ETC Network Infrastructure

Design Guide

Rev: A

Released: 2018-11

Introduction

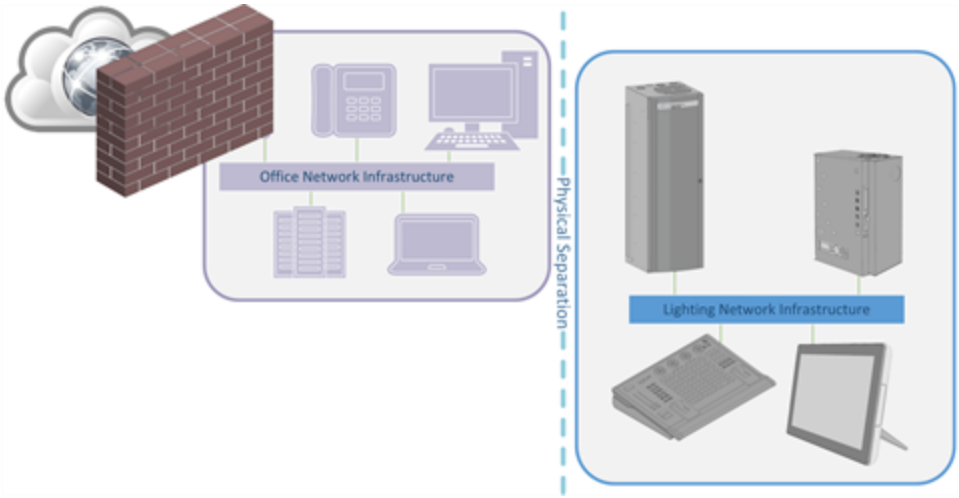
This document summarizes best practices and compatibility details for installing current networked ETC products. Additionally, ***Appendix: Securing the Lighting Network on page 10*** addresses network isolation security choices and ramifications.

The following sections are relevant to typically designed networked ETC lighting systems. Specific installations may differ. Any questions you have should be referred to ETC sales, project management or systems engineering.

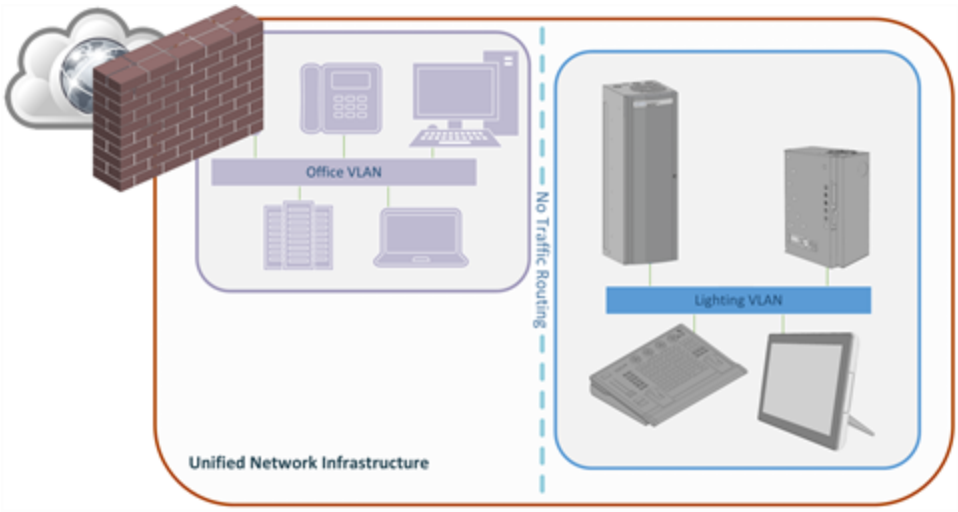
Uncoordinated deviations from the recommendations and requirements provided in this document could result in a non-functional system. Alterations must be discussed with ETC prior to scheduling system installation and could significantly impact overall time and costs for project completion.

Overview

ETC lighting systems have traditionally used flat, isolated networks with dedicated network hardware and cabling - completely separate from corporate intranets and the outside world. ETC strongly recommends this type of network arrangement, and it remains the best practice.



If network infrastructure must be shared, ETC recommends recreating the isolated environment as closely as possible. This increases serviceability and maximizes reliability, particularly in the systems' mission-critical and sometimes life-safety related duties.



