Router security

- Simple Network Management Protocol
- Web-based Interfaces

Even if routers are only being used to transfer IP traffic, it is imperative that their security is not compromised. If intruders manage to obtain control of a router or firewall then they will be able to remove (temporarily or permanently) any traffic management rules used to protect the network. They may also be able to read or re-direct any traffic passing through the device, or simply to create havoc by breaking the organisation's local and wide area connections.

Most network devices can now be managed remotely across the network. This is normally done using the Telnet protocol but others may also be used. Whatever protocol is used, it is essential that the ability to login, and hence configure the device, is protected by at least a password. Some routers, such as those made by Cisco®, have two levels of privilege, each protected by a separate password. The lower level gives access to 'read only' functions, the higher to 'read/ write' functions. Both levels must be adequately protected via passwords and these passwords should be chosen and managed with at least as much care as any other passwords for privileged accounts on other IT facilities.

If a router can be managed over a network connection, it is possible for hostile attackers to try to access the management function, just as legitimate administrators would. Such attacks may come from inside or outside the organisation. Wherever possible, the router should be set to refuse connection requests that do not come from pre-configured IP addresses. These should normally be addresses within the organisation, since other filtering rules should already restrict the ability to forge them. If there is a requirement to manage network devices from outside the network, then additional security measures such as encryption (described in the following sections) should be considered.

Many routers and other devices also allow management to be carried out using other protocols. Most of these allow aspects of the devices' configuration and logging to be read remotely. Some also allow management parameters to be set. The most common protocols used are SNMP and HTTP.

Simple Network Management Protocol

This has an authentication mechanism that uses 'community strings'. In effect these are passwords, so they should only be known to the controlled device and those who are authorised to control it. Different community strings may be used for different groups of management functions. Anyone who can learn or guess a community string can gain access to the management functions on the device. Many network devices are delivered with default community strings. These should always be changed when a new device is installed and should be managed in the same way as any other privileged password.

Each SNMP request sent over the network includes the community string as authorisation.

Although newer versions of the protocol make it possible to encrypt the community string, this is not yet widely supported, so there is a risk that the community string will be intercepted. Unless encrypted community strings can be used, it is recommended that network devices are configured to ensure that SNMP can only be used to read information and not to update it.

Web-based Interfaces

Similar considerations apply to web-based interfaces to network devices. Like SNMP, these transmit unencrypted passwords to authorise changes to the configuration of the device. Web browsers use the SSL protocol to provide encrypted communications, but unless the network device also supports this, it cannot be used.

Routers and firewalls are a critical part of an organisation's network infrastructure and are therefore an obvious target for attackers wishing to cause disruption. The systems used to manage the routers should therefore be designed to ensure the best possible security. The protocols through which a device can be managed should be known and controlled so that, if possible, management requests will only be accepted from fixed IP addresses. Protocols that will not be used should be disabled. Furthermore, if management commands are to be sent across untrusted networks (which may well include the organisation's own LAN) then any systems available should be used to prevent the communication being intercepted. Each of the common protocols has the possibility of encryption - SSH protocol in place of Telnet, SNMP version 3, SSL for web interfaces - and these should be chosen whenever possible.

Enquiries about the security aspects of setting up an access router may be directed to Janet CSIRT [1] or the Janet Service Desk [2]. FE colleges may also contact their JISC RSC [3] for advice.

Links
[1] http://community.ja.net/library/janet-services-documentation/janet-csirt
[2] mailto:service@ja.net
[3] http://www.jisc.ac.uk/whatwedo/services/as_rsc/rsc_home/rscs_contact.aspx