

200-601 Dumps

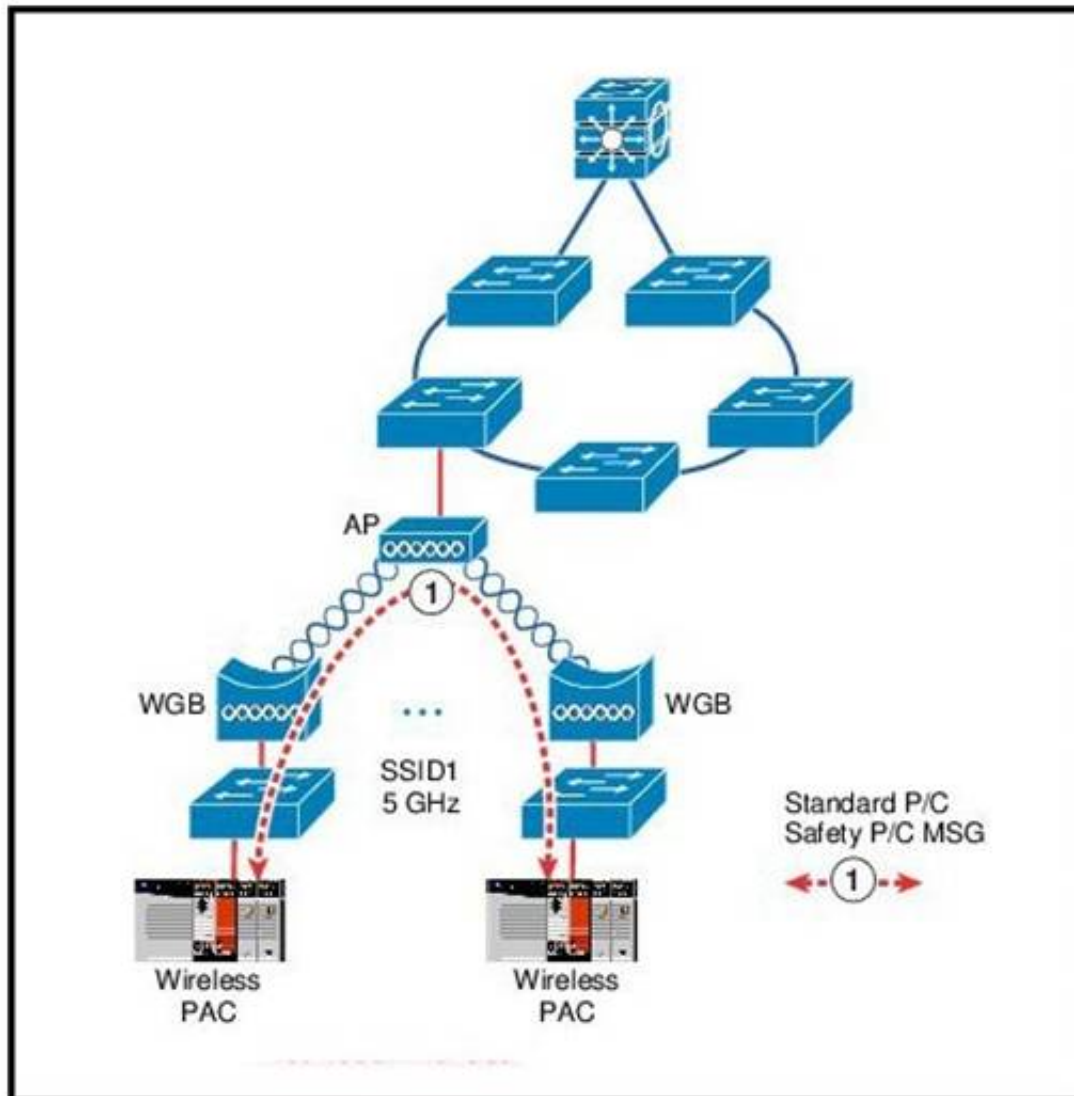
Managing Industrial Networking for Manufacturing with Cisco Technologies

<https://www.certleader.com/200-601-dumps.html>



NEW QUESTION 1

Refer to the exhibit.



What issue does this topology present for the represented traffic flow?

- A. Standard Produce/Consume traffic is not suitable for an 802.11 wireless environment.
- B. Only one of the Work Group Bridges can transmit at a time, because 802.11 is half duplex.
- C. The Converged Plant-wide Ethernet best practices for 802.11 wireless don't allow for PAC to PAC traffic.
- D. I/O control traffic should utilize the 2.4 GHz band based on best practices.

Answer: B

NEW QUESTION 2

What is the purpose of Spanning Tree Protocol?

- A. to prevent routing loops
- B. to create a default route
- C. to provide multiple gateways for hosts
- D. to maintain a loop-free Layer 2 network topology
- E. to enhance the functions of SNMP

Answer: D

NEW QUESTION 3

A small manufacturing company has a Class C network address on the plant floor and needs to create five subnets, each accommodating 25 endpoints. Which subnet mask needs to be configured?

- A. 255.255.240.0
- B. 255.255.255.128
- C. 255.255.255.192
- D. 255.255.255.224
- E. 255.255.255.240
- F. 255.255.255.248

Answer: D

NEW QUESTION 4

Refer to the exhibit. Which lines represent a CIP connection being established between two devices?

