

Cisco Catalyst 6500: Continued Innovations... Continuous Success



ENABLE NEW SERVICES WITH INTEGRATED SERVICES MODULES

Cisco Catalyst 6500 Series Switches Service Integration

Cisco® Catalyst® 6500 Series Switches provide a scalable and high-performance platform on which services from the network to the applications level can be enabled for every port, allowing for reduced total cost of ownership (TCO) while obtaining high performance and innovative and secured IP services. Benefits will be realized in four primary areas:

Infrastructure Simplification

- Network integration: Shared functionality and collaborative processes between the switch and service modules greatly simplify network design and enable innovative capabilities.
- Virtualization: Allows network managers capability to configure, deploy, and manage network functions on a single device as if they were separate devices. Resource manager allocates resources per virtual context to help ensure high availability.
- Enhanced manageability: Provides the flexibility of centralized configuration.
- High availability across all service modules without the need for external cabling or multiple, redundant stand-alone devices.

Maximum Return on Network Investment

- Investment protection: All service modules use existing infrastructure and administrator expertise to deliver new services.

- Simplified maintenance and management: Integration of service modules into one chassis allows for ease of use and support for network administrators. Role-based remote access control fosters collaboration for IT managers.
- Reduced environmental and operating costs and complexity: Integrated services reduce overall power, cabling, and rack space compared to standalone devices.

Services Innovation

- Industry-leading scalability and performance.
- Complements Layer 2-3 platform services with Layer 4-7 intelligent and application-aware services.
- Services convergence enhances performance, application, and security services, monitoring, reporting, and configuration.

Pervasive Security

- Broad protection suite: Security modules provide a comprehensive set of high-performance security services within the Cisco Catalyst 6500 Series chassis.
- End-to-end security: Protect all layers of network by enforcing granular security policies.
- Every port is a security port within the platform.

Cisco Catalyst 6500 Series Switches
Industry's most successful networking platform,
surpassing \$20 billion in sales since its introduction
in 1999.

Figure 1. Cisco Catalyst 6500 Series Switches



As the premier Cisco modular LAN switching platform, Cisco Catalyst 6500 Series Switches offer high levels of availability and integrated security, strong support for converged applications, superior operational efficiency, leading scalability, high flexibility, and superior long-term investment protection among Cisco switching products designed for medium-sized business, enterprise, and service provider networks. The flexible range of Cisco Catalyst 6500 Series options makes this platform ideal for networkwide deployments, from the data center to the wiring closet.

The Cisco Catalyst 6500 Series continues to provide innovations for high-end LAN switching, including:

- High availability
- High level of integrated security
- Strong support for converged applications
- Superior operational efficiency



- Leading scalability and flexibility
- Long-term investment protection

The Right Solution for Your Business Needs

Enterprise networks have become increasingly complex as multiple systems supporting new technologies and applications are added to the basic infrastructure over time. The Cisco Catalyst 6500 platform addresses the challenge of reducing network complexity through an integrated services module architecture. The modular switching and service application solution eliminates the need to purchase, manage, and maintain specialized appliances or redesign the network to incorporate new technologies and services.

Integrated services modules are available in five main technology areas to fit the needs of your business:

Security

- Cisco Catalyst 6500 Series ASA Services Module
- Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module
- Cisco Catalyst 6500 Series IP Security (IPsec) VPN Shared Port Adapter (SPA)
- Cisco IOS® Secure Sockets Layer (SSL) VPN Services Module (WebVPN SM)
- Distributed-Denial-of-Service (DDoS) Traffic Anomaly Guard Service Modules (ADM, AGM)

Application Networking Services

- Application Control Engine (ACE)
- Application-Oriented Networking (AON) Module

Network Monitoring

- Network Analysis Modules (NAM-1, NAM-2)

Wireless

- Wireless Services Module (WiSM)

IP Communications

- Communication Media Module (CMM)

Table 1. Cisco Catalyst 6500 Series Services Modules

| Component | Description |
|----------------------------|--|
| ASA Services Module | <ul style="list-style-type: none"> • Exceptional scalability: Supports up to four times the session count of other network security modules – scaling up to 10 million concurrent sessions. Also supports 250 security contexts and 1,000 VLANs. Up to four ASA Services Modules can be used, scaling to provide up to 64Gbps in a single chassis. • Unmatched performance: Delivers the fastest firewall data rates in the industry, with 16 Gbps of multi-protocol firewall throughput. Also delivers 300,000 connections per second – more than twice the performance of the nearest competitor. • Leading-edge security: Uses the Cisco ASA platform, the most widely deployed firewall in the industry, to provide exceptional security protection at Layers 2-7. Delivers advanced firewall capabilities, including application and protocol inspections. • Superior ROI: Builds on the existing network to take advantage of the infrastructure to deliver new services. Full firewall capabilities can be added by sliding a blade into an empty slot in the existing Catalyst 6500 Series switch – no additional rack space, cabling, power, or physical interfaces are required. |
| IDSM-2 | <ul style="list-style-type: none"> • High performance: 500 Mbps per IDSM, multigigabit (up to eight IDSMs per chassis) with Cisco EtherChannel load balancing • Thousands of dynamic signatures: Integrates with Trend Micro Outbreak Prevention Service • Day-zero protection: Knowledge base anomaly detection to prevent worm propagation • Endpoint collaboration: Provides the ability to use contextual analysis from Cisco AnyConnect™ Secure Mobility Client • Multivector threat identification and accurate inline prevention, with risk rating and metaevent correlation |
| IPsec VPN SPA | <ul style="list-style-type: none"> • High performance: 2.5 Gbps of AES and 3DES IPsec, 8000 tunnels, 10 SPAs per chassis, 25 Gbps, 5 million pps • Next-generation encryption: Includes all key sizes (128-, 192-, and 256-bit keys) • Attractive form factor: Half-slot form factor reduces slot consumption and increases total performance per slot |



| Component | Description |
|-------------------------|---|
| WEBVPN SM | <ul style="list-style-type: none"> High performance: 8000 tunnels; 32,000 maximum connections; 300 Mbps throughput; 128 virtual contexts; 356 certificates; up to four WebVPN Services Modules per chassis Clientless, port forwarding, and full tunnel support |
| Traffic ADM, AGM | <ul style="list-style-type: none"> High performance: One 1-Gbps interface; 1.5 million concurrent connections; 150,000 dynamic filters; less than 1 ms latency or jitter Detects and mitigates the broadest range of DDoS attacks Behavioral anomaly recognition: Helps ensure accuracy to forward legitimate transactions |
| NAM-1, NAM-2 | <ul style="list-style-type: none"> LAN and WAN monitoring: Gain visibility into the LAN and WAN and troubleshoot “hot spots” in remote parts of the network, all from one device Quick to deploy and use: access the NAM’s embedded Web-based GUI at any time and from any desktop to view easy-to-read performance reports on data, voice, and video traffic. Collect data from multiple NAMs using Cisco Performance Visibility Manager for consolidated monitoring, reporting, and troubleshooting Help assure the integrity of network traffic: analyze network data to plan and manage the growth of a secure worldwide network, applications, and services |
| ACE Module | <ul style="list-style-type: none"> Centralized control: virtual partitions and role-based access control enable IT simplification of the deployment and management of applications while allowing individual groups to administer and manage their own network application infrastructure Industry-leading application and device performance: 4-8-16-Gbps throughput software licensed in the single module and 345,000 L4 sustained connection setups per second to handle large-scale operations IRich levels of security: many security features, including SSL encryption/decryption, ACLs, TCP header validation, checks for protocol compliance, transaction logging and reporting for security forensics |
| WiSM | <ul style="list-style-type: none"> Enterprise reliability: in the event of an access point failure, the Cisco WiSM automatically adjusts power on adjacent lightweight access points to cover the area where the failed access point provided service Multiple redundancy options: maximize network uptime for wireless traffic Intelligent RF management: Cisco WiSM comes equipped with embedded software for adaptive real-time RF management |
| AON Module | <ul style="list-style-type: none"> Security: to enforce application security policy within the network, Cisco AON provides a set of services that help enable message-level access and control Visibility: because Cisco AON can act as a network interception point for application message traffic, each node can be configured to act as a sensor that can capture, process, and log highly granular information about application messages Intelligent message routing: AON provides rich application message-level services, including content-based routing, content transformation and protocol translation |
| CMM | <ul style="list-style-type: none"> Cisco Unified CallManager redundancy: use the robust, fault-tolerant architecture of clustered Cisco Unified CallManager systems Survivable Remote Site Telephony (SRST): Increases network resiliency by allowing the Cisco CMM to manage connections temporarily for Cisco IP phones when a connection to Cisco CallManager is unavailable |