

COD Network Module

The living network inventory, from IT to OT

Hand-maintained device lists are outdated the day they are written. The **COD Network Module** automatically discovers every IP-addressable device, from office IT all the way into OT, and maintains a **living inventory** from it. Every asset gets its own workspace, rooms, racks, and cabling become assessable, and the **L3 topology** shows real routing paths instead of guessed agencies.

At a glance: auto-discovery of all IP devices (IT & OT) • live status per device • asset workspace, rooms, racks & layer-1 cabling • L3 topology with real routing relations • global search (Ctrl+K) across network & firewall • role-based, ready for critical-infrastructure (KRITIS) environments.

Discover, document, and track



Automatic discovery & living inventory

Finds every IP-addressable device on its own: IT, network hardware, and OT, multi-vendor via SNMP, SSH, and vendor APIs (Cisco, Ruijie, Allied Telesis, MikroTik, and others). A **live status column** per device shows OK, error, or unknown with timestamp, cause, and source. Devices without a collection method say so honestly instead of glowing green forever. Plus a model-accurate port view with PoE, live throughput, cable test, and port up/down.



Asset workspace per device (new)

Every asset gets a detail page with tabs: **Overview** (inline editable), **Monitoring** (Zabbix host card), **Placement** (rack & rack unit), **Connectivity** (NIC ports with an "Add range" generator), **Contacts & Contracts** (encrypted license keys) and **Dependencies**. Assets can be moved across sites and tenants, fully audited.



Rooms, racks & cabling (new)

Buildings, floors, and rooms are now assessable assets, nestable via drag and drop. **Racks** offer a live rack elevation with occupancy validation, and the **layer-1 patch bay** connects two assets port by port with live patch status. The physical cabling is documented at last.



L3 topology with real routing paths (new)

Edges are created only when one device actually routes via the address of the other, instead of being guessed from shared subnets. Firewalls are first-class nodes. A **simulated route trace** walks the routing tables hop by hop, even through firewalls (IPv4). HA pairs and clusters are grouped automatically, and a **VLAN path check** verifies the LLDP paths (Cisco IOS trunk lists).

Your network, always up to date. See COD live in your environment, hands-on, with no sales pressure.

extoco.de • extocode GmbH

