

اهم هف و PPP CHAP ة ق داصم ني وكت

تا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ت ا ح ا ل ط ص ا ل ا](#)

[ة ي س ا س ا ت ا م و ل ع م](#)

[CHAP ني وكت](#)

[ه ا ج ت ا ل ا ة ي ئ ا ن ث و ه ا ج ت ا ل ا ة ي د ا ح ا ة ق د ا ص م](#)

[CHAP ني وكت ت ا ر ا ي خ و ر م ا و ا](#)

[ي ل ع ا ف ت ل ا ث م](#)

[ة م ل ا ك م](#)

[ي د ح ت](#)

[ة ب ا ج ت س ا](#)

[\(ع ب ا ت\) ة ب ا ج ت س ا ل ا](#)

[CHAP ن م ق ق ح ت ل ا](#)

[ة ج ي ت ن](#)

[ه ا ح ا ل ص ا و CHAP ا ط ا خ ا ف ا ش ك ت س ا](#)

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

ة م د ق م ل ا

ل ا ص ت ا ل ا د ي ك ا ت ل ة ق د ا ص م ل ا ل و ك و ت و ر ب ة ح ص ن م ق ق ح ت ل ا ة ي ف ي ك د ن ت س م ل ا ا ذ ه ح ص و ي ه ا ج ت ا ل ا ة ي ث ا ل ث ة ح ف ا ص م ل ا ل ا خ ن م ر ي ط ن ة ي و ه ل (CHAP) ي د ح ت ل ا ة م ي ق ب

ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ة ي ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت

- encapsulation ppp erasecat4000_flash ل ا ل خ ن م ة ه ج ا و ل ا ي ل ع PPP ن ي ك م ت ة ي ف ي ك
- [ح ي ح ص ت ب ص ا خ ل ا PPP ض و ا ف ت ج ا ر خ ا م ه ف](#) ع ج ا ر . ر م ا ل ج ا ر خ ا | debug ppp negotiation ر م ا ل ا ض ر ع ي ت ا م و ل ع م ل ا ن م د ي ز م ي ل ع ل و ص ل ل [ا ط ا خ ا ل ا](#)
- ي ف م ك ح ت ل ا ل و ك و ت و ر ب ة ل ح ر م ن و ك ت ا ل ا م د ن ع ا ح ا ل ص ا و ا ط ا خ ا ل ا ف ا ش ك ت س ا ة ي ف ي ك ل م ت ك ت ي ت ح ا د ب ت ا ل PPP ة ق د ا ص م ة ل ح ر م ن ا ، ب ب س ب ا ذ ه و . ج ت ف ل ا ة ل ا ح ي ف (LCP) ط ا ب ت ر ا ل ا ، ح و ت ف م LCP ن ا ي ل ا ر م ا ل ا ر ي ش ي a l debug ppp negotiation ا ذ ا . ج ت ف ل ا ة ل ا ح ي ف ن و ك ت و LCP ة ل ح ر م ة . ة ب ا ت م ل ا ل ب ق ا ح ا ل ص ا و ة ل ك ش م ل ا ه ذ ه ا ط ا خ ا ف ا ش ك ت س ا ك م ز ل ي

(2 ر ا د ص ا ل ا و ا 1 ر ا د ص ا ل ا) MS-CHAP د ن ت س م ل ا ا ذ ه ل و ا ن ت ي ا ل : ة ط ح ا ل م

ةمدختسمل تانوكملا

ةني عم ةي دام تانوكموجمارب تارادصل ىلع دننتسمل اذهرصتقي ال

ةصاخ ةيلمعم ةئيبي في ةدوجوملا ةزهجال نم دننتسمل اذهي ةدراول تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دننتسمل اذهي ةمدختسمل ةزهجال عيمج تادب رمايال لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تش

تاحالطصال

Cisco تاحيملت تاحالطصا عجار، تادنتسمل تاحالطصا لوح تامولعمل نم ديزم ىلع لوصحلل ةنيقتلا.

