Case Studies

Document Reference: GEN-DOC-005 - *Please see here [1] for additional document control information.*

4. Case Studies

The following sections describe various examples of guest facilities provided by Janet-connected organisations. The organisations, and their requirements to support guests, vary widely, so it is not surprising that the solutions are very different. Most use a combination of the tools described in the previous section – a table showing the main tools used in each case study is in section 4.8 – and all are based on a careful and continuing analysis of the organisation's requirements and the risks they must address. Because requirements and circumstances vary between organisations it is unlikely that a particular solution will be a perfect match for any other organisation. However it is hoped that describing a range of solutions will help others to identify an appropriate selection of tools to satisfy their own requirements.

4.1 Library Kiosks

For some applications, fixed terminals managed by the organisation may be sufficient to meet the requirements of guests. Library catalogues are a long-established example where fixed terminals are dedicated to a single purpose. Typically these are Windows terminals configured only to run a single web browser in kiosk mode: there is a fixed home page (usually the library's OPAC (Online Public Access Catalogue)) from which users can follow links but not enter their own URLs. Such kiosks can be used to access online resources if these are added to the OPAC's links page.

Licences for online resources often permit access by anyone physically in the library, by analogy with their access to physical copies of books or journals, and this is included in the JISC/NESLI2 model licence. However not all publishers include guests in their licences so it is important to check before adding any resource to a publicly accessible catalogue, particularly for resources that use a library IP address as their only source of authorisation. If the same kiosk is used to provide access both to resources that permit walk-in access and those that do not, it will be necessary to identify whether a user is a member of the local organisation or a guest. This can be done either by requiring all users to login to the kiosk, with guests being provided with a temporary account that reveals their status, or else requiring logins only for those local users who wish to access restricted resources.

Since access to most libraries is physically controlled, unaccompanied guests usually need to ask a helpdesk to let them in. At this point they can be informed of the policies applying to library use and be issued with any temporary credentials that may be required, using any of the processes described in section 4.4 below.

Further details of walk-in use, licences and technology issues can be found on the web page of the HAERVI project.

4.2 Physical Spaces

These two case studies explicitly use the physical environment – the walls of buildings – as one way to manage guest access to the network. This works well for wired connections; for wireless it will only be suitable for particular buildings, and requires careful design of the wireless installation and regular monitoring to ensure that the intended containment is still effective.

4.2.1 Residences

One of the simplest requirements is where guests have their own rooms, for example in university or college accommodation. Where the room has a live network socket, it seems reasonable to make the occupant of the room responsible for all use of that socket during their stay. Some residences have the facility to enable and disable sockets depending on whether the current occupant wishes to use them. At the same time guests can be informed of the Acceptable Use Policy and asked to indicate their agreement to it.

As with any facility where guests connect their own equipment, it may be appropriate to consider some filtering or bandwidth management on these sockets to restrict the harm that can be caused by unexpected configurations or software on such equipment. Switches that prevent guest devices talking directly to one another and force traffic to go via a filtering router may help prevent the spread of problems. Bandwidth controls are generally a good idea to prevent traffic to or from the residence interfering with the normal business traffic of the organisation.

4.2.2 Work Places

Where an organisation’s buildings are physically secure, with controlled access, it may also be possible to use the physical perimeter to control access to a wireless network. Since the radio signals used by wireless networking equipment can pass through walls and windows it is important to plan the internal wireless deployment to minimise the signal reaching outside the building and to carry out frequent external surveys to confirm that no usable signal is escaping. However, depending on the construction and shape of individual buildings this may be impossible to achieve.

Since there is always a risk that an uninvited visitor may be able to connect to the network, for example by using a more powerful wireless antenna or by gaining access to the building, the connectivity available should be tightly controlled and monitored. For example one organisation uses a VPN to ensure that traffic from its wireless access points can only be routed to a web proxy that gives unauthenticated users access to a limited range of sites, and at relatively low bandwidth. The use of a proxy also means that guest machines can be given private (RFC1918) IP addresses, which are not routed anywhere outside the VPN. When a machine first connects, the proxy displays the Acceptable Use Policy for the wireless network facility. The proxy also keeps a time-stamped record of all sites visited as well as attempts to access blocked sites. This record is monitored and access can be further restricted or withdrawn if there are any signs of problems. These arrangements have been discussed with the local police to confirm that they considered the measures sufficient to address any concerns about possible criminal use.

