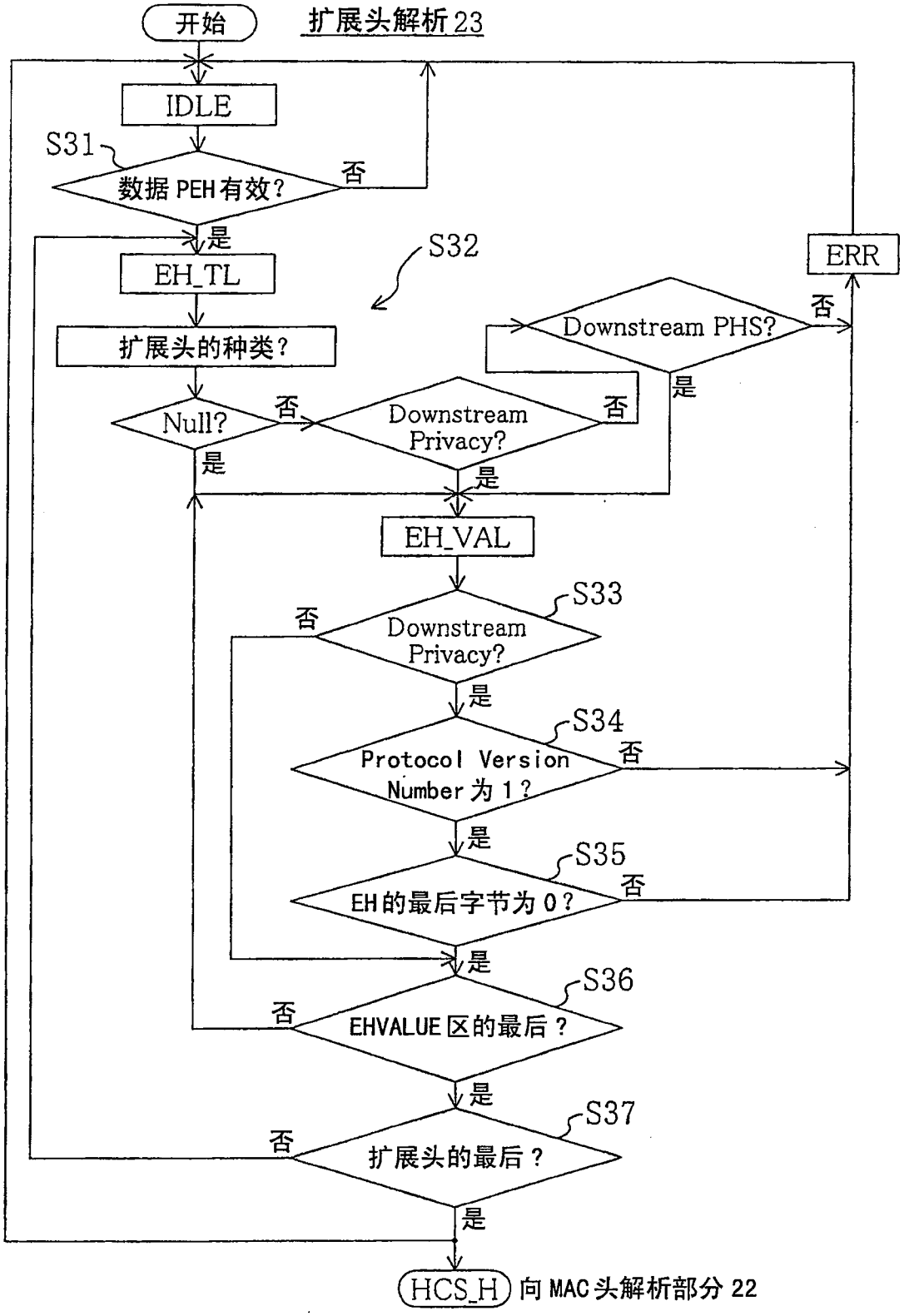

开始
扩展头解析23
IDLE
S31
数据 PEH有效?
否
是
EH_TL
S32
扩展头的种类?
Null?
否
是
Downstream Privacy?
否
是
Downstream PHS?
否
是
ERR
EH_VAL
S33
Downstream Privacy?
否
是
S34
Protocol Version Number 为 1?
否
是
S35
EH的最后字节为 0?
否
是
S36
EHVALUE 区的最后?
否
是
S37
扩展头的最后?
否
是
HCS_H
向 MAC 头解析部分 22

