This is a pretty complex but robust switch configuration with almost maximum access layer security in mind. I call it L2-security and it includes:

- 802.1x (used with Microsoft Radius service for user authentication)
- DHCP Snooping
- Dynamic Arp Inspection (DAI)
- IP Source Guard (IPSG)
- IntraVLAN ACL to block user to user traffic
- IP phones restriction
- Storm control
- STP protection

Used this configuration for more than one year. I don't recommend to use "change vlan" feature. Still pretty unstable with Win7&login scripts.

VLAN assignment for users done via radius attributes (Tunnel-*).

Hardware: Cisco 3750 Catalyst.

Software: IOS 12.2(55)SE4 with advanced IP services license, standard radius service in Microsoft 2008 Server, Win7&WinXP as clients. PEAP with windows machine accounts authentication only (passwords). Standard Microsoft supplicant.

Please note: If you just copy-paste it to your working enviroment it will effectively stops all users' traffic not just because of 802.1x and ACL, but because DAI and IPSG require DHCP snooping database to be prefilled with live DCHP-requests. Introduce DHCP Snooping first and then other features.

Switch: Complex L2-security config

```
aaa new-model
!
aaa group server radius radDC
 server 10.1.2.16 auth-port 1645 acct-port 1646
 server 10.1.2.17 auth-port 1645 acct-port 1646
 backoff exponential max-delay 3 backoff-retry 8
 deadtime 5
!
aaa authentication dot1x default group radDC
aaa authorization network default group radDC
aaa accounting dot1x default start-stop group radDC
!
ip dhcp excluded-address 10.1.8.1 10.1.8.15
ip dhcp pool Users
   network 10.1.8.0 255.255.255.0
   default-router 10.1.8.1
   domain-name corporate.local
   dns-server 10.1.2.16 10.1.2.17
!
ip dhcp excluded-address 10.1.15.1 10.1.15.15
ip dhcp pool IPT
   network 10.1.15.0 255.255.255.0
   default-router 10.1.15.1
```

```
   option 150 ip 10.1.7.16
!
!
vlan 2
 name Servers
!
vlan 7
 name CUCM
!
vlan 8
 name Users
!
vlan 15
 name IPT
!
vlan 999
 name Stub
!
!
interface Vlan2
 description Servers
 ip address 10.1.2.1 255.255.255.0
!
interface Vlan7
 description CUCM
 ip address 10.1.7.1 255.255.255.0
!
interface Vlan8
 description Users
 ip address 10.1.8.1 255.255.255.0
!
interface Vlan15
 description IP phones
 ip address 10.1.15.1 255.255.255.0
 ip access-group IPTin in
!
!
ip dhcp snooping vlan 8,15
no ip dhcp snooping information option
ip dhcp snooping database flash:DHCP_snooping_db.txt
ip dhcp snooping
ip arp inspection vlan 8,15
!
dot1x system-auth-control
no dot1x logging verbose
dot1x guest-vlan supplicant
```

```
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 8192
!
!
vlan access-map Users2Users 10
 action forward
 match ip address Users2User_exception
!
vlan access-map Users2Users 20
 action drop
 match ip address Users2User
!
vlan access-map Users2Users 30
 action forward
 match ip address Users2Any
!
vlan filter Users2Users vlan-list 8
!
!
interface range GigabitEthernet1/0/1-2
description Servers
 switchport access vlan 2
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/3
description CUCM
 switchport access vlan 7
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 ip arp inspection trust
 ip dhcp snooping trust
!
interface range GigabitEthernet1/0/4-24
 description Users
 switchport mode access
 switchport nonegotiate
 switchport voice vlan 15
 switchport voice detect cisco-phone
```

```
 authentication event fail retry 0 action authorize vlan 999
  authentication event no-response action authorize vlan 999
  authentication port-control auto
  authentication violation restrict
 auto qos voip cisco-phone
  dot1x pae authenticator
  dot1x timeout tx-period 10
  dot1x max-req 1
  dot1x max-reauth-req 1
  storm-control broadcast level 20.00
  storm-control multicast level 20.00
  spanning-tree portfast
  spanning-tree bpdufilter enable
  spanning-tree bpduguard enable
  ip verify source
  ip dhcp snooping limit rate 100
 !
 !
 ip access-list extended Users2User
  permit ip 10.1.8.0 0.0.0.255 10.1.8.0 0.0.0.255
 !
 ip access-list extended Users2Any
  permit ip 10.1.8.0 0.0.0.255 any
  permit ip any 10.1.8.0 0.0.0.255
 !
 ip access-list extended Users2User_exception
  permit udp any eq bootpc any eq bootps
  permit udp any eq bootps any eq bootpc
 !
 ip access-list extended IPTin
 permit udp any eq bootps any eq bootpc
  permit udp any eq bootpc any eq bootps
  permit ip any 10.1.7.0 0.0.0.255
  permit udp any any range 16384 32767
  deny ip any any
 !
 access-list 91 permit 10.1.2.16
 access-list 91 permit 10.1.2.17
 access-list 91 deny   any log
 !
 !
 radius-server host 10.1.2.16 auth-port 1645 acct-port 1646 timeout 5 key PleaseChangeMe!
 radius-server host 10.1.2.17 auth-port 1645 acct-port 1646 timeout 5 key PleaseChangeMe!
 !
 ! NTP is mandatory with DHCP Snooping
 !
```

```
ntp access-group peer 91
ntp server 10.1.2.16
ntp server 10.1.2.17
```