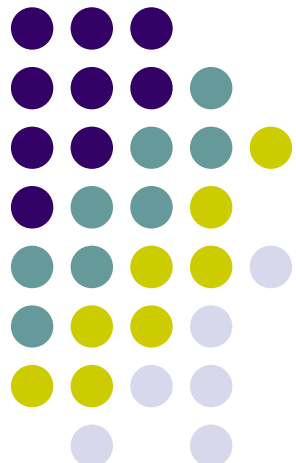
MOBIKEプロトコルの設計に関する検討

渡邊研究室
063432019
東　長俊
2006/05/11



本資料について

本資料は下記文献を基にして作成されたものです。この文書の内容の正確さは保障できないため、正確な知識や情報を求める方は原文を参照してください

著者：T. Kivinen，H. Tschofenig
文献名：Design of the MOBIKE Protocol
<draft-ietf-mobike-design-02.txt>
種類：Internet Draft
発表日：March 3, 2006

流れ

- はじめに
- シナリオ
- MOBIKEの範囲
- プロトコル設計に関する考慮事項
  - アドレスの選択
  - NAT Traversal
  - SA変化の範囲
  - ゼロアドレスセットの機能
  - 往復経路検査
- プロトコルの細部
- セキュリティに関する考慮事項

はじめに (1)
MOBKIEとは

- MOBIKE(IKEv2 MobilityとMultihoming)：**インターネット鍵交換プロトコルバージョン**2(IKEv2)**の拡張**
- IKEv2**を拡張することにより，1端末が複数**IP**アドレスを持ち，移動やマルチホーム時において**IP**アドレスの変更が伴うリンク切替えが起こる場合に，暗号化鍵や認証鍵の再配布 (リキー) や再認証を行うことなく**Security Association (SA) **を継続して利用することが可能な技術**

はじめに (2)
Mobile IPv6と異なるところ

- Mobile IPv6技術は両方のエンドポイントの移動を許容する
- MOBIKE技術は片方のエンドポイントだけが移動するケースで利用される技術となる
  - 例：遠隔地からの固定したゲートウェイへリモートアクセスするようなケースでMOBIKE技術が適用される

用語

- Peer
- Available address
- Locally operational address
- Operational address pair
- Path
- Current path
- Preferred address
- Peer address set
- Bidirectional address pair
- Unidirectional address pair

シナリオ

- MOBIKEプロトコルのために3つの典型的な使用シナリオ
  - **モビリティ シナリオ**

    Mobility Scenario
  - **マルチホーミング シナリオ**

    Multihoming Scenario
  - **マルチホーム ラップトップ シナリオ**

    Multihomed Laptop Scenario

モビリティ シナリオ

- このシナリオでMOBIKEの目標はＭＮとGWが、既存のSAsを使用し続けて、新しいIKE SAをセットアップするのを避けるのを可能にする
- break-before-makeシナリオにおいて、古いIPアドレスに到着することができなかったあと 、MNが新しいIPアドレスを得る
- make-before-breakシナリオでは、MNは特定の期間の間、古いIPアドレスと新しいIPアドレス両方で届く
- MOBIKEは、上記のシナリオの両方ともで働かなければならない

モビリティ シナリオの図

MN (mobile node)

OAR ("old" access router)

NAR (new access router)

