

EARNEST

Campus Issues Sub study

Final Report

1 Executive summary

There is no doubt that a well-managed modern network offering up-to-date networking services is a key element of the infrastructure of successful European research and education institutions in the 21st century.

Staff and students are becoming more mobile as they exploit the establishment of a European Higher Education Area following the Bologna Declaration of 1999, and researchers take advantage of the growing opportunities for collaboration offered by the European Research Area. Much of the success of these ventures will depend on pervasive, effective, high quality networking – not least within campuses. Institutions which exploit the power of networking services to the full will undoubtedly gain a competitive edge in their research and education activities.

1.1 Findings

The EARNEST Campus Issues sub study undertook a survey of the current state of networking in European research and education institutions. The questionnaire also asked respondents to give some indication of their future plans and expectations in this area.

Evidence from the survey and other sources, such as the parallel survey conducted by the EARNEST Researchers' Requirements sub study, indicates there has been a significant investment in networking infrastructure in institutions since the SERENATE study in 2002-3. There is little evidence of persistent bottlenecks at the campus level, although there are still pockets of low bandwidth and obsolescent equipment and cabling to be upgraded. It is also likely that some bottlenecks arise from unnecessarily stringent security arrangements.

Results from the survey show that the networking infrastructure in institutions is generally satisfactory though, in many cases this state of affairs appears to have happened accidentally rather than by good planning. Networking strategy needs to be addressed systematically at the highest level within institutions. There needs to be a coherent networking policy developed in conjunction with end users, and preferably with formal mechanisms to consult them. This is especially important where there are demanding applications and projects, for example in particle physics research. Institutional networking policies should include topics such as :

- Networking services available ;

- Replacement policy for cabling and equipment;
- Security ;
- Acceptable use policy ;
- Relationships with other Internet domains, e.g. NRENs;
- Raising awareness of networking services ;
- Training ;
- Arrangements for consulting users.

There are clear indications from the EARNEST surveys undertaken that some of the potential beneficiaries of networking services are not aware of their availability, or even existence in some cases. Institutions should take steps to actively promote greater awareness of the scope and availability of networking services (e.g. videoconferencing), and offer training to help users make better use of networking facilities.

In many institutions the networking support team is too small to meet current day demands. As a consequence team members spend much of their time ‘fire fighting’ and cannot risk offering new services to their user community, even though it is technically feasible to do so, because they would not be able to cope with the extra workload. In particular they would not have sufficient staff or expertise to provide adequate training and support. As they plan future strategy it is vitally important that senior managers recognise the increasing dependence of their institutions on networking services and allocate sufficient funds and resources to exploit the network effectively.

Responses to the Campus Issues survey indicated good collaboration between NRENs and institutions in some countries, but room for improvement in others. Effective networks depend as much on good human collaboration and cooperation as on the technical infrastructure.

Finally, it is important to emphasise the paradigm shift taking place in networking, from only providing connectivity to offering and supporting networking services. Institutions should carefully assess whether they are sufficiently equipped to support the rapidly changing nature of networking and take appropriate steps if necessary

1.2 Technologies

1.3 Main Recommendations

For Institutions

NETWORKING POLICY

- *Define networking policy at the highest level within institutions, covering the following topics:*
 - *Strategic plans to meet the aims and objectives of end users*
 - *Annual budget to deliver the planned objectives and keep infrastructure and services up-to-date*

- *Provision for a well-resourced network support team*
- *Rules for network security*
- *Arrangements for end user participation in policy making*
- *Adoption of national guidelines*
- *Arrangements for collaboration with NRENs, other institutions, etc*

INFRASTRUCTURE AND SERVICES

- *Set aggressive replacement policies for equipment with a maximum life expectancy of 5 years*
- *Adopt institution-wide specifications for networking infrastructure, including elements controlled by departments or faculties*
- *Ensure seamless end-to-end connectivity where a particular quality of service is required*
- *Provide support and training for performance optimisation, especially to Class C users*

SECURITY

- *Adopt security measures which are appropriate for purpose and do not hinder the effective use of the network*
- *Establish an institution-wide security team with a high degree of independence*

END USER REPRESENTATION AND AWARENESS

- *Ensure end users are involved in defining networking policy*
- *Establish formal procedures to identify end user requirements*
- *Circulate an Acceptable Use Policy (AUP) to all end users which sets out clearly their rights and obligations when they use the network*

COLLABORATION

- *Establish strong, formalised arrangements for collaboration other management domains, e.g. NRENs, intermediate networks, other institutions*
- *Encourage networking teams to share their expertise with colleagues in other management domains*

RAISING AWARENESS AND TRAINING

- *A cultural change in networking is taking place with the emphasis moving from providing connectivity to network services. To speed up this change of focus institutions should:*
 - *Provide training courses and good quality documentation for end users to raise awareness of the network services available and promote their use, including videoconferencing, Multicast, video broadcasting, video on demand, Voice over IP telephony*
 - *Make arrangements for network support teams to retrain to keep up-to-date with fast-changing technologies*

For NRENs

- *Collaborate more closely with institutions in the following areas:*
 - *Deploying key services*
 - *Sharing strategic information*
 - *Organising training for innovative services*
 - *Coordinating working groups of networking staff to share expertise*
 - *Understanding the demands of high-end users*
- *Assist institutions to provide support and training to end users about performance optimisation, especially Class C users*
- *Provide guidelines for institutional networking policies*

2 Background

The EARNEST foresight study has looked at the expected development of research and education networking in Europe over the next 5-10 years. The study was carried out between March 2006 and November 2007. EARNEST was funded by the European Union through the GN2 project, which also provides the funding for the current generation of the pan-European research and education backbone network, GÉANT2. The aim of EARNEST was to provide input for initiatives that could help to keep the evolution of European research networking at the forefront of worldwide developments and enhance the competitiveness of the European Research Area. EARNEST prepared the ground for the planning of the development of research and education networking infrastructure and services after the completion of the GN2 project, at the local, national, European and intercontinental level.

EARNEST can be seen as the successor of the very successful study that was carried out in the SERENATE project in the period from May 2002 until December 2003. The results of the SERENATE study, and in particular the recommendations in its Summary Report, have been very influential on the planning and development of research and education networking in Europe in subsequent years.

After an initial preparatory phase, the EARNEST work has focused on seven study areas: researchers' requirements, technical issues, campus issues, economic issues, geographic issues, organisation and governance issues, and requirements of users in schools, the healthcare sector and the arts, humanities and social sciences. Reports have been published on the results of each of these sub-studies, as well as an additional report on regulatory issues. The EARNEST study was rounded off by a Summary Report containing recommendations for the relevant stakeholders.

The Campus Issues sub study group (CAMP) looked at networking in research and education institutions. It took as its starting point the assertion in the report of the earlier SERENATE study (December 2003) that *"The campus is often the weakest link in the network chain"* and the report's recommendations that:

"In Europe, campus networks are now often the weakest link in the chain of the end-to-end services needed for research and education. Therefore, universities and research institutes and their supervisory and funding authorities need to ensure that their campus networks are appropriately resourced.

In general, expenditure for ongoing technical upgrade in campus networks is best treated as a budget expense on an annual basis. "

and

"Research and education institutions should consider acquiring their own fibre infrastructure between their Local Area Network(s) and the point(s) of presence of key service and/or infrastructure providers, if necessary by commissioning its construction. "

CAMP investigated whether campus networks were now resourced better and looked at other issues including :-

- changing emphasis from connectivity to network services
- rollout of IPv6
- training network support staff
- collaboration

3 Preliminary remarks

The following important points of explanation are made at the outset.

