Eagle Eye Application Note - AN015

Best Practices for Deploying Multiple Eagle Eye Networks Bridges on a Single Site

2025-01-30 Revision 1.0

Target Audience

This Application note is intended for installers and resellers of Eagle Eye Cloud VMS whose deployment size or site architecture necessitates the use of multiple Eagle Eye Networks Bridges or CMVR devices sharing a single internet connection. This document serves as a vital resource for installers, IT professionals, resellers, and system architects, providing them with the knowledge and tools needed to execute successful multi-bridge deployments.

Introduction

The Application Note outlines the critical considerations and best practices for deploying multiple Eagle Eye Networks Bridges or CMVR devices on a single site. It explores the potential challenges that can arise from default configurations, particularly related to CamLAN architecture and bandwidth management settings, and provides detailed guidance on how to mitigate these issues through careful planning and network design. By addressing the potential conflicts in CamLAN configurations, such as DHCP server clashes and IP address conflicts, and by carefully managing bandwidth allocation across devices, users can ensure a stable and efficient surveillance network. Whether opting for segregated CamLAN networks or a managed network CamLAN setup, understanding the implications of each approach will help optimize the deployment and operation of multiple bridges or CMVR devices.

Expanding on the critical points, this Application Note emphasizes the importance of proper planning and execution when deploying multiple Eagle Eye Networks Bridges or CMVR devices on a single site. We discuss the complexities that can arise when multiple devices share a single internet connection, particularly in environments where default configurations can lead to network instability and reduced system performance.

Important Considerations

The two primary approaches—segregated and managed CamLAN networks—each offer distinct advantages depending on the specific needs and constraints of the deployment site. Segregated networks help avoid conflicts by isolating each bridge or CMVR, ensuring stable operation and reducing the likelihood of IP address conflicts. On the other hand, managed CamLAN networks provide greater flexibility by allowing cameras to operate on an existing end user managed network, without the need to provide tertiary switches.

When deploying multiple bridge or CMVR units on a single site, in certain architectures, their default configuration may cause the units to adversely affect each other's operation. For this reason it is important to give consideration to a number of design aspects before deployment.

The primary considerations when deploying multiple bridges or CMVR devices on a single site are:

- CamLAN architecture. (The network responsible for the cameras)
- Configuration of bandwidth management settings. (The amount of outgoing WAN bandwidth available at the site)
- Existing LAN architecture. (The network type and the amount of bandwidth available on the local network)

Background

When proper consideration is not given to the different network architectures or bandwidth management settings of a Cloud VMS deployment utilizing multiple bridge or CMVR devices, the following adverse effects may be experienced:

CamLAN Architecture

By default, the CamLAN network interface on an Eagle Eye Networks Bridge or CMVR device is configured to act as a DHCP server, meaning it will serve IP addresses to network devices attached to the CamLAN network. The CamLAN is also configured to occupy a specific IP address within the subnet (10.143.0.1). When two or more bridges or CMVR devices are sharing a CamLAN, in their default configuration, they will be occupying the same IP address and serving conflicting IP addresses to camera devices in the network. The likely side effects of this configuration will be cameras frequently dropping offline, being unavailable to add, and general instability within the CamLAN network.

Configuration of Bandwidth Management Settings

In their default configuration, Eagle Eye Networks Bridges and CMVR devices are configured to use 50% of the detected bandwidth available to them. To achieve this, they perform periodic bandwidth speed tests with Eagle Eye Networks cloud data centers. The site must have sufficient upload bandwidth for any and all bridge or CMVR devices connected to the same internet connection.

As an example, for a site with three bridges sharing a single internet connection, where each bridge requires 50Mbps of upload speed, the site must have a minimum bandwidth of 150Mbps for all three bridges. It is strongly suggested that once a system like this is set up, the default transmit bandwidth is set to **Fixed** for each bridge, providing them the required bandwidth.

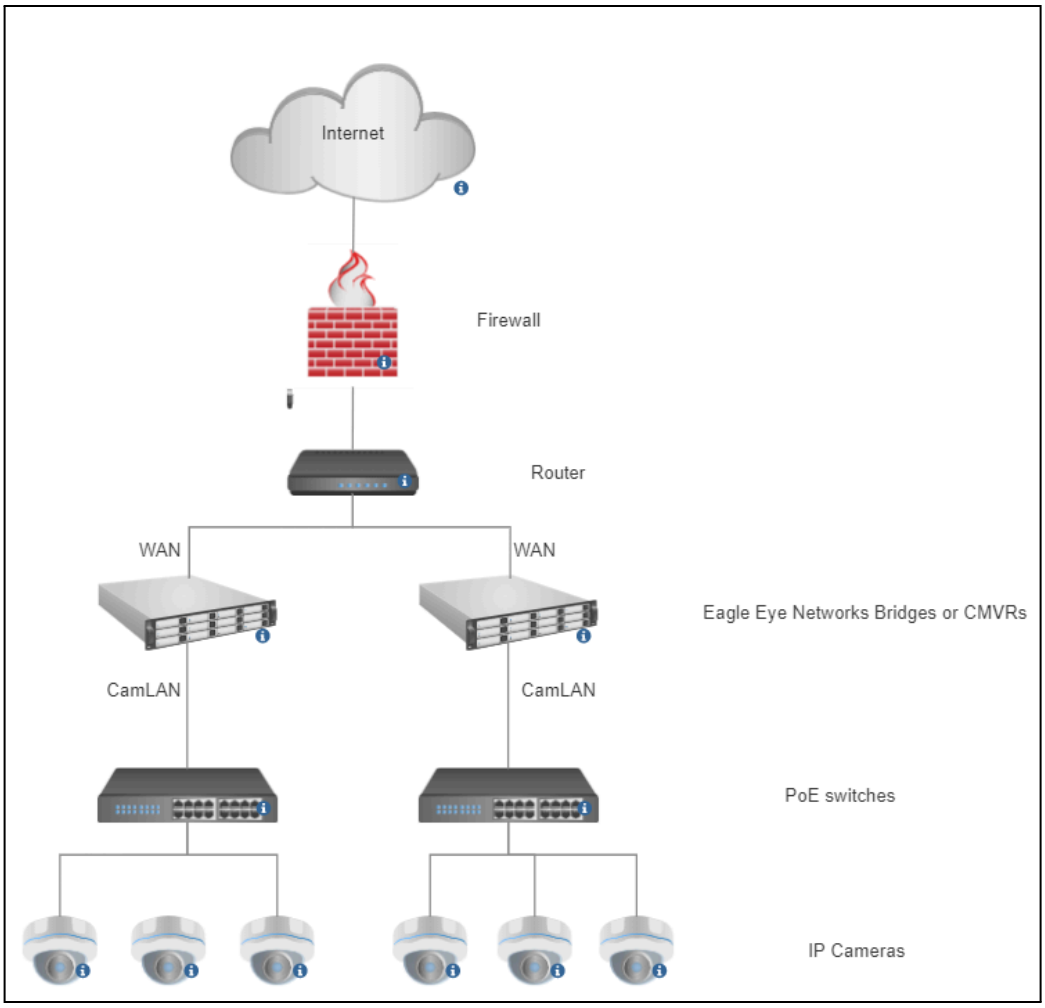
If the system is configured differently, and the bridge or CMVR is not supplied a sufficient amount of bandwidth, the likely side effect will be that devices will compete for the little bandwidth available, leading to loss of recorded footage or "purging."

Existing LAN architecture
Similar to the outgoing WAN bandwidth supplied by the ISP, some sites have multiple buildings across a large campus that utilize a backbone network sharing a single Internet connection. Also, some larger buildings utilize fiber backbones to span large distances to attach IDF's to the MDF. These types of networks are typically managed and have existing network traffic from the client. It is strongly suggested that the client's IT administrators confirm the amount of available bandwidth across those LAN segments. For example, if the end user is already utilizing 80% of their LAN backbone and a multiple bridge/CMVR arrangement requires 30% of the bandwidth, congestion and packet loss will occur due to the unavailable bandwidth. Cameras stream video almost all hours of the day, utilizing their required bandwidth. Also, any network, WAN or LAN, should never exceed 70–80% of its total capacity. Otherwise, this can lead to failures of the switches, which are not designed to run at 100% power constantly.

Design and Configuration of the CamLAN Network

To overcome any DHCP and IP address conflicts caused by deploying multiple bridge or CMVR devices at a single site, use one of the following CamLAN architectures:

1. **Segregated CamLAN networks for each bridge or CMVR**
   In this deployment, a separate and segregated CamLAN network is established for each bridge or CMVR device deployed on site, achieved by deploying separate power over Ethernet (PoE) switches. This deployment is typically used for flat unmanaged networks. Please see the following diagram for suggested deployment.



In a segregated CamLAN architecture the default CamLAN configuration can be used. It is typically not necessary to reconfigure the CamLAN interface; however, different factors may require a static IP address, such as system takeovers where the existing cameras all have static IP addresses and it is too burdensome to have to change them to dynamic. Load balancing should be considered in this type of layout if both bridges and CMVR devices reside in the same MDF. Carefully consider sensor size and duty cycle when balancing the cameras between bridges or CMVR devices.

2. **Managed network for all bridge and CMVR devices utilizing the same managed switches**
   In this deployment, all bridges and CMVR devices share a managed LAN network. This type of network requires the end user's IT administrator to assign IP addresses for every device on the network, including the CamLAN. This requires that each bridge and CMVR device receive its own unique static IP address for each CamLAN port. The CamLAN must also be set to static.

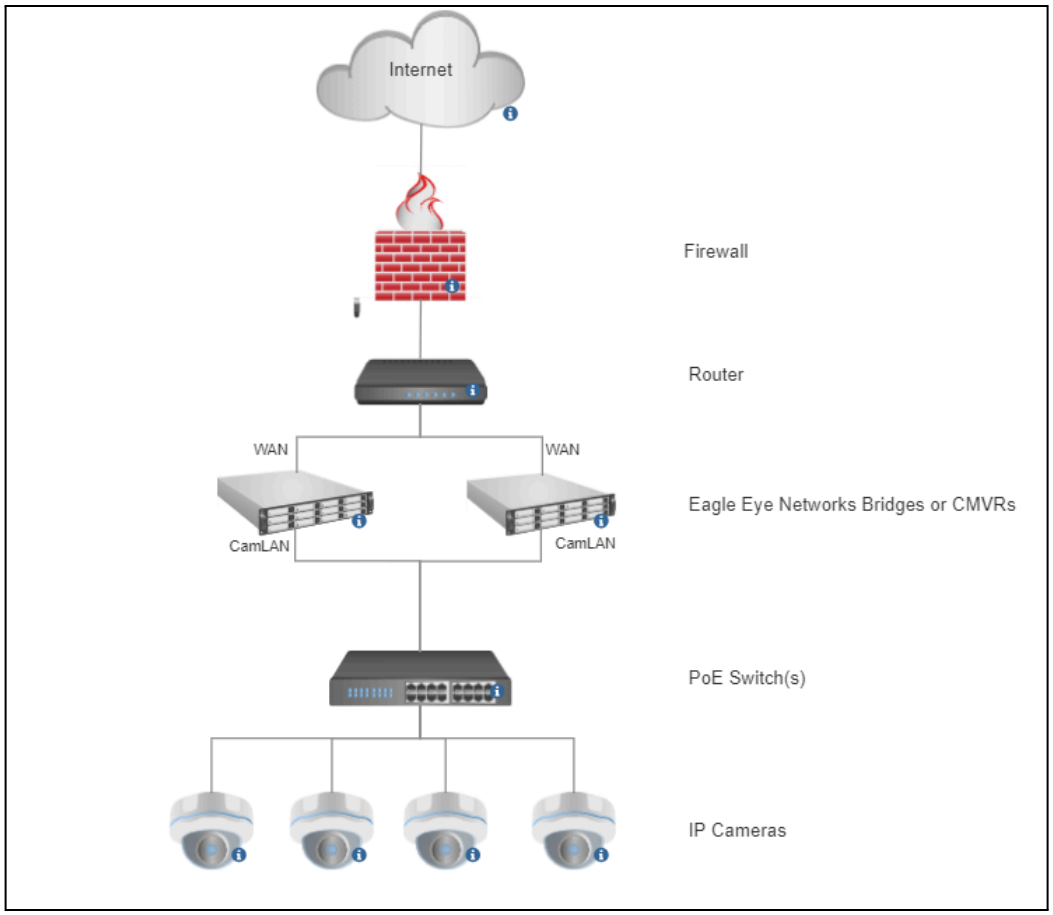
   Best practices dictate that these IP addresses be segmented into separate VLANs for each bridge or CMVR. This reduces confusion when all cameras, bridges, and CMVRs share the same subnet. When separate bridge, CMVR, and camera devices are placed on their own unique VLAN, it is easy to determine that a camera belongs to a particular bridge or CMVR,

which is necessary information for installation and service. With this type of application, cameras can physically share the same switch, while virtually being on separate networks.

As an example, a customer might have a fully integrated LAN network where all devices can be seen or “pinged” from any subnet or portion of the network. In a network with a single VLAN dedicated to the cameras, a camera in Building D can be seen from a computer or bridge in Building A. While that might seem beneficial, if Building A is four hops (switches) away from Building D and the camera from Building D is attached to a bridge or CMVR in Building A, the camera will fail or continually drop offline due to the latency across such a large network.

When deploying bridge or CMVR devices in a scenario such as this, contact your Eagle Eye Networks Sales Engineer for assistance and to learn about the best alternatives to projects that utilize end-user operated managed networks.

Please see the diagram below for suggested deployment:



Appendix

CamLAN: A secondary ethernet network port on the back of all bridges and CMVR devices. The CamLAN has a built-in DHCP server that dynamically distributes IP addresses to all cameras connected to it. The CamLAN is segregated and has no ability to connect to an outbound WAN network from the bridge or CMVR. This network port is meant exclusively to bring live camera feeds into the Eagle Eye Video Surveillance Software so they may be recorded and encrypted.

WAN: A wide-area network (WAN) is the technology that connects your offices, data centers, cloud applications, and cloud storage together. It is called a wide-area network because it spans beyond a single building or large campus to include multiple locations spread across a specific geographic area, or even the world.