如果响应报文是通过代理转发的，一定要确保代理没有修改 Server 首部。Server 首部是用于原始服务器的。代理应该添加的是 Via 条目。

5. Via的隐私和安全问题

有时候，我们并不希望在 Via 字符串中使用确切的主机名。总地来说，除非显式地允许了这种行为，否则，当代理服务器作为网络防火墙的一部分使用时，是不应该转发防火墙后面那些主机的名字和端口号的，因为防火墙后面的网络结构信息可能
154 会被恶意群体利用。[14]

如果不允许进行 Via 节点名转发，作为安全防线的一部分使用的代理就应该用适当的假名来取代那台主机的名字。一般来说，即使隐藏了真实名称，代理也应该尝试着为每台代理服务器保留一个 Via 路标条目。

对那些有着非常强烈的隐私要求，需要隐藏内部网络设计和拓扑结构的组织来说，代理应该将一个（接收协议值相同的）有序 Via 路标条目序列合并成一个联合条目。比如，可以将：

```
Via: 1.0 foo, 1.1 devirus.company.com, 1.1 access-logger.company.com
```

压缩成：

```
Via: 1.0 foo, 1.1 concealed-stuff
```

除非这些条目都在同一个组织的控制之下，而且已经用假名取代了主机名，否则就不能将其合并起来。同样，接收协议值不同的条目也不能合并起来。

6.6.2 TRACE方法

代理服务器可以在转发报文时对其进行修改。可以添加、修改或删除首部，也可以将主体部分转换成不同的格式。代理变得越来越复杂，开发代理产品的厂商也越来越多，互操作性问题也开始逐渐显现。为了便于对代理网络进行诊断，我们需要有一种便捷的方式来观察在通过 HTTP 代理网络逐跳转发报文的过程中，报文是怎样变化的。

通过 HTTP/1.1 的 TRACE 方法，用户可以跟踪经代理链传输的请求报文，观察报文经过了哪些代理，以及每个代理是如何对请求报文进行修改的。TRACE 对代理流的调试非常有用。[15]

注 14：恶意用户可以通过计算机名字和版本号来了解安全防线之后的网络结构。这类信息可能有助于进行安全攻击。而且，计算机名还可能泄露一个组织内部私有项目的线索。

注 15：但是，它还没有得到广泛的实现。