

IP Premium risk management issues for Regional Networks

1 INTRODUCTION

This document describes a framework around which Regional Networks can create their own risk analysis programme. It builds on work previously undertaken in the area of general Risk Analysis by Mike Tedd and Pat Crocker for the JISC and by UKERNA and others as part of the SuperJANET4 project. Specific issues concerning the IP Premium service, highlighted by Jonathan Couzens and Roland Trice will also be addressed.

The document is presented in two distinct parts. The first an overview of the major steps necessary to roll out an IP Premium service under operational conditions. The second is a template of issues and risks that need to be investigated and addressed.

The introduction of an IP Premium pilot will cause the most far-reaching changes to the JANET network since IP replaced X.25 in the early 1990s. While the NOSC has completed a risk analysis and risk reduction study for the JANET backbone, similar work is required from Regional Networks that will be participating in the IP Premium pilot.

The QoS development group has established that the steps necessary to prepare the JANET backbone for the IP Premium pilot will take until the beginning of Q4 2003. Regional networks differ in size and topological complexity so it is important that a reasonable estimate of the time and staff effort be made at the outset. Once this cost has been identified, a Regional Network Operator will be able to determine if it can provide sufficient resources to enable participation in the IP Premium pilot.

2 IMPLEMENTING THE IP PREMIUM PILOT

A number of processes need to be performed before an IP Premium service may be piloted on the JANET backbone. Similar work needs to be undertaken in Regional Networks wishing to participate in the project. The following steps must be performed in sequence and each step must be complete before the following step is started.

Instrumentation

Traffic is examined, in order to predict the effect of policing policy on the existing service.

Traffic reclassification

Traffic from institutions not participating in the QoS Pilot marked for anything other than BE or LBE will be remarked as BE. Traffic from participating institutions that do not use the recognised values for LBE, BE and IP Premium will be re-marked as BE.

Policing

The Regional Network will impose restrictions on the amount of inbound IP Premium traffic entering their backbone from their institutions' sites. Volumes of traffic exceeding this limit will be dropped.

Enable differential queuing

IP premium packets will be given increased priority through the Regional Network.

Tuning

There are a number of parameters associated with the classification and policing of packets. Controlled changes to these parameters in order to select the optimal configuration across the Regional Network and at the handoff point into the JANET backbone.

2.1 Instrumentation

The Differentiated Services (DiffServ) model makes use of a field in the header of each IP packet termed the Differentiated Services Code Point (DSCP). The current configuration of the JANET network only uses the DSCP to identify LBE traffic. Packets marked with all other values of DSCP are treated as BE. No classification or policing is applied at the edge because there is no danger of the LBE traffic having an adverse effect on the other traffic. Many Regional Networks operate in a similar way.

It is essential to determine how much traffic is being transmitted into the Regional Network with DSCP values set to IP Premium. This is because if a regional network were already transmitting more packets marked for IP Premium than the rate to which it will be policed during the pilot, turning on policing would cause existing service traffic to be dropped.

Whereas DiffServ uses the DSCP to distinguish between packets in particular services classes, queue management used in the GSR routers in the backbone is based on examining the Precedence field, which forms part of the DSCP bit field.

As well as the DSCP value corresponding to the IP Premium service, seven other DSCP values map to the same value of IP Precedence (named the "Near Premium" DSCPs in this document); hence, the routers will need access control entries to look for all eight DSCP combinations.

It will be necessary to closely monitor all traffic classes to assess performance before, during and after any changes are made to the network.

Many Regional Networks use other routing equipment than Cisco GSRs. It is essential that the features of each Regional Network's hardware and operating system, which apply to traffic classification, marking and priority queuing, be thoroughly understood before work is started.

2.2 Traffic reclassification

All packets entering the Regional Network will now be examined and processed. Packets from institutions not involved in the IP Premium pilot with the DSCP field set to the IP Premium or Near-Premium values will all be re-marked for the BE service. All packets marked for LBE or BE will be left unchanged.

Traffic from participating institutions that does not use the recognised values for LBE, BE and IP Premium will be re-marked as BE.

Before the backbone begins to police IP Premium traffic levels, each of the regional networks that are participating in the pilot will need to state in writing that all traffic marked for IP Premium is authorised to do so. They will not be able to do this until their own backbone has been instrumented.

Once a regional network has made this undertaking, the NOSC can begin to police traffic from the regional network into the backbone. Participating Regional Networks will also need to police inbound traffic from their institutions in order to ensure that the outbound traffic from the Regional Network does not exceed the policing limit imposed at the BAR.

2.3 Policing

Packets from institutions participating in the pilot marked for IP premium will be let through so long as they do not exceed the permitted bandwidth assigned to the institution. Traffic exceeding the permitted bandwidth will be dropped.

The JANET backbone will not shape IP Premium traffic outbound to the regional networks, because this could increase jitter. It will, of course, be necessary for the regional network to police IP Premium traffic inbound to their network, or run the risk of a DoS attack (marked for IP Premium) consuming all their incoming bandwidth.

2.4 Enabling preferential queuing

Once every institution's connection has been instrumented and policing has been applied, it will be possible to enable the preferential queuing of packets marked for IP Premium.

This will require that all backbone routers in the Regional Network have new queuing structures configured with what we believe to be appropriate "first guess" parameters. This work needs to be done on any router in the regional backbone that could provide transit between any two participating institutions.

This must be the case under all failure conditions; so all non-edge routers in the regional backbone will need to be so configured. However, it will only be necessary to configure preferential queuing in edge routers that are connecting to institutions participating in the IP Premium pilot.

2.5 Tuning

It is extremely likely that the configuration parameters chosen for the previous phases of the pilot will need to be changed in the light of experience. Two distinct sets of parameters can be manipulated to change the way traffic is handled. These are:

The parameters associated with the policing of traffic, as implemented as part of phases one and two of the pilot. For example, we have the choice to re-mark or drop traffic that is outside the bounds of the permitted traffic contract.

The parameters associated with congestion management. These include queue depths, mark probabilities/thresholds and relative queue priorities.

It is generally accepted that the values of the congestion management parameters depend on the specific traffic mix on the network concerned. As such, the initial values are very much a guess, albeit an informed one. These parameters will inevitably require adjustment.

As the traffic mix on JANET and the Regional Networks change due, for example, to new applications, these parameters will require constant monitoring and regular adjustment to maintain an optimal balance between packet loss and bandwidth utilisation.

3 RISK ANALYSIS

Taking the now standard risk headings, the second part of this paper will discuss the risks involved in piloting an IP Premium service. It is not intended to provide answers to particular risks for particular Regional Networks, due to the differences between Regional Networks and the JANET backbone. However, it should act as a template to suggest areas for consideration.

Regional Network Operators should already have completed risk analysis programmes on their networks as part of the RPAN contract. It is anticipated that the areas of risk examined in this paper will be analysed using existing mechanisms and infrastructures.

The four major areas of risk identified in the Tedd report, are Architectural, Capacity, Environmental and Security. Environmental risks may be left to one side, since they are not likely to change with the introduction of a QoS pilot. The other areas should be considered in detail.

3.1 Architecture risks

Evaluate the changes you will need to make to your network and the likely impact on service reliability. If you are unable to test new features outside of a production environment, the risks will increase. Issues to consider may include:

The network becomes more difficult to manage due to additional complexity.

The deployment of particular software or configuration triggers bugs caused by interaction with other software or hardware features running in the network.

Human error increases due to complexity.

An increased reliance may be placed on the few key members of staff who understand what is going on.

The network behaves in unexpected ways, either through insufficient experience of your IP engineers, or through poor vendor documentation.

Your Network Management Systems lack the necessary tools to monitor the performance of IP Premium facilities, making problem detection and resolution more difficult.

3.2 Capacity

Examine the capacity of your network in order to evaluate your ability to set aside bandwidth for IP Premium testing. Existing services should not be affected by the pilot project so it is vital that sufficient bandwidth is set aside for Best Efforts traffic. Other capacity issues include:

You need to evaluate the ability of your network equipment to distinguish between different traffic classes and to queue and forward packets as necessary. There is doubt about the ability of some equipment (Cisco 75xx routers for example) to cope with the extra CPU load. This may be especially true if packet classification and access control is performed in software rather than hardware.

You need to determine the amount of staff effort that will be required to effectively participate in the project, considering that involvement will mean undertaking all the steps described in item 2 above.

3.3 Security risks

There is a risk that a Denial of Service (DoS) attack will be directed against the IP Premium class and that all the pilot traffic is dropped.

If a participating institution in your MAN has a low bandwidth connection, a DoS attack may result in the complete loss of service to that institution. This is because it is probable that the entire bandwidth of a low capacity link would need to be treated as IP Premium, in order that the total bandwidth is sufficiently useful.

4 REFERENCE

The following documents are available from

<http://www.superjanet4.net/risk/index.html>

Technical Advisory Unit JANET Risk Analysis Study Final Report

Mike Tedd & Pat Crocker November 1999

Results of the UKERNA Risk Analysis Programme

Roland Trice February 2000

Notes from Discussion Session of the SuperJANET4 Managing Risks
Workshop

Bob Day February 2000

Risk Analysis for MANs

Roland Trice October 2000

The following documents are available from the password restricted QoS pages:

<http://www.ja.net/development/qos-private/meeting/meeting.html>

Overview of QoS Deployment Risk Analysis (PowerPoint presentation)

Roland Trice November 2002

Technology and Instrumentation Update (PowerPoint presentation)

Jonathan Couzens November 2002