



中华人民共和国通信行业标准

YD/T 2937-2015

扩展消息与表示协议 (XMPP) 地址格式

Extensible messaging and presence protocol (XMPP)
— Address format

2015-07-14 发布

2015-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 缩略语.....1

4 地址.....1

 4.1 基础.....1

 4.2 域部分.....2

 4.3 本地部分.....3

 4.4 资源部分.....3

5 国际化事项.....4

6 安全性事项.....4

 6.1 Stringprep的重用.....4

 6.2 Unicode的重用.....4

 6.3 地址欺骗.....4

7 IANA事项.....6

 7.1 Stringprep的Nodeprep文本.....6

 7.2 Stringprep的Resourceprep文本.....6

8 一致性要求.....6

附录A（规范性附录）Nodeprep.....8

附录B（规范性附录）Resourceprep.....10

前 言

本标准是XMPP系列标准之一，本系列标准的名称和结构预计如下：

- 扩展消息与表示协议 核心协议；
- 扩展消息与表示协议 即时消息与表示；
- 扩展消息与表示协议 地址格式；
- 扩展消息与表示协议 端到端的签名与对象加密。

本标准按照GB/T1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：重庆邮电大学、中国信息通信研究院、国家电网公司信息通信分公司。

本标准主要起草人：王 平、王 恒、王 浩、唐晓铭、李瑞雪、谢昊飞、罗志勇、严 冬、兰 飞、赵 锋、张 炎、谢金凤、刘建明、陈 星。

扩展消息与表示协议 (XMPP)

地址格式

1 范围

本标准规定了扩展消息与表示协议 (XMPP) 的地址格式, 以便于在任意两个或多个网络实体之间接近实时的消息通信。该地址格式重用了“stringprep”技术来预备非ASCII字符串STRINGPREP, 包括用于国际化域名的名字空间规范, 对应于两个XMPP特有的用于localpart(本地部分) 和resourcepart(资源部分)的规范。

本标准适用于即时通讯系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件, 仅所注日期的版本适用于本文件。凡是不注日期的引用文件, 其最新版本 (包括所有的修改单) 适用于本文件。

- IETF RFC1035 域名的实现与定义 (Domain names - implementation and specification)
- IETF RFC3454 国际化字符串的预配置 (Preparation of Internationalized Strings ("stringprep"))
- IETF RFC3987 国际化资源标识符 (Internationalized Resource Identifiers (IRIs))
- XSF XEP-0045 多用户聊天协议 (Multi-User Chat)

3 缩略语

下列缩略语适用于本文件。

HTTP	Hyper Text Transport Protocol	超文本传输协议
IQ	Info/Query	信息/查询
IRIs	Internationalized Resource Identifiers	国际化资源标识符
JID	Jabber Identifier	标识符
Nameprep	Preparation of Internationalized Name	国际化名字的与预配置
Nodeprep	Preparation of Internationalized Node	国际化节点的与预配置
Resourceprep	Preparation of Internationalized Resource	国际化资源的与预配置
SASL	Simple Authentication and Security Layer	简单认证与安全层协议
Stringprep	Preparation of Internationalized Strings	国际化字符串的预配置
XML	Extensible Markup Language	可扩展标记语言
XMPP	Extensible Messaging and Presence Protocol	扩展消息与表示协议

4 地址

4.1 基础

一个XMPP实体就是任何可网址化并能使用XMPP通信的实体。由于历史原因, 一个XMPP实体的本地地址称为Jabber身份或JID。一个合法的JID就是一个UNICODE编码所代表的字符串, 使用UTF8编码, 结构顺序是localpart、 domainpart和resourcepart (这里前两个部分使用 ‘@’ 字符分割, 后两个部分使用 ‘/’ 字符分割)。

JID的语法定义如下:

jid = [本地部分 "@"]域部分["/" 资源部分]

本地部分 = 1*(节点) /*一个“节点”就是一个UTF-8编码的Unicode代码点, 这个点满足stringprep中的Nodeprep示例*/

域部分 = IP文字/IPv4地址/合法域名ifqdn /*“IPv4地址”和“IP文字”规则定义于RFC3986, 匹配过程应用RFC3986定义的先到先得匹配(又名“贪婪”)机制。注意从RFC3986中对于IP文字规则的重用表明IPv6地址由方括号包含(也就是用 '[' 开始, 用 ']' 结束)。*/

ifqdn = 1*(名字点) /*一个“名字点”就是一个UTF-8编码的Unicode代码点, 符合stringprep的Nameprep规范*/

resourcepart = 1*(资源点) /*一个“资源点”就是一个UTF-8编码的Unicode代码点, 符合stringprep的Resourceprep规范*/

所有JID都是基于上述结构的。

一个JID的每个允许的部分(本地部分、域部分和资源部分)的字节数不能为零且不能大于1023, 即总的最大字节数(包含 '@' 和 '/' 分割符)为3071。

为了达到通过一个XMPP网络(如一个XMPP节的'to'或'from'地址)来通信的目的, 实体地址必须是一个JID, 而不是统一资源标识符URI或国际化资源标识符IRI。一个XMPP URI本质上是一个JID带上一个'xmpp:'前缀。在任何条件下, 用于XMPP的本地地址格式只是一个不带URI的JID。XMPP URI仅被用于XMPP自身的上下文在外部的标识和交互, 例如当从一个Web页面连接到一个JID。XMPP URI描述了其如何安全地从一个XMPP URI或IRI提取出一个JID的过程。

实现要求: 当把一个JID分解成各个部分时, 一个应用在使用任何转换机制之前需要匹配分隔符 '@' 和 '/', 因为转换可能导致把特定的Unicode代码点分解成分隔符(如U+FE6B SMALL COMMERCIAL AT可能分解成U+0040 COMMERCIALAT)。

4.2 域部分

一个JID的域部分就是 '@' 符号(如果有这个符号)后面和 '/' 符号(若有)前面的部分。它是一个主要的标识符并且是一个JID唯一必需的元素(仅仅是域部分就可以成为一个合法的JID)。一个典型的域部分标识了客户端连接的“主机”服务器, 用来作为XML路由和数据管理功能。在任何条件下, 一个XMPP域部分不一定是标识一个提供核心XMPP服务功能的实体(如一个域部分可能标识其他实体, 一个多用户聊天服务, 一个发行-订阅服务或一个用户目录)。

每个XMPP服务的域部分必须是一个完全规范的域名(FQDN; 见DNS), IPv4地址、IPv6地址或自定义的主机名(也即一个文本标签可在本地网络解析)。

兼容性要求: 域部分是IP地址, 可能无法被其他服务接受来进行服务器到服务器的通信, 域部分是自定义的主机名不能用于公共网络, 因为它只能被本地网络解析。

如果域部分包含一个被认为是单独标签的最后一个字符, 这个字符必须是在用于路由一个XML节之前从域部分中分离出来的, 与另一个JID相比或构建一个XMPP URI。准确地说此字符必须是在任何其他规范化步骤被采取之前被分离。

域部分组成的一个完全合格的域名必须是一个“规范化的域名”, 也即是, 它必须是“这个域名中的每一个标签都是一个规范化的标签”和必须符合[IDNA2003]中定义的构建规范化域名的准则。当为表

示准备一个文本标签作为构建一个XMPP域部分或比较两个XMPP域部分进程中的国际化标签时，应用程序必须确保每一个文本标签带有使用STD3 ASCII准则标签设置（从而禁止ASCII编码点而不是字母、数字和连接符）的到ASCII操作的成功申请是可能的。如果到ASCII操作能被申请成功，那么标签是国际化标签。尽管XMPP应用不与无线上的ASCII操作（“ACE标签”）的输出进行通信，申请操作成功的每一个国际化标签必须是可能的。如果XMPP实现接收一个ACE标签的输入，它应该在包括一个XMPP域部分中的标签将要与一个XMPP网络进行无线通信之前使用到Unicode操作将ACE标签转换为国际化标签（然而，代替转换标签，有合法的理由解释为什么一个实现可能代替拒绝输入的信息，并且返回一个错误到提供错误数据的实体）。

一个域部分的长度不能为0字节，并且其长度不能超过1023字节。在由stringprep（如Nodeprep中的一些字符可能被映射到空集，这可能导致字符串的长度为0）的Nodeprep 文件的应用导致的任何映射或规范化之后，此规则是被强制的。通常地，长度限制了DNS的申请，对于克服这些更多的功能限制，本标准不作详细的描述。

