

Specification for pure IP links on the Washington-Tokyo-Melbourne MTN segment

(Version 2.3)

1. Circuit configuration and protocols in transport

(1) Physical level

Circuit type : Leased circuit (digital circuit)
Carriers : MCI WorldCom (USA portion)
 : KDD (Japan portion)
 : TELSTRA (Australia portion)
Physical speed : 64kbps
Round trip time : 272 msec. (Washington – Tokyo)
 : 140 msec. (Melbourne – Tokyo)

(2) Link level

Protocol : Cisco HDLC
Framing : HDLC Framing
Authentication : None

Note 1) It is more efficient to use the Cisco default encapsulation method (Cisco HDLC) than PPP between Cisco routers on serial links.

Note 2) In case of ISDN backup in future, PPP (Point to Point Protocol) with CHAP (Challenge Handshake Authentication Protocol) might be used.

Note 3) It should be noted that if Frame Relay network is used in the future then the encapsulation will need to be set to Frame Relay.

Compression : None

Note 1) It is possible to configure point-to-point software compression on serial interfaces that use HDLC encapsulation. Compression reduces the size of a HDLC frame via lossless data compression.

Note 2) Compression might significantly affect router performance.

Especially in case of CPU load exceeds 65 %, compression should not be used.

(3) Network level

Protocol : IP v4 (Internet Protocol version 4)
 : ICMP (Internet Control Message Protocol) for PING and TRACEROUTE

(4) Transport level

Protocol : TCP (Transmission Control Protocol)
 : UDP (User Datagram Protocol) may be used for connectionless applications such as SNMP (Simple Network Management Protocol), TFTP (Trivial File Transfer Protocol) and so on in future.

(5) Routing protocol : Border Gateway Protocol version 4 (BGP-4)

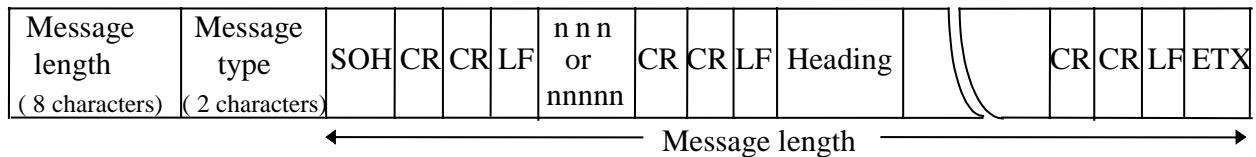
2. Message Switching System (MSS) application

In regard to reception/transmission, MSS application will be changed from X.25 to TCP socket basis. For easy and safe migration to IP, however, existing mechanism such as store-and-forward, queuing and other message processing should be kept.

2.1 Message structure in TCP socket stream

The message structure basically complies with the "Use of TCP/IP on the GTS". The structure in TCP socket stream is shown in Figure 1.

- Each message is preceded by a message length field of eight ASCII characters and a message type field of two ASCII characters.
- Message length is counted from SOH to ETX inclusive and must be leading zeroes as necessary.
- Message type must be encoded as AN for alphanumeric, BI for binary or FX for facsimile.



Message length : Length from SOH to ETX (e.g. 00001826 = 1826bytes)
 Message type : AN for alphanumeric, BI for binary, FX for facsimile
 nnn : 3 digit channel sequence number (001 to 999, and 000)
 nnnnn : 5 digit channel sequence number (00001 to 99999, and 00000)

The channel sequence number 000 (or 00000) should indicate an initialisation, and should not cause retransmission requests.

Figure 1 Message structure for TCP socket

2.2 Usage of TCP socket

(1) Separate connections for the message types

Each of alphanumeric, binary messages and T4 charts flows on each connection, respectively.

(2) Separate connections for transmission and reception

Messages/charts are sent on a connection and are received on other connection. So-called one-way connection is adopted. As the result, the number of TCP connections between two centers becomes six in total (see Figure 2).

(3) Establishing a connection by sender

The sender always establishes the connection for transmission. In short, the sender opens a connection by ACTIVE OPEN and the receiver opens it by PASSIVE OPEN.

(4) Permanent connections

Once established a connection is left up indefinitely as long as there is not special reason such as losing synchronization and switching host in backup MSS. In short, existing X.25 PVC concept could be succeeded.

Note) Function of idle timer may be implemented in the socket application to enable so-called SVC like use. In that case, the idle time should be practically infinite.

(5) Message synchronization

All new connections must begin with a message length and type structure. Receiver should always check the message synchronization as follows:

- the first 8 characters are ASCII numeric (essential check)
- the 9th and 10th characters are AN, BI or FX (essential check)
- the 11th character is SOH (optional check)
- the last character is ETX (optional check)

If the synchronization is lost, the receiver shall break the connection.

(6) Minimal data loss within simple mechanism

Although each center makes an effort to minimize data loss, some messages might be lost at a connection break. Any complicated mechanism should not be used to recover the messages because the basic concept of TCP socket is simple and light message handling.

