



# Investigation into IP Quality of Service (QoS) for the JANET Video Conferencing Service (JVCS)

Philip Davison  
Welsh Video Network  
Swansea University

March 2007

## **Executive Summary**

The purpose of this project is to investigate the feasibility of implementing network Quality of Service (QoS) based on the Differentiated Services Code Point (DSCP) for the Joint Academic NETWORK (JANET) VideoConferencing Service (JVCS).

The first phase of the project involved deploying network monitoring infrastructure equipment at each of the geographically dispersed locations where the Multipoint Control Units (MCUs) are located. This was required to provide metrics on the network service to these locations. Devices were deployed at all locations during June 2006 and have been reporting network performance statistics back to a centralised service operated by the United Kingdom Education and Research Networking Association (UKERNA) ever since.

The second phase of the project involved investigating the ability of the production MCUs, the Polycom Media Gateway Controller (MGC), to set DSCP values. In summary, it is possible for the MCU to set DSCP values of between 0 and 63 (decimal) for video and audio packets (independently) leaving the network interface of the MCU. This would permit a production service to be deployed if required. Further policy work is necessary to determine which DSCP values should be applied.

It is recommended that any future Operational Requirement used to procure replacement MCUs contains detailed questions on the ability of the proposed equipment to process QoS settings.

## **Acknowledgements**

We would like to express our thanks to the following people for their contribution towards this work:

- Steve Williams – UKERNA
- John Martin – JVCS Management Centre
- Trevor Phillips – Polycom
- Mark Wilkinson – Polycom
- Staff at the JVCS Management Centre
- Staff at the Welsh Video Network (WVN) Support Centre
- Swansea University Networking Team

and to all of the others who assisted with the project.

## **Introduction**

JVCS is the videoconferencing switching and gatewaying service provided by UKERNA for use by the education and research sector across the United Kingdom (UK). The JVCS infrastructure is based on carrier grade Polycom MGC MCUs, which are distributed geographically across the UK and located near the JANET backbone. JVCS introduced an Internet Protocol (IP) service, JVCS-IP in 2003. The JVCS-IP service utilises the International Telecommunications Union (ITU) H.323 umbrella protocols for IP videoconferencing.

In light of the JANET QoS Project Phase 2, the scope of this project is to investigate the impact of a production QoS service on the JVCS and the capabilities of the Polycom MGC to process QoS marked IP packets.

### **Phase 1 – Deployment of network monitoring devices**

In order to offer a production videoconferencing service utilising a QoS enabled backbone, it is necessary to collect network performance metrics to demonstrate that the level of service being provided meets the agreed Service Level Agreement (SLA). At the inception of the project these metrics were not being collected, therefore it was necessary to deploy appropriate monitoring devices at the physical locations of the MCUs in order to collect and store network performance information. UKERNA has previously developed a monitoring system to record network performance and it was decided to deploy this system at the locations of the MCUs.

The monitoring system is based on a 1U Cisco 1760 router running Service Assurance Agent (SAA). This is located at the site to be monitored and reports network performance information back to a central server, which stores the information and presents meaningful graphs of network performance.

Monitoring units were preconfigured for installation at the location of each of the JVCS MCUs, namely the JANET co-location facilities at Reading and Leeds, and for the JVCS Management Centre in Edinburgh. JVCS allocated IP addresses within the appropriate subnets and allocated a switch port for each of the monitoring devices. The JANET Network Operations and Service Centre (NOSC) applied appropriate changes to Access Control Lists (ACLs) to permit the monitoring devices to communicate with the back-end of the monitoring system.

The unit for Edinburgh was couriered to the JVCS Management Centre and was installed on June 28 2006. A site visit to the unattended JANET Co-location facility at Reading was arranged for June 21 2006 and to Leeds for June 22 2006.



