

machpower®



SCHEDA TECNICA
HOTSPOT GATEWAY NETWORK
ACCESS CONTROL

MODELLO: WL-EDHOWA

DESCRIZIONE

WL-EDHOWA L3 della linea wireless enterprise di MACH POWER- è nato come soluzione per la gestione della rete di accesso pubblico, come Wi-Fi-Hotspot, la gestione della rete di accesso clienti, le implementazioni di ospitalità - che richiedono affidabilità, efficienza e sicurezza. Esso combina un IPRouter / Firewall, Multi-WAN / QoS e Access Controller per un controllo a livello enterprise della rete wireless. WL-EDHOWA L3 è in grado di gestire le wireless LAN fino a 5000 utenti sia attraverso RADIUS esterno sia con radius interno senza cioè bisogno di un server esterno, gestisce il protocollo AAA ,autenticazione, autorizzazione, accounting e routing per Internet fino a 500 utenti simultanei. Le autenticazioni così come le autorizzazioni e accounting (AAA) sono gestite, anche queste, la necessità di server esterni, naturalmente qualora il sistema lo renda necessario è possibile anche usare server esterni.

WL-EDHOWA L3 Network Access Gateway / controller fornisce l'autenticazione, l'autorizzazione e la L'accounting anche per un reti cablate e wireless contemporanea, utilizzando tecniche di fast roaming (handoff) che eliminano la latenza, gli utenti pure passando da un Access point all'altro non sentiranno alcuna variazione potendo inoltre utilizzare un unico SSID per tutti gli AP collegati. Le funzioni L3 consentono la gestione remota di tutta la rete rendendo l'assistenza immediata ed economicamente sostenibile, la tecnologia captive portal implementa funzione di advertising e centralizzazione degli accessi e del loro monitoraggio. La tecnologia Hotspot consente ai provider Internet di offrire l'accesso alla rete locale ed Internet ai clienti, imponendo le regole d'uso e limitazioni necessarie (autorizzazione) come ad esempio la banda garantita, il tempo a disposizione, i siti internet che può visitare, .Gli ambienti operativi quindi resto i più disparati: Internet caffè, hotel, aeroporti, ospedali, scuole e università.

