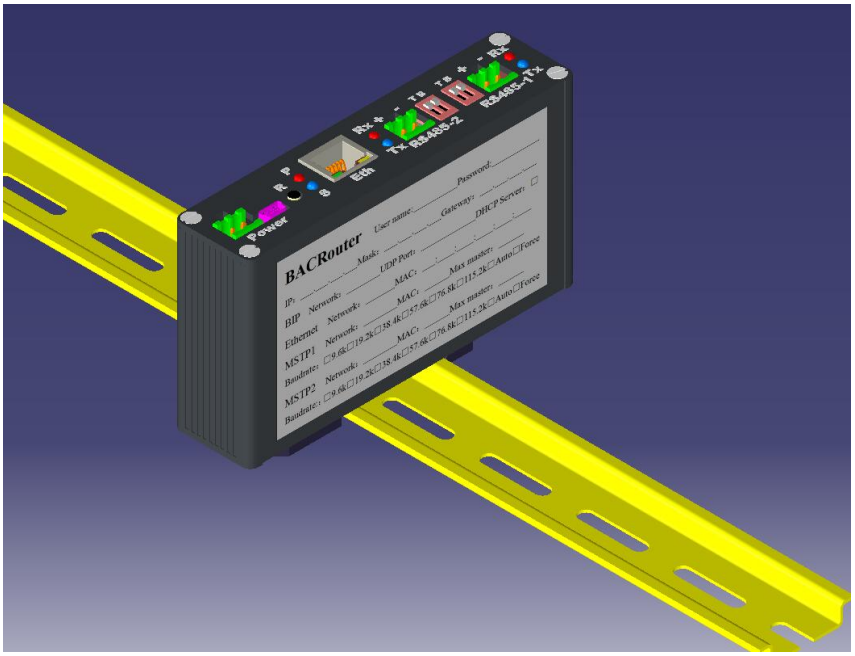
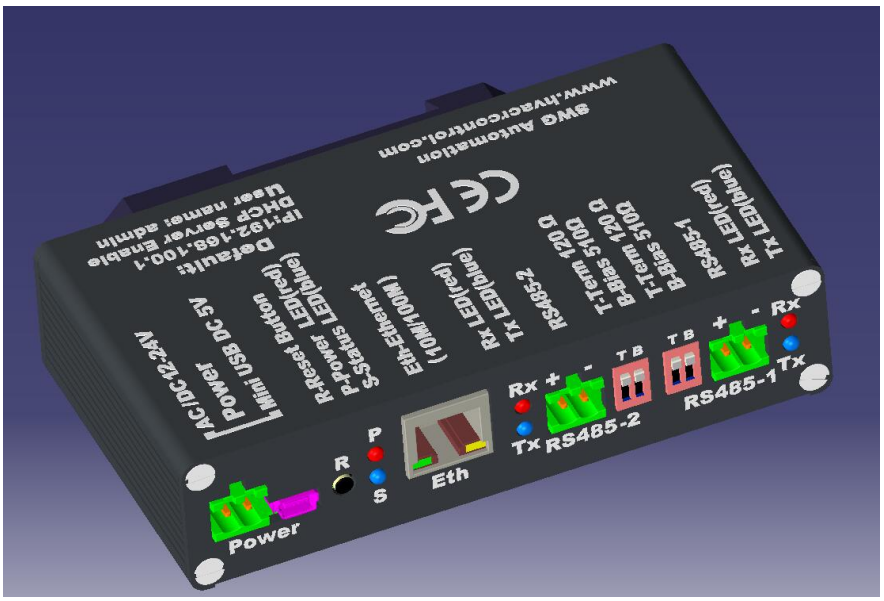
BACRouter

说明书

BACnet 路由器，Modbus 转 BACnet 网关，BBMD，从站代理





目 录

目 录（续)

特性:

BACRouter 是一款内嵌 Modbus 网关; BBMD; 从站代理功能的 BACnet 路由器。

MS/TP:

- 两个端口 1500V 独立隔离的收发器，15kV（空气放电）8kV（接触放电）ESD 保护，可以容忍误接 220VAC 电源。
- 全波特率范围（9.6kbps~115.2kbps）。支持自动波特率及波特率强制功能。
- RS485 的 AB 线允许对调。支持根据总线偏置在运行时自动检测极性。
- 1/8 收发器负载，低电容设计，支持 256 个节点以 115.2kbps 速率共存于 900 米（其它速率允许 1200 米）的总线上。
- 自带用于使能总线偏置及终端电阻的 DIP 开关。
- 提供选项以兼容不支持扩展帧的旧路由。
- 扩展的快速设备功能，加速主站轮询及设备扫描。
- 支持从设备代理功能，允许自定义搜寻范围以节省总线带宽。
- 支持按网络优先级排队。最大包延迟保证（10 秒）。
- 实时操作系统的 5 微秒精度定时与冲突检测功能，避免了帧失步，减少了总线争用。在 115.2kbps 时可达 99.6%的带宽利用率。
- 侦听模式可以在不干涉总线运行的前提下，探测总线运行情况，记录总线数据。
- 动态探测地址冲突、最大扫描地址及最近活动站点。
- 端口独立的 Tx/Rx LED 状态指示灯。

Ethernet:

- 自动协商的 10/100 Mbps 半双工/全双工端口，线缆交叉自适应。
- 绿色 LED 灯指示网络状态。

BIP:

- 支持 10 个 BACnet/IP（标准附件 J）网络运行于不同的 UDP 端口。
- 两个兼容性选项：接收错误的全局广播包、接受不匹配的目标地址。
- 支持三种运行模式：正常、广播管理设备、外部设备。
- 广播管理设备模式支持 148 个广播分布表项与 148 个外部设备表项，支持广播分布表推送到其它广播管理设备，支持网络地址映射（NAT）。
- 潜在的广播管理设备配置错误将在配置界面及运行中检测到。
- 避免广播管理设备错误配置引发的广播风暴。

路由:

- 为复杂 BACnet 网络设计的架构，性能稳定，即使多达 65534 个子网络均运转自如。
- 对网络拓扑变化快速反应，可以从配置错误中迅速恢复。
- 避免网络路由回环时的广播风暴。

包捕捉:

- 所有端口均支持包捕捉（除了 VBUS 端口）。包捕捉记录以 Wireshark 的 PCAP 格式下载。
- 将 MSTP 扩展帧转为常规数据帧，方便 Wireshark 解析。
- MSTP 支持包间隔格式，可以在 Wireshark 中精确显示包前的空闲时间，是时序与性能分析的利器。
- 支持持续化包捕捉，提供 API 接口，方便自动化流量记录以备事后分析与审计。
- 捕捉控制功能可映射到 BACnet 侧的多状态值对象。可以通过程序自动在发现通讯问题时锁定现场以备分析诊断。

Modbus 网关:

- 支持 TCP/RTU/ASCII 从站设备。
- 两种可选择的映射模式：单设备模式与虚拟设备模式。
- 物理上的单个从站设备可以映射成多个逻辑上的从站。
- 不同波特率，奇偶校验，RTU/ASCII 模式的从站可以共存于一条 RS485 总线。
- 有赖于实时系统，更多的从站设备挂载于一条 RS485 总线下仍能保证性能。
- 最多可定义 100 个主站，100 个从站，1000 个点。
- 支持 AI/AO/AV/BI/BO/BV/MI/MO/BV 等 BACnet 对象类型。
- 支持最多 2048 个 COV 订阅。可以限制 COV 通知发送速率以避免网络风暴。
- 方便的 WebUI 配置功能用以处理大量的映射及从站。
- 在线测试可以节省大量的验证调试时间。

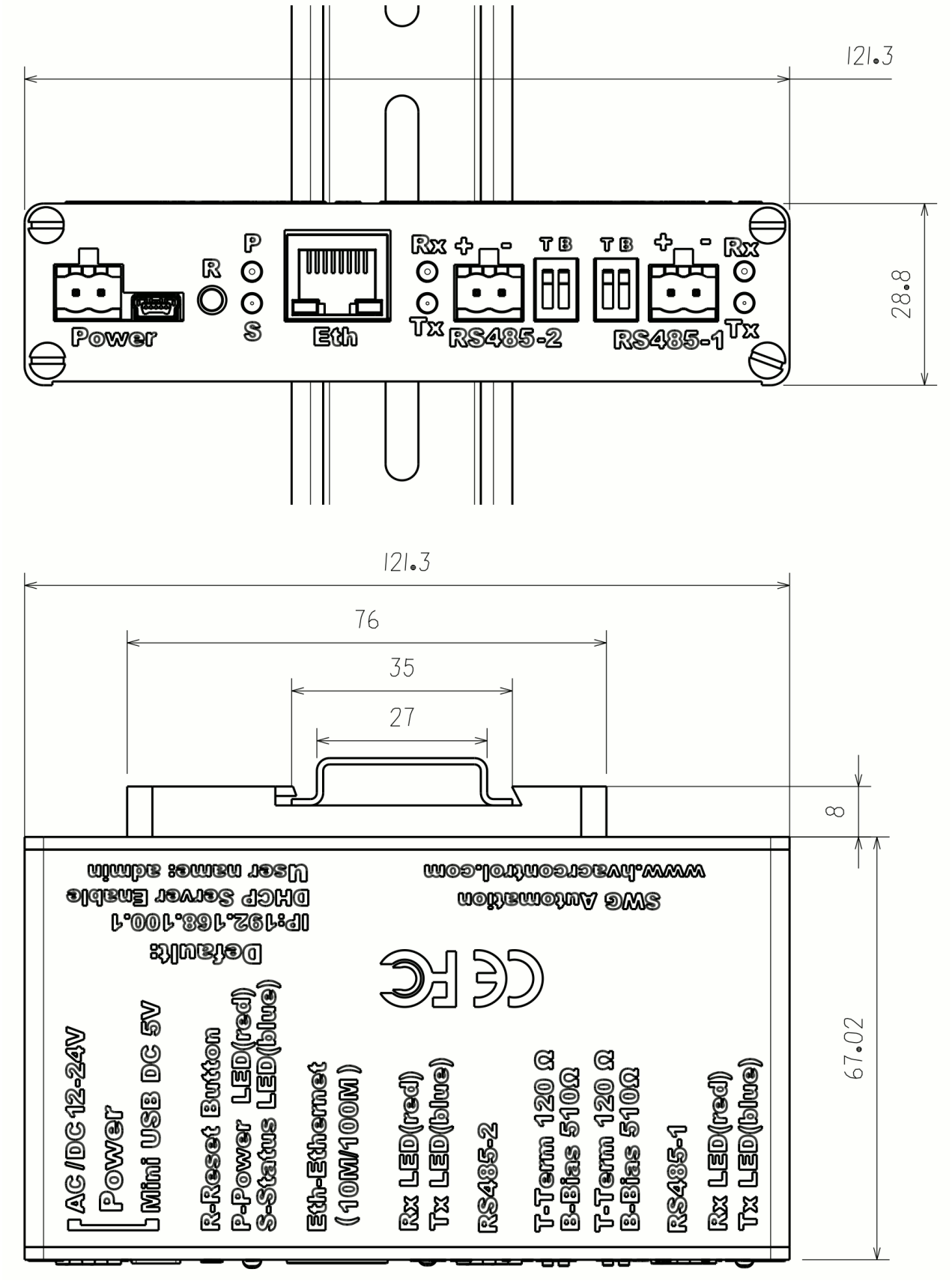
调试:

- 由密码保护的 Web 配置界面支持现代浏览器：IE(10+), Edge, 火狐，Chrome，Safari。
- 支持离线配置。可将配置导出到文件或从文件中导入配置。
- 支持由 mini USB 供电，方便现场调试时由笔记本供电。外型紧凑便携。
- 金属外壳上的 DIN 导轨卡扣方便现场安装。
- 出厂自带 DHCP 服务器，不需手工配置 PC 的 IP 地址。
- 复位按钮可将设置恢复为出厂。
- 电源灯与状态态指示设备状态。
- 详细的运行信息与日志用以诊断分析。

规格：

电源供应	12~24V ±10%交流（47~63HZ）直流两用，可插拔式两线端子座 5V 直流，mini USB 座
消耗电流	最大 3W 功率。电源为 24V 直流时，典型电流 60ma，最大 120ma
工作温度	-10ºC~80ºC
储存温度	-40ºC~90ºC
相对湿度	0 to 95%，无凝露
防护	IP30
尺寸/重量	121mm * 75mm * 29mm 金属外壳，净重 220g
以太网	IEEE 802.3 10/100M 全/半双工，线缆交叉自适应 10BASE-T, 100BASE-TX 物理层 RJ45 端子座 100 米（最大）CAT5 线缆长度
RS485	ANSI/ASHRAE 135 (ISO 16484-5) 9600, 19200, 38400, 57600, 76800, 115200 波特率 1500V 隔离 EIA-485 接口 TVS 与 PTC 提供 15kV 空气放电与 8kV 接触放电 ESD 保护 1/8 节点负载，1200 米（最大）电缆长度（115.2kbps 时 900 米） 可插拔两线端子座 DIP 开关提供 120Ω 终端电阻 DIP 开关提供 510Ω 总线偏置
合规性	CE 标志; CFR 47, 15 部分 B 类
配件	3 个两线端子，1 米 mini USB 线缆

尺寸 (毫米)：



安装：

1. 电源供应:

可在以下两种电源供应方式中选择：可插拔两线端子接入交直流通用 12~24V 电源，或 mini USB 接入直流 5V 电源。

2. 导轨安装:

通过轻推导轨卡扣的弹簧喉舌，可以轻松地将其扣入导轨上或由导轨上取下。

3. MS/TP 布线:

线缆：EIA-485 网络必须使用特性阻抗为 100~130Ω（标准 120Ω）的屏蔽双绞电缆。如果网络中的其它设备有要求，可以附加一条导线作为公用信号地。导线间的分布电容必须小于 100pF/米。屏蔽层必须单端接地以避免地环流。

连接：EIA-485 网络必须采用菊花链式连接。支线长度越短越好。T 形连接应避免采用。

最大节点数：一个网段的最大节点数是 32（针对标准负载节点）或 64（针对 1/2 负载节点）、128（针对 1/4 负载节点）、256（针对 1/8 负载节点）。更多的节点只能通过中继器连接。

