

HOW, WHAT & WHY NETWORK SETUP GUIDE

A practical Dhruv network guide explaining what is needed, why it is needed, how to configure it, and how to prove it works.

For customer IT teams, network engineers, installers and Dhruv administrators.
Use the baseline profile, then add only the streaming and management profiles selected for the site.

The practical starting point

For the repository-documented HTTPS player design, plan device-initiated TCP 443 to the approved Dhruv service and media destinations, plus the site's DNS, time and address services. Do not create internet port-forwards to screens for ordinary signage. Streaming requirements depend on the transport and endpoint actually selected. [R2-R5, S1]

Document control	Record
Reference	DHRUV-NET-SETUP-001
Version / prepared	v1.1 - How / What / Why edition
Scope	SoC signage, approved players, Amino H200, live streaming, hosted or local services
Evidence basis	Repository source and current primary vendor/protocol documentation
Release condition	Complete the site register and pass the relevant commissioning tests before acceptance

Important: This is a setup and approval guide, not a certificate that a live server, stream, screen model or deployment has passed testing. No firewall, server or player configuration was changed while preparing it.

Source snapshot: [satinder-source/dhruv-platform](#)
9a372468f73656754fdff5f8b83fddd5e6ad8907

01 / NETWORK SETUP

HOW / WHAT / WHY

How to use this guide

Every network requirement in this guide should be read in four steps: WHAT Dhruv needs; WHY the service is needed; HOW the customer IT team or installer should configure it; and PROVE IT - the evidence that confirms the path works. This prevents a port list from being treated as a blanket firewall instruction.

WHAT	WHY	HOW	PROVE IT
DNS resolution	Dhruv uses hostnames for CMS, Player and approved media services; hard-coded IP addresses are not a durable design.	Provide a reachable site DNS resolver. Permit the Player VLAN to query only the approved resolver(s).	Resolve the approved Dhruv hostname from the Player network and record the returned addresses and timestamp.
Accurate time	TLS validation, schedules, authentication leases and operational logs depend on correct time.	Provide DHCP-supplied or explicitly configured NTP/time service. Keep UDP 123 limited to the approved time source where applicable.	Compare device time with the approved source; verify timezone and scheduled playback behaviour.
Outbound HTTPS - TCP 443	The repository-documented Player design uses HTTPS for enrolment/content/control contracts and secure content delivery.	Permit device-initiated TCP 443 only to approved Dhruv and media destinations. No WAN-to-screen port-forward is required for normal signage.	From the Player VLAN, resolve the hostname, complete TLS, enrol the device, retrieve an assignment and observe a successful heartbeat.
Live-stream transport - only when used	A live encoder or Player may use a transport other than HTTPS, such as SRT, RTSP/RTP, RTMPS or multicast.	Open only the exact protocol, direction, host/group and configured port(s) selected for that stream.	Run the real stream on the target device and record sustained playback, bitrate/packet-loss evidence and reconnect behaviour.
Local display control - only when supported	Some professional displays expose manufacturer control over the LAN. This is separate from ordinary cloud Player traffic.	Keep control traffic on a management VLAN and allow only the Dhruv controller to the exact display IP/port supported by that adapter.	Use Test Connection/status first, then a harmless supported command; record the real device response and audit event.

Fast decision: what does this site actually need?

Standard signage normally starts with IP addressing, DNS, time and outbound HTTPS. Web URL content adds access to specifically approved external origins. Live streaming adds only the selected stream transport. Local hardware control adds only the manufacturer-specific LAN rule. Remote support is a separate optional service. Do not combine these profiles into an “open everything” firewall rule.

Start here: choose the right profile

There is no single “open all Dhruv ports” rule. Approve the core profile first, then the smallest set of optional profiles needed by the installation.

Profile	Select when	Network addition
A • Standard signage	Players download assigned content and report to Dhruv.	Approved HTTPS destinations on TCP 443; site DNS, NTP and DHCP as applicable.
B • HTTPS live playback	The selected device/app accepts an approved HLS or DASH service.	TCP 443 to manifests, media, redirects and required key/licence services.
C • Contribution / low latency	An encoder, gateway or decoder uses RTMP, RTSP or SRT.	Only the configured receiver/control/media ports; see sections 09–10.
D • LAN IPTV multicast	One headend distributes channels to multiple local receivers.	Assigned multicast groups and UDP ports, with IGMP-aware switching; section 11.
E • WebRTC	The selected application actually implements WebRTC.	Its ICE/STUN/TURN and media configuration; section 12.
F • Amino management	H200 provisioning uses Amino Orchestrate / Resolve.	The separate vendor destination matrix in section 13.
G • Remote support	A separately approved support service is installed.	Its named servers and narrowly scoped management rules; section 14.

One-page IT handover: minimum Dhruv network request

Give this summary to the customer IT/network team before installation. Values marked “site-specific” must be completed from the approved deployment; they are not universal Dhruv defaults.

WHAT	WHY	HOW	PROVE IT
Player network	Provide a managed wired VLAN/subnet for fixed Players/screens where practical. DHCP reservations may be used where operationally helpful.	Stable addressing, isolation and troubleshooting are easier than on guest networks.	Connect one Player on the final VLAN and verify address, gateway, DNS and time.
Outbound HTTPS	TCP 443 from Players to approved Dhruv/media FQDNs, including the repository-documented production Player origin https://player.dhruv.org.uk where that is the deployed target.	Enrolment, content, schedules, heartbeat/control contracts and HTTPS media require secure outbound connectivity.	Enrol one device and complete a content publish/heartbeat cycle.
CMS access	HTTPS TCP 443 from authorised administrator networks to the deployed CMS origin, repository evidence referencing https://cms.dhruv.org.uk .	Operators need secure browser access to manage content, screens and schedules.	Sign in from an authorised admin network and complete a read-only screen/status check.
DNS / time	DNS to approved	Hostnames, TLS,	Record successful

WHAT	WHY	HOW	PROVE IT
	resolver(s); time synchronisation to approved source(s).	schedules and authentication depend on them.	resolution and device clock/timezone.
Live streaming	Site-specific only: exact HLS/DASH/RTMPS/SRT/RTSP-RTP/WebRTC or multicast rules selected for the implementation.	Streaming transport requirements vary; no universal live-stream UDP range exists.	Play the actual live channel on target hardware for the agreed soak period.
Display control	Site-specific only: controller-to-display LAN ports for supported manufacturer adapters.	Power/input/volume controls, where supported, are separate from cloud Player HTTPS.	Test connection and one approved command on the physical display.
Inbound internet to Players	None for normal Dhruv signage unless a separately documented service explicitly requires it.	Normal Player operation is device-initiated; unsolicited WAN exposure is unnecessary.	External scan confirms no unintended Player listener is exposed.

The minimum IT handover

Record the site, player models, installed firmware/app builds, device VLAN/subnet, DNS and time servers, CMS/player base URLs, media hosts, stream source and transport, authentication owner and maximum simultaneous screens. Missing values stay **TBC**, not assumed defaults.

