

Ambu[®] aView[™] 2 Advance

Troubleshooting guide for DICOM connectivity with PACS



This document is property of Ambu A/S. No part of it may be reproduced or used in any form or by any means without written permission of the owner.

1. Purpose of this document

This document aims to provide healthcare IT professionals with additional troubleshooting tips, when setting up the PACS connectivity with Ambu aView 2 Advance monitor. For step-by-step instruction of setting up the network and PACS connectivity, please make sure to go through section 4.2.3 and 4.2.4 of *Ambu aView 2 Advance IFU* and *Ambu aView 2 Advance Reference Manual*, which is available on www.ambu.com.

This document contains information about:

- Prerequisites to establish the connection with aView 2 Advance.
- How to retrieve the MAC address and IP address of aView 2 Advance.
- Step-by-step troubleshooting tips to check when experiencing connectivity problems.
- Basic terminologies and how to find more information.

Notice that some of the troubleshooting tips described in this document can only be performed by trained IT professionals, with the experiences of IT infrastructure, firewall, and administrative tasks. Please also ensure you always follow the IT policy defined in your organization.

2. Supported capability for network connection

aView 2 Advance uses **Dynamic hostname resolution** and expects a **DHCP** and **DNS** service to be running to provide the hostname resolution. Notice that the device supports dynamic IP. Currently it **does not support static IP** address configuration.

The following tables covers supported WIFI and DICOM capability on the aView 2 Advance.

WIFI support	
Supported	NOT supported
WPA	WEP
WPA2	

DICOM support	
Supported	NOT supported
Export pictures	CMS (Cryptographic Message Syntax) encryption
Export videos	Modality worklist
	Import of pictures or videos

3. Prerequisites for PACS connectivity

aView 2 Advance supports DICOM application protocol to connect to a PACS server. The transport protocol of DICOM is based on TCP, via either ethernet or WIFI to the target PACS server.

In order to establish PACS connectivity, users must obtain the *port number*, *AE title*, and *hostname* of the PACS server on the network, and enter the information into aView 2 Advance. Notice that you need to login to aView 2 Advance either as a "admin user" or "service user" to enter the settings.

After login to aView 2 Advance, you can configure a new PACS server under **Settings > DICOM setup > Add new**. See Figure 1 PACS server configuration for an example.

- Enter the **PACS AE title** (PACS Application Entity Titles), which is an identifier for the PACS Server.
- The **“Host name”** can be resolved by either using a hostname of the PACS server such as “myhospital.pacs.server” or by entering the IP address of the PACS server.
- Enter the **“Port number”** of the PACS server. This info should be provided by your PACS server in order to setup the PACS connection with the aView 2 Advance. (Port number commonly used by DICOM are 104, 2761, 2762, or 11112).

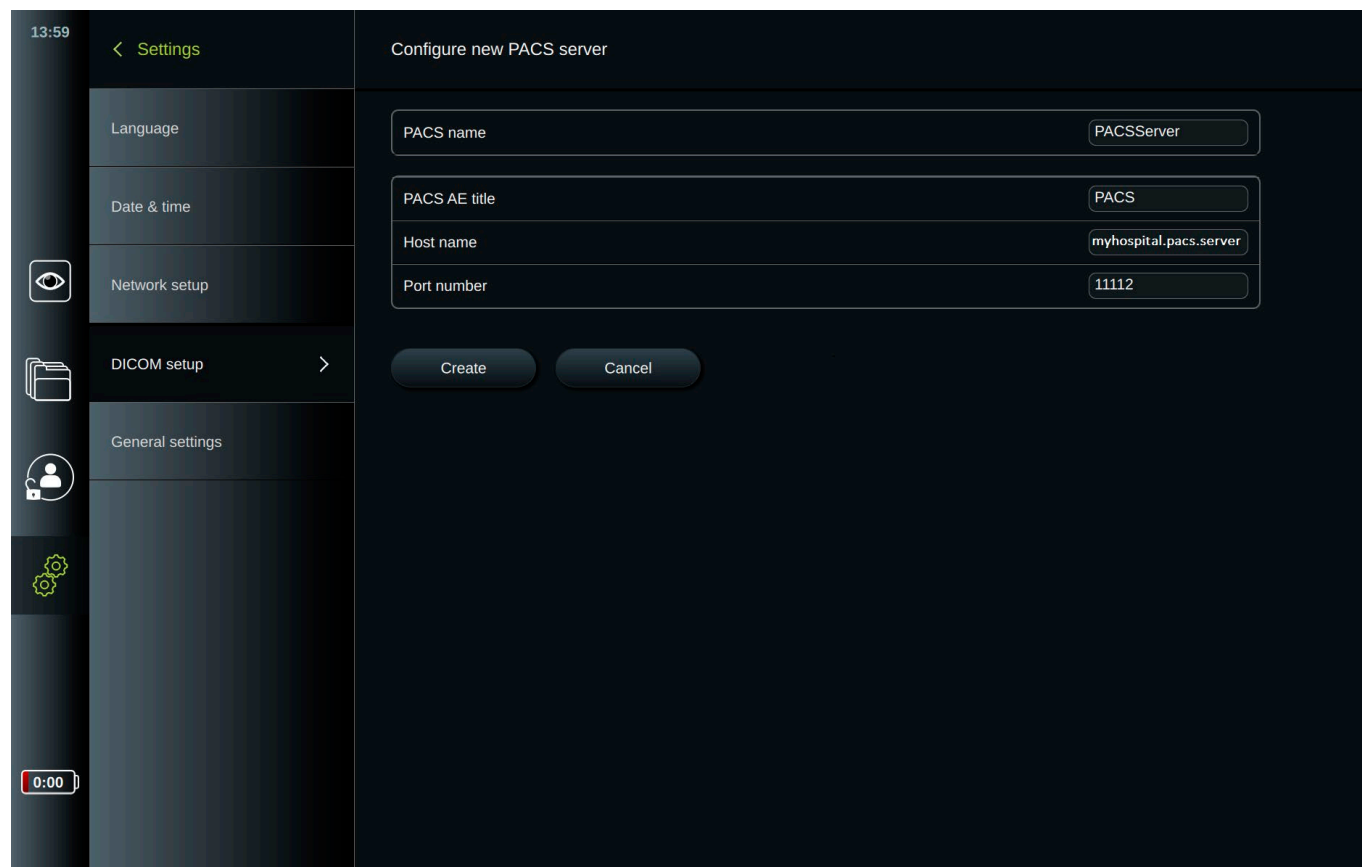



Figure 1 PACS server configuration

4. How to retrieve MAC address and IP address of aView 2 Advance

Turn on aView 2 Advance, then:

1. Login as an “admin user” or “service user”
2. Go to “Settings” 
3. Go into the settings submenu, select “About”
4. Go into the submenu “Device Info” under “About”
5. On the right information should be presented
 - a. Find the information tab “Network”
 - b. Identify Ethernet or Wi-Fi (depending on which interface is needed)
 - i. The MAC address is a 48-BIT address grouped into 6 octets.
Example: “3C:18:a0:13:a6:eb” in the sample screenshot below, highlighted in a red box.
 - ii. The IP address assigned by your network can also be found.
Example: 10.9.136.88, in the sample screenshot below, highlighted in a blue box.

