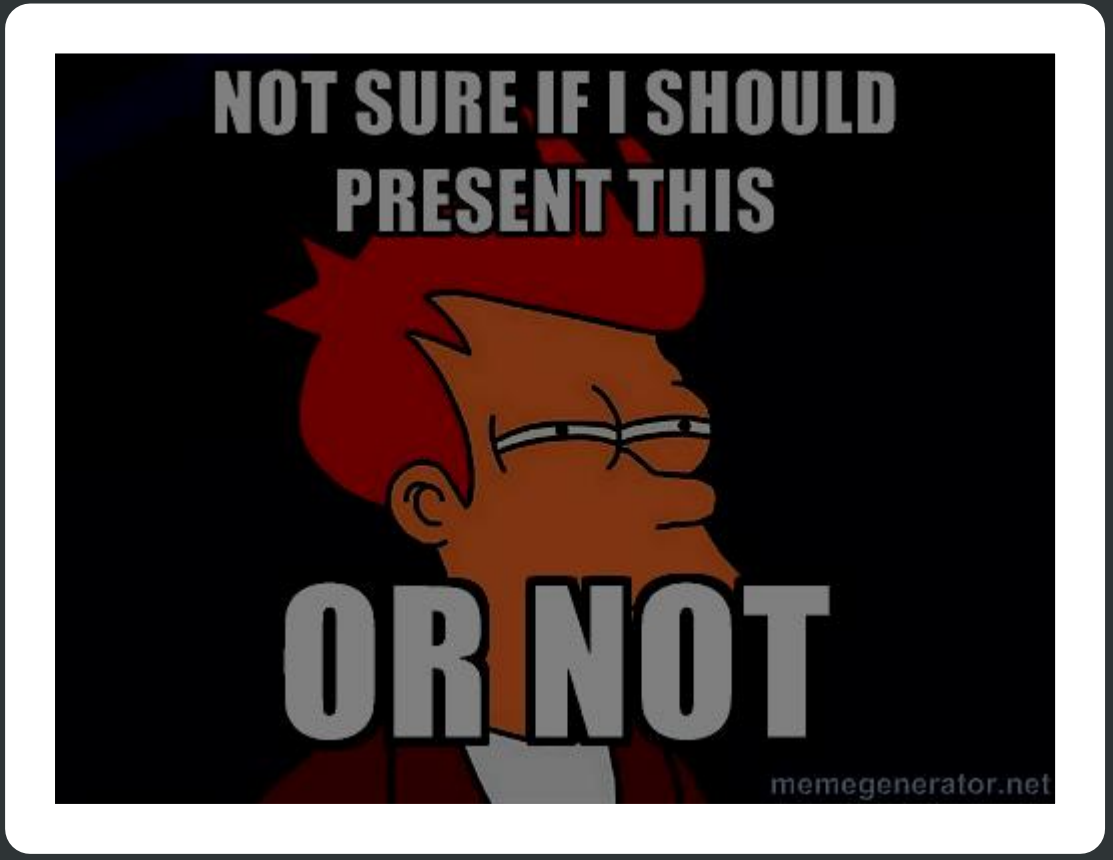
Napad na wps zaščito

Peter Kavčič

Zakaj to predavam

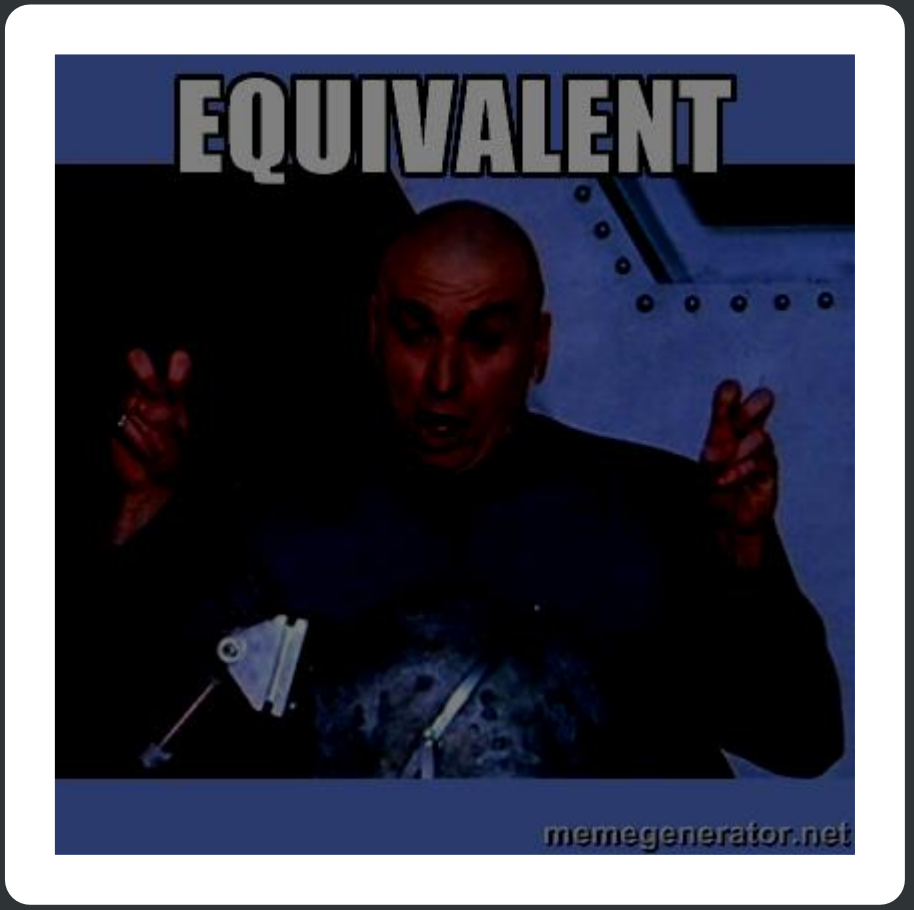
- Prelahko da bi bilo res (bomo videli)
- Nimamo časa zvedeti vse o vsem



