ESACOM: The ESA Communications Network

S. Zatti, M. Incollingo, C. Kröll* & M. Boele**
Network Planning and Engineering Unit, Informatics Department,
ESA Directorate of Administration, ESRIN, Frascati, Italy

The goal of the ESA Informatics Department with respect to communications is to provide the Agency with efficient and reliable networking services to meet the users' evolving requirements at the best market conditions. It fulfils its mandate by offering a baseline for networking services targeted at the whole Agency, although networking support for spacecraft operations is not part of the Department's responsibilities. The general-purpose network engineered and operated by the Department is called "ESACOM". This article describes both the network and its basic service philosophy, as well as its potential role in a future ESA Corporate Highway.

Introduction

In accordance with the Agency's strategy regarding procurement of information services, ESACOM is based on an infrastructure offered by means of industrial contracts. Such contracts specify all services to be performed, the sites to be connected, the protocols to be supported, and all relevant service performance parameters. The delivery of the service parameters as specified in the contract is guaranteed on the basis of a Service-Level Agreement between the Agency and the industrial provider. Appropriate tools are provided to monitor the performance of the services and whenever necessary to initiate actions to restore service in the event of failures. This approach corresponds to modern established industry practice whereby a company concentrates its activities on its core businesses and leaves to industrial partners the provision of enabling services. The success of this approach is based on how well an intrinsically stable and static arrangement like a contract can capture the services expected by the customer and their dynamic evolution. The experience of the customer's staff responsible for the establishment and the maintenance of the arrangement, as well as the experience of the provider's staff responsible for its provision, are key to this success.

The experience gathered so far by ESA in its industrial partnerships has shown that the approach is feasible and can be used to successfully fulfil most networking requirements of a modern high-tech distributed organisation. The outsourced wide-area networks Data Dissemination Network (DDN) and Level 3 ESANet have been operating for almost three years with satisfactory performance. The expected cost reductions with respect to in-house provision have been achieved. The flexibility afforded by this approach enables the core corporate

Internal Organisation

Within the Informatics Department's Infrastructure Division, ADM-IT, responsible for the whole computing infrastructure, ADM-ITR, based in ESRIN, has the responsibility for the operations and the security of the ESA wide-area networks, as well as for the ESRIN Local Area Network. LANs at the other Establishments are operated by the respective infrastructure sections. The responsibility for network planning and engineering on an ESA-wide basis rests with the ESA Network Planning and Engineering Unit (ADM-ITN), which:

- Endeavours to be the centre of competence and expertise for networking in ESA.
- Continuously monitors the technology evolution.
- Defines the road map for the evolution of ESA networks, accommodating future user requirements.
- Procures the best services from industry at the best market conditions.
- Consults with projects on their telecommunications requirements and tailors the network infrastructure to satisfy them.
- Conducts studies to assess new concepts.

* Based at ESOC
** Based at ESTEC

requirements, as well as any project-specific connectivity requirements arising within ESA, to be catered for, with the beneficial effects of cost reductions deriving from synergy, avoidance of duplication, and economies of scale.

The network

ESACOM has a core (Fig. 1) that caters to the general-purpose data-networking requirements of the Agency by providing the following services, all based on the TCP/IP communications protocol:

– Local Area Network services.
– Wide-area data connectivity:
  • Interconnections between ESA Establishments and sites where the Agency has a permanent presence, such as the ESA ground stations (Redu, Vilspa), Brussels, Cologne, Washington, Moscow, Kourou, and Toulouse
  • Access to public networks: Internet, Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), provided at all sites via different local providers.
– Protection and security according to ESA policy.
– Operation and monitoring of the above.

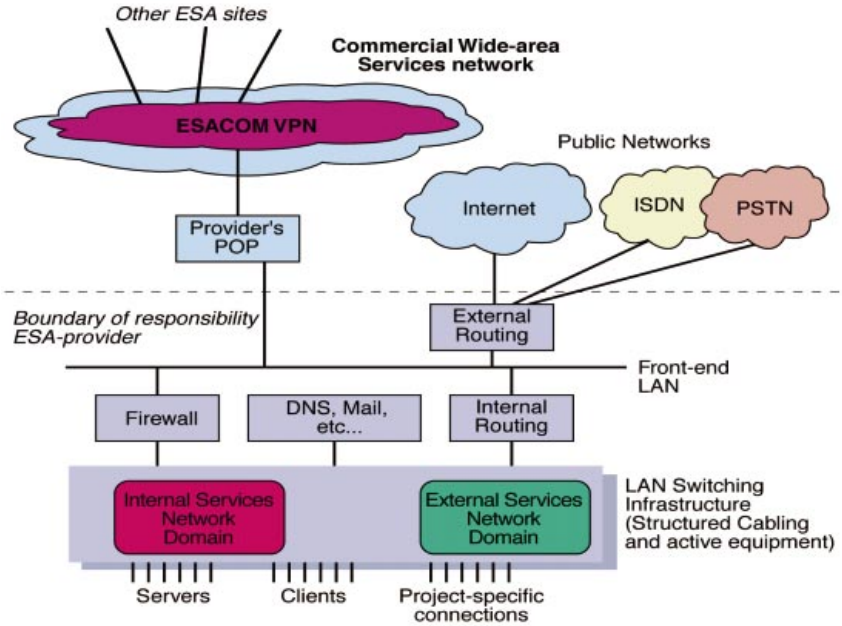


Figure 1. The ESACOM model

Additional communications services can be offered by ESACOM to cater to project-specific requirements, as described below.

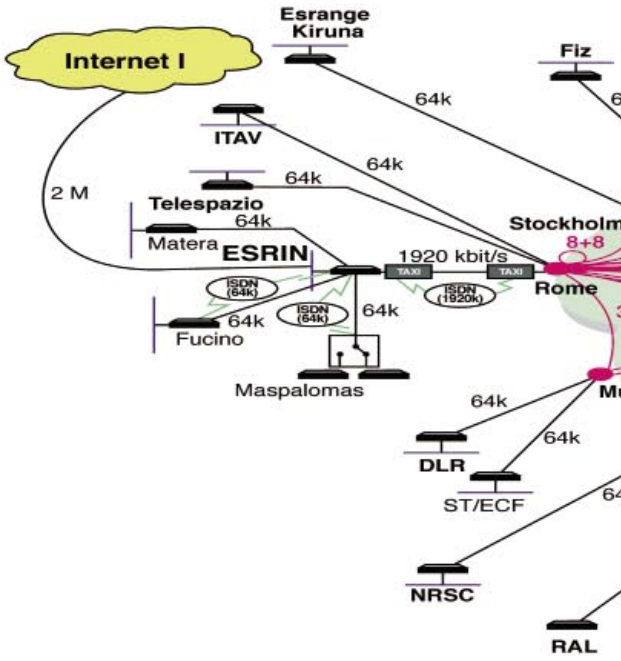
Local Area Network services

The Local Area Networks (LANs) at all main sites are organised according to a uniform criterion of structured cabling and LAN switching that allows optimal performance and maximum flexibility. Each wall outlet (in offices or computer rooms) can be associated to a different logical community, a virtual LAN, according to criteria like security (traffic isolation) and performance (traffic optimisation). The same cabling system can also be used to support telephone connections or special high-speed connections.

Wide-area connectivity

The wide-area data connectivity of ESACOM between ESA sites and stable project partners is provided by means of an outsourcing contract, where DDN, ESANet, and Level 3 have converged. The industrial telecommunications service provider, BT, offers connectivity all the way to the Customer Premises via dedicated routers used as Points of Presence (POP), connected via access lines to the nearest point of the provider's core network. The outsourced network is under the constant control and monitoring of the provider. ESA itself also monitors the status of the outsourced services, interacting with the provider to ensure that the service parameters are constantly met.

The model sketched in Figure 1 is instantiated in the five major ESA sites to provide wide-area connectivity via the commercial frame-relay network service offered by BT, CFRS (Concert Frame Relay Services), and via the external Public Networks. The dotted line in the figure indicates the boundary between the contractual responsibility of the providers and that of ESA (other network nodes follow a simpler model, without public networks).



Permanent Virtual Circuits pair-wise-connecting all major ESA sites constitute the ESACOM Virtual Private Network (VPN), realising a global ESA Intranet. ESA present and future Corporate Applications will all be supported by this network. Several other nodes of the network correspond to locations that are involved with ESA in the framework of a particular project, e.g. ERS or Envisat, as described below. The full structure of the ESACOM wide-area network, with the circuits interconnecting ESA sites and their partners, is shown in Figure 2.