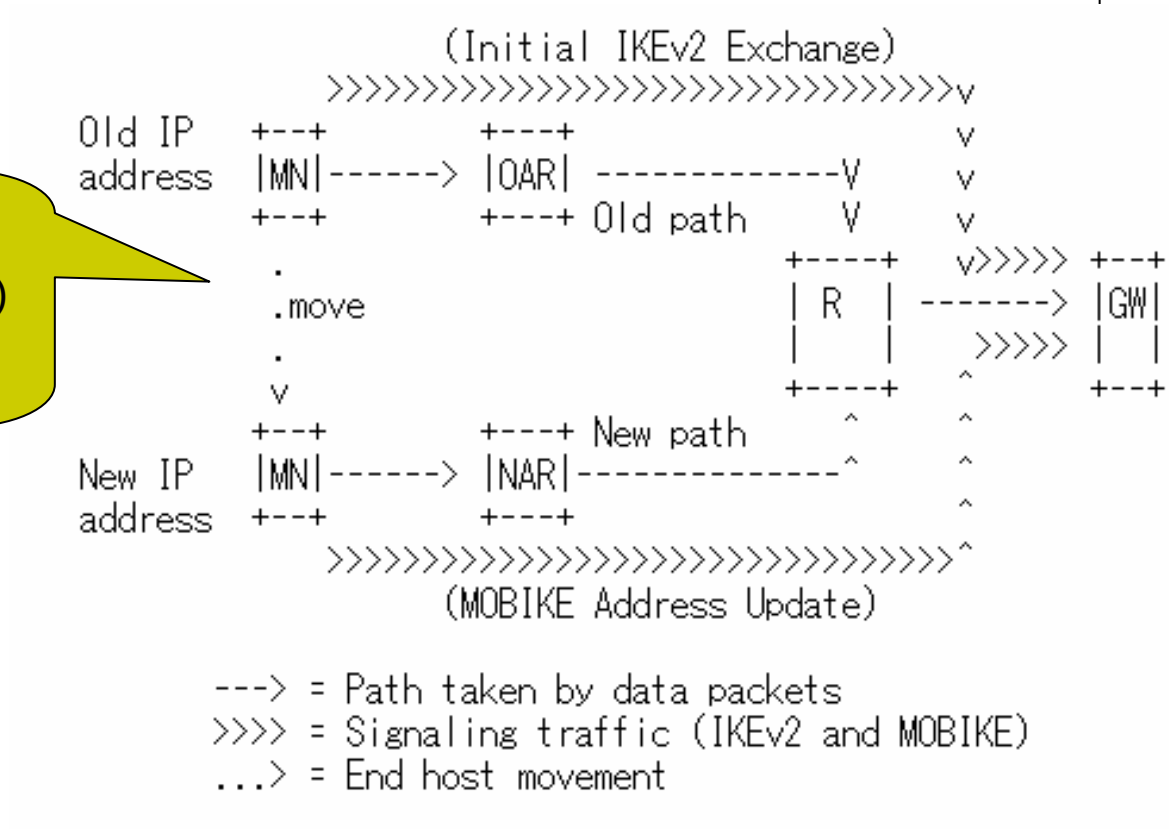


Figure 1: Mobility Scenario

マルチホーミング シナリオ

- MOBIKEペアは、複数のインターフェース（複数のIPアドレス）を備えている。ペアAは2つのIPアドレス、IP_A1とIP_A2で2枚のインターフェースカードを持っている。そして、ペアBは2つの IPアドレス、IP_B1とIP_B2を持つ
- 各々のペアは、そのIPアドレスのうちの1つをpreferred addressとして選ぶ。
- いろいろな理由（例えばハードウェアまたはネットワークリンク失敗）は、1つのインターフェースからもう一つまで変わることをペアに要求するかもしれない
- MOBIKEが複数のIPアドレスの間のロードバランス（load balancing）を支持しない。即ち、各々のペアは所定の時間でavailable address pairsのうちのひとつだけを使用する

