

Lay Byes and Fast Lanes . . .

How network optimisation can fast track performance
in all the right ways



In this, the third in a four article series about network optimisation and the way modern technology trends are impacting network flows, we take a closer look at how rogue and other unsolicited traffic can derail the smooth running of the network.

Checkpoint: Some hints and tips for optimisation strategies

Through the course of our 20 year-long network heritage, we've come to some insights about maximising the network. The first of these is that when it comes to optimising your network, it's important to consider the whole chain – all the elements and interdependencies – you cannot just assess the network in isolation. So an integral step in any optimisation project is to consider the impact of all the diverse applications you run on the network (as we have done by looking at some of emerging technology trends in this series of articles).

Secondly, understanding current performance is a critical starting point. If you don't know what your current "performance posture" is, how do you measure anything (trends, user complaints, impact analysis, capacity planning, etc)? Without this grasp of your existing performance posture, it's almost impossible to optimise successfully.

You can use these factors as a starting point to consider some common, and often unplanned for loads on your network, such as rogue traffic and unsolicited traffic.

You can use these factors as a starting point to consider some common, and often unplanned for loads on your network, such as rogue traffic and unsolicited traffic.

Consumers have become rapid adopters of new technology, **and they are skilled users of these new technologies** – everything from SKYPE to MSN to Instant Messenger (IM).

More bottlenecks on the information highway

Rogue traffic is a phenomenon that can have a far-reaching impact on the network. Consumerisation and the socialisation of IT are arguably two of the biggest drivers of change in IT today – and we still don't fully understand the scale and reach of their impact. For the first time ever, consumers are ahead of IT departments. They no longer learn technology in the workplace – they do that at home – and are using technology and services well in advance of the tools they are provided with in the workplace.

Consumers have become rapid adopters of new technology, and they are skilled users of these new technologies –everything from SKYPE to MSN to Instant Messenger (IM). Leading industry analysts suggest that more than 50% of traffic on corporate networks

is not business-related, and that companies have very little visibility of this. They have even less idea how this rogue traffic impacts on corporate or enterprise traffic and applications. For example, to guarantee acceptable voice quality, SKYPE always sets the "Type of Service" (TOS) field to the highest value to guarantee highest priority for its traffic in a network – this means that the SKYPE traffic of a corporate user talking to a friend, will always be guaranteed better treatment than say, data sessions to a company ERP system – warning signs should be flashing for your network performance! Add to this, the existence of more than 700 million IM users – that includes just about every office worker – all using socialisation applications that can sap the bandwidth resources of companies during working hours.

The key challenge facing most companies is that they have so little visibility, policies or controls around how to manage this rogue traffic. Workers incorporate these services into their daily working habits and this has significant impact on the overall performance of the corporate network. It would be short-sighted to ignore or overlook the impact of these social and technology trends when reviewing your overall approach to performance engineering and optimisation.

Security and unsolicited traffic represent another growing trend that is having huge impact on the conduct of business. Security threats are often the source of unwanted loads on the networks – for example, spam and high graphic pop-ups. Network congestion as a result of worms, viruses and denial-of-service attacks are also frequently the cause of poor performance of key enterprise applications and need to be addressed to safeguard and optimise the network. Performance management in this new world of security challenges and unsolicited traffic is as much about keeping unnecessary or malicious traffic off your network, as it is about controlling and engineering your legitimate traffic.

In the next and final article in this series, we put the trends of convergence, rich content and globalisation, under the optimisation microscope, and shine a light on some pitfalls and solutions.

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • GHANA • KENYA
MOROCCO • NAMIBIA • NIGERIA
SAUDI ARABIA • SOUTH AFRICA
TANZANIA • UGANDA
UNITED ARAB EMIRATES

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES