

إلى (ACL) لوصول في مكحتل مئوق نيوكت عئاش لكشب ةمدختسم ال IP

تايوت حمل

[ةمدق مل](#)

[ةيساس الابل طت مل](#)

[تابل طت مل](#)

[ةمدختسم مل تانوك مل](#)

[ةيساس ا تامول عم](#)

[نيوكت مل](#)

[ةكبش لل ال لوصول ولابل Select Host ةادل حمل مل](#)

[ةكبش لل ال لوصول ولابل Select Host ةادل لوصول و صفر](#)

[ةبرولحت مل IP نيوانع نم قاطن ال لوصول ولابل حمل مل](#)

[\(23 ذف نمل، Telnet \(TCP\) رورم صفر](#)

[TCP ةسلج يف ةدبلابل ةيلخا دلل تاكلبش لل لوصول ولابل حمل مل](#)

[\(21 ذف نمل، FTP \(TCP\) رورم صفر](#)

[\(ةطش نمل، FTP رورم حمل مل\)](#)

[\(ةطش نمل، رورم حمل مل\)](#)

[\(ICMP\) لاصل تالابل تخا رماو ابل حمل مل](#)

[FTP و POP3 و Mail و Telnet و HTTP حمل مل](#)

[DNS حمل مل](#)

[هيجوت مل تاثيري دحتب حمل مل](#)

[\(ACL\) لوصول ولابل مكحتل ةمئوق ال ابل نمل رورم مل اعاطخ ا حيرصت](#)

[MAC ناونع ةيفصت](#)

[ةحص لل نم ققحت مل](#)

[اهجال ص او اعاطخ ال فاشكت سا](#)

[ةلص تاذا تامول عم](#)

ةمدق مل

ةمدختسم ال IP إلى (ACLs) لوصول في مكحتل مئوق تانوكت لاجذومن دننتم مل اذه فصي
IP مزح ةيفصت ب موقت يتل او، عئاش لكشب

ةيساس الابل طت مل

تابل طت مل

نيوكت مل اذه ةبرجت لبق تابل طت مل هذه ةيبلت نم دكأت:

- IP ةنونعل يساس ال مه لل

يُسمح لوصول دجلا ني مدختس ملل ةي عرف تاك بش يلا مي س ق ت ل او IP ةن ونع يلا ع ج را ةي فاضا تام ول عم .

ةمدختس ملل تانوك ملل

ةني عم ةي دام تانوك م و ج مار ب تار ادصا يلع دن ت س ملل اذ ه ر ص ت ق ي ال .

ةصاخ ةي لم عم ةئي ب ي ف ةدو ج و ملل ةزه ج ا ل ا ن م دن ت س ملل اذ ه ي ف ةدرا و ل ا تام و ل عم ل ا ع ا ش ن ا م ت ت ن ا ك ا ذ ا . (يضا ر ت ف ا) ح و س م م ن ي و ك ت ب دن ت س ملل اذ ه ي ف ةمدختس ملل ةزه ج ا ل ا ع ي م ج ت ا د ب ر م ا ي ا ل ل م ت ح م ل ا 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 .

ةي س ا س ا تام و ل عم

يلا دن ت س ت IP يلا ل و ص و ل ا ي ف م ك ح ت ل ا م ئ ا و ق :

- ر د ص م ل ا ن ا و ن ع
- ة ه ج و ل ا ن ا و ن ع
- ة م ز ح ل ا ع و ن
- ر ص ا ن ع ل ا ه ذ ه ن م ة ع و م ج م ي ا

ن ا ك ا ذ ا ا م ي ف (ACLs) ة ك ب ش ل ا ي ف م ك ح ت ل ا م ئ ا و ق م ك ح ت ت ، ة ك ب ش ل ا ر و ر م ة ك ر ح ة ي ف ص ت ل ة م ز ح ل ك ك ي د ل ة ج و م ل ا ص ح ف ي . ة ج و م ل ا ة ه ج ا و ي ف ا ه ر ط ح و ا ة ج و م ل ا م ز ح ل ل ه ي ج و ت ة د ا ع ا م ت ي س ن م ض ا ه د د ح ت ي ت ل ا ر ي ي ا ع م ل ا ي ل ع ا ن ا ب ا ه ط ا ق س ا و ا ة م ز ح ل ا ه ي ج و ت ة د ا ع ا م ت ي س ن ا ك ا ذ ا ا م د ي د ح ت ل ي ل ع (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ر ي ي ا ع م ل م ت ش ت و . (ACL) ل و ص و ل ا ب م ك ح ت ل ا ة م ئ ا ق :

- ر د ص م ل ل ر و ر م ل ا ة ك ر ح ن ا و ن ع
- ة ه ج و ل ل ر و ر م ل ا ة ك ر ح ن ا و ن ع
- ا ي ل ع ل ا ة ق ب ط ل ا ل و ك و ت و ر ب

ةدرا و ل ا ة ل ث م ا ل ا ح ص و ت ا م ك (ACL) ل و ص و ل ا ي ف م ك ح ت ة م ئ ا ق ع ا ش ن ا ل ة ي ل ا ت ل ا ت ا و ط خ ل ل م ك ا ف دن ت س ملل اذ ه ي ف :

1. (ACL) ل و ص و ل ا ي ف م ك ح ت ة م ئ ا ق ع ا ش ن ا .
2. ة ه ج ا و ي ل ع (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ق ي ب ط ت .

ن م ة ي ل س ل س ت ة ع و م ج م ن ع ة ر ا ب ع (IP) ت ن ر ت ن ا ل ا ل و ك و ت و ر ب ل (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق م ز ح ل ا ر ا ب ت خ ا ب ة ج و م ل ا م و ق ي . IP ة م ز ح ي ل ع ا ه ق ي ب ط ت م ت ي ي ت ل ا ض ف ر ل ا و ح ا م س ل ا ط و ر ش ل ك ي ف ة د ح ا و ة م ز ح (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ي ف ةدرا و ل ا ط و ر ش ل ا ر ف و ت ن م ق ق ح ت ل ل ة ر م .