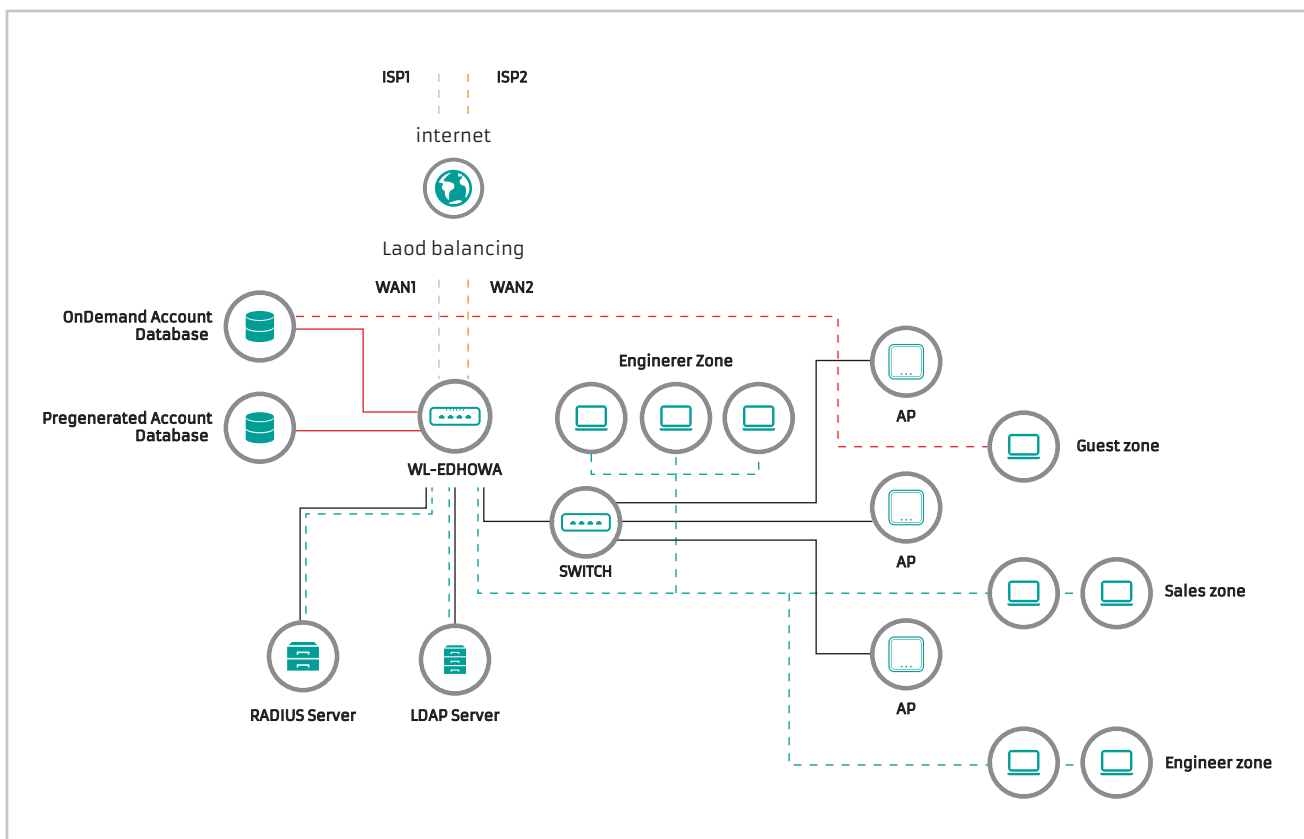
Il provider di Internet sarà in grado di avere il syslog di rilevamento del tempo trascorso sulla rete, la quantità di dati inviati / ricevuti, contabilità in tempo reale, il roaming veloce, Voice over Wi-Fi e molto altro ancora. Per iniziare la navigazione, un client deve passare attraverso un processo di registrazione che può avvenire in diversi modi: a) ticketing pregenerato ossia deve immettere un codice di accesso / Username di accesso in un finestra di accesso del browser che appare quando si tenta una pagina web oppure associare delle credenziali al proprio device attraverso la fornitura del MAC address. Questa procedura è l'evoluzione delle tecniche PSK (pregenerated shared key) in cui anziché dare un'unica password per tutti vengono generate credenziali in funzione della persona e/o del device appartenente a quell'utente. Ovvero si genera quello che viene definita una PSK privata; 2) POP3 questo metodo utilizza le credenziali di un qualsivoglia portale per autenticarsi, nel caso delle scuole ad esempio il docente potrà autenticarsi in tutti gli istituti che saranno dotati dell'EDHOWA utilizzando le stesse credenziali del sito www.istruzione.it. Questo potente metodo di autenticazione esclusivo di MACH POWER EDHOWA va anche nel senso dell'entità federATA.; autenticazione likegate che prevede l'utilizzo di like su facebook ad esempio oppure twitter ect; LDAP che consente l'autenticazione su appositi portali grazie al quale si potrà anche vendere pubblicità sul portale stesso. Infine LOCAL RADIUS. Inoltre se dotata dell'appliance iHAS (vedi apposita brochure) saranno possibili autenticazioni attraverso SMS, server RADIUS o servizi di advertising, newsletter automatiche, servizi di gruppo ect.

Le funzioni di accounting inoltre consentono il monitoraggio dello stato degli AP, le statistiche in rela time degli utenti collegati ai singoli AP, che rendono possibile l'ottimizzazione della disposizione fisica degli stessi; i record di tutti i singoli syslog dei singoli utenti e/o devices rende possibile ricostruire tutta la storia dei singoli collegamenti mettendo al sicuro da sinistri deresponsabilizzando il gestore o il dirigente dello scenario. La possibilità di creare appositi gruppi separati con diverse autorizzazioni e/o prestazioni (banda, orari di uso ect) permette la personalizzazione in base alla categoria (ad esempio in una scuola si possono separare i gruppi

docenti, studenti amministrazione). Le Vlan conseguenti possono essere separate anche sotto differenti SSID (nome della rete o gruppo). Inoltre i diversi gruppi possono essere collegati o meno a secondo delle esigenze (ad esempio il docente deve poter essere collegato al gruppo amministrativo in sede di utilizzo del registro elettronico).

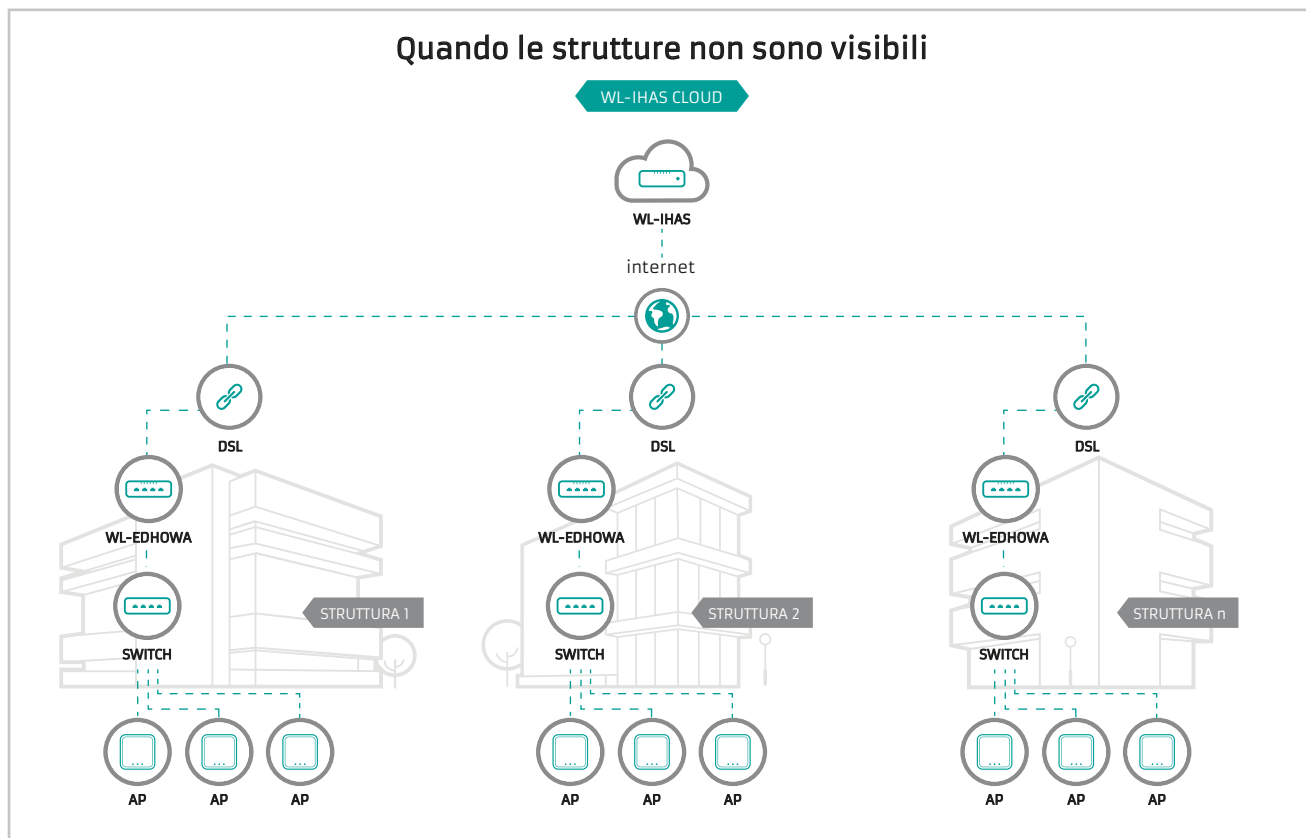
Le due porte Wan di cui è dotato WL-EDHOWA consentono l'utilizzo in contemporaneo di due linee DSL fino a 100 Mbps per ogni porta LAN che potranno lavorare in modalità load balancing o fail over. Le quattro porte LAN gigabit 1000 BASE -T di cui è dotato consentono la gestione centralizzata di fino a 120 Access point della linea enterprise senza costi o licenze aggiuntive. Gli access point di questa linea supportano fino a 16 SSID e fino a 256 utenti per ogni access point. Infine se collegato al controller della linea professional consente la gestione di reti disposte su più scenari lontani fra loro in maniera centralizzata e risparmiando sui costi totali laddove il budget non consente escursioni troppo elevate. La centralizzazione delle autenticazioni in questo caso potrà essere garantita implementando anche l'appliance Ihas oppure in cloud (locale o remoto).

