徹底攻略ポケット

Cisco CCNA Routing&Switching 直前対策

株式会社ソキウス・ジャパン 編著

重要項目だけを選りすぐり!

試験直前に確認すべき216問。
コマンド文例集付き

CCNA対策書で実績NO.1※黒本のポケット版

インプレス

本書は、CCENT（Cisco Certified Entry Networking Technician）、CCNA（Cisco Certified Network Associate）Routing and Switching の受験用教材です。著者、株式会社インプレスは、本書の使用による対象試験への合格を一切保証しません。

本書の内容については正確な記述に努めましたが、著者、株式会社インプレスは本書の内容に基づくいかなる試験の結果にも一切責任を負いません。

CCENT、CCNA、Cisco、Cisco IOS、Catalyst は、米国 Cisco Systems, Inc. の米国およびその他の国における登録商標です。
その他、本文中の製品名およびサービス名は、一般に各開発メーカーおよびサービス提供元の商標または登録商標です。なお、本文中には TM および ® は明記していません。

インプレスの書籍ホームページ

書籍の新刊や正誤表など最新情報を随時更新しております。

http://book.impress.co.jp/

はじめに

Cisco CCNA は、コンピューターネットワーク分野のリーディングカンパニーであるシスコシステムズの認定資格です。ネットワーク技術者の登竜門となるアソシエイトレベルの資格でありながら、難易度は決して低くありません。その理由のひとつとして、非常に広範な試験範囲を挙げることができます。技術の急速な進歩に伴い試験で問われる分野も拡大し、受験者には、一般的なネットワーキングの知識、シスコ製品のハードウェアやソフトウェアについての知識に加え、最新のネットワーク技術についての知識も要求されるようになりました。試験範囲全般の知識を一から身に付けるには、厚い対策書籍を長時間かけて学習する必要がありますが、あまりにも多くのことを学んでいるため、試験直前に何をどう復習してよいのかわからない、ということになりがちです。

本書は CCNA およびその下位資格である CCENT 受験のための直前学習に特化した問題集です。すでに試験範囲の技術やシスコ機器の操作方法を理解している方が、広い試験範囲を効率的に復習するのに最適な構成になっています。両資格の取得要件である「ICND1」「ICND2」「CCNA」の試験範囲のうち、合格のために必ず押さえておきたいテーマに絞り込み、「問題」「問題を解くために理解しておかなければならない重要事項」「問題の解き方」の 3 点を簡潔にまとめました。

試験範囲全般を総復習するには、CCNA もしくは CCENT の対象問題すべてに取り組んで、合格のために必要な事項や出題傾向の最終確認をしてください。ご自分の弱点を把握している方は、苦手分野の問題を試験直前まで何度も確認してください。

また、各技術を詳細に学習したい方は、既刊の『徹底攻略 Cisco CCENT/CCNA Routing & Switching 教科書 ICND1 編』および『徹底攻略 Cisco CCNA Routing and Switchig 教科書 ICND2 編』にじっくり取り組んでください。

CCNA、CCENT は、取得するための努力に見合う価値のある資格です。本書をご活用いただき、一人でも多くの方が目指す資格を取得されますことを願ってやみません。

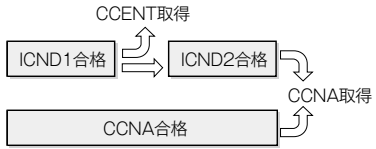
2015 年 7 月　著者

Cisco CCNA Routing & Switchingについて

シスコ技術者認定(Cisco Career Certification)は、シスコシステムズがインターネットワーキングや同社のスイッチやルータ製品に関する技術力を認定する資格制度です。技術分野別の11のトラックに分類されており、エントリー、アソシエイト、プロフェッショナル、エキスパート、アーキテクトの5つの認定レベルがあります。本書ではルーティング＆スイッチングトラックの、エントリーレベルの資格である「CCENT」とアソシエイトレベルの資格である「CCNA Routing & Switching」の試験範囲を対象にしています。

CCENTはICND1試験に合格することで取得できます。

CCNA Routing & Switchingは、 ICND1およびICND2の2つの試験に合格するか、 CCNA試験に合格することで取得できます。



各試験の概要は次のとおりです。

試験名：CCNA（200-120J）
試験時間：90分、問題数：50～60問、受験料：30,090円＋税
試験名：ICND1（100-101J）
試験時間：90分、問題数：40～50問、受験料：15,300円＋税
試験名：ICND2（200-101J）
試験時間：75分、問題数：50～60問、受験料：15,300円＋税

申し込みはいずれも、ピアソンVUEで受け付けています。

なお、上記の試験要項は予告なく変更される場合がありますので、必ず受験前にシスコシステムズのWebサイトで確認をしてください。

学習に役立つツールや資料

試験インターフェイスチュートリアル
http://www.cisco.com/web/JP/learning/exams/cert_exam_tutorial.html

シミュレーション問題のインターフェイスをはじめ、試験のさまざまな出題形式を体験することができます。

シスコラーニングネットワークジャパン

https://learningnetwork.cisco.com/community/connections/jp

シスコが主催する、受験者のための総合情報サイト。試験情報のほか、オンラインで受講できる試験対策セミナーや、学習者が情報交換をすることができるコミュニティ機能なども用意されています。

利用するには、無料の会員登録が必要です。また、一部のコンテンツは英語で提供されています。

インプレス刊『徹底攻略』シリーズを使用したおすすめの学習方法

1. 「教科書」で試験範囲の基礎学習

『徹底攻略Cisco CCENT/CCNA Routing & Switching教科書 ICND1編』は「CCNA」および「ICND1」の試験範囲に、『徹底攻略Cisco CCNA Routing & Switching教科書 ICND2編』は「CCNA」および「ICND2」の試験範囲に沿った構成で、ネットワークやシスコ機器の基礎を丁寧に解説しています。ネットワークの構成図や出力を豊富に掲載しているので、実際にCiscoネットワークを操作・検証しながら学習する機会がない方でも十分な学習効果が得られ、基礎知識をしっかりと身につけることができます。