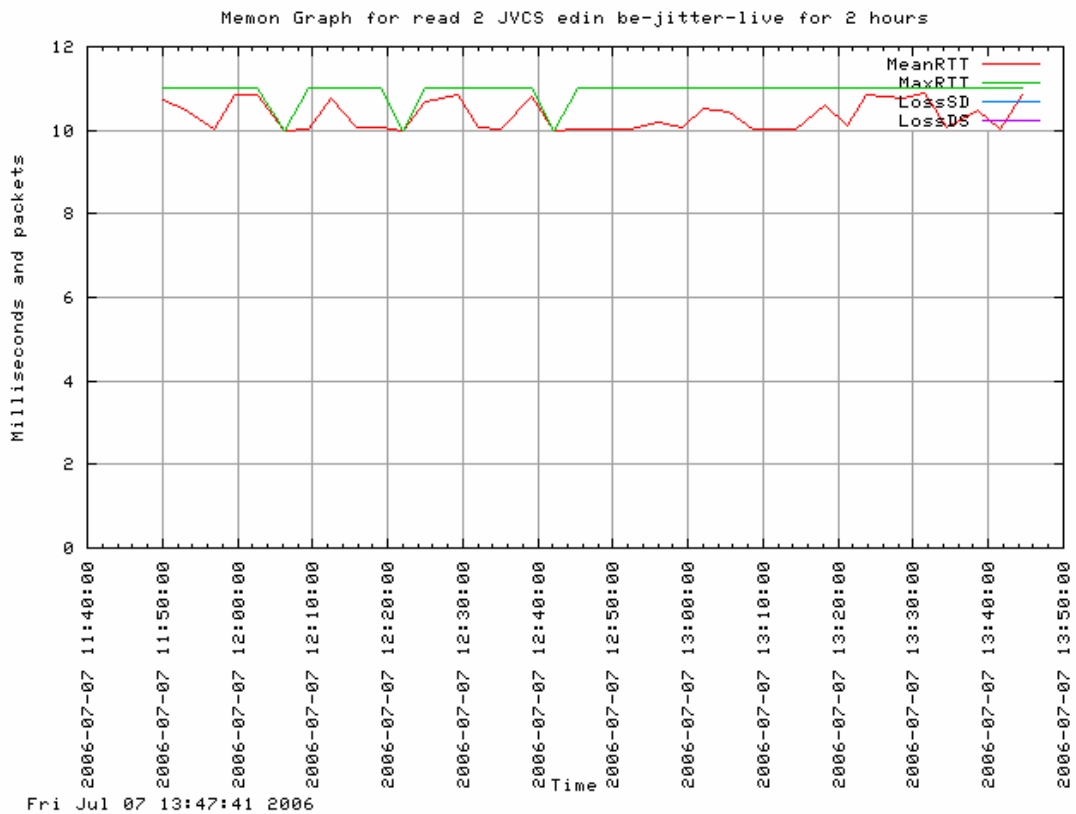
**JANET Co-location Facility**

# Investigation into IP QoS for the JANET VideoConferencing Service (JVCS)



UKERNA Network Monitoring Device installed at Co-location facility

Administration of the monitoring devices was handed over to JVCS following successful deployment of the devices. The chart below show a sample of the charts created by the networking monitoring system:



## Phase 2 – Ability of MCUs to manipulate QoS values

In order to verify that the MCUs were marking IP packets with appropriate QoS values as set administratively, it was necessary to find a method of capturing the IP packets and inspecting the DSCP values. Testing was conducted at the JVCS Management Centre in Edinburgh as this provided the most accessible location for the connection of testing devices. A visit to JVCS in Edinburgh was arranged for January 29-30 2007.

In order to capture the IP packets that were destined for, and originated from, the MCU, a Network Test Access Point (TAP) was connected to the appropriate MCU network interface. The MGC has several network interfaces; the interface used for a particular call is allocated dynamically and so it was necessary to disable all interfaces on the development MCU with the exception of one to guarantee that packets were captured from the correct interface.

The Network TAP used for this purpose was a NetOptics 10/100BaseT Teeny TAP ([http://www.netoptics.com/products/product\\_family\\_details.asp?cid=1&pid=159](http://www.netoptics.com/products/product_family_details.asp?cid=1&pid=159)), which is an in-line, passive, zero delay device. The TAP is connected between the MCU network interface and the network switch; two ports are provided on the TAP for this purpose. The TAP uses CATegory 5 (CAT5) cables with standard RJ45 connections; interestingly either the cable connecting the TAP to the switch or the TAP to the MCU needs to be a cross over cable. A further two RJ45 connections on the TAP now supply duplicate IP packets to monitoring devices for analysis, one of the interfaces supplies packets destined to the MCU and the other packets from the MCU.

In the picture below, the blue cable connects to the MGC (marked A on the TAP) and the green cable to the network switch (marked B on the TAP). The TAP passes traffic from A to B and copies the IP packets to the first purple cable for capture (marked A on the TAP, with the black cable tie) and passes traffic from B to A and copies the IP packets to the second purple cable for capture (marked B on the TAP, with the white cable tie).



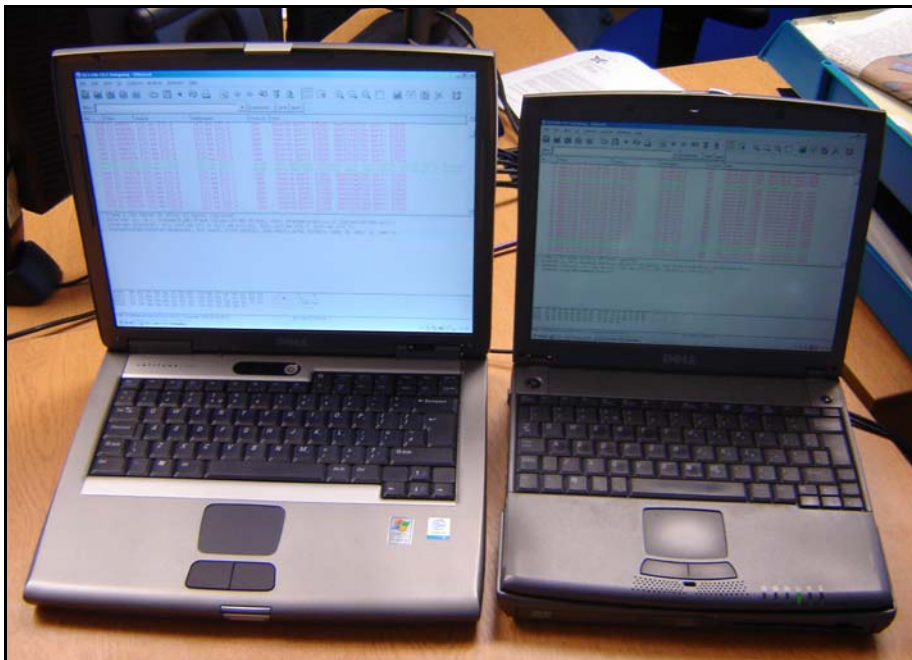
NetOptics Teeny Tap

The monitoring ports on the TAP need to be connected to a device that captures and stores the copied IP packets for future inspection. As a full duplex 100 Mega bits per second (Mbps) device can potentially

generate this amount of traffic in both directions, it is necessary to have two capturing devices (otherwise the 100 Mbps interface on the capturing device would have to discard packets); the TAP is a passive device which does not have any buffering/queuing. As a result, two laptops with 100 Mbps network interfaces were used to capture the full duplex IP traffic between the MCU and the network switch, one laptop capturing traffic from the network to the MCU and the other capturing traffic from the MCU to the network. Of primary interest for this investigation is the traffic from the MCU to the network as the MCU can have no effect on the DSCP value of packets it has not yet received; it is nevertheless useful for completeness to monitor traffic in both directions as some videoconferencing endpoints allow us to set the DSCP values at source and we can verify that the MCU receives these correctly.

