Ejemplo: Cisco Catayst 6500-E

Chasis

	Catalyst 6503-E	Catalyst 6504-E	Catalyst 6506-E	Catalyst 6509-E	Catalyst 6513-E	Catalyst 6509-V-E
Slots	3	4	6	9	13	9 vertical
Max 10/100/1000 ports	97	145	241	385	529	385
Max 1 GE ports[1]	99	147	243	387	534	387
Max 10 GE ports[2]	34	50	82	130	180	130
Max 40 GE ports	8	12	20	32	44	32
Maximum forwarding performance (IPv4)	150 Mpps	210 Mpps	330 Mpps	510 Mpps	720 Mpps	510 Mpps
Height (RU)	4	5	11	14	19	21
Weight (chassis)	33 lbs (15 kg)	40 lbs (17.8 kg)	50 lbs (22.7 kg)	60 lbs (27.3 kg)	79.1 lbs (35.9 kg)	121 lbs (54.9 kg)

[1] Assumes use of supervisor uplinks in single supervisor configuration

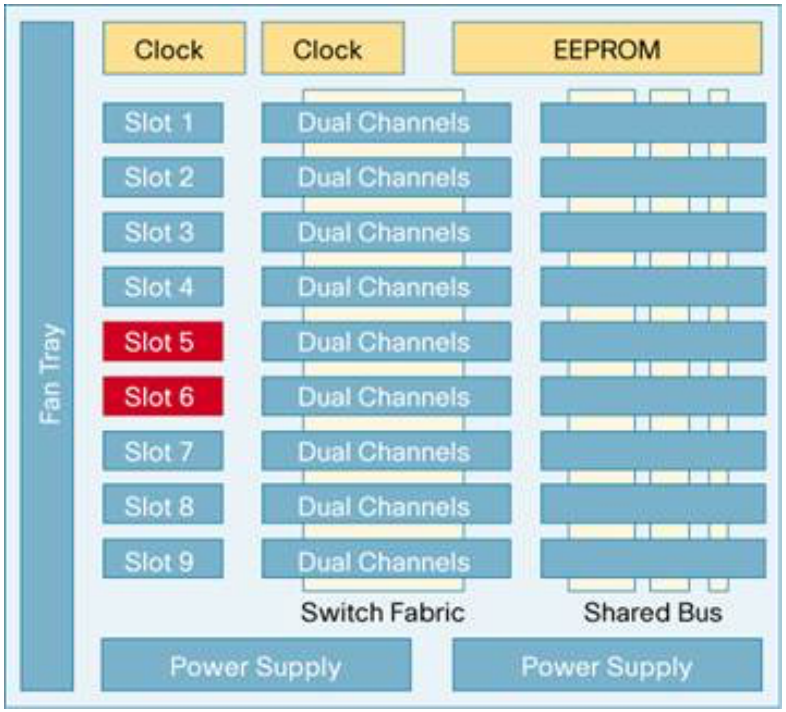
[2] Assumes use of supervisor uplinks in single supervisor configuration

1Mpps x 64 Bytes/paquete = 512 Mbps
1Mpps x 1518 Bytes/paquete = 12.1 Gbps
100Mpps x 64 Bytes/paquete = 51.5 Gbps
100Mpps x 1518 Bytes/paquete = 1.21 Tbps

http://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/index.html

Backplane

- Dos backplanes
  - Inicialmente (1999) un bus a 32Gbps
  - Y un crossbar (*Switch Fabric Modules*) de 256Gbps (hoy integrado en la tarjeta supervisora)
- Cada tarjeta tiene dos canales con la matriz de conmutación



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

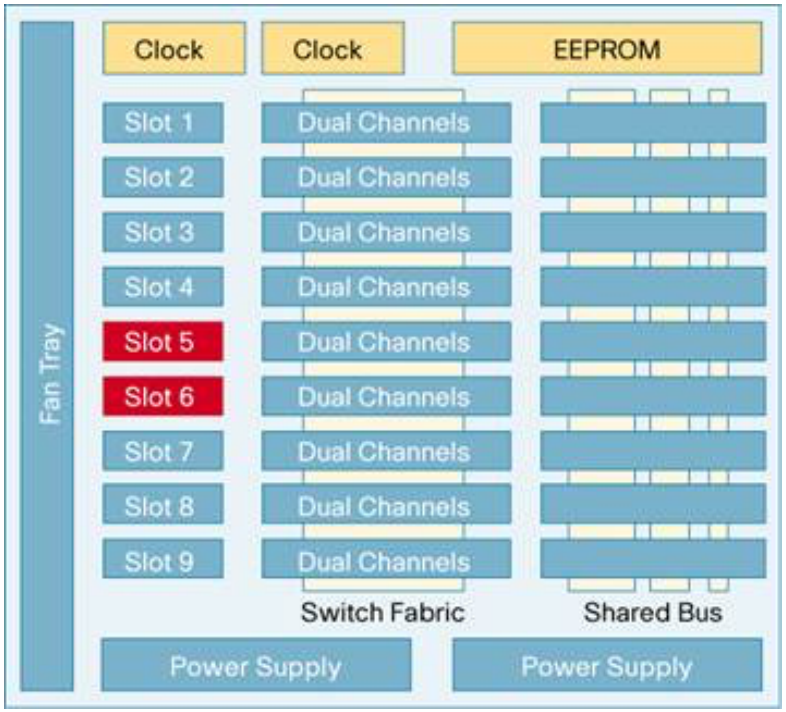
Supervisoras

Catalyst Supervisor Engines

	6T	6T-XL	2T	2T-XL	720-10G	720-10G-XL	720-3B	720-3BXL
Switch fabric	Integrated T6	Integrated 6T	Integrated 2T	Integrated 2T	Integrated 720G	Integrated 720G	Integrated 720G	Integrated 720G
Virtual Switching System (VSS)	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Uplinks	2 x 40GE (QSFP) 8 x 10GE (SFP+) RJ-45 / SFP Management Ports		3 x 1 GE (SFP) 2 x 10 GE (X2) 1 management (CMP)		2 x 1 GE (SFP) 2 x 10 GE (X2) 1 x 10/100/1000 RJ-45		1 x 1 GE (SFP) 1 x 1 GE (SFP) or 10/100/1000 RJ-45	
Chassis	E-Series only	E-Series only	E-Series only	E-Series only	6503/6503-E 6504-E 6506/6506-E 6509/6509-E 6509-NEB-A 6509-V-E 6513/6513-E	6503/6503-E 6504-E 6506/6506-E 6509/6509-E 6509-NEB-A 6509-V-E 6513/6513-E	6503/6503-E 6504-E 6506/6506-E 6509/6509-E 6509-NEB 6509-NEB-A 6513/6513-E	6503/6503-E 6504-E 6506/6506-E 6509/6509-E 6509-NEB 6509-NEB-A 6513/6513-E

Shared bus

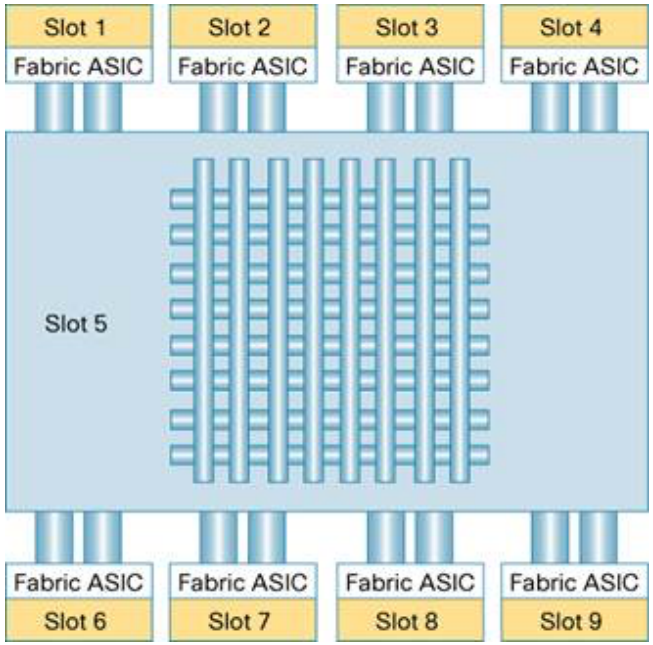
- Interfaz de entrada logra acceso al bus
- Envía por él la trama a la supervisora (32Gbps)
- El resto de tarjetas copian el paquete al pasar por el bus
- La supervisora decide el reenvío del paquete
- Notifica a las tarjetas si deben enviarla o descartarla
- Soporta ráfagas



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Crossbar Switching Fabric

- Originalmente en módulo independiente; ahora en la propia supervisora
- Cada canal es a 8Gbps o 20Gbps (según otras tarjetas presentes)
- Con 2 canales en algunos slots es un máximo de 40Gbps por tarjeta
- Internamente la supervisora 720 tiene un *speedup* 3x (60Gbps)
- Diferentes modos de funcionamiento
  - Sin crossbar, enviar paquete por bus a la supervisora (máx 15Mpps)
  - Con crossbar, solo la cabecera se pasa a la supervisora por el bus, los datos por el crossbar (máx 30Mpps)

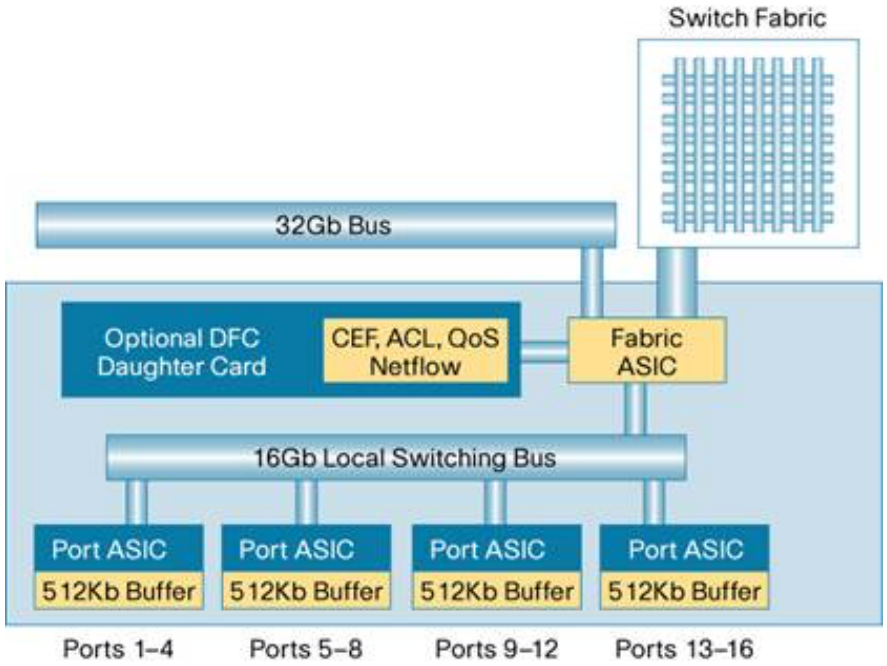


10Mpps x 64 Bytes/paquete = 5.12 Gbps
10Mpps x 1518 Bytes/paquete = 121 Gbps

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Line Cards

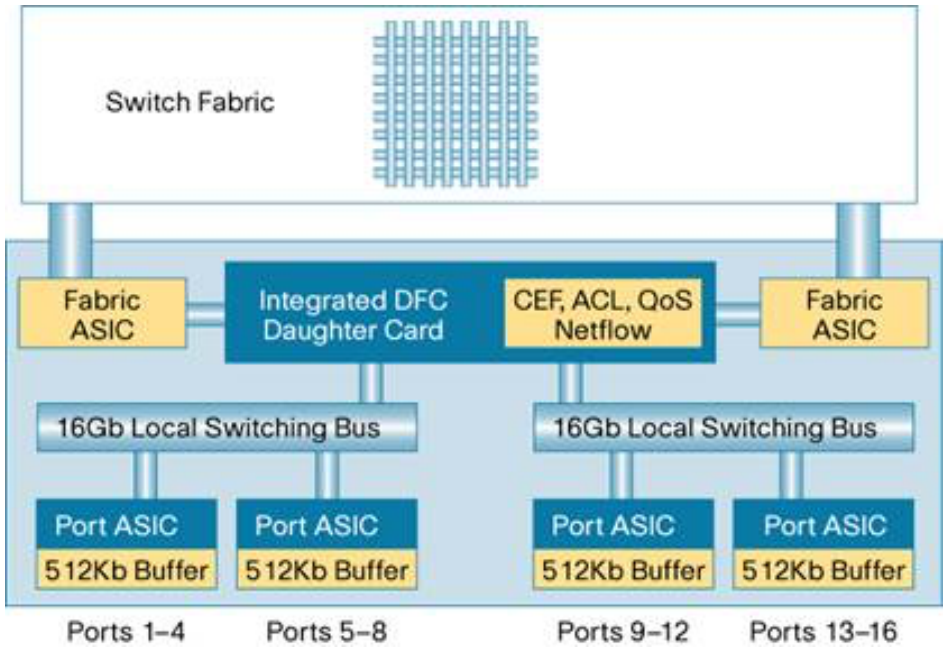
- Pueden contener un bus interno para conmutación local
- En tarjetas con conexión a 8Gbps al fabric tienen un bus interno a 16Gbps
- Si la tarjeta soporta *Distributed Forwarding* evita enviar el paquete por el chasis (nativamente o con módulo)
- El DF requiere no solo el forwarding básico (L2 y/o L3) sino también implementar las políticas de seguridad (ACLs)