2. 「問題集」で実戦的な試験対策

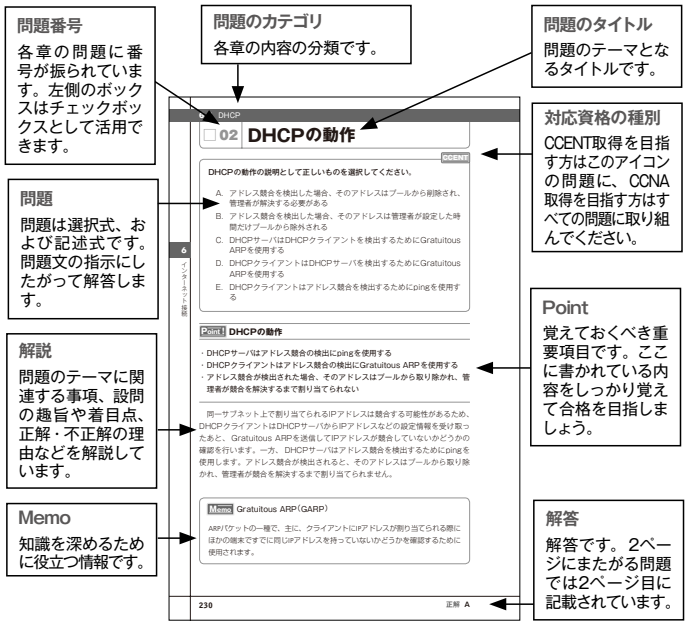
『徹底攻略Cisco CCNA Routing & Switching/CCENT問題集』は、実戦的な問題を数多く掲載した問題集です。問題を解き、解説を読み進めながら出題傾向や解答のポイントを把握することができ、合格に必要な知識を効率よく習得できます。

3. 本書「ポケット」で試験直前のラストスパート

本書で、試験の重要項目をおさらいします。 CCNA試験はきわめて試験範囲が広く、教科書や問題集での学習に数カ月を要します。そのため、学習し始めたころに覚えたことを忘れてしまうこともあるでしょう。また、似たような事項を学んでいくうちに知識が混乱し、いったん理解したはずの内容があやふやになってしまうことも考えられます。重要事項のおさらいをすることで試験直前に記憶をよみがえらせ、試験での取りこぼしをなくし、得点アップにつなげることができます。

本書の活用方法

本書は、CCNA、CCENTを取得するために、特に重要な項目をおさえた厳選問題216問を掲載しています。問題を解きながら、重要事項をしっかりとマスターすることができます。



構文は次のルールで記述しています。

- < > ……引数。該当する文字や値を入力する
- [ ] ……オプション。必要に応じて設定する要素
- { | } ……選択。{ }で括られたものから、いずれか1つを選択して入力する
  例){ a | b } →「a」か「b」のいずれかを入力する
- モード……構文の見出し後に示した(コンフィギュレーションモードを除く)
  (>、 #): ユーザEXECモードと特権EXECモードのいずれにも対応
  (#): 特権EXECモードにのみ対応
- プロンプト …ユーザEXECモードと特権EXECモードのいずれにも対応する場合は「#」で示した
- キーワードおよびオプションは主要なもののみ掲載した

目　次

Chapter 1

Cisco IOS基本設定とルータの管理

□01 Ciscoルータの基本設定

CCENT

初期状態のルータに「Central」と名前を付け、2つのインターフェイスにIPアドレスを設定して通信ができるようにします。必要なコマンドはどれですか。（4つ選択）

IP:172.16.1.2/26
GW:172.16.1.1

A. (config-if)#ip address 172.16.1.80 255.255.255.240
B. (config-if)#ip address 172.16.1.49 255.255.255.240
C. (config-if)#shutdown
D. (config-if)#description Central
E. (config-if)#ip address 172.16.1.90 255.255.255.240
F. (config-if)#no shutdown
G. (config-if)#ip address 172.16.1.1 255.255.255.192
H. (config)#hostname Central

Point! ルータの主な基本設定コマンド

● ルータに名前を設定
(config)#hostname <hostname>
● IPアドレスの設定
(config-if)#ip address <ip-address> <subnet-mask>
● インターフェイスの有効化／無効化
(config-if)#no shutdown …… 有効化
(config-if)#shutdown …… 無効化
● インターフェイス説明文の設定
(config-if)#description <説明文>
● 二重モードの設定
(config-if)#duplex { auto | full | half }
・auto …… オートネゴシエーションに設定する（デフォルト）
・full …… 全二重にする
・half …… 半二重にする

● 速度の設定

(config-if)#speed { 10 | 100 | 1000 | auto }

・10 …… 10Mbps にする
・100 …… 100Mbps にする
・auto …… オートネゴシエーションに設定する（デフォルト）

CentralルータのFa0/0インターフェイスには、接続しているホストのデフォルトゲートウェイ172.16.1.1をサブネットマスク255.255.255.192で設定します。

Fa0/1インターフェイスには、172.16.1.90をサブネットマスク255.255.255.240で設定します。

・172.16.1.1/26 ……ネットワークアドレス：172.16.1.0
　　ブロードキャストアドレス：172.16.1.63
　　ホストアドレス範囲：172.16.1.1～62
・172.16.1.90/28 …ネットワークアドレス：172.16.1.80
　　ブロードキャストアドレス：172.16.1.95
　　ホストアドレス範囲：172.16.1.81～94

選択肢Bの172.16.1.49は、Fa0/0インターフェイスに割り当てたネットワーク172.16.1.0/26のホストアドレス範囲に含まれています。このためFa0/1インターフェイスにBの設定をすると、「% 172.16.1.48 overlaps with FastEthernet0/0」という、172.16.1.48のネットワークアドレスがFa0/0と重複していることを示すエラーが返されます。

選択肢Aのアドレスはネットワークアドレスであるため誤りです。

ルータのインターフェイスは、初期状態でshutdownコマンドが設定されて無効になっています。使用するにはno shutdownコマンドで有効にする必要があります。

必要な設定は次のとおりです。

```
Router#configure terminal
Router(config)#hostname Central
Central(config)#interface fa0/0
Central(config-if)#ip address 172.16.1.1 255.255.255.192
Central(config-if)#no shutdown
Central(config-if)#interface fa0/1
Central(config-if)#ip address 172.16.1.90 255.255.255.240
Central(config-if)#no shutdown
Central(config-if)#end
Central#
```

02 特権モードパスワード

CCENT

R1ルータに対して以下のコマンドを入力しました。次回、ユーザEXECモードから特権EXECモードに移行するために必要なパスワードはどれですか。

```
R1>enable
R1#configure terminal
R1(config)#enable password ICND1
R1(config)#enable secret ICND2
R1(config)#exit
R1#disable
R1>
```

A. enable
B. ICND1
C. ICND2
D. ICND1またはICND2

Point! パスワードの設定コマンド

● 特権EXECモードに移行するときのパスワード

・イネーブルパスワードの設定(暗号化なし)

```
(config)#enable password <password>
```

・イネーブルシークレットパスワードの設定(MD5による暗号化)

```
(config)#enable secret <password>
```

※ 両方のコマンドを設定した場合、シークレットパスワードを優先

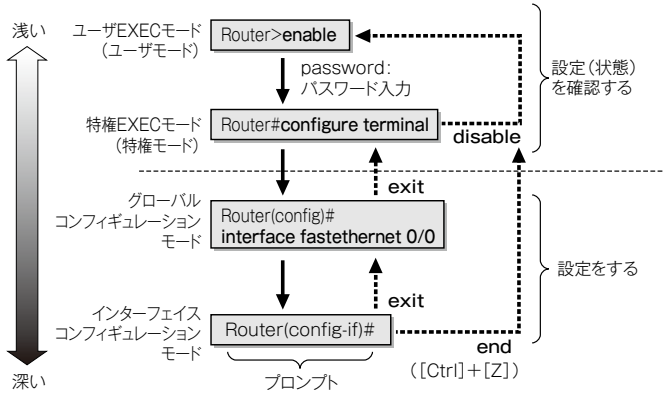
特権モードパスワードを設定すると、特権EXECモードと各種コンフィギュレーションモードを保護することができます。

イネーブルパスワードは設定したパスワードがプレーンテキストで表示されてしまうため、show running-configコマンドの出力中に、背後から覗かれるなどしてパスワードが読み取られる危険性があります。特別な事情がない限り、イネーブルシークレットパスワードのみを設定します。

イネーブルパスワードとイネーブルシークレットパスワードの両方が設定された場合、イネーブルシークレットパスワードが優先されます。したがって、設問のケースでユーザモードから特権モードへ移行する際には「ICND2」と入力する必要があります。

● Cisco IOSのCLIモード

CLIの階層レベル



●特権モードパスワードの設定と検証

```
R1(config)#enable password ICND1
R1(config)#enable secret ICND2
R1(config)#exit
R1#show running-config
Building configuration...

Current configuration : 756 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R1
!
enable secret 5 $1$6T6o$sftqlQjt.mcWFnczHDP5l. ←MD5で暗号化
enable password ICND1    ←プレーンテキスト
!
<output omitted>
ip subnet-zero
!
```

03 コンソールパスワード

CCENT

ルータのコンソールポートにPCを接続してログインする際に、パスワードciscoの入力が必要になるように設定し、一定時間操作しないときは自動的にEXECセッションをタイムアウトしたいと考えています。要件を満たすためのコマンドはどれですか。

A.
```
(config)#line console 1
(config-line)#password cisco
(config-line)#exec-timeout 10
```

B.
```
(config)#line console 1
(config-line)#login password
(config-line)#password cisco
(config-line)#exec-timeout 10
```

C.
```
(config)#line console 0
(config-line)#password cisco
(config-line)#login
```

D.
```
(config)#line console 0
(config-line)#password cisco
(config-line)#login
(config-line)#exec-timeout 0
```

Point! コンソールポートの設定

● コンソールパスワードの設定

```
(config)#line console 0
(config-line)#password <password>
(config-line)#login
```

※デフォルトはno login(パスワード要求なし)

● EXECセッションのタイムアウト時間の設定

```
(config-line)#exec-timeout <minutes> [<seconds>]
```

※デフォルトは10分間でタイムアウトする

● 割り込みメッセージのコマンド再表示

```
(config-line)#logging synchronous
```

コンソールパスワードを設定すると、コンソールポートから管理アクセスを試みたときにパスワード入力を要求するプロンプト「Password:」が表示され、正しいパスワードが入力されるまでユーザEXECモードに移行することはできません。

コンソールポートは1つだけなので、常にline console 0でラインコンフィギュレーションモードへ移行します。

loginコマンドは、パスワードによるコンソール認証を有効化するための設定です。コンソール接続の際にパスワードを要求させるには、passwordコマンドとloginコマンドの両方が必要です。no loginコマンドで無効にしている場合、たとえpasswordコマンドを設定していてもパスワード要求はありません。また、no passwordコマンドでパスワードを削除すると、loginコマンドが有効でもパスワード要求はありません。

ルータに管理的にアクセスしている状態で一定時間何も操作しないでいると、IOSは自動的にセッションを切断します。これによって、管理者が特権EXECモードでアクセスしたまま席を離れたり、ログアウトなしでターミナルソフトウェアを終了してしまったりしたときに、第三者に不正にアクセスされるのを防ぐことができるため、セキュリティが向上します。

セッションのタイムアウトは、デフォルトで10分間に設定されています。このタイムアウト時間を変更するには、exec-timeoutコマンドを使用します。なお、セッションを自動的にタイムアウトさせない場合は、exec-timeout 0コマンド(またはno exec-timeoutコマンド)を実行します。

Memo コマンドの権限レベル

ルータにはいくつかのコマンドの権限レベルがあります。

- 権限レベル1 …… Router> すべてのユーザレベルコマンドが使用可能
- 権限レベル15…… Router# すべての特権レベルコマンドが使用可能
- デフォルトは権限レベル1(ユーザEXECモード)でログイン
- 権限レベル15(特権EXECモード)でログインするための設定

```
(config-line)#privilege level 15
```

□04 VTY(仮想端末)パスワード

CCENT

R1に対して次のコマンドを設定しました。

```
R1(config)#line vty 0 4
R1(config-line)#password CCENT
R1(config-line)#login
```

リモートからR1に対するpingは成功します。このとき、R1に関する説明が正しいものを選んでください。(2つ選択)

A. R1へTelnet接続するには、no loginコマンドが必要である
B. R1へTelnet接続するとき、パスワードCCENTが必要である
C. 同時に最大4台のホストがR1へTelnet接続できる
D. パスワードCCENTは、running-config上に暗号化して保存される
E. no loginコマンドを設定すると、パスワードCCENTは使用されない

Point! VTY(仮想端末)の設定

● VTY(仮想端末)パスワードの設定

```
(config)#line vty <line-number>
(config-line)#password <password>
(config-line)#login
```

※ デフォルトはlogin(パスワード要求あり)

※ 仮想端末ポートにパスワード設定がないと「Password required, but not set」メッセージが表示され、Telnetセッションは拒否される

● プレーンテキストのパスワード暗号化

```
(config)#service password-encryption
```

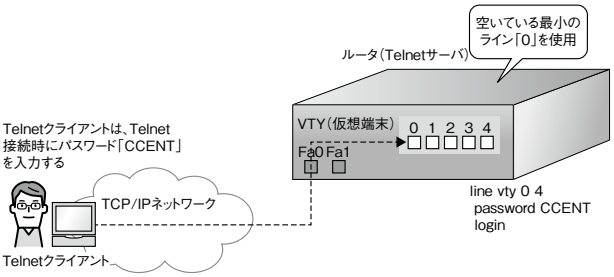
※デフォルトはno service password-encryption

・コンソールポートと同様に、exec-timeoutコマンドとlogging synchronousコマンドの設定が可能(問03を参照)。

VTY(仮想端末)パスワードを設定すると、離れた場所からTCP/IPネットワーク経由でTelnetを使用してルータやスイッチに管理接続できます。

各ポートには0から始まる連番でライン(回線)番号が付けられています。たとえば、1個のVTYポートだけに設定する場合は「line vty 0」、5個のVTYポートに対して設定する場合は「line vty 0 4」でラインコンフィギュレーションモードに移行します。設問ではline vty 0 4に対してパスワードを設定しているため、同時に最大5台のホストがTelnet接続することができます。

Telnetクライアントは、ルータやスイッチにEXEC接続するため、使用するVTYのライン番号を選択することはできません。 IOSはTelnet接続の要求があると、その時点で空いている最小のライン番号を割り当てます。



service password-encryptionコマンドは、すでに設定されたプレーンテキストのパスワードと、これから設定されるすべてのパスワードを暗号化します。暗号化されたことを示すために暗号文字列の前に「7」が追加されます。

なお、デフォルトはno service password-encryptionであり、パスワードは暗号化されません。

● service password-encryptionを設定している例

```
R1#show running-config
<output omitted>

line vty 0 4
 password 7 ##########    ← 「CCENT」が暗号化された
```

暗号化されたことを示している

05 管理アクセスの保護

CCENT

R1に対してTelnet接続する際に、ユーザ名(admin1)とパスワード(ccna)を要求するようにします。ユーザ名とパスワードはセキュリティ性の高い設定をする必要があります。設定が正しいものを選んでください。

A.
```
(config)#username admin1 secret ccna
(config)#line vty 0 4
(config-line)#login local
```

B.
```
(config)#username admin1 password ccna
(config)#service password-encryption
(config)#line vty 0 4
(config-line)#login
```

C.
```
(config)#line vty 0 4
(config-line)#username admin1 secret ccna
(config-line)#login
```

D.
```
(config)#username admin1 privilege 15 password ccna
(config)#line vty 0 4
(config-line)#login local
```

Point! ローカル認証の設定

● ユーザアカウント(ユーザ情報)の作成

(config)#username <username> password <password>

※暗号化なし(パスワードはプレーンテキストで保存される)

または

(config)#username <username> secret <password>

※暗号化あり(パスワードはMD5で暗号化される)

● ローカル認証の有効化

(config-line)#login local

コンソールポートやVTY(仮想端末)ポートを使用して管理アクセスするとき、ユーザ名とパスワードの入力を要求し、ユーザ認証するように構成できます。

ユーザ認証を行うには、事前にユーザアカウント(ユーザ情報)をデータベースとして用意しておく必要があります。ユーザアカウントをコンフィギュレーションファイル内に格納してルータ(またはスイッチ)自身で認証を行う方法をローカル認証といいます。

Cisco IOSでローカル認証を行う場合、ユーザアカウントにusernameコマンドを使用して「ユーザ名とパスワード」の組み合わせを登録します。username secretコマンドでは、ユーザ名とMD5で暗号化されたパスワードを設定します。MD5は強力な暗号化方式です。暗号化されたテキストを保存することにより、セキュリティが向上します。

login localコマンドは、ローカル認証の機能を有効にします。loginコマンドの場合、ログイン時にpasswordコマンドで設定されたパスワードのみを要求します。

なお、usernameコマンドにオプションのprivilege 15を付加すると、ユーザは最初から権限レベル15(特権EXECモード)でログインすることができます。これは今回の設問の要件ではありません。

● username secretコマンドの設定例(パスワード暗号化)

```
R1#show running-config
<output omitted>

username admin1 secret 5 $1$V8Pg$uu2sRatPtYAoCzWtIT9GT1
!                        ↑
!          username secretコマンドを設定(MD5でパスワード暗号化)
line vty 0 4
 password ccna  ←このパスワードは使用されない
login local     ←ローカル認証を行う
!
```

● username passwordコマンドの設定例(パスワード暗号化なし)

```
R1#show running-config
<output omitted>

username admin1 password 0 cisco
!                          ↑
!          username passwordコマンドを設定(パスワード暗号化なし)
line vty 0 4
 password ccna  ←ログイン時に使用するパスワード
login   ←ログイン時にパスワードのみ要求
!
```

06 SSH

CCENT

あるルータの仮想端末ポートに以下のコマンドを追加設定しました。このときの説明として正しいものはどれですか。

```
(config)#line vty 0 4
(config-line)#transport input ssh
```

A. ルータはTelnet接続とSSH接続を受け入れることができる
B. ルータはSSH接続のみ受け入れることができる
C. ルータに対してSSH接続を試み、失敗した場合はTelnet接続することができる
D. SSH接続を無効にするための設定である

Point! SSH(Secure SHell)

・暗号化と認証機能により安全なリモート接続を提供

● SSH接続のみ許可するための設定
`(config-line)#transport input ssh`
● TelnetとSSH接続を許可するための設定
`(config-line)#transport input telnet ssh`
● SSH接続の状態を表示(>、#)
`#show ssh`
● SSHのバージョンと設定情報を表示(>、#)
`#show ip ssh`

SSHは暗号化と認証機能によって安全にリモート接続するためのプロトコルです。ログイン後にやり取りするデータはすべて暗号化され、Telnetよりも安全にリモート接続することができます。

transport input sshコマンドを設定するとSSH接続のみ受け入れ、Telnet接続はできなくなります。TelnetとSSHの両方を受け入れたい場合は、transport input telnet ssh(またはtransport input ssh telnet)コマンドを設定します。

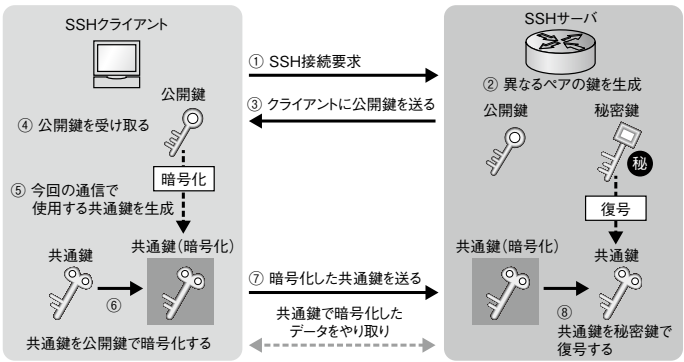
なお、デフォルトはtransport input allであり、SSHとTelnet両方(すべて)を許可しています。

Ciscoルータ（またはCatalystスイッチ）をSSHサーバとして設定するための手順は、次のとおりです。

① ユーザアカウント（ユーザ情報）の作成
```
(config)#username <username> { password | secret } <password>
```
② ホスト名の設定（暗号鍵の生成で使用）
```
(config)#hostname <hostname>
```
③ ドメイン名の設定（暗号鍵の生成で使用）
```
(config)#ip domain-name <domain-name>
```
④ 暗号鍵の生成（このコマンドを実行すると、鍵長の入力を求められる）
```
(config)#crypto key generate rsa
```
⑤ SSHバージョンの設定
```
(config)#ip ssh version { 1 | 2 }
```
⑥ SSHの許可
```
(config)#line vty <line-number>
(config-line)#transport input ssh
```
（SSH接続のみを許可。デフォルトはall）

⑦ ローカル認証の有効化
```
(config-line)#login local
```

● SSHによる通信手順



07 バナーメッセージ

CCENT

あるルータにTelnet接続した際に「Warning!」というメッセージを表示するコマンドはどれですか。

A. (config)#banner motd #Warning!#
B. (config)#line vty 0 4
   (config-line)#banner motd #Warning!#
C. (config)#vty banner #Warning!#
D. (config)#telnet banner #Warning!#

Point! バナーメッセージ

● バナーメッセージの種類
- motdバナー　……Message of The Dayの略。日々変わる可能性があるメッセージで利用
- loginバナー ……永続的なメッセージで利用
- execバナー　……ログインが許可されたあとにバナー表示

● 3種類のバナーを設定したときの表示順
① motdバナー ⇒ ② loginバナー ⇒ ③ execバナー

● motdバナーの設定
(config)#banner motd 〈区切り文字〉

・バナーメッセージ中に「Welcome」のような文言の使用は避ける

バナーメッセージは、ルータにログインする際にコンソール画面に表示させるメッセージです。 Enter キーを押すことで複数行にまたがって作成することができるため、区切り文字を使ってメッセージの始めと終わりをIOSに通知します。区切り文字にはメッセージ中に使用されない「#」のような記号を用います。なお区切り文字は、 running-config上では「^C」に変換されます。

● motdバナーの設定と検証

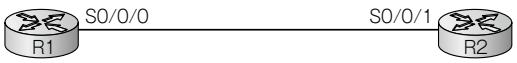
```
R1(config)#banner motd #    ← 区切り文字を「#」に指定
Enter TEXT message.  End with the character '#'.
Warning!     ←バナー
#      ← 終わりを示す「#」
R1(config)#exit
R1#logout      ← 検証のためにいったんログアウトする


R1 con0 is now available


Press RETURN to get started.    ← Enter キーを押して、再びログインする


Warning!    ←motdバナーが表示された


User Access Verification

R1>enable
R1#
```

セキュリティの観点から、バナーによって不正アクセスを防止することは重要です。バナーメッセージに侵入者をひきつけるような「Welcome」や「please」といった言葉を使用しないでください。このようなバナーは、悪意のあるアクセスをも歓迎するような雰囲気を表しているため、推奨されていません。

08 シリアルインターフェイスの設定

CCENT

出力を参照し、説明が適切なものを選んでください。




```
R1#show ip interface brief
Interface       IP-Address OK? Method Status                Protocol
FastEthernet0/0 172.16.1.1 YES manual up                    up
Serial0/0/0     172.16.2.1 YES manual up                    down
FastEthernet0/1 unassigned YES unset  administratively down down
Serial0/0/1     unassigned YES unset  administratively down down
R1#show controllers s0/0/0
Interface Serial0/0/0
Hardware is GT96K
DTE V.35 TX and RX clocks detected.
idb at 0x6324BD80, driver data structure at 0x632534A4
<output omitted>
```

A. R1のS0/0/0インターフェイスでclock rateコマンドが必要
B. R2はDCEデバイスとして動作している
C. R1とR2間で通信を行うことができる
D. R1とR2の両方にbandwidthコマンドが必要

Point! シリアルインターフェイスの設定

- 帯域幅の設定
  `(config-if)#bandwidth <kbps>`
- DCEとして送信するクロック信号を設定
  `(config-if)#clock rate <bps>`
- 接続しているケーブルの種類、DTEとDCEを確認(>、#)
  `#show controllers [<interface-type>]`

・バックツーバック接続の場合、DCEコネクタ側を持つルータでclock rateコマンドが必要

通常、プロバイダに接続する場合はルータはDTE側になりますが、図のようにバックツーバック接続（ルータのシリアルインターフェイス同士を直接接続）している場合には、片方のルータをDCEにする必要があります。

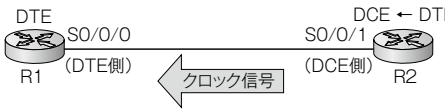
R1のS0/0/0インターフェイスは「up, down」で通信できない状態です。これは、バックツーバック接続で、DCEコネクタ側にclock rateが設定されていないことが原因と考えられます。

show controllersコマンドの出力の3行目は、R1のコネクタがDTE側であることを示しています。したがって、R2（DCE側）でclock rateコマンドが必要です。なお、R1（DTE側）でclock rateを実行すると「Error: This command applies only to DCE interface」というエラーが返されます。

R1－R2間で通信を行うために帯域幅の設定は必要ありません。

DCEとDTEの詳細は『Chapter7問01』を参照してください。

● バックツーバック接続におけるclock rateコマンドの設定例




```
R2(config)#interface s0/0/1
R2(config-if)#clock rate 128000  ←クロックレートを128kbpsに設定
R2(config-if)#end
R2#show controllers s0/0/1
Interface Serial0/0/1
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 128000  ←DCE（ケーブルタイプV.35）、クロック128kbps
idb at 0x816403B8, driver data structure at 0x81647E64
<output omitted>
```

Memo シリアルケーブルの未接続

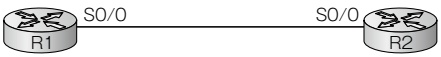
シリアルインターフェイスのDCE/DTEは、シリアルケーブルが適切に接続されることによって認識されます。シリアルケーブルを接続していない状態でshow controllersコマンドを実行すると「No serial cable attached」が表示され、DCE/DTEについては表示されません。

```
RT1#show controllers s0/0/0
Interface Serial0/0/0
Hardware is GT96K
No serial cable attached ←シリアルケーブルが未接続
idb at 0x4986EBD4, driver data structure at 0x49870DAC
wic_info 0x498713D8
<output omitted>
```

09 インターフェイスのステータス①

CCENT

図の構成でR1−R2間で通信をしています。R1のSerial0/0インターフェイスでshutdownコマンドを実行したときの各ルータのSerial0/0インターフェイスのステータスはどのようになりますか。



A. R1 : Serial0/0 is down, line protocol is down
   R2 : Serial0/0 is up, line protocol is down
B. R1 : Serial0/0 is administratively down, line protocol is down
   R2 : Serial0/0 is administratively down, line protocol is down
C. R1 : Serial0/0 is down, line protocol is down
   R2 : Serial0/0 is up, line protocol is down
D. R1 : Serial0/0 is administratively down, line protocol is down
   R2 : Serial0/0 is down, line protocol is down

Point! インターフェイスのステータスの見方

Serial0/0 is [物理層レベル], line protocol is [データリンク層レベル]
↑ キャリア　　↑ キープアライブ

インターフェイスのステータスで、カンマ(,)を挟んで左側には物理層レベルの状態が表示されます。シリアルインターフェイスの場合、対向機器からキャリア検知信号を受信しているかどうかを示します。

右側はデータリンク層レベルの状態を表しています。ここでは、キープアライブが受信されているかどうかを示しています。

R1のS0/0インターフェイスをshutdownした場合、R1側のステータスは「管理的に無効」であることを示す「administratively down, line protocol is down」になります。一方、R2側のステータスは対向でshutdownしているため、物理層レベルで無効の「down, line protocol is down」になります。

正解 D

□10 インターフェイスのステータス②

CCENT

show interfaces serial0/0コマンドの出力で、物理層に問題がある場合の表示はどれですか。

A. Serial0/0 is up, line protocol is up
B. Serial0/0 is down, line protocol is up
C. Serial0/0 is administratively down, line protocol is down
D. Serial0/0 is down, line protocol is down

Point! インターフェイスのステータス

● Serial0/0 is up, line protocol is up
・物理層、データリンク層で正常。通信が可能な状態

● Serial0/0 is up, line protocol is down
・データリンク層に問題がある。
<原因>・カプセル化タイプが不一致
・DCE側でclock rateの設定がない
・キープアライブを受信していない

● Serial0/0 is administratively down, line protocol is down
・shutdownコマンドによって管理的に無効な状態
・通信できるようにするにはno shutdownが必要

● Serial0/0 is down, line protocol is down
・物理層に問題がある。
<原因>・ケーブルが未接続、ケーブルに問題がある
・対向のインターフェイスでshutdown(無効)している

