

Cisco ルータ 入門

テクニカルコース

本講座が皆様のお役にたてれば幸いに存じます。

Contents

1 初期設定 2

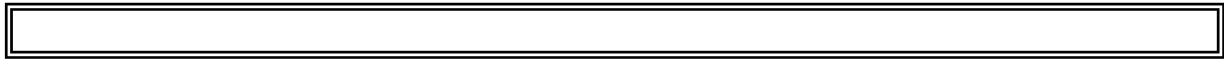
1.1	特権モードと非特権モード.....	2
1.2	特権モードと非特権モードの移行.....	3
1.3	メモリの種類と設定	4
1.4	コンフィギュレーションファイルの管理	5
1.5	設定モード.....	6
1.6	NETWORK INTERFACE の名称.....	8
1.7	NETWORK INTERFACE の設定方法	9
1.8	IOS と環境設定の管理.....	12
実習	Network Interface の設定.....	13

2 経路制御 15

2.1	ルーティング方法.....	15
2.2	静的経路制御（STATIC ROUTING）	16
2.3	動的経路制御（DYNAMIC ROUTING）	17
2.4	ルーティングプロトコルの分類.....	18
2.5	ルーティングアルゴリズム.....	19
2.6	静的経路情報の設定	20
2.7	経路情報の参照.....	22
2.8	動的経路情報（RIP） の設定	24
2.9	RIP VERSION 1 と RIP VERSION 2	26
2.10	参考コマンド	27
実習	静的経路設定	29
実習	動的経路設定	30

3 Router 管理入門 32

3.1	ISP の NETWORK の現状.....	32
3.2	ROUTER の環境設定	33
3.3	TELNET による環境設定	34



3.4	TFTP による環境設定	36
3.5	TFTP サーバと ROUTER の関係	38
実習	telnet を使用したルータとの接続	39

4 TFTP サーバ入門 41

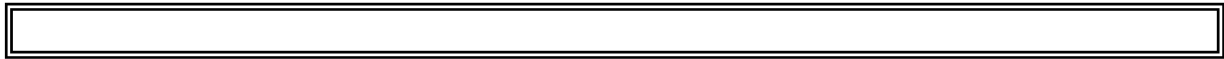
4.1	TFTP サーバ	41
4.2	TFTP サーバ の構成	42
	■ (inetd.conf の設定)	42
	■ ファイル転送先のディレクトリの作成	44
	■ hosts.allow の設定	45
	■ inetd の再起動	46
4.3	ルータから TFTP サーバへの書き出し	47
	■ 転送先のファイルを作成	47
	■ Router から TFTP サーバへ転送	48
4.4	TFTP サーバからルータへの読み込み	49
4.5	TFTP サーバ と ROUTER の関係	50
実習	TFTP サーバの構成	51
実習	ルータから TFTP サーバへのファイル転送	52
実習	TFTP サーバからルータへのファイル転送	52

5 syslog 管理 54

5.1	システムログ	54
5.2	LOG LEVEL について	56
5.3	SYSLOG サーバの構成	57
	■ Cisco ルータの設定	57
	■ syslog サーバの環境設定	58
	■ syslogd の起動	59
実習	ルータ log の収集	60

6 SNMP 管理 62

6.1	SNMP の歴史的変遷	62
6.2	SNMP 関連の RFC	63



6.3	SNMP で管理できる項目	64
6.4	SNMP の基本概念	65

7 SNMP 動作 67

7.1	基本動作プロトコル	67
7.2	SNMP の5つのコマンド	68
7.3	GET プロトコル動作 1	69
7.4	GETNEXT プロトコル動作 2	70
7.5	SET プロトコル動作 3	71
7.6	TRAP プロトコル動作 4	72

8 M I B 74

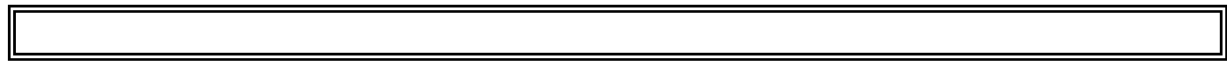
8.1	MIB と SMI	74
8.2	MIB	75
8.3	MIB の構造	76
8.4	MIB2 (RMON グループ)	77
8.5	標準 MIB と拡張 MIB	78

9 ネットワーク管理ツール 80

9.1	MRTG	80
9.2	HP OPENVIEW と SUN NET MANAGER	81
9.3	その他の管理ツール	82
9.4	SNMP による管理の問題点	83

10 MRTG 85

10.1	MRTG とは	85
10.2	MRTG SAMPLE	86
10.3	MRTG の構築	87
10.4	MRTG の導入	88
	■ libtool-1.3.4	88



	■ libjpeg.v6.....	89
	■ libpng-1.0.12	90
	■ gd-1.8.4.....	91
	■ mrtg-2.9.17.....	92
	■ Apache のインストール.....	93
10.5	対象ネットワーク機器の設定	94
10.6	MRTG の環境設定.....	95
	■ cfgmaker を使用して mrtg.cfg を作成	95
	■ cron の設定	96
	■ mrtg.cfg の設定変更	97
10.7	MRTG の応用.....	98
	■ Ping 応答計測	98
	■ 気象データ計測	99
実習	監視対象機器の設定	100
実習	MRTG の導入.....	101
実習	MRTG の環境設定.....	102

11 Security 104

11.1	環境設定の際のセキュリティ	104
11.2	パスワードの設定(1).....	105
11.3	パスワードの設定(2).....	107
11.4	問題点.....	108
	■ Telnet による環境設定の問題点	108
	■ Router のフィルタリング	109
	■ 踏み台サーバを利用する	111
	■ 電話回線を用いてバックドアを作り対応する	112
実習	アクセス設定	113
実習	踏み台サーバの設定	114
実習	アクセスリストの設定	115
実習	ダイヤルアップの設定	116

索引.....117

--

1 章 初期設定

1

初期設定

1.1 特権モードと非特権モード

Cisco ルータはモードによって使用できるコマンドレベルが異なります。

非特権モード（ユーザーモード）

Cisco IOS のデバイスのステータスを確認することのみができますが、パラメータの変更はできません。

Cisco IOS 上では プロンプトが「>」 で表記されています。

```
Router>
```

特権モード（enable モード）

パラメータの変更をすることが可能となります。

Cisco IOS 上では プロンプトが「#」 で表記されています。

```
Router#
```

特権モードでは、ユーザーモードより多くのコマンドを利用でき、設定の変更もできます。ユーザーモードから特権モードに移るためには、**enable** コマンドを実行します。このときパスワード入力を求められるのでシステム設定ダイアログで設定した **enable secret** のパスワードを入力します。この時入力したパスワードの文字列は画面に表示されません。パスワードが正しく入力されるとプロンプトが「#」に変わります。

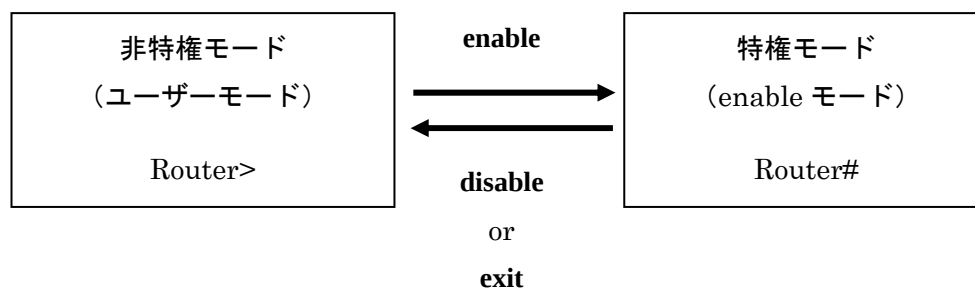
exit または **quit** コマンドを入力すると特権モードとユーザーモードどちらも抜けてルータからログアウトできます。

1.2 特権モードと非特権モードの移行

非特権モードから特権モードに移行するには **enable** コマンドを使用します。

ただし、非特権モードから特権モードの移行には **enable password** の入力が必要となります。

特権モードから非特権モードに移行するには **disable** コマンドまたは **exit** コマンドを使用します。



ただし、特権モードへの移行は
enable password が必要

特権モードでは、ユーザーモードより多くのコマンドを利用でき、設定の変更もできます。ユーザーモードから特権モードに移るためには、**enable** コマンドを実行します。このときパスワード入力を求められるのでシステム設定ダイアログで設定した **enable secret** のパスワードを入力します。この時入力したパスワードの文字列は画面に表示されません。パスワードが正しく入力されるとプロンプトが「#」に変わります。

exit または **quit** コマンドを入力すると特権モードとユーザーモードどちらも抜けてルータからログアウトできます。

1.3 メモリの種類と設定

Cisco ルータに搭載されているメモリには役割の異なる 3 種類のものがあります。

NVRAM

NVRAM は不揮発性メモリです。

Cisco IOS のイメージとスタートアップ時の設定（startup-config）が格納されます。

ルータの電源が入ると同時に NVRAM から RAM に設定情報がロードされます。

通常、管理者が設定を変更する場合には、RAM を変更しますので、次の起動時に、変更した情報で起動したい場合は、必ず NVRAM に設定を保存する必要があります。

RAM

RAM は揮発性メモリです。

実行中の Cisco IOS のイメージと実行中の設定（running-config）が格納されます。

ルータの起動時に Flash から IOS を、NVRAM から設定情報をロードします。すなわち RAM にロードされた情報でルータが動作しているわけです。RAM のロード情報には、ルーティングテーブルや ARP キャッシュ、アクティブなデバイス設定、また、それを動作させる IOS が含まれます。

しかし、電源を落とすと RAM の内容は、完全に消失します。通常のコンピュータのメモリと同様のイメージです。

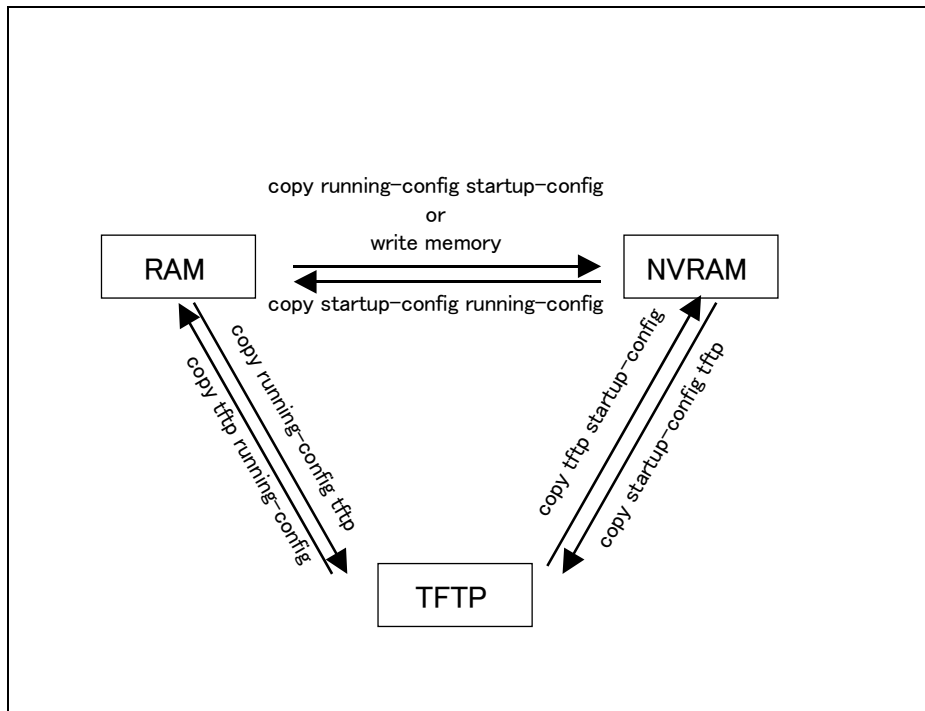
変更した情報を保存したい場合は、必ず NVRAM または TFTP サーバに設定を保存する必要があります。

Flash

Flash には Cisco IOS のイメージとスタートアップ時の設定（startup-config）が格納されます。Flash の容量や機種にもよりますが、1 つのデバイスに複数の IOS を保存することも可能です。また、フラッシュメモリの内容は、電源を落としたときや再起動したときも保持されます。フラッシュメモリの内容は、`show flash` コマンドで表示します。

1.4 コンフィギュレーションファイルの管理

各メモリに格納されたコンフィギュレーションは、IOS コマンドでコピーし管理します。



copy running-config startup-config

RAM 内のアクティブな設定を NVRAM へ保存します。

copy startup-config running-config

NVRAM に保存してある設定を RAM 内へ読み込みます。

copy running-config tftp

RAM 内のアクティブな設定を TFTP サーバへ保存します。

copy tftp running-config

TFTP サーバへ保存してある設定を RAM 内へ読み込みます。

copy startup-config tftp

NVRAM に保存してある設定を TFTP サーバへ保存します。

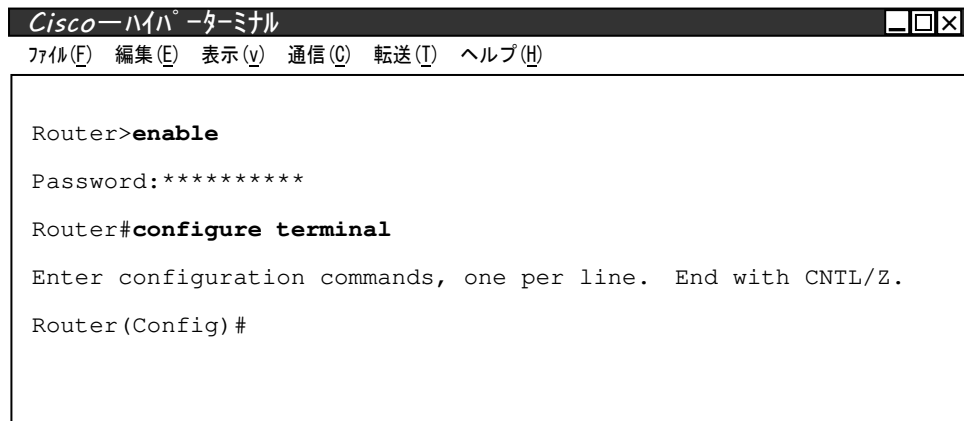
copy tftp startup-config

TFTP サーバへ保存してある設定を NVRAM に保存します。

1.5 設定モード

特権モードの Exec コマンド **configure** と入力すると、Cisco ルータを設定モードになります。この **configure** コマンドは、何を元に設定するかというコマンドです。

Cisco ルータで設定を行う場合、特権モード（enable モード）で **configure** を使用します。



```
Cisco - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(Config)#
```

ここで設定された内容は、直ちに「running-config」に反映されます。特にリモートで環境設置をする場合は十分に注意が必要です。例えば、アクセスリスト等の変更には細心の注意が必要です。

「startup-config」には反映されません。設定した内容を保存する場合は、「**copy running-config startup-config**」、または「**write memory**」が必要です。

configure コマンドには次の 3 種類の方法があります。

■ **configure terminal**

ターミナル（端末）から設定する場合に指定します。通常設定する場合は必ずと言っていいほど使用するコマンドです。

■ **configure memory**

NVRAM の設定を RAM にロードする場合に指定します。設定変更をした RAM の状態を起動時の状態に戻すときに、この指定をします。

■ **configure network**

TFTP の設定を RAM にロードする場合に指定します。あらかじめ TFTP に指定情報を用意している場合などに指定します。

configure コマンドを実行すると、引数を聞かれますので、デフォルトの値である [terminal] に設定します。最初から **configure terminal** を入力すると、1 回の入力で端末（terminal）からの設定を選択したことになります。ほとんどの場合、**configure terminal** のみしか使いません。

1.6 Network Interface の名称

Cisco ルータは Network Interface を増設することが可能なため、Network Interface の種類（規格）とボードにより Interface の名称が決まります。

<u>Network Interface 名+ Slot/port</u>	<u>名前付け方法</u>
Ethernet0/0	10Base-T の Ethernet ボードのうち、最も小さい番号の Slot に差し込まれている Ethernet ボードの 1 番 Port
Ethernet0/1	その次の Port
Ethernet1/3	10Base-T の Ethernet ボードのうち、2 番目に小さい番号の Slot に差し込まれている Ethernet ボードの 4 番 Port
Fddi0/2.....	FDDI ボードうち、最も小さい番号の Slot に差し込まれている FDDI ボードの 3 番 Port
Serial0/1	Serial ボードうち、最も小さい番号の Slot に差し込まれている Serial ボードの 2 番 Port

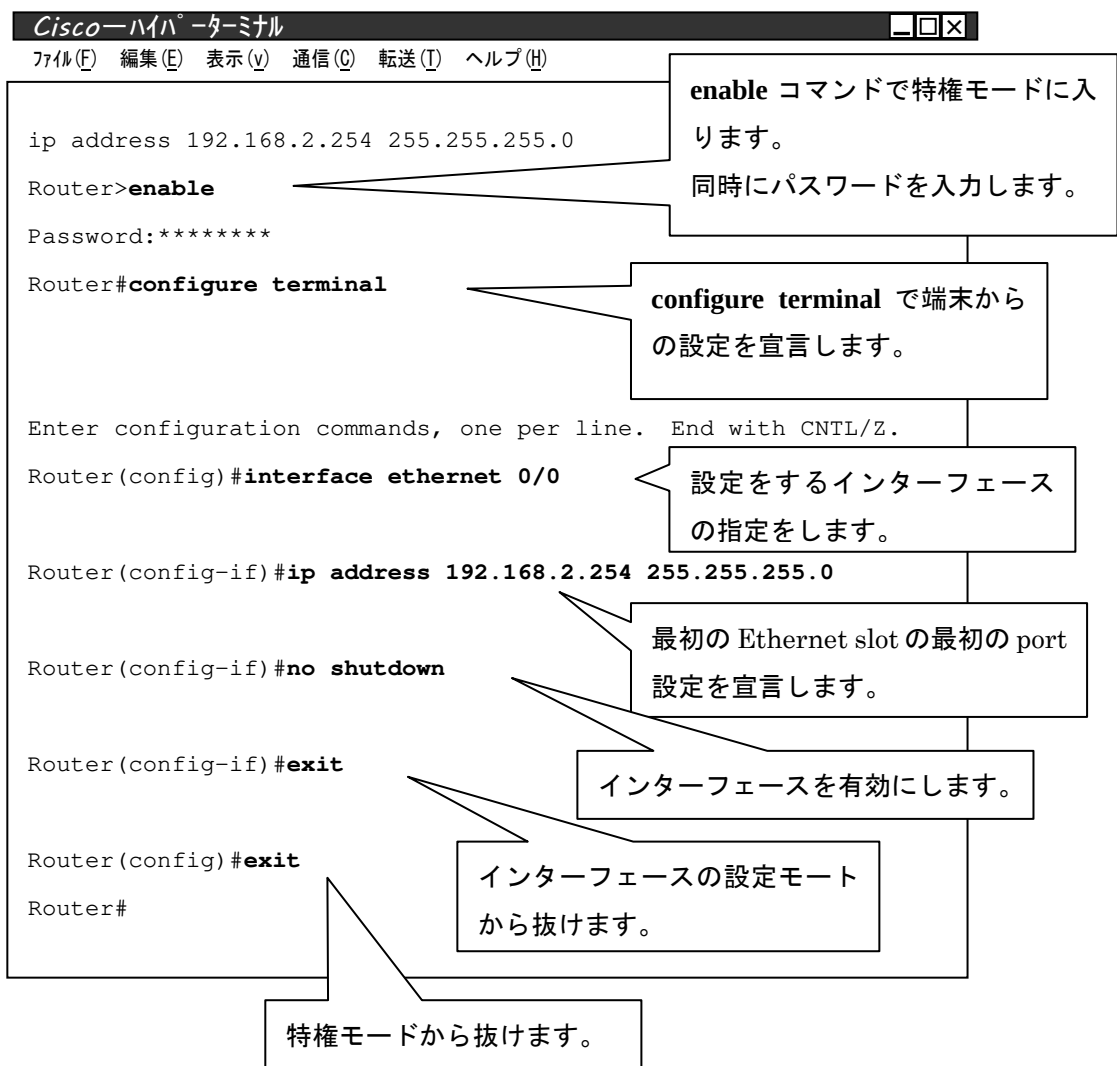
ただし、同一機能の場合は規格が異なっても同じ名称になる場合があります。

AUI → Ethernet

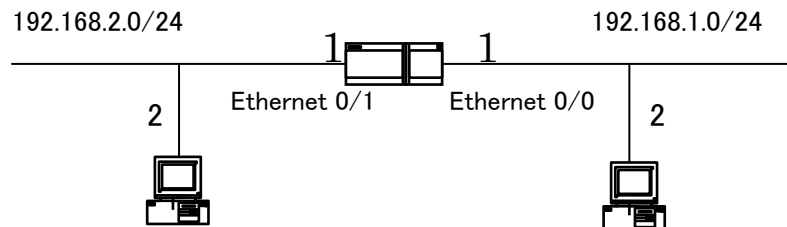
1.7 Network Interface の設定方法

各 Network Interface の ip address の設定は、各 Network Interface の環境設定モード(**configure** モード) にて次のように行います。

no shutdown コマンドはその Network Interface を有効にするコマンドです。



設定例



```

Cisco - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface ethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router(config)#interface ethernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
Router#

