Operational Procedures for Ethernet Private Networks

Rev 1.5 (published 02/28/19)

Network Infrastructure and Services (NI&S) encourages the use of NI&S installed and managed Ethernet portals for all connections to the campus network. However, there may be cases where a user wishes to set up a private network of Ethernet hosts connecting to the campus network via a single managed portal. NI&S permits the connection of these wired local area networks (LANs) to the campus network under certain conditions.

All private networks are required to be registered. By doing so, you are implicitly agreeing to the “Conditions of Use” (link) which outlines responsibilities of LAN operators and NI&S. .

What Qualifies as a Private Network?

A typical connection to the campus Ethernet network is a single host (e.g. computer or network connected printer) with a single Ethernet Media Access Control (MAC) address attached to a NI&S-managed network portal via a NI&S-provided Ethernet jumper cable. A private LAN constitutes any connection to the campus network that is either multiple individual hosts (machines utilizing a private switch, including virtual hosts utilizing a hypervisor layer of software to provide “guest” systems and/or router for access to the NI&S maintained network) or hosts with multiple MAC addresses (as in a virtualized environment). This includes:

- 10/100 megabits per second (Mbps) and/or 1 gigabit per second (Gbps) hubs and switches;
- Routers, wired and wireless;
- Ethernet repeaters;
- Other devices enabling multiple machines to simultaneously connect to a single wall jack; and/or
- Software that emulates multiple Ethernet stations on the same physical computer, e.g. hypervisors.

NI&S recognizes many legitimate use cases for such networks including, but not limited to:

- Testing and securing devices before deploying to the public network
- For “intranet-like” file sharing
- For higher bandwidth on such an intranet
- To implement virtualization
- To restrict access by means of a firewall or other middlebox device
- For ease of management of multiple machines, such as in labs
- To provide quick and easy access for university guests
- To provide a service or use case that NI&S cannot currently provide

Publicly routable IP addresses versus Private (RFC 1918) addresses

Those who wish to utilize private network connections (PNCs) must do so with private Internet Protocol (IP) addresses conforming to Internet Engineering Task Force (IETF) Request for Comments (RFC) 1918 since IPv4 address space is in very short supply at Virginia Tech. PNC’s that require access to off campus services have the following options.

- Allocation of VT globally routed IPv6 addresses
- Allocation of NI&S campus routed RFC-1918 addresses (172.16.0.0/12) in conjunction with dynamic Network Address Translation (NAT) services now in use at the campus border.

Registration

Departments may register private LANs through their departmental liaison. When ordering the private network connection, operators will need to know the network portal number where the LAN connects to the campus network. The portal number should be labeled on the portal faceplate. A registration fee applies for each order, but the fee is designed to provide flexibility for the users while covering the associated infrastructure and maintenance costs incurred by NI&S.

This program is not intended to replace managed ports provided by NI&S and bandwidth monitoring (sustained and peak measurements) will be engaged on all registered ports to ensure use does not negatively impact other network traffic within the building. Increased traffic needs could be accommodated by a graduated fee if a sustained need is required.

NI&S reserves the right to disable any Private Network connection from accessing the public network if the connection activity is deemed to be negatively affecting either the performance or security of the shared network. NI&S will work with departments to minimize impact loss of such a connection would have on operations.

Wireless Routers

Students are not permitted to connect personal wireless routers to the Virginia Tech network in buildings with Virginia Tech wireless service. Each residence hall room has one active 1 Gigabit per second (Gbps) wired network portal. Residents may purchase an Ethernet switch to provide more *wired* network connections.

Faculty and staff are prohibited without permission from NI&S from using wireless routers due to interference and security issues. NI&S will work with all units to assess needs and ensure proper technical and security implementation where situations warrant the use of a private wireless systems. Periodic, unannounced audits and RF surveys will be conducted by NI&S staff to ensure compliance with this policy.

Unregistered private wireless networks will be documented and NI&S staff will engage with departmental communications and network liaisons to resolve potential issues. Some of these will likely be the result of misconfigured devices or unintended open networks from printers or other devices that need defaults (which are usually set to “open”) reset. NI&S staff will endeavor to assist in securing such networks, including consulting on proper channel and frequency use, whenever and wherever possible.

Disclaimer

NI&S reserves the right to disconnect any device or private LAN from the network that negatively impacts the performance of the campus network. For example, NI&S may disconnect the private LAN if a machine on the private LAN is misconfigured in such a way as to cause significant disruption to the campus network or creates security vulnerabilities or events. IT Security Office policies apply to these ports as they do for all NI&S managed ports. Before disconnecting any service, NI&S will attempt to notify the registered contact person when possible. The goal is to trace these types of issues as quickly as possible.

Regulations and Enforcement

The operation, maintenance, and troubleshooting of the private LAN is the sole responsibility of the private operator. At the request of the department or operator, NI&S may assist in troubleshooting efforts. Dependent on the level of effort required, this assistance may trigger a fee or charge for services.

Similarly, any cabling or other infrastructure installations required to instantiate a private network must conform to building and safety regulations as interpreted and enforced by the University Building Official. Inspections conducted on any part of a building may bring this cabling and infrastructure in scope. Violations will be cited and mitigation could include removal of said infrastructure. NI&S can be contracted to provide consulting and/or installation services to ensure compliance with all regulations.

Operators of private LANs must also comply with the rules and specifications governing the design of computer networks as described by the IEEE 802.3 standard. Failure to do so will result in degraded performance on your private LAN and between your private LAN and remote networks on campus or via the Internet. Access to your private LAN from machines on remote networks may be similarly affected. For more information about this visit http://www.ieee.org/.

Glossary of Terms:

Portal: Ethernet connection point generally located on a wall, ceiling, floor or patch panel within the users' workspace or office. A portal will be identified with a label that may read something like 203TP01B, 984DA1700F.

Private LAN (PLAN): constitutes any connection to the campus network that is either multiple individual hosts (machines utilizing a private switch/or router for access to the NI&S maintained network) or hosts with multiple MAC addresses (as in a virtualized environment).

Private Network Connection (PNC): An Ethernet service provided by NI&S for the purpose of connecting a PLAN to the university data network.

Private Ethernet connection (PE): An ethernet connection that has been offered by NI&S for several years for the convenience of customers. Unlike the PNC, this connection is for less business critical connections and will be treated differently during security incidents (see Guidelines below)

Process Guidelines for Security Incidents involving Private Network Connections

Rev 1.1; Issue date 02-28-19

Purpose -

Define procedures for handling security incidents pertaining to network outlets with NI&S Private Network Connection (PNC) and legacy Private Ethernet (PE) services. (See definitions above.)

Scope -

This applies to all Private Network Connection and Private Ethernet services. A security incident may include a violation of the Virginia Tech Acceptable Use of Information Systems Policy or other activity deemed as a violation of other applicable policies or law.

Responsibilities

ITSO personnel will determine the impact level of each reported or discovered incident.

This procedural document addresses HIGH level incidents ONLY.

Critical cases will continue to result in termination of access immediately, including after-hours and on weekends/holidays, as this often means outflow of data is actively occurring.

Procedure

- The IT Security Office (ITSO) receives a report of or discovers a violation.
- ITSO determines the validity of the information, then classifies the severity of the incident.
- ITSO creates a ServiceNow (SN) incident containing relevant data and severity level.
- IT Experience & Engagement (ITEE) E or NI&S Network Engineering Operations (NeO) performs analysis to determine the location and responsible parties of the identified system or host (drawn from Network Liaison data. The Abuse contact, and primary and secondary contacts will be provided. Goal is to provide three unique individuals' info for contact.).
- If the identified system is a member of a PNC, the Information Center will attempt to contact the responsible parties as follows:
    - Make 2 attempts via all available methods - ServiceNow, email, office phone, mobile phone.
    - If contact is made, allow responsible party to resolve the issue.
    - If the responsible party directs NI&S to administratively disable the service, comply with the request.
    - If contact is not made within 20 minutes (Individual contacted must only acknowledge receipt of the ticket or voice call to avoid disabling of the port), or if the issue is not resolved in a timely manner as determined by the ITSO, NeO will administratively disable the service for

that outlet. (Contacted individual need only acknowledge the call or email message to avoid the portal being disabled.)

- ServiceNow incident will be updated
- Port description will be appended with the SN Incident number

- If the identified host is a member of a PE:
    - NeO will administratively disable the switchport used by the PE
        - ServiceNow incident will be updated
        - Port description will be appended with the SN Incident number
    - Information Center will attempt to make contact with the responsible parties as follows
        - Make 2 attempts via 2 different methods (ServiceNow, email, office phone, mobile phone) over three days.
    - User may contact the Information Center realizing there is a problem. Standard incident processes will reveal that the port is disabled due to a security incident.