Basic connectivity to the Internet for all ESA users at all ESA sites is considered part of the core network services. Internet is a fundamental business tool for dynamic access to information and to support both traditional and innovative types of human interaction. Internet is also fundamental, on the other hand, to making ESA's information and services generally accessible to the World. This implies that standard naming structures, levels of protection, and a fair share of the link capacity, are available without distinction to all users of the ESA corporate network.

The four ESA Establishments and Vilspa are connected to the respective national academic Internet Service Providers. The national networks, in turn, are interconnected via a high-speed international European backbone called TEN-34, which also provides a high-speed link to the United States.

A basic policy requirement is that no Internet traffic in any direction shall burden the Intranet links. To this end, major sites are visible to the Internet via their own national connection. As an exception to that requirement, minor ESA sites are attached to the major ones via secure tunnels, so that their Internet access will occur via one of the national connections described above.

A Remote Access Service to travelling or home-based users is provided via the Public Switched Telephone Network (PSTN), the Integrated Services Digital Network (ISDN), or a corporate account with a commercial Internet Service Provider, as appropriate. The same infrastructure also provides connectivity from ESA sites to remote users on public networks (dial-out).

Access to public networks is granted in all cases via the site's LAN and an external routing function, subject to the constraints of the security policy described later. Direct connectivity of a user's PC or work station located within any ESA premises to any public networks is not allowed, as this would bypass the whole security infrastructure.

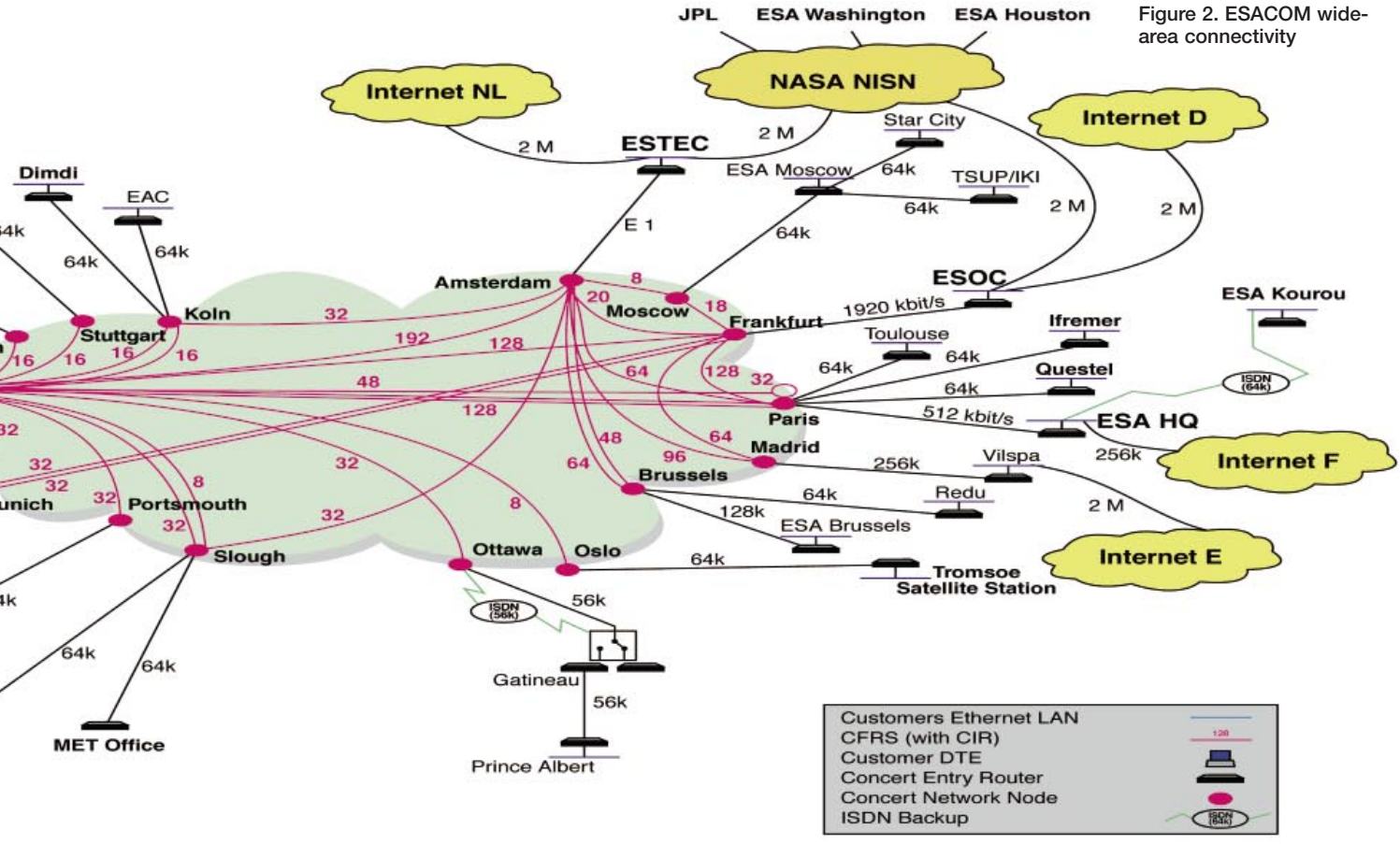


Figure 2. ESACOM wide-area connectivity

Network security

The ESA network infrastructure is subdivided from a security point of view into four network domains, as shown in Figure 3: the "External Networks", the "ESA External Services Networks", the "ESA Internal Services Networks" and the "ESA Restricted Networks".

At the boundary between the second and the third domain, as well as between the third and fourth, security facilities control all traffic. It is not possible for a single bit of information to enter or leave the ESA Internal Services Networks or the ESA Restricted Networks without passing through these facilities.

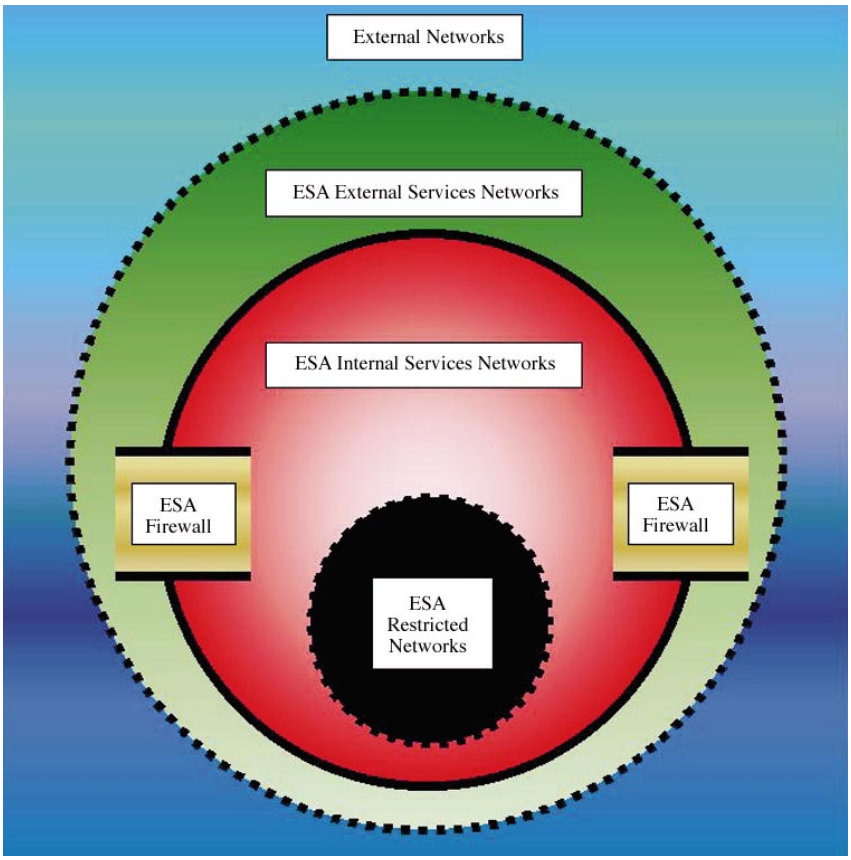


Figure 3. The ESA network security architecture

Each security facility comprises a set of mechanisms, implemented via one or more hardware components, that are individually tailored to handle the connectivity required within the scope of the involved classes. The mechanisms themselves are not static. They are established on the basis of available technology, the scope of the user requirements, and the overall ESA security and access policy.

– External Networks are networks supplied or owned by off-site industrial partners, national space agencies, or scientific institutes, national or international research networks and networks of Internet Service Providers as well as the Global Internet. Telephone networks used for data exchange, whether analogue (PSTN) or digital (ISDN), operated by any PTT or private provider, are also treated as External Networks.

– ESA External Services Networks are ESA networks that allow unrestricted access to and from the External Networks, in particular from the Global Internet. Connection to the ESA External Services Networks is foreseen for Information Servers that present the Agency to the World. For example, the ESA External World-Wide Web (WWW) Servers and ESA Public File Transfer Protocol (FTP) Servers are placed on the ESA External Services Networks.

– ESA Internal Services Networks include networks for the support of Software Development and those for the support of the Agency's Office Automation System. Software development users may typically need to access the ESA External Services Networks or External Networks, due to the frequent use of external contract support for software development and exchange of data with other space agencies and scientific institutes. Office Automation users typically need a high degree of connectivity to the outside world to support mail and data exchange with external bodies, in a controlled manner given the sensitivity of the data exchanged.

– ESA Restricted Networks allow access only to selected subsets of the ESA user community. They offer additional security mechanisms protecting against unauthorised access from the ESA Internal Services Networks. Typical examples of ESA Restricted Networks are those that support the Agency's Financial and Personnel Management Systems. The Mission Support Networks are implemented as ESA Restricted Networks. These networks support the mission-control systems and access is therefore restricted to a minimum and extremely carefully controlled.

The ESA Network Security Architecture described above is implemented by means of ESA Firewalls (Fig. 4), which strike a balance between open access from and to the External Networks and the ESA External Services Networks and the security requirement of the ESA internal communications. The ESA Firewalls control all traffic crossing this boundary on the basis of the principle that anything that is not explicitly permitted is denied. It is not possible for any traffic to enter

or leave the ESA Internal Services Networks from or to the ESA External Services or External Networks, without passing through the ESA Firewalls and being positively authenticated or permitted. All accesses, successful and unsuccessful, are logged.

Operations and monitoring

The wide-area portion of ESACOM is operated from ESRIN by means of an industrial operations contract that provides monitoring, reporting, and management of the front-end equipment. The ESACOM Network Control Room is shown in Figure 5. The LANs are maintained and operated by the respective Establishments' infrastructure sections. The industrial contract, by also covering the WAN interfaces at all sites and their consistency, ensures smooth interactions with the respective sites' LANs. This function has proved invaluable in keeping the outsourcing firm constantly focused on the provision of an acceptable service level.

The outsourced network is monitored by the same ESA industrial contract via an off-the-shelf network management tool that is used also to monitor the site's LANs (Fig. 6). This tool is able to browse, in real time, the operational and statistical data contained in the network provider's equipment at any site (local and

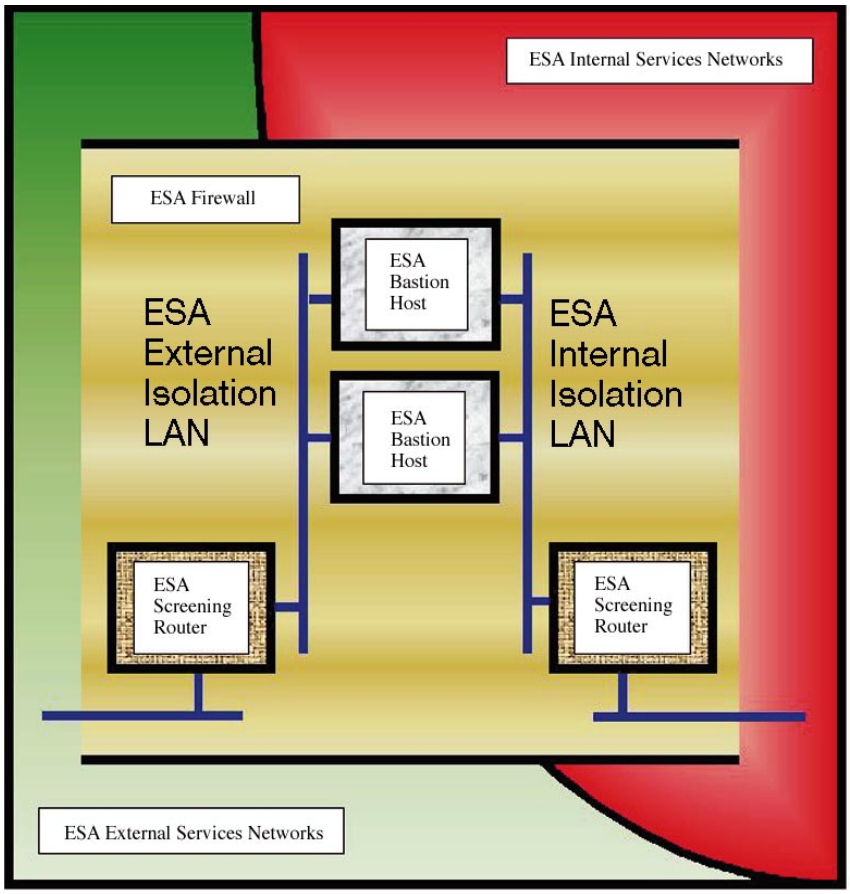


Figure 4. An ESA firewall providing high-level security

Figure 5. The ESACOM Network Control Room

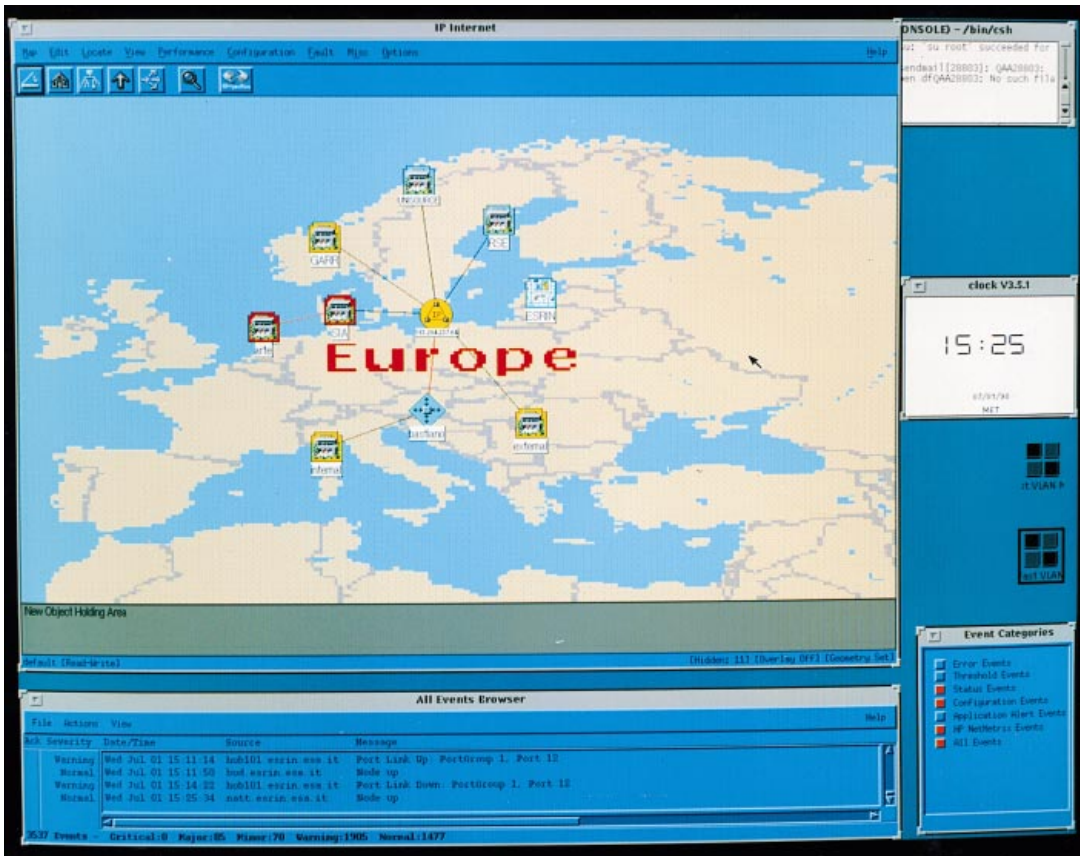


Figure 6. The ESACOM network management tool

remote) of the network; the network operators can thus check the status of the network at any time and produce any statistics that they or the customer may require to check on the quality or the availability of the contracted service, such as the fulfilment of an internal service-level agreement.

Meeting project-specific networking requirements

In addition to the core services described above, ESACOM caters to specific project networking requirements based on the same core infrastructure, by providing customers with:

- network engineering efforts and consulting
- additional communication links directly related to the projects
- dedicated LAN connectivity throughout a site
- networking equipment at project-specific locations
- ISDN and PSTN on-demand connections
- dedicated access to public networks (e.g. Internet)
- extra security arrangements (e.g. access control lists)
- project-specific operations and maintenance (e.g. round-the-clock support).