Three rules that prevent most configuration errors

Direction matters. “Outbound TCP 443” means the site device initiates a connection to a destination listening on 443. It does not mean forwarding 443 from the internet to the display. Stateful return traffic normally follows the established session. [S11]

A protocol default is not a deployment instruction. SRT needs a configured UDP port; RTP media ports are negotiated or configured; HTTPS on a non-standard port still requires that exact port. [S4–S6]

Open does not mean compatible. Codec, DRM, firmware, app capabilities and authorisation must also pass. Keep unsupported SoC controls unavailable; do not expose debug ports to make a feature appear supported. [R3, R6]

Sources are identified as [R...] for repository evidence and [S...] for external primary documentation. Full references appear in sections 22–24.

02 / NETWORK SETUP

Evidence, scope and reader's map

Repository evidence establishes what the inspected files say. It does not identify the running production build or prove any physical installation.

Item	Evidence at preparation	What remains to be verified
Dhruv main	Pinned commit 9a372468f736; full identifier on the cover. [R1]	Which image/revision is running on Hetzner and each device.
CMS / Player targets	cms.dhruv.org.uk and player.dhruv.org.uk are named in the source material. [R3, R5]	Live DNS, certificate, reverse-proxy mounts and authorised responses.
Internal API	Dashboard Nginx points to api:3001. [R2]	Actual production networking and absence of public exposure.
Amino service	An independent hotel IPTV/H200 workstream exists. [R6]	Its public host, enabled routes, firmware transport and real H200 acceptance.
Hosting capacity	Planning context: existing Hetzner server described as about 80 GB; Mac Docker for local work.	Actual free space, CPU/RAM, network allowance, load and recovery evidence.

Status language: Repository-confirmed = inspected source. Vendor-documented = external product requirement. Example = replace before use. Site TBC = not yet supplied/verified. No item is marked live-verified, hardware-accepted or USER VERIFIED by this document.

Reader's map

Sections	Use
03–05	Survey the site, understand the connections and identify destination hosts.
06–08	Check Dhruv API paths and prepare baseline/server firewall rules.
09–13	Choose streaming transports, multicast, WebRTC and Amino requirements.
14–17	Approve support access, hosting, TLS/proxy behaviour and capacity.
18–21	Run diagnostics, commission, troubleshoot and obtain sign-off.
22–24	Open the pinned repository and primary technical references.

This document is network-focused. It does not grant content rights, device compatibility, licences, cloud access or permission to publish a release. Optional EPOS, ESL, CRM, booking, AI and emergency integrations require their own provider endpoint records and acceptance tests.

Key terms

SoC: the screen's built-in computing platform. **FQDN:** a complete hostname. **VLAN:** a logical network segment. **DNS:** hostname resolution. **DHCP:** automatic address assignment. **NTP:** network time. **TLS:** authenticated encrypted transport. **CDN:** distributed content delivery. **NAT:** network address translation. **DRM:** content-rights enforcement. **TBC:** to be confirmed.

03 / NETWORK SETUP

Site prerequisites and survey

Complete this survey before equipment arrives. Use the final network, not a guest Wi-Fi connection or an installer's mobile hotspot, for acceptance.

Area	Required information / preparation
Ownership	Site name; IT, AV and Dhruv owners; approved change window; emergency contact; remote-access approver.
Devices	Manufacturer, exact model, MAC address, firmware, player/app build, screen location, power mode and wired/Wi-Fi capability.
Network	Player VLAN/subnet, gateway, DHCP scope/reservations, DNS resolvers, NTP servers, IPv4/IPv6 policy, MTU and routing.
Access policy	802.1X/NAC or approved MAC registration; unattended connectivity; no interactive captive portal. Confirm device support before choosing authentication.
Cabling / power	Tested switch ports and cabling, negotiated link speed, suitable power supply or verified PoE budget, UPS requirements and labelled ports.
Service identity	Approved CMS/player FQDNs, valid certificates, reverse-proxy owner, service identities and secure enrolment delivery.
Streaming	Source, destination, transport, codec, resolution, frame rate, peak bitrate, audio, DRM, latency requirement and simultaneous receivers.
Operations	Monitoring, log retention, certificate renewal, storage alerts, patching, backups and a tested restore/rollback owner.

Recommended logical separation

Use separate policy groups or VLANs for players, encoders/headend, servers and privileged management. Guest/student/public-client networks should not initiate connections to display management or backend services. A kiosk's public user interface does not justify access to the entire corporate LAN.

Allow player-to-player or controller-to-player traffic only for an explicitly implemented feature. Normal cloud content polling does not require a flat LAN. Where multicast is selected, design the multicast domain rather than simply disabling segmentation. [R3, S7]

Addressing and time

Prefer managed reservations for headends, controllers and devices requiring inbound LAN control. Record real addresses in the handover; do not copy illustrative subnets from this guide. Keep the selected time source reachable and check the displayed timezone/schedule as well as UTC clock accuracy.

Proposed baseline: wired connectivity for fixed live-streaming receivers; Wi-Fi requires a site survey and load test. Do not treat a good signal indicator as evidence of sustained streaming capacity.

04 / NETWORK SETUP

Connection architecture

Separate content management, media transport and device management. These may use different hosts and ports even when presented through one Dhruv interface.

Control and content flow

Initiator	Destination	Transport / purpose
Administrator browser	Approved CMS HTTPS edge	TCP 443: sign-in, configuration, upload and publish.
HTTPS edge / dashboard	Internal dashboard and Core API	Internal dashboard HTTP 80; Core at api:3001 in inspected Nginx. [R2]
Core service	Approved private database	Configured database connection; PostgreSQL commonly TCP 5432 with production TLS. [R5, S1]
Player / SoC app	Approved Player HTTPS edge	Device-initiated enrolment exchange, content polling, asset download and heartbeat. [R3-R5]
Player / browser	Approved additional media host	Only when the assigned content uses an external origin; its auth and host rules must be recorded.

Live streaming flow

Camera / encoder

- > configured ingest endpoint (for example SRT or RTMPS)
- > media server / packager / authorised provider
- > playback endpoint (for example HTTPS HLS)
- > approved decoder or SoC application
- > display

The encoder's ingest protocol need not be the player's playback protocol. A site streaming SRT to a provider can receive HLS over HTTPS without opening SRT to every screen. The CMS must not be assumed to transcode, relay or store live video merely because it holds the stream URL. [S3, S4]

Local and management paths

For LAN IPTV, the headend sends to the allocated multicast group; receivers join the channel through the switching/routing infrastructure. For manufacturer management, an H200 may separately contact Amino Orchestrate. Neither path is replaced by the Dhruv CMS firewall rule. [S7, S13]

Normal signage design: no unsolicited WAN-to-screen connections. A deliberately selected site-hosted streaming listener or LAN control adapter is an exception requiring an explicit owner, source restriction, authentication and acceptance test.

05 / NETWORK SETUP

Destination host register

These are the starting records for the allowlist. A firewall matches destination hosts/IPs and ports; an HTTP-aware proxy can additionally match paths. Do not confuse the two.

