epati

SSH Kullanım Kılavuzu

Ürün: Antikor v2 - Layer2 Tünelleme

Kılavuzlar

www.epati.com.tr

SSH Kullanım Kılavuzu

Kullanıcı adı ile Antikor'a SSH bağlantısı yapmak için SshClient, Putty vb. programlar kullanılabilmektedir. Kurum içinden bağlanılıyorsa Antikor'un iç IP adresi, kurum dışından bağlanılıyorsa dış IP adresi kullanılır. Port numarası 22022'dir. Kullanıcılar kendi kullanıcı adları ile giriş yapabilirler.

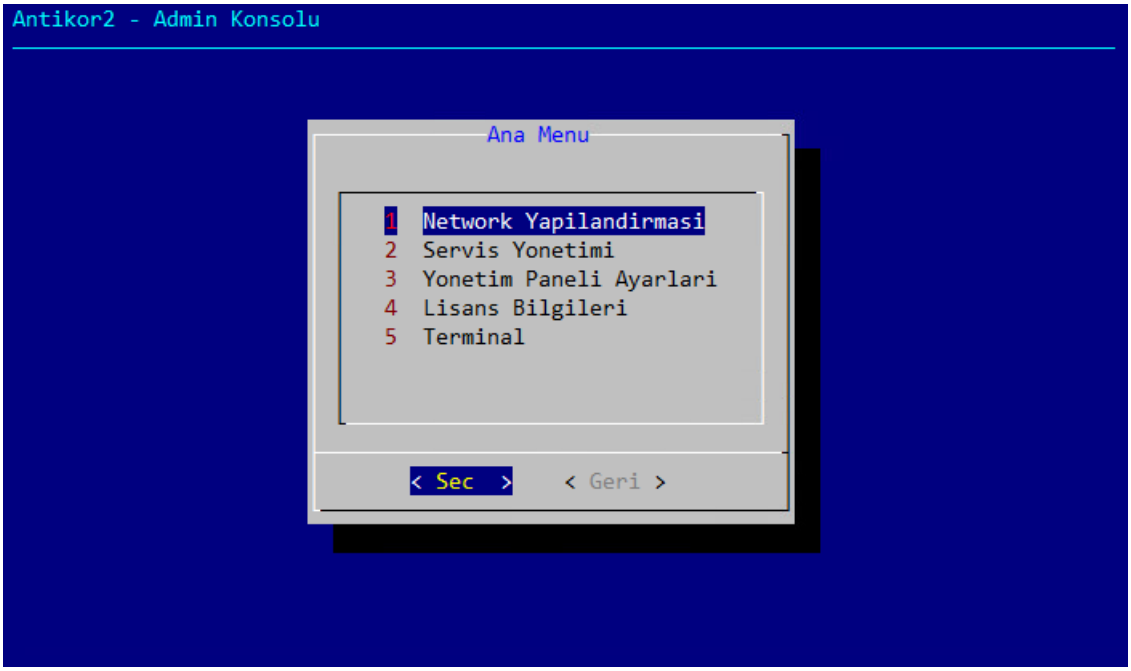
Önemli Not: Yanlışlıkla 22 portuna yapılacak SSH isteklerinde, Balküpü servisi açıksa; balküpü ayarları varsayılanda 22 portundan gelen bir istek olduğunda bunu saldırı olarak görmekte ve kullanıcının belirlediği süre boyunca (varsayılan 30 dakika) o IP adresini engellemektedir.

SSH Komutları

```
C:\Users\test>ssh epatisiber@10.2.1.146 -p 22022
Enter passphrase for key 'C:\Users\test/.ssh/id_rsa':
================================
==    Antikor L2 Tunelleme    ==
================================
Komut listesi icin '?' komutunu kullanabilirsiniz.
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$
```

- **adminKonsolu** komutu,

> Monitör ve klavye aracılığıyla erişilebilen konsol arayüzü, SSH bağlantısı aracılığıyla da erişilebilir.



- **arp** komutu,

> IP adresi bilinen cihazların fiziksel adreslerini öğrenmemizi sağlayan protokoldür. Parametreleri listeleyerek kullanım genişletilebilir.

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ arp
10.2.1.254 dev ens32 lladdr a0:36:9f:d4:3b:e8 STALE
10.2.1.253 dev ens32 lladdr dc:a5:f4:8b:19:43 STALE
10.2.1.69 dev ens32 lladdr 00:0c:29:ec:e5:5d REACHABLE
10.2.1.155 dev ens32 lladdr 00:50:56:a1:e7:f4 REACHABLE
10.2.1.45 dev ens32 lladdr 68:f7:28:94:32:7f REACHABLE
```

- **cd** komutu,

> Dizinler arası geçişi sağlar. Bir adım geriye dönmek için “cd ..” komutu kullanılır.

- **clear** komutu,

> SSH bağlantısında ekranda bulunan bilgileri temizler.

- **cluster-durumu** komutu,

> Tünel üzerinde (Cluster oluşturulmuş ise) Cluster durumu (state) hakkında bilgi vermektedir.

- **disk-bilgisi** komutu,

> Disk tercihi yapılarak, disk performans bilgisini verir. ada0 adlı diskin performans sonuçları;

```
yonetici:~$ disk-bilgisi ada0
ada0
        512             # sectorsize
        500107862016    # mediasize in bytes (466G)
        976773168       # mediasize in sectors
        4096            # stripesize
        0               # stripeoffset
        969021          # Cylinders according to firmware.
        16              # Heads according to firmware.
        63              # Sectors according to firmware.
        846ASZ7HS       # Disk ident.