ETC control systems depend on constant unicast and multicast communication throughout the network. Use hardwired technologies whenever possible and reserve wireless networking for limited, specifically-coordinated control interface applications.

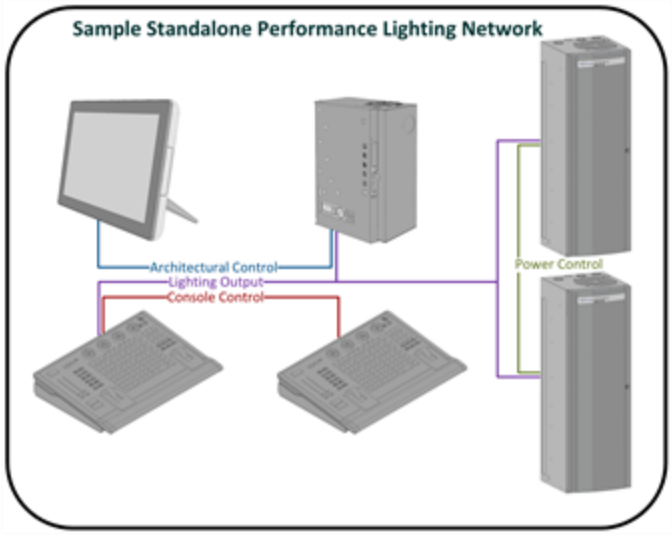
Understanding Network Functions

Networked ETC control systems support several Ethernet networks with differing functions:

- ***Lighting Control*** networks facilitate communication between most ETC lighting products, allowing the coordination of system activities. Lighting control network functions typically combine peer-to-peer and client-server network usage patterns, both transmitting real-time interaction data.
- ***Lighting Output*** networks carry computed streaming level data (e.g. sACN/ ANSI E1.31) from control interface products (e.g. Paradigm Architectural Control Processors) to power control devices (e.g. Echo Relay Panels) or protocol converters (e.g. Response DMX/RDM Gateways) connected to lighting fixtures. Lighting output network functions typically follow client-server network usage patterns for real-time streaming data and servers are often physically distributed throughout a facility.
- ***Intranet*** network connectivity enables communication to standard office infrastructure for corporate or external network resources (e.g. building management system interaction, control access from specific users' desktop computers, or email alerts of system issues). Any global Internet connectivity is expected to route via the intranet and be appropriately secured behind organizational protective measures.

Note: *Most installations combine some lighting output functions onto the lighting control network.*

A typical small performance lighting network serves as a control network between lighting console components, architectural system equipment, and power control products. Simultaneously, the network also serves output functions from the primary console and architectural processors to the power controllers. Specific products and installations can add additional discrete lighting control or output networks. In some applications, output networks carry non-ETC proprietary protocols with different requirements.



Shared Network Design Recommendations

When physical infrastructure is shared between lighting users and others, you should consider the following three best practices:

Best Practice 1

Use an isolated Virtual Local Area Network (VLAN) for lighting traffic. Standard lighting control and output networks do not require or want Internet or corporate network connectivity.

If your site requires UDP protocol string integration, targeted permissions can be required allowing routed ICMP and UDP protocols sent to/from one or more specific light control VLAN IP address/port combinations.

***CAUTION:** You should provide a static bandwidth allocation to your lighting network. Do not apply traffic shaping to the lighting VLAN. Dynamic bandwidth allocation can result in lighting communication sequencing or timing failures.*

Best Practice 2

Enable Internet Group Management Protocol (IGMP) for lighting control and lighting output networks and enable an IGMP v2 querier within lighting designated networks.

- ETC devices implement IGMP V3, V2, or V1 (varies by device type)
- Querier interval must be short (e.g. 30 seconds) to facilitate rapid re-convergence in the event of mid-point switch failure
- All VLAN multicast traffic should be available to all hardwired ports contingent on IGMP responses. Attempting to filter multicast traffic affects the behavior of the lighting system.
- Sample settings:
  - IGMP Snooping: Enabled on device and VLAN
  - Querier: Enabled on device near network center
  - Query Robustness: 5
  - Query Interval: 30
  - Query Max Response Interval: 6
  - Last Member Query Counter: 7
  - Last Member Query Interval: 8000

Best Practice 3

Apply Rapid Spanning Tree Protocol (STP) to help avoid incidental loops that can cause loss of communication and control.

