

BÀI 4. AN TOÀN AN NINH TRÊN HẠ TẦNG TRUYỀN DẪN

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

1

1. AN TOÀN BẢO MẬT TẦNG VẬT LÝ VÀ TẦNG LIÊN KẾT DỮ LIỆU

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

2

2

Các nguy cơ tấn công

- Nghe lén:
 - Với các mạng quảng bá (WiFi, mạng hình trục, mạng sao dùng hub): dễ dàng chặn bắt các gói tin
 - Với các mạng điểm-điểm:
 - ✓ Đoạt quyền điều khiển các nút mạng
 - ✓ Chèn các nút mạng một cách trái phép vào hệ thống
 - Công cụ phân tích: tcpdump, Wireshark, thư viện winpcap, thư viện lập trình Socket
- Giả mạo thông tin: tấn công vào giao thức ARP, VLAN, cơ chế tự học MAC của hoạt động chuyển mạch
- Phá hoại liên kết: chèn tín hiệu giả, chèn tín hiệu nhiễu, chèn các thông điệp lỗi...
- Thông thường tấn công vào mạng LAN do kẻ tấn công bên trong gây ra.

3

3

Tấn công nghe lén trên tầng vật lý

- Nghe trộm tín hiệu trên cáp đồng



Faulty Amplifier



Wire Tap

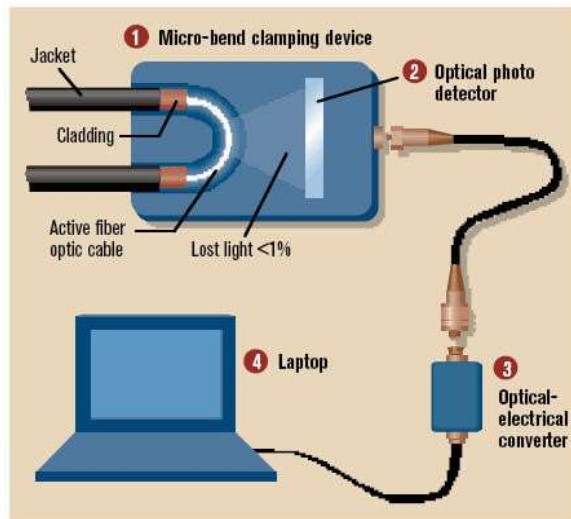


4

4

Tấn công nghe lén trên tầng vật lý

- Nghe trộm tín hiệu trên cáp quang



5

5

AN TOÀN BẢO MẬT MẠNG WLAN

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

6

6

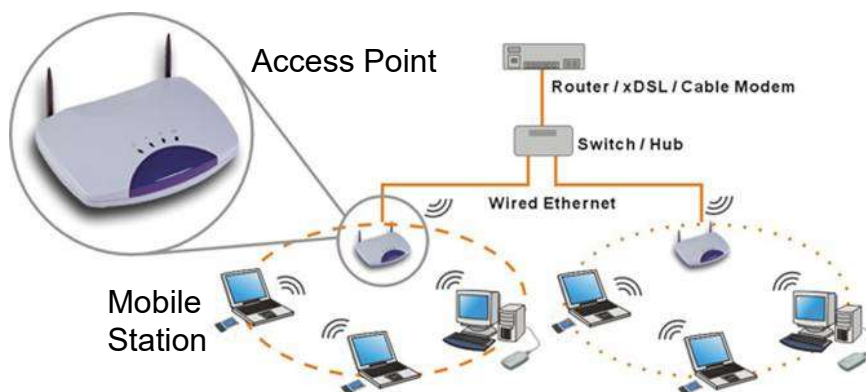
Giới thiệu chung

- WLAN (Wireless Local Area Network) là mạng máy tính liên kết 2 hay nhiều thiết bị sử dụng môi trường truyền dẫn vô tuyến
- Chuẩn IEEE 802.11 gốc chính thức được ban hành năm 1997
- IEEE 802.11x (chuẩn WiFi) biểu thị một tập hợp các chuẩn WLAN được phát triển bởi ủy ban chuẩn hóa IEEE LAN/MAN (IEEE 802.11)
 - IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n các chuẩn quy định hạ tầng và công nghệ truyền dẫn
 - IEEE802.11i: chuẩn quy định về các giao thức bảo mật trong WLAN
 - ...
- IEEE802.1X: điều khiển truy cập cho WLAN

7

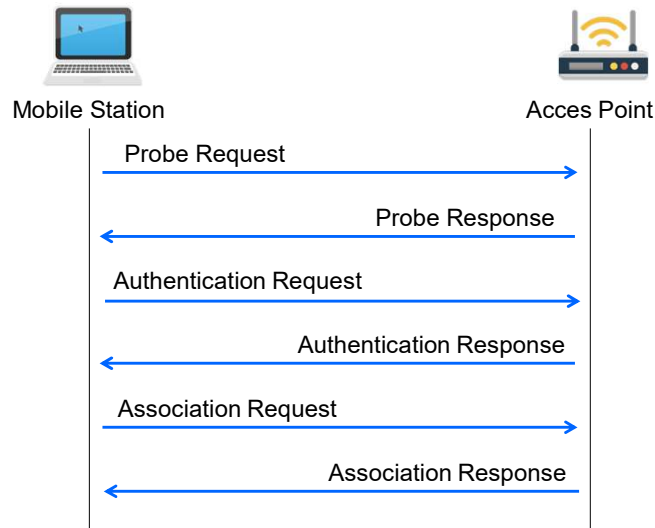
Cấu trúc của WLAN

- Một WLAN thông thường gồm có 2 phần: các thiết bị truy nhập không dây (Mobile Station-MS), các điểm truy nhập (Access Points – AP).



8

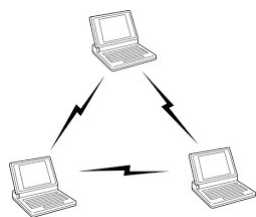
Giao thức kết nối mạng WLAN



9

9

Các mô hình triển khai



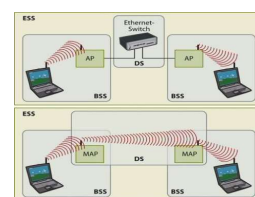
Ad-hoc

- Không cần AP
- Kết nối ngang hàng



BSS

- Kết nối tập trung



ESS

- Kết nối tập trung
- Mở rộng bằng cách kết nối các BSS

10

Vấn đề ATBM trên mạng không dây

- Sử dụng sóng vô tuyến để truyền dẫn dữ liệu
 - dễ dàng có thể thu bắt sóng và phân tích để lấy dữ liệu
 - dễ dàng kết nối và truy cập
 - dễ dàng can nhiễu
 - dễ dàng để tấn công man-in-the-middle

11

Coffee Shop

1. Kết nối mạng WiFi



Thiết lập kết nối
(**Có thể** thực hiện các giao thức
xác thực, mã hóa bảo vệ)

12

12

Coffee Shop

WEP Open:
Không thực hiện các giao thức xác thực, mã hóa bảo vệ

Dễ dàng nghe lên thông tin

Eve 13

13

Coffee Shop

WEP Shared:
- Xác thực bằng pre-shared key
- Mã hóa bằng RC4, 40 bit

Bẻ khóa trong khoảng < 1 phút

Eve 14

14

Coffee Shop

WPA/WPA2:

- **Xác thực:** Tùy thuộc chế độ
- **WPA:** Mã hóa bằng RC4, 128 bit
- **WPA2:** Mã hóa bằng AES-128



SSID: WifiStation
password: guessme!