Vrste zaščite za wifi

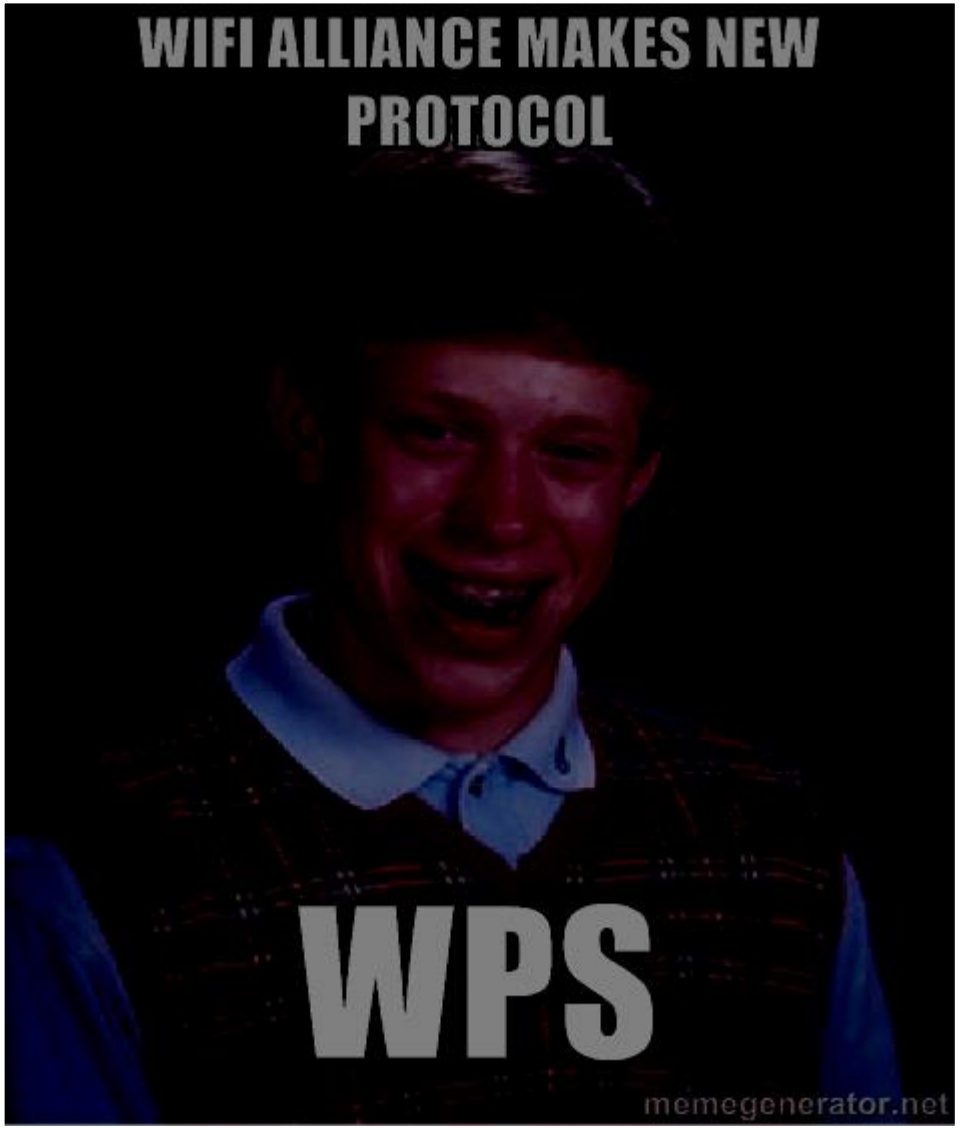
- WEP
- WPA\2
- RADIUS

- WPS



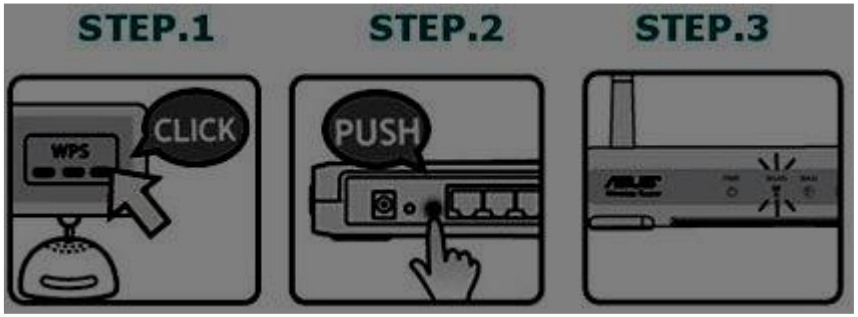
Kaj je WPS?

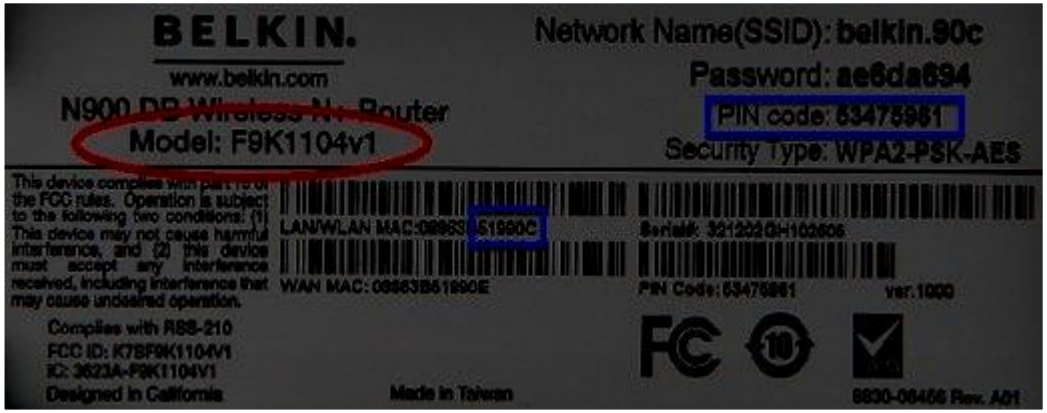
- Protokol za povezovanje
- WiFi alliance



Povezovanje

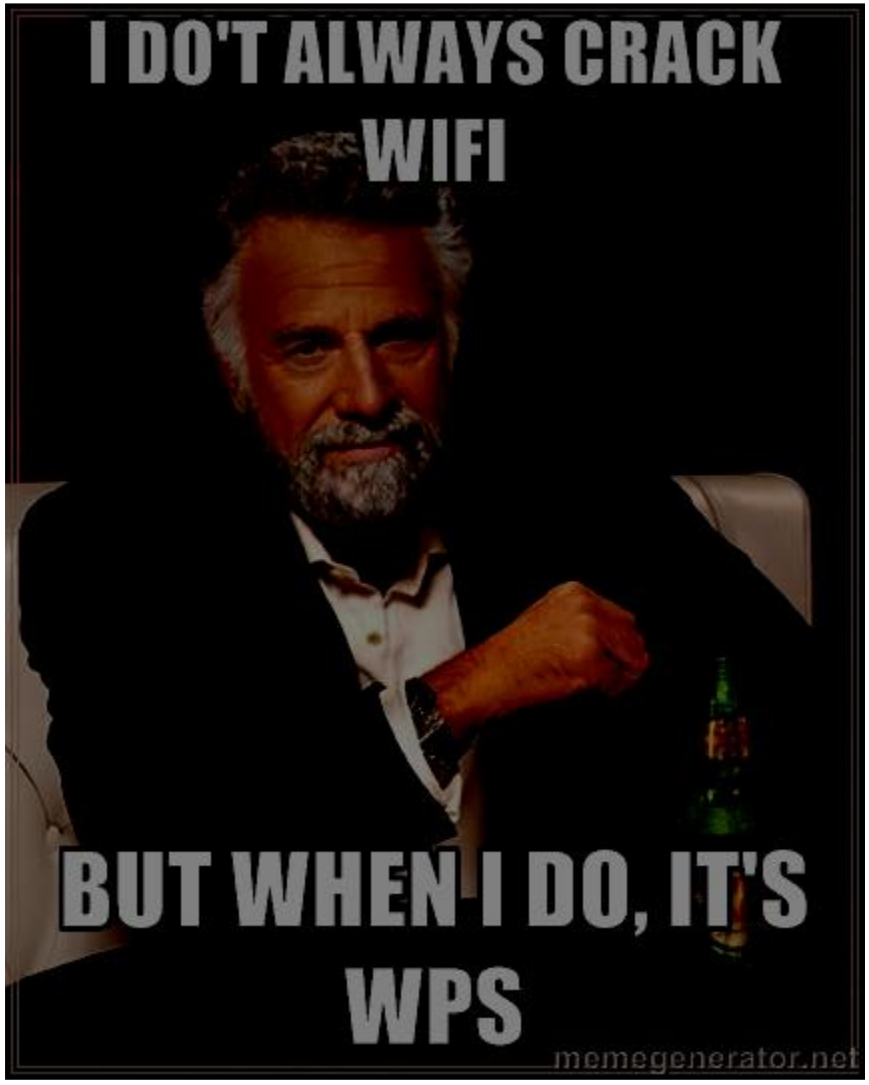
- 8 mestna stevilka
- Gumb
- Nfc





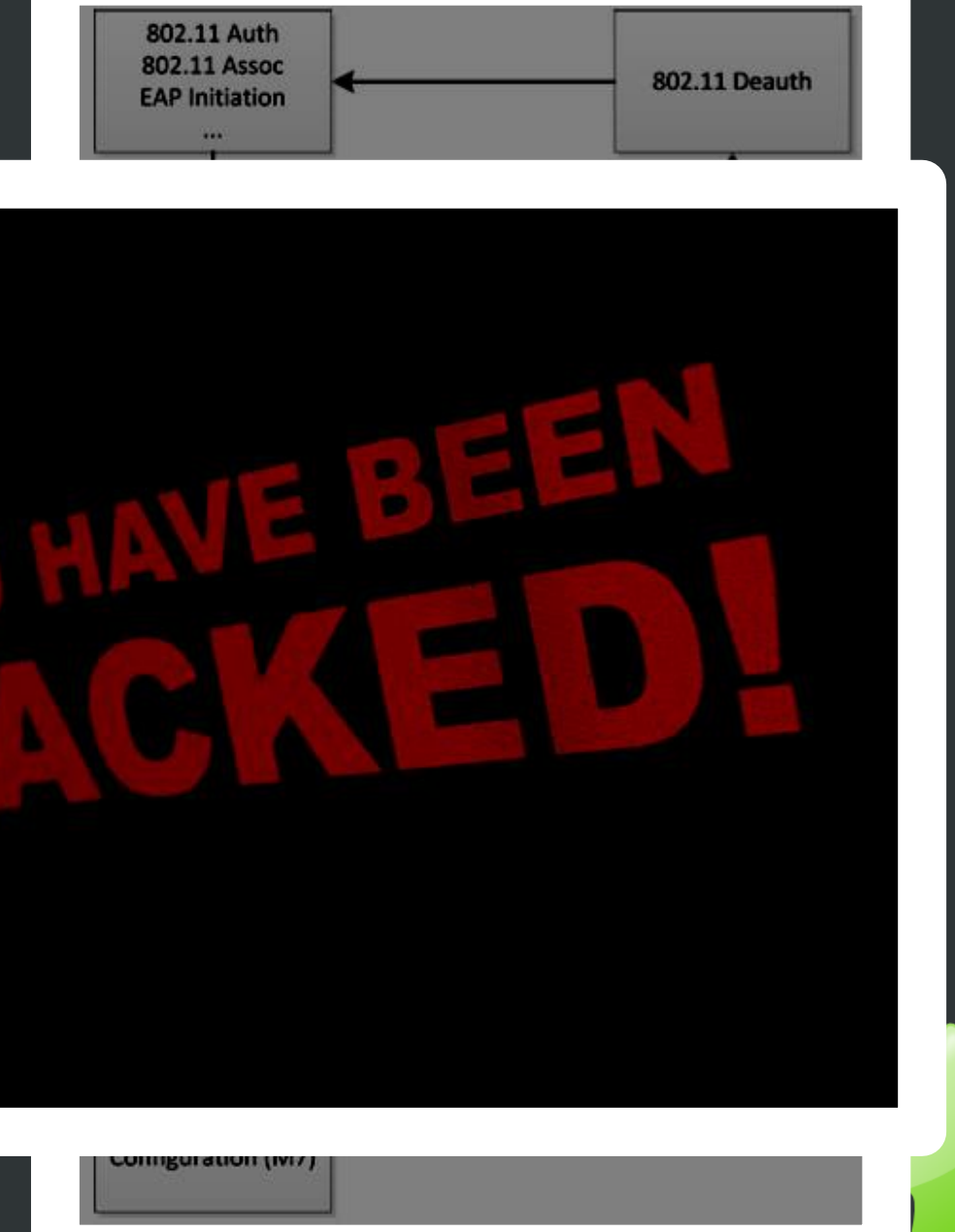
Metodi napada:

- Bruteforce online napad
- Pixie dust



Bruteforce

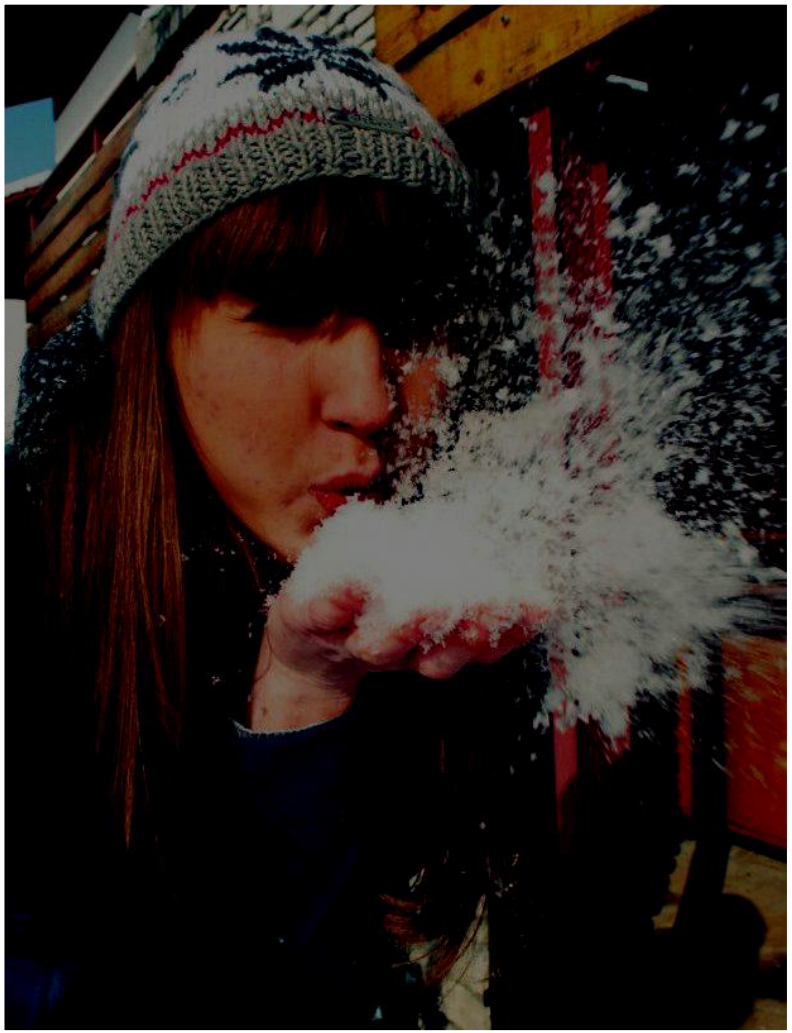
- EAP-NACK po M4
- EAP-N
- $10^4+1$0
- 10h
- pocase



