

ALLEN-BRADLEY CONTROLLOGIX AND COMPACTLOGIX PLC APP NOTE FOR VIPER SYSTEM

PN 009-5008-325
Revision 0
Released November 2011



TECHNICAL SERVICE SUPPORT BULLETIN

CONTENTS

1.	Overview	3
2.	Allen-Bradley CompactLogix/ControlLogix PLCs	3
2.1.	PLC ladder logic on restart opens all connections at once instead of sequentially	3
2.2.	AB CompactLogix/ControlLogix series PLCs EtherNet/IP connection timeout	4
2.3.	AB CompactLogix/ControlLogix series PLCs sends to many “CIP Forward Open” and “CIP Forward Close”	6
2.4.	AB CompactLogix/ControlLogix series PLCs sends many TCP/IP keepalive messages	9
3.	Viper	10
3.1.	Setup Viper in router mode (instead of Bridge mode)	10
3.2.	Filtering TCP keepalive with Viper TCP proxy mode	10
3.3.	Replacing or resetting a Viper using proxy mode without restarting polling	10

1. OVERVIEW

A guide to assist with Allen-Bradley CompactLogix/ControlLogix communication setup between master PLC and remote PLC using AB EtherNet/IP TCP protocol between PLCs.

PLC communication via serial lines or serial terminal server is not covered here, never the less some of the information could apply.

NOTE: Please consult the CalAmp's "Viper General PLC setup" support bulletin for important information on setting-up systems with PLCs.

2. ALLEN-BRADLEY COMPACTLOGIX/CONTROLLOGIX PLCS

Below is a list of important settings to improve communication when used with a limited bandwidth Viper network. More information on communication can be found in the CalAmp's "[Viper General PLC setup](#)" support bulletin on CalAmp's support Web page.

NOTE: When required, contact your PLC provider or Allen Bradley / Rockwell Automation support.

2.1. PLC LADDER LOGIC ON RESTART OPENS ALL CONNECTIONS AT ONCE INSTEAD OF SEQUENTIALLY

When PLC ladder program is setup to have at startup all write message **rungs set to true**, all TCP connections are triggered "simultaneously". This creates an overload of TCP SYNs and somewhat could congest the on-air traffic depending on the system.

It is recommended to setup the ladder write message rungs not to start up simultaneously. Write messages should be setup to open the TCP connection sequentially. For more information contact your PLC provider or Allen Bradley / Rockwell Automation support.

2.2. AB COMPACTLOGIX/CONTROLLOGIX SERIES PLCS ETHERNET/IP CONNECTION TIMEOUT (SETTING TIMEOUT TO SHORT CAN CAUSE PROBLEMS!)

When using the Ethernet/IP with Allen-Bradley CompactLogix/ControlLogix (Logix series), the **TCP Connection timeout** is set on a per message instruction basis using “Message Configuration” rather than “Channel configuration - Channel 1” of the MicroLogix series.

When messages are defined using “Message Configuration” and using path ex: “LocalENB, 2, 192.168.1.9:1,0”.

Brief description:

- TCP connection is opened when the first message is sent.
- The TCP connection timeout is set by default to 120 sec since the inactivity default setting is 120 sec.
- While connection is established with same remote IP and same port, ex: 192.168.1.9 , other messages will use the same TCP connection, and therefore resetting the timeout count for each message sent.
- When all messages are using the same default inactivity time (120 sec) the TCP connections stays open as long the next message is sent within the inactivity timeout period.
- The TCP connection is closed after the last message plus the inactivity period (default 120 sec).
- The TCP connection can also be terminated based on network connection problems.

Example using default inactivity timeout (120 sec).



Overwriting the default inactivity timeout for the TCP connection in “Message Configuration”:

(Not recommended unless required)

It is possible to overwrite the “Message Configuration” default inactivity timeout value by using path ex: “LocalENB, 2, 192.168.1.9:inactivity-100,1,0”. Using “inactivity-100” would set the inactivity timeout to 100 seconds instead of the default 120 seconds. (Note: Setting of “inactivity-x”: where x can be between 1 and 120 seconds, using x > 120 seconds will disable the message completely).