15

15

Coffee Shop


WPA2 Personal

WifiStation
Connecting


Enter the network security key

guessme!

Next
Cancel



SSID: WifiStation
password: guessme!



Laptop và AP cùng tính toán:

$$K = \text{PBKDF2}(\text{HMAC-SHA-1}, \text{password}, \text{SSID}, \text{SSID_length}, 4096, 256)$$


16

16

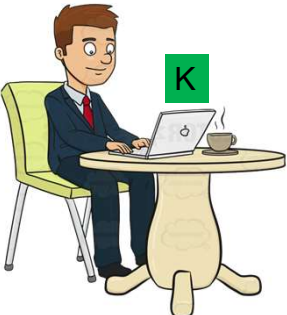
Coffee Shop

WPA2 Personal

K



SSID: WifiStation
password: guessme!



Laptop và AP cùng chia sẻ giá trị bí mật K. Giá này được sử dụng để sinh khóa dùng cho quá trình mã hóa và xác thực dữ liệu trao đổi giữa 2 bên


17

17

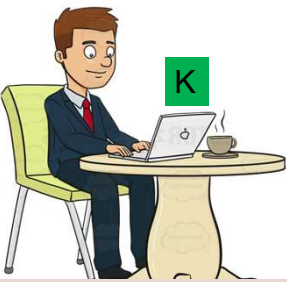
Coffee Shop

WPA2 Personal

K




SSID: WifiStation
password: guessme!



Tấn công nghe lén thụ động

Nếu mật khẩu được giữ bí mật, Eve cần thực hiện tấn công vét cạn hoặc tấn công từ điển để đoán mật khẩu.
Tốc độ rất chậm do hàm PBKDF2 thực hiện vòng lặp.

Laptop và AP cùng tính toán:
 $K = \text{PBKDF2}(\text{HMAC-SHA-1}, \text{password}, \text{SSID}, \text{SSID_length}, 4096, 256)$



Eve 18

18

Coffee Shop

WPA2 Personal

Tấn công nghe lén thụ động

K

SSID: WifiStation
password: guessme!

Tất nhiên, đơn giản hơn,
Eve có thể mua một ly café
và có được mật khẩu truy
cập → tính toán khóa K và
giải mã các gói tin bắt được

Laptop và AP cùng tính toán:

$$K = \text{PBKDF2}(\text{HMAC-SHA-1}, \text{password}, \text{SSID}, \text{SSID_length}, 4096, 256)$$

Eve 19

19

Coffee Shop

WPA2 Enterprise – An toàn hơn nhưng
triển khai cũng phức tạp hơn

HEY SSID, TÔI MUỐN KẾT NỐI VỚI ANH!

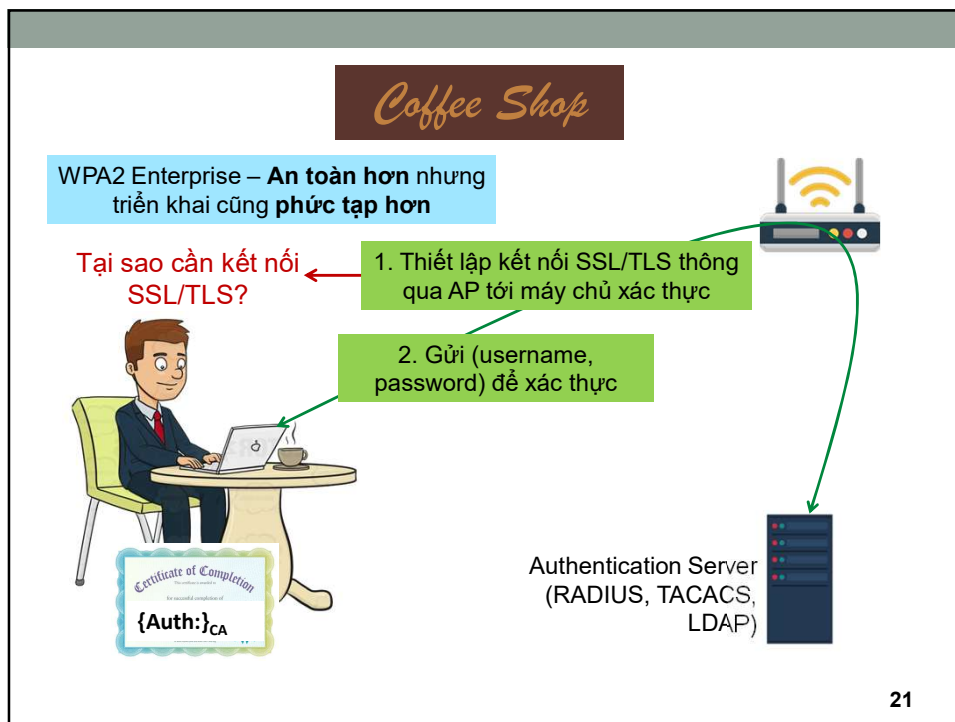
HÃY XÁC THỰC VỚI AS TRƯỚC!