SCHEMA ILLUSTRATIVO DI UN IMPIANTO

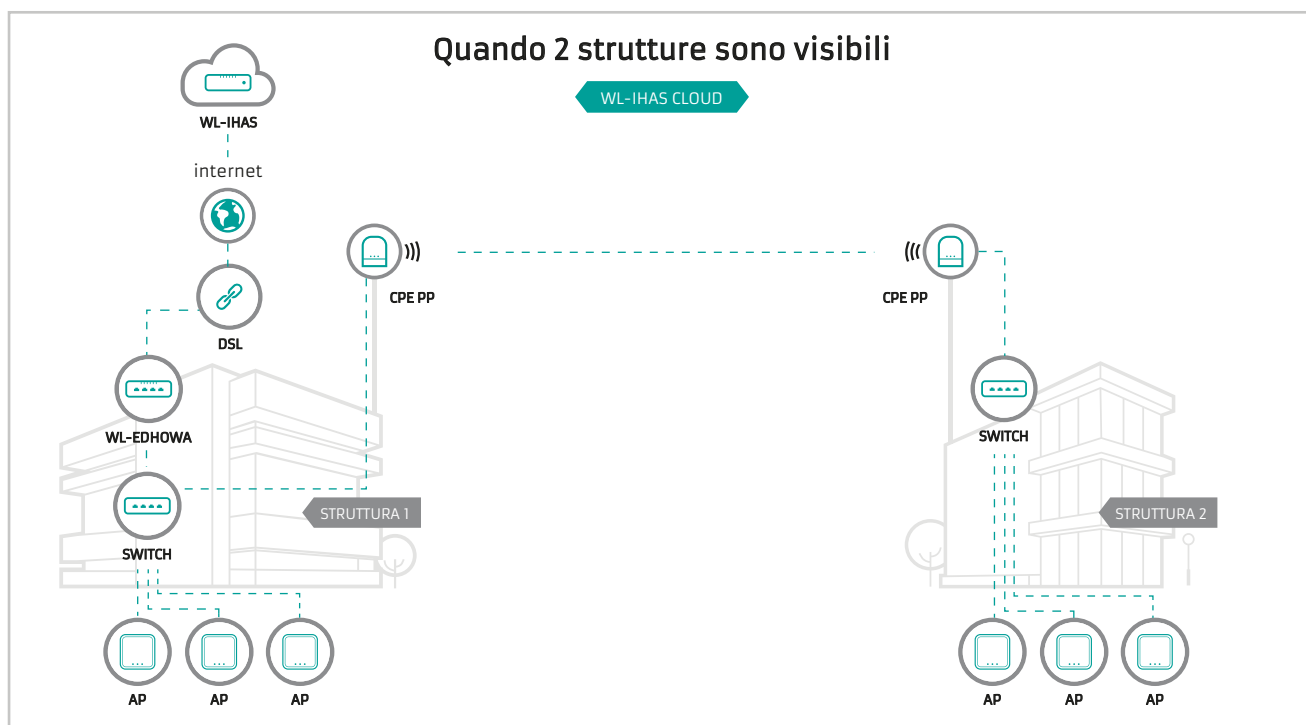


SCHEMA IMPIANTO PER LA REGISTRAZIONE E LA GESTIONE AUTONOMA E CENTRALIZZATA DEGLI UTENTI

Quando le strutture non sono visibili

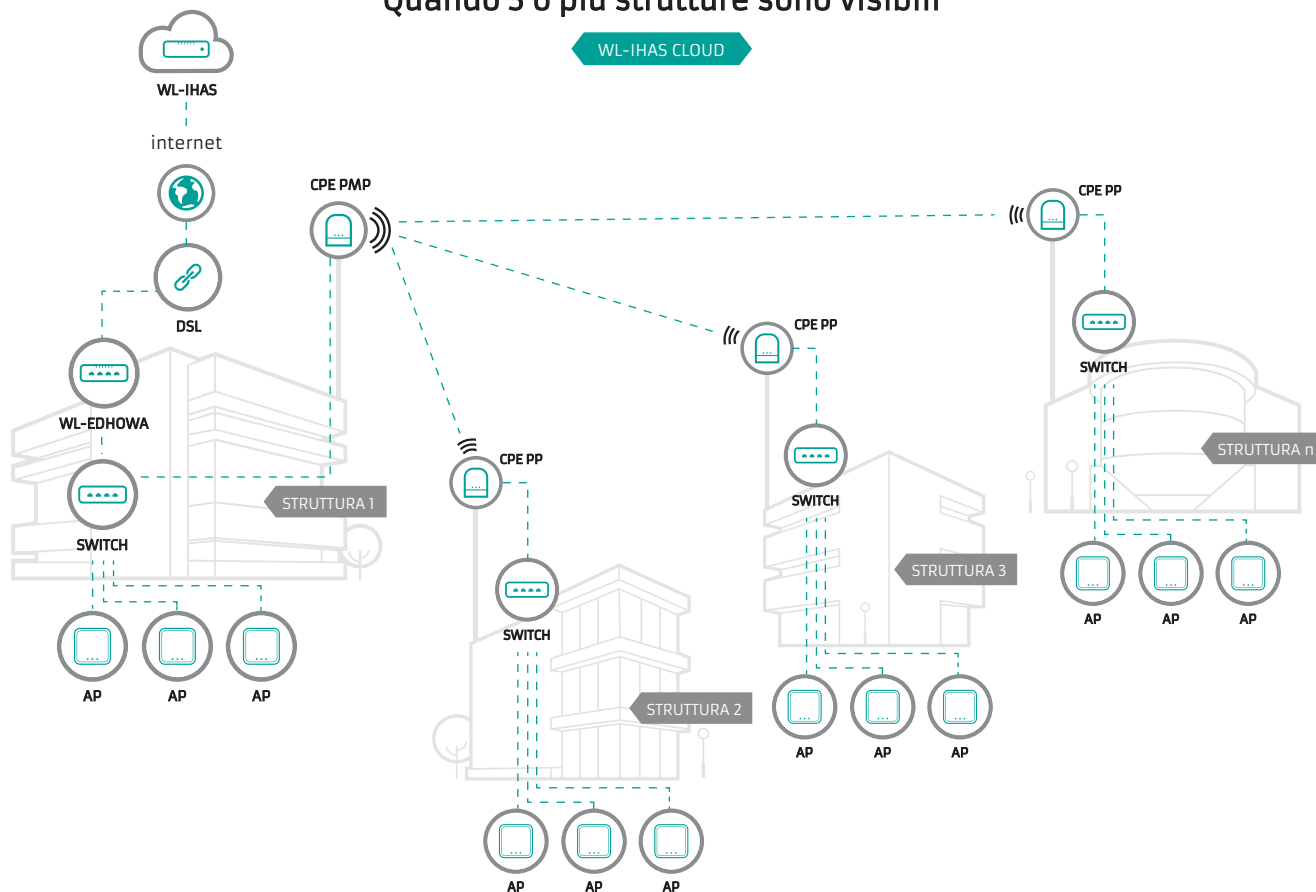


Quando 2 strutture sono visibili



Quando 3 o più strutture sono visibili

WL-IHAS CLOUD



CARATTERISTICHE

Gestione e Supporto Access Point

- Max: 120 Access Points per Controller
- Max: 500 utenti simultanei per Controller
- Local Account : 5000 utenti
- Possibilità di connessione in serie di più controller
- Autenticazioni Multiple su VLAN (Possibilità di impostare diversi metodi di autenticazione su diverse VLAN)
- Autenticazione Centralizzata a mezzo CLOUD iHAS

Gestione centralizzata Access Point

- Gestione di gruppi access point consente di impostare regole che semplifica il compito di assegnare la stessa impostazione a più AP
- Automatica configurazione e gestione degli AP
- Gestione locale e remota dei profili degli AP
- Auto rilevamento degli AP
- Ripristino automatico degli AP in caso di errore
- Aggiornamento del firmware centralizzato e contemporaneo degli AP
- Aggiornamento Firmware da remoto
- Tecnologia Zero Configuration che consente il ripristino degli AP in sostituzione ai difettosi

Controlli Centralizzati AP

- Controllo MAC Address: che fornisce la lista dei MAC Address dei device connessi per ogni AP
- Filtro Accessi
- Controllo accessi basato sul tempo
- Singola Interfaccia utente per aggiornamento e il ripristino degli AP
- Partizione WLAN – Se attiva gli utenti non sono autorizzati a scambiare dati attraverso gli AP
- Controllo degli AP massimi consentiti
- Supporta Roaming – Intra-Switch , Inter-band , Inter-Switch

Monitoraggio Centralizzato AP

- Monitoraggio stato AP
- Il numero di client associati alla AP
- Le informazioni AP RF
- Lista degli AP associati
- Lista IP associati
- Bilanciamento del carico in base al numero di utenti
- Bilanciamento del carico in base all'utilizzo
- Statistiche – Memorizza la storia dei singoli clienti raffigurando diagrammi statistici
- Supporta il monitoraggio IP di Access Point di terze parti
- Report di stato e di errore
- Analisi topologica - Elenco dei dispositivi monitorati aggiornando periodicamente lo stato
- Controllo in tempo reale dello stato degli AP (AP Health Checking)

- Gestione remota centralizzata HTTP /SNMP
- Supporta MIB's: 802.11, 802.1X, MIBII, RADIUS authentication, RADIUS Accounting
- Supporta SYSLOG incluso server remoti
- Log-system Log: operator action Log

Gestione delle risorse radio

- Assegnazione automatica dei canali e di impostazione della potenza degli AP
- Monitoraggio simultaneo degli utenti
- Auto diagnostica delle condizioni RF
- Ottimizzazione della capacità di distribuzione
- BSSID Multiplo: 8 per Radio
- Hot Standby in modalità AP (Supporta File Over)
- Carico Bilanciato con altri AP disponibili
- Radio Management
- Rilevamento delle interferenze

Copertura

- 8 code per porta
- IEEE802.11p Class of Service/Quality of Service (CoS/QoS)
- IEEE802.11e Wi-Fi Multimedia (WMM)
- DiffServ Codpoint (DSCP)

Criptografia Wireless

- WPA personal and enterprise
- WPA2 personal and enterprise
- AES(CCMP): 128bit (FIP-197)
- WEP40/64 and 104/128-bit
- TKIP: RC4-40
- SSL and TLS: RC4 128-bit and RSA1024 and 2048 bit
- EAP-TLS, EAP-TTL/MSCHAPv2

Sicurezza Wireless

- IEEE802.1x network login user authentication (EAP-MD5/TLS/TTLs)
- EAP over LAN (EAPoL) transport with PEAP and EAP-TLS authentication
- RADIUS server authentication (RFC2618)
- IEEE802.1x gestione dell'autenticazione via Telnet e console
- Multipli livelli di accesso privilegiato
- Gestione delle gerarchie e della protezione tramite password
- Scalabilità e modulabilità EAP offload per AAA server
- Stateful 802.1X authentication for standalone APs
- Autenticazione via SSID
- Supporta Multi-SSID per operatione di multiple WLANs
- Supporta WLAN distribuite e centralizzate

Criteria di sicurezza per le autenticazioni

- 802.1X Authentication with WPA,WAP2 and 802.11i
- Local Accounts of 802.1X Authentication
- Supporta RADIUS / LDAP per AAA server
- Username e chiave criptata
- Local User Data Base for AAA fail-over protection

Wireless Roaming

- supporta Intra-controller/ Inter-controller roaming e Intra-subnet/ Inter-subnet roaming
- Fast roaming (Handoff IAPP, 802.11r)
- L2 roaming

Gestione Utente

- Max 500 utenti simultanei
- Max 5000 Autenticazioni pregenerate/On-Demand/ Local RADIUS
- Gestione sessioni utenti
- Gestione e configurazione utenti in black list
- Autenticazione attraverso MAC Address (privat psk)
- Metodi di autenticazione supportati: ticketing pregenerato/On-Demand (detto anche PSK enterprise), Local RADIUS, LDAP, Remote RADIUS e POP3
- Protezione login SSL
- Timer di inattività con gestione Time Out
- Controllo delle sessioni di account expiration
- Notifica via email automatica degli UserLog e Traffic Statistics
- Controllo dei login time frame
- Gestione del limite della sessione
- Reporting degli utenti online in real time
- Supporta local account roaming
- Gestione degli utenti rilevando il loro percorso tra gli AP

Autenticazione

- Gestione e possibilità di personalizzazione della pagina login e logout con la possibilità di inserimento di avvisi e/o pubblicità varie
- Autenticazioni Single Sign On (SSO) per il dominio locale, LDAP, RADIUS locale e remota, autenticazione con MAC Address, 802.1x (PSK Enterprise), UAM (Universal Access Method), POP3 locale e remota
- Numero dei server RADIUS registrati
- Supporta MAC Control List (ACL)
- Supporta login multipli su un account (BYOND)
- Supporta auto-expired guest accounts
- Suddivisione degli utenti in gruppi ed ogni gruppo può accedere ad differente reti in differenti zone
- Massimo simultaneous user session (TCP/UDP) limit
- Gestione della black list
- CLOUD iHas (SMS e ID / Password)

- Esportazione e importazione di utenti tramite un file di testo
- Web-based Captive Portal per SSL browser-based authentication
- Authentication Type
- IEEE802.1X (EAP, LEAP, EAP-TLS, EAP-TTLS, EAP-GTC, EAP-MD5)
- RFC2865 RADIUS Authentication
- RFC3579 RADIUS Support for EAP
- RFC3748 Extensible Authentication Protocol
- MAC Address authentication
- Web-based captive portal authentication

Autorizzazione

- Controllo degli accessi alla rete protetta (intranet, internet) prevede la gestione della larghezza di banda, le VPN e i azioni di firewall
- Gestione delle autorizzazioni con tutti i metodi di autenticazione suportati, incluso il POP3

Accounting

- Piani di accouting pregenerati, On-Demand in base al tempo e alla quantità di dati indicando il dettiglio dello storico del traffico
- Supporta Server RADIUS esterni e locali
- Prevede fino a 10 diversi piani On-Demand
- Supporta la gestione del pagamento tramite carte di credito e paypal
- Controllo della sessione di scadenza degli account On-Demand con storia del traffico inviata automaticamente via email
- Gestione Accounting del POP3

Modalità di lavoro delle porte WAN

- Le 2 WAN possono lavorare in 2 modalità: Load Balancing e Fail Over
- Supporta multiplo dominio e
- Gestione della banda su differenti network

