Advanced communication services for Extranets

I. Bartolini, G. De Zen*, L. Lazza, G. Ricagni, G. Rigolio - ITALTEL SPA

*Giovanna De Zen, Italtel
Palazzo Laboratori - C02
20019 Castelletto di Settimo Milanese (MI)
Italy
tel: + 39 02 4388 7393
email: giovanna.dezen@italtel.it

Keywords: Extranet, Internet, Internet / PSTN Interworking, Integrated Services, Differentiated Services, Quality of Service, N-ISDN, B-ISDN, Guaranteed Bandwidth

Subject Area: Business Application, Internetworking

Presentation Preference: Technical Speech Sessions

Abstract: The paper deals with the issue of Quality of Service over Extranets, proposing four different approaches to provide extra bandwidth on links between different corporate sites to those employees running applications that require it. The basic idea is that of having a cheaper corporate Extranet, either because it is designed for lower capacity or because it is an Internet based Virtual Private Network, and to add bandwidth whenever required. The additional bandwidth requests are handled by the Sistina platform which controls the set up of on demand connections between corporate sites, based on ISDN, B-ISDN or on the Integrated Services signalling protocol (RSVP). In case of a Differentiated Services core network, Sistina provides a mechanism for admission control to the resources available at the various Differentiated Service levels. Major points of added value with respect to traditional solutions are the possibility to apply complex policies to authorise bandwidth request from employees, the possibility to set up RSVP reservations for RSVP unaware applications, as well as the possibility, foreseen by some of the scenarios, to have the additional on demand switched connections dedicated to the transport of traffic generated by (or directed to) a single user, who can enjoy, in this way, hard bandwidth, delay and jitter guarantees. This results in a substantial improvement in the quality perceived by users of those services requiring higher bandwidth than that provided by the plain best effort Internet. Examples of such services are video conferences, audio conferences, on line audio/video interactions, tele learning applications and high speed file transfers.

1. Introduction

Most corporate networks span a number of sites. The term Extranet defines that part of private networks located outside of corporate boundaries. Extranets can be implemented in many ways, ranging from a full mesh of fixed bandwidth leased lines, to networks based on Frame Relay or ATM (Asynchronous Transfer Mode), to tunnels over the public Internet, the so called Virtual Private Networks (VPNs). In each of these cases, Quality of Service (QoS) is an issue. If users on the Internet have become accustomed to the well known World Wide Wait, similar performances are not something one would expect from a private network. This paper deals with the issue of QoS over Extranets, proposing four different approaches (see Figure 1) to provide extra bandwidth to those employees running applications that require it. The basic idea is that of having a cheaper corporate Wide Area Network (WAN), either because it is designed for lower capacity or because it is an Internet based VPN, and to add bandwidth whenever required. The additional bandwidth is provided by on demand connections established between corporate sites, based on Integrated Services Digital Network (ISDN) technology, Broadband-ISDN (B-ISDN) or on the Integrated Services (IntServ) Resource reSerVation Protocol (RSVP). A fourth approach foresees a Differentiated Services (DiffServ) core network, and a mechanism to provide admission control to the bandwidth available at the various DiffServ levels, defined by the Service Level Specification (SLS). Major points of added value with respect to well known Bandwidth-on-Demand solutions are the possibility to apply complex policies to authorise bandwidth request from employees, as well as the possibility, foreseen by some of the scenarios, to have the additional on demand switched connections dedicated to the transport of traffic generated by (or directed to) a single user, who can enjoy, in this way, hard bandwidth, delay and jitter guarantees. At the core of the system, a centralised server, the Sistina Service Node (SSN), acting as policy decision point for the authorisation of bandwidth allocations, as a database containing all the information required to establish connections, as well as a manager that controls routers to set up the requested connections. SSN also provides RSVP unaware applications with the capability to allocate bandwidth via RSVP between corporate sites.
An analysis of costs and benefits of the proposed solutions is provided.

