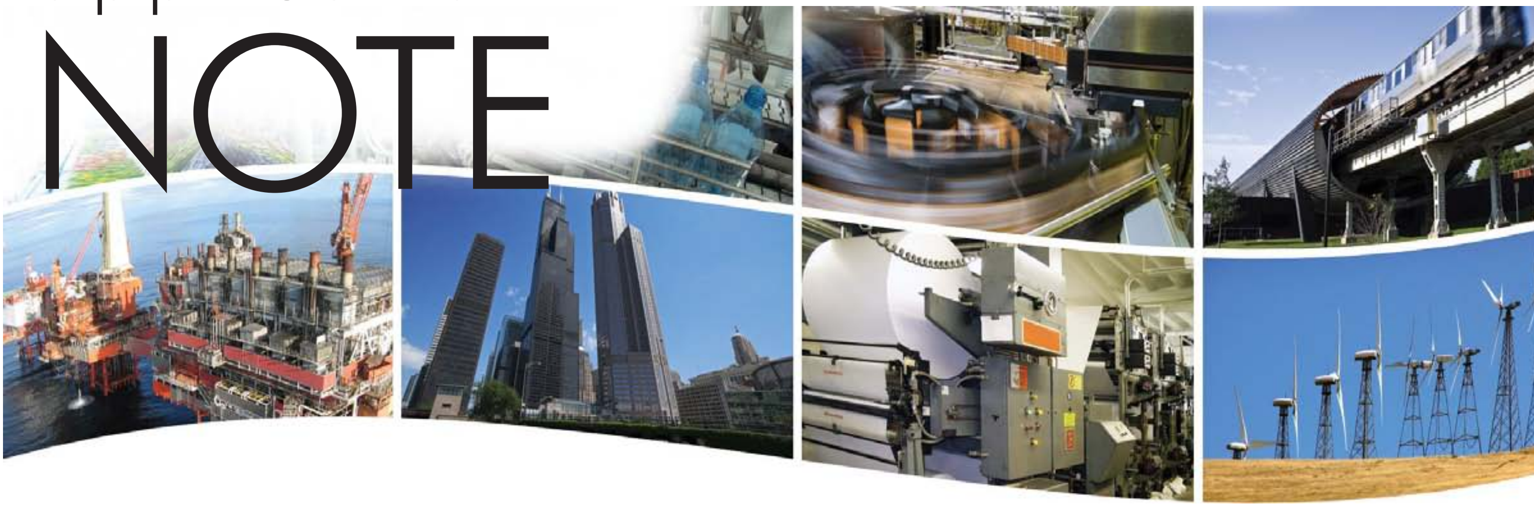
application
NOTE



Using the Skorpion Diagnostic Switch with Wireshark®

One benefit of switched Ethernet technology is that the switch restricts directed messages to only those ports party to the communication. This improves overall network throughput by not burdening end stations with useless traffic. However, this feature makes protocol debugging difficult because a sniffer (protocol analyser) tool attached to an unused port on the switch cannot observe any directed messages on other ports. In the past, the solution was to change out the switching hub with a repeating hub — but with the Skorpion Diagnostic Switch this is unnecessary.

The ***Skorpion Diagnostic Switch*** retains all the virtues of switched Ethernet technology (including Auto-MDIX and auto-negotiation) but with one exception — no address learning. Thus, all messages (directed, multicast, broadcast) are ***flooded*** to all switch ports so that network sniffers such as Wireshark can be used to observe all network traffic that passes through the switch. The switch can be permanently installed or carried from one site to another as needs arise. It can be used for control panel installations if you need the ability to diagnose problems in the field. It can also be used in a development environment when debugging code.

Wireshark and the “fin” logo are registered trademarks of the Wireshark Foundation which can be accessed at www.wireshark.org.

The Wireshark.org website claims that Wireshark is the world’s foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It supports hundreds of protocols including BACnet thanks to the numerous individuals who support the Wireshark open-source application. It can work with both wired and wireless networks. It is extremely handy when troubleshooting tough network problems as long as you can capture the traffic of interest. With switched Ethernet this can be a problem and that is where the Diagnostic Switch comes into play.

Using the Skorpion Diagnostic Switch with Wireshark calls for some special considerations which are discussed in this Application Note.

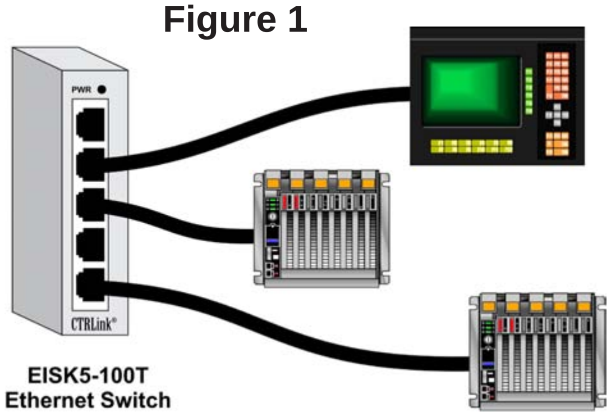
EISK5-100T/H

Scenario #1 — Installing the Diagnostic Switch Temporarily

The Skorpion diagnostic switch can be installed permanently in an installation or replaced with a regular Skorpion switch after commissioning or troubleshooting is complete. Each method has its advantages and disadvantages.

Using the Skorpion diagnostic switch temporarily may be popular -— but it might be impractical in some circumstances. The basic issue is the inescapable need to interrupt the network for the time needed to first ***insert*** and eventually ***remove*** the switch. The situation is illustrated below.

Figure 1



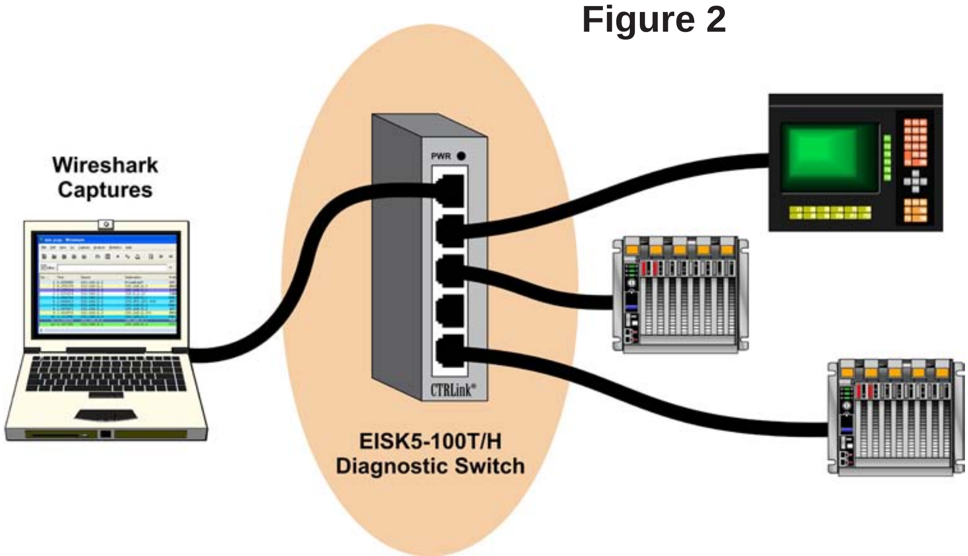
The network in Figure 1 uses a normal Skorpion unmanaged switch in which each directed (non-broadcast) message leaves the switch via just the one port that delivers the message. If you attach a PC to an unused switch port for the purpose of “listening” to traffic, the PC will “miss” all of the directed messages.

In Figure 2, the normal switch has been replaced with the diagnostic switch. Also a laptop has been connected as a platform for running Wireshark. Because the diagnostic switch forwards all messages to all ports (except for the port the message arrived on), Wireshark can capture ***all*** the network traffic.

When troubleshooting is done, the diagnostic switch and the laptop are removed — and the network of Figure 1 is restored.

If the network disruption described above is acceptable, this scenario may be your best choice.

Figure 2



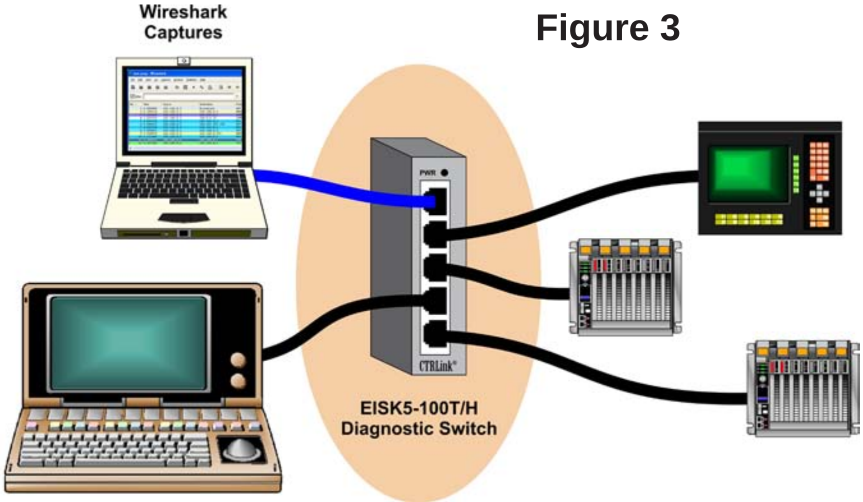
Scenario #2 — Installing the Diagnostic Switch Permanently

The Skorpion diagnostic switch can be installed permanently in an installation, if desired. It is important to note that some benefits of using a switch will be lost — but in master-slave networks, this is unlikely to be a significant issue.

In Figure 3, the network is served continuously by the Skorpion diagnostic switch — with the permanent cables shown in black. When diagnostic work is to be done, the laptop hosting Wireshark is connected temporarily through an unoccupied port on the diagnostic switch. When this temporary work is finished, the diagnostic laptop is removed to be utilized for some other job in another location. The network under scrutiny is never interrupted at any time during this procedure.

Of course the PC hosting Wireshark could be left in place permanently — if desired.

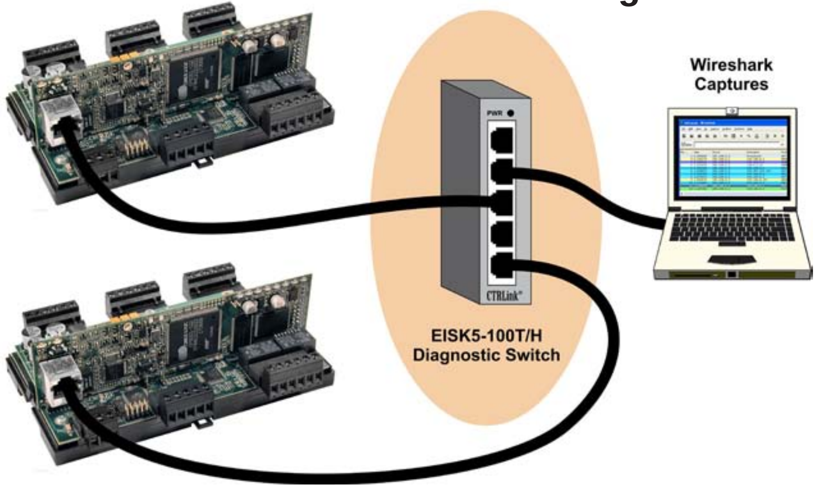
Figure 3



Scenario #3 — The Diagnostic Switch and Embedded Peer-to-Peer Devices

The Skorpion Diagnostic Switch can also be useful when developing embedded Ethernet devices because you can connect the Skorpion Diagnostic Switch between two embedded Ethernet devices and view their messages using Wireshark.

Figure 4



When your system contains a PC-based device, you can load Wireshark onto the PC and watch messages going in and out of the PC. But when the system only contains ***embedded*** Ethernet devices then, to watch the Ethernet messages exchanged between these devices, you will need to introduce a PC. An Ethernet hub could be used in this case, but they are difficult to find and may not support 100 Mbps operation. The diagnostic switch will do the trick.

Figure 4 shows a situation in which two embedded Ethernet devices are engaged in ***peer-to-peer*** communications. Here the diagnostic switch must be installed so that it is connected to ***all cabling***.

Scenario #4 — The Diagnostic Switch in a Cascaded Switch Network

With a cascaded switch network with peer-to-peer traffic there may not be a single place to install the diagnostic switch in order to see all the traffic. However, most industrial networks like that of Figure 5 have either master-slave or client-server networks where the client or the master initiates all the traffic with servers and slaves responding accordingly. In this situation it is only necessary to add a diagnostic switch to intercept the client or master communications. With the arrangement shown in Figure 6, all traffic will be captured. But if peer-to-peer communication exists among the devices it will be necessary to move the diagnostic switch to gain party to the communications.

Figure 5

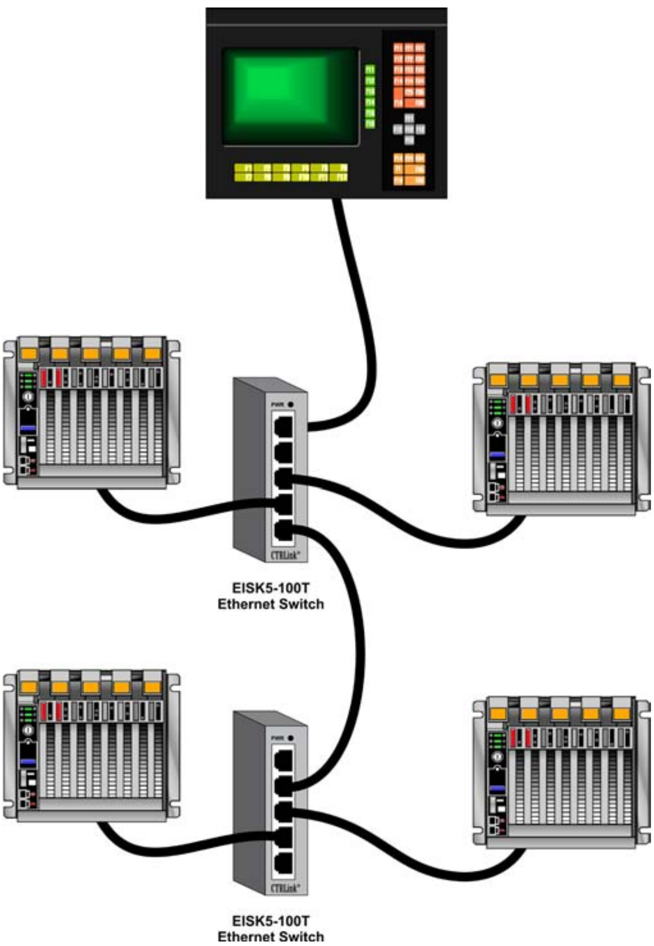
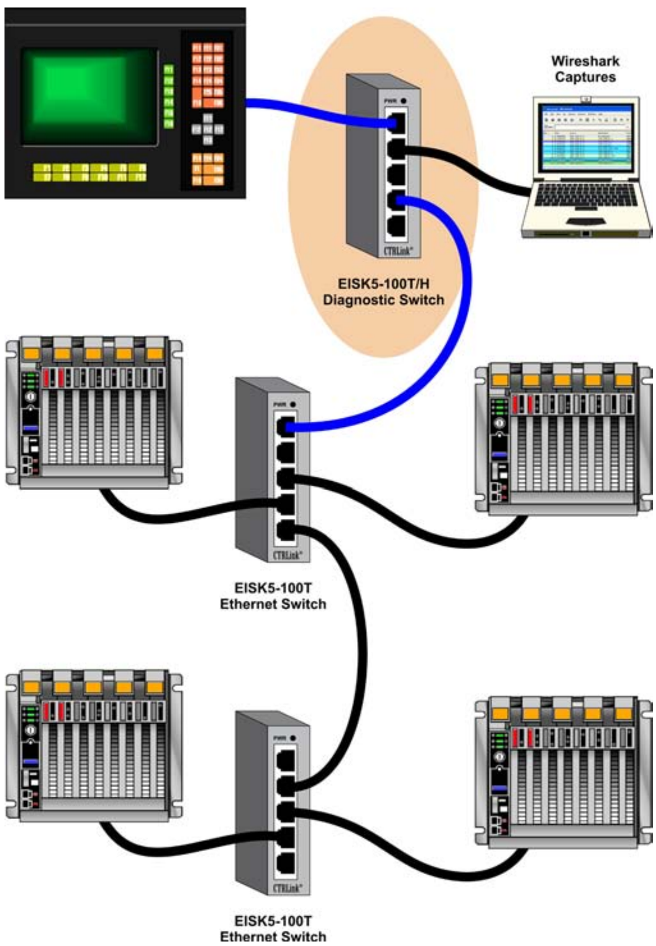
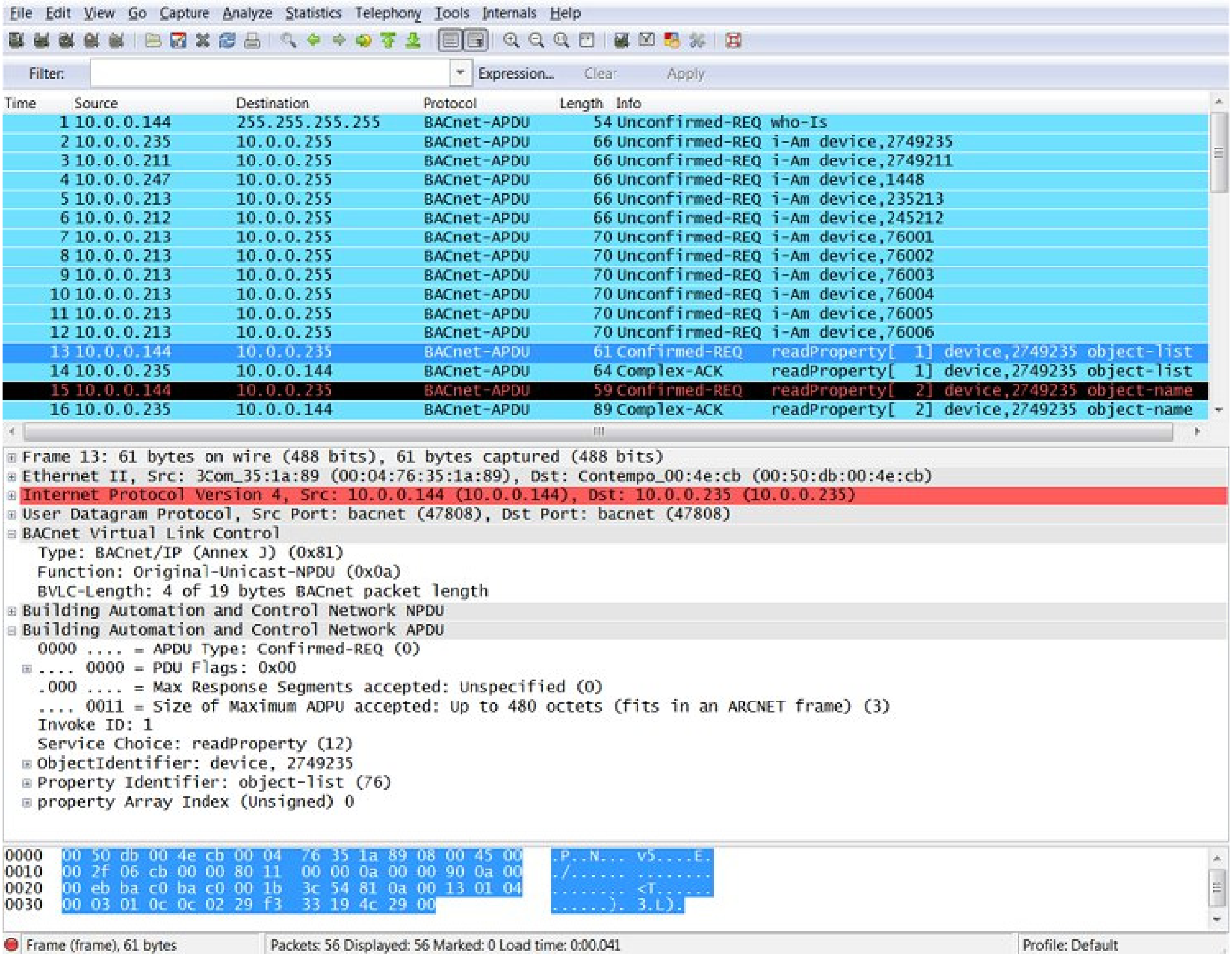


Figure 6



Typical Wireshark Capture



United States
Contemporary Control Systems, Inc.
2431 Curtiss Street
Downers Grove, IL 60515
USA

Tel: +1 630 963 7070
Fax:+1 630 963 0109

info@ccontrols.com
www.ccontrols.com

China
Contemporary Controls (Suzhou) Co. Ltd
11 Huoju Road
Science & Technology Industrial Park
New District, Suzhou
PR China 215009

Tel: +86 512 68095866
Fax: +86 512 68093760

info@ccontrols.com.cn
www.ccontrols.asia

United Kingdom
Contemporary Controls Ltd
14 Bow Court
Fletchworth Gate
Coventry CV5 6SP
United Kingdom

Tel: +44 (0)24 7641 3786
Fax:+44 (0)24 7641 3923

info@ccontrols.co.uk
www.ccontrols.eu

Germany
Contemporary Controls GmbH
Fuggerstraße 1 B
04158 Leipzig
Germany

Tel: +49 341 520359 0
Fax: +49 341 520359 16

info@ccontrols.de
www.ccontrols.eu