Laerdal Network Requirements

Document name	Laerdal Network Requirements
Revision	L
Revision date	31-Jan-2022
Internal reference	00066667
Public reference	https://laerdal.com/no/services-and-programs/technical-services/network-services/network-requirement-service-documentation/

1 Introduction

This document describes the main settings of the network environment required by Laerdal equipment to perform medical simulations. It includes the specifications of the network interfaces of Laerdal equipment.

A Laerdal Medical simulation session consists of medical procedures performed on a *manikin* patient (i.e., Laerdal human-looking computerized equipment) and analysis of the symptoms and results of the simulation on computers and tablet devices running other software components of Laerdal simulation ecosystem.

In addition, Audio/Video equipment and video processing software can be used to record, store and play simulation sessions for training and other educational purposes.

The manikins and the auxiliary simulation devices exchange data and commands over a local area network (LAN).

Short-range device communication and synchronization over Bluetooth technology is automatically configured and handled by the simulation devices.

In addition, Laerdal's products require a connection to Internet for software maintenance, security upgrades, telemetry reporting, use of other cloud services and remote technical support.

The remaining sections of the document discuss the architecture, interfaces, protocols, IP addressing, security policies and other settings of the network required by the Laerdal Medical simulations environment.

1.1 Bandwidth assumptions

Laerdal devices require a minimum 1 Mbps bandwidth capacity across the network used for simulations. During different phases of application execution devices may produce peaks of traffic exceeding 1 Mbps.

Simulation setups using SimCapture, specifically with video, will demand higher bandwidth. Each SimCapture device requires a 1 Gbps connection over a cabled local-area network and a highspeed Internet connection.

2 High-level network architecture

Figure 1 shows the high-level architecture of a network which provides local and Internet connectivity for Laerdal simulation equipment. The simulation network is a separate subnet inside customer's enterprise network. Certain Laerdal simulation applications require access through the enterprise network over Internet to Laerdal cloud and third-party cloud services.

Figure 1: The high-level architecture of a simulation network
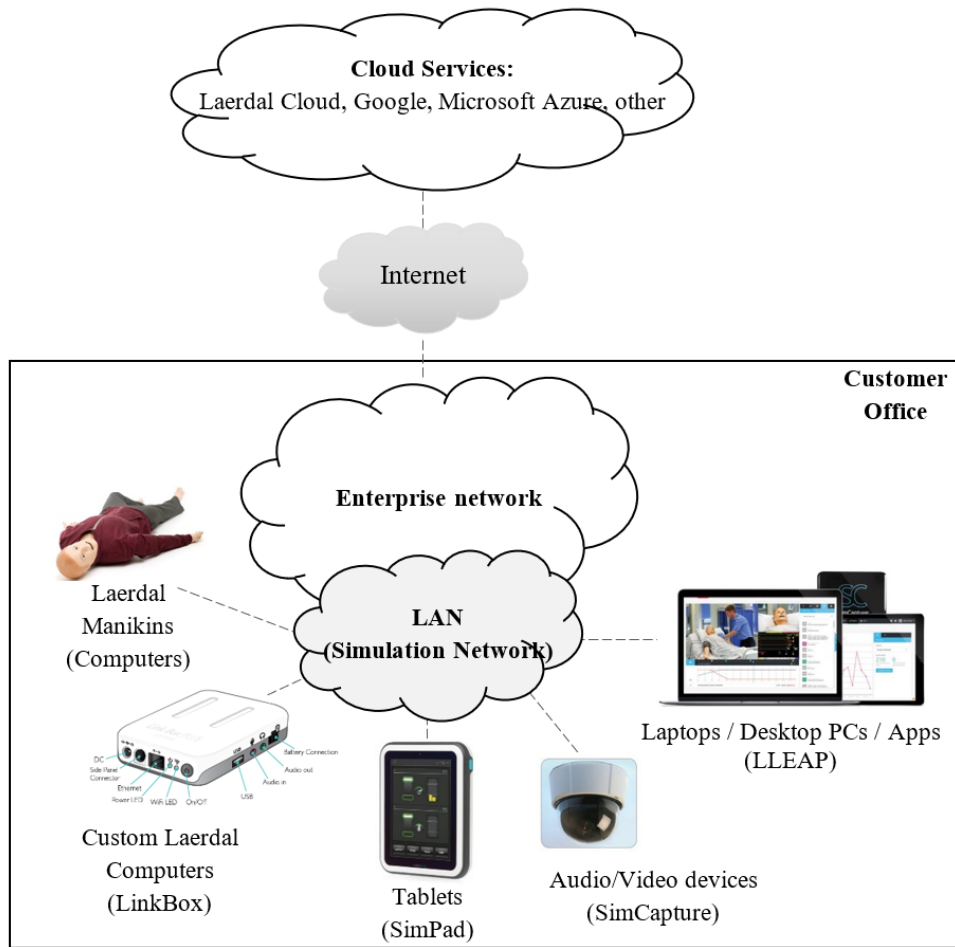
Possible architectures for the local-area network used to connect the simulation equipment are shown in the following drawings.

