Helvar

HELVAR (IP) MANAGED NETWORK + FAQs

Dit document kan geraadpleegd worden als er problemen of vragen zijn met betrekking tot een DALI netwerksysteem.

Helvar in Nederland
Lighting Controls B.V.
Ambachtstraat 3
4143 HB Leerdam
Nederland

T +31 (0)345 633679
E info@helvar.nl
I www.helvar.nl

Helvar in België
Lighting Controls BVBA
Industriepark Noord 27
9100 Sint-Niklaas
België

T +32 (0)37 77 81 77
E info@helvar.be
I www.helvar.be

e20218

1. Managed Network FAQs

This section is to address some of the common concerns and issues that IT managers have relating to a distributed Helvar Lighting Router system .

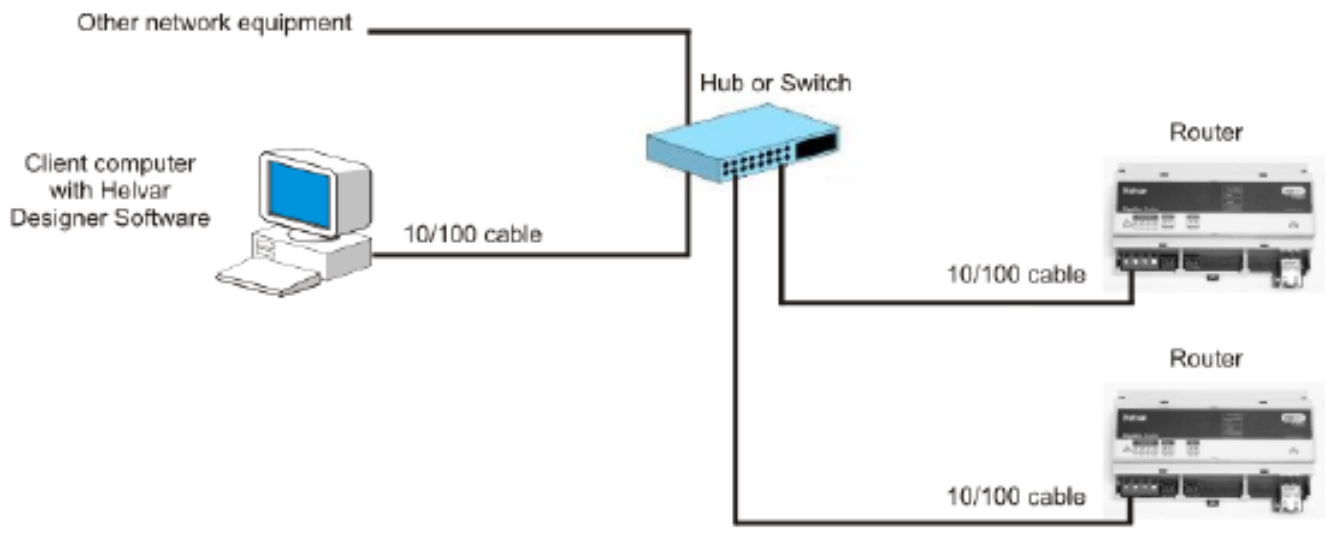
A lighting system may be small and localized on a single network switch or it may be large and distributed around a building on many network routers. In either case all of the Helvar Lighting Routers in the system must be able to discover and communicate to each other and also to one (more) client PC's running the Helvar Designer programming software.

All the lighting system devices transmit a discovery message using either UDP Broadcast or UDP Multicast. This is configurable in the Helvar Lighting Routers, appropriate to the installation requirements.

During system operation either UDP Broadcast or UDP Multicast messages are used to configure the Helvar Lighting Routers and then maintain synchronisation. Action and event communications will then use acknowledged UDP messages between Helvar Lighting Routers to invoke functional responses, such as scene recalls.

Helvar application software (including but not limited to the Helvar SceneSet Android/IOS App, Tridium Niagara Driver, Touchstudio, uSee, 435 BACnet Gateway) or Third party devices and systems may also query and control the Helvar Lighting Routers with the simple published HelvarNET protocol using either TCP or UDP. UDP and TCP ports are required to be opened if using HelvarNET as the routers use these port to send messages between themselves. Refer to the port summary table later in this section.

Additionally, any Helvar Lighting Router in a system may also be used to transmit data packets to third party devices (such as Audio Visual Systems) using either TCP or UDP. UDP or TCP ports will be required to be opened if using HelvarNET. Refer to the port summary table later in this section



Typical Helvar Lighting Router Network Rev 1

2. IP Adresses

It is recommended that all Helvar Lighting Routers and clients in a system must have the same prefix. The IP address prefix is defined by the first two octets of the address, i.e. for the IP address 10.254.1.1, the prefix is 10.254. The prefix can be set to almost anything, provided that the addresses comply with the rules of the Internet Protocol (IP).

3. Discovery – Broadcast/Multicast

Components in a lighting system discover one another by transmitting and receiving either broadcast or multicast packets. All Helvar Lighting Routers on the network, and any client PC's running the Helvar Designer software, are required to transmit and receive these discovery packets.

If the network is a layer 2 network, the client and all Helvar Lighting Routers will receive the UDP broadcast message.

If the network is a layer 3 managed network, the UDP broadcast may not be permitted through managed switches and therefore, the Helvar Lighting Routers also allow for the discovery message to be transmitted via UDP multicast. The type of protocol used for transmitting the discovery message can be set in the properties of the relevant Helvar Lighting Router. This also allows each to be enabled or disabled.

Broadcast Discovery Address
The default Broadcast Address is 255.255.255.255 this may be changed providing that the address complies with the rules of the Internet Protocol (IP) and IT structure being implemented on the network. The UDP Broadcast Discovery message uses socket port 60000 that cannot be changed and any network port restrictions would have to be opened to allow communication via this port.

Multicast Discovery Address
The default Multicast Address is 239.0.0.1 but may be changed in the following range from 224.0.0.0 to 239.255.255.255 providing it complies with the IP and IT structure. The UDP Multicast Discovery message uses socket port 60009 that cannot be changed and any network port restrictions would have to be opened to allow communication via this port.

4. Event communications – UDP

Helvar Lighting Routers communicate system trigger information such as scene recalls with one another by transmitting and receiving acknowledge UDP packets on ports 60004 & 60007 . Depending on the configuration, Helvar Lighting Routers will use Rev 1

the cluster comms port (in single cluster the default is 60005) within the same cluster and a cross cluster port 60006 to send messages to other clusters.
Any client PC's running the Helvar Designer software are also required to also transmit and receive acknowledge UDP packets. Communication from the routers to Designer uses the TCP Listener Port 60002 and communication from Designer to routers use the acknowledge UDP via the cluster master.

5. Helvar Application software or Third party communications (via HelvarNET)

The Helvar Application software or third-party device must be able to instigate a TCP connection with a Helvar Lighting Router or send UDP messages to a Helvar Lighting Router.

To establish a TCP connection and therefore communicate with the Helvar Lighting Router, it is required to connect to TCP listener port number 50000 that cannot be changed and any network port restrictions would have to be opened to allow communication via this port.

If using a UDP connection to communicate with the Helvar Lighting Router, the port number 50001 is used.
It is recommended to use UDP for HelvarNET messages.

6. Helvar Lighting Router controlling Third party devices

The Helvar Lighting Router in a system can also be used to transmit data packets to third party devices (such as Audio Visual Systems) using either TCP or UDP.

To send a TCP message from the Helvar Lighting Router to a third-party device, the Helvar Lighting Router connects to a listener port provided from the third-party device. It is recommended that this listener port is in the range from 49152 to 65535. If using UDP there is no requirement to connect to a listener port.

The IP address and port (if required) of the targeted third-party device is configured in the Helvar Lighting Router along with the message being sent in line with devices communication protocol.

There is a limitation of 40 bytes per packet to be sent regardless of the method used.

7. Helvar Lighting Router Port Summary

The Helvar Lighting Routers in a system along with any client PC's with Designer installed will require the following ports to be unrestricted within the network to allow full communication where noted option points are shown. Rev 1

Description	Port	Required
UDP Discovery (Broadcast)	60000	Yes
TCP Listener	60002	Yes
UDP Message	60004	Yes
UDP Message Local Cluster (default Cluster Comms Port)	60005	Yes – Single Cluster
UDP Message Cross Cluster	60006	Yes – Multi Cluster
UDP Acknowledge	60007	Yes
UDP Diagnostic	60008	Yes
UDP Discovery (Multicast)	60009	Yes
UDP Message Local Cluster (User Assigned Cluster Comms Port)	60100 - 65535	Yes – Multi Cluster
HelvarNET TCP Listener	50000	Optional
HelvarNET UDP Message	50001	Optional
HelvarNET UDP Message Internal (Broadcast)	50002	Optional
HelvarNET Query Interval	50003	Optional
3rd Party Listener Port (TCP or UDP)	49152 - 65535	Optional

