



Switch security



Hoofdstuk 6



Inleiding



Switch ports



Secure remote access

Inleiding

Wat weet je nog over switch verbindingen en veiligheid uit netwerken1?



Paswoorden

Enable
secret

Shutdown

MAC-table

Manage
VLAN

Encryptie

Telnet

SSH

Console

VLAN 1

MotD

Inleiding

FUTURE-PROOF

PEOPLE-CENTRIC

➔ We kijken dieper naar:

✓ Poort beheer

✓ SSH

Switch ports

- ➔ Ongebruikte poorten:
 - ✓ Maak ze onbruikbaar
 - ⇒ Shutdown command
 - ✓ Preventie fysieke aanvallen

Switch ports

➔ Zet een poort in shutdown

```
SW1# conf t
SW1 (config)#int f0/1
SW1 (config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
SW1 (config-if)#
```

➔ Er kan ook op een hele range van ports gewerkt worden

⇒ Switch(config)# **interface range** *type module/first-number – last-number*

```
SW1# conf t
SW1 (config)#int range f0/2-24
SW1 (config-if-range)#shutdown
```

Switch ports

→ Aantal MAC's limiteren op een poort

→ verschillende methodes:

✓ Static secure MAC addresses

✓ Dynamic secure MAC addresses

✓ Sticky secure MAC addresses

Switch ports

✓ Static secure MAC addresses

- ⇒ Manueel ingegeven MAC-adressen
- ⇒ Command: switch port-security mac-address
- ⇒ Opgeslagen in de table op de running config

Switch ports

→ Aantal MAC's limiteren op een poort

→ verschillende methodes:

✓ Static secure MAC addresses

✓ Dynamic secure MAC addresses

✓ Sticky secure MAC addresses

Switch ports

✓ Dynamic secure MAC addresses

- ⇒ MAC-adressen worden dynamisch geleerd
- ⇒ Word enkel in de table opgeslagen
- ⇒ Deze adressen worden gewist als de switch reboot of de port op down word gezet

Switch ports

→ Aantal MAC's limiteren op een poort

→ verschillende methodes:

✓ Static secure MAC addresses

✓ Dynamic secure MAC addresses

✓ Sticky secure MAC addresses

Switch ports

✓ Sticky secure MAC addresses

- ⇒ Dynamisch geleerd adres toegevoegd aan zowel de tabel als de running config
- ⇒ Command: *"switch port-security mac-address sticky"*
- ⇒ Als de deze niet worden opgeslagen naar de startup configuration file word dit niet bijgehouden na een reboot van de switch

Secure remote access

➔ Veiligere remote verbinding = SSH

➔ verbetering op Telnet

⇒ geëncrypteerde verbinding

Secure remote access

→ Programma's zoals Wireshark onderscheppen communicatie

⇒ Probleem bij telnet:

✓ plaintext

⇒ Oplossing:

✓ encryptie = SSH

Secure remote access

Telnet

SSH

```
Stream Content:
.....
User Access Verification
Username: .....P.....vt100..8Boobb
Password: cisco
R1>eenn
Password: class
R1#
```

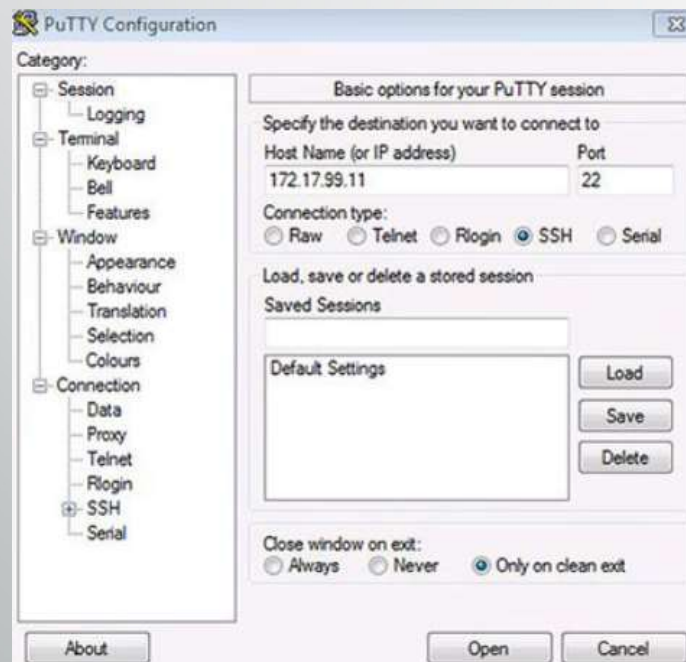
```
Stream Content
SSH-1.99-cisco-1.25
SSH-2.0-TTSSH/2.56 win32
...T...Ga...5...Ydiffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1...ssh-rsa...aes128-cbc,3des-cbc,aes192-cbc,aes256-
cbc...aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc...+hmac-sha1,hmac-sha1-96,hmac-
md5,hmac-md5-96...+hmac-sha1,hmac-sha1-96,hmac-md5,hmac-
md5-96...none...none...g.K=...g[...x...ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group1-sha1...Kecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-
dss...aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,3des-ctr,3des-
cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,arcfour,cast128-ctr,cast128-
cbc...aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,3des-ctr,3des-
cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,arcfour,cast128-ctr,cast128-
cbc...hmac-sha1,hmac-md5...hmac-sha1,hmac-
md5...none,zlib@openssh.com,zlib...none,zlib@openssh.com,zlib...1.o3....
".....m
.&.....!h.4..b.....).N..g.t...."QJ.y.4.....:C.O+
m...70.5mmQ.E...vb^...LB..7.k...8k.Z....$.|K..I(fQ[...=.|.c...M6.U..i.?..
$.e]#...b.V..R...)p..mg.5Nj...t!...!2.^F.6;..w.....].OLR..
+...X..9.I...j...&.....R.Z...-3..
.Pz3.U!...d...X..
{...qW}...}...3....J%a...&...k./....d.v.s>.jdr.+..
{...wza]lw...F...O.t..1C.[...K...!...r<.....q...[&..'j..<.h4....
%...L...(|YGNK...O...#;..Q[...a)p.....v!
pH...Z.....M.5.4.1.....
|..X]..bH5...mf..R...+..D...AP.I...V.81x.|...w...k...
...hv1+w<...1d.&.EUB...$I3P(...!O.|sO...?M...%z$'c..w...k.
..^.#...V...^...K...!$X.&x..j.)Y9.R.IW..f.|{.O=T...}j;..Z(..H...+.3.wt.
C.I...Q..w@...a.zg(..<...
(I...e...DB.x.zg.....f....p..^k<.k...0.Jx..BIS.I...<..Q..$...."
```

Secure remote access

→ SSH activeren:

```
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
S1(config)# username admin secret ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)#
```


Secure remote access





PT_switchport_security

Practice
Makes Perfect