No.	Time	Source	Destination	Protocol	Length	Info
2909	2015-04-03 09:06:43.343660000	192.168.1.2	192.168.1.2	ENIP	76	Connection: ID=0x000B49EE, Seq=0002627468
2910	2015-04-03 09:06:43.347531000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940702
2911	2015-04-03 09:06:43.352179000	192.168.1.2	192.168.1.2	TCP	66	62601->44818 [SYN] Seq=0 win=8192 Len=0 MSS=1426 SACK_PERM=1 WS=1
2912	2015-04-03 09:06:43.352179000	192.168.1.3	192.168.1.2	TCP	66	44818->62601 [SYN, ACK] Seq=0 Ack=1 win=10000 Len=0 MSS=1426 SACK_PERM=1 WS=1
2913	2015-04-03 09:06:43.352180000	192.168.1.2	192.168.1.3	TCP	60	62601->44818 [ACK] Seq=1 Ack=1 win=8192 Len=0
2914	2015-04-03 09:06:43.352184000	Rockwell_1a:4a:c	Broadcast	ARP	60	who has 192.168.1.2? Tell 192.168.1.3
2915	2015-04-03 09:06:43.352185000	Rockwell_1c8:17:4	Rockwell_1a:4a:c	ARP	60	192.168.1.2 is at 00:00:bc:c8:17:42
2916	2015-04-03 09:06:43.353492000	192.168.1.2	192.168.1.3	ENIP	82	Register Session (Req), Session: 0x00000000
2917	2015-04-03 09:06:43.353495000	192.168.1.3	192.168.1.2	ENIP	82	Register Session (Rsp), Session: 0x04000100
2918	2015-04-03 09:06:43.353497000	192.168.1.2	192.168.1.3	CIP CM	154	Forward Open
2919	2015-04-03 09:06:43.355730000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938324
2920	2015-04-03 09:06:43.355735000	192.168.1.3	192.168.1.2	ENIP	98	Connection: ID=0x00D240D4, Seq=0000000000
2921	2015-04-03 09:06:43.355737000	192.168.1.3	192.168.1.2	CIP CM	146	Success
2922	2015-04-03 09:06:43.366424000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, Seq=0002628115
2923	2015-04-03 09:06:43.366458000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940703
2924	2015-04-03 09:06:43.371153000	192.168.1.2	192.168.1.3	ENIP	86	Connection: ID=0x005E40D4, Seq=0000000000
2925	2015-04-03 09:06:43.373605000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, Seq=0002627469
2926	2015-04-03 09:06:43.375686000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938325
2927	2015-04-03 09:06:43.387157000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940704
2928	2015-04-03 09:06:43.395590000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938326
2929	2015-04-03 09:06:43.395594000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, Seq=0002628116
2930	2015-04-03 09:06:43.403825000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, Seq=0002627470
2931	2015-04-03 09:06:43.405574000	192.168.1.3	192.168.1.2	ENIP	98	Connection: ID=0x00D240D4, Seq=0000000001
2932	2015-04-03 09:06:43.407320000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940705
2933	2015-04-03 09:06:43.415818000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938327
2934	2015-04-03 09:06:43.421235000	192.168.1.2	192.168.1.3	ENIP	86	Connection: ID=0x005E40D4, Seq=0000000001
2935	2015-04-03 09:06:43.426793000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, Seq=0002628117
2936	2015-04-03 09:06:43.426797000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940706
2937	2015-04-03 09:06:43.432648000	192.168.1.2	192.168.1.3	CIP CM	230	Forward Open
2938	2015-04-03 09:06:43.432653000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, Seq=0002627471
2939	2015-04-03 09:06:43.436110000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938328
2940	2015-04-03 09:06:43.441156000	192.168.1.3	192.168.1.2	CIP CM	144	Success
2941	2015-04-03 09:06:43.447344000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940707
2942	2015-04-03 09:06:43.452305000	192.168.1.2	192.168.1.3	ENIP	134	Connection: ID=0x000E40D5, Seq=0000000000
2943	2015-04-03 09:06:43.455330000	192.168.1.3	192.168.1.2	ENIP	98	Connection: ID=0x00D240D4, Seq=0000000002
2944	2015-04-03 09:06:43.455337000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938329
2945	2015-04-03 09:06:43.455339000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, Seq=0002628118
2946	2015-04-03 09:06:43.463863000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, Seq=0002627472
2947	2015-04-03 09:06:43.467320000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940708
2948	2015-04-03 09:06:43.471247000	192.168.1.2	192.168.1.3	ENIP	86	Connection: ID=0x005E40D4, Seq=0000000002
2949	2015-04-03 09:06:43.471252000	192.168.1.2	192.168.1.245	TCP	60	[TCP keep-alive] 44818->1890 [ACK] Seq=1 Ack=1 win=8192 Len=1
2950	2015-04-03 09:06:43.471254000	192.168.1.245	192.168.1.2	TCP	66	[TCP keep-alive ACK] 1890->44818 [ACK] Seq=1 Ack=2 win=352 Len=0 SLE=1 SRE=2
2951	2015-04-03 09:06:43.475876000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938330
2952	2015-04-03 09:06:43.483801000	192.168.1.3	192.168.1.2	ENIP	410	Connection: ID=0x01D240D5, Seq=0000000000
2953	2015-04-03 09:06:43.486451000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, Seq=0002628119
2954	2015-04-03 09:06:43.486482000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, Seq=0003940709
2955	2015-04-03 09:06:43.493659000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, Seq=0002627473
2956	2015-04-03 09:06:43.494335000	192.168.1.202	192.168.1.255	ENIP	66	List Identity (Req)
2957	2015-04-03 09:06:43.494670000	192.168.1.202	192.168.1.255	ENIP	66	List Identity (Req)
2958	2015-04-03 09:06:43.495733000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, Seq=0003938331

- A. 2914 and 2915
- B. 2918 and 2921
- C. 2920 and 2924
- D. 2937 and 2940

Answer: B

NEW QUESTION 5

Which five are characteristics that describe Cisco Industrial switches? (Choose five)

- A. Din rail mount
- B. 19 inch rack mount
- C. Fanless
- D. Fans
- E. Swappable SD flash card
- F. Alarm relay
- G. -5°C to 45°C operating environment
- H. ProfiNET conformance class C compliance

Answer: ABCEF

NEW QUESTION 6

Why is SSH preferred over Telnet as a method of accessing a network device to alter or view the configuration?

- A. Telnet encrypts only the login information, not the entire transmission.
- B. SSH requires fewer network resources and no additional configuration.
- C. Telnet is more difficult to use and configure than SSH.
- D. SSH encrypts the login and session information.

Answer: D

NEW QUESTION 7

Refer to the exhibit. Which lines represent an I/O connection running at a 20ms RPI?

No.	Time	Source	Destination	Protocol	Length	Info
2909	2015-04-03 09:06:43.343660000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, SEQ=0002627468
2910	2015-04-03 09:06:43.347531000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940702
2911	2015-04-03 09:06:43.352174000	192.168.1.2	192.168.1.3	TCP	66	62601->44818 [SYN] Seq=0 Win=8192 Len=0 MSS=1426 SACK_PERM=1 WS=1
2912	2015-04-03 09:06:43.352178000	192.168.1.3	192.168.1.2	TCP	66	44818->62601 [SYN, ACK] Seq=0 Ack=1 Win=10000 Len=0 MSS=1426 SACK_PERM=1 WS=1
2913	2015-04-03 09:06:43.352180000	192.168.1.2	192.168.1.3	TCP	60	62601->44818 [ACK] Seq=1 Ack=1 Win=8192 Len=0
2914	2015-04-03 09:06:43.352184000	Rockwell_1a:4a:cb:broadcast	ARP	60	who has 192.168.1.2? Tell 192.168.1.3	
2915	2015-04-03 09:06:43.352185000	Rockwell_1c8:17:4:Rockwell_1a:4a:	ARP	60	192.168.1.2 is at 00:00:bc:c8:17:42	
2916	2015-04-03 09:06:43.353492000	192.168.1.2	192.168.1.3	ENIP	82	Register Session (Req), Session: 0x00000000
2917	2015-04-03 09:06:43.353495000	192.168.1.3	192.168.1.2	ENIP	82	Register Session (Rsp), Session: 0x04000100
2918	2015-04-03 09:06:43.353497000	192.168.1.2	192.168.1.3	CIP CM	154	Forward Open
2919	2015-04-03 09:06:43.355730000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938324
2920	2015-04-03 09:06:43.355735000	192.168.1.3	192.168.1.2	ENIP	98	Connection: ID=0x00D240D4, SEQ=0000000000
2921	2015-04-03 09:06:43.355737000	192.168.1.3	192.168.1.2	CIP CM	146	Success
2922	2015-04-03 09:06:43.366424000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, SEQ=0002628115
2923	2015-04-03 09:06:43.366458000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940703
2924	2015-04-03 09:06:43.371153000	192.168.1.2	192.168.1.3	ENIP	86	Connection: ID=0x005E40D4, SEQ=0000000000
2925	2015-04-03 09:06:43.373605000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, SEQ=0002627469
2926	2015-04-03 09:06:43.375686000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938325
2927	2015-04-03 09:06:43.387157000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940704
2928	2015-04-03 09:06:43.395590000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938326
2929	2015-04-03 09:06:43.395594000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, SEQ=0002628116
2930	2015-04-03 09:06:43.403825000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, SEQ=0002627470
2931	2015-04-03 09:06:43.405574000	192.168.1.3	192.168.1.2	ENIP	98	Connection: ID=0x00D240D4, SEQ=0000000001
2932	2015-04-03 09:06:43.407320000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940705
2933	2015-04-03 09:06:43.415818000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938327
2934	2015-04-03 09:06:43.421235000	192.168.1.2	192.168.1.3	ENIP	86	Connection: ID=0x005E40D4, SEQ=0000000001
2935	2015-04-03 09:06:43.426793000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, SEQ=0002628117
2936	2015-04-03 09:06:43.426797000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940706
2937	2015-04-03 09:06:43.432648000	192.168.1.2	192.168.1.3	CIP CM	230	Forward Open
2938	2015-04-03 09:06:43.432653000	192.168.1.9	192.168.1.2	ENIP	76	Connection: ID=0x000B49EE, SEQ=0002627471
2939	2015-04-03 09:06:43.436110000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938328
2940	2015-04-03 09:06:43.441156000	192.168.1.3	192.168.1.2	CIP CM	144	Success
2941	2015-04-03 09:06:43.447344000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940707
2942	2015-04-03 09:06:43.452305000	192.168.1.2	192.168.1.3	ENIP	134	Connection: ID=0x000E40D5, SEQ=0000000000
2943	2015-04-03 09:06:43.455330000	192.168.1.3	192.168.1.2	ENIP	98	Connection: ID=0x00D240D4, SEQ=0000000002
2944	2015-04-03 09:06:43.455337000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938329
2945	2015-04-03 09:06:43.455339000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, SEQ=0002628118
2946	2015-04-03 09:06:43.463863000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, SEQ=0002627472
2947	2015-04-03 09:06:43.467320000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940708
2948	2015-04-03 09:06:43.471247000	192.168.1.2	192.168.1.3	ENIP	86	Connection: ID=0x005E40D4, SEQ=0000000002
2949	2015-04-03 09:06:43.471252000	192.168.1.2	192.168.1.245	TCP	60	(TCP keep-alive) 44818->1890 [ACK] Seq=1 Ack=1 Win=8192 Len=1
2950	2015-04-03 09:06:43.471254000	192.168.1.245	192.168.1.2	TCP	66	(TCP keep-alive ACK) 1890->44818 [ACK] Seq=1 Ack=2 Win=352 Len=0 SLE=1 SRE=2
2951	2015-04-03 09:06:43.475876000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938330
2952	2015-04-03 09:06:43.483801000	192.168.1.3	192.168.1.2	ENIP	410	Connection: ID=0x01D240D5, SEQ=0000000000
2953	2015-04-03 09:06:43.486451000	192.168.1.9	192.168.1.2	ENIP	72	Connection: ID=0x005240C0, SEQ=0002628119
2954	2015-04-03 09:06:43.486482000	192.168.1.2	192.168.1.4	ENIP	74	Connection: ID=0x11EF00A1, SEQ=0003940709
2955	2015-04-03 09:06:43.493659000	192.168.1.2	192.168.1.9	ENIP	76	Connection: ID=0x000B49EE, SEQ=0002627473
2956	2015-04-03 09:06:43.494335000	192.168.1.202	192.168.1.255	ENIP	66	List Identity (Req)
2957	2015-04-03 09:06:43.494670000	192.168.1.202	192.168.1.255	ENIP	66	List Identity (Req)
2958	2015-04-03 09:06:43.495733000	192.168.1.4	192.168.1.2	ENIP	359	Connection: ID=0x015240C2, SEQ=0003938331

- A. 2919, 2923, 2926
- B. 2920, 2926, 2929
- C. 2922, 2929, 2935
- D. 2914, 2915, 2916

Answer: A

NEW QUESTION 8

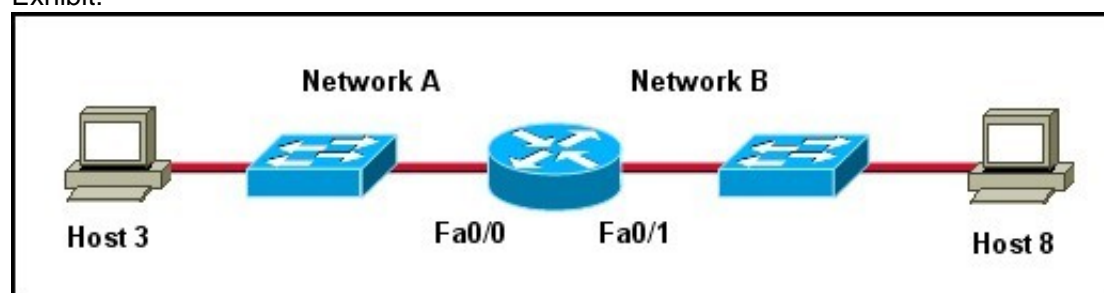
Given the CIA triad elements, which ensures first that the data is encrypted and secure, second that the data is trustworthy, and third that the data is accessible by those who need it?

- A. CIA
- B. ICA
- C. ACI
- D. CAI

Answer: A

NEW QUESTION 9

Exhibit:



Refer to the exhibit. Host 3 on Network A is sending data to Host 8 on Network B. Which address is the default gateway of Host 3?

- A. the address of the switch interface that is connected to router interface Fa0/0
- B. the address of the switch interface that is connected to router interface Fa0/1
- C. the address of the host that is connected to Network A
- D. the address of the host that is connected to Network B
- E. the address of the router interface Fa0/0
- F. the address of the router interface Fa0/1

Answer: E

NEW QUESTION 10

Which option allows an EtherNet/IP I/O device to be safely installed where it is subject to water immersion?

- A. The device is rated IP20 and the power wiring is installed securely to the terminal block.
- B. The device is rated IP67 and a power cordset is used.
- C. The device is rated IP67 and immersed to 10 m.
- D. The device is rated IP20 and immersed to 10 m.

Answer: B

NEW QUESTION 10

You are called at home at 3am by an unskilled machine operator with a suspected network related problem; the controller LEDs are all normal but the output module's communications LED is not on. The operator has verified the cable is functional and correctly connected from the communication module to the switch. What is the next check that you ask the unskilled machine operator to make?

- A. Log onto the switch using the console port and check that IGMP snooping is enabled
- B. Open Wireshark and check whether the controller is issuing a forward open instruction to the device
- C. Open the diagnostic faceplate on the HMI for the control panel switch and check that the relevant ports are enabled and not in alarm
- D. Open Studio 5000 and check the module status tab for the affected output module

Answer: C

NEW QUESTION 12

Which two ports does EtherNet/IP use to communicate? (Choose two.)