As the network interfaces on the laptops do not need to be active they have been set to promiscuous mode and all protocols have been disabled. A Network Protocol Analyser must be loaded onto each laptop to capture the copied IP packets and to display and store them in an appropriate format. Several software products were looked at for this purpose, and Ethereal (<http://www.ethereal.com/>) was chosen due to the features of the product and because it is Open Source Software. Ethereal stores capture files in libpcap format, a system-independent interface for user level packet capture. Therefore it is possible to open the capture files with any software that supports libpcap files. Ethereal allows custom colouring rules to be applied to capture files. By writing colour rules it was possible for Ethereal to highlight packets marked with DSCP 46 in red, DSCP 0 (default) in black and all other DSCP values in green. Sample Ethereal output is shown below in figures T4 and T5. The colouring rules are shown below for future reference:

```
@DEFAULT DSCP@ ip.dsfield.dscp == 0x0@[65535,65535,65535][67,67,67]
@DSCP EF@ip.dsfield.dscp == 0x2e@[65535,65535,65535][63474,2761,7212]
@OTHER@ip.dsfield.dscp > 0x0@[65535,65535,65535][12904,49835,10883]
```



Laptops running Ethereal capturing traffic to and from MCU

When analysing DSCP values it is important to remember that the DSCP value is stored as part of the Differentiated Services (DS) Field, which also contains other information. The DS Field is defined in

RFC2474 (<http://tools.ietf.org/html/rfc2474>). The DSCP value is stored in the first 6 bits of the field (i.e. bit number 0-5 in the diagram below), the remaining two bits (6 and 7 in the diagram below) are not used and do not relate to the DSCP value. For example:

Bit Number	0	1	2	3	4	5	6	7
Contents	DSCP bit 1	DSCP bit 2	DSCP bit 3	DSCP bit 4	DSCP bit 5	DSCP bit 6	Unused	Unused
Decimal value	128	64	32	16	8	4	2	1
DSCP value	32	16	8	4	2	1	-	-
Example 1 – DSCP 0	0	0	0	0	0	0	?	?
Example 2 – DSCP 46	1	0	1	1	1	0	?	?

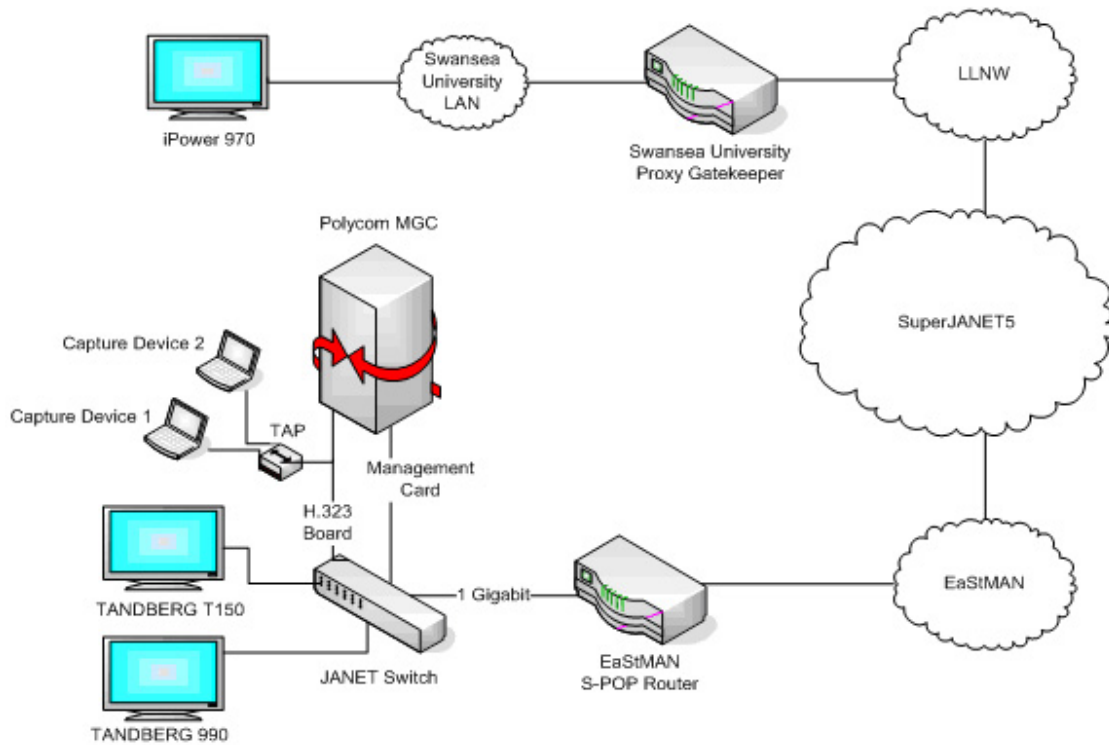
From the two examples above we can see that because only the first 6 bits are significant to the DSCP value that DS field values (in decimal) 0, 1, 2 and 3 all relate to DSCP 0 and that DS field values 184, 185, 186 and 187 all relate to DSCP 46. To make things more complicated, some DSCP values are given special names:

Name	DSCP (Decimal)
Default	0
AF11	10
AF12	12
AF13	14
AF21	18
AF22	20
AF23	22
AF31	26
AF32	28
AF33	30
AF41	34
AF42	36
AF43	38
EF	46

Some systems allow the user/operator to set the DSCP value, others such as the MCU allow the user/operator to set the DS Field. It is also necessary to take care to ensure that the correct number base is used when setting values, for example the TANDBERG T150 requires a **decimal value** to set the **DSCP value** while the MCU requires a **hexadecimal** value for the **DS Field**.

A TANDBERG T150 videoconferencing endpoint was used as a test device to receive videoconferencing calls from the MCU, and the IP traffic in both directions was captured using Ethereal on the two laptops. The network diagram below outlines the network topology used for the testing; for the duration of the testing the MCU was assigned IP address 193.60.198.164 and the TANDBERG T150 was assigned 193.60.198.150. In addition, a TANDBERG 990 assigned IP address 193.60.198.170 connected to the same network switch and a Polycom iPower 970 assigned IP address 194.83.178.211 located at Swansea University were used during the testing.

Investigation into IP QoS for the JANET VideoConferencing Service (JVCS)



**Network Topology Diagram.**

Throughout the tests the Polycom MGC was running software version 7.0.2.1, the TANDBERG T150 was running software version L4.0, the TANDBERG 990 was running software version F3.0PAL and the Polycom iPower was running software version 6.2.0.521.

A test plan was prepared that involved making controlled changes to either the videoconferencing endpoint or the MCU, observing the results and recording whether the results were as anticipated. The test plan is shown below and the capture files have been retained for future reference/analysis if required. Polycom, the manufacturer of the MGC, supplied useful QoS configuration details and copies of manual pages to assist in the production of the test plan.

Most of the tests were conducted using the Local Area Network (LAN) that the Development MCU was connected to, however some tests were made using Regional Area Networks and the JANET Backbone. Tests were conducted after the JANET Backbone was upgraded to SuperJANET5 and so DSCP values should be transparent across the backbone (SJ4 re-marked DSCP values to default for all ingress/egress traffic except for those involved in the QoS trials).

The following table summarises the purpose of each test that was conducted:

Test number	Purpose of test
1	To determine "out of the box" default QoS settings for the Polycom MGC and TANDBERG T150 videoconferencing endpoint.
2	To verify that when QoS settings are enabled on the MCU, packets leaving the MCU are marked appropriately.
3	To verify that when QoS settings are enabled on the TANDBERG T150 videoconferencing endpoint, these are applied correctly by the endpoint and received by the MCU.
4	To ensure that it is possible to amend the DSCP value that the MCU uses to mark packets

	and to verify that the amended value is applied correctly to packets leaving the MCU.
5	To ensure that it is possible to amend the DSCP values that the MCU uses to mark packets independently for video packets and audio packets and to verify that the amended values are applied correctly to packets leaving the MCU.
6	To verify that it is possible for the MCU to apply DSCP values to packets leaving the MCU for selected videoconferencing endpoints only, i.e. that applying QoS settings is not universal for all endpoints using the MCU.
7	To verify that incoming IP packets to the MCU that have travelled across RAN and the JANET backbone, reach the MCU with their DSCP values preserved. To verify that using the Global Dialling Scheme (GDS) to connect the videoconference calls using E.164 numbers does not have any affect on the DSCP values. To verify that when an endpoint in a videoconference is set manually to disable QoS, packets are marked appropriately.
8	To verify that when an endpoint in a videoconference is set to inherit QoS settings from the MCU, the DSCP values are set correctly.
9	To verify that when an endpoint in a videoconference is manually set to enable QoS using DSCP, packets leaving the MCU are marked appropriately.
10	For completeness, to verify that, in addition to marking with DSCP values, the MCU is also capable of setting IP Precedence values.

The following test plan details changes made, the expected outcome and the actual observed outcome:

Test Number	Changes Made	Expected Result	Actual/Observed Result
1	None – default settings.	Unknown.	DSCP value from MCU to endpoint <b>default</b> , DSCP value from endpoint to MCU <b>default</b> . Packets from MCU shown black on Ethereal display, packets from endpoint shown black on Ethereal display.
2	On MCU: enable 'IP Quality of Service' with 'DiffServ' option in 'Quality of Service' button located in 'Network Service Properties' for appropriate H.323 card under 'IP' in 'Network Services' under 'MCU Configuration'. See figure T1 below.	IP Packets from MCU marked with DS field value stored in MGC system configuration file. See figure T2 below. By default the DS field is set at hex 88, this is DSCP 34 or AF41.	DSCP value from MCU to endpoint <b>34</b> , DSCP value from endpoint to MCU <b>default</b> . Packets from MCU shown green on Ethereal display, packets from endpoint shown black on Ethereal display. Test passed.
3	On TANDBERG T150, set 'QoS Type' to 'DSCP' then set 'Audio', 'Video', 'Data' and 'Signalling' to decimal '46'.	Packets from MCU to endpoint marked with DSCP 34 (as test 2), packets from T150 to MCU marked with DSCP 46.	DSCP value from MCU to endpoint <b>34</b> , DSCP value from endpoint to MCU <b>46</b> . Packets from MCU shown green on Ethereal display, packets from endpoint shown Red on Ethereal display. Test passed.

4	On MCU, amend SysConfig file, 'QOS PARAMS' section, items 'DIFF_SERV_AUDIO' and 'DIFF_SERV_VIDEO' to '0xb8' (DSCP 46). Note that MCU must be reset following amendment to SysConfig file, ensure no calls in progress.	Packets from MCU to endpoint marked with DSCP 46, packets from T150 to MCU marked with DSCP 46 (as test 3).	DSCP value from MCU to endpoint <b>46</b> , DSCP value from endpoint to MCU <b>46</b> . Packets from MCU shown red on Ethereal display, packets from endpoint shown red on Ethereal display. Test passed.
5	On MCU, amend SysConfig file, 'QOS PARAMS' section, items 'DIFF_SERV_AUDIO' to '0x88' (DSCP 34) and 'DIFF_SERV_VIDEO' to '0xb8' (DSCP 46).	Some packets from MCU to endpoint marked with DSCP 46 (video packets), others with DSCP 34 (audio packets), packets from T150 to MCU marked with DSCP 46 (as test 4).	DSCP value from MCU to endpoint <b>46</b> for some packets and <b>34</b> for other packets, DSCP value from endpoint to MCU <b>46</b> . Packets from MCU shown both red and green on Ethereal display, packets from endpoint shown red on Ethereal display. Test passed.
6	On MCU, amend SysConfig file, 'QOS PARAMS' section, items 'DIFF_SERV_AUDIO' to '0xb8' (DSCP 46). Under 'MCU Configuration', 'Network Serices', 'IP', 'H323', select the 'Quality of Service' button and remove the tick from 'Enable' (see figure T1 below). On TANDBERG 990, ensure QoS values set as default ('Network', 'LAN Settings', 'QoS', 'OFF'). On MCU, setup conference between MCU, T150 and 990. Select conference, right click on T150, select 'Properties' then 'Advanced' tab and set 'Quality of Service' to 'Enable' and 'DiffServ' (see figure T3).	Packets between MCU and T150 marked as DSCP 46 in both directions. Packets between MCU and 990 marked as default in both directions.	As expected. Packets from MCU to T150 shown red on Ethereal display, packets from T150 to MCU shown red on Ethereal display, packets from MCU to 990 shown black on Ethereal display, packets from 990 to MCU shown black on Ethereal display. Test passed.
7	On MCU, setup conference to iPower system using E.164 number via GDS.	Packets from MCU to iPower marked as default DSCP, packets from iPower to MCU marked as DSCP 46 (pre-configured behaviour of iPower).	Packets from MCU marked <b>default</b> , packets from iPower marked DSCP <b>46</b> . Packets from MCU show black on Ethereal display, packets from iPower show red on Ethereal display.

Investigation into IP QoS for the JANET VideoConferencing Service (JVCS)

			Test passed.
8	On MCU, setup conference to iPower system using E.164 number via GDS. Set 'Quality of Service' to 'From Service' (see figure T3).	No change as IP service has QoS disabled (in test 6).	Packets from MCU marked <b>default</b> , packets from iPower marked DSCP <b>46</b> . Packets from MCU show black on Ethereal display, packets from iPower show red on Ethereal display. Test passed.
9	On MCU, setup conference to iPower system using E.164 number via GDS. Set 'Quality of Service' to 'Enable' and ensure 'DiffServ' is selected (see figure T3).	Packets from MCU to endpoint marked with DSCP 46 and from endpoint to MCU marked with DSCP 46.	Packets from MCU marked DSCP <b>46</b> , packets from iPower marked DSCP <b>46</b> . Packets from MCU show red on Ethereal display, packets from iPower show red on Ethereal display. Test passed.
10	On MCU, select 'Enable' in 'Network Services', 'IP', 'H323', 'Quality of Service' button. Select 'Precedence', set 'Audio' to '5', 'Video' to '5' and 'TOS' to 'Delay'. Setup conference to T150.	Packets from T150 to MCU marked with DSCP 46, packets from MCU to T150 with different value.	Packets from T150 to MCU marked as DSCP <b>46</b> , packets from MCU to T150 marked with DS field <b>44</b> (dec).

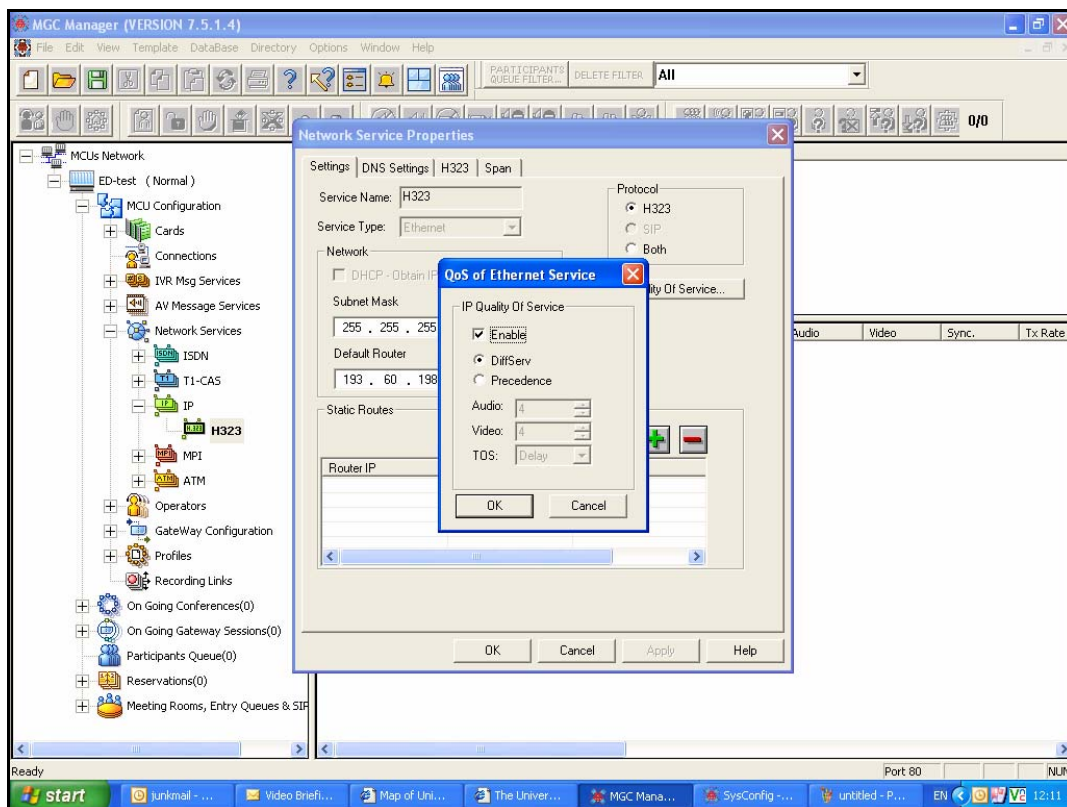


Figure T1 - Enabling QoS using Polycom MGC Manager (test 2).

Investigation into IP QoS for the JANET VideoConferencing Service (JVCS)

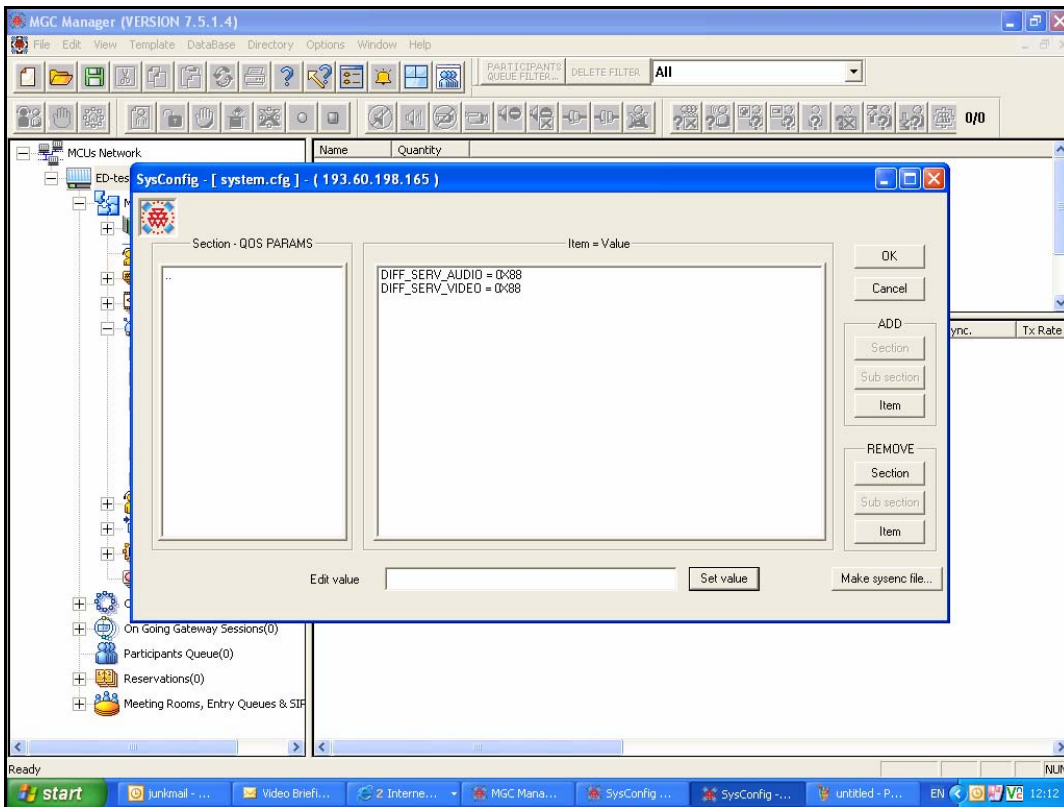


Figure T2 – Polycom MGC SysConfig file (test 2) showing default DS field values.