Figure 2: Architectures of the local simulation network
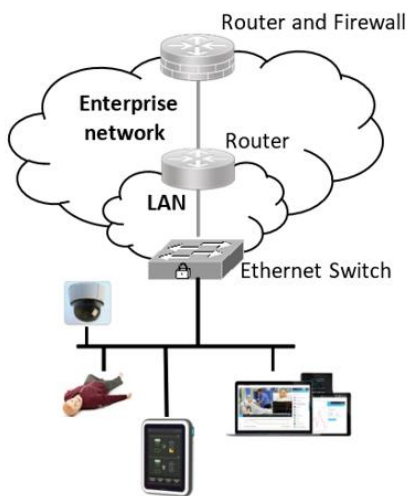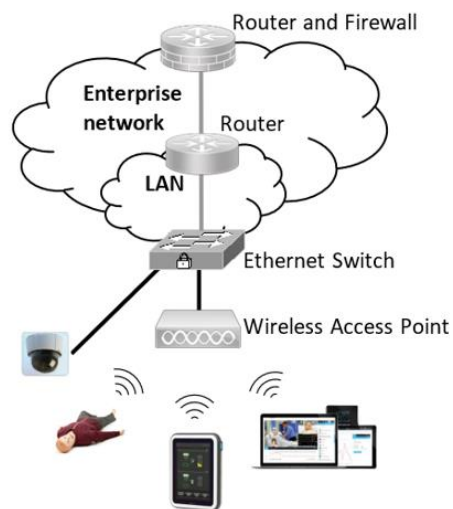

Figure 2.a: Ethernet wired LAN   Figure 2.b: Wireless LAN and wired LAN

All devices used in a simulation must be connected to the same subnetwork.

3   Devices Connectivity

3.1   Local cabled network

The manikins and other Laerdal simulation devices are equipped with Ethernet network interface cards (NIC) which can be used to connect the devices to a local-area network switch or hub using minimum category 5 UTP (CAT5) copper cables.

Figure 3 shows the side panel found in several manikin devices which includes an Ethernet interface, a power on/off button and a power plug. The side panel provides external access to manikin's internal operating system (Windows or Linux) for network configuration and applications traffic.

Figure 3: Manikin's side panel with RJ45 port
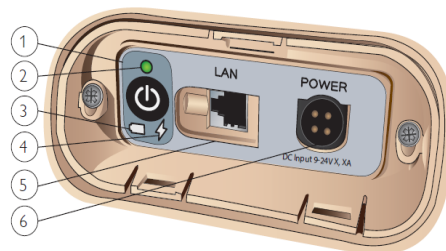
The NIC interfaces of the simulation devices are compatible with 100BASE-TX standard and support maximum 100 Mbps. The interfaces are configured to automatically negotiate the speed and duplex mode settings.

The computers systems used for SimCapture have 1 Gbps interfaces (1000BASE-T).

If the enterprise network uses virtual LAN (VLAN) capability for optimization and flexibility, then all Laerdal equipment must be connected to network interfaces allocated to the same VLAN identifier (VLAN ID).

The following subset of Laerdal provided devices must always be connected to the network over UTP cables, not over wireless connections:

- Axis cameras;
- SimCapture nodes;
- Axis audio module;
- Axis Analog to IP Encoders
- Symetrix DSP;
- Stewart Amp;
- JTECH;
- Control/Debrief/Exam Workstations;
- SimCapture UltraPortable;
- ASL 5000.

3.2   Local wireless network

Several Laerdal simulation devices can be connected to an enterprise network over wireless local-area networks (WLANs) as shown in Figure 2.b.

The WLAN devices used by Laerdal devices are compatible with the protocol specifications of the Wi-Fi standards (802.11).

The recommended topology for the Wi-Fi simulation network is the network infrastructure mode (i.e., BSS mode). In the Wi-Fi architecture Laerdal devices are clients of the Wi-Fi network.

Laerdal manikins have inside their torso installed a wireless communication equipment which can be configured locally over an RJ45 port connection. Dependent on the manikin model, these Wi-Fi network devices can be a router, a dongle or a built-in circuit module.

The following table lists the main features of the wireless devices used by Laerdal simulation equipment:

Wi-Fi	Compatible Simulation Devices
2.4-Ghz channels 1-11	All
5-Ghz channels 36, 40, 44, 48	All devices except: SimPad or LinkBox Classic based models (Some devices may support additional 5-Ghz channels)
Release 4 (Wi-Fi 4, 802.11N)	SimPad Plus, LinkBox PLUS, SimBaby, SimNewB, Nursing Anne Simulator, SimMan 3G with WRN500 router, Laerdal provided computers
Release 5 (Wi-Fi 5, 802.11AC)	SimMan 3G model equipped with a Wi-Fi dongle (LM Technologies dongle)
WPA-2 Personal or Enterprise[1] Encryption	All. Some older manikin models require a hardware upgrade.

3.3   Communication over Internet

3.3.1   Connectivity to cloud services

The simulation network should be connected to Internet for device and application communication with cloud services.

3.3.2   Connectivity for Laerdal technical support

For technical support, the enterprise customer shall provide VPN access to the simulation network and to the network used by the Audio/Video (AV) simulation equipment. The simulation network shall be configured as per the requirements described in this document.

---

[1] Requires LLEAP or SimPad PLUS using software version 7.3.0 or newer.

The VPN connection for the Audio/Video network must have an IP address in the same subnet with the AV equipment (i.e., "Dante VLAN" described in chapter 6 of this document).

4   IP addressing

The Laerdal devices used in simulations must be assigned private IPv4 addresses. All allocated IP addresses must belong to the same subnet range to facilitate device discovery and stability of the simulation session.

The following range of IP addresses which are used internally by Laerdal manikins should not be used in the simulation network (wired or wireless): 192.168.168.*.

The allocation of the IP addresses should be performed by an enterprise DHCP server, which should reserve permanently the addresses to the simulation devices.

The Audio/Video equipment related to SimCapture must be allocated static IP addresses.

5   Network services, protocols and applications

5.1   Devices and services discovery

Laerdal applications use Bonjour services (multicast Domain Name Services – mDNS – and DNS Service Discovery – DNS-SD) and a proprietary method (named hereafter 'Legacy') to discover manikins, simulation devices, services and other computers connected over the simulation network.

The Bonjour services must be enabled in the enterprise network devices (wireless routers, wired routers, firewalls, any network devices used in the simulation network which block the Bonjour services).

Laerdal Learning Application (LLEAP) can use both methods for device discovery - Bonjour and 'Legacy'. Only Bonjour is supported for the discovery of Laerdal LinkBox devices while only Legacy is supported for updating SimMan3G simulators.

5.1.1   Discovery using Bonjour services

LLEAP application uses mDNS and DNS-SD to publish and discover services over the network. These service discovery technologies are known under different names based on their implementation name: Apple Bonjour, Avahi, zero-configuration networking or zeroconf.

Bonjour sends mDNS messages as multicast UDP packets to IPv4 address 224.0.0.251 using UDP port 5353. Each device uses Bonjour to publish its relevant information using a predefined service name which allow other devices (clients) to discover them.

The following table lists the Bonjour service names defined by Laerdal for LLEAP, SimPad and LinkBox devices.

Service name	Device/Application	Description
_simbridge._tcp	SimPad Link Box	Used by LLEAP to connect to Link Box
_simmonitor._tcp	SimPad Link Box	Used by Patient Monitors to connect to Link Box when running on SimPad
_simlink._tcp	SimPad Link Box	Used by SimPad to connect to Link Box
_simse._tcp	LLEAP Simulation Engine	Used by LLEAP and Patient Monitor to connect to a Simulation Engine (SE). SimMan 3G manikins run the SE in the manikin itself. For all other manikins, the SE runs on the PC running LLEAP application.
_simvca._tcp	Voice Conference Application (VCA)	Used by VCA to connect to another VCA, typically running inside a 3G family simulator, but also on a PC running with a LinkBox type simulator
_simventures._tcp	SimView/Session Viewer	Used by LLEAP and SimPad to connect to a SimView Server or Session Viewer
_http._tcp	Screen Capture	Used by SimView Server or Session Viewer to connect to a screen capture service
_workstation._tcp	SimPad update service	Used by LLEAP to update software on SimPad
_ssh._tcp	LLEAP/SimPad Link Box update	Used to update SimPad and Link Box
_lleaphost._tcp	LLEAP PC (IA, PM)	Used to configure PCs
_ctgserver._tcp	SimMom LLEAP PC (IA, PM)	Used to find the server for Cardiotocography curves
_lleapsimupdate._tcp	SimMan3G-family	Used to find the SimMan3G manikin update service

Note that, for certain network equipment manufacturers, the above service names must be added, configured and enabled in the network devices following the instructions included in the vendor manuals. Different equipment vendors require different procedures and settings to define the Bonjour service names.

5.1.2   Discovery using Laerdal 'legacy' method

The LLEAP, Ingmar Lung and VitalsBridge systems use broadcast and multicast UDP for device discovery. Legacy discovery is required to update SimMan3G simulators.

5.2   Application TCP/UDP ports and network security policies

This section describes the protocols and the ports used by Laerdal simulation devices which must be considered when implementing the security policies in the enterprise network.

The main protocols used by Laerdal systems inside the simulation network are IP, TCP, UDP, IGMP, NBNS, DHCP, DNS, SMTP, RTSP, SSH, WebRTC, HTTP and HTTPS.

The traffic generated by Laerdal devices flows within and between two main network zones as shown in Figure 4.

Figure 4: Traffic flow zones
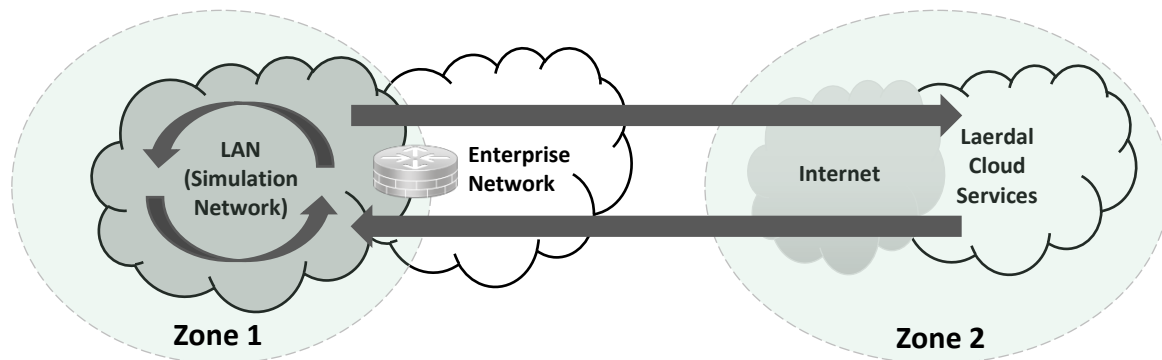
The security control measures (access control lists, ACLs, and firewall filtering) implemented in the network equipment in Zone 1 and Zone 2 shall not restrict the traffic flows and shall not block the TCP/UDP ports used by the simulation devices and applications.

Sections 5.2.1 and 5.2.2 describe the ports used by Laerdal devices and applications inside Zone 1 and between the two zones, respectively.

5.2.1   Traffic inside the simulation network

The following table describes the ports used by Laerdal applications inside Zone 1 (that is Zone 1 to Zone 1 traffic).

Protocol	Ports	Devices	Description
TCP	22	SimPad, LinkBox, Client PC[2]	Rsync, WinSCP and sFTP used to transfer files to and from the client and the manikin
TCP	80	SimMan3G simulators SimView SimCapture On-Premise	
TCP	443	SimView SimCapture On-Premise SimCapture Cloud	Web application access via a browser Local automated health checks internally and outgoing communication

---

[2] Client PCs are computers or laptops running simulation components of the Laerdal Learning Application (LLEAP) such as: Patient Monitor, Simulator Firmware and Network Wizard, Debrief Application.

Protocol	Ports	Devices	Description
TCP	554	SimCapture On-Premise SimCapture Cloud	Internal Audio and Video communication between the
TCP	1935	SimCapture On-Premise	Legacy Flash Streaming (obsolete as of January 2021)
TCP	2000-2001	SimPad Resusci Anne Plus	Serial data communication of the ventilation and compression performed on the manikin used to calculate QCPR score
TCP	2813	SimCapture On-Premise	For use with the OSCE SimCapture CCM Exam System
TCP	3389	SimMan3G SimCapture	Remote Desktop
UDP	3478	SimCapture Cloud	WebRTC signaling for live videos for outgoing internet access and between subnets
UDP	5353	All	Bonjour / mDNS / DNS-SD, zeroconf discovery Udp://224.0.0.251:5353
TCP	5671	Client PC	Data Analytics
UDP	6681-6682	SimMan3G simulators Client PC Debrief PC SimView SimCapture Cloud SimCapture On-Premise	For the Patient Monitor Remote Screen Capture Software
UDP	6797-6798	SimMan3G-family Client PC	Used by Laerdal 'legacy' discovery as described in section 5.1.2
UDP	7557-7558	Linkbox simulators	Laerdal VS params and unified params Build on protocol buffers message subscription service
UDP	8935	SimCapture On-Premise	Live WebRTC Viewing
TCP	9897	SimMan3G-family	Configuration of SimMan 3G simulator
TCP	9898	Simulator PC Client PC	Voice conferencing control
UDP multicast	11000-11006	Simulator PC Client PC SimPad, LinkBox	Voice conferencing. Binary data stream of data using OPUS encoder/decoder
UPD broadcast	13000	Simulator PC Client PC	Legacy alive data

Protocol	Ports	Devices	Description
TCP	14997	Client PC VitalsBridge	VitalsBridge Communication
UDP	14998	Client PC VitalsBridge	VitalsBridge advertising
UDP multicast	15000-15007	Simulator PC Client PC	Alive data
TCP	15020-15024	LinkBox, SimPad Simulator PC Client PC	Configuration and control, file transfer. Used to communicate with Patient Monitor application using webservice (wsdl) protocol
TCP	15029	Simulator PC Client PC	Computers used in simulation
UDP	15030-15033	Simulator PC Client PC	CTG server stream for SimMom
TCP, UDP	21935	SimCapture On-Premise SimCapture Cloud	Live WebRTC Viewing
UDP	54915, 52734	Client PC ASL5000	ASL 5000 device discovery
TCP	55195, 52719	Client PC ASL5000	ASL 5000 device control and data

5.2.2   Traffic to the cloud services

The following table describes the ports used by Laerdal devices and applications transferring traffic between Zone 1 to Zone 2.

The ports listed in this table shall be <u>outbound</u> open in the security devices sitting on the communication path from Zone 1 to Zone 2.

Protocol	Ports	Target URL	Function	Data
TCP	443	*.laerdal.com	Online activations of licenses and Laerdal products. It is required by Laerdal products to work. Software updates for Laerdal products downloaded manually.	License keys information – REST api Installation files for miscellaneous products.
TCP	80, 443	cdn.laerdal.com laerdalcdn.blob.core.windows.net	Software updates for LLEAP and SimPad. Detection of needed software updates.	Installation files / executables for Windows and Linux
TCP	80, 443	scenariocloud.laerdal.com	Online Laerdal Scenario Cloud synchronization	Zip-archives containing xml and media files

