

問題

問 1

正解

完璧



直前
CHECK

BGP-4 における AS に関する記述として、適切なものはどれか。

- ア あるルータが作成した Router-LSA が伝播^{はば}するルータの集合である。
- イ 接続されるルータの数、ブロードキャストやマルチキャストの使用の有無、トポロジ種別などによって分けられたネットワーク群であり、Hello プロトコルによって隣接関係を確立する。
- ウ 同一の管理ポリシーによって管理されるネットワーク群であり、2 オクテット又は 4 オクテットの AS 番号によって識別される。
- エ リンクステート型の共通のプロトコルを使用して、ルーティング情報を相互に交換するルータの集合である。

問 2

正解

完璧



直前
CHECK

高速無線通信で使われている多重化方式であり、データ信号を複数のサブキャリアに分割し、各サブキャリアが互いに干渉しないように配置する方式はどれか。

- ア CCK イ CDM ウ OFDM エ TDM

問 3

正解

完璧



直前
CHECK

CS-ACELP (G.729) による 8k ビット/秒の音声符号化を行う VoIP ゲートウェイ装置において、パケットを生成する周期が 20 ミリ秒のとき、1 パケットに含まれる音声ペイロードは何バイトか。

- ア 20 イ 160 ウ 200 エ 1,000

**問 1****ウ**

BGP-4 (Border Gateway Protocol version 4) : 大規模なネットワークの経路制御に利用されるプロトコル。主にプロバイダ間の経路制御に用いられる。**AS** (Autonomous System) は、BGP で制御する各ネットワークの単位を示す。

ア : Router-LSA (Link-State Advertise) とは、ルータが自身のつながっているネットワークの経路の状態をネットワーク上の近くのルータに知らせることである。知らせる範囲は、つながっているネットワーク全体である。

**問 2****ウ**

CCK (Complementary Code Keying) : 無線 LAN で採用されている変調方式。ビット列のデータと電波を対応付けて変調する。

CDM (Code Division Multiplexing) : 符号分割多重。拡散符号を各情報に乗じることにより、一つの回線を共有して使うことができる。

OFDM (Orthogonal Frequency Division Multiplexing) : 直交波周波数分割多重と訳される。複数の通信の周波数を分け、直交性を利用して搬送波をオーバーラップしながら多重化して通信する方式。

TDM (Time Division Multiplexing) : 時間分割多重。複数の通信が回線を共用する際に、時間で区切って順番に回線の利用権を割り当てる方式。

**問 3****ア**

解答の単位がバイトであるので、8k ビット/秒を 1k バイト/秒として計算する。

パケットを生成する周期が 20 ミリ秒であるから、1 秒 / 20 ミリ秒 = 50 回となるから、パケットを 1 秒あたりに 50 回生成することとなる。1 秒あたり 1k バイトのペイロードとなるため、1k バイト / 50 回 = 20 バイトが 1 パケットあたりの音声ペイロードとなる。

8k ビット/秒と指定されている数値が 1 秒あたりのペイロードを示すところが本問のポイントとなる。

問題

問 4

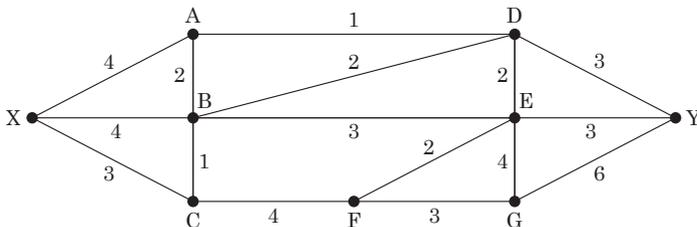
正解

完璧



直前
CHECK

図のネットワークで、数字は二つの地点間で同時に使用できる論理回線の多重度を示している。X 地点から Y 地点までには同時に最大幾つの論理回線を使用することができるか。



ア 8

イ 9

ウ 10

エ 11

問 5

正解

完璧



直前
CHECK

ADSL の上りの伝送速度が下りよりも遅くなっていることの説明として、適切なものはどれか。

- ア ISDN との干渉を防止するためである。
- イ 加入者宅の ADSL モデムとその対向先である ADSL 集合モデムとの間を流れる ATM セル仕様で制限されているからである。
- ウ 通信事業者やインターネットサービスプロバイダ側でセキュリティチェックを行うからである。
- エ 上りの変調周波数帯域が、下りの変調周波数帯域と比べて狭いからである。