Destination	Role / port	Status and boundary
https://cms.dhruv.org.uk	CMS browser origin; planned TCP 443.	Repository-named target. Confirm deployment, DNS, TLS and routes before approval. [R5]
https://player.dhruv.org.uk	Android Player base URL; TCP 443.	Source-configured target, not a live test result. [R3]
Media / object storage / CDN	Exact hosts returned by the approved content or stream service; usually HTTPS.	Site TBC. Inventory manifest, segments, redirects, keys and licences; avoid unrestricted wildcard egress.
Identity provider	Approved sign-in/discovery/token endpoints for the configured SSO tenant.	Conditional. Administrator/browser or server traffic as actually required; not a blanket Player dependency.
Licence authority	The authority used by the deployed product entitlement service.	Site TBC. Do not invent licence.dhruv.org.uk or assume direct device access.
H200 configuration / lineup	Approved Orchestrate or self-hosted provisioning origin.	Conditional; see section 13. Do not assume the hotel service shares the Core API host.
Staging / support / integrations	Exact staging, relay and third-party hosts approved for this installation.	Site TBC; separate identities and rules from production.

Installation URLs are not yet verified

The repository handover describes target shapes <https://player.dhruv.org.uk/install/lg> and <https://player.dhruv.org.uk/install/samsung>. Treat these as **installation design targets**, not confirmed download services or proof that any model is supported. [R9]

How to maintain the register

For every destination, record the FQDN, resolved addresses, destination port, protocol, initiating component, authentication, owner and date tested. Use provider-managed hostname rules where available. An IP-only firewall needs an approved address-maintenance process; one DNS lookup is not a permanent CDN IP list.

A redirect introduces another destination. Test the complete content journey, including browser resources and signed URL expiry. Keep media URLs without secrets in the shared register; store credentials and unredacted signed links in approved secret storage.

06 / NETWORK SETUP

PROVE IT: Validate the deployed release: unauthorised calls fail correctly; an enrolled Player can retrieve only its authorised content and report heartbeat/status.

HOW: Map the repository-defined paths to the deployed HTTPS origin. Preserve authentication headers and do not expose private database or container ports.

WHY: IT teams often need both the hostname/port and the application path to diagnose proxies, WAFs, authentication and content delivery.

WHAT: The HTTP/API paths used by the CMS and enrolled Players.

Dhruv application endpoints

Paths below are repository-documented contracts. Validate their public host mapping against the running release; the same path can be unavailable on a different gateway or build.

Method and path	Caller / purpose
GET /api/auth/me	CMS session validation; also used by the internal dashboard auth subrequest. [R2]
GET /api/core/devices	Authorised CMS administration: device inventory. [R5]
POST /api/core/device-enrolments/bootstrap	Privileged CMS enrolment creation; returns a protected one-use sidecar. Not a network smoke test. [R5]
POST /api/device-enrolments/exchange	Device-side exchange of the authorised one-use enrolment material. [R5]
POST /api/device-credentials/verify	Device credential verification. Do not supply a shared fleet credential. [R5]
GET /api/players/:deviceId/content	Assigned content manifest for that authenticated device. [R4]
GET /api/player/assets/:assetId	Governed content delivery to an authorised device. [R4]
POST /api/players/heartbeat/:deviceId	Authenticated device status/heartbeat. [R4]
GET /api/core/screens/:screenId/status	Authorised CMS screen status in the permitted scope. [R4]
POST /api/core/schedules/:scheduleId/publish	Authorised publishing with an Idempotency-Key. This changes state. [R4]
POST /api/player/authorization	Site-scoped service identity with player:authorize; not anonymous public access. [R4]

Browser and gateway paths

The inspected dashboard serves /cms/ behind session validation, forwards /api/ and /uploads/ to Core, and keeps /_dhruv_cms_auth internal. A generic browser password gate must not inadvertently challenge device, media or webhook requests. [R2, R8]

A route existing in source is not proof of deployment. Do not invent a /health endpoint, command-poll path or WebSocket URL. Obtain the running service's route contract before writing path-specific WAF rules. A 200 response containing the SPA's index.html is not a successful API test.

Endpoint rules must preserve tenant/site/device authorisation. Network allowlisting never replaces authentication. Test only authorised disposable identities for negative and enrolment tests; never paste production tokens into shared command examples.

07 / NETWORK SETUP

PROVE IT: Test each rule from the same VLAN and device class that will run Dhruv. Record hostname, destination port, result and date.

HOW: Start with DNS/time and outbound HTTPS. Add external content, live-stream or hardware-control rules only when the feature is selected. Keep stateful return traffic rather than opening inbound WAN rules to Players.

WHY: Dhruv needs connectivity to named services, but broad internet or east-west access increases risk without improving normal playback.

WHAT: A least-privilege set of rules for the Player VLAN and any server/management VLANs.

Baseline site firewall matrix

Allow only the applicable rows. Ports shown are destination ports unless the source port is explicitly stated. Use established/stateful return traffic rather than unrestricted inbound ephemeral ranges.

Rule	Initiator → destination	Protocol / port	When / restriction
B01	Players → approved Player service	TCP 443	Core HTTPS profile; exact approved host.
B02	Admin clients → approved CMS service	TCP 443	CMS use; restrict administration as site policy requires.
B03	Players / clients → approved media origins	TCP 443	Only hosts actually needed by assigned content.
B04	Devices / servers → approved DNS resolvers	UDP and TCP 53	Name resolution; not all internet DNS servers.
B05	Devices / servers → approved time servers	UDP 123	Time synchronisation where NTP is used.
B06	DHCPv4 client ↔ server / relay	UDP 68 → 67; replies 67 → 68	Local address service; not a WAN port-forward.
B07	DHCPv6 client ↔ server / relay	UDP 546 / 547	Only when DHCPv6 is used. IPv6 also needs an approved ICMPv6/RA/ND policy.
B08	Clients → specified legacy / probe host	TCP 80	Exception only; plain HTTP is not the Android Player baseline.
B09	Approved clients → configured HTTP/3 service	UDP 443	Optional QUIC/HTTP/3, not required for ordinary TCP HTTPS. [S21]
B10	Approved management source → VPN / bastion	Configured VPN transport / port	Separate approved design; no guessed universal VPN port.

Basis: Dhruv HTTPS source and standard service assignments. IPv6 policy must be designed separately rather than copying IPv4 rules. [R3, S1, S17]

Default restrictions

Deny unsolicited internet-to-player traffic. Deny player access to unrelated corporate, guest and management destinations. Do not publish ADB, database, development servers, screen control APIs or remote desktop ports to the internet. Apply equivalent policy to both address families.

What “required” means here

DNS, address and time services may be supplied locally. Devices using static addresses do not need a new DHCP rule merely because it is listed. A selected integration can require additional egress, but that is approved against its exact service record, not by opening every optional row in this guide.

Keep essential ICMP / ICMPv6 error handling available under site policy so MTU discovery and IPv6 functions are not broken. "Deny all ICMP" is not a safe substitute for a designed firewall policy. [S17]

08 / NETWORK SETUP

PROVE IT: Scan from outside the host/network: only approved public services should answer. Confirm private ports are unreachable externally and the HTTPS route reaches the correct application health/readiness path.

HOW: Expose only the authorised HTTPS edge publicly. Bind application and database services privately or to loopback/internal networks unless a documented architecture requires otherwise.

WHY: Publishing an internal service port directly bypasses the intended TLS, authentication, logging and rate-control edge.

