JANOG8 Meeting
NANOG Update

東京通信ネットワーク株式会社
小島 章裕
akojima@ttnet.ad.jp

2001/07/27

TTNet

NANOG概要

- North American Network Operator's Group
  - 非営利団体のMerit Network, Inc.が中心として、北米各種団体により運営されている
  - もともとは、NSFNETのオペレーティングに関する議論の場として始まる
  - 1994年からISPも参加し、現在の名称に変更
- インターネットの発展に必要な情報交換、コミュニティ間の協調に必要な場として、中心的な役割を果たしている
- 活動
  - Mailing Listによる活動が中心
  - 年3回のMeetingにより、発表、議論が行われている

NANOG 21 & 22 Meeting 開催概要

- NANOG21 Meeting
  - 期間：2001/2/18（日）～2/20（火）
  - 場所：Atlanta Sheraton Hotel（Atlanta，Georgia，U.S.A）
  - Local Host: Riverstone Networks.
  - 参加者：約650名（登録数）
  - 会場内ネットワーク
    - IPv4/IPv6, unicast/multicast(中継用、H.261，MPEG-1/2）
    - Ethernet(10Base-T）、無線LAN（802.11[2 Mb/s, 11 Mb/s], 2.4 GHz/915 MHz)
- NANOG22 Meeting
  - 期間：2001年5月20日(日)～5月22日(火)
  - 場所：DoubleTree Hotel（Scottsdale，AZ，U.S.A）
  - Local Host: Centergate Research.
  - 参加者：約650名（登録数）
  - 会場内ネットワーク
    - NANOG21と同じ
    - 無線LANが主流となり、有線LANは会場の後ろ側一部のみで少数派

会場風景（NANOG22）

会場外風景（NANOG22 in Scottsdale）

NANOG 21 Meeting Topics

TTNet

Agenda

http://www.nanog.org/mtg-0102/agenda.html

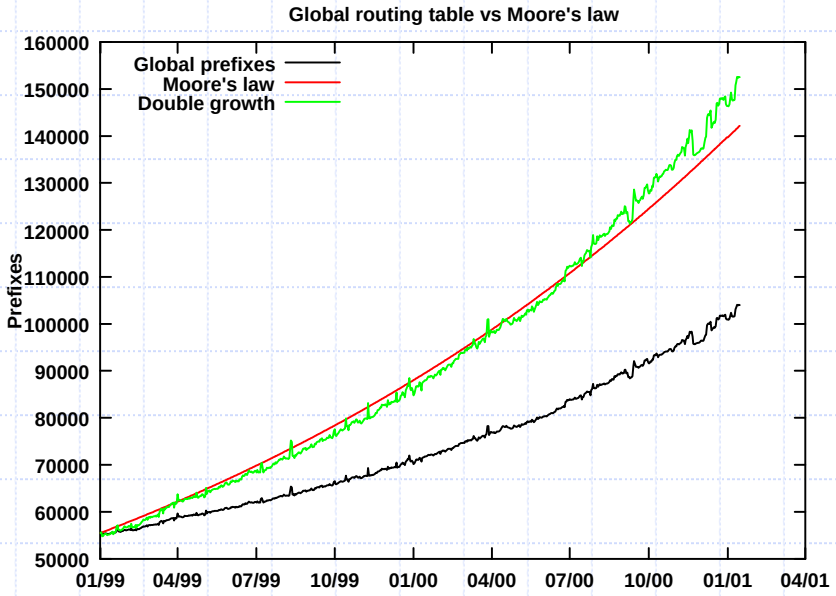
- General Session 2/19
  - Multiservice Core Design
  - Reasons Not to Deploy RED (or, "On the Limits of Active Queue Management")
  - DDoS Attacks and Pushback
  - Review & Analysis of Y2K vs. Previous Years' Outages
    Analysis of Network Outages and Events in the Year 2000 Compared to Previous Years
  - FlowScan
  - Single Source Multicast: The Multicast Broadcast Model
  - Blurring the Lines Between Circuits and Protocols:
    Plans to Re-Organize Sub-IP Technologies in the IETF
  - BGP MED Oscillation
  - Dynamic Service Provisioning in Converged Network Infrastructure
  - Panel: Provider-Provisioned VPNs