Possible means in this issue are:

- To set the "send buffer (stream buffer) size" to a low value in consideration of throughput performance
 Each send buffer size in operation is:
 - (a) Melbourne : 4 kbytes
 - (b) Tokyo : 4 kbytes
 - (c) Washington : 8 kbytes
- To close a connection in due course when it is necessary to break it

- To use the existing request/reply (repeat) mechanism by addressed message when the message loss happens (refer paragraph 2.3)

Note1) In case of sudden break and re-establishment of a connection, some messages might be duplicated intentionally or accidentally. It seems that such duplication does not cause any problems because of the existing function for duplication check and elimination at each center.

Note2) Channel sequence number will be expanded from 3 digits to 5 digits in the near future for convenience of the request/reply. Between Washington and Tokyo, 5 digit sequence numbers are used in the preliminary test and subsequent operation.

(7) Port numbers agreed by the three centers

In an active open at the sender, an agreed number is used for the destination port field to connect with the corresponding process at the receiver, and a dynamically assigned number is used for the source port field.

In short, the receiver's port number is fixed but the sender's source port number is changeable.

Agreed port numbers for connections are:

(a) at Melbourne

- 30053 - Tokyo text input
- 30054 - Tokyo binary input
- 30055 - Tokyo chart input
- 30056 - Washington text input
- 30057 - Washington binary input
- 30058 - Washington chart input

(b) at Tokyo

- 25103 - Washington text input
- 25104 - Washington binary input
- 29035 - Washington chart input
- 25203 - Melbourne text input
- 25204 - Melbourne binary input
- 29037 - Melbourne chart input

Note) Range of dynamically assigned source port numbers in active open at Tokyo is 1024 to 5000. Washington and Melbourne are able to filter incoming packets from Tokyo with source port numbers without the range if necessary.

(c) at Washington

- 30001 - Tokyo text input
- 30002 - Tokyo binary input
- 30003 - Tokyo chart input
- 30004 - Melbourne text input
- 30005 - Melbourne binary input
- 30006 - Melbourne chart input

(8) Second connection attempt

If the Receiver receives a new connection request then it should close any existing connection and accept the new connection. *(This is because Melbourne has seen cases where the sender believes the call has been dropped but the receiver is unaware of it.)*

(9) Message segmenting of fax messages

WMO message segmenting should NOT be used on the fax connection.

