

## 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 security services within the Cisco Catalyst 6500 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

- Firewall Services Module (FWSM)
- Intrusion Detection System Services Module (IDSM-2)
- IP Security (IPsec) VPN Shared Port Adapter (SPA)
- 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)



# Cisco Catalyst 6500: Continued Innovations...Continuous Success At-A-Glance

## Enable New Services with Integrated Services Modules

Table 1. Cisco Catalyst 6500 Series Services Modules

Component	Description
<b>FWSM</b>	<ul style="list-style-type: none"> <li>High performance and scalability: 5 Gbps; 2.8M pps; 1M concurrent connections; 100,000 cps; 250 virtual firewalls; 80,000 access control lists (ACLs); 1000 VLANs; 4 FWSMs per chassis</li> <li>Stateful-inspection firewall: tracks the state of all network communications and prevents unauthorized access</li> <li>Virtual firewalls: provides all firewall policies, monitoring, and logging to each virtual firewall, including resource management to limit resource usages</li> <li>Application and protocol inspection engines: examine network flows at Layers 4–7, including protection for port 80 misuse, IM, P2P, VoIP, and multimedia</li> <li>Superior network integration: transparent Layer 2 firewall combined with Layer 3 firewall, integration with VRF, private VLAN, intra- and inter-chassis active-active and Active-Standby failover and other Catalyst 6500 network infrastructure capabilities</li> </ul>
<b>IDS-2</b>	<ul style="list-style-type: none"> <li>High performance: 500 Mbps per IDS, multigigabit (up to 8 IDSs per chassis) with Cisco EtherChannel® load balancing</li> <li>Thousands of dynamic signatures: integrates with Trend Micro Outbreak Prevention Service</li> <li>Day-zero protection: knowledge base anomaly detection to prevent worm propagation</li> <li>Endpoint collaboration: provides the ability to use contextual analysis from Cisco Security Agent</li> <li>Multivector threat identification and accurate inline prevention: with risk rating and metaevent correlation</li> </ul>
<b>IPsec VPN SPA</b>	<ul style="list-style-type: none"> <li>High performance: 2.5 Gbps of AES and 3DES IPsec, 8000 tunnels, 10 SPAs per chassis, 25 Gbps, 5M pps</li> <li>Next-generation encryption: includes all key sizes (128-, 192-, and 256-bit keys)</li> <li>Attractive form factor: half-slot form factor reduces slot consumption and increases total performance per slot</li> </ul>
<b>WEBVPN SM</b>	<ul style="list-style-type: none"> <li>High performance: 8000 tunnels; 32,000 maximum connections; 300 Mbps throughput; 128 virtual contexts; 356 certificates; up to 4 WEBVPN SMs per chassis</li> <li>Clientless, port forwarding, and full tunnel support</li> </ul>
<b>Traffic ADM, AGM</b>	<ul style="list-style-type: none"> <li>High performance: one 1-Gbps interface; 1.5M concurrent connections; 150,000 dynamic filters; less than 1 ms latency or jitter</li> <li>Detects and mitigates the broadest range of DDoS attacks</li> <li>Behavioral anomaly recognition: helps ensure accuracy to forward legitimate transactions</li> </ul>
<b>NAM-1, NAM-2</b>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>Help assure the integrity of network traffic: analyze network data to plan and manage the growth of a secure worldwide network, applications, and services</li> </ul>
<b>ACE Module</b>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> </ul>
<b>WiSM</b>	<ul style="list-style-type: none"> <li>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</li> <li>Multiple redundancy options: maximize network uptime for wireless traffic</li> <li>Intelligent RF management: Cisco WiSM comes equipped with embedded software for adaptive real-time RF management</li> </ul>
<b>AON Module</b>	<ul style="list-style-type: none"> <li>Security: to enforce application security policy within the network, Cisco AON provides a set of services that help enable message-level access and control</li> <li>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</li> <li>Intelligent message routing: AON provides rich application message-level services, including content-based routing, content transformation and protocol translation</li> </ul>
<b>CMM</b>	<ul style="list-style-type: none"> <li>Cisco Unified CallManager redundancy: use the robust, fault-tolerant architecture of clustered Cisco Unified CallManager systems</li> <li>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</li> </ul>