Agenda(2)

- Evening BOF 2/19
  - Network Policy
  - FlowScan
  - AAA
  - Data Center BOF II
- General Session 2/20
  - Panel: Global Routing System Scaling Issues
  - IPv6 in Mobile Wireless Networking
  - Network Policies: Current and Proposed (BOF Follow-Up)
  - New Version of the RIPE Database
  - Very Short Reach OC-192/STM-64 Interfaces
  - Florida Exchanges Facing South: NOTA and the MIX
- Tutorial 2/18
  - Exterior Routing 201: The Full Picture
  - Understanding Standards Track IETF MIBs
  - Customer Satisfaction 201

Panel: Global Routing System Scaling Issues

- 傾向
  - Global Routing tableの増大、IP addressの割当てpolicyの変化、AS番号割当てが指数関数的に増加。
- Routing Table増大に対するﾊｰﾄﾞｳｪｱの対応
  - ﾑｰｱの法則の1/2の増加率
  - ISPへの推奨
    - Global Prefixの浪費回避
    - ﾊｰﾄﾞｳｪｱのUpgradeをTrack
    - RRの採用、外部接続を増やす前にprocessorのUpgrade
  - Communityへの推奨
    - New routing architecture



- その他
  - prefix分布、BGPのUpdate/Withdrawの分析など
  - AS番号の4Byte化について
    - Protocolの確定：2001/1Q、Testが2001/2Q、初期採用2001年中

Panel: Provider-Provisioned VPNs

- 最近のIETFでのVPNに関する動向
  - 2000/7にNetwork-based VPN(NBVPN) BOFが開催された
  - 活動ﾀｰｹﾞｯﾄを広げ 2000/12のIETFにてProvider Provisioned VPN (PPVPN)と名称変更
- 発表概要
  - MPLS-based Layer2 VPNs
    - これまでの典型的なVPNは、ATM/FRを利用したﾌﾙﾒｯｼｭの形態
    - Provisioningの複雑性、ﾄﾗﾋｯｸよりﾄﾎﾟﾛｼﾞｰにｺｽﾄ依存、複数ﾈｯﾄﾜｰｸのため運用負荷大
    - MPLSを利用し、ｺｱとｴｯｼﾞの機能分離を目標
    - 1つのﾈｯﾄﾜｰｸですべてのｻｰﾋﾞｽを提供：L2 VPNs, L3 VPNs, etc.
  - Network based IP VPN Architecture using Virtual Routers
    - 目標：ｽｹｰﾗﾌﾞﾙな手法で付加価値を付与したVPNｻｰﾋﾞｽ提供
    - VRの定義：ｿﾌﾄ/ﾊｰﾄﾞｳｪｱ両面で実ﾙｰﾀをemulation
  - Deployment of MPLS VPN in Large ISP Networks
    - MPLS VPNを段階的にﾈｯﾄﾜｰｸへ導入する手法紹介
- 議論：ｲﾝﾀｰﾈｯﾄ派とIPｻｰﾋﾞｽ派間での論争
  - 複雑性、ｽｹｰﾗﾋﾞﾘﾃｨ等

Network Policies

- NANOG21と22の2回、BOFとSession
- 各ISPなどの意見を集めながら、Layer3のPolicy（Routing, Filtering）の現状と将来動向を集約
- Peer Routing Policy
  - Registry情報からのFiltering（Qualityはまだ課題）
  - 割当境界でのFiltering、max-prefix countでのFiltering
  - 余分なAddress取得
- Customer Routing Policy
  - Peer routing policyよりaggressive
  - AS path filterよりprefix filterが一般的
  - Multi-homingが一般的、specificな経路が増える問題あり
- Filtering Policy
  - Reverse Path Filtering(loose/strict)
  - 未割当てアドレス空間のFiltering（ACL）、draft-manning-dsua-06.txt
- なぜこのようなことをするのか？
  - 終わりが近い
  - *Do what you can to keep your corner clean*