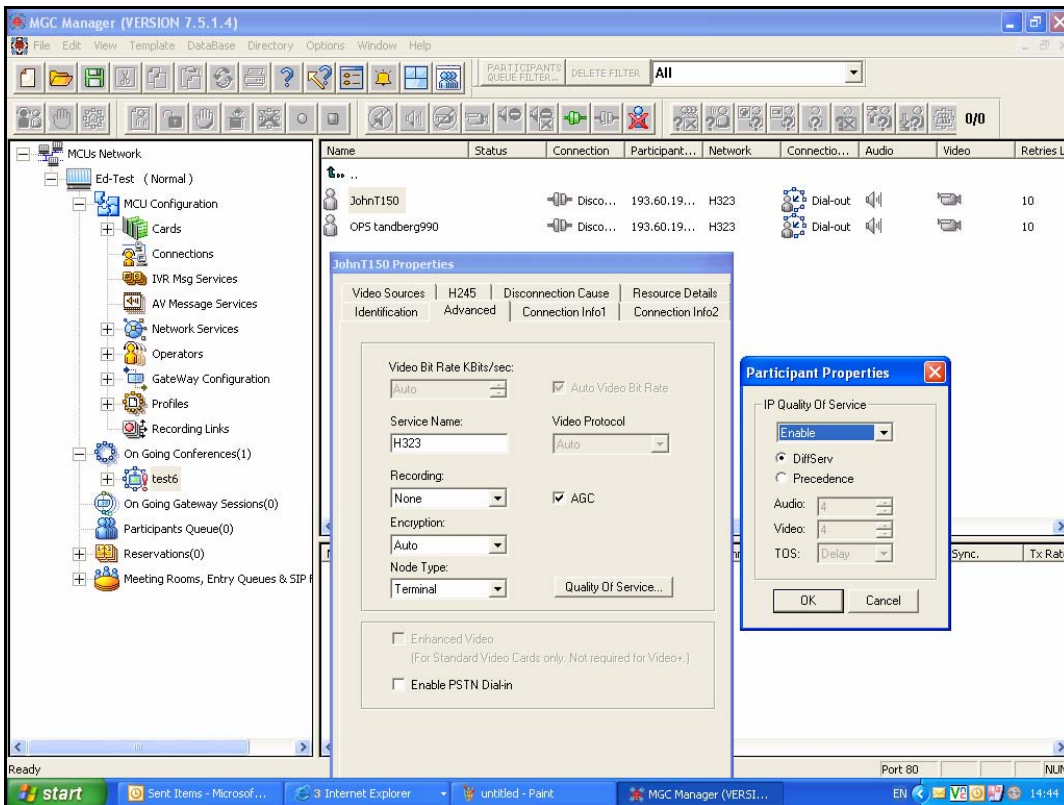


Figure T3 – Amending QoS settings on a per participant basis.

Investigation into IP QoS for the JANET VideoConferencing Service (JVCS)

The screenshot shows the Wireshark interface for a capture named '290107-Test5-Outbound - Ethereal'. The main packet list pane shows a series of UDP packets from source 193.60.198.164 to destination 193.60.198.150. Packet 149 is highlighted in blue. The packet details pane for packet 149 shows the Differentiated Services Field (DSCP) set to Expedited Forwarding (EF) with a value of 0xb8. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Info
138	2007-01-29 14:23:35.754370	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
139	2007-01-29 14:23:35.774947	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
140	2007-01-29 14:23:35.794441	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
141	2007-01-29 14:23:35.805031	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
142	2007-01-29 14:23:35.814962	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
143	2007-01-29 14:23:35.834464	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
144	2007-01-29 14:23:35.854960	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
145	2007-01-29 14:23:35.874409	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
146	2007-01-29 14:23:35.894904	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
147	2007-01-29 14:23:35.894915	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
148	2007-01-29 14:23:35.914749	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
149	2007-01-29 14:23:35.934926	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
150	2007-01-29 14:23:35.954461	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
151	2007-01-29 14:23:35.974939	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
152	2007-01-29 14:23:35.994461	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
153	2007-01-29 14:23:36.015090	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
154	2007-01-29 14:23:36.034481	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
155	2007-01-29 14:23:36.054881	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
156	2007-01-29 14:23:36.074518	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
157	2007-01-29 14:23:36.094884	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
158	2007-01-29 14:23:36.114740	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334
159	2007-01-29 14:23:36.134842	193.60.198.164	193.60.198.150	UDP	Source port: 49248 Destination port: 2336
160	2007-01-29 14:23:36.154367	193.60.198.164	193.60.198.150	UDP	Source port: 49152 Destination port: 2334

Packet 149 details:

- Frame 149 (1090 bytes on wire, 1090 bytes captured)
- Ethernet II, Src: AccordVi\_00:09:53 (00:90:ca:00:09:53), Dst: Tandberg\_01:25:41 (00:50:60:01:25:41)
- Internet Protocol, Src: 193.60.198.164 (193.60.198.164), Dst: 193.60.198.150 (193.60.198.150)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0xb8 (DSCP 0x2e: Expedited Forwarding; ECN: 0x00)
  - 1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (0x2e)
  - .... .. = ECN-Capable Transport (ECT): 0
  - .... .. = ECN-CE: 0
  - Total Length: 1076
  - Identification: 0x42af (17071)
  - Flags: 0x00

Packet bytes:

```

0000 00 50 60 01 25 41 00 90 ca 00 09 53 08 00 45 08 .P.%A...S.E
0010 04 34 42 af 00 00 1e 11 45 9e c1 3c c6 a4 c1 3c .4B....E...<
0020 c6 96 c0 60 09 20 04 20 00 00 80 e1 00 22 00 02 ... ..
0030 df 99 29 2e 87 00 21 e2 60 4f ac 7a e7 b9 a6 4d ..)....OZ...W
0040 79 9f f0 47 49 6c 9d 27 5b 1f 0b c7 80 df 04 c0 y.GIL' [.....
0050 bf 60 8c 83 eb 69 9e 3f f8 9b 63 a2 ec ca 28 7d .....i?...c...
    
```

Figure T4 – Ethereal display for test 5 showing traffic from the MCU to the endpoint. Note audio packets are coloured green (DSCP 34) and video packets red (DSCP 46). The DS Field of packet 149 has also been highlighted and displayed for information.

## Investigation into IP QoS for the JANET VideoConferencing Service (JVCS)

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays a series of UDP packets from source 193.60.198.150 to destination 193.60.198.164. Packet 149 is highlighted in red, indicating it has a DSCP value of 46. The packet details pane for packet 149 shows the Differentiated Services Field (DSCP) set to Expedited Forwarding (EF) with a Codepoint of 0x2e. The packet is 1254 bytes long and has an identification of 0x6ac3 (27331).

**Figure T5 - Ethereal display for test 5 showing traffic to the MCU from the endpoint. Note both audio and video packets are coloured red (DSCP 46). The DS Field of packet 149 has also been highlighted and displayed for information.**

The following table summarises the conclusions that can be made from each test:

Test number	Conclusion
1	By default the MCU has QoS settings disabled and sets the DSCP value to 0 (default) for outgoing IP packets.
2	When QoS settings are enabled, the MCU marks outbound videoconferencing traffic (both audio and video) with DSCP 34, AF41. In order to enable QoS on the MCU, the H.323 card must not be involved in a running conference.
3	The TANDBERG T150 sets the DSCP value correctly according to the user settings.
4	It is possible to set the DSCP value that the MCU uses to mark outgoing packets to any value between 0 and 63 (decimal). The entire MCU must be reset for changes to be applied; this implies that the setting should not be changed frequently and can only take place when there are no active conferences.
5	It is possible to set the audio packet DSCP value independently between 0 and 63 (decimal) for traffic leaving the MCU and the video packet DSCP value between 0 and 63 (decimal) for traffic leaving the MCU. There do not appear to be any options for setting other types of packet such as data or signalling.
6	It is possible to enable QoS settings on a per videoconferencing endpoint per conference basis, within the endpoint profile or at MCU (system) level. Priority is conference, profile, system. The DSCP value assigned to QoS enabled endpoints is stored in the SysConfig file and is generic to all endpoints using QoS (diffserv), it is not possible to assign different DSCP values to different endpoints. It is possible to assign QoS (IP Precedence) values on a per endpoint basis.

7	Using E.164 numbering via the GDS has no effect on the QoS settings. The Lifelong Learning Network for Wales (LLNW), the SuperJANET5 backbone and the Edinburgh and Stirling Metropolitan Area Network (EaStMAN) preserve DSCP values. Manually disabling QoS settings at the per endpoint per conference level on the MCU operates as expected.
8	Videoconferencing endpoints can be set to inherit the QoS settings from the IP service on the MCU that is being used for a conference.
9	Manually enabling QoS settings at the per endpoint per conference level on the MCU operates as expected. Therefore, settings exist at the per conference level to disable QoS settings, enable QoS settings or to use the settings from the IP service assigned (conclusion 7, 8, 9).
10	It is possible for the MCU to use IP Precedence in place of DiffServ. The MCU can use values between 0 and 5 (decimal) for video and audio and can set the TOS value to either 'Delay' or 'None'.

## General Conclusions and Recommendations

It would be possible to mark all traffic originating from the JVCS MCUs to any value between DSCP 0 and 63 (decimal). This could be applied at the system level and would affect all endpoints in all conferences (unless manually overridden). It is not possible to set different DSCP values for different endpoints, in effect a static DSCP must be chosen and this is either applied or not to endpoints in a videoconference. The MCU must be restarted if a change is made to the DSCP value used. As the SuperJANET5 backbone preserves DSCP values end to end it would be a relatively simple change (technically) to apply the settings to all MCUs that comprise the JVCS service. The UKERNA JANET QoS Development Project group should decide which DSCP value (if any) is applied for both audio and video from the JVCS MCUs. This would require a detailed policy decision as there are wide ranging views related to the relative priority that should be assigned to audio over video. Some of the factors involve the impact on Voice over IP (VoIP), the amount of IP traffic created by video, the effect of lost packets on the quality of the experience for videoconferencing participants, whether audio is more or equally important as video, reservation of bandwidth, network over provisioning, etc.

The DSCP value chosen should be published to the community so that Regional Network Operators and LAN operators can adhere to the chosen value or set their equipment to map DSCP values at their boundaries appropriately. The JVCS MCUs can only mark traffic that originates from them; for a true QoS service for videoconferencing to exist, the videoconferencing endpoint or the first capable device in the network should mark traffic destined for the MCU (or other destinations if appropriate) with an appropriate DSCP value.

It is recommended that if the JVCS MCUs are re-procured at any time, the Operational Requirement used as part of the procuring process contains specific and appropriate questions about the ability of the equipment to mark and process QoS settings. This would be necessary to ensure continuity of service should a QoS scheme for JVCS become production.

The MCU displays information on packet loss to/from a videoconferencing endpoint during a videoconference. It is not clear whether this information is subsequently stored within a log file that can be analysed or whether the details on packet loss can be provided through the Application Programming Interface (API) to the MCU or via other methods such as Simple Network Management Protocol (SNMP). It may be beneficial, should sufficient resources exist, to develop an automated mechanism that can notify either the videoconferencing venue administrator or a central support service (such as

UKERNA's Bandwidth Management Advisory Service (BMAS)) when a videoconferencing endpoint experiences regular and repeated packet loss during videoconferences. This would ensure that administrators are aware that network issues exist and lead to an increased quality videoconferencing experience for users. Further work in this area would be possible subject to appropriate resources being available from UKERNA.

As a result of investigating the ability to inspect IP traffic 'on the wire' and the relative ease with which this can be achieved, it may be beneficial to investigate how easy it is to reconstruct the H.323 media streams in order to play back a videoconference. This does not relate to the QoS project but may be beneficial for future security recommendations. Products such as ClearSight Analyzer (<http://www.clearsightnet.com/>) claim to be able to reconstruct the media streams stored in libpcap files, and although this is a commercial product, which makes it more difficult to obtain, it is likely that open source software will become available at some time in the future. Clearly access to the 'wire' would be required for a potential security breach.

## Glossary of terms

Acronym	Definition
ACL	Access Control List
API	Application Programming Interface
BMAS	Bandwidth Management Advisory Service
CAT5	CATegory 5
DS	Differentiated Services
DSCP	Differentiated Services Code Point
EaStMAN	Edinburgh and Stirling Metropolitan Area Network
GDS	Global Dialling Scheme
IP	Internet Protocol
ITU	International Telecommunications Union
JANET	Joint Academic NETwork
JVCS	JANET VideoConferencing Service
LAN	Local Area Network
LLNW	Lifelong Learning Network Wales
Mbps	Mega bits per second
MCU	Multipoint Control Unit
MGC	Media Gateway Controller
NOSC	Network Operations and Service Centre
QoS	Quality of Service
SAA	Service Assurance Agent
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TAP	Test Access Point
UKERNA	United Kingdom Education and Research Networking Association
VoIP	Voice over Internet Protocol
WVN	Welsh Video Network