

# Guest and Public Network Access

This factsheet suggests some ways for organisations that wish to provide guest and/or public network access for external visitors to do so.

The purpose of the JANET network is to support education and research in the UK. Education and research organisations connect to the network and may make it available to their own staff, students and pupils, as well as to individuals visiting the organisation for educational or research purposes (including for academic conferences). This last group, referred to in this factsheet as **guests**, may come from other JANET-connected organisations or elsewhere.

Within the overall limits of this userbase, each connected organisation can decide as a matter of local policy what level(s) of access to JANET it provides and to whom. The JANET Security Policy requires organisations to have appropriate measures in place for giving, controlling and accounting for access to JANET. This normally involves each local or guest user having their own unique username and password (see the JANET factsheet on User Authentication<sup>1</sup>). However, some educational organisations may wish to provide Internet connections, for a fee or free of charge, to members of the public who are not guests of the organisation (for example delegates at commercial conferences, or members of the public using accommodation or other facilities or simply walking across the campus). The Terms for Provision of the JANET service and the status of JANET as a private network prohibit the use of JANET to connect these users (referred to in this factsheet as **public users**) to the Internet. An alternative method of connection must be provided for them.

## Providing Guest Access

The simplest and safest way to provide access for guests from other educational organisations in the UK and abroad is to join JANET Roaming<sup>2</sup> as a visited organisation. JANET Roaming provides a link between organisations so that a guest from another JANET Roaming member (or a member of the international eduroam federation<sup>3</sup>) can use their home organisation username and password to authenticate to a guest network provided by the visited site. That network must provide access to JANET but need not give any access to local services. By providing a JANET Roaming visitor facility, an organisation knows that visitors who use it are current members, in good standing, of another educational organisation and, because that home organisation is bound by the JANET Roaming Policy, that it will take responsibility for its user's actions (including, if necessary, investigating and punishing any reported misuse of the visitor network facility or JANET).

Where a guest does not come from a JANET Roaming or eduroam member organisation, a facility for creating temporary local accounts may be required. A number of JANET organisations allow authorised members of staff to assign short-lived accounts to visitors to their departments: these staff members are responsible for ensuring that the guest complies with local and JANET policy requirements. This system relies heavily on the sponsor and their personal knowledge of the guest, since the guarantees provided by JANET Roaming are not available. Many mechanisms can be used to assign such accounts, from an option in an identity management system to pre-prepared sealed envelopes or scratch cards that each contain one visitor username and password.

The JANET Security Policy<sup>4</sup> requirement to control access to JANET means that it is not

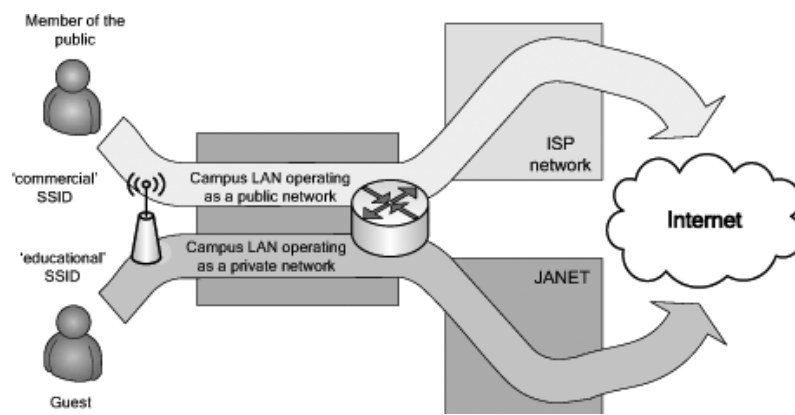
- 1 <http://www.ja.net/services/publications/factsheets/041-user-authentication.pdf>
- 2 Described in detail at <http://www.ja.net/services/network-services/roaming/>
- 3 For more information, see <http://www.eduroam.org>
- 4 <http://www.ja.net/services/publications/policy/security-policy.pdf>

appropriate simply to provide guests with access to an unauthenticated network port or open wireless network. It is also inadvisable to allow a local user to log the guest on using their own credentials since this is likely to give the guest far more access to local systems and to JANET than was intended. Similarly, if the organisation does not provide a separate segment or VLAN for guests then care will be needed to ensure that guests do not gain unintended access to internal or licensed resources which may trust IP addresses for authorisation.

## Providing Public Access

If an organisation wishes to provide Internet access to members of the public who are on its premises other than as guests then the JANET network cannot be used to do so.

Organisations (and Regional Network Operators) that provide public Internet access have made various arrangements with commercial ISPs to provide the necessary connections. In some cases this has been achieved by allowing the ISP to install their own separate equipment on the premises; more usually, the existing wireless LAN infrastructure has been shared with the ISP and a dedicated link provided to their network.



In a typical installation of the latter kind, wireless access points are configured to broadcast at least two different SSIDs (Service Set Identifiers). Guest users connect to the 'education' SSID (often the JANET Roaming standard SSID 'eduroam'), are presented with a JANET Roaming login dialogue, and authenticate with their local or JANET Roaming credentials. Their traffic is then routed via JANET. Public users connect to the 'commercial' SSID, are invited to enter their subscription or credit card details and are connected to the Internet via the commercial ISP. Each SSID is associated with a VLAN that logically segregates the traffic and routes it to the appropriate upstream connectivity, JANET or commercial ISP.

Organisations considering such partnerships should note that any network that offers Internet access to the public is likely to be classified in law as a **public** network, whereas JANET and the networks of its customers are generally classified as **private**. Operating a public network is likely to involve more onerous duties, for example:

- protection of the privacy of users (*Regulation of Investigatory Powers Act 2000* and *Privacy and Electronic Communications (EC Directive) Regulations 2003*)
- provision of information to users (*Communications Act 2003*) and
- (possibly in the future) retention of data about usage for criminal investigations (*Anti-Terrorism, Crime and Security Act 2001* and the *European Data Retention Directive 2006/24/EC*).

It seems likely that these obligations would only apply to those parts of the network that actually carry public traffic, so segregating this traffic either logically or physically should allow the rest of the organisation's LAN to continue to operate on a private network basis. **Organisations should seek individual legal advice on the implications for their own networks.**

The privacy-related duties of a public network provider are likely to apply to both the organisation and the ISP. Responsibility for compliance with other laws and policies should be assigned by contract between the organisation and the ISP.