

CISCO CATALYST 2960 SERIES SWITCHES

Ethernet and Gigabit Ethernet connectivity, enabling enhanced LAN services for entry-level enterprise, mid-market, and branch office networks.
The Catalyst 2960 Series offers integrated security, including network admission control (NAC), advanced quality of service (QoS), and resiliency
to deliver intelligent services for the network edge.
The Cisco Catalyst 2960 Series offers:

- Intelligent features at the network edge, such as sophisticated access control lists (ACLs) and enhanced security
- Dual-purpose uplinks for Gigabit Ethernet uplink flexibility, allowing use of either a copper or a fiber uplink—each dual-purpose uplink port has
one 10/100/1000 Ethernet port and one Small Form-Factor Pluggable (SFP)-based Gigabit Ethernet port, with one port active at a time
- Network control and bandwidth optimization using advanced QoS, granular rate limiting, ACLs, and multicast services
- Network security through a wide range of authentication methods, data encryption technologies, and network admission control based on users,
ports, and MAC addresses
- Easy network configuration, upgrades, and troubleshooting using Cisco Network Assistant software
- Auto-configuration for specialized applications using Smartports

CONFIGURATIONS

The Cisco Catalyst 2960 Series comprises the following switches (Figure 1):

- Cisco Catalyst 2960-24TT: 24 Ethernet 10/100 ports and 2 fixed Ethernet 10/100/1000 uplink ports; 1 rack unit (RU)
- Cisco Catalyst 2960-48TT: 48 Ethernet 10/100 ports and 2 fixed Ethernet 10/100/1000 uplink ports; 1 RU
- Cisco Catalyst 2960-24TC: 24 Ethernet 10/100 ports and 2 dual-purpose uplink ports; 1 RU
- Cisco Catalyst 2960-48TC: 48 Ethernet 10/100 ports and 2 dual-purpose uplink ports; 1 RU
- Cisco Catalyst 2960G-24TC: 24 Ethernet 10/100/1000 ports, 4 of which are dual-purpose; 1 RU

Figure 1. Cisco Catalyst 2960 Series Switches



The Cisco Catalyst 2960 Series software image is a rich suite of intelligent services, including advanced QoS, rate limiting, and ACLs. The SFPbased
Gigabit Ethernet ports accommodate a range of SFP transceivers, including the Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-BX,
1000BASE-ZX, 100BASE-FX, 100BASE-LX10, 100BASE-BX, and coarse wavelength-division multiplexing (CWDM) SFP transceivers.

GIGABIT ETHERNET

At speeds of 1000 Mbps, Gigabit Ethernet provides the bandwidth to meet new and evolving network demands, alleviate bottlenecks, and boost
performance while increasing the return on existing infrastructure investments. Today's workers are placing higher demands on networks, running
multiple concurrent applications. For example, a worker joins a team conference call through an IP videoconference, sends a 10-MB spreadsheet to
meeting participants, broadcasts the latest marketing video for the team to evaluate, and queries the customer relationship management (CRM)
database for the latest real-time feedback. Meanwhile, a multigigabyte system backup starts in the background and the latest virus updates are
delivered to the client.

ENHANCED SECURITY

The wide range of security features that the Cisco Catalyst 2960 Series offers helps businesses protect important information, keep unauthorized

people off the network, guard privacy, and maintain uninterrupted operation.
The Cisco Identity Based Networking Services (IBNS) solution provides authentication, access control, and security policy administration to secure
network connectivity and resources. Cisco IBNS in the Cisco Catalyst 2960 Series prevents unauthorized access and helps ensure that users get only
their designated privileges. It provides the ability to dynamically administer granular levels of network access. Using the 802.1x standard and the
Cisco Secure Access Control Server (ACS), users can be assigned a VLAN upon authentication, regardless of where they connect to the network.
This setup allows IT departments to enable strong security policies without compromising user mobility, and with minimal administrative overhead.
To guard against denial-of-service and other attacks, ACLs can be used to restrict access to sensitive portions of the network by denying packets
based on source and destination MAC addresses, IP addresses, or TCP/User Datagram Protocol (UDP) ports. ACL lookups are done in hardware, so
forwarding performance is not compromised when implementing ACL-based security.
Port security can be used to limit access on an Ethernet port based on the MAC address of the device to which it is connected. It also can be used to
limit the total number of devices plugged into a switch port, thereby protecting the switch from a MAC flooding attack as well as reducing the risks
of rogue wireless access points or hubs.
assignment by augmenting a host IP address request with the switch port ID.
The MAC Address Notification feature can be used to monitor the network and track users by sending an alert to a management station so that
network administrators know when and where users entered the network. Secure Shell Protocol Version 2 (SSHv2) and Simple Network
Management Protocol Version 3 (SNMPv3) encrypt administrative and network-management information, protecting the network from tampering or
eavesdropping. TACACS+ or RADIUS authentication enables centralized access control of switches and restricts unauthorized users from altering
the configurations. Alternatively, a local username and password database can be configured on the switch itself. Fifteen levels of authorization on
the switch console and two levels on the Web-based management interface provide the ability to give different levels of configuration capabilities to
different administrators.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip forGood, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, SpectrumExpert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)