



M Ű E G Y E T E M 1 7 8 2

Budapesti Műszaki és Gazdaságtudományi Egyetem

Villamosmérnöki és Informatikai Kar
Távközlési és Médiainformatikai Tanszék

Juniper mérési segédlet

Felkészülés az Információs Rendszerek Üzemeltetése (IRÜ) tantárgyi mérésre

Tartalomjegyzék

1. Bevezetés	2
2. A Junos OS működése.....	3
3. Vezérlési és továbbítási síkok (Control and Forwarding planes).....	4
3.1 Áthaladó forgalom (Transit Traffic)	5
3.2 Kivételes forgalom (Exceptional Traffic)	5
4. Kezelői felületek: Webes GUI és CLI	6
4.1 A Command Line Interface (CLI)	7
4.2 Segítség kérése - (?)	8
4.3 Konfigurációs változtatások	8
4.4 Ne felejtjük el érvényesíteni a változásokat	9
5. Szintaxis	10
6. A kezdő konfiguráció lépései.....	11
6.1 A gyári alapbeállítások visszaállítása	12
7. Routing konfiguráció.....	13
7.1 A routing bejegyzések forrásai.....	13
7.2 A forwarding tábla.....	15
7.3 Konfiguráció CLI-n keresztül.....	16
8. Biztonsági beállítások.....	17
8.1 Routing vezérelv (Routing policy)	17
8.2 Biztonsági zónák.....	18
9. A mérés során használt leggyakoribb parancsok.....	19

1. Bevezetés

Ahhoz, hogy napjainkban a hálózatok és szolgáltatások világában alkotó mérnökként tudjunk tevékenykedni, szükség van egy bizonyos szintű tudásra, szakértelemre a témával kapcsolatban. A számítógép-hálózatok alapjait követően érdemes részletesebben is megismerkednünk a hálózati eszközök felépítésével, működésével, a hálózattervezés alapjaival, valamint az útvonalválasztás (routing) témakörével is. Ezt a tudást valódi eszközök működésének megismerésével tovább mélyíthetjük.

Jelen segédlet célja, hogy megismertesse a hallgatót vállalati környezetben is használatos hálózati eszközökkel (switchek, routerek, tűzfalak), valamint betekintést nyújtson alapszintű konfigurációs és hibaelhárítási lehetőségekbe is. A segédlet többnyire a Juniper Networks cég termékeit, technológiáját veszi alapul.

A Juniper Networks, Inc. fő profilja hálózati szolgáltatások és eszközök tervezése és gyártása. A céget 1996-ban alapították, székhelye a kaliforniai Sunnyvale-ben található. Világszerte közel 10.000 alkalmazottal dolgoznak és a Cisco egyik legnagyobb konkurenciájaként működnek. A laboratóriumi mérés keretében ezen gyártó eszközein oldanak meg különféle feladatokat a hallgatók.

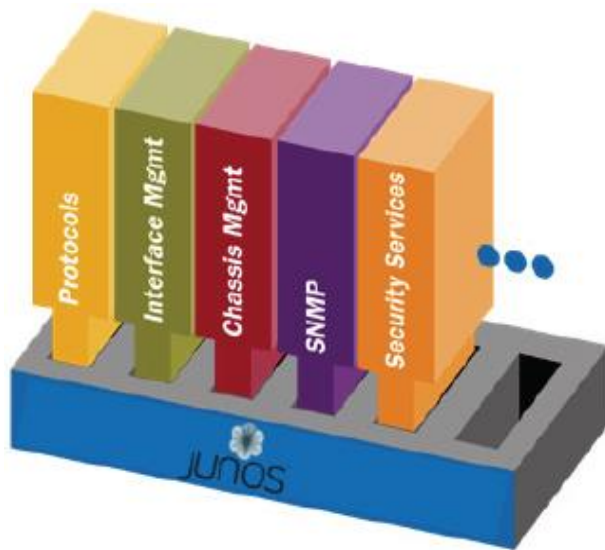


További információ a cégről az alábbi dokumentumban olvasható:

<http://www.juniper.net/assets/us/en/local/pdf/fact-sheets-backgrounder/3000054-en.pdf>

2. A Junos OS működése

A Junos OS egy FreeBSD UNIX alapokra épülő robusztus, moduláris felépítésű hálózati operációs rendszer. A cég különböző platformjain és eszközein ugyanezen rendszer különféle változatai futnak. Ez azért előnyös, mert így elég egyszer megismerkednünk a rendszerrel, a különböző termékeket hasonló módokon tudjuk konfigurálni, üzemeltetni. Számos vezérlési, beállítási és lekérdezési funkciót azonos módon érünk el más és más eszközön, ezzel is leegyszerűsítve a hálózatunk üzemeltetésével és karbantartásával járó feladatokat.

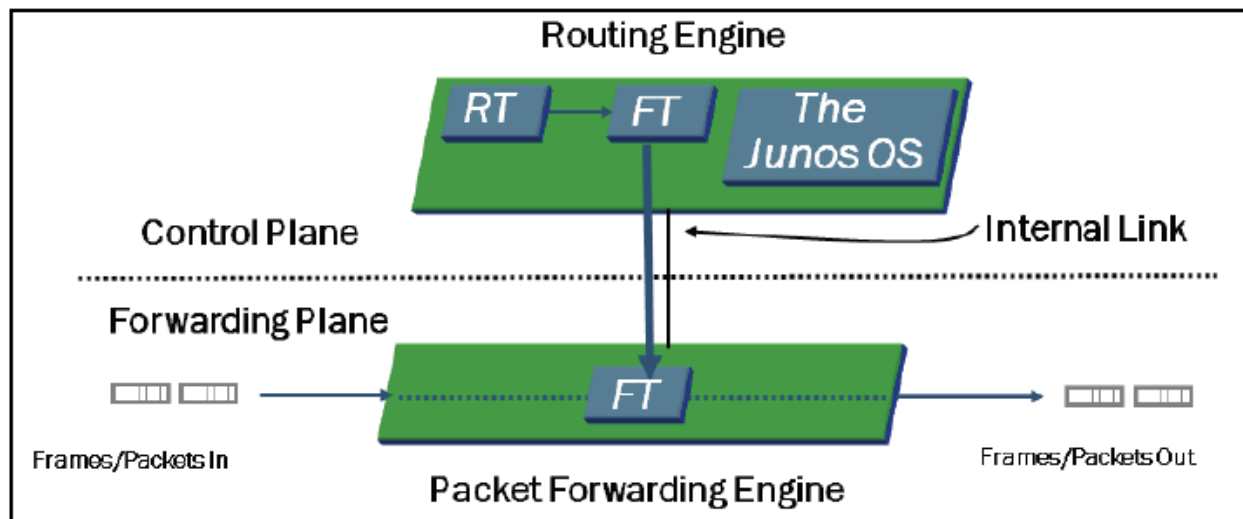


1. ábra. A Junos OS moduláris felépítése.