```

設定が次回起動時にも反映するように RAM から NVRAM にコピー・保存します。



Cisco-ハイパーターミナル [最小化] [最大化] [閉じる]

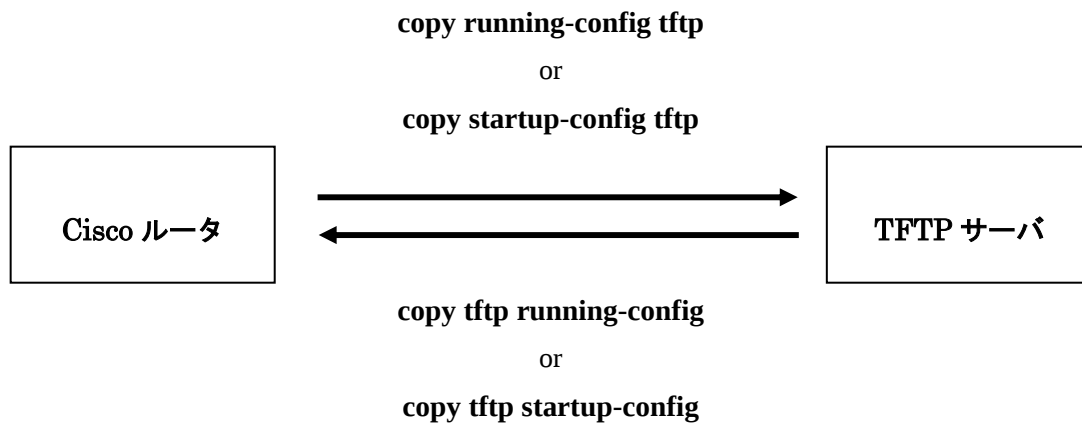
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

```
running-config:
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
ip address 192.168.2.1 255.255.255.0
!
```

1.8 IOS と環境設定の管理

Cisco ルータは基本的に Diskless System です。そこで、

- ① 必要なファイル（IOS、Config File ）は内蔵のメモリ（ NVRAM ）に記録されます。
- ② しかし障害発生時に必要なファイルが破壊、もしくは消失する可能性があります。
- ③ そのため上記②の対策として tftp を用いて、Cisco ルータ から TFTP サーバにファイルを書き出し、保存を行い、必要に応じてアップロードする作業が発生します。



ちなみに、Diskless なシステムの場合、tftp を用いて管理をおこなう場合が多いものです。

 練習

Network Interface の設定

IP Address などの情報はインストラクターから得ます。

1. オペレータのコンソールから Cisco ルータに接続します。
2. テキストを参考に「enable モード」にします。
3. インターフェースに、IP Address を設定します。（設定するインターフェースと使用する IP Address はインストラクターから指示されます。）
4. インターフェースを有効にします。
5. 設定が完了したら「ユーザーモード」に抜けます。

 確認

ルータを再起動してターミナルのルータ起動画面を確認します。



2 章 経路制御

2

経路制御

2.1 ルーティング方法

ルーティング方法には次の二種類があります。

- 1 **スタティックルーティング**（静的ルーティング）
管理者が手動でルーティングテーブルを作成します。
- 2 **ダイナミックルーティング**（動的ルーティング）
機器が自動的にルーティングテーブルを作成します。

スタティックルートの設定には **ip route** コマンドを使い、パラメータには、送信先のネットワークアドレスとマスク、送信先への経路にあるネクストホップのアドレスもしくは、**interface** を指定します。

現在の IP ルーティングテーブルを表すコマンドは **show ip route** です。パラメータを指定することで特定の経路についてのみの情報を表示できます。

ネットワーク全体にスタティックルートを使用していると、管理者の手間がかかるだけでなく、停電やネットワーク構成に変更が起こったときにすぐに対応することはできません。このような心配をなくすため、ダイナミックルーティングプロトコルが開発されました。

2.2 静的経路制御 (Static Routing)

静的経路制御 (Static Routing) とは管理者が手動で経路制御を設定する方法です。

メリットとして

- ・ ルータ間でのルーティング情報交換が必要ないため帯域の消費を抑えられます。
- ・ ルータは設定されたルート以外知らないため、他のユーザがアクセスすべきでないリソースを遮断することが可能となり、セキュリティの 1 手段として利用できます。
- ・ 他のルータの影響を受けません。

デメリットとして

- ・ ネットワークトラブルの際、自動的に回避することができません。(フォールトトレラントではありません)
- ・ ネットワークの構成が変更された場合、各ルータの設定を管理者が行わなければなりません。設定箇所が膨大の場合、管理者に多大な負担となります。
- ・ そのためネットワークが大規模になると管理が困難です。

使用例

- ・ 経路が 1 つしかない環境で使用されます。
- ・ ダイヤルアップ環境に利用されます。
- ・ サーバの経路情報に利用されます。
- ・ デフォルトルートの設定に使用します。
- ・ Network の増設が少ない場合に使用します。

2.3 動的経路制御 (Dynamic Routing)

動的経路制御 (Dynamic Routing) とは、ネットワークの構成変更に対して自動的にルータの持つ経路情報に変更をかけ常に最適経路に解決する方法です。(AS (Autonomous System) 自律システムを実現する1手法です。自律システムとは、共通の経路情報を共有し1つの管理実体のもとに存在するネットワークの集まりのことです。)

動的経路制御に設定したルータは通信可能な経路情報を維持し最適経路を解決するために、他のルータと通信し経路情報を交換します。この最適経路を解決するために使用するプロトコルがルーティングプロトコルです。

メリットとして

- ・ルーティング情報を自動的に最新のものへ書き換えることができるため常に最適なルーティングを行うことができます。
- ・管理者によるルーティング管理が軽減されます。
- ・あて先までに複数経路が存在する場合にネットワーク障害が発生した場合でもルータ間で自動的にルーティングテーブルを更新でき、通信可能です。(フォールトトレラントなシステムです。)

デメリットとして

- ・ルータ間で流れるルーティング情報のためネットワークに負担がかかります。
- ・他のルータからの経路情報に影響を受けます。

使用例

- ・大規模ネットワーク (OSPF、RIP) に利用されます。
- ・インターネット (BGP) に利用されます。
- ・ルータに利用されます。

2.4 ルーティングプロトコルの分類

TCP/IP スイートでは何種類ものルーティングプロトコルが定義されています。ルーティングプロトコルはその用途によって大きく二つに分けられます。

自律システム内部でのルーティングを実行する Interior Gateway Protocol と、複数の自律システム間のルーティングを実行する Exterior Gateway Protocols です。

組織内ルーティングプロトコル IGP(Interior Gateway Protocols)

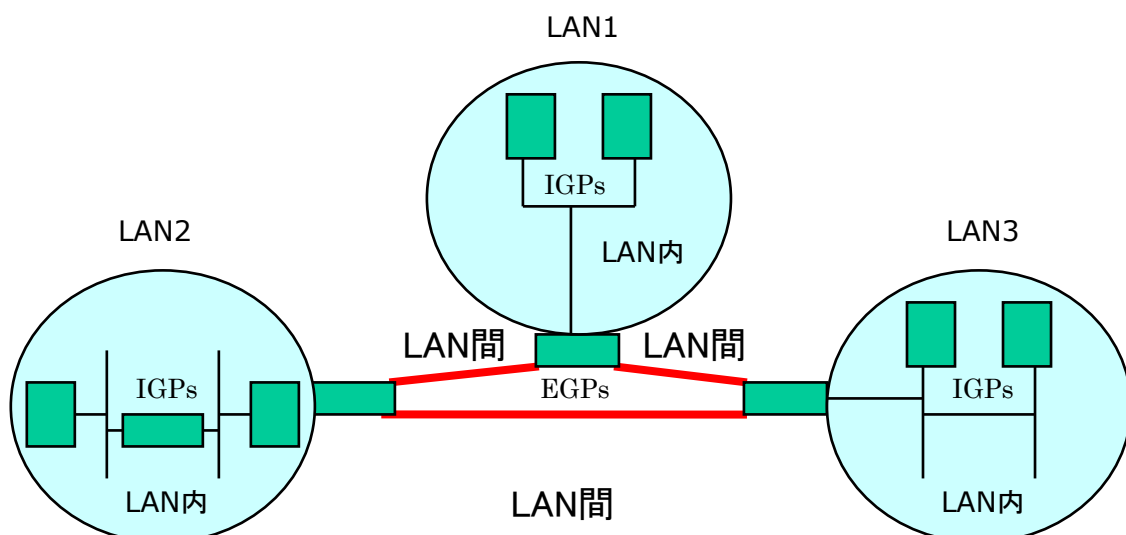
企業内ネットワークのような同じ管理機関や所轄機関におけるネットワーク（自律システム）内で使われます。

代表的なプロトコル：RIP (Routing Information Protocol) OSPF (Open Shortest Path First)
IGRP(Interior Gateway Routing Protocol) EIGRP(Enhanced IGRP)

組織間ルーティングプロトコル EGP(Exterior Gateway Protocols)

複数の自律システム間のルーティングを実行します。いわゆる“インターネット”で使われます。

代表的なプロトコル：BGP (Boarder Gateway Protocol) EGP (Exterior Gateway Protocol)



2.5 ルーティングアルゴリズム

ルーティングプロトコルは最適経路解決の実現方法の違いにより以下に説明するタイプとそれぞれの特徴を兼ね備えたハイブリッドタイプに区別できます。

	ディスタンスベクター型	リンクステート型
特徴	途中経由するネットワーク数を数えて、最も少ないルートを選択する。 ↓ <i>距離と方向で判断＝道路標識型</i>	ルータがネットワーク構成情報を持ち、最適ルートを選択する。 ↓ <i>地図（構成図）により判断＝道路地図型</i>
方式	ルータ間でネットワークの方向と距離に関する情報をやりとりする。	ルータがネットワーク全体の構成を理解してルーティングテーブルを作成する
メリット	ルートを決定するのにルータ数しか見ないので比較的簡単な方法である。	ネットワークが複雑になっても各ルータは正しい経路情報を持ち、安定した経路制御が可能
デメリット	ネットワークの構造が複雑な場合、経路制御情報が安定するまで時間がかかり、経路にループが発生するなどの問題点がある	経路情報の処理にはルータに高性能の CPU とメモリが必要
プロトコル	RIP・RIP2	OSPF

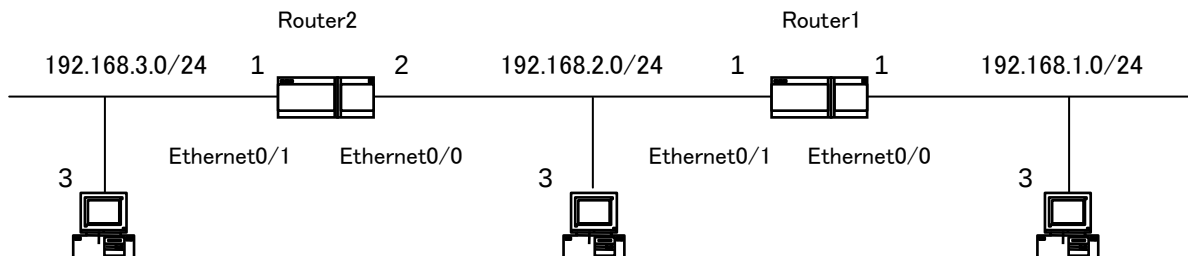
2.6 静的経路情報の設定

静的経路情報（Static Routing）として設定する例を以下に示します。

設定コマンドの書式は

ip route 宛て先のネットワークアドレス パケットの投げ先のアドレス

です。



Router 1

Cisco ハイパターミナル

ファイル(F) 編集(E) 表示(V) 通信(C) 転送(I) ヘルプ(H)

```

Router1>enable
password:*****
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
Router1(config)#exit
Router1#copy running-config startup-config
Router1#exit
Router1>
  
```

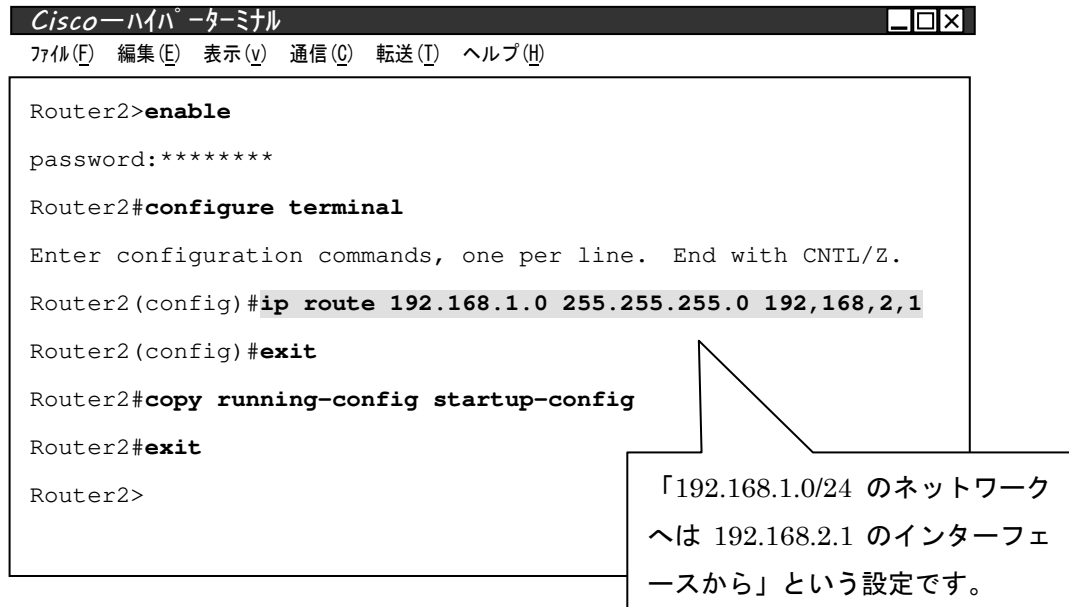
特権モードに入ります。

ターミナルからの設定を宣言します。

「192.168.3.0/24 のネットワークへは192.168.2.2のインターフェースから」という設定です。

設定変更がすんだ後は次回起動時にも設定が反映するように RAM から NVRAM へ設定情報をコピーしておきます。

Router 2



```
Cisco - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router2>enable
password:*****
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
Router2(config)#exit
Router2#copy running-config startup-config
Router2#exit
Router2>
```

「192.168.1.0/24 のネットワークへは 192.168.2.1 のインターフェースから」という設定です。

2.7 経路情報の参照

経路情報を参照コマンドは

show ip route

です。パラメータを指定することで特定の経路についてのみの情報を表示できます。

前ページの二台のルータでは、それぞれ以下のようなルーティング情報を持っています。

Router 1

```

Cisco - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router1>enable
password:*****

Router1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static
P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Ethernet0/0
C    192.168.2.0/24 is directly connected, Ethernet0/1
S    192.168.3.0/24 [1/0] via 192.168.2.2

Router1#exit
Router1>

```

あて先へのルーティング情報がない場合のあて先は設定されていません。

192.168.1.0/24 のネットワークへは Ethernet0/0 のインターフェースが、192.168.2.0/24 のネットワークへは Ethernet0/1 のインターフェースが、それぞれ接続しています。

192.168.3.0/24 のネットワークへは 192.168.2.2 のインターフェースから経由する静的経路設定があります。

Router 2

Cisco ハイパーターミナル

ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

```

Router2>enable
password:*****
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODP
P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.2.0/24 is directly connected, Ethernet0/0
C    192.168.3.0/24 is directly connected, Ethernet0/1
S    192.168.1.0/24 [1/0] via 192.168.2.1
Router2#exit
Router2>

```

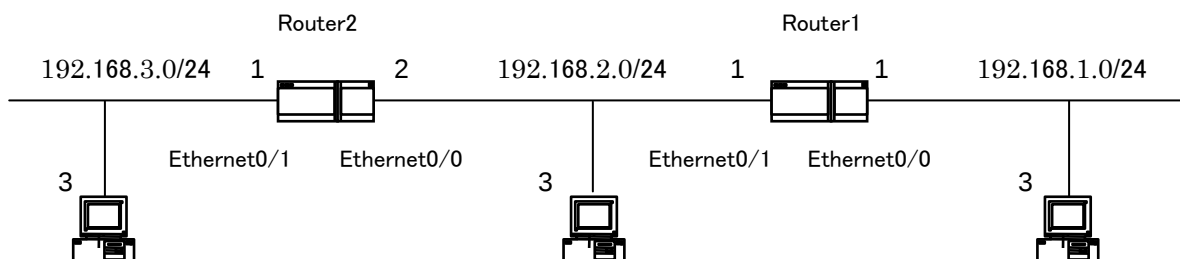
あて先へのルーティング情報がない場合のあて先は設定されていません。

192.168.2.0 / 24 のネットワークへは Ethernet0/0 のインターフェースが、192.168.3.0 / 24 のネットワークへは Ethernet0/1 のインターフェースが、それぞれ接続しています。

192.168.1.0/24 のネットワークへは 192.168.2.1 のインターフェースから経由する静的経路設定があります。

2.8 動的経路情報（RIP）の設定

RIP を例にして動的経路設定をします。



動的経路情報（RIP）として設定する例を以下に示します。

router rip	動的経路情報プロトコルで RIP を使用します
version 2	RIP version 2 を使用します
network	広報するネットワークアドレスを表記します

Router 1

```

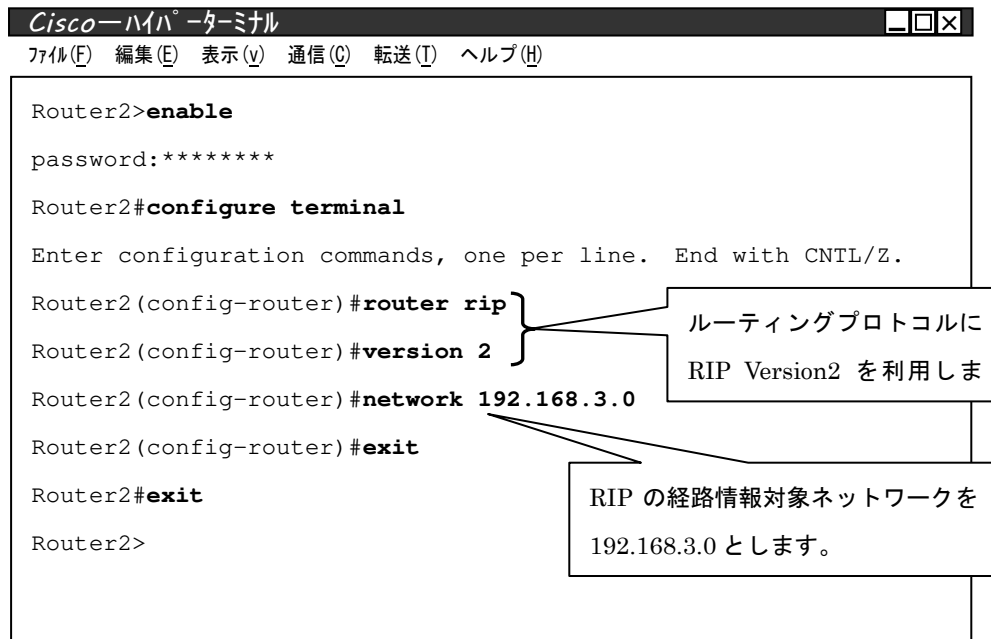
Cisco-ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router1>enable
password:*****
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config-router)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 192.168.1.0
Router1(config-router)#exit
Router1#exit
Router1>
  
```

ルーター1のCLI操作ログと解説:

- `Router1>enable`: 特権モードに入ります。
- `password:*****`: パスワードを入力します。
- `Router1#configure terminal`: 設定モードに入ります。
- `Router1(config-router)#router rip`: ルーティングプロトコルにRIPを使用します。
- `Router1(config-router)#version 2`: RIP Version 2を利用します。
- `Router1(config-router)#network 192.168.1.0`: RIPの経路情報対象ネットワークを192.168.1.0とします。
- `Router1(config-router)#exit`: 設定モードを終了します。
- `Router1#exit`: 特権モードを終了します。
- `Router1>`: 実行モードに戻ります。

Router 2



```
Cisco-HyperTerminal
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router2>enable
password:*****
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config-router)#router rip
Router2(config-router)#version 2
Router2(config-router)#network 192.168.3.0
Router2(config-router)#exit
Router2#exit
Router2>
```

ルーティングプロトコルに
RIP Version2 を利用しま

RIP の経路情報対象ネットワークを
192.168.3.0 とします。

2.9 RIP version 1 と RIP Version 2

RIP はメトリックとしてネットワーク経路上にあるルータの数（ホップ数）を使用するディスタンスベクタ方式のルーティングプロトコルです。

Version1 と Version2 の違いは、Version1 がクラスフルのルーティングプロトコルでネットマスク情報を伝えないこと、Version2 がクラスレスのプロトコルで CIDR（Classless Interdomain Routing）・VLSM（可変長サブネットマスク）・経路集約に対応していることです。