图 9

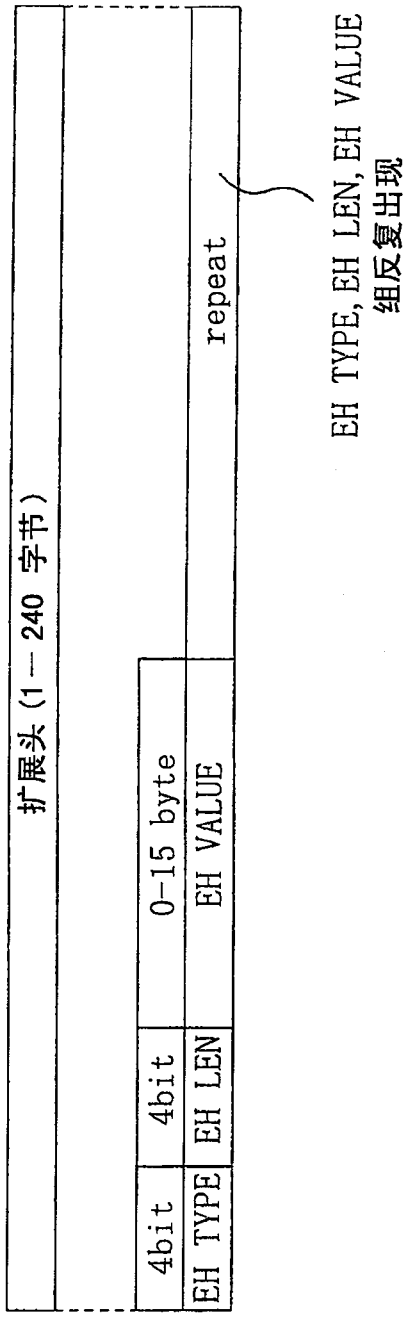

扩展头（1－240 字节）
4bit
4bit
0-15 byte
EH TYPE
EH LEN
EH VALUE
repeat
EH TYPE, EH LEN, EH VALUE
组反复出现

图 10

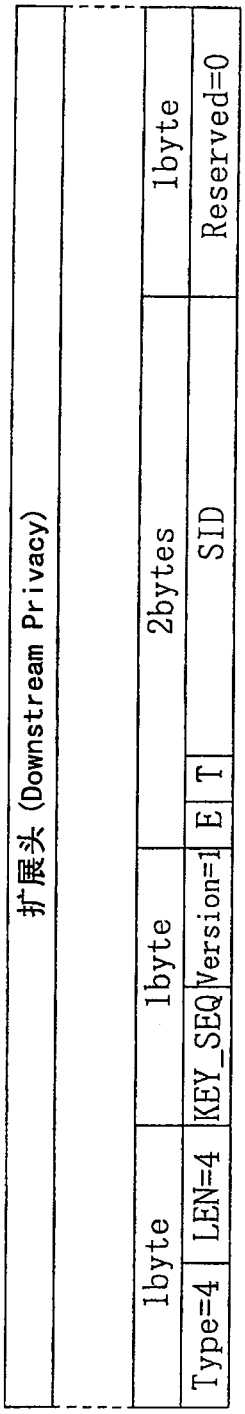

扩展头 (Downstream Privacy)
1byte
1byte
2bytes
1byte
Type=4
LEN=4
KEY_SEQ
Version=1
E
T
SID
Reserved=0

图 11

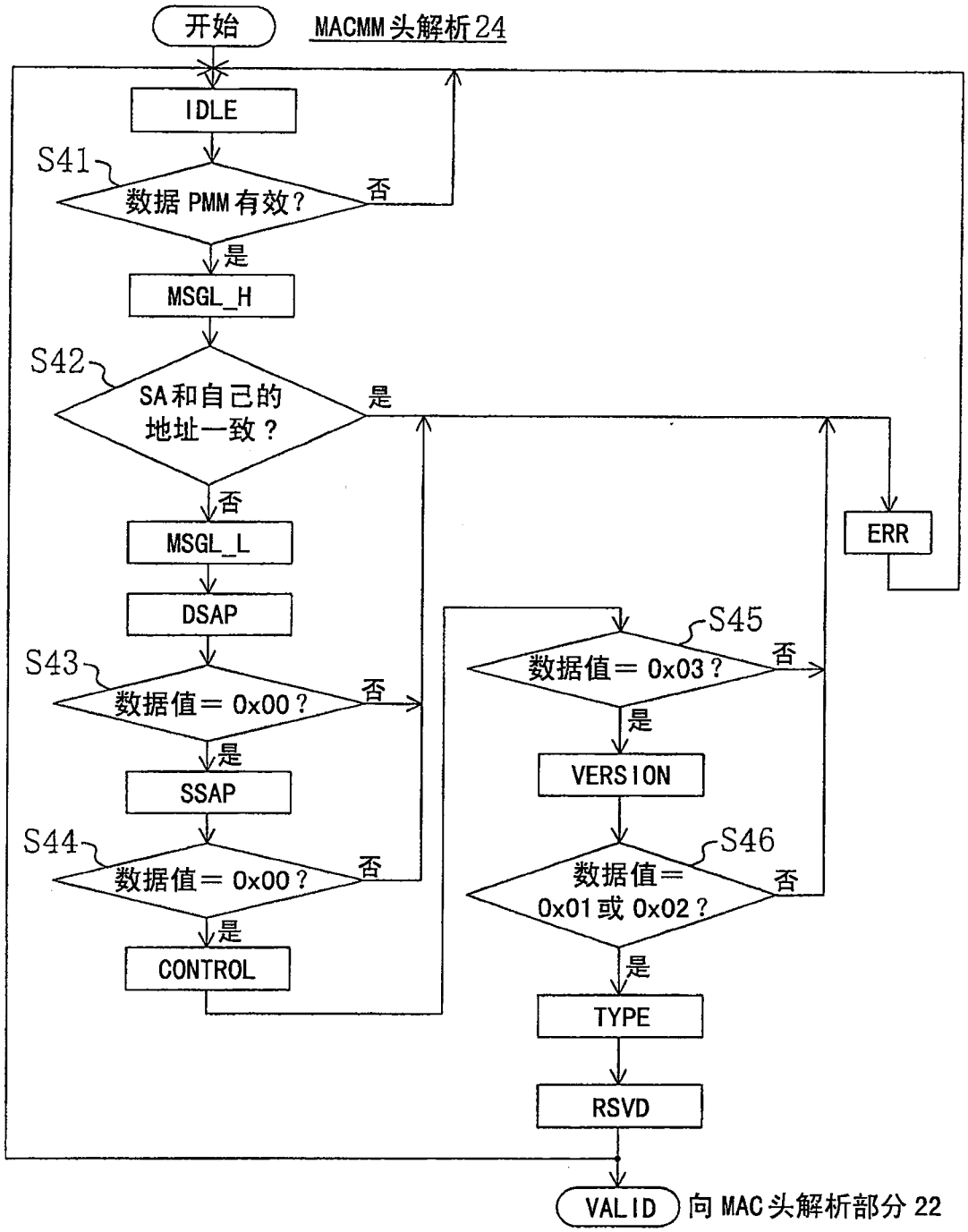

开始
MACMM头解析24
IDLE
S41
数据 PMM 有效？
否
是
MSGL_H
S42
SA和自己的
地址一致？
是
否
MSGL_L
DSAP
S43
数据值＝ 0x00？
否
是
SSAP
S44
数据值＝ 0x00？
否
是
CONTROL
ERR
S45
数据值＝ 0x03？
否
是
VERSION
S46
数据值＝
0x01或 0x02？
否
是
TYPE
RSVD
VALID
向 MAC头解析部分 22

图 12

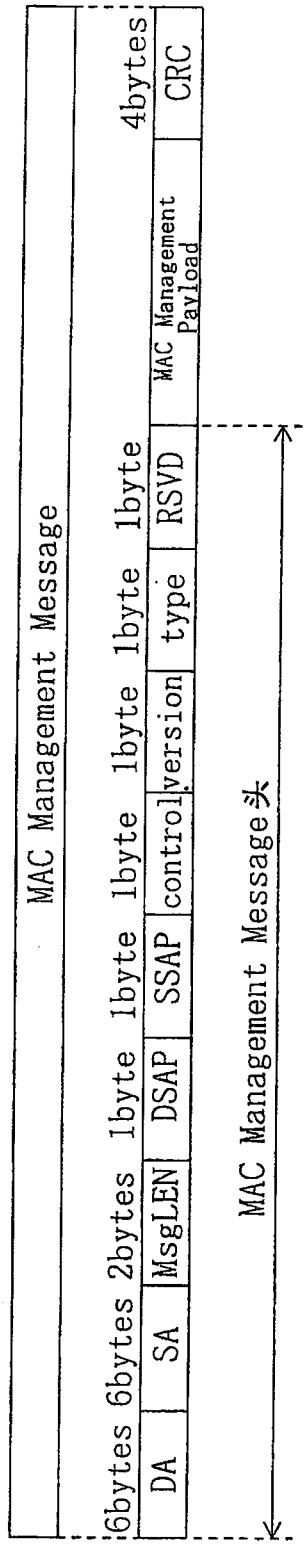

MAC Management Message
6bytes
DA
6bytes
SA
2bytes
MsgLEN
1byte
DSAP
1byte
SSAP
1byte
control
1byte
version
1byte
type
1byte
RSVD
MAC Management Payload
4bytes
CRC
MAC Management Message头

图 13

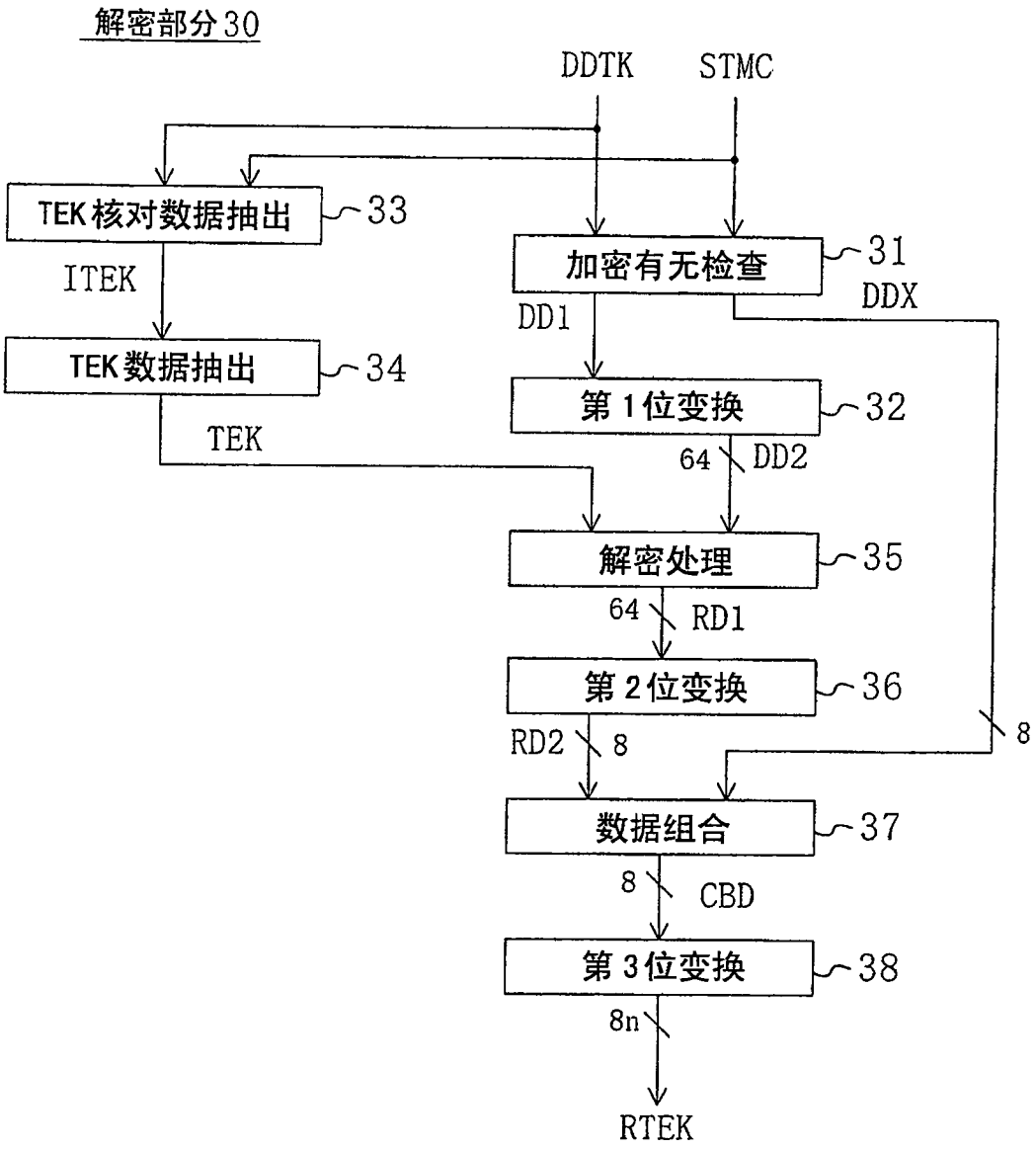

解密部分30
DDTK
STMC
TEK核对数据抽出
33
ITEK
TEK数据抽出
34
TEK
加密有无检查
31
DDX
DD1
第1位变换
32
64
DD2
解密处理
35
64
RD1
第2位变换
36
RD2
8
8
数据组合
37
8
CBD
第3位变换
38
8n
RTEK

图 14