

Implementing a hybrid LDAP directory at Monash University to provide access to external users

*Mr Nathan Bailey, *Ms Kerryn Jackson, *Mr Leslie Liew, *Mr Peter Schendzielorz, *Dr Andrew Treloar, *Mr Leon Troeth
{*Faculty of Law|*Information Technology Services}, Monash University
Wellington Road, Clayton, 3168, AUSTRALIA
Principal Author's Email: Andrew.Treloar@its.monash.edu.au

A common problem at many universities is providing access for external users to resources normally limited to internal users. The Monash Hybrid Directory Service (HDS) is a combination of our existing Monash Directory Service (MDS) for internal users and the External Directory Service (EDS) for everyone else. Registered categories of users throughout the university are able to add people into the EDS. University services can then choose to use the HDS as their authentication source. This solution has met a vigorously-stated customer need, removed Information Technology Services from making the authorisation decisions, and ensured that access to critical services remains controlled. This paper will describe the drivers for the HDS, the implementation of the solution, and the benefits for all concerned.

1 Overview of Monash and ITS

Monash University was originally based in Clayton, Victoria, Australia. Over the past decade, the university has expanded, and now has six campuses in Victoria, as well as campuses in Malaysia and South Africa, a number of smaller locations at various Victorian hospitals, overseas study centers in London and Prato (Italy), and an office in central Melbourne. Monash University plans to continue to expand globally over the coming years. Monash currently has around 10,000 staff and 65,000 students.

The Information Technology Services (ITS) Division is the central information technology and communications group of Monash University. ITS is responsible for much of the University's IT infrastructure including network and internet connections, workgroup and central host servers, corporate databases, lecture theatre support, helpdesk and information services, that keep Monash at the leading edge of innovation in its core activities of teaching, learning and research. IT planning is centered around the IT Strategic Plan that describes a framework for the application and usage of IT within Monash University. Its aim is to ensure that University-wide IT initiatives are directly aligned to the overall mission, strategies and operational needs of the University. ITS has developed a Services Catalogue as part of a Service Management initiative outlined in the Monash University Support Services Strategic Plan. The Services Catalogue identifies the major services and service outcomes currently provided to the Monash community.

The vision for ITS in 2002 can be summarised as:

- Aligning IT to the strategic goals and global aspirations of Monash
 - Being responsive to the service needs of the Monash community
 - Deploying leading edge IT solutions where appropriate
 - Adopting efficient and cost effective methods
 - Engaging in multidisciplinary teams across organisational boundaries
 - Being transparent in processes and accountable for performance
-

2 Getting directory-enabled

Monash has been a large user of Novell for some years now. As part of this, we have an extensive Novell Directory Service (NDS) tree, with entries for every staff member and student. In fact, the primary network login for most staff and all students is still a Netware login. However, the NDS has traditionally been used primarily within the Novell environment and has not been seen by Monash as a candidate for an enterprise directory. In order to fill this need, it was felt that an LDAP-based directory would be more appropriate.

The opportunity to build such a directory came from an unexpected direction. In 1996, Monash was looking for a replacement messaging and scheduling system. After careful evaluation of user requirements and examination of a number of contenders, we ended up selecting the Corporate Communications Suite (CCS) from what was then Netscape Corporation (later iPlanet, and now Sun).

The CCS consisted of:

- Directory Server
- Messaging Server
- Collabra (an LDAP-authenticated news server)
- Compass (Web search engine)
- Calendar
- Certificate Server
- Web Server

We decided to initially implement Messaging Server, Collabra and Calendar as the new Monash Messaging System (MMS). In order to do this, we had to build a central LDAP [1, 2, 3] directory (both to store configuration information for the servers and authentication and profile information for our users). At the time our NDS was not able to provide the services required to implement the Suitespot bundle. We therefore decided to implement Directory Server and call this new directory the Monash Directory Service (MDS).

The Monash Directory Service

The MDS currently contains over 90,000 entries. The data feed model we have adopted is that for each type of entity there is a single authoritative source database. All changes to data are made at the source, and these changes then flow 'downhill' into the MDS. We never push changes back 'uphill'. For student entities, the primary source is Callista (our Student Administration system). For staff entities, the primary source is SAP-HR (the Human Resources module in our Enterprise Resource Planning (ERP) system). Staff who are not paid employees of Monash can be entered into SAP-HR as Visitors/Honorarys/Contractors, which ensures that they appear in the normal data feed. We also take a number of data feeds from other systems, such as legacy staff systems and the telephone directory.

Changes to data sources are propagated into the directory overnight via a series of batch jobs. We are currently implementing a number of changes to our processes to move closer to real-time change propagation. We also provide web-forms to allow for immediate changes to values that are only held in the directory, such as passwords. We are currently providing a form of synchronization between the MDS and NDS via the somewhat brute-force approach of only allowing password changes using a special web-form. This form then pushes the changes out to both the MDS and NDS. We are also hoping to re-engineer this in the future. The MDS-based password authentication mechanism is called AuthCate within Monash. A user's AuthCate password is now the main authentication token that they use to access IT resources at Monash.

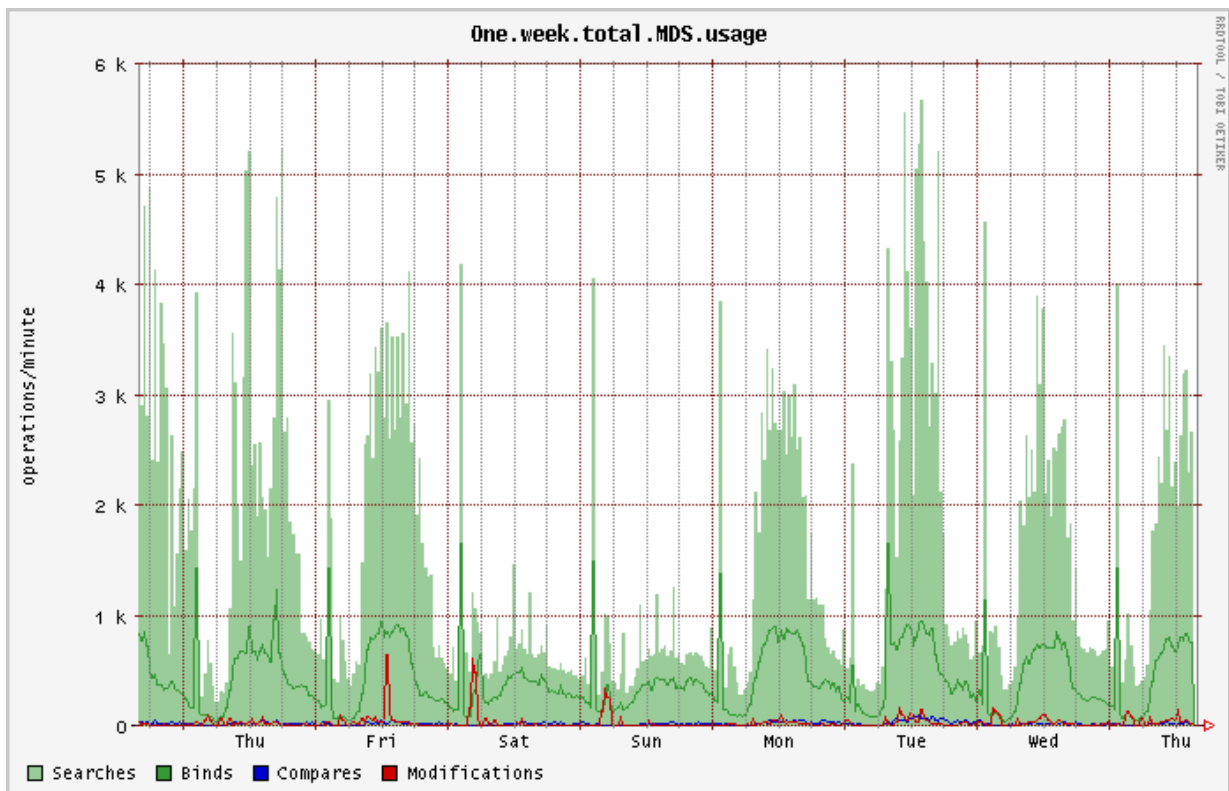


Figure (1): A typical week in the life of the MDS

The infrastructure behind the MDS is currently a farmlet of two Sun E250s, each with 2 GB of RAM, and 6*36GB of disk (striped and mirrored). These machines (called carrot and lettuce) are currently behind a layer-4 switch which distributes traffic across the farm. We are about to double the number of machines in the directory farm by replicating this infrastructure at our alternate production site. This farm is used for all general MDS requests. There are also a number of other instances of the Monash Directory Service that are used by larger applications. For example, the staff mail server has its own directory instance, as does the student mail server, calendar server and digital certificates server. Other instances exist at the Monash campus in South Africa for services that are based there.

Traffic on the Monash Directory Service is, as one would expect fairly cyclical. Figure (1) shows the traffic in a single week over the MDS servers. Spikes occur during regular processes that update the MDS or other systems that use the MDS as a data source.

Since its inception as a point-solution directory, the MDS has quickly grown in popularity. Driven by the trend towards using a single username and password for many services (same sign-on), LDAP support in applications, and the ready availability of sample code, more and more areas of the university are using the MDS. Current applications that rely¹ on the MDS include:

- Staff and student email
- The main time/resource scheduling system (Calendar)
- News group/collaboration server (Collabra)
- The my.monash portal

¹ I.e. the applications don't work when it goes away, and their owners get very upset ...

- Dialin modem banks
- Innumerable .htaccess files on web servers around the university
- Proxy authentication for external Internet access
- Employee self-service through SAP-HR
- Many faculty databases
- Monash Public Key Infrastructure (Digital Certificates)
- An increasing range of online applications such as student self-service (WES) and course and unit publications information (CUPID)

The joys of demanding clients

Not content with the MDS, a number of our clients started asking us for a way to authenticate users who were not in the MDS. The driver for these sorts of requests were the need to provide short-term access to categories of users who were not part of our normal data feeds. Examples from the student domain might be students outside Monash (both Australian and overseas) who were taking part in a unit shared between Monash and some other university. A staff example might be the need for an external person to take part in a unit for a few weeks as a guest lecturer or non-Monash staff be able to audit a course. In particular, the Law Faculty, driven by a University climate promoting stronger industry links and encouraging entrepreneurial activities as a means of attracting funding, required extensive use of a facility such as this in implementing innovative teaching models.

In developing stronger industry links, the Law Faculty was inviting industry members, such as High Court Judges, to moderate online discussion groups and to act as guest lecturers for a short period. Such people required access to the my.monash portal, the Collabra service, and, web based materials restricted by .htaccess. It was seen as a potential detractor to require them to make a special trip to Clayton in order to fill in forms and have their photograph taken in order to get their details into SAP-HR and thus the MDS². This was particularly inappropriate when much of their involvement with the Faculty would take part either in the Monash city premises or from their own remote connection. Thus, a mechanism whereby these category of people could authenticate to Monash online services without being in the MDS was required.

At the same time this service was being requested, the Law Faculty was also working with other Faculties and another section of ITS, the Flexible Learning and Teaching (FLT) team, in redeveloping InterLearn, an online collaborative teaching and learning environment designed at Monash. The Law Faculty, in partnership with other Australian universities, was planning to use InterLearn to provide practical legal training to law firms across the country. Monash was to host the system via the my.monash portal, and coordinate the development of the learning materials to be used by teaching staff from all partner universities. Students would enrol only in the partner university within their state, but all would require access to the Monash hosted learning environment. Providing access to students and staff was to be the responsibility of the Law Faculty's IT team. The involvement of non-Monash teaching staff and students made the need for authenticating users not in the MDS a strategic imperative.

Clearly we needed to come up with something to meet these needs.

² This was the provisioning model at the time, but is not longer the case - to have a staff member added, the relevant department now just needs to fill in a form and send it to HR

Designing the right solution

First we had to define the users. We realised that this system would have both intermediary users (those in Monash who authorised external access) and end users (external users who were granted access to Monash services). Next we needed to decide on the design guidelines. After a minimum amount of introspection, it was clear that whatever we implemented needed to have a number of characteristics.

The first of these was devolved management. We had no idea how popular the system was going to become, but we knew that we didn't want to be the bottleneck. An environment where ITS had to authorise each individual would be frustrating for our clients and us. Fortunately, we already had a well-established network of IT support officers in the Faculties who already had delegated rights over other parts of the centrally-provided infrastructure. We were able to see how we could hook into this network and allow them to authorise these new users.

One of the main concerns was related to security. In the process of creating accounts for external users, it was important to ensure that they only obtain access to the specific services that they required. If the external users were added to the Monash Directory Service, they would have obtained access to a wide range of services and restricted information by default. By default, services are only published to the MDS, and service administrators have to explicitly allow HDS access to their service if appropriate. Another security concern was to ensure that the external accounts would be removed when they are no longer required.

It was important that any solution was consistent with our existing infrastructure. One worst-case scenario would have been to provide duplicate staff and student data services. This would have been a lot of work, for little return. Doing something that was an easy extension to our existing services was a much more compelling proposition.

Because many of the ultimate end-users of this service would only be accessing our systems infrequently, we wanted it to be as transparent and as simple as possible. Providing them with a single username/password combination that they could then use for all their interactions with Monash was deemed to be the best way to do this. For a range of implementation reasons, usernames that were issued to external staff had to be designed not to conflict with existing Monash usernames.

Finally, it needed to be easy for Faculty IT staff to use. They would be using this infrequently, but possibly in concentrated burst (as when adding a batch of external students). We wanted to reduce load on the ITS HelpDesk and we also wanted to provide a good user-experience for our intermediary users.

The solution

Based on the above list, we decided to provide a second directory service, which could be separately managed and combined with the existing MDS as necessary. We decided to call this the External Directory Service (EDS).

Figure (2): Data Entry screen for creating a generic external user.

The EDS is implemented as a separate directory instance, running on the same servers as the MDS but on a different port. Intermediary users are provided with a web-based data entry form to allow them to enter and manage the external end-users to whom they wish to provide access. A sample data-entry screen is shown as Figure (2). As this example screen shows, each user has associated with them an expiry date to simplify management. Intermediary users do not have to remember to delete users – they are automatically expired every six months or on the specified date unless their access rights are renewed. Entries in the EDS contain similar details to those recorded for users in the MDS, including information about the ‘owning’ faculty/department and their role. This allows for finer-grained control over access. For instance, access to a given application or resource can be limited to all users listed under the Law Faculty. Intermediary users are constrained as to where in the organization they can add new external users. For instance, Law Faculty intermediary users can only add new external users under the Law Faculty. To avoid any conflict with existing Monash usernames, all usernames for external users are prefixed with “ext-”.

We now had a way to store and manage external users. But having the users in a directory is of little use unless the directory is actually used to control access to services. With two directories (EDS and MDS) there are three possible combinations: EDS only, EDS+MDS, MDS only. In practice only the latter two are used. In other words, the EDS is a means to an end, rather than an end in itself. The EDS is combined with the MDS to create the Hybrid Directory Service (HDS).

Users in the Monash Directory Service exist in one of the following three directory trees:

- Ou=Staff, o=Monash University, c=AU
- Ou=Associated Organizations, o=Monash University, c=AU
- Ou=Student, o=Monash University, c=AU

External users are stored in the EDS in the following tree:

- Ou=External Users, o=Monash University, c=AU

The Hybrid Directory Service receives a data feed from both the MDS and the EDS and contains all four database trees:

- Ou=Staff, o=Monash University, c=AU
- Ou=Associated Organizations, o=Monash University, c=AU
- Ou=Student, o=Monash University, c=AU
- Ou=External Users, o=Monash University, c=AU

The HDS can then be used as the authentication source for services that wish to grant access to both Monash and non-Monash users. Given that access for external users was generally required for broadly available services such as the my.monash portal, Collabra news server and some restricted web pages, access controls are in place to ensure that the Hybrid Directory Service can only be used from these specific services. This is added as a precaution to prevent external users from gaining access to services that they are not authorised to use.

Because both directories are configured and run in the same way, users and administrators of services will see the same access control and management functions whether they use the MDS or the HDS.

This solution meets all the design criteria:

- Devolved management: Once the web-form was created, ITS does not need to intervene in the day-to-day management of external users
- Security: External users are prevented from gaining access to services that they should not have access to. External user accounts are removed automatically when they are no longer required.
- Consistent infrastructure: We are using another instance of the core infrastructure that we are already familiar with
- Transparency: End-users are provided with a unique AuthGate username and password that they use in the same way as the rest of the Monash community
- Ease of use: The web-form provides a simple way for intermediary users to manage end-user information

And the response

The system was first made available for use in semester 1, 2001. Since that time we have had a total of 329 account creations. The HDS is now used as the authentication source for the my.monash portal, Collabra (which is used heavily for subject-based discussion groups) and a small percentage of restricted web pages. Figures (3) and (4) show graphs comparing searches and binds on the MDS versus the HDS over a typical week. The majority of the HDS traffic is generated by the portal (which serves students of units which involve external staff/students), since it uses the HDS as its main authentication source. However, only a small percentage of the requests that are handled by the HDS are for external users.

In addition, we have not yet heavily marketed the HDS service within the university. As a result, we have a small (but important) group of 186 users in the EDS, compared to 84130 in the MDS. The decision on internal marketing was a deliberate one. We didn't want users to see this as the 'easy' way to give access to services to 'anomalous' users who didn't fit the normal categories. Our preferred mechanism was (and is) having people with an ongoing Monash association entered into SAP-HR as Visitors/Honoraries/Contractors. Now that we have established this model, and the HR processes are less onerous, we can be less constrained about promoting the benefits of the HDS for those users for whom it was designed.

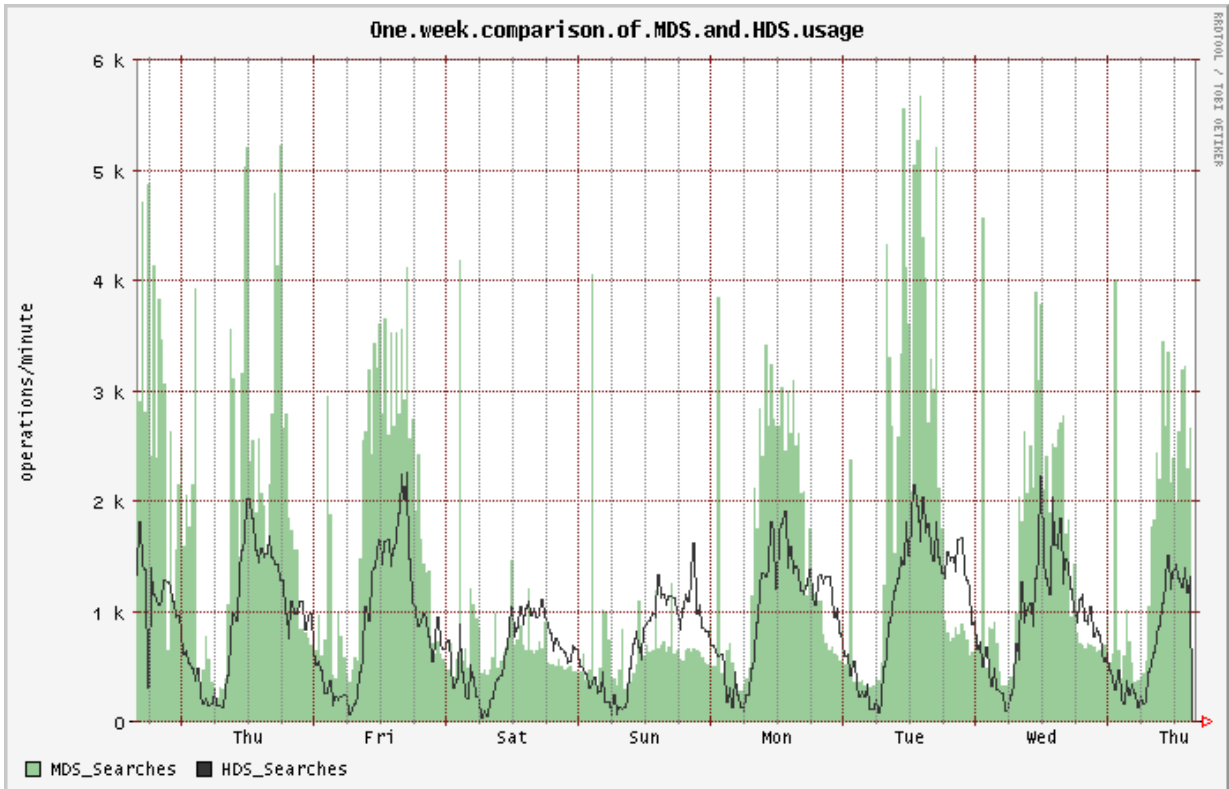


Figure (3): Comparative usage (searches) for directory (MDS) and hybrid (HDS).