WHAT: The separation between public HTTPS ingress and private application/database/container services.

Hosted edge and private service ports

External clients should reach the approved HTTPS edge, not the database or application container directly. Match these rules to the actual deployed composition.

Traffic / service	Port / transport	Exposure policy
Client → public HTTPS edge	TCP 443	Public Player origin as designed; CMS administration can be further restricted.
ACME HTTP-01 / approved redirect	TCP 80	Only if that certificate/redirect design needs it. DNS-01 does not require inbound 80. [S10]
Admin → SSH host	TCP 22, unless deliberately changed	Approved VPN/bastion or tightly scoped sources; key-based access and no public password login.
Edge → dashboard	Internal TCP 80	Observed dashboard listen port; not a requirement to expose raw HTTP publicly. [R2]
Dashboard → Core API	Internal TCP 3001	api:3001 in inspected Nginx; deny direct public access. [R2]
Core → PostgreSQL	Configured port; commonly TCP 5432	Private app-to-database only. Production store requires database TLS. [R5, S1]
Independent H200 service	Container TCP 3000 in local Compose	Separate workstream. Do not reuse public 3000 as the production API design. [R6, R7]
Optional presentation controller	Internal TCP 8092	Only if the presentation module is actually deployed. Not needed by standard screens. [R2]
Monitoring / backup / update traffic	Actual approved destinations and ports	Server-originated; do not grant players the server's maintenance access.

Container publication is a separate security boundary

A Docker port published on all interfaces can be reachable even when the application is considered “internal”. Docker also manages firewall rules, and its published traffic can bypass the usual UFW path. Review the actual Docker firewall backend, provider firewall and host rules together. [S2]

Prefer no host publication for private services. Where local diagnostic access is justified, bind to loopback, for example 127.0.0.1:<host-port>:<container-port>, and verify the resulting socket bindings. Do not run a generic firewall script from this document against an existing production host.

Opening inbound 443 on Hetzner and opening outbound 443 at the customer site are different changes. The first permits access to the server; the second permits a device to initiate a request to it.

09 / NETWORK SETUP

PROVE IT: Test the complete encoder-to-platform-to-screen journey, including authentication, codec support, reconnect and sustained playback.

HOW: Choose the actual stream architecture first, then approve its exact listener, direction, destination and media range. Never use a generic high-UDP range unless the configured service genuinely requires it.

WHY: “Live streaming” is not one port. HLS over HTTPS, SRT, RTSP/RTP, multicast and WebRTC have different connection and firewall behaviour.

WHAT: A protocol selection table for live contribution and playback.

Live-streaming port matrix

Choose the transport from the actual ingest or playback URL and device configuration. This table describes protocol behaviour, not universal support by all Dhruv players or SoC models.

Transport	Typical listener / destination	Required network decision
HLS / DASH over HTTPS	TCP 443; custom port if specified	Player → playback origin/CDN. Include manifests, segments and required key/DRM destinations. [S3]
HTTP playback	TCP 80 or configured port	Legacy/provider exception only; do not disable Android TLS protections to use it. [R3]
RTMP / RTMPS ingest	RTMP commonly TCP 1935; RTMPS uses the provider-configured TLS port	Encoder → ingest listener. Do not assume a universal RTMPS port or open 1935 to every player. [S1]
RTSP / RTSPS control	RTSP TCP 554; RTSPS TCP 322; 8554 is an alternative service setting	Client → RTSP server. Confirm transport/version on both endpoints. [S5]
RTP / RTCP media	Negotiated/configured UDP ports; or RTSP TCP-interleaved media	Record the exact range and both endpoint roles. Port 554 alone may not carry video. [S5]
SRT	Configured UDP port; 9000 is only an example	Record listener, caller, NAT mapping and media direction. No fixed universal SRT port. [S4]
UDP / RTP multicast IPTV	Assigned group address and UDP destination port	Headend → joined LAN receivers; IGMP is separate control traffic. [S7, S8]
WebRTC / TURN	Application-specific media; TURN defaults 3478 / 5349	Record ICE servers, relay range, signalling and fallback. See section 12. [S6]
HTTP/3 / QUIC	UDP 443 when enabled	Optional HTTPS transport optimisation; test permitted fallback to TCP. [S21]

Do not approve guessed media ranges

Ranges such as “all UDP high ports” or “10000–20000” are not generic Dhruv requirements. Use the range configured on the actual RTP receiver, media server or TURN server, then test both normal operation and reconnection. A range from a different vendor’s example is not evidence for this installation.

A hostname and open port are insufficient to define a stream. Record channel/path, protocol, codec, bitrate, latency, encryption, authentication, source restrictions and failover behaviour. Validate content rights and the selected application’s playback capability before commissioning.

10 / NETWORK SETUP

Setting up unicast live streams

Keep contribution (encoder to platform) separate from distribution (platform to screens). Approve one complete end-to-end path before adding more channels or devices.

HTTPS HLS / DASH playback

Create a stream record using an approved playback URL. HLS playlists can refer to further playlists, media segments, initialisation data and encryption keys; those destinations also need to be reachable. For a browser player, check cross-origin policy and mixed-content restrictions. [S3]

```
Example only – not a Dhruv endpoint:  
https://stream.example.com/live/channel01/index.m3u8  
https://stream.example.com/live/channel01/manifest.mpd
```

Test with the intended device and credentials, including redirects and URL renewal. Confirm that a live playlist advances and actual audio/video play for the agreed soak period. A successful request for the first playlist is not a streaming acceptance result. Set stream-loss fallback and alerting; cached signage does not cache a continuing live event.

RTSP / RTP

Agree whether media use negotiated UDP ports or TCP interleaving. With UDP, record the receiver range, source and return/control behaviour; with interleaving, verify that both endpoints support it. Do not assume a proxy will automatically handle RTSP negotiation or NAT. Keep unauthenticated camera/encoder services off public networks. [S5]

SRT

Set one endpoint's connection role and the other's matching role. Caller/listener identifies who establishes the connection, not who sends the video. An outbound caller at the site can simplify firewall traversal, but the receiving listener still needs a reachable configured UDP socket. [S4, S19]

```
Example contribution path only:  
Encoder (caller) -> ingest.example.com : UDP 9000  
Listener -> established return traffic to encoder  
Player -> approved HTTPS playback origin : TCP 443
```

Record the actual port, stream ID, encryption policy, latency and NAT/public address. Keep passphrases outside URLs in shared documentation. Test packet loss, reconnect and the selected latency under representative load. A TCP port test does not verify SRT. If the chosen listener is behind carrier-grade NAT, obtain a supported relay/outbound design rather than promising an ordinary port-forward. [S19]

Do not route SRT, raw RTMP or TURN through an ordinary HTTP reverse-proxy location. They need transport-appropriate listeners or gateways. The current Dhruv dashboard's /api/ proxy does not establish a streaming server. [R2]

11 / NETWORK SETUP

PROVE IT: Join/leave channels on real receivers, verify switch group tables, confirm no flooding to unrelated ports, and test multiple simultaneous receivers.

HOW: Use an IPTV VLAN, IGMP snooping, a querier where required, controlled routing/PIM only when designed, and explicitly allocated multicast groups/UDP ports.