3.1 Categories of end user

This report makes frequent references to “*end-users*”, i.e. the researchers, teachers, staff and students of research and education institutions in Europe. However the networking requirements of end users differ greatly depending on their research domains, teaching and learning disciplines, etc. The report uses a widely recognised convention to divide different networking requirements into three categories, **Classes A, B** and **C** reflecting **baseline, medium** and **heavy** usage respectively.

- **Class A** broadly requires e-mail handling and Web browsing , the basis for all professional activity nowadays. This class of usage does not require much of its network facilities apart from reliable access, mobility and a satisfactory level of bandwidth.

Class A is estimated to be more than 80% of end users in 2007

- **Class B** covers two additional activities; the handling (via file transfer or database access) of significant volumes of data for the regular use of audio and video streams; and access to grids resources. Streaming, especially when human interaction is involved, often has more demanding performance requirements than conventional file transfer. Grids also have their constraints especially in term of latency and jitter. These two usages may require guaranteed bandwidth and guaranteed stability for jitter and latency, but are still reasonable regarding the level of bandwidth required.

Class B is estimated to be less than 15% of end users in 2007

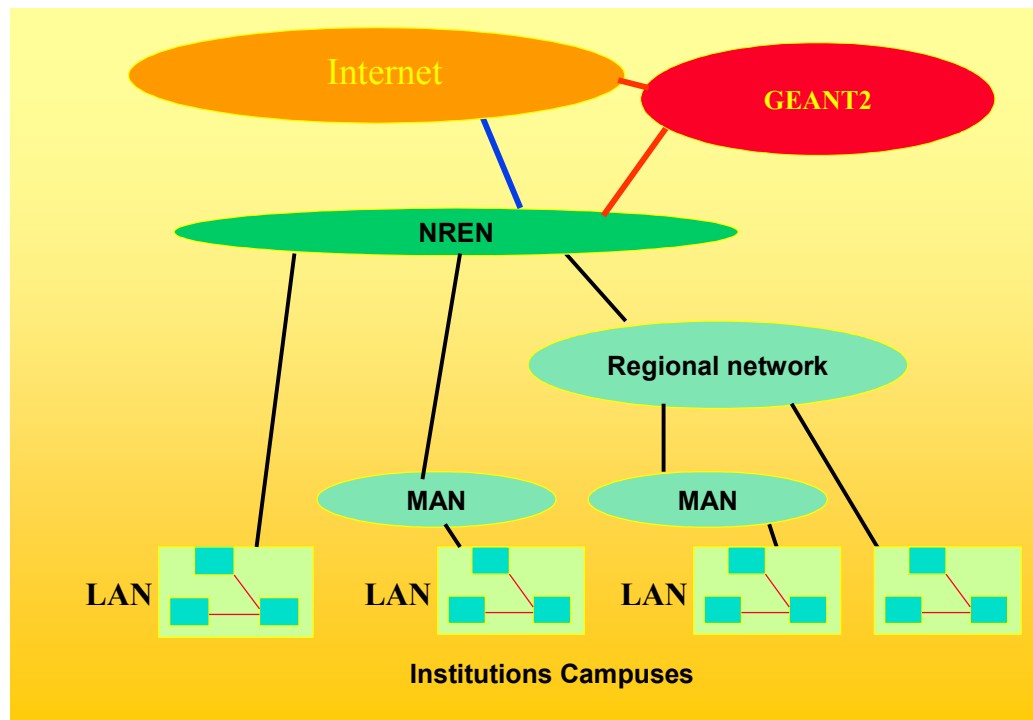
- **Class C** usage covers the sustained, but often temporary, handling of extremely large volumes of data, either by transfer of very large files, or increasingly via the use of technologies such as grids and virtual presence.

Class C is estimated to be a very small percentage of end users in 2007

3.2 Boundaries of the Campus Issues study area

In the strictest sense the Campus Issues sub study should have been limited to networks within research and education institutions only. However the underlying structure of most research and education networks is multi-layered and to look at the ‘network’ from the perspective of the end user, especially when searching for potential bottlenecks it was necessary to look at other components, or intermediate networks, between NRENs and institutional networks.

The infrastructure from which Europe’s research and education communities obtain their networking is often quite complex, and is provided by a variety of domains including Géant2, NRENs, Regional Networks, Metropolitan Area Networks and campus networks.



In order to provide good network connectivity for research and education institutions the different levels of infrastructure involved in delivering services must operate in a coherent way. In Europe connectivity and service provision for the end user typically depends on three, but sometimes as many as four or even five, different categories of infrastructure. These are shown in the diagram above and they are:

- The Local Area Network (LAN) infrastructure of the site where the user has his or her main office. This will be under the responsibility and control of the research and education institution - university, research centre, etc. Each institution may have multiple sites and each site is considered to have a “campus network” in the context of this study. The term “campus network” is used regardless of type of institution, which includes all organisations served by NRENs.
- Metropolitan Area Network (MAN). The MAN typically provides access to an optical fibre infrastructure, which can be used to interconnect LANs inside one city. While the LANs of the individual sites are under the responsibility and control of the institution (university, research centre, etc), MANs tend to be run, either by commercial infrastructure operators; by a consortium where local government plays a significant role; or under the responsibility of a formal collaboration of academic institutions.
- Regional Network. In some countries, such as France, Spain and the UK, Regional Networks form a very important element for providing connectivity between the NREN and campuses. In those countries NRENs usually have Points of Presence (PoPs) in large cities, often the regional capital if one exists. From the PoPs, NRENs can connect to all institutions within the city, either directly or via a local MAN, while other sites spread around the region will be connected via the Regional Network. These networks typically offer connectivity and other services, rather than just simple infrastructure. Usually they are built, operated and funded by a consortium of various public and private sector institutions and the local government.
- National Research and Educational Network (NREN). In each country the NREN infrastructure typically makes direct provision for national connectivity to other

research and education institutions, and for onward connection to European and intercontinental destinations. NRENs operate on a variety of different governance and funding models, depending on the national political consensus.

- GÉANT2. On the pan-European level the GÉANT2 project, developed, operated and evolved by DANTE on behalf of the NRENs, and co-funded by the European Commission, provides the primary international infrastructure for production traffic. However for important projects it is not exceptional for experimental traffic for an NREN also to directly acquire connectivity to various pan-European or intercontinental destinations.

4 Methodology

Phase 1 was a fact-finding exercise to discover the current situation of campus networking within research and education institutions, mainly universities, research institutions, etc.

A questionnaire was developed by the Campus Issues subgroup (CAMP) for completion by the heads of IT in European research and education institutions. The questionnaire was circulated through several different channels including NRENs, EUNIS, and TERENA. Preparation took place in January and February 2007, and the online questionnaire was made available at the beginning of March 2007 and closed three weeks later. A first rough analysis was presented to a joint meeting of the Researchers Requirements and Campus Issues subgroups on the 2nd and 3rd of April 2007.

The main results from this work were presented at the NREN PC meeting in Bratislava on 27th April and at the ENPG meeting in Amsterdam on 8th May 2007.

To clarify some responses follow-up interviews by telephone took place with colleagues in Spain, France, UK and Ireland. These took place in late April and early May, and the additional results were integrated with the initial ones.

Phase 2 looked at the strategic directions of research networking and aims to provide a view of the possible future of campus networking. The subgroup took into account ongoing technological developments on the vendor side as well as various experimental projects taking place in the research and education networking community (GN2, Internet2, and NRENs). The intention was to assess the impact these developments could have in the near future on the campus networks and on the interface between NRENs and the institutions, and to provide guidance and recommendations to senior management in institutions for developing campus network strategies.

5 Phase 1

5.1 The Campus Issues survey

The SERENATE study said that campus networks were “*often the weakest link in the network chain*” and thus limited the performance of networking services provided to end-users. This finding was the outcome of a survey of researchers, where respondents mentioned “campus bottlenecks” as a factor inhibiting optimal usage of the network. The views of institutional Network Managers and heads of IT were not sought.