問 6

正解

完璧



直前
CHECK

CSMA 方式の LAN 制御に関する記述として、適切なものはどれか。

- ア キャリア信号を検出し、データの送信を制御する。
- イ 送信権をもつメッセージ（トークン）を得た端末がデータを送信する。
- ウ データ送信中に衝突が起こった場合は、直ちに再送を行う。
- エ 伝送路が使用中でもデータの送信はできる。



問 4

ウ

多重度の最大値とは、各経路の最小回線数を求めれば良い。

経路	論理回線数
X-(A, B, C)	$4+4+3=11$
(A, B, C)-(D, E, F)	$1+2+3+4=10$
(A, B, F)-(D, E, G)	$1+2+3+2+3=11$
(D, E, G)-Y	$3+3+6=12$

表より、最小回線数は 10 となる。



問 5

エ

ADSL (Asymmetric Digital Subscriber Line) は、アナログ電話回線を使用して高速なデータ通信を行うサービスである。上りと下りでは速度に差があり、下りのほうが高速である。これは、一方の通信帯域を削り、もう一方にその分の帯域を割り当てているからである。

パソコンと ADSL 回線を接続するためには ADSL モデムが必要となる。音声信号と ADSL 用通信の信号は、ADSL モデム内にあるスプリッタと呼ばれる機器で分離される。スプリッタはモデムと分離されている場合もある。



問 6

ア

CSMA (Carrier Sense Multiple Access) は搬送波感知多重アクセスと訳される。ユーザがパケットを送出する際、LAN 上のキャリア信号を検出することにより回線の空き状況を調べてから送出手続きを実行する方式である。

イ：トークンパッシングに関する説明である。

ウ：衝突が発生した場合、CSMA 方式では送信を中断し、一定時間が経過した後、改めて LAN 上のキャリア信号検出を行う。

エ：伝送路にキャリア信号が検出された場合、送信を中断し、一定時間が経過した後、改めて LAN 上のキャリア信号検出を行う。

問題

問 7

正解

完璧

直前
CHECK

IP ネットワークのルーティングプロトコルの一つである OSPF の説明として、適切なものはどれか。

- ア 自律システム間の接続に使用され、経路が変化したときだけ、その差分を送信する。
- イ 自律システム内で使用され、距離ベクトルとリンクステートの両アルゴリズムを採用したルーティングプロトコルである。
- ウ ネットワークを、エリアと呼ぶ単位に分割し、エリア間をバックボーンで結ぶ形態を採り、回線速度などを考慮した最小コストルーティングのプロトコルである。
- エ ホップ数に基づいて最短経路を動的に決定する。サブネット情報を通知できないので、大規模のネットワークには不向きである。

問 8

正解

完璧

直前
CHECK

ハミング符号の用途の説明として、適切なものはどれか。

- ア Bluetooth 通信で、ビット誤りを訂正するために使われている。
- イ G3 ファクシミリで画像データの圧縮に使われている。
- ウ HDLC フレーム内のビット誤りを検出するために使われている。
- エ MP3 でオーディオデータの圧縮に使われている。

問 9

正解

完璧

直前
CHECK

DNS の A レコードに関する記述のうち、適切なものはどれか。

- ア ゾーン内の登録データの開始マークである。
- イ ドメイン名とメールサーバの対応を示すものである。
- ウ ホスト名から IP アドレスへの対応を示すものである。
- エ ホスト名に別名を付けるためのものである。

**問 7****ウ**

OSPF (Open Shortest Path First) は、ネットワークをエリアと呼ぶ単位に分割し、経路選択 (ルーティング) するプロトコルである。一般的にルータに設定し、複数のルーティング情報を自動的に更新する。隣接するルータの状態のほか、サブネットマスクを参照して隣接ルータとやり取りする情報を少なくしている。