注：IDNA2008中，一个JID的域部分是一个“域名时隙”。

4.3 本地部分

一个JID的本地部分是一个可选的标识符，在域部分之前并与后者用‘@’字符隔开。通常，一个本地部分唯一标识实体请求，并使用服务器（如本地账户）所提供的网络访问，尽管它可能也代表实体的其他类型（如与一个多用户聊天服务连接的一个聊天室）。由一个XMPP本地部分所代表的实体被一个指定域（如<localpart@domainpart>）的文本标识。

一个本地部分必须被申请成功（附录A）的 STRINGPREP 中的Nodeprep文本格式化。

在两个本地部分比较之前，实现必须首先确保Nodeprep文本已经被用于每一个标识符（只要它在比较之前已经被申请了，此文本就不需要在每次比较时申请）。

一个本地部分的长度不能是0字节，并且其长度不能超过1023字节，在由stringprep（如Nodeprep中的一些字符可能被映射到空集，这可能导致字符串的长度为0）的Nodeprep 文本实现导致的任何映射或规范化之后，此规则是被强制的。

4.4 资源部分

一个JID的资源部分是一个可选的标识符，被置于域部分之后并与后者使用‘/’字符分开。一个资源部分可以修改一个<localpart@domainpart>地址或一个仅是<domainpart>的地址。通常情况下，一个资源部分唯一标识一个连接到XMPP本地域的实体所指定的连接（如<localpart@domainpart/resourcepart>）。

一个资源部分必须被可能申请成功（见附录B）的 STRINGPREP 的Resourceprep文本。

格式化。两个资源部分在进行比较之前，必须首先确保Resourceprep文本已经应用到每一个标识符（只要它在比较之前已经被申请了，此文本就不需要在每次比较时申请）。

一个资源部分的长度不能为0字节，并且其长度不能超过1023字节。stringprep（如Nodeprep中的一些字符可能被映射到空集，这可能导致字符串的长度为0）的Nodeprep 文本实现导致的任何映射或规范化之后，此规则是被强制的。

消息要求：由于历史原因，术语“资源标识符”通常被用在XMPP中涉及到一个符合域部分和“/”分隔符的XMPP地址的的可选部分。为了防止XMPP“资源标识符”、“资源”和“标识符”的意义之间的混淆，本标准使用术语“资源部分”代替“资源标识符”。

XMPP实体应该考虑到资源部分是不透明的字符串，并且不应该归咎于任何被给定的资源部分。准确地说：

- 使用‘/’字符作为域部分和资源部分之间的分隔符并不表示 XMPP 地址以 HTTP 地址分层的那种方式进行分层。例如，形如 <localpart@domainpart/foo/bar> 格式的一个 XMPP 地址不识别与“localpart@domain”实体相关的资源分层中存在于资源“foo”之下的资源“bar”。
- 在资源部分中，‘@’字符是被允许的，并且它经常被用在 XMPP 聊天室中显示“nick”。例如，JID<room@chat.example.com/user@host>描述了一个实体，此实体是包含一个<user@host>昵称的房间<room@chat.example.com>中的一个用户。然而，聊天室服务不必为用户的实际 JID 核查声明一个昵称。

5 国际化事项

XMPP服务器必须，和XMPP客户端应该支持域部分，IETF RFC3454中附录A文本的本地部分和IETF RFC3454中附录B文本的资源部分。这使得XMPP地址包括US-ASCII范围之外的多种特性。XMPP相关文档中提供的XMPP地址格式被强制执行。

6 安全性事项

6.1 Stringprep 的重用

IETF RFC3454 中描述的安全性事项适用于本标准中定义的XMPP本地部分和资源部分的Nodeprep（附录A）和Resourceprep（附录B）文本。IETF RFC3454中描述的安全性事项适用于此处重新使用的XMPP域部分的Nameprep文本。

6.2 Unicode 的重用

Unicode安全性事项中描述的安全性事项适用于XMPP地址中Unicode字符的使用。

6.3 地址欺骗

地址欺骗有两种格式：伪造和模仿。

6.3.1 伪造地址

在XMPP技术的文本中，当实体生成一个XML节时，有可能产生伪造地址，其中此XML节的‘from’地址与网络上被授权实体的认证账户不对应。或一个已授权的实体“juliet@im.example.com”能从“nurse@im.example.com”或“romeo@example.net”中发送XML节，并产生伪造地址。

伪造地址在XMPP系统中是很顽固的，对于发送服务器，给定一个请求发送‘from’地址，对于接收服务器，通过服务器-服务器认证验证发送的域。如果发生以下情况，可能产生伪造地址：

- 执行力不强的服务器忽略要求发送‘from’地址，只需要域名部分与服务器的发送域相匹配，这将使任何已被服务器授权的实体从任何<localpart@domainpart>中发送节。
- 活跃的恶意服务器生成节来取代任意已注册的账户。

因此，在一个特定服务器的安全周期之外的实体的不可靠的区分服务器上格式如<localpart@domainpart>的JIDs和那些只能验证包含保密的任何级别的JIDs的域部分。本标准没有定义发现或撤销执行力不强或恶意服务器的方法。然而，端到端的认证或XMPP节的签署有助于缓解这一风险，因为它将请求恶意的服务器以生成错误的证书附加到已修改的‘from’地址上。

此外，如果没有使用DNS安全扩展，攻击者有可能在JIDs中伪造DNS中毒攻击。

6.3.2 模仿地址

模仿地址发生在当实体提供合法的身份验证凭据和从帐户发送XML节时。此帐户的JID与人类用户使用的另一个JID相同。比如，一些客户端的地址“juliet@example.org”（本地部分的第三个字符是‘1’）似乎和“juliet@example.org”（小写字母的‘L’）相同，视觉检测容易失误。这种现象有时也被称为“typejacking”。模仿地址更为复杂的例子可能涉及使用相似的扩展拉丁文：一个块的Unicode代码点，比如来自Cherokee块的字符+13DA U+13A2 U+13B5 U+13AC U+13A2 U+13AC U+13D2代替看起来相似的US-ASCII字符“STPETER”。

在一些模仿地址的例子中，普通用户不太可能区分真JID和假JID之间的区别。（事实上，没有哪种编程方法能充分判定假JID和真JID；一些通信文档中，Cherokee字符组成的JID可能是真JID，而US-ASCII字符组成的JID可能像假JID。）因为JIDs可包含几乎所有的正确编码的Unicode代码点，它可以比较容易在XMPP系统中模仿一些JIDs。模仿地址的可能性引入安全漏洞也困扰着万维网，具体现象称之为网络钓鱼。出现这种问题是因为Unicode和ISO/IEC 10646有许多看起来相似的指令系统（即所谓的“混淆的字符”或“混淆”）。在许多情况下，XMPP用户可能执行视觉匹配，如在和通信另一方进行JID比较时。因为没有大量的上下文字符，XMPP用户不可能绘制外观类似字符。以STRINGPREP和STRINGPREP为基础的技术（如Nameprep、Nodeprep和Resourceprep）不能映射外观类似的字符，也不能禁止某些字符，因为它们看起来和其他的一样。因此，XMPP的本地和资源部分可能包含混淆的字符，生产的JIDs模仿其他的JIDs，从而导致如下的安全漏洞：

- 一个本地部分可以作为 XMPP 实体地址的一部分。一个常见的用法是作为一个即时消息的用户名，另一种是作为一个多用户聊天室的名称，以及作为许多其他种类的实体可使用部分地址的本地部分。这类服务的安全性可能会大大降低，因为国际上存在不同的本地部分的解释。比如，用户进入一个单独的国际化的本地部分，可以访问其他用户的账户信息，或用户可以进入一个隐藏的或以其他方式限制的聊天室或服务。

- 一个资源部分可以作为 XMPP 实体地址的一部分。一个常见的用法是作为用户的连接资源的即时消息名，另一个是作为多用户聊天室的用户昵称，以及作为许多其他种类的实体可使用部分地址的资源部分。这类服务的安全性可能会大大降低，因为国际上存在不同的资源部分的解释。例如，存在两个或两个以上混淆的资源，可以在同一时间侵犯同一限制的账户（造成使用完整的 JIDs 的 XMPP 应用程序的授权不一致），或用户可以发送消息给某一个人，而不是多用户聊天室中预期的接收者。

尽管在Unicode安全性事项中的混淆字符的识别和处理有些具体的建议，但是确实目前没有全面的技术方案解决混淆字符的问题。模仿的JIDs包含来自脚本字符，或特定的用户使用的通常脚本，或语言使用者的群体的字符，这是不容易克服的（如前面所述的简单typejacking攻击，typejacking攻击依赖于字符“1”和“L”间表达的相似性）。然而，模仿地址包含来自超过一个脚本字符，或由一个特定的用户使用的通常脚本，或语言使用者群体的字符，可以通过在XMPP服务上的实行恰当的注册策略和在XMPP客户端软件上实现表达策略，从而在一定程度上减轻模仿地址的可能性。因此，可考虑以下策略。

a) 因为一个XMPP服务允许XMPP用户帐户的注册（本地部分）所扮演的角色类似注册表DNS域名，所以这样的服务应该建立有关的字符块和脚本的策略，它被允许在服务的本地部分中。这样的策略很有可能被使用在写注册账户名中的语言和脚本通告。准确地说，是减少混淆，服务可能会禁止XMPP本地部分的多个脚本字符注册，并限制来自极少数的脚本字符的注册。这种策略也适用于XMPP服务，此XMPP服务允许XMPP资源部分的暂时或永久性注册，如资源绑定或连接基于XMPP聊天室。对于在域名注册方

面的相关注意事项，请参考[IDNA-PROTO]的4.3节和[IDNA-RATIONALE]的3.2节。注意：强制约束的方法超出了本标准讨论的范围。

b) 由于每一个XMPP客户端的人类用户可能有首选语言（或者，在某些情况下，一套小的首选语言集），所以XMPP客户端应显式或隐式的从用户设备的操作系统中收集信息。此外，由于大多数语言通常由一个脚本表示（或者一系列脚本），以及大多数脚本通常包含在一个或多个字符块中，所以，当用户提交来自混合多个脚本或块字符的JID时，或用户使用的字符超出了正常的首选语言范围时，XMPP客户端应该警告用户。这项建议的目的不是阻止来自不同社区之间的语言使用者的沟通。相反，它认同这样的群体存在，并提出当对用户系统呈现陌生的脚本或字符时，应当谨慎。

7 IANA 事项

7.1 Stringprep 的 Nodeprep 文本

Stringprep的Nodeprep文本被定义在Nodeprep中（附录A）。IANA已经注册了“Stringprep 文本”注册表中的Nodeprep。

此文本的名字：Nodeprep

定义此文本的RFC文档：IETF RFC6122

指示是否是文本的最新版本：这是第一个Nodeprep的版本。

7.2 Stringprep 的 Resourceprep 文本

Stringprep的Resourceprep文本被定义在Resourceprep（附录B）中。IANA已经在“Stringprep文本”的注册表中注册了Resourceprep。

此文本的名字：Resourceprep

定义此文本的RFC文档：IETF RFC6122

指示是否是文本的最新版本：这是第一个Resourceprep的版本

8 一致性要求

本章描述了协议的功能集，总结了本标准的一致性要求。此功能集在软件认证、互操作性测试和实现报告中得到了合适的使用。针对每一个功能，本节提供了下面的信息。

- 一个人类可读的名字；
- 一个信息描述；
- 本文档的某个特定部分规范化定义功能的一个参考；
- 此功能是否适用于客户端角色、服务器角色或两种都适用（N/A 表示功能不适用指定的角色）。

此处定义的功能集试图遵守由Larry Masinter在IETF的网络工作组于2005年中提供的概念和格式。

功能：地址域长度

描述：确保一个XMPP地址的域部分的长度至少有一个字节和最多有1023字节，符合基本的底层长度的限制。

章节：第4.2节。

角色：两者都必须。

功能：地址域前缀。

描述：确保一个XMPP地址的域部分符合stringprep的Nameprep文本。

章节：第4.2节。

角色：客户端应该，服务器必须。

功能：地址本地部分长度。

描述：确保一个XMPP地址的本地部分的长度至少为1个字节和至多为1023字节。

章节：第4.3节。

角色：两者都必须。

功能：地址本地部分前缀。

描述：确保一个XMPP地址的本地部分符合stringprep的Nodeprep文本。

章节：第4.3节。

角色：客户端应该，服务器必须。

功能：地址资源长度。

描述：确保一个XMPP地址的资源部分的长度至少一个节和至多1023个节。

章节：第4.4节。

角色：两者都必须。

功能：地址资源前缀

描述：确保一个XMPP地址的资源部分符合stringprep的Resourceprep文本。

章节：第4.4节

角色：客户端应该，服务器必须。

附 录 A
(规范性附录)
Nodeprep

A.1 介绍

本附录定义了stringprep的“Nodeprep”文本。对此，它定义了用户可以使用国际化的XMPP域部分的处理规则，并且有获得字符串修正内容的最佳机会（XMPP的本地部分在XMPP地址中是可选的，在XMPP域部分之前，并用‘@’分开；它通常不是完全的即时消息用户名）。这些处理规则仅被用于XMPP的本地部分，并且不用于任意文本或XMPP地址的其他方面。

根据[STRINGPREP]要求，此文本定义如下。

- 文本的应用：XMPP 里的本地部分的国际化；
- Stringprep 的输入与输出的字符集：Unicode 3.2，定义在 A.2 中；
- 映射使用：定义在 A.3 中；
- Unicode 规范化使用：定义在 A.4 中；
- 字符的禁止输出：定义在 A.5 中；
- 双向的字符处理：定义在 A.6 中。

A.2 字符集

此文件使用了包含表A.1中未分配编码点的清单的Unicode 3.2，都定义在IETF RFC3454的附录A中。

A.3 映射

映射的使用符合IETF RFC3454中的表B.1和表B.2。

A.4 正规化

此文件指定了来自KC的Unicode规范化的使用，其描述见IETF RFC3454。

A.5 双字节

禁止指定核查双向的字符串，其描述见IETF RFC3454中的第6章。

A.6 注释

由于附加的字符串被Nodeprep禁止是在规范化之后禁止的，一个实现不能使一个人类用户输入任何的Unicode编码点，其分解包括那些字符串；如编码点包括但不必限制以下完全的信息：

- U+2100 (ACCOUNT OF)
- U+2101 (ADDRESSED TO THE SUBJECT)
- U+2105 (CARE OF)
- U+2106 (CADA UNA)
- U+226E (NOT LESS-THAN)
- U+226F (NOT GREATER-THAN)
- U+2A74 (DOUBLE COLON EQUAL)

- U+FE13 (PRESENTATION FORM FOR VERTICAL COLON)
- U+FE60 (SMALL AMPERSAND)
- U+FE64 (SMALL LESS-THAN SIGN)
- U+FE65 (SMALL GREATER-THAN SIGN)
- U+FE6B (SMALL COMMERCIAL AT)
- U+FF02 (FULLWIDTH QUOTATION MARK)
- U+FF06 (FULLWIDTH AMPERSAND)
- U+FF07 (FULLWIDTH APOSTROPHE)
- U+FF0F (FULLWIDTH SOLIDUS)
- U+FF1A (FULLWIDTH COLON)
- U+FF1C (FULLWIDTH LESS-THAN SIGN)
- U+FF1E (FULLWIDTH GREATER-THAN SIGN)
- U+FF20 (FULLWIDTH COMMERCIAL AT)

附 录 B
(规范性附录)
Resourceprep

B.1 介绍

此附录定义了STRINGPREP的“Resourceprep”。它规范了在扩展消息和XMPP中可以访问国际化resourceparts的规则，并且有获得字符串修正内容的最佳机会（XMPP resourcepart是XMPP domainpart和“/”分隔后面的XMPP地址的可选部分）。这些处理规则只针对XMPP resourceparts，而不是任意文本或其他方面的XMPP地址。

根据IETF RFC3454的要求，此配置文件定义如下：

- 配置文件的适用性：XMPP 内的国际化 resourceparts；
- 向 stringprep 发送的输入和输出字符指令；
- 映射的使用：在 B.3 中描述；
- Unicode 正规化的使用：在 B.4 中描述；
- 禁止输出的字符：在 B.5 中描述；
- 双向字符处理：在 B.6 中描述。

B.2 字符集

根据IETF RFC3454表A.1中的未分配的代码点名单使用Unicode3.2，在IETF RFC3454的Appendix A中也有定义。

B.3 映射

此文件定义的映射使用遵循IETF RFC3454 中的表。

B.4 正规化

此文件定义了来自KC的Unicode正规化的使用，其描述见IETF RFC3454 。

B.5 双字节

此文件定义了双向字符串的核查，其描述见IETF RFC3454中的第6章。

中华人民共和国
通信行业标准
扩展消息与表示协议 (XMPP)
地址格式

YD/T 2937-2015

*

人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码: 100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本: 880×1230 1/16 2016 年 2 月第 1 版
印张: 1 2016 年 2 月北京第 1 次印刷
字数: 25 千字

15115 · 866

定价: 10 元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492