作者： 李小宁
职务： 产品经理 技术工程师
日期： 2019-12-23
邮箱： Xiao.li@beckhoff.com.cn
电话： 021-66312666-896（可选）

BECKHOFF New Automation Technology
中国上海市静安区汶水路 299 弄 9-10 号
市北智汇园 4 号楼（200072）
TEL: 021-66312666
FAX: 021-66315696

ADS 通信与诊断

摘　要：ADS 是倍福 TwinCAT 实时核与外部环境交互的接口，在日常使用 TwinCAT 中经常会遇到各种通信和故障诊断的问题，因此，本文将重点介绍在使用 ADS 遇到问题时如何能够快速进行故障排除。

关键字：ADS 通讯、ADS 诊断

附　件：

序 号	文件名	备注

历史版本：

2019-06-20	李小宁	ADS 通信与诊断 V1.pdf
2019-06-30	李小宁	ADS 通信与诊断 V2.pdf

免责声明：

我们已对本文档描述的内容做测试。但是差错在所难免，无法保证绝对正确并完全满足您的使用需求。本文档的内容可能随时更新，也欢迎您提出改进建议。

参考信息：

目 录

1. ADS 简介

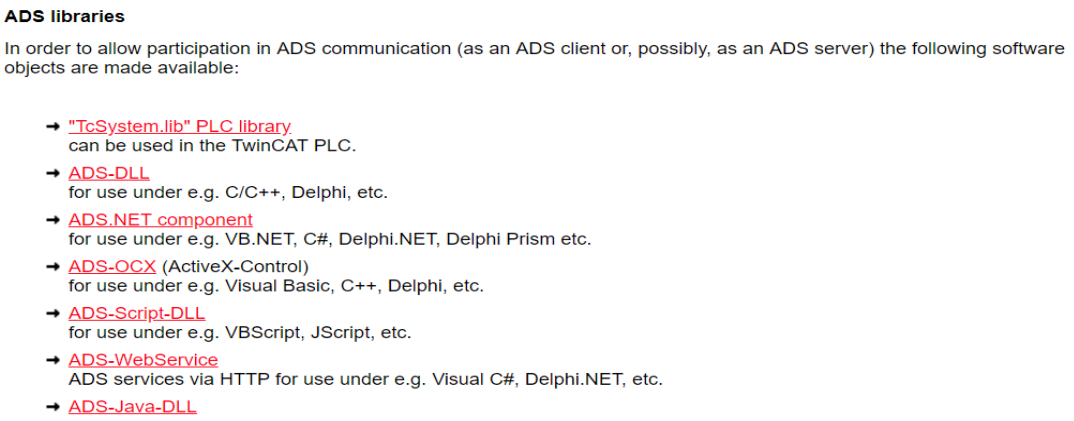
ADS 全称为 Automation Device Specification，是倍福 TwinCAT 实时核与外部环境交互的接口，该协议是倍福定义和开发的，倍福的软件和硬件产品均支持 ADS 协议。

由于 TwinCAT 是基于微软 Windows 系统并具备实时逻辑处理的工程软件，因此微软的 WinCE5、WinCE6、XP、WES7、Win10 等的 X86 位和 X64 位系统中均可以运行 TwinCAT 软件。当前用户可以购买的 TwinCAT 软件分为 TwinCAT 2（简称 TC2） 和 TwinCAT 3（简称 TC3）两大类。TC 3 是基于 TC2 功能基础上推出的全新架构的工程软件，在 ADS 通信方面 TC3 向下兼容 TC2，但 TC3 的 ADS 通信又有了一些新功能的扩展如 ADS over MQTT 和 ADS Serurity 等。

