Layer 3 Enhanced Network Switch

Installation Guide
Contents

Introduction .................................................................................3
Important Safeguards .................................................................5
Installing The Unit ...................................................................7
Configuring the Unit ................................................................16
Example Configurations .........................................................24
Appendix A - Detected Camera Defaults .................................32
Appendix B - FoxyBonjour .......................................................33
Index ......................................................................................34
Introduction

Dedicated Micros is proud to unveil its ground breaking Closed IPTV system and Integrated Layer 3 Enhanced CCTV Switch.

Applying the long-established formula of traditional CCTV to the IP environment – Dedicated Micros’ Closed IPTV solution makes deploying an IP CCTV system safe, secure and simple. Combining patent-pending technology with existing networking protocols, Closed IPTV removes the need to laboriously configure IP addresses of individual components. Simply Power up, Plug in and the system is ready to operate.

Once all products are connected together the system is completely deterministic; discovering and assigning IP addresses to IP cameras automatically and associating them with a specific network port so they cannot be hacked or intercepted. This ground breaking solution provides a secure answer to video over IP networks - requiring little prior knowledge of IP network configurations.

Closed IPTV is hack protected by the way the routing of the networked video is exclusively managed and tracked through the integrated Layer 3 Enhanced CCTV Switch, making it extremely difficult for any hacking tool to identify and intercept the streams.

A crucial component in Dedicated Micros Closed IPTV solution – the Layer 3 Enhanced CCTV Switch offers a simple plug and play solution for IP cameras. Specifically designed for IP CCTV networks the switch provides a zero configuration solution for IP cameras allowing installers to deploy a safe, secure and simple IP CCTV solution.

Combine your existing installed analogue cameras with secure IP and HD cameras from a Closed IPTV system by simply adding a Layer 3 enhanced CCTV switch. Connecting a Layer 3 Enhanced CCTV switch to an existing Closed IPTV ready system, such as an SD Advanced, allows it to be quickly and easily expanded.

Alternatively, cascading multiple switches together enables the Closed IPTV system to grow incrementally, all the time retaining its secure capabilities thanks to its unique Closed IPTV technology.

Features

- Plug and play, secure, IP video product solution
- Deterministic IP camera assignment to network port
- Provides all the physical security of a traditional Closed Circuit TV system – over IP!
- The essence of simplicity – just connect the cameras to the NVR or Layer 3 Enhanced CCTV Switch and the system will automatically assign IP addresses to the IP cameras
- Removes the headaches of a traditional IP CCTV installation such as configuring firewalls
- Requires no manual configuration of IP addresses
- Standard or High Definition cameras supported
- Lock down cameras to specific network ports to ensure security

Security Protection

Rogue Device Access
Camera ports on the Layer 3 Enhanced CCTV Switch switch can be locked to the MAC address of the camera connected to the port. This prevents casual access by rogue devices from this port to the rest of the system (NVR and other cameras).

Rogue Device Access with MAC spoofing
More sophisticated attackers could bypass the Layer 3 Enhanced CCTV Switch MAC address rules by spoofing the MAC address of the camera connected to the port. The Trusted Endpoint feature identifies such attackers through video signature verification.
Injection of Rogue Video
Trusted Endpoint prevents new video being generated by rogue devices, as they are unable to sign the video correctly, resulting in detection by the receiving NVR. This is a distinct advantage over analogue systems in which analogue camera signals can be easily replaced.

Camera Port to Camera Port: Comms
Switch rules prevent access between two camera ports, acting as a hard firewall to stop Denial of Service or other attacks on cameras in a different location. This prevents a camera in a public location from affecting a camera in the safe vault.

AutoIP Address Bounce: Camera Denial of Service (DoS)
AutoIP Address Bounce includes a conflict resolution system to detect and deal with two devices selecting the same IP address. This technique could be used to temporarily or permanently DoS a camera, even on a different port, by a rogue device permanently claiming to own any IP address which the camera tries to use.

AutoIP conflict detection can still occur while the system is in configuration mode, but once locked down, a rogue device cannot change the IP address of a camera on a different port, even if mDNS names are used.

AutoIP Address Bounce: NVR Denial of Service (DoS)
A rogue device on a camera port could bounce the NVR off its AutoIP address in a similar manner to camera DoS above. This is prevented by disabling AutoIP conflict resolution on the NVR while in lockdown mode.
Important Safeguards

Read Instructions
All the safety and operating instructions should be read before the unit is operated.

Power Sources
This unit should be operated only from the type of power source indicated on the manufacturer’s label.

Servicing
Do not attempt to service this unit yourself as opening or removing covers may expose you to dangerous voltage or other hazards.
Refer all servicing to qualified service personnel.

Ventilation
Ensure unit is properly ventilated to protect from overheating.
All the safety and operating instructions should be read before the unit is operated.

To prevent fire or shock hazard, do not expose this equipment to rain or moisture. The lightning flash with arrowhead symbol within an equilateral triangle is intended to alert the user of this equipment that there are dangerous voltages within the enclosure which may be of sufficient magnitude to constitute a risk of electric shock.

WARNING
This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Lightning Strike
The unit has some in-built protection for lightning strike, however it is recommended that isolation transformers be fitted to the system in areas where lightning is a common occurrence.

Regulatory Notes and FCC and DOC Information
(USA and Canadian Models Only)
Warning: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

If necessary, the user should consult the dealer or an experienced radio/television technician for corrective action. The user may find the following booklet prepared by the Federal Communications Commission helpful: “How to Identify and Resolve Radio-TV Interference Problems”.

This booklet is available from the US Government Printing Office, Washington, DC20402, Stock No. 004-000-00345-4.
This reminder is provided to call the CCTV system installer’s attention to Art. 820-40 of the NEC that provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

CE Mark

If this product is marked with the CE symbol it indicates compliance with all applicable directives. Directive 89/336/EEC.
A ‘Declaration of Conformity’ is held at Dedicated Micros Ltd.,
1200 Daresbury Park, Daresbury, Cheshire, WA4 4HS, UK.
Installing The Unit

Front Panel connections

**ETH-A**  
RJ45 Gigabit Ethernet socket for Closed IPTV control.

**ETH-B**  
RJ45 Gigabit Ethernet socket for General Corporate network connection.

**ETH-C**  
RJ45 Gigabit Ethernet socket for Closed IPTV cascading.  
*Used for cascading multiple switches.*

**ETH-D**  
RJ45 Gigabit Ethernet socket for zero-conf.  
*Used for cascading multiple switches but also could be used for;  
Connect laptop to communicate with cameras over closed side of the network. This is an engineering function.  
Ethernet mirror port, this can be used to view traffic on other ports including public port. This is a monitor function.*

**Private video LAN, this is used for inter connectivity several NVRs which can access data from each other without going on the general corporate network.**

**10/100 Network Ports 1-16**  
RJ45 camera connection ports x16

Rear Panel connections

**DM/NSW/CP**

**Power**

**POWER**  
12v DC Power Socket
Power

POWER

48v DC Power Socket - Supplies power for Power Over Ethernet (POE) function on DM/NSW/CPP

Base Panel

Address

Address Switch

Rotary address switch settings 0 - F (16 addresses)
Step 1 - Set the switch Hardware identifier
There is a rotary switch on the base of the Layer 3 Enhanced CCTV Switch used by the NVR to identify the unit.

- The first external switch attached to an SD Advanced should be set to ‘0’, the next one set to ‘1’ etc.

Step 2 - Connecting the Layer 3 Enhanced CCTV Switch to a compatible Dedicated Micros NVR

Connect the Layer 3 Enhanced CCTV Switch to the NET socket on the back of the Dedicated Micros NVR (being used for control/configuration purposes) via a CAT5 Ethernet cable.
By default the Ethernet port labelled ‘ETH-A’ is designated the ‘Closed IPTV control’ port. The Closed IPTV control port is intended to securely link the Layer 3 Enhanced CCTV Switch to the Dedicated Micros NVR.

Step 3 - Connecting Power to the Unit
The connected NVR will automatically discover the switch once power is applied.

DM/NSW/CP

Use the supplied 12vDC power cable to connect the 12vDC power socket on the rear of the unit to a local power source.
DM/NSW/CPP (POE Version)

Use the supplied 48vDC power cable to connect the 48vDC power socket on the rear of the unit to a local power source.

**NOTE:** The 48vDC power socket will only be available on the Power Over Ethernet (POE) supporting model

To be compliant with wiring regulations in some countries, an Alarm/Security device should be connected to a fused spur and not a wall outlet socket (check local regulations before installation).

**Step 4 Connecting the Unit to the General Network (optional)**

*ETH-B is provided for connection to the General Corporate network.*

If the NVR and Switches are going to be configured using a local monitor and USB mouse into the NVR, this connection to the corporate network will be used for viewing only and does not need to be made until configuration is complete and the system is secure. This connection is only required if the NVR and Switches are going to be configured using a PC on the General Corporate network.

If all configuration will be carried out using the local interface, and viewing over the General Corporate network is not required, this step is not needed. The NVR assigns DHCP addresses to the connected cameras from its built in DHCP server, making connection to the General Corporate network unnecessary.

**Important:** If the cameras connected to the NVR are exposed on the General Corporate network (i.e. ETH-B will be left as visible), the Closed IPTV SD Advanced unit must be in Configure mode to find any existing units on the network that have addresses within the range it can automatically assign. It can then give suitable IP addresses for new cameras, avoiding potential IP address clashes.
Use a CAT5 ethernet cable to connect ETH-B on the Layer 3 Enhanced CCTV Switch to a suitable network port to make it available on the network, or to the router provided by your Internet Service Provider (ISP), please consult documentation provided by your ISP for guidance on connecting the CAT5 ethernet cable to the router. The NVR is DHCP capable by default and can obtain an IP address on the General Corporate network (if a DHCP server is present). Otherwise a static IP address can be set on the NVR Network -> Network configuration page. The NVR has a built in proxy server that generates the addresses for connected cameras, DHCP will not be used to allocate addresses to the connected cameras.

**Step 5 - Connecting a Camera to the Unit**

All variants of the SD Advanced can provide up to 32 Closed IP video channels. The SD Advanced 8 can provide up to 32 Closed IP video channels OR up to 8 analogue video channels and 24 Closed IP video channels. The SD Advanced 16 can provide up to 32 Closed IP video channels OR up to 16 analogue video channels and 16 Closed IP video channels. The SD Advanced 32 can provide up to 32 Closed IP video channels OR up to 32 analogue video channels OR up to 32 Closed IP video channels.

