Exam Questions 200-601

Managing Industrial Networking for Manufacturing with Cisco Technologies

https://www.2passeasy.com/dumps/200-601/

NEW QUESTION 1
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 2
Which configuration enables an Industrial Ethernet switch to participate in PTP clock selection and sets the priority value that would break the tie between switches with matching default criteria to 50?

A. ptp mode boundary ptp priority1 10ptp priority2 50
B. ptp mode boundary ptp priority1 50ptp priority2 10
C. ptp mode e2etransparent ptp priority1 50ptp priority2 10
D. ptp mode e2etransparent ptp priority1 10ptp priority2 50

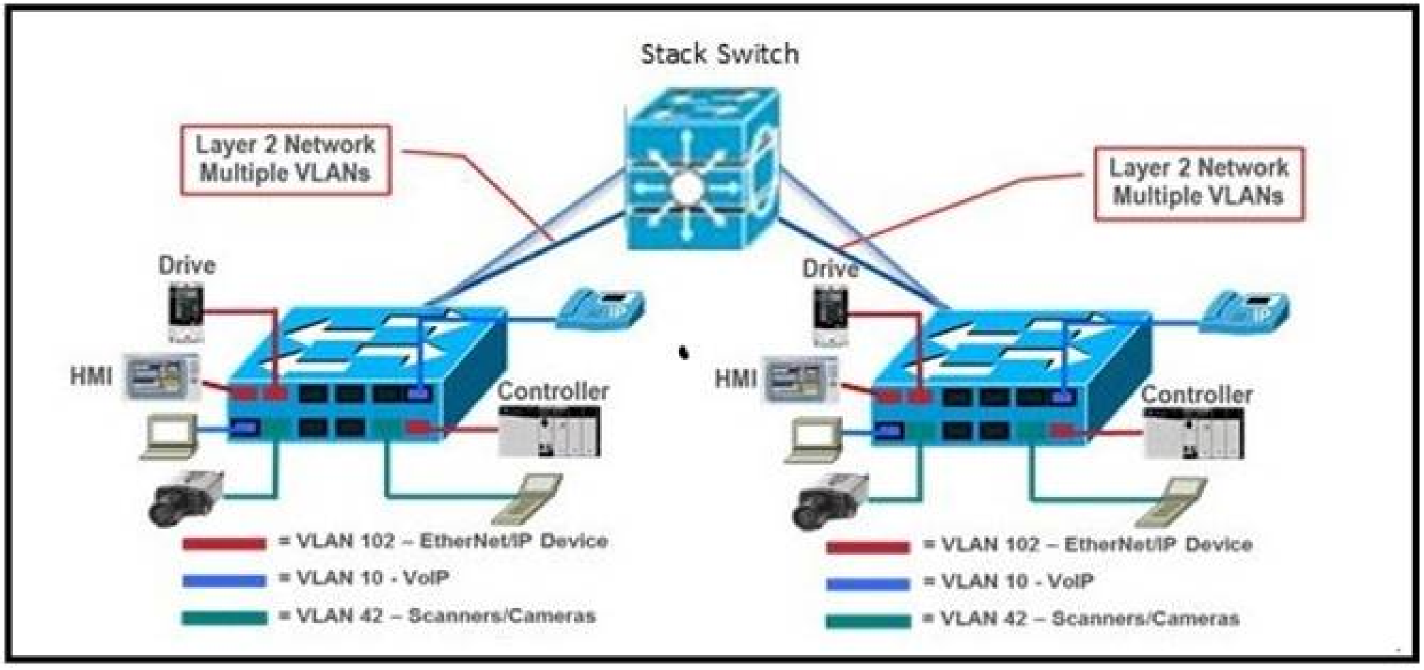
Answer: A

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

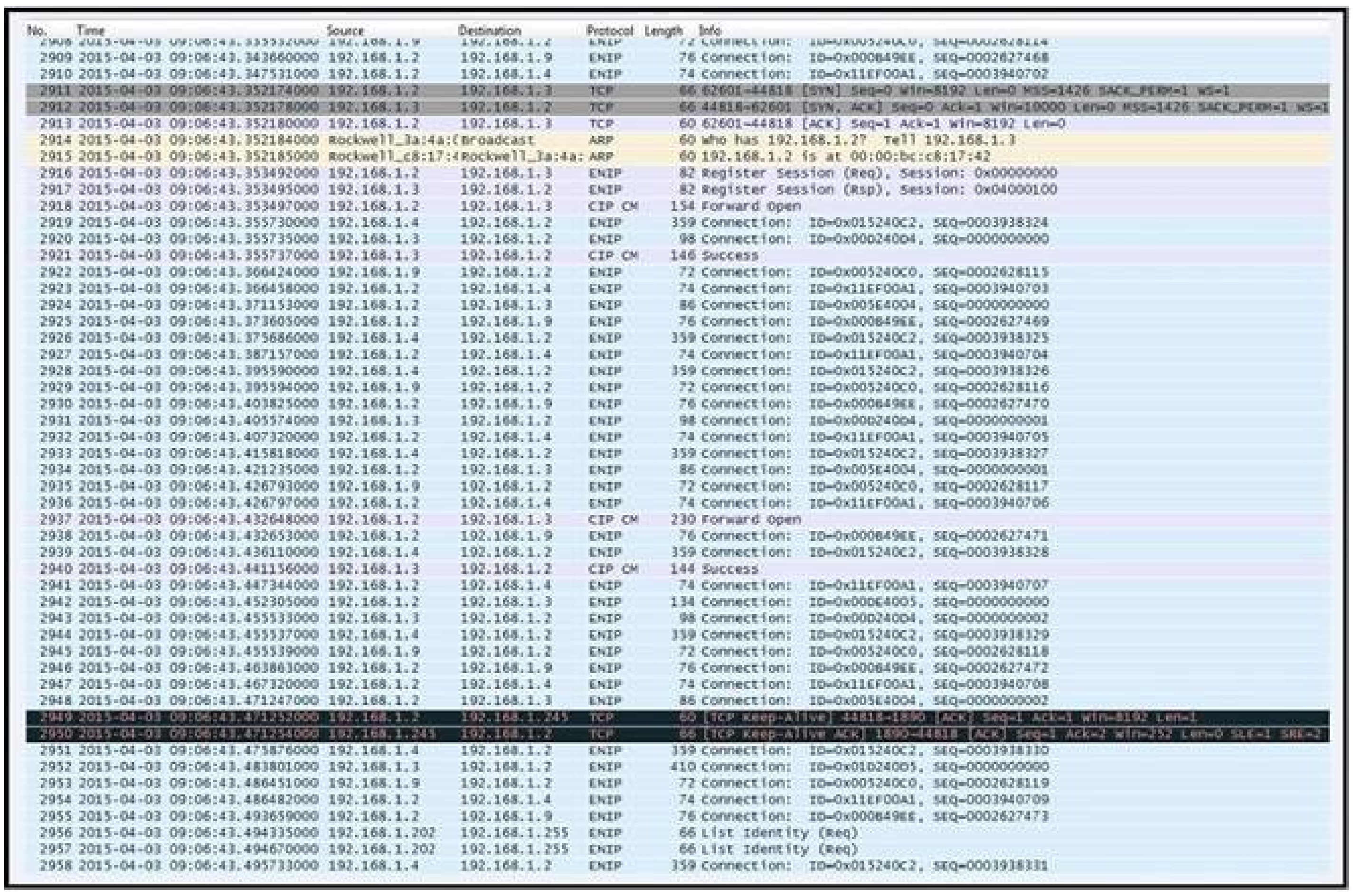
NEW QUESTION 4
Refer to the exhbit. Which three elements would enable high availability and predictable performance for a motion control application spread across two switches (with video and I/O traffic)? (Choose three)


Stack Switch
Layer 2 Network Multiple VLANs
Layer 2 Network Multiple VLANs
Drive
HMI
Controller
Drive
HMI
Controller
= VLAN 102 – EtherNet/IP Device
= VLAN 10 - VoIP
= VLAN 42 – Scanners/Cameras
= VLAN 102 – EtherNet/IP Device
= VLAN 10 - VoIP
= VLAN 42 – Scanners/Cameras

A. Configure QoS to give PTP traffic the highest priority
B. Fiber optic uplinks
C. Redundant uplinks
D. Configure QoS to give I/O traffic the highest priority
E. Copper uplinks
F. Interconnect the two switches

Answer: ABC

NEW QUESTION 5
Refer to the exhibit. Which lines represent a CIP connection being established between two devices?

