使用WCCP发现路径MTU时的WSA行为

目录

简介

本文描述在您的配置包括Web缓存通信协议(WCCP)和路径最大传输单位(MTU)发现时，路由器丢弃数据包时遇到的问题，并提供了问题的解决方案。

背景信息

预阶段

单独查看时，许多功能非常适合处理特定问题。但有时，如果将两三种技术结合起来，就会产生一些尴尬的行为，您必须引入其他功能或解决方法才能使其正常工作。例如，使用生成树和开放最短路径优先(OSPF)和第2层(L2)融合比OSPF（如果使用最小死区间，则为1s）花费的时间要长(20s)，但将生成树替换为多生成树(MST)，并且它会再次正常运行。

WCCP和路径MTU发现之间也观察到相同的互操作性行为；许多人认为这是通用路由封装(GRE)报头问题。但是，本文档说明了真正的原因。

路径MTU发现和WCCP如何分开工作

路径MTU发现

每行都对数据包的大小有限制。如果发送的数据包比支持的数据包大，则会将其丢弃。路上的第3层设备（路由器）的一个作用是注意并切断从一条线路到另一条线路的大数据包，以确保端到端通信对每条线路的功能透明。

但有时，终端主机的配置方式使其数据包无法被切分（例如，加密文件、语音呼叫）。 此信息通过

IP报头内的“不分段(DF)”位传达。路由器会丢弃此类数据包，但路由器会尝试通过互联网控制消息协议(ICMP)消息（类型3-Destination unreachable，代码4 — 需要分段，但DF位已设置）向终端主机报告。 这样，主机就知道将来会发送较小的数据包。

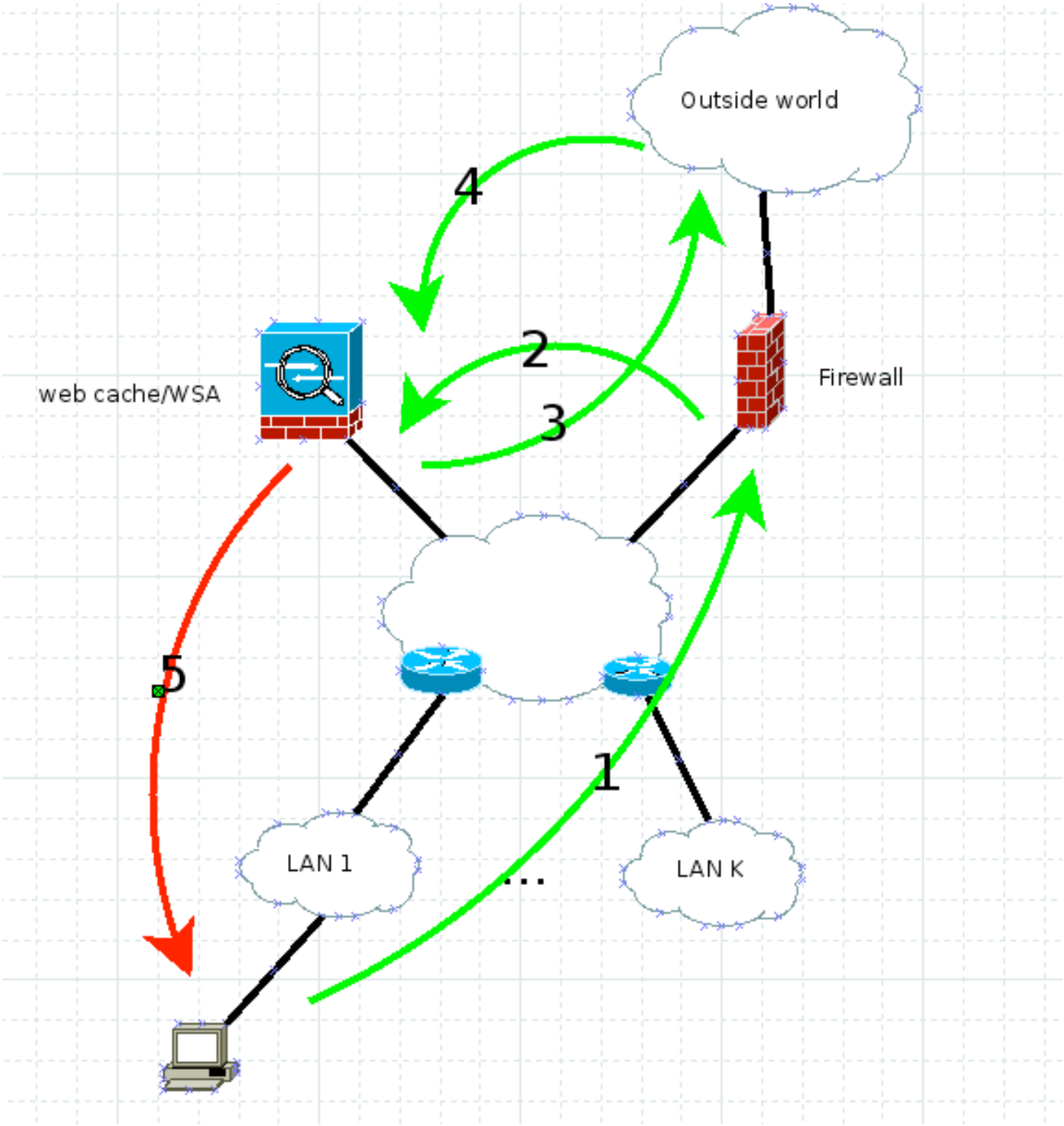
这是路径MTU发现的核心。您可以发送设置了DF位的大数据包，以查看它们是否到达终点，或者您是否收到如前所述的ICMP报告。确定最大可用数据包大小后，将其用于任何进一步通信。有关详细信息，请参阅 RFC 1191。

网络安全设备(WSA)默认使用路径MTU发现。因此，其生成的所有数据包都使用默认配置设置DF位。

WCCP

如果您需要在他人不知情的情况下对网络流量实施安全保护，您将通过不可见的代理运行其流量。WCCP是用于拦截设备（路由器/防火墙）和Web缓存引擎/代理（在本例中为WSA）之间通信的协议。

此图说明了此场景中的流量传输方式：



它的工作方式如下：

1. 客户端发送HTTP GET和IP源、其IP地址（客户端IP地址）和目的服务器IP地址。

2. 防火墙或路由器拦截HTTP GET并通过WCCP GRE或纯L2将其转发到Web缓存/WSA。源仍是客户端IP地址，目的仍是Web服务器IP地址。

3. WSA会检查请求，如果请求合法，会将其镜像到Web服务器。此处，目标IP地址是Web服务器IP地址，源IP地址可能是WSA或客户端，具体取决于您是否启用了客户端IP地址欺骗。在本例中，这并不重要，因为两种情况下的返回流量都必须到达WSA。

4. 返回流量在WSA中检查。

5. WSA将响应发送给客户端，其中包含源IP地址、始终为Web服务器IP地址（因此客户端不会可疑）和目的客户端IP地址。

问题

如果图中的路由器必须对流量进行分段，会发生什么情况？WSA将DF位放在数据包编号5上，但必须对其进行分段。路由器会丢弃它，并告知发送方需要分段，但DF位已设置（ICMP第3类代码4）。 毕竟，RFC 1191必须立即运行，并且发送方必须减小其数据包大小。

使用WCCP时，源IP地址是Web服务器IP地址，因此此ICMP从不发往WSA;相反，它会尝试访问真正的Web服务器（请记住，底部的此路由器不知道WCCP）。 WCCP和路径MTU发现有时会破坏网络设计。

解决方案

解决此问题的方法有四种：

- 发现实际MTU，然后在WSA上使用**etherconfig**降低接口的MTU。请记住，TCP报头为60,IP为20，当您使用ICMP时，它会向IP报头添加8个字节。
- 禁用路径MTU发现(**pathmtudiscovery** CLI WSA命令)。 这会导致TCP MSS为536，这可能导致性能问题。
- 更改网络，使WSA和客户端之间不存在第3层分段。
- 在相关接口的路上，在每台Cisco路由器上使用**ip tcp mss-adjust 1360**（或其他计算的编号）命令。

其他说明

在调查此问题时，发现如果将代理显式设置到客户端中几分钟然后将其删除，则问题将在接下来的四到五小时内得到解决。这是因为，在显式模式下，WSA和客户端之间的路径MTU发现机制工作正常。一旦WSA发现路径MTU，它会将其与发现的TCP MSS一起存储到内部表中以供参考。显然，此表每四到五小时刷新一次，这样，解决方案在过多时间后就无法再次运行。