***Introduction to Configure Trunking between switches, WAPs, Servers***

***Understanding DTP and the Native VLAN***

The various modes of DTP and how they work.

Tagging done between switches with 802.1q Protocol

Tag Removed on Exiting Access Port

Trunk ports configured on each Interface

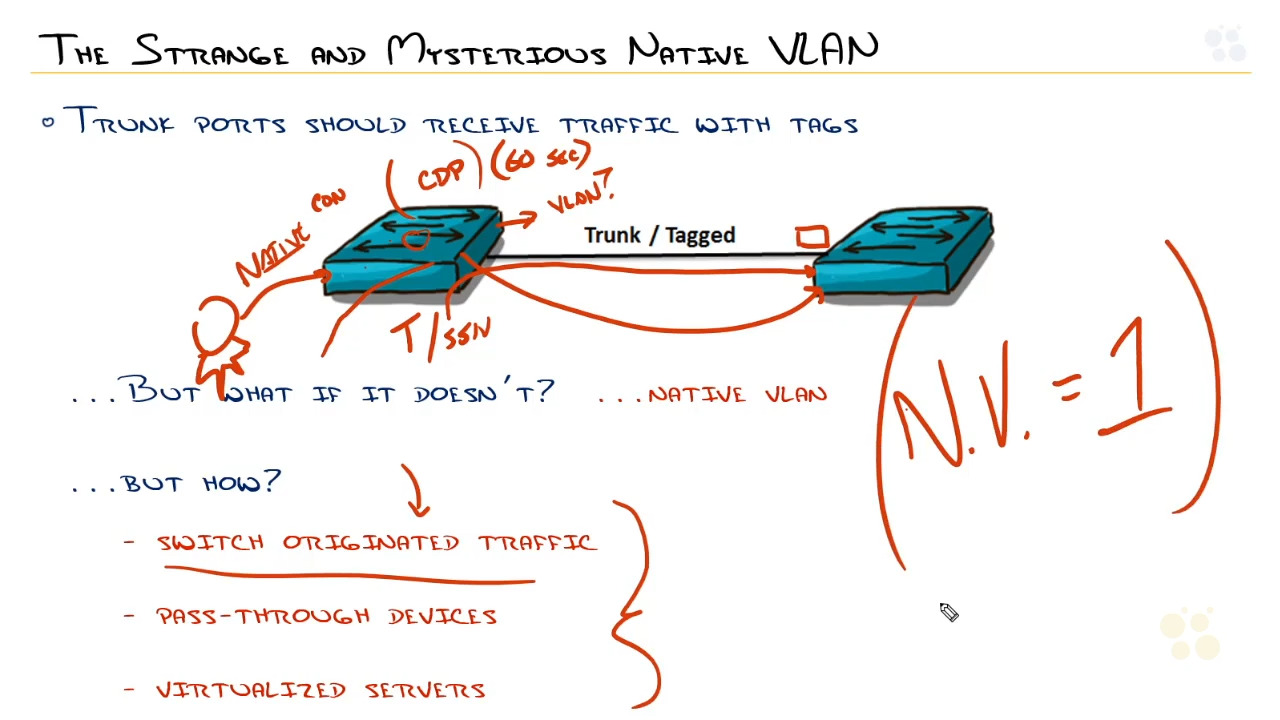
How the Dynamic Trunking Protocol works

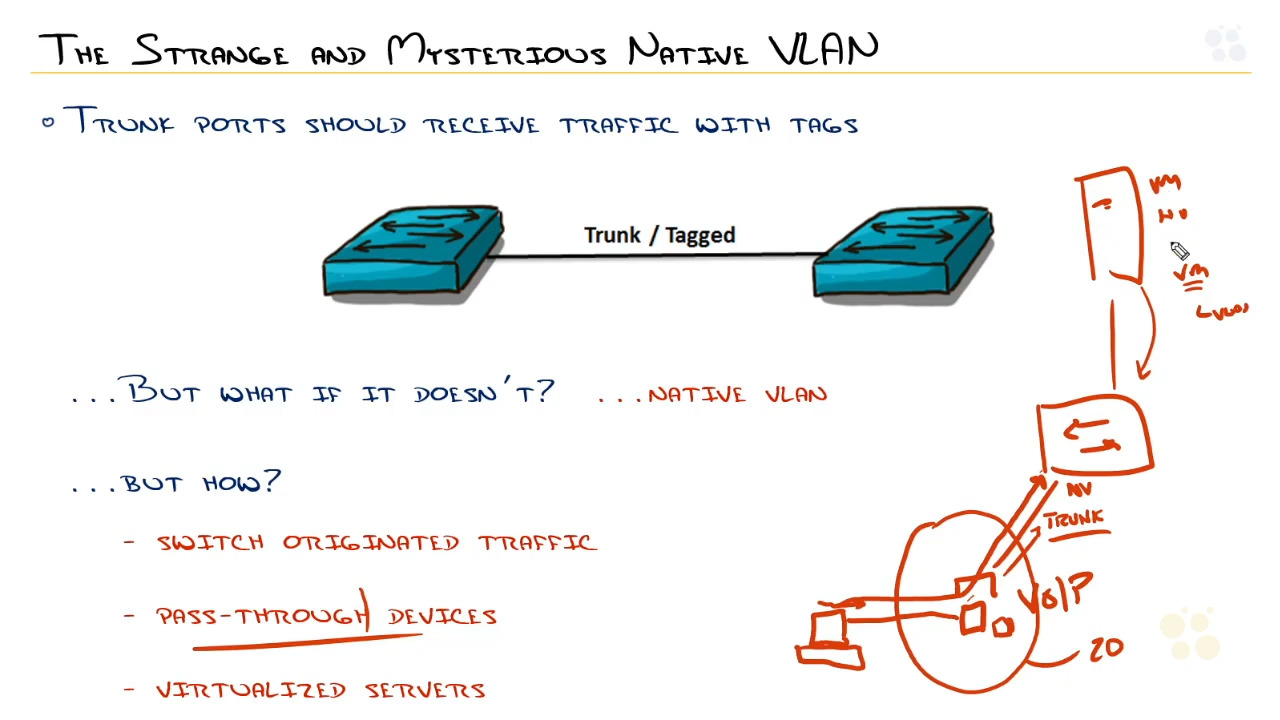
1. Enabling trunk ports
   1. Manual Configuration ( Trunk/ no-negotiate).
      1. This tells the port to become a trunk immediately and you don’t need to negotiate.
   2. Dynamic Configuration (Dynamic Auto / Dynamic Desirable) (default mode of DTP).
      1. The Auto mode is always waiting for someone to send a dtp. If you have two auto modes configured nothing will happen because they are both waiting for a request.
2. Dynamic Configuration can be creepy; use no-negotiate.

Switchport mode trunk encapsulation dot1q

Switchport mode trunk

Switchport nonegotiate





If you wanted to change the native vlan of a port you can type in

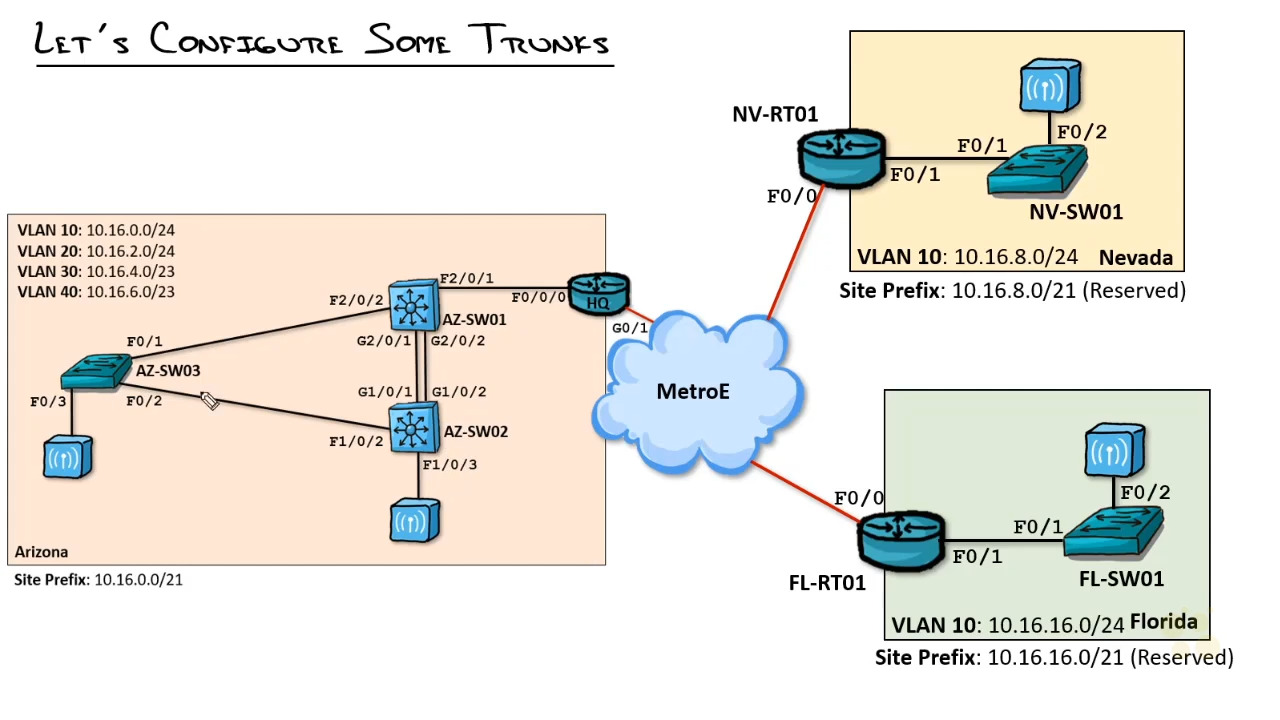
#> int fa0/10

#>Switchport trunk native vlan 10

Switches A and B are connected. Switch A is set to Dynamic Auto and switch B is configured as Dynamic Desirable. Which of the following modes will the two switches negotiate to?

TRUNK

***Configuring Trunks the right way***



* AZ-SW01#show cdp neighbors
  + This shows what neighbors your device is connected to
* AZ-SW01#conf t
  + AZ-SW01(config)#int fa2/0/2
    - AZ-SW01(config-if)#switchport mode trunk
      * Turns on trunking for that port
    - AZ-SW01(config-if)#switchport trunk encapsulation dot1q
      * Sets the trunking protocol for that port to dot1q or 801.1Q
    - AZ-SW01(config-if)#switchport nonegotiate
      * Turns off the DTP to make it a trunk right away.
  + AZ-SW01(config)#int range g2/0/1-2
    - AZ-SW01(config-if)#switchport trunk encapsulation dot1q
    - AZ-SW01(config-if)#switchport mode trunk
    - AZ-SW01(config-if)#switchport nonegotiate
* AZ-SW02#conf t
  + AZ-SW02(config)# int range g1/0/1-2
    - AZ-SW02(config-if)#switchport trunk encapsulation dot1q
    - AZ-SW02(config-if)#switchport mode trunk
    - AZ-SW02(config-if)#switchport nonegotiate
  + AZ-SW02(config)#int fa1/0/2
    - AZ-SW02(config-if)#switchport trunk encapsulation dot1q
    - AZ-SW02(config-if)#switchport mode trunk
    - AZ-SW02(config-if)#switchport nonegotiate
* AZ-SW03#conf t
  + AZ-SW03(config)#int fa0/1
    - AZ-SW03(config-if)#switchport trunk encapsulation dot1q
    - AZ-SW03(config-if)#switchport mode trunk
    - AZ-SW03(config-if)#switchport nonegotiate

AZ-SW03#show interfaces fastEthernet 0/1 switchport

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Place the keywords in the correct order to create the configuration command that enables the 802.1Q trunking protocol on a switch port.

1. Switchport
2. Trunk
3. Encapsulation
4. dot1Q

***Weird and wacky world of VTP***

A new switch with a unique VTP domain has a different VTP revision compared to others in the switch stack. Which of the following will happen if the new switch establishes a trunk link to the stack of switches?

The new switch will not do anything because it is not the same domain name as the others.

BTW virtuallan trunking protocol is not a trunking protocol, it is a protocol that tells others about what revision it has and copies its database over.

***Configuring VTP***

VTP Operating Mode:

1. Server
   1. Default configuration: Can create, delete, add Vlans
2. Client
   1. Just receives updates from other switches. Can not create or delete
3. Transparent
   1. Pass updates but ignores the updates passed through it.

We are going to setup the network for VTP and see how it works.

First we are going to be doing the network configurations on 1

With the command:

AZ-SW01# show vtp status

Here we can see the different status of the VTP currently is operating in Server mode. In transparency mode it will pass the updates through it but will not change on the updates.

We are going to change to VTP version 2

AZ-SW01(config)# vtp version 2

AZ-SW01(config)# vtp domain ARIZONA

Now when we go to AZ-SW02 switch and do a #show VTP status, we can see that it copied the domain ARIZONA from the other switch. This is because out of the box, switches are configured to copy the neighbors and it will be ARIZONA also.

Now when we create vlan 10 on the AZ-SW02 it will show the vlan on AZ-SW01.

AZ-SW02(config)#vlan 10

AZ-SW02(config-if)#name STATIC

We can see the vlan on SW-01 by #show vlan

And it shows that SW01 has the VLAN 10 as the name STATIC also.

On SW01 if we change the VTP mode to client

AZ-SW01(config)#vtp mode client

Then we try to type in the command

AZ-SW01(config)#vlan 20

It will not allow us to create the vlan because it is a client

You can change it back by typing in

AZ-SW01(config)#vtp mode server

Now looking at AZ-SW03 we can see that everything has been copied over

We are going to go ahead and create vlan 20 and 30 with the names, CLIENT AND BYOD.

After this we can disable to VTP mode with:

AZ-SW03(config)#vtp mode transparent

Now it is no longer taking updates from other devices but is sending the updates if it gets one from its neighbors to its other neighbors that has #vtp mode server or #vtp mode client

Three switches have different VTP modes configured. Switch A VTP mode is Server, switch B VTP mode is Transparent, and switch C VTP mode is Client. Which of the following will Switch B and C do with a new revision update from switch A?

Switch B will ignore the revision and pass the update to switch C

***Limiting or adding VLANs to Trunks***

Situation: What if we wanted to create a vlan that does not propagate out to other switches. Lets say you have a development vlan in an area and you don’t want it to go to administrative areas.

Task: Apply to Arizona-sw01 ad sw02

Action:

AZ-SW02(config)#vlan 45

AZ-SW02(config-vlan)#name DEV

Now that we have added it to AZ-SW02 it will not automatically replicate to AZ-SW01 because it’s a transparent mode switch.

AZ-SW01(config)#vlan 45

AZ-SW01(config-vlan)#name DEV

Now if we wanted to limit vlans on an interface we could do.

AZ-SW01(config)#int fa2/0/2

AZ-SW01(config-if)# switchport trunk allowed vlan 10,20,30,40

Or

AZ-SW01(config-if)# switchport allowed vlan remove 45

When you do # show interface trunk

You can now see the vlans that are allowed across the trunk.

***Connecting Trunks to Servers, WAPs, and More***

Lightweight Access points – controller based access points

Capwap tunnel – tunnels everything back to the controller. And the controller puts it on the switch network.

BYOD – vlan 10, Corporate – vlan 20, Student – vlan 30

Autonomous access points

If you're using autonomous wireless access points, then the tagging will be done right here, between the switch and the wireless access point, so your trunk configuration will happen right there. If you're using lightweight wireless access-- I said autonomous.

Server virtualization

The best way to segment traffic from multiple SSIDs on a wireless access point is to use tagging. True or false?

TRUE

***Deploying VLSM in a VLAN network***

So by the time we're done here, we will apply a multilayer switch configuration to a router Etherswitch module to provide routing for Arizona.

***Configuring VLANs, Trunking, and Routing Lab***

SVI – Switch virtual interfaces.

When you create virtual vlans.

When you type in int vlan x, you create a layer 3 SVI for that device.

AZ-RT01(config)# interface vlan 10

AZ-RT01(config-if)# ip address 10.16.0.1 255.255.255.0

This will be the default gateway for any connection on vlan 10. This subnetmask of 255 allows the connections within that subnet to communicate with each other. Int

https://en.wikiversity.org/wiki/Cisco\_Networking/CCENT/VLANs

***Review of configure Trunking Between Switches, WAPs, Servers, and More***