

能共同饿死该 HTTP 会话。理想情况下,一种服务要与各类流量有隔离度,以保护一种流量类型免受其他流量类型干扰。这种保护能够在网络中的不同地方实现,在每台路由器中,在进入网络的首个入口,或在网络边界域间。这则是我们的第2个见解。

见解2: 希望在流量类型之间提供**流量隔离** (traffic isolation) 的度,以便一类流量不会受到另一类异常流量的负面影响。

我们将考察在流量类型之间提供这种隔离的特定机制。这里我们注意到,有两大类方法可以使用。首先,可以执行如图 7-15 所示的**流量监管** (traffic policing) 方法。如果流量类型或流必须满足一定的准则 (例如,音频流不超过 1Mbps 的峰值速率),那么可以设置一个监管机制来确保这些准则的确被遵守。如果被监管的应用行为异常,这个监管机制将采取某种行动 (例如,丢弃或者延时那些违反这些准则的分组),以便实际进入网络的流量符合这些准则。我们很快将考察的漏桶机制也许是使用最广泛的监管机制。在图 7-15 中,分组分类和标记机制 (见解1) 以及监管机制 (见解2) 都一起在网络的边缘实现,或在端系统中实现,或在边界路由器中实现。

为流量类型之间提供隔离的一种互补的方法是,链路级的分组调度机制为每种类型明确地分配固定量的链路带宽。例如,在 R1 能够给音频类型分配 1Mbps,能够给 HTTP 流分配 0.5Mbps。在这种情况下,音频和 HTTP 流分别看到了容量为 1.0Mbps 和 0.5Mbps 的逻辑链路,如图 7-16 所示。通过严格执行链路级的带宽分配,一种类型仅能够使用已经分配的带宽量;特别是,它不能利用其他应用现在未使用的带宽。例如,如果音频流静默了 (例如,如果谈话者停顿,不产生音频分组),HTTP 流在 R1 到 R2 的链路上的传输带宽仍然不能够超过 0.5Mbps,即使音频流分配的 1Mbps 带宽在那个瞬间没有使用。由于带宽是一种“使用它或丢失它 (use-it-or-lose-it)”的资源,没有理由妨碍 HTTP 流量使用没有由音频流使用的带宽。我们将希望尽可能高效地使用带宽,当能够以别的方法使用它时决不浪费带宽。这引发我们的第3个见解。

见解3: 当为流量类型或流之间提供隔离时,希望尽可能有效地使用资源 (例如链路带宽和缓存)。

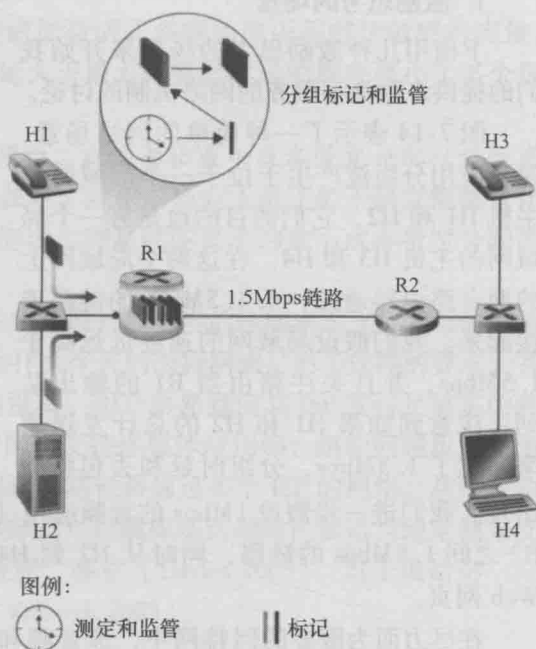


图 7-15 监管 (与标记) 音频与 HTTP 流量类型

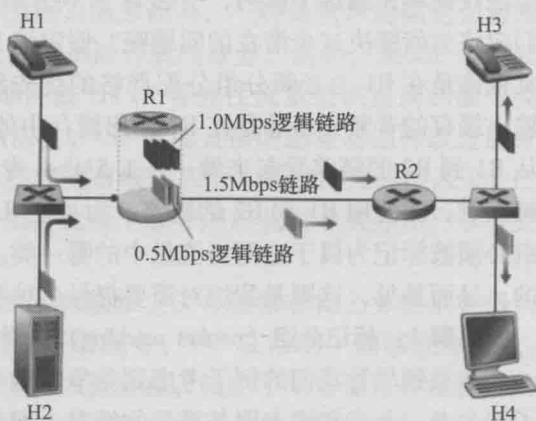


图 7-16 音频与 HTTP 流量类型的逻辑隔离