



Routing and Switching

20 martie 2014

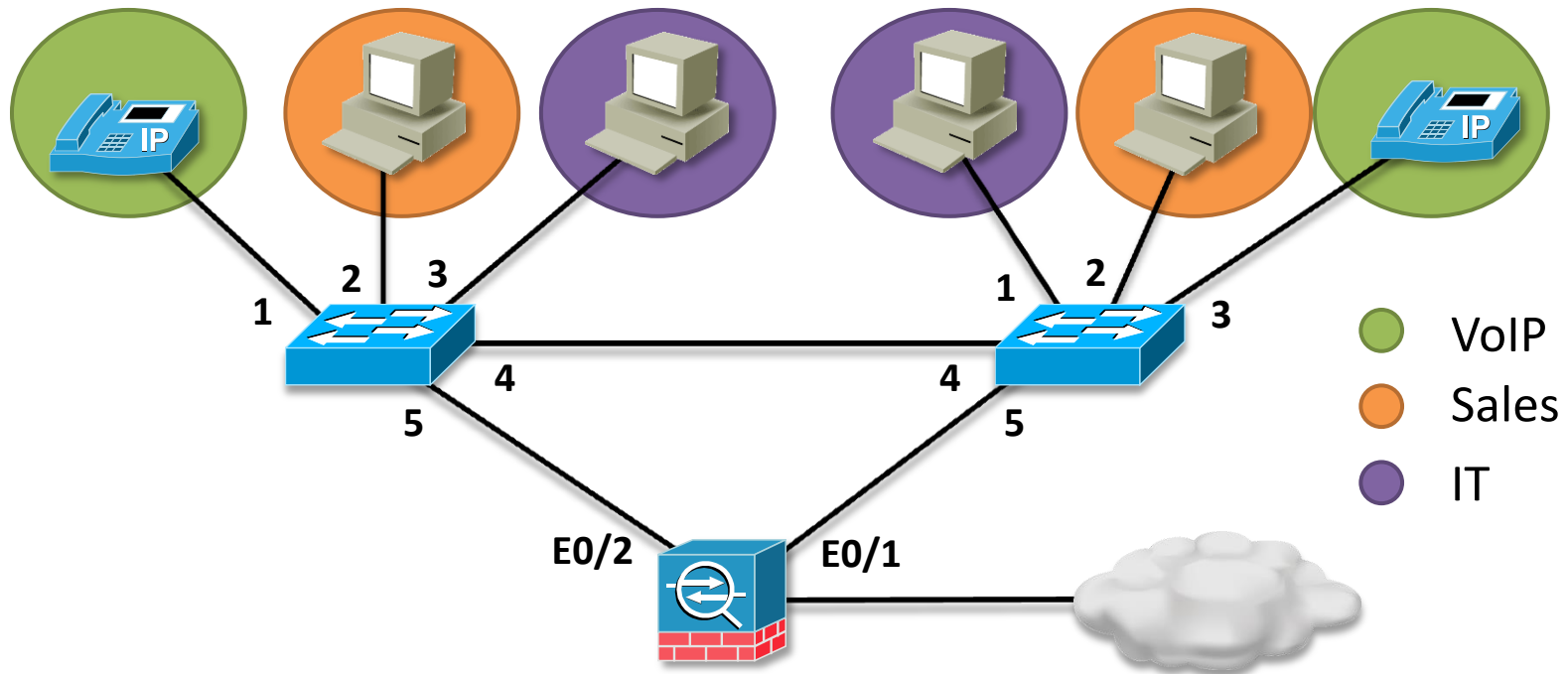
Obiective

- ▶ VLAN-uri
 - ❑ Separarea rețelei prin VLAN-uri
 - ❑ Inter-VLAN Routing
- ▶ Rutare
 - ❑ Statică vs. Dinamică
 - ❑ Concepte de rutare dinamică
 - ❑ Procesarea rutelor în tabela de rutare
 - ❑ Routing Information Protocol (RIP)
 - ❑ Open Shortest Path First (OSPF)
 - ❑ Policy-Based Routing (PBR)
 - ❑ Bidirectional forward detection (BFD)
- ▶ Configurații Cisco
- ▶ Configurații Fortinet

VLAN-uri

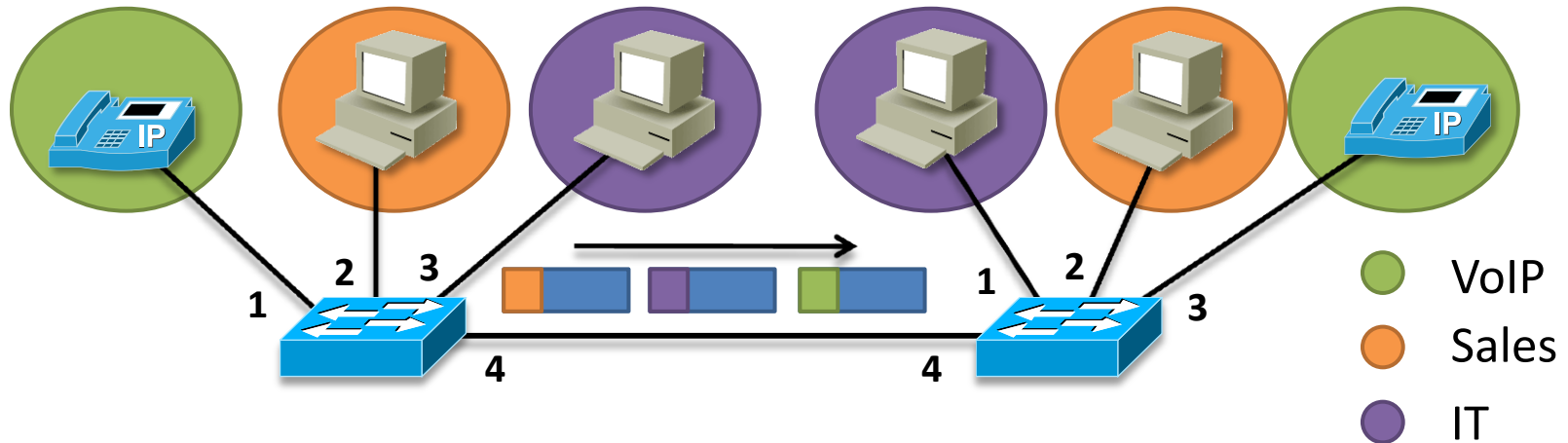
- ▶ Terminologie în VLAN-uri
 - ❑ VLAN
 - ❑ Trunk
 - ❑ Inter-VLAN Routing
 - ❑ Tagging
- ▶ VLAN - posibilitatea de a separa stațiile dintr-un LAN în mai multe domenii de broadcast
- ▶ Scenarii comune de utilizare a VLAN-urilor?
 - ❑ Separarea departamentelor într-o companie (Marketing, Programming etc)
 - ❑ Separarea traficului de date de cel de management/monitorizare
 - ❑ Separarea rețelei de date de rețeaua de VoIP (astfel este posibil QoS de nivel 2)