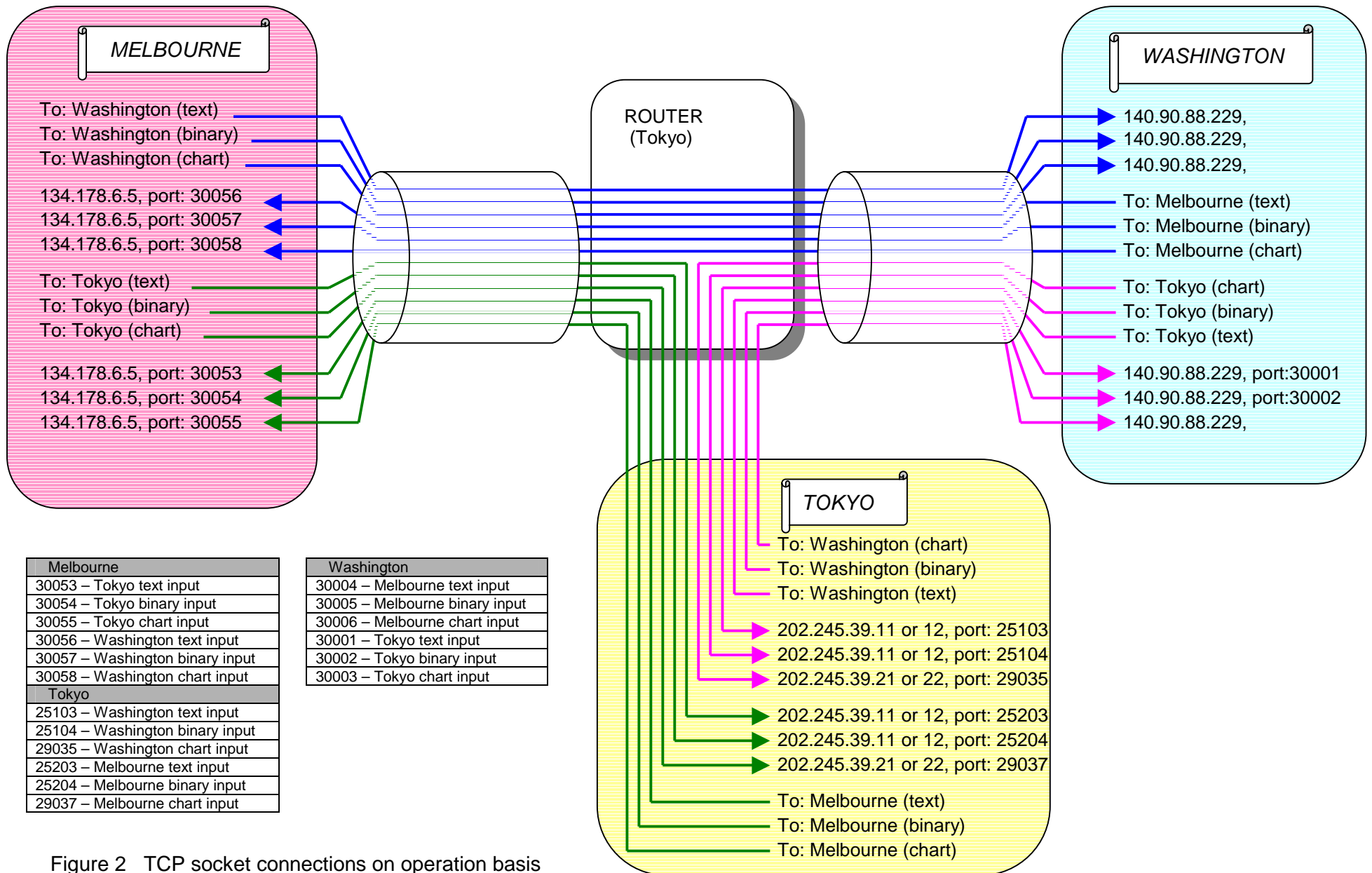


Figure 2 TCP socket connections on operation basis

2.3 Procedures for recovery of missing data

(1) Request/Repeat of missing text messages

Requests for missing text messages should be sent on the text connection. T₁T₂ (in message header) of "BM" should be used. The request formats are:

(a) Requesting a message

```
(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BMRR01 CaCaCaCa YYGgGg
(CR)(CR)(LF) CCCC
(CR)(CR)(LF) SQN nnnnn= [or SQN nnn=]
(CR)(CR)(LF)(ETX)
```

(b) Requesting a selected number of messages

```
(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BMRR01 CaCaCaCa YYGgGg
(CR)(CR)(LF) CCCC
(CR)(CR)(LF) SQN nnnnn/nnnnn/nnnnn= [or SQN nnn/nnn/nnn=]
(CR)(CR)(LF)(ETX)
```

(c) Requesting a continuous series of messages

```
(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BMRR01 CaCaCaCa YYGgGg
(CR)(CR)(LF) CCCC
(CR)(CR)(LF) SQN nnnnn-nnnnn= [or SQN nnn-nnn=]
(CR)(CR)(LF)(ETX)
```

A requested message should be retransmitted with its original heading and with the latest channel sequence number.

Note1) In case of the "nnnnn-nnnnn=" request, the quoted numbers should be included in repetition. For example, "SQN 00210-00213=" indicates a request for repetition of 00210, 00211, 00212 and 00213.

Note2) There is limitation at RTH Tokyo in the reply function. That is, the maximum number of repetition messages per a request is 60.

Note3) When there is an error in a request message, Tokyo replies to it with a notification message in the following format:

```
(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BMDA01 CaCaCaCa YYGgGg
(CR)(CR)(LF) RJTD
(CR)(CR)(LF) ERR (the erroneous request line)
(CR)(CR)(LF)(ETX)
```

(e.g. in case of missing "=")

```
(SOH)
(CR)(CR)(LF) 20015
(CR)(CR)(LF) BMDA01 KWBC 290105
(CR)(CR)(LF) RJTD
(CR)(CR)(LF) ERR SQN 19991-19999
(CR)(CR)(LF)(ETX)
```

(e.g. in case of a request for more than 60 messages)

```
(SOH)
(CR)(CR)(LF) 555
(CR)(CR)(LF) BMDA01 AMMC 051215
(CR)(CR)(LF) RJTD
(CR)(CR)(LF) ERR SQN 101-200=
(CR)(CR)(LF)(ETX)
```

Note4) When a requested message is not available, Tokyo replies to it with a notification message in the following format:

(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BMDA01 CaCaCaCa YYGGgg
(CR)(CR)(LF) RJTD
(CR)(CR)(LF) NIL (unavailable channel sequence number(s))=
(CR)(CR)(LF)(ETX)

(e.g.)
(SOH)
(CR)(CR)(LF) 00000
(CR)(CR)(LF) BMDA01 KWBC 082345
(CR)(CR)(LF) RJTD
(CR)(CR)(LF) NIL 78333-78340=
(CR)(CR)(LF)(ETX)

(2) Request/Repeat of missing binary messages

Requests for missing binary messages should be sent on the binary connection. T_1T_2 (in message header) of "BI" should be used. The request formats are:

(a) Requesting a message

(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BIRR01 CaCaCaCa YYGGgg
(CR)(CR)(LF) CCCC
(CR)(CR)(LF) SQN nnnnn= [or SQN nnn=]
(CR)(CR)(LF)(ETX)

(b) Requesting a selected number of messages

(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BIRR01 CaCaCaCa YYGGgg
(CR)(CR)(LF) CCCC
(CR)(CR)(LF) SQN nnnnn/nnnnn/nnnnn= [or SQN nnn/nnn/nnn=]
(CR)(CR)(LF)(ETX)

(c) Requesting a continuous series of messages

(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BIRR01 CaCaCaCa YYGGgg
(CR)(CR)(LF) CCCC
(CR)(CR)(LF) SQN nnnnn-nnnnn= [or SQN nnn-nnn=]
(CR)(CR)(LF)(ETX)

A requested message should be retransmitted with its original heading and with the latest channel sequence number.

Note1) The quoted numbers of "nnnnn-nnnnn=" should be inclusive the same as the text connection case.

Note2) There is limitation at RTH Tokyo in the repetition messages (max.60) the same as the text connection case.

Note3) When there is an error in a request message, Tokyo replies to it with a notification message in the following format:

(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BIDA01 CaCaCaCa YYGGgg
(CR)(CR)(LF) RJTD
(CR)(CR)(LF) ERR (the erroneous request line)
(CR)(CR)(LF)(ETX)

Note4) When a requested message is not available, Tokyo replies to it with a notification message in the following format:

(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BIDA01 CaCaCaCa YYGGgg
(CR)(CR)(LF) RJTD
(CR)(CR)(LF) NIL (unavailable channel sequence number(s))=
(CR)(CR)(LF)(ETX)

(3) Request/Repeat of missing fax messages

Requests for missing fax messages should be sent on the fax connection as for other messages. T₁T₂ (in message header) of "BM" or "BI" may be used.

Note) As Tokyo FAX system does not implement the addressed message function, a request for missing fax messages to Tokyo should be sent on the alphanumeric connection in plain message like follows:

```
(SOH)
(CR)(CR)(LF) nnnnn [or nnn]
(CR)(CR)(LF) BMAA01 RJTD YYGGgg
(CR)(CR)(LF) CCCC
(CR)(CR)(LF) TO TELECOM SUPERVISOR OF RTH TOKYO
(CR)(CR)(LF) PLS RE-TRANSMIT THE FOLLOWING FAX CHART:
(CR)(CR)(LF) SQN nnnnn= [or SQN nnn=]
[and/or (CR)(CR)(LF) TTAAii CCCC YYGGgg=]
(CR)(CR)(LF)(ETX)
```

3. File transfer of satellite imagery data

METEOSAT imagery data are currently transferred by FTP from Melbourne to Tokyo on operational basis. Furthermore the file switching mechanism has been tested on the Washington-Tokyo-Melbourne segment since June 1998. In near future, GOES imagery data provided by Washington may be reached Tokyo and Melbourne by the mechanism. Encapsulation technique is currently used to enable FTP on X.25 link. With this time migration to pure IP, the encapsulation will become unnecessary.

4. Addressing

(1) General concepts

Addressing concepts accord with the "Use of TCP/IP on the GTS". A pair of official IP addresses assigned by WMO Secretariat are used for a link between routers at two centers, and a few official IP addresses prepared by each center are used for end hosts eligible to use the GTS.

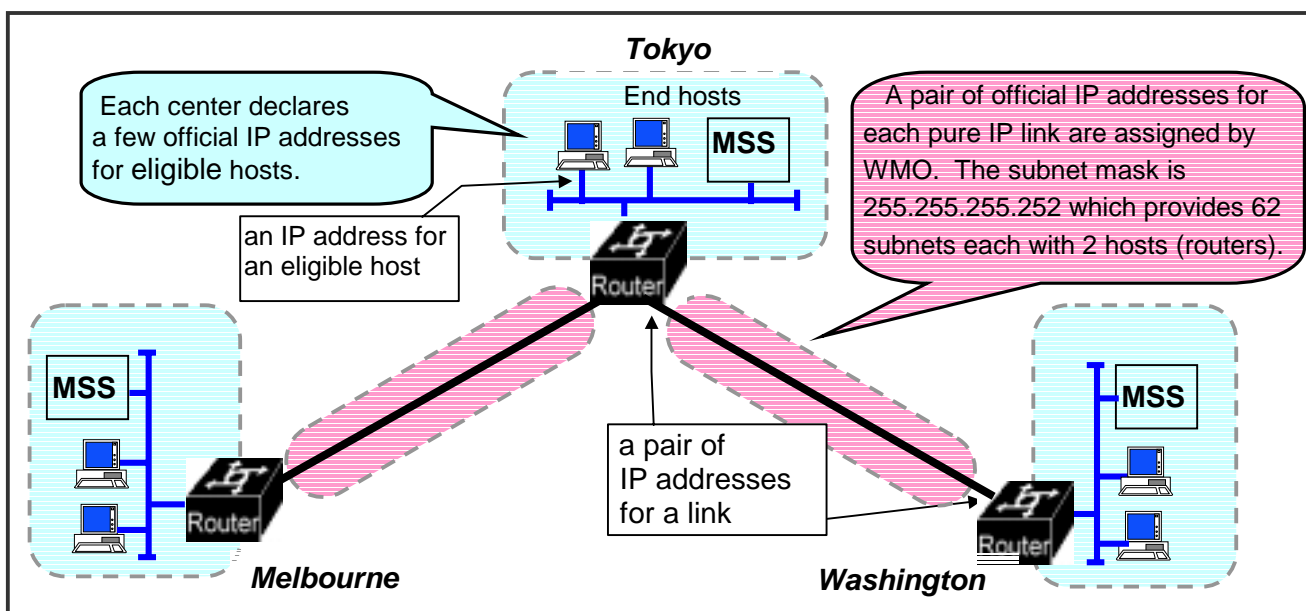


Figure 3 General concepts of Addressing

(2) IP addresses for operation

(a) IP addresses for links

- Washington – Tokyo pure IP link
 - Sub-network with mask : 193.105.178.28 / 30
 - Washington router : 193.105.178.29
 - Tokyo router : 193.105.178.30
- Melbourne – Tokyo pure IP link
 - Sub-network with mask : 193.105.178.20 / 30
 - Melbourne router : 193.105.178.21
 - Tokyo router : 193.105.178.22

(b) IP addresses for eligible hosts

- Washington
 - MSS :140.90.88.229
 - FTP server :140.90.88.142
 - Note) Although Washington has a backup host, they must make a manual switch if problems occur. Both hosts use the same IP address.
- Tokyo
 - MSS (cadess1) : 202.245.39.11
 - MSS (cadess2) : 202.245.39.12
 - FAX system (acxs1) : 202.245.39.21
 - FAX system (acxs2) : 202.245.39.22
 - FTP server (jmasv1) : 202.245.36.1
 - FTP server (jmasv2) : 202.245.36.2
- Melbourne
 - COMMS1 : 134.178.6.2
 - COMMS2 : 134.178.6.1
 - COMMS (notional operational machine): 134.178.6.5

5. Routing and filtering

(1) Routing protocol

BGP-4 (Border Gateway Protocol version 4) [RFC1771] is used as dynamic routing protocol on IP links. It allows centers to create loop free inter-domain routing between autonomous systems.

BGP-4 can distribute subnetted routes. Instead of propagating host-based routes or full network routes, routing can be based on subnetted networks thanks to this feature. That is to say, instead of declaring hosts eligible to use the GTS, a center could declare a full subnet of eligible hosts. In that case, the routing information consists of just an IP address and a subnet mask.

An outline of procedures are:

- Two neighboring routers which speak BGP-4 form a TCP connection (port number 179) and exchange messages to open and confirm the connection parameters (OPEN) ;
- The neighboring routers initially exchange their full BGP routing tables (INITIALIZE) ;
- From the initializing, update information is exchanged only when the routing table changes (UPDATE) ;
- Keepalive packets are exchanged every 30 seconds (default value) to ensure that the connection is alive (KEEPALIVE).

(2) Autonomous System (AS)

An Autonomous System (AS) indicates an entity comprising IP networks having a single clearly defined routing policy. In most case of the GTS, each center operates each AS. Inside an AS, IP packets can be routed using one or more Interior Routing Protocols such as RIP (Routing Information Protocol) and OSPF (Open Shortest Path First), although BGP-4 should be running between two different ASs.

For the time being, the three centers use not official but private AS numbers assigned by WMO Secretariat considering the draft allocation scheme in Table 1.

The AS numbers for the centers are:

- Washington : AS 64513
- Melbourne : AS 64512
- Tokyo : AS 64520

Table 1 Draft allocation scheme of private AS numbers

Regions	Range	Available number
MTN centers and reserve	64512 to 64639	128
Centers within RA I	64640 to 64767	128
Centers within RA II	64768 to 64895	128
Centers within RA III	64896 to 65023	128
Centers within RA IV	65024 to 65151	128
Centers within RA V	65152 to 65279	128
Centers within RA VI	65280 to 65407	128
Antarctic and reserve	65408 to 65471	64
Private use by GTS Centres	65472 to 65535	64
(1) The IANA (Internet Assigned Numbers Authority) allocates from 64512 to 65535 as private AS numbers in RFC1930. (2) That is to say, WMO can use 1024 AS numbers within the GTS. (3) WMO assigns them to centers which decided to use not an official but a private AS number, according to the above rule.		

(3) Filtering

Each center should filter incoming and outgoing traffic in accordance with the following conditions.

- To allow only agreed protocols (port numbers)
- To allow only agreed destination IP addresses
- To allow only agreed source IP addresses

6. Consideration of duplicated system (Backup issue with an IP based GTS)

(1) MSS application case

Since an individual IP address is generally associated with only one host, a duplicated MSS which is comprised of two hosts has a pair of IP addresses. In a moment, either of them is for an operational host, and the other is for backup one. It is necessary to control establishing a connection between operational hosts at both sides.

Control rules are:

- (a) In a backup host
 - TCP socket ports for MSS applications must be NOT OPEN (both active and passive).
- (b) In an operational host
 - Receiver must keep the agreed TCP socket ports being passive OPEN.
 - Sender must implement the algorithm to control an alternate IP address.
 - When active open towards Receiver with an IP address fails, Sender must try ANOTHER IP address.

These general conditions and rules do not apply at Washington and Melbourne - refer (a)(b) below.

Each center's backup conditions are:

(a) Washington

Although Washington has a backup host, they must make a manual switch if problems occur.

Both hosts use the same IP address of 140.90.88.229.

(b) Melbourne

The notional operational machine is 'COMMS' with IP address 134.178.6.5. This normally maps to actual machine 'COMMS1' 134.178.6.2. The backup and test machine is 'COMMS2' 134.178.6.1. The generic COMMS machine 134.178.6.5 will map to either COMMS1 or COMMS2 depending on which machine is in operational service. No action by neighbouring Centre is necessary when Melbourne's backup machine is in operational service.

In active OPEN from Washington or Tokyo, the destination IP address should be 134.178.6.5. However, it should be noted that the real IP addresses of 134.178.6.1 and 134.178.6.2 are used for the source IP address in a packet from Melbourne. Therefore Washington and Tokyo must allow 134.178.6.1 and 134.178.6.2 as agreed source IP addresses in filtering configuration.

(c) Tokyo

- A pair of IP addresses for MSS : 202.245.39.11 and 202.245.39.12
- A pair of IP addresses for FAX system : 202.245.39.21 and 202.245.39.22

(2) FTP case (satellite imagery data)

In METEOSAT case, the following simple manner is used for handling IP addresses of two hosts.

- Tokyo always keeps "ftpd" (TCP No.21) of the backup host being disable.
- When Melbourne fails in ftp PUT, they try another host.

Table 2 Manner to handle IP addresses of two hosts

Host status	IP communication	ftpd (ftp daemon)	ftp session
Operational host	Enable (IP reachable)	Enable	Enable
Backup host	Enable (IP reachable)	Disable	Disable

- 7. System configuration and specification
 - (1) System configuration at each center
 - (a) Washington

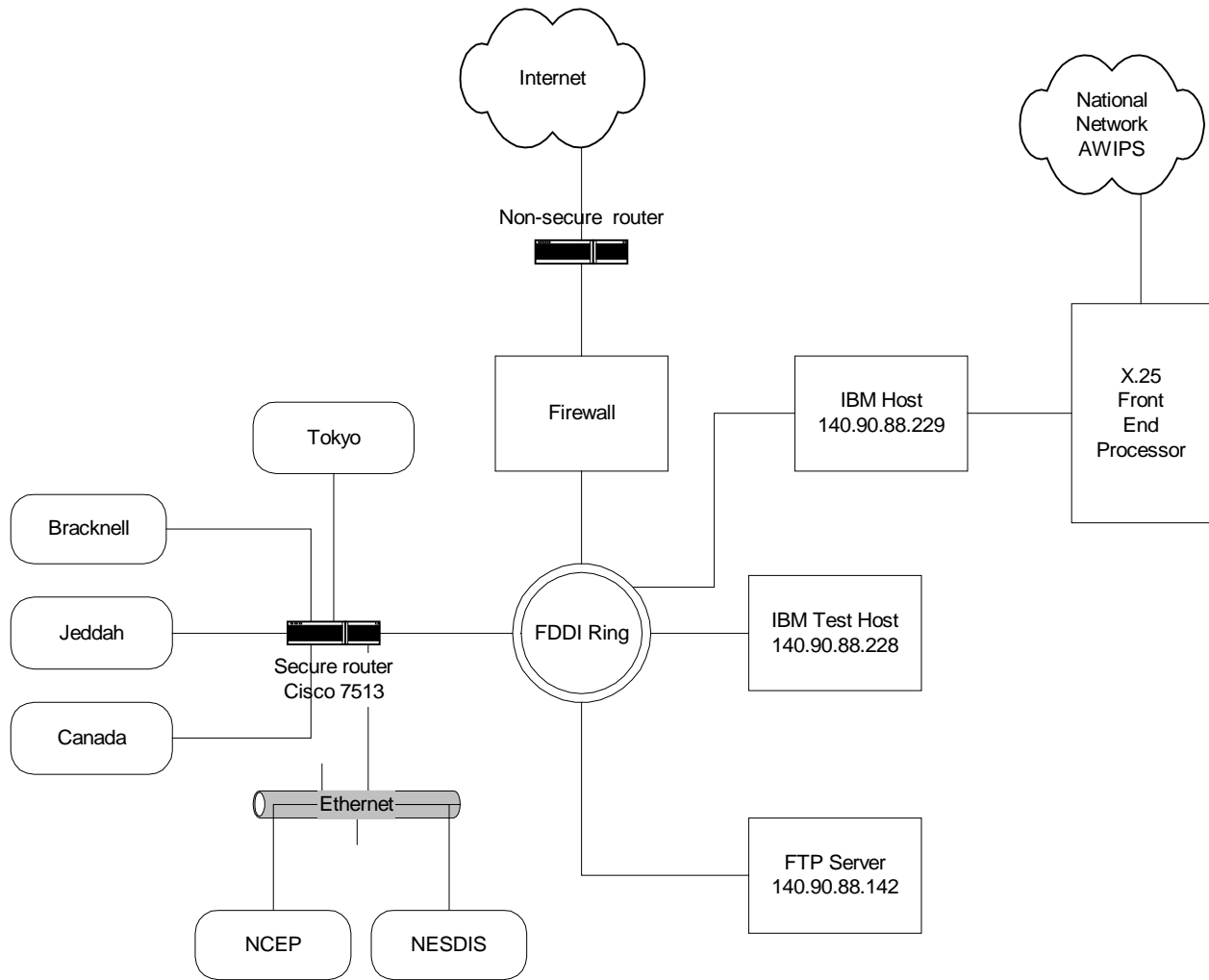


Figure 4 WAFC Washington - Conceptual Communications Configuration for GTS TCP/IP Connections

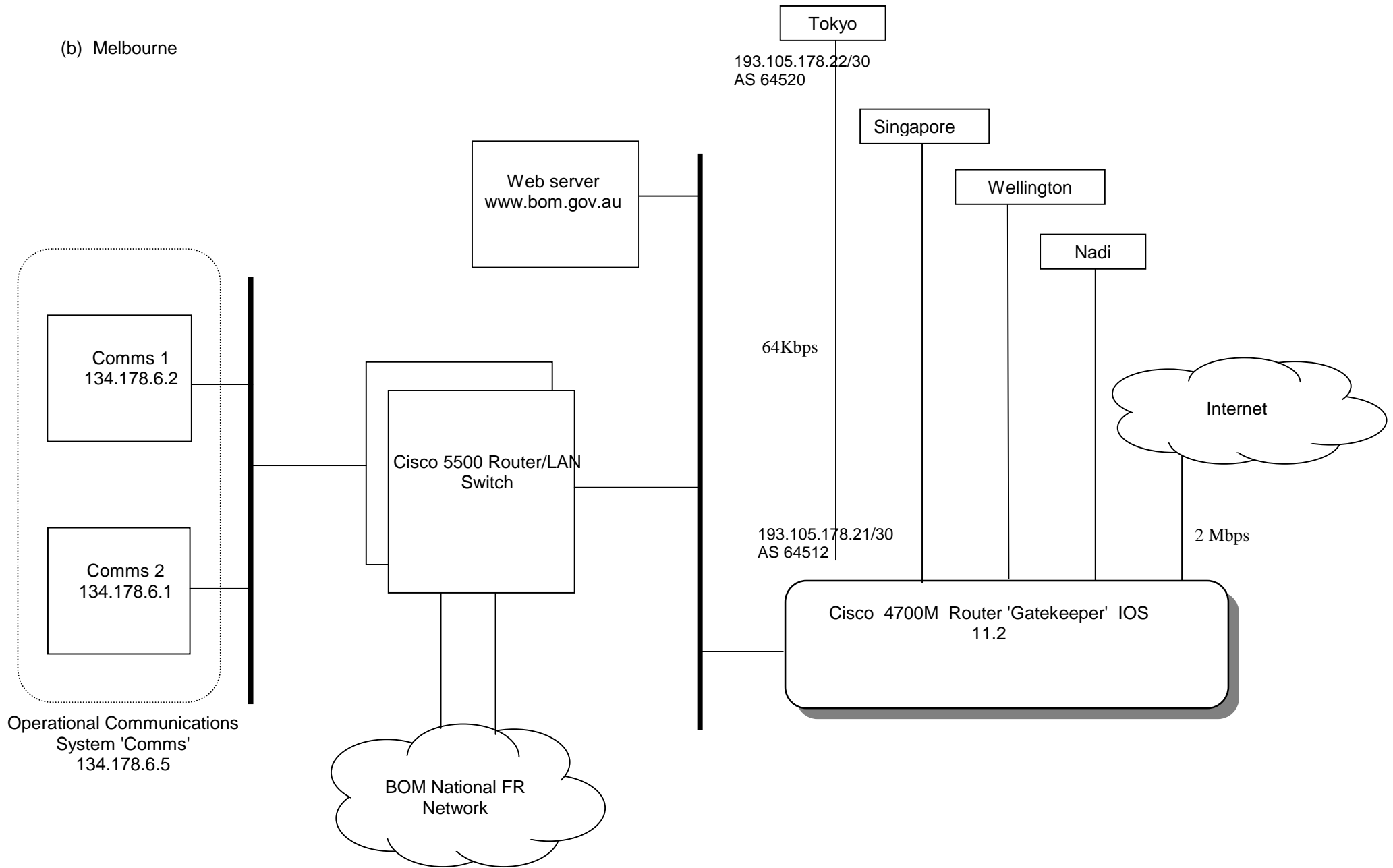


Figure 5 WMC Melbourne - Conceptual Communications Configuration for GTS TCP/IP Connections

(c) Tokyo

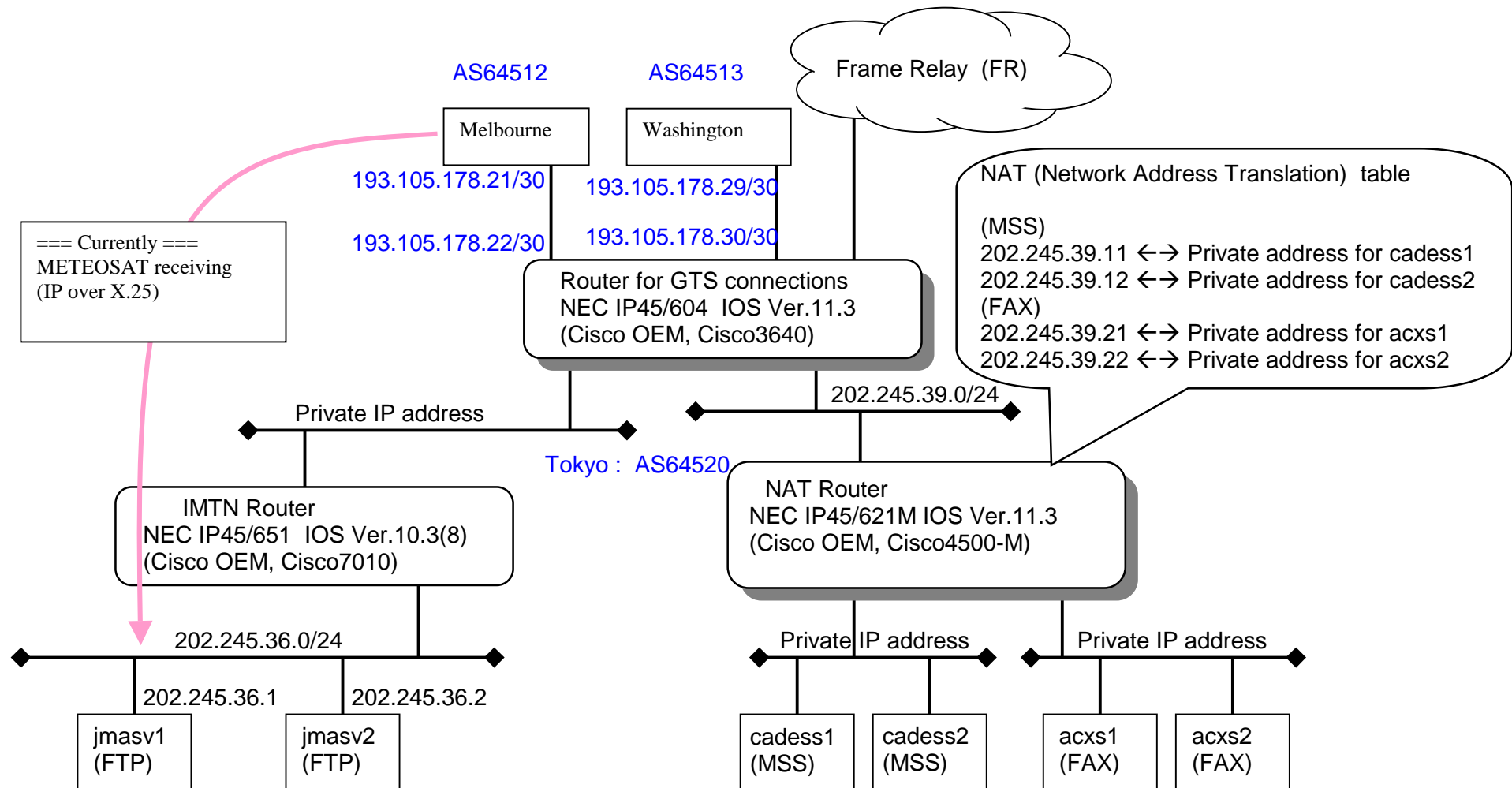


Figure 6 RTH Tokyo - Conceptual Communications Configuration for GTS TCP/IP Connections

(2) Router specification

Each of the three centers uses a Cisco (or Cisco OEM) router for IP links. The model and IOS (Cisco Internetwork Operating System) version of each center are:

(a) Washington

Model : Cisco 7513
IOS version : 11.2

(b) Melbourne

Model : Cisco CS4700-M
IOS version : 11.2

(c) Tokyo

Model : NEC IP45/604 (Cisco OEM, corresponding model Cisco3640)
IOS version : 11.3