=== ch02.docx

[chap]2章　ケーブルにもぐりこむ

有効なパケット解析の鍵となるのは、データを適切にキャプチャするのに、パケットスニッファをどこで使うかの決定です。パケットアナリストの間ではこのことをワイヤをスニッフする、ネットワークをタップする、あるいはワイヤをタップするなどと言います。簡単にいえば、ネットワーク上の適切な位置にパケットスニッファを配置するプロセスです。

残念ながらスニッフィングは、単純にノートPC をネットワークポートに接続してパケットをキャプチャすればよいというものではありません。実際には、パケットを解析するよりもスニッファをつなぐネットワーク上の位置を決めるほうが難しいこともあります。

なぜスニッファの配置が難しいかというと、ネットワーク機器の種類が非常に多いからです。図2-1がこの典型的な状況を示しています。ハブ、スイッチ、ルータといった、現代のネットワークで使われている3つの主なネットワーク機器は、それぞれがまったく違った形で通信を扱うため、解析するネットワークにスニッファを配置する際にはその点を十分考慮しなければなりません。

図2-1　スニッファを配置する位置を決めることが、もっとも難しいかもしれない

スニッファ

この章の目的は、さまざまなネットワークトポロジでのスニッファの配置方法を理解することです。しかしまず、もぐりこむネットワークを横切るすべてのパケットを実際に見るにはどうすればいいのかを見ていきましょう。

プロミスキャスモードの使用

ネットワーク上でパケットを監視するには、プロミスキャスモードをサポートしているNIC（Network Interface Card ：ネットワークインターフェースカード）が必要です。ネットワークを横切るすべてのパケットを見ることができるようにするのが、プロミスキャスモードです。

1章のブロードキャストトラフィックで学んだように、実際には自分宛でないパケットをクライアントが受け取るのはよくあることです。特定のIPアドレスに対応するMACアドレスを決定するのに使われるARPは、どのネットワークにおいても必需品であり、宛先以外のホストに送られるトラフィックのよい例といえます。一致するMACアドレスを見つけるため、ARPは正しいクライアントが応答してくれるよう祈りつつ、ブロードキャストドメインにあるすべての通信機器に、ブロードキャストパケットを送信します。

ブロードキャストドメイン（コンピュータが他のコンピュータに、ルータを介さずに直接送信できるネットワークセグメント）は複数のコンピュータで構成できますが、送信されるARPブロードキャストパケットに関われるのは、1つのクライアントのみとすべきです。ネットワーク上のすべてのコンピュータが実際にARPブロードキャストパケットを処理するというのは、とてつもなく非効率だからです。その代わり、ネットワーク上の宛先でない通信機器のNICが、そのパケットが自分には役に立たないと認識し、処理のためにCPUに渡さずに、廃棄します。

パケットの廃棄は、宛先でないホストの処理効率を向上させますが、パケット解析にとってはあまりよいとはいえません。アナリストとしては、ネットワークに送られるすべてのパケットを見たいし、重要な情報の断片を見逃したくないからです。

NICのプロミスキャスモードを使えば、トラフィックのすべてを確実にキャプチャすることができます。プロミスキャスモードで操作する場合、アドレスに関わらず、NICは発見したすべてのパケットをホストのプロセッサに渡します。パケットがCPUにたどり着くと、パケットスニッフィングアプリケーションが獲得し、解析します。

現在のNICのほとんどがプロミスキャスモードをサポートしており、Wiresharkはlibpcap/WinPcapドライバを含んでいるため、Wireshark GUIからNICを直接プロミスキャスモードに切り替えることができます（libpcap/WinPcapについては3章で詳しく説明します）。

本書の目的をかなえるには、NICと、プロミスキャスモードの使用が可能なOSが必要になります。プロミスキャスモードでスニッフィングする必要がないのは、スニッフィングしているインターフェースのMACアドレスに直接送られるトラフィックのみを見たい場合だけです。