ةيساسا تامولعمل

ةيوه نم (RFC 1994 في ددحمل) (CHAP) حفاصلتلا يدحتب ةقداصلملا لوكوتورب ققحتي CHAP: في اهذيفنت متي يتلا ةماعلا تاوطلال يلي امي. ةيثالث ةحفاصلم لالخنم ريظنلا

- الك نيبي CHAP ضوافت، (طابترالا في مكحتلا لوكوتورب) LCP ةلحرم لامتك دعب 1. ريظنلا ىلي يدحت ةلاسرق دصملا لسري، ني زاهجال
- صخلم) هاجتلا ةيداحأ ةئجت ةفيظو لالخنم اهباسح متي ةميقب ريظنلا بيحتسي 2. (MD5) 5 ةلاسرلا
- اذ. ةعقوتملا ةئجتلا ةميقل صاخلا هباسح لباقم ةباجتسال نم قداصلملا ققحتي 3. لاصلتالا اهان متي، الؤ. ةحجان ةقداصلملا نوكت، ميقل تقباطت

لاسرا متي ال. ريظنلاو ةقداصلملا طقف فورعم "رس" ىلع هذه ةقداصلملا ةقيرط دمتعت ضوافتلا كنكمي، طقف دحاو هاجتلا في نوكت ةقداصلملا نأ نم مغرلا ىلع. طابترالا ربع رسلا ةلدابتملا ةقداصلملا ةيرسلا ةومجمل سفن نم ةدعاسم، ني هاجتالا الك في CHAP ىلع

عجار، [RFC 1994](#) CHAP، لوكوتورب بويعو ايازمل لوح تامولعمل نم ديزمل

CHAP نيوكت

، ني هجوم كي دل نأ ضررتفنل، لاثملا لبيس ىلع. ام دح ىلي طيسب CHAP نيوكتل عارجال او 1. لكشلا في حضورم وه امك، ةكبش ربع ني لصلتم، راسي و ني مي



```
hostname left
username right password
  someone
int async 0
encapsulation ppp
ppp authentication CHAP
```

```
hostname right
username left password
  someone
int async 0
encapsulation ppp
ppp authentication CHAP
```

اهجوم

ةكبشلال ربع نالصت م ن

ةكبشلال ربع نالصت م ناهجوم — 1 لكش

ةيلالات تاوطخلال لمكأ، CHAP ةقداصم نيوكتل

1. رادصاب مق، ةهجاوإلى ع encapsulation ppp رمألا رادصاب مق، ةهجاوإلى ع.
2. مادختساب نيهجومالالكلى ع CHAP ةقداصم مادختساب نيكمت chap erasecat4000_flash:.
3. رادصاب مق، كلذب مايقلل. رورمال تاملكو نيمدختسملامسا نيوكتب مق. ريرظنلل فيضملامسا وه فيضملامسا شح، رمألا username username password password. رورمال ةملكو هجومالامسا. ني فرطالالك يف ةقباطتم رورمال تاملك: يلى ام نامض فرحألا ةلأجل ناساسح امهألا، امامت نالاثامتم.

هسفن فيرعتل هب صاخلال فيضملامسا هجومالمدختسي، يضارتفالكشب: **ةظحال** hostname ppp chap لالخنم اذه CHAP مدختسم مسا ريغت نكمي، كلذعمو. ريرظنلل erasecat4000_flash: عجار. [PPP chap لوكوتورب بلط رمألا مادختساب PPP ةقداصم](#) عجار. [PPP لوكوتورب ةقداصم](#) و. تامولعملانم ديزملى ع لوصحلل PPP لوكوتورب ةقداصم و.

هجاتإلا ةيئانثو هجاتإلا ةيداح ةقداصم

الك في CHAP مدختست كنإف، كلذعمو. هجاتإلا ةيداح ةقداصم ةقيرطك CHAP فيرعت متي أدبي، هجاتإلا يئانث CHAP لوكوتورب عم، كلذل. هجاتإلا ةيئانث ةقداصم عاشنإل ني هجاتإلا هجاتإلا ةيئانث ةلصفنم ةحفاصمب بناجلك.

