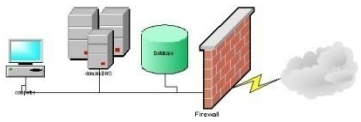
Hálózati rendszerek adminisztrációja JunOS OS alapokon

- áttekintés és példák -

Varga Pál

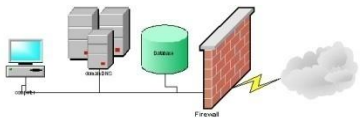
pvarga@tmit.bme.hu

BME VIK TMIT

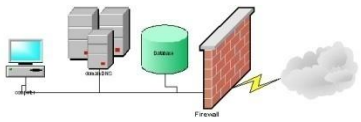


Áttekintés

- Általános laborismeretek
- Junos OS – bevezető
- Routing - alapok
- Tűzfalbeállítás – alapok
- A mérés indulása – kivonat a jegyzőkönyv-vázból



ÁLTALÁNOS LABORISMERETEK

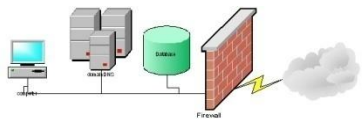


Általános laborismeretek

- A használandó Junos OS-alapú eszközök a TMIT-en futnak, virtuális gépekbe ágyazva
- A HSZK-ból távoli eléréssel kapcsolódunk hozzájuk, és ezen keresztül konfiguráljuk őket
- A feladatok mellett: apró segítségek
  - Milyen parancsot használjunk:

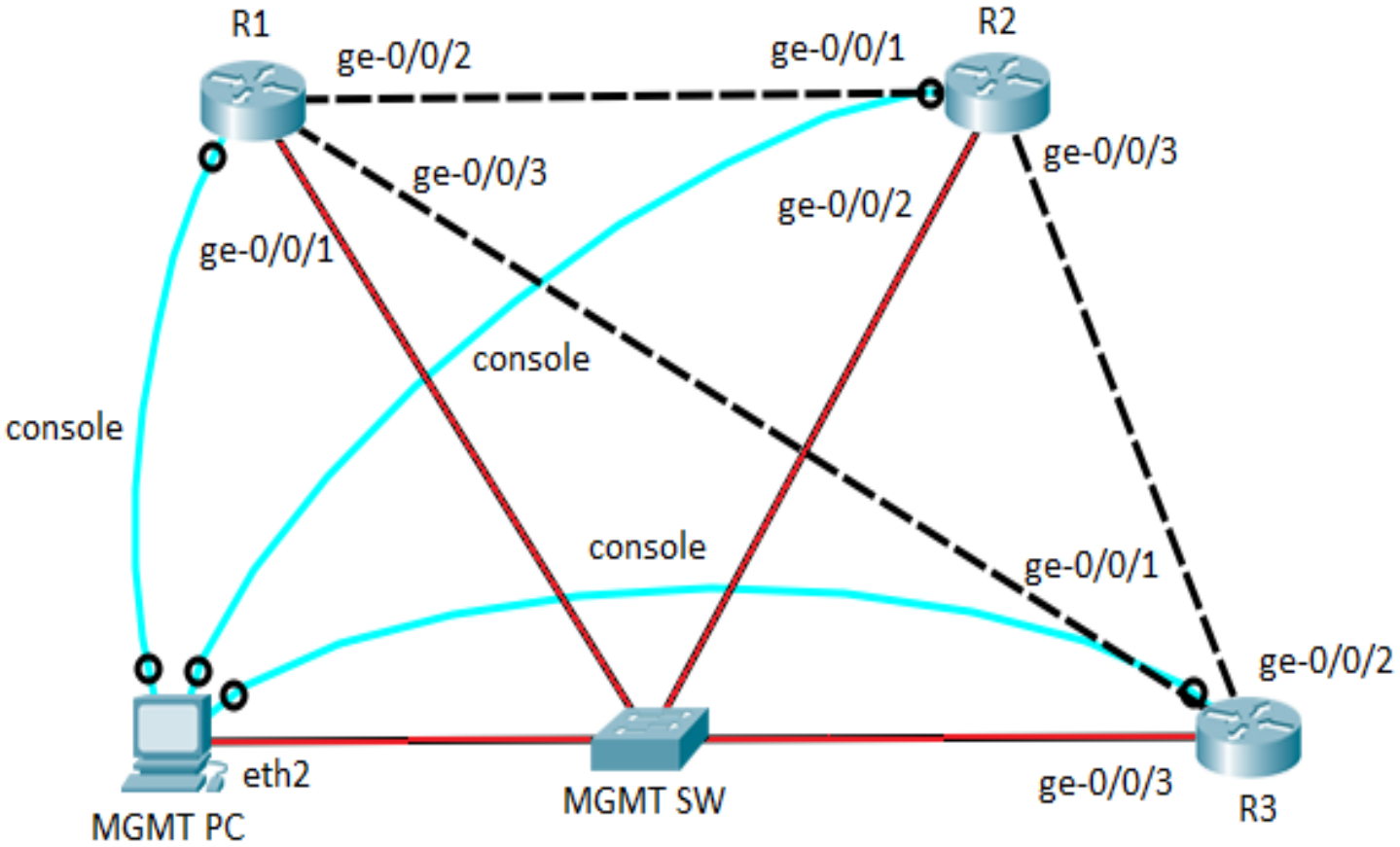
    ?

