ちょっとだけ

SFC について調べてみた

浅間 正和 @ 有限会社 銀座堂

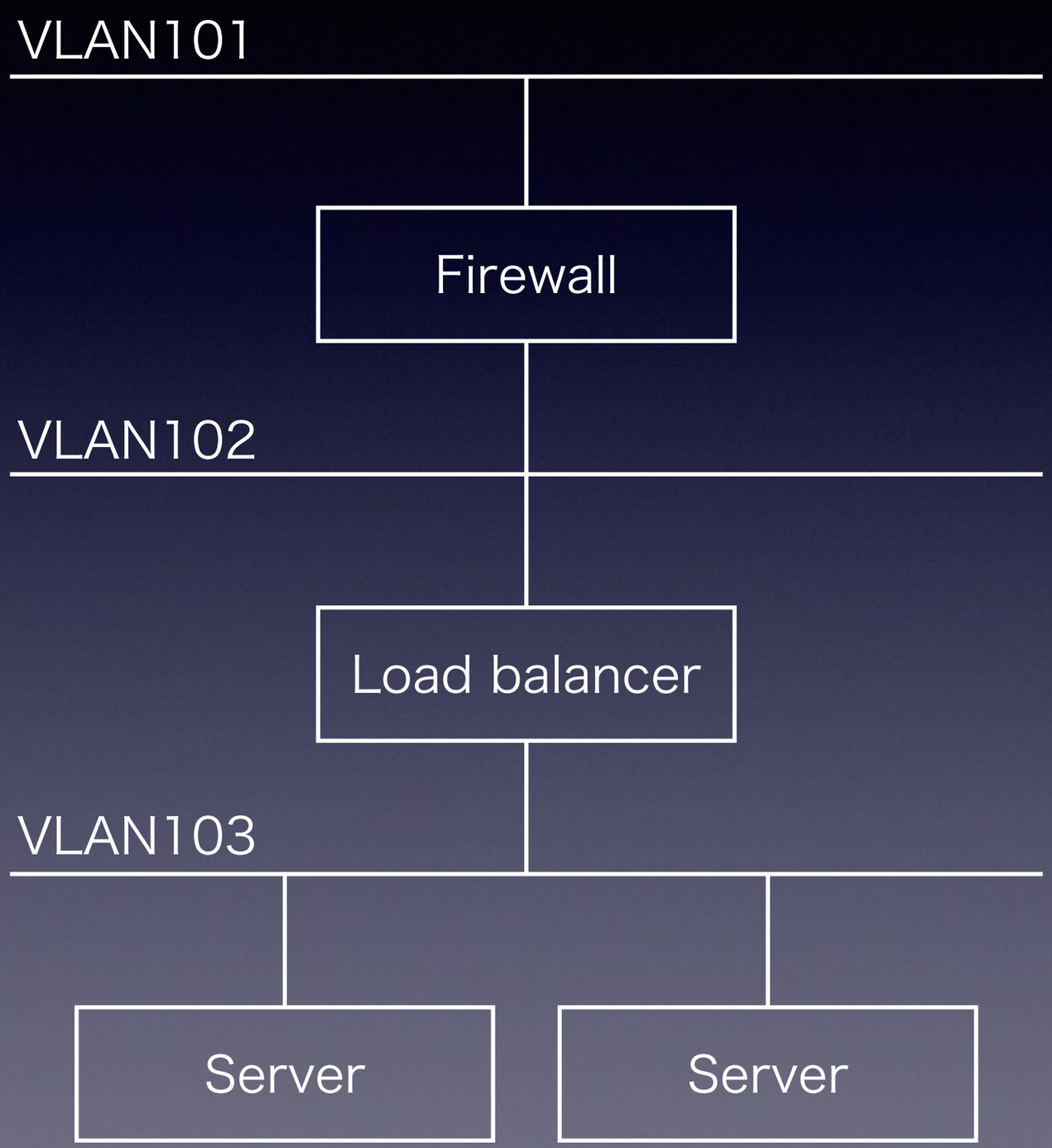
アジェンダ

- ざっくり SFC
- いまどんな状態？
- ちょっとくわしく SFC

SFC とは？

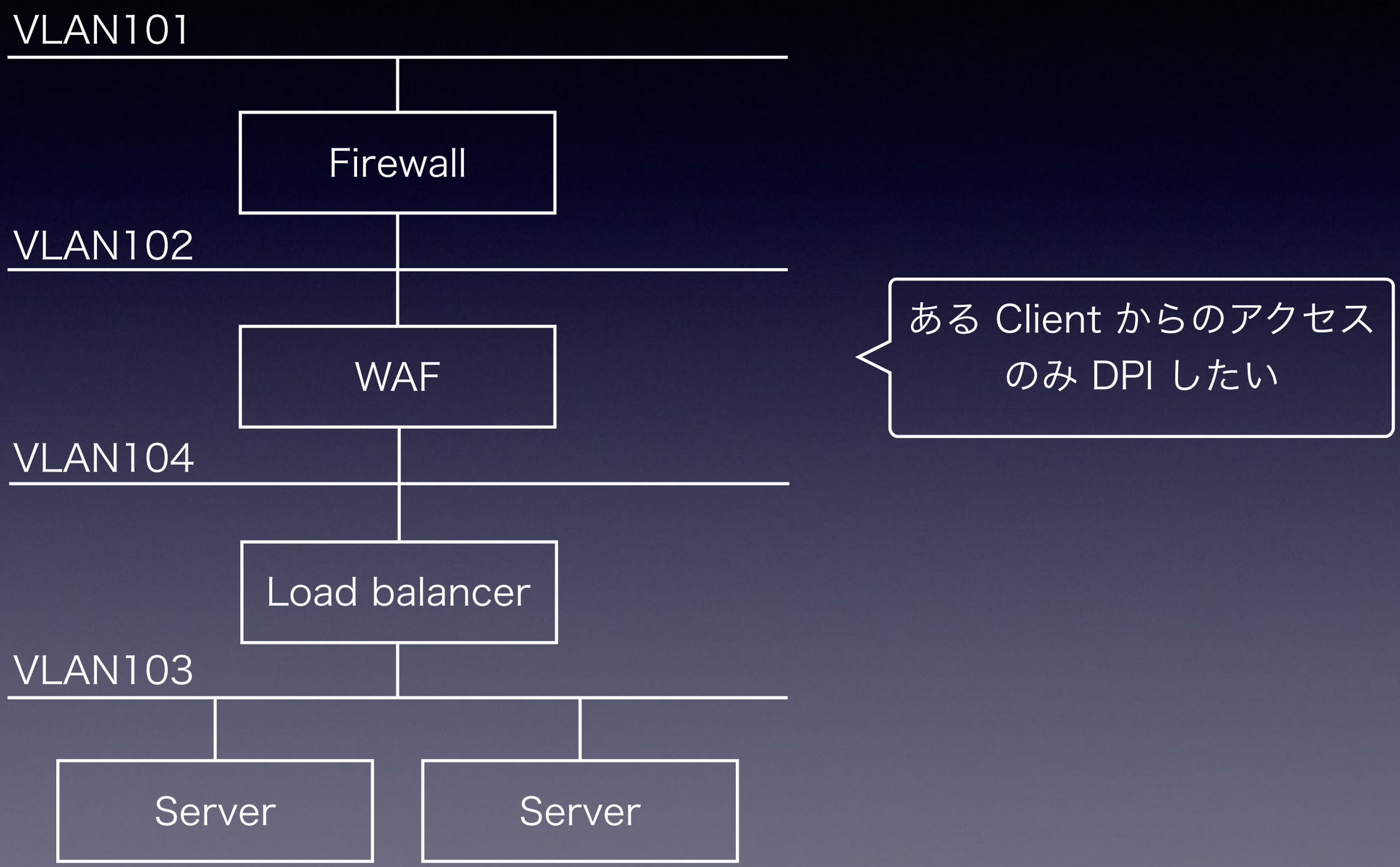
- Service Function Chaining の略
- いわゆる SDN や NFV を実装するためのプロトコルのひとつ
- Firewall、Deep Packet Inspection、Load balancer、NAT44、NAT64 といった Service Function の “連なり” を柔軟に適用できるようにする為のプロトコル
- IETF SFC WG で標準化が進められている

こんなときどうする？

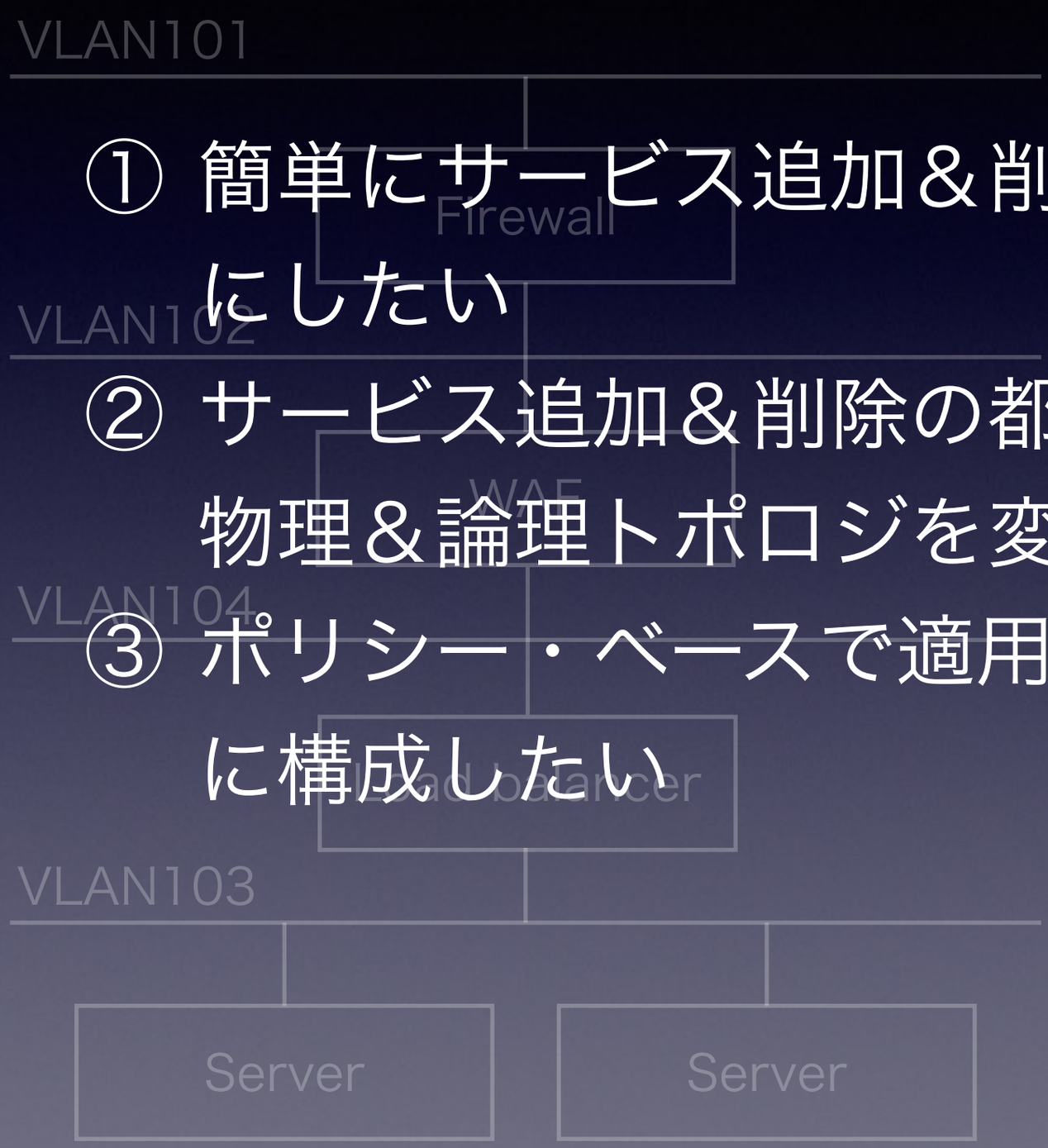


やっぱり Web Application Firewall も入れたい

こんなときどうする？


VLAN101
Firewall
VLAN102
WAF
VLAN104
Load balancer
VLAN103
Server
Server
ある Client からのアクセス
のみ DPI したい