فرطالايعدتسملال فرطالاقداصي نأ بجي، يضارتفالكشبو، Cisco CHAP ذي فننت في ةيداحألا ةقداصم لإف، يلاتلابو. (لمالكلاب ةقداصم لايغشت فاقيا متي مل ام) لصتملال نكمي، كلذعمو. ةقداصم لال نكمم لال نألا دجالا يه يمسمال فرطالاهل هتسي يتلا هجاتإلا ةيئانث ةقداصم كلذنع جتننو، يعدتسملال فرطالايوه نم ققحتلالاضيا لاصتالال فرطال هجاتإلا.

Cisco ل ةعبات ريغ ةزهجأب لاصتالال دنع ةبولطم هجاتإلا ةيداح ةقداصم لال نوكت ام ابلاغ.

هجوملى ع رمألا ppp authentication chap callin نيوكتب مق، هجاتإلا ةيداح ةقداصم لال ةبسنلاب لالاصتالال.

يلاعافت لاثم

CHAP ةقداصم ءانثأ ثدحت يتللا ثادحلأ ةلسلس مسقلا اذه يف ةدراول تاطلخملا ضرعت رملأا جارخا debug ppp negotiation يف ترهظ يتللا ةيلعفلل لئاسرلا لثمت ال هذه .نېهجوم نېب .ءاطلألأا حيحصت ب صاغلأا PPP ضوافت جارخا مهف عجار ،تامولعمل نم ديزمل

ةملاكم



يتأت ةوع

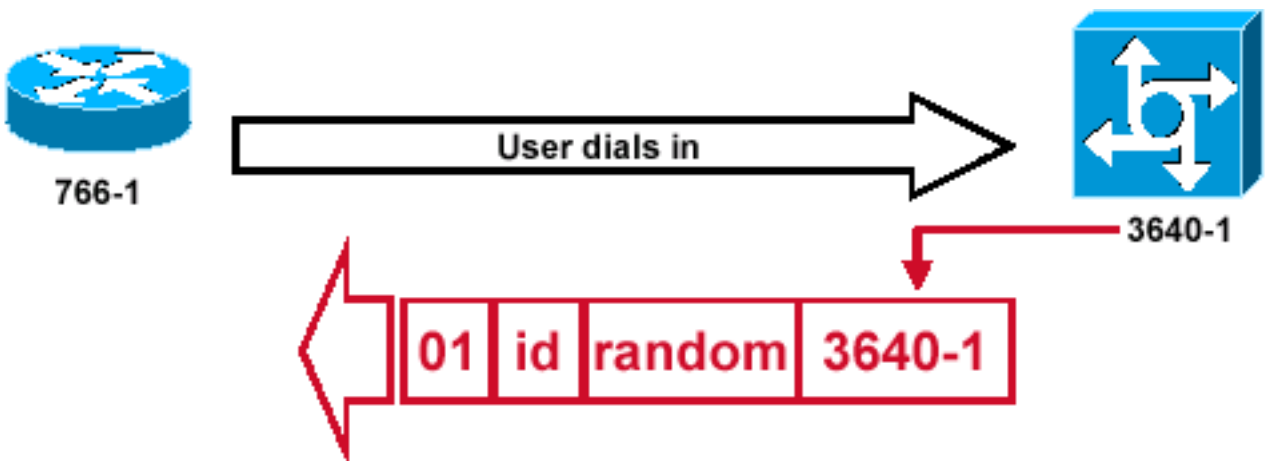
دلأ

لاصتالا مت — 2 لكش

ةيلتلا تاطلخملا ضرعي [2 لكشلا](#):

1. مادختساب ةدراول ةهجاولل نيوكت مت 3640-1 لىل ةملاكملا لصت .
erasecat4000_flash: .
2. تامولعمل نم ديزم لىل لوصحلل MD5 و CHAP لوكوتورب عم LCP لوكوتورب ضوافتي .
ءاطلألأا حيحصت ب صاغلأا PPP ضوافت جارخا مهف لىل عجار ،لكلذ ديدحت ةيفي لوج
3. ةملاكملا هذه يف لاصتالا هجوم لىل 3640-1 نم CHAP يدحت ءارجل بجي .