    Google it!
  - Parancsok opciói/kapcsolói/szintaxisa: helyben kitalálandó!
- Hasznos felkészülés - Junos OS mérési segédlet



Mérési konfiguráció

- Mindenkinek saját maga által adminisztrált, több eszközből álló konfigurációja van



Interfészek elnevezése

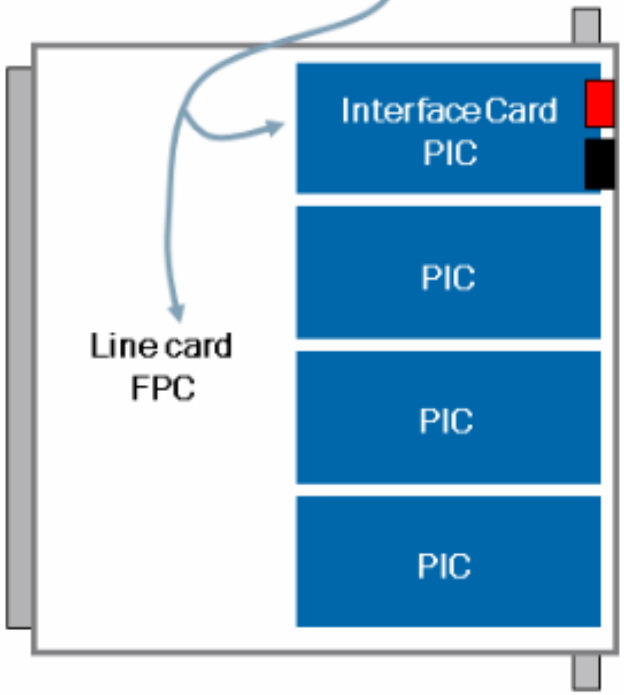
- Most interfaces are named according to:
  - Interface media type (ge, so, at, and so forth)
  - Line card (FPC) slot number
  - Interface card (PIC) slot number
  - Port number

Note: While different platforms use different names for line cards and interface cards, the CLI almost always uses FPC and PIC

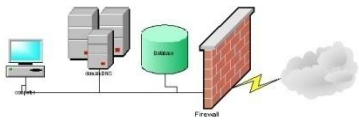
Interface naming example:

ge-0/2/3 = port 3 of a Gigabit Ethernet PIC in slot 2 on FPC 0

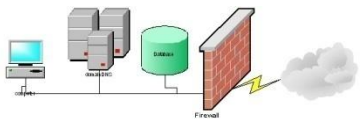
Note: Slot and port numbering begins with zero (0) rather than one (1)



- Other interface name designations exist, such as `lo0`, `vlan`, `ae`, and so forth

