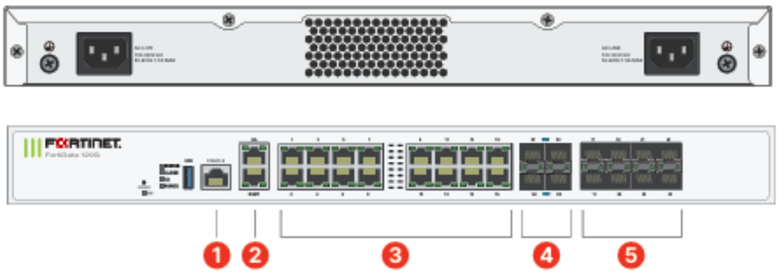
ps
Počítačová společnost

Specifikace A

FortiGate 120G 3Y UTP bundle

Firewall nové generace (NGFW), **SD-WAN gateway** a výkonný **router FortiGate 120G** poskytuje špičkové **security řešení** v kompaktním stolním provedení. Jedná se o uživatelsky přívětivé, cenově dostupné a snadno nasaditelném řešení vhodné pro menší a středně velké společnosti. Chrání síť před kybernetickými hrozbami pomocí **specializovaného čipu** a špičkově zabezpečené SD-WAN v jednoduchém, cenově dostupném a snadno implementovatelném boxu. Díky vlastnímu procesoru je zaručena **vysoká propustnost** i při zapnutých bezpečnostních funkcích a hloubkové inspekci provozu. Při **IPS inspekci** je propustnost modelu FortiGate 120G **5.3 Gbps**, při zapnutém **NGFW** pak **3.1 Gbps** a při plném využití **UTP** pak **2.8 Gbps**.

FortiGate 120G/121G Series



Interfaces

1. 1x RJ45 Console Port
2. 2x RJ45 HA and Management Ports
3. 16x GE RJ45 Ports
4. 4× 10GE SFP+ FortiLink Slots
5. 8x SFP Ports

S produkty řady **FortiGate** je krom standadních funkcí stavového firewallu, routeru nebo SD-WAN gateway možno využít i pokročilé security funkce, které posunou zabezpečení sítě na vyšší úroveň:

- **Systém ochrany IPS** - nejdůležitější prvek UTM, tj. signatury striktně síťových útoků a vzory doprovodných anomálií, navíc konfigurovatelné pomocí zásad a senzorů. Identifikuje tisíce aplikací v síťovém provozu pro hloubkovou kontrolu a podrobné prosazování zásad, chrání před malwarem, exploity a škodlivými weby v šifrovaném i nešifrovaném provozu. Předchází známým útokům a detekuje je pomocí nepřetržitého zpravodajství o hrozbách z bezpečnostních služeb FortiGuard Labs s umělou inteligencí. Proaktivně blokuje neznámé sofistikované útoky v reálném čase pomocí FortiSandbox.

- **Filtr obsahu v síti**, který chrání před škodlivými webovými stránkami a umožňuje blokovat webové stránky kvůli nežádoucímu obsahu (např. hazardní hry, pornografie, internetové obchody atd.).

- **Ochrana elektronické pošty + Antispam** - je přítomna v základním rozsahu u každé brány FortiGate se systémem FortiGuard.

- **Podpora VPN** - umožňuje vytvářet bezpečné a snadno použitelné VPN tunely (IPsec a SSL) na základě integrace s AD nebo jinými řešeními SSO.

- **Fortinet Security Fabric -** který dokáže pomocí jedné platformy s centrální správou řídit kompletní zabezpečení sítě na všech úrovních. Díky propojení všech prvků z celého světa do jendé sítě dokáže efektivně odhalovat hrozby ještě dříve, než dorazí.

Firewall	**Fortigate**
Gigabit LAN	**ano**
Management	**Ano**
Počet USB portů	**1**
Podpora IPv6	**ano**
Síťové rozhraní (Mbps)	**100/1000/2500/5000/10000**
Ventilátor	**ne**
Fyzické parametry	
Hloubka (mm)	**254**
Hmotnost (kg)	**5.52**

Provedení	**Rackmount**
Šířka (mm)	**432**
Výška (mm)	**44**
Napájení	
Napájení	**DC**
Příkon (W)	**40**
Parametry Ethernet	
Počet RJ45 portů	**18**
Parametry napájení	
Provozní teplota	**0° až +40 °C**

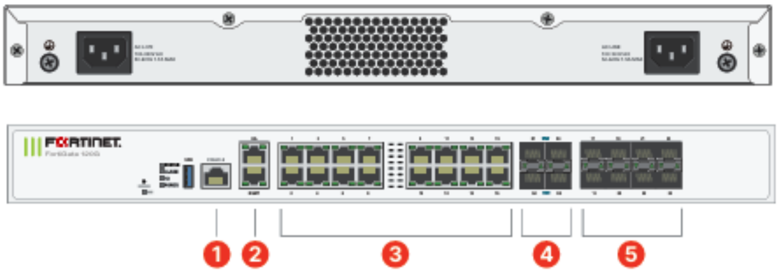
Záruka 36 měsíců

Specifikace B

FortiGate 50G 3Y UTP bundle

Firewall nové generace (NGFW), **SD-WAN gateway** a výkonný **router FortiGate 120G** poskytuje špičkové **security řešení** v kompaktním stolním provedení. Jedná se o uživatelsky přívětivé, cenově dostupné a snadno nasaditelném řešení vhodné pro menší a středně velké společnosti. Chrání síť před kybernetickými hrozbami pomocí **specializovaného čipu** a špičkově zabezpečené SD-WAN v jednoduchém, cenově dostupném a snadno implementovatelném boxu. Díky vlastnímu procesoru je zaručena **vysoká propustnost** i při zapnutých bezpečnostních funkcích a hloubkové inspekci provozu. Při **IPS inspekci** je propustnost modelu FortiGate 120G **5.3 Gbps**, při zapnutém **NGFW** pak **3.1 Gbps** a při plném využití **UTP** pak **2.8 Gbps**.

FortiGate 120G/121G Series



Interfaces

1. 1x RJ45 Console Port
2. 2x RJ45 HA and Management Ports
3. 16x GE RJ45 Ports
4. 4× 10GE SFP+ FortiLink Slots
5. 8x SFP Ports

S produkty řady **FortiGate** je krom standadních funkcí stavového firewallu, routeru nebo SD-WAN gateway možno využít i pokročilé security funkce, které posunou zabezpečení sítě na vyšší úroveň:

- **Systém ochrany IPS** - nejdůležitější prvek UTM, tj. signatury striktně síťových útoků a vzory doprovodných anomálií, navíc konfigurovatelné pomocí zásad a senzorů. Identifikuje tisíce aplikací v síťovém provozu pro hloubkovou kontrolu a podrobné prosazování zásad, chrání před malwarem, exploity a škodlivými weby v šifrovaném i nešifrovaném provozu. Předchází známým útokům a detekuje je pomocí nepřetržitého zpravodajství o hrozbách z bezpečnostních služeb FortiGuard Labs s umělou inteligencí. Proaktivně blokuje neznámé sofistikované útoky v reálném čase pomocí FortiSandbox.

- **Filtr obsahu v síti**, který chrání před škodlivými webovými stránkami a umožňuje blokovat webové stránky kvůli nežádoucímu obsahu (např. hazardní hry, pornografie, internetové obchody atd.).

- **Ochrana elektronické pošty + Antispam** - je přítomna v základním rozsahu u každé brány FortiGate se systémem FortiGuard.

- **Podpora VPN** - umožňuje vytvářet bezpečné a snadno použitelné VPN tunely (IPsec a SSL) na základě integrace s AD nebo jinými řešeními SSO.

- **Fortinet Security Fabric -** který dokáže pomocí jedné platformy s centrální správou řídit kompletní zabezpečení sítě na všech úrovních. Díky propojení všech prvků z celého světa do jendé sítě dokáže efektivně odhalovat hrozby ještě dříve, než dorazí.

Parametry

Firewall	Fortigate
Gigabit LAN	ano
Management	Ano
Počet USB portů	1
Podpora IPv6	ano
Síťové rozhraní (Mbps)	100/1000/2500/5000/10000
Ventilátor	ne
Fyzické parametry	
Hloubka (mm)	254
Hmotnost (kg)	5.52
Provedení	Rackmount
Šířka (mm)	432
Výška (mm)	44

Napájení	
Napájení	**DC**
Příkon (W)	**40**
Parametry Ethernet	
Počet RJ45 portů	**18**
Parametry napájení	
Provozní teplota	**0° až +40 °C**

Záruka 36 měsíců

Specifikace C

Cisco Catalyst řady 1300 jsou managovatelné switche Gigabit Ethernet Layer 3 podnikové třídy určené pro malé a střední podniky a pobočky. Tyto jednoduché, flexibilní a bezpečné switche jsou ideální pro nasazení mimo rozvodnou skříň. Řada Catalyst 1300 pracuje na přizpůsobeném softwaru operačního systému Linux s intuitivním grafickým rozhraním, který zjednodušuje nastavení sítě a pokročilými funkcemi, které urychlují digitální transformaci, zatímco všudypřítomné zabezpečení chrání kritické obchodní transakce. Přepínače řady 1300 poskytují ideální kombinaci cenové dostupnosti a možností pro malé a střední podniky a pomáhají vám vytvořit efektivnější a lépe propojenou pracovní sílu.

Stránky produktu: C1300-24XS

Performance

Switching capacity and forwarding rate (All

switches are wire-speed and nonblocking)	
Capacity in millions of packets per second (mpps) (64-byte packets)	357.14
Switching capacity in gigabits per second (Gbps)	480
Layer 2 switching	
Spanning Tree Protocol (STP)	Standard 802.1d spanning tree support Fast convergence using 802.1w (Rapid Spanning Tree Protocol [RSTP]), enabled by default Multiple spanning tree instances using 802.1s (MSTP); 8 instances are supported Per-VLAN Spanning Tree Plus (PVST+); 126 instances are supported Rapid PVST+ (RPVST+); 126 instances are supported
Port grouping/link aggregation	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) Up to 8 groups Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad link aggregation
VLAN	Support for up to 4093 VLANs simultaneously Port-based and 802.1Q tag-based VLANs, MAC-based VLAN, protocol-based VLAN, IP subnet-based VLAN Management VLAN Private VLAN with promiscuous, isolated, and community port Private VLAN Edge (PVE), also known as protected ports, with multiple uplinks Guest VLAN, unauthenticated VLAN Dynamic VLAN assignment via RADIUS server along with 802.1X client authentication Customer premises equipment (CPE) VLAN Auto surveillance VLAN (ASV)
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS. Voice Services Discovery Protocol (VSDP) delivers networkwide zero-touch deployment of voice endpoints and call control devices

Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. This feature is also known as Multicast VLAN Registration (MVR)
VLAN translation	Support for VLAN one-to-one mapping, in which customer VLANs (C-VLANs) on an edge interface are mapped to service provider VLANs (S-VLANs), and the original C-VLAN tags are replaced by the specified S-VLAN
Q-in-Q	VLANs transparently cross a service provider network while isolating traffic among customers
Selective Q-in-Q	Selective Q-in-Q is an enhancement to the basic Q-in-Q feature and provides, per edge interface, multiple mappings of different C-VLANs to separate S-VLANs Selective Q-in-Q also allows configuring of the Ethertype (Tag Protocol Identifier [TPID]) of the S-VLAN tag Layer 2 protocol tunneling over Q-in-Q is also supported
Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP)	GVRP and GARP enable automatic propagation and configuration of VLANs in a bridged domain
Unidirectional Link	UDLD monitors physical connections to detect unidirectional links caused by incorrect
Detection (UDLD)	wiring or cable/port faults to prevent forwarding loops and blackholing of traffic in switched networks
DHCP relay at Layer 2	Relay of DHCP traffic to a DHCP server in a different VLAN; works with DHCP Option 82
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; it supports 2000 multicast groups (source-specific multicasting is also supported)
IGMP querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router

IGMP proxy	The IGMP proxy provides a mechanism for multicast forwarding based on IGMP membership information without the need for more complicated multicast routing protocols
Head-of-Line (HOL) blocking	HOL blocking prevention
Loopback detection	Loopback detection provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. It operates independently of STP
Layer 3	
IPv4 routing	Wire-speed routing of IPv4 packets Up to 990 static routes and up to 128 IP interfaces
IPv6 routing	Wire-speed routing of IPv6 packets
Layer 3 interface	Configuration of a Layer 3 interface on a physical port, LAG, VLAN interface, or loopback interface
Classless Interdomain Routing (CIDR)	Support for CIDR
Routing Information Protocol (RIP) v2	Support for RIP v2 for dynamic routing
Policy-Based Routing (PBR)	Flexible routing control to direct packets to a different next hop based on an IPv4 or IPv6 Access Control List (ACL)
DHCP server	Switch functions as an IPv4 DHCP server, serving IP addresses for multiple DHCP pools or scopes Support for DHCP options
DHCP relay at Layer 3	Relay of DHCP traffic across IP domains
User Datagram Protocol (UDP) relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of Bootstrap Protocol (BOOTP)/DHCP packets
Stacking	
Hardware stacking	Up to 8 switches in a stack. Up to 200 ports managed as a single system with hardware failover Stacking is supported on the following models: Family 1: C1300-16P-4X, C1300-24T-4X, C1300-24P-4X, C1300-24FP-4X,

	C1300-48T-4X, C1300-48P-4X, C1300-48FP-4X, C1300-8MGP-2X, C1300-24MGP-4X, C1300-48MGP-4X Family 2: C1300-12XT-2X, C1300-12XS, C1300-16XTS, C1300-24XS, C1300-24XT, C1300-24XTS PIDs from the same Family can be stacked together. Cross-stacking between Families is not supported.
High availability	Fast stack failover delivers minimal traffic loss. Support for LAG across multiple units in a stack
Plug-and-play stacking configuration/management	Active/standby for resilient stack control Auto-numbering Hot swap of units in stack Ring and chain stacking options, auto stacking port speed, flexible stacking port options
High-speed stack interconnects	Cost-effective high-speed 10 Gigabit Ethernet fiber interfaces
Security	
Secure Shell (SSH) Protocol	SSH is a secure replacement for Telnet traffic. Secure Copy Protocol (SCP) also uses SSH. SSH v1 and v2 are supported
Secure Sockets Layer (SSL) SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based management GUI in the switch	
IEEE 802.1X (authenticator role)	802.1X: RADIUS authentication and accounting, MD5 hash, guest VLAN, unauthenticated VLAN, single/multiple host mode, and single/multiple sessions Supports time-based 802.1X, dynamic VLAN assignment, and MAC authentication
IEEE 802.1X supplicant	A switch can be configured to act as a supplicant to another switch. This enables extended secure access in areas outside the wiring closet (such as conference rooms)

Web-based authentication	Web-based authentication provides network admission control through a web browser to any host devices and operating systems
STP Bridge Protocol Data Unit (BPDU) Guard	A security mechanism to protect the network from invalid configurations. A port enabled for BPDU Guard is shut down if a BPDU message is received on that port. This avoids accidental topology loops
STP Root Guard	Prevents edge devices not in the network administrator's control from becoming STP root nodes
STP loopback guard	Provides additional protection against Layer 2 forwarding loops (STP loops)
DHCP snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as DHCP servers
IP Source Guard (IPSG)	When IPSG is enabled at a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP address spoofing
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there are no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or destination addresses in the ARP packet. This prevents man-in-the-middle attacks
IP/MAC/port binding (IPMB)	The preceding features (DHCP snooping, IPSG, and DAI) work together to prevent Denial-of-Service (DoS) attacks in the network, thereby increasing network availability
Secure Core Technology (SCT)	Makes sure that the switch will receive and process management and protocol traffic no matter how much traffic is received
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, and so on) securely on the switch, populating this data to other devices and a secure auto-configuration. Access to view the sensitive data as plain text or encrypted is provided according to the user-configured access level and the access method of the user
Trustworthy systems	Trustworthy systems provide a highly secure foundation for Cisco products Run-time defenses (Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC])

Private VLAN	Provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic; supports multiple uplinks.
Layer 2 isolation	
Private VLAN Edge (PVE)	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN; supports multiple uplinks
Port security	Ability to lock source MAC addresses to ports and limit the number of learned MAC addresses
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client
RADIUS accounting	The RADIUS accounting functions allow data to be sent at the start and end of services indicating the number of resources (such as time, packets, bytes, and so on) used during the session
Storm control	Broadcast, multicast, and unknown unicast
DoS prevention	DoS attack prevention
Multiple user privilege levels in CLI	Level 1, 7, and 15 privilege levels
ACLs	Support for up to 1024 rules Drop or rate limit based on source and destination MAC, VLAN ID, IPv4 or IPv6 address, IPv6 flow label, protocol, port, Differentiated Services Code Point (DSCP)/IP precedence, TCP/UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag; ACL can be applied on both ingress and egress sides Time-based ACLs supported
Quality of service	
Priority levels	8 hardware queues
Scheduling	Strict priority and Weighted Round-Robin (WRR)
Class of service	Port-based, 802.1p VLAN priority-based, IPv4/IPv6 IP precedence/Type of Service (ToS)/DSCP-based, Differentiated Services (DiffServ), classification and remarking ACLs, trusted QoS Queue assignment based on DSCP and Class of Service (802.1p/CoS)
Rate limiting	Ingress policer; egress shaping and rate control per VLAN, per port, and flow based; dual-rate 3-color (2R3C) policing

Congestion avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization
iSCSI traffic optimization	A mechanism for giving priority to iSCSI traffic over other types of traffic
Standards	
Standards	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN, IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 826, RFC 879, RFC 896, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 920, RFC 922, RFC 950, RFC 951, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1213, RFC 1215, RFC 1286, RFC 1350, RFC 1442, RFC 1451, RFC 1493, RFC 1533, RFC 1541, RFC 1542, RFC 1573, RFC 1624, RFC 1643, RFC 1700, RFC 1757, RFC 1867, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2030, RFC 2131, RFC 2132, RFC 2233, RFC 2576, RFC 2616, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 3164, RFC 3176, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 4330
IPv6	
IPv6	IPv6 host mode, IPv6 over Ethernet, dual IPv6/IPv4 stack IPv6 neighbor and router discovery (ND), IPv6 stateless address auto-configuration, path Maximum Transmission Unit (MTU) discovery Duplicate Address Detection (DAD), ICMP version 6 DHCPv6 stateful client

	IPv6 over IPv4 network with Intrasite Automatic Tunnel Addressing Protocol (ISATAP) tunnel support
IPv6 QoS	Prioritize IPv6 packets in hardware
IPv6 ACL	Drop or rate-limit IPv6 packets in hardware
IPv6 First Hop Security	RA guard ND inspection DHCPv6 guard Neighbor binding table (snooping and static entries) Neighbor binding integrity check
Multicast Listener Discovery (MLD v1/2) snooping	Deliver IPv6 multicast packets only to the required receivers
MLD proxy	The MLD proxy provides a mechanism for multicast forwarding based on MLD membership information without the need for more complicated multicast routing protocols
IPv6 applications	Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, Telnet client, DHCP client, DHCP auto-config, IPv6 DHCP relay, TACACS+
IPv6 RFCs supported	RFC 4443 (which obsoletes RFC 2463): ICMP version 6 RFC 4291 (which obsoletes RFC 3513): IPv6 address architecture RFC 4291: IPv6 addressing architecture RFC 2460: IPv6 specification RFC 4861 (which obsoletes RFC 2461): neighbor discovery for IPv6 RFC 4862 (which obsoletes RFC 2462): IPv6 stateless address auto-configuration RFC 1981: path MTU discovery RFC 4007: IPv6 scoped address architecture RFC 3484: default address selection mechanism RFC 5214 (which obsoletes RFC 4214): ISATAP tunneling RFC 4293: MIB IPv6: textual conventions and general group RFC 3595: textual conventions for IPv6 flow label
Management	
Cisco Business Dashboard	Support for embedded probe for Cisco Business Dashboard running on the s witch. Eliminates the need to set up a separate hardware or virtual machine for the Cisco Business Dashboard Probe onsite

Cisco Business mobile app	Mobile app for Cisco Business switch and wireless products. Helps to set up a local network in minutes and provide easy management at your fingertips
Cisco Network Plug and Play (PnP) agent	The Cisco Network PnP solution provides a simple, secure, unified, and integrated offering to ease new branch or campus device rollouts or for provisioning updates to an existing network. The solution provides a unified approach to provision Cisco routers, switches, and wireless devices with a near-zero-touch deployment experience. Supports Cisco PnP Connect
Web user interface	Built-in switch configuration utility for easy browser-based device configuration (HTTP/HTTPS) Supports simple and advanced mode, configuration, wizards, customizable dashboard, system maintenance, monitoring, online help, and universal search
SNMP	SNMP versions 1, 2c, and 3 with support for traps, and SNMP version 3 User-Based Security Model (USM)
Remote Monitoring (RMON)	Embedded RMON software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis
IPv4 and IPv6 dual stack	Coexistence of both protocol stacks to ease migration
Firmware upgrade	Web browser upgrade (HTTP/HTTPS) and TFTP and upgrade over SCP running over SSH Dual images for resilient firmware upgrades
Port mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer or RMON probe. Up to 8 source ports can be mirrored to one destination port
VLAN mirroring	Traffic from a VLAN can be mirrored to a port for analysis with a network analyzer or RMON probe. Up to 8 source VLANs can be mirrored to one destination port
Flow-based redirection and mirroring	Redirect or mirror traffic to a destination port or mirroring session based on flow
Remote Switch Port Analyzer (RSPAN)	Traffic can be mirrored across a Layer 2 domain to a remote port on a different switch for easier troubleshooting

sFlow agent	Switch can export sFlow sample to external collectors. sFlow provides visibility into network traffic down to the flow level
DHCP (options 12, 59, 60, 66, 67, 82, 125, 129, and 150)	DHCP options facilitate tighter control from a central point (DHCP server) to obtain IP address, auto-configuration (with configuration and image file download), DHCP relay, and hostname
Secure Copy (SCP)	Securely transfer files to and from the switch
Auto-configuration with SCP file download	Enables secure mass deployment with protection of sensitive data
Text-editable configuration files	Configuration files can be edited with a text editor and downloaded to another switch, facilitating easier mass deployment
Smartports	Simplified configuration of QoS and security capabilities
Auto Smartports	Applies the intelligence delivered through the Smartport roles and applies it automatically to the port based on the devices discovered over Cisco Discovery Protocol or LLDP-MED. This facilitates zero-touch deployments
Text view CLI	Scriptable CLI. A full CLI as well as a menu-based CLI is supported. User privilege levels 1, 7, and 15 are supported for the CLI
Localization	Localization of GUI and documentation into multiple languages
Login banner	Configurable multiple banners for web as well as CLI
Other management	Traceroute, single IP management, HTTP/HTTPS, SSH, RADIUS, port mirroring, TFTP upgrade, DHCP client, BOOTP, SNTP, Xmodem upgrade, cable diagnostics, ping, syslog, Telnet client (SSH secure support), automatic time settings from management station
Green (power efficiency)	
Energy detect	Automatically turns power off on an RJ-45 port when the detecting link down. Active mode is resumed without loss of any packets when the switch detects the link is up
Cable length detection	Adjusts the signal strength based on the cable length. Reduces the power consumption for shorter cables

EEE compliant (802.3az)	Supports IEEE 802.3az on all copper Gigabit Ethernet ports
Disable port LEDs	LEDs can be manually turned off to save energy
Time-based port operation	Link up or down based on user-defined schedule (when the port is administratively up)
General	
Jumbo frames	Frame sizes up to 9000 bytes. The default MTU is 2000 bytes
MAC table	16,000 addresses
Chip guard	Detects tampering attempts and responds during bootup
Boot integrity	Boot integrity visibility allows Cisco's platform identity and software integrity information to be visible and actionable
Discovery	
Bonjour	The switch advertises itself using the Bonjour protocol
Link Layer Discovery Protocol (LLDP) (802.1ab) with LLDP-Media Endpoint Discovery (MED) extensions	LLDP allows the switch to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a MIB. LLDP-MED is an enhancement to LLDP that adds the extensions needed for IP phones.
Cisco Discovery Protocol	The switch advertises itself using the Cisco Discovery Protocol. It also learns the connected device and its characteristics via Cisco Discovery Protocol
Hardware	
Power consumption (worst case)	
System power consumption	110V=49.46W 220V=49.02W
Heat dissipation (BTU/hr)	220.77

Idle Power	110V=21.5W 220V=21.3W
Ports	
Total system ports	20 x 10G SFP+ + 4 x 10G copper/SFP+ combo + 1 x GE OOB management
RJ-45 ports	20 x 10G SFP+
Combo ports (RJ-45 + Small Form-Factor Pluggable [SFP])	4 x 10G copper/SFP+ combo
Console port	Cisco standard RJ-45 console port and USB Type C port
USB port	USB Type C port on the front panel of the switch for easy file and image management as well as console port
Buttons	Reset button
Cabling type	Unshielded Twisted Pair (UTP) Category 5e or better for 1000BASE-T
LEDs	System, Link/Act, PoE, Speed
Flash	512 MB
CPU	ARM dual-core at 1.4 GHz
DRAM	1 GB DDR4
Packet buffer	All numbers are aggregate across all ports, as the buffers are dynamically shared: 8 MB
Supported SFP modules	MGBSX1 MGBLX1 MGBLH1 MGBT1 GLC-SX-MMD GLC-EX-SMD GLC-ZX-SMD GLC-LH-SMD GLC-BX-U GLC-BX-D GLC-TE

	CWDM-SFP-1470 CWDM-SFP-1490 CWDM-SFP-1510 CWDM-SFP-1530 CWDM-SFP-1550 CWDM-SFP-1570 CWDM-SFP-1590 CWDM-SFP-1610 SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-10G-SR SFP-10G-LR SFP-10G-SR-S SFP-10G-LR-S SFP-10G-ER SFP-10G-ER-S SFP-10G-T-X SFP-10G-BXD-I SFP-10G-BXU-I SFP-H10GB-CU1-5M SFP-H10GB-CU2M SFP-H10GB-CU2-5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
Environmental	
Unit dimensions (W x D x H)	445 x 350 x 44 mm (17.5 x 13.77 x 1.73 in)
Unit weight	4.15 kg (9.15 lb)
Power	100-240V 50-60 Hz, internal

Certifications	UL (UL 62368), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A
Operating temperature	23° to 122°F (-5° to 50°C)
Storage temperature	-13° to 158°F (-25° to 70°C)
Operating humidity	10% to 90%, relative, noncondensing
Storage humidity	10% to 90%, relative, noncondensing
Acoustic noise and mean time between failures (MTBF)	
FAN (number)	1
Acoustic noise	25°C: 27.6 dBA
MTBF at 25°C (hours)	993,232
Warranty	Limited lifetime with return-to-factory replacement
Package contents	
	Cisco Catalyst 1300 Series Switch
	Power cord
	Mounting kit
	Pointer card
Minimum requirements	
	Web browser: Chrome, Firefox, Edge, Safari
	Category 5e Ethernet network cable
	TCP/IP, network adapter, and network operating system (such as Microsoft Windows, Linux, or Mac OS X) installed

Specifikace D

Cisco Catalyst switch C1300-48T-4X

Cisco Catalyst řady 1300 jsou managovatelné switche Gigabit Ethernet Layer 3 podnikové třídy určené pro malé a střední podniky a pobočky. Tyto jednoduché, flexibilní a bezpečné switche jsou ideální pro nasazení mimo rozvodnou skříň. Řada Catalyst 1300 pracuje na přizpůsobeném softwaru operačního systému Linux s intuitivním grafickým rozhraním, který zjednodušuje nastavení sítě a pokročilými funkcemi, které urychlují digitální transformaci, zatímco všudypřítomné zabezpečení chrání kritické obchodní transakce. Přepínače řady 1300 poskytují ideální kombinaci cenové dostupnosti a možností pro malé a střední podniky a pomáhají vám vytvořit efektivnější a lépe propojenou pracovní sílu.

Stránky produktu: C1300-48T-4X

Performance	
Switching capacity and forwarding rate (All switches are wire-speed and nonblocking)	
Capacity in millions of packets per second (mpps) (64-byte packets)	130.94
Switching capacity in gigabits per second (Gbps)	176.0
Layer 2 switching	
Spanning Tree Protocol (STP)	Standard 802.1d spanning tree support Fast convergence using 802.1w (Rapid Spanning Tree Protocol [RSTP]), enabled by default Multiple spanning tree instances using 802.1s (MSTP); 8 instances are supported Per-VLAN Spanning Tree Plus (PVST+); 126 instances are supported Rapid PVST+ (RPVST+); 126 instances are supported
Port grouping/link aggregation	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) Up to 8 groups Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad link aggregation

VLAN	Support for up to 4093 VLANs simultaneously Port-based and 802.1Q tag-based VLANs, MAC-based VLAN, protocol-based VLAN, IP subnet-based VLAN Management VLAN Private VLAN with promiscuous, isolated, and community port Private VLAN Edge (PVE), also known as protected ports, with multiple uplinks Guest VLAN, unauthenticated VLAN Dynamic VLAN assignment via RADIUS server along with 802.1X client authentication Customer premises equipment (CPE) VLAN Auto surveillance VLAN (ASV)
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS. Voice Services Discovery Protocol (VSDP) delivers networkwide zero-touch deployment of voice endpoints and call control devices
Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. This feature is also known as Multicast VLAN Registration (MVR)
VLAN translation	Support for VLAN one-to-one mapping, in which customer VLANs (C-VLANs) on an edge interface are mapped to service provider VLANs (S-VLANs), and the original C-VLAN tags are replaced by the specified S-VLAN
Q-in-Q	VLANs transparently cross a service provider network while isolating traffic among customers
Selective Q-in-Q	Selective Q-in-Q is an enhancement to the basic Q-in-Q feature and provides, per edge interface, multiple mappings of different C-VLANs to separate S-VLANs Selective Q-in-Q also allows configuring of the Ethertype (Tag Protocol Identifier [TPID]) of the S-VLAN tag Layer 2 protocol tunneling over Q-in-Q is also supported
Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP)	GVRP and GARP enable automatic propagation and configuration of VLANs in a bridged domain
Unidirectional Link	UDLD monitors physical connections to detect unidirectional links caused by incorrect

Detection (UDLD)	wiring or cable/port faults to prevent forwarding loops and blackholing of traffic in switched networks
DHCP relay at Layer 2	Relay of DHCP traffic to a DHCP server in a different VLAN; works with DHCP Option 82
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; it supports 2000 multicast groups (source-specific multicasting is also supported)
IGMP querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router
IGMP proxy	The IGMP proxy provides a mechanism for multicast forwarding based on IGMP membership information without the need for more complicated multicast routing protocols
Head-of-Line (HOL) blocking	HOL blocking prevention
Loopback detection	Loopback detection provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. It operates independently of STP
Layer 3	
IPv4 routing	Wire-speed routing of IPv4 packets Up to 990 static routes and up to 128 IP interfaces
IPv6 routing	Wire-speed routing of IPv6 packets
Layer 3 interface	Configuration of a Layer 3 interface on a physical port, LAG, VLAN interface, or loopback interface
Classless Interdomain Routing (CIDR)	Support for CIDR
Routing Information Protocol (RIP) v2	Support for RIP v2 for dynamic routing
Policy-Based Routing (PBR)	Flexible routing control to direct packets to a different next hop based on an IPv4 or IPv6 Access Control List (ACL)

DHCP server	Switch functions as an IPv4 DHCP server, serving IP addresses for multiple DHCP pools or scopes Support for DHCP options
DHCP relay at Layer 3	Relay of DHCP traffic across IP domains
User Datagram Protocol (UDP) relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of Bootstrap Protocol (BOOTP)/DHCP packets
Stacking	
Hardware stacking	Up to 8 switches in a stack. Up to 200 ports managed as a single system with hardware failover Stacking is supported on the following models: Family 1: C1300-16P-4X, C1300-24T-4X, C1300-24P-4X, C1300-24FP-4X, C1300-48T-4X, C1300-48P-4X, C1300-48FP-4X, C1300-8MGP-2X, C1300-24MGP-4X, C1300-48MGP-4X Family 2: C1300-12XT-2X, C1300-12XS, C1300-16XTS, C1300-24XS, C1300-24XT, C1300-24XTS PIDs from the same Family can be stacked together. Cross-stacking between Families is not supported.
High availability	Fast stack failover delivers minimal traffic loss. Support for LAG across multiple units in a stack
Plug-and-play stacking configuration/management	Active/standby for resilient stack control Auto-numbering Hot swap of units in stack Ring and chain stacking options, auto stacking port speed, flexible stacking port options
High-speed stack interconnects	Cost-effective high-speed 10 Gigabit Ethernet fiber interfaces
Security	
Secure Shell (SSH) Protocol	SSH is a secure replacement for Telnet traffic. Secure Copy Protocol (SCP) also uses SSH. SSH v1 and v2 are supported
Secure Sockets Layer (SSL) SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based	

management GUI in the switch	
IEEE 802.1X (authenticator role)	802.1X: RADIUS authentication and accounting, MD5 hash, guest VLAN, unauthenticated VLAN, single/multiple host mode, and single/multiple sessions Supports time-based 802.1X, dynamic VLAN assignment, and MAC authentication
IEEE 802.1X supplicant	A switch can be configured to act as a supplicant to another switch. This enables extended secure access in areas outside the wiring closet (such as conference rooms)
Web-based authentication	Web-based authentication provides network admission control through a web browser to any host devices and operating systems
STP Bridge Protocol Data Unit (BPDU) Guard	A security mechanism to protect the network from invalid configurations. A port enabled for BPDU Guard is shut down if a BPDU message is received on that port. This avoids accidental topology loops
STP Root Guard	Prevents edge devices not in the network administrator’s control from becoming STP root nodes
STP loopback guard	Provides additional protection against Layer 2 forwarding loops (STP loops)
DHCP snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as DHCP servers
IP Source Guard (IPSG)	When IPSG is enabled at a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP address spoofing
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there are no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or destination addresses in the ARP packet. This prevents man-in-the-middle attacks
IP/MAC/port binding (IPMB)	The preceding features (DHCP snooping, IPSG, and DAI) work together to prevent Denial-of-Service (DoS) attacks in the network, thereby increasing network availability

Secure Core Technology (SCT)	Makes sure that the switch will receive and process management and protocol traffic no matter how much traffic is received
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, and so on) securely on the switch, populating this data to other devices and a secure auto-configuration. Access to view the sensitive data as plain text or encrypted is provided according to the user-configured access level and the access method of the user
Trustworthy systems	Trustworthy systems provide a highly secure foundation for Cisco products Run-time defenses (Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC])
Private VLAN	Provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic; supports multiple uplinks.
Layer 2 isolation Private VLAN Edge (PVE)	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN; supports multiple uplinks
Port security	Ability to lock source MAC addresses to ports and limit the number of learned MAC addresses
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client
RADIUS accounting	The RADIUS accounting functions allow data to be sent at the start and end of services indicating the number of resources (such as time, packets, bytes, and so on) used during the session
Storm control	Broadcast, multicast, and unknown unicast
DoS prevention	DoS attack prevention
Multiple user privilege levels in CLI	Level 1, 7, and 15 privilege levels
ACLs	Support for up to 1024 rules Drop or rate limit based on source and destination MAC, VLAN ID, IPv4 or IPv6 address, IPv6 flow label, protocol, port, Differentiated Services Code Point (DSCP)/IP precedence, TCP/UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag; ACL can be applied on both ingress and egress sides Time-based ACLs supported

Quality of service	
Priority levels	8 hardware queues
Scheduling	Strict priority and Weighted Round-Robin (WRR)
Class of service	Port-based, 802.1p VLAN priority-based, IPv4/IPv6 IP precedence/Type of Service (ToS)/DSCP-based, Differentiated Services (DiffServ), classification and remarking ACLs, trusted QoS Queue assignment based on DSCP and Class of Service (802.1p/CoS)
Rate limiting	Ingress policer; egress shaping and rate control per VLAN, per port, and flow based; dual-rate 3-color (2R3C) policing
Congestion avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization
iSCSI traffic optimization	A mechanism for giving priority to iSCSI traffic over other types of traffic
Standards	
Standards	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN, IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 826, RFC 879, RFC 896, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 920, RFC 922, RFC 950, RFC 951, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1213, RFC 1215, RFC 1286, RFC 1350, RFC 1442, RFC 1451, RFC 1493, RFC 1533, RFC 1541, RFC 1542, RFC 1573, RFC 1624, RFC 1643, RFC 1700, RFC 1757, RFC 1867, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2030, RFC 2131, RFC 2132, RFC 2233, RFC 2576, RFC

	2616, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 3164, RFC 3176, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 4330
IPv6	
IPv6	IPv6 host mode, IPv6 over Ethernet, dual IPv6/IPv4 stack IPv6 neighbor and router discovery (ND), IPv6 stateless address auto-configuration, path Maximum Transmission Unit (MTU) discovery Duplicate Address Detection (DAD), ICMP version 6 DHCPv6 stateful client IPv6 over IPv4 network with Intrasite Automatic Tunnel Addressing Protocol (ISATAP) tunnel support
IPv6 QoS	Prioritize IPv6 packets in hardware
IPv6 ACL	Drop or rate-limit IPv6 packets in hardware
IPv6 First Hop Security	RA guard ND inspection DHCPv6 guard Neighbor binding table (snooping and static entries) Neighbor binding integrity check
Multicast Listener Discovery (MLD v1/2) snooping	Deliver IPv6 multicast packets only to the required receivers
MLD proxy	The MLD proxy provides a mechanism for multicast forwarding based on MLD membership information without the need for more complicated multicast routing protocols
IPv6 applications	Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, Telnet client, DHCP client, DHCP auto-config, IPv6 DHCP relay, TACACS+
IPv6 RFCs supported	RFC 4443 (which obsoletes RFC 2463): ICMP version 6 RFC 4291 (which obsoletes RFC 3513): IPv6 address architecture RFC 4291: IPv6 addressing architecture RFC 2460: IPv6 specification RFC 4861 (which obsoletes RFC 2461): neighbor discovery for IPv6 RFC 4862 (which obsoletes RFC 2462): IPv6 stateless address auto-

	configuration RFC 1981: path MTU discovery RFC 4007: IPv6 scoped address architecture RFC 3484: default address selection mechanism RFC 5214 (which obsoletes RFC 4214): ISATAP tunneling RFC 4293: MIB IPv6: textual conventions and general group RFC 3595: textual conventions for IPv6 flow label
Management	
Cisco Business Dashboard	Support for embedded probe for Cisco Business Dashboard running on the s witch. Eliminates the need to set up a separate hardware or virtual machine for the Cisco Business Dashboard Probe onsite
Cisco Business mobile app	Mobile app for Cisco Business switch and wireless products. Helps to set up a local network in minutes and provide easy management at your fingertips
Cisco Network Plug and Play (PnP) agent	The Cisco Network PnP solution provides a simple, secure, unified, and integr ated offering to ease new branch or campus device rollouts or for provisioning updates to an existing network. The solution provides a unified approach to provision Cisco routers, switches, and wireless devices with a near-zero-touch deployment experience. Supports Cisco PnP Connect
Web user interface	Built-in switch configuration utility for easy browser-based device configuration (HTTP/HTTPS) Supports simple and advanced mode, configuration, wizards, customizable dashboard, system maintenance, monitoring, online help, and universal search
SNMP	SNMP versions 1, 2c, and 3 with support for traps, and SNMP version 3 User-Based Security Model (USM)
Remote Monitoring (RMON)	Embedded RMON software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis
IPv4 and IPv6 dual stack	Coexistence of both protocol stacks to ease migration
Firmware upgrade	Web browser upgrade (HTTP/HTTPS) and TFTP and upgrade over SCP running over SSH Dual images for resilient firmware upgrades

Port mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer or RMON probe. Up to 8 source ports can be mirrored to one destination port
VLAN mirroring	Traffic from a VLAN can be mirrored to a port for analysis with a network analyzer or RMON probe. Up to 8 source VLANs can be mirrored to one destination port
Flow-based redirection and mirroring	Redirect or mirror traffic to a destination port or mirroring session based on flow
Remote Switch Port Analyzer (RSPAN)	Traffic can be mirrored across a Layer 2 domain to a remote port on a different switch for easier troubleshooting
sFlow agent	Switch can export sFlow sample to external collectors. sFlow provides visibility into network traffic down to the flow level
DHCP (options 12, 59, 60, 66, 67, 82, 125, 129, and 150)	DHCP options facilitate tighter control from a central point (DHCP server) to obtain IP address, auto-configuration (with configuration and image file download), DHCP relay, and hostname
Secure Copy (SCP)	Securely transfer files to and from the switch
Auto-configuration with SCP file download	Enables secure mass deployment with protection of sensitive data
Text-editable configuration files	Configuration files can be edited with a text editor and downloaded to another switch, facilitating easier mass deployment
Smartports	Simplified configuration of QoS and security capabilities
Auto Smartports	Applies the intelligence delivered through the Smartport roles and applies it automatically to the port based on the devices discovered over Cisco Discovery Protocol or LLDP-MED. This facilitates zero-touch deployments
Text view CLI	Scriptable CLI. A full CLI as well as a menu-based CLI is supported. User privilege levels 1, 7, and 15 are supported for the CLI
Localization	Localization of GUI and documentation into multiple languages
Login banner	Configurable multiple banners for web as well as CLI
Other management	Traceroute, single IP management, HTTP/HTTPS, SSH, RADIUS, port mirroring, TFTP upgrade, DHCP client, BOOTP, SNTP, Xmodem upgrade, cable

	diagnostics, ping, syslog, Telnet client (SSH secure support), automatic time settings from management station
Green (power efficiency)	
Energy detect	Automatically turns power off on an RJ-45 port when the detecting link down. Active mode is resumed without loss of any packets when the switch detects the link is up
Cable length detection	Adjusts the signal strength based on the cable length. Reduces the power consumption for shorter cables
EEE compliant (802.3az)	Supports IEEE 802.3az on all copper Gigabit Ethernet ports
Disable port LEDs	LEDs can be manually turned off to save energy
Time-based port operation	Link up or down based on user-defined schedule (when the port is administratively up)
General	
Jumbo frames	Frame sizes up to 9000 bytes. The default MTU is 2000 bytes
MAC table	16,000 addresses
Chip guard	Detects tampering attempts and responds during bootup
Boot integrity	Boot integrity visibility allows Cisco's platform identity and software integrity information to be visible and actionable
Discovery	
Bonjour	The switch advertises itself using the Bonjour protocol
Link Layer Discovery Protocol (LLDP) (802.1ab) with LLDP-Media Endpoint Discovery (MED) extensions	LLDP allows the switch to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a MIB. LLDP-MED is an enhancement to LLDP that adds the extensions needed for IP phones.
Cisco Discovery Protocol	The switch advertises itself using the Cisco Discovery Protocol. It also learns the connected device and its characteristics via Cisco Discovery Protocol

Hardware	
Power consumption (worst case)	
System power consumption	110V=40.01W 220V=39.77W
Heat dissipation (BTU/hr)	136.5
Idle Power	110V=13.12W 220V=12.93W
Ports	
Total system ports	48 x Gigabit Ethernet + 4 x 10G
RJ-45 ports	48 x Gigabit Ethernet
Combo ports (RJ-45 + Small Form-Factor Pluggable [SFP])	4 x SFP+
Console port	Cisco standard RJ-45 console port and USB Type C port
USB port	USB Type C port on the front panel of the switch for easy file and image management as well as console port
Buttons	Reset button
Cabling type	Unshielded Twisted Pair (UTP) Category 5e or better for 1000BASE-T
LEDs	System, Link/Act, PoE, Speed
Flash	512 MB
CPU	ARM dual-core at 1.4 GHz
DRAM	1 GB DDR4
Packet buffer	All numbers are aggregate across all ports, as the buffers are dynamically shared: 1.5 MB

Supported SFP modules	MGBSX1 MGBLX1 MGBLH1 MGBT1 GLC-SX-MMD GLC-EX-SMD GLC-ZX-SMD GLC-LH-SMD GLC-BX-U GLC-BX-D GLC-TE CWDM-SFP-1470 CWDM-SFP-1490 CWDM-SFP-1510 CWDM-SFP-1530 CWDM-SFP-1550 CWDM-SFP-1570 CWDM-SFP-1590 CWDM-SFP-1610 SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-10G-SR SFP-10G-LR SFP-10G-SR-S SFP-10G-LR-S SFP-10G-ER SFP-10G-ER-S SFP-10G-T-X SFP-10G-BXD-I SFP-10G-BXU-I SFP-H10GB-CU1-5M SFP-H10GB-CU2M SFP-H10GB-CU2-5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M

	SFP-10G-AOC7M SFP-10G-AOC10M
Environmental	
Unit dimensions (W x D x H)	445 x 288 x 44 mm (17.5 x 11.33 x 1.73 in)
Unit weight	4.35 kg (9.59 lb)
Power	100-240V 50-60 Hz, internal
Certifications	UL (UL 62368), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A
Operating temperature	23° to 122°F (-5° to 50°C)
Storage temperature	-13° to 158°F (-25° to 70°C)
Operating humidity	10% to 90%, relative, noncondensing
Storage humidity	10% to 90%, relative, noncondensing
Acoustic noise and mean time between failures (MTBF)	
FAN (number)	1
Acoustic noise	25°C: 29.7 dBA
MTBF at 25°C (hours)	1,473,382
Warranty	Limited lifetime with return-to-factory replacement
Package contents	
	Cisco Catalyst 1300 Series Switch
	Power cord
	Mounting kit
	Pointer card
Minimum requirements	

Web browser: Chrome, Firefox, Edge, Safari

Category 5e Ethernet network cable

TCP/IP, network adapter, and network operating system (such as Microsoft Windows, Linux, or Mac OS X) installed

Specifikace E

Cisco Catalyst switch C1300-48FP-4X

Cisco Catalyst řady 1300 jsou managovatelné switche Gigabit Ethernet Layer 3 podnikové třídy určené pro malé a střední podniky a pobočky. Tyto jednoduché, flexibilní a bezpečné switche jsou ideální pro nasazení mimo rozvodnou skříň. Řada Catalyst 1300 pracuje na přizpůsobeném softwaru operačního systému Linux s intuitivním grafickým rozhraním, který zjednodušuje nastavení sítě a pokročilými funkcemi, které urychlují digitální transformaci, zatímco všudypřítomné zabezpečení chrání kritické obchodní transakce. Přepínače řady 1300 poskytují ideální kombinaci cenové dostupnosti a možností pro malé a střední podniky a pomáhají vám vytvořit efektivnější a lépe propojenou pracovní sílu.

Stránky produktu: C1300-48FP-4X

Performance

Switching capacity and forwarding rate (All switches are wire-speed and nonblocking)	
Capacity in millions of packets per second (mpps) (64-byte packets)	130.94
Switching capacity in gigabits per second (Gbps)	176.0

Layer 2 switching

Spanning Tree Protocol (STP)	Standard 802.1d spanning tree support Fast convergence using 802.1w (Rapid Spanning Tree Protocol [RSTP]), enabled by default Multiple spanning tree instances using 802.1s (MSTP); 8 instances are supported Per-VLAN Spanning Tree Plus (PVST+); 126 instances are supported Rapid PVST+ (RPVST+); 126 instances are supported
Port grouping/link aggregation	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) Up to 8 groups Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad link aggregation
VLAN	Support for up to 4093 VLANs simultaneously Port-based and 802.1Q tag-based VLANs, MAC-based VLAN, protocol-based VLAN, IP subnet-based VLAN Management VLAN Private VLAN with promiscuous, isolated, and community port Private VLAN Edge (PVE), also known as protected ports, with multiple uplinks Guest VLAN, unauthenticated VLAN Dynamic VLAN assignment via RADIUS server along with 802.1X client authentication Customer premises equipment (CPE) VLAN Auto surveillance VLAN (ASV)
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS. Voice Services Discovery Protocol (VSDP) delivers networkwide zero-touch deployment of voice endpoints and call control devices
Multicast TV VLAN	Multicast TV VLAN allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. This feature is also known as Multicast VLAN Registration (MVR)
VLAN translation	Support for VLAN one-to-one mapping, in which customer VLANs (C-VLANs) on an edge interface are mapped to service provider VLANs (S-VLANs), and the original C-VLAN tags are replaced by the specified S-VLAN
Q-in-Q	VLANs transparently cross a service provider network while isolating traffic among customers
Selective Q-in-Q	Selective Q-in-Q is an enhancement to the basic Q-in-Q feature and provides, per edge interface, multiple mappings of different C-VLANs to separate S-VLANs

	Selective Q-in-Q also allows configuring of the Ethertype (Tag Protocol Identifier [TPID]) of the S-VLAN tag Layer 2 protocol tunneling over Q-in-Q is also supported
Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP)	GVRP and GARP enable automatic propagation and configuration of VLANs in a bridged domain
Unidirectional Link	UDLD monitors physical connections to detect unidirectional links caused by incorrect
Detection (UDLD)	wiring or cable/port faults to prevent forwarding loops and blackholing of traffic in switched networks
DHCP relay at Layer 2	Relay of DHCP traffic to a DHCP server in a different VLAN; works with DHCP Option 82
Internet Group Management Protocol (IGMP) versions 1, 2, and 3 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; it supports 2000 multicast groups (source-specific multicasting is also supported)
IGMP querier	IGMP querier is used to support a Layer 2 multicast domain of snooping switches in the absence of a multicast router
IGMP proxy	The IGMP proxy provides a mechanism for multicast forwarding based on IGMP membership information without the need for more complicated multicast routing protocols
Head-of-Line (HOL) blocking	HOL blocking prevention
Loopback detection	Loopback detection provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. It operates independently of STP
Layer 3	
IPv4 routing	Wire-speed routing of IPv4 packets Up to 990 static routes and up to 128 IP interfaces
IPv6 routing	Wire-speed routing of IPv6 packets

Layer 3 interface	Configuration of a Layer 3 interface on a physical port, LAG, VLAN interface, or loopback interface
Classless Interdomain Routing (CIDR)	Support for CIDR
Routing Information Protocol (RIP) v2	Support for RIP v2 for dynamic routing
Policy-Based Routing (PBR)	Flexible routing control to direct packets to a different next hop based on an IPv4 or IPv6 Access Control List (ACL)
DHCP server	Switch functions as an IPv4 DHCP server, serving IP addresses for multiple DHCP pools or scopes Support for DHCP options
DHCP relay at Layer 3	Relay of DHCP traffic across IP domains
User Datagram Protocol (UDP) relay	Relay of broadcast information across Layer 3 domains for application discovery or relaying of Bootstrap Protocol (BOOTP)/DHCP packets
Stacking	
Hardware stacking	Up to 8 switches in a stack. Up to 200 ports managed as a single system with hardware failover Stacking is supported on the following models: Family 1: C1300-16P-4X, C1300-24T-4X, C1300-24P-4X, C1300-24FP-4X, C1300-48T-4X, C1300-48P-4X, C1300-48FP-4X, C1300-8MGP-2X, C1300-24MGP-4X, C1300-48MGP-4X Family 2: C1300-12XT-2X, C1300-12XS, C1300-16XTS, C1300-24XS, C1300-24XT, C1300-24XTS PIDs from the same Family can be stacked together. Cross-stacking between Families is not supported.
High availability	Fast stack failover delivers minimal traffic loss. Support for LAG across multiple units in a stack
Plug-and-play stacking configuration/management	Active/standby for resilient stack control Auto-numbering Hot swap of units in stack Ring and chain stacking options, auto stacking port speed, flexible stacking port options

High-speed stack interconnects	Cost-effective high-speed 10 Gigabit Ethernet fiber interfaces
Security	
Secure Shell (SSH) Protocol	SSH is a secure replacement for Telnet traffic. Secure Copy Protocol (SCP) also uses SSH. SSH v1 and v2 are supported
Secure Sockets Layer (SSL) SSL support: Encrypts all HTTPS traffic, allowing highly secure access to the browser-based management GUI in the switch	
IEEE 802.1X (authenticator role)	802.1X: RADIUS authentication and accounting, MD5 hash, guest VLAN, unauthenticated VLAN, single/multiple host mode, and single/multiple sessions Supports time-based 802.1X, dynamic VLAN assignment, and MAC authentication
IEEE 802.1X supplicant	A switch can be configured to act as a supplicant to another switch. This enables extended secure access in areas outside the wiring closet (such as conference rooms)
Web-based authentication	Web-based authentication provides network admission control through a web browser to any host devices and operating systems
STP Bridge Protocol Data Unit (BPDU) Guard	A security mechanism to protect the network from invalid configurations. A port enabled for BPDU Guard is shut down if a BPDU message is received on that port. This avoids accidental topology loops
STP Root Guard	Prevents edge devices not in the network administrator’s control from becoming STP root nodes
STP loopback guard	Provides additional protection against Layer 2 forwarding loops (STP loops)
DHCP snooping	Filters out DHCP messages with unregistered IP addresses and/or from unexpected or untrusted interfaces. This prevents rogue devices from behaving as DHCP servers

