

ITaP Administered Subnets Port Restriction Plan and Purdue Subnet Port Restriction Plan

This document adds to the following existing documents:

- ResNet Security Plan
- ECN Network Security Plan
- Computer Sciences Port Restriction Plan
- AgIT CES/IHETS Port Restriction Plan

In the initial phase of this implementation, ITaP will implement measures to prevent attacks against computers on ITaP administered networks. These measures are Microsoft Remote Procedure Call (RPC) and NetBIOS service port restrictions. These port restrictions are part of the overall implementation plan to block direct off-campus network access to these ports for the entire campus network. The tentative schedule for implementing these port restrictions is May 12th, 2004 for ITaP networks and May 26th, 2004 for the entire campus.

Purdue ADSL connections and Purdue modem pools will be considered to be part of the campus network. Future updates to this plan may re-define these groups as external to the campus network for purposes of port restrictions.

ITaP Administered Subnets

The following subnets are currently ITaP administered:

128.210.0.0	128.210.17.0	128.210.40.0	128.210.105.0	128.210.191.0
128.210.1.0	128.210.22.0	128.210.47.0	128.210.106.0	128.210.192.0
128.210.5.0	128.210.25.0	128.210.59.0	128.210.107.0	128.210.193.0
128.210.6.0	128.210.26.0	128.210.62.0	128.210.112.0	128.210.239.0
128.210.7.0	128.210.27.0	128.210.63.0	128.210.166.0	128.210.242.0
128.210.8.0	128.210.28.0	128.210.66.0	128.210.167.0	128.210.250.0
128.210.9.0	128.210.29.0	128.210.81.0	128.210.176.0	128.210.251.0
128.210.10.0	128.210.35.0	128.210.86.0	128.210.177.0	128.210.254.0
128.210.11.0	128.210.36.0	128.210.90.0	128.210.181.0	
128.210.12.0	128.210.37.0	128.210.91.0	128.210.182.0	
128.210.13.0	128.210.38.0	128.210.92.0	128.210.186.0	
128.210.15.0	128.210.39.0	128.210.104.0	128.210.189.0	

This list is subject to change, and an updated list will be maintained as part of the port restriction plan.

Port Restrictions

NetBIOS is a network protocol used for communication between Microsoft Windows and Samba hosts using SMB, or Server Message Block format. Windows file and printer sharing servers utilize NetBIOS to provide remote access to file systems and printers. For example, ICS student home directories are mounted to lab machines via NetBIOS. In order to prevent constant scanning and compromise of ITaP machines through externally accessible NetBIOS services, and to prevent the large traffic burden that these scans and attacks can cause, ITaP Data Networking will block access to the following network ports from non-Purdue networks. Before these restrictions are put in place, ITaP should ensure that their user community is made aware of the changes, the impact on access, and changes to how services may be accessed from off campus.

The following table describes the ports to be blocked.

Port number	Protocol	Description
135, 593	TCP and UDP	Microsoft RPC
137, 138, 139	TCP and UDP	Microsoft NetBIOS
445	TCP and UDP	Microsoft Data Service

ITaP users will remain able to access shares on the campus network. Users of non-Purdue networks with Purdue career accounts will be able to access on-campus services via the Purdue VPN service¹, Purdue dial-up service², or Purdue ADSL service³. Blocking the ports listed above will prevent off-campus entities from accessing services via NetBIOS or Microsoft RPC on ITaP machines if one of these services is used.

Current threats that this will help address include:

- Systems locking out legitimate users due to brute force password guessing attacks from off campus machines
- Enumeration of systems, shares, and user accounts.
- Worms and viruses that attack via SMB using account enumeration and weak passwords.
- Accidental sharing of information via open shares.
- Theft of data from ITaP machines.
- Use of ITaP machines by hackers to attack other computers or networks.

¹ <http://www.itap.purdue.edu/telecom/vpn/>

² <http://www.itap.purdue.edu/resnet/offcampus/dialUpGeneral.cfm>

³ <http://www.itap.purdue.edu/resnet/offcampus/ADSL.cfm>

Service Name	UDP	TCP
Browsing datagram responses of NetBIOS over TCP/IP	138	
Browsing requests of NetBIOS over TCP/IP	137	
Client/Server Communication		135
Common Internet File System (CIFS)	445	139, 445
DCOM (SCM uses UDP/TCP to dynamically assign ports for DCOM)	135	135
DHCP Manager		135
DNS Administration		139
Exchange Server		
Client Server Communication		135
Exchange Administrator		135
RPC		135
IIS RPC Proxy Services		593
File shares name lookup	137	
File shares session		139
Login Sequence	137, 138	139
Microsoft Message Queue Server		135
NetBT datagrams	138	
NetBT name lookups	137	
NetBT service sessions		139
NetLogon	138	
Pass Through Verification	137, 138	139
Printer sharing name lookup	137	
Printer sharing session		139
RPC user manager, service manager, port mapper		135
SCM used by DCOM	135	135
SQL Named Pipes encryption over other protocols name lookup	137	
SQL RPC encryption over other protocols name lookup	137	
SQL session		139
SQL session mapper		135
WINS Manager		135
WINS NetBIOS over TCP/IP name service	137	
WINS Proxy	137	
WINS Registration		137

Table 1: Blocked Services, Programs, and Data

Roles and Responsibilities

In order to implement the port restrictions with the least amount of disruption to users, each group has a set of responsibilities to fulfill. The ITaP is responsible for notifying users of systems on the affected subnets of the change. ITaP Data Networking will make changes on campus routers to implement the port restrictions, and ITaP Security's role is to coordinate the port restriction process and provide technical assistance and information about the port restrictions.