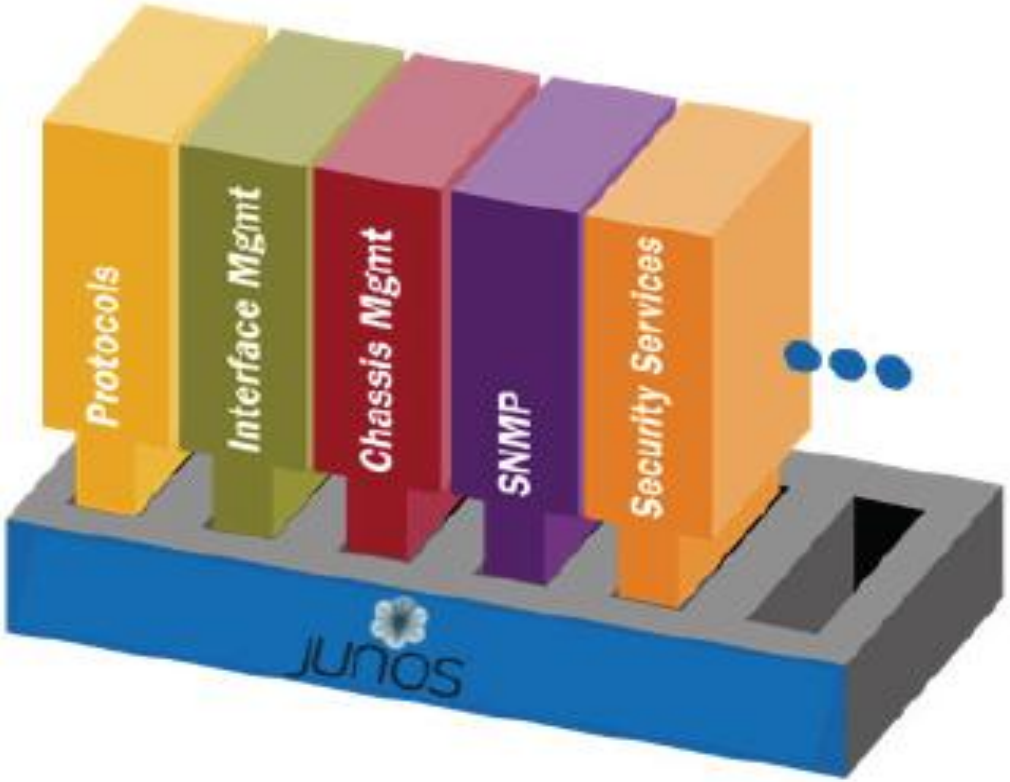


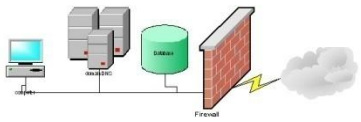
JUNOS OS - BEVEZETŐ



A Junos OS működése

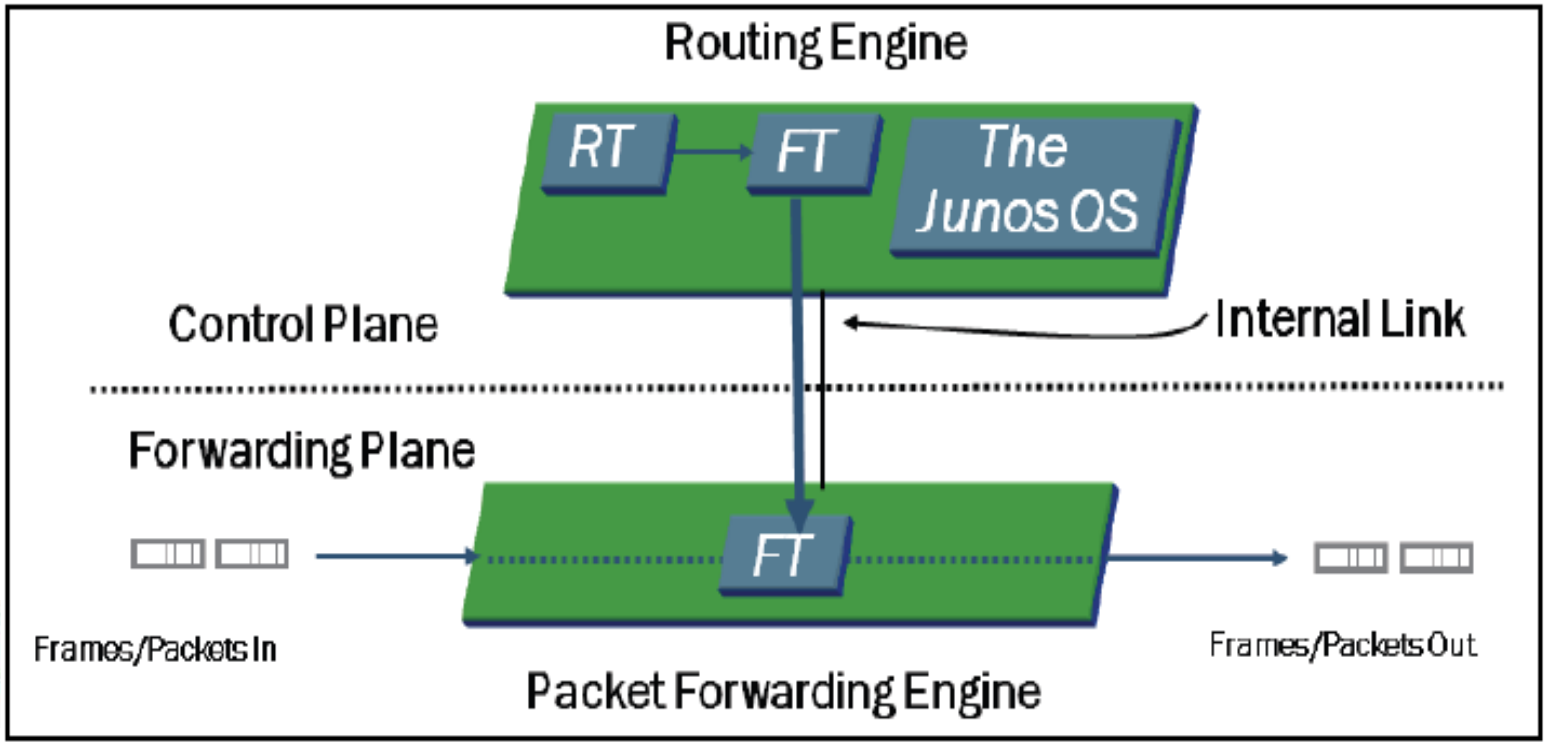
- Moduláris felépítésű, FreeBSD UNIX alapú OS
- A működési folyamatoknak saját memóriaterületük van





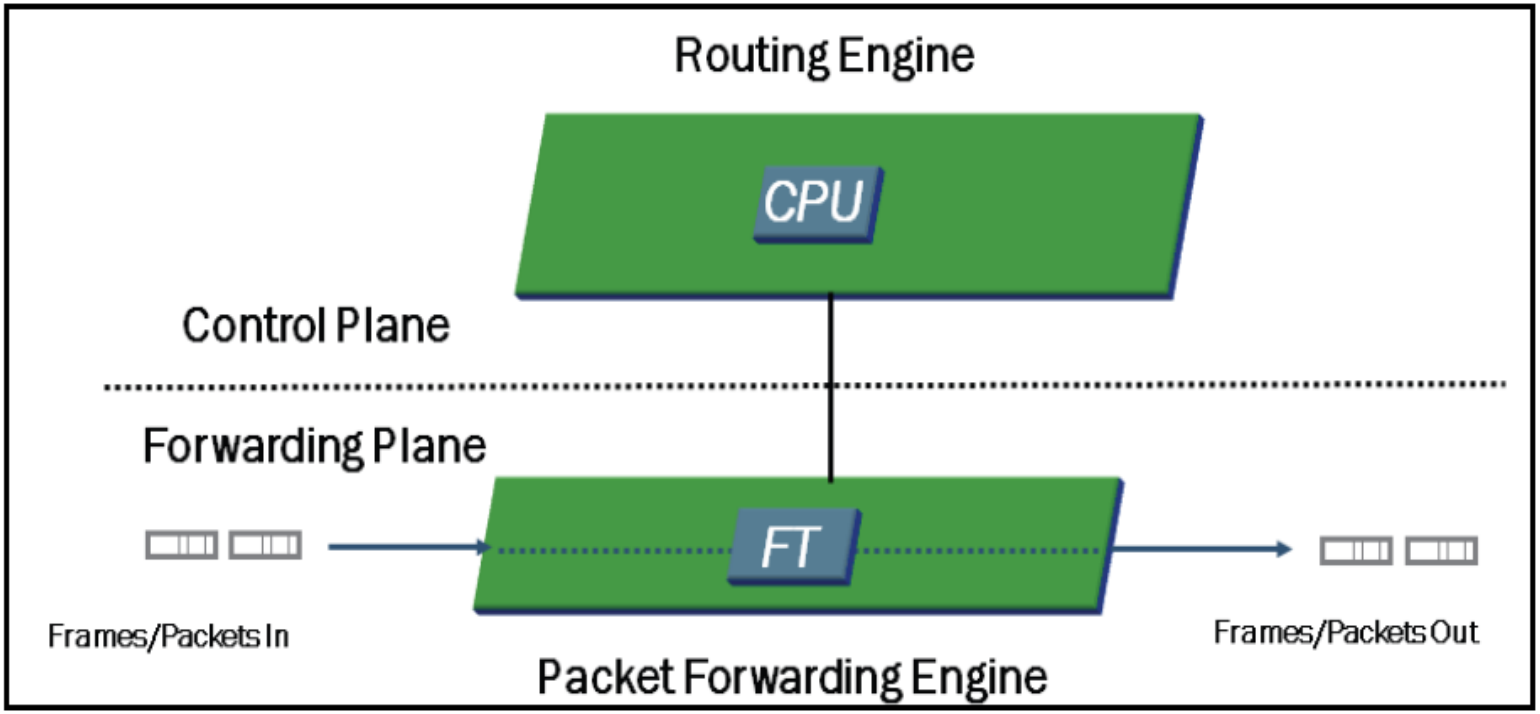
Routing / Switching

- A protokollok vezérlése és a csomagok/keretek továbbítása külön van választva
  - Vezérlési sík - Control Plane
  - Továbbítási sík - Forwarding Plane