Pixie dust

Linear Feedback Shift Register

- Seme
- Permutacija
- E-S1
- E-S2



Potek napadov

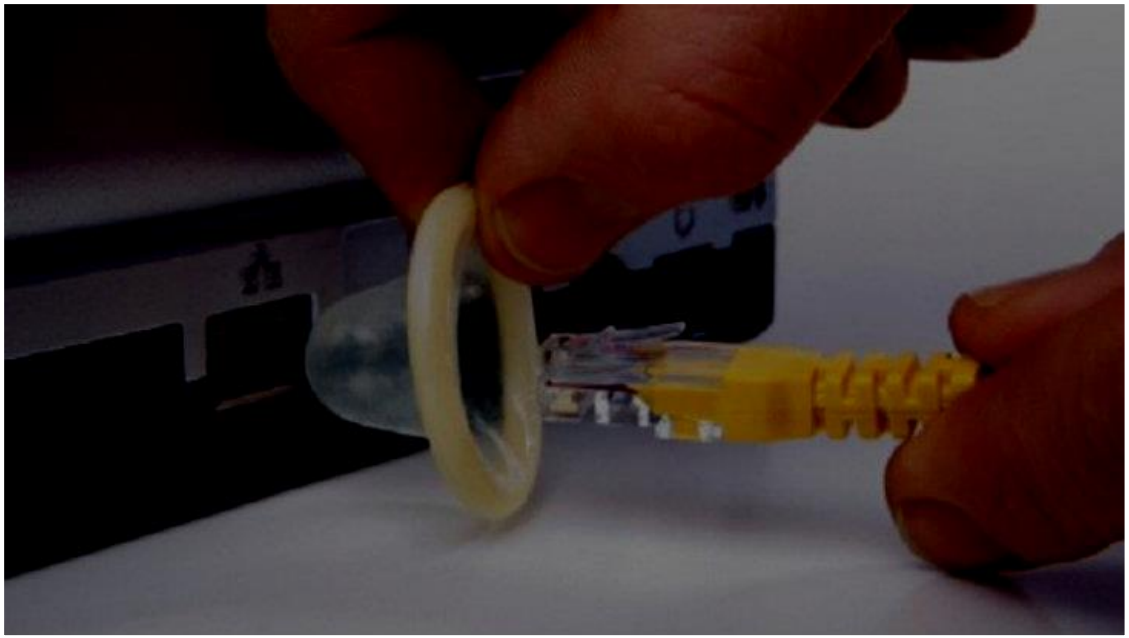
- Izberemo wifi adapter
- Monitor mode
- Iskanje potencialnih žrtev
- Napad

Težavnost napada

- Kali linux
- Reaver 1.6

Zaščita

- Time out
- Router brez WPS
- Firmware upgrade (dd-wrt)
- Penetracija
-



QR kode

- Bolj podrobno o napadu
- Seznam DD-WRT

Hvala za pozornost!

Pogosta vprašanja

- Zakaj meni to ne dela
- Različna oprema, različne interference, različni parametri
- Lahko to naredim tudi jaz?
- Lahko, a samo na ruterjih katerih lastnikova dovoljenja imaš
- Ali lahko sam naložim ddwrt?
- V primeru, da route[illegible], da. Seznam je objavljen na: