抽象语法记法ASN.1
原理与应用

鲍忠贵　刘贵全

国防工业出版社
National Defense Industry Press

抽象语法记法 ASN.1 原理与应用

鲍忠贵　刘贵全　等编著

国防工业出版社
·北京·

内容简介

本书主要对信息技术中常用的 ASN.1 的抽象语法和编码规则进行了描述和研究，旨在让读者对 ASN.1 有一个既全面又深入的认识和理解。第 1 章对 ASN.1 背景进行了回顾，并且简要介绍了其语法。第 2 章详细介绍了 ASN.1 的语法基础。第 3 章逐一介绍了 ASN.1 的各种常用类型。第 4 章介绍了对象的抽象语法记法。第 5 章首先介绍了 ASN.1 语法的参数化赋值，然后介绍了其约束规范。第 6 章关于 ASN.1 编码规则，主要介绍了基本编码规则、非典型编码规则、正则编码规则以及紧缩编码规则。第 7 章我们还提供了几个应用实例，为读者进一步领悟 ASN.1 提供了很好的平台。第 8 章针对 ASN.1 语法与常用的 C 语言进行了映射，最后，附录部分我们给出了一些应用程序来帮助读者理解 ASN.1。

本书主要面向那些从事信息技术开发、信息化标准研究的学者和工程技术人员，特别是正在从事协议规范研究或基于 ASN.1 的协议实现方面的读者。

图书在版编目(CIP)数据

抽象语法记法 ASN.1 原理与应用 / 鲍忠贵等编著. —北京：国防工业出版社，2011.6

ISBN 978-7-118-07373-7

Ⅰ. ①抽… Ⅱ. ①鲍… Ⅲ. ①抽象语法 Ⅳ. ①TP301.2

中国版本图书馆 CIP 数据核字(2011)第 065388 号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号　邮政编码 100048）

国防工业出版社印刷厂印刷

新华书店经售

*

开本 787×1092　1/16　印张 12　字数 296 千字

2011 年 6 月第 1 版第 1 次印刷　印数 1—3500 册　定价 32.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422　　发行邮购：(010)68414474

发行传真：(010)68411535　　发行业务：(010)68472764

前　言

抽象语法记法(ASN.1)是一种 ISO/ITU - T 标准,是一种对数据和协议进行表示、编码、传输和解码的形式化描述方法。该标准可分成两部分,一部分是抽象语法,另一部分是传送语法。数据类型的 ASN.1 描述称为抽象语法,网络中对等实体之间通信时对用户信息的描述规则称为传送语法。ASN.1 的编码规则定义了它的传送语法,不同的编码规则定义不同的传送语法。

ASN.1 的应用非常广泛,如在协议描述、协议测试、综合业务数字网、ITU - T 和多媒体标准、PKCS、PKIX、SET 和其他安全相关的协议以及其他互联网规范等各方面的应用。

本书不仅详细描述了 ASN.1 抽象语法,而且在编码规则方面也给出了很细致的讲解。本书不是一般单纯地、笼统地介绍 ASN.1,而是从概念入手,结合示例,循序渐进地介绍了 ASN.1 抽象语法的语法基础及其类型。在对 ASN.1 有了初步认识之后,又对对象的抽象语法记法和 ASN.1 的参数化赋值与约束分别进行了讲解。在对 ASN.1 的这些抽象语法有了较深的认识和理解之后,本书开始描述 ASN.1 一些常用的编码规则。最终帮助读者真正熟练掌握所学习的 ASN.1 内容。

本书主要对 ASN.1 的抽象语法和编码规则进行了描述和研究,旨在让读者对 ASN.1 有一个既全面又深入的认识和理解。第 1 章对 ASN.1 背景进行了回顾,并且简要介绍了其语法。第 2 章详细介绍了 ASN.1 的语法基础。第 3 章逐一介绍了 ASN.1 的各种常用类型。第 4 章介绍了对象的抽象语法记法。第 5 章首先介绍了 ASN.1 语法的参数化赋值,然后介绍了其约束规范。第 6 章关于 ASN.1 编码规则,主要介绍了基本编码规则、非典型编码规则、正则编码规则以及紧缩编码规则。第 7 章给出了几个应用实例,为读者进一步领悟 ASN.1 提供了很好的平台。第 8 章针对 ASN.1 语法与常用的 C 语言进行了映射。最后,附录部分给出了一些应用程序来帮助读者理解 ASN.1。

本书主要面向那些从事协议规范或基于 ASN.1 的协议实现方面的读者。无论读者是刚刚接触 ASN.1 还是对 ASN.1 已经有了较深的认识,认真研读本书,都将在这方面获得新的认识和突破。我们也期待更多的对 ASN.1 有研究的读者对本书感兴趣。

鉴于目前 ASN.1 方面的书籍十分缺乏,作者结合自己这方面多年的工作体会与国内外的标准和研究成果编撰了此书,参考和引用的成果及文献在参考文献中列出,在此对其作者一并表示感谢! 由于作者水平有限,书中难免有不足之处,欢迎各位专家和读者不吝指正。

编者

2011 年 3 月于北京

目　录

第1章　抽象语法记法概述

1.1　问题的背景

在现代计算机技术中，不同的计算机系统之间、各种应用程序之间都需要进行大量的、复杂的信息交换和传递，例如移动电话、空中管制系统、空气污染检测系统等。目前，随着计算机通信网络技术的飞速发展和应用领域的日趋广泛，传统的支持远程登录、E－mail、文件传输以及万维网的通信技术逐渐走向成熟，而新兴的应用如电子钱包、网上拍卖、电子交易、视频点播等也得到了迅速的发展，这些系统也都要以网络间的信息交换和传递作为基础。对于这些需要传递和交换的信息，人们需要有一种详细而准确的规范来表示，以便不同的计算机系统、不同的应用程序和不同的网络之间能够传递这些信息，为此，人们需要制定相应的应用协议。

20世纪70年代，由于计算机技术和通信条件的限制，广泛采用字节序列的方式定义交换信息的详细内容，通过位、字节的编码和量化参数定义传输的标识、类型、长度和参数值，这种方法在链路层以下定义描述种类不是很多的协议信息，或者应用软件通过直接访问内存数据的应用背景下（如汇编或C语言等），证明是成功而有效的。但是随着TCP/IP网络的普及和应用，系统间的交互任务主要通过应用层的协议和信息的约定实现，通过字节序列的方式定义几十甚至上百上千种信息，已不能胜任任务需求的不断变化对灵活性、扩展性、可读性和自解释自适应性的要求。

那么，我们需要一种什么样的工具来定义或描述协议和协议数据单元，这种工具希望解决哪些问题？

1. 简化接口关系

在国际标准组织网络互联参考模型中，上三层（会话层、表示层和应用层）的信息交换具有以下几个特点：①数据结构的复杂性；②应用的分布性；③环境的异质性（包括不同的计算环境、不同的编程语言和不同的网络环境）。这就需要一种统一通用的高级语言对交换信息进行抽象描述，并通过编解码方法把应用层的数据与可传输的二进制码流进行有效转换。希望通过信息描述与编解码的分离，使得原先每个应用系统对每个信息交换定义不同的数据结构和解析处理，统一到对抽象语法的处理上，极大简化了系统的复杂度，如图1.1所示。

2. 找一种形式化的方法定义接口

以往的接口和协议主要通过图表和文字的方法定义数据结构，例如，表1.1是一种典型的传统描述方法，这种方法通过对传输字节（位图）的编排，定义传输的语义和数据结构，由于是直接面向字节或位图定义，支持的基本数据种类主要采用无符号二进制整数、二进制代码和二进制补码，并通过不同的数据字段长度和量化参数解析信息。随着试验信息系统综合业务的进一步开展和互操作性的进一步增强，字符、字符串、时间格式、实数和复杂结构数据将进一步得到应用，采用二进制表示方法将很难统一定义和描述。