Seek times:
        Full stroke:      250 iter in   7.947133 sec =   31.789 msec
        Half stroke:      250 iter in   6.113373 sec =   24.453 msec
        Quarter stroke:   500 iter in   9.766473 sec =   19.533 msec
        Short forward:    400 iter in   2.955254 sec =    7.388 msec
        Short backward:   400 iter in   3.999140 sec =    9.998 msec
        Seq outer:       2048 iter in   0.182564 sec =    0.089 msec
        Seq inner:       2048 iter in   0.232245 sec =    0.113 msec
Transfer rates:
        outside:       102400 kbytes in   1.285826 sec =    79638 kbytes/sec
        middle:        102400 kbytes in   1.527101 sec =    67055 kbytes/sec
        inside:        102400 kbytes in   2.459787 sec =    41630 kbytes/sec
```

- **disk-listesi** komutu,

> Donanımdaki mevcut disklerin bilgisini gösterir. ada0 adlı diskin, açıklaması, boyutu vb. bilgileri içeren çıktı;

```
yonetici:~$ disk-listesi
Geom name: ada0
Providers:
1. Name: ada0
   Mediasize: 500107862016 (466G)
   Sectorsize: 512
   Stripesize: 4096
   Stripeoffset: 0
   Mode: r5w3e10
   descr: TOSHIBA MQ01ABF050
   lunid: 50000395b5a82568
   ident: 846ASZ7HS
   rotationrate: 5400
   fwsectors: 63
   fwheads: 16
```

- **donanim-bilgisi** komutu,

> Sunucunun (ram, cpu vb.) donanım özelliklerini gösterir. Enter tuşuna basılarak çıktının devamı görülebilir.

- **eth-logs**

> Ethernet durumlarına ait logları görüntüler.

- **ethernet** komutu,

> Ethernet yazıp entere basıldığında bütün Ethernetlerin ve VLAN Ethernetlerinin anlık gönderme/alma trafiği görülür. Burada Rx Download, Tx Uploaddır. h harfine basarak yardımdan kullanılabilecek değerler ve zaman alınır.

- d değerleri Byte/KB/MB/GB otomatik çevirir.
- u değerleri bytes, bits, packets, errors cinsinden gösterir. Her u bastığımızda bir sonrakine geçer. Buradaki packets saniyedeki paket sayısı, errors ise saniyedeki hata sayısı
- t ortalama 30 saniye için başlangıçtan itibaren mevcut ve max oranları görüntülenir.
- a Kullanılmayan ethernetleri de gösterir.
- ”+” Normalde 0.500 s dir. Her + bastığımızda 100 ms süreyi artırır.
- ”-“ Normalde 0.500 s dir. Her - bastığımızda 100 ms süreyi azaltır.
- n input değerini değiştirir.
- q Programdan çıkışı sağlar.

Ethernet komutunun çıktısı aşağıdaki ekran görüntüsünde verilmiştir.

```
bwm-ng v0.6.3 (probing every 0.500s), press 'h' for help
input: /proc/net/dev type: rate
-         iface                   Rx                   Tx                Total
==============================================================================
            lo:           0.00  b/s            0.00  b/s            0.00  b/s
         ens32:         958.08  b/s            2.59 kb/s            3.54 kb/s
         ens33:           0.00  b/s            0.00  b/s            0.00  b/s
------------------------------------------------------------------------------
         total:         958.08  b/s            2.59 kb/s            3.54 kb/s
```

- **exit** komutu,

> Bağlandığınız kullanıcının SSH oturumunu düşürür.

- **grep** komutu,

> Girdi olarak verilen dosyalarda belirlenen kelimeyi satır satır arama işlemi yapar.

- **help** komutu,

> Yardım menüsünü açar, “?” ile aynı işlevi görmektedir.

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ help
adminKonsolu     ip           poweroff             sw-stats
arp              iperf        route                tcpdump
cd               ipsec        servis               telnet
clear            ipsec-debug  soket-yeniden-baslat traceroute
cluster-durumu   kullanici    ssh                  tunel-ayarlari
cluster-shell    less         sudo                 tunnel-flows
disk-bilgisi     lisans       sw-list              tunnel-tcpdump
disk-listesi     lpath        sw-mac-table         uname
donanim-bilgisi  lsudo        sw-mac-table-clear   uptime
eth-logs         mgmt-shell   sw-mac-table-stats   uygula
ethernet         more         sw-port-stats        webTarayici
exit             ndp          sw-show-interfaces   yedek-olustur
grep             netstat      sw-show-lacp         yenidenBaslat
help             nslookup     sw-show-lacp-stats
history          paket        sw-show-rstp
ifconfig         ping         sw-show-stp
```

- **history** komutu,

> SSH'ta en son kullanılmış komutların çıktısını gösterir.

- **ifconfig** komutu,

> Temel amacı gerçek ethernetler ile oluşturduğumuz VLAN ethernetlerine IP vermektir. IP bilgilerini görmek için de "ifconfig" komutu aracılığıyla bilgilere ulaşılabilir. IP vermek için, `sudo ifconfig bge0 10.2.2.1/24 up` yazılmalıdır.

