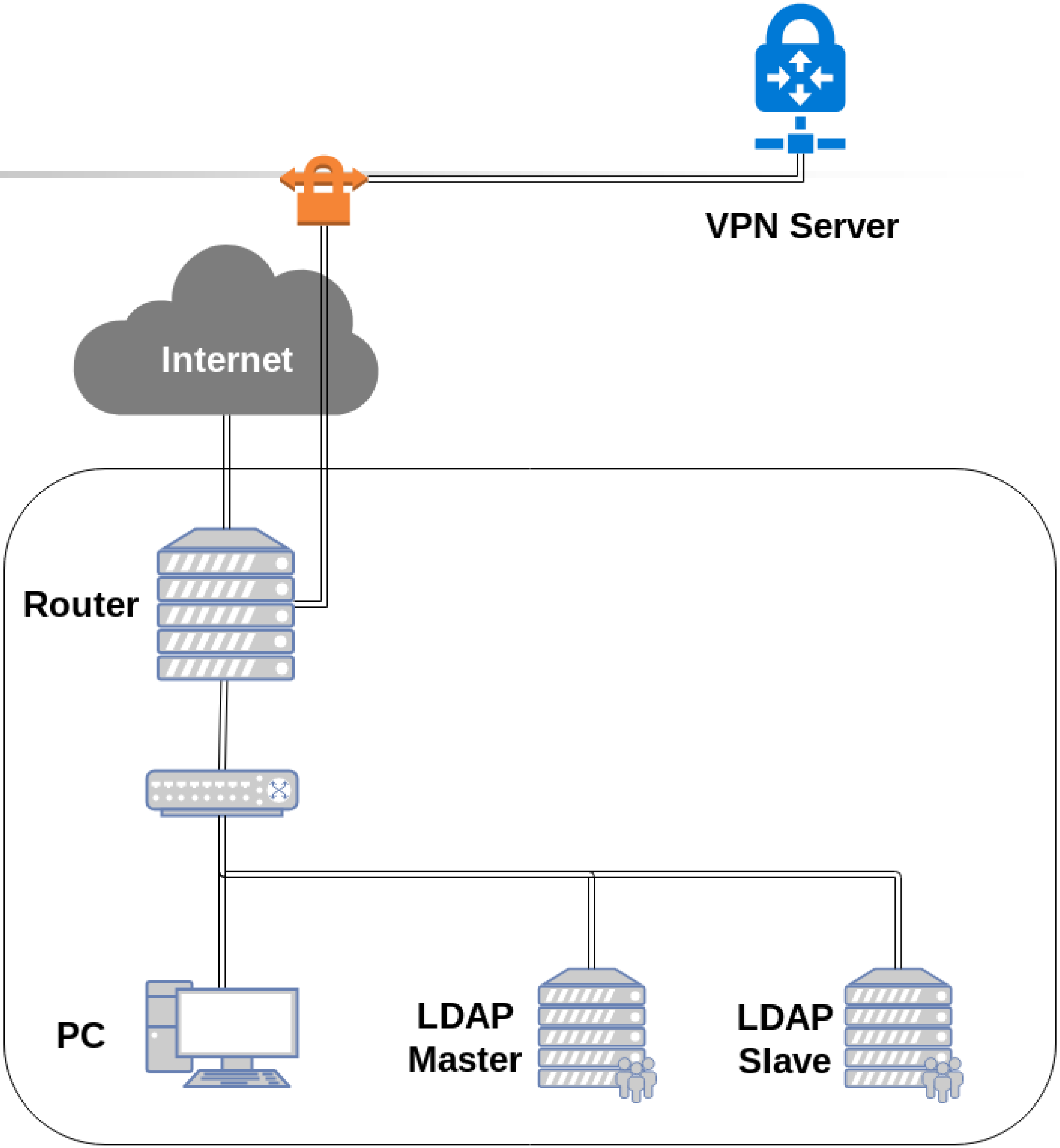
Network Administration HW2

tzute

Purposes

- ❑ Build a primary-replica architecture LDAP service
- ❑ Understand how to define LDAP schema from scratch
- ❑ Understand how to manage LDAP datas using LDIF
- ❑ Understand how to integrate other applications with LDAP

Overview



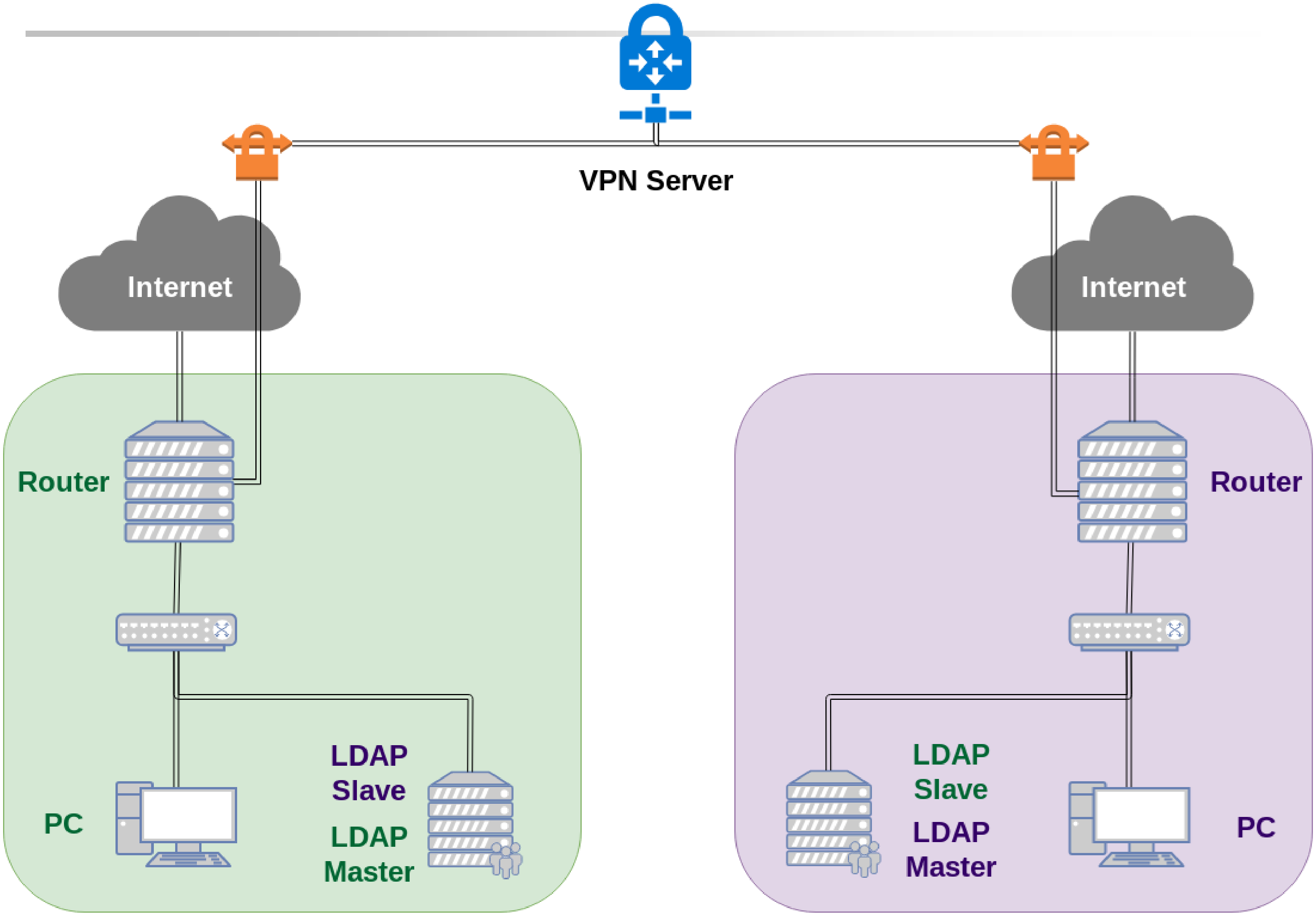
Overview (cont.)

- ❑ One LDAP master server
  - Providing LDAP service
  - Connecting into your intranet

- ❑ One LDAP slave server
  - Providing LDAP service
  - Connecting into your intranet
  - Auto-sync datas from master

- ❑ You can find a teammate and do this homework together

Overview (cont.)



Requirements (1/6)

- ❑ LDAP master
  - IP: 10.113.x.11/24 with static DHCP
    - ➢ Which means you have to re-configure your DHCP server to offer this server static IP
  - Base DN: dc=<student-id>,dc=nasa
  - StartTLS on LDAP service
    - ➢ Use self-signed certificate
  - Support SASL
    - ➢ Store hashed password into each DN's userPassword

Requirements (2/6)

- LDAP master (cont.)
  - Enable ACL
    - Everyone can read all datas expect userPassword
    - Authenticated users can write their own userPassword
    - Only slave server can bind to DN "cn=Syncer"
    - "cn=Syncer" can read all datas
- Specific DN "cn=Syncer"
  - Set credential to "hahaYouCatchMe" (excluding double-quotes)

Requirements (3/6)

❑ LDAP slave

- Same as master, but
- Choose any IP you want but bind with static DHCP
- Bind to "cn=Syncer" while syncing from master
- Sync from master every 60 seconds

Requirements (4/6)

❑ objectClass "clusterInfo"

- attributeType "address"

❑ Specific DN "cn=master,ou=ldap,dc=<student-id>,dc=nasa"

- objectClass="clusterInfo"
- address should be LDAP master server address (10.113.x.11)

❑ Specific DN "cn=slave,ou=ldap,dc=<student-id>,dc=nasa"

- objectClass="clusterInfo"
- address should be LDAP slave server address

Requirements (5/6)

- ❑ Router, Client, LDAP master, LDAP slave
  - Should can login with LDAP posixAccount
    - ➢ At least, login via SSH should be worked
  - Users can execute passwd to change their own password
- ❑ Specific user "cn=<student-id>"
  - uidNumber: 3001
  - set your own password

Requirements (6/6)

- ❑ objectClass "publicKeyLogin"
  - attributeType "sshPublicKey"
- ❑ Specific DN "cn=TA"
  - objectClass: posixAccount
  - objectClass: publicKeyLogin
  - uidNumber: 3000
  - sshPublicKey: <TA's public key>
  - Should can login SSH with sshPublicKey
- ❑ Retrieve TA's public key here
  - http://navpn.nctucs.cc/ta_rsa.pub (or access via 10.113.0.254)

DEMO

- TAs will try to login via public key and execute some script to validate your works.
- Due date:

Tips

- Google "How to get your own OID"
- Google "sshd_config AuthorizedKeysCommand"

Help!

- ❑ Email to ta@nasa.cs.nctu.edu.tw
  - Don’t send email by E3new
- ❑ EC 3F CSCC