マルチホーミング シナリオの図

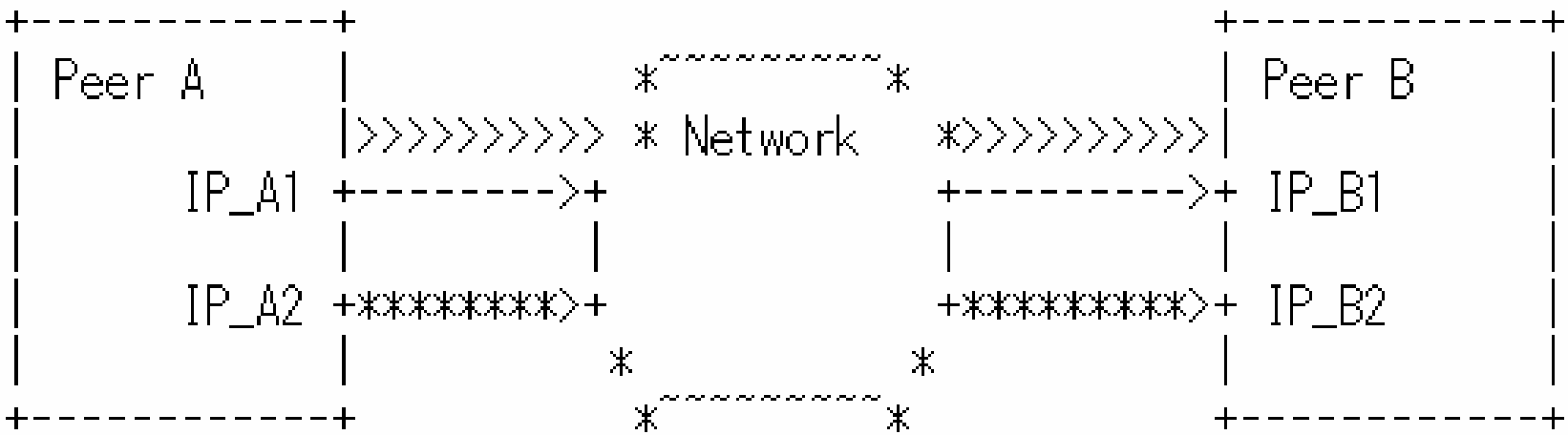


Figure 2: Multihoming Scenario

マルチホーム ラップトップ シナリオ

- ラップトップは、複数のインタフェースカードを持っていて、ネットワークに接続する方法がいくつか持っている。
  - 例えば、固定イーサネットカード、WLANインタフェース、GPRSアダプター、ブルートゥースインタフェースまたはUSBハードウェア
  - どのインターフェースがネットワークに接続するかについて決定するポリシーはMOBIKEプロトコルの範囲外である
- しかしながら、ラップトップがネットワークへの接続のポイントが変わるのに従って、 ラップトップにアクセスされることできるIPアドレスセットはまた変わる

共通点

- 三つのシナリオの全てに、IPアドレスがインタフェースの切り換えや移動のために変わるとしても、IKEv2の中のペイロード設定で得られたIPアドレスは影響を受けないままで残っている
- IKEv2ペイロード設定を通して得られたIPアドレスはIPsecトンネルの内側のIPアドレスの設定を許す
- このように、アプリケーションはどんな変化でも見つけないかもしれない

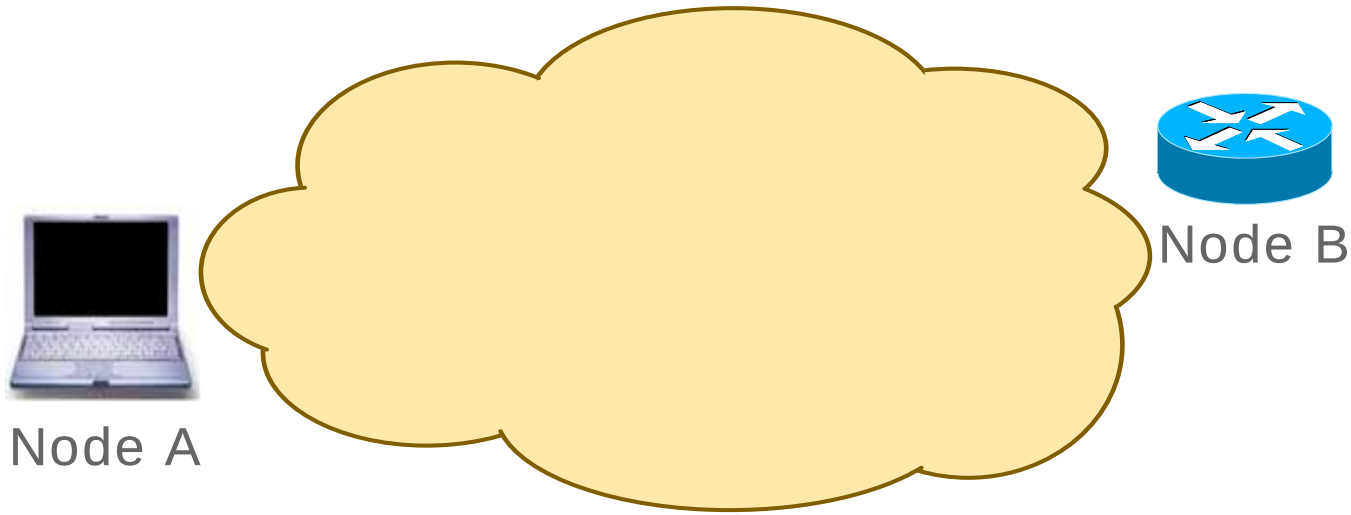
MOBIKEの範囲 (1)

- モビリティとマルチホームを実現するのは、多くの異なるコンポーネントが一緒に動くことを要求する
  - 例えば、異なる層、異なるモビリティメカニズムとIPsec/IKEの間で調和して動く こと
  - それらの面の大部分はMOBIKEの範囲を超えている
- MOBIKEは、2つのペアが相互接続に必要なIKEv2レベルで同意するために必要とすることだけに集中する
  - トンネルモードに集中する

MOBIKEの範囲（2）

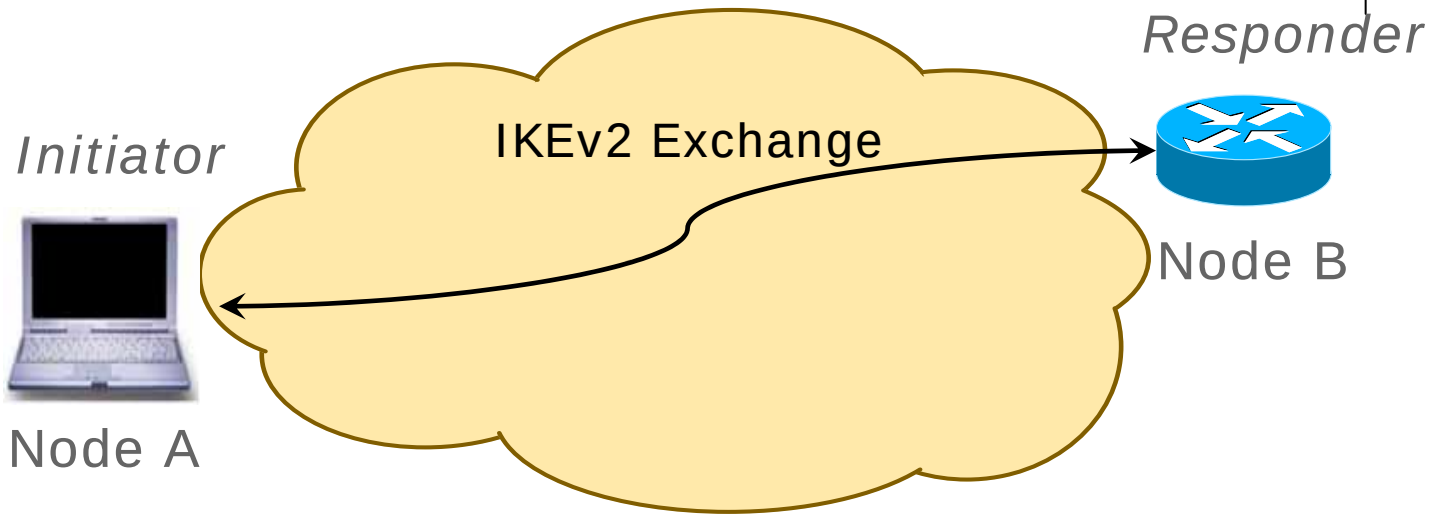
- MOBIKEプロトコルは以下の操作ができる
  - 片方のペアにpeer address setを知らせる
  - 片方のペアにpreferred addressを知らせる
  - 接続性をテストして、停止期間状況を検出 する
  - preferred addressを変える
  - peer address setを変える
  - NATデバイスに対処する

MOBIKEの例
Initialize



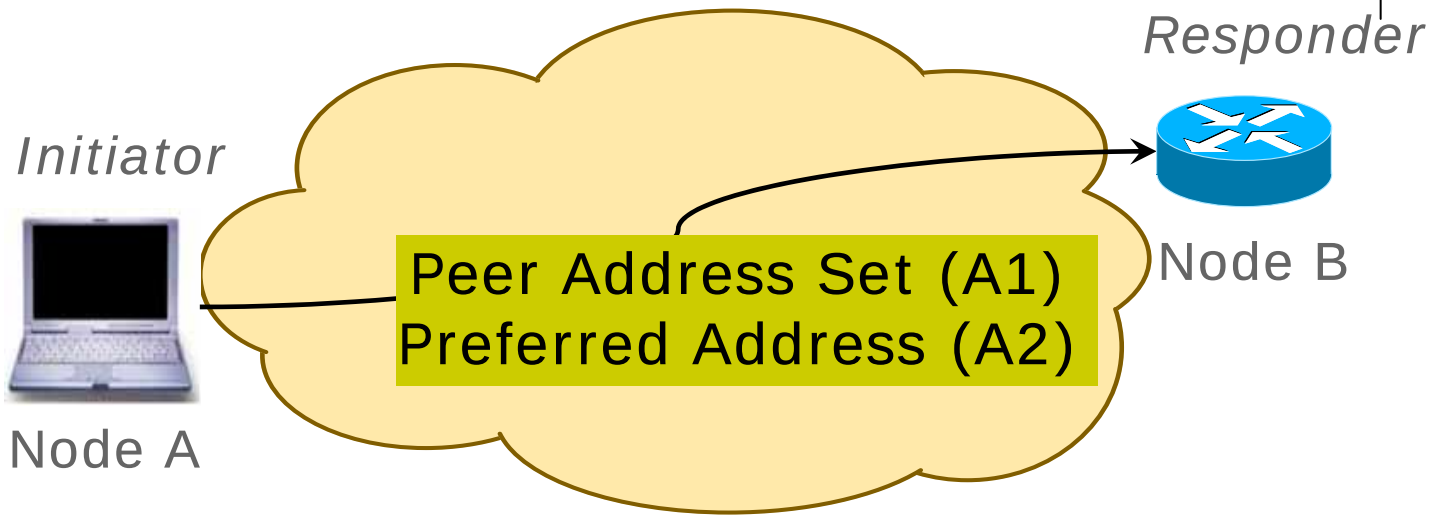
- Node A and Node B have two interfaces.
- Local configuration at the MOBIKE daemon indicates that both addresses may be used (=peer address set)

Starting the exchange



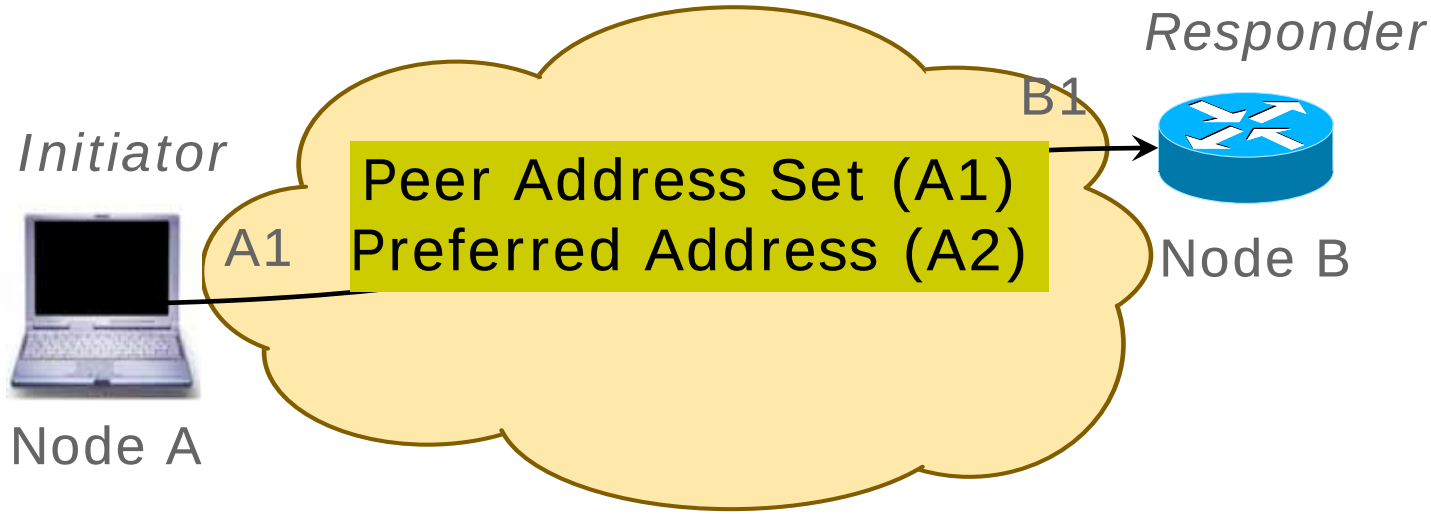
- Node A discovers node B somehow.
- Initial message exchange with IKEv2 already performs connectivity test.
- Node B returns message where it came from!