注　Windows を含むほとんどのOSで、プロミスキャスモードでのNICは、高い権限がないと使用できません。プロミスキャスモードを使用するための権限が合法的に取得できないなら、スニッファを使うべきではありません

ハブで構成されたネットワークでのスニッフィング

ハブで構成されたネットワークでのスニッフィングがもっとも簡単です。1章ですでに学んだとおり、トラフィックはハブのすべてのポートに流れます。したがって、ハブに接続されているコンピュータのトラフィックを解析するためには、ハブ上の空いているポートにスニッファがインストールされたコンピュータを接続するだけでよいのです。そのコンピュータに向かう、またそのコンピュータからのすべての通信だけでなく、そのハブに接続したすべての通信機器とのコミュニケーションも見られるようになります。これで**図2-2** にあるように、スニッファは、ハブに接続されているすべてのコンピュータの通信を見ることができます。

図2-2　ハブで構成されたネットワークでは、すべてをスニッフィングできる

スニッフィングできる範囲

スニッファ

コンピュータA　コンピュータB　コンピュータC　コンピュータD　コンピュータE　コンピュータF

注　本書ではスニッファがスニッフィングできるコンピュータの範囲を、「スニッフィングできる範囲」という枠で示しています。

残念ながら、ハブで構成されたネットワークは、ネットワーク管理者の頭痛の種となるために、今ではほとんど使われていません。ハブは1 回に1 つの通信しか扱えないため、ハブを通して接続されているコンピュータは、通信しようとしている他のコンピュータと帯域幅を取り合うことになります。2 台以上のコンピュータが同時に通信しようとすると、図2-3 に示すようなパケットの衝突が起こります。その結果としてパケットが消失し、コンピュータがパケットを再送して消失を穴埋めしようとするため、ネットワークが込み合い、さらに衝突が起きます。トラフィックが増え、衝突が増えると、コンピュータはパケットを3 回4 回と送信しなければならないため、ネットワークのパフォーマンスが劇的に落ちてしまいます。現在のネットワークがハブでなくスイッチを使用している理由はそこにあります。

図2-3　 2つのコンピュータが同時にパケットを送信すると、パケットの衝突が起こる

パケットを送信したコンピュータ

パケットを送信したコンピュータ

衝突

ハブ

スイッチで構成されたネットワークでのスニッフィング

1章で説明したように、現在のネットワーク環境でもっとも一般的に使用されているネットワーク機器はスイッチです。スイッチはブロードキャスト、ユニキャスト、マルチキャストのデータを効率的に転送します。さらに、スイッチは全二重の通信が可能なため、データの送信と受信を同時に行うことができます。しかし、スイッチで構成されたネットワーク上でのスニッフィングは、ハブで構成されたネットワークほど単純ではありません。図2-4 が示すとおり、スイッチに接続されたスニッファは、ブロードキャストパケットとスニッファがインストールされているコンピュータ宛のパケットしか見ることができないのです。

スイッチで構成されたネットワークで、特定のコンピュータの通信をキャプチャする4 つの主な方法として、ポートミラーリング、ハブを使用する、タップを使う、ARP キャッシュポイゾニングという方法があります。

図2-4　スイッチで構成されたネットワークでは、スニッファがインストールされているコンピュータが接続されているポートしかスニッフィングできない

スニッフィングできる範囲

スニッファ

コンピュータA　コンピュータB 　コンピュータC　コンピュータD　コンピュータE　コンピュータF

ポートミラーリング

ポートミラーリング、またはポートスパニングは、スイッチを使ってパケットをキャプチャするもっとも簡単な手段です。ミラーリングを利用すれば、特定のコンピュータが送受信するパケットをキャプチャすることができます。ポートミラーリングを使用するためには、ターゲットとなるマシンが接続されているスイッチを、コマンドまたはWebマネジメントインターフェースを使って操作する必要があります。加えて、スイッチがポートミラーリングをサポートしていること、そのスイッチに、スニッファ用コンピュータを接続するための空きポートがあることも必要です。

