Multicast IP — Private Addressing & UDP Ports (with Aruba Notes)

Antonio Pérez

September 2025

Introduction

IP *multicast* addressing enables efficient data delivery to multiple receivers. A multicast flow is defined by *group IP + UDP/port* in most applications (TCP does not apply to native multicast). In enterprise networks, it is recommended to separate ranges by application and choose ports that avoid conflicts with well-known services.

Reserved Multicast IPv4 Address Ranges

The IANA defines ranges for different purposes. Table 1 summarizes the main ones.

Address Range	**Purpose**
224.0.0.0 – 224.0.0.255	Link-local (non-routable; protocol control)
224.0.1.0 – 224.0.1.255	Routable control/services (e.g., NTP 224.0.1.1)
224.0.2.0 – 224.0.255.255	Reserved / future use
233.0.0.0 – 233.255.255.255	GLOP addressing (RFC 2770)
239.0.0.0 – 239.255.255.255	**Administratively Scoped** (private use)

Table 1: Reserved IPv4 multicast ranges (IANA).

Common Multicast UDP Ports by Application

Common ports in popular applications (reference). Avoid collisions with these when defining internal services.

Application / Protocol	Typical Address	UDP Port
RTP/RTSP (Streaming)	239.x.x.x / 232.x.x.x	5004–5005
SAP/SDP (Session Announce)	224.2.127.254	9875
mDNS / AirGroup (Apple)	224.0.0.251	5353
SSDP / UPnP discovery	239.255.255.250	1900
NTP (multicast sync)	224.0.1.1	123
OSPF (routing)	224.0.0.5 / 224.0.0.6	(IP protocol, no UDP)
PIM / IGMP control	224.0.0.x	(no UDP/TCP)
Video conference (dynamic RTP)	239.x.x.x	16384–32767
IPTV / DVB	232.x.x.x / 239.x.x.x	5000–5500
GDOI/GMS (Key management)	224.0.0.x	848

Table 2: Common multicast UDP ports by application.

Recommended Private Addressing (Administratively Scoped)

For private networks, use **239.0.0.0/8**. Practical suggestions:

- Reserve **blocks per application/project**:
  - **239.16.0.0/16** → Internal video / IPTV (e.g., `239.16.x.x`).
  - **239.20.0.0/16** → Telemetry / IoT (e.g., `239.20.x.x`).
- Avoid `224.0.0.x` (link-local control for routing/protocols).
- Document subranges (e.g., per VLAN/campus) to avoid overlaps.

Safe UDP Port Ranges (to avoid conflicts)

Range / Port	Category	Notes
`0-1023`	Well-known (do not use)	Reserved by IANA for standard services.
`123`	Avoid specific	NTP (time sync).
`1900`	Avoid specific	SSDP / UPnP discovery.
`5004`	Avoid specific	RTP (media streams).
`5353`	Avoid specific	mDNS / AirGroup.
`9875`	Avoid specific	SAP/SDP (session announce).
`20000-29999`	Recommended internal	Internal video/audio streams.
`40000-49999`	Recommended internal	Lab testing / telemetry.

Table 3: Safe UDP port ranges and specific ports to avoid in multicast deployments.

Best Practices on Aruba (CX 6400 / WLAN 7220)

- On switches: enable **IGMP snooping**; forwarding is based on ports with *IGMP Join*.
- On WLAN: use **Dynamic Multicast Optimization (DMO)** where applicable; filter unnecessary *broadcast*.
- Verification:
  - `show igmp-snooping groups vlan <ID>`
  - `show ip igmp interface vlan <ID>`
- Example of internal flow: `239.16.0.2:20001/UDP`; only delivered to ports with active IGMP membership.

Conclusion

Using **239.0.0.0/8** with separated blocks (`239.16.x.x` for video, `239.20.x.x` for IoT) and ports **UDP 20000–29999 / 40000–49999** reduces conflicts and simplifies operations. On Aruba CX/WLAN, validate IGMP memberships and apply DMO/broadcast-filter where needed.