终端电阻：在网段的每一端必须有一个 120Ω 的终端电阻。其它部位不得再有终端电阻。注：本路由器已内置了终端电阻，只需通过 DIP 开关启用。

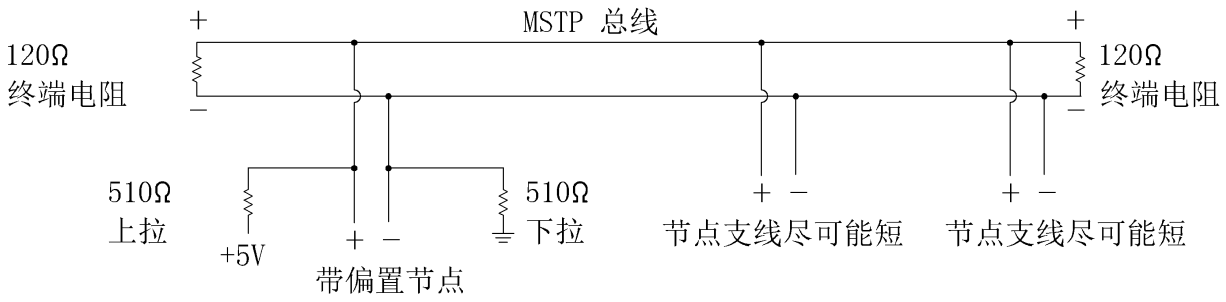


图 1: 带终端电阻与偏置的 MS/TP 总线

总线偏置：偏置电阻的使用如上图所示，每套偏置电阻由上拉电阻与下拉电阻组成，阻值均

为 510Ω 。一个网段中要有至少一套，至多两套偏置电阻（以我们的经验，两套偏置电阻会削弱收发器的总线驱动能力）。如果采用了两套偏置电阻，它们应该安装在远离的两个节点，最好靠近网段的两端，这样即使有一套偏置电阻失电，也可以维持适当的偏置电压。注：本路由器已内置了偏置电阻，只需通过 DIP 开关启用。

配置：

1. 离线配置与导入/导出:

用户不必连接 BACRouter 就可以配置它，然后将配置结果导出到文件。在现场调试时，再导入事先导出的配置文件，点击“提交并保存”就可以生效。

更多：http://www.hvacrcontrol.com/离线配置与导入导出/

2. 出厂设置及恢复:

出厂默认设置如下：IP 地址 192.168.100.1，DHCP 服务器启用。Web 界面用户名“admin”，无密码。

如需恢复到出厂设置，在正常运行状态下，使用针状物顶压小孔内的“Reset”按钮 3 秒钟以上再松开，路由器将重启并恢复到出厂设置。

3. Web 界面与系统设定:

将个人电脑的 IP 设置成自动获取（如果路由器未启用 DHCP 服务器，须将 IP 设置成与路由器同一网段）。用网线将 PC 连接到路由器的 RJ45 端口。用浏览器打开“http://192.168.100.1”（如果路由器 IP 地址已更改，请采用更改后的 IP）。如果失败，请等待 15 秒再试（DHCP 需要一些时间来分配 IP，如果一直失败，请拔出网线，等待 10 秒再插入）。

如果连接成功，浏览器将弹出窗口要求输入用户名与密码，然后出现“系统设定”配置界面。

用户名与密码：用以保护 Web 界面不被非授权访问。注意：HTTP 报文在网络上是明文传输，不能防范网络抓包的方式窃取信息。请勿在非安全环境下访问路由器。

DHCP 服务器：DHCP 服务能自动分配 IP 地址，所以连接的个人电脑不需要配置 IP 地址。注意：在生产环境下，为避免与其它 DHCP 服务器冲突，应关闭这个选项。

Root 密码：通过 SSH 程序访问路由器进行内部维护时必须提供 root 密码。Root 密码只能通过「立即设置」按钮进行修改。注意：因为安全原因，在用于生产环境前，请修改 root 密码并记下新密码。

图 2: 系统设定

4. 一般设定流程:

提交与复原：在每个配置页面上端都有「提交」与「复原」按钮，当对本页面内容做了修改后，这两个按钮将使能（未做修改前不可用）。注意：点击「提交」按钮仅表示修改被确认，但是还未保存在路由器上，如果此时刷新浏览器，提交的内容将丢失，必须在"系统设定"页面上进行保存才会生效。

保存与重启：在“系统设定”页面，有「保存并重启」按钮，如果当前有修改被提交，则此按钮将使能，点击后提交的修改将被保存，并重启路由器。

软重启通常在 5 秒钟之内完成。如果 IP 地址 / 地址掩码 / 网关 / 启用 DHCP 的选项被改动，路由器将进行**硬件重启**（相当于重新上电），以便用户确认系统设定正确生效，所以可能需要 30 秒钟完成。

如果只是点击该页面的「重启路由」按钮，则已提交的修改将被放弃，并重启路由器。

5. BACnet 侧修改：

一些参数可以从 BACnet 侧修改。这些参数在后续会提及。如果有参数被 BACnet 服务修改，BACRouter 将每三分钟保存一次修改。如在尚未保存时断电，则修改将丢失。

6. 日志:

在“系统设定”配置页面，点击上方的「日志」按钮，将弹出日志窗口。日志记录本路由器的运行信息，对故障诊断非常有用。当您需要报障时，烦请提供日志文本或截图。

图 3: 日志对话框

7. 指示灯:

Power LED 灯为红灯，当路由器上电后将长亮。

Status LED 灯为兰灯，当路由器上电或硬件重启后点亮 5 秒，然后熄灭，直至路由器软件初始化完成正常工作后，该 LED 灯将以 3 秒一次的频率闪烁。

8. 升级固件:

在“系统设定”配置页面，点击上方的「升级固件」按钮，将弹出右方所示窗口，选择固件文件后点击「提交」按钮。

固件升级需要一至两分钟，中途勿断电。升级成功后页面将自动刷新，同时”系统设定“页面将显示新的固件版本号。

如果“保留配置”未被选中，则当前配置将被缺省配置覆盖。

固件文件名的格式为 bacnet_router_X_Y.tar.gz，其中 X 为版本号，Y 为校验值。

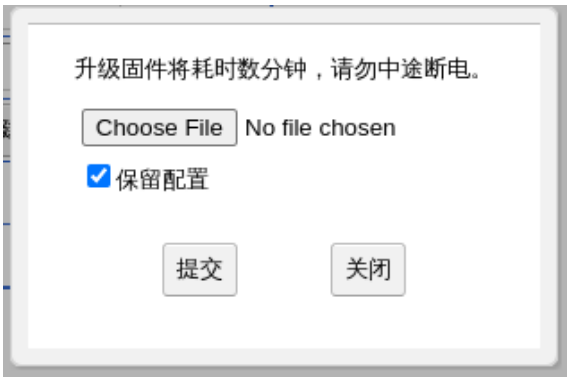


图 5: 固件升级

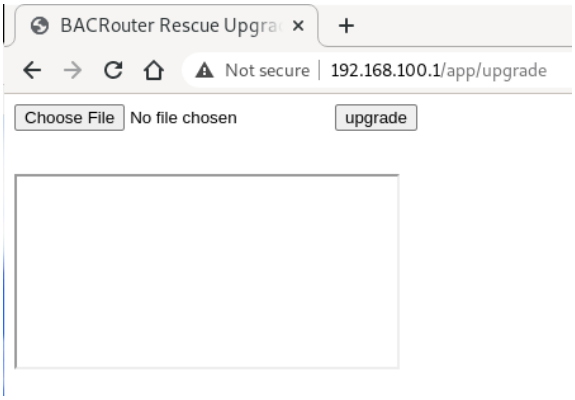


图 4: 固件紧急升级

紧急升级：WebUI 是一个复杂的 Javascript 程序，有时程序缺陷有可能导致用户无法进入配置界面，此时也无法升级到其它版本。BACRouter 提供一个紧急升级的入口，位于：

http://ip/app/upgrade 紧急升级界面仅由 HTML 构造，所以可以工作于任何浏览器中。

网络层设定:

网络层最多可以创建 10 个端口。

1. VBUS 端口：

VBUS 是虚拟的链路层端口，最大 NPDU 长度为 1497 字节，可容纳最多 254 个虚拟 BACnet 设备，用于网关功能。如仅须路由功能，此端口应被删除或停用。

图 6: 网络层设定

2. 路由表：

路由表可以此处显示。如果路由表项超过限制（此限制大于 1000 个），超出的表项将被忽略。如果任一个网络配置被修改，此功能将停用。

3. 网络号:

