

NYU-NET Operational Principles

Network Operations Center (NOC)

Information Technology Services, New York University

Version 1.1, December 1, 1998

Version 1.2, November 8, 2002

The following statements express many of the fundamental principles governing the day-to-day operation and configuration of NYU-NET as managed by the university's central Network Operations Center (NOC).

These principles are followed so as to maintain the smooth and reliable operation of NYU-NET through careful adherence to widely-recognized, industry-standard approaches.

Network configuration and management at the school or departmental level must be performed in conformance with these principles.

If a topic of interest is not mentioned explicitly below, the NOC staff at noc@nyu.edu should be consulted.

Network Infrastructure

Equipment

The purchase and/or installation of data network and communications infrastructure equipment—such as hubs, switches, repeaters, wireless networking equipment, bridges and routers—must be done in consultation with the central NOC.

Wiring

Fiber-optic or twisted-pair copper network cabling, including data jacks and telecommunications closet terminations, may not be installed in a building or department location without coordination with NOC staff.

Routers

Except as implemented by the NOC, no routers of any type may be attached to NYU-NET. Doing so can seriously disrupt the reliability of the network and compromise the security of NYU-NET as a whole.

A router may be a dedicated hardware device purchased for this purpose, a Layer-3 network switch that participates in routing protocols, or a computer with multiple network interfaces (including a modem link, a tunnel or a virtual network interface) that forwards network traffic between these interfaces. Connecting a computer via more than one network interface to NYU-NET is not permitted without permission of the NOC.

Firewalls

Network firewall hardware or software may not be installed except in collaboration with the NOC.

Radio Frequency (RF) Spectrum

ITS is building a variety of wireless services for use by the University community that utilize radio frequency spectrum. To maintain the reliability of these services, it is necessary for ITS to coordinate the use of the wireless spectrum on University premises. With the exception of cellular phones, any device that is going to be installed or utilized on University premises that generates RF transmission signals must be approved by ITS. Installation of wireless access points for wireless data networking by non-ITS organizations is generally not permitted.

Network Management and Analysis

SNMP Management

Any network infrastructure equipment purchased for attachment to NYU-NET must run an SNMP agent, in order to ensure that the NOC can effectively manage and troubleshoot the equipment.

SNMP Agents

SNMP agents should be run on all UNIX machines, Novell servers, and NT servers.

Network Analysis and Scanning

The NOC and NYU Computer and Network Security groups are the only two groups of individuals that may run any type of network analysis or network scanning equipment or software on NYU-NET at large, unless express permission is granted to departmental or school network managers. Such devices can be used to manipulate the network, impact connectivity at large and damage individual machines. Any such activity detected on NYU-NET will be considered a security event.

Network Discovery

Software that uses SNMP or ICMP to automatically "discover" or identify entities on a network generally can have a negative impact on the network at large. Such software scans the entire network, flooding it and its intended target agents with an overwhelming amount of SNMP traffic. The end result is reduced bandwidth to the local networks and diminished router performance. Such software includes management applications like SunNet Manager, HP OpenView and the HP JetAdmin software when searching for Hewlett Packard printers. The current state of such software technology does not allow us to permit the use of such software across NYU-NET, though JetAdmin in a non-Search mode can safely be used to manage individual printers in a departmental, local-area network context.

Network Naming & Addressing

External Hostnames/Domain Registrations

External hostnames or domain names may not be registered with Internet Service Providers (ISPs) or the InterNIC against NYU DNS name space, address space or name servers.

Private IP Address Space

Private address space specified in RFC 1918 cannot be arbitrarily used on NYU-NET. Since the NOC is making heavy use of this address space for production use on NYU-NET, any use for such addresses must be coordinated with the NOC.

Registration

The proper operation of NYU-NET relies on all computers and networking equipment being registered on the network with `hostmaster@nyu.edu`. Designated individuals from each department should contact hostmaster for reporting any additions, changes or removal of computers from NYU-NET.

LAN Network Numbers

Network numbers should be acquired by LAN administrators from hostmaster. No arbitrary selection of IPX or AppleTalk network numbers are permitted, due to the routing conflicts that result from such activity and result in disrupted connectivity for parts or all of NYU-NET.

Acceptable Use

Commercial Activities

Commercial services of any type may not be offered on NYU-NET, nor may anyone use an NYU-NET connection or computer account for commercial purposes.

Unauthenticated Access to the Internet

Unauthenticated access to the Internet via NYU-NET is not permitted. A department requiring a public computing lab should work with the ITS to ensure that such a network is attached to the dedicated NYU-NET Classroom sub-network. This network is firewalled from the Internet and students can access the Web via a dedicated proxy server the ITS runs for NYU-NET. Telnet and FTP access to the Internet can be achieved by first logging into a UNIX or similar account on NYU-NET, and subsequently using that account to access the desired resource.

Remote Access and External Network Connections

Remote access to NYU-NET

ITS runs a central dial-in modem pool on behalf of the university; due to the security and bandwidth issues associated with running such a service, no department or individual may offer remote access to NYU-NET via modem or ISDN, except as specially arranged with the NOC. This includes modem pools (of any size), "RAS servers" and devices like the Ascend Pipeline access products.

Remote Connections to Outside Networks

Remote connections to other networks or the Internet are not permitted on NYU-NET, except by special arrangement with the NOC. This includes "dual-homed" machines, with a network attachment to NYU-NET and a modem link to a remote network.

Tunnel Connections to Outside Networks

Tunnels between an NYU-NET host and another host or network infrastructure component on another network are not permitted. Doing so exposes NYU-NET to security risks by circumventing access controls already in place to protect NYU-NET from attacks. Such tunnels include those used for carrying IPX, AppleTalk, NetBEUI, DVMRP/IP Multicast, IPv6 and VPNs (Virtual Private Networks).

Network Services

Non-routable Protocols

NYU-NET, being a multiprotocol routed network, supports IP, IPX, AppleTalk and DecNET protocols; however, non-routable protocols such as NetBEUI (used by Windows NT/95 for Microsoft Networking) pose significant scalability problems by not properly functioning on a routed network. Hence they are not supported for communications across NYU-NET.

Domain Name Service

NYU-NET supports the IETF/Internet host naming scheme called the Domain Name Service (DNS). Due to significant incompatibilities with this standard, the Microsoft naming scheme, WINS, is not supported.

Name and Boot Servers

The central NOC runs triply-redundant BOOTP, DHCP and DNS servers on behalf of NYU-NET. These servers ensure the uninterrupted and reliable assignment and registration of IP addresses for all hosts on NYU-NET. Individual departments may not run such servers of their own, except under special arrangement with the NOC. The NOC sets the standards for all network services in DNS services and servers.

News Servers

The NOC runs a pair of central, high-performance USENET News servers on behalf of New York University. Departments or individuals requiring USENET news access should request such access from their local LAN support staff, who can then contact hostmaster@nyu.edu to arrange for news server access. Since news servers consume a very large amount of bandwidth on the network and the university-wide connection to the Internet, we do not support any additional servers on NYU-NET.

WWW Proxy Server

ITS runs an HTTP proxy server on behalf of the university. Such devices can consume a large amount of bandwidth on the network, and pose a security risk to NYU-NET unless extremely carefully managed. As a result, no other HTTP proxy servers may be run on the network.

FTP and Web Server Appropriate Use

FTP or Web servers for the intention of distributing copyrighted or pirated software on NYU-NET or the Internet are illegal and not permitted on NYU-NET. Any group wishing

to establish an FTP or Web server for distribution of large amounts of data should contact ITS for guidance. Such activity impacts traffic flows on the network and has a direct impact on performance of NYU-NET at large.

High-bandwidth Network Applications

High-bandwidth projects or activities, including streaming video and videoconferencing should also be conducted in coordination with ITS.

Local Area Networks and Servers

Backup

Backups of computers over NYU-NET is not currently supported, due to the bandwidth requirements of such activities. Individuals may use the network to back up machines local to their LAN, but such traffic traversing the NYU-NET backbone can negatively impact the connectivity of others on NYU-NET.

Network Connections

All NYU-NET attached hosts may have only one network connection. "Dual-homing" between two or more networks, or multiple connections to a single LAN are not permitted. This is due to a wide variety of issues including: network address resource limitations, network reliability, network security, and conflicts arising with other hosts on the connected LAN(s).

Server-based Applications

ITS strongly discourages the running of microcomputer applications over NYU-NET from a Novell or NT server. Applications are best run locally on the machine, with servers used as data/file repositories.

Network Operations Center, noc@nyu.edu

Document contact: [Jimmy Kyriannis](#)

All contents copyright

© New York University

All rights reserved

Page last revised: **November 8, 2002**

Page last reviewed: August 22, 2006