Node A switches interface



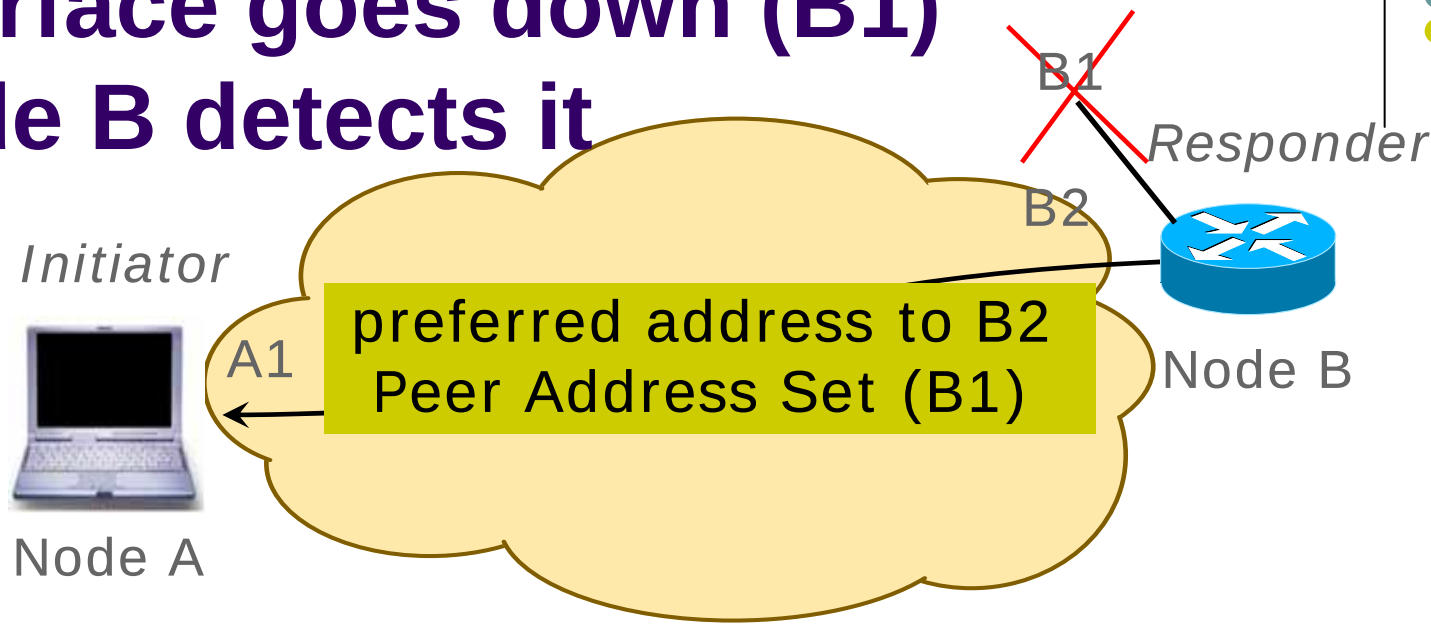
- MOBIKE messages should use A2 instead of A1 as preferred address.
- Node A needs to tell Node B that the preferred address has changed.

Interface goes down (A2) Node A detects it



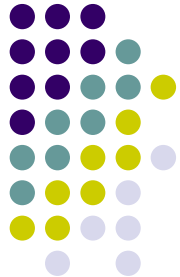
- MOBIKE messages should use A1 instead of A2 as preferred address
- Break-before-make scenario

Interface goes down (B1) Node B detects it



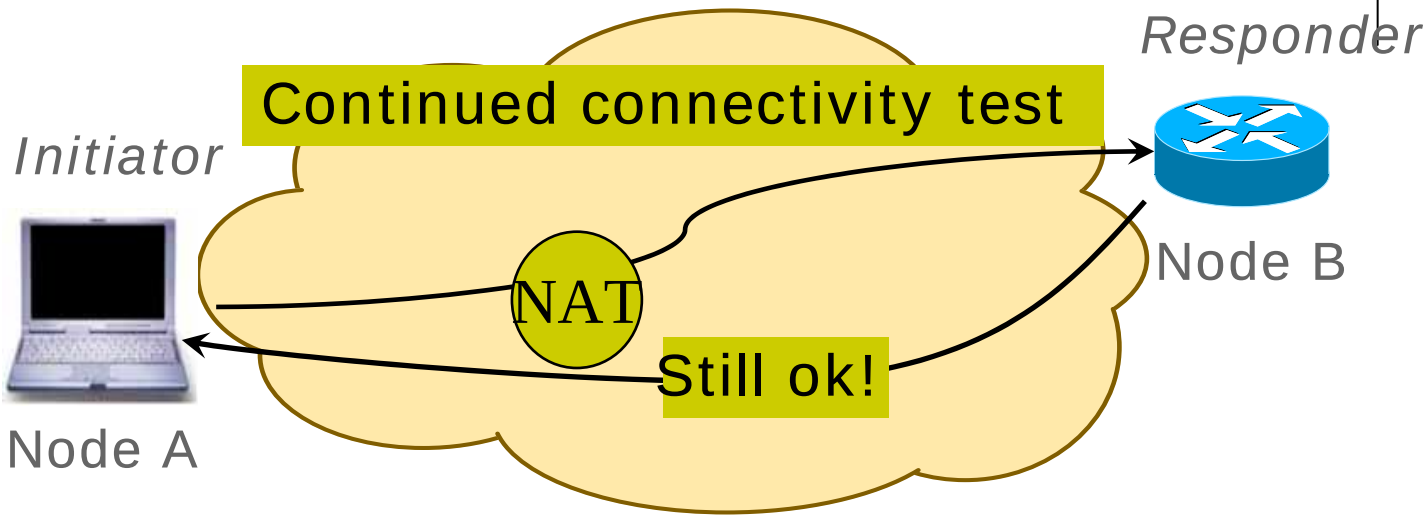
- Node A should address MOBIKE messages to B2 instead of B1

プロトコル設計に関する考慮事項
アドレスの選択



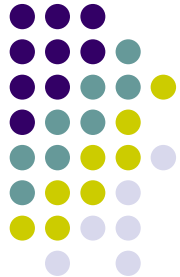
- MOBIKEプロトコルのコアの一つはIPsecパケットを送るためのアドレスの選択
- 接続性
  - MOBIKEは、双方向性アドレスペアだけに対処する
  - IPv4とIPv6アドレスを同じIPヘッダに入れるのは働いていない
- 接続性検査
  - MOBIKEペアが返事を受けるならば、働く（双方向性の）アドレスペアの存在が確かである。
  - MOBIKEペアが複数の転送の後に返事を見ないならば、テストされたアドレスペアが壊れていると仮定するかもしれない
  - 接続失敗が混雑で引き起こされるかもしれないので、接続性テストは、混雑問題を考慮しなければならない
- 意思決定
  - MOBIKEプロトコルを設計することにおける主な問題の1つは、失敗が検出されるとき、誰がどのように状況を修理するかという決定すること。
  - 意思決定における対称 vs. 非対称

Connectivity Tests



- Purpose of connectivity test:
  - Determine whether a given address pair offers bi-directional connectivity
- IKEv2 provides support via the Dead Peer Detection (DPD) mechanism

NAT Traversal（1）---背景と制約



- NAT TraversalはNATを越えて端末間 P2P 接続を実現する技術
- MOBIKEのもう一つのコアは、異なるNATsとNAPTsの処理
  - IKEv2では、IKEv2ペイロードの中にトンネルヘッダーIPアドレスを送りない、このように、片側がセルフでアドレス修理する必要はない
  - IKEパケットの外側のIPヘッダーからトンネルヘッダーIPアドレスを取る、その結果、NATは既にそれらを処理する
- NAT検出ペイロードは、IPヘッダーのアドレスが経路に沿ったNATによって変更されたかどうか決定するのに使用される。
  - NATを検出するのは、IPsec ESPパケットのUDPカプセル化に要求する
- MOBIKEプロトコルは、MOBIKEとNAT-Tがどのように一緒に使用されるかを定義する必要がある
- NAT-Tサポートはオプションである

NAT Traversal (2) ---基本的な制限

- MOBIKEの中で実行することができない若干のケースがある
  - 例えば：対称形のNATの外のパーティーはそのアドレスをもう片方のペアが知りない何かに変更する (古いアドレスは働くのを中止した)
    - NATの後ろのパーティーが新しいIPアドレスを知らないので、NAT状態を造ることができない
  - IKEv2の外のランデブーメカニズムを使って解決が可能

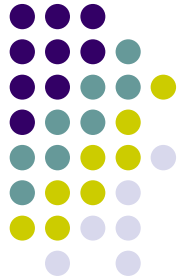
NAT Traversal (3)
Moving to behind a NAT and back

- MOBIKEは最初にNATの後ろにいないペアがNATの後ろに移ることができるメカニズムを提供する
- 同様に、MOBIKEはNATed経路が非NATed経路に変わるかを検出するためにメカニズムを提供する
- NAT-Tを可能にすると、いくつかのものを含む:
  - 1つは、ESP パケットのUDPカプセル化を可能にすること
  - もう一つは、IKE SAポートを500から4500まで変えること

NAT Traversal（4）---NAT Prevention

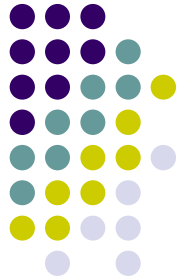
- MOBIKEによって造られた1つの新機能がNAT防止
  - すなわち、ペアの間のNATを検出するなら、私たちはそのアドレスペアが使用されるのを許さない
    - ノード(例えば、IPv6やsite-to-siteの固定VPN)の間にNATがない場合におけるIPアドレスを保護するに用いられることができる
    - ヘッダーのアドレスを変更する経路上の攻撃者のどんな可能性でも避ける

SA変化の範囲（1）



- preferred addressを変えると、IPsec SAデータベースのエントリーは影響される
- 基本的な問題は、新しいアドレスペア(MOBIKE signaling trafficと同じアドレスペア)を使用するためにどのようにIPsec SAsを変えるかということ
  - 1つのオプションは、IKE SAアドレスを変えるとき、それと共にすべての関連するIPsec SAsを自動的に新しいアドレスペアに移動する
  - もう一つのオプションは、別々にIPsec SAsを移動するために別々の交換をする

SA変化の範囲 (2)