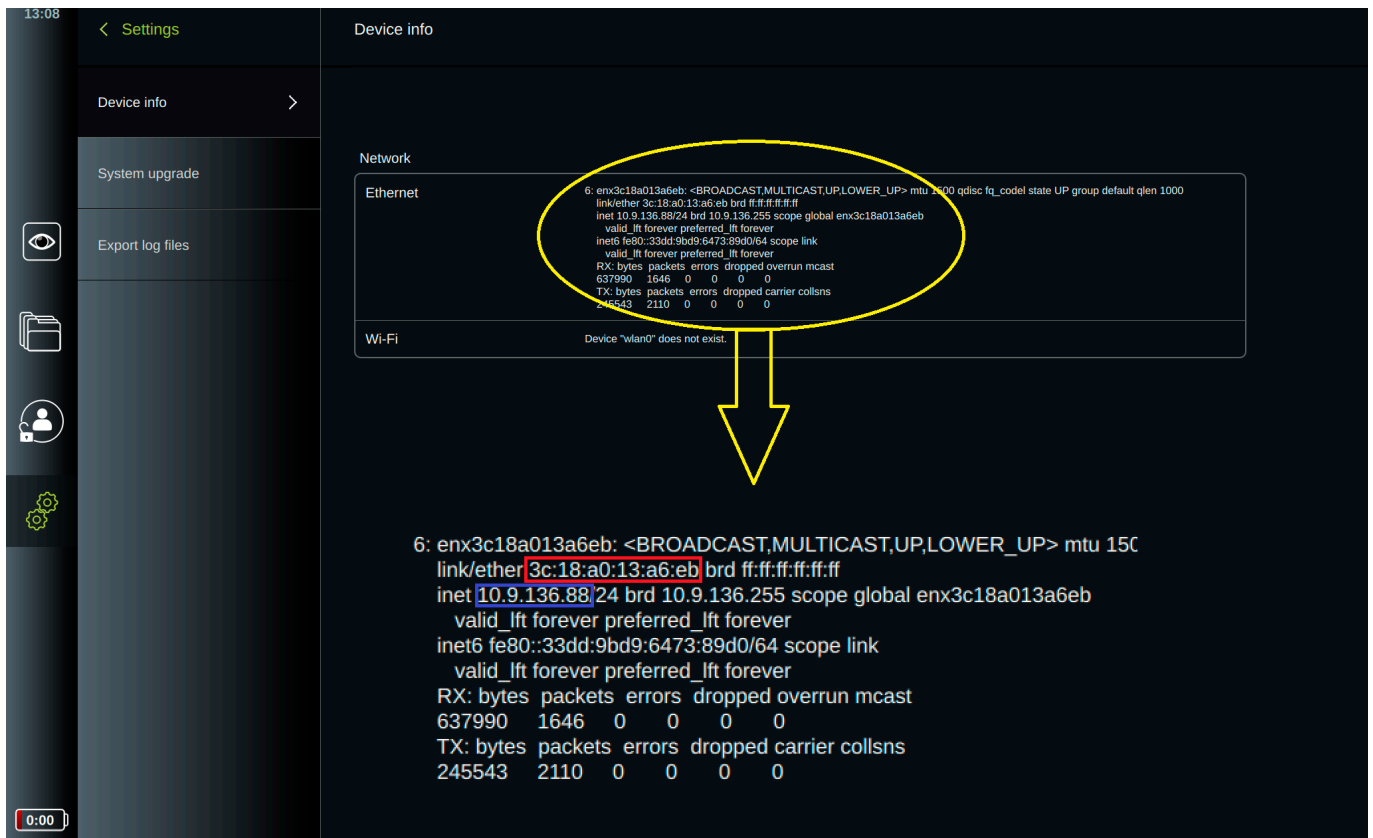


Figure 2 Retrieving MAC address and IP address of aView 2 Advance

5. Troubleshooting steps

1. Check connectivity by pinging the device (see IP address in "About" page)
2. If no connectivity;
 - a. If using Ethernet/LAN; check if the ethernet cable is RJ45 and attached properly.
 - b. If using WIFI; check if the WIFI network is correctly selected and the password is correct (go to **Settings** → **Network** setup).
 - i. While looking up the WIFI network, make sure the device has received an IP address from your network DHCP server. If it has not received an IP address, contact local IT support to make sure the device is properly installed on the network.
- c. Connect a laptop to the same network as the aView 2 Advance, and test the following on the laptop:
 - i. Check connectivity within one switch / Access-point region (LAN / WLAN).
 - ii. Check connectivity within one router region: If trouble check router rules and gateway configuration.
 - iii. Check if DHCP is working: Ipconfig /all for windows in command-line, check DHCP enabled for WIFI/ethernet and see if the device receives an IP address, as well as have a default gateway and DHCP server.
 - iv. Check DNS resolution:
 - Before debugging the DNS, check if the resolved (result) IP can directly be used.
 - Can nslookup (Command line tool) resolve the host name in the PACS host name field?
 - Consider using traceroute (tracert, windows) to trace when the connection is dropped (at what hop).
 - v. Check if another device on the same network is having the same trouble.
3. If the device has managed to connect to the network:
 - a. Go through step 2 with a laptop as well, but use tools like ICMP (pinging) the device and tracert to the device to trouble-find why it's not reaching the device for DICOM.

4. Check if your PACS system requires aView 2 Advance MAC address.
5. Check firewall configuration (Check if the PACS server port is open and if the PACS server is set to receive DICOM). Contact IT personnel for this.
6. **For IT personnel:** consider sniffing the packages using tools (eg. Wireshark) to figure out where the packages are dropped.

6. Glossaries

This section offers a more detailed view into some of the glossaries introduced in the quick steps and device expectations.

Hostname

A hostname is a named variable such as "google.com" which are associated with an IP address. A hostname is sent through a DNS server which (simplified) looks the variable up in a large lookup table returning the IP address to the device, this changing a named variable to an IP address is named DNS resolution when resolving a variable to an IP address.