IP Source Guard (IPSG)	When IPSG is enabled at a port, the switch filters out IP packets received from the port if the source IP addresses of the packets have not been statically configured or dynamically learned from DHCP snooping. This prevents IP address spoofing
Dynamic ARP Inspection (DAI)	The switch discards ARP packets from a port if there are no static or dynamic IP/MAC bindings or if there is a discrepancy between the source or destination addresses in the ARP packet. This prevents man-in-the-middle attacks
IP/MAC/port binding (IPMB)	The preceding features (DHCP snooping, IPSG, and DAI) work together to prevent Denial-of-Service (DoS) attacks in the network, thereby increasing network availability
Secure Core Technology (SCT)	Makes sure that the switch will receive and process management and protocol traffic no matter how much traffic is received
Secure Sensitive Data (SSD)	A mechanism to manage sensitive data (such as passwords, keys, and so on) securely on the switch, populating this data to other devices and a secure auto-configuration. Access to view the sensitive data as plain text or encrypted is provided according to the user-configured access level and the access method of the user
Trustworthy systems	Trustworthy systems provide a highly secure foundation for Cisco products Run-time defenses (Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC])
Private VLAN	Provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic; supports multiple uplinks.
Layer 2 isolation Private VLAN Edge (PVE)	PVE (also known as protected ports) provides Layer 2 isolation between devices in the same VLAN; supports multiple uplinks
Port security	Ability to lock source MAC addresses to ports and limit the number of learned MAC addresses
RADIUS/TACACS+	Supports RADIUS and TACACS authentication. Switch functions as a client
RADIUS accounting	The RADIUS accounting functions allow data to be sent at the start and end of services indicating the number of resources (such as time, packets, bytes, and so on) used during the session

Storm control	Broadcast, multicast, and unknown unicast
DoS prevention	DoS attack prevention
Multiple user privilege levels in CLI	Level 1, 7, and 15 privilege levels
ACLs	Support for up to 1024 rules Drop or rate limit based on source and destination MAC, VLAN ID, IPv4 or IPv6 address, IPv6 flow label, protocol, port, Differentiated Services Code Point (DSCP)/IP precedence, TCP/UDP source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, IGMP packets, TCP flag; ACL can be applied on both ingress and egress sides Time-based ACLs supported
Quality of service	
Priority levels	8 hardware queues
Scheduling	Strict priority and Weighted Round-Robin (WRR)
Class of service	Port-based, 802.1p VLAN priority-based, IPv4/IPv6 IP precedence/Type of Service (ToS)/DSCP-based, Differentiated Services (DiffServ), classification and remarking ACLs, trusted QoS Queue assignment based on DSCP and Class of Service (802.1p/CoS)
Rate limiting	Ingress policer; egress shaping and rate control per VLAN, per port, and flow based; dual-rate 3-color (2R3C) policing
Congestion avoidance	A TCP congestion avoidance algorithm is required to minimize and prevent global TCP loss synchronization
iSCSI traffic optimization	A mechanism for giving priority to iSCSI traffic over other types of traffic
Standards	
Standards	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN, IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE

	802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 826, RFC 879, RFC 896, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 920, RFC 922, RFC 950, RFC 951, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1157, RFC 1213, RFC 1215, RFC 1286, RFC 1350, RFC 1442, RFC 1451, RFC 1493, RFC 1533, RFC 1541, RFC 1542, RFC 1573, RFC 1624, RFC 1643, RFC 1700, RFC 1757, RFC 1867, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2030, RFC 2131, RFC 2132, RFC 2233, RFC 2576, RFC 2616, RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 3164, RFC 3176, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 4330
IPv6	
IPv6	IPv6 host mode, IPv6 over Ethernet, dual IPv6/IPv4 stack IPv6 neighbor and router discovery (ND), IPv6 stateless address auto-configuration, path Maximum Transmission Unit (MTU) discovery Duplicate Address Detection (DAD), ICMP version 6 DHCPv6 stateful client IPv6 over IPv4 network with Intrasite Automatic Tunnel Addressing Protocol (ISATAP) tunnel support
IPv6 QoS	Prioritize IPv6 packets in hardware
IPv6 ACL	Drop or rate-limit IPv6 packets in hardware
IPv6 First Hop Security	RA guard ND inspection DHCPv6 guard Neighbor binding table (snooping and static entries) Neighbor binding integrity check
Multicast Listener Discovery (MLD v1/2) snooping	Deliver IPv6 multicast packets only to the required receivers

MLD proxy	The MLD proxy provides a mechanism for multicast forwarding based on MLD membership information without the need for more complicated multicast routing protocols
IPv6 applications	Web/SSL, Telnet server/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, syslog, DNS client, Telnet client, DHCP client, DHCP auto-config, IPv6 DHCP relay, TACACS+
IPv6 RFCs supported	RFC 4443 (which obsoletes RFC 2463): ICMP version 6 RFC 4291 (which obsoletes RFC 3513): IPv6 address architecture RFC 4291: IPv6 addressing architecture RFC 2460: IPv6 specification RFC 4861 (which obsoletes RFC 2461): neighbor discovery for IPv6 RFC 4862 (which obsoletes RFC 2462): IPv6 stateless address auto-configuration RFC 1981: path MTU discovery RFC 4007: IPv6 scoped address architecture RFC 3484: default address selection mechanism RFC 5214 (which obsoletes RFC 4214): ISATAP tunneling RFC 4293: MIB IPv6: textual conventions and general group RFC 3595: textual conventions for IPv6 flow label
Management	
Cisco Business Dashboard	Support for embedded probe for Cisco Business Dashboard running on the s witch. Eliminates the need to set up a separate hardware or virtual machine for the Cisco Business Dashboard Probe onsite
Cisco Business mobile app	Mobile app for Cisco Business switch and wireless products. Helps to set up a local network in minutes and provide easy management at your fingertips
Cisco Network Plug and Play (PnP) agent	The Cisco Network PnP solution provides a simple, secure, unified, and integr ated offering to ease new branch or campus device rollouts or for provisioning updates to an existing network. The solution provides a unified approach to provision Cisco routers, switches, and wireless devices with a near-zero-touch deployment experience. Supports Cisco PnP Connect
Web user interface	Built-in switch configuration utility for easy browser-based device configuration (HTTP/HTTPS) Supports simple and advanced mode, configuration, wizards, customizable

	dashboard, system maintenance, monitoring, online help, and universal search
SNMP	SNMP versions 1, 2c, and 3 with support for traps, and SNMP version 3 User-Based Security Model (USM)
Remote Monitoring (RMON)	Embedded RMON software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis
IPv4 and IPv6 dual stack	Coexistence of both protocol stacks to ease migration
Firmware upgrade	Web browser upgrade (HTTP/HTTPS) and TFTP and upgrade over SCP running over SSH Dual images for resilient firmware upgrades
Port mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer or RMON probe. Up to 8 source ports can be mirrored to one destination port
VLAN mirroring	Traffic from a VLAN can be mirrored to a port for analysis with a network analyzer or RMON probe. Up to 8 source VLANs can be mirrored to one destination port
Flow-based redirection and mirroring	Redirect or mirror traffic to a destination port or mirroring session based on flow
Remote Switch Port Analyzer (RSPAN)	Traffic can be mirrored across a Layer 2 domain to a remote port on a different switch for easier troubleshooting
sFlow agent	Switch can export sFlow sample to external collectors. sFlow provides visibility into network traffic down to the flow level
DHCP (options 12, 59, 60, 66, 67, 82, 125, 129, and 150)	DHCP options facilitate tighter control from a central point (DHCP server) to obtain IP address, auto-configuration (with configuration and image file download), DHCP relay, and hostname
Secure Copy (SCP)	Securely transfer files to and from the switch
Auto-configuration with SCP file download	Enables secure mass deployment with protection of sensitive data
Text-editable configuration files	Configuration files can be edited with a text editor and downloaded to another switch, facilitating easier mass deployment

Smartports	Simplified configuration of QoS and security capabilities
Auto Smartports	Applies the intelligence delivered through the Smartport roles and applies it automatically to the port based on the devices discovered over Cisco Discovery Protocol or LLDP-MED. This facilitates zero-touch deployments
Text view CLI	Scriptable CLI. A full CLI as well as a menu-based CLI is supported. User privilege levels 1, 7, and 15 are supported for the CLI
Localization	Localization of GUI and documentation into multiple languages
Login banner	Configurable multiple banners for web as well as CLI
Other management	Traceroute, single IP management, HTTP/HTTPS, SSH, RADIUS, port mirroring, TFTP upgrade, DHCP client, BOOTP, SNTP, Xmodem upgrade, cable diagnostics, ping, syslog, Telnet client (SSH secure support), automatic time settings from management station
Green (power efficiency)	
Energy detect	Automatically turns power off on an RJ-45 port when the detecting link down. Active mode is resumed without loss of any packets when the switch detects the link is up
Cable length detection	Adjusts the signal strength based on the cable length. Reduces the power consumption for shorter cables
EEE compliant (802.3az)	Supports IEEE 802.3az on all copper Gigabit Ethernet ports
Disable port LEDs	LEDs can be manually turned off to save energy
Time-based port operation	Link up or down based on user-defined schedule (when the port is administratively up)
Time-based PoE	PoE power can be on or off based on a user-defined schedule to save energy
Persistent PoE	Provides PoE power while the device is rebooting
General	
Jumbo frames	Frame sizes up to 9000 bytes. The default MTU is 2000 bytes
MAC table	16,000 addresses

Chip guard	Detects tampering attempts and responds during bootup
Boot integrity	Boot integrity visibility allows Cisco's platform identity and software integrity information to be visible and actionable
Discovery	
Bonjour	The switch advertises itself using the Bonjour protocol
Link Layer Discovery Protocol (LLDP) (802.1ab) with LLDP-Media Endpoint Discovery (MED) extensions	LLDP allows the switch to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a MIB. LLDP-MED is an enhancement to LLDP that adds the extensions needed for IP phones.
Cisco Discovery Protocol	The switch advertises itself using the Cisco Discovery Protocol. It also learns the connected device and its characteristics via Cisco Discovery Protocol
Power over Ethernet (PoE)	
802.3af PoE, 802.3at PoE+ (The following switches support 802.3at PoE+, 802.3af, and Cisco pre-standard (legacy) PoE. The total power available for PoE per switch is as follows)	
Power dedicated to PoE	740W
Number of ports that support PoE	48
Hardware	
Power consumption (worst case)	
System power consumption	110V=49.89 220V=49.03

Power consumption (with PoE)	110V=874.52W 220V=831.71W
Heat dissipation (BTU/hr)	2983.99
Idle Power	110V=21.78W 220V=21.05W
Ports	
Total system ports	48 x Gigabit Ethernet + 4 x 10G
RJ-45 ports	48 x Gigabit Ethernet
Combo ports (RJ-45 + Small Form-Factor Pluggable [SFP])	4 x SFP+
Console port	Cisco standard RJ-45 console port and USB Type C port
USB port	USB Type C port on the front panel of the switch for easy file and image management as well as console port
Buttons	Reset button
Cabling type	Unshielded Twisted Pair (UTP) Category 5e or better for 1000BASE-T
LEDs	System, Link/Act, PoE, Speed
Flash	512 MB
CPU	ARM dual-core at 1.4 GHz
DRAM	1 GB DDR4
Packet buffer	All numbers are aggregate across all ports, as the buffers are dynamically shared: 1.5 MB
Supported SFP modules	MGBSX1 MGBLX1 MGBLH1 MGBT1 GLC-SX-MMD GLC-EX-SMD

GLC-ZX-SMD
GLC-LH-SMD
GLC-BX-U
GLC-BX-D
GLC-TE
CWDM-SFP-1470
CWDM-SFP-1490
CWDM-SFP-1510
CWDM-SFP-1530
CWDM-SFP-1550
CWDM-SFP-1570
CWDM-SFP-1590
CWDM-SFP-1610
SFP-H10GB-CU1M
SFP-H10GB-CU3M
SFP-H10GB-CU5M
SFP-10G-SR
SFP-10G-LR
SFP-10G-SR-S
SFP-10G-LR-S
SFP-10G-ER
SFP-10G-ER-S
SFP-10G-T-X
SFP-10G-BXD-I
SFP-10G-BXU-I
SFP-H10GB-CU1-5M
SFP-H10GB-CU2M
SFP-H10GB-CU2-5M
SFP-H10GB-ACU7M
SFP-H10GB-ACU10M
SFP-10G-AOC1M
SFP-10G-AOC2M
SFP-10G-AOC3M
SFP-10G-AOC5M
SFP-10G-AOC7M
SFP-10G-AOC10M

Environmental

Unit dimensions (W x D x H)	445 x 350 x 44 mm (17.5 x 13.78 x 1.73 in)
Unit weight	5.16 kg (11.38 lb)
Power	100-240V 50-60 Hz, internal
Certifications	UL (UL 62368), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A
Operating temperature	23° to 122°F (-5° to 50°C)
Storage temperature	-13° to 158°F (-25° to 70°C)
Operating humidity	10% to 90%, relative, noncondensing
Storage humidity	10% to 90%, relative, noncondensing
Acoustic noise and mean time between failures (MTBF)	
FAN (number)	1
Acoustic noise	25°C: 48.7 dBA
MTBF at 25°C (hours)	1,469,406
Warranty	Limited lifetime with return-to-factory replacement
Package contents	
	Cisco Catalyst 1300 Series Switch
	Power adapter
	Mounting kit
	Pointer card
Minimum requirements	
	Web browser: Chrome, Firefox, Edge, Safari
	Category 5e Ethernet network cable

TCP/IP, network adapter, and network operating system (such as Microsoft Windows, Linux, or Mac OS X) installed

Specifikace F

UBNT UniFi U7-Pro

Popis produktu
Ubiquiti U7 Pro je nový třípásmový access point. K síti jej připojíte pomocí běžného LAN portu s rychlostí až 2,5 Gb/s. Bezdrátové frekvence jsou 2,4 GHz s rychlostí 688 Mb/s, 5 GHz s rychlostí 2880 Mb/s a 6 GHz pásmo s rychlostí 5760 Mb/s. Access point je napájen pomocí protokolu PoE+ a jeho maximální spotřeba je 21 W. Poskytuje internetové připojení pro více než 300 zařízení najednou.
Klíčové vlastnosti

- Vysoká rychlost až 5760 Mb/s v pásmu 6 GHz
- Napájení přes PoE+
- Připojení pro více než 300 zařízení zároveň

Obsah balení

- Zařízení
- Montážní kit na zeď/strop

Technické parametry
Bezdrátové vlastnosti
Bezdrátové frekvence:2.4 + 5 + 6 GHz (triple band)
WiFi standardy:802.11n, 802.11a, 802.11ac, 802.11b/g, 802.11ax, 802.11be
MU-MIMO:Ano
Přenosová rychlost - 5GHz [Mb/s]:2880
Přenosová rychlost - 2.4GHz [Mb/s]:688
Přenosová rychlost - 6GHz [Mb/s]:5760
Vysílací výkon 2.4GHz [dBm]:22
Vysílací výkon 5GHz [dBm]:26
Vysílací výkon 6GHz [dBm]:23
Šifrování:WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)
2.4GHz MIMO:2 x 2
5GHz MIMO:2 x 2
6GHz MIMO:2 x 2
Typ antény:Vestavěná
Počet vestavěných antén:6
Konektory a rozhraní
Rychlost LAN:(1) 100/1000/2500Mbps
Gigabit LAN:Ano

Napájení
Napájení přes PoE:802.3at+
Max. spotřeba energie [W]:21
Fyzické charakteristiky
Použití:Vnitřní
Tlačítka:Reset
Provozní teplota [°C]:-30 až 60
Hmotnost [g]:680
Šířka [mm]:206
Výška [mm]:46
Hloubka [mm]:206
Software
Operační mód:Access Point

Záruka 36 měsíců

Specifikace G

DAC SFP+ 10Gbps pro Cisco délky 0,5m.

SFP+ pasivní metalický kabel pro lokální propojení dvou aktivních prvků přes SFP+ sloty, 10Gbps multirate, délka 0,5m, Cisco/ Fortinet kompatibilní verze do 3m délky AWG30, nad 3m AWG24

Záruka 36 měsíců

SFP+ transceiver 10Gbps, 10GBASE-T, do 30m (CAT 6A či 7), RJ-45, 0 až 70°C, Cisco komp.

SFP+ transceiver 10Gbps, 10GBASE-T, do 30m, RJ-45, 0 až 70°C, Cisco komp. dosah do 30m (CAT 6A či 7) multirate 10Gbps/ 5Gbps/ 2,5Gbps/1Gbps 1000M Transmission Distance: 100m 2.5G, 5G Transmission Distance: 50m 10G Transmission Distance: 30m

Záruka 36 měsíců

SFP+ transceiver 10GBASE-SR/SW, multirate, MM, OM3-300/OM2-82/OM1-33m, 850nm VCSEL, LC duplex, DMI , Cisco

SFP+ transceiver 10GBASE-SR/SW, MM, 850nm VCSEL, LC Duplex, DMI diagnostika, Cisco kompatibilní Dosah dle vlákna - OM1 - 33m, OM2 - 82m, OM3 - 300m, OM4 - 400m

Záruka 36 měsíců

10GBASE-SR LC duplex multimode optický patch kabel, délka cca 2 m

Záruka 36 měsíců

kabel UTP cat6 délky 0,5m šedý

Záruka 36 měsíců

kabel UTP cat6 délky 1m šedý

Záruka 36 měsíců

kabel UTP cat6 délky 0,5m žlutý

Záruka 36 měsíců

kabel UTP cat6 délky 1m žlutý

Záruka 36 měsíců

kabel UTP cat6 délky 0,5m zelený

Záruka 36 měsíců

kabel UTP cat6 délky 1m zelený

Záruka 36 měsíců

ps

Digitálně podepsal Jakub Frank
Datum: 2025.09.30 15:02:10 +02'00'