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Line Cards

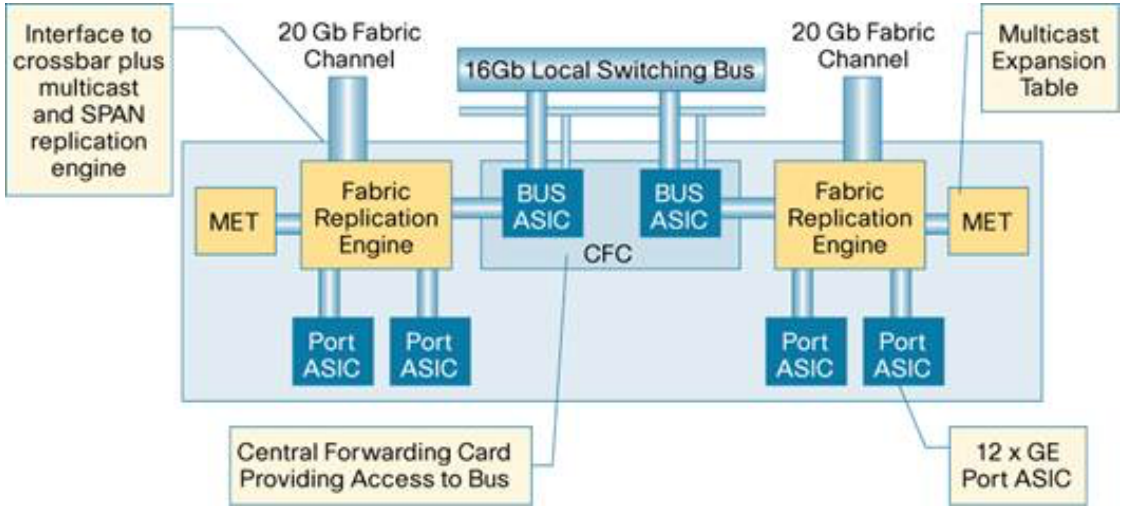
- Pueden contener dos buses internos (16Gbps cada uno)
- Paquetes de un bus al otro pasan por el fabric
- En esta arquitectura doble conexión al fabric



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Line Cards

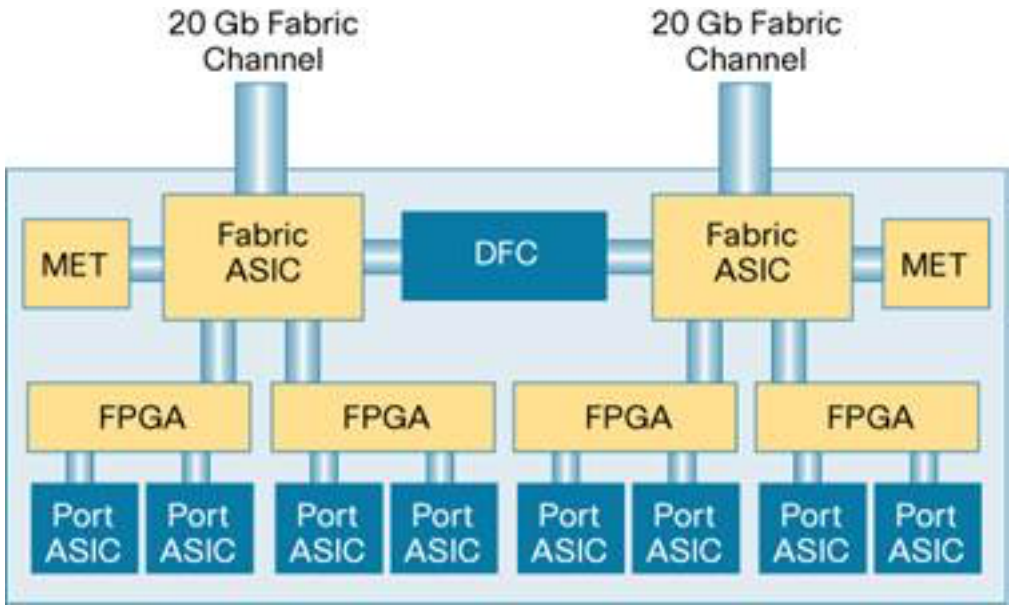
- En esta arquitectura la comunicación interna entre dos bloques de puertos es por un bus local



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Line Cards

- Podemos encontrar sobresubscripción en la conexión al fabric
- Por ejemplo esta arquitectura tiene 40Gbps al fabric pero hay tarjetas con 8 puertos 10GE
- 48Mpps con reenvío distribuido

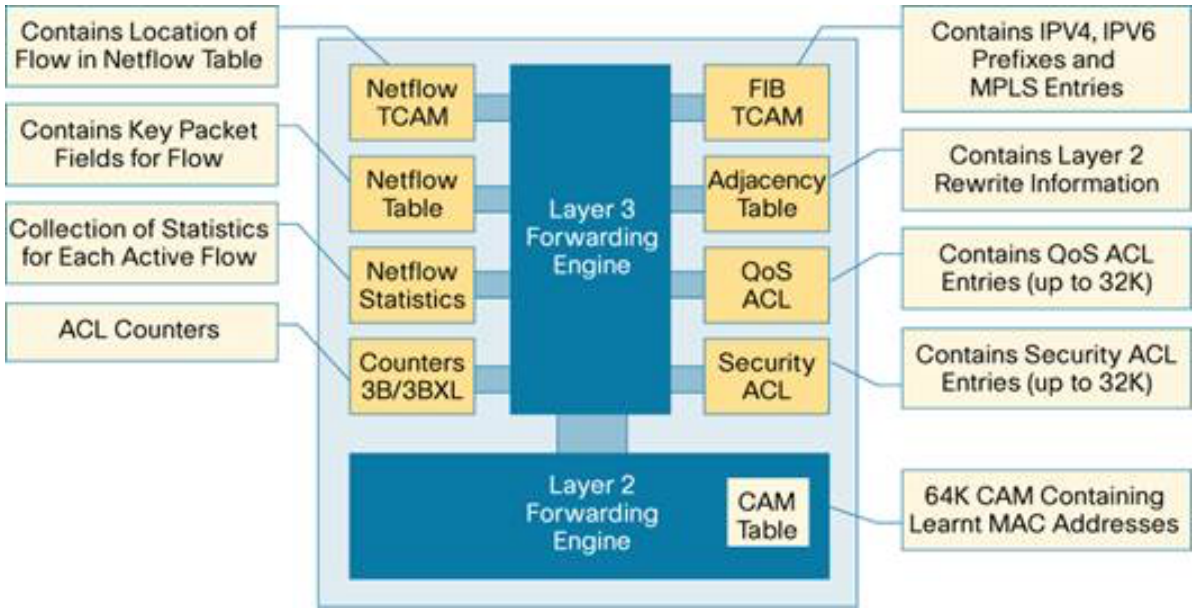


10Mpps x 64 Bytes/paquete = 5.12 Gbps
10Mpps x 1518 Bytes/paquete = 121 Gbps

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Distributed Forwarding

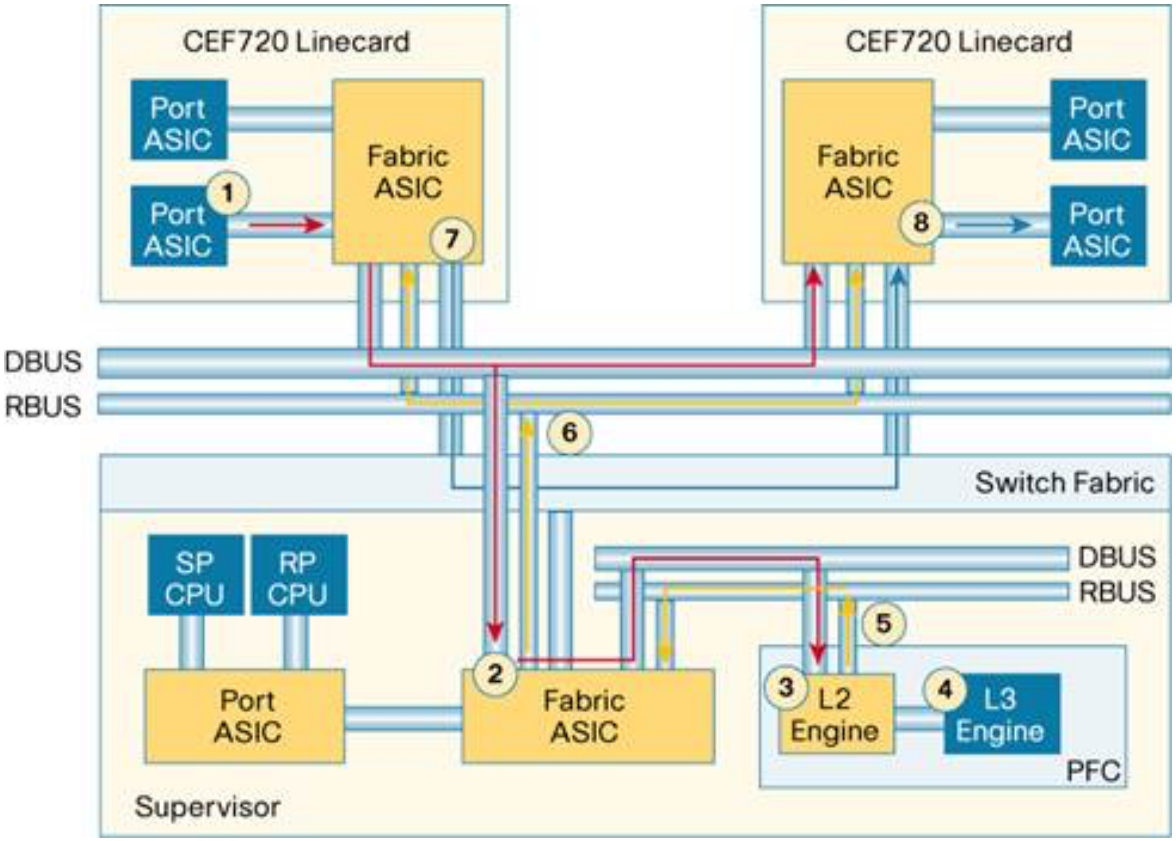
- FIB
  - *Forwarding Information Base*
  - TCAM
- QoS y ACLs
  - Búsquedas simultáneas a la búsqueda en la FIB
  - De nuevo TCAMs



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Ejemplo: Centralizado

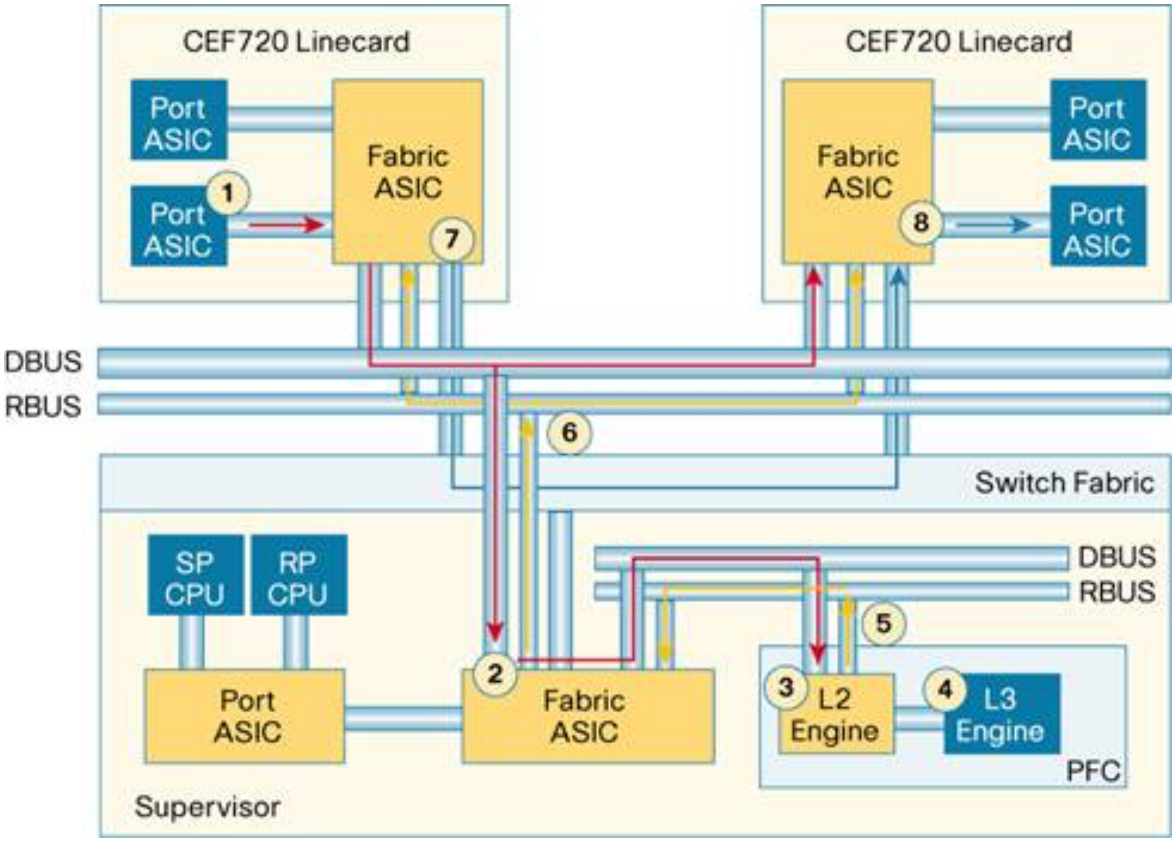
- Step 1. The packet arrives at the port and is passed to the fabric ASIC.
- Step 2. The fabric ASIC arbitrates for bus access and forwards the header (and not the data payload) over the bus to the supervisor. All line cards connected to the bus will see this header.



