Admintech.jpミニ勉強会

は･じ･め･て･の....Cisco♪

2007/4/21

Masa

レベル:★☆☆☆☆

講師自己紹介

- 都内某IT企業に勤務
- 業務は、Networkを中心としたインフラの設計／構築／運用を担当
  - Cisco CCIE 17235(Routing&Switching)　2つめを狙うでー！
  - あとはCCSP、SCSecAなどを取得
- 複数の企業にて、Network関連の講師を担当
  - 担当したコース：CCNA、CCNP、CCSP etc.
  - 新人教育もやります。ご相談ください。

本日の内容

- Cisco機器のパスワード
  - 本当に安全なのかい？？
- Cisco機器のログインレベル
  - ログインレベルによるコマンドの違い
  - 内部統制な内容も含めまして。

本日の勉強会について

- 全体的に、基本レベルの内容です。
  - 主に運用側に視点を置いての説明となります。
  - 説明がくどいかもしれませんが、ご容赦を….
- TCP/IPの基礎知識があればOKです。
- 説明だけでなく、Hands-Onもやりますかね。

本日使用する機器

- Cisco 806
  - Ethernet×2、PPPoEも使えます。
  - IOS：12.2(8)IP Feat.

は･じ･め･て･の....Cisco♪ その1

Cisco機器のパスワード①

IPv4アドレスについて

- ....は、すまん。パス。

- クラスA～CのPrivate Addressについて復習です。
  - クラスA　10.0.0.0 /8
  - クラスB　172.16.0.0 /12
  - クラスC　192.168.0.0 /16

Cisco機器でのモードについて①

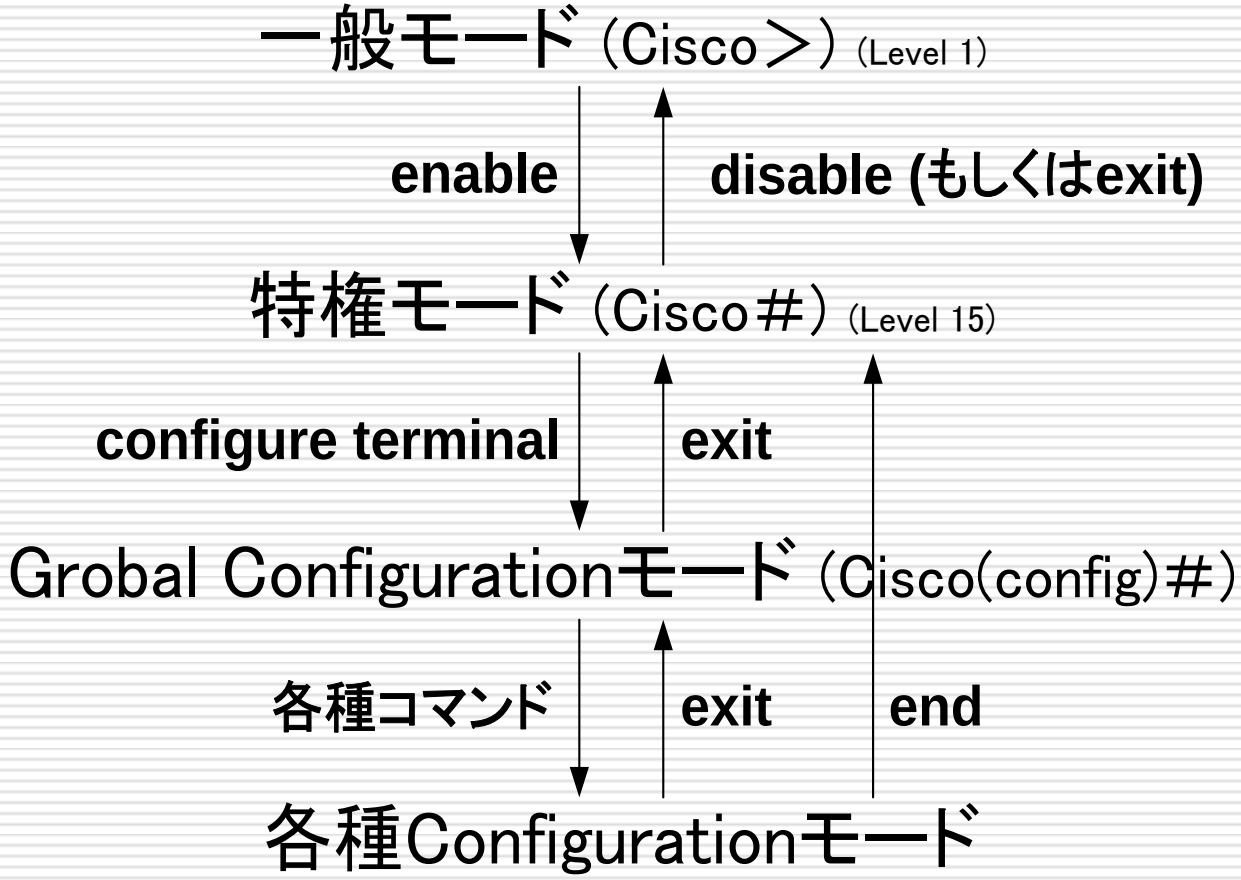
- 一般モード(コンソール　Cisco>)
  - 機器に最初にログインしたときの状態(レベル1)
  - 使用できるコマンドは、かなり限られている。