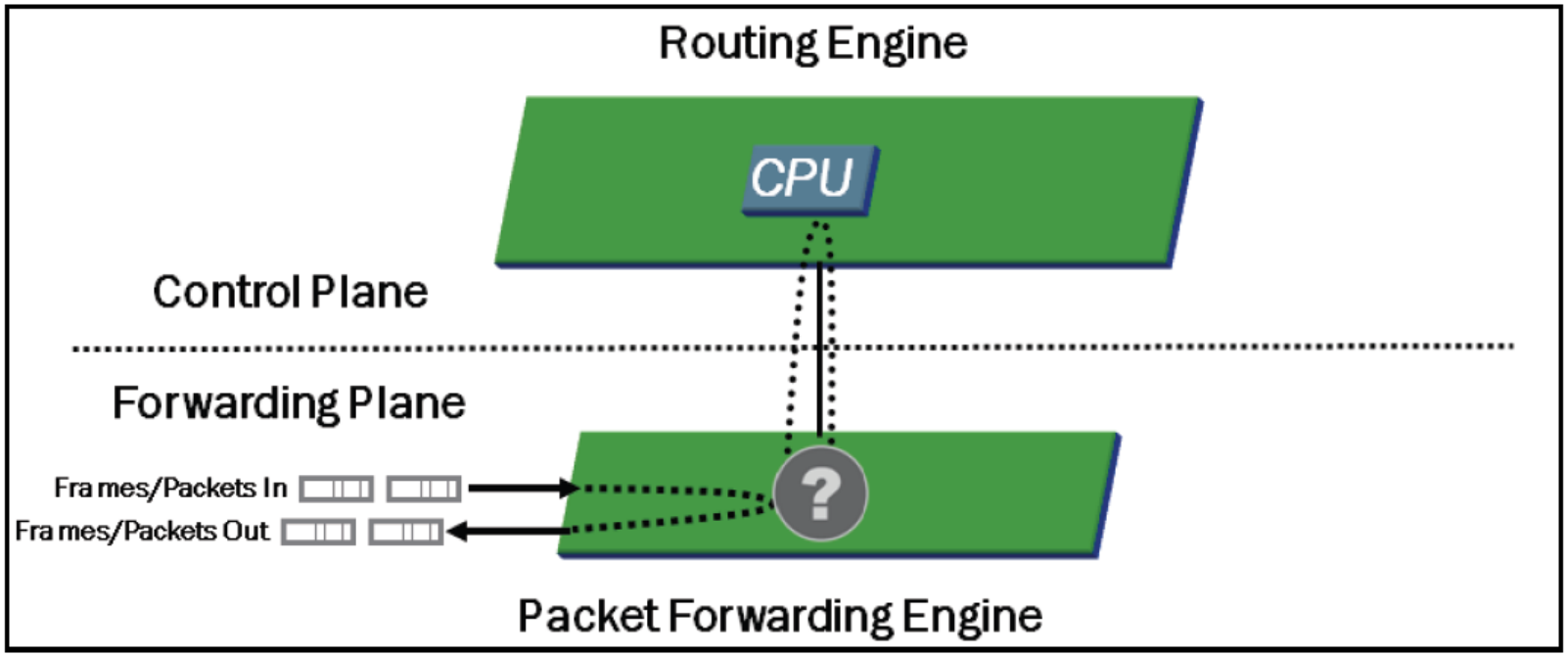
Forgalom-irányítás – 1
Áthaladó forgalom

- A beérkező csomagok/keretek az FT bejegyzéseivel összehasonlítva a legteljesebb egyezést mutató szabály szerint továbbítódnak



Forgalom-irányítás – 2
Kivételes forgalom

- A következők vezérlését a Routing Engine (RE) végzi:
  - Routing protokoll frissítések, és RE-kérések válaszai
    - telnet session, ping, traceroute
  - IP csomagok IP beállításokkal (ritka)
  - ICMP üzeneteket generáló forgalom.

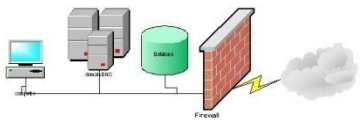


Belépés & első élmények

- Telnet, SSH vagy konzol portos csatlakozással

- **Normal user:**
- Operational módba kerülünk: **>** karakter a promptban
  - Az eszköz SW és HW-ének, hálózatának monitorozására, hibakeresés
- Configuration mód: belépés **configure** paranccsal
  - hálózati interfészek, routing protokollok, és egyéb funkciók beállítása

- **root belépéssel**
- A shell-be kerülünk: **%** karakter a promptban
- **cli** parancs segítségével kerülünk Operation módba

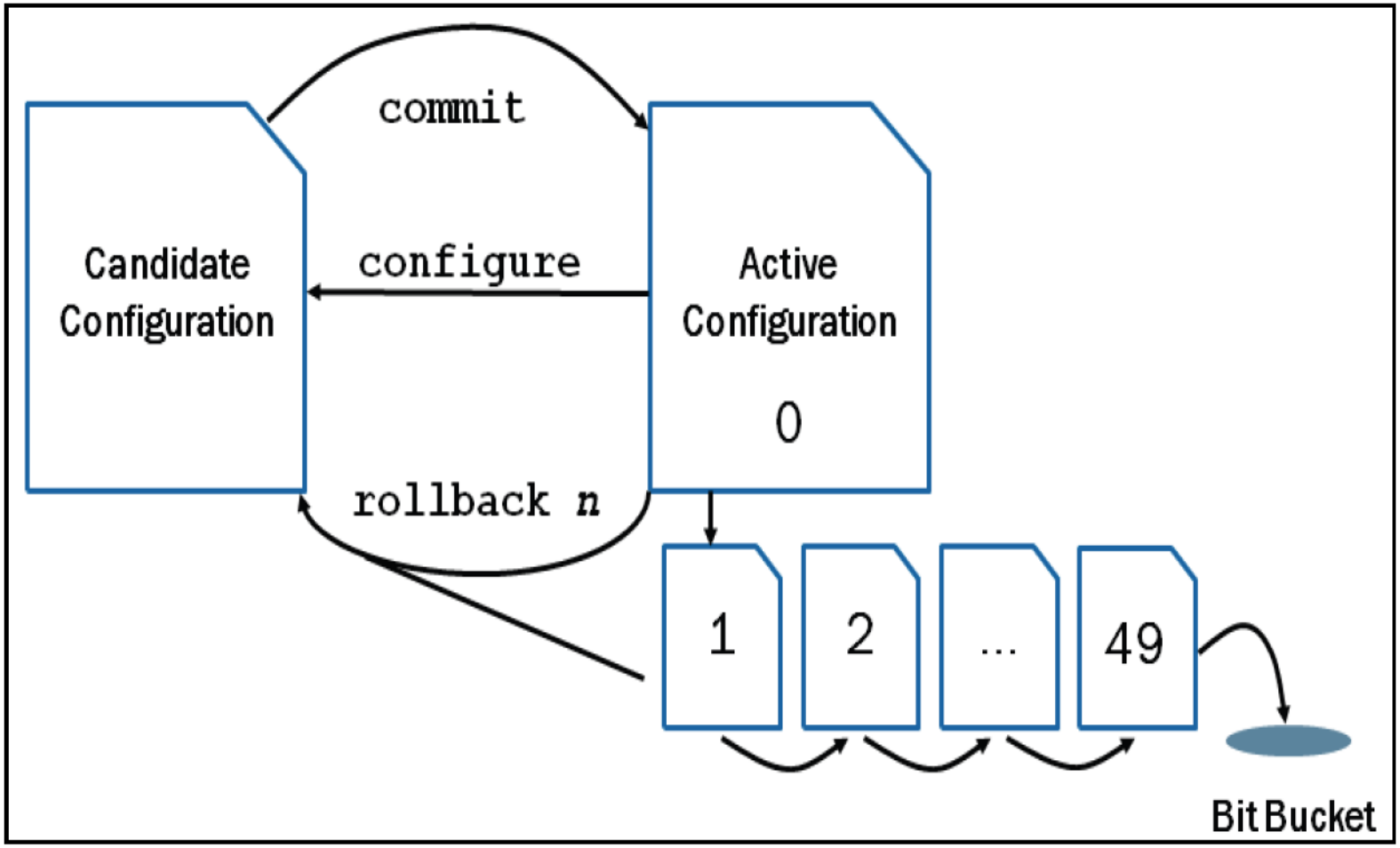


Hogyan tovább - ?

- Context-sensitive (környezetfüggő) help: ?

```
user@router> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  op                   Invoke an operation script
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  save                 Save information to file
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

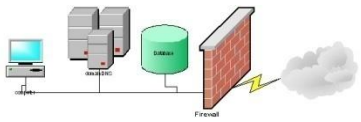
Aktív konfiguráció és konfig. jelölt



A változtatásokat érvényesíteni kell!

- commit check
  - ellenőrzi, hogy a parancsok szintaktikailag helyesek-e

- commit confirmed
- commit confirmed time-out <n>
  - default időn belül…, illetve
  - <n> percen belül újabb commit-ot vár, különben rollback 1



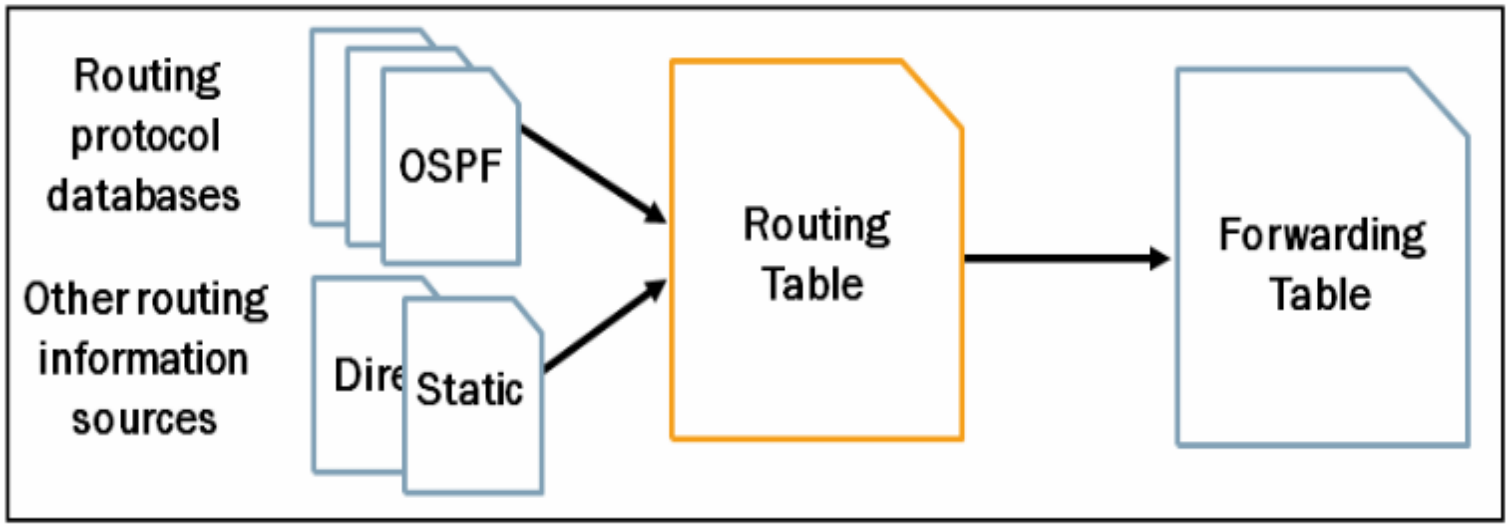
Nézzük meg, milyen lett a konfig…

- Use `show configuration` to view the results:

```
root@router> show configuration
## Last commit: 2011-05-01 21:00:46 UTC by root
version 12.1R1.9;
system {
    host-name host;
    time-zone America/Los_Angeles;
    root-authentication {
        encrypted-password "$1$e/FUEOVo$JF6NiAZxuufGFxDs1OMAr/"; ##
SECRET-DATA
    }
    services {
        ssh;
        telnet;
    }
    syslog {
...
```

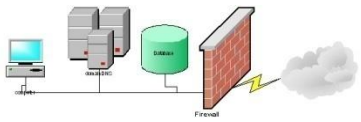
Routing beállítások

- Statikus routing
  - az útvonalat az adminisztrátora kézzel állítja be
- Dinamikus routing
  - különféle routing protokollok segítségével választódnak ki a megfelelő útvonalak
    - RIP: Routing Information Protocol
    - OSPF: Open Shortest Path First



Előre definiált routing táblák

- `inet.0`: Used for IPv4 unicast routes;
- `inet.1`: Used for the multicast forwarding cache;
- `inet.2`: Used for Multicast Border Gateway Protocol (MBGP) routes to provide reverse path forwarding (RPF) checks;
- `inet.3`: Used for MPLS path information;
- `inet.4`: Used for Multicast Source Discovery Protocol (MSDP) route entries;
- `inet6.0`: Used for IPv6 unicast routes; and
- `mpls.0`: Used for MPLS next hops.

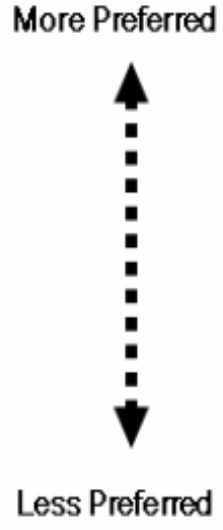


Melyik tábla alapján lesz kiválasztva az útvonal?

- Ha egy hálózat felé többféle forrásból is rendelkezésre áll routing információ, akkor a preferencia-érték dönt

Route Preference Values

Routing Information Source	Default Preference
Direct	0
Local	0
Static	5
OSPF internal	10
RIP	100
OSPF AS external	150
BGP (both EBGP and IBGP)	170



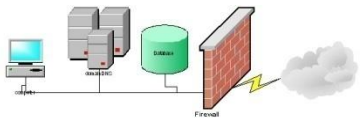
Routing tábla példa

```
user@router> show route

inet.0: 6 destinations, 7 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.1.1.0/24             *[Static/5] 00:10:24
                         > to 172.29.30.253 via ge-0/0/10.0
                        [OSPF/10] 00:03:38, metric 2
                         > to 172.18.25.2 via ge-0/0/13.0
172.18.25.0/30          *[Direct/0] 00:11:05
                         > via ge-0/0/13.0
172.18.25.1/32          *[Local/0] 00:11:05
                            Local via ge-0/0/13.0
172.29.30.0/24          *[Direct/0] 00:11:05
                         > via ge-0/0/10.0
172.29.30.1/32          *[Local/0] 00:11:05
                            Local via ge-0/0/10.0
...
```

Route source and preference

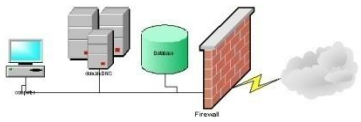
Asterisk (*) indicates that the route is selected as active

Route table name



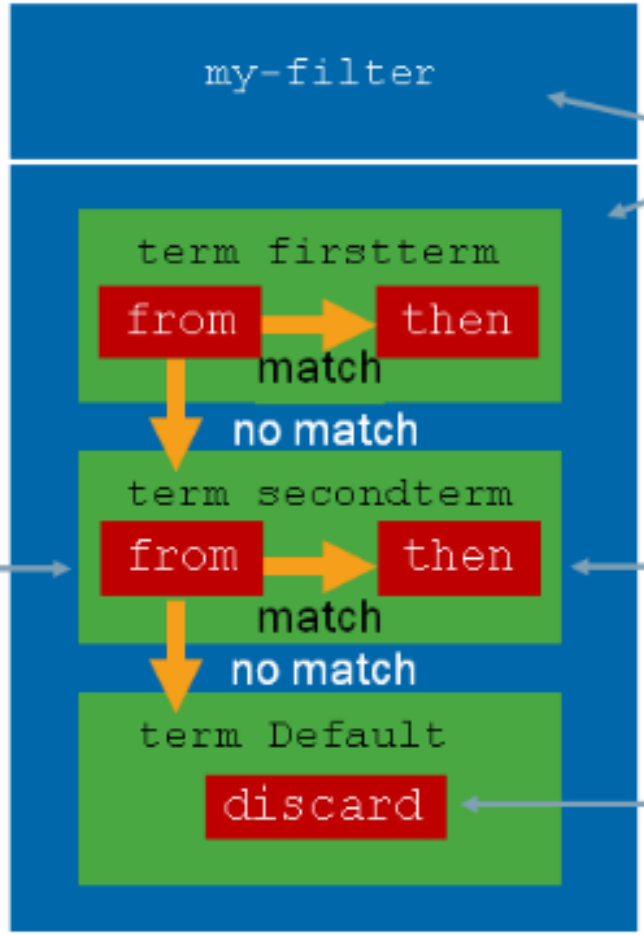
Forwarding tábla példa

```
user@router> show route forwarding-table
Routing table: inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            user     0 0:17:cb:4e:ae:81   ucst   520     3 ge-0/0/0.0
default            perm     0                    rjct    36     1
0.0.0.0/32         perm     0                    dscd    34     1
172.19.0.0/16      user     0 200.1.4.100        ucst   535     3 ge-0/0/3.0
172.19.52.0/24     user     0 200.1.2.100        ucst   529     3 ge-0/0/1.0
172.19.52.16/28    user     0 200.1.3.100        ucst   534     3 ge-0/0/2.0
```

Tűzfal-szabályok

Firewall filters consist of one or more terms; the software evaluates terms sequentially until it reaches a terminating action



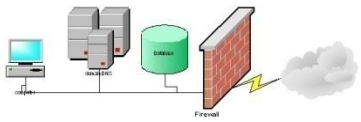
User-defined filter and term names

`from` statements describe match conditions

`then` statements describe the actions to take if a match with the `from` statement occurs

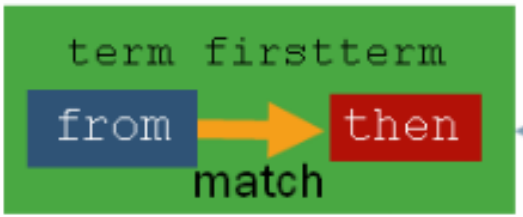
Default action for packets not explicitly allowed

Note: Ordering matters! If you must reorder terms within a filter, consider using the **`insert`** CLI command.

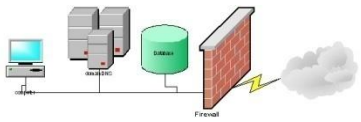


Mi történjen, ha a szabály betalál?

- Terminating actions:
  - accept
  - discard
  - reject
- Flow control:
  - next term
- Action modifiers:
  - count, log, and syslog
  - forwarding-class and loss-priority
  - policer



then statements describe the actions to take if a match with the from statement occurs

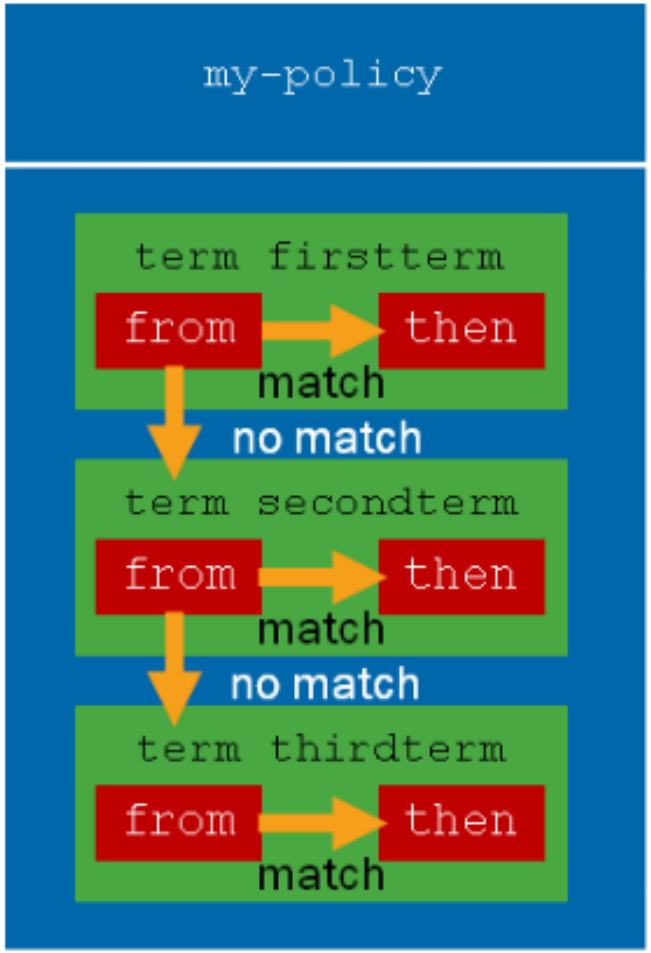


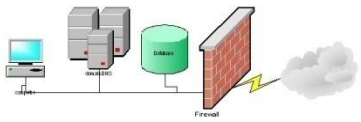
Tűzfal szűrő definíció

```
[edit firewall family inet
user@router# show
filter filter-in {
    term block-some-packets {
        from {
            source-address {
                10.10.10.0/24;
            }
        }
        then {
            count spoof-in;
            discard;
        }
    }
    term accept-others {
        then accept;
    }
}
…
```

The software applies `family inet` filters only to interfaces running IPv4

If `discard` is not present then packets are accepted





Szűrő definíció – és alkalmazás

Definition

```
filter limit-ssh-access {
    term ssh-accept {
        from {
            source-prefix-list {
                trusted;
            }
            protocol tcp;
            destination-port ssh;
        }
        then accept;
    }
    term ssh-reject {
        from {
            protocol tcp;
            destination-port ssh;
        }
        then {
            discard;
        }
    }
    term else-accept {
        then accept;
    }
}
```

Application

```
lo0 {
    unit 0 {
        family inet {
            filter {
                input limit-ssh-access;
            }
            address 10.255.71.48/32;
        }
    }
}
```

Affects incoming traffic destined to the routing engine!

Think About It

Which problems might occur if you omit the `else-accept` term?

Policing példa – rate limit

```
[edit firewall]
user@router# show
policer p1 {
    if-exceeding {
        bandwidth-limit 400k;
        burst-size-limit 100k;
    }
    then discard;
}
family inet {
    filter rate-limit-subnet {
        term match-subnet {
            from {
                source-address {
                    192.100.1.0/24;
                }
            }
            then {
                policer p1;
            }
        }
        term else-accept {
            then accept;
        }
    }
}
```

Policer defined

You must apply filter!

Policer referenced

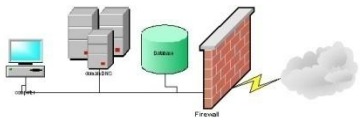
Note: Filter must account for routing and management protocols

bandwidth-limit

* In bits per second
* 30,520 bps to 4.29 Gbps

burst-size-limit

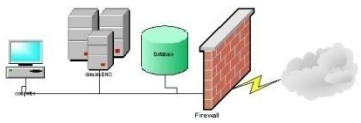
* In bytes
* Minimum should = 10 times MTU (low speed) or bandwidth times 3–5 milliseconds (high speed)



…most gyere és nézd meg mit csináltál

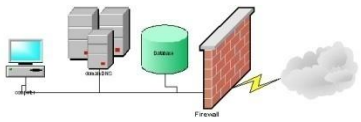
```
user@R1> show firewall log
Log :
Time      Filter    Action Interface     Protocol Src Addr                Dest Addr
07:23:16  pfe       D      ge-0/0/1.0    TCP      172.27.102.10           172.27.102.100
07:23:13  pfe       D      ge-0/0/1.0    TCP      172.27.102.10           172.27.102.100
07:23:10  pfe       D      ge-0/0/1.0    TCP      172.27.102.10           172.27.102.100
07:19:38  pfe       D      ge-0/0/3.0    ICMP     192.168.100.2           192.168.24.1
07:19:38  pfe       D      ge-0/0/3.0    ICMP     192.168.100.2           192.168.24.1
07:19:37  pfe       D      ge-0/0/3.0    ICMP     192.168.100.2           192.168.24.1
…
```

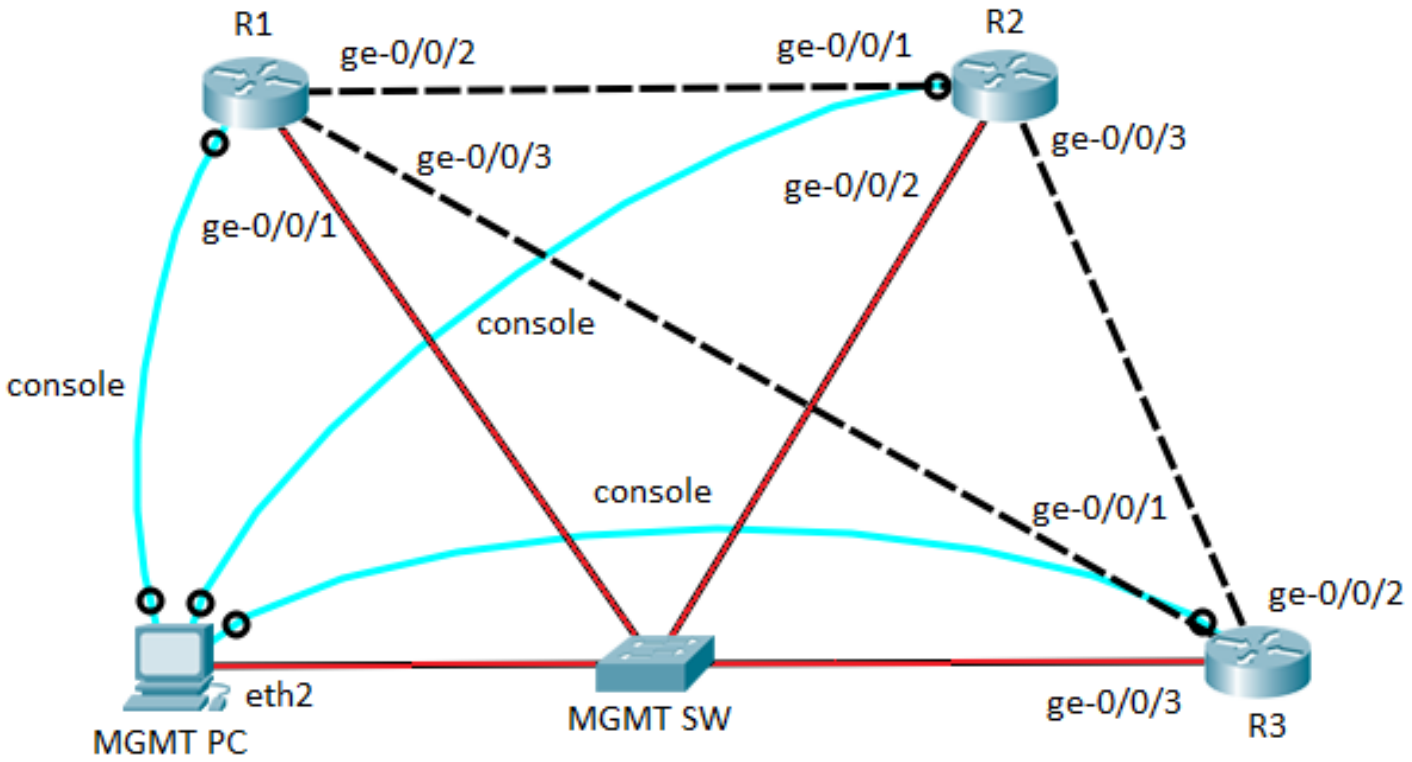
Interface on which the device received the packet



A MÉRÉS INDULÁSA

Kivonat a jegyzőkönyv-vázból



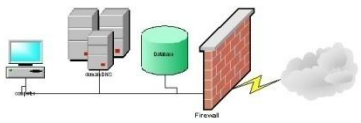


- Menedzsment PC címe: 152.66.247.11:402X
  - X-et a mérésvezető adja a mérést végző hallgatónak.
- A routerek konzol portjai:
  - R1: telnet 192.168.2.252 10211
  - R2: telnet 192.168.2.252 10212
  - R3: telnet 192.168.2.252 10213

Induló konfiguráció

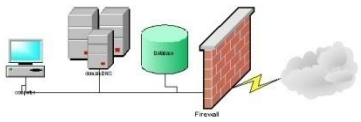
- Ha új eszköz érkezik hozzánk,
- …vagy gyári alapbeállításba került (load factory-default)

1. root jelszó beállítása
2. az eszközt egyértelműen azonosító név beállítása
3. a pontos dátum és idő beállítása
4. a megfelelő menedzsment interfészeken keresztüli hozzáférés (pl. telnet, SSH) engedélyezése
5. a megfelelő statikus útvonalakat felvétele a menedzsment-forgalom számára



Néhány tipikus mérési feladat

- Alapbeállítások
  - root jelszó, router név, menedzsment cím
- Router interfész konfiguráció, alhálózatok beállítása
- Virtuális (loopback) interfész beállítása
- Routing és Forwarding táblák ellenőrzése, vizsgálata
- Statikus routing beállítása
  - Asymmetric routing
  - Loop
  - Most Specific Route
- Tűzfalbeállítások
- Dinamikus Routing: RIP



A mérés során gyakori parancsok

cli
?
commit
rollback <n>
commit check
commit confirmed
commit confirmed time-out
show system commit
show log
show route
show route forwarding table
set interfaces
set routing-options