在 BACnet 互联网络中，每个子网的有效网络号范围是 1~65534（0 代表本地网络，65535 代表全局广播），且不得重复。如果仅有一个子网，则网络号无意义。

自动学习：在标准附录 135-2008g 中，引入了 What-IS-Network-Number 与 Network-Number-Is 两种网络层报文，允许路由器在运行中自动学习网络号。本路由器支持这个功能，如将网络号配置为 0，则启动后将自动查询网络号，直到得到结果。

网络号也可被 BACnet 侧的 Initialize-Routing-Table 服务请求所修改。

4. 包捕捉:

本路由器每个启用的端口均支持包捕捉。包捕捉可以配置成自动开启或运行中手动开启。

图 7: 包捕捉对话框

自动开启：须在端口的配置界面，选择包捕捉缓冲区大小，保存重启后自动开启包捕捉。

运行中手动开启：则需在启用的端口的 Web 配置页面中，点示上方「包捕捉」按钮，在弹出的窗口中，选择包捕捉缓冲区大小，然后点击「开始捕捉」。注：如果任何配置被修改并提交，「包捕捉」按钮将失效。

缓冲区大小：缓冲区大小可选范围为 64k～16M 字节，或不启用。注意：所有端口启用的缓冲区大小总和不能超过 16M，否则将报错。

下载：包捕捉记录可以用 Wireshark 的文件格式下载，然后在 Wireshark 中浏览分析。下载的文件名格式为：

TX_Y_Z.cap，其中 T 为捕捉格式，正常为 n，X 为启用的端口序号，Y 为本下载第一个包的序号，Z 为本下载之后的包序号，cap 为 Wireshark 包捕捉文件后缀名。

下载历史与继续下载：因为缓冲区的大小有限，如果捕捉的时间过长，则旧数据将被覆盖。为方便长时间地保存通讯记录，本路由器保存了 4 次下载历史记录，可以从相应下载历史记录接续下载。在每次下载后，刷新包捕捉页面，可以看到下载历史将被更新。下载历史以起初包序号与下一包序号作为标记，点击每个下载历史的继续下载，就可以接续原先的下载（包序号是前后搭接的），这样可以把长时间的捕捉数据，分为多个文件下载。多个接续的

下载文件可以在 Wireshark 中合并成一个单独的文件。

更多：https://www.wireshark.org/docs/wsug_html_chunked/ChIOMergeSection.html

从 BACnet 侧控制：如果下一节中的客户端模式未使能，BACnet 应用层将被启用，捕捉控制功能将被映射为多状态值对象。

每个支持包捕捉的路由端口将有 2 个多状态值对象。一个对象用于缓冲区的大小，有“64K”, “128K”, “256K”, “512K”, “1M”, “2M”, “4M”, “8M” 与 “16M”等状态值。另一个对象用于控制，有“Stop&Clean”, “Start” 与 “Stop”等状态值。

5. **一般运行信息:**

图 8: 一般的运行信息

在每个启用的端口的配置界面，点击「运行信息」按钮，将弹出运行信息窗口。注：如任意配置被修改并提交，则「运行信息」按钮将失效。

网络号：网络层报文 Initializing_Routing_Table 与 Network_Number_Is 可以修改网络号。此处显示当前网络号与网络号状态。网络号状态分为：本地或网络配置，动态学习，未配置。

BIP 相关设定:

BIP 端口的 IP 地址将会自动从”系统设定“中提取。

1. **接收错误的广播:** BACnet 标准要求 BIP 广播使用子网广播地址，但是有的设备（大部分为 Windows 系统下的软件）不正确地采用了 255.255.255.255 全局广播地址。为兼容这部分

设备，可以选择本选项。注：当工作模式为外部设备，或为广播管理设备且启用了 NAT 时，本选项无效。

2. **接受不正确的地址:** BIP 的 Original-Unicast-NPDU 报文为单播报文，Original-Broadcast-NPDU 报文为广播报文。但是有的设备没有正确地采用。选择本选项将接受这些错误的报文，否则将丢弃。注：当工作模式为外部设备，或为广播管理设备且启用了 NAT 时，本选项无效。

图 9: BIP 正常模式设定

3. **广播管理设备模式:**

在 IP 网络中，跨网段的数据包通过 IP 路由器传递，为了减少广播流量，IP 路由器一般不会转发广播包。为了解决这个问题，需要在每个 IP 子网内设置一个广播管理设备（BACnet 标准附录 *135-2008o* 允许一个 IP 子网内有多个广播管理设备，但是须小心配置以免造成广播风暴，建议每个 IP 子网仅有一个广播管理设备）。广播管理设备主要两个功能：转发 BACnet 广播包，接受外部设备注册。

同子网多个广播管理设备：当本路由器发现某个广播管理设备不在本地的广播分布表中时，可能该子网内有多个广播管理设备。如果本选项未被选中，则本路由器将拒绝此广播管理设备转发的包并在日志中记录错误。

广播分布表推送：在传统的广播管理设备方案中，每个子网仅有一个广播管理设备，所以所有的广播管理设备中的广播分布表都是一致的。为了方便管理多个广播管理设备的广播分布表，可以在本 BIP 端口上启用广播分布表推送，然后在其它的广播管理设备上设置接受广播分布表写入。那么只要在本 BIP 端口上修改一次广播分布表，其它的广播管理设备上的广播分布表将同时得到更新。当”同子网多个广播管理设备“功能被启用时，此选项不可用。

图 10: BIP 广播管理设备模式设定

网络地址映射：当需要与外网联接时，外网 IP 路由器可工作于网络地址映射（NAT）方式，把外网的 IP：端口映射到本地的 IP：端口，因此需要启用本 BIP 端口的网络地址映射，并将外网的 IP：端口填入。当处于网络地址映射方式时，因为内网的其它节点无法与外网直接通讯，建议本路由器创建独立的 BIP 端口与内网通讯，本 BIP 端口专用于与外网通讯。注：为安全起见，在接入互联网时，请与 VPN（虚拟专用网络）配合使用，以防止未授权访问。

跨网广播支持：网络地址映射未选中时有效，指本 IP 子网的 IP 路由器是否支持跨网广播。

注：市面大多数 IP 路由器不支持本功能。

接受广播分布表写入：启用后，接受广播分布表的写入（可以配合上面的广播分布表推送功能工作）。为了防止误写入，可以关闭这个功能。

接受外部设备注册：启用后，可以接受外部设备注册。

广播分布表：记录所有广播管理设备，可以添加及修改。注：本 BIP 端口作为广播管理设备，将由后台自动加入广播分布表，不需在此处输入。

运行信息中的外部设备表：当前注册的外部设备，每行一个设备，格式为

X:Y Z T，其中 X 为 IP 地址，Y 为 UDP 端口，Z 为存活时间（秒），T 为剩余时间（秒）。

图 11: BIP 运行信息

4. 外部设备模式:

外部设备通过注册到广播管理设备来接收 BIP 广播，不接收本地的广播包。

图 12: BIP 外部设备模式设定

注册时间间隔：固定时间间隔进行注册，以免存活时间到期后注册无效。

注册存活时间：存活到期后将被广播管理设备删除，建议大于注册时间间隔的 3 倍。

MS/TP 相关设定:

1. 简单模式及扩展模式:

本路由器在 BACnet 的标准之外，增加了许多扩展功能。为了方便配置，提供两种配置模式：简单模式只提供标准定义功能的配置项，扩展模式提供所有功能的配置项。

图 13: MS/TP 简单模式设定

图 14: MS/TP 扩展模式设定

2. 波特率:

BACnet 的标准定义了 9600，19200，38400，57600，76800，115200 六种固定波特率。本路由器扩展了自动与强制波特率。

更多：http://www.hvacrcontrol.com/mstp-固定自动强制-波特率/

自动波特率：此为扩展功能。启动后，监听总线，切换波特率，直至检测到正确的帧头。

注：如启动时总线空闲，因为无法检测到正确的帧头，将一直处于等待模式。

在运行中，如果长时间连续错误，认为波特率出错，再次切换波特率，直至检测到正确帧头，或检测到总线空闲，采用上次检测到的波特率。

强制波特率：此为扩展功能 。预设一个波特率，在运行中，将总线波特率强制为预设的波特率。此机制与自动波特率类似，除了 2 个地方：A. 启动后，如总线空闲，采用预设的波特率。B. 取得令牌后，采用预设的波特率。

强制波特率的设备可以将自动波特率的设备的波特率切换到预设值。

3. AB 线极性:

此为扩展功能。如设为“自动”，在运行中，如果长时间连续错误，认为极性出错，切换极性重试，直至检测到正确帧头或总线空闲。

4. 侦听模式:

此为扩展功能。此模式下，路由器静默地侦听总线上通讯，所有接收与请求发送的 NPDU 全部抛弃。在此模式下，以下配置项均无效。

5. 扩展帧支持:

标准修订版 16 引入了扩展帧。但是在支持扩展帧的设备与旧路由之间存在互操作性问题。如果同总线上有其它旧路由，请关闭此功能。即便取消扩展帧支持，BACRouter 仍然与支持扩展帧的设备保持兼容。

更多：http://www.hvacrcontrol.com/mstp 支持扩展帧设置与旧设备的互操作问题/

6. 本地 MAC 地址 / 最大扫描地址:

本地 MAC 地址在本总线上必须唯一，有效值为 0~127。所有节点的最大扫描地址设置必须相同。

为了选择一个未被使用的本地 MAC 地址及与其它节点一致的最大扫描地址，可以将 BACRouter 运行于侦听模式，然后根据运行信息页面的“最近活动的其它站点”，选择一个未被使用的 MAC 地址，从“当前最大扫描地址”中找到当前使用的最大扫描地址。

第一个 MS/TP 端口的最大扫描地址设置可以从 BACnet 侧修改。

7. 一次最大发包数:

该数值为本地取得令牌后，发送多少数据包才传出令牌。数值最高，本地发包速度越大，但有可能造成过长时间的令牌占用。

第一个 MS/TP 端口的一次最大发包数设置可以从 BACnet 侧修改。

根据令牌占用时间：此为扩展功能 。MS/TP 发送每一个包占用的时间不同，牵涉到包长度，是否等待应答及应答占用时间。采用发包数做为计量单位，并不能线性地计量发包速率与令牌占用时间，影响总线实时性。选择本选项后，将采用令牌占用时间来计量（以一次发包占用 32 个字节的发送时间为基准），时间到就不再发包，并传出令牌。

更多：http://www.hvacrcontrol.com/一次最大发包数与根据令牌占用时间/

8. 快速设备:

此为扩展功能。为兼容慢速的设备，BACnet 标准中的超时参数较大，造成带宽浪费，特别是在高波特率时。BACRouter 在标准超时参数外，增加一组快速超时参数，该组参数可以应用于指定的快速设备以提高网络性能。

如果快速设备通过中继器连接，中继器带来的延迟（包括发送延迟及接收延迟）须考虑在内。BACnet 标准允许每个中继器 2 位且整个总线最多 10 位的延迟。

快速设备超时：快速设备的轮询超时，快速主站设备的回应超时，快速从站设备的回应超时，这三个超时参数定义了快速设备的性能。

快速设备选择：选择哪些设备为快速设备。

图 15: 选择 MS/TP 总线上的快速设备

9. 从设备代理:

MS/TP 从站及不支持 Who-IS 功能的主站，称为从设备。从设备代理为他们提供 Who-IS 功能支持。从设备代理采用 ReadProperty 或 ReadPropertyMultiple 服务请求由从设备中读取信息并保存在本地，当收到对应的 Who-IS 查询时，替代从设备发送 I-AM 应答。

扫描时间间隔：有效值 120 秒～65535 秒。每隔一段时间重新读取并更新从设备的信息。

自动搜寻：除了在手动绑定中定义的从设备外，自动搜录其它的从设备。注：自动搜寻会占用大量的带宽，建议加大扫描时间间隔，或启用**快速设备**与下面选择搜寻节点两项扩展功能以节省带宽。

选择搜寻站点：此为扩展功能。只有被选中的站点而不是所有站点，才会被自动搜寻。

图 16: MS/TP 从设备代理设定

手动绑定：根据 BACnet 标准 ，ReadProperty 或 ReadPropertyMultiple 服务请求中的设备实例号可以采用 4194303 这一特殊值来匹配任何设备，因此事先无需知道设备的实例号。不幸的是，在早期版本的标准中，不支持此功能。如果从这些设备中读取设备信息，必须知道其设备实例号。手动绑定功能就是服务于这些旧版本设备，将其 MAC 地址与对应设备实

例号记录在此。

10. Tx/Rx 指示灯:

每个 MS/TP 端口均有一个 Tx 灯（兰色）与一个 Rx 灯（红色）。Tx 灯在发送任何数据时闪烁（因此当路由器加入令牌循环后，Tx 灯将持续闪烁），Rx 灯仅当收到发给本地或广播的数据帧时闪烁。注：在侦听模式下，收到任何数据帧，Rx 灯均闪烁。

11. 运行信息:

图 17: MS/TP 运行信息

令牌循环速率：代表每分钟令牌循环了多少轮。显示的是最近 30 秒的平均值。

错误计数：计有：引导字节错，帧头错，帧数据错，扩展帧解码错，传递令牌重试，传递令牌失败，可能的令牌冲突，令牌丢失，BACnet 请求无应答，帧间隔过小。如果某计数持续不断地增加，总线上就可能存在问题。

当前最大扫描地址：实时监测到的当前最大扫描地址。注：如果标注”与本地配置不符“，可

能总线上有其它站点的配置值不一致。

最近活动的其它站点：记录最近三十秒内收到所有帧的源 MAC 地址。注：如果 MAC 地址为红色字体，表示可能存在地址冲突。

波特率与 AB 线极性：此为扩展功能，当波特率设定为“自动”或“强制”，或 AB 线极性为自动时有效。显示当前波特率、AB 线极性或“探测中”。

代理的从设备：当从设备代理启用时有效。每行显示一个代理中的从设备，格式如下：

X:Y, L, S, I:N 其中 X 为 MAC 地址，Y 为设备实例号，L 为最大 APDU 长度，S 为数据包分段支持，I 为生产商 ID，N 为生产商名称。

12. 包捕捉特性:

如何分帧：基于两个规则：正确解析的帧结束后的数据视为新的一帧。总线空闲超过 33 位时长视为新一帧开始。

更多：http://www.hvacrcontrol.com/mstp 帧失步解决方案/

错误处理：错误分为几种：信号噪声，停止位不符，字节间隔过长（根据 BACnet 标准，两个字节之间的空闲时长不得超过 20 位），数据校验错（包括 CRC 校验，包长校验），数据不完整。发现错误后，本身产生错误的数据及之后的所有数据不被记录，直至新一帧开始。

扩展帧处理：标准附录 *135-2012an* 定义扩展帧，使用 CRC32 校验及 COBS 编码。其中帧类型 BACnet Extended Data Expecting Reply 与 BACnet Extended Data Not Expecting Reply 用于 BACnet 通讯。包捕捉在错误校验时，仅做 CRC32 校验，不对 COBS 编码较验。因为 Wireshark 不支持扩展帧的解码，所以在输出包捕捉文件时，作如下处理：

如果帧类型为 BACnet Extended Data Expecting Reply 与 BACnet Extended Data Not Expecting Reply，尝试 COBS 解码，如果解码成功，将帧类型改为 BACnet Data Expecting Reply 与 BACnet Data Not Expecting Reply，并生成 CRC16 校验码。这样在 Wireshark 中就会视为正常的 MS/TP 数据包，并解析网络层与应用层内容。如果 COBS 解码不成功，生成 CRC16 校验码输出，这样在 Wireshark 中就会视为未知类型的 MS/TP 数据包。

其它帧类型只生成 CRC16 校验码输出，这样在 Wireshark 中就会视为未知类型的 MS/TP 数据包。

图 18: MS/TP 包捕捉

包间隔格式：在分析 MS/TP 时序错误与响应性能时，包的绝对时间不重要，而前后两包之间的空闲间隔时间更需关心。包间隔格式的时间戳以包间隔的时间长计时（5 微秒精度）。下载文件以 i 打头（正常格式以 n 打头）

在 Wireshark 中打开包间隔格式，在上方菜单选择“视图”->“时间显示格式”->“自上一捕获分组经过的秒数”。在下方的包时间栏中显示的秒数即为包前的空闲间隔。

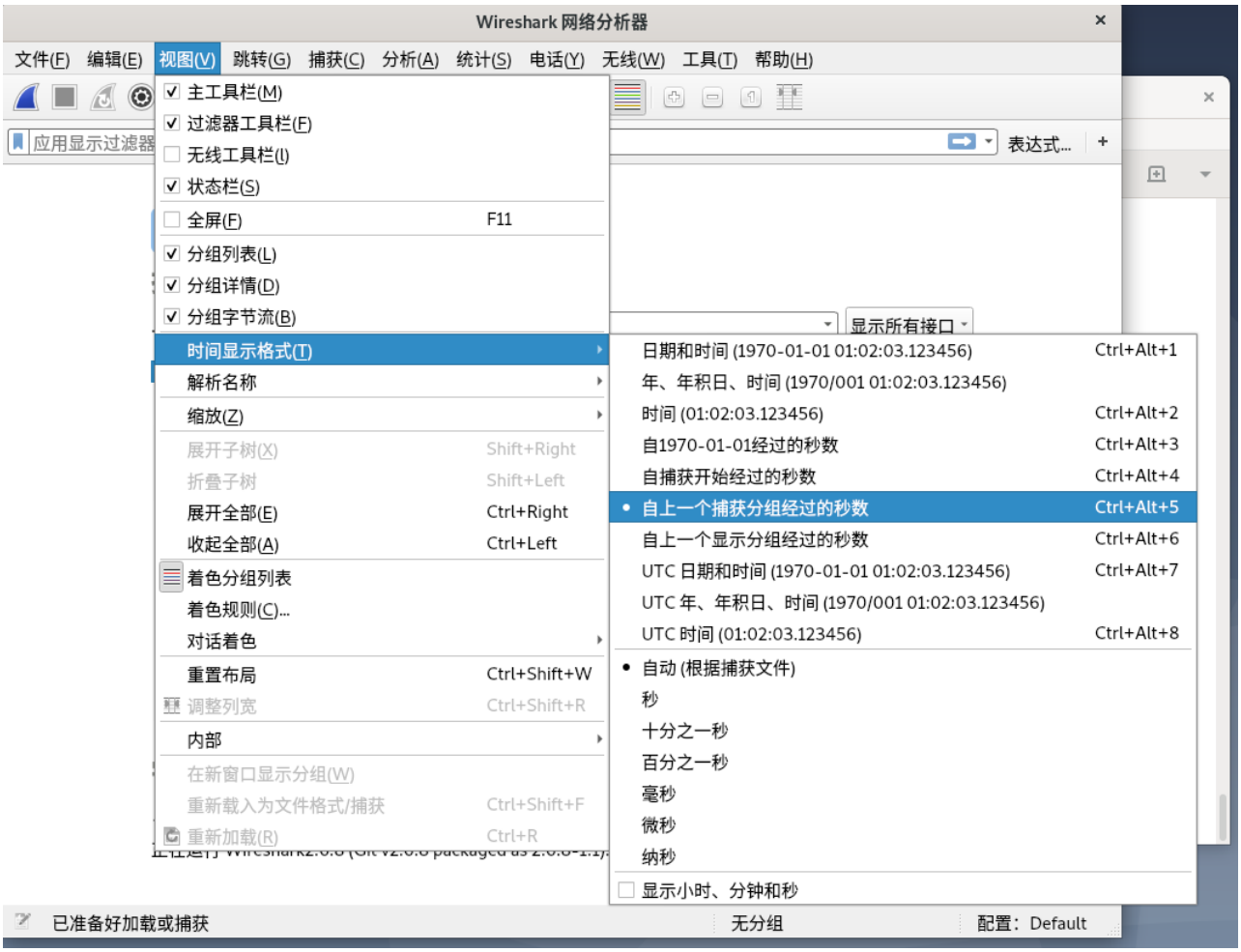


图 19: 为包间隔格式设置 Wireshark 时间显示格式

应用层设定:

配置界面选择左边的「应用层」，打开应用层配置界面。

1. APDU 超时与重试：

这两个参数用于 BACnet 有确认服务，可以从 BACnet 侧修改。如果在 BACRouter 内有虚拟设备，则所有设备共享这两个参数。

2. 客户端模式：

路由器的路由层功能不需要应用层，如果不考虑标准的兼容性，可以启用客户端模式，如此就不需要配置“设备实例号”等参数。注：客户端模式不支持网关功能。

图 20: 应用层设定

3. 设备实例号：

实例号有效范围 0~4194302 且必须全网唯一。此参数可从 BACnet 侧修改。

4. 名称分隔符：

BACRouter 内的 BACnet 对象名可能由多个部分组成，比如 Modbus 映射点的对象名可能由主站名，从站名，点名组成，这些组成部分由名称分隔符连接形成最后的对象名。

5. COV 通知发送限制：

BACRouter 支持最多 2048 个 COV 订阅。当被订阅的对象值改变时，BACRouter 可能发出大量的 COV 通知，特别是在映射的 Modbus 从站上线/下线时。为了避免网络风暴，在这里可以限制 COV 通知的发送速率。注：如果 COV 通知发送速率达到限值，通知将被延迟发送。

Modbus 网关:

具体的 Modbus 网关实现细节，可以参考：

http://www.hvacrcontrol.com/bacrouter 中的 modbus-网关/

1. 映射模式：

单设备模式：如果 VBUS 端口未使能，BACRouter 将工作于单设备映射模式下，所有 Modbus 从站都将映射到“应用层设定”中定义的 BACnet 设备中，每一个从站占据 1000 个独立的对象实例空间。

虚拟设备模式：如果 VBUS 端口被使能，每一个 Modbus 从站将被映射为 VBUS 虚拟网络上的虚拟 BACnet 设备。其 MAC 地址将从 1 开始自动分配。虚拟设备的设备实例号可从 BACnet 侧修改。

2. 在线测式：

如果主站已使能且配置修改已保存，当配置从站时，在线测试就可以节省大量的验证调试时间。

点测试：当编辑点映射时，有一栏“测试裸数据“及「读」按钮及「写」按钮（如该对象可写），点击按钮，”测试结果“栏将显示结果。

裸数据的含义为未经换算。

图 21: Modbus 点测试

编组读取测试：在”编组读取“对话框，「测试」按钮将按编组进行读取并显示测试效果。

图 22: Modbus 编组读取测试

如果从站类型是 RTU/ASCII，测试结果将包含响应时间，可参考其在”Modbus 参数“对话框中设置恰当的”回应超时“参数。

3. 运行信息：

如果主站从站均已使能且配置修改已保存，「运行信息」将显示从站与各点的当前状态。

图 23: Modbus 运行信息

4. 映射建议：

对于不经 BACnet 控制的 Modbus 点，建议采用 BACnet 输入（Input）或值（Value）对象。

对于仅由 BACnet 控制的 Modbus 可写点，建议采用 BACnet 输出（Output）或值（Value）对象。

对于由 BACnet 和其它机制同时控制的 Modbus 可写点，可以有 3 种映射机制：

a. BACnet 值（Value）对象。Present_Value 属性将是可写的，来自 BACnet 的写动作将被转发到 Modbus。从 Modbus 读回的值将更新 Present_Value 属性。

b. BACnet 输出（Output）对象。Modbus 读回的值将更新 Relinguish_Default 属性。注：BACRouter 不支持 SubscribeCOVProperty 服务，所以没有办法为 Relinguish_Default 发出 COV 通知。

c. 一个 BACnet 输出（Output）对象及另一个 BACnet 输入（Input）或值（Value）对象。BACnet 输出（Output)对象用于命令逻辑，BACnet 输入（Input）或值（Value）对象反映 Modbus 读回的值。

当一个从站设备内的不同 Modbus 地址代表多个不同的真实设备时，可以将其映射成多个逻辑上的从站，每个逻辑从站映射不同的 Modbus 地址以反映不同的真实设备。

5. 批量处理技巧：

「导入 CSV」与「导出 CSV」可用于创建大量的映射，采用 CSV 格式可以轻松地在 Excel 软件中输入编辑对象名与描述。

「批量换算」可用于修改所有模拟量对象的换算系数。

「批量地址」可用于批量修改点的 Modbus 地址。

「导入点表」由从站的配置文件导入点表。从站自身的配置保持不变。

「复制」以当前主站或从站的配置为模板生成新的主站/从站。

「批量导入」由主站的配置文件导入其中的所有从站。当前已有从站保持不变。

「批量实例号」修改所有从站的对象实例号。

「批量点表」由从站的配置文件导入点表，并应用于多个从站。

常见问题:

1. 路由回环:

BACnet 标准不允许任何路由回环，即任意两个设备之间，只能有一条路由通路。路由回环导致广播风暴与丢包。常见的配置错误如：两个同网段的设备同时开启 IP 端口与 Ethernet 端口，形成 IP 与 Ethernet 两个路由通路。日志中频繁的路由错误或警告信息可以辅助判断路由回环。

2. 网络号冲突:

BACnet 互联网络中每个子网的网络号必须是唯一的。如果冲突，将造成丢包。日志中的路由错误或警告信息可以辅助判断网络号冲突。

3. MS/TP 无法通讯:

最常见的 MS/TP 无法通讯的原因是：**总线未偏置**。如果没有正确的偏置，当两个包之间总线空闲时，AB 线间的电压接近 0，此时总线的抗干扰能力极弱。请确保总线有一处偏置（最简单的是把本路由器上的偏置 DIP 开关打到“ON”的位置）。

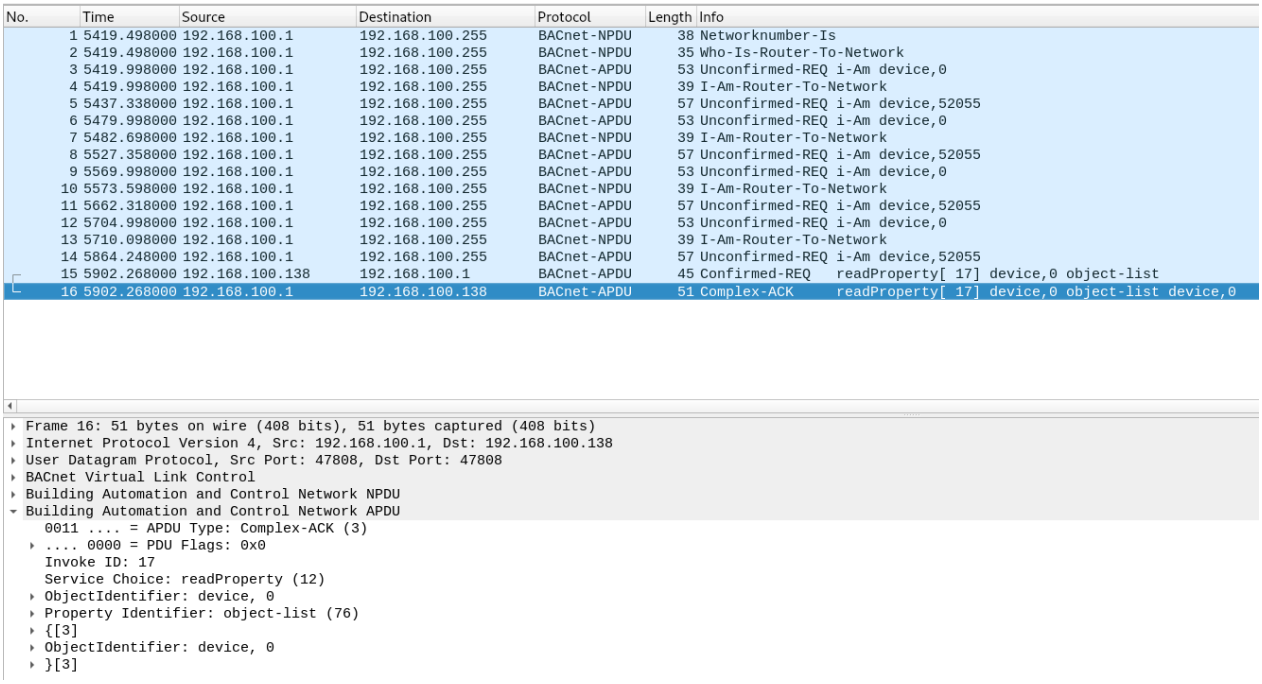
最大扫描地址不匹配可能导致部分设备无法得到令牌，请注意运行信息中的当前最大扫描地址信息，确保所有主站设备的 MAC 地址小于等于此数值。

其它原因包括波特率不匹配、AB 线极性错误，MAC 地址冲突等。不恰当的扩展功能设置也是可能原因。

4. Wireshark 软件:

Wireshark 的下载地址：https://www.wireshark.org/download.html

下图为 BIP 捕捉文件分析界面：

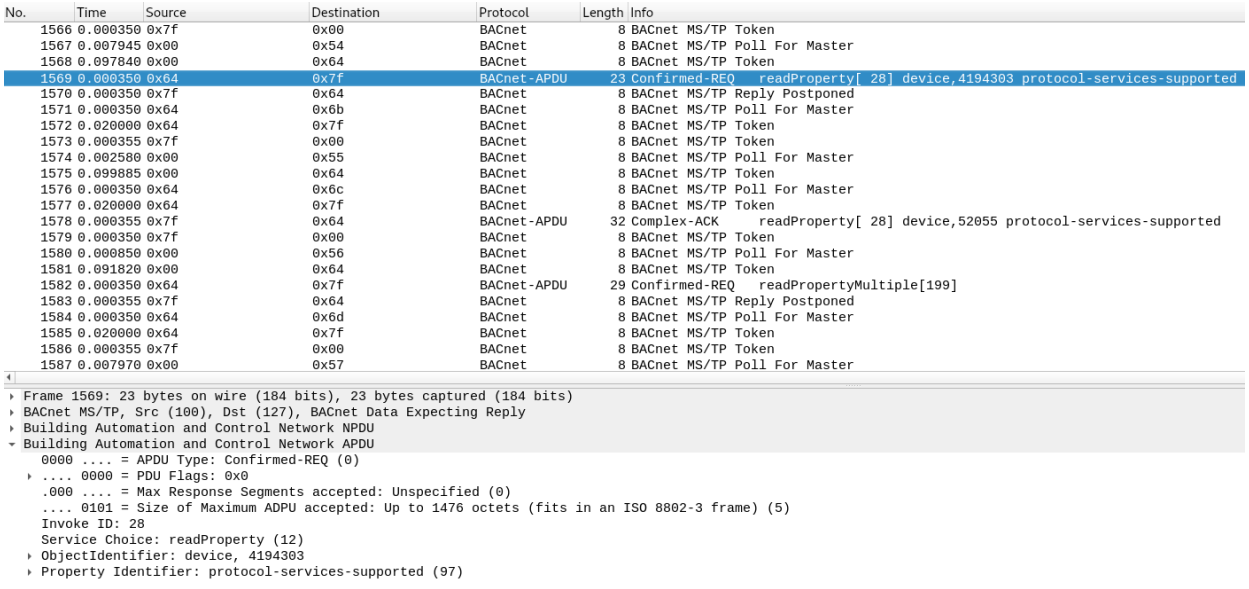


No.	Time	Source	Destination	Protocol	Length	Info
1	5419.498000	192.168.100.1	192.168.100.255	BACnet-NPDU	38	Networknumber-Is
2	5419.498000	192.168.100.1	192.168.100.255	BACnet-NPDU	35	Who-Is-Router-To-Network
3	5419.998000	192.168.100.1	192.168.100.255	BACnet-APDU	53	Unconfirmed-REQ i-Am device,0
4	5419.998000	192.168.100.1	192.168.100.255	BACnet-NPDU	39	I-Am-Router-To-Network
5	5437.338000	192.168.100.1	192.168.100.255	BACnet-APDU	57	Unconfirmed-REQ i-Am device,52055
6	5479.998000	192.168.100.1	192.168.100.255	BACnet-APDU	53	Unconfirmed-REQ i-Am device,0
7	5482.698000	192.168.100.1	192.168.100.255	BACnet-NPDU	39	I-Am-Router-To-Network
8	5527.358000	192.168.100.1	192.168.100.255	BACnet-APDU	57	Unconfirmed-REQ i-Am device,52055
9	5569.998000	192.168.100.1	192.168.100.255	BACnet-APDU	53	Unconfirmed-REQ i-Am device,0
10	5573.598000	192.168.100.1	192.168.100.255	BACnet-NPDU	39	I-Am-Router-To-Network
11	5662.318000	192.168.100.1	192.168.100.255	BACnet-APDU	57	Unconfirmed-REQ i-Am device,52055
12	5704.998000	192.168.100.1	192.168.100.255	BACnet-APDU	53	Unconfirmed-REQ i-Am device,0
13	5710.098000	192.168.100.1	192.168.100.255	BACnet-NPDU	39	I-Am-Router-To-Network
14	5864.248000	192.168.100.1	192.168.100.255	BACnet-APDU	57	Unconfirmed-REQ i-Am device,52055
15	5902.268000	192.168.100.138	192.168.100.1	BACnet-APDU	45	Confirmed-REQ readProperty[17] device,0 object-list
16	5902.268000	192.168.100.1	192.168.100.138	BACnet-APDU	51	Complex-ACK readProperty[17] device,0 object-list device,0

```
▸ Frame 16: 51 bytes on wire (408 bits), 51 bytes captured (408 bits)
▸ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.138
▸ User Datagram Protocol, Src Port: 47808, Dst Port: 47808
▸ BACnet Virtual Link Control
▸ Building Automation and Control Network NPDU
▾ Building Automation and Control Network APDU
    0011 .... = APDU Type: Complex-ACK (3)
  ▸ .... 0000 = PDU Flags: 0x0
    Invoke ID: 17
    Service Choice: readProperty (12)
  ▸ ObjectIdentifier: device, 0
  ▸ Property Identifier: object-list (76)
  ▸ {[3]
  ▸ ObjectIdentifier: device, 0
  ▸ }[3]
```

图 24: 用 Wireshark 中打开捕获的 BIP 包

下图为 MS/TP 捕捉文件分析界面（波特率为 115.2kbps，注意这里采用了包间隔显示格式）：



No.	Time	Source	Destination	Protocol	Length	Info
1566	0.000350	0x7f	0x00	BACnet	8	BACnet MS/TP Token
1567	0.007945	0x00	0x54	BACnet	8	BACnet MS/TP Poll For Master
1568	0.097840	0x00	0x64	BACnet	8	BACnet MS/TP Token
1569	0.000350	0x64	0x7f	BACnet-APDU	23	Confirmed-REQ readProperty[28] device,4194303 protocol-services-supported
1570	0.000350	0x7f	0x64	BACnet	8	BACnet MS/TP Reply Postponed
1571	0.000350	0x64	0x6b	BACnet	8	BACnet MS/TP Poll For Master
1572	0.020000	0x64	0x7f	BACnet	8	BACnet MS/TP Token
1573	0.000355	0x7f	0x00	BACnet	8	BACnet MS/TP Token
1574	0.002580	0x00	0x55	BACnet	8	BACnet MS/TP Poll For Master
1575	0.099885	0x00	0x64	BACnet	8	BACnet MS/TP Token
1576	0.000350	0x64	0x6c	BACnet	8	BACnet MS/TP Poll For Master
1577	0.020000	0x64	0x7f	BACnet	8	BACnet MS/TP Token
1578	0.000355	0x7f	0x64	BACnet-APDU	32	Complex-ACK readProperty[28] device,52055 protocol-services-supported
1579	0.000350	0x7f	0x00	BACnet	8	BACnet MS/TP Token
1580	0.000850	0x00	0x56	BACnet	8	BACnet MS/TP Poll For Master
1581	0.091820	0x00	0x64	BACnet	8	BACnet MS/TP Token
1582	0.000350	0x64	0x7f	BACnet-APDU	29	Confirmed-REQ readPropertyMultiple[199]
1583	0.000355	0x7f	0x64	BACnet	8	BACnet MS/TP Reply Postponed
1584	0.000350	0x64	0x6d	BACnet	8	BACnet MS/TP Poll For Master
1585	0.020000	0x64	0x7f	BACnet	8	BACnet MS/TP Token
1586	0.000355	0x7f	0x00	BACnet	8	BACnet MS/TP Token
1587	0.007970	0x00	0x57	BACnet	8	BACnet MS/TP Poll For Master

```
▸ Frame 1569: 23 bytes on wire (184 bits), 23 bytes captured (184 bits)
▸ BACnet MS/TP, Src (100), Dst (127), BACnet Data Expecting Reply
▸ Building Automation and Control Network NPDU
▾ Building Automation and Control Network APDU
    0000 .... = APDU Type: Confirmed-REQ (0)
  ▸ .... 0000 = PDU Flags: 0x0
    .000 .... = Max Response Segments accepted: Unspecified (0)
    .... 0101 = Size of Maximum ADPU accepted: Up to 1476 octets (fits in an ISO 8802-3 frame) (5)
    Invoke ID: 28
    Service Choice: readProperty (12)
  ▸ ObjectIdentifier: device, 4194303
  ▸ Property Identifier: protocol-services-supported (97)
```

图 25: 用 Wireshark 打开捕获的 MS/TP 包（115.2kbps，包间隔格式)

5. 包捕捉下载 API:

通过 API 可以方便地自动化下载包捕捉存档，方便事后分析审计。

HTTP 鉴权方式：Digest

读取配置信息：http://192.168.100.1/app/config

读包捕捉概要：http://192.168.100.1/app/capture_summary

读包捕捉：http://192.168.100.1/app/read_capture

Python 示例程序下载 http://www.hvacrcontrol.com/wp-content/uploads/api.py