2. ADS 协议

ADS 协议是开放的，用户可以查阅倍福官方在线文档 https://infosys.beckhoff.com/index_en.htm 来了解 ADS 协议原理。AdsMonitor 是倍福开发的对 ADS 报文抓取和报文分析、数据诊断的小工具，功能类似于 Wireshark。如果用户希望使用 ADS 客户端进行开发时，只需要安装 TwinCAT 即具备了 ADS 客户端与 Server 端通信能力。TwinCAT 提供了标准的 ADS DLL 和完善 ADS API 接口可供各种开发语言来调用，也提供了大量的帮助文档和示例程序供用户参考。如果客户需要以 Linux、MAC OS、IOS、Andriod 等平台作为 ADS 客户端的话，也可以自行开发 ADS 客户端，开发客户端无需任何 SDK，倍福也不提供相关 SDK，当然，为了降低客户端的开发难度，倍福在 https://github.com/Beckhoff/ADS 上面共享了一个基于 VS C++的 ADS 客户端代码，用户可以自行下载并集成到项目中，这只是一个基础的 ADS Client 协议封装的代码，如果用户需要承载大批量的数据通信，则需要学习并掌握该代码后自行完善相关功能。除非特殊需求，客户才需要基于开源代码来开发 ADS 客户端。

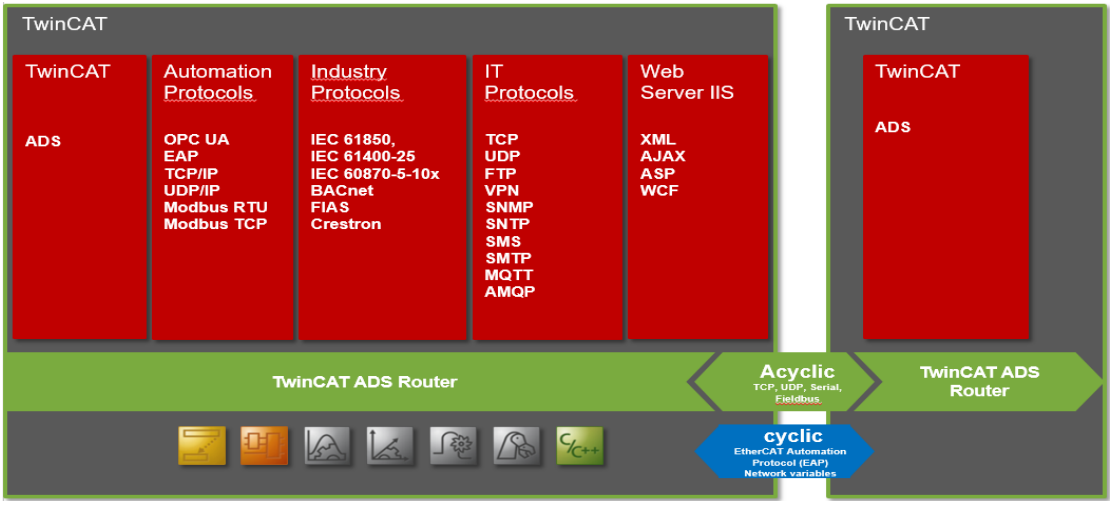
ADS 本质上是 TCP 通信，只是对 TCP 的收发数据进行了一系列的规范，以更好的适应不同的应用需求。ADS 对外通信的端口统一为 48898，客户无法修改端口。



(图 1　高级语言调用 ADS 的库文件)

3. ADS Router

ADS Router 是 ADS Client 与 TwinCAT 实时核交互的接口，ADS Router 通过 48898 接收 ADS Client 发送来的请求，并把请求命令交付于实时核处理，实时核处理完请求并做出反馈，ADS Router 把反馈结果响应给 ADS Client。ADS Router 是 TwinCAT 底层不可或缺的功能，如果用户使用 TwinCAT 来作为 ADS Client 的话，也具备了 ADS Router 的功能。由于 ADS 通信是通过两端的 ADS Router 来完成的，也就意味着两端接收数据的端口均为 48898（端口不可更改，这个地方与常规的 TCP 通讯是有区别的）。由于一台 Windows 控制器只能安装唯一的 TwinCAT，而一个 TwinCAT 只有唯一的 ADS Router，也就意味着一台控制器只能有一个 ADS Router 来承接所有外部所有通信请求。



（图 2　ADS Router 原理）

ADS Router 可以查找本网络里面所有已安装 ADS Router（即 TwinCAT）的控制器，也就是我们所说的扫描目标控制器，扫描功能发送的是 UDP 报文，端口为 48899（端口不可更改）。ADS Router 通过 48899 接收到扫描报文请求后，会把本机的 TwinCAT 和系统相关信息反馈给扫描端的 ADS Router（48899），扫描端把扫描到的信息呈现在扫描对话框中。

添加路由（Add Route ）发送的是 ADS 请求报文，实现双方通信前把建立通信所必要的对方信息报备到本地的 ADS Router 列表中，以便后续建立流畅的 ADS 通信，添加路由后进行通信也是工业设备互相通信的安全要求。

4. ADS 诊断

ADS 协议已经有 20 年的应用历史，可谓非常稳定了，由于 ADS 非常灵活，因此在使用前对 ADS 理解不到位，就必然会产生一些应用故障。这些故障一般会发生在通信建立之前（即扫描添加路由时）和正常通信一段时间后，下面对着两种故障进行详细介绍：

4.1. 无法扫描或添加路由

4.1.1. 网卡 IP 地址设置分析

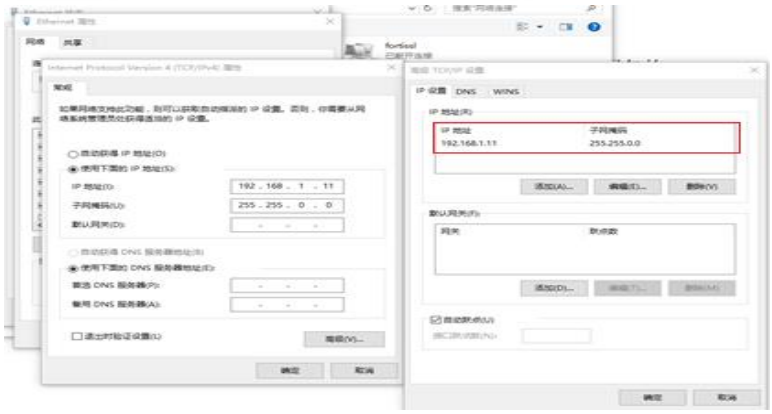
如果 IP 地址设置不合理，则 ADS 通信一定无法建立，两端控制器的 IP 是否在同一网段，子网掩码设置是否合理，如：A 控制器设置为：192.168.1.11，B 控制器设置为：192.168.1.22，子网掩码均为：255.255.0.0。

如果需要连接外网的话，网关设置是否合理，如果不需要外网通信，请不要设置网关。

不可在同一个网卡上设置多个 IP 地址，这会造成 ADS 通讯无法添加路由或者后续出现通讯不稳定。

建议先禁用其他不进行 ADS 通信的网卡，等 ADS 通信已经建立完成后，再使能其他网卡（TC2 环境下会更有效果）。

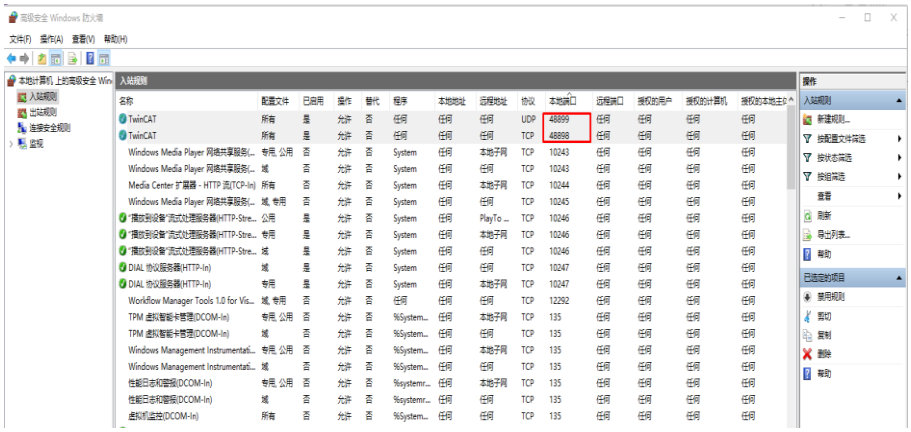
打开命令行界面，ping 对方 IP，看看是否能够 ping 通，如果不通，则继续以上几步看看哪里设置不合理；如果可以 ping 通则尝试在 TwinCAT 中进行扫描和添加路由。



（图 3　IP 设置）

4.1.2. 防火墙设置分析

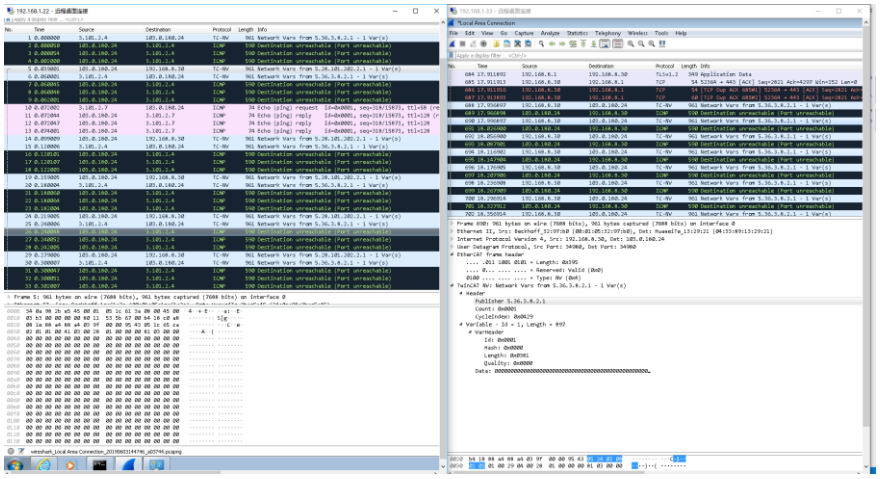
如果是 WES7 或者 Win10 的系统，在初次添加路由时防火墙可能会阻止 UDP 报文的收发，因此需要关闭防火墙或者在防火墙中开放入站端口（48898 和 48899），一般情况，先关闭防火墙，Client 和 Server 两端的防火墙都需要关闭，扫描到目标机并添加了路由后，再启动防火墙。



（图 4　防火墙设置）

4.1.3. 网络交换机或路由器设置分析

有些用户的局域网中禁止发送 UDP 报文，因此会在路由器或者交换机上设置了 UPD 报文包过滤的屏障，这会导致目标机无法正确收发 UDP 扫描报文，这个情况可以通过在控制器两段分别安装 Wireshark 来实时抓取网络数据包来分析，看看本机是否可以接收到目标 IP 发送过来的请求或响应报文。广域网之间的 TwinCAT 进行通讯 ADS 通讯时，经常会遇到这个问题，需要在设置 VPN 传输时，设置透传功能，这样目标控制器收到的报文中的 src IP 信息不会被路由器自动修改了。这个现象也可以通过 Wirshark 来抓取两端的数据包进行分析 src IP 和 dst IP 是否匹配即可找到问题的症结。



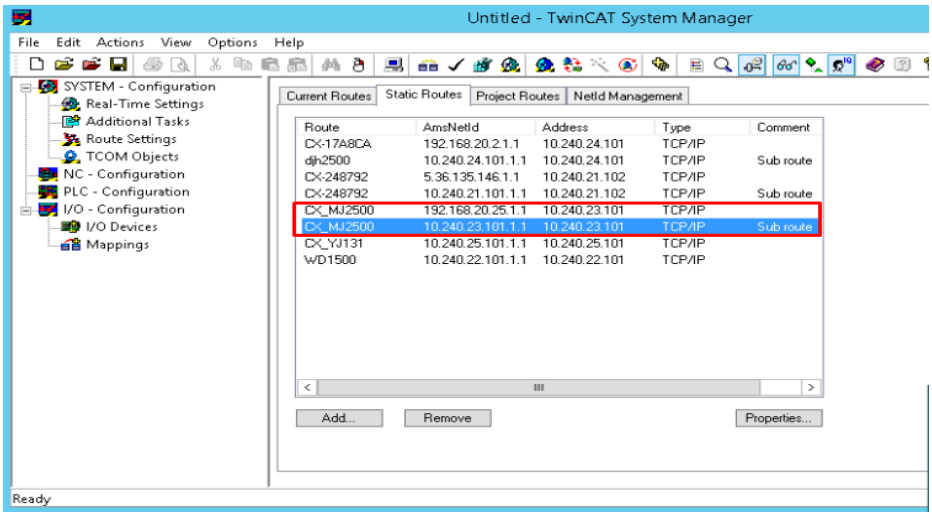
（图 5　Wireshark 抓取数据包）

4.2.　运行一段时间后出现故障

这种情况经常发生在 ADS Client 与 Server 进行通信一段时间后，在 Client 侧通过 TwinCAT 扫描 Server 时出现无法找到 Server 或者无法添加路由的情况，此时有可能已存在的 ADS 连接依然可以正常通讯，主要原因是由于 Server 端对 Client 端发送过来的 UDP 报文或者 Add Route 报文不在响应造成，可能的原因分析是：

4.2.1.　可能原因分析 1：

Server 在之前的运行过程中曾经有人连接过，并进行过添加路由操作，而添加时 Client 侧的 ADS 通信必要（Host Name、IP、NetID）信息和 Server 端已备案的信息产生冲突： 如之前通过 IP 地址添加的路由，而现在改为 host Name 添加路由；直接通过 Host Name 添加路由；添加路由的 IP 地址、NetID、HostName 等信息不同但是在已建立通信的连接中存在等情况。这会导致 Ads Router 出现处理异常，严重时会导致以后再也无法建立连接，需要重启控制器才可以解决问题。解决办法：尝试删除 Router 表中重复的，不需要的路由信息，以 Host Name 添加的路由等，并重新激活或重启控制器。



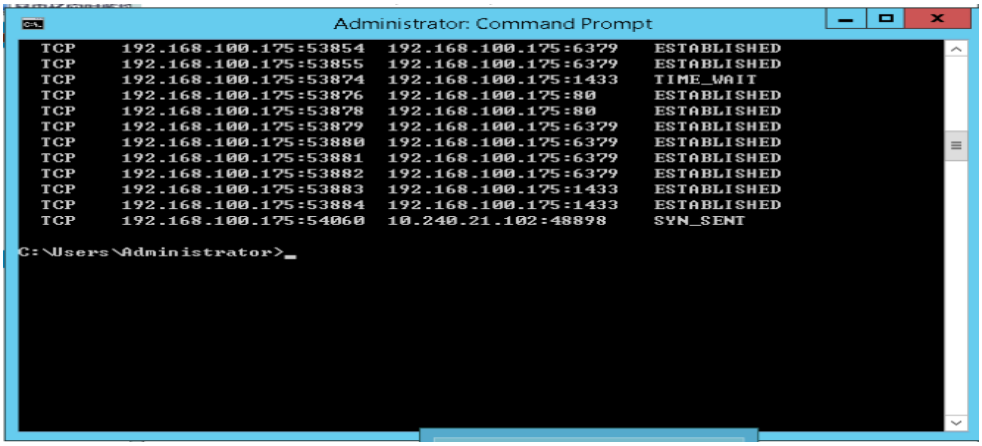
（图 6　Router 表）

4.2.2.　可能原因分析 2：

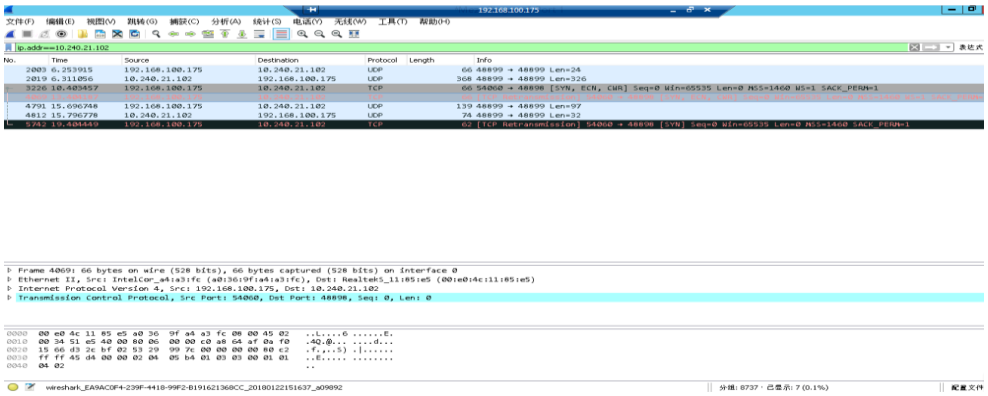
新 Client 在添加路由时采用 Host Name 添加，由于 Host Name 一般为控制器的名称，如果包含一些特殊字符或者中文等信息，在添加路由后，会导致控制器运行一段出现无法添加新的路由，即使重启控制器也无法解决。必须要手动删除控制器 Router 列表的信息后，重启控制器才可以解决问题。因此，我们不建议中国用户添加路由时选择 Host Name 添加。

4.2.3. 可能原因分析 3：

网络延迟严重，在跨网通信时，经常会出现网络延时较大的情况，如：Client 端发送了请求报文，由于网络延时原因，Client 在超时到达时依然没有收到 Server 的响应，这时，Client 端就会断开当前 TCP 连接而重新创建新的连接，而新的连接又发送新的请求给 Server 端，这会导致 Server 对老的连接释放和新连接的管理的混乱，这主要是由于 TCP 的几次握手时间和网络延时造成，从而导致 ADS 通信不稳定或无法再建立新连接。用户可以通过命令行命令 netstat 查看网络连接状态，如果出现通信不稳定或者时好时坏时，则 TCP 连接状态表中将会出现 TIME_WAIT、CLOSE_WAIT 等多种状态。由于 TCP 连接在出现异常后的消失需要较长时间，不同系统有所差异，有的可能 2-4 小时，有的会半天等待，因此，也会有一种现象是在发生通信故障一段时间后网络还会恢复正常。出现这种情况，需要通过优化网络环境、延长通信超时设定、降低通信频率、减少通信数据量等办法来逐步解决。



