IDIS

One Solution. One Company.

Essential installation guidelines for DR-8364 physical installation.

Table of Contents

1 <Background>

The DR-8364 is an NVR that can record up to 64 cameras, generating a lot of network traffic.

If all camera traffic is connected to one network interface, the port may not be able to handle all the traffic, or depending on the network installation, a Circuit / Loop will occur, causing the following problems:

-Video loss

-IP Camera disconnection

NVR boot failure

These issues are particularly relevant when using a DR-8364(64ch) NVR, and care should be taken when designing and configuring the camera network.

A few facts:

===

- In most NVRs, you have PoE ports + a single VIN port, and all these ports are effectively a single switch.

- In most cases, we advise a single separate cam subnet for each NVR

- If you have multiple NVRs and need to share a single camera subnet among them, extreme care should be taken to avoid creating or loop a circuit between the switches.

Loops will create a path over which broadcasting packets travel indefinitely flooding the cam subnet till it crashes.

* https://en.wikipedia.org/wiki/Broadcast_radiation

* https://en.wikipedia.org/wiki/Switching_loop

2 Solution #1 : Physically divide the camera connection.

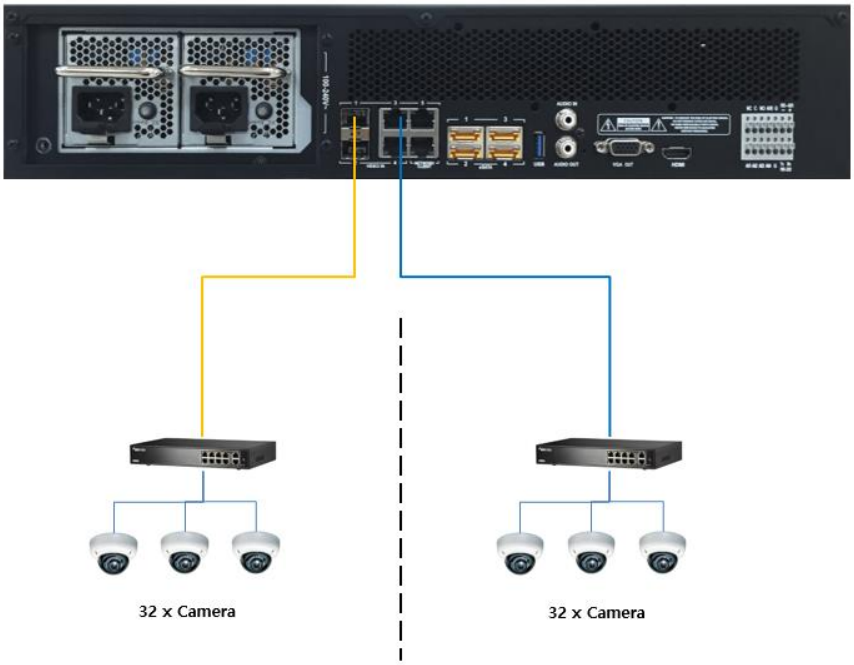
- The DR-8364 series NVR's come with multiple VIN ports (2 SPFs + 3 Gb Ethernet).

- Each Gb port can handle the payload of about 700Mbps incoming traffic. So if the total Live/Remote/Recording streams from all 64 IPCs are more than 700Mbps, then you should use two or more VIN ports with a separate switch on each port.