TTCN

Other Topics

- FlowScan - http://www.caida.org/tools/utilities/flowscan/
  - ﾈｯﾄﾜｰｸﾄﾗﾋｯｸのﾚﾎﾟｰﾄ、ﾋﾞｼﾞｭｱﾙ化ﾂｰﾙ
  - ﾌﾘｰのopen system用ｿﾌﾄｳｪｱﾊﾟｯｹｰｼﾞ
- BGP MED Oscillation
  - RRやConfederationにおけるMED設定により、endlessなconver-gence loopを発生させる恐れがある
- Florida Exchanges Facing South
  - フロリダに新しく設立される2つの次世代IXの紹介
  - NOTA(NAP of The America)
    - NSFの支援なく、CarrierやISPが連携して構築するNAP
    - PacBell NAP、Ameritech AADS NAPを手がけたTelcordiaが設計
  - FloridaMIX
    - BellSouthによる、ﾏｲｱﾐｴﾘｱで場所によらず相互接続可能な施設

NANOG 22 Meeting Topics

TTNet

Agenda

http://www.nanog.org/mtg-0105/agenda.html

- SUNDAY TUTORIALS – 5/20
  - BGP Techniques for Service Providers
  - Basic ISP Traffic Engineering Tools and Practices
  - ARIN Policies and Guidelines)
- MONDAY GENERAL SESSIONS – 5/21
  - Welcome, Introductions
  - Estimating Global Denial-of-Service Activity
  - Observations and Experiences Tracking Denial-Of-Service Attacks Across a Large Regional ISP
  - Practical Approaches to Dealing with DDoS Attacks
  - A Fine-Grained View of High-Performance Networking
  - Some Initial Measurements of Prefix Length Phyltreing
  - IPv4 Address Space Allocation and Usage Trends
  - Progress With the DNS Security Extensions
  - A View of the Future: The IP-Only Internet

Agenda(2)

- MONDAY BREAKOUT SESSIONS *new*
  - Introduction to IP Multicast Practice
  - SNMP Update
  - More on Network Policy - Sequel to a BOF, Prelude to a Tutorial
- Monday Evening BOF
  - Internet Routing Registry Coordination
- TUESDAY GENERAL SESSION – 5/22
  - The New IETF Sub-IP Area - A Brief Summary for Service Providers
  - MPLS Enhancements to Support Layer 2 Transport Services
  - Very Pleasant/Painful Networking: The Highs and Lows of Building and Maintaining VPNs
  - Operational Experience with IPv6 Migration
  - An Information Sharing and Analysis Center for the Internet
  - Inter-Domain Content Networking
- Closing Remarks

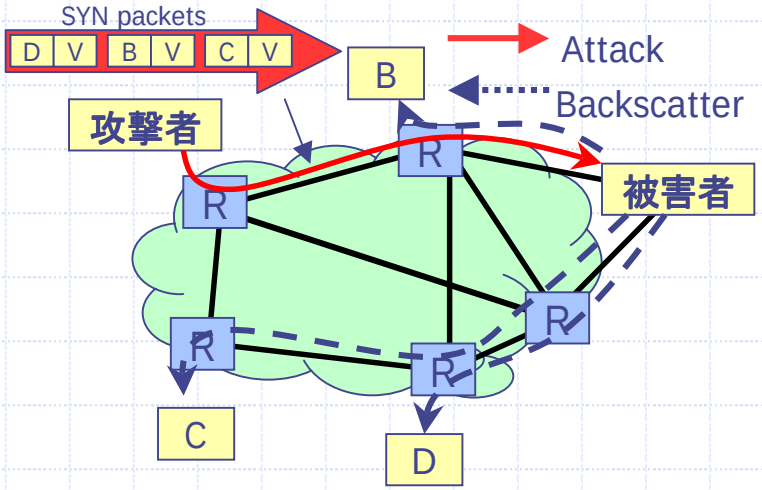
DDoS Attackに関する発表（3件）

- DDoS Attackが増加
  - 2000/2 Yahoo, Ebay, E*tradeなどが1連のDoS Attackを受ける
  - 2001/1 MicrosoftのDNSが被害を受け、この後も多くのサイトで被害が増加している
  - しかし、CSI/FBIの調査報告以外に、実態の分析に必要なデータが得られにくい
- 個別の発表概要
  - Estimating Global Denial-of-Service Activity
    （http://www.caida.org/outreach/papers/backscatter/usenixsecurity01.pdf）
    - 実際にInternet上で発生しているDDoS Attackの実態を推測
  - Observations and Experiences Tracking DoS Attacks Across a Large Regional ISP
    - 特定のISPにて実際のDoSの状況を観測した結果のレポート
  - Practical Approaches to Dealing with DDoS Attacks
    - DDoS Attackの検出装置を分散設置することにより、検出及びFilteringによる対応を行う手法の紹介

Estimating Global Denial-of-Service Activity

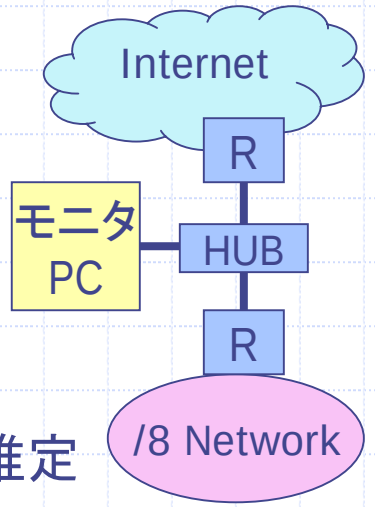
分散攻撃

- 多量のパケットを送り込むことにより
  装置の処理能力をオーバフローさせる
- 典型的な攻撃の手法：TCP/SYN->TCP/ACK等
- 送信元アドレスを偽ることにより
  攻撃元を隠し、攻撃力を増加させる
- この送信元アドレスは、ランダムに生成されることが多い
  - 一般的な攻撃ツールはそのようにプログラムされている
  - 例：Shaft, TFN, TFN2k, trinoo等
- これらの攻撃を“backscatter”と呼ぶ
  （右図）
  - ランダム送信元アドレス（B,C,D）
    を持つSYNパケットを攻撃元から
    送信
  - 被害者（V）は、B~DへSYN/ACKを
    送り返そうと試みる



Estimating Global DoS Activity（2）

- 定量的な分析手法
  - 送信元アドレスがランダムであることに着目し、いくつかの仮定を置いた上で、Internet上でのDoSの実態を定量的に分析
  - 仮定
    - Spoofされているアドレスがランダムであること
    - 攻撃者→被害者のトラヒックが完全に配送されており、かつbackscatterがモニタに完全に配送されていること
    - 要求していないトラヒックで受信されたものがすべてbackscatterであること
  - 測定手法（右図）・結果概要
    - /8のネットワークに対するbackscatterを収集
    - /8は、全アドレス空間の1/256
    - 3週間（2001/2/1～2/25）の測定期間
    - 攻撃数：12,805、被害アドレス：5,000超
    - 全インターネットでは、20万を超える攻撃があったと推定



Estimating Global DoS Activity（3）

- 分析結果（詳細は、レポート参照）
  - 1時間ごとの攻撃件数：30～200弱まで分布
  - 反応プロトコルの詳細
    - TCP(RST ACK)が約50%
    - これはSYN flood or 予期しないTCP攻撃の結果と推定される
  - プロトコル分布
    - TCPが支配的
  - ポート分布
    - 複数ポートが多い。その他、IRC，HTTP，Telnet，Authdなど
  - 攻撃継続時間
    - 2分～30分程度が多いが、長いものは1～2日

