ASA Release 9.2.1 OSPF Enhancements Configuration Example

Contents

Introduction

This document explains new features and commands introduced in Adaptive Security Appliance (ASA) Software Release 9.2.1 related to the Open Shortest Path First (OSPF) protocol.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco ASA 5500-X Series Firewall that runs Cisco ASA Software Release 9.2.(1) and later.
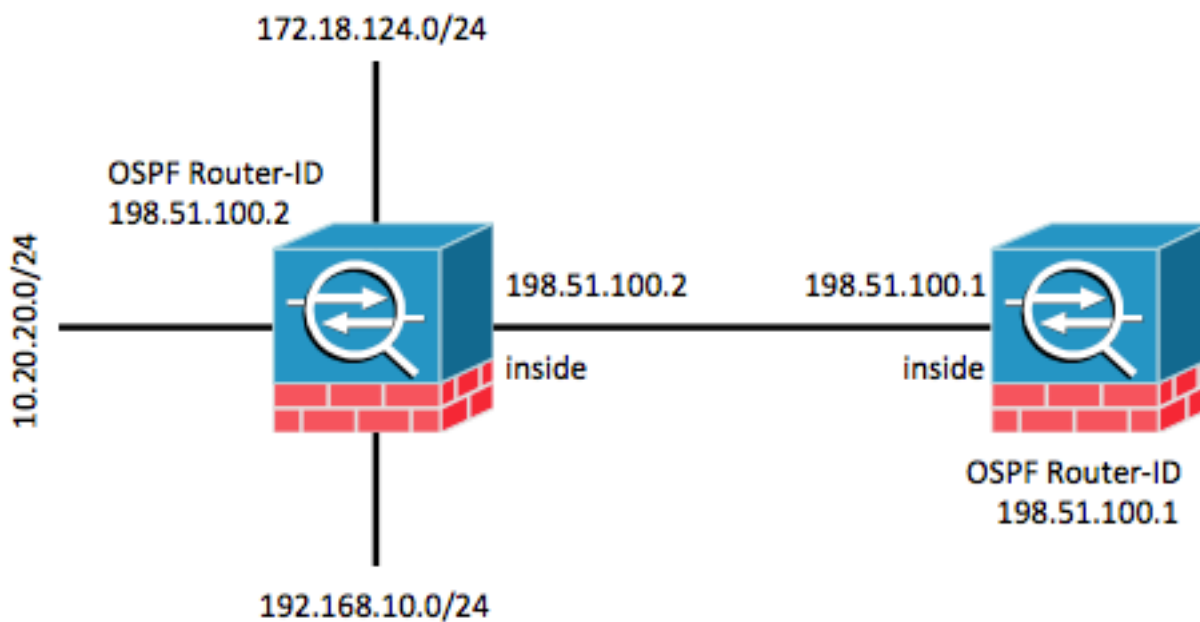
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Configure

Network Diagram

Configurations

OSPF Support for Fast Hellos

OSPF hello packets are packets that an OSPF process sends to its OSPF neighbors in order to maintain connectivity with those neighbors. These hello packets are sent at a configurable interval (in seconds). The defaults are 10 seconds for an Ethernet link and 30 seconds for a non-broadcast link. Hello packets include a list of all neighbors for which a hello packet has been received within the dead interval. The dead interval is also a configurable interval (in seconds) and defaults to four times the value of the hello interval. The value of all hello intervals must be the same within a network. Likewise, the value of all dead intervals must be the same within a network.

OSPF fast hello packets refer to hello packets that are sent at intervals of less than 1 second. In order to enable OSPF fast hello packets, enter the **ospf dead-interval** command. For sub-second hellos, the dead interval is set to 1 second or **minimal** and the hello-multiplier value is set to the number of hello packets you want sent in that 1 second. For example, if the dead interval is set for 1 second, and the hello-multiplier is set for 4, hellos will be sent every 0.25 seconds.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received

over this interface is ignored. It is important to note that the **the dead interval must be consistent on a segment.** Whether it is set to 1 second (for fast hello packets) or set to any other value, it must be consistent across neighbors in that segment. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

In order to enable fast hellos with a multiple of 4, enter the **ospf dead-interval minimal hello-multiplier 4** command under the appropriate interface configuration.

```
 interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 198.51.100.1 255.255.255.0
ospf dead-interval minimal hello-multiplier 4

router ospf 1
network 198.51.100.0 255.255.255.0 area 0
```

Verify with the **show ospf interface** command.

```
asa(config)# show ospf interface

inside is up, line protocol is up
Internet Address 198.51.100.1 mask 255.255.255.0, Area 0
Process ID 928, Router ID 198.51.100.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 198.51.100.1, Interface address 198.51.100.1
No backup designated router on this network
Timer intervals configured, Hello 250 msec, Dead 1, Wait 1, Retransmit 5
Hello due in 48 msec
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

New OSPF Timer Commands for Link-State Advertisement and SPF Throttling

These commands were introduced in ASA Release 9.2.1 and later: **timers lsa arrival**, **timers pacing**, **timers throttle lsa** and **timers throttle spf** as part of the OSPF router configuration.

```
asa(config-router)# timers ?

router mode commands/options:
lsa OSPF LSA timers
pacing OSPF pacing timers
throttle OSPF throttle timers
```

These commands have been removed: **timers spf** and **timers lsa-grouping-pacing**.

More information about the benefits of Link State Advertisement (LSA) and Shortest Path First (SPF) throttling can be found in these documents:

- OSPF Shortest Path First Throttling
- OSPF Link-State Advertisement (LSA)

OSPF Route Filtering with an ACL

Route filtering with an Access Control List (ACL) is now supported. This is achieved with the **distribute-list** command to filter routes.

For example, in order to filter out routes for 10.20.20.0/24, the configuration would look like this:

```
access-list ospf standard deny host 10.20.20.0
access-list ospf standard permit any4
!
router ospf 1
 network 198.51.100.0 255.255.255.0 area 0
 log-adj-changes
 distribute-list ospf in interface inside
```

When the associated ACL is checked, it indicates that it has incrementing hit counts:

```
asa(config)# show access-list ospf
access-list ospf; 2 elements; name hash: 0xb5dd06eb
access-list ospf line 1 standard deny host 10.20.20.0 (hitcnt=1) 0xe29503b8
access-list ospf line 2 standard permit any4 (hitcnt=2) 0x51ff4e67
```

In addition, one can check the Routing Information Base (RIB) on the ASA in order to further verify functionality. Enter the **show ospf rib detail** command in order to report back the full routing information database for the OSPF router process. The 'flags' associated with each route indicate whether or not it has been installed in the RIB.

```
asa(config)# show ospf rib detail

         OSPF Router with ID (198.51.100.10) (Process ID 1)
OSPF local RIB
Codes: * - Best, > - Installed in global RIB

*>  172.18.124.0/32, Intra, cost 11, area 0
    SPF Instance 13, age 0:13:59
    Flags: RIB, HiPrio
     via 198.51.100.2, inside, flags: RIB
      LSA: 1/198.51.100.2/198.51.100.2
*   10.20.20.0/32, Intra, cost 11, area 0
    SPF Instance 13, age 0:13:59
    Flags: HiPrio
     via 198.51.100.2, inside, flags: none
      LSA: 1/198.51.100.2/198.51.100.2
*>  192.168.10.0/32, Intra, cost 11, area 0
    SPF Instance 13, age 0:13:59
    Flags: RIB, HiPrio
     via 198.51.100.2, inside, flags: RIB
      LSA: 1/198.51.100.2/198.51.100.2
*   198.51.100.0/24, Intra, cost 10, area 0
    SPF Instance 13, age 0:52:52
    Flags: Connected
     via 198.51.100.10, inside, flags: Connected
      LSA: 2/198.51.100.2/192.151.100.10
```

In the above output, the routers listed with flags 'RIB' have been installed, while the route with flags 'none' has not been installed. This should be reflected in the global routing table as well. Check with the **show route** command.

```
asa(config)# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
          ia - IS-IS inter area, * - candidate default, U - per-user static route
          o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.106.44.1 to network 0.0.0.0

S*     0.0.0.0 0.0.0.0 [1/0] via 10.106.44.1, tftp
O          172.18.124.0 255.255.255.0 [110/11] via 198.51.100.2, 00:00:03, inside
O          192.168.10.0 255.255.255.0 [110/11] via 198.51.100.2, 00:00:03, inside
O          10.20.20.0 255.255.255.0 [110/11] via 198.51.100.2, 00:00:03, inside
S          10.76.76.160 255.255.255.255 [1/0] via 10.106.44.1, tftp
C          10.86.195.0 255.255.255.0 is directly connected, management
L          10.86.195.1 255.255.255.255 is directly connected, management
```

OSPF Monitoring Enhancements

These commands have been introduced in order to help monitor and observe the OSPF router process. Sample outputs from those commands are provided for reference.

show ospf interface brief

Enter the **show ospf interface brief** command in order to get a quick snapshot of the adjacencies present on this ASA.

```
asa(config)# show ospf interface brief

Interface PID Area IP Address/Mask Cost State Nbrs F/C
inside 1 0 198.51.100.2/255.255.255.0 10 DR 1/1
```
show ospf statistics [Detail]

The **show ospf statistics detail** command provides a brief description about when SPF was run last and how many times it has been run. It also indicates how many new LSAs are added to database.

```
asa(config)#show ospf statistics detail


            OSPF Router with ID (198.51.100.10) (Process ID 1)

 Area 0: SPF algorithm executed 12 times

SPF 3 executed 00:32:56 ago, SPF type Full
 SPF calculation time (in msec):
 SPT    Intra  D-Intr Summ    D-Summ Ext7    D-Ext7 Total
      0       0      0       0       0       0       00
 LSIDs processed R:2 N:1 Stub:1 SN:0 SA:0 X7:0
 Change record 0x0
 LSIDs changed 1
 Changed LSAs. Recorded is LS ID and LS type:
 198.51.100.2(R)

SPF 4 executed 00:28:16 ago, SPF type Full
 SPF calculation time (in msec):
 SPT    Intra  D-Intr Summ    D-Summ Ext7    D-Ext7 Total
      0       0      0       0       0       0       00
 LSIDs processed R:1 N:1 Stub:0 SN:0 SA:0 X7:0
 Change record 0x0
 LSIDs changed 2
 Changed LSAs. Recorded is LS ID and LS type:
 198.51.100.2(R) 198.51.100.10(R)
```

```
SPF 5 executed 00:28:06 ago, SPF type Full
 SPF calculation time (in msec):
 SPT    Intra D-Intr Summ   D-Summ Ext7   D-Ext7 Total
       0      0      0      0       0       0     00
 LSIDs processed R:2 N:1 Stub:1 SN:0 SA:0 X7:0
 Change record 0x0
 LSIDs changed 1
 Changed LSAs. Recorded is LS ID and LS type:
 198.51.100.2(R)

SPF 6 executed 00:26:40 ago, SPF type Full
 SPF calculation time (in msec):
 SPT    Intra D-Intr Summ   D-Summ Ext7   D-Ext7 Total
       0      0      0      0       0       0     00
 LSIDs processed R:1 N:1 Stub:0 SN:0 SA:0 X7:0
 Change record 0x0
 LSIDs changed 2
 Changed LSAs. Recorded is LS ID and LS type:
 198.51.100.2(R) 198.51.100.10(R)
```

show ospf events neighbor

This is a useful command to check OSPF neighbor state, specifically in the case when OSPF is flapping. It provides a list of events and state transitions for each neighbor along with the timestamp of those events. In this example, neighbor **10.10.40.1** transitioned through the states from **DOWN** to **FULL**.

```
asa(config)# show ospf events neighbor


          OSPF Router with ID (198.51.100.10) (Process ID 1)

 279 May 15 13:07:31.737: Neighbor 198.51.100.2, Interface inside state changes from
LOADING to FULL
 280 May 15 13:07:31.737: Neighbor 198.51.100.2, Interface inside state changes from
EXCHANGE to LOADING
 281 May 15 13:07:31.737: Neighbor 198.51.100.2, Interface inside state changes from
EXSTART to EXCHANGE
 290 May 15 13:07:31.737: Neighbor 198.51.100.2, Interface inside state changes from
2WAY to EXSTART
 296 May 15 13:07:31.738: Neighbor 198.51.100.2, Interface inside state changes from
INIT to 2WAY
 297 May 15 13:07:31.728: Neighbor 198.51.100.2, Interface inside state changes from
DOWN to INIT
```

show ospf events lsa

This command is useful to check which all LSAs have been generated and received. These are useful in case of link flapping and LSA flooding.

```
asa(config)# show ospf events lsa


          OSPF Router with ID (198.51.100.10) (Process ID 1)

 253 May 15 13:07:49.167: Rcv Changed Type-1 LSA, LSID 198.51.100.2,
Adv-Rtr 198.51.100.2, Seq# 80000002, Age 1, Area 0
 271 May 15 13:07:32.237: Generate New Type-2 LSA, LSID 198.51.100.1,
Seq# 80000001, Age 0, Area 0
 275 May 15 13:07:32.238: Generate Changed Type-1 LSA, LSID 198.51.100.10,
Seq# 80000002, Age 0, Area 0
 276 May 15 13:07:32.228: Rcv New Type-1 LSA, LSID 198.51.100.2,
Adv-Rtr 198.51.100.2, Seq# 80000001, Age 1, Area 0
```

show ospf events neighbor rib

This command provides information about routes added in the RIB and the type of route installed (Intra/Inter).

```
asa(config)# show ospf events neighbor rib

 255 May 15 13:07:54.168: RIB Update, dest 172.18.124.0, mask 255.255.255.255,
gw 198.51.100.2, via inside, source 198.51.100.2, type Intra
 287 May 15 13:07:31.738: Neighbor 198.51.100.2, Interface inside state changes from
LOADING to FULL
 288 May 15 13:07:31.738: Neighbor 198.51.100.2, Interface inside state changes from
EXCHANGE to LOADING
 289 May 15 13:07:31.738: Neighbor 198.51.100.2, Interface inside state changes from
EXSTART to EXCHANGE
 298 May 15 13:07:31.738: Neighbor 198.51.100.2, Interface inside state changes from
2WAY to EXSTART
 304 May 15 13:07:31.738: Neighbor 198.51.100.2, Interface inside state changes from
INIT to 2WAY
 305 May 15 13:07:31.728: Neighbor 198.51.100.2, Interface inside state changes from
DOWN to INIT
```

show ospf events spf

As the SPF calculation is run, the resulting run-times and LSA chances are logged in the SPF events list.

```
asa(config)# show ospf events spf
 235 May 15 13:07:54.167: End of SPF, SPF time 0ms, next wait-interval 10000ms
 240 May 15 13:07:54.167: Starting External processing in area 0
 241 May 15 13:07:54.167: Starting External processing
 244 May 15 13:07:54.167: Starting summary processing, Area 0
 250 May 15 13:07:54.167: Starting Intra-Area SPF, Area 0, spf_type Full
 251 May 15 13:07:54.167: Starting SPF, wait-interval 5000ms
 254 May 15 13:07:49.167: Schedule SPF, Area 0, spf-type Full, Change in LSA
Type RLSID 198.51.100.2, Adv-Rtr 198.51.100.2
 255 May 15 13:07:37.227: End of SPF, SPF time 0ms, next wait-interval 10000ms
 260 May 15 13:07:37.228: Starting External processing in area 0
 261 May 15 13:07:37.228: Starting External processing
 264 May 15 13:07:37.228: Starting summary processing, Area 0
 268 May 15 13:07:37.228: Starting Intra-Area SPF, Area 0, spf_type Full
 269 May 15 13:07:37.228: Starting SPF, wait-interval 5000ms
 272 May 15 13:07:32.238: Schedule SPF, Area 0, spf-type Full, Change in LSA
Type NLSID 198.51.100.1, Adv-Rtr 198.51.100.10
 274 May 15 13:07:32.238: Schedule SPF, Area 0, spf-type Full, Change in LSA
Type RLSID 198.51.100.10, Adv-Rtr 198.51.100.10
 277 May 15 13:07:32.228: Schedule SPF, Area 0, spf-type Full, Change in LSA
Type RLSID 198.51.100.2, Adv-Rtr 198.51.100.2
```

show ospf events generic

This output contains generic process-wide events such as Designated Router (DR) election and adjacency changes.

```
asa(config)# show ospf events generic
 236 May 15 13:07:54.167: Generic:   ospf_external_route_sync0x0
 237 May 15 13:07:54.167: Generic:   ospf_external_route_sync0x0
 238 May 15 13:07:54.167: Generic:   ospf_external_route_sync0x0
 239 May 15 13:07:54.168: Generic:   ospf_external_route_sync0x0
 242 May 15 13:07:54.168: Generic:   ospf_inter_route_sync0x0
 243 May 15 13:07:54.168: Generic:   ospf_inter_route_sync0x0
```

```
245 May 15 13:07:54.168: Generic:  post_spf_intra0x0
246 May 15 13:07:54.168: Generic:  ospf_intra_route_sync0x0
248 May 15 13:07:54.168: Generic:  ospf_intra_route_sync0x0
249 May 15 13:07:54.168: DB add:  172.18.124.00x987668 204
252 May 15 13:07:51.668: Timer Exp:  if_ack_delayed0xcb97dfe0
256 May 15 13:07:37.228: Generic:  ospf_external_route_sync0x0
257 May 15 13:07:37.228: Generic:  ospf_external_route_sync0x0
258 May 15 13:07:37.228: Generic:  ospf_external_route_sync0x0
259 May 15 13:07:37.228: Generic:  ospf_external_route_sync0x0
262 May 15 13:07:37.228: Generic:  ospf_inter_route_sync0x0
263 May 15 13:07:37.228: Generic:  ospf_inter_route_sync0x0
265 May 15 13:07:37.228: Generic:  post_spf_intra0x0
266 May 15 13:07:37.228: Generic:  ospf_intra_route_sync0x0
267 May 15 13:07:37.228: Generic:  ospf_intra_route_sync0x0
270 May 15 13:07:34.728: Timer Exp:  if_ack_delayed0xcb97dfe0
273 May 15 13:07:32.238: DB add:  198.51.100.100x987848 206
278 May 15 13:07:32.228: DB add:  198.51.100.20x987938 205
283 May 15 13:07:31.738: Elect DR:  inside198.51.100.10
284 May 15 13:07:31.738: Elect BDR:  inside198.51.100.2
285 May 15 13:07:31.736: i/f state nbr chg:  inside0x5
287 May 15 13:07:31.736: Elect DR:  inside198.51.100.10
288 May 15 13:07:31.736: Elect BDR:  inside198.51.100.2
289 May 15 13:07:31.736: i/f state nbr chg:  inside0x5
291 May 15 13:07:31.736: nbr state adjok:  198.51.100.20x3
293 May 15 13:07:31.736: Elect DR:  inside198.51.100.10
294 May 15 13:07:31.736: Elect BDR:  inside198.51.100.2
295 May 15 13:07:31.736: i/f state nbr chg:  inside0x5
```

show ospf rib detail

This command, mentioned previously, allows an administrator to see what routes have been learned from peers and whether or not those routes have been installed in the RIB. Routes might not be installed in the RIB due to route filtering (listed previously).

```
asa(config)# show ospf rib detail

          OSPF Router with ID (198.51.100.1) (Process ID 1)
OSPF local RIB
Codes: * - Best, > - Installed in global RIB

*>  172.18.124.0/32, Intra, cost 11, area 0
    SPF Instance 13, age 0:13:59
    Flags: RIB, HiPrio
     via 198.51.100.2, inside, flags: RIB
      LSA: 1/198.51.100.2/198.51.100.2
*   10.20.20.0/32, Intra, cost 11, area 0
    SPF Instance 13, age 0:13:59
    Flags: HiPrio
     via 198.51.100.2, inside, flags: none
      LSA: 1/198.51.100.2/198.51.100.2
*>  192.168.10.0/32, Intra, cost 11, area 0
    SPF Instance 13, age 0:13:59
    Flags: RIB, HiPrio
     via 198.51.100.2, inside, flags: RIB
      LSA: 1/198.51.100.2/198.51.100.2
*   198.51.100.0/24, Intra, cost 10, area 0
    SPF Instance 13, age 0:52:52
    Flags: Connected
     via 198.51.100.10, inside, flags: Connected
      LSA: 2/198.51.100.2/192.151.100.10
```

show ospf neighbor detail

The **show ospf neighbor detail** command allows you to detail the status of the OSPF adjacency.

```
 asa(config)# show ospf neighbor detail

Neighbor 198.51.100.2, interface address 198.51.100.2
In the area 0 via interface ISP
Neighbor priority is 1, State is FULL, 6 state changes
DR is 198.51.100.10 BDR is 198.51.100.2
Options is 0x12 in Hello (E-bit, L-bit)
Options is 0x52 in DBD (E-bit, L-bit, O-bit)
Dead timer due in 0:00:16
Neighbor is up for 00:02:45
Index 1/1, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
```

OSPF Redistribute BGP

In order to support Border Gateway Protocol (BGP) redistribution in and out of other routing protocols, the **redistribute bgp** command has been introduced to the OSPF router configuration. Enter this command in order to redistribute the routed learned via BGP into the running OSPF process.

```
asa(config)# router ospf 1
asa(config-router)# redistribute bgp ?
router mode commands/options:
100  Autonomous system number
ASA-1(config-router)# redistribute bgp 100
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.