# Eagle Eye Application Note - AN051

# Network Topology and Installation Best Practices

2023-12-01 Revision 2.1

## Target Audience

This Application Note is designed to cover network topology and best practices when installing an Eagle Eye Cloud VMS system and is intended for intermediate to advanced technical users and installers. Although this is meant for any size/class of user, it will mainly apply to larger clients with more extensive networks. In addition, design engineers, estimators, and on-site technical staff will also benefit from the details outlined below. Resellers, too, should be aware of the network topology when designing new systems or taking over existing ones. Note that Camera Direct Complete installations will vary slightly based upon the different architecture and the fact that no Bridge/CMVR is utilized.

## Introduction

IP networks are used to connect Eagle Eye Bridges to IP cameras. While Eagle Eye itself does not set up those networks, they are required to connect IP cameras to the Eagle Eye Bridge. Networks that are correctly set up and optimized work more efficiently to deliver uninterrupted video surveillance. Following these guidelines will help ensure that quality video feeds are always sent to the cloud.

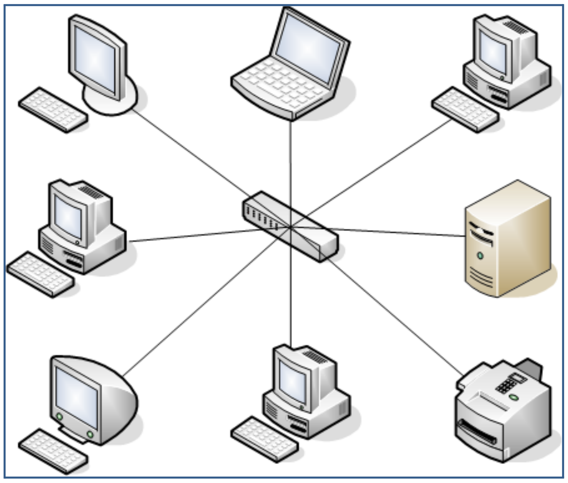
## Background

Eagle Eye Bridges should be correctly installed at the router or MDF (Main Distribution Frame) with a direct line out to the internet or WAN (Wide Area Network). In many cases, there is a firewall between the Bridge and the internet, but by following these firewall guidelines, there should be nothing preventing the video data from streaming to the cloud. [Click here to read the Essential Firewall Configuration Guide for Securing Eagle Eye Cloud VMS.] Also note that because of the nature of the system and because data is flowing to the cloud, Eagle Eye does not normally employ port blocking which would prevent traffic from leaving the Bridge. The same cannot be said for the internal network, or the LAN (Local Area Network). LANs come in all sizes and shapes, and it is this interface that requires more attention... Some LANS are centrally located and span out from a single point in a building or property; others can have a central point, but with multiple intermediate points across a campus or multi-floored building, Streaming video generates massive data flows, which can create challenges when the topology type changes.

**Star Topology (the recommended topology choice)**
Star topology networks (also known as hub-and-spoke networks) are the most straightforward and efficient networks for Eagle Eye systems. These networks tend to have a single point (hub) from which network feeds (spokes) return with data. The data is funneled from each spoke to the hub, which transfers the data into the CamLAN port on the Bridge via gigabit connection. That data is then buffered on the Bridge, encrypted, and transferred to the cloud via the WAN port on the Bridge.

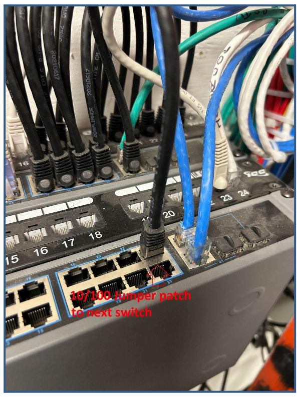
**Segmented Topology (not recommended)**
Segmented Topology Networks (also called Daisy Chain Networks) typically have multiple switches, with each one plugging directly into the next, creating a chain of switches, with each switch passing data through to the next. Every switch downstream from the first switch is considered a hop (a hop occurs when data is passed from one switch to the next). Whether a network is managed or unmanaged, each hop increases latency —— the time it takes information to get from point A (the camera) to point B (the Bridge). For non-managed networks there is additionally the risk of dropped packets and interrupted communications. . Daisy chaining switches should be avoided at all costs.

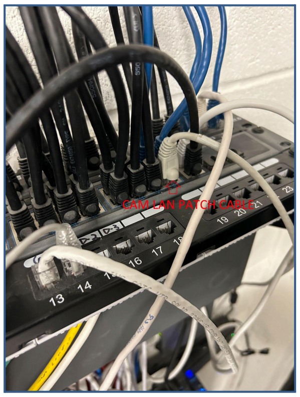
## The Most Efficient Network Topology



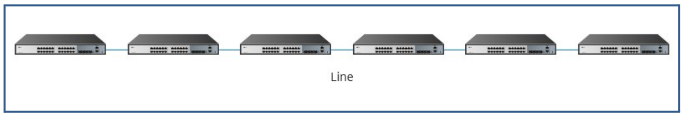
Star topology is the most ideal method of data transmission for our networks - a hub and spoke type of network. This design incorporates switches in the field (Intermediate Distribution Frames, or IDFs) that connect via Cat6 or fiber to a centralized switch (MDF) where the Bridge or CMVR resides. Field switches should always connect to the MDF, and the center switch should have a capacity of at least 1G. IDFs with five switches should have five copper or fiber home run feeds back to the MDF. If cameras are terminated at the MDF, they are also considered a spoke and should be patched into a main switch that handles all incoming Cat6 or fiber feeds from the field. If there are multiple CMVRs or Bridges, they should have their own designated main switch to take on incoming network connections from the field switches containing the cameras they are assigned to. In a managed network, this can be handled via multiple VLANs and port management, which is typically handled by the end user’s IT Admin. In this example, the integrator would be assigned IP addresses by the IT Admin and enter those addresses statically into all of the devices, including the Bridge or CMVR.

# Avoid Daisy Chain (Segmented) Network Topology





Surveillance networks that are designed by looping a trunk or backbone feed into one switch and out to another are considered Daisy Chained. While it is totally normal to have a transmission switch at the MDF and to connect that switch to a switch at another IDF, it is strongly recommended that no further switches be connected to the switch in the IDF. If a secondary switch is required at that IDF, or at an IDF in a separate area (such as a higher floor), that secondary switch should have its own home run Cat6 or fiber connection back to the MDF main switch. In the example images shown to the right, not only were these switches daisy chained, the pass-through ports offered a lower transmission speed (10/100), which effectively created a bottleneck of data at these ports.



As illustrated above, daisy chaining switches beyond two hops increases the latency of network data. When cameras are installed past the second hop, users may experience issues with latency, camera disconnection, undiscoverable cameras, and more. This leads to a poor user experience with end users typically complaining of slow load times for cameras. Another issue you might encounter with daisy chaining switches is the inability to locate the cameras on the network, which causes further frustration for end users.