（图 7-1 netstat）



（图 7-2 Wrieshark）

4.2.4. 可能原因分析 4：

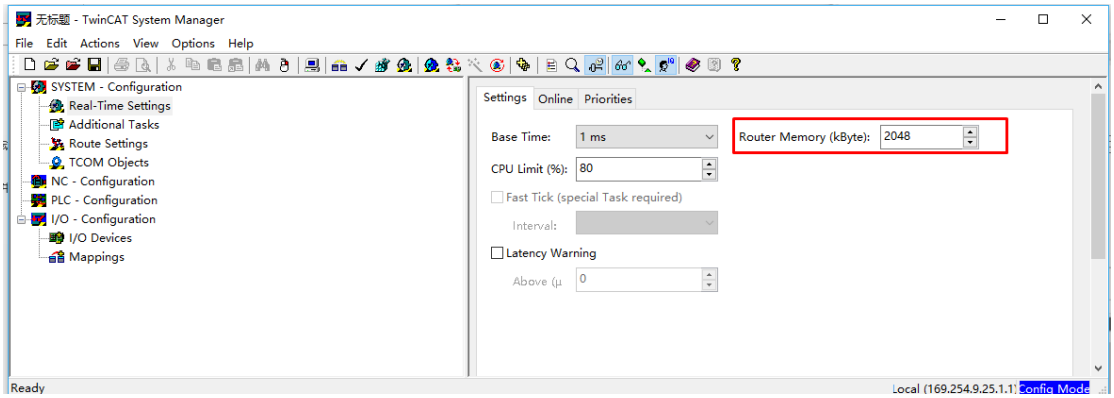
ADS 通讯报文存在错误，由于客户的 ADS Client 在请求报文中的数据信息存在异常（如 GroupIndex、OffsetIndex 等信息错误），导致 Server 在接收到请求报文会进行一些异常处理，如果这种异常报文非常多，而且可能是来之于不同的 Client 侧的，这就会导致 Ads Router 会频繁处理错误报文，如果再加之某一瞬间，CPU 的使用率有会很高时，就会导致 Ads Router 处理报文的任务被大量阻塞或过悬挂，这也会造成 Router 内存的增长（TC2 默认为 2M）、这些被阻塞或悬挂的任务也会新影响新的请求命令，这样持续运行一段时间后就会导致 Ads Router 无法再继续响应 Client 端发送的任何报文了，进而出现无法 Client 端的任何请求报文了，这样通过抓取网络报文和分析 Client 端的代码来解决。

4.2.5. 可能原因分析 5：

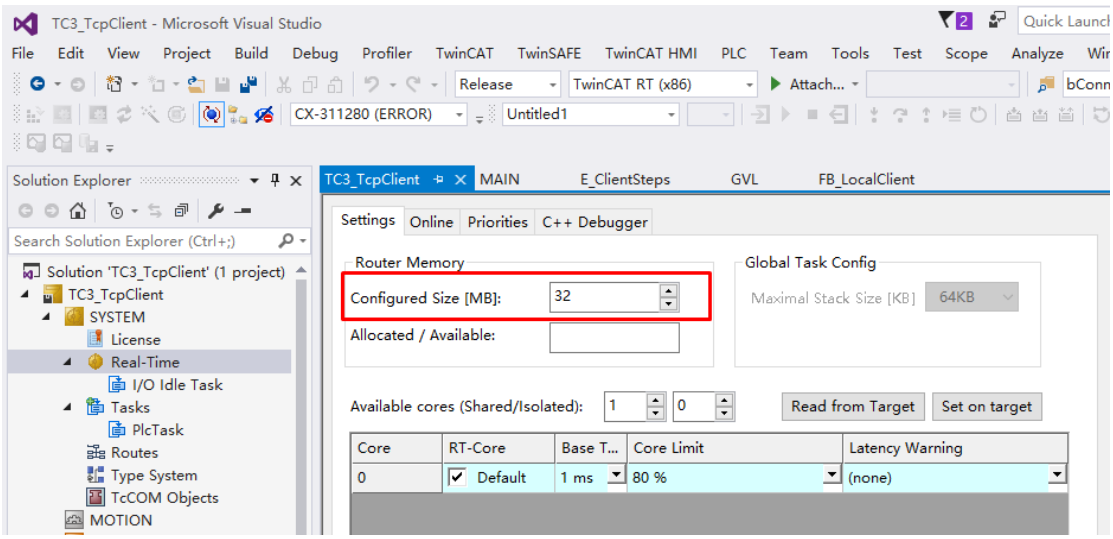
ADS Client 端代码的进行 ADS 读写方式不合理造成，ADS 通信可以采用单个变量方式读写，多个变量批量方式读写，注册事件回调方式。如果客户的代码采用批量方式读写，即多个变量的读写请求可以通过一个 ADS 报文来

