Design activities

Session I

1. Topology

- Selecting and placing devices
- Interconnecting devices

2. Providing connectivity between directly connected devices

- Configuring addresses for servers and hosts
- Configuring DHCP servers
- Configuring network interface cards

3. Testing

4. Technical report (1-2 pages)

Session II

1. Configuring VTP, VLAN and STP at layer 2 equipments

2. Configuring routes and routing protocols at layer 3 equipments

3. Testing

4. Technical report (1-2 pages)

Session III

1. Configuring NAT on the routers connected to Internet

2. Testing

3. Technical report (1-2 pages)

Session IV

1. Configuring HTTP, FTP, DNS and MAIL servers

2. Testing

3. Technical report (1-2 pages)

Session V

1. Securing the network

2. Testing

3. Technical report (1-2 pages)

Session VI

1. Test scenarios

2. Technical report (1-2 pages)

Session VII

10. Final presentation

Project topics

Theme 1:

It is considered a commercial building with 3 levels. Use network address 172.27.0.0/16 for intranet network, network address 210.2.2.64/27 for DMZ and network address 210.2.2.32/27 for access to the exterior. Design four VLANs (one for each floor and one for traffic management). VTP protocol will be used to configure VLANs. Redundancy will be provided through network cabling and configuration. Hosts addresses will be assigned dynamically using DHCP servers. The minimum number of users served by each VLAN is 200. HTTP, FTP, DNS and Mail servers will be placed in the DMZ and will have real addresses. Web domain name will include the student's name. To ensure connectivity static routes will be configured. Access to the exterior will be done using NAT on the router that controls the DMZ, on the following range of real addresses: 210.2.2.35-210.2.2.62. Routing equipments will be layer 3 switches.

Connecting to the ISP will be achieved through an Ethernet interface. ISP address is 210.2.2.33/27. Internet network will be simulated through a server and a computer.

For securing network devices the following configurations will be performed: users on different privilege levels will be defined, passwords will be encrypted, remote configuration will be done only through ssh, VTP protocol will be secured.

Two additional security measures will be presented and implemented.

Tema 2:

Se considera o cladire comerciala cu 3 nivele. Se va folosi adresa de retea 172.27.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.64/27 pentru DMZ si adresa de retea 210.2.2.32/27 pentru accesul in exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj si unul pentru traficul de management). Pentru configurarea VLAN-urilor se va folosi protocolul VTP. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind un singur server de DHCP aflat in VLAN-ul corespunzator primului etaj. Numarul minim de utilizatori deserviti de catre fiecare VLAN este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Pentru asigurarea conectivitatii se vor configura rute statice. Accesul in exterior se va realiza folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.35-210.2.2.62. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, se va securiza protocolul VTP.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

Tema 3:

Se considera o institutie comerciala cu 3 cladiri. Se va folosi adresa de retea 172.27.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.64/27 pentru DMZ si adresa de retea 210.2.2.32/27 pentru accesul in exterior. Se vor proiecta 3 subretele pentru utilizatori (una pentru fiecare cladire). Utilizatorii vor avea posibilitatea de a se conecta la retea atat prin cablu cat si wireless. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind cate un server de DHCP. Numarul minim de utilizatori deserviti de catre fiecare subretea este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Rutarea se va face cu ajutorul protocolului RIP pentru care se vor implementa optiunile de securitate. Accesul in exterior se va realiza folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.35-210.2.2.62. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, retelele wireless vor fi securizate cu WPA2.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

Tema 4:

Se considera o institutie comerciala cu 3 cladiri. Se va folosi adresa de retea 172.27.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.64/27 pentru DMZ si adresa de retea 210.2.2.32/27 pentru accesul in exterior. Se vor proiecta 3 subretele pentru utilizatori (una pentru fiecare cladire). Utilizatorii vor avea posibilitatea de a se conecta la retea atat prin cablu cat si wireless. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind servere de DHCP configurate la nivelul ruterelor. Numarul minim de utilizatori deserviti de catre fiecare subretea este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Rutarea se va face cu ajutorul protocolului RIP pentru care se vor implementa optiunile de securitate. Accesul in exterior se va realiza folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.35-210.2.2.62. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, retelele wireless vor fi securizate cu WPA2.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

Tema 5:

Se considera o institutie comerciala cu 3 cladiri. Se va folosi adresa de retea 172.27.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.64/27 pentru DMZ si adresa de retea 210.2.2.32/27 pentru accesul in exterior. Se vor proiecta 3 subretele pentru utilizatori (una pentru fiecare cladire). Utilizatorii vor avea posibilitatea de a se conecta la retea atat prin cablu cat si wireless. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind servere de DHCP configurate la nivelul ruterelor. Numarul minim de utilizatori deserviti de catre fiecare subretea este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Rutarea se va face cu ajutorul protocolului OSPF pentru care se vor implementa optiunile de securitate. Accesul in exterior se va realiza folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.35-210.2.2.62. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, retelele wireless vor fi securizate cu WPA2.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

Tema 6:

Se considera o cladire comerciala cu 3 nivele. Se va folosi adresa de retea 10.1.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.16/29 pentru DMZ si adresa de retea 210.2.2.8/29 pentru accesul in exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj si unul pentru traficul de management). Pentru configurarea VLAN-urilor se va folosi protocolul VTP. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind cate un server de DHCP. Numarul minim de utilizatori deserviti de catre fiecare VLAN este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Pentru asigurarea conectivitatii se vor configura rute statice. Accesul in exterior se va realiza folosind NAT Overload pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.11-210.2.2.14. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.9/29. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, se va securiza protocolul VTP.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

Tema 7:

Se considera o cladire comerciala cu 3 nivele. Se va folosi adresa de retea 10.1.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.16/29 pentru DMZ si adresa de retea 210.2.2.8/29 pentru accesul in exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj si unul pentru traficul de management). Pentru configurarea VLAN-urilor se va folosi protocolul VTP. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind un singur server de DHCP aflat in VLAN-ul corespunzator primului etaj. Numarul minim de utilizatori deserviti de catre fiecare VLAN este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Pentru asigurarea conectivitatii se vor configura rute statice. Accesul in exterior se va realiza folosind NAT Overload pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.11-210.2.2.14. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.9/29. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, se va securiza protocolul VTP.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

Tema 8:

Se considera o institutie comerciala cu 3 cladiri. Se va folosi adresa de retea 10.1.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.16/29 pentru DMZ si adresa de retea 210.2.2.8/29 pentru accesul in exterior. Se vor proiecta 3 subretele pentru utilizatori (una pentru fiecare cladire). Utilizatorii vor avea posibilitatea de a se conecta la retea atat prin cablu cat si wireless. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind cate un server de DHCP. Numarul minim de utilizatori deserviti de catre fiecare subretea este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Rutarea se va face cu ajutorul protocolului RIP pentru care se vor implementa optiunile de securitate. Accesul in exterior se va realiza folosind NAT Overload pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.11-210.2.2.14. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.9/29. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, retelele wireless vor fi securizate cu WPA2.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

Tema 9:

Se considera o institutie comerciala cu 3 cladiri. Se va folosi adresa de retea 10.1.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.16/29 pentru DMZ si adresa de retea 210.2.2.8/29 pentru accesul in exterior. Se vor proiecta 3 subretele pentru utilizatori (una pentru fiecare cladire). Utilizatorii vor avea posibilitatea de a se conecta la retea atat prin cablu cat si wireless. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind servere de DHCP configurate la nivelul ruterelor. Numarul minim de utilizatori deserviti de catre fiecare subretea este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Rutarea se va face cu ajutorul protocolului RIP pentru care se vor implementa optiunile de securitate. Accesul in exterior se va realiza folosind NAT Overload pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.11-210.2.2.14. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.9/29. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, retelele wireless vor fi securizate cu WPA2.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

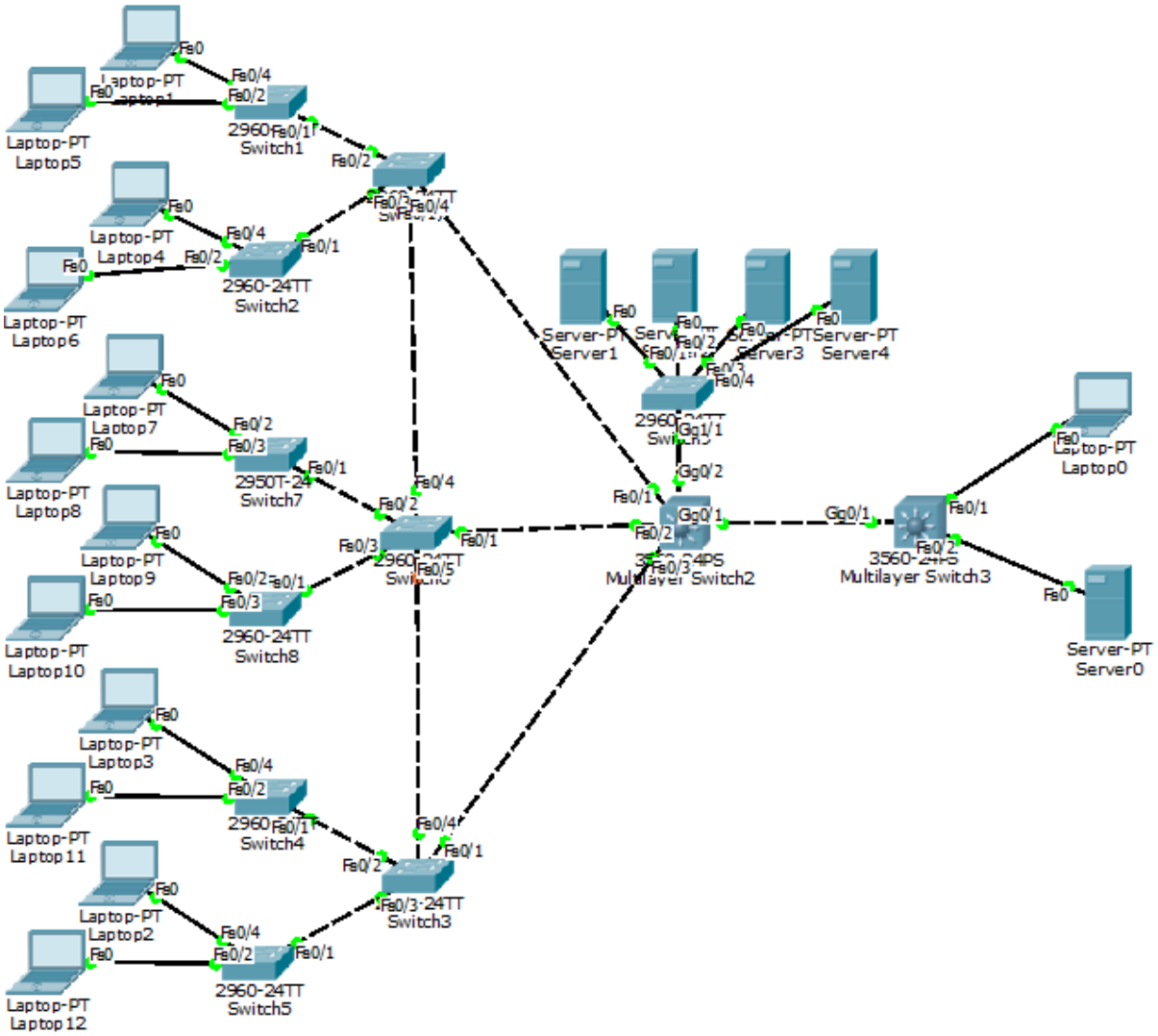
Tema 10:

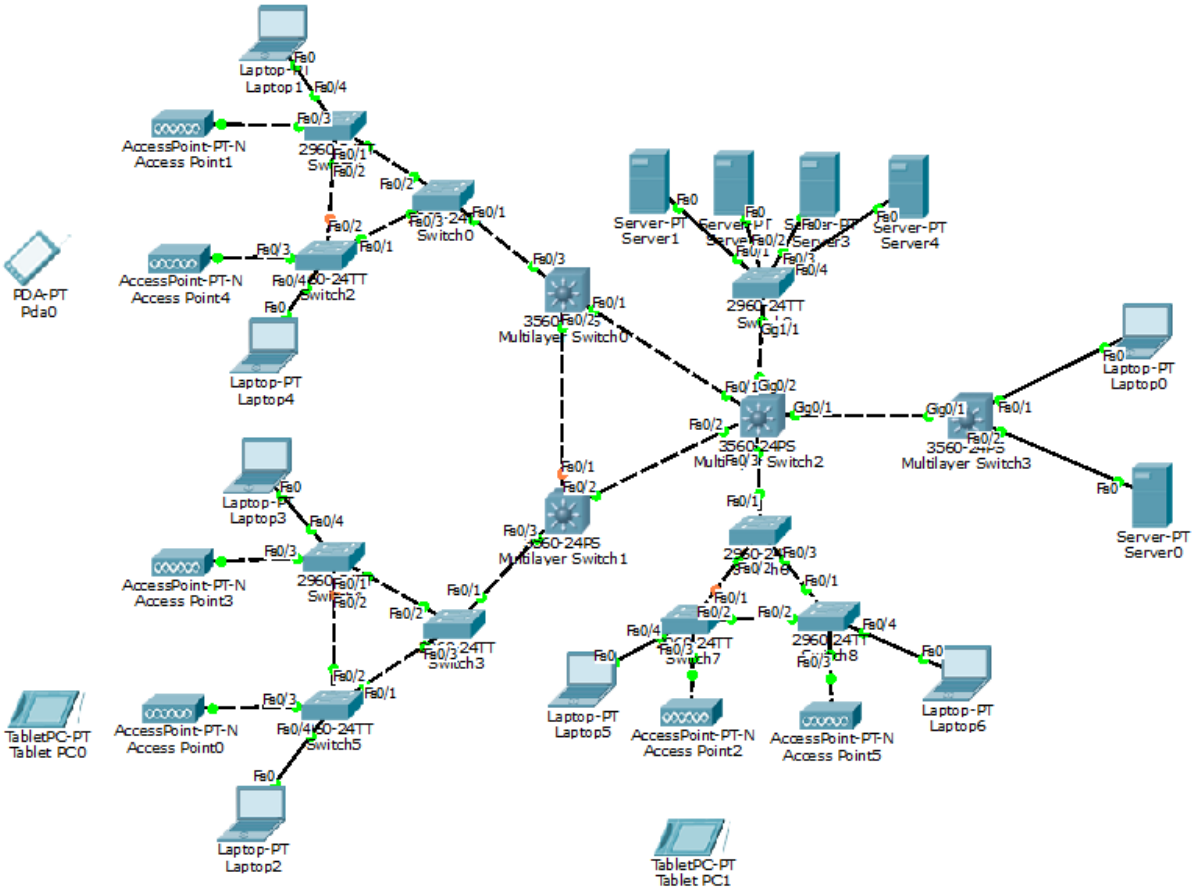
Se considera o institutie comerciala cu 3 cladiri. Se va folosi adresa de retea 10.1.0.0/16 pentru reteaua intranet, adresa de retea 210.2.2.16/29 pentru DMZ si adresa de retea 210.2.2.8/29 pentru accesul in exterior. Se vor proiecta 3 subretele pentru utilizatori (una pentru fiecare cladire). Utilizatorii vor avea posibilitatea de a se conecta la retea atat prin cablu cat si wireless. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind servere de DHCP configurate la nivelul ruterelor. Numarul minim de utilizatori deserviti de catre fiecare subretea este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese reale. Numele domeniului web va include numele studentului. Rutarea se va face cu ajutorul protocolului OSPF pentru care se vor implementa optiunile de securitate. Accesul in exterior se va realiza folosind NAT Overload pe routerul care controleaza DMZ, pe urmatorul interval de adrese reale: 210.2.2.11-210.2.2.14. Echipamentele de rutare vor fi switch-uri cu layer 3.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet. Adresa ISP-ului este 210.2.2.9/29. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, retelele wireless vor fi securizate cu WPA2.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.


Laptop-PT
Laptop5
Laptop-PT
Laptop4
Laptop-PT
Laptop6
Laptop-PT
Laptop7
Laptop-PT
Laptop8
Laptop-PT
Laptop9
Laptop-PT
Laptop10
Laptop-PT
Laptop3
Laptop-PT
Laptop11
Laptop-PT
Laptop2
Laptop-PT
Laptop12
2960-24TT
Switch1
2960-24TT
Switch2
2950T-24
Switch7
2960-24TT
Switch8
2960-24TT
Switch4
2960-24TT
Switch5
Switch3
Server-PT
Server1
Server-PT
Server3
Server-PT
Server4
Multilayer Switch2
3560-24PS
Multilayer Switch3
Laptop-PT
Laptop0
Server-PT
Server0


Laptop-PT
Laptop1
AccessPoint-PT-N
Access Point1
Switch0
Switch2
AccessPoint-PT-N
Access Point4
PDA-PT
Pda0
Laptop-PT
Laptop4
Server-PT
Server1
Server-PT
Server4
Multilayer Switch0
Multilayer Switch2
Multilayer Switch3
Laptop-PT
Laptop0
Server-PT
Server0
Laptop-PT
Laptop3
AccessPoint-PT-N
Access Point3
Multilayer Switch1
Switch3
Switch5
TabletPC-PT
Tablet PC0
AccessPoint-PT-N
Access Point0
Laptop-PT
Laptop2
Laptop-PT
Laptop5
AccessPoint-PT-N
Access Point2
AccessPoint-PT-N
Access Point5
Laptop-PT
Laptop6
TabletPC-PT
Tablet PC1