Protocol	Ports	Target URL	Function	Data
TCP	443	laerdalmedicalb2c.b2clogin.com	Laerdal Active Directory B2C login	Verification of user credentials
TCP	443	gigya.com	Identity management required for Laerdal cloud services (Scenario Cloud, Laerdal Connect)	Verification of user credentials
TCP	443	api.ipify.org	IoT external lookup, LLEAP and SimPad	URL Redirects & Lookup of geolocation data about users.
TCP	25	smtp.gmail.com	LLEAP and SimPad feedback forms, errors reporting and log files for debugging. Users can trigger an e-mail to be sent to Laerdal with crash logs and other forensic information for troubleshooting system errors.	E-mail
TCP	443	*.teamviewer.com	Remote desktop application used for remote support. Must be initialized by user on the local computer.	See www.teamViewer.com
TCP	443	*.simcapture.com	SimCapture Cloud debriefing and video recording services	Video streams, debrief data (zip archive containing xml, media, and other files)
TCP	443	*.amazonaws.com	SimCapture uploading of the recorded video files	Video files recorded on the local SimCapture Node/Server
TCP	80, 443	*.SonoSim.com	LLEAP software updates and content for SonoSim Ultrasound simulator	Windows installation files + content in the form of multimedia files.
TCP	443	SonoSim.auth0.com	LLEAP SonoSim Ultrasound Simulator authentication server	Device (probe) ID to authenticate use
TCP	443	update.VitalsBridge.com	LLEAP software updates for VitalsBridge	Installation files / executables
TCP	443	www.ingmarmed.com	LLEAP software updates for Ingmar ASL 5000 ventilator	Windows installation files / executables
TCP	443	*.googleapis.com *.gstatic.com	Google Telemetry data Anonymized data (no personal information) used for	Telemetry data

Protocol	Ports	Target URL	Function	Data
			improving our products, preventive maintenance etc.	
TCP	443	applicationinsights.azure.com applicationinsights.microsoft.com services.visualstudio.com	LLEAP and SimPad, MS Application Insight Telemetry data. Anonymized data (no personal information) used for improving our products, troubleshooting, preventive maintenance etc.	Telemetry data
TCP	443	servicebus.windows.net	Microsoft EventHub Telemetry data. Anonymized data (no personal information) used for improving Laerdal products, troubleshooting, preventive maintenance etc.	Telemetry data
UDP	3478	*.amazonaws.com *.simcapture.com	SimCapture Cloud	WebRTC signaling for live videos for outgoing internet access

6   Appendix A: High-level requirements for SimCapture network

The network for the SimCapture Cloud with Advanced Audio Package and with either the Simulation Center control room or headphone station package uses a technology named Dante networking which should be configured on a separate virtual LAN network (Dante VLAN) which connects all Digital Signal Processors (DSP) and Dante amplifiers for real-time audio transmission without the need to run extra audio cabling. This network is used for paging also.

The communication path for audio services starts from the control station microphones and continues as follows: -> DSP -> in-room Dante amplifiers -> speaker. The DSP processes the analog microphone signal and transmits it over UDP to the amplifiers, which then sends the amplified analog signal to the speakers.

This low-latency network can be used also for audio monitoring by transmitting a copy of the audio signal from the room's microphones to the control station headphones.

> The Dante VLAN is only required when SIMULATION CENTER control room(s) or headphone station package(s) are purchased.

6.1   Audio/Video devices on Dante VLAN

Device	IP Address	Network Type	Notes
In-Room Stewart Amplifier	Static IP	PoE+	Not compatible with Cisco uPoE.

Device	IP Address	Network Type	Notes
In-Room Symetrix DSP Ethernet Port 1	Static IP	PoE+	Not compatible with Cisco uPoE. This is configured on the Dante VLAN if a control station or headphone package exists.
In-Room Symetrix DSP Dante Port 1	Static IP	Ethernet	
Control Room Symetrix DSP Ethernet Port 1	Static IP	PoE+	Not compatible with Cisco uPoE.
Control Room Symetrix DSP Dante Port 1	Static IP	Ethernet	

6.2   Requirements for Dante VLAN switch

Configuration Setting	Value	Notes
Energy Efficiency Ethernet	Disabled	This will cause the DSP and Amp devices to go offline.
IGMP Snooping	Disabled	Must be disabled on the Dante VLAN only. Dante uses Precision Time Protocol to sync clocks. We use unicast traffic, not multicast.
Packet filtering	Disabled	This will cause latency.
VPN	Dante VLAN	The IP assigned after a VPN connection is made must be on the Dante VLAN. This allows for Dante Controller to diagnose/update the Dante configuration.
*We highly recommend all devices on the Dante VLAN to be on the same physical switch.		

The above settings are required to avoid audio clicks/pops and drop-outs of the audio communication.

6.3   Power over Ethernet

SimCapture AV equipment requires Power over Ethernet (PoE or PoE+). Note that Symetrix DSP cannot use Cisco's uPoE (Universal Power over Ethernet).