(For IT personnel) If further details are needed, it could be considered to lookup the ARP (Address Resolution Protocol) communication, ARP is used to check for the symbolic named variable (hostname) from other devices in the network it's coupled up to. ARP tables are provided on the device, a switch and a router. Each ARP table holds a record of resolved hostnames, in rare cases it have been seen that the ARP tables can be corrupt, overpopulated or contain invalid data.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a central server, which provides individual devices with a configuration file, explaining; their relative IP address, their DNS server and how the network communication is configured.

The idea is that every device does not need to bookkeep their own configuration but can get it dispatched from a central source.

To check up on this look up if the Network Interface Card (NIC) is setup to enable DHCP, for windows this would be to investigate 'ipconfig /all' for the devices enabled NICs, for Linux it would be 'ip a'.

If there's problems with the DHCP server, contact IT.

Configuring DHCP daemons for Linux or DHCP servers for Windows are beyond the scope of this and should be handled by professional IT personnel only.

DNS

(Domain Name System) Server is a server with the central purpose of consuming request for resolving hostnames variables into IP addresses. Domain name spaces are hierarchical, an ARP communication request for resolving a hostname can travel through more than one DNS space, this depends on the infrastructure.

If a DNS server is present, but the hostname does not resolve contact IT personnel with this information as they're likely to debug the closest DNS server first, inform of the name of the specific hostname to investigate in which part of the DNS space hierarchy it's defined in.

Afterwards IT personnel can aggregate the hostname to a closer DNS node in the network to the device.

TCP

(Transmission Control Protocol) is a transport protocol used to transmit information in a controlled manner.

TCP won't be covered in detail here but are mentioned to inform which kind of transport protocol is used to transmit DICOM information from device to PACS server.

DICOM

(Digital Imaging and Communication in Medicine) is a NEMA standard for communicating medical images.

The DICOM standard is beyond the scope of this document but is covered to inform the user that the application layer protocol used is the DICOM format when exporting DICOM from the device to a PACS server.

Firewall

A firewall is a set of rules working on the active network in real-time preventing special packages to be carried over into the system.

A simplified view of firewalls is that they have rules for when they allow a package to come through, or when the package is dropped. This can be for protocols, IP versions and ports, more specialized firewalls also allow granularity for specific transport and application protocols.

Firewalls have a steep learning-curve and have a critical effect on infrastructure, a firewall should never be configured by personnel from outside the IT department or other professional IT personnel.

Configuring or modifying firewalls will thereby not be describe in this document, ask IT personnel to verify if the specific ports set in the PACS setting for Port Number is open for communication.

Router

A router is a level 3. layer network device, which from a routing table determines traffic delivery.

An explanation of routers is beyond the scope of the document.

The router can be configured as well, talk with your IT personnel to discover if there's any issues on the router-side, such as routing or firewall rules. Different manufactures such as Cisco provides their own operating systems such as IOS (Interactive OS), which can allow more detailed debugging, but logging into a router should only be done by professional IT personnel.

Check that the cables are correctly setup, ask IT personnel to login into the switch to verify that the configurations are the same as the one trying to use on the device.

Switch

Check that the cables are correctly setup, ask IT personnel to login into the switch to verify that the configurations are the same as the one trying to use on the device.

LAN

(Local Area Network) is the ethernet coupled local network, if you expect the device to be present on the LAN network make sure the cables are connected and if the ICMP (ping) can be send to/from different devices expected to be on the system.

VLAN

(Virtual Local Area Network) check the VLAN_TAG is correct via Wireshark and see if the Network Interface Card (NIC) is correctly setup for the VLAN, and what routes are provided for the VLAN, as well as the default gateway for the VLAN allow to reach the expected devices.

802.1Q (VLAN) in greater details are beyond the scope of this document, but it can quickly become very entangled for a larger network infrastructure, this topic has a steep learning curve, and if in doubt contact IT personnel about this.

WLAN

(Wireless Local Area Network) is provided by a local Access-Point, have IT personnel login to the AP to determine if the configuration is the same as the expected setup for the device.

WIFI

The supported WIFI for the aView 2 Advance and aBox 2 is: 802.11ac/a/b/g/n.

The WIFI requires 802.11i WPA/WPA2. Lower grade security or older legacy formats such as WEP is not supported.

The WIFI supports 802.1X EAPOL enterprise, but the infrastructure must support their own RADIUS server (or DIAMETER, etc.).

If connectivity is poor, consider placing aggregate access-point to amplify the signal or consider the material in the walls / room layout. Recall that WIFI is radio technology, in which 802.11ac/a/b/g/n is regulated by Radio Directives / Regulation authorities, the radio waves must be proper dissipated and transmitted through the rooms / area to be have a good connectivity, any technology prone to interrupt radio will therefore also reduce WIFI performance.

Consider debugging the WIFI by using a mobile device such as a phone or a laptop.

Have IT personnel log into the access-point or router to see if the WIFI configuration is setup as the device expects it to be (SSID, password, etc.)

WPA/WPA2

WIFI Protected Access I or II are the 802.11i standards for secure transmission for WIFI using the WPA-personal with a WPA-PSK (Pre-Shared-Key), which are usually seen on local networks. WPA-Enterprise uses EAP (Extensible Authentication Protocol) and EAPOL (EAP On LAN) through an enterprise authentication server such as RADIUS.

For reference WPA/WPA2 uses TKIP (WPA) and CCMP (WPA2) as encryption protocols.

The TKIP and CCMP provides channel / connection based encryption, like secure channel on a regular radio transmitter, but does not provide encryption within the communication, meaning that if an individual is authenticated to be on the WIFI, the datagrams transmitted inside the WIFI is not encrypted (per default).

MAC address

From the IEEE 802 standard the MAC address is a unique identifier for a hardware component, such as a network interface controller (NIC), it's used to identify the interface on the broad network.

Usage beyond this and deeper explanation into MAC addresses are beyond the scope of this document, consult the IEEE 802 standard for more information.

 **Ambu A/S**

Baltorpbakken 13,
DK-2750 Ballerup, Denmark

T +45 72 25 20 00

ambu.com