WHY: Multicast can distribute one stream efficiently to many receivers, but unmanaged flooding can disrupt a signage or corporate LAN.

WHAT: Local one-to-many IP video using multicast groups and multicast-aware switching.

LAN IPTV and multicast

Use multicast only when the selected headend, switches, routing and receivers have been designed and tested together. It is not a public-internet distribution method.

Channel allocation example

Record	Illustrative value	Replace with
Headend source	10.20.30.10	Approved source address and interface
Multicast group	239.10.10.10	Site-assigned administratively scoped group
Destination port	UDP 5000	Actual channel port from encoder/lineup
Receiver network	AV player VLAN	Actual VLAN/subnet and switch ports
TTL / hop scope	Set for the approved path	Documented headend and routing setting
Join mode	IGMP version agreed by design	Version and source-specific support of all devices

All addresses and ports in this example are illustrative. Administratively scoped IPv4 multicast addressing is defined in RFC 2365. [S8]

Switching and routing checklist

Enable and verify IGMP snooping on receiver VLANs and ensure there is a working elected querier. Check receiver membership, channel changes and group ageing. Do not enable fast-leave on a port carrying multiple downstream receivers without a validated design. [S7, S20]

IGMP is IP protocol 2, not TCP or UDP port 2. It manages IPv4 membership; the channel payload uses its assigned UDP port. Cross-VLAN multicast needs explicit multicast routing and scope/ACL policy, not merely ordinary unicast routing. IPv6 multicast requires its own MLD/ICMPv6 design. [S7, S17, S18]

Limit source, group, receiver VLANs and routed scope. Avoid flooding multicast to guest Wi-Fi, unrelated users or all switch ports. A single channel can consume bandwidth on every forwarding uplink; verify shared trunks and downstream fan-out, not only the headend NIC.

Acceptance evidence

Record group membership and counters, verify every receiver displays the correct channel, change channels repeatedly, restart one receiver, and test after the agreed membership-ageing interval. Check that non-member ports are not unexpectedly flooded and that a querier failure is detected. Record packet loss, visible artefacts and recovery under load.

Wi-Fi multicast behaviour varies by access-point configuration. Use a validated multicast-to-unicast or other supported design where required; do not assume an Ethernet success proves a wireless installation.

12 / NETWORK SETUP

WebRTC, timing and multi-screen playback

These are conditional network profiles. The repository's ordinary HTTPS polling does not by itself prove that a WebRTC or frame-synchronised playback path is deployed.

WebRTC connection inventory

Layer	Record before opening rules
Signalling	Actual HTTPS/WSS hostname, path, port and authentication.
ICE discovery	Exact STUN/TURN hostnames, URLs, transport and credentials policy.
TURN access	Common defaults: UDP/TCP 3478; TLS-over-TCP or DTLS-over-UDP 5349. Use the deployed configuration. [S6]
Media / relay	Actual SFU/media listener and configured relay allocation range; peer/source policy.
Restricted-network fallback	A deliberately configured TURN-over-TLS path, sometimes on 443; forced-relay test required.
Capacity	Maximum sessions, codecs, bitrate and server relay egress; do not size on signalling traffic alone.

HTTPS/WSS connectivity does not prove media connectivity. TURN also allocates relay addresses/ports for the peer path. Do not assume that opening 3478 alone completes every TURN firewall path, or that any HTTPS server on 443 can accept TURN. [S6]

When placing TURN TLS and HTTPS on port 443, provide separate addresses or a documented compatible transport-layer design. Keep the relay range constrained to the server's actual configuration. Test direct and forced-relay calls from the final site network, including restrictive egress conditions.

Screen groups and synchronised content

Provide reliable time service, consistent device timezone/schedule settings, sufficient download capacity and preloading where supported. But NTP, shared Wi-Fi or identical playlists do not establish frame-accurate synchronisation. The inspected Android source explicitly separates readiness preparation from physical synchronised-start evidence. [R3]

For a multi-screen splash, record the supported player/runtime, control path and any actual local timing transport. Do not open PTP, broadcast or peer-to-peer ports unless the selected implementation uses them. Test all screens together and measure start skew, drift, recovery and fallback against an agreed tolerance.

Keep a working ordinary signage page available when an optional control or synchronisation capability is unsupported. Missing model-specific support is not a reason to open every management port or disable authorisation.

Amino H200 setup and cloud ports

Select the provisioning method first. H200 can use Orchestrate, a self-hosted configuration service or USB provisioning; a self-hosted installation does not automatically require all Orchestrate destinations. [S14]

Hardware and application prerequisites

Record the H200/H200W model, firmware and application, Ethernet/HDMI path, power arrangement, configuration/lineup origin and approved playback transport. Amino documents gigabit Ethernet and model-dependent PoE/Wi-Fi options. Verify the actual unit and switch power budget. The Dhruv H200 workstream still requires firmware transport confirmation and real-device acceptance. [S14, R6]

Orchestrate destination matrix — conditional

Vendor-published requirements, updated 2 April 2026. These are device-originated management connections, not general signage ports. Confirm the assigned region and current vendor policy before applying. [S13]

Destination	Destination port / transport
connectivitycheck.gstatic.com	TCP 80 — connectivity probe
www.google.com	TCP 443 — connectivity probe
orch-accs.aminoengage.com	TCP 7743 — HTTPS configuration / TR-069
ensight-cmd.aminoengage.com	TCP 443 — command redirection
orch-logfile.aminoengage.com	TCP 10446 — HTTPS log upload
gcs.amino-orchestrate.com files.amino-orchestrate.com	Vendor table groups TCP 80 / 443 for firmware; confirm exact host/URL pairing.
orch-stun.aminoengage.com	UDP 3478 — management STUN
EMEA Resolve cluster: ensight-cmd31.aminoengage.com ensight-cmd32.aminoengage.com ensight-cmd33.aminoengage.com ensight-cmd34.aminoengage.com	TCP 22, TCP 10444 and UDP 1194 Only for the applicable device-access service/region.

Do not open both US and EMEA clusters by assumption. Reconfirm DNS/IP requirements with Amino; resolve the firmware table's grouped entries before narrowing production rules. Cloud management STUN is not evidence that Dhruv playback uses WebRTC. [S13]

Local H200 control is a separate record

For an enabled local EELM/vendor API, record the exact firmware manual, transport, listening port, authentication and controller source. None is treated as a universally verified local control port here. Channel media follows the selected streaming profile; cloud management ports do not replace it.

Display control and remote support

Use the normal authenticated device channel for supported controls. Local control and remote support need their own approval, access scope and audit trail.

SoC and panel control

Do not assign one universal Samsung, LG, SOLUM or Android management port. Exact model, firmware, enabled API and installed adapter determine the transport. A controller on the LAN may need a device listener; another model may use only device-initiated HTTPS. RS-232 and HDMI-CEC do not themselves require TCP/UDP firewall ports.

Keep unsupported power/input/brightness functions unavailable rather than enabling a debug service to simulate support. Check whether the panel's network interface remains reachable in standby before promising remote power-on. Record Wake-on-LAN or vendor wake behaviour only when explicitly supported and tested.

