

Network Protocol Configuration

This document contains the following sections:

- [Introduction](#)
- [DHCP Servers](#)
- [IP Routing](#)
- [Virtual Hosting](#)
- [Running an SAP Agent](#)
- [Microsoft Protocols and Services](#)
 - o [Running Your Own Windows Domain](#)

For information related to this topic refer to:

- [Network Bridging \(http://www.cmu.edu/computingdoc/network/bridge/index.html\)](http://www.cmu.edu/computingdoc/network/bridge/index.html)
- [Network Protocol Guideline \(http://www.cmu.edu/computingguideline/network.html\)](http://www.cmu.edu/computingguideline/network.html)

Last Updated: 2/14/08

Introduction

This document describes a collection of network services and protocols that may cause network problems at Carnegie Mellon. In some cases, the protocol or service has potential to be so harmful that it has been banned from use on campus. This document also provides information to assure that your machine does not inadvertently perform a specific function. To preserve the integrity of our network, a host that is using or offering one of these prohibited services may be removed from the network immediately.

Last Updated: 2/14/08

DHCP Servers

The Carnegie Mellon Network Group offers Dynamic Host Configuration Protocol (DHCP) service for all computers on our campus network. This service provides a variety of functionality and is required for some machines to work properly.

If you need to register a machine, you may use our [online registration service \(http://netreg.net.cmu.edu/\)](http://netreg.net.cmu.edu/).

Running your own DHCP service for any reason anywhere on our network is prohibited. If a rogue DHCP server is located, the machine will be removed from the network, and (if registered) its owner contacted.

A rogue DHCP server may hand out incorrect information to booting machines, and any machine that listens to this rogue DHCP server's offers will not function correctly. As this will cause users with properly configured machines to lose all network connectivity, running a DHCP server of your own is **banned**. To be sure that you do NOT accidentally turn on this service when installing the operating system:

Windows XP: Do NOT enable Internet Connection Sharing (i.e., Network Bridging) while connected to the campus network. Also, do NOT install the Microsoft DHCP Server or DHCP Relay Agent network services.

Mac OS X: Do NOT enable Internet Connection Sharing while connected to the campus network.

Linux / UNIX: Do NOT install DHCP server packages. Most distributions include a DHCP client, which you are encouraged to use.

Last Updated: 2/14/08

IP Routing

Some operating systems offer the ability to act as a router and forward IP packets from one network interface to another based on its internal routing tables. No machines on campus should have a need to do this. Because of this, IP Routing is **banned**.

If a machine is configured to route IP packets from one interface to another and both are on the same physical network, the packets will appear on the wire twice. As a result, ARP caches may become corrupt because two possible interfaces have received packets for one host.

When hosts are incorrectly configured as routers, information is disseminated incorrectly. In order to advertise which networks are available on other interfaces, the host must send route advertisements in one format or another. These advertisements may impair the real routers from receiving information or may cause them to advertise the incorrect routes. To be sure that you do NOT configure your operating system for IP routing:

Windows XP: Do NOT enable Internet Connection Sharing (Network Bridging).

Mac OS X: Do NOT enable Internet Connection Sharing while connected to the campus network.

Last Updated: 2/14/08

Virtual Hosting via Multiple IP Addresses

Users may sometimes have a network host that will serve WWW data for multiple virtual sites. These sites may have different hostnames (www.cmu.edu, www.mit.edu) that are short and easy to remember. Carnegie Mellon does not provide multiple IP addresses to hosts. If this functionality is needed, the host may be setup with multiple valid hostnames.

To establish a host with multiple valid hostnames, consider these tips:

- The host may have two separate hostnames, and the web server is smart enough to determine which hostname was used, or the host may have two separate hostnames which point to two separate IP addresses, which the web server uses to determine what the request was for.
- Linux users should not configure "Networking options: Network aliasing: IP: aliasing support." Aliasing support is not permitted on the campus network.

Last Updated: 2/14/08

Running an SAP Agent

Service Advertising Protocol (SAP) broadcasts tell other hosts on a subnet which services are available. Typically sent by NetWare servers, these broadcasts occur approximately every 60 seconds. Other hosts on the network listen for them, and use the information provided.

If a host that is advertising services via SAP disappears, clients that were using this information may have problems. To be sure that you do NOT configure your operating system for SAP:

Windows XP: These Operating Systems do not utilize SAP in a harmful way.

Linux: Do NOT install mars_nwe or ipxsapd.

Last Updated: 2/14/08

Microsoft Protocols and Services

These services are only available on Microsoft operating systems. However, as they could cause problems for other Microsoft users, they are listed here to inform you of what you should and should not use.

Running Your Own Windows Domain

Due to a shortcoming in the Microsoft implementation of NetBIOS name lookups, running your own domain can cause additional network traffic for no real reason. When a user selects a domain to browse (i.e., "CAMPUS"), the client asks the local browse master for information on this new domain. If all domain controllers for the domain are unavailable, the client begins to send subnet broadcasts and malformed DNS requests looking for the domain controllers. After performing these lookups numerous times, it finally gives up and times out.

Because of the additional network load that can be created, the Network Group requires all Windows domains to be supported by at least two (2) domain controllers. This way, if one fails, another is there to back it up. These domain controllers must be available 24 hours a day. If one of the domain controllers is down for an extended period of time, we strongly suggest bringing another one up until the original is operational again.

As long as there are at least two domain controllers, a Windows domain should cause no additional traffic on our network.

Last Updated: 2/14/08