A Junos OS működése több folyamatra van bontva. Minden folyamat az eszköz funkcióinak egy részhalmazáért felel. A folyamatok külön-külön egy-egy védett memóriaterületen működnek, ezzel biztosítva, hogy egy folyamat ne tudjon közvetlenül hozzáférni egy másikhoz. Amennyiben egy folyamat leáll, az nem feltétlenül vonja maga után a teljes rendszer leállítását. Ennek a felépítésnek köszönhetően a rendszerhez úgy adhatók hozzá új funkciók, hogy közben az aktuális működést nem zavarjuk.

3. Vezérlési és továbbítási síkok (Control and Forwarding planes)

A Junos OS kialakításának különlegessége, a Vezérlési (Control) és a Továbbítási vagy Adat (Forwarding) síkok szétválasztása. Azok a folyamatok, amik az útvonalválasztást (routing) és a kapcsolási (switching) protokollokat vezérik, teljesen szét vannak választva azoktól a folyamatoktól, amik csomagok vagy keretek továbbításával foglalkoznak. Ez a kialakítás lehetővé teszi, hogy ezek a folyamatok a lehető leghatékonyabb és legmegbízhatóbb környezetben működjenek.



2. ábra. A vezérlési és továbbítási síkok.

A fenti ábra a Junos architektúrát mutatja be, kiemelve a Control és Forwarding síkokat. A Control sík futtatja a Routing Engine-t (RE). A Routing Engine tartja karban a különféle adatbázisokat, melyek az eszköz működéséhez elengedhetetlenek. Erre példa az útvonalválasztó tábla (Routing Table, RT) vagy a csomagtovábbító tábla (Forwarding Table FT). A vezérlési síkon történik továbbá a készülékházzal kapcsolatos adatok (hőmérséklet, hűtés, stb.) monitorozása is, valamint ez a sík látja el a csomagtovábbító (Packet Forwarding Engine, PFE) vezérlését is. A Routing Engine-en futó különböző folyamatok védett memóriaterületek alkalmazásával különülnek el egymástól. Az RE és a PFE egy belső buszon keresztül kapcsolódik egymáshoz.

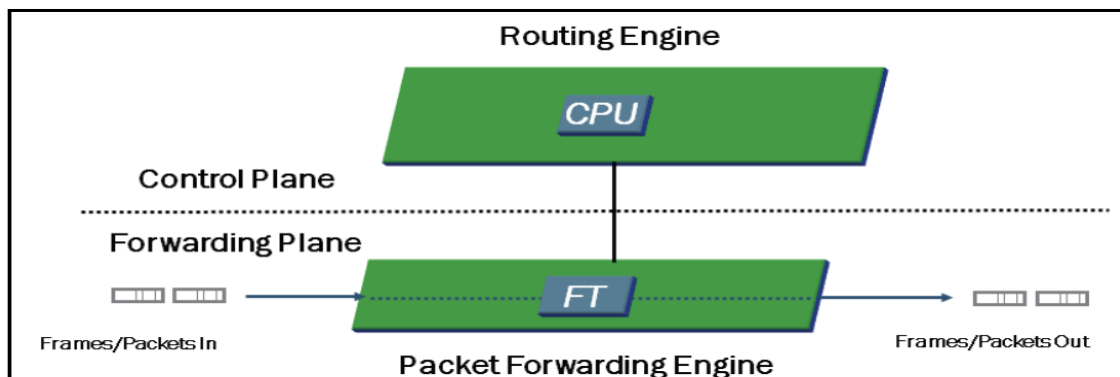
Az ábrán a Packet Forwarding Engine a szaggatott vonal alatt látható; ennek oka, hogy a PFE általában a Routing Engine-től elkülönült hardveren fut. A PFE az eszközön áthaladó csomagok továbbításáért felelős, a Forwarding Table (FT) által vezérelt módon. Azokat a csomagokat, melyeket magának az eszköznek címeztek, valamint azokat, melyekre vonatkozóan még nincs bejegyzés a FT-ben, a vezérlési síkbeli Routing Engine dolgozza fel.

Bizonyos, Junos-t használó platformok a magasabb teljesítmény érdekében speciális integrált áramköri megoldásokat használnak a PFE alkalmazás futtatására. Ezek architektúráis kialakítása különválasztja a vezérlő utasításokat (protokoll frissítések és rendszer management) a csomagtovábbító műveletektől.

Érdekesség, hogy a két sík közötti belső kapcsolat korlátozott sebességű, ezáltal elkerülhetőek az eszközt érő esetleges szolgáltatás-megtagadásos támadások (Denial of Service, DoS), ugyanis torlódás esetén a vezérlési adatok prioritást élveznek az egyéb adatforgalommal szemben.

3.1 Áthaladó forgalom (Transit Traffic)

Az összes továbbítandó csomag, ami az eszközhöz érkezik, összehasonlításra kerül a PFE-ben lévő Forwarding Table bejegyzéseivel, és az adott csomag mindig a leghosszabb, legteljesebb egyezést mutató szabály szerint továbbítódik (most specific route). Az ilyen forgalom soha nem jut el a vezérlő síkra, annak a CPU-ját nem terheli (lásd az alábbi ábrán).



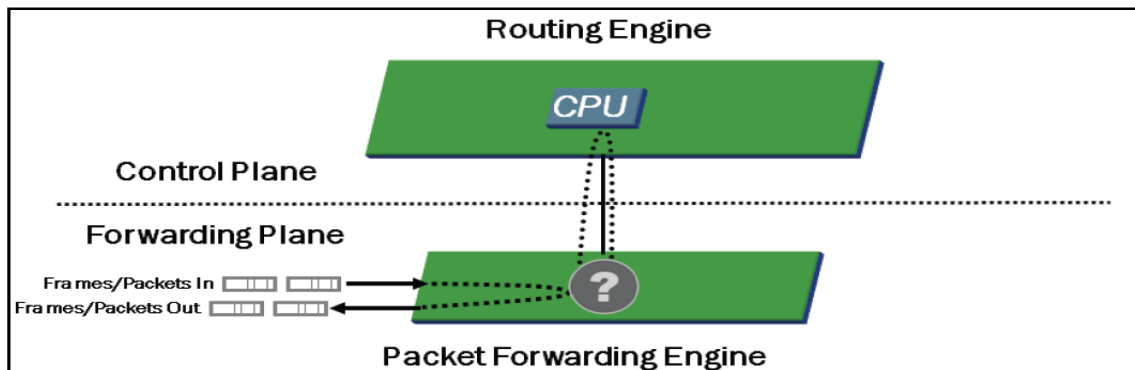
3. ábra. Az áthaladó forgalom.

3.2 Kivételes forgalom (Exceptional Traffic)

Az áthaladó forgalommal ellentétben léteznek olyan kivételek, amikor a bemenő csomagokkal nem a PFE foglalkozik, hanem egyből továbbítja a vezérlési síknak. Ilyen csomagok lehetnek:

- Routing protokoll frissítések, telnet session, ping, traceroute – illetve válaszok, amik az RE-ből kezdeményezett forgalomra érkeznek.
- IP csomagok IP beállításokkal (Az IP fejlécen belül érkező beállítások elég ritkák, de a PFE szándékosan nem is próbálja meg kezelni őket, ezeket a csomagokat az RE dolgozza fel.)
- Olyan csomagok, amelyekre válaszul ICMP üzeneteket kell generálni.

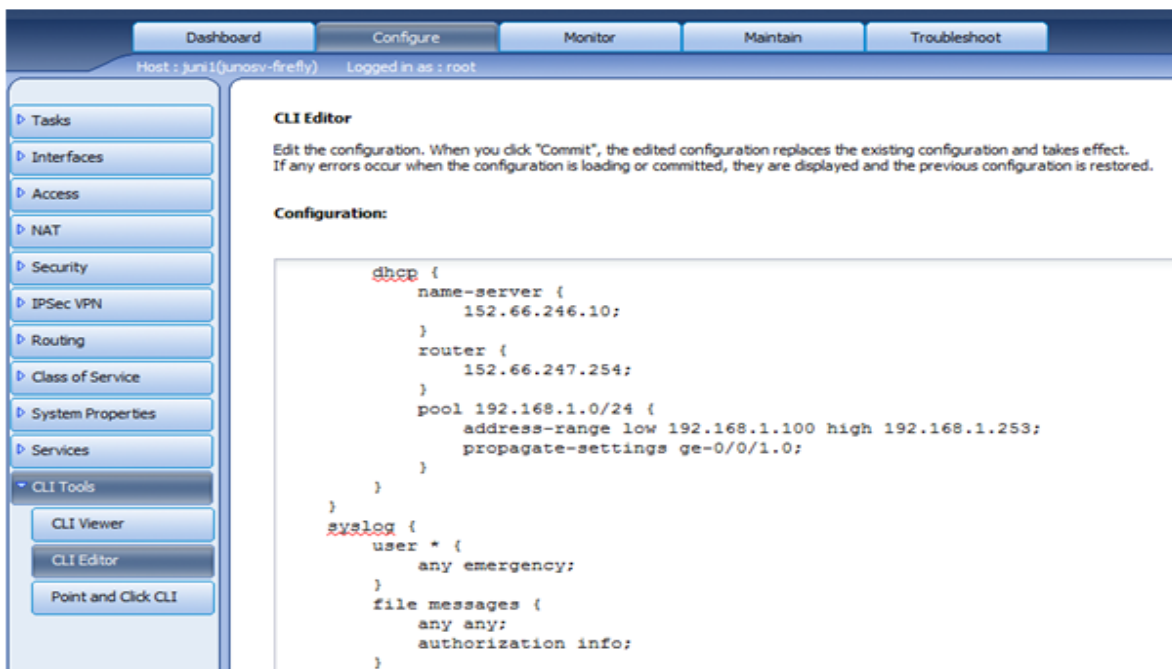
A forgalom vezérlését ilyenkor a Routing Engine CPU-ja végzi, ahogyan az alábbi ábra is mutatja.



4. ábra. A kivételes forgalom.

4. Kezelői felületek: Webes GUI és CLI

A különböző gyártók hálózati eszközei általában két fő konfigurációs módszerrel rendelkeznek. Ezek egyike a Command Line Interface (CLI), azaz a parancssoros felület, míg a másik lehetőség a webes grafikus felület használata. A J-Web GUI-n elérhető konfigurációs lehetőségek gyártónként eltérnek egymástól. A Cisco, illetve a Juniper is elsősorban a CLI használatát javasolja konfigurációs feladatok ellátására. Az alábbi képen a JunOS webes kezelői felületéről látható egy részlet. A mérés során ezzel szemben kizárólag a parancssoros vezérléssel (CLI-vel) fogunk dolgozni.



5. ábra. Részlet a J-Web grafikus kezelői felületről.

4.1 A Command Line Interface (CLI)

Célszerű a konfigurációval kapcsolatos ismerkedést a CLI-nél kezdeni, hiszen ez az a felület, melyen a hálózati eszköz minden funkciója, szolgáltatása kivétel nélkül elérhető. Sokan hónapokat, éveket foglalkoznak egy-egy gyártó parancssori felületével, míg igazán kiismerik magukat a rendszerben. Ennek a mérésnek a célja a legfontosabb ismeretek elsajátítása – ebben az útmutatóban a CLI használatához szükséges alapvető ismereteket is összefoglaljuk. A mérés során a feladatokat a CLI segítségével fogjuk megoldani.

A parancssoros kezelői felület segítségével lehetőségünk nyílik a hálózati eszközök konfigurálására, illetve a hibaelhárításra is megkapjuk a szükséges eszközöket. A CLI két móddal rendelkezik, ezek az **Operational** (működtetési) és **Configuration** (konfigurációs) módok. Operational módban az eszköz szoftverének és hardverének, valamint a hálózatnak a monitorozására – illetve az ezekkel kapcsolatos hibakeresésre van lehetőségünk. A Configuration mód ad lehetőséget a hálózati interfészek, útvonalválasztó protokollok, illetve egyéb funkciók beállítására.

Első belépéskor (mely történhet Telnet, SSH, vagy konzol portos csatlakozás segítségével) a felhasználót egy login prompt fogadja. A helyes felhasználónév/jelszó páros megadását követően automatikusan Operational módba kerülünk. Az **Operational módot a > karakter jelöli** a képernyő bal oldalán, a felhasználói adatok mellett. Erre mutat példát az alábbi CLI-ből kimásolt kódrészlet (az eszköz hosztjának neve IRUlab, a felhasználó neve pedig hallgato – a beírt jelszó biztonsági okokból nem olvasható a konzol kimenetén):

```
IRUlab (ttyd0)
login: hallgato
Password:
--- Junos 10.4R1.9 built 2010-12-08 16:25:40 UTC
hallgato@IRUlab>
```

Amennyiben a **root** jogosultságú felhasználóval jelentkezünk be, az Operational mód helyett közvetlenül **a shell-be kerülünk, melyet a % karakter szemléltet a > helyett**). Ebben az esetben a `cli` parancs kiadásával indíthatjuk el a parancssori folyamatot és léphetünk Operational módba.

Operational módból **a configure paranccsal léphetünk Configuration módba, amit a # karakter jelöl**.

4.2 Segítség kérése - (?)

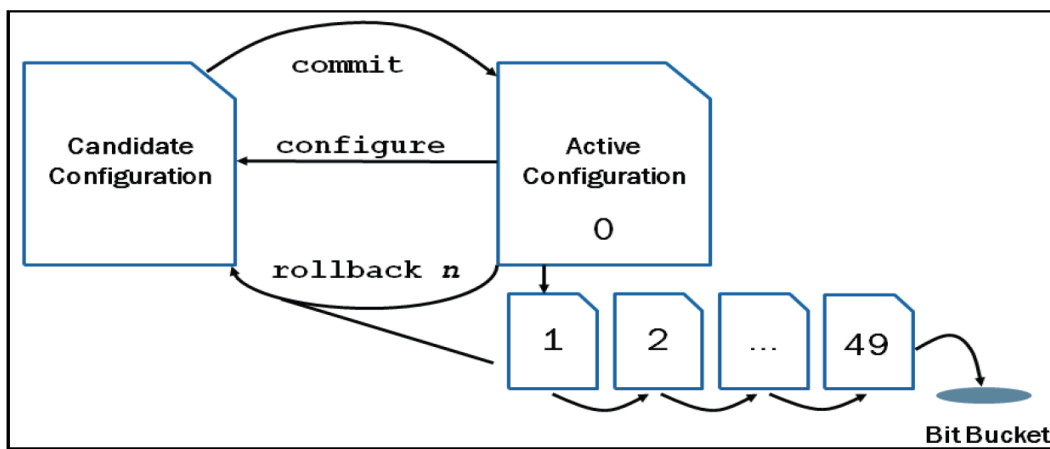
A CLI a könnyebb felhasználhatóság érdekében környezetfüggő (context-sensitive) segítséget nyújt, bárhol járunk is a command line-ban. Elmondja, milyen használható beállítási lehetőségeink vannak az adott ponton és részletes leírással is segíti az utasítás további opcióinak megértését. Ha bárhol elakadunk, vagy nem tudjuk, hogy az adott parancs után milyen elérhető lehetőségeink vannak, csak gépeljük be egy kérdőjelet (?). Az entert nem kell lenyomni, mert amint begépelésre kerül a kérdőjel az operációs rendszer rögtön kilistázza az elérhető felhasználói beállításokat vagy lehetséges további opciókat. A listázás után rögtön visszakerülünk a command line-ban arra a pontra, ahol beírtuk a kérdőjelet.

4.3 Konfigurációs változtatások

A konfigurációs változtatások a Junos OS-en belül nem lépnek rögtön érvénybe. Ezzel lehetőségünk van arra, hogy csoportosítsuk a konfigurációs beállításokat, mielőtt hozzáadnánk azokat egy már futó konfigurációhoz.

A konfigurációk típusai:

- Aktív konfiguráció (Active Configuration): Az éppen rendszeren futó konfiguráció. Ezt tölti be a rendszer egy adott bootoláskor.
- Jelölt konfiguráció (Candidate Configuration): Egy átmeneti konfiguráció, amiből aktív konfiguráció is lehet. Amikor egy futó eszközön változtatjuk a konfigurációs beállításokat, akkor a rendszer létrehoz egy jelölt konfigurációt, amin tudunk dolgozni. Utána lehetőségünk van arra, hogy ezt megtegyük aktívnak úgy, hogy az összes változtatásunkat élesítjük (**commit**) az eszközön. Ekkor válik a jelölt konfiguráció aktívvá. Ezt mutatja be az alábbi ábra.



6. ábra. A konfigurációk típusai.

Amikor az eszközön a konfigurációs módba lépünk (a `configure` parancs kiadásával), a rendszer létrehoz egy jelölt konfigurációt, amit az éppen aktív konfiguráció beállításával tölt fel.

Ahhoz, hogy a jelölt konfigurációnak legyen bármi hatása, `commit`olnunk kell. Egy `commit` után a Junos OS ellenőrzi, hogy szintaktikailag helyes-e az a konfiguráció, amit éppen élesnek szeretnénk megtenni. Ha bármi hibát talál, akkor egy hibaüzenetet dob, és a jelölt konfiguráció egyik része sem aktiválódik. Ahhoz, hogy valóban élesítsük, ki kell javítani a hibaüzenetben jelzett problémákat.

Könnyen vissza tudunk térni egy korábbi, már működő konfigurációkhoz a `rollback n` paranccsal (ahol `n` az a szám, ahova szeretnénk rollbackelni [0-49]). A Junos OS az előző 50 aktív konfigurációt tárolja, amiknek a sorszama minden `commit` esetén 1-gyel növekszik (lásd 6. ábra). Ebben az 50-ben az éppen aktív konfiguráció is benne van a 0. indexen. Miután `rollback`-eltünk, a rendszer betölti az adott konfigurációs fájlt, és utána ugyanúgy `commit`-olni kell, különben nem lesz változás a rendszeren futó aktív konfigurációban.

4.4 Ne felejtsük el érvényesíteni a változásokat

Az élesztésnek (`commit`) rettentő fontos szerepe van a konfigurálás során. A továbbiakban áttekintjük azokat az élesztési opciókat, amiket a labor alatt használnunk kell majd, illetve amiről hasznos, ha minden hallgató tud.

- `commit check`: ellenőrizni tudjuk vele a jelölt konfiguráció szintaktikáját, anélkül, hogy ténylegesen megpróbálnánk aktiválni.

```
[edit]
user@router# commit check
[edit interfaces ge-0/0/10 unit 0]
  'family'
    When ethernet-switching family is configured on an interface, no
    other family type can be configured on the same interface.
error: configuration check-out failed
```

- `commit confirmed`: Természetesen a `commit check` nem tudja ellenőrizni a konfigurációban lévő logikai problémákat. Mi történik akkor, ha egy eszközt távolról konfigurálunk, és egy logikai hiba (pl. hibás gateway IP cím beírása) miatt kizárnánk magunkat az eszköz távoli kapcsolatától? Az ilyen esetek kezelésére jó a `commit confirmed time-out` parancs, ami elindít egy időzítőt, miközben egy `commit` parancsot vár. Ha a `time-out` idő alatt nem érkezik `commit` parancs, a rendszer végrehajt egy `rollback 1, commit`

parancssort, ami a commit előtti aktív konfigurációt hozza vissza. Természetesen az addigi változtatások nem vesznek el, mivel el lehet érni a logikailag rossz konfigurációt is az automatikus rollback után a `rollback 1` paranccsal.

```
[edit]
user@router# commit confirmed
commit confirmed will be automatically rolled back in 10 minutes unless
confirmed
commit complete
```

- `commit comment`: Naplóbejegyzést ad hozzá a commit-hoz, a `commit comment "comment-string"` paranccsal. Ezeket a naplókat a `show system commit` paranccsal lehet elérni később.

```
[edit]
user@router# commit comment "Changed OSPF
configuration"
commit complete

user@router> show system commit
0 2010-05-11 15:32:42 UTC by user via cli
    Changed OSPF configuration
```

5. Szintaxis

A CLI parancsok felépítése hierarchikus. Tekintsük az alábbi példát:

```
hallgato@IRUlab# set system host-name IRUlab
                (1)   (2)   (3)   (4)
```

- (1) : parancs típusa: `set` -> felülírunk valamilyen értéket
- (2) : parancs pontosítása: `system` -> rendszerbeállításról van szó
- (3) : `host-name` nevű rendszerparamétert akarjuk módosítani
- (4) : módosítás értékét adjuk meg

Miután megismertük a parancsokat, azokat nem kell minden alkalommal teljesen beírunk. Ha a begépelés közben lenyomjuk a **szóköz** billentyűt, a CLI befejezi helyettünk a parancsot. Pl. a `show` parancs beírásánál:

```
hallgato@IRUlab> sh<szóköz>ow ipv6
```

A **Tab** billentyűvel hasonlóan kiegészíthetjük a parancsokat, továbbá az általunk definiált változók neveit is kiegészíti így a rendszer. Ilyen változó lehet pl.: szabályok nevei, IP címek.

```
hallgato@IRUlab> show policy-statement lab<tab>or-policy
```

Ha egy parancs paramétereiben nem vagyunk biztosak, a ? beírásával a rendszer megmutatja a lehetséges opciókat.

```
hallgato@IRUlab> clear ?  
Possible completions:  
amt  
arp  
auto-configuration  
...
```

A begépett konfigurációs utasítások aktiválásához be kell írunk a `commit` parancsot. Ezután a rendszer elmenti a módosításokat. A változtatások teszteléséhez nem kell elhagynunk a konfigurációs módot, **a `run` parancs segítségével operational módbeli parancsot is futtathatunk konfigurációs módban.**

```
[edit interfaces ge-0/0/12]  
user@router# set unit 0 family inet address 10.250.0.141/16  
  
[edit interfaces ge-0/0/12]  
user@router# commit  
commit complete  
  
[edit interfaces ge-0/0/12]  
user@router# run ping 10.250.0.149 count 1  
PING 10.250.0.149 (10.250.0.149): 56 data bytes  
64 bytes from 10.250.0.149: icmp_seq=0 ttl=255 time=0.967  
ms  
  
--- 10.250.0.149 ping statistics ---  
1 packets transmitted, 1 packets received, 0% packet loss  
round-trip min/avg/max/stddev = 0.967/0.967/0.967/0.000 ms
```

Use `run` to test configuration changes without leaving configuration mode

A prompt felett található szögletes zárójelben láthatjuk a CLI hierarchiában az aktuális pozíciókat. A fenti példában az `[edit interfaces ge-0/0/12]` azt jelenti, hogy a `ge-0/0/12`-es interfészre vonatkozó beállításokat végzünk.

6. A kezdő konfiguráció lépései

A Junos első indulásakor – tehát például amikor megérkezik hozzánk a megvásárolt eszköz – szükség van néhány alapvető konfigurációs feladat elvégzésére. (Az első indítást követő állapotot elérhetjük a gyári beállítások visszaállításával.)

- Első feladatunk egy root jelszó beállítása, mely azt biztosítja, hogy illetéktelenek ne tudják módosítani eszközünk beállításait.

- Célszerű beállítani egy, az eszközt egyértelműen azonosító nevet, a pontos dátumot és időt.
- Engedélyezni kell a megfelelő menedzsment interfészekon keresztüli hozzáférést (pl. Telnet, SSH).
- Fontos, hogy a menedzsment-forgalom számára felvegyük a megfelelő statikus útvonalakat is.

Ezen feladatokat a mérés során is el fogjuk végezni.

6.1 A gyári alapbeállítások visszaállítása

A Junos OS-t használó eszközök első üzembe helyezésükkor már tartalmaznak egy alapértelmezett, gyári konfigurációs fájlt. Ennek betöltésével érdemes kezdeni a beállítást. Ha az eszköz használata során átláthatatlanná válna a konfiguráció, a gyári alapbeállítások visszaállításával bármikor visszatérhetünk egy biztos kiindulási alaphoz.

A gyári konfiguráció paraméterei nem azonosak minden eszköz esetén, különböző funkcionalitású berendezéseknél eltérőek lehetnek.

CLI-t használva két lehetőségünk van, hogy visszaállítsuk alapállapotba az eszközt. Ezen parancsok eltérő módon viselkednek:

- **request system zeroize**

Törli az összes naplófájlt, adatot, és visszatölti az eszköz gyári konfigurációját. Újraindulást követően nem kér jelszót. Az elejéről kell kezdeni az eszköz teljes beállítását.

- **load factory-default**

A parancs csak a beállításokat törli, és visszatölti az alap konfigurációt. Az utasítás commitolása (véglegesítés) előtt meg kell adni az újraindulás után használni kívánt root jelszót.

A beállítás megkezdéséhez a gyári konfiguráció engedélyezi a felhasználónak a root (rendszergazdai) hozzáférést. Alapértelmezetten a root fiókhoz nem tartozik jelszó, de mielőtt módosítanánk a rendszer beállításokat, meg kell adnunk egyet. A jelszavak választásánál vegyük figyelembe, hogy a jelszónak legalább hat karakter hosszúnak kell lennie, és tartalmaznia kell írásjelet vagy számot is.

A rendszer alapértelmezetten naplófájlokat készít az eseményről és az elvégzett műveletekről. Később könnyen lekérdezhajük ezen fájlok tartalmát a `show log` paranccsal; így az esetleges hibák okát is felfedhetjük.

7. Routing konfiguráció

Amint elhagyjuk a helyi hálózatot (LAN-t), valamilyen módon meg kell határoznunk, hogy a célhálózat milyen úton érhető el. Ezt a célt szolgálja a hálózati útvonalválasztás (routing). A routing logikai címekkel dolgozik (IP cím), az OSI-modell 3. rétegében, TCP/IP-modell szerinti Internet rétegben.

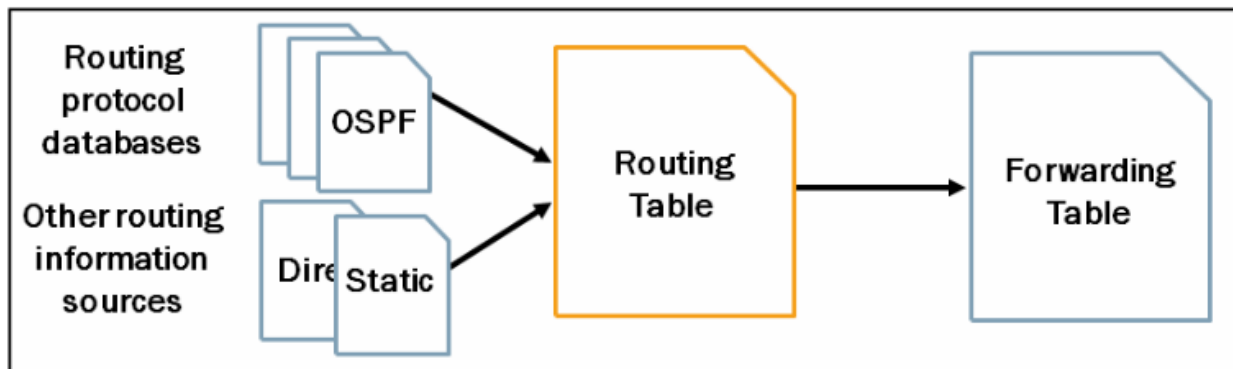
A routingnak két fajtája létezik: statikus és dinamikus. Statikus routing esetén az útvonalat a hálózat adminisztrátora kézzel állítja be, míg dinamikusnál egy routing protokoll választja ki a megfelelő útvonalakat. Ilyen dinamikus routing protokoll például a RIP (Routing Information Protocol), illetve az OSPF (Open Shortest Path First). A RIP egy távolság (distance vector) alapú protokoll, ami mértékegységként hop-count-ot használ, azaz azt figyeli, hogy hány köztes router található az aktuális router és a célállomás közt.

Routing konfigurálásához elkerülhetetlen az alhálózatokra bontás (subnetting) folyamatának ismerete. Korábbi tanulmányok során más tárgykból volt róla szó, ezért most nem térünk ki rá részletesen. Ezzel a témával kapcsolatos esetleges hiányosságok többek között innen pótolhatók:

<https://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-interfaces-and-routing/ipv4-addressing.html#ipv4-addressing-section>

7.1 A routing bejegyzések forrásai

A routing bejegyzéseknek több forrása is lehet. Az információk érkezhettek különböző routing protokollok felől (például RIP, OSPF), de beállíthatók statikusan is, illetve közvetlen kapcsolatból is adódhatnak. Ezek a bejegyzések bekerülnek a routing táblába. A router minden hálózat felé kiválaszt egy aktív útvonalat, ami bekerül a forwarding táblába. A különböző csomagok továbbítása a forwarding táblában lévő bejegyzések alapján történik.




7. ábra. A routing és a forwarding tábla forrásai.

Junos OS-t futtató eszközök több routing táblát is tartalmaznak. Az egyik ilyen tábla az inet.0, ami az IPv4 unicast routing bejegyzéseket tartalmazza. Opcionálisan létrehozhatóak újabb táblák. Az előre definiált routing táblák a következők:

- `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.

Ha egy hálózat felé több forrásból érkező routing információ is rendelkezésre áll, akkor a Junos OS az útvonal-preferencia értékek alapján választ aktív útvonalat. Az alapértelmezett preferencia értékek különböző források esetén az alábbi táblázatban láthatók. Az értékek változtathatók, ha egy adott forrásból érkező routing információt szeretnénk előnyben részesíteni. Ez alól kivétel a **direct** és a **local routing** információ, amik mindig előnyt élveznek más bejegyzésekkel szemben. Bizonyos gyártók az útvonal-preferencia értékek (route preference values) helyett az adminisztratív távolság (administrative distance) elnevezést használják.

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



8. ábra. Az alapértelmezett útvonal-preferencia értékek.

Alább egy `show route` parancs eredménye látható.

- Az `inet.0` jelöli az IPv4 unicast route-ok tábláját,
- a különböző célhálózatokhoz tartozó bejegyzések forrása és preferencia értéke a szögletes zárójelben található,

- a bejegyzés előtt lévő csillag (*) aktív útvonalat jelöl, ami a forwarding táblába is bekerül.

A példában a 10.1.1.0/24-es hálózat felé egy statikus és egy OSPF által szolgáltatott útvonal is megtalálható, amik közül a router az előbb ismertetett preferenciaértékek alapján a statikus útvonalat választja aktívnak.

```

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

...

```

7.2 A forwarding tábla

A forwarding táblában található az aktív útvonalak és a továbbításhoz használt információk, mint például a célállomásokhoz tartozó kimeneti interfész és a next-hop IP/MAC-cím. Alább egy forwarding tábla látható.

```

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

```

Az első két oszlop a célállomást és annak típusát jelöli.

A táblában látható még a next-hop (a cél felé vezető következő interfész címe) és annak típusa, az utolsó oszlopban pedig a bejegyzéshez tartozó kimeneti interfész.

A célállomás típusai közül a `user` statikus route-ot, vagy routing protokolltól származó bejegyzést jelent, míg a Junos kernel által hozzáadott bejegyzést a `perm` típus jelöli. Az egyik ilyen bejegyzés a `default`, ahol a next hop típusa `rjct` (reject). Amelyik csomag csak ennek a bejegyzésnek felel meg, azt a router egy ICMP Unreachable üzenet generálása mellett eldobja. A `dscd` (discard) típus ICMP üzenet nélküli eldobást jelent, míg az `ucst` a unicast bejegyzést.

A router egy beérkező csomag esetén (amennyiben nem az adott router a címzett) összeveti a cél címét a forwarding táblában található bejegyzésekkel, és annak megfelelően továbbítja, vagy eldobja azt. Ha több hálózati cím (prefix) is megfelel a célállomásnak, akkor a router mindig a legpontosabb bejegyzés (most specific entry) szabályának megfelelő irányba küldi a csomagot.

Vegyük például a fent látható forwarding táblát:

- Egy 172.19.52.101-es cél IP címmel rendelkező csomag esetén megfelelő célállomás a 172.19.0.0/16-os prefix is, de a legpontosabb bejegyzést a 172.19.52.0/24-es hálózat adja, így a kimeneti interfész a ge-0/0/1.0.
- 172.19.52.21-es cél IP esetén már a 172.19.52.16/28-as hálózat is megfelelő, ez adja a leghosszabb egyezést. A csomag a ge-0/0/2.0 interfészen lesz továbbítva.
- Ha a cél IP cím 172.25.100.27, akkor nem felel meg egyik prefix sem, így a csomag a felhasználó által definiált alapértelmezett (default) útvonalon továbbítódik, azaz a kimeneti interfész a ge-0/0/0.0 lesz.

7.3 Konfiguráció CLI-n keresztül

A routing beállítása CLI-n keresztül Configuration módban végezhető.

A statikus routing az `[edit routing-options static]` hierarchia szinten módosítható. Routing bejegyzés a `set` paranccsal adható hozzá a routing táblához, ahol meg kell adni a célhálózatot, illetve a next-hop címet.

Tegyük fel, hogy a 10.10.2.0/24-es alhálózat elérhető a 192.168.10.2-es közvetlenül kapcsolódó interfészen. Ezt a bejegyzést a `set routing-options static route 10.10.2.0/24 next-hop 192.168.10.2` paranccsal adhatjuk hozzá a routing táblához.

A routing megfelelő működéséhez elengedhetetlen az interfészek helyes konfigurációja. Ez ugyancsak a `set` paranccsal végezhető, az `[edit interfaces]` hierarchia

szinten. Meg kell adni a beállítani kívánt interfész nevét (1), a protokollcsaládot (2), az interfész IP címét és az alhálózati maszkot (3).

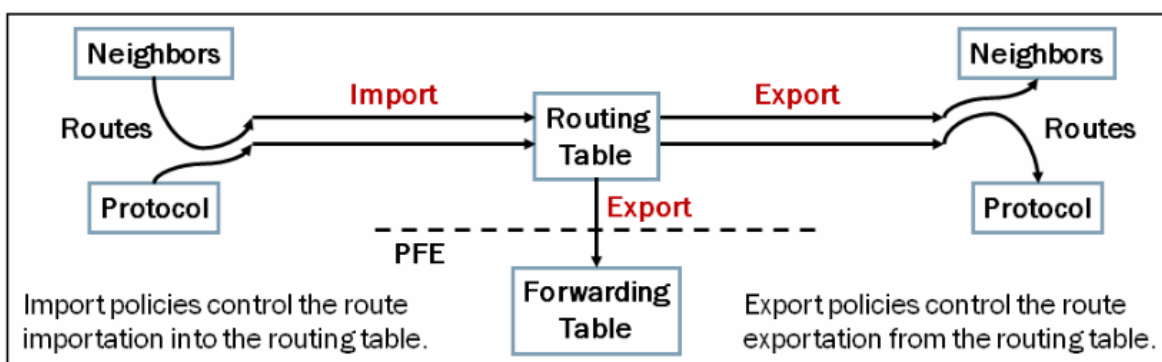
```
(1)          (2)          (3)
set interfaces ge-0/0/2 unit 0 family inet address 192.168.10.1/30
```

8. Biztonsági beállítások

Az eszközök konfigurációjának szerves részét képezik a biztonsági beállítások is. Ezeknek a segítségével garantálható a routing információk biztonsága, és megakadályozható az illetéktelen hozzáférés. Egyes beállítások védelmet nyújtanak különböző hálózati támadások ellen is.

8.1 Routing vezérelv (Routing policy)

A routing vezérelvek beállításával szabályozható a routing táblába bekerülő, illetve az onnan továbbított routing információk áramlása. Ennek egy áttekintése látható a következő ábrán.



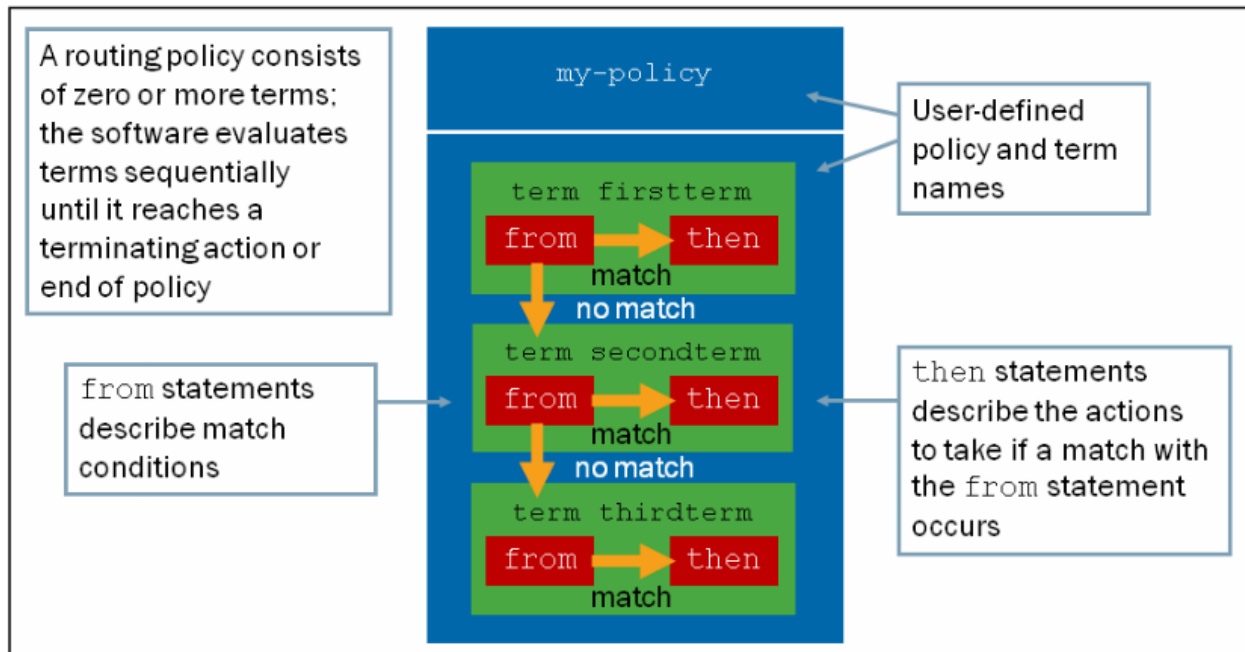
9. ábra. A routing vezérelvek áttekintése.

Az import vezérelvek a routing táblába bekerülő, az export vezérelvek az onnan kikerülő routing információkat szabályozzák. Minden routing protokoll rendelkezik egy alapértelmezett routing vezérelvvel.

RIP protokoll esetén az alapértelmezett import vezérelv az, hogy a router a beállított RIP szomszédoktól minden RIP útvonalat elfogad, és eltárolja azt az inet.0 routing táblába. Export esetén azonban a beállított RIP szomszédoknak sem küld útvonalakat. Így ha útvonalat szeretnénk hirdetni a szomszédos routereknek, akkor létre kell hozni egy export routing vezérelvet, ami ezt engedélyezi.

Ahogy a következő ábrán is látható, a vezérelveket egymást követő kifejezések (term) alkotják. A kifejezésekben megadható egy feltétel, aminek a teljesülése esetén

különböző műveletek végezhető. A művelet többek között lehet elfogadás (accept) és elutasítás (reject) is.



10. ábra. A routing vezérelvek felépítése.

RIP protokoll esetén egy routing export vezérelv lehet a következő:

```

policy-statement advertise-routes-through-rip {
  term match-rip-routes {
    from protocol [ rip ];
    then accept; }
}

```

Ez a vezérelv a RIP protokoll által létrehozott útvonalak exportját engedélyezi.

8.2 Biztonsági zónák

A biztonsági zónák logikai egységek, amelyekhez egy vagy több interfész tartozhat. Ezeknek a segítségével szabályozható, hogy az adott interfészeken milyen típusú forgalom haladhat bejövő, illetve kimenő irányban.

Juniper eszközök esetén alapértelmezetten két biztonsági zóna van létrehozva, az egyik a megbízható (trust), a másik a nem megbízható (untrust) zóna. A megbízható zónába gyárilag kizárólag a menedzsment interfész tartozik. Ezen engedélyezve van a http, https, ssh, telnet és dhcp forgalom, de semmi más.

A forgalom szabályozása a zónák között meghirdetett biztonsági vezérelvekkel történik, amik a korábban ismertetett routing vezérelvekhez hasonlóak. A gyári konfiguráció engedélyezi a megbízható zónában található interfészekről származó forgalmat, de tiltja azt a forgalmat, ami a nem megbízható zónában található interfésztől származik.

Ahhoz, hogy az eszköz bármilyen neki címzett forgalomra válaszoljon, a fogadó interfészt a megbízható zónába kell helyezni, és a kívánt alkalmazást (például ping, traceroute) engedélyezni kell. Ez Configuration módban az `[edit security zones security-zone trust interfaces]` hierarchia szinten végezhető.

9. A mérés során használt leggyakoribb parancsok

<code>?</code>	Környezetfüggő segítségkérés az adott hierarchia szinten
<code>% cli</code>	A parancssoros interfész indítása shellből
<code>> show route</code>	A routing tábla megjelenítése
<code>> show route forwarding table</code>	A forwarding tábla megjelenítése
<code>> show interfaces</code>	Interfész beállítások megjelenítése
<code>> show configuration</code>	Az aktív konfiguráció megjelenítése
<code>> show configuration interfaces</code>	Az aktív konfiguráció interfész beállításainak megjelenítése
<code>> configure</code>	Belépés Configuration módba
<code># run</code>	Operational módbeli parancs futtatása
<code># commit</code>	A jelölt konfiguráció aktíválása
<code># rollback <u>n</u></code>	Egy korábbi aktív konfiguráció visszaállítása
<code># commit check</code>	Konfigurációs változtatások szintaktikai ellenőrzése
<code># commit confirmed <u>time-out</u></code>	Automatikus rollback <u>time-out</u> időn belül
<code># commit comment</code>	Megjegyzés fűzése a változtatásokhoz
<code># set</code>	Konfiguráció beállítása
<code># delete</code>	Konfigurációs bejegyzés törlése
<code># rename ... to ...</code>	Meglévő konfiguráció módosítása
<code># set interfaces</code>	Interfész konfiguráció beállítása
<code># set routing-options static</code>	Statikus routing beállítása
<code># set security zones</code>	A biztonsági zónák beállítása
<code># set protocols</code>	Dinamikus routing protokollok beállítása
<code># set policy-options</code>	Vezérelvek beállítása
<code># show compare</code>	Az aktív és a jelölt konfiguráció összehasonlítása