ポートミラーリングを使用可能にするには、スイッチのコマンドラインインターフェースを使い、特定のポートの通信を他のポートにコピー（ミラーリング）するように、コマンドを入力する必要があります。たとえば、ポート3 のパケットをキャプチャするには、スニッファ用コンピュータをポート4 に接続し、ポート3 からポート4 にミラーリングするように設定すればよいのです。それによって、ポート3 のコンピュータの通信を見ることができるようになります。図2-5はポートミラーリングを示したものです。

図2-5　ポートミラーリングによって、スニッフィングできる範囲を広げることができる

コンピュータBのポートをスニッファのポートにミラーリングする

スニッファ

スニッフィングできる範囲

コンピュータA　コンピュータB　コンピュータC　コンピュータD　コンピュータE　コンピュータF

ポートミラーリングのための設定は、スイッチのメーカーによって異なります。ほとんどのスイッチでは、コマンドラインインターフェースにログインし、ポートミラーリングコマンドを入力する必要があります。表2-1 は、一般的なポートミラーリングコマンド一覧です。

注　ポートミラーリングをオプションとする、WebベースGUIを提供するスイッチもありますが、あまり一般的ではなく、標準化もされていません。しかし、GUIを使ってポートミラーリングを効率的に設定できるなら、使わない手はありません。

表2-1　ポートミラーリングを可能にするコマンド

メーカー　コマンド

Cisco　Enterasys　Nortel

set span <ミラーリング元> <ミラーリング先>

set port mirroring create <ミラーリング元> <ミラーリング先>

port-mirroring mode mirror-port <ミラーリング元> monitor-port <ミラーリング先>

ポートミラーリングを使用するときは、ミラーリングしているポートのスループットに注意してください。スイッチの中には、2 台以上のコンピュータの通信を同時に解析できるようにするため、複数のポートを1 つのポートにミラーリングできるものがあります。しかしながら、たとえば24 ポートのスイッチで、100Mbps、全二重で通信する23 ポートの通信を1 つのポートにミラーリングした場合を考えてみてください。4,600Mbps ものパケットが1 つのポートに流れることになります。そうなればかなりの確率でポートを通るパケットの量が物理的な限界を超えることになり、パケットの消失やネットワークの遅延を引き起こすことになります。スイッチは通信を抑制するために、処理しきれないパケットをすべて破棄したり、内部回路を停止させたりします。パケットをキャプチャする際には、このような状況にならないように気をつけてください。

ハブの使用

スイッチで構成されたネットワーク上でパケットをキャプチャするもう1 つの方法は、ハブを使用することです。パケットをキャプチャしたコンピュータとスニッファ用コンピュータを、ハブに接続することで同じネットワークセグメント上に置いてしまうのです。多くの人々は、そのようにハブを使用することは不正行為だと思っていますが、ポートミラーリングが使えない環境で、かつキャプチャしたいコンピュータが接続されているスイッチに物理的に触ることが可能ならば、ハブの使用はスニッフィングを実現する完璧な方法といえます。

ハブを使用してコンピュータの通信をスニッフィングするために必要なのは、ハブと数本のネットワークケーブルだけです。必要なものが揃ったら、次のように接続します。

1．スイッチのある場所に行き、ターゲットマシンのケーブルを抜きます。

2．ターゲットマシンのケーブルをハブにつなぎます。

3．スニッファ用コンピュータとハブをケーブルでつなぎます。

4．ハブとスイッチをケーブルでつなぎます。

これで、スニッファ用コンピュータとターゲットマシンが同じブロードキャストドメイン上に存在することになります。図2-6のように、ターゲットマシンが送受信するパケットは、ハブに接続されているすべてのコンピュータにブロードキャストされることになり、スニッファがパケットをキャプチャすることができるようになります

