UNIVERSITY STANDARD

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL
DATA NETWORK STANDARD

Introduction

PURPOSE

This standard is intended to provide structure for effective operation of data networks for the University in accordance with the UNC-Chapel Hill Data Network Policy.

UNC-Chapel Hill Information Technology Services (ITS) has been mandated by the University to manage the campus network to ensure reliability, integrity and interoperability. This management supports the University mission of education, service, and research. It is the responsibility of ITS to coordinate, monitor, and manage University network traffic and activities. ITS must ensure that campus facilities adhere to FCC and other regulatory requirements, do not disrupt statewide or national networks and maintain good connectivity to the network for all campus users.

SCOPE OF APPLICABILITY

All University units and Constituents responsible for devices or services connected to University data network facilities.

Standard

Data Network Management

An aggregation of separate, discrete, and privately-managed backbone or “backbone-like” data, voice or video networks does not constitute a utilities infrastructure that can meet institutional goals, nor does it provide for the best and most efficient return on the University’s investment in this infrastructure.
To ensure a high-performance, high-availability, production-quality communications infrastructure at UNC-Chapel Hill, ITS must provide a number of components and architectural considerations, as described below.

1. To maximize reliability, security and efficient use of limited resources, ITS must develop and implement the physical connectivity design: how buildings connect to the campus fiber infrastructure. The design architecture for the physical layer consists of all campus buildings being designated as hubs or spurs, based on the fiber path and proximity to other buildings.

2. To optimize compatibility, mobility, bandwidth and security, ITS must design, implement and maintain the campus networking architecture.

3. To reinforce compatibility and high performance, ITS must maintain campus Internet connectivity. This connectivity is presently based on redundant high speed links, which requires a single campus entity for coordination and management.

4. To foster security, only appropriate ITS personnel authorized by the AVC for Communications Technology or Chief Information Security Officer will be permitted to monitor traffic over backbone links through network protocol analyzers (sniffers). The design of both the fiber physical connectivity and of the networking architecture do not allow random, unauthorized traffic eavesdropping across the links.

Device Management

In addition to the requirement that only ITS may install and maintain switches and routers on the campus data network, no device with multiple network interfaces (including, but not limited to, VPN gateways, firewalls, and servers) may be connected to the network without advance approval from ITS. This advance notice must be submitted in the form of a Help Request ticket (use the category labeled “general topics”). Failure to provide this advance notice will result in such devices being isolated from and unable to communicate on the network. If the connection of a device is of an emergency nature (such as replacing an existing device), the ticket can be marked as Critical and will receive immediate attention.

Local Departmental Technical Liaisons

Every University operating unit connected to the UNC-Chapel Hill Communications Network must have a designated technical liaison registered with ITS. The technical liaison will be contacted when problems arise with that particular segment of the
network. The liaison will be expected to respond with appropriate priority and act with appropriate authority. This person should be reachable during normal business hours. Departmental contact procedures for nights and weekends should be made available to the ITS Operations Center at 919-962-6503.

Local departmental technical liaisons must be cooperative and responsive to ITS requests. When problems arise, ITS will advise and work with the technical liaison. However, if the technical liaison or a designated representative/alternate cannot be contacted in an appropriate amount of time, ITS will take whatever steps are necessary to restore the proper functioning of the University Network for the majority of campus users. This will include disconnecting a department or building from the campus network if necessary. For this reason, and to ensure reliability, security and high performance, network electronics (switches and routers) connected to the campus backbone must be managed and maintained by ITS. In all cases, ITS will notify the technical liaison of any actions that have been taken and will work with the technical liaisons to correct any problems.

TCP/IP Subnet Assignments

Any network device intended to have Internet connectivity must have a registered IP address within the 152.2.0.0, 152.19.0.0 or 152.23.0.0 Class B Internet networks assigned to UNC at Chapel Hill. Subnet number ranges (both IPv4 and IPv6) are assigned by ITS. Technical liaisons must send requests for new assignments via help ticket. ITS is prepared to provide whatever level of addressing is required to meet departmental business needs. Requests should include subnet ranges of an appropriate size to meet anticipated growth as well as current need; however, departments are encouraged to use campus DHCP whenever possible.

Related to the issue of IP subnets is the role of routers in a campus network environment. Due to the increased complexity of routers over switches, and the impact that improperly configured IP routers can have on campus network access, any routers that need to deployed for either broadcast/multicast containment or security reasons that cannot be met by virtual LAN configurations must be authorized by ITS. Furthermore, because misconfigured routers can produce routing protocol management issues on a large network, ITS must manage all routers on the UNC at Chapel Hill network to ensure compatibility and reliability.

IPV6

The ITS Networking IP Services group at UNC-Chapel Hill will only register globally unique, routable IPv6 addresses in campus DNS. ITS reserves the right to refuse any non-global or non-native (i.e. tunneled) IPv6 address. ITS encourages clients to request
ITS-distributed IPv6 addresses appropriate for their assigned VLAN to register in campus DNS. As with IPv4, if a system is going to be seen on the network by others, it should be registered in DNS.

IPv6 addresses registered on the campus DNS servers should be from an existing campus IPv6 network, or approved external IPv6 network. Please submit any IPv6 address that was not distributed by ITS Networking to the ITS Networking staff for review by submitting a ticket specifying the IPv6 address, the source of the address, and the reason that a campus network based IPv6 address is not an acceptable option.

**UNC Domain Names**

Requests for ‘name.unc.edu’ domains must be originated at the department level and each request should include the following:
- ‘unc.edu’ domain name being requested
- the associated department
- the department contact for that domain name
- a description of the purpose for the domain relative to UNC-CH
- a signed and dated memo of understanding (MOU) for the domain requested.

This information must be sent to ITS-IP Services via support ticket. The MOU form can be initiated online. The MOU explains the conditions of ownership for the domain. A copy of the approved MOU signed by ITS will be returned to the requestor as the official notice of registration. The requestor should contact ITS if there are any changes in the information provided on your original ‘unc.edu’ domain application.

**Non-UNC Domain Names**

ITS shall determine the best manner to provide guidance in the registration of non-‘unc.edu’ domains for non-commercial University business purposes and may include such names in University DNS only in accordance with best practices and the best interests of the University. Only faculty or staff may use UNC-Chapel Hill DNS services for non-UNC domain names. Personal use is not acceptable. Use of non-unc.edu domain names on the UNC network for commercial or personal business will result in loss of network access.

In order to register a non-unc.edu domain name (.com or .org or .net) on a system using UNC-Chapel Hill DNS services, you must be a UNC faculty or staff member. Application may be made via support ticket and ITS will determine whether use of University DNS would be appropriate.
Domain names for services accepting online payments

UNC-Chapel Hill is under constant attack by outside hackers attempting to compromise university systems to obtain unauthorized access to university data, including credit card information used for online payments of university events or goods. To not attract unnecessary attention to such websites and minimize the threat of a credit card compromise, any websites involved in accepting online payments within the unc.edu name space should not use a name that exposes their function.

Naming a website with words including, but not limited to, “payment”, “donation”, or “credit card” must be avoided. To get approval for any payment-related website, the business units should work with the University CERTIFI committee (certifi@unc.edu).

IP/Host Registration

Although IP subnets are assigned by ITS, individual IP addresses for departmental network devices are assigned within that department by the department’s technical liaison. However, assigned addresses and corresponding hostnames MUST be appropriately registered with ITS or with an appropriately configured departmental DNS (domain name server) that is recognized by ITS. Send host registration information via help ticket.

Failure to appropriately register host names and addresses could result in those devices being blocked at the nearest network switch.

Network Use Standards

The University Communications Network supports use policies in accordance with its suppliers of Internet connectivity and will enforce those policies to the best of its ability. ITS supports those elements of Internet policy that demand network etiquette and due consideration for user’s rights to privacy. In addition, the University Communications Network also endorses the policies and responsibilities for host and network managers contained in Internet RFC 1173; in particular, the policy that “Internet sites should not have ‘general use’ accounts, or ‘open’ (without password) terminal servers that can access the rest of the Internet.”

EXCEPTIONS

Specific or blanket/process exceptions to the application of this standard may be made by the Vice Chancellor for Information Technology, Associate Vice Chancellor for Information Technology, Assistant Vice Chancellor for ITS Communications or their delegate(s) and documented in writing.
Definitions

**UNC-Chapel Hill Constituent:** UNC-Chapel Hill faculty, staff, students, retirees, contractors, distance learners, visiting scholars and others who require UNC-Chapel Hill resources to work in conjunction with UNC-Chapel Hill.

**Tunneled:** Technology enabling one network to send its data via another network’s connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

Related Requirements

**EXTERNAL REGULATIONS AND CONSEQUENCES**

- [Link to Internet RFC 1173](#)

**UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES**

- [UNC-Chapel Hill Data Network Policy](#)
- [UNC-Chapel Hill Wireless Standard](#)
- [DNS Memorandum of Understanding Form](#)

Contact Information

**PRIMARY CONTACT(S)**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>ITS Policy Office</td>
<td>919-962-HELP</td>
<td><a href="mailto:Its_policy@unc.edu">Its_policy@unc.edu</a></td>
</tr>
<tr>
<td>Networking</td>
<td>ITS Communications Technology</td>
<td>919-962-HELP</td>
<td>help.unc.edu</td>
</tr>
</tbody>
</table>
Important Dates

- Effective Date and title of Approver: Effective 5/2/2017. Deputy Chief Information Officer.
- Revision and Review Dates, Change notes, title of Reviewer or Approver: Standard derived from superseded Data Network Infrastructure Policy dated 5/29/2014