Failover Strategies for Micro Local™ Cameras – Best Practices

By Dan Desjardins – Director/Owner Videstra LLC

“Hardware: The parts of a computer system that can be kicked.” - Jeff Pesis

When Bad Things Happen to Good System…

As you integrate live local cameras (aka Micro Local Cameras) and shared camera feeds into your live newscasts, the Videstra system is designed to streamline and unify the workflow ensuring the best possible on-air product. One area that remains a risk, though, is the often-unreliable Internet connections between the cameras and the station or Videstra CloudShare systems. The Videstra system is designed to manage these risks as well. This paper provides a high-level technical background on these processes.

Many failover strategies involve having backup technology at-the-ready. With Micro Local cameras it's not practical to do this – it would more than double your cost and would provide a true failover in only a very small number of cases. Since Micro Local camera streams are delivered over the public Internet or private WAN connection – creating a backup isn't feasible. The common practice of eliminating (or reducing) the number of *single points of failure* while noble, is not always reasonable. There is a technical truth to this approach:

> *You can not eliminate any single point of failure; you can only move it.*

The important part of a failover strategy then becomes one of preparedness. Being prepared with the right information can be the difference between a short and relatively easy, or long and arduous recovery time.

The Videstra system design offers a variety of automated technologies to restore connections while providing ongoing notification to the appropriate station personnel and status indicators to the operators.

There are, essentially, six **Categoryes** of connection-types to cameras being managed by the Videstra system:

Failure Category	Category Definition
Category 1	**Cameras owned by a station and connected directly to the Videstra system via a station owned/managed Internet connection** • There is a full resolution connection from the camera to the station's local Videstra system • Any cameras shared to the group require a secondary (low-bandwidth connection to the camera for CloudShare™
Category 2	**Cameras owned by a station and connected to the Internet using a 3rd party's Internet service (such as a client, government body, or a friendly source)**
Category 3	**Cameras owned by a station and connected over a local LAN** • These are typically on-site cameras at the station
Category 4	**Cameras owned by a station and connected to Videstra through Videstra Camera CloudShare™**
Category 5	**Cameras *not* owned by the station that have been shared from other stations in a group**
Category 6	**Cameras owned by third parties for which you have permission to use**

With Videstra, failures can trigger one or more of the following events automatically through the Videstra system:

1. Automatic notification of the failure to an individual, multiple individuals or group via email or text message
2. Automatic reboot of camera
3. Automatic reboot of all equipment at remote demarc
4. Manual reboot of camera
5. Manual reboot of all equipment at remote demarc
6. Manual retry on Internet connection (though this is generally unnecessary)

Failover Strategies (by Category)

Category 1 Connection Failover

A failure in this category means either the camera hardware has failed, or the on-location Internet connection is compromised. If either automatic or manual reboots of equipment do not correct the issue, then a Category 1 connection failure falls to an engineering maintenance issue. As such correction can only be done by directly addressing the failure by repair or replacement of hardware or re-establishing the Internet connection through standard troubleshooting methods such as:

- Rebooting/restarting remote equipment.
- Reflashing remote equipment

The problem with troubleshooting is that trouble often shoots back…
A cynical, but wise engineer

Category 2 Connection Failover

This is the same as Category 1 except you will need to deal with the owner/manager of the 3rd party Internet connection. This can be considerably more difficult – which is why you should use caution when using another party's Internet connection for a service you may become reliant upon. At the very least you will require the following:

- Name and phone number of person(s) responsible for the third-party Internet service/demarc
- Additional on-site contacts of people who might be available to "pull the plug" to force a complete restart of the equipment at the demarc if required
- Keep the above current – after a year or more the players often change
- Have an agreement in-place on use of the service so that it is considered more than a "favor" to the station. For this to be effective it is best to offer on-air recognition of the arrangement.

Category 3 Connection Failover

This is likely the least concerning for failover recovery because everything is under the control of your own engineering and/or IT department.

Category 4 Connection Failover

If a failure occurs within the Videstra Camera CloudShare the failover procedure is simple and quick. Any camera owned by a station can connect either through CloudShare or directly. If connection to a camera through CloudShare is lost it is possible to completely bypass Camera CloudShare and establish a direct connection within less than one minute by simply switching the connection method in camera panel settings.

Category 5 Connection Failover

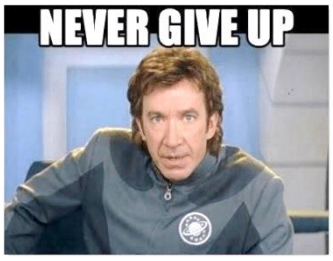
Videstra does not currently offer a Category 5 Connection failover strategy. Any Category 5 Connection failure is a maintenance issue for either Videstra Customer support and/or the owner of the shared camera.

Category 6 Connection Failover

Simply make sure you have full contact information of people to contact when a camera in this category stops working. It is common for cameras in this category to have their IP Addresses change, ports closed, etc.

How the V-Streamer/V-Manager Cope with Failures

There is a philosophy regarding the way the V-Streamer maintains a connection to a remote stream endpoint.



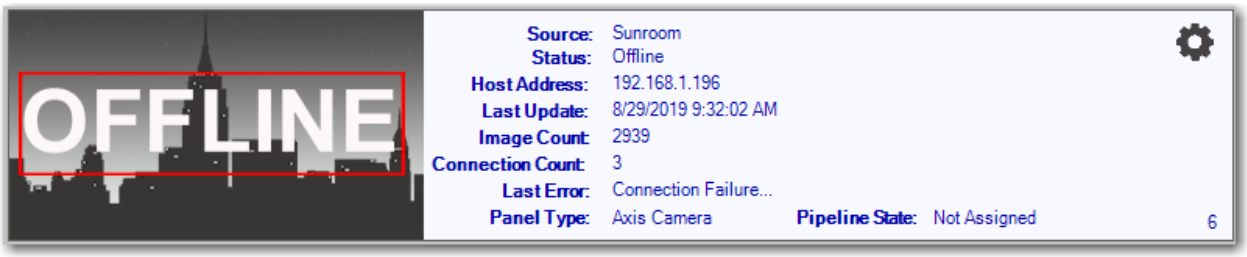
*

The V-Streamer™ Will Never Give Up!

**Galaxy Quest is Copyright 1999, Dreamworks Pictures*

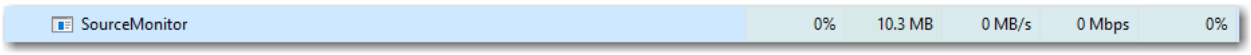
While it is common for some devices to limit the number of times it retries a connection (usually to save bandwidth/CPU/memory resources) – the V-Streamer has been tuned so that it will continue to retry an assigned connection as long as it is powered up. This typically means that transient disconnections are automatically recovered – *even if it takes minutes/hours/days or weeks*.

Likewise – the V-Manager also has a similar philosophy and *Never Gives Up*, but there is one small difference. The V-Manager application does take a disconnected source OFFLINE after a definable number of failures (Defined in V-Manager settings).



A Troubled Source Taken Offline by the V-Manager

However, the V-Manager automatically starts a background process (Called SourceMonitor) that polls the source once per minute checking for signs of life.



The Videstra SourceMonitor as it Appears in Task Manager

If a source becomes available, the SourceMonitor will tell the V-Manager to automatically reconnect to that source and put it back on-line.

> **Note:** *There may be multiple SourceMonitors as a new one is started for each source that becomes disconnected*.

A simple chart you should keep for each remote location

IP Access Information of all equipment at the demarc

Site Location (Address, company name, etc)

_____

_____

_____

_____

_____

Device	**Make/Model**	**Credentials**	**Local IP Address**	**Ports**
Public IP Address				
Camera				
Router				
IP Power Switch				

Contact names (at least three names)

Name	Responsibility	email	Office Phone	Mobile Phone