Estimating Global DoS Activity（4）

- 結果の信憑性
  - 仮定を設定しているため、結果がどこまで現実と一致しているか？
    →かなり信憑性が高い
  - その理由
    - Backscatterとして観測されたﾊﾟｹｯﾄはPort Scanなどでは説明できない。
      これは、98%のbackscatterのﾊﾟｹｯﾄは応答を返さないため
    - 別の独立したﾈｯﾄﾜｰｸ（3×/16）にて、一致した結果を得ている
    - Asta Networksのバックボーンで検出された実攻撃と一致
- 結論
  - 多くの攻撃が行われており、いくつかはかなり大規模
  - 3週間で12,000を超える攻撃、1週間では5,000を超える
  - たいていは、1,000pps以下だが、いくつかは、600,000pps
  - 誰でも、潜在的なターゲットと成りうる
  - 新しい攻撃スタイル
    - 瞬間的／定期的攻撃
    - ルータなどインフラやブロードバンドが攻撃対象

Some Initial Measurements of Prefix Length Phyltreing
（http://psg.com/~randy/010521.nanog/）

- Prefix Length Filteringによる削減経路数と不到達度の検証
  - Telstra（内部）、Univ. of Oregon、RIPE、Verio customerのBGP Tableを利用
- 測定方法
  - Private AddressなどをFilter outしたものをﾍﾞｰｽとして設定
  - 以下のFilterを適用した場合の削減経路数と未到達アドレスを測定
    - /24より長いprefixを削除
    - RIRの割当より長いClass A･Bのprefixを削除
    - 206以上でRIRの割当より長いClass Cのprefixを削除
- 注意事項
  - RIRが公開している割当ブロックが間違っていたり、公開されていない点
  - 冗長アナウンスの原因がマルチホームだとすると、Filteringによりその効果が得られない状態が発生する
    →サービスに対してPayしないものが我々のリソースを消費するのは許せない
- 結論
  - 経路数削減の恩恵の大半は、A及びBに対するFilterから（3~4万経路減、未達約0.15%）
  - 不到達の不具合の大半は、Cに対するFilterから（3~4万経路減、未達約0.3%）
  - この中間を取るのが有効かもしれない

MPLS Enhancements to Support Layer 2 Transport Services

- 目的
  - Layer2転送は、MPLSの新しいアプリケーション
  - IP/MPLSネットワークを保有しているプロバイダに対して、Layer2サービスの提供を可能とする
  - MPLSのLabel stackingの機能によるコアネットワークの拡張性
  - ネットワークのコアにおいては、より少ないコネクションのみ運用するだけでよい
  - 個別のサービスは、ネットワークのエッジにてProvisioning
- 利用技術
  - MPLS-based Layer 2VPNs (L2VPN)
    - draft-kompella-mpls-12vpn-02.txt
  - Transport of Layer 2 frames over MPLS
    - draft-martini-l2circuit-trans-mpls-05.txt
    - draft-martini-l2circuit-encap-mpls-01.txt
    - Full or partial mesh provisioning requires automated management tools

Operational Experience with IPv6 Migration

- 東大の加藤さん（現在USC/ISI）による発表
- NSPIXP6の状況やIPv6 IXの実況報告

Other Topics

- A Fine-Grained View of High-Performance Networking
  - 99.99%の信頼性から99.999%への技術的取組み
- IPv4 Address Space Allocation and Usage Trends
  - IPv4のアドレス割当状況の分析とRIRのﾃﾞｰﾀ公開/予測の必要性PR
- A View of the Future: The IP-Only Internet
  - 将来の通信網の基幹を、IPv4 Transport Coreと考えるIdea
- An Information Sharing and Analysis Center for the Internet
  - 障害情報などを共有するセンターの設立案の紹介と協力要請
- Very Pleasant/Painful Networking
  - IPsecﾍﾞｰｽのVPN構築のメリット･デメリットに関する報告
- Inter-Domain Content Networking
  - 複数のCDN間でのContents配信の連携方法に関する技術動向紹介

Next NANOG Meeting

- NANOG 23 Meeting
  - Date: October 21-23, 2001
  - Place: Oakland CA
  - Host: Cisco Systems, Inc.

References

- NANOG
  - http://www.nanog.org/
- NANOG21 Meeting
  - http://www.nanog.org/mtg-0102/
- NANOG22 Meeting
  - http://www.nanog.org/mtg-0105/

Thank you!