يدحت



CHAP Challenge ةمزح ءاشنأ م

ت

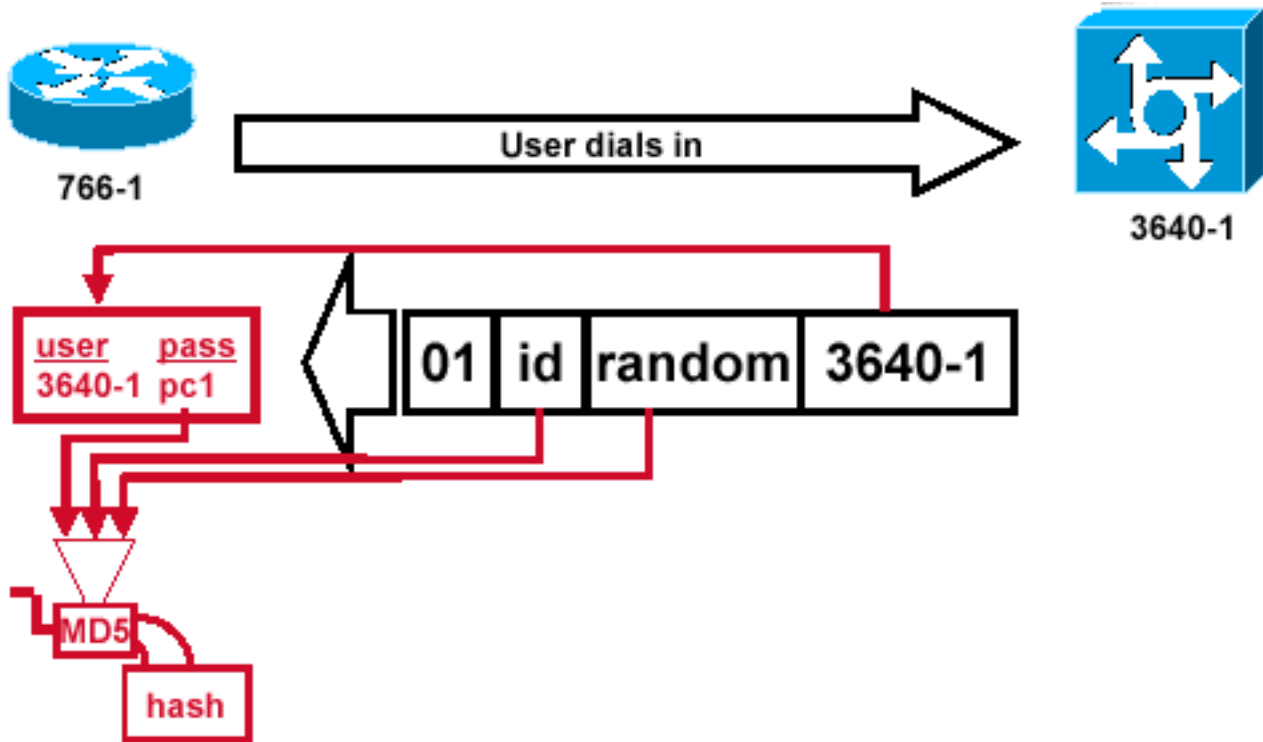
CHAP يدحت ةمزح ءاشنأ مت — 3 لكش

نېهجوملا نېب CHAP ةقداصم يف تاطلخملا هذه حضوي 3 لكشلا

1. ةمزح عون فرعم = 01: ةيلتلا صئاصللا مادختساب CHAP تايديحت ةمزح ءاشنأ متي .
لوقعم يئوشع مقرر = يئوشع يدحتلا ددحي يذلا يلسلسلا مقرر = فرعمللا يدحتلا
س فانملا ةقداصم مسا = 3640-1. هجوملا ةطساوب هؤاشنأ مت

2. ىمسمل هجوملا ىلع ةيئاوشعل ميقلاو فرعملاب ظافتحال متي.
3. تاي دحتلاب ةمئاقب ظافتحال ىرجيو .لاصتالا هجوم ىلا يدحتلا ةمزح لاسرا متي .
ةقلعمل

ةباجتسا



لتسالا

ريظنلا نم يدحتلا ةمزحل MD5 ةجلالعموم

ريظنلا نم يدحتلا ةمزحل MD5 ةجلالعموم مالتسالا — 4 لكشلا

ةمزح هجوملا جلاعي (MD5) اهتجالعمو ،ريظنلا نم يدحتلا ةمزح يقلت ةيئيكي حضوي 4 لكشلا
ةقيرطالا هذبه ةدراول CHAP تاي دحت

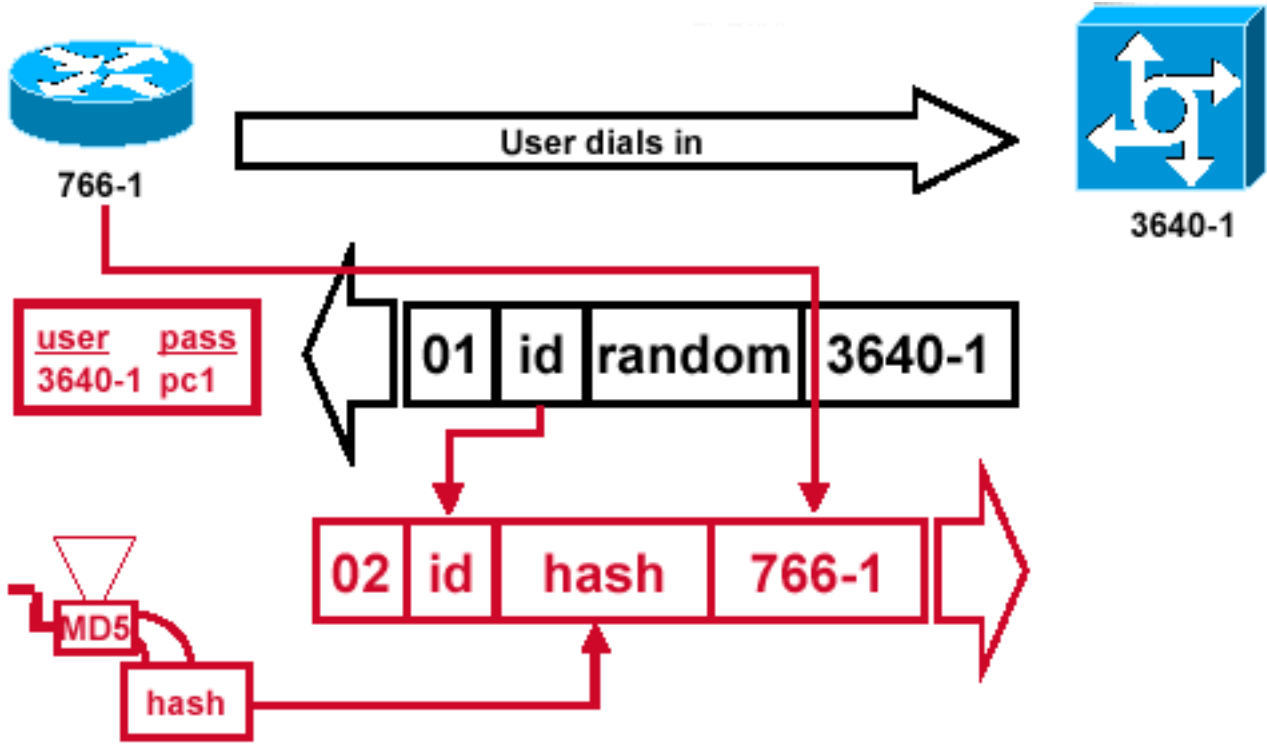
1. MD5 ةئزت دلوم ي فرعمل ةميق لاخدا متي.
2. MD5 ةئزت دلوم ي ةيئاوشعل ةميقلا لاخدا متي.
3. مساقباطي لاخدا نع هجوملا شحبي .رورملا ةملك نع شحلل 3640-1 مسالا مادختسا متي .
نع شحت ،لاثملا اذه ي .يدحتلا ي فرمدختسمل

```
username 3640-1 password pc1
```