ن ا ل ا ر ط ن . ا ه ض ف ر ي و ا ة م ز ح ل ا ل ب ق ي Cisco IOS® Software ج م ا ن ر ب ن ا ك ا ذ ا ا م ي ل و ا ل ا ة ق ب ا ط م ل ا د د ح ت ب ي ت ر ت ن ا ف ، ي ل و ا ل ا ة ق ب ا ط م ل ا د ع ب ط و ر ش ل ا ر ا ب ت خ ا ن ع ف ق و ت ي Cisco IOS software ج م ا ن ر ب ة م ز ح ل ا ة ج و م ل ا ض ف ر ي ، ط و ر ش ل ا ن م ي ا ق ب ا ط ا ت م د ع ة ل ا ح ي ف . ة ي م ه ا ل ا غ ل ا ب ا ر م ا د ع ي ط و ر ش ل ا ل . ل ك ل ا ض ف ر ب ة ي ن م ض ة ل م ج ب ب س ب .

ن ك م ي ي ت ل ا (IP) ت ن ر ت ن ا ل ا ل و ك و ت و ر ب ل (ACLs) ل و ص و ل ا ي ف م ك ح ت ل ا م ئ ا و ق ي ل ع ة ل ث م ا ه ذ ه Cisco IOS Software ج م ا ن ر ب ي ف ا ه ن ي و ك ت :

- سياسة الوصول في مكدتال مئوق
- عسومال لوصول في مكدتال مئوق
- (حاتفملاو لقلال) ةكيمانيدلا (ACLs) لوصول في مكدتال مئوق
- IP قفو ةامسُملا (ACLs) لوصول في مكدتال مئوق
- ةيسكعلا (ACL) لوصول في مكدتال مئوق
- تقولا تاقاطن مدختست يتلا تقولا لىل ةدنتسُملا (ACLs) لوصول في مكدتال مئوق
- اهيلع قيلعتلا مت يتلا IP لىل (ACL) لوصول في مكدتال مئوق تالخدإ
- قايسل لىل ةدنتسُملا (ACLs) لوصول في مكدتال مئوق
- ةقداصملا لىل
- Turbo نم (ACL) لوصول في مكدتال مئوق
- تقولا لىل ةدنتسُملا ةزوملا (ACL) لوصول في مكدتال مئوق

ةيسايقلال مادختسالال ةعئاش (ACLs) لوصول في مكدتال مئوق ضعب دنتسُملا اذه شقانيل وحتامولعملال نم ديزم لىل لوصولل [IP لىل لوصول مئوق نيوكت](#) لىل عجرا. ةسوملاو Cisco IOS جمانرب في ةمومدملا (ACLs) لوصول في مكدتال مئوق نم ةفلتخملال عاونالال اهررتو (ACLs) لوصول في مكدتال مئوق نيوكت ةيفيكيو Software.

access-list access-list-number {permit|deny} {host|source source-wildcard|any} (ACL) لوصول في مكدتال مئوق لرمال ةغايص قيسنت

يتلا نيوانعلا باب ردصملا IP مزح ناووع ةيسايقلال (ACLs) لوصول في مكدتال مئوق نراقت رورملا ةكرح في مكدتال مئوق لىل (ACL) لوصول في مكدتال مئوق نيوكت مت

نيوانعلا باب ةهجولال او ردصملا IP مزح نيوانع ةسوملا (ACL) لوصول في مكدتال مئوق نراقت رورملا ةكرح في مكدتال مئوق لىل (ACL) لوصول في مكدتال مئوق نيوكت مت يتلا اهنوكت متي ناو ةقد رثكأ ةسوملا (ACLs) لوصول في مكدتال مئوق لعج كنكمي امك لثم ريياعم بسح رورملا ةكرح ةيفصتل لصفأ ةجرب:

- لوكوتوربلا
- ذفانملا ماقرا
- (DSCP) ةزيامتلا تامدخلال دوك ةطقن ةميقي
- ةيقبسألا ةميقي
- (SYN) يلسلستلال مقررلا نمازتلا تب ةدحو ةلاح

يه ةسوملا (ACLs) لوصول في مكدتال مئوق لرمال ةغايص تاقيسنت

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination destination-wildcard
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

(ICMP) تنرتنلال في مكدتال لئاسر لوكوتورب

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard destination destination-wildcard
[[icmp-type] [icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

(TCP) ل قنلا في مكحتلا لوكوتورب

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard [operator
[established] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

(UDP) مدختسمل تانايب ططخم لوكوتورب

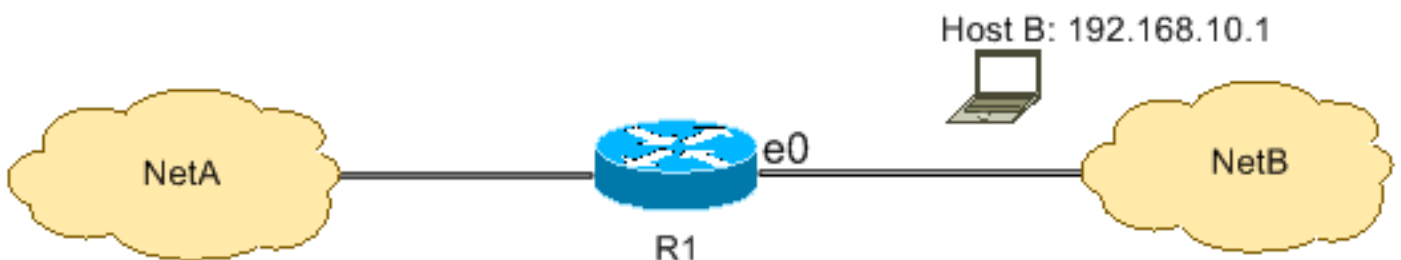
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

نيوكتلا

(IP) تترت نإلا لوكوتورب (ACLs) لوصول في مكحتلا مئوق هذه نيوكتلا ةلثمأ مدختست أعويش رثكألا

ةكبشلا إلا لوصولاب Select Host ةادل حامسلا

عيجب حامسلا متي. ةكبشلا إلا لوصول نذال حنم مت دحم فيضم نأ ةروصلا هذه حضوت رورملا تاكرح عيجب ضم فر متي و، NetA إلا ةهجت مل او B فيضملا نم ةرداصل رورملا تاكرح NetA إلا ةهجت مل او NetB نم ةرداصل إرخألا



اذه حضوي. فيضملا إلا لوصولا ةينام ةكبشلا حنم مت فيك R1 لودج في جرخملا حضوي نأ جرخملا


- إلا Ethernet 0 ةهجاو لال خ نم IP 192.168.10.1 ناو نع ب فيضملا ل طقف حمسي نيوكتلا R1.


