Planificarea rețelei

Capitolul 11

hackademy

Întrebarea zilei

Cum proiectăm o rețea?

hackademy

Etapa 1: Topologia

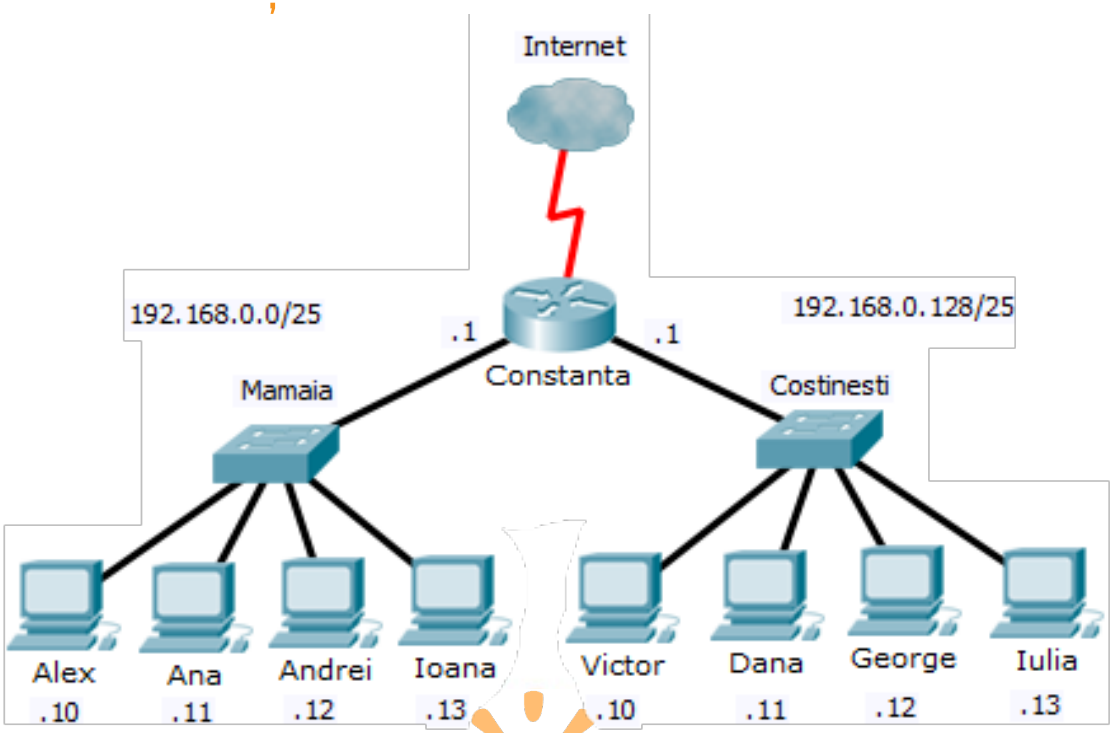
hackademy

Alegerea echipamentelor

- Criterii de alegere:
  -  Cost
  -  Viteză
  -  Număr/tipuri de porturi
  -  Versiunea de SO

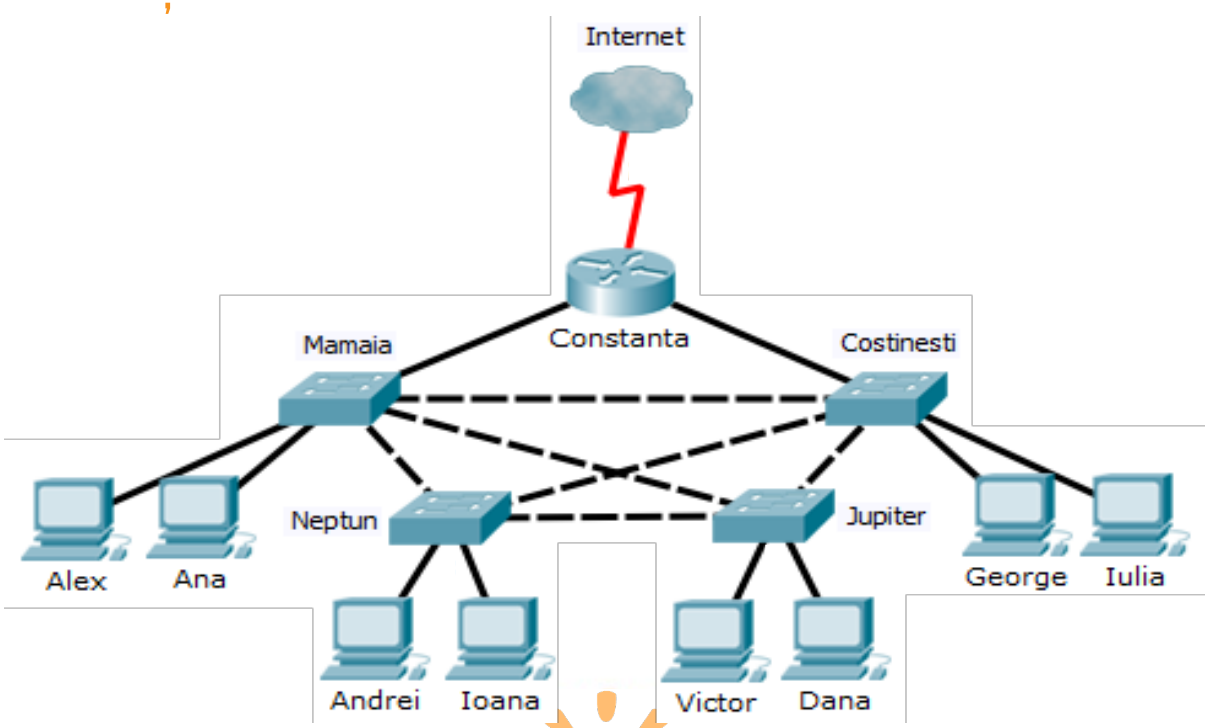
Adresarea IP

- Schema de adresare trebuie să fie bine documentată și actualizată mereu



Design practic

- Rețeaua trebuie construită astfel încât să aibă o toleranță crescută la defecte => redundanță



Etapa 2: Servicii

hackademy

Protocoale necesare

- DNS
- DHCP
- HTTP
- FTP
- SMTP, IMAP, POP3
- SSH

hackademy

Aplicații în timp real

- VoIP = Voice over IP
  - Un ruter convertește vocea umană în semnale digitale, care circulă în rețea ca pachete obișnuite
- Telefonie IP
  - Conversia e realizată de telefon, metoda având ca rezultat o calitate superioară a comunicării

Etapa 3:
Salvarea configurațiilor

hackademy

Salvarea pe echipament

- În cazul opririi neprevăzute a unui echipament, configurările nesalvate se pierd
- Care sunt comenzile folosite pentru salvarea locală a configurațiilor?

Salvarea folosind TFTP

- Salvarea pe un server oferă un plus de siguranță.

```
Constanta#copy running-config tftp
Address or name of remote host []? 10.0.0.2
Destination filename [Constanta-confg]? Constanta-config
Writing running-config...!!
[OK - 864 bytes]
864 bytes copied in 0.001 secs (864000 bytes/sec)
```

Restaurarea configurațiilor

```
Constanta#copy tftp running-config
Address or name of remote host []? 10.0.0.2
Source filename []? Constanta-config
Destination filename [running-config]? running-config
Accessing tftp://10.0.0.2/Constanta-config...
Loading Constanta-config from 10.0.0.2: !
[OK - 864 bytes]
864 bytes copied in 0.001 secs (864000 bytes/sec)
```