- **ip** komutu,

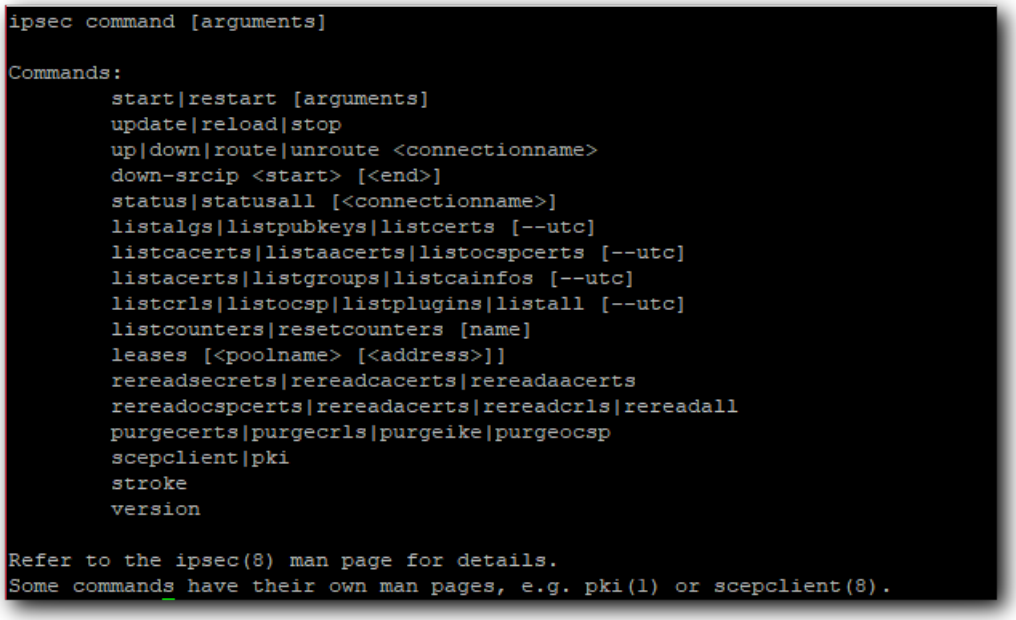
> IP ile ilgili işlemler yapılır. Link, address ve route gibi.

- **iperf** komutu,

> İki istemci arasındaki network hız testi için kullanılır.
> iperf -s paremetresi, bir istemcinin server olmasını sağlar.
> iperf -c host parametresi, bir istemcinin client olmasını sağlar.

- **ipsec** komutu,

> IPSec ayarlarına müdahele edilmektedir. Ayrıca start, restart, update ve versiyon gibi paremetreler de barındırmaktadır.

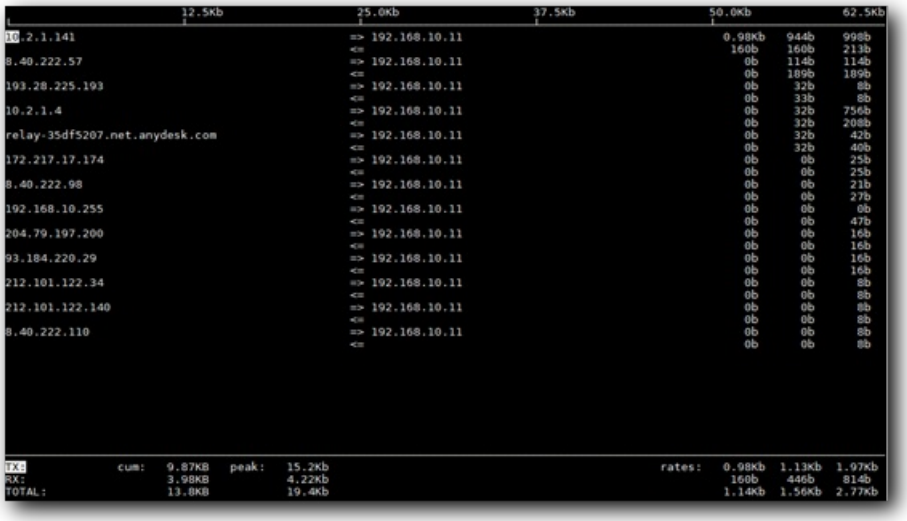


- **kullanici** komutu,

> Etherneti kullanan kullanıcı bilgileri görülür.

- kullanici –i bge0, Yerel Ağımızdaki IP'ler ile internetteki IP adreslerini gösterir.
- kullanici –i bge1, Dış taraftaki gerçek IP'ler ile internetteki IP adreslerini gösterir.
- kullanici –i bge2, Sunucu bölgesindeki IP'ler ile internetteki IP adreslerini gösterir.

> Antikor'un Web arayüzündeki Anlık Web Erişimi sadece Web isteklerini gösterirken burada 65536 portun tamamı görülebilmektedir. Dolayısıyla torrent kullanıcılarına ait trafik belirlenebilir. Ekran görüntüsü aşağıdaki gibidir.



Sadece bir VLAN'daki kullanıcılara bakılması halinde kullanici –i bge0.166

- **less** komutu,

Ekrana sığmayacak olan uzun çıktılar less komutu ile ekrana sığdırılarak gösterilir.

- **lisans** komutu,

Antikor'un lisans bilgilerini gösterir.

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ lisans
```

Lisans Sahibi	ePati Siber Güvenlik A.Ş. - Demo
Lisanslı Ürün	antikor Layer2 TN Staging - STAGING
Sözleşme Başlangıç Tarihi	30.04.2019 12:00:00
Sözleşme Bitiş Tarihi	31.12.2021 12:00:00

- **lpath** komutu,

Yetkili olunan klasörleri listeler.

- **lsudo** komutu,

Sudo yetkili olan komutları listeler.

- **mgmt-shell** komutu,

Kullanıcı bağımsız yönetim için oluşturulmuş olan ethernet arayüzünde yapılacak işlemler için management shell'e düşer.

- **more** komutu,

Bir komutun daha fazla bilgi vermesi için kullanılan komuttur.

- **ndp** komutu,

IPv4 protokolünde kullanılan ARP, ICMP vb. özelliklerin yerini almıştır.

- ndp – a, Geçerli tüm ndp girişlerini gösterir.
- ndp –d, Bir süper-user kullanıcısı –d paremetresi ile hostname olarak adlandırılan ana makine için bir girişin silinmesine olanak tanır.
- ndp –i, Bir ndp girişi -s parametresi ile eklendiğinde kullanılacak arabirimin dizinini belirtir.
- ndp –I, ndp için varsayılan Ethernet keşif arayüzünü siler.
- ndp –s, Donanım adresi ile ana makine adı için bir ndp girişi oluşturur. Temp komutta belirtilmedikçe giriş

kalıcıdır.

```
yonetici:~$ ndp -a
Neighbor                        Linklayer Address  Netif Expire    S Flags
fe80::1%bge1                    00:e0:66:c4:58:d9   bge1 permanent R
fe80::1%bge0_                   00:e0:66:c1:0c:2f   bge0 permanent R
```

- **netstat** komutu,

Ağ bağlantıları bilgilerini gösterir. (TCP, UDP, Port Numarası, Durum bilgisi.) Birçok parametresi vardır.

- netstat –m, Network durumu hakkında bilgi verir.
- netstat –n, Sunucu üzerinde kurulmuş bağlantıların listesini verir.

```
yonetici:~$ netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 localhost.6379         localhost.22559        LAST_ACK
tcp4       0      0 localhost.6379         localhost.14552        LAST_ACK
tcp4       0      0 10.2.1.141.22022       10.2.1.141.14535       ESTABLISHED
tcp4       0      0 10.2.1.141.14535       10.2.1.141.22022       ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.141.37400       ESTABLISHED
tcp4       0      0 10.2.1.141.37400       10.2.1.141.22022       ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.12.1423         ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.12.1422         ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.12.1415         ESTABLISHED
tcp4       0      0 localhost.postgresql   localhost.59082        ESTABLISHED
```

- **nslookup** komutu,

DNS Serverin düzgün çalışıp çalışmadığı kontrol etmek için kullanılır.

- **paket** komutu,

Antikor paketlerinin sürüm ve durum bilgilerini gösterir.

Paket Sürüm Listesi

Paket	Sürüm	Durum
Yapılandırma Yöneticisi - Staging	2.0.59	Güncel
Arayüz Modülü - Staging	2.0.157	Güncel
Araç Kutusu - Staging	2.0.5	Güncel
Yönetimsel Araçlar	2.0.16	Güncel
Haberleşme Modülü - Staging	2.0.160->2.0.161	Kurulmaya Hazır
Haberleşme Aracısı	2.0.15	Güncel
Modül Yöneticisi	2.0.15	Güncel
Yönetici Konsolu - Staging	2.0.17	Güncel
Haberleşme Yöneticisi (Router)	2.0.5	Güncel
Eklenti - Ortam Sağlayıcı	2.0.11	Güncel
Eklenti - Bildirim İletici	2.0.40	Güncel
Eklenti - İzleyici	2.0.31	Güncel
Eklenti - Bildirim Gönderici Modülü	2.0.17	Güncel
Eklenti - Syslog	2.0.22	Güncel

- **ping** komutu,

Hedef bilgisayar, sunucu gibi cihazların çalışmasını, uzaklığını vb. işlevleri tespit için kullanılır.

```
Icmp_seq, Paketin başlık bilgisi, her ping paketinde başlık sırası artacaktır.
TTL (time to live),  Paketin yaşam süresi.
Time, Ping iletişiminin ne kadar zamanda gerçekleştiği bilgisi.
```

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ ping 10.2.1.253
PING 10.2.1.253 (10.2.1.253) 56(84) bytes of data.
64 bytes from 10.2.1.253: icmp_seq=1 ttl=255 time=0.762 ms
64 bytes from 10.2.1.253: icmp_seq=2 ttl=255 time=0.891 ms
64 bytes from 10.2.1.253: icmp_seq=3 ttl=255 time=0.854 ms
64 bytes from 10.2.1.253: icmp_seq=4 ttl=255 time=0.989 ms
```

- **poweroff** komutu,

> Tünel sunucunun kapatılmasını sağlar.

- **route** komutu,

> İşletim sistemine yeni route eklemek veya silmek için kullanılır.