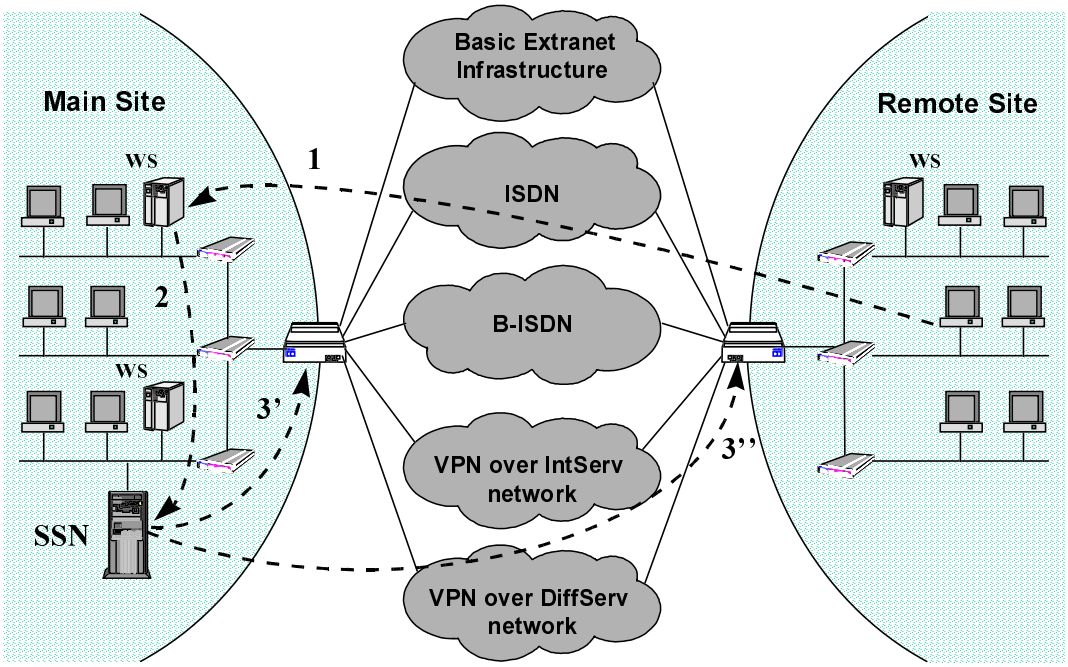

Figure 1

2. Advanced communication services in the Sistina environment

The SISTINA environment (Solutions for Integrated Services à la TINA - Telecommunications Information Networking Architecture, [1]) foresees different network scenarios where advanced communication services can be provided. Sistina is the result of a research activity performed by Italtel aimed at supplying QoS services to both residential and business IP users. As far as residential users are concerned, the Sistina solution [2] is applied in the context of web browsing, to enhance the WWW experience with high quality video conferences and multimedia streaming, while for business users it is applied to Extranet connections within enterprises with many geographically distributed sites.

When the connections between the end user and the Web or between two corporate sites are supplied by a Best Effort Internet (BE Internet) service, the problem of the QoS is solved by Sistina exploiting the advantages of two apparently contrasting worlds such as the Internet and the Public Switched Telecommunication Networks (PSTN). In detail, Sistina enables the provision of high quality services in BE Internet by setting up ISDN or B-ISDN dedicated switched connections and by routing the IP traffic concerning the user's QoS requests towards these links.
On the other hand, when a QoS Aware Internet service is available, Sistina is capable of providing diversified quality of services by routing the IP traffic not through a PSTN dedicated switched connection, but instead on QoS aware communication channels across Internet. It is the case of Integrated Services and Differentiated Services.
In both scenarios, Sistina supplies its service by controlling commercial network equipment like Routers and Acces Servers and by instructing them to route the IP traffic towards an appropriate path (PSTN or QoS Aware Internet). This results in a substantial improvement in the quality perceived by users of those services requiring higher bandwidth than that provided by the plain BE Internet. Examples of such services are video conferences, audio conferences, on line audio/video interactions, tele learning applications and high speed file transfers. Moreover, we want to stress that Sistina is much more than a Bandwidth-on-Demand solution in that it provides fine grain policies, that allow for a personalised management of advanced communication services. To this end, Sistina provides a user classification that includes different levels of privileges and that is able to give to each user the qualification to access a specific pool of services.
A question could arise from the reader: "How are these advanced communication services made available to the user?". In our solution, users can access QoS enabled services, like a QoS video conference, by means of web servers, which offer a user friendly WWW interface. As shown in Figure 1, upon a service invocation, the web server interacts with the main actor, the SSN, in order to verify, on the basis of the user profiles, if the involved users are allowed to enjoy the requested service. In the positive case, the SSN dynamically configures the interfaces of the dialup[1] routers (or the edge[2] routers) located in the communicating sites to route the QoS flows through a specific path defined over one of the possible networks. Such path can be defined over a Public Switched Telecommunication Network, such as ISDN or B-ISDN or a Virtual Private Network based on an Integrated or Differentiated Services network.
Sistina only requires the addition of a single centralized SSN within each corporate network. Intranet web servers must communicate their requests to the centralized node which, in turn, manages commercial routers to allocate the requested resources.
Summarising, the SSN is in charge of verifying user privileges, configuring routers, accounting the cost of communication services and charging them to the different cost centres.

3. Quality aware Internet

One of the main motivations to adopt solution like the one presented here is the need to ensure, in some cases and for selected applications, the quality of the transmission. Presently the Internet technology only offers a flat best effort service, and quality sensitive applications might suffer; hence, the need to "divert" the traffic of sensitive applications onto a more reliable transport, like a dedicated switched connection, e.g. by means of the services offered by the SSN.
However, in the Internet (and Intranets) of today, bandwidth has become undoubtedly an important subject. More and more people are using the Internet for business and private purposes, or even for leisure. Moreover, new real time applications, such as Internet phone, and video conferencing or video retrieval need a lot more bandwidth than previous applications and they are more sensitive to delay and packet loss. Therefore, new concepts are being developed for the next generation Internet aimed at guaranteeing a specific QoS, enhancing the basic IP protocol stack which currently only provides best effort service.
New strategies are being developed to provide enhanced services in the Internet; today there are two main approaches accredited to bring QoS to the Internet:

- Integrated Services
- Differentiated Services

Integrated Services [3] brings enhancements to the IP Network Model to support real time transmissions and guaranteed bandwidth for specific flows. A flow is roughly defined as a stream of correlated datagrams from a unique sender to a unique receiver, within a session, that requires the same QoS. By

[1] the site or departmental routers, with BRI/PRI ISDN or B-ISDN interfaces, which are configured by the SSN to setup switched connection towards other remote dialup routers
[2] routers which connect the Intranet with the Integrated / Differentiated Services QoS Aware Internet

means of a specific signalling protocol (the most accredited one being RSVP) appropriate amount of network resources are assigned to the flow, enough to guarantee the required Quality.
In the other approach, Differentiated Services mechanism [4], no use of per flow signalling is foreseen. Different service levels can be allocated to different groups of Internet users, which means that the whole traffic is split into groups with different QoS parameters. This surely reduces the Quality control overhead in comparison to Integrated Services, but at the cost of a coarser quality support. Next sections briefly expose the details of these two approaches.

3.1 Integrated Services and RSVP

To support the Integrated Services model, an Internet router must be able to provide an appropriate QoS for each flow, in accordance with the service model.
The router function that provides different qualities of service is referred to as “traffic control”.
It accounts for:
Packet scheduler: manages the priority in forwarding packets.
Packet classifier: identifies packets of an IP flow to receive a certain level of service.
Admission control: the algorithm that the router apply to determine if there are enough resources available to guarantee the QoS requested by a new flow.
The Integrated Services use RSVP for the signalling of the reservation messages. The RSVP protocol runs on top of IP and/or UDP and must be implemented in all routers on the reservation path. The RSVP protocol is receiver initiated. Using RSVP signalling messages, the sender provides a specific QoS to the receiver, which sends an RSVP reservation message back with the QoS that should be reserved for the flow from the sender to the receiver. This behaviour has been defined to optimally account for the different QoS requirements for heterogeneous receivers in large multicast groups.
This infrastructure is used to offer the user a choice of services, which enhance the pure best effort service. Two quality aware services have been identified in the integrated service model, namely Guaranteed Service (GS)” and “Controlled Load (CL)”.

Controlled Load Service
If an application uses the Controlled Load Service, the performance of a specific data flow does not degrade even if the network load increases.
The Controlled Load Service class does not define specific target values for control parameters such as bandwidth, delay or loss, but only offer the same behaviour of lightly loaded network, independently from the actual load over the network.

Guaranteed Service
The Guaranteed Service model provides functions that assure that packets will arrive within a guaranteed delivery time. Every packet of a flow that conforms to the traffic specifications will arrive at least at the maximum delay time that is specified in the flow descriptor. Guaranteed Service is used for applications that need the guarantee that a datagram will arrive at the receiver not later than a certain time after it was transmitted by its source.

3.2 Differentiated Services

Analogously with the Integrated Service model, the goal of the Differentiated Services approach is to provide differentiated classes of service for Internet traffic, to support various types of applications and specific traffic requirements. DS offers predictable performance (delay, throughput, packet loss, etc.) for a given load at a given time. The difference between IS and DS is that DS provides scalable service discrimination in the Internet without the need of per flow state and signalling at every hop. With DS, the Internet traffic is split into different classes with different QoS requirements. A central component of DS is the SLS, a service contract between a customer and a service provider that specifies the details of the traffic and the corresponding forwarding service a customer should receive.
Unlike in Integrated Services, applications using DS don't need to set up QoS reservations for specific data packets. A specific bit pattern, called the DS byte, in each IP packet is used to mark a particular forwarding treatment the packets will receive at each network node
Each DS capable router must implement a known, specific “Behaviour” (known as Per Hop Behaviour, PHB): on this basis, the forwarding treatment a packet receives depends on the value of the DS byte. The PHB can be described as a set of parameters inside of a router that can be used to control how packets are scheduled onto an output interface.

4. Advanced communication scenarios exploiting Sistina services

Multi site enterprises typically exploit Extranet solutions to allow for data exchange between different sites. Companies can take advantage of different technologies to build their Extranet. A first solution consists in creating a fully meshed network of leased lines between the locations which need to be interconnected. This is a very expensive solution, since connectivity providers request very high annual fees for leasing their lines. On the other side, the company is guaranteed that the leased lines are dedicated to the company data traffic. Therefore, this solution is not advantageous for companies with small subsidiaries or low inter site traffic. With the wide spreading of Internet and VPN services, the opportunity of building Extranet solutions at a lower price has emerged. In fact, the possibility of using the Internet for the transfer of private encrypted data allows to save the cost of the dedicated inter site connections with the drawback of a quality of service detriment (the classical Internet is a best effort network which is not able to guarantee any quality of service). Moreover, the availability of Virtual Private Dial up Networks (VPDNs) enables the utilisation of dial up connections for VPN access and therefore the minimisation of access costs with respect to leased lines.

4.1 Internet/N-ISDN interworking scenario

In such Extranet scenarios, the advantages deriving from the introduction of the Sistina capabilities is very appealing. In fact, thanks to the integration of the Internet and ISDN networks, Sistina enables the transparent activation of switched ISDN connections which are used for data communication between two remote sites only for a limited time. This capability is very interesting as it allows an efficient and suitable management of spot bandwidth requests. Quite often, it turns out that a leased line or a Internet based VPN is not able to satisfy an extra bandwidth request or to guarantee that a particular data communication takes place with the required QoS, in terms of bandwidth and maximum delay. It may happen because the Extranet is undersized to keep fixed costs low, the VPDN dial up connections have a low bit rate (e.g. only 64kbps), or the VPN is built on top of a best effort and congestioned Internet backbone.

Services like video conferences between remote departments, tele learning or multimedia interactive applications shared by remote users could be activated by the company employees interacting with the Sistina platform via Intranet web servers, as shown in Figure 2. Using the Sistina technology the company has no need to oversize its Extranet, since the inter site extra bandwidth requests are traduced in the activation of dedicated ISDN connections between the involved sites for the duration of the requested service. The ISDN connections can be established making calls to the E.164 addresses belonging to an ISDN VPN for exploiting special charging policies.

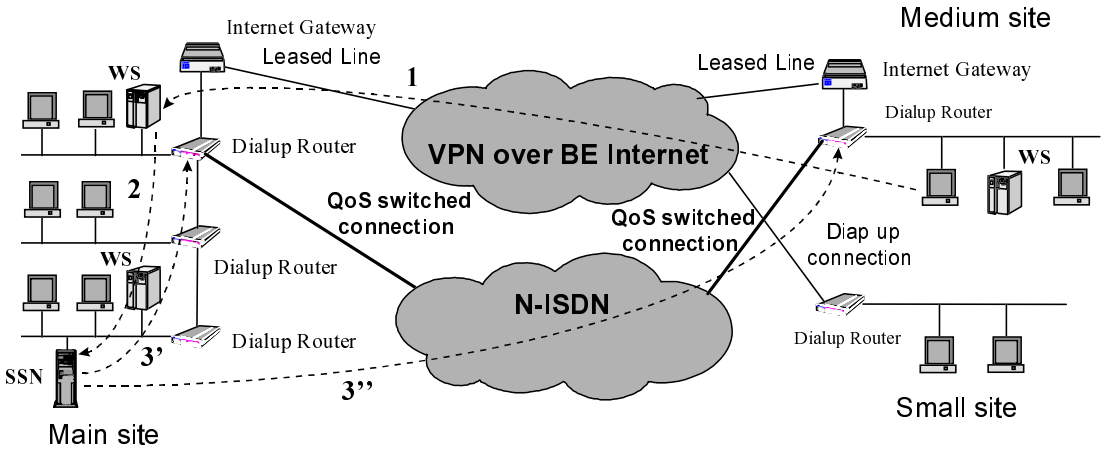

Figure 2

4.2 Internet/B-ISDN interworking scenario

The availability of a B-ISDN infrastructure can add even more value to Sistina switched services. The benefit in terms of increased end to end bandwidth, and reduced delay provided by the switched connection will be even more noticeable. Switched ATM connections will be used to convey IP traffic between different company premises, and will be set up at user request, when the service to be provided requires that extra QoS (bandwidth, delay, jitter) that the corporate Extranet cannot provide, as depicted in Figure 3. Once again, the added value with respect to simpler Bandwidth-on-Demand solution is that

- policies based on the requesting user's privileges can be applied. They are enforced by the SSN, also in charge of authenticating users and of controlling routers involved in the connection set up;
- the switched connection can be entirely dedicated to the transport of traffic from the requesting user: it is something more than just another pipe that all packets heading for that same destination can use.

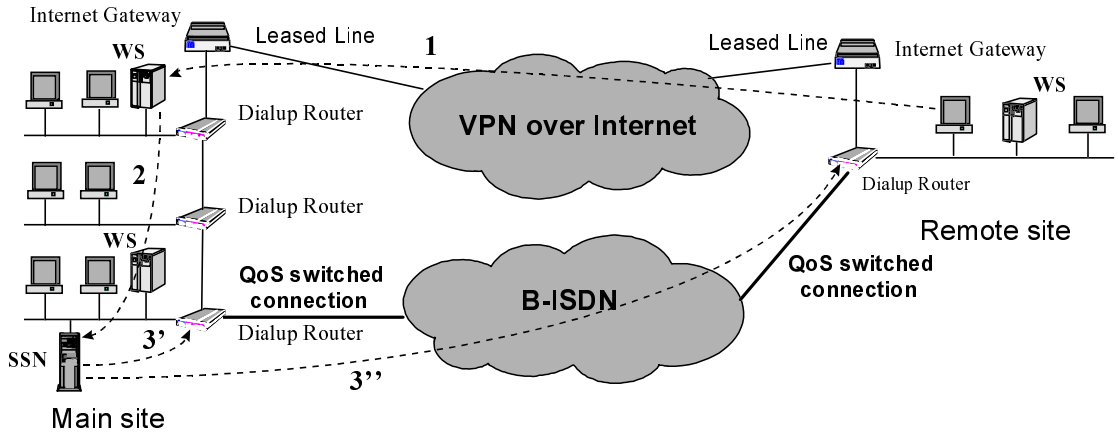

Figure 3

4.3 QoS aware Internet scenario

The scenario can be greatly different if the public Internet is able to offer diversified quality of services, in addition to the plain Best Effort transport. In fact, in this hypothesis, to offer the necessary quality to the Extranet applications according to the philosophy already described, the spectrum of options is enriched, and includes the possibility to route the session not only on a dedicated switched connection, but also on adequately quality instructed communication channels across the Internet.
As mentioned, the evolution of Internet toward quality aware services is progressing along two main directions, namely Integrated Services and Differentiated Services.

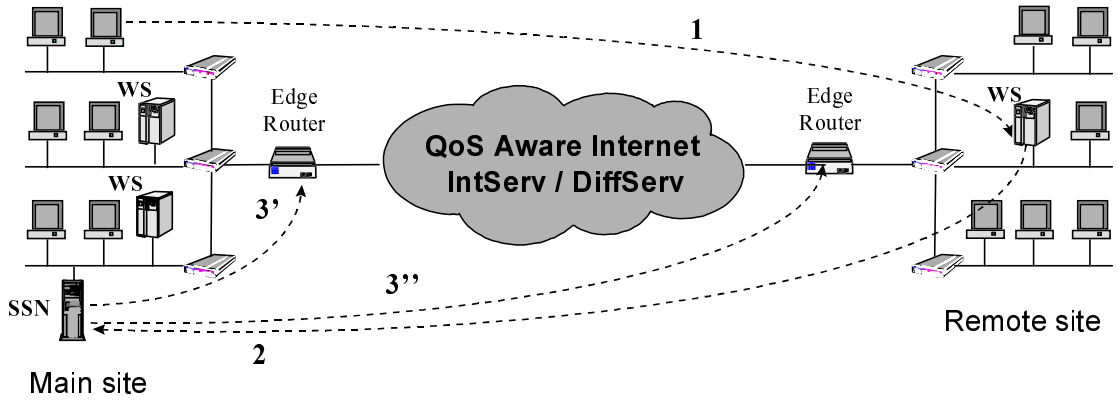

Figure 4

4.3.1 Integrated Services in the Internet

The first scenario requires the applications to be able to initiate RSVP sessions, i.e. to require the core Internet to set up communication paths with enough resources to adequately support the requirements of the applications itself.
The application environments of the future will possibly directly offer RSVP, which in fact it is expected, for example, to be embedded in most future versions of the mainstream operating systems. However, the diffusion of such QoS aware tools will not surely be a matter for the immediate future, and existing applications, non RSVP capable, will persist for long. In addition, in an Extranet environment, it is highly realistic that the usage of quality–assured communication services will have to observe restrictions on who/when is allowed to benefit of them, according to specific company policy, similarly to what happens now e.g. for restrictions on international calls.

And here comes the role of the SSN: as soon as an Extranet multimedia session is required, having intrinsic Quality of Service requirement, one Extranet user might access a specific web page on a Sistina enabled Intranet web server, that than forwards the request to the centralised node, see Figure 4. The SSN, in addition to all the other functionality (Admission, Security, …) operates as a centralised RSVP controller-manager; therefore, once completed all the required checks, it operates as initiator of the RSVP session on behalf of the "RSVP blind" application. In this role, the SSN will then generate the appropriate commands to instruct the edge router (offering access to the public Internet, and RSVP capable) to act as sender in the RSVP session to be. Another command will be sent by the SSN to the edge router of the remote Extranet site hosting the destination terminal, forcing it to act as receiver of the session. By this, according to normal RSVP procedures, a channel will be created across the core IP network, with enough quality guarantees to accommodate the needs of the application. It must be noted that resources will not be allocated in intra LAN segments of the two Extranet sites, but this is not seen as restrictive as this is normally a lightly loaded branch, and the real problem is in the path across the public Internet.

4.3.2 Differentiated Services in the Internet

The other possibility the Internet of the next future might offer to support QoS is the Differentiated Service approach. As said, in this case no per session (or per flow) resource reservation is guaranteed, but access to network resources is managed according to mutual agreement between the ISP and the customer. IP packets are "marked" as eligible for a given quality handling by appropriately setting the DS byte, and on this basis they will obtain a given priority along the core Internet paths.
Again, in this scenario, the hypothesis is that terminals and applications are not directly enabled to run DiffServ procedures, and the whole solution will be managed under the control of the SSN. On instruction of the SSN, stimulated by a user initiated procedure via a web page as normally assumed here, the local access router toward the public Internet will have to set the DS byte in the outgoing packets to force the public network to prioritise their handling.
However, the use of DS is possible only when the SLS regarding the local network access has been defined with the ISP. In this action is easy to imagine a remarkable role for the SSN. By controlling the type and the amount of applications requiring QoS sessions across the public Internet, and by arbitrating the eligibility of any of the attempt initiated within the local network, the SSN is in the best position to limit the traffic volume and the traffic profile originated within the local network. On this basis, it can evaluate whether the actual traffic profile matches the SLS as agreed with the ISP, and thus accept or deny incoming requests for quality assured applications.
As a further evolution of the role, and if this will be supported by the ISP, SSN will even be able to dynamically estimate the exact terms of the contract e.g. along the hours of the day or the days of the week, and thus to dynamically modify the SLS as required to follow the variation of the traffic interest among the different Extranet sites.

5. Considerations on benefits and costs

As described in the paper, the Sistina solution allows for a lower corporate WAN cost, either because the network is designed for lower capacity or because it is an Internet based VPN. Bandwidth can be added whenever required by means of on demand connections established between corporate sites, based on ISDN technology, B-ISDN or RSVP. ISDN connections can be set up making use of an ISDN VPN to take advantage of special charging policies. Another major important benefit is the possibility to have a high degree of control on communication costs, in that the SSN allows for the application of fine grain policies on the user groups allowed to allocate resources on the Extranet. Moreover it is possible to keep trace of such costs and to attribute them to each of the company departments. The admission control functionality, provided by the SSN in case of a DiffServ core network, allows for the control of who and when accesses the valuable resources purchased at the various DiffServ levels.
No investment must be made in new routers, as in most cases existing equipment can be used and dynamically configured by the SSN. The main investment required by the Sistina architecture is the SSN itself (which is a Unix server) in terms of both hardware and software. As far as the connectivity costs are concerned, the market has not yet given an answer to the question on how much RSVP/DiffServ allocated bandwidth will cost. Anyway, in case of switched (ISDN and B-ISDN) connections, it must be noticed that they are only activated for the duration of the service, and that ISDN/B-ISDN VPNs can be exploited, since the connections are only set up between the corporate sites.

6. Conclusions

Multi site enterprises can successfully take advantage of Sistina capabilities which allow both to minimise inter site connection costs, guaranteeing the on demand availability of extra bandwidth, and to control the utilisation of such additional communication resources on a per user and per service basis, enabling the QoS costs charging to the different cost centres. A large number of multimedia and interactive applications would exploit this possibility empowering business users to increase their productivity.

Benefits can be appreciable not only in the current Internet scenario but even in a QoS Aware Internet. Whenever Integrated Services are provided by the ISP but RSVP is not yet supported by end user applications, Sistina allows for a smooth transition towards the target scenario as well as the enforcement of policies on resource allocation requests. In the case of a Differentiated Services network, Sistina enables the implementation of admission control policies which are particularly useful in presence of not RSVP capable terminals.

In conclusion, the great advantage of the proposed solution in supplying advanced communication services is its capability to combine, in an efficient and flexible way, the management of routers' capabilities with the handling of user privileges and policies.

7. References

[1] G. De Zen, M.A. Marsiglia, G. Ricagni, L. Vezzoli, H. Hussmann, H. Schoenbauer, M. Sevcik, A. Zoernack: "Value-added Internet: a pragmatic TINA-based path to the Internet and PSTN integration", TINA Conference, Santiago of Chile, November 1997

[2] G. De Zen, M.A. Marsiglia, G. Ricagni, L. Vezzoli: "Accountable and Guaranteed Services in Internet", IS&N98, Anversa, May 1998

[3] Braden, Clark, Shenker, "Integrated Services in the Internet Architecture: an Overview", RFC1633, ISI, MIT, and PARC, June 1994

[4] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss "An Architecture for Differentiated Services" RFC2475, Torrent, EMC, Sun, Nortel, Bell Labs, Lucent, December 1998