Temporary engineering access

Legacy Android ADB over TCP commonly uses 5555; modern wireless debugging uses a pairing/connection workflow with negotiated ports. Neither is required for ordinary Dhruv operation. Restrict any approved temporary use to a management host/VLAN, then disable it and re-test isolation. Never expose it publicly. [S9]

Optional RustDesk self-hosted profile

Service	Destination ports	Approval boundary
ID / connection / NAT test	TCP 21115; TCP and UDP 21116	Clients → approved ID server; server listener/firewall must match.
Relay	TCP 21117	Clients → approved relay; test forced relay and bandwidth.
Web client only	TCP 21118 / 21119 internally	Keep closed if unused. If used, restrict to the trusted reverse proxy.
Pro console only	TCP 21114	Not an OSS baseline requirement; restrict administration separately.

The official RustDesk documentation warns that direct access to its WebSocket listeners permits spoofed forwarding headers. Put those listeners behind a correctly configured trusted proxy when used. No RustDesk server or hostname is confirmed deployed by this guide. [S15, S16]

Prefer approved relay-only support where direct peer connectivity is not permitted; test that mode rather than allowing arbitrary destinations. Remote-control permissions, unattended access, server identity keys and operator logging are separate from opening the server ports.

15 / NETWORK SETUP

Hetzner hosting and Mac Docker

Use the existing server only after confirming its current composition and capacity. Local development, hosted staging and production must remain separate security and data boundaries.

Hosted setup sequence

- 1. Inventory and back up.** Record running services/images, compose/launch files, mounts, certificate management, listening sockets, DNS, free disk, private networks and rollback route. Capture configuration without exposing environment secrets.
- 2. Choose service origins.** Confirm the production CMS/player hosts and create a separately approved staging hostname only when DNS, TLS and the owner are available. A placeholder such as api-staging.example.com is not a provisioned service.
- 3. Isolate deployments.** Use separate databases/volumes, credentials, ports and networks. Do not let staging enrol devices against production or reuse its signing/licensing secrets. Expose the approved HTTPS edge only; keep service listeners private.
- 4. Verify all firewall layers.** Hetzner Cloud Firewalls are stateful; once outbound rules are added, unmatched outbound traffic is denied. The retrieved FAQ says they do not secure private Cloud Network traffic, so enforce appropriate host/container controls too. Confirm this applies to the actual Hetzner product in use. [S11]
- 5. Prove the running route.** From the final client network, test DNS/TLS, authenticated API access and content delivery. From an authorised external test host, verify private backend/database ports are unreachable. Preserve evidence before widening access.

Mac Docker development

Identify the maintained workstream's actual compose file rather than assuming a root-level docker-compose.yml exists. Prefer loopback-only publication for developer tools. The independent H200 example maps 3000:3000; harden the effective development binding where LAN access is not needed. [R7, S2]

```
Illustrative port-binding fragment only:
ports:
  - "127.0.0.1:3000:3000"
# Use the correct service and reviewed override for the chosen stack.
```

A phone or screen's localhost is that device, not the Mac. To test a physical device, use an approved reachable Mac/LAN address and the application's supported trusted-TLS configuration, with source-restricted host firewall access. Keep production credentials out of local files and shared screenshots.

The described 80 GB disk and one-to-two-connection staging workload are planning inputs, not proof of streaming, transcoding or production capacity. Measure storage and bandwidth; keep backups outside the single host and test restoration.

16 / NETWORK SETUP

DNS, TLS, proxies and authentication

Connectivity must preserve the application's security model. Do not "fix" a certificate, proxy or authentication error by disabling validation or sharing one device credential.

Topic	Required setup / validation
DNS / identity	Correct A/AAAA records, gateway and resolver reachability; stable approved FQDNs. Avoid raw-IP URLs when the certificate and auth origin expect a hostname.
TLS trust	Use a valid hostname-matching certificate and complete chain. Test device trust stores and clock. The Android source uses system trust anchors and disables cleartext. [R3]
TLS inspection	Document the site inspection policy. Use an explicitly approved endpoint exception if interception is incompatible; do not set "trust all" or use curl -k as acceptance.
Proxy / content filters	Confirm unattended device proxy support. Exclude interactive captive portals and browser-only authentication challenges from device paths.
Cross-host media	The Android source attaches device credentials only to its exact configured HTTPS origin. Use an approved signed URL/auth mechanism for other origins; never forward the bearer token blindly. [R3]
Methods / downloads	Permit the actual route methods. Test authorised uploads, media byte-range delivery when required and signed URL renewal; do not cache personalised API responses.
CORS / embedding	A browser media/widget may need approved origins, redirects and subresources. An open TCP port does not override browser CORS, CSP or mixed-content checks.
Certificates / renewal	Record renewal owner and challenge. HTTP-01 needs TCP 80; DNS-01 can avoid inbound 80; TLS-ALPN-01 uses 443 with supporting infrastructure. [S10]

Known reverse-proxy review point

The inspected dashboard API proxy has an 8-second read timeout and WebSocket upgrade headers. That does not prove a long-lived socket/SSE or streaming endpoint exists. For an implemented long-lived route, review timeout, buffering and heartbeat behaviour specifically; do not relax every API route indiscriminately. [R2, S12]

Keep /api/ handling ahead of the single-page application fallback. Preserve the trusted forwarding chain and session/device distinction. Do not apply a browser Basic Auth prompt to machine device endpoints, and do not allow a service token to bypass a browser-only administration gate. [R2, R8]

17 / NETWORK SETUP

Capacity, bandwidth and continuity

The figures below are worked planning examples, not measured Dhruv performance or minimum hardware guarantees. Replace every bitrate, concurrency and headroom assumption with the selected service's data.

Bandwidth calculations

Scenario / assumption	Calculation	Planning result
20 unicast screens, each 8 Mb/s; 30% headroom	$20 \times 8 \times 1.30$	208 Mb/s site downstream
One 8 Mb/s outgoing encoder; 30% headroom	8×1.30	10.4 Mb/s site upstream
50 unicast screens, each 6 Mb/s; 30% headroom	$50 \times 6 \times 1.30$	390 Mb/s site downstream
One 8 Mb/s stream for one hour; decimal units	$8 \times 3,600 \div 8 \div 1,000$	3.6 GB per receiver-hour before overhead
20 devices each fetch 1 GB in 15 minutes	$20 \times 1 \times 8,000 \div 900$	177.8 Mb/s average before overhead

These calculations treat the stated bitrate as the total selected stream payload. Add audio separately if it was excluded, and account for peaks, retransmission, adaptive variants, background downloads, VPN overhead and shared business traffic. The 30% factor is an illustrative design allowance, not a universal engineering standard.

Distribution and storage

Unicast generally scales with simultaneous receivers. Multicast forwarding depends on channels and membership on each link; a shared uplink may carry one copy per channel while each receiver link still carries its selected stream. Verify the real topology and switch counters. [S7]

The CMS need not carry every video byte if an approved origin/CDN supplies media. Conversely, a self-hosted relay/packager adds its own egress, CPU and storage load. Do not estimate transcoding capacity from disk size. Set separate capacity budgets for database, media, logs, images and backups.

Continuity policy

Set download windows and staged rollouts so a full fleet does not update simultaneously. Define which cached content remains eligible during outages, how an interrupted download is recovered, and what viewers see when a live stream stops. The Android source validates an offline cache, but this document does not establish hardware network-loss acceptance. [R3]

Agree recovery-time and data-loss objectives, a stream fallback, alerts, and an observed restart/reconnect procedure. Test the final number of screens through a representative content cycle and live-stream soak; record measured latency, start skew, drift, bandwidth and free storage.

18 / NETWORK SETUP

Network diagnostic commands

Run only on systems and endpoints you are authorised to test. These examples are read-only checks; they were not executed against your live deployment while preparing this guide.

DNS and TCP reachability

```
# macOS / Linux – repository-named targets, not live-verified
dig +short cms.dhruv.org.uk A
dig +short cms.dhruv.org.uk AAAA
dig +short player.dhruv.org.uk A

# Windows PowerShell
Resolve-DnsName player.dhruv.org.uk
Test-NetConnection player.dhruv.org.uk -Port 443
```

TLS and route behaviour

```
# Certificate chain and hostname verification; never add -k
openssl s_client -connect player.dhruv.org.uk:443 \
  -servername player.dhruv.org.uk \
  -verify_hostname player.dhruv.org.uk \
  -verify_return_error </dev/null

# An unauthenticated route probe: no production token included
curl --connect-timeout 5 --max-time 15 -sS -D - \
  -o /dev/null https://cms.dhruv.org.uk/api/auth/me
```

Record DNS answers, certificate identity/expiry and HTTP status/content type. An unauthorised response can demonstrate that a route was reached, but does not establish successful sign-in. A login redirect or 200 HTML response must not be labelled an API pass. Perform the authenticated check through the approved client or secure test harness.

Read-only host inventory

```
# Linux host – output may contain sensitive topology
sudo ss -lntup
docker ps --format 'table {{.Names}}\t{{.Ports}}'
df -h

# macOS listening TCP services
lsof -nP -iTCP -sTCP:LISTEN
```

Verify unexpected 0.0.0.0 / [::] bindings, internal-service exposure and free disk. Use the correct deployed configuration files, but do not attach environment dumps or secrets to the handover. Test from the actual player VLAN as well as from an administrator's laptop.

Ping and TCP tests do not prove UDP media, authentication or playback. Use the actual decoder, server counters and an authorised bounded packet capture for SRT/RTP/multicast diagnostics. Redact credentials and signed URLs from logs and captures.

19 / NETWORK SETUP

Commissioning and acceptance checklist

Leave each box unmarked until evidence is retained. “Not applicable” needs a reason and owner. A passed network test does not automatically pass application, hardware or user acceptance.

Check	Pass condition / evidence	Result
01 • Inventory	Models/builds, VLANs, assigned addresses, switch ports and approved endpoints recorded.	[]
02 • Address / DNS / time	Correct DHCP/static config, A/AAAA resolution, gateway and time; survives reboot.	[]
03 • TLS / egress	Valid certificate chain/hostname from real devices; only intended service destinations permitted.	[]
04 • CMS session	Authorised user signs in; correct tenant/site; unauthorised requests fail as expected.	[]
05 • Enrolment	Disposable approved device enrolls once; credential bound to correct device/site; no secret leakage.	[]
06 • Publish / content	Approved test asset is delivered and visibly plays; manifest/asset identity recorded; heartbeat reports it.	[]
07 • Device controls	Only supported controls shown; actual commands and acknowledgements verified on each required model.	[]
08 • Live playback	Correct channel, video/audio/DRM, latency and quality on intended hardware for agreed soak.	[]
09 • Selected transports	RTSP media path, SRT roles/UDP, multicast membership or WebRTC forced relay tested as applicable.	[]
10 • Restart / outage	Power restart, WAN loss/recovery and interrupted download tested; approved fallback and status truthful.	[]
11 • Isolation / exposure	Private API/DB/debug ports unreachable from unauthorised sources; IPv4/IPv6 and staging separation tested.	[]
12 • Load / renewal	Full target concurrency, content refresh, token/certificate lifecycle and storage thresholds evidenced.	[]
13 • Handover	Owners, firewall change IDs, backups, restore evidence and unresolved issues recorded.	[]
14 • User acceptance	Named customer/user signs the actual installation outcome separately from engineering checks.	[]

Proposed test record: timestamp/timezone; operator; device ID/model/build; service revision; source VLAN; destination/port; expected result; actual result; log/screenshot/capture reference; issue/owner. Set the required soak duration and recovery tolerance before starting, not after seeing the result.

No row above is marked complete by this guide. An unavailable external dependency blocks its specific acceptance test; it does not justify treating unrelated completed tests as failed or claiming an untested feature passed.

20 / NETWORK SETUP

Troubleshooting by symptom

Start with the initiating component and its exact destination. Separate network, TLS, identity, media and device capability failures rather than repeatedly opening more ports.

Symptom	Likely checks	Next evidence
CMS opens; screen stays offline	Different CMS/player origins; device VLAN egress; clock/TLS; enrolment credential.	Device request status, DNS answers, gateway/firewall logs and authenticated heartbeat.
API returns 200 but data are missing	SPA fallback caught /api/; proxy route mismatch; wrong deployed build.	Content-Type and body shape; active proxy config/revision. [R2]
Signage works; live stream is blank	Separate media host/port; redirects/keys; expired signed URL; unsupported codec/DRM.	Full media request chain plus actual decoder error and source output.
TLS fails only on the screen	Device clock; incomplete chain; trust-store age; interception; wrong hostname.	Screen clock, verified certificate chain and inspection policy. [R3]
RTSP connects; no video	RTP/RTCP UDP range or NAT blocked; incompatible interleaving.	Negotiated transport, source/destination media sockets and decoder logs. [S5]
SRT does not connect	Wrong UDP port; two callers/listeners in incompatible setup; NAT; stream ID/encryption mismatch.	Both endpoint roles/configuration and bounded UDP capture. [S4]
Multicast stops after a delay	Missing querier; membership ageing; snooping/routing mismatch.	Querier and group membership state over time; port counters. [S7]
Works on laptop, not player VLAN	Different DNS/proxy/NAC policy; browser trust differs; test device not on final network.	Repeat on intended device and VLAN, not through hotspot.
Drops during updates or peak hours	Link congestion; Wi-Fi contention; server egress/storage; shared uplink saturation.	Time-aligned traffic, loss, CPU/disk and download/stream logs.
Control works when on, not in standby	Panel NIC sleeps; unsupported wake/control path; model capability mismatch.	Manufacturer-supported standby behaviour and real device test.
H200 plays, but Orchestrate fails	Management ports/hosts differ from media destinations; wrong assigned region.	Vendor endpoint matrix, device management logs and approved rule hits. [S13]
A 502 appears after container replacement	Proxy/upstream discovery or readiness; wrong internal port.	Actual backend health and resolution; preserve maintained Docker DNS behaviour. [R2]

Keep a dated problem record and reverse any temporary diagnostic exception after testing. Do not leave public debug ports, bypassed certificate validation or anonymous media/admin routes behind as a “temporary fix”.

