

DRAFT

OSUNet Technical Standards and Operational Requirements

**Enterprise Networking
Office of Information Technology
The Ohio State University**

March 10, 2004

Index

1. Overview

- 1.1 OSUNet Connection Procedures**
- 1.2 OSUNet Connection Requirements**
- 1.3 Monitoring of the Network**
- 1.4 OSUNet Best Practices**
- 1.5 OSUNet Principles**
- 1.6 References**

2. Domain Name Service (DNS) Requirements

- 2.1 The osu.edu domain**
- 2.2 The ohio-state.edu domain**
- 2.3 Non ohio-state.edu domains**
- 2.4 Hosting DNS on campus**
- 2.5 Windows Active Directory and DNS**
- 2.6 References**

3 Host Security Requirements

- 3.1 Installation Requirements**
- 3.2 Password Requirements**
- 3.3 Antivirus Requirements**
- 3.4 Monitoring Requirements**
- 3.5 References**

4 Network Security Requirements

- 4.1 Firewalls**
- 4.2 Local Network Enabled Devices**
- 4.3 Network Monitoring**
- 4.4 Authentication Requirements**
- 4.5 Campus Border Port Blocking**
- 4.6 References**

5 Host Unblocking Requirements

- 5.1 Responsibility**

5.2 Blocked Host Message
5.3 Multiple Unblock Requests
5.4 Questions
5.5 References

6 Logging Requirements
6.1 Guidelines
6.2 Best Practices
6.3 References

7 Authentication Requirements
7.1 Requirements
7.2 References

8 Glossary

1. Overview

The technical standards and operational requirements outlined in this document are designed to provide guidance for all academic and administrative units that desire to connect to OSUNet. In collaboration with the campus technical user community OIT will develop and continuously update these technical guidelines and standards for devices connected directly or through unit facilities to OSUNet, communications protocols supported on OSUNet, and both operational and security requirements for use of OSUNet. The community will be represented by the PlanIT Stakeholders Group and the Ohio State University Network Working Group (NETWOG).

All decisions, notifications, or measures taken under these technical standards and operational requirements may be appealed to the CIO through the CIO Office Director of Information Technology Policy and Services. Appeals should be submitted by email to ITPolicy@osu.edu.

1.1 OSUNet Connection Procedures

1. All OSUNet connections are initiated by submitting an [application form](#), with the appropriate financial commitments and approvals, to the Director of Enterprise Networking, or his designee.
2. All academic or administrative units connected to OSUNet are required to have both a Departmental Network Administrator and one or more secondary network contacts.

The Department Network Administrator (DNA) will act as the focal point for interfacing with OIT and will provide first level network support to their users. This person's name, phone numbers, postal address, and name.n are to be provided to OIT. To become a

DNA, or to determine the identity of your DNA, contact the university [hostmaster](#). All DNAs are required to comply with the [Minimum Expectations of DNAs](#).

The secondary network contact(s) will be registered by OIT, and contacted in the event of a serious incident or if the primary DNA is unavailable. It is recommended but not required that the secondary network contact(s) meet the [Minimum Expectations of DNAs](#). To register these contacts the DNA for the network must provide the correct name.n and contact information to the university [hostmaster](#).

3. DNAs will be allocated a range of IP addresses to meet their academic or administrative unit's needs. DNAs are responsible to administer that address space in conformance with the terms outlined in this document, along with any other responsibilities and guidelines imposed by their department.
4. Purchase of equipment that requires static network routes (e.g. *routing firewalls*) should be avoided. Utilization of such equipment may incur an additional monthly charge for route maintenance.
5. Before purchasing network hardware, software or consultation services, departments are encouraged to consult with OIT to ensure OSUNet compatibility of their purchases.

1.2 OSUNet Connection Requirements

1. DNAs are required to register **all** *hosts* that use IP addresses in the OSUNet Domain Name System (DNS). Registration information should be sent to the university [hostmaster](#) (Information and assistance is available from the [Hostmaster FAQ](#), or call 688-HELP). The university DNS requirements are outlined in Section 2 of this document
2. DNAs are responsible for patching and maintaining their devices in conformance with the OSUNet Host Security Requirements and the Network Security Requirements that are outlined in Sections 3 and 4 of this document.
3. The university is responsible for Internet activity originating from campus; therefore all activity must be traceable to a responsible person. To help meet this responsibility, user activity from and within OSUNet must be authenticated. The OSUNet authentication requirements are outlined in Section 6 of this document.
4. To identify how the university network is being targeted, any computer security *incident* must be reported to the Network Security Group Incident Response Team (IRT) security@net.ohio-state.edu.
5. For numerous reasons (e.g. email blacklists, site licensed content and software) open mail relays, open proxies and other mechanisms (e.g. formmail.pl cgi scripts) that can be abused to relay email or network connections are prohibited

6. Anyone that receives an OSUNet connection cannot also connect their network with another ISP, service provider or other entity without prior written approval from the director of Enterprise Networking.

7. All wireless devices connected to OSUNet must comply with the [*Policy on Deployment and Use of Wireless Data Networks*](#).

1.3 Monitoring of the Network

OIT reserves the right to monitor any network connected to OSUNet. This includes examining packet headers and trailers to determine operational characteristics, such as protocol types, proper use of network addresses, traffic demand, etc. and the scanning of devices connected to identify security vulnerabilities in accordance with all applicable legal regulations and the [*University Policy on Responsible Use of University Computing Resources*](#).

In a perceived emergency situation OIT may take immediate steps, including fully or partially blocking OSUNet access, to ensure the integrity of the university data network and systems, safeguard the health and safety of university community members and property, or protect the university from liability. The process of having a device unblocked is outlined in Section 5 of this document.

OIT also requires departments to allow echo request and echo reply response packets across the campus network, except from the student-housing network (RESNET), to aid in central statistical and trouble shooting functions.

1.4 OSUNet Best Practices

[*Host Security Best Practices*](#)

[*Network Best Practices*](#)

[*Password Best Practices*](#)

1.5 OSUNet Principles

1. The financial model for OSUNet is based on partial cost recovery for at least one port in each building in which a department has a presence.

2. A department may request the aggregation of multiple buildings to a single OSUNet port. The Director of Enterprise Networking will review the request, and may approve it based on the technical requirements of the request. If the request is approved, the minimum per building charges will continue to apply.

3. IPV4 is the standard communications protocol; IPV6 is available for non-production use.
4. No department devices will be connected directly to the OSUNet backbone.
5. Local traffic from any OIT service including Public Computing Sites is isolated from the rest of the building's network. We also recommend that departmental student labs follow this procedure and be kept separate from the rest of the department's network.
6. Excessive or abusive use of OSUNet bandwidth is not permitted. For example, excessive network traffic and *spam* are not permitted on OSUNet. Devices or networks may be blocked or disabled if necessary to protect the network.
7. If an academic or administrative department has expanded since their initial IP address allocation and so requires additional IP space the DNA should contact the OIT help desk at 688-HELP or shelp@osu.edu. Additional address space is available at no charge and we strongly recommend against the use of Network Address Translation (NAT) except as outlined in the [Host Security Best Practices](#).

1.6 References

ITPolicy@osu.edu

OSUNet [application form](#)

Contact the university [hostmaster](#)

[Minimum Expectations of DNAs](#)

[Hostmaster FAQ](#)

[Policy on Deployment and Use of Wireless Data Networks](#)

[University Policy on Responsible Use of University Computing Resources](#)

[Host Security Best Practices](#)

[Network Best Practices](#)

[Password Best Practices](#)

shelp@osu.edu

[8 Glossary](#)

Return to Index

2. Domain Name Service (DNS) Requirements

Enterprise Networking maintains the OSUNet Domain Name Service (DNS) servers. All devices and domains operated on OSUNet must be registered with Enterprise Networking. To register a device the DNA for the network must submit email to the university [hostmaster](#). To review the format guidelines required of requests view the [Hostmaster FAQ](#).

2.1 The osu.edu domain

The osu.edu name space has been opened up to departments on campus on a case-by-case basis. The following rules govern its use:

1. The osu.edu domain is intended for short URL's to web sites. However to maintain a standard format all names are limited to < name>.osu.edu. To aid users that type www.<name>.osu.edu, a www.<name>.osu.edu record will be created to direct the user to the same server that houses the <name>.osu.edu site.
2. To provide everyone with an equal opportunity to request names and to provide a central reviewing body the [Web Policy Committee](#) has been asked to review and approve all names in the osu.edu name space.
3. All approved requests are maintained as aliases (CNAME records) to a server located in the department's ohio-state domain, and are required to be directed to a server on the university network.

2.2 The ohio-state.edu domain

All devices connected to OSUNet should resolve to an academic or administrative units ohio-state.edu subdomain. The use of the ohio-state.edu domain is limited to devices that are connected to OSUNet.

If a department is interested in requesting a new subdomain name in the ohio-state.edu name space the DNA should fill out the [Subdomain Request form](#) and document in a brief letter the intended use and number of [hosts](#) for the new domain.

2.3 Non ohio-state.edu domains

In those cases where the standard ohio-state and osu.edu domains do not reflect the purpose of a web site (e.g. a joint project with external organizations and /or universities) OIT will entertain requests for alternative domains and if approved, provide hosting services for other Top Level Domains (TLD's). These domains should, however, reflect in their name an association with the university. Any group that requests a non-standard

domain must show why the traditional ohio-state domain does not work for their situation. The requesting group also must demonstrate that the project supports the mission of the university.

The one TLD for which OIT will not provide hosting is the .com TLD. (.com's are intended to be used by commercial organizations, according to [RFC1591](#).) Since Ohio State is a non-profit, state funded institution .com names do not represent the university and will not be allowed on the network.

For a domain to be approved using one of the alternative TLDs, the requesting party must submit the following:

A letter on departmental letterhead signed by the unit chair/dean/director addressing the following:

1. A description of the purpose/function/nature of the organization that includes the participants involved (including physical locations for both the on and off campus parts of the organization) and the role the university plays in the organization.
 - a. If the university already provides hosting for other domains for the parties involved how the new request differs.
2. That it is not a private business or other commercial venture.
3. Agreeing to a periodic review and renewal process of approved domains to insure that the content matches the original signed agreement and that no commercial activity is taking place.
4. Stating that they understand it is the organization's responsibility to incur any additional costs in the registration process, including but not limited to transferring or renewing the domain name registration with the appropriate domain registrar.

A second technical letter from the DNA is also needed that addresses the following:

1. The billing contact in the organization.
2. Agreeing to coordinate the creation of the domain with OIT at Network Solutions, with the following conditions:
 - a. OIT will maintain the domains' primary and secondary name servers.
 - b. The "Administrative" and "Billing" contacts will be listed as someone in the organization.
 - c. The "Registrant" and "Technical" contact information will be the registered NIC handle for the University, ZE146-ORG.

3. Providing the IP (s) that will be used with the new domain.
4. Agreeing that OIT will only support published domain names, and will not provide DNS for other domains that are variations of the published name. (e.g., Publishing <name>.org and asking for <name>.net to point to the same place.)

Both of these documents should be mailed or faxed to the following:

Ohio State Hostmaster
320 West 8th Ave
Columbus, Ohio 43201-2331
614-292-9525 fax

2.4 Hosting DNS on campus

OIT is responsible for all aspects of OSUNet including DNS. As a consequence, all domains using university resources are required to reside on the OIT name servers.

Any domain that is found that was created without consulting OIT will be reviewed, and if it meets both the requirements for hosting and residing on the university network, it will be added to the OIT name servers after the department complies with the requirements outlined in Section 2.3 of this document. If a domain is discovered on the university network that does not meet the requirements set forth by OIT, it will be removed from OSUNet

This also includes previously approved domains that did not continue the stated purpose/function/or nature of the domain.

2.5 Windows Active Directory and DNS

Enterprise Networking supports the records required by Microsoft active directory. However due to the security issues that accompany allowing dynamic updates to the campus name servers, dynamic updating is not allowed.

The Active Directory [configuration page](#) explains DNS options for departments. To use the available features of the directory structure Microsoft requires extra records in DNS. It is important, and somewhat time sensitive, for these records to be passed on to the university [hostmaster](#) by the DNA in a timely manner otherwise unexplained/unexpected complications in the Active Directory structure may occur.

For more information concerning the implementations of Active Directory at OSU the NT/2000 administrators have been asked to use the [osu.windows.misc](#) newsgroup to provide their experiences with deployments and to help others thinking of installing Windows 2000.

2.6 References

Contact the university [hostmaster](#)

[Hostmaster FAQ.](#)

[Web Policy Committee](#)

[Subdomain Request form](#)

[RFC1591](#)

Active Directory [configuration page](#)

The [osu.windows.misc](#) newsgroup

[8 Glossary](#)

Return to Index

3 Host Security Requirements

For a more detailed discussion of these and other best practices, and more detailed best practices for a variety of operating systems, see the OSU [Host Security Best Practices.](#)

3.1 Installation Requirements

When installing a *host* on OSUNet, administrators are expected to adhere to the following list of best practices:

1. Installation of the *host* operating system and all applicable security patches should be done with the *host* disconnected from OSUNet, or otherwise isolated from all network traffic.
2. Before the *host* is connected to a network, any services not used or required for operation should be disabled.
3. If a host-based *firewall* is available, it should be enabled before the *host* is connected to the network.

3.2 Password Requirements

Administrators must make sure that all accounts have good passwords. If accounts have default passwords, they must be changed or the account completely disabled before a *host*

is connected to the network. For more information on passwords, please review our [*Password Best Practices*](#).

3.3 Antivirus Requirements

For operating systems for which the university owns site-licensed anti-virus software, these systems should have real time virus scanning enabled, along with daily updates to their virus library (e.g. daily DAT file downloads). Please see [*Site Licensed Software*](#).

3.4 Monitoring Requirements

All systems should be evaluated by their administrators for security vulnerabilities. Part of this evaluation process includes reviewing system logs. Logging requirements are outlined in Section 6 of this document. Any serious vulnerability must be corrected.

3.5 References

[*Host Security Best Practices*](#)

[*Password Best Practices*](#)

[*Site Licensed Software*](#)

[*8 Glossary*](#)

Return to Index

4 Network Security Requirements

4.1 Firewalls

A *bridging firewall* should be installed to protect all *hosts* on the departmental network. If the department has *hosts* in multiple buildings, multiple *firewalls* may be required.

When deploying a *firewall*, the types of traffic it allows directly affects its effectiveness, so when creating a ruleset a good starting point is to deny inbound traffic by default. For additional information about deploying a *firewall* we have created a [*Firewall FAQ*](#).

Departments may request the Director of Enterprise Networking to approve the aggregation of multiple buildings behind a single department *firewall*; however minimum per building charges would continue to apply, and such a solution may introduce certain performance, capacity and scale limitations.

4.2 Local Network Enabled Devices

All network-enabled devices should have their management interfaces password protected. For devices only used on the local network such as printers that do not need to be accessed from beyond the local network, the default gateway should not be configured.

4.3 Network Monitoring

Unless SNMP is used to monitor or configure devices on the network it should be disabled; if it is used all SNMP facilities should have a password (even read-only facilities), and all default passwords **must** be changed. To reduce the access to SNMP information, devices used to manage a network are recommended to be segmented onto a separate management network or to filter the SNMP traffic to only the management devices.

All use of network diagnostic tools such as nmap, tcpdump, etc. must comply with all applicable legal regulations and the [University Policy on Responsible Use of University Computing Resources](#).

4.4 Authentication Requirements

All computer labs must authenticate users before they are allowed access past the local network segment, even if the lab requires a keycard or other key for access.

4.5 Campus Border Port Blocking

The Director of Enterprise Networking in consultation with the Network Engineering and Network Security Groups, may set up blocks on specific ports at the OSUNet border. OIT will attempt to notify all DNAs before the blocks take effect, and will attempt to limit the amount of time these blocks are in place. A list of the ports currently blocked, and their review dates can be found at the site; [What does the University block at the Internet border?](#).

4.6 References

[Firewall FAQ](#)

[University Policy on Responsible Use of University Computing Resources](#)

[What does the University block at the Internet border?](#)

[8 Glossary](#)

Return to Index

5 Host Unblocking Requirements

5.1 Responsibility

When Enterprise Networking blocks a *host*, the network contacts will be notified by e-mail, and by other means if practical. The network contacts are responsible for notifying the affected users, and either fixing the problem or passing the notification to the responsible parties so that they can address the problem. The following are guidelines when dealing with the Network Security Group Incident Response Team (IRT) regarding blocked *hosts*.

5.2 Blocked Host Message

When the IRT sends out a notice about the blocking of a *host*, the message will include as much information as possible on the incident, along with instructions on how to have the *host* unblocked. To verify which *hosts* are blocked the IRT maintains a list at; <http://www.net.ohio-state.edu/security/restricted/BH/blackhole.cgi>

To have a *host* unblocked, the following items need to be completed. The administrator must send e-mail to security@net.ohio-state.edu, which includes:

1. An explanation of what was wrong with the *host* (found viruses, a backdoor, etc.).
2. How the problem was corrected.
3. If the incident was a result of a lack of patches or virus protection, a list of steps taken to prevent the reoccurrence of the infection should be included. If steps are being taken but have not been deployed, to prevent a reoccurrence, please indicate them in your response.

The IRT would prefer that you reply to or forward a copy of the initial “block” e-mail complete with the original subject when requesting that a *host* be unblocked. Otherwise you will need to specify the IP address and incident number so that we can handle your request properly. Failure to properly identify the *host*, the incident, and the steps taken to clean up and prevent recurrences may result in delays in unblocking the address.

5.3 Multiple Unblock Requests

If an administrator has multiple *hosts* to be unblocked as part of the same incident, they can be included in a list in a single e-mail that includes the incident number and IP addresses. However, failure to properly identify the *hosts*, the incident, and the steps taken to clean up and prevent recurrences may result in delays in unblocking the addresses.

If administrators have multiple *hosts* from different incidents, it will aid in the tracking of the individual incidents if the administrator sends separate e-mail replies to their respective block messages, including the steps taken to clean up and prevent recurrences.

5.4 Questions

If you have any security related questions send them to security@net.ohio-state.edu. Please try to include the *OSU-IRT incident number* if your question pertains to a blocked *host*, or a particular incident.

5.5 References

<http://www.net.ohio-state.edu/security/restricted/BH/blackhole.cgi>

Contact the Enterprise Networking Security Group security@net.ohio-state.edu

[8 Glossary](#)

[Return to Index](#)

6 Logging Requirements

6.1 Guidelines

University academic and administrative units are responsible for OSUNet traffic originating in the facilities and areas they administer, and are responsible for verifying that they can supply authentication logs for any lab or general use computers (including wireless access points) that are in their jurisdiction. All authentication logs must be kept a minimum of 30 days, but can be kept longer at the discretion of the group or department. Logs other than authentication logs are often useful in diagnosing a problem, and should be kept for a minimum of 14 days.

6.2 Best Practices

All computers, servers and workstations, should be configured to log events that occur. In the case of Microsoft Windows machines, the administrator should expand the amount of logging done to increase the chances that a compromise can be detected or confirmed. If possible logs should be sent to a central departmental logging server.

6.3 References

[8 Glossary](#)

[Return to Index](#)

7 Authentication Requirements

7.1 Requirements

To help the university responsibly administer network traffic, all OSUNet access must be authenticated and logged.

The following requirements deal with user authentication on devices connected to OSUNet.

All devices, where they have the technical capability, should be configured to authenticate users and keep the authentication logs for at least the minimum log period.

All computer labs, public or locked, must authenticate users before they are allowed access beyond the local network.

Authentication information (generally username and password information) should not be sent "in the clear" (unencrypted). Please see the [Password Best Practices](#) for further information on how to protect your password information.

7.2 References

[Password Best Practices](#)

[8 Glossary](#)

[Return to Index](#)

8 Glossary

Bridging Firewall - A device that filters packets to a network as a bridge. This type of firewall is network architecture dependent. The advantages of a Bridging firewall are that it is easy to retrofit the firewall into an existing network without reconfiguring the workstations on the network. [Firewalls FAQ](#)

Desktop - A computer primarily used to provide direct access (via a locally attached keyboard, mouse and monitor) to applications such as web browsers, email clients, office productivity and data analysis tools for use usually by one individual at a time.

Firewall – A system designed to prevent unauthorized access to or from a local network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized access to secure networks connected to the Internet. All message entering or leaving the local network pass through the firewall, which examines all network traffic and blocks traffic that does not meet the specified security criteria. [Firewalls FAQ](#)

Incident - An incident is the act of violating an explicit or implied security policy. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations. These include but are not limited to attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Network Address Translation - (NAT) is a way to map an entire network (or networks) to one or many IP address (es). NAT is usually used when the number of IP addresses assigned by an Internet Service Provider is less than the total number of computers that you wish to provide Internet access for. NAT is described in RFC 1631. The use of NAT on OSUNet is strongly discouraged, and should not be used for security purposes.

[Reasons not to use NAT](#)

OSU-IRT incident number – To assist the OSU incident response team in handling computer security and abuse investigations they create a unique incident number used to identify the parties involved.

Routing Firewall - A device that becomes the default gateway or static route for network traffic to flow through. This type of firewall communicates with routers and shares routing information to help determine where the traffic should be routed and if the traffic should be passed. This often requires reconfiguration of network routers and workstations on the network. A [Firewalls FAQ](#) has been created to answer common questions about firewalls.

Server - A computer used primarily to provide network-based services (e.g. web, file, or email), for use typically by multiple users. Servers are typically not used as a desktop.

spam – Unsolicited commercial email.

Workstation - See Desktop.

Host – Any network-enabled device connected to the campus network. Examples include desktops, servers, workstations, printers, firewalls, and network switches.