Securitate

hackademy

Amenințări hardware


Daune fizice


Mediu nepotrivit

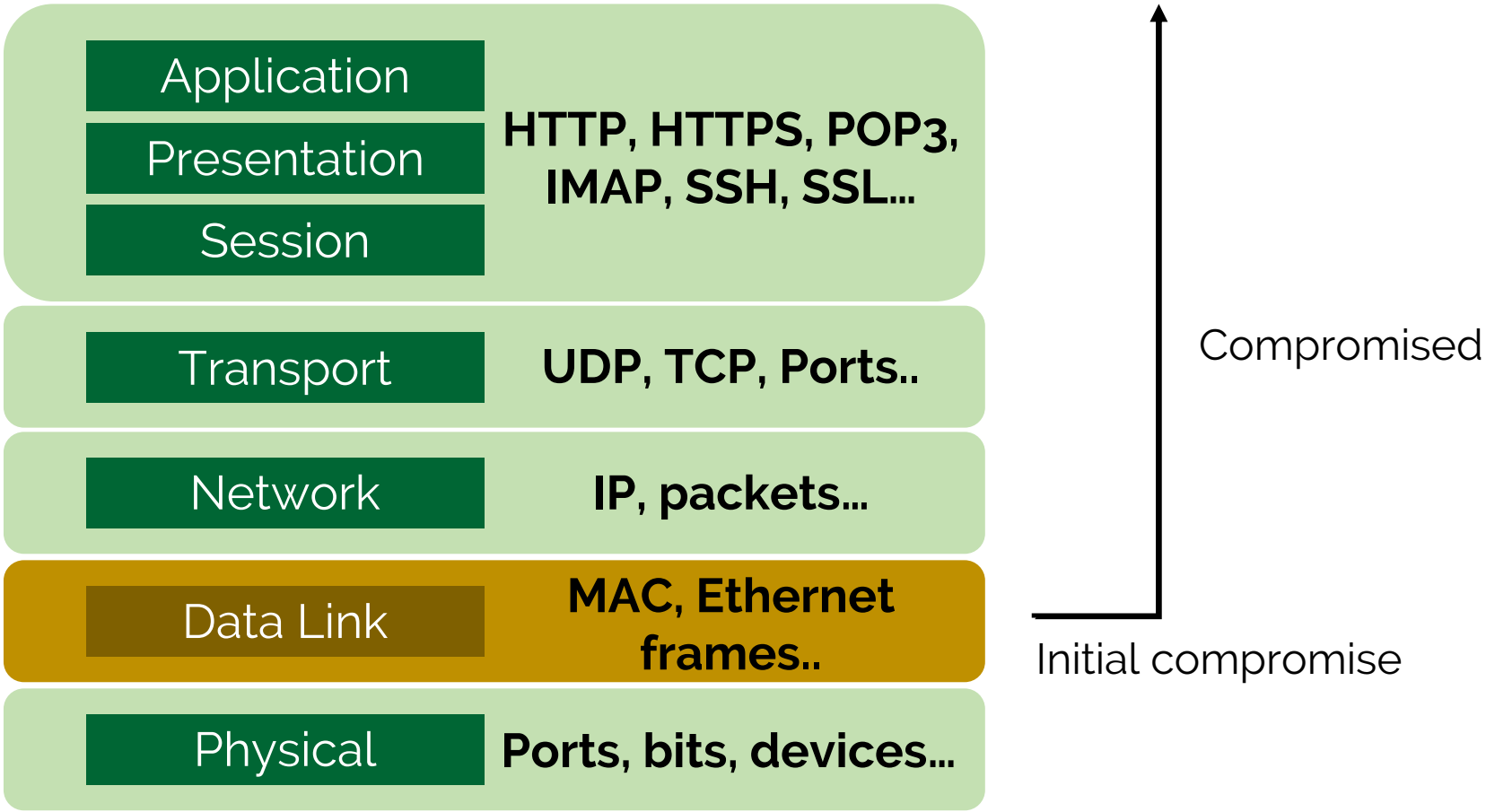

Probleme electrice


Probleme de mentenanță

Amenințări software

- Furt de informații
- Furt de identitate
- Pierderea datelor
- Întreruperea serviciilor (DoS)

Stiva OSI - reminder



Tipuri de vulnerabilități

- Tehnologice (exploits)
- De configurare
- Politici de securitate nerespectate

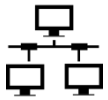
hackademy

Tipuri de atacuri (1)

Viruși, viermi și troieni

- Majoritatea virușilor nu își manifestă prezența în sistem
- Viermii pot infecta sistemele fără să ruleze cod (de cele mai multe ori se răspândesc prin e-mail sau servicii precum FTP sau HTTP)
- Tendință actuală: transformarea viermilor în „boți”
- Troienii sunt executabile care pretind că sunt altceva pentru a fura date confidențiale

Tipuri de atacuri (2)



Atacuri de recunoaștere

- Constau în recoltarea informațiilor despre o anumită rețea
- Se caută orice informație utilă care poate fi folosită în defășurarea unui atac ulterior
- Utilitare de recunoaștere: nmap, wireshark, tcpdump

Tipuri de atacuri (3)

Atacuri de acces

- Accesarea datelor printr-un cont de utilizator obișnuit sau cu privilegii superioare
- Etape:
  - Colectare informații
  - Exploatare
  - Deteriorare

Tipuri de atacuri (4)

Atacuri de tip DoS (Denial of Service) și DDoS (Distributed DoS)

- Se trimite un număr mare de cereri pentru a preveni procesarea cererilor normale (DoS)
- Constau în trimiterea cererilor de la mai multe sisteme către o singură țintă (DDoS)
- Exemple: Smurf Attack, TCP Syn Flood

DHCP Starvation Attack

- Atacatorul creează DoS (Denial of Service) al serviciului de DHCP
- Ex. tool-ul **Globber**
  - Generează mesaje DHCP Discovery cu adrese MAC sursă false
  - Toate adresele IP din pool-ul DHCP vor fi asignate unor stații inexistente

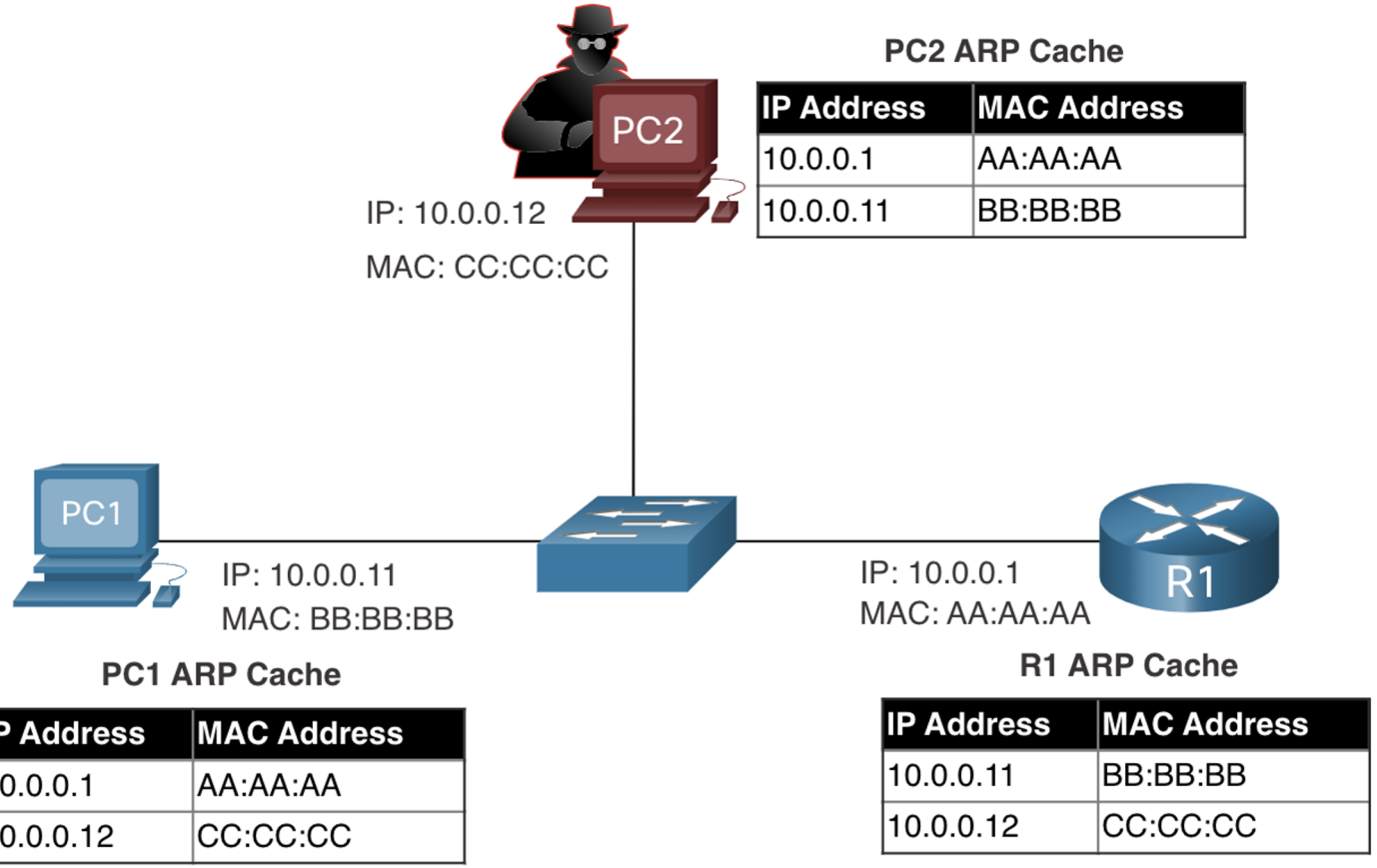
DHCP Spoofing Attack

- Atacatorul se conectează ca un server DHCP
- Va oferi servicii false clienților
  - Default gateway greșit (toate pachetele către internet vor trece prin atacator)
  - DNS Server greșit (clientul se va conecta la adrese web nefavorabile/malițioase)
  - Adresă IP greșită

ARP Attacks

- Pentru a afla MAC-ul unui host, o stație trimite un ARP Request
- Host-ul cu IP-ul cerut răspunde cu un ARP Reply
- Un atacator poate trimite un ARP Reply fals
- Toate stațiile din rețea vor asocia IP-ul respectiv cu stația atacatorului (ex. Default Gateway)

ARP Attacks (1)



PC2 ARP Cache

IP Address	MAC Address
10.0.0.1	AA:AA:AA
10.0.0.11	BB:BB:BB

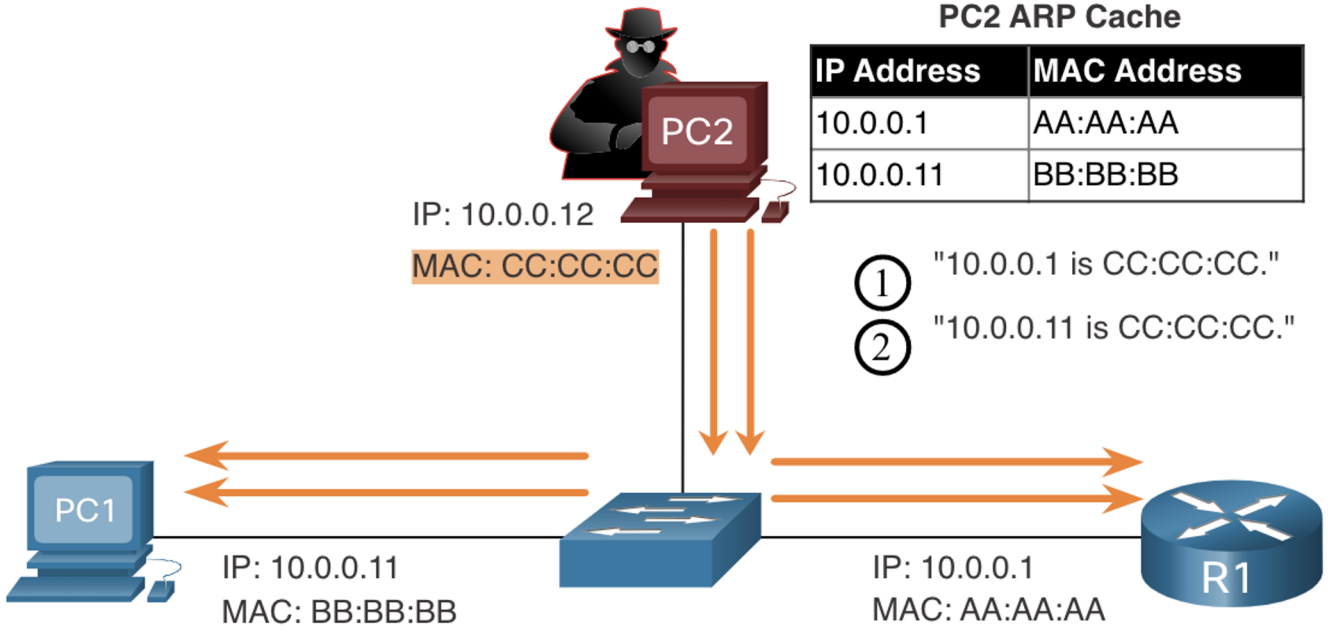
PC1 ARP Cache

IP Address	MAC Address
10.0.0.1	AA:AA:AA
10.0.0.12	CC:CC:CC

R1 ARP Cache

IP Address	MAC Address
10.0.0.11	BB:BB:BB
10.0.0.12	CC:CC:CC

ARP Attacks (2)



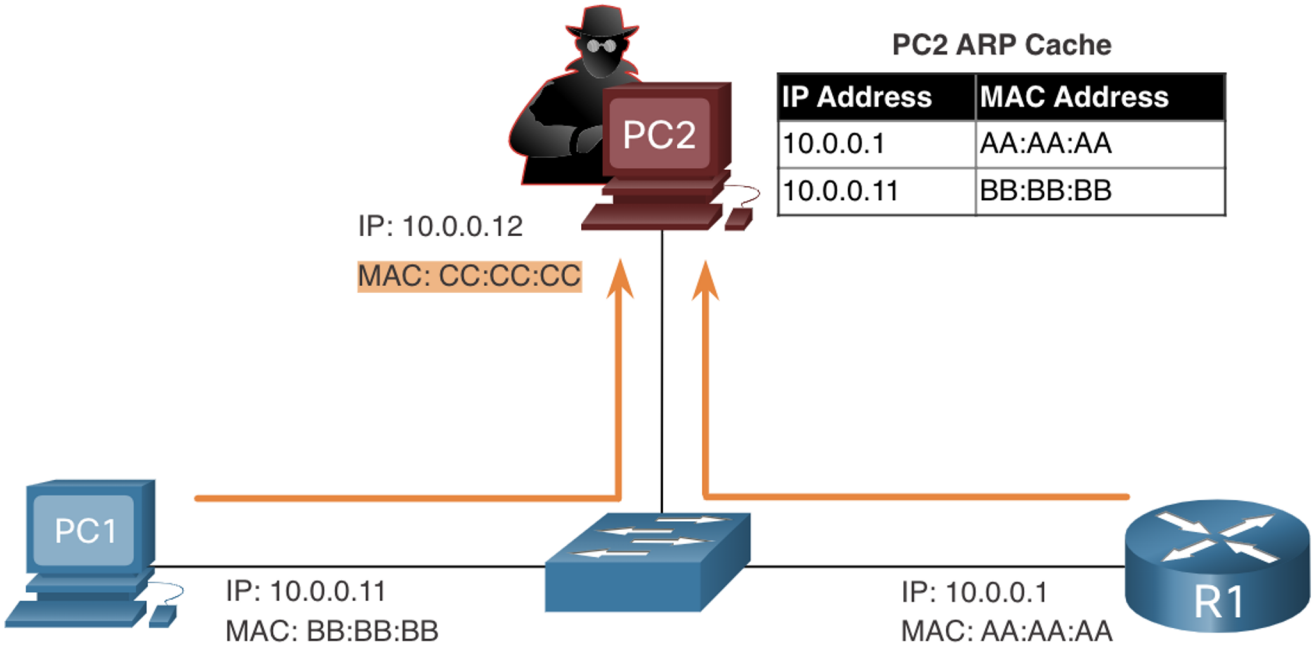
PC1 ARP Cache

IP Address	MAC Address
10.0.0.1	AA:AA:AA
10.0.0.12	CC:CC:CC

R1 ARP Cache

IP Address	MAC Address
10.0.0.11	BB:BB:BB
10.0.0.12	CC:CC:CC

ARP Attacks (3)



PC2 ARP Cache

IP Address	MAC Address
10.0.0.1	AA:AA:AA
10.0.0.11	BB:BB:BB

PC1 ARP Cache

IP Address	MAC Address
10.0.0.1	CC:CC:CC
10.0.0.12	CC:CC:CC

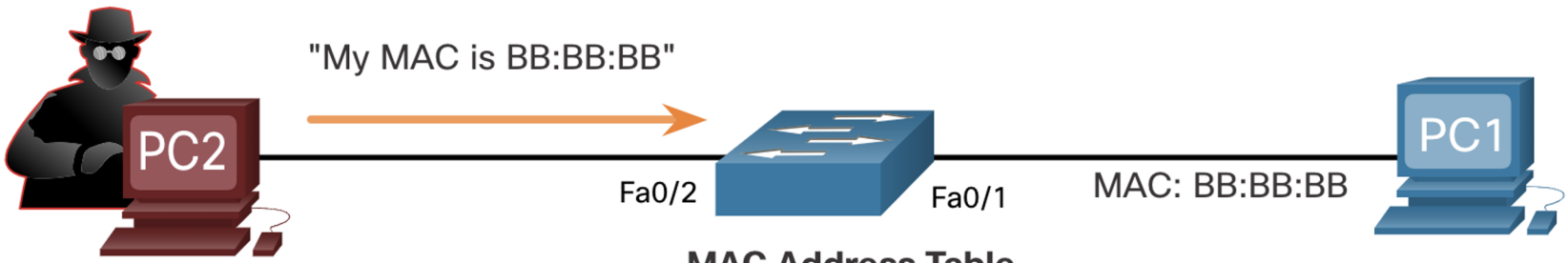
R1 ARP Cache

IP Address	MAC Address
10.0.0.11	CC:CC:CC
10.0.0.12	CC:CC:CC

Address spoofing attack

- Atacatorul preia o adresă IP/MAC validă a unei stații din rețeaua locală
- Este greu de prevenit, dacă atacatorul se află deja în LAN
- Poate fi prevenit totuși cu IPSG

Address spoofing attack



MAC Address Table

Port	MAC Address
Fa0/1	
Fa0/2	BB:BB:BB

Metode de prevenție

- Software antivirus
- Metode de verificare a identității
- Firewall-uri
- Politici de securitate

Testare și depanare

hackademy

Verificarea conectivității

- traceroute
  - Poate determina ruta echipament cu echipament, până la destinație
  - Pe IOS
  - Se întrerupe cu Ctrl + Shift + 6
- tracert

hackademy

Verificarea conectivității

- traceroute
- tracert
  - Are aceeași funcție ca traceroute
  - Pe Windows
  - Se întrerupe cu Ctrl + C

Probleme comune

- Adresa IP sau masca stației sunt greșite
- Adresa IP sau masca Default Gateway-ului sunt greșite
- O rută din tabela de rutare este greșită
- Probleme de DHCP
- Probleme de DNS

Răspunsul zilei

Răspunsul zilei

Cum proiectăm o rețea?

hackademy