Guide to ETC Network Requirements

Understanding Networked ETC Lighting Control Systems

Rev: A

Released: 2021-11

Introduction

This document expands on information described in the *ETC Network Requirements* document, which outlines minimum network requirements for ETC lighting control systems. You should review the *ETC Network Requirements* document prior to proceeding. In addition, this document summarizes best practices and compatibility details for installing current networked ETC products.

Overview

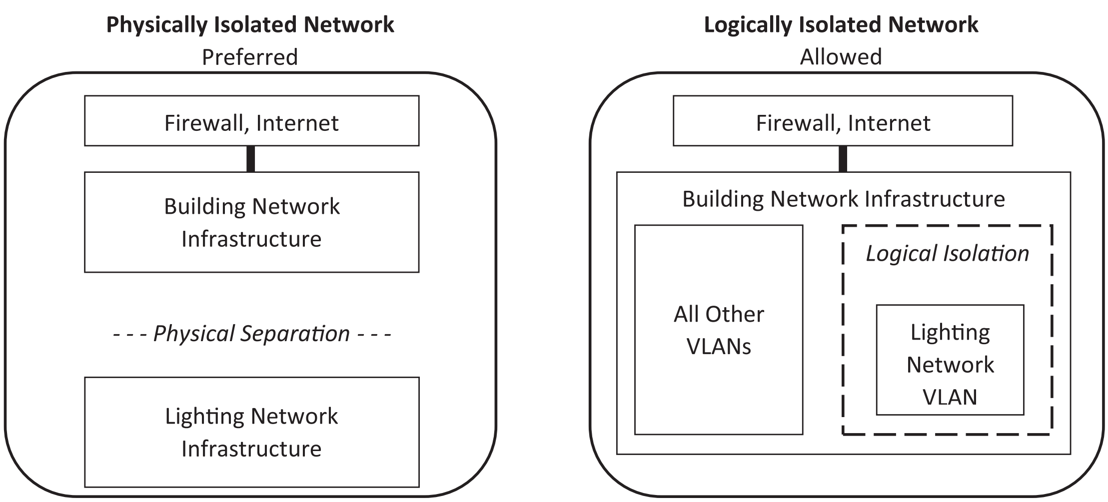
ETC lighting systems have traditionally used flat, isolated networks with dedicated network hardware and cabling that are separate from corporate intranets and the outside world. This is the preferred network arrangement and remains the best practice.

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 system's mission-critical and sometimes life-safety related duties.

The sections in this document are relevant to typically-designed networked ETC lighting systems. Specific installations may vary. Any questions 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-functioning system. Alterations must be discussed with ETC prior to scheduling system installation and could significantly impact overall time and costs for project completion.

System Layout Examples



Installation Coordination

You should ask any questions and have implementation discussions with your site's assigned ETC Project Manager prior to ETC beginning work on site. When the site is ready for ETC to begin work, a *System Startup Request - Network Addendum* will be sent. This document contains questions pertinent to the information in the *ETC Network Requirements* document and requires site contact information for the network administrator. Once you receive the *System Startup Request*, you should review it in association with the following content.

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

- Networks shall be installed and functional prior to ETC Technicians arriving on-site to begin ETC system startup.
- If ETC supplies network switches that will be added to a network infrastructure by others, identify and communicate the configured IGMP (Internet Group Management Protocol) query and timer expiration intervals to ETC prior to the shipping of the network equipment.
- Provide any facility prescribed address ranges (if applicable), including IP and subnet mask in the *System Startup Request*.
- Troubleshooting of network interactions may sometimes require packet captures of lighting network data. On-site ETC personnel shall be authorized to request and coordinate appropriately configured troubleshooting ports on a temporary basis as needed.
- On-site ETC personnel shall be furnished with 24-hour contact information for unified network support with the authority and access to implement network configuration and wiring changes as needed.
- ETC Project Management and on-site personnel shall be kept apprised of planned and unplanned network outages and restarts during the System Startup process.

Understanding Network Functions

Lighting Control

Lighting Control facilitates communication between most ETC lighting products, allowing the coordination of system activities. Lighting Control network functions typically combine peer-to-peer and client-server usage patterns, both transmitting real-time interaction data. Lighting Control uses a combination of unicast, multicast, and broadcast. Examples include:

- Processor and/or show file synchronization
- Third-party integration
- System configuration
- User interaction (web interfaces, touchscreens, software applications)

Lighting Output

Lighting Output describes lighting levels (i.e., sACN/ANSI E1.31) sent from controllers to power control devices (e.g., relay panels, dimming cabinets) or protocol converters (e.g., DMX gateways, 0-10V gateways) . Lighting Output network functions typically follow client-server network usage patterns for real-time streaming data and servers are often physically distributed throughout a site. This means that multiple devices on the network can act as the source or the recipient (or both) of lighting output information.

Lighting Output primarily uses multicast. The output hardware (e.g., dimmer cabinets, relay cabinets, DMX gateways) rely heavily on the reception and timing of multicast packets to determine behavior, such as the outputting of live lighting levels or executing Data Loss Behavior in the absence of levels. The organization of multicast over the network is very dependent on IGMP. Examples of Lighting Output include:

- Lighting Levels (sACN, Art-Net™, KiNET, et cetera)

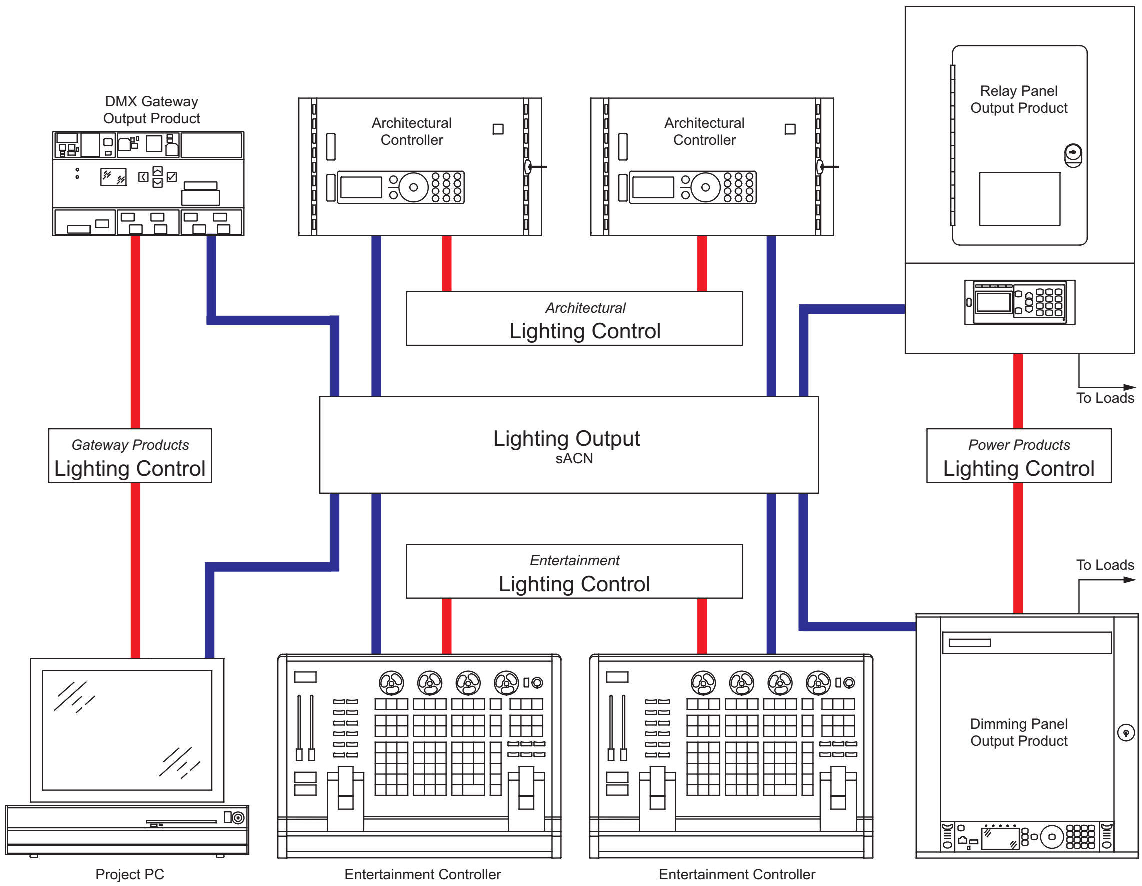
Intranet

Intranet connectivity enables communication to standard office infrastructure for corporate or external network resources (e.g., building management system interaction, control access from specific user’s desktop computers, email alerts of system issues). Any global internet connectivity is expected to route via the local intranet and be appropriately secured behind organizational protective measures. Intranet and internet are not required for an ETC lighting system to function. The scope of work for an ETC lighting network connected to a building's intranet is dependent on the site's control intent. For specific ETC hardware information, please refer to *Site Intranet-Exposed Control Devices on page 9*. Examples of control intent that would require connectivity to a local intranet include:

- BACnet
- System SMS/email alerts
- Remote triggering

Usage Example Riser

The riser below is a logical network example of an ETC lighting system. Physically, each of these devices only has a single network connection to a network switch. This example shows Lighting Control (red lines) information shared between entertainment controller hardware, architectural controller hardware, and power control/output hardware. Simultaneously, the network also provides Lighting Output (blue lines) functions between the control sources and the output products. This example uses a combination of unicast, multicast, and broadcast. Intranet is excluded from these risers but is detailed in other sections of this document.



Network Requirements

The following section expands on the information in the *ETC Network Requirements* document. This expanded information will aid in the design and implementation of the network infrastructure.

Managed Vs Unmanaged Network Switches

It is recommended that you use managed switches for ETC lighting networks as they can be configured based on the best practices outlined in this document and the *ETC Network Requirements* document.

For the purposes of this document, a managed switch is defined as a switch that allows the user to configure individual settings for features such as Spanning Tree, IGMP, and VLAN.

Unmanaged switches should only be used in smaller scale sites that utilize a limited quantity of networked devices. An example would be a venue where all networked devices exist on the same network switch and no third-party integration is required. Even then a managed switch is still preferred.

For the purposes of this document, an unmanaged switch is defined as a switch with no interface from which to configure settings for features such as Spanning Tree, IGMP, and VLAN.

Managed switches are preferred with ETC lighting control systems. However, a managed switch that is not properly configured can be more detrimental to system operation than using an unmanaged switch.

Switch Port Configuration

Follow these requirements when configuring network switch ports:

- Hardwired lighting ports shall be statically assigned to output untagged data from the relevant VLAN (Virtual Local Area Network).
- If Network Access Control (NAC) is required, ETC equipment is compatible with MAC Authentication Bypass.
- Usage of MAC Authentication Bypass or any limitations on the quantity of active MAC addresses for any port should be coordinated prior to installation.
- No login mechanism (e.g. 802.1x) should be required for a connected device to gain access upon connection.
- To facilitate quick troubleshooting, including swapping of ETC hardware without IT intervention, enforcing security by limiting physical access to the assigned lighting network ports is preferred.

Programming Port Placement

Programming ports are needed for ETC technicians to access, configure, and troubleshoot the ETC lighting control system during startup and as needed for maintenance after the startup is completed.

Follow these recommendations when determining where to place programming ports:

- Labeled, permanent system programming ports configured on the lighting VLAN should be installed in all rooms containing networked equipment and any control areas with visibility to illuminated spaces. If a list of locations or areas hosting ETC hardware is not known, contact the site's assigned ETC Project Manager.
  - Failure to have programming ports in close proximity to ETC network hardware or illuminated areas in control by ETC hardware may cause significant delays at the time of startup and programming.

Permanent programming ports should not be subject to usage or security audit and remain active throughout the life of the facility. If this is not possible, it is recommended that you use MAC filtering.

- Temporary system programming ports configured on the lighting 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 site visits.

Multicast Usage and Settings

In an ETC lighting control network, there will always be more than one source of multicast traffic. Depending on the size and scale of the installation, there could be a large quantity of nodes that will act as both a source of multicast as well as a receiver of multicast.

The quantity of multicast addresses that can be sourced or received by nodes is determined by the specific product. It is common for a single ETC node to host 10s, 100s, or even 1000s of multicast addresses (depending on the product).

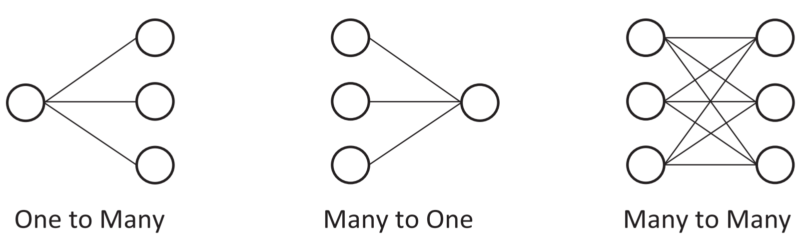
The multicast address ranges used by ETC are part of industry accepted standards and protocols and are non-negotiable. They cannot be modified. As an example, the most common use of multicast in an ETC lighting control system is lighting levels using sACN protocol (ANSI E1.31). This protocol allows for up to 64000 multicast addresses to exist on a single lighting control network.

While it is unlikely that all multicast addresses for sACN will be used, it is important to understand the capacity and usage of multicast in a lighting network. For this reason, **an IGMP querier is required**.

Enable IGMP and a querier within lighting designated networks. Any distribution or edge switches must have IGMP snooping enabled.

- ETC devices implement IGMP v1, v2, or v3 (varies by device type).
- A short querier interval (e.g. 30 seconds) will facilitate rapid re-convergence in the event of mid-point switch failure.
- All multicast traffic should be available to all hardwired ports contingent on IGMP responses. Attempting to filter multicast traffic can introduce unpredictable and/or undesired behavior into the lighting control system.
- Example IGMP Querier Settings:
  - IGMP Snooping: Enabled on device and VLAN
  - Querier: Enabled on device near network center
  - Query Robustness: 2 (minimum)
  - Query Interval: 30 seconds
  - Query Max Response Interval: 6 seconds
  - Last Member Query Counter: 7
  - Last Member Query Interval: 8000 milliseconds
- Network Infrastructure should allow at least 50 simultaneous join requests per ETC node (per IGMP report packet).

An ETC network utilizes multiple variations of multicast simultaneously, often on the same device. Anycast is not supported.



Shared Network Recommendations

When physical isolation of the lighting network is not possible and a shared network must be used, consider the following best practices:

VLAN Setup

Use an isolated VLAN for lighting traffic. The lighting VLAN must be kept isolated from all other VLANs in the same physical network. Intranet and internet connectivity is not required or requested for the lighting control system to function.

If the site requires UDP string integration (third-party control integration), targeted permissions may be required allowing routed ICMP and UDP sent to/from one or more specific lighting controllers.

Provide a static bandwidth allocation to the lighting network. Do not apply traffic shaping to the lighting VLAN. Dynamic bandwidth allocation can result in lighting communication sequencing or timing failures.

Jumbo Frames should be permitted.

Spanning Tree

Apply Rapid Spanning Tree Protocol (RSTP) 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 with RSTP Edge Port Enabled to allow data forwarding as rapidly as possible upon port connection.

Color Codes and Labels

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.

Site Intranet-Exposed Control Devices

Some ETC lighting products have secondary network ports designed for corporate/building intranet connectivity. Contact ETC Project Management to determine if any of these products exist at the site.

IPv4 addresses for these ports may be static or assigned using DHCP, however, they must reside outside the IPv4 range/subnet in use by the lighting network. (e.g., lighting network subnet of 10.101/16, corporate intranet subnet of 192.168/16).

Below is a list of ETC products that support secondary network connections and specific features for each. Secondary network use is optional and determined by the control intent for the installation.

Conductor

This is a network services gateway for the ETC lighting system that, amongst other tasks, can act as a DHCP server, an NTP server, and a syslog repository. Below are the features currently accessible using the secondary network port.

- Client NTP access to a site time server (server address provided by the facility).
- FTP and HTTP access to the greater internet for select alerts via SMS message or email.
  - Site-provided proxy credentials can be entered at system startup.
  - Lighting system reconfiguration will be required for future changes to proxy servers or credentials.

Paradigm Central Control Server (P-CCS)

This hardware is responsible for the coordination of one or more Paradigm control systems if they exist as part of the same installation. Below are the features currently accessible using the secondary network port.

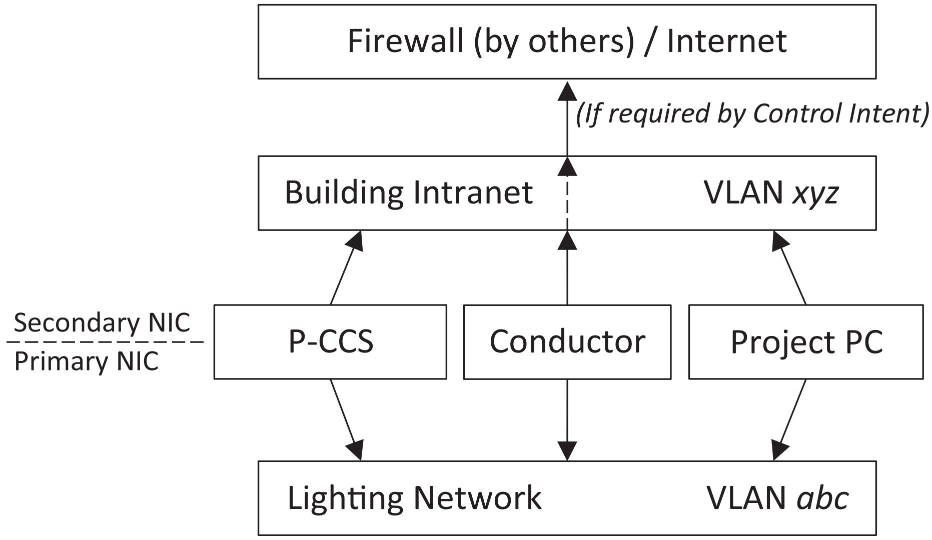
- There must be no access from the greater internet to the P-CCS.
- Standard TCP/IP communication with corporate computers for use with the Paradigm Virtual Touchscreen software application.
- BACnet/IP communication with corporate building management systems.
  - Default properties: Device Instance # 108, UDP # 47808, Network ID # 0.
    - Network ID cannot be changed at this time.
  - BACnet PICS datasheet available upon request.

BACnet/IP communication is restricted to the local broadcast domain unless third-party BACnet specific networking equipment (by others) coordinates forwarding.

ETC Project PC

- These are Windows PC desktop or laptop computers supplied by ETC.
- These computers are used for system startup, site configuration, and maintenance of the ETC lighting control system.
- Secondary network port may be used to provide VPN or other site-approved and secured remote desktop access to the computer.

Example Riser for Site Intranet-Exposed Control Devices



Wireless Network Implementation Requirements

Wireless network is not needed at every ETC installation. Its use is determined by the control intent for the site. If it is determined that wireless networking is necessary, the following is a list of requirements for wireless network implementation.

Limited Usage

Due to continuous streams of data and expected responsiveness used for the lighting network, 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 the network system design.

Wireless LAN connectivity shall not be used for permanently installed lighting equipment, only for portable control or programming interfaces as required by site conditions. Contact ETC Project Management for a list of wireless devices specified for the installation.

Not all ETC software is designed for use over a wireless connection. ETC software including but not limited to the following is not currently supported in a wireless environment: Paradigm LightDesigner, Paradigm ControlDesigner, Mosaic Designer, Concert, Eos, ETCnomad, UpdaterAtor.

Access

For proper operation, once connected to the wireless lighting network, a wireless client should be treated as a peer with the same access as a hardwired member of the lighting network VLAN. Consideration is needed for the IPv4 address scheme for wireless in relationship to the hardwired IPv4 address scheme designated for lighting control network. Some ETC wireless applications need to establish both unicast and multicast connections with hardwired ETC devices.

For security of the wireless network, consider the following:

- Use choice of industry standard wireless network encryption.
- Because physical security of a wireless network is non-existent, ETC encourages an additional MAC address filtering security layer for wireless lighting control network access (by others).

Multicast

Consider the following points regarding multicast over wireless:

- Some streaming multicast/broadcast data protocols such as sACN (ANSI E1.31) 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 to the lighting network.
- All other lighting control network multicast traffic should be available to all wireless endpoints contingent on IGMP responses.

Routing and Divided Subnets

It is recommended that all ETC networked hardware exist on the same IPv4 subnet without routing.

The need for routing is usually applied to scenarios in which networked hardware exists on different IPv4 subnets and need to communicate with one another. Example: Device A with an IPv4 address of 10.101.10.101/16 needs to communicate to Device B with an IPv4 address of 192.168.10.101/16. This scenario is avoided on the lighting network by keeping all ETC provided networked devices on the same subnet. Exceptions to this are detailed below.

Configuration Access Inhibited

Currently, ETC devices and ETC configuration software do not support the configuration and session synchronization of networked devices that reside on a subnet outside that of the device's own IP subnet. This falls under the category of Lighting Control as referenced in *Understanding Network Functions on page 3*. Expanding on the previous example, configuration software may reside on a PC with an IPv4 address of 10.101.10.102/16. The PC would be able to view and configure Device A but not Device B. Likewise, Device A would not be able to join a session with Device B as they cannot see each other. Even with a router applied to this scenario, packets may be forwarded, however, configuration would still not be possible as software inhibits configuration for devices on non-local subnets.

Lighting Output is primarily made up of multicast traffic (sACN/ANSI E1.31). Multicast traffic can traverse divided subnets on the same VLAN as they use a reserved IPv4 range of 224.0.0.0 - 239.255.255.255.

As the majority of ETC networked hardware only has a single network connection, the concepts of Lighting Control and Lighting Output both must fall under the same IPv4 address and therefore must exist on the same subnet. Examples of ETC product lines that utilize a single network connection are Paradigm (architectural controllers), Echo (relay and dimming cabinets), and Response Gateways (protocol converters).

Divided Subnet Exceptions

The exceptions to this rule are for those ETC devices that incorporate multiple network cards or when integration with other networks is involved.

ETC High-Output Controllers

Examples of ETC product lines that utilize multiple network cards are Eos Family Consoles (entertainment controllers) and Mosaic (architectural controllers). Specific Eos and Mosaic hardware equipped with multiple network cards are designed so that Lighting Control and Lighting Output can be isolated from one another. Some hardware, such as Mosaic MSCX requires each network card to be in a different IPv4 subnet. This is intentional as the Eos and Mosaic hardware platforms can deal with higher quantities of Lighting Output numbering above 1000 multicast addresses .

Site-Intranet Exposed Devices

As explained in *Site Intranet-Exposed Control Devices on page 9*, the Paradigm Central Control Server, Conductor, and Project PC have specific features designed to be accessed from a secondary network connection that is not on the same subnet or network as that of the lighting network. See *Site Intranet-Exposed Control Devices on page 9* for more details.

While the Paradigm Central Control Server is expected to live on two different networks, only one of the two network ports can be routed due to a shared IP Gateway between the ports.

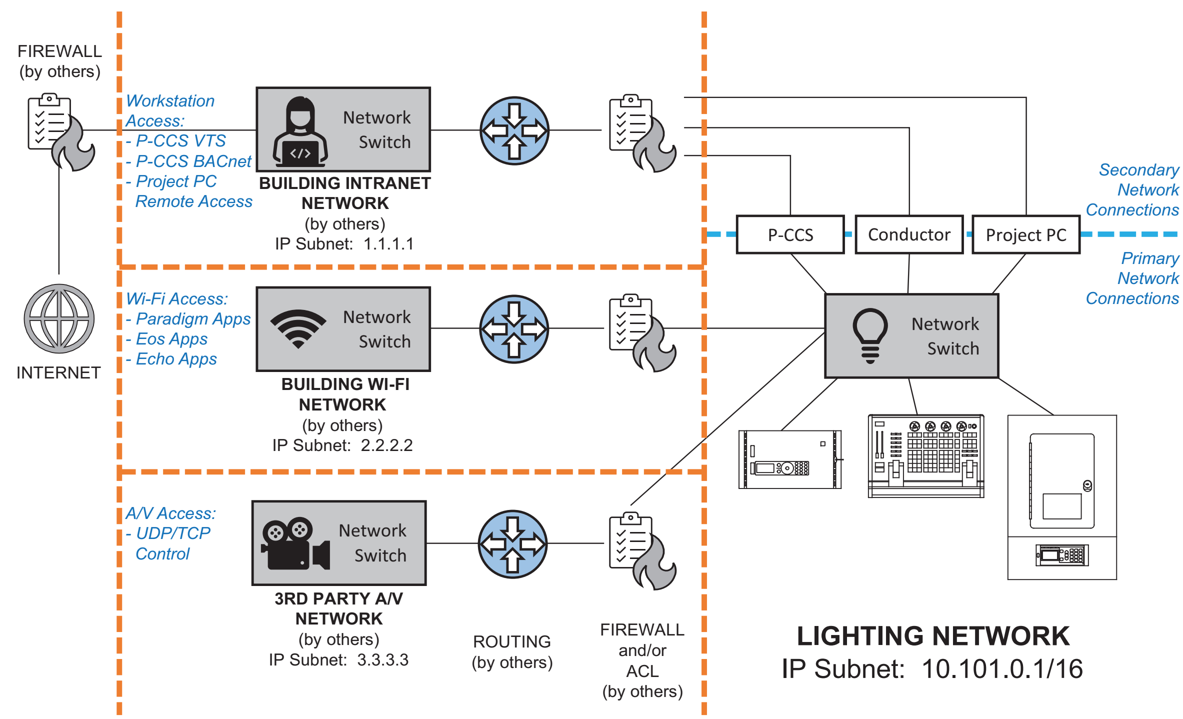
Third-Party Integration

At sites where third-party integration is required over a network connection, it may be required to route traffic from the third party's network to the ETC lighting network. The most common example is sending UDP commands and status messages back and forth between two controllers. It is also recommended in this scenario, as mentioned before, that additional measures be put into place to prevent cross-traffic between the two networks, such as implementing Access Control List or Firewall protections.

Example Riser: Routing and Divided Subnets

This is an example of the scenarios explained above.

All references to "(by others)" indicate that this network component is the responsibility of others to design, supply, install, integrate, and manage.



When working with third-party A/V integration, it is still preferred to explore serial RS232 options prior to exploring networking options.

Appendix: Securing the Lighting Network

ETC strongly recommends isolating lighting networks from other internal and external computing systems whenever possible. Additionally, 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. 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 ("Air Gap")
- Logical isolation (VLAN, ACL, firewall)

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 recommended by ETC 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 (e.g., power plants, government installations, 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 Network
- 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 specifically allow 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 NGFW capabilities. Though this introduces some risk, the threat vector can be reduced further.

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 lighting product documentation for specific projects as required.