<table>
<thead>
<tr>
<th>Analogue</th>
<th>Recode/IP</th>
<th>NetVu</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD Advanced 8ch</td>
<td>8 or</td>
<td>8 or 32</td>
</tr>
<tr>
<td>SD Advanced 8ch</td>
<td>8 or</td>
<td>8 and 24</td>
</tr>
<tr>
<td>SD Advanced 16ch</td>
<td>16 or</td>
<td>16 or 32</td>
</tr>
<tr>
<td>SD Advanced 16ch</td>
<td>16 or</td>
<td>16 and 16</td>
</tr>
</tbody>
</table>

Analogue channels can be utilised by the BNC connections on the back of the unit OR by the sockets on the switch. If an IP source is plugged into a channel occupied by a BNC connection, the BNC will take priority and possess the channel, whilst the IP connection will be added to an unallocated cameras list, allowing it to be tied to an available channel through the configuration pages.

Connect the video sources to the Layer 3 Enhanced CCTV Switch. Connect each video source using an RJ45 link cable. Individual cameras should be connected in sequential order, i.e. connect the first camera to port number 1 on the Layer 3 Enhanced CCTV Switch. When this connection is registered by the NVR, it will display a notification on the Main Monitor showing the recognised details of the new video source, including resolution, name and MAC address. There will also be a notification if a camera is disconnected.
Configuring Closed IPTV

It is only possible to change Closed IPTV settings when the connected NVR is in Configuration mode (Closed IPTV->Settings). The Closed IPTV logo in the top corner of the configuration pages gives a quick indication of whether the system is in Secure or Configuration mode. On initial boot, the NVR will default to Configuration mode.

Secure Mode

Configuration Mode

Note: If an IP camera is connected to a channel occupied by an existing BNC connection, it will be recognised but not assigned as the BNC connection will take priority. It will instead be added to an unassigned list of cameras, which can be tied to a channel in the configuration pages.

Note: If a BNC camera is connected to a channel occupied by an existing IP connection, the BNC connection will take priority. The IP connection will be dropped and added to an unassigned list of cameras, which can be tied to a channel in the configuration pages.
Camera Allocation

When the Layer 3 Enhanced CCTV Switch recognises the server.

- The available channels (those without Analogue or IP connections) on the Layer 3 Enhanced CCTV Switch are categorised as Port Free. 'Connected' analogue channels are categorised as taken (this status is displayed on the Closed IP Settings configuration page on the NVR).
- Port Free channels are available for Auto-IP connection of NetVu Connected source.

The camera details are auto-detected and passed to the controlling NVR which will apply a default recording profile based upon the detected details. This recording profile can then be amended in the NVR configuration pages.

If more than 16 IP camera connections are needed an additional Layer 3 switch can be connected to Ethernet port (ETH-C) which is the ‘Cascade’ port, refer to ‘Connecting an Additional Layer 3 Enhanced CCTV Switch’ for further guidance.

Multi channel encoder camera allocation (DV-IP NV1)

A NetVu Connected multi-channel server can be can be added to any of the camera ports as a video source. The available channels are then allocated as follows:

As the Layer 3 Enhanced CCTV Switch detects video sources on the NetVu Connected multi-channel server it allocates them to consecutive Port Free channels, starting at the port on which the video source is added.

If the process encounters a channel that does not have “Port Free” status then the video source will be added to the un-allocated list; consecutive cameras will only be applied to channels that are Port Free.

For example the Layer 3 Enhanced CCTV Switch has channel ports 1,3,4 listed as Port Free, 2 is an Analogue camera. If one 4 channel ICR encoder is added to camera 1. The result is;

- ICR Encoder - Camera 1 -> Camera 1 NVR
- ICR Encoder - Camera 2 -> Unallocated, Cameras
- ICR Encoder - Camera 3 -> Camera 3 NVR
- ICR Encoder - Camera 4 -> Camera 4 NVR.
When a multichannel encoder is connected to the Layer 3 Enhanced CCTV Switch, the NVR will receive information from the encoder about how many cameras are connected. Channels set as Not Connected on the encoder, when presented to the Enhanced Layer 3 switch will not be eligible for Auto IP.

In the scenario shown below, the NVR is set at defaults and the Layer 3 Enhanced CCTV Switch has an ICR encoder with three analogue camera inputs connected at positions 1, 3 and 4. Position 2 is not used. The Closed IPTV NVR would be auto configured on four consecutive ports, camera 2 would not be allocated to port 2, instead port 2 would be registered as assigned to a failed camera.

Analogue channels take precedence. If an analogue camera is present and connected to analogue port 2, the channel needs to be set to ‘Not Connected’ on the Closed IP NVR configuration pages to avoid the ‘failed’ camera being de-allocated.

The de-allocated cameras are added to the Camera->Unallocated Cameras page on the NVR, which shows a tabulated list of all unallocated cameras connected to the switch, showing all the camera details (DNS, Auto IP Address, MAC, Classification, Channel number and Native resolution). Each camera has a drop down list showing all ‘Port Free’ channels available for allocation to the video source.
Any errors in setting up the cameras can be rectified by simply disconnecting and reconnecting the camera to the switch in whilst configuration mode, which will allow the camera to reallocate. If multiple changes are made, it is recommended that the NVR is reset after correcting the configuration to ensure perfect allocation.

**IMPORTANT:** To ensure absolute system security, the unit should now be configured before connecting it to the network, refer to ‘Configuring the Unit’ before proceeding to Step 4 Connecting the unit to the network.

**Step 6 - Connecting an Additional Layer 3 Enhanced CCTV Switch (Cascade port option)**

More than sixteen camera connections can be configured by cascading an additional Layer 3 Enhanced CCTV Switch. Sixteen additional cameras can then be connected to this switch. All 32 cameras will then be viewable and available for configuration via the controlling NVR.

The Layer 3 Enhanced CCTV Switch address is set using the hardware dial on the base of the unit. Each switch needs to have a unique address in the chain.

- The second external switch attached to an SD Advanced should be set to ‘1’, the next one set to ‘2’ etc. Connect a CAT5 Network cable between the ethernet port labelled ‘ETH-C’ on the first (master) Layer 3 Enhanced CCTV Switch and the ethernet port labelled ‘ETH-A’ on a second (cascade) Layer 3 Enhanced CCTV Switch.

Once the switch has been physically added, the NVR needs to be configured to use it. If the NVR is in Configuration mode when the switches are added, the switches will be automatically discovered and added. If the NVR is in secure mode, the switches can be physically discovered. Navigate to ‘Closed IPTV -> Discover’ and click on the green ‘Discover’ button. Information on the switches seen by the NVR is updated in the table.

**Connecting an additional Layer 3 Enhanced CCTV Switch as a Cascade unit**

**Step 7 - Connecting a ZeroConf Network Connection**

The Layer 3 Enhanced CCTV Switch supports zero-conf networking (sometimes known as Bonjour), this enables automatic discovery of computers, devices, and services on IP networks. Zero-conf uses industry standard IP protocols to allow devices to automatically discover each other without the need to enter IP addresses or configure DNS servers.

The Layer 3 Enhanced switch can utilise the zero-conf facilities to discover cascaded switches whilst it is in Configuration Mode. Navigate to ‘Closed IPTV -> Discover’ and click on the green ‘Discover’ button. Information on the switches seen by the NVR is updated in the table. Press ‘Accept’ to force the NVR unit to use the revised switch topology for camera inputs, refer to the manual for further details.
Configuring the Unit

The Layer 3 Enhanced CCTV Switch is only configured via a connected Closed IPTV Dedicated Micros NVR. When the Layer 3 Switch is connected to a suitable NVR, the configuration pages will be active.

The key security goal of Closed IPTV is to protect camera ports in potentially vulnerable locations. Closed IPTV aims to:

- prevent rogues with access to exposed endpoints from spoofing the cameras and gaining access to the NVR or Corporate network.
- prevent rogues with access to exposed endpoints from affecting other cameras with less exposed endpoints (ie carpark cameras cannot be used to affect cameras in a secure vault).

Access the NVR configuration pages and navigate to Closed IP -> Settings.

Settings

The on-screen image of the Layer 3 Enhanced CCTV Switch provides instant information regarding camera connection ports.

Port Illustration Colour Key

Port Free (Black) — No video source currently connected to the port and nothing assigned to that channel.
Analog Connection (Blue)  - Analogue camera input using the BNC connection for this channel on the back of the NVR. Analogue cameras take priority over IP cameras when channels are being assigned; if an IP camera is put into the port on the switch associated with an a channel allocated to an analogue input, the IP camera will go into the un-allocated camera list.

Single IP Connected (Green)  - A single IP camera is connected directly to the port and will be auto assigned to the channel.

Single IP Assigned (Turquoise)  - A camera that has either been configured manually independently outside Closed IP or is one of the cameras (above camera 1 of the encoder) assigned by Closed IP by connecting a multi channel encoder.

Multiple IP Connections (Yellow)  - A port that is hosting a multiple channel input eg a connection to a multi channel encoder. The cameras after this are treated by the NVR as Single IP Assigned.

Duplicate Channel Allocation (Orange)  - A port that has analogue and IP connection applied to it. The IP source will be un-allocated.

Overview (Red Button) - Select this option to open the NVR Camera Connection Overview menu, showing all cameras connected to the NVR and whether they are connected locally (via BNC) or via IP.

Discover (Green Button) - Opens the Closed IPTV Discover page on the NVR which can be used to initiate discovery of all Layer 3 Enhanced CCTV Switches connected to the NVR.

Upgrade (Yellow Button) - Opens the Closed IPTV Upgrade Page on the NVR, refer to ‘Upgrade’.

Advanced (Blue Button) - Opens the Closed IPTV Advanced Page on the NVR, refer to ‘Advanced’.

Security Level - Select from Configuration Mode’ or ‘Secure Mode’. On initial boot, the NVR will default to Configuration Mode.

In Configuration mode, the security settings of all cascaded Layer 3 Enhanced CCTV Switches and the configuration of video sources connected to the Layer 3 Enhanced CCTV Switch can be globally edited.

Use this mode when configuring the Closed IPTV system only. The switch is not secure in this mode, but it allows the NVR to discover cameras and additional switches. Cameras can be physically swapped around and configured by the user as required.

Note: In Configuration mode, there is no registration of a camera fail. The cameras are either in a not connected state or connected when present.

In Secure Mode, Closed IPTV security is enabled and the selected security settings listed below are applied. These are Restrict between end point ports, Restrict public access (Port B), Restrict multicast from general network, Lock ports by MAC, Signature verify remote codecs and Restrict end point access to NVR.

Note: In Secure Mode, video sources are either successfully connected or port free. A configured source that is not sending will be registered as a camera fail.