8. FAQ - Integration issues

Q. How will the Helvar Router solution tie in with my current IT infrastructure?
All of Helvar Router products can co-exist on your IT infrastructure. Designer will most likely be on a computer that is already a member of your Domain or Active Directory, This will appear in the Network Neighbourhood and can be browsed. A connection to Helvar Routers to allow configuration or reprogramming can only be made via Designer.

Security access to the Helvar Router system is provided by local authentication on the PC Workstation with Designer installed, with password access integral to the software providing different levels of user control.

9. FAQ - Network issues

Q: What does a system of Helvar Routers and Designer do to my network traffic and bandwidth?
There are three categories of traffic that will affect network bandwidth:
• **Configuration Traffic** – This is traffic that is associated with the initial setup and commissioning of a Helvar Router implementation. During system commissioning bandwidth varies depending on the number and type of objects being configured.

• **Real Time Data/Router Traffic** – This is data that is transferred between Helvar Lighting Routers for operational purposes. Traffic consists of internal m onitoring / synchronization data and event communications such as scene recall or constant light events. On a 100MB network the typical requirement for background communications is minimal Rev 1
The bandwidth requirement can vary dependent on the nature of the events, for example if the scene recall needs to be transmitted locally on the Helvar Lighting Router only or across the network to additional Helvar Lighting Routers.
In the case of an active constant light function that needs to transmit across the network from Helvar Lighting Routers, bandwidth requirement would increase during data transmission but would still have little or no impact on the overall bandwidth requirement.

• **HelvarNET Traffic** – This is data that is sent during the connection of a Helvar software application such as the Tridium Driver or by a 3rd party device or application.
Bandwidth varies depending on the number and type of connections and how they are configured for use.
Your Helvar Systems Integrator will work with you to properly configure your system to ensure minimal impact to your networking environment.

Q: Does Helvar Router Systems support DHCP?
DHCP is not supported by Helvar Router Systems

10. FAQ - Security issues

Q. How will Helvar systems tie in to my security policy?
PC's with Designer installed can support your current policies for security access. Access to the Helvar routers for programming and configuration can only be achieved by use of the Designer software. Designer software has local password protection for specific user rights.

Q: How do I protect someone from hacking into my Helvar Router system?
Good physical security of the entire Helvar system is important. Do not allow unauthorised access to the routers or the network. Communication is not encrypted.
Using a VLAN is highly recommended when sharing a network with other services. This will prevent access to the Helvar system, as well as minimising network traffic being processed by the routers.
Our software and Helvar Lighting Routers uses a proprietary protocol running on top of TCP/IP.
There is however a published protocol called HelvarNET that would allow a user should they have access to the physical network to transmit HelvarNET commands to the system. These commands generally allow actions such as scene recalls to be carried out or queries to be requested such as device output information but do not allow for system configuration.

Q: How secure is the Helvar systems? Do any existing IT security measures have to be compromised to allow the Helvar system to work?

The Helvar Lighting Routers can only be accessed from a PC with Helvar Designer installed. If you need to access the Router system from over the Internet or via a VPN connection you will need to use one of the following methods: Rev 1
A. A remote connection software such as PC Anywhere, TeamViewer or UltraVNC with their associated security requirements being met.
B. A secure VPN Tunnelling solution/ device such as a Tosibox

11. FAQ - Interconnectivity issues

Q: How do we access a Helvar Router over the Internet/VPN?
There is no direct connection available to the router via Internet/VPN. Connection to Helvar routers is only available from a PC with Designer installed. If you need to access the Router system from over the Internet or via a VPN connection you will need to use one of the methods in the above question.

Q. What firewalls does your system work with?
Any firewall that can filter on the port level will work with our products.

Q. How is the Helvar router protected from viruses?
The Helvar Lighting Routers are proprietary hardware and firmware, not a typical client machine. They do not use any embedded windows or linux software, which are the usual targets for virus.
As part of normal operations, routers do not download any files. However, you may want to install virus protection for a PC that has Helvar Designer software installed if it is used for other (non-Helvar) functions and is exposed to the Internet.