4. MD5 ةئزت دلوم ي فرورملا ةملك لاخدا متي.

CHAP ةباجتسا ي فرىرأ ةرم هل لاسرا متي يذلا MD5-hashed CHAP يدحت يه ةجيتنلاو

ةباجتسالا (عبات)



م ت
 قدصملا ىلإ اهل اسرلا مت يتي ال CHAP ةباجتسا ةمزح عاشنإ

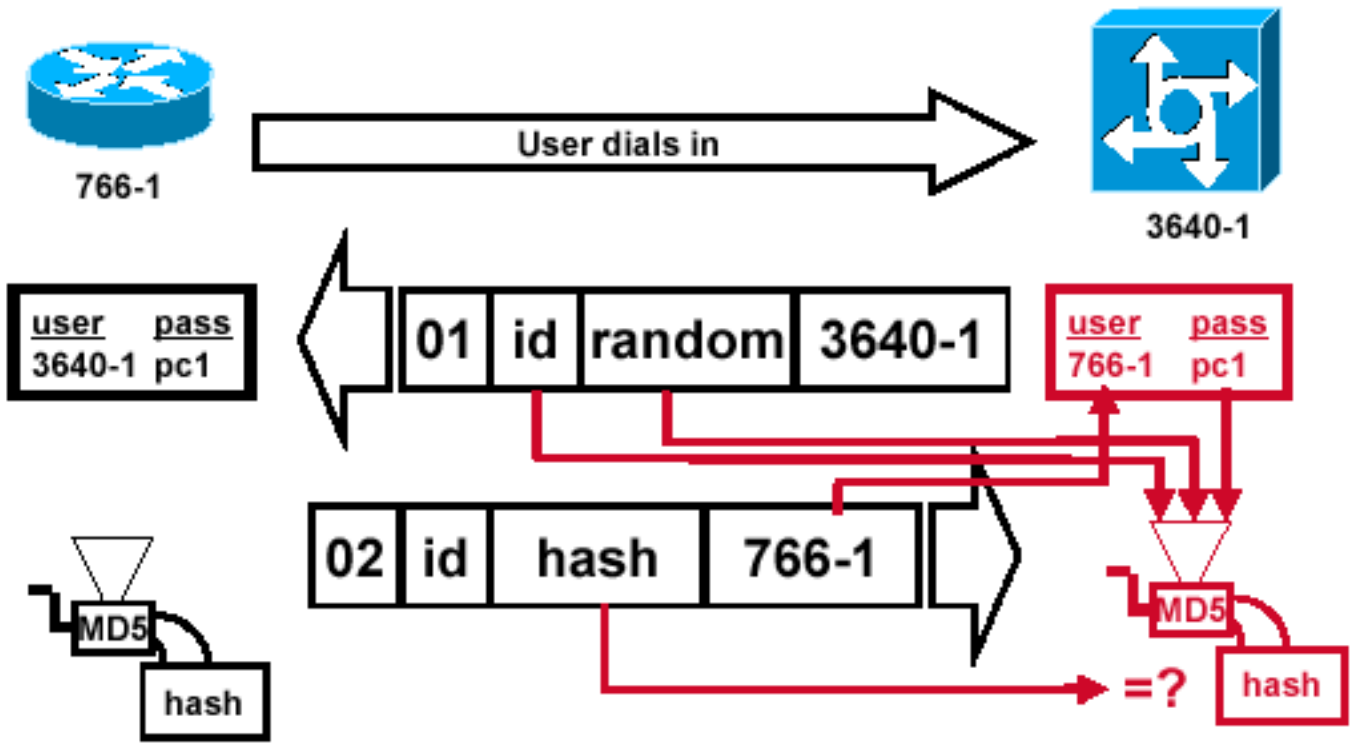
5 لكشلا

قدصملا ىلإ اهل اسرلا مت يتي ال CHAP ةباجتسا ةمزح عاشنإ ةيفي ك حضوي 5 لكشلا
 ةيلاتلا تاوطخلا ططخملا اذه:

1. ةباجتسا ةمزح عون فرعم = 02: ةيلاتلا تانوكملا نم ةباجتسالا ةمزح عيمجت متي. MD5 ةئزجت دلوم نم جارخال = ةئزجتلا. نايبتسالا ةمزح نم هخسن مت = فرعملا. CHAP اذه رفوت مزلي. زاهجال اذه ةقداصم مسا = 766-1. (يدحتلا ةمزح نم ةعمجملا تامولعمل) بولطملا رورملا ةملاك و مدختسملا مسا لاخذنا عثحب لابل ريظنلا موقوي كل رمالا [نم ققحتلا](#) مسق في لىصافتلا نم ديزمب كلذ حرش متي) ةيوهلا نم ققحتلل ([CHAP لوكوتورب](#)).
2. سفانملا ىلإ ةباجتسالا ةمزح لاسرا كلذ دعب متي.

CHAP نم ققحتلا

كب صاخلا نيوكتلا نم ققحتلا ةيفي ك لوح تاحيملت مسقلا اذه مدقي.



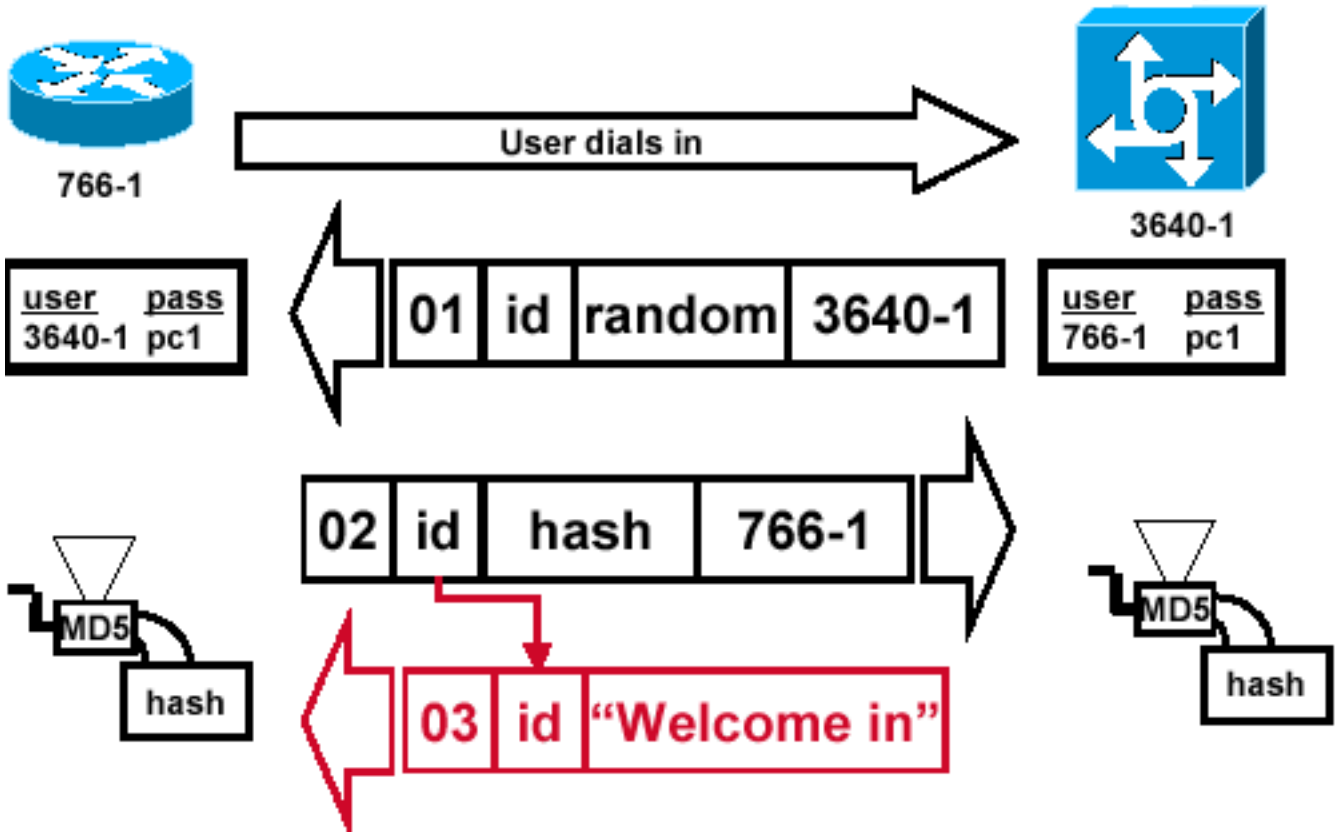
ةباجتسالا ةمزح ةجلالعمب Challenge موقبي

ةباجتسالا ةمزح Challenge جلالعي — 6 لكشلا

ةينعمل تاوطخل يلي اميف .ةباجتسالا ةمزحل سفانملا ةجلالعم ةيفيك حضوي 6 لكشلا (قدصملا يلع) CHAP ةباجتسالا ةمزح ةجلالعم دنع

1. ةيلصلأا نايبتسالا ةمزح يلع روثلل فرعمل مادختسا متي .
2. MD5 ةئزت دلوم يف فرعمل لاخدا متي .
3. MD5 ةئزت دلوم يف يلصلأا يدحتلل ةيئاوشعل ةميقلا ةيذغت متي .
4. تانايب ةدعاق:رداصملا هذه دحأ نم رورملا ةملك نع شحلل 766-1 مسالا مادختسا متي . TACACS+ و RADIUS مداخ.ةيلحمل رورملا ةملك و مدختسملا مسا
5. MD5 ةئزت دلوم يف رورملا ةملك لاخدا متي .
6. ةئزت ةميقب ةباجتسالا ةمزح يف اهيقلت متي يتلا ةئزتلا ةميق ةنراقم متت مئب .ةبوسحمل ةئزتلا ميق تناك اذا CHAP ةقداصم جئنت .اهباسح مت يتلا MD5 ةيواستم ةملتسملاو

ةجيتن



لاصتالال هجوم ىلا حاجنلا ةلاسرا لاسرا م