When the EARNEST study was set up it was decided to make Campus Issues one of the main areas of investigation. As a consequence the issue of campus bottlenecks (real or imagined) was one of the areas surveyed in the questionnaire sent to heads of IT in institutions. But the scope of the survey was broadened and extended to a whole range of issues affecting campus networking. The various topics are listed below with the main findings coming out of the survey.

Details of the Campus Issues Questionnaire and analysis of the responses are available from TERENA on request.

5.1.1 Bandwidth to the NREN

In responses to the Campus Issues survey the level of bandwidth from institutions to their NREN represents a very wide spectrum from 2Mb/s to 10 Gigabits/s. These figures are not easy to interpret, since low bandwidth is often adequate for small institutions with few end-users. However a significant number of medium sized institutions also have low bandwidth to their NREN, and this appears to be due mainly to their obligation to use an intermediate network to connect to the NREN. To attempt to make meaningful comparisons between institutions, the average bandwidth available per computer was calculated. Results ranged from 8Kb/s to 100Mb/s per computer. This represents a huge gap in bandwidth, and it is not easy to explain how an institution providing, around 10 to 50Kb/s, copes with this situation. It is not possible to draw any clear conclusions from the survey but it is evident that end users with such small bandwidth cannot exploit the full range of networking services.

5.1.2 The phenomenon of many users served satisfactorily by low bandwidth connections.

25% of the institutions taking part reported they had relatively low bandwidth from their Campus to the NREN, at less than 34 Mb/s. Some of these institutions were small with few students, but some were not, with more than 5000 students recorded. We would have expected the larger institutions to be less than content with the bandwidth available to their user community. However we were surprised to note that 81% of respondents considered the bandwidth to the NREN per user to be sufficient.

It is likely that many end users, especially Class A users, will not access external services directly but via proxy servers, caching servers, central email servers, etc. In this way it is possible to cope with many thousands of Class A users on low bandwidth connections. However it is very important to manage such servers properly. See 5.1.11 below.

The subgroup has not been able to investigate in greater depth why these institutions appear to be satisfied with their low bandwidth, but it may be worth looking into later. One possible reason is that the expectations of the user community in these institutions are unusually low and they are content to have only basic networking services at their institutions.

5.1.3 High bandwidth to the NREN, but little use of network services.

The EARNEST surveys of Campus Issues and Researchers Requirements, and the latest published TERENA Compendium, indicate that issues of low bandwidth identified in the SERENATE study are now largely resolved. At the present time many institutions have adequate (or better) bandwidth to meet the current needs of their user communities; and the phenomenon of network bottlenecks – whether on campus or elsewhere – is now rare.

However there is not much evidence of innovative use of the network to take advantage of the bandwidth available. There appears to be several different reasons for this:

- Many end users are not aware of the range of network services available to them e.g. videoconferencing. (See Researchers Requirements sub study report)
- Some institutional network teams are not aware of the network services they could provide for their user.
- Some institutions are reluctant to promote new services because their network teams are too small or do not have the right skills to provide adequate support
- Some network services are not simple to implement and to use, e.g. videoconferencing, Multicast, IPv6. (See 5.1.8)
- In some cases there are still limitations in end-to-end communications software or hardware. (See 5.1.12)
- Many users do not need advanced services. A dependable, reasonably fast network providing email and web access is sufficient for them.
- Many users are not familiar with the technical side of their network and may not even be aware that higher bandwidth has been provided for them.
- Innovative services often require a prolonged development period. For example this appears to be the case with some Grid projects where structuring the user community takes longer than expected.
- Cultural changes are often required. Both user communities and their network service providers need to become more imaginative in their approach to networking. Frequently the technological infrastructure seems to change more quickly than the mindset.

5.1.4 Performance of the core network on campuses

Although, overall, there have been great improvements in the infrastructure of campus networks in recent years, there are still isolated pockets which do not have adequate bandwidth, for a variety of reasons including out of date equipment, problems with buildings, fragmented institutional management, geographical remoteness and lack of funding for networking.

One third of survey respondents pointed to some part of their core network being an obstacle to propagating Gigabit connectivity to end-users.

5.1.4.1 Inter Campus Connectivity within institutions

Responses to the Campus Issues survey indicate some institutions have problems connecting remote campuses. Their interconnection links appear to run at unacceptably low data rates. The survey shows that only 25% of the responding institutions have internal connectivity greater than 1.2 Gb whilst 35% of the institutions taking part in the survey have connectivity to their NREN of greater than 1.2 Gb. There may be several reasons for this disparity in connection speeds. It could be that there is a great difference in size of the different campuses and that smaller ones merit lower rates of connectivity, or that the pace of growth of external connectivity has outstripped that of the internal network. Another reason for low bandwidth between campuses could be the obligation to use regional networks where

remote campuses are some distance from the main site. It is even possible that telecommunication costs for better connectivity are prohibitively expensive.

5.1.4.2 'Last 100 Metre' Problem

There are indications that there are problem areas on the campuses which have outdated wiring and switches/repeaters. 41% of the respondents (out of 150) reported that it was impossible to establish a high bandwidth connection (1Gb) between any two points on the campus and of these 70% reported that the reason was out of date hardware or cabling. Possible reasons for this include

- The reluctance of faculties/departments to invest in upgraded equipment and cabling
- Demarcation disputes between departments and central service providers about funding upgrades
- Problems in making alterations to older buildings, including the presence of asbestos

A surprising finding of the survey is that 51% of respondents have users connected at lower than 10Mb. These users must be severely hindered in the use of the network, with poor end-to-end performance. Low bandwidth connections such as these adversely affect the network performance. For example a person on a gigabit connection is likely to have their performance impaired when they are communicating with a colleague on a slow speed network.

In the worst-case scenario researchers may be unable to take part in collaborative projects requiring high-speed connectivity, the cumulative effect of which would seriously damage an institution's research reputation.

5.1.4.3 Progress Towards Improvements

The Campus Issues survey shows institutions are rolling out Gigabit networking on their campuses. However its availability is limited. Approximately 5% of the institutions can provide 90% of their users with a Gigabit connection. This would not be a major problem for the majority of Class A users. But it would have serious repercussions if it were uniformly applied across an institution with Class B and C users if only 5% were able to access Gigabit networking.

One of the recommendations below states that a high proportion of new end-point networking equipment should provide Gigabit points as standard. There may be a slight extra cost in the purchase of such switches today, but the labour costs in installing and managing them will be similar to lower grade equipment, and the investment now will be repaid later as the demand for higher bandwidth increases. It is also strongly recommended that institutions with out of date cabling should also plan replacement as quickly as possible.

Recommendations

- ***1. Aggressive replacement policies for network equipment should be put in place with a maximum turnover period of 5 years.***

- *2. An inventory of institutional wiring should be kept. Total replacement of the core and end-point wiring should take place at least every 10 years. This period may prove to be too long where radical changes in technology take place.*
- *3. A high proportion of all new network switches and end-points should be Gigabit enabled. Purchasing lower speed equipment at this stage is a very poor investment.*
- *4. Even if the core network is not Gigabit enabled, Gigabit enabled host network interfaces should be installed for the end user.*
- *5. Early adoption and rollout of higher specification equipment may be required for intensive services such as central servers or for high end Class C users.*
- *6. There should be an internal process to define specifications to follow for departments and/or faculties local infrastructures when installing and/or upgrading the part of the infrastructure under their own responsibility.*

5.1.4.4 Future Survey Work

Whilst the current survey and project is a single snapshot in time and presents the current status of the campus networks, it is recommended that an annual survey is performed to show the progress in advancing **end to end network performance**. As has been stated, the perception of the network can be seriously degraded by a single slow connection and users may decide not to trust a network that is unreliable.

