

潤沁實業

潤沁網路大學

博客園 首頁 新動態 聯系 訂閱 管理

HL7传输协议

HL7消息通过各种TCP/IP传输发送，其中一些包括：

- 下层协议（LLP）
- 文件传输协议（FTP）
- 简单对象访问协议（SOAP）
- 简单邮件传输协议（SMTP）

尽管HL7可以使用多种传输协议进行数据传输，但用于实时点对点接口的最常见传输方法是LLP；对于需要批量处理HL7的系统，通常使用FTP。

基础知识：基于TCP/IP的通信

在研究常见的HL7传输方法之前，了解基于TCP/IP的通信的基础知识对于实现HL7接口时的客户端和服务端角色非常重要。

实施HL7接口时，您的接口将充当**Client**或**Server**。

TCP/IP服务器

TCP/IP服务器是一个侦听TCP/IP端口的程序，该端口号接收来自客户端的连接。例如，Web服务器是侦听端口号80的特殊类型的TCP/IP服务器。TCP/IP服务器可以连接许多不同的TCP/IP客户端。

您可能希望在其中实施HL7服务器的一个典型示例是，当您希望接收ADT（入院/出院/转院）申请以提取例如患者人口统计信息时。通常，您会将接口编写为TCP/IP服务器。

然后，您将侦听可以与对方协商的端口号，并且向您发送ADT消息的设备将连接到您的服务器。这意味着您需要将正在监听的主机和端口号提供给ADT feed 的管理员，以便他们知道如何与您连接。

TCP/IP客户端

TCP/IP客户端是连接到TCP/IP服务器的程序。例如，Netscape和Internet Explorer是连接到Web服务器的TCP/IP客户端程序。TCP/IP客户端必须同时指定主机地址或IP地址以及要连接的端口号。

当您要将实验室结果发送到HIS（医院信息系统）时，可能要在其中实现HL7客户端的一个典型示例。HIS系统的管理员需要向您提供其HL7服务器的主机或IP地址以及正在侦听的端口号。

确认消息

最后一个使许多人感到困惑的点是应如何发送**HL7确认消息**。重要的是要理解，当建立TCP/IP连接时，它是**双向**通讯通道。

当客户端与服务端建立连接时，客户端可以在其中一个通道上将数据发送到服务器，而服务器可以在另一个通道上将数据发送回客户端。后一个通道应用于发送ACK消息。

有时有必要为产品的HL7接口同时实现客户端和服务端组件。

如果您可以选择的话，请充分利用可以使用第二个通信通道发送回ACK消息，因为这是一种更加简洁的设计。

参考资料：

- <https://blog.interfaceware.com/tcpip-basics/>
- <https://help.interfaceware.com/v6/secure-protocols-for-hl7>

LLP-较低层协议

低层协议（LLP）有时被称为**最小低层协议（MLLP）**，是用于通过TCP/IP传送HL7消息的绝对标准。

由于TCP/IP是字节的连续流，因此需要包装协议才能使通信代码能够识别每个消息的开头和结尾。LLP是最常见的HL7传输机制，用于通过TCP/IP通过局域网（例如医院中的TCP/IP）发送未加密的HL7。

使用LLP时，必须使用标头和尾标包装HL7消息，以表示消息的开头和结尾。这些标头和尾标通常是不可打印的字符，不会在HL7消息的实际内容中显示。

下表描述了通过LLP发送的HL7消息的典型结构。它包含四个部分：

标头	HL7讯息	尾标	回车
垂直制表符 (0x0B)	HL7消息使用头标、尾标和紧随其后是回车进行包装： MSH ^~\& 。 199908180016 ADT ^ A04 ADT.1.1698593 P 2.5	字段分隔符 (0x1C)	回车 (0x0D)

公告

昵称： 潤沁網路大學
园龄： 1年10个月
粉丝： 2
关注： 0

<	2021年3月		
日	一	二	三
28	1	2	3
7	8	9	10
14	15	16	17
21	22	23	24
28	29	30	31
4	5	6	7

搜索

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

我的标签

Mirth(18)
HL7(7)
DataBase(2)

随笔分类

DataBase(2)
HL7(7)
Mirth(15)

随笔档案

2021年2月(2)
2021年1月(20)

文章分类

Mirth(3)

