

فیض ملا تاھوی رانی سل 2.0 IBNS نیوکت ددعتملا لاجمل او دھاولما

تاھوی و تھملا

[قەمدقەملا](#)

[قىس اس، ألا، تابل طتملا](#)

[تابل طتملا](#)

[قەمدختسەملا تانوکەملا](#)

[نیوکتلى](#)

[نیوکتلى قىرطن](#)

[دھاولما فيض مللى، وئىرانىس](#)

[ةكېشىلى، ئىطىطختىلى مىسىزلى](#)

[تانىوکتلى](#)

[قددعتملا تاھوی رانی سل](#)

[ةكېشىلى، ئىطىطختىلى مىسىزلى](#)

[تانىوکتلى](#)

[قەھىلى، انم، ق، قىحتلى](#)

[اهىالىص، او، ئاطخىلا، فاش، كتسا](#)

قەمدقەملا

ةي وهلا ىلإ ۋە دەنەتسەملا ئەكېشلى تامىخ نیوکت ئېفيك دەنەتسەملا اذە فەصىي ددعتملا لاجمل او دھاولما فيض ملا تاھوی رانی سل 2.0 (IBNS) ئىۋەلە.

قىس اس، ألا، تابل طتملا

تابل طتملا

ئەيلاتلا عيوض اوملاپ ئەفرۇم كىيىدىل نوکت نأب Cisco يىصوت:

- ئەيلەحەملا ئەقطەنملا ئەكېش ربع عسۇوتەملا ئەقاداصەملا لوكۇتورب (EAPoL)
- RADIUS لوكۇتورب
- Cisco Identity Services Engine، 2.0 رادىس إلە

قەمدختسەملا تانوکەملا

ئەيلاتلا ئەداملا تانوکەملا و جماربلا تارادىصى ىلإ دەنەتسەملا اذە يەف ئەدراؤلا تامولۇملا دەنەتسەت:

- Cisco Identity Service Engine، 2.0 Patch 2 رادىس إلە
- Windows 7 لىيغىشتىلا ماظننىب ئېاهەنلا ئەطقن
- Cisco Switch 3750X عىسۇ IOS 15.2(4)E1 لوحەملا
- Cisco 3850 عىسۇ 03.02.03.SE لوحەملا

• Cisco IP Phone 9971 تنرتن إلأ لوكوتورب فتاه

ةـصـاخـ ةـيـلـمـعـ ةـيـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاـشـنـاـ مـتـ
تنـاـكـ اـذـاـ (ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ
رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـلـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

نيـوـكـتـلـاـ

نيـوـكـتـلـاـ ةـيـرـظـانـ

حـاتـفـمـ ciscoـ ىـلـعـ بـوـلـسـأـ زـايـتـمـاـ يـفـ رـمـأـلـاـ ذـفـنـيـ نـأـ جـاتـحـتـ تـنـأـ ،ـIBNSـ 2.0ـ تـنـكـمـ

```
#authentication display new-style
```

حـضـوـمـ وـهـ اـمـكـ رـمـأـلـاـ مـادـخـتـسـابـ IBNSـ 2.0ـ لـ switchportـ نـيـوـكـتـبـ مـقـ

```
access-session host-mode {single-host | multi-domain | multi-auth}  
access-session port-control auto  
dot1x pae authenticator  
{mab}  
service-policy type control subscriber TEST
```

امـدـنـعـ .ـةـهـجـاـولـاـ ىـلـعـ MACـ (ـMABـ)ـ ةـقـدـاـصـمـ زـوـاجـتـ ،ـايـرـايـتـخـاـوـ ،ـةـقـدـاـصـمـ رـمـأـلـاـ هـذـهـ نـكـمـتـ
نـمـ ضـرـغـلـاـ Access-sessionـ.ـعـمـ أـدـبـتـ يـتـلـاـ رـمـأـلـاـ مـدـخـتـسـتـ كـنـإـفـ ،ـةـدـيـدـجـلـاـ ةـغـايـصـلـاـ مـدـخـتـسـتـ
اعـدـبـ)ـ ةـمـيـدـقـلـاـ ةـغـايـصـلـاـ مـدـخـتـسـتـ يـتـلـاـ رـمـأـلـلـلـ ةـبـسـنـلـابـ لـاحـلـاـ وـهـ اـمـكـ هـسـفـنـ وـهـ رـمـأـلـاـ هـذـهـ
يـتـلـاـ ةـسـاـيـسـلـاـ ةـطـيـرـخـ دـيـدـحـتـلـ ةـمـدـخـلـاـ ةـسـاـيـسـ قـيـبـطـتـ.ـ(ـةـقـدـاـصـمـلـلـ ةـيـسـاسـأـلـاـ ةـمـلـكـلـابـ
ةـهـجـاـولـلـ اـهـمـادـخـتـسـاـ نـكـمـيـ.

لـيـبـسـ ىـلـعـ .ـةـقـدـاـصـمـلـاـ عـاـنـثـأـ (ـقـدـصـمـلـاـ)ـ لـوـحـمـلـاـ كـوـلـسـ ةـرـوـكـذـمـلـاـ ةـسـاـيـسـلـاـ ةـطـيـرـخـ دـدـحـتـ
نيـوـكـتـ كـنـكـمـيـ ثـدـحـ لـكـلـ .ـةـقـدـاـصـمـلـاـ لـشـفـ ةـلـاحـ يـفـ ةـلـاحـ يـفـ ثـدـحـيـ نـأـ نـكـمـيـ اـمـ دـيـدـحـتـ كـنـكـمـيـ ،ـلـاـثـمـلـاـ
هـتـحـتـ اـهـنـيـوـكـتـ مـتـ يـتـلـاـ ةـئـفـلـاـ ةـطـيـرـخـ يـفـ قـبـاطـتـمـلـاـ ثـدـحـلـاـ عـونـىـلـاـ اـدـانـتـسـاـ ةـدـدـعـتـمـ تـاعـارـجـاـ
لـشـفـ ةـلـاحـ يـفـ .ـ(ـP~o~l~i~c~y~-~m~a~p~ T~E~S~T~4~)ـ حـضـوـمـ وـهـ اـمـكـ ةـمـئـاـقـلـاـ ىـلـعـ ةـرـظـانـ قـلـأـ ،ـكـلـذـ ىـلـعـ لـاـثـمـكـ وـهـ
عـاـجـإـلـاـ ذـيـفـنـتـ مـتـيـ ،ـجـهـنـلـاـ اـذـهـ قـيـبـطـتـ مـتـيـ ثـيـحـ نـرـاقـلـابـ ةـلـصـتـمـلـاـ ،ـةـيـاهـنـ ةـطـقـنـ
لـثـمـ تـاـئـفـلـلـ كـوـلـسـلـاـ سـفـنـ دـيـدـحـتـ يـفـ بـغـرـتـ تـنـكـ اـذـاـ DOT1X_FAILEDـ يـفـ فـرـعـمـلـاـ
ةـئـفـلـاـ ةـطـيـرـخـ -ـ ةـيـضـارـتـفـالـاـ ةـئـفـلـاـ مـادـخـتـسـاـ كـنـكـمـيـفـ ،ـ

امـئـادـ

```
policy-map type control subscriber TEST4  
(...)  
event authentication-failure match-first  
 10 class DOT1X_FAILED do-until-failure  
    10 terminate dot1x  
(...)
```

```
40 class always do-until-failure  
    10 terminate mab  
    20 terminate dot1x  
    30 authentication-restart 60  
(...)
```

عونلار يف مكحوللا كرتشم ىلع امياد 2.0 IBNS ملسا ختم يوتحي نأ بجي
وقيرطلا هذهب ۋەتاملا ثادحألا ۋەتاملا چۈچىمى:

```
Switch(config-event-control-policymap)#event ?
aaa-available           aaa-available event
absolute-timeout        absolute timeout event
agent-found             agent found event
authentication-failure authentication failure event
authentication-success authentication success event
authorization-failure authorization failure event
inactivity-timeout      inactivity timeout event
session-started         session started event
tag-added                tag to apply event
tag-removed              tag to remove event
template-activated       template activated event
template-activation-failed template activation failed event
template-deactivated     template deactivated event
template-deactivation-failed template deactivation failed event
timer-expiry             timer-expiry event
violation                session violation event
```

تايـفـلـا مـيـقـتـ ةـيـفـيـكـ دـيـدـحـتـ ةـيـنـاـكـمـاـ كـيـدـلـ ،ـدـحـلـاـ نـيـوـكـتـ يـفـ

```
Switch(config-event-control-policymap)#event authentication-failure ?  
  match-all    Evaluate all the classes  
  match-first  Evaluate the first class
```

ذيفنت ةيفيك نيعت انه كنأ نع امغر، ةيفلا طئارخ لثامن تارايخ فيرعت كنكامي كب ةصالحلا ةيفلا ققاباطم للاح يف تايملعمل:

```
Switch(config-class-control-policymap)#10 class always ?  
do-all Execute all the actions  
do-until-failure Execute actions until one of them fails  
do-until-success Execute actions until one of them is successful
```

هنكمي امك .ؤفلا ةطيرخ وه dot1x ديدجلا طمنلا يف نيوكتلا نم (يرايتحا) ريخألا عزلجا نيوكت .ةنيعم رورم ةكرح وأ كولس ةقباطمل همامدختسا متيلو ،مكحتلا اكترتشم ةباتك يأ وأ ،قباطتت نأ بجي طورشلا لك نأ نوييعت كنكمي .ؤفلا ةطيرخ ةلاح مييق تابلطتم

قباطت طورشلا نم دحأ ال وأ ،قباطت ينأ بجي طرش.

```
Switch(config)#class-map type control subscriber ?  
  match-all  TRUE if everything matches in the class-map  
  match-any  TRUE if anything matches in the class-map  
  match-none TRUE if nothing matches in the class-map
```

قداصم لشف قباطم يف odemdotx سملأ ةئفلأ ةطيرخ ىلع لاثم اذه

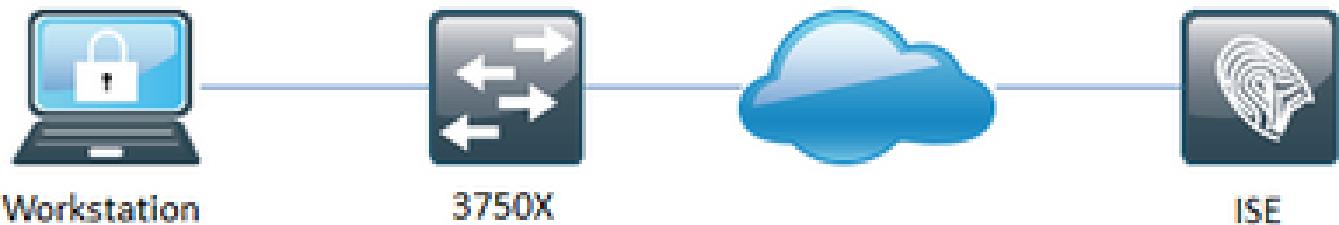
```
class-map type control subscriber match-all DOT1X_FAILED  
  match method dot1x  
  match result-type method dot1x authoritative
```

نيوكت ةفاضا ىلإ جاتحت ،ةمدخلاب لاق مادختسا دنع ابلاغ ،تاويرانيسلا ضعبل ةبسنلاب ضيوفتلاريفغل (CoA):

```
aaa server radius dynamic-author  
client 10.48.17.232 server-key cisco
```

دحاولا فيضممل ويرانيس

ةكبشلل يطيطلخلا مسرا



تانيوكتل

ىلع هرابتخا مت يذلا دحاولا فيضممل ويرانيسلا 802.1X رسبي ساسأ نيوكت مزلي جمانرب مادختساب ويرانيسلا رابتخا مت. Windows Catalyst 3750X IOS 15.2(4)E1 و Cisco AnyConnect Native Plus.

```
aaa new-model  
!  
aaa group server radius tests
```

```

server name RAD-1
!
aaa authentication dot1x default group tests
aaa authorization network default group tests
!
dot1x system-auth-control
!
policy-map type control subscriber TEST
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
!
interface GigabitEthernet1/0/21
  switchport access vlan 613
  switchport mode access
  access-session host-mode single-host
  access-session port-control auto
  dot1x pae authenticator
  service-policy type control subscriber TEST
!
radius server RAD-1
  address ipv4 10.48.17.232 auth-port 1812 acct-port 1813
  key cisco

```

ةددعتملا تالاجملاويرانيس

ةكبشلل يطيطختلما مسرلما



تانيوكتلما

ببساب IOS 03.02.03.SE مادختساب Catalyst 3850 ىلع تالاجملاددعتم ويرانيس رابتخا مت
تنرتن إلأ لوكوتورب فتاهل (PoE) تنبثي ٰكبش رباع ٰقاطلاب ديزتللا تابلطتم
Cisco IP Phone 9971).

```

aaa new-model
!
aaa group server radius tests
  server name RAD-1
!
aaa authentication dot1x default group tests
aaa authorization network default group tests
!
aaa server radius dynamic-author
  client 10.48.17.232 server-key cisco
!

```

```

dot1x system-auth-control
!
class-map type control subscriber match-all DOT1X
  match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
  match method dot1x
  match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
  match method dot1x
  match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
  match method mab
!
class-map type control subscriber match-all MAB_FAILED
  match method mab
  match result-type method mab authoritative
!
policy-map type control subscriber TEST4
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
      20 authenticate using mab priority 20
  event authentication-failure match-first
    10 class DOT1X_FAILED do-until-failure
      10 terminate dot1x
    20 class MAB_FAILED do-until-failure
      10 terminate mab
      20 authenticate using dot1x priority 10
    30 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
      20 authentication-restart 60
    40 class always do-until-failure
      10 terminate mab
      20 terminate dot1x
      30 authentication-restart 60
  event agent-found match-all
    10 class always do-until-failure
      10 terminate mab
      20 authenticate using dot1x priority 10
  event authentication-success match-all
    10 class always do-until-failure
      10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
!
interface GigabitEthernet1/0/1
  switchport access vlan 613
  switchport mode access
  switchport voice vlan 612
  access-session host-mode multi-domain
  access-session port-control auto
  mab
  dot1x pae authenticator
  spanning-tree portfast
  service-policy type control subscriber TEST4
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server vsa send cisco-nas-port
!
```

```
radius server RAD-1
address ipv4 10.48.17.232 auth-port 1812 acct-port 1813
key cisco
```

ةحصـلـا نـم قـقـحتـلـا

حيـصـلـكـشـبـنـيـوـكـتـلـاـلـمـعـدـيـكـأـتـلـمـسـقـلـاـاـذـهـمـدـخـتـسـاـ.

ـتـالـوـحـمـلـاـعـيـمـجـنـمـلـمـعـلـاـتـاسـلـجـدـرـسـلـرـمـأـلـاـاـذـهـمـدـخـتـسـاـ،ـقـقـحتـلـاـضـارـغـأـلـاـ.

```
show access-session
```

ـدـيـحـوـنـمـسـلـجـلـوـحـةـيـلـيـصـفـتـتـامـوـلـعـمـتـدـهـاـشـاضـيـأـعـيـطـتـسـيـتـنـأـ switchport:

```
show access-session interface [Gi 1/0/1] {detail}
```

اهـحـالـصـاـوـعـاطـخـأـلـاـفـاشـكـتـسـاـ

اهـحـالـصـاـوـنـيـوـكـتـلـاـعـاطـخـأـفـاشـكـتـسـاـاـهـمـادـخـتـسـاـاـكـنـكـمـيـتـامـوـلـعـمـمـسـقـلـاـاـذـهـرـفـوـيـ.

ـسـفـنـبـعـاطـخـأـلـاـحـيـحـصـتـنـيـكـمـتـكـنـكـمـيـ،ـاهـحـالـصـاـوـعـاطـخـأـلـاـ802.1Xـعـقـلـعـتـمـلـاـ802.1Xـعـاطـخـأـلـاـفـاشـكـتـسـاـاـلـاـ802.1Xـمـيـدـقـلـاـطـمـنـلـاـةـغـاـيـصـلـةـبـسـنـلـاـبـلـاحـلـاـوـهـاـمـكـةـقـيـرـطـلـاـ:

```
debug mab all
debug dot1x all
debug pre all*
```

*ـنـمـدـحـلـلـطـقـفـةـدـعـاـقـلـاـوـأـوـثـدـحـلـاـمـاـدـخـتـسـاـاـكـنـكـمـيـ،ـاـقـبـسـمـعـاطـخـأـلـاـحـيـحـصـتـلـاـيـرـاـيـتـخـاـIBNS 2.0ـبـةـلـصـلـاـتـاـذـتـامـوـلـعـمـلـاـىـلـعـجـاـرـخـاـلـاـ.

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).