SNS Networking at BNL

BNL/SNS TECHNICAL NOTE

NO. 056

J. Smith

January 24, 1999

ALTERNATING GRADIENT SYNCHROTRON DEPARTMENT
BROOKHAVEN NATIONAL LABORATORY
UPTON, NEW YORK 11973

SNS Networking at BNL

John Smith

Jan 24, 1999

Introduction

The SNS project at Brookhaven National Laboratory will utilize people from several departments. While a majority of the people are from the AGS department, some are from RHIC, Information Technology Systems, the National Synchrotron Light Source, and other departments. People will be situated in several buildings around the site, each building having its own networking hardware. There will be several control system development laboratories in the AGS department, RHIC, the NSLS and other buildings. In addition engineering and physicists will need access to central SNS computers used by the controls group. The network must give all SNS personnel easy computer access to all the components of the control systems.

Requirements

The following summarizes the network requirements for the SNS at BNL.

1) SNS people will be located in several buildings at BNL. Many will need access to the SNS control system workstations and IOC's.

2) Each building has its own network configuration. Some may have restricted access, for example firewalls installed, which tend to restrict access to computers outside the building.

3) BNL is developing just a portion of the SNS Integrated Control System. Other portions are being developed by other laboratories,(Los Alamos, Berkeley, ANL and Oak Ridge). We need to share development software and therefore need to allow off-site access to SNS control system computers from the collaborating labs. This is particularly true for the setup of the development environment. We need to allow access from outside collaborators without compromising security.

4) The network should simulate to the extent possible the network to be installed at Oak Ridge. This will ensure the systems delivered will operate at Oak Ridge without reconfiguration.

5) We need to verify the performance of the control system. The program response to operator commands or the time it takes to read and display data are of concern. We wish to demonstrate and optimize if necessary the system performance before delivery. This means the network must support 100Mhz connections to IOC's and workstations. It should also support a high performance (ATM or Gigabit ethernet) backbone.

6) The network should be easy to maintain. IOC's and workstations will occasionally have to be moved to various locations for testing and demonstrations. Reconfiguring the network via a software database change is preferably to having to change computer configurations(IP address, gateway address, name servers etc.)

7) The SNS network architecture will likely not be chosen for two years. Network technology is changing rapidly and the hardware chosen today will not necessarily be the choice made two years from now. While the use of 100Mhz Ethernet is becoming common for the desktop the choice for the backbone is still not decided. For the backbone we still have a choice of 100MHz Ethernet, 1Gig Ethernet and ATM(OC3 & OC12). The new network should allow for the installation of new hardware to check out the performance of a different architecture (e.g. gigabit ethernet) before final decisions are made.

8) The SNS will have X-terminals, PC's, IOC's, Workstations and printers. Most of the SNS computers should be on the same subnet. This will allow the use of broadcasts wherever convenient. Bootp for IOC or Xterminal startup as an example.

9) Netmeeting software is being used by the ICS working group for computer conferencing between laboratories. The setup of the BNL network should allow communicating using netmeeting with computers at the other labs. This may require two networks, one for protected nodes and a second for public access.

10) The security of the network will have to be maintained. While security for the SNS computers is not expected to be a serious concern at least early in the project, SNS personnel will be working in areas where security must be maintained. If security is lax, hackers can invade the network and cause damage to computes on other networks. Each group is expected to maintain security to ensure that the security of the whole network is maintained. Firewalls, SecureID cards, Secure shell and other options will be considered. The goal is to have maximum security without making it difficult to meet the other requirements above.

DESCRIPTION

Figure 1 is a simplified diagram showing the possible distribution of computers at BNL for the SNS project. This is not a final configuration but is based on the initial placement of controls staff. As space becomes available and more personnel are brought to the SNS project other buildings may be added to the configuration. It is necessary to have a system that accommodates the anticipated requirements but is also sufficiently general such that it will handle changes. The figure shows that there will be laboratories and offices with computers in several buildings distributed around BNL.

