CAN Bus vs Ethernet

Unsurprisingly the fundamental purpose of the Can to Ethernet bridge is to connect CAN Bus networks to Ethernet based networks and support bi-directional communications.

CAN Bus is a commonly used network protocol used to control vehicles and other systems that need a highly reliable, low latency, near real time control capability.

Ethernet is the most common networking protocol found in general use today and underpins TCP and UDP which is used by PC or internet connected devices.

CAN Bus achieves its high levels of reliability by constantly sending packets of data where the packet contains an ID indicating the device and then a set of values. It has a clever mechanism that allows it to prioritise packets based on their importance using the ID.

For example if you are sending a packet that contains the position of the

accelerator in a car, that information will have an ID for the accelerator and might be send 10 times a second. Should a network glitch occur and a packet be lost, then largely that is not or any importance, as in most cases the next packet will arrive within 1/10 of a second, sufficient to retain control of the vehicle.

Ethernet works somewhat differently and has two distinct modes that it can operate under, being TCP and UDP.

Unlike CAN Bus which is a network protocol designed with vehicle control in mind, Ethernet is a general purpose protocol used for all modern internet communications. It's a lot more complex in its operation, here is some important concepts to understand before you read on.

UDP vs TCP

Ethernet has two distinct modes in which it can be used and the CAN Bus bridge supports both. In both cases the CAN Bus bridge is having a 'conversation' with Profinity or the Tritium tools. But the way that conversation works is completely different. To make this a bit easier initially, lets just think of it in the same way we communicate as people.

User Datagram Protocol (UDP)

UDP is a network broadcast model.

Think of it as being like a conversation where a CAN-Ethernet Bridge (in this case a person) is simply shouting out the CAN Bus packets as they fly past to anyone who wants to listen on the Ethernet side. Perhaps no one is listening, perhaps many people are. UDP is the default behaviour of the CAN Bus bridge, it detects a CAN Bus packet on the CAN Bus network side and shouts the values from the packet on to the Ethernet side using UDP.

In some ways this is a great model.

Just like CAN Bus, we don't need to worry about reliability. If a packet is lost on the network, a short time later it is resent via a new shout. But there are

also issues, UDP is noisy, multiple CAN Bus bridges shouting on the same network can all be shouting at once, which would be like multiple people shouting in a room and this makes it hard to figure out who to listen to.

Finally network routers need to make decisions on how far they want all this noise to travel in a network.

Obviously we don't want all this shouting to go too far otherwise we are just going to flood the network with UDP packets, so networking devices (like WiFi access points) are often very aggressive about how far they will let UDP go in a network and will often drop the packets to prevent a network flood.

Transmission Control Protocol (TCP)

TCP is a point to point communication model.

Its closet analogy in real life is to two people having a conversation. This has got some real benefits and some disadvantages. One of the key benefits is the communication can now be reliable, if one party misses part of the conversation it can ask for it to be repeated and hence not lost.

Also it's a lot less noisy and because of that network routers are happy to allow the conversation to be transmitted long distances. Because of this TCP is the underlying protocol used to power things like the internet, where reliability and ability to transmit long distances is very important.

On the downside, TCP is a one to one style communication model and the CAN-Ethernet Bridge works this way, talking to one TCP connection at a time. Also the reliability TCP provides is very useful at times, but can also be a bit of a challenge with fast moving protocols like CAN Bus which manage reliability via a completely different approach.

In summary there are pros and cons each way and depending on what you are trying to achieve, different protocols make sense. Want multiple people to be listening to a CAN-Ethernet Bridge at once, UDP is your best (in fact only) option. Want reliability or transmission over long distances, then TCP is the way to go.

DHCP vs Static IP

In TCP mode, the setting of your IP address is the single thing most likely to determine the success or failure when setting up the bridge.

All devices connected to a network are assigned an IP address. It's an address unique to that device on the network that allows the router to determine where to send traffic. Separately to their IP Address, all Ethernet connected devices also have a MAC address which is a unique address for that device globally.

We will not deal with MAC addresses here is it is not particularly important for the purposes of the bridge, but if it comes up, that's what it does.

IP Addresses are either dynamically set or statically set.

In the dynamic configuration, when the Network Adapter or the bridge connects to a network it asks a DCHP server to provide it an IP address. The DCHP server which is generally contained inside your network router knows all the devices that are currently on the network and assigns the device an IP address from a valid and currently unused range.

In the static IP approach you manually assign the device and IP address, basically doing the job of the DHCP server.

Two things are very important here.

1. The IP Address needs to be unique on your network
2. The digits assigned to the IP address are important and will determine the behaviour of the network.

You could write a whole book on networking and lots of people have but the key piece of information that you need to know is that for most situations the first three digits of your IP address are critical to its operation.

For example, consider the following network

Device	IP Address	Comments

Device	IP Address	Comments
Router	192.168.16.1	Your Wifi or ethernet router, the DHCP Server is probably running here
PC	192.168.16.60	This is where Profinity or the Tritium tools are running
CAN-Ethernet Bridge	192.168.16.90	This is where the Tritium or Prohelion CAN-Ethernet Bridge is running

This is a well setup network and will probably cause you no problems with either Profinity or the Tritium tools.

The reason simply is that **the first three digits of the IP addresses are the same** or in networking terms the devices are all running **in the same subnet**.

This means that the Router (192.168.16.1) does not need to do anything tricky to send information between these devices.

However, lets consider another network setup.

Device	IP Address	Comments
Router	192.168.16.1	Your Wifi or ethernet router, the DHCP Server is probably running here
PC	192.168.16.60	This is where Profinity or the Tritium tools are running
CAN-Ethernet Bridge	169.254.82.45	This is where the Tritium or Prohelion CAN-Ethernet Bridge is running

Here we can see we have a problem.

The CAN-Ethernet Bridge is running with an IP address where the first three

digits are completely different. For some scenarios this might still actually work, but it's going to cause you issues and ideally the system should never be setup this way.

The fact that the IP address starts with 169.254 also indicates a key issue, that the device was not assigned a static IP address and when it asked a DHCP server for an address, no response was forthcoming.

This is a fairly common scenario that causes problems. This issue often happens when setting up the bridge with a direct connection to a PC and no router in the middle. In this scenario we would always recommend a static IP address be used.

If you want to understand the scenario where this configuration could work see the Supported Network Setups section of this document and read about the configuration **ADVANCED - Direct TCP Connection using a router or WiFi** as there is a scenario where you might actually want this configuration, but it is fairly unusual and requires a very specific setup to work.

If you take two things from this whole article it's should hopefully be the "he subnet (the first three digits) is very critical to the reliable operation f the bridge and ideally don't leave your bridges running in the IP ddress range of 169.254.x.x that means they are not setup right.

Bridge Fundamentals

Supported Network Setups

Prohelion Documentation