

DRAFT Policy Statement – State Network Requirements

Title: State Network Requirement Policy

Document Number: PS-60

Effective Date: 8/30/2002

Published by: Office of Information Technology

1.0 Purpose

The primary purpose of the policy is to create and maintain a manageable, efficient and secure network environment by establishing requirements for entities attached to the state network.

2.0 Scope

This network policy applies to all entities attached to the Arkansas State Network, which physically or logically access data through the state's network infrastructure. This includes, but is not limited to, all state agencies, local and county agencies, public schools, boards, commissions, and institutions of higher education.

3.0 Background

3.1 The Arkansas statewide network connects approximately 3,000 entities to the Internet. The Arkansas Department of Information Systems (DIS) is vested with the powers and duties necessary for implementing and managing the state-wide network. Arkansas Code 25-4-105 states that DIS responsibilities include, "conceptualizing, designing, developing, building, and maintaining common information technology infrastructure elements used by state agencies and governmental entities;" Arkansas Code 25-4-109 (d) states, "Agencies shall use the state core telecommunications, data, application, and security infrastructures." With respect to technical issues in connecting to the network, the point at which DIS responsibility ends and entity responsibility begins, called the demarcation point, is sometimes vague, as explained below.

- 3.1.1** In cases where the router is owned by the entity, DIS service stops at the router; although, historically, the demarcation point has not always been clear.
- 3.1.2** For institutes of higher education, DIS service stops at the campus router, unless the DIS network service agreement states otherwise.
- 3.1.3** In cases where DIS owns the router, DIS service extends to the Ethernet interface of that router.
- 3.1.4** DIS offers network support to the Arkansas Public Schools. DIS network service responsibilities extend to the public school's Ethernet interface.
- 3.1.5** This policy seeks to address or remedy trouble areas that have been identified on the state network.

4.0 References

- 4.1** Arkansas Code 25-4-105: Department of Information Systems – General powers and duties.
- 4.2** Arkansas Code 25-4-109(d): Information technology centers

5.0 Policy

- 5.1** Entities will abide by the state network service agreement with the Department of Information Systems (DIS).
- 5.2** An agreed upon demarcation point is established in writing with each new service implementation or renewal of each existing service agreement.
- 5.3** DIS will have access necessary to control the configuration of the equipment providing the network service; access will be permitted up to the demarcation point.
 - 5.3.1** Justification: The demarcation point between an entity's local area network (LAN) and DIS operational responsibility is sometimes unclear. This is especially true in cases where entities purchase their own routers.
- 5.4** Inside the demarcation point (typically the Ethernet portion of the network), network management is the responsibility of the participating entity unless stated otherwise in the entity's network service agreement with DIS.
 - 5.4.1** Typically, DIS is not responsible for any cabling on the entity's side of the agreed upon demarcation point.
- 5.5** Each entity is required to designate a primary contact whom DIS support staff may contact via phone or email to assist in resolving network issues.
 - 5.5.1** Recommendation: For agencies with multiple divisions, the primary network contact should maintain a list of second-level network contacts from the individual field offices.
 - 5.5.2** Recommendation: The designated contact(s) should have a general understanding of the entity's network design.
 - 5.5.3** Justification: Many of the smaller entities on the State Network do not have a designated network contact person, this makes it difficult to resolve and troubleshoot network problems.
- 5.6** Entities will implement networks that are practical, and that will meet their needs; in addition, entities will have resources available to provide basic network maintenance. Entities will consider the on-going maintenance costs associated with providing adequate technical support for all new network implementations or upgrades.
 - 5.6.1** Justification: In the past, some state entities have implemented excessive network infrastructures that could not be supported and maintained by local support staff.
- 5.7** Entities on the State Network will take proper steps to minimize wide spread virus attacks. If an entity is negligent, unwilling, or unable to take proper protocol steps to minimize a wide-spread attack, they are in jeopardy of being removed from the State Network until the vulnerability has been identified and resolved.
- 5.8** Entities will ensure that there are sufficient authentication and access control mechanisms to allow only authorized access to network resources.
- 5.9** Entities will not conduct non-authorized port scanning activities beyond their demarcation point (outside the entity's local area network). These are considered hacking activities and are prohibited on the State Network.

- 5.10 Entities receiving Internet access through the State Network are not permitted to provide offsite or dial-in Internet access to persons outside their service area.
 - 5.10.1 Entities receiving Internet access through the State Network are not permitted to provide or resell this service to the community at large.
- 5.11 If the State Network personnel detect any type of network activity that adversely affects other entities, DIS will notify the instigating entity of the problem. If, after notification, the instigating entity is negligent in rectifying the issue, or is unable or unwilling to do so, DIS has the authority to disconnect the entity from the network, until the problem has been resolved.
- 5.12 It is recommended that networks be designed according to network standard specifications from IEEE.
 - 5.12.1 Networks should adhere to the following industry standards: Cabling - CAT5E UTP or better; Ethernet - IEEE 802.3; LAN protocol - TCP/IP; Wireless LAN - IEEE 802.11b; LAN device connectivity – Switching.
 - 5.12.2 Where industry standards do not exist, networks should follow the de-facto product standards.

6.0 Procedures

- 6.1 Entities shall abide by their Department of Information System's (DIS) Network Service Agreement.
- 6.2 Each entity on the state network shall designate a network contact person whom DIS support staff can contact via phone or email to assist in resolving network issues.
- 6.3 Entities with a DIS Network Service Agreement shall take necessary actions to ensure that all their network users shall abide by this Agreement.
- 6.4 Entities with a DIS Network Service Agreement shall take necessary actions to ensure that their sub-entities receive and adhere to this Agreement.
- 6.5 Entities which are not immediately able to provide compliance with this policy must have a plan, within 90 days after this policy goes takes effect, that includes a target date for compliance.

7.0 Revision History

Date	Description of Change
08/30/2002	Original Policy Statement Published
07/15/2005	Link updates, header updated

8.0 Definitions

- 8.1 Ethernet: The most widely-installed Local Area Network (LAN) technology. Specified in the standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wire. The most common Ethernet systems are called 10BASE-T Ethernet systems and provide transmission speeds up to 10 Mbps. Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems, supporting workstations with 10BASE-T cards. Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second.
- 8.2 Demarcation Point: The distinct separation point (or boundary) between entities. That point at which operational control or ownership of communications facilities changes from one organizational entity to another.

- 8.3** Service Area: An entity's service area personnel are eligible to receive remote Internet access if that access is required to support projects, tasks, and goals set forth by the entity.
- 8.4** Local Area Network (LAN): A local area network is generally a private network. It is under the control of the owner and used by a set of related individuals and/or workgroups, typically within a single building or over a group of neighboring buildings. LANs are groups of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).
- 8.5** Router: On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each Internet point-of-presence. A router is often included as part of a network switch.
- 8.6** Switch: An internetworking device that intelligently segments networks to increase overall bandwidth, isolate traffic and provide an interface to high-speed networks. The switch selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router (see section 8.3) In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.
- 8.7** Virus: Software used to infect and harm a computer. A virus buries itself within an existing program. Once that program is executed, the virus code activates and attaches copies of itself to other programs, which in turn, again replicate the virus when executed. Viruses can damage or destroy data, software, the operating systems, and hardware.
- 8.8** Wide Area Network (WAN): A geographically-dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately-owned or rented, but the term usually means the inclusion of public (shared user) networks. A wide area network connects local area networks to one another, generally using public infrastructure or services. The connections are made using the shared public infrastructure, public infrastructure leased for private use, and, sometimes, private infrastructure (e.g., fiber) with public services.

9.0 Related Resources

- 9.1** State Contract Information for LAN equipment: The LAN contract covers Ethernet driven devices consisting of hubs and switches and all hardware and software ancillary to these devices. http://fiscal.state.ar.us/wan_home.html

10.0 Inquiries

Direct inquiries about this policy to:

Office of Information Technology
Shared Technical Architecture
124 W. Capitol Ave., Suite 990, Little Rock, AR 72201
Voice: 501-682-4300
FAX: 501-682-2040
Email: SharedArchitecture@arkansas.gov

OIT policies can be found on the Internet at: <http://www.cio.arkansas.gov/techarch>