- NetA. بـ ةصاخ ل IP تامدخ ىل لوصول قح فيضم ل اذه كلت مي
- NetA. ىل لوصول قح NetB في رخآ فيضم كلت مي ال
- (ACL). لوصول في مكحت ل ةمئاق في ضفرة رابع يا نيوكت متي مل

لوصول في مكحت ةمئاق لك ةيانهن في لك لال ضفر ب ةي نمض ةلمج دجوت ،يضارتفا لكشب
 حيرص لكشب هرورم ب حامس لال متي مل عيش يا ضفر متي (ACL).

R1

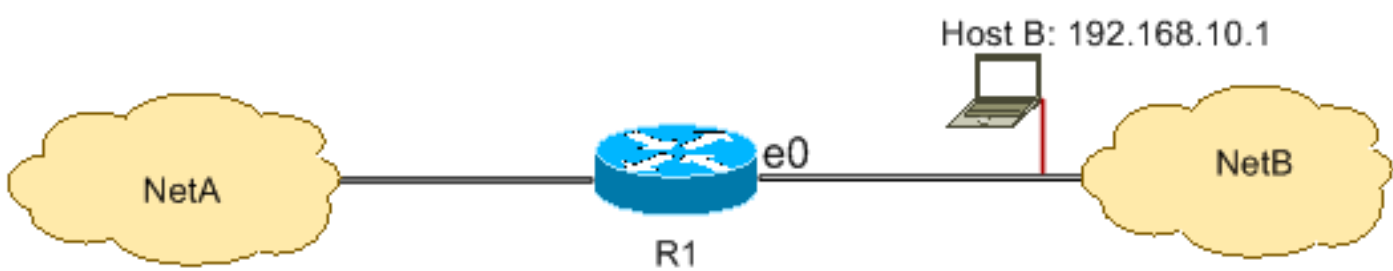
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

 NetA، ىل NetB نم IP مزح ةي فصتب لوصول في مكحت ل ةمئاق موقت :ةظالم
 نم ةدمت سمل مزح لال ب حمسي لازي ال B. فيضم لال نم ةدمت سمل مزح لال اناثت سب
 ل NetA، ىل B فيضم لال

 ةقيرط وه 192.168.10.1 0.0.0.0 لوصول ةمئاق ل (ACL) لوصول ةمئاق حيرصت :ةظالم
 اهسفن ةدعاق لال نيوكت ل رخآ

ةكبش لال ىل Select Host ةادا لوصول و ضفر

NetA، ىل ةهجوم لال B فيضم لال نم ةدمت سمل رورم لال ةكح ضفر متي هنا ةروصل لال هذه حضوت
 NetA، ىل لوصول لال NetB نم ىرخآ لال رورم لال تاكح عي مجب حامس لال متي امن بي



R1 ىل Ethernet 0 لال نم 192.168.10.1/32 فيضم لال نم مزح لال عي مجب نيوكت لال اذه ضفري
 لكشب حامس لال access list 1 permit any رم الال مادختسا لكي لع بجي . رخآ عيش لكب حمسي و
 في مكحت ةمئاق لك عم لك لال ضفر ب ةي نمض ةلمج دجوت ب بسب رخآ عيش لكب حيرص
 لوصول (ACL).

R1

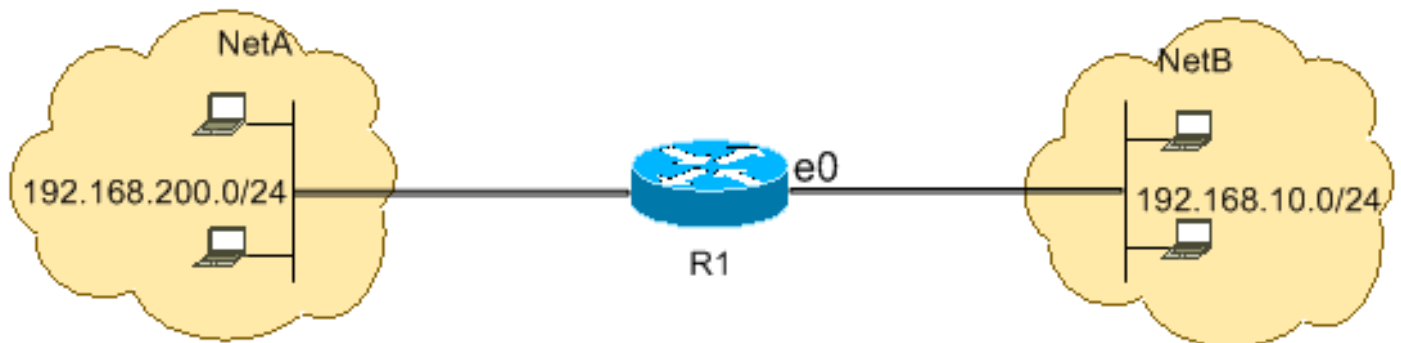
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