最新评论

1. Re:第八課-Channel Study
Custom JAR Lib
受益匪淺!!!

阅读排行榜

	PID 1 000395122 LEVERKUHN ^ ADRIAN ^ C ^^^ 19880517180606 M		
--	---	--	--

此外，还必须确保每个段都以0x0D（回车）字符结尾，这是标准要求的；但是通常HL7日志数据可以通过FTP或电子邮件接收，这时段分隔符已转换为0x0A字符。

有多种方法可以保护通过LLP的数据：

- **VPN隧道**：虚拟专用网络（VPN）是一种专用网络，使用Internet将远程站点链接在一起，同时使用安全加密技术来确保未经授权的用户无法读取它。这是解决HL7加密问题的一种非常流行的方法，尤其是在当今的大环境下，因为许多常见的云平台都将VPN连接作为其平台产品的一部分提供。
- **SSH隧道连接**：这与使用VPN连接的概念相似，在VPN连接中，SSH服务器用于在系统之间安全的建立隧道连接LLP通信。每个Linux发行版都有一个内置的SSH服务器，也有Windows的选项，例如VShell。
- **TLS/SSL**：HL7消息也可以通过传输层安全性（TLS）或安全套接字层（SSL）加密协议进行传输，以确保对消息进行身份验证和加密。

HLLP-混合下层协议

混合低层协议（HLLP）是更广泛地使用低层协议的变体。与LLP一样，HLLP使用TCP/IP作为其传输方式，但通过在消息末尾使用校验和来进行错误检测和验证。

校验和用于验证数据有没有被破坏。通常为发送应用程序发出的每个数据块计算校验和，然后在接收应用程序中验证其准确性。

HLLP中使用的校验和是非标准的，这意味着它们可能因实现而异。

HLLP中使用的一种常见的校验和类型称为**BCC**（块字符检查），它是一个块中所有字符的总和。BCC校验和被视为弱校验和，因为可能很容易找到生成相同块校验和的不同块。尽管BCC校验和相对容易实现，但它可能不符合大多数公司的通信标准。

实际上，大多数供应商选择使用基于LLP的TCP/IP，而不是HLLP。LLP是一种非常简单的协议，可用于代替HLLP，因为TCP/IP通道可提供HL7消息无错误传递所需的所有服务。这包括：

1.连接握手

两个系统启动通信的过程，开始和结束监听用于开始/停止数据传输。

2.全双工数据传输

系统同时发送和双向接收数据的过程。

3.错误检测和重传

传输层检测传输失败的段并根据需要重新传输这些段的过程。

4.流量控制

TCP通过使用ACK和NACK来管理系统之间消息流的过程。通过在HL7应用程序中使用ACK / NACK和其他内置机制，您可以管理数据流以确保有效且可靠地传输消息。

5.连接终止

每个系统通过握手独立结束连接的过程。

在大多数情况下，只要两个通信系统都使用可靠的开放系统互连（OSI）传输层，就不需要HLLP，因为底层的OSI已经验证了消息的传输以及消息的完整性。

HLLP仅用于不可靠的传输（例如，通过串行电缆传输消息），大多数供应商认为不需要。

使用TCP/ IP，数据和标头上的校验和已经是该协议固有的。这意味着该协议能检测到校验和错误，并在必要时请求重新传输数据。这意味着与HLLP相关的辅助校验和不会进一步保证数据传输，而只会增加传输开销。

参考资料：

- <https://blog.interfaceware.com/common-hl7-transport/>
- <https://blog.interfaceware.com/hybrid-lower-layer-protocol-hllp/>

FTP-文件传输协议

文件传输协议（FTP）是应用程序层TCP/IP协议，可在本地和远程文件系统之间移动文件，反之亦然。

FTP并行启动两个TCP连接以传输文件、控制连接、用于发送与服务器交互（例如，进行身份验证）、启动文件操作（例如，下载或重命名文件）的命令、数据连接以发送文件。

发送包含电子受保护的健康信息（ePHI）的HL7消息时，使用安全协议发送文件是必须的。

有两种方法可以使用FTP提供HL7消息的安全传输：

- SFTP（SSH文件传输协议）是SSH协议的扩展，可为任何数据流提供安全的文件传输、访问和管理功能。
- FTPS（FTP安全）提供对TLS（传输层安全性）和SSL（安全套接字层）协议的支持。

SFTP和FTPS通常被认为是FTP的安全“扩展”，但事实并非如此，这两个协议实际上是不兼容的。

HL7批处理涉及通过FTP协议或作为电子邮件附件发送文件。

根据HL7标准，任何HL7消息都必须以MSH段开头，但是在发送一批HL7消息时，规则会更改。

1. HL7传输协议(161)
2. 第壹課-Install: Mirth Connect安装步骤(99)
3. 开篇:Mirth Connect系统集5)
4. HL7标准的版本(75)
5. 第三課：信道学习Source C Destinations File Writer(60)

评论排行榜

1. 第八課-Channel Study For R Lib(1)

批处理包含多个HL7消息（每个消息均以其起始MSH段标记），如以下示例HL7批处理文件中所示，批处理标识由批处理'标头FSH和BSH'以及批处理'尾部FTS和BTS'本身进行标识：

```
FHS|^~\&|MESA|XYZ_HOSPITAL|IHIE|IHIE|20120703094005|||  
BHS|^~\&|MESA|XYZ_HOSPITAL|IHIE|IHIE|20120703094005|||  
MSH|^~\&|MESA_ADT|XYZ_ADMITTING|iFW|XYZ_HOSPITAL|||ADT^A04|101102|P|2.3.1|||  
EVN||200004211000|||200004210950  
PID||583020^^^ADT1||WHITE^CHARLES||19980704|M|AI|7616 STANFORD AVE^^ST. LOUIS^MO^63130|||20-98-1701|||  
PV1||E||||5101^NELL^FREDERICK^P^^DR|||||||V1002^^^ADT1|||||||200004210950|||  
MSH|^~\&|MESA_OP|XYZ_HOSPITAL|iFW|XYZ_RADIOLOGY|||ORM^001|101104|P|2.3.1|||  
PID||583020^^^ADT1||WHITE^CHARLES||19980704|M|AI|7616 STANFORD AVE^^ST. LOUIS^MO^63130|||20-98-1701|||  
PV1||E|$PATIENT_LOCATION$|||$ATTENDING_DOCTOR$|5101^NELL^FREDERICK^P^^DR|||||||V1002^^^ADT1|||||||200004210950|||  
ORC|NW|A101Z^MESA_ORDPLC|||1^once^^^S||200004210955|^ROSEWOOD^RANDOLPH|7101^ESTRADA^JAIME^P^^DR||3145551212|200004210955|922229-10^THE-  
RAD^IHE-CODE-231||  
OBR|1|A101Z^MESA_ORDPLC||P1^Procedure 1^ERL_MESA|||||xxx||Radiology^^^R|7101^ESTRADA^JAIME^P^^DR|||||||1^once^^^S||WALK|Project  
Manager|||||||A||  
MSH|^~\&|MESA_ADT|XYZ_ADMITTING|iFW|XYZ_HOSPITAL|||ADT^A06|101126|P|2.3.1|||  
EVN||200004211000|||200004210950  
PID||583020^^^ADT1||WHITE^CHARLES||19980704|M|AI|7616 STANFORD AVE^^ST. LOUIS^MO^63130|||20-98-1701|||  
PV1||I|E^111^1^XYZ_HOSPITAL|||P^PRIOR_LOCATION$|1234^WEAVER^TIMOTHY^P^^DR|5101^NELL^FREDERICK^P^^DR|||||||V1002^^^ADT1|||||||  
||||200004210950|||  
BTS|3|Batch Message Count  
FTS|1|Have a Nice Day
```

参考资料：

- <https://help.interfaceware.com/processing-a-batch-of-hl7-messages.html>
- <https://help.interfaceware.com/v6/secure-protocols-for-hl7>

潤沁網路大學

分类: [HL7](#)

标签: [HL7](#)

好文要顶

关注我

收藏该文

潤沁網路大學

关注 - 0

粉丝 - 2

0

0

« 上一篇: [HL7消息类型](#)
» 下一篇: [第八課-Channel Study For Caller Custom JAR Lib](#)

posted @ 2021-01-25 13:30 潤沁網路大學 阅读(161) 评论(0) 编辑 收藏

[刷新评论](#) [刷新页面](#) [返回顶部](#)

发表评论

编辑 预览

B

支持 Markdown

自动补全

提交评论

退出

[Ctrl+Enter快捷提交]

- 【推荐】大型组态、工控、仿真、CAD\GIS 50万行VC++源码免费下载!
- 【推荐】亚马逊云科技在线研讨会：借助图神经网络实现实时欺诈检测
- 【推荐】华为开发者联盟--邀友同注册，解锁阶梯“豪”礼
- 【推荐】限时秒杀！国云大数据魔镜，企业级云分析平台

园子动态:

- 发起一个开源项目: 博客引擎 fluss
- 云计算之路-新篇章-出海记: 开篇
- 博客园2005年6月1日首页截图

最新新闻:

- 黄峥勇退: 一年之内卸任CEO和董事长 想去“寻找幸福”
- 百度二次上市, 三重价值
- 快手三年游戏路, 路在何处?
- 谷歌涂鸦庆祝爱尔兰圣帕特里克节
- NASA的SMA轮胎技术即将商用 30倍于钢的可恢复应变
- » 更多新闻...

Copyright © 2021 潤沁網路大學
Powered by .NET 5.0 on Kubernetes

潤沁網路大學