NOTE: Secure mode should always be enabled once configuration is complete. If left in Configuration mode the system will be insecure and vulnerable to attacks. A visible warning will be displayed on the local viewer if Secure mode is not applied.
Restrict between end point ports

End points are defined as the extreme edges of the network, normally video sources, which could be exploited as potentially insecure connections into the Closed IPTV network.

When the Closed IPTV network is configured, the NVR notes the MAC addresses of the end point connections that are to be trusted. This option acts as a hard firewall to stop DoS or other attacks on cameras in a different location (e.g. prevents a camera in a public location from affecting a camera in the safe vault).

**Warning:** If this option is not enabled, it will still be possible to connect devices to the camera ports and access other cameras via the switch.

Restrict public access (Port B)

Select to restrict all network data between the General/Corporate network to the video end points. No outside connections except the NVR are allowed to communicate with end points directly, and endpoints are separated from the General/Corporate Network.

**Note:** The NVR itself on standard DHCP address will still be accessible from this port if physically connected to network.

**Note** Non NetVu Connected cameras will only be allocated DHCP addresses by the external network if this option is disabled.

**Warning:** If this option is not enabled it will be still be possible for external systems connected to the general corporate network (via port Eth-B) to access the NVR and all cameras.

**Warning:** If this option ever needs to be enabled at a later date, it will expose the connected cameras to the general corporate network. If other hardware has been added to the network using the Bonjour protocol after the configuration and isolation of these cameras, there is a slim chance that the new hardware items could have the same IP address as the cameras.

Restrict multicast from general network

This disables client network access to the multicast MAC services in the camera, but does not disable standard web access for camera configuration etc. unless ‘Restrict public access’ is enabled. If this option is ticked, it only allows clients to receive multicast video data through SAP service group broadcasts from the NVR.

**Warning:** Multicasting requires this option is disabled to ensure public access is unrestricted.

Lock ports by MAC

Camera ports on the Layer 3 Enhanced CCTV Switch can be locked to the MAC address of the camera connected to that port. This prevents casual access from the port to the rest of the system (DVR, other cameras). No additional MAC address will be allowed on that port - however network data is still free to travel in any direction. This is a low level of security in that it allows multi-cast, direct camera access etc but protects the client network to a limited degree from the exposed end point.

**Warning:** If this option is not enabled then cameras or other devices can be swapped in and out of the port with no restrictions on their network data ie an alternative ‘hacked’ video source could be introduced to the Layer 3 switch in place of a legitimate source.

Signature Verify Remote Codecs

More sophisticated attackers could bypass the Layer 3 Enhanced CCTV Switch MAC address rules (described in ‘Lock Ports by MAC’) by spoofing the MAC address of the camera connected to the port. We can identify such attackers using Trusted Endpoint.
**Restrict End Point Access to NVR**

To limit the potential intrusion methods available from the camera ports, the standard set of TCP and UDP services on the NVR can be completely disabled to traffic from the camera ports. If a camera has been swapped for a device that has been given a spoof MAC address the NVR will still only accept data from that connection via the usual HTTP port. The port can only supply video, and this will be flagged as unsigned due to the Trusted Endpoint feature (if enabled).

**Security Violations**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolate from network</td>
<td>On detection of a security breach this option will prevent any device connected to the breached port from accessing the general corporate network (if available). Video will continue to be streamed on the Closed IP side of the network.</td>
</tr>
<tr>
<td>Isolate from Closed IP</td>
<td>If a security breach is detected, the video source is isolated from the Closed IPTV network.</td>
</tr>
<tr>
<td>Generate system event</td>
<td>Select this option to report port violation as system events which can be used as a input to an alarm zone (e-mail, alarm etc ) on the NVR.</td>
</tr>
<tr>
<td>Reconnect after</td>
<td>Reconnection to the network will be attempted after a security breach once this period has elapsed. If the security breach is detected again, connection to the general corporate network will remain blocked.</td>
</tr>
</tbody>
</table>
Discover

This page shows the currently connected switches and allows discovery of all Layer 3 Enhanced CCTV Switches connected to the NVR. The Layer 3 Enhanced CCTV Switch supports zero-conf networking (sometimes known as Bonjour), which enables automatic discovery of computers, devices, and services on IP networks. The NVR will automatically discover switches as they are connected if it is in configuration mode. Zero-conf uses industry standard IP protocols to allow devices to automatically discover each other without the need to enter IP addresses or configure DNS servers.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
<td>Details the appropriate port variable value.</td>
</tr>
<tr>
<td>Discover (Green Button)</td>
<td>Information on the switches seen by the NVR is updated in the table.</td>
</tr>
<tr>
<td>Accept (Blue Button)</td>
<td>Force the NVR to use the revised switch topology for video inputs.</td>
</tr>
</tbody>
</table>
Upgrade

This page shows the current state of software for each connected module along with some basic information (such as connection status etc). It provides the option to upgrade a selected switch (or all switches)

Once a switch is connected and Discovered, the connected NVR will automatically upgrade it. A switch can also be deliberately upgraded. Select the switch to be upgraded and press the Upgrade button. The NVR automatically sends the required file to the switch and restarts it.
Advanced

This page allows access to the advanced facilities on the NVR such as Autosync and setting the base camera number of a switch. Ports on the switches are allocated using a combination of base switch and configuration page. Each Layer 3 Enhanced CCTV Switch has a hardware configuration dial on the base to allow a unique (in the chain) identifier to be set. This identifier is used by the configuration pages to configure the base camera number.