こんなときどうする？

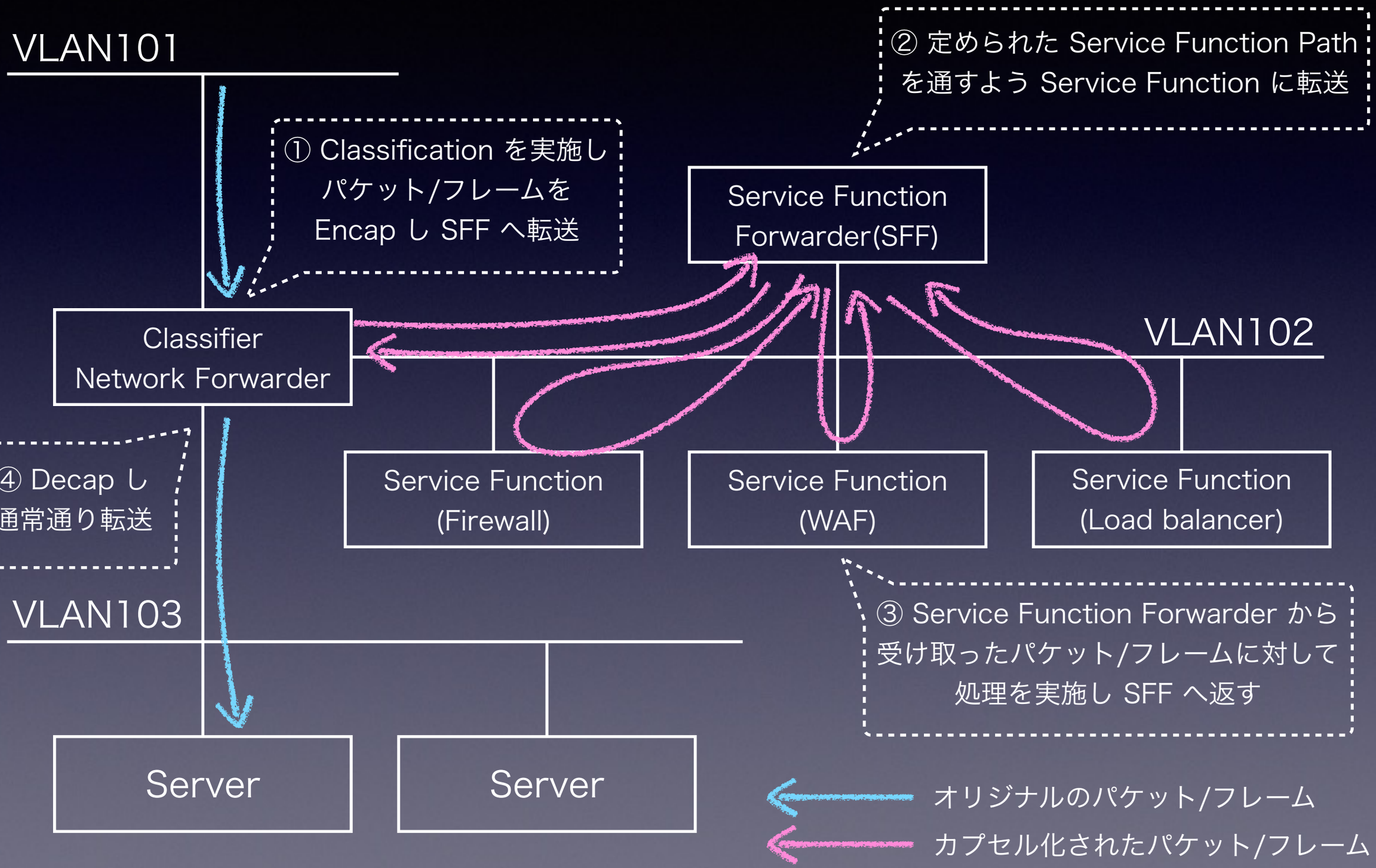


① 簡単にサービス追加＆削除を設定できるようにしたい

② サービス追加＆削除の都度にネットワークの物理＆論理トポロジを変えたくない

③ ポリシー・ベースで適用するサービスを柔軟に構成したい

SFC ならこうなる？


VLAN101
① Classification を実施し
パケット/フレームを
Encap し SFF へ転送
② 定められた Service Function Path
を通すよう Service Function に転送
Service Function
Forwarder(SFF)
Classifier
Network Forwarder
VLAN102
Service Function
(Firewall)
Service Function
(WAF)
Service Function
(Load balancer)
④ Decap し
通常通り転送
③ Service Function Forwarder から
受け取ったパケット/フレームに対して
処理を実施し SFF へ返す
VLAN103
Server
Server
オリジナルのパケット/フレーム
カプセル化されたパケット/フレーム

いまどんな状態？

- Problem Statement
  - draft-ietf-sfc-problem-statement
  - draft-ietf-sfc-dc-use-cases
  - draft-ietf-sfc-use-case-mobility
- Architecture
  - draft-ietf-sfc-architecture
- Generic SFC Encapsulation
  - draft-quinn-sfc-nsh
  - draft-guichard-sfc-nsh-dc-allocation
  - draft-napper-sfc-nsh-mobility-allocation
  - draft-zhang-sfc-sch
- Control Plane Mechanisms
  - draft-ww-sfc-control-plane
- Manageability
  - たくさん

いまどんな状態？

- Goals and Milestones(2014-03-05 charter)
  - Apr 2014 - Submit to IESG Information document defining the SFC problem statement and core use cases
  - Apr 2014 - Consult with OPS area on possible SFC charter modifications for management and configuration of SFC components related to the support of Service Function Chaining
  - Jan 2015 - Submit to IESG Informational document defining the architecture for SFC
  - Jan 2015 - Informational document defining the control plane requirements for conveying information between control or management elements and SFC implementation points
  - Aug 2015 - Submit to IESG Standards Track document specifying the generic service function chaining header encapsulation

SFC 用語

- Service Function
  - 受信パケットに対してなにかの処理を施す機能
    (例: Firewall、 DPI、 Load balancer、 NAT44、 NAT64、 NPTv6、 …)
- Service Function Chain
  - 抽象的な Service Function の順序付き集合
    (例: Firewall → DPI → NAT44)
- Service Function Path
  - Service Function Chain から具体的に決定した Service Function の経路
    (例: DC#1の Firewall#1 → DC#1 の DPI#1 → DC#1 の NAT44#1)

SFC 用語

- Classification
  - 定義されたポリシーとパケットの情報から Service Function Path を決定する行為
- Classifier
  - Classification を実行するひと
- Service Function Forwarder
  - Service Function Path に従いパケットを Service Function に転送する＆から受け取るひと
- SFC Proxy
  - SFC に対応していない機器のためにパケットから SFC ヘッダを取って転送したり逆に受け取ったパケットに SFC ヘッダをつけたりしてくれるひと

Network Service Header(NSH)

