# シスコサポートコミュニティ ライブ Expert Webcast

# ルーティングプロトコルのネイバーダウンに関するトラブルシューティング

**東村　誉(Higashimura Takashi)**

**テクニカルサポート部門 カスタマーサポートエンジニア**

**2012年06月19日**

# シスコサポートコミュニティー ライブ Expert Webcast


**東村　誉（ヒガシムラ タカシ）**

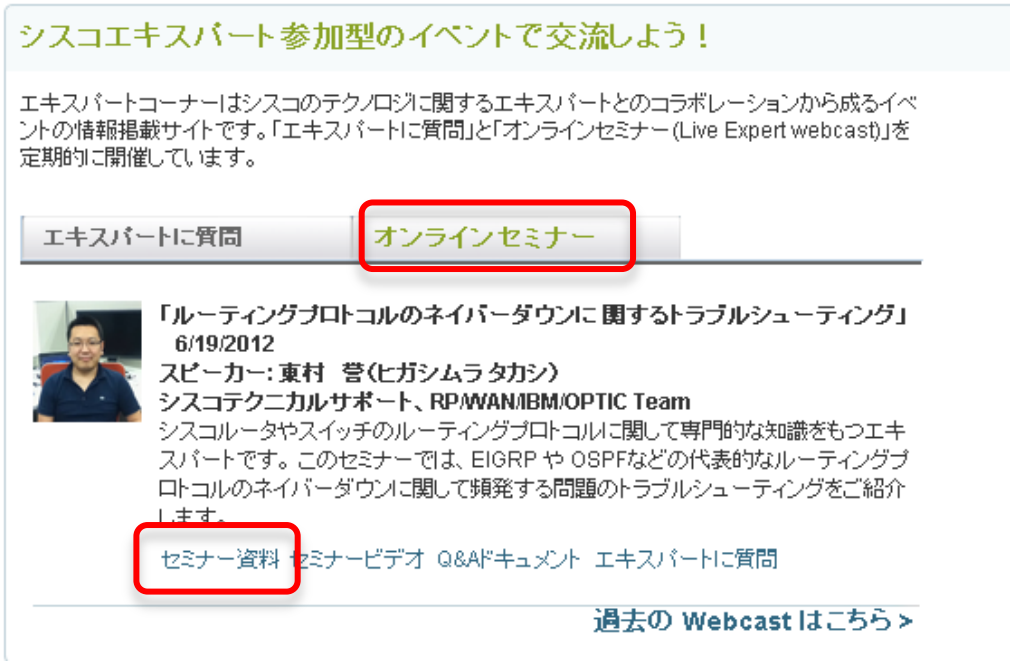
**CCIE 27598 in Routing and Switching**

# ご参加ありがとうございます

**今日のプレゼンテーション資料のコピーはチャットウィンドウ内のリンクからダウンロードいただけます**

https://supportforums.cisco.com/community/csc-japan/ask-the-experts#view=webcasts

Or, https://supportforums.cisco.com/docs/DOC-25173



# 質問の受付を開始します

Q&A パネルから”**ALL PANELIST**” を選択したまま送信してください。

# 投票質問1

## OSPF, EIGRP等の種類を問わずルーティングプロトコルの設定/対応経験は下記のどれになりますでしょうか?

a) まったく経験がなく、知らない。

b) 資格勉強等で知ってはいるが、設定やトラブルシューティングはしたことがない

c) 特定のルーティングプロトコルであれば、設定/障害対応も可能。

d) どんなルーティングプロトコルでも設定/障害対応に自信がある。

# シスコサポートコミュニティ
# ライブ Expert Webcast

# ルーティングプロトコルのネイバーダウンに関するトラブルシューティング

**東村　誉(Higashimura Takashi)**
テクニカルサポート部門 カスタマーサポートエンジニア

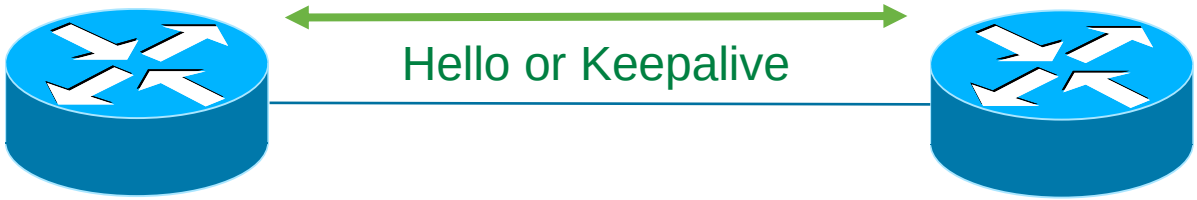
**2012年06月19日**

# アジェンダ

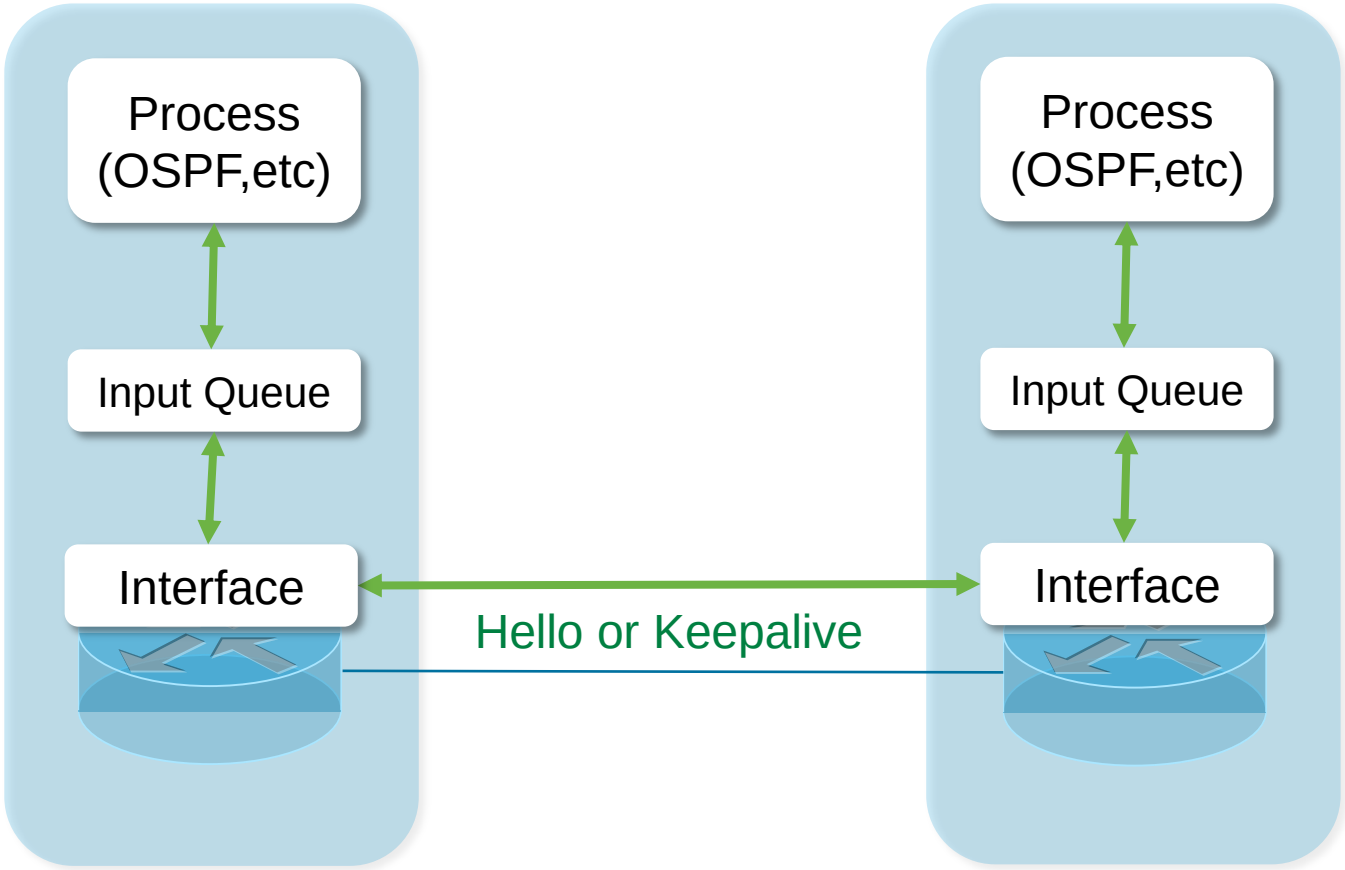
- ルーティングプロトコルのネイバーダウンに関するトラブルシューティング
  - ルーティングパケットの処理
  - EIGRP のネイバーダウン事例と調査方法
  - OSPF のネイバーダウン事例と調査方法
  - BGP のネイバーダウン事例と調査方法
- ネイバーダウン時の取得コマンド一覧
- まとめ

# ルーティングパケットの処理

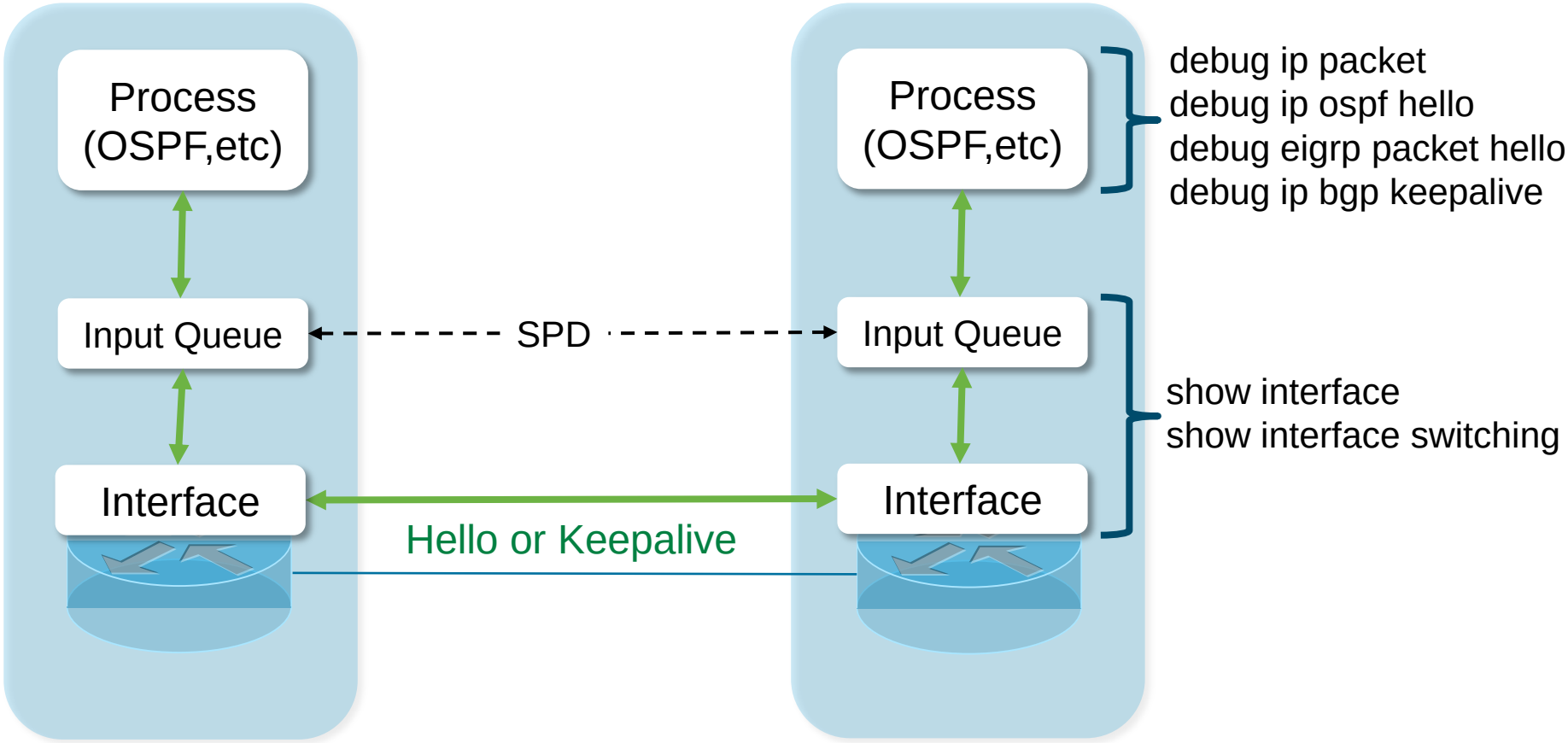
# ルーティングパケットの処理



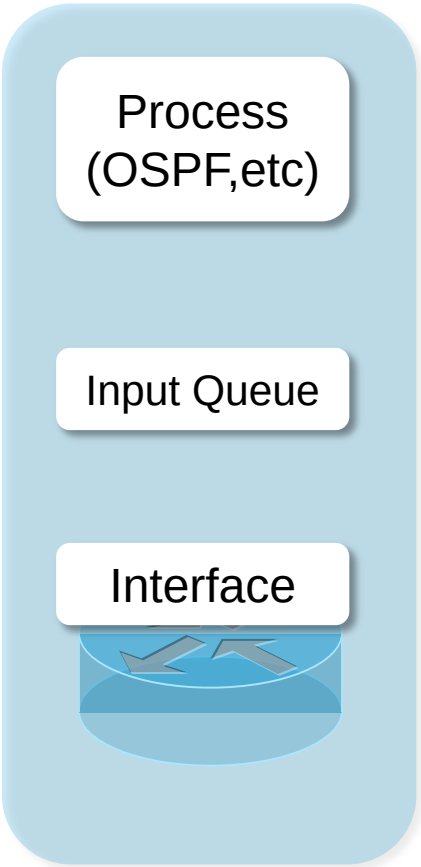
# ルーティングパケットの処理



# ルーティングパケットの処理



# チェックする箇所を理解する




```
C1812J# debug ip ospf hello
OSPF hello debugging is on
Jun 12 14:13:28.418 JST: OSPF-1 HELLO Fa1: Rcv hello from 10.3.3.3
area 0 192.168.2.2
```

```
C1812J# sh int fa0 | i queue
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 332
  Output queue: 0/40 (size/max)
```

```
C1812J# sh int fa0 | i error
     67 input errors, 0 CRC, 67 frame, 0 overrun, 0 ignored
     0 output errors, 0 collisions, 0 interface resets
```

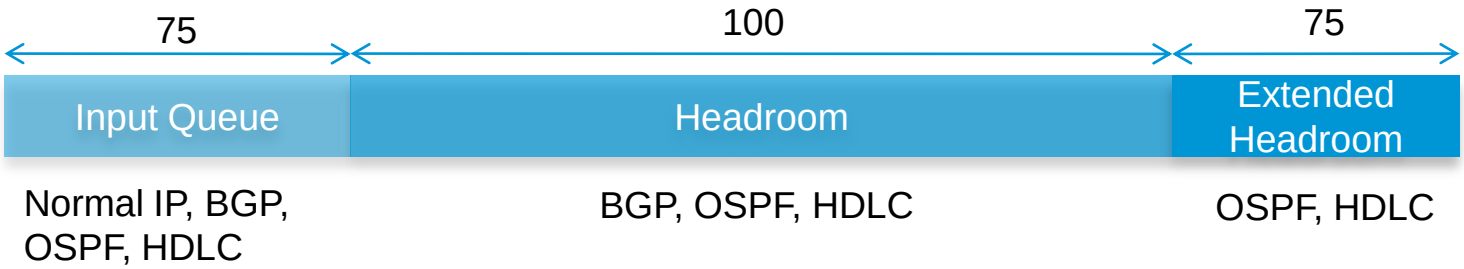
```
C1812J# sh ip int fa0 | i Multicast
  Multicast reserved groups joined: 224.0.0.10 224.0.0.5 224.0.0.6
```

```
C1812J# sh controllers fa0 | i address filter|5e00
 Software MAC address filter(hash:length/addr/mask/hits):
  0x58:  0  0100.5e00.0006  0000.0000.0000        0
  0x5B:  0  0100.5e00.0005  0000.0000.0000    17633
```

# SPD(Selective Packet Discard)

Input Queue 75 (Normal queue) に headroom / extended headroom を追加し、headroom でルーティングプロトコルを保護する機能。

```
C1812J# sh int fa0
FastEthernet0 is up, line protocol is up
(snip)
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
(snip)
```




**BGP/OSPF パケットはNormal IP パケットよりも、深いキューで保護される。**

詳細は下記ページを参照ください。

- 選択的パケット破棄(SPD)の理解と利用
  http://www.cisco.com/web/JP/product/hs/ios/tec/spd.html

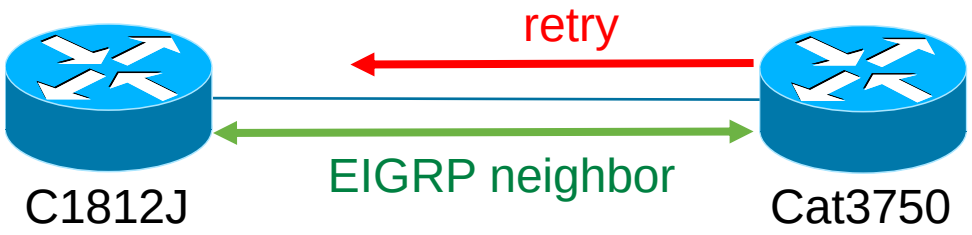
# EIGRPのネイバーダウン事例と調査方法

# EIGRP：ルータ追加後のネイバーダウン

**問題:**
**ネットワークにルータを追加後、下記メッセージが出力され、**
**ネイバーダウンが発生し、ネイバーが確立できなくなった。**

```
Jun 10 10:14:28.315 JST: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.1
(GigabitEthernet1/0/1) is down: retry limit exceeded
Jun 10 10:14:28.894 JST: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.1
(GigabitEthernet1/0/1) is up: new adjacency
%EIGRP: Failed to get client handle from BFD
Jun 10 10:15:23.881 JST: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.1
(GigabitEthernet1/0/1) is down: retry limit exceeded
Jun 10 10:15:24.191 JST: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.1
(GigabitEthernet1/0/1) is up: new adjacency
```

**以前は問題なくネイバーが張れており、問題がなかったのに。。**



# EIGRP : ルータ追加後のネイバーダウン

まずはメッセージを意味を知る。

```
Jun 10 10:14:28.315 JST: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.1.1
(GigabitEthernet1/0/1) is down: retry limit exceeded
```

上記メッセージは EIGRP が 送信パケットに対する ACK を受信できない場合に、再送を繰り返し、16回再送を繰り返し ACK が無ければ “retry limit exeeded” により一旦ネイバーがリセットされたことを示す。

```
Cat3750# show ip eigrp neighbors detail
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.1.1             Gi1/0/1          12 00:00:16 1997  5000  1  98
   Version 6.0/3.0, Retrans: 2, Retries: 2
   Topology-ids from peer - 0
    UPDATE seq 98 ser 1-79 Sent 14470 Sequenced
```

**何故 ACK が返ってこないかを考える**

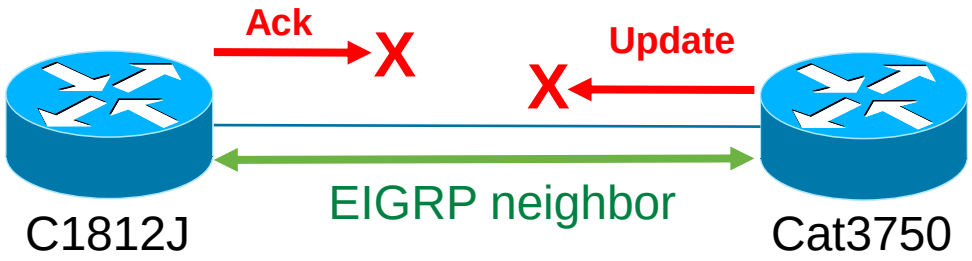
- そもそも Update を送信していない?
- ネイバー間の区間で Update or ACK が drop されている?

# EIGRP：ルータ追加後のネイバーダウン

**何故 ACK が返ってこないかを考える**

**確認1)そもそも Update を送信できていない?**


**確認2)ネイバー間で Update or ACK が drop されている?**



# EIGRP : ルータ追加後のネイバーダウン

**確認1) そもそも Update を送信できていない?**

debug eigrp packets update により Update の送受信を両ルータで確認。

```
Cat3750# debug eigrp packets update
    (UPDATE)
EIGRP Packet debugging is on
.Jun 10 10:58:35.183 JST: EIGRP: Sending UPDATE on GigabitEthernet1/0/1 nbr 192.168.1.1,
retry 1, RTO 300 tid 0
.Jun 10 10:58:35.183 JST:   AS 1, Flags 0x0:(NULL), Seq 112/112 interfaceQ 0/0 iidbQ un/rely
0/0 peerQ un/rely 0/1 serno 1-79
.Jun 10 10:58:35.485 JST: EIGRP: Sending UPDATE on GigabitEthernet1/0/1 nbr 192.168.1.1,
retry 2, RTO 450 tid 0
```

上記 Update 送信側は送信しているが、下記対向ルータでは受信していない。

```
C1812J# debug eigrp packets update
    (UPDATE)
EIGRP Packet debugging is on
C1812J# <<<<< 何も表示されない。Update を受信していない。
```

**Note: ルータ or 回線上 の問題を切り分けるためにパケットキャプチャも有効**

# EIGRP：ルータ追加後のネイバーダウン

**確認1) そもそも Update を送信できていない?（続き）**

EIGRP Update を送信する際に MTU を超過する場合には、フラグメントを行い送信する。送信パケットサイズを確認するため debug ip packet を使う。

```
access-list 110 permit eigrp any host 192.168.1.1

Cat3750# debug ip packet 110
Jun 10 11:11:28.925 JST: IP: s=192.168.1.2 (local), d=192.168.1.1 (GigabitEthernet1/0/1), len 1528, sending
```

上記から、len 1528 (bytes) となっており、送信パケットサイズがEthernet で一般的な **MTU 1500byte 以上となっている**ことが確認できる。

**Note:**
debug ip packet では大量の出力があるため、上記のように ACL を作成しておき、必要最小限の debug のみを確認するようにする。

# EIGRP：ルータ追加後のネイバーダウン

**確認2) ネイバー間で Update or ACK が drop されている?**

```
Cat3750# sh int gi1/0/1 | i MTU|Last|queue|error
  MTU 1600 bytes, BW 100000 Kbit, DLY 100 usec,
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Output queue: 0/40 (size/max)
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 output errors, 0 collisions, 0 interface resets
```

上記ログの下記に着目する。

1. MTU 値
2. Last input/output がリセットされているか。
3. Input/output queue で drops/flushes が増加していないか。
4. input/output で errors が増加していないか。

Update 送信側では特に問題がない。

# EIGRP：ルータ追加後のネイバーダウン

**確認) ネイバー間で Update or ACK が drop されている?**

```
C1812J# sh int fa0 | i MTU|Last|queue|giant|error
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 02:09:34
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Output queue: 0/40 (size/max)
     0 runts, 1083 giants, 0 throttles
     1083 input errors, 0 CRC, 1083 frame, 0 overrun, 0 ignored
     0 output errors, 0 collisions, 0 interface resets
```

送信側と比較し、MTU値が異なるため対向からの 1528bytes のパケットが MTU 1500byte より大きいため giants として破棄していると判断できる。

**対策:**

MTU の不一致を解消する。Catalyst3750 ではインタフェース毎には MTU を変更できず、下記 system mtu routing コマンドで変更する。

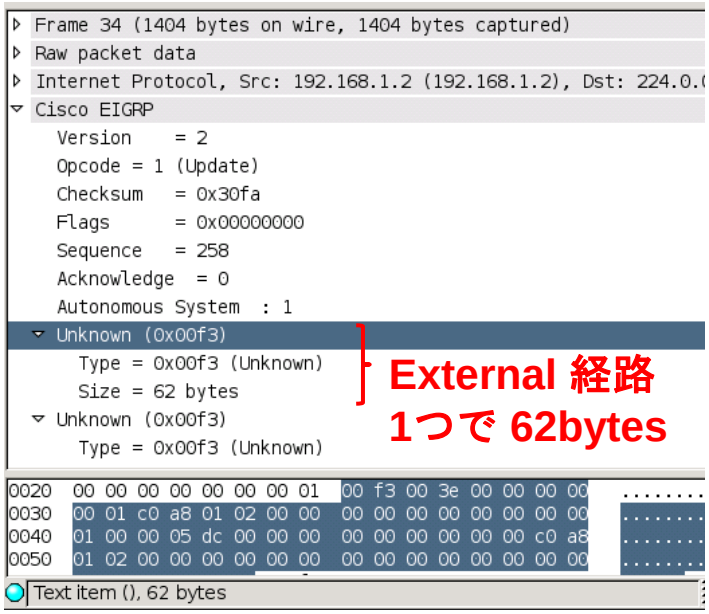
```
Cat3750(config)# system mtu routing 1500
```

# EIGRP : ルータ追加後のネイバーダウン

**補足:**

原因は MTU の不一致と特定できたが、以前は問題なかった点を考える。

Cat3750# **debug ip packet 110**
Jun 10 11:11:28.925 JST: IP: s=192.168.1.2 (local), d=192.168.1.1 (GigabitEthernet1/0/1), **len 1528**, sending




**パケットキャプチャからExternal経路が62byte必要だと分かる。**

1528 = IP Header 20 + EIGRP Header 20
+ EIGRP External 62 * 24 routes

**要因:**
ルータの追加により **24経路 以上**の Update が発生したため。

以前は 1500byte を超える Update を送信することが無かったため問題なかった。

# 投票質問2

**RFCをどのように活用しているか教えてください。**

**※ RFC (Request for Comments)**

a) RFC を知らない。

b) 聞いたことはあるが、読んだことはない。

c) ルーティングプロトコルを知るため、RFCを見たことがある。

d) トラブルシューティングにおいて、RFCを合わせて確認しRFCに違反した動作がないか確認をしたことがある。

# OSPFのネイバーダウン事例と調査方法

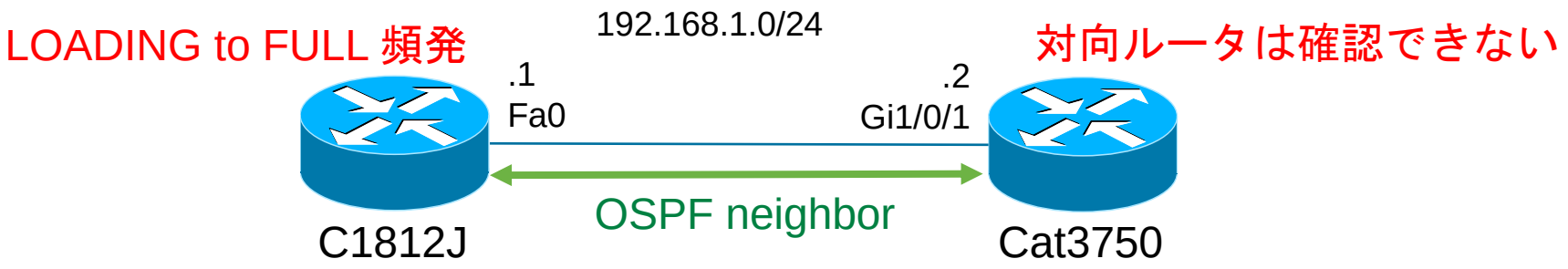
# OSPF : LOADING to FULL メッセージ

**問題:**

**不定期に下記メッセージが出力され、OSPF ネイバーが不安定に見える。**

```
Jun 10 13:33:40.813 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from LOADING to FULL, Loading Done
Jun 10 13:34:27.990 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from LOADING to FULL, Loading Done
Jun 10 13:35:25.708 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from LOADING to FULL, Loading Done
Jun 10 13:36:13.554 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from LOADING to FULL, Loading Done
```

**何故 DOWN のメッセージが出ないんだろう。。。**



# OSPF : LOADING to FULL メッセージ

まずは DOWN のメッセージが出ていない事を考える。

```
Jun 10 13:33:40.813 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from LOADING to FULL, Loading Done
```

このメッセージは下記 default 設定によって出力されている。

```
C1812J(config)# router ospf 1
C1812J(config-router)# log-adjacency-changes ※ default 設定
```

Cisco.com 上のコマンドリファレンスを確認する。

**log-adjacency-changes**

The **log-adjacency-changes** command is on by default but **only up/down (full/down) events** are reported, unless the **detail** keyword is also used.

default では up/down (full/down) しか表示されず、detail オプションがあると分かる。

# OSPF : LOADING to FULL メッセージ

log-adjcancy-changes detail を設定すると、FULL or DOWN 以外の状態遷移も確認ができる。

```
Jun 10 13:53:09.243 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from FULL to INIT, 1-Way
Jun 10 13:53:09.247 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from INIT to 2WAY, 2-Way Received
Jun 10 13:53:09.247 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from 2WAY to EXSTART, AdjOK?
Jun 10 13:53:09.247 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from EXSTART to EXCHANGE, Negotiation Done
Jun 10 13:53:09.259 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from EXCHANGE to LOADING, Exchange Done
Jun 10 13:53:09.263 JST: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0
from LOADING to FULL, Loading Done
```

上記を見ると、FULL から INIT になっていることが分かり、DOWN にはなっていないため、default の設定では表示されなかったことが分かる。

# OSPF : LOADING to FULL メッセージ

OSPF neighbor がどのような状況で Init になるかを RFC で確認する。

**RFC2328**
OSPF Version 2

10.1. Neighbor states

Init

In this state, an Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet). All neighbors in this state (or higher) are listed in the Hello packets sent from the associated interface.

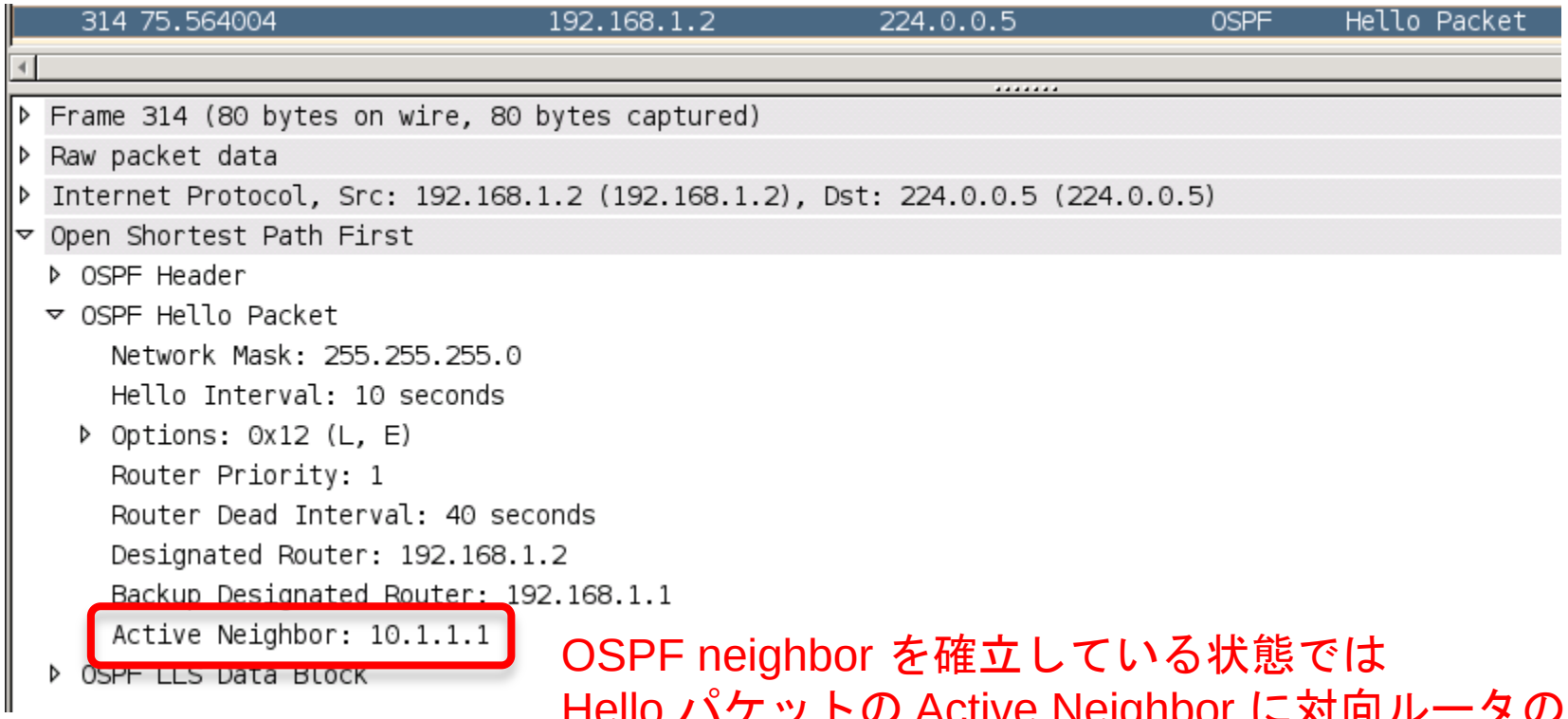
上記によると、対向ルータからの Hello パケットにはネイバーを確立しているネイバーのリストを入れて送信される。

**すなわち、今回の場合は対向ルータ側で DOWN し、Hello パケットのネイバーリストが削除された Hello を送信したため、DOWN ではなく Init に遷移し、そこから再度 FULL になったと想定できる。**

※RFCはインターネット上で公開されています。

# OSPF : LOADING to FULL メッセージ

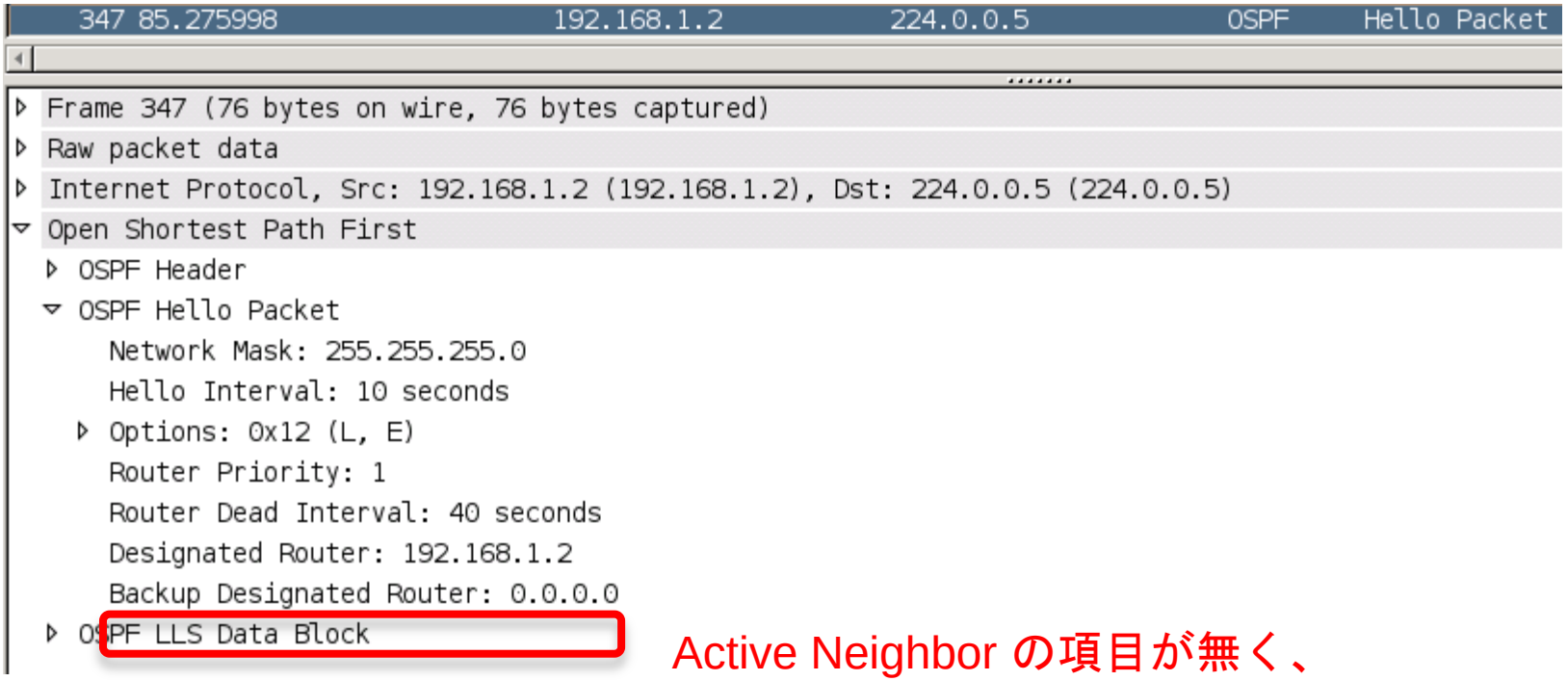
OSPF Hello のネイバーリストについてキャプチャから見てみる。
下記は OSPF neighbor を確立している状態の Hello パケット。




OSPF neighbor を確立している状態では
Hello パケットの Active Neighbor に対向ルータの
Router-ID を入れて送信。

# OSPF : LOADING to FULL メッセージ

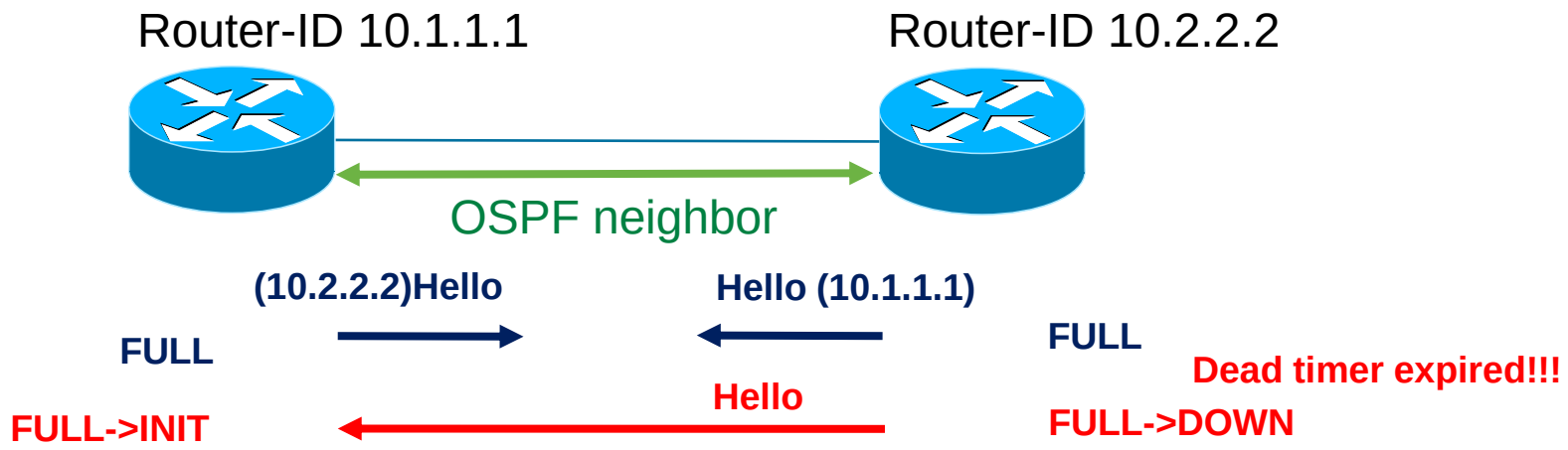
FULL to Init になる要因となった OSPF Hello パケット。




Active Neighbor の項目が無く、
確立している neighbor がいないことを
示している。

# OSPF : LOADING to FULL メッセージ

OSPF Hello パケットの Active Neighbor から Router-ID が消えたということは、
対向側では OSPF neighbor が DOWN したということ。




これより、本ルータ(左側)には被疑が無く、対向ルータ側で OSPF Down が
発生した要因を調べる必要がある。下記は考えられる要因。

- 対向ルータが OSPF Hello を drop した(トラフィック過多)
- ルータ間の L2 区間で OSPF Hello が drop された(トラフィック過多)
- 対向ルータ側のインタフェースが down/up した (直結でない場合)

# 投票質問3

## 弊社のバグ検索ツール (Bug Toolkit) について あなたの経験を教えてください。

a) そんなツール知らない。

b) 知っているが、あまり使わない。

c) トラブルシューティングでは既知不具合の検索で よく使うが、うまく該当のものを見つけられない。

d) Bug Toolkit の使い方をマスターし、既知不具合が あれば大体見つけることができる

**参考:**

Bug Toolkit は Bug Search Tool という新しいツールに移行される予定です。

※ご契約内容により本ツールが使えない場合もございます。

# BGPのネイバーダウン事例と調査方法

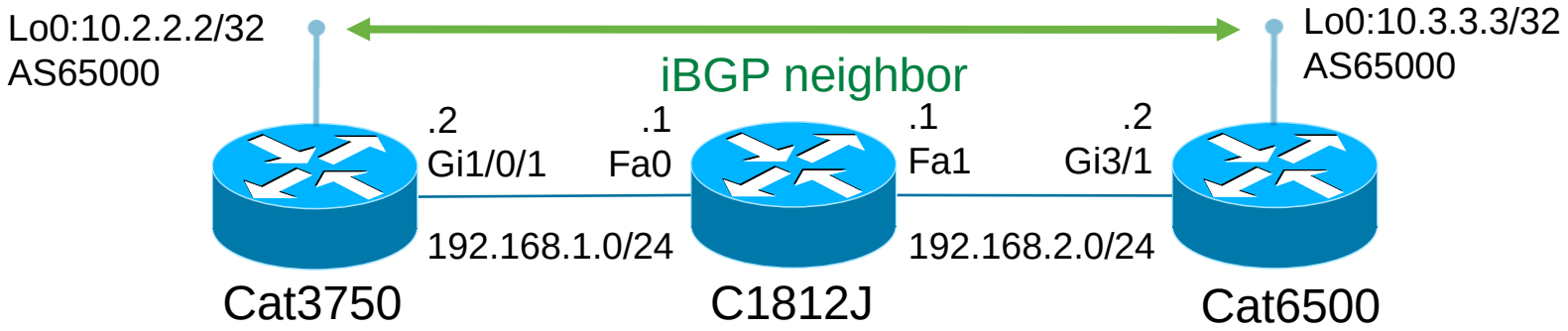
# BGP : hold time expired でのダウン

**問題:**

**一旦ピアはアップするが、hold time expired で down/up を繰り返す。**

```
Jun 10 18:30:10.679 JST: %BGP-5-ADJCHANGE: neighbor 10.3.3.3 Up
Jun 10 18:33:11.286 JST: %BGP-5-ADJCHANGE: neighbor 10.3.3.3 Down BGP Notification
sent
Jun 10 18:33:11.286 JST: %BGP-3-NOTIFICATION: sent to neighbor 10.3.3.3 4/0 (hold time
expired) 0 bytes
Jun 10 18:33:11.294 JST: %BGP_SESSION-5-ADJCHANGE: neighbor 10.3.3.3 IPv4 Unicast
topology base removed from session  BGP Notification sent
```

**一旦アップするということは、到達性はあるということなのに。。。**



# BGP : hold time expired でのダウン

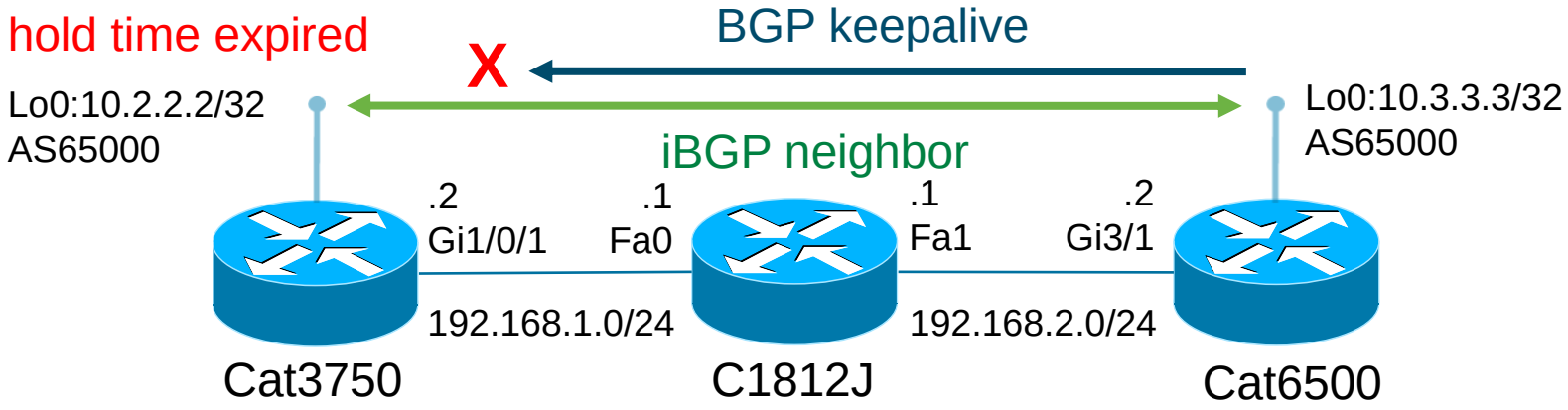
まずはメッセージの意味を理解する。

```
Jun 10 18:33:11.286 JST: %BGP-3-NOTIFICATION: sent to neighbor 10.3.3.3 4/0 (hold time expired) 0 bytes
```

Cat3750 で BGP keepalive が hold time の間、受信できなかったためネイバーをダウンさせ、NOTIFICATION メッセージを送信している。

```
Cat3750# sh ip bgp nei 10.3.3.3 | i hold time
  Last read 00:01:39, last write 00:00:47, hold time is 180, keepalive interval is 60 seconds
```

上記から hold time は 180秒、keepalive は 60秒だと分かる。(default)



# BGP : hold time expired でのダウン

Cisco のBGP実装では、BGP Update の受信でも hold time をリセットする。

```
Cat3750# sh ip bgp nei 10.3.3.3 | i hold time
  Last read 00:01:39, last write 00:00:47, hold time is 180, keepalive interval is 60 seconds
```

**Last read** : BGP Update or Keepalive の受信でリセットされる

Keepalive の interval 以上になっていることから、リセットされていないことが分かる。

```
Cat6500# sh ip bgp nei 10.2.2.2 | i hold time is
  Last read 00:00:04, last write 00:01:45, hold time is 180, keepalive interval is 60 seconds
```

**Last write** : BGP Update or Keepalive を送信後、Ack を受信したらリセットされる

対向側では、last write がリセットされないことが見える。
そのため、原因としては下記が想定できる。

- 確認1)BGP Update が何らかの理由で対向に届いていない?
- 確認2)BGP Update / Keepalive の Ack が受信できていない?

# BGP : hold time expired でのダウン

**確認1) BGP Update が何らかの理由で対向に届いていない?**

```
Cat6500# sh ip bgp sum | b Neighbor
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.2.2.2        4 65000      68       20      511    0    1 00:00:22        0
```

上記から OutQ が 0 でないため、何らかのパケットの送信が完了しない状態であることが分かる。送信が完了していないとは、BGP Update を送信し Ack が受信できていない状況を言う。

```
access-list 180 permit tcp any any eq bgp
access-list 180 permit tcp any eq bgp any

Cat6500# debug ip bgp update
Cat6500# debug ip tcp transaction
Cat6500# debug ip packet 180
```

上記 debug から BGP update の送信状況を確認する。出力は次ページ。

# BGP : hold time expired でのダウン

```
Jun 10 19:09:05.503 JST: BGP(0): 10.2.2.2 send UPDATE (prepend, chgflags: 0x0)
10.3.251.0/24, next 10.3.3.3, metric 0, path Local
(snip)
Jun 10 19:09:05.551 JST: IP: s=10.3.3.3 (local), d=10.2.2.2 (Vlan100), len 1520,
 post-encap feature, MTU Processing(4), rtype 1, forus FALSE, sendself FALSE, mt
u 0
Jun 10 19:09:15.583 JST: IP: s=10.3.3.3 (local), d=10.2.2.2 (Vlan100), len 1520,
 post-encap feature, MTU Processing(4), rtype 1, forus FALSE, sendself FALSE, mt
u 0
Jun 10 19:09:15.583 JST: TCP0: timeout #1 - timeout is 10754 ms, seq 4242800389
Jun 10 19:09:15.583 JST: TCP: (35287) -> 10.2.2.2(179)
```

BGP Update

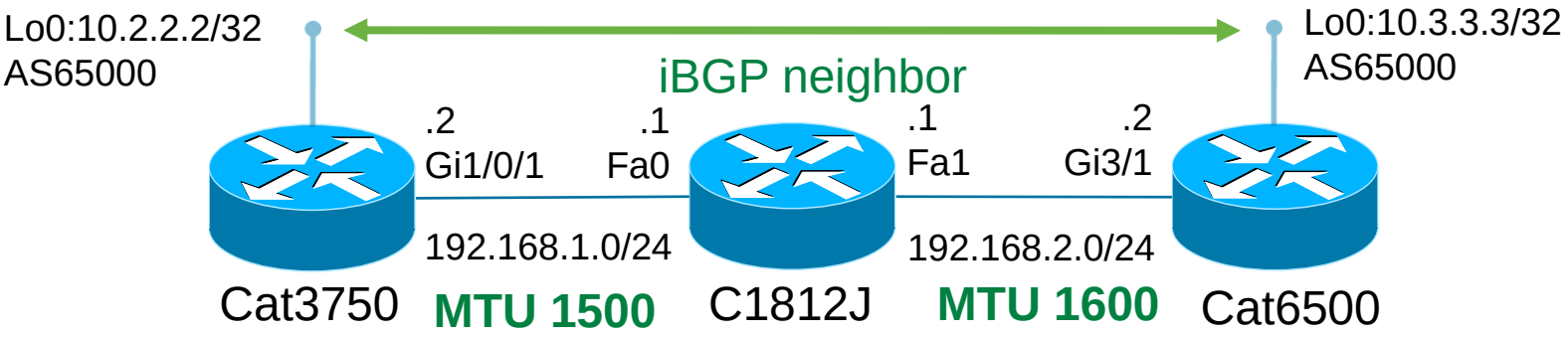
再送1回目

上記 debug ip bgp update 及び debug ip packet のタイムスタンプが同じことから、
BGP Update のサイズが 1520byte になっていることが分かる。
また、同1520byteのパケットが再送されているのも分かる。

**※ 再送は TCP レベルで行われるため、debug ip bgp update では最初しか表示されないことに注意。**

# BGP : hold time expired でのダウン

BGP Update のサイズが問題となり、再送を繰り返している状況のため、
MTUの問題が考えられる。




MTU値 が C1812J を境に MTU 1500 <-> MTU 1600 で異なることが分かる。
Cat6500 から 1520byte で送信すれば、Cat3750 へ届かないことが分かる。

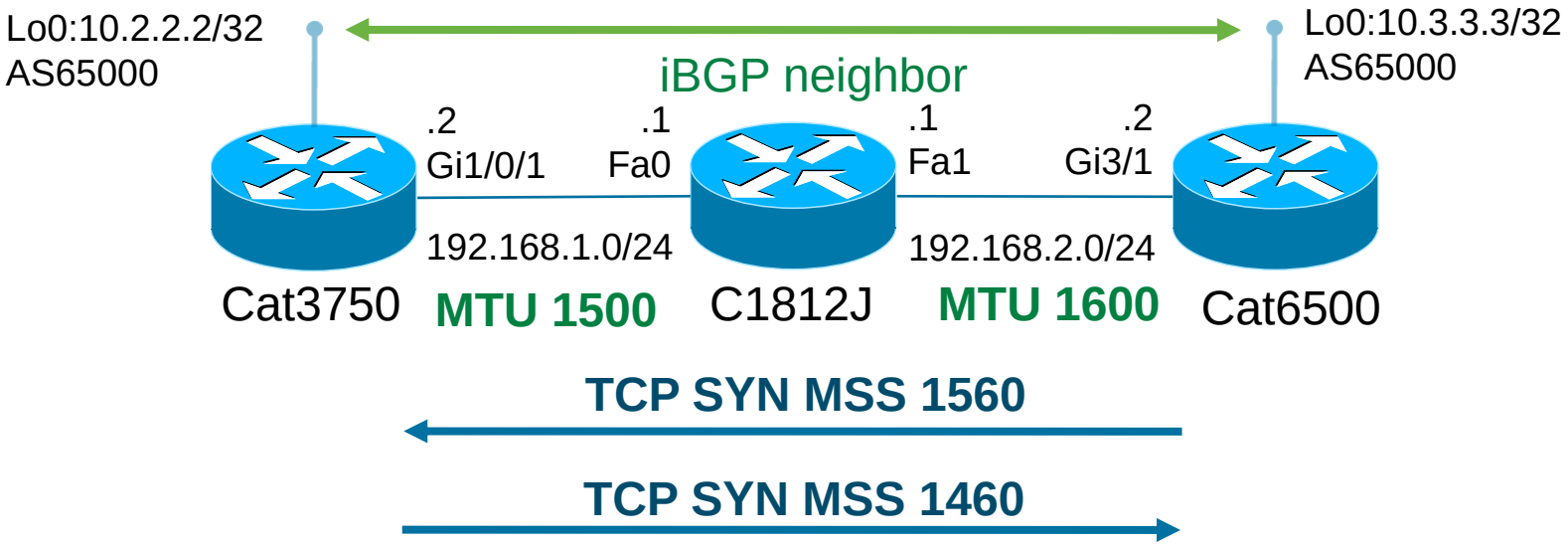
iBGPネイバーの場合には、**Path MTU Discovery** という機能により、
ネイバー区間の最低MSS値を検出する機能がある。

**MSS = MTU – (IP Header 20byte + TCP Header 20byte)**

上記計算式から、Cat3750 では MSS 1460、Cat6500 では MSS 1560 となる。
この MSS 値は **TCP 3-way handshake によって低い方が使われる**。

# BGP : hold time expired でのダウン

**PMTUD(Path MTU Discovery) の動作を理解する**




MSS は低い値が使われる。下記は Cat6500 での debug ip tcp transaction での動き。

Jun 10 19:32:50.682 JST: TCP: sending SYN, seq 3067784728, ack 0
Jun 10 19:32:50.682 JST: TCP0: Connection to 10.2.2.2:179, advertising **MSS 1540**
Jun 10 19:32:50.686 JST: TCP0: tcb 51B5EF38 connection to 10.2.2.2:179, received **MSS 1460**,
**MSS is 1460** ⟵ **MSS 1460 を選択**

# BGP : hold time expired でのダウン

MSS = MTU – (IP Header 20byte + TCP Header 20byte)

となるため、今回は MSS = 1500-(20+20) = 1460 で問題ない。
念の為、両ルータでの MSS 値を show コマンドから確認しておく。

```
Cat3750# sh ip bgp nei 10.3.3.3 | i seg
Datagrams (max data segment is 1460 bytes):
```

```
Cat6500# sh ip bgp nei 10.2.2.2 | i seg
Datagrams (max data segment is 1460 bytes):
```

両ルータとも 1460 bytes になっており、特に問題ないことが分かる。

1520byte の BGP Update を投げていることから、余分な 20bytes について考えてみる。BGP設定を確認する。

```
Cat6500# sh run | b router bgp
router bgp 65000
(snip)
 neighbor 10.2.2.2 remote-as 65000
 neighbor 10.2.2.2 password cisco
 neighbor 10.2.2.2 update-source Loopback0
(snip)
```

TCPオプションヘッダ(20bytes)を使う

# BGP : hold time expired でのダウン

1520bytes = MSS 1460 + IP Header 20 + TCP Header 20 **+ TCP Option 20**

となっている可能性があるため、password 設定を外して切り分けを行う。
両ルータで password 設定を外して Cat6500 からの Update を確認。

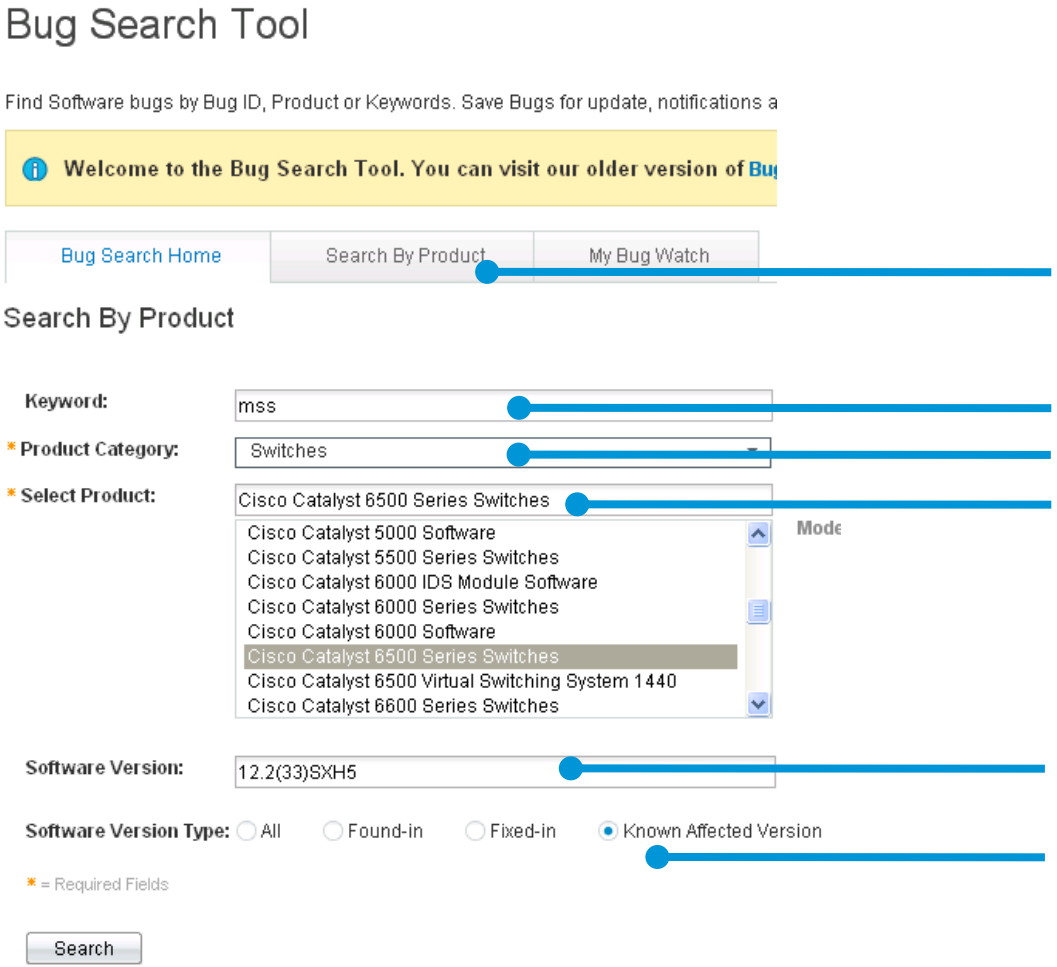
```
Jun 10 20:04:13.933 JST: BGP(0): 10.2.2.2 send UPDATE (prepend, chgflags: 0x0) 1
0.2.1.0/24, next 10.3.3.3, metric 0, path Local
(snip)
Jun 10 20:04:13.933 JST: IP: s=10.3.3.3 (local), d=10.2.2.2 (Vlan100), len 1500, post-encap
feature, MTU Processing(4), rtype 1, forus FALSE, sendself FALSE, mtu 0
<<<< TCP の再送無
```

上記から、password 設定をした場合に MTU1500を超過したパケットを生成する
**問題(不具合)**があると判断ができる。

Cat6500 は 12.2(33)SXH5 で動作しているため、既知不具合を調査してみる。

# BGP : hold time expired でのダウン

Bug Search Tool へアクセスする。




Search By Product をクリック

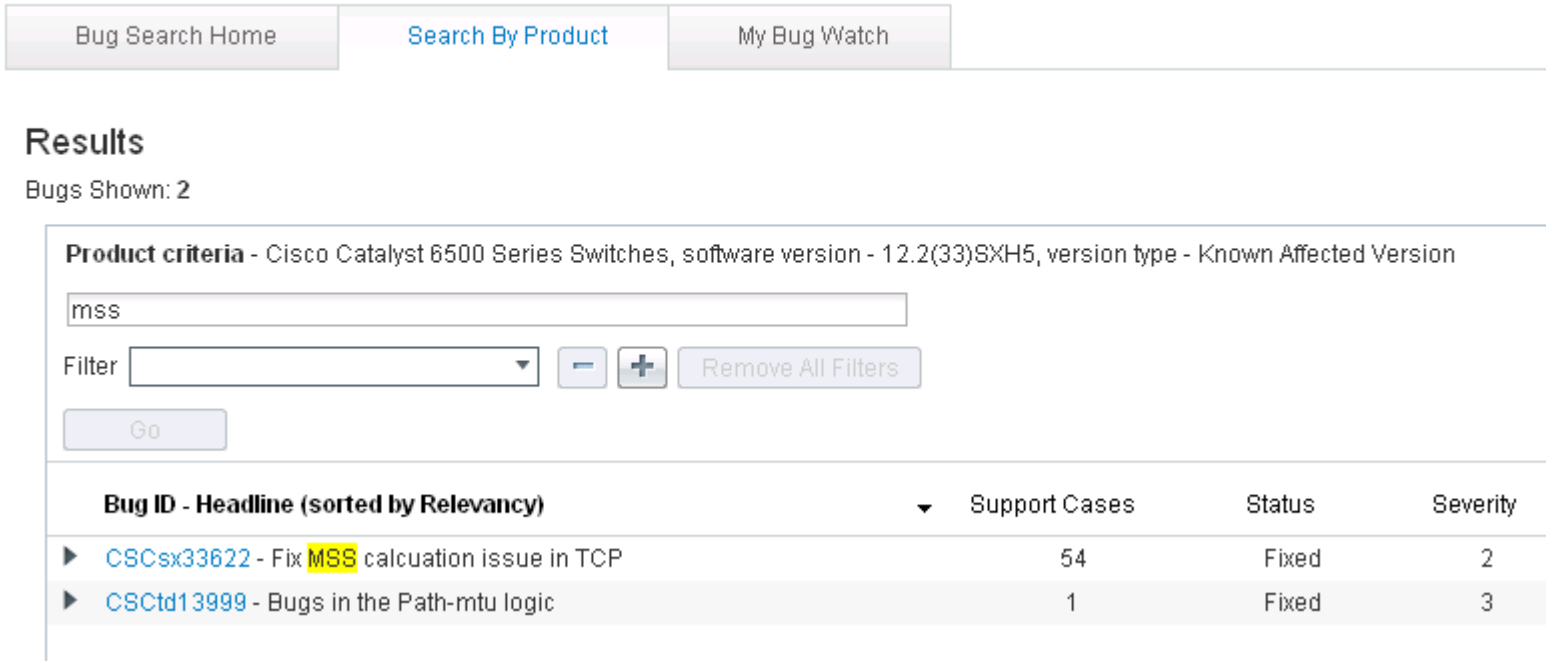
キーワードに “mss”
Product Category を “Switches”
Product に Catalyst6500

バージョン “12.2(33)SXH5”

12.2(33)SXH5 が該当する不具合

# BGP : hold time expired でのダウン

## Bug Search Tool




上記 **CSCsx33622** が本事象に関連した不具合に該当している可能性が高いことが不具合のタイトルからも判断できる。

# BGP : hold time expired でのダウン

**CSCsx33622 - Fix MSS calcuation issue in TCP**

Save To My Bug Watch

## Description

**Symptom:**

Flapping BGP sessions occur in the network when a Cisco IOS application sends full-length with TCP options.

**Conditions:**

This issue is seen when a Cisco IOS device that is configured to send TCP options sends its Maximum Segment Size (MSS) during the three-way handshake. In this case, the router incor accounts for 20 bytes of TCP options when it sends this initial MSS.

This issue occurs when a "fixed" IOS communicates with a "non-fixed" IOS.

Note: The "non-fixed" behavior is to subtract the 20 TCP option bytes when MSS values are in exchanged. The "fixed" behavior is to not subtract the 20 TCP option bytes when MSS values exchanged.

**Workaround:**

Set the MSS value on the "non-fixed" router to be the MSS received from the "fixed" router minu options (20 bytes). Use the global command ip tcp mss to adjust the MSS value that the route

**Fixed in: (56)**

15.1(1.5.1)PIA13,15.1(1)XB,15.1(1)SG5.1,15.0(1)M
12.4(25b)M,12.4(25a)M0,12.4(24.6.5)PIL12
12.4(24.6)T5,12.4(24.6)PI11g,12.4(24)YG,12.4(24)YE
12.4(24)T1,12.4(24)MDA1,12.4(24)MD,12.4(24)GC2
12.4(24)GC1,12.4(23c)M,12.4(22)YE2,12.4(22)XR
12.4(22)T2,12.4(22)MDA1,12.4(20)T3,12.4(15)T12
12.2(53.6)SIN3,12.2(50)SY,12.2(33.5.30)SRB
12.2(33.5.18)SXH,12.2(33.4.9)SRC
12.2(33.2.13)SB11,12.2(33.1.7)MCP5
12.2(33.1.10)SRD,12.2(33.0.9)XND,12.2(33)ZI
12.2(33)XND,12.2(33)XNC1,12.2(33)SXI2
12.2(33)SXH6,12.2(33)SRD2,12.2(33)SRC5
12.2(33)SRB6,12.2(33)SCD1,12.2(33)SCC4
12.2(32.8.12)REC186,12.2(32.8.11)YST273.3.1
12.2(32.8.11)XJC273.1,12.2(32.8.11)XJC246.24
12.2(32.8.11)SX256,12.2(32.8.1)YCA273.3
12.2(32.8)SCE,12.2(18.16.16)SXF,12.2(18)ZYA3c
12.2(18)ZYA3,12.2(18)SXF17

**12.2(33)SXH6 で修正されている**

12.2(33)SXH6 へのバージョンアップや release-note の回避策で
事象が解消することを確認し、該当可否を最終判断。

# デモ

# ネイバーダウン時の取得コマンド一覧

# ネイバーダウン時の取得コマンド一覧

## EIGRP:

**show command:**
show ip protocols
*show ip route summary
*show ip traffic
*show ip eigrp traffic
*show ip eigrp neighbor
*show ip eigrp neighbor detail
*show ip eigrp interface
* show ip eigrp interface detail
show ip eigrp event
*show interface
*show interface switching
show tech
show logging

*は複数回取得

**debug command:**
debug ip eigrp
debug ip eigrp neighbor
debug eigrp packet
debug eigrp fsm
debug eigrp neighbor
debug eigrp transmit
debug ip packet <ACL>

# ネイバーダウン時の取得コマンド一覧

## OSPF:

**show command:**
show ip protocols
*show ip traffic
*show ip route summary
show ip ospf
*show ip ospf traffic
*show ip ospf interface brief
*show ip ospf interface
*show ip ospf neighbor
*show ip ospf neighbor detail
show ip ospf event
*show interface
*show interface switching
show tech
show tech ospf detail
show logging

*は複数回取得

**debug command:**
debug ip ospf hello
debug ip ospf adj

# ネイバーダウン時の取得コマンド一覧

## BGP:

**show command:**
show ip protocols
*show ip traffic
*show ip route summary
*show ip bgp summary
*show ip bgp neighbor
show ip bgp
*show interface
*show interface switching
show tech
show logging

*は複数回取得

**debug command:**
debug ip bgp
debug ip bgp keepalive
debug ip bgp update
debug ip tcp transaction

# ログ取得時の推奨設定

show / debug ログの取得にあたっては、下記2点を実施の上、コマンド投入の
タイムスタンプが確認できるよう、また debug ログは console ではなく
サイズを大きく調整した buffer にすることを推奨いたします。

1) timestamp に msec を指定及びコマンド入力時にtimestampを記録してください
   また、時刻が同期されていない場合は時刻を合わせてください。
   (config)# service timestamps debug datetime localtime msec
   (config)# service timestamps log datetime localtime msec
   (config)# line con 0 (または line vty 0 4)
   (config-line)# exec prompt timestamp
2) 2) buffer size を大きくし、debugメッセージをログに記録する
   (config)# logging console informational
   (config)# logging buffered <size> debugging

※各機器の時刻は NTP 等で合わせるようにお願いします。

# まとめ

- チェックする箇所の理解
- interface, input/output queue, プロセスの動作
- show コマンドで調べられる限界を理解する
- プロトコルの動作は debug から把握
- RFC を参照し、期待する動作をチェック
- 怪しい動作の場合は既知不具合をチェック
- いざという際の取得コマンドを知っておく

# 質問を受付中です

Q&A パネルから”**ALL PANELIST**” を選択したまま送信してください。

# References参考資料（日本語）

- 選択的 パケット 廃棄（SPD）の理解と利用
  http://www.cisco.com/web/JP/product/hs/ios/tec/spd.html
- EIGRP ネイバーが Down する場合のトラブルシューティング
  http://www.cisco.com/cisco/web/support/JP/100/1006/1006272_eigrp_neighbor_down.html
- OSPF ネイバールータの問題について
  http://www.cisco.com/cisco/web/support/JP/100/1007/1007790_29-j.html
- OSPF 近隣ルータの状態
  http://www.cisco.com/cisco/web/support/JP/102/1021/1021744_13-j.html

# References参考資料（日本語）

- show ip ospf neighbor コマンドで Init 状態にあるネイバーが表示される理由
  http://www.cisco.com/cisco/web/support/JP/107/1075/1075674_7-j.html
- BGP ネイバーが Down する場合のトラブルシューティング
  http://www.cisco.com/cisco/web/support/JP/100/1006/1006273_bgp_neighbor_down.html
- BGP 近隣ルータがアイドル、接続、アクティブ状態間を切り替わる理由
  http://www.cisco.com/cisco/web/support/JP/100/1008/1008067_24-j.html

# 質問を受付中です

Q&A パネルから”**ALL PANELIST**” を選択したまま送信してください。

# Q & A

# みなさまのご意見をお寄せください

**本日の Webcast 評価アンケートを提出いただいた方の中から3名様へ Amazon ギフト券をプレゼントいたします！**

**アンケートはブラウザを閉じると自動的に表示されます**

# Ask The Expert (with Takashi Higashimura)

今日聞けなかった質問は、今回のエキスパートが担当するエキスパートに質問（ 6月20日～ 7月1日まで開催）へお寄せください！
https://supportforums.cisco.com/thread/2155078

Webcastの内容やQ&Aドキュメントは、本日より5営業日以内にこのサイトへ掲載いたします。
https://supportforums.cisco.com/community/csc-japan/ask-the-experts#view=webcasts

# 次回のCSC ライブExpert Webcast 予告

詳細が決まり次第、CSCホームページやソーシャルメディアでお知らせいたします

# ソーシャルメディアを使って
# シスコサポートコミュニティと繋がろう

http://www.facebook.com/CiscoSupportCommunityJapan

https://twitter.com/cscjapan

http://www.youtube.com/user/ciscosupportchannel

http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8

http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019

Newsletter Subscription:
https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=589&keyCode=146298_2&PHYSICAL%20FULFILLMENT%20Y/N=NO&SUBSCRIPTION%20CENTER=YES

# 今後参加したい Webcast に投票！

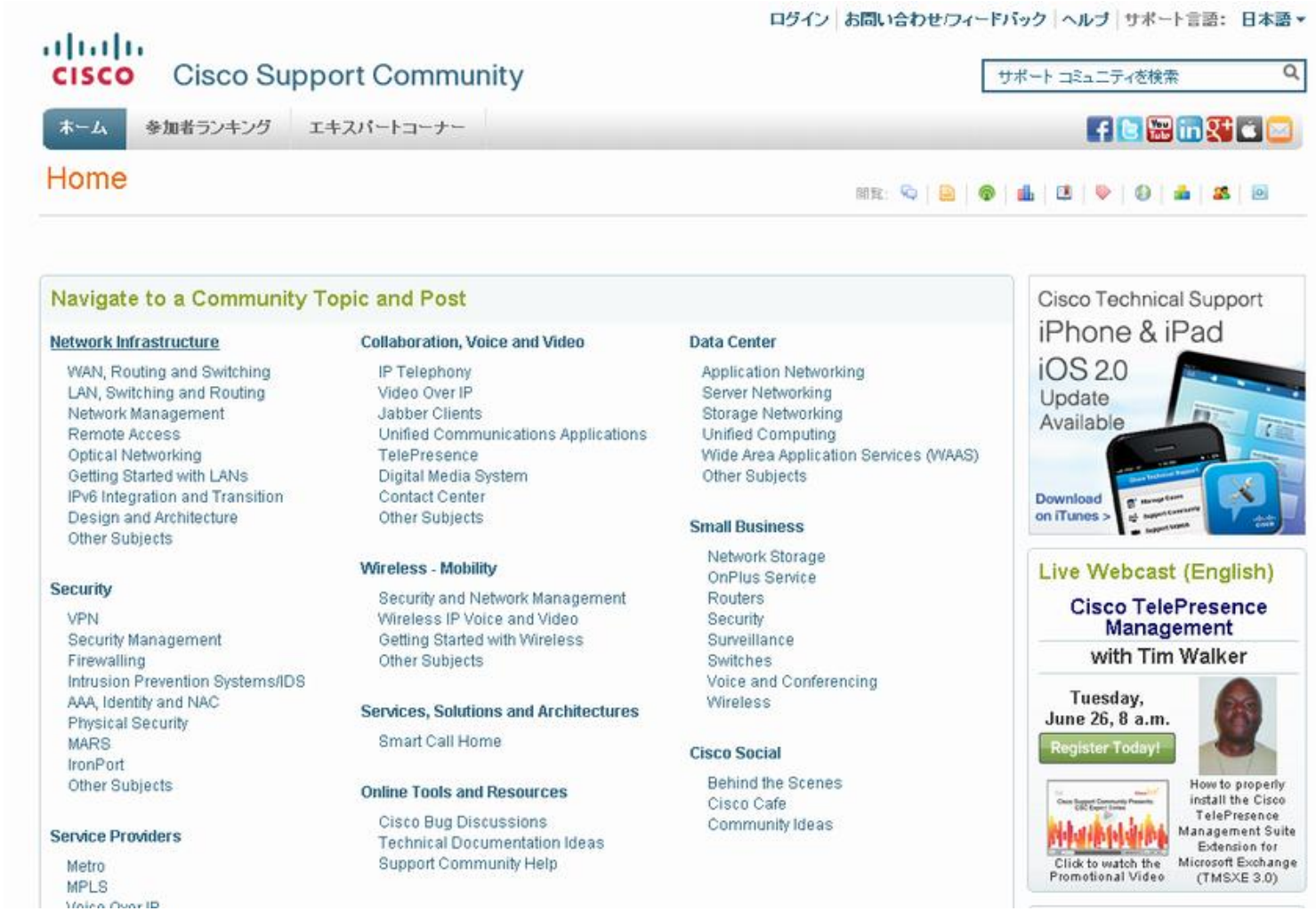

**サポートコミュニティにログインすると投票ボタンが表示されます（投票は匿名です）**

# コンテンツ評価へご協力ください


# 評価ポイントはユーザの総合得点として積算

# 英語版サポートコミュニティ

https://supportforums.cisco.com



# シスコ認定ラーニングパートナー

| スペシャリゼーション | ラーニングパートナー | リンク |
|---|---|---|
| データセンター | NGN-SF | http://ngn-sf.co.jp/ |
| データセンター | ネットワンシステムズ | https://www.netone.co.jp/academy/index.html |
| コラボレーション | グローバルナレッジ | http://www.globalknowledge.co.jp/ |

- シスコ認定ラーニングパートナーでは皆様のソリューションを最適化するために、Ciscoの認定したカリキュラムを使ったトレーニングを提供しております。

- また、シスコ認定ラーニングパートナーの中でも、シスコスペシャライズドパートナーは特にその専門分野においてのスキルを認められたパートナーのみが授与される認定資格となっております。

# ご参加ありがとうございました

評価アンケートへのご協力をよろしくお願いいたします

Thank you.