Certificate of Completion
for successful completion of
{Auth:}CA

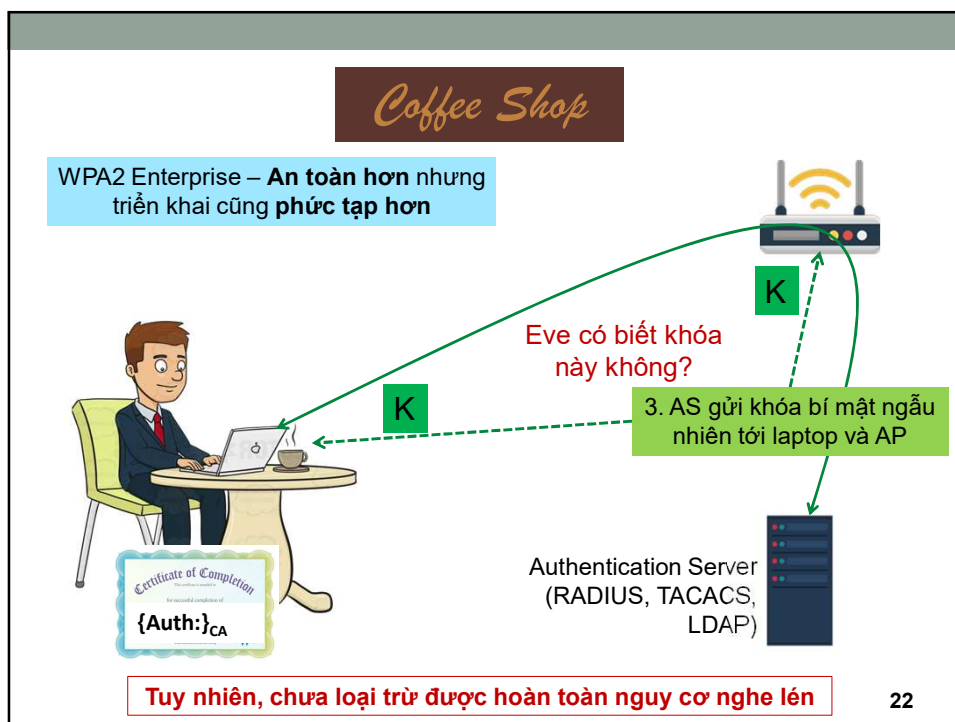
Authentication Server
(RADIUS, TACACS,
LDAP...)

20

20



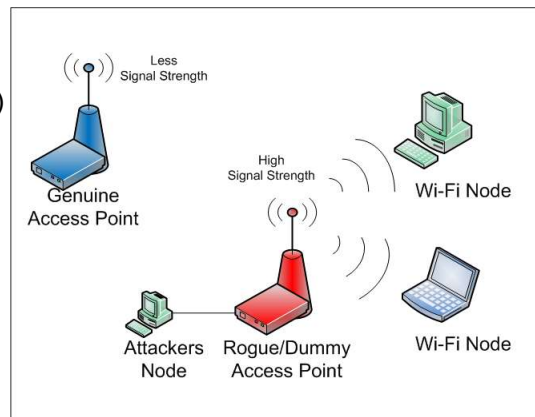
21



22

Các nguy cơ các trong mạng WLAN

- Chèn sóng (jamming): Cố tình gây nhiễu bằng cách phát ra tín hiệu cùng tần số với công suất lớn hơn
- Mục đích:
 - Giả mạo máy trạm
 - Giả mạo AP(Rogue AP)
 - DoS: phá kết nối giữa máy trạm và AP



23

23

Các nguy cơ khác trong mạng WLAN

- Disassociation: gửi disassociation frame tới máy trạm hoặc AP để ngắt kết nối đã được thiết lập
- Deauthentication attack: gửi deauthentication frame tới máy trạm để yêu cầu xác thực lại
- Mục đích: kết hợp 2 loại tấn công
 - Bắt, phân tích tải để tìm SSID ẩn
 - Đánh lừa máy trạm khi thực hiện kết nối lại sẽ kết nối với AP giả mạo
- Giả mạo AP (Rogue AP):
 - Thu thập thông tin xác thực giữa AP và máy trạm
 - Nghe lén chủ động
 - Tấn công man-in-the-middle
 - Phòng chống: sử dụng các công cụ quản trị mạng để phát hiện sự có mặt của thiết bị lạ

24

24

NGUY CƠ AN TOÀN BẢO MẬT TRONG MẠNG LAN

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

25

25

Tấn công cơ chế tự học MAC (chuyển mạch)

- Tấn công MAC flooding: gửi hàng loạt các gói tin với địa chỉ MAC nguồn là giả → bảng MAC bị tràn → Các gói tin thực sự bắt buộc phải chuyển tiếp theo kiểu quảng bá:
 - Gây bão quảng bá → chiếm dụng băng thông đường truyền, tài nguyên của các nút mạng khác
 - Nghe trộm thông tin
- Giả mạo địa chỉ MAC
- Phòng chống: Port Security

26

26

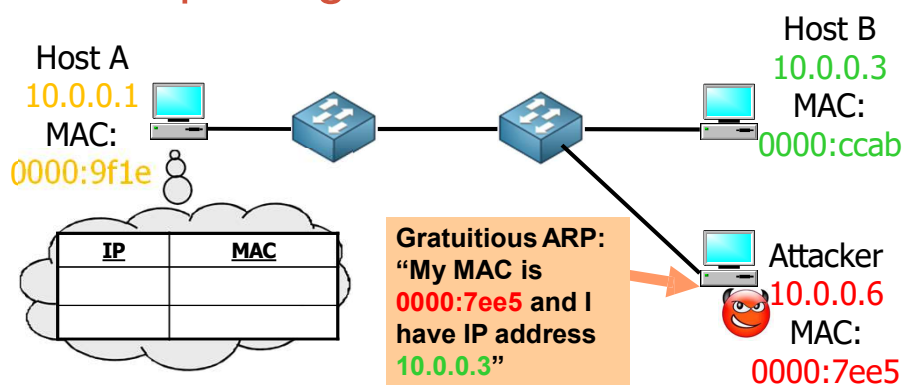
Tấn công giao thức ARP

- Address Resolution Protocol: tìm địa chỉ MAC tương ứng với địa chỉ IP
- Sử dụng phương thức quảng bá ARP Request:
 - Không cần thiết lập liên kết
- Không có cơ chế xác thực ARP Response
- Tấn công:
 - Giả mạo: ARP Spoofing
 - DoS
- Phòng chống: Dynamic ARP Inspection

27

27

ARP Spoofing



- Đặc biệt nguy hiểm khi đưa địa chỉ MAC giả mạo gateway router, Local DNS Server:
 - Nghe lén
 - Man-in-the-middle