Cisco ルータでは **router rip** コマンドで RIP が使用可能になります。Version 設定には **version** コマンドを使用しパラメータとして 1 または 2 を指定します。指定しない場合には RIP Version1 の経路情報を送信し、Version1 と 2 の両方の更新を受信します。

RIP Version 1 と Version2 を比較

RIP Version 1 は	Classless に非対応です
RIP Version 2 は	Classless に対応しています

↓

RIP Version 1 は RIP Version 2 のすべてを理解できるわけではありません。

↓

そのため混在している場合、トラブルになる可能性があります。

対応方法

各 Network Interface で対応できるようにします。

ip rip send version 1 2

ip rip receive version 1 2

この方法はそれぞれのインターフェースごとに設定でき、また、グローバル設定コマンドで指定したバージョンより優先します。

注意

Cisco ルータで classless を使用する場合は **ip classless** の設定が必要です。
classless で扱う場合が多いので、基本的に設定していても問題はないでしょう。
しかし、設定した場合、必ず RIP Version 2 を指定しましょう。

2.10 参考コマンド

以下は Cisco ルータの設定によく使用するコマンドです。

hostname ホストネームを設定する

```
Router(config)#hostname hoge hoge  
hoge hoge(config)#
```

ip subnet-zero subnet zero を使用できるようにする

```
Router(config)#ip subnet-zero
```

Subnet zero とはサブネット指定をするときに「ネットマスクのビットがすべてゼロである先頭のネットワーク」を使用しない場合に利用するコマンドです。

clock timezone タイムゾーンの設定

```
Router(config)#clock timezone JST 9
```

timeZone はグリニッジ標準時を基準とするため、日本標準時で表示するには JST 9 (Japanese Standard 9)を指定します。

ip domain-name ドメイン名の設定

```
Router(config)# ip domain-name ico-g.com
```

ip name-server ネームサーバの設定(複数設定可能)

```
Router(config)#ip nam-server 210.134.161.66
```

ntp server ntp サーバの設定

```
Router(config)#ntp server 210.134.161.66
```

Network Time Protocol を使用して他の NTP デバイスとの関連性を定義づけします。Cisco ルータは NTP クライアントにも NTP サーバにも設定できます。設定例では IP アドレス 210.134.161.66 のホストと従属的な時刻の同期をとっています。

ip classless classless の設定

```
Router(config)#ip classless
```

show interface 各 Network Interface の状態の確認（Interface の指定も可能）

```
Router#show interface
```

show running-config 現在の環境設定の確認

```
Router#show running-config
```

show ip route 現在の経路情報の確認

```
Router#show ip route
```

パラメータを指定することで特定の経路情報のみ表示が出来ます。

```
Router#show ip route connected
```

直接接続され動作可能なインターフェースによって学習された経路のみ表示できます。

```
Router#show ip route static
```

手動で設定された経路のみ表示できます。

```
Router#show ip route <IP Address>
```

指定したネットワークアドレスの経路に関連した情報のみ表示できます。

実習**静的経路設定**

1. インストラクターから指示されたターゲットネットワークへの静的ルートを設定します。

確認

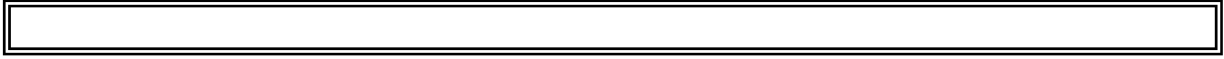
-
2. 設定したルートを確認します。

実習**動的経路設定**

3. インストラクターから指示されたターゲットネットワークへの rip を使用したルートを設定します。

確認

-
4. 設定したルートを確認します。

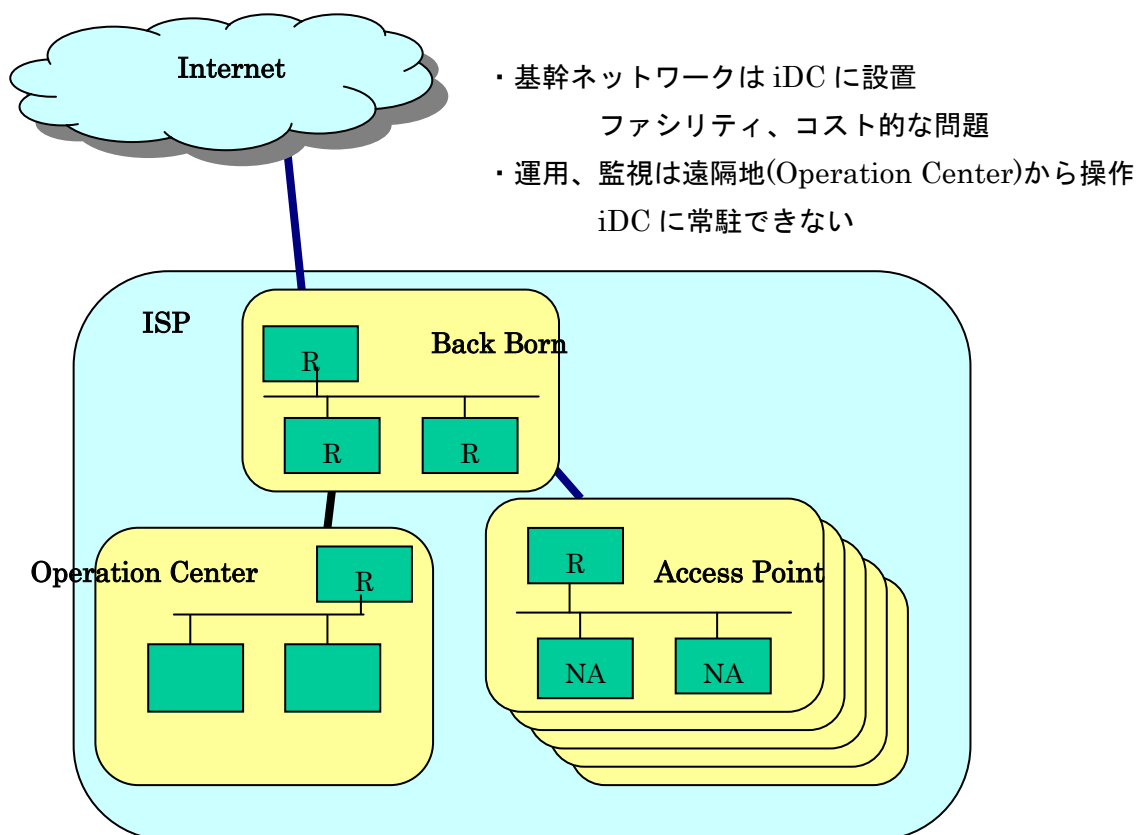


3 章 Router 管理入門

3

Router 管理入門

3.1 ISP の Network の現状



ISP の Network の現状は、上図に示すとおりです。

基幹ネットワークはファシリティ、コスト的な問題から iDC に設置しています。

運用、監視は「iDC に常駐できない」という理由から、遠隔地(Operation Center)からリモート操作をしています。

3.2 Router の環境設定

Router の環境設定方法は、

- ① 期設定時や障害時に現場で環境設定に用いるコンソールからの環境設定と、
- ② 運用・監視時に telnet で遠隔地からリモートで接続する方法、
- ③ 運用・監視時に ftp で遠隔地からリモートで接続する方法、

の三つです。

運用、監視は遠隔地から telnet または tftp でリモート接続して行う方法が基本です。

コンソールからの環境設定は初期設定時または障害時のみ、ターゲットルータにローカル接続して行いましょう。

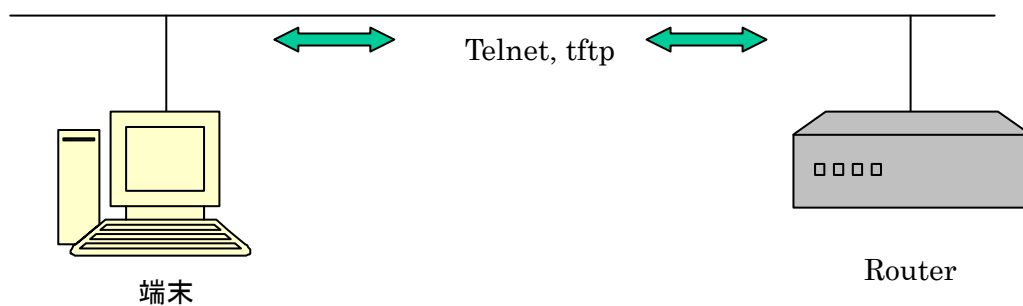
Router の環境設定方法

- | | | |
|---|----------------|------------|
| ① | コンソールからの環境設定 | 現場での環境設定 |
| ② | telnet による環境設定 | 遠隔地からの環境設定 |
| ③ | tftp による環境設定 | 遠隔地からの環境設定 |



運用、監視は遠隔地から行う方法が基本

- ② telnet による環境設定
- ③ ftp による環境設定



コンソールからの環境設定は初期設定、障害時のみ

3.3 Telnet による環境設定

Cisco ルータを Telnet でリモート管理できるように設定します。

- ① **enable** コマンドで特権モードに入ります。
- ② ターミナルからの設定モードにします。
- ③ **line** コマンドで telnet からの接続数の設定をします。
- ④ **login** コマンドで telnet からの接続有効化設定をします。
- ⑤ **password 0** コマンドで telnet からの接続時に使用するパスワードを設定します。可能な
らば User を設定したほうがよいでしょう。
- ⑥ パスワードの暗号化設定をします。
- ⑦ 設定変更を次回起動時にも反映するために環境設定を保存します。

Cisco ルータで Telnet を使用するための環境設定の例を以下に示します。

The screenshot shows a Cisco Hypertext Terminal window with the following commands and callouts:

```

Router>enable
Password:*****
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#passwd 0 *****
Router(config-if)#exit
Router(config)#service password-encryption
Router(config)#exit
Router#copy running-config startup-config
Router#
  
```

Callouts (日本語):

- telnet で接続できる端末の数 (この場合、5 接続まで可)
- telnet で接続できるように許可するコマンド
- telnet で接続する場合のパスワード
- 可能ならば User を設定した方がいい
- password を暗号化。前もって設定してある場合、自動的に暗号化する。
- 環境の保存

注意

telnet を使用する場合、注意しなければならないこととして、

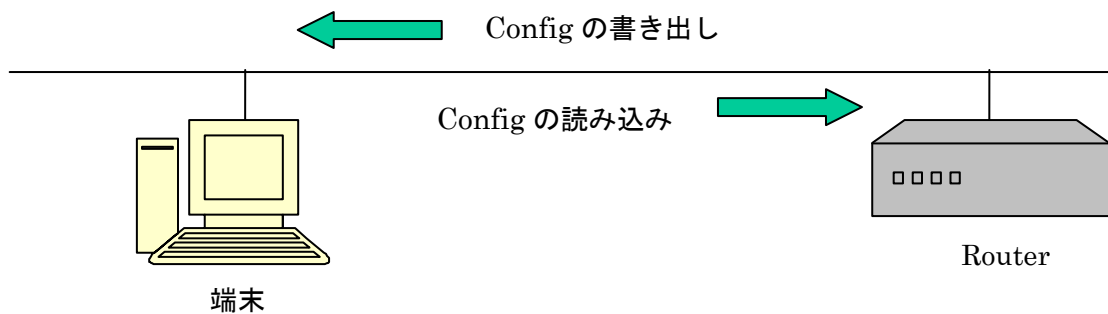
- ① telnet による環境設定がデフォルトでは使用できない Router が多いことです。Cisco ルータはデフォルトでは telnet 接続が不可能となっています。
- ② 特定のオペレータにのみアクセスを許すため password の設定が必須となります。また password を設定した場合必ず暗号化することを心がけます。telnet の場合、暗号化していない password はそのままテキストで流れるので第三者が読み取ることが可能です。そのため Security 的な対策が必要となります。
- ③ 予期しない者からのアクセスをさせない為にアクセスできる端末を制限します。
(アクセスリスト)
- ④ 同様に予期しない第三者からのアクセスさせない為に Internet からの接続もできないようにします。

などがあります。

参考) Juniper などは ssh (Secure Shell) での接続が可能となっています。

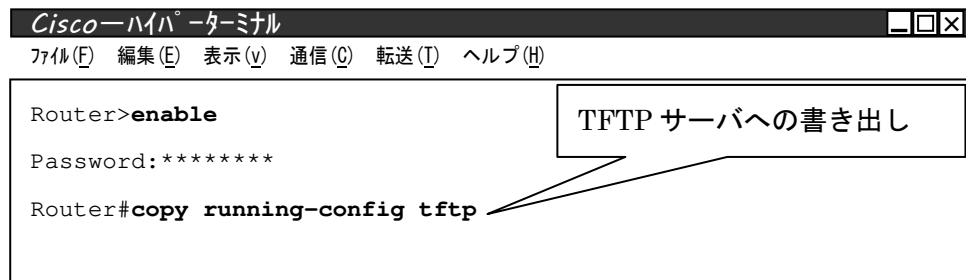
3.4 TFTP による環境設定

Cisco ルータの環境設定は **copy** コマンドを使用してファイルとして保存できます。保存先はルータ内部の NVRAM だけでなく、ネットワーク上に用意した TFTP サーバに保存できます。また **copy** コマンドは TFTP サーバから Cisco ルータへ環境設定ファイルの読み込みにも利用できます。



Cisco ルータで tftp を使用した環境設定の例を以下に示します。

リモートルーターから Config を書き出すには



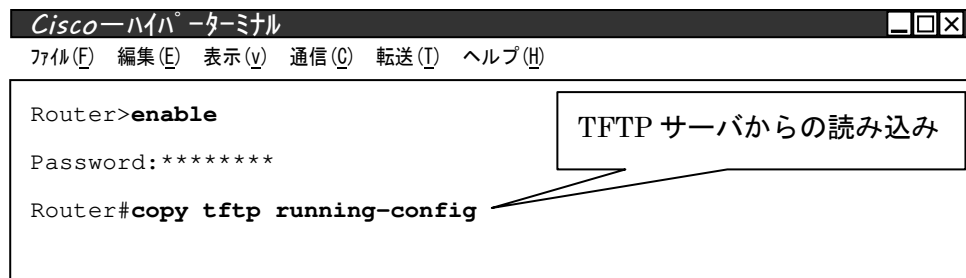
The image shows a Cisco HyperTerminal window with the title "Cisco ハイパーターミナル". The menu bar includes "ファイル(F)", "編集(E)", "表示(V)", "通信(C)", "転送(T)", and "ヘルプ(H)". The terminal text shows the user entering "enable" and a password, then the command "copy running-config tftp". A callout box points to the "tftp" part of the command with the text "TFTP サーバへの書き出し".

```
Cisco ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#copy running-config tftp
```

とします。

リモートルーターへ Config を読み込むには、



The image shows a Cisco HyperTerminal window with the title "Cisco ハイパーターミナル". The menu bar includes "ファイル(F)", "編集(E)", "表示(V)", "通信(C)", "転送(T)", and "ヘルプ(H)". The terminal text shows the user entering "enable" and a password, then the command "copy tftp running-config". A callout box points to the "tftp" part of the command with the text "TFTP サーバからの読み込み".

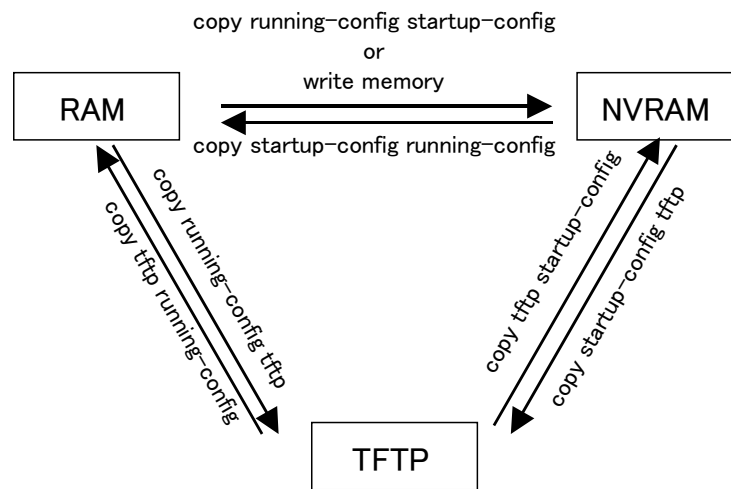
```
Cisco ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#copy tftp running-config
```

とします。

3.5 TFTP サーバと Router の関係

以下に TFTP サーバ と Router の関係 を図示します。



実習**telnet を使用したルータとの接続**

ユーザー名・パスワード設定についてはインストラクターから情報を得ます。

1. Cisco ルータで Telnet を受付ける設定にします。
2. 任意のホストから Telnet を使って接続します。

確認



4 章 TFTP サーバ 入門

4

TFTP サーバ入門

4.1 TFTP サーバ

TFTP サーバ とは、

- ・ ファイル転送用のプロトコル TFTP(Trivial File Transfer Protocol)を使用したサーバです。
- ・ FTP の簡易版で比較的に簡単に使用することができます。
- ・ 認証なしでファイル転送を行うプロトコルですからセキュリティ的に問題があります。
- ・ サーバ側は必要なとき以外は起動しないようにすることが重要です。
- ・ inetd 経由での起動するシステムです。
- ・ Tcp-Wrapper でのアクセス制御は可能です。(inetd 経由であるため)
- ・ 基本的に POSIX 互換 OS に標準で付属しているため、簡単に使用できます。

4.2 TFTP サーバ の構成

コンピュータを TFTP サーバとして構成するための設定手順を以下に述べます。

■ (inetd.conf の設定)

次のように inetd.conf を変更します。これによって tftpd を有効にします。

作業内容は inetd.conf 内にある tftp 設定の行のコメントアウト(#)をはずすことです。

変更前の inetd.conf (FreeBSD 4.2)の一部

```
Kterm  inetid.conf
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

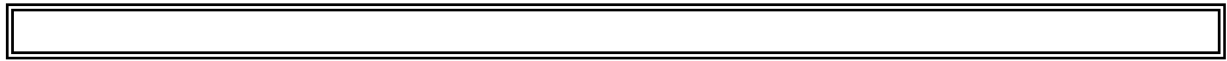
#comsat dgram udp wait tty:tty /usr/libexec/comsat comsat
#ntalk dgram udp wait tty:tty /usr/libexec/ntalkd ntalkd
#tftp dgram udp wait nobody /usr/libexec/tftpd tftpd /tftpboot
#bootps dgram udp wait root /usr/libexec/bootpd bootpd
```

変更後の inetd.conf (FreeBSD 4.2)の一部

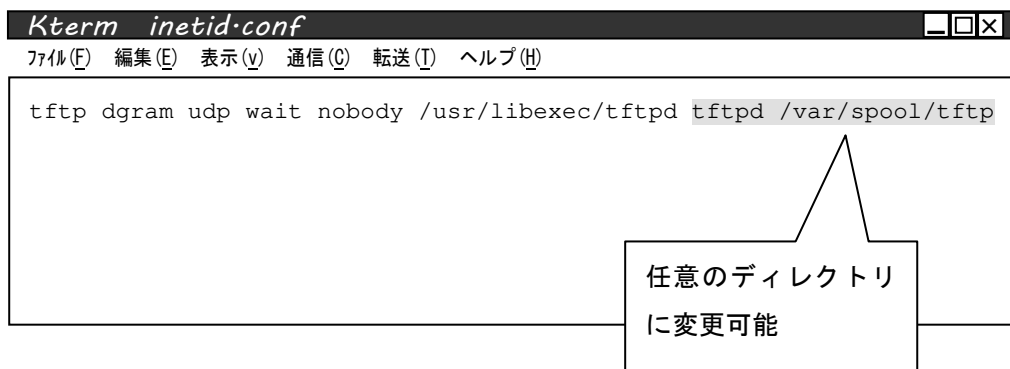
```
Kterm  inetid.conf
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

#comsat dgram udp wait tty:tty /usr/libexec/comsat comsat
#ntalk dgram udp wait tty:tty /usr/libexec/ntalkd ntalkd
tftp dgram udp wait nobody /usr/libexec/tftpd tftpd /tftpboot
#bootps dgram udp wait root /usr/libexec/bootpd bootpd
```

コメントアウト”#”をとる。

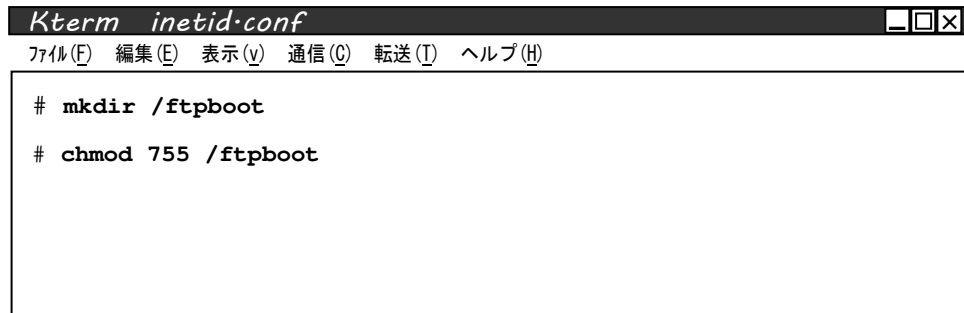


この設定では転送されたファイルは/tftpbootの中に收容されます。收容するディレクトリは任意のディレクトリに変更可能です。例えば、root directory を/var/spoop/tftp にしたい場合、次のようになります。



■ ファイル転送先のディレクトリの作成

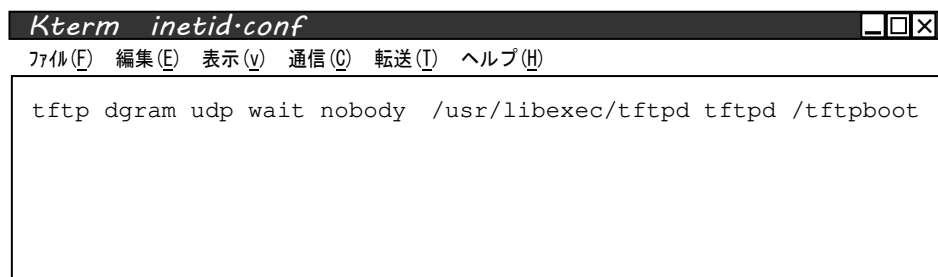
inetd.conf を変更したら、以下に示すコマンドを使用して、今回の設定に適した転送先の Directory の作成します。permission は 755 に設定します。



```
Kterm inetid.conf
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

# mkdir /ftpboot
# chmod 755 /ftpboot
```

今回の設定 inetd.conf の変更内容をもう一度確認しておきましょう。



```
Kterm inetid.conf
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

tftp dgram udp wait nobody /usr/libexec/tftpd tftpd /tftpboot
```

注意事項

- ・Directory の permission は 755 に設定します。777 が最も簡単ですが、セキュリティ的に問題があるので 777 には設定しないようにします。
- ・Owner は root、Group は wheel とします。
- ・作業は root で行います。

■ hosts.allow の設定

セキュリティ確保のために/etc/hosts.allow の設定は必須です。以下に設定例を示します。

/etc/hosts.allow の設定例

```

Kterm inetid.conf
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

:
tftpd : 192.168.1.1 : allow
tftpd : 192.168.2.0/255.255.255.0 : allow
:
ALL : ALL : deny
  
```

以下は注意事項です。

- ・ セキュリティ的に TFTP サーバは問題があるので、必要なホスト以外からのアクセスはさせるべきではありません。つまり、Network ではなく、Host でアクセス制御を行うべきです。
- ・ アクセス制御は/etc/hosts.allow のファイルを保存すれば可能となります。
- ・ 他に tcp_wrapper を使用するアプリケーションがある場合、その部分もきちんと書く必要があります。もし書かない場合、その機能が使えなくなります。
- ・ 最後の行 ALL:ALL:deny は必須です。忘れないようにしましょう。

■ inetd の再起動

すべての設定が終了したら、inetd を再起動して変更を反映します。

inetd の起動には以下のコマンドを使用します。

```
# killall -HUP inetd
```

次に TFTP サーバ の起動を確認します。コマンド `netstat -a` を実行して tftp と書かれた行があることを確認します。

```

> netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 0 *.pop3 *.* LISTEN
tcp4 0 0 *.1023 *.* LISTEN
tcp4 0 0 *.ssh *.* LISTEN
tcp4 0 0 *.smtp *.* LISTEN
tcp4 0 0 *.sunrpc *.* LISTEN
:
udp4 0 0 *.tftp *.* LISTEN
:

```

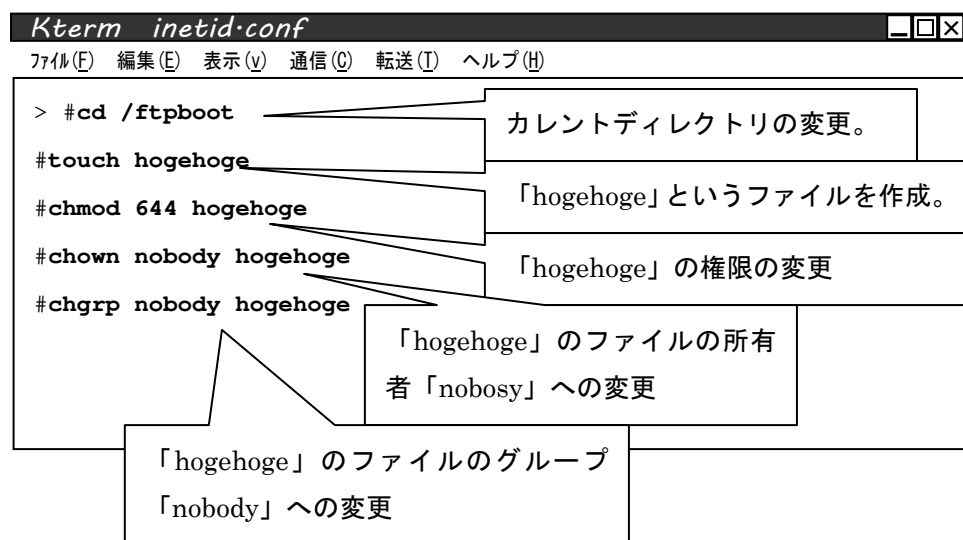
以上で TFTP サーバの設定は終了です。

4.3 ルータから TFTP サーバへの書き出し

次に、ルータから TFTP サーバへの書き出しを説明します。

■ 転送先のファイルを作成

ftp サーバでは、サーバ側に転送先ファイル(Destination file)を用意する必要があります。以下にそのオペレーションを示します。



ファイル名として適切なものを用意した方が実際には管理し易くなります。例えば、2001 年 6 月 10 日に IP Address が 210.134.129.67 の Router の環境設定のためのファイルを作成した場合は、

210.134.129.67-20010610-01

というようにファイル名に何らかの意味をもたせたものを設定する方がよいでしょう。

■ Router から TFTP サーバへ転送

それでは Router の環境設定を TFTP サーバに転送します。以下はルータ上でのオペレーションです。

```
Cisco - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#copy startup-config tftp
Address or name of remote host []? 10.177.129.201
Destination filename [startup-config]? Hogehoge
!!
2071 bytes copied in 3.105 secs (690 bytes/sec)
Routeri#exit
Router>
```

4.4 TFTP サーバからルータへの読み込み

以下は TFTP サーバ からルータへ環境設定を読み込むルータ上でのオペレーションです。

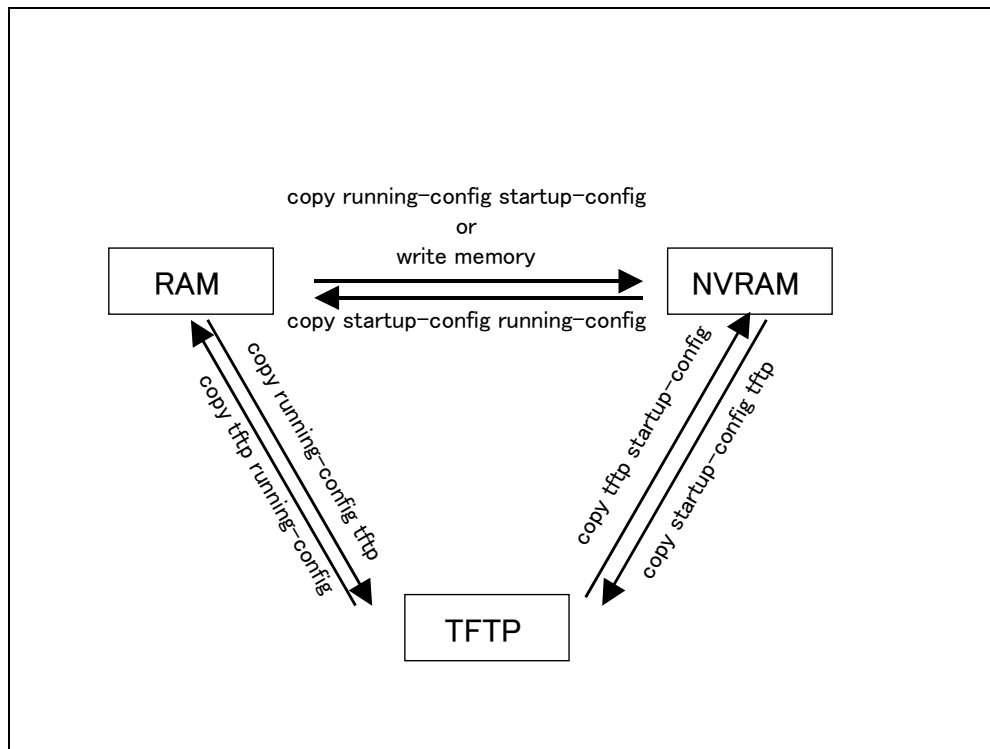
```
Cisco - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>en
Password:*****
Router#copy tftp startup-config
Address or name of remote host []? 10.177.129.201
Source filename []? Hogehoge
Destination filename [startup-config]?
Accessing tftp://10.177.129.201/hogehoge...
Loading hogehoge from 10.177.129.201 (via Ethernet0/1): !
[OK - 2071/4096 bytes]
2071 bytes copied in 19.520 secs (109 bytes/sec)
Router#exit
Router>
```

注意事項

直接、running-config に読み込めますが、読み込んだ瞬間に環境が反映されるので、記入ミス等に対する注意が必要です。

4.5 TFTP サーバ と Router の関係



 練習

TFTP サーバの構成

1. テキストを参考に `ined.conf` を変更します。（`tftpd` の有効化・ファイル保存ディレクトリの設定・`hosts.allow` の設定）
2. ファイル転送先ディレクトリを作成します。
3. `inetd` を再起動します。

 確認

実習**ルータから TFTP サーバへのファイル転送**

4. TFTP サーバとして構成したコンピュータ上で、転送先ファイルを作成します。
5. Cisco ルータから環境設定を TFTP サーバに転送します。

確認

-
6. Cisco ルータの起動画面を確認します。

実習**TFTP サーバからルータへのファイル転送**

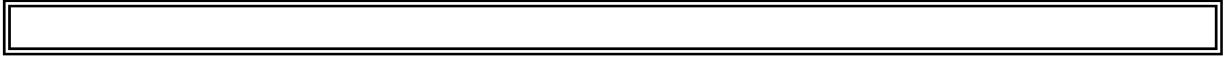
7. Cisco ルータ上で TFTP サーバから環境設定を読み込みます。

確認

ターミナルにルータの起動画面が出力されましたか？ 出力されたらルータの電源を落としてください。

出力されない場合は、ケーブルの接続や設定を確認しましょう。

- 8.



5 章 syslog 管理

5 syslog 管理

5.1 システムログ

ルータの運用管理においてシステムログの収集閲覧は重要です。ログを収集することで①システムの利用傾向の把握と②潜在的な問題の発見が図れます。これらの情報を収集することで基本的なトラフィック管理が行え、ネットワークダウンなどの大きな障害が発生する前に対処することも出来ます。

普段から管理するシステムのログをとりその傾向をつかんでおくことが大切です。

Cisco ルータで System Log の閲覧方法を以下に示します。

```
Cisco - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 94592 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: disabled
  Trap logging: level debugging, 94596 message lines logged
  Logging to 210.134.161.66, 94558 message lines logged
  Log Buffer ( 4096 bytes ):
Mar 17 17:45:56: %LINK-3-UPDOWN: Interface Serial0, changed stste to down
Mar 17 17:46:40: %LINK-3-UPDOWN: Interface Serial0, changed stste to up
```

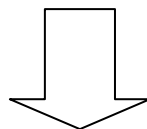
ルータでログを取るときの問題点として

- ① Cisco ルータは Diskless System なのでディスク上にログを残すことが出来ません。
- ② しかも、メモリ上にログを残すこともその搭載容量からして現実的ではありません。
- ③ また、電源を落とした場合、メモリ上のログは消失してしまいます。
- ④ Router が多数あると管理に負担の負担が増えます。

という問題があります。

上記問題の解決方法として syslog サーバを使用する、という方法があります。

ディスク上にログを残すことが出来ない。
メモリの容量に制限がある(例えば、4048byte、8096byte 等)
電源を切った場合、log は消失する。
機器の増加に伴う管理負担の増大



Syslog サーバで解決

5.2 Log Level について

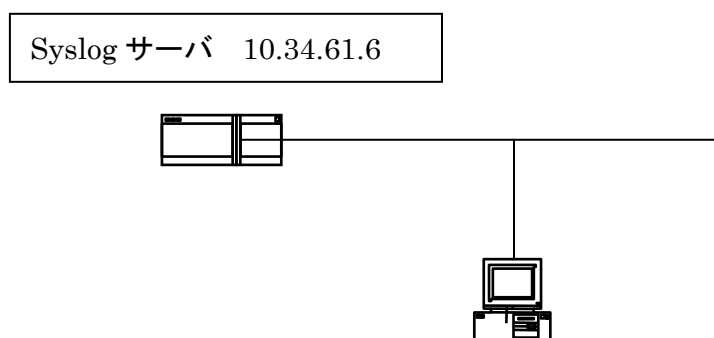
Level 0	Emergencies	緊急	システムが利用できなくなっている
Level 1	Alerts	警報	システムを安定させるために迅速な対応が必要
Level 2	Critical	注意	注意すべき危険な状態である
Level 3	Errors	エラー	問題を究明できるエラー状態である
Level 4	Warnings	警告	重大な問題ではないが注意すべき状態である
Level 5	Notifications	通知	正常だが注意すべき状況になったために通知が発生した
Level 6	Informational	情報	特別な対応を必要としない情報メッセージ
Level 7	Debugging	デバッグ	システムのトラブルシューティング用のデバッグメッセージ

Cisco ルータでは Log Level の設定により収集できるログの内容が変わります。基本的に Level が大きいほうが詳細に情報をすることができます。しかし、運用管理上、深刻度の低い情報も多く、実運用でどの Log Level を使用するかは運用目的と運用状況により判断します。例えば、実験・検証段階やシステム構築後の運用初期の段階では Level 7 で状態の監視を行い、システムが安定に稼動している期間の長さや状況に応じて徐々に Log Level を下げ、深刻度の高い情報のみを収集するようにしています。

5.3 syslog サーバの構成

■ Cisco ルータの設定

Cisco ルータ上で Log の収集レベルを設定し、収集した情報を syslog サーバに送る設定をします。設定には **logging** コマンドを使用します。



```
Cisco ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#logging 10.34.61.6
Router(config)#logging trap debugging
Router(config)#logging facility local0
Router(config)#exit
Router#copy running-config startup-config
Router#exit
Router>
```

Syslog サーバを指定

debugging Level でシステムログを収集

facility の設定。Default で local7 facility.log level である。この設定の場合、syslog.conf には Syslog サーバ内の syslog.conf 内の最初の項目に該当し、

■ syslog サーバの環境設定

syslog サーバは POSIX 互換 OS を使用して構築を行います。ここでは FreeBSD の場合を例にとり、構築を行います。syslogd は基本的にデフォルトでインストールされているので、環境設定のみで構築が可能となります。

1) /etc/syslog.conf の編集

```

Kterm syslog.conf
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

# $FreeBSD: src/etc/syslog.conf,v 1.13 2000/02/08 21:57:28 rwatson Exp $
#
#      Spaces are NOT valid field separators in this file.
#      Consult the syslog.conf(5) manpage.
#
#*.err;kern.debug;auth.notice;mail.crit        /dev/console
#
#*.emerg
#
local7.debug /var/log/Router
# uncomment this to enable logging of all log messages to /var/log/all.log

```

ただし、local7.debug は Router の設定と同じにする必要があります。この場合は、

Facility	local7
Log Level	debugging

とします。ときには Facility が別のアプリケーションと衝突する場合があります。その場合は、別の Facility に変更して対応します。

■ syslogd の起動

syslogd の起動の設定は以下の方法でおこないます。

1) /etc/rc.conf の編集

```
syslogd_enable="YES"
```

を追加します。基本的に故意に停止していない限り、この部分の編集は必要ありません。

2) log File の作成

```
# touch /var/log/router
```

ここでは、syslog.conf で指定したファイルの作成を行います。基本的に空ファイルを使用します。

3) syslogd を再起動

```
# killall -HUP syslogd
```

上記コマンドを入力して起動します。

実習**ルータ log の収集**

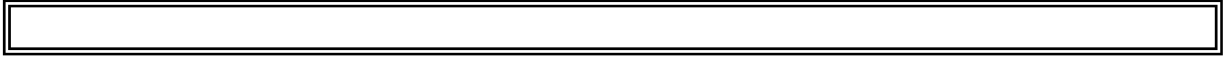
インストラクターから Log Level の指示があります。

1. syslog サーバを構成します。（syslog.conf の編集・syslogd の再起動）
2. Cisco ルータで現在のロギングの確認をし、インストラクターから指示された構成への変更と syslog サーバへのロギング転送設定を構成します。

確認

ターミナルにルータの起動画面が出力されましたか？ 出力されたらルータの電源を落としてください。

出力されない場合は、ケーブルの接続や設定を確認しましょう。

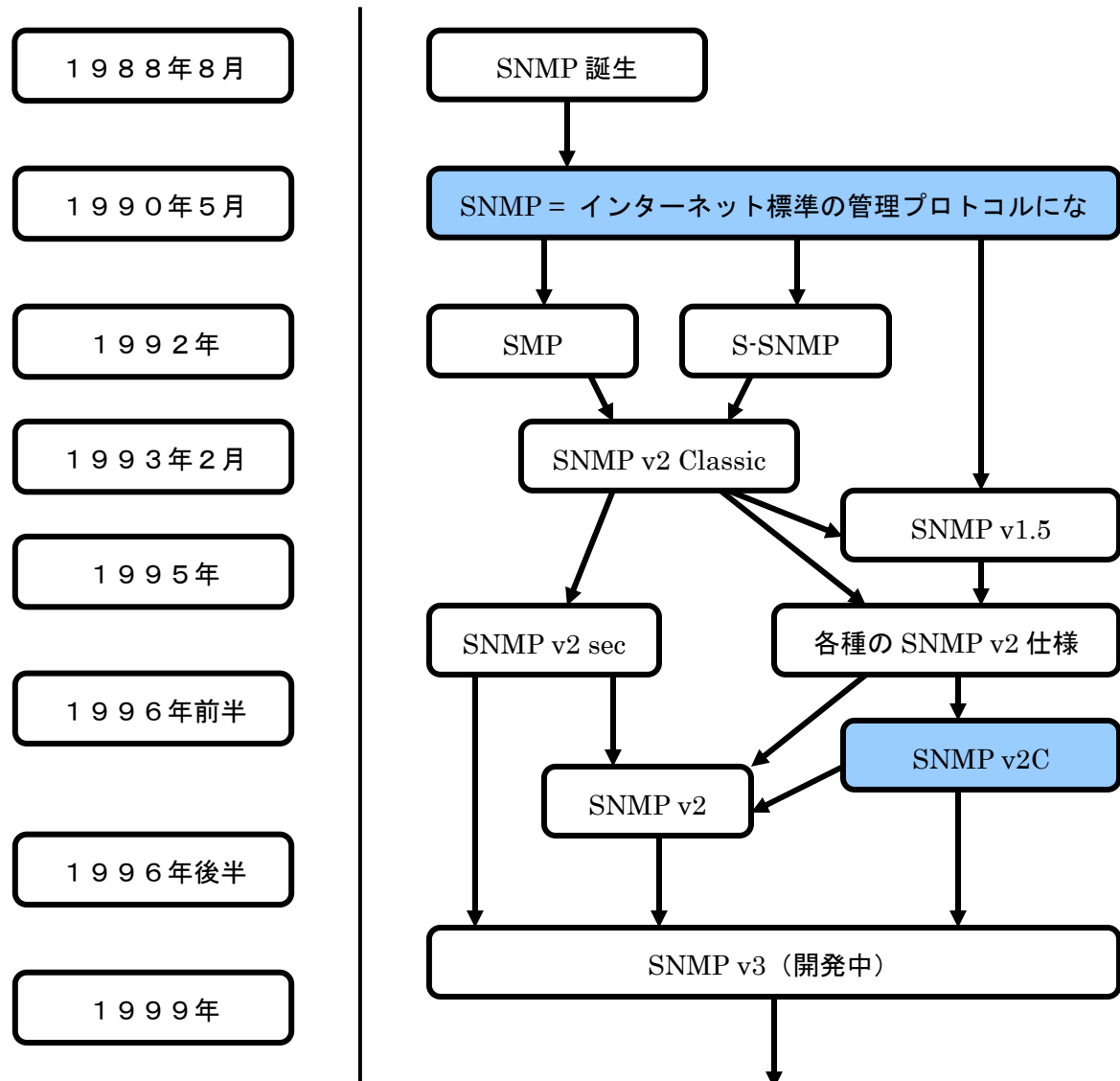


6 章 SNMP 管理

6

SNMP 管理

6.1 SNMP の歴史的変遷



SMP : Simple Management Protocol

S-SNMP: Secure SNMP

6.2 SNMP 関連の RFC

構成要素	SNMP バージョン	RFC 番号	内容
データ定義言語	SNMPv1	RFC1155	SMIv1
	SNMPv1	RFC1212	MIB モジュールの定義方法
管理プロトコル	SNMPv1	RFC1157	SNMP
	SNMPv2,v3	RFC1905	プロトコル操作
	SNMPv2,v3	RFC1906	トランスポート層へのマッピング
管理情報	SNMPv1	RFC1213	MIB- II
イベント情報	SNMPv1	RFC1215	SNMPv1 の TRAP 定義
セキュリティと運用管理	SNMPv2c	RFC1901	コミュニティ版 SNMPv2
	SNMPv2u	RFC1910	ユーザベースセキュリティモデル
	SNMPv2u	RFC1909	ユーザベースセキュリティモデル
その他	SNMPv2	RFC1908	SNMPv2 と SNMPv1 の共存

