

# *White Paper* **The Architecture and Design Guide for the FlexWAN Module for the Cisco 7600 Series and Cisco Catalyst 6000 Series**

## **Overview**

The FlexWAN module adds to the already wide breadth of WAN and metropolitan-area network (MAN) interfaces and capabilities provided on the Optical Services Modules for the Cisco 7600 Series Router and the Cisco Catalyst® 6000 Series switches. The FlexWAN module is designed to enable the use of Cisco 7200 and 7500 series single-wide port adapters ranging from fractional T1 or E1 to 155 Mbps while providing the same distributed services available on Cisco 7500 Series versatile interface processors (VIPs). This paper discusses the packet switching and services architecture in a FlexWAN module-equipped system. Figure 1 shows a picture of the FlexWAN module.

**Figure 1: FlexWAN Module**





## Software Requirements

The FlexWAN module requires a supervisor engine with both multilayer switch and policy feature cards (MSFCs and PFCs). Software for the FlexWAN module comes in two types: “native” and “hybrid” modes. Although both modes are robust and full featured, native is preferred because most software and new feature development occurs in this mode. A brief description of the two modes follows.

Native refers to Cisco IOS Software running on both the PFC and MSFC. The Cisco IOS image name must contain a “v,” such as *c6sup22-jsv-mz*. The “v” is the same paradigm used for the Cisco 7500 Series routers and denotes distributed processing on the VIP modules. The minimum software version for native mode is Release 12.1(8)E.

Hybrid refers to running two separate operating systems on the supervisor engine: the Cisco Catalyst Operating System (CatOS) on the PFC and Cisco IOS Software on the MSFC. In a hybrid configuration, a minimum of CatOS Version 5.4(1) is required on the PFC, and Cisco IOS 12.1(1)E is required on the MSFC. The same Cisco IOS image-naming convention exists in this mode, with image names similar to *c6msfc-jsv-mz*. The FlexWAN module is also supported with Supervisor Engine 2 coupled with the MSFC2. Minimum software requirements for this configuration are CatOS 6.1(1) on the PFC and Cisco IOS 12.1(3a)E on the MSFC.

The FlexWAN module is configured completely from the MSFC. The interfaces appear in a way similar to the way they appear in a Cisco 7500 Series with VIP modules. For example, if you have a FlexWAN module in slot 3 and packet-over-SONET port adapters in bay 0 and bay 1, then the interfaces appear on the MSFC as *interface POS 3/0/0* and *interface POS 3/1/0*.

## Interface Support

The FlexWAN module is hot swappable, but the port adapters installed in the module are not. Screws are used when installing the port adapters to seat them correctly and to prevent accidental removal. All Cisco 7600 and Cisco Catalyst 6000 chassis slots can be populated with FlexWAN modules.

Port adapters supported in the FlexWAN module are listed in Table 1 (for the latest port adapter support, refer to the FlexWAN data sheet, available at [www.cisco.com](http://www.cisco.com)).



**Table 1: Supported Cisco 7200 and 7500 Series WAN Port Adapters**

<b>T1 or E1</b>	<b>T3 or E3</b>	<b>HSSI</b>	<b>ATM</b>	<b>Packet over SONET</b>
PA-4T+	PA-T3	PA-H	PA-8T1IMA	PA-POS-OC3MM
PA-8T-V35	PA-T3+	PA-2H	PA-8E1IMA	PA-POS-OC3SMI
PA-8T-232	PA-E3		PA-A3-T3	PA-POS-OC3SML
PA-8T-X21	PA-2T3		PA-A3-E3	
PA-MC-2T1	PA-2T3+		PA-A3-OC3MM	
PA-MC-4T1	PA-2E3		PA-A3-OC3SMI	
PA-MC-8T1	PA-MC-T3		PA-A3-OC3SML	
PA-MC-8E1/120	PA-MC-E3			
PA-MC-8TE1+	PA-MC-2T3+			

### **Interface Limitations**

The FlexWAN module does not support any LAN interface or dual-wide port adapters. Each port adapter is managed by its own CPU, preventing the double-wide port adapters (part numbers PA-A2-4T1-xxxx and PA-SRP-OC12xx) from being used. The Cisco 7500 Series utilizes a single CPU to manage the two PCI buses on the VIP, whereas the FlexWAN module utilizes a CPU per PCI bus. The following port adapters not supported by FlexWAN:

### **Unsupported Cisco 7200/7500 Series Port Adapters:**

- Ethernet, Fast Ethernet and Gigabit Ethernet
- Token Ring
- Fiber Distributed Data Interface (FDDI)
- Channel Port Adapter
- Encryption Service Module
- Compression Service Module
- Double-wide port adapters (OC-12 DPT)



## Table of Contents

Overview .....	1
Contents .....	3
Network Design with the FlexWAN Module.....	4
FlexWAN Architecture .....	7
Ingress Packet Processing.....	9
Egress Packet Processing .....	9
QoS Processing .....	11
ACL Processing.....	13
High Availability and the FlexWAN Module.....	13
Configuration Synchronization between MSFCs .....	14
Features Not Supported on the FlexWAN Module.....	14
Configuring and Monitoring the FlexWAN Module .....	15