28

28

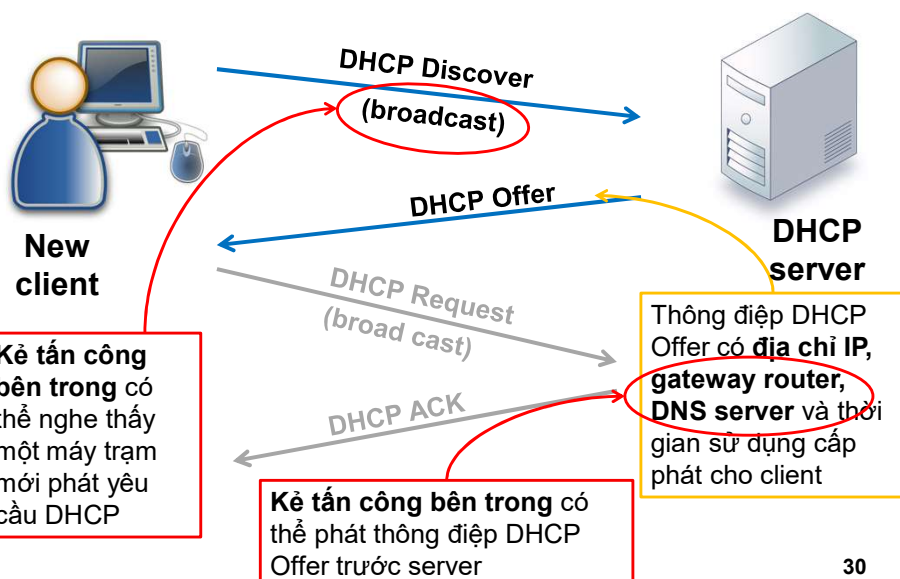
Tần công dịch vụ DHCP

- Dynamic Host Configuration Protocol
- Cấp phát các cấu hình IP tự động cho máy trạm:
 - Địa chỉ IP
 - Địa chỉ gateway router
 - Địa chỉ DNS server
- Sử dụng UDP, cổng 67(server) và 68(client)

29

29

Hoạt động của DHCP



30

30

Các nguy cơ tấn công DHCP

- Lỗi hỏng: Bất kỳ máy trạm nào yêu cầu cũng được cấp phát địa chỉ IP
 - Nguy cơ: Tấn công DoS làm cạn kho địa chỉ(DHCP Starvation)
- Lỗi hỏng: Không xác thực cho các thông tin cấp phát từ DHCP server → DHCP Spoofing
 - Nguy cơ: Thay địa chỉ DNS server tin cậy bằng địa chỉ DNS của kẻ tấn công.
 - Nguy cơ: Thay địa chỉ default router, cho phép kẻ tấn công:
 - ✓ Chặn bắt, do thám thông tin
 - ✓ Tấn công phát lại
 - ✓ Tấn công man-in-the-middle
 - Phòng chống: DHCP Snooping

31

31

Tấn công trên VLAN

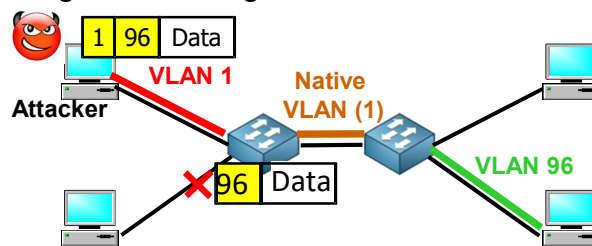
- VLAN: miền quảng bá logic trên các switch → phân tách các lưu lượng mạng ở tầng 2
- Các cơ chế ATBM có thể triển khai trên VLAN: điều khiển truy cập (access control), cách ly tài nguyên quan trọng
- Các VLAN được gán các dải địa chỉ IP khác nhau
- Các khung tin Ethernet được gắn thêm VLAN tag (802.1Q hoặc ISL)
- Chuyển mạch chỉ thực hiện trong 1 VLAN
- Trao đổi dữ liệu giữa các VLAN: định tuyến (inter VLAN routing)

32

32

Tấn công: VLAN hopping

- Mục đích: truy cập vào các VLAN khác từ Native VLAN
- Lỗi hổng: các dữ liệu chuyển trong Native VLAN không cần gắn tag
- Đánh lừa switch chuyển tiếp các gói tin vào VLAN
- Double-tag attack trên giao thức IEEE 802.1Q



- Phòng chống?

33

33

Tấn công VLAN: DTP và VTP

- Dynamic Trunking Protocol: tự động cấu hình chế độ trunking cho các cổng của VLAN
 - Tấn công giả mạo các gói tin DTP để lừa 1 switch kết nối vào VLAN của kẻ tấn công
 - Phòng chống: Tắt chế độ dynamic, gán chế độ access cho các cổng của switch
- VLAN Trunking Protocol: tự động chuyển tiếp thông tin cấu hình VLAN từ VTP server tới các VTP client
 - Tấn công giả mạo các gói tin để xóa 1 VLAN (DoS) hoặc thêm 1 VLAN gồm tất cả các switch (tạo bão quảng bá – broadcast storm)
 - Phòng chống: chỉ định VTP trên các cổng tin cậy, thiết lập cơ chế xác thực cho VTP

34

34

Tấn công giao thức STP

- Spanning Tree Protocol: khử loop trên mạng kết nối switch có vòng kín
- Bầu chọn root:
 - Mỗi nút có giá trị priority (mặc định là 38464)
 - Các nút trao đổi thông điệp BPDU chứa giá trị priority
 - Nút có priority nhỏ nhất trở thành root
 - Nếu có nhiều switch cùng priority, switch có cổng địa chỉ MAC nhỏ nhất là root
- Thiết lập cây khung: các nút còn lại
 - Mỗi nút còn lại tìm đường đi ngắn nhất tới nút gốc (giá của liên kết xác định dựa trên bảng thông)
 - Giữ cổng gần nút gốc nhất hoạt động, tạm ngắt các cổng "xa" nút gốc hơn
- STP không có cơ chế xác thực

35

35

Tấn công giao thức STP

- Tấn công vào STP: đoạt quyền root switch
 - DoS: black-hole attack, flooding attack
 - Chèn dữ liệu giả mạo vào luồng trao đổi thông tin
 - Tấn công man-in-the-middle
- Tấn công DoS: BPDU Flooding
- Phòng chống:
 - Root guard
 - BPDU guard
 - BPDU filtering

36

36

3. AN TOÀN BẢO MẬT TẦNG LIÊN MẠNG

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

37

37

Giao thức IP và ICMP

- Internet Protocol:
 - Giao thức kết nối liên mạng
 - Hướng không kết nối (connectionless), không tin cậy
- Internet Control Message Protocol
 - Nằm trên giao thức IP
 - Hướng không kết nối (connectionless), không tin cậy
 - Kiểm tra trạng thái hoạt động của các nút mạng khác
- Vấn đề của giao thức IP và ICMP:
 - Không cần thiết lập liên kết: có thể lợi dụng để quét mạng
 - Dễ dàng giả mạo địa chỉ IP nguồn trên các gói tin
 - Có thể gửi liên tục với số lượng lớn các gói tin → tấn công từ chối dịch vụ