Gestione QoS

- Classificazione dei pacchetti tramite DSCP (Differentiated Services Code Point)
- Diff / ToS
- IEEE802.11p / Cos
- Controllo priorità Tag VLAN IEEE 802.1Q
- WMM IEEE 802.11e
- Mappatura automatica delle priorità WMM per 802.1pe IP DSCP
- Snooping IGMP per la gestione multicast efficiente
- Gestione del traffico di upload e download

Firewall

- Protezione integrata attacco DoS
- Completa ispezione stateful packet filter

- Access Control List
- Layer 7 Protocollo di blocco
- Content Filter
- URL Filtering
- Parental Control
- Supporto domini multipli
- Sessioni di Firewall attive - 16.000

Network

- Supporto NAT o modalità Router
- Supporto IP statico , IP dinamico (DHCP client) , PPPoE e PPTP sulla connessione WAN
- Server DHCP per interfaccia ; Reti DHCP multipli
- 802.3 Bridging
- Proxy DNS / DNS dinamico / reindirizzamento destinazione IP Port
- Mappatura del server DMZ
- Virtual Server Mapping
- Pass-through H.323
- integrato con server DHCP
- Supporto routing statico
- Binding VLAN con interfaccia Ethernet
- Supporta MAC filter
- Supporta IP filter
- Supporto Walled Garden (zona di navigazione libera)
- Supporta MAC address e IP address pass through
- Supporta IP Plug and Play (PnP IP)

Amministrazione di sistema

- Tre account amministratore
- Fornire accesso personalizzabile e il logout alla pagina del portale
- Accesso CLI (gestione remota) via Telnet e SSH
- aggiornamento del firmware remota (via web)
- Utilità di backup e ripristino della configurazione del sistema
- Statistiche complete e reporting di stato
- Monitoraggio del traffico in tempo reale
- Ping Watchdog

Gestione network

- Syslog eventi
- monitoraggio dello stato degli utenti on-line
- monitoraggio basata su IP di dispositivi di rete
- stato della connessione di interfaccia
- supporta Syslog per la diagnosi e la risoluzione dei problemi
- la registrazione della cronologia di traffico degli utenti

- Log di sessione per l'utente possono essere inviati al server Syslog
- Segnalazione remota Syslog a server esterni
- Analisi del traffico e statistiche
- SNMP v1 , v2c , v3
- Trap SNMP ad un elenco di indirizzi IP
- Supporto MIB -II
- NTP Sincronizzazione
- Accesso amministrativo : HTTP / HTTPS

SPECIFICHE

Generali	
Piattaforma di Base	32-bit , MIPS24K Processor
Velocità CPU Clock	680 MHz
Porta seriale	1 (DB-9)
Porta USB	1 (Interfaccia radio 3G opzionale con tutti i maggiore brand - solo ODM)
Interruttore di ripristino	Push-button momentary contact switch
Configurazione Ethernet	10/100/1000 Base-TX auto-negotiation x 6 porte Ethernet (connettore RJ-45) WAN x 2 / LAN x 4
DRAM	256Mbytes
Flash	32 Mbytes
Presenza CF	1 (riservato per l'opzione)
Indicatori LED	1 x Power ; 1 x Status, 1 x Net Status (Questo è per la gestione AP, quando il sistema non può rilevare la gestione AP)
Caratteristiche ambientali e meccaniche	
Temperatura di esercizio	0 °C ~ 55 °C
Umidità di funzionamento	10% to 80% (senza condensa)
Umidità di conservazione	5% to 90% (senza condensa)
Alimentazione elettrica	110 – 220V AC Power; 12 VDC, 1.5A input.
Dimensioni (mm)	243 x 150 x 45.5 (Larghezza x Profondità x Altezza)
Peso (kg)	1.4
Caratteristiche fisiche	Montaggio a parete , Case di metallo
Certificazioni	FCC / CE / EN 60601-1- 2:200

Per Life Warranty si intende 8 anni.

© 2016 Mach Power. Tutti i diritti riservati. MACH POWER è un marchio registrato.
Le specifiche sono soggette a modifiche senza preavviso.
Le immagini utilizzate possono essere a scopo illustrativo.