物理層に問題があり、データリンク層が正常になることはないため、選択肢Bの「Serial0/0 is down, line protocol is up」という状態になることはありません。

□11 インターフェイスの検証

CCENT

次のルータの出力を参照し、インターフェイスに関する説明が正しいものを選んでください。（2つ選択）

```
R1#
              is up, line protocol is up
  Hardware is Gt96k FE, address is 001f.caec.d6ba (bia 001f.caec.d6ba)
  Internet address is 192.168.5.65/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

A. サブネットマスクは255.255.255.192である
B. このインターフェイスはFastEthernetである
C. カプセル化タイプはHDLCである
D. show interfacesコマンドの出力である
E. show ip interface briefコマンドの出力である

Point! インターフェイスの主な検証コマンド

- インターフェイスの詳細情報を表示(>、#)
  `#show interfaces [<interface-id>]`
- インターフェイスのIPに関する情報を表示(>、#)
  `#show ip interface [<interface-id>]`
- すべてのインターフェイスの状態を要約表示(>、#)
  `#show ip interface brief`

設問の出力はFastEthernetインターフェイスでのshow interfacesコマンドの結果です。

```
R1#show interfaces fa0/0
FastEthernet0/0 is up, line protocol is up   ←ステータス
  Hardware is AmdFE, address is 0004.278e.d740 (bia 0004.278e.d740)
  Internet address is 192.168.5.65/27      ←IPアドレス
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,  ←帯域幅（BW）
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set  ←カプセル化タイプ
  Keepalive set (10 sec)
<output omitted>
```

192.168.5.65/27のサブネットマスクは255.255.255.224です。

出力の4行目の「BW 100000 Kbit」は帯域幅が100Mbpsであることを示しており、このことからインターフェイスはFastEthernetと判断できます。6行目の「Encapsulation ARPA」からカプセル化タイプがARPA（EthernetII）であることがわかります。カプセル化タイプにはほかにHDLC、PPP、FRAME-RELAYなどがあります（シリアルインターフェイスの場合）。

show ip interface briefコマンドでは、割り当てたIPアドレスやポートの状態がインターフェイスごとに1行で表示されます。

● 特定のインターフェイスの要約情報を表示

```
Ro-A#show ip interface brief fa0/0
Interface       IP-Address OK? Method Status              Protocol
FastEthernet0/0 10.7.2.4   YES manual up                  up
```

● すべてのインターフェイスの要約情報を表示

```
Ro-A#show ip interface brief
Interface       IP-Address OK? Method Status                Protocol
FastEthernet0/0 10.7.2.4   YES manual up                    up
Serial0/0/0     172.16.1.1 YES manual up                    up
FastEthernet0/1 unassigned YES unset  administratively down down
Serial0/0/1     unassigned YES unset  administratively down down
```

show ip interfaceコマンドの出力は『Chapter5問20』を参照してください。

□12 Cisco IOSでのTelnet操作

CCENT

次の出力を参照し、説明が正しいものを選択してください。(2つ選択)

```
R1#telnet 172.16.3.3
Trying 172.16.3.3 ... Open

User Access Verification

Password:
R3> Ctrl + Shift + 6⇒X キー
R1#
```

A. R1からR3へTelnet接続したあとにTelnetセッションを終了している
B. R3へのTelnetセッションを中断している
C. telnetコマンドでR3へのTelnetセッションを再開できる
D. Telnetセッションを表示するにはshow telnetコマンドを使用する
E. Enterキーを押すと、プロンプトはR3> になる

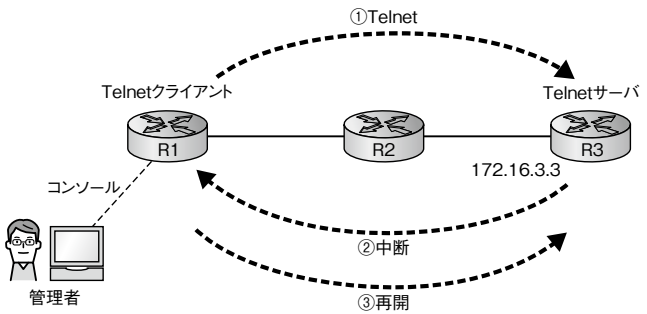
Point! CiscoIOSでのTelnet操作

● Telnet接続を実行(>、#)
`#telnet { <ip-address> | <hostname> }`
● 接続状況の確認(>、#)
`#show users`
● Telnetセッションの中断
Ctrl + Shift + 6⇒X キー
● 中断しているセッション情報の表示(>、#)
`#show sessions`
● Telnetセッションの再開(>、#)
`#resume` または Enter キー (直前のセッション再開)
`#resume { <connection-number> | <hostname> }` (特定のセッション再開)
● Telnetセッションの終了(>、#)
`#exit` または `#logout` (リモートデバイスで終了)
`#disconnect [{<connection-number> | <hostname>}]` (中断セッションの終了)
`#clear line <line-number>` (Telnetサーバ側でセッションの終了)
※ clear lineコマンドのみ特権EXECモード(#)でのみ実行可能

Cisco IOSではTelnet（またはSSH）セッションを保持したままの状態で、元のデバイスのCLIに戻る「セッションの中断」ができます。セッションを再開する際は再びパスワードを入力する必要はなく、中断前と同じプロンプトで操作をすぐに再開することができるため、管理者は目的のデバイスにすばやくアクセスして作業が行えます。

セッションを中断するには、Ctrl＋Shift＋6キーを押し、3つのキーを放した直後にXキーを押します。この操作を行うと、セッションを保持した状態でローカルのプロンプトに戻ります。

● Telnet接続の中断と再開の例




```
R1#telnet 172.16.3.3 ←Telnet実行（①）
Trying 172.16.3.3 ... Open

User Access Verification

Password:
R3>  ←Ctrl＋Shift＋6⇒Xキーを押してTelnetセッション中断（②）

R1#show sessions
Conn Host                Address             Byte  Idle Conn Name
*  1 172.16.3.3          172.16.3.3             0     0 172.16.3.3

R1#  ←Enterキーを押してTelnetセッション再開（③）

[Resuming connection 1 to 172.16.3.3 ... ]

R3>  ←R3へのTelnetセッションが再開された
```

□13 CDPの概要

CCENT

次の出力を参照し、適切な説明を選んでください。（2つ選択）

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Local Intrfce     Holdtme  Capability  Platform  Port ID
R2           Ser 0/0/0         175       R S I      2811      Ser 0/0/1
SW1          Fas 0/0           164         S I      WS-C2960- Fas 0/9
```

A. R1のS0/0/0インターフェイスにR2が接続されている
B. R1のFastEthernet0/9ポートにSW1が接続されている
C. R1には2台のCiscoデバイスが直接接続されている
D. S0/0/0インターフェイスがダウンするとすぐにR2のエントリは消去される

Point! CDP（Cisco Discovery Protocol）の特徴

・シスコ独自のレイヤ2プロトコル（データリンク層で動作）
・隣接するCiscoデバイスの情報を収集するツール
・CDPパケットはSNAPでカプセル化されてマルチキャストで送信
・CDPはデフォルトで有効化されている
・60秒間隔でCDPパケットを送信し、ホールドタイムは180秒

CDPは、隣接しているCiscoデバイスの情報を収集する管理ツールで、データリンク層で動作します。

● CDPの位置付け

レイヤ	プロトコル
ネットワーク層	IP、Novell IPX、AppleTalkなど
データリンク層	CDP
物理層	SNAPをサポートする物理メディア、イーサネット、フレームリレー、ATMなど

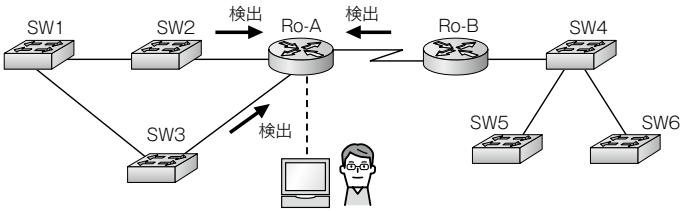
● CDPで収集できる主な情報

情報	説明
Device ID	隣接するCiscoデバイスのホスト名
Local Intrfce	自身のインターフェイスまたはポート
Holdtime	受信したCDP 情報を保持する時間(デフォルト：180秒)
Capability	隣接デバイスがサポートしている機能
Platform	隣接デバイスの製品型番(例：Cisco 2811の場合「2811」)
Port ID	隣接デバイスのインターフェイスまたはポート番号
Address	隣接デバイスのIPアドレス(ネットワーク層アドレス)
IOS Software, Version	隣接デバイスのIOSソフトウェアとバージョン

「Local Intrfce」はR1自身のインターフェイス、「Port ID」は隣接デバイスのポート情報です。 R2とSW1のエントリが表示されているため、 R1には2台のCiscoデバイスが接続されています。

S0/0/0がダウンすると、ホールドタイムの175秒後にR2のエントリは消去されます。

● CDPによるネイバー検出



※ Ro-AはCDPによって3台(Ro-B、 SW2、 SW3)の隣接するCiscoデバイスの情報を知ることができる

CDPはレイヤ2プロトコルです。ケーブルを接続してインターフェイスを有効化(no shutdown)すると、 CDPは使用できます。つまり、 IPアドレスの設定なしでも使用可能です。

□14 CDPコマンド

CCENT

Ciscoルータにログインし、隣接しているCatalystスイッチにTelnet接続をするために、IPアドレスを調べなければなりません。このとき使用するコマンドはどれですか。（2つ選択）

A. show cdp address *
B. show cdp neighbors *
C. show cdp neighbors detail
D. show cdp entry *

Point! CDPの主なコマンド

- CDPのグローバルな情報（タイマー、バージョンなど）を表示（>、#）
  #show cdp
- 隣接するCiscoデバイスの要約情報を表示（>、#）
  #show cdp neighbors
- 隣接するCiscoデバイスの詳細情報を表示（>、#）
  #show cdp neighbors detail
- 隣接するすべてのCiscoデバイスの詳細情報を表示（>、#）
  #show cdp entry *
- 隣接する特定デバイスの詳細情報を表示（>、#）
  #show cdp entry <device-id>
- CDPパケットの詳細情報を表示（>、#）
  #show cdp traffic
- インターフェイスおよびCDPタイマー情報を表示（>、#）
  #show cdp interface [<interface-id>]
- デバイス全体でCDPの無効化
  (config)#no cdp run
- 特定のインターフェイスでCDPを無効化
  (config-if)#no cdp enable

show cdp neighbors detailコマンドとshow cdp entry *コマンドは、直接接続されているCiscoデバイスのIPアドレスを表示します。


```
R1#show cdp neighbors detail
-------------------------
Device ID: R2
Entry address(es):
  IP address: 10.3.0.2   ←R2のIPアドレス
Platform: Cisco 2811,  Capabilities: Router Switch IGMP
Interface: Serial0/0/0,  Port ID (outgoing port): Serial0/0/0
Holdtime : 168 sec

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 12.4
(12a), RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 22-Feb-07 17:12 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''

-------------------------
Device ID: SW1
Entry address(es):192.168.2.2   ←SW1のIPアドレス
Platform: cisco WS-C2960-48TT-L,  Capabilities: Switch IGMP
Interface: FastEthernet0/0,  Port ID (outgoing port): FastEthernet0/9
Holdtime : 157 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE3,
RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 22-Feb-07 13:57 by myl

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=00
000000FFFFFFFF010220FF00000000000000001B54AF9C80FF0000
VTP Management Domain: 'CCNA'
Native VLAN: 1
Duplex: full
```

※show cdp entry *コマンドでも同じ出力結果が得られる

選択肢AとBは不正なコマンドです。