- 特権モード(コンソール　Cisco#)
  - Cisco機器での管理者モード(レベル15)
  - 機器の各種設定の確認の他、設定を削除することもできる。

Cisco機器でのモードについて②

- configurationモード(コンソール　Cisco(config)#)
  - 機器に設定を行う際のモード。
  - 実際には、configurationモードの中にも、設定の項目に応じて、何種類かのモードがある。
    - General configurationモード(Cisco(config)#)
    - Interfaceのconfigurationモード(Cisco(config-if)#)
    - Lineのconfigurationモード(Cisco(config-line)#)
    - Routingのconfigurationモード(Cisco(config-rt)#)

Cisco機器のモードについて



Cisco機器でのパスワード

- vtyライン(Virtual TeletYpe)用のパスワード
  - telnetやsshでの接続時に使いる
- ctyライン(Console TeletYpe)用のパスワード
  - コンソール接続時に使いる
- 特権モードになる用のパスワード

Cisco機器Hands-On①

では、ここまでの内容を、実際に設定してみましょう。

Cisco機器Hands-On① 設定内容

- 初期状態：出荷時状態

- ホスト名：Admintech
- Ethernet0のアドレス：192.168.1.1 /24
- Ethernet1のアドレス：172.16.1.1 /24
- cty接続用のパスワード：admintech
- vty接続用のパスワード：admintech
- enable用のパスワード：cisco

は･じ･め･て･の....Cisco♪ その1

Cisco機器のパスワード②

パスワードの暗号化レベル①

- パスワードには、次の3種類の暗号化がある。
  - 平文;暗号化されていない
  - 弱い暗号化(Type 7)
    - Cisco独自の暗号化アルゴリズム。
    - 16進数で表記されている。
    - 解析ツールを使えば、簡単に解析される。
  - 強い暗号化(Type 5)
    - MD5ハッシュ方式を用いた暗号化。
    - 基本的に、解読は不可能。

パスワードの暗号化レベル②

- Cisco機器では、パスワードを全体的に暗号化するコマンドがある。(Grobal configuration モードで設定)
  Cisco(config)# **service␣password-encryption** ↵

			全体の暗号化	
			×	○
暗号化	vtyライン		平文	弱い暗号化(Type 7)
	ctyライン		平文	弱い暗号化(Type 7)
	特権Mode	enable password	平文	弱い暗号化(Type 7)
		enable secret	強い暗号化(Type 5)	強い暗号化(Type 5)

アカウントの設定

- Cisco機器では、ログインするアカウント／パスワードを設定することが出来る。
  - アカウントごとにログインレベルを設定することができる→詳細は後述

- 設定は、Cisco機器内でも行うことができるし、tacacs+(*1)サーバに設定することもできる。

(*1) Cisco Systems社によりtacacs (Terminal Access Control Access)を独自に拡大したもの。

じゃあ、どう設定する？①

- enable用のパスワードは、やはり**enable secret**で設定しよう。(特権モードと言うのは、UNIXでいうrootですので….)
- **service password-encryption**コマンドは設定しよう。
- でもその前に、パスワードは複雑なものにしよう。当たり前だけど….

Cisco機器Hands-On②

では、ここまでの内容を、実際に設定してみましょう。

Cisco機器Hands-On② 設定内容

- 初期状態：Hands-On①終了時

- **service password-encryption**コマンドを設定

は･じ･め･て･の....Cisco その2

Cisco機器のログインレベル

Cisco機器のログインレベル

- 0～15のログインレベルが設定されている。
  - 1は(vtyライン、ctyラインで)ログインした状態
  - 15は特権モード

- それぞれのレベルで、入力できるコマンドが異なる。

各ログインレベルで使用できるコマンド

- 別紙でお渡しします。
- Level 0とLevel 15以外は、全てのレベルで同じって....orz

Cisco機器内での設定方法

- enableコマンドで指定する

  Cisco(config)# **enable␣(password | secret)␣level␣**(ログインレベル)**␣**(パスワード)

  - 各レベルごとにパスワードを作成しないと使えない。
  - 設定したレベルのコマンドのみ使うことができる。

- アカウント毎に指定する

  Cisco(config)# **username␣(アカウント)␣priviledge␣(ログインレベル)␣password␣(パスワード)**

  Cisco(config)# **line␣vty␣0␣4**

  Cisco(config-line)# **login␣local**

  - **priviledge**で指定したレベル以下の全てのコマンドが使える。

tacacs+サーバで指定する

- Cisco Secure ACSを用いて、tacacs+サーバを構築することが出来る。
- tacacs+サーバに設定したアカウント毎にログインレベル、及びパスワードを設定することが出来る。
- あとは、Cisco機器でtacacs+を使うように設定してください。

何故にtacacs+？？

- 複数ある機器のアカウント、及びパスワードを一元管理することができる。
- tacacs+サーバにおいて、カウント別でのイベントのログを採取することができる。
- レベル別で使えるコマンドを制限できる。
  →内部統制という観点でも必要では？？

Cisco機器Hands-On③

では、ここまでの内容を、実際に設定してみましょう。

Cisco機器Hands-On③ 設定内容

- 初期状態：Hands-On②終了時

- Level 0～15のアカウント／パスワードを設定する。
  アカウント：admintech_(レベルの数字)
  パスワード：cisco_(レベルの数字)
- 果たして、設定したレベルで入れますか？

さいごに....

- ご静聴、ありがとうございました。
- 次、これして欲しいとかあります？ありましたら、アンケートにお書きいただけますと助かります。
- 後日、質問があります場合には mailto:NetWork@ml.admintech.jp にMailをください。