✎ لوصول في مكحلتا عمئاق لئغشتل ةيمهألا غلاب ارمأ تانايبلا بيترت دعئ: ةظالم لك قباطي لوألا رطسلا نإف، رمألا اذره ظئ امك، تالاخلال بيترت سكع مت اذئ (ACL). رظح في (ACL) لوصول في مكحلتا عمئاق لشفت، كلذل. ةمزحلل ردصم ناوع NetA. لوصول نم 192.168.10.1/32 فيضملا

```
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

ةرواجتملا IP نيوانع نم قاطن لوصول حامسلا

ةكبشلا ناوع تاذ NetB في ةفيضملا ةزهألا عئمچ نأ ةروصولا هذو حضوت NetA. في 192.168.200.0/24 ةكبشلا لصلت نأ نكمئ



في ردصم ناوع نمضتئ في ذللا IP ناوع لعل يوتحت يتلا IP مزحل نيوكتلا اذو حئتي لوصول ةيناملا 192.168.200.0/24 ةكبشلا في ةهجو ناوعو 192.168.10.0/24 ةكبشلا يتلاو (ACL) لوصول في مكحلتا عمئاق ةيانه في لكلا ضفرب ةئنمض ةلمچ كانه NetA. R1 لعل ةدراو Ethernet 0 رب ع رورم ةكرح لك ضفرت

R1

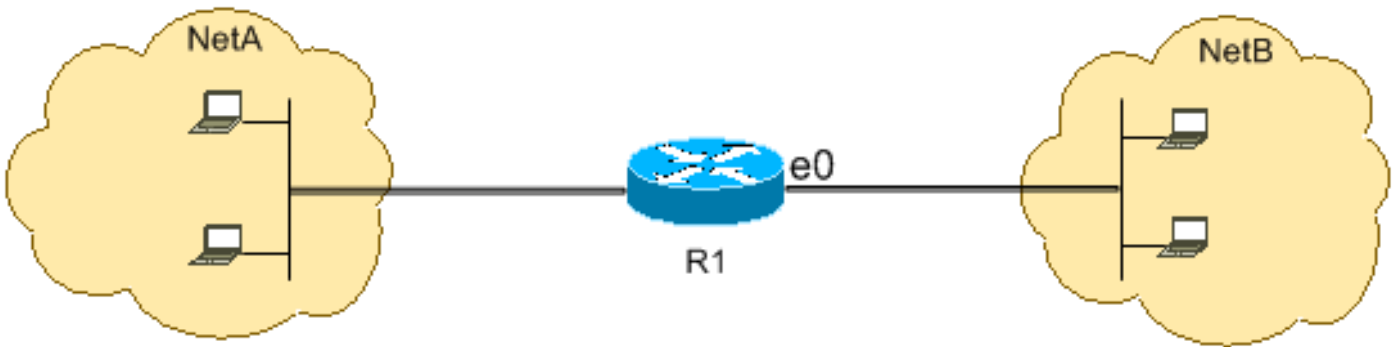
```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

✎ ملاحظة: في هذا المثال، سيتم تطبيق قائمة الوصول 101 على عنوان IP 192.168.10.0.0.255 192.168.200.0.0.255، وهو عنوان الشبكة 192.168.10.0. سيتم تطبيق قائمة الوصول 102 على عنوان IP 0.0.0.255، وهو عنوان الشبكة 0.0.0.255. في هذا المثال، سيتم تطبيق قائمة الوصول (ACL) لوصول في مكدس التوجيه من أجل منع الوصول من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24. سيتم تطبيق قائمة الوصول ACL لوصول في مكدس التوجيه من الشبكة 192.168.200.0/24 إلى الشبكة 192.168.10.0/24.

تماماً مثل ما نرى في المثال السابق، فإننا نحتاج إلى إجراء مكدس التوجيه من أجل منع الوصول من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24. سيتم تطبيق قائمة الوصول (ACLs) لوصول في مكدس التوجيه من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24.

رسم تخطيطي لـ Telnet (TCP، 23) في مكدس التوجيه

عند إجراء مكدس التوجيه في مكدس التوجيه، فإننا نحتاج إلى إجراء مكدس التوجيه من أجل منع الوصول من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24. سيتم تطبيق قائمة الوصول (ACLs) لوصول في مكدس التوجيه من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24.



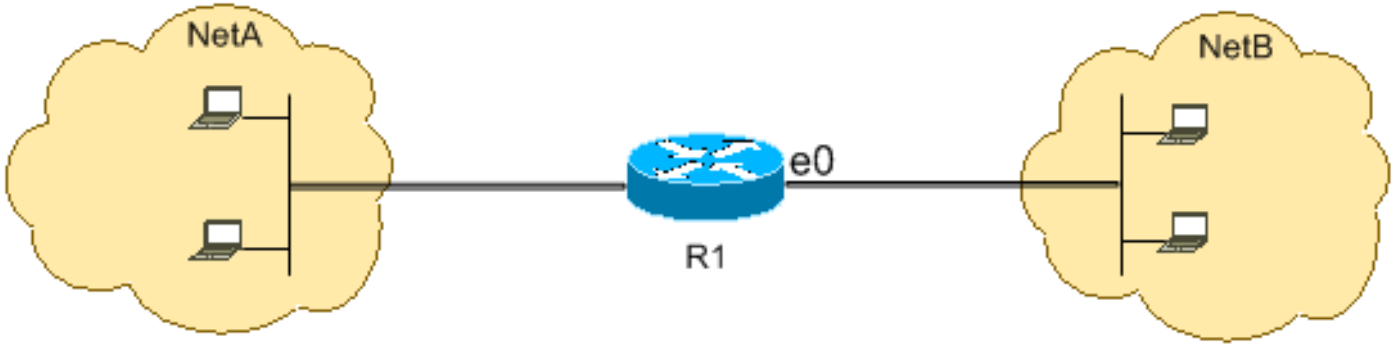
رسم تخطيطي لـ Telnet (TCP، 23) في مكدس التوجيه. هذا هو الرسم التخطيطي الذي نحتاجه لمنع الوصول من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24. سيتم تطبيق قائمة الوصول (ACLs) لوصول في مكدس التوجيه من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

رسم تخطيطي لـ Telnet (TCP، 23) في مكدس التوجيه

رسم تخطيطي لـ Telnet (TCP، 23) في مكدس التوجيه. هذا هو الرسم التخطيطي الذي نحتاجه لمنع الوصول من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24. سيتم تطبيق قائمة الوصول (ACLs) لوصول في مكدس التوجيه من الشبكة 192.168.10.0/24 إلى الشبكة 192.168.200.0/24.