Rețea redundantă cu VLAN-uri

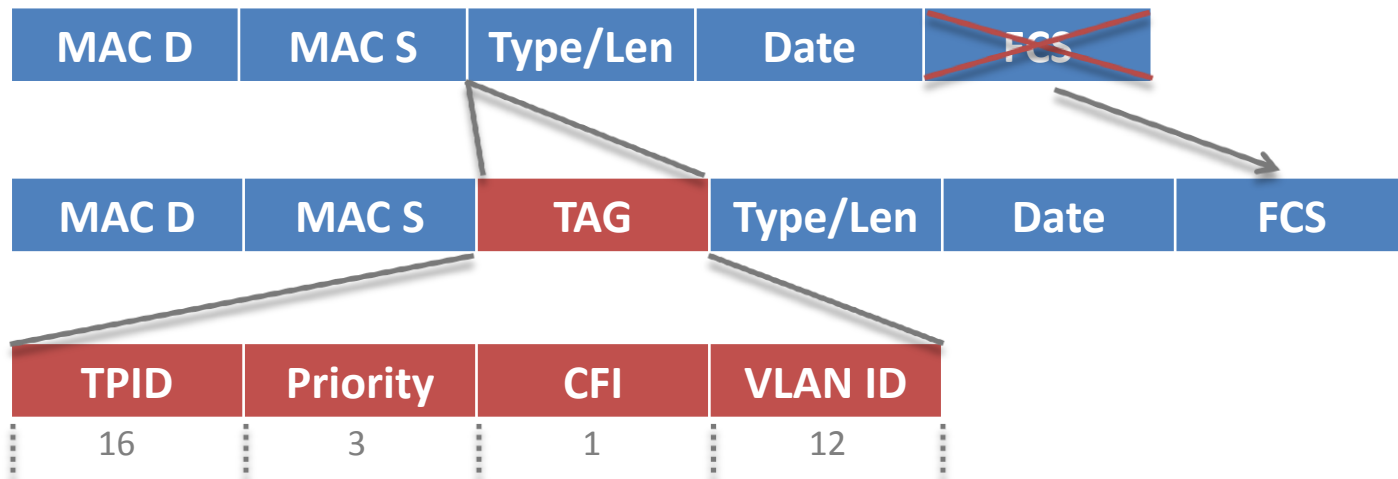


- ▶ VLAN-urile se configurează la nivelul interfețelor switch-urilor
- ▶ Comunicarea între 2 stații din același VLAN se face întotdeauna pe cea mai scurtă cale de nivel 2
- ▶ Q: În ce VLAN se află link-urile dintre switch-uri sau dintre switch-uri și firewall?
 - ▣ A: În nici un VLAN; sunt link-uri de tip **trunk**

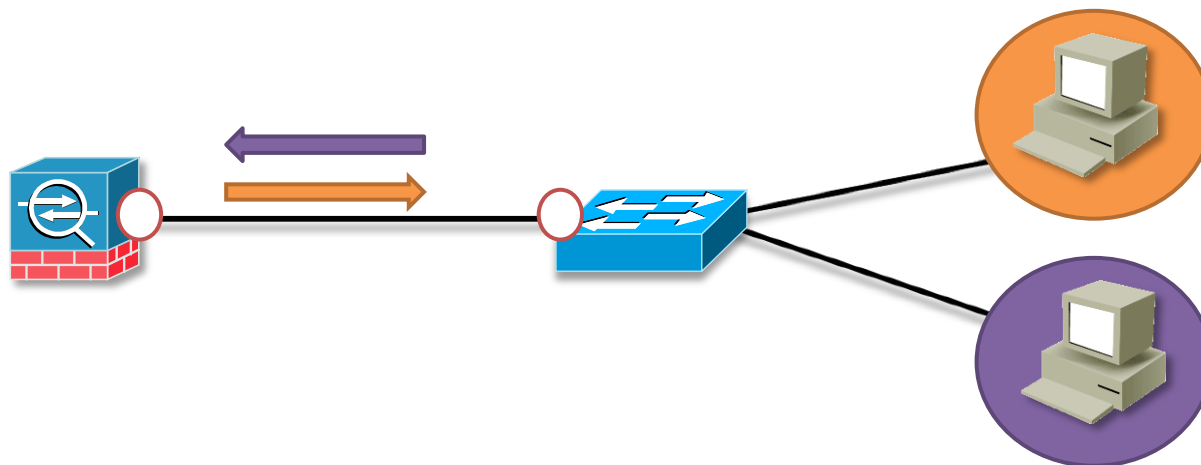
Trunking



- ▶ Pentru a putea separa traficul fiecărui VLAN peste aceeași legătură fizică trebuie folosit un protocol separat – **802.1q**

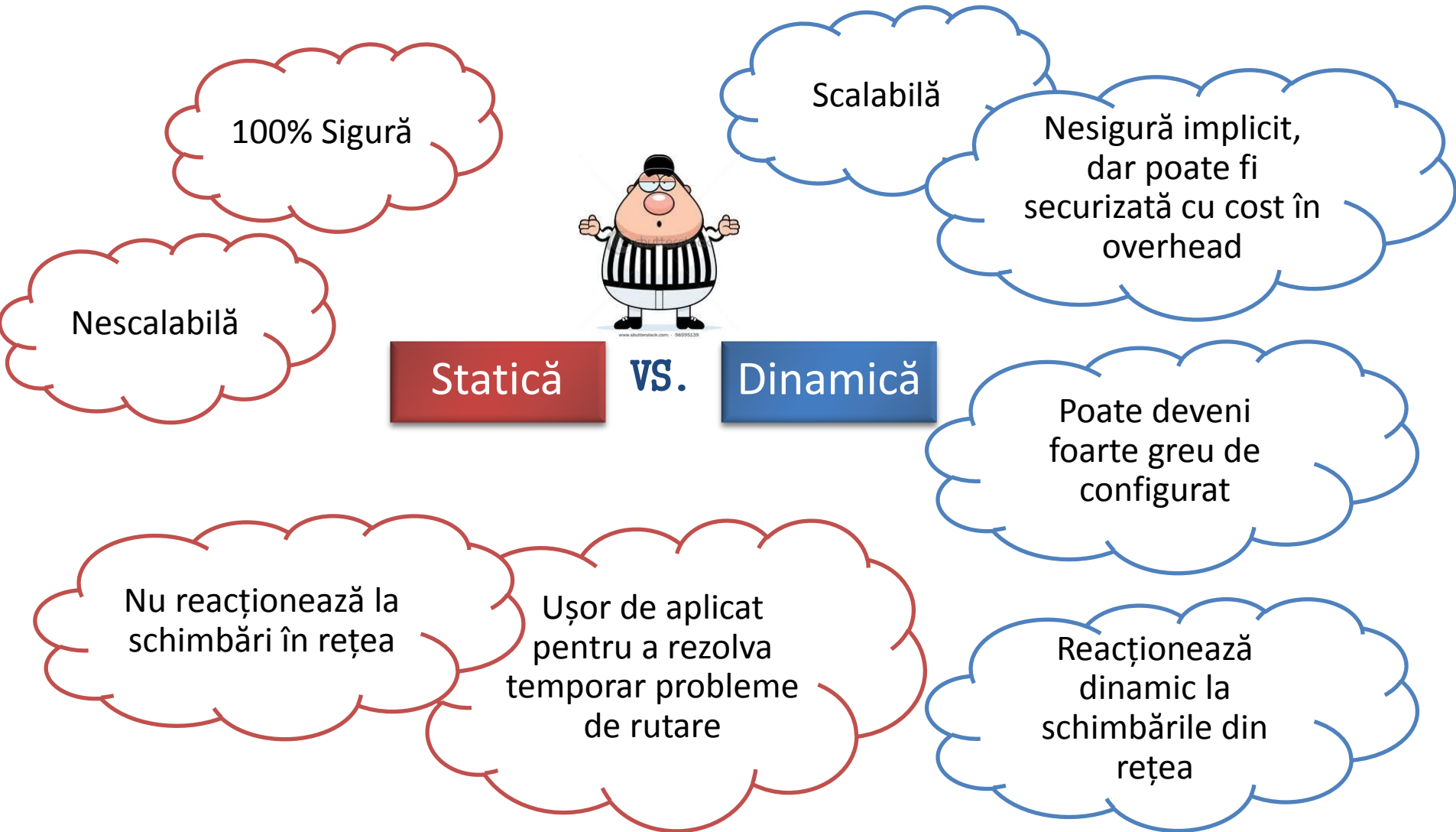


Inter-VLAN Routing



- ▶ S-ar putea să existe nevoia comunicării între 2 stații din VLAN-uri diferite
 - ❑ Ex: Trafic de monitorizare, administratorul dorește să acceseze orice VLAN etc.
- ▶ Trebuie folosit un dispozitiv capabil de rutare
- ▶ Portul switch-ului trebuie configurat ca trunk
- ▶ Portul firewall-ului poate fi configurat ca trunk?
 - ❑ Nu pentru ca este un port L3
 - ❑ Este însă necesară o configurație specială care să permită firewall-ului să recunoască ID-ul dot1q și să ia o decizie pe baza sa

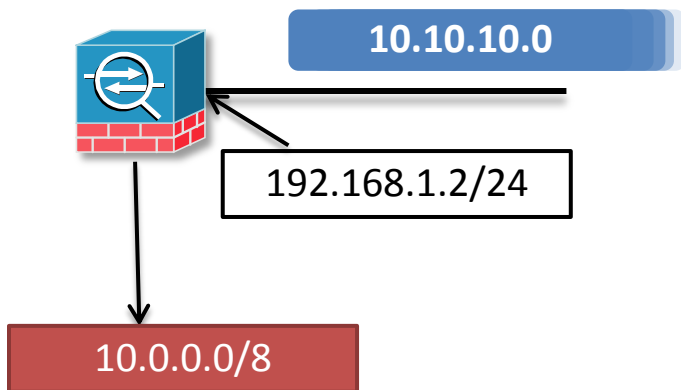
Rutare – statică vs. dinamică



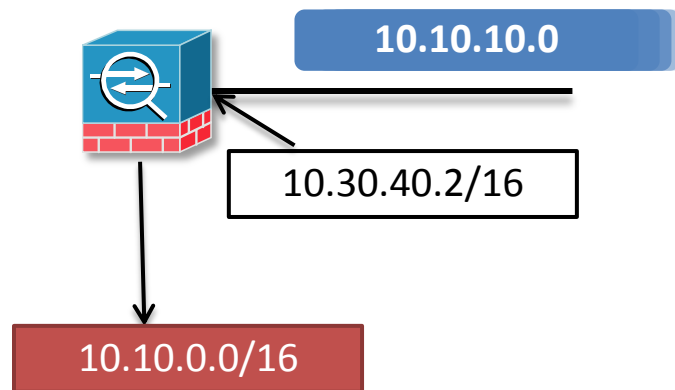
Protocoale de rutare – classful vs classless

- ▶ Sunt clasificate după mai multe criterii
- ▶ Criteriul 1: Classful vs Classless
- ▶ Care este diferența?
 - ❑ Protocoalele de rutare classful nu trimit masca de rețea în mesaje de update
- ▶ Ce mască de rețea este reținută în tabela de rutare?

Cazul 1:



Cazul 2:



Protocoale de rutare – DV vs. LS

▶ Distance vector

- ❑ Cunosc rețeaua prin intermediul adresei next-hop și distanței până la destinație
- ❑ Nu știu nimic despre rețea dincolo de next-hop
- ❑ Trimit update-uri de rutare la intervale fixe care conțin în general toată tabela de rutare
- ❑ Rulează algoritmul Bellman-Ford

▶ Link-state

- ❑ Cunosc toată rețeaua (e.g câte hopuri există până la destinație, care este costul între hop-ul 3 și hop-ul 4 etc)
- ❑ Trimit update-uri triggered și doar cu informația necesară
- ❑ Rulează algoritmul Dijkstra

Procoale de rutare – DV vs. LS (analogie)

Citesc indicatoarele și funcție de distanță și destinație iau o decizie.



Dacă se produce o modificare nu trebuie decât să urmăresc alt indicator. E ușor să urmărești indicatoare.

Am o hartă și știu exact cum să ajung la destinație.



Dacă se produce o modificare, trebuie să îmi recalculiez toată harta.

Protocoale de rutare – IGP vs EGP

► Interior gateway protocols (IGP)

- ❑ Protocoale LS sau DV
- ❑ Folosite în cadrul aceleiași organizații (Autonomous System)
- ❑ AS – un grup de rutere aflate sub administrație comună
- ❑ Scop principal: găsirea celei mai scurte rute!




► Exterior gateway protocols (EGP)

- ❑ BGPv4
- ❑ Folosite între AS-uri
- ❑ Scop principal: flexibilitatea de a putea alege calea preferată care nu întotdeauna este cea mai scurtă.



Short routing quiz

- ▶ Ce este distanța administrativă?
 - ▶ Ce este metrica?
 - ▶ Se primesc următoarele rute de către un ruter. Ce rute vor fi introduse în tabela de rutare și în ce ordine?
 1. 10.10.10.0/24 [120/3]
 2. 10.10.10.128/25 [110/5]
 3. 10.10.11.0/24 [130/8]
 4. 10.10.11.0/24 [100/5]
 5. 10.10.11.0/24 [130/2]
 6. 192.168.0.0/16 [190/3]
 7. 192.168.0.0/16 [190/2]
- 

1. 10.10.10.128/25 [110/5]
2. 10.10.10.0/24 [120/3]
3. 10.10.11.0/24 [100/5]
4. 192.168.0.0/16 [190/2]

RIP (1)

- ▶ Protocol distance vector ce rulează peste **UDP port 520**
- ▶ Trimite toată tabela de rutare odată la **30 de secunde** tuturor vecinilor
- ▶ Folosește ca și metrică **hop-count (15 = ∞)**
- ▶ Are implementate funcționalități pentru îmbunătățirea timpului de convergență și evitarea buclelor de rutare
 - ❑ **Triggered updates** – imediat cum o rută este pierdută sau adăugată, aceasta informație este transmisă către toți vecinii
 - ❑ **Split horizon** - o rută nu se va transmite ruterului care este next-hop pentru ruta respectivă

RIP (2)

- ▶ RIPv1
 - ❑ Classful
 - ❑ Transmite update-uri folosind adresa 255.255.255.255
- ▶ RIPv2
 - ❑ Classless
 - ❑ Transmite update-uri folosind adresa 224.0.0.9
- ▶ Care este diferența între a transmite update-uri folosind broadcast vs multicast?

OSPF (1)

- ▶ Protocol link-state
 - ❑ Triggered updates
 - ❑ Folosește **Dijkstra** pentru a păstra în memorie un arbore a celor mai scurte căi
 - ❑ Folosește bandwidth ca și cost (formula costului = $10^8/\text{bandwidth}$)
- ▶ Rulează direct peste IP (IP protocol **number 89**)
 - ❑ Implementează propriul sistem de ACK-uri
- ▶ Distanță administrativă: **110**

OSPF (2)