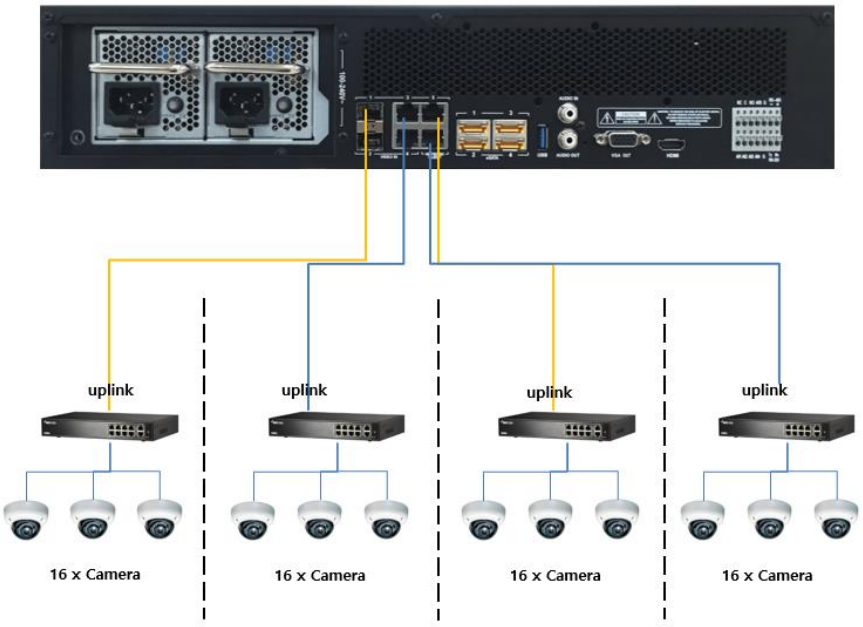
- In most cases that the peak incoming video traffic should not be more than 700Mbps if only 2MP H.265 cameras are used, but when using multiple H.264 or 5/8/12MP IPCs, the traffic can exceed 700Mbps during peak times, multiple motion events and many live viewers.

- In most cases you need at least two switches and balance the incoming traffic from the cameras. For example, cam 1~32 connected to PoE switch 1 and the uplink is connected to VIN1, and cam 33~64 are connected to another PoE switch 2 with its uplink is connected to VIN2 for. There should be no connection between switch1 and switch2 to avoid creating a switching circuit/loop mentioned above.

