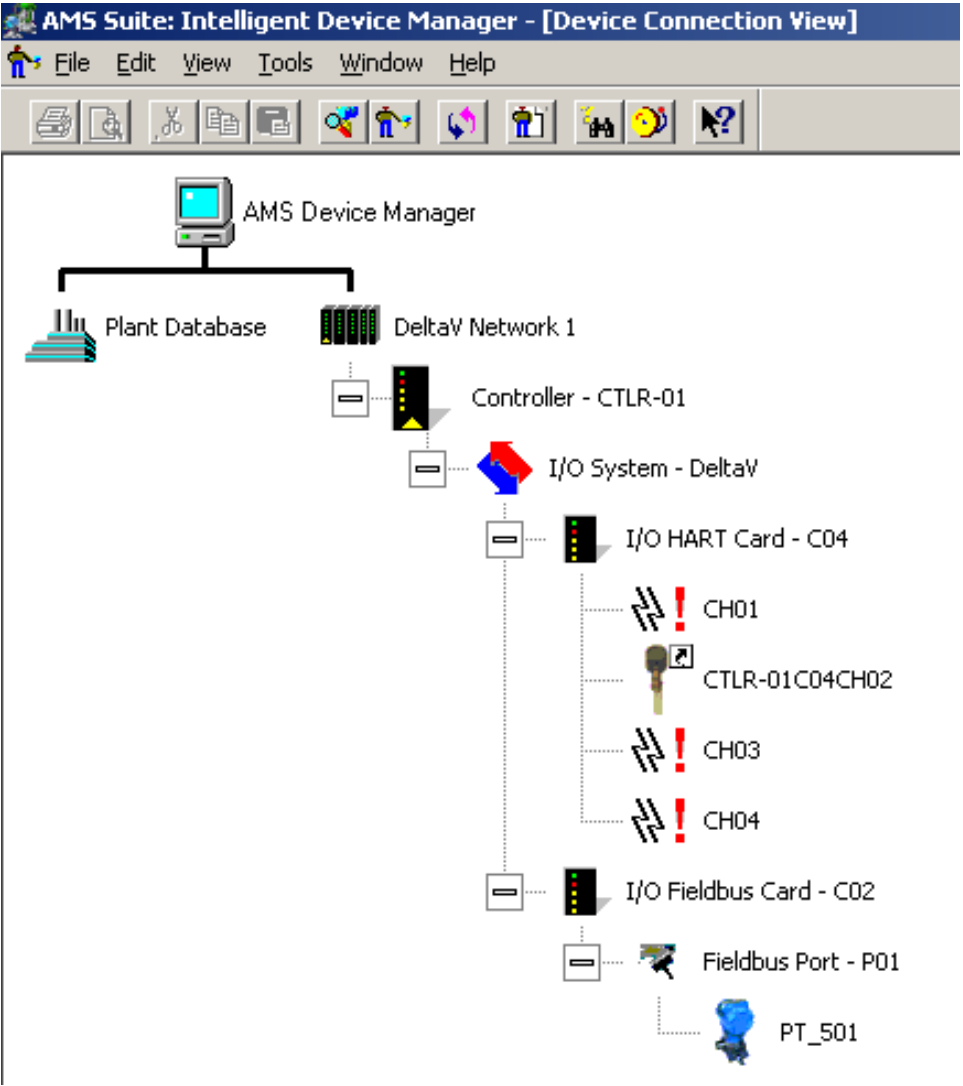

AMS Suite: Intelligent Device Manager - [Device Connection View]
File Edit View Tools Window Help
AMS Device Manager
Plant Database
DeltaV Network 1
Controller - CTLR-01
I/O System - DeltaV
I/O HART Card - C04
CH01
CTLR-01C04CH02
CH03
CH04
I/O Fieldbus Card - C02
Fieldbus Port - P01
PT_501

-1022

Six hundred and three

$$\underset{10^2}{6}\ \underset{10^1}{0}\ \underset{10^0}{3} = (6 \times 10^2) + (3 \times 10^0)$$ *Decimal representation*

$$\underset{2^9}{1}\ \underset{2^8}{0}\ \underset{2^7}{0}\ \underset{2^6}{1}\ \underset{2^5}{0}\ \underset{2^4}{1}\ \underset{2^3}{1}\ \underset{2^2}{0}\ \underset{2^1}{1}\ \underset{2^0}{1} = 2^9 + 2^6 + 2^4 + 2^3 + 2^1 + 2^0$$ *Binary representation*

$10^3 - 1$

$2^{10} - 1$

Negative three hundred and ninety six

(Two's complement binary notation)

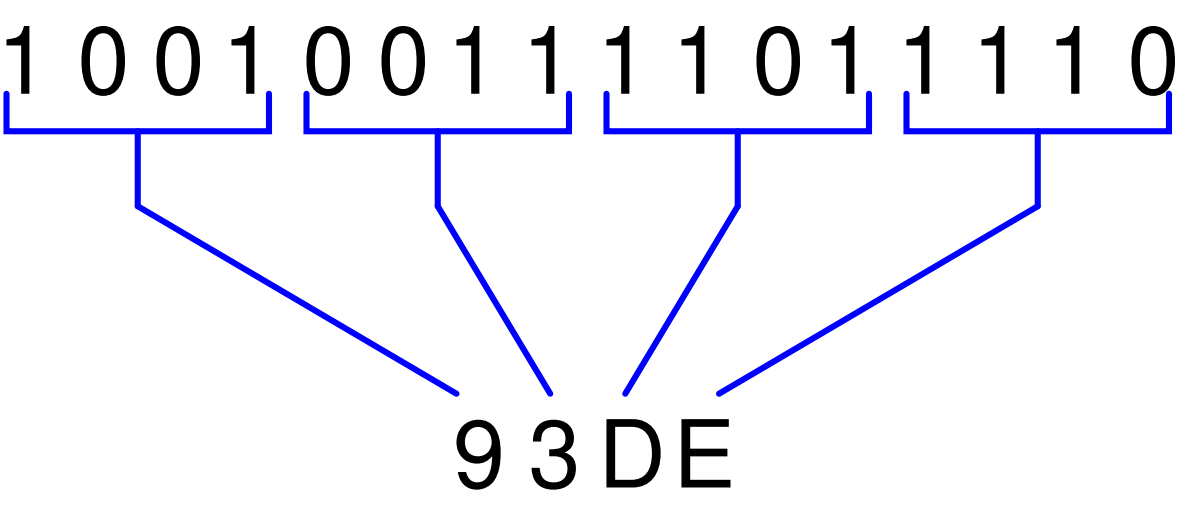
$$\underset{-2^9}{1}\ \underset{2^8}{0}\ \underset{2^7}{0}\ \underset{2^6}{1}\ \underset{2^5}{1}\ \underset{2^4}{1}\ \underset{2^3}{0}\ \underset{2^2}{1}\ \underset{2^1}{0}\ \underset{2^0}{0} = -2^9 + 2^6 + 2^5 + 2^4 + 2^2$$

$2^9 - 1$

-2^9

-512

-32768


1 0 0 1 0 0 1 1 1 1 0 1 1 1 1 0
9 3 D E

Fixed-point binary notation

$$\underset{2^6}{1}\ \underset{2^5}{0}\ \underset{2^4}{0}\ \underset{2^3}{0}\ \underset{2^2}{1}\ \underset{2^1}{1}\ \underset{2^0}{0}\ \bullet\ \underset{2^{-1}}{0}\ \underset{2^{-2}}{1}\ \underset{2^{-3}}{1} = 2^6 + 2^2 + 2^1 + 2^{-2} + 2^{-3}$$

= 70.375 *(decimal notation)*

O

$$1002349 = 1.002349 \times 10^6$$

$$678.331 = 6.78331 \times 10^2$$

$$0.00004532 = 4.523 \times 10^{-5}$$

m

$\pm 1.m \times 2^E$

$\pm 1.m \times 2^E$

$m = 0$

$E = 0$

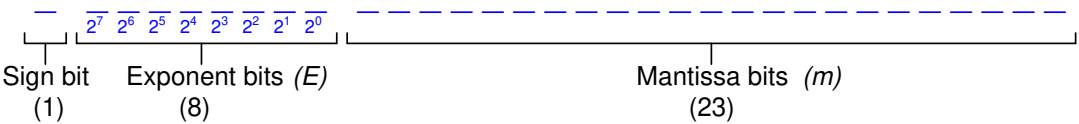
$\pm 0.m \times 2^E$

2^0

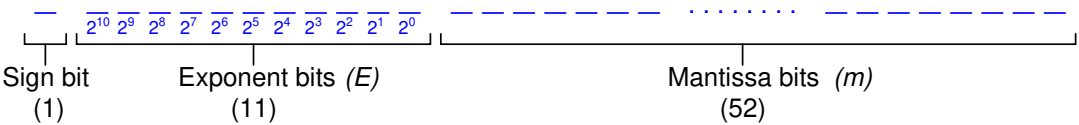
2^{-bias}

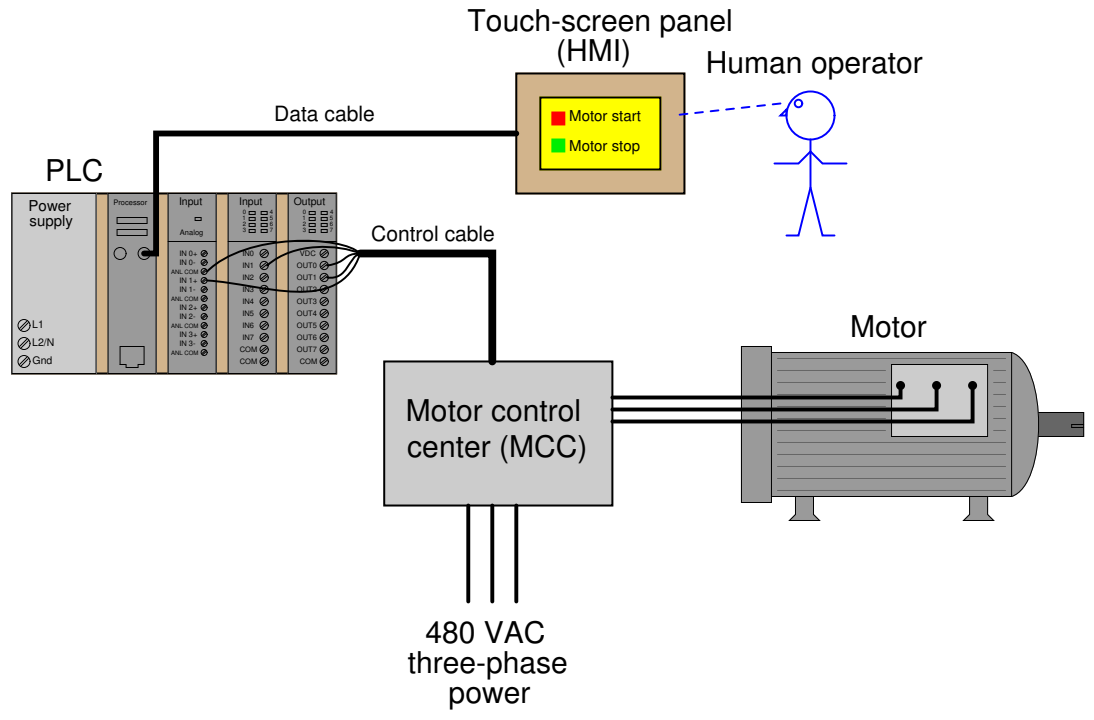
-127

Single-precision IEEE floating-point number format



Double-precision IEEE floating-point number format




Touch-screen panel
(HMI)
Human operator
Motor start
Motor stop
Data cable
PLC
Power
supply
Processor
Input
Analog
Input
Output
L1
L2/N
Gnd
Control cable
Motor
Motor control
center (MCC)
480 VAC
three-phase
power

Tag Name Database

Device Name: PLC_01

Fill Down

☑ Display System Tags
☐ Highlight

☑ Display Internal Tags
☐ Highlight

☐ Highlight Unused Tags

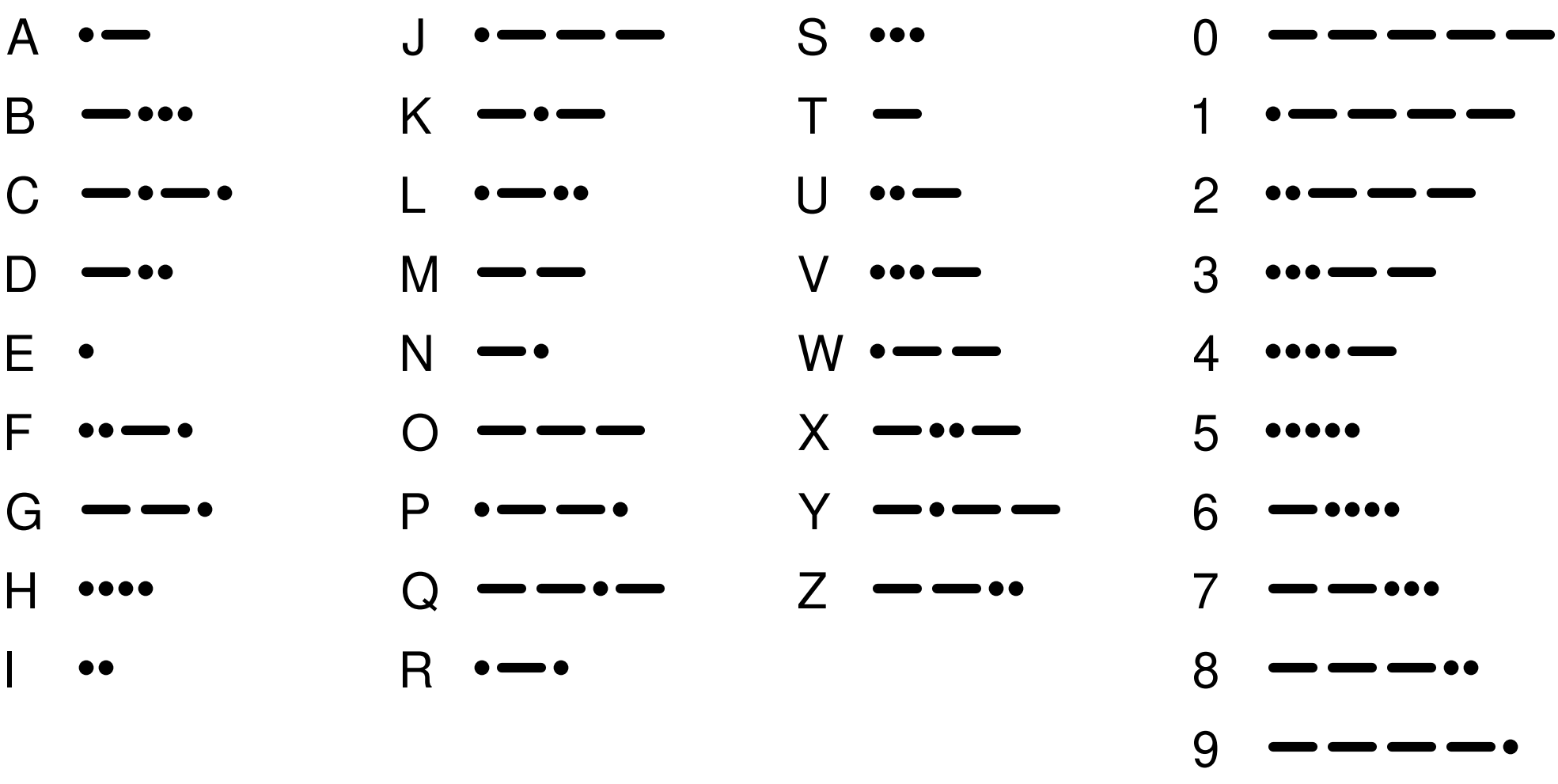
No.	Tag Name	Data Type	PLC Address	Device Name	Attribute
1	START_PUSHBUTTON	Discrete	10024	PLC_01	R
2	STOP_PUSHBUTTON	Discrete	10031	PLC_01	R
3	MOTOR_RUN	Discrete	00005	PLC_01	R/W
4	MOTOR_RUN_TIMER	Unsigned int 32	40010	PLC_01	R/W
5	START_COUNTER	Unsigned int 16	40242	PLC_01	R/W
6	MOTOR_TEMPERATURE	Floating PT 32	30008	PLC_01	R
7	ERROR_MESSAGE	Ascii String	40560	PLC_01	R/W
8	MOTOR_SPEED	Floating PT 32	30017	PLC_01	R

$2^{32} - 1$

$2^{16} - 1$

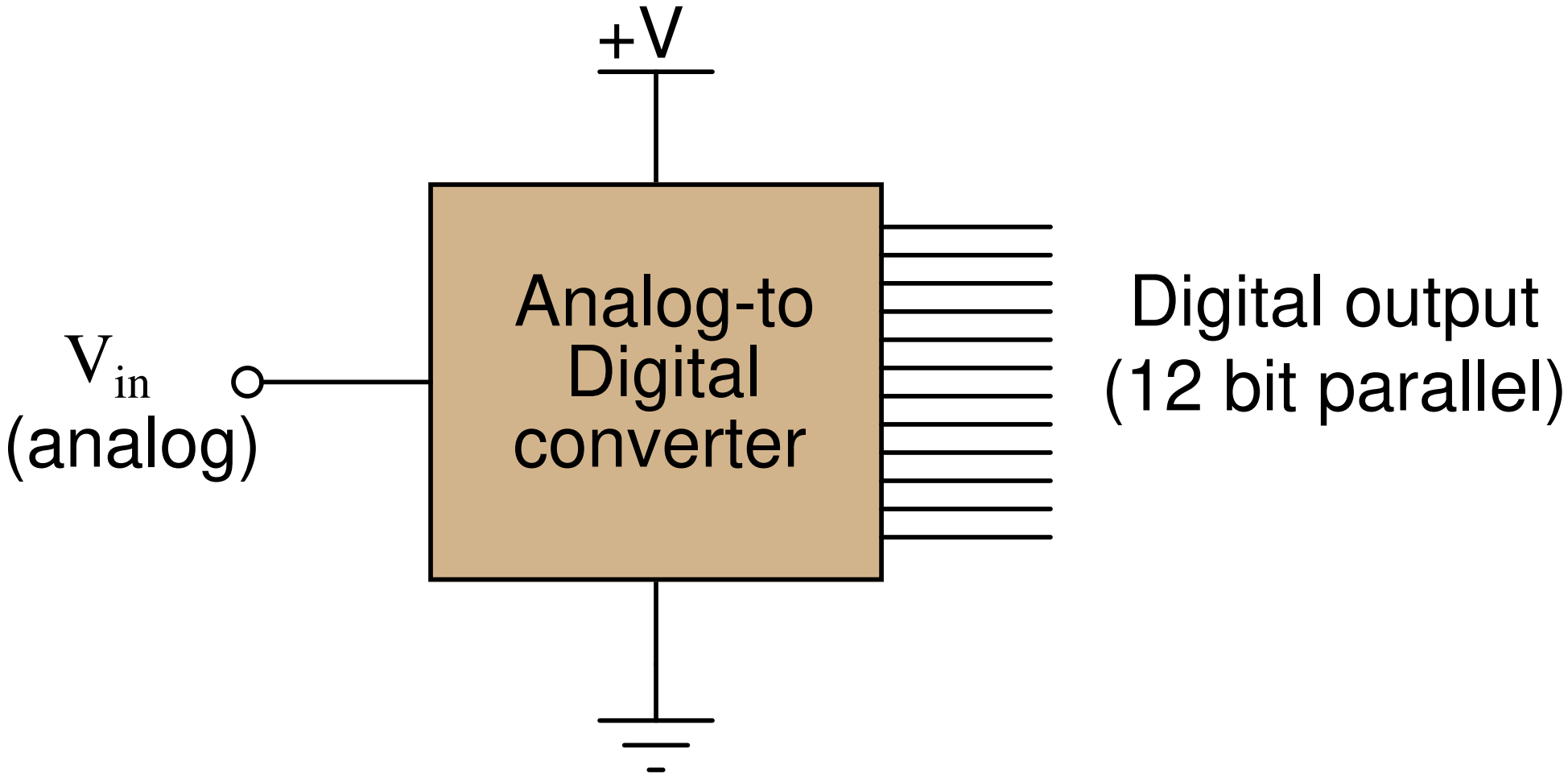
-327.68

International Morse Code (English letters and Arabic numerals only)



2^8

↓ LSB / MSB →	000	001	010	011	100	101	110	111
0000	NUL	DLE	SP	0	@	P	‘	p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	”	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EOT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	’	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	\	l	|
1101	CR	GS	−	=	M	]	m	}
1110	SO	RS	.	>	N	ˆ	n	˜
1111	SI	US	/	?	O	_	o	DEL


+V
Analog-to
Digital
converter
V_{in}
(analog)
Digital output
(12 bit parallel)

2^{12}

$2^{12} - 1$

$$\text{Analog resolution} = \frac{\text{Analog span}}{2^n - 1}$$

n

$$\frac{V_{in}}{V_{fullscale}} = \frac{\text{Counts}}{2^n - 1}$$

V_{in}	Counts (decimal)	Counts (hex)
0 V	0	000
2.46 mV	1	001
3.85 V	1576	628
4.59 V	1879	757
6.11 V	2502	9C6
9.998 V	4094	FFE
10 V	4095	FFF

-3.3

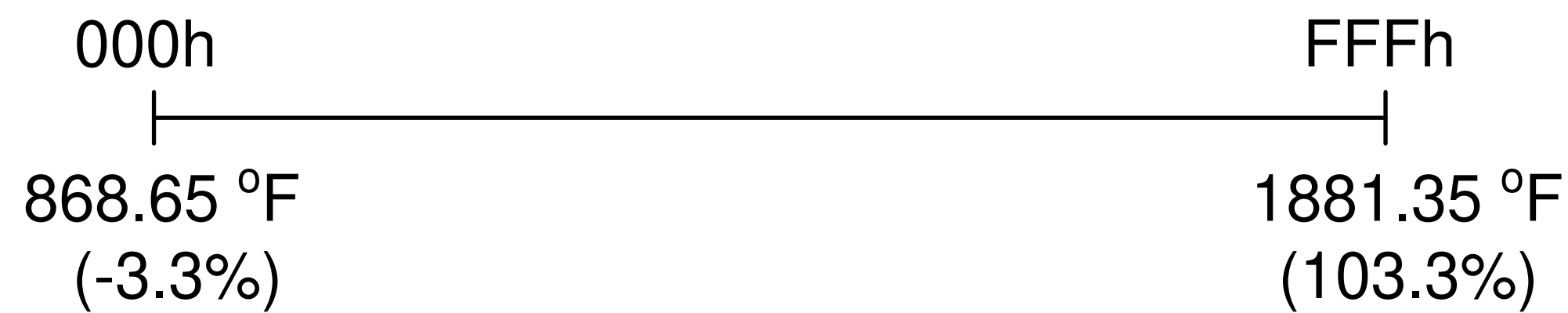

000h
FFFh
-3.3%
103.3%

-100

$$\frac{300-(-100)}{450-(-100)}=0.7273 \text{ per unit}$$

$$(0.7273)(16) + 4 = 15.636 \text{ mA}$$

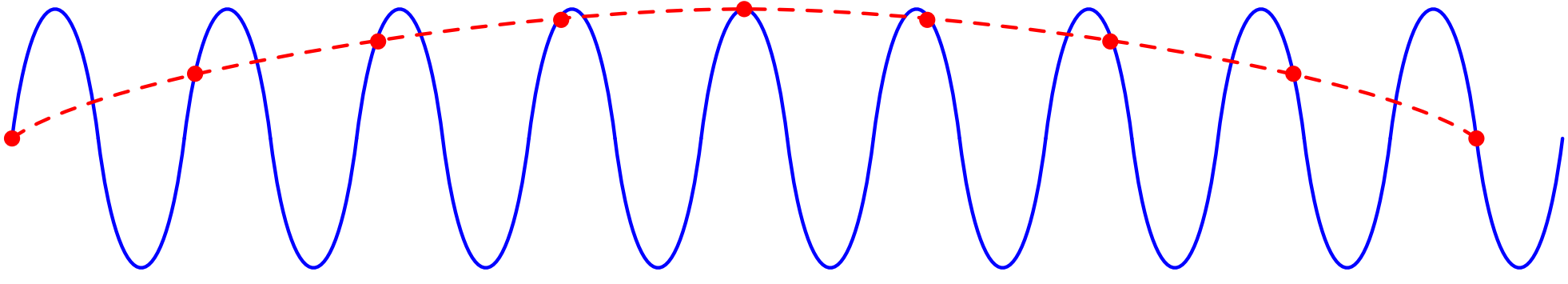
$$\frac{26.7-(-3.3)}{103.3-(-3.3)}=\frac{30}{106.6}=0.2814 \text{ per unit}$$


000h
FFFh
868.65 °F
(-3.3%)
1881.35 °F
(103.3%)

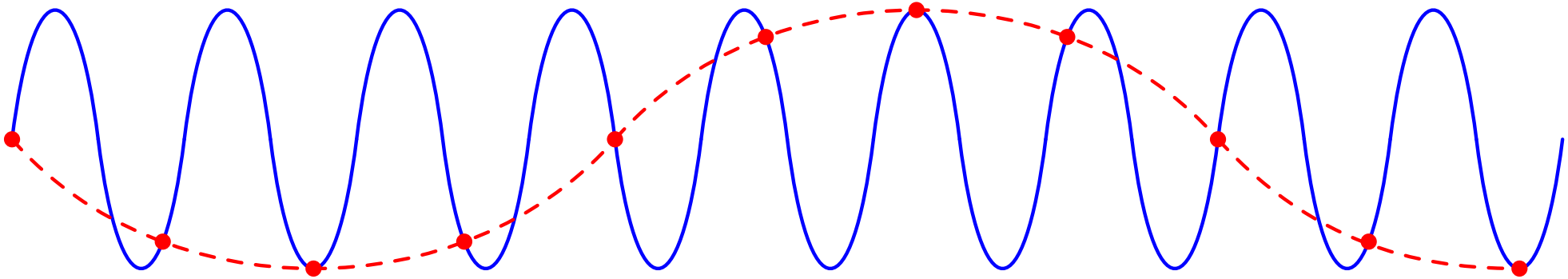
$$\frac{2649}{4095} = 0.6469 \text{ per unit}$$

$$(0.6469)(1881.35 - 868.65) + 868.65 = 1523.75 \text{ degrees F}$$

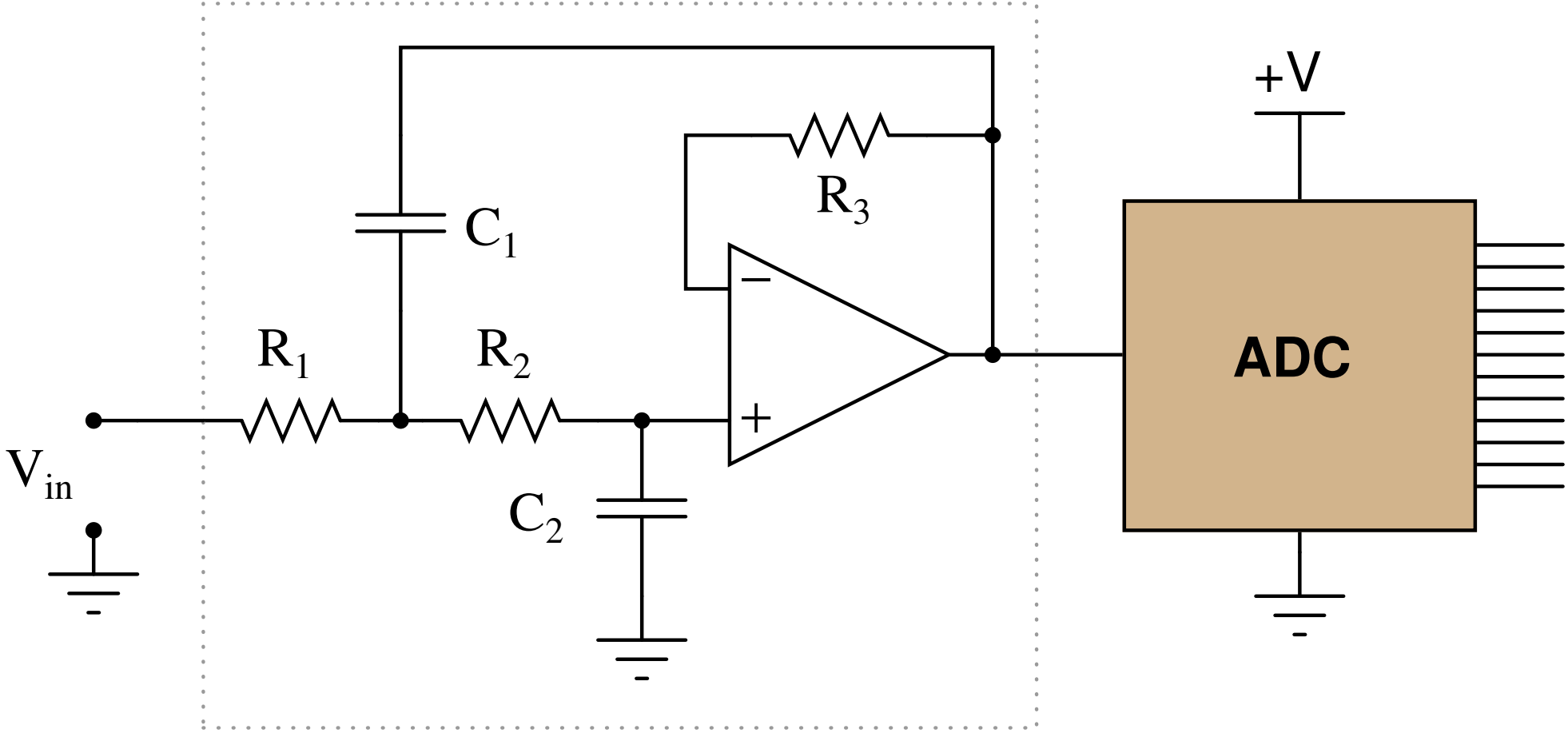
Sample interval slightly longer than one wave cycle

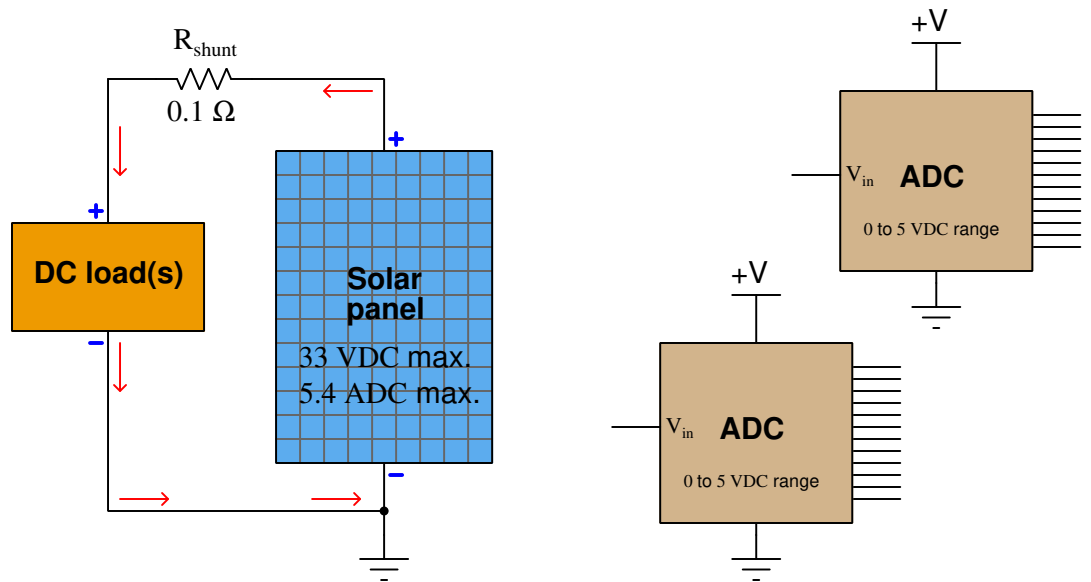


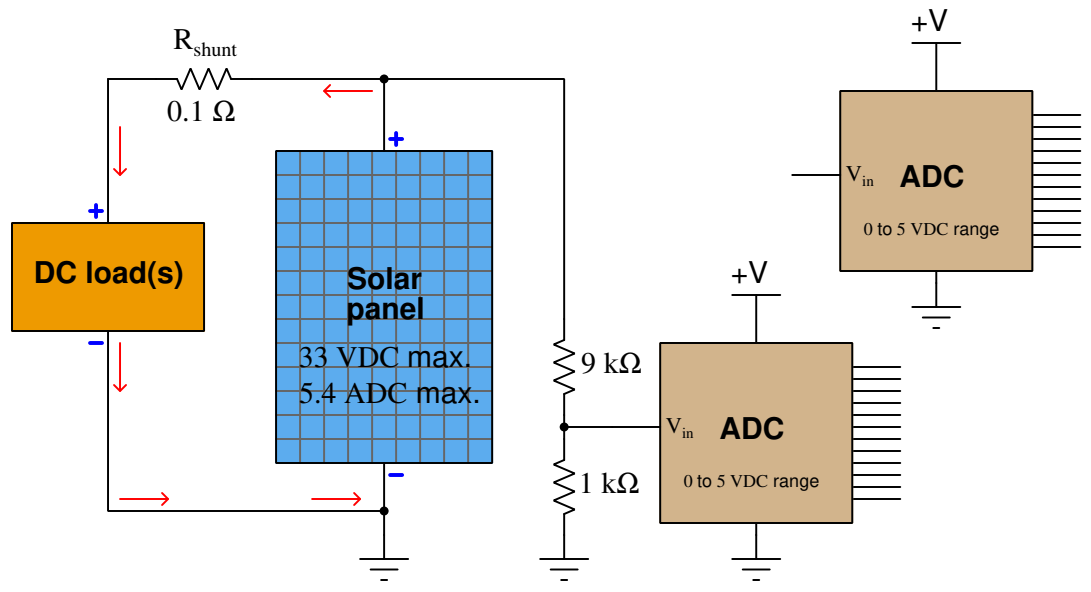
Sample interval slightly shorter than one wave cycle

