



# ***i-Witness Digital CCTV Service Network Requirements***

This specification sets out some general guidelines relating to the conditions required from a network used for the interconnection of i-Witness system hosts.

## **1. Service Overview**

i-Witness is a digital CCTV service which is used for the provision of CCTV storage, command and control (camera PTZ), video switching and video facility management. The interconnection of the numerous subsystems that form part of an i-Witness solution present specific requirements on the underlying network.

## **2. Network Interface**

2.1 The network interface presented by i-Witness is a 100BASE-T Ethernet port (copper RJ-45 connector) which can be configured either for auto negotiation or 100Mbit/s full duplex.

## **3. IP Multicast**

3.1 i-Witness uses IP multicast to transmit video streams from sources to (many) destinations. The network links should therefore be capable of transmitting multicast traffic (destination addresses 239.0.0.0/8).

*Note:* Switches that are not IP multicast aware are likely to treat the traffic as broadcast, flooding all ports, having a detrimental affect on the overall performance of the network.

3.2 IP multicast configuration differs for switched and routed networks:

- For local, switched networks, switches should be IGMP aware so traffic can be snooped. IGMP version 2 is required.
- For routed WAN links (running routing protocols like OSPF), PIM in Sparse Mode is required. Note that not all versions of Cisco IOS support PIM In Sparse Mode.

3.3 i-Witness systems are typically deployed onto closed, switched local networks - no WAN links nor routing protocols are used.

3.4 The key multicasting mechanism employed by i-Witness is therefore IGMP snooping. The switch snoops IGMP messages and according to these IGMP messages, the switch knows which ports have requested which multicast streams. This makes the network bandwidth

more efficient because the switch only respectively sends the multicast streams to the ports which need the streams.

3.5 IGMP snooping requires an 'IGMP querier' to exist in the network. If no IGMP querier exists in the network, the multicast receivers will not send proper IGMP messages to tell the switch which multicast streams they need. The Cisco IGMP snooping feature provides an integrated partial-function IGMP querier. This partial-function IGMP querier is typically used and eliminates the need for a 'real IGMP querier'. This functionality is not restricted to the Layer 3 switches normally used with i-Witness (Cisco 3750 series). Some Cisco Layer 2 switches such as Cisco 2960 also have this capability.

3.6 The switch sends IGMP version 2 messages, but it accepts version 1, 2 or 3.

3.7 Furthermore the "fast leave" or "immediate leave" option should be enabled to ensure prompt disconnection of video when leaving the multicast group. This makes sure that the multicast forwarding is stopped efficiently when it is unsubscribed. However, "immediate leave" should only be enabled when there is only one receiver connected to each switch port. In other words, if there is more than one switch (a Cisco switch-stack is regarded as one) "immediate-leave" should not be enabled as "immediate-leave" may cause temporary video stream interruption elsewhere in the network.

3.8 If routers use access lists, the addresses (both unicast and multicast) and port numbers can be used to block/allow traffic. Host/stream IP addresses and port numbers should therefore be agreed prior to delivery.

3.9 Overall bandwidth requirements depends on how many streams are transmitted. Example bandwidths for a *single* video stream are:

- 25fps/4CIF stream is circa 5.5Mbit/s.
- 25fps/2CIF stream is circa 3Mbit/s
- 12fps/2CIF stream is circa 1.5Mbit/s
- 2fps/2CIF stream is circa 500kbit/s



# ***i-Witness Digital CCTV Service Network Requirements***

3.10 Typical UDP port numbers used by i-Witness:

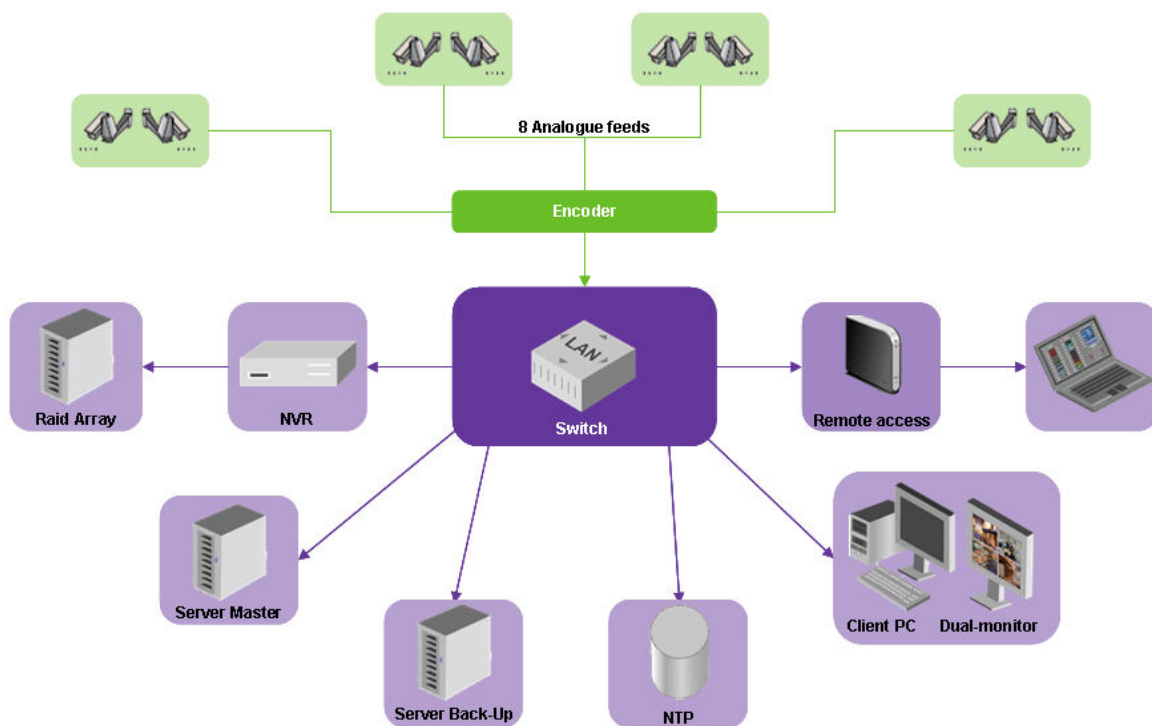
- 5008: live video streams from encoders
- 1031: recorded video streams from NVRs

Typical i-Witness network architecture:

3.11 Typical TCP port numbers used by i-Witness:

- 1717: database connection
- 45653: database multicast
- 6001-6008: process connections – http
- 6101-6108: process connections – CLI
- 6201-6208: process connections – XML
- 161-162: encoder and alarm connections
- 7123: alarm database sync connection
- 7118: bandwidth manager connection
- 700x: terminal server connections
- 7101-2: CCL connections
- 7201-16: audio connections

## **The Architecture**



To find out more about BT Redcare i-Witness,

email:  
[redcare@bt.com](mailto:redcare@bt.com)

or call:  
0800 800 828