Activitati de proiectare

Sedinta I

1. Realizare topologie

   - alegerea si amplasarea dispozitivelor
   - interconectarea dispozitivelor (alegerea cablurilor corespunzatoare, selectarea corecta a interfetelor)

2. Asigurarea conectivitatii intre dispozitivele direct conectate.

   - configurarea adreselor hosturilor si a serverelor
   - configurarea serverelor de DHCP
   - configurarea interfetelor dispozitivelor de retea

3. Testare configurari

4. Memoriu tehnic (1-2 pagini)

Sedinta II

1. Configurare VTP, VLAN si STP la nivelul echipamentelor de nivel 2

2. Configurarea rutelor la nivelul echipamentelor de nivel 3

3. Testare configurari

4. Memoriu tehnic (1-2 pagini)

Sedinta III

1. Configurarea NAT pe ruterele conectate spre Internet

2. Testare configurari

3. Memoriu tehnic (1-2 pagini)

Sedinta IV

1. Configurarea servelor de HTTP, FTP, DNS si MAIL

2. Testare configurari

3. Memoriu tehnic (1-2 pagini)

Sedinta V

1. Securizarea retelei

2. Testare configurari

3. Memoriu tehnic (1-2 pagini)

Sedinta VI

1. Scenarii de test

2. Memoriu tehnic (1-2 pagini)

Sedinta VII

10. Prezentare finala

Teme de proiect

Tema 1:

Se considera o cladire comerciala cu 3 nivele. Se va folosi adresa de retea 172.16.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.64/27 pentru DMZ si adresa de retea 210.1.1.32/27 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 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 publice. 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 publice: 210.1.1.35-210.1.1.62.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. 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 2:

Se considera o cladire comerciala cu 3 nivele. Se va folosi adresa de retea 172.16.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.64/27 pentru DMZ si adresa de retea 210.1.1.32/27 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 publice. 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 publice: 210.1.1.35-210.1.1.62.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. 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 172.16.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.64/27 pentru DMZ si adresa de retea 210.1.1.32/27 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 publice. 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 publice: 210.1.1.35-210.1.1.62.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. 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 172.16.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.64/27 pentru DMZ si adresa de retea 210.1.1.32/27 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 publice. 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 publice: 210.1.1.35-210.1.1.62.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. 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 172.16.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.64/27 pentru DMZ si adresa de retea 210.1.1.32/27 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 publice. 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 publice: 210.1.1.35-210.1.1.62.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. 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 10.2.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.16/29 pentru DMZ si adresa de retea 210.1.1.8/29 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 publice. 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 publice: 210.1.1.11-210.1.1.14.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.10/29. Adresa ISP-ului este 210.1.1.9/29. 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 10.2.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.16/29 pentru DMZ si adresa de retea 210.1.1.8/29 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 publice. 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 publice: 210.1.1.11-210.1.1.14.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.10/29. Adresa ISP-ului este 210.1.1.9/29. 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 10.2.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.16/29 pentru DMZ si adresa de retea 210.1.1.8/29 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 publice. 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 publice: 210.1.1.11-210.1.1.14.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.10/29. Adresa ISP-ului este 210.1.1.9/29. 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 10.2.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.16/29 pentru DMZ si adresa de retea 210.1.1.8/29 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 publice. 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 publice: 210.1.1.11-210.1.1.14.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.10/29. Adresa ISP-ului este 210.1.1.9/29. 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 10.2.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.16/29 pentru DMZ si adresa de retea 210.1.1.8/29 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 publice. 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 publice: 210.1.1.11-210.1.1.14.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.10/29. Adresa ISP-ului este 210.1.1.9/29. 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.