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Ejemplo: Centralizado

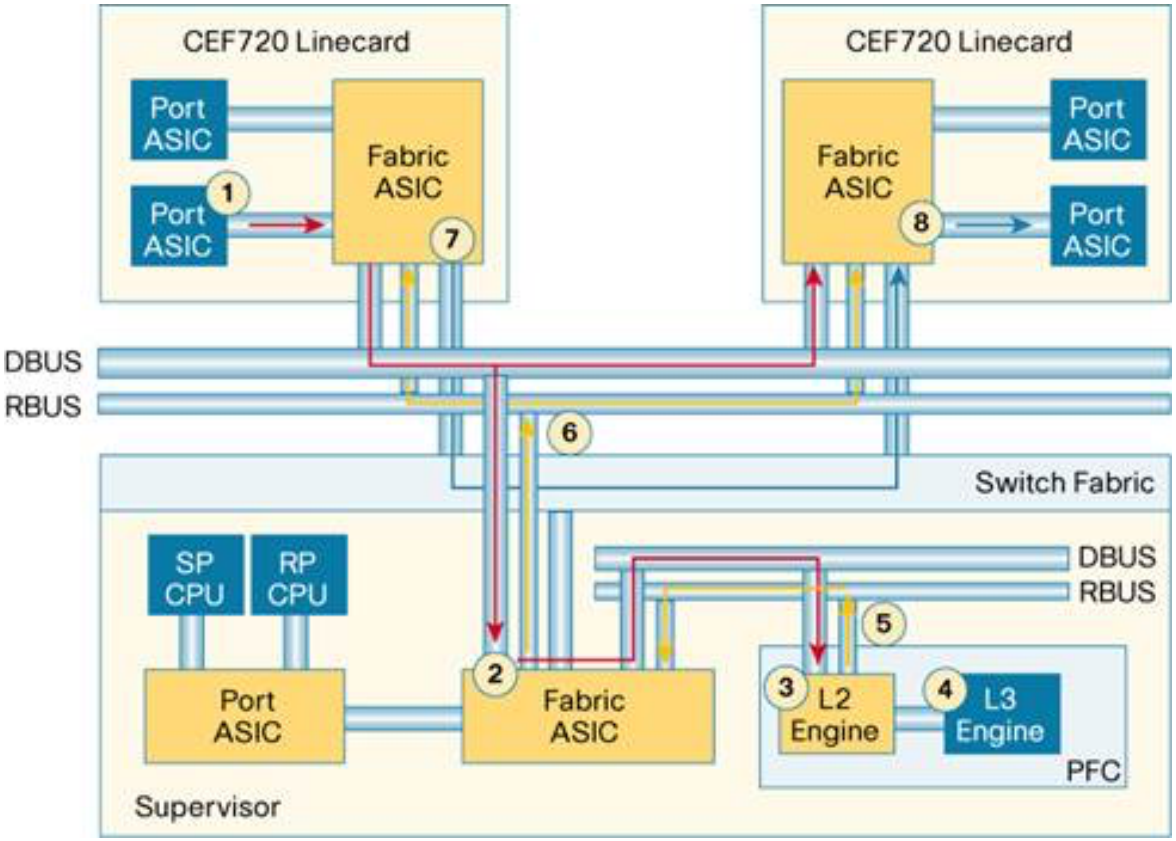
- Step 3. The supervisor will forward the packet header to the Layer 2 forwarding engine for a Layer 2 lookup.
- Step 4. The Layer 2 forwarding engine then forwards the packet to the Layer 3 engine for Layer 3 and 4 processing which includes NetFlow, QoS ACL, Security ACL and Layer 3 lookups.



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Ejemplo: Centralizado

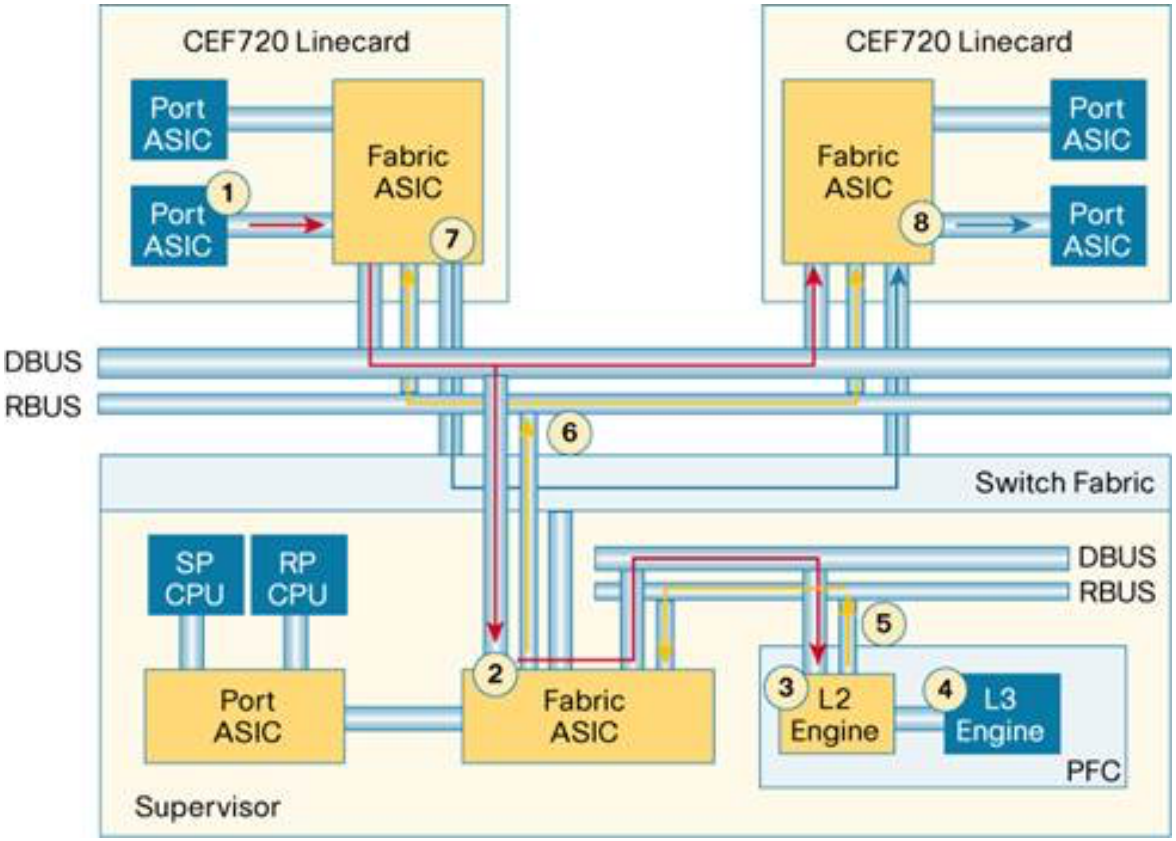
- Step 5. The PFC will combine the results of the multiple lookups and pass the results of the process back to the central supervisor.
- Step 6. The supervisor will forward the result of this lookup back over the results bus to all connected line cards.



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Ejemplo: Centralizado

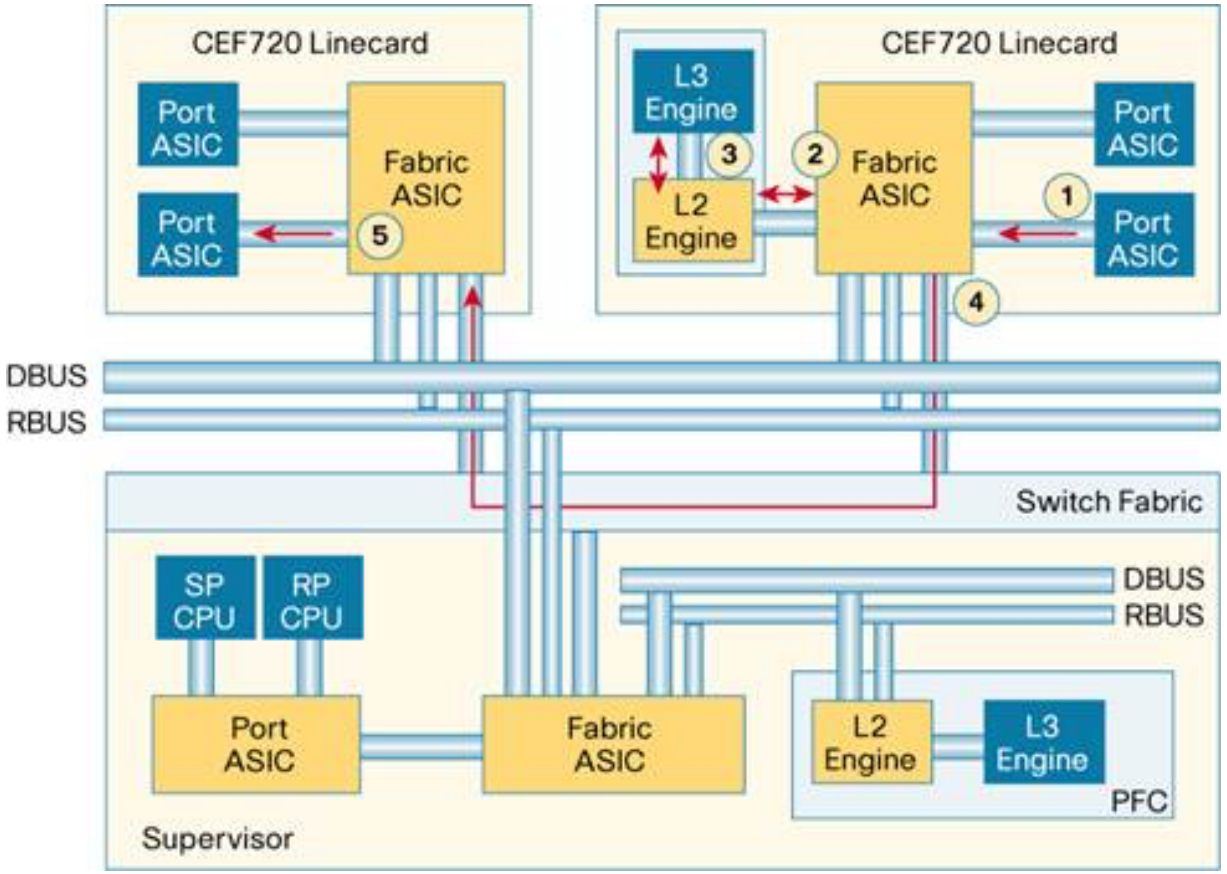
- Step 7. Once the source line card sees the result, it will send the packet data over the switch fabric to the destination line card.
- Step 8. The destination line card will receive the packet and forward the data out the destination port.



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Ejemplo: Distribuido

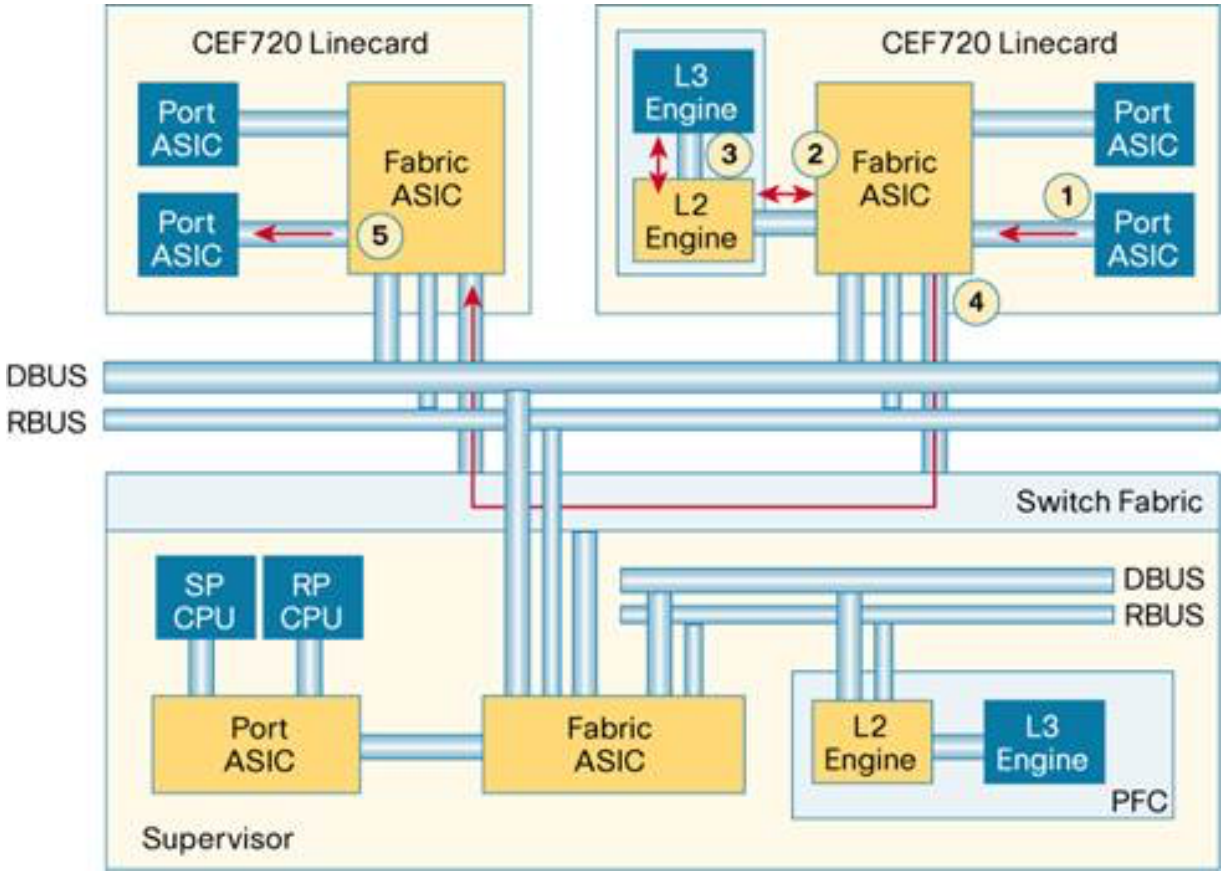
- Step 1. The packet arrives at the port and is passed to the fabric ASIC.
- Step 2. The fabric ASIC forwards the packet headers are sent to the local DFC.