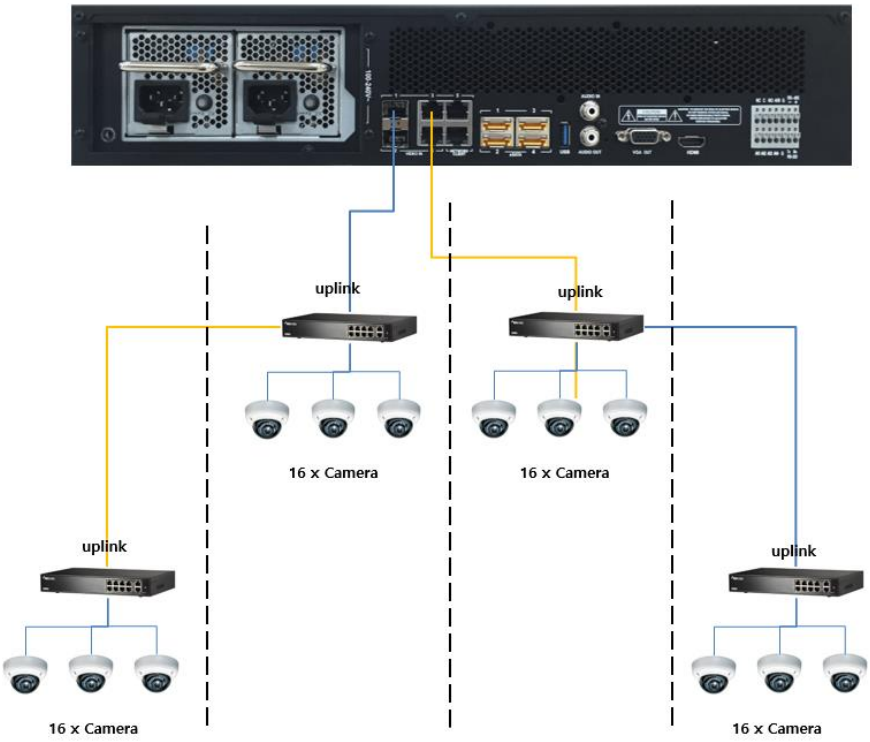
<Example #1>



<Example #2>



<Example #3>

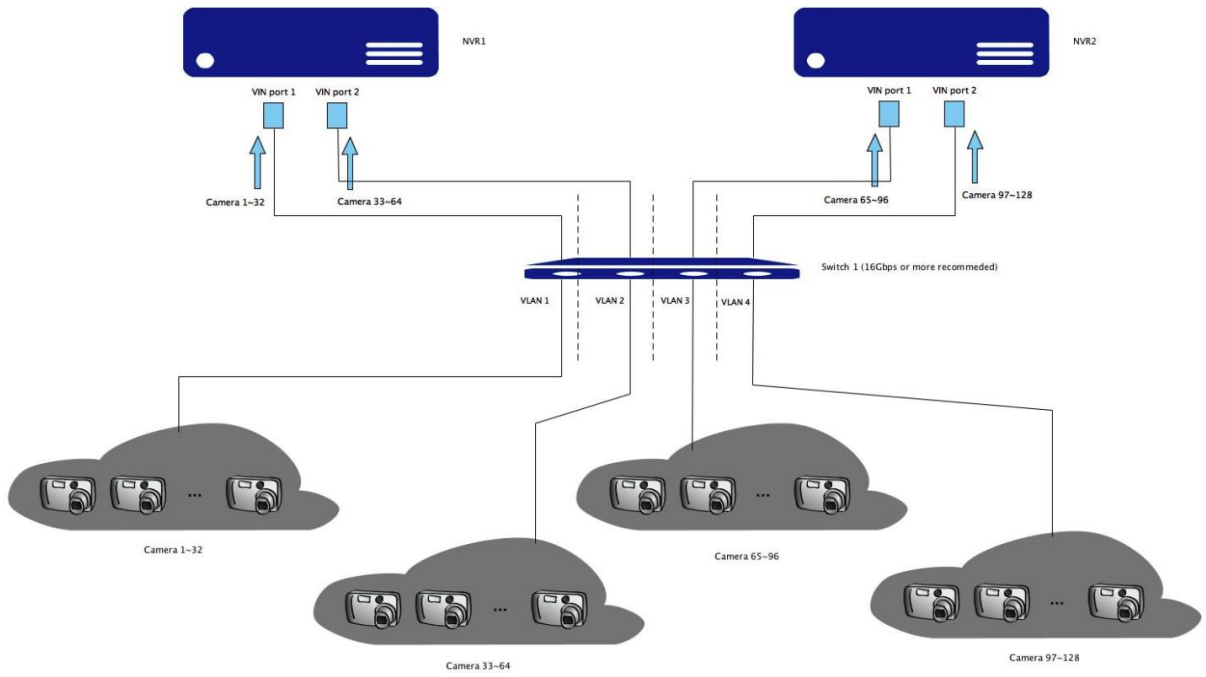

uplink
uplink
16 x Camera
16 x Camera
uplink
uplink
16 x Camera
16 x Camera

3 Solution #2 : use VLAN

- What if you have multiple DR-8364s and have to share the cam subnet?
- Because of the 700Mbps condition stated above, you should use VIN1/2 of each NVR to balance the incoming traffic, but this results in creating a switching loop/circuit in the shared camera subnet. So how can this be avoided?

- Fortunately, in most cases with a large number of cameras in the network, a managed network with managed switches are normally used. The camera subnets should be divided into **multiple separate VLAN segments**, and each VLAN assigned to a different VIN port, for example connecting/configuring VLAN1 => VIN1 of DR-8364-1 and VLAN2 => VIN2 of DR-8364-1, and VLAN3 => VIN1 of DR-8364-2 and VLAN4 => VIN2 of DR-8364-2 and so on. This is effectively the same as using separate switches for each VIN.
- Also take care to avoid creating bottlenecks in each VLANs over the switching fabric. Remember that each camera is streaming potentially 2~3 different streams for live and recorded video, so there is a high risk of potential bottlenecks.

<Example #1>



4 Solution #3 : use LACP (for NVR FailOver)

When IDIS NVR Failover is used (DR-8364(D)F) to provide FO for multiple NVRs, all the DR-8364(D)(F) have to share the camera subnet, and, so, the disjointed VLAN scheme will not work. The FO NVR DR-8364(D)F, must have access to ALL the cameras connected to ALL NVR's.

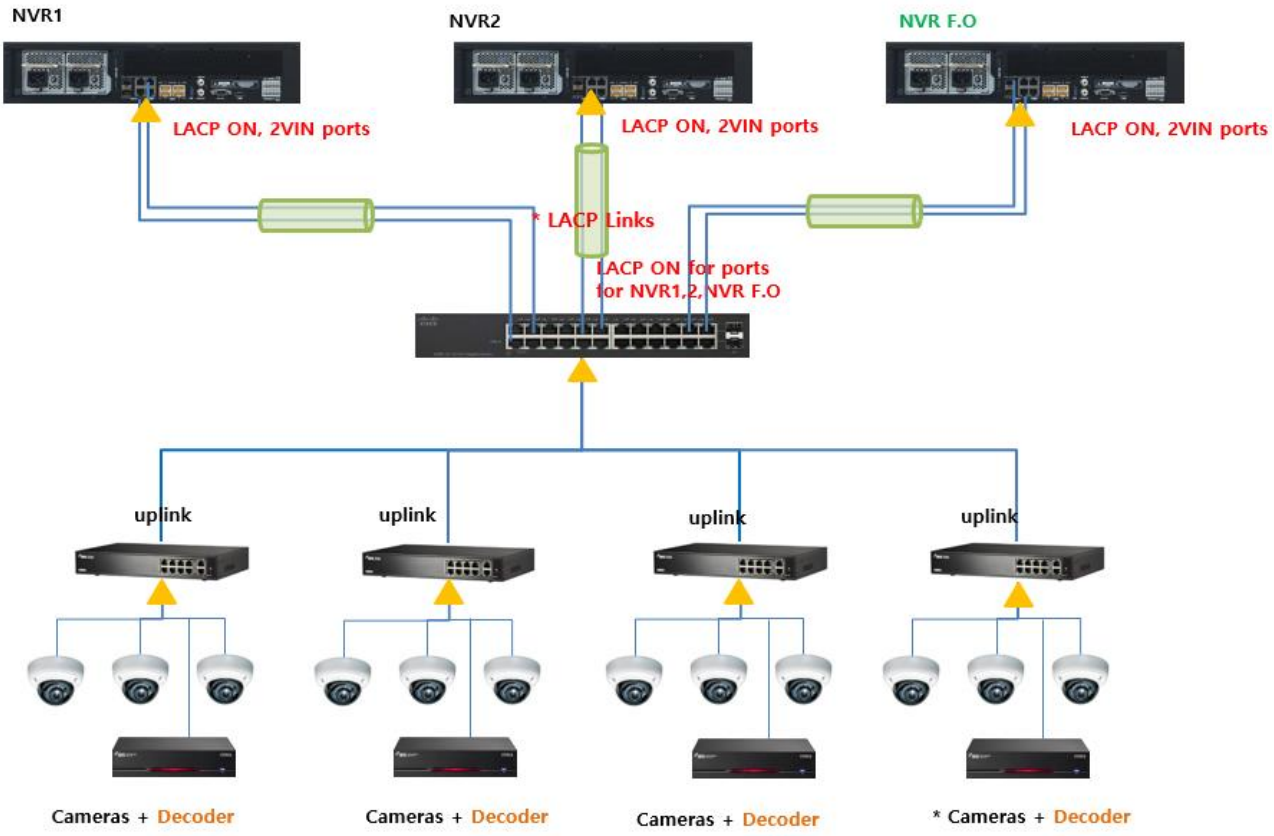
Thus, the VLANs cannot be defined/configured to be separate from each other.... so how can this be solved?

- Use the LACP/bonding (Link Aggregation) feature of the DR-8364(D)(F).
- Most managed switches should have the LACP/bonding feature to bond multiple ethernet connections providing higher bandwidth, load balancing and redundancy. https://en.wikipedia.org/wiki/Link_aggregation
- Once the managed switch is configured for LACP/bonding mode, then the NVR's VIN ports can be configured for LACP/bonding mode also. Then it is possible to connect 2 or more VIN ports to the same switch and increase the bandwidth.
- the bonded VIN1/2 can provide 2Gbps (~ 1400Mbps payload bandwidth), which is enough for any combination of cameras used for DR-8364s

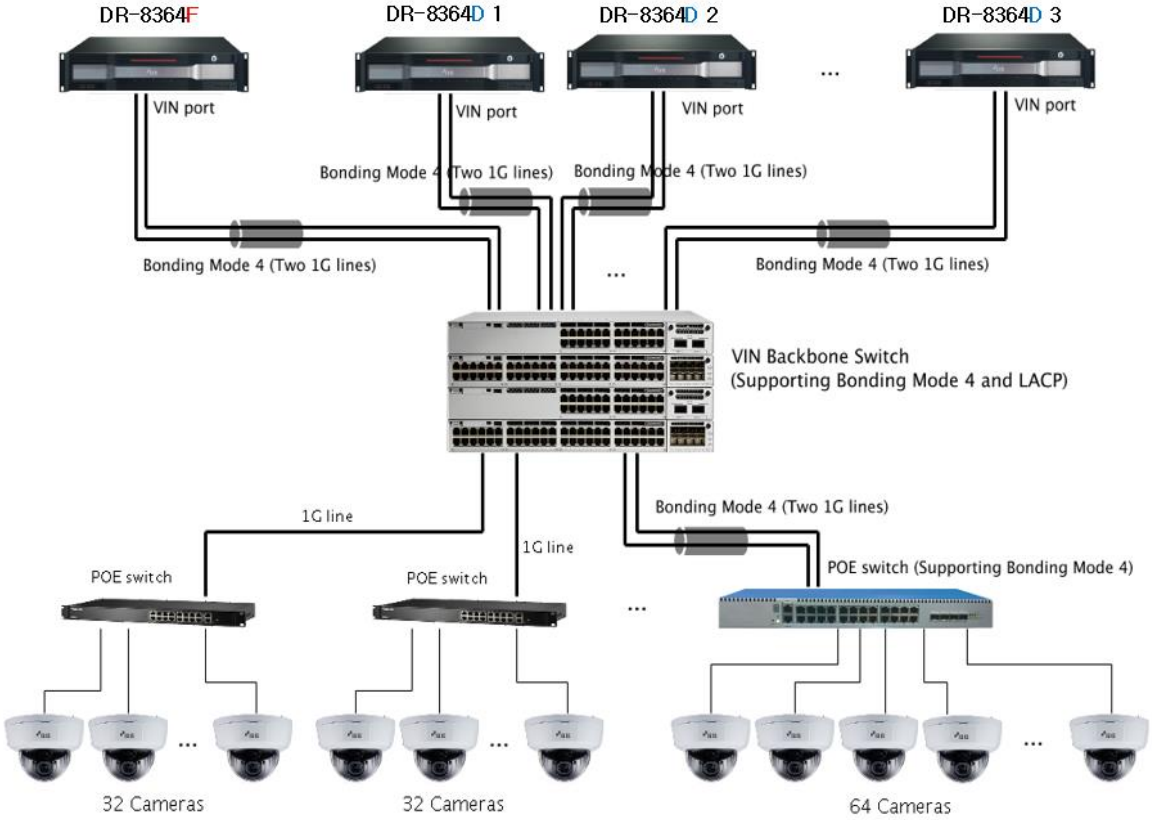
DECODER TRAFFIC

- When using the decoders, try and match the decoder switch connection to the same switch that connects the cameras displayed by the decoder. This will localize camera traffic to the decoders rather than carrying the additional traffic over the already congested network.

<LACP network Diagram #1>



<LACP network Diagram #2>



- The following two conditions dictates when a switch that supports LACP must be connected to the NVR, and bonding mode 4 / LACP must be configured respectively.

-If a BackBone switch is used between the camera switch and the NVR,

-If you use NVR Failover,

In both cases, there will be a BackBone switch, which must follow the conditions below.

* Recommended setting of switch connected to NVR

* Enable IEEE 802.3ad dynamic link aggregation function

* LACP function enabled and enable Bonding mode in the NVR VIN settings.

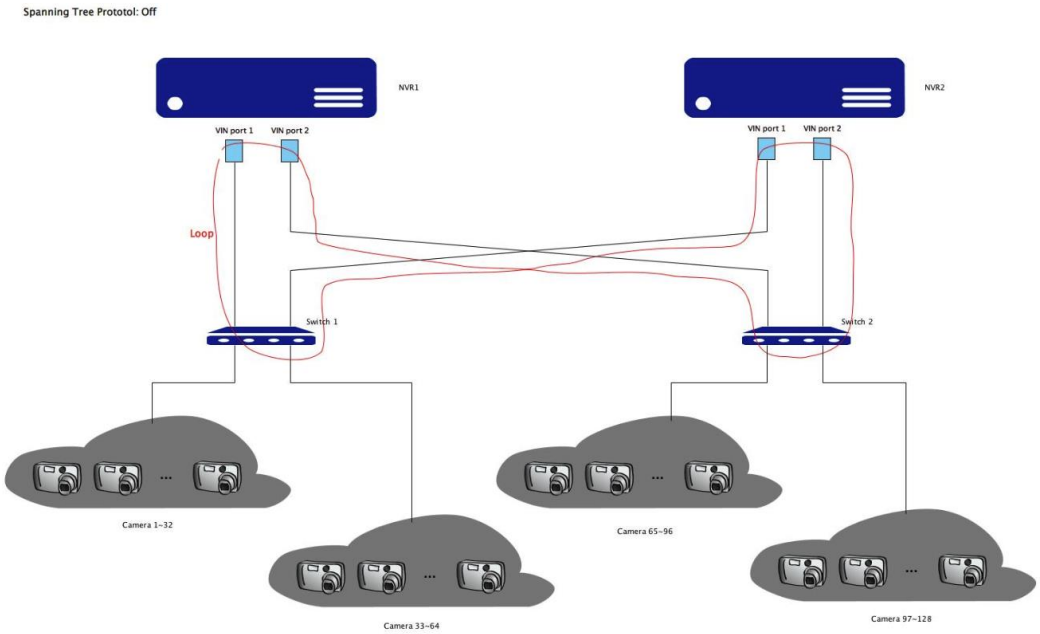
* The packet routing method is ‘srcmac’ (because it is a packet from a large number of sources (cameras) to a small number of destinations (NVRs) in most network loads).

(For SWITCH's LACP and bonding mode 4 settings, please contact your switch vendor.)

5 Appendix :

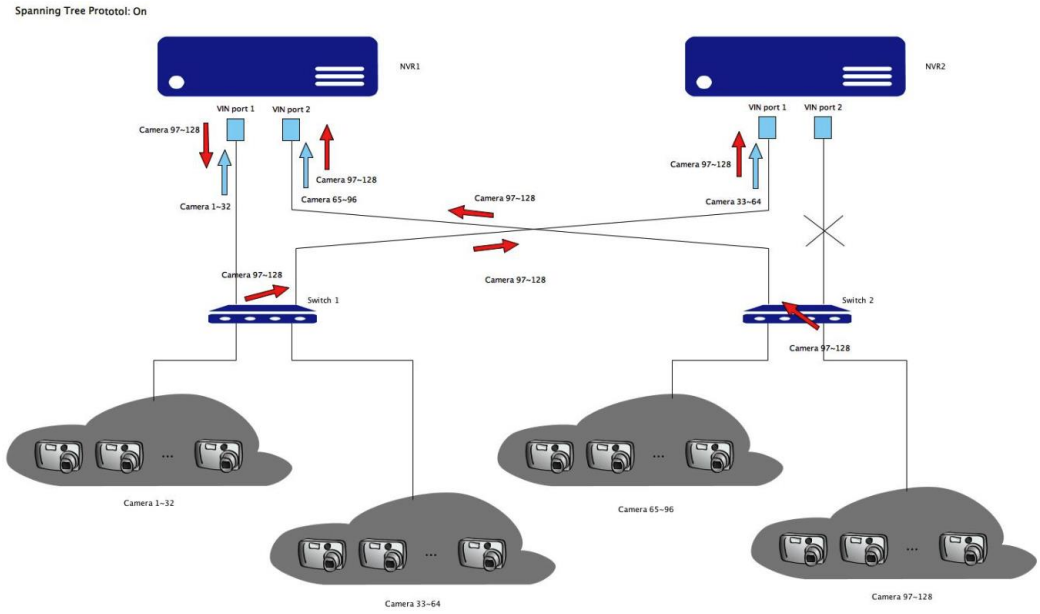
5.1 <Incorrect installation Case #1 : Circuit/Loop occurs – Spanning Tree Off>

The V-in port of the NVR also acts as a switch. If the network is installed as follows a Circuit (Loop) is created.



5.2 <Incorrect Installation Case #2: Unintended traffic causes network problems >

To prevent a Circuit/Loop, turning on Spanning Tree Protocol (STP), Communication can be lost in random zones. Unintentional excessive traffic can be generated as shown below.



Version History

Version	Writer	Revision Date	Remarks
1.00	Roy Lee	200113	Initial Release
1.01	Roy & Leon	200121	Modification of Diagram