Recommendations for Transport Port Uses

draft-ietf-tsvwg-port-use-00
IETF 85 - Atlanta

Joe Touch, USC/ISI
As presented by Gorry Fairhurst

Purpose

- BCP advice to ***protocol designers***
  - – Encourage port conservation
  - – Encourage use of existing services
  - – Discourage ‘reinventing the wheel’
  - – Clarify how to describe a service in an application and/or ID
- **NOT**
  - – Direction to the IESG or Expert Review team

Current Status

- ietf-tsvwg-port-use
  - Now a WG-named doc. (Nov. 10)
- Current doc:
  - Detailed history
  - Skeleton of issues
    - Many established conservation issues
    - Discuss TCP service with UDP discovery
    - Discuss multiple ports for insecure/secure
    - Discuss system/user boundary

Poll Issues

1. System vs. User ports
2. Non-secure ports
3. Copies of existing services
4. Local (non Internet-traversing) services
5. UDP expectations
6. Discovery ports

Issue 1: system vs. user

- Currently:
  - System ports (<1024) distinct from user ports
    - Different assumption about user vs. root access
    - Different IANA application requirements
- Issue:
  - Port ranges no longer differentiate privilege
- Proposal:
  - Deprecate the difference as meaningful
    - SHOULD apply only for user ports
    - SHOULD NOT treat ports as implying different security or privilege

Issue 2: non-secure ports

- Currently:
  - Some services have both insecure and secure ports
- Issue
  - New insecure ports create vulnerability
  - Services shift ports to avoid port blocking protections
- Proposal:
  - New services SHOULD include security
  - New services that don't want security SHOULD determine how to support insecure variants on the same port so that port numbers alone are not considered a substitute for security

Issue 3: service copies

- Currently:
  - Some legacy services have duplicates (80, 8080)
  - IANA requires that new services not be duplicates of existing services
- Issue:
  - Web is increasingly a control interface
  - "X over HTTP" is not an issue
- Proposal:
  - Need practical implementation/deployment advice for running multiple web servers on the same machine with different URL spaces

Issue 4: local services

- Currently:
  - Port requests are for both services over the public Internet and to avoid configuration collision in private nets
- Issue:
  - Private net or LAN-only use should not consume global port numbers
- Proposal:
  - Need practical implementation/deployment advice for running services in a private net or within a LAN that avoids needing a global port assignment

Issue 5: UDP expectations

- Currently:
  - UDP is used in some services for performance (low latency, higher bandwidth)
- Issue:
  - UDP doesn't react to congestion
- Proposal:
  - UDP services SHOULD be limited to <?? Mbps or <X % of link capacity
  - UDP services SHOULD NOT be used for bulk transfer
  - Assigned ports SHOULD NOT be used for high performance services

Issue 6: discovery ports

- Currently:
  - Applicants frequently ask for both TCP and UDP, where UDP is solely for “discovery” of a running server on the corresponding TCP port
- Issue:
  - Common use begs for a common service
  - Current alternatives (mDNS) considered too heavyweight
- Proposal:
  - UDP SHOULD NOT be used solely as discovery; if for discovery then TCP SHOULD run on a dynamic port announced by the discovery response

Final Issue – Suggestions

- Current detailed outline needs input
  - Suggest items / issues to address
  - Provide text addressing an issue
  - Provide a position on the existing 6 issues
    - Pro, con, suggest alternate approach, etc.