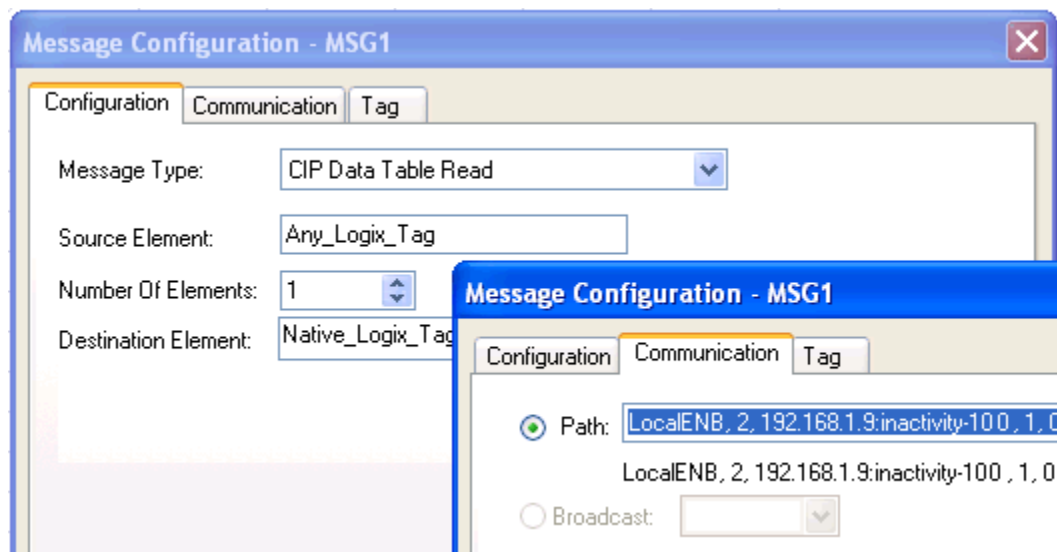
Overwriting the default inactivity timeout is normally not required and can cause additional side effects. One of these side effects would be when the inactivity timeout is less than the longest delay between two messages; additional IP messages

are sent for each close and re-open of the TCP connection. This adds a lot of on-air traffic and impacts the system performance.

Note when using different inactivity timeout values for messages with the same TCP connection:

When different messages for the same remote share the same TCP connection, each different message's inactivity timeout would restart the timeout timer. Message example: msg1 inactivity-60, msg2 inactivity-100, msg3 inactivity-30. These messages are then sent as follows: msg1 is sent, msg2 is sent, msg3 and then a wait is done. Since the last message was msg3 with inactivity timeout of 30 seconds, the TCP connection would close after 30 seconds of msg3.

Setting example using custom inactivity timeout (100 sec).



Summary on TCP connection timeout (inactivity setting)

Since the longest inactivity timeout per TCP connection with a remote unit (PLC/RTU) is 120 seconds (based on message inactivity max of 120 seconds), it is important that each remote (PLC/RTU) is polled with the 120 second period to avoid extra traffic resulting from additional TCP/IP open and close connection messages. For systems where polling is done infrequently (> 120 sec) the additional TCP traffic needs to be considered for the system traffic plan.

For normal operation the inactivity timeout does not need to be specified in the "Path" setting. Master and remotes should be set this way, especially if remote PLCs send unsolicited messages or initiate communication with other remotes. If a system has a mix of PLCs (CompactLogix/ControlLogix with MicroLogix/SLC), then also refer to CalAmp's "Allen-Bradley PLC for Viper System" support bulletin available on CalAmp's WEB site under support.

2.3. AB COMPACTLOGIX/CONTROLLOGIX SERIES PLCS SENDS TO MANY “CIP FORWARD OPEN” AND “CIP FORWARD CLOSE”

When using the EtherNet/IP with CIP communication protocol with Allen-Bradley CompactLogix/ControlLogix PLCs (and with other Logix series PLCs), the option to use “Connected” or “Unconnected” is available in the “Message Configuration”. By default the “Connected” checkbox is selected and therefore it will add additional messages (CIP forward open and CIP forward close messages) for each read / write operation when next message is sent outside the message timeout period (default = 30sec).

To lower the on-air traffic the **“Connected” checkbox should be unchecked (Unconnected)**.

Connected or Unconnected operation description for CIP:

When the **“Connected” checkbox is checked (Connected)**, if there's not a CIP connection already established, then the controller sends an open forward CIP connection command and waits for the good response prior to transmitting the read or write command. The CIP connection remains open as long as there is activity prior to the timeout (default = 30 sec). Any message instruction sending commands to the same device can use the same CIP and TCP connection. If this timeout is reached, a close CIP connection command is sent.

When the **“Connected” checkbox is unchecked (Unconnected)**, the controller uses the Unconnected CIP service to transmit the read or write command, so there is less overhead.

The **Connection timeout** is on a per message instruction basis as shown below - this is with regards to the CIP Connection only not the TCP connection, which is only controlled by the Inactivity Timeout:

Mnemonic	Data Type	Description
.UnconnectedTimeout	DINT	Time out for an unconnected message or for making a connection. The default value is 30 seconds.
		If the message is Then
		Unconnected The ER bit turns on if the controller doesn't get a response within the UnconnectedTimeout time.
		Connected The ER bit turns on if the controller doesn't get a response for making the connection within the UnconnectedTimeout time.
.ConnectionRate	DINT	Time out for a connected message once it has a connection. This time out is for the response from the other device about the sending of the data.
.TimeoutMultiplier	SINT	<ul style="list-style-type: none">• This time out applies only after the connection is made.• The time out = ConnectionRate x TimeoutMultiplier.• The default ConnectionRate is 7.5 seconds.• The default TimeoutMultiplier is 0 (which is a multiplication factor of 4).• The default time out for connected messages is 30 seconds (7.5 seconds x 4 = 30 seconds).• To change the time out, change the ConnectionRate and leave the TimeoutMultiplier at the default value.

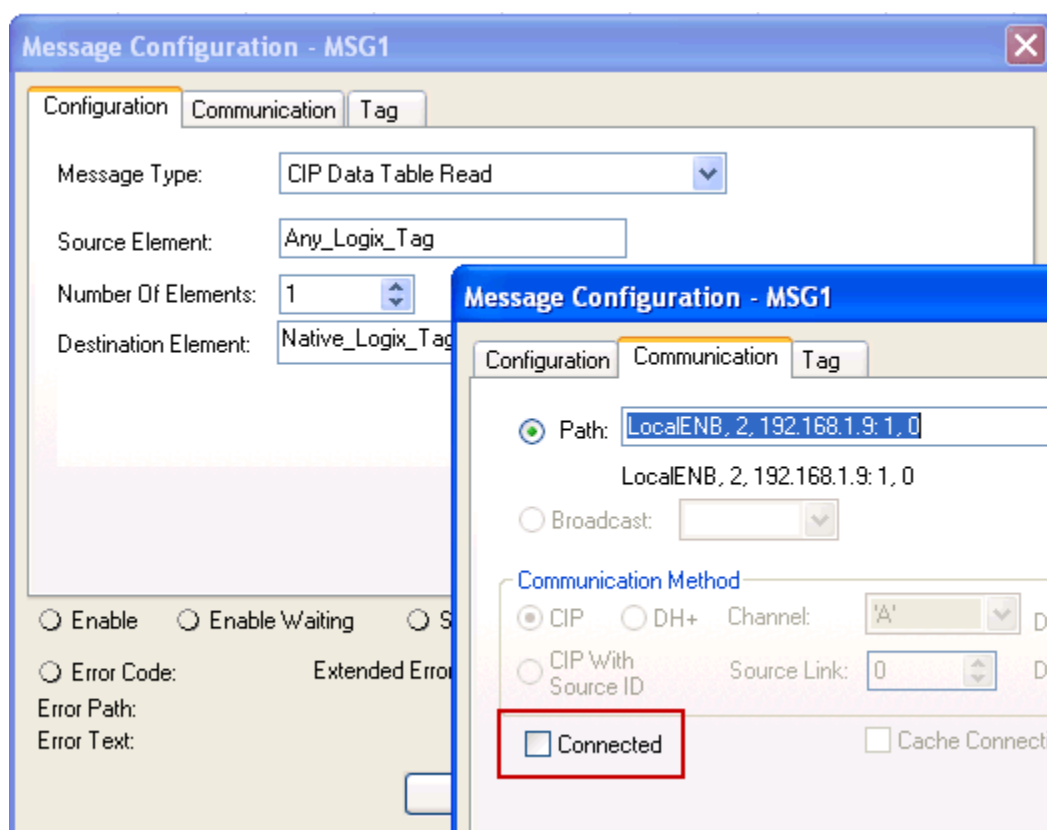
For the Logix controllers, the **UnconnectedTimeout** has to be individually adjusted in each message instruction tag. The default is 30,000,000 microseconds (30 seconds):

MSG1.UnconnectedTimeout	30000000
MSG1.ConnectionRate	7500000
MSG1.TimeoutMultiplier	0

When using "Message type" EtherNet/IP CIP protocol.

To lower the on-air traffic un-check "Connected" in the "Message Configuration" method.

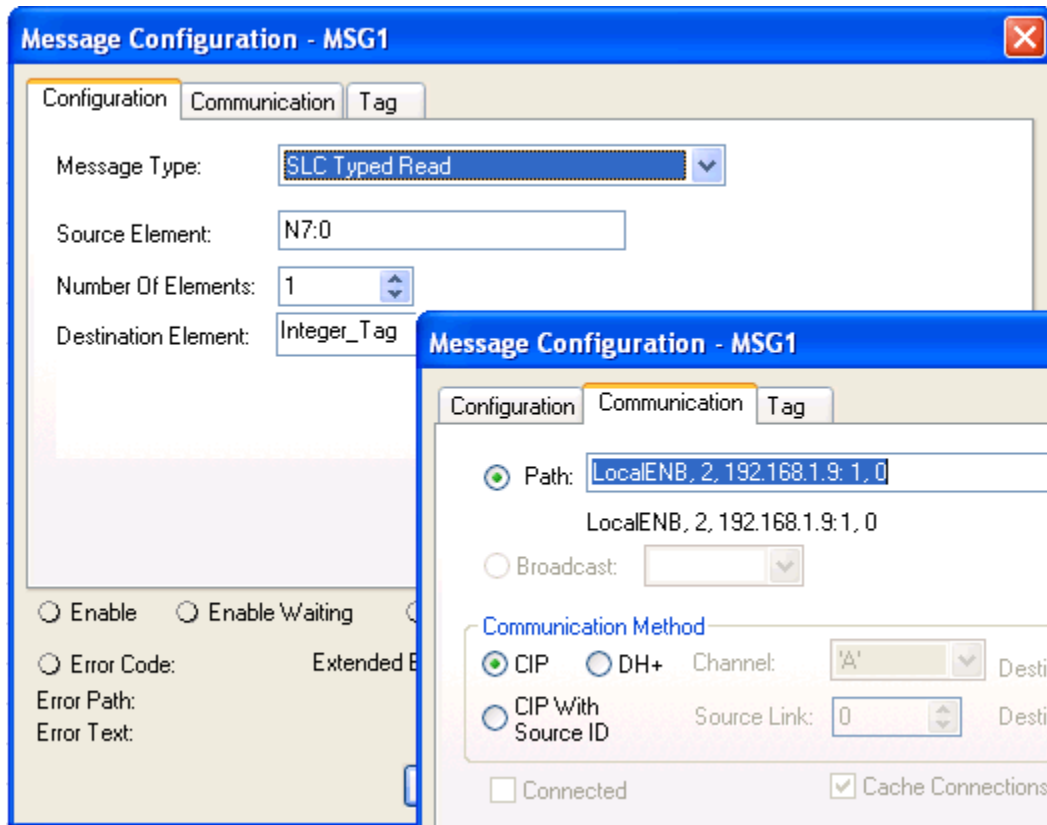
Below is an example when the Message Type is "CIP Data Table Read" or "CIP Data Table Write". Note that the "Connected" checkbox should be unchecked, this is because if you leave it checked, then every time the MSG instruction is executed a CIP connection (with CIP open message) will be established and broken (with CIP close message) which adds unnecessarily to the network traffic.



When communication between ControlLogix/CompactLogix and other Logix series PLCs.

These PLCs/Controller usually use EtherNet/IP CIP unconnected protocol to communicate between each other.

Note (see below) that when the Message Type is "SLC Typed Read" or "SLC Typed Write", the Logix MSG instruction always uses an Unconnected CIP (notice that the "Connected" checkbox is unchecked and grayed out). For example this is used when using PCCC encapsulated in EtherNet/IP command. Others than read or write for SLC types are not described in this document.



Summary of Connected or Unconnected operation

With “Connected” option selected and polling interval between Messages for the same remote CIP connection is longer than the “UnconnectedTimeout” (default 30 seconds), “CIP Forward Open” and “CIP Forward Close” messages add 4 extra on-air messages (includes msg reply) for each unit polled. **If each poll is 2 messages (msg and reply) the 4 extra messages increase the message load (on-air) by 200%.**

Therefore **“Connected” checkbox should be unchecked (Unconnected)** to avoid sending “CIP Forward Open” and “CIP Forward Close” messages. If “Connected” is required then increase the “UnconnectedTimeout” and “ConnectionRate” timeout to a value greater than the polling interval per remote (use precaution with this).

Timeouts used for message responses over EtherNet/IP “Connected” or “Unconnected” should not be too short, therefore should not be set lower than 15 sec (normally) in the event it is required being lower than 30 sec for application level retransmission. The TCP/IP communication driver does its own retransmissions and will not require application retransmissions of messages since a TCP connection will not lose a message unless the connection terminates normally or due to a problem. Therefore with TCP longer timeouts within reason are ok. Longer timeouts (ex 30 sec) are ok since they

minimize duplicated message being buffered by TCP in the event of network congestion or communication problems with remote unit.

With future releases of PLC software/firmware the described operation could change. It is always recommended to be informed on PLC release changes from your PLC provider or Allen Bradley / Rockwell Automation support.

2.4. AB COMPACTLOGIX/CONTROLLOGIX SERIES PLCS SENDS MANY TCP/IP KEEPALIVE MESSAGES

The CompactLogix/ControlLogix series PLCs sends TCP/IP keepalive messages every 8 seconds in both directions for each TCP connection. When several PLCs do the same it is possible that a good part of the on-air bandwidth is used up by the keepalive traffic.

We recommend that the Viper is configured in router mode and that TCP proxy is enabled. The Viper TCP proxy feature will filter out the TCP/IP keepalive messages.

The PLCs TCP keepalive cannot be disabled nor adjusted. Recommended to Allen-Bradley / Rockwell Automation to have an option in the PLC settings to disable keepalive and having user settable keepalive intervals. This could potentially become available in future releases of PLC firmware.

3. VIPER

3.1. SETUP VIPER IN ROUTER MODE (INSTEAD OF BRIDGE MODE)

Info: Viper Bridge mode cannot filter keepalive and cannot operate in TCP proxy mode.

If the system has very few units and few messages Viper Bridge mode could be used. But for larger systems and PLC doing many keepalives, or on-air network being contentious, it may be required to use router mode. Router mode allows retransmission of messages lost due to on-air contention. Bridge mode only does broadcasts without retries. In Bridge mode the application needs to retry lost messages.

3.2. FILTERING TCP KEEPALIVE WITH VIPER TCP PROXY MODE

When using TCP protocol and having PLCs where the TCP keepalive rate cannot be controlled, it is important to enable Viper TCP (OIP proxy) mode. This requires that all Vipers are configured in router mode (Viper Bridge mode cannot filter keepalive and cannot operate in TCP proxy mode).

Note: For PLCs where the keepalive can be controlled and are required, set keepalive to 4 minutes.

One of the Viper's TCP proxy mode usages allows filtering of keepalive messages and prevents them to be sent over the air. Without this filtering, several PLCs sending keepalive messages could easily load the on-air network.

See Viper user manual and Web pages to enable proxy. By default Viper proxy mode is enabled. See Viper Web page Advanced setup -> OIP optimizations. Also under Network management -> Neighbor Tables (neighbor management) make sure that neighbors are configured with the proxy attribute.

3.3. REPLACING OR RESETTING A VIPER USING PROXY MODE WITHOUT RESTARTING POLLING

When replacing or resetting: a remote Viper, a Viper used as a repeater, or even a master Viper connected through a switch, the Viper proxy context is lost and will operate without the proxy benefit.

To reestablish TCP proxy context for the TCP connection, the PLC needs to close the old TCP connection and re-open a new TCP connection. Therefore normally after doing Viper maintenance the master PLC needs to be restarted. Future Viper firmware may reestablish proxy automatically.