

【改正資料】

本書の内容につきまして試験制度変更に伴い、改正点が発生致しましたので以下の点につきまして情報の追加をお願い申し上げます。

『Network+ COMPLETE テキスト WAN 技術編』 (初版第1刷 ISBN4-8125-2217-X C3055 Y2800E DAI-X 出版)

P.41 最後に追加

インターネット接続回線

インターネットに接続するためのサービスにはさまざまな種類がありますが、今日のインターネットを支えている技術に既設の電話回線を使用する ISDN や ADSL、光ファイバを使用した FTTH などがあります。

ISDN

ISDN(Integrated Services Digital Network)は、電話、FAX、およびデータ通信を統合して扱うデジタル通信網です。伝送速度は 128kbps です。ISDN では、すべてのデータをデジタルデータとして扱います。デジタル通信のメリットとして、長距離データ通信が可能なが挙げられます。ISDN では、電話局と加入者間の距離に左右されずに一定の速度で通信ができますが、IDSL 国際規格では、電話局と加入者間の接続最大距離は 5.5km までと定められています。

最近では、さらに高速なサービスが登場したこともあり、ISDN は企業のバックアップ回線など一部の用途としてのみ使われることが多くなっています。

ADSL

既存の一般電話回線を使用して高速なデジタル通信を実現するサービスの総称として xDSL があります (P.38 参照)。xDSL では、電話で使用する周波数帯より高い周波数帯を使用するため、音声通話と同時にデータ通信を行うことができます。その中でもインターネット接続サービスとして最も普及しているのが ADSL です。ADSL は、電話局と加入者宅間で上りと下りのデータ通信速度が非対称なのが、特徴です。

現在では最大 50Mbps の伝送速度を実現したサービスもあります。

しかし、一般的に xDSL 等の高速通信においては、電話局からの距離が長くなるほど伝送損失は大きくなり、通信速度が低下していき、条件によっては通信ができなくなる場合もあります。このように、接続環境によって通信速度や回線の品質が変化するサービスを「ベストエフォート型サービス」といいます。ADSL の場合、電話局から加入者宅までの最大距離は 5.5km までといわれていますが、12Mbps や 50Mbps のように高周波数帯を使用するサービスほど最大距離は短くなります。一般的には 2km を超えると通信速度は一気に低下するといわれています。

FTTH

最近加入者数が増加しているサービスとして、FTTH (Fiber To The Home) があります。

FTTH では、伝送メディアに光ファイバを使用し、回線も一般電話回線とは別に敷設された回線網を利用します。FTTH では、最大伝送速度は 100Mbps と高速データ通信が可能になります。また、光ファイバの場合は、外部からのノイズや干渉を受けにくい性質を持つため長距離にわたる高速データ通信が可能になります。FTTH の最大のデメリットとして「コストが高い」といわれてきましたが、最近ではコストも下がり導入しやすくなったことを受けて加入者数が増加しています。

FTTH のサービスとしては、NTT 東西の「B フレッツ」などさまざまなサービスがあります。

P.61 Lesson06 最後に追加

リモートアクセスの認証

リモートアクセスの認証は、PPP(Point to Point Protocol)の中で実施されます。PPP の認証は、認証を要求する側を Peer(ピア)、Peer からユーザ名とパスワードを受け取り真正性を検査する側を Authenticator(認証者)とよびます。例えば、ダイヤルアップクライアントは Peer で、アクセスサーバが Authenticator です。

次の表は、主な PPP の認証のプロトコルです。

名 称	特 徴
PAP	Password Authentication Protocol ・ RFC 1334 で公開 ・ パスワードを暗号化せず回線上にクリアテキストで流す
CHAP	Challenge Handshake Authentication Protocol ・ RFC 1994 で公開 ・ パスワードを回線上に流さない ・ 乱数で生成される短いチャレンジを Authenticator から Peer に送信 ・ Peer はチャレンジとパスワードをハッシュ関数 (MD5) に与え得た値を返す ・ Authenticator も同じチャレンジと登録済みパスワードを MD5 に与える ・ Authenticator の計算と、Peer の応答を比較し真正性を検査する
MS-CHAP	Microsoft PPP CHAP Extensions ・ CHAP を Microsoft が拡張した独自認証 ・ ハッシュ関数に MD4 を使用 ・ 拡張機能 (RFC 2433 で公開) は、パスワードの変更、認証失敗時の再入力、PPTP でデータの暗号化に使用する慣用 (対称鍵) 暗号の秘密鍵の交換機能など
MS-CHAP v2	Microsoft PPP CHAP Extensions Version 2 ・ MS-CHAP のぜい弱性を改良 ・ 相互認証機能を追加
EAP	PPP Extensible Authentication Protocol ・ RFC 2284 で公開 ・ 認証方式が選択可能な枠組みを提供するプロトコル ・ 新しい認証プロトコル、ハードウェアを組み合わせた認証 (スマートカード認証など) を使用する際に利用