Auto-Synchronise NVR variables with cameras

When a new camera is connected and the unit is in configuration mode, the NVR will synchronise some of the settings (eg camera title) with the camera. This synchronisation will only occur for Remote Codec cameras (ie NetVu Connected cameras and video servers) and only in configuration mode.

Switch

Displays the switches that have found and accepted by the NVR, refer to ‘Discover’.

Base Camera

Each switch can have up to 16 video sources attached to it. A switch may not have all ports configured with a video source, so there may be more than two switches attached to the NVR. This option sets the base camera number on the selected switch, all subsequent video sources on that switch will receive a consecutive number.
Cameras

Displays the camera numbers that have been assigned to the switch by the Closed IPTV NVR. The NVR recognises how many cameras are attached to the switch and assigns cameras numbers accordingly.
EcoSense NVR for up to 32 channels

Example Configurations

1. **Layer 3 Enhanced CCTV Switch**
   - 16 Cameras addressed \( \Rightarrow \) 16
   - (Internal Switch address = 0 \( \Rightarrow \) base camera No. 1)

2. **Layer 3 Enhanced CCTV Switch**
   - 16 Cameras Addressed \( \Rightarrow \) 32
   - (Switch address = 1 \( \Rightarrow \) base camera No. 17)

**Port Allocation**

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETH A</td>
<td>Closed IPTV Control Port</td>
</tr>
<tr>
<td>ETH B</td>
<td>General / Corporate Network</td>
</tr>
<tr>
<td>ETH C</td>
<td>Closed IPTV Cascade Port</td>
</tr>
<tr>
<td>ETH D</td>
<td>Zeroconf Network Port (Default) - or Closed IPTV Cascade Port</td>
</tr>
</tbody>
</table>

**Key**

- **Closed IPTV Network Connection**
- **General / Corporate Network Connection**
- **Single IP Connected**
Closed IPTV system mixed with analogue cameras

Port Allocation

Layer 3 Switch

Key

SD Advanced

Closed IPTV Network Connection
General / Corporate Network Connection
Closed IPTV Cascade Port
Closed IPTV Cascade Port (Default)
Closed IPTV Cascade Port - Extended Channel Port
SD Advanced

Port Allocation

Layer 3 Switch

2x Ports reserved for the analogue connections on DVR

Layer 3 Enhanced CCTV Switch

16 cameras

Layer 3 Enhanced CCTV Switch

14 IP cameras

NetVu Console

PC For Remote Configuration And Access To Cameras

PC With NetVu Observer (Via General Network)
Closed IPTV system with cascaded Layer3 Enhanced CCTV switches

**Layer 3 Switch**

*SD Advanced

32 channel SD Advanced
Max 32 streams. Any mix of IP or analogue

8 Cameras addressed 1 – 8
*(Switch address = 0 ➝ base camera No. 1)*

8 Cameras addressed 9 – 16
*(Switch address = 1 ➝ base camera No. 9)*

8 Cameras addressed 17 – 24
*(Switch address = 2 ➝ base camera No. 17)*

8 Cameras addressed 25 – 32
*(Switch address = 3 ➝ base camera No. 25)*

**Port Allocation**

| ETH A: | Closed IPTV Control Port |
| ETH B: | General / Corporate Network |
| ETH C: | Closed IPTV Cascade Port |
| ETH D: | Zeroconf Network Port (Default) |
|        | - or Closed IPTV Cascade Port |

*Example shown is 32 channel product, 8 and 16 channel product also supports 32 IP cameras*
Additional Layer 3 Enhanced CCTV Switches deployed in a 'star' layout.

Key:
- Closed IPTV Network Connection
- General / Corporate Network Connection
- Single IP Connected
- Camera not connected
- Closed IPTV - transparent ports

Port Allocation:
- ETH A: Closed IPTV Control Port
- ETH B: General / Corporate Network
- ETH C: Closed IPTV Cascade Port
- ETH D: Zeroconf Network Port (Default)
  - or Closed IPTV Cascade Port

*Example shown is 32 channel product, 8 and 16 channel product also supports 32 IP cameras.
Layer 3 Switch

Spanning a General network with distributed Closed IPTV Layer 3 Enhanced CCTV switches

- General network
  - Layer 2 managed switches (VLAN)
  - Both ports with same VLAN ID
  - Capable of handling 'Jumbo' frames

- Layer 2 Managed Switch VLAN

- Layer 3 Enhanced CCTV Switch

- 8 Cameras addressed 1 → 8
  - (Switch address = 0 ⇒ base camera No. 1)

- Layer 2 Managed Switch VLAN

- Layer 3 Enhanced CCTV Switch

- 8 Cameras addressed 9 → 16
  - (Switch address = 1 ⇒ base camera No. 9)

- Layer 2 Managed Switch VLAN

- Layer 3 Enhanced CCTV Switch

- 16 Cameras Addressed 17 → 32
  - (Switch address = 2 ⇒ base camera No. 17)

Key

- Closed IPTV Network Connection
- General / Corporate Network Connection
- VLAN Interconnection such as Cisco's ISL (Inter-switch link) and 3COM's VLT (Virtual LAN Trunk)
- Single IP Connected
- Camera not connected
- General Network Port
- Closed IPTV - transparent ports

Port Allocation

ETH A: Closed IPTV Control Port
ETH B: General / Corporate Network
ETH C: Closed IPTV Cascade Port
ETH D: Zeroconf Network Port (Default) - or Closed IPTV Cascade Port

*Example shown is 32 channel product. 8 and 6 channel product also supports 32 IP cameras.
Extended Cascading of a Closed IPTV System

**Key**
- Closed IPTV Network Connection
- General / Corporate Network Connection
- Single IP Connected
- Camera not connected

**Port Allocation**
- ETH A: Closed IPTV Control Port
- ETH B: General / Corporate Network
- ETH C: Closed IPTV Cascade Port
- ETH D: Zeroconf Network Port (Default) - or Closed IPTV Cascade Port

*Example shown is 32 channel product, 8 and 16 channel product also supports 32 IP cameras*
Connection to a Closed IPTV decoder (Pure IP system)

NV1 (DV-IP Decoder) connected to Closed IPTV secure port is used to provide secure connection for monitoring. The NV1 acts as a receiving station for multiple video images transmitted from NetVu Connected video sources on the Closed IPTV secure network. The NV1 receives the compressed digital data over the Closed IPTV secure network and converts this into a format that can be displayed on a monitor.

Within the Console on the DV-IP NV1, the NetVu Connected video sources will be assigned as to system 1 ie source 1 will become System 1 - Server URL 1, source 2 is System 1 - Server URL 2 etc.

Network (AOE) Storage connected to Closed IPTV secure port is used to save images, in addition to on-board storage on each CamVu2000, providing a central archive of recorded images.
Connection to a Closed IPTV decoder using NVR recording (Pure IP system)

NV1 (DV-IP Decoder) connected to Closed IPTV secure port is used to provide secure connection for monitoring. The NV1 acts as a receiving station for multiple video images transmitted from NetVu Connected video sources on the Closed IPTV secure network. The NV1 receives the compressed digital data over the Closed IPTV secure network and converts this into a format that can be displayed on a monitor.

Within the Console on the NV1, the NetVu Connected video sources will need to be manually assigned by inputting each IP address. The system detail can then be detected using the ‘Auto Fill’ option on the page.

Network (AOE) Storage connected to Closed IPTV secure port is used to save images, in addition to on-board storage on each CamVu2000, providing a central archive of recorded images.
Appendix A - Detected Camera Defaults

The Layer 3 Enhanced CCTV Switch auto-detects the presence of a camera when it is connected, and passes the detected detail to the connected NVR. The NVR will then apply default settings to the camera to allow instant recording and viewing. These settings can all be changed in the NVR configuration pages.

Classification

When a camera is connected and recognised, the NVR will apply the following resolution options as standard.

camera_class id = standard_resolution_ip
Possible resolutions 4CIF,2CIF,CIF,QCIF

camera_class id = vga_class
Possible resolutions VGA,QVGA,Q2VGA

camera_class id = megapixel_class
Possible resolutions VGA,SVGA,UXGA,QVGA,Q2VGA,XGA,XGA+,SXGA+,QXGA

camera_class id = standard_resolution_analogue
Possible resolutions 4CIF,2CIF,CIF,QCIF

Recording Defaults

When a camera is connected and recognised, the NVR will apply the following MPEG recording default as standard.

<table>
<thead>
<tr>
<th></th>
<th>PPS</th>
<th>BR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAL</td>
<td>6.25</td>
<td>750</td>
</tr>
<tr>
<td>NTSC</td>
<td>7.5</td>
<td>900</td>
</tr>
<tr>
<td>VGA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAL</td>
<td>6.25</td>
<td>750</td>
</tr>
<tr>
<td>NTSC</td>
<td>7.5</td>
<td>900</td>
</tr>
<tr>
<td>MegaPixel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAL</td>
<td>6.25</td>
<td>1024</td>
</tr>
<tr>
<td>NTSC</td>
<td>7.5</td>
<td>1024</td>
</tr>
</tbody>
</table>
Appendix B - FoxyBonjour

The Layer 3 Enhanced CCTV Switch supports zero-configuration networking (sometimes known as Bonjour), this enables automatic discovery of computers, devices, and services on IP networks. Zero-configuration uses industry standard IP protocols to allow devices to automatically discover each other without the need to enter IP addresses or configure DNS servers. By loading a suitable free add-on to your web browser such as Bonjour for Windows for Internet Explorer or BonjourFoxy for FireFox zero configuration devices such as this unit can easily be discovered and accessed.

Changelog

1-2v1 ClosedIPTV logo added
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Layer3 Enhanced CCTV Switches deployed in a ‘star’ layout</td>
<td>27</td>
</tr>
<tr>
<td>Address</td>
<td>8</td>
</tr>
<tr>
<td>Advanced</td>
<td>22</td>
</tr>
<tr>
<td>Appendix A - Detected Camera Defaults</td>
<td>32</td>
</tr>
<tr>
<td>Appendix B - FoxyBonjour</td>
<td>33</td>
</tr>
<tr>
<td>AutoIP Address Bounce: Camera Denial of Service (DoS)</td>
<td>4</td>
</tr>
<tr>
<td>AutoIP Address Bounce: NVR Denial of Service (DoS)</td>
<td>4</td>
</tr>
<tr>
<td>Base Panel</td>
<td>8</td>
</tr>
<tr>
<td>camera_class id = megapixel_class</td>
<td>32</td>
</tr>
<tr>
<td>camera_class id = standard_resolution_analogue</td>
<td>32</td>
</tr>
<tr>
<td>camera_class id = standard_resolution_ip</td>
<td>32</td>
</tr>
<tr>
<td>camera_class id = vga_class</td>
<td>32</td>
</tr>
<tr>
<td>Camera Port to Camera Port: Comms</td>
<td>4</td>
</tr>
<tr>
<td>Classification</td>
<td>32</td>
</tr>
<tr>
<td>Closed IPTV system mixed with analogue cameras</td>
<td>25</td>
</tr>
<tr>
<td>Closed IPTV system with cascaded Layer3 Enhanced CCTV switches</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Closed IPTV</td>
<td>12</td>
</tr>
<tr>
<td>Configuring the Unit</td>
<td>16</td>
</tr>
<tr>
<td>Connecting an additional Layer 3 Enhanced CCTV Switch as a Cascade unit</td>
<td>15</td>
</tr>
<tr>
<td>Connection to a Closed IPTV decoder (Pure IP system)</td>
<td>30</td>
</tr>
<tr>
<td>Connection to a Closed IPTV decoder using NVR recording (Pure IP system)</td>
<td>31</td>
</tr>
<tr>
<td>Discover</td>
<td>20</td>
</tr>
<tr>
<td>DM/NSW/CPP</td>
<td>7</td>
</tr>
<tr>
<td>EcoSense NVR for up to 32 channels</td>
<td>24</td>
</tr>
<tr>
<td>Example Configurations</td>
<td>24</td>
</tr>
<tr>
<td>Extended Cascading of a Closed IPTV System</td>
<td>29</td>
</tr>
<tr>
<td>Features</td>
<td>3</td>
</tr>
<tr>
<td>Front Panel connections</td>
<td>7</td>
</tr>
<tr>
<td>Important Safeguards</td>
<td>5</td>
</tr>
<tr>
<td>Index</td>
<td>34</td>
</tr>
<tr>
<td>Injection of Rogue Video</td>
<td>4</td>
</tr>
<tr>
<td>Installing The Unit</td>
<td>7</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Lightning Strike</td>
<td>5</td>
</tr>
<tr>
<td>Port Illustration Colour Key</td>
<td>17</td>
</tr>
<tr>
<td>Power</td>
<td>7</td>
</tr>
<tr>
<td>Power Sources</td>
<td>5</td>
</tr>
<tr>
<td>Read Instructions</td>
<td>5</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Rear Panel connections</td>
<td>7</td>
</tr>
<tr>
<td>Recording Defaults</td>
<td>32</td>
</tr>
<tr>
<td>Regulatory Notes and FCC and DOC Information</td>
<td>5</td>
</tr>
<tr>
<td>Rogue Device Access</td>
<td>3</td>
</tr>
<tr>
<td>Rogue Device Access with MAC spoofing</td>
<td>3</td>
</tr>
<tr>
<td>Secure Mode/Configuration Mode</td>
<td>12</td>
</tr>
<tr>
<td>Security Protection</td>
<td>3</td>
</tr>
<tr>
<td>Security Violations</td>
<td>19</td>
</tr>
<tr>
<td>Servicing</td>
<td>5</td>
</tr>
<tr>
<td>Settings</td>
<td>17</td>
</tr>
<tr>
<td>Spanning a General network with distributed Closed IPTV Layer3 Enhanced CCTV switches</td>
<td>28</td>
</tr>
<tr>
<td>Step 1 - Set the switch Hardware identifier</td>
<td>9</td>
</tr>
<tr>
<td>Step 2 - Connecting the Layer 3 Enhanced CCTV Switch to a compatible Dedicated Micros NVR</td>
<td>9</td>
</tr>
<tr>
<td>Step 3 - Connecting Power to the Unit</td>
<td>9</td>
</tr>
<tr>
<td>Step 4 Connecting the Unit to the General Network (optional)</td>
<td>10</td>
</tr>
<tr>
<td>Step 5 - Connecting a Camera to the Unit</td>
<td>11</td>
</tr>
<tr>
<td>Step 6 - Connecting an Additional Layer 3 Enhanced CCTV Switch (Cascade port option)</td>
<td>15</td>
</tr>
<tr>
<td>Step 7 - Connecting a ZeroConf Network Connection</td>
<td>15</td>
</tr>
<tr>
<td>Upgrade</td>
<td>21</td>
</tr>
<tr>
<td>Ventilation</td>
<td>5</td>
</tr>
</tbody>
</table>
Dedicated Micros Ltd.
1200 Daresbury Park, Daresbury,
Cheshire, WA4 4HS, UK

Dedicated Micros Germany
Hamtorstraße 9
41460 Neuss, Germany

Dedicated Micros France
9-13 rue du Moulinet
75013 Paris, France

Dedicated Micros Slovenia
Delavska Cesta 26,
4208 Sencure, Slovenia

Dedicated Micros Middle East
Building 11, Suite 405 – 407
P.O.Box 500291, Dubai Internet City,
Dubai, United Arab Emirates

Dedicated Micros (Malta) Ltd.
BLB017, Bulebel Industrial Estate,
Zejtun, ZTN3000, Malta

Dedicated Micros USA.
14434 Albemarle Point Place, Suite 100,
Chantilly, Virginia 20151 USA

Dedicated Micros, Australia PTY.
PO Box 6480, Baulkam Hills BC
NSW 2153, Australia, NSW 2153

Dedicated Micros, Asia PTY
2 Kallang Pudding Road
#08-08 Mactech Industrial Building
Singapore 349307

Dedicated Micros Benelux
Joseph Chantraineplantsoen 1,
3070 Kortenberg, Belgium