- sudo route delete default, o anki route siler.
- sudo route add default 10.2.1.253

> Aşağıdaki görüntüde ilk önce route silinip sonra yeniden eklenmiştir.

```
yonetici:~$ sudo route delete default
delete net default
yonetici:~$ sudo route add default 10.2.1.253
add net default: gateway 10.2.1.253
```

- **servis** komutu,

> Antikor servislerinin durumları hakkında bilgi verir. Servisler “Çalışıyor, Kapalı, Bypass ya da Yapılandırılmadı” olarak aşağıda görülmektedir.

```
Servis Listesi
+-------------+-------------------------+-----------------+
| Servis      | Açıklama                | Durum           |
+-------------+-------------------------+-----------------+
| tunel       | Layer2 Tünelleme Motoru | Çalışıyor       |
| routing     | Layer3 Yönlendirme      | Kapalı          |
| vpn-ipsec   | VPN - IPSec Servisi     | Yapılandırılmadı|
| snmp-servisi| SNMP Servisi            | Kapalı          |
+-------------+-------------------------+-----------------+
```

- **soket-yeniden-baslat** komutu,

> Soketin yeniden başlatılması için kullanılır.

- **ssh** komutu,

> Uzak bağlantı için kullanılan bir protokoldür.

```
10.2.1.141 - PuTTY
login as: yonetici
Using keyboard-interactive authentication.
Password for yonetici@antiKor2.epati.com.tr:
Last login: Tue Feb 27 08:51:43 2018 from 10.2.1.141
================================
== ePati Bilisim Teknolojileri ==
==   Antikor v2 UTM Firewall   ==
================================
Komut listesi icin '?' komutunu kullanabilirsiniz.
yonetici:~$
```

- **sudo** komutu,

> Sudo, çalıştırma yetkisi olan komutları root yetkili olarak çalıştırılmasını sağlar. Route ekleme ve silme işlemlerinin yapılabilmesi için, sudo yetkilendirmesi gerekmektedir.

```
yonetici:~$ route delete default
route: must be root to alter routing table
```

- **sw-list** komutu,

Switchleri listeler.

```
 switch_id |  adi   | aciklama
-----------+--------+----------
 switch1   | Merkez | Merkez
(1 row)
```

- **sw-mac-table** komutu,

Komut sonuna girilen switch için port,VLAN ve MAC adresi bilgilerini listeler. (Örnek kullanım:`sw-mac-table switch1`)

```
port            VLAN MAC                Age
tunel3           250 1c:75:08:33:48:8e    0
ens34            250 00:50:56:a1:d6:54    0
```

- **sw-mac-table-clear** komutu,

Komut sonuna girilen switch'in MAC adresi tablosunu temizler. (Örnek kullanım:`sw-mac-table-clear switch1`)

```
table successfully flushed
epati:~$
```

- **sw-mac-table-stats** komutu,

Komut sonuna girilen switch'in MAC tablosuna ait durumları listeler. (Örnek kullanım:`sw-mac-table-stats switch1`)

```
Statistics for bridge "switch1":
  Current/maximum MAC entries in the table: 2/131072
  Current static MAC entries in the table : 0
  Total number of learned MAC entries     : 9
  Total number of expired MAC entries     : 3
  Total number of evicted MAC entries     : 0
  Total number of port moved MAC entries  : 0
```

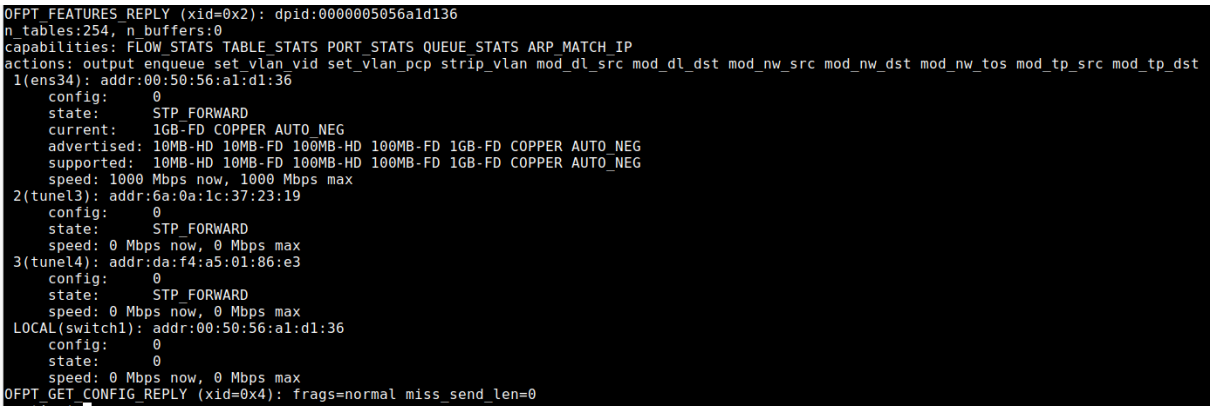
- **sw-port-stats** komutu,

Portlara ait durumlar listelenir.

```
PORT                RX-PKT          RX-BYTE          TX-PKS          TX-BYTE
ens34:              916072        786960358           35732          3222069
tunel3:              16183          1339194           14852         30851284
tunel4:                  0                0             914            77053
```

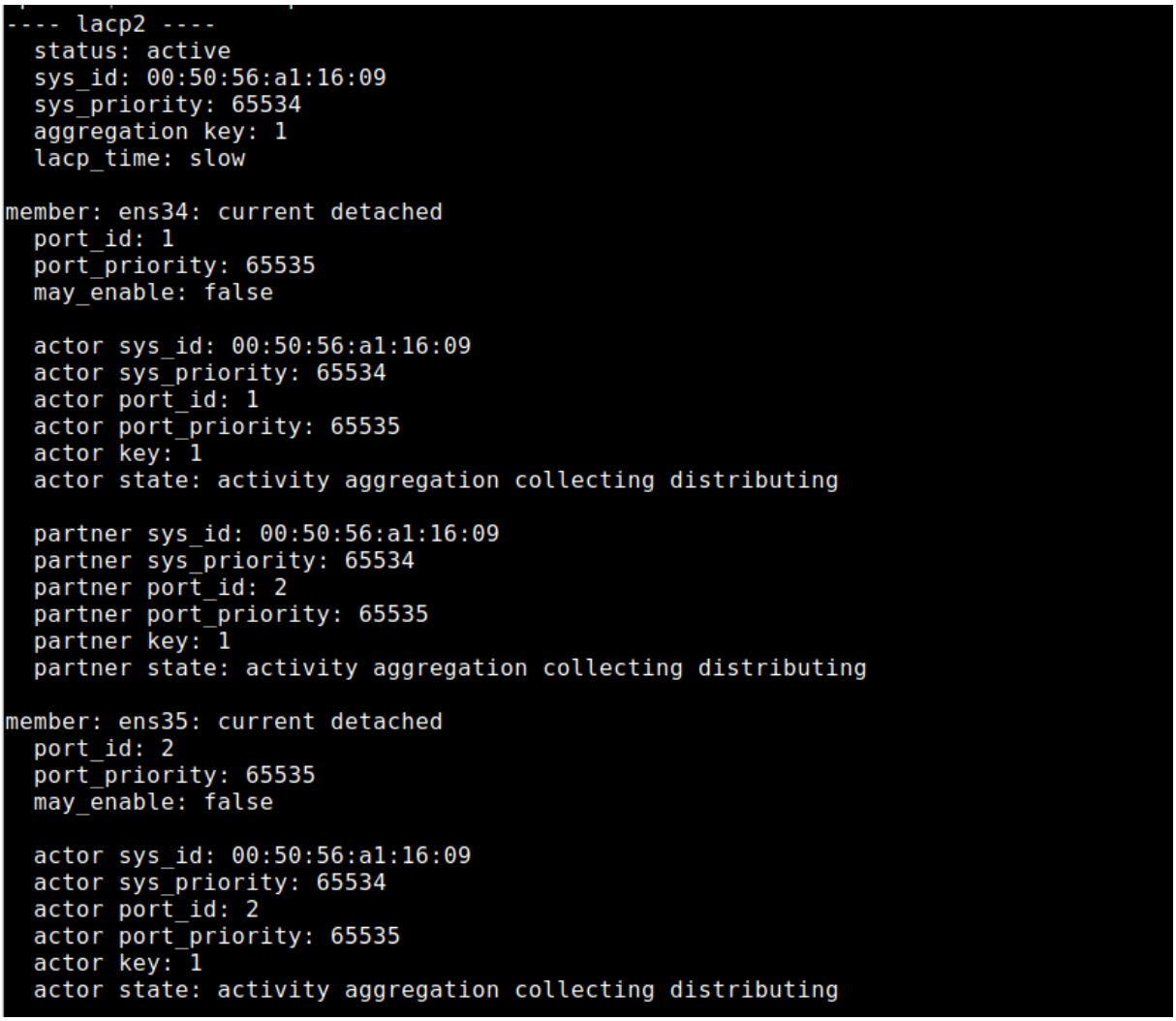
- **sw-show-interfaces** komutu,

Komut sonuna girilen switch'e üye arayüzleri listeler. (Örnek kullanım:`sw-show-interfaces switch1`)



- **sw-show-lacp** komutu,

> Komut sonuna girilen switch için lacp arayüzleri listeler. (Örnek kullanım:`sw-show-lacp switch1`)



- **sw-show-lacp-stats** komutu,

> Komut sonuna girilen switch için lacp arayüzlerine ait durumları listeler. (Örnek kullanım:`sw-show-lacp-stats switch1`)

```
---- lacp2 statistics ----

member: ens34:
  TX PDUs: 32
  RX PDUs: 32
  RX Bad PDUs: 0
  RX Marker Request PDUs: 0
  Link Expired: 0
  Link Defaulted: 0
  Carrier Status Changed: 0

member: ens35:
  TX PDUs: 32
  RX PDUs: 32
  RX Bad PDUs: 0
  RX Marker Request PDUs: 0
  Link Expired: 0
  Link Defaulted: 0
  Carrier Status Changed: 0
```

- **sw-show-rstp** komutu,

> Switch'te rstp devredeyse; komut sonuna girilen switch'e ait rstp bilgilerini listeler. (Örnek kullanım:`sw-show-rstp switch1`)

```
No such RSTP object
ovs-appctl: ovs-vswitchd: server returned an error
epati:~$ sw-show-rstp switch1
---- switch1 ----
Root ID:
  stp-priority    32768
  stp-system-id   00:50:56:a1:1e:f0
  stp-hello-time  2s
  stp-max-age     20s
  stp-fwd-delay   15s
  This bridge is the root

Bridge ID:
  stp-priority    32768
  stp-system-id   00:50:56:a1:1e:f0
  stp-hello-time  2s
  stp-max-age     20s
  stp-fwd-delay   15s

  Interface  Role       State      Cost     Pri.Nbr
  ---------- ---------- ---------- -------- -------
  tunel4     Designated Forwarding 200000   128.1
  lagg1      Designated Forwarding 20000    128.2
```

- **sw-show-stp** komutu,

> Switch'te stp devredeyse; komut sonuna girilen switch'e ait stp bilgilerini listeler. (Örnek kullanım:`sw-show-stp switch1`)

```
---- switch1 ----
Root ID:
  stp-priority  32768
  stp-system-id   4a:a6:e4:b3:6a:4d
  stp-hello-time  2s
  stp-max-age     20s
  stp-fwd-delay   15s
  This bridge is the root

Bridge ID:
  stp-priority  32768
  stp-system-id   4a:a6:e4:b3:6a:4d
  stp-hello-time  2s
  stp-max-age     20s
  stp-fwd-delay   15s

  Interface  Role       State      Cost  Pri.Nbr
  ---------- ---------- ---------- ----- -------
  tunel4     designated listening  19    128.1
```

- **sw-stats** komutu,

> Komut sonuna girilen switch'e ait istatistiksel verileri listeler.

```
Event coverage, avg rate over last: 5 seconds, last minute, last hour,  hash=d7d9e943:
rev_mac_learning           0.0/sec     0.033/sec        0.0056/sec   total: 45
mac_learning_learned       0.0/sec     0.033/sec        0.0053/sec   total: 23
mac_learning_expired       0.0/sec     0.000/sec        0.0008/sec   total: 7
mac_learning_moved         0.0/sec     0.000/sec        0.0000/sec   total: 38
epati:~$
```

s

- **tcpdump** komutu,

> Ağ dinlemek için kullanılan tcpdump komutunun, birçok parametresi vardır.

- tcpdump –D, Ağ üzerinde dinlenebilecek bütün arayüzleri listeler.
- tcpdump –i bge0, bge0 arayüzünün dinlenmesini sağlar.
- tcpdump -n src net 10.2.1.141 Belirtilen ağ adresinden gelen paketleri listeler.
- tcpdump –ni bge, Yerel ağın trafiğini izler. bge ethernet arayüzüne bağlı VLAN'ları da gösterir.
- tcpdump –ni bge0.166 host 10.2.2.2, 166 vlanındaki sadece bu IP'nin trafiğini gösterir.
- tcpdump ether host 11:22:33:44:55:66, bu mac adresli bilgisayarın trafiğini gösterir.
- tcpdump -i bge0.166 host 10.2.2.2 or 10.2.2.10, Bu 2 IP'nin trafiğini gösterir.
- tcpdump udp and (src port 161 or 162 or 514), UDP ile kaynak portu 161,162 ve 514 olanları göster. Örnekleri çoğaltmak mümkün.

```
yonetici:~$ tcpdump -ni bge1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bge1, link-type EN10MB (Ethernet), capture size 65535 bytes
09:14:45.424123 IP 10.2.1.141.22022 > 10.2.1.12.1415: Flags [P.], seq 1477914982:1477915018, ack 155735475
5, win 128, length 36
09:14:45.424447 IP 10.2.1.12.1415 > 10.2.1.141.22022: Flags [.], ack 36, win 2048, length 0
09:14:46.086969 ARP, Request who-has 10.2.1.190 tell 10.2.1.254, length 46
09:14:46.439086 IP 10.2.1.141.22022 > 10.2.1.12.1415: Flags [P.], seq 36:240, ack 1, win 128, length 204
09:14:46.479312 IP 10.2.1.12.1415 > 10.2.1.141.22022: Flags [.], ack 240, win 2053, length 0
```

- **telnet** komutu,

> Uzaktan bir bilgisayara ya da servera bağlanmak için kullanılan komuttur. SSH'a göre daha az güvenlidir. Aşağıdaki görüntü gibi bağlantı sağlayabilirsiniz, telnet için ayarlarınız yapılı ise bağlantı oturumu kurulacaktır.

```
yonetici:~$ telnet 10.2.1.50
Trying 10.2.1.50...
```

- **traceroute** komutu,

> IP paketinin hedefe giderken, hangi routerlar üzerinden geçtiğinin bilgisini vermektedir.

- **tunel-ayarlari** komutu,

> Tünel network ayarlarını görüntüler.

- **tunnel-flows** komutu,

> Bir porttan geçen anlık sessionları görüntüler.

- **tunnel-tcpdump** komutu,

> Tünele ait trafiğin dinlenmesi için kullanılır.

- **uname** komutu,

> İşletim sistemini çıktı olarak verir. (-a parametresi ile birlikte kullanıldığında işletim sistemine ait tüm detayları çıktı olarak verir.)

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ uname -a
Linux Antikor-v2.epati.com.tr 5.10.79-1-lts #1 SMP Fri, 12 Nov 2021 19:04:00 +0000
x86_64 GNU/Linux
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ uname
Linux
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$
```

- **uptime** komutu,

> Cihazın ne kadar süredir açık olduğu bilgisini verir.

