Cisco Catalyst 2955 Series Switches

Cisco® Catalyst® 2955 Series Switches are industrial-grade switching products that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for deployment in harsh environments. The Cisco Catalyst 2955 Series operates in environments such as industrial networking solutions (industrial Ethernet deployments), intelligent transportation systems (ITS), and transportation network solutions. It integrates into military equipment, Supervisory Control and Data Acquisition (SCADA) systems, power generation systems, waste water treatment facilities, building automation systems, warehouses, and any other facilities or applications where the environmental conditions or suspended solid concentrations exceed the specifications of other commercial switching products.
The Cisco Catalyst 2955 Series uses industrial-grade components, a compact form factor, convection cooling, and relay output signaling to extend intelligent services such as enhanced security, high availability, and advanced quality of service (QoS) to areas that cannot be served by traditional commercial-grade Ethernet switches.

Embedded in all Cisco Catalyst 2955 Series Switches is the Cisco Device Manager software, which allows users to easily configure and monitor the switch using a standard Web browser, eliminating the need for more complex terminal emulation programs and knowledge of the command-line interface (CLI). Customers can easily initialize the switch with Web-based Cisco Express Setup, without using the CLI. In addition, with Cisco Network Assistant, a standalone network management application, customers can simultaneously configure and troubleshoot multiple Cisco Catalyst desktop switches. Cisco Device Manager, Cisco Express Setup, and Cisco Network Assistant reduce the cost of deployment by enabling less-skilled personnel to set up switches quickly. Furthermore, Cisco Catalyst 2955 Series Switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks.

This product line offers Cisco IOS® Software functionality for traditional data, video, and voice services, with enhanced intelligent services features for additional security, advanced QoS, and high availability. Intelligent services are critical in supporting the reliability and determinism of proprietary Layer 2 solutions typical of industrial Ethernet deployments, while providing the advantages (standardization, open connectivity, bandwidth, integration, etc.) of an advanced Ethernet switching architecture. These intelligent services include Layers 2-4 traffic prioritization, rate limiting, and security filtering, helping to ensure the high uptime, low latency, deterministic performance, and data integrity critical for industrial automation control networks.

Cisco Catalyst 2955 Series Switches consist of the following devices:

- **Cisco Catalyst 2955T-12**—Twelve 10/100 ports and two fixed 10/100/1000BASE-T uplink ports
- **Cisco Catalyst 2955C-12**—Twelve 10/100 ports and two fixed 100BASE-FX multimode uplink ports

- **Cisco Catalyst 2955S-12**—Twelve 10/100 ports and two fixed 100BASE-LX single-mode uplink ports

Intelligence in the New Ethernet Networks

Currently, non-Ethernet Layer 2 networks are evolving from traditional field buses or proprietary technologies to standards-based Ethernet networks. The progression to Ethernet is driven by a multitude of factors, including:

- **Standardization**—There are hundreds of millions of Ethernet devices around the world; Ethernet has become the prevalent Layer 2 technology based on widely adopted standards.
- **IP Connectivity**—Ethernet is the most ubiquitous Layer 2 technology for Internet connectivity, in turn providing unprecedented communications potential to networks that have been traditionally isolated.
- **Bandwidth**—Orders of magnitude above other existing technologies, Ethernet takes advantage of the increased computational power of the new network hosts (I/O devices, motion machinery, sensors, intelligent electronic devices, etc.) being deployed today. This allows for real-time control and data gathering for a multitude of applications that were not previously feasible, including preventive maintenance, total quality control monitoring, remote monitoring, and asset management and optimization.
- **Multiple services on a single infrastructure**—Intelligent Ethernet allows a single network to carry multiple vendor implementations of control (EtherNet/IP, Modbus TCP, Foundation Fieldbus High Speed Ethernet [HSE] and various Advanced Traffic Management Systems [ATMSs]), and to use the same investment to also deliver traditional voice (telephony), data (e-mail, technical support, and browsing), and video services (video monitoring).
- **Multilayer Integration**—All of the elements described above allow for the integration of higher-level applications such as enterprise resource planning (ERP), manufacturing execution systems (MES), and advanced traffic management systems to the floor control layer (programmable logic controllers [PLCs], PC-based control systems, traffic control equipment, and human-machine interfaces [HMIs]). This allows for a true flow of data and automation from the demand side (customer placing and order) to the factory floor (assembly line) or from the monitoring devices in a freeway all the way to the emergency response systems, as well as real-time control in SCADA applications. As organizations increasingly rely on Ethernet networks, it is important to help ensure high availability, security, scalability, and control. By adding Cisco IOS Software functionality to new network applications, users can now deploy network-wide intelligent services that address these requirements in a consistent way—from the I/O or monitoring device to the core and through the WAN.

Network Security through Advanced Security Features

Cisco Catalyst 2955 Series Switches offer enhanced data security through numerous security features. These features allow customers to enhance network security with capabilities to secure traffic through the protection of passwords and configuration information; to provide options for network security based on users, ports, and Media Access Control (MAC) addresses; and to enable more immediate reactions to intruder and hacker detection.

Secure Shell (SSH) Protocol and SNMPv3 protect information from tampering or eavesdropping by encrypting information being passed along the network, thereby guarding administrative information. Private VLAN Edge isolates ports on a switch, helping ensure that traffic travels directly from the entry point to the aggregation device through a virtual path and cannot be directed to another port.

Port-based access control parameters (ACPs) restrict sensitive portions of the network by denying packets based on source and destination MAC addresses, IP addresses, or Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports. ACP lookups are done in hardware, so forwarding performance is not compromised when implementing this type of security in the network. In addition, time-based ACPs allow configuration of differentiated services based on time periods. ACPs can also be applied to filter traffic based on differentiated services code point (DSCP) values. Port security provides another means to help ensure that appropriate users are on the network, by limiting access based on MAC addresses.

For authentication of users with a Terminal Access Controller Access Control System (TACACS+) or RADIUS server, 802.1x provides port-level security. 802.1x in conjunction with a RADIUS server allows for dynamic port-based user authentication. 802.1x-based user authentication can be extended to dynamically assign a virtual LAN (VLAN) based on a specific user, regardless of where that user connects on the network. This intelligent adaptability provides greater flexibility and mobility to the network's stratified user populations. By combining access control and user profiles with secure network connectivity, services, and applications, customers can more effectively manage user mobility and drastically reduce the overhead associated with granting and managing access to network resources.

With multilayer Cisco Catalyst 2955 Series Switches, network managers can implement high levels of console security. Multilevel access security on the switch console and a Web-based management interface prevent unauthorized users from accessing or altering switch configurations. TACACS+ or RADIUS authentication enable centralized access control of the switch and restrict unauthorized users from altering the configuration. Deploying security can be done through Cisco Network Assistant security wizards, which ease the deployment of security features that restrict user access to a server, a portion of the network, or the entire network.

Network Control through Advanced QoS and Rate Limiting

Cisco Catalyst 2955 Series Switches offer superior and highly granular QoS based on Layers 2–4 information, to help ensure that network traffic is classified and prioritized, and that congestion is avoided in the best possible manner. These switches can classify, reclassify, police (determine if the packet is in or out of predetermined profiles and affect actions on the packet), and mark or drop the incoming packets before the packet is placed in the shared buffer. Packet classification allows the network elements to discriminate between various traffic flows and to enforce rate-limiting policies based on Layer 2 and Layer 3 QoS fields.

To implement QoS, these switches first identify traffic flows or packet groups. They classify or reclassify these groups using the DSCP field in the IP packet and/or the 802.1p class of service (CoS) field in the Ethernet packet. Classification and reclassification can also be based on criteria as specific as the source or destination IP address, source or destination MAC address, or the Layer 4 TCP/UDP ports. At the ingress (incoming port) level, Cisco Catalyst 2955 Series Switches can also perform policing and marking of the packet.

After the packet goes through classification, policing, and marking, it is assigned to the appropriate queue before exiting the switch. Cisco Catalyst 2955 Series Switches support four egress (outgoing port) queues per port, allowing the network administrator to be more discriminating and specific in assigning priorities for the various applications on the network. At the egress level, the switch performs scheduling—an algorithm that determines the order in which the queues are processed. The switches support Weighted Round Robin (WRR) scheduling, strict priority queuing or strict priority scheduling. The WRR scheduling algorithm helps ensure that lower-priority packets are not entirely starved for bandwidth and are serviced without compromising the priority settings administered by the network manager. Strict priority scheduling helps ensure that higher-priority packets will always get serviced first, ahead of other traffic in lower-priority queues.

These features allow for prioritization of mission-critical, such as motion-control traffic, critical I/O or sensor data, video monitoring of security areas over voice (IP telephony traffic), ERP (Oracle, SAP, etc.), and CAD/CAM, which, in turn, would be scheduled to have precedence over less time-sensitive applications such as FTP or e-mail (SMTP). For example, it would be highly undesirable to have a large file download destined to one port on a switch and have quality implications, such as increased latency in industrial control traffic, destined to another port on the switch. This condition is avoided by helping ensure that the control traffic is properly classified and prioritized throughout the network. Other applications, such as Web browsing, can be treated as low priority and handled on a best-efforts basis.

Cisco Catalyst 2955 Series Switches allocate bandwidth based on several criteria, including MAC source address, MAC destination address, IP source address, IP destination address, and TCP/UDP port number. Bandwidth allocation is essential in network environments that require service-level agreements, or when it is necessary for the network manager to control the bandwidth given to certain users. Cisco Catalyst 2955 Series Switches support up to six policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. This gives the network administrator granular control of the network bandwidth.

Network Availability

To provide efficient use of resources for bandwidth-hungry applications like multicasts (common in producer-consumer data distribution models), intelligent Cisco Catalyst 2955 Series Switches support Internet Group Management Protocol (IGMP) snooping in hardware. Through the support and configuration of IGMP snooping via Cisco Network Assistant, Cisco Catalyst 2955 Series Switches deliver outstanding performance and ease of use in administering and managing multicast applications on the LAN.

The IGMP snooping feature allows the switch to "listen in on" the IGMP conversation between hosts. When a switch hears an "IGMP join" request from a host for a given multicast group, the switch adds the host's port number to the group destination address (GDA) list for that group. When the switch hears an "IGMP leave" request, it removes the host's port from the Content Addressable Memory (CAM) table entry.

Per VLAN Spanning Tree Plus (PVST+) allows users to implement redundant uplinks while distributing traffic loads across multiple links. This is not possible with standard Spanning-Tree Protocol implementations. Cisco UplinkFast technology helps ensure immediate transfer to the secondary uplink, a vast improvement over the traditional 30-to-60-second convergence time.

Network Management

Customers can configure one switch at a time with the embedded Cisco Device Manager or configure and troubleshoot multiple switches with Cisco Network Assistant, a standalone network management software application optimized for LANs of small and medium-sized businesses with up to 250 users. Cisco Device Manager offers a simple and intuitive GUI interface for configuring and monitoring the switch. The software is Web-based and embedded in Cisco Catalyst 3750, 3650, 3550, 2970, 2960, 2955, 2950, and 2940 Series Switches. Cisco Device Manager reduces the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches.

Cisco Network Assistant software provides an integrated management interface for delivering intelligent services, such as multilayer switching, QoS, multicast, and security ACLs. Cisco Network Assistant software allows administrators make use of benefits formerly reserved for only the most advanced networks without having to learn the CLI, or even the details of the technology. With Cisco Network Assistant, customers can configure multiple ports and switches simultaneously, perform software updates across multiple switches at once, and copy configurations to other switches for rapid network deployments. Bandwidth graphs and link reports provide useful diagnostic information, and the topology map gives network administrators a quick view of the network status. Cisco Network Assistant supports a wide range of Cisco Catalyst intelligent switches from Cisco Catalyst 2940 through Cisco Catalyst 4506. Through a user-friendly GUI, users can configure and manage a wide array of switch functions and start the device manager of Cisco routers and Cisco wireless access points.

The Cisco Network Assistant Software Guide Mode leads the user step by step through the configuration of advanced features and provides enhanced online help for context-sensitive assistance. Cisco AVVID (Architecture for Voice, Video and Integrated Data) wizards provide automated configuration of the switch to optimally support video streaming or videoconferencing, voice over IP (VoIP), and mission-critical applications. In addition, Smartports offers a set of verified feature macros per connection type in an easy-to-apply manner. With these macros, users can consistently and reliably configure essential security, availability, quality of service, and manageability features recommended for Cisco Business-Ready Campus solutions with minimal effort and expertise. These wizards and Smartports can save hours of time for network administrators, eliminate human errors, and help ensure that the configuration of the switch is optimized for these applications.

In addition to Cisco Network Assistant software, Cisco Catalyst 2955 Series Switches provide extensive management tools using SNMP network management platforms such as CiscoWorks. Managed with CiscoWorks, Cisco Catalyst switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Coupled with CiscoWorks, Cisco Resource Manager Essentials, a Web-based management tool, offers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Enhanced Hardware Features

The Cisco Catalyst 2955 Switch has been designed for deployment in harsh environments. Through the use of special thermal design techniques and industrial-rated components, the Cisco Catalyst 2955 is rated to operate at extreme temperatures (-40°to 60°C; -40°to 140°F). Robust mechanical specifications allow for its deployment as a mobile platform and under extreme vibration and shock environments (50G trapezoidal shock pulse). The compact form factor, DIN rail mounting, and dual cabling orientations facilitate its deployment into industrial enclosures, traffic control cabinets, and transportation vehicles. Two normally open relays can be associated with the different port alarms, power alarms, and high temperature conditions to send an output signal to other external mechanisms (visible or audible alarms, for example), HMIs, or PLCs for a controlled shutdown. Dual power inputs provide for optional redundant power supplies, guaranteeing an even higher level of resiliency and reliability.

Figure 1. Cisco Catalyst 2955 Series Switches

Table 1. Product Features and Benefits

Feature	Benefit
Availability	
Superior redundancy for fault backup	• IEEE 802.1D Spanning-Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • Support for Cisco Spanning-Tree Protocol enhancements such as UplinkFast, BackboneFast, and PortFast technologies helps ensure quick failover recovery, enhancing overall network stability and availability. • IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) provides rapid convergence of the spanning tree, independent of spanning tree timers. • Per VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. • Provides unidirectional link detection (UDLD) and Aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.

Feature	Benefit
Integrated Cisco IOS Software features for bandwidth optimization	• Bandwidth aggregation of up to 4 Gbps (two ports full duplex) through Cisco Gigabit EtherChannel® technology and up to 1.6 Gbps (eight ports full duplex) through Fast EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches, to routers and individual servers. Port Aggregation Protocol (PAgP) is available to simplify configuration. • VLAN1 minimization allows VLAN1 to be disabled on any individual VLAN trunk link. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall system performance. • Per virtual LAN (VLAN) Spanning Tree Plus (PVST+) allows for Layer 2 load sharing on redundant links, to efficiently use the extra capacity inherent in a redundant design. • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) allows a spanning-tree instance per VLAN, enabling Layer 2 load sharing on redundant links. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports on the switch. • Internet Group Management Protocol Version 3 (IGMPv3) snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. Multicast VLAN Registration MVR, IGMP filtering, and fast-join and immediate leave are available as enhancements. The number of IGMP groups can be limited with IGMP throttling. IGMP Snooping time can be adjusted to optimize the performance of multicast data flows. • MVR continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons. • Supports additional frame formats: Ethernet II (tagged and untagged), 802.3 (SNAP encapsulated, tagged and untagged frames).
Security	

Feature	Benefit
Network Security Features	• Filtering of incoming traffic flows based on Layer 2, Layer 3, or Layer 4 ACPs prevents unauthorized data flows. ◦ The following Layer 2 ACPs or a combination can be used for security classification of incoming packets: source MAC address, destination MAC address, and 16-bit Ethertype. ◦ The following Layer 3 and Layer 4 fields or a combination can be used for security classification of incoming packets: source IP address, destination IP address, TCP source or destination port number, UDP source, or destination port number. ACLs can also be used to filter based on DSCP values. ◦ Time-based ACLs allow configuration of differentiated services based on time periods. • Private VLAN edge provides security and isolation between ports on a switch, helping ensure that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. • Support for the 802.1x standard allows users to be authenticated, regardless of which LAN port they are accessing, and provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network. ◦ IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user, regardless of where the user is connected. ◦ IEEE 802.1x with voice VLAN gives an IP phone access to the voice VLAN, regardless of the authorized or unauthorized state of the port. ◦ IEEE 802.1x with port security authenticates the port and manages network access for all MAC addresses, including the clients'. ◦ IEEE 802.1x with guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN. • SSHv2 and SNMPv3 provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSHv2 and the crypto version of SNMPv3 require a special crypto software image because of U.S. export restrictions. • Port Security and unicast MAC filtering secure the access to a port based on MAC addresses. The aging feature of port security removes the MAC address from the switch after a specific time frame to allow another device to connect to the same port. Unicast MAC filtering allows non-IP packets to be filtered as well. • With unknown unicast/multicast port blocking, the switch will not flood packets with unknown destination MAC addresses to all Ethernet ports. Unknown unicast/multicast port blocking disables flooding on a per-port basis. • MAC address notification allows administrators to be notified of new users added or removed from the network. • Spanning-tree root guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning-Tree Protocol root nodes. • The Spanning-Tree Protocol PortFast/bridge protocol data unit (BPDU) guard feature disables access ports with Spanning-Tree Protocol PortFast enabled upon reception of a BPDU, and increases network reliability, manageability, and security. • Multilevel console access security prevents unauthorized users from altering the switch configuration. • TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. • The user-selectable address-learning mode simplifies configuration and enhances security. • Trusted Boundary provides the ability to trust the QoS priority settings if a Cisco IP phone is present and to disable the trust setting if the IP phone is removed, preventing a rogue user from overriding prioritization policies in the network. • IGMP Filtering provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port. • Support for dynamic VLAN assignment through implementation of VLAN Membership Policy Server (VMPS) client functionality provides flexibility in assigning ports to VLANs. Dynamic VLAN enables fast assignment of IP addresses. • SPAN support of intrusion detection systems (IDSs) to monitor, repel, and report network security violations. • Cisco Network Assistant software security wizards ease the deployment of security features for restricting user access to a server, a portion of the network, or the network.
QoS	

Feature	Benefit
Overview	• The switches support the aggregate QoS model by enabling classification, policing/metering, and marking functions on a per-port basis at ingress and queuing/scheduling functions at egress. • The switches support configuring QoS ACPs on all ports, using ACPs to help ensure proper policing and marking on a per-packet basis. Up to four ACPs per switch are supported in configuring either QoS ACPs or security filters. • Automatic QoS (Auto-QoS) greatly simplifies the configuration of QoS in voice-over-IP (VoIP) networks by issuing interface and global switch commands that allow the detection of Cisco IP phones, the classification of traffic, and egress queue configuration.
QoS Classification Support at Ingress	• The switches support QoS classification of incoming packets for QoS flows based on Layer 2, Layer 3, and Layer 4 fields. • The following Layer 2 fields (or a combination) can be used for classifying incoming packets to define QoS flows: source/destination MAC address or 16-bit Ethertype. • The switches support identification of traffic based on Layer 3 type of service (ToS) field DSCP values. • The following Layer 3 and Layer 4 fields (or a combination) can be used to classify incoming packets to define QoS flows: source/destination IP address, TCP source/destination port number, or UDP source/destination port number.
QoS metering/policing at ingress	• Support for metering/policing of incoming packets restricts incoming traffic flows to a certain rate. • The switches support up to six policers per Fast Ethernet port, and 60 policers on a Gigabit Ethernet port. • The switches offer granularity of traffic flows at 1 Mbps on Fast Ethernet ports, and 8 Mbps on Gigabit Ethernet ports.
QoS marking at ingress	• The switches support marking and remarking packets based on the state of policers/meters. • The switches support marking and remarking based on the following mappings: from DSCP to 802.1p, and from 802.1p to DSCP. • The switches support 14 well-known and widely used DSCP values. • The switches support classifying or reclassifying packets based on the default DSCP per port, and support classification based on DSCP values in the ACL. • The switches support classifying or reclassifying frames based on the default 802.1p value per port. • The switches support 802.1p override at ingress.
QoS scheduling support at egress	• Four queues per egress port are supported in hardware. • The WRR queuing algorithm helps ensure that low-priority queues are not starved. • Strict Priority Scheduling helps ensure that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Sophisticated traffic management	• The switch offers the ability to limit data flows based on MAC source or destination address, IP source or destination address, TCP/UDP port numbers, or any combination of these fields. • The switch offers the ability to manage data flows asynchronously upstream and downstream from the end station or on the uplink.
Management	

Feature	Benefit
Superior manageability	• An embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • The switch supports all nine RMON groups through the use of a Cisco SwitchProbe® Analyzer Switched Port Analyzer (SPAN) port, permitting traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe. • A SPAN port monitors traffic of a single port from a single network analyzer or RMON probe. • Remote SPAN (RSPAN) allows network administrators to locally monitor ports in a Layer 2 switch network from any other switch in the same network. • DHCP Snooping Option 82 enables more sophisticated IP address assignment by the DHCP server. • The Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device. • Crash Information Support enables the switch to generate a crash file for improved troubleshooting. • Show Interface Capabilities provides information on the configuration capabilities of any interface. • RTTMON-MIB allows users to monitor network performance between a Cisco Catalyst switch and a remote device.
Cisco Network Assistant software	• Cisco Network Assistant software is free, standalone network management application software that simplifies the administration of networks of up to 250 users. It supports a wide range of Cisco Catalyst intelligent switches from Cisco Catalyst 2940 through Cisco Catalyst 4506. With Cisco Network Assistant, users can manage Cisco Catalyst switches plus launch the device managers of Cisco integrated services routers (ISRs) and Cisco Aironet® WLAN access points by simply clicking their icon in the topology map. • Cisco AVVID wizards use just a few user inputs to automatically configure the switch to optimally handle different types of traffic: voice, video, multicast, and/or high-priority data. • A security wizard is provided to restrict unauthorized access to servers and networks and to restrict certain applications on the network. • One-click software upgrades can be performed across multiple switches simultaneously, and configuration cloning enables rapid deployment of networks. • Cisco Network Assistant software supports multilayer feature configurations such as ACPs and QoS parameters. • Cisco Network Assistant Software Guide Mode assists users in the configuration of powerful advanced features by providing step-by-step instructions. • Cisco Network Assistant software provides enhanced online help for context-sensitive assistance. • Easy-to-use GUI provides both a topology map and front-panel view of the switches. • Multidevice and multiport configuration capabilities allow network administrators to save time by configuring features across multiple switches and ports simultaneously. • User-personalized interface allows users to modify polling intervals, table views, and other settings within Cisco Network Assistant software and to retain these settings the next time they use Cisco Network Assistant. • Alarm notification provides automated e-mail notification of network errors and alarm thresholds.
Support for CiscoWorks	• Manageable through CiscoWorks network management software on a per-port and per-switch basis, providing a common management interface for Cisco routers, switches, and hubs. • SNMPv1, v2, and v3 (non-crypto) and Telnet interface support deliver comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • Cisco Discovery Protocol versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • CiscoWorks is supported by the CiscoWorks 2000 LAN Management Solution.

Feature	Benefit
Ease of use and ease of deployment	• Cisco Device Manager is embedded Web-based software that allows the customer to easily configure and troubleshoot the switch, eliminating the need for more complex terminal emulation programs and CLI knowledge, and reducing the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches. • Smartports offers a set of verified feature macros per connection type in an easy-to-apply manner. With these macros, users can consistently and reliably configure essential security, availability, quality of service, and manageability features recommended for Cisco Business-Ready Campus solutions with minimal effort and expertise. • Autoconfiguration eases the deployment of switches in the network by automatically configuring multiple switches across a network via a boot server. • Autosensing on each Ethernet port] detects the speed of the attached device and automatically configures the port for 10-, 100-, or 1000-Mbps operation, easing the deployment of the switch in mixed 10, 100, and 1000BASE-T environments. • Autonegotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • DTP enables dynamic trunk configuration across all ports in the switch. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier network administration and troubleshooting. • Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports on the switch. • PAgP automates the creation of Cisco Fast EtherChannel or Gigabit EtherChannel groups, enabling linking to another switch, router, or server. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This is similar to Cisco EtherChannel and PAgP. • The default configuration stored in Flash helps ensure that the switch can be quickly connected to the network and can pass traffic with minimal user intervention.

Table 2. Product Specifications

Feature	Description
Performance	• 13.6 Gbps switching fabric • Cisco Catalyst 2955T-12: 6.4 Gbps maximum forwarding bandwidth • Cisco Catalyst 2955C-12: 2.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2955S-12: 2.8 Gbps maximum forwarding bandwidth • (Forwarding rates based on 64-byte packets) • Cisco Catalyst 2955T-12: 4.8 Mpps wire speed forwarding rate • Cisco Catalyst 2955C-12: 2.0 Mpps wire speed forwarding rate • Cisco Catalyst 2955S-12: 2.0 Mpps wire speed forwarding rate • 8 MB memory architecture shared by all ports • Up to 32 MB SDRAM and 16 MB Flash memory • Configurable up to 8000 MAC addresses
Management	• BRIDGE-MIB • CISCO-ACCESS-ENVMON-MIB • CISCO-BULK-FILE-MIB • CISCO-C2900-MIB • CISCO-CDP-MIB • CISCO-CLUSTER-MIB • CISCO-CONFIG-MAN-MIB • CISCO-ENTITY-ALARM-MIB • CISCO-ENTITY-MIB • CISCO-ENVMON-MIB • CISCO-FLASH-MIB • CISCO-FTP-CLIENT-MIB • CISCO-HSRP-MIB • CISCO-IGMP-FILTER-MIB • CISCO-IMAGE-MIB • CISCO-LAG-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAE-MIB • CISCO-PAGP-MIB • CISCO-PORT-SECURITY-MIB • CISCO-PRIVATE-VLAN-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-SYSLOG-MIB • CISCO-TCP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • ETHERLIKE-MIB • HC-RMON-MIB • IEEE8021-PAE-MIB • IEEE8023-LAG-MIB • IF-MIB • IP-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-FLASH-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB • OLD-CISCO-SYSTEM-MIB

Feature	Description
	• OLD-CISCO-TS-MIB • RFC1213-MIB • RFC1398-MIB • RMON-MIB • RMON2-MIB • SMON-MIB • SNMP-FRAMEWORK-MIB • SNMP-MPD-MIB • SNMP-TARGET-MIB • SNMPv2-MIB • TCP-MIB • UDP-MIB
Standards	• IEEE 802.1x support • IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning-Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3ad Link Aggregation Control Protocol (LACP) • IEEE 802.3ah Ethernet in the First Mile (EFM) • RMON I and II standards • SNMPv1, SNMPv2c, and SNMPv3
Connectors and cabling	• 10BASE-T/100BASE-TX ports: RJ-45 connectors; four-pair Category 5 UTP cabling • 1000BASE-T ports: RJ-45 connectors; four-pair Category 5 UTP cabling • 100BASE-FX ports: MT-RJ connectors; 50/125 or 62.5/125 micron multimode fiber-optic cabling • 100BASE-LX ports: LC connectors; 9/125 micron single-mode fiber-optic cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-RJ-45 rollover cable with RJ-45-to-DB9 adapter for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately from Cisco, part number ACS-DSBUASYN=)
MT-RJ patch cables for Cisco Catalyst 2955	Type of cable, Cisco part number • One-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-1M • Three-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-3M • Five-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-5M • One-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-1M • Three-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-3M • Five-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-5M • Two-meter, LC to SC single-mode cable, CAB-CP-LCSC-2M
Indicators	• Per-port status LEDs: Link integrity, disabled, activity, and indications • Dual-power-supply indicators • Major and minor alarm-relay indicators
Dimensions and weight (HxWxD)	• 3.78x8.07x5.03 in. (9.60x20.50x12.78 cm): Connectors facing forward • 5.03x8.07x3.78 in. (12.78x20.50x9.60 cm): Connectors facing downward • 3.0 lb (1.4 kg)
Relay contacts	• Surge withstand between open contacts: 1500V, FCC Part 68 • Surge withstand between contact and coil: 2500V, Bellcore • Maximum switching capacity: 1A @ 30 VDC • Maximum switching voltage: .3A @ 125 VAC

Feature	Description
Environmental ranges	• Recommended operating temperature range: -40°to 140 °F (-40°to 60°C) • Recommended storage temperature range: -40°to 185°F (-40°to 85°C) • Operating relative humidity: 10 to 95% (noncondensing) • Operating altitude: 9843 ft (3000 m) @ 104°F (40° C) • Storage altitude: Up to 29,500 ft (9000 m) • Shock: 50 g trapezoidal shock (meets or exceeds ASTM D3332) • Vibration: 500 Hz (meets or exceeds MIL-STD-810, Method 514.5)
Power requirements	• External 24V (dual-redundant DC input, screw-down connectors) • Power consumption: 23W maximum, 78.53 BTU/hour • 18V minimum; 32V maximum
Predicted mean time between failure (MTBF)	• WS-C2955T 235,022 hours • WS-C2955C 206,378 hours • WS-C2955S 205,115 hours • Telcordia SR-332 Gf
Fiber port specifications	• 100BASE-FX (MT-RJ connectors @ 1,300 nm): • Optical receiver sensitivity: -30 dBm • Optical transmitter power: -19 to -14 dBm • Maximum distance: 2 km • 100BASE-LX (LC connectors @ 1,300 nm): • Optical receiver sensitivity: -38 to -31 dBm • Optical transmitter power: -15 to -8 dBm • Maximum distance: 15 km
Regulatory Agency Approvals	
Safety certifications Hazardous locations	• CE Marking • UL 60950 • CSA 22.2/60950 • TUV GS: CB Report to IEC 60950 • UL 508 • CSA 22.2/142 • AS/NZS 3260 • NOM • UL 1604—Class I, Div 2 Group A, B, C, D • CSA 22.2/213—Class 1, Div 2 Group A, B, C, D • EN 50021—Class I, Zone 2
Electromagnetic emissions certifications	• FCC Part 15 Class A • ICES-003 Class A • EN 55022: (CISPR22 Class A) • EN 55024: (CISPR24) • VCCI Class A • AS/NZS CISPR 22 Class A • VCCI Class 1 • CE Marking • CNS 13438 • BSMI Class A • MIC Class A • EN 61131-2 • EN 55011 (CISPR 11) Class A
ITS	NEMA TS-2
Warranty	Limited five-year warranty
External DIN Rail Mountable Power Supply	
Input voltage	AC100-120/220-240V (switchable) 47-63 Hz
Input current	<1.3A (switch in 115V position)
Input current	<0.7A (switch in 230V position)
Output voltage	24 VDC (+5%, -1%)
Size (WxHxD)	1.92x4.92x4.05 (50x125x103 mm)

Feature	Description
Weight	1 lb (460 g)
Worldwide approvals	UL, EN, CSA, and CB
Overload protection	Over 1.5 times normal current
Cooling	Normal convection cooling
Temperature range	• -25º to +85ºC (storage) • -10º to +60ºC (operating)

Service and Support

The service and support programs described in Table 3 are available as part of the Cisco Desktop Switching Service and Support solution, and are available directly from Cisco and through resellers.

Table 3. Cisco Service and Support Programs

Service and Support	Features	Benefits
Advanced Services		
Total Implementation Solutions (TIS)—available direct from Cisco Packaged Total Implementation Solutions (Packaged TIS)—available through resellers	• Project management • Site survey and configuration deployment • Installation, text, and cutover • Training • Major moves, adds, or changes • Design review and product staging	• Supplements existing staff • Helps ensure that functionality meets customer needs • Mitigates risk
Technical Support Services		
Cisco SMARTnet® and SMARTnet Onsite—available direct from Cisco Packaged SMARTnet—available through resellers	• 24x7 access to software updates • Web access to technical repositories • Telephone support through the Technical Assistance Center • Advance replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers cost of ownership by using Cisco expertise and knowledge • Minimizes network downtime

Table 4. Ordering Information

Model Numbers	Configuration
WS-C2955T-12	Twelve 10/100 ports and two 10/100/1000BASE-T ports
WS-C2955C-12	Twelve 10/100 ports and two 100BASE-FX ports
WS-C2955S-12	Twelve 10/100 ports and two 100BASE-LX ports
PWR-2955-AC=	DIN Rail mountable 24V power supply (85 to 264 VAC, or 90 to 375VDC input)
STK-RACKMNT-2955=	DIN Rail Adapter for 19" rack mounting

For More Information on Cisco Products

- **United States and Canada**: 800 553-NETS (6387)
- **Europe**: 32 2 778 4242
- **Australia**: 612 9935 4107
- **Other**: 408 526-7209
- http://www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**

Printed in USA

C78-380621-00 11/06