Assignment 1

January 11, 2023 4:14 PM

groups of 4

part 1:
pick a technology that is:
obsolete
emerging
failed

part 2:
get assigned a topic (unrelated)

Start week 8 for presenting

3d tvs - failed

1 - Intro to network design

January 11, 2023 3:01 PM

form follows function

function - does it work
form - best practices / design

Network Design Goals:

1. Function - it must work!
2. High Availability
3. Scale - it must able to grow and adapt
4. Manageability
5. Security

Make a diagram first (it is good)

When you can, focus on standards (sometimes you cant use the standard)

DOCUMENT - you're a fool if you don't
(you must troubleshoot, aka doomed)

Network Architecture Characteristics:

1. High Availability
    a. fault tolerance - multiple switches, EtherChannel
    b. redundancy -
2. Scalability
3. Manageability
4. Security

Network Security principles:

Integrity - things that are how they are supposed to be
Confidentiality - only who needs to know, knows.
Availability - it hasn't been hacked/stolen

Identification - user claiming to be someone
Authentication - validates who the user is
Authorization - permissions allocated to user
Accountability - logging behaviours of a single individual

Best practices:
Policy - WRITTEN IN STONE - overall thing that makes the company work
- formal statements made and supported by senior management
- think like academic integrity, code of ethics and conduct, or security policies
- NAIT slide template

Standards - required protocols
- mandatory actions/rules that support policies
- think like employment standards

Procedures - following policy WRITTEN IN STONE
- step by step guide, how to do something

Guidelines - examples for procedure, WHAT YOU SHOULD DO (not specifically have to do)
- recommendation, not what you HAVE to do, but what you should do

- IETF makes RFCs (request for comments)

What makes a standard:
1. voluntary
2. collective work & arrived at by consensus
3. approved by a recognized body

de jure (by law) - recognized and official standard
de facto - no formal recognition, but accepted and adopted by the market

Why standards are required:

- proprietary hard/software would never be able to interact with each other
- standards allow them to interact and interface with each other

Layered:

- allows for modification to a single layer without fucking up everything else (this was hugely important)

Telecommunications - tele > far off, communicare > to share

International Standards Bodies

- ISO (international organization for standardization) - means equal
- IEC (international electrotechnical commission)
- ITU (international telephony union)

- IETF (internet engineering task force) - only USA I think?
- EIA (electronic industries alliance)
- TIA (telecommunications industries association)
- IEEE (institute of electrical and electronics engineers)

Three-tier model / Three Layer Design model: the building block of large enterprise or campus networks, enterprise comprised of multiple of these blocks

ACCESS - provides access to network for users / end-devices
DISTRIBUTION - provides policy-based routing for access to and through the core
CORE - provides connectivity between blocks, to the internal (private) and external (public) Data Center and also internet

Two-Tier Model / Top-of-Rack (ToR):

Version 1:
Collapsed Distribution / Access
CORE

Version 2:
Access
Collapsed Core / Distribution

Collapsed - meaning they are in the same spot as whatever they are collapsed into

2- Introduction to layer 2 switching

January 13, 2023 8:06 AM

LAN - defined by who owns / administers it - usually the whole thing

Network - part of a LAN

(historically it was the 5-4-3 rule, 5 switches, 4 links between them, 3 can be populated)

Bridge:
segment = collision domain
interconnects segments via software @ L2
2-4 segments

Switch: hardware
link = segment = collision domain
connects devices or segments
8-24 devices/segments

Main functions of L2 Switch:

- address learning
    - MAC address table is called a "CAM table" - content accessible memory
- data frame forwarding/filtering
    - flooding, check for frame size
- loop avoidance

when destination mac address is not in table, floods the mac address (copies it then sends it out every active interface)
flood = behavior, broadcast = address

3 - Spanning Tree - Redundancy and Loop Avoidance

January 18, 2023 3:03 PM

Collisions were impossible on a switched network, **UNLESS** you are using half-duplex

Redundancy is good, loops are bad

Loops bad:
- layer 2 can't do anything about the loop so it fully saturates the network with lost packets and slows everything down like hardcore. Broadcast messages basically duplicate and keep sending it to the next guy (even if they have already gotten it)
- layer 3 has TTL and other flags to kill packets

STP (spanning tree protocol)
- provides redundant intersegment connections (and prevents loops)
- the yellow light used to be called the "blocking state"

802.1D - standard (aka Common Spanning Tree / CST) - takes minimum of 30 seconds, but most commonly used
802.1w (Rapid Spanning Tree / RST) - takes like maybe 5 seconds
802.1s (Multiple Spanning Tree / MST) - also very quick
- **802.1D** has **w** and **s** in it now.

common spanning tree is the default because it is backwards compatible and you're probably not gonna need it anyways since spanning tree is the least of your worries while setting it up

Physical Topology - How devices are connected
Logical Topology - How data flows

- By default, all layer 2 switches support and use spanning tree

The switch with the lowest **BridgeID** is the **root bridge** (only ever 1)
- **bridgeID** is a combination of (**priority** and **mac address**)
- priority - default to 32768 (cisco goes down in chunks of 4096)

packet tracer vlan 1 mac address is the same as the base mac address (this is not the case in the real world)

root port
- **best** path from non root bridge TO the root bridge
- where you **recieve** BPDUs from (designated port) root bridge
    - lowest cost to root bridge - quickest path (two 1gb jumps vs one 100mb | two 1gb ones win) not least jumps

designated port
- **sends** BPDUs to root ports (**Bridge Protocol Data Units** - contains all spanning tree data)

alternate port
- port that will become active if the root fails (yellow, always discarding)
- always opposite of a designated port

- (CANNOT SEND ANYTHING OR RECIEVE **DATA)**

disabled port
- "bpduguard" - goes into errdisabled state, aka shuts down
- not a trunk so it can't make a loop

edge port
- end devices are plugged into edge ports
- all edge ports are disabled ports, not other way around

backup port
- used to connect to a hub (lame as hell, wont be asked about)

dont ever disable stp ever

Discarding
- a port that would cause a switching loop if it were active
- no data is sent or received, but BPDU data is still received
- Alternate & Backup ports

Forwarding
- normal operation, receiving and forwarding frames
- monitors BPDUs that would tell it to turn into blocking state
- Root & Designated ports

Point-to-point / shared link type
- used for trunk / tagged links

RST Path Cost:
FE (100 mbps) - 200,000
GE (1 gbps) - 20,000
10G (10 gbps) - 2,000
100G (100 gbps) - 200

Bridge Protocol Data Unit (BPDU)
- contain info that allows a switch to build redundant but loop free topologies
- CST - does listening and learning (2x forward delay 15 seconds) to reach convergence (picking a root bridge)
    - CST, every switch just relays it and increases message age by 1

- RST - uses flags to figure out who the root bridge is, happens to be way fucking faster
    - RST, every switch sends a hello message every 2 seconds

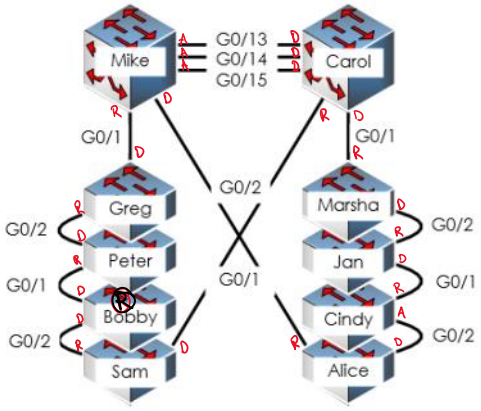
802.1w
- only ever reply to a proposal from a switch that is better than you (lower priority/mac address)

PVST - per vLAN spanning tree
- spanning tree works on a single LAN
- vLANs are just virtual LANs

- Sw1(config)#spanning-tree mode rapid-pvst | how to change from CST to RST
- Sw1(config)#spanning-tree vlan [id] priority [value] | changes the priority of a switch
- Sw1(config)#spanning tree vlan [id] root [primary/secondary] | changes the value

STP port role practice 3

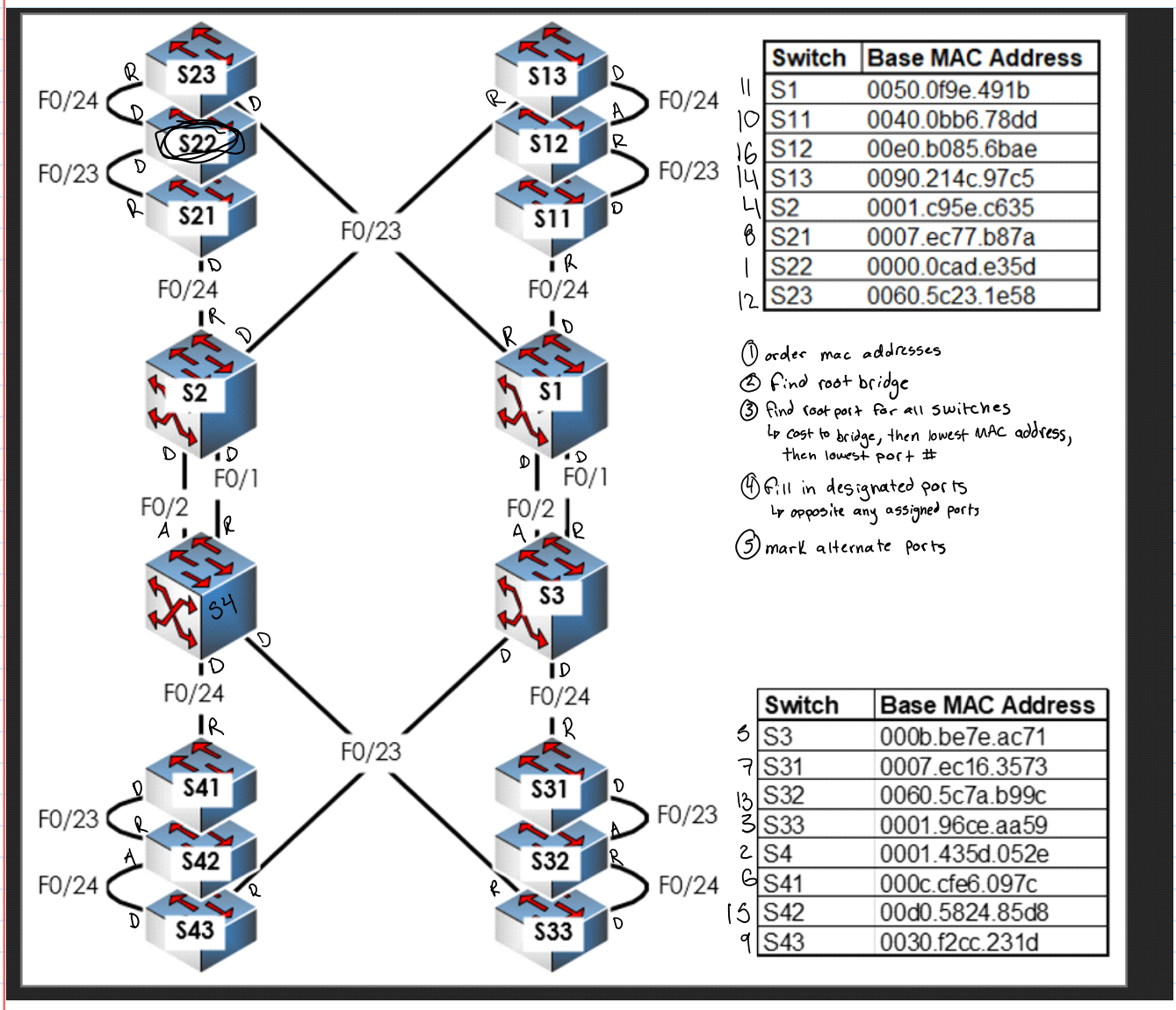
January 20, 2023 8:56 AM



Switch	Base MAC Address
Carol	00e0.a349.6a86
Mike	000b.be1b.b671
Marsha	0060.47ec.25d7
Greg	0060.702b.c141
Jan	0004.9a04.5b44
Peter	0050.0f5d.21bc
Cindy	0060.702b.4baa
Bobby	0002.4a4d.7aa8
Alice	0007.ecb8.418b
Sam	0090.21ce.96b3

terry port roles 4

January 25, 2023 3:07 PM



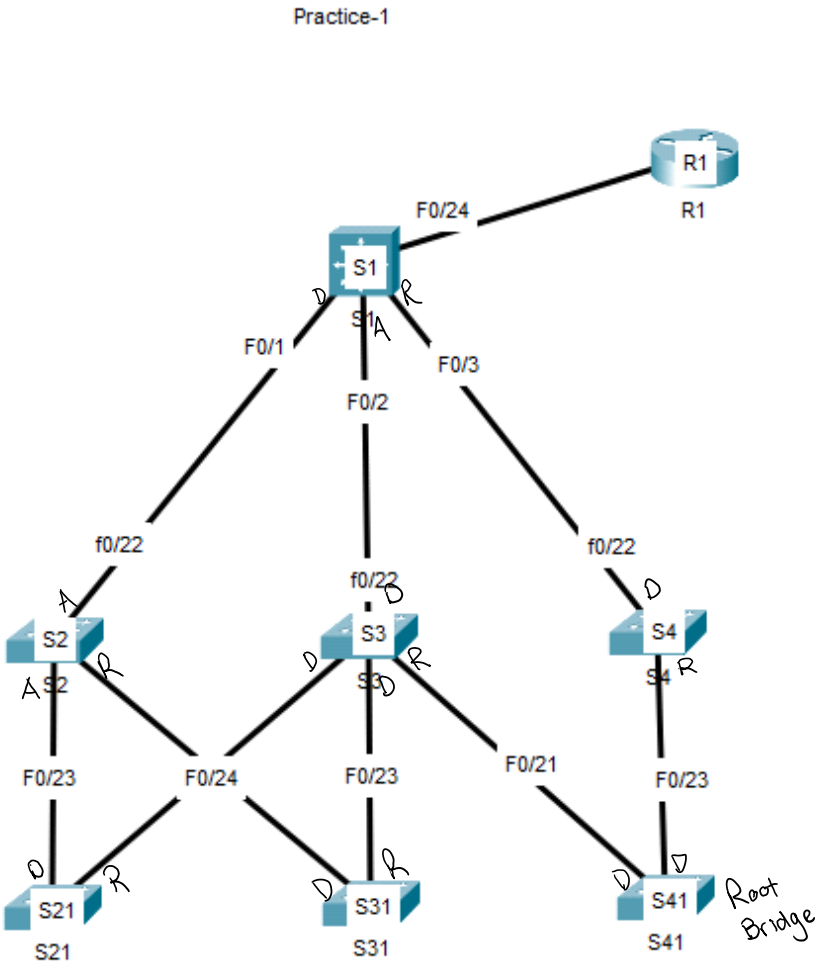
Switch	Base MAC Address
S1	0050.0f9e.491b
S11	0040.0bb6.78dd
S12	00e0.b085.6bae
S13	0090.214c.97c5
S2	0001.c95e.c635
S21	0007.ec77.b87a
S22	0000.0cad.e35d
S23	0060.5c23.1e58

1. order mac addresses
2. find root bridge
3. find root port for all switches
   - cost to bridge, then lowest MAC address, then lowest port #
4. fill in designated ports
   - opposite any assigned ports
5. mark alternate ports

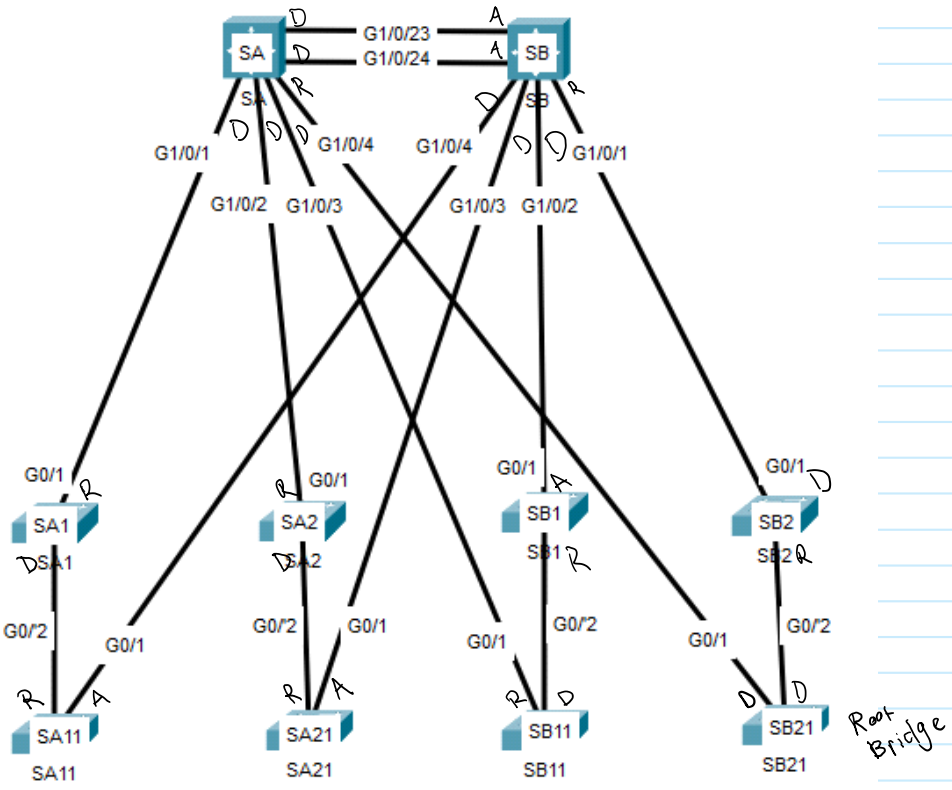
Switch	Base MAC Address
S3	000b.be7e.ac71
S31	0007.ec16.3573
S32	0060.5c7a.b99c
S33	0001.96ce.aa59
S4	0001.435d.052e
S41	000c.cfe6.097c
S42	00d0.5824.85d8
S43	0030.f2cc.231d

practice thang

January 26, 2023 12:31 PM

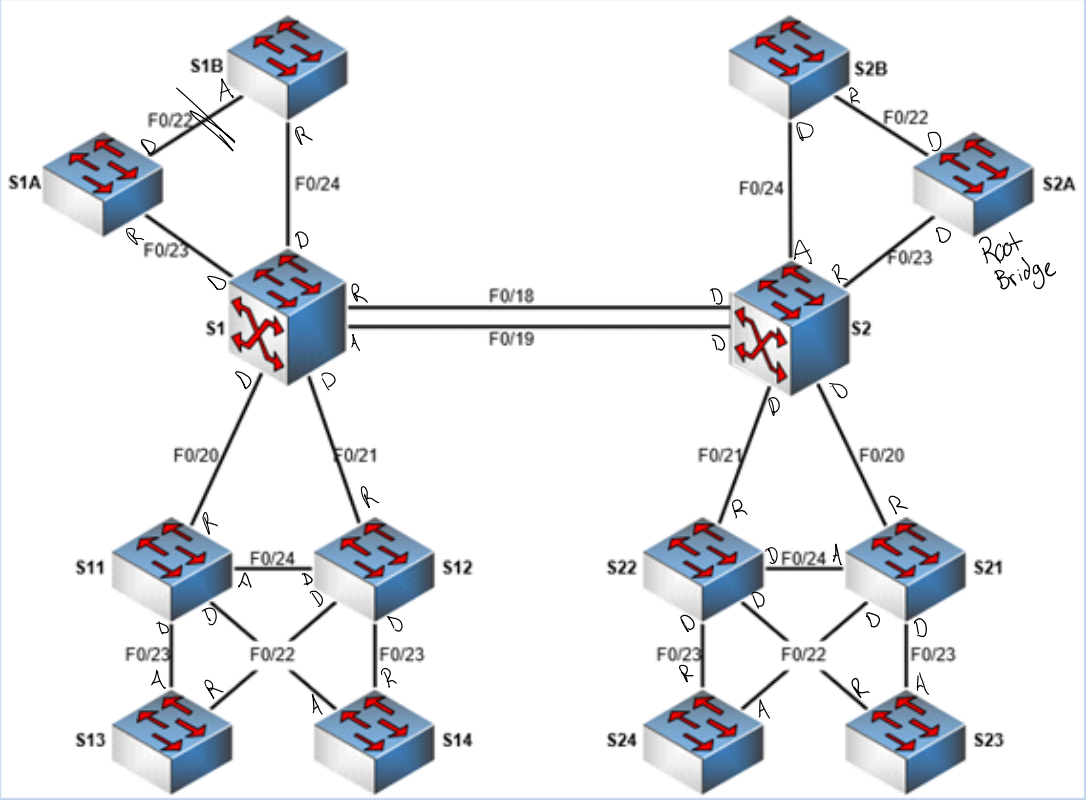


Practice-2


SA
SB
G1/0/23
G1/0/24
D
A
SA
SB
G1/0/1
G1/0/2
G1/0/3
G1/0/4
G0/1
G0/2
SA1
SA2
SB1
SB2
SA11
SA21
SB11
SB21
Root Bridge

Assignment 2

January 27, 2023 8:03 AM



Switch	Base MAC Address
S1	000d.e78a.f098
S1A	0001.1234.fedd
S1B	0009.bbab.babe
S11	001c.caca.dada
S12	000a.76af.2319
S13	0002.3153.4264
S14	0006.ed01.d34a
S2	000d.65ef1043
S2A	0001.1234.fedc
S2B	0009.babe.baba
S21	001c.4321.9876
S22	000a.8acb.bba1
S23	0002.9801.1369
S24	0006.ed01.23da

Virtual Local Area Networks (VLANs)

February 1, 2023 3:00 PM

physical segment - connection from device to device - cable
logical segment - subnet

ARP & DHCP - biggest broadcast traffic

VLAN - purpose was to manage size of broadcast domains
- aka make it so you dont have to arp every single god damn thing at once

IEEE 802.1Q - (encapsulation) VLANs
VLAN Tag 4 bytes - AKA shim
VLAN frame - 1522 bytes

- **trunk** carries **ALL VLANs**

VLAN benefits:
- Network Administration / Organization -
  - can group people by departments easily
- Improved Security
  - set a "blackhole" VLAN to VLAN 1 - any unused port goes to that VLAN (doesn't have a subnet to it)
  - locks down phones - can only call emergency and inside building
- Easier Fault Management - smaller chunks that makes it easier to tell where the issue is
- Improved Quality of Service -

VLAN 1 is the default native VLAN, all switch ports are member by default
- its the easiest one to figure out, so don't use it
- vlan 1 has no VLAN tag - meaning it is legacy / has backwards compatibility
- cisco uses VLAN 1 for identifying neighboring switches so you cant change name or anything

switchport mode access - accessing specified VLANs
switchport mode trunk - every VLAN

IEEE 802.1Q Tag - 4 bytes
- Tag Protocol Identifier (TPID) - always 0x8100 (ethernet) : 16 bits
- Tag Control Information (TCI) : 16 bits
  - PCP - Priority Code Point - used for priority and QOS, gets some packets through before others : 12 bits
  - DEI - Discard Eligible Indicator - used with IP/TCP to get rid of congestion : 1 bit
  - VID - VLAN Identifier - 4094 possible VLANs (cant use 0 or 4095) : 12 bits

VLAN Interfaces
Untagged Port - **Access**
- any int connected to end device (edge port)
- carries data associated with THAT VLAN

Tagged Port - **Trunk**
- any link between switches or between switch and router
- carries data associated with all VLANs

(802.1Q term - untagged / tagged | cisco term - access / trunk)

VLAN membership:

- port-based VLANs or static VLANs - assigned VLANs
- "show vlan brief"

- MAC-based VLANs or dynamic VLANs - outsources the switch checking VLANs to a RADIUS server
- not used as much now

VLAN TYPES:

- default (1) - everything auto assigned to this, dont use it
- native - used for backwards compatibility, not used much
- management - used for network management, **ONLY layer 2 SWITCHES** are members of **VLAN**
- data - every **user** is a member of a data VLAN, just dont use VLAN 1 please god
- voice - "switchport voice vlan 100" - can be paired up with another VLAN for data

every access port can be connected to two VLANs - one can be anything, the other **HAS** to be voice

VLAN Design Guidelines

- biggest subnet size of /22
- **document everything**
- separate management and user data traffic
- **DONT USE VLAN 1**
- ensure only trusted users can access the management VLAN
- set native VLAN to an unused VLAN
- clear native VLAN from all trunks > 'switchport trunk allow [allowed vlans here]'
- unused ports into 'blackhole VLAN'
- configure user ports as static access
- shutdown unused ports

VLAN Design REQUIREMENTS:

trunk must have the following as same on both sides

- link speed & duplex setting
- encapsulation
- allowed VLANs - only uses ID # not name
- native VLAN

VLAN 1:

- cannot be renamed or deleted
- native VLAN on trunk port (cant be removed)

VTP (VLAN trunking protocol) - terry hates it - too complex for the same thing as notepad

- needs a vtp domain and password, but then it figures out VLAN tables for you
- vtp mode transparent - doesn't need any of that shit ^ | this is basically off mode, this shit dumb as hell

Port Security

February 9, 2023 12:06 PM

Port Security - used to restrict input to interface by only allowing specific MAC addresses to the switch port

- config#'switchport port-security'

- config#'switchport port-security maximum [# of MAC addresses]'

MINIMUM OF 3 PORT FOR VOIP (OPTIONAL) (least you can have for max is 3 for us because cisco and stuff)

- config#'switchport port-security mac-address sticky'

learns MAC addresses (up to max) to lock down switch port
remove sticky to manually do MAC addresses

- config#'switchport port-security violation [<protect> | <restrict> | <shutdown>]'

(OPTIONAL, DEFAULT TO SHUTDOWN)

  - protect - don't allow the MAC address through, leave the interface up
  - restrict - don't allow that MAC address through, leave the interface up , but store as a LOG
  - shutdown - if a violation occurs, 'err-disabled' aka shut that bitch DOWN (and log event) [MUST BE SHUTDOWN THEN BROUGHT BACK UP TO FIX]

- 'show port-security interface {interface type/number}'

Port Security Settings

- 'show port-security address'

secure MAC address

Config Guidelines:

- secure port cannot be destination port for SPAN (can't be done on a trunk)
- a secure port cannot be a part of EtherChannel (can't be on a trunk)
- when switchport is a member of Voice VLAN, ensure max is AT LEAST 2 (3 for us)

Link Aggregation

February 9, 2023 12:26 PM

LAG - Link Aggregation Group (this is also known as EtherChannel)
- 8 links per LAG, 2 LAGs per switch (in packet tracer)

all packets need to be on the SAME link for LAG (because it can't make a loop so it won't do that)
- link aggregation algorithm + RSTP = no packets loss even when links are lost

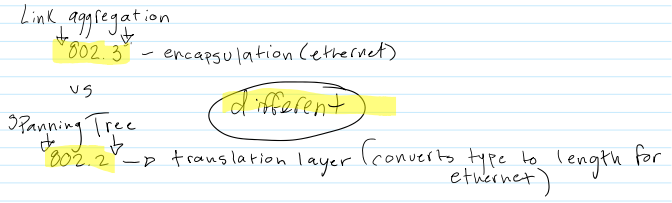
Implementation Restrictions:
- link speed must be same
- duplex settings must be same
- spanning-tree path cost must be same
- allowed VLANs must be same
- native VLAN must be same
- LAG link member cannot be a destination for port-mirroring

Static LAG (manually set) / LACP (link aggregation control protocol) (dynamic):
no protocol is used, both ends of each link are manually configured to be part of a LAG (not recommended in LAN (static)

turning it on
- 'interface range gigabitEthernet 1/0/1-4'
- 'channel-group 1 mode [<active> | <passive> | <on (only for static)>]'

Mode types:
- Active - exchange LACP frames with neighbour switch regardless of neighbour switch config
- Passive - exchanging LACP frames with neighbour switch only upon receiving LACP frame from neighbour switch
- (this means at LEAST one of them needs to be active to do anything)

Link Aggregation - runs on top of 802.3 (rather than spanning tree that runs on top of 802.2 which acts as a translating layer for 802.3)
Spanning Tree (802.1D in todays world) - runs on top of 802.2



Link Aggregation commands:

- config#'interface range gigabitEthernet 1/0/1-4'
- ★ config-if#'switchport trunk native vlan [native vlan number]'
- config-if#'switchport trunk encapsulation dot1q'
- config-if#'switchport mode trunk'
- config-if#'channel-group [group #] mode active
- config-if#'spanning-tree link-type point-to-point'

(more basic version)
on switch 1
- int range 1/0/3-4
- switchport mode trunk
- channel-group 3 mode active

on switch 2
- int range g0/1-2
- switchport mode trunk
- channel-group 3 mode active

Commands Page :)

February 8, 2023 3:45 PM

- to trace the root bridge

'show span'

- change STP to RSTP

config# 'spanning-tree mode rapid-pvst'

- changing priority of a switch in STP

config# 'spanning-tree vlan [number] root [primary <or> secondary]'
or
config# 'spanning-tree vlan [number] priority [increment of 4096]' (good practice to set 8192 on root)

- setting up edge ports

config# 'interface range FastEthernet 0/1-24' (note: 0/1-24 is a range)
config-if-range# 'switchport mode access'
config-if-range# 'spanning-tree portfast'

- enable port guarding (be careful, this can brick your switch)

config-if-range# 'spanning-tree bpduguard enable'

- configuring point-to-point link type ports (for legacy/other vendors since RSTP does this by default)

config# 'interface range GigabitEthernet 1/0/2-24'
config-if-range# 'spanning-tree link-type point-to-point'

DHCP - HELPER ?????
port security
link aggregation
vlan database
spanning tree

router on a stick vs vsi ??

February 15, 2023 3:03 PM

spanning tree upon first activation of a switch:
- always in designated mode
- state = discarding

PRIORITY OF QUESTIONS vvv

VLANS
SPANNING TREE
PORT SECURITY
SWITCHING
LINK AGGREGATION
like 2 of something else? subnetting maybe?

802.1Q
802.1D (technically no w or s)

3650 - switchport mode trunk
3560 - switchport encapsulation dot1q **and** switchport mode trunk

router on a stick - need to tell 802.1q
- int g0/0/1
- encapsulation dot1q

802.3 is encapsulation

if DHCP server
- ip helper for clients to get to DHCP server:)

better commands one

February 15, 2023 4:19 PM

helpful commands:
do show int trunk

how to make vlans (EASY, NOT PATCHED, STILL WORKING)***

'vlan [#]'
'name [name of vlan]'

layer 2 switch commands for spanning tree, vlans, port security:

- for making an ip address for the switch:
- recognize what vlan the ip address is about (management vlan probably)

'int vlan [management vlan #]'
'ip address [the ip it wants] [subnet mask for it]'

Router on a stick commands:

'en'
'conf t'

'int g0/0.[vlan # here]'
'encapsulation dot1Q [vlan # here again]'
'ip address [subnet address here, ex. 172.17.5.254] [subnet mask]'
'ip help-address [ip address of DHCP server]' (only if there is a dhcp server)

- dont need to do it for voice or for native (unless specified nerd)

layer 3 switch:

'spanning-tree mode rapid-pvst'
- add in vlans (check top section)
- set root bridge v

'spanning-tree vlan [vlan range (10-15 for ex)] priority 4096' (or other if specified)
'spanning-tree vlan [vlan range (10-15 for ex)] root [primary / secondary]'

- for making an ip address for the switch:
- recognize what vlan the ip address is about (management vlan probably)

'int vlan [management vlan #]'
'ip address [the ip it wants] [subnet mask for it]'

LINK AGGREGATION: LAST THING YOU DO BECAUSE EVERYTHING HAS TO WORK RIGHT FIRST

(MAKE SURE THEY HAVE THE SAME SPANNING TREE THANG)

'interface range [g1/0/1 - whatever]'
'description Connection to 4-link LAG on Sw2' (for example)
'switchport trunk native vlan [native vlan #]'
~~'switchport trunk encapsulation dot1q'~~
'switchport mode trunk'
'channel-group [LAG # (1 or 2)] mode [active or passive]'
'spanning-tree link-type point-to-point'
'exit'
'interface Port-channel [LAG # (1 or 2)]'
'description LAG between Sw1 and Sw2'
'switchport trunk native vlan [native vlan #]'
~~'switchport trunk encapsulation dot1q'~~
'switchport mode trunk'
'do write'

practice test stuff

February 16, 2023 11:05 PM

```
vlan 10
name Pippin
vlan 11
name Boromir
vlan 13
name Elrond
vlan 14
name Galadriel
vlan 15
name Deagol

switchport mode trunk
switchport trunk native vlan 15

switchport mode access
switchport access vlan 11
switcport voice vlan 14

spanning-tree portfast
spanning-tree bpduguard enable

switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation shutdown
do write


vlan 10
name Pippin
vlan 11
name Boromir
vlan 12
name Gandalf
vlan 13
name Elrond
vlan 14
name Galadriel
vlan 15
name Deagol

ip helper-address 172.16.6.200

switchport mode access
switchport access vlan 12
switchport voice vlan 14
spanning-tree portfast
```

```
spanning-tree bpduguard enable

switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation shutdown
do write
```

MASTER COMMANDS PAGE

February 16, 2023 8:23 AM

helpful for troubleshooting:
show vlan brief
show int trunk
show port
show int access (?)
show span
show cam
show int portchannel (#)
show ip protocols
show ip ospf
show ip ospf interface

Switch(config)#spanning-tree mode rapid-pvst <---change the spanning tree version

---Change the root bridge---
Switch(config)#spanning-tree vlan 1 root [primary/secondary]
--or--
Switch(config)#spanning-tree vlan 1 priority ?
<0-61440> bridge priority in increments of 4096

---For edge ports---
Switch(config)#interface range FastEthernet 0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast

Switch(config-if-range)#spanning-tree bpduguard enable <--to prevent connections from other switches

---For switch to switch connections with RTSP---
Switch(config)#interface range GigabitEthernet 1/1/1-4
Switch(config-if-range)#spanning-tree link-type point-to-point

---VLAN's---
---creating vlans---
Switch(config)#vlan <69> <---vlan id number
Switch(config vlan)#name <nice> <---vlan name

Sw1(config)#interface range g1/1-4
Sw1(config-if-range)#switchport trunk native vlan 999 <---changing the native vlan

Sw1(config)#interface range g1/0/1-24
Sw1(config-if-range)#switchport access vlan 11 <---changing the port vlan
Sw1(config-if-range)#switchport voice vlan 66 <---changing the voice vlan

---vlan routing---
--router on a stick--
R1(config)#interface G0/0
R1(config-if)#no ip address
R1(config-if)#no shut
R1(config-if)#interface G0/0.x
(x = subinterface ID – should match the VLAN ID)
R1(config-subif)#encapsulation dot1q x
R1(config-subif)#ip address A.B.C.D A.B.C.D
R1(config)#ip helper-address [dhcp server IP] <--- if there is a dhcp server

--layer 3 switch with routing--
Sw2(config)#ip routing
Sw2(config)#interface vlan 1
Sw2(config-if)#no ip address
Sw2(config-if)#shut
Sw2(config-if)#interface vlan x
Sw2(config-if)#ip address A.B.C.D A.B.C.D
Sw2(config-if)#no shut
Sw1(config)#ip helper-address [dhcp server IP] <--- only if using switch routing and there is a dhcp server

---layer 2/3 switch (no routing)---
enter in vlans
Sw1(config)#interface vlan 1
Sw1(config-if)#no ip address
Sw1(config-if)#shut
Sw1(config)#int vlan [# of network management]
Sw1(config-if)#ip address [highest ip of vlan subnet - this is the default gateway] [subnet mask]

---Port Security---

Sw3(config)#interface range f0/1-24 <---Don't put this on a trunk because it will mess up your network
Sw3(config-if-range)#switchport port-security
Sw3(config-if-range)#switchport port-security maximum 3 <---should be set to 3 if you have a voice vlan
Sw3(config-if-range)#switchport port-security mac-address sticky
Sw3(config-if-range)#switchport port-security violation shutdown
Sw3(config-if-range)#do write

---Link Aggregation---

Sw1(config)#interface range g1/1/1-4
Sw1(config-if-range)switchport mode trunk
Sw1(config-if-range)switchport trunk native vlan 777 <---make sure both switches have the same native vlan
Sw1(config-if-range)#channel-group 1 mode active

Sw1(config)#interface Port-channel 1
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#switchport trunk native vlan 777 <---just to make sure

---ACL---

ip access-list standard <ForRemoteAccess>
permit host 172.16.0.1 - used for specific hosts
permit 172.16.0.0 0.0.0.255 -- this has a wildcard, it is used for whole subnets
line vty 0 15
login local
transport input ssh
access-class <ForRemoteAccess> in

---SSH---

hostname s1
enable secret cisco
username admin password class
ip domain-name bubba.local
crypto key generate rsa modulus 1024
ip ssh v 2
line vty 0 15
login local
transport input ssh

---OSPF--- **make sure you advertise your network management VLAN**

router ospf 1 - (this number doesn't matter)
ip ospf priority 200 - optional
router-id 1.1.1.254 - need a designated router - ethernet is a multiaccess media (always)
^^^ it is not an IP address. ***HIGHEST NUMBER WINS. (this will be second guy)***

auto-cost reference-bandwidth 1000 - in Mbps, so 1000 is gigabit **(you need to change this for every router in the domain - change so they match)**
network 192.168.255.254 0.0.0.0 area 0 - this tells you which network to look for interfaces on - **through the interface 192.168.255.254** to **0.0.0.0 (everything) * DO THIS ON ALL THE INTERFACES ***
default-information originate - propagate default route to the rest of the network

---EIGRP---

Router eigrp 100
Network <your networks that you want to broadcast outwards>
No auto-summary

WiFi Fundamentals

March 2, 2023 12:03 PM

802.11 - WiFi - **know this**
802.15 - Bluetooth - BLUETOOTH IS NOT WIFI
- predominately for peripherals

wireless: communication over wireless link
mobility: handling the mobile user who changes point of attachment to network

mobility benefits:
- access / availability
- coverage area
- increased flexibility
- cheaper

WiFi - Wireless LAN (WLAN)

1G: analog, voice only
2G: digital, voice and limited data (SMS only)
3G: digital overlay on 2G networks (adds mobile internet, video, mobile TV)
4G and 5G: faster speeds but less coverage

Collision avoidance vs Collision detection

802.11 Wireless LAN (WLAN)
- management frame and data frame - never collide

connection type
802.11 (WLAN) - Shared
802.3 (LAN) - Dedicated

wireless LAN components:
wireless client
- need a radio and antenna
- compatibilities vary according to:
  battery
  size, type & number of antennas
  802.11 standard supported

wireless access point (AP)
- requires radio and antenna
- usually has a wired 802.3 port
  (for connecting to network, and POE)

Autonomous AP = Thick AP = Standalone AP = (WAP)
- this means you need to manage the unit by connecting to the device (individually configured)
- super rare for being in a business
- multi-functional (can do DNS kinda)

Lightweight AP = Thin AP = Intelligent Antennas
-managed by a WLC
have a central configuration

wireless LAN controller
- software or hardware
- embedded or standalone

Antennas
- omnidirectional Wi-Fi antennas (this is used the most) at most like 150m
- Directional Wi-Fi Antennas (like satellite dish) can go km
- Yagi antennas (shortwave, looks like the old RV antenna) can go km

802.11a - single input, single output (SISO)

802.11n - multiple input, multiple output (MIMO)
- multiple streams (rx and tx)

Multi-User MIMO - the standard for today
- serves multiple devices at the same time

Single-User MIMO
- serves one device at a time

CAPWAP - management frames > absolutely needed with multiple standalone APs

WLAN topology
- doesnt matter where the AP is, its where its being used
- usually in distribution or edge tho

Ad Hoc Mode
- like airdrop
- you are connected device to device to transfer data

Tethering
- linking a device to another thing that has connection
- like an ipad to an iphone

Infrastructure Mode - it is the network

Service Set Identifier (SSID)
- name of network

Basic Service Set (BSS)

Basic Service Set Identifier
- AP MAC address

Extended Service Set (ESS)
- all BSS in a WLAN

Wireless Connectivity Process:
- beacon or probe for a network (DORA basically, probe, authenticate, associate)

Discovering AP
passive mode
- ap advertises its service by sending broadcast beacon frames containing the SSID
- beacon's primary purpose is to allow wireless clients to find networks

active mode
- clients must know the SSID
- client initiates the process by broadcasting a probe request frame on multiple channels

authentication frame - always send one of em
open - no password, still needs it
shared key - need a password (WEP - terrible (sucks), WPA2 - key stored internally (good))
SAE Handshake (WPA3 - key stored externally (great))

802.1x - adds authentication to port security (you use 802.1x *and* port security)

802.11n - wifi 4
802.11ac - wifi 5
802.11ax - wifi 6

management frame - important
- a series of management frames checks the network (in a type field)

carrier sense multiple access with collision avoidance (CSMA/CA)

radio frequency spectrum -
- 902 - 928 MHz
- 2.4 - 2.4835 GHz
- 5GHz

Security:

Rogue AP - dangerous
- man in the middle attack
- allow a malicious intruder in, capture data, >make changes to it > send it back into the network

Packet Sniffing:
- you can get them easily
- if you know what you're looking for you can find some crazy shit

- things he didnt discuss until later

wifi security WPA2 BARE MINIMUM
think about 802.1x

hiding SSID doesnt do much
MAC filtering - think of it like port security (not sticky, but manually set - for things that will never be changed)

- not really that secure, because MAC address spoofing = im in

wireless technology is not controlled like ethernet

- its out there, just everywhere
- the cable acts like the sound proof bubble in get smart

March 15, 2023 3:37 PM

router to router - IP address to IP address

R1		R2
interface GigabitEthernet 0/1	to	interface GigabitEthernet 0/1
ip address 192.0.2.1 255.255.255.252		ip address 192.0.2.2 255.255.255.252

switch to router - IP routing on switch, no switchport, IP address to IP address (this is pretty common)

S1		
ip routing		R2
interface GigabitEthernet 1 /0/1	to	interface GigabitEthernet 0/1
no switchport		ip address 192.0.2.2 255.255.255.252
ip address 192.0.2.1 255.255.255.252		

switch to router (vlan) - set switch to vlan, access mode, IP address to IP address

S1		
ip routing		
interface GigabitEthernet I /0/1		R2
switchport mode access		interface GigabitEthernet 0/1
switchport access vlan 13	to	ip address 192.0.2.2 255.255.255.252
spanning-tree portfast		
interface vlan 13		
ip address 192.0.2.1 255.255.255.252		

switch to router (router vlans) - trunk with vlan, matches sub interface, IP address to IP address (this is the most common ?)

S1		R2
ip routing		interface GigabitEthernet 0/1
interface GigabitEthernet 1 /O/I	to	no ip address
switchport trunk encapsulation dotl q		no shutdown
switchport mode trunk		interface GigabitEthernet 0/1 . 1 3
interface vlan 13		encapsulation dot Iq 13
ip address 192.0.2.1 255.255.255.252		ip address 192.0.2.2 255.255.255.252

switch to switch - L3 to L3 - ip routing, trunk to trunk, same vlan, IP address to IP address (ALWAYS using this (VLANs)) #1

S1		R2
ip routing		ip routing
interface GigabitEthernet I /0/1		interface GigabitEthernet I /0/1
switchport trunk encapsulation dotl q	to	switchport trunk encapsulation dotl q
switchport mode trunk		switchport mode trunk
interface vlan 13		interface vlan 13
ip address 192.0.2.1 255.255.255.252		ip address 192.0.2.2 255.255.255.252

switch to switch - L3 to L3 - ip routing, no switchport on both, IP address to IP address (not very common) #2

S1 S2

switch to switch - L3 to L3 - ip routing, no switchport on both, IP address to IP address (not very common) #2

S1		S2
ip routing		ip routing
interface GigabitEthernet I /0/1		interface GigabitEthernet I /0/1
no switchport	to	no switchport
ip address 192.0.2.1 255.255.255.252		ip address 192.0.2.1 255.255.255.252

Dynamic Routing

March 16, 2023 12:33 PM

Interior Gateway Protocols

road sign, or **distance vector** - only sees the next hop

RIP - Routing Information Protocol
EIGRP - Enhanced Interior Gateway Routing Protocol

road map, or **link state** - sees the whole network

OSPF - Open Shortest Path First
IS-IS - Intermediate System to Intermediate System

Exterior Gateway Protocols

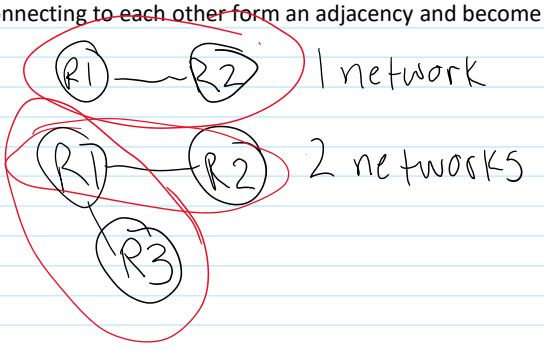
Path Vector

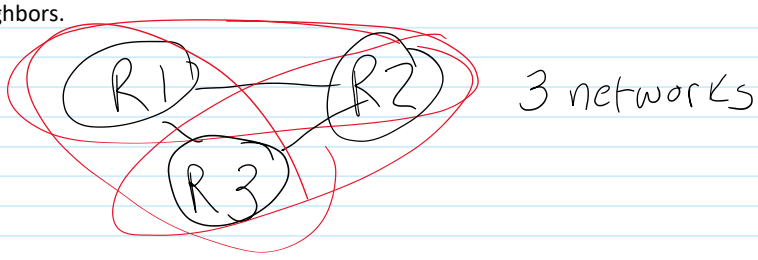
BGP - Border Gateway Protocol

Dynamic Routing Terms

Autonomous System
- a group of routers under the same IP network prefix (/?) and under administrative control of one entity. (they can all communicate to each other)
- the connection out of the network is called a **border router**

Neighbors
- routers connecting to each other form an adjacency and become neighbors.





- only neighbors can communicate with each other

Administrative Distance
- the first thing a router looks at to determine which route source to use if the router communicates with more than one other.
- the lower the administrative distance, the more trusted, and it will by default use this link.

- connected interface 0
- Static Route - 1
- EIGRP - 90
- OSPF - 110
- IS-IS - 115
- RIP - 120
- **DEFAULT STATIC ROUTE - 254(terry says 255)** > only ever used if NOTHING else is connected > question on test will look for 255
- unknown - 255?

Routing Algorithms
- RIP - Bellman-Ford
- OSPF - Dijkstra
- IS-IS - Dijkstra
EIGRP - Diffusing Update (DUAL) - Cisco Proprietary

Dynamic Routing Components

- Data Structures
> neighbor table
> topology table
> routing table

Dynamic Routing Operation Fundamentals

1. Directly connected routes added to routing table
2. static routes (if configured) added to routing table
3. neighbour discovery & establishment
4. network discovery - exchange of connected routes with neighbours
5. exchange of complete routing table entries with neighbours
6. achieve convergence !

Device Vector Protocols: know thy neighbor

- RIPv1 - 1st gen, legacy
- RIPv2 - simple, not scalable
- IGRP - obsolete, cisco proprietary
- EIGRP - cisco developed, proprietary, RFC as of 2014 (the one)

Link State Protocols: know thy whole neighborhood

- OSPF - Dijkstra algorithm - it is an open standard!
> metric - "cost" or "shortest path"

Classful vs Classless

Classful

- does not send subnet mask info in routing updates
- does not support subnetting or VLSM
- RIPv2 - classful by default

Classless

- Includes subnet mask information in routing updates
- supports VLSM and subnetting

Routing Table

R 172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0

R - route source
172.16.4.0/28 - destination network
[120 - administrative distance
2] - metric (for ospf it is cost)
209.165.200.226 - next-hop IP
00:00:12 - route timestamp
Serial0/0/0 - outgoing interface

Levels of Routes:

Ultimate Route - in the routing table

/ Level 1 Route

- the subnet address (192.168.1.**0**/24)

Level 1 Parent Route

- only a parent route if it is a **supernetted** address

Level 2 Child Route

- the actual subnet itself (192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/28)

why rip sucks

March 23, 2023 12:13 PM

when a link fails, it marks it as "possibly down"
- then 30 seconds later (this is the hold down timer) it checks
then it gets marked as "down" and flushed from the system

those hold down timers are the thing that takes forever

OSPF - Open Shortest Path First (single area)

March 23, 2023 12:02 PM

- OSPF is old (1989)

OSPF areas
- the backbone area is **Area 0** always
- they are autonomous systems - meaning a single organization management

OSPF features
- the outer most router is an "autonomous system boundary router"
- a router that is the interface of two **AREAS** is an "area border router"
- still converges - all routers know all other routers in a network

OSPF Routing Algorithm (Dijkstra)
- the only method is cost, it looks for lowest cost path
- anything 100 mbps or faster = cost of 1

create an LSDB (link state database)
- this contains the link state, the link cost

OSPF: The beginning.
- sends a "hello" packet to all of its neighbors.
  - it does this to form an **adjacency**
- a neighbor is a router that shares the same link and is running OSPF protocol

OSPF Neighbor Process
stage 1 - down state: this is before the router knows about its neighbors (immediately after pressing enter to make it OSPF)

stage 2 - init state: R2 and R3 receive the hello packet from R1 - put it in the **OSPF neighbor table**

stage 3 - two-way state: R2 and R3 are sending hello packets **back**
- this is where they find out neighbor IDs, and can become adjacent

stage 4 - ExStart stage - specifies that DR & BDR (designated and backup designated routers) have been elected.
- initial sequence number for adjacency formation is also selected

stage 5 - exchange state - OSPF routers exchange Database Descriptor (DBD) packets
- contain LSA (Link State Advertisement) headers that tells routers the full content of the Link State Database (LSDB)
- they compare the info from their own to see if updates need to be made)

stage 6 - loading state - all the info is syncing up

stage 7 - full state - all functioning, everything is fully synced, normal operations.

224.0.0.5 - hello packets are sent to THIS multicast address (all OSPF routers)
224.0.0.6 - all OSPF DR (designated) / BDR (backup designated routers)

Designated router: (method one)
- command (OSPF Priority) - based on router ID (ALWAYS HIGHEST)
- no router ID? - highest loopback ID
- no loopback? - highest physical interface IP

(method 2 - terry method)
- command - interface priority (decimal value, 0-255) - default is 1 (still looking for highest)

setting OSPF metric
- auto-cost reference-bandwidth ?
- the ? is the amount of mbps that will be the reference (so 1000 is gig, 10000 is 10 gig) > this part might be wrong !

you can manually change the cost of a single interface (dont do that)

R 172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0

R - route source
172.16.4.0/28 - destination network
[120 - administrative distance
2] - metric (for ospf it is cost)
209.165.200.226 - next-hop IP
00:00:12 - route timestamp
Serial0/0/0 - outgoing interface

Passive interface does NOT send hello packets
- passive-interface g0/0

not necessary to mark point to point routers, but you can (within OSPF)

frame relay (dont worry about)
- protocol that does not support broadcast messages

OSPF Designated Router (DR)
- the point is to have the designated and backup designated to be the only 2 who "collect" all info and redistribute it out
-they use 244.0.0.6 to communicate (still multicast)

OSPF Router ID
"show ip protocols"
"show ip ospf"
"show ip ospf interface"

'router ospf x' - where x is a number that represents the router ID (doesn't need to be the same as the neighbor, but should be)

Initial Config: Single Area OSPF
interface loopback0
 ip address 172.16.1.1 255.255.255.128
 ip ospf network point-to-point
!
interface g0/2
 ip address 192.168.0.253 255.255.255.252
 ip ospf priority 200
!
router ospf 14
 router-id 172.16.255.255 - sets the router ID
 passive-interface g0/0 - sets this interface to a passive interface
 network 172.16.1.1 0.0.0.0 area 0 - this looks for this router specifically throughout that interface
^^THIS IS NOT ALL THE COMMANDS

OSPF does not go through TCP or UDP (it is right in the IP packet)
- protocol field of 89

we don't do authentication in first year,
- **Au Type and authentication field contain all 0's for us** because we dont use it

OSPF Packet Types:
1 - hello - discovers and builds adjacencies between neighbors
2 - database description (DBD) - checks for database sync between OSPF routers
3 - link-state request (LSR)
4 - link-state update (LSU)
5 - link-state acknowledgement (LSAck)


once convergence has happened, **hello packets are sent by default every 10 seconds**
- the dead interval timer (40s) starts, after 40 seconds, it flushes that link

why would you use multi area OSPF
- you want to be able to summarize large routing tables (does not summarize by default)

typical exam network - will have around 10-11 routers

OSPF Demo

March 29, 2023 3:02 PM

Thing you always have to remember with OSPF:
- CCNA all routing is done on routers.

In an OSPF autonomous system the shared link is: Network Management VLAN

HAVE to make sure that you advertise the NETWORK MANAGEMENT VLAN

4 different ways to do a network statement: (identify the interfaces on that network)
- for us, best practice is explicit address, network address with subnet mask

- method 2 - network address for int with wildcard mask - not very common **ON CISCO CCNA**

- method 3 - arguably most common - 0.0.0.0 255.255.255.255 - find any interface, all in the case of single area

- method 4 - summary method (that doesn't summarize) - 192.168.0.0 0.0.3.255 - this IS NOT a summary, it FINDS interfaces

OSPF single area (area 0) CANNOT be summarized

a network statement in OSPF finds interfaces,

COMMANDS
1. router ospf
2. router id
3. autocross reference bandwidth
4. passive interface **(do not send hello's, you can only do this on routed layer 3 or routers)**

default route is an external route
we propagate this through OSPF

DEMO FOLLOW ALONG:
all IPs are configured

R1
- going out G0/3/0 (OUTSIDE NAT)
- going inside through G0/0/0 (INSIDE NAT)

'router ospf 34' - (this number doesnt matter)
'router-id 1.1.1.254' - need a designated router - ethernet is a multiaccess media (always)
^^^ it is not an IP address. **HIGHEST NUMBER WINS. (this will be second guy)**
'auto-cost reference-bandwidth 1000' - in Mbps, so 1000 is gigabit **(you need to change this for every router in the domain)**
'network 192.168.255.254 0.0.0.0 area 0' - this tells you which network to look for interfaces on
'default-information originate' - propagate default route to the rest of the network

VLAN 16 is shared logical link - (NetMgmt VLAN, and doesnt have a helper address)

S2
'int vlan 16'
'ip ospf priority 200' - only for the shared link (vlan 16)
'exit'

'router ospf 56'
'router-id 1.1.1.255' - this makes this the default router for **EVERYTHING**
'auto-cost reference-bandwidth 1000' - setting cost to same as R1
'network 192.168.13.254 0.0.0.0 area 0' - for VLAN 13
'network 192.168.14.254 0.0.0.0 area 0' - for VLAN 14 (these are setup for HSRP, you don't need to do this)
'network 192.168.15.254 0.0.0.0 area 0' - for VLAN 15 (
'network 192.168.16.254 0.0.0.0 area 0' - **for VLAN 16**
'network 192.168.255.253 0.0.0.0 area 0' - this is the command that makes an adjacency with **R1**

R1 will now have connections to 192.168.(13-16).0 - they were found through S2 and OSPF

S1
(dont need ospf priority because the designated router already has one, and there's no point)
'router ospf 1'
'router-id 1.1.1.1'
'auto-cost reference-bandwidth 1000'
'network 192.168.10.254 0.0.0.0 area 0' - for VLAN 10
'network 192.168.11.254 0.0.0.0 area 0' - for VLAN 11
'network 192.168.12.254 0.0.0.0 area 0' - for VLAN 12
'network 192.168.17.254 0.0.0.0 area 0' - for VLAN 17
'network 192.168.16.253 0.0.0.0 area 0' - makes the adjacency with **S2**

passive interface command:
'passive-interface vlan X'
'passive-interface vlan 10'
'passive-interface vlan 11'
'passive-interface vlan 12'
'passive-interface vlan 17'
SETTING PASSIVE-INTERFACE ON VLAN 16 WILL BREAK OSPF, THIS IS THE ONLY FORM OF COMMUNICATION.

What is the definition of passive interface: DO NOT *SEND* HELLO'S

First Hop Redundancy Protocols - HSRP

April 5, 2023 3:02 PM

- add a redundant gateway to servers & clients in case one goes down.
- devices today very rarely fail, not the case a ton of years ago.

router redundancy
- introduces the **virtual router (192.168.1.254)**

- **active gateway** - the gateway that currently owns the virtual router address (192.168.1.253 **& 192.168.1.254)**
- standby router - the backup for the active router, will automatically switch to own virtual router address upon old active gateway failure. (192.168.1.252)

the default priority is - 100 | higher is better.
- you will see 105, and 110 often.

- pre empt command - allows one to come up after another fails.

HSRP Groups
- Group Number - terry likes group number as VLAN ID (good practice)
(ex. Active 10/11 & Standby 10/11)

HSRP Priority and Preemption commands

interface vlan 10
ip address 172.20.127.253 255.255.255.0
standby version 2
standby 10 ip 127.20.127.254
standby 10 priority 105 - sets priority to 105
standby 10 preempt - sets highest priority router to active router RIGHT NOW
standby 10 track g1/0/1 - lets you monitor the interface

HSRP default mac address: -
version 1 - 0000.0c07.acXX
version 2 - 0000.0c97.fXXX

TEST:
a combo of OSPF and HSRP **IN THE SAME FILE**
theory test - 42 questions
- vast majority about routing
- 1 or 2 are static routing (based on default route)
- generic dynamic routing
- a bunch of ospf questions
- a few subnetting
- a few HSRP

Practical -
no more than 6 infrastructure devices

- ospf
- hsrp

out of 60 marks, mostly repetitve

router ospf
router id
autocost
network statement
originate

version
standby version
standby ip
standby priority
standby preempt

ip route

OSPF Config Notes

April 13, 2023 10:24 AM

ospf, then HSRP, explicit IP network statements
PAY ATTENTION TO AUTOCOST

OSPF NOTES:

router ospf <#> || any number, doesn't really matter

router-id <a.b.c.d> || the highest ID number gets to be the master router, in IP format, (ex. 1.1.1.255)
|| you want to set this for any IP that is connecting to an OSPF device

ip ospf priority (?) || for setting priority (goes above router ID) on an individual interface

auto-cost reference-bandwidth <1000> || 1000 sets gigabit to the standard. make sure its the same on all

network <a.b.c.d> 0.0.0.0 area 0 || a.b.c.d is the IP OF YOUR OUTGOING NETWORK ON THAT DEVICE. 0.0.0.0 is
|| saying that it is a direct connection (interface, best practice) **

(network <a.b.c.d> <a'.b'.c'.d'> area 0) || network finder, not best practice (subnet going out, then wildcard of subnet)

(network 0.0.0.0 255.255.255.255 area 0) || identifies all networks, not best practice, but it works.

default-information originate || only if you are trying to propagate default route info throughout ospf
|| default route info HAS to be on THAT device if this command is turned on

show ip route || this is to see the connections of OSPF on that device

show ip ospf neighbor || this is to see the OSPF neighbor table (direct connections)

show ip protocols || this shows what this will tell you what ospf protocol is being used on a device

show ip ospf || this shows the ospf id number

show ip ospf database || this shows the ip ospf database

show ip int br | e una || show the interfaces (excludes the ones that are unavailable)

==========
==========
==========

OSPF TEMPLATE

ORIGINATING ROUTER:

!
ip route 0.0.0.0 0.0.0.0 A.B.C.D
ip route 0.0.0.0 0.0.0.0 INTERFACE
router ospf # (Any. Keep the same.)
 router-id 1.1.1.254 (highest number wins for designated router)
 auto-cost reference-bandwidth # (same on every router)
 network 192.168.255.254 0.0.0.0 area 0 (router int ip)
 default-information originate
 do write
!

MAIN (MOST CENTRAL) ROUTING DEVICE:

show run (for vlans to use)

!
router ospf # (Any. Keep the same.)
 router-id 1.1.1.255 (Highest ID)
 auto-cost reference-bandwidth # (same as above)
 network 192.168.13.254 0.0.0.0 area 0 (each configured VLAN)
 network 192.168.14.254 0.0.0.0 area 0 ^
 network 192.168.15.254 0.0.0.0 area 0 ^
 network 192.168.255.253 0.0.0.0 area 0 (int ip connected to router)
!

ROUTING DEVICE NOT CONNECTED TO ROUTER:

show run (for vlans to use)

!
router ospf # (Any. Keep the same.)
 router id 1.1.1.1
 auto-cost reference-bandwidth # (same as above)
 network 192.168.10.254 0.0.0.0 area 0 (each configured VLAN)
 network 192.168.11.254 0.0.0.0 area 0 ^

network 192.168.12.254 0.0.0.0 area 0 ^
network 192.168.17.254 0.0.0.0 area 0 ^
network 192.168.16.253 0.0.0.0 area 0 ^
!

show ip osfp neighbor

HSRP Config Notes

April 13, 2023 10:29 AM

HSRP NOTES:

interface vlan 10	|| doing in this in vlan 10
ip address <a.b.c.d> <subnet>	|| a.b.c.d is replaced by the second or third highest address || (.253 or .252)
standby version 2	|| this sets the HSRP version to 2
standby 10 ip <a.b.c.d>	|| a.b.c.d is replaced by the virtual default gateway (.254)
standby 10 priority <#>	|| 100 is default, the higher the better
standby 10 preempt	|| forces the highest priority to become the active router
standby 10 track <int>	|| allows you to monitor the interface for HSRP
show standby brief	|| to show the HSRP info you need

==========
==========
==========
==========

HSRP TEMPLATE

L3 ROUTING:

ACTIVE L3 ROUTER (HIGHEST PRIORITY):
!
int vlan 10 (vlan id for gateway)
 ip address 172.20.127.253 255.255.255.0 (vlan ip/mask)
 standby version 2
 standby 10 ip 172.20.127.254 (Ghost router)
 standby 10 priority 105 (Higher than other router)
 standby 10 preempt
 standby track G1/0/1 (Int to virtual router)
 standby track G1/0/2 (Int to network)
!

NON-ACTIVE L3 ROUTER:
!
int vlan 10 (vlan id for gateway)
 ip address 172.20.127.252 255.255.255.0 (vlan ip/mask)
 standby version 2
 standby group# ip 172.20.127.254 (Ghost router)
 standby group# priority 100 (Lower than other router)
 standby group# preempt
 standby track G1/0/1 (Int to virtual router)

standby track G1/0/2 (Int to network)
!

ROUTER:

ACTIVE L3 ROUTER (HIGHEST PRIORITY):
!
int G0/0 (int for gateway)
ip address 172.20.127.253 255.255.255.0 (gateway ip/mask)
standby version 2
standby G0/0 ip 172.20.127.254 (Ghost router)
standby G0/0 priority 105 (Higher than other router)
standby G0/0 preempt
standby track G1/0/1 (Int to virtual router)
standby track G1/0/2 (Int to network)
!

NON-ACTIVE ROUTER (LOWER PRIORITY):
!
int G0/0 (int for gateway)
ip address 172.20.127.252 255.255.255.0 (gateway ip/mask)
standby version 2
standby group# ip 172.20.127.254 (Ghost router)
standby group# priority 100 (Lower than other router)
standby group# preempt
standby track G1/0/1 (Int to virtual router)
standby track G1/0/2 (Int to network)
!

April 13, 2023 11:59 AM

16 255.255.192.0

11 000000

2
32
+ 16
+ 8
+ 4
+ 2
+ 1
63

20 255.255.240.0

1111 0000

128
+ 64
+ 32
+ 16
240

128
+ 64
+ 32
224

8
+ 4
2
1
15

172.16.1-16

2
16
+ 8
+ 4
+ 2
+ 1
31

127 - 64

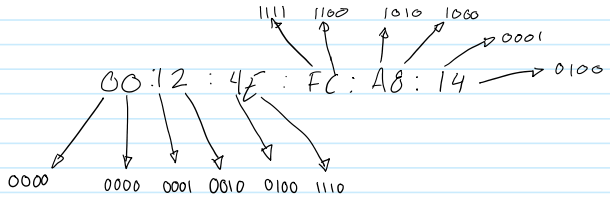
012
127
- 64
63

IPV6

April 19, 2023 3:00 PM

why do we need IPv6? - running out of IP addresses

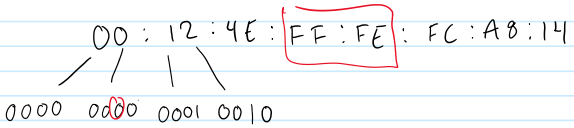
what does IPv6 give us:
- 340 undecillion addresses
it doesnt play well with nat tho :/



★ **theres 128 bits in an IPv6 address**
- broken up into 8 hextets
1 hextet = 16 bits
★ **each hextet is separated by a COLON ONLY**

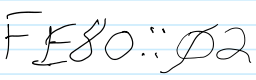
prefix = subnet mask (we use prefix now)

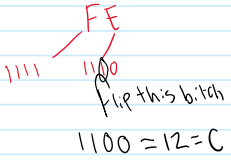
we don't subnet in IPv6 because we got so damn networks
- we are given 65000 NETWORKS



★ **the global routing prefix is 48 bits always**
★ **subnet range is 16 bits - we control this one**
interface ID is 64 bits

★ - know slide 8





IPV6 zero elimination/suppression
- you remove any leading 0s in a hextet
- :0001: becomes :1:

IPv6 sets of 0s become either
- :0:1abc:0:0:
or - :0: and ::
double colons are only for the largest set of 0000s, only ever put :: not more.

★ **anycast is not used in the LAN, it is only used in the WAN**
- multiple different hosts will belong to the same anycast
- used for streaming often
    - it sends to the BEST member of the anycast group

multicast
FF02::6/8 - this is the OSPF designated routers
- exact same way as IPv4

unicast types
★ - link-local (**NOT ROUTABLE**) MANDATORY
    - just like 169 (APIPA)
    - FE80::/10 (always /10, don't have to show it)
    - EVERY link in a network NEEDS a link-local address
    - best practice for DG = FE80::1/10

- global unicast
    - public topology first 48 bits
    - site topology is next 16 bits
    - interface identifier last 64 bits

★ - slide 19

- unique local address (**ROUTABLE**)
    - the same as a private address in ipv4
    - FC00 - globally assigned addressing
    - FD00 - locally assigned addressing

★ **any IPv6 client that accesses the internet needs at LEAST 2 IP addresses.**

loopback address
    - ::1: - the same as 127.0.0.1

unspecified address
    - ::/128 - the same as 0.0.0.0 255.255.255.255

default route
    - ::/0 - the same as 0.0.0.0 0.0.0.0

enabling IPv6 on cisco routers
- IPv6 routing is not enabled by default

'ipv6 unicast-routing' - enables IPv6 routing
int g0/1
'ipv6 address FE80::1 link-local' - creates the link local address (NEEDED)
'ipv6 address 2620::/64 eui-64' - creates a global unicast address on the interface

★ **Extended Unique Identifier (EUI-64) - KNOW SLIDE 30**
- it takes the mac address (48 bits)
- puts FFFF in the middle of the two halves
- swaps the second last bit of the first hextet

00:21:2F:B5:6E:10 -> 02:21:2F:FF:FF:B5:6E:10

★ **Network Discovery Protocol (NDP)** - uses local-link
- the ipv6 version of ARP and ICMP (ALL IN ONE)

neighbor side
- neighbor solicitation (NS) - requests L2 address from neighbor
- neighbor advertisement (NA) - response to NS

router side
- router advertisement (RA) - the router will send a request to the client when it comes up
- router solicitation (RS) - the client will send a request to the router when it comes up

IPv6 static routing
- ipv6 route ?
ipv6 route 2002:FC::/64 g0/2 2002:EF::1

CISCO IPv6 needs IOS 15 or greater

17 questions:
- no subnetting
- but there will be 0 suppression

make sure there is 8 hextets
make sure it's only 0-9&a-f

★

IPv6 Demo Notes

April 20, 2023 12:01 PM

test: will have 5 routers

- IPv6 only - auto-configuration where the client gets an IP from the router network

R1:

en
conf t

ipv6 unicast-routing - this allows you to use IPv6

int g0/0
ipv6 enable - enables ipv6 on the interface
ipv6 address 2620:FC:1::1/64 -
do show ipv6 int g0/0

ipv6 address FE80::1 link-local
no shut

terry likes to do global unicast first because:
- common practice for default gateway is ::1
- it automatically sets it to the EUC-64 ID
- if the link-local address is made first, the global unicast takes from the link-local address

S1:
en
sho flash - check to see if you are using version 15
to enable ipv6 on a switch:
sdm prefer dual-ipv4-and-ipv6 default
to go back to only ipv4 on a switch:
sdm prefer default
en
conf t
int vlan 1
ipv6 enable
ipv6 address autoconfig
no shut

show ipv6 interface vlan 1
ip should now be on there??

R1:
int g0/1
ipv6 enable
ipv6 address FE80::1 link-local
ipv6 address 2001:db8:1::1/64
no shut

exit
ipv6 route 2620:FC:2::/64 g0/1 2001:db8:1::2

R2:
en
conf t
ipv6 unicast-routing
int g0/0
ipv6 enable
ipv6 address FE80::2 link-local

ipv6 address 2620:FC:2::1/64
no shut

S2:
en
conf t
sdm prefer dual-ipv4-and-ipv6 default
reload
int vlan 1
ipv6 enable
ipv6 address autoconfig
no shut

R2:
int g0/1
ipv6 enable
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:1::2/64
no shut

ipv6 route ::/0 g0/1 2001:DB8:1::1

PC1 should now be able to ping PC2

R3:
en
conf t
ipv6 unicast-routing
int g0/0
ipv6 enable
ipv6 address FE80::3 link-local
ipv6 address 2620:FC:3::1/64
no shut

S3: - only difference is you don't need to enable it globally (like on layer 2 switch)
en
conf t
int vlan 1
ipv6 enable
ipv6 address autoconfig

April 26, 2023 2:57 PM

2001:db8:0:1

000b:be FF FE 1d:9dd6

0000 0010

2001:db8:0:1:020b:beff:fe1d:9dd6