

SUPERNET SHARED VPN - PUBLIC IP ADDRESSING STANDARD

Category:	Network
Effective Date:	September 2004
Review Date:	January 2007

Summary:

All Alberta Learning sites will use public (registered) IP addresses between the Customer Edge Device (CED) and SuperNet Edge Device (SED) when participating on a SuperNet VPN with other organizations.

Specification:

In order to support connectivity across all government agencies using SuperNet, public (registered) IP addresses will be used between the CED and SED when participating on an external or public SuperNet VPN with other organizations (see notes):

- Public IP addresses must be used when connecting to external or public SuperNet VPNs either from any of the organization's locations or from the organization's hub, if using a hub and spoke network model.
- If the organization is using a firewall at the hub location, the use of public addresses would be outside of this firewall.

Rationale:

- The use of private IP addresses will not ensure uniqueness.
- The use of public IP addresses will ensure that there are no conflicts in addresses when connecting to other users within or between sectors.
- Government, Learning, Health, Libraries, and Municipalities (GLHLM) agencies have agreed to use public IP addresses.
- Connections outside of the GLHLM user group will also be free of conflicts through the use of registered IP addresses by the GLHLM users.

Timeline:

This standard becomes effective immediately and must be implemented at the same time that each learning site is connected to the Alberta SuperNet.

Notes:

- The organization can continue to use non-registered IP addresses within the organization's private network. However, when connecting to SuperNet with the intention of sharing information with any other cross-sector organization, each organization must adopt the use of public IP addresses.
- A proposed central organization to handle the assignment and distribution of new IP addresses is under consideration.
- Network address translation (NAT) to a public address can be used for private IP addressed networks participating on an external or public SuperNet VPN.
- A VPN can be classified in three ways:
 - Internal or Intranet VPN - no external nodes (outside the jurisdiction or institution), with exception of shared service
 - External or Extranet VPN – two or more organizations participating as members, all IP addresses must be public
 - Public VPN - connects to Internet or other public network, must use Public IP addresses

Contact:

Technology Standards Office (TSO)
Stakeholder Technology Branch
E-mail: tso@learning.gov.ab.ca