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Ejemplo: Distribuido

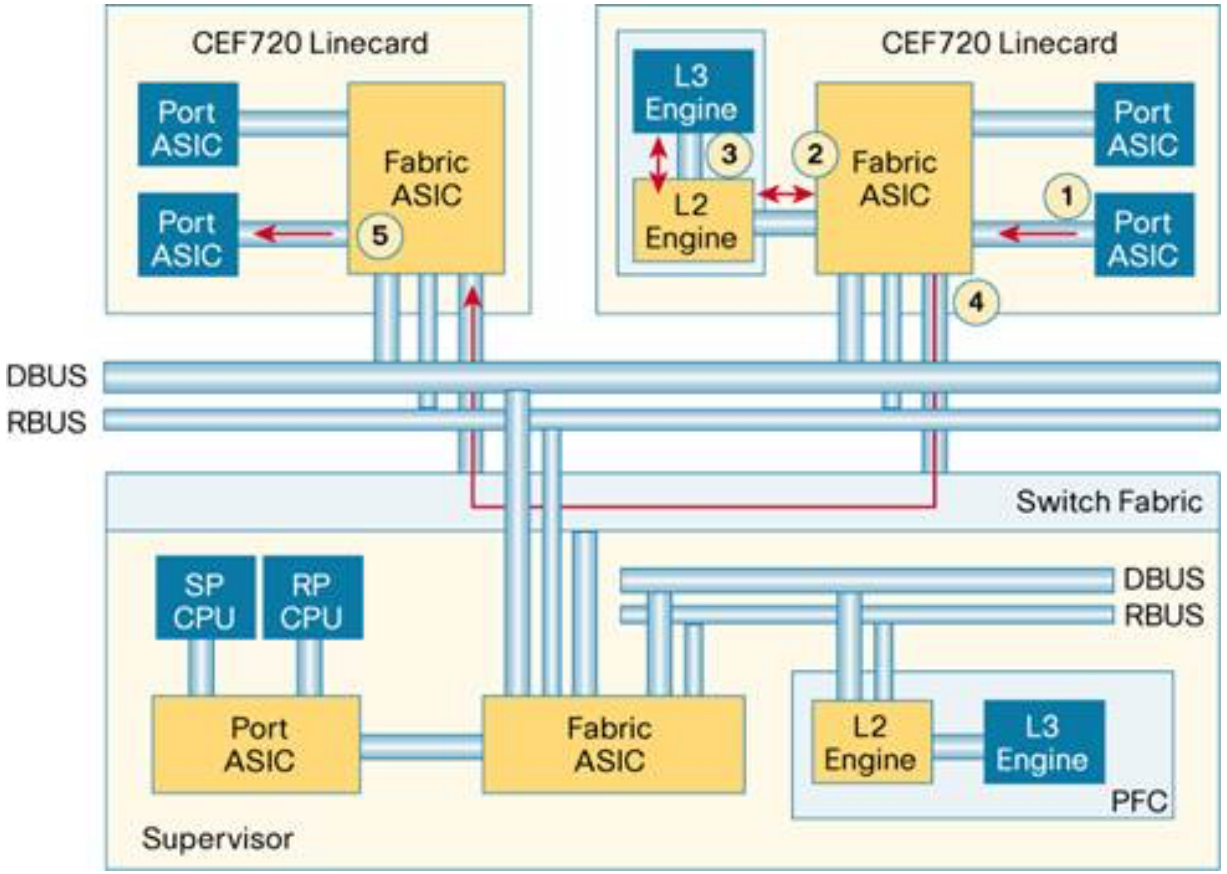
- Step 3. The DFC will perform a forwarding lookup, along with a lookup into the QoS and Security ACLs to determine if any QoS or security policies need to be applied to the packet. The results of the lookup are passed back to the fabric ASIC.



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

Ejemplo: Distribuido

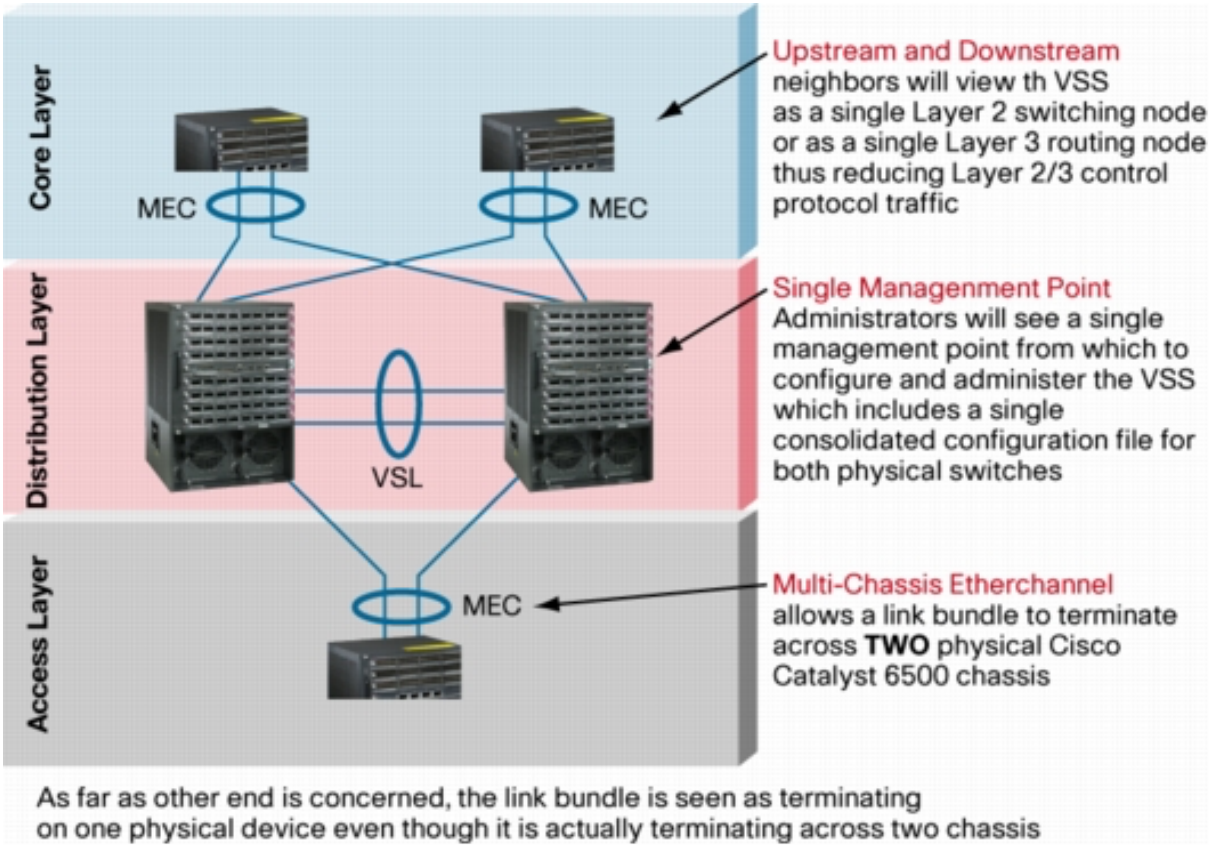
- Step 4. The fabric ASIC will forward the packet data over the switch fabric to the destination port.
- Step 5. The destination line card will receive the packet and forward the data out the destination port.



http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd80673385.html

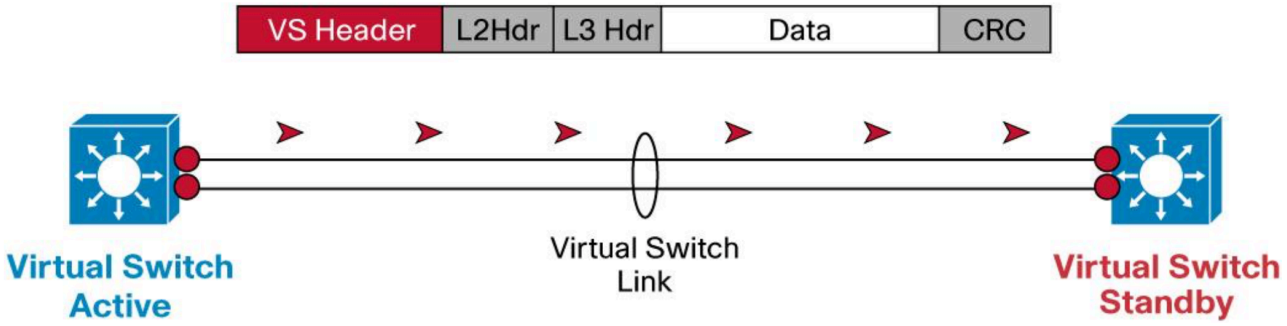
Virtual Switching System (VSS)

- Desde 2008
- Soportado solo por ciertas tarjetas supervisoras



Virtual Switch Link (VSL)

- Lleva tráfico normal y tráfico de control del VSL
- Las tramas del VSL llevan una cabecera adicional (32 bytes) tras el preámbulo

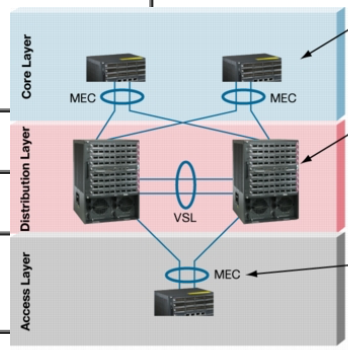


http://www.cisco.com/c/dam/en/us/products/collateral/interfaces-modules/network-modules/white_paper_c11_429338.pdf

Virtual Switching System (VSS)

Table 1. Specifications of the Cisco Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet uplinks

Feature	Cisco Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet uplinks (PFC 3C)	Cisco Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet uplinks (PFC 3CXL)
Support for Cisco VSS 1440	Yes	Yes
MAC entries	96,000	96,000
IP Routes	256,000 (IPv4); 128,000 (IPv6)	1,000,000 (IPv4); 500,000 (IPv6)
IPv4 Routing	• In hardware • Up to 450 Mpps*	• In hardware • Up to 450 Mpps*
IPv6 Routing	• In hardware • Up to 225 Mpps*	• In hardware • Up to 225 Mpps*
Layer 2 Bridging	• In hardware • Up to 450 Mpps*	• In hardware • Up to 450 Mpps*
NetFlow Entries	128,000	• 256,000
MPLS	• MPLS in hardware to enable use of Layer 3 VPNs and EoMPLS tunneling. • Up to 1024 virtual routing and forwarding instances (VRFs) with a total of up to 256,000 routes per system.	• MPLS in hardware to enable use of Layer 3 VPNs and EoMPLS tunneling. • Up to 1024 VRFs with a total of up to 1,000,000 routes per system.
GRE	In hardware	In hardware
NAT	Hardware-assisted	Hardware-assisted



* With Cisco Distributed Forwarding Card 3C (DFC3C)

100Mpps x 64 Bytes/paquete = 51.5 Gbps
100Mpps x 1518 Bytes/paquete = 1.21 Tbps

2014: Tabla de rutas BGP excede las 500k entradas

Supervisor Engine 32

- No se vende desde 2012 (soporte hasta 2017)
- 32Gbps Shared Bus
- Hasta 15 Mpps IPv4

10Mpps x 64 Bytes/paquete = 5.1 Gbps
10Mpps x 1518 Bytes/paquete = 121 Gbps

http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-supervisor-engine-32/product_data_sheet0900aecd801c5cab.html

