



MPF for Broadband LAC, LNS, and PTA

The Multi-Processor Forwarding (MPF) for Broadband L2TP Access Concentrator (LAC), L2TP Network Server (LNS), and PPP Termination and Aggregation (PTA) feature significantly improves broadband feature performance by accelerating features with a fast-forwarding method of switching packets on the second CPU.

History for the MPF for Broadband LAC, LNS, and PTA Feature

Release	Modification
12.3(14)YM2	This feature was introduced for the Cisco 7301 router and Cisco 7204VXR and Cisco 7206VXR routers.
12.4(4)T	This feature was integrated into Cisco IOS Release 12.4(4)T. Support for QoS Group commands, L2TP Load Balancing with Random Tunnel Selection, Multicast User Authentication and Profile Support was added.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for MPF for Broadband LAC, LNS, and PTA, page 2](#)
- [Restrictions for MPF for Broadband LAC, LNS, and PTA, page 2](#)
- [Information About MPF for Broadband LAC, LNS, and PTA, page 3](#)
- [Configuring MPF for Broadband LAC, LNS, and PTA, page 20](#)
- [Configuration Examples for MPF for Broadband LAC, LNS, and PTA, page 23](#)
- [Additional References, page 27](#)
- [Command Reference, page 29](#)
- [Glossary, page 55](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Prerequisites for MPF for Broadband LAC, LNS, and PTA

- You must have an upgraded ROM monitor (ROMmon) 2.0 image before you can download the software to enable use of the second CPU.
 - The upgraded ROMmon 2.0 image is available by default for newly purchased Cisco 7301 and Cisco 7200 VXR routers.
 - If you have a ROMmon version earlier than 2.0 and you would like to use the MPF capability, a Cisco-qualified support engineer (SE) can perform the ROMmon 2.0 upgrade on site.
- Minimum required ROMmon version:
 - For the Cisco 7301, ROMmon version 12.3(4r)T2
 - For the Cisco 7200 VXR NPE-G1, ROMmon version 12.3(4r)T3
- Cisco Express Forwarding (CEF) is enabled.
- Minimum system memory for the Cisco 7301 or Cisco 7204 and 7206 VXR NPE-G1:
 - 512 MB for less than 8000 sessions, but 1 GB is highly recommended
 - 1 GB for deployments of more than 8000 sessions
 - See the [“System Memory Requirements” section on page 19](#) for more system memory information by type of deployment and whether deployed with or without features.

Restrictions for MPF for Broadband LAC, LNS, and PTA

- MPF for Broadband LAC, LNS, and PTA is only supported on the Cisco 7301 and Cisco 7204 and Cisco 7206 VXR NPE-G1 routers.
- MPF for Broadband LAC, LNS, and PTA only supports native Gigabit Ethernet (GE) interfaces.
- Port adapter traffic is not accelerated by MPF and is processed by standard Cisco IOS software. Only the following port adapters are supported for the Cisco 7301 and Cisco 7200 VXR NPE-G1 routers in an MPF network:

Enhanced ATM port adapters:

- PA-A3-OC3 (SMI/SML/MM)
- PA-A3-T3
- PA-A3-E3
- PA-A6-OC3 (SMI/SML/MM)
- PA-A6-T3
- PA-A6-E3

Fast Ethernet/Gigabit Ethernet LAN port adapters:

- PA-FE-TX
- PA-2FE-TX
- PA-2FE-FX

See the [“Port Adapter Coexistence with MPF” section on page 5](#) for more information.

- Punted features and ignored features are not MPF accelerated. See the [“Punted Features” section on page 15](#) and the [“Ignored MPF Features” section on page 16](#) for descriptions of these features.

- Context-based Access Control (CBAC) Configuration Restrictions

CBAC is only supported for Virtual Access Interfaces (VAIs) and cannot be configured for any MPF-accelerated interfaces. MPF does not accelerate any CBAC features. Instead MPF punts any CBAC-configured VAI session traffic to Cisco IOS for CBAC feature processing. Due to this design limitation, CBAC security ACL filters can only be applied to VAIs and non-MPF port adapter interfaces. CBAC ACL filters cannot be applied to any MPF-accelerated, native GE interfaces.

In addition, the CBAC “pin-hole” feature that allows specified inspect traffic to flow through the CBAC security ACL filters does not work on MPF-accelerated interfaces.

Information About MPF for Broadband LAC, LNS, and PTA

To understand MPF for Broadband LAC, LNS, and PTA, you should read the following sections:

- [MPF for Broadband LAC, LNS, and PTA Overview, page 3.](#)
- [MPF Accelerated Features, page 5](#)
- [MPF-Supported Control Plane Features, page 13](#)
- [Punted Features, page 15](#)
- [Ignored MPF Features, page 16](#)
- [System Memory Requirements, page 19](#)
- [MPF Scalability, page 19](#)

MPF for Broadband LAC, LNS, and PTA Overview

MPF for Broadband LAC, LNS, and PTA is a method of accelerating a subset of broadband aggregation features on the Cisco 7301 and Cisco 7200 VXR routers by enabling fast-forwarding software on the second CPU. MPF for Broadband LAC, LNS, and PTA significantly improves performance by at least two times that of a regular Cisco 7301 or Cisco 7200 VXR router without any hardware changes.

MPF for Broadband LAC, LNS, and PTA is accomplished by the second CPU, CPU1, running fast-forwarding (FF) software to switch packets. Standard Cisco IOS features use a single CPU, CPU0, for both control plane and data functionality. MPF has moved the data plane traffic to the second CPU where LAC features, and LNS and PTA applications are processed at an accelerated rate, thus improving the performance of these broadband features. The MPF microcode running in CPU1 forwards traffic at approximately twice the forwarding performance of standard Cisco IOS software, allowing up to 1-Gbps line rate throughput. MPF can run all basic LAC, LNS, and PTA functionality with minimal impact to configuration and to Cisco IOS Release 12.3T and later functionality.

All control plane and data plane traffic is fast-forwarded to CPU1 for processing. A subset of MPF features is accelerated. Some non-MPF features that are not accelerated are punted to CPU0 where the non-MPF features are processed by standard Cisco IOS software running on CPU0. Some non-MPF features are considered unsupported and ignored in an MPF system.

When the Cisco IOS image containing MPF is loaded, fast-forwarding is enabled by default and LAC, LNS, and PTA features are accelerated. The first CPU, CPU0, always comes up first, and then the second CPU, CPU1, comes up. MPF is best deployed in networks requiring only MPF accelerated and punted features. The MPF image should not be used as a general purpose router image.

The Cisco IOS Release 12.4(4)T image is the recommended image for deploying MPF.

The NPE-G1 is required for the Cisco 7200 VXR router. LAC, LNS, and PTA functionality for both the Cisco 7301 and Cisco 7200 VXR routers is supported only on native Gigabit Ethernet (GE) ports. Traffic forwarding using the second CPU is only supported on the native GE ports. For example, the three native GE interfaces (G0/0, G0/1 and G0/2) on the Cisco 7301 router use the second CPU for traffic forwarding.

No port adapter traffic is accelerated by the second CPU. Any traffic from these port adapters will be forwarded using just the first CPU. We recommend you migrate any existing port adapter traffic to the native GE ports to take full advantage of the MPF accelerated features.

The benefits of improved network performance are important due to the rapid increase in broadband users. Existing customers who deploy an LNS network can gain performance without adding additional hardware into their network. Service providers can offer services to more subscribers while maintaining their current network topology. Customers who want to add LNS functionality can purchase the LNS MPF image on a new Cisco 7301 or Cisco 7200 VXR NPE-G1 router.

Figure 1 Typical LAC/LNS Network Topology

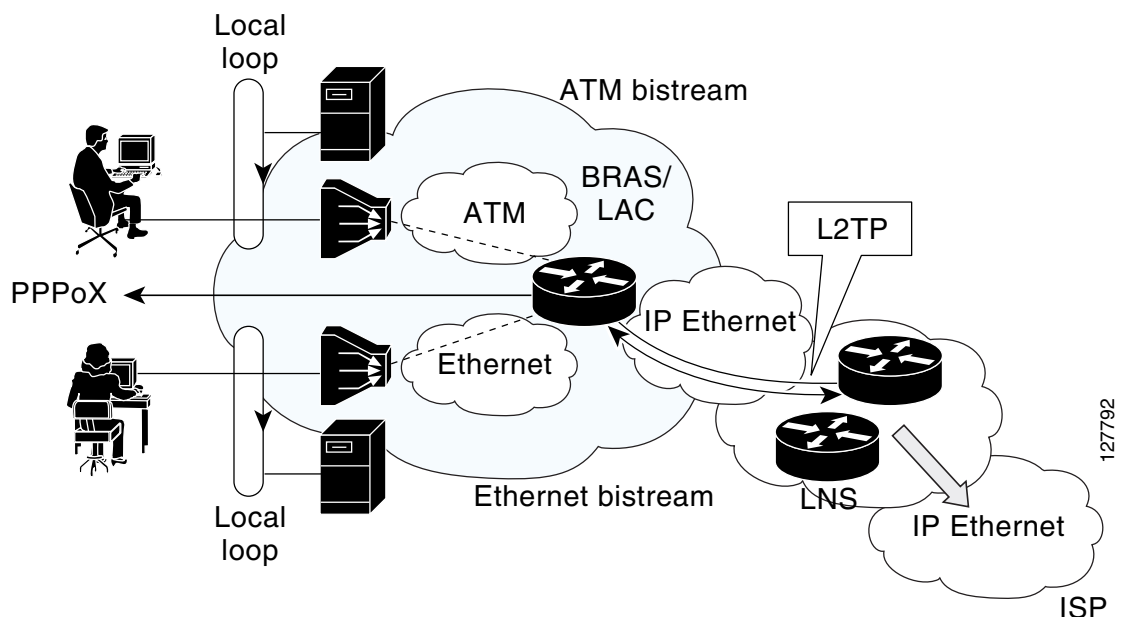


Figure 1 depicts a typical LAC/LNS solution deployment. In Figure 1, both wholesale and retail broadband models are supported. Either GE or ATM are on the LAC access side and connect to either a GE-DSL Access Multiplexer (DSLAM) or ATM-DSLAM, respectively. MPF accelerated features are only supported for the Cisco 7301 or Cisco 7200 VXR NPE-G1 native GE ports, which require the service provider and Internet core to be Ethernet-based. ATM and MPLS are not accelerated on the LAC side.

The fast-forwarding software is bundled together with the Cisco IOS software image. When the Cisco IOS image is loaded, the second CPU is enabled by default. To disable fast-forwarding, use the **no ip mpf** command. In addition, **show** and **debug** commands monitor forwarding on the second CPU and provide statistics.

The MPF for Broadband LAC, LNS, and PTA feature requires the purchase of software to enable the second CPU. You may purchase the special image when you purchase a new Cisco 7301 or Cisco 7200 VXR router, or you may purchase the special MPF image as an upgrade. Contact your Cisco field representative or sales support team for more information.

MPF Accelerated, Punted, and Ignored Features

When a system is enabled for MPF by enabling fast forwarding on the second CPU (CPU1), all features are fast forwarded to CPU1. All MPF-supported features, comprising a subset of Cisco IOS features, are accelerated. See the [“MPF Accelerated Features” section on page 5](#) for a list of accelerated features.

Another subset of Cisco IOS features that is not accelerated by MPF and considered non-MPF features is punted to the first CPU for standard Cisco IOS processing. See the [“Punted Features” section on page 15](#) for a list of punted features.

Some non-MPF features may not undergo correct packet switching and are considered ignored. See the [“Ignored MPF Features” section on page 16](#) for a list of ignored features.

Port Adapter Coexistence with MPF

MPF does not accelerate any port adapter traffic. Because the first CPU, CPU0, controls all port adapters, there is no MPF accelerated feature support for any traffic that is switched to and from port adapters.

Port adapters generally can functionally coexist with the MPF architecture and are supported by MPF from the standpoint of functionality and stability. Port adapters operate normally within standard Cisco IOS software and port adapter traffic is directly controlled by Cisco IOS.

Certain port adapters are considered MPF-supported. For a list of the supported port adapters, see the [“Restrictions for MPF for Broadband LAC, LNS, and PTA” section on page 2](#).

If you switch traffic from a native MPF-accelerated GE port to a port adapter, or from a port adapter to a native MPF-accelerated GE port, standard Cisco IOS performance is not guaranteed. We recommend you migrate any existing port adapter traffic to the native Gigabit Ethernet interfaces to gain the full benefit of MPF accelerated features.

If all port adapter traffic is isolated to CPU0, the native GE port-to-GE port fast-forwarding performance is not affected.



Note

The behavior of using an unsupported port adapter is unpredictable and may cause interoperability and performance problems with the native, MPF-accelerated Gigabit Ethernet ports.

MPF Accelerated Features

MPF accelerated features are a subset of Cisco IOS features. They are Cisco IOS data plane features that are fast forwarded to the second CPU, CPU1, where packet switching is accelerated by MPF fast forwarding software.

Where applicable, all MPF accelerated features can be applied to interfaces, subinterfaces, Remote Authentication Dial-In User Service (RADIUS) per-user profiles, and per-user virtual templates (VTs), unless noted otherwise. RADIUS per-user profile features generally implement global policy maps or use access-group VSAs, that are defined locally on the router, to allow session scalability.

Although a RADIUS per-user profile can specify a customized, per-user Access Control List (ACL) that does not use any locally defined access group on the router, this approach is not recommended due to scaling and performance issues.

Additionally, all existing Cisco IOS Release 12.3(14)T or later CLI syntax is preserved for all features, whether they are MPF accelerated or not.

**Note**

All Virtual Access Interfaces (VAIs) are considered MPF accelerated. This limits all VAI features to the MPF accelerated feature subset, whether the VAI is exclusively used by MPF or a non-MPF port adapter.

[Table 1](#) describes the MPF accelerated features. Because these features are already documented in existing Cisco IOS releases or in technical notes, a link to the documentation is provided where relevant.

Table 1 *MPF Accelerated Features*

MPF Accelerated Feature	Notes and Restrictions
Supported encapsulations are: <ul style="list-style-type: none"> • L2TP • PPPoEoE • PPPoEoVLAN • 802.1Q (IP) • 802.3 ARPA ETH • LLC/SAP • LLC/SNAP 	<p>Support for L2TP, PPPoEoE, PPPoEoVLAN, 802.1Q (IP), and 802.3 ARPA ETH encapsulations was introduced in Cisco IOS Release 12.3(7)XI1.</p> <p>Support for LLC/SAP and LLC/SNAP encapsulations was introduced in Cisco IOS Release 12.3(14)YM2.</p>
L2TP access concentrator (LAC) support	<p>Support was introduced in Cisco IOS Release 12.3(7)XI1.</p> <p>LAC is a device that is typically (although not always) located at a service provider's point-of-presence (POP), where initial configuration and ongoing management are done by the service provider. Packets sent through tunnels to and from L2TP are accelerated.</p>
IPv4 forwarding	Support was introduced in Cisco IOS Release 12.3(7)XI1.
IP fragmentation	<p>Support was introduced in Cisco IOS Release 12.3(7)XI1.</p> <p>For more information, see the <i>IP Fragmentation and PMTUD</i> white paper.</p>
L2TP network server (LNS)	<p>Packets sent to the LNS are accelerated. LNS is the termination point for an L2TP tunnel. The LNS initiates outgoing calls and receives incoming calls from the LAC.</p> <p>For more information, see the following:</p> <ul style="list-style-type: none"> • Configuring Virtual Private Networks chapter in Part 3: Virtual Private Networks in the <i>Cisco IOS Dial Services Configuration Guide, Release 12.1</i>. • Understanding VPDN tech note

Table 1 *MPF Accelerated Features (continued)*

MPF Accelerated Feature	Notes and Restrictions
Managed LNS/Virtual Home Gateway (VHG)	<p>VPN Routing and Forwarding (VRF) Lite support only (no MPLS tag switching).</p> <p>VRF Lite is a feature that enables a service provider to support two or more VPNs (using only VRF-based IPv4), where IP addresses can be overlapped among the VPNs.</p> <p>Managed VRF is a new VRF functionally in broadband that allows a wholesale access provider to offer Virtual Private Networks to each respective Internet Service Provider (ISP) customer or corporate customer using not only the access provider's shared IP or MPLS infrastructure, but also using the same Cisco 7200 VXR or Cisco 7401ASR providing LNS or PTA functionality.</p>
PPP Termination and Aggregation (PTA)	<p>PTA is a PPP selection method in which service selection is based on a structured domain name (for example, username@service.com). PTA terminates the PPP session into a single routing domain. Users can only access one service and do not have access to the default network.</p> <p>For applicable information, see the “Service Selection Methods” chapter of the <i>Cisco 10000 Series Router Service Selection Gateway Configuration Guide</i>.</p>
Managed PTA	<p>VPN Routing and Forwarding (VRF) Lite support only (no MPLS tag switching).</p>
Access Control Lists (ACLs)	<p>ACLs can only be applied at the following:</p> <ul style="list-style-type: none"> • Physical interface • Subinterface (802.1Q encapsulated VLAN subinterface) • Per session (RADIUS and virtual template) <p>The show ip access-list command is the only supported CLI.</p> <p>See the “Access Control Lists Support” section on page 10 for types of ACLs accelerated, restrictions, and detailed support information.</p>

Table 1 MPF Accelerated Features (continued)

MPF Accelerated Feature	Notes and Restrictions
<p>The following QoS features and Modular QoS CLI (MQC) have limited support:</p> <ul style="list-style-type: none"> • Single-Rate Policer For information on the Single-Rate Policer, see the Traffic Policing feature module. • Two-Rate Policer (also known as dual rate policer) • QoS Packet Marking • QoS classification 	<p>Only QoS classification, policing, and packet marking using the policy map name at the global level is supported.</p> <p>Policing on an individual interface is supported for the following:</p> <ul style="list-style-type: none"> • Per session (RADIUS and virtual template) • Subinterface (802.1Q encapsulated VLAN subinterface) • Physical interface <p>The following are <i>not</i> supported:</p> <ul style="list-style-type: none"> • Class-Based Weighted Fair Queueing (CBWFQ), Weighted Random Early Detection (WRED), Committed Access Rate (CAR), and traffic shaping • Link Fragmentation and Interleaving (LFI) • NetFlow • Hierarchical policer nested service policies <p>Limited support. Only the following QoS packet marking policy map actions are supported:</p> <ul style="list-style-type: none"> • set precedence or set ip precedence command • set dscp or set ip dscp command • set qos-group command <p>Note The set precedence and set dscp commands apply to both IPv4 and IPv6 packets. IPv6 packet marking is processed by Cisco IOS because all IPv6 packets are punted to Cisco IOS. IPv4 packet marking is MPF-accelerated.</p> <p>All other set CLI commands are <i>not</i> supported.</p> <p>Limited support. Only the following QoS classification CLI commands to configure a class map for a per-session policy map are supported:</p> <ul style="list-style-type: none"> • match access-group command • match ip precedence command • match ip dscp command • match qos-group command • match not command <p>All other match commands are <i>not</i> supported.</p> <p>Refer to the Cisco IOS Quality of Service Solutions Command Reference for information on the match commands</p>

Table 1 *MPF Accelerated Features (continued)*

MPF Accelerated Feature	Notes and Restrictions
Tunnel Switching	<p>Tunnel switching allows the LAC or LNS tunnel switching device to terminate tunnels from LACs and forward the sessions through new L2TP tunnels selected independently of the client-supplied domains.</p> <p>For applicable information, see the L2TP Tunnel Switching feature module, Cisco IOS Release 12.1(1)DC.</p>
Multipath Load Balancing	<p>This feature was introduced in Cisco IOS Release 12.3(14)YM2.</p> <p>Enabled for:</p> <ul style="list-style-type: none"> • Physical interface • Subinterface (802.1Q encapsulated VLAN subinterface) <p>See the “Multipath Load Balancing” section on page 12 for more information.</p>
Unicast Reverse Path Forwarding (uRPF)	<ul style="list-style-type: none"> • ACL Suppressed Drops are not supported. • Multicast RPF is not supported. • uRPF must be applied at: <ul style="list-style-type: none"> – Physical interface – Subinterface (802.1Q encapsulated VLAN subinterface) – Per session (RADIUS and virtual template) <p>uRPF allows the router to see if any IP packet received at a router interface arrives on the best reverse path (return route) to the source address of the packet.</p> <p>See the Unicast Reverse Path Forwarding feature module, Cisco IOS Release 11.1.</p> <p>Also, see the “Configuring Unicast Reverse Path Forwarding” chapter of the <i>Cisco IOS Security Configuration Guide, Release 12.2</i>.</p>
IP Reassembly	<p>MPF supports IPv4 reassembly of L2TP tunnels and all IPv4 traffic using the second CPU to perform fast-forwarding reassembly of L2TP-encapsulated packets. The MPF reassembly path handles all fragmented IPv4 traffic that is destined for the router, whether it is L2TP traffic or not.</p> <p>For more information, see the IP Fragmentation and PMTUD white paper.</p>
Jumbo frames	<p>Support for jumbo frames that have a maximum transmission unit (MTU) size greater than 1500 bytes on Ethernet and Gigabit Ethernet interfaces. Larger MTUs can enhance performance by eliminating fragmentation.</p> <p>For applicable information, see the “Configuring Jumbo Frame Support” section of the <i>Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX</i>.</p>

Table 1 *MPF Accelerated Features (continued)*

MPF Accelerated Feature	Notes and Restrictions
ip tcp adjust-mss command function	<p>Command behaves as a standard Cisco IOS command.</p> <p>The ip tcp adjust-mss command must be applied at:</p> <ul style="list-style-type: none"> Physical interface Subinterface (802.1Q encapsulated VLAN subinterface) Per session (RADIUS and virtual template) <p>For more information, see the ip tcp adjust-mss command in the “Broadband Access: PPP and Routed Bridge Encapsulation Commands” chapter of the <i>Cisco IOS Wide-Area Networking Command Reference, Release 12.2T</i>.</p>
l2tp ip tos reflect command function	<p>Use in VPDN group configuration mode. Command behaves as a standard Cisco IOS command does.</p> <p>For more information, see the l2tp ip tos reflect command in the <i>Cisco IOS Dial Technologies Command Reference</i>.</p> <p>The closely-related commands, ip tos and ip precedence, are documented in the <i>Cisco IOS Bridging and IBM Networking Command Reference</i>.</p>
PPP Keep-alives	<ul style="list-style-type: none"> Applied at per-session (RADIUS and virtual template) level. Keep-alives response part is processed in MPF, generation part is processed in Cisco IOS.
IPv4 ICMP	<ul style="list-style-type: none"> ICMP unreachable errors due to the DF bit set, MTU exceeded, and ICMP redirects are accelerated.

Access Control Lists Support

When MPF is enabled, Turbo Access Control Lists is enabled by default. If MPF is disabled, all ACL packets are punted for Cisco IOS processing on all interfaces.

[Table 2](#) describes the support for different types of access control lists (ACLs) in an MPF network and whether the ACL is accelerated or not supported by MPF and thus ignored. The table lists ACLs by the type of ACL, such as time-based ACL, or the different methods of configuring ACLs, such as with QoS classification commands or configured with or without a RADIUS profile.

Table 2 *ACL Support in an MPF Network*

Type of ACL or Method of Configuring ACL	MPF Accelerated	Ignored by MPF
Security ACL with IP L3/L4 ACEs	Yes	No
Security ACL with any other format	No	Yes

Table 2 *ACL Support in an MPF Network (continued)*

Type of ACL or Method of Configuring ACL	MPF Accelerated	Ignored by MPF
QoS classification CLI commands	Yes, with restrictions. For details on restrictions and QoS classification CLI supported, see the Notes and Restrictions column for the “The following QoS features and Modular QoS CLI (MQC) have limited support:” row in Table 1.	No, if restrictions are complied with.
Any other QoS classification configuration CLI	No	Yes
Security ACL logging	Yes	No
Time-based ACL	No	Yes
Reflexive ACL	No	Yes
Virtual template-based per-session or per-user security ACL, configured with QoS classification	Yes, with restrictions. For details on restrictions and QoS classification CLI supported, see the Notes and Restrictions column for the “The following QoS features and Modular QoS CLI (MQC) have limited support:” row in Table 1.	No, if restrictions are complied with.
Context-based Access Control (CBAC) user ACLs (RADIUS profile configured)	No	Yes These packets are punted to Cisco IOS for processing.
CBAC user ACLs (non-RADIUS profile configured)	No	Yes These packets are punted to Cisco IOS for processing.
Other RADIUS ACLs	No	Yes
RADIUS profile configured QoS using ACL (called attribute 11 access-group support)	Yes, with restrictions. For details on restrictions and QoS classification CLI supported, see the Notes and Restrictions column for the “The following QoS features and Modular QoS CLI (MQC) have limited support:” row in Table 1.	No, if restrictions are complied with.

Table 2 *ACL Support in an MPF Network (continued)*

Type of ACL or Method of Configuring ACL	MPF Accelerated	Ignored by MPF
Marking, after QoS classification	Yes, with restrictions. For details on restrictions and QoS classification CLI supported, see the Notes and Restrictions column for the “ The following QoS features and Modular QoS CLI (MQC) have limited support: ” row in Table 1 .	No, if restrictions are complied with.
ACLs with unsupported Access Control Entries (ACEs) (such as L2 MAC-address, MPLS EXP)	No	Yes
ACLs on port adapters	No	Yes Cisco IOS directly handles all port adapter features. All MPF ACL and QoS restrictions do not apply to port adapters.

Multipath Load Balancing

The MPF Multipath Load Balancing feature optimizes resource usage by distributing traffic over multiple paths to transfer data to a destination when more than one path to the same destination is available.

Multipath Load Balancing supports per-destination load balancing, but not per-packet load balancing. Load balancing decisions are made on the outbound interface. When you configure load balancing, configure it on outbound interfaces. Per-destination load balancing is enabled by default when MPF is enabled. Disabling MPF disables MPF Multipath Load Balancing.

Multipath Load Balancing decides which path (or adjacency) to use, based on the source and destination IP addresses and the IP field of the packet. Network nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. If only IP information is considered, packets with the same source and destination IP address pair are forwarded out of the same path. However, packets with different source and destination IP addresses typically go out different paths.

Per-Destination Load Balancing

Per-destination load balancing allows the router to use multiple paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple paths are available. Traffic destined for different pairs tends to take different paths.

Per-destination load balancing ensures that packets destined for a given host pair arrive in order and are routed over the same links. Load sharing becomes more effective as the number of source-destination pairs increase because per-destination load balancing depends on the statistical distribution of traffic.

Multipath Load Balancing Algorithm

The data used to make a Multipath Load Balancing decision is passed through a hash function. The router uses the result of the hash function to pick the path or adjacency to load share. The hash function is based on the Bob Jenkins' algorithm. This algorithm is different from the one used by CEF Load Balancing and is found at the following URL: <http://burtleburtle.net/bob/hash/evahash.html>.

Restrictions

Multipath Load Balancing does not support port adapter interfaces.

Traffic is not load-balanced when traffic is sent between a native Gigabit Ethernet interface and a port adapter interface. Only 25% of the traffic is sent through the port adapter.

The traffic is equally divided at input, so that 50% of the traffic is MPF accelerated and is load-balanced via Multipath Load Balancing. The other 50% of the traffic is punted. The 50% that is punted is processed by standard Cisco IOS CEF load balancing, resulting in 25% of the traffic going to the port adapter and 25% going to the Gigabit Ethernet interface.

Multipath Load Balancing Command

The following command is supported to show which routing decision (next hop) is made for a given IP address pair:

```
show mpf ip exact-route [vrf vrf_name] src-ip-addr dst-ip-addr
```

See the **show mpf ip exact-route** command reference page in this document for more information.

MPF-Supported Control Plane Features

The first CPU continues to manage the control plane features, which are typically not accelerated. MPF supports the standard control plane features in Cisco IOS Release 12.3(14)T and later. [Table 3](#) describes the MPF-supported control plane features and any exceptions. The exception is that although Cisco IOS data counters are supported, protocol-specific counters and class map counters are not supported.

MPF accelerated features are compatible with the control plane features in providing accurate information or proper data plane configuration setup.

Table 3 *MPF-Supported Control Plane Features*

MPF-Supported Control Plane Feature	Notes and Restrictions
Logical line ID (LLID) blocking	See “Related Documents” section on page 27 for documentation information.
Per VRF AAA	
Domain to VRF Mapping	
MTU Adjust features	The following are <i>not</i> MPF-supported: <ul style="list-style-type: none"> Virtual Template (VT) policy-based routing (PBR) to clear Don't Fragment (DF) ip pmtu command in VPDN group configuration mode

Table 3 *MPF-Supported Control Plane Features (continued)*

MPF-Supported Control Plane Feature	Notes and Restrictions
L2TP Load Balancing with Random Tunnel Selection	Support was introduced in Cisco IOS Release 12.4(4)T. For more information, see the “Configuring L2TP Tunnel Server Load Balancing and Failover Using the RADIUS Tunnel Preference Attribute” section in “How to Configure AAA for VPDNs” in the <i>Cisco IOS VPDN Configuration Guide</i> .
DHCP Option 82	Supported for: <ul style="list-style-type: none"> • PPPoEoE • PPPoEoVLAN • IPv4 • IPv4 802.1Q
SNMP	
MIBs	CISCO-PROCESS-MIB was modified to retrieve statistics for both the first CPU (CPU0) and second CPU (CPU1). CPU0 always comes up first, and then CPU1. In the cpmCPUTotalTable, the second entry is statically reserved for MPF CPU1; the first entry is IOS CPU0. See the “MIBs” section on page 28 for more information.
Cisco IOS Statistics—all Cisco IOS counters are supported, with exceptions.	The exceptions are that protocol-specific counters, class map counters, and class-default counters are <i>not</i> supported. See the “Unsupported Cisco IOS Counters” section on page 14 for more information.
Cisco IOS show commands	
All standard RADIUS Accounting is supported.	
All standard RADIUS Attributes are supported.	
SYSLOG messages	
ACL logs	

Unsupported Cisco IOS Counters

In an MPF system, when a **show policy-map interface** command is issued, the class map counters display zero packets matched, even though packets are classified.

In the following example, policing and packet marking are configured in the same class map. Issuing the **show policy-map interface** command displays “0” matches, but shows packets being marked. The bold-faced text is for documentation purposes only.

```
Router# show policy-map interface
GigabitEthernet0/1

Service-policy input: pmap2
```

```

Class-map: cmap3 (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps =>MPF does not update class map counts

Match: access-group 21
  0 packets, 0 bytes
  5 minute rate 0 bps          =====>MPF does not update match counts

police:
  cir 8000 bps, bc 1500 bytes
  conformed 15 packets, 1500 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    drop
  conformed 0 bps, exceed 0 bps      =====>MPF and Cisco IOS update policer counts

QoS Set
  precedence 5
  Packets marked 15          =====>MPF and Cisco IOS update marking counts

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any          =====>MPF does not update class-default counts

```

Punted Features

Packets of features that are not accelerated MPF features are punted to CPU0 where the packets are processed by standard Cisco IOS software. Punted packets can be either control plane or data plane features.

When a punted packet type is received by MPF on CPU1, MPF sends the packet to CPU0 using a priority queue, where packets are flow-controlled via a credit-based design. Control plane packets are given higher priority over data plane packets.

Punted packets are completely handled by Cisco IOS software for all ingress and egress features and are viewed by Cisco IOS as packets received by the Cisco IOS port adapter driver.



Note

During the fast-forwarding process, partial feature packet modification may occur, but does not cause any unexpected Cisco IOS drops, crashes, network instability, or major behavioral differences. Impact is limited to policing and QoS marking features.

In the case of a port adapter-to-port adapter switching path or a hybrid switching path where one interface is a native MPF accelerated GE interface and the other is a port adapter running Cisco IOS (for example, ATM), the packets are punted to CPU0 for standard Cisco IOS feature processing of both ingress and egress features. Therefore your system gains no MPF performance improvements when you deploy port adapter-to-port adapter traffic switching as opposed to deploying MPF accelerated, native GE interface-to-GE interface traffic switching. See the [“Port Adapter Coexistence with MPF”](#) section on page 5 for more information on port adapters.

Table 4 describes the punted features in an MPF system.

Table 4 Punted Features

Punted Feature	Notes and Restrictions
Multicast for IPv4 and IPv6 Multicast User Authentication and Profile Support (IPv4 and IPv6)	Multicast User Authentication and Profile Support for IPv6 was introduced in Cisco IOS Release 12.4(4)T. For more information, see the Implementing IPv6 Multicast module in the <i>Cisco IOS IPv6 Configuration Guide</i> .
IPv6 Unicast	
VAI Context-based Access Control (CBAC)	
L2TP Keep-Alives (Hello request/replies)	
Packets destined to router, except for MPF accelerated features (LNS packets)	
Broadcast packets (including DHCP)	
CEF Accounting	
ARP	ARP packets are punted at high priority.
PPP IP Control/Unaccelerated PPP Datagrams including but not limited to: <ul style="list-style-type: none"> 8021: IP Control Protocol (NCP) C021: Link Control Protocol (exception: echo-request handled by MPF) C023: Password Authentication Protocol (PAP) C025: Link Quality Report C223: Challenge Handshake Authentication Protocol (CHAP) 0201: PPP 802.1d Hello 	Excluding IP datagram and PPP echo-replies

Ignored MPF Features

Ignored features in an MPF network are those Cisco IOS features that are neither accelerated by MPF nor punted for Cisco IOS processing. When an ignored MPF feature is applied to a native GE interface on an MPF system, the system accepts the configuration. However the unsupported MPF feature is ignored for traffic going through that native GE interface.

An ignored MPF feature is not punted and not processed by Cisco IOS software. The feature is ignored and does not cause any unexpected Cisco IOS drops, crashes, network instability, or major behavioral differences.

Ignored Warning Message

When an ignored MPF feature is configured, the system issues a console warning message for main physical interfaces and virtual templates. To avoid console loading issues, a single warning message is issued only for the first occurrence of the specific ignored feature for subinterfaces (VLANs) and virtual accesses (sessions).

Depending on whether the ignored feature is configured on the input or output direction for the interface or both, the warning message notes the configured input or output feature.

An example of the warning message follows:

```
Router#
%MPF-4-IGNOREDFEATURES:Interface Gi0/3:Input "PBR" configurations are
not MPF supported and are IGNORED.
%SYS-5-CONFIG_I:Configured from console by console
Router#

Router(config-if)#
%MPF-4-IGNOREDFEATURES:Interface Gi0/3:Input "PBR" configurations are
not MPF supported and are IGNORED.
%MPF-4-IGNOREDFEATURES:Interface Gi0/3:Output "NetFlow" configurations
are not MPF supported and are IGNORED.
```

Ignored Warning for Class-Map Feature Configuration—Tip

The following tip advises you of MPF behavior. When you make a policy configuration change to an already configured class-map feature definition, MPF issues an ignored warning message for any QoS feature that is ignored by MPF, even though you are not changing the QoS feature.

The following example shows an existing policy as configured on Gigabit Ethernet0/2 and the resulting ignored warning message when a change in precedence value is made to class-map 2:

Existing policy on Gigabit Ethernet0/2 is:

```
class-map match-all Class1
  match any
class-map match-all Class2
  match any

policy-map Policy1
class Class1
set precedence 2
set qos-group 5
class Class2
set precedence 0
set qos-group 5
```

You change the precedence value for class-map 2 from a value of 0 to 2, which MPF processes. However, the resulting ignored warning message is issued, even though you are not actually changing the QoS group feature:

```
Router(config)# policy-map Policy1
Router(config-pmap)# class Class2
Router(config-pmap-c)# set precedence 2
```

```
*Aug 3 01:58:37.184: %MPF-4-NOFEATURESUPPORT: Interface Gi0/2: QOS SET:'set local
QoS-group' is an unsupported MPF feature and is IGNORED.
```

Major Ignored MPF Features

Many of the ignored MPF features are related to QoS policing and QoS packet marking. See [Table 5](#) for a list of some of the major ignored MPF features. Note that this is not a comprehensive list of all Cisco IOS features that are not supported by MPF.

Table 5 Major Ignored MPF Features

Ignored Features	Notes and Restrictions
The following encapsulations are not supported: <ul style="list-style-type: none"> Q-in-Q (IP) PPPoEoQinQ 	
Layer 2 Forwarding (L2F) protocol	
The following QoS features and Modular QoS CLI (MQC) are not supported: <ul style="list-style-type: none"> Policer—Unsupported sets Packet marking—Unsupported sets Nested service policies and policers QoS Policing: Committed Access Rate (CAR) Traffic Shaping Weighted Random Early Detection (WRED) Class-Based Weighted Fair Queueing (CBWFQ) NetFlow drop command 	<ul style="list-style-type: none"> Link Fragmentation and Interleaving (LFI) is not supported. Any other QoS feature, except QoS classification, policing, and packet marking, is also not supported. Hierarchical policer nested service policies are not supported.
uRPF Suppressed Drop ACLs	
ACLs: <ul style="list-style-type: none"> Non-IP Layer 3/Layer 4 Security ACLs/ACEs Unsupported QoS MATCH classifications Time-based ACLs Reflexive ACLs 	See the “Access Control Lists Support” section on page 10 for additional information on unsupported ACLs.
Network Address Translation (NAT)	
Network-Based Application Recognition (NBAR)	
Virtual Template Pre-Cloning	The Cisco IOS Release 12.3(14)T CLI is not officially supported. We strongly recommend that you do <i>not</i> enable this feature because it disables the Cisco IOS idb scaling and session performance enhancement features.

System Memory Requirements

The second CPU, CPU1, uses shared system memory for various accelerated features. [Table 6](#) describes the minimum system memory requirements for all supported routers by type of deployment and whether the deployment is “basic” or features are turned on.

Table 6 *MPF Minimum System Memory Requirements*

Network Deployment	Supported Session Range	Minimum System Memory
LAC (basic, no features)	0–4000 sessions	256 MB
LAC (basic, no features)	4000–8000 sessions	512 MB 1 GB is highly recommended.
LNS/PTA (basic, no features)	0–8000 sessions	512 MB 1 GB is highly recommended.
LAC/LNS/PTA (with features)	0–8000 sessions	512 MB 1 GB is highly recommended.
LAC/LNS/PTA (basic or with features)	8000–16000 sessions	1 GB is required.

Basic Deployment

In a basic deployment, there are no configured features and only minimal routes. Specifically there is no use of ACLs, QoS Policers, or VRF instances. The maximum number of required routes fit into the available memory space.

Features Deployment

In a features deployment, any features and number of routes can be configured.

MPF Scalability

MPF supports the same scaling limits set by the Cisco 7200 series and Cisco 7301 routers.

MPF accelerated features are subject to the same scaling limits imposed by Cisco IOS Release 12.3T and do not attempt to increase the actual customer-usable scalability limits.

Configuring MPF for Broadband LAC, LNS, and PTA

This section contains the following tasks:

- [Disabling MPF for Broadband LAC, LNS, and PTA, page 20](#) (optional)
- [Enabling MPF for Broadband LAC, LNS, and PTA, page 21](#) (optional)
- [Verifying MPF for Broadband LAC, LNS, and PTA Is Enabled, page 22](#) (optional)

Disabling MPF for Broadband LAC, LNS, and PTA

This section contains the procedure to disable fast-forwarding on the second CPU on a Cisco 7301 or Cisco 7200 VXR router for MPF for Broadband LAC, LNS, and PTA.

Prerequisites

You have installed the MPF software image.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip mpf**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	no ip mpf Example: Router(config)# no ip mpf	Disables forwarding on the second CPU. The second CPU is enabled by default when the MPF image is installed.
Step 4	end Example: Router(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Enabling MPF for Broadband LAC, LNS, and PTA

This section contains the procedure to re-enable fast-forwarding on the second CPU on a Cisco 7301 or Cisco 7200 VXR router for MPF for Broadband LAC, LNS, and PTA.

Prerequisites

- You have installed the MPF software image.
- You must have IP routing turned on before enabling fast-forwarding on the second CPU.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mpf**
4. **scheduler allocate** *interrupt-time process-time* (required only for hybrid traffic)
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip mpf Example: Router(config)# ip mpf	Re-enables MPF if you have disabled MPF fast-forwarding on the second CPU. Note The second CPU is enabled by default when the MPF image is installed.

	Command or Action	Purpose
Step 4	<p><code>scheduler allocate interrupt-time process-time</code></p> <p>Example: Router(config)# <code>scheduler allocate 4000 800</code></p>	<p>(Optional) This step is only required when an MPF router enables applications which have hybrid traffic loads that are both MPF-switched and Cisco IOS-switched. Configure the scheduler allocate command as shown in the example to allow a critical Cisco IOS process-level application, CPUMON, enough processing CPU cycles to complete time-critical tasks.</p> <p><i>interrupt-time</i>—Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network interrupt context. The range is 400 to 60000 microseconds. We recommend the 4000 microseconds default.</p> <p><i>process-time</i>—Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled. The range is 100 to 4000. The default is 200 microseconds. We recommend 800 microseconds.</p> <p>An example of a hybrid MPF and Cisco IOS switched traffic is IPv6 or PPPoEoA, which is handled by Cisco IOS, and IPv4 L2TP, which is switched by MPF.</p> <p>If CPUMON does not receive enough CPU processing cycles, the following error message may be generated:</p> <pre>00:54:15: %R4K_MP-3-CPUMON_QFULL: CPU Monitor queue full</pre>
Step 5	<p><code>end</code></p> <p>Example: Router(config)# <code>end</code></p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

Verifying MPF for Broadband LAC, LNS, and PTA Is Enabled

Perform this optional task to verify that MPF fast-forwarding is enabled for the second CPU.

SUMMARY STEPS

1. `enable`
2. `show version`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	Router# show version Example: Router# show version	Displays information about the currently loaded software version along with hardware and device information, including information about whether the second CPU (CPU1) is enabled for MPF.

Configuration Examples for MPF for Broadband LAC, LNS, and PTA

This section contains examples of the following **show** commands used to verify MPF configurations.

- [Example of show version Command, page 23](#)
- [Example of show mpf cpu Command, page 25](#)
- [Example of show mpf cpu history Command, page 25](#)
- [Example of show mpf punt Command, page 26](#)
- [Example of show ip interface Command, page 26](#)
- [Example of show interface stats Command, page 27](#)

Example of show version Command

The following **show version** command example displays the second CPU (CPU1) enabled for MPF for Broadband LAC, LNS, and PTA. Note that the **show version** output displays “SB-1 CPU” when processor 1 is enabled. Some of the output is set in boldface for documentation purposes to show that the MPF software is present.

Cisco 7301 show version Command Example

```
Router# show version
```

```
Cisco IOS Software, 7301 Software (C7301-I12S-M), Experimental Version
12.3(20040524:050554) [REL-v123_7_xi_throttle.ios-weekly 114]
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Mon 24-May-04 06:26 by userid
```

```
ROM:System Bootstrap, Version 12.3(4r)T2, RELEASE SOFTWARE (fc1)
BOOTLDR: Cisco IOS Software, 7301 Software (C7301-BOOT-M), Experimental Version
12.3(20040514:051116) [userid-v123_7_xi_throttle-ios-nightly-task 117]
```

```
Router uptime is 1 hour, 50 minutes
System returned to ROM by reload at 18:05:37 UTC Wed Mar 22 2004
System image file is "disk0:c7301-i12s-mz"
```

Cisco 7301 (NPE) processor (revision C) with 229376K/32768K bytes of memory.
Processor board ID 74806813

SB-1 CPU at 700MHz, Implementation 1, Rev 0.2, 512KB L2 Cache
1 slot midplane, Version 3.0

Last reset from watchdog nmi

CPU 1 Multi-Processor Forwarding, Fri May 21 14:21:57 2004 [dailybuil 119]

1 FastEthernet interface
3 GigabitEthernet interfaces
509K bytes of NVRAM.

62976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
32768K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0

Cisco 7200 VXR show version Command Example

Router# **show version**

Cisco IOS Software, **7200 Software (C7200-I12S-M)**, Version 12.3(BSNOP4_NIGHTLY.050202)
UBUILDIT Image, CISCO DEVELOPMENT TEST VERSION
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 02-Feb-05 04:57 by
ROM: System Bootstrap, Version **12.3(4r)T3**, RELEASE SOFTWARE (fc1)
BOOTLDR: Cisco IOS Software, 7200 Software (C7200-KBOOT-M),
12.3(20040712:050512) [REL-v123_7_xi_throttle.ios-weekly 115]
Lacl uptime is 16 hours, 22 minutes
System returned to ROM by reload at 18:12:49 UTC Mon Feb 7 2005
System image file is
"tftp://223.255.254.254/auto/tftpboot-users/agiye/c7200-i12s-mz.2005-02-02.BSNOP4_NIGH"
Last reload reason: Reload command

Cisco 7206VXR (NPE-G1) processor (revision 0xFF) with 983040K/65536K bytes of memory.
Processor board ID 31650243

SB-1 CPU at 700MHz, Implementation 1025, Rev 0.2, 512KB L2 Cache
6 slot VXR midplane, Version 2.7

Last reset from power-on

CPU 1 Multi-Processor Forwarding, Tue Feb 1 00:48:42 PST 2005 [userid 100]

PCI bus mb1 (Slots 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb1 has a total of 400 bandwidth points.
This configuration is within the PCI bus capacity and is supported.
PCI bus mb2 (Slots 2, 4 and 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 700 bandwidth points.
The set of PA-2FE, PA-POS-2OC3, and I/O-2FE qualify for "half
bandwidth points" consideration, when full bandwidth point counting
results in oversubscription, under the condition that only one of the
two ports is used. With this adjustment, current configuration on bus
mb2 has a total of 700 bandwidth points.
This configuration has oversubscribed the PCI bus and is not a
supported configuration.

Please refer to the following document "Cisco 7200 Series Port
Adaptor Hardware Configuration Guidelines" on CCO <www.cisco.com>,
for c7200 bandwidth points oversubscription/usage guidelines.

WARNING: PCI bus mb2 Exceeds 600 bandwidth points

1 Ethernet interface
2 FastEthernet interfaces
5 Gigabit Ethernet interfaces
1 ATM interface
509K bytes of NVRAM.

62976K bytes of ATA PCMCIA card at slot 2 (Sector size 512 bytes).
16384K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2

CPU% per hour (last 72 hours)
 * = maximum CPU% # = average CPU%

Example of show mpf punt Command

Use the **show mpf punt** command to display the per-box punt reason and punt packet counts.

```
Router# show mpf punt
slns#show mpf punt
Type           Message                               Count
l2tp           unknown session errors                7
l2tp           L2TP control                          6
ipv4/verify    adjacency punt                        1
ethernet       unknown ethernet type                 542
ppp            punts due to unknown protocol         333
arp            ARP request                            6
```

Example of show ip interface Command

This example uses the **show ip interface** command to show interface information on interface Gigabit Ethernet0/3. The example shows that MPF is enabled and the PBR and NetFlow features are not supported by MPF and ignored. The highlighted arrow (for documentation purposes only) shows the configured output and input features and the additional MPF interface information.

```
Router# show ip interface g0/3
GigabitEthernet0/3 is up, line protocol is up
  Internet address is 155.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
```

```

IP Multi-Processor Forwarding is enabled <===== MPF information
IP Input features, "PBR",
    are not supported by MPF and are IGNORED
IP Output features, "NetFlow",
    are not supported by MPF and are IGNORED

```

Example of show interface stats Command

Use the **show interface stats** command to display counters for MPF switched packets in an MPF network.

```
Router# show interface stats
```

```

GigabitEthernet0/1
    Switching path    Pkts In   Chars In   Pkts Out   Chars Out
    Processor         33090    6424353   86353     8645650
    Route cache       2         116       0          0
    Multi-Processor Fwding 1004    158632   5004     790632
    Total             34096    6583101   91357     9436282

```

Additional References

The following sections provide references related to MPF for Broadband LAC, LNS, and PTA.

Related Documents

Related Topic	Document Title
Cisco 7301 router: Upgrading and Troubleshooting Tasks, using the show version command	<i>Cisco 7301 Installation and Configuration Guide</i> , “ Starting and Configuring the Router ” chapter
Cisco 7200 VXR routers: NPE-G1 Installation and Configuration Information	<i>Network Processing Engine and Network Services Engine Installation and Configuration</i> , “ NPE-G1 Installation and Configuration Information ” chapter, “ Enabling the Second Processor ”
IP commands: command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services, Release 12.3T</i>
Logical Line ID (LLID) blocking functionality	See the <i>RADIUS Logical Line ID and L2TP Calling Station ID Suppression</i> feature modules for information on using LLID.

Standards

Standards	Title
RFC 2661	L2TP—Internet Engineering Task Force (IETF) standard
Gigabit Ethernet IEEE 802.3z	—
IEEE 802.1Q	—

MIBs

MIBs	MIBs Link
<p>CISCO-PROCESS-MIB is used to retrieve statistics for both the first CPU (CPU0) and second CPU (CPU1). CPU0 always comes up first, and then CPU1. For the second CPU, only the cpmCPUTotalTable is supported (for overall information of CPU load). In the cpmCPUTotalTable, the second entry is statically reserved for MPF CPU1; the first entry is IOS CPU0.</p> <p>No new MIBs are supported by this feature and support for existing MIBs has not been modified by this feature.</p>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
<p>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</p>	<p>—</p>

Technical Assistance

Description	Link
<p>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

This section documents only new and modified commands.

New Commands

- `clear mpf interface`
- `clear mpf punt`
- `show mpf ip exact-route`
- `show mpf cpu`
- `show mpf interface`
- `show mpf punt`
- `sw-module heap fp`

Modified Commands

- `ip mpf`
- `show interface stats`
- `show ip interface`

clear mpf interface

To clear Multi-Processor Forwarding (MPF) packet counts on all physical interfaces, use the **clear mpf interface** command in user EXEC or privileged EXEC mode.

clear mpf interface

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines This command has no output. It resets the packet counters shown in the **show mpf interface** command output.

Examples The following example uses the **clear mpf interface** command to reset the packet counters displayed in the output of the **show mpf interface** command:

```
Router# clear mpf interface
```

Related Commands	Command	Description
	clear mpf punt	Clears MPF per-box punt reason and count.
	ip mpf	Enables MPF on the second CPU of Cisco 7200 VXR and Cisco 7301 routers.
	show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
	show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
	show mpf interface	Displays packet count information on each physical interface.
	show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
	show mpf punt	Displays the punt reason and punt packet count for the chassis.
	sw-module heap fp	Fine-tunes the MPF heap memory allocation.

clear mpf punt

To clear Multi-Processor Forwarding (MPF) per-box punt reason and counts, use the **clear mpf punt** command in user EXEC or privileged EXEC mode.

clear mpf punt

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines This command clears all punt counters and implicitly generates **show mpf punt** output. It resets for each box or router chassis the punt packet counters shown in the **show mpf punt** command output. Packets that are punted are directed for Cisco IOS processing and are not accelerated by MPF.

Examples The following example clears the type of packets (Type), the reasons for the punt (Message), and the punt packet counts (Count) for the router chassis, then implicitly generates **show mpf punt** output.

```
Router# show mpf punt
```

Type	Message	Count
l2tp	unknown session errors	7
l2tp	L2TP control	6
ipv4/verify	adjacency punt	1
ethernet	unknown ethernet type	542
ppp	punts due to unknown protocol	333
arp	ARP request	6

```
Router# clear mpf punt
```

Type	Message	Count
arp	ARP request	38
ethernet	unknown ethernet type	591
l2tp	unknown session errors	71790
l2tp	unsupported output feature	24000

[Table 7](#) describes the fields in the **clear mpf punt** output display.

Table 7 *clear mpf punt Field Descriptions*

Field	Description
Type	Packet type or encapsulation, such as ARPA, Ethernet, or L2TP.
Message	Reason for the punt of the packet to Cisco IOS processing.
Count	Punt packet count.

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
ip mpf	Enables MPF on the second CPU of Cisco 7200 VXR and Cisco 7301 routers.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays packet count information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

ip mpf

To enable Multi-Processor Forwarding (MPF) on the second CPU of a Cisco 7200 VXR and Cisco 7301 routers, use the **ip mpf** command in global configuration mode. To disable MPF, use the **no** form of this command.

ip mpf

no ip mpf

Syntax Description

This command has no arguments or keywords.

Command Default

MPF is enabled by default on the second CPU.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XI1	This command was introduced for the Cisco 7301 router.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

This command allows you to disable and reenabling MPF.

MPF is enabled by default on the second CPU (CPU1). The special MPF image is bundled together with the Cisco IOS image and must be purchased.



Note

A prerequisite for MPF is that Cisco Express Forwarding (CEF) must be enabled. MPF cannot be enabled unless CEF is enabled first. CEF cannot be disabled (using the **no ip cef** command) unless MPF is disabled first.

Because MPF is enabled by default when the special MPF image is booted up, if CEF is not enabled, MPF is not enabled and boots up with an error message in the error log.

Examples

The following example disables MPF on the second CPU:

```
Router(config)# no ip mpf
```

The following configuration example shows a system where CEF is disabled and the resulting error message showing that MPF cannot be enabled:

```
00:00:13:%MPF-4-NOIPCEF:MPF disabled due to IP CEF disabled
00:00:13:%MPF-6-MODULE:CPU 1 switching module is ready
```

The following configuration example shows that 1) CEF cannot be disabled until MPF is disabled first; and 2) MPF cannot be enabled until CEF is enabled first:

```
Router(config)# no ip cef
%Cannot disable CEF on this platform
Router(config)# no ip mpf
Router(config)# no ip cef
Router(config)# ip mpf
%Can not enable MPF when CEF is disabled.
Router(config)# ip cef
Router(config)# ip mpf
```

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip cef	Enables CEF.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays MPF packet counter information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

show interface stats

To display numbers of packets that were process switched, fast switched, and distributed switched, use the **show interface stats** command in user EXEC or privileged EXEC mode.

show interface *type number* **stats**

Syntax Description	<i>type number</i>	Interface type and number about which to display statistics.
--------------------	--------------------	--

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	11.0	This command was introduced.
	12.3(14)YM2	This command was modified to show the counter for Multi-Processor Forwarding (MPF) switched packets.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines Use this command on the RP.



Note

When fast switching is configured on the outbound interface, and RSP optimum, RSP flow, and VIP DFS switching modes are all specified on the incoming interface, the interface on which RSP optimum, RSP flow, and VIP DFS switching modes is not enabled can still show packets switched out via those switching paths when packets are received from other interfaces with RSP optimum, RSP flow, and VIP DES switching modes enabled.

Examples

The following sample output is from Cisco IOS Release 12.3(14)YM2 and shows counters for both Multi-Processor Forwarding (MPF) switched packets on native GigabitEthernet interfaces and for non-MPF FastEthernet interfaces:

```
Router# show interface stats
GigabitEthernet0/0
  Switching path  Pkts In   Chars In   Pkts Out   Chars Out
  Processor       0         0          225        77625
  Route cache     0         0           0           0
  Multi-Processor Fwding  950      221250    500         57000
  Total           950      221250    725        134625
GigabitEthernet0/1
  Switching path  Pkts In   Chars In   Pkts Out   Chars Out
  Processor       1         60         226        77685
  Route cache     0         0           0           0
  Multi-Processor Fwding  500      57000     500         57000
  Total           501      57060     726        134685
GigabitEthernet0/2
  Switching path  Pkts In   Chars In   Pkts Out   Chars Out
  Processor       1         60         226        77685
```

■ **show interface stats**

```

                Route cache          0          0          0          0
      Multi-Processor Fwding         0          0          0          0
                Total                1         60         226       77685
FastEthernet1/0
      Switching path   Pkts In   Chars In   Pkts Out   Chars Out
      Processor       34015   5331012   1579      158190
      Route cache      0        0         0         0
      Total           34015   5331012   1579      158190

```

The following is sample output from the **show interface stats** command:

Router# **show interface fddi 3/0/0 stats**

```

Fddi3/0/0
      Switching path   Pkts In   Chars In   Pkts Out   Chars Out
      Processor       3459994  1770812197  4141096  1982257456
      Route cache     10372326  3693920448   439872  103743545
      Distributed cache 19257912  1286172104  86887377 1184358085
      Total           33090232  2455937453  91468345 3270359086

```

[Table 8](#) describes the significant fields in the display.

Table 8 *show interface stats Field Descriptions*

Field	Description
Fddi3/0/0	Interface for which information is shown.
Switching path	Column heading for the various switching paths below it.
Pkts In	Number of packets received in each switching mechanism.
Chars In	Number of characters received in each switching mechanism.
Pkts Out	Number of packets sent out each switching mechanism.
Chars Out	Number of characters sent out each switching mechanism.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

```
show ip interface [type number] [brief]
```

Syntax Description	
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(3)T	This command was expanded to include the status of ip wccp redirect out and ip wccp redirect exclude add in commands.
	12.2(14)S	This command was expanded to display the status of NetFlow on a subinterface.
	12.2(15)T	The command output enhancements introduced in Cisco IOS Release 12.2(14)S were integrated into Cisco IOS Release 12.2(15)T.
	12.3(6)	The command output was modified to identify the downstream VRF in the output.
	12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
	12.3(14)YM2	This command was modified to show the usability status of interfaces configured for Multi-Processor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface can send and receive packets. If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see information for that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

The **show ip interface brief** command can be used to view a summary of the router interfaces. This command displays the IP address, interface status, and additional information.

Examples

The following examples from Cisco IOS Release 12.3(14)YM2 show:

- Configuration information on interface Gigabit Ethernet0/3, where the IP flow egress feature is configured on the output side (where packets go out of the interface) and the policy route-map named PBR_NAME is configured on the input side (where packets come into the interface).
- Interface information on Gigabit Ethernet interface 0/3 showing that MPF is enabled and that both features are not supported by MPF and are ignored.

The highlighted arrows (for documentation purposes only) show the configured output and input features and the additional MPF interface information.

```
Router# show running-config interface g 0/3

interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress                <== output
 ip policy route-map PBR_NAME  <== input
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

```
Router# show ip interface g 0/3

GigabitEthernet0/3 is up, line protocol is up
 Internet address is 10.1.1.1/16
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP CEF switching is enabled
 IP Feature Fast switching turbo vector
 IP VPN Flow CEF switching turbo vector
 IP multicast fast switching is enabled
 IP multicast distributed fast switching is disabled
 IP route-cache flags are Fast, CEF
 Router Discovery is disabled
 IP output packet accounting is disabled
 IP access violation accounting is disabled
 TCP/IP header compression is disabled
 RTP/IP header compression is disabled
 Policy routing is enabled, using route map PBR
 Network address translation is disabled
 BGP Policy Mapping is disabled
```

```

IP Multi-Processor Forwarding is enabled <===== MPF information
  IP Input features, "PBR",
    are not supported by MPF and are IGNORED
  IP Output features, "NetFlow",
    are not supported by MPF and are IGNORED

```

The following example identifies a downstream VRF. The highlighted line (for documentation purposes only) identifies the downstream VRF.

```
Router# show ip interface vi 3
```

```

Virtual-Access3 is up, line protocol is up
Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
Broadcast address is 255.255.255.255
Peer address is 10.8.1.1
MTU is 1492 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN CEF switching turbo vector
VPN Routing/Forwarding "U"
Downstream VPN Routing/Forwarding "D"
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled

```

Table 9 describes the significant fields shown in the display.

Table 9 *show ip interface Field Descriptions*

Field	Description
Virtual-Access3 is up	If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Displays the broadcast address.
Peer address is	Displays the peer address.
MTU is	Displays the MTU value set on the interface.
Helper address	Displays a helper address, if one has been set.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	Specifies the IP Security Option (IPSO) security level set for this interface.
Split horizon	Indicates that split horizon is enabled.
ICMP redirects	Specifies whether redirect messages will be sent on this interface.
ICMP unreachable	Specifies whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.
IP fast switching	Specifies whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Specifies whether Flow switching is enabled for this interface.
IP CEF switching	Specifies whether Cisco Express Forwarding is enabled for the interface.
Downstream VPN Routing/Forwarding “D”	Specifies the VRF where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Specifies whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast, Flow init, CEF, Ingress Flow	Specifies whether NetFlow has been enabled on an interface. Displays “Flow init” to specify that NetFlow is enabled on the interface. Displays “Ingress Flow” to specify that NetFlow is enabled on a subinterface using the ip flow ingress command. Specifies “Flow” to specify that NetFlow is enabled on a main interface using the ip route-cache flow command.

Table 9 *show ip interface Field Descriptions (continued)*

Field	Description
Router Discovery	Specifies whether the discovery process has been enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Specifies whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
WCCP Redirect outbound is disabled	Indicates the status of whether packets received on an interface are redirected to a cache engine. Displays “enabled” or “disabled.”
WCCP Redirect exclude is disabled	Indicates the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays “enabled” or “disabled.”

The following is sample output from the **show ip interface brief** command:

```
Router# show ip interface brief
```

```
Interface      IP-Address      OK? Method Status Protocol
Ethernet0      10.108.00.5     YES NVRAM  up      up
Ethernet1      unassigned      YES unset  administratively down down
Loopback0      10.108.200.5    YES NVRAM  up      up
Serial0        10.108.100.5    YES NVRAM  up      up
Serial1        10.108.40.5     YES NVRAM  up      up
Serial2        10.108.100.5    YES manual up      up
Serial3        unassigned      YES unset  administratively down down
```

Table 10 *show ip interface brief Field Descriptions*

Field	Description
Interface	Type of interface.
IP-Address	IP Address assigned to the interface.
OK?	“Yes” means that the IP Address is currently valid. “No” means that the IP Address is not currently valid.

Table 10 show ip interface brief Field Descriptions (continued)

Field	Description
Method	<p>The method field has the following possible values:</p> <ul style="list-style-type: none"> • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request • BOOTP—Bootstrap protocol • TFTP—Configuration file obtained from TFTP server • manual—Manually changed by CLI command • NVRAM—Configuration file in NVRAM • IPCP—ip address negotiated command • DHCP—ip address dhcp command • unassigned—No IP address • unset—Unset • other—Unknown
Status	<p>Indicates the status of interface. Valid values and their meanings are:</p> <ul style="list-style-type: none"> • up—Interface is administratively up. • down—Interface is administratively down. • administratively down—Interface is administratively down.
Protocol	<p>Indicates the operational status of the routing protocol on this interface.</p>

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autclassify	Enables VRF autclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show mpf ip exact-route

To display the exact route for a source-destination address IP pair in a Multi-Processor Forwarding (MPF) system, use the **show mpf ip exact-route** command in user EXEC or privileged EXEC mode.

```
show mpf ip exact-route [vrf vrf-name] src-ip-addr dst-ip-addr
```

Syntax Description	Parameter	Description
	vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
	<i>vrf-name</i>	(Optional) Name assigned to the VRF.
	<i>src-ip-addr</i>	Specifies the network source address.
	<i>dst-ip-addr</i>	Specifies the network destination address.

Command Default No default behavior or values.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and supported on the Cisco 7200 VXR and Cisco 7301 routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines When you are load balancing per destination, this command shows the exact next hop that is used for a given IP source-destination pair.

Examples The following sample output displays the exact next hop (10.1.104.1) for the specified source IP address (10.1.1.1) and destination IP address (172.17.249.252):

```
Router# show mpf ip exact-route 10.1.1.1 172.17.249.252
10.1.1.1          -> 172.17.249.252 :GigabitEthernet2/0 (next hop 10.1.104.1)
```

[Table 11](#) describes the significant fields shown in the output example.

Table 11 *show mpf ip exact-route* Field Descriptions

Field	Description
10.1.1.1 -> 172.17.249.252	From source 10.1.1.1 IP address to destination IP address 172.17.249.252.
GigabitEthernet2/0 (next hop 10.1.104.1)	Next hop is 10.1.104.1 on GigabitEthernet interface 2/0.

■ **show mpf ip exact-route**

Related Commands	Command	Description
	clear mpf interface	Clears MPF packet counts on all physical interfaces.
	clear mpf punt	Clears MPF per-box punt reason and count.
	ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
	show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
	show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
	show mpf interface	Displays MPF packet count information on each physical interface.
	show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.
	sw-module heap fp	Fine-tunes the MPF heap memory allocation.

show mpf interface

To display Multi-Processor Forwarding (MPF) packet counter information on each physical interface, use the **show mpf interface** command in user EXEC or privileged EXEC mode.

```
show mpf interface [interface-name-and-number] [dot1q-vlan-num]
```

Syntax Description	
<i>interface-name-and-number</i>	(Optional) Displays punt counts for a specified Gigabit Ethernet interface and its slot number and port number.
<i>dot1q-vlan-num</i>	(Optional) Displays punt counts on a specific subinterface by specifying the 802.1Q VLAN number.

Command Default No default behavior or values.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines This command is supported for physical interfaces and subinterfaces. There is no support for the virtual access interface (VAI).

You can display the interface count information for a specific Gigabit Ethernet interface by specifying the interface name and number. To display interface information for a specified subinterface only, you must use the 802.1Q VLAN number for the subinterface because the MPF software does not recognize the subinterface number.

Using the **show mpf interface** command without arguments displays the interface information for all Gigabit Ethernet interfaces and subinterfaces.

Using the **clear mpf interface** command resets the interface packet counters shown in the **show mpf interface** command output.

Examples

The following example using the **show mpf interface** command without arguments displays interface information about up or down state, type of counter (receiving or transmitting packet or bytes), and count number for packets or bytes for all Gigabit Ethernet interfaces (only GigabitEthernet0/1 in this example) and subinterfaces:

```
Router# show mpf interface
```

Name	Index	State	Counter	Count
Gi0/1	0	up	RX packets	1004
			RX bytes	158632
			TX packets	5004
			TX bytes	790632
Gi0/1	1	up	RX punts	32961
			TX punts	85972
			RX packets	1004
			RX bytes	158632
Gi0/1.100	100	up	TX packets	5004
			TX bytes	790632
			RX punts	25
			RX packets	1004
Gi0/1.101	101	up	RX bytes	158632
			RX punts	25
Gi0/1.102	102	up	TX packets	5004
			TX bytes	790632
Gi0/1.105	105	up	RX punts	29
			RX packets	1004
Gi0/1.106	106	up	TX bytes	790632
			TX packets	5004
Gi0/1.107	107	up	RX punts	26114
			RX packets	1004
Gi0/1.200	200	up	TX bytes	790632
			TX packets	5004
Gi0/1.201	201	up	RX punts	29
			RX packets	1004
Gi0/1.202	202	up	TX bytes	790632
			TX packets	5004
Gi0/1.206	206	up	RX punts	26114
			RX packets	1004
Gi0/1.2002	602	up	TX bytes	790632
			TX packets	5004
Gi0/1.2004	604	up	RX punts	26114
			RX packets	1004

The following example specifies interface information for Gigabit Ethernet interface 0/1 subinterface 100. However, all Gigabit Ethernet interface and subinterface information is displayed because MPF does not recognize the subinterface number, unless it is a VLAN number.

```
Router# show mpf interface GigabitEthernet0/1.100
```

Name	Index	State	Counter	Count
Gi0/1	0	up	RX packets	1004
			RX bytes	158632
			TX packets	5004
			TX bytes	790632
Gi0/1	1	up	RX punts	32996
			TX punts	86062
			RX packets	1004
			RX bytes	158632
Gi0/1.100	100	up	TX packets	5004
			TX bytes	790632
			RX punts	25
			RX packets	1004
Gi0/1.101	101	up	RX bytes	158632
			RX punts	25
Gi0/1.102	102	up	TX packets	5004
			TX bytes	790632
Gi0/1.105	105	up	RX punts	29
			RX packets	1004
Gi0/1.106	106	up	TX bytes	790632
			TX packets	5004
Gi0/1.107	107	up	RX punts	26142
			RX packets	1004
Gi0/1.200	200	up	TX bytes	790632
			TX packets	5004
Gi0/1.201	201	up	RX punts	29
			RX packets	1004
Gi0/1.202	202	up	TX bytes	790632
			TX packets	5004
Gi0/1.206	206	up	RX punts	26142
			RX packets	1004
Gi0/1.2002	602	up	TX bytes	790632
			TX packets	5004
Gi0/1.2004	604	up	RX punts	26142
			RX packets	1004

The following example displays the interface information for VLAN number 100 on Gigabit Ethernet interface 0/1, including up state, receiving packet count, receiving bytes count, transmitting packet count, transmitting byte count, and receiving punt count:

```
Router# show mpf interface GigabitEthernet0/1 100

Name          Index  State  Counter          Count
Gi0/1.100     100   up     RX packets       1004
              RX bytes         158632
              TX packets       5004
              TX bytes         790632
              RX punts         25
```

Table 12 describes the fields shown in the output examples.

Table 12 show mpf interface Field Descriptions

Field	Description
Name	Gigabit Ethernet interface name and number.
Index	This is for internal use and can be ignored.
State	Up or down state of interface.
Counter	Type of counter.
Count	Number of packets or bytes.
RX packets	Packets received through the Gigabit Ethernet interface and processed by the second CPU, CPU1. These packets are MPF accelerated.
RX bytes	Bytes received and processed by the second CPU, CPU1.
RX punts	Packets received through the Gigabit Ethernet interface and punted by the second CPU, CPU1, to CPU0 for Cisco IOS processing.
RX drop	Packets received through the Gigabit Ethernet interface but dropped by the second CPU, CPU1.
TX packets	MPF accelerated packets transmitted from the Gigabit Ethernet interface using the second CPU, CPU1.
TX bytes	Bytes transmitted by the second CPU, CPU1.
TX punts	Packets transmitted from the second CPU, CPU1. Packets that have been punted to CPU0 and processed by Cisco IOS software are redirected to CPU1 for transmitting from the relevant Gigabit Ethernet interface.
TX drop	Packets that were dropped by the second CPU, CPU1, while in the process of being transmitted from the Gigabit Ethernet interface.

■ **show mpf interface**

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

show mpf punt

To display the Multi-Processor Forwarding (MPF) punt reason and punt packet count for the chassis, use the **show mpf punt** command in user EXEC or privileged EXEC mode.

show mpf punt

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines The punt reason and punt packet count are collected for each box or chassis, not for each interface. Packets that are punted are directed for Cisco IOS processing and are not accelerated by MPF.

Examples The following example displays the types of packet, the reasons for the punt, and the punt packet counts for the router chassis.

```
Router# show mpf punt

      Type           Message                               Count
-----
l2tp                unknown session errors                7
l2tp                L2TP control                          6
ipv4/verify        adjacency punt                         1
ethernet           unknown ethernet type                542
ppp                punts due to unknown protocol        333
arp                ARP request                           6
```

[Table 13](#) describes the fields in the **show mpf punt** output display.

Table 13 show mpf punt Field Descriptions

Field	Description
Type	Packet type or encapsulation, such as ARPA, Ethernet, or L2TP.
Message	Reason for punting the packet to Cisco IOS processing.
Count	Punt packet count.

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays MPF packet count information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

sw-module heap fp

To fine-tune the Multi-Processor Forwarding (MPF) heap memory allocation required for specific session scaling and application needs, use the **sw-module heap fp** command in global configuration mode. To return the setting to the default (32 MB), use the **no** form of the command.

```
sw-module heap fp [megabytes]
```

```
no sw-module heap fp
```

Syntax Description	<i>megabytes</i>	(Optional) The heap size in megabytes (MB) for the MPF processor. The default size is 32 MB.
---------------------------	------------------	--

Command Default The default heap memory allocation size is 32 MB.

Command Modes Global configuration

Command History	Release	Modification
	12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines The default heap size is 32 MB if you do not specify otherwise. Once you have changed and saved the MPF heap memory configuration, reboot the router for the MPF memory size adjustment to take effect. The following table lists the recommended heap memory size by type of deployment and number of sessions configured:

Table 14 Recommended Heap Memory Sizes

Type of Deployment	Number of Sessions	Recommended Heap Size
PTA/LAC/LNS	8000 and over	80 MB

Examples The following example sets or changes the MPF heap memory size in a router to 80 MB:

```
Router(config)# sw-module heap fp 80
```

Related Commands	Command	Description
	clear mpf interface	Clears MPF packet counts on all physical interfaces.
	clear mpf punt	Clears MPF per-box punt reason and count.

Command	Description
ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays MPF packet count information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.

Glossary

broadband—Transmission methodology that multiplexes multiple independent signals onto one cable. In telecommunications, broadband is classified as any channel with bandwidth greater than 4kHz (typical voice grade). In LAN terminology, broadband is classified as a coaxial cable on which analog signaling is employed.

FF—fast-forwarding. Accelerates broadband features by enabling the second CPU on the Cisco 7301 and Cisco 7200 VXR routers.

MPF accelerated features—A subset of Cisco IOS features that is fast forwarded to CPU1 for processing, which significantly improves performance by up to two times that of a regular Cisco 7301 or Cisco 7200 VXR router without any hardware changes.

All control plane and data plane traffic is fast forwarded to CPU1 for processing.

punted—Non-MPF features that are not accelerated; packets are punted to CPU0 where they are processed by standard Cisco IOS software running on CPU0.

ROMmon—ROM monitor. ROMmon is the initializing software that is executed when the router is powered up.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