```
%epatisiber@10.2.1.146 - ePati Siber Guvenlik A.S.:~$ uptime
 15:47:56 up  4:52,  1 user,  load average: 0.23, 0.27, 0.19
```

- **uygula** komutu,

> Arayüzde “Tanımları Uygula” butonu ile aynı işlevi görmektedir.

- uygula –a Uygulanması beklenen tanımları uygular.
- uygula –cf istenilen kuralın uygulanmasını sağlar.

> Mesela aşağıdaki görüntüde DNS ayarları tekrardan uygulanmıştır.

```
yonetici:~$ uygula -cf dns-ayarlari
```

- uygula –fa, Antikordaki bütün kuralları tekrardan uygular.
- uygula –la, Servislerin durumlarına dair bilgiler verir.

Uygulama Listesi

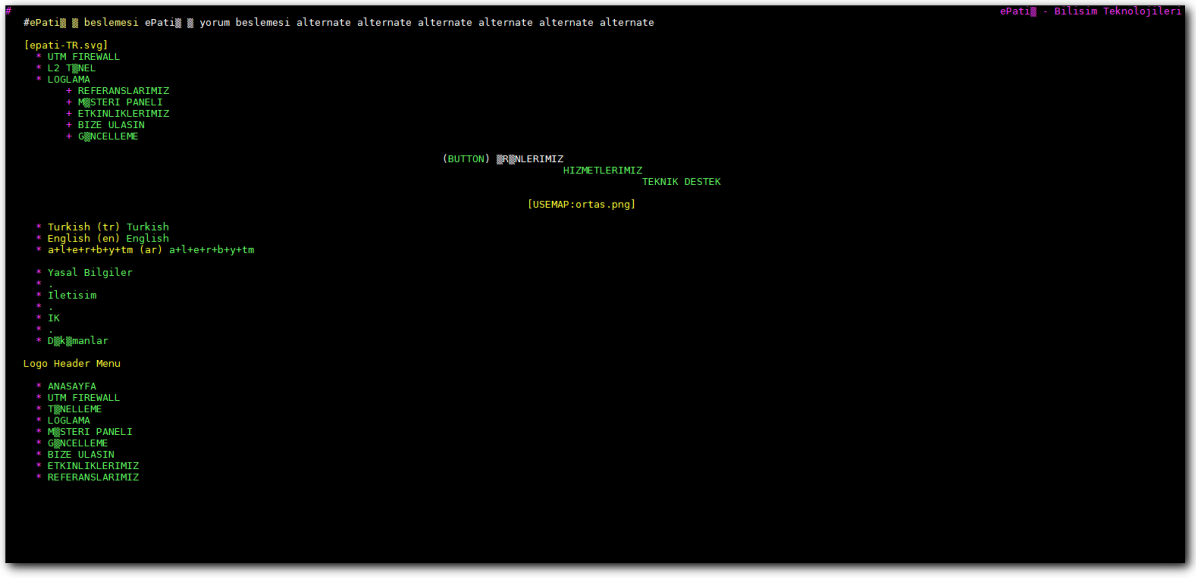
Uygulama	Açıklama	Durum
ag-tanim-yenile	Ağ Tanımları Yenileme	Güncel
ag-yapilandirmasi	Ağ Yapılandırması	Güncel
giris-banner	Giriş Banner Yapılandırıcı	Güncel
ssh-kullanici	Ssh Kullanıcıları	Güncel
ssh-yetki	Ssh Yetkileri	Güncel
cluster-senkronizasyonu-full	Cluster Senkronizasyonu (Full)	Güncel
dns-ayarlari	DNS Yapılandırması	Güncel
ethernet-atama	Ethernet Atama	Güncel
panel-erisim	Web Paneli Erişim Yapılandırması	Güncel
sanal-ethernet-lagg	Sanal Ethernet - Birleştirme	Güncel
sanal-ethernet-loopback	Sanal Ethernet - Loopback	Güncel
sanal-ethernet-vlan	Sanal Ethernet - VLAN Etiketi Tabanlı	Güncel
snmp	Snmp	Güncel
statik-yonlendirme	Statik Yönlendirme	Güncel
syslog	Syslog Ayarları	Güncel
tunnel	Tünel Yapılandırması	Güncel
vpn-ipsec	IPsec VPN Yapılandırması	Güncel
yonetim-paneli	Yönetim Paneli Ayarları	Güncel
cluster	Cluster Ayarları	Güncel
ethernet-web-arayuzu-erisimi	Ethernet Web Arayüzü Erişimi	Güncel
cluster-guncelleme-senkronizasyonu	Cluster Güncelleme Senkronizasyonu	Güncel
cluster-senkronizasyonu	Cluster Senkronizasyonu	Güncel
yeniden-uygulama-buffer	[Gizli] Yeniden Uygulama Buffer (Cluster Pasif Cihaz)	Güncel
cluster-servis-senkronizasyonu	Cluster Servis Senkronizasyonu	Güncel

- **yedek-olustur** komutu,

Cihazın yedek dosyası oluşturulur.

- **webTarayici** komutu,

Konsol üzerinde web siteleri açmak için kullanılan komuttur.



- **yenidenBaslat** komutu,

Sunucuyu yeniden başlatmak için kullanılır.

- **?** komutu,

Yardım menüsünü açar, “help” ile aynı işlevi görmekte.