Supervisor Engine 32 vs 720

Feature	Supervisor Engine 720	Supervisor Engine 32
Uplinks	Two Gigabit Ethernet ports-one gigabit interface converter (GBIC) based and one configurable to GBIC based or 10/100/1000 RJ-45 based	• Eight Gigabit Ethernet ports, SFP based + one 10/100/1000 RJ-45 port OR • Two 10 Gigabit Ethernet ports, XENPAK based + one 10/100/1000 RJ-45 port
Uplink Queue Structure	• Tx 1p2q2t • Rx 1p1q4t • 512 KB buffer per port	• Tx 1p3q8t • Rx 2q8t • 9.5 MB buffer per Gigabit Ethernet port • 100 MB buffer per 10 Gigabit Ethernet port
Uplink Port Scheduler	WRR	DWRR or SRR
USB Port	No	Two USB 2.0 ports-one host port and one device port
Self-Power Cycling	No, power cycle line cards only	Yes, power cycle remotely through console port
Backplane	720 Gbps integrated switch fabric module (SFM)	32 Gbps shared bus
Performance	Up to 400 Mpps for Cisco Express Forwarding interface modules	Up to 15 Mpps IPv4 services
Cisco Express Forwarding	Yes	Yes, hardware-based forwarding with MSFC2A
Distributed Cisco Express Forwarding	Yes, with a DFC3 present	No

Feature	Supervisor Engine 720	Supervisor Engine 32
SP NVRAM	2 MB (SP)	2 MB (SP)
SP Dynamic RAM (DRAM)	512 MB default, upgradeable to 1 GB on Supervisor Engine 720 and Supervisor Engine 720-3B; 1 GB default on Supervisor Engine 720-3BXL	512 MB default, upgradeable to 1 GB
SP Onboard Flash (BootFlash)	64 MB upgradeable to 512 MB, 1GB	256 MB, through internal compact flash (referred to as bootdisk in command-line interface), upgradeable to 512 MB, 1 GB
Removable Memory	Compact flash type II-64, 128, and 256 MB; hardware capable to support 512 MB, 1 GB	Compact flash type II-64, 128, and 256 MB; hardware capable to support 512 MB, 1 GB; USB
Chassis Supported	All Cisco Catalyst 6500 Series chassis and Cisco 7600 Series chassis with fan tray 2 or E-Series fan tray and 2500W power supplies or above	All Cisco Catalyst 6500 Series chassis with fan tray 2 or E-Series fan tray and 2500W power supplies or above; Cisco 7604, Cisco 7606, Cisco 7609, and Cisco 7613 with high speed fan tray
Minimum Software Support	• Cisco Catalyst 6500 Series: · CatOS 8.1(1) · Cisco IOS ® Software 12.2(14)SX • Cisco 7600 Series: Future	• Cisco Catalyst 6500 Series: · CatOS 8.4(1) · Cisco IOS 12.2(18)SXF • Cisco 7600 Series: IOS 12.2.18SXF
Slot Requirements	Slots 1 and 2 in a 3-slot chassis, slots 5 and 6 in a 6- or 9-slot chassis, and slots 7 and 8 in a 13-slot chassis	Slots 1 and 2 in a 3-slot and 4 slot chassis, slots 5 and 6 in a 6- or 9-slot chassis, and slots 7 and 8 in a 13-slot chassis

Tx 1pNqMt = 1 cola de prioridad estricta, N colas normales con M umbrales de WRED
Rx {1p}NqMt = {1 cola de prioridad estricta,} N colas normales con M umbrales de *drop-tail*

Supervisor Engine 32

Features	Benefits
Identity-based networking services with IEEE 802.1x: • VLAN ID assignment • Security ACL assignment • QoS policy assignment • Unidirectional controlled port for "wake-on-LAN" applications • Authentication identity-to-port description mapping • Domain Name System (DNS) resolution for RADIUS server configuration	Allows close control over which users can access the network and what privileges they are granted
Intrusion detection and spoofing protection mechanisms: • DHCP snooping, dynamic ARP inspection, IP source guard-Cisco Catalyst 6500 Security Toolkit • CPU rate limiting • Control Plane Policing • Port-based ACLs • User-based rate limiting • Hardware-based MAC learning • Cisco Catalyst 6500 IDS module • Broadcast and multicast suppression • Port Security on Access, 802.1Q Trunks and 802.1Q Tunneling ports	Provides local containment of security threats and protects networks against security vulnerabilities, including malicious and inadvertent intrusion
Hot-Swapping of Standby Supervisor Engines • Layer 2 rapid convergence protocol suite includes: · IEEE 802.1s, multiple spanning trees · IEEE 802.1w, rapid reconfiguration of spanning tree · Per-VLAN rapid spanning tree (PVRST) • Hardware redundancy with subsecond stateful failover and Layer 2 resiliency through 802.1x high availability • Fault management: · Fault detection and troubleshooting · System health check · Enhanced memory protection · Proactive detection and prevention of network equipment failures using GOLD	Ensures business continuity through minimizing network downtime for mission-critical applications
Switched Port Analyzer (SPAN), Remote SPAN (RSPAN)	Enables remote troubleshooting from anywhere, reducing troubleshooting time and tool costs
Two USB 2.0 ports (hardware ready, software support post-first customer shipment [FCS])	Enables direct access from laptops for network management, simplifies software downloading using USB memory devices, and enhances security by enabling USB keys on console port to limit access to authorized personnel
ACE counters	Identifies frequency that specific ACL entries are hit for ease of management

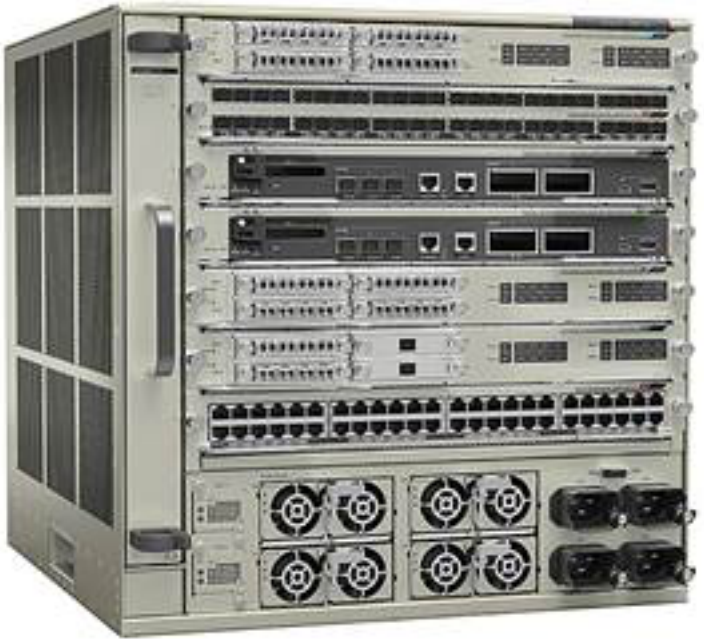
Supervisor Engine 32

Cisco SmartPort macros, config rollback, and switch profiles	Simplifies operational complexity
SNMPv3, SSH Protocol Version 2, Secure Copy Protocol (SCP)	Provides secure management
Multicast capabilities: • Hardware-based multicast • Bidirectional Protocol Independent Multicast (PIM) • Internet Group Management Protocol (IGMP) Querier • Router-port Group Management Protocol (RGMP), Multiprotocol Border Gateway Protocol (MBGP) • PIM SM, PIM SSM and PIM snooping • IGMP version 3	Enables efficient video broadcasting, e-learning, and information sharing
Integrated high-density uplinks-eight Gigabit Ethernet SFP-based ports or two 10-Gigabit Ethernet XENPAK-based ports	Increases uplink density and saves slots to deploy integrated service modules or higher-density chassis
Backward compatibility-supports all Cisco Catalyst 6500 classic and Cisco Express Forwarding 256-based modules and services modules; supported in all Cisco Catalyst 6500 Series and Cisco 7600 Series Router chassis	Allows deployment of new advanced services on existing equipment, prolonging the deployment lifetime of interface modules and providing greater return on investment
• Advanced QoS uses packet classification and marking and congestion avoidance based on Layer 2-4 header information • User-based rate limiting enforces any of 64 policy rates, maintaining service-level agreements on a per-user basis independent of traffic type or IP address • QoS scheduling rules with thresholds can be configured in the switch for multiple receive and transmit queues	Superior traffic management enables efficient handling of converged networks that carry a mix of mission-critical, time-sensitive, and bandwidth-intensive multimedia applications
• Hardware-enabled MPLS-Enables use of VPNs and Layer 2 tunneling while improving traffic engineering for QoS and adding multiprotocol support • Hardware-enabled IPv6-Expands available IP addresses, enabling better address allocation and address aggregation and supporting greater end-to-end connectivity and services • Hardware-enabled GRE tunnels for IP traffic • NAT (hardware ready, software support post-FCS)-Translates addresses for inbound and outbound traffic in hardware, allowing clean separation between internal and external networks	Advanced Layer 2-4 forwarding enables service providers and enterprises to build feature-rich networks

Cisco Catalyst 6800

- Evolución del 6500 y 6700
- Varias opciones en cuestión de número de slots
- También opción compacta

Catalyst 6800ia



Catalyst 6807-XL

Supervisoras 6T y 6T-XL

- Integran un crossbar switch fabric a 6Tbps

Attribute	C6800-SUP6T	C6800-SUP6T-XL
MAC entries	128K	128K
Routes	256K (IPv4) 128K (IPv6)	Upto 1024K (IPv4) Upto 512K (IPv6)
ACL entries	64K shared for QoS and security	256K shared for QoS and security
NetFlow entries	512K per EARL	1024K per EARL
Multicast routes	Up to 128K (IPv4) Up to 128K (IPv6)	Up to 128K (IPv4) Up to 128K (IPv6)
IPv4 routing	In hardware Up to 780 Mpps*	In hardware Up to 780 Mpps*
IPv6 routing	In hardware Up to 390 Mpps*	In hardware Up to 390 Mpps*
Layer 2 bridging	In hardware Up to 780 Mpps	In hardware Up to 780 Mpps
Jumbo frame support	Up to 9216 bytes (for bridged and routed packets)	Up to 9216 bytes (for bridged and routed packets)
VLAN	4K	4K
Bridge domains	16K	16K
MPLS	MPLS in hardware to support use of Layer 3 VPNs and Ethernet over (EoMPLS) tunneling. Up to 8192 VRFs, with a total of up to 256K forwarding entries per system.	MPLS in hardware to support use of Layer 3 VPNs and EoMPLS tunneling. Up to 8192 VRFs, with a total of up to 1024K forwarding entries per system

http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6800-series-supervisor-engine-6t/datasheet-c78-736408.html

Supervisoras 6T y 6T-XL

Logical interfaces	128K	128K
EtherChannel hash	8 bits	8 bits
VPLS	In hardware (up to 390 Mpps)	In hardware (up to 390 Mpps)
Generic Routing Encapsulation (GRE)	In hardware (up to 390 Mpps)	In hardware (up to 390 Mpps)
Network Address Translation (NAT)	Hardware assisted	Hardware assisted
Onboard memory	4 GB	4 GB
Ingress buffers	1.25 MB per 10-Gb port in 2:1 mode 2.5 MB per 10-Gb port in 1:1 mode (10 MB per port ASIC)	1.25 MB per 10-Gb port in 2:1 mode 2.5 MB per 10-Gb port in 1:1 mode (10 MB per port ASIC)
Egress buffers	250 MB per 10-Gb port in 2:1 mode 1 GB per 40-Gb port in 2:1 mode 500 MB per 10-Gb port in 1:1 mode 2 GB per 40-Gb port in 1:1 mode (2 GB per FIRE ASIC)	250 MB per 10-Gb port in 2:1 mode 1 GB per 40-Gb port in 2:1 mode 500 MB per 10-Gb port in 1:1 mode 2 GB per 40-Gb port in 1:1 mode (2 GB per FIRE ASIC)

* Requires a fully populated 6513-E chassis with Distributed Forwarding Card4 (DFC4) and DFC4XL

http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6800-series-supervisor-engine-6t/datasheet-c78-736408.html

Supervisoras 6T y 6T-XL

Feature	C6800-SUP6T	C6800-SUP6T-XL
Layer 3 classification and marking access control entries (ACEs)	64K shared for QoS and security	256K shared for QoS and security
Aggregate traffic rate-limiting policers	16,348	16,348
Flow-based rate-limiting method; number of rates	Per source address, destination address, or full flow; 64 rates	Per source address, destination address, or full flow; 64 rates
Layer 2 rate limiters	20 ingress, 6 egress	20 ingress, 6 egress
Class of service (CoS) and differentiated services code point (DSCP)-based queue mapping	Yes	Yes
Deficit Weighted Round Robin Scheduler (DWRR) and Weighted Random Early Detection Scheduler (WRED)	Yes	Yes
Traffic shaping	Yes	Yes
Hierarchical QoS	2-level	2-level
Receive and transmit queues	Default: 1p7q4t Configurable: 2p6q4t	Default: 1p7q4t Configurable: 2p6q4t

Tx 1pNqMt = 1 cola de prioridad estricta, N colas normales con M umbrales de WRED
Rx {1p}NqMt = {1 cola de prioridad estricta,} N colas normales con M umbrales de *drop-tail*

http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6800-series-supervisor-engine-6t/datasheet-c78-736408.html

Módulos 1GE

	Catalyst 6800 Series			Catalyst 6700 Series		
	6848-SFP	6848-TX	6824-SFP	6748-SFP	6748-TX	6724-SFP
Ports	48	48	24	48	48	24
Optics	SFP	None (RJ-45)	SFP	SFP	None (RJ-45)	SFP
Onboard memory	1 GB	1 GB	1 GB	256 MB, upgradable to 512 MB or 1 GB	256 MB, upgradable to 512 MB or 1 GB	256 MB, upgradable to 512 MB or 1 GB
Forwarding engine	DFC4A(XL)	DFC4A(XL)	DFC4A(XL)	CFC, optional DFC3B(XL) / DFC3C(XL)upgradable to DFC4A(XL)	CFC, optional DFC3B(XL) / DFC3C(XL)upgradable to DFC4A(XL)	CFC, optional DFC3B(XL) / DFC3C(XL)upgradable to DFC4A(XL)
Supported with Sup 2T	Yes	Yes	Yes	Requires CFC or DFC4A(XL)	Requires CFC or DFC4A(XL)	Requires CFC or DFC4A(XL)
Supported with Sup 720 / Sup 720 10G	No	No	No	Yes	Yes	Yes

Módulos 10GE

	Catalyst 6900 Series	Catalyst 6800 Series		Catalyst 6700 Series			
	6908-10G	6816-10G	6816-10T	6716-10G	6716-10T	6708-10G	6704-10G
Ports	8	16	16	16	16	8	4
Optics	X2, OneX adapter, SFP+	X2, OneX adapter, SFP+	None (RJ-45)	X2, OneX adapter, SFP+	None (RJ-45)	X2, OneX adapter, SFP+	XENPAK
Switch fabric connection	80 Gbps	40 Gbps	40 Gbps	40 Gbps	40 Gbps	40 Gbps	40 Gbps
Over-subscription	1:1	4:1 (1:1 performance mode)	4:1 (1:1 performance mode)	4:1 (1:1 performance mode)	4:1 (1:1 performance mode)	2:1 (1:1 performance mode)	1:1
Onboard memory	2 GB	1 GB	1 GB	1 GB	1 GB	1 GB	256 MB, upgradable to 512 MB or 1 GB

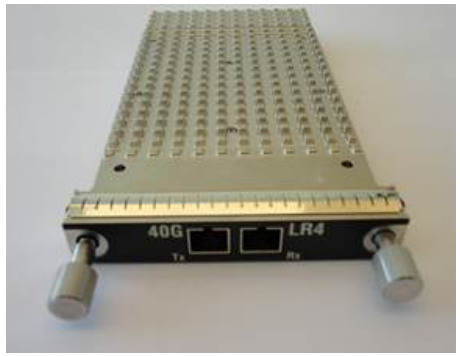
OneX Converter Module

10GBASE SFP+ Module

10GBASE X2 and Xenpak Modules

Módulos 40GE

	Catalyst 6900 Series		
	6904-40G		
	40 GE mode	10 GE mode	Mixed mode
Ports	4 x 40 GE	16 x 10 GE	2 x 40 GE 8 x 10 GE
Optics	CFP	FourX adapter, SFP+	CFP, FourX Adapter, SFP+
Switch fabric connection	80 Gbps	80 Gbps	80 Gbps
Over-subscription	2:1 (1:1 performance mode)	2:1 (1:1 performance mode)	2:1 (1:1 performance mode)
Onboard memory	2 GB	2 GB	2 GB
Forwarding engine	DFC4E(XL)	DFC4E(XL)	DFC4E(XL)
Supported with Sup 2T	Yes	Yes	Yes
Supported with other Sup	No	No	No

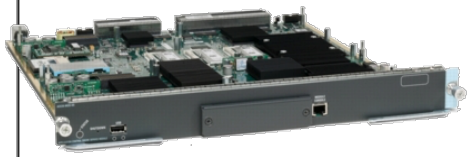


40GBASE-LR4 CFP Module

FourX converter Module con 4 puertos 10GBASE (SFP+)

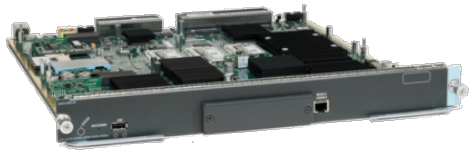
Application Control Engine Module

Features	Benefits
Available	
Application switching	The Cisco ACE Module represents the next generation of application switches, delivering tightly integrated, essential application service functions in a single powerful system. It provides load-balancing and content switching functions with granular traffic control based on customizable Layer 4 through 7 rules. • Intelligent device load balancing: Cisco ACE provides support for Domain Name System (DNS), cache, transparent caches, firewalls, intrusion detection system (IDS), intrusion prevention system (IPS), VPNs, and SSL VPN. • Generic protocol parsing (GPP): Cisco ACE has native understanding of the following protocols: HTTP, FTP, DNS, Internet Control Message Protocol (ICMP), Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), Extended RTSP, RADIUS, and Microsoft Remote Desktop Protocol (RDP). • Cisco ACE's GPP feature enables you to configure application switching and persistence policies based on any information in traffic payload for custom and packaged applications without requiring any programming. • The Cisco ACE performs payload parsing through hardware using a powerful regular-expression engine to obtain high performance, unlike other software-based solutions. • HTTP header manipulation: Cisco ACE supports the capability to modify, insert, or delete HTTP headers in both client requests and server responses. • Partial server farm failover: Cisco ACE provides the capability to determine which server farm (primary or backup) receives new traffic based on the number of available real servers (rservers.). • TCP dump: Cisco ACE can capture real-time packet information for the network traffic that passes through the Cisco ACE Module, for enhanced troubleshooting. • Source Network Address Translation (NAT) for virtual IP: Source NAT for virtual IP allows you to include a virtual IP address in the NAT pool for dynamic NAT and Port Address Translation (PAT), saving real-world IP addresses on the client-side network. • Source NAT for server farm: Source NAT can back up to a server farm multiple hops away during the failure of a primary server farm, resulting in continuous application availability even during a primary server farm failure. • Flexible network deployment: The Cisco ACE Module uses internal VLAN interfaces. VLANs can be assigned from the supervisor engine to the Cisco ACE. Corresponding VLAN interfaces then can be configured on the Cisco ACE as either routed or bridged. The Cisco ACE Module can be configured in the following modes: • Routed mode: Cisco ACE can be configured to route the traffic when the client-side and server-side VLANs are on different subnets. • Bridge mode: Cisco ACE can be configured to bridge traffic when the client-side and server-side VLANs are on the same subnets. • Asymmetric server normalization (ASN): Cisco ACE can load balance an initial request from the client to a real server; however, the server directly responds to the client, bypassing Cisco ACE.
Predictors	Cisco ACE performs a series of checks and calculations to determine the server that can best service each client request depending on the load-balancing algorithm or predictor. Cisco ACE uses the following predictors to select the best server to satisfy a client request: adaptive response, least loaded, least bandwidth, least connections, round-robin, hash address, hash cookie, hash header, and hash URL.



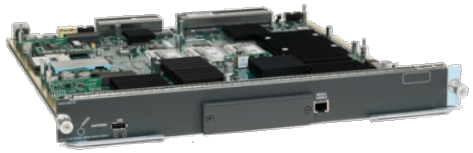
Application Control Engine Module

Server health monitoring	To instruct Cisco ACE to check the health of servers and server farms, you can configure health probes (sometimes referred to as keepalives). The following probes are supported: ICMP, TCP, UDP, ECHO {tcp | udp}, Finger, HTTP, HTTPS, FTP, Telnet, DNS, Simple Mail Transfer Protocol (SMTP), Internet Mail Access Protocol (IMAP), Post Office Protocol (POP), RADIUS, scripted, Keepalive Appliance Protocol (KAL-AP), RTSP, SIP, HTTP return-code parsing, and Simple Network Management Protocol (SNMP) probes.
Persistence and stickiness	Cisco ACE provides stickiness that allows the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session. Cisco ACE supports the following sticky methods: source or destination IP address, cookie, HTTP header, and SSL session ID.
Redundancy	The Cisco ACE Module offers three types of high availability: • Interchassis: A Cisco ACE Module in one Cisco Catalyst 6500 Series or Cisco 7600 Series device is protected by a Cisco ACE Module in a peer Cisco Catalyst 6500 Series or Cisco 7600 Series device. • Intrachassis: A Cisco ACE Module in a Cisco Catalyst 6500 Series or Cisco 7600 Series device is protected by another Cisco ACE Module in the same Cisco Catalyst 6500 Series or Cisco 7600 Series device. • Inter-virtual devices: A Cisco ACE Module supports high availability between virtual devices configured across two modules to allow specific devices to fail over without affecting the other devices and applications on a given module. Cisco ACE integrated with the Cisco Global Site Selector (GSS) can provide a multiple-data center failover system.
Fast	
User Datagram Protocol (UDP) booster	Cisco ACE can boost performance of UDP-based applications such as DNS load balancing to millions of requests per second.
UDP fast aging	Cisco ACE can provide very high scalability in terms of number of clients serviced for applications requiring a single response per request.



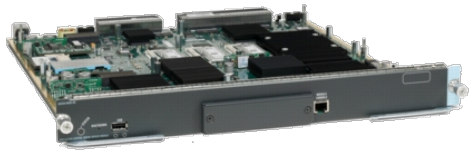
Application Control Engine Module

SSL acceleration	• The Cisco ACE solution integrates SSL acceleration technology, which offloads the encryption and decryption of SSL traffic from external devices (servers, appliances, etc.), thereby allowing the Cisco ACE to look more deeply into encrypted data and apply security and application switching policies. This enables the Cisco ACE to make more intelligent policy decisions and also helps ensure that your application-delivery platform complies with internal and external regulations. • With reencryption capabilities, Cisco ACE's SSL acceleration feature helps ensure end-to-end encryption of sensitive data while providing the capability to apply intelligent policies. • SSL features supported: SSL termination and initiation, SSL Version 3.0, Transport Layer Security (TLS) Version 1.0, back-end SSL, exportable Rivest, Shamir, and Adelman (RSA) cipher suites, session ID stickiness, SSL URL rewrite (HTTP header rewrite), session ID reuse, client authentication, HTTP header insert of client and server certificate fields and SSL session parameters, HTTP Redirect on client authentication failure, strong RSA cipher suites, and Advanced Encryption Standard (AES) cipher suites. • SSL accelerated protocols: HTTPS, Secure IMAP (IMAPS), Secure Lightweight Directory Access Protocol (LDAPS), Secure Network News Transfer Protocol (NNTPS), Secure POP Version 3 (POP3S), and Secure Telnet (STELNET) • SSL accelerated ciphers: rsa-with-rc4-128-md5, rsa-with-rc4-128-sha, rsa-with-des-cbc-sha, rsa-with-3des-ede-cbc-sha, rsa-export-with-rc4-40-md5, rsa-export-with-des40-cbc-sha, rsa-export1024-with-rc4-56-md5, sa-export1024-with-des-cbc-sha, rsa-export1024-with-rc4-56-sha rsa-with-aes-128-cbc-sha, and rsa-with-aes-256-cbc-sha • Public key exchange algorithm: RSA 512-bit, 768-bit, 1024-bit, 1536-bit, and 2048-bit • Digital certificates: All major digital certificates from certificate authorities, including the following: VeriSign, Entrust, Netscape iPlanet, Windows 2000 Certificate Server, Thawte, Equifax, and Genuity • Sample SSL key and certificate pair
TCP offloading	TCP offloading directs traffic in the most efficient manner by analyzing and directing incoming traffic at the request level. TCP offloading breaks the dependency between application requests and the transport layer. It multiplexes and demultiplexes application-level requests onto persistent connections to back-end servers. It keeps client and server TCP connections alive independent of each other and reuses TCP connections, enabling granular application layer policy and offloading TCP processing from web servers, saving CPU cycles.



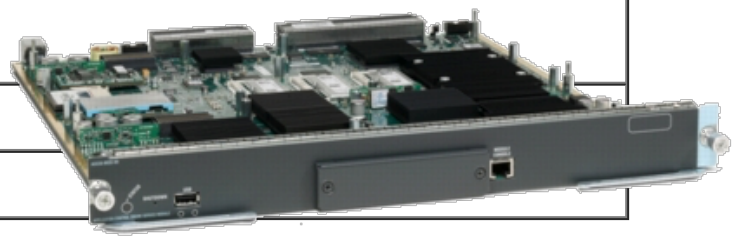
Application Control Engine Module

Features	Benefits
Secure	
Data center security	The Cisco ACE Module is designed to serve as a last line of defense for servers and applications in data centers. The data center security protects against protocol and denial-of-service (DoS) attacks and encrypts mission-critical content. The Cisco ACE data center security capabilities protect the data center and critical applications from malicious traffic with the following features: • HTTP deep packet inspection: HTTP header, URL, and payload • Bidirectional NAT and PAT • Support for static, dynamic, and policy-based NAT and PAT. • Access control lists (ACLs) to selectively allow traffic between ports • TCP connection state tracking • Virtual connection state for UDP • Sequence number randomization • TCP header validation • TCP window-size checking • Unicast Reverse Path Forwarding (URPF) checking at session establishment • ACL object grouping • TCP SYN cookies, providing distributed DoS (DDoS) protection. • Rate limiting: Cisco ACE rate limiting capabilities can be applied to a set of real servers, virtual servers, or both.
Application security	Integrated hardware-accelerated protocol control offers efficient inspection and filtering of popular data center protocols such as HTTP, RTSP, DNS, FTP, ICMP, SIP, Skinny Client Control Protocol (SCCP), and LDAP.



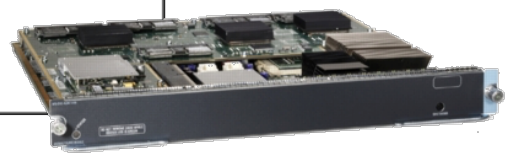
Application Control Engine Module

Feature	Maximum Performance and Configuration
Global Parameters	
Throughput	16 Gbps*, 8 Gbps*, and 4 Gbps
Syslogs per second	350,000
Global Configuration	
Total VLANs (client and server)	4000
Probes	ICMP, TCP, UDP, Echo, Finger, DNS, Telnet, FTP, HTTP, HTTPS, SMTP, POP3, IMAP, RTSP, RADIUS, SIP, SNMP, KAL-AP, and TCL Scripts
NAT entries	1 million
Virtual partitions	Up to 250*; 5 virtual partitions (devices) included in base price
SSL Performance	
SSL throughput	3.3 Gbps
SSL TPS	1000 TPS included in base price, and 5000, 10,000, or 15,000 TPS with licensing
Application Switching Performance	
Maximum connections per second	325,000 complete transactions sustained rate
Concurrent connections	4 million
Sticky table entries	4 million

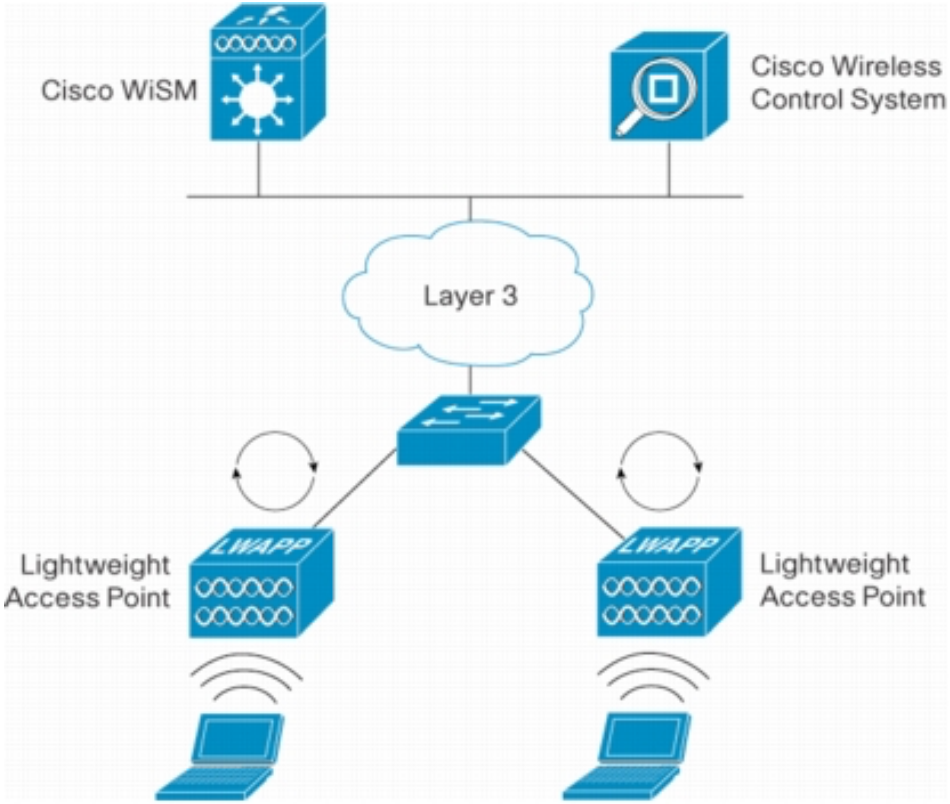


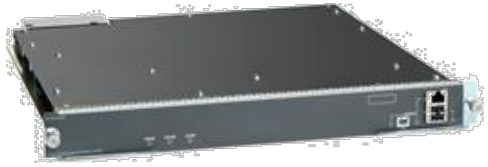
Anomaly Guard Module

Feature	Description
Attack Protection	• Spoofed and non-spoofed attacks • TCP (syns, syn-acks, acks, fins, fragments) attacks • User Datagram Protocol (UDP) attacks (random port floods, fragments) • Internet Control Message Protocol (ICMP) attacks (unreachable, echo, fragments) • Domain Name System (DNS) attacks • Client attacks • Inactive and total connections attacks • HTTP Get Flood attacks • Border Gateway Protocol (BGP) attacks • Session Initiation Protocol (SIP) voice over IP (VoIP) attacks
Continuous Learning and Protection	• Can operate in continuous learning and protection mode (Release 5.0 and later) • Simultaneously adjusts thresholds and protect from attacks • Switches between learning and protection modes automatically • Returns to learning mode after an attack is completed
Traffic Analysis	• Ability to capture and packets that are traversing the guard and save them as pcap files. • The GUI allows extensive analysis of the captured packets. • The user may limit capture to packets with a certain decision value only (forward, drop, reply). • The user may filter the capture using a tcpdump expression.
Signature Extraction-Deep Packet Inspection	• Ability to find prominent patterns in the payload of captured packets • Automated algorithm analyzes packet capture to extract a signature found only in malicious packets • Content-based filter can be applied for extracted signature
Content-Based Filter	• Provides ability to look for patterns in the payload • Can define multiple content-based filters • Can be configured to either just count packets, or drop them



Wireless Services Module 2



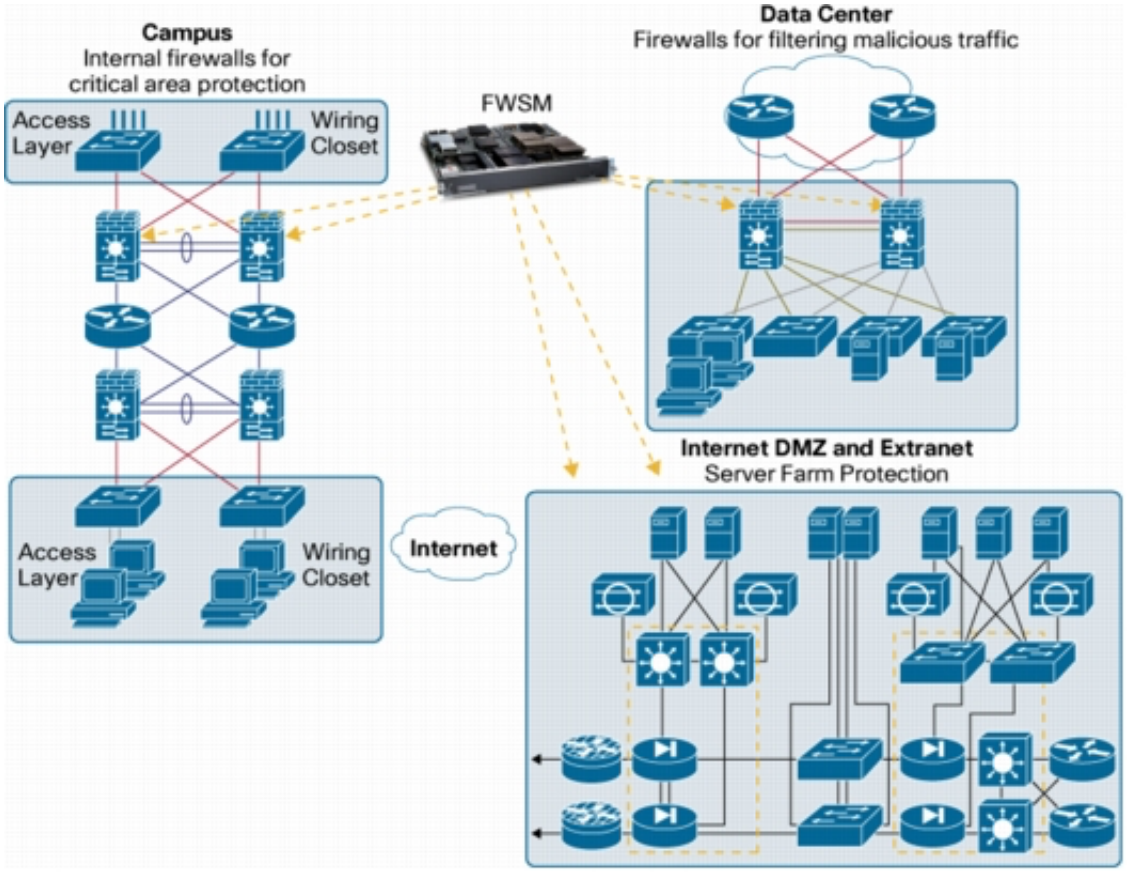


Wireless Services Module 2

Feature	Benefits
Scalability	• Supports 100, 300, 500 and 1000 access points for business-critical wireless services at locations of all sizes
High Performance	• Wired-network speed, nonblocking performance for 802.11n and optimized for 802.11ac networks
RF Management	• Provides both real-time and historical information about RF interference impacting network performance across controllers, through systemwide Cisco CleanAir technology integration
High-Performance Video	• Integrates Cisco VideoStream technology as part of the Cisco medianet framework to optimize the delivery of video applications across the WLAN
End-to-End Voice	• Supports Unified Communications for improved collaboration through messaging, presence, and conferencing • Supports all Cisco Unified IP Phones for cost-effective, real-time voice services
Comprehensive End-to-End Security	• Offers control and provisioning of wireless access points (CAPWAP)-compliant Datagram Transport Layer Security (DTLS) encryption to help ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links
Cisco OfficeExtend	• Supports corporate wireless services for mobile and remote workers with secure wired tunnels to the Cisco Aironet 600, 1130, or 1140, 3500, 3600 Series Access Points • Extends the corporate network to remote locations with minimal setup and maintenance requirements (zero-touch deployment) • Improves productivity and collaboration at remote site locations • Separate service set identifier (SSID) tunnels allow both corporate and personal Internet access • Reduced carbon dioxide emissions from a decrease in commuting • Higher employee job satisfaction from ability to work at home • Improves business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather
Cisco Enterprise Wireless Mesh	• Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network • Available on select Cisco Aironet access points, Cisco Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing

CAPWAP = Control And Provisioning of Wireless Access Points (RFC 5415)

Firewall Services Module



Firewall Services Module

	Capacities
Performance	• 5.5 Gbps throughput per service module • Up to 4 FWSMs (20 Gbps) per Catalyst 6500 chassis with static VLAN or IOS Policy-based Routing • 2.8 Mpps • 1 million concurrent connections • 100,000 connection setups and teardowns per second • 256,000 concurrent NAT or PAT translations • Jumbo Ethernet packets (8500 bytes) supported
VLAN Interfaces	• 1000 total per service module • 256 VLANs per security context in routed mode • 8 VLAN pairs per security context in transparent mode
Access Lists	• Up to 80,000 Access Control Entries in single context mode • Note: the FWSM implements Layer 3 and 4 access control security checks in hardware with virtually no performance impact using non-upgradeable high-speed memory
Virtual Firewalls (Security Contexts)	• 20, 50, 100, 250 Virtual Firewall licenses • 2 Virtual Firewalls and 1 administrative context are provided for testing purposes.

Firewall Services Module

Features	Summary
Scalable Architecture to Support Up to 20+ Gbps of Firewall Services within the Catalyst 6K Infrastructure	• A variety of industry proven clustering techniques deliver a seamless method to scale firewall performance to 20 Gbps and beyond.
Visibility into Encrypted Threats	• Leveraging SSL decryption capabilities within the Catalyst 6K infrastructure, the FWSM has the ability to gain visibility into encrypted policy violations to which traditional firewalls have no visibility.
Intelligent Network Services	• Layer 2 Firewall (transparent mode) with NAT and PAT support • Layer 2 Firewall (transparent mode) with NAT and PAT support • Layer 3 Firewall (route and/or NAT mode) • Mixed Layer 2 and Lyer 3 firewall per FWSM • Dynamic/static NAT and PAT • Policy-based NAT • VRF-aware NAT • Destination NAT for Multicast • Static routing support in signle- and multiple security content mode • Dynamic routing in single security context mode: Open Shortest Path First (OSPF). Routing Initiation Protocol (RIP) v1 and v2, PIM Sparse Mode v2 multicast routing, Internet Group Management Protocol (IGMP) v2. • Dynamic routing in single and virtual security context mode using stub iBGP (Licensed feature) • Transparent mode supports static routing only • Private VLAN for L2 and L3 firewall enables firewall security policies between isolated ports. • Asymmetric routing supporting without redundancy by using asymmetric routing groups • IPv6 networking and management access using IPv6 HTTPS, Secure Shell Protocol (SSH) v1 and v2, and Telnet

Firewall Services Module

Core Stateful Firewall	• NAT Translate bypass enhances scalability by not creating NAT translate entries when no NAT-control or NAT except is used • Selective TCP State Bypass on a per flow basis • Timeout on a per flow for TCP and non-TCP flows • ACLs: Extended ACL for IP traffic, Ethertype ACL for non-IP traffic, standard ACL for OSPF route distribution, per-user Cisco Secure Access Control Server (ACS)-based ACLs, per-user ACL override, object fgrouping for ACLs, time-based ACLs • Cisco Modular Policy Framework (MPF) with flow-based security policies • Cut-through user authentication proxy with local database and external AAA server support: TCP, HTTP, FTP, HTTPS, and others • URL filtering: Filter HTTP, HTTPS, and FTP requests by Websense Enterprise or HTTP filtering by N2H2 (now part of Secure Computing Corporation) • Same security-level communication between VLANs (without NAT/static policies) and per-host maximum connection limit • Protection from denial of service (DoS) attacks: DNS Guard, Flood Defender, Flood Guard, TCP Intercept with SYN cookies organization, Unicast Reverse Path Forwarding (uRPF), Mail Guard, FragGuard and Virtual Reassembly, Internet Control Message Protocol (ICMP) stateful inspection, User Datagram Protocol (UDP) rate control, TCP stream re-assembly and deobfuscation engine, TCP traffic normalization services for attack detection • Address Resolution Protocol (ARP) inspection in transparent firewall mode • DHCP server, DHCP relay to upstream router with per interface configuration