図2-6　ハブを使うことで、ターゲットマシンとスニッファ用コンピュータを同じブロードキャストドメインに置くことができる

スニッフィングできる範囲

スニッファ

ハブ

コンピュータA　コンピュータB　コンピュータC　コンピュータD　コンピュータE　コンピュータF

ほとんどの場合、ハブを使えば全二重の通信が半二重に半減されることになります。ハブの使用は最良の方法とはいえませんが、ポートミラーリングをサポートしていない場合は、この方法を使うしかありません。ただしハブには電源が必要であり、これを見つけるのが難しい場合もあることを覚えておいてください。

注　ついでに言っておくと、CEOが使っているコンピュータのケーブルを抜くのは楽しい作業になるでしょう。

「本物の」ハブを見つける

ハブを使用する場合、インチキのラベルが貼られたスイッチではなく、本物のハブを使うよう注意してください。実際には性能の低いスイッチの機能しか持たないにも関わらず、ハブとして宣伝、販売するという悪習を持つメーカーが存在するからです。性能が証明されたテスト済みのハブでないと、ターゲットマシンのパケットではなく、自分のパケットしか見ることができません。

ハブを見つけたら、それが本物のハブかどうかテストしましょう。本物であればラッキーです。本物のハブかどうかを判断する最良の方法は、2台のコンピュータに接続して、片方のコンピュータがもう1台との通信をスニッフィングできるかどうか、またネットワーク上の他のコンピュータやプリンタなどの機器との通信をスニッフィングできるかどうかを確認することです。それができれば、本物のハブだということになります。

ハブは時代遅れなため、現在ではあまり製造されていません。店頭で本物のハブを購入するのはほとんど不可能なため、少々努力が必要です。地元の学校区での中古品オークションは貴重な機会です。公立学校は廃棄処分する前にオークションを行うことが義務付けられているうえに、古い機器が放置されていることがよくあります。白い豆とコーンブレッドよりも安い値段で、数台のハブを中古オークションで入手した人々を知っています。またeBayもよい入手先ですが、ハブだと偽ったスイッチをつかまされることがあるので、注意が必要です。

タップを使う

「ステーキがあるのに、どうしてチキンを食べるのか」という言い回しはよく知られています（南部出身なら「揚げボローニャがあるのに、どうしてハムなんだ」というかも知れませんが）。この選択は、タップの使用とハブの使用にも当てはまります。

ネットワークタップは、2つのシステムの間に置いて、この2点間のパケットをキャプチャするためのハードウェア機器です。ハブの場合、ネットワーク内にハードウェアを配置して、必要なパケットをキャプチャします。ハブとの違いは、ネットワーク解析のために特別に設計されたハードウェアを使うという点です。

ネットワークタップには、主に統合型と非統合型の2種類があります。どちらのタップも2台の機器の間に配置され、通信をスニッフします。統合型タップと非統合型タップの主な違いは、非統合型には図2-7で示したように4つのポートがあるのに対し、統合型には3つしかないことです。

図2-7　Barracuda非統合型タップ

またタップには通常電源が必要ですが、なかにはコンセントにつながなくても、短時間であればパケットスニッフィングが可能な電池内蔵型もあります。

統合型タップ

統合型タップの使い方は簡単です。双方向通信をスニッフする、物理的な監視ポートは1つしかないからです。

スイッチに接続された1台のコンピュータのすべての通信を、統合型タップを使ってキャプチャするには、次のように行います。

1．コンピュータをスイッチから外します。

2．ネットワークケーブルの一方をコンピュータにつなぎ、もう一方をタップの「入力」ポートにつなぎます。

3．別のケーブルの一方をタップの「出力」ポートにつなぎ、もう一方をネットワークスイッチにつなぎます。

4．最後のケーブルの一方をタップの「監視」ポートにつなぎ、もう一方をスニッファとして機能するコンピュータにつなぎます。

統合型タップは図2-8のように接続されているはずです。この時点で、スニッファはタップに接続したコンピュータのすべての通信をキャプチャすることになります。

図2-8　統合型タップを使ってネットワークトラフィックをキャプチャする

統合型タップ

コンピュータ

モニター

スイッチ

スニッファ

非統合型タップ

非統合型タップは統合型よりも少し複雑ですが、通信のキャプチャという点ではより柔軟性があります。双方向通信の監視に使えるポートがひとつだけでなく、2つあるからです。片方の監視ポートを一方の通信のスニッフに用い（タップに接続されたコンピュータからの通信）、もう一方を逆方向の通信（コンピュータに入っていく通信）に使うことができるのです。

