YACHTBYTE

Official resource

DNS and DHCP First 30 Minutes Triage Sheet

SLUG	dns-and-dhcp-first-30-minutes-triage-sheet
SUMMARY	Printable first-response triage sheet for yacht DNS, DHCP, gateway, Wi-Fi, and local core-service failures that look like internet outages.
RESOURCE TYPE	Checklist
RESOURCE AREA	Connectivity, IT & cyber
INTENDED AUDIENCE	ETOs, AV/IT crew, IT providers, captains, yacht managers
ESTIMATED USE MINUTES	15
DOCUMENT LABEL	Download PDF
PDF	dns-and-dhcp-first-30-minutes-triage-sheet-v1-0.pdf
VERSION	1.0
PUBLICATION STATUS	Published resource archive
IMPORTANT NOTE	This resource is practical operational guidance. It does not replace the vessel SMS, flag or class requirements, manufacturer manuals, competent network/security advice, or the authority of the Captain and responsible technical officers onboard.

YachtByte Official Resource

Fault boundary

- [ ] Affected network identified: guest, crew, owner, AV/control, CCTV, technical, bridge-adjacent or OT.
- [ ] Wired and wireless impact compared.
- [ ] One device, one area, one VLAN or whole-yacht impact recorded.
- [ ] Recent changes, support sessions, WAN failover, shore-power event or reboot recorded.
- [ ] Bridge, captain or duty officer informed where operationally relevant.

Addressing check

- [ ] Affected device IP address recorded.
- [ ] Gateway recorded.
- [ ] DNS server recorded.
- [ ] SSID or switch port recorded.
- [ ] VLAN or subnet checked against the IP plan.
- [ ] `169.254` or missing gateway condition noted where present.
- [ ] Known-good comparison device checked where available.

Connectivity check

- [ ] Gateway reachability tested.
- [ ] Public IP reachability tested where policy allows.
- [ ] Local service reachability tested.
- [ ] Firewall or router WAN status checked.
- [ ] SD-WAN, Starlink, VSAT, 5G/LTE or marina Wi-Fi status checked only after local tests.
- [ ] Result recorded before reboot or reset.

DNS check

- [ ] Public name resolution tested.
- [ ] Internal name resolution tested where used.
- [ ] DHCP-provided DNS server tested.
- [ ] Firewall DNS proxy or resolver status checked.
- [ ] Upstream DNS forwarder checked.
- [ ] Temporary DNS change recorded with approval and rollback note if used.

DHCP check

- [ ] Authoritative DHCP server identified.
- [ ] Scope enabled status checked.
- [ ] Lease pool exhaustion checked.
- [ ] Reservations and conflicts checked.
- [ ] DHCP relay or helper address checked where used.
- [ ] Duplicate or rogue DHCP source considered.
- [ ] Guest network lease time reviewed where device count is high.

Closeout

- [ ] Root cause or likely cause recorded.
- [ ] Temporary action recorded.
- [ ] Permanent corrective action assigned.
- [ ] IP plan, DHCP scope, DNS record or firewall notes updated where needed.
- [ ] Logs, screenshots and test results stored.
- [ ] Captain or management summary provided in plain language.