

WCTRL-256-SFP+

287775

WiFi
Controlador



El controlador WCTRL-256-SFP+ ha sido diseñado para satisfacer las necesidades de empresas medianas y grandes, como hoteles, campus, oficinas, etc., simplificando la estructura de la red y reduciendo significativamente la dificultad de configuración, operación y mantenimiento de los dispositivos. Gracias a su procesador ARM de 64 bits y a la adopción de la tecnología SDN (red definida por software), ofrece un alto rendimiento y eficiencia. Admite gestión automática de canales, regulación de radiofrecuencia, balanceo de carga e itinerancia de usuarios. El modelo WCTRL-256-SFP+ puede gestionar hasta un máximo de 2048 puntos de acceso.

Especificaciones técnicas

- Controlador con licencias para 256 puntos de acceso
- Capacidad máxima: 2048 puntos de acceso
- Gestión de hasta 25 000 usuarios
- Procesador ARM de 64 bits de alto rendimiento
- Protocolo 802.11
- Difusión multi-SSID y ocultación de SSID
- NAT y QoS
- SNMP
- Pantalla LCD de estado

WCTRL-256-SFP+		
Código		287775
Caratteristiche		
Instalación		1U rack
Salida LAN		<ul style="list-style-type: none">• 1 x 10G SFP+ WAN• 2 x 10/100/1000M RJ45 WAN• 2 x 1G SFP WAN• 8 x 10/100/1000M RJ45 LAN
Interfaz USB		1 x USB
LED de estado		Alimentación, funcionamiento, LCD de estado

Sezione Wifi

Compatibilidad estándar		<ul style="list-style-type: none"> • 802.11 a/b/g/n/ac/ax • 802.11g, 802.11d, 802.11h • 802.11i, 802.11e • 802.3, 802.3ab, 802.3u • 802.3x, 802.3z, ARP, Reverse ARP • multi-LAN ARP/Proxy ARP • STP/802.1Q L2 forwarding • RFC791 IP, RFC792 ICMP, RFC793, TCP, RFC768 UDP • RFC854 Telnet, RFC1542 BOOTP • RFC1191 Path MTU Discovery
-------------------------	--	---

Caratteristiche principali

Tensión de alimentación	V/A	100-240 (50-60Hz)
Consumo	W	Max. 50
Temperatura de trabajo	°C	De 0 a +50
Humedad relativa	%	De 10 a 90 (sin condensación)

Dimensiones y embalaje

Embalaje		Individual
Piezas		1
Código EAN		8016978108558
Dimensiones del embalaje	mm	500 x 320 x 80
Dimensiones del producto	mm	440 x 180 x 44
Peso bruto	kg	3.3
Peso neto	kg	2.3

Gestión

- Canal automático
- Soporta configuración estática de canal
- Potencia de transmisión automática
- Soporta el ajuste de potencia de transmisión estática
- Soporta potencia de transmisión automática para corrección de cobertura
- Soporta potencia de transmisión automática basada en STA (cliente) para mejorar el rendimiento
- Tasa automática
- Soporta selección automática de tasa basada en STA
- Soporta limitar la tasa de transmisión máxima

VLAN

4096 VLAN

QoS

- Control de flujo a nivel de usuario: Soporta control basado en el usuario o en la información del contrato del servidor Radius.
- Control de flujo basado en dominio: Utiliza la VLAN o el SSID como dominio de configuración.
- Soporte 802.11e: Proporciona diferentes servicios según la prioridad de la sesión.
- Mapeo de QoS por SSID: Soporta asignar niveles de QoS a los usuarios según el SSID al que se conectan.
- Prioridad L2: Soporta mapeo de prioridad de paquetes de Capa 2 y 802.1p.
- Interconexión AP/AC: Basada en prioridad y carga.
- Balanceo de carga entre APs: Distribución automática de clientes entre APs adyacentes basada en la cantidad de usuarios y el flujo de datos.

Inalámbrico

- Reenvío distribuido (Distributive forwarding)
- Redundancia de puertos: vinculación de múltiples puertos (Link Aggregation)
- Reenvío centralizado
- Reenvío local: reenvío de servicios específicos de AP o SSID localmente en un AP ligero (Thin AP)
- RTLS (Sistemas de Localización en Tiempo Real)
- Conexión AP/AC mediante túnel de seguridad de Capa 3 (L3)
- Intercambio de servicios de Capa 2: centralizado, distribuido e híbrido
- Reenvío centralizado total: reenvío de todos los servicios tras centralizarse en el AC
- Redundancia de AC (Failover): conmutación de carga de un AC con problemas a otro AC operativo

DHCP

- Tabla DHCP: 2K

Seguridad

- Sistema abierto (Open system)
- WEP, WPA/WPA2 PSK
- 802.1x, 802.11i
- WAPI, ACL (Listas de Control de Acceso)
- Prevención de ataques DDoS
- IPS/IDS inalámbrico (Sistema de Prevención y Detección de Intrusiones)
- Detección de AP ilegales, verificación de terminales ilegales (no autorizados)
- Aislamiento de servicios de usuarios
- Lista blanca (Whitelist)
- Lista negra estática/dinámica, filtrado de URL