38

38

AN TOÀN BẢO MẬT CÁC GIAO THỨC ĐỊNH TUYẾN

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

39

39

Giới thiệu chung về định tuyến

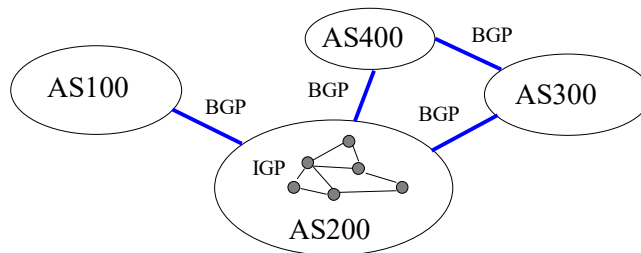
- Định tuyến: tìm ra đường đi ngắn nhất tới các mạng đích
 - Bảng định tuyến: lưu thông tin đường đi
- Định tuyến tĩnh: người dùng định nghĩa nội dung của bảng định tuyến → an toàn nhưng không cập nhật theo sự thay đổi trạng thái của các liên kết
- Định tuyến động: router tự động xây dựng nội dung bảng định tuyến
- Đặc điểm của định tuyến trong mạng IP:
 - Mỗi nút chỉ chắc chắn về các thông tin cục bộ
 - Các nút trao đổi thông tin định tuyến theo cơ chế flooding

40

40

Định tuyến trên mạng Internet

- Chia thành các vùng tự trị định tuyến AS
 - Thường được đăng ký và quản lý bởi ISP
- Phân cấp:
 - Định tuyến nội vùng(IGP): RIP, OSPF, IGRP, EIGRP
 - Định tuyến ngoại vùng(EGP): BGP



41

41

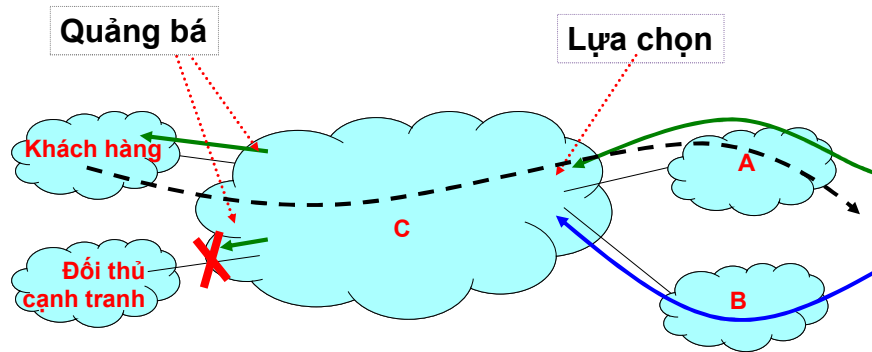
Hoạt động của BGP(tóm tắt)

- Hỗ trợ định tuyến không phân lớp
- Tìm đường tới các vùng tự trị (AS)
- Trao đổi thông điệp BGP với hàng xóm qua kết nối TCP
- Mỗi router quảng bá thông tin đường đi tới các router khác bằng bản tin UPDATE
 - Thông tin đường đi: danh sách các AS trên đường đi tới AS đích
- Thực hiện các chính sách trong quá trình chọn đường
 - Lựa chọn đường ra
 - Quảng bá đường vào
 - ...

42

42

BGP: Chính sách lựa chọn-quảng bá

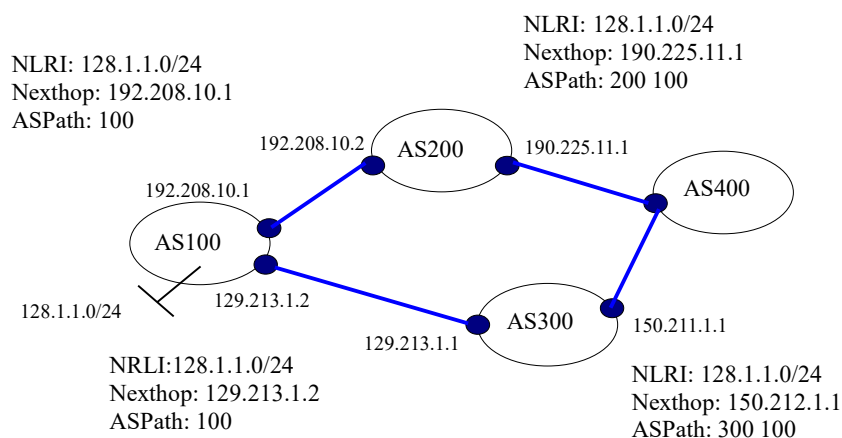


- **Lựa chọn:** Đường đi nào được dùng để chuyển dữ liệu tới AS đích?
 - Kiểm soát thông tin ra khỏi AS
- **Quẳng bá:** Quảng bá cho AS khác đường đi nào?
 - Kiểm soát thông tin vào AS

43

43

Hoạt động của BGP – Ví dụ



44

44

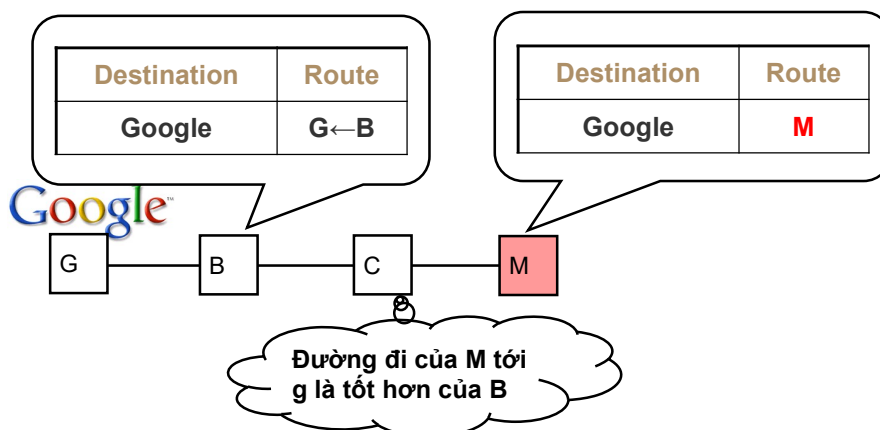
Tấn công các giao thức định tuyến

- RIPv1: không hỗ trợ các cơ chế xác thực thông tin trao đổi giữa các nút → khai thác tấn công thay đổi, giả mạo thông tin
- RIPv2, OSPF, BGP: hỗ trợ cơ chế xác thực sử dụng pre-shared key
 - Khóa không ngẫu nhiên, do người dùng lựa chọn
- OSPF: Lợi dụng cơ chế quảng bá thông tin LSA giả để tấn công DoS (black-hole attack)
- BGP: Giả mạo thông tin định tuyến để điều hướng dữ liệu → Hậu quả: tấn công từ chối dịch vụ, man-in-the-middle, thư rác...