تي

لاصتالال هجوم ىلا حاجنلا ةلاسرا لاسرا م تي — 7 لكش

تاوطخلال نمضتي اذهو .لاصتالال هجوم ىلا اهلاسرا مت يتل حاجنلا ةلاسرا حضوي 7 لكشلال ةيلاتلال:

- 03: ةيلاتلال تانوكملا نم CHAP حاجن ةمزح عاشنل متيسف ، ةحجان ةقداصملا تناك اذا .يه "يف كب ابجرم". ةباجتسالال ةمزح نم خسنللا مت = فرعلملا. CHAP حاجن ةلاسرا عون م.دختسملال لبق نم هتءارق نكمي اريسفت رفوت ةيصن ةلاسرا ةطاسبب.
- 04: ةيلاتلال تانوكملا نم CHAP لشف ةمزح عاشنل متيسف ، ةقداصملا تلشف اذا .عون = "ةقداصملا لشف". ةباجتسالال ةمزح نم خسنللا مت = فرعلملا. CHAP لشف ةلاسرا م.دختسملال لبق نم هتءارق نكمي اجرش رفوت ، ىرخأ ةيصن ةلاسرا
- لاصتالال هجوم ىلا لشفلا وأ حاجنلا ةمزح لاسرا كلذ دعب متي .

متي ، هاجتلالا ةيئانث ةقداصم ي . هاجتلالا ةقداصملا لاثملا اذه حضوي : ةظحال م . ىلوالا يدحتلالا ةيئيهتب لاصتالال هجوم موقوي ، كلذ عمو . لمالكلاب ةيلمعلال هذه راركت

اهجالص او CHAP ءاطخأ فاشكتسأ

لوح تامولعم ىلع لوصحلل [اهجالص او \(PAP او CHAP\) PPP ةقداصم ءاطخأ فاشكتسأ](#) عجار اهجالص او ةلكشملا هذه ءاطخأ فاشكتسأ ةيئيهتب

ةلص تاذا تامولعم

- [PPP ءاطخأ حيحصت تاضوافم جارخا مهف](#)
- [PPP ةقداصم و PPP chap hostname لوكوتورب اعادتسأ رماو مادختساب PPP ةقداصم](#)
- [Cisco نم تاليزنتلالا وينقتلالا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة يرش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ل أ مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا