Ineternet Week 2014 [T2]
TCP/IP再認識～忘れちゃいけない UDP、ICMP

スカイリンクス株式会社
技術本部
國武　功一

Agenda

SKYLINKS

- 虐げられた？ICMP、その背景
- そもそもICMPとは？
- ICMPが消えた世界では
- どうすべきなのか

- 虐げられた？ICMP、その背景
- そもそもICMPとは？
- ICMPが消えた世界では
- どうすべきなのか

虐げられた？ICMP、その背景

SKYLINKS

- Broadcast Address というのがありまして

  そのセグメントにいるノードは、みんなお返事してくれた。

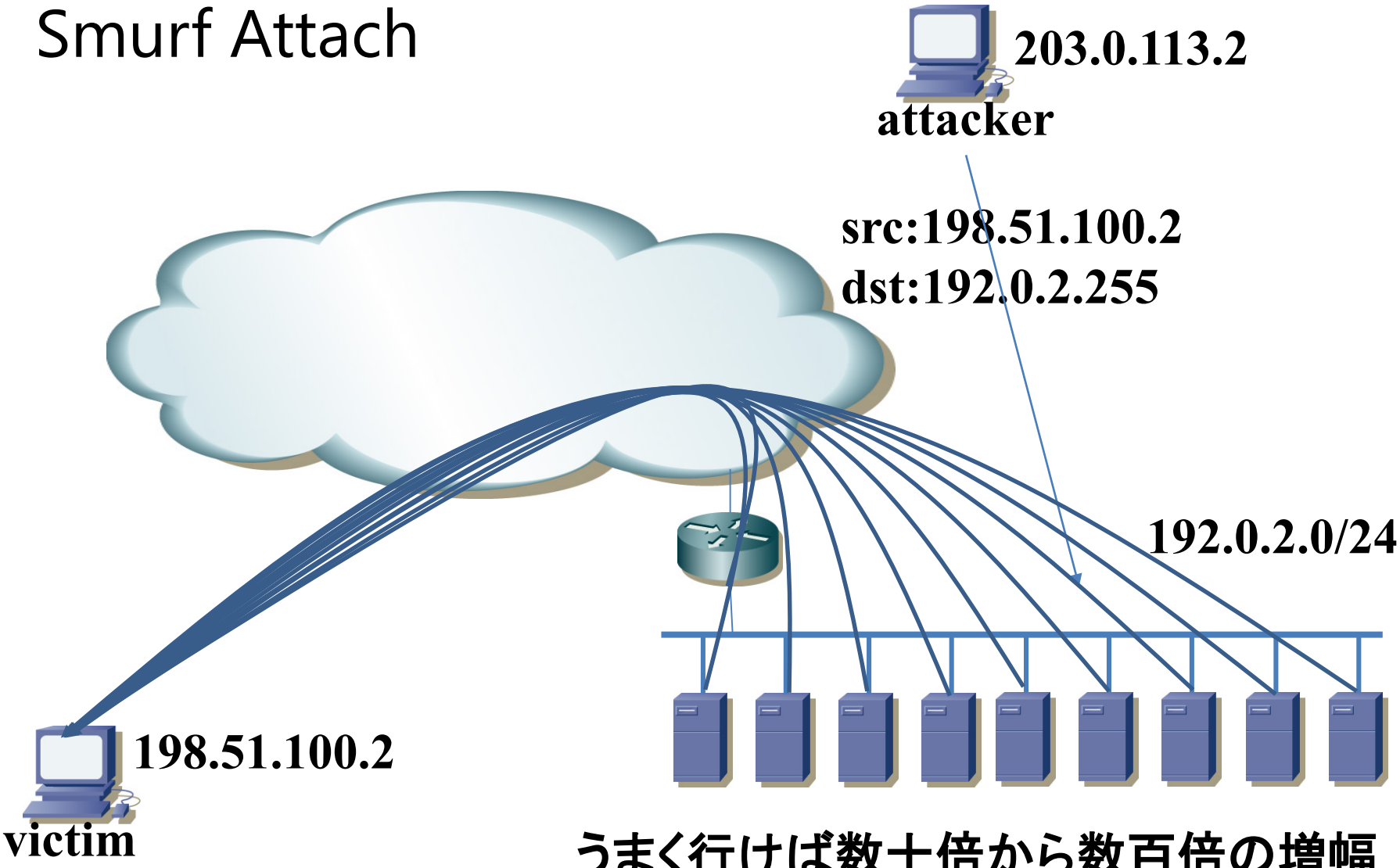
- ネットワークゲームがありまして

  遅延が低いクライアントがとても有利だった

- いまより、ずっと処理性能が低いクライアントがありまして

こんな攻撃が大流行（１）

- Smurf Attach

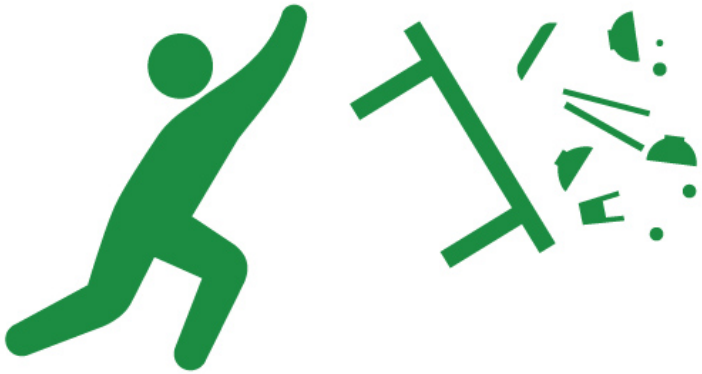


うまく行けば数十倍から数百倍の増幅

こんな攻撃が大流行（２）

- ちょうど、同時期に Ping of Death

  あるICMPを受け取ると、クライアントが死んだ



Loki

- まぁいわゆる ICMP tunneling

  ICMPの Echo / Replyのペイロードに、秘密のメッセージを埋め込む。

  => 情報漏洩の懸念

その結果...

- ICMPを Firewall で落とすことが大流行

で、いまも落とす必要あるの？

SKYLINKS

- Smurf Attach

  今日日、サーバは broadcast address に
  応答しない設定が標準

- Ping of Death

  さすがに、そんなバグを持ったOSはもうない（よね？？）

- Loki

  すべてのセグメントに適用するようなものでもない

でも……

- 疑わしきは罰せよ？
- 落とせばハッピー＆万事解決？

  ICMPをすべて落とすと、通信障害に繋がる！

- 虐げられた？ICMP、その背景
- そもそもICMPとは？
- ICMPが消えた世界では
- どうすべきなのか

そもそもICMPとは？

SKYLINKS

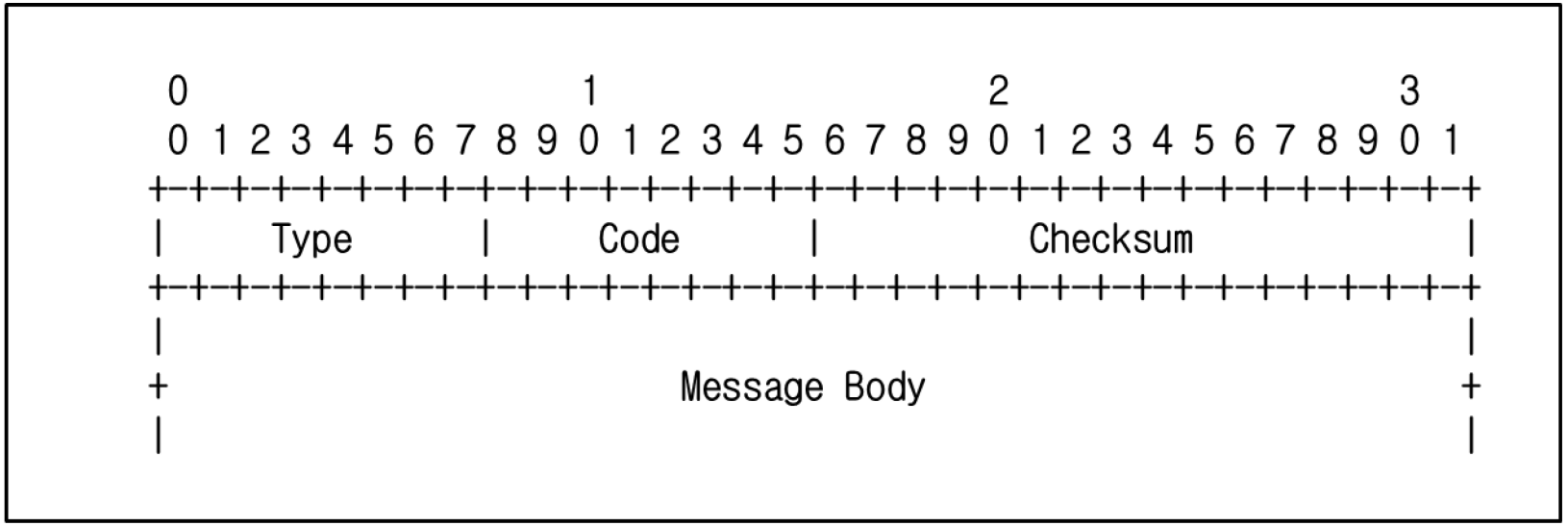
Internet Control Message Protocol

ICMP, uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module.
(RFC792 INTERNET CONTROL MESSAGE PROTOCOL)

ICMPは本来、IP通信において必要不可欠な存在

ICMPv4 フォーマット

TypeとCodeとの組み合わせで、機能が変わる



ICMPv4

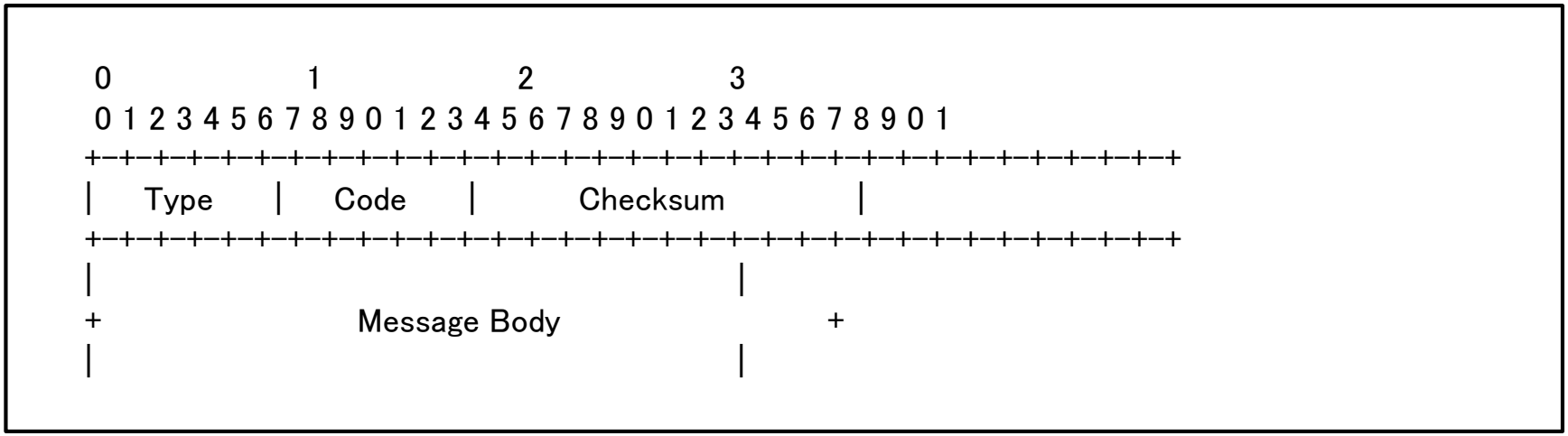
SKYLINKS

Type	Name	Reference
0	Echo Reply	[RFC792]
1	Unassigned	
2	Unassigned	
3	Destination Unreachable	[RFC792]
4	Source Quench (Deprecated)	[RFC792][RFC6633]
5	Redirect	[RFC792]
6	Alternate Host Address (Deprecated)	[RFC6918]
7	Unassigned	
8	Echo	[RFC792]
9	Router Advertisement	[RFC1256]
10	Router Solicitation	[RFC1256]
11	Time Exceeded	[RFC792]
12	Parameter Problem	[RFC792]
13	Timestamp	[RFC792]
14	Timestamp Reply	[RFC792]
15	Information Request (Deprecated)	[RFC792][RFC6918]
16	Information Reply (Deprecated)	[RFC792][RFC6918]
17	Address Mask Request (Deprecated)	[RFC950][RFC6918]
18	Address Mask Reply (Deprecated)	[RFC950][RFC6918]
19	Reserved (for Security)	[Solo]
20-29	Reserved (for Robustness Experiment)	[ZSu]
30	Traceroute (Deprecated)	[RFC1393][RFC6918]
31	Datagram Conversion Error (Deprecated)	[RFC1475][RFC6918]
32	Mobile Host Redirect (Deprecated)	[David Johnson][RFC6918]
33	IPv6 Where-Are-You (Deprecated)	[Simpson][RFC6918]
34	IPv6 I-Am-Here (Deprecated)	[Simpson][RFC6918]
35	Mobile Registration Request (Deprecated)	[Simpson][RFC6918]
36	Mobile Registration Reply (Deprecated)	[Simpson][RFC6918]
37	Domain Name Request (Deprecated)	[RFC1788][RFC6918]
38	Domain Name Reply (Deprecated)	[RFC1788][RFC6918]
39	SKIP (Deprecated)	[Markson][RFC6918]
40	Photuris	[RFC2521]
41	ICMP messages utilized by experimental□ mobility protocols such as Seamoby	[RFC4065]
42-252	Unassigned	
253	RFC3692-style Experiment 1	[RFC4727]
254	RFC3692-style Experiment 2	[RFC4727]
255	Reserved	[JBP]

※http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

ICMPv6 フォーマット

TypeとCodeとの組み合わせで、機能が変わるのはICMPと同じだが、ARP相当の機能がICMPv6に取り込まれるなど、より重要度を増しており、またICMPと互換性があるわけではない



ICMPv6 (1)

Type	Name	Reference
0	Reserved	
1	Destination Unreachable	[RFC4443]
2	Packet Too Big	[RFC4443]
3	Time Exceeded	[RFC4443]
4	Parameter Problem	[RFC4443]
100	Private experimentation	[RFC4443]
101	Private experimentation	[RFC4443]
102-126	Unassigned	
127	Reserved for expansion of ICMPv6 error messages	[RFC4443]
128	Echo Request	[RFC4443]
129	Echo Reply	[RFC4443]
130	Multicast Listener Query	[RFC2710]
131	Multicast Listener Report	[RFC2710]
132	Multicast Listener Done	[RFC2710]
133	Router Solicitation	[RFC4861]
134	Router Advertisement	[RFC4861]
135	Neighbor Solicitation	[RFC4861]
136	Neighbor Advertisement	[RFC4861]
137	Redirect Message	[RFC4861]
138	Router Renumbering	[Matt_Crawford]
139	ICMP Node Information Query	[RFC4620]
140	ICMP Node Information Response	[RFC4620]
141	Inverse Neighbor Discovery Solicitation Message	[RFC3122]
142	Inverse Neighbor Discovery Advertisement Message	[RFC3122]
143	Version 2 Multicast Listener Report	[RFC3810]

ICMPv6 (2)

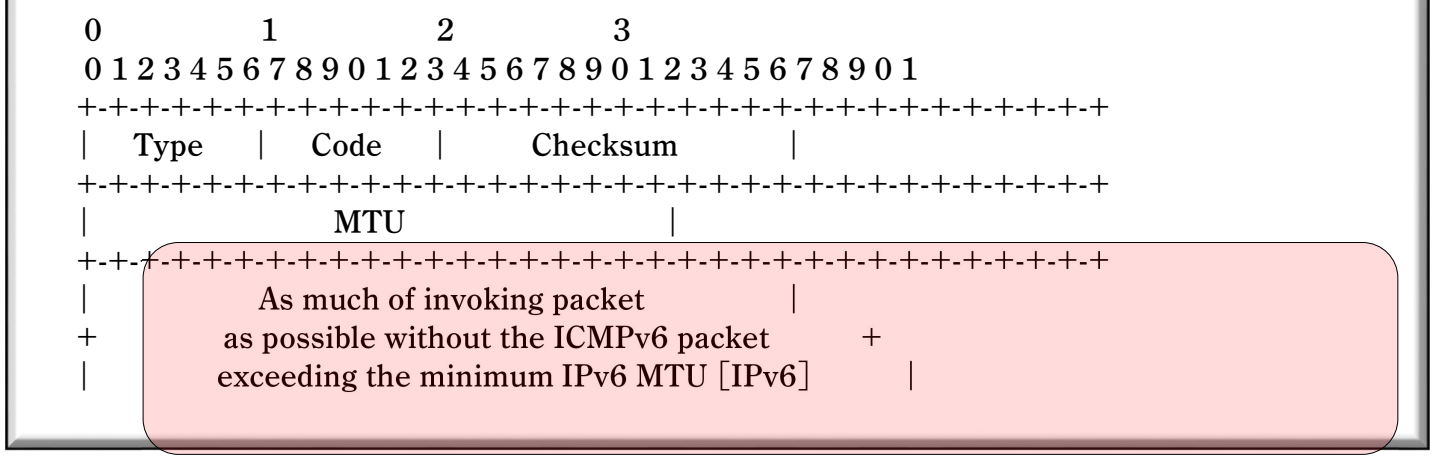
Type	Name	Reference
144	Home Agent Address Discovery Request Message	[RFC6275]
145	Home Agent Address Discovery Reply Message	[RFC6275]
146	Mobile Prefix Solicitation	[RFC6275]
147	Mobile Prefix Advertisement	[RFC6275]
148	Certification Path Solicitation Message	[RFC3971]
149	Certification Path Advertisement Message	[RFC3971]
150	ICMP messages utilized by experimental mobility protocols such as Seamoby	[RFC4065]
151	Multicast Router Advertisement	[RFC4286]
152	Multicast Router Solicitation	[RFC4286]
153	Multicast Router Termination	[RFC4286]
154	FMIPv6 Messages	[RFC5568]
155	RPL Control Message	[RFC6550]
156	ILNPv6 Locator Update Message	[RFC6743]
157	Duplicate Address Request	[RFC6775]
158	Duplicate Address Confirmation	[RFC6775]
159-199	Unassigned	
200	Private experimentation	[RFC4443]
201	Private experimentation	[RFC4443]
255	Reserved for expansion of ICMPv6 informational messages	[RFC4443]

※http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml

補足

- 特定のエラー処理に伴う応答パケットには、原因となったパケットのIPヘッダおよびデータが埋め込まれるものがある。

3.2. Packet Too Big Message



- 虐げられた？ICMP、その背景
- そもそもICMPとは？
- ICMPが消えた世界では
- どうすべきなのか

たとえばICMPが消えたなら…

たとえばICMPが消えたなら…

- Path MTU Discovery が動かず通信ができない！
- IPv6では、L2のアドレス解決ができず、通信ができない！
- DHCPv6でアドレスを配ることができなくなる！

机上の空論ではなく、一部起きてしまっている

現実に起きてしまっているICMPのない世界

Path MTU Discovery Blackholeとは？

Path MTU Discoveryおさらい

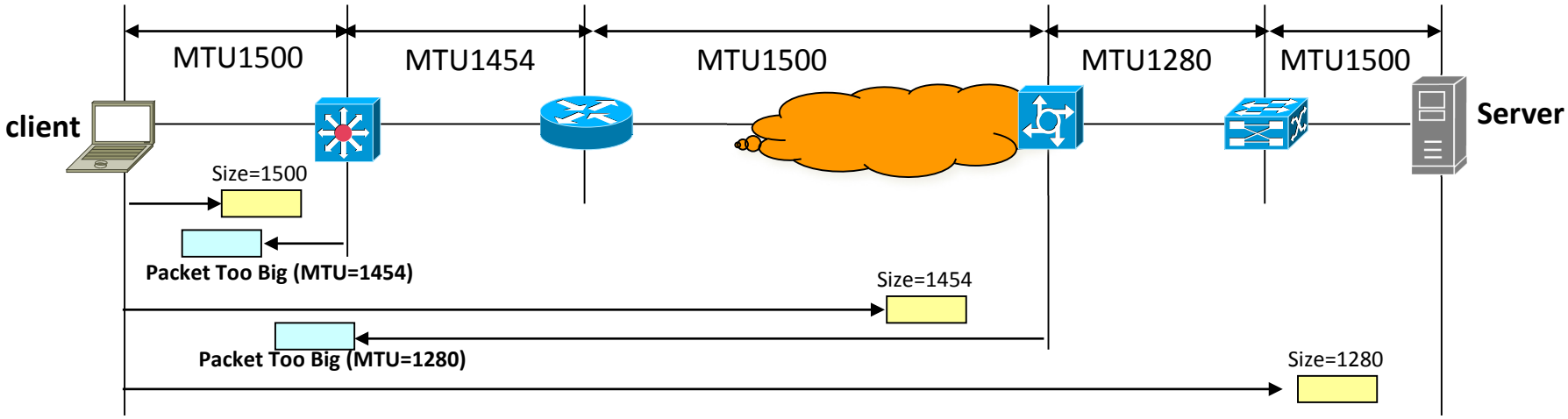
SKYLINKS

- IPv6 では中継ノードでフラグメントしない（始点ノードが実施）
- IPv4 ではルータ等の中継ノードがフラグメントを実施

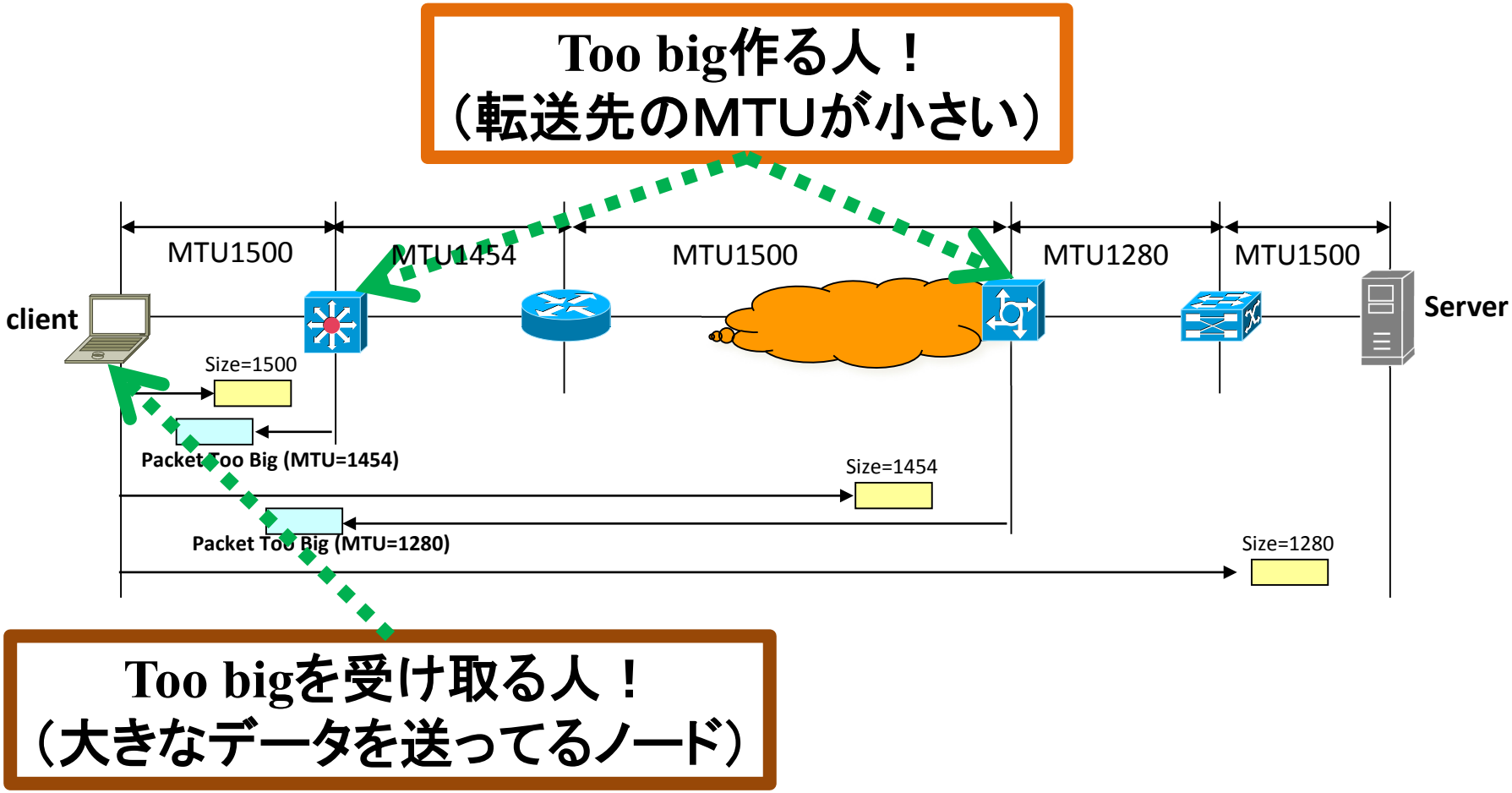
  ただし、DFビットが立っているパケットはフラグメントされず（この場合はIPv6の場合と同様）
- 送信パケットに対する ICMP Error Message を受信時、MTU を変更（最初のリンクのMTU が初期値）
  - IPv4の場合
    - ICMP Type 3/Code 4のパケットを受信時、始点ノードでフラグメントして再送
  - IPv6の場合
    - ICMPv6 Packet Too Big Message 受信時、始点ノードでフラグメントして再送
- L2 SWのMTUにひっかかった場合は破棄される

Path MTU Discoveryおさらい

IPv6での例



Path MTU Discoveryおさらい



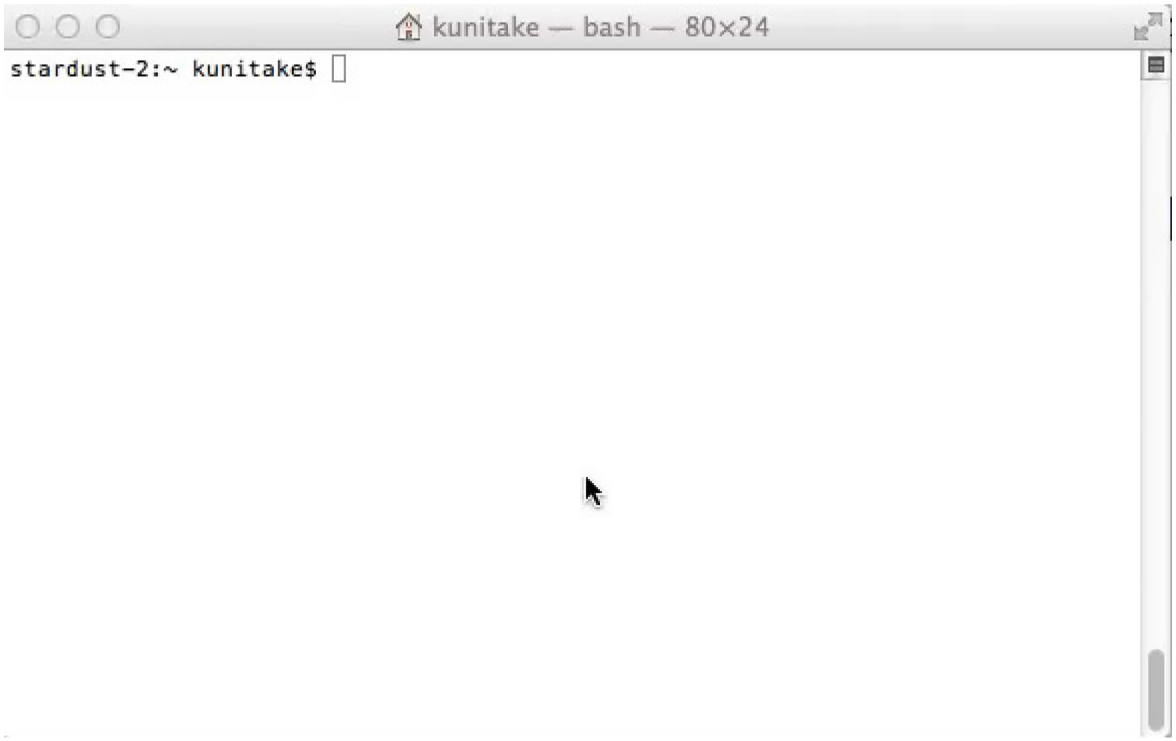
Too big 受け取るのはだれ？

- コンテンツを送信する側
  - ウェブサーバ
  - メール送信者(大きな添付ファイルとか)
  - Dropbox的ななにか

PMTUD Blackholeなぜ困る？

- Path MTU Discovery Blackholeとは、必要なICMPパケットが届かない現象を指す。
- PMTU Dicoveryが動作しないと、適切なサイズでのパケットの再送ができず、通信ができない。

実際の現象（デモ）

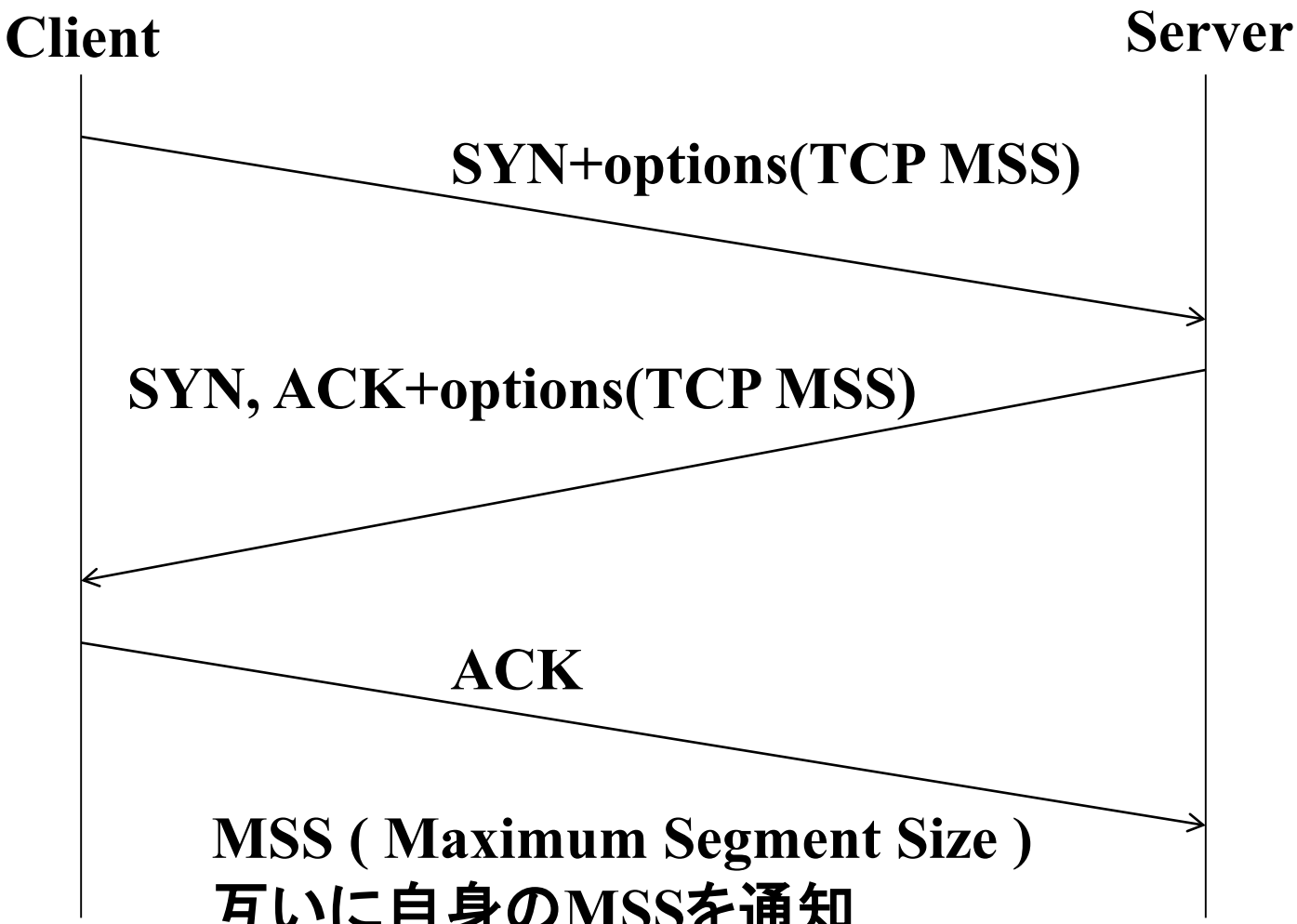


それってIPv6だけだよね？

- IPv4でも発生している＆かつてよく発生していた
  - なぜフラグメントしないの？

    サーバから送出されるパケットは、ほとんどがDFビットが立っており、フラグメントが禁止されるため。
  - なぜ現在、IPv4で目立っていないのかというと、一般家庭でよく利用されている、いわゆるブロードバンドルータに、TCP MSS調整機能(TCP MSS Clamping機能）があるから

TCP 3way handshake復習



TCP MSS Clamping機能

- 途中経路のルータが、MSSオプションを書き換える。
- TCPに限って言えば、よく効く
  - TCPの再送が抑制される
  - サーバのMTUキャッシュの抑制

    ただし、必ずしもPath MTU値に調整できるとは限らないし、UDPなどは救済できない

- 虐げられた？ICMP、その背景
- そもそもICMPとは？
- ICMPが消えた世界では
- どうすべきなのか

どうすべきなのか

- 安易にICMPを止めてしまうのは通信障害を招き、また切り分けを難しくさせてしまう。
- ICMP/ICMPv6への理解を深め、適切なパケットは通す。

”個人的な“おすすめは、エラー関連のICMPを通すこと

- **Destination unreach**
- **Fragmentation Needed / Packet Too big**
- **Time Exceeded (Tracerouteを許可するなら)**
- **Parameter Problem**

Q&A?