Unless otherwise stipulated, all lighting device and programming ports should be configured as RSTP Edge ports to allow data forwarding as rapidly as possible upon port connection.

The following configuration example shows how to enable Rapid PVST+ (Rapid Spanning Tree) on a Cisco switch:

```
configure terminal
spanning-tree mode rapid-pvst
```

The following configuration example shows how to enable spanning tree on a Cisco switch port:

```
interface interface-id
spanning-tree portfast
```

General Network Implementation Requirements

The following sections provide general requirements when designing your network.

Switch Port Configuration

You must follow these requirements when configuring your network switch ports:

- Hardwired lighting ports shall be statically assigned to output untagged data from the relevant VLAN.
- To facilitate quick troubleshooting, including swapping of hardware controllers without IT intervention, you should enforce security by securing and limiting physical access to the assigned physical lighting network ports.
  - No Network Access Control (NAC) or credential based security should be used
  - No login mechanism (e.g. 802.1x) should be required for a connected device to gain access upon connection.
  - There should not be any limitation on active MAC address count for any ports.

Programming Port Placement

You must follow these requirements when determining where to place your programming ports:

- Labeled, permanent system programming ports configured on the lighting control VLAN should be installed in all rooms containing networked equipment and any control booth areas with visibility to illuminated spaces.

Note: *Permanent programming ports should not be subject to usage or security audit and remain active throughout the life of the facility.*

- Temporary system programming ports configured on the lighting control VLAN may be required in proximity to any lighting related "features" such as areas with color changing or moving fixtures.
  - Temporary programming ports should not be subject to usage audit during system startup and only deactivated after completion of relevant work. This should be coordinated with on-site ETC personnel.
  - Temporary programming ports may require coordinated reactivation for future lighting system troubleshooting, maintenance, and/or reprogramming visits.

Installation Coordination

Consider the following to allow for a coordinated effort in the network installation:

- Networks should be installed and functional before you begin programming connected equipment as a part of ETC system startup.
- If ETC supplied switches will be included in the installation, identify and communicate the configured IGMP query and timer expiration intervals to ETC prior to the shipping of your network equipment.
- Provide any facility prescribed range(s) (if applicable) including IP and subnet mask at least two weeks prior to ETC on-site presence for beginning system installation.
- Troubleshooting of network interactions may, in some cases, require packet captures of lighting network data. On-site ETC personnel shall be authorized to request and coordinate appropriately configured ports on a temporary basis as needed.

- On-site ETC personnel shall be furnished with 24 hour contact information for unified network support with authority and access to implement network configuration and wiring changes as needed.
- Bringing any converged network online is a growing process. Recognizing this, ETC project management and on-site personnel should be kept apprised of planned and unplanned network outages and restarts during the system startup process.

Wired Network Implementation Recommendation

For effective field identification, ETC recommends identifying a unique hardware color code for lighting network infrastructure. This color code could be applied to patch cable jacket selection and/or physical patch bay ports as well as labeling.

Wireless Network Implementation Requirements

The following sections provide requirements for implementing a wireless network.

Limited Usage

Due to continuous streams of data and expected responsiveness used for Lighting Control and Lighting Output, wireless connectivity is inappropriate for some control and programming functions but acceptable for others.

Any application of wireless technology to lighting network functions shall be coordinated with ETC during network system design.

Wireless connectivity shall not be used for permanently installed lighting equipment or lighting output networking, only for portable control or programming interfaces as required by site conditions.

Access

Access to your wireless network should be managed by hiding your SSID, using proper security measures and allowing full access to the network when connected appropriately.

Lighting control network wireless connection should be done using an unbroadcast SSID network, typically on the same wireless infrastructure as other facility networks.

For security on your wireless network, consider the following:

- Use your network provider choice of industry standard wireless network encryption
- Because you cannot physically secure access to a wireless network, ETC encourages an additional MAC address filtering security layer for wireless lighting control network access

Do not place restrictions on the wireless network. For proper operation, once connected to the wireless lighting control network, a wireless client should be a fully functional connected peer with the same access as a hardwired member of the lighting control network VLAN.

Multicast

Consider the following points regarding multicast:

- Some streaming multicast/broadcast data protocols such as sACN (ANSI e1.31) or Art-Net can create performance issues on wireless infrastructure.
- As system design is being finalized and during implementation, ETC may provide Access Control List (ACL) information to restrict extraneous traffic at the wireless network entry point.
- All other lighting control network multicast traffic should be available to all wireless endpoints contingent on IGMP responses.

Corporate Intranet-Exposed ETC Lighting Control Devices

Two ETC lighting products (Net3 Conductor and Paradigm Central Control Server) have secondary network ports designed for corporate intranet connectivity. IP addresses for these ports may be static or assigned using DHCP, however, they must reside outside the range for the rest of the Lighting Control and Lighting Output networks.

Note: *Access requirements on these ports may vary with site requirements.*

Typically, Net3 Conductor requires:

- NTP access to a site time server (server address provided by the facility)
- FTP and HTTP access to the greater Internet
  - Site provided proxy credentials can be entered by the startup technician
  - Lighting system reconfiguration will be required for changes to proxy servers or credentials

Typically, Paradigm Central Control Server requires no Internet access, but may require:

- BACnet/IP communication with corporate building management systems

Note: *BACnet/IP communication is restricted to the local broadcast domain unless other BACnet specific networking equipment coordinates forwarding*

- Standard TCP/IP communication with certain corporate desktop or wireless client computers for Paradigm Virtual Touchscreen interactions

Appendix: Securing the Lighting Network

ETC strongly recommends isolating lighting networks from other internal and external computing systems, whenever possible. Also, physically protect portable devices and safeguard any non-isolated lighting devices using standard information technology security practices.

Unless specifically tailored for higher security, most dedicated lighting products use embedded operating systems engineered for long-term stability and efficiency. This equipment does not typically need to operate on a corporate intranet or the Internet. Applying security software can alter system responsiveness and compromise interoperability between lighting control products.

Users and facility administrators should ensure system security by allowing lighting network access only for necessary devices. Up-to-date security measures should be maintained whenever a portable device with lighting functions (laptop, tablet, phone, etc.) is used elsewhere.

Facility IT professionals must maintain best practice safeguards between intranet-connected network lighting equipment and the Internet. As with any device, external access should only be enabled for specific hosts, ports, and functions; and only with safeguards appropriate for entering a corporate network.

Network Isolation

Network isolation is a primary way of securing any network. Isolating a network reduces risk by limiting which hosts can interact with the protected equipment and in what ways. There are three key elements to an isolated network:

- Place protected equipment within the isolated network structure
- Keep unneeded equipment outside the protected network
- Restrict communication into and out of the network

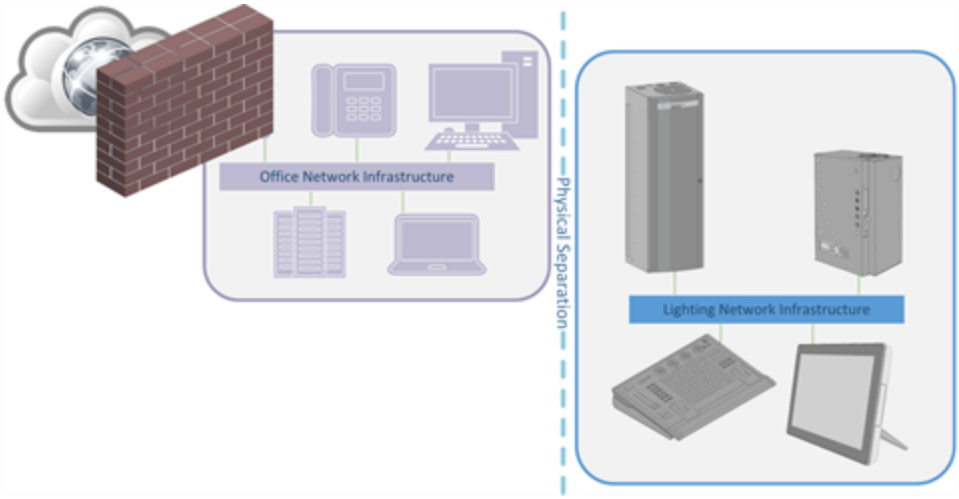
Organizational IT departments typically use isolation to safeguard internal hosts from the larger risks of the global Internet. ETC recommends an additional security layer—isolating the lighting network from the organizational business network.

Two primary options exist for creating an isolated network:

- **Physical Isolation** (aka "Air Gap")
- **Logical Isolation**

Physical Isolation

A complete network infrastructure can be dedicated to the lighting system where the network's sole purpose is connecting lighting devices. This has long been ETC's recommendation and remains the best practice. It not only increases security, but also reduces coordination demands and simplifies system design, implementation, and troubleshooting.



Physical isolation is often found in environments where an extremely high level of security is required (i.e. nuclear power plants, missile launch sites, theme park ride control systems, lighting networks).

Logical Isolation

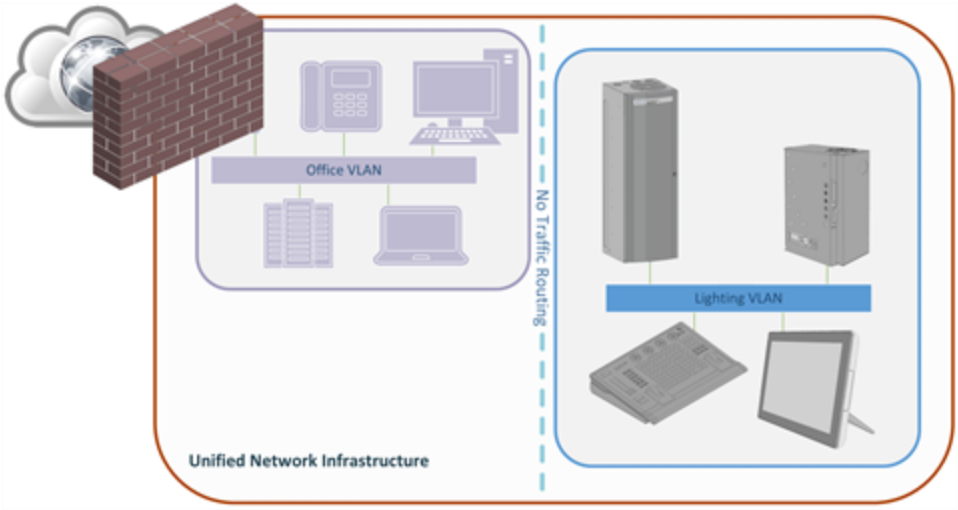
Another approach to network security is logical isolation: using modern networking equipment features to create a logical separation of networks.

There are three common implementations for logically isolated networks:

- **Isolated Virtual Local Area Networks**
- **Traditional Firewalls and Access Control Lists**
- **Next-Generation Firewalls**

Isolated Virtual Local Area Network

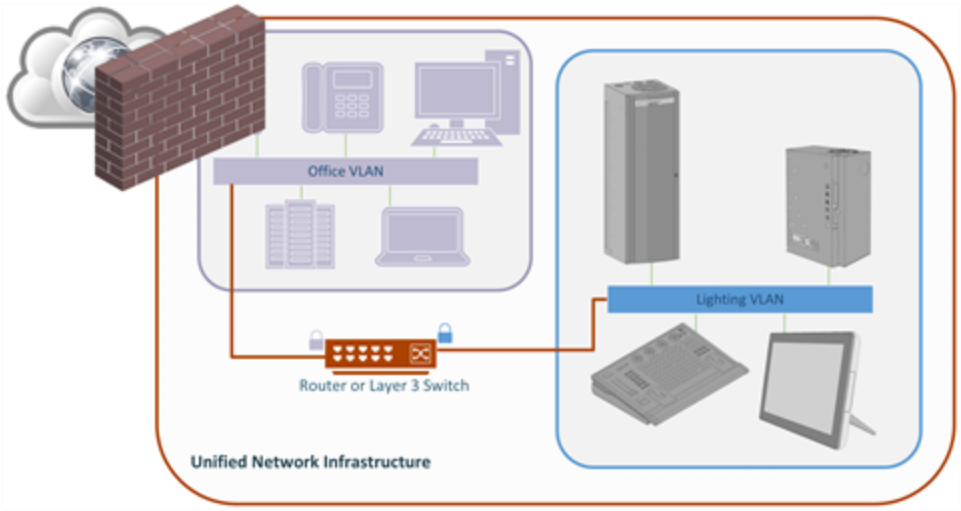
Distinct Virtual Local Area Networks (VLANs) provide network security by creating logically separate layer-2 networks defined on shared network equipment.



For the most secure implementation, network traffic will not be routable to the organization's network or beyond. Devices on this network should only be reachable by other devices on this network.

Traditional Firewalls and Access Control Lists

Traditional Firewalls and Access Control Lists (ACLs) provide network security by permitting or blocking network traffic as determined by the administrator. Typically, access is granted at the port, protocol, source, and destination level with a default deny-all for data both entering and leaving the lighting network.

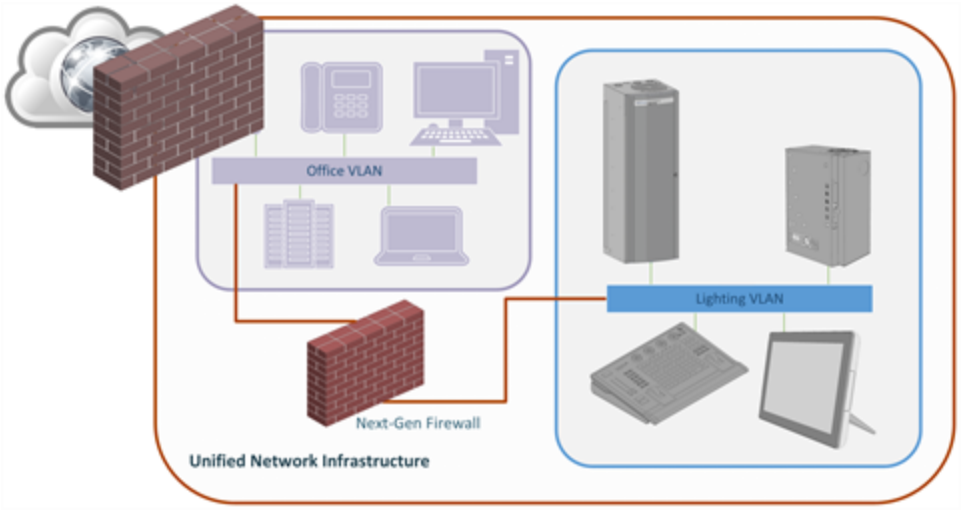


In this case, the lighting network is separated from the organization's network by a traditional firewall, router, or VLAN on a layer-3 switch and administrators specify allowed traffic using ACLs. Though this introduces some risk, the threat vector remains small.

Next-Generation Firewalls

Firewalls provide network security by providing a mechanism to inspect, filter, and block traffic based on rulesets defined by the administrator.

Setting up a next-generation firewall (NGFW) with filtering capabilities like an intrusion prevention system (IPS) and deep packet inspection can be a great benefit. This added filtering can watch for any malicious traffic destined for the network and prevent it from entering.



In this case, the lighting network is separated from the organization's network by a firewall, and administrators can select what traffic to allow using the next-gen firewall capabilities. Though this introduces some risk, the threat vector can be even smaller.

Support Availability

Configuration for protection devices between lighting networks and other systems varies depending on the lighting equipment provided, its configuration, and any necessary ties to other building systems. ETC Systems Engineering can provide relevant documentation for specific projects as required.

Corporate Headquarters ■ Middleton, WI, USA ■ Tel +608 831 4116 ■ Service: (Americas) **service@etcconnect.com**
London, UK ■ Tel +44 (0)20 8896 1000 ■ Service: (UK) **service@etceurope.com**
Rome, IT ■ Tel +39 (06) 32 111 683 ■ Service: (UK) **service@etceurope.com**
Holzkirchen, DE ■ Tel +49 (80 24) 47 00-0 ■ Service: (DE) **techserv-hoki@etcconnect.com**
Hong Kong ■ Tel +852 2799 1220 ■ Service: (Asia) **service@etcasia.com**
Web: etcconnect.com
Rev A ■ Released 2018-11