45

45

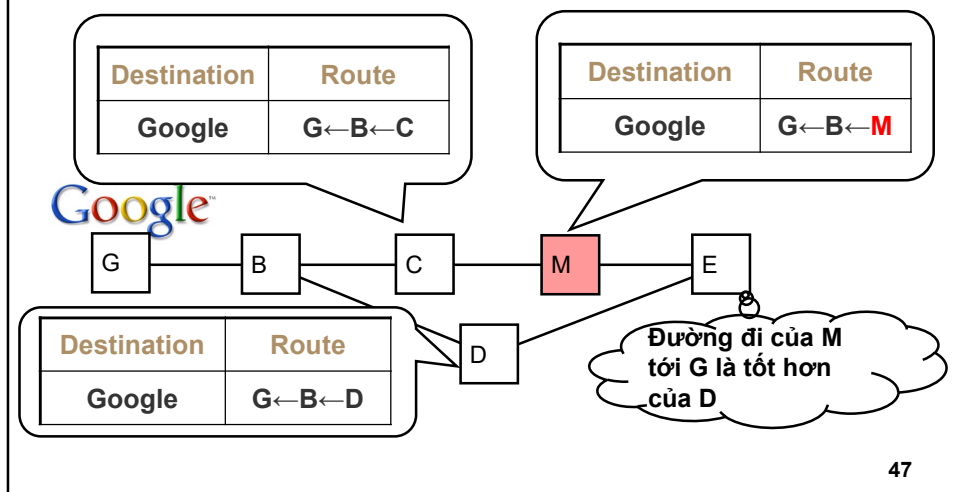
Tấn công BGP: Giả mạo thông tin đường đi



46

46

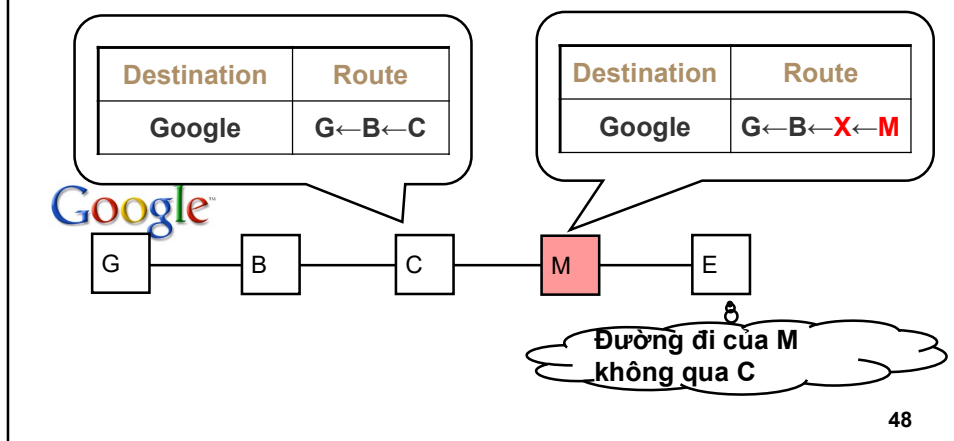
Tấn công BGP: Giả mạo thông tin đường đi



47

Tấn công BGP: Giả mạo thông tin đường đi

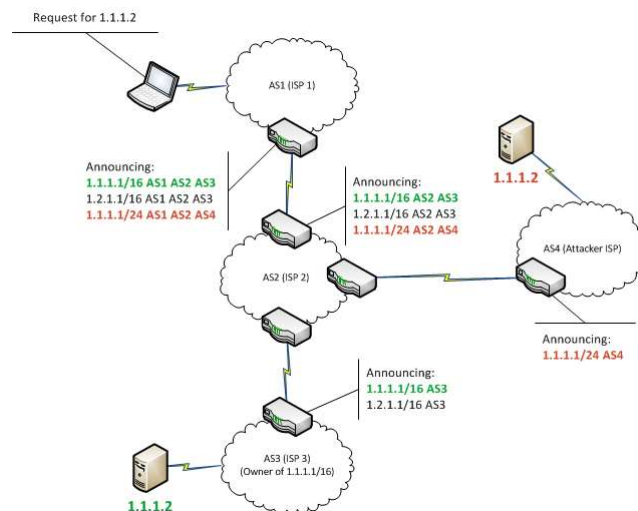
- Chính sách của E: Không lựa chọn đường đi qua C



48

Tấn công BGP: Path hijack

- Lợi dụng cơ chế Longest Matching



49

49

BGP hijacking – Ví dụ

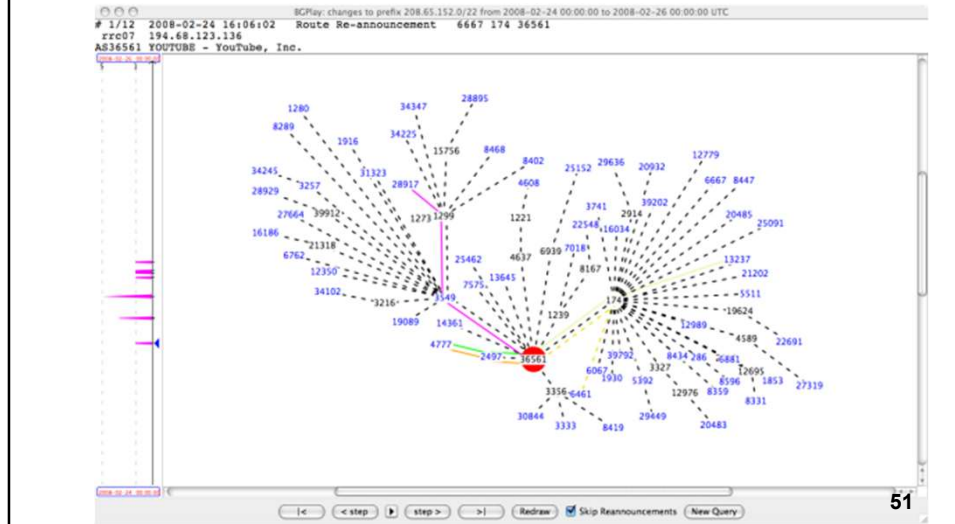
- Tháng 02/08: chính phủ Pakistan ngăn cản các truy cập vào trang Youtube:
 - Địa chỉ của Youtube: 208.65.152.0 /22
 - youtube.com: 208.65.153.238 /22
 - Pakistan Telecom loan báo một thông tin định tuyến BGP tới mạng 208.65.153.0 /24 → các router trên Internet cập nhật đường đi mới theo quy tắc longest matching → bị đánh lừa youtube.com nằm ở Pakistan → không thể truy cập youtube.com trong 2 giờ
- Tháng 03/2014: dịch vụ DNS của bị Google tấn công với địa chỉ 8.8.8.8/32
 - Không thể truy cập được từ một số nước ở Nam Mỹ trong 22 phút

50

50

BGP hijacking - Youtube

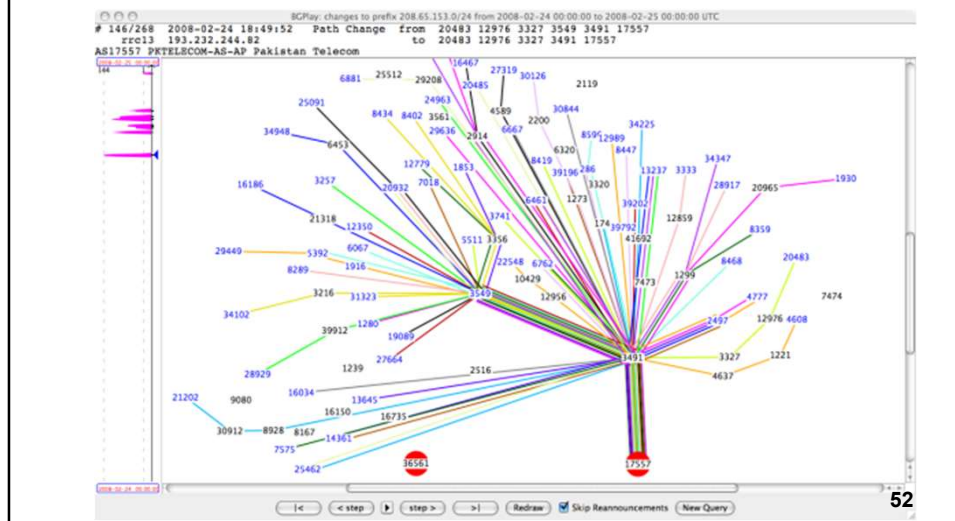
- AS36561(Youtube) loan báo về đường đi tới địa chỉ 208.65.152.0/22



51

BGP hijacking - Youtube

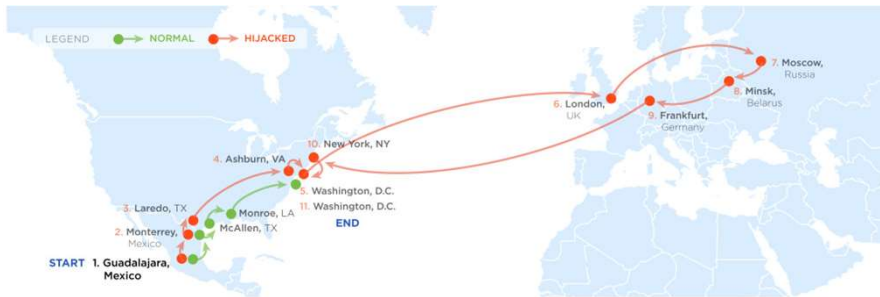
- AS17557 (Pakistan Telecom) loan báo đường đi tới địa chỉ 208.65.153.0/24 trong 2 phút



52

BGP hijacking – Ví dụ

- Tháng 2/2013: đường đi từ các AS Guadalajara tới WashingtonDC chuyển hướng qua Belarus trong vài giờ
 - Đường đi đúng: Alestra (Mexico) → PCCW (Texas) → Qwest (DC)



- Tương tự: tấn công tấn công Dell SecureWorks năm 2014, ISP của Italia vào 6/2015

53

53

Yêu cầu bảo mật với BGP

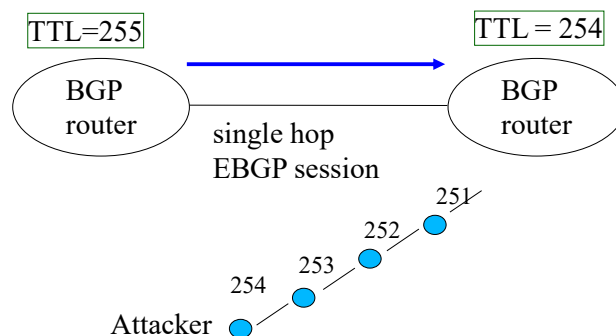
- Xác minh được “sự sở hữu” không gian địa chỉ: router BGP có thực sự kết nối tới AS sử dụng địa chỉ IP đó không?
- Xác thực giữa các AS
- Xác thực và ủy quyền cho các router trong AS
 - Quảng bá địa chỉ
 - Quảng bá đường đi
- Kiểm tra tính toàn vẹn, chính xác và tính đúng thời điểm của toàn bộ lưu lượng BGP

54

54

Phòng chống tấn công BGP

- Gửi thông điệp BGP cho hàng xóm với giá trị TTL trên gói tin IP là 255
- Từ chối tất cả các gói tin có TTL < 254
- Hạn chế: chỉ chống lại tấn công bằng giả mạo mà không xuất phát từ router hàng xóm



55

55

Phòng chống tấn công BGP

Xác thực với MD5 và pre-share-key

- Hai router hàng xóm được cấu hình để chia sẻ một giá trị bí mật
- ```
(config-router) # neighbor addr password passphrase
```
- Các gói tin TCP mang theo thông điệp BGP trường Options chứa mã băm  $MD5(BGP\ message || passphrase)$  để xác thực
  - Chỉ chống lại tấn công giả mạo thông tin định tuyến từ bên ngoài
  - Nguy cơ: không chống lại được tấn công giả mạo thông tin định tuyến từ router trong mạng

56

56

## Yêu cầu bảo mật với BGP

- Xác minh được “sự sở hữu” không gian địa chỉ: router BGP có thực sự kết nối tới AS sử dụng địa chỉ IP đó không?
- Xác thực giữa các AS
- Xác thực và ủy quyền cho các router trong AS
  - Quảng bá địa chỉ
  - Quảng bá đường đi
- Kiểm tra tính toàn vẹn, chính xác và tính đúng thời điểm của toàn bộ lưu lượng BGP

57

57

## Secure BGP(S-BGP)

- Cấp phát chứng thư số theo mô hình phân cấp:
  - ICANN cấp phát chứng thư số (certificate) chứng thực quyền sở hữu địa chỉ cho AS
  - AS cấp phát chứng thư số cho các router của nó
- Tạo chứng thực địa chỉ IP(Address Attestation-AA) và gửi cho các AS:
  - Ký bởi chứng thư do ICANN phát hành
  - Thông tin được phân phối ngoài lưu lượng BGP (out-of-band)
- Chứng thực thông tin đường đi(Route Attestation-RA):
  - Loan báo thông tin đường đi bằng các thông điệp BGP Update
  - Mỗi router ký lên thông điệp BGP Update mà nó phát đi bằng chứng thư do AS cấp phát
- Có thể sử dụng thêm IPSec để bảo mật thông tin

58

58

## Xử lý Thông điệp S-BGP Update

Giả sử router A(thuộc AS1) gửi thông điệp S-BGP Update để loan báo thông tin về AS của nó tới router B( thuộc AS2)

1. Nhận AA cho địa chỉ IP mà AS sở hữu:  $\text{Sig}(\text{KR}_{\text{AS1}}, \text{IPprefix})$
2. Tạo  $\text{RA}_1$  với AS2 là next-hop của tuyến đường:  $\text{Sig}(\text{KR}_A, \text{AS1} \rightarrow \text{AS2})$
3. A gửi thông điệp S-BGP Update cho B. Cấu trúc của thông điệp gồm AA || Path vector ||  $\text{RA}_1$
4. B kiểm tra AA và RA bằng khóa công khai tương ứng
5. B xác minh nó là next-hop của tuyến đường
6. B tạo  $\text{RA}_2$  với C(một router trên AS khác) là next-hop và chuyển thông điệp cho C

- Tại sao S-BGP chống lại được các dạng tấn công đã nêu?

59

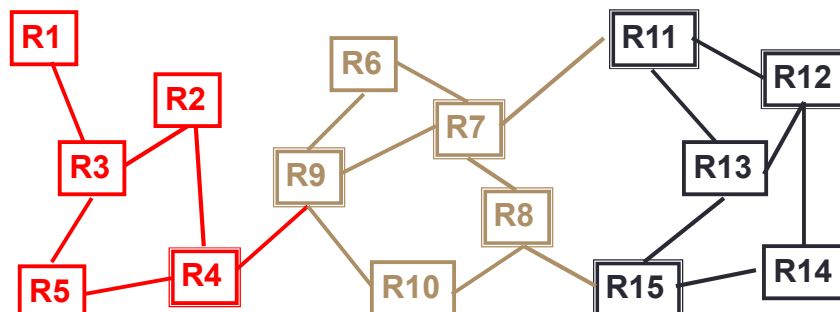
59

## Thông điệp S-BGP Update –Ví dụ

AA:  $\text{Sig}(\text{KR}_{\text{AS1}}, \text{IP\_prefix})$

R4  $\rightarrow$  R9: AA || [path: AS1] ||  $\text{Sig}(\text{KR}_{\text{R4}}, \text{AS1} \rightarrow \text{AS2})$

R7  $\rightarrow$  R11: AA || [path: AS1, AS2] ||  $\text{Sig}(\text{KR}_{\text{R4}}, \text{AS1} \rightarrow \text{AS2})$  ||  $\text{Sig}(\text{KR}_{\text{R7}}, \text{AS1} \rightarrow \text{AS2} \rightarrow \text{AS3})$



60

60

## Khó khăn khi triển khai S-BGP

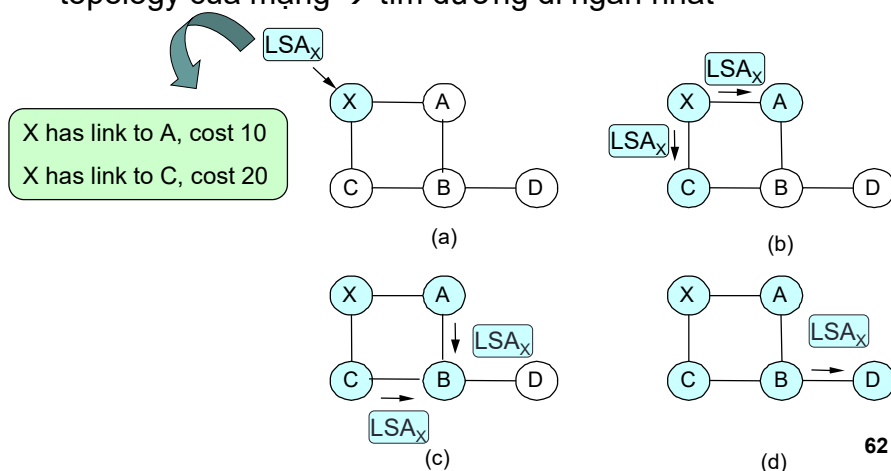
- Độ phức tạp tính toán của các thuật toán mật mã
- Chỉ thực sự hiệu quả nếu tất cả các AS cùng cài đặt
- Phức tạp khi mở rộng
- Hiện trạng:
  - Khoảng 5% số AS hỗ trợ S-BGP trên mạng Internet
  - Đang được vận động để trở thành một chuẩn

61

61

## Hoạt động của OSPF(tóm tắt)

- Router quảng bá thông tin liên kết LSA trên mạng
- Mỗi router thu thập các thông tin LSA → xây dựng topology của mạng → tìm đường đi ngắn nhất



62

## Các cơ chế ATBM trên OSPF

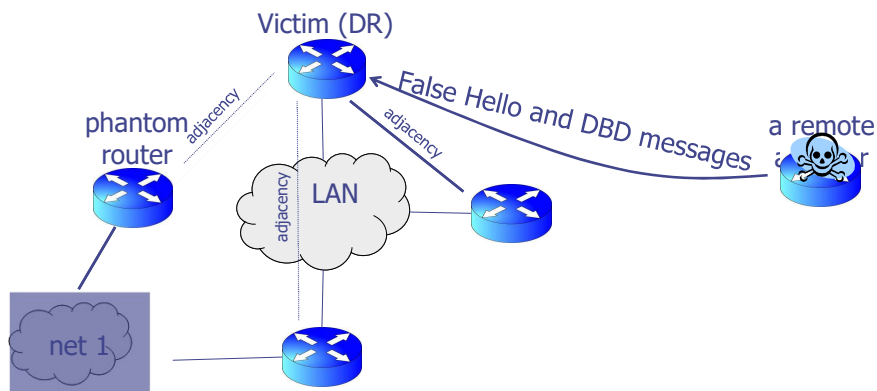
- Xác thực các bản tin LSA
  - Trên mỗi liên kết, 2 router chia sẻ một giá trị bí mật
  - Sử dụng hàm MAC để tạo mã xác thực:  
$$\text{MAC}(k, m) = \text{MD5}(\text{data} \parallel \text{key} \parallel \text{pad} \parallel \text{length})$$
- Cơ chế “fight back”: nếu router nhận được LSA của chính nó với giá trị timestamp mới hơn, ngay lập tức quảng bá bản tin LSA mới.

63

63

## Tấn công giao thức OSPF

- Kẻ tấn công gửi thông tin LSA giả mạo để các router cập nhật đường đi ngắn nhất qua router không có thực
- Ví dụ



64

64



Bài giảng sử dụng một số hình vẽ và ví dụ từ các khóa học:

- Computer and Network Security, Stanford University
- Computer Security, Berkeley University
- Network Security, Illinois University
- Computer and Network Security, University of Maryland

65