وهذا هو الـ ACL (Access Control List) لوصولها في مكدتها عملاق نم ضرغها نإ:

- فيضمها زهجال اهسي سأتو TCP سولج ادبب NetA في فيضمها زهجال حامسها في NetB.
- فيضمها زهجال هجت TCP سولج عاشنإو ادب نم NetB في فيضمها زهجال عنم NetA.

امدنع R1 هجومها لعل هدرالها Ethernet 0 ههجال لالخ تاناها لاطخم رورمب نيوكتها اذه حمسي تاناها لاطخم كلمي:

- TCP لمع سولج لريشت) اهب فرتعمها RESET (RST) وأ ACK) تب تادحو هومجم
- 1023 نم ربكأ ههجو ذفنم هميقي

R1

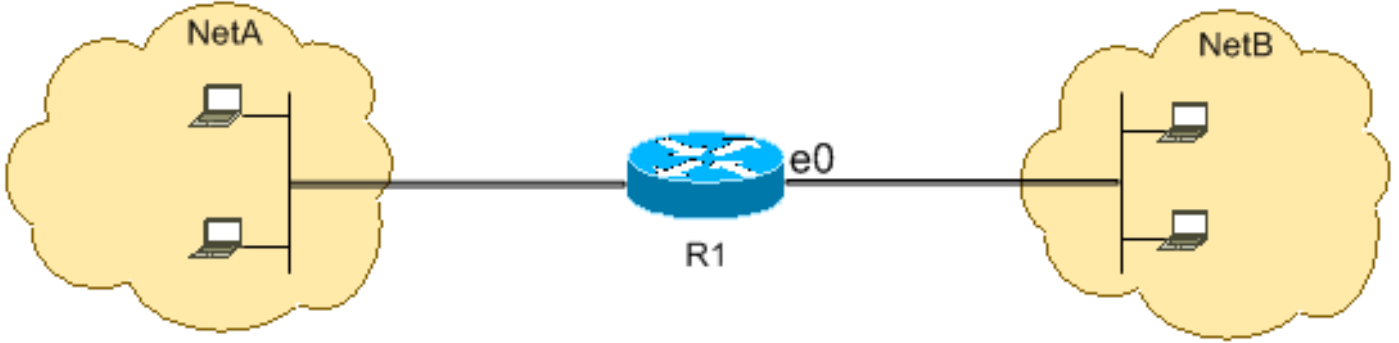
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

اطخمها نإ 1023 نم لقا مميقي مدختست IP تامدخ هفورعمها ذفانمها مظعم نأل ارظنو هسأوب هضفر متهي هنيعم ريغ ACK/RST تب هدحو وأ 1023 نم لقا ههجو ذفنمب تاناها لاصتا ههتت NetB نم فيضم مومي امدنع، كذل 102 (ACL) لوصولها في مكدتها عملاق نم لقا مقر ذفنم (set تب SYN/RST) طبر ادب/هنمزم نودب) TCP همزح لو لسريو TCP NetA نم اهؤدب متهي ل TCP تاسلجب حامسها متهي. TCP سولج لشفي وهضفر متهي، 1023 مميقي مدختست و مزحها اعجال ACK/RST تب تادحو هومجم لعل يوتحت ههنا NetB لعل ههجتملهاو 1023 نم ربكأ ذفنم.

ذفانمها لعل ههنا عملاق لعل لوصولها RFC 1700 لعل اعجرا.

(21 ذفنمها، TCP) FTP رورمب هضفر

رورمها هكرح (20 ذفنمها) FTP و (21، port) FTP تاناها هضفر متهي ههنا هروصلها ههنا هضوت لعلها IP رورم هكرح هيمجب حامسها متهي امنها، NetA لعل ههجومها NetB نم هدمصمها.



21 ذفنم لى لى ةهجوم لى TCP رورم ةكرح ضفر م تي . 20 ذفنم لى او 21 ذفنم لى FTP مدختسي
 حيرص لكش ب رخ آ عيش لك ب حامس لى م تي و 20 ذفنم لى او

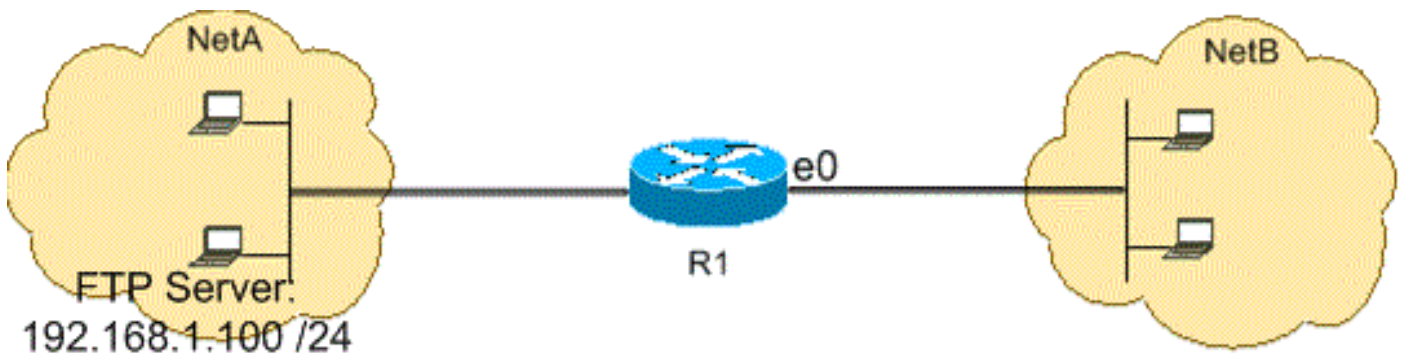
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

(ةطشن لى FTP) رورم ب حامس لى

لماخ و طشن لى مسم تحت ني فل تخم ني عضو ي ف FTP لمعي نأ نكمي

20 ذفنم لى او ، مكحت لى لى 21 ذفنم لى FTP مداخ مدختسي ، طشن لى لى عضو لى ف FTP لمعي ام دنع
 رورم ةكرح ب حومسم هنأ ةروصل لى هذه حضوت . NetA ي ف (192.168.1.100) FTP مداخ عقي . تاناي ب لى
 FTP مداخ لى لى NetB نم اههيجوت م تي ي تلى لى (20 ذفنم لى) FTP و (TCP، port 21) FTP تاناي ب
 لى رخ لى IP رورم ةكرح عي م ج ضفر م تي ام ني ب ، (192.168.1.100)



R1

```
hostname R1
!
interface ethernet0
```

```

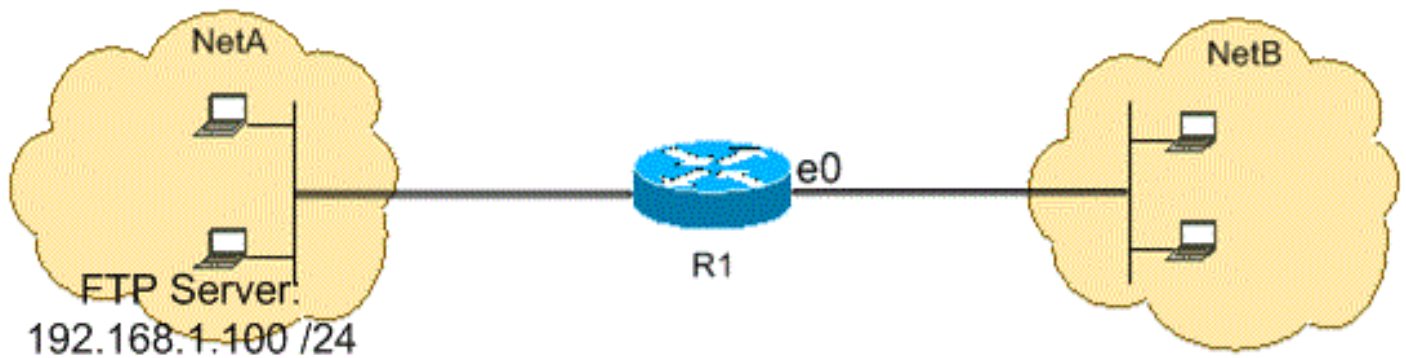
ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any

```

ةطيشن لال ريغ FTP) FTP رورمب حامس لال

لماخو طشن مسم تحت ني فل تخم ني عضو في FTP لمعي نا نكمي.

ذفانم لاولم كحت لل 21 ذفانم لال FTP مداخ مدختسي، لماخال عضو لال في FTP لمعي ام دنع في (192.168.1.100) FTP مداخ عقي. تانايب لل 1024 يواست يتلا ونا نم ربك الال اكي ماني دلال ذفانم لال) FTP تانايب و (TCP، port 21) رورم ةكرب حومسم هنا ةروصلال هذه حضوت NetA. ام ني ب، (192.168.1.100) FTP مداخ لال NetB نم اههيجوت متي يتلا (1024 يواست ونا نم ربك الال يخال IP رورم ةكرب عي مجض فر متي.



R1

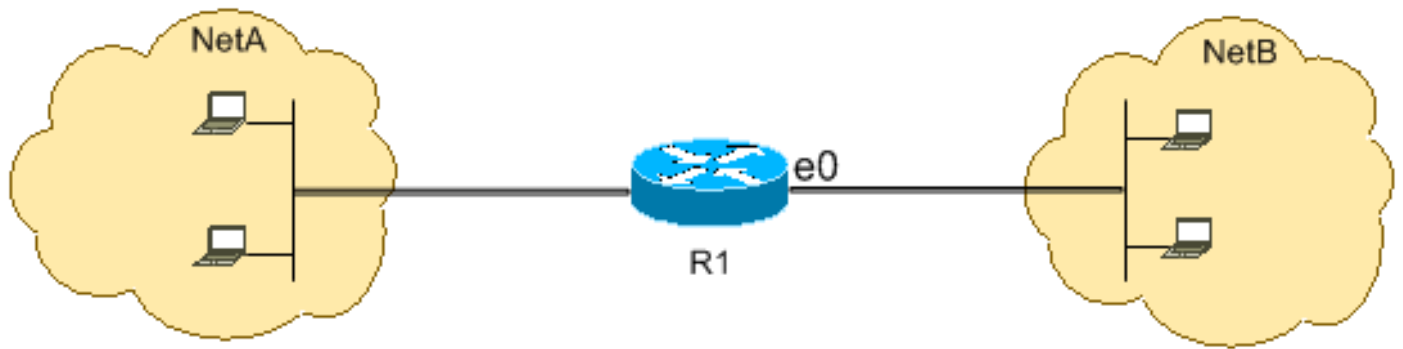
```

hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established

```

لالصتالال رابتخا رماو اب حامس لال (ICMP)

ضفر متي و NetB، لى هجوم ال NetA نم يردصم ال ICMP ب حامس ال متي هنأ ةروصل ال هذه حضوت
 NetA. لى هجوم ال NetB نم ةيردصم ال لاصلت ال تارابتخا