完成，这就会使得该报文会较大，加之网络传输延时，可能会出现报文在传输过程中出现延迟较大或部分丢失的现象，一般在 TC2 环境下单个报文包含的变量个数不要超过 300 个（以简单数据类型计算），如果变量为复杂数据类型 Array、Struct 等，则变量个数要适当减小如 100 个，具体要依照实际报文大小来确定。 不建议客户通过注册事件回调方式进行长时间、网络间的通信。推荐的应用场景如：客户希望在一段时间内进行数据录播，在录播结束后就退出了注册回调方式通信；HMI 和 PLC 处于同一台控制器上，有一些逻辑要求在变量发生更改后能够带有时间戳的应用场合。这会造成通讯及其不稳定，注册事件回调一般适用于本机方式，且通讯一段时间后就停止的应用场景。这是由于 PLC 是以 ms 级别进行周期性执行，每个周期会产生大量的新数据，如果采用回调方式通信，则 Client 侧需要有足够快响应能力才可以使用如此之快的数据发送，否则会造成网络堵塞或者 Socket 底层异常。

当然，也可以通过设置 Router Memory 大小来提高通信的响应性和稳定性，默认 TC2 设置为 2048K，我建议用户设置为 8192K，TC2 最大可以设置到 32767K。TC3 默认为 32M，最大可以设置为 1024M。具体请依实际网络情况、通信数据量、控制器内存大小来设置。Router Memory 大小往往在 SCADA 侧尤为重要，因为 SCADA 会同时连接多个 Server 进行通信，因此 TC 环境时强烈建议设置到 32767K。 设置了 Router Memory 后一定要进行激活并重启控制器才可以生效，如果客户使用 X64 位 TC2 环境也需要点击激活按钮，即便他无法切换到运行模式。



（图 8-1　TC2 Router Memory）



（图 8-2　TC3 Router Memory）

4.2.6.　可能原因分析 6：

使用开源的 ADS Client 代码进行开发：这部分代码只实现了 ADS 协议解析和分装，只是个 demo 程序，没有自动添加路由的功能，没有 ADS Router 的功能，也没有网络可靠性方面的代码，因此，客户在使用该代码时，请合理增加 Socket 在通讯方面参数优化的部分，以提高代码稳定性，这也对开发人员提出了挑战，而且在出现通讯故障时，也是比较难于诊断的，因此除非你有足够的能力来掌控这些代码，否则还是建议选择 TwinCAT 提供的标准 ADS DLL 进行通讯。出现问题时，请选择 Wireshark 进行网络抓包，并配合代码逻辑来具体问题具体分析。

上海（ 中国区总部）
中国上海市静安区汶水路 299 弄 9号（市北智汇园）
电话：021-66312666 传真：021-66315696 邮编：200072

北京分公司
北京市西城区新街口北大街 3 号新街高和大厦 407 室
电话：010-82200036 传真：010-82200039 邮编：100035

广州分公司
广州市天河区珠江新城珠江东路16号高德置地G2603室
电话：020-38010300/1/2 传真：020-38010303 邮编：510623

成都分公司
成都市锦江区东御街18号 百扬大厦2305 房
电话：028-86202581 传真：028-86202582 邮编：610016

请用微信扫描二维码
通过公众号与技术支持交流

倍福中文官网：
http://www.beckhoff.com.cn/
倍福虚拟学院：
http://tr.beckhoff.com.cn/

招贤纳士：job@beckhoff.com.cn
技术支持：support@beckhoff.com.cn
产品维修：service@beckhoff.com.cn
方案咨询：sales@beckhoff.com.cn