Blocking LAN service ports

Some ports have historically been associated with security vulnerabilities, but see little legitimate use on a WAN or the general Internet. They present a risk to your network and little to no legitimate use is prevented by blocking them. If your network is partitioned with one or more firewalls so that different parts support different functions or groups of users, you should consider applying the same restrictions at the firewalls between them.

The LAN service ports

There is nothing intrinsically wrong with the services assigned to these ports. Historically, however, many worm and virus programs have exploited vulnerabilities in the services and it is common for worm and virus software to scan address ranges for a vulnerable listener as part of their mechanism for propagation. Eight years since it's release we still see traffic on 1433/udp from SQL Slammer infections.

- **Port 135 RPC endpoint mapper**

  TCP port 135 and UDP port 135 are reserved for the service which enables the low-level Remote Procedure Call facility to register each available procedure and invoke it when appropriate.
  Windows LAN applications make heavy use of RPC; on other platforms it is not generally enabled by default.

- **Port 137 NetBIOS name service**

  TCP port 137 and UDP port 137 are reserved for the service which translates between IP addresses and Windows NetBIOS names in a LAN.

- **Port 139 NetBIOS session service**

  TCP port 139 and UDP port 139 are reserved for the connection-based transport underlying most Windows LAN applications such as those using SMB.

- **Port 161/udp SNMP**

  SNMP is commonly used for the querying, management and configuration of network devices. We frequently see scanning on this port caused by misconfiguration network discovery applications, typically when an address range is entered incorrectly. These

probes can be a source of alarm to neighbouring network operators even though there may be no malicious intent. Please consider blocking this port, creating exceptions to this rule for known remote hosts that need to be queried.

- **Port 445 SMB**

  TCP port 445 is reserved for the Microsoft Server Message Block protocol underlying current file sharing and messaging applications.
  The name of the service is “Microsoft-DS”, reflecting an earlier use for Windows Directory service. UDP port 445 is reserved for the same thing.

- **Ports 1025 and 1026 Active Directory logon and directory replication**

  One of ports 1025 and 1026, both TCP and UDP, will normally be chosen for Active Directory support within the LAN. Port 1026, both TCP and UDP, is registered for Calendar Access, and the UDP port is often available to Windows Messenger.
  Actual intrusions through these ports seem not to be common in Janet, but they are the focus for considerable scanning activity.

- **Ports 1433 and 1434 SQL Server**

  Ports 1433 and 1434, both TCP and UDP, are reserved for the Microsoft SQL Server product; but abuse is not limited to systems that have MS-SQL installed.
  At the time of writing the ports most commonly used by worm and virus software are TCP port 1433 and UDP port 1434

Impact of blocking

Most of the ports are usually associated with Windows applications. They appeal to writers of worms and viruses because of the wide deployment of Windows in environments where little or no expertise is available in system administration or network security. Any vulnerability is certain to remain for some time on a large number of computers, which become the prime target for malicious software.

The services using these ports are not designed to be used across a Wide Area Network or between management domains, particularly over paths including Janet or the public Internet; so blocking the ports will have no impact on properly designed applications. A few older applications may depend on the LAN services; they should be updated or replaced.

It is in the interest of Janet and all Internet providers and users that you do not support the spread of these kinds of abuse from your network to others.
Please remember, though, that the immediate benefit to your own network of blocking these ports is limited. Your systems will no longer be exposed to some classes of abuse directly from the Internet, but the same worms and viruses may still be introduced to your network in other ways; for instance, through e-mail or a laptop connected to your network after being compromised elsewhere. You will still need to keep each individual computer fully patched

and managed.

Configuring your firewall

It is not practicable to give specimen configuration instructions for the range of packet filtering devices deployed in Janet organizations. Specific details may also depend on what is already configured, and to some extent on the nature of the organization’s network.

If you operate with a “default deny” policy you need only check that none of these ports are mentioned as exceptions to the policy.

Log information

A side effect of blocking traffic for these ports is that when worm or virus infection does occur your firewall or router will log events (packets or connection attempts) that conflict with the blocking rules; you will then be able to spot rogue computers in your network with virus or worm infections as soon as they start scanning.

Again, specific details vary widely between available products.