6.3 SNMP で管理できる項目

SNMP で管理できる項目には次のものがあります。

構成管理	ネットワークを構成している機器の状態監視、動作を制御する機能
性能管理	ネットワークを構成している機器の性能を測定する機能
機密管理	ネットワーク内への利用に制限をつけ、それらの資源に対する 利用が正しく 行われるように制御する機能
課金管理	ネットワーク内の資源の利用状況を利用者ごとに記録をとる機能
セキュリティ管理	ネットワークの不正利用やサーバの不正利用を監視する機能

上記の項目からネットワークの構成・障害・パフォーマンスを管理します。

特定のベンダでは特定の機器用のマネージャを用意し、機器固有の管理情報や定義情報の表示・更新を出来るようにしています。

6.4 SNMP の基本概念

現在、LAN の管理ツールとして最も一般的なものが SNMP (Simple Network Management Protocol) です。LAN のような分散的に配置されたネットワーク機器を集中管理するために考えられたしくみです。

SNMP の仕組みは、エージェントが持つ MIB と呼ばれる各種情報にマネージャからアクセスし、機器の情報を把握し、機器の定義・構成情報の変更を行うものです。

マネージャからアクセスするだけでなく、エージェント異常が発生したときにエージェントから情報を送信するトラップというし機能も用意されています。

1. SNMP マネージャ

管理する側の端末

サーバ機器 (UNIX・Windows NT)

2. SNMP エージェント

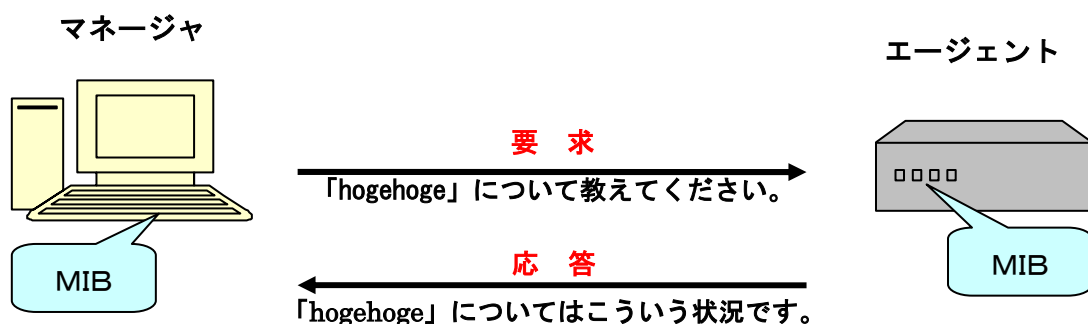
管理される側の機器

ルータ、ハブ、PC 等

3. MIB (Management Information Base)

管理情報の集まり

マネージャ、エージェントの両方に位置づけられる





7 章 SNMP 動作

7

SNMP 動作

7.1 基本動作プロトコル

SNMP はサーバ/クライアント型のプロトコルです。SNMP 用語ではマネージャ/エージェント型プロトコルといいます。要求/応答型のプロトコルとも言います。

基本的に SNMP では UDP が使用されます。(TCP ではありません) それぞれの「要求」が「応答」生成するのでコネクションの信頼性はあまり高くなくてもよいということです。

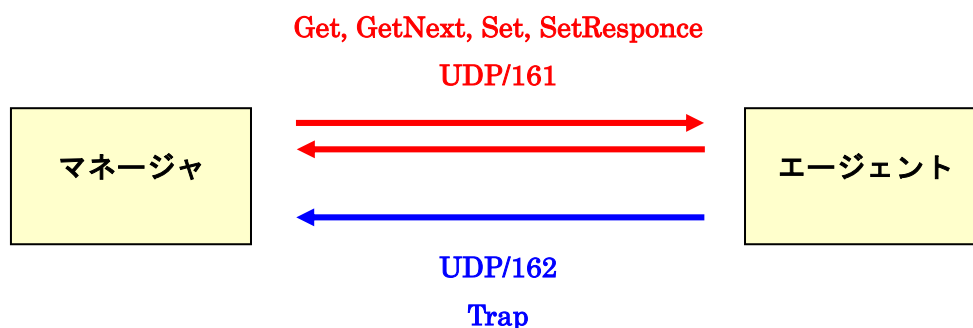
理由は

- 1) 監視によるネットワークトラフィックを最小限にするため
- 2) 故障した装置に TCP の大きなオーバーヘッドを負わせない

為です。

SNMP アプリケーションに応答が返されなかったときには「要求」の再発行をします。「要求」も「応答」も単独のデータグラムなので「シーケンス処理」は不要です。

SNMP 自体はとても単純に出来ているため、ターゲットのエージェントに対して情報を要求するときには、5 種類のコマンドに MIB を指定しその機器に対して「要求」送出したあとはその機器からのレスポンスを待つだけです。



7.2 SNMP の 5 つのコマンド

SNMP がデータグラムとして送る「要求」と「応答」のメッセージコマンドを PDU といいます。

マネージャはこれらのメッセージコマンドを使用して管理情報の要求をします。

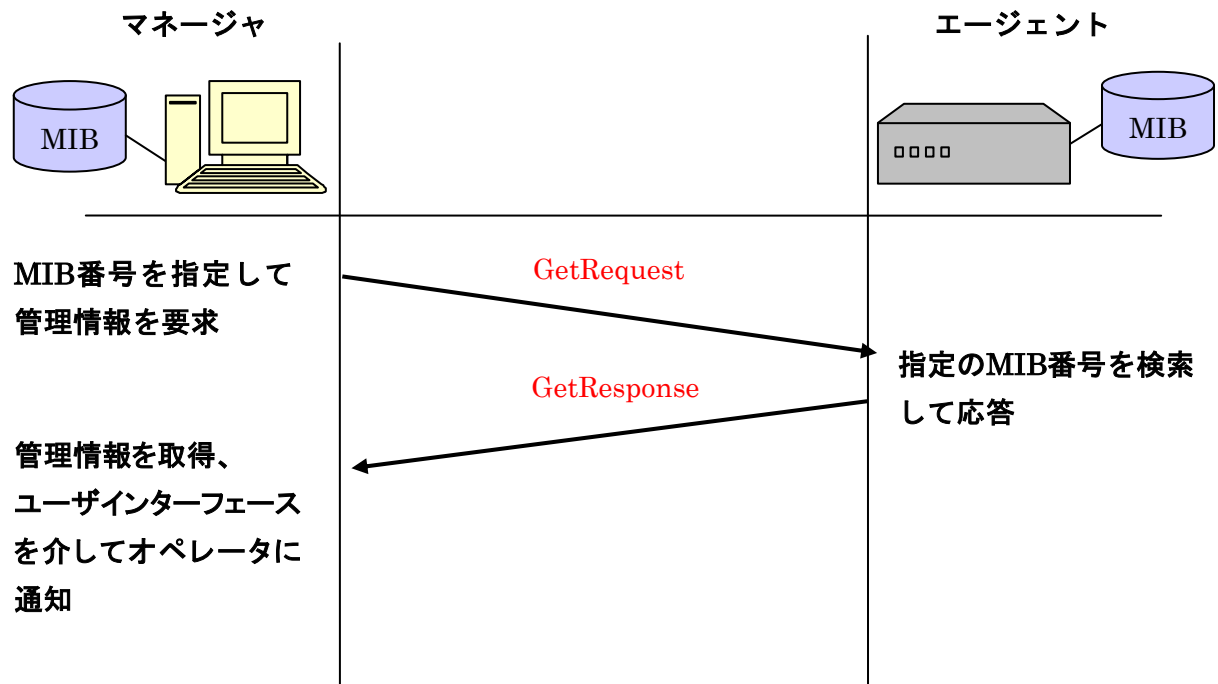
エージェントはこれらのメッセージコマンドを使用して管理情報の要求をします。

前ページの図にあるように PDU は UDP ポート 161 を使用します。Trap のみは UDP ポート 162 を使用します。五つの PDU(メッセージコマンド)で Get・GetNext・Set・Trap という四つのプロトコル動作を構成します。

PDU(Protocol Data Unit)の種類

PDU	説 明
GetRequest	マネージャが更新情報を要求する
GetNextRequest	マネージャがテーブルの次のエントリを要求する
GetResponse	エージェントがマネージャからの要求に応答する
SetRequest	マネージャが管理対象装置のデータを修正する
Trap	エージェントがマネージャに異常を通知する

7.3 Get プロトコル動作 1

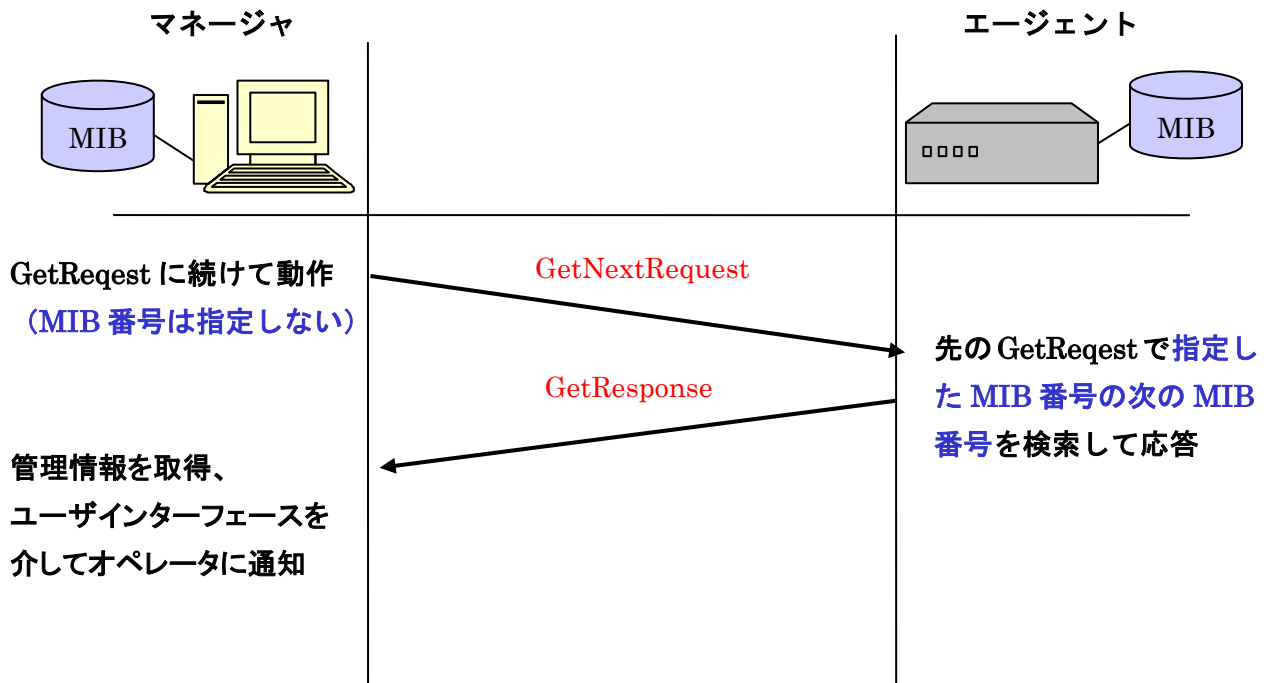


Get プロトコル動作は GetRequest GetResponse メッセージコマンドから成立します。

- ① マネージャがエージェントに対して MIB 番号を指定して管理情報を「要求」します。
- ② エージェントが指定の MIB 番号を検索して「応答」を返します。
- ③ マネージャは取得した管理情報をオペレータに対して表示します。

という三つのフェーズです。

7.4 GetNext プロトコル動作 2



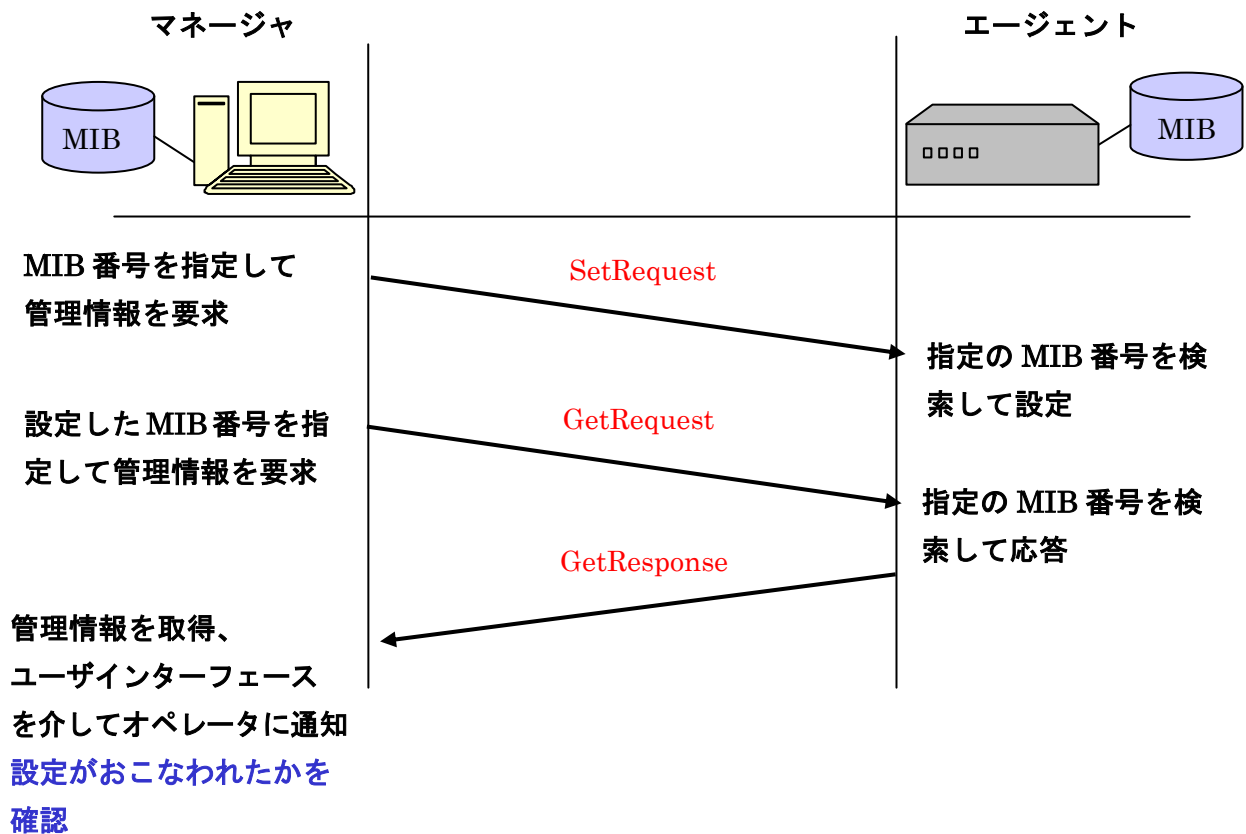
GetNext プロトコル動作は GetNextRequest GetResponse メッセージコマンドから成立します。

GetNext プロトコル動作は GetRequest に続けて行われます。そこで MIB 番号は既に GetRequest で指定してあるので今回指定不要です。あくまでも GetRequest で要求した MIB 番号の次の番号を要求します。

Get 動作と同様、三つのフェーズから成立します。

- ① マネージャが先に動作した GetRequest で指定した MIB 番号の次の番号の管理情報をエージェントに対して「要求」します。
- ② エージェントが先に「応答」した MIB 番号の次の番号を検索して「応答」を返します。
- ③ マネージャは取得した管理情報をオペレータに対して表示します。

7.5 Set プロトコル動作 3

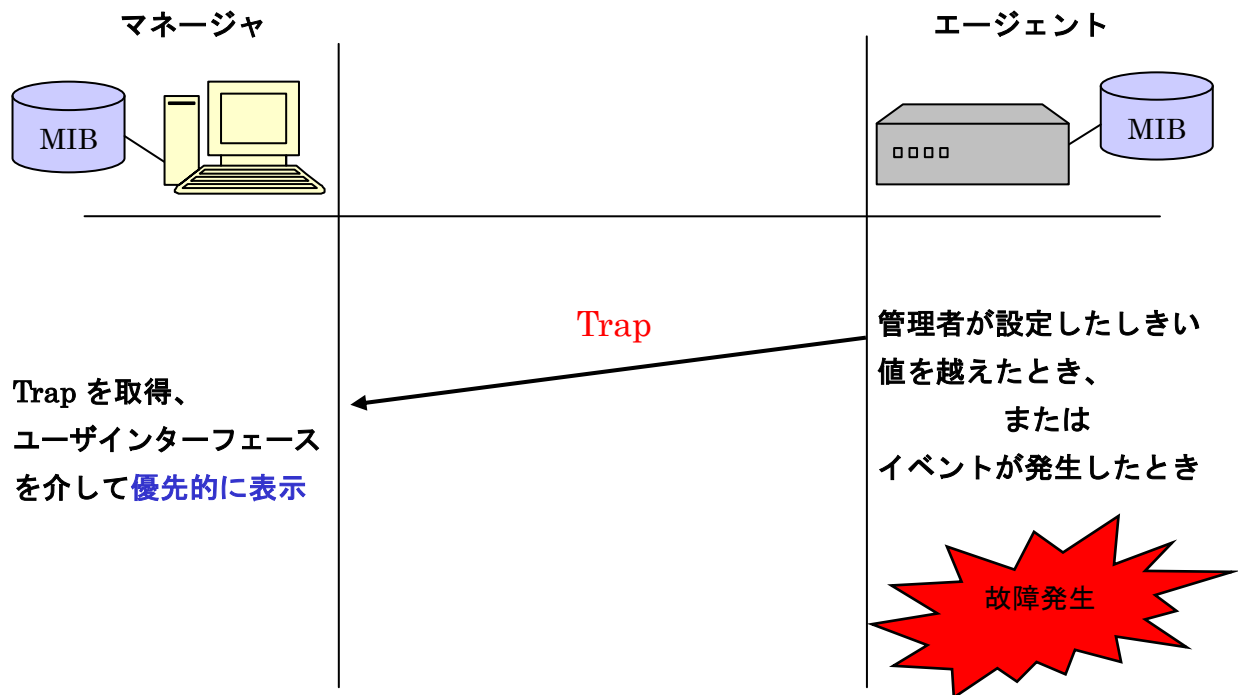


UDP を利用するため確認作業が必要になります

Set 動作は

- ① マネージャがエージェントに対して MIB 番号を指定して管理情報の設定を「要求」します。
- ② エージェントが指定の MIB 番号を検索して「設定」します。
- ③ マネージャがエージェントに対して MIB 番号を指定して管理情報を「要求」します。
- ④ エージェントが指定の MIB 番号を検索して「応答」します。
- ⑤ マネージャは取得した管理情報をオペレータに対して表示します。

7.6 Trap プロトコル動作 4



Trap はエージェント上にあらかじめ定義していたイベントが発生したときにかかる「割込み」です。Trap イベントが発生すると即座に情報をマネージャに送信します。この Trap 動作のみ、(マネージャからの要求に対する)「応答」ではありません。

--

8 章 M I B



8

M I B

8.1

MIB と SMI

MIB (Management Information Base)

SNMP によって管理されるすべてのオブジェクト（オブジェクトごとの一意の識別子・BER 準拠のエンコードなど）をまとめたグループを MIB といいます。

SNMP マネージャからアクセスされる各機器の定義・動作状態を表すものです。大別すると RFC で定められたものと各機器ベンダが任意に定義したプライベート MIB と呼ばれるものがあります。

TCP/IP を監視するための標準 MIB は MIBII です。

- ・ マネージャとエージェント間でやりとりされる管理情報
- ・ マネージャから検索、指定可能なようにツリー状に名前付けされている
- ・ 現在利用されているのは、標準 MIB、拡張 MIB

SMI (Structure of Management Information)

SNMP 環境で使用するデータ表現形式を定義したものです。管理対象オブジェクト（managed objects）の名前・構文・エンコードなどが規定されています。

- ・ 管理情報（MIB）を定義するためのルール
- ・ データ構造、データのタイプ、名前付け

8.2 MIB

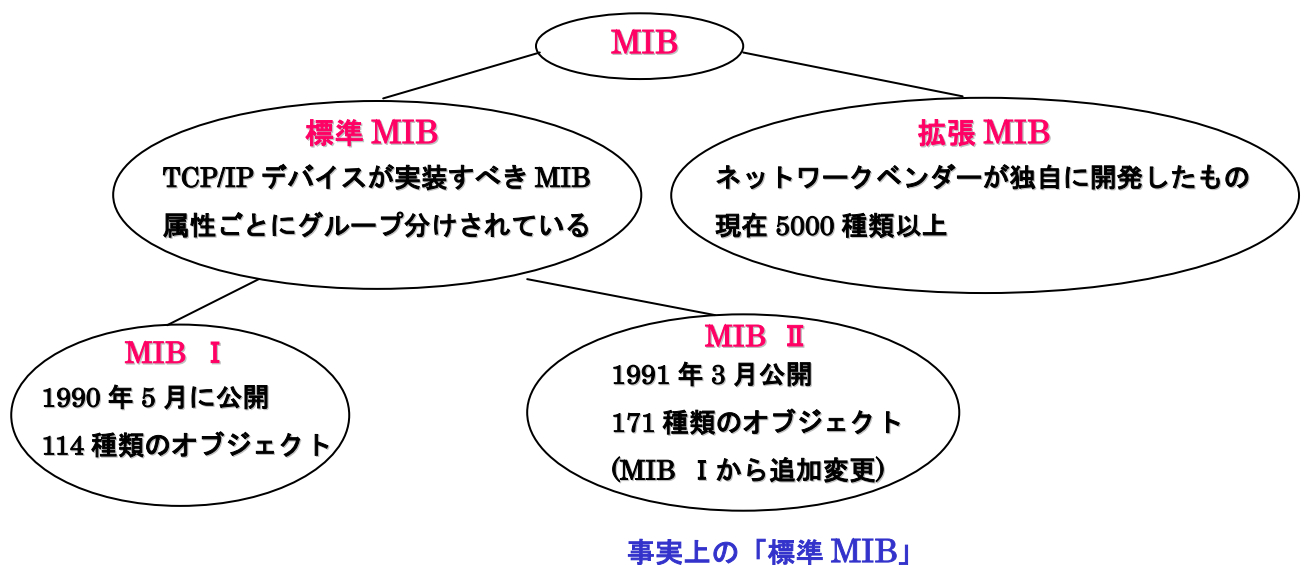
基本の MIB で OSI 参照モデルの第二階層データリンク層のレベルと TCP/IP に関するパケットのエラーも含めたパケットの入出力個数をカバーしています。ここれらの情報は①利用傾向の把握・②潜在的問題の発見に有効です。これにより基本的なトラフィック管理が行えます。

MIB とは、

管理情報の集まり

SMI によって定義されている

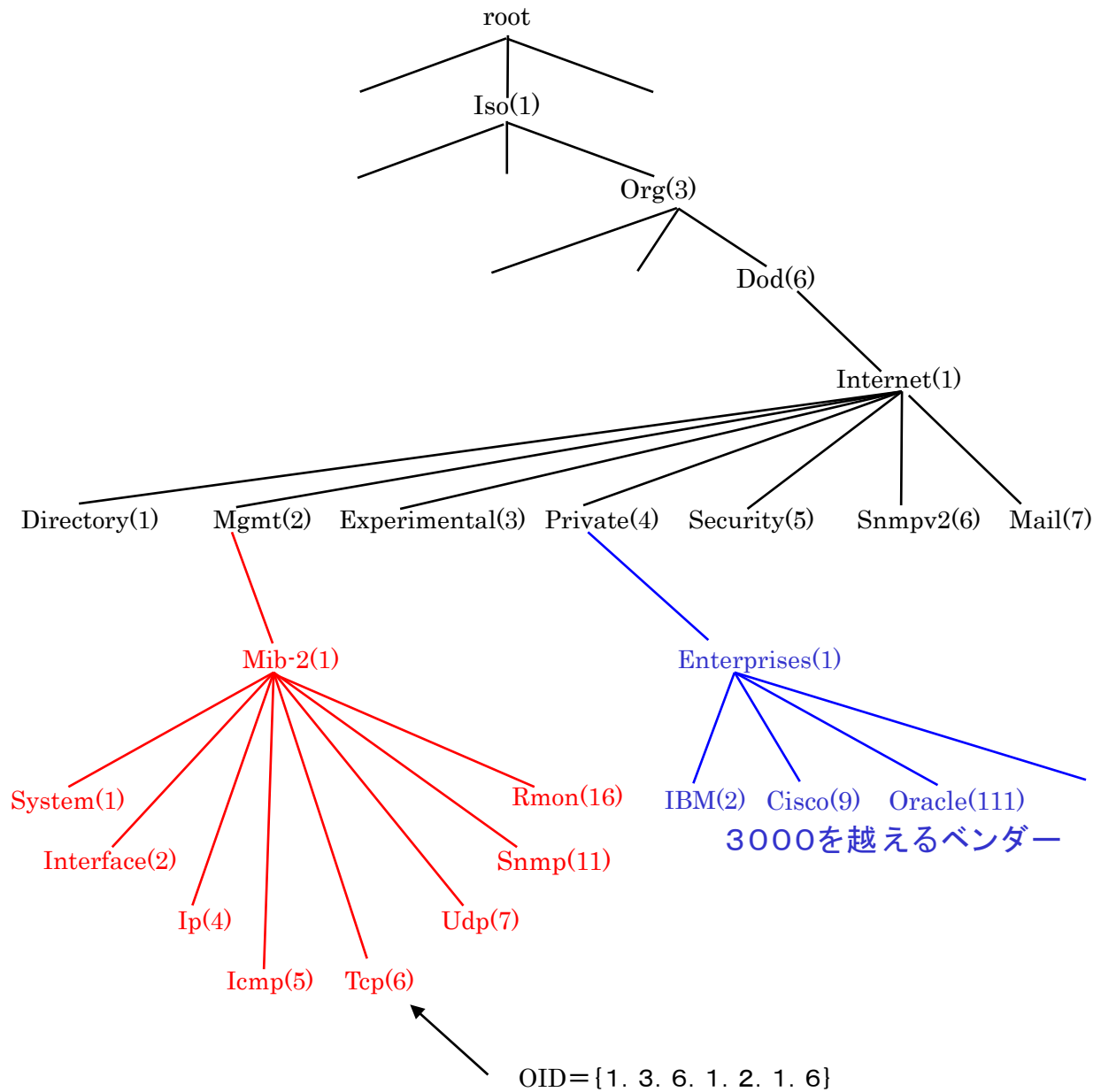
マネージャとエージェントの両方に位置付けられる



8.3 MIB の構造

OID (object Identifier)

オブジェクト識別子という一意な識別子が割り当てられます。



8.4 MIB2 (RMON グループ)

RMON MIB と、その他の標準 MIB の比較

	標準 MIB 管理	RMON MIB 管理
実装	ルータ・スイッチ・ハブ等	プローブ
通信量の計測	エージェント自身の情報	LAN セグメントの情報
データ収集処理	マネージャに依存	エージェント（プローブ）自身
障害の検知	エージェントに問題が生じた時	LAN セグメントに問題が生じた時
トラフィック負荷	比較的多い	少ない

- 長所
- ・ ネットワーク管理によるトラフィックを減少することができます。
 - ・ 詳しいトラフィック統計情報が収集できます。

- 短所
- ・ プローブ（監視専門の装置）が別途必要となります。

8.5 標準 MIB と拡張 MIB

標準 MIB と拡張 MIB の比較

	標準 MIB	拡張 MIB
開発元	IETF (RFC で標準化)	ベンダ独自
実装機器	機器全般	自社製品のみ
定義内容	大まか	非常に細かい
管理アプリケーション	対応	未対応が多い

実装例 : Cisco 製品 = 標準 MIB + Cisco 独自の拡張 MIB

マネージャは基本的に標準 MIB しかサポートしていません。マネージャが拡張 MIB をサポートするには、プラットフォームにそのベンダの管理アプリケーションを使うか、拡張 MIB を別途、追加インストールする必要があります。



9 章 ネットワーク管理ツール

9

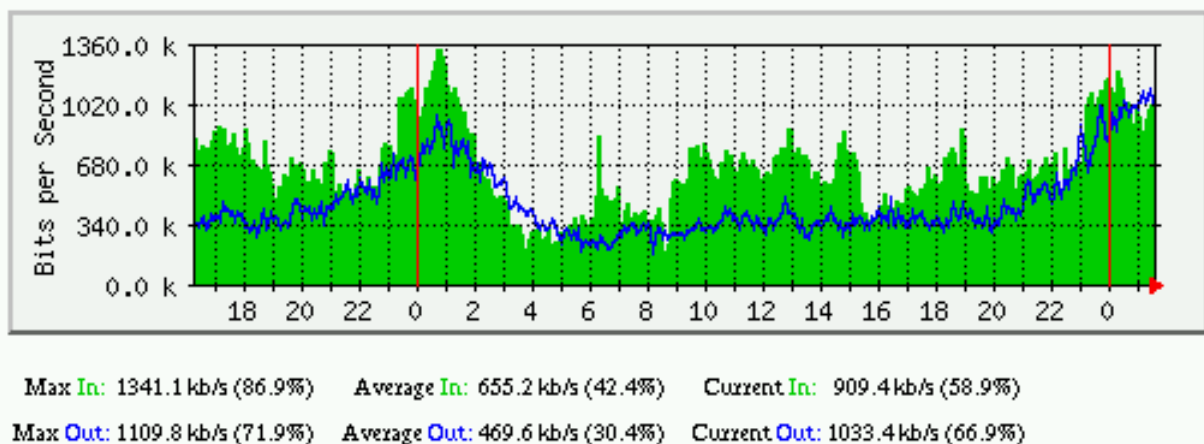
ネットワーク管理ツール

9.1 MRTG

WindowsNT/2000,Windows95/98/ME,各種 UNIX で動作するフリーソフトです。
収集した情報をブラウザにグラフで表示します。

ルータを流れるトラフィック量をチェックして変化を見やすいグラフにしてくれるソフトです。
計測結果を HTML ファイルとグラフで表示します。

‘Daily’ Graph (5 Minute Average)



利用環境は、

- ① 監視される機器
- ② MRTG と実行するサーバ
- ③ その結果を閲覧する端末

の三つで構成されます。

ネットワーク装置の監視には SNMP を使用しています。このことは「監視される装置は SNMP に対応していればよい。」ということです。

9.2 HP OpenView と Sun Net Manager

HP OpenView

ネットワーク管理製品の事実上の標準とも言うべき存在です。

単体では SNMP の基本的な 3 つの機能（構成、障害、性能管理）しか備えていませんが、API などを外部に公開しているので追加拡張できます。

Sun Net Manager

正式名称は「Solstice SunNetMnager」といい、Solaris 上で動作します。

SNMP マネージャの標準機能に加えて OSI ネットワーク管理プロトコルである CMIP や DECnetNICE、IBM NetView、FDDI/SMT などをサポートしています。

HP OpenView と同様に API を公開しているので、追加拡張が可能です。

9.3 その他の管理ツール

管理ツールのいろいろ

- Tivoli NetView
- Info Vista
- JP1
- NetCool
- TWSNMP マネージャ

できること

Ping
Port Scan
SNMP
SNMP Trap 等

9.4 SNMP による管理の問題点

問題点

- ① 監視によるトラフィック量がエージェントの数に比例して増加する。
- ② セキュリティがほとんどない。
- ③ MIB が企業固有領域に大きく依存している。

対応策

- ①
 - SNMPv2 を使って、管理範囲を分割する。
 - RMON を使用してトラフィックを減少させる。
 - ポーリングの頻度をさげて、トラップ重視のネットワーク管理をする。
- ② 設定変更コマンド（SetRequest）を使用しない。（エージェントに制限を与える）
- ③ 管理範囲内のエージェント機器メーカーを統一して、そのベンダの管理アプリケーションを使う。



10 章 MRTG

10

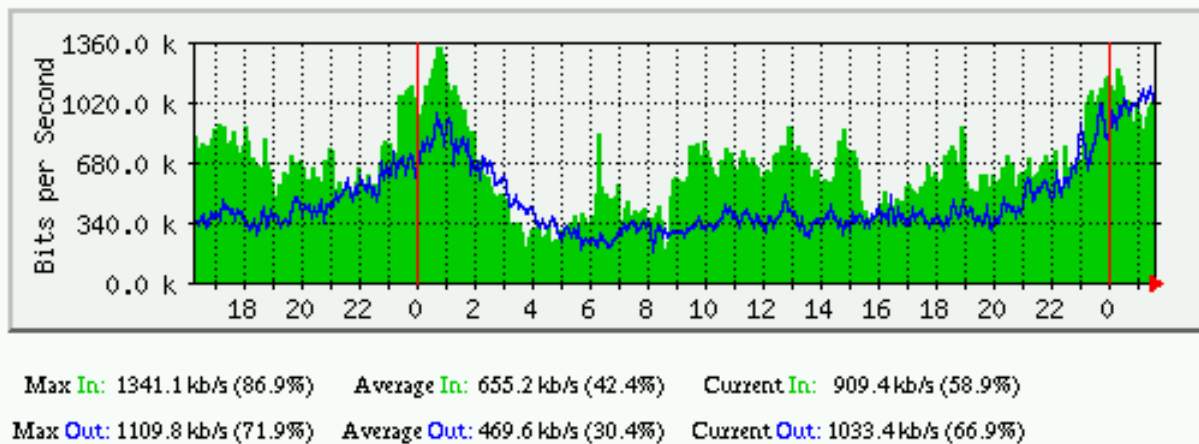
MRTG

10.1 MRTG とは

WindowsNT/2000,Windows95/98/ME,各種 UNIX で動作するフリーソフトです。
収集した情報をブラウザにグラフで表示します。

ルータを流れるトラフィック量をチェックして変化を見やすいグラフにしてくれるソフトです。
計測結果を HTML ファイルとグラフで表示します。

'Daily' Graph (5 Minute Average)



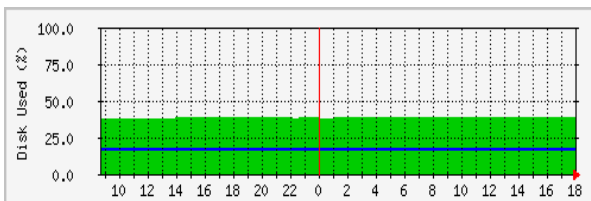
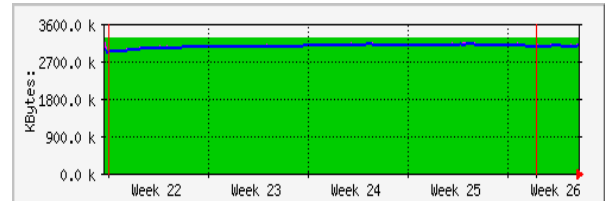
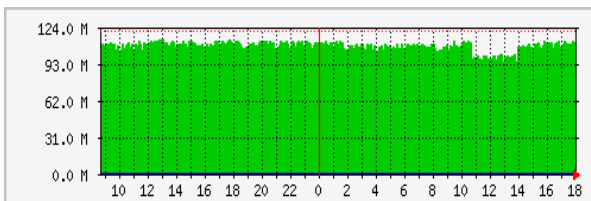
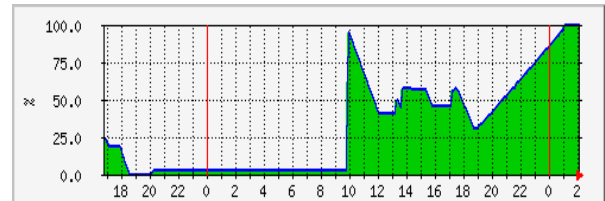
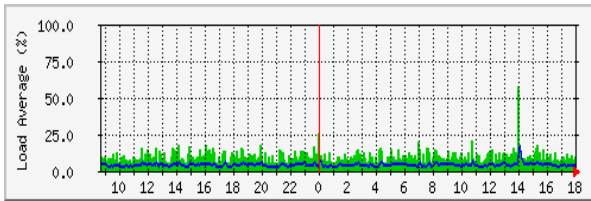
利用環境は、

- ④ 監視される機器
- ⑤ MRTG と実行するサーバ
- ⑥ その結果を閲覧する端末

の三つで構成されます。

ネットワーク装置の監視には SNMP を使用しています。このことは「監視される装置は SNMP に対応していればよい。」ということです。

10.2 MRTG Sample



10.3 MRTG の構築

MRTG の監視までのプロセスは、

- ① MRTG の導入
- ② 監視対象の SNMP 設定
- ③ mrtg.cfg の作成
- ④ mrtg の実行

の四つです。

MRTG の仕組み

監視対象ネットワーク機器から SNMP を用いて機器情報を収集し、情報を解析しグラフ化します。

Netscape、Internet Explorer 等のブラウザを用いて結果を見ます。

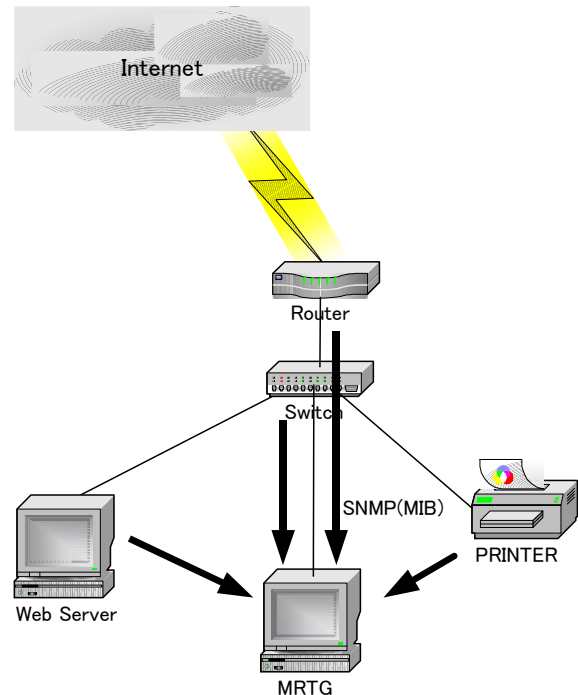
監視対象

SNMP に対応している機器であればネットワーク機器でなくても監視できます。例えば、

温度測定器、UPS 等)
traffic (input、output 等)
UPC 負荷 等です。

構築に必要なアプリケーション

mrtg-2.9.17.tar.gz	MRTG 本体です
libpng-1.0.12.tar.gz	png library です。
libjpeg.v6.tar.gz	jpeg library です。
gd-1.8.4.tar.gz	グラフ作成 library です。
Apache-1.3.19.tar.gz	Web サーバです。他の web アプリケーションでも可能です。
zlib	場合により必要です。すでに install されている場合もあります。



10.4 MRTG の導入

MRTG の導入に必要なソフトウェアのインストールです。基本的にソースからコンパイルしてインストールをします。

■ libtool-1.3.4

ライブラリを作成するツールです。

I libtool-1.3.4.tar.gz の展開 (適当な作業ディレクトリでソースの展開を行います。)

```
> cd ${WORK_DIRECTORY}
> tar xvfz libtool-1.3.4.tar.gz
```

II 初期設定

```
> cd ${WORK_DIRECTORY}/libtool-1.3.4
> ./configure --disable-ltdl-install
```

III コンパイル

```
> cd ${WORK_DIRECTORY}/libtool-1.3.4
> make
```

IV インストール

```
> cd ${WORK_DIRECTORY}/libtool-1.3.4
> make install
```

■ libjpeg.v6

Jpeg のライブラリです。

I jpegsrc.v6.tar.gz の展開

```
> cd ${WORK_DIRECTORY}
> tar xvfz jpegsrc.v6.tar.gz
```

II 初期設定

```
> cd ${WORK_DIRECTORY}/jpeg-6b
> ./configure --enable-shared --enable-static CC='cc' CFLAGS='-O'
```

III コンパイル

```
> cd ${WORK_DIRECTORY}/jpeg-6b
> make
```

IV インストール

```
> cd ${WORK_DIRECTORY}/jpeg-6b
> su
# make install
```

■ libpng-1.0.12

png のライブラリです。

I libpng-1.0.12.tar.gz の展開

```
> cd ${WORK_DIRECTORY}
> tar xvfz libpng-1.0.12.tar.gz
```

II Makefile の編集

```
> cd ${WORK_DIRECTORY}/libpng-1.0.12
> cp scripts/makefile.std makefile
> vi makefile
```

```
----- 変更前 -----
# Where the zlib library and include files are located
#ZLIBLIB=/usr/local/lib
#ZLIBINC=/usr/local/include
ZLIBLIB=../zlib
ZLIBINC=../zlib
-----
```

```
----- 変更後 -----
# Where the zlib library and include files are located
ZLIBLIB=/usr/lib
LIBINC=/usr/include
#ZLIBLIB=../zlib
#ZLIBINC=../zlib
-----
```

コメントアウトを取り、ディレクトリを変更します。

コメントアウト設定します。

III コンパイル

```
> cd ${WORK_DIRECTORY}/libpng-1.0.12
> make
```

IV インストール

```
> cd ${WORK_DIRECTORY}/libpng-1.0.12
> su
# make install
```

■ gd-1.8.4

gd のライブラリです。

I gd-1.8.4.tar.gz の展開

```
> tar xvfz gd-1.8.4.tar.gz
```

II コンパイル

```
> cd gd-1.8.4
> make
```

III インストール

gd-2.0.1 では、コンパイルは 下記のように行います。

```
> su
# make install
```

■ mrtg-2.9.17

MRTG 本体です。

I mrtg-2.9.17.tar.gz の展開

```
> cd ${WORK_DIRECTORY}
> tar xvfz mrtg-2.9.17.tar.gz
```

II 初期設定

```
> cd ${WORK_DIRECTORY}/mrtg-2.9.17
> ./configure --with-gd-lib=/usr/local/lib
               --with-gd-inc=/usr/local/include
               --with-z-lib=/usr/lib
               --with-z-inc=/usr/include
               --with-png-lib=/usr/local/lib
               --with-png-inc=/usr/local/include
```

III コンパイル

```
> cd ${WORK_DIRECTORY}/mrtg-2.9.17
> make
```

IV インストール

```
> cd ${WORK_DIRECTORY}/mrtg-2.9.17
> su
# make install
```

■ Apache のインストール

Web サーバです。

I Apache-1.3.19.tar.gz の展開

```
> cd ${WORK_DIRECTORY}
> tar xvfz apache-1.3.19.tar.gz
```

II 初期設定

```
> cd ${DWORK_DIRECTORY}/apache-1.3.19
> ./configure --with-port=80 --with-layout=Apache
```

III コンパイル

```
> cd ${DWORK_DIRECTORY}/apache-1.3.19
> make
```

IV インストール

```
> su
# make install
```

V 環境設定

必要に応じて行います。基本的に default でも使うことは可能ですが Security 的には問題あります。

VI 起動

```
# /usr/local/apache/bin/apachectl start
```

10.5 対象ネットワーク機器の設定

SNMP が実装されているネットワーク機器で SNMP を有効にします。(今回は Cisco ルータを例にします。)

SNMP を使用するためには、①Community 名・②アクセス許可するホストの IP Address・③情報を読み取り専用か読書きも可能にするかの設定、の三つを決めます。

Community 名は public を標準で設定するとアクセスを許可する相手の記述のみで利用できますが、完全に閉じられた外部との接続を持たないネットワーク以外の場合は、Security 上独自の Community 名を用意したほうがよいでしょう。

SNMP によるネットワーク機器の状態を調査するために必要なもの

- ① Community 名 認証キーみたいなもの。標準で public を使用するので別のものを使用すること。Security 上必須
- ② アクセス可能なサーバの IP Address MRTG サーバの IP Address。Security 上必須。
- ③ 読取専用か読書き可能かの設定 基本的には読込み専用。

設定例 Cisco IOS の場合

The screenshot shows a Cisco IOS terminal window titled "Cisco-ハイパ-ターミナル". The terminal output is as follows:

```
Router>enable
Password:*****
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 2 permit 10.138.111.5
Router(config)#snmp-server community hoge RO 2
Router(config)#snmp-server community ujauja RW 2
Router(config)#exit
Router#copy running-config startup-config
Router#
```

Callouts explain the configuration:

- アクセス可能な IP Address の設定を行う。** (Setting the accessible IP Address): Points to the `access-list 2 permit 10.138.111.5` command.
- 読込み専用の場合の設定。「hoge」が community 名** (Setting for read-only mode. 'hoge' is the community name): Points to the `snmp-server community hoge RO 2` command.
- 最後の「2」という番号が access-list 番号** (The number '2' at the end is the access-list number): Points to the `2` in the `snmp-server community` commands.
- RO: 読み込み専用の場合のキーワード
RW: 読書き可能の場合のキーワード** (RO: Keyword for read-only mode
RW: Keyword for read-write mode): Points to the `RO` and `RW` keywords.
- 読書き可能の場合の設定。「ujauja」が community** (Setting for read-write mode. 'ujauja' is the community): Points to the `snmp-server community ujauja RW 2` command.

10.6 MRTG の環境設定

MRTG で監視動作させる設定をします。

■ cfgmaker を使用して mrtg.cfg を作成

MRTG の環境を設定するファイル `mrtg.cfg` を作成します。MRTG には `cfgmaker` というツールが用意されています。

```
# /usr/local/mrtg-2/bin/cfgmaker hoge@ 10.1.1.1 >mrtg.cfg
```

`hoge@ 10.1.1.1`

監視対象のネットワーク機器の `community` 名と IP Address で作成したアドレス。この場合、「`hoge`」という `community` 名であり、監視対象の IP Address が「`10.1.1.1`」ということです。

`mrtg.cfg`

MRTG が実行されるときに読込まれる環境設定ファイル名。ファイル名は任意です。2 個以上の監視対象のネットワーク機器がある場合は、別にする必要があります。作成したファイルは適当なところに保存します。例えば、「`/usr/local/mrtg-2/cfg`」のディレクトリ内などです。

■ cron の設定

5分おきに MRTG を実行するための設定を UNIX 標準のスケジュールプログラム cron に反映します。

crontab -e コマンドを実行する方法と **vi** を実行する方法があります。

#crontab -e

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * /usr/local/mrtg-2/bin/mrtg /usr/local/mrtg-2/cfg/mrtg.cfg
```

#vi /etc/crontab

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * root /usr/local/mrtg-2/bin/mrtg /usr/local/mrtg-2/cfg/mrtg.cfg
```

vi を利用する方法の場合、cron をどのユーザとして実行するのか明示します。この場合、root です。

cron とは UNIX 標準のスケジュールプログラムです。実行スケジュールは crontab ファイルで指定します。crontab は 1 行に 1 つずつコマンドが指定されたリストであり、指定の時刻に自動実行されます。その書式は

分 時 日 月 曜日 実行するコマンド

となっています。ひとつのスケジュールフィールドに複数の数値を入れるときにはカンマ”,”で区切ります。コマンドフィールドにはパイプ”|”が使用出来ます。

上記 mrtg の例では、時・日・月・曜日のフィールドがワイルドカードなのでそれぞれ「毎時」「毎日」「毎月」「毎曜日」を表しています。分フィールドに 5 分毎の数値を指定して「5 分おきに実行」を実現しています。

■ mrtg.cfg の設定変更

cfgmaker で作成した mrtg.cfg ファイルに変更を加えます。

環境設定での基本変更点

WorkDir : MRTG で作成されるファイルを収容する Directory です。基本的に Web サーバでアクセスできる Directory を指定します。例えば、/usr/local/apache/htdocs/mrtg などです。

変更しておく便利なところ

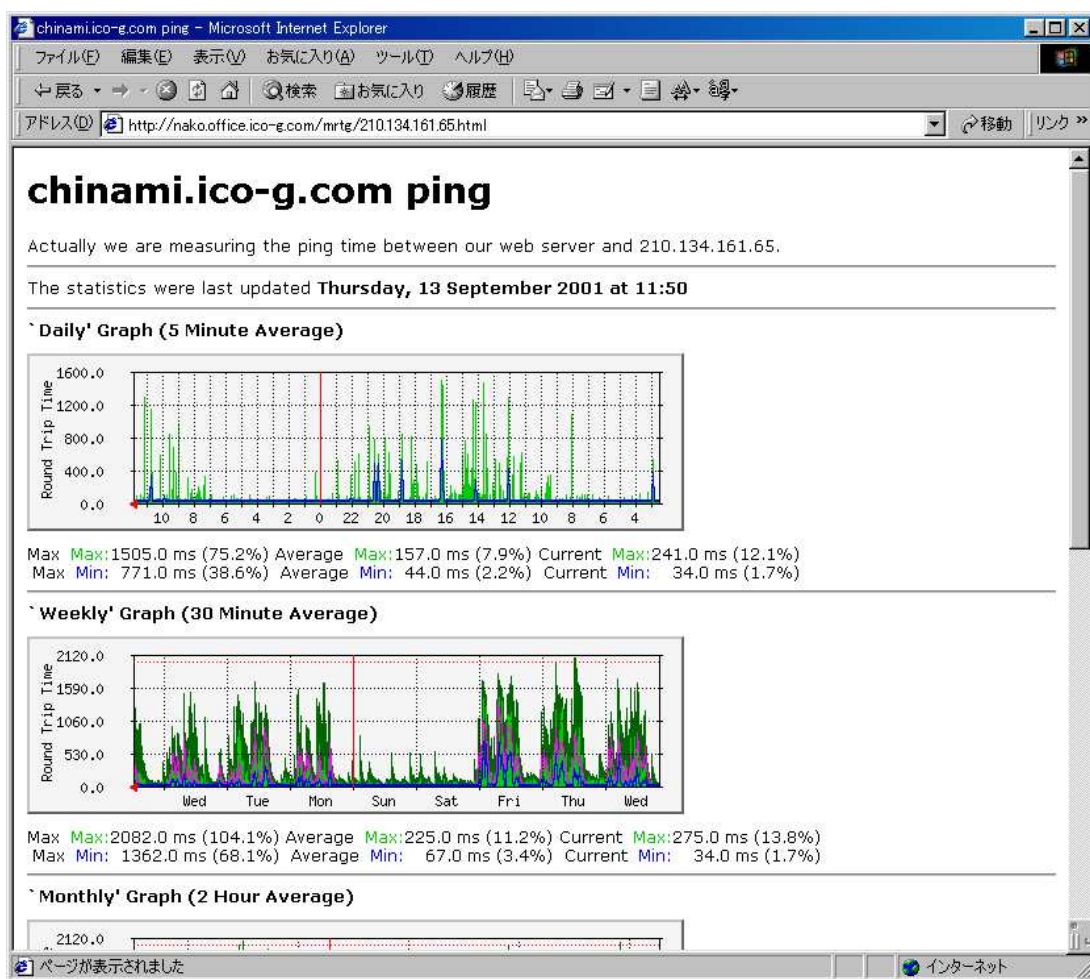
Target []	モニタする機器の指定。
SetEnv []	モニタする機器情報の環境設定。
MaxBytes []	取得データの最大値。 超過は無視します。
Title []	HTML ページのタイトル。
PageTop []	HTML ページの上部に記載する内容。

Router は複数の Network Interface を持つのでそれぞれを識別しやすいように変更をかけるとよいでしょう。

10.7 MRTG の応用

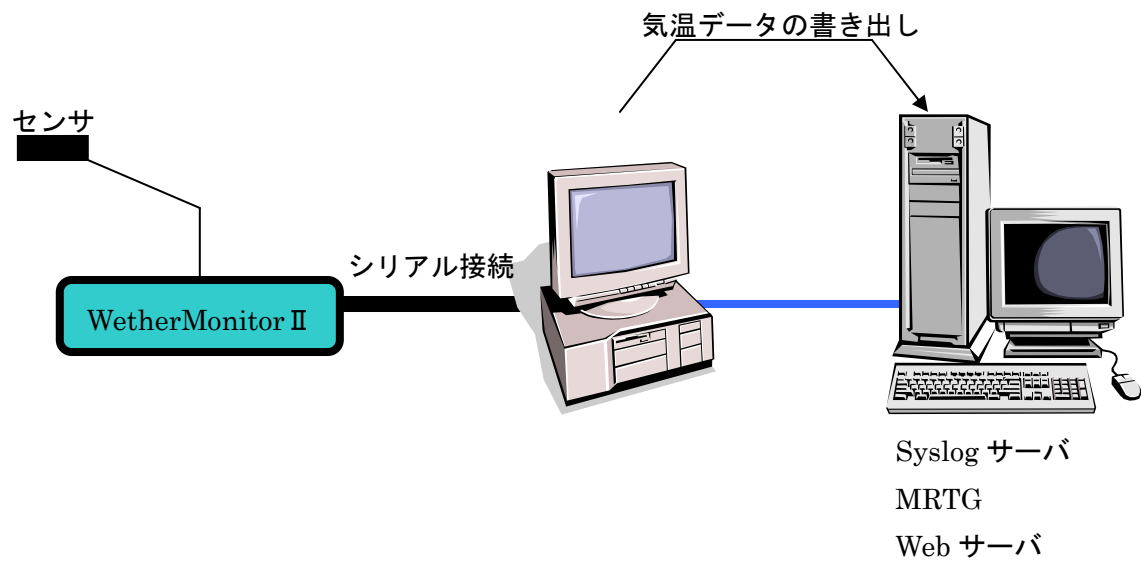
■ Ping 応答計測

ターゲットサーバーと MRTG ホスト間の Ping 応答時間計測の例です。



■ 気象データ計測

MRTG は SNMP に対応していれば管理対象として監視できます。群馬県のボランティアグループ「インターネットつなぎ隊」では MRTG を利用して全国の小中学校の気象データをインターネットで見るシステムを考案しています。（「Software Design 2000 年 4 月号技術評論社」より）



練習

監視対象機器の設定

MRTG で監視する対象機器の SNMP 設定をします。①Community 名・②アクセス許可するホストの IP Address・③情報の Read only か Write enable か、など設定に必要な情報をインストラクターから得ます。

確認

 練習

MRTG の導入

MRTG を導入するにあたって必要なソフトウェアをインストールします。

ターゲットフォルダ等必要な情報はインストラクターから得ます。

各ソフトウェアインストールの手順は本文を参考にします。

(基本は、展開・初期設定・コンパイル・インストール、です)

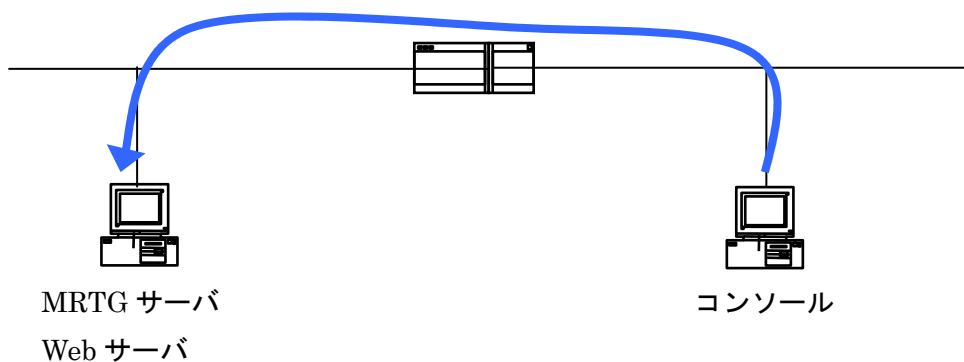
1. libtool-1.3.4 をインストールします。
2. libjpeg.v6 をインストールします。
3. libpng-1.0.12 をインストールします。
4. gd-1.8.4 をインストールします。
5. mrtg-2.9.17 をインストールします。
6. Apache をインストールします。

 確認

実習**MRTG の環境設定**

環境設定ファイルの作成・自動実行スケジュールの作成・環境設定の変更です。
ターゲットフォルダ等必要な情報はインストラクターから得ます。

7. cfgmaker を利用して mtrg.cfg を作成します。
8. cron で MRTG の情報収集を自動実行するように設定します。
9. mrtg.cfg の設定変更をします。
10. MRTG でのデータ収集をはじめます。
11. 収集データ web ブラウザで収集情報を確認します。

**確認**



11 章 Security

11 Security

11.1 環境設定の際のセキュリティ

ルータの環境設定を行う方法には次のものがあります。

- ① コンソール Console ポートからの設定（一番最初の設定時に利用します。）
- ② AUX AUX ポートからの設定（あまり利用実績がありません。）
- ③ telnet Cisco ルータ にリモートから telnet し設定（常時の運用時に利用します。）

↓

telnet 利用時には認証が必要です。

telnet を利用した設定方法はパスワード設定が必要です。

パスワード設定が必要な項目 → 設定しなければ telnet で作業できない

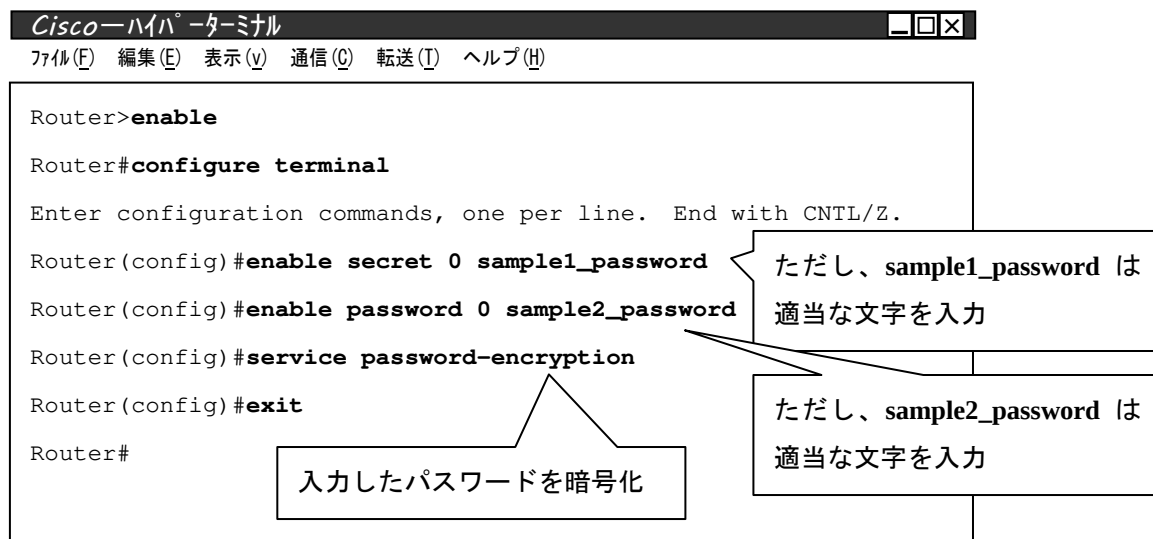
設定するパスワードには

- ① enable の際に使用するパスワード（ enable password,enable secret ）
- ② telnet の際に使用するパスワード
- ③ その他（ユーザを作成した場合）

があります。

11.2 パスワードの設定(1)

Enable password と Secret password の設定



The image shows a Cisco HyperTerminal window titled "Cisco - ハイパーターミナル". The menu bar includes "ファイル(F)", "編集(E)", "表示(V)", "通信(C)", "転送(T)", and "ヘルプ(H)". The terminal output shows the following commands and prompts:

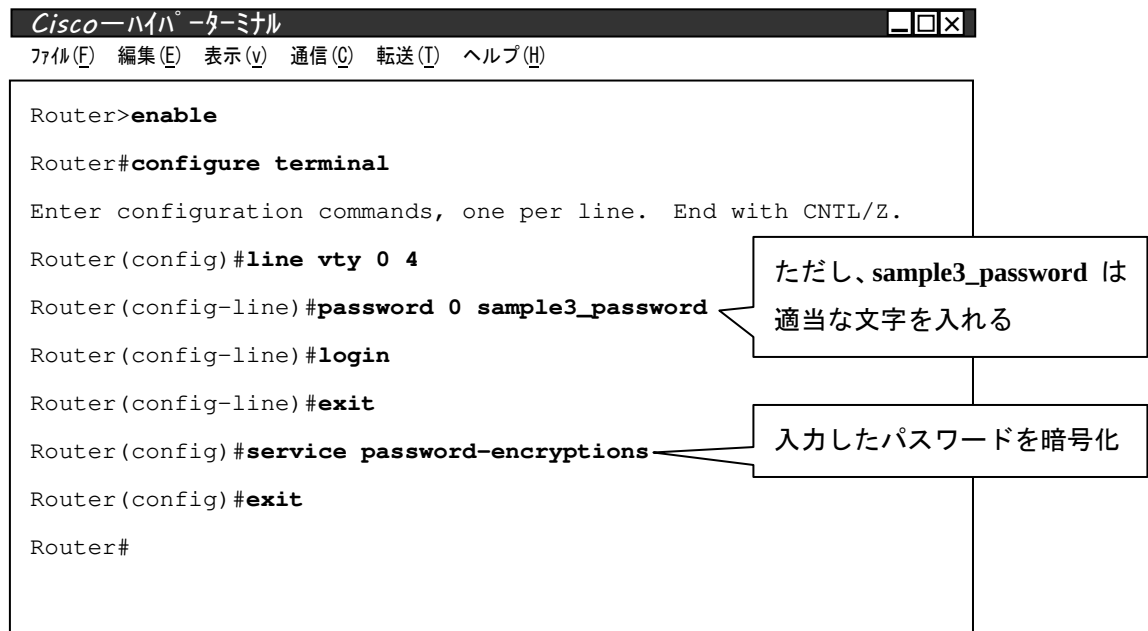
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret 0 sample1_password
Router(config)#enable password 0 sample2_password
Router(config)#service password-encryption
Router(config)#exit
Router#
```

Three callout boxes provide additional information:

- A box pointing to the `sample1_password` command: "ただし、sample1_password は 適当な文字を入力"
- A box pointing to the `sample2_password` command: "ただし、sample2_password は 適当な文字を入力"
- A box pointing to the `service password-encryption` command: "入力したパスワードを暗号化"

enable password には enable secret が使用される

Telnet の際に使用する password の場合