Firewall Services Module

Features	Summary
Service Virtualization (Multiple Security Context Mode)	• Transparent • Routed Mode • NAT/PAT • ACL • Protocol Inspection • SNMP • Syslog • DHCP • Resource management controls resource usage per security context
Inspection Engines	• Application policy enforcement • Protocol conformance checking • Protocol state tracking • Security checks • NAT/PAT support • Dynamic port allocation • Core internet protocols: HTTP, FTP, Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP), DNS, Extended DNS (EDNS), ICMP, TCP, UDP • Database/OS services: Internet Locator Services/Lightweight Directory Access Protocol (ISL/LDAP), Oracle/SQL*Net v1 and v2, NetBIOS over IP, NFS, Remote Shell Protocol (RSH), sUNrpc/nis+, XWindows (SDMCP), Registration Admission and Status (RAS) v2 • Multimedia/VoIP: H.323 v1–4, H.323 Gatekeeper Cluster GUP message support, Session Initiation Protocol (SIP), SCCP (Skinny), Skinny Video, GPRS Tunneling Protocol (GTP) v0 and v1 (3G Mobile Wireless), Media Gateway Control Protocol (MGCP) v0.1 and v1.0, Real-Time Streaming Protocol (RTSP), Telephony Application Programming Interface (TAPI) and Java TAPI (JTAPI) T.38 Fax over IP, Gatekeeper Routed Control Signaling (GKRCS), fragmented and segmented multimedia stream inspection • Specific applications: Microsoft Windows Messenger, Microsoft NetMeeting, Real Player, Cisco IP phones, Cisco SoftPhone • Security services: Point-to-Point Tuneling Protocol (PPTP)
High Availability	• Intrachassis and interchassis • Active-Standby stateful failover • Active-Active stateful failover support in multiple context mode • Asymmetric routing support with Active-Active redundancy
Application Inspection Control	• Advanced HTTP inspection services: RFC compliance checking for protocol anomaly detection, HTTP command filtering, MIME type filtering content validation, Uniform Resource Identifier (URI) length enforcement, and more • Tunneling application control: AOL Instant Messenger, Microsoft Messenger, Yahoo Messenger, peer-to-peer applications (such as KaZaA and Gnutella), and other applications (such as GoToMyPC)

Ejemplo: HPE 5400 zl

Chassis

- 6 ó 12 slots

Ports	6 open module slots Supports a maximum of 48 10GbE ports or 144 autosensing 10/100/1000 ports or 144 mini-GBICs, or a combination	12 open module slots Supports a maximum of 96 10GbE ports or 288 autosensing 10/100/1000 ports or 288 mini-GBICs, or a combination
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	4 power supply slots 2 minimum power supplies required (ordered separately)
Memory and processor		
Gigabit module	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM	ARM9 @ 200 MHz; packet buffer size: 144 Mb QDR SDRAM
10G module	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM	ARM9 @ 200 MHz; packet buffer size: 36 Mb QDR SDRAM
Management module	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash, 128 MB compact flash, 256 MB DDR SDRAM	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash, 128 MB compact flash, 256 MB DDR SDRAM
Performance		
1000 Mb Latency	< 3.7 µs (FIFO 64-byte packets)	< 3.7 µs (FIFO 64-byte packets)
10 Gb/s Latency	< 2.1 µs (FIFO 64-byte packets)	< 2.1 µs (FIFO 64-byte packets)
Throughput	up to 282.1 million pps	up to 564.2 million pps
Routing/Switching capacity	379.2 Gb/s	758.4 Gb/s
Switch fabric speed	379.2 Gb/s	758.4 Gb/s
Routing table size	10000 entries (IPv4), 5000 entries (IPv6)	10000 entries (IPv4), 5000 entries (IPv6)
MAC address table size	64000 entries	64000 entries

http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA2-6511ENW

QoS

- Advanced classifier-based QoS

  Classifies traffic using multiple match criteria based on L2, L3, and L4 information; and applies QoS policies such as setting the priority level and rate limiting to selected traffic on a per-port or per-VLAN basis

- L4 prioritization

  Enables prioritization based on TCP/UDP port numbers

- Traffic prioritization

  Allows real-time traffic classification into eight priority levels that are mapped to eight queues

- Bandwidth shaping

  - Port-based rate limiting

    Enabled per-port ingress/egress-enforced bandwidth increase

  - Classifier-based rate limiting

    Uses an access control list (ACL) to enforce increased bandwidth for ingress traffic on each port

  - Reduced bandwidth

    Provides per-port per-queue egress-based bandwidth reduction

- Class of service (CoS)

  Sets the IEEE 802.1p priority tag based on the IP address, IP type of service (ToS), L3 protocol, TCP/UDP port number, source port, and DiffServ

Gestión

- Remote intelligent mirroring

  Mirrors selected ingress/egress traffic based on an ACL, port, MAC address, or VLAN to a local or remote HPE 8200 zl, 6600, 6200 yl, 5400 zl, or 3500 switch anywhere on the network

- Remote monitoring (RMON), Extended RMON (XRMON), and sFlow v5

  Provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events

- IEEE 802.1ab link-layer discovery protocol (LLDP)

  Advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications

- Unidirectional link detection (UDLD)

  Monitors the cable between two switches and shuts down the ports on both ends if the cable is broken, turning the bidirectional link into a unidirectional one; this helps prevent network problems such as loops

- Management simplicity

  Provides common software features and CLI implementation across all ProVision-based switches (including the zl and yl switches)

- Command authorization

  Leverages the RADIUS to link a custom list of CLI commands to an individual network administrator's login; an audit trail documents the activity

- Friendly port names

  Allows assignment of descriptive names to ports

- Dual flash images

  Provides independent primary and secondary operating system files for backup while upgrading

- Multiple configuration files

  Are easily stored with a flash image

Conectividad

- Jumbo frames

  Allow high-performance remote backup and disaster-recovery services on GbE and 10GbE ports

- Auto-MDIX

  Provides automatic adjustments for straight-through or crossover cables on all 10/100 and 10/100/1000 ports

- IPv6

  - IPv6 host

    Enables switches to be managed in an IPv6 network

  - Dual stack (IPv4 and IPv6)

    Provides the transition mechanism from IPv4 to IPv6; and supports connectivity for both protocols

  - MLD snooping

    Forwards IPv6 multicast traffic to the appropriate interface

  - IPv6 ACL/QoS

    Supports ACL and QoS for IPv6 network traffic

  - IPv6 routing

    Supports static and open standard path first (OSPF) v3 routing protocols

  - 6-in-4 tunneling

    Supports encapsulation of IPv6 traffic in IPv4 packets

  - Security

    Provides RA guard, DHCPv6 protection, dynamic IPv6 lockdown

Resiliency and high availability

- Virtual router redundancy protocol (VRRP)

  Allows groups of two routers to dynamically back each other up to create highly available routed environments for IPv4 and IPv6 networks

- Multiple spanning tree protocol (STP) and IEEE 802.1s

  Offers high link availability in multiple VLAN environments by allowing multiple spanning trees; encompasses IEEE 802.1d STP and IEEE 802.1w Rapid STP

- IEEE 802.3ad link-aggregation-control protocol (LACP) and HPE port trunking

  Support up to 144 trunks, each with up to eight links (ports) per trunk

- Distributed trunking

  Enables loop-free and redundant network topology without using STP; and allows a server or switch to connect to two switches using one logical trunk for redundancy and load sharing

- Optional redundant power supply (With the 5400 Switch Series)

  Provides uninterrupted power supply; and allows hot swapping of the redundant power supplies when installed

- Hot-swappable modules (with the 5400 zl Switch Series)

  Allows modules, mini-GBICs, and power supplies in a redundant power supply configuration to be added or swapped without interrupting the network

L2 switching

L2 switching

- VLAN support and tagging

  Supports the IEEE 802.1Q standard and 2,048 VLANs simultaneously

- IEEE 802.1v protocol VLANs

  Isolate select non-IPv4 protocols automatically into their own VLANs

- GARP VLAN registration protocol

  Allows automatic learning and dynamic assignment of VLANs

- IEEE 802.1ad Q-in-Q

  Increases the scalability of an Ethernet network by providing a hierarchical structure; and connects multiple LANs on a high-speed campus or metro network

- MAC-based VLAN

  Provides granular control and security; and uses the RADIUS to map a MAC address/user to specific VLANs (requires v2 modules)

- Rapid per-VLAN spanning tree (RPVST+)

  Allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+

- Hewlett Packard Enterprise switch meshing

  Enables dynamic load balancing across multiple active redundant links to increase the aggregate bandwidth availability; and allows concurrent L3 routing with v2 modules

L3

- User datagram protocol (UDP) helper function

  Allows UDP broadcasts to be directed across router interfaces to specific IP unicast or subnet broadcast addresses; and helps prevent server spoofing for UDP services such as DHCP

- Loopback interface address

  Defines an address in the routing information protocol (RIP) and OSPF, improving the diagnostic capability

- Route maps

  Provide more control during route redistribution; and allow filtering and altering of route metrics

- **NEW** DHCP server

  Centralizes and reduces the cost of IPv4 address management

- Static IP routing

  Provides manually configured routing for both IPv4 and IPv6 networks

- RIP

  Includes RIPv1 and RIPv2 routing

- OSPF

  Provides OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing

- Policy-based routing

  Uses a classifier to select traffic that can be forwarded based on the policy set by the network administrator (requires v2 modules)

- IPv4 border gateway routing protocol

  Is scalable, robust, and flexible

Security

- ACLs

  Provide filtering based on the IP field, source/destination IP address/subnet and source/ destination TCP/UDP port number on a per-VLAN or per-port basis

- Multiple user authentication methods

  - IEEE 802.1X users per port

    Enables authentication of multiple IEEE 802.1X users per port

  - Web-based authentication

    Authenticates from the Web browser for clients that do not support the IEEE 802.1X supplicant

  - MAC-based authentication

    Provides client authentication with a RADIUS server, based on the client's MAC authentication

  - Concurrent IEEE 802.1X, Web, and MAC authentication schemes per port

    Allows a switch port to accept up to 32 sessions of IEEE 802.1X, Web, and MAC authentications

- Virus throttling

  Detects traffic patterns typical of worm-type viruses; and either throttles or helps entirely prevent the virus from spreading across the routed VLANs or bridged interfaces without requiring external appliances

- DHCP protection

  Blocks DHCP packets from unauthorized DHCP servers, mitigating denial-of-service attacks

- Secure management access

  Delivers secure encryption of all access methods (CLI, GUI, and MIB) through SSHv2, SSL, and/or SNMPv3

- Switch CPU protection

  Provides automatic protection against malicious network traffic trying to shut down the switch

- ICMP throttling

  Defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic

Security

- Identity-driven ACL

  Enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user

- STP bridge protocol data units (BPDUs) port protection

  Blocks BPDUs on ports that do not require BPDUs, mitigating forged BPDU attacks

- Dynamic IP lockdown

  Works with DHCP protection to block traffic from unauthorized hosts, mitigating IP source address spoofing

- Dynamic ARP protection

  Blocks ARP broadcasts from unauthorized hosts, helping prevent eavesdropping or theft of network data

- STP root guard

  Protects the root bridge from malicious attacks or configuration mistakes

- Port security

  Allows access only to specified MAC addresses, which can be learned or specified by the administrator

- MAC address lockout

  Helps prevent certain configured MAC addresses from connecting to the network

- Source-port filtering

  Allows only specified ports to communicate with each other

- RADIUS/TACACS+

  Eases switch management security administration by using a password authentication server

Security

- Secure shell (SSH)

  Encrypts all transmitted data for secure remote CLI access over IP networks

- Secure sockets layer (SSL)

  Encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch

- Secure FTP

  Allows secure file transfer to and from the switch; and protects against unwanted file downloads or unauthorized copying of a switch configuration file

- Management interface wizard

  Helps secure management interfaces such as SNMP, telnet, SSH, SSL, Web, and USB at the desired level

- Switch management logon security

  Helps secure switch CLI logon by optionally requiring either RADIUS or TACACS+ authentication

- Security banner

  Displays a customized security policy when users log in to the switch

Convergence

- IP multicast routing

  Includes PIM sparse and dense modes to route IP multicast traffic

- IP multicast snooping (data-driven IGMP)

  Helps prevent flooding of IP multicast traffic

- LLDP-media endpoint discovery (MED)

  Defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones

- PoE allocations

  Supports multiple methods—automatic, IEEE 802.3af class, LLDP-MED, or user specified—to allocate PoE power for more efficient energy use

- Auto VLAN configuration for voice

  - RADIUS VLAN

    Uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones

  - CDPv2

    Uses CDPv2 to configure legacy IP phones

- Local MAC authentication

  Assigns attributes such as VLAN and QoS, using a locally configured profile that can be a list of MAC prefixes