All ENCOR (350-401) AND ENSARI (300-410) Commands Scott Empson Patrick Gargano

VLAN can support its own instance of spanning tree. VLANs can be extended across multiple interconnected switches by tagging the VLAN number on each Ethernet frame transmitted or received between them. This tagging of frames is supported by 802.1Q trunking.

*Creating Static VLANs using VLAN Configuration Mode*

Static VLANS occur when a switch port is manually assigned by the network administrator to belong to a VLAN. Each port is associated with a specific VLAN. By default, all ports are originally assigned to VLAN 1. You create VLANs using the VLAN configuration mode. VLAN database mode has been deprecated in IOS Version 15.

* Switch (config) # vlan 3 – Creates VLAN 3 and enters VLAN configuration mode for further definitions.
* Switch(config-vlan) # name Engineering – Assigns a name to the VLAN. The length of the name can be from 1 to 32 characters.
* Switch (config-vlan) # exit – applies changes, increases the VTP revision number by 1, and returns to global configuration mode. Note the VLAN is not created until you exit VLAN configuration mode

Use this method to add normal-range VLANs (1-1005) or extended-range VLANs (1006-4094). Configuration information for normal-range VLANs is always saved in the VLAN database, and you can display this information by entering the show vlan privileged EXEC command. The VLAN Trunking Protocol (VTP) revision number is increased by one each time a VLAN is created or changed. VTP Version 3 supports propagation of extended-range VLANs. VTP Versions 1 and 2 propagate only VLANs 1-1005. Transparent mode does not increment the VTP revision number.

*Assigning Ports to Data and Voice VLANs*

* Switch (config) # interface fastethernet 0/1 moves to interface configuration mode
* Switchport mode access # sets the port to access mode
* Switchport access vlan 10 – assigns this port to data VLAN 10
* Switchport voice vlan 11 – Assigns this port to include tagged voice frames in VLAN 11

When the switchport mode access command is used, the port will operate as a nontrunking single VLAN interface that transmits and receives untagged frames. An access port can only belong to one VLAN. When the switchport voice command is used together with the switchport access command, a pseudo-trunk is created allowing two VLANs on the port, one for voice traffic and one for all other traffic. The voice traffic is forwarded in 802.1Q tagged frames and the remaining nonvoice VLAN has no 802.1Q tagging (native VLAN). The internal mini-switch in a Cisco VoIP phone will pass untagged frames to an attached PC and forward 802.1Q tagged VoIP traffic with a differentiated services code point (DSCP) quality of service (QoS) value of EF (or Expedited Forwarding) to the switch port. In this special case, the switch port can belong to two VLANs, one for data and one for voice traffic.

*Using the range Command*

* Interface range fastethernet 0/1 – 9 enables you to set the same configuration parameters on multiple ports at the same time. Depending on the model of switch, there is a space before and after the hyphen in the interface range command. Be careful with your typing.
* Switch (config-if-range) # switchport mode access – Sets ports 1-9 as access ports.
* Switch (config-if-range) # switchport access vlan 10 – assigns ports 1-9 to VLAN 10.
* Switch (config-if-range) # switchport voice vlan 11 – assigns ports 1-9 to include tagged voice frames in VLAN 11

*Dynamic Trunking Protocol (DTP)*

* Switch (config) # interface fastethernet 0/1 – moves to interface configuration mode
* Switch (config-if) # switchport mode dynamic desirable – makes the interface actively attempt to convert the link to a trunk link. With the switchport mode dynamic desirable command set, the interface becomes a trunk link if the neighboring interface is set to trunk, desirable, or auto.
* Switch (config-if) # switch port mode dynamic auto – Makes the interface able to convert into a trunk link. With the switchport mode dynamic auto command set, the interface becomes a trunk link if the neighboring interface is set to trunk or desirable.
* Switch (config-if) # switchport nonegotiate – Prevents the interface from generating DTP frames. Use the switchport mode nonegotiate only when the interface switchport command is access or trunk. You must manually configure the neighboring interface to establish a trunk link.
* Switch (config-if) # switchport mode trunk – puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. With the switchport mode trunk command set, the interface becomes a trunk link even if the neighboring interface is not a trunk link.

The default mode is dependent on the platform. For the 2960/9200 series, the default mode is dynamic auto. On a 2960/9200 series switch, the default for all ports is to be an access port. However, with the default DTP mode being dynamic auto, an access port can be converted into a trunk port if that port receives DTP information from the other side of the link and htat other side is set to trunk or desirable. It is therefore recommended that you hard-code all access ports as access ports with the switchport mode access command. This way, DTP information will not inadvertently change an access port to a trunk port. Any port with the switchport mode access command ignores any DTP requests to convert the link. VLAN Trunking Protocol (VTP) domain names must match for a DTP to negotiate a trunk.

*Setting the Trunk Encapsulation and Allowed VLANs*

Depending on the series of switch that you are using, you may have a choice as to what type of trunk encapsulation you want to use: The Cisco proprietary Inter-Switch Link (ISL) or IEEE 802.1Q (dot1q). Cisco ISL has been deprecated. Depending on the age and the model of your Cisco switch, you may still be able to change the encapsulation type between dot1q and ISL. The 2960, 2960-x, and 9200 series of switches support only dot1q trunk-ing. Therefore, some commands such as switchport trunk encapsulation {isl | dot1q} are not available.

* Switch (config) # interface fastethernet 0/1 – moves to interface configuration mode
* Switch (config-if) # switchport mode trunk – puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link
* Switch (config-if) # switchport trunk encapsulation isl - Specifies ISL encapsulation on the trunk link. This command is only available on switches that support ISL.
* Switch (config-if) # switchport trunk encapsulation dot1q – Specifies 802.1Q encapsulation on the trunk link. This command may not be required on newer switches.
* Switch (config-if) # switchport trunk encapsulation negotiate – Specifies that the interface negotiate with the neighboring interface to become either an ISL or dot1q trunk, depending on the capabilities or configuration of the neighboring interface. This command may not be required on newer switches.
* Switch (config-if) # switchport trunk allowed vlan 10,12,18-22 – Configures the list of VLANs allowed on the trunk. All VLANs are allowed by default.
* Switch (config-if) # switchport trunk allowed vlan add 44, 47-49 - Configures the list of VLANs to add to the existing VLANs allowed on the trunk.
* Switch (config-if) # switchport trunk allowed vlan remove 44,47-49 – Configures the list of VLANs to remove from the existing VLANs allowed on the trunk.

*VLAN Trunking Protocol (VTP)*

VTP is a Cisco proprietary protocol that allows for VLAN configuration (addition, deletion or renaming of VLANs) to be consistently maintained across a common administrative domain.

* Switch (config) # vtp mode client – Changes the switch to VTP client mode.
* Switch (config) # vtp mode server – Changes the switch to VTP server mode. By default, all Catalyst switches are in server mode.
* Switch (config) # vtp mode transparent – Changes the switch to VTP transparent mode.
* Switch (config) # no vtp mode – Returns the switch to the default VTP server mode.
* Switch (config) # vt domain **domain-name** – Configures the VTP domain name. The name can be from 1 to 32 characters long and is case sensitive. All switches operating in VTP server or client mode must have the same domain name to ensure communication.
* Switch (config) # vtp password **password** – Configures a VTP password. In Cisco IOS Software Release 12.3 and later, the password is an ASCII string from 1 to 32 characters long. If you are using a Cisco IOS Software release earlier than 12.3, the password length ranges from 8 to 64 characters long. To communicate with each other, all switches must have the same VTP password set.
* Switch (config) # vtp version **number** – Sets the VTP Version to Version 1, Version 2, or Version 3. VTP sessions are not interoperable. All switches must use the same version (with V1 and V2). The biggest difference between Versions 1 and 2 is that Version 2 has support for Token Ring VLANs. Version 3 has added new features such as the creation of a VTP primary server to prevent the accidental deletion of VLANs that occurred in V1 and V2. V3 also supports extended VLANs, private VLANs, Multiple Spanning Tree Protocol (MSTP), and the ability to be disabled per interface as well as globally. VTP Version 3 is compatible with Version 2, but not Version 1.
* Switch # vtp primary – changes the operation state of a switch from a secondary server (the default state) to a primary server and advertises the configuration to the domain. If the switch password is configured as hidden, you are prompted to reenter the password. This happens only if configured in Version 2. This prompt occurs in privileged EXEC mode but not in global configuration mode. The vtp primary-server [vlan | mst | force] commands are only available on older model switches. On newer switches running more recent IOS/IOS-XE, use the vtp primary [vlan | mst | force] command instead.
* Switch # vtp primary vlan – (Optional) Configures the device as the primary VTP server for VLANs.
* Switch # vtp primary mst – (Optional) Configures the devices as the primary VTP server for the multiple spanning tree (MST) feature.
* Switch # vtp primary force – (Optional) Configures the device to not check for conflicting devices when configuring the primary server.
* Switch (config) # vtp pruning – Enables VTP pruning. By default, VTP pruning is disabled. You need to enable VTP pruning on only one switch in VTP server mode.

Only VLANs included in the pruning-eligible list can be pruned. VLANs 2 through 1001 are pruning eligible by default on trunk ports. Reserved VLANs and extended-range VLANs cannot be pruned. To change which eligible VLANs can be pruned, use the interface-specific switchport trunk pruning vlan command.

* Switch (config-if) # switchport trunk pruning vlan remove 4,20-30 ! Removes VLANs 4 and 20-30
* Switch (config-if) # switchport trunk pruning vlan except 40-50 ! All VLANs are added to the pruning list except for 40-50

Due to the inherent risk in having VTP servers overwrite each other and cause VLANs to disappear, Cisco recommends as a best practice deploying VTP in transparent mode. If you are going to use a client/server model, use Version 3 and the use of a VTPv3 primary server to prevent accidental database overwrite.

*Verifying VTP*

* Switch # show vtp status – Displays general information about VTP configurations.
* Switch # show vtp counters – Displays the VTP counters for the switch.
* Switch # show vtp password – Displays the VTP passwords

If trunking has been established before VTP is set up, VTP information is propagated throughout the switch fabric almost immediately. However, because VTP information is advertised only every 300 seconds (5 minutes), unless a change has been made to force an update, it can take several minutes for VTP information to be propagated.

*Verifying VLAN Information*

* Switch # show vlan – Displays VLAN information
* Switch # show vlan brief – Displays VLAN information in brief
* Switch # show vlan id 2 – Displays information of VLAN 2 only
* Switch # show vlan name marketing – Displays information of VLAN named marketing only
* Switch # show interfaces trunk – Displays trunk ports, trunking modes, encapsulation, and native and allowed VLANs.
* Switch # show interfaces switchport – Displays the administrative and operational status of trunks, encapsulation, private VLAN, voice VLAN, and trunk VLAN pruning.
* Switch # show interface fastethernet 0/1 trunk – Displays the administrative and operational status of a trunking port

*Saving VLAN Configurations*

The stored configurations of VLANs 1 through 1005 are always saved in the VLAN database; the filename is v*lan.dat* and is stored in *flash:.* After creating or disabling a VLAN in VLAN configuration mode, the exit command will apply any new changes to the VLAN database. If you are using VTP transparent mode, the configurations are also saved in the running configurations, and can be saved to the startup configuration using the copy running-config startup-config command. If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration are used. The VLAN database revision number remains unchanged in the VLAN database.

*Erasing VLAN Configurations*

* Switch# delete flash:vlan.dat – Removes entire VLAN database from flash. Make sure there is no space between the colon : and the characters vlan.dat. You can potentially erase the contents of the flash with this command if the syntax is not correct. Make sure to read the output from the switch. If you need to cancel, press Ctrl + C to escape back to privileged mode: Delete filename [vlan.dat]? Delete flash:vlan.dat? [confirm] Switch #
* Switch (config) # interface fastethernet 0/5 – Moves to interface configuration mode
* Switch (config-if) # no switchport access vlan 5 – Removes port from VLAN 5 and reassigns to VLAN 1 (the default VLAN)
* Switch (config-if) # exit – Moves to global configuration mode
* Switch (config) # no vlan 5 – Removes VLAN 5 from the VLAN database

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch. You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005. When you delete a VLAN, any ports assigned to that VLAN become inactive. This “inactive” state can be seen using the show interfaces switchport command for the port or ports in question. The ports remain associated with the VLAN (and thus inactive) until you assign those ports to a defined VLAN. Therefore, it is recommended that you reassign ports to a new VLAN or the default VLAN before you delete a VLAN from the VLAN database.

*Configuration Example: VLANs*

Figure 1-1 shows the network topology for the configuration that follows, which demonstrates how to configure VLANs using the commands covered in this chapter.

3650 Switch

Switch > enable – Moves to privileged EXEC mode.

Switch # configure terminal – Moves to global configuration mode

Switch (config) # hostname Switch3650 – Sets the host name

Switch (config) # vtp mode server – Changes the switch to VTP server mode. Note that server is the default setting for a 3650 switch.

Switch3650 (config) # vtp domain ENCOR – Configures the VTP domain name to ENCOR.

Switch3650 (config) # vtp password Order66 – Sets the VTP password to Order66

Switch3650 (config) # vlan 10 – Creates VLAN 10 and enters VLAN configuration mode

Switch3650 (config-vlan) # name Admin – Assigns a name to the VLAN

Switch3650(config-vlan) # exit – Increases the revision number by 1 and returns to global configuration mode

Switch3650 (config) # vlan 20 – Creates VLAN 20 and enters VLAN configuration mode

Switch3650 (config-vlan) # name Accounting – Assigns a name to the VLAN

Switch3650 (config-vlan) # vlan 30 – Creates VLAN 30 and enters VLAN configuration mode. You do not have to exit back to global configuration mode to execute this command. The VTP revision number would be incremented because VLAN 20 was created.

Switch3650(config-vlan) # name Engineering – Assigns a name to VLAN.

Switch3650 (config-vlan) # exit – Exiting VLAN configuration mode adds VLAN 30 to the VLAN database, which increases the revision number by 1, and returns to global configuration mode.

Switch3650 (config) # interface range gigbitethernet 1/0/1-8 – Enables you set the same configuration parameters on multiple orts at the same time.

Switch3650 (config-if-response) # switchport mode access – Sets ports 1-8 as access ports

Switch3650 (config-if-range) # switchport access vlan 10 – Assigns ports 1-8 to VLAN 10

Switch3650 (config-if-range) # interface range gigabitethernet 1/0/9-15 – Enables you to set the configuration parameters on multiple ports at the same time

Switch3650 (config-if-range) # switchport mode access – Sets ports 9-15 as access ports

Switch3650 (config-if-range) # switchport access vlan 20 – Assigns ports 9-15 to VLAN 20

Switch3650 (config-if-range) # interface range gigabitethernet 1/0/16-24 – Enables you to set the same configuration parameters on multiple ports at the same time

Switch3650 (config-if-range) # switchport mode access – sets ports 16-24 as access ports

Switch3650 (config-if-range) # switchport access vlan 30 – Assigns ports 16-24 to VLAN 30

Switch3650 (config-if-range) # exit – Returns to global configuration mode

Switch3650 (config) # interface gigabitethernet 1/1/1 – Moves to interface configuration mode. Using this interface will require the installation of a Gigabit Ethernet SFP module in the appropriate uplink port

Switch3650 (config-if) # switchport mode trunk – Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link.

Switch3650 (config-if) # exit – Returns to global configuration mode

Switch3650 (config-if) # vtp version 3 – Enables VTP Version 3

Switch3650 (config) # vtp pruning – Enables VTP pruning on this switch

Switch3650 (config) # end – returns to privileged EXEC mode

Switch3650 # vtp primary vlan force – Configures the 3650 to be the VTP primary server

Switch3650 # copy running-conifg startup-config – Saves the configuration in NVRAM

2960 Switch

Switch> enable – Moves to privileged EXEC mode

Switch # configure terminal – moves to global configuration mode

Switch2960(config) # hostname Switch2960 – Sets the host name

Switch2960(config) # vtp mode client – Changes the switch to VTP server mode

Switch2960(config) # vtp domain ENCOR – Configures the VTP domain name to ENCOR

Switch2960(config) # vtp password Order66 – Sets the VTP password to Order66

Switch2960(config) # interface range fastethernet 0/1-8 – Enables you to set the same configuration parameters on multiple ports at the same time

Switch2960 (config-if-range) # switchport mode access – Sets ports 1-8 as access ports

Switch2960 (config-if-range) # switchport access vlan 10 – Assigns ports 1-8 to VLAN 10

Switch2960 (config-if-range) # interface range fastethernet 0/9-15 – Enables you to set the same configuration parammeters on multiple ports at the same time

Switch2960 (config-if-range) # interface range fastethernet 0/16-24 – Enables you to set the same configuration parameters on multiple ports at the same time

Switch2960 (config-if-range) # switchport mode access – sets ports 16-24 as access ports

Switch2960(config-if-range) # switchport access vlan 30 – Assigns ports 16-24 to VLAN 30

Switch2960(config-if) # switchport mode trunk – Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link

Switch2960(config-if) # exit – Returns to global configuration mode

Switch2960 (config) # vtp version 3 – Enables VTP Version 3 on this switch

Switch2960 (config) # vtp pruning – Enables VTP pruning on this switch

Switch2960(config) # exit – Returns to privileged EXEC mode

Switch2960# copy running-config startup-config – Saves the configuration in NVRAM

*Layer 2 Link Aggregation*

EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. An EtherChannel consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link. If a link within an EtherChannel fails, traffic previously carried over that failed link changes to the remaining links within the EtherChannel.

Table: Interface Modes in EtherChannel

Mode: On, Protocol: None, Description: Forces the interface into an EtherChannel without Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP). Channel only exists if connected to another interface group also in On mode.

Mode: Auto, Protocol: PAgP/Cisco, places the interface into an active negotiating state (will send PAgP packets to start negotiations)

Mode: Desirable, Protocol: PAgP/Cisco, Places the interface into an active negotiating state (will send PAgP packets to start negotiations)

Mode: Passive, Protocol: LACP/IEEE, Places the interface into a passive negotiating state (will respond to LACP packets but will not initiate LACP negotiation)

Mode: Active, Protocol: LACP/IEEE, Places the interface into an active negotiating state (will send LACP packets to start negotiation)

*Default EtherChannel Configuration*

Feature/Default Setting

Channel groups/None assigned

Port-channel logical interface/None defined

PAgP mode/No default

PAgP learn method/Aggregate-port learning on all ports

PAgP priority – 128 on all ports

LACP mode/No default

LACP learn method/aggregate port-learning on all ports

LACP port priority – 32768 on all ports

LACP system priority – 32768

LACP system ID – LACP system priority and the switch (or switch stack) MAC address

Load balancing – Load distribution on the switch is based on the source MAC address of the incoming packet

*Guidelines for Configuring EtherChannel*

* PAgP is Cisco proprietary and is not compatible with LACP
* LACP is defined in 802.3ad
* The number of supported EtherChannels varies by switch platform model. For instance, you can create up to 6 EtherChannels on a Cisco Catalyst 2960 access layer switch, 48 EtherChannels on a Catalyst 3560 L3 Switch, or up to 128 EtherChannels on a Catalyst 3650 switch.
* A single PAgP EtherChannel can be made by combining anywhere from two to eight parallel links
* A single LACP EtherChannel can be made by combining up to 16 Ethernet ports of the same type. Up to eight ports can be active and up to eight ports can be in standby mode.
* All ports must be identical:
  + Same speed and duplex
  + Cannot mix Fast Ethernet and Gigabit Ethernet
  + Cannot mix PAgP and LACP in a single EtherChannel
  + Can have PAgP and LACP EtherChannels on the same switch, but each EtherChannel must be exclusively PAgP or LACP
  + Must all be VLAN trunk or nontrunk operational states
* All links must be either Layer 2 or Layer 3 in a single channel group
* To create a channel in LACP, sides must be set to either:
  + Active-Active
  + Active-Passive
* To create a channel without using PAgP or LACP, sides must be set to On-On
* Do **not** configure a GigaStack gigabit interface converter (GBIC) as part of an EtherChannel
* An interface that is already configured to be a Switched Port Analyzer (SPAN) destination port will not join an EtherChannel group until SPAN is disabled
* Do **not** configure a secure port as part of an EtherChannel
* When using trunk links, ensure that all trunks are in the same mode—Inter-Switch Link (ISL) or 802.1Q (dot1q)
* Interfaces with different native VLANs cannot form an EtherChannel
* When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of the parameters, you must also make the changes to all the ports in the group:
  + Allowed-VLAN list
  + Spanning-tree path cost for each VLAN
  + Spanning-tree priority for each VLAN
  + Spanning-tree PortFast setting
* Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1X port. If you try to enable IEEE 802.1X on an EtherChannel port, an error message will appear, and IEEE 802.1X is not enabled.
* For a Layer 3 EtherChannel, assign the Layer 3 address to the port-channel logical interface, not the physical ports in the channel.

*Configuring a Layer 2 EtherChannel*

* Switch(config) # interface port-channel {number} – Specifies the port-channel interface. Once in the interface configuration mode, you can configure additional parameters just like for any other physical device.
* Switch(config) # interface range fastethernet 0/1-4 – Moves to interface range configuration mode.
* Switch(config-if-range) # channel-group 1 mode on – Creates channel group 1 as an EtherChannel and assigns interfaces FastEthernet 0/1 to 0/4 as part of it. The other end of the EtherChannel would need to be configured the same way for the link to work correctly.
* Switch(config-if-range) # channel-group 1 mode desirable – Creates channel group1 as a PAgP channel and assigns interfaces 01 to 04 as part of it. The other end of the EtherChannel would need to be configured either as desirable or auto for the link to work correctly.
* Switch(config-if-range) # channel-group 1 mode active – Creates channel group 1 as an LACP channel and assigns interfaces 01 to 05 as part of it. The other end of the EtherChannel would need to be configured either as active or passive for the link to work correctly.

If you enter the channel-group command in the physical port interface mode without first setting a port channel command in global configuration mode, the port channel will automatically be created for you.

*Configuring a Layer 3 EtherChannel*

* L3Switch (config) # interface port-channel {number} – Creates the port-channel logical interface and moves to interface configuration mode. Valid channel numbers are 1 to 128 for a 3650 series switch. For a 2960 series switch with L3 capabilities, the valid channel numbers are 1 to 6
* L3Switch(config-if) # no switchport – Puts the port channel into Layer 3 mode
* L3Switch(config-if) # ip address 172.16.10.1 255.255.255.0 – Assigns the IP address and netmask to the port channel
* L3Switch(config-if) # exit – Moves to global interface mode.
* L3Switch(config) # interface range gigabitethernet 1/0/20-24 – Moves to interface range configuration mode
* L3Swtich(config-if) # no switchport – Puts the interface into Layer 3 mode.
* L3Switch(config-if-range) # no ip address – Ensures that no IP addresses are assigned to the interfaces
* L3Switch (config-if-range) # channel-group 1 mode on – Creates channel group 1 as an EtherChannel and assigns interfaces 20 to 24 as part of it. The other end of the EtherChannel would need to be configured the same way for the link to work correctly.
* L3Switch(config-if-range) # channel-group 1 mode desirable – Creates channel group 1 as a PAgP channel and assigns interfaces 20 to 24 as part of it. The other end of the EtherChannel would need to be configured as desirable or auto for the link to work correctly.
* L3Switch(config-if-range) # channel-group 1 mode active – Creates channel group 1 as an LACP channel and assigns interfaces 20 to 24 as part of it. The other end of the EtherChannel would need to be configured either as passive or active for the link to work correctly. The channel group number must match the port channel number.

*Configuring EtherChannel Load Balancing*

* L3Switch (config) # port-channel load-balance src-mac – Configures an EtherChannel load-balancing method. The default value varies between different switch models. Select one of the following load-distribution methods:
  + Dst-ip – Specifies destination host IP address
  + Dst-mac – Specifies destination host MAC address of the incoming packet
  + Dst-mixed-ip-port – Specifies destination host IP address and the TCP/UDP port
  + Dst-port – Specfiies destination TCP/UDP port
  + Extended – Specifies extended load-balance methods (combination of source and destination methods beyond those available with the standard command)
  + Ipv6-label – Specifies the IPv6 Flow Label
  + L3-proto – Specifies the Layer 3 protocol
  + Src-dst-ip – Specifies the source and destination host IP address
  + Src-dst-mac – Specifies the source and destination MAC add
  + Src-dst-mixed-ip-port – Specifies the source and destination host IP address and TCP/UDP port
  + Src-ip – specifies source host IP address
  + Src-mac – Specifies source host MAC address (this is the default setting)
  + Src-mixed-ip-port – Specifies the source host IP address and the TCP/UDP port
  + Src-port – Specifies the source TCP/UDP port

*Configuring LACP Hot-Standby Ports*

When LACP is enabled, by default the software tries to configure the maximum number of LACP-compatible ports, up to a maximum of 16 ports. Only eight ports can be active at one time; the remaining eight links are placed into hot-standby mode. If one of the active links becomes inactive, a link in hot-standby mode becomes active in its place. You can overwrite the default behavior by specifying the number of active ports in a channel, in which case the remaining ports become hot-standby ports (if you only specify five ports in a channel, the remaining 11 ports become hot-standby ports). If you specify more than eight links for an EtherChannel group, the software automatically decides which of the hot-standby ports to make active based on LACP priority. For every link that operates in LACP, the software assigns a unique priority made up of the following (in priority order):

* LACP system priority
* System ID (the device MAC address)
* LACP port priority
* Port number
  + Switch(config) # interface port-channel 2 – Enters interface configuration mode for port channel 2. The range for port channels is 1 to 128.
  + Switch(config-if) # lacp max-bundle 3 – Specifies the maximum number of LACP ports in the port-channel bundle. The range is 1 to 8.
  + Switch(config-if) # port-channel min-links 3 – Specifies the minimum number of member ports (in this example, 3), that must be in the link-up state and bundled in the EtherChannel for the port-channel interface to transition to the link-up state. The range of this command is 2 to 8.
  + Switch (config-if) # exit – Returns to global configuration mode.
  + Switch (config) # lacp system-priority 32000 – Configures the LACP system priority. The range is 1 to 65535. The default is 32768. The lower the value, the higher the system priority.
  + Switch (config) # interface gigabitethernet 1/0/2 – Moves to interface configuration mode
  + Switch (config-if) # lacp port-priority 32000 – Configures the LACP port priority. The range is 1 to 65535. The default is 32768. The lower the value, the more likely that the port will be used for LACP transmission.
  + Switch (config-if) # end – Returns to privileged EXEC mode

*Monitoring and Verifying EtherChannel*

* Switch # show running-config – Displays a list of what is currently running on the device
* Switch # show running-config interface fastethernet 0/12 – Displays interface fastethernet 0/12 information
* Switch # show interfaces fastethernet 0/12 etherchannel – Displays EtherChannel information for specified interface
* Switch # show etherchannel – Displays all EtherChannel information
* Switch # show etherchannel 1 port-channel – Displays port channel information
* Switch # show lacp neighbor – Shows LACP neighbor information
* Switch # show pagp neighbor – shows PAgP neighbor information
* Switch # clear pagp 1 counters – Clears PAgP channel group 1 information
* Switch # clear lacp 1 counters – Clears LACP Channel group 1 information

*DLSwitch (3650)*

* Switch > enable – Moves to privileged EXEC mode
* Switch # configure terminal – Moves to global configuration mode
* Switch (config) # hostname DLSwitch – sets the host name
* DLSwitch (config) # vtp mode server – changes the switch to VTP server mode
* DLSwitch(config) # vtp domain – Configures the VTP domain name to **testdomain**
* DLSwitch(config) # vlan 10 – Creates VLAN 10 and enters VLAN configuration mode
* DLSwitch (config-vlan) # name Accounting – Assigns a name to the VLAN
* DLSwitch (config-vlan) # exit – Returns to global configuration mode
* DLSwitch(config) # vlan 20 – Creates VLAN 20 and enters VLAN configuration mode
* DLSwitch(config-vlan) # name Marketing – Assigns a name to the VLAN
* DSwtich(config-vlan) # exit – returns to global configuration mode

**Instructions for the Practice Test**

When preparing for the CBAP exam, following specific instructions for the practice test can help maximize your study efficiency. Here are some key points to keep in mind:

* **Time Management**: Allocate 210 minutes for the practice test, mirroring the actual exam duration.
* **Number of Questions**: Engage with 150 multiple-choice questions to simulate the exam experience accurately.
* **Multiple Attempts**: Feel free to retake the practice exam multiple times to reinforce your learning and identify areas for improvement.
* **Review Answers**: After completing the test, review your answers to understand your mistakes and clarify concepts where necessary.
* **Focus Areas**: Pay attention to questions that challenge you the most; these may highlight areas that require additional study.

By adhering to these instructions, you can effectively utilize the cbap practice test to enhance your readiness for the CBAP certification.

**CBAP Mock Questions (Answers after the questions section)**

**Case 1**

Owing to increased regulatory scrutiny, overwhelming number of regulations, and complex market, credit and operational risks, financial institution FinTech Corp Inc. felt the need to adopt a more effective and integrated GRC approach that would replace multiple systems catering to individual departments and functions.

FinTech Corp decides to go with Delaware Inc., an organization with a wealth of experience in the GRC solutioning space, amassed over 20 years in order to assist them with ensuring compliance with regulatory requirements, increased collaboration between teams and enhanced business performance.

Delaware’s Governance, Risk and Compliance solution called GRCPerfect has primarily been developed for the IT and ITES domain with the objective to help companies implement Governance, Quality, and Information Security Management Systems in an integrated manner. It has various modules, one of which is the project management module, where users can plan and track projects and programs using standards such as CMMI, ISO 9001, ISO 27001 etc.

Key benefits of deploying GRCPerfect are:

 Minimum 50% effort reduction in deploying GRC frameworks in the organization

* Unified tool to implement best practices from multiple-world class frameworks such as ISO (9001, 27001, 20000, 14000, 18000), CMMI, ITIL, Business
* Senior Management and client visibility into Organizational, Account and Project level performance parameters
* Improved data and metrics integrity, thus helping in better decision making
* Significant help in ongoing process sustenance beyond audit and assessment
* Complete automation of project management artifacts and reporting – significant savings on management effort

Key features of GRCPerfect are:

* Complete Program and Project Planning and Tracking supporting CMMI, ISO 9001, ISO 27001 and Agile
* Schedule, Defect, Effort, Risk, Issue, Change Requests, Quantitative Process Management, Sub-Process Metrics and other 40+ data capture needed by CMMI, ISO 9001 and ISO 27001
* Supports workflow for approvals in Time Sheet, Requests
* Supports flexible organizational hierarchy
* Complete role-based permissions for data confidentiality and integrity
* Multi-level view – From Organization to Account to Project
* Status and Metrics reports generated automatically from the system
* Built on industry standard Microsoft SQL Server and .Net
* Completely web-enabled and does not require any installation on user machines
* Light-weight interface making it suitable to work on internet
* Compliance management includes audit planning, tracking and reporting
* Best practices drawn from internationally renowned organizations
* Substantially reduced time and effort in model adoption and implementation
* Enables complete context and role-based view of policies and processes
* Configurable to company’s requirements
* Available to the Client as an Open-Code option which enables Client to obtain the source code of the product

FinTech Corp would like Delaware Inc. to customize the solution to suit its need. The business analyst from Delaware Inc. in discussion with the stakeholders of FinTech Corp has developed the following requirements:

**Q1:** FinTech Corp. has asked the BA to plan the GRC system such that it can handle an increased number of users anywhere between 1000 to 10000 in the next 5 years. The REQ2000 is missing which of the following characteristics?

1. Specific
2. Consistent
3. Concise
4. Feasible

**Q2:** FinTech Corp would like to have visual dashboards with Red, Green, Amber indicators providing its senior management with at a glance awareness of the organization’s current performance. How can the BA make requirement REQ7000 more specific?

1. The dashboard shall have color coded indicators like red, green etc.
2. The dashboard shall have colors coded indicators like red (#FF0000), amber (#FFFF00) and green (#00FF00)
3. The dashboard shall have the ability to drill down to the extent possible
4. The dashboard shall have three color coded indicators and the ability to drill down multiple levels

**Q3:** There’s a need from various project teams in FinTech Corp that the system must have a functionality to add attachments to various transaction documents and master records. How can the requirement REQ9000 be made unambiguous?

1. When a new attachment is added to the document, the application shall generate an attachment ID.
2. The system shall allow users to attach one or more images or documents in PDF, Word, Excel, PowerPoint and Visio format to the selected requirement.
3. The system shall allow users to manage attachment content.
4. The system shall not allow users to attach documents beyond a size limit.

**Q4:** As a web-based system may behave exactly as desired in one browser but might have issues in other browsers which may hamper the functionality of the solution, the key stakeholders have insisted on the ability of the solution to be easily viewed across different browsers. This requirement belongs to which NFR category?

1. Scalability
2. Security
3. Stability
4. Portability

**Q5:** Among the following requirements, which one will provide the maximum value to the stakeholders?

1. Having a visual dashboard indicating the issues tracked and resolved for the most important project so that senior management can focus on ways to enhance the performance of that particular project.
2. Allowing the project manager to view attachment related to work product, policies, guidelines within the schedule itself.
3. Having the ability to drill down and create open ended WBS for adding a large number of multiple tasks on an ongoing basis for long term, open-ended projects.
4. Ability to get an insight of the performance of all projects in the organization and be able to project revenue.

**Q6:**A is a business analyst for Project R. Stakeholder Z has good familiarity with traceability chains. Z insists that the project follows the approach. Business analyst A's response should be

1. Accept the stakeholder’s suggestion as traceability matrix is very popular.
2. Explain that there are many ways to maintain traceability.
3. Traceability is not required as the project is of medium complexity.
4. Maintain traceability only at feature level.

**Q7:**Stakeholder S provided the following requirement, “The system should be able to manage schedule”. The project glossary document does not describe the verb, Manage. It is possible that the term manage can be broken down further. The reason why the requirement needs revision is because the requirement is

1. Not clear.
2. Not atomic.
3. Not testable.
4. Not understandable.

**Q8:**While discussing with Implementation SMEs of Project X, Business analyst A finds that the implementation team is working on integrating a map feature. The same feature was already implemented in Project Q. The reason for repeat development could be because

1. Past requirements were not baselined.
2. Past requirements were not tested.
3. Past requirements were not maintained.
4. Past requirements were not packaged.

**Q9:** A works as the business analyst for a project to introduce a new electronic gadget. Projects such as this have been lengthy, involved multiple stakeholders, and included thousands of requirements. When selecting a business analysis approach for the project, which of the following is A most likely to consider?

1. A predictive approach because of the highly regulated environment
2. An adaptive approach because these approaches tend to be better for new products
3. The approach depends on more factors than are given
4. A combination of predictive and adaptive approaches; given the complexity of the project

**Q10:** A has scheduled a focus group to determine the current attitudes towards a new product that the company is developing. Stakeholder S suggests using the Kano model. Another stakeholder R argues that the group should use the benchmarking approach. What should business analyst A do?

1. Adopt the benchmarking approach as the stakeholder has high authority.
2. Explain that multiple techniques can’t be used for elicitation.
3. Since 'A' knows Kano model, choose the same.
4. Explain that multiple techniques can be used for elicitation.

**Q11:** A is a business analyst for Project P. A obtained signoff on requirements from three stakeholders; the sponsor, the project manager, and the product manager. The project management office rejected A's requirements for implementation due to insufficient signoffs. What should have A checked for?

1. Whether the requirements signoff was matching the RACI matrix.
2. Project manager's preference for signoff.
3. Lack of quality assurance team's signoff.
4. Lack of implementation team's signoff.

**Q12:**Business Analyst A is working on a project to automate several business processes. A just received confirmation of the budget and it is clear that there is enough money to either build an in-house solution or purchase a COTS package. What is the most logical next step for A?

1. Pursue an RFP.
2. Pursue an RFI.
3. Purchase a COTS product as budget is available.
4. Insist on developing an in-house solution.

**Q13:** Business analyst A is implementing a new order processing system for a direct marketer. A is concerned that with the holiday season approaching, the system’s performance may be inadequate. A could not find any document which has the application performance criteria mentioned. A would like to evaluate the performance of the system, but can’t because

1. The performance metrics have not been defined.
2. The stakeholder and solution requirements were incomplete and the stakeholders complained of poor solution performance.
3. When A gathered the actual performance metrics, A found that the solution performance was indeed better than anticipated.
4. Neither the solution validation nor the organizational readiness assessment had been completed.

**Q14:** Business analyst B uses hierarchical decomposition to break down B's business analysis deliverables into activities and tasks. B then adds the hours needed and can give an accurate estimate of the time needed to complete the BA work. What type of estimation has Business analyst B used?

1. Delphi estimation.
2. Historic analysis.
3. Parametric estimation.
4. Bottom-up estimation.

**Q15:** Business analyst A conducted several interviews this week for a project. Several problems have come up. As many issues have come up, A's project manager suggested that A tracks the issues formally in an item tracker. Why?

1. In order to use it for historical purposes and project planning by the project manager.
2. To ensure that the issues produced during elicitation are tracked down to resolution.
3. Used to ensure that the help desk and service management teams are kept in loop.
4. Issue tracking is not expected in agile based projects

**Question 1**

**Correct Option: A.**Specific

**Explanation:** REQ2000 does not clearly say how many number of users and hence is not specific.

**Question 2**

**Correct Option: B.**The dashboard shall have colors coded indicators like red (#FF0000), amber (#FFFF00) and green (#00FF00)

**Explanation:** Option b is specific as it also provides the color codes to avoid any kind of confusion.

**Question 3**

**Correct Option: B.**The system shall allow users to attach one or more images or documents in PDF, Word, Excel, PowerPoint and Visio format to the selected requirement.

**Explanation:** This requirement clearly tells in which format the attachments can be done.

**Question 4**

**Correct Option: D.**Portability

**Explanation:** Ability to work in multiple environments is Portability.

**Question 5**

**Correct Option: D.**Ability to get an insight of the performance of all projects in the organization and be able to project revenue.

**Explanation:** REQ6000 has a value of 5

**Question 6**

**Correct Option:** **B.**Explain that there are many ways to maintain traceability.

**Explanation:** All activities in business analysis can be carried in multiple ways and there is no unique best way.

Page vi - The BABOK® Guide should not be construed to mandate that the practices described in this publication should be followed under all circumstances. Any set of practices must be tailored to the specific conditions under which business analysis is being performed.

**Question 7**

**Correct Option:** **B.**Not atomic.

**Explanation:** Words like "Manage" can be broken down, so they are non-atomic.

BABoK V3.0 - Section 7.2.4 - Elements - Atomic - self-contained and capable of being understood independently of other requirements or designs.

**Question 8**

**Correct Option:** **C.**Past requirements were not maintained.

**Explanation:** Not maintaining requirements results in the same requirements being implemented multiple times. BABoK V3.0 - Section 5.2.1 - Purpose - The purpose of Maintain Requirements is to retain requirement accuracy and consistency throughout and beyond the change during the entire requirements life cycle, and to support reuse of requirements in other solutions.

**Question 9**

**Correct Option:** **C.** The approach depends on more factors than are given

**Explanation:** Remember; often the factors can be more than those given in the question

BABoK V3.0 - Section 3.1.4 - Elements - Paragraph 9 - Other considerations that may affect the approach include:

* the change is complex and high risk;
* the organization is in; or interacts with; heavily regulated industries;
* contracts or agreements necessitate formality;
* stakeholders are geographically distributed;
* resources are outsourced;
* staff turnover is high and/or team members may be inexperienced;
* requirements must be formally signed off; and
* business analysis information must be maintained long-term or handed over for use on future initiatives.

**Question 10**

**Correct Option: B.**Explain that multiple techniques can be used for elicitation.

**Explanation:** Techniques are not mutually exclusive. Point to remember.

BABoK V3.0 - Section 1.4.5 - Techniques - Techniques provide additional information on ways that a task may be performed. The list of techniques included in the BABOK® Guide is not exhaustive. There are multiple techniques that may be applied alternatively or in conjunction with other techniques to accomplish a task. Business analysts are encouraged to modify existing techniques or engineer new ones to best suit their situation and the goals of the tasks they perform.

**Question 11**

**Correct Option:** **A.**Whether the requirements signoff was matching the RACI matrix.

**Explanation:** Remember: All sign-offs are conducted as per the defined RACI matrix.

BABoK V3.0 - Section 3.1.4.6 - Acceptance - The business analysis approach is reviewed and agreed upon by key stakeholders. In some organizations, the business analysis process may be more structured and require key stakeholders to sign off on the approach to ensure all business analysis activities have been identified, estimates are realistic, and the proposed roles and responsibilities are correct.

**Question 12**

**Correct Option: B.**Pursue an RFI.

**Explanation:** It is always better to collect information before deciding. Availability of funds is one factor, not the only factor.

BABoK V3.0 - Section 10.49.2 - Description - The assessment may be formal through the submission of a Request for Information (RFI), Request for Quote (RFQ), Request for Tender (RFT), or Request for Proposal (RFP).

**Question 13**

**Correct Option: A.**The performance metrics have not been defined.

**Explanation:** The value of a solution is difficult to determine without defining the performance metrics. BABoK V3.0 - Section 8.2.4 - Elements - .1 Solution Performance versus Desired Value Business analysts examine the measures previously collected in order to assess their ability to help stakeholders understand the solution’s value.

**Question 14**

**Correct Option:** **D.**Bottom-up estimation.

**Explanation:** Work Breakdown Structure (WBS) approach helps in bottom-up estimation. BABoK V3.0 - Section 10.19.3 - Elements Paragraph 3 - Bottom-up: using the lowest-level elements of a hierarchical breakdown to examine the work in detail and estimate the individual cost or effort, and then summing across all elements to provide an overall estimate.

**Question 15**

**Correct Option:** **B.**To ensure that the issues produced during elicitation are tracked down to resolution.

**Explanation:** This is the main purpose of problem tracking. BABoK V3.0 - Section 10.26.1 - Purpose - Item tracking is used to capture and assign responsibility for issues and stakeholder concerns that pose an impact to the solution.