スイッチに接続された1台のコンピュータにおける双方向通信をすべてキャプチャするには、次のようにします。

1．コンピュータをスイッチから外します。

2．ネットワークケーブルの一方をコンピュータにつなぎ、もう一方をタップの「入力」ポートにつなぎます。

3．別のケーブルの一方をタップの「出力」ポートにつなぎ、もう一方をネットワークスイッチにつなぎます。

4．3本目のケーブルの一方をタップの「監視A」ポートにつなぎ、もう一方をスニッファとして機能するコンピュータのNICにつなぎます。

5．最後のケーブルの一方を「監視B」ポートにつなぎ、もう一方をスニッファとして機能するコンピュータのもうひとつのNICにつなぎます。

非統合型タップは図2-9のように接続されているはずです。

図2-9　非統合型タップを使ってネットワークトラフィックをキャプチャする

非統合型タップ

コンピュータ

モニターA　モニターB

スイッチ

スニッファ

ネットワークタップを選ぶ

2種類のタップの違いを説明しましたが、どちらがいいのでしょうか。多くの場合、必要なケーブル本数が少なく、スニッファとして機能するコンピュータに2つのNICを必要としない統合型が好まれます。しかし大量の通信をキャプチャする場合や、一方向の通信のみをキャプチャする場合は、非統合型タップがよいでしょう。

150ドル程度のシンプルなイーサネットタップから、5桁の企業クラスの光ファイバータップまで、多種多様なタップが購入できます。筆者はNet OpticsとBarracuda Networksのタップを使っていますが、非常に満足しています。他にも優れたタップが数多くあると思います。

ARPキャッシュポイゾニング

ケーブルにもぐりこむテクニックのなかでもお気に入りのひとつが、ARPキャッシュポイゾニングです。ARPプトロコルの詳細については6章で説明しますが、このテクニックの使い方を理解するには、ここで簡単に説明する必要があります。

ARPプロセス

1 章では、パケットのアドレスにはレイヤ3 のものとレイヤ2 のものの2 種類があるということを学びました。レイヤ2 のアドレス（MAC アドレス）は、レイヤ3 のアドレスに連動して使用されます。本書では（そして業界標準用語では）、レイヤ3 のアドレスをIP アドレスと呼びます。

レイヤ3 を使用するネットワーク機器はすべて、IP アドレスを使います。スイッチはOSI 参照モデルのレイヤ2 で動作し、レイヤ2のMACアドレスしか認識しないため、パケットにはこの情報を含ませる必要があります。適切な機器にパケットを転送するためには、MACアドレスが不明な場合、既知のレイヤ3のIPアドレスを使ってこれを取得しなければなりません。この変換のプロセスは、ARP（Address Resolution Protocol）と呼ばれるレイヤ2のプロトコルを通して行われます。

コンピュータがイーサネットネットワークに接続している場合、1台のコンピュータが別のコンピュータと通信しようとすると、ARPプロセスが始まります。送信側のコンピュータはまずARPキャッシュをチェックし、受信側のコンピュータのIPアドレスに関連するMACアドレスをすでに取得していないかどうかを確認します。取得していなければ、1章で説明したように、データリンクレイヤのブロードキャストアドレスFF:FF:FF:FF:FF:FFに、ARPリクエストを送ります。このパケットはブロードキャストパケットであるため、特定のイーサネットセグメントにあるすべてのコンピュータが受信することになります。パケットは「MACアドレスXX:XX:XX:XX:XX:XXを所有するIPアドレスはどれですか？」と質問しているわけです。

このIPアドレスを持たないコンピュータは、ARPリクエストを破棄します。受信相手のコンピュータは、ARP応答によってMACアドレスをパケットに知らせます。最初に送信したコンピュータは、ここでリモートコンピュータとの通信に必要な情報を知らせるデータリンクレイヤを取得し、すぐに検索できるよう、ARPキャッシュにこの情報を保管します。

ARPキャッシュポイゾニングの働き

ARPスプーフィングとも呼ばれるARPキャッシュポイゾニングは、偽のMACアドレス（レイヤ2）を含むARPメッセージをイーサネットスイッチまたはルータに送信し、別のコンピュータのトラフィックに割り込むプロセスです。図2-10はこの設定を図式化したものです。

ARPキャッシュポイゾニングは、スイッチで構成されたネットワークにもぐりこむ高度な手法です。一般に、通信への割り込みやDoS 攻撃（Denial of Service attack ：サービス不能攻撃）を仕掛けるために、偽装したアドレスを持ったパケットをコンピュータやネットワーク機器に送信するため、攻撃者によって使用されます。しかしながら、スイッチで構成されたネットワーク上で、特定のコンピュータのパケットをキャプチャする手段としても使うことができます。

図2-10　 ARPキャッシュポイゾニングによって、ターゲットマシンの通信に割り込む

通常の通信　ターゲットマシン　スイッチ　ルータ　スニッファ

ARPキャッシュポイゾニング　ターゲットマシン　スイッチ　ルータ　スニッファ

Cain & Abelの使用

ARP キャッシュポイゾニングを使用するには、まず必要なツールを取得して情報を集める必要があります。ここではデモとして、有名なセキュリティツールであり、Windowsに対応しているOxid.it（http://www.oxid.it/）のCain & Abel を使います。Webサイトの説明に従ってダウンロードし、インストールしてください。

Cain & Abel をインストールする前に、スニッファ用コンピュータのIP アドレス、トラフィックをキャプチャしたいターゲットマシン、そのコンピュータが接続されているルータの情報などを集める必要があります。

Cain & Abel を起動すると、ウィンドウのトップにいくつかのタブが見えるはずです（ARP キャッシュポイゾニングは、Cain & Abel の多くの機能の1 つにすぎません）。ARP キャッシュポイゾニングは、［Sniffer］タブで利用することができます。［Sniffer］タブをクリックすると、図2-11のように空の表が表示されるはずです。

図2-11　 Cain & Abel の［Sniffer］タブ

以下の手順に沿って、Cain & Abel の「スニッファ」機能（パケットをキャプチャする、いわゆるスニッフィング機能ではなく、ARP スプーフィングの機能）を使って、ネットワーク上のコンピュータをスキャンしてください。

1．ツールバーの左から2 番目、NIC のアイコンに似たアイコンをクリックします。

2．スニッフィングに利用するインターフェース を聞かれます。ARP キャッシュポイゾニングを利用したいネットワークに接続しているインターフェースを選択してください。選択したら[OK]をクリックします（Cain & Abelのスニッファ機能を有効にするため、かならずこのボタンを押してください）。

3．[+]アイコンをクリックし、ネットワークコンピュータのリストを作成します。すると図2-12のようなMACアドレススキャナーダイアログが表示されるので、[All hosts in my subnet]ラジオボタンを選択します（あるいは必要であればアドレス範囲を指定します）。[OK]をクリックします。

図2-12　Cain & Ableのネットワーク検出ツール

これで表には、ネットワークに接続しているコンピュータのMACアドレス、IPアドレス、ベンダ情報などの一覧が表示されます。これらの情報を利用して、ARPキャッシュポイゾニングを使用します。

ウィンドウの下部には、[Sniffer]　がタブ上で使用できる機能のタブが表示されているはずです。コンピュータのリストを作成したら、[ARP]タブをクリックします（ARPポイゾンルーティングのため）。タブをクリックして、ARPウィンドウへ切り替えます。

[ARP]タブをクリックすると、上下2つに分かれた空の表が表示されます。設定を完了すると、上部の表にはARPキャッシュポイゾニングを実行しているコンピュータの情報が、下部の表にはそのコンピュータを介して通信しているすべてのコンピュータの情報が表示されます。

ARPキャッシュポイゾニングの設定手順は以下のとおりです。

1．画面の上半分の空白部分をクリックし、次にツールバー上にある[+]アイコンをクリックします。

2．左右2つに分かれたウィンドウが表示されます。左側の表で、ARPキャッシュポイゾニングによる通信の割り込みが可能なコンピュータのリストが表示されます。ターゲットマシンのIPアドレスをクリックすると、右側の表には残りのコンピュータのリストが表示されます。

3．右側の表で、図2-13に示したようにターゲットマシンが接続されているルータのIPアドレスをクリックし、[OK]をクリックします。これで、標的のコンピュータとルータのIPアドレスが、メインのウィンドウの上部の表に表示されます。

4．最後に、ツールバー上にある黄色と黒の放射能のマークをクリックします。これで、Cain & AbelのARPキャッシュポイゾニング機能が有効になり、ターゲットマシンとルータの通信の間に割り込むことができるようになります。

これで、スニッファを使って通信を解析できるようになりました。パケットのキャプチャが終了したら、黄色と黒の放射能マークをクリックすれば、ARPキャッシュポイゾニングを停止することができます。

図2-13　ARPキャッシュポイゾニングを利用してターゲットマシンを選択する。

ARPキャッシュポイゾニングを使う際の注意

ARPキャッシュポイゾニングは、ネットワークの構成に注意して使用してください。たとえば、1Gbpsでファイルサーバを利用していて、かつパケットキャプチャしているコンピュータが100Mbpsの場合など、大量のパケットが発生するような場所ではこの方法を使うべきではありません。そんな状況でARPキャッシュポイゾニングを利用すれば、大量のパケットが通信に割り込んでいるコンピュータに流れ込みますから、そのコンピュータがボトルネックになってしまいます。これではあなたのコンピュータがDoS攻撃を受けているのと同じことになり、ネットワークのパフォーマンスを下げ、解析もうまくいかないでしょう。

注　非対称ルーティングと呼ばれる機能を使えば、解析しているコンピュータにすべてのパケットが流れ込む事態を回避することができます。この方法についての詳しい情報は、oxid.it User Manual (<http://www.oxid.it/ca_um/topics/apr.htm>)を参照してください。

ルータで構成されたネットワークでのスニッフィング

スイッチで構成されたネットワークでのパケットキャプチャの方法は、そのままルータで構成されたネットワークでも使えます。ルータを含むネットワークでは、複数のネットワークセグメントにまたがる問題を解決しようとしたときにスニッファをどこに設置するか、ということを考えなければいけません。

すでに学んだとおり、パケットがルータを通過すると、反対方向からのパケットの通過を待つため、ブロードキャストドメインはルータで途切れてしまいます。複数のルータをデータが移動する環境では、ルータを通過するすべてのパケットを解析する必要があります。

いくつかのネットワークセグメントが複数のルータに接続されている場合に直面するかも知れない通信問題について考えてみましょう。このネットワークでは、各セグメントはデータを保管、検索するために、アップストリームセグメントで通信します。図2-14のように、ダウンストリームサブネットであるネットワークDが、ネットワークAのコンピュータと通信できないという問題が発生したとしましょう。

他のネットワークのコンピュータと通信できない問題を抱えているネットワークDのトラフィックをスニッフすると、他のネットワークへ送信されるデータは見ることができますが、そこから返ってくるデータを見ることができません。スニッファを設置する場所を再考し、ネットワークBでパケットの監視を始めてみると、何が起こっているかが明確に分かるはずです。ネットワークBのルータがパケットを破棄している、あるいは間違ってルートしていたのです。これで問題の原因がルータの設定にあることが分かり、設定を治せば問題は解決です。このシナリオは少々おおざっぱではありますが、ここでの教訓は複数のルータやネットワークセグメントに取り組む場合、全体図を把握するには、スニッファを何度か動かす必要があるということです。

複数のセグメント上にスニッファを設置しなければならない理由が、この例から分かると思います。

図2-14　ネットワークD上のコンピュータが、ネットワークAと通信できない

ネットワークA　ネットワークB ネットワークC　ネットワークD

ネットワーク地図

今までネットワークについての説明の中で、いくつかのネットワーク地図を見てきました。ネットワーク地図（またはネットワーク構成図）には、ネットワーク上のコンピュータやネットワーク機器がどのように接続されているかが描かれています。

スニッファの設置場所を決定するには、ネットワーク地図を明確にすることが一番です。ネットワーク地図はトラブルシューティングや解析に非常に役に立つので、可能なら常に手元に置いておきましょう。もっと詳細なネットワーク地図が欲しいとさえ思うかもしれません。トラブルシューティングにおける最大の難関は、往々にして正しいデータを収集できるかにあります。

スニッファを実際に設置してみる

スイッチで構成された環境におけるパケットのキャプチャについて、4つの方法を見てきました。1台のコンピュータにスニッファアプリケーションをインストールするだけ（ダイレクトインストール方法）という、もうひとつの簡単な方法について説明します。5つもあると、どの方法が最適かを決めるのに少々悩んでしまうかもしれません。表2-2は各方法についての一般的なガイドラインを示しています。

表2-2　スイッチで構成された環境におけるスニッファのガイドライン

方法　ガイドライン

ポートミラーリング

ネットワークフットプリントを残さず、追加のパケットが生成されないため、一般に好まれる。

クライアントをオフラインにせずに設定可能なため、ルータやサーバのポートをミラーリングする場合に便利。

ハブの使用

ホストを一時的にオフラインにしても問題ない場合に理想的な方法。

複数ホストからのパケットをキャプチャする場合は、ネットワーク障害やパケットの消失が起こりうるため不向き。

本物のハブは10Mbpsであるため、現在の100/1000Mbps環境ではパケット消失の恐れあり。

タップの使用

ホストを一時的にオフラインにしても問題ない場合に理想的な方法。

光ファイバー接続の場合はタップしか使えない。

タップは現代の高速ネットワークに対応するよう設計されているため、ハブよりも優れている。

予算が厳しい場合にはコスト的に困難。

ARPキャッシュポイゾニング

スニッファするマシンを介してトラフィックをリルートするよう、ネットワーク上にパケットを流すため、ずさんな方法とみなされている。

ポートミラーリングが使えない場合、コンピュータをオフラインにせずにパケットを即座にキャプチャする必要がある際に有効。

ダイレクトインストール

パケットが消失あるいは操作され、正確でなくなるという問題が発生するため、ホストに問題がある場合は推奨できない。

ホストのNICをプロミスキャスモードにする必要がない。

テスト環境、検査および性能テスト、他で作成されたキャプチャファイルの検査には最適。

解析は、可能な限りステルスでなければなりません。フットプリントを一切残さずにデータを収集するのが理想です。法医学検査官が犯行現場を汚染したくないのと同様、私たちもキャプチャしたパケットを汚染したくないのです。

後の章での実践的なシナリオを通じて、ケースバイケースでのデータの最適なキャプチャ方法について説明していきます。当面は、パケットのキャプチャに使用する最適な方法を決めるのに、図2-15のフローチャートが役立つでしょう。このフローチャートは一般的な参照に過ぎず、ネットワークにもぐりこむすべての場合をカバーしているわけではないことは覚えておいてください。

図2-15　ネットワークにもぐりこむ最適の方法を決めるのに役立つ図表

ネットワークにもぐりこむ

スイッチはミラーリングをサポートしている？

はい　いいえ

ポートミラーリングを使う

クライアントを一時オフラインにできる？

はい　いいえ

ARPキャッシュポイゾニングを使う

タップが使える？

はい　いいえ

ハブを使用

タップを使用