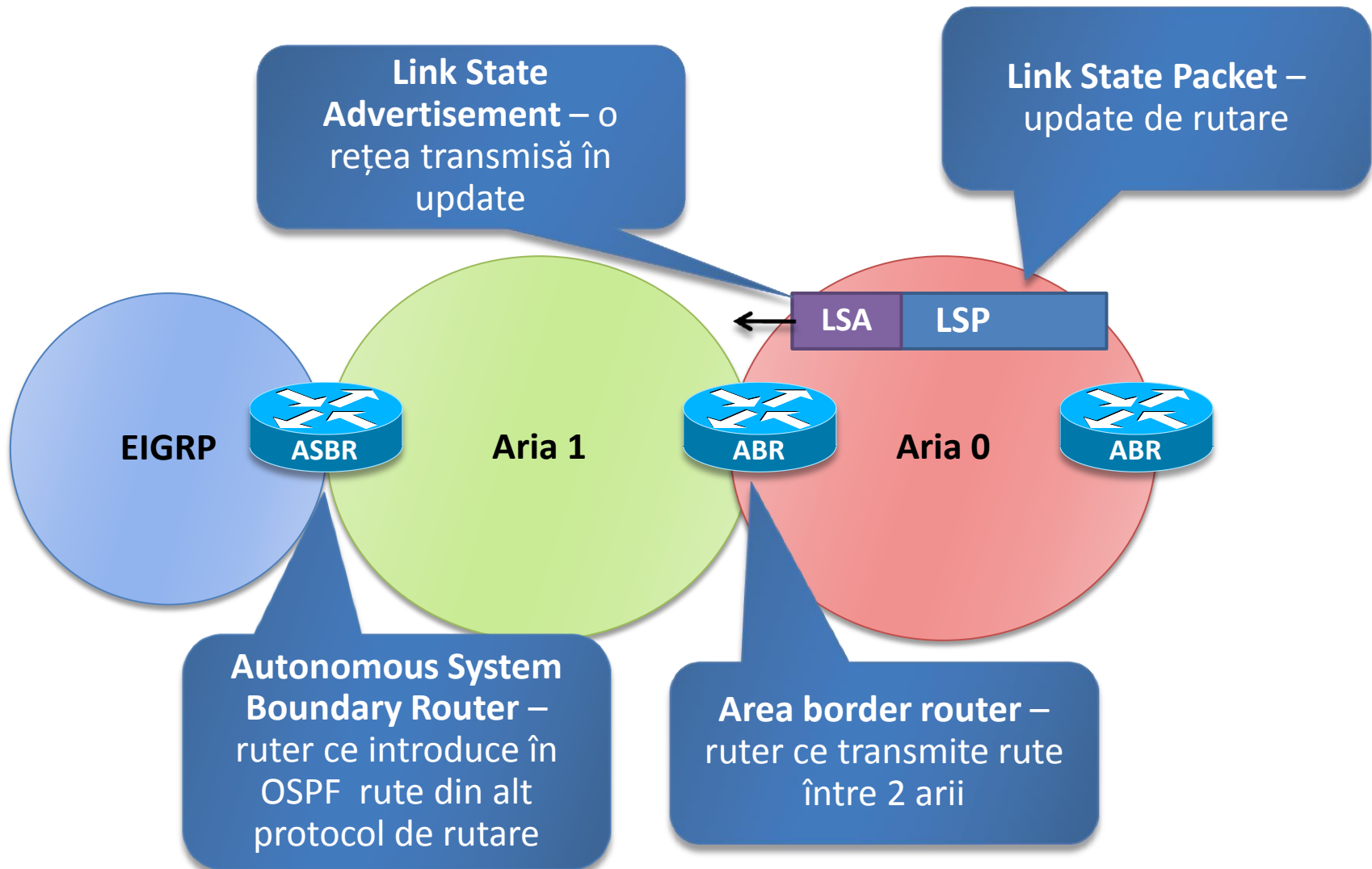
- ▶ Folosește multicast pentru transmiterea update-urilor
 - ❑ 224.0.0.5, 224.0.0.6
- ▶ Creează adiacențe cu vecinii
 - ❑ Fiecare ruter este identificat de un Router-ID pe 32 de biți (de obicei setat de administrator)
 - ❑ Update-urile sunt transmise doar la vecini adiacenți
 - ❑ Între vecini sunt transmise mesaje Hello pentru a detecta rapid schimbările

Scalabilitatea OSPF

- ▶ Care este dezavantajul unui protocol link-state?
 - ❑ Costisitor pentru CPU
- ▶ Care este soluția implementată de OSPF?
 - ❑ Împărțirea rețelei în arii
 - ❑ Un firewall/ruter rulează full-Dijkstra doar pentru rețelele din aceeași arie cu el
- ▶ Există o singură constrângere de design la implementarea OSPF multi-area
 - ❑ Toate ariile trebuie legate la aria 0.
- ▶ OSPF permite personalizarea ariilor sale (filtrarea unor anumite tipuri de rute pentru a reduce încărcarea pe CPU)
 - ❑ Mai multe la CCNP ROUTE



OSPF multi-area - terminologie



Policy-Based routing

- ▶ Reprezintă capabilitatea de a suprascrie decizia de rutare a unui ruter/firewall
- ▶ Este o configurație statică, doar administratorul poate configura reguli pentru PBR



Bidirectional forwarding detection

- ▶ BFD este un protocol de nivel 3 folosit pentru a identifica un link-failure chiar și atunci când link-ul nu suportă astfel de metode (Ethernet, MPLS, tunele etc.)
- ▶ Standardizat în 2010 în
 - ❑ RFC 5580 – descrie folosirea BFD ca o metodă generală pentru verificarea link-failure indiferent de protocoalele de nivel inferior
 - ❑ RFC 5581 – descrie folosire BFD împreună cu OSPF și ISIS pentru a obține convergențe rapide
- ▶ Detectează un link-failure în <50ms (aceeași viteză cu SONET, cel mai rapid protocol serial în termeni de detectare a unui link-failure)



Cisco ASA – Routing and Switching

Suport de VLAN-uri pe ASA

ASA – Base License

| Model ASA | Număr interfețe fizice | Număr VLAN-uri |
|-----------|------------------------|----------------|
| 5510 | 5 | 0 |
| 5520 | 5 | 25 |
| 5540 | 5 | 100 |

ASA – Security Plus License

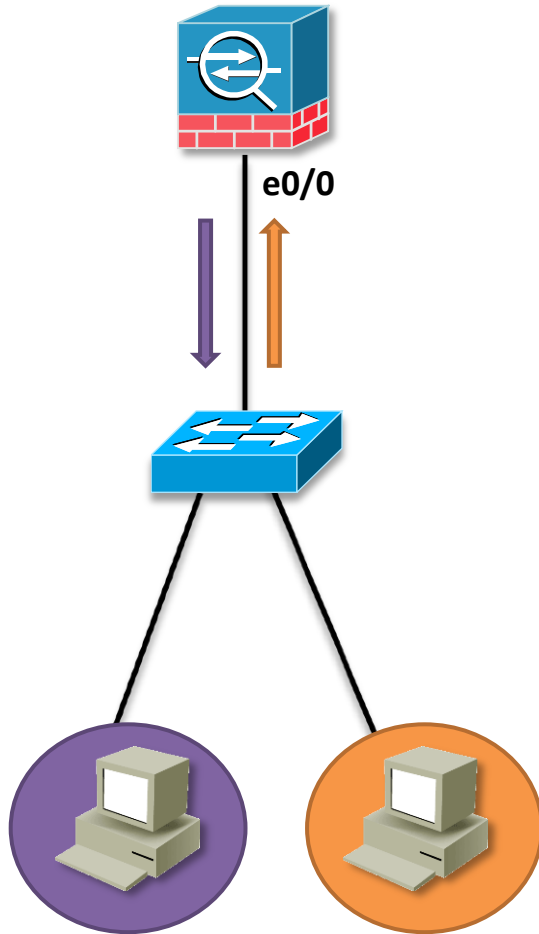
| Model ASA | Număr interfețe fizice | Număr VLAN-uri |
|-------------|------------------------|----------------|
| 5510 | 5 | 10 |
| 5520 | 5 | 25 |
| 5540 | 5 | 100 |

Definirea de VLAN-uri

- ▶ Pe ASA se pot defini VLAN-uri în 2 moduri:
 - ❑ Routed mode – VLAN-urile se definesc la nivel de subinterfață logică și sunt folosite pentru a identifica tag-ul dot1q în Inter-VLAN Routing
 - ❑ Transparent mode – VLAN-urile se definesc la nivel de interfață fizică și funcționează la fel ca pe un switch
- ▶ În continuare se va studia Routed mode

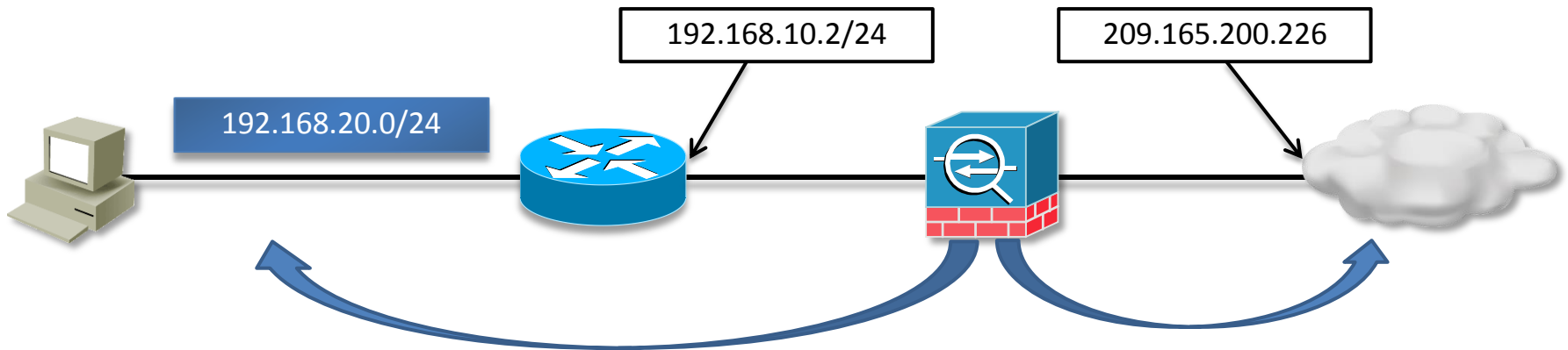
```
Waters(config)# int e0/0.20
Waters(config-subif)# vlan 20
Waters(config-subif)# nameif inside_20
INFO: Security level for "inside_20" set to 0 by default.
Waters(config-subif)# ip address 10.20.0.1 255.255.255.0
Waters(config-subif)# no sh
```

Configurarea Inter-VLAN Routing



```
Waters(config)# int e0/0
Waters(config-if)# no sh
Waters(config-if)# no nameif
Waters(config-if)# no security-level
Waters(config-if)# no ip address
Waters(config)# int e0/0.20
Waters(config-subif)# vlan 20
Waters(config-subif)# nameif inside_20
Waters(config-subif)# ip address 10.20.0.1 255.255.255.0
Waters(config-subif)# no sh
Waters(config-subif)# security-level 75
Waters(config)# int e0/0.30
Waters(config-subif)# vlan 30
Waters(config-subif)# nameif inside_30
Waters(config-subif)# ip address 10.30.0.1 255.255.255.0
Waters(config-subif)# no sh
Waters(config-subif)# security-level 75
Waters(config)# same-security-traffic permit inter-interface
```

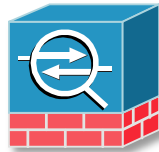

Rutare statică



```
Waters(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.226 1
Waters(config)# route inside 192.168.20.0 255.255.255.0
192.168.10.2 1
```

- ▶ Cifra folosită ca ultim parametru definește **distanța administrativă**
- ▶ Se pot configura maxim 3 rute statice cu aceeași distanță administrativă și cu aceeași interfață de ieșire pentru load-balancing

Vizualizarea tabelii de rutare



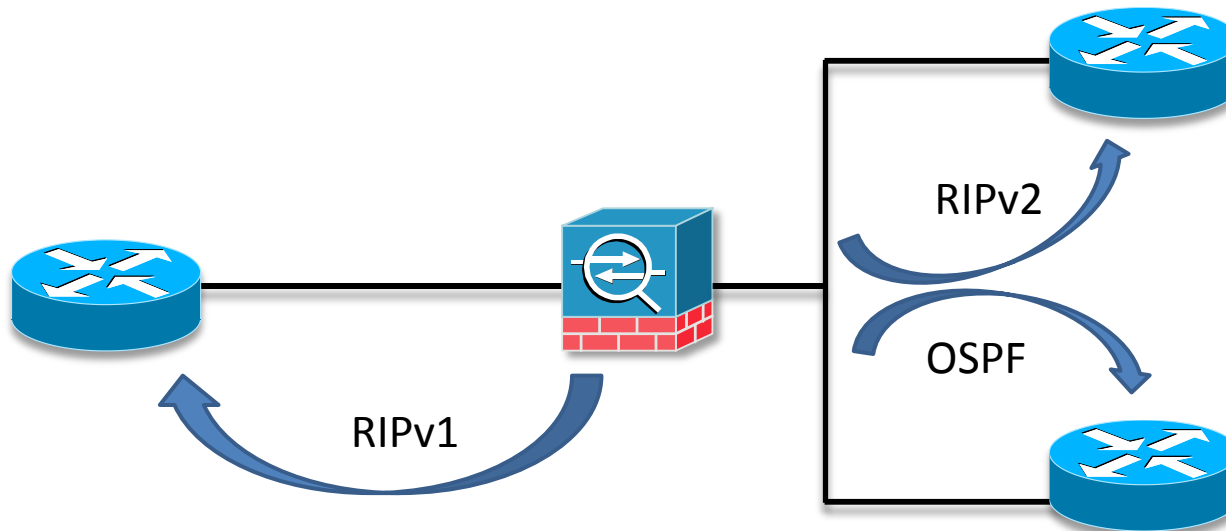
```
Waters# show route
```

```
S    0.0.0.0 0.0.0.0 [1/0] via 209.165.200.226, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
S    192.168.20.0 255.255.255.0 [1/0] via 192.168.10.2, inside
C    209.165.200.224 255.255.255.224 is directly connected,
outside
```

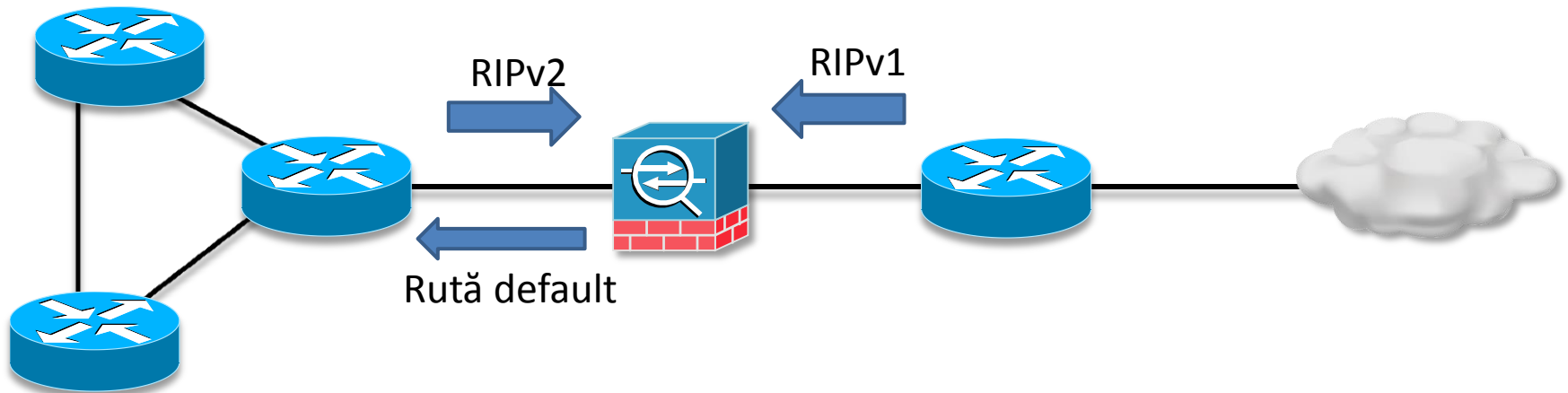
- ▶ Ca și în IOS, nu reflectă ordinea în care rutele vor fi procesate la rutarea unui pachet

Protocoale de rutare

- ▶ ASA suportă:
 - ❑ RIP v1/v2
 - ❑ OSPF
- ▶ ASA nu suportă:
 - ❑ BGP
 - ❑ PBR
- ▶ Poate rula toate 3 protocoalele în același timp



Configurarea RIP



```
Chicago# configure terminal
Chicago(config)# rip inside passive version 2
Chicago(config)# rip inside default version 2
Chicago(config)# rip outside passive version 1
```

- ▶ Cuvântul cheie **default** injectează o rută default spre inside
- ▶ Cuvântul cheie **passive** împiedică RIP să trimită update-uri pe interfața respectivă

RIPv2 - autentificare

- ▶ RIPv2 suportă autentificarea update-urilor
 - ❑ Plain text sau MD5

```
Chicago# configure terminal
Chicago(config)# rip inside default version 2 authentication
md5 cisco 1
```

- ▶ Vizualizarea tabelii de rutare

```
Chicago# show route
R    0.0.0.0 0.0.0.0 [120/1] via 209.165.200.226, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
R    192.168.20.0 255.255.255.0 [120/1] via 192.168.10.2, inside
R    192.168.13.0 255.255.255.0 [120/2] via 192.168.10.2, inside
C    209.165.200.224 255.255.255.224 is directly connected, outside
```

Depanarea RIP

- ▶ RIPv1 nu este compatibil cu RIPv2

```
Chicago# debug rip
debug rip enabled at level 1
Chicago# RIP: interface inside sending v2 update to 224.0.0.9
RIP: received packet from interface inside [pif=2]
      (192.168.10.2:520)
RIP: interface inside received v1 update from 192.168.10.2
```

- ▶ Pot exista probleme de autentificare

```
Router# debug ip rip
2d09h: RIP: received packet with MD5 authentication
2d09h: RIP: ignored v2 packet from 192.168.10.1 (invalid
authentication)
```

OSPF

- ▶ Migrarea la OSPF – care este comanda care șterge toate configurațiile RIP din memoria ASA?
 - ❑ clear configure rip
- ▶ Configurarea OSPF

```
Chicago# configure terminal
Chicago(config)# router ospf 1
Chicago(config-router)# network 192.168.10.0 255.255.255.0 area 0
Chicago(config-router)# exit
```

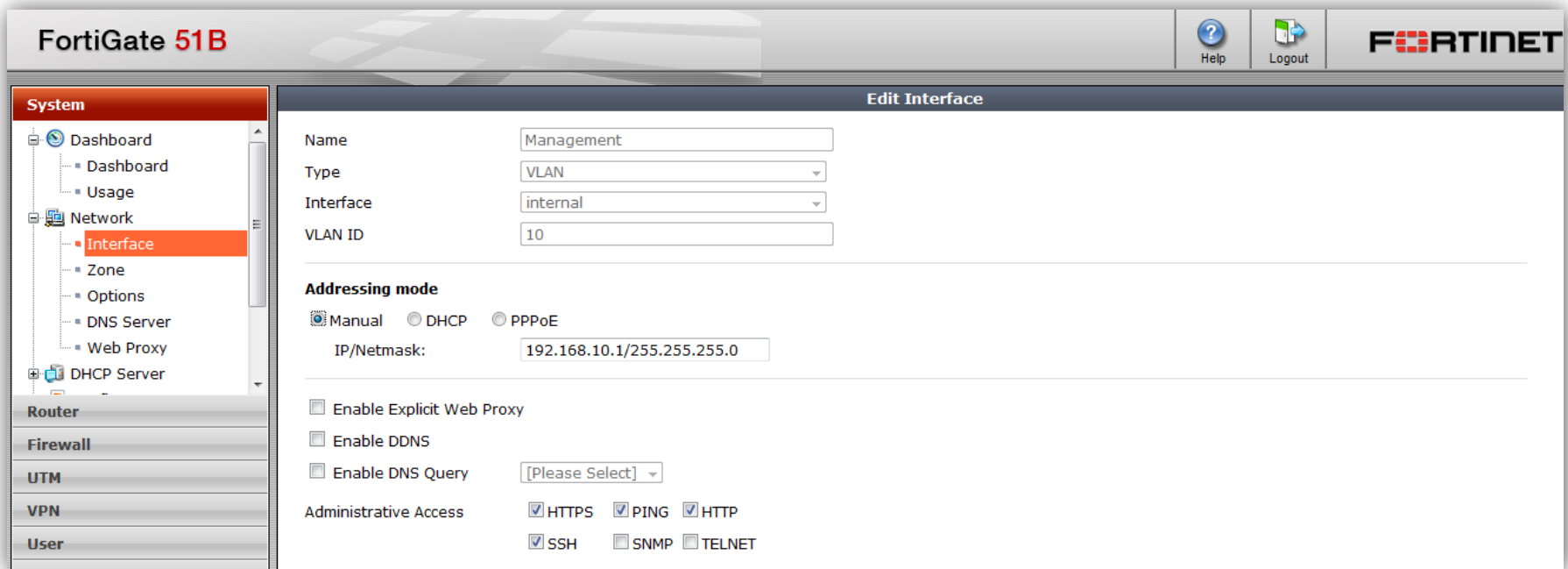
- ▶ Pentru cei obișnuiți cu IOS: atenție, nu se folosește wildcard, ci masca de rețea



Fortinet – Routing and Switching

VLAN-uri

- ▶ Pe FortiOS se creează interfețe virtuale de tip “VLAN” care se atașează interfețelor fizice
- ▶ Se definesc din aceeași interfață ca interfețele fizice



The screenshot displays the FortiGate 51B web management interface. The top navigation bar includes the device name 'FortiGate 51B', a 'Help' icon, a 'Logout' icon, and the 'FORTINET' logo. The left sidebar shows a tree view with categories: System, Router, Firewall, UTM, VPN, and User. Under 'System', the 'Network' section is expanded, and 'Interface' is selected. The main content area is titled 'Edit Interface' and contains the following configuration fields:

- Name: Management
- Type: VLAN
- Interface: internal
- VLAN ID: 10

Addressing mode

- Manual DHCP PPPoE
- IP/Netmask: 192.168.10.1/255.255.255.0

Enable Explicit Web Proxy

Enable DDNS

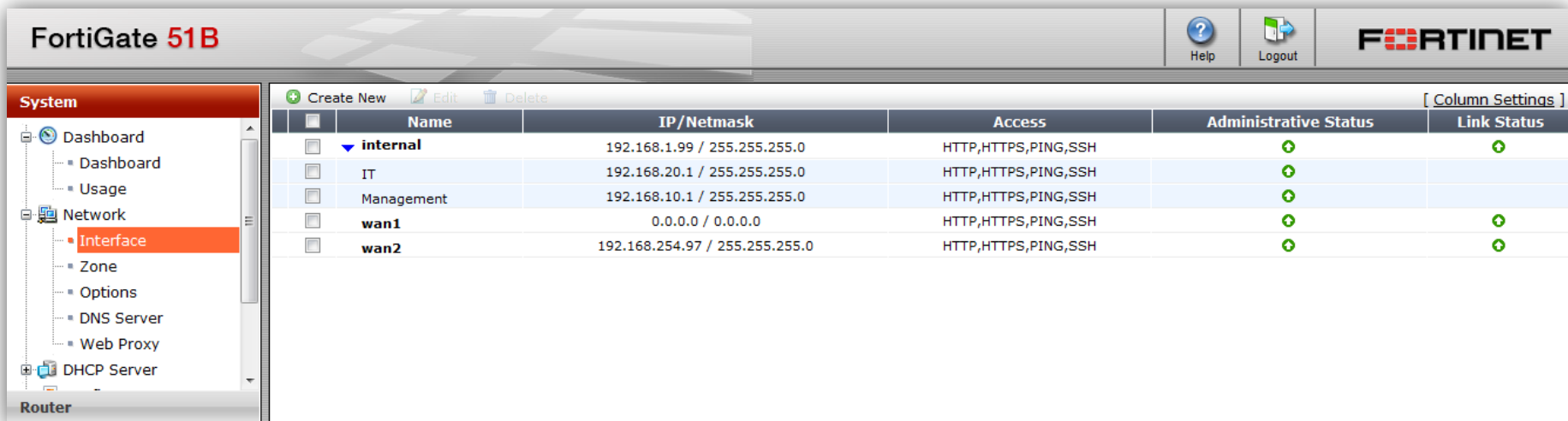
Enable DNS Query [Please Select]

Administrative Access

- HTTPS PING HTTP
- SSH SNMP TELNET

VLAN Nativ

- ▶ 802.1q suportă noțiunea de VLAN nativ (VLAN care nu este tagged peste un trunk)
- ▶ Este permisă configurarea unui IP pe interfața fizică (se consideră trafic din VLAN nativ)
- ▶ Interfețele VLAN nu au link-status, fiind virtuale



FortiGate 51B

Help Logout FORTINET

System

- Dashboard
- Usage
- Network
 - Interface
 - Zone
 - Options
 - DNS Server
 - Web Proxy
- DHCP Server

Router

Create New Edit Delete [Column Settings]

| | Name | IP/Netmask | Access | Administrative Status | Link Status |
|--------------------------|------------|--------------------------------|---------------------|-----------------------|-------------|
| <input type="checkbox"/> | ▼ internal | 192.168.1.99 / 255.255.255.0 | HTTP,HTTPS,PING,SSH | ⬆ | ⬆ |
| <input type="checkbox"/> | IT | 192.168.20.1 / 255.255.255.0 | HTTP,HTTPS,PING,SSH | ⬆ | |
| <input type="checkbox"/> | Management | 192.168.10.1 / 255.255.255.0 | HTTP,HTTPS,PING,SSH | ⬆ | |
| <input type="checkbox"/> | wan1 | 0.0.0.0 / 0.0.0.0 | HTTP,HTTPS,PING,SSH | ⬆ | ⬆ |
| <input type="checkbox"/> | wan2 | 192.168.254.97 / 255.255.255.0 | HTTP,HTTPS,PING,SSH | ⬆ | ⬆ |

Inter-VLAN routing

- ▶ Pentru a putea trece trafic între interfețele de tip VLAN, trebuie create politici de firewall
 - ❑ dacă se dorește ca traficul să poată fi inițiat din oricare VLAN, este nevoie de 2 politici

FortiGate 51B

Help Logout FORTINET

System

Router

Firewall

Policy

- Policy
- Central NAT Table
- DoS Policy
- Sniffer Policy
- Protocol Options

Address

Service

Schedule

Traffic Shaper

UTM

VPN

User

WAN Opt. & Cache

Endpoint

Log&Report

New Policy

Source Interface/Zone: Management

Source Address: all Multiple

Destination Interface/Zone: IT

Destination Address: all Multiple

Schedule: always

Service: ANY Multiple

Action: ACCEPT

Log Allowed Traffic

NAT

No NAT

Enable NAT Dynamic IP Pool

Use Central NAT Table

Enable Identity Based Policy

UTM

Traffic Shaping [Please Select]

Routing panel

► Fortinet suportă protocoalele dinamice:

- RIP
- OSPF
- Full-BGP (iBGP, eBGP)

FortiGate 51B

Help Logout FORTINET

System

Router

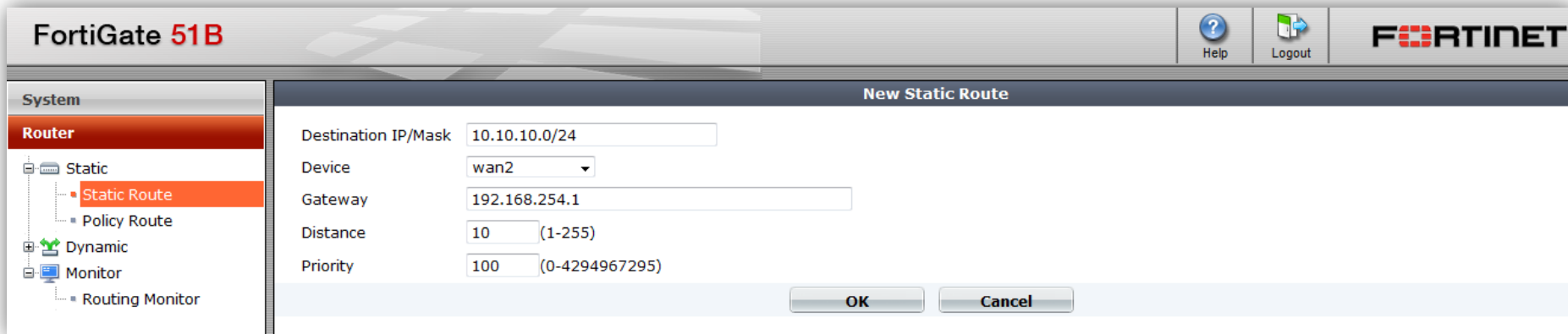
- Static
 - Static Route
 - Policy Route
- Dynamic
- Monitor
 - Routing Monitor

Type: All Network: Gateway: Apply Filter

| Type | Subtype | Network | Distance | Metric | Gateway | Interface | Up Time (d h:m:s) |
|-----------|---------|------------------|----------|--------|---------------|------------|-------------------|
| Static | | 0.0.0.0/0 | 10 | 0 | 192.168.254.1 | wan2 | |
| Connected | | 192.168.1.0/24 | 0 | 0 | 0.0.0.0 | internal | |
| Connected | | 192.168.10.0/24 | 0 | 0 | 0.0.0.0 | Management | |
| Connected | | 192.168.20.0/24 | 0 | 0 | 0.0.0.0 | IT | |
| Connected | | 192.168.254.0/24 | 0 | 0 | 0.0.0.0 | wan2 | |

Rute statice

- ▶ Distanța administrativă e implicit 10
- ▶ Pe lângă distanța administrativă, FortiOS permite specificarea priorității pentru o rută
 - ❑ Prioritatea implicită e 0
 - ❑ Prioritatea mai mică = mai bună



The screenshot displays the FortiGate 51B web interface. The top navigation bar includes the device name 'FortiGate 51B', a 'Help' icon, a 'Logout' icon, and the 'FORTINET' logo. The left sidebar shows the 'System' menu with 'Router' selected, and a sub-menu containing 'Static', 'Dynamic', and 'Monitor'. Under 'Static', 'Static Route' is highlighted. The main content area is titled 'New Static Route' and contains the following configuration fields:

| | |
|---------------------|---|
| Destination IP/Mask | <input type="text" value="10.10.10.0/24"/> |
| Device | <input type="text" value="wan2"/> |
| Gateway | <input type="text" value="192.168.254.1"/> |
| Distance | <input type="text" value="10"/> (1-255) |
| Priority | <input type="text" value="100"/> (0-4294967295) |

At the bottom of the form are two buttons: 'OK' and 'Cancel'.

ECMP

- ▶ Equal-Cost Multi-Path – este de fapt load-balancing folosit mai multe rute statice
- ▶ Poate fi controlat funcție de diferite criterii
 - ❑ IP sursă – se face load balancing funcție de adresa IP sursă a pachetelor; aceasta este setarea implicită
 - ❑ Weighted – se configurează ponderi pentru fiecare interfață de ieșire, iar traficul este balansat funcție de aceste ponderi
 - ❑ Spill-over – pentru fiecare interfață de ieșire a unei rute statice, se configurează o limită de bandă; când această limită este depășită, se folosește următoarea rută statică (traficul face spill-over).

```
config system settings
  set v4-ecmp-mode {source-ip-based | usage-based |
  weight-based}
end
```

ECMP

- ▶ ECMP suportă detecția gateway-ului și comutarea automată pe următoarea rută statică

The screenshot displays the FortiGate 51B web interface. The left sidebar shows the navigation menu with 'Interface' selected under the 'Network' category. The main content area is titled 'Edit Interface' and contains the following configuration options:

- Enable Explicit Web Proxy
- Enable DDNS
- Override Default MTU Value: 1500 (bytes)
- Administrative Access: HTTPS, PING, HTTP, SSH, SNMP, TELNET
- Detect Interface Status for Gateway Load Balancing
 - Detect Server: 192.168.254.1
 - Detect Protocol: Ping, TCP Echo, UDP Echo
 - Weight: 0
 - Spillover Threshold: 0 KBps
- Description (63 characters): [Empty text box]
- Administrative Status: Up, Down

At the bottom of the page, there are three buttons: 'OK', 'Cancel', and 'Apply'.

PBR

- ▶ Tabela de policy-route este analizată înaintea tabelii de rutare
- ▶ Suportă specificarea
 - IP Protocol
 - Interfețe
 - Adrese IP
 - ToS și porturi destinație

FortiGate 51B

Help Logout FORTINET

System

Router

- Static
 - Static Route
 - Policy Route
- Dynamic
 - RIP
 - OSPF
 - BGP
 - Multicast
- Monitor
 - Routing Monitor

Firewall

New Routing Policy

If incoming traffic matches:

Protocol: 0

Incoming interface: internal

Source address / mask: 0.0.0.0/0.0.0.0

Destination address / mask: 0.0.0.0/0.0.0.0

Destination Ports: From: 1 To: 65535

Type of Service: bit pattern: 00 (hex) bit mask: 00 (hex)

Force traffic to:

Outgoing interface: [dropdown]

Gateway Address: 0.0.0.0

OK Cancel

RIP

- ▶ Ce controlează parametrul **default-information-originate**?
- ▶ Se pot seta timerele, activa protocolul și redistribui rute

FortiGate 51B

System

Router

Static

Dynamic

RIP

OSPF

BGP

Multicast

Monitor

Firewall

UTM

VPN

User

WAN Opt. & Cache

Endpoint

Log&Report

RIP Version 1 2

▼ Advanced Options(Defaults, Timers, Route Redistribution)

Default Metric (1-16)

Enable Default-information-originate

RIP Timers:(seconds)

Update Timeout Garbage

Redistribute:

Connected OSPF

Metric (1-16) Metric (1-16)

Static BGP

Metric (1-16) Metric (1-16)

Apply

Networks

IP/Netmask: Add

Delete

IP/Netmask

No RIP network defined.

Interfaces

Edit Delete

Create New

| Interface | Version | | Authentication | Passive |
|---------------------------|---------|---------|----------------|---------|
| | Send | Receive | | |
| No RIP Interface defined. | | | | |

OSPF

- ▶ Pe FortiOS Router-ID-ul trebuie configurat manual
 - ❑ Nu se poate activa OSPF dacă RID-ul nu este configurat

FortiGate 51B

Router ID: 0.0.0.0

Advanced Options (Default, Redistribution)
Default Information: None Regular Always

Redistribute

| | | | |
|------------------------------------|-------------------------|------------------------------|-------------------------|
| <input type="checkbox"/> Connected | Metric: 10 (1-16777214) | <input type="checkbox"/> RIP | Metric: 10 (1-16777214) |
| <input type="checkbox"/> Static | Metric: 10 (1-16777214) | <input type="checkbox"/> BGP | Metric: 10 (1-16777214) |

Areas

Create New Edit Delete

| Area | Type | Authentication |
|-----------------------|------|----------------|
| No OSPF area defined. | | |

Networks

Create New Edit Delete

| Network | Area |
|--------------------------|------|
| No OSPF network defined. | |

Interfaces

Create New Edit Delete

| Name | Interface | IP | Authentication |
|----------------------------|-----------|----|----------------|
| No OSPF interface defined. | | | |

BFD

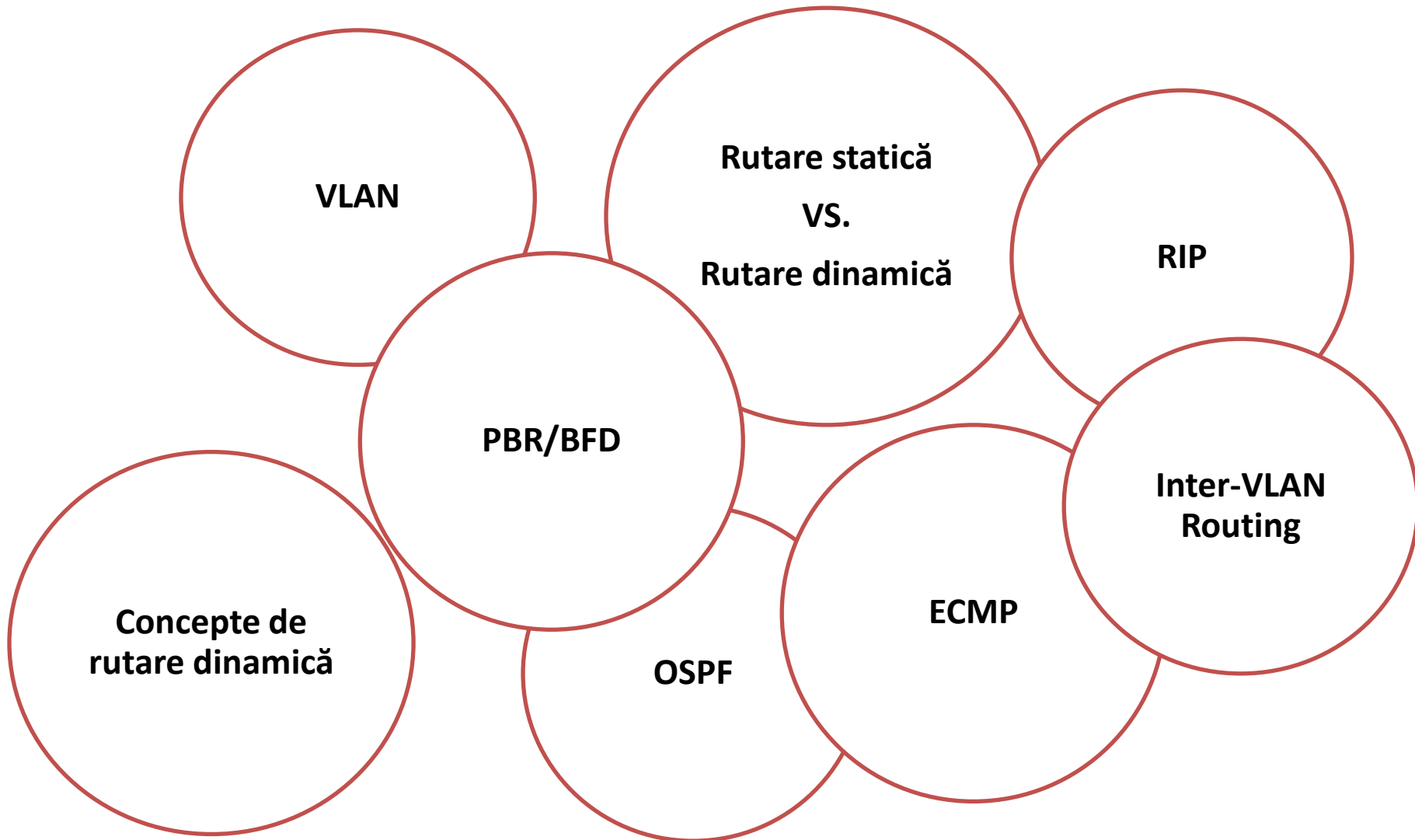
- ▶ Se poate activa pe tot echipamentul FortiGate

```
config system settings
set bfd enable
set bfd-desired-min-tx 50
set bfd-required-min-rx 50
set bfd-detect-mult 3
```

- ▶ Se poate activa/dezactiva la nivel de interfață

```
config system interface
edit <interface>
set bfd disable
end
```

Overview



Cursul viitor...

- ▶ Virtual Firewalling
 - ❑ ASA – contexte de securitate
 - ❑ FortiGate - VDOM-uri

