

目次

まえがき

第1部 ネットワークスペシャリスト試験の出題ポイント

- 第1章 出題傾向分析 8
- 第2章 学習方法 17
- 第3章 本書の使い方 20

第2部 午前II（専門知識）試験の対策ポイント 23

第3部 午後問題の重点対策

- 第1章 午後試験に対する取組み方 36
 - 1.1 試験問題への対応方法 36
 - 1.2 答案の作成方法 39
 - 1.3 答案作成の具体例 40
 - 1.4 午後II試験問題の解き方 63
- 第2章 LANの方式 86
 - 2.1 伝送媒体とアクセス制御方式 86
 - 2.2 無線LAN (IEEE 802.11) 90
 - 2.3 ADSLとFTTH 98
 - 2.4 PPPとPPPoE 101
- 第3章 IPとTCP/UDP 140
 - 3.1 IPアドレスとルーティングテーブル 140
 - 3.2 アドレス変換 150
 - 3.3 IPマルチキャスト 154
 - 3.4 DHCP 157
 - 3.5 VRRP 159
 - 3.6 IPv6 162
 - 3.7 TCPとUDP 165

■ 第 4 章	アプリケーションプロトコル	232
4.1	HTTP とクッキー情報	232
4.2	FTP	239
4.3	SNMP	242
4.4	NTP	245
■ 第 5 章	DNS の仕組み	261
■ 第 6 章	電子メールの仕組み	288
■ 第 7 章	VoIP	318
■ 第 8 章	ネットワーク機器	359
8.1	ブリッジとルータ	359
8.2	ルーティングプロトコル	363
8.3	LAN スイッチ	371
8.4	NAS と SAN	385
8.5	IP-VPN と広域イーサネット	388
■ 第 9 章	ネットワークセキュリティ	470
9.1	暗号化技術	470
9.2	認証技術	472
9.3	ファイアウォールと IDS	480
9.4	IPsec	487
9.5	SSL/TLS	494
9.6	その他のセキュリティプロトコル	499
■ 第 10 章	ネットワークの設計・運用	568
10.1	ネットワークの設計構築	568
10.2	ネットワークの運用管理	574
索引		616

商標表示

各社の登録商標及び商標、製品名に対しては、特に注記のない場合でも、これを十分に尊重いたします。

第1章

出題傾向分析

ネットワークスペシャリスト試験は、午前Ⅰ（共通知識）、午前Ⅱ（専門知識）、午後Ⅰ、午後Ⅱという四つの試験が実施されます。このため、ネットワークスペシャリストの資格を取得するには、すべての試験で合格基準点をクリアすることが必要です。

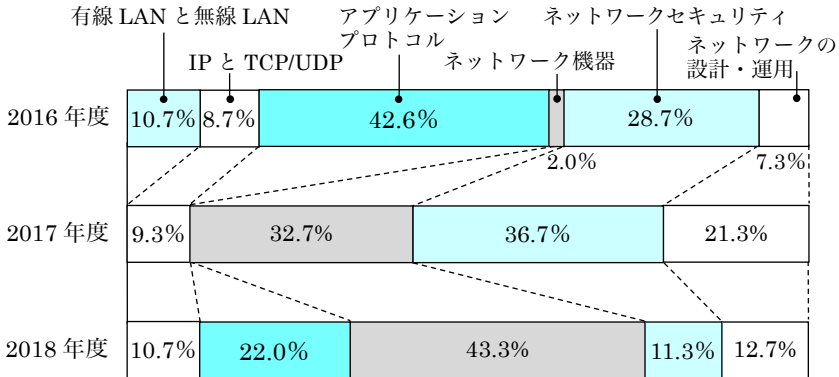
(1) 午前の試験

午前の試験は、午前Ⅰ（共通知識）、午前Ⅱ（専門知識）という二つの試験が実施されます。ここでは、その注意点などを述べることにします。

午前Ⅰ試験は、各高度試験に共通した試験で、出題数は30問、試験時間は50分です。そして、合格基準点は満点の60%（18問の正解）です。出題分野は、テクノロジー系（基礎理論、コンピュータシステム、技術要素、開発技術）、マネジメント系（プロジェクトマネジメント、サービスマネジメント）、ストラテジ系（システム戦略、経営戦略、企業と法務）の全分野にわたります。

表 1-1 午前Ⅰ試験 分野別出題数

分野	大分類	2017年度 秋期	2018年度 春期	2018年度 秋期
テクノロジー系 (17問)	基礎理論	3	3	4
	コンピュータシステム	4	4	3
	技術要素	8	8	8
	開発技術	2	2	2
マネジメント系 (5問)	プロジェクトマネジメント	2	1	2
	サービスマネジメント	3	4	3
ストラテジ系 (8問)	システム戦略	2	3	3
	経営戦略	4	3	3
	企業と法務	2	2	2
合計		30	30	30



分野	技術内容
有線LANと無線LAN	CSMA/CD, MAC フレーム, CSMA/CA, WEP, TKIP, CCMP, WPA, WPA2, WPA3, 無線LANの高速化技術など
IPとTCP/UDP	IPアドレス, CIDR, ルーティングテーブル, アドレス変換, ICMP (ping 試験の方法など), IP マルチキャスト, IGMP, PIM, DHCP, VRRP, TCP, UDP など
アプリケーションプロトコル	HTTP, クッキー, プロキシサーバ, 負荷分散方法, DNSの仕組み (キャッシュ, DNSサーバの信頼性対策, DNSリフレクタ攻撃, DNSSECなど), 電子メール配送の仕組み, 電子メールのセキュリティ (SMTP-AUTH, SPF, DKIM, DMARC, S/MIMEなど), 迷惑メール対策, VoIP (SIP, RTP, 優先制御など), SNMP, NTP など
ネットワーク機器	LANスイッチ (スイッチングハブ) の機能・動作, 仮想スイッチ, 仮想NIC, スパニングツリー, VLAN, VXLAN, ルータの機能・動作, ルーティングプロトコル (RIP, OSPF, BGP-4), TRILL, NAS, FC-SAN, IP-SAN, FCoE, ネットワーク仮想化, SDN (オーバーレイ方式, ホップバイホップ方式, OpenFlow) など
ネットワークセキュリティ	暗号化技術, 認証技術 (デジタル署名, ワンタイムパスワード, 時刻認証, メッセージ認証など), 電子証明書の検証方法, ファイアウォールの設定, IDS, IPS, WAF, IPsec, SSL/TLS, VPN, IEEE 802.1X/EAP, RADIUS など
ネットワークの設計・運用	ネットワークにおけるボトルネックやバックアップの考え方, ネットワーク構成法, 必要帯域 (回線速度) の検討, トラフィック計算, データ転送量, 移行方式の検討, 故障切分け, 保守運用のノウハウなど

注 出題比率は、設問ごとに配点を予想し、集計したものを総配点で割って求めたもの。また、技術区分は上記の表に従って分類した。

図 1-1 午後 I 問題の技術分野別出題比率



要点チェック

Check

- 問題の出題形式
- IP アドレス問題
- 回線速度、データ転送時間などの計算方法
- ビット誤り率に関する計算方法
- PCM 符号化速度に関する計算方法
- トラフィック量 (アーラン) の計算方法
- ADSL の理論的な通信速度の計算方法
- 音声パケットの大きさの計算方法



要点解説

Study

1. 問題の出題形式

(1) 午前II試験の出題形式は、四肢選択式ですが、内容的には次の三つのパターンに分けることができます。

- ① 適切な用語を選択する問題
- ② 適切な記述を選択する問題
- ③ IP アドレスや計算問題

(2) 適切な用語を選択する問題については、用語の意味を知らなければ、基本的に正解を得ることは難しいと思います。しかし、正解する確率をできるだけ高くするように努力していくことは可能です。

例えば、四つの選択肢の中から適当に選べば、正解する確率は25%です。しかし、四つの選択肢の中には、各自が知っている用語も含まれているはずですから、関係ない用語については消し込んでいくようにしましょう。二つ消し込むことができれば、正解する確率は50%にアップします。午前II試験の出題範囲は、ネットワーク技術、セキュリティ技術のほか、コンピュータシステムと開発技術分野からも出題されます。コンピュータシステムと開発技術分野の問題に適用すれば有効であると考えられます。

(3) 適切な記述を選択する問題は、それぞれの選択肢の内容をよく確認しましょう。記述内容の前半部分は正しい内容である半面、後半部分が間違っている場合などがあります。また、記述内容を速攻で読んでいくと、思い違いをしたり



演習問題

Exercise

問1 IPv6 が利用できるネットワークに接続した PC において、二つの IPv6 アドレスが割り当てられていた。

(H26 秋 NW 午前II問1)

(1) 2001:db8::b083:ba94:60c7:7c36

(2) fe80::200:c0ff:fea8:2

このうち、(2)はリンクローカルユニキャストアドレスである。この説明として適切なものはどれか。

ア 下位のビットにこの PC の IPv4 アドレスを埋め込み、IPv6 アドレスと IPv4 アドレスを関連付けて管理を容易にするアドレスである。

イ グローバルユニキャストアドレスが取得できなかったときだけに有効なアドレスである。

ウ このアドレスを使った場合、パケットはネットワークには送信されず、自分自身の PC 内で動作しているプログラムとだけ通信できる。

エ このアドレスをもつネットワークインタフェースからルータを介さずに直接接続できる相手との通信にだけ使用できるアドレスである。

【解説】

この問題は、適切な記述を選択する問題の例ですが、(1)、(2)の二つの IPv6 アドレスが記載されています。このため、この二つを同時に考えてしまいがちですが、この問題では(2)のリンクローカルユニキャストアドレスの説明として適切なものが問われていますので、(2)に限定して考えていきましょう。

リンクローカルユニキャストアドレスは、同一リンク内の通信、つまり、ルータを介さずに直接接続できる相手との通信に限って使用できるものです。したがって、正解は (エ) です。

なお、(1)の 2001:db8::b083:ba94:60c7:7c36 は、IPv6 グローバルユニキャストアドレスを示しますが、これは 2001:db8::/32 というプレフィックスをもつことから、文書記述用の IPv6 アドレス、つまり、設定のサンプル用として用いられています (このアドレスを実際の通信に用いることはできません)。ちなみに、2001:db8::/32 というプレフィックスの使用方法は、RFC 3849 (IPv6 Address Prefix Reserved for Document) で規定されています。

午後試験に対する取り組み方

1.1 試験問題への対応方法

ネットワークスペシャリスト試験で合格するには、午前Ⅰ、午前Ⅱ試験で合格基準点をクリアした上で、さらに午後Ⅰ、午後Ⅱ試験とも 60 点以上の点数を確保することが必要です。

午前Ⅰ、午前Ⅱの試験は、四肢択一の選択問題ですから、ある程度の技術知識があれば比較的容易にクリアできます。しかし、午後の試験は、数十字で解答する記述式の問題が大半を占めるので、午後Ⅰ、午後Ⅱの試験で合格基準点をクリアすることは並大抵のことではありません。TCP/IP や仮想化技術、ネットワークセキュリティなどをはじめ、ネットワーク関連の詳細な技術知識を十分に身に付けた上で、しかも、問題の記述内容を正しく把握して、設問で問われていることに合致した答案を作成していくことなどが要求されます。こうした作業をうまく行うには、幾つかのポイントがあります。

ここでは、午後試験の問題に取り組むときの注意点などを紹介することにします。

(1) 決してあせらない

ネットワークに関する基本的な技術知識をしっかりと身に付けて試験に臨めば、午後試験においても合格基準点をクリアすることは、それほど難しいというわけではありません。そこで、どのような問題が出題されても落ち着いて問題に取り組んでいくようにしましょう。また、記述式の問題は、思うように得点できないので、少し気楽に考えることも必要です。

午後Ⅰ、午後Ⅱ試験は、午前試験と違って過去問題と同じ問題は出題されません。このため、問題にさっと目を通すと、どれも難しそうな問題ばかりに見えます。しかし、この時点であせってしまうと、冷静に問題に取り組むことができなくなります。午後Ⅰ試験は 3 問の中から 2 問を、午後Ⅱ試験は 2 問の中から 1 問を選択すればよいので、得意分野の問題を選択するようにしましょう。そして、落ち着いて問題に取り組んでいけば、徐々に正解を思いついたり、正解を導いた

問 ネットワーク監視の改善に関する次の記述を読んで、設問1, 2に答えよ。

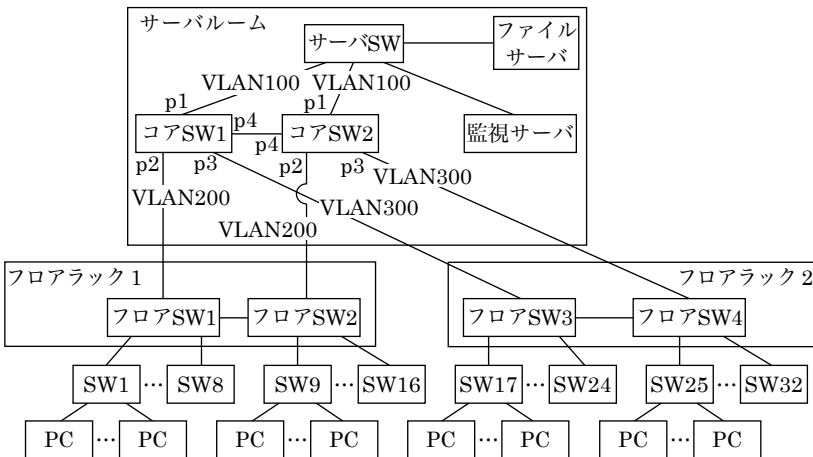
A社は従業員数200人の流通業者である。A社のシステム部門では、統合監視サーバ（以下、監視サーバという）を構築し、A社のサーバやLANの運用監視を行っている。

監視サーバは、pingによる死活監視（以下、ping監視という）とSYSLOGによる異常検知監視（以下、SYSLOG監視という）を行っている。現在定義されているLANに関するSYSLOG監視は、ポートのリンク状態遷移、STP（Spanning Tree Protocol）状態遷移及びVRRP（Virtual Router Redundancy Protocol）状態遷移の3種類である。

ある日、“従業員が使用するPCからファイルサーバを利用できない”という苦情が、システム部門に多数寄せられた。調査した結果、ケーブルの断線による障害と判明して対処したが、監視サーバで検知できなかったことが問題視された。

〔A社LANの概要〕

A社は、オフィスビルの1フロアを利用している。A社LANの構成を、図1に示す。



SW：スイッチ

注記1 コアSW1, コアSW2は、レイヤ3スイッチである。

注記2 フロアSW1～フロアSW4, サーバSW, SW1～SW32は、レイヤ2スイッチである。

注記3 p1～p4は、スイッチのポートを示す。

注記4 VLAN100, VLAN200, VLAN300は、スイッチのアクセスポートのVLAN IDを示す。

図1 A社LANの構成 (抜粋)

題に対応できると考えた。

SNMP のインフォームでは、MIB に変化が起きた際に、SNMP エージェントが直ちにメッセージを送信し、SNMP マネージャからの確認応答を待つ。確認応答を受信できない場合、SNMP エージェントは、SNMP マネージャがメッセージを受信しなかったと判断し、メッセージの再送信を行う。Cさんは、③今回と同様なネットワークの異常が発生した場合に備えて、SNMP マネージャがインフォームの受信を行えるよう、SNMP エージェントの設定パラメタを考えた。

その後、CさんはSNMPのインフォームを用いたネットワーク監視の改善策をB課長に報告し、その内容が承認された。

設問1 [障害発生時の状況確認] の下線①について、フロア SW1 が送信した SYSLOG メッセージが監視サーバに到達できなかったのはなぜか。“スパンニングツリー”の字句を用いて25字以内で述べよ。

設問2 [ネットワーク監視の改善策の立案] について、(1)、(2)に答えよ。

- (1) 本文中の下線②について、ポーリングとトラップの問題を、それぞれ35字以内で述べよ。
- (2) 本文中の下線③について、SNMP エージェントが満たすべき動作の内容を、40字以内で述べよ。

この問題を読んで、次のような箇所にアンダーラインが引かれていると、問題の読み方としては、よいでしょう。

- ・ 現在定義されている LAN に関する SYSLOG 監視は、ポートのリンク状態遷移、STP (Spanning Tree Protocol) 状態遷移及び VRRP (Virtual Router Redundancy Protocol) 状態遷移の3種類である
- ・ コア SW1 はループ構成の一つである。IEEE 802.1D で規定されている STP を用いて、レイヤ2ネットワークのループを防止している。正常時はコア SW1 がルートブリッジとなるように設定している
- ・ リンクダウンなどの異常が発生した機器は、監視サーバに対して直ちに SYSLOG メッセージを送信する
- ・ ケーブル1の断線によって、フロア SW2 の p1 ポートの STP のポート状態がブロッキングから、リスニング、ラーニングを経て、フォワーディングに遷移した。また、監視サーバでは、SYSLOG 監視によって、ケーブル1が接続されているポートのリンク状態遷移が発生したことを検知した

す。SNMPは通信の効率性を重視していますので、トランスポート層プロトコルにUDPを使用しています。[監視サーバの概要と問題]に「SYSLOGは、トランスポートプロトコルとしてRFC 768で規定されているUDPを用いている」と記述されていますので、少なくともこの記述に気付けば問題ないでしょう。

このように、SNMPはトランスポート層プロトコルにUDPを使用します。UDPは、パケットを効率的にやり取りすることができる半面、パケットの到達を確認する手順がないため、SNMP エージェントから SNMP マネージャへ送信したメッセージが通信途中で失われると、そのままになってしまい、メッセージを回復させる手段がありません。したがって、トラップの問題としては、「到達確認がないのでメッセージが失われる可能性がある」旨の解答を導くことができます。

トラップの問題点について、図 1-1 に示したような、解答作成のステップ例をまとめると、図 1-2 のようになります。

(1) 設問内容の確認

・トラップを使用して監視しても、今回発生したネットワークの異常においては問題があることの原因



(2) 問題の記述箇所

・トラップは、MIB に変化が起きた際に、SNMP エージェントが直ちにメッセージを送信し、SNMP マネージャがメッセージを受信することによって、機器の状態を取得できる



(3) 必要な技術知識

・SNMP は、トランスポート層プロトコルに UDP を使用する
 ・UDP の特徴は、効率良く通信できるが、メッセージの送達確認機能をもたない



(4) 解答案の作成

・トラップは到達確認がないのでメッセージが失われる可能性がある

設問内容を満たす解答であるかどうかを確認することがポイント

図 1-2 記述式問題に対する解答作成のステップ例 (2)

(c) 設問 2 (2)

この設問は、「下線③について、SNMP エージェントが満たすべき動作の内容を、40 字以内で述べる」ものです。なお、下線③は「今回と同様なネットワークの異常が発生した場合に備えて、SNMP マネージャがインフォームの受信を行えるよう、SNMP エージェントの設定パラメタを考えた」です。

第3章

IP と TCP/UDP

3.1 IP アドレスとルーティングテーブル



要点チェック

Check

- IP アドレスの種類とその意味
- CIDR による IP アドレスの表示方法とその特徴
- IP アドレスとサブネットマスク、デフォルトゲートウェイの関係
- ルーティングテーブルの検索方法
- IP アドレスと MAC アドレスの関係
- ARP の仕組み
- モバイル IP



要点解説

Study

1. IP アドレスの種類とその意味

- (1) IP アドレスについては、32 ビット長の IPv4 と、128 ビット長の IPv6 の二つがあります。これまでのネットワーク試験の午後問題では、IPv4 に関する問題しか出題されていませんでした。しかし、初めて平成 24 年度の午後Ⅱ問 2 の一部として出題されたので、IPv6 についても、理解を深めていくようにしましょう。
- (2) IPv4 のアドレス空間は、図 3-1 のように定義されていて、クラス A～E という分類がされています。クラス A～C については、クラスという概念を外した CIDR (Classless Inter-Domain Routing) という割当て方式が主流になります。なお、クラス D はマルチキャスト用のアドレスです。
- 一方、IPv6 のアドレスは、ユニキャストアドレス (この中には、リンクローカルアドレス、グローバルアドレス、ユニークローカルアドレスがあります)、エニーキャストアドレス、マルチキャストアドレスという 3 種類が定義されて

- (4) 途中で NAT 対応ルータが存在するとき、接続の張り方はどのようになるのでしょうか。NAT 対応ルータは、内部のネットワークからインターネット側に出ていくときには、送信元 IP アドレスを NAT 対応ルータが持つグローバル IP アドレスに書き換えるだけなので、接続の終端にはなりません。つまり、TCP 接続は PC と Web サーバ間に張られます。

4. UDP の特徴

- (1) UDP は、TCP とは異なり、接続の確立のほか、ウィンドウ制御や再送制御などを行いません。このため、UDP のヘッダ情報には、送信元ポート番号 (16 ビット)、宛先ポート番号 (16 ビット)、メッセージ長 (16 ビット)、チェックサム (16 ビット) という四つのフィールドしかありません。
- (2) UDP のデータ長 (UDP ヘッダも含む) は、IP パケットのフラグメントが発生しないように、通常、512 バイトに制限されています。



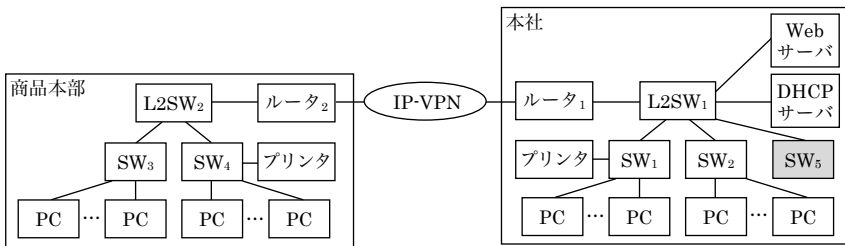
演習問題

Exercise

問1 端末の管理強化に関する次の記述を読んで、設問1～3に答えよ。

(H25 秋 NW 午後1問2)

Z社は、生活雑貨の企画、製造及び販売を行う企業である。本社は東京にあり、商品の製造と配送を行う商品本部が山梨にある。ネットワーク管理は、本社の情報管理課が行っている。Z社の現在のネットワーク構成を、図1に示す。



L2SW：レイヤ2スイッチ

SW：アクセス用レイヤ2スイッチ

注記 SW₅は、増設予定のSWである。

図1 Z社の現在のネットワーク構成(抜粋)

設問1 本文中の ～ に入れる適切な字句を答えよ。

ア	<input type="text"/>	イ	<input type="text"/>
ウ	<input type="text"/>	エ	<input type="text"/>
オ	<input type="text"/>		

設問2 [IPアドレス割当ての仕組みと経緯] について、(1)～(3)に答えよ。

(1) 本文中の に入れる適切な数値を答えよ。

a	<input type="text"/>
---	----------------------

(2) 本文中の下線①では、何が起きたことで通信に障害が発生したのか。15字以内で答えよ。

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

(3) 本文中の下線②では、BBルータのポートのうち、SWに接続したポートは何を接続すべきポートであったのか。15字以内で答えよ。

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

設問3 [端末の管理強化策の立案と確認] について、(1)～(4)に答えよ。

(1) 本文中の , に入れる適切な数値を答えよ。

b	<input type="text"/>	c	<input type="text"/>
---	----------------------	---	----------------------

(2) O主任がU君に指示した、固定IPアドレスの割当て及び暫定運用中の対処に必要なDHCPサーバの機能を、それぞれ30字以内で述べよ。

固定IPアドレス の割当て	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

暫定運用中の 対処	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
--------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

(3) 作業3の動作確認中に起きた障害の原因となった機器の動作を、図1中の機器名を用いて、35字以内で述べよ。

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

(4) O主任が本文中の下線③で実現しようとしているネットワーク構成を、“VLAN”という字句を用いて、40字以内で述べよ。

た」、「L2SW₁に設定の誤りがあり、DHCP スヌーピング機能が動作していません」と記述されています。

これらの内容を基に考察していきましょう。まず、DHCP サーバから PC2 向けの DHCPOFFER 及び DHCPACK がブロードキャストされると、本社の L2SW₁ から SW₁ 及び SW₂ に対してもブロードキャストされます。そして、L2SW₁ から SW₁ にブロードキャストされると、PC2 は SW₁ に接続されているので折り返し転送されることはありませんが、SW₂ に送られたブロードキャストフレームは、SW の不具合のために L2SW₁ に折り返し転送されます。しかも、L2SW₁ では DHCP スヌーピング機能が動作していないので、L2SW₁ は、DHCP サーバの接続ポート以外から受信した DHCPOFFER 及び DHCPACK でも、それを破棄することなく、そのまま SW₁ に DHCPOFFER 及び DHCPACK をブロードキャストしてしまいます (図 A 参照)。この結果、DHCP サーバから PC2 に対し、DHCPOFFER 及び DHCPACK が 2 度送られるので、正規のメッセージ数よりも多い 6 メッセージがトラフィックモニタの結果、観測されることになります。したがって、空欄 c には“6”が入ります。

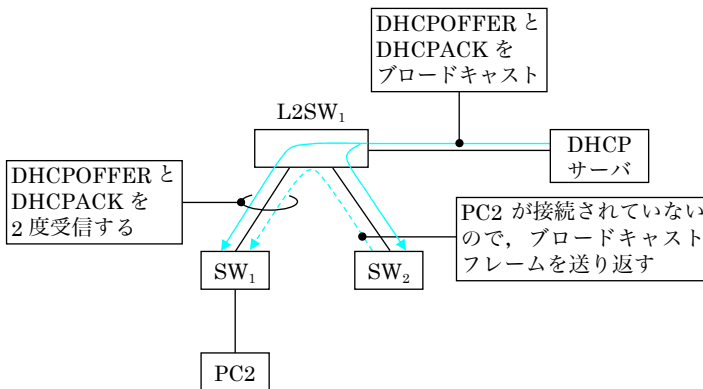


図 A SW₂がブロードキャストフレームを折り返すときの状況

なお、DHCP スヌーピングとは、レイヤ 2 スイッチ (L2SW) がもつ機能の一つで、L2SW のポートに DHCP パケットが流れているかどうかを監視する機能のことです。このため、L2SW₁ で DHCP スヌーピング機能を動作させれば、L2SW₁ は、DHCP サーバを接続したポート以外から送られてくる DHCPOFFER 及び DHCPACK を破棄することができます。

(2) この設問は、固定 IP アドレスの割当て及び暫定運用中の対処に必要な DHCP

解答例

- [設問1] ア：リレーエージェント イ：ARP ウ：製造者
エ：ミラー オ：DHCPDISCOVER
- [設問2] (1) a：5
(2) IPアドレスの重複割当て
(3) PCを接続すべきポート
- [設問3] (1) b：24 c：6
(2) 固定IPアドレスの割当て：MACアドレスに対応付けたIPアドレスを割り当てる。
暫定運用中の対処：MACアドレスが未登録でもIPアドレスを割り当てる。
(3) SW₁とSW₂の間でのブロードキャストフレームの折り返し
(4) SW単位にVLANを設定し、VLAN間経路制御とDHCPリレーを行う構成

問2 ネットワークシステムの再構築に関する次の記述を読んで、設問1～3に答えよ。

(H24秋NW午後II問2改)

A社は、従業員300名のコンピュータ関連製品の販売会社で、営業所が2か所ある。主に販売店経由で製品を販売しているが、一部の製品については、エンドユーザーに直接販売している。A社では、販売店向けの販売店支援システムとエンドユーザー向けのインターネット販売システムを、Webサーバで稼働させている。

本社では、販売、購買、会計などの業務処理を支援する業務システムのサーバ（以下、業務サーバという）を、4台運用している。A社の現在のネットワークシステム構成を、図1に示す。



索引

数字

3ウェイハンドシェイク	165
4B/5B 変換	87
6to4	164
8B/10B 変換	87

A

A レコード	263
AAAA レコード	263
ABR	364
ACE	267
ACK ビット	480
ADSL	98
AH	488
anonymous FTP	239
ARP	146
ARP キャッシュ	145
ARP テーブル	145
AS	361
ASBR	365
AS_PATH 属性	367
AS 境界ルータ	365
AS パスプリペンド	368
Automatic MDI/MDI-X	89

B

B2BUA	322
BGP-4	366
BGP スピーカ	366
BPDU	378
BSS	93
BSSID	94

C

CA	476
CA 証明書	476
CBC	497
CCK	90
CCMP	96
CE ルータ	389
CHAP	102
CIDR	140
CIFS	385
Cookie	236
CoS	326
CRL	477
CSMA/CA	91
CSMA/CD	88

D

DATA	289
DHCP	157
DHCP スヌーピング	373
DHCP リレーエージェント	158, 361
Diffie-Hellman	487
dig	575
DKIM	296
DMARC	298
DNS	261
DNS amplification 攻撃	269
DNSSEC	270
DNS キャッシュポイズニング攻撃	269
DNS サーバ	262
DNS ラウンドロビン	267, 570
DNS リフレクタ攻撃	269
DoS 攻撃	166
DS	325
DSL	98