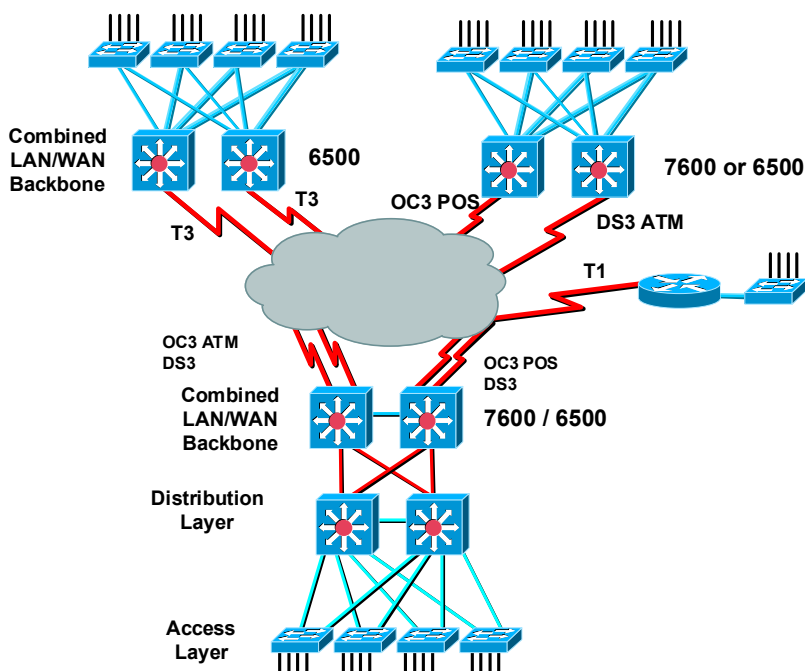


## Network Design with the FlexWAN Module

The FlexWAN module for the Cisco 7600 Series Router and the Cisco Catalyst 6000 Series of switches allows for the integration of WAN and MAN access with LAN switching, simplifying network design and consolidating the network infrastructure. The result is fewer network elements to manage in the total solution. The FlexWAN module is designed to deliver WAN access and sophisticated quality-of-service (QoS) features such as Class-Based Weighted Fair Queuing (CBWFQ), low-latency queuing (LLQ), and Weighted Random Early Detection (WRED). It delivers a broad range of WAN media options by using existing Cisco 7000 Series port adapters. The module expands the high-speed interfaces on the Cisco 7600 and allows the Cisco Catalyst 6000 Series to function as an external WAN router.

With new network deployments, the FlexWAN module can be used to converge LAN, MAN, and WAN connections from other campuses. Cisco 7600 Series routers or Cisco Catalyst 6000 Series switches acting as the core or distribution elements with FlexWAN modules can terminate connections from other campuses in the MAN and WAN. The central Cisco 7600 Series or Cisco Catalyst 6000 Series switches in Figure 2 use serial DS3 and ATM DS3 and OC-3 packet over SONET to terminate remote sites.

**Figure 2: WAN Network Utilizing FlexWAN Module**

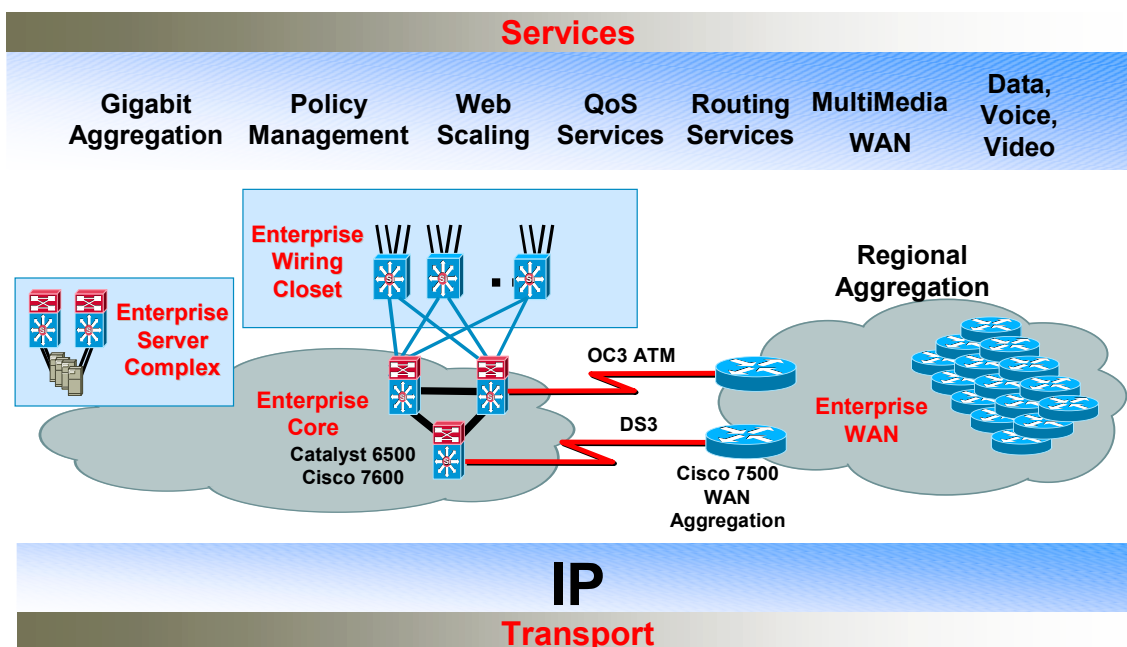




The FlexWAN module allows the Cisco 7600 Series and Cisco Catalyst 6000 Series to be used as an aggregator for higher-speed remote WAN links. The architecture can support up to 16 OC-3 ATM or Packet-over-SONET port adapters in a 9-slot chassis or 24 in a 13-slot chassis. The extensive capacity of the backplane and processing engine makes it a valuable option in terminating high-speed MAN and WAN connections. The number of virtual interfaces and IP routing neighbors supported is discussed in the “Configuring and Monitoring the FlexWAN Module” section.

A system configured with the FlexWAN module can perform many of the functions normally performed by the Cisco 7200 and 7500 series. However, there are some functions it cannot perform, including ISDN termination, encryption, and Layer 2 Tunneling Protocol (L2TP) tunneling. The FlexWAN module is ideal for terminating DS1 to OC-3 speed links, which require sophisticated QoS functionality.

**Figure 3 The FlexWAN module depicted in an Enterprise network model.**



The optimal places to utilize the FlexWAN module are in the enterprise core connecting to the WAN edge, and MAN sites that require DS3 to OC-3 connectivity, as illustrated in Figure 3. The FlexWAN module in the core Cisco 7600 Series or Cisco Catalyst 6000 Series is connected to a pair of Cisco 7500 Series routers doing WAN aggregation at a regional location for remote sites. The Cisco Catalyst 6000 Series can also be used as the distribution layer in the campus network to connect wiring closet switches to the enterprise core.

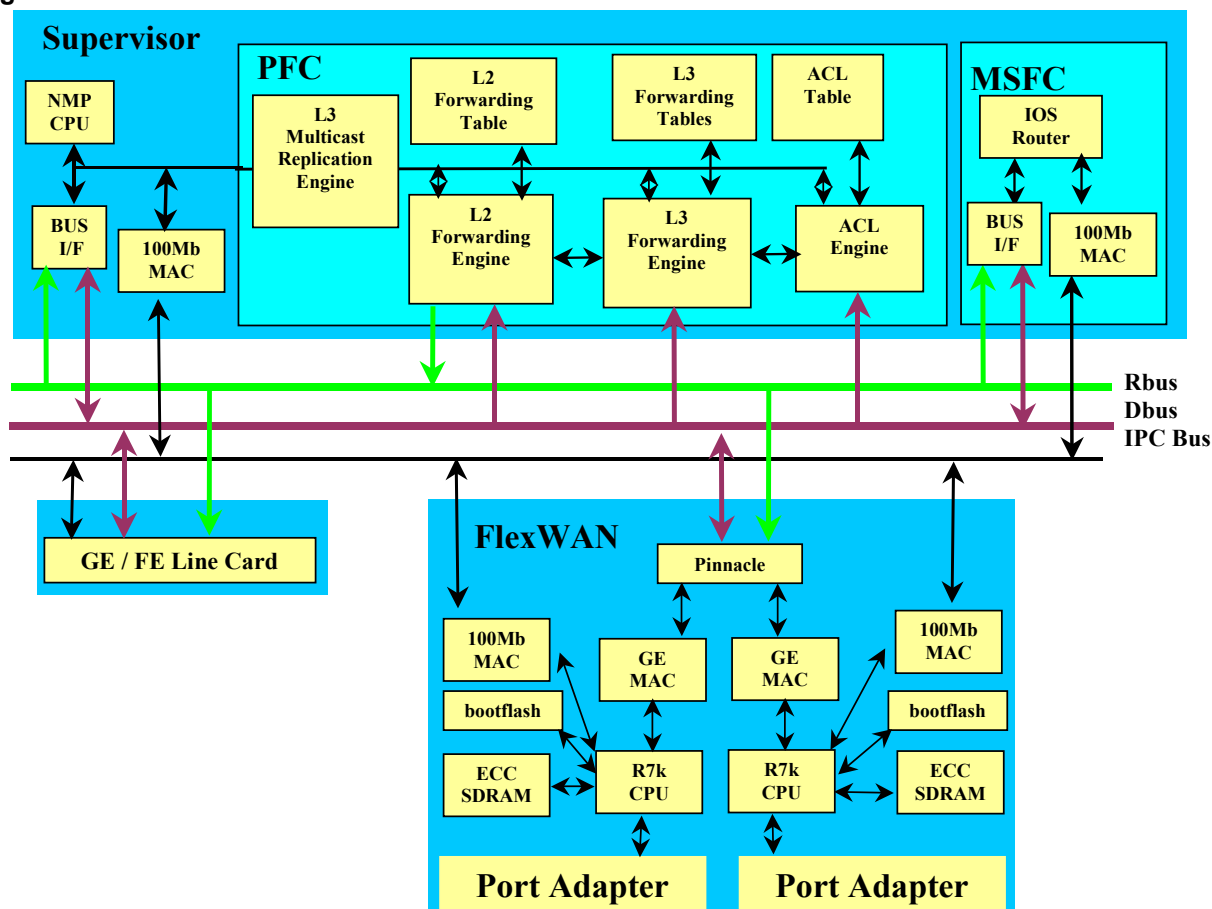


## FlexWAN Architecture

The FlexWAN module supports two modular port adapters. Each port adapter has a dedicated millions-of-instructions-per-second (MIPS) RM7000 RISC CPU and 64 or 128 MB of Error-Correcting Code (ECC) synchronous dynamic random access memory (SDRAM) to handle packet encapsulation, de-encapsulation, and QoS services to and from the WAN via the backplane. The interface of the CPU to the backplane is a Pinnacle application-specific integrated circuit (ASIC). This setup is illustrated in Figure 4. The MSFC treats each CPU as a separate entity and communicates with each via the IPC bus. (Note that all references to MSFC or PFC apply equally to the MSFC1 or PFC1, MSFC2 or PFC1, or MSFC2 or PFC2; the IPC bus is also referred to as the Ethernet out-of-band channel [EOBC]). All data and routing control traffic traverses the data bus, but only system control information between the MSFC and the FlexWAN module traverses the IPC bus.

**Note:** The FlexWAN module does not perform local switching. All packet switching is handled by either the centralized PFC or MSFC.

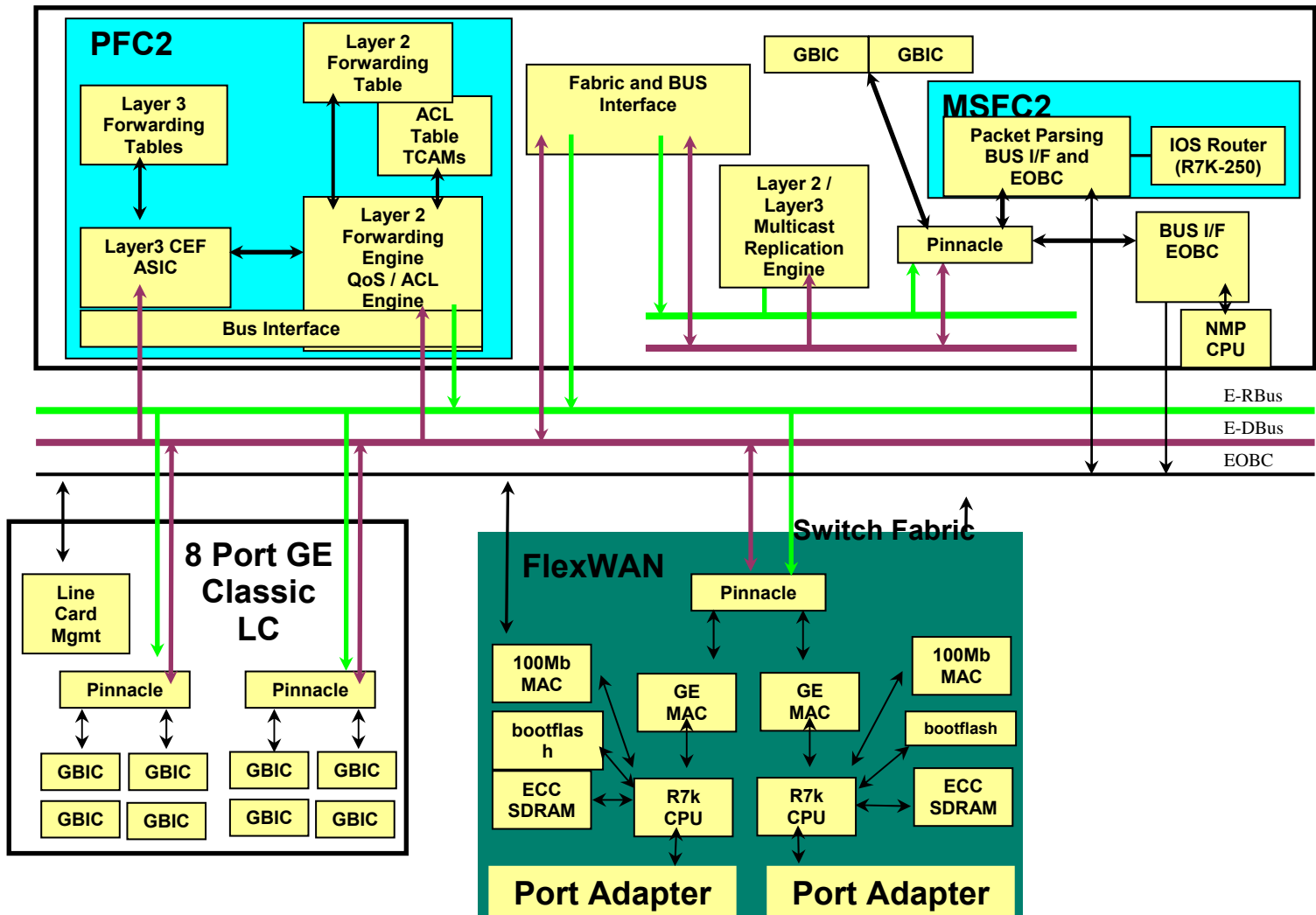
**Figure 4: Cisco 7600 Series and Cisco Catalyst 6000 Series MSFC and PFC1 and FlexWAN Block Diagram**



The Supervisor Engine and bus on the Cisco 7600 and Cisco Catalyst 6000 use an Ethernet frame format. To take advantage of the Supervisor-based hardware switching engines for IP Unicast and multicast, the FlexWAN module transmits and receives Ethernet frames to the bus (refer to Figure 5).

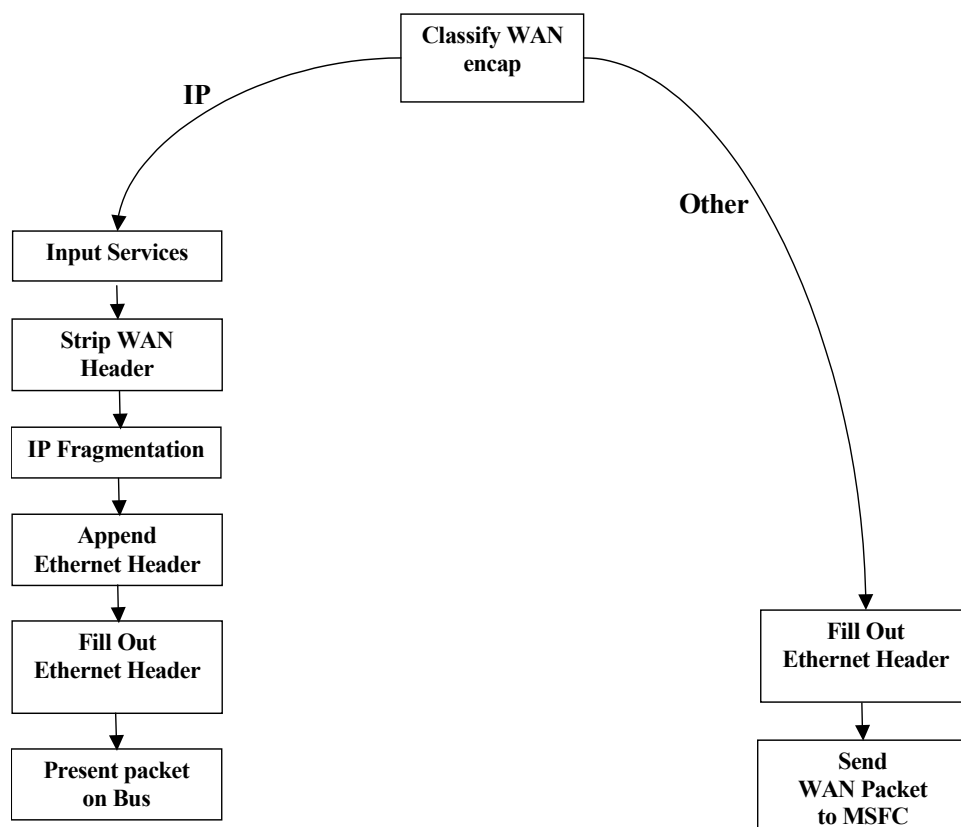


Figure 5: Block Diagram of Supervisor Engine 2 with the MSFC2



To use the hardware forwarding engines on the PFC, each physical interface and logical sub-interface is assigned a “hidden VLAN ID.” These virtual LAN (VLAN) IDs are used to transfer traffic from the FlexWAN card to the MSFC and PFC. Hidden VLAN IDs are created for each physical or logical sub-interface on the FlexWAN module; therefore, every physical and logical sub-interface has a VLAN ID associated with it. These VLAN IDs do not come out of the range of VLANs typically used (below 1000), but start at VLAN 1024. If an 802.1q VLAN ID in the range of the hidden VLANs has already been used, then that particular VLAN ID is not used as a hidden VLAN. If a VLAN in the hidden VLAN range is configured for an 802.1q VLAN, then the existing hidden VLAN ID is moved to a new hidden VLAN. Each time an interface is administratively shut down, the hidden VLAN allocated to that interface is de-allocated. When the interface is administratively brought up again, it is allocated a hidden VLAN ID, which may not be the same hidden VLAN ID that was previously assigned. The system hardware can support 4096 VLANs. Each hidden VLAN is treated as a logical point-to-point connection. Therefore, FlexWAN interfaces can be associated with only one MSFC at a time.

Figure 6: FlexWAN Ingress Packet Handling



## Ingress Packet Processing

The FlexWAN module handles input and output features for the WAN interfaces, and the MSFC and PFC perform the packet-switching task. The FlexWAN module can take advantage of the hardware forwarding shortcuts of the PFC for IP Unicast and multicast. Figure 6 illustrates the functions performed by the FlexWAN module for inbound packets.

Inbound WAN packets are initially classified into one of two types for further processing by the FlexWAN module. The simplest case is for packets that are not IP, ranging from AppleTalk to ATM signaling packets. These have their header on the data bus filled out, so they are sent to the MSFC to be handled.

IP traffic is initially sent through input services, for example, policing and Multilink PPP (MLPPP). The WAN header is then stripped from the packet, and if the packet is larger than 1500 bytes, IP fragmentation takes place. The system bus can handle Ethernet Jumbo frames up to 9000 bytes in size, but if the packet is to be switched by the PFC directly to a standard Ethernet port it is dropped because it is too large. An Ethernet header is then appended to the frame, and the DBUS header is filled out with the appropriate hidden VLAN information.

## Egress Packet Processing

When the FlexWAN module receives a packet from the system bus, it first checks the frame type to determine what processing it needs to do. If the packet is already a WAN packet from the MSFC, the FlexWAN module determines the destination by looking at the VLAN ID to determine the egress interface. The MSFC for non-IP



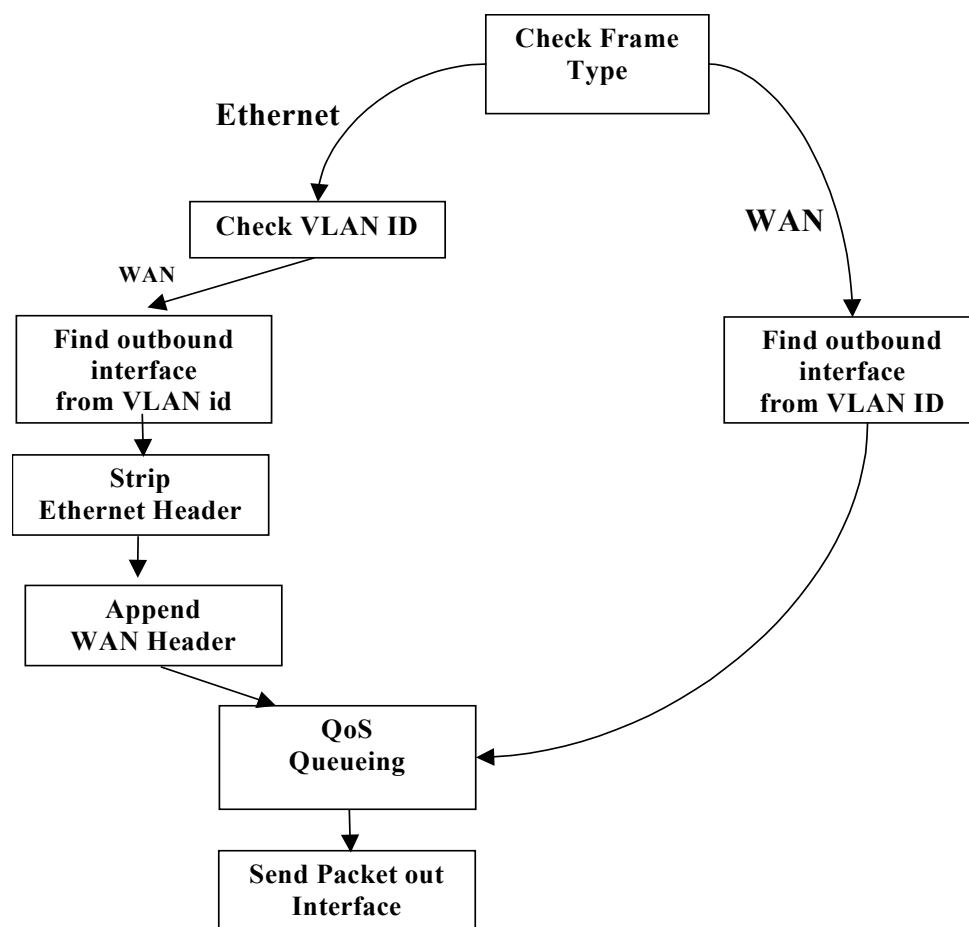
frames builds the WAN encapsulation itself, and then places the resulting frame inside an Ethernet frame to be delivered to the FlexWAN module.

If the packet received is an IP Ethernet packet, the VLAN ID is checked to determine if the frame is an IP packet that has been routed. If it is an IP packet, the Ethernet header is stripped and the WAN header is appended.

All packets are then sent to the QoS routines. When completed, the packet is placed on the interface transmit buffer ring to be sent out. Figure 7 illustrates the egress packet processing done on the FlexWAN module.



Figure 7: FlexWAN Egress Packet Handling



### QoS Processing

The FlexWAN module performs all QoS processing for WAN packets, and provides a rich set of QoS features. The QoS features that FlexWAN implements originate from the Cisco 7500 Series distributed switching path. The PFC card implements policing between ports in the Cisco 7600 and Cisco Catalyst 6000, but with the FlexWAN module this feature is disabled for WAN ports only. The FlexWAN module handles policing itself because WAN packets generally have smaller headers than LAN packets. If the PFC did the policing, inaccuracies would result. High-Level Data Link Control (HDLC) has a header size of 4 bytes, and Ethernet (which is used on the backplane) has a header size of 14 bytes. If the policing were configured for 64 kbps and 40-byte IP frames were being sent, Ethernet framing would result in 125pps and HDLC in 181pps.



## **QoS Features Provided by FlexWAN Module**

### ***Queuing***

- Weighted Fair Queuing (WFQ)
- CBWFQ
- LLQ
- ATM per virtual circuit WFQ

### ***Congestion Avoidance and Policing***

- WRED
- Policing (Committed Access Rate [CAR])

### ***Traffic Shaping***

- Generic traffic shaping
- Frame Relay traffic shaping

### ***Additional QoS Features – H1 CY '03***

- Fragmentation of Frame Relay (FRF.12)
- Link fragmentation and interleaving (LFI)
- Compressed Real-Time Protocol (cRTP)
- QoS-over-MLP links

The QoS features are configured principally by the modular QoS CLI (MQC), which was first introduced in Cisco IOS 12.0(5) T. The QoS features available on the FlexWAN module are directly related to the QoS features that are available in the distributed path on the Cisco 7500 Series with VIPs. Figure 8 shows LLQ, CBWFQ, and distributed WRED (dWRED) on an ATM sub-interface.



**Figure 8: Example QoS Configuration for FlexWAN Module**

```
class-map match-all class_all_tcp
  match access-group 100
class-map match-all class_all_udp
  match access-group 101
class-map match-all class_all_voice
  match access-group 102
!
policy-map atm_cbwfg
  class class_all_tcp
    bandwidth 128
    random-detect
    fair-queue
  class class_all_udp
    bandwidth 128
    random-detect
    fair-queue
  class class_all_voice
    priority 64
!
interface ATM6/0/0.100 point-to-point
  ip address 47.1.1.2 255.255.255.0
  no ip directed-broadcast
  pvc 1/100
  vbr 10000 8000 1000
  !
  service-policy output atm_cbwfg
!
ip access-list 100 permit tcp any any
ip access-list 101 deny udp any any range 16384 20000
ip access-list 101 deny udp any any range 53000 56000
ip access-list 101 permit udp any any
ip access-list 102 permit udp any any range 16384 20000
ip access-list 102 permit udp any any range 53000 56000
```

```
ATM6/0/0.100
service-policy output: atm_cbwfg
  class-map: class_all_tcp (match-all)
    0 packets, 0 bytes
    5 minute rate 0 bps
  match: access-group name all_tcp
  class-map: class_all_udp (match-all)
    0 packets, 0 bytes
    5 minute rate 0 bps
  match: access-group name all_udp
  class-map: class_all_voice (match-all)
    0 packets, 0 bytes
    5 minute rate 0 bps
  match: access-group name all_voice
  priority: priority queueing
```

## ACL Processing

IP Unicast and multicast access control lists (ACLs) are handled by the MSFC and PFC. The ACLs configured on the MSFC are compiled and downloaded to the TCAM (ternary content-addressable memories) on the PFC. The ACLs for IP traffic are done this way because the FlexWAN module utilizes the Layer 3 Forwarding engines on the PFC for packet switching.

ACLs are also downloaded to the FlexWAN processors, because ACLs are also used by many of the QoS features performed by the FlexWAN module. The FlexWAN module does not handle security ACLs—they are handled by the MSFC and PFC. Multi-protocol traffic (DECnet, Open System Interconnection [OSI], AppleTalk) ACLs are all handled by the MSFC, because the MSFC handles the switching of these packets.

## High Availability and the FlexWAN Module

The 5.4 release of the Cisco Catalyst Operating System (CatOS) Software provides new high-availability options where the states of Layer 2 protocols are synchronized between the supervisor engines. Layer 3 state is not synchronized between the MSFCs. The FlexWAN modules are not shared between the MSFCs—they are controlled by the designated MSFC. The designated MSFC is usually the one that is on the active supervisor engine. The designated MSFC can be determined by issuing the **show fm features** command on the MSFC.

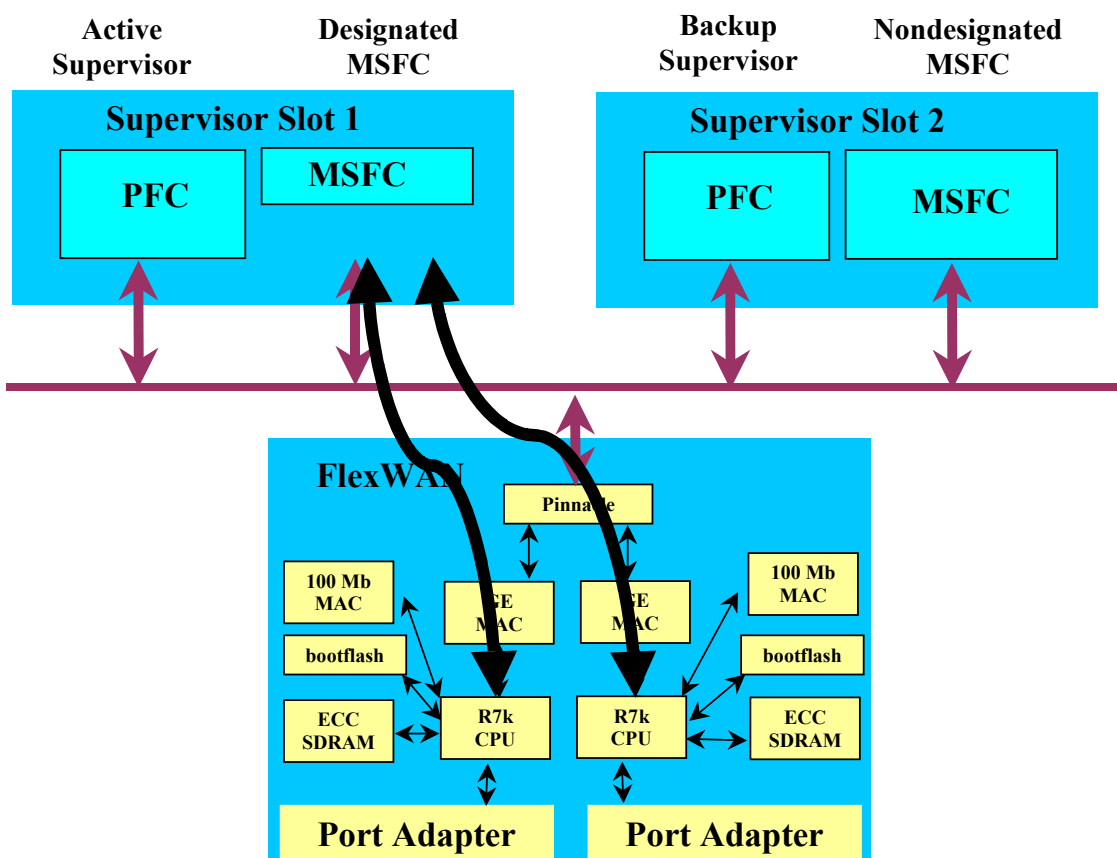
Hidden VLANs used by the FlexWAN module are considered to be point-to-point connections. The reason is that WAN links generally have only two ends, like the case of a point-to-point serial interface. It does not make sense for a serial link to have three possible endpoints, and this is why FlexWAN interfaces are present only on the designated MSFC.



The FlexWAN module is an intelligent module that can boot independently of the MSFC. After the FlexWAN module has booted, it attempts to communicate to the designated MSFC. The booting process of the FlexWAN module is more like online insertion and removal (OIR) than the booting process of the Cisco 7500 Series VIP. The MSFC places onto the deferred list any FlexWAN modules it cannot contact when parsing the configuration for the first time. When the FlexWAN modules do contact the MSFC, the interfaces are moved from the deferred list to the active interface list. If the designated MSFC can be discovered, MSFCs can be changed without requiring that the FlexWAN module reboot.

The Supervisor Engine in slot one is active and has the designated MSFC, and the supervisor engine in slot 2 is in backup mode. If the supervisor in slot 1 fails, then the supervisor in slot 2 “realizes” this, and the MSFC in slot 2 becomes the designated MSFC. The FlexWAN module realizes that the designated MSFC has changed and connects to the newly designated MSFC. This process takes approximately 17 to 20 seconds (refer to Figure 9).

**Figure 9: Cisco 7600 and Cisco Catalyst 6000 Series High Availability**



### Configuration Synchronization Between MSFCs

The Cisco IOS 12.1(3a)E Software release provides a feature that allows synchronization of the configuration between MSFCs. This feature is disabled by default, and results in the configuration for both MSFCs being done solely from the designated MSFC.



## Features Not Supported on the FlexWAN Module

Some features supported by the Cisco 7200 and 7500 Series Routers are not supported by the FlexWAN module. They include:

- ISDN, Multi-chassis Multilink PPP
- L2TP, Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F)
- IP Security (IPSec) (supported in future with service module)
- ATM LAN Emulation (LANE)
- PPP over ATM
- Frame Relay FRF.9, FRF.11 (future), and FRF.12 (future)
- cRTP (future)
- Frame Relay switched virtual circuits (SVCs)
- Systems Network Architecture (SNA) protocols, Synchronous Data Link Control (SDLC), Frame Relay Access Support (FRAS) boundary network node (BNN), FRAS boundary access node (BAN)

## Configuring and Monitoring the FlexWAN Module

One significant difference between the VLAN interfaces and FlexWAN interfaces on the MSFC is packet counts. On VLAN interfaces, statistics exist only for packets that the MSFC processes. FlexWAN interface counters show the total number of packets sent and received when either the MSFC or the PFC switches the packet. This is illustrated in Figure 10. The view of the FlexWAN module from the supervisor engine is minimal. With the **show module** command, you can see that a FlexWAN module is in a particular slot, but you cannot see what port adapters are in it. The output of the **show module** command is shown in Figure 11.



**Figure 10: FlexWAN show interface Command**

```
Sunshine-msfc#sh int atm 6/0/0
ATM6/0/0 is up, line protocol is up
Hardware is ENHANCED ATM PA
MTU 4470 bytes, sub MTU 4470, BW 149760 Kbit, DLY 80 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Keepalive not supported
Encapsulation(s): AAL5
1024 maximum active VCs, 603 current VCCs
VC idle disconnect time: 300 seconds
Signalling vc = 1, vpi = 0, vci = 5
UNI Version = 4.0, Link Side = user
2 carrier transitions
Last input 00:00:00, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 2674 drops; input queue 0/75, 0 drops
30 second input rate 22000 bits/sec, 36 packets/sec
30 second output rate 331000 bits/sec, 34 packets/sec
  211176 packets input, 6210868 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  208716 packets output, 9983500 bytes, 0 underruns
  0 output errors, 0 collisions, 2 interface resets
  0 output buffer failures, 0 output buffers swapped out
sunshine-msfc#
```

**Figure 11: Output of show module Command**

```
Console-albury> (enable) sh mod
Mod Slot Ports Module-Type Model Status
-----
-
1 1 2 1000BaseX Supervisor WS-X6K-SUP1A-2GE ok
15 1 1 Multilayer Switch Feature WS-F6K-MSFC ok
4 4 8 1000BaseX Ethernet WS-X6408-GBIC ok
5 5 48 10/100BaseTX (RJ-45) WS-X6248-RJ-45 ok
6 6 0 FlexWAN Module WS-X6802 ok
```

The difference between Cisco Catalyst (LAN) interfaces and FlexWAN interfaces is that FlexWAN interfaces are numbered starting at zero, whereas Cisco Catalyst interfaces start at one. This was done because the port adapters from the Cisco 7200 and 7500 series routers begin at zero. The FlexWAN module also uses the Cisco 7500 Series VIP naming convention in that ports are referenced by slot, bay, and then port.

Because the FlexWAN module uses hidden VLANs and Multilayer Switching (MLS), shortcut entries are created in the MLS switching cache. Figure 12 shows the output of the **show mls entries** command from the supervisor engine and the **show cwan VLANs** command from the MSFC. In the output of the **show mls entry** command, the output port 6/1 is the port on the pinnacle to which the CPU controlling the port adapter is connected. Bay 0 is connected to port 1 and bay 1 is connected to port 2 on the Pinnacle ASIC. The hidden VLAN allocated to ATM interface 6/0/0.100 is 1250.



Figure 12: MLS and Hidden VLANs in Hybrid [EDITS: Port; VLAN]

```
Console-albury> (enable) sh mls entry
Destination-IP  Source-IP      Destination-Mac  Vlan EDst  ESrc  DPort
SPort
-----
--
MSFC 10.1.1.235 (Module 15):
10.30.11.102    -              00-00-06-00-00-03 1250 ARPA  ARPA  6/1    5/48

```

**Hidden VLAN** →

```
albury-msfc#sh cwan vlans
0 Hidden VLAN operations pending, 0 swidbs on defer list
Hidden VLAN  Interface
-----
1024         used to be Serial6/1/1.100 (now 1025)
1250         ATM6/0/0.100

```

→ **FlexWAN Pinnacle Port**

### Conclusion and Summary

To conclude, the FlexWAN module for the Cisco 7600 Series Router and the Cisco Catalyst 6000 Series of switches is a well-developed technology of choice for enterprise, metropolitan, and wide-area networks. The FlexWAN module provides for an excellent migration path from current Cisco 7500 Series installations, taking advantage of existing port adapters. When combined with industry-leading features in multicast, routing support, and resiliency, the FlexWAN module coupled with the Cisco 7600 Series Routers and the Cisco Catalyst 6000 Series clearly provides a superior solution for networks today and tomorrow.



Copyright 2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site 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. (0301R)