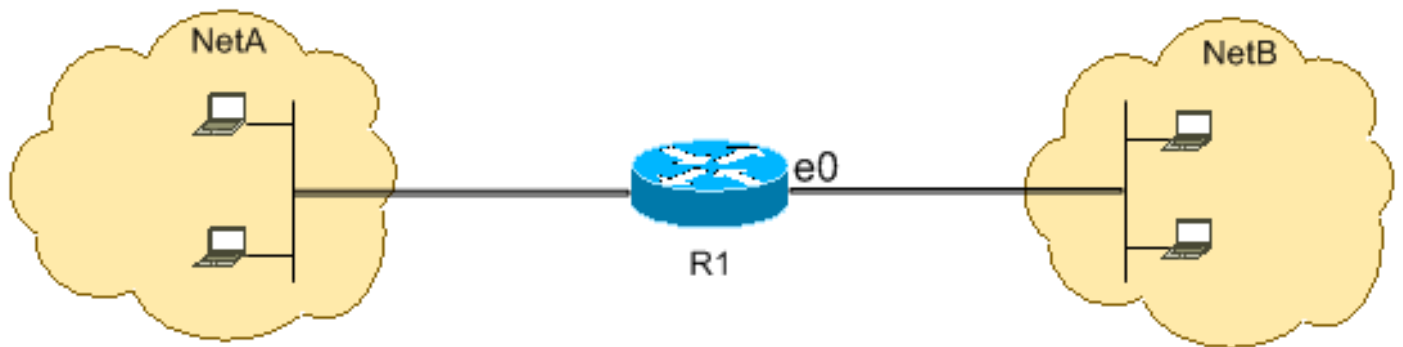
لعل لوخذلاب (لاصلت ال رابتخا رمأ ةباجتسا) دادترال ال ةباجتسا مزحل طوق نيوكت ال اذه حمسي
 ةصاخ ال ICMP مزح عي مج رطحي نيوكت ال نإف، كلذ عم و NetA هاجت اب NetB نم Ethernet 0 هجاو
 ،كلذل لى اهيجوت و NetB ي لاصلت ال رابتخا رماو ا رادصا متي ام دنع دادترال بلطب
 ، NetB ي ةفيضم ال ةزهجال لاصلت ال رابتخا رمأ رادصا NetA ي ةفيضم ال ةزهجال نكمي
 ي ةفيضم ال ةزهجال لاصلت ال رابتخا رما رادصا NetB ي ةفيضم ال ةزهجال نكمي ال نكلو
 NetA.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

FTP و POP3 و Mail و Telnet و HTTP - ب حامس ال

ت Simple Mail Transfer Protocol و telnet و HTTP رورم ةكرح ب طوق حومسم هنأ ةروصل ال هذه حضوت
 NetA. لى هجوم ال NetB نم ةدمتسم ال رورم ال ةكرح ةيقب ضفر متي و، FTP و POP3 و SMTP (SMTP)



WWW تانايب قباطت ي ال ةهجال ذفنم مي ق تاذ TCP رورم ةكرح ب نيوكت ال اذه حمسي
 (ذفنم ال) FTP و (110 ذفنم ال) POP3 و (25 ذفنم ال) SMTP و (23 ذفنم ال) Telnet و (80 ذفنم ال)
 لوصول ي فم كحت ال ةمئاق ةهان ي ف ينمض ضفر ةلمج نأ طحال. (20 ذفنم ال) FTP و (21

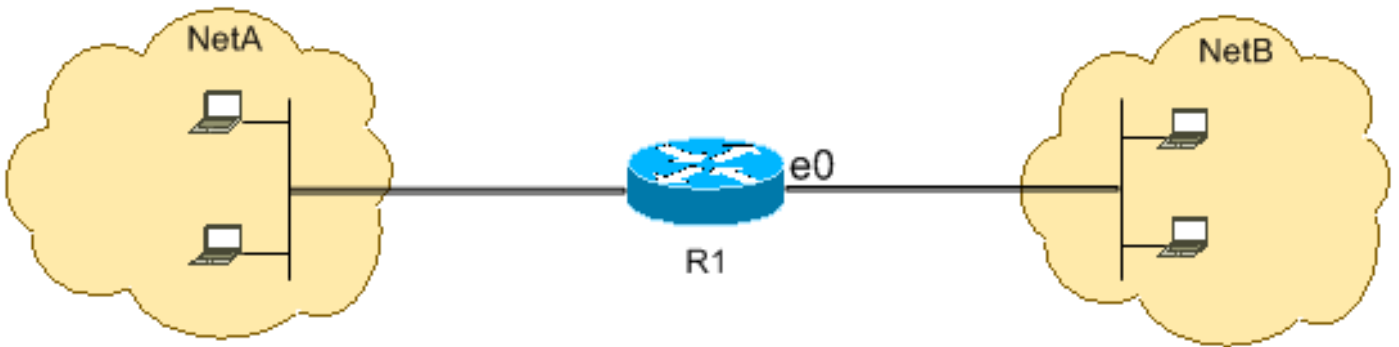
حامسلا تارابع عم قفاوتت ال يتلا، ىرخألا رورملا تاكرح عيمج ضفرت ACL

R1

```
hostname R1
!  
interface ethernet0  
 ip access-group 102 in  
!  
access-list 102 permit tcp any any eq www  
access-list 102 permit tcp any any eq telnet  
access-list 102 permit tcp any any eq smtp  
access-list 102 permit tcp any any eq pop3  
access-list 102 permit tcp any any eq 21  
access-list 102 permit tcp any any eq 20
```

DNS - حامسلا

ضفرت متيو، طقف (DNS) لاجملا مسا ماظن رورم ةكرح حامسلا متي هنا ةروصولا هذه حضوت
NetA. لىل ةهجوملا NetB نم اهليلع لوصحلا مت يتلا رورملا ةكرح ةقبق



ضفرلا طارش ضفري. 53 ةهجولا ذف نم ةميق عم TCP رورم ةكرح نيوكتلا اذه حمسي
يتلاو، ىرخألا رورملا تاكرح عيمج (ACL) لوصولا يف مكحتلا ةمئاق ةياهن يف لكل ينمضلا
صىخرتلا طورش قباطت ال

R1

```
hostname R1
!  
interface ethernet0  
 ip access-group 102 in  
!  
access-list 102 permit udp any any eq domain  
access-list 102 permit udp any eq domain any  
access-list 102 permit tcp any any eq domain  
access-list 102 permit tcp any eq domain any
```

هيجوتال تاتي دحتب حامسلا

ةيفصت مدع نم دكأت ،ةهجاو ىلع ةنمضملا (ACL) لوصولا يف مكحتلا ةمئاق قيبطت دنع ةمئاقلا هذه نم ةلصلا تاذا (ACL) لوصولا يف مكحتلا ةمئاق مدختسا .هيجوتال تاتي دحتب هيجوتال لوكوتورب مزحب حامسلا

