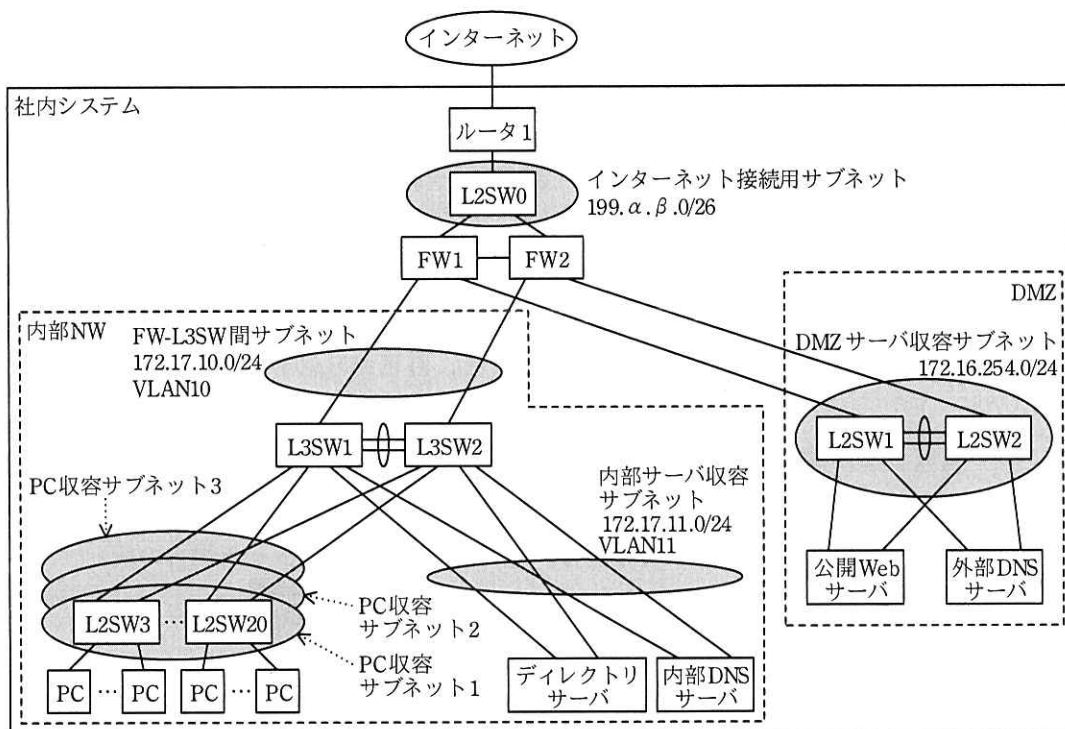


問1 社内システムの更改に関する次の記述を読んで、設問1～6に答えよ。

G社は、都内に本社を構える従業員600名の建設会社である。G社の従業員は、情報システム部が管理する社内システムを業務に利用している。情報システム部は、残り1年でリース期間の満了を迎える、サーバ、ネットワーク機器及びPCの更改を検討している。

〔社内システムの概要〕

G社の社内システムの構成を図1に示す。



L2SW：レイヤ2スイッチ L3SW：レイヤ3スイッチ FW：ファイアウォール NW：ネットワーク

⊕：リンクアグリゲーションを用いて接続している回線

注記1 199.alpha.beta.0/26は、グローバルIPアドレスを示す。

注記2 PC収容サブネット1のIPアドレスブロックは172.17.101.0/24、VLAN IDは101である。

注記3 PC収容サブネット2のIPアドレスブロックは172.17.102.0/24、VLAN IDは102である。

注記4 PC収容サブネット3のIPアドレスブロックは172.17.103.0/24、VLAN IDは103である。

注記5 L2SW3～L2SW20は、PC収容サブネット1～PC収容サブネット3を構成している。

図1 G社の社内システムの構成（抜粋）

G社の社内システムの概要は、次のとおりである。

- ・外部 DNS サーバは、DMZ のドメインに関するゾーンファイルを管理する権威サーバであり、インターネットから受信する名前解決要求に応答する。
- ・内部 DNS サーバは、社内システムのドメインに関するゾーンファイルを管理する権威サーバであり、PC 及びサーバから送信された名前解決要求に応答する。
- ・内部 DNS サーバは、DNS であり、PC 及びサーバから送信された社外のドメインに関する名前解決要求を、ISP が提供するフルサービスリゾルバに転送する。
- ・全てのサーバに二つの NIC を実装し、アクティブ/スタンバイのチーミングを設定している。
- ・L3SW1 及び L3SW2 で VRRP を構成し、L3SW1 の を大きく設定して、マスタールータにしている。
- ・L3SW1 と L3SW2 間のポートを、VLAN10、VLAN11 及び VLAN101 ～ VLAN103 を通すトランクポートにしている。
- ・L2SW3 ～ L2SW20 と L3SW 間のポートを、VLAN101 ～ VLAN103 を通すトランクポートにしている。
- ・内部 NW のスイッチは、IEEE 802.1D で規定されている STP (Spanning Tree Protocol) を用いて、経路を冗長化している。
- ・内部 DNS サーバは DHCP サーバ機能をもち、PC に割り当てる IP アドレス、サブネットマスク、デフォルトゲートウェイの IP アドレス、及び①名前解決要求先の IP アドレスの情報を、PC に通知している。
- ・FW1 及び FW2 は、アクティブ/スタンバイのクラスタ構成である。
- ・FW1 及び FW2 に静的 NAT を設定し、インターネットから受信したパケットの宛先 IP アドレスを、公開 Web サーバ及び外部 DNS サーバのプライベート IP アドレスに変換している。
- ・FW1 及び FW2 に NAT を設定し、サーバ及び PC からインターネット向けに送信されるパケットの送信元 IP アドレス及び送信元ポート番号を、それぞれ変換している。

G社のサーバ及び PC の設定を表 1 に、G社のネットワーク機器に設定する静的経

路情報を表 2 に、それぞれ示す。

表 1 G 社のサーバ及び PC の設定（抜粋）

機器名	IP アドレスの 割当範囲	デフォルトゲートウェイ		所属 VLAN
		機器名	IP アドレス	
公開 Web サーバ	172.16.254.10 ~ 172.16.254.100	FW1, FW2	172.16.254.1 ¹⁾	なし
外部 DNS サーバ				
ディレクトリサーバ	172.17.11.10 ~ 172.17.11.100	L3SW1, L3SW2	172.17.11.1 ²⁾	11
内部 DNS サーバ				
PC	172.17.101.10 ~ 172.17.101.254	L3SW1, L3SW2	172.17.101.1 ²⁾	101
	172.17.102.10 ~ 172.17.102.254	L3SW1, L3SW2	172.17.102.1 ²⁾	102
	172.17.103.10 ~ 172.17.103.254	L3SW1, L3SW2	172.17.103.1 ²⁾	103

注¹⁾ FW1 と FW2 が共有する仮想 IP アドレスである。

注²⁾ L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

表 2 G 社のネットワーク機器に設定する静的経路情報（抜粋）

機器名	宛先ネットワーク アドレス	サブネットマスク	ネクストホップ	
			機器名	IP アドレス
FW1, FW2	172.17.11.0	255.255.255.0	L3SW1, L3SW2	172.17.10.4 ¹⁾
	172.17.101.0	255.255.255.0	L3SW1, L3SW2	172.17.10.4 ¹⁾
	172.17.102.0	255.255.255.0	L3SW1, L3SW2	172.17.10.4 ¹⁾
	172.17.103.0	255.255.255.0	L3SW1, L3SW2	172.17.10.4 ¹⁾
	0.0.0.0	0.0.0.0	ルータ 1	199.α.β.1
L3SW1, L3SW2	0.0.0.0	0.0.0.0	FW1, FW2	172.17.10.1 ²⁾

注¹⁾ L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

注²⁾ FW1 と FW2 が共有する仮想 IP アドレスである。

情報システム部の J 主任が社内システムの更改と移行を担当することになった。更改と移行に当たって、上司である M 課長から指示された内容は、次のとおりである。

- (1) 内部 NW を見直して、障害発生時の業務への影響の更なる低減を図ること
- (2) 業務への影響を極力少なくした移行計画を立案すること

〔現行の内部 NW 調査〕

J 主任は、まず、現行の内部 NW の設計について再確認した。内部 NW のスイッチは、一つのツリー型トポロジを STP によって構成し、全ての VLAN のループを防止している。② L3SW1 に最も小さいブリッジプライオリティ値を、L3SW2 に 2 番目に

小さいブリッジプライオリティ値を設定し、L3SW1 をルートブリッジにしている。

ルートブリッジに選出された L3SW1 は、STP によって構成されるツリー型トポロジの最上位のスイッチである。L3SW1 はパスコストを 0 に設定した BPDU (Bridge Protocol Data Unit) を、接続先機器に送信する。BPDU を受信した L3SW2 及び L2SW3 ~ L2SW20 (以下、L3SW2 及び L2SW3 ~ L2SW20 を非ルートブリッジという) は、設定されたパスコストを加算した BPDU を、受信したポート以外のポートから送信する。非ルートブリッジの L3SW 及び L2SW の全てのポートのパスコストに、同じ値を設定している。

STP を設定したスイッチは、各ポートに、ルートポート、指定ポート及び非指定ポートのいずれかの役割を決定する。ルートブリッジである L3SW1 では、全てのポートが ポートとなる。非ルートブリッジでは、パスコストやブリッジプライオリティ値に基づきポートの役割を決定する。例えば、L2SW3 において、L3SW2 に接続するポートは、 ポートである。

STP のネットワークでトポロジの変更が必要になると、スイッチはポートの状態遷移を開始し、 テーブルをクリアする。

ポートをフォワーディングの状態にするときの、スイッチが行うポートの状態遷移は、次のとおりである。

- (1) リスニングの状態に遷移させる。
- (2) 転送遅延に設定した待ち時間が経過したら、ラーニングの状態に遷移させる。
- (3) 転送遅延に設定した待ち時間が経過したら、フォワーディングの状態に遷移させる。

J 主任は、内部 NW の STP を用いているネットワークに障害が発生したときの復旧を早くするために、IEEE 802.1D-2004 で規定されている RSTP (Rapid Spanning Tree Protocol) を用いる方式と、スイッチのスタック機能を用いる方式を検討することにした。

[RSTP を用いる方式]

J 主任は、トポロジの再構成に掛かる時間を短縮したプロトコルである RSTP について調査した。RSTP では、STP の非指定ポートの代わりに、代替ポートとバックア

アップポートの二つの役割が追加されている。RSTP で追加されたポートの役割を、表 3 に示す。

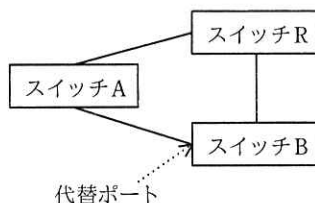
表 3 RSTP で追加されたポートの役割

役割	説明
代替ポート	通常、ディスカーディングの状態であり、ルートポートのダウンを検知したら、すぐにルートポートになり、フォワーディングの状態になるポート
バックアップポート	通常、ディスカーディングの状態であり、指定ポートのダウンを検知したら、すぐに指定ポートになり、フォワーディングの状態になるポート

注記 ディスカーディングの状態は、MAC アドレスを学習せず、フレームを破棄する。

RSTP では、プロポーザルフラグをセットした BPDU（以下、プロポーザルという）及びアグリーメントフラグをセットした BPDU（以下、アグリーメントという）を使って、ポートの役割決定と状態遷移を行う。

調査のために、J 主任が作成した RSTP のネットワーク図を図 2 に示す。



注記 1 全てのスイッチに RSTP を用いる。

注記 2 スイッチ R がルートブリッジである。

図 2 J 主任が作成した RSTP のネットワーク図

スイッチ A において、スイッチ R に接続するポートのダウンを検知したときに、スイッチ A とスイッチ B が行うポートの状態遷移は、次のとおりである。

- (1) スイッチ A は、トポロジチェンジフラグをセットした BPDU をスイッチ B に送信する。
- (2) スイッチ B は、スイッチ A にプロポーザルを送信する。
- (3) スイッチ A は、受信したプロポーザル内のブリッジプライオリティ値やパスコストと、自身もつブリッジプライオリティ値やパスコストを比較する。比較結果から、スイッチ A は、スイッチ B が RSTP によって構成されるトポロジにおいて f であると判定し、スイッチ B にアグリーメントを送信し、指定ポー

トをルートポートにする。

- (4) アグリーメントを受信したスイッチ B は、代替ポートを指定ポートとして、フォワーディングの状態に遷移させる。

J 主任は、調査結果から、STP を RSTP に変更することで、③内部 NW に障害が発生したときの、トポロジの再構成に掛かる時間を短縮できることを確認した。

[スイッチのスタック機能を用いる方式]

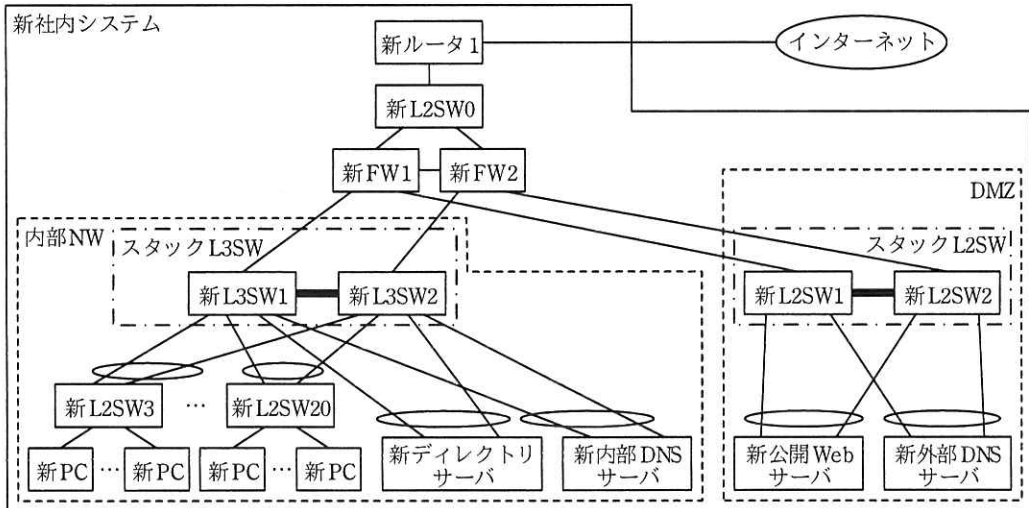
次に、J 主任は、ベンダから紹介された、新たな機器が実装するスタック機能を用いる方式を検討した。新たな機器を用いた社内システム（以下、新社内システムという）の内部 NW に関して、J 主任が検討した内容は次のとおりである。

- ・新 L3SW1 と新 L3SW2 をスタック用ケーブルで接続し、1 台の論理スイッチ（以下、スタック L3SW という）として動作させる。
- ・スタック L3SW と新 L2SW3～新 L2SW20 の間を、リンクアグリゲーションを用いて接続する。
- ・新ディレクトリサーバ及び新内部 DNS サーバに実装される二つの NIC に、アクティブ/アクティブのチーミングを設定し、スタック L3SW に接続する。

検討の内容を基に、J 主任は、スタック機能を用いることで、障害発生時の復旧を早く行えるだけでなく、④スイッチの情報収集や構成管理などの維持管理に係る運用負荷の軽減や、⑤回線帯域の有効利用を期待できると考えた。

[新社内システムの構成設計]

J 主任は、スイッチのスタック機能を用いる方式を採用し、STP 及び RSTP を用いない構成にすることにした。J 主任が設計した新社内システムの構成を、図 3 に示す。



: スタック用ケーブル : リンクアグリゲーションを用いて接続する回線
 注記 スタック L2SW は、新 L2SW1 と新 L2SW2 をスタック用ケーブルで接続した 1 台の論理スイッチである。

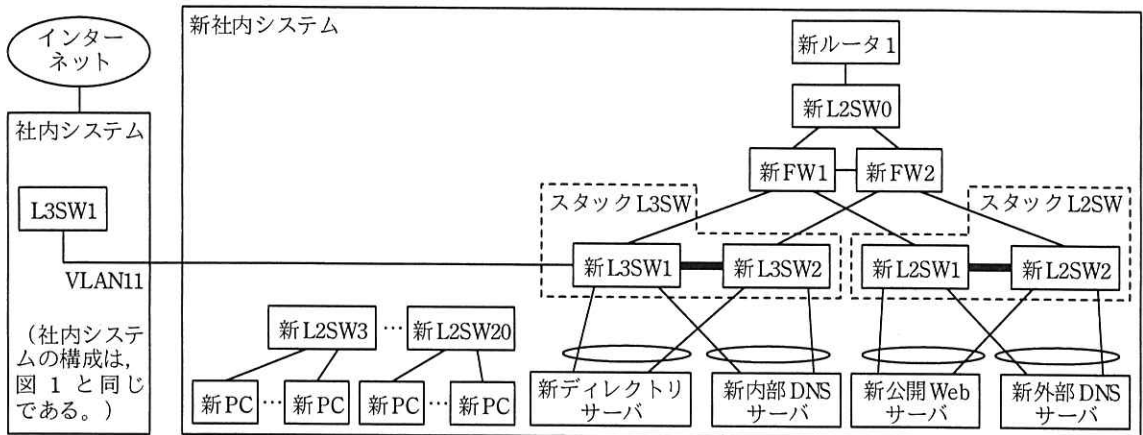
図 3 新社内システムの構成（抜粋）

〔新社内システムへの移行の検討〕

J 主任は、現行の社内システムから新社内システムへの移行に当たって、五つの作業ステップを設けることにした。移行における作業ステップを表 4 に、ステップ 1 完了時のネットワーク構成を図 4 に示す。ステップ 1 では、現行の社内システムと新社内システムの共存環境を構築する。

表 4 移行における作業ステップ（抜粋）

作業ステップ	作業期間	説明
ステップ 1	1 か月	・ 図 4 中の新社内システムを構築し、現行の社内システムと接続する。
ステップ 2	1 か月	・ ⑥現行のディレクトリサーバから新ディレクトリサーバへデータを移行する。 ・ ⑦現行の社内システムに接続された PC から、新公開 Web サーバの動作確認を行う。
ステップ 3	1 日	・ 現行の社内システムから、新社内システムに切り替える。(表 8 参照)
ステップ 4	1 か月	・ 新社内システムの安定稼働を確認し、新サーバに不具合が見つかった場合には、速やかに現行のサーバに切り戻す。
ステップ 5	1 日	・ 現行の社内システムを切り離す。



⊕ : リンクアグリゲーションを用いて接続する回線

注記1 新L2SW3～新L2SW20と新L3SW1, 新L3SW2間は接続されていない。

注記2 スタックL3SWには, VLAN101～VLAN103に関する設定を行わない。

図4 ステップ1完了時のネットワーク構成(抜粋)

ステップ1完了時のネットワーク構成の概要は、次のとおりである。

- ・新ディレクトリサーバ及び新内部DNSサーバに、172.17.11.0/24のIPアドレスブロックから未使用のIPアドレスを割り当てる。
- ・⑧新公開Webサーバ及び新外部DNSサーバには、172.16.254.0/24のIPアドレスブロックから未使用のIPアドレスを割り当てる。
- ・現行のL3SW1と新L3SW1間を接続し、接続ポートをVLAN11のアクセスポートにする。
- ・スタックL3SWのVLAN11のVLANインタフェースに、未使用のIPアドレスである172.17.11.101を、一時的に割り当てる。
- ・全ての新サーバについて、デフォルトゲートウェイのIPアドレスは、現行のサーバと同じIPアドレスにする。
- ・新社内システムのインターネット接続用サブネットには、現行の社内システムと同じグローバルIPアドレスを使うので、新外部DNSサーバのゾーンファイルに、現行の外部DNSサーバと同じゾーン情報を登録する。
- ・現行の内部DNSサーバ及び新内部DNSサーバのゾーンファイルに、新サーバに関するゾーン情報を登録する。
- ・新FW1及び新FW2は、アクティブ/スタンバイのクラスタ構成にする。

- ・新 FW1 及び新 FW2 には、インターネットから受信したパケットの宛先 IP アドレスを、新公開 Web サーバ及び新外部 DNS サーバのプライベート IP アドレスに変換する静的 NAT を設定する。
- ・新 FW1 及び新 FW2 に NAPT を設定する。
- ・新サーバの設定を表 5 に、新 FW 及びスタック L3SW に設定する静的経路情報を表 6 に、FW 及び L3SW に追加する静的経路情報を表 7 に示す。

表 5 新サーバの設定 (抜粋)

機器名	IP アドレスの 割当範囲	デフォルトゲートウェイ		所属 VLAN
		機器名	IP アドレス	
新公開 Web サーバ	(設問のため省略)	新 FW1, 新 FW2	172.16.254.1 ¹⁾	なし
新外部 DNS サーバ				
新ディレクトリサーバ	(省略)	L3SW1, L3SW2	172.17.11.1 ²⁾	11
新内部 DNS サーバ				

注¹⁾ 新 FW1 と新 FW2 が共有する仮想 IP アドレスである。

注²⁾ L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

表 6 新 FW 及びスタック L3SW に設定する静的経路情報 (抜粋)

機器名	宛先ネットワーク アドレス	サブネットマスク	ネクストホップ	
			機器名	IP アドレス
新 FW1, 新 FW2	172.17.11.0	255.255.255.0	スタック L3SW	172.17.10.4
	172.17.101.0	255.255.255.0	スタック L3SW	172.17.10.4
	172.17.102.0	255.255.255.0	スタック L3SW	172.17.10.4
	172.17.103.0	255.255.255.0	スタック L3SW	172.17.10.4
	0.0.0.0	0.0.0.0	スタック L3SW	172.17.10.4
スタック L3SW	172.16.254.128	255.255.255.128	新 FW1, 新 FW2	172.17.10.1 ¹⁾
	0.0.0.0	0.0.0.0	L3SW1, L3SW2	172.17.11.1 ²⁾

注¹⁾ 新 FW1 と新 FW2 が共有する仮想 IP アドレスである。

注²⁾ L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

表 7 FW 及び L3SW に追加する静的経路情報 (抜粋)

機器名	宛先ネットワーク アドレス	サブネットマスク	ネクストホップ	
			機器名	IP アドレス
FW1, FW2	172.16.254.128	255.255.255.128	L3SW1, L3SW2	172.17.10.4 ¹⁾
L3SW1, L3SW2	172.16.254.128	255.255.255.128	スタック L3SW	172.17.11.101

注¹⁾ L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

次に、J 主任は、ステップ 3 の現行の社内システムから新社内システムへの切替作業について検討した。J 主任が作成したステップ 3 の作業手順を、表 8 に示す。

表 8 ステップ 3 の作業手順（抜粋）

作業名	手順
インターネット接続回線の切替作業	・ 現行のルータ 1 に接続されているインターネット接続回線を、新ルータ 1 に接続する。
DMZ のネットワーク構成変更作業	<ul style="list-style-type: none"> ・ 新 FW1 及び新 FW2 に設定されているデフォルトルートのネクストホップを、新ルータ 1 の IP アドレスに変更する。 ・ ⑨現行の FW1 と L2SW1 間、及び現行の FW2 と L2SW2 間を接続している LAN ケーブルを抜く。 ・ ⑩ステップ 4 で、新サーバに不具合が見つかったときの切戻しに掛かる作業量を減らすために、現行の L2SW1 と新 L2SW1 間を接続する。 ・ ⑪インターネットから新公開 Web サーバに接続できることを確認する。
内部 NW のネットワーク構成変更作業	<ul style="list-style-type: none"> ・ 現行の L3SW1 及び L3SW2 の VLAN インタフェースに設定されている全ての IP アドレス、並びに静的経路情報を削除する。 ・ スタック L3SW の VLAN11 の VLAN インタフェースに設定されている IP アドレスを、<input type="text" value="g"/> に変更する。 ・ スタック L3SW に設定されているデフォルトルートのネクストホップを新 FW1 と新 FW2 が共有する仮想 IP アドレスに変更する。 ・ スタック L3SW に設定されている宛先ネットワークアドレスが 172.16.254.128/25 の静的経路情報を削除する。
ディレクトリサーバの切替作業	・ 新ディレクトリサーバをマスタとして稼働させる。
DHCP サーバの切替作業	<ul style="list-style-type: none"> ・ 現行の内部 DNS サーバの DHCP サーバ機能を停止する。 ・ 新内部 DNS サーバの DHCP サーバ機能を開始する。 ・ ⑫スタック L3SW に DHCP リレーエージェントを設定する。
新 PC の接続作業	<ul style="list-style-type: none"> ・ スタック L3SW に、VLAN101～VLAN103 の VLAN インタフェースを作成し、IP アドレスを設定する。 ・ 新 L2SW3～新 L2SW20 と新 L3SW1、新 L3SW2 に、VLAN101～VLAN103 を通すトランクポートを設定し、接続する。 ・ 新 PC から新ディレクトリサーバに接続できることを確認する。

J 主任が作成した移行計画は M 課長に承認され、J 主任は更改の準備に着手した。

設問 1 〔社内システムの概要〕について、(1)、(2)に答えよ。

(1) 本文中の , に入れる適切な字句を答えよ。

(2) 本文中の下線①の名前解決要求先を、図 1 中の機器名で答えよ。

設問 2 〔現行の内部 NW 調査〕について、(1)、(2)に答えよ。

(1) 本文中の下線②の設定を行わず、内部 NW の L2SW 及び L3SW に同じブリッジプライオリティ値を設定した場合に、L2SW 及び L3SW はブリッジ ID の何を比較してルートブリッジを決定するか。適切な字句を答えよ。また、L2SW3 がルートブリッジに選出された場合に、L3SW1 と L3SW2 が VRRP の情報を交換できなくなるサブネットを、図 1 中のサブネット名を用いて全て答えよ。

(2) 本文中の ～ に入れる適切な字句を答えよ。

設問 3 [RSTP を用いる方式] について、(1), (2) に答えよ。

(1) 本文中の に入れる適切な字句を答えよ。

(2) 本文中の下線③について、トポロジの再構成に掛かる時間を短縮できる理由を二つ挙げ、それぞれ 30 字以内で述べよ。

設問 4 [スイッチのスタック機能を用いる方式] について、(1), (2) に答えよ。

(1) 本文中の下線④について、運用負荷を軽減できる理由を、30 字以内で述べよ。

(2) 本文中の下線⑤について、内部 NW で、スタック L3SW～新 L2SW 以外に回線帯域を有効利用できるようになる区間が二つある。二つの区間のうち一つの区間を、図 3 中の字句を用いて答えよ。

設問 5 図 3 の構成について、STP 及び RSTP を不要にしている技術を二つ答えよ。

また、STP 及び RSTP が不要になる理由を、15 字以内で述べよ。

設問 6 [新社内システムへの移行の検討] について、(1)～(8) に答えよ。

(1) 表 4 中の下線⑥によって発生する現行のディレクトリサーバから新ディレクトリサーバ宛での通信について、現行の L3SW1 とスタック L3SW 間を流れるイーサネットフレームをキャプチャしたときに確認できる送信元 MAC アドレス及び宛先 MAC アドレスをもつ機器をそれぞれ答えよ。

(2) 表 4 中の下線⑦によって発生する現行の PC から新公開 Web サーバ宛での通信について、現行の L3SW1 とスタック L3SW 間を流れるイーサネットフレームをキャプチャしたときに確認できる送信元 MAC アドレス及び宛先 MAC アドレスをもつ機器をそれぞれ答えよ。

(3) 本文中の下線⑧について、新公開 Web サーバに割り当てることができる IP アドレスの範囲を、表 1 及び表 5～7 の設定内容を踏まえて答えよ。

- (4) 表 8 中の下線⑨を行わないときに発生する問題を、30 字以内で述べよ。
- (5) 表 8 中の下線⑩の作業後に、新公開 Web サーバに不具合が見つかり、現行の公開 Web サーバに切り替えるときには、新 FW1 及び新 FW2 の設定を変更する。変更内容を、70 字以内で述べよ。また、インターネットから現行の公開 Web サーバに接続するときには経由する機器名を、【転送経路】の表記法に従い、経由する順に全て列挙せよ。

【転送経路】

インターネット →

経由する順に全て列挙

 → 公開 Web サーバ

- (6) 表 8 中の下線⑪によって発生する通信について、新 FW の通信ログで確認できる通信を二つ答えよ。ここで、新公開 Web サーバに接続するための IP アドレスは、接続元が利用するフルサービスリゾルバのキャッシュに記録されていないものとする。
- (7) 表 8 中の

g

 に入れる適切な IP アドレスを答えよ。
- (8) 表 8 中の下線⑫について、スタック L3SW は、PC から受信した DHCPDISCOVER メッセージの giaddr フィールドに、受信したインタフェースの IP アドレスを設定して、新内部 DNS サーバに転送する。DHCP サーバ機能を提供している新内部 DNS サーバは、giaddr フィールドの値を何のために使用するか。60 字以内で述べよ。