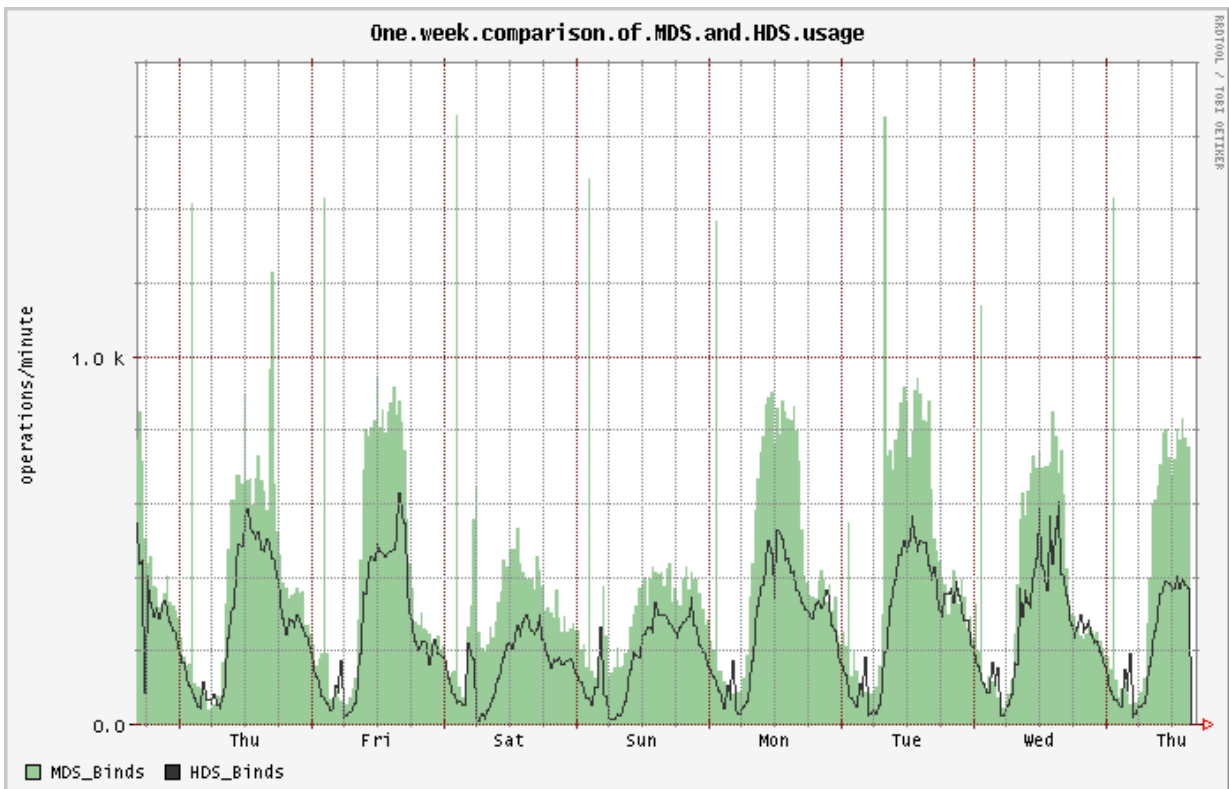


Figure (4): Comparative usage (authenticated connections (binds)) for directory (MDS) and hybrid (HDS).

Conclusion

The HDS meets the needs of its target users well. It has been implemented in a way that supports devolved management, is consistent with our other infrastructure, meets the relevant security concerns, is transparent to the end-users and is easy to use for the support staff. It has been an excellent example of how to take an existing service and, by thinking laterally, to extend its utility. Early in 2003 we will be reviewing it after its first two years of operation and considering the best way of promoting its benefits to the Monash community.

References

1. W. Yeong, T. Howes, and S. Kille (1995), *Light Weight Directory Protocol*, <http://www.ietf.org/rfc/rfc1777.txt>
 2. J. Morgan and R. Hodges (2002), *Lightweight Directory Access Protocol (v3): Technical Specification*, <http://www.ietf.org/rfc/rfc3377.txt>
 3. T. Howes and M. Smith (1995). "A Scalable, Deployable, Directory Service Framework for the Internet", *Proceedings of INET '95*, Honolulu. <http://www.isoc.org/HMP/PAPER/173/html/paper.html>
-