(RIP): هيجوتال تامولعم لوكوتوربب حامسلا لجأل رمألا اذه لخدا

```
access-list 102 permit udp any any eq rip
```

(IGRP): ةلخادلا ةرأبعلا هيجوت لوكوتوربب حامسلا لجأل رمألا اذه لخدا

```
access-list 102 permit igmp any any
```

(EIGRP): نسحُملا IGRP لوكوتوربب حامسلا لجأل رمألا اذه لخدا

```
access-list 102 permit eigrp any any
```

(OSPF): أل وأ راسم رصقأ حتف لوكوتوربب حامسلا لجأل رمألا اذه لخدا

```
access-list 102 permit ospf any any
```

(BGP): دودحلا ةرأبع لوكوتوربب حامسلا لجأل رمألا اذه لخدا

```
<#root>
```

```
access-list 102 permit tcp any any eq
```

```
179
```

```
access-list 102 permit tcp any eq
```

```
179
```

```
any
```

(ACL) لوصولاب مكحتلا ةمئاق ىلإ أدانتسا رورملا ءاطخأ حيحصت

دقوة جلاعمل القاطوة ركاذلا لثم ماظنلا دراوم صيصخت debug رمأ مادختسا بلطتي debug رمأ مدختسا. لمحللا ليقت ماظنل فقوت شودح يف يوصقلا تالاحللا يف ببستتي للاححتت يتلا رورملا كرح ديدحت لجأ نم (ACL) لوصوللا يف مكحت عمئاق مدختسا. عمئاق صيفصتت موقيا لنيوكتلا اذله لثم debug رمألا ريثأت ليلقتل يئاقنتنا لكشب صيفللا مزحيا.

10.1.1.1 و 172.16.1.1 نيفيفضملا نيب مزحلل طقف debug ip packet رمألا نيوكتلا اذله لغشي

```
<#root>
```

```
R1(config)#  
access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1  
R1(config)#  
access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1  
R1(config)#  
end
```

```
R1#debug ip packet 199 detail  
IP packet debugging is on (detailed) for access list 199
```

ريثأت لوح فيفاض تامولعم يلعل لوصولل [ءاطخألا حيصت رمأا لوح عمءاه تامولعم](#) يلا عجرا ءاطخألا حيصت رمأا.

يلعل لوصولل [Traceroute رمأا](#) و [Ping رمأا مهف](#) مسق [ءاطخألا حيصت رمأا مادختسا](#) يلا عجرا debug رمأا عم (ACL) لوصوللا يف مكحتلا مئاق مادختسا لوح فيفاض تامولعم.

MAC ناووع فيفصت

نكمي. عمءو ناووع وأ نيعم MAC عمقبط عمطحم رصم مادختساب تاراطإلا فيفصت كنكمي بسح فيفصتلا لجأ نم. ءادألا يلعل عمقبوعم نودب ماظنلا يف نيوانعل نم ددعيا نيوكت ماعلا نيوكتلا عضو يف رمألا اذله مدختسا، MAC عمقبط ناووع:

```
<#root>
```

```
Router#  
config terminal  
Router(config)#  
bridge irb  
Router(config)#  
bridge 1 protocol ieee  
Router(config)#
```

```
bridge 1 route ip
```

عمىاق مادختساب رورملا ةكرح ةيفصت لىل اجاتحت ةهجاو لىل رسجلا لوكوتورب قىب طت
ةمىاق مادختساب رورملا ةكرح ةيفصت لىل اجاتحت ةهجاو لىل رسجلا لوكوتورب قىب طت
bridge-group <group number> {input-address-list
<ACL number> | output-address-list <ACL Number>}:
ةمىاق مادختساب رورملا ةكرح ةيفصت لىل اجاتحت ةهجاو لىل رسجلا لوكوتورب قىب طت

```
<#root>
```

```
Router#
```

```
config terminal
```

```
Router(config-if)#
```

```
interface fastEthernet0/0
```

```
Router(config-if)#
```

```
no ip address
```

```
Router(config-if)#
```

```
bridge-group 1 input-address-list 700
```

```
Router(config-if)#
```

```
exit
```

ةيداملا تنرثي ةهجاول هنيىعت مت يذلا IP ناوع قبطو رسج ةيضارتفا ةهجاو عاشناب مق

```
<#root>
```

```
Router#
```

```
config terminal
```

```
Router(config-if)#
```

```
int bvi1
```

```
Router(config-if)#
```

```
ip address 192.168.1.1 255.255.255.0
```

```
Router(config-if)#
```

```
exit
```


```
Router(config)#
```

```
access-list 700 deny aaaa.bbbb.cccc 0000.0000.0000
```

```
Router(config)#
```

```
access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

عمئاق ىلع اهنىوكت مت يتيلا MAC نىوانعب طقف هجولم حمسي ، نىوكتلا اذه مادختساب
<mac address> صفر <ACL Number> access-list لوصولا عمئاق رمأ عم 700 لوصولا
حامس لاب مق مئ لوصول هل نوكتي نأ نكمي ال يذلا MAC ناونع صفر مق ، 0000.000.000،
لاثلما لىبس ىلع) (aaa.bbbb.cccc، لىبس لىلع) يقابلاب

 MAC ناونع لكل لوصولا عمئاق نم رطس لك عاشنإ: عظهارم

عحصلا نم ققحتلا

نىوكتلا اذه عحص نم ققحتلل عارجا آيلاح دجوي ال

اهحالص او عاطخال فاشكتسا

نىوكتلا اذهل اهلص او عاطخال فاشكتسال ةدحتم تامولعم آيلاح رفوتت ال

ةلص تاذا تامولعم

- [IP ىلا لوصولا مئاق نىوكت](#)
- [لوصولا مئاق معد ةحفص](#)
- [IP هيجوت معد ةحفص](#)
- [ةجؤملا IP تالوكتورب معد ةحفص](#)
- [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل