Minimum Network Requirement
N-Series Product Guide

Introduction

As you investigate an N-Series solution and try to decide what type of network topology and infrastructure will be best suited for your application, some minimum network requirements must be considered when choosing the hardware to deploy a Networked AV system. The requirements presented in this guide cover the necessary protocols and features needed to drive an N-Series stream.

NOTE: Specific configuration recommendations given in this document are based on the Cisco Catalyst series switch. These recommendations could vary from manufacturer to manufacturer.

1. Managed Network Switch
2. Gigabit Ethernet (N1000/N2300, N2400, N2600, N3000, N3300D Based Systems)
3. Internet Group Management Protocol (IGMP) Version 2 or Version 3 for N2600 and N3300D Series
   - a. IGMP Snooping
     - i. Snooping must be enabled on all switches that are communicating with the querier.
   - b. IGMP Snooping Querying
     - i. The network must include at least one IGMP Querier to maintain stream connections.
       - 1. It is recommended to have all capable switches with the querier enabled and allow IGMP auto-elect to determine the Designated Querier (DQ).
         - a. The lowest IP-addressed switch determines DQ but can be manually assigned. However, this would need to be manually configured on all switches to bypass the auto-elect.
     - ii. Query interval – 30s
       - 1. Interval between sending IGMP general queries.
     - iii. Query Response Interval – 10s
       - 1. The maximum time the system waits for a response to general queries.
     - iv. Last Member Query Interval – 100ms
       - 1. The interval to wait for a response to a group-specific or group-and-source-specific query message.
     - v. Immediate Leave (required for all N-Series devices)
       - 1. Used to immediately break up multicast groups when a leave message is received.
       - 2. Immediate Leave will break any daisy chaining of multiple units together with a single home run and as such you will not be able to have both Immediate Leave and daisy chaining in the same VLAN.
       - 3. Some manufacturers do not have Immediate Leave as an option and use Fast Leave instead.
         - a. Fast Leave does not guarantee an immediate leave from the multicast group and can affect switching speeds and performance.
     - vi. Optional Protocols
       - 1. IGMP Robustness – Default 2
         - a. Robustness can be adjusted generally from 2-10. The higher the value, the more leave latency is added.
         - b. This protocol is effectively inactive when Immediate Leave is enabled.
   - c. Warnings/Notices
     - i. There is a known behavior within IGMP V2 that Encoder streams, whether requested across an uplink or not, will be requested by the DQ and will be present on the uplinks of all switches between the stream source switch and the DQ.
       - 1. Essentially, this means that even though you may not be routing a stream to another switch, the DQ's request will still put the stream on the uplink. Therefore, ensure that you have accounted for all streams forwarding to the DQ.
       - 2. A good rule of thumb, when planning for bandwidth considerations on uplinks, is not to exceed 80% of the uplink's total bandwidth capacity to give plenty of overhead for spikes and additional traffic.
       - 3. Multicast routing capabilities on each switch (configured for PIM-SM and with an established rendezvous point) can be designed to limit or mitigate this behavior.
     - ii. When a multicast host leaves a group, it sends an IGMP leave message. When the switch receives the leave message, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message and starting a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router/querier switch. Lower interval times will increase bandwidth utilization slightly as querying will happen more often.

iii. Unregistered multicast traffic should be prohibited on network ports to enhance the protection of devices that are being inundated with unregistered multicast traffic.
1. Switchport block multicast is the command Cisco Catalyst network switches use to prevent unregistered multicast traffic from flooding a device that is not attempting to subscribe.

4. Protocol Independent Multicast (PIM)
a. Used to route multicast between VLANs
b. PIM Source-Specific Multicast (PIM-SSM)
i. Requires IGMPv3
ii. Only compatible with N2600 and N3300D when those devices are configured to use IGMPv3.
c. PIM Sparse Mode (PIM-SM)
i. Recommended for use with N-Series multicast products.
ii. PIM-SM uses a pull model to deliver multicast traffic. Only network segments with active receivers explicitly requesting the data will receive the traffic.
iii. Requires configuration of a Rendezvous Point (RP).
1. Must be configured by the administrator.
2. Similar to the DQ in IGMP.
3. All multicast sources must register with the RP to be able to be routed throughout the network.
d. Other PIM modes – not recommended for N-Series
i. Dense Mode (PIM-DM)
ii. Bidirectional (BIDIR-PIM)
e. The N2300 Series is not compatible with PIM

5. Jumbo Frames Enabled (For N2300 and N2600 Series)
a. The N2300 and N2600 Series Encoders and Decoders produce a frame payload larger than 1500 bytes.
i. Recommended to be set to a minimum of MTU of 9000

6. Quality of Service (QOS): Managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution.
a. Not required for use with N-Series devices
b. Policing
i. A policer typically drops traffic.
ii. Differentiated Services Code Point (DSCP) values can be configured in N-Series devices if QOS is required on the network.
c. Shaping
i. A shaper typically delays excess traffic using a buffer, or queueing mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected.
ii. Cannot be used with the N2300 series.

7. TCN Flood Off
a. TCN (Topology Change Notification) flooding will cause unnecessary backplane and bandwidth usage when adding or removing a device on the network, which can cause stream interruptions as the flooding sweeps through the network.
i. Note that this command must be assigned individually per port that is assigned to that VLAN. However, it is not necessary to have ports on the same switch that will not be set up on the same VLAN as the N-Series devices.
b. Command Example: NO IP IGMP SNOOPING TCN FLOOD