21 / NETWORK SETUP

Firewall request and site handover

Copy this page into the installation change record. The final approved rule set is the populated site-specific register, not every possible port listed in this guide.

Site and service record

Field	Approved value
Site / change ticket / change window	To complete
Player VLAN / subnet / gateway	To complete
DNS / NTP / DHCP or static assignment	To complete
CMS / Player HTTPS origins	To complete and live-verify
Media hosts / stream URLs (redacted)	To complete
Encoder / receiver models and builds	To complete
Streaming / management profiles selected	To complete; mark unused profiles not applicable

One record for each firewall rule

Field	Required entry
Source → destination	Exact VLAN/host/service group → exact FQDN/IP/group
Transport / destination port	TCP, UDP or IP protocol; single port or justified configured range
Direction / initiating component	Site outbound, server inbound, private LAN or multicast; stateful return policy
Reason / authentication / lifetime	Feature, credential owner, permanent or time-limited, expiry/review date
Validation / rollback	Test ID, evidence, expected rejection test and rollback action

Separate sign-offs

Approval	Name / date / evidence
Network rules and isolation	To complete
Dhruv application / deployed revision	To complete
AV hardware and live-stream acceptance	To complete
Customer / USER VERIFIED	To complete; never inferred from a merge or successful build

Outstanding dependency / risk: _____

Owner / next action / review date: _____

22 / NETWORK SETUP

Repository references

All repository references use the inspected source snapshot, not an assumption that the same revision is deployed. Some endpoint/Compose entries were established from indexed excerpts rather than a full-file review.

[R1] Repository main snapshot

Commit 9a372468f73656754fdff5f8b83fddd5e6ad8907. Read 16 September 2026; commit timestamp 06:12:42 UTC.

[Open source](#)

[R2] Dashboard reverse proxy

Full configuration reviewed: internal listen 80, api:3001, optional presentation-demo:8092, API/upload routing, session gate and 8-second read timeout.

[Open source](#)

[R3] Android signage Player

Full README reviewed: Player HTTPS origin, system trust, credential binding, content cache and explicit hardware/production acceptance boundaries.

[Open source](#)

[R4] Core application route contract

Indexed excerpts reviewed for device content/assets/heartbeat, screen status, publishing and player-authorization route contracts.

[Open source](#)

[R5] Device credentials and enrolment

Full contract reviewed: administrative and device-only routes, secure enrolment, PostgreSQL TLS and live-deployment evidence boundary.

[Open source](#)

[R6] Independent hotel IPTV / Amino H200 workstream

Full README reviewed: separate service, scoped APIs, pairing/telemetry and outstanding vendor transport / hardware acceptance.

[Open source](#)

[R7] H200 local Compose example

Indexed excerpt reviewed: local port 3000 mapping and PostgreSQL connection. Example credentials intentionally not reproduced.

[Open source](#)

[R8] CMS-only perimeter auth snippet

Indexed excerpt reviewed: scope the browser gate to CMS; do not apply it indiscriminately to Player/device/webhook paths.

[Open source](#)

[R9] LG and Samsung installation handover

Indexed excerpt reviewed: /install/lg and /install/samsung are target public shapes, not live-verified services.

[Open source](#)

23 / NETWORK SETUP

Protocol and infrastructure references

Primary technical documentation consulted on 16 September 2026. Service defaults describe protocols; deployment owners must confirm the configured listener and supported implementation.

[S1] IANA service name and transport port registry

Reference for standard service assignments, including baseline network services. A registry entry does not make a port necessary for every Dhruv installation.

[Open source](#)

[S2] Docker: packet filtering and firewalls

Published-port behaviour, Docker-managed firewall rules and the interaction with UFW.

[Open source](#)

[S3] RFC 8216: HTTP Live Streaming

Playlists, media references, keys and associated HLS resources. DASH is listed as a separate selected HTTP media profile, not asserted as universal player support.

[Open source](#)

[S4] Haivision: SRT stream settings

Primary vendor description of SRT caller/listener addressing and configured UDP ports. Product-specific latency defaults are not adopted as Dhruv requirements.

[Open source](#)

[S5] RFC 7826: Real-Time Streaming Protocol 2.0

RTSP/RTSPS defaults and negotiated/interleaved media transport. Confirm the RTSP version and options actually supported by both devices.

[Open source](#)

[S6] RFC 8656: TURN

TURN server transport defaults, relayed addresses and associated peer traffic.

[Open source](#)

[S7] RFC 4541: IGMP/MLD snooping considerations

Multicast membership-aware forwarding and snooping behaviour; supports the multicast design and test checklist.

[Open source](#)

[S8] RFC 2365: administratively scoped multicast

IPv4 administratively scoped multicast address planning. The example channel allocation is not a deployed Dhruv service.

[Open source](#)

[S9] Android Developers: Android Debug Bridge

ADB TCP/IP and wireless debugging. Debugging is conditional engineering access, not a standard signage firewall dependency.

[Open source](#)

24 / NETWORK SETUP

Vendor, hosting and security references

Vendor-hosted endpoints and service behaviour can change. Recheck the appropriate reference at commissioning and retain the dated, approved site register.

[S10] Let's Encrypt: challenge types

HTTP-01, DNS-01 and TLS-ALPN-01 requirements; port 80 is conditional, not universally required by a TLS deployment.

[Open source](#)

[S11] Hetzner Cloud Firewalls FAQ

Stateful behaviour, inbound/outbound default policy and the documented private Cloud Network limitation. Confirm the actual Hetzner product and applied resources.

[Open source](#)

[S12] Nginx: WebSocket proxying

Upgrade handling and proxy timeout considerations for implemented long-lived routes.

[Open source](#)

[S13] Amino: Orchestrate Network Requirements

Vendor page updated 2 April 2026. Source of the conditional Orchestrate/EMEA Resolve destination matrix; grouped firmware entries require site confirmation.

[Open source](#)

[S14] Amino: H200 Quick Start Guide

Vendor page updated 30 June 2026. Provisioning options, basic interfaces and model-dependent power/wireless features.

[Open source](#)

[S15] RustDesk Server OSS: Docker

Port roles for ID, NAT test, relay and optional web clients; Pro console distinction.

[Open source](#)

[S16] RustDesk Server OSS: installation

Security warning and trusted-proxy restrictions for the optional WebSocket listeners.

[Open source](#)

[S17] RFC 4890: filtering ICMPv6

IPv6 firewall considerations, including essential control/error traffic. IPv4 MTU error policy should also be reviewed by the network owner.

[Open source](#)

[S18] IANA protocol numbers

IP protocol-number registry; IGMP uses IP protocol 2, distinct from TCP/UDP port numbers.

[Open source](#)

[S19] Haivision: real-time video through a firewall

SRT connection roles, firewall traversal and deployment patterns; media direction is distinct from connection initiation.

[Open source](#)

[S20] RFC 3376: IGMP version 3

Membership queries, reports and multicast router state. Use the IGMP version supported by the chosen equipment.

[Open source](#)

[S21] RFC 9114: HTTP/3

HTTP over QUIC and handling connectivity failure; HTTP/3 is conditional rather than the base TCP HTTPS profile.

[Open source](#)