The annual survey can be used to benchmark the progress in upgrading all components of the network and could be a valuable tool for institutions in leveraging extra resources where they identify that they are falling behind a European norm or their peers, or it can be used by institutions as a powerful supporting argument when bidding for research projects.

A possible list of items that could be measured annually and published:

- The number and percentage of users connected by GB points
- The number and percentage of users connected via shared media
- The bandwidth of the central core network
- The bandwidth of the inter campus connectivity
- The bandwidth to the NREN

Some thought should be put into the campus of the future. For example, will there be much of a wired infrastructure at all? Or will many connections be done wirelessly (where appropriate) using future generations of networking technology?

Class B and C users will require the greater bandwidth that cabling infrastructure (optical fibre or copper) provides, but the needs of Class A users will probably be satisfied with wireless access, although there needs to be a cautious assessment of pros and cons before making a large commitment to wireless.

The networking architecture within institutions will need to be extremely well-designed to accommodate the needs of the various classes of user cost-effectively using appropriate technology.

Similarly, modern networks must operate on a device-agnostic basis. Provided there are appropriate arrangements, users must be facilitated in connecting any device to the network without prior clearance or approval of the network operations centre

5.1.5 Campus Network security issues

5.1.5.1 IT Security Policy

The Campus Issues survey showed quite a variety of attitudes to IT security policies in the institutions which took part.

Some institutions lack any formal IT security policy. This can result in management imposing ad-hoc solutions to security issues as they arise.

At the other extreme some IT security policies are too formal and rigid, translated from businesses or companies and not appropriate to the requirements of a research or educational establishment.

IT security is a vital component for any organisation using IT. For research and education institution, whose main asset is its intellectual capital, IT security must be seen as indispensable. Ranging from EU, through national to institutional regulation, laws regarding Data Protection, Privacy, Confidentiality, Copyright etc must be adhered to. Research contracts, whether from state or private sources, require that much of the work is performed in a secure environment and that research results are not provided to competitors or leaked to unauthorised parties.

In passing it should be noted that where IT security audits have been performed by the large consulting companies, the resulting recommendations are often not appropriate for research and education environments.

An IT security model should be based on some recognised standard such as ISO27001, ISO17799, BS7799 or Cobit. Some countries have national recommendations for IT security and some of the university IT organisations in these countries have specific recommendations and tools for their implementation in the research and education community, for example UCISA in the UK.

Education of the user community in conforming to an institutional IT Security Policy is vital. Users must understand why such policies are being set and what they need to do to conform. Equally, the central IT security management must do all it can to protect its users from compromise, usually unwittingly.

Standard tools such as Anti-Virus, Patch Management, Intrusion Detection and prevention seem to be increasingly deployed. However there are institutions that do not seem to actively manage these. To be effective these tools must be actively managed, preferably from a central point in the institution.

Particular attention should be paid to the areas of Identity and Password Management. Good implementations of these will allow users to perform their tasks and duties more easily, without interference from repeated requests for passwords. Some form of two-factor authentication is recommended, but this may prove costly in large institutions.

Too often, security is given as an excuse for why things cannot be done, an excuse that local management might use if they feel that a request is difficult to satisfy. The vague response “security problem” can be a throwaway negative answer that is difficult to question. These local decisions are sometimes made despite that fact that no formal policies exist, which makes the implementation of strong IT security policies even more important.

Clear policies, coupled with Acceptable Use Statements, should enhance the service offered to users and not necessarily be considered as a negative action. The policies should be sufficiently flexible to recognise that the institutions are at the leading edge of research and development.

No information was gathered about the existence of formal independent Security Teams in the institutions.

Recommendation

- ***7. It is recommended that such teams be formed and that they should have an institution wide remit, with a considerable degree of independence from the central IT service.***

The Campus Issues questionnaire was a snapshot survey to gather information for the EARNEST study.

Recommendation

- ***8. It is recommended that the survey be carried out on an annual basis to measure progress as institutional IT services develop.***

Examples of best practice in the implementation of campus security policies could then be derived and published from the results.

5.1.5.2 Firewalls

It appears from the survey that a reasonable proportion of institutions have firewalls installed; this is both a positive and a potentially negative finding. Positive in the protection provided by the firewall, but potentially negative in that the firewall may introduce performance limitations which are a hindrance to end users.

The design of a firewall and its positioning in the campus network is of critical importance. Also the performance of the firewall and its capability for handling high traffic rates must be examined closely. In a research and education environment, the installation of the highest specification of firewall should be considered. Its day to day

performance should then be monitored closely to ensure that there is sufficient scope. Research traffic can peak very quickly and result in short term bottlenecks that may not be identified by most monitoring tools.

Today, powerful firewalls are available capable of performing deep packet inspection at high speed, but these are more expensive than the standard commodity firewalls that many institutions are installing. It would be advisable that institutions look to install high performance firewalls to complement the high speed networks that the NRENs are delivering.

Recommendation

- ***9. Provide direct network access, under controlled conditions, to researchers who sign up to an agreement to ensure that privileged access is utilised responsibly. This direct access could allow for traffic to go around a standard***

5.1.5.3 Peer to Peer (P2P)

The survey asked a range of questions around the use of P2P protocols and the results could be interpreted as indicating a rather dictatorial style by the network managers. In approximately 25% of the institutions responding, all peer to peer traffic is forbidden, with no reference to the possibility of allowing “good” peer to peer traffic.

There is a perception that all peer to peer traffic is associated with nefarious activity on the network, such things as illegal file sharing breaching copyright legislation etc. Of course, there is some truth in this argument and much of the P2P traffic is actually unwanted and undesirable.

However there are numerous cases where P2P traffic is valid and valuable, for example Bittorrent for large file transfers. However Bittorrent would normally be banned in a regime of total prohibition. Similarly P2P protocols are used in legitimate systems such as Skype, but these would be banned too.

A policy that states that P2P traffic is generally banned, but that individual people may request access to the protocols in a properly documented manner might be appropriate, provided the policy was well advertised.

A better policy for P2P would be to formally allow all P2P and not impose technical limitations, but to impose policy restrictions on personal usage. This could mean that the illegal and antisocial uses of P2P could be prohibited whilst allowing proper use of P2P to take place. Attempting to stop all P2P activities may be difficult from a technical point of view.

It is wrong to assume that, just because something is new and has its roots in the networking underworld, it cannot be useful. Skype was developed by the same people that developed Kazaa which is widely used for illegal file sharing.

Another solution to the abuse of P2P may be provided by Traffic Shaping or metering facilities in modern networks, though this may be more relevant to inhibiting those in Class A who abuse the network than the high performance Class C users.

Recommendation

- ***10. Do not impose blanket bans on particular types of network traffic without careful consideration of the underlying activities that are being performed***

5.1.5.4 Network Address Translation (NAT)

In the Campus Issues survey a significant minority of institutions (42%) reported that few (or even none) of their end user computers were given public IP addresses.

At one time there was a shortage of IP addresses available for IPv4 users. Clearly IPv6 will eliminate this problem when it is implemented by institutions. In the meantime one of the solutions implemented by many commercial ISPs was Network Address Translation (NAT). NAT allows many devices to be hidden behind one public IP address. NAT allows users to avail themselves of a set of IPv4 address space that is designated “Private” and these IP addresses are never propagated out to the internet.

Whilst NAT is useful in that it conserves IP address space, enabling a whole university to live behind one IP address, another use has emerged. That is using NAT to hide internal services and machines from the internet, usually for security purposes. This practice probably poses no problems for the more traditional internet users and companies, but it is a severe blockage and hindrance for many researchers and services who require their network address to be propagated across the internet.

Whilst it is acceptable in many circumstances that most commodity internet users, Class A, can be hidden behind NAT, some special treatment must be provided for any user who requires more advanced services (e.g. videoconferencing) and there must be a way for their network services to be broadcast on the internet. A hybrid model where the majority of the institution uses NAT and the specialists have the possibility of obtaining public IP addresses would be acceptable. Once again, a rigid security policy that required NAT with no escape clause would be counterproductive to a well provisioned research network.

Many institutions have ample IPv4 address space available to them and users who require public address space should be able to justify its provision readily. Clearly, when there is a move to IPv6, then shortage of address space will no longer be a valid reason for hiding behind NAT.

5.1.5.5 Private Network Links for Researchers

Many network users feel that institutional networks constrain them in their research or teaching in that there are usually restrictions imposed by local policies. Sometimes they are tempted by unrestricted network connection from a commercial ISP, thus

avoiding the restrictions of the institution's central policies. There is some slight evidence that users have purchased ADSL connections to avoid such policies.

Similarly, users at home with their own "broadband" service, frequently using ADSL, may feel that they have much greater freedom and access to the network than they have at their institution. Indeed it is probably true that there are far fewer restrictions on these sorts of networks.

Most telecom operators have a privileged legal standing and may not have responsibility for the activities of the end users of their network and therefore do not have the need to restrict users with the imposition of policies.

In general, research and education institutions have no such legal immunity and have direct responsibility for the activities of all users on their network. So the activities of a single staff member or student could result in legal action being taken against the institution. An offended person or body may find taking legal action against an institution much more profitable than against a less well-off individual.

This means that strong policies governing network use are required by institutions and that these policies have to apply to all users, whether they use the central network or lease links directly to their research unit. The legal implications cannot be evaded.

It is especially important that researchers are provided with tools and solutions to meet their networking needs, and which give them any special network facilities in a monitored and controlled manner. Special rules should be laid down for them and they should be responsible enough to ensure that they comply and conform. Clearly, breaches of the rules should result in their specialist privileges being withdrawn.

5.1.6 Obstacles and bottlenecks

Few respondents said that their campus networks were the root cause of bottlenecks. Bottlenecks arise for many different reasons: obsolescent cabling and equipment in building was often quoted, the same for core network equipments (routers, switches, etc.). Other reasons include: a shortage of networking expertise, links between buildings and between campuses, and security measures. But no dominant reason emerged from the survey.

Many respondents thought raising the awareness of senior management in institutions would significantly help resolve some of their difficulties. It would also help if guidelines and recommendations were published at European or national level. This would help institutional managers to better understand the benefits of up-to-date networking services, and how to acquire them.

The idea of benchmarking by national or European organisations was also welcomed by respondents. And finally, setting up formal procedures for identifying and incorporating the needs of end-users into networking policy and funding plans.

Recommendation

- *11. Strengthen collaboration between NRENs and institutions to improve the deployment of key services ; share strategic information ; raise awareness of innovative services at senior levels ; coordinate working groups ; get feed back from end-users, especially those with demanding requirements*

5.1.7 Networking services provided to end-users

5.1.7.1 How to identify end-users needs.

When establishing policy for the provision of networking services at an institution, one should take into consideration the different categories of usage of the network. Therefore categorising end-user requirements (Baseline usage, Medium usage, Heavy usage; see section 3.1 for more details) is an important element of the strategic process to gather pertinent inputs for policy making. Only 10% of the institutional respondents have actions in their policy making processes for identifying demanding or very demanding projects, and appropriate procedures for requesting particular services. In many cases there are mechanisms for taking informal soundings, but these are not totally satisfactory.

5.1.7.2 Networking services in the questionnaire

For the sake of clarity Part 2 of the questionnaire organised networking services (26 services) into three categories: the ones called "upper layers services" close to the applications; those depending on the basic network infrastructure (links, switching and routing equipment, etc.) called "lower layers services"; and the third category "Middleware and Security services".

IPv6, Multicast, and QoS, were dealt with apart (see 5.1.8 below).

For each service, it was asked if the service was provided to STUDENT and/or STAFF, users and if not provided why it was not provided; INTERNAL reasons (reasons related to the organisation of the institution, policy, security considerations, lack of expertise, lack of resources, etc.) or EXTERNAL reasons (reasons out of control of the institution, e.g. NREN or intermediate network not supporting the service in question, etc.)

What follows is a short synthesis of the survey's results on the provision of network services.

5.1.7.2.1 Upper layers services

Almost all respondents run personal mail services as well as mailing list management services and web services (Web storage, WEBDAV, Wikis, collaborative environments, etc.) for staff. For students, things are a bit different; they do usually have personal mail services, but only half of the respondents provide mailing list management and web services for students.

From 50% to 75% of the institutions responding provide videoconferencing and Voice over IP (VOIP) for staff. Fewer institutions provide the following services; audio-video stream, grid dedicated services, virtual organisation dedicated services and

HDTV (High Definition TV), the proportions decreasing from 41% to 5%. The numbers are much lower for these services provided to students.

5.1.7.2.2 Lower layers services

Wireless connectivity is almost ubiquitous. If the same survey were repeated in one year coverage would probably reach 100%, for staff as well as for students. Wireless roaming services (e.g. eduroam) are progressing, but so far they are provided by only 40% of the institutions, which means that there is still, some way to go to reach a global service. Possibly IT Managers consider the provision of VPNs to be a good alternative for eduroam, since VPNs are provided in the majority of institutions. Bandwidth on demand and provisioning of light-path are still very low in numbers (8 to 15%).

5.1.7.2.3 Middleware and security services

Among the services run by most institutions, for students as well as for staff, are: authentication and authorisation for network access; environments for securing email (antivirus, anti-spam, etc.); protection against attacks and denial of services; backup mechanism to ensure reliability. They are “traditional” or “classical” services, and they are considered more and more to be essential if not mandatory by IT managers and CSOs (Chief Security Officers).

It is not satisfactory that only about sixty percent of respondents provide confidentiality of data communications and disaster recovery. These should be considered essential for protecting the assets of the institution and ensuring continuity of crucial activities.

Identity federation services are one area on which much emphasis has to be put. Only one third of the institutions responding are running such a service. It is a “young” area, and it needs to be strongly supported.

5.1.8 Rollout of videoconferencing, Multicast, IPv6 and QoS

5.1.8.1 Videoconferencing Services

Videoconferencing services have been available in research and education institutions in Europe since the early nineteen-nineties. Early versions were expensive, but in the last ten years the arrival of IP connectivity, reduced hardware costs and better video compressions algorithms have changed the scenario enormously.

In spite of these improvements the current use of video conferencing is below expectations. There are several reasons for this, the main one being that videoconferencing is not as easy to use as the telephone, which is often a perfectly acceptable alternative. There is also evidence that many end users are not aware that their institutions offer a videoconferencing service.

The use of videoconferencing is likely to grow, but at an unpredictable rate. To increase its use institutions should take steps to promote awareness of their videoconferencing services, provide suitable training for users and offer good technical support, especially in the early stages of implementation. This should include

not only the network-related aspects of the service but also the audio-visual setup of the room: recommendations about lighting, projectors, cameras and microphones locations, etc. Once users become acquainted with the service the level of support can be reduced.

Embedded systems should be made available for group video conferences in two versions: specially arranged ready-to-use rooms for virtual meetings conveniently distributed in the institution, and portable units ready to be installed on request when necessary, for example for remote participation in conferences, symposium, etc. Those facilities should be managed by the IT department and leased to the users on request.

The use of MCUs (Multipoint Control Units) either owned by the institution or leased to an external company should be considered part of the service. Sharing MCUs between institutions should be encouraged, either at regional or national level (in that case the NREN itself should help set up the service).

Most potential users are not aware of the possibilities and benefits of videoconferencing. In order to increase its use 'demo' dissemination sessions could be organized as part of user meetings and other public events. Training courses oriented towards the end users should be organized frequently, and documentation about use of videoconference services for non-specialists should be made readily available to everybody in the form of web pages, for example

Recommendations:

- ***12. Institutions should actively promote videoconferencing and provide full technical support to users of video conference systems, especially to untrained occasional users***
- ***13. There should be full technical support for videoconferencing service, especially in the early stages***

5.1.8.2 Multicast

The history of Multicast is similar to videoconferencing. This technology was first specified in 1989. There were expectations that it would quickly become widely used, especially for multipoint videoconferencing services and video streaming. But Multicast did not become popular with commercial ISPs, many of whom still do not support it. At the present time Multicast is not widely used. The main application for this technology would be video streaming, but there appears to be little demand from potential users. According to the TERENA Compendium 2006, only 60% of NRENs offer Multicast. And those that do not offer Multicast tend to be the smaller NRENs.

The major benefit of Multicast is reduced load on networks and servers. However there are several drawbacks, namely

- complex and unreliable routing protocols
- complex and incipient address allocation schemes
- low security

These issues make commercial ISPs reluctant to adopt Multicast. The future growth of Multicast is less easy to predict than videoconferencing, but it is likely to become more popular when the current drawbacks are resolved. As with videoconferencing there is the question of raising user awareness to be addressed.

Recommendations:

- ***14. NRENs should encourage institutions in their respective countries to implement multicast in their networks and organise awareness campaigns to promote its use and increase the multicast content in their network. For example some universities already have TV channels on the air with scope in most cases limited only to the internal network or the metropolitan area. Those TV channels could be delivered by Multicast with good quality video using 4-5 Mb/s and made available worldwide in a very simple way and at a very reduced extra cost.***
- ***15. In those cases where the NREN does not provide multicast a plan should be devised to introduce the support gradually in the network with the goal of making it available to all the connected institutions.***

5.1.8.3 IPv6

The story of IPv6 is similar to videoconferencing and Multicast. In this case protocols have been around since 1995 but they have not fulfilled expectations.

The pan-European network GEANT2 provides complete support of IPv6, but it is not clear whether all NRENs do. In 2004, the TERENA Compendium showed that 70% of NRENs supported IPv6, but there is no later information available. Similarly it is not known whether intermediate networks support this protocol. It is feasible that an institution and its NREN are able to offer IPv6, but the intermediate network does not.

According to the Campus Issues survey only a small proportion of academic institutions in Europe have deployed IPv6 in their core networks. The main reason for not deploying IPv6 is again the lack of end-user demand. Other reasons are lack of compatible hardware or software and lack of training.

It must be acknowledged that IPv6 has essentially only one benefit - a much bigger address space. The advantage of a bigger address space is not especially attractive for R&E institutions in Europe because IPv4 currently meets their needs. Moreover, a significant number of those institutions are using NAT in their networks today, presumably as a basic firewalling procedure (blocking incoming connections) rather than as a mechanism to save address space. But a side effect of using NAT is to reduce the need for IP addresses, thus reducing the pressure to migrate to IPv6.

Sooner or later the migration to IPv6 will have to take place because the internet continues to grow quickly, and with it the need for more address space. Also, more and more host implementations support IPv6. The use of NAT is not a satisfactory solution since it is not completely transparent to the applications and requires extra effort from software developers.

It will not be possible to put off implementing IPv6 indefinitely. Institutions should begin making preparations to move soon.

Recommendations:

- ***16. All NRENs and intermediate networks (MAN or regional) should provide IPv6 services natively to allow institutions to prepare for a smooth transition to IPv6.***
- ***17. Institutions should provide their users with IPv6 services at all layers (network, transport and application) at least in their core network, and ideally in the whole network. They should request address allocation to the responsible entity (either their NREN or RIPE). This IPv6 enabled network should be connected to the rest of the IPv6 Internet***

5.1.8.4 Quality of Service (QoS)

Quality of Service (QoS) is another set of protocols that are at least 10-15 years old yet do not come anywhere close to meeting initial expectations. However there are some peculiarities in this case.

According to the survey a significant proportion of academic institutions in Europe have deployed QoS inside their campus networks, but in only a few cases is it available also in the Internet connection. In the cases where there is no QoS the main reasons are no need (i. e. plenty of bandwidth) or no demand from users.

The most important application using QoS is IP telephony, followed by video conferencing and multimedia streaming. In most cases IP telephony has probably been the main reason for deploying of QoS. This would explain why so many institutions have QoS support only inside their network (since IP telephony normally generates IP traffic only inside the institution network, and uses gateways to connect with the traditional telephone network for external calls).

In most institutions IP Telephony is a relatively new service offered by IT departments, so we forecast increasing deployment of QoS in campus networks in the near future as these services become more popular, but it is likely to be restricted mainly to the institutional network. In a later phase QoS could also be implemented at the NREN level if institutions start to exchange IP telephony traffic natively.

In order to facilitate the implementation of QoS services, institutions should ensure that their network equipment supports the relevant standards and protocols. They should also carefully evaluate the benefits (and possibly drawbacks) of having equipment from one single vendor in the core, especially from the point of view of configuration, management and maintenance simplicity.

5.1.9 Operational structures, control of the services

80% of the institutions surveyed have central Network Operational Centres (NOCs) and most of them provide services like: Incident Handling, Metering, Performance

Monitoring and Testing. However only 65% have formal links with their respective NREN NOC, and less than 50% have control of the complete institution infrastructure. “Peripheral” parts of the campus network (cabling, local servers, etc.) are often the responsibility of departments, faculties or laboratories, not the central NOC. In such situations it is extremely difficult to take a global vision of end-to end services and to ensure appropriate levels of security.

Recommendations:

- ***18. Central NOCs in institutions should have formal links with their NREN NOCs, and a formal responsibility to manage the campus network***
- ***19. The special needs of end users should be taken into account in defining networking policy. There should be formal procedures for end users to request special services***

5.1.10 Obstacles to seamless end-to-end connectivity

Inevitably in this complex multi-domain topology there are sometimes obstacles to seamless end-to-end connectivity, such as:

- **Bandwidth shortage.** In the campus issues survey it was found that some institutions of moderate size have low bandwidth to the NREN. Of these, the majority are connected to their NREN through intermediate networks, most often a Regional Network. Regional Networks have much evolved in the last years, and current initiatives (in UK, France, Spain) tend to show that these infrastructures are being upgraded to Gigabits speeds. This will be sufficient for Class A and possibly Class C users. However there may still be a limitation in the near future for institutions with Class C users who require 10 Gigabits or even more. The NRENs will soon be able to deliver such throughput but Regional Networks risk lagging behind unless they make the necessary investment.
- **Lower level of reliability and performance.** Each domain has its own NOC (Network Operational Centre). Multiple layers of management inevitably increase the risk of failures of communication, making coordination difficult sometimes. As a consequence service disruption may take more time to be fixed. If the different levels of infrastructure are under the same management responsibility the problem diminishes. There is no common set of tools or procedures to identify the cause of poor performance, or to monitor the end-to-end connectivity.
- **Discontinuity of services.** Harmonisation of services at OSI level 2 and level 3 is crucial to facilitate and enhance the collaboration of researchers at national and international level. Any unavailability of service may undermine the participation of researchers to important projects. Below is a list of different services which NRENs offer, most of which should also be provided by intermediate networks.
 - IPv6, Multicast and QoS should be available throughout the research and education networking infrastructure, but their deployment is not always guaranteed in every component between the NRENs and the institution campuses.
 - Virtual Private Networks. In some cases, only the NREN is providing level 2 and/or level 3 MPLS services as well as TE (Traffic Engineering) facilities. These are the basis for virtual networks for specific projects or communities of interest, etc. Level 2 VPNs could also be used as a

platform by the NREN to directly connect institution sites across a Regional Network for instance. Thus they would be able to provide all the services to end sites which they normally can offer only to sites with a direct physical connection.

- Bandwidth on demand.
- Light path allocation.

A priority of future research and education networking policy must be to guarantee end-to-end functionality, including bandwidth, services, supervision, etc. To reach this goal, with a complex networking infrastructure of many domains, there should be strong coordination of the activities of NRENs, Regional Networks, MANs and institutions.

Closer collaboration between domains is needed to:

- identify the requirements of researchers, teachers, students, etc. before finalising the main strategic policy orientations, architecture, topology, services, etc. of each project;
- plan greater homogeneity and continuity of technologies and services at each level of the global infrastructure. This may mean having common elements in procurement documents;
- set up common operational procedures with formal interfaces between NOCs; common or inter operable tools for performance metering and monitoring, incidents handling, etc.

Recommendations:

- ***20. The specific requirements of end user communities should be recognised and incorporated into the operational specifications in the different domains serving those communities***
- ***21. Continuity of the services provided by NRENs should be guaranteed by all the networking domains involved to enable seamless E2E connectivity when a particular quality of service is requested.***
- ***22. The interface between different management domains should be formalised, e.g. by common SLAs between domains and especially between Regional Networks, Metropolitan Networks and the NREN.***
- ***23. The following services have high priority: IPv6, Multicast, QoS, MPLS (L2, L3) plus Traffic Engineering.***
- ***24. Infrastructures for optical continuity (links as well as basic optical equipments) should be planned in areas where communities of researchers are identified as potentially heavy users of networking services.***
- ***25. There should be strong and formalised structures for collaboration between different management domains.***

5.1.11 Connectivity to Commercial ISP sites

During the last few years Research and Education Networks (RENs) in Europe have improved their capacity by several orders of magnitude. There has been significant investment in infrastructure and technology by many organisations in different domains: campus networks, intermediate networks (metropolitan or regional) where

applicable, NRENs and also at the European level by the different generations of networks set up by DANTE: EuropaNET, TEN-34, TEN-155, GÉANT and GÉANT2. DANTE also provides connectivity to several important RENs located in North and South America, the Mediterranean area, and Asia.

As a consequence of these continuous improvements, the vast majority of the research and education community in Europe today enjoys excellent connectivity with most of their peers in the rest of the world, with short delays, high bandwidth and high quality services operating on a 24x7 basis.

But the situation is not so good when the remote destination is not within the research and education community. Sometimes there is a noticeable increase in the response time when the user tries to reach a server located in the commercial part of the Internet. The fact that the user is accustomed to short delays within the REN makes the experience even more frustrating.

Long response times may be caused by bottlenecks somewhere in the network path or an overloaded server. In many cases solutions to the problem are outside the scope of the REN domain. But in spite of its complexity it is important to resolve the problem because, from the user's point of view, it does not matter where the delay is. He/she is suffering poor network performance and therefore low quality service.

To overcome this problem caching proxy servers are sometimes deployed. If the hit ratio of the proxy server is high (i.e. there is high repetition in the pages downloaded by the users) this is a good solution. However proxy servers have several important drawbacks that outweigh the benefits in most cases. These include:

- Many pages are dynamic and non-cacheable nowadays, significantly reducing the hit ratio. A list of known HTTP proxy/caching problems is compiled in RFC 3143
- The hard disk performance of the proxy server becomes a limitation in high load conditions
- If Internet access is configured through a proxy server, the server becomes a critical part of the service

Recommendation:

- ***26. Do NOT use a caching proxy server except in very specific conditions when the benefits clearly outweigh the drawbacks.***

Another way to improve the response time in low bandwidth situations is to use Content Delivery Networks (CDN). Whilst caching proxy servers are reactive, i. e. they bring the content when the user requests it, CDNs are proactive, in the sense that they try to bring the content in advance to have it located near the user before he/she requests it. Unlike proxy servers which are configured and maintained by the hosting institutions exclusively, CDN requires close cooperation and coordination with the content provider in order to be effective.

There are some obvious similarities between proxy servers and CDNs and some of the drawbacks regarding proxy servers also apply to CDNs. But it is generally accepted that the CDN approach is more efficient because it is not completely automatic. CDN

is managed by the content provider who knows which content is cacheable and thus can take an informed decision to make the process more efficient. Also the proactive strategy of CDN gives the benefit of a fast response even for the first user.

Some European NRENs (e. g. RedIRIS in Spain, SWITCH in Switzerland) have agreements for hosting Akamai servers in their network nodes. Akamai decides which content is replicated in the servers, the NREN decides which users can access the servers. Having a CDN infrastructure owned by the NREN would permit them to decide the content according to the interests of their users.

Recommendation:

- ***27. Each NREN should consider establishing a pilot CDN infrastructure to test the scope for improved response times in accessing popular content in the commercial part of the Internet***

5.1.12 Software restrictions

Many research and education institutions in Europe have network infrastructures providing 100 Mb or even Gigabit Ethernet connections to the desktop. However, users are sometimes not able to obtain the full benefit of the bandwidth available due to limitations in end-to-end communication.

The limitations happen for a variety of reasons, such as problems in the communications software (typically at the transport or application layer); poor system performance produced by some operating system component; or even by hardware issues. Fine tuning of the software is needed to improve performance, but institutions often do not have sufficiently skilled engineers to do the work.

Recommendations:

- ***28. Careful selection of protocols and implementations is recommended to avoid bandwidth limitations. Skilled tuning of software and systems can improve performance considerably. However this requires expertise beyond the skills of the average user. Since the user gets his/her work done anyway he/she may not even be aware there is a problem and does not seek specialist support.***
- ***29. Institutions and NRENs should provide support, training and documentation about performance optimisation issues, especially for the needs of Class C users.***

5.1.13 Governance, funding and operation of the network infrastructures and services

5.1.13.1 Connections to the NREN

The majority of respondents to the questionnaire were connected to the Internet via an NREN, either directly (50%) or through an intermediate network (40%). A small proportion use ISP connections. The funding of NREN connections varied considerably with only a minority fully subsidised.

Respondents were asked to identify the benefits of NREN services.

The most often cited advantage was the ability to get more capacity and higher bandwidth at reasonable prices, and in a flexible manner, without having to undergo time consuming negotiations with ISPs.

Most NRENs provide more services than ISPs, and the services provided are of better quality. The services are normally state of the art compared to ISPs, and NRENs often give some flexibility to run extra services, or pilot services not yet considered to be operational. The services are tailored better to their connected institutions. ISPs are often said to be more business oriented. NRENs generally know what an institution's business is, and are more aware of the needs of the academic community.

5.1.13.2 Networking management, policy design and funding at institution level

The majority of responding institutions have an Acceptable Use Policy (AUP) supported by the governing body of the institution. However a significant minority (26%) either have no AUP or, if it exists, the AUP has not been approved at a senior level in the institution. This should be a cause for concern because it suggests the institution's senior management does not recognise the strategic importance of networking. It is also significant that only about 30% of respondents formally consult their user community about networking policy. In some institutions even the head of IT services does not appear to know how to influence the institution's networking strategy.

Interestingly, in response to a question about the effectiveness of recommendations and guidelines from NRENs the majority said they believed such guidance had real influence on their institution's networking policy.

