

Nexus 7K/N9Kでのマルチキャストフィルタリングの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[汎用トポロジ](#)

[設定例](#)

[FHR：通常、マルチキャストSRCがここで直接接続される](#)

[LHR：通常、マルチキャストRECがここで直接接続される](#)

[PIM:FHR/LHRとして機能する有効ルータ](#)

[RP：これがランデブーポイントです](#)

[マルチキャストのハードウェアエントリの節約の設定](#)

[PACL](#)

[RACL](#)

[関連情報](#)

概要

このドキュメントでは、Nexus 7000/9000スイッチで特定のマルチキャストトラフィックをブロックまたはフィルタリングする方法を設定するさまざまな方法について説明します。また、マルチキャストリソースの節約にも使用できます。一般的な例の1つは、SSDPを使用してサーバ間の通信を行うMicrosoftのユニバーサルプラグアンドプレイ操作の実装です。

前提条件

要件

PIMスパスモードを使用したAny-Source Multicast(ASM)がNexusプラットフォームでどのように動作するかを理解しておくことをお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- NXOS 7.3(4)D1(1)を実行するF3/M3 LCを搭載したNexus 7000
- Nexus N9K-C93180YC-EX/FX(7.0(3)I7(9)または9.3(5))

注：SW/HWが異なる場合、結果は異なる可能性があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスから作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定から開始します。ネットワークが稼働中である場合は、コマンドの潜在的な影響について理解しておく必要があります。

背景説明

使用される略語のリストを次に示します。

RP：ランデブーポイント

FHR：ファーストホップルータ

LHR：ラストホップルータ

SRC：マルチキャストソース

REC:Multicast Receiver

PACL:port access-list

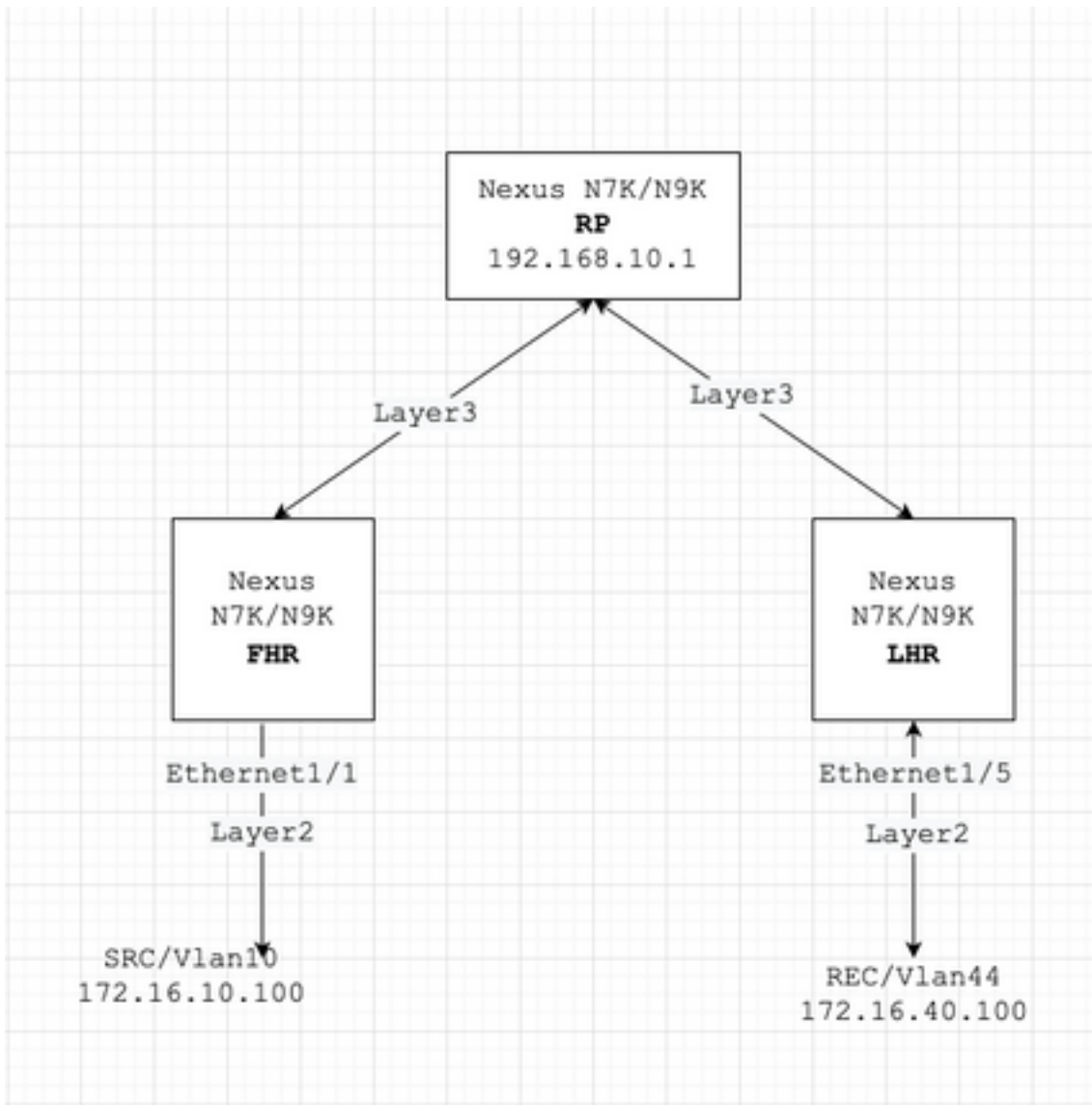
RACL：ルーテッドアクセスリスト

SVI：スイッチ仮想インターフェイス

ACL：アクセスコントロールリスト

設定

汎用トポロジ



設定例

次のように仮定します。

RPのIPアドレスは192.168.10.1です。

SRCのIPアドレスは172.16.10.100/32です。

SSDPグループ : 239.255.255.250/239.255.255.253

次に、デバイスの役割に基づいた設定について説明します。たとえば、FHR、LHR、RPなどです。

FHR : 通常、マルチキャストSRCがここで直接接続される

1.既存のRPに対する登録のフィルタ。

```

ip pim rp-address 192.168.10.1 route-map filter-registration ! Route-map filter-registration deny 5 mat
multicast source 172.16.10.100/32 group 239.255.255.250/32 // Above line is specific to SRC/GROUP pair
map filter-registration deny 7 match ip multicast group 239.255.255.250/32 // Above line is for any SRC
specific group ! Route-map filter-registration permit 100 Match ip multicast group 224.0.0.0/4
  
```

2. SSDPグループに対して存在しない偽のRP(1.1.1.1など)を定義して、RPに対する登録をフィルタリングします。この場合、FHRはRPの役割を担います。

```
ip route 1.1.1.1/32 Null0 ! ip pim rp-address 1.1.1.1 route-map SSDP_groups ! Route-map SSDP_groups permit 10 match ip multicast group 239.255.255.250/32 Route-map SSDP_groups deny 20 match ip multicast group 224.0.0.0/4 ! ip pim rp-address 192.168.10.1 route-map all_other_groups ! Route-map all_other_groups deny 5 match ip multicast group 239.255.255.250/32 Route-map all_other_groups deny 10 match ip multicast group 239.255.255.253/32 Route-map all_other_groups permit 20 match ip multicast group 224.0.0.0/4
```

次を確認します :

```
Nexus9K_OR_N7K# show ip pim rp PIM RP Status Information for VRF "default" BSR disabled Auto-RP disabled RP Candidate policy: None BSR RP policy: None Auto-RP Announce policy: None Auto-RP Discovery policy: None RP: 192.168.10.1, (0), uptime: 00:00:27 priority: 0, RP-source: (local), group-map: Filter-registration group rangs: 224.0.0.0/4 239.255.255.253/32 (deny) 239.255.255.250/32 (deny) Nexus9K_OR_N7K# show ip mrib IP Multicast Routing Table for VRF "default" (172.16.10.100/32, 239.255.255.250/32), uptime: 00:04:12, Incoming interface: Vlan10, RPF nbr: 172.16.10.100 Outgoing interface list: (count: 0) Nexus9K_OR_N7K# system internal mfw event-history pkt pkt events for MCASTFWD process 2021 Jan 1 11:11:41.792316 mcast [21914]: [21933]: Create state for (172.16.10.100, 239.255.255.250) Nexus9K_OR_N7K # show ip pim internal event-history null-register 2021 Jan 01 11:15:19.095711: E_DEBUG pim [21935]: Null Register not sent for (172.16.10.100/32, 239.255.255.250/32) yes
```

上記の出力は、FHRがストリームをRPに登録していないことを示しています。

LHR : 通常、マルチキャストRECがここで直接接続される

3.入力SVI (RECが存在する場所) でのIGMPポリシーの適用 ここでの考え方は、RECからSSDPグループのIGMPメンバーシップレポートをフィルタリングすることです。

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4 ! route-map filter-SSDP-joins deny 5 match ip multicast group 239.255.255.250/32 route-map filter-SSDP-joins deny 6 match ip multicast group 239.255.255.253/32 route-map filter-SSDP-joins permit 100 match ip multicast group 224.0.0.0/4 ! Interface VlanXX ip igmp report-policy filter-SSDP-joins
```

次を確認します :

```
Nexus9K_OR_N7K (config)# show ip mroute 239.255.255.250 IP Multicast Routing Table for VRF "default" Group not found ! Nexus9K_OR_N7K (config)# show ip igmp snooping groups vlan 44 Type: S - Static, D - Dynamic Router port, F - Fabricpath core port Vlan Group Address Ver Type Port list 44 */* - R Vlan44 44 239.255.255.250 v2 D Eth1/5 ! Nexus9K_OR_N7K (config)# show ip igmp internal event-history debugs debug events for IGMP process 2021 Jan 1 11:52:21.277915 igmp [1125]: : Filtered group 239.255.255.250 2021 Jan 1 11:52:21.277903 igmp [1125]: : Received v2 Report for 239.255.255.250 from 172.16.44.100 (Vlan44)
```

上記の出力は、IGMPメンバーシップレポートがフィルタリングされており、(*,G)参加がRPに送信されていないことを示しています。

PIM:FHR/LHRとして機能する有効ルータ

要件に応じて、オプション1または2と3を組み合わせて使用できます。

以下に、いくつかの例を示します。

4.既存のRP (FHRルール) への登録のフィルタ :

```
ip pim rp-address 192.168.10.1 route-map filter-registration ! Route-map filter-registration deny 5 match ip
multicast source 172.16.10.100/32 group 239.255.255.250/32 Route-map filter-registration deny 7 match ip
multicast group 239.255.255.250/32 ! Route-map filter-registration permit 100 Match ip multicast group
224.0.0.0/4
```

5. REC (LHRルール) からIGMPメンバーシップレポートをフィルタリングするIGMPポリシー。

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4 ! route-map filter-SSDP-joins deny 5 match ip mul
group 239.255.255.250/32 route-map filter-SSDP-joins deny 6 match ip multicast group 239.255.255.253/32
route-map filter-SSDP-joins permit 100 match ip multicast group 224.0.0.0/4 ! Interface VlanXX ip igmp
report-policy filter-igmp-joins
```

次を確認します :

上記の点Cと点Dで行った検証とほぼ同じです。

```
Show ip mroute Show ip pim rp Show ip pim internal event-history join-prune Show ip igmp internal event
history debugs
```

RP : これがランデブーポイントです

6. FHRからのSSDPグループの登録をブロックする登録ポリシー。

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4 ip pim register-policy all_groups ! Route-map
all_groups deny 5 match ip multicast group 239.255.255.250/32 Route-map all_groups deny 10 match ip mul
group 239.255.255.253/32 Route-map all_groups permit 20 match ip multicast group 224.0.0.0/4
```

次を確認します :

```
Nexus9K_OR_N7K (config)# show ip mroute 239.255.255.250 IP Multicast Routing Table for VRF "default" Gr
not found ! Nexus9K_OR_N7K (config)# show ip pim internal event-history data-register-receive 2021 Jan
03:33:06.353951: E_DEBUG pim [1359]: Register disallowed by policy 2021 Jan 08 03:33:06.353935: E_DEBUG
[1359]: Received DATA Register from 172.16.10.1 for (172.16.10.100/32, 239.255.255.250/32) (pktlen 1028
Jan 08 03:29:42.602744: E_DEBUG pim [1359]: Add new route (172.16.10.100/32, 239.1.1.1/32) to MRIB, mul
route TRUE F241.01.13-C93180YC-EX-1(config)# show ip pim internal event-history null-register 2021 Jan
03:35:40.966617: E_DEBUG pim [1359]: Send Register-Stop to 172.16.10.1 for (172.16.10.100/32,
239.255.255.250/32) 2021 Jan 08 03:35:40.966613: E_DEBUG pim [1359]: Register disallowed by policy 2021
08 03:35:40.966597: E_DEBUG pim [1359]: Received NULL Register from 172.16.10.1 for (172.16.10.100/32,
239.255.255.250/32) (pktlen 20)
```

上記の出力は、RPがグループ239.255.255.250の登録をブロックしていることを示しています。

7. RPにJoin-pruneポリシーを適用する – pim (*,G) joinと(S,G)の両方がSSDPグループに対してのみ参加します。

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4 ip pim register-policy all_groups ! Route-map
all_groups deny 5 match ip multicast group 239.255.255.250/32 Route-map all_groups deny 10 match ip mul
group 239.255.255.253/32 Route-map all_groups permit 20 match ip multicast group 224.0.0.0/4 ! Interfac
Ethernet/Y ip pim sparse-mode ip pim jp-policy all_groups
```

次を確認します：

```
Nexus9K_OR_N7K # show ip mroute 239.255.255.253 IP Multicast Routing Table for VRF "default" Group not
! F241.01.13-C93180YC-EX-1# show ip pim internal event-history join-prune 2021 Jan 08 03:53:41.643419:
E_DEBUG pim [1359]: Join disallowed by inbound JP policy
```

上記の出力は、(*,G)PIM参加がRPによってブロックされていることを示しています。

マルチキャストのハードウェアエントリの節約の設定

セクションA、B、またはCで説明したすべてのオプションは、FHR、LHR、またはFHR/LHRがストリームをRPに登録したり、PIM参加(*,G)をRPに送信したりすることを防止します。mrouteまたはスヌーピングエントリは引き続き作成され、マルチキャストHWエントリを消費します。

注：VPCが設定されている場合は、入力SVIまたはレイヤ2インターフェイス/ポートチャネル/VPCポートチャネルでRAACLまたはPAACLを使用できません。SRC/RECが異なるVLANまたはL2インターフェイスに分散されている場合は、RAACLまたはPAACLをこれらすべてに適用する必要があることを意味します。ただし、HW/SW (主にハードウェアの制限による)の結果は異なる場合があります。

PAACL

入力レイヤ2ポートまたはポートチャネルまたはVPCポートチャネルでPAACLを設定し、SSDPトラフィックをブロックするか、FHRで(S、G)エントリを作成します。

注：使用するHW (例：Nexus N9000)によっては、PAACLを適用するためにTCAMを事前に分割する必要があります (リロードが必要です)。

以下に、いくつかの例を示します。

```
ip access-list BlockAllSSDP Statistics per-entry 10 deny ip any 239.255.255.250/32 20 deny ip any
239.255.255.253/32 30 permit ip any any ! Interface Ethernet X/Y Or Interface port-channel XX ip port-a
group BlockAllSSDP in
```

次を確認します：

```
F241.01.13-C93180YC-EX-1# sh ip mroute 239.255.255.250 IP Multicast Routing Table for VRF "default" Gro
found ! show ip access-lists BlockAllSSDP IP access list BlockAllSSDP statistics per-entry 10 deny ip a
239.255.255.250/32 [match=3] -> Drop counters 20 deny ip any 239.255.255.253/32 [match=0] 30 permit ip
any [match=0]
```

マルチキャストトラフィックとIGMPメンバーシップポートは両方ともPAACL経由でブロックされるため、スヌーピングとmrouteエントリは表示されません。基本的に、PAACLは両方をドロップしています。

RAACL

SRCが存在する入力SVIでRAACLを設定できますが、使用されているSW/HWに応じて設定できま

す。(S、G)エントリが引き続き作成されるか、トラフィックが他のローカルVLANに転送される可能性があります。

```
ip access-list BlockAllSSDP Statistics per-entry 10 deny ip any 239.255.255.250/32 20 deny ip any 239.255.255.253/32 30 permit ip any any ! Interface VlanXX ip port-access group BlockAllSSDP in
```

次を確認します：

PACLとほぼ同じですが、RAACLオプションではPACLと同じ結果が得られない場合があります。ハードウェアの制限についても前述しています。

関連情報

- これは、拡張要求のバグ[CSCvm44596](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)