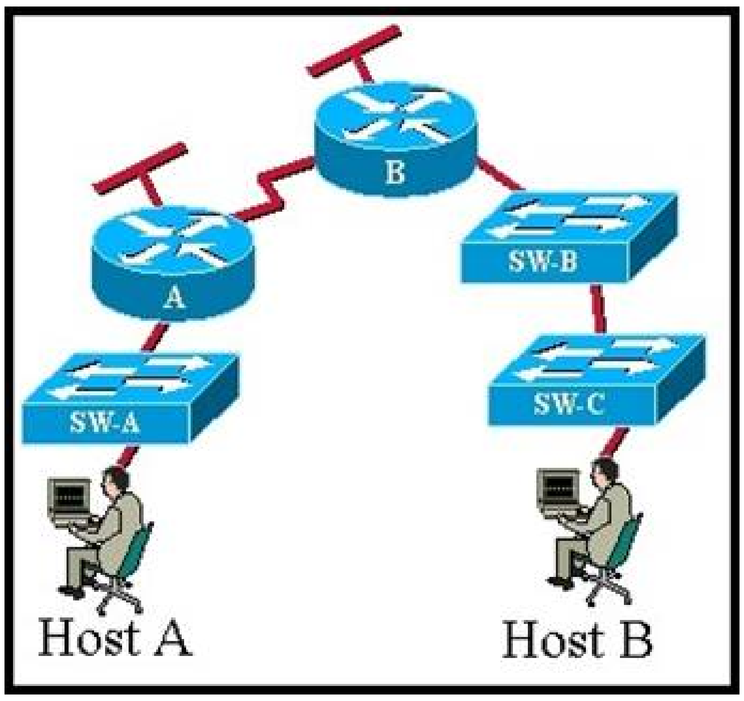


```
No.   Time                          Source             Destination        Protocol Length Info
2908 2015-04-03 09:06:43.333532000 192.168.1.9        192.168.1.2        ENIP      72 Connection:  ID=0x005240C0, SEQ=0002628114
2909 2015-04-03 09:06:43.342660000 192.168.1.2        192.168.1.9        ENIP      76 Connection:  ID=0x000849EE, 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_3a:4a:(Broadcast          ARP       60 Who has 192.168.1.2?  Tell 192.168.1.3
2915 2015-04-03 09:06:43.352185000 Rockwell_c8:17:4Rockwell_3a: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 09:06:43.366438000 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=0x005E4004, SEQ=0000000000
2925 2015-04-03 09:06:43.373605000 192.168.1.2        192.168.1.9        ENIP      76 Connection:  ID=0x000849EE, 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=0x000849EE, 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=0x005E4004, 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=0x000849EE, 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=0x00DE4005, SEQ=0000000000
2943 2015-04-03 09:06:43.455533000 192.168.1.3        192.168.1.2        ENIP      98 Connection:  ID=0x00D240D4, SEQ=0000000002
2944 2015-04-03 09:06:43.455537000 192.168.1.4        192.168.1.2        ENIP     359 Connection:  ID=0x015240C2, SEQ=0003938329
2945 2015-04-03 09:06:43.455539000 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=0x000849EE, 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=0x005E4004, 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=252 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=0x000849EE, 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 6
Exhibit:



Refer to the exhibit. CCNA.com has the industrial network shown in the exhibit. All switches are configured as layer 2 switches and are using VLAN 1 as their management VLAN. Each VLAN 1 interface has been assigned the correct IP address. What is the purpose of assigning a default gateway to SW-C switch?

A. allows connectivity between the VLAN 1 interface on SW-C and other devices in the network.
B. allows connectivity between Host A and other devices in the network.
C. allows connectivity between Host B and other devices in the network.
D. allows the switch to pass traffic between Host A and Host B

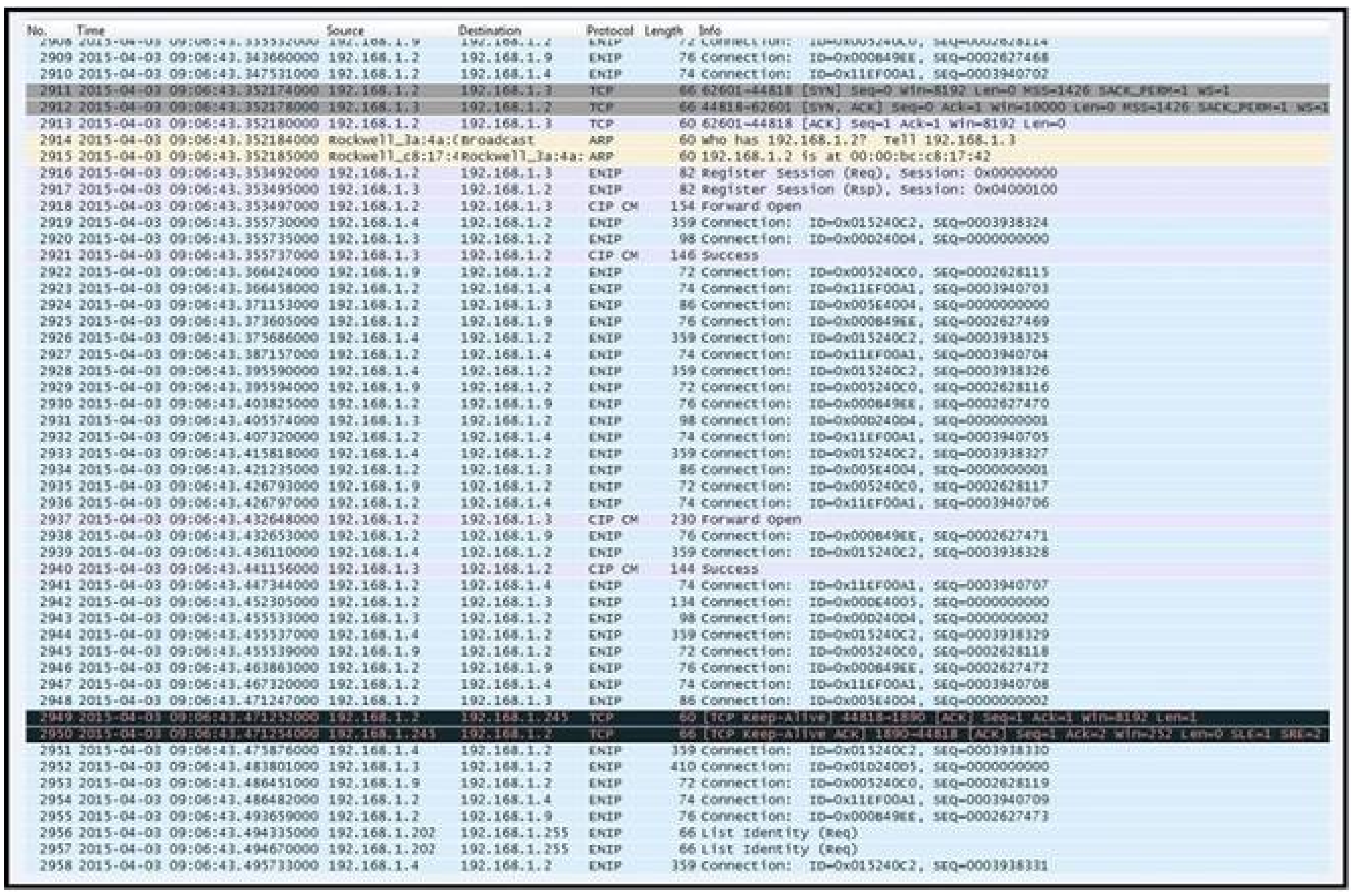
Answer: A

NEW QUESTION 7
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 8
Refer to the exhibit. Which lines represent an I/O connection running at a 20ms RPI?



```
No.  Time                          Source             Destination        Protocol Length Info
2908 2015-04-03 09:06:43.335552000 192.168.1.9        192.168.1.2        ENIP      72 Connection:  ID=0x005240C0, SEQ=0002628114
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_3a:4a:(Broadcast         ARP       60 Who has 192.168.1.2?  Tell 192.168.1.3
2915 2015-04-03 09:06:43.352185000 Rockwell_c8:17:4Rockwell_3a: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=0x005E4004, 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=0x005E4004, 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=0x000E4005, SEQ=0000000000
2943 2015-04-03 09:06:43.455533000 192.168.1.3        192.168.1.2        ENIP      98 Connection:  ID=0x00D240D4, SEQ=0000000002
2944 2015-04-03 09:06:43.455537000 192.168.1.4        192.168.1.2        ENIP     359 Connection:  ID=0x015240C2, SEQ=0003938329
2945 2015-04-03 09:06:43.455539000 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=0x005E4004, 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=252 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 9
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 10
Which prompt is used to configure parameters for the Ethernet ports of an industrial switch?

A. Switch(config-if)#
B. Switch(config-if-ind)#
C. Switch(config-line)#
D. Switch(config-ind)#
E. Switch(config-vlan)#

Answer: A

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 verfied 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 15
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 17
You are a 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 21
Which scenario represents the correct configuration to support the SSIDs of this autonomous access point?

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

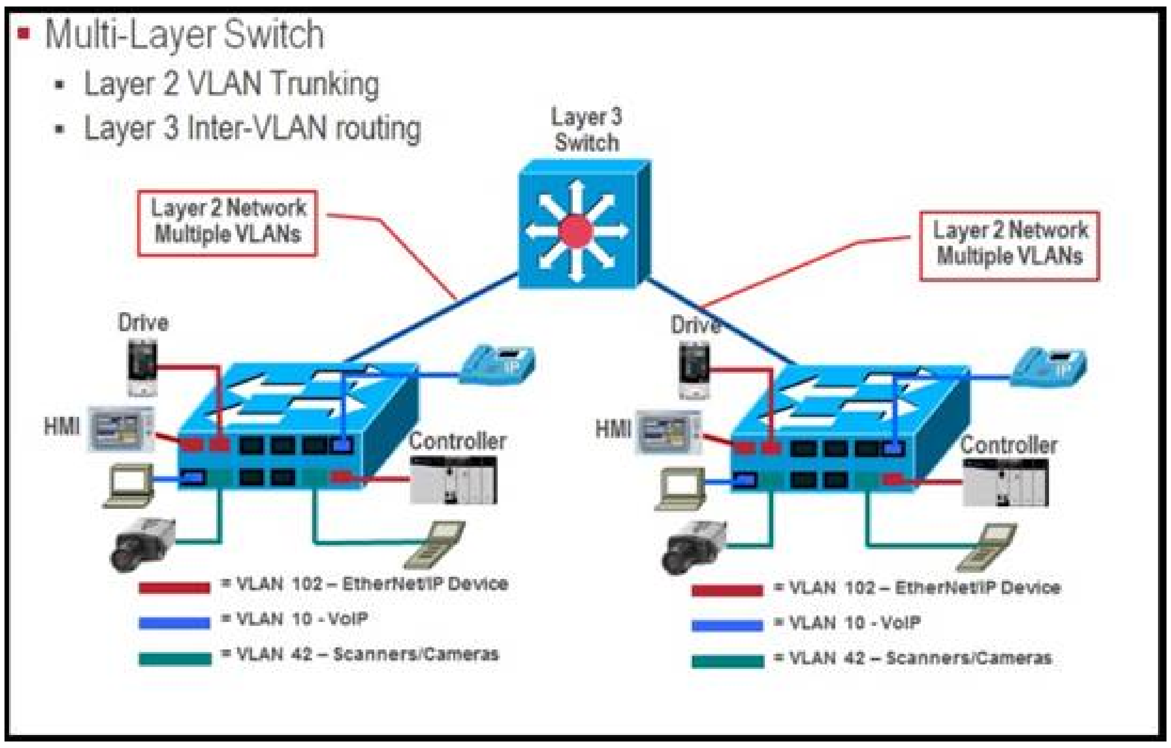
Answer: D

NEW QUESTION 26
It is common to use Resilient Ethernet Protocol (REP) on the manufacturing floor as a resiliency protocol, as opposed to the Enterprise where it is not generally deployed. What are two reasons why REP is more suitable for the plant floor? (Choose two)

A. REP is only supported on Industrial Ethernet switches, it is not supported on Catalyst switches.
B. REP converges faster than Spanning Tree, allowing for greater network availability.
C. REP supports Industrial Ethernet protocols better because it moves the packets faster.
D. Running dual cables from access switches to an aggregation switch can have a much higher cost on the plant floor than in the Enterprise and running a ring protocol like REP provides resiliency at a lower cost.
E. Industrial protocols can be negatively impacted by the number of nodes the Ethernet frame traverses, REP provides a topology with no more than 3 nodes for any data path.

Answer: BD

NEW QUESTION 31
Exhibit:



- Multi-Layer Switch
  - Layer 2 VLAN Trunking
  - Layer 3 Inter-VLAN routing

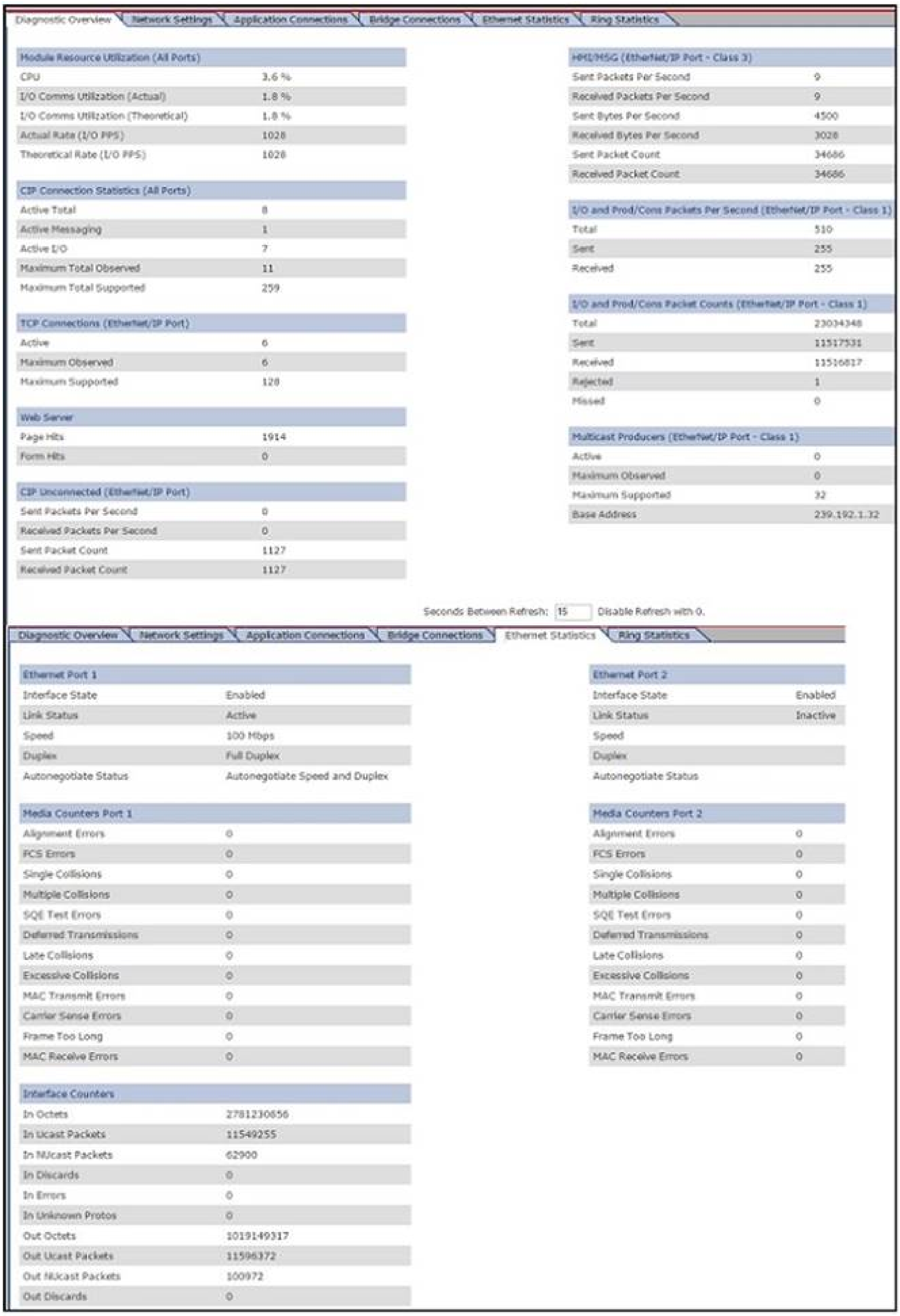
Layer 3 Switch
Layer 2 Network Multiple VLANs
Layer 2 Network Multiple VLANs
Drive
HMI
Controller
Drive
HMI
Controller
🟥 = VLAN 102 – EtherNet/IP Device
🟦 = VLAN 10 - VoIP
🟩 = VLAN 42 – Scanners/Cameras
🟥 = VLAN 102 – EtherNet/IP Device
🟦 = VLAN 10 - VoIP
🟩 = VLAN 42 – Scanners/Cameras

Refer to the exhibit. What are three traffic and interconnection requirements for the devices in the exhibit? (Choose three.)

A. The EtherNet/IP drive connections are in a high-voltage area and need protection from electromagnetic noise, so shielded cable that is rated for 600 V is advised.
B. EtherNet/IP devices such as the controller, drive, VoIP phone, and IP camera should be in the same VLAN.
C. CIP traffic has the highest bandwidth requirement so it needs the highest QoS setting.
D. EtherNet/IP drive traffic has high sensitivity to random drops, latency, and jitter.
E. Real-time motion control and VoIP traffic can share the same VLAN with the proper QoS setting.
F. IEEE1588 and PTP are important for ensuring real-time synchronization.

Answer: ADF

NEW QUESTION 32
Refer to the exhibit.



Module Resource Utilization (All Ports)	
CPU	3.6 %
I/O Comms Utilization (Actual)	1.8 %
I/O Comms Utilization (Theoretical)	1.8 %
Actual Rate (I/O PPS)	1028
Theoretical Rate (I/O PPS)	1028

CIP Connection Statistics (All Ports)	
Active Total	8
Active Messaging	1
Active I/O	7
Maximum Total Observed	11
Maximum Total Supported	259

TCP Connections (Ethernet/IP Port)	
Active	6
Maximum Observed	6
Maximum Supported	128

Web Server	
Page Hits	1914
Form Hits	0

CIP Unconnected (Ethernet/IP Port)	
Sent Packets Per Second	0
Received Packets Per Second	0
Sent Packet Count	1127
Received Packet Count	1127

HMI/MSG (Ethernet/IP Port - Class 3)	
Sent Packets Per Second	9
Received Packets Per Second	9
Sent Bytes Per Second	4500
Received Bytes Per Second	3028
Sent Packet Count	34686
Received Packet Count	34686

I/O and Prod/Cons Packets Per Second (Ethernet/IP Port - Class 1)	
Total	510
Sent	255
Received	255

I/O and Prod/Cons Packet Counts (Ethernet/IP Port - Class 1)	
Total	23034348
Sent	11517531
Received	11516817
Rejected	1
Missed	0

Multicast Producers (Ethernet/IP Port - Class 1)	
Active	0
Maximum Observed	0
Maximum Supported	32
Base Address	239.192.1.32

Seconds Between Refresh: 15 Disable Refresh with 0.

Ethernet Port 1	
Interface State	Enabled
Link Status	Active
Speed	100 Mbps
Duplex	Full Duplex
Autonegotiate Status	Autonegotiate Speed and Duplex

Ethernet Port 2	
Interface State	Enabled
Link Status	Inactive
Speed	
Duplex	
Autonegotiate Status	

Media Counters Port 1	
Alignment Errors	0
FCS Errors	0
Single Collisions	0
Multiple Collisions	0
SQE Test Errors	0
Deferred Transmissions	0
Late Collisions	0
Excessive Collisions	0
MAC Transmit Errors	0
Carrier Sense Errors	0
Frame Too Long	0
MAC Receive Errors	0

Media Counters Port 2	
Alignment Errors	0
FCS Errors	0
Single Collisions	0
Multiple Collisions	0
SQE Test Errors	0
Deferred Transmissions	0
Late Collisions	0
Excessive Collisions	0
MAC Transmit Errors	0
Carrier Sense Errors	0
Frame Too Long	0
MAC Receive Errors	0

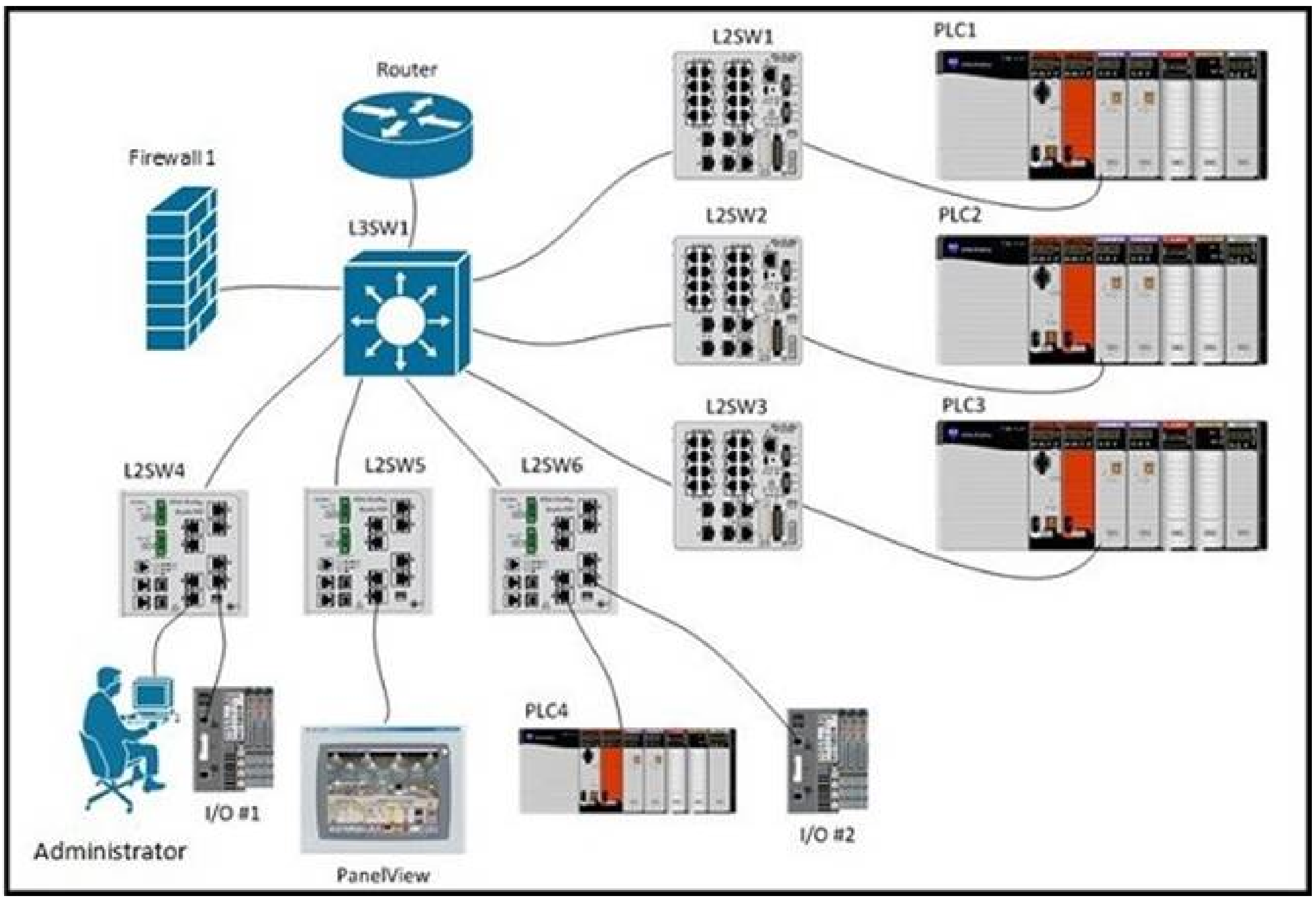
Interface Counters	
In Octets	2781230656
In Ucast Packets	11549255
In NUcast Packets	62900
In Discards	0
In Errors	0
In Unknown Protos	0
Out Octets	1019149317
Out Ucast Packets	11596372
Out NUcast Packets	100972
Out Discards	0

Which two parameters can be used to diagnose an overloaded system? (Choose two)

A. Ethernet Port 1 Speed
B. Module Resource Allocation Actual Rate
C. Class 3 Received bytes per second
D. Media Counters Alignment Errors
E. TCP Connections Active

Answer: BE

NEW QUESTION 33
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 37

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 42

Which best describes the difference between 802.11n and 802.11ac?

A. 802.11ac offers more channels over more bands than 802.11n
B. 802.11ac MCS 1 is about twice as fast as 802.11n MCS1
C. 802.11ac offers more modulation schemes than 802.11n
D. 802.11ac 1SS MCS 9 is allowed over a 20, 40, 80 and 160 MHz channel, while 802.11n 1SS MCS 9 is only allowed over a 20 or 40 MHz channel.

Answer: C

NEW QUESTION 47

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 enoug
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 enoug
H. RPVST+ is a suitable resiliency protocol for CIP motion.

Answer: B

NEW QUESTION 50
Given a ring topology, which loop prevention mechanism provides the fastest reconvergence time after a link failure?

A. Rapid Per-VLAN Spanning Tree Protocol
B. Resilient Ethernet Protocol
C. Multiple Spanning Tree Protocol
D. Spanning Tree Protocol

Answer: B

NEW QUESTION 55
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 59
What security component can be deployed to increase the defense in depth and specifically can be positioned against 'man-in-the-middle' attack?

A. Deploy 802.1AE
B. Deploy 802.1X
C. Deploy 802.1Q
D. Deploy 802.1AX

Answer: A

NEW QUESTION 61
What are the two most relevant factors in determining the class of administration that is required to maintain the telecommunications infrastructure? (Choose two.)

A. the size of the infrastructure
B. the complexity of the infrastructure
C. the age of the infrastructure
D. the industry that the infrastructure supports
E. the physical environment of the infrastructure

Answer: AB

NEW QUESTION 66
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 70
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. Lattency 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 73
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 74
What are three Cisco best practices for running I/O control traffic in a wireless environment? (Choose three)

A. 3200 packets per second and 20% bandwidth for HMI and maintenance traffic.
B. 2200 packets per second and 20% bandwidth for HMI and maintenance traffic
C. I/O control traffic can be run on 2.4 or 5 GHZ channels
D. I/O control traffic should be run on 5GHZ channels only
E. Standard I/O RPIs less than 20ms are not practical for wireless media because the maximum latency and jitter become comparable or greater than the RPI
F. Standard I/O RPIs less than 10ms are not practical for wireless media because the maximum latency and jitter become comparable or greater than the RPI

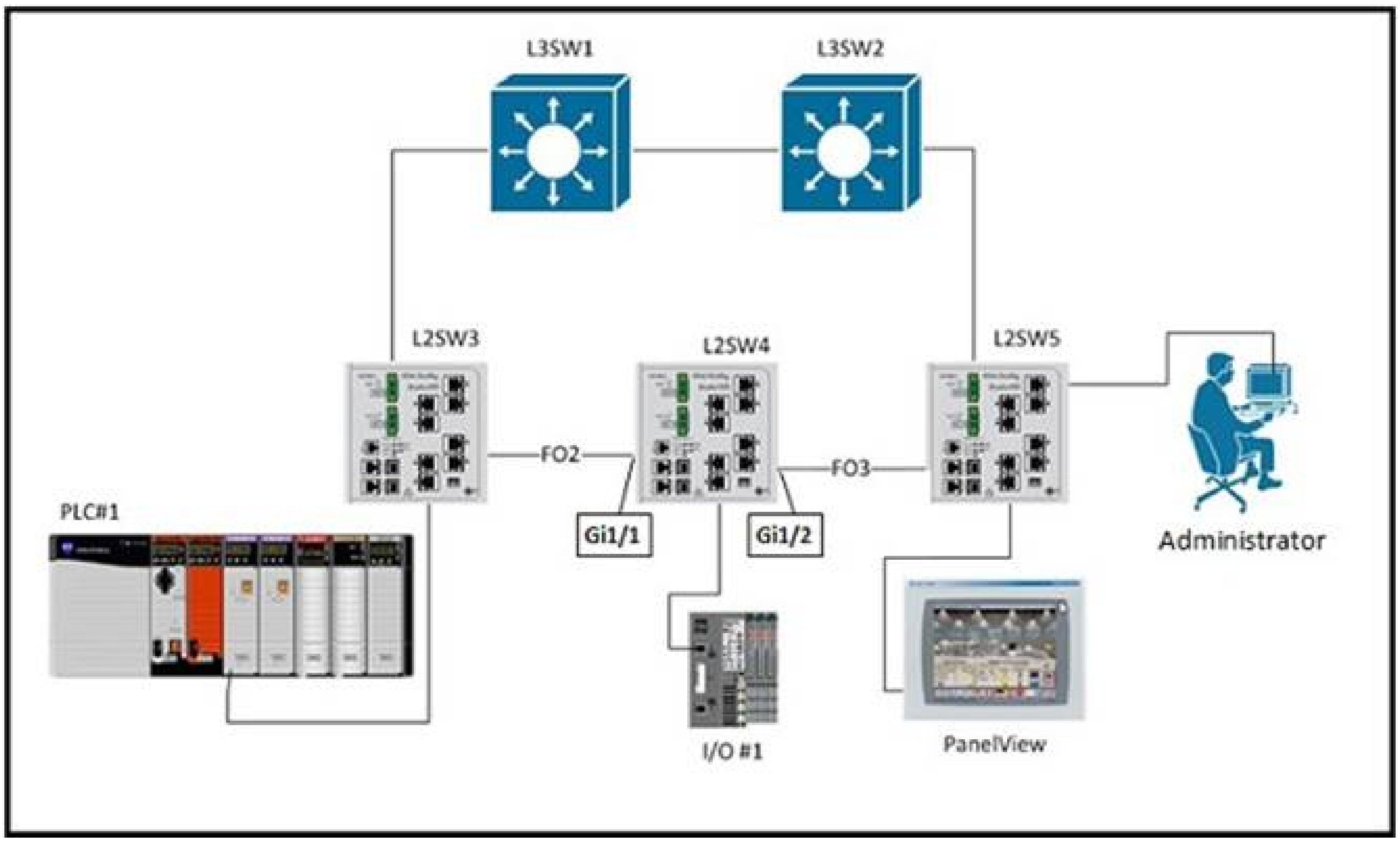
Answer: BDF

NEW QUESTION 79
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 81
Refer to the exhibit.



CIP Implicit messages from I/O#1 are being marked IP DSCP 47 by the endpoint and this
marking is trusted by L2SW4. L2SW4 is configured to map DSCP 47 to output queue 1 threshold 1. You have received feedback that some of these messages are not being received. Executing the show mls interface GigabitEthernet statistics command on L2SW4 results in:
L2SW4# show mls interface GigabitEthernet 1/1 statistics
<output omitted>
output queues dropped:
queue: threshold1 threshold2 threshold3 queue 0 0 0 0
queue 1 309232345 450 0
queue 2 300 10 0
queue 3 91 0 0
Repeating this command results in the counters incrementing for queue 1 threshold 1. What are two options for reducing the packet loss on this interface while preserving the end-to-end DSCP marking? (Choose two)

A. Configure I/O#1 to mark this traffic with a different DSCP that is mapped to a less congested queue
B. Increase the buffer allocation for input queue 1
C. Increase the buffer allocation for output queue 1
D. Alter the service policy to police to a higher CIR
E. Change the egress queue map on L2SW4 to map this traffic to a less congested queue

Answer: CE

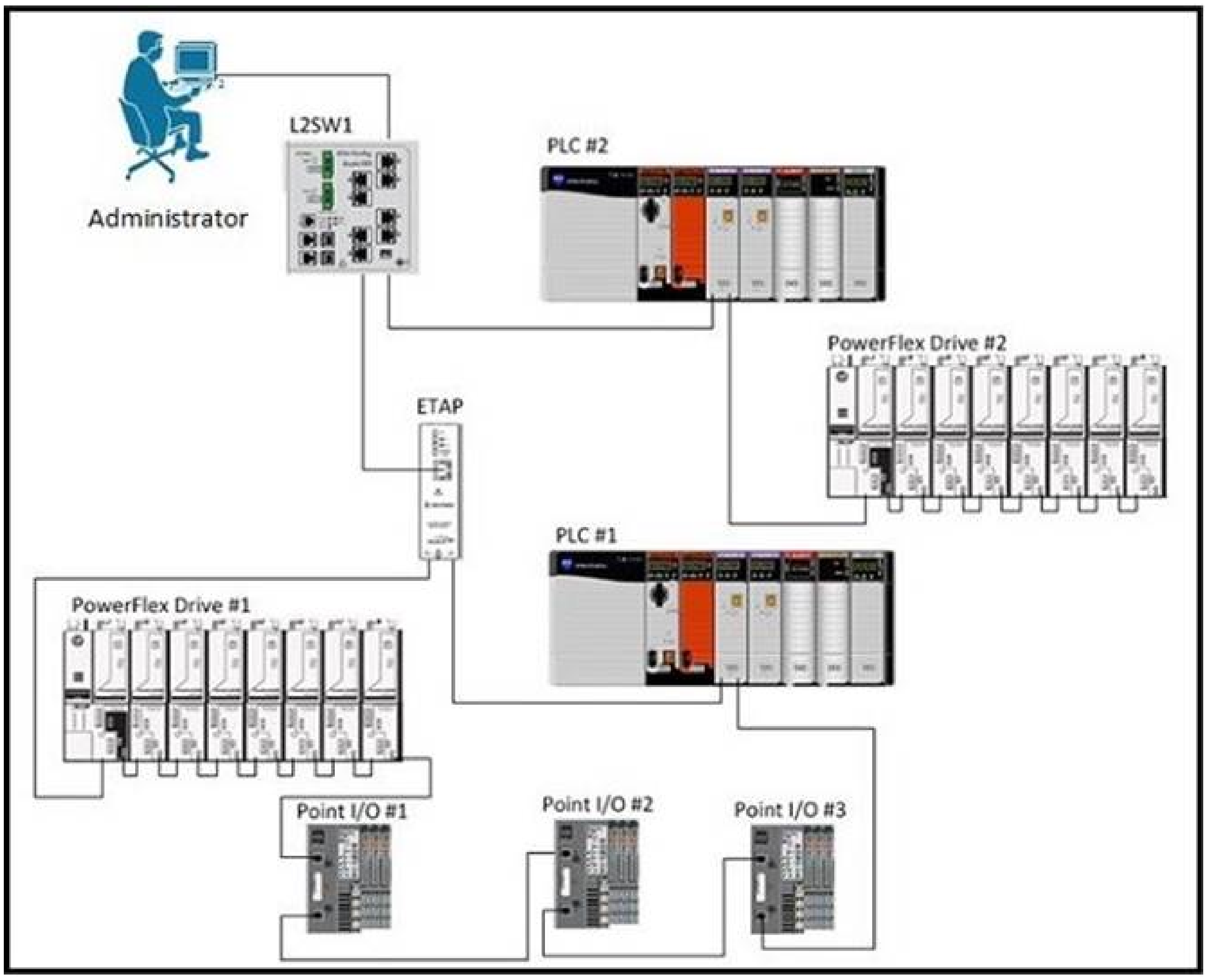
NEW QUESTION 84
How are I/O timeout and Safety I/O timeout calculated?

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/Otimeout 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 88
Refer to the exhibit.



An expansion project added an E-Tap and Device Level Ring to interface FastEthernet1/1 of L2SW1. The administrator has looked at the logs of L2SW1 and found that FastEthernet1/1 was in an error-disabled state.Using command line access on L2SW1, the administrator issued the following commands in configuration mode:
L2SW1(config)# interface FastEthernet 1/1 L2SW1(config-if)# shutdown L2SW1(config-if)# no shutdown
The administrator checked the logs of L2SW1 and found the following:
Mar 30 02:23:17.588: %PM-4-ERR_DISABLE: bpduguard error detected on Fa1/1, putting Fa1/1 in err-disable state
The administrator checked the software configuration of the switch port and found the following:
interface FastEthernet1/1 switchport access vlan 310 switchport mode access speed 100
duplex full no mdix auto
spanning-tree portfast
spanning-tree bpduguard enable
Why has the port gone error-disabled?

A. interface FastEthernet1/1 is configured as an access port on the wrong VLAN.
B. There is a duplex mismatch between interface FastEthernet1/1 and the E-Tap.
C. The E-Tap is not configured as a ring supervisor causing a loop on interface FastEthernet1/1.
D. The E-Tap is configured at 10Mbps and the switch port is configured at 100Mbps.
E. Automatic MDI Crossover detection is disabled.

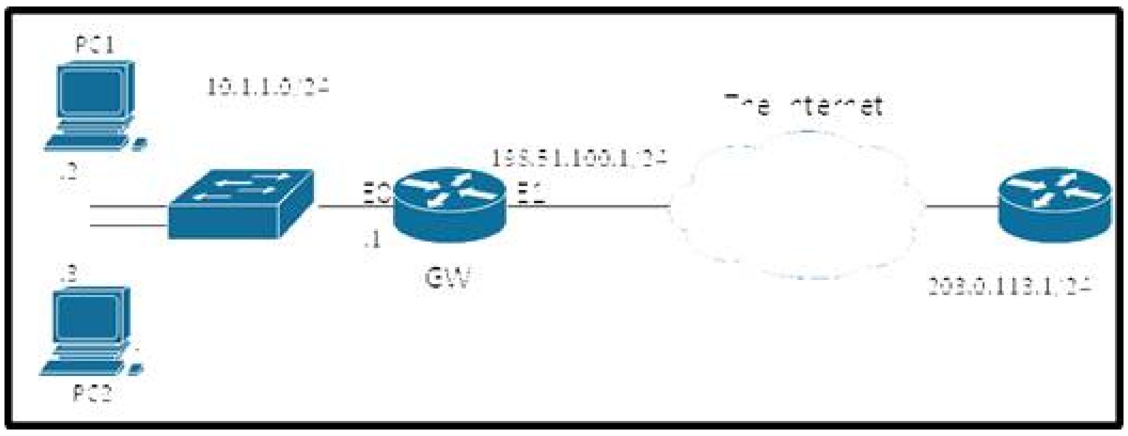
Answer: C

NEW QUESTION 90
Your controller has a high performance EtherNet/IP interface with port speed of >30,000 packets per second and 80% spare capacity. A new PowerFlex 753 drive will be added to the system with an RPI of 2ms and has been connected to a switch; you have been asked to set up the switch port. You open the EDS file and see that the drive will support 16 CIP connections and has transmit and receive capacity of 1,000 control packets per second.
What do you set as the storm control pps threshold limit for the port?

A. 16
B. 1,000
C. 2,500
D. 25,000

Answer: C

NEW QUESTION 92
Refer to the exhibit.



Which three options are needed to configure NAT on router GW so PC1 and PC2 will be able to ping 203.0.113.1? (Choose three)

A. interface Ethernet0 ip nat insideinterface Ethernet1 ip nat outside
B. ip access-list standard ACL_NAT permit 10.1.1.0 0.0.0.255
C. ip nat inside source static tcp 10.1.1.0 80 interface Ethernet1 80
D. interface Ethernet0 ip nat outside interface Ethernet1 ip nat inside
E. ip nat inside source list ACL_NAT interface Ethernet1 overload
F. ip access-list extended ACL_NAT permit tcp 10.1.1.0 0.0.0.255 any eq 80

Answer: ABE

NEW QUESTION 93
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 98
AP CAPWAP control traffic should be isolated from wireless client traffic. Which scenario represents the correct configuration to support the SSIDs of this controller-based access point in FlexConnect local switching mode?

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

Answer: C

NEW QUESTION 102
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

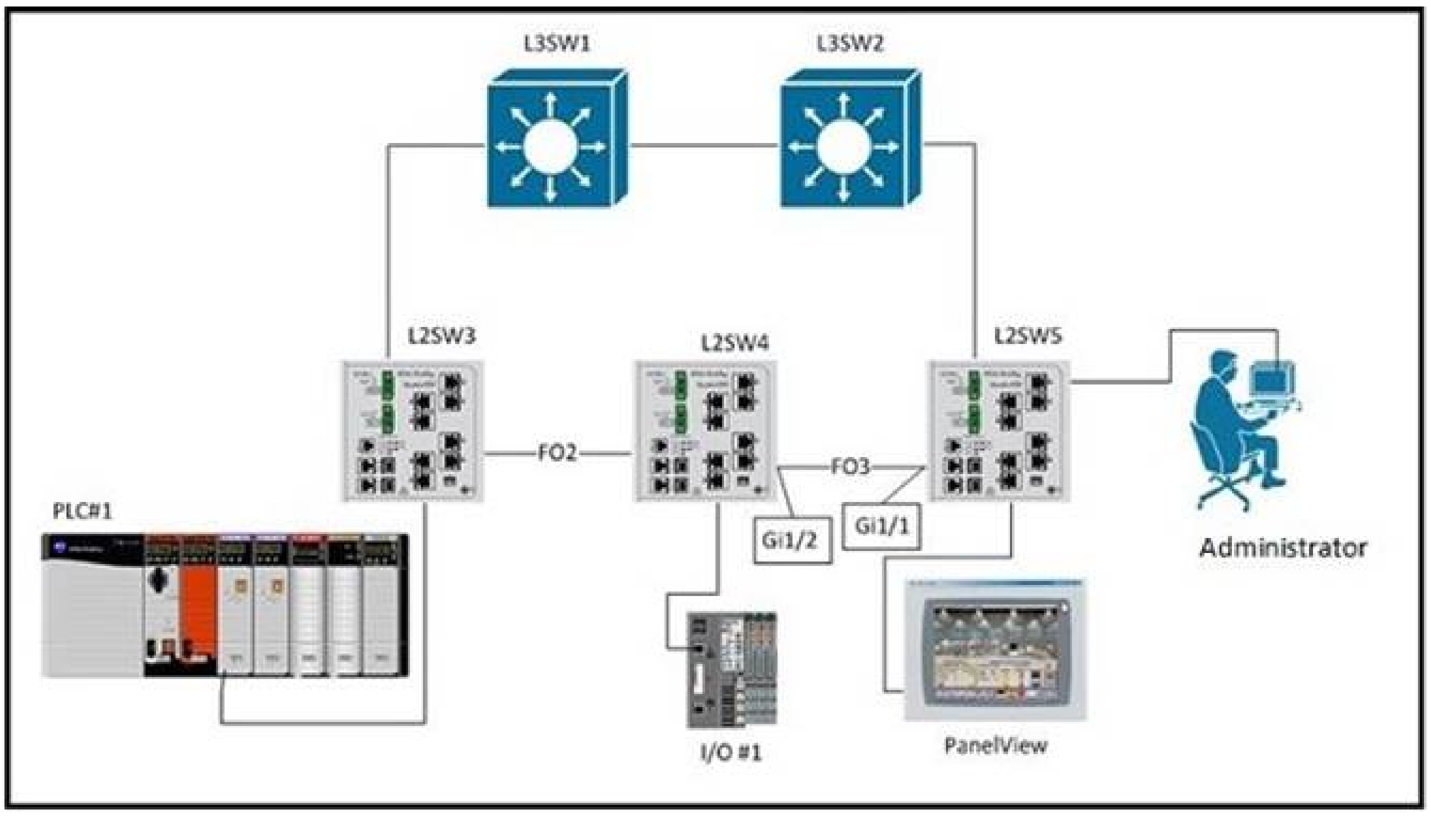
Answer: A

NEW QUESTION 104
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 108
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 111
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

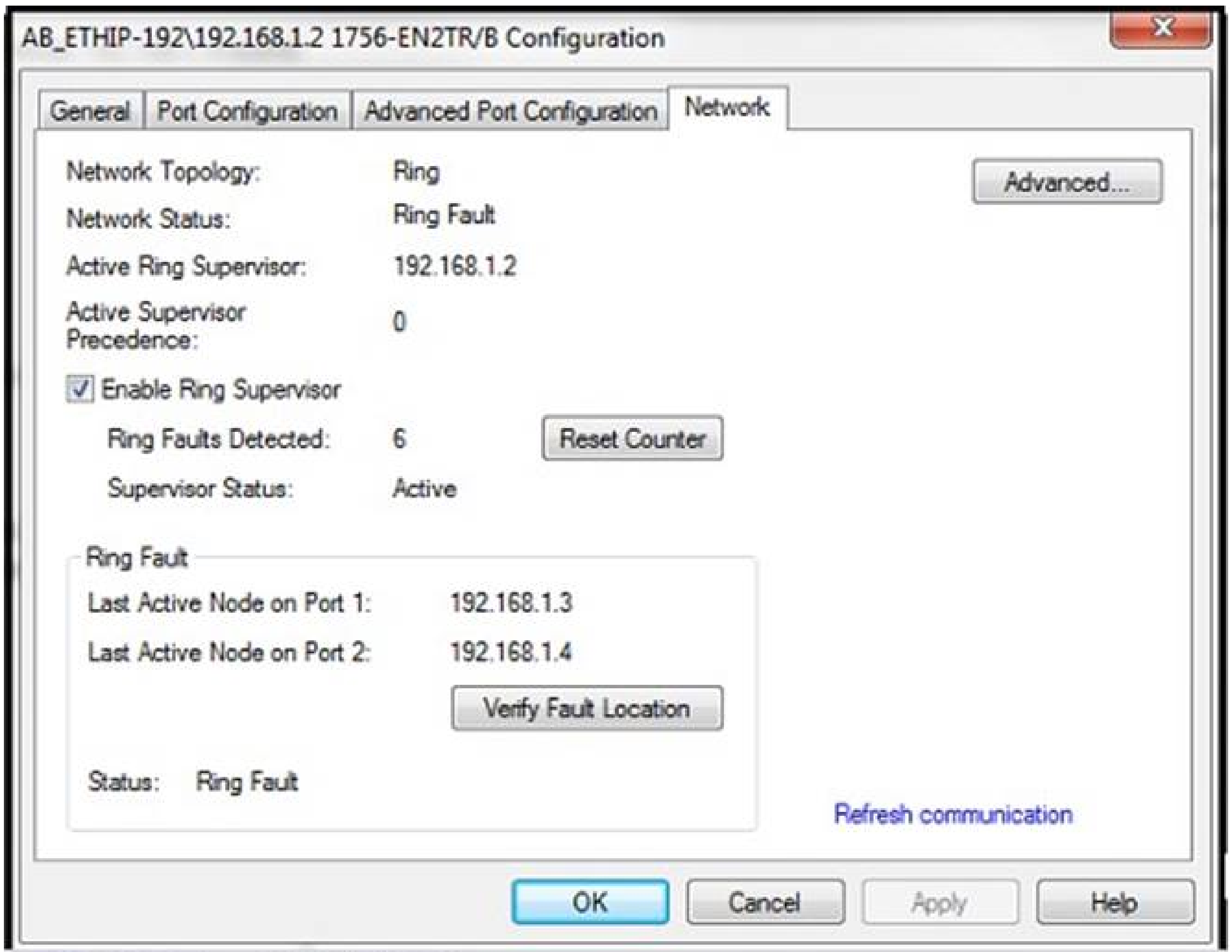
Answer: A

NEW QUESTION 114
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 116
Refer to the exhibit.



AB_ETHIP-192\192.168.1.2 1756-EN2TR/B Configuration

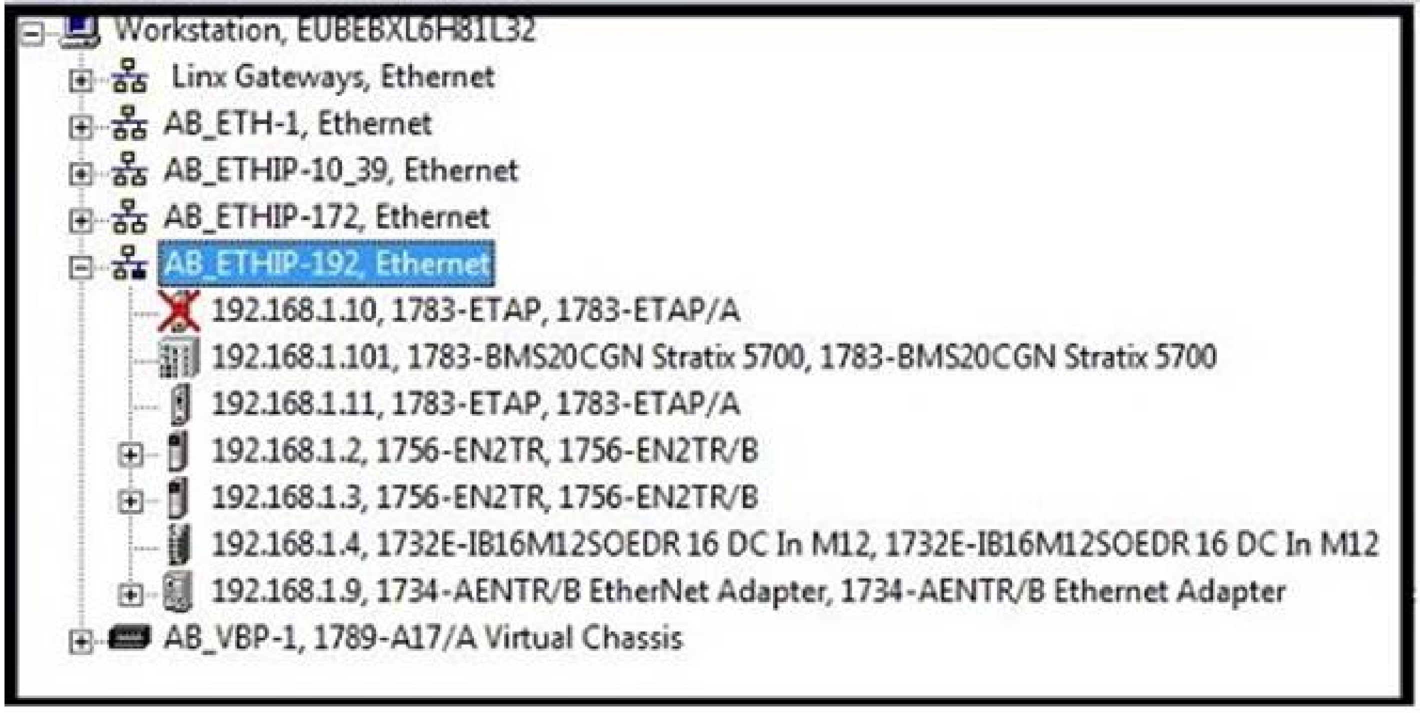
Network Topology: Ring
Network Status: Ring Fault
Active Ring Supervisor: 192.168.1.2
Active Supervisor Precedence: 0

☑ Enable Ring Supervisor

Ring Faults Detected: 6
Supervisor Status: Active

Ring Fault
Last Active Node on Port 1: 192.168.1.3
Last Active Node on Port 2: 192.168.1.4

Status: Ring Fault



```
Workstation, EUBEBXL6H81L32
    Linx Gateways, Ethernet
    AB_ETH-1, Ethernet
    AB_ETHIP-10_39, Ethernet
    AB_ETHIP-172, Ethernet
    AB_ETHIP-192, Ethernet
        192.168.1.10, 1783-ETAP, 1783-ETAP/A
        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 RSLinx. Which most accurately represents the network configuration?

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

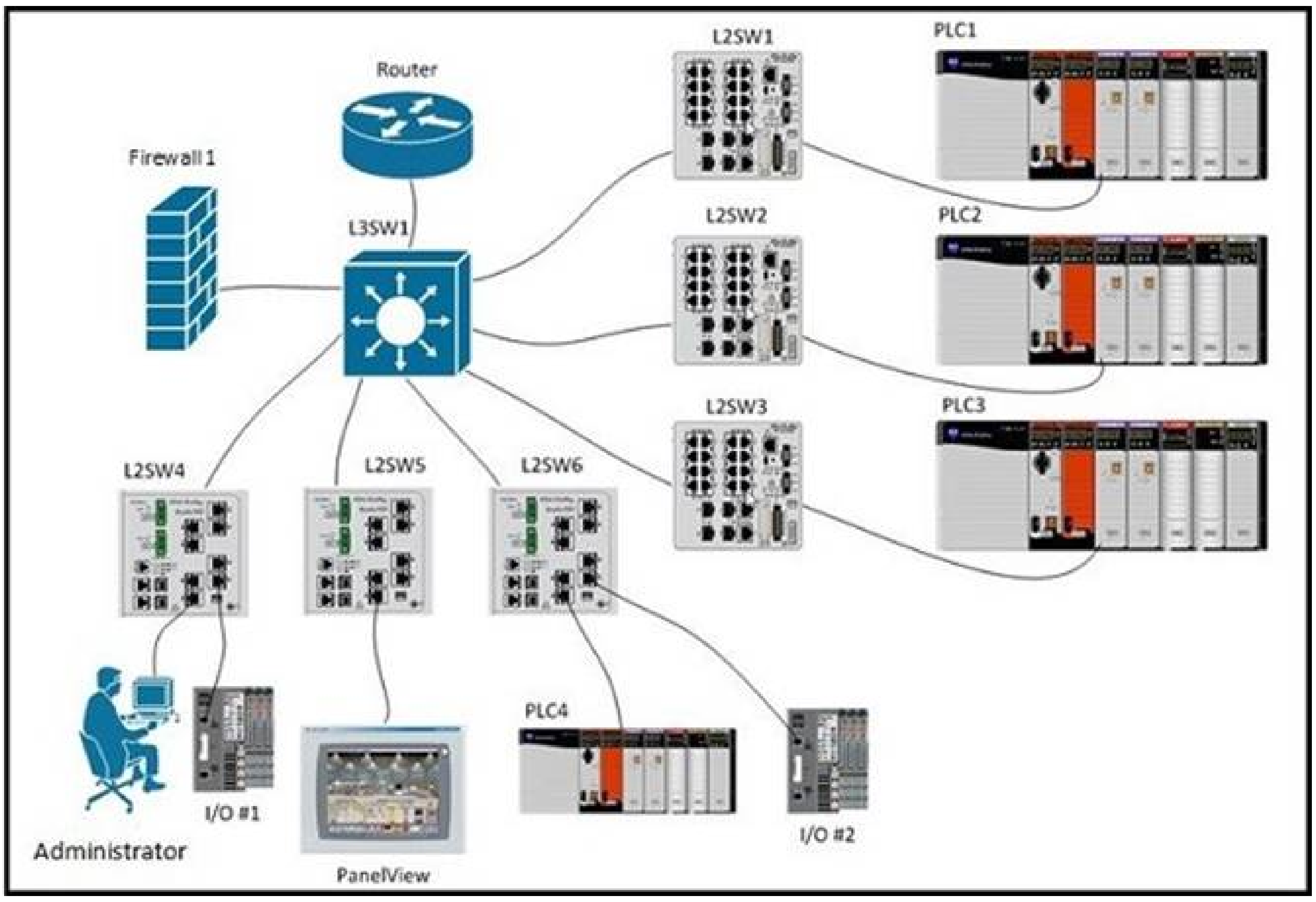
Answer: B

NEW QUESTION 119
Which in-depth approach is used when deploying defense in an industrial zone?

A. Besides using a dedicated firewall / DMZ construction use an IOS based firewall on the WAN router connecting the industrial site to the Internet.
B. Use NTP to make sure that time stamps of log messages are synchronized such that you can do root cause analysis.
C. Deploy an IDS solution with knowledge about industrial protocols in the industrial zone in combination with a firewall.
D. Use multiple firewalls from different vendors in such a way that network traffic will have to traverse both firewalls so that security holes of one firewall is caught by the other firewall.

Answer: C

NEW QUESTION 124
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:

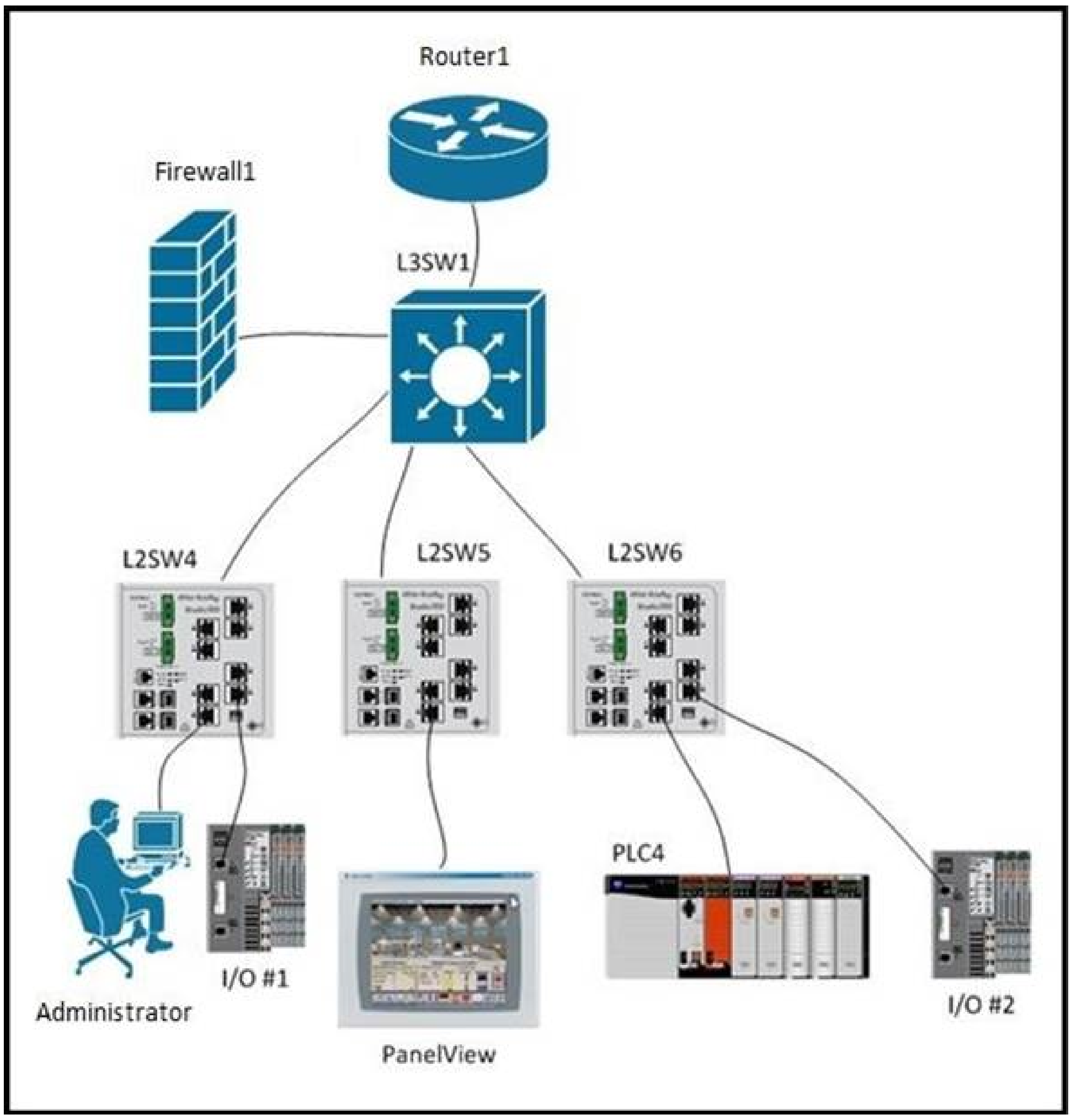
```
L3SW1# show run interface
interface Vlan1 no ip address shutdown
!
interface Vlan191
ip address 10.10.27.125 255.255.255.192
ip helper-address 165.28.96.96
ip helper-address 165.28.32.235 no ip redirects
standby 191 ip 10.10.27.126
standby 191 priority 120
standby 191 preempt delay minimum 90 no 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 129
Refer to the exhibit.



You are required to implement traffic segmentation in the network. See the table for relevant device details:
L2SW4, L2SW5, and L2SW6 are connected to L3SW1 with 802.1Q trunks with VLAN 191 and VLAN 398 allowed on the trunk.
You have the following information from L3SW1:

```
L3SW1# show run interfaces
interface Vlan1 no ip address shutdown
!
interface Vlan2
ip address 10.2.2.2 255.255.255.248
!
interface Vlan191
ip address 10.10.27.126 255.255.255.192
!
interface Vlan200
ip address 10.20.20.1 255.255.255.248
!
interface Vlan398
ip address 10.15.153.1 255.255.255.0
L3SW1# show ip route
*** Output Omitted ***
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks C 10.2.2.1/29 is directly connected, Vlan2
C 10.10.27.64/26 is directly connected, Vlan191 C 10.15.153.0/24 is directly connected, Vlan398 C 10.20.20.0/29 is directly connected, Vlan200 S
10.200.200.0/24 [1/0] via 10.20.20.2
S* 0.0.0.0/0 [1/0] via 10.2.2.1
```

You are required to implement a configuration that will meet the following connectivity requirements:
• The Administrator's Station must have full access to PanelView
• PanelView should have limited access, based on specific TCP ports, to PLC#1 and I/O#1
• The Administrator's Station should have no access to PLC#1 and I/O#1
• PLC#1 and I/O#1 should be able to communicate with each other on any port Which action will allow you to meet the connectivity requirements?

A. Put interface VLAN 191 and interface VLAN 398 into different Virtual Routing and Forwarding (VRF) instances on L3SW1
B. Deploy an inbound ACL on interface VLAN 191 to control the traffic from the Administrator's Station and PanelView to PLC#1 and I/O#1
C. No change is required, the traffic is already limited appropriately by the VLAN segmentation
D. Implement an ACL on Firewall1 to control the traffic flow between VLAN 191 and VLAN 398

Answer: B

NEW QUESTION 133
When troubleshooting a high packet loss condition in the network, the inspection area has an assessed M.I.C.E. value of M=1, I=1, C=3 and E=1. Which condition could be suspect?

A. Use of shielded Patch Cables, Bonded on one end only.
B. Use of unshielded Patch Cables.
C. Broken seal on bulkhead connector.
D. Oxidation on Shielded RJ45 Patch Plug

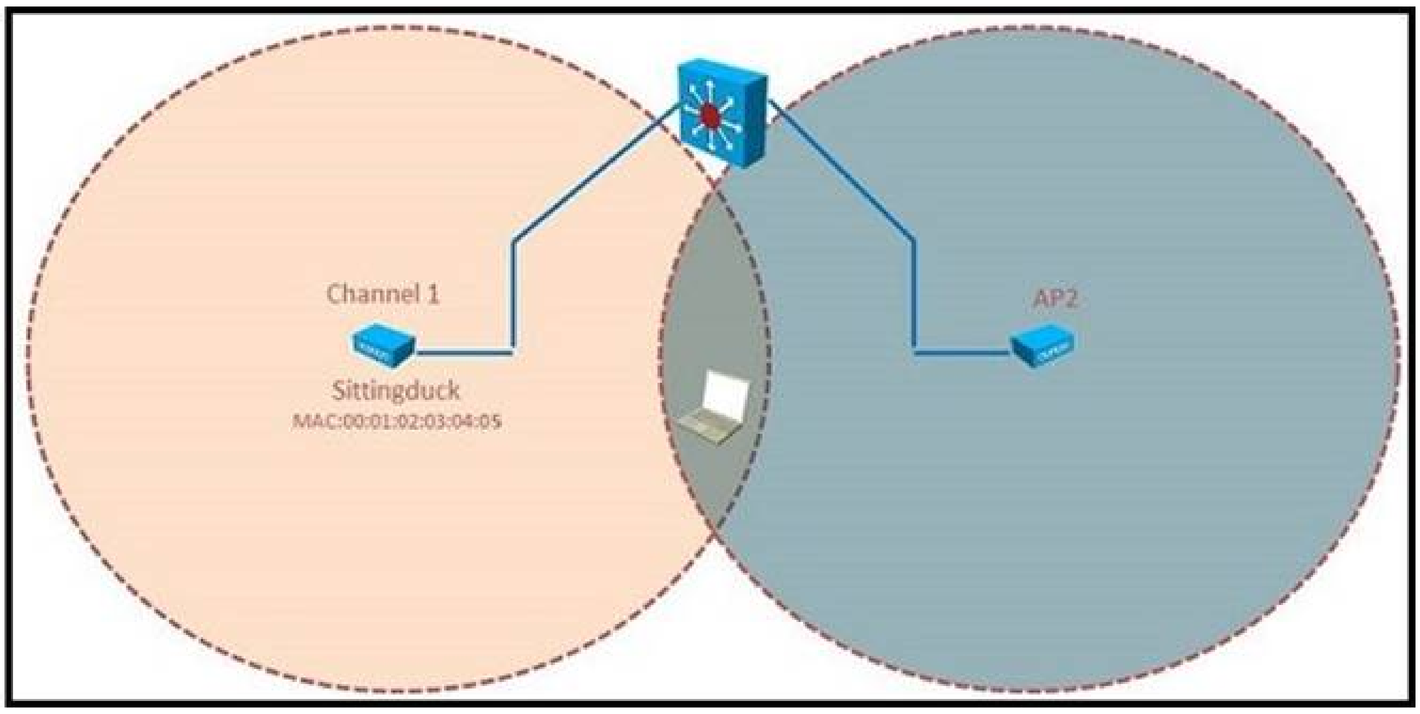
Answer: D

NEW QUESTION 137
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 141
Refer to the exhibit.



Which values are correct for AP 2 to allow for efficient roaming?

A. Channel 6, SSID Sittingduck, BSSID 00:0a:0b:0c:0d:0e
B. Channel 1, SSID Sittingduck, BSSID 00:01:02:03:04:05
C. Channel 1, SSID Sittingduck, BSSID 00:0a:0b:0c:0d:0e
D. Channel 6, SSID Sittingduck, BSSID 00:01:02:03:04:05

Answer: A

NEW QUESTION 144
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 146
......