Windows におけるリモートアクセスの認証

Windows でリモートアクセス認証をする場合、PPP の認証方式として MS-CHAP を使用します。MS-CHAP は、通常の CHAP をさらに拡張し、よりセキュリティを強化した Microsoft 独自の認証方式です。

MS-CHAP では WindowsNT3.X や Windows95 で利用された LanManager 認証のサポートなど下位互換性を保っている反面、暗号化に MD4 という関数が使用され、一方向の認証しかできないなど、セキュリティ面で問題があります。

MS-CHAP での問題点を解決し、よりセキュリティを高めたものが MS-CHAPv2 です。MS-CHAPv2 では、暗号化に MD5 が使われ、認証も相互で行われるなど、さまざまな改良が加えられています。

Windows2000 からは、デフォルトで MS-CHAPv2 が使用されます。WindowsNT3.x や Windows95 では、VPN 接続以外は下位との互換性を保つため、MS-CHAP を使用します。そのため、WindowsNT3.x または、Windows95 が認証サーバとなっている場合は、正しく認証できない場合があります。

P.138 RADIUS 認証の後に追加

Kerberos(ケルベロス)とは、マサチューセッツ工科大学(MIT)と IBM、DEC の共同プロジェクト Athena(アテナまたはアテナ)の中で開発された認証プロトコルです。Microsoft では Windows2000 以降のサーバ OS で標準サポートしており、クライアントとサーバ間の認証に使用されています。また、Linux や MAC OS でもサポートされています。

Kerberos では、クライアントとサーバ間での認証に共通鍵暗号を使用するため、従来の公開鍵方式よりも高いセキュリティを実現できます。さらに通信する相手ごとにパスワードをその都度変えて使用する、セッション鍵という暗号方式を使用するため盗聴を防止することができます。

認証は、通常通信を行う両者間で行われますが、Kerberos では KDC(Key Distribution Center: 鍵配布センター)という認証サーバが認証を一括管理しています。一度 KDC に身元を保証してもらくと、それ以降はユーザがユーザ名・パスワードを入力しなくても目的のサーバにアクセスできる「シングルサインオン」を導入しています。

Kerberos に関するコンポーネントは、次のようなものがあります。

コンポーネント		説明
Kerberos サーバ (KDC)	KDC	KDC (Key Distribution Center) は、Kerberos 認証サーバです。AS と TGS の機能を持ちます。
	AS	AS (Authentication Server) は、Kerberos クライアントからの認証要求を受け付け、データベースを検索し認証を行います。
	TGS	TGS (Ticket Granting Server) は、Kerberos クライアントからのチケット要求を受け付け、チケットを配布します。
チケット	TGT	TGT (Ticket Granting Ticket) は、アクセスチケットを要求する際に、提示が必要となるチケットです。ユーザは、KDC に認証されると TGT を受け取り、アクセスチケットを要求する時に提示します。 TGT には、セッション鍵 (TGS とクライアント間) 認証データ、有効期間が入り、KDC の暗号鍵で暗号化されます。
	アクセス チケット	サーバ (リソース) にアクセスする際に必要となるチケットです。

Kerberos でのユーザ認証の動作

1. Kerberos 認証クライアントが、ユーザアカウント名とパスワードを KDC に送信します。
2. KDC は、Kerberos 認証クライアントから送られてきた情報を元に認証を行い、正しく認証が行われると、目的のリソースにアクセスするためのチケット(アクセスチケット)発行用のチケット(TGT)を発行します。
3. TGTを受け取ったクライアントは、実際にアクセスしたいサーバの情報をTGTと一緒に KDC に送信します。
4. KDC では、クライアントから送られてきたTGTの認証を行い、情報が正しければリソースへアクセスするためのアクセスチケットを発行します。
5. クライアントはアクセスチケットを使用してリソースにアクセスします。

Kerberos 認証の動作



P.221 VLAN とは の後

VLAN の利用目的

VLAN とは、物理的な LAN の配置に関係なく、仮想的に LAN を構築できる技術です。同一のスイッチに接続されたノードは、1つのブロードキャストドメインとなり、ブロードキャストドメイン内に存在するノード数が増加すると、輻輳の原因となります。そのため、通常ルータを用いてネットワークをセグメント化する方法がとられていますが、この場合物理的な配置の変更が必要になります。VLAN では、スイッチを使用しながら、物理的な配置は変えずに設定上でセグメントを自由に分割することが可能です。

例えば、同じスイッチに接続されたノードを2つのグループ (VLAN1、VLAN2) に分けます。VLAN1 と VLAN2 は物理的には1つのセグメントですが、論理的には2つのスイッチに分けられたこととなります。

VLAN は以下のような場合に有効です。

- ・ オフィスのレイアウトが頻繁に変更する
- ・ 1つのフロア内に複数の部署がある
- ・ 重要なデータやサーバがあり、アクセスを制限したい

VLAN で仕切られたノード間では、別々のネットワークとなるため輻輳を防止する他に、セキュリティの向上が図れます。

VLAN の設定はスイッチにログインして、PC 上から行うことができますが、VLAN 対応スイッチまたはレイヤ3スイッチが必要です。