Figure 1 also shows the configuration of the BNL networking. The ITD department maintains the BNL network infrastructure that interconnects the building and different departments at BNL. Until recently all buildings were connected via an FDDI backbone. Recently BNL has started converting to a ATM backbone. The AGS and NSLS departments are presently connected via ATM. Other buildings are still connected with the FDDI ring. The buildings connected via the ATM network will normally have been updated at least partially to a switched ethernet system. Switched ethernet not only gives greater performance but the hardware being newer provides new features. Fortunately most of the SNS personnel will be located in buildings (AGS, CCD, RHIC, NSLS) which have updated hardware. The NSLS, where the control system will be developed has replaced much of the older network hardware with switched ATM and switched Ethernet hardware(fig 2).

Recently the ITD department has been deploying backbone equipment that supports the use of Virtual Lans (VLANs). Virtual Lans take the place of physical lans. Any combination of ports on any set of switches in any building can be associated as a broadcast domain and assigned to be a subnet. Previously a subnet was constrained to be in one physical location, one building, one floor of a building etc. It would have taken a large investment in cabling, hubs and routers to have a subnet that spanned several buildings and coexisted with other subnets. The new Ethernet switches purchased by ITD and the NSLS does support VLANs. This will allow us to use VLAN technology to create an SNS subnet spanning mutiple buildings.

BNL has assigned to SNS a subnet with 256 addresses. One subnet will probably be sufficient but another can be obtained if necessary. The subnet will be given the sns.bnl.gov domain name. Another subnet will be needed if we decide a public and private SNS network is needed. This could be the case if we wish to have an secure and insecure network.

The ITD networking group will program the central and local switches so that the sns.bnl.gov network is supported wherever needed. While the ITD group supports and encourages VLANS it is up to the departments to purchase and deploy the network equipment needed.

While the larger buildings at BNL support the new technology some of the smaller buildings do not. Since we plan to locate some labs in these smaller buildings we are making plans to upgrade the networking to meet our requirements. The trailers shown in figure 1 are an example of a location still using shared hubs and which does not support high speed (100MHz) networking. The internal network will be upgraded by installing Cat-5 cabling and ethernet 10/100Mhz switches where needed.

VLANS allow easily moving nodes to different locations. When a computer is moved normally the IP address, gateway and name server would have to be changed because the new network would be on a different subnet. This is a problem because the control system relies on broadcast data and broadcast data does not normally get transmitted through routers to different subnets. With VLANS, changes in the computer configurations are unnecessary when moving between buildings as long as we move between ports on the same network. The network group can change the configuration of the network with software. Any port on any switch in any building can be added to the sns.bnl.gov subnet if needed. This can be done from the network administrator's office over the network. No physical changes have to be made. After the network configuration is changed, the node is moved to the new location and connected to the assigned port on the appropriate switch. In general ports on switches in buildings used for SNS can be preprogrammed for the SNS subnet.

For the first installations some ports on the NSLS and CCD switches will be programmed to use the SNS subnet. The building 725 hardware can be expanded by the installation of boards to the Cisco 5500 switch to provide the capacity needed. The building 728 switch has VLAN capability but the switch has to be updated to bring 100MHz to the building and to increase the number of ports. The network to the trailers has not been upgraded and cannot support switched ethernet, 100Mzh ethernet or VLANs. The network to the trailers will be upgraded by the installation of a network switch and a fiber connection to the ATM switch in building 725. The existing ATM switch can be upgraded as needed by adding ATM ports.

We are still in the process of evaluating the requirements for the other buildings that are likely to be used for SNS development. This is difficult for two reasons. Firstly, it has not been firmly established which buildings will be used by SNS. Secondly, the BNL network upgrade is continuing. Some of the buildings that are likely to be used by the SNS may be upgraded in the coming year. We will be working with the ITD department to coordinate our efforts and minimize costs to all projects.

Firewalls can easily be installed between the SNS subnet and the outside network. We plan on installing a firewall as shown in Fig 3. We are working with ITD on the installation of the firewall. The goal is to allow us to meet the requirements list above without imposing undue restrictions. We wish to allow specific computers at the collaborating institutions access while inhibiting the general public. We will control the configuration of this firewall and be able to enable any special protocols needed. For example we can enable the netmeeting protocol for selected hosts. We can add nodes to an public network if outside access is needed to a large number of users but do not expect this will be the case. We will also look into SecureID cards and Secure shell since one-time passwords are strongly recommended by BNL.

The ITD department is in the process of installing Gigabit ethernet switches. Later in the year BNL will have experience with this technology and SNS will have the opportunity to incorporate gigabit hardware into the system if desired. We will not require gigabit speeds for the local control system needs however it will be available for testing is we so wished. In fact with the recent increase in network bandwidth, from a shared 10MHz network to switched 10MHz and now to switched 100MHz systems, the network bandwidth should be more than adequate.

Summary

Building a computer/control system that is distributed in several buildings around the lab could have been difficult except for recent advances in network technology. Recent and planned changes in the network hardware at BNL will allow us to meet the network requirements for the SNS. We are working closely with the ITD, NSLS, AGS/RHIC departments to make sure that the network hardware will have the capability needed. Working very closely with collaborators at labs around the country offers other challenges. We wish to give remote access to SNS computers while maintaining good security. We are in the process of testing with the ITD department a firewall on the SNS network with the goal to provide security without unduly hindering access or slowing productivity.

We are planning the installation of cabling and the purchase of network components to provide the capability needed. This process will continue over the next year.

Simplified Network Diagram (AGS, NSLS, ITD)

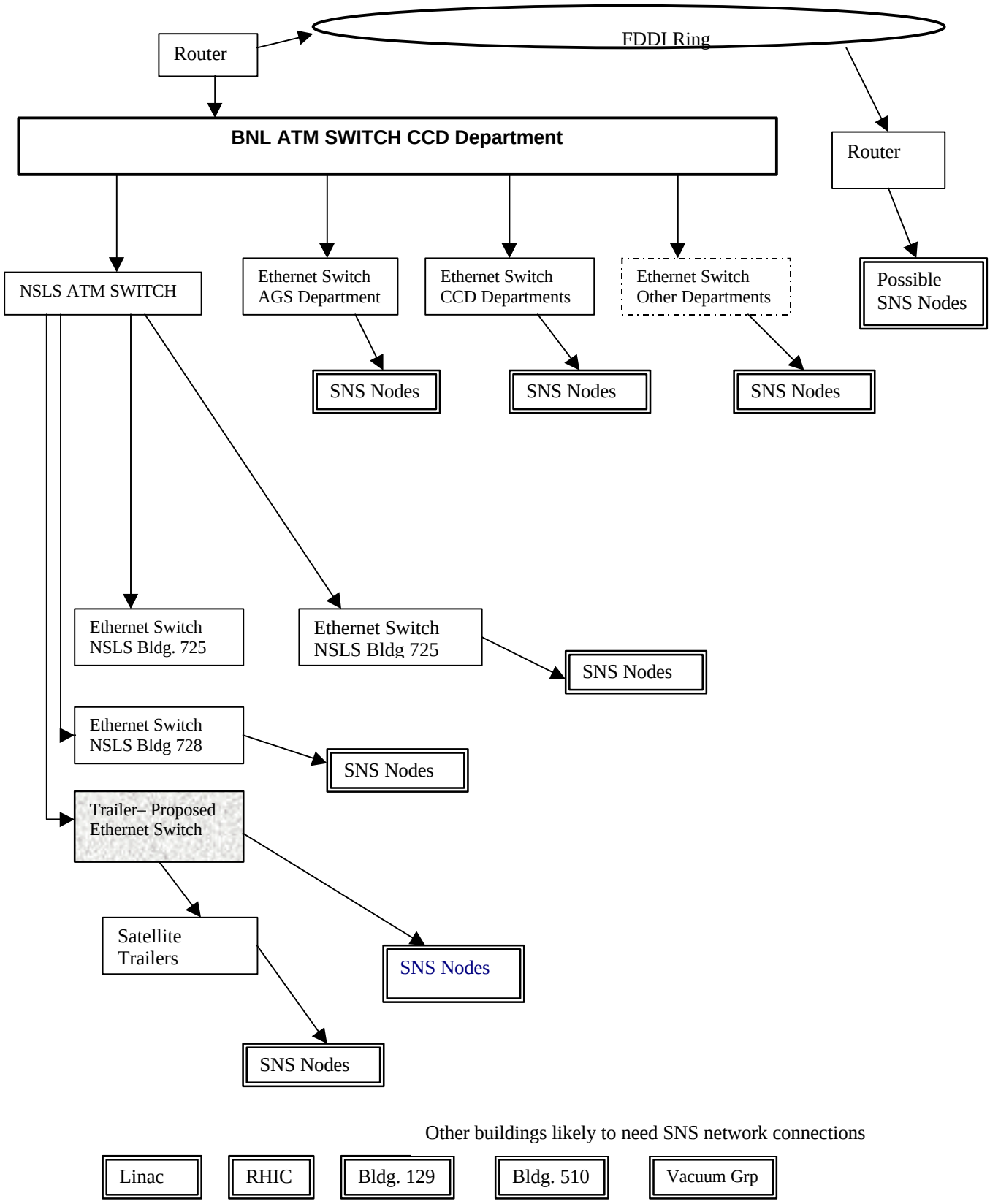


Figure 1.

NSLS Network Hardware Configuration

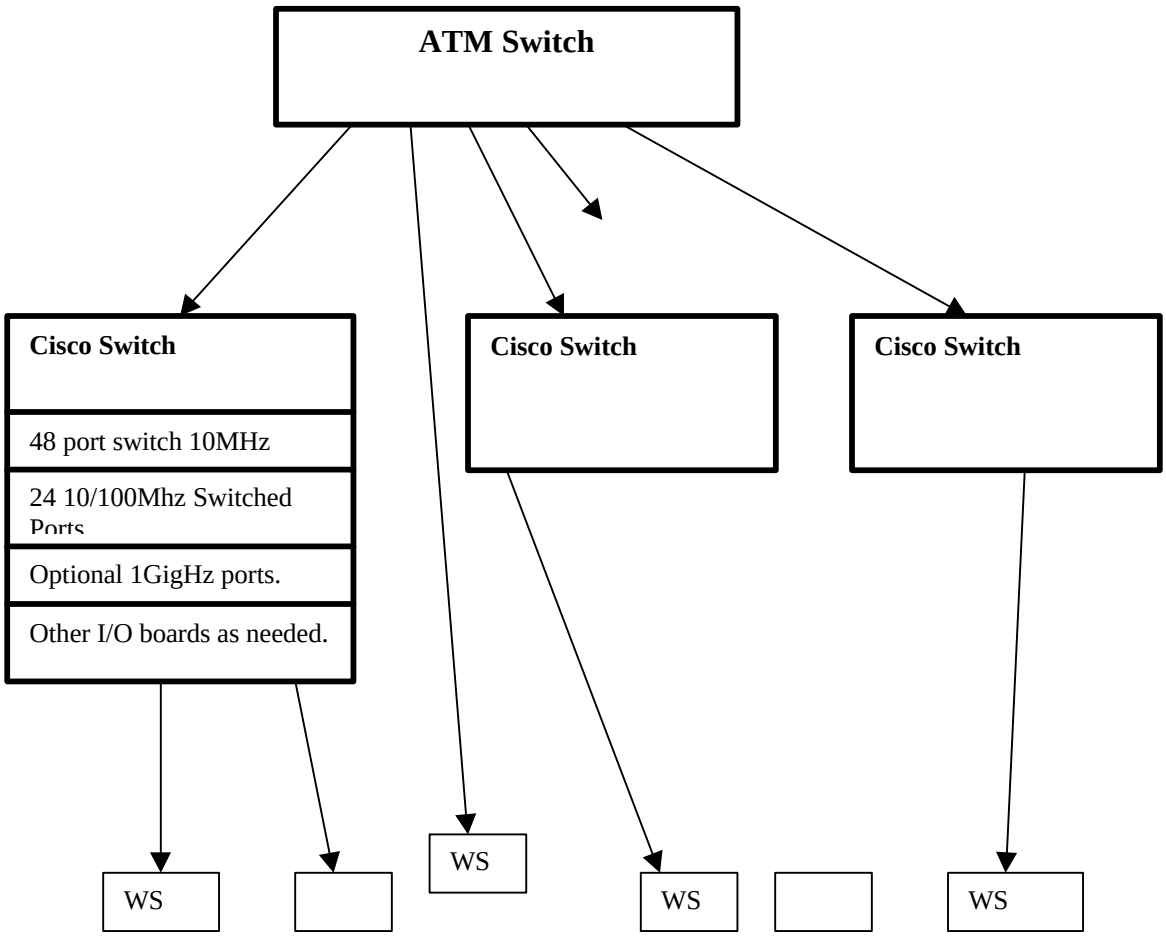
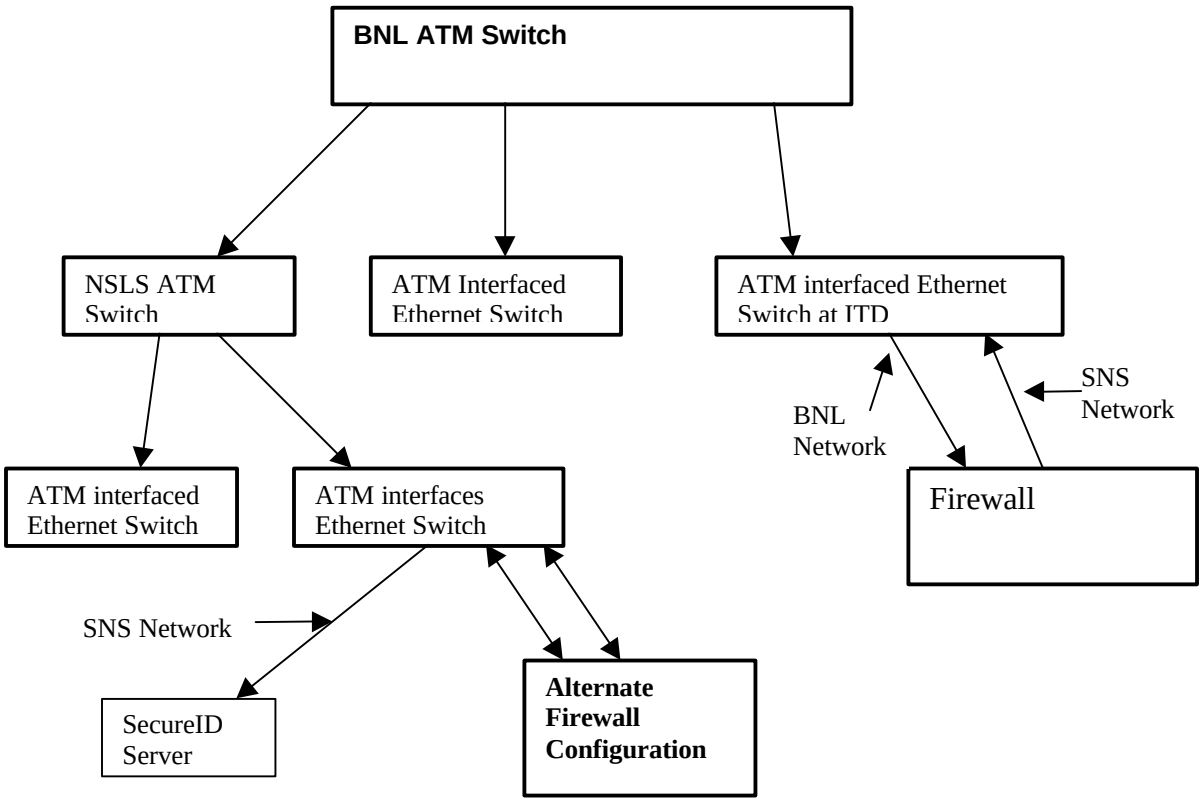


Figure 2

SNS Network Security



A Firewall can be added to the system whenever needed. With the use of VLANs the firewall can be placed at any convenient location.

A SecureID server may be used to enable access to the SNS network from users outside of BNL. During the development phase extra security will probably not be needed but it can be installed if deemed necessary. SecureID requires one-time password cards to access the network.

Figure 3.