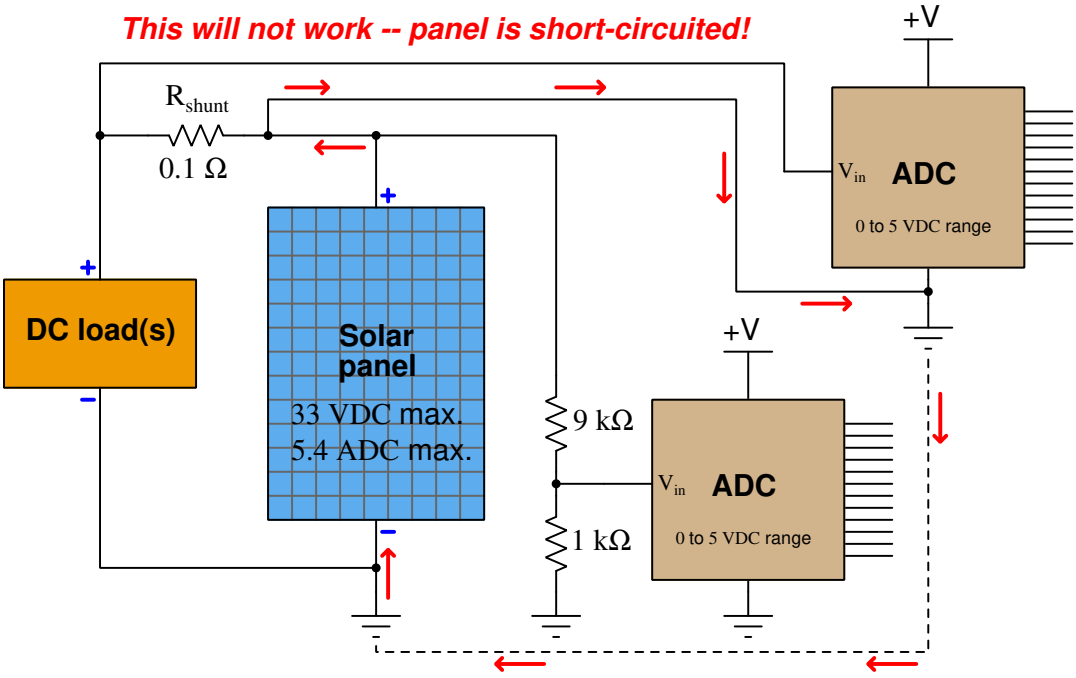


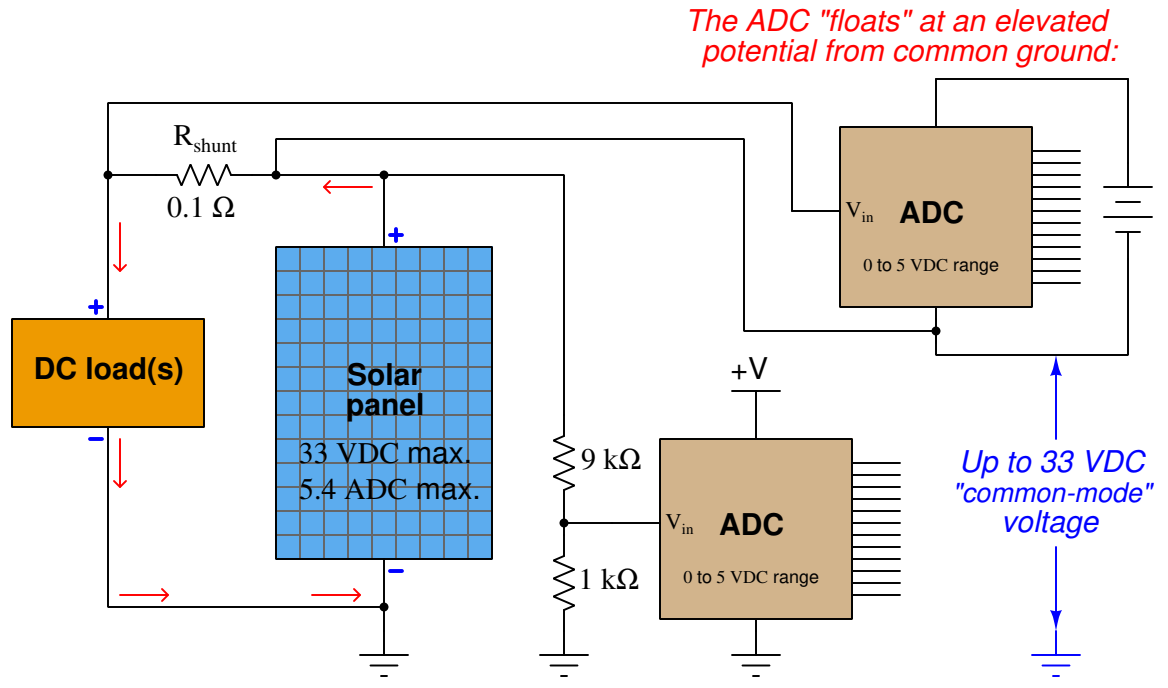
Low-pass ("anti-aliasing") filter circuit front-end to ADC

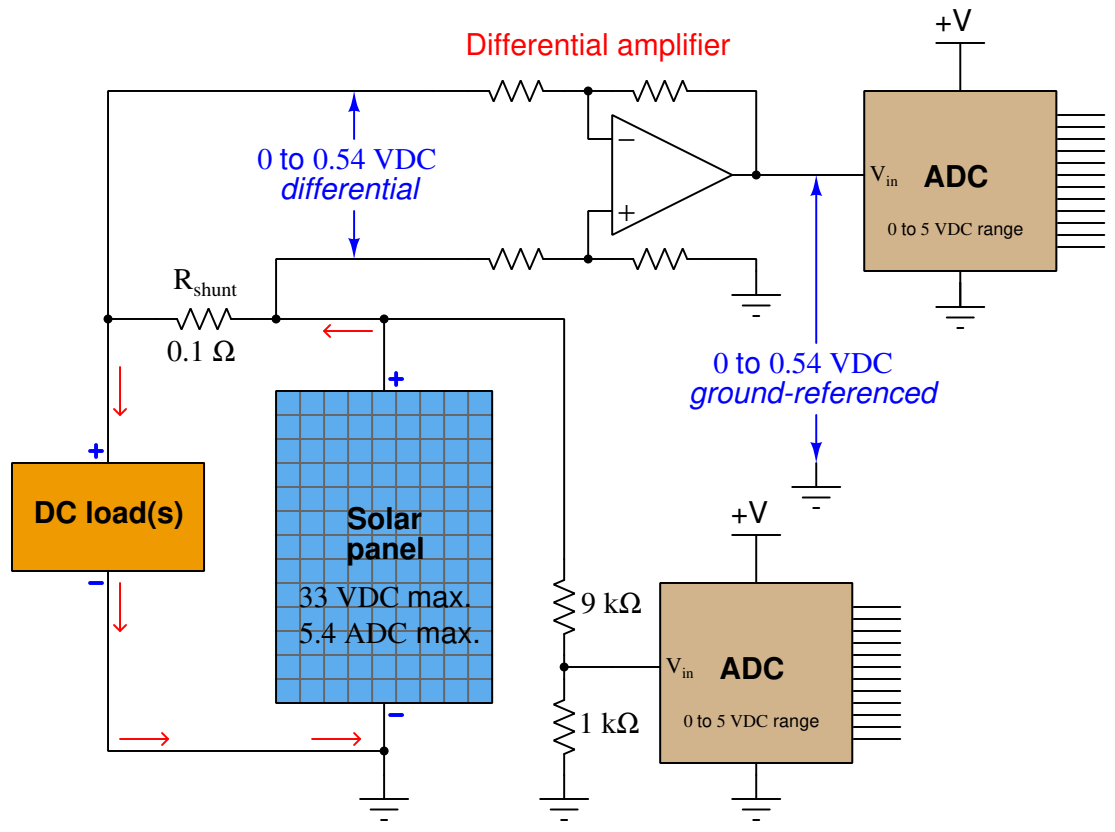


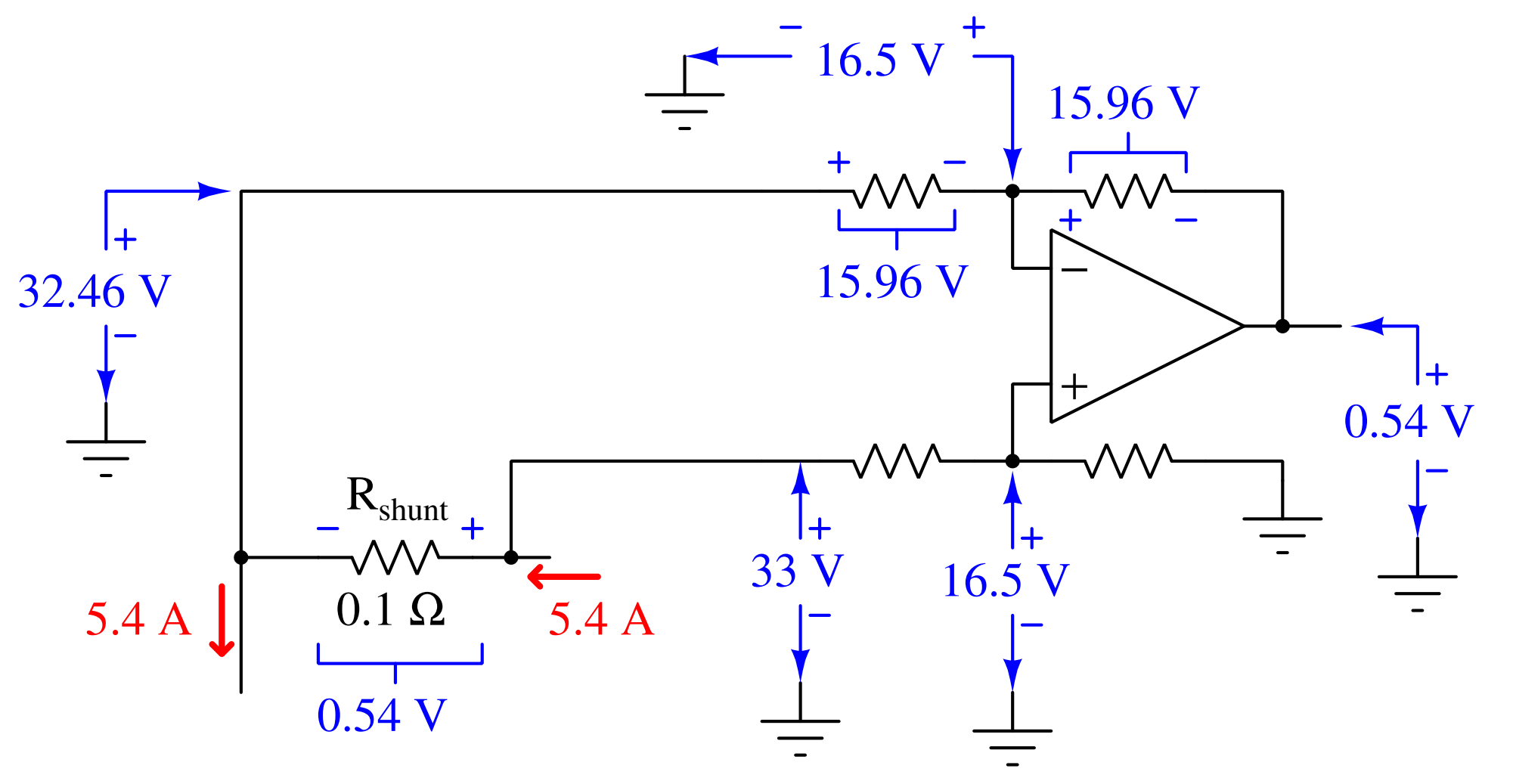

R shunt
0.1 Ω
+
DC load(s)
−
+
Solar panel
33 VDC max.
5.4 ADC max.
−
+V
V in
ADC
0 to 5 VDC range
+V
V in
ADC
0 to 5 VDC range


R shunt
0.1 Ω
+
DC load(s)
−
+
Solar panel
33 VDC max.
5.4 ADC max.
−
9 kΩ
1 kΩ
+V
V in
ADC
0 to 5 VDC range
+V
V in
ADC
0 to 5 VDC range

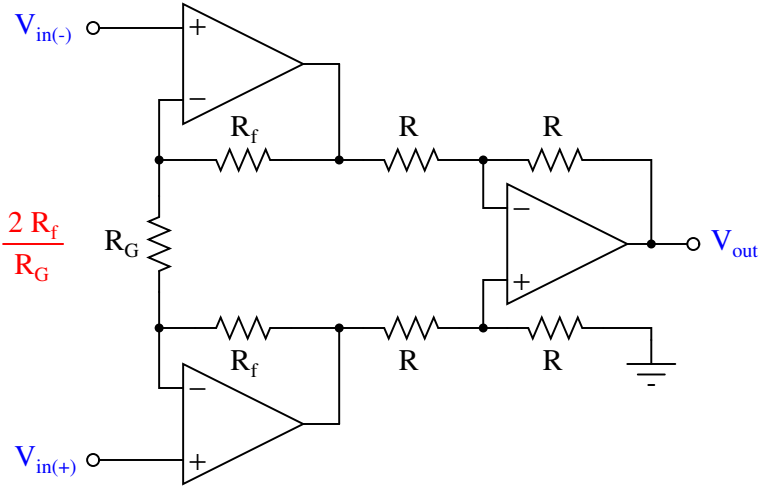

This will not work -- panel is short-circuited!
+V
R shunt
0.1 Ω
V in
ADC
0 to 5 VDC range
DC load(s)
Solar panel
33 VDC max.
5.4 ADC max.
9 kΩ
1 kΩ
+V
V in
ADC
0 to 5 VDC range


The ADC "floats" at an elevated potential from common ground:
R_{shunt}
0.1 Ω
DC load(s)
Solar panel
33 VDC max.
5.4 ADC max.
V_{in} ADC
0 to 5 VDC range
+V
9 kΩ
1 kΩ
V_{in} ADC
0 to 5 VDC range
Up to 33 VDC "common-mode" voltage


Differential amplifier
+V
0 to 0.54 VDC
differential
V in
ADC
0 to 5 VDC range
R shunt
0.1 Ω
0 to 0.54 VDC
ground-referenced
DC load(s)
Solar
panel
33 VDC max.
5.4 ADC max.
+V
9 kΩ
1 kΩ
V in
ADC
0 to 5 VDC range

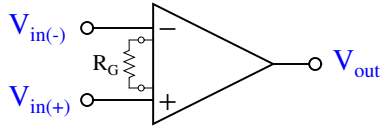

16.5 V
15.96 V
15.96 V
32.46 V
0.54 V
R_{shunt}
0.1 Ω
5.4 A
5.4 A
0.54 V
33 V
16.5 V

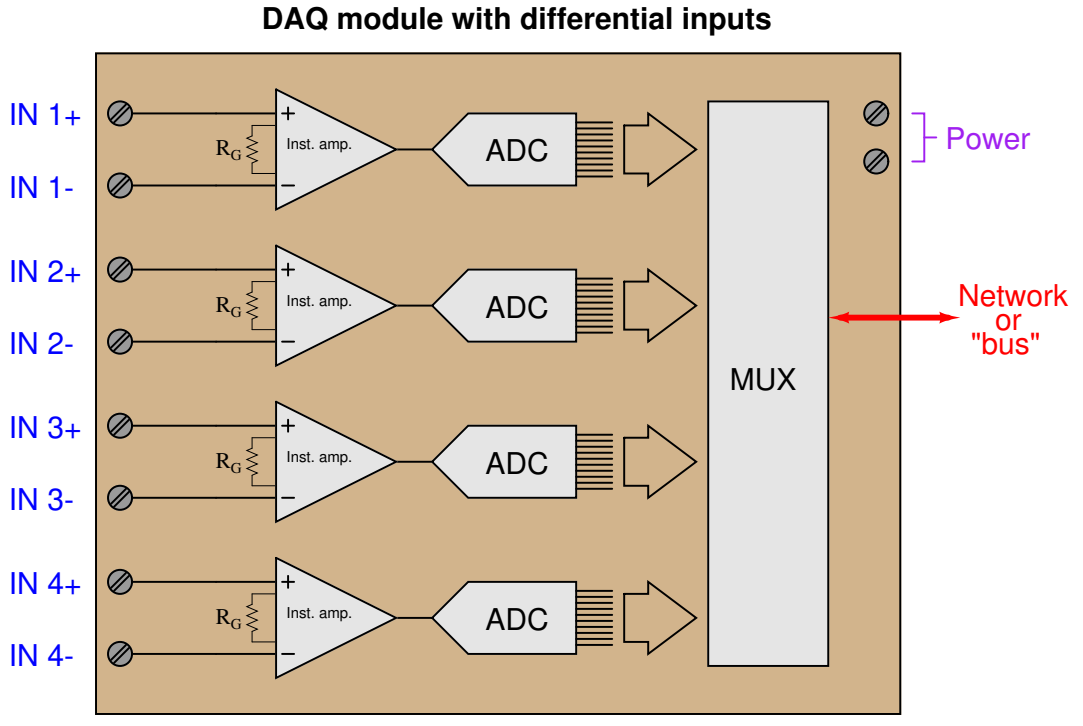
Instrumentation amplifier

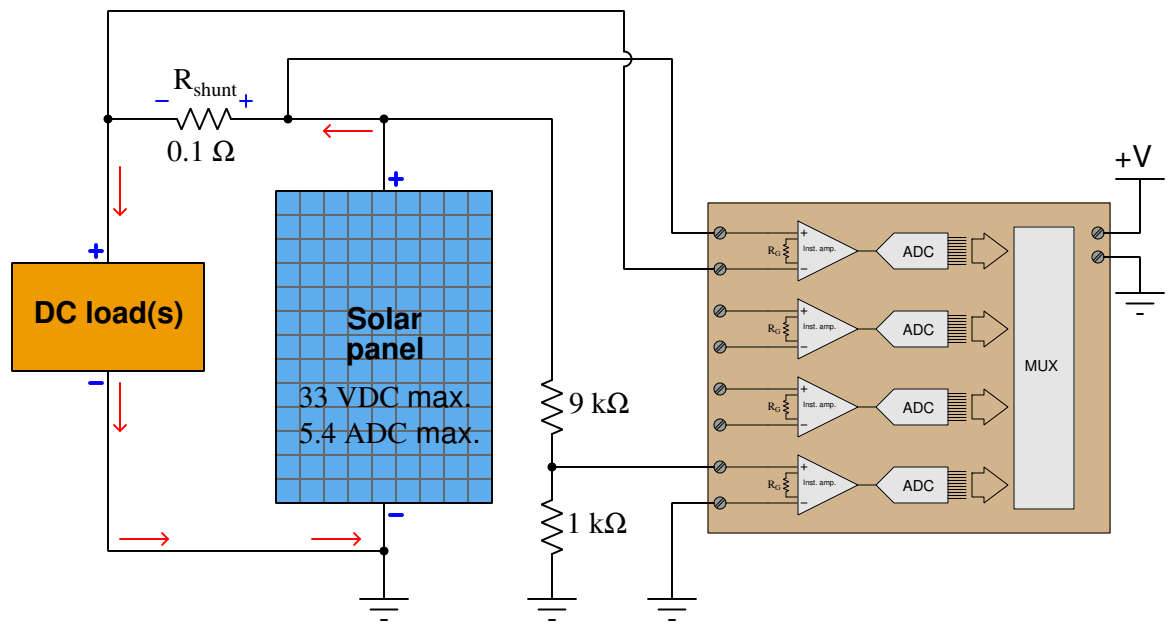


$$\text{Voltage gain} = 1 + \frac{2\,R_f}{R_G}$$

(Simplified diagram)



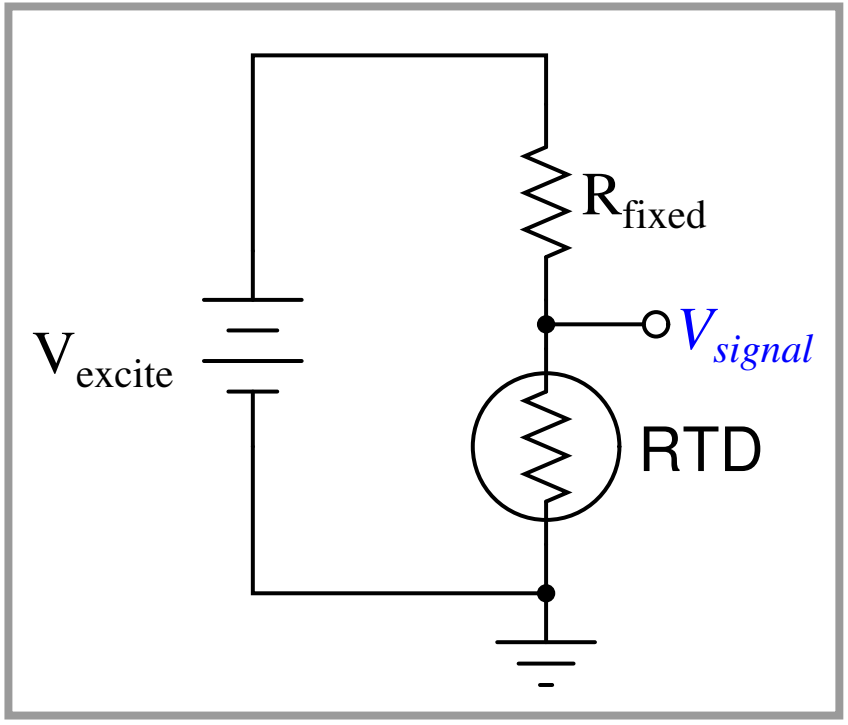

DAQ module with differential inputs
IN 1+
IN 1-
IN 2+
IN 2-
IN 3+
IN 3-
IN 4+
IN 4-
R_G
Inst. amp.
ADC
MUX
Power
Network
or
"bus"


R shunt
0.1 Ω
DC load(s)
Solar panel
33 VDC max.
5.4 ADC max.
9 kΩ
1 kΩ
+V
Inst. amp.
ADC
MUX

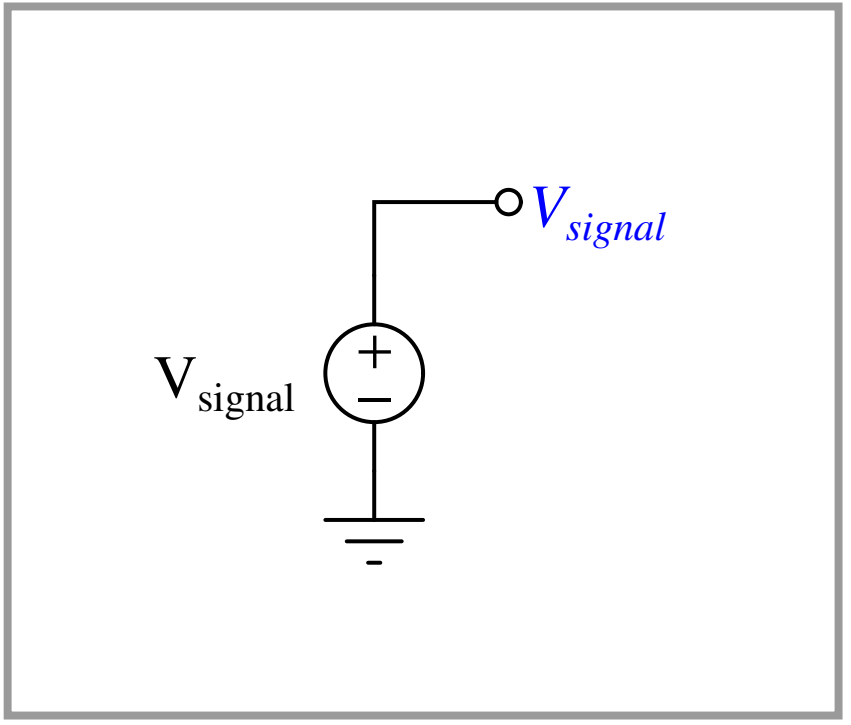

R_{fixed}

Ground-referenced voltage signal

Real circuit

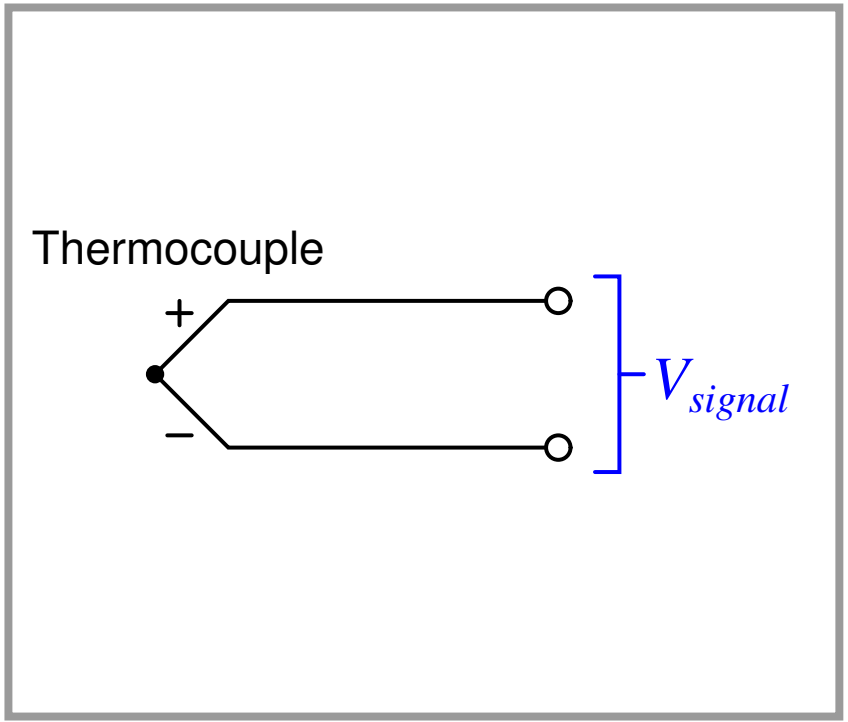


Voltage-source model

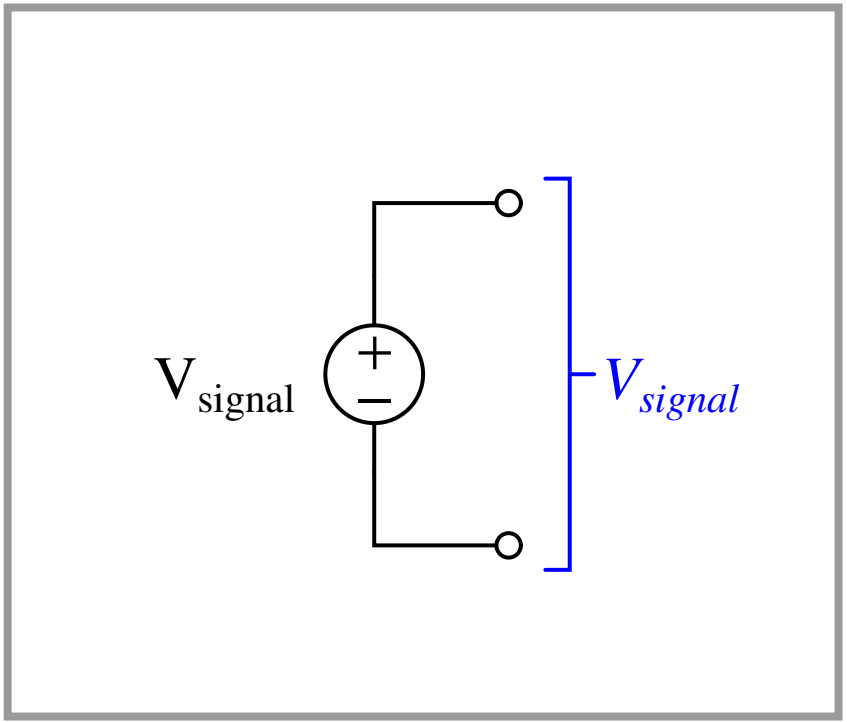


Floating voltage signal

Real circuit

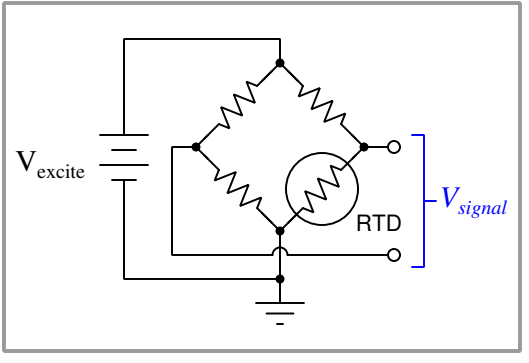


Voltage-source model

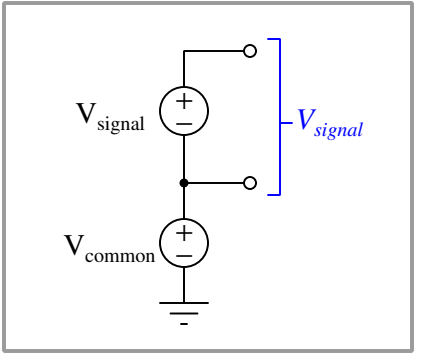


Elevated voltage signal (signal + common-mode voltage)

Real circuit

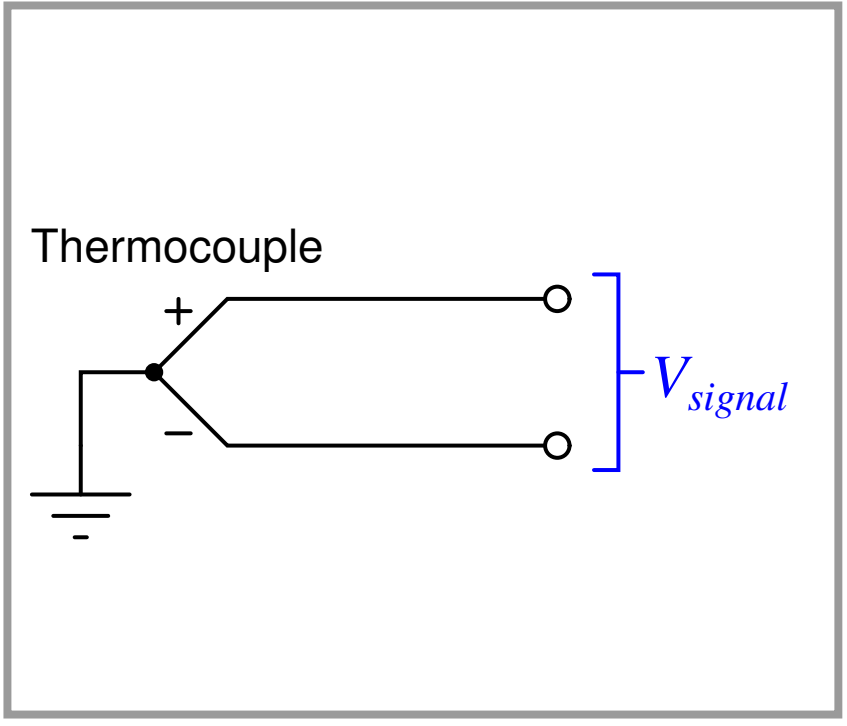


Voltage-source model

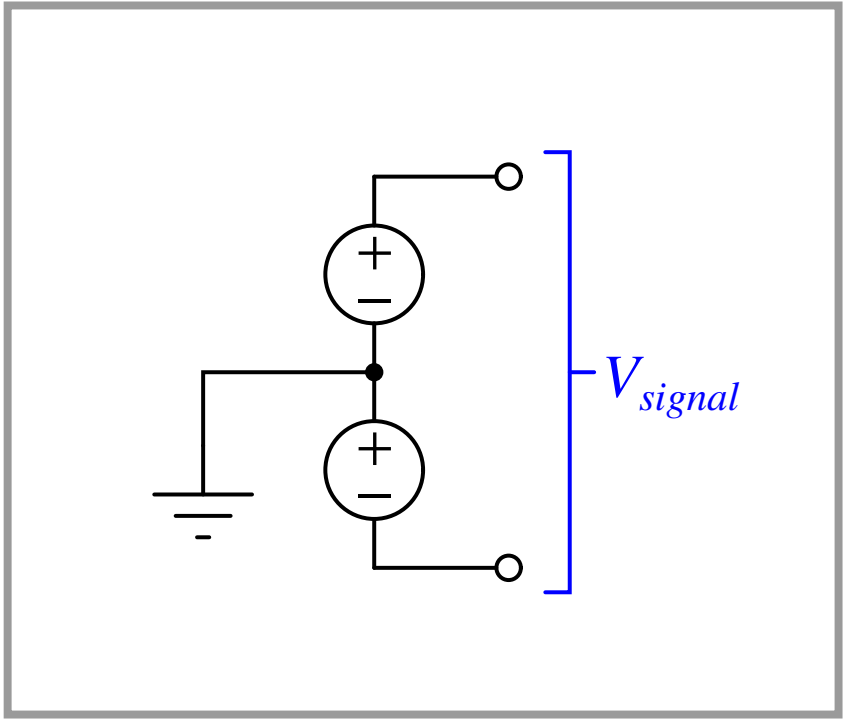


Center-grounded voltage signal

Real circuit

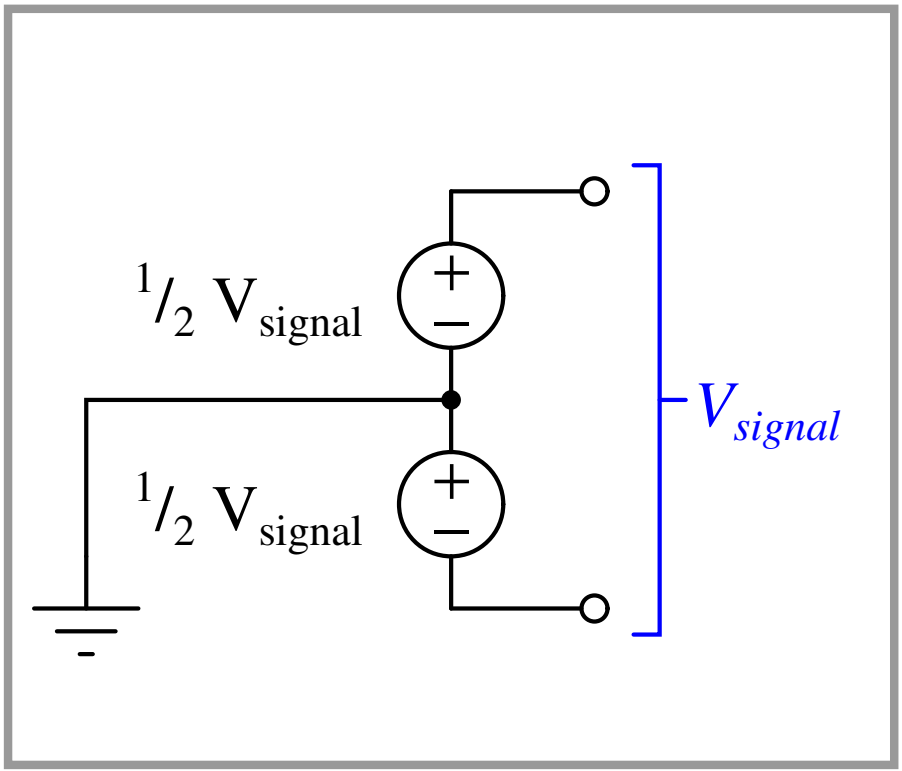


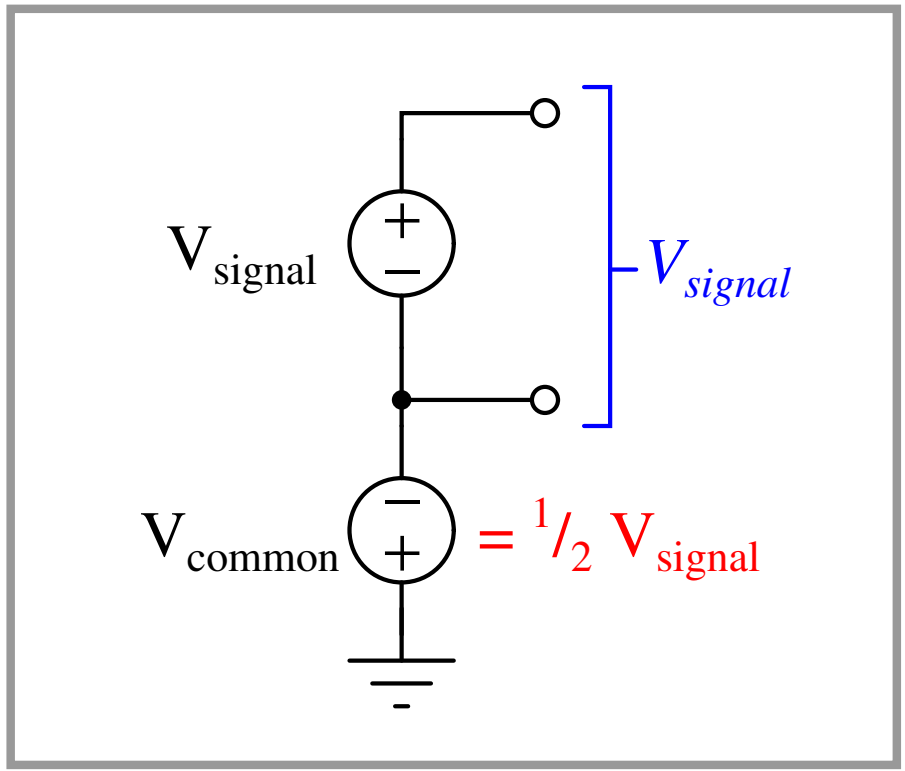
Voltage-source model

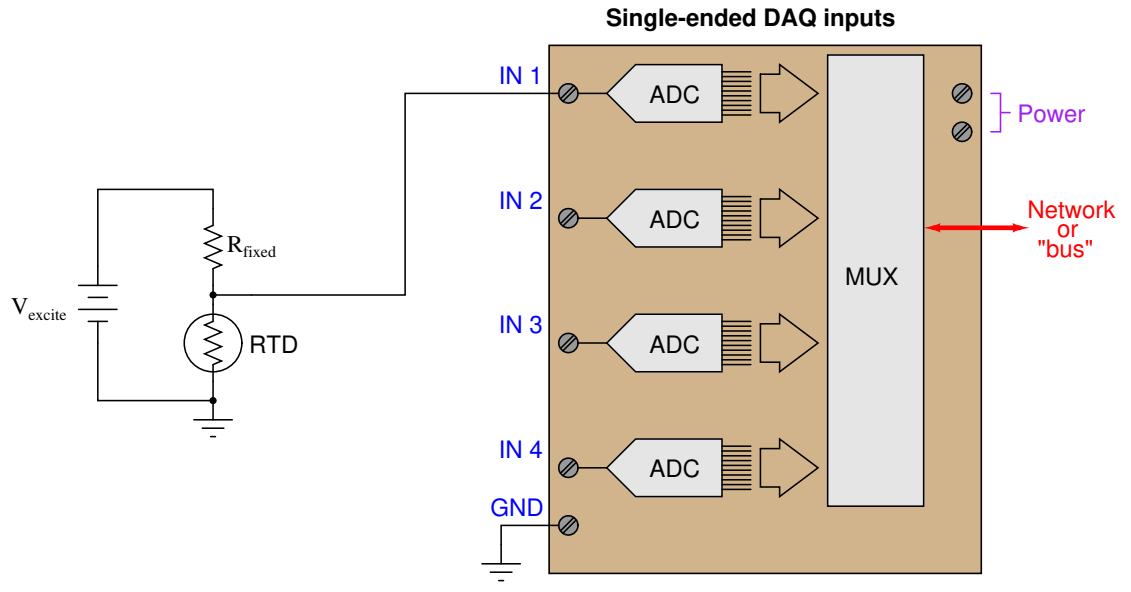


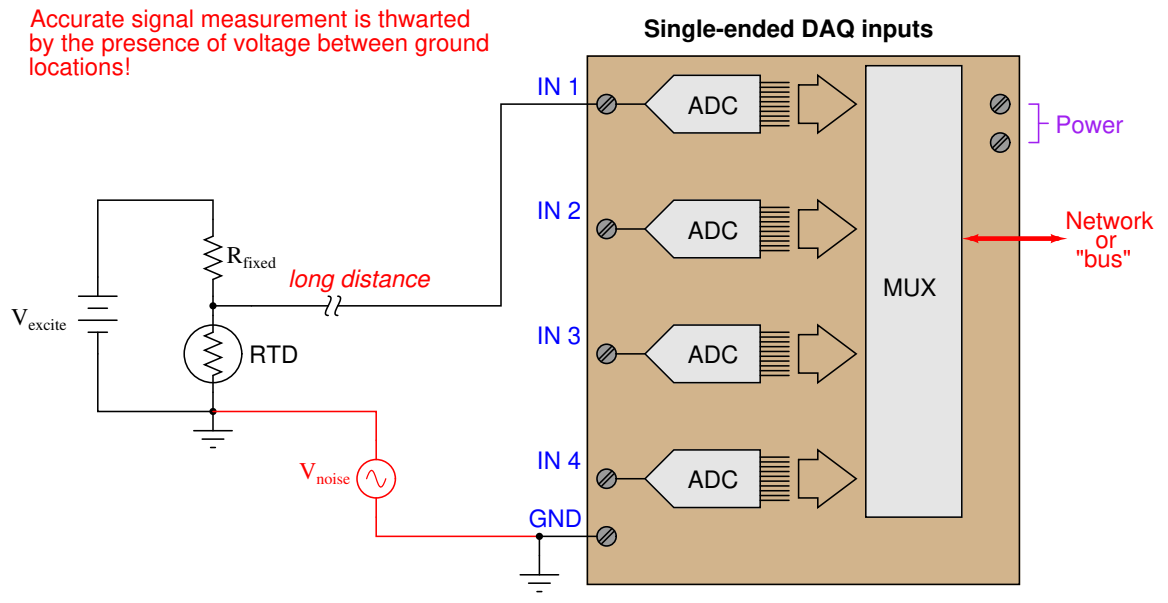
-15

Center-grounded voltage signal

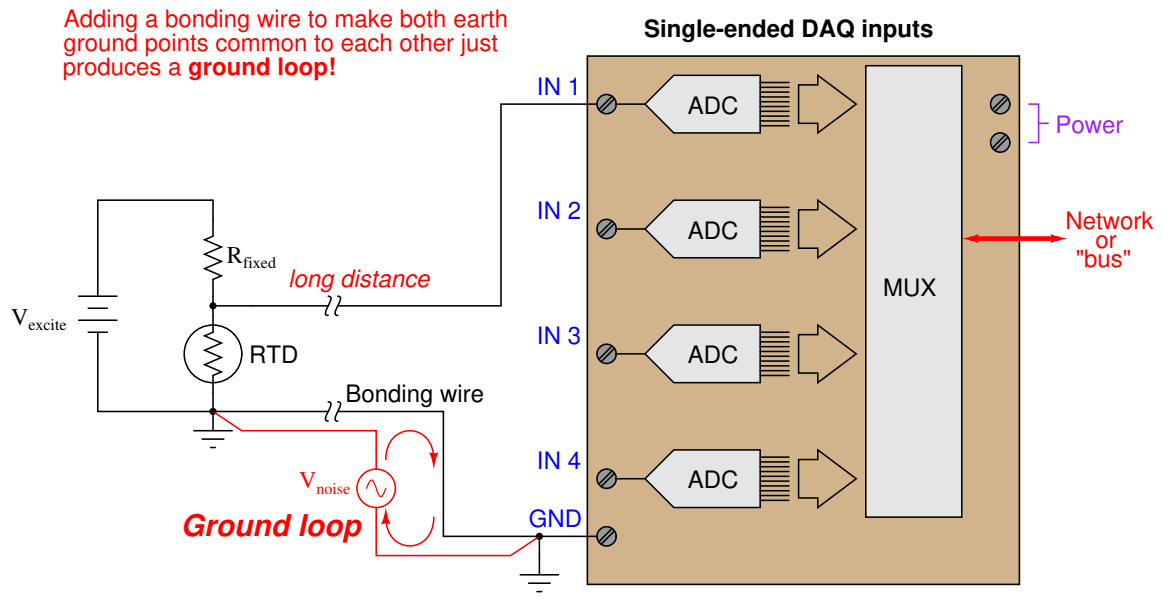


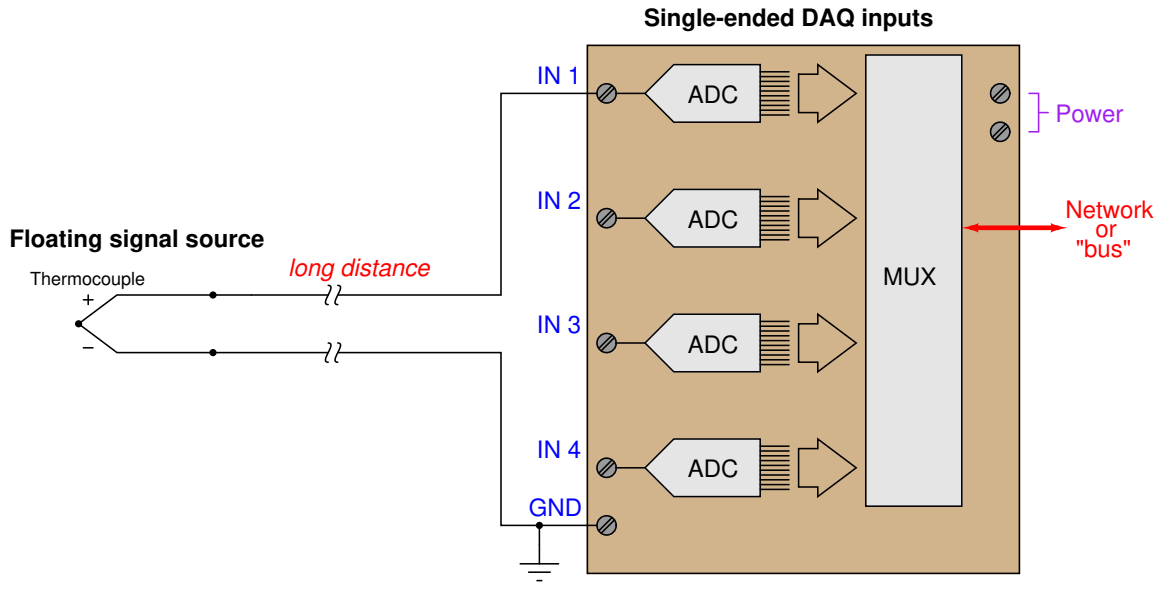


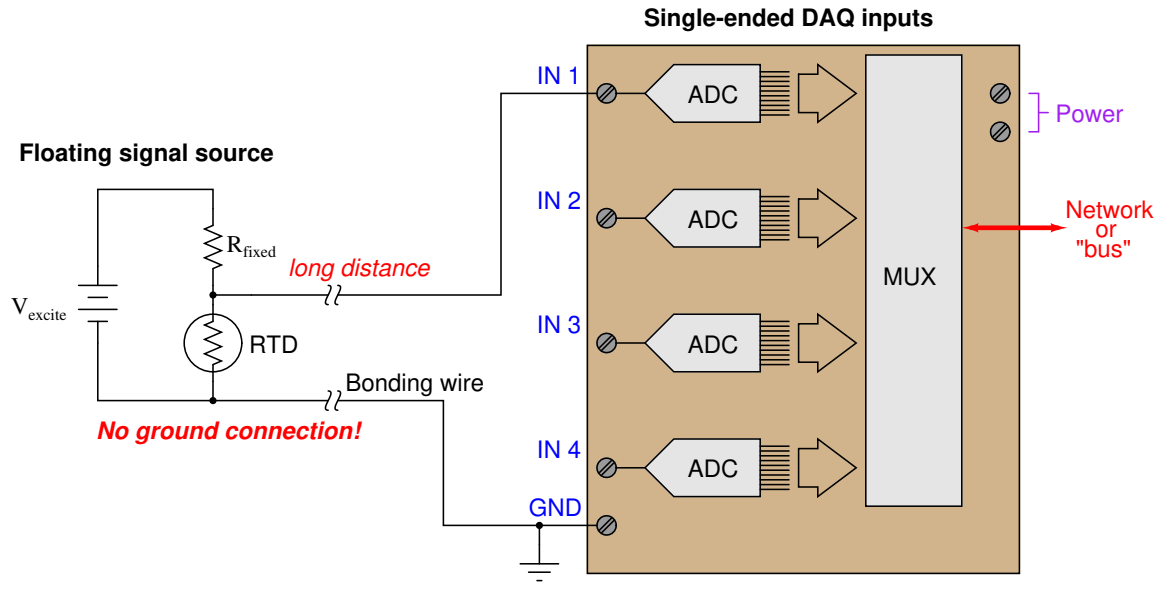

Single-ended DAQ inputs
IN 1
IN 2
IN 3
IN 4
GND
ADC
ADC
ADC
ADC
MUX
Power
Network
or
"bus"
R_{fixed}
V_{excite}
RTD

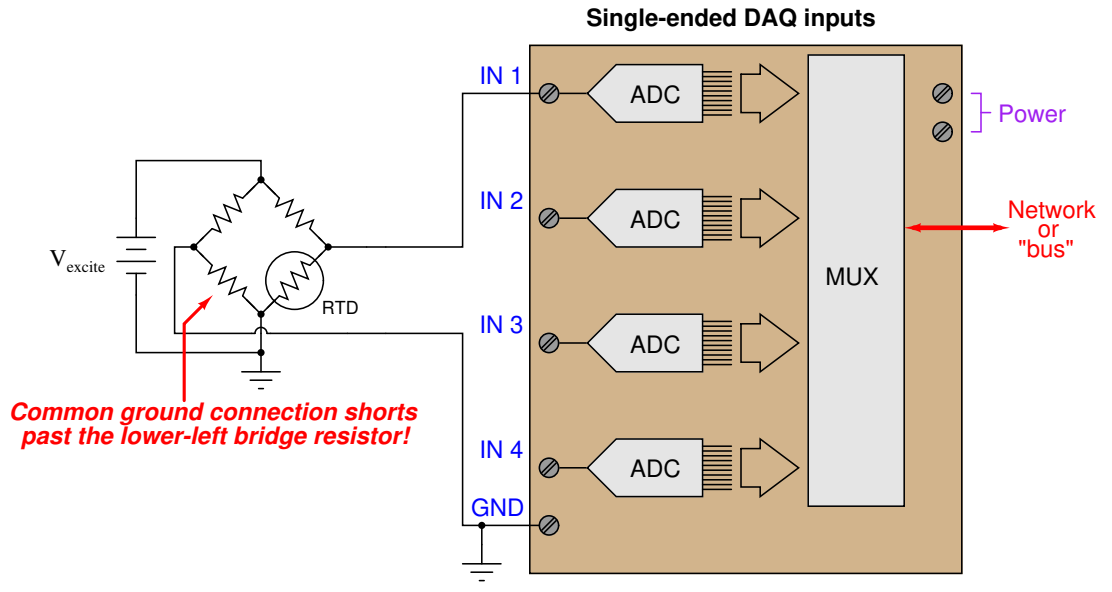

Accurate signal measurement is thwarted by the presence of voltage between ground locations!
Single-ended DAQ inputs
IN 1
IN 2
IN 3
IN 4
GND
ADC
ADC
ADC
ADC
MUX
Power
Network or "bus"
R fixed
long distance
V excite
RTD
V noise

$$V_{noise} = I_{ground} R_{wire}$$

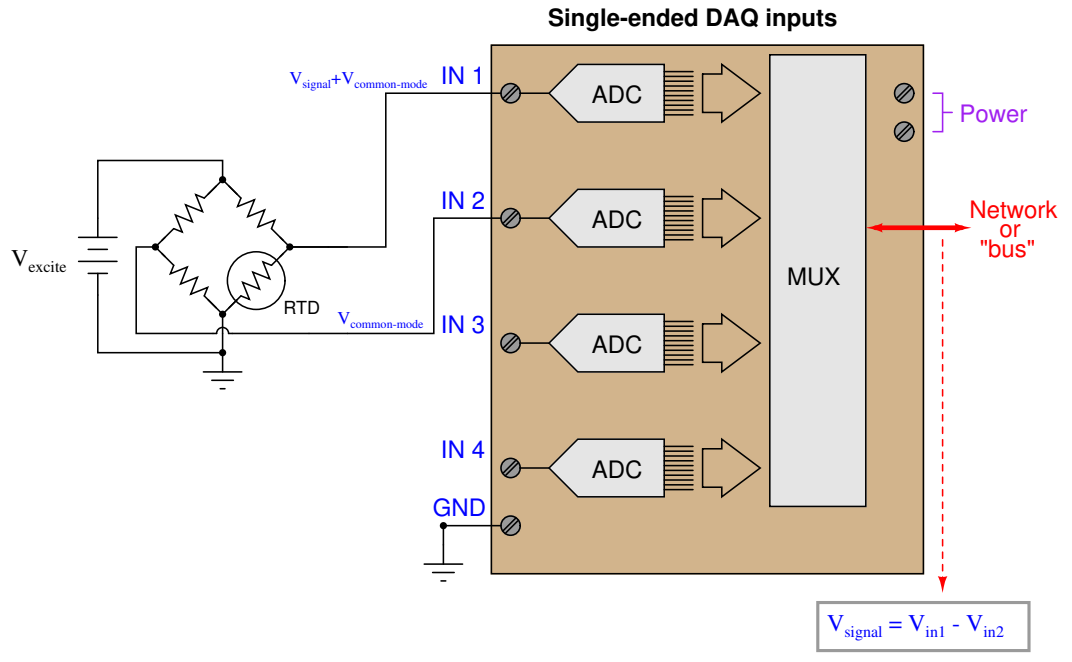

Adding a bonding wire to make both earth ground points common to each other just produces a **ground loop!**
Single-ended DAQ inputs
IN 1
IN 2
IN 3
IN 4
GND
ADC
ADC
ADC
ADC
MUX
Power
Network or "bus"
R_{fixed}
long distance
V_{excite}
RTD
Bonding wire
V_{noise}
Ground loop

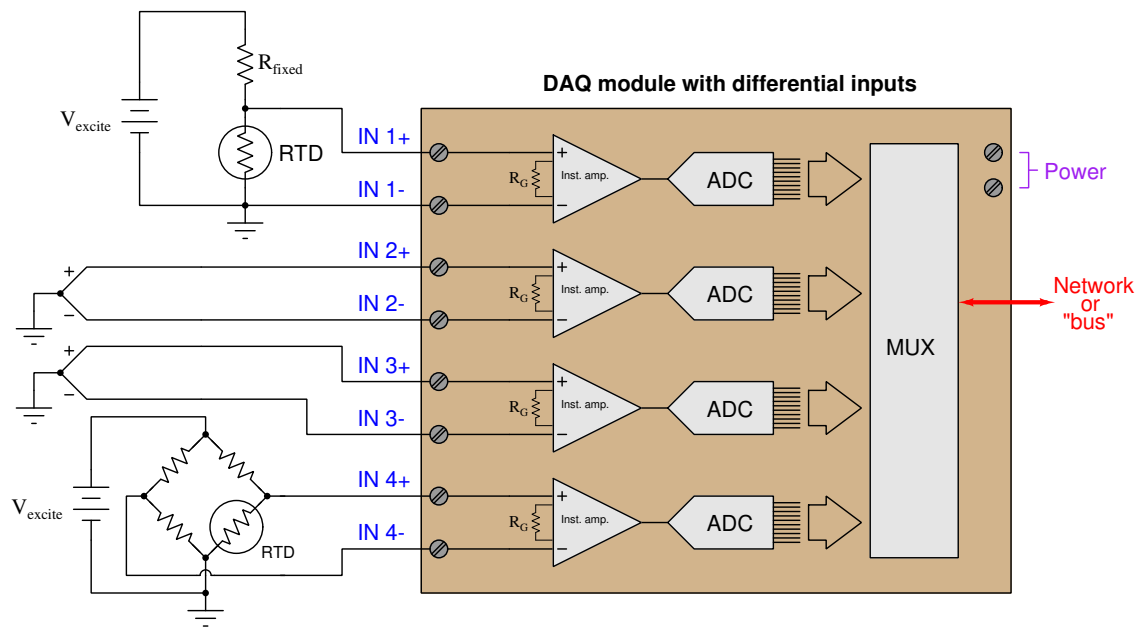

Single-ended DAQ inputs
IN 1
IN 2
IN 3
IN 4
GND
ADC
ADC
ADC
ADC
MUX
Power
Network
or
"bus"
Floating signal source
Thermocouple
+
–
long distance

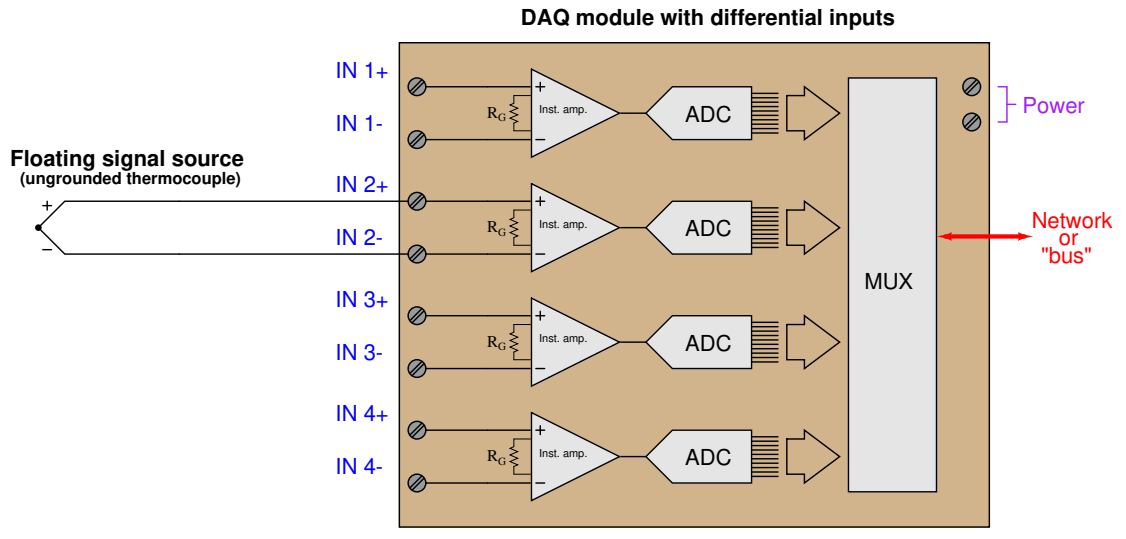

Single-ended DAQ inputs
Floating signal source
R_{fixed}
long distance
V_{excite}
RTD
Bonding wire
No ground connection!
IN 1
IN 2
IN 3
IN 4
GND
ADC
ADC
ADC
ADC
MUX
Power
Network
or
"bus"

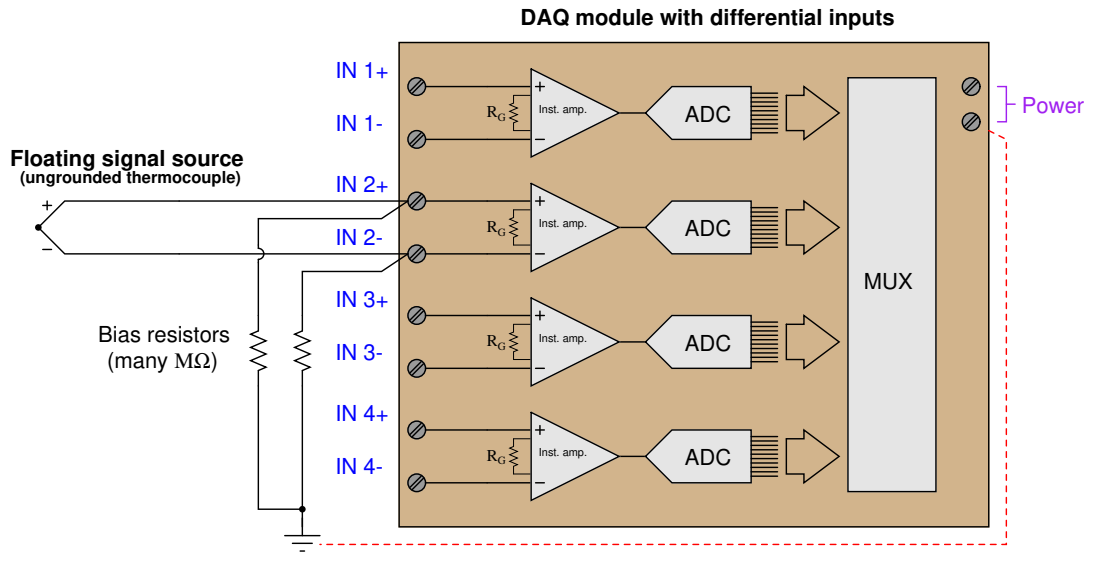

Single-ended DAQ inputs
IN 1
IN 2
IN 3
IN 4
GND
ADC
ADC
ADC
ADC
MUX
Power
Network
or
"bus"
V excite
RTD
Common ground connection shorts
past the lower-left bridge resistor!

$$V_{signal} + V_{common-mode}$$


Single-ended DAQ inputs
$V_{signal}+V_{common-mode}$
IN 1
IN 2
IN 3
IN 4
GND
ADC
ADC
ADC
ADC
MUX
Power
Network
or
"bus"
V_{excite}
RTD
$V_{common-mode}$
$V_{signal} = V_{in1} - V_{in2}$


DAQ module with differential inputs
R fixed
V excite
RTD
IN 1+
IN 1-
IN 2+
IN 2-
IN 3+
IN 3-
IN 4+
IN 4-
R G
Inst. amp.
ADC
MUX
Power
Network
or
"bus"
V excite
RTD


DAQ module with differential inputs
Floating signal source
(ungrounded thermocouple)
+
–
IN 1+
IN 1-
IN 2+
IN 2-
IN 3+
IN 3-
IN 4+
IN 4-
R_G
Inst. amp.
ADC
MUX
Power
Network
or
"bus"


DAQ module with differential inputs
IN 1+
IN 1-
IN 2+
IN 2-
IN 3+
IN 3-
IN 4+
IN 4-
Floating signal source
(ungrounded thermocouple)
+
−
Bias resistors
(many MΩ)
R_G
Inst. amp.
ADC
MUX
Power

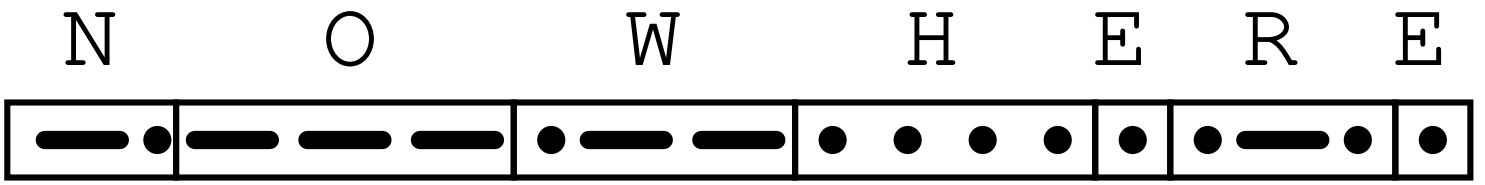
Analog	**Digital**
Only one signal per channel	Many signals per channel possible
Instantaneous	Time-delayed

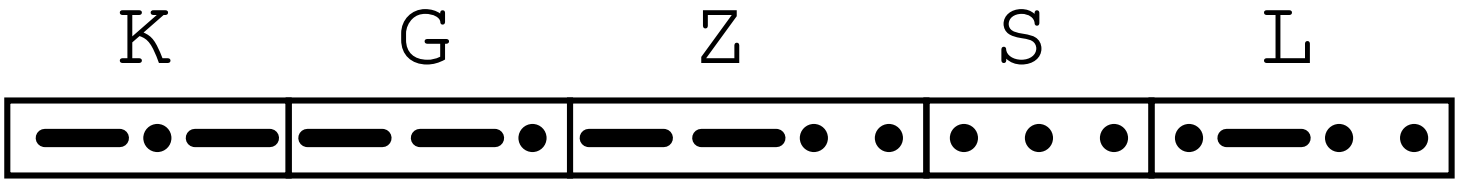
Analog	Digital
Corrupted by any amount of noise	Immune to certain (limited) amounts of noise
Unlimited resolution	Limited resolution

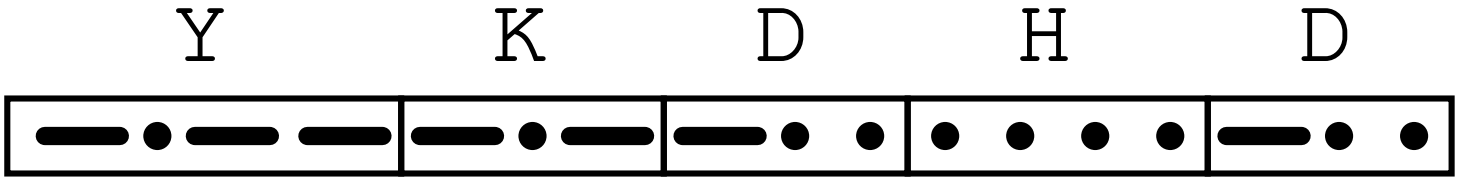
2^{16}

"NOWHERE"

Same sequence of "dots" and "dashes," with multiple interpretations!

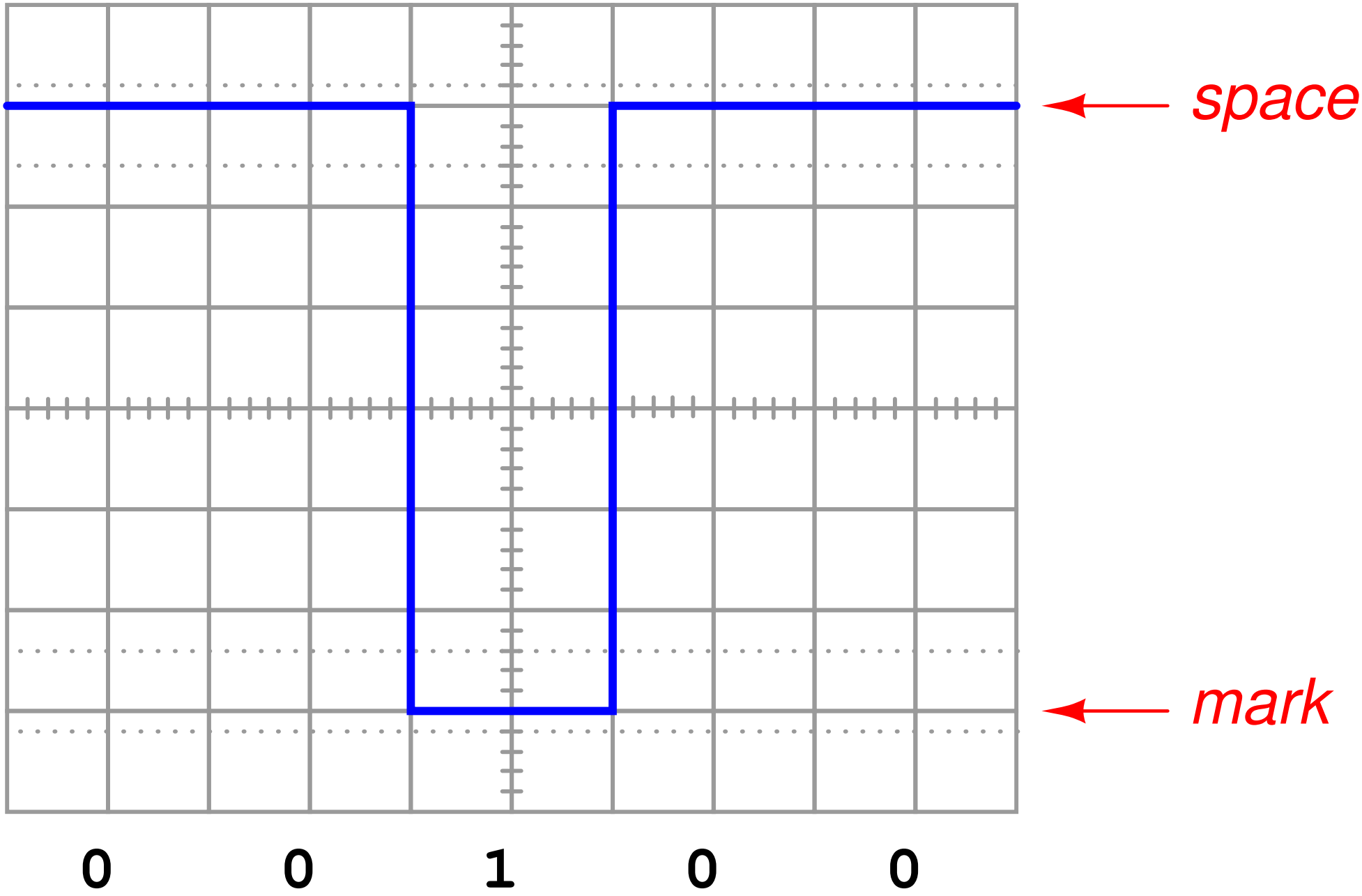




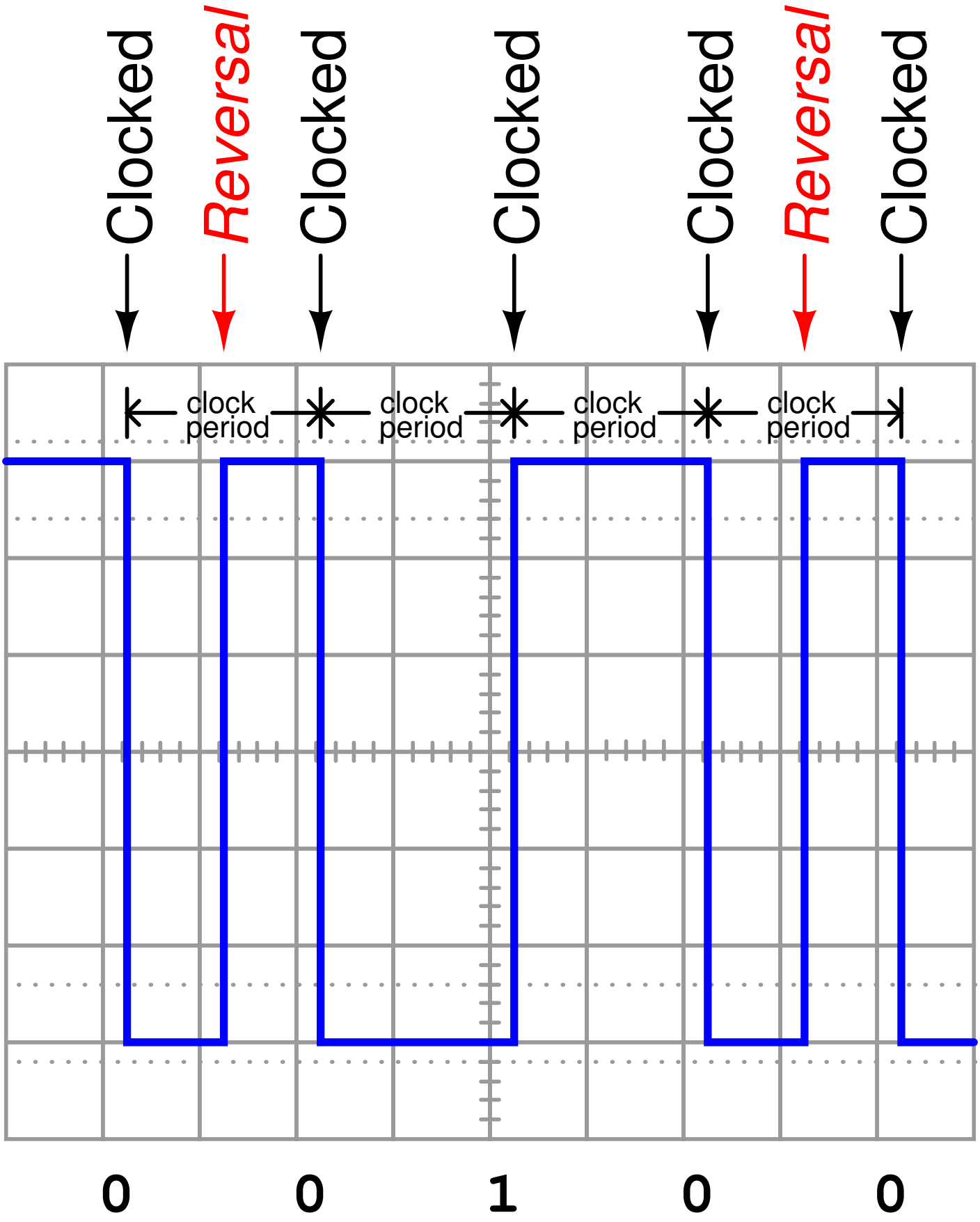


-3

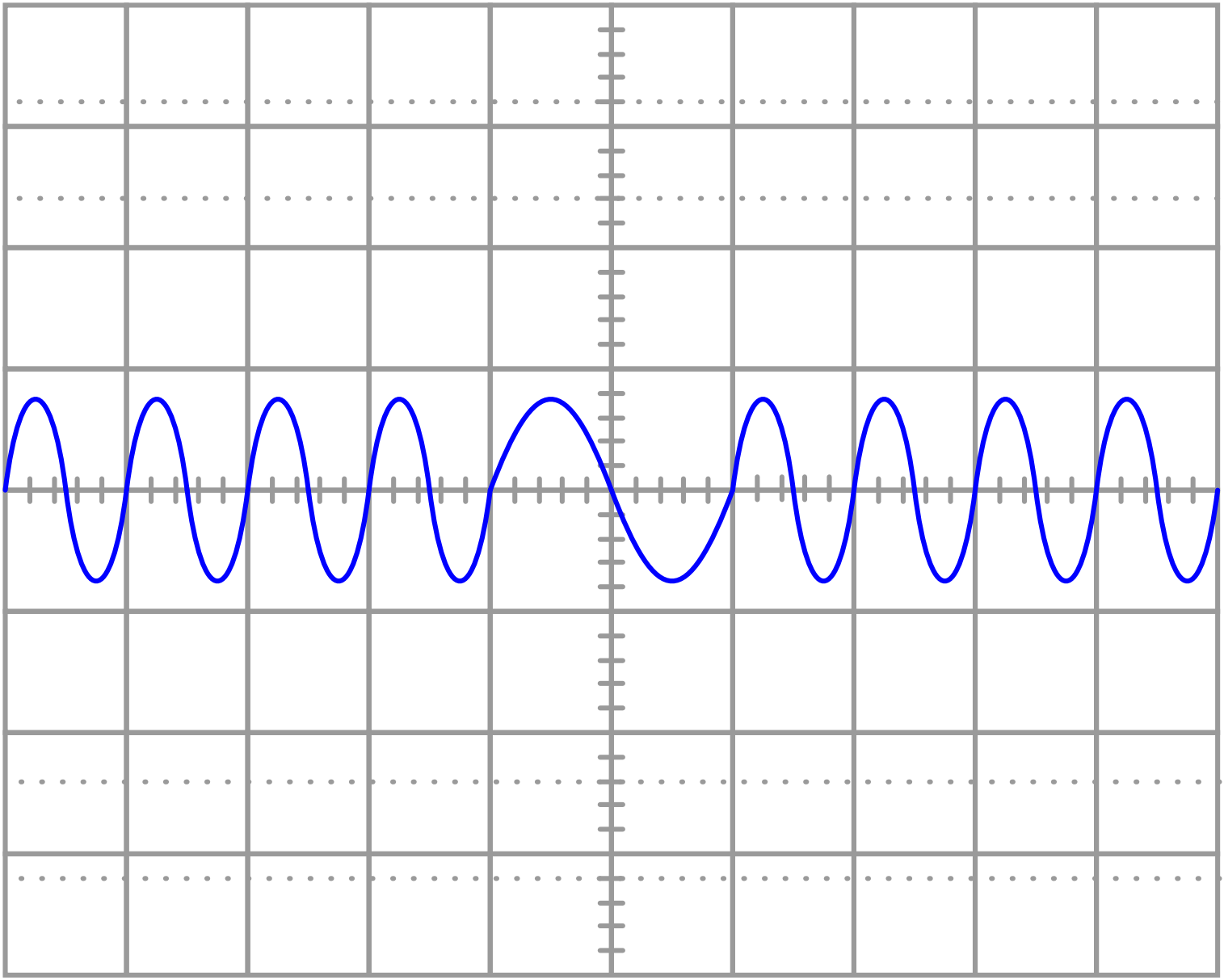
Non-Return-to-Zero (NRZ) encoding



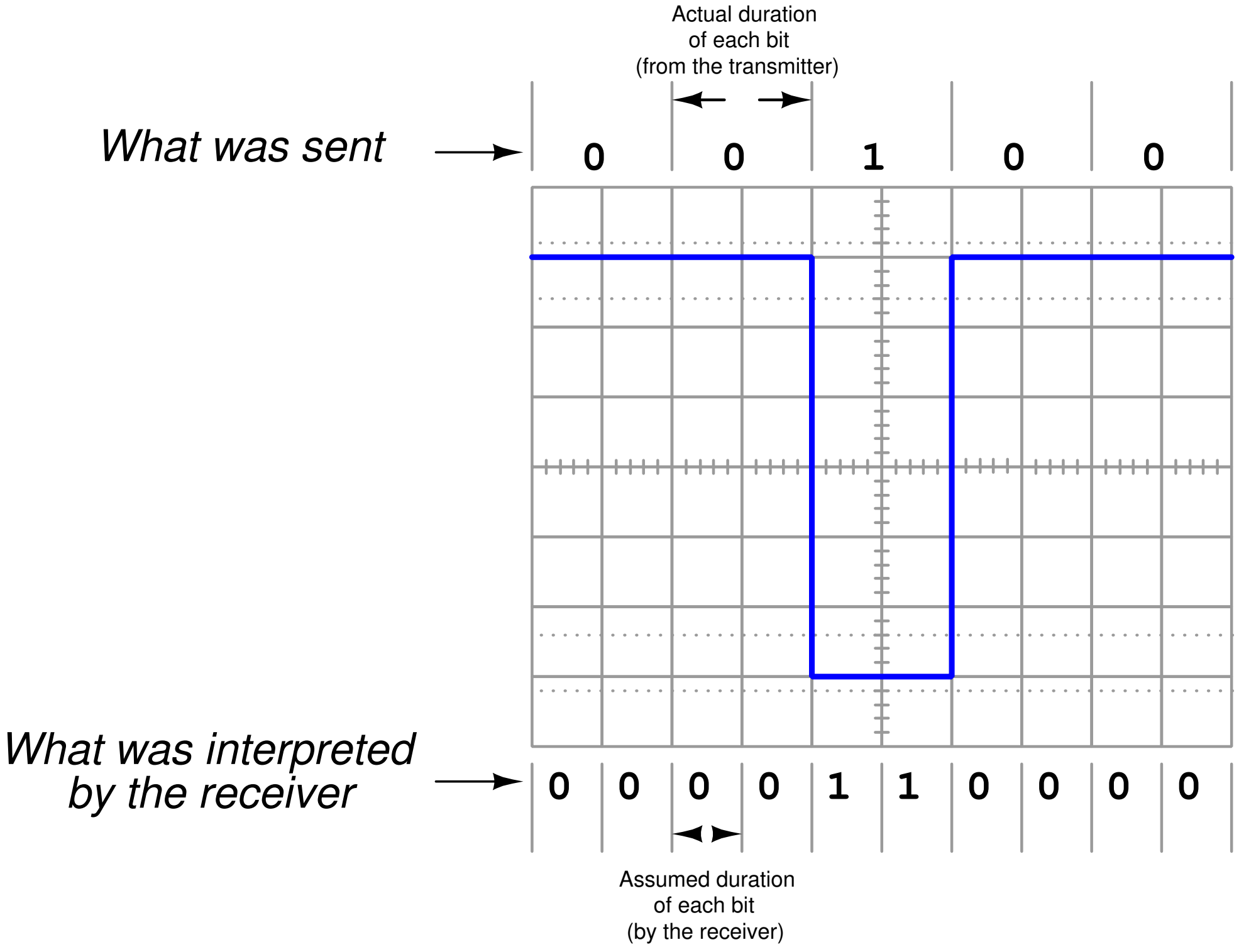
Manchester encoding

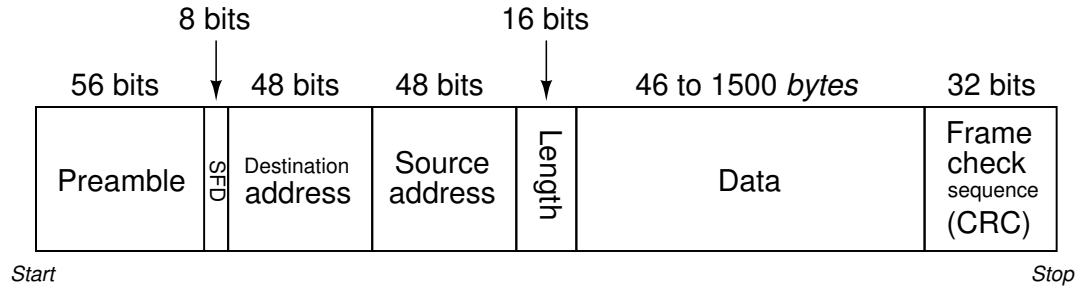


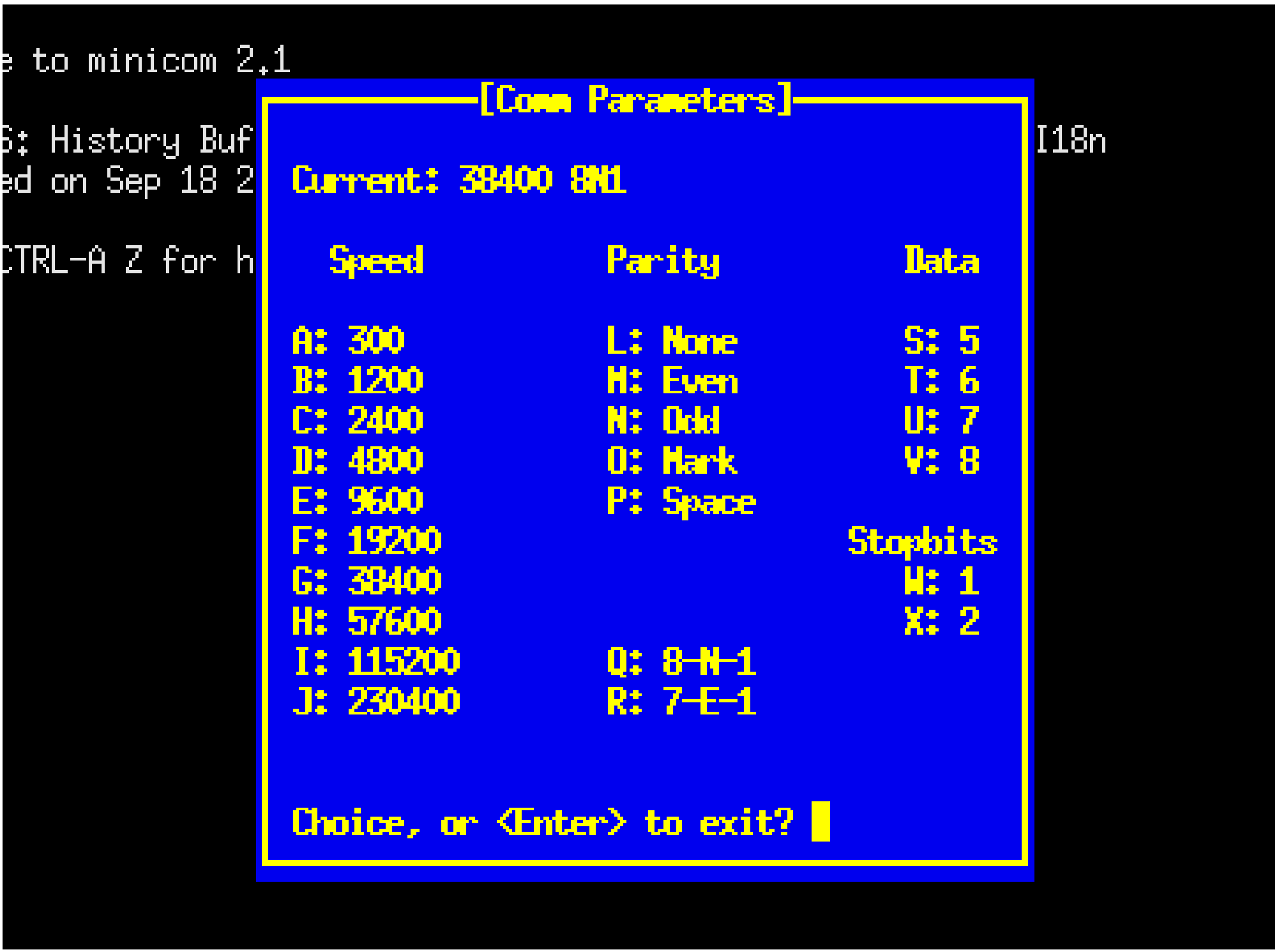
Frequency Shift Key (FSK) encoding

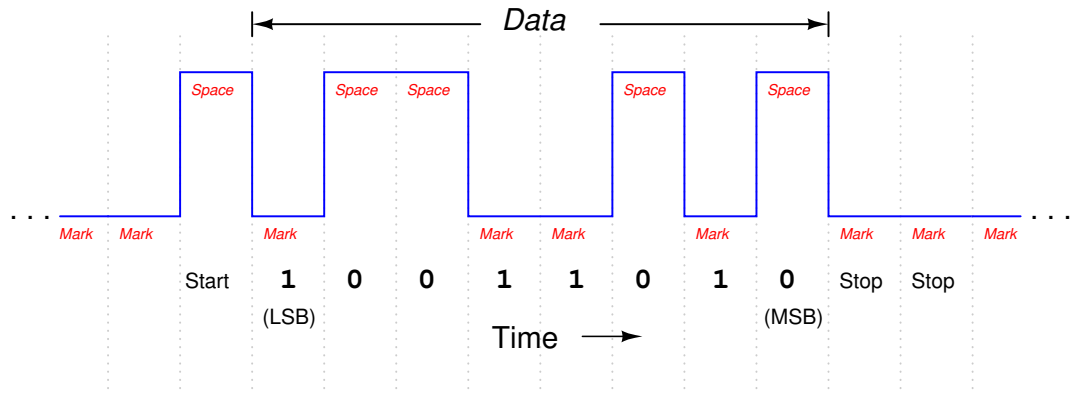


0 0 1 0 0

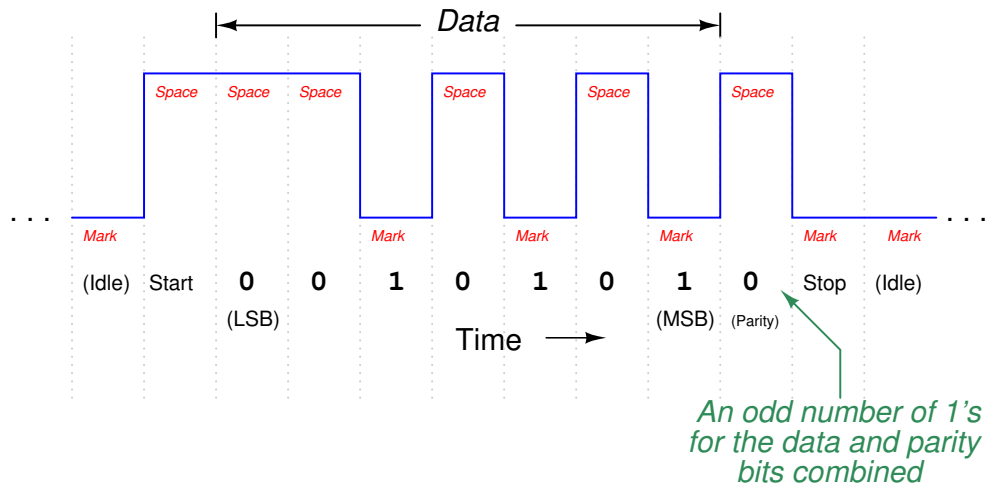

Actual duration
of each bit
(from the transmitter)
What was sent
0
0
1
0
0
What was interpreted
by the receiver
0
0
0
0
1
1
0
0
0
0
Assumed duration
of each bit
(by the receiver)

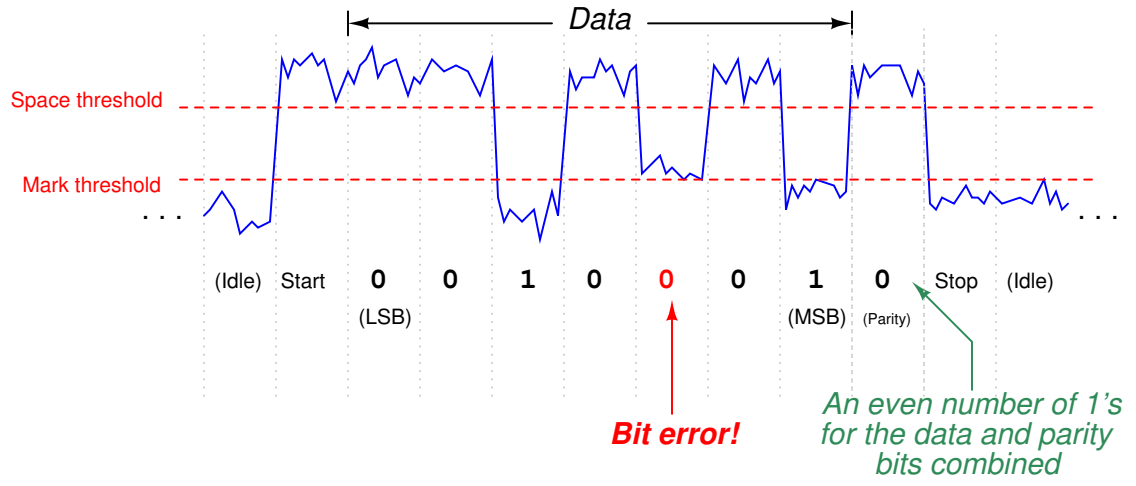

8 bits
16 bits
56 bits
48 bits
48 bits
46 to 1500 bytes
32 bits
Preamble
SFD
Destination address
Source address
Length
Data
Frame check sequence (CRC)
Start
Stop


e to minicom 2.1
6: History Buf
I18n
ed on Sep 18 2
CTRL-A Z for h
[Comm Parameters]
Current: 38400 8N1
Speed
Parity
Data
A: 300
B: 1200
C: 2400
D: 4800
E: 9600
F: 19200
G: 38400
H: 57600
I: 115200
J: 230400
L: None
M: Even
N: Odd
O: Mark
P: Space
Q: 8-N-1
R: 7-E-1
S: 5
T: 6
U: 7
V: 8
Stopbits
W: 1
X: 2
Choice, or <Enter> to exit?

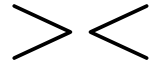


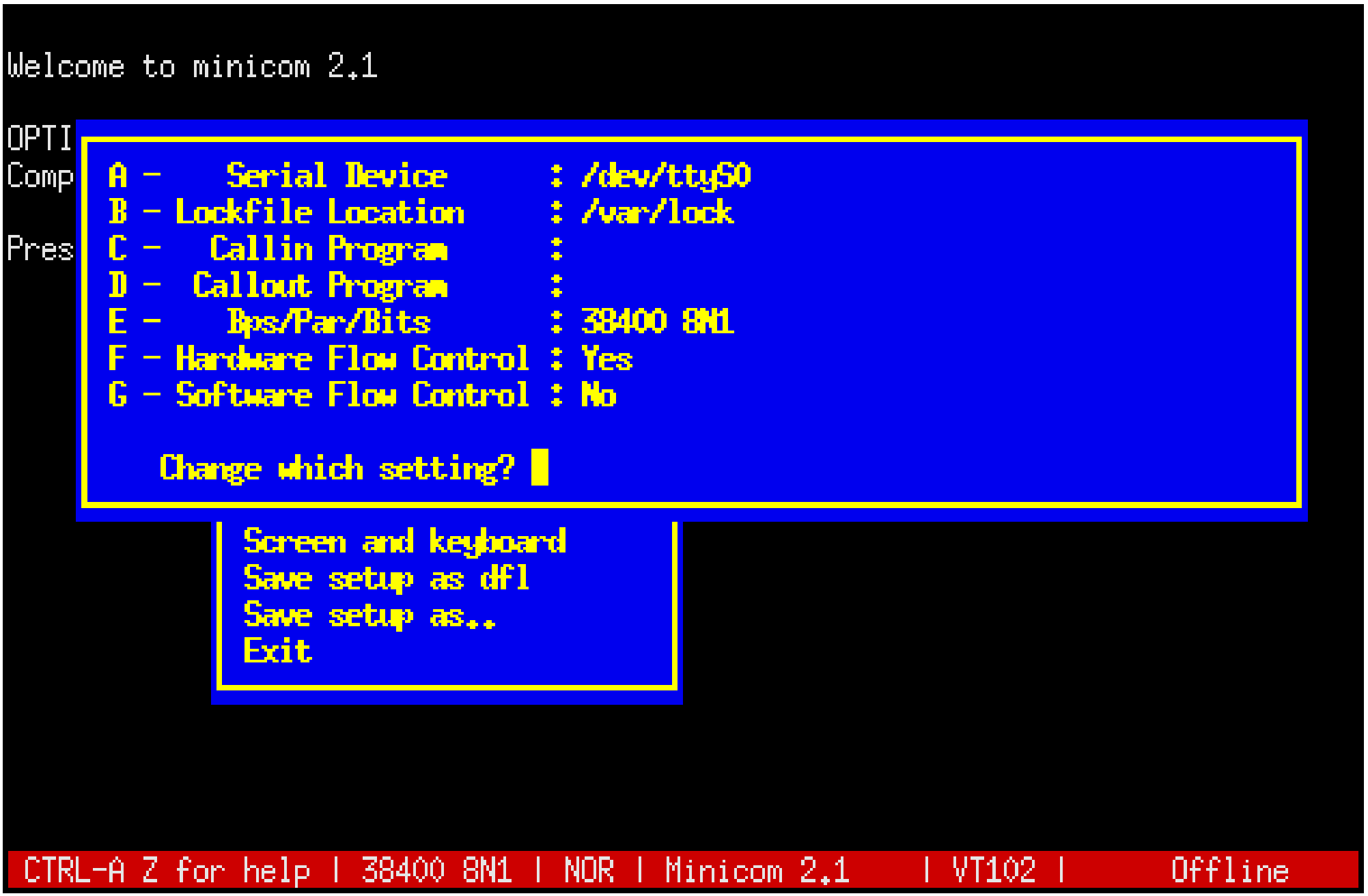
Serial bitstream for the digital byte 01011001, where the least-significant bit (LSB) is sent first


Data
Space
Space
Space
Space
Space
Space
Mark
Mark
Mark
Mark
Mark
Mark
(Idle)
Start
0
0
1
0
1
0
1
0
Stop
(Idle)
(LSB)
(MSB)
(Parity)
Time
An odd number of 1's for the data and parity bits combined

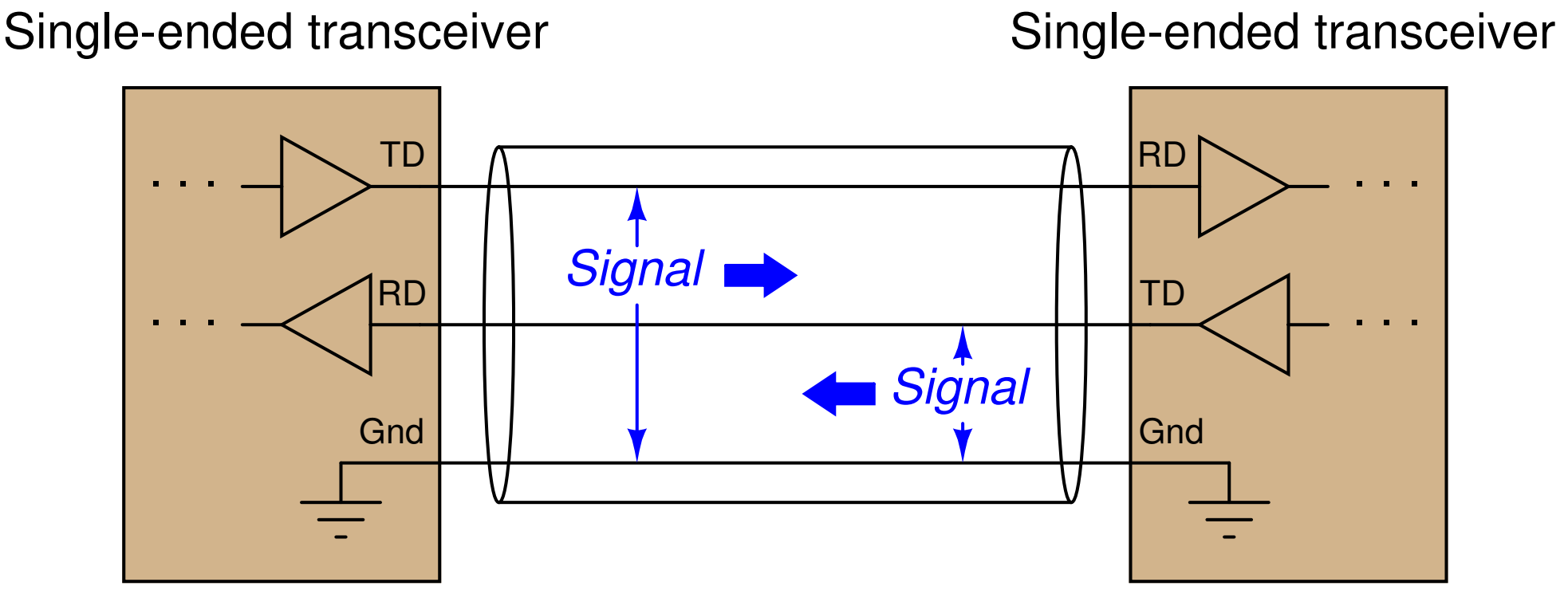

Data
Space threshold
Mark threshold
(Idle)
Start
0
(LSB)
0
1
0
0
0
1
(MSB)
0
(Parity)
Stop
(Idle)
Bit error!
An even number of 1's for the data and parity bits combined

10^{14}



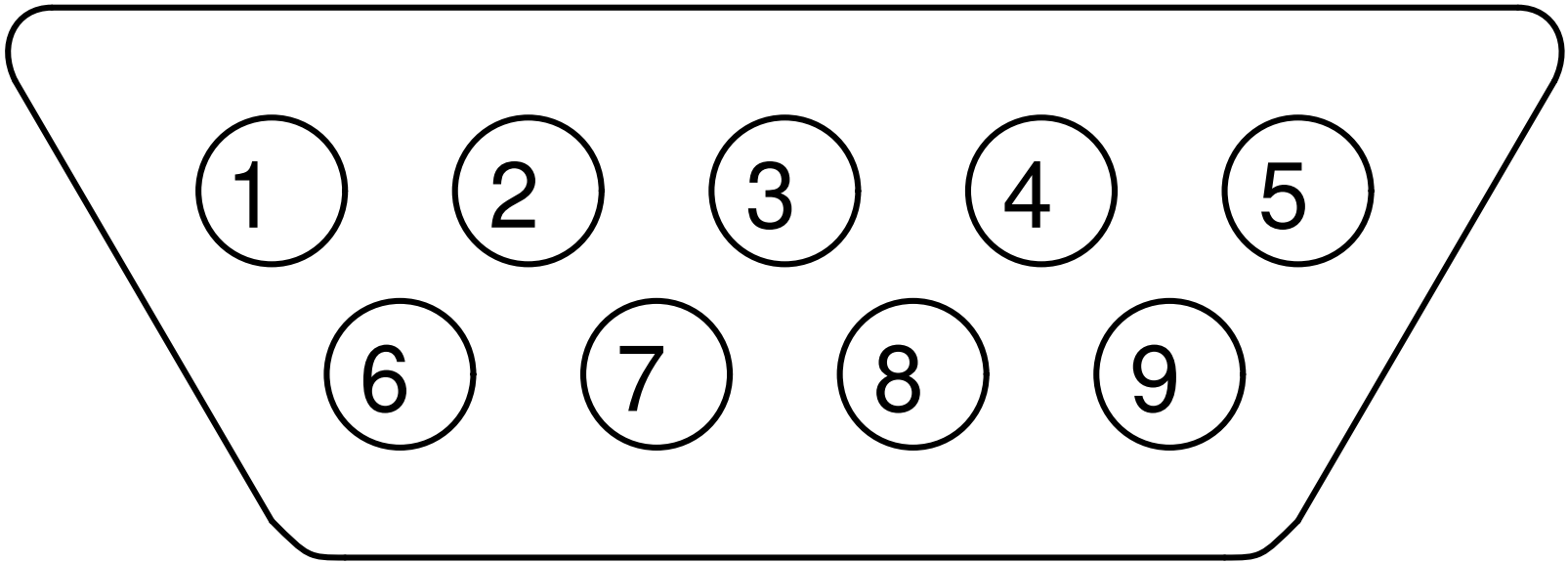

Welcome to minicom 2.1
OPTI
Comp
Pres
A - Serial Device : /dev/ttyS0
B - Lockfile Location : /var/lock
C - Callin Program :
D - Callout Program :
E - Bps/Par/Bits : 38400 8N1
F - Hardware Flow Control : Yes
G - Software Flow Control : No
Change which setting?
Screen and keyboard
Save setup as dfl
Save setup as..
Exit
CTRL-A Z for help | 38400 8N1 | NOR | Minicom 2.1 | VT102 | Offline

Layer 7 **Application**	This is where digital data takes on practical meaning in the context of some human or overall system function. *Examples: HTTP, FTP, HART, Modbus*
Layer 6 **Presentation**	This is where data gets converted between different formats. *Examples: ASCII, EBCDIC, MPEG, JPG, MP3*
Layer 5 **Session**	This is where "conversations" between digital devices are opened, closed, and otherwise managed for reliable data flow. *Examples: Sockets, NetBIOS*
Layer 4 **Transport**	This is where complete data transfer is handled, ensuring all data gets put together and error-checked before use. *Examples: TCP, UDP*
Layer 3 **Network**	This is where the system determines network-wide addresses, ensuring a means for data to get from one node to another. *Examples: IP, ARP*
Layer 2 **Data link**	This is where basic data transfer methods and sequences (frames) are defined within the smallest segment(s) of a network. *Examples: CSMA/CD, Token passing, Master/Slave*
Layer 1 **Physical**	This is where data bits are equated to electrical, optical, or other signals. Other physical details such as cable and connector types are also specified here. *Examples: EIA/TIA-232, 422, 485, Bell 202*


Single-ended transceiver
Single-ended transceiver
TD
RD
Gnd
Signal
Signal
RD
TD
Gnd

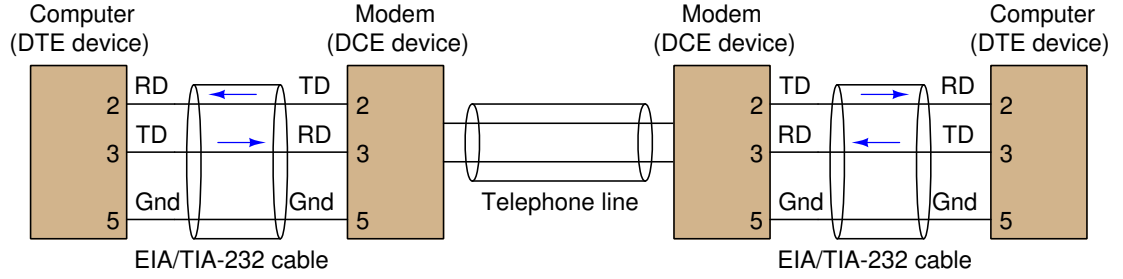
-5

DE-9 cable connector

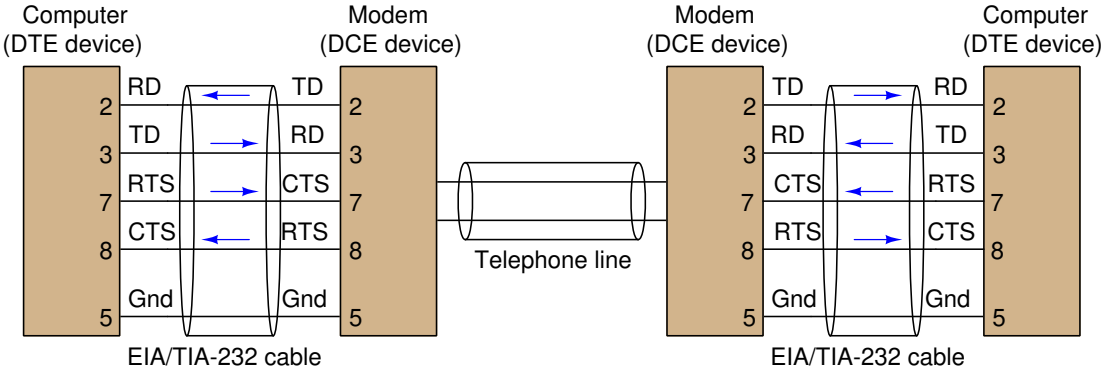


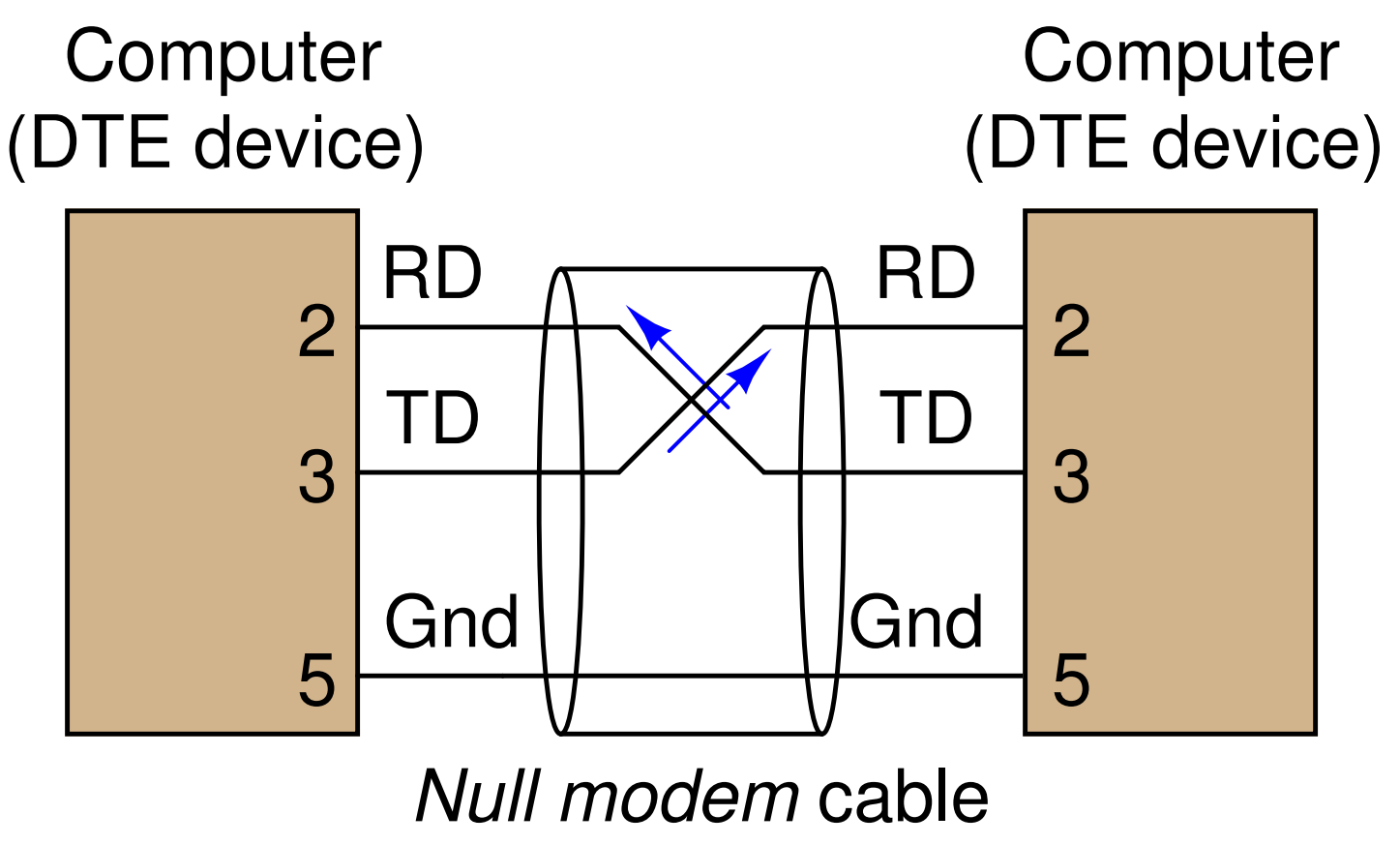
Pin number	**Assignment**	**Abbreviation**
1	Carrier Detect	CD
2	**Received Data**	**RD**
3	**Transmitted Data**	**TD**
4	Data Terminal Ready	DTR
5	**Signal Ground**	**Gnd**
6	Data Set Ready	DSR
7	Request To Send	RTS
8	Clear To Send	CTS
9	Ring Indicator	RI

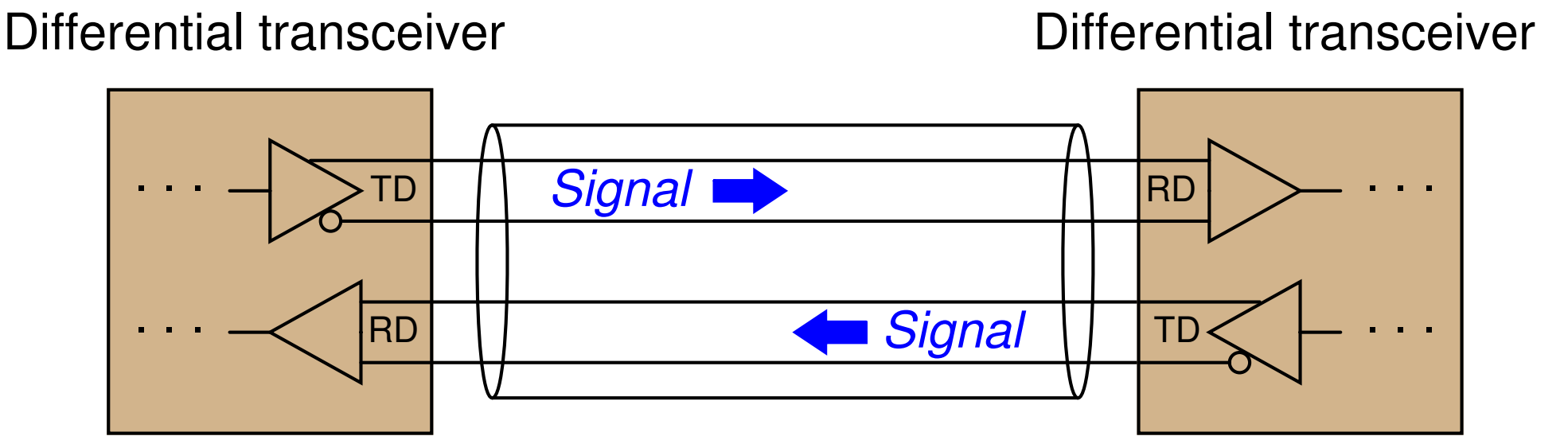
EIA/TIA-232 communication using software flow control

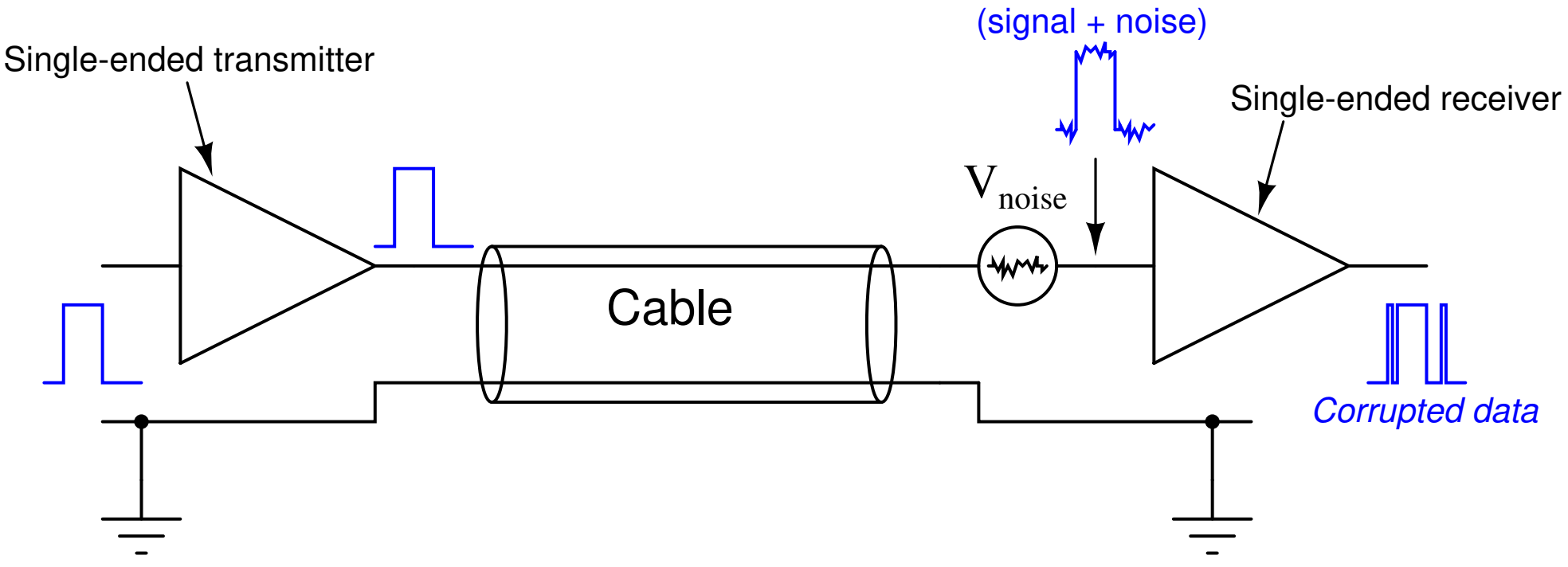


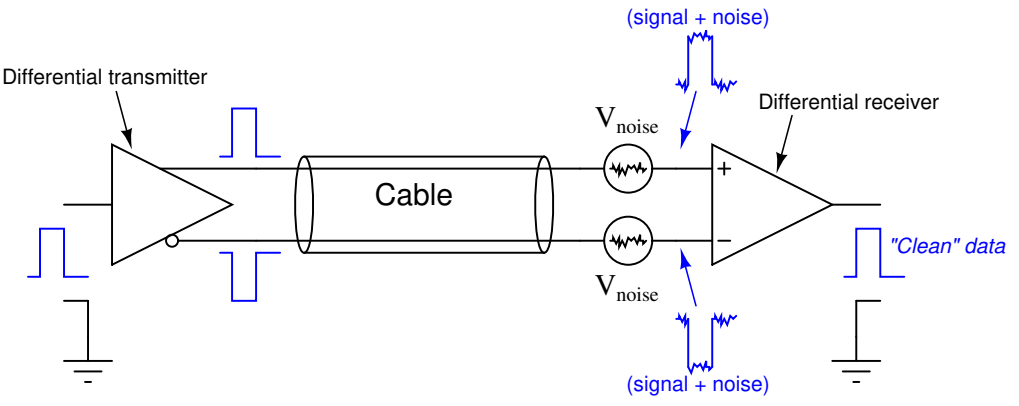
EIA/TIA-232 communication using hardware flow control




Computer
(DTE device)
Computer
(DTE device)
RD
2
TD
3
Gnd
5
RD
2
TD
3
Gnd
5
Null modem cable


Differential transceiver
Differential transceiver
TD
RD
Signal
Signal
RD
TD


(signal + noise)
Single-ended transmitter
Single-ended receiver
V_{noise}
Cable
Corrupted data

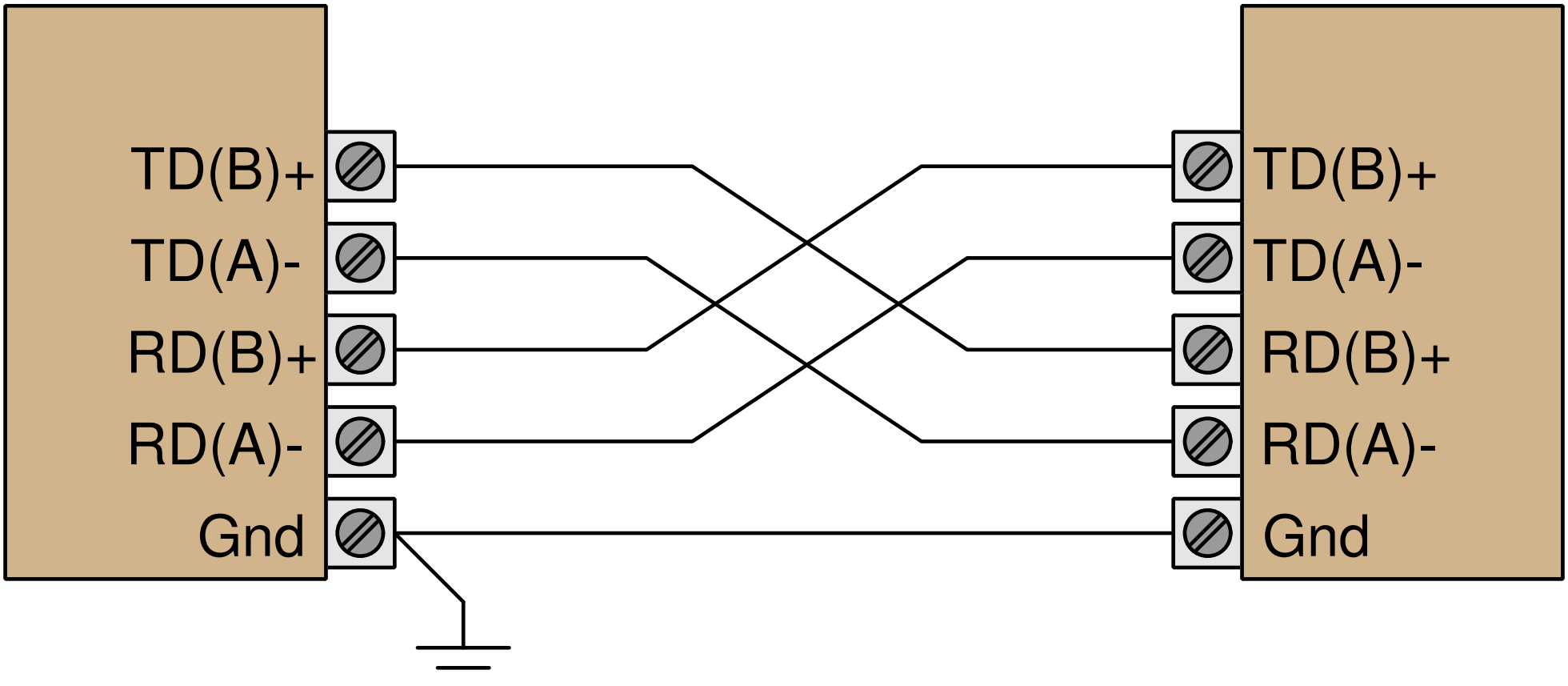

(signal + noise)
Differential transmitter
Differential receiver
V_{noise}
Cable
+
−
"Clean" data
V_{noise}
(signal + noise)

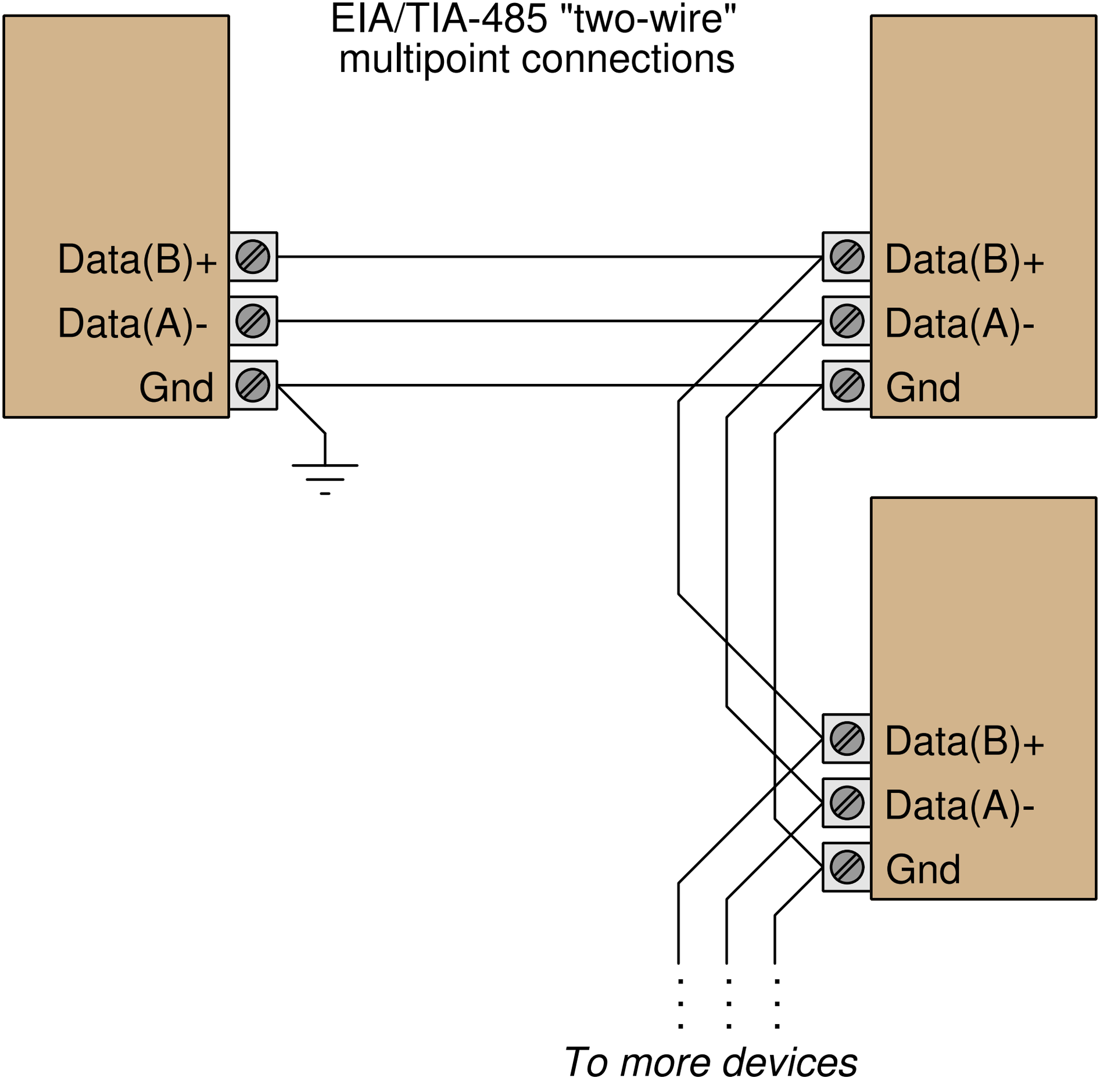
-200

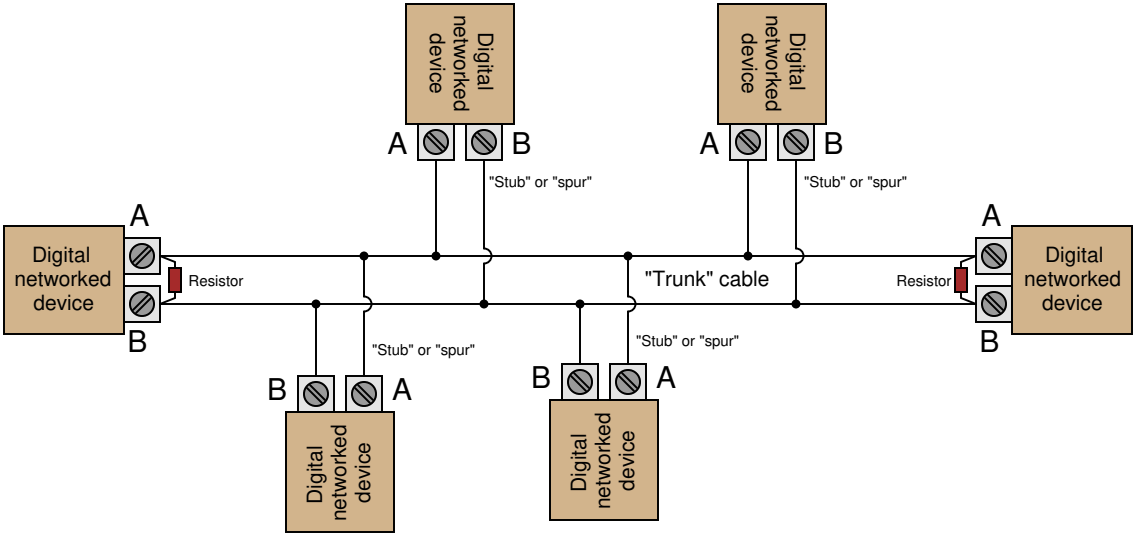
-2

-1.5

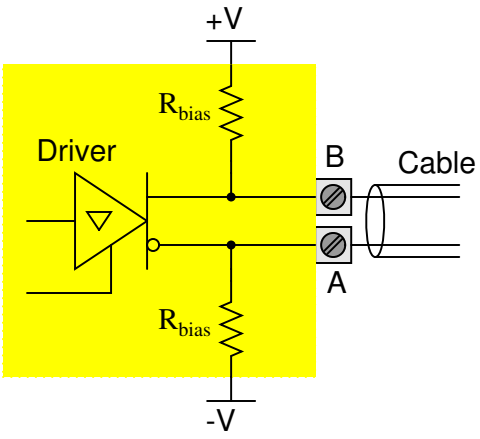
EIA/TIA-485 full-duplex connections



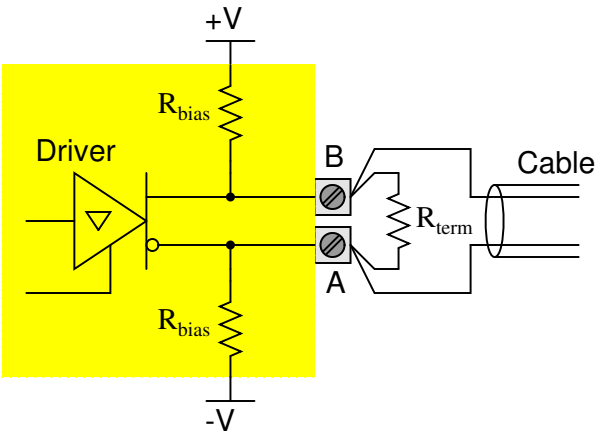

EIA/TIA-485 "two-wire"
multipoint connections
Data(B)+
Data(A)-
Gnd
Data(B)+
Data(A)-
Gnd
Data(B)+
Data(A)-
Gnd
To more devices

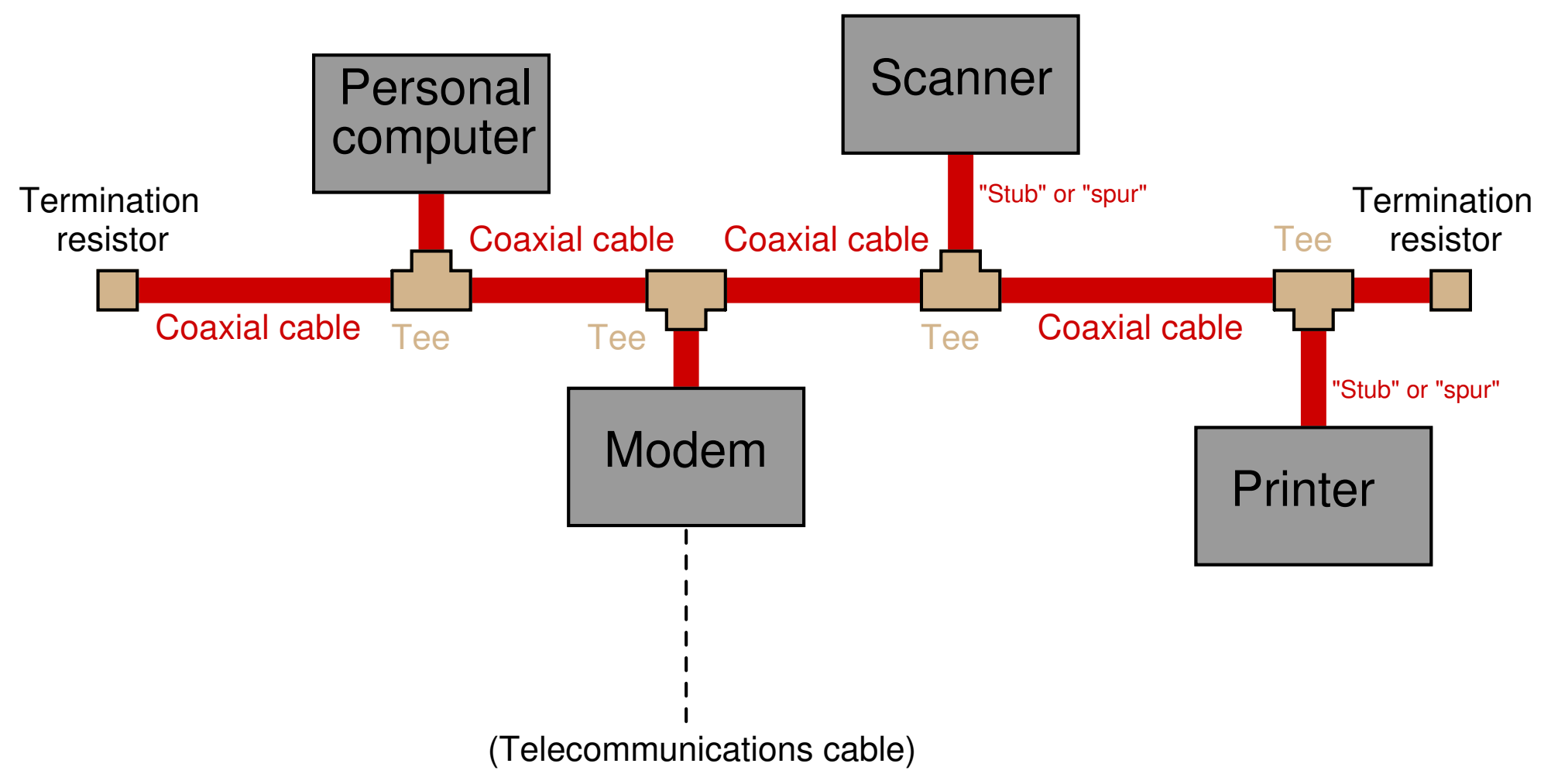

Digital networked device
A
B
Resistor
"Trunk" cable
"Stub" or "spur"
Digital networked device
A
B
"Stub" or "spur"
Digital networked device
A
B
"Stub" or "spur"
Digital networked device
B
A
"Stub" or "spur"
Digital networked device
B
A
Resistor
Digital networked device
A
B

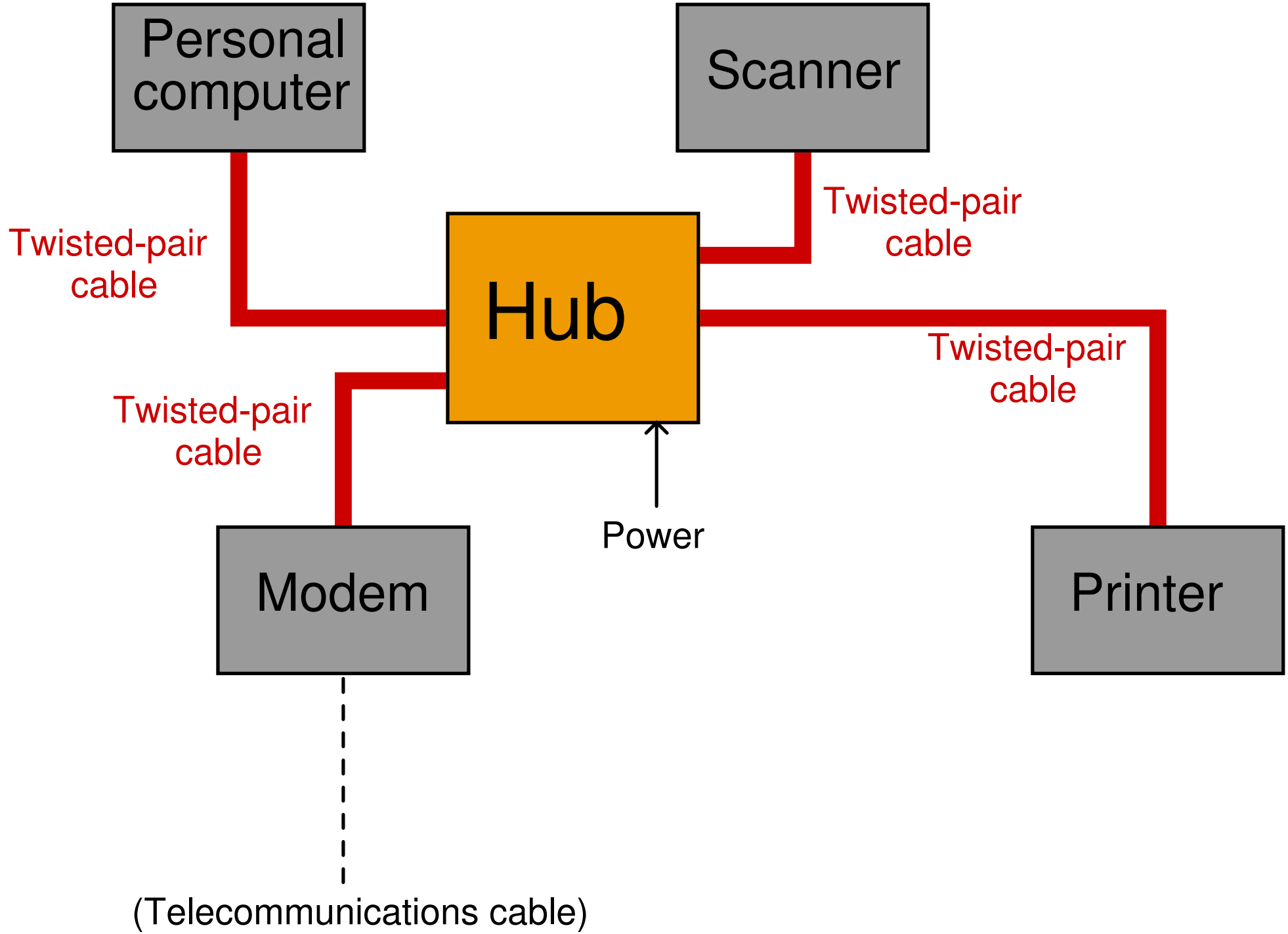
No termination resistor

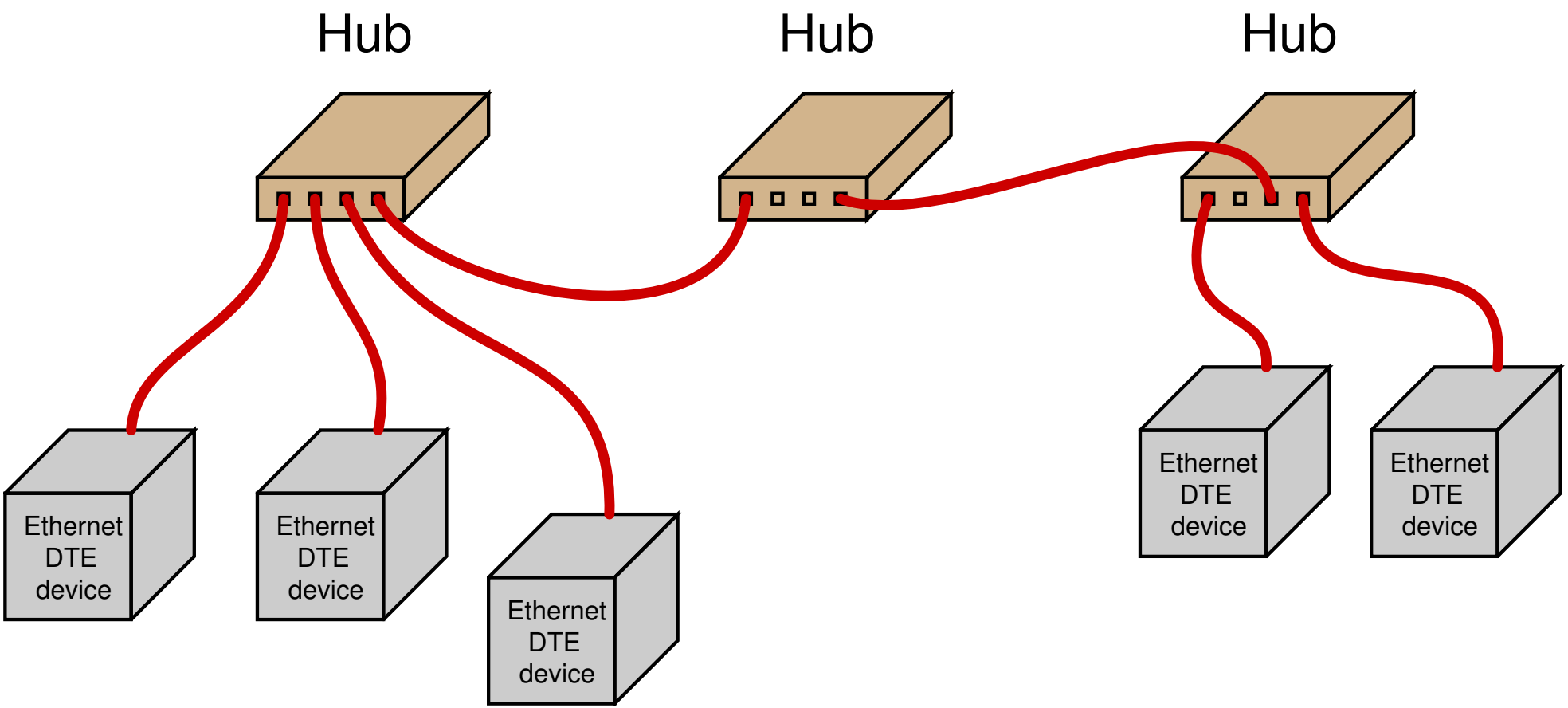


With termination resistor

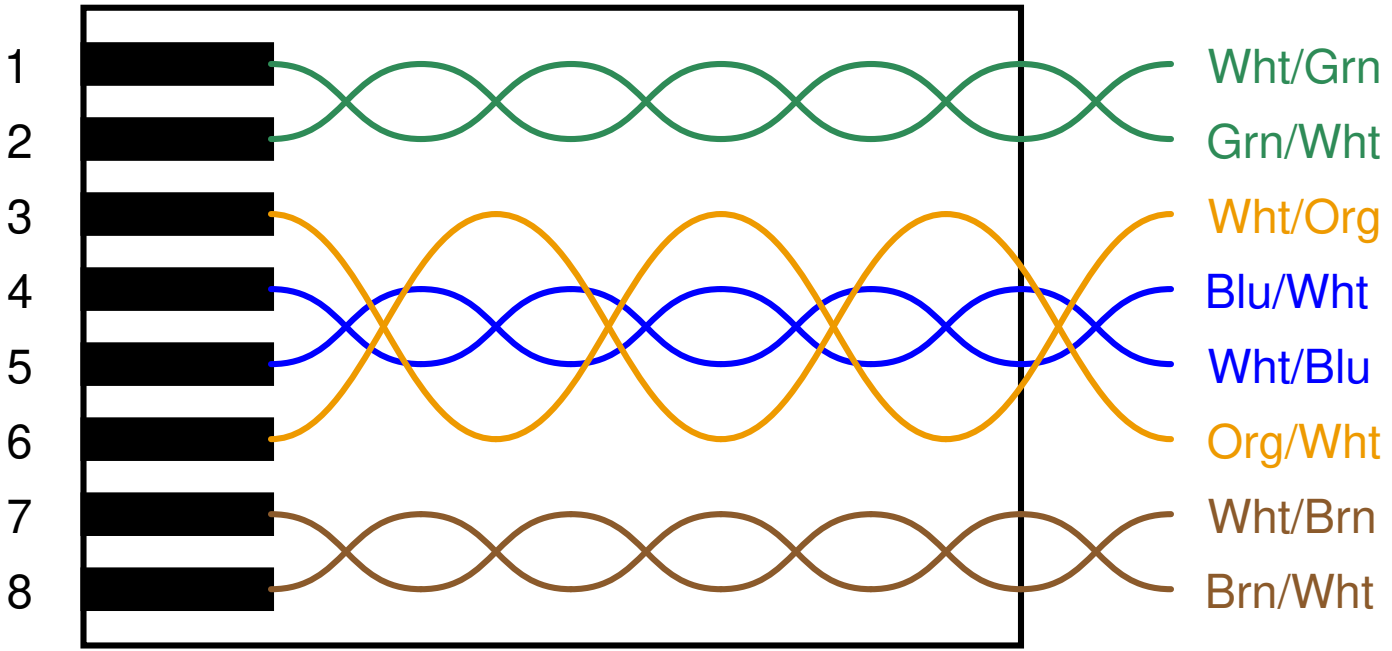



Personal computer
Scanner
Termination resistor
"Stub" or "spur"
Coaxial cable
Coaxial cable
Tee
Termination resistor
Coaxial cable
Tee
Tee
Tee
Coaxial cable
"Stub" or "spur"
Modem
Printer
(Telecommunications cable)


Personal computer
Scanner
Twisted-pair cable
Twisted-pair cable
Hub
Twisted-pair cable
Twisted-pair cable
Power
Modem
Printer
(Telecommunications cable)


Hub
Hub
Hub
Ethernet DTE device
Ethernet DTE device
Ethernet DTE device
Ethernet DTE device
Ethernet DTE device

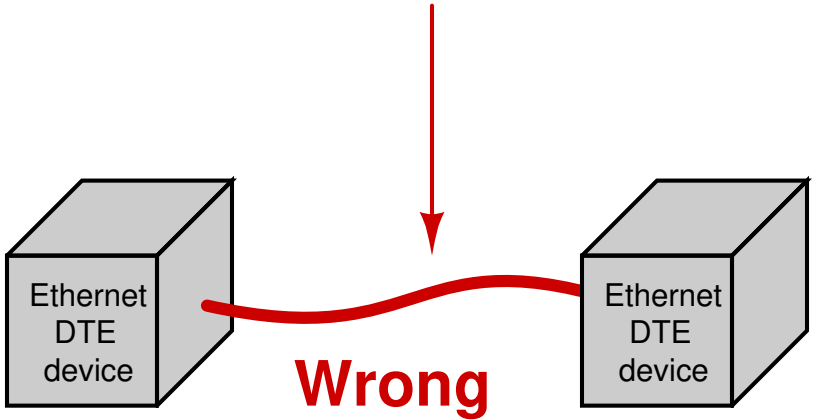
RJ-45 cable connector



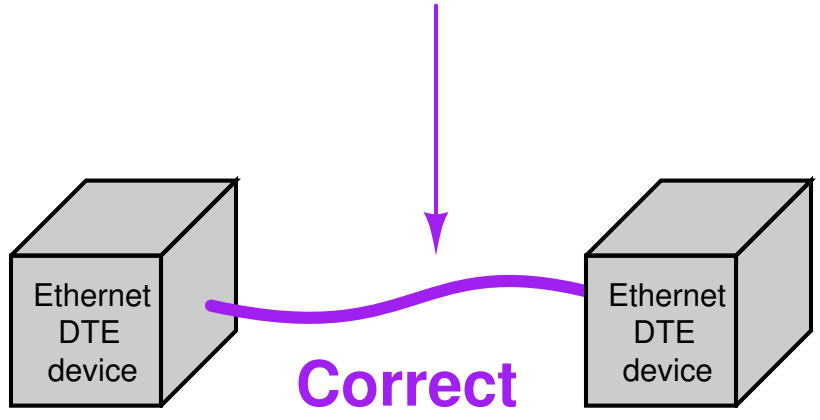
Pin number	Assignment	Abbreviation
1	Transmit Data (+)	TD+
2	Transmit Data (−)	TD−
3	Receive Data (+)	RD+
4	(not used)	
5	(not used)	
6	Receive Data (−)	RD−
7	(not used)	
8	(not used)	

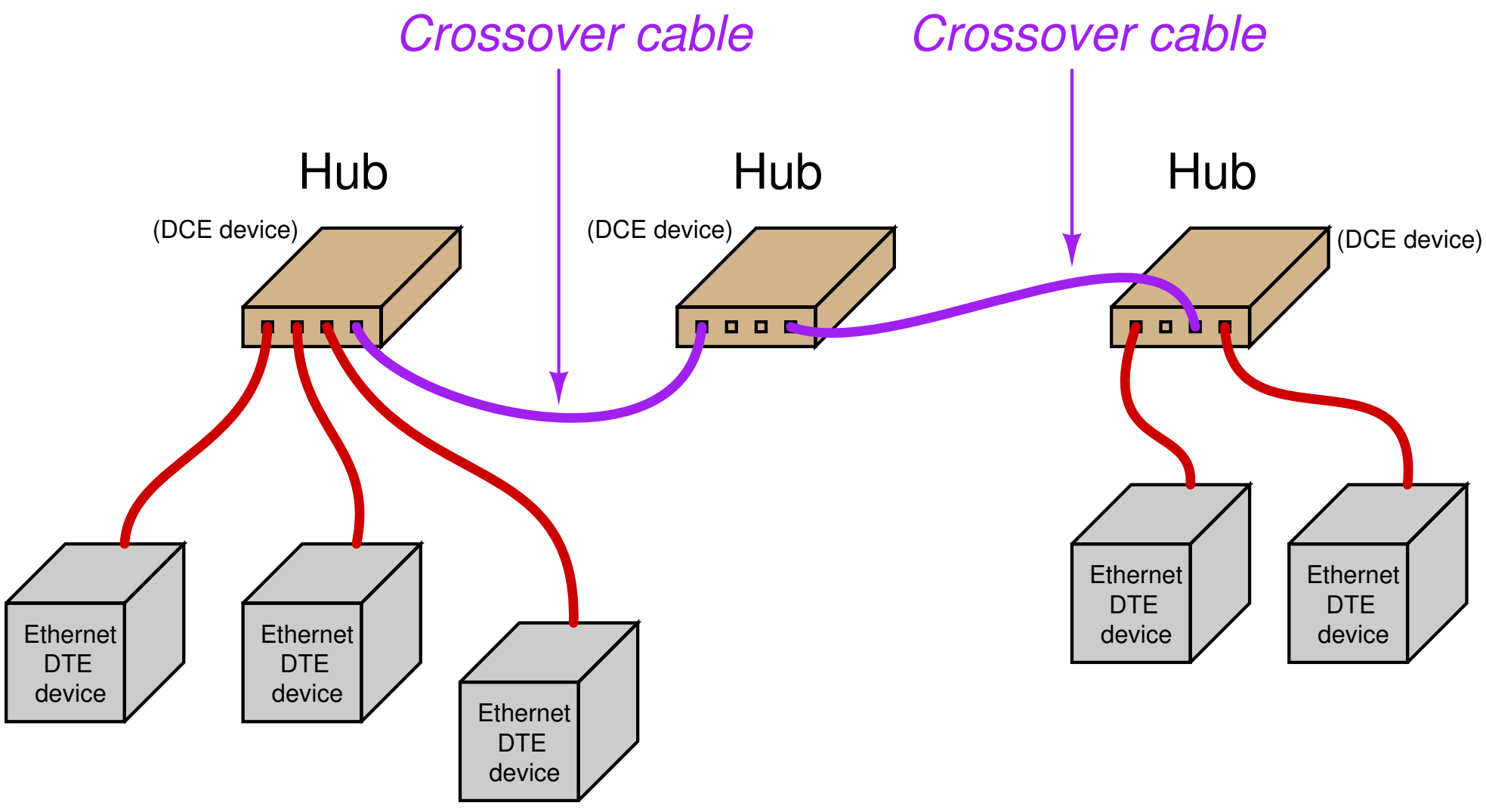
Pin number	Assignment	Abbreviation
1	Pair “A” (+)	BI_DA+
2	Pair “A” (−)	BI_DA−
3	Pair “B” (+)	BI_DB+
4	Pair “C” (+)	BI_DC+
5	Pair “C” (−)	BI_DC−
6	Pair “B” (−)	BI_DB−
7	Pair “D” (+)	BI_DD+
8	Pair “D” (−)	BI_DD−

A regular "straight" Ethernet cable will not work here!

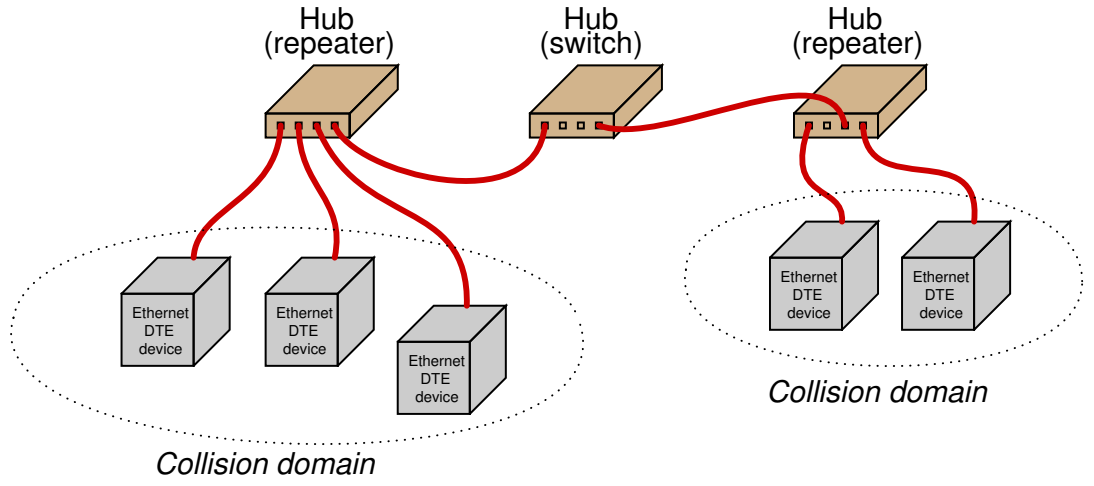


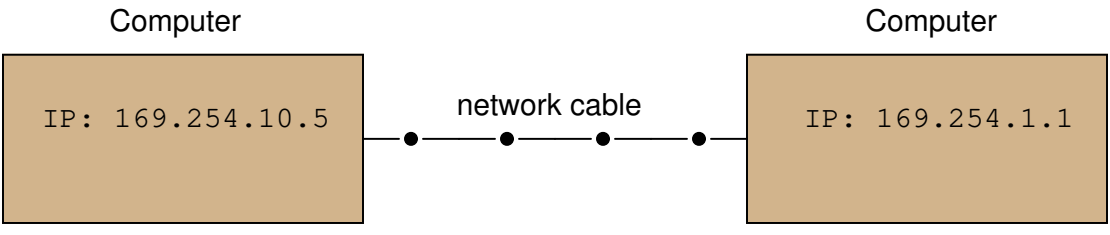
You must use a crossover cable in this application!



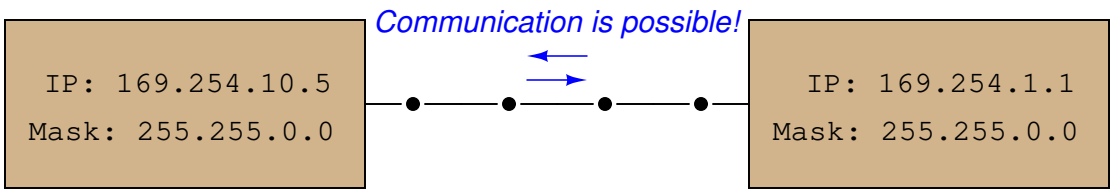

Crossover cable
Crossover cable
Hub
Hub
Hub
(DCE device)
(DCE device)
(DCE device)
Ethernet DTE device
Ethernet DTE device
Ethernet DTE device
Ethernet DTE device
Ethernet DTE device

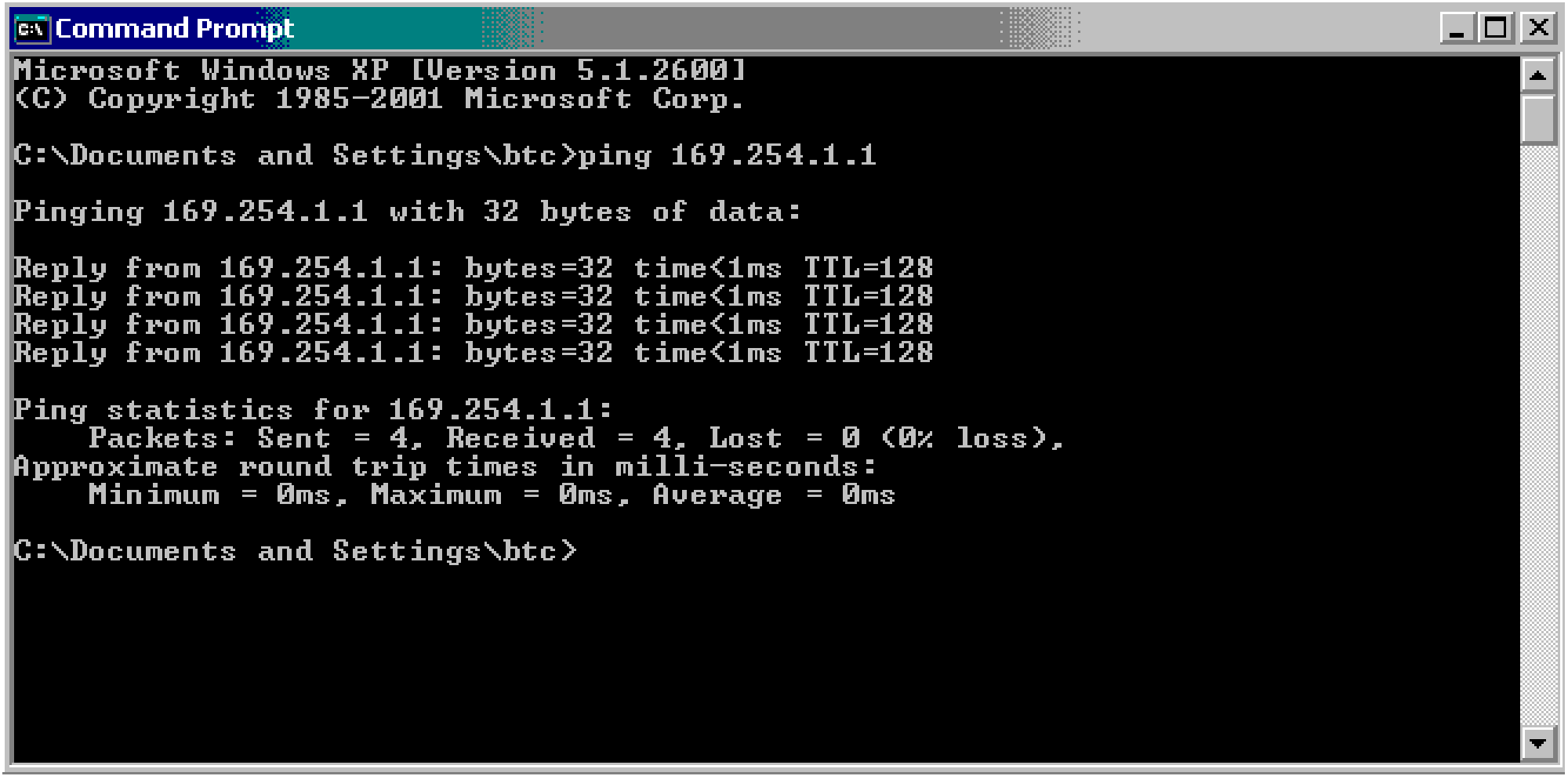

NETGEAR
4 Port 10/100 Ethernet Hub
MODEL EN104TP
NETGEAR HUB EN104TP
Pwr
Col
Link
Rx
Normal / Uplink

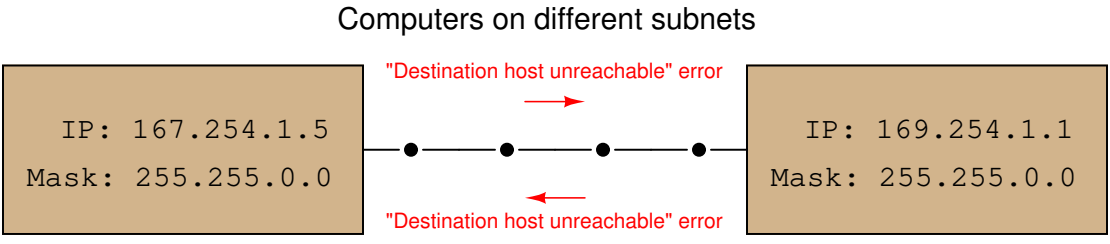

Hub
(repeater)
Hub
(switch)
Hub
(repeater)
Ethernet
DTE
device
Ethernet
DTE
device
Ethernet
DTE
device
Ethernet
DTE
device
Ethernet
DTE
device
Collision domain
Collision domain

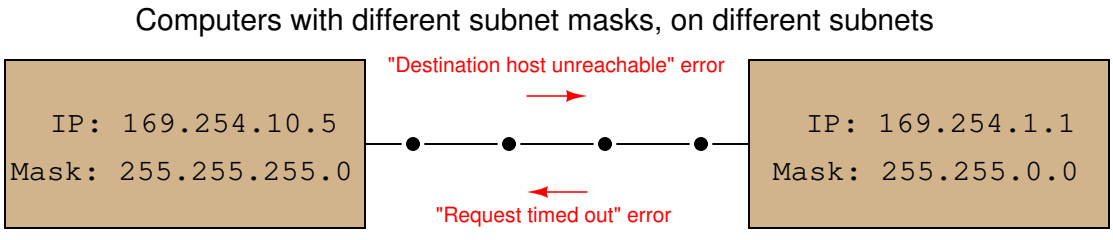

Computer
Computer
IP: 169.254.10.5
network cable
IP: 169.254.1.1

2^{32}


Communication is possible!
IP: 169.254.10.5
Mask: 255.255.0.0
IP: 169.254.1.1
Mask: 255.255.0.0


Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\btc>ping 169.254.1.1
Pinging 169.254.1.1 with 32 bytes of data:
Reply from 169.254.1.1: bytes=32 time<1ms TTL=128
Reply from 169.254.1.1: bytes=32 time<1ms TTL=128
Reply from 169.254.1.1: bytes=32 time<1ms TTL=128
Reply from 169.254.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 169.254.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\btc>


Computers on different subnets
"Destination host unreachable" error
IP: 167.254.1.5
Mask: 255.255.0.0
IP: 169.254.1.1
Mask: 255.255.0.0
"Destination host unreachable" error

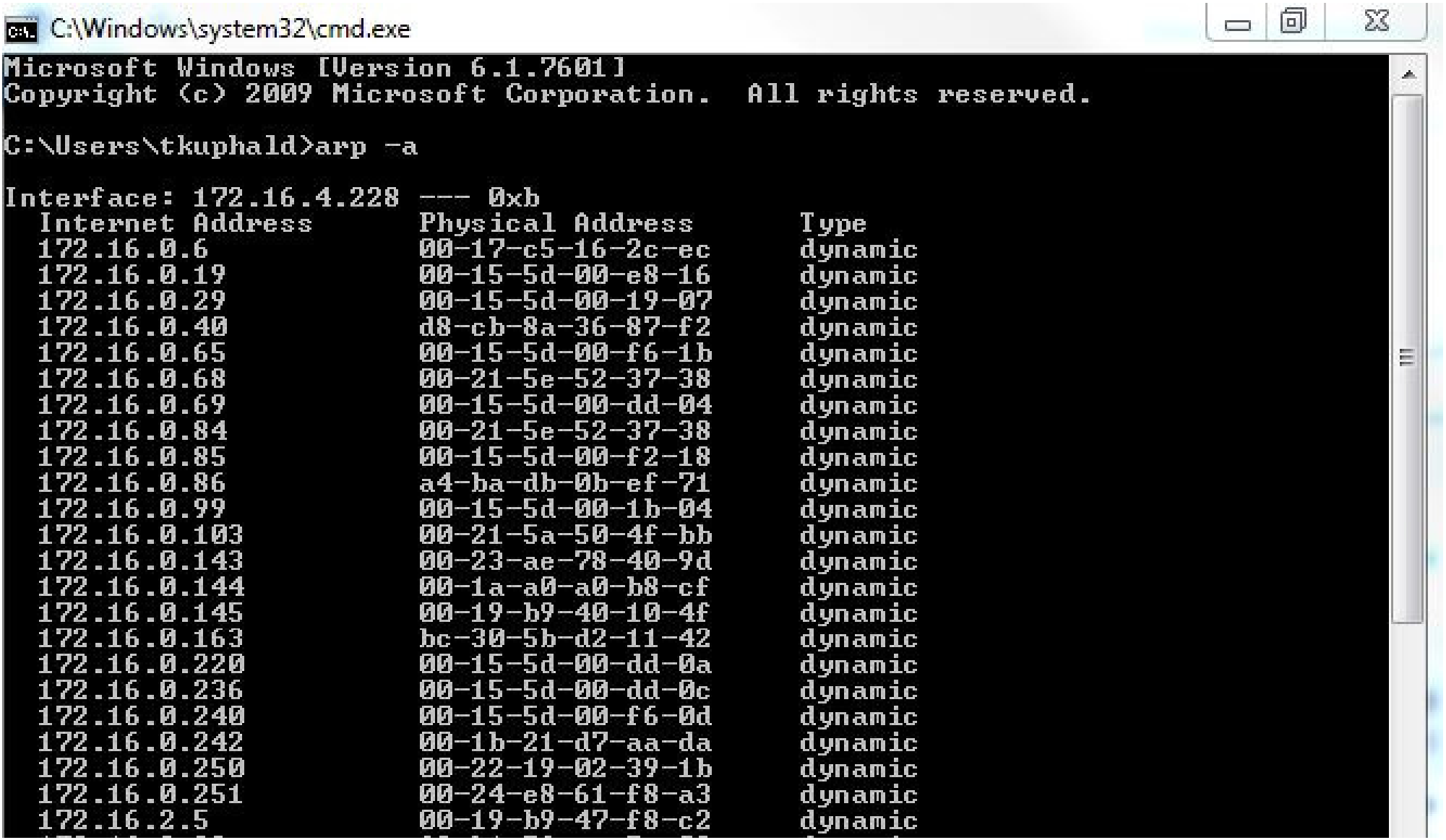

Computers with different subnet masks, on different subnets
"Destination host unreachable" error
IP: 169.254.10.5
Mask: 255.255.255.0
IP: 169.254.1.1
Mask: 255.255.0.0
"Request timed out" error

2^{128}

3.4×10^{38}

5.98×10^{24}

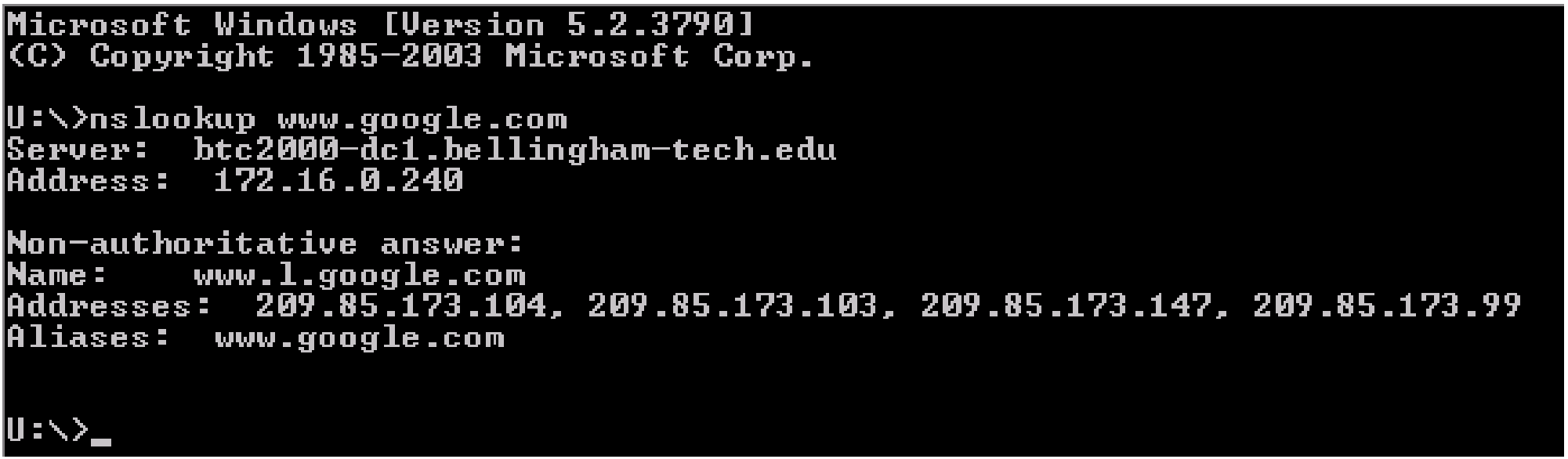
5.98×10^{27}


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\tkuphald>arp -a
Interface: 172.16.4.228 --- 0xb
Internet Address Physical Address Type
172.16.0.6 00-17-c5-16-2c-ec dynamic
172.16.0.19 00-15-5d-00-e8-16 dynamic
172.16.0.29 00-15-5d-00-19-07 dynamic
172.16.0.40 d8-cb-8a-36-87-f2 dynamic
172.16.0.65 00-15-5d-00-f6-1b dynamic
172.16.0.68 00-21-5e-52-37-38 dynamic
172.16.0.69 00-15-5d-00-dd-04 dynamic
172.16.0.84 00-21-5e-52-37-38 dynamic
172.16.0.85 00-15-5d-00-f2-18 dynamic
172.16.0.86 a4-ba-db-0b-ef-71 dynamic
172.16.0.99 00-15-5d-00-1b-04 dynamic
172.16.0.103 00-21-5a-50-4f-bb dynamic
172.16.0.143 00-23-ae-78-40-9d dynamic
172.16.0.144 00-1a-a0-a0-b8-cf dynamic
172.16.0.145 00-19-b9-40-10-4f dynamic
172.16.0.163 bc-30-5b-d2-11-42 dynamic
172.16.0.220 00-15-5d-00-dd-0a dynamic
172.16.0.236 00-15-5d-00-dd-0c dynamic
172.16.0.240 00-15-5d-00-f6-0d dynamic
172.16.0.242 00-1b-21-d7-aa-da dynamic
172.16.0.250 00-22-19-02-39-1b dynamic
172.16.0.251 00-24-e8-61-f8-a3 dynamic
172.16.2.5 00-19-b9-47-f8-c2 dynamic

```
C:\Documents and Settings\btc>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 169.254.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\btc>
```

```
root@Renegade2:/home# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:13:20:08:ec:e6
          inet addr:192.168.0.64  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::213:20ff:fe08:ece6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170901 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107550 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:212178154 (212.1 MB)  TX bytes:14005068 (14.0 MB)

eth1      Link encap:Ethernet  HWaddr 00:0e:35:a2:1b:7f
          inet6 addr: fe80::20e:35ff:fea2:1b7f/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:441 errors:0 dropped:0 overruns:0 frame:0
          TX packets:570 errors:0 dropped:6 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:18 Base address:0x2000 Memory:48005000-48005fff

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:516 (516.0 B)  TX bytes:516 (516.0 B)

root@Renegade2:/home#
```

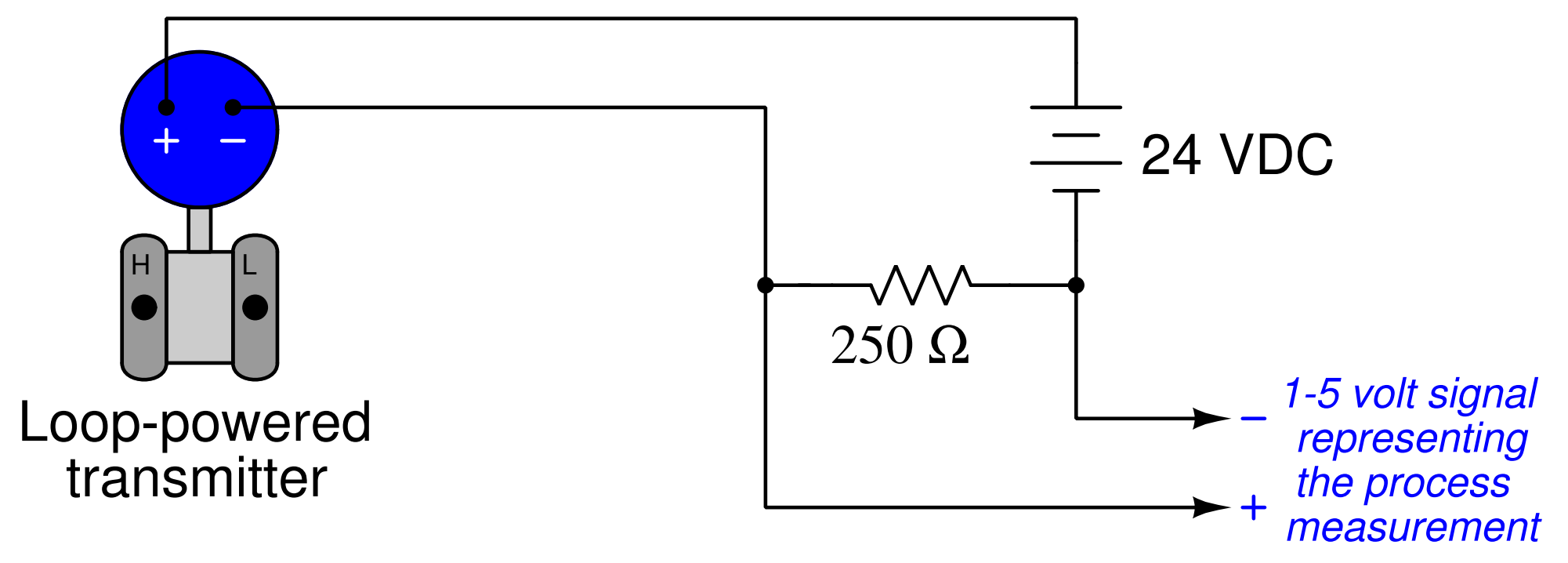
```
root@Renegade2:/home# nslookup www.google.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
www.google.com  canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 74.125.53.103
Name:   www.l.google.com
Address: 74.125.53.147
Name:   www.l.google.com
Address: 74.125.53.99
Name:   www.l.google.com
Address: 74.125.53.104
```

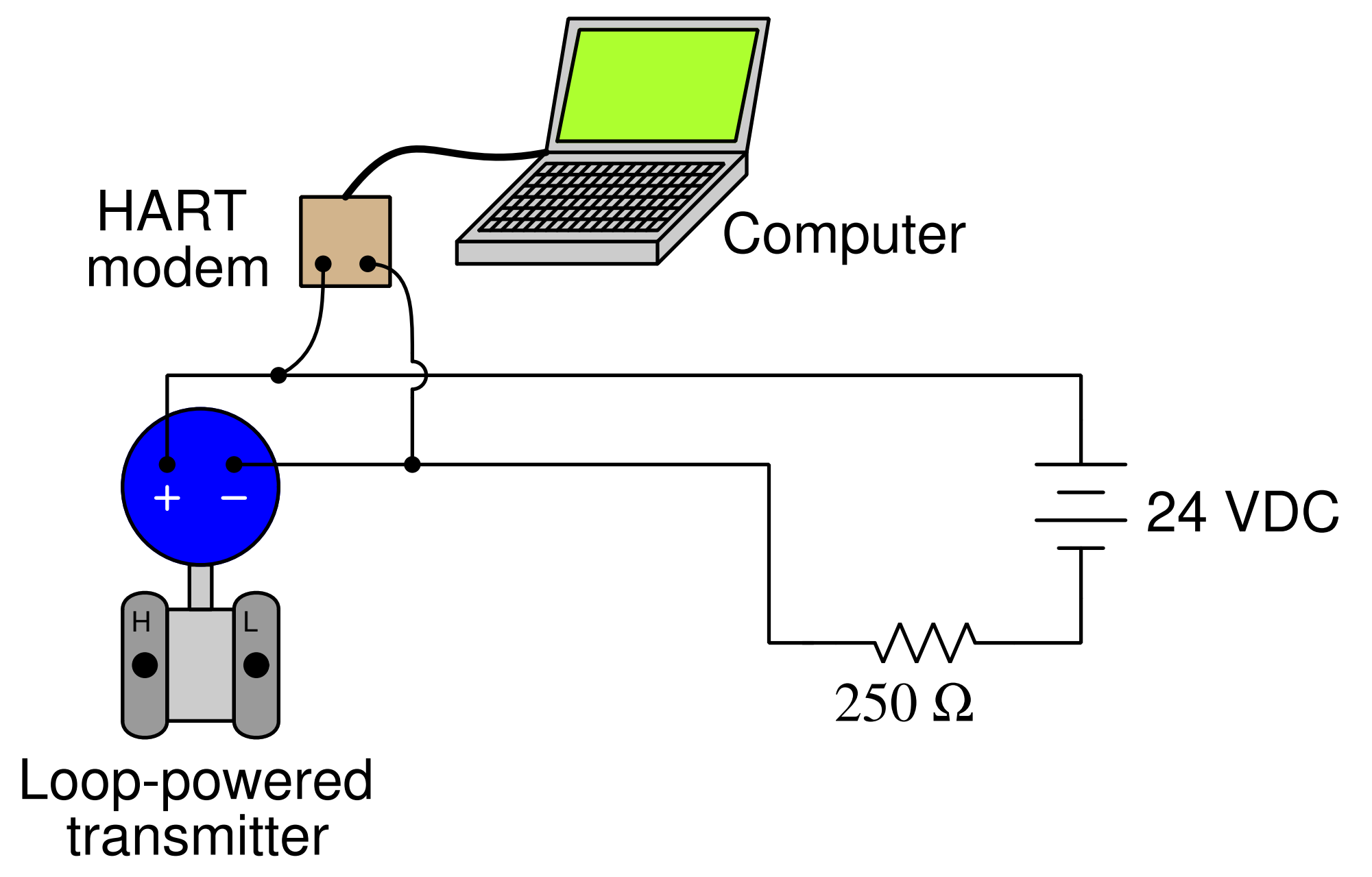

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
U:\>nslookup www.google.com
Server: btc2000-dc1.bellingham-tech.edu
Address: 172.16.0.240
Non-authoritative answer:
Name: www.l.google.com
Addresses: 209.85.173.104, 209.85.173.103, 209.85.173.147, 209.85.173.99
Aliases: www.google.com
U:\>

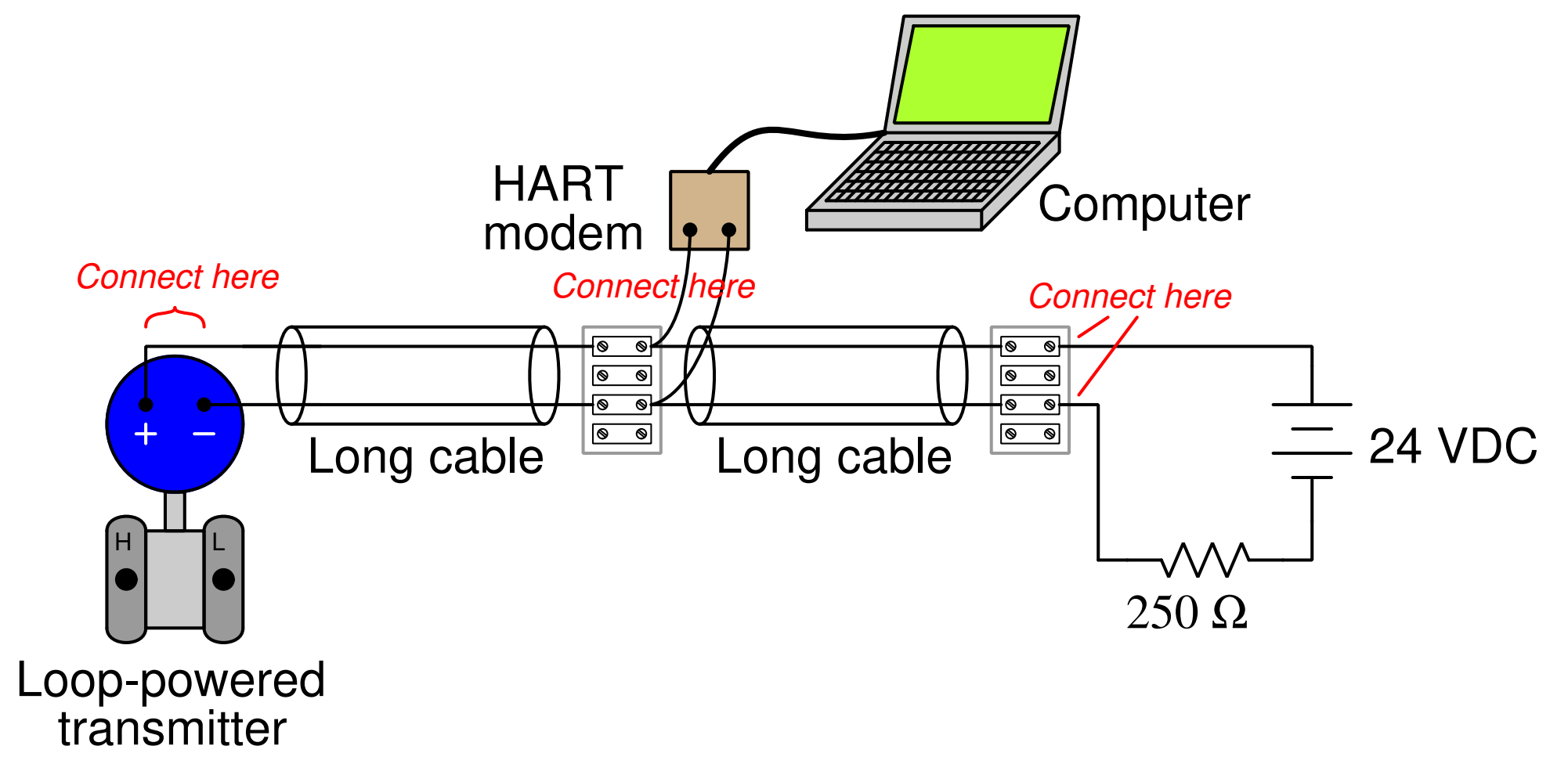
```
root@Renegade2:/home# traceroute www.google.com
traceroute to www.google.com (74.125.53.147), 30 hops max, 40 byte packets
 1  home (192.168.0.1)  4.763 ms  4.803 ms  4.784 ms
 2  tukw-dsl-gw22-214.tukw.qwest.net (63.231.10.214)  57.927 ms  59.993 ms  61.916 ms
 3  tukw-agw1.inet.qwest.net (71.217.184.169)  63.924 ms  65.905 ms  67.882 ms
 4  sea-core-01.inet.qwest.net (67.14.1.194)  71.775 ms  71.784 ms  73.609 ms
 5  sea-brdr-01.inet.qwest.net (205.171.26.54)  75.642 ms  77.442 ms  79.421 ms
 6  63.146.26.198 (63.146.26.198)  81.438 ms  67.052 ms  68.856 ms
 7  sl-gw20-sea-0-0-0.sprintlink.net (144.232.6.8)  70.633 ms  56.617 ms  60.219 ms
 8  sl-googl13-199181-0.sprintlink.net (144.224.13.138)  62.133 ms  64.301 ms  66.162
 9  209.85.249.32 (209.85.249.32)  68.140 ms 209.85.249.34 (209.85.249.34)  70.028 ms
10  216.239.46.204 (216.239.46.204)  79.865 ms  81.739 ms  85.587 ms
11  64.233.174.121 (64.233.174.121)  249.193 ms 64.233.174.129 (64.233.174.129)  113.
12  72.14.232.70 (72.14.232.70)  93.458 ms 72.14.232.10 (72.14.232.10)  99.574 ms 72.
13  72.14.232.6 (72.14.232.6)  68.876 ms 72.14.232.2 (72.14.232.2)  70.251 ms pw-in-f
root@Renegade2:/home#
```

```
U:\>tracert www.google.com

Tracing route to www.l.google.com [209.85.173.99]
over a maximum of 30 hops:

  1  4294964928 ms  4294964927 ms  4294964927 ms  134.39.250.1
  2  4294964927 ms  4294964927 ms  4294964927 ms  bellingham-2691.ctc.edu [192.6
4.1.105]
  3  4294964931 ms  4294964931 ms  4294964930 ms  ge-0-1-0--941.seawescar1.infra
.wa-k20.net [68.179.207.210]
  4  4294964931 ms  4294964931 ms  4294964930 ms  ge-3-0-3--0.seawescore1.infra.
wa-k20.net [68.179.203.26]
  5  4294964931 ms  4294964931 ms  4294964931 ms  ge-2-2-0--311.iccr-sttlwa01-02
.infra.pnw-gigapop.net [209.124.188.182]
  6  4294964931 ms  4294964930 ms  4294964931 ms  pnwgp-cust.tr01-sttlwa01.trans
itrail.net [137.164.131.186]
  7  4294964931 ms  4294964931 ms  4294964931 ms  te4-3--301.tr01-sttlwa01.trans
itrail.net [137.164.131.185]
  8  4294964931 ms  4294964931 ms  4294964931 ms  137.164.130.158
  9  4294964931 ms  4294964931 ms  4294964931 ms  209.85.249.32
 10  4294964935 ms  4294964938 ms  4294964938 ms  216.239.46.208
 11  4294964936 ms  4294964937 ms  4294964937 ms  64.233.174.127
 12  4294964937 ms  4294964936 ms  4294964937 ms  209.85.251.149
 13  4294964943 ms  4294964937 ms  4294964941 ms  209.85.251.145
 14  4294964941 ms  4294964944 ms  4294964937 ms  mh-in-f99.google.com [209.85.1
73.99]

Trace complete.

U:\>_
```

```
C:\Documents and Settings\btc>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5152         0.0.0.0:0              LISTENING
  TCP    169.254.1.2:23         169.254.1.1:1116       ESTABLISHED
  TCP    169.254.1.2:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1062           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:7725           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1063         *:*
  UDP    127.0.0.1:1066         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    169.254.1.2:123        *:*
  UDP    169.254.1.2:137        *:*
  UDP    169.254.1.2:138        *:*
  UDP    169.254.1.2:1900       *:*

C:\Documents and Settings\btc>
```

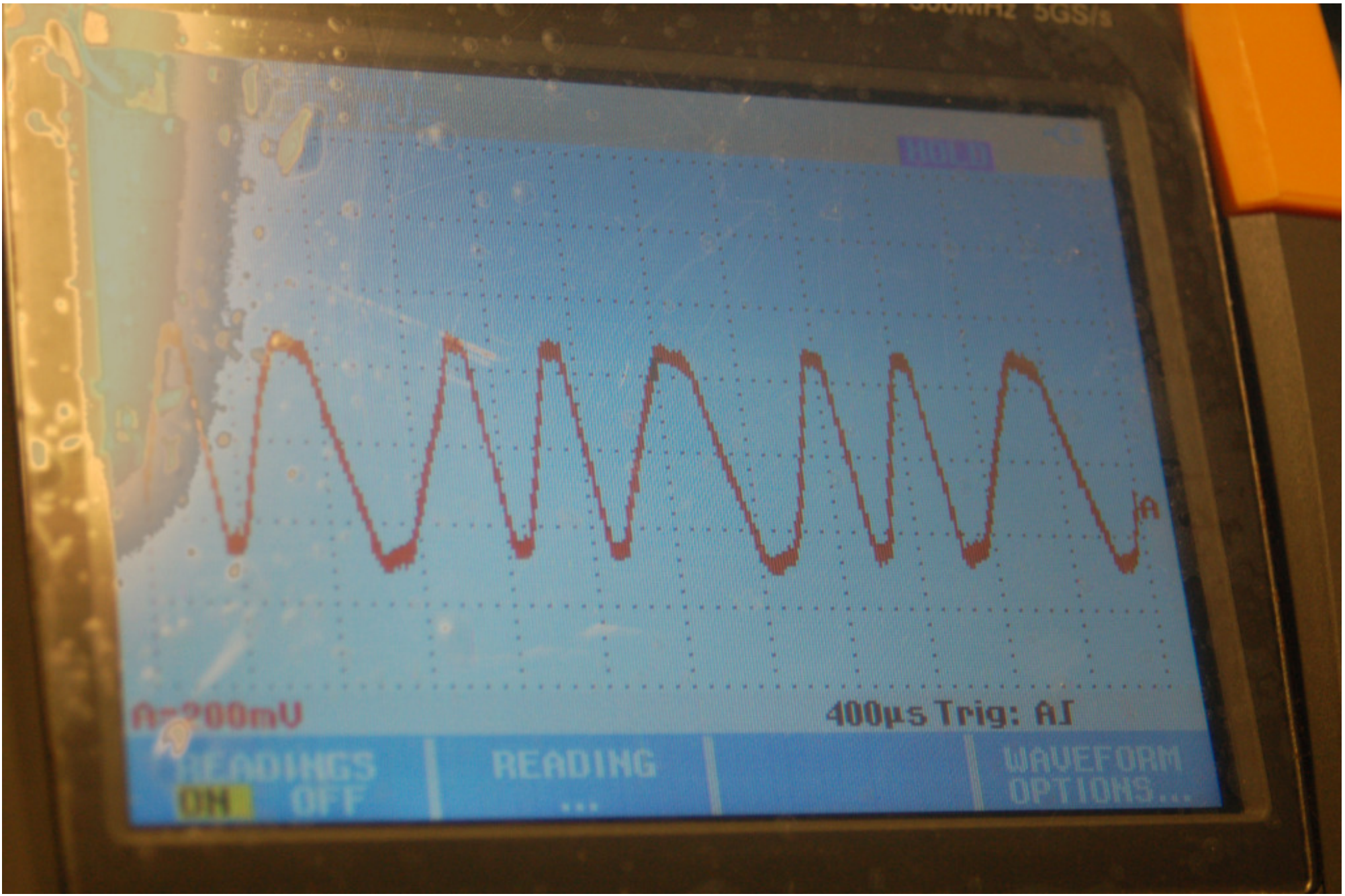

+
−
H
L
Loop-powered transmitter
24 VDC
250 Ω
−
1-5 volt signal representing the process measurement
+

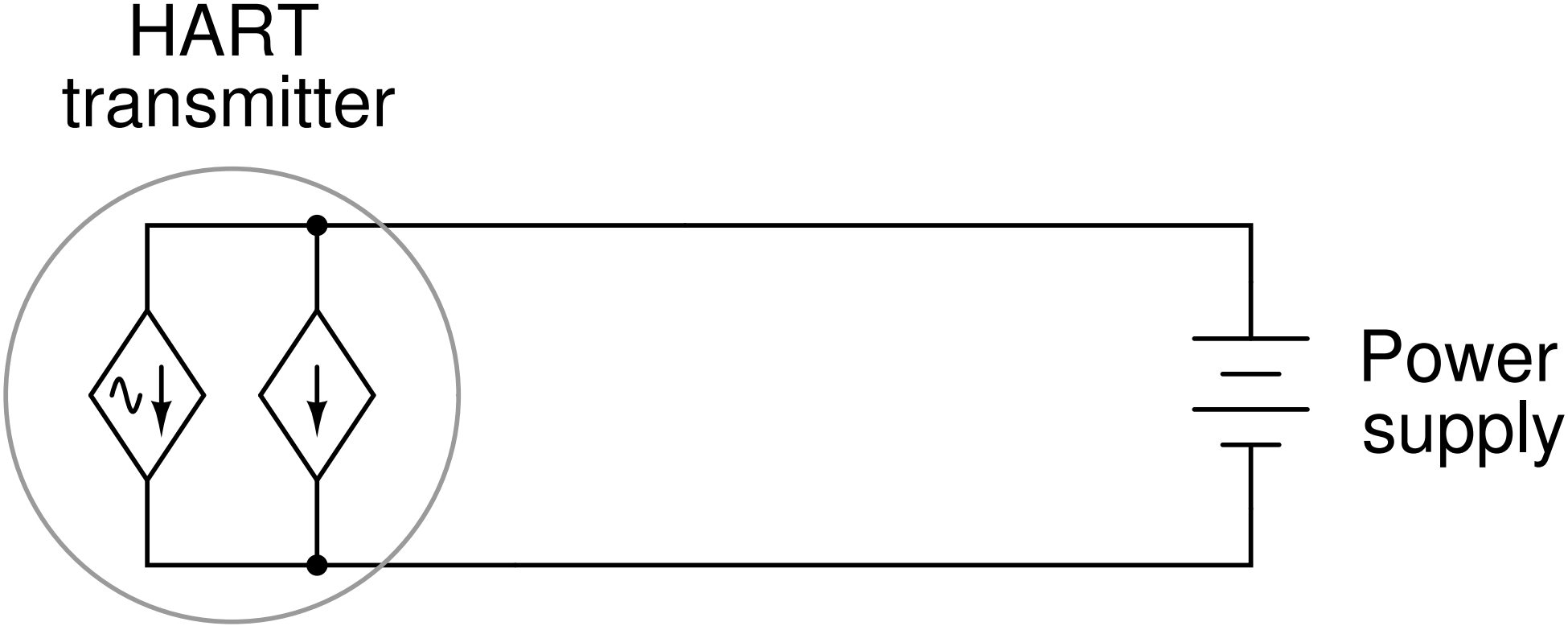

HART
modem
Computer
+
−
H
L
24 VDC
250 Ω
Loop-powered
transmitter

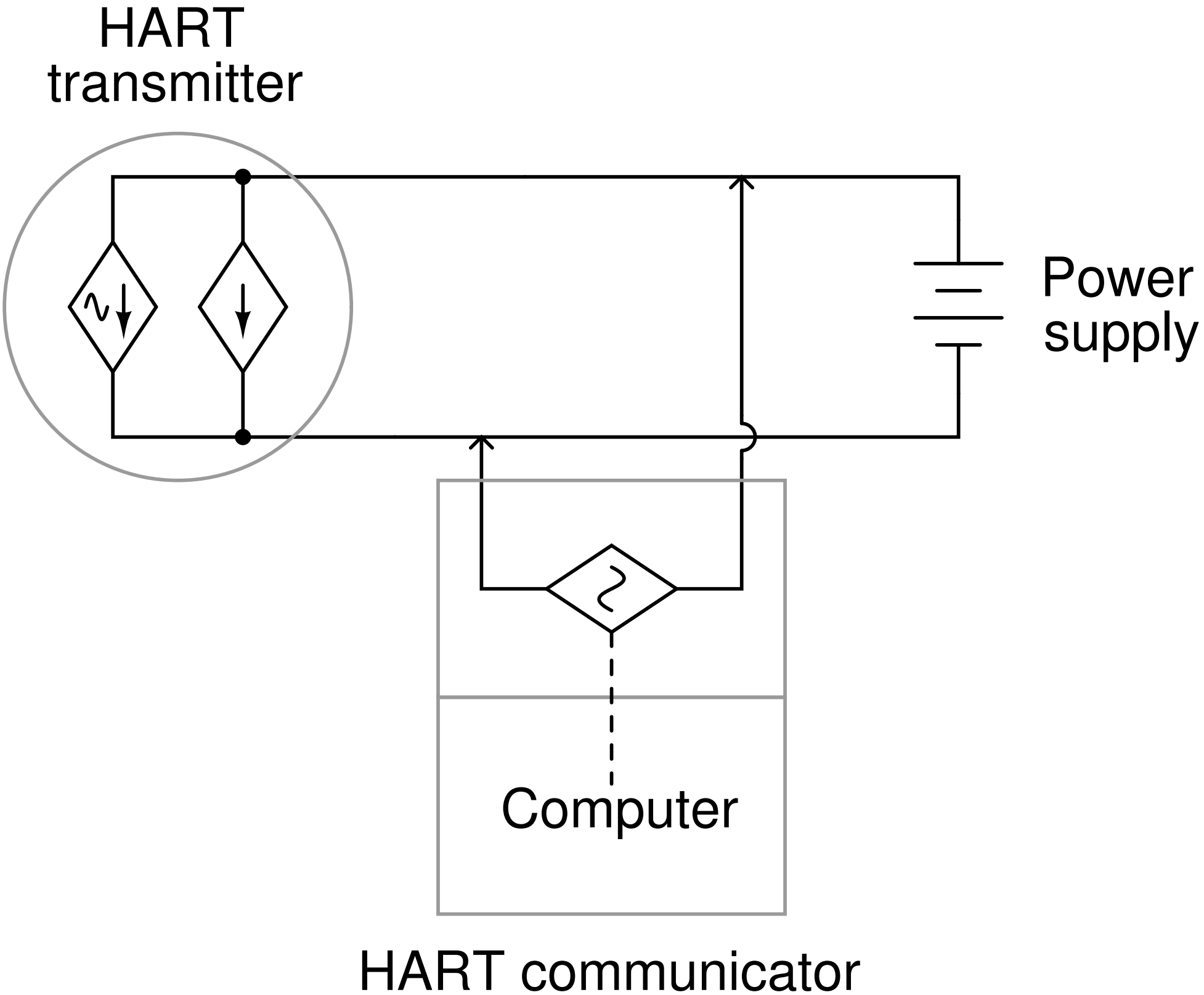

HART
modem
Computer
Connect here
Connect here
Connect here
+
−
Long cable
Long cable
24 VDC
H
L
250 Ω
Loop-powered
transmitter

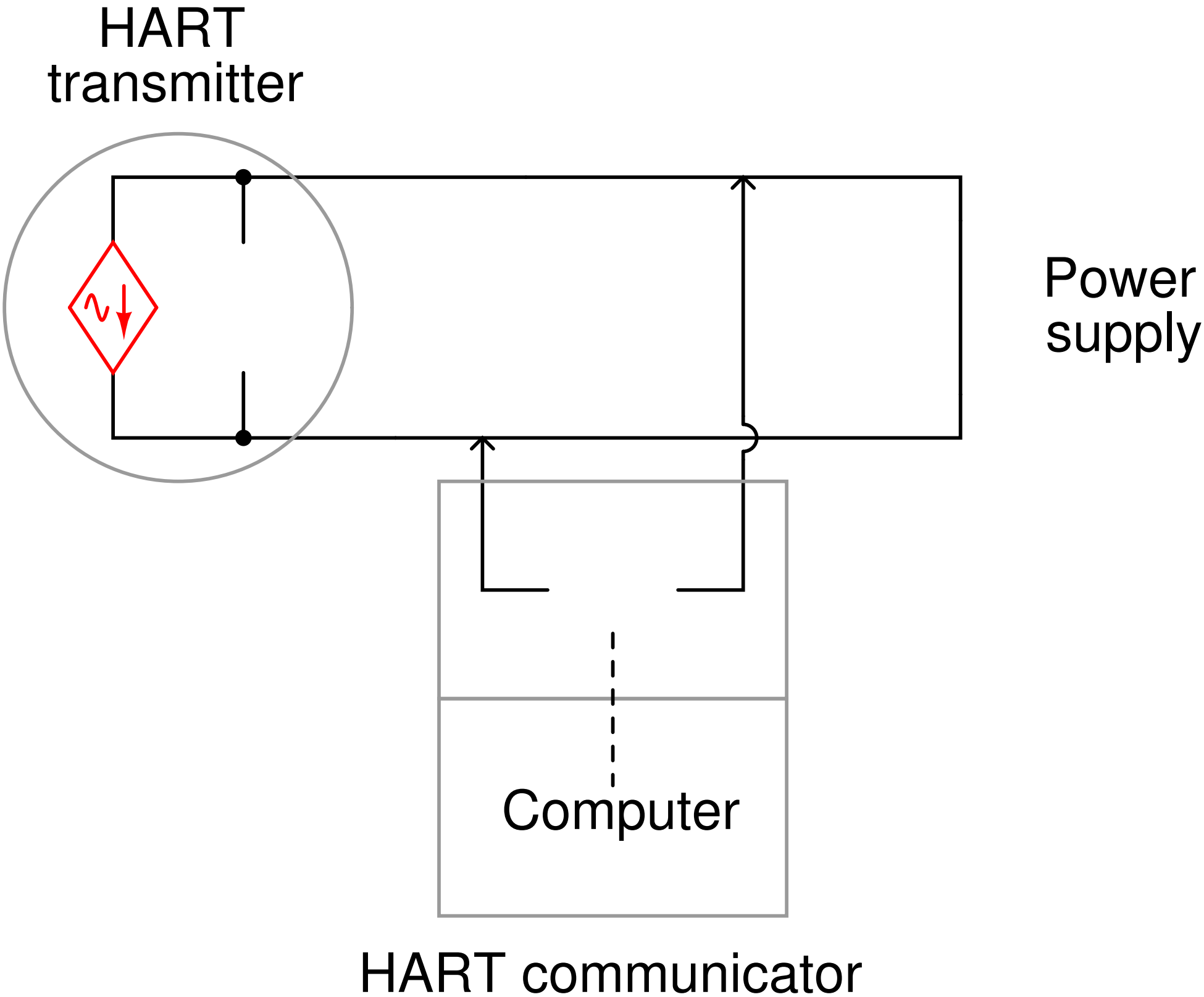

Rosemount®
F1
F2
F3
F4
Rosemount HART™ Communications
SMART FAMILY® INTERFACE
268
ON/OFF
PROCESS VARIABLE
REVIEW
HELP
RESTART
PREVIOUS FUNCTION
A B C 7
D E F 8
G H I 9
J K L 4
M N O 5
P Q R 6
S T U 1
V W X 2
Y Z # 3
@ % & 0
SPACE .
+ / * -
SHIFT
SHIFT
SHIFT
ALPHABET/SYMBOLS

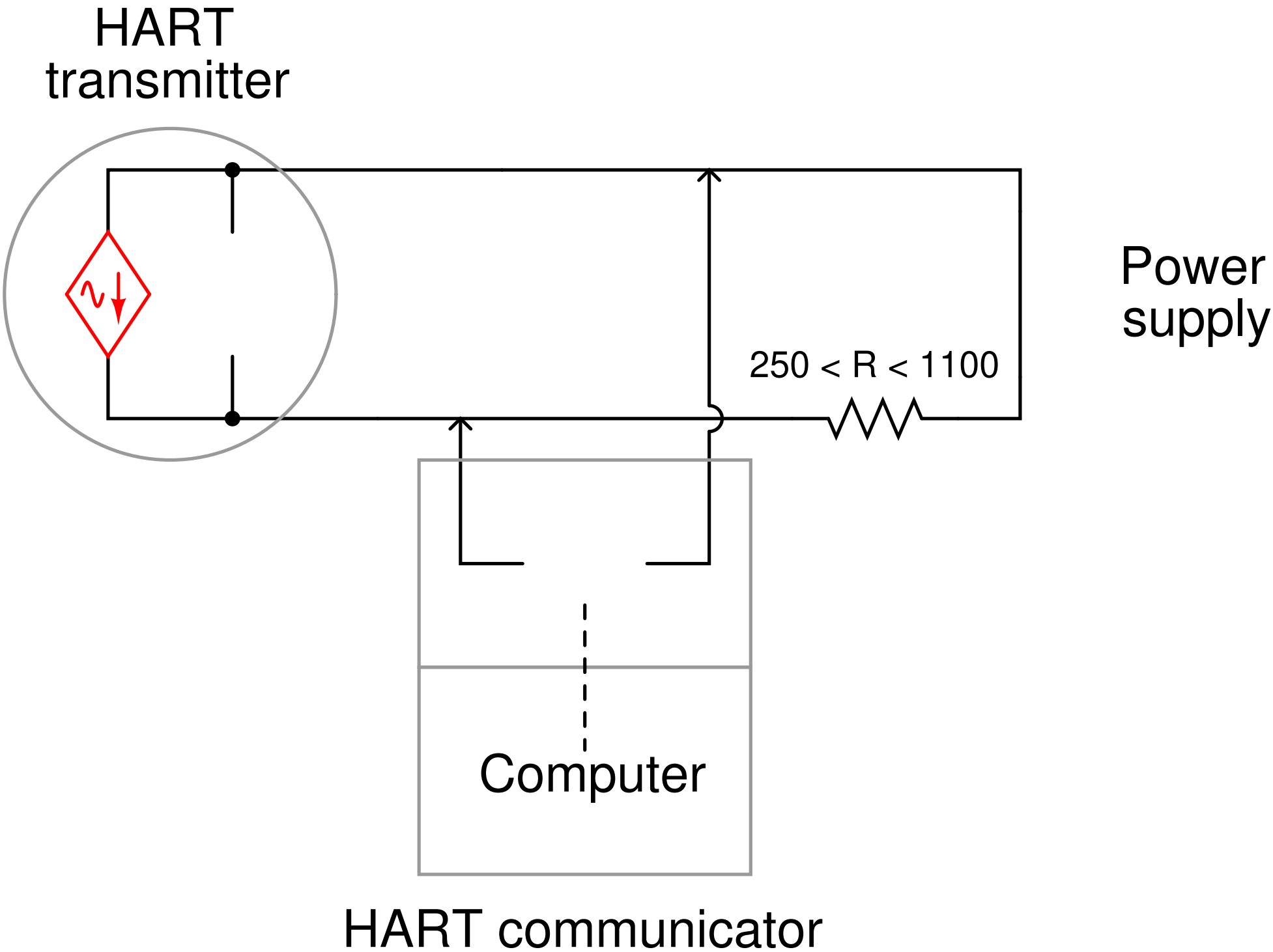

Fieldbus
HART
Fn
% & 1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PQRS 7
TUV 8
WXYZ 9
375
FIELD COMMUNICATOR

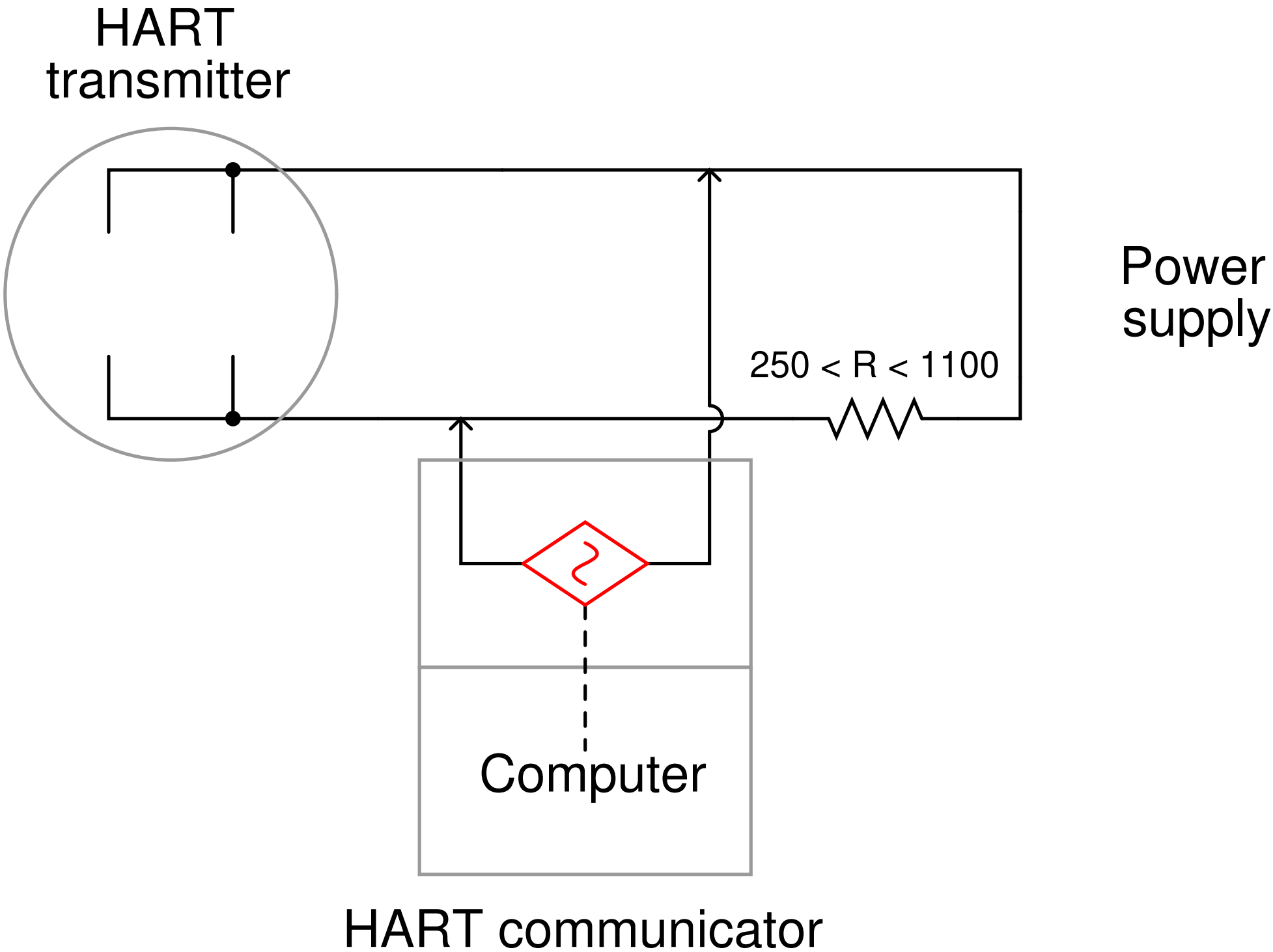

A:200mV
400µs Trig: AI
READINGS
ON OFF
READING
...
WAVEFORM
OPTIONS...

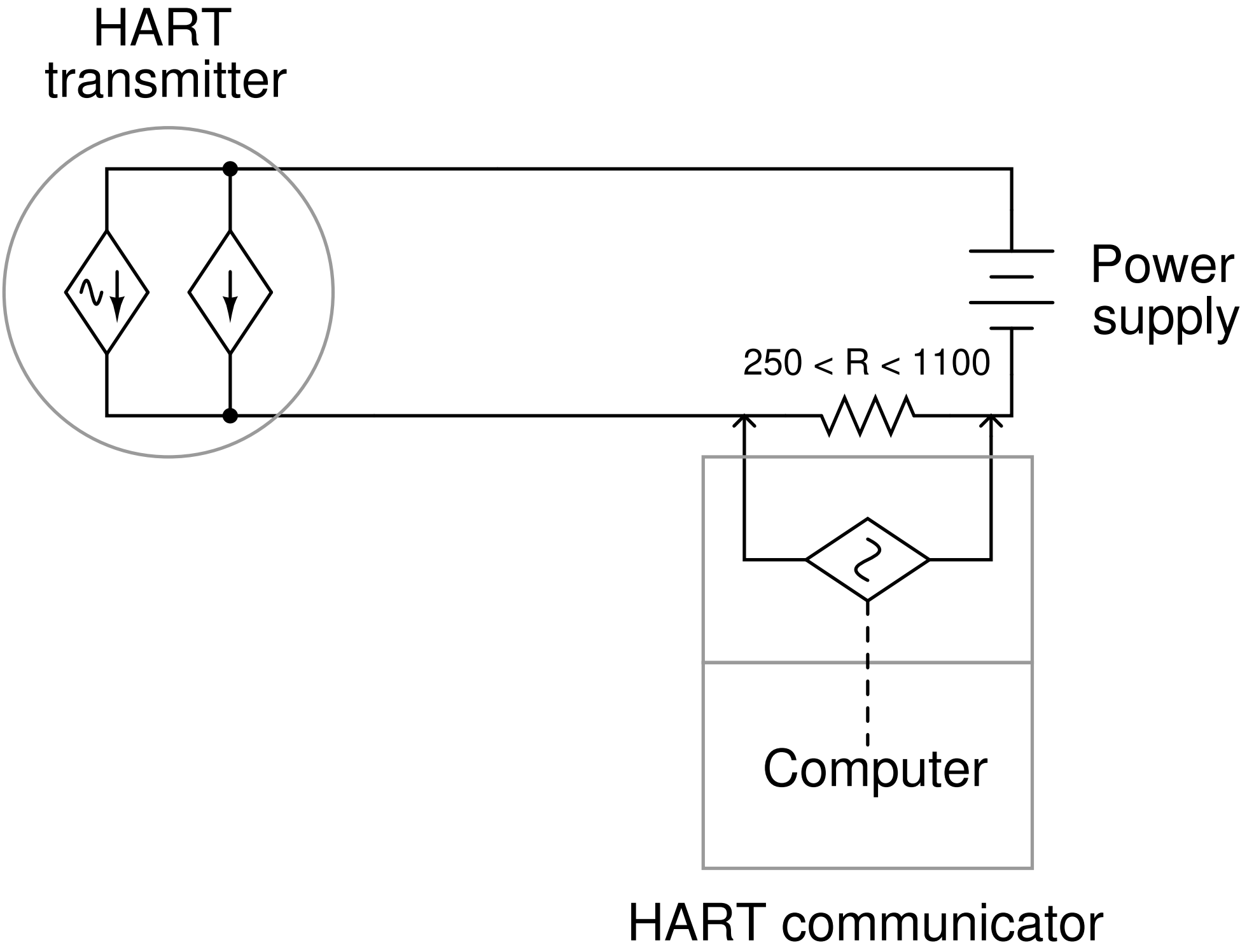

HART
transmitter
Power
supply

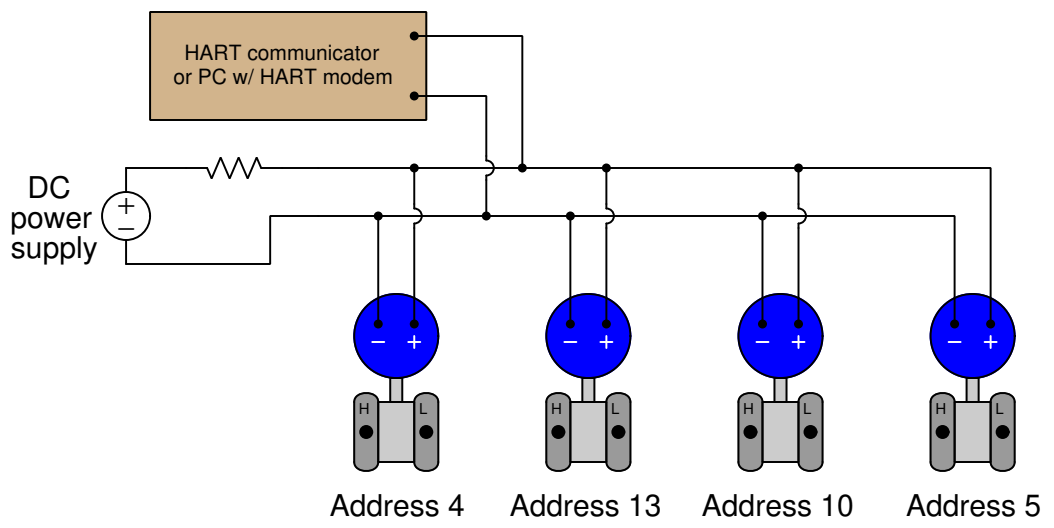

HART
transmitter
Power
supply
Computer
HART communicator

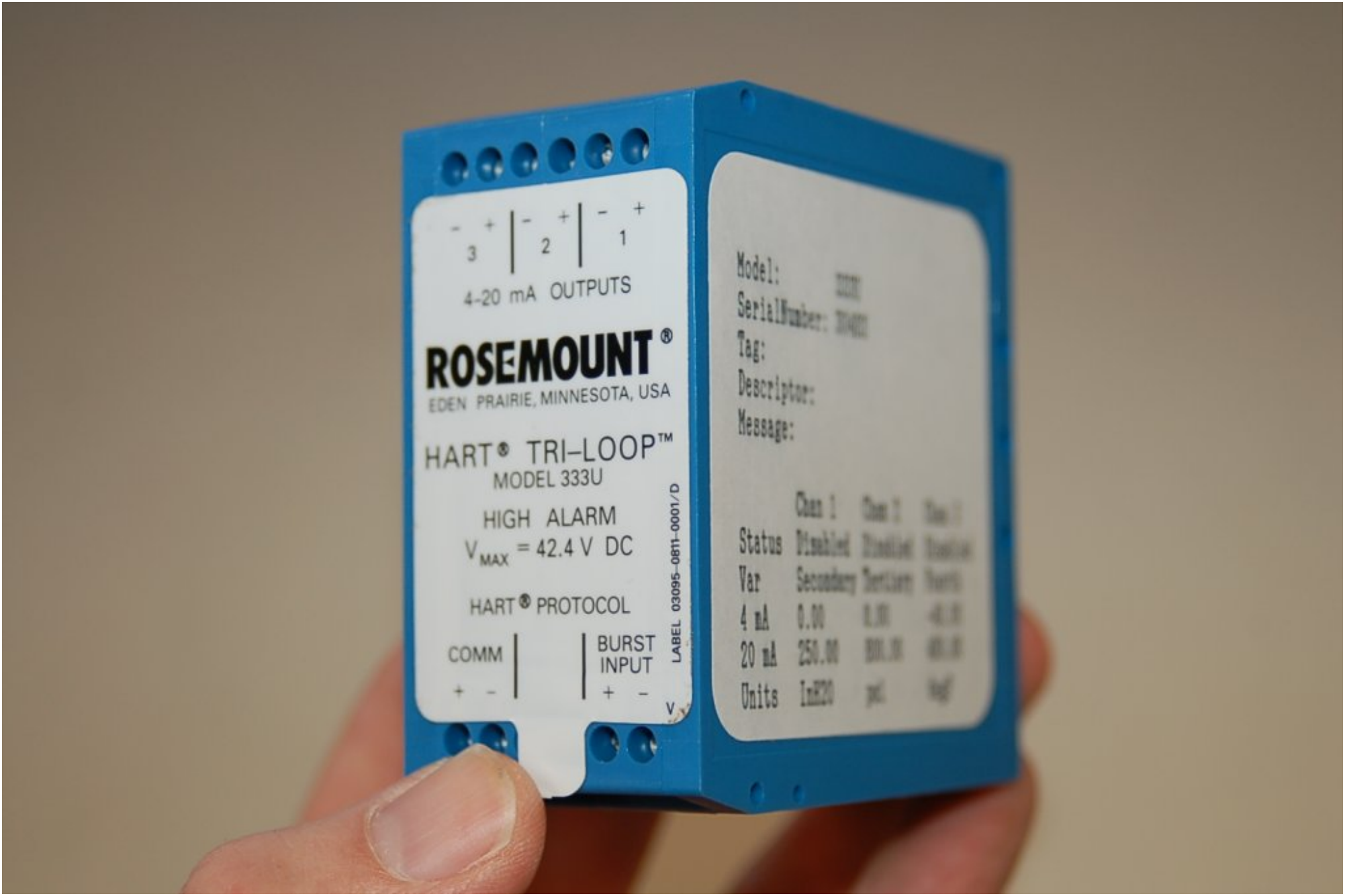

HART
transmitter
Power
supply
Computer
HART communicator

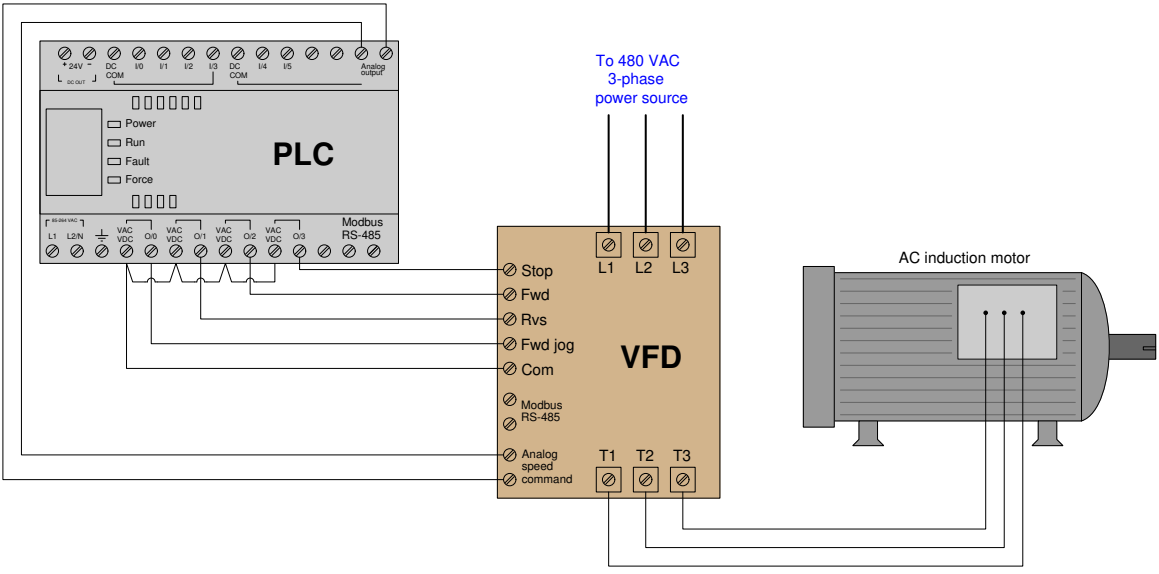

HART
transmitter
Power
supply
250 < R < 1100
Computer
HART communicator

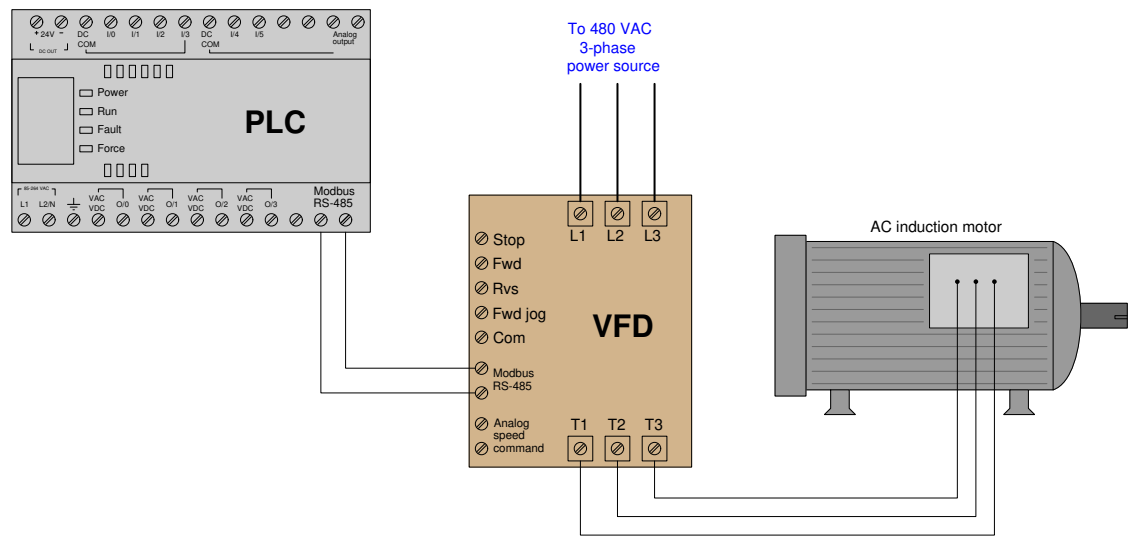

HART
transmitter
Power
supply
250 < R < 1100
Computer
HART communicator

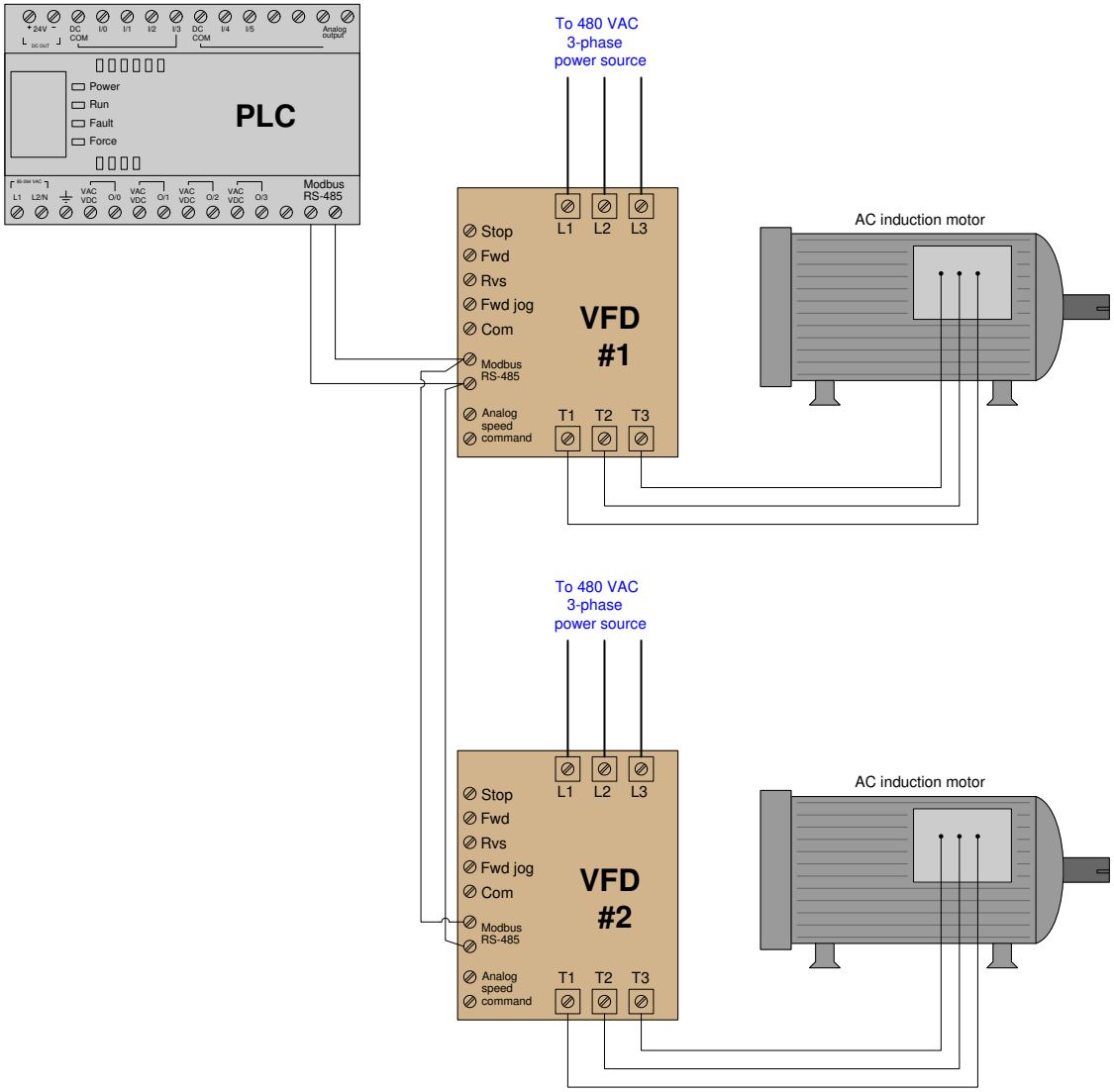

HART
transmitter
Power
supply
250 < R < 1100
Computer
HART communicator


HART communicator
or PC w/ HART modem
DC
power
supply
+
−
− +
H
L
Address 4
Address 13
Address 10
Address 5

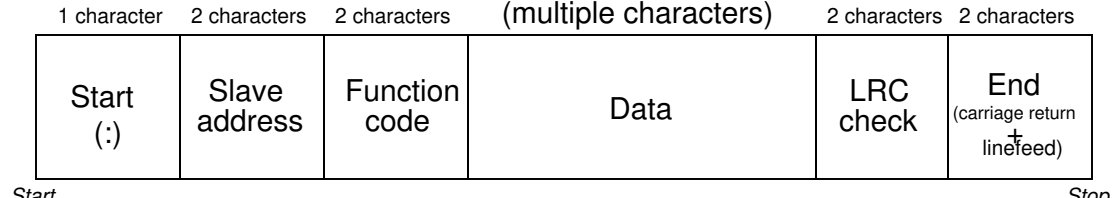

- + - + - +
3 2 1
4-20 mA OUTPUTS
ROSEMOUNT®
EDEN PRAIRIE, MINNESOTA, USA
HART® TRI-LOOP™
MODEL 333U
HIGH ALARM
V_{MAX} = 42.4 V DC
HART® PROTOCOL
COMM
+ -
BURST INPUT
+ -
LABEL 03095-0611-0001/D
Model:
SerialNumber:
Tag:
Descriptor:
Message:
Chan 1
Status
Var
4 mA
20 mA
Units
Disabled
Secondary
0.00
250.00
InH2O


To 480 VAC
3-phase
power source
PLC
Power
Run
Fault
Force
Modbus
RS-485
VFD
Stop
Fwd
Rvs
Fwd jog
Com
Modbus
RS-485
Analog
speed
command
L1
L2
L3
T1
T2
T3
AC induction motor

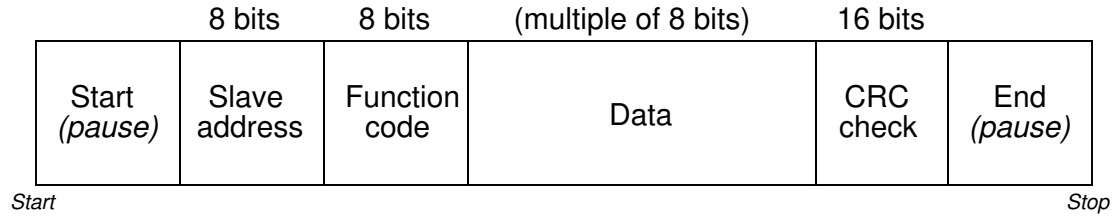

To 480 VAC
3-phase
power source
PLC
Power
Run
Fault
Force
Modbus
RS-485
L1
L2
L3
Stop
Fwd
Rvs
Fwd jog
Com
VFD
Modbus
RS-485
Analog
speed
command
T1
T2
T3
AC induction motor


PLC
Power
Run
Fault
Force
Modbus RS-485
To 480 VAC 3-phase power source
L1
L2
L3
Stop
Fwd
Rvs
Fwd jog
Com
Modbus RS-485
Analog speed command
VFD #1
T1
T2
T3
AC induction motor
To 480 VAC 3-phase power source
VFD #2
AC induction motor

Modbus ASCII message frame



Modbus RTU message frame



Modbus code (decimal)	**Function**
01	Read one or more PLC output “coils” (1 bit each)
02	Read one or more PLC input “contacts” (1 bit each)
03	Read one or more PLC “holding” registers (16 bits each)
04	Read one or more PLC analog input registers (16 bits each)
05	Write (force) a single PLC output “coil” (1 bit)
06	Write (preset) a single PLC “holding” register (16 bits)
15	Write (force) multiple PLC output “coils” (1 bit each)
16	Write (preset) multiple PLC “holding” registers (16 bits each)

Modbus codes (decimal)	**Address range** (decimal)	**Purpose**
01, 05, 15	00001 to 09999	Discrete outputs ("coils"), *read/write*
02	10001 to 19999	Discrete inputs ("contacts"), *read-only*
04	30001 to 39999	Analog input registers, *read-only*
03, 06, 16	40001 to 49999	"Holding" registers, *read/write*

EMERSON.
Process Management

Smart Wireless Gateway

Modbus Register Map

admin

- 169.254.5.12
- Diagnostics
- Explorer
- Setup
  - Network
  - Ethernet protocol
  - Security
  - Log Settings
  - Time
  - System Backup
  - Page Options
  - Restart Apps
  - Firmware Upgrade
  - Firmware Options
  - HART
  - Changes
  - Modbus
    - Communication
    - Mapping
    - Import/Export

Show/Hide System Registers

	Register	Point Name	State	Invert
☐	30001	TT-101.PV		☐
☐	30011	TT-101.QV		☐
☐	30021	TT-101.ACTIVE_NEIGHBORS		☐
☐	30031	TT-101.BURST_178_RELIABILITY		☐
☐	30033	TT-101.RSSI		☐
		Point does not exist		
☐	30041	LSL-78.SV		☐
☐	30051	TT-ORANGE.PV		☐
☐	30061	TT-101.PV_STATUS		☐

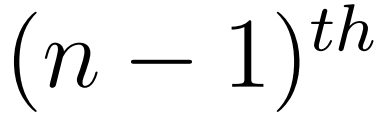
|<< First | << Previous | Search | Page 1 of 1 | Next>> | Last>>|

New entry

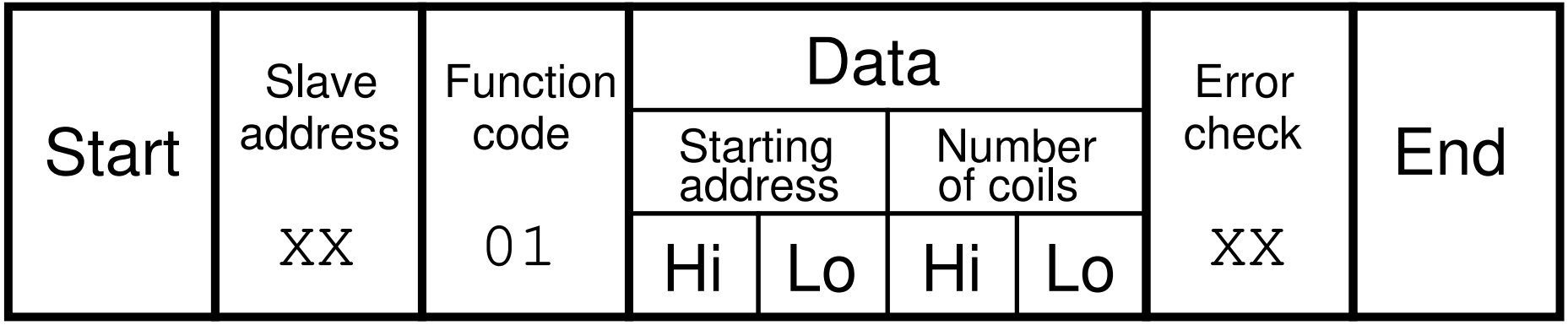
Delete selected | Select All None Errors

```
#include <stdio.h>
#include <modbus.h>
\par
modbus_t *Device;
\par
int main (void)
{
  int read_count;
  uint16_t inreg_word[4];
\par
Device = modbus_new_tcp ("192.168.0.10", 502);
  modbus_set_error_recovery (Device, MODBUS_ERROR
\par
read_count = modbus_read_registers (Device, 9000,
\par
printf("Number of registers read = %i \n", read_co
  printf("Value of register 49001 = %i \n", inreg_
  printf("Value of register 49002 = %i \n", inreg_
  printf("Value of register 49003 = %i \n", inreg_
  printf("Value of register 49004 = %i \n", inreg_
\par
modbus_close (Device);
  modbus_free (Device);
\par
return read_count;
}
```

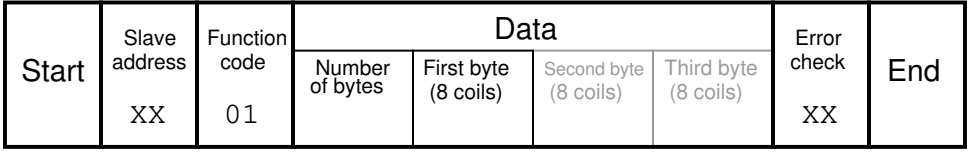
```
#include <stdio.h>
#include <modbus.h>
\par
modbus_t *Device;
\par
int main (void)
{
   int read_count;
   uint16_t inreg_word[3];
\par
Device = modbus_new_tcp ("192.168.0.10", 502);
   modbus_set_error_recovery (Device, MODBUS_ERROR
\par
read_count = modbus_read_input_registers (Device,
\par
printf("Number of registers read = %i \n", read_co
   printf("Value of register 30015 = %i \n", inreg_
   printf("Value of register 30016 = %i \n", inreg_
   printf("Value of register 30017 = %i \n", inreg_
\par
modbus_close (Device);
   modbus_free (Device);
\par
return read_count;
}
```



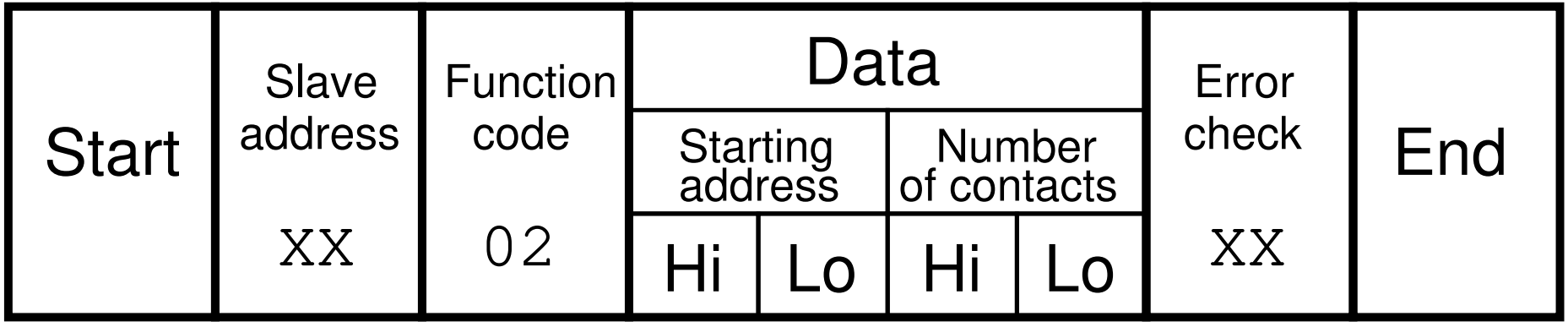
Query message (Function code 01)



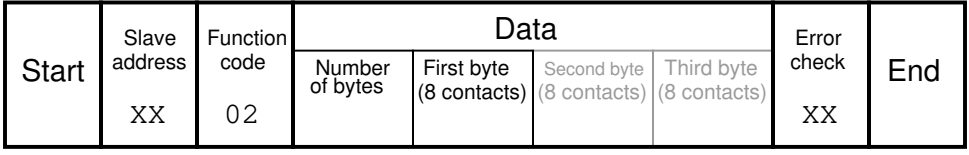
Response message (Function code 01)



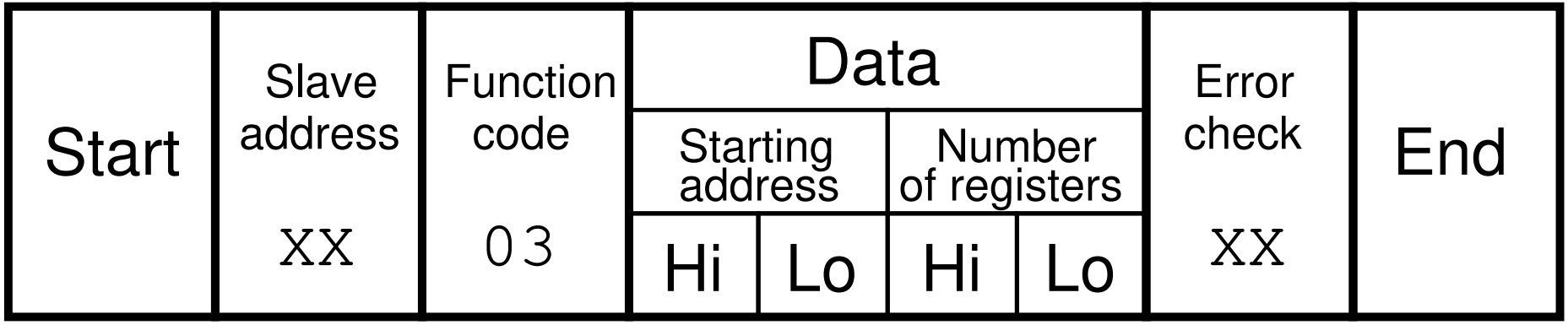
Query message (Function code 02)



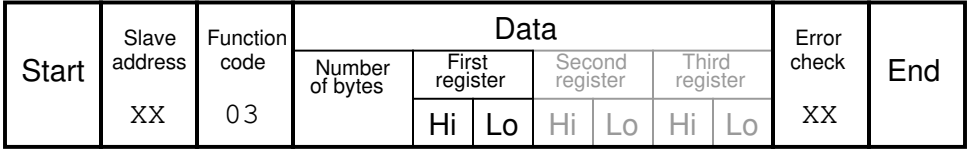
Response message (Function code 02)



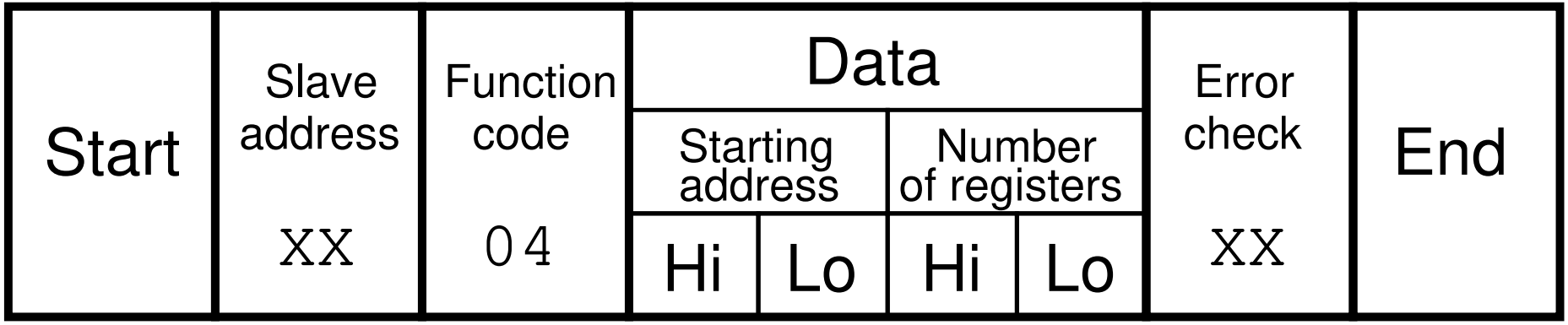
Query message (Function code 03)



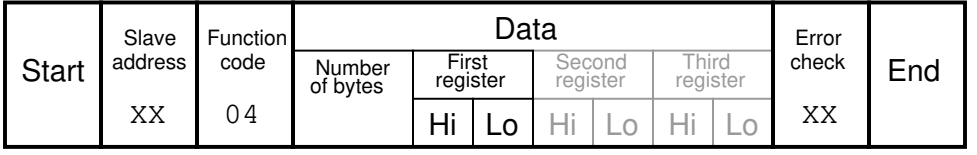
Response message (Function code 03)



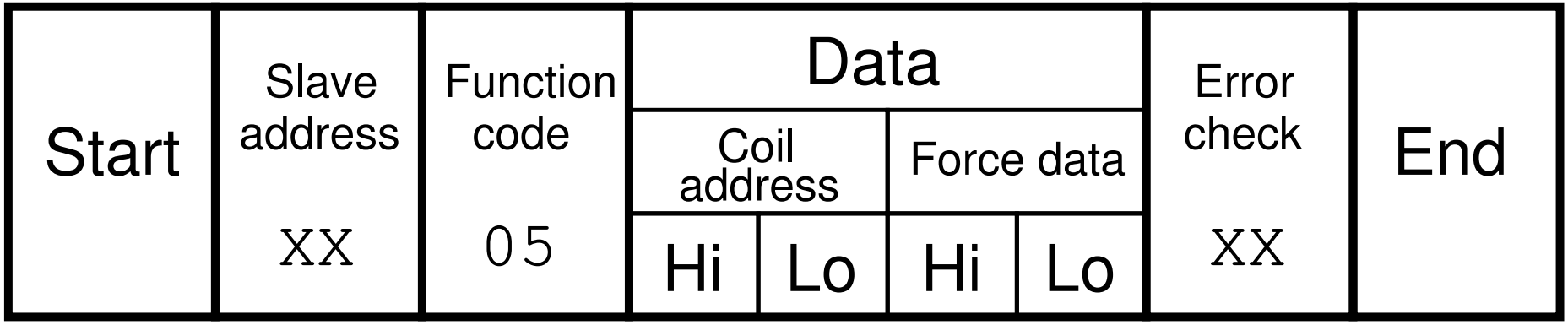
Query message (Function code 04)



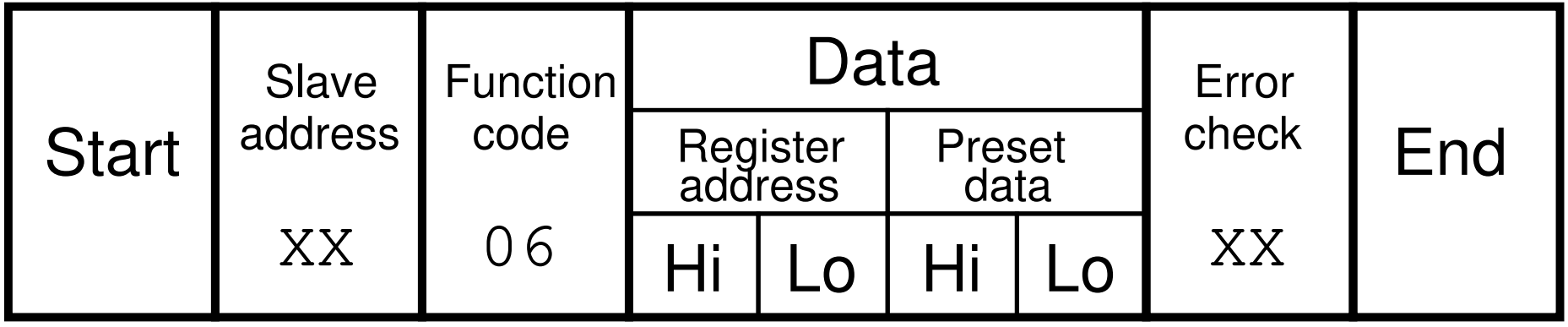
Response message (Function code 04)



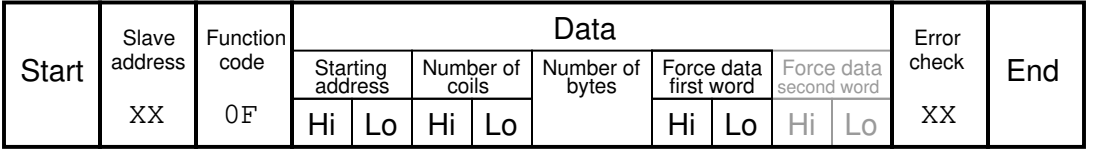
Query/Response message (Function code 05)



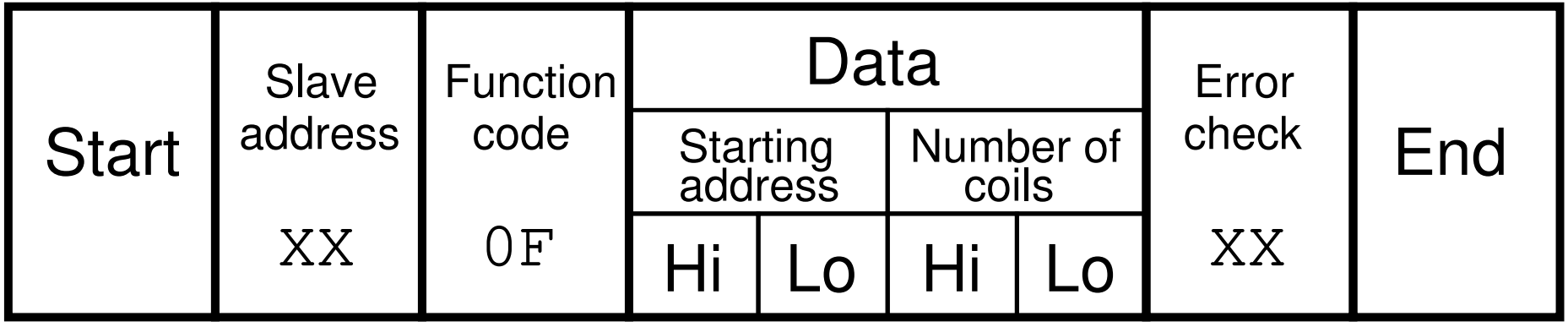
Query/Response message (Function code 06)



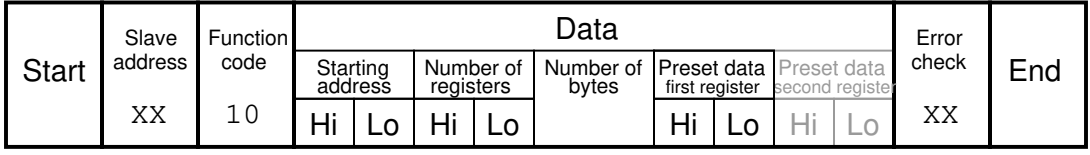
Query message (Function code 15)



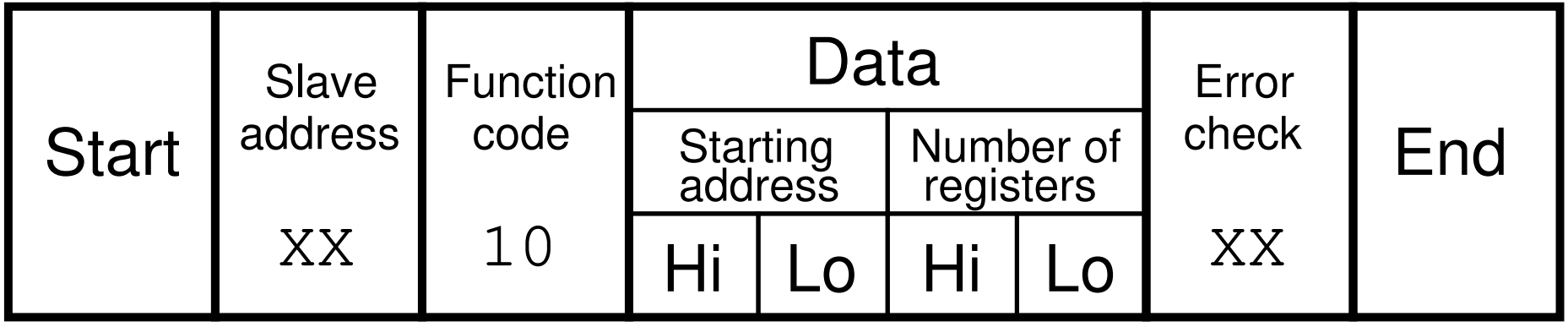
Response message (Function code 15)



Query message (Function code 16)



Response message (Function code 16)



```
\par
union {
    float fp;
    uint16_t intg[2];
    uint8_t by[4];
  } junk;
\par
```

```
#include <stdio.h>
#include <modbus.h>
\par
modbus_t *Device;
\par
int main (void)
{
  int read_count;
\par
union {
    uint16_t word[2];
    uint8_t byte[4];
  } in;
\par
union {
    float real;
    uint8_t byte[4];
  } out;
\par
Device = modbus_new_tcp ("192.168.0.10", 502);
  modbus_set_error_recovery (Device, MODBUS_ERROR
\par
read_count = modbus_read_input_registers (Device,
\par
printf("Value of 16-bit register 30020 = %i \n", i
  printf("Value of 16-bit register 30021 = %i \n",
\par
out.byte[0] = in.byte[2];
  out.byte[1] = in.byte[3];
  out.byte[2] = in.byte[0];
  out.byte[3] = in.byte[1];
\par
printf("Value of 32-bit floating-point number = %f
  \par
modbus_close (Device);
  modbus_free (Device);
\par
return read_count;
}
```

```
#include <stdio.h>
#include <modbus.h>
\par
modbus_t *Device;
\par
int main (void)
{
  int read_count;
  uint16_t word[2];
  float real;
\par
Device = modbus_new_tcp ("192.68.0.10", 502);
  modbus_set_error_recovery (Device, MODBUS_ERROR
\par
read_count = modbus_read_input_registers (Device,
\par
printf("Value of 16-bit register 32999 = %i \n", v
  printf("Value of 16-bit register 33000 = %i \n",
\par
real = modbus_get_float(word);
\par
printf("Value of 32-bit floating-point number = %f
  \par
modbus_close (Device);
  modbus_free (Device);
\par
return read_count;
}
```