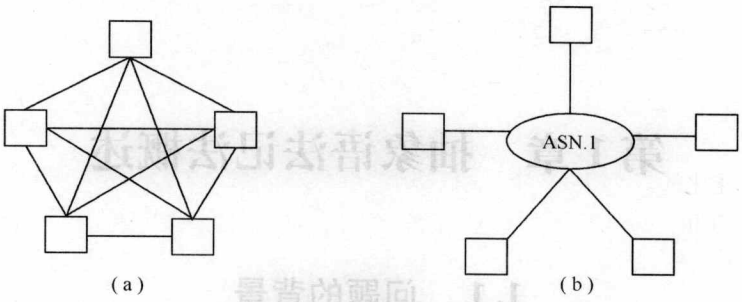

图 1.1　抽象语法标记法 ASN.1 对系统优化的示意

(a)端对端信息独立描述与处理示意；(b)端对端信息统一描述与处理示意。

表 1.1　一个典型的包交换格式

S	D	M	B	L	DATA
源标识	目的标识	任务标识	信息类别	数据域长度	数据域
1	1	1	1	2	N

我们希望抽象语法可以用精确的和形式化的方法描述应用层协议数据单元 PDU 及其他数据结构，能够屏蔽不同高级语言的编译特征，支持丰富的数据类型，如字节、整数、实数、字符串、逻辑数值定义和它们的任意组合，满足对复杂数据结构的定义。

3. 找一种快捷、稳定、灵活性和可扩展性的方法定义和描述接口

用抽象语法实现信息描述与编码的分离，从而使信息约定只关注与信息本身含义的描述，而不必关注在内存或传输线路上的位流编码，抽象语法描述的数据结构实例化后，由编码规则进行传输空间的位流和字节定义，从而使信息的描述与具体的数据耦合性降低，达到结构稳定，灵活性和可扩展性得到极大的提高。

同一种数据结构的描述，可以用不同的编码方案进行传输，以更好地适应不同的传输应用场景，例如，在带宽富裕和强调应用简单的场合可以采用信息冗余度高但处理简单的编码方案；在强调带宽利用率高的场合可以采用紧凑型的编码；在面向信息服务的应用场合可以采用面向 XML 的编码方案，但数据的描述是不变的。

4. 有成熟的方法解析和编码

技术是成熟可行的，已经实现了标准化的定义，并被广泛使用，从而保证技术和应用的投入是持续发展的。

1.2　ASN.1 简介

ITU－T 组织制定的 ASN.1(Abstract Syntax Notation One)标准，正是针对上述问题提出的一整套完整的解决方案。它提供了丰富的数据类型和高效多样的编解码规则，适合描述复杂的通信协议，使得多个制造商设备之间，不同的应用系统之间可以进行有效无误的数据传输。

ASN.1 标准可分成两部分，一部分是抽象语法，一部分是传送语法。数据类型的 ASN.1 描述称为抽象语法记法，网络中对等实体之间通信时对用户信息的描述规则称为传送语法。ASN.1 的编码规则定义它的传送语法，不同的编码规则定义不同的传送语法。这些编码规则(如 BER，PER)相当于从局部语法到传送语法之间的转换规则。将 ASN.1 描述的数据转换成

二进制数据流，通信双方在交互信息之前，对要传输的数据进行 ASN.1 数据类型的抽象描述，按照编码规则将数据转换成字节流，接收方将接收到的数据按照相应的解码规则转换成原始数据，由于编码规则可以保证数据的正确解释，这样双方尽管是不同的操作系统，但只要按照相同的规则和同一种语法描述作数据解析就可以保证数据的正确性。

国际相关标准化组织如 ISO、ITU－T、ITEF、OMG 和 CCSDS 以及一些国际公司如 IBM、微软和 SUN 等，从 20 世纪 80 年代起，就开展了这些方面的研究和设计，先后制定了各种系统互连和信息交换标准和技术。其中抽象语法记法 ASN.1 由于具有良好的适应性，目前已被各标准化组织广泛采用，并在目标系统中进行了很好的应用。

ASN.1 的研究起始于 1982 年，1986 年发布国际标准，即 ISO 8824:1986《信息技术 开放系统互连 抽象语法记法——(ASN.1)规范》和 ISO 8825:1986《信息技术 开放系统互连 抽象语法记法——(ASN.1)基本编码规则规范》，之后该国际标准被多次修订、补充、完善，先后经历了 1990 年版、1998 年版、2002 年版，目前仍在不断补充、完善。至今已形成了包括 XML 记法和编码规则在内的几种规范记法和编码规则。依据国际标准，我国已经制定了抽象语法记法及其编码规则的系列国家标准，具体如下：

GB/T 16262.1《信息技术 抽象语法记法 1(ASN.1):基本记法规范》；

GB/T 16262.2《信息技术 抽象语法记法 1(ASN.1):对象规范》；

GB/T 16262.3《信息技术 抽象语法记法 1(ASN.1):约束规范》；

GB/T 16262.4《信息技术 抽象语法记法 1(ASN.1):ASN.1 规范的参数化》；

GB/T 16263.1《信息技术 ASN.1 编码规则:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)的规范》；

GB/T 16263.2《信息技术 ASN.1 编码规则:紧缩编码规则(PER)规范》。

目前 ASN.1 已在信息处理系统和通信领域得到了广泛应用，成为开发应用协议的常用工具。下面是 ASN.1 具体的应用：

(1)Internet 上的声音和视频、电子商务、数字证书、电子邮件、无线寻呼以及不断出现的新技术，如交互式电视、财经服务系统、使用 ASN.1 的网络和计算操作系统及其编码规则；

(2)微软 Internet 浏览器、NetMeeting 和 Outlook；诺基亚、爱立信和摩托罗拉的无线应用；Internet 上提供信用卡交易安全性的加密技术；生物测定学、ATM 交易、800 号码呼叫路由、飞机起飞和着陆等均用到了 ASN.1；

(3)汽车和卡车的诊断监视系统，设备生产的故障检测系统。

以下几点使得 ASN.1 成为广泛使用的规范记法：

(1)ASN.1 是国际标准化的，与供应商、平台及语言无关的一种高级抽象的数据结构的记法；

(2)在计算机网络上进行传送时，有将数据结构值表示为精确的位形式的规则规范；

(3)支持多数平台和编程语言工具，能够实现和高级语言很好的映射；

(4)有良好的可扩展性支持，多种编码规则的发展，可以满足多种条件下的协议与接口的定义。

本书将从语法、基本类型、面向对象、编码规则、应用实例等几个方面，力求采取通俗易懂的方式，介绍 ASN.1 的语法与应用。

1.3 ASN.1 和网络协议

计算机协议可以定义为一组被完善定义的信息集合，集合里的每条信息都包含了一种既定

的含义和操作的规则。一个协议很少单独使用,它往往是某个协议栈的一部分。协议栈中多个独立的协议规范共同决定一个完整信息的发送,例如一些协议规范负责中间节点或者交换节点之间的信息交换,另一些协议规范保证远程终端的信息正确性。这就是“分层协议技术”。

在这种分层协议中,一些协议定义了信息包的包头部分,而把剩余的“孔”预留,它提供了一种能够传输“孔”中信息的服务,而另一些协议则定义了这些“孔”的内容。

图 1.2 描述了 TCP/IP 协议栈,协议栈中网络接口层负责底层信息的传输,它的信息头部分包含了自身协议规范,尾部则是循环冗余校验部分(保证信息的正确性),中间的“孔”则填充了 IP 协议的所有信息。同样 IP 层信息包的“孔”也包含了其上层协议 TCP 协议的所有信息,最后用户所需发送的信息被填充到了 TCP 信息包的“孔”中得以发送。

在这种模式中,每层服务的精确性都要由其下层服务来保证,而且当一层服务在调用其下层服务之前,必须要先知道其下层服务的一些控制参数。

其实协议栈中,IP 包可以携带 TCP 信息,也可以携带 UDP 信息,它们分别提供了不同的服务。可以看出分层协议的一个很重要的优点就是,低层服务可以支持很多高层服务,即使这些低层服务在被发明时还未考虑到这些高层服务。当多种不同服务被填充在低层服务的“孔”中时,图 1.2 就演变成图 1.3。

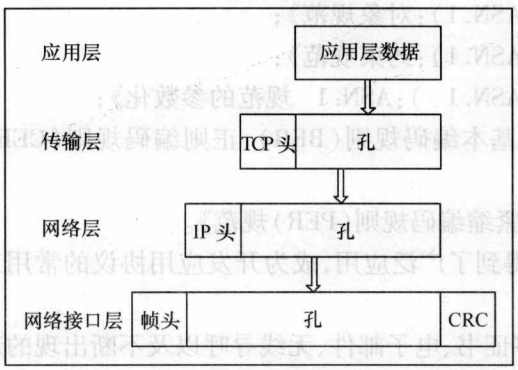

图 1.2　简单 TCP/IP 协议栈

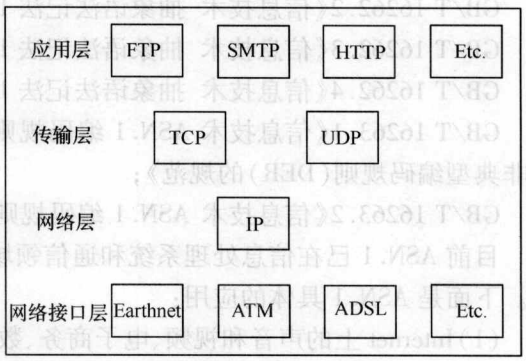

图 1.3　TCP/IP 分层协议

分层理论在国际标准化组织提出的网络协议七层模型中体现得很清楚,如图 1.4 所示。

尽管模型中很多协议在实际应用中并没有用到,但是这个标准仍然是学习网络协议规范的一个很好的理论。在这个 20 世纪 70 年代末提出的模型中,有六层协议都提供运载服务,只有最上面一层应用层中没有“孔”。但是在 80 年代,越来越多的人希望在应用层中也留下“孔”,为以后的扩展做准备或者使他们的协议能够胜任特殊的用途。例如,SET(Secure Electronic Transactions)协议不但具有详细的规则描述,而且提供了一定数量的“孔”,可以利用这些“孔”来传递那些并没有在 SET 协议中定义的信息。所以可以利用协议中的基本规范来发出请求、做出应答等,而利用这些“孔”来传递特殊信息。

“孔”其实就是在本协议中未定义的预留信息,而这些信息是被其他协议或者应用定义的。例如 IP 协议包中“孔”所携带的就是 TCP 或者 UDP 所定义的信息。

能不能很好地提供这些“孔”来满足应用的需要,这点已经是衡量一个协议好坏的标准了。在过去的几十年中,ASN.1 在这方面做得很好,本书的后半部分将详细讨论 ASN.1 在网络协议中的应用。

早期的协议都运行在单一链路上,并且这些协议规范都是与单独的硬件相对应的,不同的

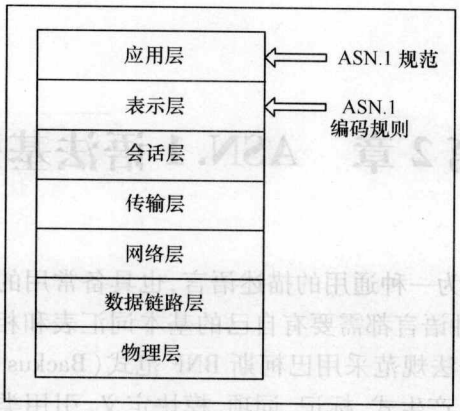

图 1.4　OSI 网络协议模型和 ASN.1

硬件使用不同的协议来实现应用程序间的通信，这就造成了，如果要运行不同的应用程序就需要重新定义、构建硬件系统。分层理论的一个重要优点在这就显而易见了，它能够增强硬件系统的可复用性，从而支持更多不同的高层协议和应用，就像图 1.2 里显示的那样。

ASN.1 就诞生在这种分层协议中，它运作的前提是已经有下层协议完成了在网络中寻址、纠错、正确传输等功能。在 ASN.1 层中，假设已经可以保证八位位组数据在不同机器间的可靠传输（注意，ASN.1 定义的所有信息都是八位位组的整数倍），如图 1.5 所示。

尽管如此，还是有许多基于 ASN.1 的应用程序在使用 ASN.1 之前调用了其他的服务规范来填充 ASN.1 中的“孔”，这些规范大多都是由其他不同的组织确定的（图 1.6）。在本书的后半部分将谈到，在 ASN.1 规范中有许多机制用来支持“孔”和“层”的运用。

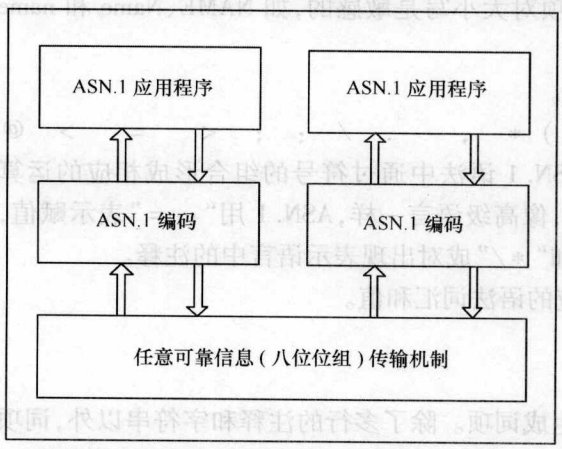

图 1.5　ASN.1 通信应用

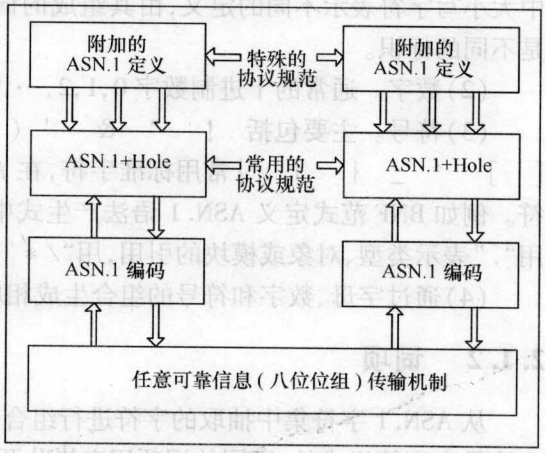

图 1.6　ASN.1 与协议

分层是一个重要的思想，它可以在不影响其他协议的前提下，大大提高协议规范的可复用性和扩展性。但是为了实现特定的应用，就需要考虑更多不同的规范，使这些规范能协同运作，而当这一应用在不同环境下执行的时候，将不能保证那些规范还能保持精确的协同性。

所以，设计一种适用性强、生命力持久的协议来保证整体协议的简单、精确是非常重要的。显然，这种协议就是 ASN.1。ASN.1 使得应用层之间的通信变得简单、快捷，它支持分层理论和可扩展性，而且在应用中完全由开发者决定是否使用该协议。ASN.1 是一个强大的规范，关于它具体的优点和优势将在后面章节详细介绍。

第2章　ASN.1语法基础

顾名思义，抽象语法作为一种通用的描述语言，也具备常用的BASIC、C和C++等计算机语言的相应规范。任何一种语言都需要有自己的基本词汇表和相关的语法定义，在国际标准化组织术语中，ASN.1的语法规范采用巴柯斯BNF范式(Backus Normal Form)定义。本章将介绍ASN.1的基本词汇表、产生式、标记、词项、模块定义、引用类型和值的定义、类型和值的定义与赋值等内容，这些内容构成了ASN.1的语法的基础，也是理解和描述后续章节内容的基础。

2.1　词汇及词法约定

2.1.1　字符集

ASN.1的字符集采用GB/T 13000.1—1993标准中规定的字符子集，不含中文字符，主要包括：

(1)字母。A,B,…,Z,a,b,…,z共26个拉丁大写字母和26个拉丁小写字母，在ASN.1中大小写字符表示不同的定义，由其组成的词项对大小写是敏感的，如NAME、Name和name是不同的标识。

