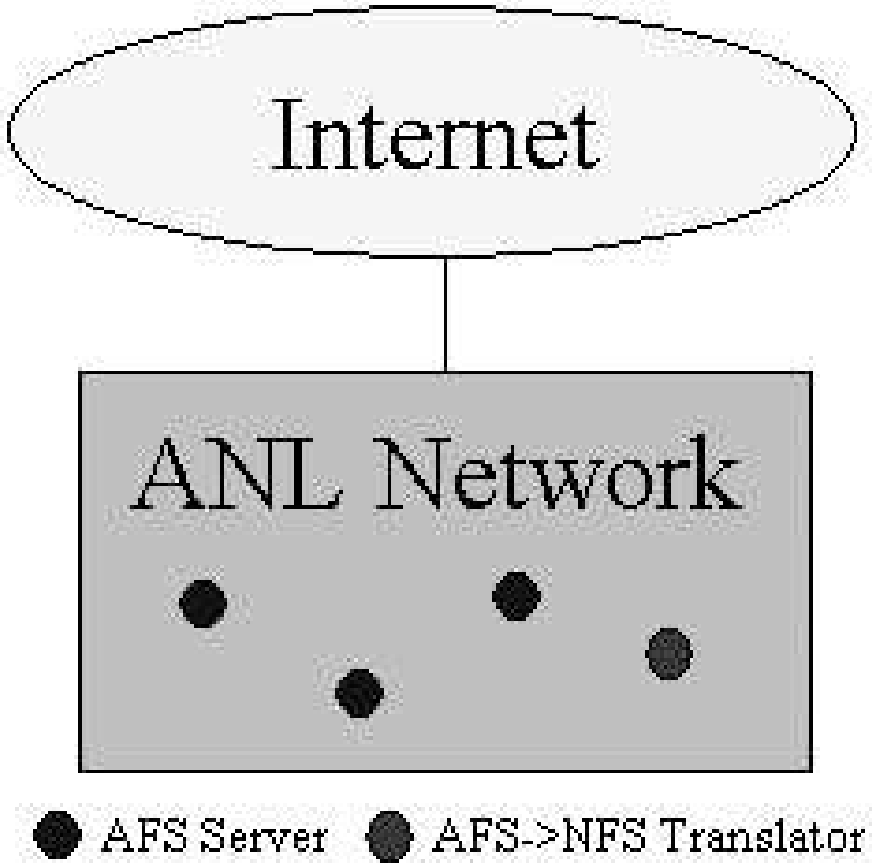
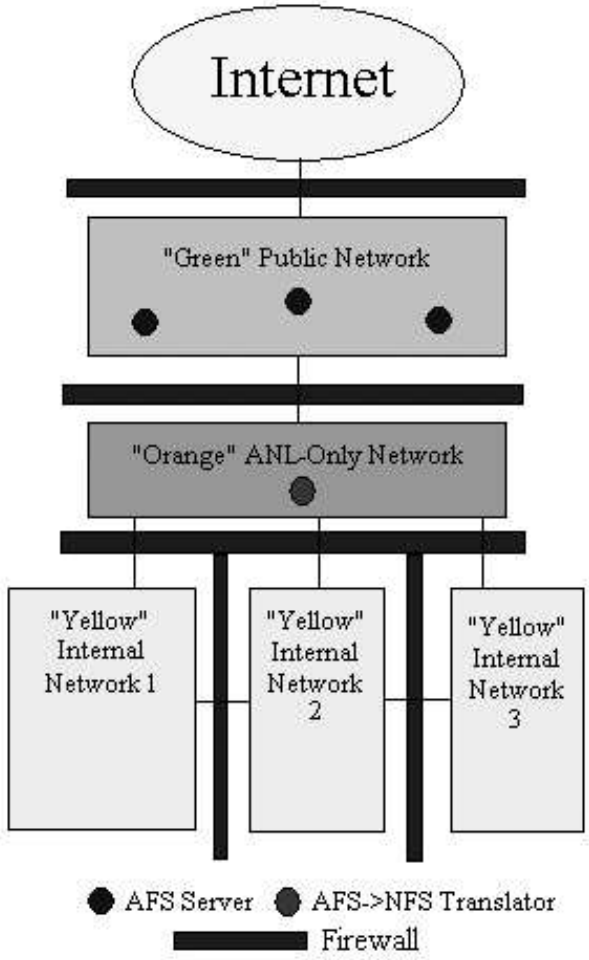
# *AFS and Firewalls*

*Brian Sebby*
*Electronics and Computing Technologies*
*Argonne National Laboratory*
*November 4, 2002*


# *Argonne's Network – Pre-Firewall*



# *Argonne's Network – Post-Firewall*



# Network Configuration

- AFS Servers are in the Green network, which is available to all hosts, both internal and External.
- AFS->NFS Translator is located in the Orange network, which is available to all ANL hosts, including all of the private Yellow networks, but not to the outside world.
- Conduits need to be created in the firewall to allow the AFS traffic to pass through.
- Conduits needed for the AFS servers:
  UDP: 7000-7009 (7020-7021,7025-7032 used for backup)
  88, 750 required for Windows AFS clients
- Conduits needed for the AFS->NFS Translator
  UDP: 111 (sunrpc), 2049, 7009, >1024 for talkback
  TCP: 2049
- Conduits needed for AFS->NFS Translator using Sun WebNFS:
  TCP : 2049
  Mount the AFS filesystem using the command:
  mount nfs://afs-translator-name:/afs /afs

# Common Problems

- The various utilities (klog, fs, vos, etc.) will use random ports >1024 UDP to communicate with the servers. However, most firewalls should allow this if the initial communication ports (7000-7009) are first contacted to initiate the data transfer.
- New conduits may be needed in unusual situations. Using your firewall's logs in the best way to find out why communication is being disrupted – we discovered that we needed to open up UDP ports 88 and 750 only after users complained that they couldn't use their Windows clients outside of the firewall. The NT/2000/XP client uses 88 UDP (the KRBv5 KDC port), while the Windows 9x client uses 750 UDP (the KRBv4 KDC port).
- NFS will want to use random ports for communication. It will not always talk to a standard port initially, so you may need to open up every port >1024 on your NFS translator unless you use Sun's WebNFS mount type, which maintains the communication on port 2049 TCP.

# Future Plans

- Tests have shown that AFS file servers existing in a private network can be restricted to use in just that network.
- The conduits allowing outside access to Green AFS servers (which are currently both our database and file servers) will allow file servers to communicate where volumes are on their disks, but not allow outside cache managers to access their data unless they are in the same private network or if conduits are created for specific hosts.
- Future plans include setting up an ANL-only file server in our Orange network, and internal file servers for individual divisions (the Yellow networks) that can only be accessed from within that division.

# *Potential Future Layout of Argonne's Network*