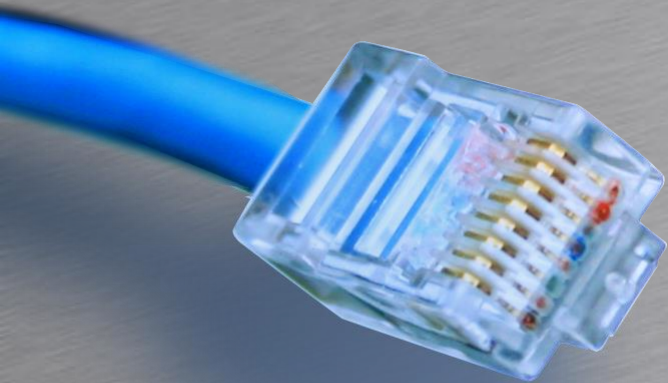


General setup



- en del af **mercantec**⁺

Udvidet konfiguration

Rasmus Elmholt V1.0



Bruger håndtering

- Lokal bruger database
 - Navne og password
 - Password krav:
 - Min. 6 karakter
 - Min. 2 forskellige karakter klasser
 - Hver konto har sin egen hjemmefolder
- Radius og TACACS+
 - Central håndtering af brugere og rettigheder



Bruger håndtering

- Database prioritering
 - Prøver indtil ACCEPT

```
# show show system authentication-order  
Authentication-order [ radius tacplus password ]
```

- Bruger altid local databasen hvis serverne ikke svarer

```
# show show system authentication-order  
Authentication-order [ radius tacplus ]
```



Bruger håndtering

- CLI aktivitet bliver enten tilladt eller afvist baseret på brugerens rettigheder
 - Brugere
 - Tilhører altid kun en enkelt klasse
 - Klasser
 - Bestemmer rettigheder og overrides
 - Der findes 4 forud definerede klasser:
 - Super-User: Alle rettigheder. Også til at oprette brugere
 - Operator: Rydde counters, og genstarte services.
 - Read-only: Kan kun lave show kommandoer
 - Unauthorized: Har ingen rettigheder.

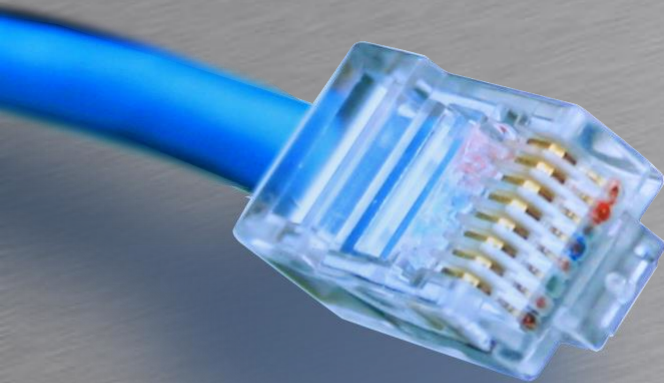


Bruger håndtering

- Lokale brugere

```
[edit system login]
rael@SRX240# show
class Custom-User {
    permissions [ clear configure network reset view ];
    deny-commands "(file)";
    allow-configuration "(protcol) |(interfaces)";
}
user rael {
    full-name "Rasmus Elmholt";
    uid 2002;
    class Custom-User;
    authentication {
        encrypted-password "$1$F5hF7XvX$GS1LJb7pngskYzbMJxdvV."; ## SECRET-DATA
    }
}
```

System Logging



HOUSE OF
TECHNOLOGY

A row of ten colorful circles in various colors and patterns, including solid colors and concentric circles.

- en del af **mercantec⁺**

Kontrol af logging



System logging

- Log system som man kender det fra *nix systemer
 - /var/log/
- Der kan laves separate logs for stort set alt
 - Definerer hvad der skal logges og hvortil
 - Samme severity levels som vi kender fra andre producenter
- Lokal eller fjernlogging med div protkoller



System logging

```
[edit system syslog]
rael@SRX240# show
user * {
    any emergency;
}
host 10.0.0.1 {
    any any;
}
file messages {
    any any;
    authorization info;
}
file interactive-commands {
    interactive-commands any;
}
file config-changes {
    change-log info;
}
```




System logging

- Brug `help syslog`

```
rael@SRX240# help syslog
```

Syslog tag	Help
ACCT_ACCOUNTING_FERROR	Error occurred during file processing
ACCT_ACCOUNTING_FOPEN_ERROR	Open operation failed on file
ACCT_ACCOUNTING_SMALL_FILE_SIZE	Maximum file size is smaller than record size
ACCT_FORK_ERR	Could not create child process

```
rael@SRX240# help syslog UI_COMMIT_PROGRESS
```

Name: UI_COMMIT_PROGRESS

Message: Commit operation in progress: <message>

Help: mgd recorded step in commit operation

Description: As it performed a commit operation, the management process (mgd) recorded its execution of the indicated step.

Type: Event: This message reports an event, not an error

Severity: info

Prøv det



Traceoptions

- Andre producenter kalder det debug!!
 - Bruges for at debugge på noget bestemt

```
[edit protocols ospf traceoptions]
rael@SRX240# show
file ospf-debug size 512k files 10 world-readable;
flag event detail;
flag hello detail;
```

- Se log filen med `show log ospf-debug`
- Debug med `monitor start ospf-debug`
- Nulstil loggen med `clear log ospf-debug`
- Slet loggen med `delete file /var/log/ospf-debug`

Denne kommando må i aldrig bruge



Tidens tand

- NTP tids synkronisering
 - Vigtig når man analyserer log filer
 - JunOS kan både virke som klient og server
 - Support for MD5 authentication

```
[edit system ntp]  
rael@SRX240# show  
boot-server 10.1.4.1;  
server 10.1.4.1;
```

- **Kontroller med** `show ntp associations`
- `Show system uptime`



Konfig arkiv

- Under `edit system archival` kan routeren sættes op til at tage backup af konfigurationen
 - Kan tage backup på bestemte tidspunkter
 - Kan tage backup ved `commit`
 - Ved flere sites bruges backup site kun hvis første fejler

```
[edit system archival]
root@CPE2# show
configuration {
    transfer-on-commit;
    archive-sites {
        "ftp://user@nms:/archive" password "$9$gJ4JD.mTFnCjHfzFnp"; ## SECRET-DATA
    }
}
```



Konfig arkiv

- Fejlsøgning via `/var/log/messages`

```
rael@SRX240> show log messages | match transfer
```

- Konfig filer i kø bliver gemt i `/var/transfer/config`
 - Filen bliver kopieret til `/var/transfer/config`
 - Når filen er overført eller en fejl er opstået kommer der en log i messages.

```
rael@SRX240> file list /var/transfer/config detail
```

```
/var/transfer/config/:
```

```
total 12
```

```
-rw-r----- 1 root wheel          498 Nov 8  01:52 CPE2_juniper.conf.gz_20111108_015216
```



SNMP

- SNMP protokollen bruges til at hente information fra udstyret
 - Kan hente information(get/getbulk)
 - Kan ændre information(set)
 - Kan sende traps

```
[edit snmp]
rael@SRX240# show
description "SRX240 Firewall";
location "Mercatenc Room 309";
contact "RaEl 112";
community public {
    authorization read-only;
    clients {
        192.168.146.0/24;
    }
}
```

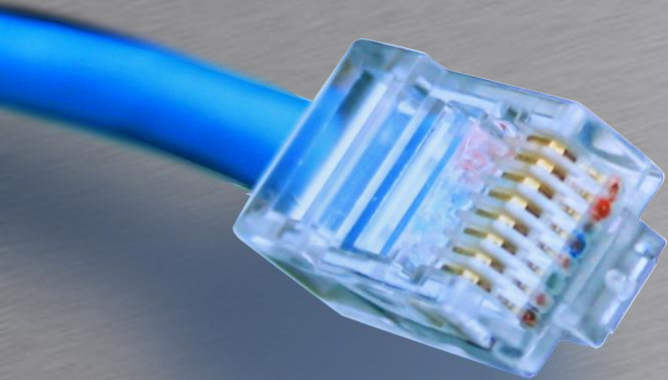
```
trap-group snmp-traps {
    version v2;
    categories {
        chassis;
        link;
    }
    targets {
        192.168.146.240;
    }
}
```



SNMP

- Test af SNMP
 - Getif
 - > show snmp mib walk .1 | no-more

Monitorering



HOUSE OF
TECHNOLOGY

A row of ten colorful circles in various colors and patterns, including solid colors and concentric circles.

- en del af **mercantec⁺**

Overvågning af udstyr



Chassis overvåring

- For at få information omkring de fysiske egenskaber kan man bruge `show chassis`

```
rael@SRX240> show chassis ?
```

```
Possible completions:
```

<code>alarms</code>	Show alarm status
<code>cluster</code>	Show chassis cluster information
<code>environment</code>	Show component status and temperature, cooling system speeds
<code>firmware</code>	Show firmware and operating system version for components
<code>forwarding</code>	Show forwarding process (fwdd) status
<code>fpc</code>	Show Flexible PIC Concentrator status
<code>hardware</code>	Show installed hardware components
<code>location</code>	Show physical location of chassis
<code>mac-addresses</code>	Show media access control addresses
<code>pic</code>	Show Physical Interface Card state, type, and uptime
<code>routing-engine</code>	Show Routing Engine status
<code>temperature-thresholds</code>	Show chassis temperature threshold settings



Interface overvåring

- For at se realtids statistik over et interface bruger `monitor interface if-navn`

```
SRX240                               Seconds: 3                               Time: 02:16:16
                                         Delay: 4/0/4
```

```
Interface: fe-0/0/7, Enabled, Link is Up
```

```
Encapsulation: Ethernet, Speed: 100mbps
```

Traffic statistics:

Current delta

Input bytes:	170279 (1800 bps)	[452]
Output bytes:	818104 (25064 bps)	[5920]
Input packets:	3112 (4 pps)	[10]
Output packets:	4809 (8 pps)	[16]

Error statistics:

Input errors:	0	[0]
Input drops:	0	[0]
Input framing errors:	0	[0]
Policed discards:	0	[0]
L3 incompletes:	0	[0]



Interface overvåring

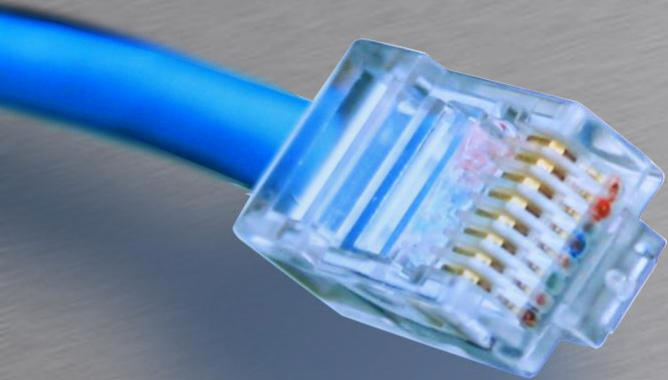
- Ping
- Traceroute
- Monitor traffic interface `ge-0/0/0`
- telnet



Opgradering

- Kræver bruger login til juniper.net
- JunOS kan hentes via web eller ftp
- `Request system software add <path>`
 - Opgraderer eller nedgraderer SW
 - Skal rebootes efter opgradering

Password Recovery



HOUSE OF
TECHNOLOGY

A row of ten colorful circles in various colors and patterns: a blue circle with a yellow center, a purple circle, a green circle with a yellow center, a blue circle with a yellow center, a green circle, a purple circle, a green circle with a yellow center, a purple circle, a green circle, and a blue circle with a yellow center.

- en del af **mercantec⁺**

Password Recovery Procedure



Password recovery

- Konsol adgang er et krav
- Genstart systemet
 - Tryk på space når den spørger om det

```
Hit [Enter] to boot immediately, or space bar for command prompt.
```

```
Booting [/kernel] in 1 second...
```

```
Type '?' for a list of commands, 'help' for more detailed help.
```

```
loader> boot -s
```

```
<output omitted>
```

```
Enter full pathname of shell or 'recovery' for root password recovery or RETURN
```

```
for /bin/sh: recovery
```

```
<output omitted>
```

```
root@SRX240> configure
```

```
[edit]
```

```
root@SRX240# set system root-authentication plain-text-password
```