Routers

Routers are network devices that forward packets of data between different networks. A router between an organisation's LAN and JANET will not have a direct connection to every other router on the Internet. It is however possible to set up that router to forward packets to their destinations by the most efficient path. The router does this by referring to its routing tables, which list all the possible paths that data can take to get from source to destination IP address. Each router on the path repeats this process until the data reaches its final destination.

Routers permit each connected network to maintain its independent identity and IP address and can also facilitate the implementation of security procedures. It is possible for example to control access to a network from the outside world by using packet filtering (see Appendix 9).

Access Routers at JANET Sites

Customers are expected to have an on-site IP router to connect their LAN to JANET. The choice of router will be determined by the capacity of the access link and the organisation's specific requirements. Organisations requiring informal advice on router products that have been successfully used by other sites on JANET should contact the JANET Service Desk for assistance.

The majority of FE colleges connecting to JANET under recent Government initiatives were supplied with a router as part of their new connection package. The JISC RSCs configured most of their routers and assisted in bringing their connections into operation.

As part of the process of setting up the router, customers need to select a suitable link-level protocol to carry IP traffic over the access link between their router and the router on the JANET core. The process of routing across the access link is sometimes referred to as encapsulation. Two link-level protocols are supported for an IP connection across JANET:

- PPP (Point to Point Protocol)
- HDLC (High Level Data Link Control).
- All organisations connecting to JANET are required to confirm which method of encapsulation will be used, by completing the appropriate section of the JCUR form.

Additional information about setting up a router may be found in Appendix 10.

Interfa?ces

The customer's access router needs a suitable WAN interface to connect to the JANET access link. If the bandwidth of an organisation's connection is 2Mbit/s or less, the PTO will normally present the leased line at the site's NTU with an X.21 DCE interface. Most routers are compatible with this type of interface and it should be possible to connect the circuit interface to the access router with an X.21 cable.

If it is not possible for the PTO to deliver a 2Mbit/s connection with an X.21 interface, the leased line will be presented at the NTU with a G.703 interface. This type of interface may also be used for 34Mbit/s connections. In these circumstances however, it will be necessary to install a DSU converter between the G.703 interface and the interface on the access router (for further information, see Appendix 11).

Organisations requiring a DSU will be supplied with a recommended box and a pair of three metre coax cables to connect it to the telecommunications termination point. If longer cables are required, the installation contact should give the JANET Service Desk prior notice of the length needed. The connecting organisation is responsible for the provision of an X.21 cable to connect its routing equipment to the DSU. The cost of the DSU and cables may be included in the connection package or charged separately, depending on the funding arrangements for the connection.

Once the connection is operational, the DSU becomes the property of the connecting organisation, which then assumes responsibility for arranging suitable maintenance cover for the DSU and cable. If there are any faults on the DSU or cable after it has been installed, the organisation is responsible for any repairs.

However, for FE colleges the DSU maintenance arrangements may vary. The organisation responsible for maintaining the site router is usually also responsible for maintaining the DSU.

It is acceptable for a connecting organisation to purchase and install a DSU on-site. However, the DSU must match the unit installed at the Janet Point of Presence and the organisation must also purchase all of the cables required. The Janet Service Desk can provide details of recommended DSU equipment for use on Janet.

Additional information about interfaces may be obtained via the Janet Service Desk. FE and specialist colleges may consult their JISC RSC if they require further advice.

Router Setup and the Janet Netsight Service

Organisations that have received assistance from contractors in setting up their access router should be aware of the requirements of the Janet Netsight network monitoring system. In order to monitor access links, the Janet NOC and the RNOs need to ping the IP address of the router interface that supports the customer's access link. A small number of sites have in the past set up routers that do not respond to pings. Please note that if a site router is set up in this way, there will be problems in providing the link status and traffic statistics via Netsight. There may also be time delays in identifying faults on these access links.

Janet and the RNOs will be happy to discuss which IP addresses should be allowed to ping a site access router. Please contact the Janet Service Desk for further information. FE and specialist colleges may initially seek advice from their JISC RSC.

Ownership and Maintenance of Routers

Some Janet sites own the router that connects their LAN to the Janet access link. In this case they are also responsible for the management and configuration of these routers and for maintenance arrangements.

There are, however, a large number of FE colleges whose router was supplied and is owned by Janet. In these circumstances the router is covered by a Janet maintenance contract. Most of these sites also receive assistance in supporting their access router from their JISC RSC or RNO. Janet informs the RSC of the fault reporting number for router problems; the RSC decides whether or not to pass the number on, depending on the level of support they provide to colleges.

Router maintenance includes both hardware and software support. The manufacturer Cisco® periodically releases newer IOS images with bug fixes and/or new features. Upgrading a router's software should result in improved system performance and reliability.

Reconfiguring a Site Access Router

Please note that reconfiguration of a router should only be undertaken by experienced technical staff. The site network may become inaccessible to the outside world or the equipment may be badly damaged if a mistake is made. It is also possible that the maintenance contract may be invalidated. Please contact the Janet Service Desk if it is not clear who should be responsible for making changes to a configuration of a site access router after the site's JANET connection has been brought into service.

Janet Managed Router Service

Janet provides a Managed Router Service for organisations connected to the network, under which the site access router is monitored and managed as part of the Janet service. Janet's contractor undertakes all fault diagnosis and resolution work on these routers, either remotely or by an engineer visiting the site. Maintenance of the hardware is also included as part of the service. Maintenance of routers provided to FE colleges by Janet through the RSCs is available as a chargeable, opt-in service. Further information is available at http://www.ja.net/products-services/janet-connect/managed-router-service [1].

Router Security

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 or the JANET Service Desk. FE colleges may also contact their JISC RSC for advice.

Further information is available in Section 7: Security.

Links
[1] http://www.ja.net/products-services/janet-connect/managed-router-service