For example, additional components to support specific project requirements can be easily and economically added to the basic building blocks of the outsourced WAN. The way in which the service is structured within the outsourcing contract allows for modification of the service parameters and of the hardware structures on demand, in order to cope with changes in requirements. A typical example would be a project requiring additional IP capacity. In this case, the speed of the access line can be increased and additional virtual circuits can be contracted. The capacity of such circuits can also be appropriately modified, whereas any desired service availability can be achieved by adding redundancy to the routers' configuration and requiring the access lines to be backed up with ISDN.

Additional requirements for Internet connectivity may also arise from specific projects, for which the basic access provided as part of core services may not be satisfactory in terms of link capacity, response times, security or even location of the connection. Such requirements can be addressed by contracting a dedicated link to the Internet with the appropriate capacity with a telecommunications services provider, to be used exclusively by the requesting project, although this service would be available at any location within the requesting site via the normal LAN connections. The provider of such service may or may not be the same provider as for ESACOM, according to the best market conditions. One such example is at ESRIN, where an Internet connection with guaranteed

bandwidth has recently been contracted for Earth Observation public data servers and the ESA Home Pages.

Whenever a modification to the current network set-up is requested, as in the above examples, the new services can be gracefully accommodated on top of the current set-up. In those situations where a component of the core infrastructure already exists, the price increase is only marginal. This proves how the synergy with an existing infrastructure may benefit the users, compared with makeshift procurement of the services directly from the industry by each specific project.

The evolution of ESACOM

The stated aim of the Informatics Department is to provide efficient and reliable networking services to all of ESA according to the users' evolving requirements. The latter must be constantly monitored and validated against the latest technological offerings in order to fine-tune the available resources.

Two apparently contradictory drivers are influencing the evolution of the Agency's communications infrastructure today: the need to keep the IT and communications budget in line with the down-sizing of the Agency's overall expenditures and, pulling in the other direction, the steadily increasing demand for network bandwidth and performance as new network computing paradigms emerge to support ESA's business processes.

The objective of the ESACOM evolution is to respond to both of these categories of requirement with the realisation and continuous optimisation of a network infrastructure, the ESA Information Highway:

– ensuring the minimum cost per unit of traffic exchanged, while offering fully satisfactory communications services to its users
– integrating all the different communications services and therefore capable of exploiting to the maximum extent possible the synergy effects of such integration.

ESA is by nature a distributed organisation with a strong need to improve the efficiency of its operations. This can be achieved especially through the enhancement of its internal and external information exchange capabilities. One possible scenario is the realisation of working environments where the project activity is not constrained by the physical location of its resources (staff, knowledge base, support facilities, partners) inside and even outside the Agency. This presupposes the adoption of a networked enterprise organisational model based on the presence of an efficient and flexible communications infrastructure.

On a general-purpose network like ESACOM, it is reasonable to expect the existence of different classes of traffic that may come up with different, more or less stringent, performance requirements. For example, the interactive traffic of a financial application like AWARDS (strict real-time requirement of the financial officer sitting in front of a screen waiting for a response) may require a higher priority than an offline file-transfer application that can be launched in background. These requirements imply the prioritisation of traffic travelling on the same circuit, or of traffic on different circuits travelling from the same source to the same destination. Modern routing protocols supporting link prioritisation and resource reservation are being explored and acquired to that end.

The distributed computing applications (like the official ESA office automation system Lotus Notes, AWARDS, WWW), the newly emerging tools for computer-supported co-operative work, including desktop video/voice conferencing, and the potential shift towards a fully fledge network computing scenario pose additional challenges to the network infrastructure. The extra requirements will appear not only in terms of the pure increase in data transmission capacity, but also in terms of the ability to support different services with different Quality of Service (QoS) guarantees (like bandwidth, delay, priority, etc.).

Today, different networks are supporting different wide-area services in ESA: ESACOM as it stands today for data communications based on a frame-relay Virtual Private Network (VPN), a recently implemented ISDN-based Virtual Private Network for voice telephony between ESA sites, public ISDN for H.320 video conferencing between ESA sites and with external partners, and the public Internet for generic data communications with external partners.

As a first step in the integration of services, the frame-relay network will be enhanced with QoS provision; in this way, in addition to data applications, IP-based desktop voice/video conferencing applications will also be supported (now standardised in the ITU H.323 framework). IP-based telephony will be introduced for pilot users in order to evaluate its performance and usability.

In the longer term, the consolidation of all services over a single infrastructure will be realised, at a date depending on the maturity of

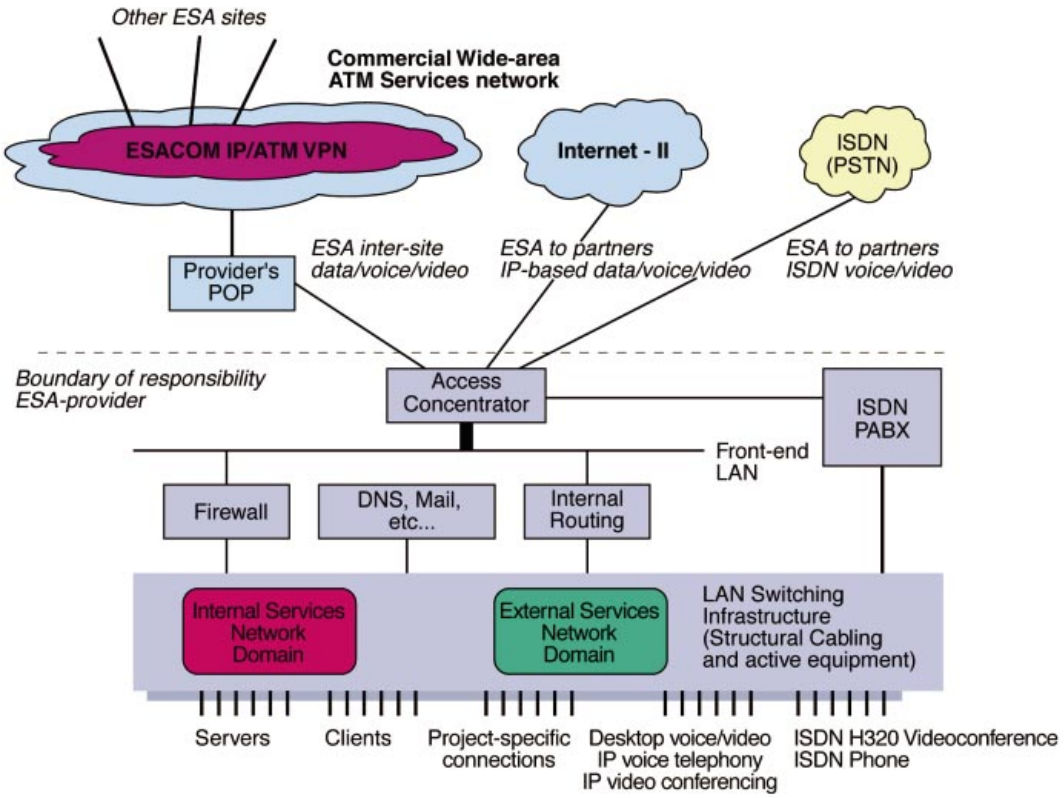


Figure 7. ESACOM Information Highway

the technology and on the availability of competitive offerings from the service providers.

It can be anticipated that a single ESACOM Information Highway will carry all the inter-site data, voice, and video services, as portrayed in Figure 7. This network will be based on IP and ATM (Asynchronous Transfer Mode) technologies. The Public ISDN (possibly, also PSTN) connectivity will be kept for off-net voice and video conferencing with external entities. The public Internet will most likely also be offering QoS guarantees (Internet II) and could be exploited for additional services with external partners and as back-up to the main ESACOM wide-area connectivity.

In the preparatory phase, a number of technologies and tools have to be investigated, evaluated, and then put in place as the building blocks of such an infrastructure. Examples are:

- new service offerings from the VPN providers, especially those geared towards service integration
- new compression and transport schemes for voice and video
- tools for end-to-end QoS management, enabling the establishment and monitoring of different classes of service
- applications measuring resource utilisation at user community/project level, to be used for capacity planning and to enable the implementation of charge-back schemes (should this need arise).

Regarding the cost aspects, while maintaining the classic financial objectives of maximising the return on capital investment and reducing recurring expenses, a new cost model for the network should be put in place. This model should enable the evaluation of the introduction of new services and technologies into the network as a business case, allowing a fair comparison between alternatives. This also implies viewing the computing and networking infrastructure more strategically; i.e. not only as a support facility with certain associated costs, but as an asset for improving ESA's efficiency and effectiveness in the future.

Conclusion

This article has described the current configuration and the expected evolution of ESACOM, whilst also trying to capture the spirit behind the endeavour. The main challenge now is to accommodate present and future Agency-wide networking requirements and show that they can be fully satisfied in the most efficient and cost-effective manner by this infrastructure and the evolution thereof. esa