



LPTS の実装

- [LPTS の概要](#) (1 ページ)
- [LPTS ポリサー](#) (1 ページ)
- [マルチキャストおよびブロードキャストのパントされたパケットにおけるポートごとのレート制限](#) (6 ページ)
- [ドメインベースの LPTS ポリサー](#) (14 ページ)
- [ダイナミック LPTS フロー タイプの定義](#) (15 ページ)

LPTS の概要

Local Packet Transport Services (LPTS) では、セキュア ドメイン ルータ (SDR) 宛てのすべてのパケットフローを記述するテーブルを保持し、これにより、意図した宛先に確実にパケットが配信されます。

LPTS では、ポート アービトラータおよびフロー マネージャという 2 つのコンポーネントを使用して、このタスクを実行します。ポート アービトラータおよびフロー マネージャは、Internal Forwarding Information Base (IFIB) と呼ばれる、論理ルータ用のパケット フローを記述するテーブルを保持するプロセスです。IFIBは、受信したパケットを適切なルートプロセッサにルーティングして処理するために使用します。

LPTS は、ルータ外からパケットを受信するすべてのアプリケーションと内部的にインターフェイスします。LPTS は、カスタマー設定の必要なく機能します。ただし、ポリサー値は、必要に応じてカスタマイズできます。カスタマーが LPTS フロー マネージャとポート アービトラータのアクティビティやパフォーマンスをモニタリングできるように、LPTS の show コマンドが用意されています。

LPTS ポリサー

Cisco IOS XR では、ルート プロセッサ (RP) 宛ての制御パケットは、着信ポートで一連の入力ポリサーを使用してポリシングされます。これらのポリサーは、ブートアップ時に LPTS コンポーネントによって静的にプログラミングされます。これらのポリサーは、着信制御トラフィックのフロー タイプに基づいて適用されます。フロー タイプは、パケット ヘッダーを調

べることで決定されます。これらの静的入力ポリサーのポリサー レートは、コンフィギュレーションファイルで定義され、ブートアップ時にルートプロセッサにプログラミングされます。これらの一連の入力ポリサーのフロータイプに基づいて、ポリサー値を変更できます。各ノードのポリサーごとにレートを設定できます。



- (注)
- デフォルトのポリサー値とフロータイプの現在のレートは、次の `show` コマンドの出力で確認できます。

```
show lpts pifib hardware police
```

- データポートを介したファイル転送を高速化するために、SSH フローの LPTS ポリサー レートを設定できます。

show lpts pifib hardware entry brief location node-id |inc SSH コマンドを使用して、LPTS のドロップを確認します。LPTS ドロップがある場合は、最大 50000 pps までレートを増やします。

pps が高いと CPU サイクルの使用率が増加するため、必要な場合にのみ値を最大にします。

次に例を示します。

```
Router#configure
Router(config)#lpts pifib hardware police location 0/0/CPU0
Router(config-pifib-policer-per-node)# flow ssh known rate 50000
Router(config-pifib-policer-per-node)#commit
```

設定例

次の値をすべてのノードにグローバルに使用して、OSPF および BGP フロータイプに LPTS ポリサーを設定します。

- ospf unicast default rate 3000
- bgp default rate 4000

```
Router#configure
Router(config)#lpts pifib hardware police
Router(config-pifib-policer-global)#flow ospf unicast default rate 3000
Router(config-pifib-policer-global)#flow bgp default rate 4000
Router (config-pifib-policer-global)#commit
```

実行コンフィギュレーション

```
lpts pifib hardware police
flow ospf unicast default rate 3000
flow bgp default rate 4000
!
```

確認

```
Router#show run lpts pifib hardware police
lpts pifib hardware police
```

```
flow ospf unicast default rate 3000
flow bgp default rate 4000
```

設定例

次の値を個々のノード 0/RP0/CPU0 に使用して、OSPF および BGP フロー タイプに LPTS ポリサーを設定します。

- ospf unicast default rate 3000
- flow bgp default rate 4000

```
Router#configure
Router(config)#lpts pifib hardware police location 0/RP0/CPU0
Router(config-pifib-policer-per-node)#flow ospf unicast default rate 3000
Router(config-pifib-policer-per-node)#flow bgp default rate 4000
Router(config-pifib-policer-per-node)#commit
```

実行コンフィギュレーション

```
lpts pifib hardware police location 0/RP0/CPU0
flow ospf unicast default rate 3000
flow bgp default rate 4000
```

確認

show lpts pifib hardware police location 0/RP0/CPU0 コマンドは、指定したノードの Pre-Internal Forwarding Information Base (IFIB) 情報を表示します。

```
Router#show lpts pifib hardware police location 0/RP0/CPU0
```

```
-----
Node 0/RP0/CPU0:
-----
Burst = 100ms for all flow types
-----
```

FlowType	Policer	Type	Cur. Rate	Burst	npu
OSPF-uc-default	32106	np	3000	1000	0
BGP-default	32118	np	4000	1250	0

確認

show controllers npu stats traps-all instance all location 0/RP0/CPU0 コマンドは、ローカルで処理されたパケットと、CPU によってドロップされたパケットを表示します。

```
Router# show controllers npu stats traps-all instance all location 0/RP0/CPU0
```

Trap Type	NPU	Trap	TrapStats	Policer	Packet
Packet	ID	ID	ID		Accepted
Dropped					
RxTrapMimSaMove (CFM_DOWM_MEP_DMM)	0	6	0x6	32037	0
RxTrapMimSaUnknown (RCY_CFM_DOWN_MEP_DMM)	0	7	0x7	32037	0
RxTrapAuthSaLookupFail (IPMC default)	0	8	0x8	32033	0
RxTrapSaMulticast	0	11	0xb	32018	0

RxTrapArpMyIp	0	13	0xd	32001	0	0
RxTrapArp	0	14	0xe	32001	11	0
RxTrapDhcpv4Server	0	18	0x12	32022	0	0
RxTrapDhcpv4Client	0	19	0x13	32022	0	0
RxTrapDhcpv6Server	0	20	0x14	32022	0	0
RxTrapDhcpv6Client	0	21	0x15	32022	0	0
RxTrapL2Cache_LACP	0	23	0x17	32003	0	0
RxTrapL2Cache_LLDP1	0	24	0x18	32004	0	0
RxTrapL2Cache_LLDP2	0	25	0x19	32004	1205548	0
RxTrapL2Cache_LLDP3	0	26	0x1a	32004	0	0
RxTrapL2Cache_ELMI	0	27	0x1b	32005	0	0
RxTrapL2Cache_BPDU	0	28	0x1c	32027	0	0
RxTrapL2Cache_BUNDLE_BPDU	0	29	0x1d	32027	0	0
RxTrapL2Cache_CDP	0	30	0x1e	32002	0	0
RxTrapHeaderSizeErr	0	32	0x20	32018	0	0
RxTrapIpCompMcInvalidIp	0	35	0x23	32018	0	0
RxTrapMyMacAndIpDisabled	0	36	0x24	32018	0	0
RxTrapMyMacAndMplsDisable	0	37	0x25	32018	0	0
RxTrapArpReply	0	38	0x26	32001	2693	0
RxTrapFibDrop	0	41	0x29	32018	0	0
RxTrapMTU	0	42	0x2a	32020	0	0
RxTrapMiscDrop	0	43	0x2b	32018	0	0
RxTrapL2AclDeny	0	44	0x2c	32034	0	0
Rx_UNKNOWN_PACKET	0	46	0x2e	32018	0	0
RxTrapL3AclDeny	0	47	0x2f	32034	0	0
RxTrapOamY1731MplsTp (OAM_SWOFF_DN_CCM)	0	57	0x39	32029	0	0
RxTrapOamY1731Pwe (OAM_SWOFF_DN_CCM)	0	58	0x3a	32030	0	0
RxTrapOamLevel	0	64	0x40	32023	0	0
RxTrapRedirectToCpuOamPacket	0	65	0x41	32025	0	0
RxTrapOamPassive	0	66	0x42	32024	0	0
RxTrap1588	0	67	0x43	32038	0	0
RxTrapExternalLookupError	0	72	0x48	32018	0	0

RxTrapArplookupFail	0	73	0x49	32001	0	0
RxTrapUcLooseRpfFail	0	84	0x54	32035	0	0
RxTrapMplsControlWordTrap	0	88	0x58	32015	0	0
RxTrapMplsControlWordDrop	0	89	0x59	32015	0	0
RxTrapMplsUnknownLabel	0	90	0x5a	32018	0	0
RxTrapIpv4VersionError	0	98	0x62	32018	0	0
RxTrapIpv4ChecksumError	0	99	0x63	32018	0	0
RxTrapIpv4HeaderLengthError	0	100	0x64	32018	0	0
RxTrapIpv4TotalLengthError	0	101	0x65	32018	0	0
RxTrapIpv4Ttl0	0	102	0x66	32008	0	0
RxTrapIpv4Ttl1	0	104	0x68	32008	0	0
RxTrapIpv4DipZero	0	106	0x6a	32018	0	0
RxTrapIpv4SipIsMc	0	107	0x6b	32018	0	0
RxTrapIpv6VersionError	0	109	0x6d	32018	0	0
RxTrapIpv6HopCount0	0	110	0x6e	32011	0	0
RxTrapIpv6LoopbackAddress	0	113	0x71	32018	0	0
RxTrapIpv6MulticastSource	0	114	0x72	32018	0	0
RxTrapIpv6NextHeaderNull	0	115	0x73	32010	0	0
RxTrapIpv6Ipv4CompatibleDestination	0	121	0x79	32018	0	0
RxTrapMplsTtl1	0	125	0x7d	32012	316278	
2249 RxTrapUcStrictRpfFail	0	137	0x89	32035	0	0
RxTrapMcExplicitRpfFail	0	138	0x8a	32033	0	0
RxTrapOamp (OAM_BDL_DN_NON_CCM)	0	141	0x8d	32031	0	0
RxTrapOamEthUpAccelerated (OAM_BDL_UP_NON_CCM)	0	145	0x91	32032	0	0
RxTrapReceive	0	150	0x96	32017	125266112	0
RxTrapUserDefine_FIB_IPV4_NULL0	0	151	0x97	32018	0	0
RxTrapUserDefine_FIB_IPV6_NULL0	0	152	0x98	32018	0	0
RxTrapUserDefine_FIB_IPV4_GLEAN	0	153	0x99	32016	0	0
RxTrapUserDefine_FIB_IPV6_GLEAN	0	154	0x9a	32016	0	0
RxTrapUserDefine_IPV4_OPTIONS	0	155	0x9b	32006	0	0
RxTrapUserDefine_IPV4_RSVP_OPTIONS	0	156	0x9c	32007	0	0
RxTrapUserDefine	0	157	0x9d	32026	0	0

RxTrapUserDefine_BFD	0	163	0xa3	32028	0	0
RxTrapMC	0	181	0xb5	32033	0	0
RxNetflowSnoopTrap0	0	182	0xb6	32018	0	0
RxNetflowSnoopTrap1	0	183	0xb7	32018	0	0
RxTrapMimSaMove (CFM_DOWM_MEP_DMM)	1	6	0x6	32037	0	0
RxTrapMimSaUnknown (RCY_CFM_DOWN_MEP_DMM)	1	7	0x7	32037	0	0
RxTrapAuthSaLookupFail (IPMC default)	1	8	0x8	32033	0	0
RxTrapSaMulticast	1	11	0xb	32018	0	0
RxTrapArpMyIp	1	13	0xd	32001	0	0

関連コマンド

- lpts pifib hardware police
- flow ospf
- flow bgp
- show lpts pifib hardware police

マルチキャストおよびブロードキャストのパントされたパケットにおけるポートごとのレート制限

この機能により、インターフェイスレベルでのマルチキャストおよびブロードキャストのパントされたトラフィックのレート制限がイネーブルになります。現在は NPU レベルごとのレート制限がサポートされています。この機能は、パントされたトラフィックのマルチキャストおよびブロードキャストストームの受信からポートを保護するため、インターフェイスレベルでのレート制限をサポートします。すべての L3 プロトコルパントパケットおよび L2 プロトコルパケット（ERPS および DOT1x のみ）のレート制限は、物理およびバンドルのメインインターフェイスでサポートされています。

マルチキャストおよびブロードキャストのパントされたトラフィックに対するレート制限の設定

マルチキャストおよびブロードキャストのレート制限は、次の 3 つのレベルで設定できます。

- インターフェイス レベル
- グローバル レベル
- ドメインレベル

マルチキャストおよびブロードキャストのパントされたトラフィックをレート制限するとともに、次のプロトコルのパントされたトラフィックに対してレート制限を設定できます。

- ARP
- CDP
- LACP

プロトコル固有の設定については、以下のセクションで説明します。

制限事項

ブロードキャストとマルチキャストのレート制限が **ARP** のレート制限とともに設定されている場合、ARP パケットによってブロードキャストカウンタとマルチキャストカウンタが増加します。

インターフェイス レベル

TenGig インターフェイスでマルチキャストおよびブロードキャストのパントされたトラフィックのレート制限を 1000 pps に設定する例を示します。



(注) インターフェイスレベルのレート制限の設定は、グローバルレベルおよびドメインレベルの設定よりも優先されます。

1. Router# configure
 コンフィギュレーション モードを開始します。
2. Router(config)# lpts punt police
 パント コンフィギュレーション モードを開始します。
3. Router(config-lpts-punt-policer)# interface TenGigE0/0/0/8/0
 インターフェイスレベルのポリサー設定ごとに開始します。
4. Router(config-lpts-punt-policer-global-if)# mcast rate 1000
 マルチキャストのパントされたトラフィックのレート制限を 1000 pps に設定します。
5. Router(config-lpts-punt-policer-global-if)# bcast rate 1000
 ブロードキャストのパントされたトラフィックのレート制限を 1000 pps に設定します。
6. Router(config-lpts-punt-policer-global-if)# commit
 設定をコミットします。

グローバルレベル

レート制限を設定する例を示します。

- マルチキャストおよびブロードキャストのパントされたトラフィックに 1000 pps

1. Router# configure
コンフィギュレーション モードを開始します。
2. Router(config)# lpts punt police
パント コンフィギュレーション モードを開始します。
3. Router(config-punt-policer-global)# mcast rate 1000
マルチキャストレート制限を 1000 pps に設定します。
4. Router(config-punt-policer-global)# bcast rate 1000
ブロードキャストレート制限を 1000 pps に設定します。
5. Router(config-punt-policer-global)# commit
設定をコミットします。

ドメインレベル

LPTS ドメインを設定し、レート制限を適用する例を示します。

- マルチキャストおよびブロードキャストのパントされたトラフィックに 1000 pps

1. Router# configure
コンフィギュレーション モードを開始します。
2. Router(config)# lpts punt police domain ACCESS
LPTS パント ドメイン コンフィギュレーション モードを開始します。
3. Router(config-lpts-punt-policer-global-ACCESS)# mcast 5000
マルチキャストレート制限を 5000 pps に設定します。
4. Router(config-lpts-punt-policer-global-ACCESS)# bcast 5000
ブロードキャストレート制限を 5000 pps に設定します。
5. Router(config-lpts-punt-policer-global-ACCESS)# exit
ドメインアクセスモードを終了します。
6. Router(config-lpts-punt-policer)# exit
LPTS パント コンフィギュレーション モードを終了します。
7. Router(config)# lpts pifib hardware domain ACCESS
LPTS ハードウェア ドメイン コンフィギュレーション モードを開始します。
8. Router(config-pifib-domain-ACCESS)# interface TenGigE0/0/0/8/1
TenGigE0/0/0/8/1 インターフェイスノードに、ドメインアクセスを適用します。
9. Router(config-pifib-domain-ACCESS)# exit
LPTS ドメインモードを終了します。

10. Router(config)# lpts punt police location 0/0/CPU0
LPTS パント ポリサー コンフィギュレーション モードを開始します。
11. Router(config-lpts-punt-policer)# protocol arp rate 500
ARP プロトコルパケットに 500 pps のレート制限を設定します。
12. Router(config-lpts-punt-policer)# protocol cdp rate 500
CDP プロトコルパケットに 500 pps のレート制限を設定します。
13. Router(config-lpts-punt-policer)# exit
LPTS パント ポリサー コンフィギュレーション モードを終了します。
14. Router(config)# lpts punt police location 0/4/CPU0
ノードロケーション 0/4/CPU0 で LPTS パントポリサーを設定します。
15. Router(config)# commit
設定をコミット



(注) 設定をコミットした後、マルチキャストおよびブロードキャストのレート制限に関して、syslog でエラーメッセージがキャプチャされているかどうかを確認します。

プロトコルのパントされたトラフィック

プロトコルのパントされたトラフィック（ARP、CDP、LACP）に対してレート制限を設定できます。

グローバルレベルでのプロトコルのパントされたトラフィックに対し、次のレート制限を設定する例を示します。

- ARP および CDP プロトコルに 500 pps

1. Router(config-punt-policer-global)# protocol arp rate 500
ARP プロトコルパケットに 500 pps のレート制限を設定します。
2. Router(config-punt-policer-global)# protocol cdp rate 500
CDP プロトコルパケットに 500 pps のレート制限を設定します。
3. Router(config-punt-policer-global)# commit
設定をコミットします。

ドメインレベルでのプロトコルのパントされたトラフィックに対し、次のレート制限を設定する例を示します。

- ARP および CDP プロトコルに 500 pps

1. Router(config)# lpts pifib hardware domain ACCESS

LPTS ハードウェア ドメイン コンフィギュレーション モードを開始します。

2. Router(config-pifib-domain-ACCESS)# interface TenGigE0/0/0/8/1
TenGigE0/0/0/8/1 インターフェイスノードに、ドメインアクセスを適用します。
3. Router(config-pifib-domain-ACCESS)# exit
LPTS ドメインモードを終了します。
4. Router(config)# lpts punt police location 0/0/CPU0
LPTS パント ポリサー コンフィギュレーション モードを開始します。
5. Router(config-lpts-punt-policer)# protocol arp rate 500
ARP プロトコルパケットに 500 pps のレート制限を設定します。
6. Router(config-lpts-punt-policer)# protocol cdp rate 500
CDP プロトコルパケットに 500 pps のレート制限を設定します。
7. Router(config-lpts-punt-policer)# exit
LPTS パント ポリサー コンフィギュレーション モードを終了します。
8. Router(config)# lpts punt police location 0/4/CPU0
ノードロケーション 0/4/CPU0 で LPTS パントポリシングを設定します。
9. Router(config)# commit
設定をコミット

ランニング コンフィギュレーション

```
lpts punt police
interface TenGigE0/0/0/8/0
  mcast rate 1000
  bcast rate 1000
!
mcast rate 1000
bcast rate 1000
protocol arp rate 700
protocol cdp rate 700
domain ACCESS
  mcast rate 5000
  bcast rate 5000
!
!
lpts pifib hardware domain ACCESS
interface TenGigE0/0/0/8/1
!
lpts punt police location 0/0/CPU0
protocol arp rate 500
protocol cdp rate 500
!
lpts punt police location 0/4/CPU0
!
```

確認

次の show コマンドの出力では、ドメインでのレート制限の設定を確認するための強調表示されたフィールドと、インターフェイスレベルを確認する必要があります。

```
Router# show lpts punt statistics location 0/0/CPU0
Fri Nov 15 06:23:20.410 UTC

Lpts Punt Policer Statistics:
-----
Punt_Reason - Ingress Packets type to be Punt policed
Scope      - Configured scope - Global/Domain/IFH
State      - Current config state
Rate       - Policer rate in PPS
Accepted   - No of Packets Accepted
Dropped    - No of Packets Dropped
Domain     - Domain name
-----

Interface Name      : any
Punt Reason       : ARP
Domain           : ACCESS
Scope              : Default
State              : Active
Configured Rate   : 1000
Operational Rate   : 986
Accepted           : 0
Dropped            : 0
Last Update (if any):
Punt Type          : ARP
Interface Handle    : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate        : 1000
Domain             : 1
CreateTime         : Fri Nov 15 2019 06:22:42.237.188
Platform:
  PolicerID        : 32398
  NPU: TCAM-entry   StatsID
    0:              172 0x80001d54
    1:              297 0x80001dd0
    2:              172 0x80001d54
    3:              172 0x80001d54
    4:              172 0x80001d54
    5:              172 0x80001d54
-----

Interface Name      : any
Punt Reason       : CDP
Domain           : ACCESS
Scope              : Default
State              : Active
Configured Rate   : 1000
Operational Rate   : 986
Accepted           : 0
Dropped            : 0
Last Update (if any):
Punt Type          : CDP
Interface Handle    : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate        : 1000
Domain             : 1
CreateTime         : Fri Nov 15 2019 06:22:42.258.192
```

マルチキャストおよびブロードキャストのパントされたトラフィックに対するレート制限の設定

```

Platform:
  PolicerID      : 32404
  NPU: TCAM-entry  StatsID
    0:           173 0x80001d55
    1:           298 0x80001dd1
    2:           173 0x80001d55
    3:           173 0x80001d55
    4:           173 0x80001d55
    5:           173 0x80001d55
-----
Interface Name      : any
Punt Reason       : ARP
Domain              : default
Scope               : Local
State               : Active
Configured Rate    : 500
Operational Rate    : 515
Accepted            : 980
Dropped             : 0
Last Update (if any):
Punt Type           : ARP
Interface Handle     : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate         : 500
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:31:25.136.800
Platform:
  PolicerID      : 32306
  NPU: TCAM-entry  StatsID
    0:           41 0x80001cd2
    1:           41 0x80001cd2
    2:           41 0x80001cd2
    3:           41 0x80001cd2
    4:           41 0x80001cd2
    5:           41 0x80001cd2
-----
Interface Name      : any
Punt Reason       : CDP
Domain              : default
Scope               : Local
State               : Active
Configured Rate     : 500
Operational Rate    : 515
Accepted            : 4292
Dropped             : 0
Last Update (if any):
Punt Type         : CDP
Interface Handle     : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate       : 500
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:31:25.513.897
Platform:
  PolicerID      : 32312
  NPU: TCAM-entry  StatsID
    0:           42 0x80001cd3
    1:           42 0x80001cd3
    2:           42 0x80001cd3
    3:           42 0x80001cd3
    4:           42 0x80001cd3
    5:           42 0x80001cd3
-----

```

```
-----  
Interface Name : TenGigE0  
Punt Reason : MCAST  
Domain : default  
Scope : Global  
State : Active  
Configured Rate : 1000  
Operational Rate : 986  
Accepted : 0  
Dropped : 0  
Last Update (if any):  
Punt Type : MCAST  
Interface Handle : 0x0800001c  
Is Virtual : 1  
Is Enabled : 1  
Packet Rate : 1000  
Domain : 0  
CreateTime : Tue Nov 12 2019 06:32:43.210.014  
Platform:  
PolicerID : 32396  
NPU: TCAM-entry StatsID  
0: 170 0x80001d52  
1: 172 0x80001d53  
2: 170 0x80001d52  
3: 170 0x80001d52  
4: 170 0x80001d52  
5: 170 0x80001d52  
-----  
Interface Name : TenGigE0  
Punt Reason : BCAST  
Domain : default  
Scope : Global  
State : Active  
Configured Rate : 1000  
Operational Rate : 986  
Accepted : 0  
Dropped : 0  
Last Update (if any):  
Punt Type : BCAST  
Interface Handle : 0x0800001c  
Is Virtual : 1  
Is Enabled : 1  
Packet Rate : 1000  
Domain : 0  
CreateTime : Tue Nov 12 2019 06:32:43.227.279  
Platform:  
PolicerID : 32397  
NPU: TCAM-entry StatsID  
0: 171 0x80001d53  
1: 173 0x80001d54  
2: 171 0x80001d53  
3: 171 0x80001d53  
4: 171 0x80001d53  
5: 171 0x80001d53  
-----
```

ドメインベースの LPTS ポリサー

単一ドメインの LPTS ポリサーを使用して、ルータの特定のポート、ポートのグループ、またはラインカードを設定できます。特定のドメインに属するポートベースのポリサーを設定すると、さまざまなタイプの入力トラフィックの適切な分類および制御が可能になります。たとえば、iBGP トラフィックはトラフィックフローのレートが高いため、iBGP トラフィックを処理するポートは、eBGP トラフィックを処理するポートに比べて高いポリサーレートで設定できます。

制約事項

- ポートまたはラインカードに対して設定されたポリサーレートは、ドメインの一部としてポートまたはラインカードが設定された後に、ドメインのポリサーレートとして転送されます。たとえば、ポート `hundredGigE 0/0/0/1` およびポート `hundredGigE 0/0/0/2` に `ospf` ユニキャストの既知のフローとしてポリサーレート 3000 が設定され、ポートがドメインコアの一部として設定されている場合、`ospf` ユニキャストの既知のフローにおけるドメインコアのポリサーレートは、特に設定されていない限り 3000 です。
- ルータごとに 1 つのドメインのみを設定できます。
- ドメイン名には任意の単語を使用できますが、最大 32 文字までです。

設定例

LPTS のドメインベースのポリサーを設定するには、次の手順を実行します。

1. LPTS ハードウェア コンフィギュレーション モードを開始し、ドメインを作成します。
2. ドメインのインターフェイスを設定します。
3. ドメインコアの LPTS ハードウェア コンフィギュレーション モードを開始し、グローバルレベルでドメインコアの入力ポリサーレートを設定します。
4. ドメインコアの LPTS ハードウェア コンフィギュレーション モードを開始し、ラインカードレベルでドメインコアの入力ポリサーレートを設定します。

設定

```
/* Enter the LPTS hardware ingress policer configuration mode and create a domain named CORE. */
Router# config
Router(config)# lpts pifib hardware domain CORE

/* Configure the interfaces for the domain CORE. */
Router(config-lpts-domains-CORE)# interface hundredGigE 0/0/0/1
Router(config-lpts-domains-CORE)# interface hundredGigE 0/0/0/2
Router(config-lpts-domains-CORE)# commit
Router(config-lpts-domains-CORE)# exit

/* Enter the LPTS hardware configuration mode for the domain CORE, and then configure the ingress policer rates for the domain CORE at the global level. */
```

```

Router(config)# lpts pifib hardware police domain CORE
Router(config-lpts-policer-global-CORE)# flow ospf unicast known rate 6000
Router(config-lpts-policer-global-CORE)# flow ospf unicast default rate 7000
Router(config-lpts-policer-global-CORE)# commit
Router(config-lpts-policer-global-CORE)# exit
Router(config-lpts-policer-global)# exit

/* Enter the LPTS hardware configuration mode for the domain CORE, and then configure
the ingress policer rates for the domain CORE at the line card level. */
Router(config)# lpts pifib hardware police location 0/0/CPU0 domain CORE
Router(config-lpts-policer-global-CORE)# flow ospf unicast known rate 7000
Router(config-lpts-policer-global-CORE)# flow ospf unicast default rate 8000
Router(config-lpts-policer-global-CORE)# commit

```

実行コンフィギュレーション

```

lpts pifib hardware domain CORE
  interface HundredGigE0/0/0/1
  interface HundredGigE0/0/0/2
!
lpts pifib hardware police
  domain CORE
    flow ospf unicast known rate 6000
    flow ospf unicast default rate 7000
!

lpts pifib hardware police location 0/0/CPU0 domain CORE
  flow ospf unicast known rate 7000
  flow ospf unicast default rate 8000
!

```

確認

設定された LPTS ドメインの情報を確認するには、次のコマンドを使用します。

```

Router# show lpts pifib domains
Thu Nov 21 15:49:31.334 IST

Domains Information: 1 Configured
-----
Domain: [1] CORE
-----
interface [-----] HundredGigE0/0/0/1
interface [-----] HundredGigE0/0/0/2
                0 local of total 2 interfaces

```

ダイナミック LPTS フロー タイプの定義

ダイナミック LPTS フロー タイプ機能を使用すると、LPTS フロー タイプを設定できるとともに、TCAM 内の各フロー タイプの最大 LPTS エントリ数を定義できます。ダイナミック LPTS フロー タイプの設定はラインカードごとに行うため、複数のラインカードにわたって複数のプロファイルを設定できます。

ルータが起動すると、デフォルトの LPTS フロー タイプが TCAM でプログラミングされます。フロー タイプそれぞれに、最大フロー エントリ数が事前に定義されています。後で、実行時にネットワーク要件に基づいてフロー タイプを選択し、最大フロー エントリ値も設定するオ

プシオンがあります。最大フロー エントリ値ゼロは、フロー タイプが設定されていないことを示します。



- (注) 設定可能なフローと設定不能なフローの両方のデフォルト最大フロー値は、次の show コマンドの出力で確認できます。

```
show lpts pifib dynamic-flows statistics location <location specification>
```

設定可能なフロー タイプと設定不能なフロー タイプのリストを次の表に示します。また、設定可能なフロー タイプと設定不能なフロー タイプのリストを表示するには、**show lpts pifib dynamic-flows statistics location** コマンドも使用できます。



- (注) すべてのフロー タイプに設定される最大 LPTS エントリの総数は、ライン カードあたり 8,000 エントリを超えないものとします。

設定例

次の例では、TCAM に BGP-known と ISIS-known の LPTS フロー タイプを設定し、ノード ロケーション 0/1/CPU0 に最大フロー エントリ 1800 と 500 を定義します。新しい最大値がデフォルト値を超えているため、他のフロー タイプを無効にして TCAM 内にスペースを作成し、ラインカードあたりのすべてのフロータイプの最大エントリ総数を 8,000 エントリを超えないようにする必要があります。そのため、次の例では RSVP-known フロー タイプがゼロに設定されています。

```
Router#configure
Router(config)#lpts pifib hardware dynamic-flows location 0/1/CPU0
Router(config-pifib-flows-per-node)#flow bgp-known max 1800
Router(config-pifib-flows-per-node)#flow ISIS-known max 500
Router(config-pifib-flows-per-node)#flow RSVP-known max 0
Router(config-pifib-flows-per-node)#commit
```

実行コンフィギュレーション

```
Router#show run lpts pifib hardware dynamic-flows location 0/1/CPU0
flow bgp known max 1800
flow isis-known 500
flow RSVP-known 0
```

確認

次の show コマンドは、ダイナミック フローの統計情報を表示します。フロー タイプの BGP-known と ISIS-known が新たに設定した最大フロー エントリ値で TCAM に設定されていることを確認できます。また、RSVP-known フロータイプが無効になっていることも確認できます。

```
Router#show lpts pifib dynamic-flows statistics location 0/1/CPU0

Dynamic-flows Statistics:
-----
```


(C - Configurable, T - TRUE, F - FALSE, * - Configured)
 Def_Max - Default Max Limit
 Conf_Max - Configured Max Limit
 HWCnt - Hardware Entries Count
 ActLimit - Actual Max Limit
 SWCnt - Software Entries Count
 P, (+) - Pending Software Entries

FLOW-TYPE	C	Def_Max	Conf_Max	HWCnt/ActLimit	SWCnt P
Fragment	F	2	--	2/2	2
OSPF-mc-known	T	600	--	2/600	2
OSPF-mc-default	F	4	--	4/4	4
OSPF-uc-known	T	300	--	1/300	1
OSPF-uc-default	F	2	--	2/2	2
ISIS-known	T	300	500	500/300	0
ISIS-default	F	1	--	1/1	1
BGP-known	T	900	1800	1800/900	0
BGP-cfg-peer	T	900	--	0/900	0
BGP-default	F	4	--	4/4	4
PIM-mcast-default	F	40	--	0/40	0
PIM-mcast-known	T	300	--	0/300	0
PIM-ucast	F	40	--	2/40	2
IGMP	T	1200	--	0/1200	0
ICMP-local	F	4	--	4/4	4
ICMP-control	F	5	--	5/5	5
ICMP-default	F	9	--	9/9	9
ICMP-app-default	F	2	--	2/2	2
LDP-TCP-known	T	300	--	0/300	0
LDP-TCP-cfg-peer	T	300	--	0/300	0
LDP-TCP-default	F	40	--	0/40	0
LDP-UDP	T	300	--	0/300	0
All-routers	T	300	--	0/300	0
RSVP-default	F	4	--	1/4	1
RSVP-known	T	300	0	0/300	0
SNMP	T	300	--	0/300	0
SSH-known	T	150	--	0/150	0
SSH-default	F	40	--	0/40	0
TELNET-known	T	150	--	0/150	0
TELNET-default	F	4	--	0/4	0
UDP-default	F	2	--	2/2	2
TCP-default	F	2	--	2/2	2
Raw-default	F	2	--	2/2	2
GRE	F	4	--	0/4	0
VRRP	T	150	--	150/150	0
DNS	T	40	--	0/40	0
NTP-default	F	4	--	0/4	0
NTP-known	T	150	--	0/150	0
TPA	T	5	--	0/5	0

Local Limit : **7960**/8000 /*The sum of maximum flow entries configured for all flow types

per line card is less than 8000*/

HWCnt/SWCnt : 45/51

上記の show コマンド出力では、最後の列の **P** でそのフロー タイプの保留中ソフトウェア フロー エントリを指定します。