Recommendations:

- ***30. Every institution should publish an Acceptable Use Policy (AUP) document, to be communicated to end users to make them aware of the services available to them, and to state their rights and obligations regarding the way they use such services. The governing body of the institution should endorse this document.***

- *31. End users should be represented in the development of policy documents which directly impact on services offered to them. National recommendations and guidelines for best practice would help to create such procedures inside institutions.*
- *32. National recommendations are perceived to be influential in developing institutional networking policies and should be encouraged where they do not already exist.*

5.1.14 Organisation of networking expertise, staffing, training

The level of quality and performance of institutional networking services, as well as their range of functionality, depends crucially on the size and the level of expertise of the networking team supporting these services.

Part four of the survey revealed the existence of a very wide diversity of situations from which it would be impossible to draw general or generic conclusions. The text below is limited to a number of observations which identify serious issues to be considered:

Size of networking teams:

About 66% of respondents felt that their networking team was not adequately resourced. In 50% of the responding institutions there were less than 5 FTE members of staff for networking. There were several large institutions in this group.

Levels of expertise:

A majority of IT Managers responding said they experienced difficulties recruiting staff with a good level of expertise. This makes the networking service vulnerable in key areas such as security; installing new services; keeping pace with developments in technology; performance monitoring; informing users of new functionalities.

Training of staff:

A significant minority of respondents provide very little training for support staff. The majority do not have systematic training plans for staff in IT service departments.

Recommendations:

- *33. There should be a clear link between an institution's networking policy and the resources available to deliver its objectives. The policy should be drawn up by senior management, working closely with end users and the network support team. The policy should specify the services to the end-users and the quality of these services (level of reliability, coverage in time, etc.), providing a "charter" between the institution and the end-users. The network support team should be adequately staffed and have appropriate expertise.*
- *34. Information Technologies keep evolving at a fast pace. Technicians and engineers frequently have to adapt to new technologies (equipment, software, protocols, architectures, services, etc.). It is vitally important that they are properly trained to carry out the tasks expected of them.*

5.1.15 Raising awareness, training and support for network users

In the analysis of responses to the Researchers Requirements Survey, there is strong evidence that many network services are under-used. Users are either not aware of the services currently available or they only make limited use of them.

For example, the Researchers Requirements Survey shows that only a minority of respondents uses IP telephony, videoconferencing, bandwidth reservation and encryption of data, and then infrequently (i.e. less than once a week). When asked about their use of specific network-related tools, a significant number of respondents replied that they did not understand some of the terms used, implying they were not aware of the availability of some commonly available network services. The Survey also asked respondents to assess aspects of the network infrastructure within which they worked. Only 41% agreed they received adequate training in network use to improve the quality of their research or teaching.

There is supporting evidence from the Campus Issues Survey that, although it is technically feasible to provide many network services, they are not as widely available as might be expected. Such services include eduroam, Multicast, bandwidth on demand, QoS, and PKI.

5.1.15.1 Possible reasons for low levels of use

There is a variety of reasons for the under-utilisation of network tools and services, including:

- A network service is available, but it is not publicised and many users do not know of its existence
- A service is available, but badly supported because, the network support team is too small to support the service or there are not enough network staff with the right level of skills to support it
- A network service is not available, even though it is technically feasible to offer it. Some institutional service providers are reluctant to offer a service, such as videoconferencing, because they know they will not be able to cope with the demand for support
- The network infrastructure is incorrectly configured in such a way as to prevent the service being offered, sometimes for questionable “security” reasons
- There is a culture of low expectations in the user community which inhibits them from demanding new services
- The service provider has not adapted to its new role of offering services rather than basic network connectivity
- There is a lack of customer focus in the service provider organisation.

5.1.15.2 How to raise awareness, train and support network users?

To improve the take-up of network services there is clearly a need for better dissemination of information about developments in this area. There should be more publicity, better training and higher levels of support for many of the network tools and services currently available. A relatively modest investment in promotional videos, on-line training material and brief explanatory documents would yield enormous benefits throughout the European higher education sector.

It is also evident that some institutions have not increased the size of their network teams to enable them to support network tools and services adequately. Some institutional network teams are too small and cannot hope to provide more than basic support for network connectivity. They spend much of their time “firefighting”. Even if they wish to introduce new services many wisely hesitate to do so because they are already overstretched. In recent years institutions have invested significantly to upgrade their campus network infrastructure. But there is evidence that many do not have enough human resources to exploit fully the benefits of their increased investment in the technology.

It is also important that users and network staff are properly trained to use and support the new services. Some training materials will be specific to the situation in individual institutions; others are more generic and could be developed for national or even international audiences.

It should be self-evident that *human* networking is an important element in the field of networking, and at the strategic and management levels there is much co-operation and collaboration. However, there should be closer collaboration at grass roots level too, to share skills and keep up to date with new developments in networking technology.

Finally, and most importantly there is a need for cultural change. There are signs that some campus network teams have not extended the scope of their service beyond providing connectivity. A paradigm shift in the nature of network support is taking place, from providing connectivity to providing network services, and some network support teams and their user communities do not appear to have recognised this.

Recommendations :

- ***35. Promote awareness of network tools and services in both the user community and service providers***
- ***36. Provide well-resourced skilled network teams in institutions***
- ***37. Encourage all network support staff to collaborate with colleagues at other institutions, regional networks and NRENs***
- ***38. Encourage a change of focus from connectivity to network services***

5.1.16 Collaboration and dissemination of information

5.1.16.1 Collaboration between NRENs and Institutions.

In most countries there are formal arrangements (one or several) at national level to bring together the networking experts of NRENs and institutions. The purpose of these arrangements is to foster collaboration, ensuring a better information dissemination process and the exchange of experience and expertise.

60% of institutions responding to the survey meet their NREN colleagues once or even less per year, which gives little opportunity for collaborative work.

There seems to be a pretty good level of information dissemination concerning announcement and events of all kinds. However the results of workshops seem not to be very well publicized, or perhaps workshops are rare events in some countries.

Information dissemination and workshops are crucial for coherent development of networking services in every domain (NREN, MANs, campus networks), especially in such a fast-changing branch of IT.

The survey shows there is little feed back from end-users to the NREN. If it exists it may certainly be improved. This would help the NREN as well as the intermediate network to leverage the quality, reliability and security of their services. According to the survey incident handling, Security, troubleshooting, performance, videoconference and authentication are among the highest on the list of topics which are submitted as problems to the NREN. It is not clear how many NRENs have formal channels to collect feedback from the user community, but they would be welcomed by end users. Better channels of communication would be beneficial all round.

5.1.16.2 Collaboration between network engineers from different institutions

The most surprising result of this part of the survey came from answers to a question about the level of collaboration between engineers from different institutions. Only one third of respondents considered there was enough collaboration, and half of the rest said that levels of collaboration had not improved in recent years.

However, many respondents recognised the potential benefits of closer collaboration with their counterparts in other institutions. In particular they said they would increase their own expertise by sharing experiences with their peers.

Recommendations:

- ***39. Increase the regularity of workshops between NREN engineers and institution engineers, on strategic issues regarding the future of networking in the R&E community. In case no such workshops exist, NREN should take steps to create regular cycles of workshops on critical issues.***
- ***40. Set up formal procedures (processes) for gathering end-users feed back for improving the quality and reliability of services. Setting up such***

procedures relies much on Networking Management decisions in each institution. End-users will not guess out of nothing how to contact their NREN and transmit their complaints or their proposition for improvement.

- *41. NRENs, funding bodies, and/or national structures which have administrative supervision on research and higher education institutions should encourage institutions to better organise collaboration between engineers, Networking Managers from institutions.*

6 Phase 2:

Technology strategic orientations, future of campus networking

Survey of research networking areas

Impact of new developments on the future of campus networking

Recommendations, Conclusions