ア: BGP (Border Gateway Protocol) の説明である。

イ: EIGRP (Enhanced Interior Gateway Routing Protocol) の説明である。

エ: RIP (Routing Information Protocol) の説明である。

**問 8****ア**

Bluetooth では、ランダム誤りの訂正にハミング符号を採用している。

イ: G3 ファクシミリでの画像の圧縮は、MH (Modified Huffman) または MR (Modified READ) 符号化が用いられる。

ウ: HDLC フレーム内のビット誤り検出には、FCS (Frame Check Sequence) が用いられる。

エ: MP3 の圧縮にはハフマン符号化が用いられる。

**問 9****ウ**

DNS の A レコードとは、ドメイン名 (ホスト名) から IP アドレスを問い合わせるためのものである。

ア: SOA レコードの説明である。

イ: MX レコードの説明である。

エ: CNAME レコードの説明である。

問題

問 10

正解

完璧



直前
CHECK

IPv4 における ICMP のメッセージに関する説明として、適切なものはどれか。

- ア 送信元が設定したソースルーティングが失敗した場合は、Echo Reply を返す。
- イ 転送されてきたデータグラムを受信したルータが、そのネットワークの最適なルータを送信元に通知して経路の変更を要請するには、Redirect を使用する。
- ウ フラグメントの再組立て中にタイムアウトが発生した場合は、データグラムを破棄して Parameter Problem を返す。
- エ ルータでメッセージを転送する際に、受信側のバッファがあふれた場合には Time Exceeded を送り、送信ホストに送信を抑制することを促す。

問 11

正解

完璧



直前
CHECK

マルチキャストグループへの参加や離脱をホストが通知したり、マルチキャストグループに参加しているホストの有無をルータがチェックするとき使用するプロトコルはどれか。

- ア ARP
- イ IGMP
- ウ LDAP
- エ RIP

問 12

正解

完璧



直前
CHECK

図は IPv4 における IPsec のデータ形式を示している。ESP トンネルモードの電文中で、暗号化されているのはどの部分か。

新 IP ヘッダ	ESP ヘッダ	オリジナル IP ヘッダ	TCP ヘッダ	データ	ESP トレーラ	ESP 認証データ
-------------	------------	-----------------	------------	-----	-------------	--------------

- ア ESP ヘッダから ESP トレーラまで
- イ TCP ヘッダから ESP 認証データまで
- ウ オリジナル IP ヘッダから ESP トレーラまで
- エ 新 IP ヘッダから ESP 認証データまで



問 10

イ

- ア：ソースルーティングが失敗したときは **Destination Unreachable** メッセージを返す。
イ：経路変更要請のメッセージは **Redirect** で正しい。
ウ：フラグメント再構成が時間切れとなった場合は、**Time Exceeded** メッセージを返す。



問 11

イ

ARP (Address Resolution Protocol)：IP アドレスからイーサネットアドレス (MAC アドレス) を得るプロトコルである。

IGMP (Internet Group Management Protocol)：マルチキャストにおいて、ホストのグループ制御に利用されるプロトコル。

RIP (Routing Information Protocol)：パケットが到達する経路の最小ルートを選択するダイナミックルーティングプロトコルである。ルータを1台経由するごとに1ホップだけカウントアップする。最大数は15ホップ。16ホップ目でパケットは破棄される。RIPはホップ数のみをカウントしているため、経路中の回線速度(コスト)や遅延、均一化は考慮されない。



問 12

ウ

ESP トンネルモードは、ネットワーク間でオリジナルパケット (オリジナル IP ヘッダからデータまで) を暗号化して送信する際に使用される。

データの暗号化では、暗号化されるデータが暗号アルゴリズムのビット長の倍数となる必要があるため、オリジナルパケットにパディングデータ (**ESP トレーラ**) を加えて、調整してから暗号化の処理を行う。そのため、暗号化されているのはオリジナル IP ヘッダから ESP トレーラまでである。

問題

問 13

正解

完璧



直前
CHECK

IPv4 と IPv6 の両方にある機能はどれか。

- ア 実時間処理用のパケットを処理するためのフローラベル
- イ パケットヘッダの誤りを検出するためのチェックサム
- ウ 一つのパケットで複数のノードにデータを配送するマルチキャスト
- エ 複数のノードのうち経路上最も近いノードにデータを配送するエニーキャスト

問 14

正解

完璧



直前
CHECK

2 台の PC を IPv6 ネットワークに接続するとき、2 台ともプレフィックスが 2001:db8:100:1000::/56 の IPv6 サブネットに入るようになる IP アドレスの組合せはどれか。

	1 台目の PC	2 台目の PC
ア	2001:db8:100::aa:bb	2001:db8:100::cc:dd
イ	2001:db8:100:1000:aa:bb	2001:db8:100:2000::cc:dd
ウ	2001:db8:100:1010:aa:bb	2001:db8:100:1020::cc:dd
エ	2001:db8:100:1100:aa:bb	2001:db8:100:1200::cc:dd

**問 13****ウ**

ア：IPv6 の機能である。

イ：IPv4 の機能である。

ウ：マルチキャスト機能は IPv4 と IPv6 の両方にある。

エ：IPv6 の機能である。エニーキャストとは、ネットワーク上で近くのあるノードにデータを配送する機能である。

▼
解答**問 14****ウ**

IPv6 の IP アドレス長は 128 ビットとなっている。表記方法は、16 ビット単位に「: (コロン)」で区切る形である。RFC5952 では、表記ルールの 0 の省略方法を示している。本問もそのルールに従って省略されている点を読み取る必要がある。

① 16 ビットの「:」区切りの先頭にある 0 は省略する

例 2001:0db8:0100 = 2001:db8:100

② 0000 が連続する場合は「::」を使用して可能な限り省略する。

③ 0000 が 1 箇所しかない場合「::」使用して省略してはならない。

④ 「::」を使用して省略可能な箇所が複数ある場合は、最も多くの 0 を省略できる箇所を省略する。ただし、省略できる 0 の数が複数の個所で同じ場合は、先の 0 を省略する。

本問には「/56」という表記があるから、左側の先頭から 56 ビットがサブネットワークとなる。

設問の「2001:db8:100:1000::/56」の 56 ビット分を省略しない形に変換すると、以下のようになる。

省略前	2001:0db8:0100:10
-----	-------------------

アとイの PC は、省略前の部分が一致する場合に同一サブネットとなる組合せといえる。したがって、ウが同一サブネットとなる組合せである。

問題

問 15

正解

完璧



直前
CHECK

MPLS の説明として、適切なものはどれか。

- ア IP プロトコルに暗号化や認証などのセキュリティ機能を付加するための規格である。
- イ L2F と PPTP を統合して改良したデータリンク層のトンネリングプロトコルである。
- ウ PPP データフレームを IP パケットでカプセル化して、インターネットを通過させるためのトンネリングプロトコルである。
- エ ラベルと呼ばれる識別子を挿入することによって、IP アドレスに依存しないルーティングを実現する、ラベルスイッチング方式を用いたパケット転送技術である。

問 16

正解

完璧



直前
CHECK

IPv4 アドレスが 192.168.10.0/24 ~ 192.168.58.0/24 のネットワークを対象に経路を集約するとき、集約した経路のネットワークアドレスのビット数が最も多くなるものはどれか。

- ア 192.168.0.0/16 イ 192.168.0.0/17
- ウ 192.168.0.0/18 エ 192.168.0.0/19

問 17

正解

完璧



直前
CHECK

HTTP の認証機能を利用するクライアント側の処理として、適切なものはどれか。

- ア ダイジェスト認証では、利用者 ID とパスワードを “:” で連結したものを、MD5 を使ってエンコードし Authorization ヘッダで指定する。
- イ ダイジェスト認証では、利用者 ID とパスワードを “:” で連結したものを、SHA を使ってエンコードし Authorization ヘッダで指定する。
- ウ ベーシック認証では、利用者 ID とパスワードを “:” で連結したものを、BASE64 でエンコードし Authorization ヘッダで指定する。
- エ ベーシック認証では、利用者 ID とパスワードを “:” で連結したものを、エンコードせずに Authorization ヘッダで指定する。

**問 15****エ**

MPLS (Multi Protocol Label Switching) : 主に WAN で使用される L3 スイッチングである。ルーティング情報にラベルを付けることでルーティングを高速化する技術である。

ア : IPsec に関する記述である。

イ : L2TP (Layer 2 Tunneling Protocol) に関する記述である。

ウ : PPTP (Point to Point Tunneling Protocol) に関する記述である。

**問 16****ウ**

設問内のサブネットがすべて包括されている範囲でかつ最少のものが解答となる。

		サブネット	ホスト部
①	192.168.10.0/24	11000000.10101000.00001010	00000000
②	192.168.58.0/24	11000000.10101000.00111010	00000000
ア	192.168.0.0/16	11000000.10101000	00000000.00000000
イ	192.168.0.0/17	11000000.10101000.0	00000000.00000000
ウ	192.168.0.0/18	11000000.10101000.00	00000000.00000000
エ	192.168.0.0/19	11000000.10101000.000	00000000.00000000

①, ②は、左から 18 ビットまでが同一である。すべてを包括するには 18 ビット以内でア, イ, ウとなり、その中でもホスト部のけた数が最少のウが正解となる。

**問 17****ウ**

HTTP のダイジェスト認証 : ユーザ名とパスワードを利用したランダムな文字列を MD5 でエンコードして、サーバで認証する仕組みである。

HTTP のベーシック認証 : 利用者 ID とパスワードを BASE64 でエンコードして、サーバへ送信し、認証する仕組みである。

ア : ユーザ ID とパスワードをそのまま MD5 でエンコードするのではない。

イ : SHA は利用しない。

エ : 何もエンコードしないのは誤りである。

問題

問 18

正解

完璧



直前
CHECK

HTTP を使って、Web サーバのコンテンツのアップロードや更新を可能にするプロトコルはどれか。

ア CSS

イ MIME

ウ SSL

エ WebDAV

問 19

正解

完璧



直前
CHECK

CRL (Certificate Revocation List) はどれか。

ア 有効期限切れになったデジタル証明書の公開鍵のリスト

イ 有効期限切れになったデジタル証明書のシリアル番号のリスト

ウ 有効期限内に失効したデジタル証明書の公開鍵のリスト

エ 有効期限内に失効したデジタル証明書のシリアル番号のリスト



問 18

I

CSS (Cascading Style Sheets) : HTML や XML はファイルの論理構造を記述するものであるが, CSS はその見栄えを記述し, 指示するものである. 論理構造と CSS の記述を対応させておけば, CSS を変更することで複数の HTML ファイルや XML ファイルの表示を変更することができる.

MIME (Multipurpose Internet Mail Extension) : テキスト以外のデータ (画像, 音声, バイナリデータなど) を電子メールで送信するための規格.

SSL (Secure Socket Layer) : インターネット上で情報を暗号化して送受信するためのプロトコル. データの盗聴や改ざん, なりすましを防ぐことができる. 公開鍵暗号方式やデジタル証明書など, いくつかのセキュリティ技術を組み合わせて実現している.

WebDAV (Web-based Distributed Authoring and Versioning) : Web サーバ上のファイルやフォルダを, HTTP を介して管理するための仕様. サーバ上のファイルやフォルダの一覧を表示したり, 複製・更新・削除などが可能となる.



問 19

I

CRL (Certificate Revocation List) : 失効したデジタル証明書のリスト. CA (Certificate Authority) によって管理されている. 退職者や異動者, 誤って発行されたものなど, 有効期間内に使われなくなったデジタル証明書の一覧. デジタル証明書の受信者は, 証明書が有効かどうかを CRL を参照して確認する.

問題

問 20

正解

完璧



直前
CHECK

チャレンジレスポンス認証の方式として、適切なものはどれか。

- ア SSL によって、クライアント側で固定パスワードを暗号化して送信する。
- イ クライアント側で端末のシリアル番号を秘密鍵を使って暗号化して送信する。
- ウ トークンという装置が表示する毎回異なったデータを、パスワードとして送信する。
- エ 利用者が入力したパスワードと、サーバから送られたランダムなデータとをクライアント側で演算し、その結果を送信する。

問 21

正解

完璧



直前
CHECK

無線 LAN のセキュリティ対策に関する記述のうち、適切なものはどれか。

- ア EAP は、クライアント PC とアクセスポイントとの間で、あらかじめ登録した共通鍵による暗号化通信を実現できる。
- イ RADIUS では、クライアント PC とアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実現できる。
- ウ SSID は、クライアント PC ごとの秘密鍵を定めたものであり、公開鍵暗号方式による暗号化通信を実現できる。
- エ WPA2 では、IEEE 802.1X の規格に沿った利用者認証及び動的に更新される暗号化鍵を用いた暗号化通信を実現できる。

問 22

正解

完璧



直前
CHECK

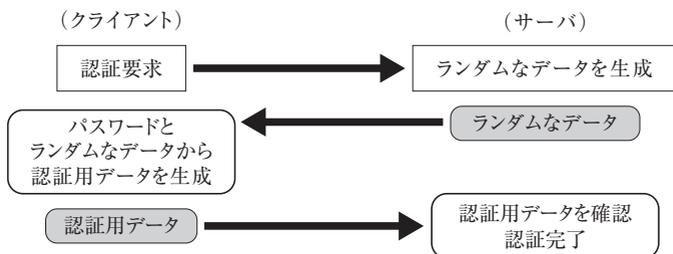
ストレージ技術におけるシン・プロビジョニングの説明として、適切なものはどれか。

- ア 同じデータを複数台のハードディスクに書き込み、冗長化する。
- イ 一つのハードディスクを、OS をインストールする領域とデータを保存する領域とに分割する。
- ウ ファイバチャネルなどを用いてストレージをネットワーク化する。
- エ 利用者の要求に対して仮想ボリュームを提供し、物理ディスクは実際の使用量に応じて割り当てる。

**問 20****工**

- ア：SSL で保護したベーシック認証の説明である。
- イ：ワンタイムパスワードの説明である。
- ウ：ハッシュ関数の説明である。
- エ：チャレンジレスポンス方式の説明である。

チャレンジレスポンスの図：

**問 21****工**

- ア：EAP (Extensible Authentication Protocol, 拡張認証プロトコル) は、認証プロトコルの一つ。様々な種類の拡張認証方式の手続きを記述したもの。
- イ：RADIUS (Remote Authentication Dial In User Service) は、ネットワーク上のサーバに認証機能を一元化して、様々なネットワーク資源を利用するための認証を実行するプロトコル。
- ウ：SSID (Service Set Identifier) は、無線 LAN 環境での混信を防ぐための識別子。最大 32 文字までの英数字で構成される。
- エ：WPA2 (Wi-Fi Protected Access 2)、無線 LAN の暗号化方式規格のひとつ。暗号化標準の AES に対応している。

**問 22****工**

シン・プロビジョニング (Thin Provisioning) とは、利用者へ割り当てるストレージ領域を仮想的に利用可能とすることで、実際に用意するストレージの物理要領を削減する技術である。

- ア：ミラーリングに関する記述である。
- イ：ディスクのパーティションに関する記述である。
- ウ：SAN (Storage Area Network) に関する記述である。



問 23

工

問題文より、 $r = 0.9$ のとき的高速化率 (E) を $r = 0.3$ のとき的高速化率の 3 倍となるように式を構成する。

$$\frac{1}{1 - 0.9 + \frac{0.9}{n}} = 3 \times \frac{1}{1 - 0.3 + \frac{0.3}{n}}$$

$$\frac{n}{0.1n + 0.9} = \frac{3n}{0.7n + 0.3}$$

$$0.7n + 0.3 = 0.3n + 2.7$$

$$n = 6$$

したがって、必要となるプロセッサの台数は 6 台である。



問 24

イ

決定表：ある事象についての条件や選択肢を表にして、事象の結果のとり得る組合せを表したもの。デシジョンテーブルともいう。

状態遷移図：システムの状態がどのように遷移するかを表した図。タスクの状態遷移図では、そのタスクが実行可能状態、実行状態、待ち状態となる様子を図示する。

データフローダイアグラム：システム間のデータの流れを示す図。データを発生・吸収・処理・蓄積するシステムの間を、データの流れを示す矢印で繋いで作成する。データの流れが明確になる。

特性要因図：ある課題について影響を及ぼす原因を系統立てて表した図。特性と要因の関係を線で結ぶと魚の骨のような形になることから、魚骨図とも呼ばれる。「QC7つ道具」の一つ。



問 25

イ

MDA (Model Driven Architecture)：モデル駆動型アーキテクチャ。プラットフォームに依存しないモデルを元にアーキテクチャを構成する手法。

OMT (Object Modeling Technique)：オブジェクト指向ソフトウェア開発技法の方法論のひとつ。

UML (Unified Modeling Language)：オブジェクトモデリングのための仕様記述言語。シーケンス図、クラス図、ユースケース図など 13 種類の図で表現する。