- A. TCP 44818
- B. UDP 44818
- C. TCP 502
- D. UDP 502
- E. TCP 2222
- F. UDP 2222

Answer: AF

NEW QUESTION 16

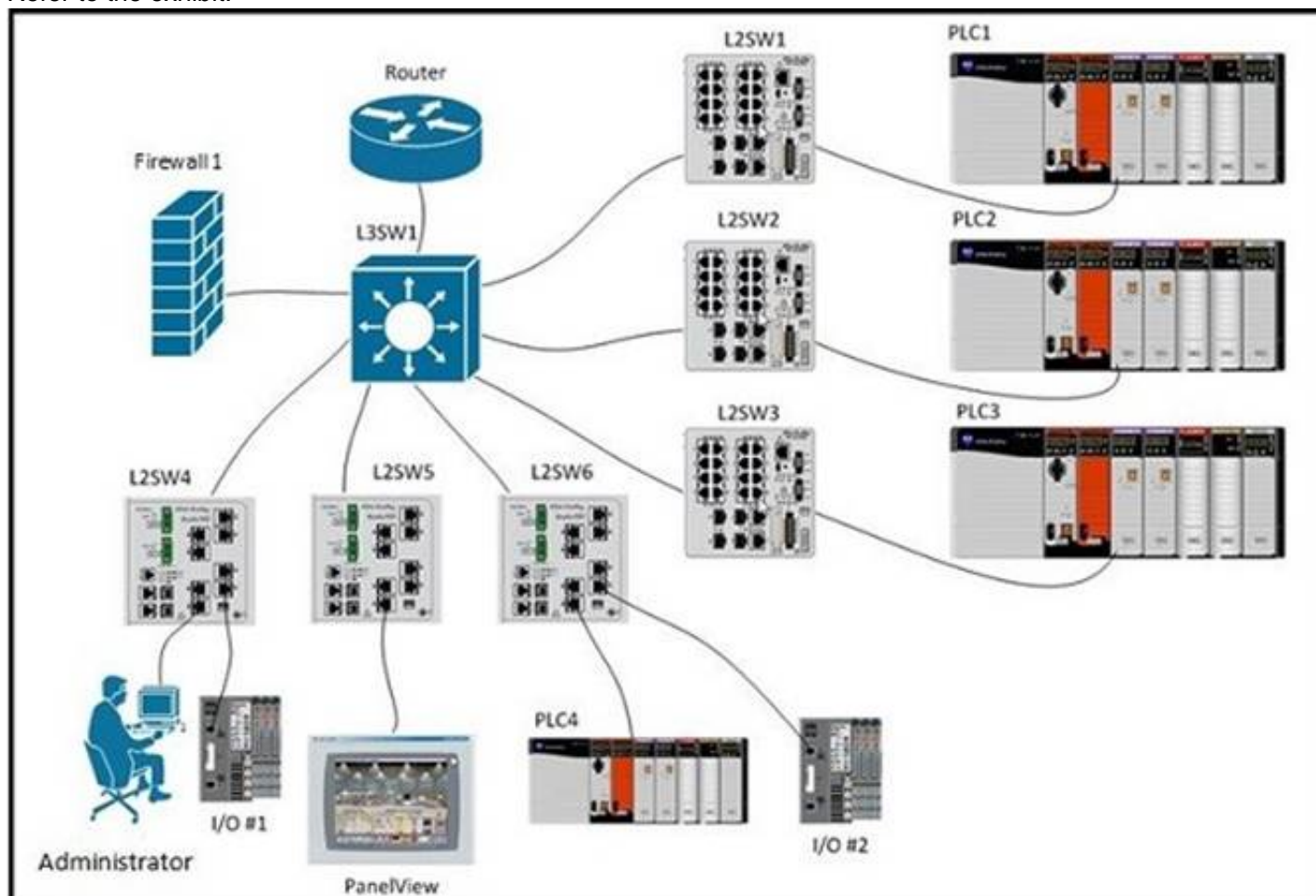
You are called upon to troubleshoot connectivity problems to a network device on a production floor. You have used ping and traceroute to verify that you cannot connect to the device from the management network. The network is 209.165.202.128/27 and the device has been given the IP address 209.165.202.158 and mask 255.255.255.224. You have verified that you can reach the device with your computer connected to the same switch as the device. What could be the cause of this problem?

- A. The device is set to the wrong subnet mask.
- B. The device is set to the wrong IP address.
- C. The device has no IP default gateway.
- D. The device is connected to a switchport in the wrong VLAN.

Answer: C

NEW QUESTION 18

Refer to the exhibit.



All of the vlans listed in the routing table below are trunked using 802.1q and are active on all switches. PLC1, PLC2, and PLC3 each has IP address 192.168.0.1/24 and are connected to ports configured for vlan 50. L2SW1, L2SW2, and L2SW3 are not using vlan trunking for vlan 50.

L3SW1 has following routing table:

10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
 C 10.3.138.0/23 is directly connected, Vlan307
 C 10.3.136.0/23 is directly connected, Vlan306
 C 10.15.153.0/24 is directly connected, Vlan398
 C 10.3.142.0/23 is directly connected, Vlan309
 C 10.3.140.0/23 is directly connected, Vlan308
 C 10.3.186.0/23 is directly connected, Vlan293
 C 10.15.154.0/24 is directly connected, Vlan399
 C 10.3.184.0/23 is directly connected, Vlan292
 C 10.3.190.0/23 is directly connected, Vlan295
 C 10.3.188.0/23 is directly connected, Vlan294
 C 10.3.182.0/23 is directly connected, Vlan291
 C 10.3.180.0/23 is directly connected, Vlan290

PLC1, PLC2, and PLC3 cannot be reconfigured. What can be done to be able to simultaneously communicate with PLC1, PLC2, and PLC3?

- A. Enable NAT on L3SW1
- B. Enable NAT on L2SW1 – L2SW3
- C. Enable NAT on L2SW4

D. Add vlan 50 to L2SW4 and assign the administrator's an IP address on 192.168.0.0/24 network

Answer: B

NEW QUESTION 22

What percentage of an I/O connection would you set the RPI in order to ensure the application has the most current data?

- A. RPI at 50% of IO rate
- B. RPI at 25% of IO rate
- C. PI to 25% of PAC scan rate
- D. Set RPI to 50% of PAC scan rate

Answer: A

NEW QUESTION 27

A shutdown in the cookie cutter machine was traced to a broken network cable. What are two reasons that explain why using DLR is an appropriate choice for network resiliency? (Choose two)

- A. DLR is designed for single network operation at the machine level
- B. Moving to a linear topology will reduce the number of cables and so reduce risk of cable failure
- C. DLR is the only resiliency technology that is supported by CIP Safety
- D. Layer 2 resiliency protocols like REP and RSTP do not have a fast enough convergence time for motion control
- E. Half of the network traffic goes clockwise on the ring and the other half counter- clockwise, reducing by 50% the impact of cable failure

Answer: AD

NEW QUESTION 31

Which is an issue with running CIP Motion on a REP network and identifies an alternate resiliency protocol that works for CIP Motion?

- A. CIP Motion requires a star topology which is not supported by RE
- B. DLR is a suitable resiliency protocol for CIP motion.
- C. REP convergence is not fast enough
- D. DLR is a suitable resiliency protocol for CIP motion.
- E. CIP Motion requires a star topology which is not supported by RE
- F. RPVST+ is a suitable resiliency protocol for CIP motion.
- G. REP convergence is not fast enough
- H. RPVST+ is a suitable resiliency protocol for CIP motion.

Answer: B

NEW QUESTION 36

Which in-depth approach is used when deploying defense in an industrial zone?

- A. Use PLCs and control systems from multiple vendors in such a way that the process will become resilient for failures of one vendor.
- B. Deploy two factor authentications for all operators which need to login remote while working from home.
- C. Collect log files at a central location for easy back-up and encryption to provide privacy.
- D. Create multiple zones in the industrial zone and protect / inspect traffic between the zones with firewalls and intrusion monitors.

Answer: D

NEW QUESTION 40

Which statement is correct regarding ProfiNET communication classes?

- A. ProfiNET-RT traffic is carried in UDP and TCP packets
- B. ProfiNET-NRT is used to carry time critical status information
- C. ProfiNET-IRT requires switches with hardware time scheduling capabilities
- D. ProfiNET-NRT is prioritized as Layer-2 Class-of-Service 1 (CoS 1)

Answer: C

NEW QUESTION 42

What are two benefits of a star network topology? (Choose two.)

- A. Disruption of the entire network is not required when adding new machines.
- B. Any problem which leaves the network inoperable can be traced to the central hub.
- C. This network type requires less cable as compared to linear bus topology.
- D. The performance of one of the numerous nodes cannot reflect on the performance of other nodes.
- E. The performance of the entire network is directly dependent on the performance of the hub.

Answer: AB

NEW QUESTION 47

You have been tasked to design an Ethernet network capable of Motion control with cycle times not to exceed 1ms. In order to create a more deterministic network, what characteristic/s should you primarily focus on?

- A. Latency and Jitter
- B. Redundancy and high availability
- C. Explicit and Implicit messaging
- D. This cycle time is not possible on an Ethernet network
- E. Gigabit port speed

Answer: A

NEW QUESTION 48

Which describes the relationship between a workgroup bridge?

- A. Wired clients of a workgroup bridge can communicate, through the workgroup bridge, with wireless clients of an autonomous or a controller-based access point
- B. Wireless clients of a controller-based AP can communicate, through the workgroup bridge, with wireless clients of an autonomous access point
- C. Wireless clients of an autonomous access point can communicate with wired clients of a workgroup bridge, but Wireless clients of a controller-based access point cannot communicate with wired clients of a workgroup bridge
- D. Wireless clients of a controller-based access point can communicate with wired clients of a workgroup bridge, but Wireless clients of an autonomous access point cannot communicate with wired clients of a workgroup bridge

Answer: A

NEW QUESTION 49

Which three of the following components must be elected before the Spanning Tree Protocol can converge in a switched LAN? (Choose three.)

- A. designated ports
- B. duplex operating mode
- C. fast mode ports
- D. root bridge
- E. root ports
- F. BDPUs priority

Answer: ADE

NEW QUESTION 52

Which command globally enables QoS on a Cisco Industrial Ethernet switch?

- A. switch(config)#qos enable
- B. switch(config)#mls queuing enable
- C. switch#enable queuing
- D. switch(config)#mls qos

Answer: D

NEW QUESTION 53

Which selection is a reason why IGMP snooping should be configured on a switched network?

- A. IGMP snooping populates the snooping table with the results of DHCP requests and can be used by Dynamic ARP Inspection to block IP spoofing attacks at Layer-2.
- B. IGMP snooping verifies the source IP address of every IPv4 packet to ensure that it hasn't been originated from a port different than its return path.
- C. IGMP snooping is used to filter ping requests and results to avoid overflowing the MAC address table of the switch.
- D. IGMP snooping allows a Layer-2 switch to limit the transmission of multicast frames to only the ports that have members of the relevant IGMP group.

Answer: D

NEW QUESTION 58

How are I/O timeout and Safety I/O timeout calculated?

- A. An I/O connection will timeout based on the lower of 4x RPI or 100m
- B. Safety I/O timeout is calculated as 4xRPI.
- C. An I/O connection will timeout based on the lower of 3x RPI or 100m
- D. Safety I/O timeout is calculated as 3xRPI.
- E. An I/O connection will timeout based on the lower of 4x RPI or 150m
- F. Safety I/O timeout is calculated as 2xRPI.
- G. An I/O connection will timeout based on the lower of 3x RPI or 150m
- H. Safety I/O timeout is calculated as 3xRPI.

Answer: A

NEW QUESTION 63

Which of the following correctly pairs the dotted decimal subnet mask with the correct number of binary bits that represent the subnet mask?

- A. 255.255.255.192 and /25
- B. 255.255.255.248 and /28
- C. 255.255.255.224 and /26
- D. 255.255.255.248 and /27
- E. 255.255.255.240 and /28
- F. 255.255.255.240 and /16

Answer: E

NEW QUESTION 65

You are making changes to a Stratix 5700 using an Add On Profile (AOP) and a controller which is on-line with RSLogix5000. When do the changes you have made get published to the switch?

- A. While online in RSLogix 5000 software the changes made in the AOP are pushed to the switch after pressing the Set button.
- B. All of the changes are automatically pushed to the switch.
- C. Changes to the AOP can only be made from the switch, not in RSLogix 5000.
- D. RSLogix 5000 will push the changes in the AOP to the Stratix 5700 when you right click on the switch, and choose download to switch

Answer: A

NEW QUESTION 69

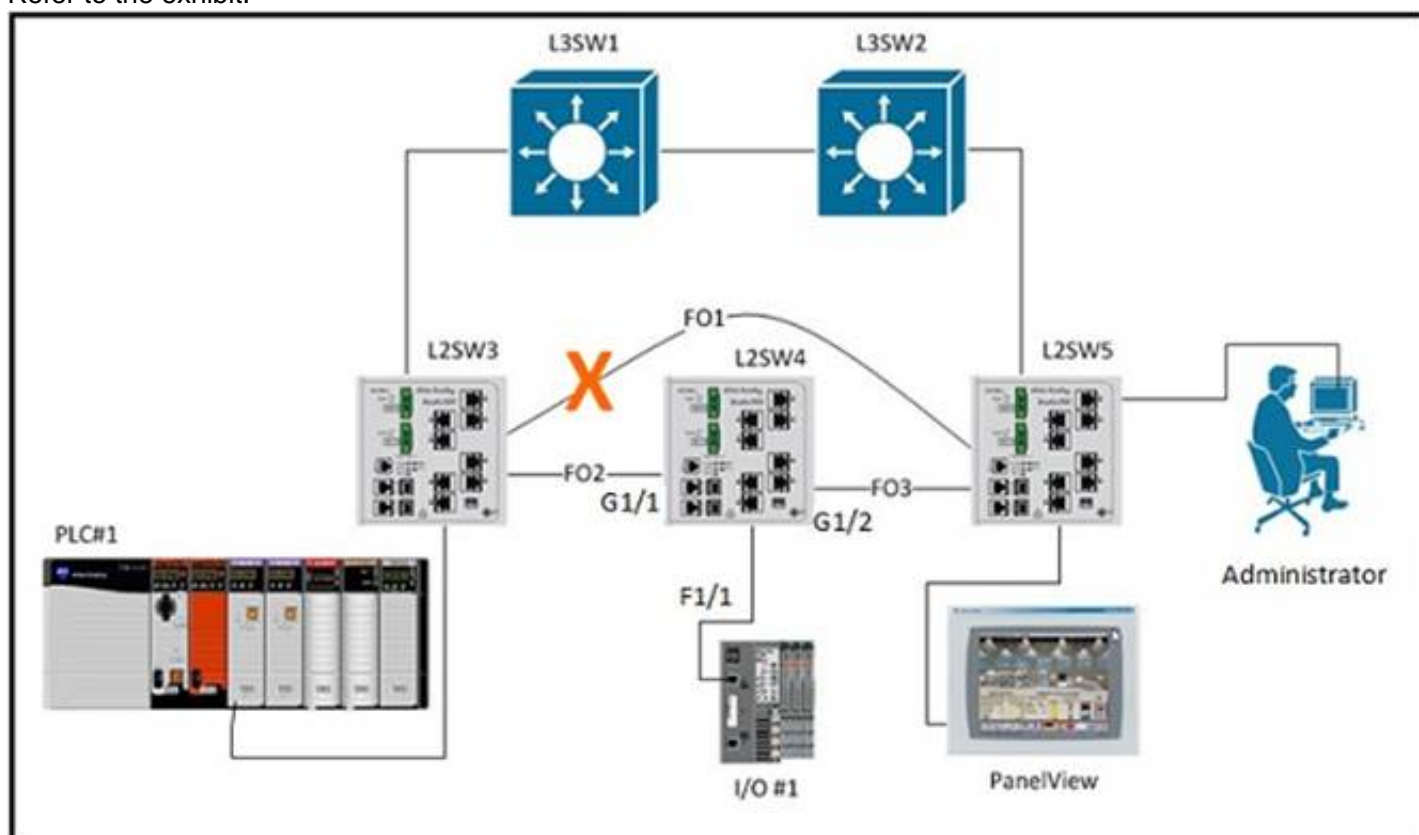
To ensure ProfiNET Layer 2 Class-of-Service markings from ProfiNET devices are trusted by the switch, which command must be entered on the interface attached to the device?

- A. switch(config-if)#mls qos trust cos
- B. switch(config-if)#qos trust cos
- C. switch(config-if)#profinet cos trust
- D. switch(config-if)#trust qos cos

Answer: A

NEW QUESTION 72

Refer to the exhibit.



The control system depicted in the exhibit uses VLAN 300 for all of its device ports and PVST is enabled on each switch to switch connection. L2SW4 was inserted between L2SW3 and L2SW5. Links FO2 and FO3 were added and FO1 was disconnected.

Prior to the installation of L2SW4, PanelView was able to communicate with PLC#1. After the change, PLC#1 and PanelView are still able to communicate but neither PLC#1 or PanelView are able to communicate with I/O #1.

L2SW4# show run interfaces FastEthernet 1/1 description I/O#1

switchport access vlan 300 switchport mode access spanning-tree portfast

spanning-tree bpduguard enable

L2SW4# show interfaces trunk

Port Mode Encapsulation Status Native vlan Gi1/1 on 802.1q trunking 1 Gi1/2 on 802.1q trunking 1 Port Vlans allowed on trunk Gi1/1 1,3-9, 301-305,400 Gi1/2 1,3-9, 301-305,400 Port Vlans allowed and active in management domain Gi1/1 1,3-9, 301-305,400 Gi1/2 1,3- 9, 301-305,400 Port Vlans in spanning tree forwarding state and not pruned Gi1/1 1,3-9, 301-305,400 Gi1/2

Based on the output from the switch, what is preventing I/O#1 from communicating with PLC#1 and PanelView?

- A. Interface FastEthernet 1/1 on LWSW4 should be configured as a trunk port
- B. The trunks connecting L2SW4 to L2SW3 and L2SW5 have the wrong encapsulation type
- C. The trunks connecting L2SW4 to L2SW3 and L2SW5 don't allow VLAN 300 traffic
- D. BPDU guard has error-disabled interface FastEthernet 1/1 on LWSW4

Answer: C

NEW QUESTION 74

DRAG DROP

Drag the steps on the left and arrange them in the order they should be completed when removing an industrial switch from a DIN rail on the right.	
Disconnect all cables and connectors from the front panel of the switch.	Step 1
Pull the bottom of the switch away from the DIN rail and lift the hooks off the top of the DIN rail.	Step 2
Turn off power to the switch.	Step 3
Release the latch from the DIN rail using a flat head screw driver.	Step 4

Answer:

Explanation:

Drag the steps on the left and arrange them in the order they should be completed when removing an industrial switch from a DIN rail on the right.	
Disconnect all cables and connectors from the front panel of the switch.	Turn off power to the switch.
Pull the bottom of the switch away from the DIN rail and lift the hooks off the top of the DIN rail.	Disconnect all cables and connectors from the front panel of the switch.
Turn off power to the switch.	Release the latch from the DIN rail using a flat head screw driver.
Release the latch from the DIN rail using a flat head screw driver.	Pull the bottom of the switch away from the DIN rail and lift the hooks off the top of the DIN rail.

NEW QUESTION 78

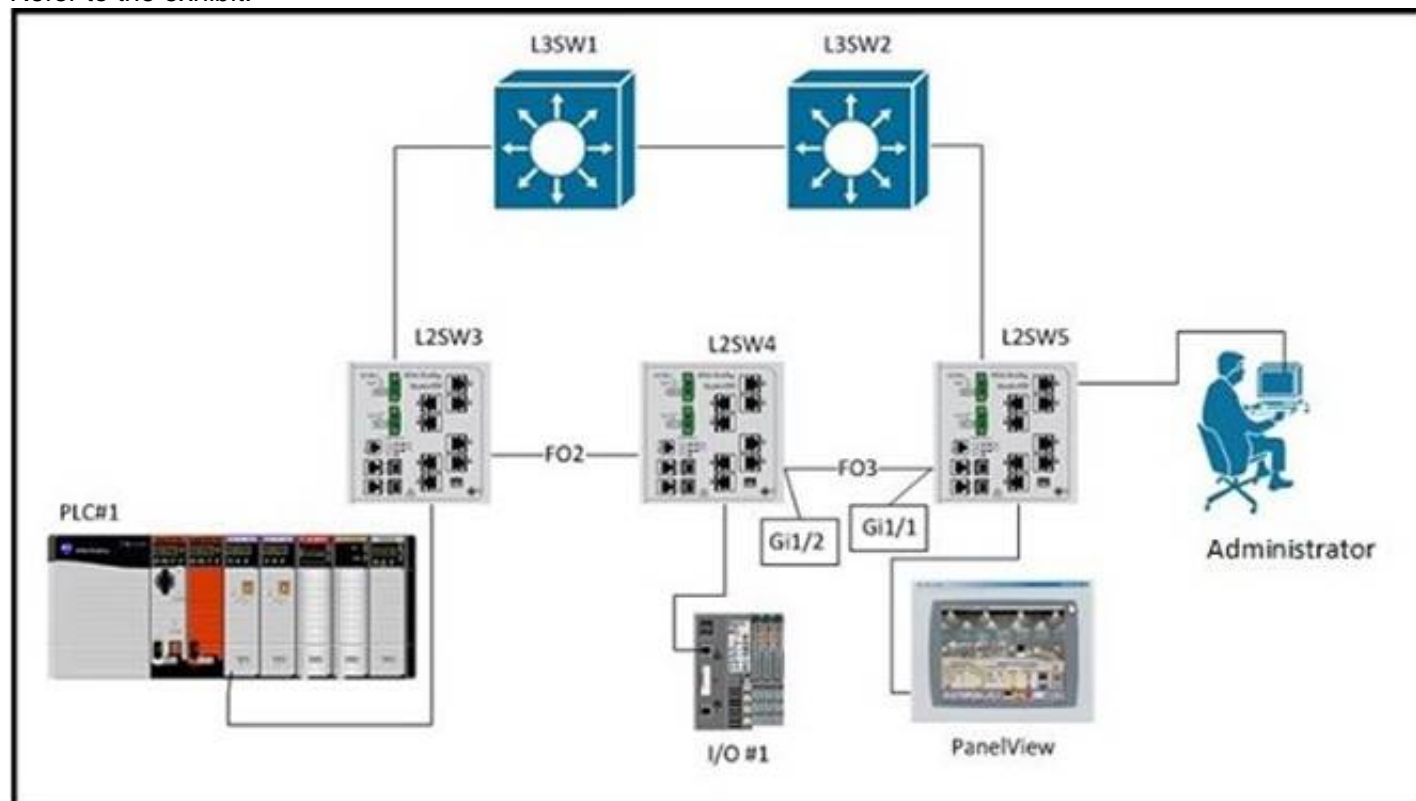
Which option best describes the ProfiNET Discovery and Configuration Protocol (DCP)?

- A. Can be used to override both static and dynamically (DHCP/BOOTP) assigned IP addresses
- B. Cannot be used to reset a device to factory defaults
- C. Is only supported in Conformance Class B and C devices
- D. Uses the ProfiNET-IRT communication class

Answer: A

NEW QUESTION 81

Refer to the exhibit.



L3SW1 has a spanning-tree priority of 8192 set on VLANs 1, 300, and 301, and these VLANs are configured on and trunked between all switches. Executing the command show spanning-tree blockedports on L2SW5 results in:

L2SW5# show spanning-tree blockedports Name Blocked Interfaces List

VLAN0001 Gi1/1 VLAN0300 Gi1/1 VLAN0301 Gi1/1

An additional VLAN, VLAN302, is defined on all switches and trunked between them. VLAN302 access ports are set up on each of the switches and PLC#1, I/O#1, and the PanelView are attached. You expect the new VLAN to be listed as blocked on interface GigabitEthernet1/1 of L2SW5 but it is not. The three new devices are able to communicate with each other.

After executing the same command on all switches you see this output on L2SW4: L2SW4# show spanning-tree blockedports Name Blocked Interfaces List

VLAN0001 Gi1/2

VLAN0300 Gi1/2 VLAN0301 Gi1/2

Why is VLAN302 forwarding on L2SW5 interface GigabitEthernet 1/1 and L2SW4 interface GigabitEthernet 1/1 and 1/2?

- A. VLAN302 is not configured in the VLAN database on L2SW5
- B. VLAN302 is not in the allowed list on the L2SW5 interface GigabitEthernet1/1 trunk
- C. L2SW4 is the spanning tree root for VLAN 302

D. The FO3 fiber-optic cable between L2SW4 and L2SW5 is damaged

Answer: C

NEW QUESTION 85

If the Link Fault alarm is connected to the minor relay and the FCS Bit Error Rate alarm is connected to the major relay, which commands will create an alarm profile called GigE with the alarms correctly mapped to the minor and major relays?

- A. Switch(config)#alarm profile GigE Switch(config-alarm-prof)#alarm 1 4Switch(config-alarm-prof)#relay major 4Switch(config-alarm-prof)#relay minor 1
- B. Switch(config)#alarm profile GigE Switch(config-alarm-prof)#alarm 1 3Switch(config-alarm-prof)#relay major 3Switch(config-alarm-prof)#relay minor 1
- C. Switch(config)#alarm profile GigE Switch(config-alarm-prof)#alarm 1 3Switch(config-alarm-prof)#relay major 1Switch(config-alarm-prof)#relay minor 3
- D. Switch(config)#alarm profile GigE Switch(config-alarm-prof)#alarm 1 4Switch(config-alarm-prof)#relay major 1Switch(config-alarm-prof)#relay minor 4

Answer: A

NEW QUESTION 90

Which statement is correct regarding Media Redundancy Protocol (MRP) in a ring of ProfiNET devices?

- A. When a link fault is detected, MRP rings must converge in less than 100 milliseconds
- B. MRP defines two device roles, Media Redundancy Master and Media Redundancy Client
- C. MRP can support rings of up to 250 devices
- D. MRP is only supported on network switches

Answer: B

NEW QUESTION 92

Refer to the exhibit.

The image shows two screenshots from an RSLogix 5000 workstation. The top screenshot is the 'AB_ETHIP-192\192.168.1.2 1756-EN2TR/B Configuration' dialog box, specifically the 'Network' tab. It shows a ring topology configuration with the following details:

- Network Topology: Ring
- Network Status: Ring Fault
- Active Ring Supervisor: 192.168.1.2
- Active Supervisor Precedence: 0
- ☒ Enable Ring Supervisor
- Ring Faults Detected: 6 (with a 'Reset Counter' button)
- Supervisor Status: Active
- Ring Fault details:
 - Last Active Node on Port 1: 192.168.1.3
 - Last Active Node on Port 2: 192.168.1.4
 - (with a 'Verify Fault Location' button)
- Status: Ring Fault
- Buttons: OK, Cancel, Apply, Help
- Link: Refresh communication

The bottom screenshot shows the 'Workstation, EUBEBXL6H81L32' network tree. The 'AB_ETHIP-192, Ethernet' node is selected and highlighted in blue. Below it, the network topology is listed:

- 192.168.1.10, 1783-ETAP, 1783-ETAP/A (marked with a red X)
- 192.168.1.101, 1783-BMS20CGN Stratix 5700, 1783-BMS20CGN Stratix 5700
- 192.168.1.11, 1783-ETAP, 1783-ETAP/A
- 192.168.1.2, 1756-EN2TR, 1756-EN2TR/B
- 192.168.1.3, 1756-EN2TR, 1756-EN2TR/B
- 192.168.1.4, 1732E-IB16M12SOEDR 16 DC In M12, 1732E-IB16M12SOEDR 16 DC In M12
- 192.168.1.9, 1734-AENTR/B EtherNet Adapter, 1734-AENTR/B Ethernet Adapter
- AB_VBP-1, 1789-A17/A Virtual Chassis

Network Faceplates have not been installed on the HMI and so you need to map a network based on information available from RSLogix. Which most accurately

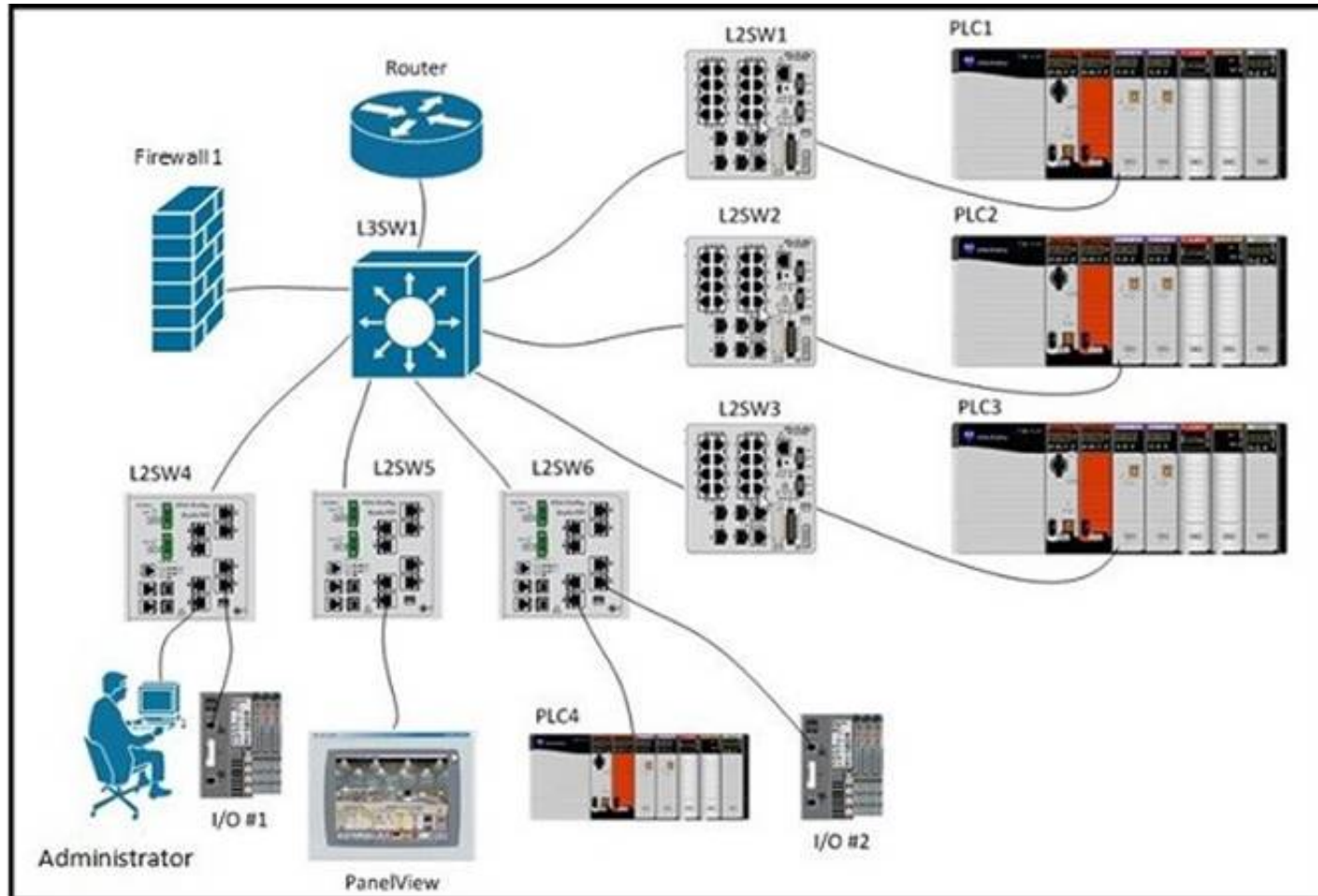
represents the network configuration?