(2)数字。通常的十进制数字0,1,2,…,9。

(3)符号。主要包括　！　"　&　'　(　)　*　,　-　.　/　:　;　<　=　>　@　[　]　^　_　{　|　}常用标准字符，在ASN.1语法中通过符号的组合形成相应的运算符。例如BNF范式定义ASN.1语法产生式中，像高级语言一样，ASN.1用“::=”表示赋值，用“.”表示类型、对象或模块的引用，用“/*”和“*/”成对出现表示语言中的注释。

(4)通过字母、数字和符号的组合生成相应的语法词汇和值。

2.1.2　词项

从ASN.1字符集中抽取的字符进行组合生成词项。除了多行的注释和字符串以外，词项应该是由字符组成的，不同的词项用空格分开。在ASN.1语法中，行的长度是不受限制的。

在ASN.1语法中，基本的词项有：

1. 类型引用或模块引用

定义一种类型或模块的名称，由一个或多个字母、数字和连字符(-)组成，以大写字母开头，不能用连字符结尾，连字符不能紧接着另一个连字符，双连字符“--”已经定义为单行的注释。以下是类型和模块定义的示例。

示例1：系统保留的类型

例如，通用时间GeneralizedTime、字符CHARACTER。

示例2：用户自定义的类型UserName

```
UserName::=SET {
  personalName          [0] VisibleString,
  organizationName      [1]  VisibleString OPTIONAL,      --默认为"None"
  countryName           [2] VisibleString OPTIONAL,       --默认为"China"
}
```

示例3:CCSDS SLE传输服务公用模块的定义

```
CCSDS-SLE-TRANSFER-SERVICE-COMMON-TYPES
{ iso org(3) standards-producing-organization(112) ccsds(4)
space-link-extension(3) sle-transfer-services(1)
forward-cltu-service(2) version-one(1) asn1-common-types(1)
}
DEFINITIONS
IMPLICIT TAGS
::= BEGIN
/*模块体*/
.....
END
```

2. 标识符或值引用

标识符或值也是由一个或多个字母、数字和连字符(-)组成,不过与类型和模块名不同,标识符或值是以小写字母开头,不能用连字符结尾,连字符不能紧接着另一个连字符。在前面用户自定义的类型 UserName 中,personalName、organizationName、countryName 都是合法的标识符。

在 ASN.1 词项的保留字中,有些值是固定用大写表示的,如 NULL(空)、TRUE(布尔值真)、FALSE(布尔值假)等。

3. 注释

也称注解(GB/T 16262.1—2006),ASN.1 中有两种注释形式:一种以"--"开始的一行注释;另一种是以"/*"开始,以"*/"结束的多行注释。注释本身没有语法意义,只作为帮助理解语法的说明,不参与编解码的过程。

4. 数

由一个或多个0,1,2,…,9个数字组成的整数。

5. 实数

即高级语言中的浮点数或双精度浮点数,表示形式可以用3.14表示,也可以用314E-2表示。

6. 二进制数串

由0和1组成的二进制数,需要用一对单引号标示,数字后用字符B表示,如'0110'B。

7. 十六进制数串

由A、B、C、D、E、F和0,1,2,…,9组成的十六进制数,需要用一对单引号标示,数字后用字符H表示,如'3F4B'H。

8. 字符串

用一对双引号" "引用的字符序列和图形符号。特别地,如果字符串中包含双引号,则用一对双引号表示一个双引号。如"ABC"表示字符串ABC,"AB" "C"表示字符串AB"C。

