Post 5

Thursday, January 24, 2019 11:19 PM

ADJUST/TROUBLESHOOT SINGLE AREA OSPF P1

OSPF: Link state routing protocol
Routers/L3 switches learn about remote networks 1 of 2 ways:

1. Manually: Remote networks entered into r-tale using static routes
2. Dynamically: Remote routes auto learned using a dynamic r-protocol like EIGRP or OSPF

Static Routing: Manual config static routes to reach a specific network

- Not automatically updated
- Must be manually reconfig'd any time topology changes
- Doesn't change until admin reconfigs it

Static routing: 3 uses:

1. Ease of r-table maintenance in smaller networks (not expected to scale)
2. Routing to/from stub networks
    - Stub network: Network accessed by a single route/router only has 1 neighbor
3. Using single route to represent any path (no specific match) w/another route in table
    - Default routes: Used to send traffic to any dest beyond next router

Dynamic Routing: Allow routers to dynamically share info about remote networks

- Routers receiving update auto add info to their routing tables
- Then determine best path/route

Benefits:

- Dynamic r-protocols exchange r-info when topology changes
- Exchange allows routers to auto learn about new networks/find alt paths when link failure occurs

Compared to static:

- Less overhead
- Expense of it is dedicating part of a router's resources for protocol operation (CPU/link/BW)

2 most common dynamic r-protocols:

- **EIGRP: Enhanced Interior Gateway Routing Protocol**
- OSPF: Open Shortest Path First

OSPF: Open Shortest Path First
Link-state r-protocol: Replacement for distance vector r-protocol RIP: Faster convergence/better scaling than RIP
OSPF features:

Classless	Supports VLSM/CIDR
Efficient	R-changes trigger updates (no periodic updates) • Uses SPF alg to choose best path
Fast convergence	Quickly propagates changes
Scalable	Works well w/small/large networks • Routers can be grouped into areas to support hierarchical sys
Secure	Supports MD5 auth • Enabled? OSPF r-only accept encrypted updates from peers w/same pre-shared passwd

Config Single-Area (OSPFv2)

```
R1(config)# int g0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-rtr)# router id 1.1.1.1
```

R1(config-rtr)# auto-cost reference-bandwidth 1000
R1(config-rtr)# network 172.16.1.0 0.0.0.255 area 0
R1(config-rtr)# network 172.16.3.0 0.0.0.3 area 0
R1(config-rtr)# network 192.168.10.4 0.0.0.3 area 0
R1(config-rtr)# passive-interface g0/0

- g0/0 int: Config'd to reflect BW
- OSPF r-config mode: r-id assigned | reference BW adjusted to acct for fast ints
- 3 networks attached (if set to advertise: Masks would be 0.0.0.0)

Verify Single-Area OSPF (OSPFv2)

sh ip ospf neighbor	**Verifies router formed adjacency w/neighbors** **If:** r-ID of neighbor router not displayed/No FULL state • No adjacency formed
sh ip protocols	**Verify OSPF config info:** • Process/Router-ID • Network router advertising? • Neighbor receiving updates • Default AD (admin distance): 110 for OSPF
sh ip ospf	**Displays:** • OSPF process/Router ID • OSPF SPF/area info
sh ip ospf int	**Displays list of:** • Every OSPF-enabled int • Helps determine whether network statements correct
sh ip ospf int br	**Displays:** Summary/Status of OSPF-enabled ints

Config Single-Area (OSPFv3)
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# auto-cost reference-bandwidth 1000
R1(config-rtr)# int g0/0
R1(config-if)# bandwidth 10000000
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# int s0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# int s0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end

- Router ID: manually assigned/reference BW adjusted to acct for fast ints
- Ints participating in OSPFv3 config'd
- No wildcard mask

Verify Single-Area (OSPFv3)

sh ipv6 ospf neighbor	**Verifies router formed adjacency w/neighbors** **If:** r-ID of neighbor router not displayed/No FULL state • No adjacency formed
sh ipv6 protocols	**Verify OSPF config info:** • Process/Router-ID • Network router advertising? • Neighbor receiving updates • Default AD (admin distance): 110 for OSPF
sh ipv6 route ospf	Specs about OSPFv3 routes in r-table
sh ipv6 ospf int br	Useful to display summary/status of OSPFv3 enabled ints

OSPF Network Types

Point-to-point	2 routers interconnected over common link • No other routers on the link • Often WAN link config
Broadcast multiaccess	Multiple routers interconnected over Ethernet network

Nonbroadcast multiaccess (NBMA)	Multiple routers interconnected in network that doesn't allow broadcasts • Such as Frame Relay • Frame Relay doesn't allow broadcasts • OSPF must be config'd accordingly to create adjacencies
Point-to-multipoint	Multiple routers interconnected in hub/spoke topology over NBMA network • Often used to connect branch sites (spokes) to central site (hub)
Virtual links	Special OSPF network used to interconnect distant OSPF areas to backbone area)

Multiaccess network: A network w/multiple devices on same shared media (sharing comms)
- Ethernet LANs: Most common example of broadcast multiaccess networks

Broadcast network: All devices on network see all broadcast/multicast frames
- Multiaccess networks b/c there may be numerous hosts/printers/routers/devices all members

Challenges in Multiaccess Networks
2 issues for OSPF regarding LSA flooding:

Creation of multiple adjacencies	Ethernet networks: Could potentially interconnect many OSPF routers over common link • Creating adjacencies w/every router: Unnecessary/undesirable • Leads to excessive LSAs exchanged bet routers
Extensive flooding of LSAs	Link-state routers flood link-state packets when OSPF initialized/when topology changes • Flooding can be excessive

Formula can be used to calc the # of required adjacencies:
# of adjacencies required for any # of routers (n) on multiaccess network:
n (n – 1) / 2

OSPF Designated Router
DR/Designated Router: Solution to managing # of adjacencies/LSA flooding on multiaccess networks
On multiaccess networks:
- OSPF elects DR to be the collection/distribution point for LSAs sent/received
- BDR (backup) also elected in case DR fails

BDR/Backup Designated Router: Listens passively to exchange/maintains relationship w/all routers.
- If DR stops producing Hello packets: BDR promotes itself/assumes role of DR

DROTHER: All other non-DR/BDR routers
- Only form full adjacencies w/DR/BDR in network
- Instead of LSA flooding to all routers: Only send LSA's to DR/BDR using multicast address 224.0.0.6 (all DR routers)

DR/BDR elections ONLY occur in multiaccess networks: They don't happen in point-to-point ones
Verify DR/BDR Roles sh ip ospf
Verify DR/BDR Adjacencies sh ip ospf neighbor
Unlike serial links that only display a state of FULL
- **State of neighbors in multiaccess networks can be:**

FULL/DROTHER	A DR/BDR router that is fully adjacent w/non-DR/BDR router **These 2 neighbors can exchange:** • Hello packets • Updates • Queries • Replies • Acknowledgments
FULL/DR	Router is fully adjacent w/indicated DR neighbor **These 2 neighbors can exchange:** • Hello packets • Updates • Queries • Replies • Acknowledgments

FULL/BDR	Router is fully adjacent w/indicated BDR neighbor **These 2 neighbors can exchange:** • Hello packets • Updates • Queries • Replies • Acknowledgments
2-WAY/DROTHER	Non-DR/BDR router has a neighbor relationship w/another non-DR/BDR router **These 2 neighbors exchange:** • Hello packets
Normal state OSPF router: Usually FULL	**If router stuck in another state: Indication that:** • There are problems in forming adjacencies **Exception to this: 2-WAY state** • Normal in a multiaccess broadcast network.

In multiaccess networks:

- DROTHERs only form FULL adjacencies w/DR/BDR
- **DROTHERs:** Still form 2-WAY neighbor adjacency w/any DROTHERs that join network
    - All DROTHER routers in multiaccess still receive Hello packets from all other DROTHERs
    - 2 DROTHERs form neighbor adjacency? Neighbor state 2-WAY/DROTHER

Default DR/BDR Election Process
How do DR/BDR get elected?
OSPF DR/BDR election decision based on following criteria in order:

- **Routers elect router w/highest int priority as DR: 2nd highest elected BDR**

    1. Priority: Any # 0 – 255
    2. Higher priority: More likely router will be selected as DR
    3. Priority set 0? Router can't become DR
    4. Multiaccess broadcast ints: Default priority = 1
    5. Unless config: All routers have equal priority value/rely on another tie break method during election

- **If int priorities equal: Router w/highest r-ID elected DR: 2nd highest r-ID is BDR**

Router ID determined 1 of 3 ways:

1. Manually config
2. If no r-IDs config: Determined by highest loopback IP
3. If no loopback ints config: r-ID determined by highest active IPv4 address
4. **In IPv6:** If no IPv4 addresses config: r-ID must be manually config w/r-ID cmd; or OSPFv3 doesn't start

Serial ints: Default priorities set 0: They don't elect DR/BDR's

- **DR/BDR election takes place as soon as 1st router w/OSPF-enabled int active on multiaccess**

    1. Can happen when powered on/OSPF network cmd for that int config
    2. Election process only takes few seconds
    3. If all of routers on multiaccess haven't booted: Possible a router w/lower r-ID becomes DR

DR/BDR Election Process
OSPF DR/BDR elections NOT preemptive:

- If a new router w/higher priority/r-ID is added after the DR/BDR election
- It doesn't take over the DR/BDR role
- Why? B/C those roles were already assigned/doesn't initiate a new election process

After DR elected: Remains DR until 1 of following happens:

- DR fails
- OSPF process on DR fails/stops
- Multiaccess int on DR fails/shuts down

If DR fails: BDR auto promoted to DR

- Even if another DROTHER w/higher priority/r-ID added to network after initial DR/BDR election.
- After BDR promoted to DR: New BDR election: DROTHER w/higher priority/r-ID elected as new BDR

OSPF Priority

DR becomes focal point for the collection/distribution of LSAs

- Must have sufficient CPU/meme to handle the workload
- Possible to influence DR/BDR election process through configs
- Instead of relying on r-ID: Better to control election by setting int priorities
- Priorities: Int-specific value: Provides better control on multiaccess
- Allows router to be DR in 1 network/DROTHER in another

Set priority of an int:

ip ospf priority value	OSPFv2: Int cmd
ipv6 ospf priority value	OSPFv3: Int cmd
Value can be	**0:** Doesn't become DR/BDR **1 – 255:** Higher priority: More likely router becomes DR/BDR on int

Propagating Default Static Route in OSPFv2

OSPF: Router connected to Internet is used to propagate a default route to other routers in OSPF routing domain

- Router is called the edge/entrance/GW router

ASBR: Autonomous System Boundary Router: OSPF: Router located bet OSPF routing domain/non-OSPF network

Propagate default route: Edge router must be config'd w/:
Default static route using: ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
default-information originate Source of default route info/propagates default static route in OSPF updates
IPv6
ipv6 route ::/0 {ipv6-address | exit-intf}
default-information originate

OSPF Hello/Dead Intervals

OSPF Hello/Dead intervals are config on per-int basis: OSPF intervals much match neighbor or adjacency doesn't occur
Verify: **sh ip ospf** | **sh ip ospf neighbor**
Modifying OSPFv2 Intervals

- May be desirable to change OSPF timers (so routers detect failures in less time)
- Doing so increases traffic: Sometimes need for quick convergence is more impt than extra traffic
- Default Hello/Dead intervals based on best practices: Should only be altered in rare situations

OSPF Hello/Dead intervals can be mod manually using int config cmds:
ip ospf hello-interval *seconds*
ip ospf dead-interval *seconds*
Reset intervals to default:
no ip ospf hello-interval
no ip ospf dead-interval

Modifying OSPFv3 Intervals
ipv6 ospf hello-interval seconds
ipv6 ospf dead-interval seconds

sh ipv6 ospf neighbor
sh ipv6 ospf int

Routers are Targets

- Often targets of network attacks
- Routing sys can be attacked by disrupting routing peers/falsifying info carried w/in r-protocol
- Falsified r-info may be used to cause sys to lie to each other, cause a DoS, or cause traffic to follow path it wouldn't normally

Consequences of falsifying r-info:

- Redirecting traffic to create routing loops
- Redirecting traffic so it can be monitored on insecure link
- Redirecting traffic to discard it

- To mitigate r- protocol attacks: Config OSPF auth

Secure Routing Updates

- When neighbor auth has been config: Router authenticates source of each r-update packet that it receives
- Accomplished by exchange of authenticating key known to both sending/receiving router
- Enable OSPF authentication
- Can be none (null)/simple/Msg Digest 5 (MD5)

OSPF supports 3 types of authentication:

Null	Default method: No authentication used for OSPF
Simple passwd auth	AKA Plaintext authentication: Passwd/update sent in plaintext over network • Legacy method of OSPF auth
MD5	Most secure/recommended method • Provides higher sec b/c passwd never exchanged bet peers • It's calc using MD5 alg: Matching results authenticate sender

RIPv2, EIGRP, OSPF, IS-IS, and BGP all support various forms of MD5 authentication.

MD5 Authentication

1. Combines routing msg w/pre-shared secret key
2. Calcs the signature using MD5: Signature AKA hash value
3. MD5 doesn't encrypt msgs: Content is easily readable
4. Packet is opened: Combined r-msg w/pre-shared secret key/calcs the sig using MD5 alg
5. If sigs match: Accepts r-update: If NOT: update discarded

OSPFv3 (IPv6): Doesn't include any auth capabilities on its own

- Relies on IPSec to secure comms bet neighbors using **ipv6 ospf authentication ipsec spi**
- Simplifies OSPFv3 protocol/standardizing its auth mehcanism

OSPF supports r-protocol auth using MD5:

- MD5 auth can be enabled globally for all ints/on per-intbasis

Enable OSPF MD5 authentication globally, configure:
ip ospf message-digest-key key md5 password
area area-id authentication message-digest router
Forces auth on all OSPF enabled ints

- If int isn't config w/**ip ospf message-digest-key** : Will not be able to form adjacencies w/OSPF neighbors

Enable MD5 auth on a per-int basis:
ip ospf message-digest-key key md5
ip ospf authentication message-digest
Verify OSPF MD5 Authentication

sh ip ospf int	Verify r-table is complete successful auth can be confirmed

OSPF adjacencies will not form if:

- ints not on same network
- OSPF network types don't match
- OSPF Hello/Dead Timers don't match
- Int to neighbor is incorrectly config as passive
- Missing/incorrect OSPF network cmd

OSPF States FULL/2WAY states normal: All other states transitory: Shouldn't remain in those states for periods of time

Troubleshooting Cmds

sh ip protocols	**Verify vital OSPF config info** • Includes: OSPF process ID, r-ID • Networks router is advertising, neighbors router receiving updates from • Default admin distance (110 for OSPF)
sh ip ospf neighbor	**Verify router formed adjacency w/neighboring routers** • Displays neighbor r-ID, neighbor priority, OSPF state, Dead timer • Neighbor int IP address, int neighbor is accessible through • If r-ID of neighboring router isn't displayed: Doesn't show as FULL/2WAY:

	• 2 routers haven't formed OSPF adjacency • If 2 routers don't establish adjacency, link-state info not exchanged • Incomplete link-state db's can cause inaccurate SPF trees/r-tables • Routes to dest networks may not exist/may not be most optimum path
sh ip ospf int	**Display OSPF params config'd on an int** • Such as: Process ID int assigned to • Area ints are in • Cost of int • Hello/Dead intervals Adding int name/# to cmd displays output for specific int
sh ip ospf	**Examine OSPF process ID/r-ID** • Displays OSPF area info: Last time SPF alg was calc
sh ip route ospf	Display only OSPF learned routes in r-table
clear ip ospf [process-id] process	Reset OSPFv2 neighbor adjacencies

Components of Troubleshooting OSPF

1. Neighbor adjacencies
2. Missing routes
3. Path selection

If adjacency bet 2 routers established:

- Verify there are OSPF routes in r-table using sh ip route ospf
- **If no OSPF routes:** Verify no other r-protocols w/lower admin distances running in network
- Verify if required networks advertised in OSPF
- Verify if access list config on router that would filter incoming/outgoing r-updates
- If all required routes in table, but path traffic takes isn't correct, verify OSPF cost on ints on path
- Be careful in cases where the ints faster than 100 Mb/s: All ints have this BW/same OSPF cost by default

Troubleshooting Neighbor Issues

- Mismatched MTU sizes on connecting ints
- MTU size is largest network layer packet router will fwd out each int
- Default to MTU size of 1500 bytes
- Value can be changed using ip **mtu sizeinterface** or **ipv6 mtu sizeinterface**
- 2 routers: Mismatched MTU values: Would still attempt to form adjacency: Wouldn't exchange LSDBs/neighbor
    - Relationship would fail