Switching Paths Overview

This chapter describes switching paths that can be configured on Cisco IOS devices. It provides an overview of switching methods. It also provides an overview of NetFlow. For specific configuration information, refer to the chapter "Configuring Switching Paths."

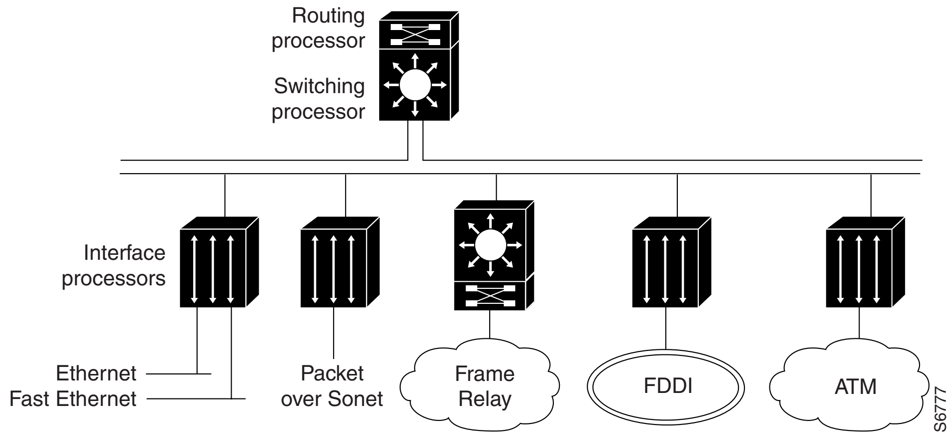
Overview of Basic Router Platform Architecture and Processes

To understand how switching works, it helps to first understand the basic router architecture and where various processes occur in the router.

Fast switching is enabled by default on all interfaces that support fast switching. If you have a situation where you need to disable fast switching and fall back to the process-switching path, understanding how various processes affect the router and where they occur will help you determine your alternatives. This understanding is especially helpful when you are troubleshooting traffic problems or need to process packets that require special handling. Some diagnostic or control resources are not compatible with fast switching or come at the expense of processing and switching efficiency. Understanding the effects of those resources can help you minimize their effect on network performance.

Figure 2 illustrates a possible internal configuration of a Cisco 7500 series router. In this configuration, the Cisco 7500 series router has an integrated Route/Switch Processor (RSP) and uses *route caching* to forward packets. The Cisco 7500 series router also uses Versatile Interface Processors (VIPs), a RISC-based interface processor that receives and caches routing information from the RSP. The VIP card uses the route cache to make switching decisions locally, which relieves the RSP of involvement and speeds overall throughput. This type of switching is called *distributed switching*. Multiple VIP cards can be installed in one router.

Figure 2 Basic Router Architecture



Cisco Routing and Switching Processes

The routing, or forwarding, function comprises two interrelated processes to move information in the network:

- Making a routing decision by routing
- Moving packets to the next-hop destination by switching

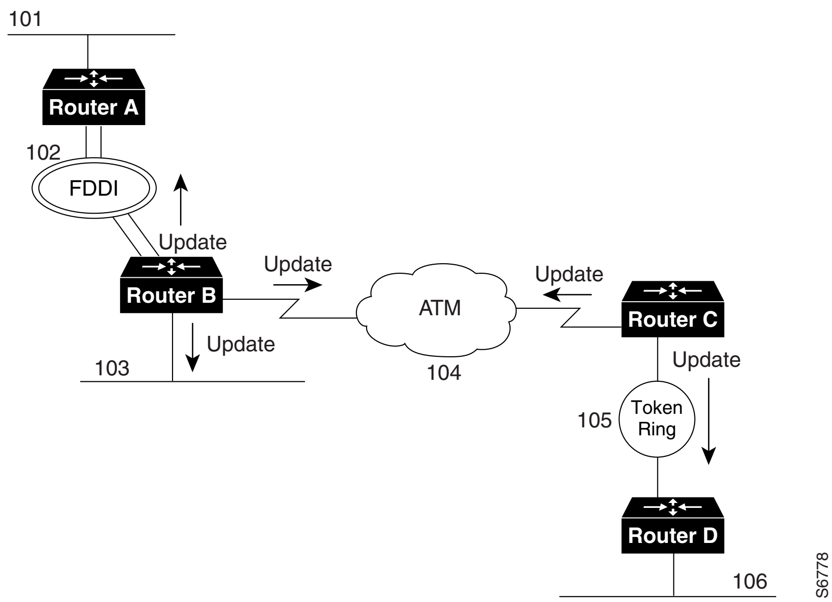
Cisco IOS platforms perform both routing and switching, and there are several types of each.

Routing

The routing process assesses the source and destination of traffic based on knowledge of network conditions. Routing functions identify the best path to use for moving the traffic to the destination out one or more of the router interfaces. The routing decision is based upon a variation of criteria such as link speed, topological distance, and protocol. Each separate protocol maintains its own routing information.

Routing is more processing intensive and has higher latency than switching as it determines path and next-hop considerations. The first packet routed requires a lookup in the routing table to determine the route. The route cache is populated after the first packet is routed by the route-table lookup. Subsequent traffic for the same destination is switched using the routing information stored in the route cache. Figure 3 illustrates the basic routing process.

Figure 3 The Routing Process

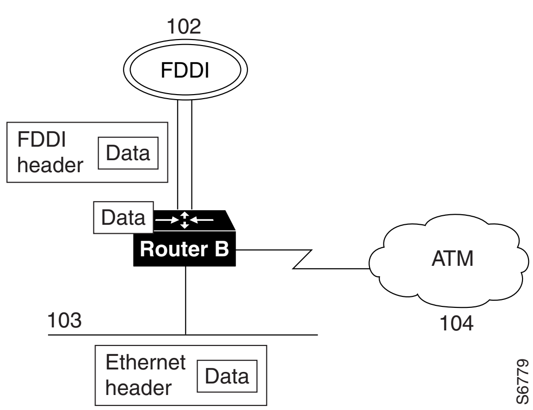


A router sends routing updates out each of its interfaces that are configured for a particular protocol. It also receives routing updates from other attached routers. From these received updates and its knowledge of attached networks, it builds a map of the network topology.

Switching

Through the switching process, the router determines the next hop toward the destination address. Switching moves traffic from an input interface to one or more output interfaces. Switching is optimized and has lower latency than routing because it can move packets, frames, or cells from buffer to buffer with simpler determination of the source and destination of the traffic. It saves resources because it does not involve extra lookups. Figure 4 illustrates the basic switching process.

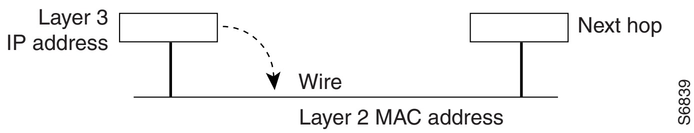
Figure 4 The Switching Process



In Figure 4, packets are received on the Fast Ethernet interface and destined for the FDDI interface. Based on information in the packet header and destination information stored in the routing table, the router determines the destination interface. It looks in the protocol's routing table to discover the destination interface that services the destination address of the packet.

The destination address is stored in tables such as ARP tables for IP and AARP table for AppleTalk. If there is no entry for the destination, the router will either drop the packet (and inform the user if the protocol provides that feature), or it must discover the destination address by some other address resolution process, such as through he ARP protocol. Layer 3 IP addressing information is mapped to the Layer 2 MAC address for the next hop. Figure 5 illustrates the mapping that occurs to determine the next hop.

Figure 5 Layer 3-to-Layer 2 Mapping



Basic Switching Paths

Basic switching paths are

- Process Switching
- Fast Switching
- Distributed Switching
- NetFlow

Process Switching

In process switching the first packet is copied to the system buffer. The router look up the Layer 3 network address in the routing table and initializes the fast-switch cache. The frame is rewritten with the destination address and sent to the exit interface that services that destination. Subsequent packets for that destination are sent by the same switching path. The route processor computes the cyclical redundancy check (CRC).

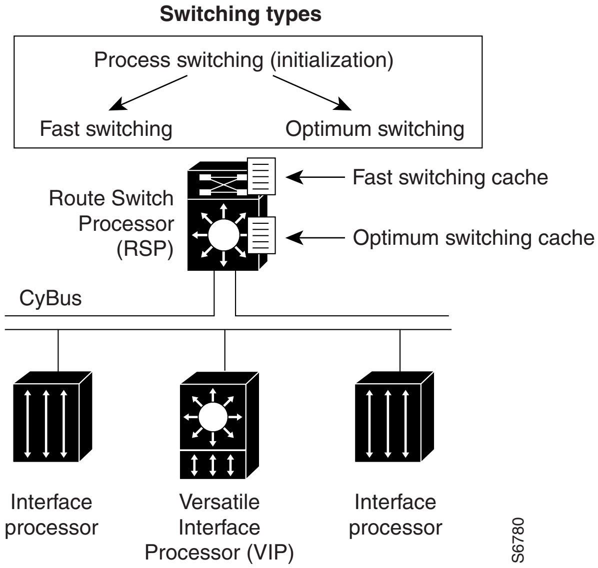
Fast Switching

When packets are fast switched, the first packet is copied to packet memory and the destination network or host is found in the fast-switching cache. The frame is rewritten and sent to the exit interface that services the destination. Subsequent packets for the same destination use the same switching path. The interface processor computes the CRC.

Distributed Switching

Switching becomes more efficient the closer to the interface the function occurs. In distributed switching, the switching process occurs on VIP and other interface cards that support switching. For model numbers and hardware compatibility information, refer to the *Cisco Product Catalog*. Figure 6 illustrates the distributed switching process on the Cisco 7500 series.

Figure 6 Distributed Switching on Cisco 7500 Series Routers



The VIP card installed in this router maintains a copy of the routing cache information needed to forward packets. Because the VIP card has the routing information it needs, it performs the switching locally, making the packet forwarding much faster. Router throughput is increased linearly based on the number of VIP cards installed in the router.

NetFlow

While in more recent IOS releases it is not a switching path, NetFlow enables you to collect the data required for flexible and detailed accounting, billing, and chargeback for network and application resource utilization. Accounting data can be collected for both dedicated line and dial-access accounting. NetFlow is supported over switched LAN or ATM backbones, allowing scalable inter-VLAN forwarding. NetFlow can be deployed at any location in the network. NetFlow is available on the Cisco 7200 Series and the Cisco 7500 Series.

NetFlow is configurable on a per-interface basis. You configure NetFlow using the *protocol* **route-cache flow** command.

NetFlow is described in "Configuring NetFlow" later in this publication.

Platform and Switching Path Correlation

Depending on the routing platform you are using, availability and default implementations of switching paths varies. Table 3 shows the correlation between Cisco IOS switching paths and routing platforms.

Table 3 Switching Paths on RSP-Based Routers

Switching Path	Cisco 7200	Cisco 7500	Comments	Configuration Command
Process switching	Yes	Yes	Initializes switching caches	**no** *protocol* **route-cache**
Fast switching	Yes	Yes	Default (except for IP)	*protocol* **route-cache**
Distributed switching	No	Yes	Using Second-Generation VIP line cards	*protocol* **route-cache distributed**

Features that Affect Performance

Performance is derived from the switching mechanism you are using. Some Cisco IOS features require special handling and cannot be switched until the additional processing they require has been performed. This special handling is not processing that the interface processors can do. Because these features require additional processing, they affect switching performance. These features include

- Queuing
- Random Early Detection
- Compression
- Filtering (using access lists)
- Encryption
- Accounting

Queuing

Queuing occurs when network congestion occurs. When traffic is moving well within the network, packets are sent as they arrive at the interface. Cisco IOS software implements four different queuing algorithms:

- Firs In, First Out (FIFO) Queuing – Packets are forwarded in the same order in which they arrive at the interface.
- Priority Queuing – Packets are forwarded based on an assigned priority. You can create priority lists and groups to define rules for assigning packets to priority queues.
- Custom Queuing – You can control a percentage of interface bandwidth for specified traffic by creating protocol queue lists and custom queue lists.
- Weighted Fair Queuing – Weighted Fair Queuing provides automatic traffic priority management. Low-bandwidth sessions have priority over high-bandwidth sessions and high-bandwidth session are assigned weights. Weighted Fair Queuing is the default for interfaces slower than 2.048 Mbps.

Random Early Detection

Random Early Detection is designed for congestion avoidance. Traffic is prioritized based on type of service (ToS), or precedence. This feature is available on T3, OC-3, and ATM interfaces.

Compression

Depending on the protocol you are using, various compression options are available in Cisco IOS software. Refer to the Cisco IOS configuration guide for the protocol you are using to see what compression options you have.

Filtering

You can define access lists to control access to or from a router for a number of services. You could, for example, define an access lists to prevent packets with a certain IP address from leaving a particular interface on a router. How access lists are used depends on the protocol. For information on access lists, refer to the appropriate Cisco IOS configuration guide for the protocol you are using.

Encryption

Encryption algorithms are applied to data to alter its appearance making it incomprehensible to those who are not authorized to see the data. For information about encryption features available with the Cisco IOS software, refer to the *Security Configuration Guide*.

Accounting

You can configure accounting features to collect network data related to resource usage. The information you collect (in the form of statistics) can be used for billing, chargeback, and planning resource usage. Refer to the appropriate Cisco IOS configuration guide for the protocol you are using for information regarding accounting features you can use.