

BGP رئاظن نيب MD5 ةقداصم نيوكت

تايوت حمل

[قم دق م ل](#)

[ةيساس ال تابل ط م ل](#)

[تابل ط م ل](#)

[ةمدخت س م ل تانوك م ل](#)

[تاجال ط ص ال](#)

[ةيساس ا تامول عم](#)

[نيوك ت ل](#)

[ةكبش ل ل ل طي ط خ ت ل م س ر ل](#)

[تانيوك ت ل](#)

[ءاطخ ال احي ص ت م ه ف](#)

[ةحص ل ل م ق ق ح ت ل](#)

[اهج الص او ءاطخ ال فاشك ت س ا](#)

[ةلص ت اذ تامول عم](#)

ةمدق م ل

نيب TCP لاصتا يلع (MD5) 5 ةلاس ر ل صخلم ةقداصم نيوكت ةيفي ك دن ت س م ل اذه فص ي BGP يراظن.

ةيساس ال تابل ط م ل

تابل ط م ل

دن ت س م ل اذهل ةصاخ تابل ط م ل دجوت ال.

ةمدخت س م ل تانوك م ل

ةني عم ةي دام تانوك م و ج م ا ر ب ت ا ر ا د ص ا يلع دن ت س م ل اذه ر ص ت ق ي ال.

3600 ةلس لس ل ا ت ا ه ج و م ن م ر م ال ت ا ج ر خ م ي ل ا دن ت س م ل اذه ي ف ة د ر ا و ل ا تامول عم ل دن ت س ت Cisco IOS® ن م 12.4(15)T14 ر ا د ص ا ل ل غ ش ت ي ت ل ا

ةصاخ ةي لم عم ةئي ب ي ف ة د و ج و م ل ا ة ز ه ج ال ن م دن ت س م ل اذه ي ف ة د ر ا و ل ا تامول عم ل اءاشن ا م ت ت ن ا ك اذ ا (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب دن ت س م ل اذه ي ف ة م د خ ت س م ل ا ة ز ه ج ال ع ي م ج ت ا د ب ر م ا ي ال ل م ت ح م ل ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

تاجال ط ص ال

[تاجال ط ص ا لوح تامول عم ل ن م د ي ز م يلع ل و ص ح ل ل ة ي ن ق ت ل ا Cisco تاجي م ل ت تاجال ط ص ا ع ج ا ر](#)

[تادنتس ملأ](#)

ةيساسأ تامولعم

م تي عطقم لك ةحص نم ققحتلا ينعي اذهو، BGP رئاظن ني ب MD5 ةقداصم نيوكت كنكمي ةم لك سفن مادختساب MD5 ةقداصم نيوكت ب جي. TCP رئاظن ني ب TCP لاصتا ىلع هلاسرا MD5، ةقداصم نيوكت دنع. امه ني ب لاصتالا ءارجا نكمي ال، ال او؛ BGP يراظن الك ىلع رورملا عطقم لك هنم ققحتلا او MD5 صخلم ءاشناب Cisco IOS جم انرب مايقي ف ببستت اهنا ف TCP لاصتا ىلع هلاسرا م تي.

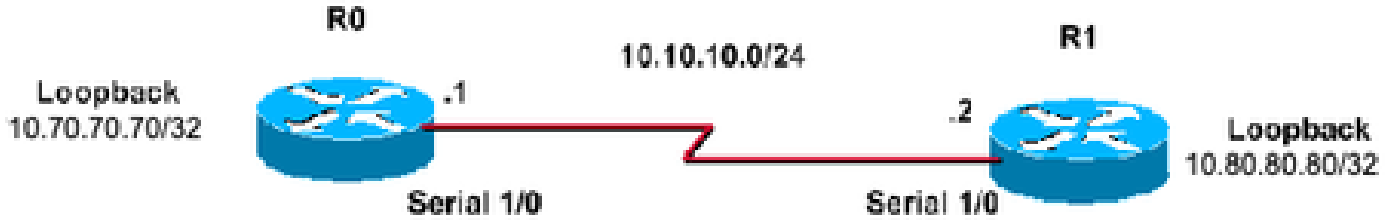
نيوكتلا

دنتس ملأ اذه في ةحضوملا تازيملأ نيوكت تامولعم مسقلا اذه في

✎ ىلع لوصحلل (Cisco نم رماوألأ رطس ةهجاو للجم) Cisco CLI Analyzer مدختسا: ةظالم Cisco مدختسم طقف عتم تي. مسقلا اذه في ةمدختس ملأ رماوألأ لوح تامولعملأ نم ديزم ةيلخادلا Cisco تامولعم و تاودأ ىلأ لوصولاب لجم ملأ.

ةكبش ل ل يطيختلا مسرلا

ي لالتلا ةكبشلا دادع | دنتس ملأ اذه مدختسي



تانويوكتلا

ةيلالتلا تانويوكتلا دنتس ملأ اذه مدختسي

0 هجوملا تانويوكت

```
<#root>
R0#
!
interface Loopback70
 ip address 10.70.70.70 255.255.255.255
!
interface Serial1/0
 ip address 10.10.10.1 255.255.255.0
 serial restart-delay 0
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
```

```
neighbor 10.80.80.80 remote-as 400

!--- iBGP Configuration using Loopback Address

neighbor 10.80.80.80 password cisco

!--- Invoke MD5 authentication on a TCP connection to a BGP peer

neighbor 10.80.80.80 update-source Loopback70
no auto-summary
!
ip route 10.80.80.80 255.255.255.255 10.10.10.2

!--- This static route ensures that the remote peer address used for peering is reachable.
```

1 هجومل تاني وكت

```
<#root>

R1#

!
interface Loopback80
 ip address 10.80.80.80 255.255.255.255
!
interface Serial1/0
 ip address 10.10.10.2 255.255.255.0
 serial restart-delay 0
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.70.70.70 remote-as 400

!--- iBGP Configuration using Loopback Address

neighbor 10.70.70.70 password cisco

!--- Invoke MD5 authentication on a TCP connection to a BGP peer

neighbor 10.70.70.70 update-source Loopback80
no auto-summary
!
ip route 10.70.70.70 255.255.255.255 10.10.10.1

!--- This static route ensures that the remote peer address used for peering is reachable.
```

ءاطخألآ حىحصت مهف

<#root>

R0#

```
clear ip bgp *
```

```
*Mar 1 01:02:17.523: %BGP-5-ADJCHANGE: neighbor 10.80.80.80 Down User reset
```

<#root>

R0#

```
debug ip bgp
```

```
BGP debugging is on for address family: IPv4 Unicast
```

```
*Mar 1 01:03:58.159: BGP: 10.80.80.80 open failed: Connection timed out;  
remote host not responding, open active delayed 1782ms (2000ms max, 28%  
jitter)
```

```
*Mar 1 01:03:58.415: %SYS-5-CONFIG_I: Configured from console by console
```

```
*Mar 1 01:03:59.943: BGP: 10.80.80.80 open active, local address 10.70.70.70
```

```
*Mar 1 01:04:00.039: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to  
10.70.70.70(64444)
```

```
*Mar 1 01:04:00.807: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(33358)  
to 10.70.70.70(179)
```

```
*Mar 1 01:04:01.991: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to  
10.70.70.70(64444)
```

```
*Mar 1 01:04:01.995: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to  
10.70.70.70(64444)
```

```
*Mar 1 01:04:05.995: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to  
10.70.70.70(64444)
```

```
*Mar 1 01:04:06.015: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to  
10.70.70.70(64444)
```

```
*Mar 1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to  
70. 70.70.70(64444)
```

```
*Mar 1 01:04:14.023: %TCP-6-BADAUTH: No MD5 digest from 10.80.80.80(179) to  
10.70.70.70(64444)
```

```
*Mar 1 01:04:29.947: BGP: 10.80.80.80 open failed: Connection timed out;  
remote host not responding, open active delayed 3932ms (4000ms max, 28%  
jitter)
```

```
*Mar 1 01:04:33.879: BGP: 10.80.80.80 open active, local address 10.70.70.70
```

```
*Mar 1 01:04:33.983: BGP: 10.80.80.80 went from Active to OpenSent
```

```
*Mar 1 01:04:33.983: BGP: 10.80.80.80 sending OPEN, version 4, my as: 400,  
hold time 180 seconds
```

```
*Mar 1 01:04:33.987: BGP: 10.80.80.80 send message type 1, length (incl.  
header ) 45
```

```
*Mar 1 01:04:34.091: BGP: 10.80.80.80 rcv message type 1, length (excl.  
header) 26
```

```
*Mar 1 01:04:34.091: BGP: 10.80.80.80 rcv OPEN, version 4, holdtime 180 seconds
```

```
*Mar 1 01:04:34.091: BGP: 10.80.80.80 rcv OPEN w/ OPTION parameter len: 16
```

```
*Mar 1 01:04:34.095: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2  
(Capability) len 6
```

```
*Mar 1 01:04:34.095: BGP: 10.80.80.80 OPEN has CAPABILITY code: 1, length 4
```

```
*Mar 1 01:04:34.095: BGP: 10.80.80.80 OPEN has MP_EXT CAP for afi/safi: 1/1
```

```
*Mar 1 01:04:34.095: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2
```

```
(Capability) len 2
*Mar 1 01:04:34.095: BGP: 10.80.80.80 OPEN has CAPABILITY code: 128, length 0
*Mar 1 01:04:34.099: BGP: 10.80.80.80 OPEN has ROUTE-REFRESH capability(old)
for all address-families
*Mar 1 01:04:34.099: BGP: 10.80.80.80 rcvd OPEN w/ optional parameter type 2
(Capability) len 2
*Mar 1 01:04:34.099: BGP: 10.80.80.80 OPEN has CAPABILITY code: 2, length 0
*Mar 1 01:04:34.099: BGP: 10.80.80.80 OPEN has ROUTE-REFRESH capability(new)
for all address-families
BGP: 10.80.80.80 rcvd OPEN w/ remote AS 400
*Mar 1 01:04:34.103: BGP: 10.80.80.80 went from OpenSent to OpenConfirm
*Mar 1 01:04:34.103: BGP: 10.80.80.80 went from OpenConfirm to Established
*Mar 1 01:04:34.103: %BGP-5-ADJCHANGE: neighbor 10.80.80.80 Up
```

تملك يدع ويوتحي ال رواجم ال هجوم ال نكلو، ناريجل اهنيوكت مت رورم ةملك هيدل هجوم ال ناك اذا
امهني ب BGP ةسلج عاشن ا تاهجوم ال ةلواجم اناثا هذه لثم ةلاسر ضرع متي، رورم

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local
router's IP address]:179
```

هذه لثم ةلاسر ضرع متي، اهنيوكت مت ةفلتخم رورم تاملك ني هجوم ال الكل ناك اذا، لثملاب

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local
router's IP address]:179
```

ةحصل ال نم ققحت ال

ححص لكشب نيوكت ال لمع ديكأتل مسقلا اذه مدختسا

- BGP ني مضت | ip bgp ناريج راهظا

```
<#root>
```

```
R0#
```

```
show ip bgp neighbors | include BGP
```

```
BGP neighbor is 10.80.80.80
```

```
,
```

```
remote AS 400
```

```
, internal link
```

```
BGP version 4, remote router ID 10.80.80.80
```

```
BGP state = Established
```

```
,  
up for 00:08:26  
BGP table version 1, neighbor version 1/0
```

- show ip bgp summary

```
<#root>  
R0#  
show ip bgp summary  
BGP router identifier 10.70.70.70, local AS number 400  
BGP table version is 1, main routing table version 1  
  
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd  
10.80.80.80 4 400 75 75 1 0 0 00:08:52 0
```

- show ip bgp summary

```
<#root>  
R1#  
show ip bgp summary  
BGP router identifier 10.80.80.80, local AS number 400  
BGP table version is 1, main routing table version 1  
  
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd  
10.70.70.70 4 400 76 76 1 0 0 00:09:27 0
```

اه حال صاوا عا طخال فاشك ت سا

ن يوك ت ل اذهل عا طغم اه حال صاوا عا طخال فاشك ت سا لوح تام ول عم ي ا ل ا ح د جوت ال

ة ل ص تا ذ تام ول عم

- [BGP رم او اع جرم: Cisco نم IOS ما ظن رب ع IP لوك وت ورب ه ي جوت](#)
- [IP ه ي جوت معد ة ح فص](#)
- [Cisco نم تال ي زنت ل او ي ن فل ا مع دل ا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچال مچرئى. ةصاغل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لاعل او
ىل اءمءاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيل وئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزلچنل دن تسمل