UT System Network Temp

We've all encountered issues reaching sites across the network. Are there things we can do within UT System to ameliorate issues?

What are the network related issues we face collaborating across institutions?

1. Network security restrictions interfere with traffic by design in order to improve security (ex: firewalls, router ACLs, IDS/IPS). Those can have unintended consequences.
2. Network bandwidth may be insufficient for some delay sensitive applications (ex: voice/video).
3. There is no definition of shared UT System applications or their network requirements. (TCP/IP port ranges, address ranges, policies etc)
4. There is no inter-institutional network contract lists or procedures to troubleshoot network connectivity problems.
5. Lack of technical expertise for vendors, application owners, end users, and sometimes network staff.
6. Lack of vendor documentation on network use (ex: TCP/IP ports and protocols utilized/required, bandwidth requirements).
7. Lack of technical expertise for end client network configuration and coordination with networking groups (ex: duplex settings and port errors, client firewalls).
8. Collision of security policy domains and resources-- security exclusive (ex:VPN required to connect to service, Layer 2 connectivity requirements, use of private address spaces).
9. Lack of application and service change control and notices (see #5,6,7 -- service upgraded without testing and consulting with networking, security and applications).
10. Differing goals/priorities/requirements between those involved (ex: applications owners v. Institution Network v. Institution ISO v. End Users v. System Network).

How can we improve?

1. Secured wiki site of UT System shared applications and their network profiles/desires.
2. Network contact list of each institution and troubleshooting guidelines (how to start a debugging process), and listservs.
3. Network review board for UT System shared applications (new applications and changes must pass the review board which can ensure implementable systems that are not security exclusive). Non-reviewed applications can of course be used (most will not be reviewed) but they won't have the same level of attention to ensure they work.
4. UT System funded network assistance to work with shared applications and their support/vendors to determine network requirements ?[likely some FTE time needed].
5. Email lists for notification and discussions regarding shared applications.
6. Scheduled windows for changes to shared applications.
7. Create templates for popular security devices to support shared applications (ex: Cisco/Juniper firewall configuration stanzas).
8. Agreement on inter-institutional QOS traffic marking guidelines.
9. Develop security blocking monitoring system. [Custom development. Deploy nodes to all institutions and application locations reporting back to a central server. Have the server and nodes probe the defined ports and escalate changing conditions (such as using nmap). Provide a console for all institutions to monitor and log these changes. Should institution X change port 8922 required by sanctioned applications that would be escalated to ensure that was intentional and alert all parties -- including application owners.] (ex: Multicast beacon, Internet weather-maps).
10. Training/documentation and appropriate tools to assist in testing and troubleshooting (ex: NDT, iperf, nmap). Not just networking staff, but application owners/debuggers.