```
Cisco—ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

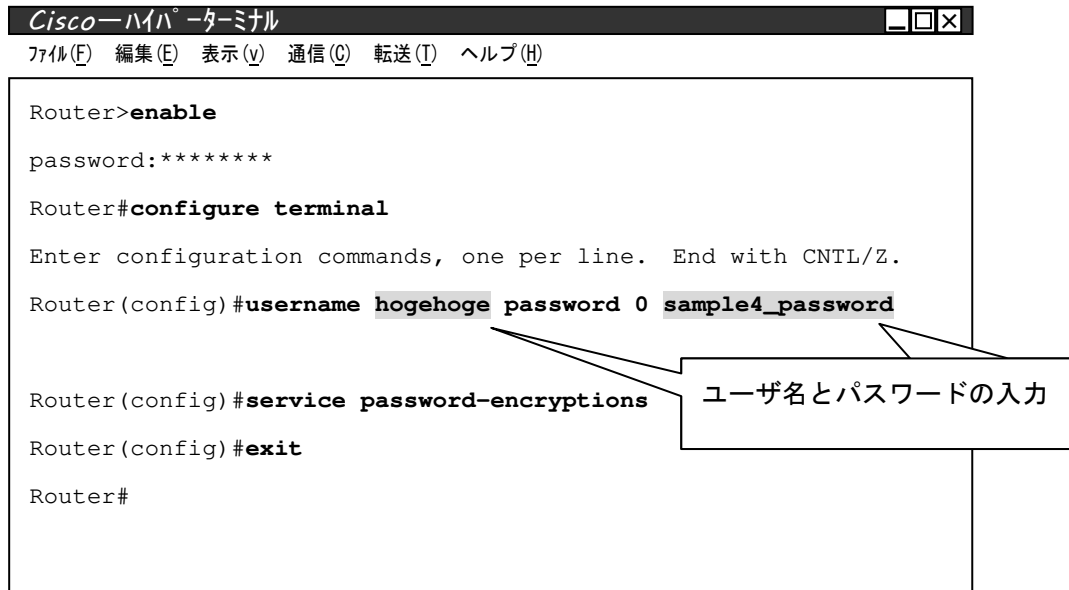
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password 0 sample3_password
Router(config-line)#login
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#exit
Router#
```

ただし、sample3_password は
適当な文字を入れる

入力したパスワードを暗号化

11.3 パスワードの設定(2)

ユーザの設定



```
Cisco-ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(I) ヘルプ(H)

Router>enable
password:*****
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#username hoge hoge password 0 sample4_password
Router(config)#service password-encryption
Router(config)#exit
Router#
```

ユーザ名とパスワードの入力

`username` の行の `hoge hoge` は適当なユーザ名を入力する。また、`sample4_password` も適切な `password` を入力する。またこれを設定した場合、telnet によるログインはユーザが使用される。

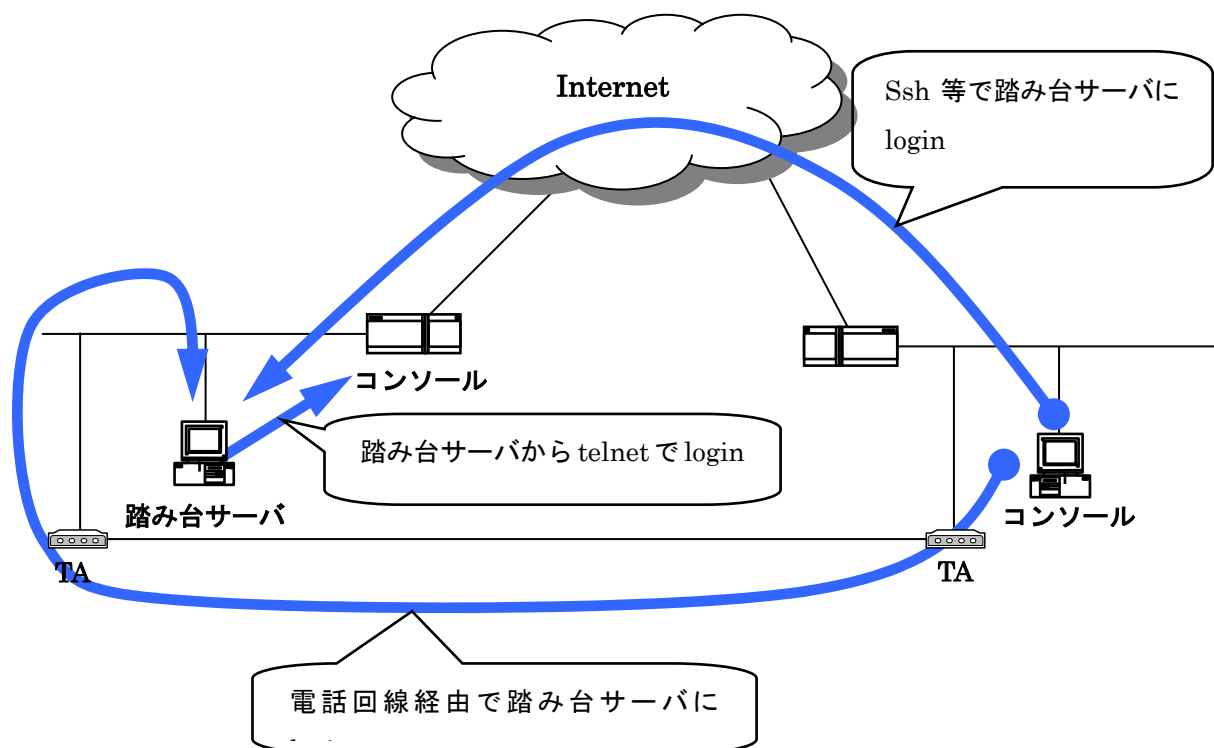
11.4 問題点

■ Telnet による環境設定の問題点

- i 暗号化されていないので、セキュアでない。
- ii セキュアでないので、インターネットを経由して使用してはいけない

↓

- ① 踏み台サーバを用意して対応する
- ② 電話回線を用いてバックドアを作り対応する



■ Router のフィルタリング

インターネット接続ルータには大きく 2 つのフィルタがかけられています。

1 telnet port のフィルタリング

- ① Router への Telnet 接続は許可しない。

2 アクセスリストによるフィルタリング

- ① インターネット側からは接続を許可している web サーバや Mail サーバ宛て以外のあて先パケットは通過させない。
- ② LAN 内部からはインターネット側に送信したいパケット以外は通過させない。

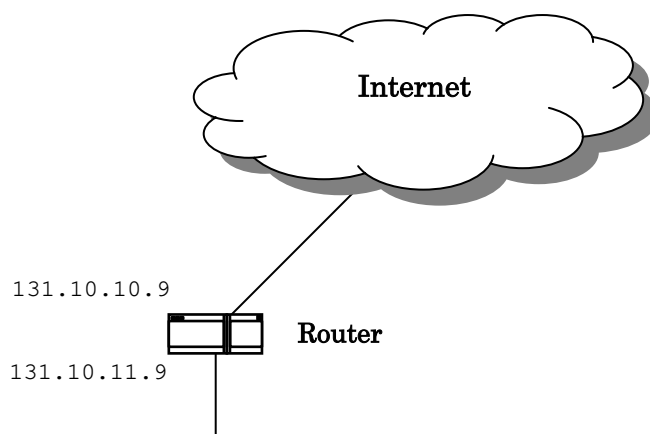
1 つ目は Router への telnet 接続の許可・不許可です。インターネット側から Router への telnet 接続を許可しない設定と、LAN 内部からも権限をもった管理者を送信元のアドレスとする Router へ telnet 接続を許可する設定です。telnet 接続を許可した Router へはインターネット側から不特定多数の接続が来てしまいます。そこで通常は Router への telnet 接続を許可しません。

2 つ目はアクセスリストです。例えば、インターネット側からは接続を許可している web サーバや Mail サーバ宛て以外のあて先パケットは通過させない、LAN 内部からはインターネット側に送信したいパケット以外は通過させない、という設定です。

これらのフィルタ設定を通過して、他の ISP 等を利用してインターネット接続ルータに telnet 接続することは出来ません。そこで Router メンテナンスで接続する場合には、

- ① 踏み台サーバを用意して対応する
- ② 電話回線を用いてバックドアを作り対応する

という 2 つのいずれかかまたは両方の方法をとります。



```

Cisco-ハイパ-ターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Router>enable
Password:*****
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface ethernet0/1
Router(config-if)#ip address 131.10.10.9 255.255.255.0
Router(config-if)#ip access-group 101 in
Router(config-if)#ip access-group 101 out
Router(config-if)#exit
Router(config)#interface ethernet1/1
Router(config-if)#ip address 131.10.11.9 255.255.255.0
Router(config-if)#ip access-group 101 in
Router(config-if)#ip access-group 101 out
Router(config-if)#exit
Router(config)#access-list 101 deny tcp any host 131.10.10.9 eq telnet
Router(config)#access-list 101 deny tcp any host 131.10.11.9 eq telnet
Router(config)#access-list 101 permit ip any any
Router(config)#^Z

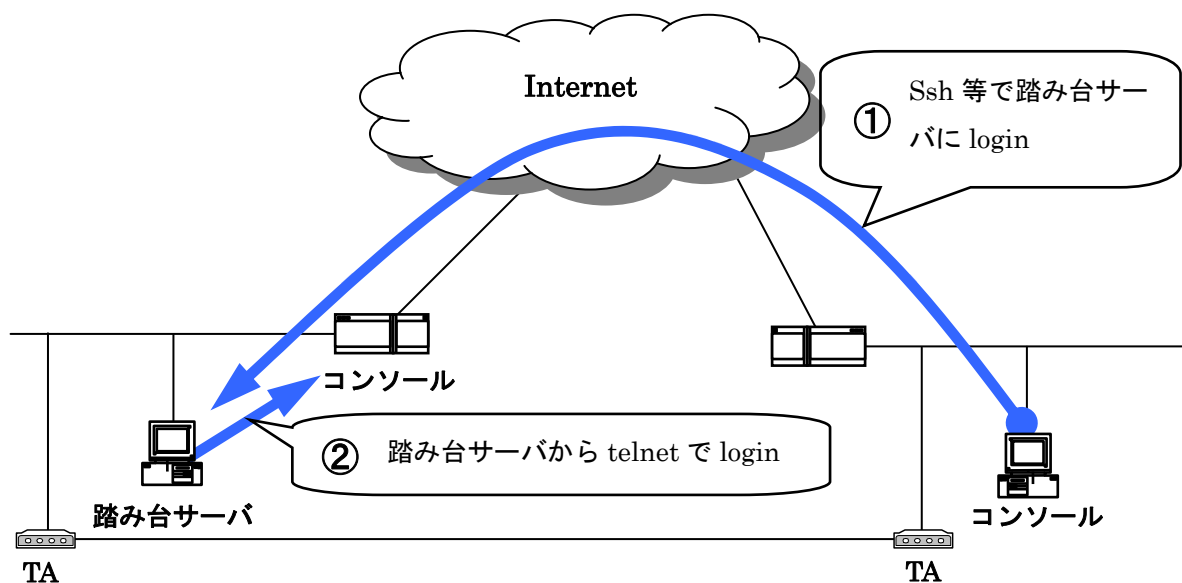
```

■ 踏み台サーバを利用する

インターネット側からは許可されたポートと宛先の組み合わせで、「踏み台サーバ」へのパケットは許可しておきます。「踏み台サーバ」はユーザ認証でアクセス可能なユーザを選別したり、host allow の設定でアクセス可能ホストを選別します。

インターネットを経由している部分をセキュアにするために ssh を利用します。ssh をサポートしている Router は多くはありませんが、サーバに対して ssh で接続できればセキュアな接続が実現できます。

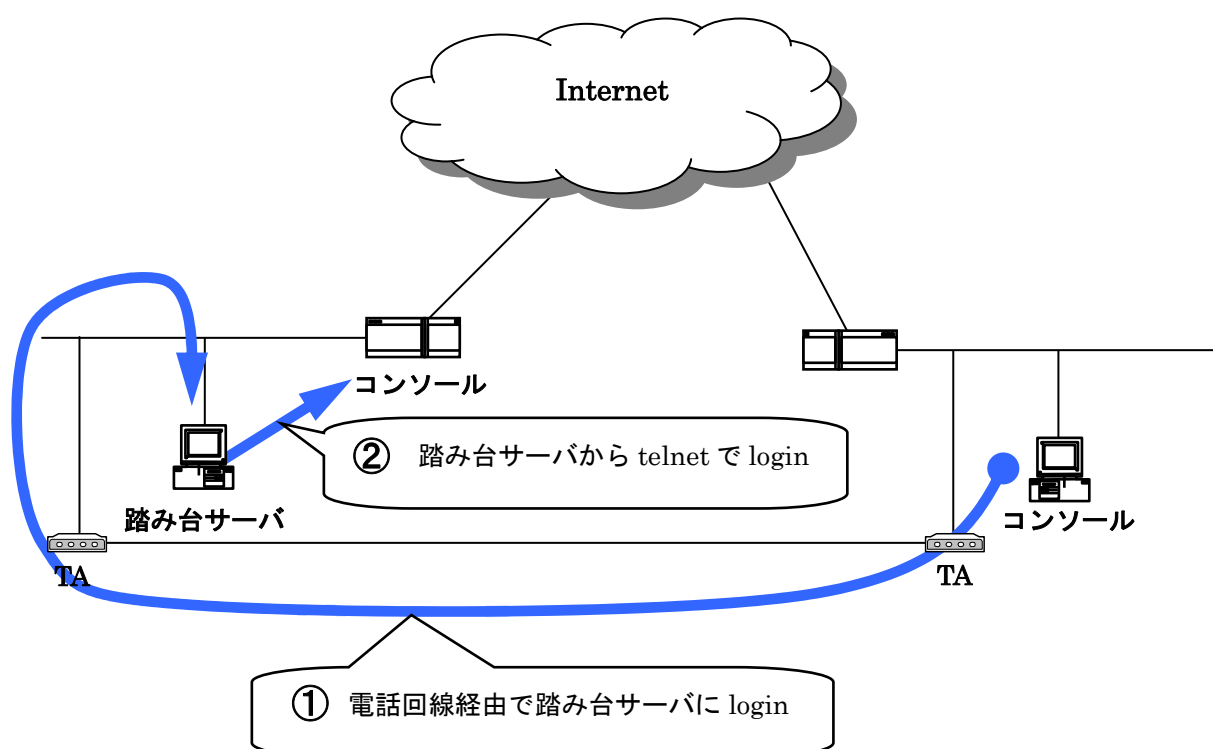
Router は「踏み台サーバ」からのアクセスのみ受け付けるようにしておきます。その後、インターネット側からのセキュアな接続が確立できているサーバから、インターネット接続ルータに telnet 接続しメンテナンスします。



■ 電話回線を用いてバックドアを作り対応する

LAN 内部に設けたメンテナンス接続用のモデム・TA から接続する方法です。インターネットを経由しないので ssh 等を利用しなくてもインターネット側からはセキュアな接続になります。

モデム・TA からユーザ認証でアクセス可能なユーザが「踏み台サーバ」にログインし、サーバからインターネット接続ルータに telnet 接続しメンテナンスします。



実習**アクセス設定**

ディレクトリ・ホスト名・IP Address・ユーザー名・パスワードなどの情報はインストラクターから得ます。

1. ルータの telnet 設定を無効にします。
2. ルータの telnet 設定を踏み台サーバのみ有効にします。
3. 踏み台サーバではないホストから telnet 接続できないことを確認します。

確認

踏み台サーバではないホストから telnet 接続できないことが確認できましたか?

実習**踏み台サーバの設定**

ディレクトリ・ホスト名・IP Address などの情報はインストラクターから得ます。

4. 踏み台サーバとなるホストにユーザを設定します。このユーザがルータをメンテナンス可能なユーザとなります。
5. 踏み台サーバからルータへ telnet 接続できることを確認します。
6. 別のホストからルータへ telnet 接続できないことを確認します。
7. 別のホストから踏み台サーバにログインします。
8. 更に踏み台サーバを通してルータに telnet 接続します。

確認

踏み台サーバから Router に telnet 接続できましたか?

実習**アクセスリストの設定**

ディレクトリ・ホスト名・IP Address などの情報はインストラクターから得ます。

9. ルータにアクセスリストを設定します。
10. 踏み台サーバからルータへ telnet 接続できることを確認します。
11. 別のホストからルータへ telnet 接続できないことを確認します。
12. 別のホストから踏み台サーバにログインします。
13. 更に踏み台サーバを通してルータに telnet 接続します。

確認

踏み台サーバから Router に telnet 接続できましたか?

実習**ダイヤルアップの設定**

回線シミュレーターがある場合に行います。

ディレクトリ・ホスト名・IP Address などの情報はインストラクターから得ます。

14. モデムまたは TA を通じて踏み台サーバにダイヤルアップできる設定を作ります。

15. 別のホストから踏み台サーバにログインします。

16. 更に踏み台サーバを通してルータに telnet 接続します。

確認

踏み台サーバから Router に telnet 接続できましたか?

索引

AS.....	23
Autonomous System	23
BGP.....	23, 24
cfgmaker	116, 118
CIDR	35
Classless Interdomain Routing	35
clock timezone	37
Community 名	114
configure	9, 11
configure memory.....	11
configure network	11
configure terminal.....	11
configure モード	13
copy	7, 8, 9, 47
cron	117
crontab.....	117
disable.....	3
Dynamic Routing	23
EGP.....	24
EGPs	24
EIGRP.....	24
enable	2, 3, 9, 45, 72, 125
enable password	3, 125
enable secret.....	2, 3, 125
enable モード	2, 9
exit	2, 3
Exterior Gateway Protocols	24
Facility.....	71
Flash	5
FreeBSD	53, 71
ftp.....	44, 60
GetNext	85
GetNextRequest	85
GetRequest	84, 85

GetResponse	84, 85
hostname	37
hosts.allow	57
HP OpenView	98
HTML	97, 102, 118
IGPs	24
IGRP	24
inetd	52, 55, 58
inetd.conf	53, 55
Interior Gateway Protocol	24
ip classless	36, 38
ip domain-name	37
ip name-server	37
ip rip receive version	35
ip rip send version	35
ip route	20, 28, 30, 38
ip subnet-zero	37
line	45
Log Level	69, 71
logging	70
login	45
Management Information Base	78, 91
MIB	78, 81, 84, 85, 86, 87, 88, 91, 92, 95
MRTG	97, 102, 105, 107, 112, 114, 116, 117, 118
mrtg.cfg	105, 116, 117, 118
netstat -a	58
network	32
no shutdown	13
ntp server	38
NVRAM	5, 7, 8, 11, 17, 47
OID	93
OSPF	23, 24, 26
password 0	45
PDU	83
permission	55, 56
Protocol Data Unit	83
quit	2, 3
RAM	5, 7, 11

RIP	23, 24, 26, 32, 35, 36
RMON.....	94
router rip	32, 35
running-config	5, 7, 9, 38, 62
Secure Shell.....	46
show flash	5
show interface	38
Simple Network Management Protocol	78
SMI	91
SNMP	77, 78, 81, 83, 91, 97, 98, 99, 102, 105, 114
ssh.....	46, 132, 133
startup-config	5, 7, 8, 9
Static Routing	22, 28
Structure of Management Information.....	91
Sun Net Manager.....	98
syslog	68, 70, 71
syslog.conf.....	71, 72
syslogd	71, 72
System Log	67
TCP	81
telnet.....	44, 45, 46, 125, 128, 130, 132, 133
tftp	7, 8, 17, 44, 48, 53, 58
TFTP サーバ	5, 7, 8, 17, 47, 49, 52, 53, 57, 58, 60, 61, 62
Trap.....	83, 89
Trivial File Transfer Protocol	52
UDP	81, 83
version 2	32
VLSM.....	35
write memory	9
エージェント	78, 81, 83, 84, 85, 86, 87, 88, 89, 91, 94, 100
応答	81, 83, 84, 86, 88, 89
オブジェクト識別子	93
可変長サブネットマスク	35
クラスフル	35
クラスレス	35
経路集約	35
自律システム	23, 24
スタティックルーティング	20



スタティックルート	20
静的経路制御	22
静的ルーティング	20
ダイナミックルーティング	20
ダイナミックルーティングプロトコル	20
ディスタンスベクタ	26
デフォルトルート	22
動的経路制御	23
動的ルーティング	20
特権モード	2, 3, 9, 45
ネットマスク	35, 37
非特権モード	2, 3
フィルタリング	130
プロトコル動作	83, 84, 85
マネージャ	77, 78, 81, 83, 84, 85, 86, 87, 88, 89, 91, 94, 95, 98
ユーザーモード	2
要求	81, 83, 84, 85, 87, 89
リンクステート	26
ルーティングテーブル	5, 20, 23, 26
ルーティングプロトコル	23, 24, 26, 35
ログ	67, 68, 69