

Common Causes of Slow IntraVLAN and InterVLAN Connectivity in Campus Switch Networks

Document ID: 23637

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Common Causes of Slow IntraVLAN and InterVLAN Connectivity

- Three Categories of Causes

- Causes for Network Slowness

Troubleshoot the Cause

- Troubleshoot Collision Domain Issues

- Troubleshoot Slow IntraVLAN (Broadcast Domain)

- Troubleshoot Slow InterVLAN Connectivity

Related Information

Introduction

This document addresses the most common issues that may contribute to network slowness. The document classifies common network slowness symptoms, and outlines approaches to problem diagnosis and resolution.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

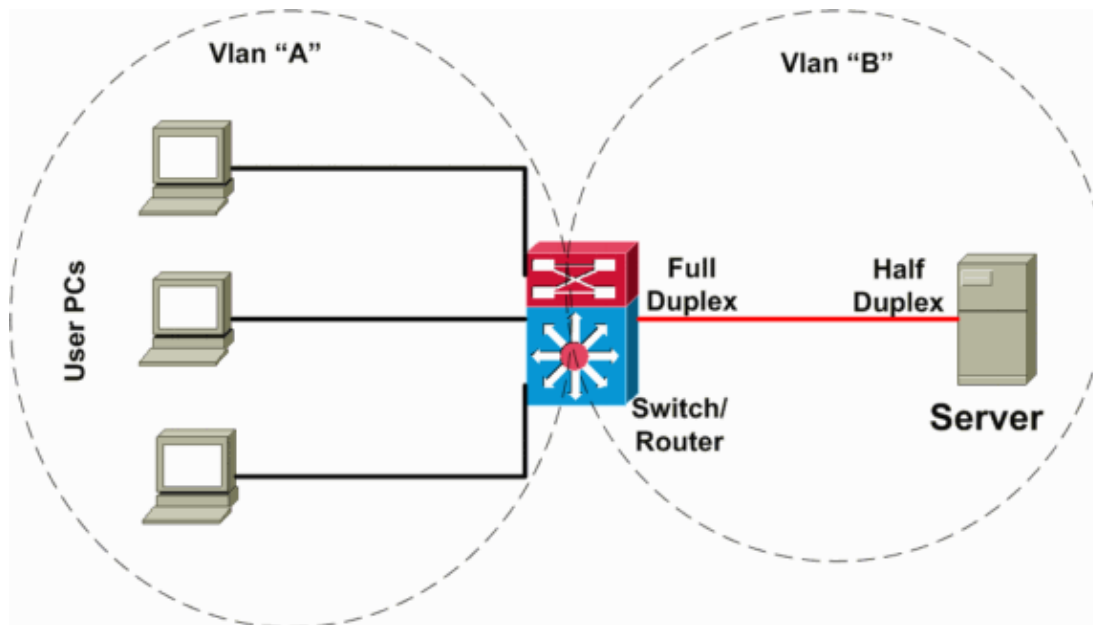
Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Common Causes of Slow IntraVLAN and InterVLAN Connectivity

The symptoms of slow connectivity on a VLAN can be caused by multiple factors on different network layers. Commonly the network speed issue may be occurring on a lower level, but symptoms can be observed on a higher level as the problem masks itself under the term "slow VLAN". To clarify, this document defines the following new terms: "slow collision domain", "slow broadcast domain" (in other words, slow VLAN), and "slow interVLAN forwarding". These are defined in the section Three Categories of Causes, below.

In the following scenario (illustrated in the network diagram below), there is a Layer 3 (L3) switch performing interVLAN routing between the server and client VLANs. In this failure scenario, one server is connected to a switch, and the port duplex mode is configured half-duplex on the server side and full-duplex on the switch side. This misconfiguration results in a packet loss and slowness, with increased packet loss when higher traffic rates occur on the link where the server is connected. For the clients who communicate with this server, the problem looks like slow interVLAN forwarding because they do not have a problem communicating to other devices or clients on the same VLAN. The problem occurs only when communicating to the server on a different VLAN. Thus, the problem occurred on a single collision domain, but is seen as slow interVLAN forwarding.



Three Categories of Causes

The causes of slowness can be divided into three categories, as follows:

Slow Collision Domain Connectivity

Collision domain is defined as connected devices configured in a half-duplex port configuration, connected to each other or a hub. If a device is connected to a switch port and full-duplex mode is configured, such a point-to-point connection is collisionless. Slowness on such a segment still can occur for different reasons.

Slow Broadcast Domain Connectivity (Slow VLAN)

Slow broadcast domain connectivity occurs when the whole VLAN (that is, all devices on the same VLAN) experiences slowness.

Slow InterVLAN Connectivity (Slow Forwarding Between VLANs)

Slow interVLAN connectivity (slow forwarding between VLANs) occurs when there is no slowness on the local VLAN, but traffic needs to be forwarded to an alternate VLAN, and it is not forwarded at the expected rate.

Causes for Network Slowness

Packet Loss

In most cases, a network is considered slow when higher-layer protocols (applications) require extended time to complete an operation that typically runs faster. That slowness is caused by the loss of some packets on the network, which causes higher-level protocols like TCP or applications to time out and initiate retransmission.

Hardware Forwarding Issues

With another type of slowness, caused by network equipment, forwarding (whether Layer 2 [L2] or L3) is performed slowly. This is due to a deviation from normal (designed) operation and switching to slow path forwarding. An example of this is when Multilayer Switching (MLS) on the switch forwards L3 packets between VLANs in the hardware, but due to misconfiguration, MLS is not functioning properly and forwarding is done by the router in the software (which drops the interVLAN forwarding rate significantly).

Troubleshoot the Cause

Troubleshoot Collision Domain Issues

So if your VLAN appears to be slow, first isolate the collision domain problems. You need to establish if only users on the same collision domain are experiencing connectivity problems, or if it is happening on multiple domains. To do this, make a data transfer between user PCs on the same collision domain, and compare this performance with the performance of another collision domain, or with its expected performance.

If problems only occur on that collision domain, and the performance of other collision domains in the same VLAN is normal, then look at the port counters on the switch to determine what troubles this segment may be experiencing. Most likely, the cause is simple, such as a duplex mismatch. Another, less frequent cause is an overloaded or oversubscribed segment. For more information on troubleshooting a single segment problem, refer to the document *Configuring and Troubleshooting Ethernet 10/100/1000Mb Half/Full Duplex Auto-Negotiation*.

If users on different collision domains (but in the same VLAN) are having the same performance issues, it still may be caused by a duplex mismatch on one or more Ethernet segments between the source and destination. The following scenario often happens: a switch is configured manually to have full-duplex on all ports in the VLAN (the default setting is "auto"), while users (network interface cards [NICs]) connected to the ports are performing an auto-negotiation procedure. This results in duplex mismatch on all ports and, therefore, bad performance on each port (collision domain). So, although it appears as if the whole VLAN (broadcast domain) is having a performance problem, it is still categorized as duplex mismatch, for the collision domain of each port.

Another case to be considered is a particular NIC performance problem. If a NIC with a performance problem is connected to a shared segment, then it may appear that a whole segment is experiencing slowness, especially if the NIC belongs to a server that also serves other segments or VLANs. Keep this case in mind because it may mislead you as you troubleshoot. Again, the best way to narrow down this issue is to perform a data transfer between two hosts on the same segment (where the NIC with the supposed problem is connected), or if only the NIC is on that port, isolation is not easy, so try a different NIC in this host, or try connecting the suspected host on a separate port, ensuring proper configuration of the port and NIC.

If the problem still exists, try troubleshooting the switch port. Refer to the document *Troubleshooting Switch Port and Interface Problems*.

The most severe case is when some or all of the incompatible NICs are connected to a Cisco switch. In this case, it appears that the switch is having performance issues. To check compatibility of the NICs with Cisco switches, refer to the document *Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues*.

You need to distinguish between the first two cases (troubleshooting collision domain slowness and VLAN slowness) because these two causes involve different domains. With collision domain slowness, the problem lies either outside the switch (or on the edge of the switch, on a switch port) or external to the switch. It may be that the segment alone has problems (for example, an oversubscribed segment, exceeding the segment length, physical problems on the segment, or hub/repeater problems). In the case of VLAN slowness, the problem most likely lies inside the switch (or multiple switches). If you diagnose the problem incorrectly, you may waste time looking for the problem in the wrong place.

So, after you have diagnosed a case, check the items listed below.

In the case of a shared segment:

- determine if the segment is overloaded or oversubscribed
- determine if the segment is healthy (including if the cable length is correct, if attenuation is within the norm, and if there are physical damages of the medium)
- determine if the network port and all NICs connected to a segment have compatible settings
- determine if the NIC is performing well (and running the latest driver)
- determine if the network port continues to show increasing errors
- determine if the network port is overloaded (especially if it is a server port)

In the case of a point-to-point shared segment, or collisionless (full-duplex) segment:

- determine the port and NIC-compatible configuration
- determine the health of the segment
- determine the health of the NIC
- look for network port errors or oversubscription

Troubleshoot Slow IntraVLAN (Broadcast Domain)

After verifying there are no duplex mismatch or collision domain issues as explained in the above section, you can now troubleshoot IntraVLAN slowness. The next step in isolating the location of the slowness is to perform a data transfer between hosts on the same VLAN (but on different ports; that is, on different collision domains), and compare the performance with the same tests in alternate VLANs.

The following may cause slow VLANs:

- traffic loop
- overloaded or oversubscribed VLAN
- congestion on the switch inband path
- switch management processor high CPU utilization
- ingress errors on a cut-through switch
- ¹ software or hardware misconfiguration
- ¹ software bugs
- ¹ hardware problems

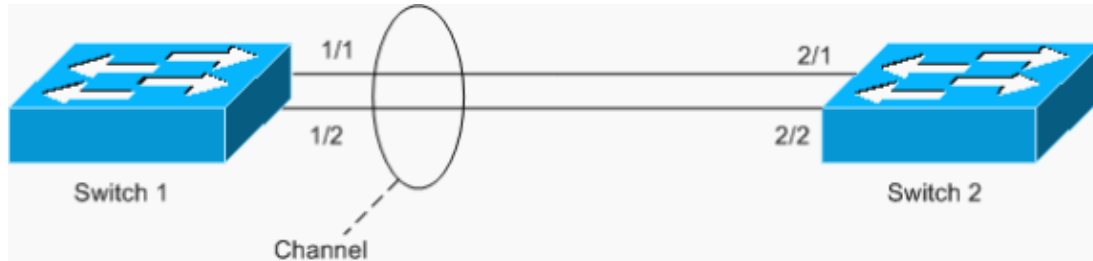
¹These three causes of slow intraVLAN connectivity are beyond the scope of this document, and may require troubleshooting by a Cisco Technical Support engineer. After ruling out the first five possible causes listed above, you may need to open a service request with Cisco Technical Support.

Traffic Loop

A traffic loop is the most common cause of a slow VLAN. Along with a loop, you should see other symptoms that indicate that you are experiencing a loop. For troubleshooting Spanning Tree Protocol (STP) loops, refer to the document Spanning Tree Protocol Problems and Related Design Considerations. Although powerful

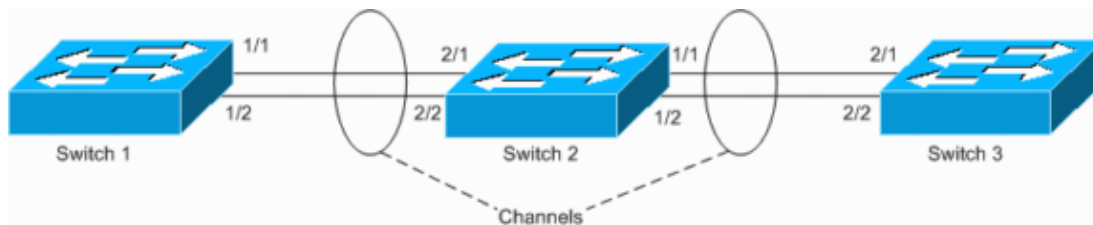
switches (like the Cisco Catalyst 6500/6000) with gigabit-capable backplanes can handle some (STP) loops without compromising the performance of the management CPU, looped packets can cause input buffers to overflow on NICs and receive/transmit (Rx/Tx) buffers on the switches, causing slow performance when connecting to other devices.

Another example of the loop is an asymmetrically configured EtherChannel, as shown in the following scenario:



In this example, ports 1/1 and 1/2 are in the channel, but ports 2/1 and 2/2 are not.

Switch 1 has a configured channel (forced channel), and Switch 2 has no channel configuration for the corresponding ports. If flooded traffic (mcast/bcast/unknown unicast) flows from Switch 1 toward Switch 2, Switch 2 loops it back into the channel. It is not a complete loop, since traffic is not looped continuously, but is only reflected once. It is one-half of the total loop. Having two such misconfigurations can create a complete loop, as shown in the example below.



The hazard of having such misconfiguration is that MAC addresses are learned on incorrect ports as traffic is incorrectly switched, which causes packet loss. Consider, for example, a router with active Hot Standby Router Protocol (HSRP) that is connected to Switch 1 (as shown in the diagram above). After the router broadcasts packets, its MAC is looped back by Switch 2 and learned off the channel by Switch 1, until a unicast packet is sent from the router again.

Overloaded or Oversubscribed VLAN

Notice if there are bottlenecks (oversubscribed segments) anywhere on your VLANs and locate them. The first sign that your VLAN is overloaded is if Rx or Tx buffers on a port are oversubscribed. If you see outdiscards or indiscards on some ports, check to see if those ports are overloaded. (An increase in indiscards does not only indicate a full Rx buffer.) In Catalyst OS (CatOS), useful commands to issue are **show mac mod/port** or **show top [N]**. In Cisco IOS® Software (Native), you can issue the **show interfaces slot#/port# counters errors** command to see discards. The overloaded or oversubscribed VLAN scenario and the traffic loop scenario often accompany each other, but they can also exist separately.

Most frequently, overload happens on the backbone ports when the aggregated bandwidth of the traffic is underestimated. The best way to work around this problem is to configure an EtherChannel between the devices for which the ports are bottlenecked. If the network segment is already a channel, add more ports into a channel group to increase the channel capacity.

Also be aware of the Cisco Express Forwarding (CEF) polarization issue. This problem happens on networks

in which traffic is load-balanced by routers, but due to the algorithm uniformity of Cisco Express Forwarding, all traffic is polarized and, on the next hop, it is not load-balanced. This problem does not occur often, however, because it requires a certain topology with load-balanced L3 links. For more information regarding Cisco Express Forwarding and load balancing, see *How-To Troubleshoot Unicast IP Routing CEF on Catalyst 6000s with a Supervisor 2 in Hybrid Mode*.

Another cause for the overloaded VLAN is an asymmetric routing problem. This type of configuration also can cause an excessively high amount of traffic flooding your VLANs. For more information, refer to the *Cause 1: Asymmetric Routing* section of the document *Unicast Flooding in Switched Campus Networks*.

Sometimes a bottleneck can be a network device itself. If you try, for example, to pump 4-gigabit traffic through the switch with a 3-gigabit backplane, you end up with a dramatic loss of the traffic. Understanding network switch architecture is out of the scope of this document; however, when considering the capacity of a network switch, pay attention to the following aspects:

- backplane capacity
- head-of-line blocking problems
- blocking and non-blocking switch/port architecture

Congestion on Switch Inband Path

Congestion on the switch inband path can result in a spanning tree loop or other types of instability on the network. The inband port on any Cisco switch is a virtual port that provides interface for management traffic (traffic such as Cisco Discovery Protocol and Port Aggregation Protocol [PAgP]) to the management processor. The inband port is considered virtual because, in some architectures, the user cannot see it, and the inband functions are combined with the normal port operation. For example, the SC0 interface on the Catalyst 4000, Catalyst 5000 and Catalyst 6500/6000 series switches (running CatOS) is a subset of the inband port. Interface SC0 provides only an IP stack for the management processor within the configured VLAN, while the inband port provides access to the management processor for bridge protocol data units (BPDUs) in any of the configured VLANs and for many other management protocols (such as Cisco Discovery Protocol, Internet Group Management Protocol [IGMP], Cisco Group Management Protocol, and Dynamic Trunking Protocol [DTP]).

If the inband port gets overloaded (due to a misconfigured application or user traffic), it may result in instability of any protocols for which the protocol state stability is based on regular messages or "hellos" received. This state can result in temporary loops, interfaces flapping, and other issues, causing this type of slowness.

It is difficult to cause congestion of the inband port on the switch, though maliciously formed denial of service (DoS) attacks may succeed. There is no way to rate-limit or reduce traffic on the inband port. A solution requires switch administrator intervention and investigation. Inband ports generally have a high tolerance for congestion. Rarely does the inband port malfunction or get stuck in the Rx or Tx direction. This would mean severe hardware outage and would affect the whole switch. This condition is difficult to recognize and is usually diagnosed by Cisco Technical Support engineers. The symptoms are that a switch suddenly becomes "deaf" and stops seeing control traffic such as Cisco Discovery Protocol neighbor updates. This indicates an Rx inband problem. (If, however, just one Cisco Discovery Protocol neighbor is seen, you can be confident that inband is working.) Correspondingly, if all the connected switches lose Cisco Discovery Protocol from a single switch (as well as all other management protocols), it indicates Tx problems from the inband interface of that switch.

Switch Management Processor High CPU Utilization

If an inband path is overloaded, it can cause a switch to experience high CPU conditions; and, as the CPU processes all that unnecessary traffic, the situation worsens. If high CPU utilization is caused by an

overloaded inband path or an alternate issue, it can affect management protocols as described in the Congestion on Switch Inband Path section, above.

In general, consider the management CPU to be a vulnerable point of any switch. A correctly configured switch reduces the risk of problems caused by high CPU utilization.

The architecture of the Supervisor Engine I and II of the Catalyst 4000 series switches is designed such that the management CPU is involved in the switching overhead. Keep in mind the following:

- CPU programs a switch fabric whenever a new path (the Supervisor Engine I and II are path-based) enters the switch. If an inband port is overloaded, it causes any new path to be dropped. This results in packet lost (silent discard) and slowness in higher-layer protocols when traffic is switched between ports. (Refer to the section Congestion on Switch Inband Path, above.)
- Since the CPU partially performs switching in the Supervisor Engine I and II, high CPU conditions can affect the switching capabilities of the Catalyst 4000. High CPU utilization on the Supervisor Engine I and II may be caused by the switching overhead itself.

Supervisor Engines II+, III and IV of the Catalyst 4500/4000 series are fairly traffic-tolerant, but MAC address learning in the Cisco IOS Software-based Supervisor Engine is still done completely in software (by the management CPU); there is a chance that high CPU utilization can affect this process and cause slowness. As with Supervisor Engine I and II, massive MAC address learning or relearning can cause high CPU utilization on Supervisor Engines II+, III and IV.

The CPU is involved in MAC learning in the Catalyst 3500XL and 2900XL series switches as well, so a process that results in fast address relearning affects CPU performance.

Also, the MAC address learning process (even if it is completely implemented in hardware) is a relatively slow process, compared to a switching process. If there is a continuously high rate of MAC address relearning, then the cause must be found and eliminated. A spanning tree loop on the network can cause this type of MAC address relearning. MAC address relearning (or MAC address flapping) may also be caused by third-party switches that implement port-based VLANs, which means that MAC addresses are not getting associated with a VLAN tag. This kind of switch, when connected to Cisco switches in certain configurations, may result in MAC leaking between VLANs. In turn, this may lead to a high rate of MAC address relearning and may degrade performance.

Ingress Errors on a Cut-Through Switch

Cut-through ingress error packet propagation is related to Slow Collision Domain Connectivity, but because the error packets are transferred to another segment, the problem appears to be switching between segments. Cut-through switches (such as the Catalyst 8500 series Campus Switch Routers (CSRs) and the Catalyst 2948G-L3 or L3 switching module for the Catalyst 4000 series) begin packet/frame switching as soon as the switch has enough information from reading the L2/L3 header of the packet to forward the packet to its destination port or ports. So, while the packet is being switched between ingress and egress ports, the beginning of the packet is already forwarded out of the egress port, while the rest of the packet is still being received by the ingress port. What happens if the ingress segment is not healthy and generates a cyclic redundancy check (CRC) error or a runt? The switch recognizes this only when it receives the end of the frame and, by that time, most of the frame is transferred out of the egress port. Since it makes no sense to transfer the rest of the erroneous frame, the rest is dropped, the egress port increments the "underrun" error, and the ingress port increments the corresponding error counter. If multiple ingress ports are unhealthy and their server resides on the egress port, it appears that the server segment is having the problem, even though it is not.

For cut-through L3 switches, watch for underruns and, when you see them, check all ingress ports for errors.

Software or Hardware Misconfiguration

Misconfiguration may cause a VLAN to be slow. These negative effects may result from a VLAN being oversubscribed or overloaded, but most often, they result from a bad design or overlooked configurations. For example, a segment (VLAN) can be easily overwhelmed by multicast traffic (for example, video or audio stream) if multicast traffic constraining techniques are not properly configured on that VLAN. Such multicast traffic may affect data transfer, causing packet loss on an entire VLAN for all the users (and flooding the segments of users who did not intend to receive the multicast streams).

Software Bugs and Hardware Problems

Software bugs and hardware problems are difficult to identify because they cause deviation, which is hard to troubleshoot. If you believe that the problem is caused by a software bug or hardware problem, contact the Cisco Technical Support engineers to have them investigate the problem.

Troubleshoot Slow InterVLAN Connectivity

Before troubleshooting slow interVLAN connectivity (between VLANs), investigate and rule out the issues discussed in the Troubleshoot Collision Domain Issues and Troubleshoot Slow IntraVLAN (Broadcast Domain) sections of this document.

Most of the time, slow interVLAN connectivity is caused by user misconfiguration. For example, if you incorrectly configured MLS or Multicast Multilayer Switching (MMLS), then packet forwarding is done by the router CPU, which is a slow path. To avoid misconfiguration and to troubleshoot efficiently when necessary, you should understand the mechanism used by your L3 forwarding device. In most cases, the L3 forwarding mechanism is based on a compilation of routing and Address Resolution Protocol (ARP) tables and programming extracted packet forwarding information into hardware (shortcuts). Any failure in the process of programming shortcuts leads to either software packet forwarding (a slow path), misforwarding (forwarding to a wrong port), or traffic black holing.

Usually a shortcut-programming failure or the creation of incomplete shortcuts (which can also lead to software packet forwarding, misforwarding, or traffic black holing) is the result of a software bug. If you suspect this to be case, have the Cisco Technical Support engineers investigate it. Other reasons for slow interVLAN forwarding include hardware malfunctions, however these causes are out of the scope of this document. Hardware malfunctions simply prevent successful shortcut creation in hardware and, therefore, traffic may either take a slow (software) path or may be black holed. Hardware malfunctions should be handled by Cisco Technical Support engineers, as well.

If you are sure that the equipment is properly configured, but hardware switching is not taking place, then a software bug or hardware malfunction may be the cause. However, be aware of device capabilities before forming this conclusion.

The following are the two most frequent situations in when hardware forwarding may cease or not take place at all:

- The memory which stores shortcuts is exhausted. Once the memory is full, the software usually ceases further shortcut creation. (For example, MLS, whether NetFlow or Cisco Express Forwarding-based, becomes inactive once there is no room for new shortcuts, and it switches to software [slow path].)
- Equipment is not designed to perform hardware switching, but it is not obvious. For example, Catalyst 4000 series Supervisor Engines III and later are designed to hardware-forward only IP traffic; all other types of traffic are software processed by the CPU. Another example is the configuration of an access control list (ACL) that requires CPU intervention (for example, with the "log" option). The traffic that applies to this rule is processed by the CPU in software.

Ingress errors on a cut-through switch can also contribute to interVLAN routing slowness. Cut-through switches use the same architectural principles to forward L3 and L2 traffic, so the troubleshooting methods provided in the section Troubleshoot Slow IntraVLAN (Broadcast Domain), above, can be applied to L2 traffic, as well..

Another type of misconfiguration that affects interVLAN routing is misconfiguration on the end-user devices (such as the PC and printers). A common situation is a misconfigured PC; for example, a default gateway is misconfigured, the PC ARP table is invalid, or the IGMP client malfunctioned. A common case is when there are multiple routers or routing-capable devices, and some or all of the end-user PCs are misconfigured to use the wrong default gateway. This may be the most troublesome case, as all of the network devices are configured and working properly, however, the end-user devices do not use them because of this misconfiguration.

If a device in the network is a regular router that does not have any type of hardware acceleration (and does not participate in NetFlow MLS), then the rate of traffic forwarding depends completely on the speed of the CPU and how busy it is. High CPU utilization definitely affects the forwarding rate. On L3 switches, however, high CPU conditions do not necessarily affect the forwarding rate; high CPU utilization affects the ability of the CPU to create (program) a hardware shortcut. If the shortcut is already installed into the hardware, then even if the CPU is highly utilized, the traffic (for the programmed shortcut) is switched in hardware until the shortcut is aged out (if there is an expiration timer) or removed by the CPU. However, if a router is configured for any type of software acceleration (such as fast switching or Cisco Express Forwarding switching), then packet forwarding may be affected by software shortcuts; if a shortcut is broken, or the mechanism itself is failing, then instead of the forwarding rate being accelerated, traffic is punted to the CPU, slowing the data forwarding rate down.

Related Information

- [Troubleshooting IP MultiLayer Switching](#)
- [How-To Troubleshoot Unicast IP Routing CEF on Catalyst 6000s with a Supervisor 2 in Hybrid Mode](#)
- [Configuring Inter-VLAN Routing with Catalyst 3550 Series Switches](#)
- [LAN Product Support Pages](#)
- [LAN Switching Support Page](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 16, 2007

Document ID: 23637