9. 赋值符号

用“::=”表示给标识符赋值或给类型、模块定义。例如：

给标识符赋 pi 值，即

pi REAL ::= 3.14

定义类型和模块可以参考前面的示例。

10. 其他词项

还包括范围分隔符(..)，省略号(…)，版本括号([[、]])和基于 XML 语言扩展的二进制数、十六进制数、字符串、XML 开始与结束标记等。

11. 保留字

以下一些标识符为 ASN.1 语法专用，在其他文献中也称关键字。本章节中不对以下保留字进行详细介绍，我们将在后续的章节中陆续介绍使用。

ABSENT	ENCODED	INTEGER	RELATIVE – OID
ABSTRACT – SYNTAX	END	INTERSECTION	SEQUENCE
ALL	ENUMERATED	ISO646String	SET
APPLICATION	EXCEPT	MAX	SIZE
AUTOMATIC	EXPLICIT	MIN	STRING
BEGIN	EXPORTS	MINUS – INFINITY	SYNTAX
BIT	ENTENSIBILITY	NULL	T61String
BMPString	EXTERNAL	NumericString	TAGS
BOOLEAN	FALSE	OBJECT	TeletexSting
BY	FROM	ObjectDescriptor	TRUE
CHARACTER	GeneralizedTime	OCTET	TYPE – IDENTIFIER
CHOICE	GeneralString	OF	UNION
CLASS	GraphicString	OPTIONAL	UNIQUE
COMPONENT	IA5String	PATTERN	UNVERSAL
COMPONENTS	IDENTIFIER	PDV	UniversalString
CONSTRAINED	IMPLICIT	PLUS – INFINITY	UTCTime
CONTAINING	IMPLIED	PRESENT	UTF8String
DEFAULT	IMPORTS	PrintableString	VideotexString
DEFINITIONS	INCLUDES	PRIVATE	VisibleString
EMBEDDED	INSTANCE	REAL	WITH

2.2 文　法

2.2.1 产生式

ASN.1 用 BNF 产生式来定义新的语法，通过定义词项和词项允许的序列，形成新的语法结构。例如定义一个布尔值的产生式为

```
BooleanValue ::= TRUE |FALSE
```

表示该布尔类型的值是 TRUE 或者是 FALSE。

在 ASN.1 中，产生式由以下几个方面组成：①需要定义的新词项，可以是类型、值、模块等；②赋值符号“::=”；③一个或多个分割符“|”，表示多个可选的项。在国标 GB/T 16262.1-2006 和 ITU-U X680 中，给出了一个通用的产生式样例：

```
ExampleProduction  ::=
        bstring     |
        hstring     |
        "{"  IdentifierList  "}"
```

该示例表示 ExampleProduction 可以是任何一个二进制字符串或十六进制字符串，或是在括号中列举的字符串。

产生式支持递归定义，支持缩写，其中主要有以下三种缩写方式。

1. 星号(*)缩写记法

表示产生式可以是空“empty”，或是以第一个词项开始和结束的序列，如：

```
C::= AB*
```

等价于

```
C::= D |empty
D::=A |ABD
```

即 C 可以是以下序列：

```
empty
A
ABA
ABABA
.....
```

2. 加号(+)缩写记法

与星号(*)类似，只是不包括空“empty”。

3. 问号(?)缩写记法

表示空“empty”或与问号前相关词项，如：

```
F::=A?
```

等价于：

```
F::= empty |A
```

2.2.2 标签

在早期的 ASN.1 语法中，标签(tag)(也称标记)是一个非常重要的概念。这是因为基于 BER 的编码方案需要通过标签来确定数据类型。随着近十年的发展变化，特别是考虑到用户可扩展性的需要，紧缩编码规则(PER)和自动标签(AUTOMATIC TAGS)置标环境的应用，标签的重要性已经降低，但仍是语法中需重点阐述的概念。标签值可以唯一区分 ASN.1 类型。也就是说，ASN.1 类型的名字并不影响它的抽象含义，只有标签才有这个作用。在 ASN.1 语法中，除了 CHOICE 和 ANY 类型以外，每种类型都有一个标签，标签由一个标签类和一个非负的标签数组成。有四类标签：

(1)通用标签类(Universal)。该类的标签包括整数、实数、字符串等基本的数据型，含义在所有的应用中都相同。

(2)应用标签类(Application)。该类型可以为用户提供自定义的数据类型，包括各种组合