- IETF SFC WG で議論されている 2 つの Encapsulation フォーマットのうちのひとつ
  - もうひとつは Service Chain Header(SCH)
- WG のメーリングリストを眺めた感じでは Encapsulation フォーマットの本命？？？
  - 固定長と可変長の 2 種類のメタデータ・タイプ
  - IPv4、IPv6、Ethernet を転送可能
  - トランスポート・プロトコルに依存しない
    - I.D. では GRE、VXLAN-gpe、Ethernet の 3 つが例として説明されている

Network Service Header(NSH)

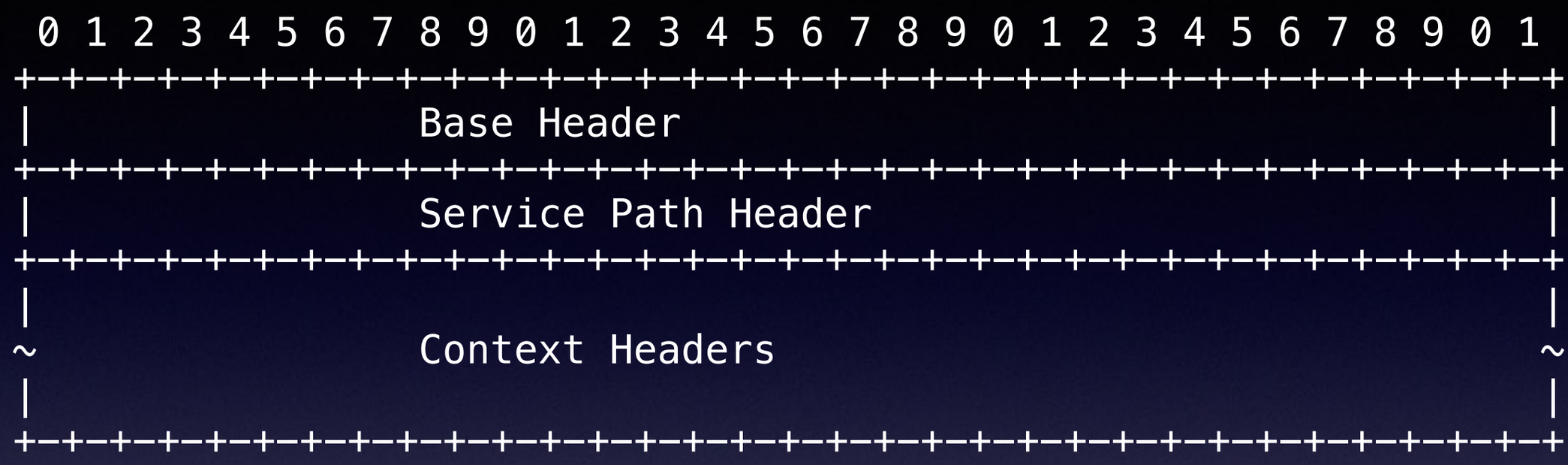


Figure 1: Network Service Header

Network Service Header(NSH)

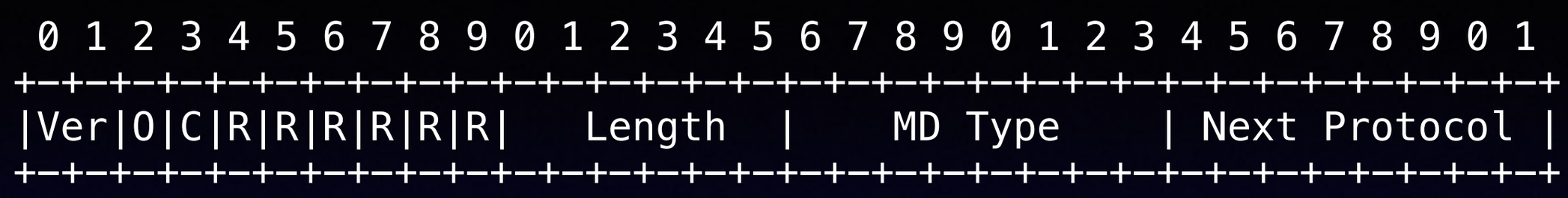


Figure 2: NSH Base Header

Base Header Field Descriptions

Version: The version field is used to ensure backward compatibility going forward with future NSH updates.

O bit: Indicates that this packet is an operations and management (OAM) packet. SFF and SFs nodes MUST examine the payload and take appropriate action (e.g. return status information).

OAM message specifics and handling details are outside the scope of this document.

C bit: Indicates that a critical metadata TLV is present (see section 3.4.2). This bit acts as an indication for hardware implementers to decide how to handle the presence of a critical TLV without necessarily needing to parse all TLVs present. The C bit MUST be set to 1 if one or more critical TLVs are present.

Network Service Header(NSH)

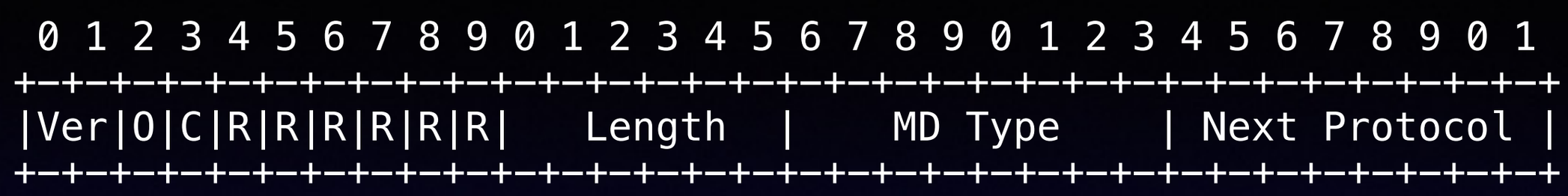


Figure 2: NSH Base Header

Length: total length, in 4 byte words, of the NSH header, including optional variable TLVs.

MD Type: indicates the format of NSH beyond the base header and the type of metadata being carried. This typing is used to describe the use for the metadata. A new registry will be requested from IANA for the MD Type.

NSH defines two MD types:

0x1 which indicates that the format of the header includes fixed length context headers.

0x2 which does not mandate any headers beyond the base header and service path header, and may contain optional variable length context information.

Network Service Header(NSH)

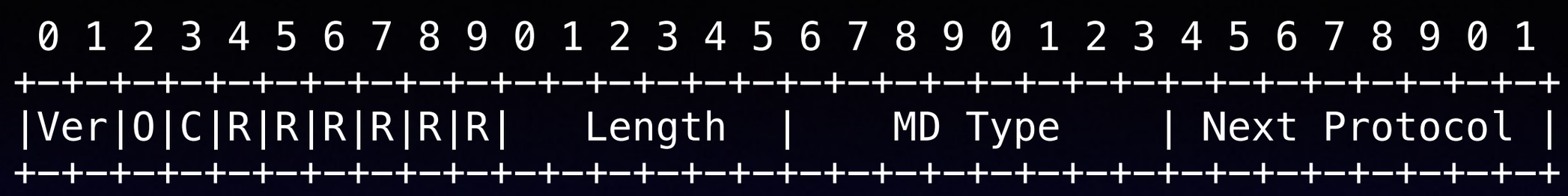


Figure 2: NSH Base Header

The format of the base header is invariant, and not described by MD Type.

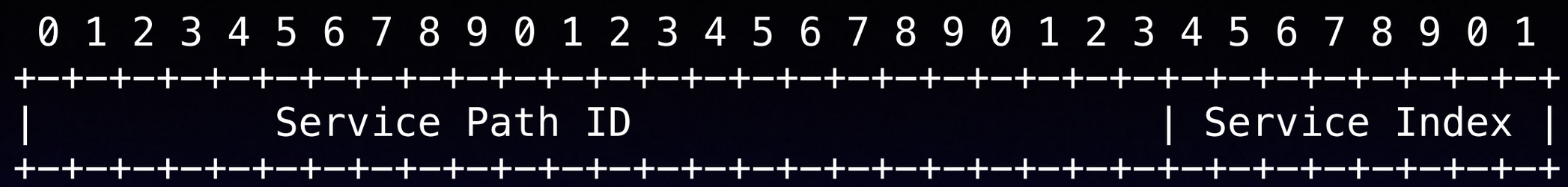
NSH implementations MUST support MD-Type 0x1, and SHOULD support MD-Type 0x2.

Next Protocol: indicates the protocol type of the original packet. A new IANA registry will be created for protocol type.

This draft defines the following Next Protocol values:

0x1 : IPv4
0x2 : IPv6
0x3 : Ethernet

Network Service Header(NSH)



Service path ID (SPI): 24 bits
Service index (SI): 8 bits

Figure 3: NSH Service Path Header

Service Path Identifier (SPI): identifies a service path. Participating nodes MUST use this identifier for path selection. An administrator can use the service path value for reporting and troubleshooting packets along a specific path.

Service Index (SI): provides location within the service path. Service index MUST be decremented by service functions or proxy nodes after performing required services. MAY be used in conjunction with service path for path selection. Service Index is also valuable when troubleshooting/reporting service paths. In addition to location within a path, SI can be used for loop detection.

Network Service Header(NSH)

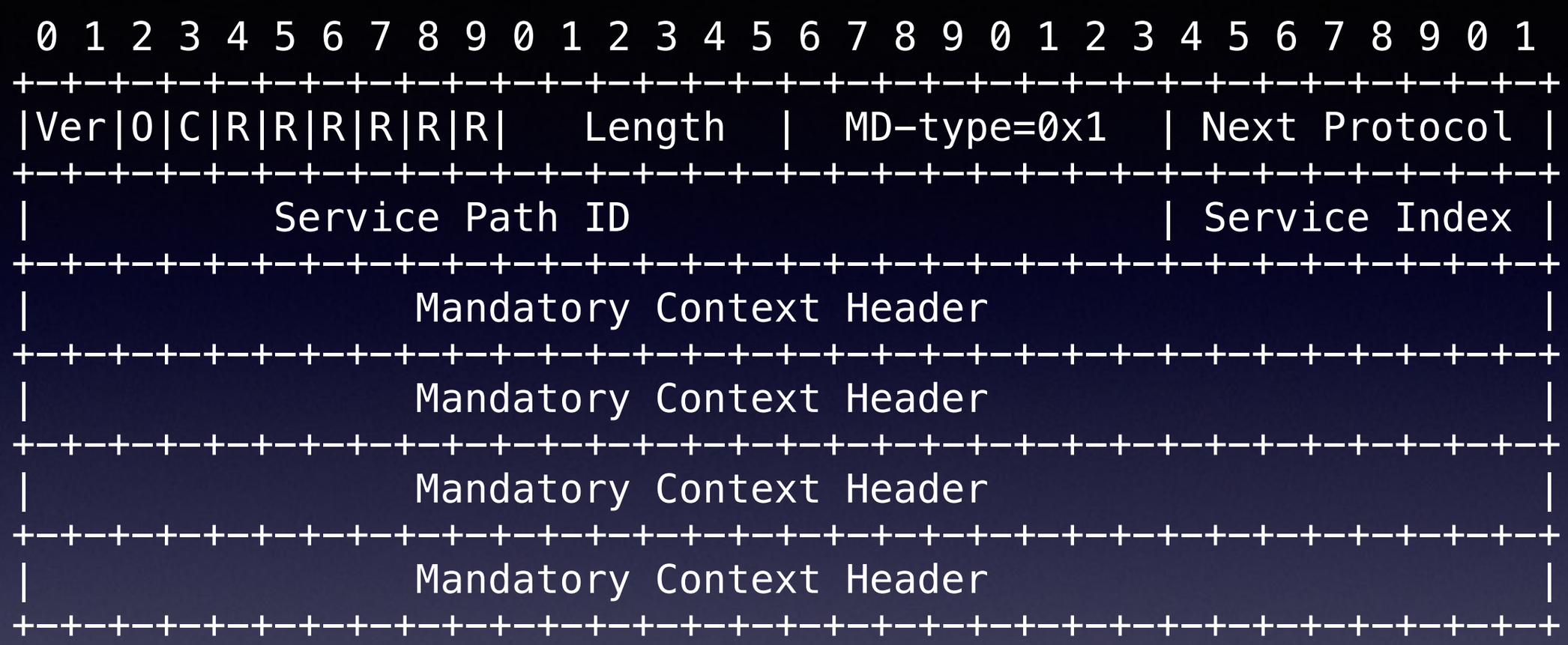


Figure 4: NSH MD-type=0x1

Network Service Header(NSH)

http://tools.ietf.org/html/draft-guichard-sfc-nsh-dc-allocation-01

4. Recommended Data Center Mandatory Context Allocation

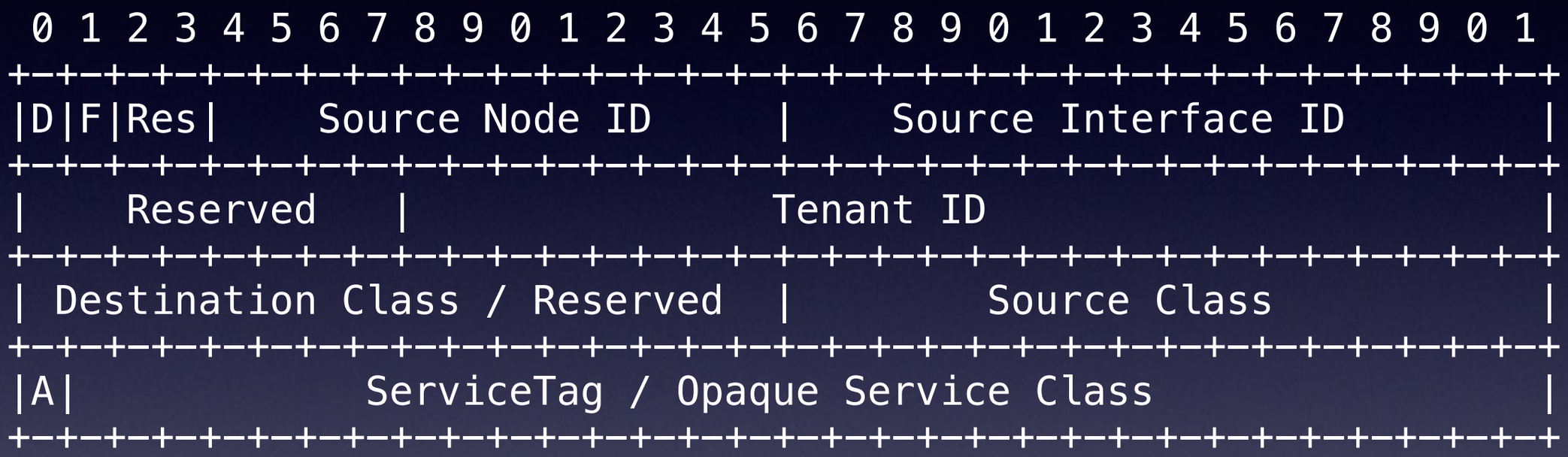


Figure 2: NSH DC Context Allocation

Network Service Header(NSH)

http://tools.ietf.org/html/draft-napper-sfc-nsh-mobility-allocation-00

4. Recommended Mobility Context Allocation

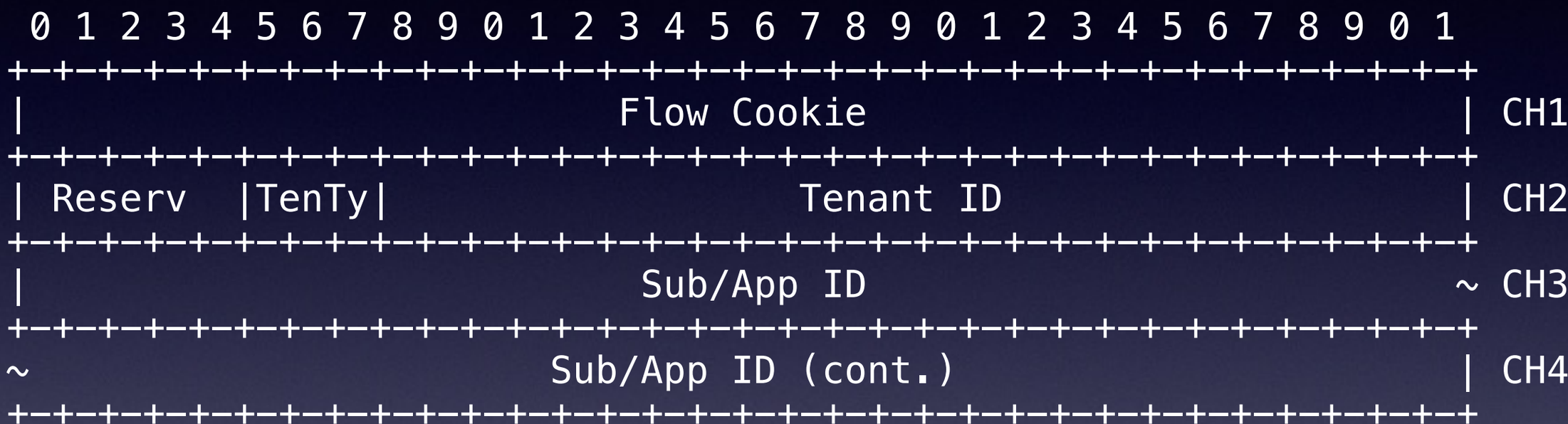


Figure 2: NSH Mobility Context Allocation

Network Service Header(NSH)

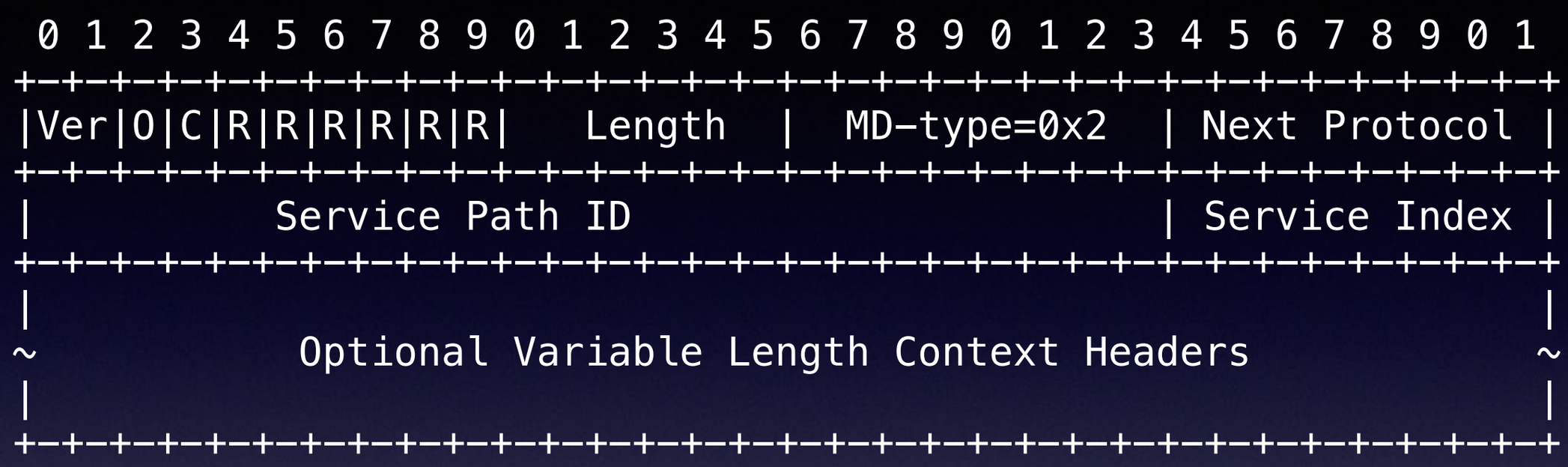


Figure 7: NSH MD-type=0x2

NSH MD Type 2 MAY contain optional variable length context headers.
The format of these headers is as described below.

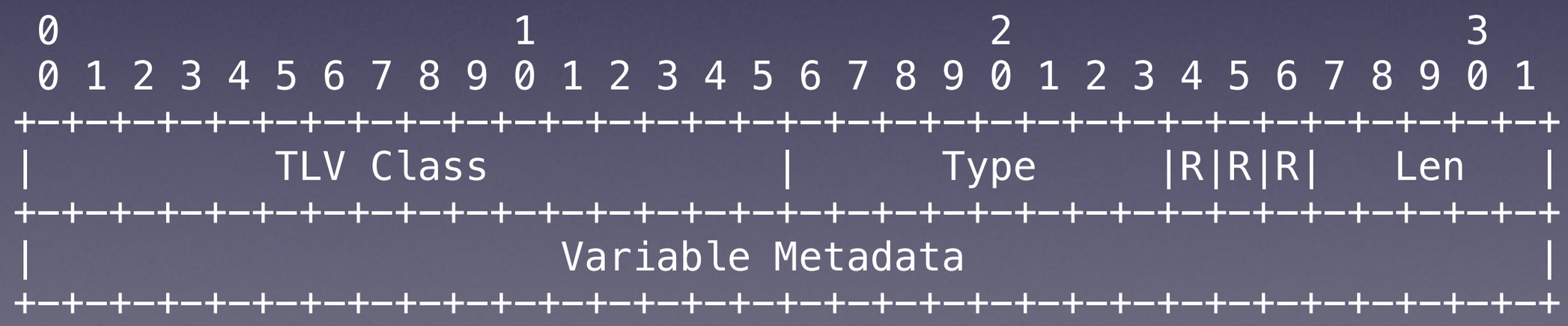


Figure 8: Variable Context Headers

Network Service Header(NSH)

TLV Class: describes the scope of the "Type" field. In some cases, the TLV Class will identify a specific vendor, in others, the TLV Class will identify specific standards body allocated types.

Type: the specific type of information being carried, within the scope of a given TLV Class. Value allocation is the responsibility of the TLV Class owner.

The most significant bit of the Type field indicates whether the TLV is mandatory for the receiver to understand/process. This effectively allocates Type values 0 to 127 for non-critical options and Type values 128 to 255 for critical options. Figure 7 below illustrates the placement of the Critical bit within the Type field.

Figure 9: Critical Bit Placement Within the TLV Type Field

Network Service Header(NSH)

11. NSH Encapsulation Examples

11.1. GRE + NSH

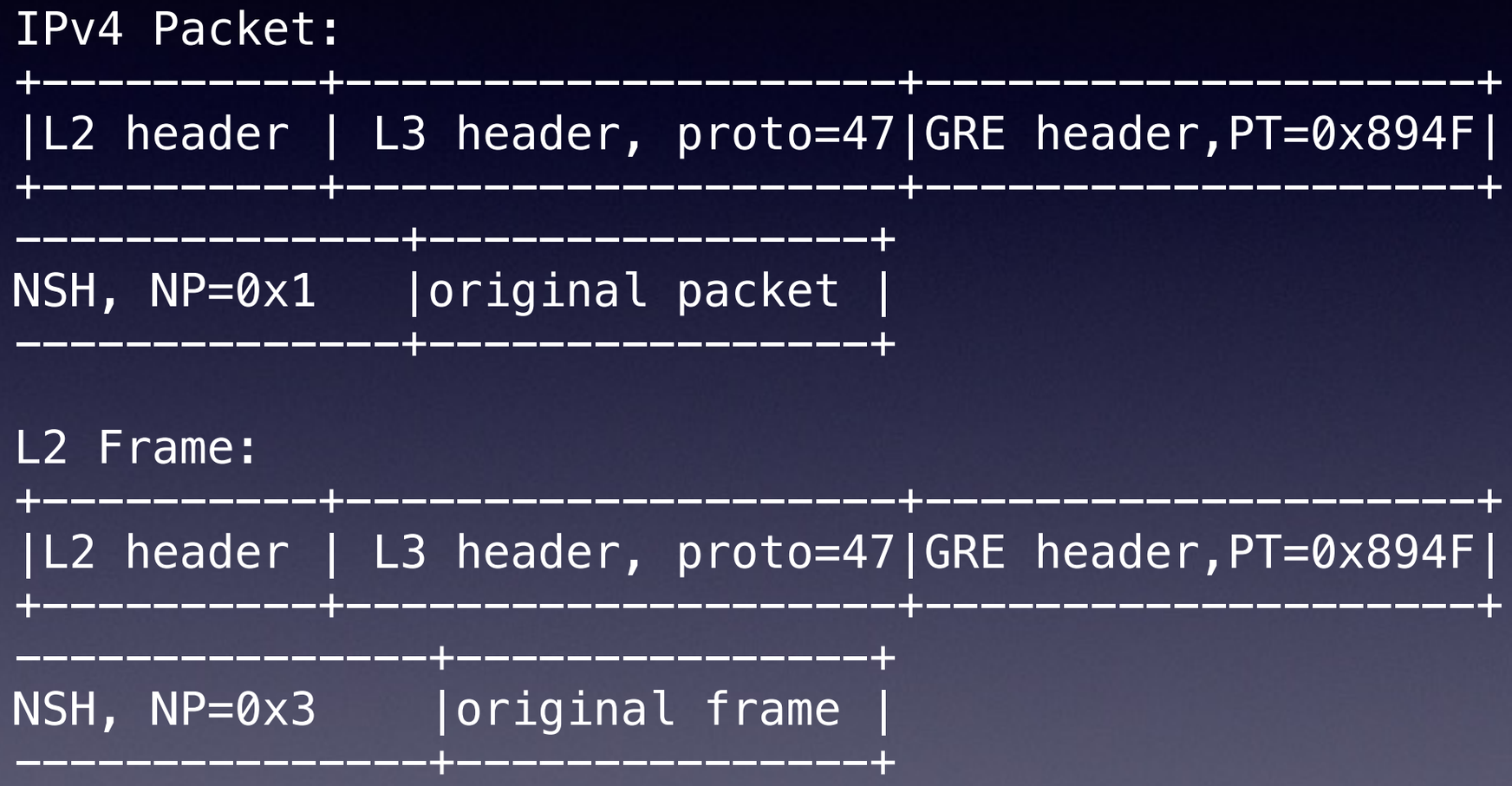


Figure 21: GRE + NSH

Network Service Header(NSH)

11. NSH Encapsulation Examples

11.2. VXLAN-gpe + NSH

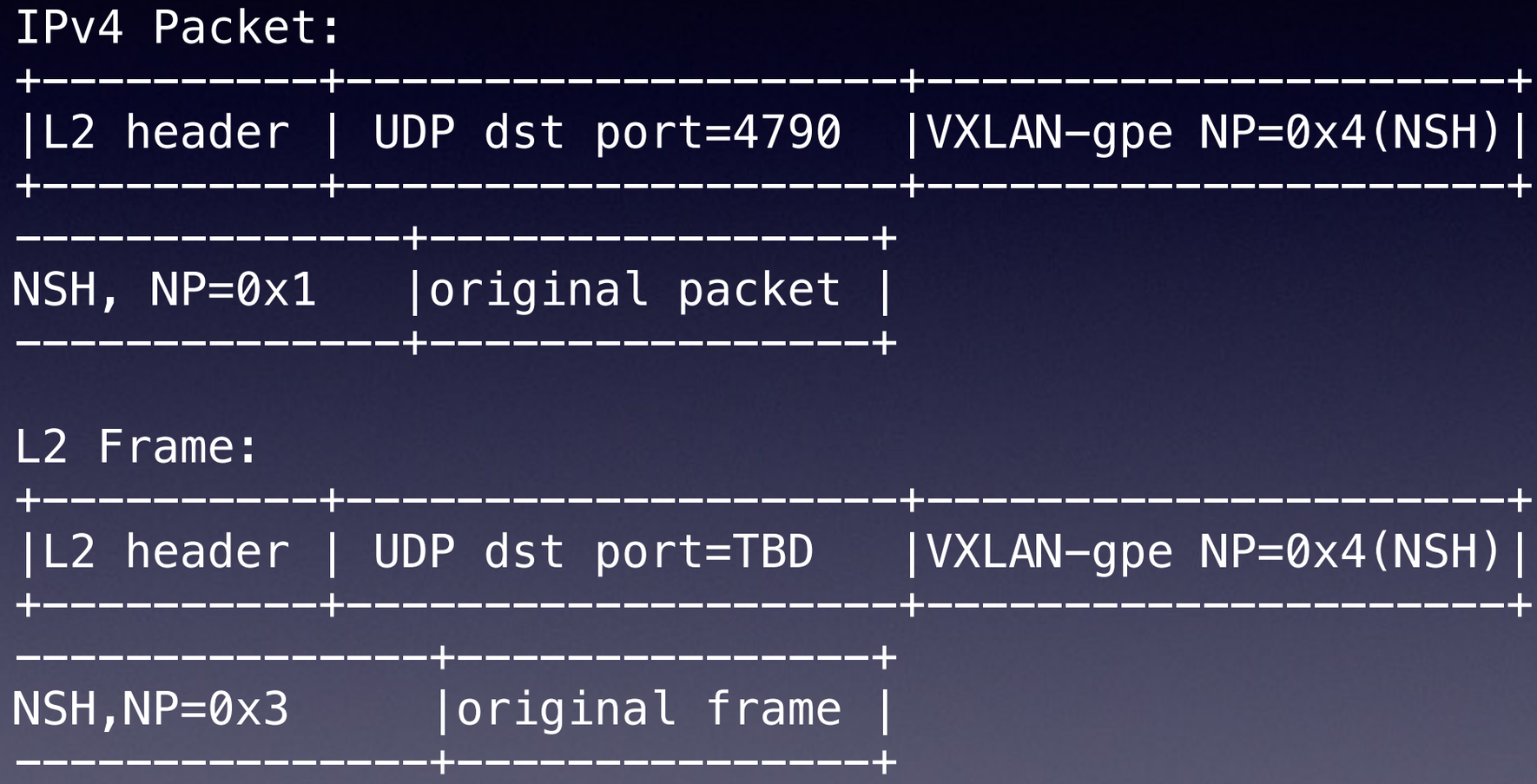


Figure 22: VXLAN-gpe + NSH

Network Service Header(NSH)

11. NSH Encapsulation Examples

11.3. Ethernet + NSH

IPv4 Packet:

L2 Frame:

Figure 23: Ethernet + NSH

SFF と SF のやりとり

① SPI と SI から次の SF のアドレスと
トランスポート・プロトコルを調べ転送

Service Function
Forwarder(SFF)

Service Function
(Firewall)

SPI	SI	NH	Transport
10	3	1.1.1.1	VXLAN-gpe
10	2	2.2.2.2	nvGRE
245	12	192.168.45.3	VXLAN-gpe
10	9	10.1.2.3	GRE
40	9	10.1.2.3	GRE
50	7	01:23:45:67:89:ab	Ethernet
15	1	Null (end of path)	None

Figure 10: SFF NSH Mapping Example

② サービス・ファンクションの処理を実施し SI を減算し SFF へ転送
③ 場合によっては Re-classification を実施し SPI と SI を再設定

まとめ

- Probrem Statement に書かれた問題をちゃんと対処できるとすれば結構便利？
- 実用できるようになる(SFC 対応の SF や SFF が一般に出回る)ようになるにはまだまだ時間がかかりそう？
- データセンター向けの Context Header の割り当てでは Multi-tenancy での利用もちゃんと考慮されているようなので高価な Service Function（たとえば Web Application Firewall）の切り売りができるようになるかも？

調べていて気になったこと

- よく Service Function Forwarder を直列させてるのを見るけどあれやると Service Function の追加・削除が面倒になるのでは？
- Service Function Forwarder がボトルネックになったりしない？スケールアウトさせる？
- Control Plane が大変そう？
  - SPI の割り当てどうすんの？
  - Service Function が Re-classification を実施するということは全ての Classifier、 Service Function Forwarder、 Service Function の間で SPI の同期が取れている必要がある？

参考情報

- http://tools.ietf.org/wg/sfc/
- http://www.ntt.co.jp/news2015/1502/150212a.html
- http://nfvwiki.etsi.org/images/PoC_proposal_Scalable_Service_Chaining-revisedv3%28final%29.pdf