

PCR-W Wireless Proxy Chaining Router

Product Datasheet · PCR-W10 / PCR-W40
ALN-DS-PCR-W-EN · v1.1 · 2026-10-26 · English translation for review

Product overview

PCR-W combines multiple wireless sub-routers and two-stage proxy chains in one device. Each SSID maps to a sub-router with separately configurable router MAC, DHCP, NAT, Relay and Landing nodes. Relay provides the intermediate connection; Landing supplies the final business egress.

PCR-W10 / W40 provide 10 / 40 sub-routers, SSIDs and proxy chains. Routine configuration uses ALTool to access ALOS functions.

Core capabilities and application value

Capability	Function and value
One chain per network	Maintain Relay and Landing nodes separately by store, device group or region.
Centralized node maintenance	Edit both stages, configure DNS, test connectivity, and import/export group lists.
SSID / MAC management	Generate names and router MACs randomly, sequentially or with custom prefixes.
Wireless controls	Configure channel, width, power, password, hidden SSIDs and client isolation.
CloudLink	Bind customer cloud servers and use a bound Host as a Relay or Landing node.
Internal access	Use access rules and internal mappings for downstream management or upstream resources.

Typical business uses

Wireless store networks, social media groups, regional advertising tests and deployments requiring separate management of relay paths and final egress.

01 / Models and Technical Specifications

Model configurations and interfaces

Item	PCR-W10	PCR-W40
Sub-routers / SSIDs	10 / 10	40 / 40
Proxy chains	10 pairs	40 pairs
Chain architecture	Relay + Landing	Same
WAN / LAN	1 × Gigabit WAN; 1 × Gigabit LAN	Same
Wireless	5 GHz; Qualcomm AC module; up to 1300 Mbps nominal	Same
Proxy protocols	SOCKS5, VMess, VLESS, HTTPS, Shadowsocks	Same
Configuration	ALOS	Same
Legacy enclosure dimensions / net weight	L205 × W106 × H244 mm / 2.7 kg	Same

Technical notes

Each full chain requires Relay and Landing resources. Current models are W10 / W40. The domestic-market enclosure uses the confirmed new appearance; legacy dimensions and weight do not confirm domestic enclosure dimensions. Nominal wireless rate is not proxy-chain throughput.

Unconfirmed quantitative specifications

Domestic enclosure dimensions/weight, supply ratings, system power consumption and environmental ratings require confirmation.

02 / Proxy Chain and Egress Management

Chain configuration specifications

Function	Configuration and behavior
Node roles	Select a sub-router in ALOS Proxy, then configure Relay Node and Landing Node separately.
Node identification	Paste details, run Identify and Confirm, then Save and Apply.
Individual editing	Change the selected sub-router's Relay or Landing; save scope and interruption behavior depend on firmware.
Single-stage operation	Existing instructions allow Relay to remain blank with only Landing configured; full two-stage chains still need Relay resources.
DNS	Set DNS for the selected sub-router and check it with the node settings.
Testing	Ping checks connectivity, not application availability or throughput.
Batch lists	Import Node / Export Node use TXT with land, relay, dns and mark fields per group.
Reset	Reset Proxy requires Save and Apply; retain a backup before resetting.

Protocols and node information

The specification lists SOCKS5, VMess, VLESS, HTTPS and Shadowsocks. The manual also includes HTTP examples; verify HTTP/HTTPS import support against delivered firmware. SOCKS5 supports authenticated or unauthenticated nodes; VMess, VLESS and Shadowsocks use tool identification. Match address, port, authentication and protocol fields.

TXT groups use sub-router identifiers such as R1 and R2: land is Landing, relay is Relay, dns is the resolver and mark is a note. Preserve group assignments when editing lists to avoid incorrect egress.

Address protection

Existing specifications list IP, DNS and WebRTC leak protection. Test chain connectivity, final egress, DNS and browser exposure separately. Ping success does not establish full application availability, and another product's failure-disconnect mechanism is not automatically a verified PCR-W behavior.

03 / Wireless, CloudLink and Internal Access

Wireless AP specifications

Function	Capability
SSID / MAC generation	Random brand, sequential or custom-prefix modes; group numbers distinguish units.
Individual editing	Edit SSIDs; use New MAC for a selected sub-router, then Apply.
Capacity	Broadcast count must stay within W10 / W40 limits.
RF settings	Frequency Channel, Frequency Width and Transmit Power.
Wireless access	Shared password, Hide SSID, and Terminal Isolation for clients on one SSID.

Plan channel, width and power for actual coverage. MAC updates change router-side identity, not phone or application fingerprints. Sub-routers share hardware and are not fully physically isolated.

CloudLink server binding

Existing instructions use static-IP cloud servers with Ubuntu 20.04 / 22.04. Enter Name, Host, SSH Port, User and login details, then Bind. In the node editor, Select a host and Set, then Save and Apply. Select bound Hosts for Relay and Landing as required.

SSH uses the configured port, default TCP 22. Documented proxy ports are 23585, 26516 and 32411 over TCP/UDP. Permit the actual required ports; servers, IPs and bandwidth are separate resources.

Internal mapping and resource access

Select Sub-Router, enter LAN IP, LAN Port and a mapped port, then Add and Apply. For example, map a business PC's RDP port 3389 to internal management port 13389; use site-specific addresses.

A management PC can reach downstream devices locally. Upstream NAS/server access follows Enable / Disable LAN Access rules. Internal management bypasses the business proxy and does not imply public remote traversal. Verify rule names and actual reachability against delivered software.

04 / Topology and Deployment Selection

Typical topology

```
Upstream network -> WAN [PCR-W] -> SSIDs -> clients
Business traffic: sub-router -> Relay -> Landing -> service
Management PC -> LAN / management Wi-Fi -> ALOS / mappings
```

Scenarios and application value

Scenario	Configuration focus	Value
Multiple stores	SSID and proxy chain per store	Maintain nodes and final egress separately.
Regional tests	Target-region Landing node	Location depends on the actual Landing proxy.
Centralized phones	Site-specific wireless planning	Maintain grouped wireless access.
Device maintenance	Internal mappings and access rules	Retain required management paths.

Model and component selection

Choose W10 for 10 chains or W40 for 40. Chain count is not a verified maximum-client count. For single-stage SOCKS5/HTTP wireless egress, compare BPR-W; for wired groups by port, consider MLR.

Deployment checks

Install antennas and wire the unit -> connect ALTool -> configure SSID/MAC -> configure both nodes and DNS -> save and test -> check final egress and leak protection -> configure internal rules -> test actual load.

Website: www.alnets.net **Email:** sale@alnets.net