

# TN0020 - FIREWALL CONSIDERATIONS FOR CAMELOT IP CAMERAS

---

## 1 CAMELOT IP CAMERAS IN THE LAN

---

Discovering a Camelot IP camera in the LAN and maintaining a session with it makes use of two UDP ports in the PC's firewall: one for control messages (PORT1) and the other for video data (PORT2).

A session with a Camelot IP camera goes through four stages.

- **Discovery Handshake**  
The application makes a UDP broadcast requesting all Camelot IP cameras to respond; the broadcast socket is bound to PORT1; the message broadcasted contains the port number of PORT2, upon which the application waits for camera responses. The camera accepts the handshake broadcast message on port 61318 and responds on source port 61320 to PC destination PORT2 specified in the content of the handshake message.  
Upon conclusion of the discovery handshake, the ports are released and will be reused.
- **Setup**  
The application can transmit messages to the camera with source port PORT1 and camera destination port 61318 for the purpose of setup – or for querying the status of various camera parameters.
- **Start Video Transport**  
When the application wishes to start video transport, it sends the camera a request with source port PORT1 and destination port 61318. The camera responds with source port 61318 to PC destination port PORT1 and it also responds with source port 61319 to PC destination port PORT2. This double response marks the beginning of the video session.
- **Video Session**  
The camera transmits video data with source port 61319 to PC destination port PORT2. The camera still waits for requests from the application on port 61318 and will respond to them with source port 61318 to PC destination port PORT1.

### 1.1 IT Considerations

The use of these two UDP ports (PORT1 & PORT2) by the application must not be blocked by the firewall. In addition, the firewall must accept incoming UDP from source ports **61318**, **61319**, & **61320**. Thus, either an exception must be made in the firewall for the application by name/path - or by the specific UDP ports it uses. The decision whether to make application exceptions or port exceptions is up to the LAN's IT supervisor. If port exceptions are decided upon, the application

programmer must specify in his code the ports in the firewall which were opened for use (PORT1 & PORT2).

Since in life cycle of the application/computer session, it is not impossible that ports used by the application are not freed due to system or application errors, it is best to make exceptions for a range of more than just two ports. More ports must be allocated according to the number of cameras the application controls concurrently.

Unless otherwise specified by the application, 'Camelot.Dll', which provides the applicative interface to Camelot IP cameras, assumes that 50 UDP ports, 21320 – 21369, are available for use.

If this is not the case, the UDP ports designated for use by the application must be explicitly specified in the application. This is done using 'Camelot.Dll's CamSetPortRange() function.

This function must be called *before* the invocation of any of the discovery functions (FillCameraList, CamEnumCameras, CamEnumCamerasEx etc).

```
void CamSetPortRange(int numPorts, unsigned short portStart)
```

**numPorts** - the number of UDP ports that were opened in the firewall.

**portStart** - the first port in the contiguous range of **numPorts** ports.

Example:

```
CamSetPortRange(10, 60000); //allows the application to use ports 60000-60009  
FindCameras();
```

## Example Session

Please refer to **Appendix A**, which is the (*WireShark*) sniffer-log of a Camelot IP camera handshake & brief video session.

In the example session log file, the PC appears at the IP address of 192.168.168.**53**; the camera appears at the IP address of 192.168.168.**254**.

- **Discovery Handshake**

The application makes a UDP broadcast requesting all Camelot IP cameras to respond (line 1); the broadcast socket is bound to 60000; the message broadcasted contains the

port number 60001, upon which the application waits for camera responses. The camera accepts the handshake broadcast message on port 61318 and responds on source port 61320 to PC destination 60001 specified in the content of the handshake message (line 2).

- **Setup**

The application transmits various messages to the camera with source port 60000 and destination port 61318 for the purpose of setup / querying the status of various camera parameters (lines 3, 5, 6, etc). The camera responds with source port 61318 and PC destination port 60000 (lines 4, 6, 8, etc).

- **Start Video Transport**

When the application wishes to start video transport, it sends the camera a request with source port 60000 and destination port 61318 (line 53). The camera responds with source port 61318 to PC destination port 60000 (line 54) and it also responds with source port 61319 to PC destination port 60001 (line 55). This double response marks the beginning of the video session. Note that something in the content of the response to PC port 60000 causes the sniffer to perceive the message protocol as DCERPC instead of UDP (line 54).

- **Video Session**

The camera transmits video data with source port 61319 to PC destination port 60001. The camera still waits for requests from the application on port 61318 and responds to them with source port 61318 to PC destination port 60000.

- **Stop Video Transport**

The application transmits various messages to the camera with source port 60000 and destination port 61318 for the purpose of stopping transport.

**Appendix A – WireShark sniffer log of a Camelot IP Session**

#	Time	Source	Destination	Size	Protocol	Source Port	Destination port
1	3.969998	192.168.168.53	255.255.255.255	554	UDP	60000	61318
2	3.970776	192.168.168.254	192.168.168.53	554	UDP	60001	61320
3	5.695138	192.168.168.53	192.168.168.254	58	UDP	60000	61318
4	5.695648	192.168.168.254	192.168.168.53	554	UDP	61318	60000
5	5.704246	192.168.168.53	192.168.168.254	58	UDP	60000	61318
6	5.705241	192.168.168.254	192.168.168.53	554	UDP	61318	60000
7	5.715908	192.168.168.53	192.168.168.254	60	UDP	60000	61318
8	5.716363	192.168.168.254	192.168.168.53	554	UDP	61318	60000
9	5.726767	192.168.168.53	192.168.168.254	74	UDP	60000	61318
10	5.7278	192.168.168.254	192.168.168.53	554	UDP	61318	60000
11	5.736488	192.168.168.53	192.168.168.254	74	UDP	60000	61318
12	5.737519	192.168.168.254	192.168.168.53	554	UDP	61318	60000
13	5.74723	192.168.168.53	192.168.168.254	74	UDP	60000	61318
14	5.74786	192.168.168.254	192.168.168.53	554	UDP	61318	60000
15	5.758057	192.168.168.53	192.168.168.254	74	UDP	60000	61318
16	5.75854	192.168.168.254	192.168.168.53	554	UDP	61318	60000
17	5.768687	192.168.168.53	192.168.168.254	528	UDP	60000	61318
18	5.769351	192.168.168.254	192.168.168.53	554	UDP	61318	60000
19	5.779428	192.168.168.53	192.168.168.254	528	UDP	60000	61318
20	5.780143	192.168.168.254	192.168.168.53	554	UDP	61318	60000
21	5.79017	192.168.168.53	192.168.168.254	528	UDP	60000	61318
22	5.790839	192.168.168.254	192.168.168.53	554	UDP	61318	60000
23	5.800976	192.168.168.53	192.168.168.254	74	UDP	60000	61318
24	7.666725	192.168.168.254	192.168.168.53	554	UDP	61318	60000
25	7.67042	192.168.168.53	192.168.168.254	74	UDP	60000	61318
26	7.671491	192.168.168.254	192.168.168.53	554	UDP	61318	60000
27	7.680743	192.168.168.53	192.168.168.254	74	UDP	60000	61318
28	7.681774	192.168.168.254	192.168.168.53	554	UDP	61318	60000
29	7.691574	192.168.168.53	192.168.168.254	74	UDP	60000	61318
30	7.692238	192.168.168.254	192.168.168.53	554	UDP	61318	60000
31	8.652361	192.168.168.53	192.168.168.254	62	UDP	60000	61318
32	8.653213	192.168.168.254	192.168.168.53	554	UDP	61318	60000
33	8.658269	192.168.168.53	192.168.168.254	62	UDP	60000	61318
34	8.660569	192.168.168.254	192.168.168.53	554	UDP	61318	60000
35	8.670067	192.168.168.53	192.168.168.254	138	UDP	60000	61318
36	8.670674	192.168.168.254	192.168.168.53	554	UDP	61318	60000

37	8.68948	192.168.168.53	192.168.168.254	70	UDP	60000	61318
38	8.69444	192.168.168.254	192.168.168.53	554	UDP	61318	60000
39	8.701237	192.168.168.53	192.168.168.254	62	UDP	60000	61318
40	8.883377	192.168.168.254	192.168.168.53	554	UDP	61318	60000
41	8.883805	192.168.168.53	192.168.168.254	59	UDP	60000	61318
42	8.8843	192.168.168.254	192.168.168.53	554	UDP	61318	60000
43	8.894845	192.168.168.53	192.168.168.254	70	UDP	60000	61318
44	8.901108	192.168.168.254	192.168.168.53	554	UDP	61318	60000
45	8.908425	192.168.168.53	192.168.168.254	66	UDP	60000	61318
46	8.91105	192.168.168.254	192.168.168.53	554	UDP	61318	60000
47	8.916061	192.168.168.53	192.168.168.254	66	UDP	60000	61318
48	8.918363	192.168.168.254	192.168.168.53	554	UDP	61318	60000
49	8.926791	192.168.168.53	192.168.168.254	66	UDP	60000	61318
50	8.929832	192.168.168.254	192.168.168.53	554	UDP	61318	60000
51	8.979002	192.168.168.53	192.168.168.254	59	UDP	60000	61318
52	8.979506	192.168.168.254	192.168.168.53	554	UDP	61318	60000
53	8.980777	192.168.168.53	192.168.168.254	59	UDP	60000	61318
54	9.217107	192.168.168.254	192.168.168.53	554	DCERPC	Request: seq: 1944 opnum: 16 len: 0 [DCE/RPC fragment]	
55	9.217362	192.168.168.254	192.168.168.53	554	UDP	61319	60001
56	9.227902	192.168.168.53	192.168.168.254	66	UDP	60000	61318
57	9.2284	192.168.168.254	192.168.168.53	554	UDP	61318	60000
58	9.239361	192.168.168.53	192.168.168.254	66	UDP	60000	61318
59	9.239928	192.168.168.254	192.168.168.53	554	UDP	61318	60000
60	9.249502	192.168.168.53	192.168.168.254	66	UDP	60000	61318
71	9.250005	192.168.168.254	192.168.168.53	554	UDP	61318	60000
72	9.261447	192.168.168.53	192.168.168.254	58	UDP	60000	61318
73	9.261928	192.168.168.254	192.168.168.53	554	UDP	61318	60000
74	9.270498	192.168.168.53	192.168.168.254	66	UDP	60000	61318
75	9.271002	192.168.168.254	192.168.168.53	554	UDP	61318	60000
76	9.281233	192.168.168.53	192.168.168.254	66	UDP	60000	61318
77	9.281702	192.168.168.254	192.168.168.53	554	UDP	61318	60000
78	9.291974	192.168.168.53	192.168.168.254	66	UDP	60000	61318
79	9.2925	192.168.168.254	192.168.168.53	554	UDP	61318	60000
80	9.30282	192.168.168.53	192.168.168.254	166	UDP	60000	61318
.							
.							
.							
.							
.	13.561924	192.168.168.53	192.168.168.254	66	UDP	60000	61318

	13.56198	192.168.168.254	192.168.168.53	1402	UDP	61319	60001
	13.563352	192.168.168.254	192.168.168.53	370	UDP	61319	60001
	13.563417	192.168.168.254	192.168.168.53	506	UDP	61319	60001
	13.564992	192.168.168.254	192.168.168.53	554	UDP	61318	60000
	13.565161	192.168.168.254	192.168.168.53	554	UDP	61319	60001
	13.571106	192.168.168.53	192.168.168.254	66	UDP	60000	61318
	13.571658	192.168.168.254	192.168.168.53	554	UDP	61318	60000
	13.582441	192.168.168.53	192.168.168.254	66	UDP	60000	61318
	13.584563	192.168.168.254	192.168.168.53	554	UDP	61318	60000
	13.592681	192.168.168.53	192.168.168.254	59	UDP	60000	61318
	13.593187	192.168.168.254	192.168.168.53	554	UDP	61318	60000

**Imaging Diagnostics** invites comments and feedback on this and all of our products and documentation. Please contact us at one of the email addresses below.

**Website**

<http://www.imagine2d.com/>

**Support**

We would appreciate any feedback you have about the Camelot EVK.

[support@imagine2d.com](mailto:support@imagine2d.com)

**Sales**

Please contact us if we can assist you in building your own custom applications.

[sales@imagine2d.com](mailto:sales@imagine2d.com)