- A. [MISSING]
- B. [MISSING]
- C. [MISSING]
- D. [MISSING]

Answer: B

NEW QUESTION 95

Refer to the exhibit.



A new device, PanelView, has been added to the network. See the table for device details:

All devices are able to ping their default gateway and all other devices except PanelView. PanelView can only ping its default gateway.

After the administrator has done some investigation they have discovered the following information:

```
L3SW1# show run interface
```

```
interface Vlan1 no ip address shutdown
```

```
!
```

```
interface Vlan191
```

```
ip address 10.10.27.125 255.255.255.192
```

```
ip helper-address 165.28.96.96
```

```
ip helper-address 165.28.32.235 no ip redirects
```

```
standby 191 ip 10.10.27.126
```

```
standby 191 priority 120
```

```
standby 191 preempt delay minimum 90 no ip route-cache
```

```
!
```

```
interface Vlan398
```

```
ip vrf forwarding mosaic
```

```
ip address 10.15.153.203 255.255.255.0
```

```
ip helper-address 10.15.154.252
```

```
ip helper-address 10.1.0.252
```

```
standby 98 ip 10.15.153.202
```

```
standby 98 priority 120
```

```
standby 98 preempt delay minimum 90
```

```
!
```

```
interface Vlan399
```

```
ip vrf forwarding mosaic
```

```
ip address 10.15.154.203 255.255.255.0
```

```
ip helper-address 10.1.0.252
```

```
ip helper-address 10.1.1.252
```

```
standby 99 ip 10.15.154.254
```

```
standby 99 priority 120
```

```
standby 99 preempt delay minimum 90
```

```
!
```

```
L3SW1# show ip route connected
```

```
10.0.0.0/8 is variably subnetted, 1149 subnets, 17 masks C 10.10.27.64/26 is directly connected, Vlan191
```

```
C 10.10.31.254/32 is directly connected, Loopback1
```

What is preventing PanelView from pinging the other endpoints in the network?

- A. Routing isn't enabled on L3SW1 for SVI 398 and SVI 399
- B. SVI 191 is in a different routing instance than SVI 398 and SVI 399
- C. Firewall1 is blocking pings from PanelView to the other endpoints
- D. An access list on L3SW1 is blocking pings from PanelView to the other endpoints

Answer: B

NEW QUESTION 99

A cookie cutter machine requires 2 standard controllers and a safety controller. All of these controllers and machine level I/O have been placed on VLAN 104. Both standard controllers must monitor a photocell on this machine. Which IP address is used to transfer this status information?

- A. 10.17.104.16
- B. 192.168.1.16
- C. 239.192.3.16
- D. 239.192.254.16

Answer: C

NEW QUESTION 100

Profinet has been disabled on a Cisco Industrial Ethernet switch, which CLI commands correctly enable ProfinET on VLAN 10?

- A. switch(config)#profinet switch(config)#profinet vlan 10
- B. switch#enable profinet switch(config)#profinet vlan 10
- C. switch(config)#profinet switch(config)#vlan 10 switch(config-vlan)#profinet
- D. switch#enable profinet switch(config)#vlan 10 switch(config-vlan)#profinet

Answer: A

NEW QUESTION 102

Which statement is true regarding ProfiSAFE?

- A. ProfiSAFE traffic must be carried on a network that is physically separated from automation traffic
- B. ProfiSAFE relies on the error detection mechanisms of Ethernet and TCP/IP to determine if there are network errors
- C. ProfiSAFE can be used in safety applications up to Safety Integrity Level 3 (SIL3)
- D. ProfiSAFE is only used by ProfiBUS PA and ProfiBUS DA devices

Answer: C

NEW QUESTION 104

A ProfiNET management system operator is unable to see diagnostic information for a Cisco Industrial Ethernet switch that has been added to a SIMATIC management station. Based on the provided CLI output, which statement is correct?

switch# show profinet status State : Enabled

Vlan : 201

Id : IE2000-Switch Connected : Yes ReductRatio : 128

GSD version : Mis-match

- A. The assigned ProfiNET VLAN is not valid and should be less than 100
- B. LLDP has been disabled on this switch
- C. The GSD file version on the switch does not match the GSD file version on the management station
- D. The Reduction Ration has been set too low

Answer: C

NEW QUESTION 107

To correctly integrate a Cisco Industrial Ethernet switch into a ProfiNET management system such as SIMATIC STEP 7 or TIA Portal, which is a mandatory action?

- A. Configure an IP address on the ProfiNET VLAN interface
- B. The General Station Description (GSD) file must be uploaded from the switch to the management system.
- C. Enable Quality of Service (QoS) and ensure the management station interface is trusted
- D. Enable SNMP on the switch

Answer: B

NEW QUESTION 110

A cookie cutter machine requires 2 standard controllers and a safety controller. All of these controllers and machine level I/O have been placed on VLAN 104. The safety controller must monitor an emergency stop connected to an I/O adapter on an adjacent machine (VLAN 105). Which packet type will be used?

- A. UDP Multicast TTL = 1
- B. UDP Multicast TTL = 2
- C. UDP Unicast
- D. TCP Unicast

Answer: C

NEW QUESTION 115

What can be done to increase the security in depth in an industrial zone?

- A. Add additional disk storage to the IDS server
- B. Add specific SCADA signatures to the IDS server
- C. Create a high availability solution for the IDS server
- D. Place a 'data diode' in front of the IDS server

Answer: B

NEW QUESTION 120

Which two are possible solutions to control which devices can communicate between industrial zones? (Choose two)

- A. Use per zone private IP addressing and deploy NAT to control traffic between zones
- B. Put access control lists on switches connecting industrial zones to control traffic
- C. Attach each zone to a firewall to control intra-zone traffic
- D. Deploy QoS traffic shaping to limit the volume of traffic between industrial zones
- E. Deploy an IDS system between the zones to control intra-zone traffic

Answer: BC

NEW QUESTION 121

You have reached the limit of IPv4 IGMP groups available on a Cisco IE 3000 switch that was deployed using the Express Setup. Which CLI command will increase the number of available IPv4 IGMP groups and multicast routes from 256 to 1000 on this switch?

- A. switch(config)#sdm prefer routing
- B. switch(config)#sdm prefer vlan igmp
- C. switch(config)#sdm prefer routing igmp
- D. switch(config)#sdm prefer vlan

Answer: A

NEW QUESTION 125

Which two actions are examples of network device hardening for Cisco Industrial Ethernet Switches? (Choose two)

- A. Disable unused services
- B. Shutdown network ports which are not in use
- C. Only allow administrative access using Telnet
- D. Deploy IP67 versions of Cisco Industrial Ethernet Switches
- E. Set the native VLAN on all trunk ports to VLAN 1

Answer: AB

NEW QUESTION 129

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 200-601 Exam with Our Prep Materials Via below:

<https://www.certleader.com/200-601-dumps.html>