The restricted access provided to unauthenticated users has proved sufficient for temporary guests but unattractive to students, staff and longer-term guests who prefer to register for individual credentials to get the wider range of connectivity provided to authenticated users.

4.3 Conference Delegates

A large, week-long international technical conference attended by delegates from both education and commercial sectors presented the administrative problem of issuing credentials to several hundred delegates within a relatively short registration period. Since delegates could be assumed to have their own computers, a wireless network was provided throughout the conference area and a sheet giving details of the supported SSIDs and locations, and the policies applicable to the network, was provided in every delegate pack.

Authentication via eduroam (see section 4.6 below) permitted those delegates able to use eduroam to obtain Janet and Internet connectivity without further assistance. For others, a separate registration desk issued unique usernames and passwords that were valid until the end of the conference. Delegates had to show their conference badge to obtain credentials and the username issued was recorded on a copy of the full delegate list to enable the host organisation to manage and contact individuals should this prove necessary. By requesting credentials the delegate was taken to have agreed to abide by the network policies. [Depending on how delegate packs are assembled it might be possible for these to include individual credentials for every delegate; however this increases the likelihood that unwanted credentials will be left lying around and does not give the positive confirmation that the delegate agrees to the policies.] Users of these credentials connected to a specific ‘conference’ SSID and entered their credentials into a web page that appeared the first time they started a web browser each day. Some rooms were shared between the conference and the organisation’s normal teaching activities. In these places VLANs were used to route traffic using the conference SSIDs from the access points back to the dedicated controller used for the conference. This controller provided traffic monitoring information that was available to the organisation’s network management and incident response staff.

Due to the nature of the conference and the fact that individual users could be traced it was not considered necessary to impose any port restrictions or bandwidth management between the conference and the Internet, though the total bandwidth assigned to the conference controller was limited to ensure that the organisation’s normal business was not affected by congestion on its access link. The conference facilities did not provide direct access to the organisation’s LAN – local users could either connect to external-facing services or else use one of the access points that offered the organisation’s internal SSID.

Since delegates were to be issued with public IP addresses it was important to ensure that sufficient of these were allocated to the conference DHCP server. Organisations concerned about this issue should contact the Janet Service Desk.

4.4 Open Day Guests

Universities and colleges often hold open days, where those considering applying to be students can visit the site and obtain information and experiences to help them make their choice of institution and course. Since open day guests are "visiting for purposes associated with the [organisation's] missions", the Janet Eligibility Policy permits the host organisation to provide them with network access during their visit, if it wishes. Such access must, however, be limited to those attending the open day and not be available to other members of the public.

One university chose to offer a dedicated wireless network for guests to connect their own mobile devices. The short duration of the visit, and the limited scope for contacting guests after the open day, meant that using a single account for all guests was considered an acceptable risk. This did, however, mean that if a serious problem were to occur there would be no option but to disable access for all visitors, since individual users could not be distinguished. Traffic on the network was monitored for signs of problems.

To ensure that only open day guests were able to access the network, the username and password were included in the documentation provided to those attending. Information about acceptable use could either be included in the same pack, or linked from the web page where users had to log in. The account and password were deleted at the end of the day, and new credentials provided for each subsequent open day.

Since the security status of guests' devices is unknown, the wireless network should be configured to reduce the likelihood of them becoming infected or infecting others. In particular the guest wireless network should not give access to the internal LAN, and any systems to which guests may gain access should presume that the connecting devices are insecure. There may also be an expectation that any internet access provided will be filtered. Devices that return to the area after the open day will continue to make unsuccessful connection attempts using the expired password, so it may be worth changing the open day SSID occasionally to reduce the load of these failed connection attempts.

4.5 Sponsored Guests

Where the requirement is to support individual guests, such as research collaborators, who are visiting particular members of staff it may be effective to permit those staff to authorise their guest’s access to the network. The host (sponsor) can be made responsible for informing the guest of the policies that apply and for ensuring good behaviour. As discussed above, guests should be given their own credentials so that they do not gain unintended access to the host’s information or resources, but it is helpful to retain a record of the link between them. A wide variety of solutions can be used, depending on the number of guests and sponsors that need to be supported and what facilities can be provided by the organisation’s user management systems.

4.5.1 Paper-based Registration

One of the simplest ways to issue credentials to guests is as a sheet of paper containing a temporary username and password.

One organisation keeps a stock of these in envelopes at each of its helpdesks. Local sponsors can either accompany their guest to a helpdesk and prove their identity by showing their staff ID card, or else write in advance to the helpdesk informing them how the guest can be identified. The guest is issued with a sealed envelope containing the password and the Acceptable Use Policy (with the username written on the outside). The guest signs a record to confirm their agreement to abide by the policy. The sponsor’s identity, the username and the date on which it was issued are also recorded. The guest can then login and gain access to the network but not, because of restrictions on the accounts, to any facilities or servers.

Since this facility is only intended for short-term guests, the username is only valid for the week in which it is issued and the user cannot change the password. After the username expires, a new password is generated and the username becomes available for reissue. Envelopes are generated centrally, by authorised staff in a secure location, as required to maintain an appropriate level of stock at each helpdesk location. Sponsors are expected to give advance notice of requests for an unusual number of guests to ensure that sufficient envelopes are available.

4.5.2 Online Registration

Many organisations use a separate controller to authenticate access to their wireless network. When a new device connects to the network it is first re-directed to a login page where the user must enter valid credentials to obtain further network connectivity. If the controller can use external sources to validate these credentials then this provides a way to support both local and guest users.

One organisation has configured its wireless controller to use LDAP queries against different databases for local and guest users. Local usernames are checked against the central Windows directory whilst guests are checked against their own dedicated LDAP server. This has the advantage that granting guests access to the wireless network cannot inadvertently give them access to other services since they never appear in the central directory. To create a guest account a local sponsor logs into a web page that is protected using the central authentication system (this prevents guests creating further accounts once they are registered) and requests the creation of a guest account. The link between the sponsor and the guest account is recorded at this stage. The system generates and returns to the sponsor a username and a one-time access code, which they give to their guest, at the same time informing the guest of the applicable policies. Where a sponsor has several guests (for example for a seminar) the system allows multiple accounts to be created at once. Guests then connect to the wireless network and login with a fixed username that gives access only to a single page where they enter their username and access code. The access code is immediately disabled (this additional step prevents the sponsor, or other guests, from knowing the guest’s password). Guests are then invited to choose a password and their account is enabled immediately, allowing them to login and obtain access to Janet and the Internet. Guest accounts have a maximum lifetime of a fortnight but this may be reduced if the sponsor wishes.

By allowing guest accounts to be created online by any member of staff and used immediately this system supports even short-term guests who may be on site for only a few hours, without overloading the central helpdesk. At the same time there is a clear record of responsibility for the guest and the temporary credentials are only known to their intended user. Although it would be possible to restrict the ability to create accounts by applying additional authorisation rules on the registration website, this has not proved necessary.

4.5.3 Identity Management

Where an organisation has an Identity Management System that supports delegation of identity creation, this can be used to allow authorised staff to create accounts for their, or their department’s, guests.

For example one organisation’s Identity Management system assigns user accounts to particular groups (e.g. by department) with the default access rights to servers, file store etc. for the user being set by the group to which they are assigned. The system may also allow these defaults to be altered for particular users, within defined limits. Authorised account administrators are allowed to create user accounts within particular departmental groups; the system then automatically generates appropriate instructions for the administrator and the user (for example details of applicable Policies for the user and an instruction to the administrator to ensure these are read and agreed to), and keeps a record of which administrator created which account. As well as departmental groups, the system can support a number of visitor groups in which designated administrators can create new users using the same web-based interface.

The access rights for guest users are set centrally by the Identity Management system but the account administrator can modify some parameters, for example to match the lifetime of the username to the duration of the guest’s expected visits. Care is needed in setting up the initial defaults, and the extent to which they can be modified, to ensure that guests do not gain unintended access to services or information. However this only has to be done once for each type of guest, not every time a guest requests access. Since all users are created though the same system, there is complete flexibility to support anything from temporary guests who only require Internet access for an afternoon to research partners who may visit many times over an extended period, and have similar access rights as the organisation’s own staff to facilities such as filestore and backup.

4.6 Device Authentication

Despite the problems identified in section 3.3 above with authenticating a guest’s device using its MAC address, one organisation has found this a useful technique for supporting mobile devices, such as PDAs, that can connect to wireless networks but do not support the encryption protocols needed to securely exchange usernames and passwords.

A special SSID is provided for these devices to use. This only provides limited access to the Internet, thereby both reducing the damage that can be caused by misuse and encouraging those whose devices can support secure authentication protocols to choose the alternative access methods, such as eduroam (see section 4.7), that the organisation provides for them.

Before the device is granted access, its MAC address must be registered through a web form which is only accessible to someone with a local username and password. Typically this will be the guest’s host or sponsor, though students are also allowed to register a single MAC address for their own personal device. A record is kept of which sponsors registered which MAC addresses, and sponsors are responsible for informing guests of the relevant

Acceptable Use Policy and for ensuring that they comply with it. Sponsors can set the duration for which the registration is valid; the fact that they remain responsible for use of it encourages them to reduce the risk of impersonation attacks by keeping this as short as possible. Finally, since wireless access is typically hard-wired into these devices, rather than being on easily exchangeable cards, the risk of a registration being accidentally transferred between devices (and owners) is reduced.

4.7 Frequent Guests

Many of the guests at Janet-connected organisations will come from other educational organisations. In the physical world it is common for universities and colleges to welcome research or teaching collaborators, or simply to make their facilities available to students living locally during vacations. Many of these guests have a common requirement to be able to connect across Janet to online facilities provided by their 'home' organisation and elsewhere on the Internet. The eduroam service, and the international eduroam® federation of which it is part, have been designed to support this requirement: the goal being to permit members of one educational organisation to obtain Internet access at other organisations while managing the risks to both organisations and reducing as far as possible the 'per-guest' effort required of both.

The eduroam service defines both policy and technical controls to reduce the risks of misuse. To use the eduroam facility at the organisation where they are a guest, users log in with their credentials from the Janet-connected organisation where they are a member. The credentials are passed over an encrypted tunnel from the user's computer to their home site's authentication server so that neither the visited site nor the network can see them; indeed neither know the identity of a particular user, just the home site to which they belong. By authenticating the user, the home site agrees under the eduroam Policy that they will support the user and investigate and deal with any complaints relating to their use. The eduroam Policy makes users subject to the Acceptable Use Policies of both their home site and the organisation where they are guests.

The eduroam Policy allows the visited site to place technical restrictions on the network access that it provides to guests authenticated through eduroam. In particular, the visited site need not provide these guests with any access to its Local Area Network if it does not wish to. However, to ensure that guests can access services provided by their home organisations there is a minimum set of ports that guests must be allowed to connect to and from Janet and the Internet. These permit web browsing, file transfer, e-mail, terminal server and VPN access, which should be all that the majority of guests require. These rules are defined in the eduroam Technical Specification and the security aspects explained in the factsheet 'Janet eduroam Security Measures' (PB/INFO/067). In order to offer an eduroam guest service an organisation needs to provide the ability to connect (usually by wireless, although wired access is also possible) to a network segment that uses IEEE 802.1X access control, with authentication requests passed to a RADIUS proxy. If the organisation does not require access to the service for its own users, this proxy can simply route all requests to the eduroam National RADIUS Proxy; otherwise it should route local usernames to a local authentication server. When allocating IP addresses to guests, organisations are recommended to use a separate address range.

An organisation that wishes to allow its own users to access eduroam facilities at other organisations needs to provide a RADIUS authentication service for them and to permit access to this from the eduroam National RADIUS Proxies. Once these facilities are set up, there should be no per-user support requirement for either the home or visitor organisation unless a user breaches the Acceptable Use Policy. Thanks to the link with the eduroam® federation, guests from eduroam® member organisations in other countries can be supported with the same facilities.

The eduroam service is recognised by the standard SSID ‘eduroam’. The eduroam(UK) Technical Specification also allows visited organisations to advertise different technical facilities (including IPv6 support and different levels of wireless encryption) using SSIDs to indicate which tier of the eduroam definition is provided). A number of case studies giving technical details of eduroam visitor and home facilities have been written and can be found on the eduroam web pages.

4.8 Wireless Access for Visitors

A number of commercial hotspot providers offer products to make their services available through other organisations’ wireless access points. These typically use a small router, installed on site, to establish a VPN tunnel back over whatever connectivity is available to the provider’s central authentication and Internet routing systems. For a small deployment, the wireless access point may be part of the router but in most cases some or all of the organisation’s own access points are configured to offer the provider’s SSID and to place any traffic for that SSID into a VLAN connecting to the router. Provided such systems satisfy the requirements of the Janet Eligibility Policy (discussed in s2.3 of this guide), in particular that the VPN is encrypted, then the VPN tunnel may be backhauled over Janet between the organisation and its hotspot provider. Depending on individual circumstances this may be easier to manage than using a dedicated link for the backhaul, or may provide more bandwidth or lower cost. A number of different commercial models appear to be available for wireless access: the cost may be met fully by users buying subscriptions or one-off payments, the organisation may pay a subscription, or there may be an intermediate model such as a short free period per device with the user paying for an extended connection periods.

If an organisation wishes to partner with a public internet access provider that does not offer backhauled wireless as a standard product, the same effect may be achieved using a pair of standard routers with appropriate configurations, one on the organisation’s network and one on that of the partner network provider, with the encrypted tunnel between them passing over Janet or any other appropriate network.

Note that in either case the tunnel, the routers and the VLANs connecting them to the wireless access points are likely to be classed as part of the public network, and must be operated according to the legal standards and obligations for such networks. These differ, including having higher penalties, from the law for private networks such as Janet.

4.9 Guests and Visitors

Finally, it is possible to combine network access for local users, guests and visitors into a single wireless network facility. One organisation entered into an agreement with a commercial wireless ISP to share access points around a city centre campus, thereby increasing the coverage of both the educational and commercial wireless networks. The access points are connected together by a network segment with access both to the organisation’s routers (for connections to Janet and the organisational LAN) and, via a dedicated backhaul link, to the commercial network’s servers and Internet connection.

All access points offer three different SSIDs, linked by VLANs to eduroam®, organisational and commercial services. The eduroam SSID uses the normal eduroam IEEE802.1X configuration to permit users from other education organisations to authenticate with their home credentials and obtain a connection to Janet and its Internet links. For conferences the same RADIUS proxy can be used to authenticate against a pool of temporary accounts for either 802.1X or web portal access. The commercial and organisational SSIDs each display web portal pages, protected by SSL, which appear as soon as the user starts their web browser. The commercial portal, hosted on the company’s servers and reached via the dedicated link, provides the usual options to login using an existing account or scratch card, or to buy connection time with a credit card, and then provides access to the commercial Internet. The organisation web portal allows users to select either a local login or re-direction to the commercial service. Users with a login to the organisation can enter their credentials and gain access to the organisation’s LAN.

A particularly interesting aspect of this installation is that different port filtering rules are applied to each of the routes off the wireless access segment. The commercial ISP, once a user has been identified and has paid for access, provides a relatively open Internet connection; eduroam applies the usual Janet eduroam port filters, as appropriate for the intended purpose of allowing guests to contact their home organisation; and the LAN connection for local users only permits ports associated with encrypted protocols (SSL, VPN, IMAPs, etc.) to reduce the risk that users will accidentally transmit their local username and password across an unencrypted wireless connection.

Source URL: https://community-stg.jisc.ac.uk/library/janet-policies/case-studies

Links
[1] https://community.ja.net/library/janet-policies/network-access-guests-technical-guide