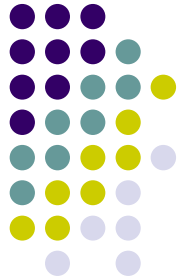


- IPsec SAsが別々に更新されるならば、帯域幅を保持するためにNotifyペイロードより効率的なフォーマットを必要とする
- 他方、私たちがIKE SAアップデートをIPsec SAアップデートに結ぶとしても、このシナリオのために別々のIKE SAsを作成することができる
- ワーキンググループは、IKE SAアドレスペアが変化するとき、すべてのIPsec SAsを移動すると決めた

ゼロアドレスセットの機能

- 役に立つ特徴のうちの1つは、接続を断つと発表すること
  - 例えば、ラップトップはスタンバイモードになる場合
    - この場合、それはzero new addressでアドレス通知を送ることができる (有効なアドレスもうないことを意味する)
- 技術的な観点から、これは次の2つの特徴を提供する
  - IPsecデータトラフィックを伝える必要がない
  - MOBIKEシグナルメッセージは無視される

往復経路検査 (1)
Return Routability Check



- Preferred addressを変えて、次のコミュニケーションにそれを使用するのは認可決定に関連している---ペアはこのアドレスを使用することができるか?
- 2つのメカニズムが提案された:
  - ペアが使用しているアドレスは証明書の一部である
  - リモートペアはそのペアのＳＡＤ (Security Association Database) でアドレスを更新する前に往復経路確認を実行する
- 認可決定を取らないで、悪意のペアは第三者かブラックホールにトラフィックをリダイレクトすることができる
- 往復経路確認の目標:第三者の爆撃攻撃から守る

往復経路検査（2）

- 往復経路検査の基本形式はＤＰＤ（dead-peer detection）検出と類似
- IKEv2 NAT-Tメカニズムは往復経路検査を実行しない
- テストされるアドレスがMOBIKEペイロードの中に運ばれるならば、敵はパケットを送り届けることができない。このように、第三者爆破は防がれる

往復経路検査失敗

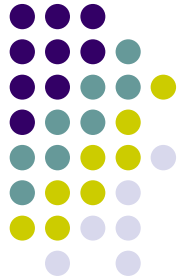
往復経路検査が失敗するなら

- **往復経路検査を送るために**IKEv2 INFORMATIONAL**交換を使用するならば、我々は**IKE SA**を取りこわす必要がある。**
- **他方、攻撃がもう一方の端までにあるならば、往復経路検査は永久に失敗することだけである、このように、**IKE SA**を取りこわすことはその場合適当な行動である**

プロトコルの細部 (1)
MOBIKE向けサポートを示す

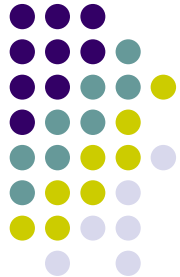
- MOBIKEが機能するために、両方のペアはIKEv2のMOBIKE拡張子を実行しなければならない。
- ペアがメッセージがもう片方のペアに理解されるかどうかに関してフィードバックの受領を確保する三つの方法
  - IKEv2メッセージ発信を使用する
  - 初期のIKEv2交換の間に交換されるVendor IDペイロードを使用する
  - Notifyペイロードを使用する

プロトコルの細部 (2)
経路テストとウインドーサイズ



- IKEv2には送信されるメッセージのウインドウがあって、送付者がそのウインドウに違反することができない
  - 即ち、ウインドウがいっぱいならば 、次に送付者はパケットを送ることができない
- IKEv2には、1のウインドサイズがある= 新しい交換を始める前に、進行中の交換を終える必要がある

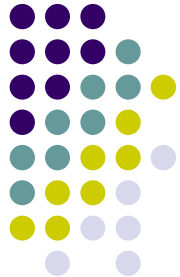
プロトコルの細部（3）
アドレスセットの更新



- Initiatorは応答者に使用されたすべてのアドレスを知ることが必要である
- 応答者はinitiatorに知られなかったアドレス更新を通知するのが必要である
- Working groupは両端が通信相手に彼らのアドレスの完全なリストを送るプロトコルフォーマットを使うことに決めた
- NAT-Tを支持するために、受けられたパケットのIP-アドレスはペアの1つのアドレスであるとみなされる

セキュリティに関する考慮事項

- すべてのパケットがIKEv2によって既に認証されるとき、どんな攻撃者もパケットのコンテンツを変更するだろうというリスクが全くない
- 攻撃者はアドレスが働いていないペアを混乱させるための努力におけるICMPエラーメッセージをだますことができる。最悪の場合で、これはサービス妨害やnon-preferred addressの使用を引き起こす
- MOBIKEプロトコルで注意される必要がある1種類の攻撃は、爆破攻撃タイプである。



終わり