Network Security Workshop

Contact: training@apnic.net

Overview

- Network Security Fundamentals
- Security on Different Layers and Attack Mitigation
- Cryptography and PKI
- Device and Infrastructure Security
- Operational Security and Policies
- Virtual Private Networks and IPsec
- DNS Security (TSIG/DNSSEC)
- IPv6 Security
- Route Filtering

Network Security Fundamentals

Network Security Workshop

APNIC

Overview

- Why We Need Security
- Definitions and Concepts
- Access Control
- Risk vs. Vulnerability
- Threats and Attack Types

Why Security?

- The Internet was initially designed for connectivity
  - Trust assumed
  - We do more with the Internet nowadays
  - Security protocols are added on top of the TCP/IP
- Fundamental aspects of information must be protected
  - Confidential data
  - Employee information
  - Business models
  - Protect identity and resources
- We can’t keep ourselves isolated from the Internet
  - Most business communications are done online
  - We provide online services
  - We get services from third-party organizations online

Internet Evolution

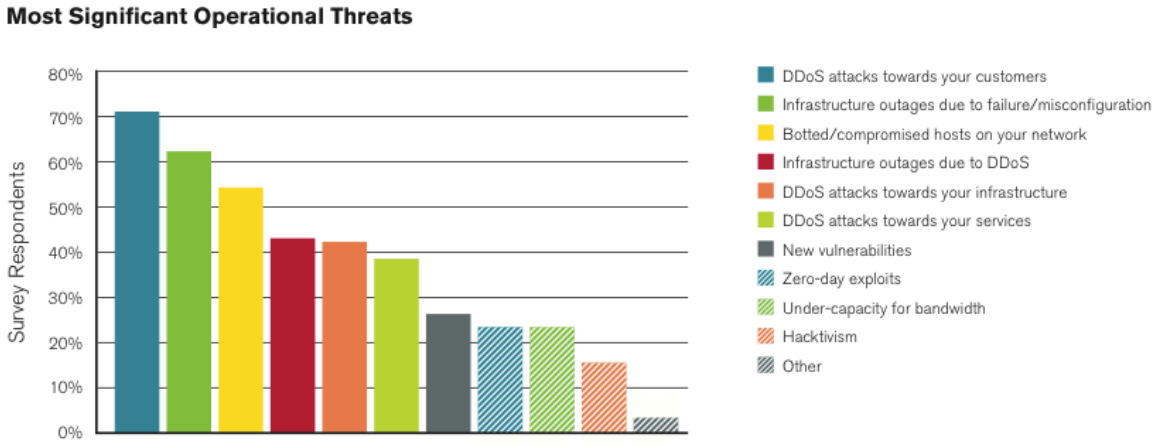
LAN connectivity

Application-specific
More online content

Cloud computing
Application/data hosted
in the cloud environment

- Different ways to handle security as the Internet evolves

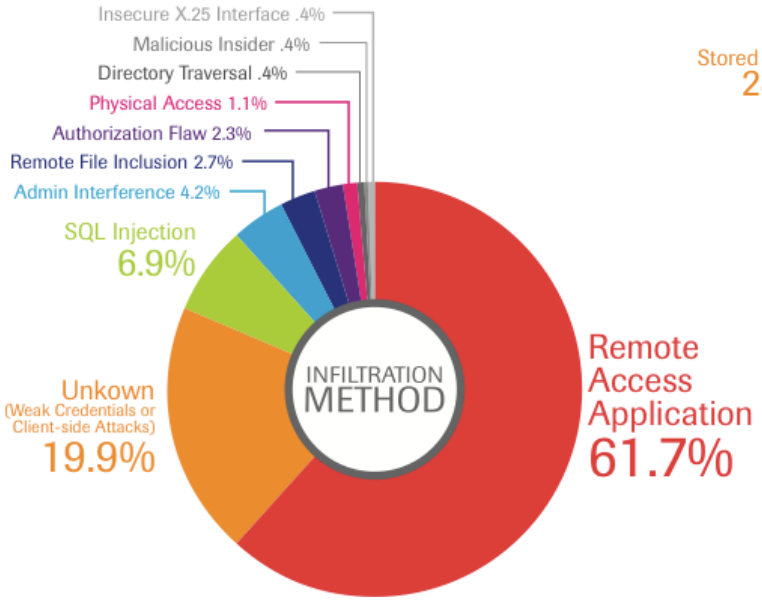
Why Security?



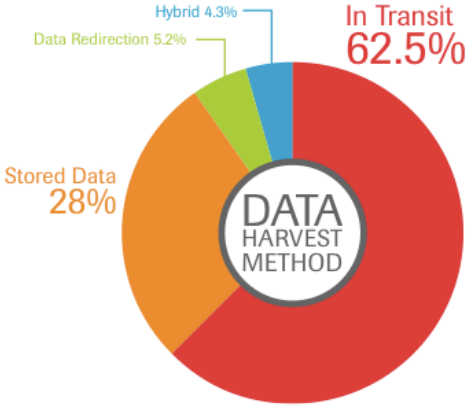
- Key findings:
  - Hacktivism and vandalism are the common DDoS attack motivation
  - High-bandwidth DDoS attacks are the ‘new normal’
  - First-ever IPv6 DDoS attacks are reported
  - Trust issues across geographic boundaries

Source: Arbor Networks Worldwide Infrastructure Security Report Volume VII

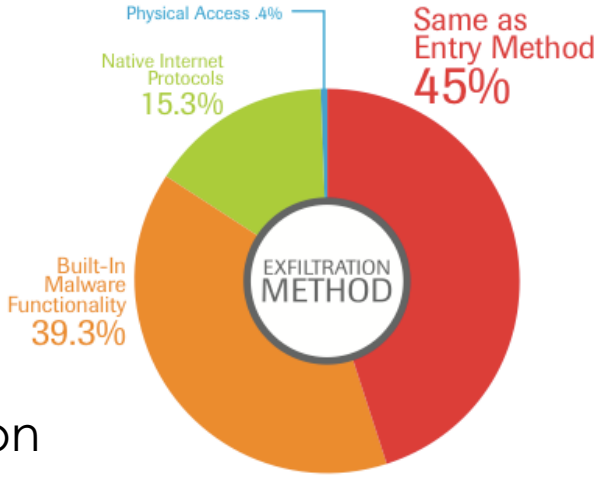
Breach Sources



Infiltration



Aggregation



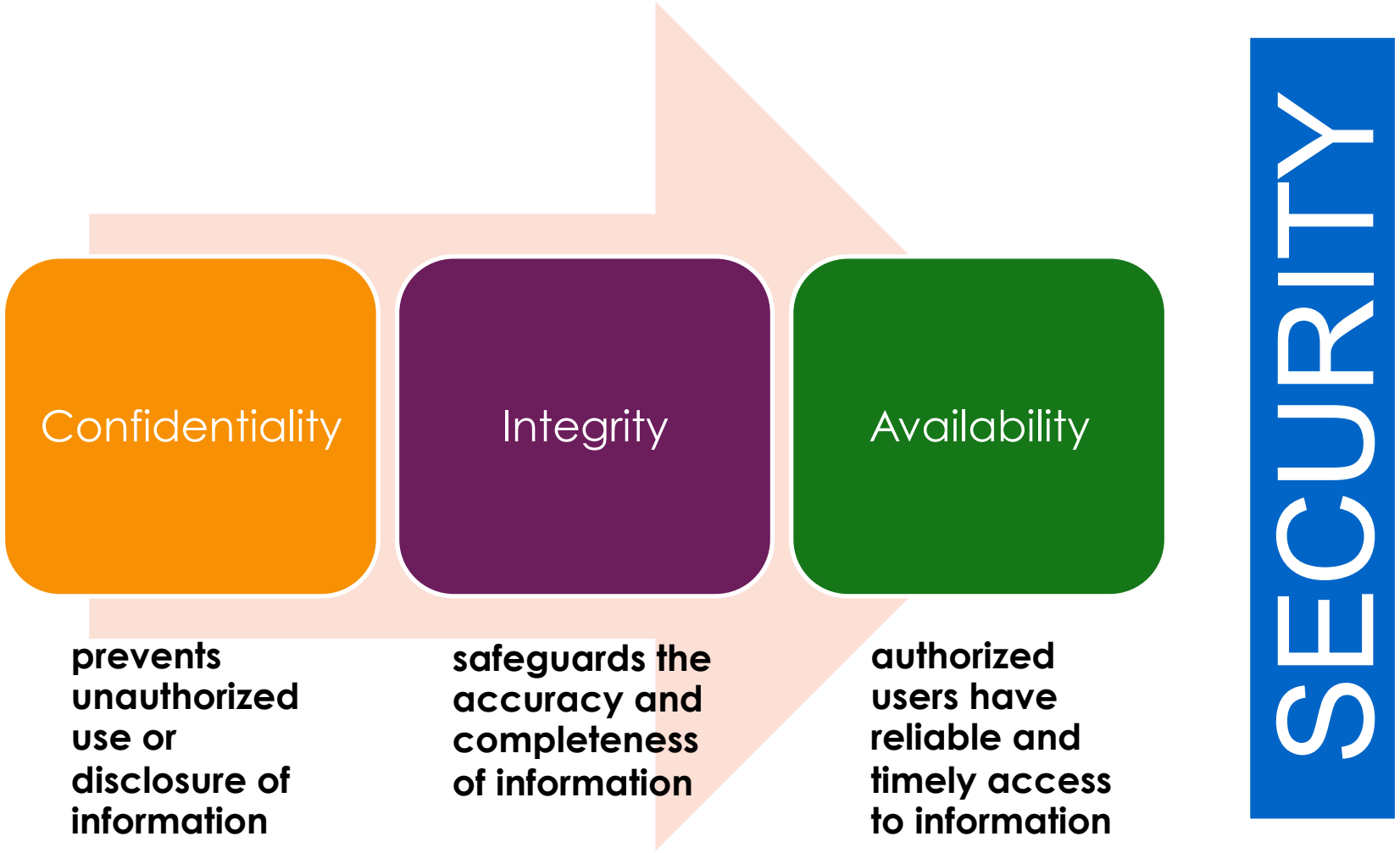
Exfiltration

Source: Trustwave 2012 Global Security Report

Types of Security

- Computer Security
  - generic name for the collection of tools designed to protect data and to thwart hackers
- Network Security
  - measures to protect data during their transmission
- Internet Security
  - measures to protect data during their transmission over a collection of interconnected networks

Goals of Information Security



Access Control

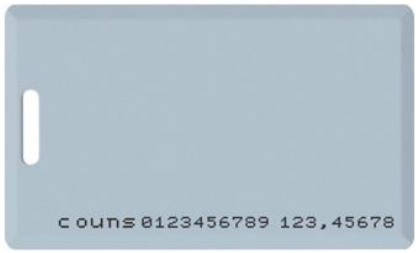
- The ability to permit or deny the use of an object by a subject.
- It provides 3 essential services:
  - Authentication (who can login)
  - Authorization (what authorized users can do)
  - Accountability (identifies what a user did)

Authentication

- A means to verify or prove a user's identity
- The term "user" may refer to:
  - Person
  - Application or process
  - Machine or device
- Identification comes before authentication
  - Provide username to establish user's identity
- To prove identity, a user must present either of the following:
  - What you know (passwords, passphrase, PIN)
  - What you have (token, smart cards, passcodes, RFID)
  - Who you are (biometrics such as fingerprints and iris scan, signature or voice)

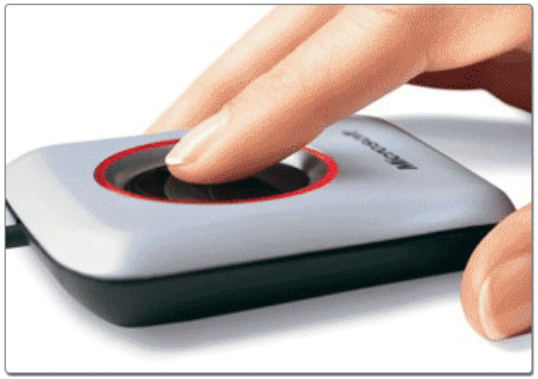
Examples of Tokens

eToken



RFID cards

Smart Cards



Fingerprint scanner

Trusted Network

- Standard defensive-oriented technologies
  - Firewall
  - Intrusion Detection
- Build TRUST on top of the TCP/IP infrastructure
  - Strong authentication
  - Public Key Infrastructure (PKI)

Strong Authentication

- An absolute requirement
- Two-factor authentication
  - Passwords (something you know)
  - Tokens (something you have)
- Examples:
  - Passwords
  - Tokens
  - Tickets
  - Restricted access
  - PINs
  - Biometrics
  - Certificates

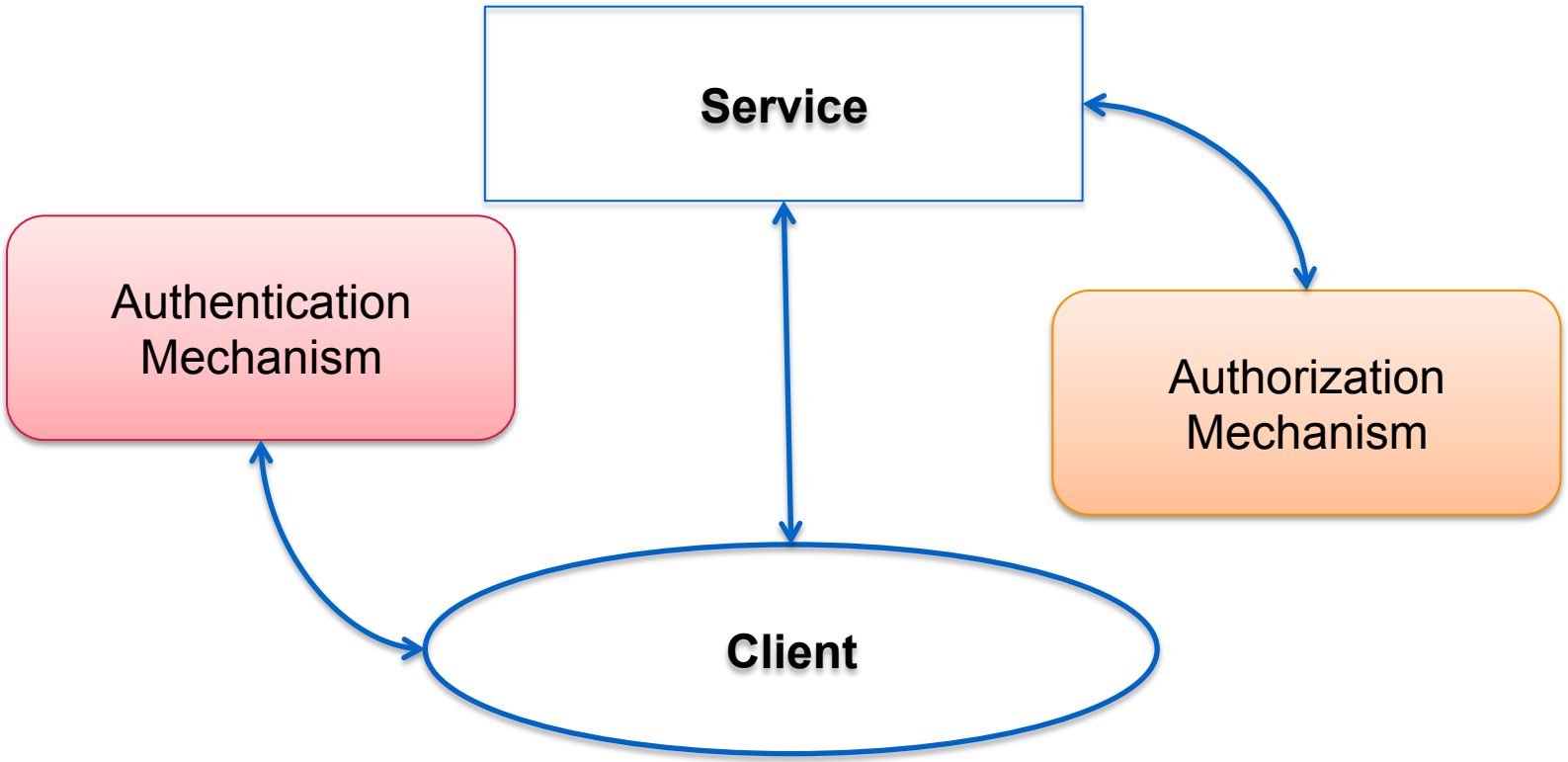
Two-factor Authentication

- Requires a user to provide at least two authentication ‘factors’ to prove his identity
  - something you know
    Username/userID and password
  - something you have
    Token using a one-time password (OTP)
- The OTP is generated using a small electronic device in physical possession of the user
  - Different OTP generated each time and expires after some time
  - An alternative way is through applications installed on your mobile device
- Multi-factor authentication is also common

Authorization

- Defines the user's rights and permissions on a system
- Typically done after user has been authenticated
- Grants a user access to a particular resource and what actions he is permitted to perform on that resource
- Access criteria based on the level of trust:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction type

Authentication vs. Authorization



“Authentication simply identifies a party, authorization defines whether they can perform certain action” – RFC 3552

Authorization Concepts

- Authorization creep
  - When users may possess unnecessarily high access privileges within an organization
- Default to Zero
  - Start with zero access and build on top of that
- Need to Know Principle
  - Least privilege; give access only to information that the user absolutely need
- Access Control Lists
  - List of users allowed to perform particular access to an object (read, write, execute, modify)

Single Sign On

- Property of access control where a user logs in only once and gains access to all authorized resources within a system.
- Benefits:
  - Ease of use
  - Reduces logon cycle (time spent re-entering passwords for the same identity)
- Common SSO technologies:
  - Kerberos, RADIUS
  - Smart card based
  - OTP Token
- Disadvantage: Single point of attack

Types of Access Control

- Centralized Access Control
  - Radius
  - TACACS+
  - Diameter
- Decentralized Access Control
  - Control of access by people who are closer to the resources
  - No method for consistent control

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
  - Senders cannot deny sending information
  - Receivers cannot deny receiving it
  - Users cannot deny performing a certain action
- Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention and after-action recovery and legal action

Source: NIST Risk Management Guide for Information Technology Systems

Integrity

- Security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity
- Data integrity
  - The property that data has when it has not been altered in an unauthorized manner
- System integrity
  - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation

Source: NIST Risk Management Guide for Information Technology Systems

Risk, Threat and Vulnerability

- Vulnerability - weakness in a system
- Risk - likelihood that a particular threat using a particular attack will exploit a particular vulnerability
- Exploit - taking advantage of a vulnerability
- Non-repudiation—assurance that both parties are involved in the transaction

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
  - Software bugs
  - Configuration mistakes
  - Network design flaw
  - Lack of encryption
- Exploit
  - Taking advantage of a vulnerability

Threat

- Any circumstance or event with the potential to cause harm to a networked system.
- These are some example of threats:
  - Denial of service
    - Attacks make computer resources (e.g., bandwidth, disk space, or CPU time) unavailable to its intended users
  - Unauthorised access
    - Access without permission issues by a rightful owner of devices or networks
  - Impersonation
  - Worms
  - Viruses

Risk

- The possibility that a particular vulnerability will be exploited
- IT-related risks arise from:
  - Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
  - Unintentional errors or omissions
  - IT disruptions due to natural or man-made disasters
  - Failure to exercise due care and diligence in implementation and operation of the IT system

Risk = Threat * Vulnerability
(* Impact)

Risk Analysis

- Identification, assessment and reduction of risks to an acceptable level
- the process of identifying security risks and probability of occurrence, determining their impact, and identifying areas that require protection
- Three parts:
  - Risk assessment – determine the possible risks
  - Risk management – evaluating alternatives for mitigating the risk
  - Risk communication – presenting this material in an understanble way to decision makers and/or the public

Risk Management vs. Cost of Security

- Risk mitigation
  - The process of selecting appropriate controls to reduce risk to an acceptable level
- The level of acceptable risk
  - Determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy
- Trade-offs between safety, cost, and availability

Attack Sources

- Active vs. passive
  - Active involves writing data to the network. It is common to disguise one's address and conceal the identity of the traffic sender
  - Passive involves only reading data on the network. Its purpose is breach of confidentiality. This is possible if:
    - Attacker has gained control of a host in the communication path between two victim machines
    - Attacker has compromised the routing infrastructure to arrange the traffic pass through a compromised machine

Active Attacks	Passive Attacks
Denial of Service attacks	Reconnaissance
Spoofing	Eavesdropping
Man in the Middle	Port scanning
ARP poisoning	
Smurf attacks	
Buffer overflow	
SQL Injection	

Source: RFC 4778

Attack Sources

- On-path vs. Off-path
  - On-path routers (transmitting datagrams) can read, modify, or remove any datagram transmitted along the path
  - Off-path hosts can transmit datagrams that appear to come from any hosts but cannot necessarily receive datagrams intended for other hosts
    - If attackers want to receive data, they have to put themselves on-path
  - How easy is it to subvert network topology?
    - It is not easy thing to do but, it is not impossible
- Insider vs. outsider
  - What is definition of perimeter/border?
- Deliberate attack vs. unintentional event
  - Configuration errors and software bugs are as harmful as a deliberate malicious network attack

Source: RFC 4778

General Threats

- Masquerade
  - An entity claims to be another entity
- Eavesdropping
  - An entity reads information it is not intended to read
- Authorization violation
  - An entity uses a service or resource it is not intended to use
- Loss or modification of information
  - Data is being altered or destroyed
- Denial of communication acts (repudiation)
  - An entity falsely denies its participation in a communication act
- Forgery of information
  - An entity creates new information in the name of another entity
- Sabotage
  - Any action that aims to reduce the availability and/or correct functioning of services or systems

Reconnaissance Attack

- Unauthorised users to gather information about the network or system before launching other more serious types of attacks
- Also called eavesdropping
- Information gained from this attack is used in subsequent attacks (DoS or DDoS type)
- Examples of relevant information:
  - Names, email address
    - Common practice to use a person's first initial and last name for accounts
  - Practically anything

Man-in-the-Middle Attack

- Active eavesdropping
- Attacker makes independent connections with victims and relays messages between them, making them believe that they are talking directly to each other overa private connection, when in fact the entire conversation is controlled by the attacker
- Usually a result of lack of end-to-end authentication
- Masquerading - an entity claims to be another entity

Session Hijacking

- Exploitation of a valid computer session, to gain unauthorized access to information or services in a computer system.
- Theft of a “magic cookie” used to authenticate a user to a remote server (for web developers)
- Four methods:
  - Session fixation – attacker sets a user’s session id to one known to him, for example by sending the user an email with a link that contains a particular session id.
  - Session sidejacking – attacker uses packet sniffing to read network traffic between two parties to steal the session cookie.

Denial of Service (DoS) Attack

- Attempt to make a machine or network resource unavailable to its intended users.
- Purpose is to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet
- Methods to carry out this attack may vary
  - Saturating the target with external communications requests (such that it can't respond to legitimate traffic) – SERVER OVERLOAD
  - May include malware to max out target resources (such as CPU), trigger errors, or crash the operating system
- DDoS attacks are more dynamic and comes from a broader range of attackers
- Examples: SYN flooding, Smurf attacks, Starvation
- Can be used as a redirection and reconnaissance technique

Questions?

Layered Security & Attack Mitigation

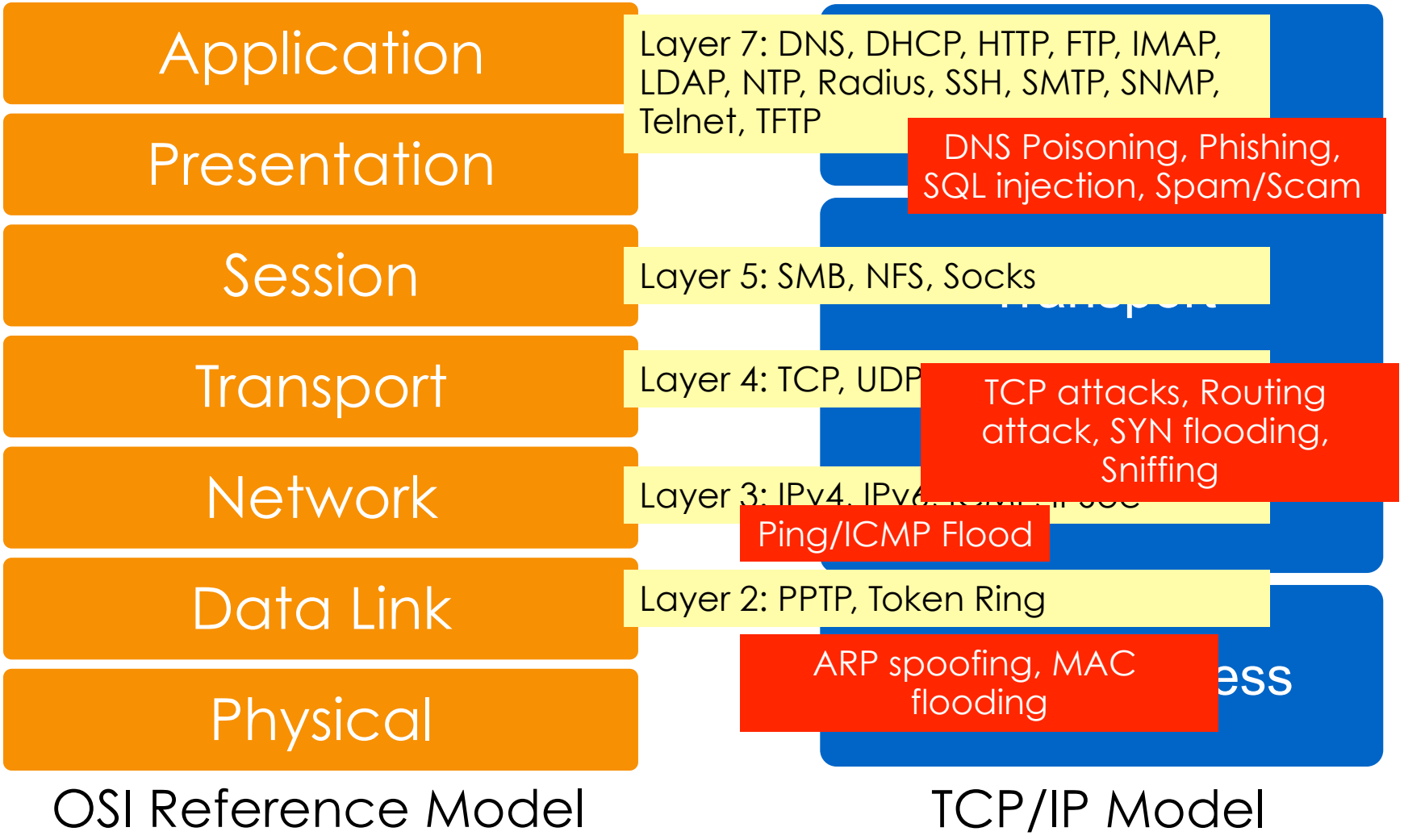
Network Security Workshop

APNIC

Overview

- Attacks in Different Layers
- Security Technologies
- Link-Layer Security
- Network Layer Security
- Transport Layer Security
- Application Layer Security

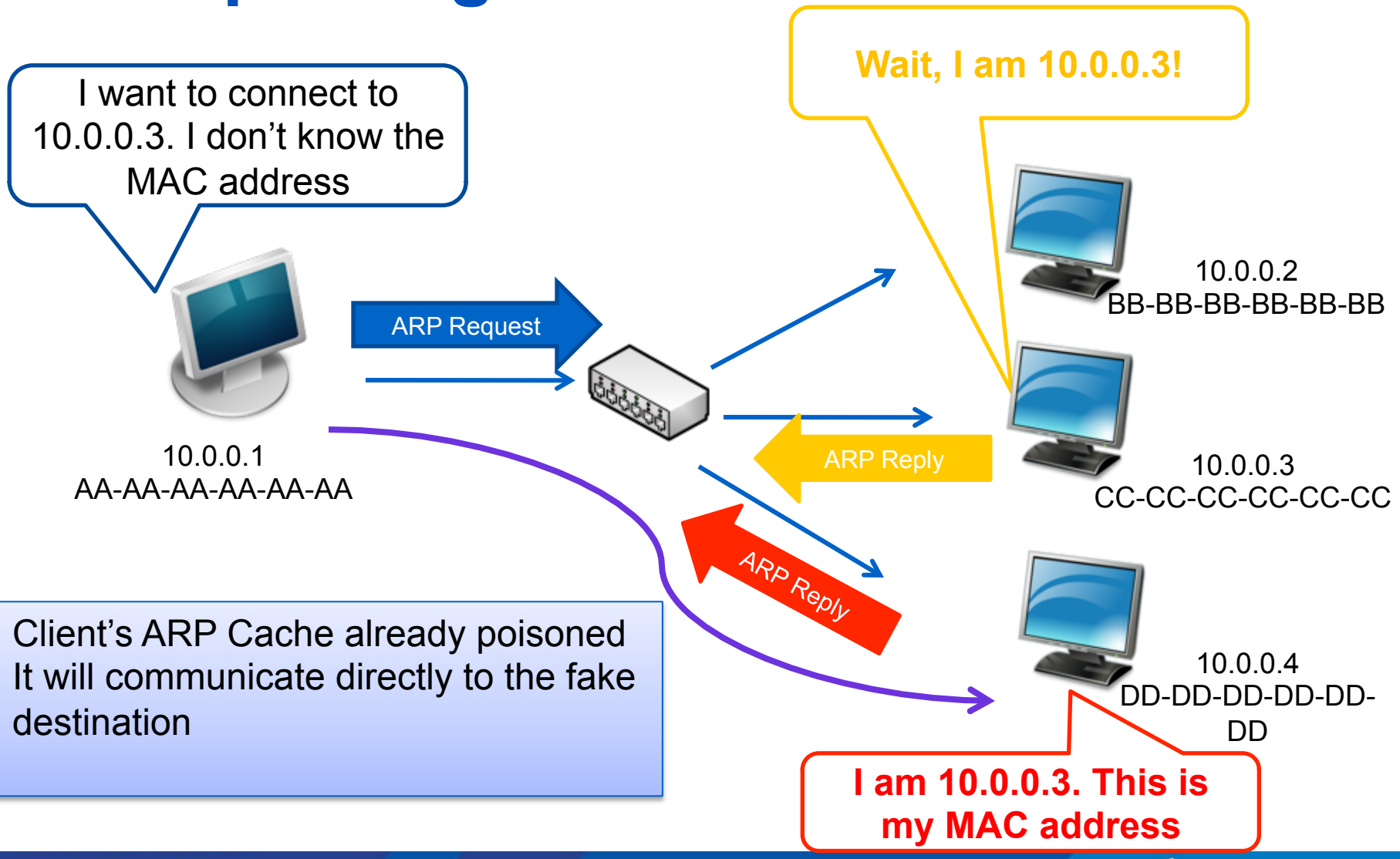
Attacks on Different Layers



Layer 2 Attacks

- ARP Spoofing
- MAC attacks
- DHCP attacks
- VLAN hopping

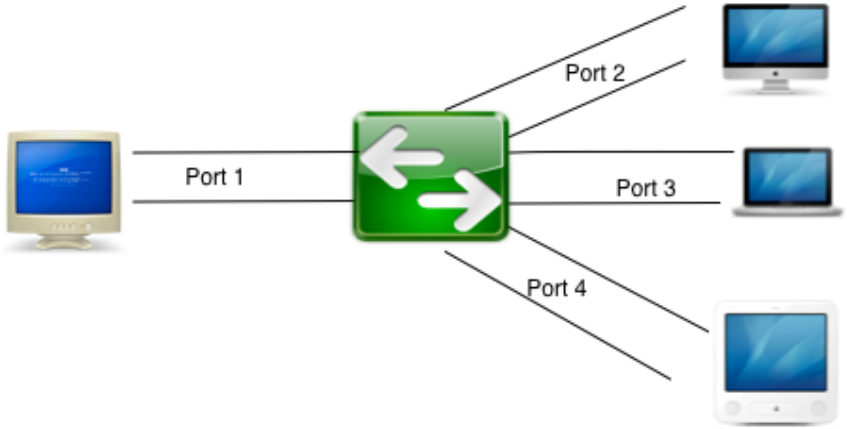
ARP Spoofing



Client's ARP Cache already poisoned
It will communicate directly to the fake destination

MAC Flooding

- Exploits the limitation of all switches – fixed CAM table size
- CAM = Content Addressable memory = stores info on the mapping of individual MAC addresses to physical ports on the switch.

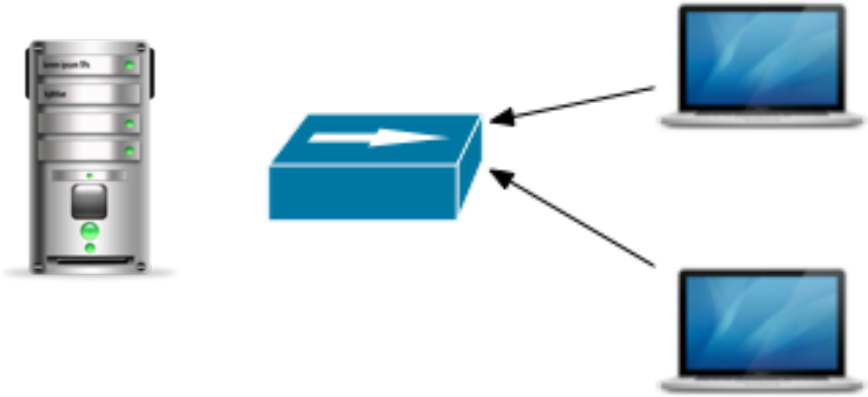


	Port 1	Port 2	Port 3	Port 4
00:01:23:45:67:A1	x			
00:01:23:45:67:B2		x		
00:01:23:45:67:C3			x	
00:01:23:45:67:D4				x

DHCP Attacks

- DHCP Starvation Attack
  - Broadcasting vast number of DHCP requests with spoofed MAC address simultaneously.
  - DoS attack using DHCP leases
- Rogue DHCP Server Attacks

Server runs out of IP addresses to allocate to valid users



Attacker sends many different DHCP requests with many spoofed addresses.

DHCP Attack Types

- Solution: enable DHCP snooping

```
ip dhcp snooping (enable dhcp snooping globally)
ip dhcp snooping vlan <vlan-id> (for specific
vlans)
ip dhcp snooping trust
ip dhcp snooping limit rate <rate>
```

Layer 3 Attacks

- ICMP Ping Flood
- ICMP Smurf
- Ping of death

Ping Flood

Attacker

Internet

Victim

Other forms of ICMP attack:
-Ping of death
-ICMP ping flood

Broadcast Enabled Network

Mitigating Sniffing Attacks

- Avoid using insecure protocols like basic HTTP authentication and telnet.
- If you have to use an insecure protocol, try tunneling it through something to encrypt the sensitive data.
- Run ARPwatch.
- Try running tools like sniffdet and Sentinel to detect network cards in promiscuous mode that may be running sniffing software.

Routing Attacks

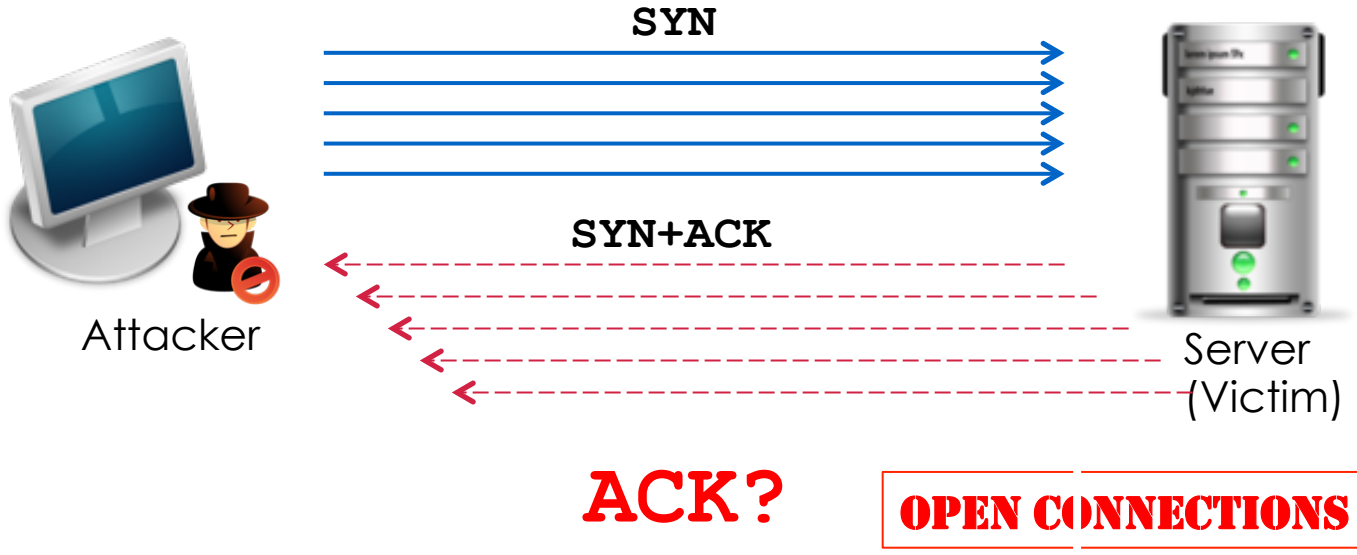
- Attempt to poison the routing information
- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP attacks
  - ASes can announce arbitrary prefix
  - ASes can alter path

TCP Attacks

- SYN Flood – occurs when an attacker sends SYN requests in succession to a target.
- Causes a host to retain enough state for bogus half-connections such that there are no resources left to establish new legitimate connections.

TCP Attacks

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



Application Layer Attacks

- Applications don’t authenticate properly
- Authentication information in clear
  - FTP, Telnet, POP
- DNS insecurity
  - DNS poisoning
  - DNS zone transfer

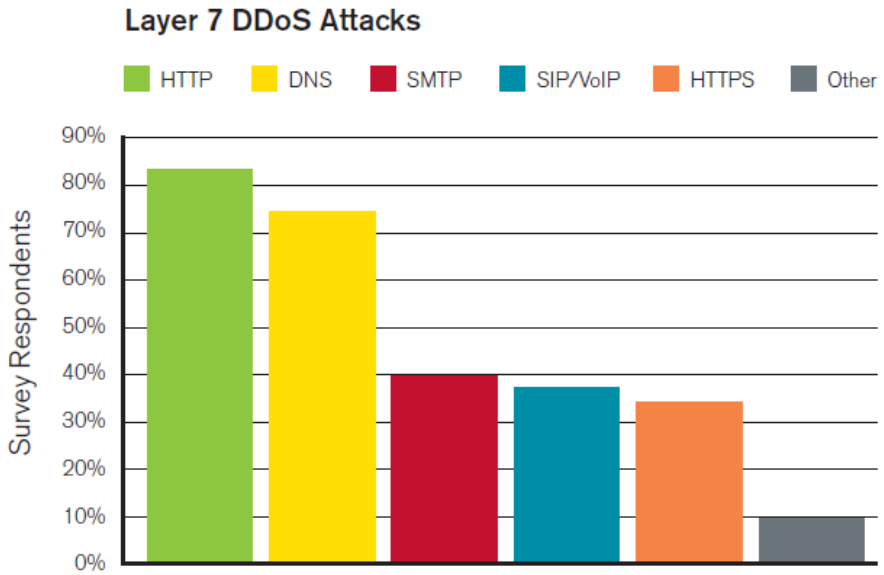
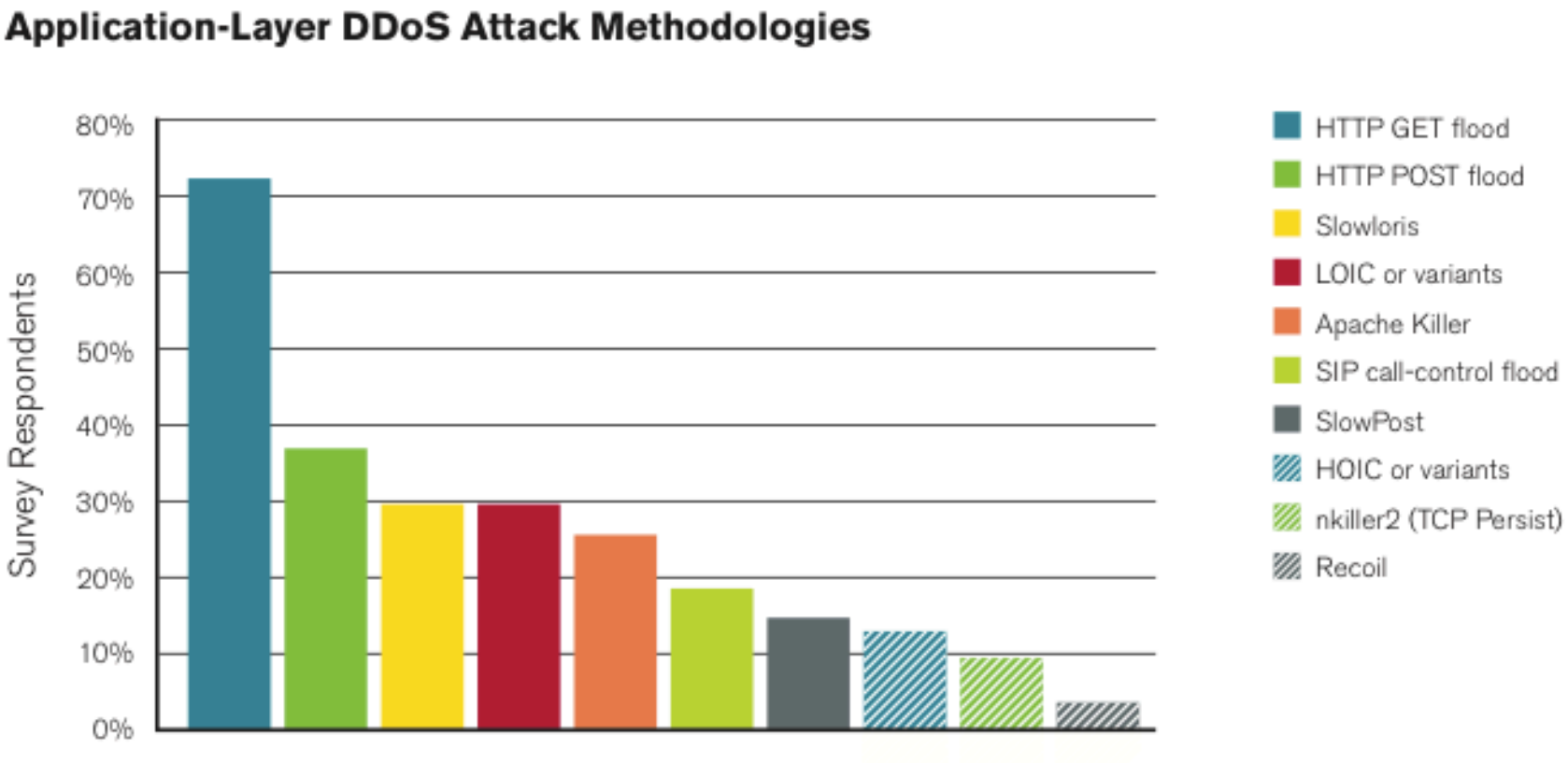


Figure 8
Source: Arbor Networks, Inc.

Application Layer Attacks

- Scripting vulnerabilities
- Cookie poisoning
- Buffer overflow
- Hidden field manipulation
- Parameter tampering
- Cross-site scripting
- SQL injection

Application-Layer Attacks



Source: Arbor Networks Worldwide Infrastructure Security Report Volume VII

Application Layer DDoS: Slowloris

- Incomplete HTTP requests
- Properties
  - Low bandwidth
  - Keep sockets alive
  - Only affects certain web servers
  - Doesn’t work through load balancers
  - Managed to work around accf_http

Web Application Security Risks

- Injection
- Cross-Site Scripting
- Broken authentication and Session Management
- Insecure Direct Object References
- Cross-site Request Forgery (CSRF)
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

Source: OWASP Top 10 Application Security Risks, 2010

DNS Changer

- “Criminals have learned that if they can control a user’s DNS servers, they can control what sites the user connects to the Internet.”
- How: infect computers with a malicious software (malware)
- This malware changes the user’s DNS settings with that of the attacker’s DNS servers
- Points the DNS configuration to DNS resolvers in specific address blocks and use it for their criminal enterprise
- For more: see the NANOG presentation by Merike

Rogue DNS Servers

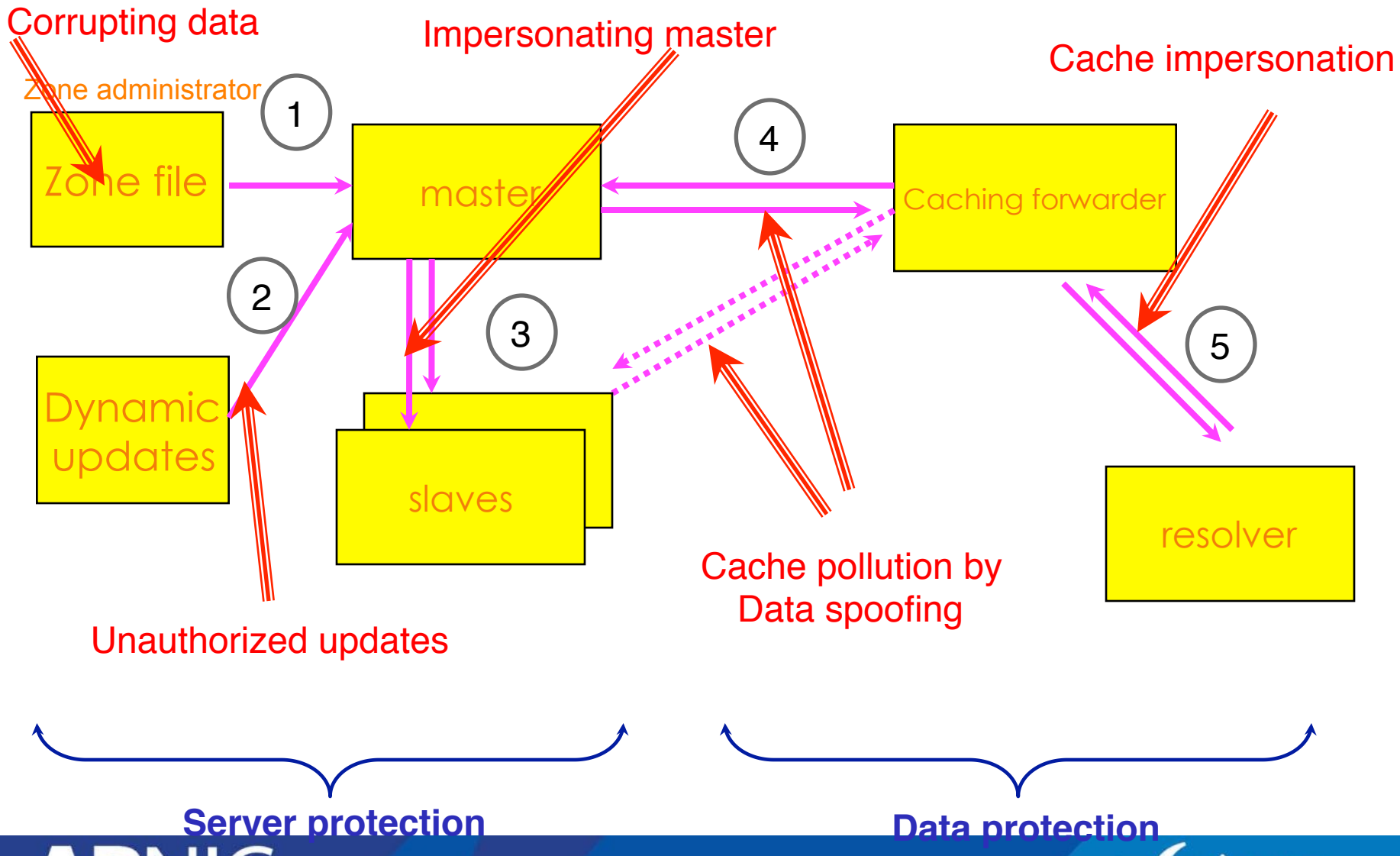
- 85.225.112.0 through 85.255.127.255
- 67.210.0.0 through 67.210.15.255
- 93.188.160.0 through 93.188.167.255
- 77.67.83.0 through 77.67.83.255
- 213.109.64.0 through 213.109.79.255
- 64.28.176.0 through 64.28.191.255

- If your computer is configured with one of these DNS servers, it is most likely infected with DNSChanger malware

Top DNS Changer Infections

- By country (as of 11 June, 2012):
  - USA - 69517
  - IT – 26494
  - IN – 21302
  - GB – 19589
  - DE – 18427
- By ASNs
  - AS9829 (India) – 15568
  - AS3269 () – 13406
  - AS7922 () – 11964
  - AS3320 () – 9250
  - AS7132 () – 6743
- More info at http://dcwg.org/

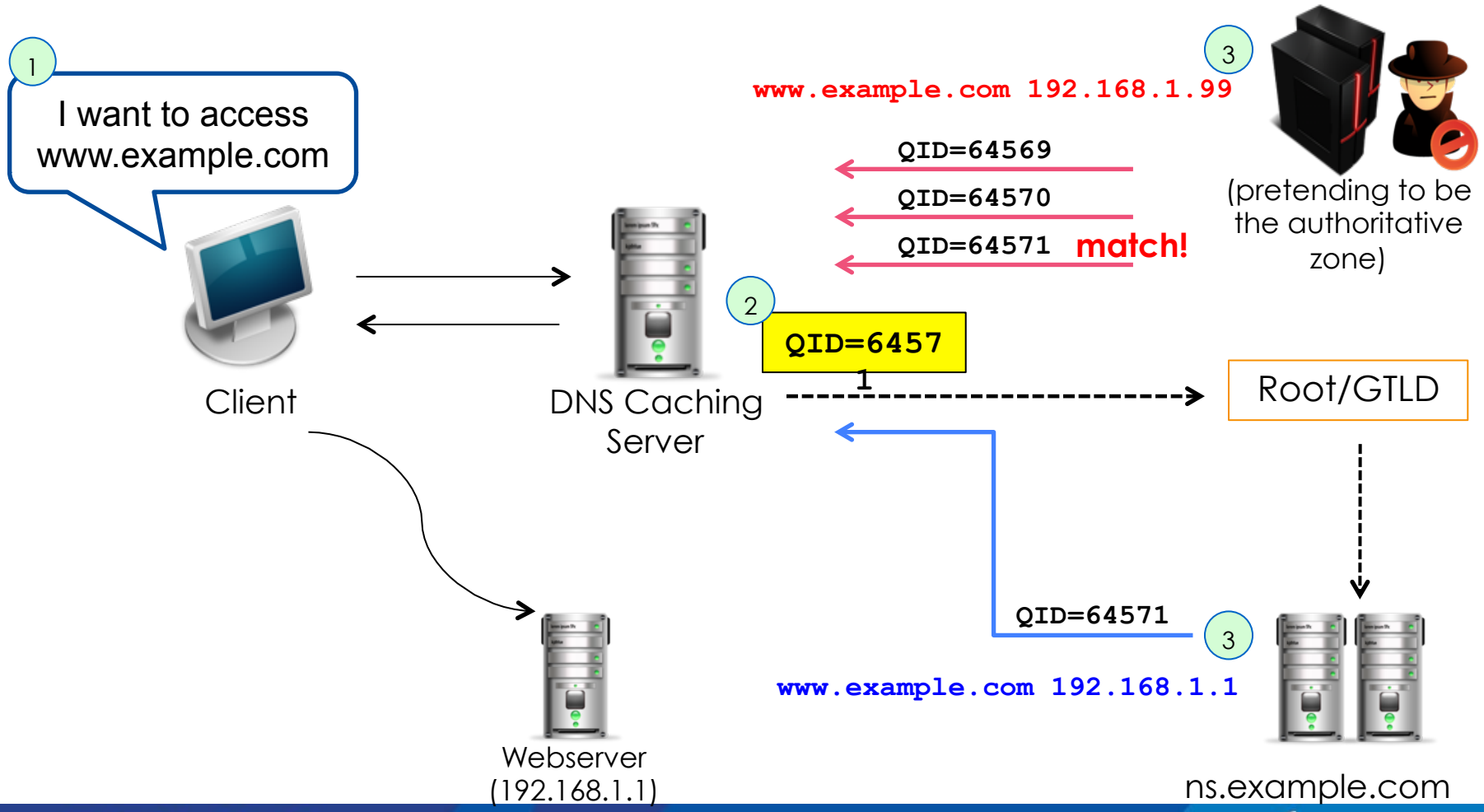
DNS Vulnerabilities



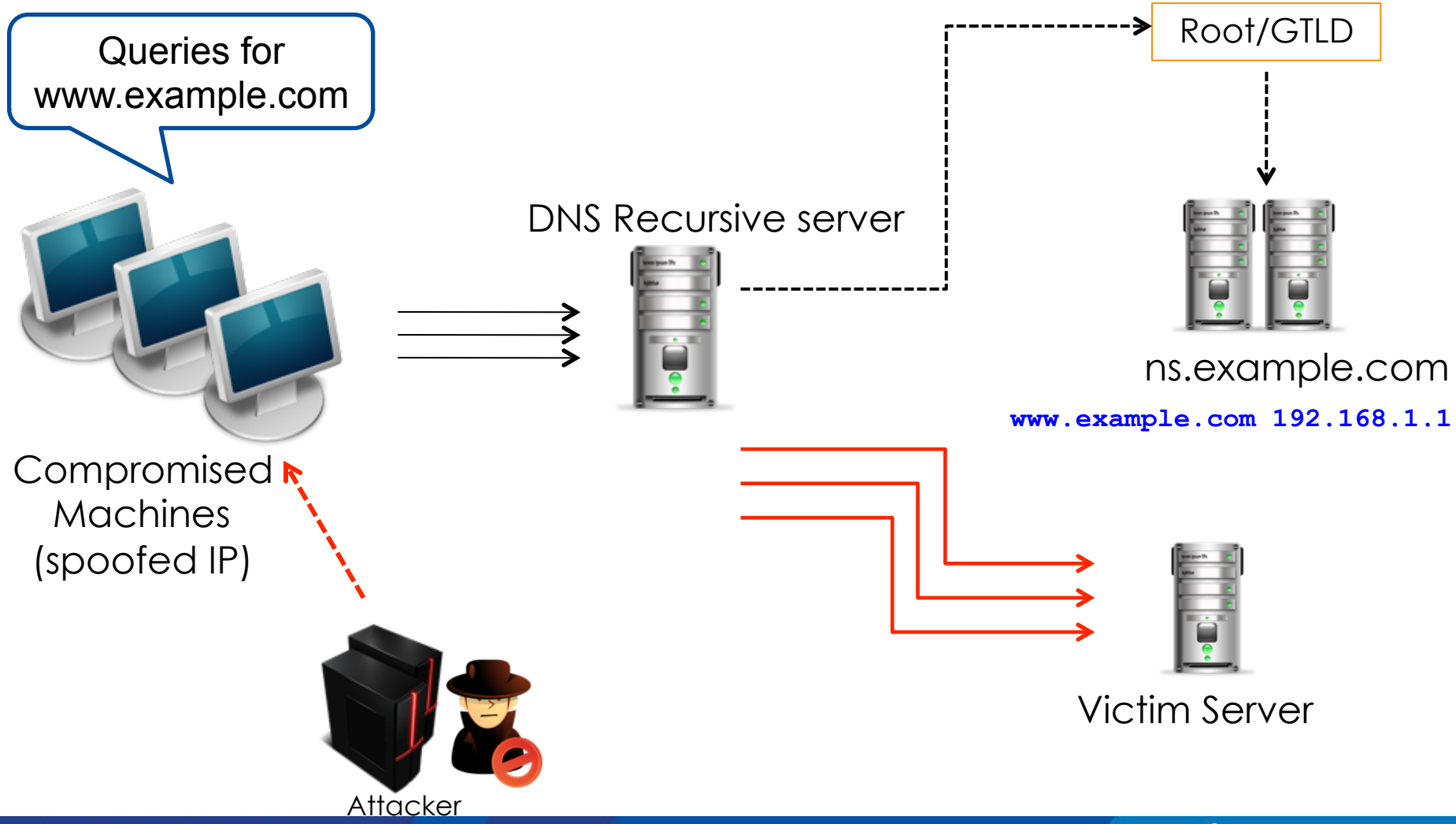
DNS Cache Poisoning

- Caching incorrect resource record that did not originate from authoritative DNS sources.
- Result: connection (web, email, network) is redirected to another target (controlled by the attacker)

DNS Cache Poisoning



DNS Amplification



Common Types of Attack

- Ping sweeps and port scans - reconnaissance
- Sniffing – capture packet as they travel through the network
- Man-in-the-middle attack – intercepts messages that are intended for a valid device
- Spoofing - sets up a fake device and trick others to send messages to it
- Hijacking – take control of a session
- Denial of Service (DoS) and Distributed DoS (DDoS)

Wireless Attacks

- WEP – first security mechanism for 802.11 wireless networks
- Weaknesses in this protocol were discovered by Fluhrer, Mantin and Shamir, whose attacks became known as “FMS attacks”
- Tools were developed to automate WEP cracking
- Chopping attack were released to crack WEP more effectively and faster
- Cloud-based WPA cracker
  - https://www.wpacracker.com/

Man in the Middle Attacks (Wireless)

- Creates a fake access point and have clients authenticate to it instead of a legitimate one.
- Capture traffic to see usernames, passwords, etc that are sent in clear text.

Botnet

- Collection of compromised computers (or ‘bot’)
- Computers are targeted by malware (malicious software)
- Once controlled, an attacker can use the compromised computer via standards-based network protocol such as IRC and HTTP
- How to become a bot:
  - Drive-by downloads (malware)
  - Go to malicious websites (exploits web browser vulnerabilities)
  - Run malicious programs (Trojan) from websites or as email attachment

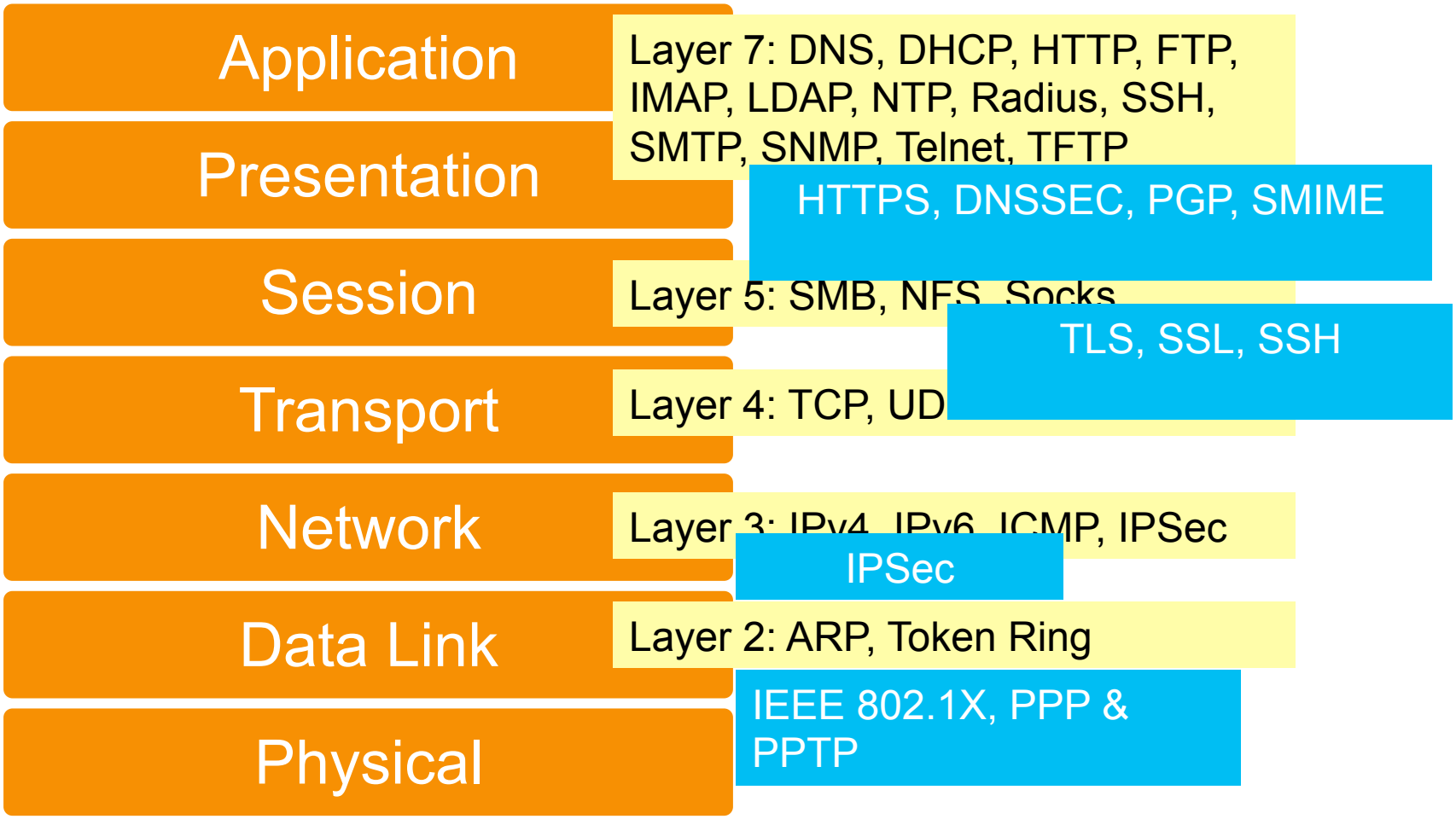
Password Cracking

- Dictionary attacks
  - Guessing passwords using a file of 1M possible password values
    - Ordinary words and people's names
  - Offline dictionary attack when the entire password file has been attacked
  - Use random characters as password with varying upper and lower case, numbers, and symbols
- Brute-force attacks
  - Checking all possible values until it has been found
  - The resource needed to perform this attack grows exponentially while increasing the key size
- Social engineering

Pharming and Phishing

- Phishing – victims are redirected to a fake website that looks genuine. When the victim supplies his account and password, this can be used by the attacker to the target site
  - Typically uses fraud emails with clickable links to fake websites
- Pharming – redirect a website's traffic to another fake site by changing the victim's DNS settings or hosts file

Security on Different Layers

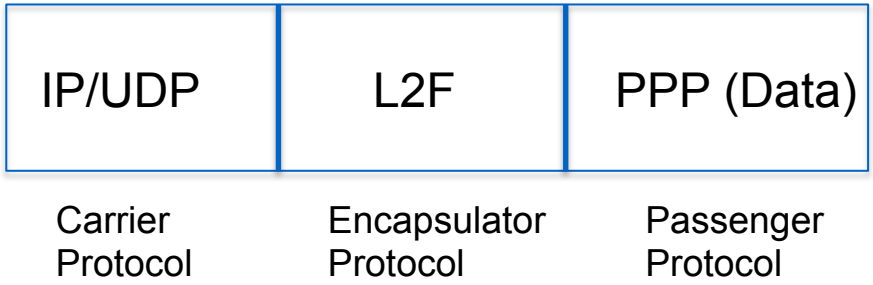


Link-Layer Security

- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

Layer 2 Forwarding Protocol

- Created by Cisco Systems and replaced by L2TP
- Permits the tunneling of the link layer – High-level Data Link Control (HDLC), async HDLC, or Serial Line Internet Protocol (SLIP) frames – of higher-level protocols



Point to Point Tunneling Protocol

- Initiated by Microsoft but later became an informational standard in the IETF (RFC 2637)
- Client/server architecture that allows PPP to be tunneled through an IP network and decouples functions that exist in current NAS.
- Connection-oriented

Layer 2 Tunneling Protocol

- Combination of L2F and PPTP
- Published as RFC 2661 and known as L2TPv2
- L2TPv3 provides additional security features and the ability to carry data links other than PPP
- The two end-points are L2TP Access Concentrator (LAC) or L2TP Network Server (LNS)

PPPoE

- PPP over Ethernet
- Defined in RFC 2516
- A means to encapsulate PPP packets over the Ethernet link layer
- Mostly used in ADSL environments to provide access control, billing, and type of service on a per-user rather than a per-site basis

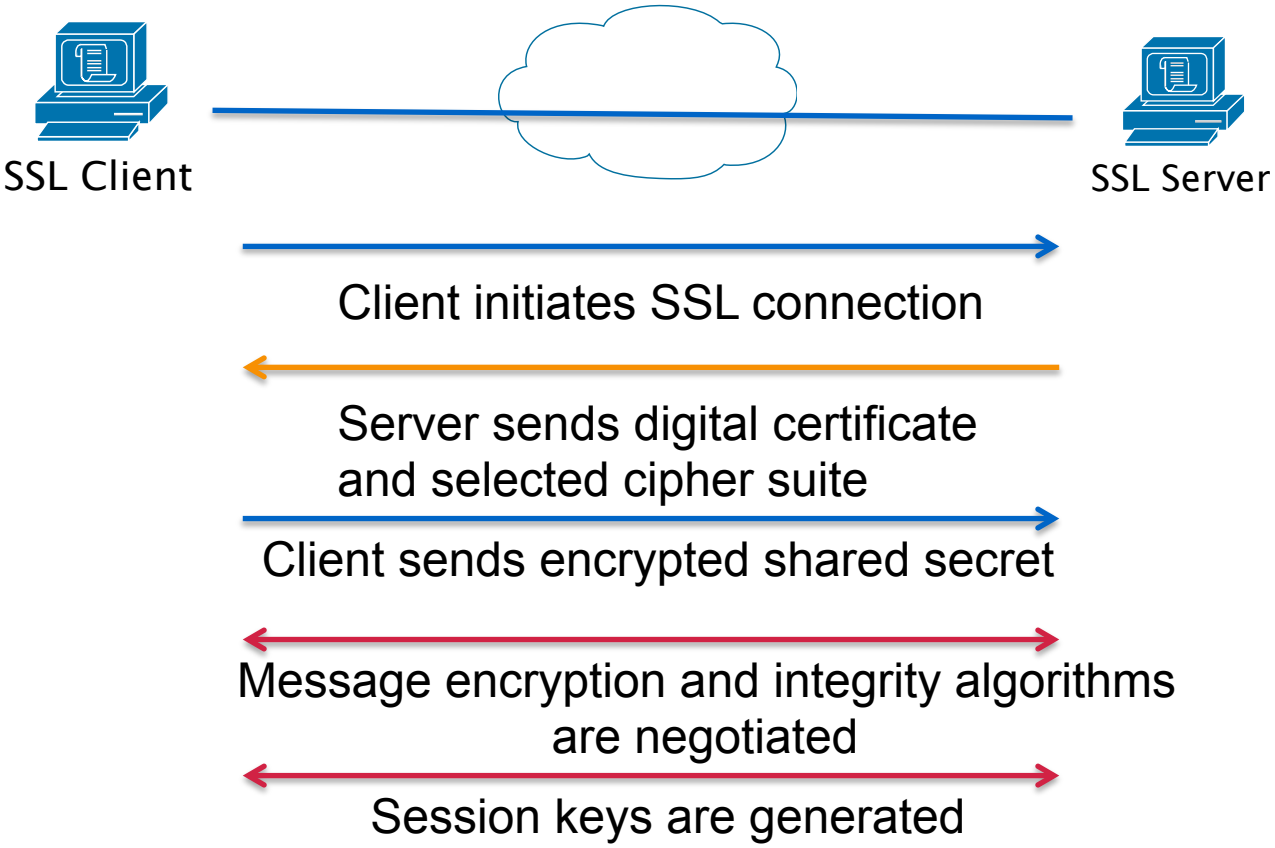
Transport Layer Security

- Secure Socket Layer (SSL)
- Secure Shell Protocol
- SOCKS Protocol

SSL/TLS

- TLS and SSL encrypts the segments of network connections above the Transport Layer.
- Versions:
  - SSLv1 – designed by Netscape
  - SSLv2 – publicly released in 1994; has a number of security flaws; uses RC4 for encryption and MD5 for authentication
  - SSLv3 – added support for DSS for authentication and DH for key agreement
  - TLS – based on SSLv3; uses DSS for authentication, DH for key agreement, and 3DES for encryption
- TLS is the IETF standard which succeeded SSL.

SSL Handshake



Advantages of SSL

- The connection is private
  - Encryption is used after initial handshake to define a secret key
  - Encryption uses symmetric cryptography (DES or RC4)
- Peer's identity can be authenticated using asmmetric cryptography (RSA or DSS)
- The connection is reliable
  - Message transport includes message integrity check using a keyed MAC. Secure hash functions (SHA or MD5) are used for MAC computation.

Applications Using SSL/TLS

Protocol	Defined Port Number	SSL/TLS Port Number
HTTP	80	443
NNTP	119	563
LDAP	389	636
FTP-data	20	989
FTP-control	21	990
Telnet	23	992
IMAP	143	993
POP3	110	994
SMTP	25	995

Secure Shell Protocol (SSH)

- Protocol for secure remote login
- Provides support for secure remote login, secure file transfer, and secure forwarding of TCP/IP and X Window System traffic
- Consists of 3 major components:
  - Transport layer protocol (server authentication, confidentiality, integrity)
  - User authentication protocol (authenticates client to the server)
  - Connection protocol (multiplexes the encrypted tunnel into several logical channels)

Application Layer Security

- HTTPS
- PGP (Pretty Good Privacy)
- SMIME (Secure Multipurpose Internet Mail Extensions)
- TSIG and DNSSEC
- Wireless Encryption - WEP, WPA, WPA2

HTTPS

- Hypertext Transfer Protocol Secure
- Widely-used, message-oriented communications protocol
- Connectionless oriented protocol
- Technically not a protocol in itself, but simply layering HTTP on top of the SSL/TLS protocol
- Encapsulates data after security properties of the session
- Not to be confused with S-HTTP

Note: A website must use HTTPS everywhere, otherwise it is still vulnerable to some attacks

Pretty Good Privacy (PGP)

- Stands for Pretty Good Privacy, developed by Phil Zimmerman in 1995
- PGP is a hybrid cryptosystem
  - combines some of the best features of both conventional and public key cryptography
- Assumptions:
  - All users are using public key cryptography and have generated private/public key pairs (using RSA or El Gamal)
  - All users also use symmetric key system (DES or Rijndael)
- Offers authentication, confidentiality, compression, e-mail compatibility and segmentation

S/MIME

- Secure Multipurpose Internet Mail Extensions
- Uses public key certificates conforming to standard X.509
- Very similar to PGP

Securing the Nameserver

- Run the most recent version of the DNS software
  - Bind 9.9.1 or Unbound 1.4.16
  - Apply the latest patches
- Hide version
- Restrict queries
  - `Allow-query { acl_match_list; };`
- Prevent unauthorized zone transfers
  - `Allow-transfer { acl_match_list; };`
- Run BIND with the least privilege (use `chroot`)
- Randomize source ports
  - don't use `query-source` option
- Secure the box
- Use TSIG and DNSSEC

DNSSEC

- DNSSEC – Domain Name Security Extensions
- A set of extensions to DNS that provides
  - Origin authentication of DNS data
  - Data integrity
  - Authenticated denial of existence
- designed to protect against attacks such as DNS cache poisoning.
- Adds four new resource record types:
  - RRSIG (Resource Record Signature)
  - DNSKEY (DNS Public Key)
  - DS (Delegation Signer)
  - NSEC (Next Secure)

Questions?

Cryptography

Network Security Workshop

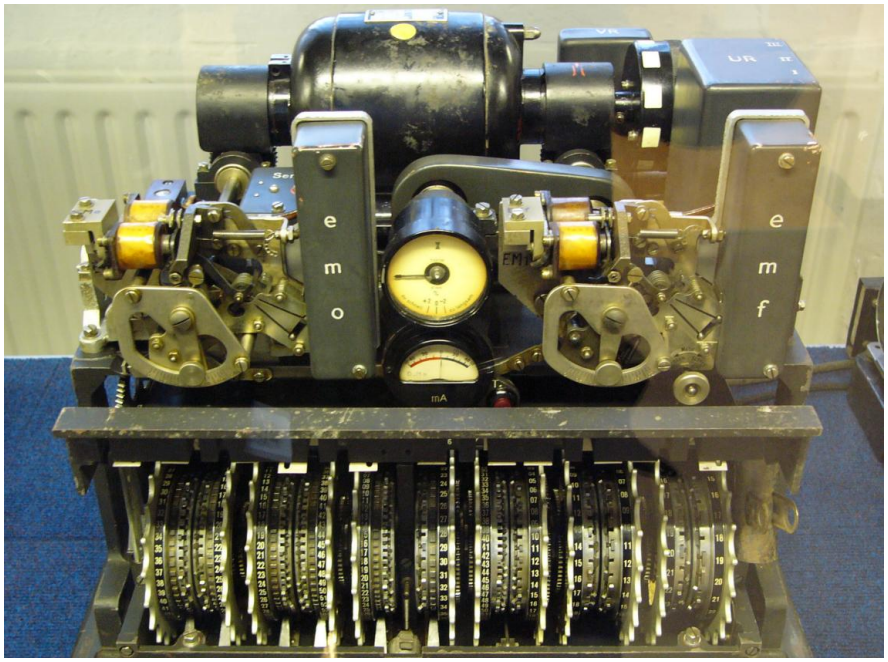
APNIC

Overview

- What is Cryptography?
- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Block and Stream Cipher
- Digital Signature and Message Digest

Cryptography

- Cryptography is everywhere



German Lorenz cipher machine

Cryptography

- Cryptography deals with creating documents that can be shared secretly over public communication channels
- Other terms closely associated
  - Cryptanalysis = code breaking
  - Cryptology
    - Kryptos (hidden or secret) and Logos (description) = secret speech / communication
    - combination of cryptography and cryptanalysis
- Cryptography is a function of plaintext and a cryptographic key

$$C = F(P, k)$$

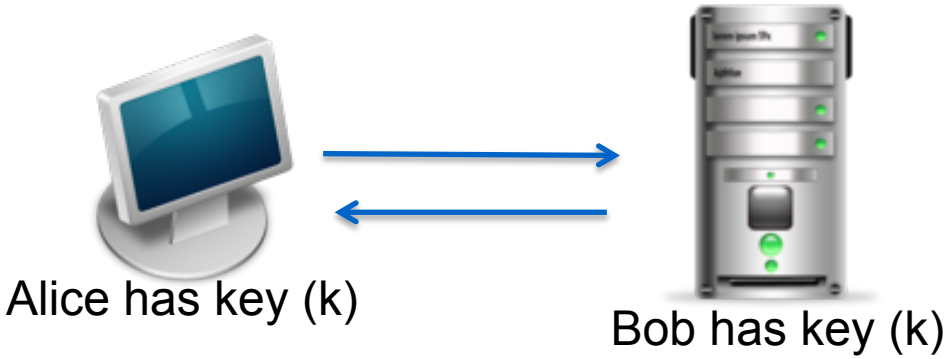
Notation:
Plaintext (P)
Ciphertext (C)
Cryptographic Key (k)

Typical Scenario

- Alice wants to send a “secret” message to Bob
- What are the possible problems?
  - Data can be intercepted
- What are the ways to intercept this message?
- How to conceal the message?
  - Encryption

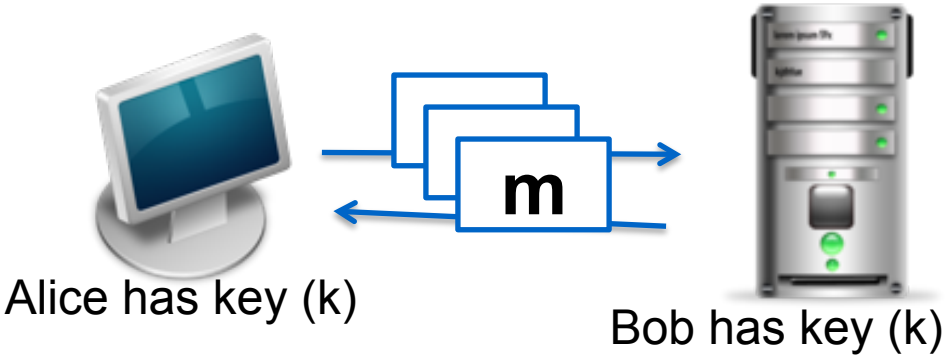
Crypto Core

- Secure key establishment



- Secure communication

Confidentiality and integrity



Source: Dan Boneh, Stanford

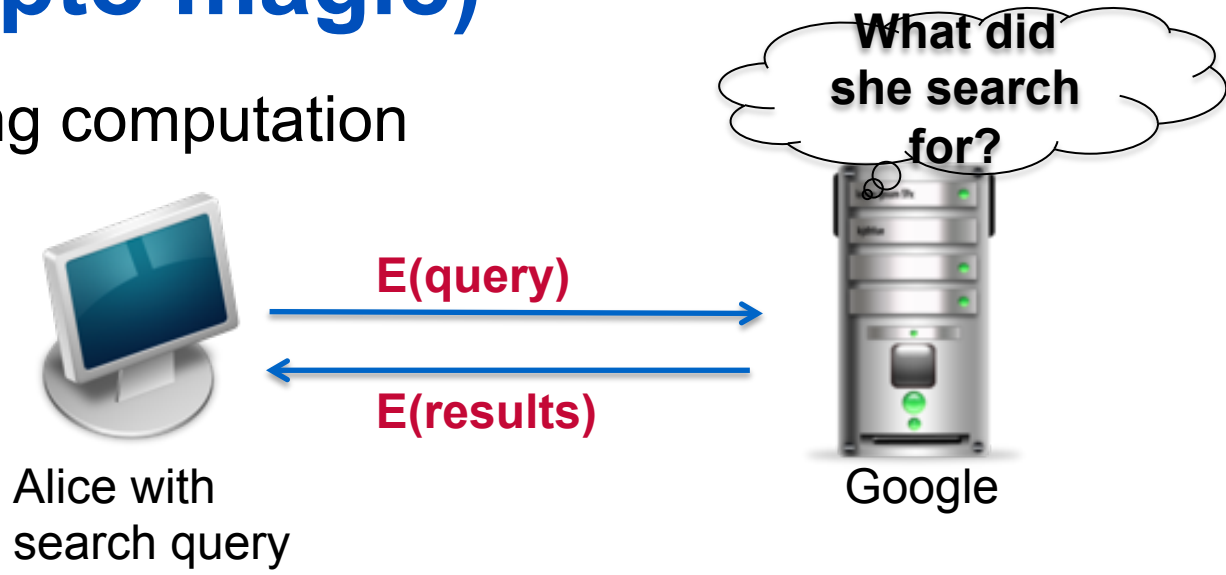
It can do much more

- Digital Signatures
- Anonymous communication
- Anonymous digital cash
  - Spending a digital coin without anyone knowing my identity
  - Buy online anonymously?
- Elections and private auctions
  - Finding the winner without actually knowing individual votes (privacy)

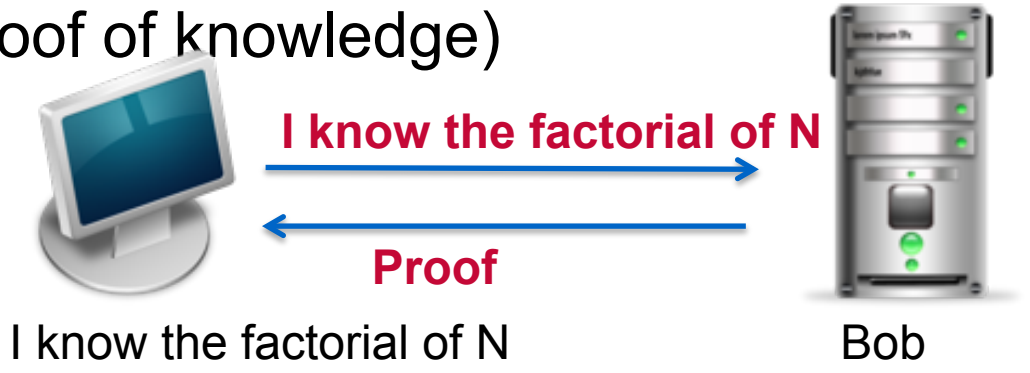
Source: Dan Boneh, Stanford

Other uses are also theoretically possible (Crypto magic)

- Privately outsourcing computation



- Zero knowledge (proof of knowledge)



Source: Dan Boneh, Stanford

History: Ciphers

- Substitution cipher
  - involves replacing an alphabet with another character of the same alphabet set
  - Can be mono-alphabetic (single set for substitution) or poly-alphabetic system (multiple alphabetic sets)
- Example:
  - Caesar cipher, a mono-alphabetic system in which each character is replaced by the third character in succession
  - Vigenere cipher, a poly-alphabetic cipher that uses a 26x26 table of characters

How to Break a Substitution Cipher

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO

FEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWN

CPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVF

ZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUB

OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

(1) Use frequency of the English letters

e = 12.7%

t = 9.1 %

a = 8.1%

(2) Use frequency of pairs of letters

he, in, an, th

In the example,

B appeared 36 times, **U** 33 times, and **P** 32 times

NC appeared 11 times, **PU** 10 times

UKB appeared 6 times

Source: Dan Boneh, Stanford

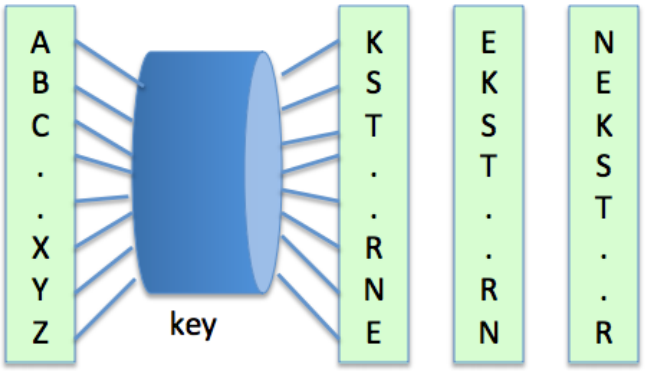
Transposition Cipher

- No letters are replaced, they are just rearranged.
- Rail Fence Cipher – another kind of transposition cipher in which the words are spelled out as if they were a rail fence.

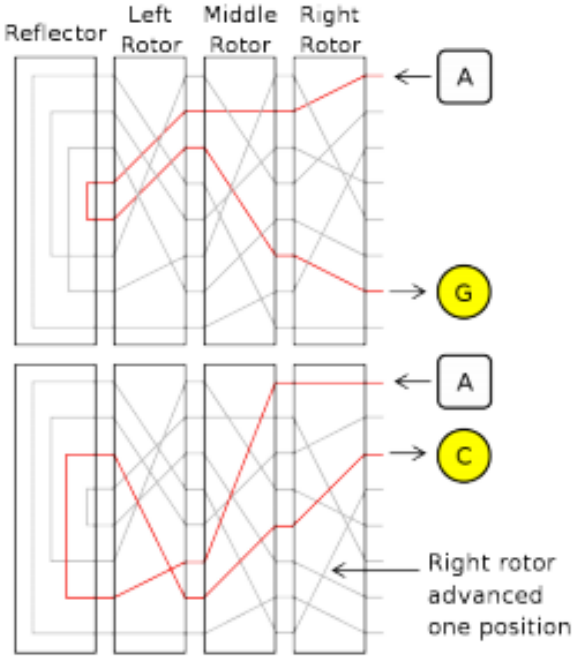
```
T...U...B...N...J...E...E...E...Y..
.H.Q.I.K.R.W.F.X.U.P.D.V.R.H.L.Z.D.G.
..E...C...O...O...M...O...T...A...O
```

History: Rotor Machines (1870-1943)

- Hebern machine – single rotor



- Enigma - 3-5 rotors



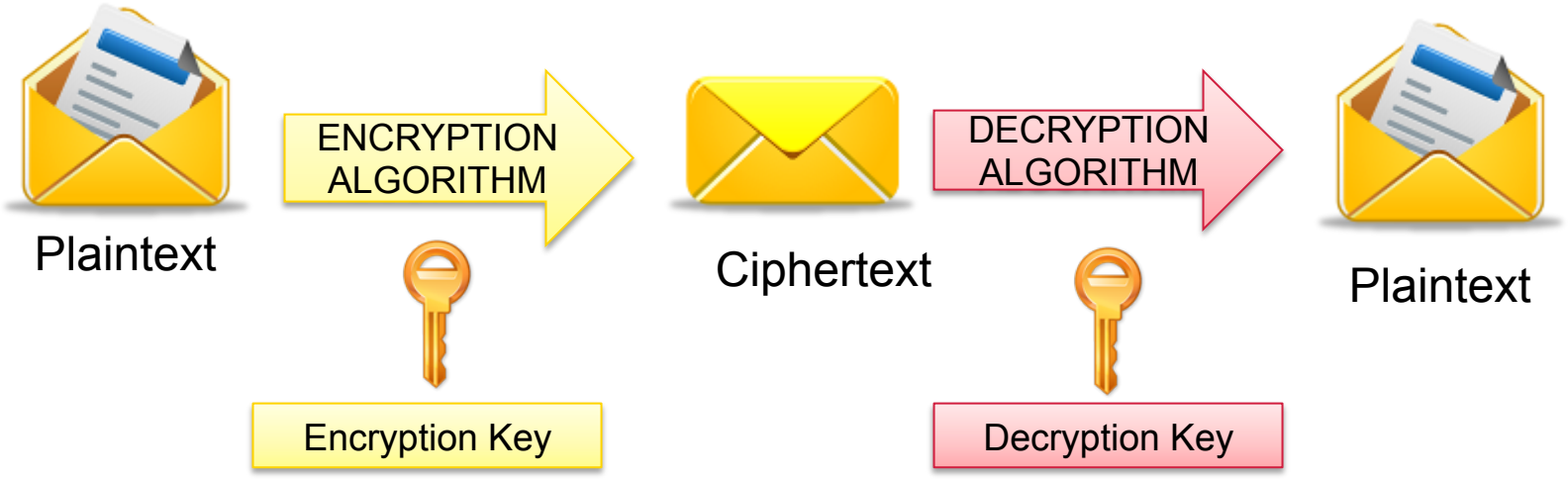
Modern Crypto Algorithms

- specifies the mathematical transformation that is performed on data to encrypt/decrypt
- Crypto algorithm is NOT proprietary
- Analyzed by public community to show that there are no serious weaknesses
- Explicitly designed for encryption

Encryption

- process of transforming plaintext to ciphertext using a cryptographic key
- Used all around us
  - In Application Layer – used in secure email, database sessions, and messaging
  - In session layer – using Secure Socket Layer (SSL) or Transport Layer Security (TLS)
  - In the Network Layer – using protocols such as IPSec
- Benefits of good encryption algorithm:
  - Resistant to cryptographic attack
  - They support variable and long key lengths and scalability
  - They create an avalanche effect
  - No export or import restrictions

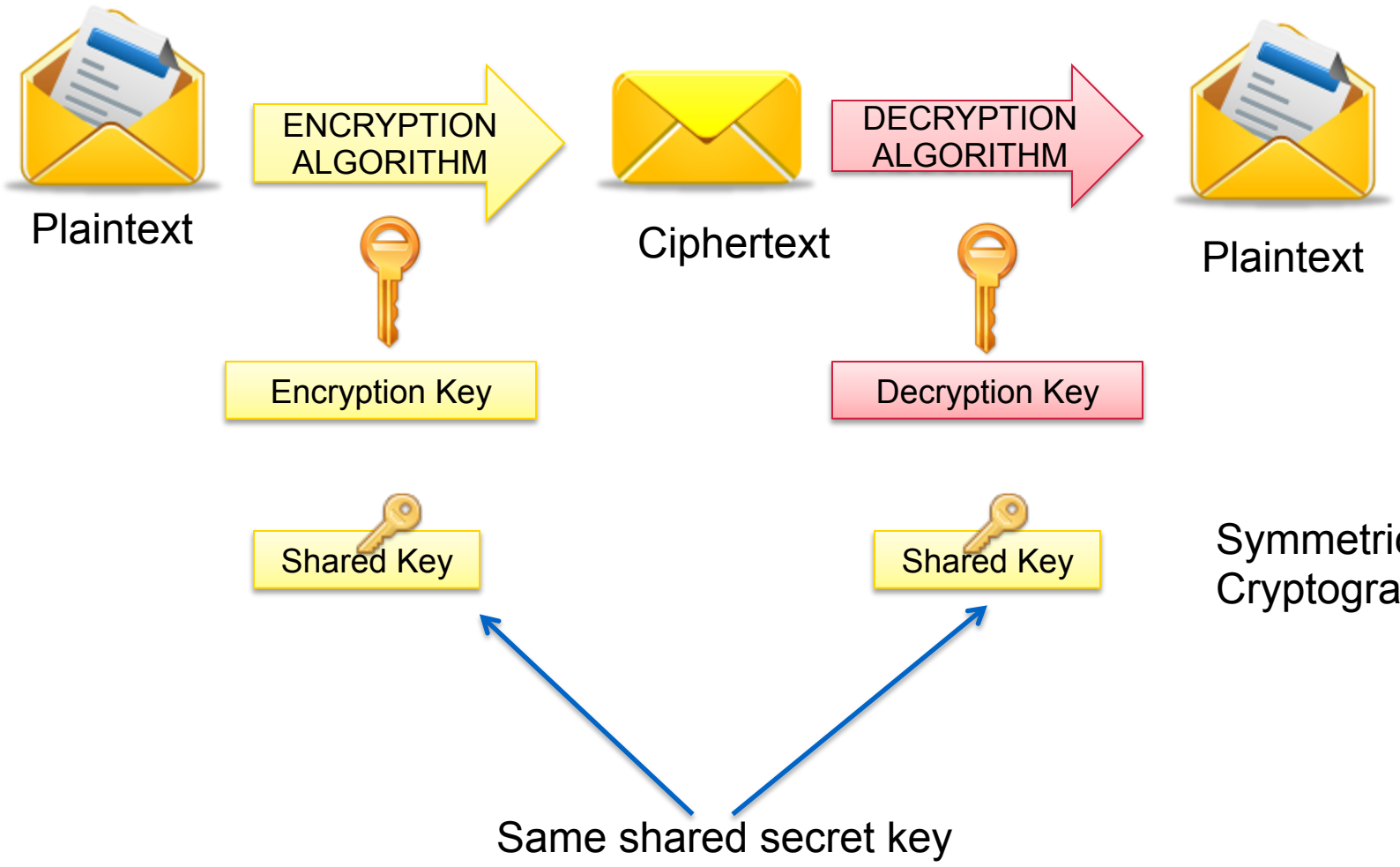
Encryption and Decryption



Symmetric Key Algorithm

- Uses a single key to both encrypt and decrypt information
- Also known as a secret-key algorithm
  - The key must be kept a “secret” to maintain security
  - This key is also known as a private key
- Follows the more traditional form of cryptography with key lengths ranging from 40 to 256 bits.

Symmetric Encryption



Symmetric Key Algorithm

- DES – block cipher using shared key encryption, 56-bit
- 3DES (Triple DES) – a block cipher that applies DES three times to each data block
- AES – replacement for DES; it is the current standard
- RC4 – variable-length key, “stream cipher” (generate stream from key, XOR with data)
- RC6
- Blowfish

Symmetric Key Algorithm

Symmetric Algorithm	Key Size
DES	56-bit keys
Triple DES (3DES)	112-bit and 168-bit keys
AES	128, 192, and 256-bit keys
IDEA	128-bit keys
RC2	40 and 64-bit keys
RC4	1 to 256-bit keys
RC5	0 to 2040-bit keys
RC6	128, 192, and 256-bit keys
Blowfish	32 to 448-bit keys

Note:
Longer keys are more difficult to crack, but more computationally expensive.

Block and Stream Cipher

- Block cipher
  - takes a block of bits and encrypts them as a single unit
  - operate on a pre-determined block of bits (one byte, one word, 512 bytes, so forth), mixing key data in with the message data in a variety of different ways.
- Stream cipher
  - encrypts bits of the message at a time
  - typically bit-wise.
  - They either have a very long key (that eventually repeats) or a reusable key that generates a repeatable but seemingly random string of bits.
  - They perform some operation (typically an exclusive OR) with one of these key bits and one of the message bits.

Block Cipher

- Transforms a fixed-length block of plain text into a block of ciphertext
- Works with data per block
- Common block ciphers:
  - DES and 3DES (in ECB and CBC mode)
  - Skipjack
  - Blowfish
  - RSA
  - AES
  - IDEA
  - Secure and Fast Encryption Routing (SAFER)

Stream Cipher

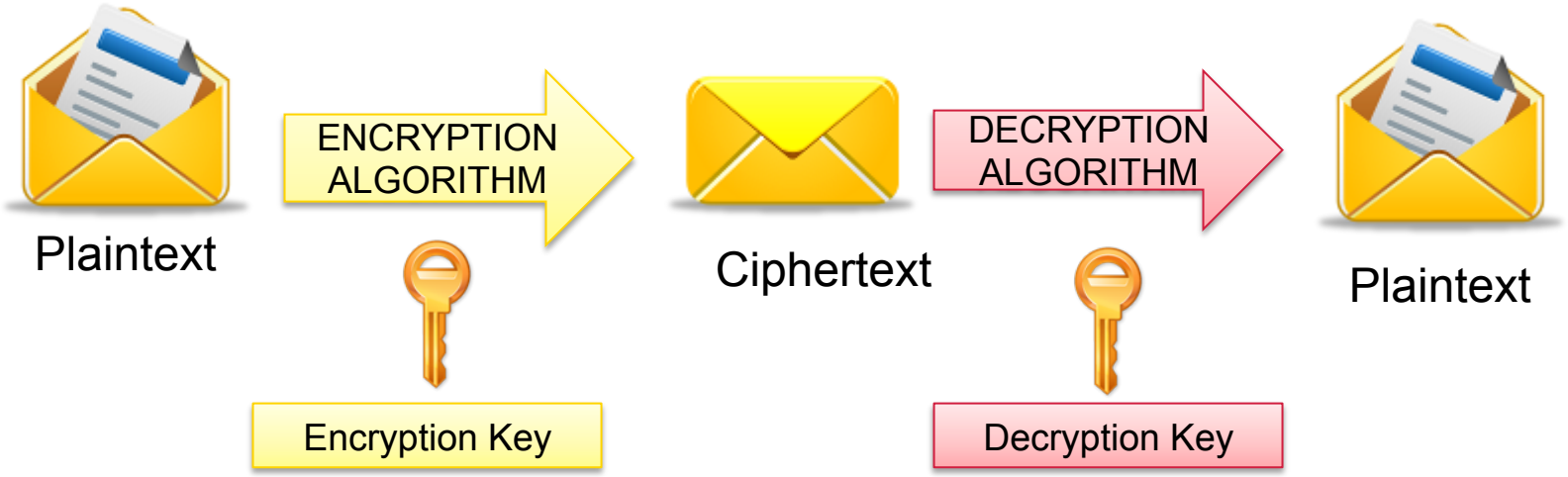
- Use smaller units of plaintext than what are used with block ciphers.
- Typically work with bits
- Common stream ciphers:
  - RC4
  - DES and 3DES (running OFB or CFB mode)
  - Software encryption algorithm (SEAL)

Data Encryption Standard (DES)

- Developed by IBM for the US government in 1973-1974, and approved in Nov 1976.
- Based on Horst Feistel's Lucifer cipher
- block cipher using shared key encryption, 56-bit key length
- Block size: 64 bits

DES: Illustration

64-bit blocks of input text



56-bit keys +
8 bits parity

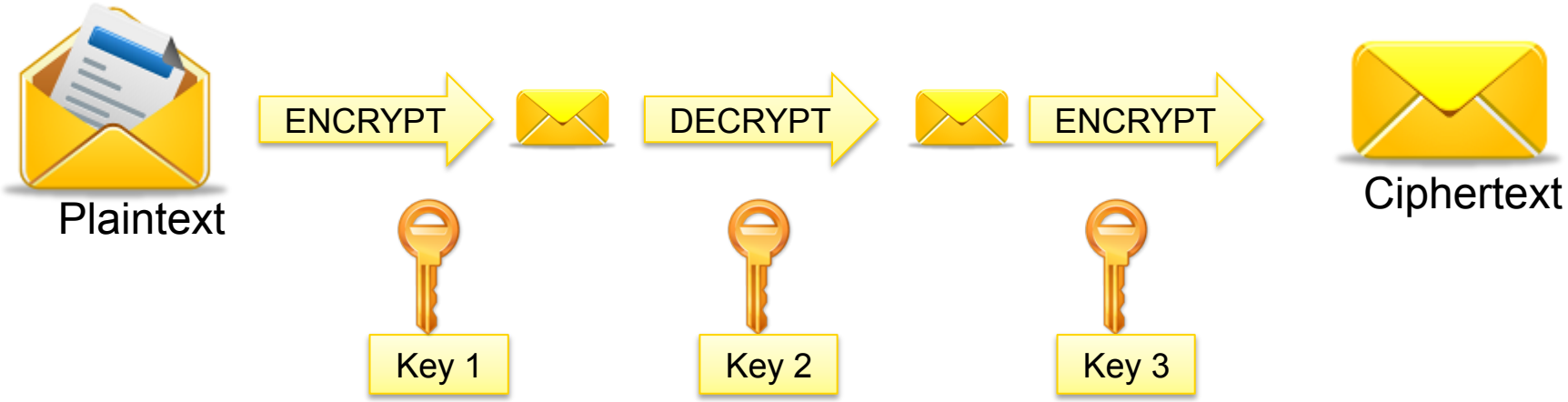
Triple DES

- 3DES (Triple DES) – a block cipher that applies DES three times to each data block
- Uses a key bundle comprising of three DES keys (K1, K2, K3), each with 56 bits excluding parity.
- DES encrypts with K1, decrypts with K2, then encrypts with K3

$$C_i = E_{K3}(D_{K2}(E_{K1}(P_i)))$$

- Disadvantage: very slow

3DES: Illustration



- Note:
  - If Key1 = Key2 = Key3, this is similar to DES
  - Usually, Key1 = Key3

Advanced Encryption Standard (AES)

- Published in November 2001
- Symmetric block cipher
- Has a fixed block size of 128 bits
- Has a key size of 128, 192, or 256 bits
- Based on Rijndael cipher which was developed by Joan Daemen and Vincent Rijmen
- Better suited for high-throughput, low latency environments

Rivest Cipher

RC Algorithm	Description
RC2	Variable key-sized cipher used as a drop in replacement for DES
RC4	Variable key sized stream cipher; Often used in file encryption and secure communications (SSL)
RC5	Variable block size and variable key length; uses 64-bit block size; Fast, replacement for DES
RC6	Block cipher based on RC5, meets AES requirement

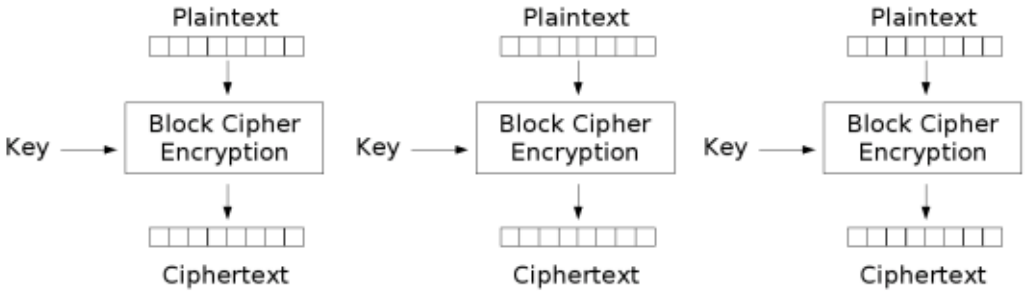
RC4

- Most widely used stream cipher
- Popularly used in Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP) protocols
- Although simple and fast, it is vulnerable and can lead to insecure systems

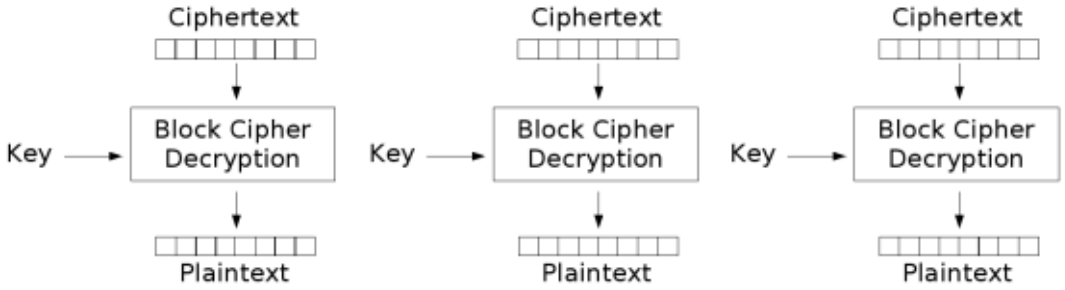
Block Cipher Modes

- Defines how the block cipher algorithm is applied to the data stream
- Four Basic Modes
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)

Electronic Codebook (ECB)

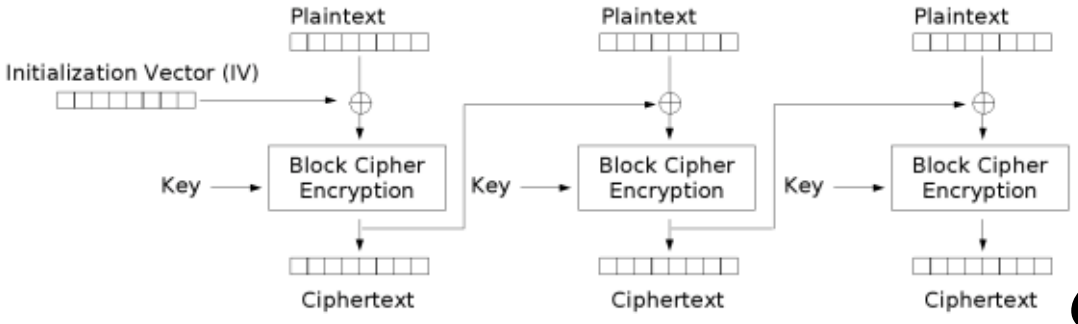


Electronic Codebook (ECB) mode encryption



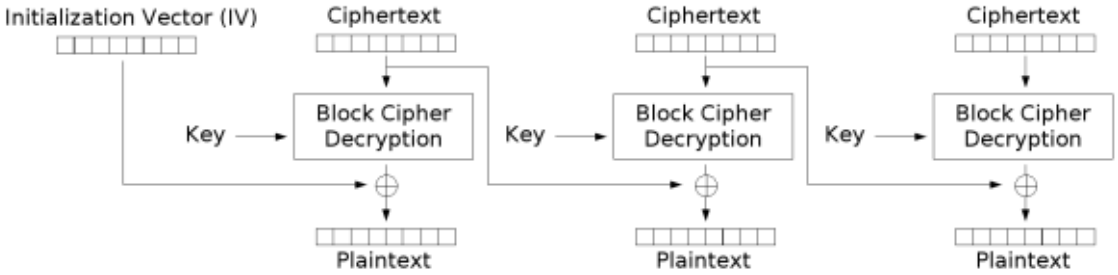
Electronic Codebook (ECB) mode decryption

Ciphertext Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

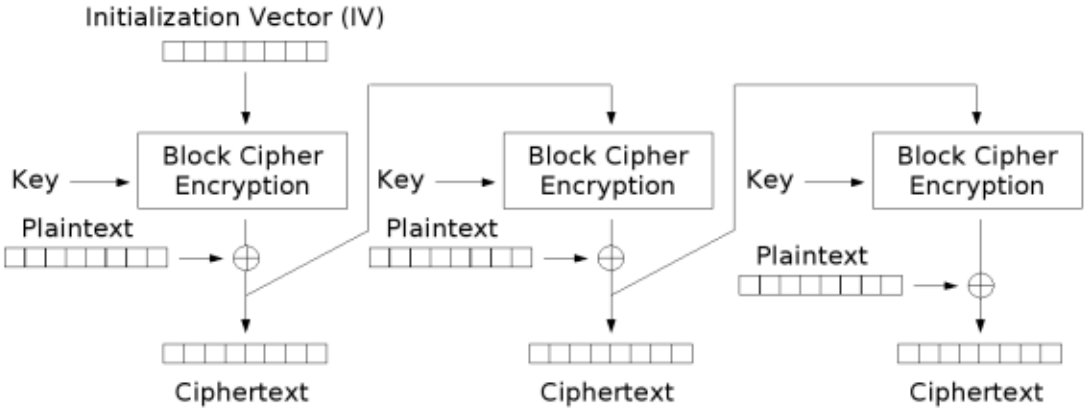
$$C_i = E_k(P_i \oplus C_{i-1}), C_0 = IV$$



Cipher Block Chaining (CBC) mode decryption

$$P_i = D_k(C_i) \oplus C_{i-1}, C_0 = IV$$

Cipher Feedback (CFB)

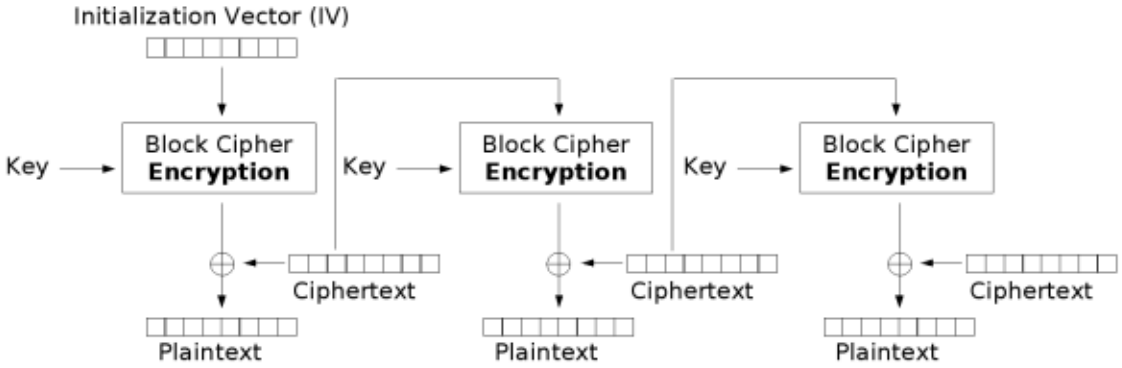


Cipher Feedback (CFB) mode encryption

$$C_i = E_k(C_{i-1}) \oplus P_i$$

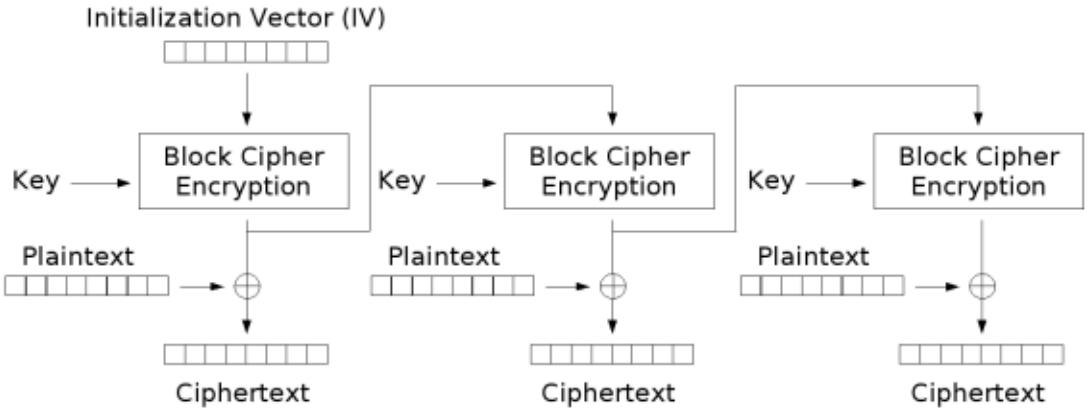
$$P_i = E_k(C_{i-1}) \oplus C_i$$

$$C_o = IV$$

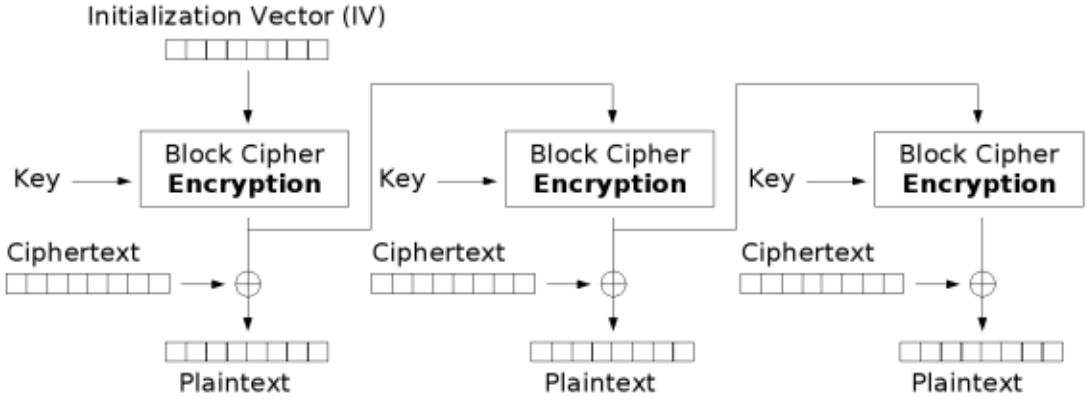


Cipher Feedback (CFB) mode decryption

Output Feedback (OFB)



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

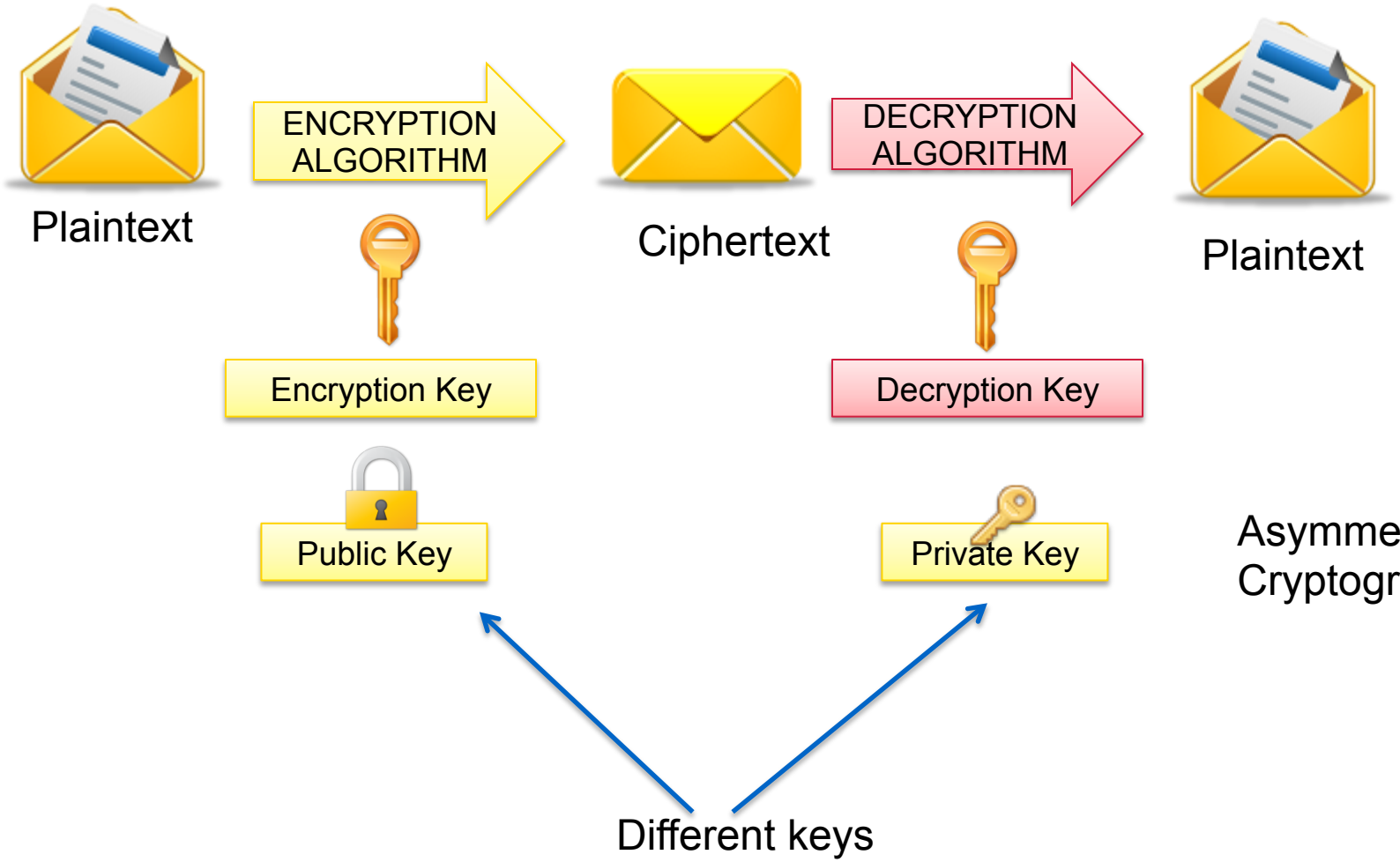
Selecting a Block Cipher Mode

- Small amounts of truly random data: ECB
  - Example: randomly generated keying material
  - Other modes can be used but ECB is most efficient
- Protocols with crypto integrity protection: CBC, CFB, OFB
- Arbitrary communications with arbitrary data: CBC, CFB
  - Repeated plaintext data is obscured
  - Constantly changing encryption keys defeat differential cryptanalysis attacks

Asymmetric Key Algorithm

- Also called public-key cryptography
  - Keep private key private
  - Anyone can see public key
- separate keys for encryption and decryption (public and private key pairs)
- Examples of asymmetric key algorithms:
  - RSA, DSA, Diffie-Hellman, El Gamal, Elliptic Curve and PKCS

Asymmetric Encryption



Asymmetric Key Algorithm

- RSA – the first and still most common implementation
- DSA – specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for authentication of messages
- Diffie-Hellman – used for secret key exchange only, and not for authentication or digital signature
- ElGamal – similar to Diffie-Hellman and used for key exchange
- PKCS – set of interoperable standards and guidelines

Symmetric vs. Asymmetric Key

Symmetric	Asymmetric
generally fast Same key for both encryption and decryption	Can be 1000 times slower Uses two different keys (public and private) Decryption key cannot be calculated from the encryption key Key lengths: 512 to 4096 bits Used in low-volume

Hash Functions

- produces a condensed representation of a message (hashing)
- The fixed-length output is called the hash or message digest
- A hash function takes an input message of arbitrary length and outputs fixed-length code. The fixed-length output is called the hash, or the message digest, of the original input message.
- A form of signature that uniquely represents the data
- Uses:
  - Verifying file integrity - if the hash changes, it means the data is either compromised or altered in transit.
  - Digitally signing documents
  - Hashing passwords

Hash Functions

- Message Digest (MD) Algorithm
  - Outputs a 128-bit fingerprint of an arbitrary-length input
- Secure Hash Algorithm (SHA)
  - SHA-1 produces a 160-bit message digest similar to MD5
  - Widely-used on security applications (TLS, SSL, PGP, SSH, S/MIME, IPsec)
  - SHA-256, SHA-384, SHA-512 are also commonly used, which can produce hash values that are 256, 384, and 512-bits respectively
- RIPEMD

Digital Signature

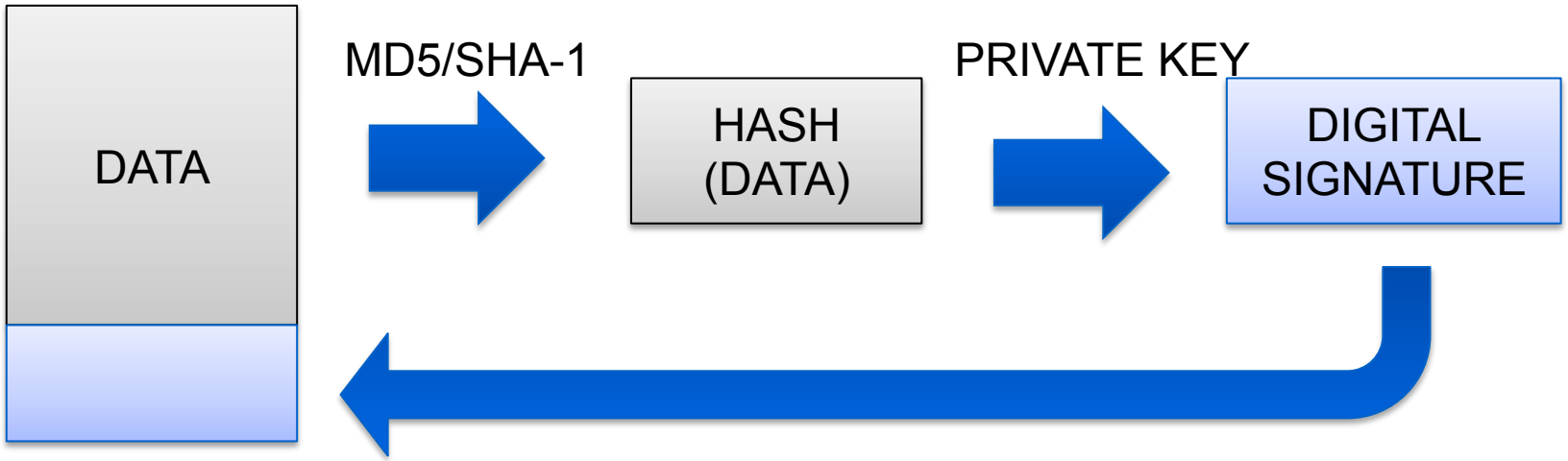
- A digital signature is a message appended to a packet
- The sender encrypts message with own private key instead of encrypting with intended receiver's public key
- The receiver of the packet uses the sender's public key to verify the signature.
- Used to prove the identity of the sender and the integrity of the packet

Digital Signature

- Two common public-key digital signature techniques:
  - RSA (Rivest, Shamir, Adelman)
  - DSS (Digital Signature Standard)
- Successful verification assures:
  - The packet has not been altered
  - The identity of the sender

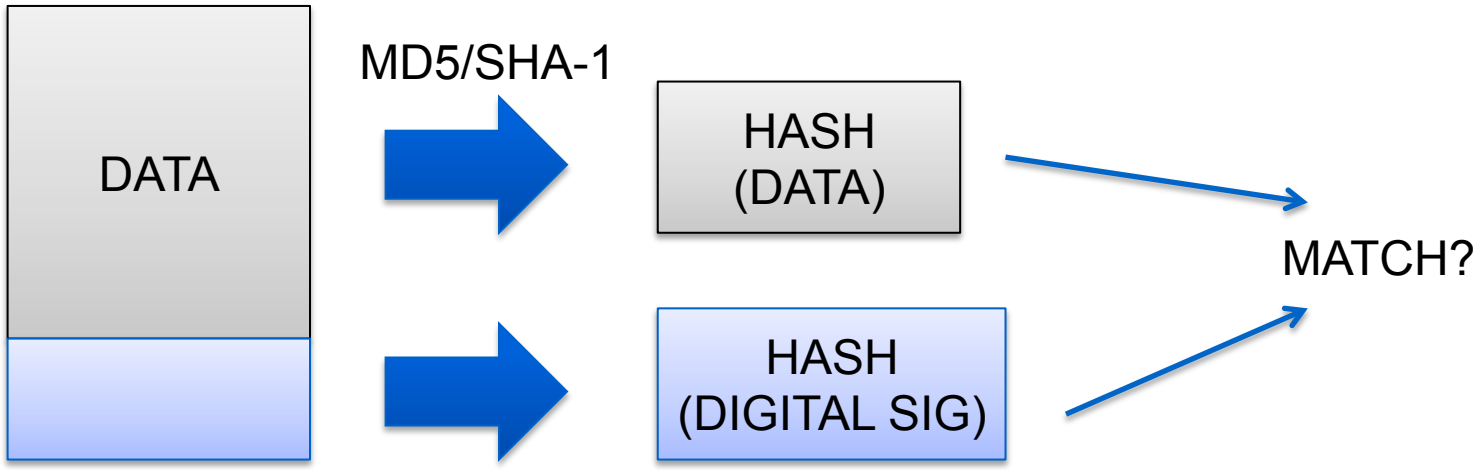
Digital Signature Process

1. Hash the data using one of the supported hashing algorithms (MD5, SHA-1, SHA-256)
2. Encrypt the hashed data using the sender's private key
3. Append the signature (and a copy of the sender's public key) to the end of the data that was signed)



Signature Verification Process

1. Hash the original data using the same hashing algorithm
2. Decrypt the digital signature using the sender's public key. All digital signatures contain a copy of the signer's public key
3. Compare the results of the hashing and the decryption. If the values match then the signature is verified. If the values do not match, then the data or signature was probably modified.



Questions?

Public Key Infrastructure

Network Security Workshop

APNIC

Overview

- Public Key Infrastructure
- Digital Certificates
- Certificate Authority
- RPKI Introduction

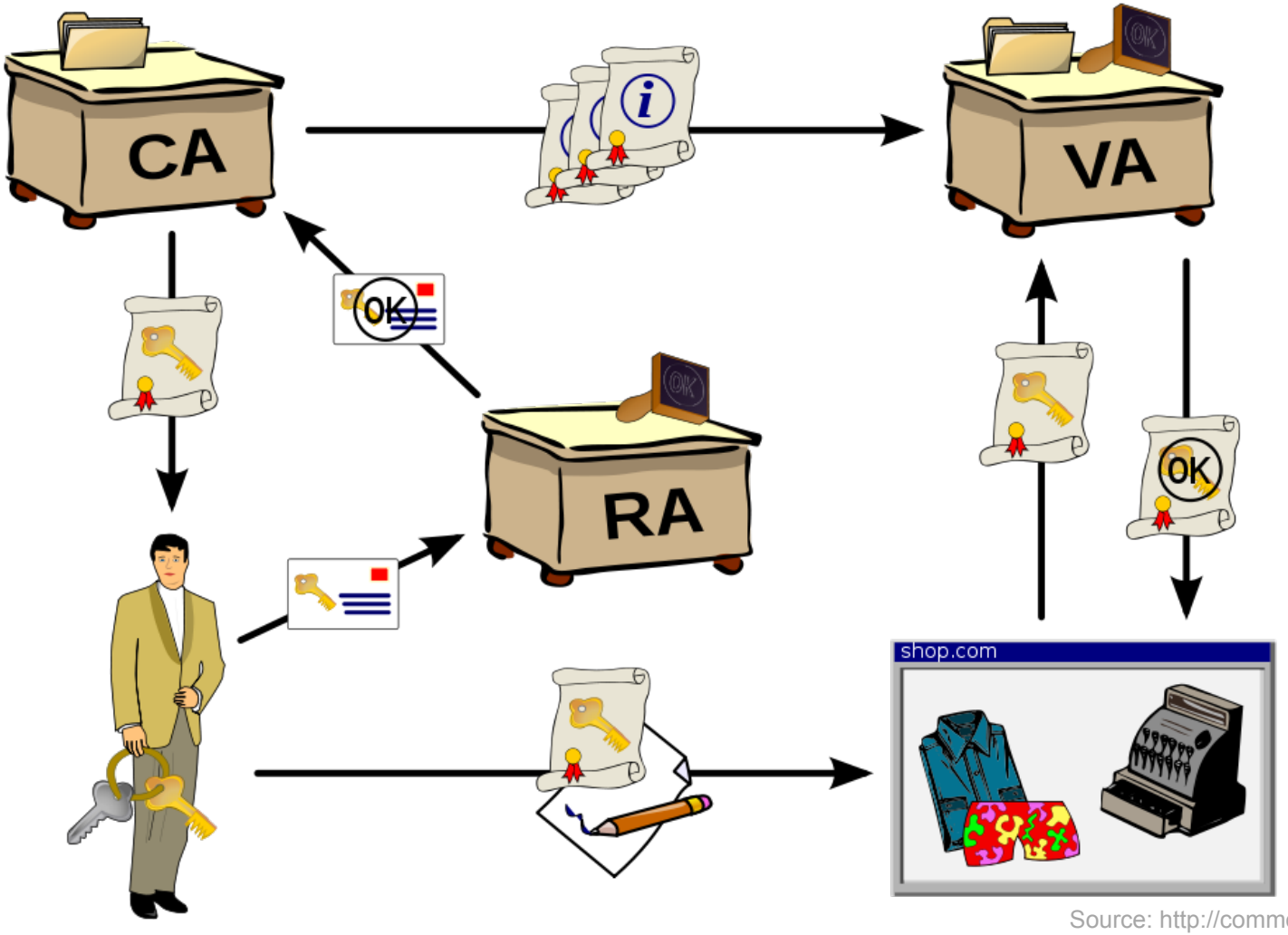
Public Key Infrastructure

- Framework that builds the network of trust
- Combines public key cryptography, digital signatures, to ensure confidentiality, integrity, authentication, nonrepudiation, and access control
- Protects applications that require high level of security

Functions of a PKI

- Registration
- Initialization
- Certification
- Key pair recovery
- Key generation
- Key update
- Cross-certification
- Revocation

Public Key Infrastructure



Source: http://commons.wikimedia.org

Components of a PKI

- Certificate authority
  - The trusted third party
  - Trusted by both the owner of the certificate and the party relying upon the certificate.
- Validation authority
- Registration authority
  - For big CAs, a separate RA might be necessary to take some work off the CA
  - Identity verification and registration of the entity applying for a certificate
- Central directory

Certificates

- Public key certificates bind public key values to subjects
- A trusted certificate authority (CA) verifies the subject's identity and digitally sign each certificate
  - Validates
- Has a limited valid lifetime
- Can be used using untrusted communications and can be cached in unsecured storage
  - Because client can independently check the certificate's signature
- Certificate is NOT equal to signature
  - It is implemented using signature
- Certificates are static
  - If there are changes, it has to be re-issued

Digital Certificate

- Digital certificate – basic element of PKI; secure credential that identifies the owner
- Also called public key certificate

Digital Certificate

- deals with the problem of
  - Binding a public key to an entity
  - A major legal issue related to eCommerce
- A digital certificate contains:
  - User's public key
  - User's ID
  - Other information e.g. validity period
- Certificate examples:
  - X509 (standard)
  - PGP (Pretty Good Privacy)
  - Certificate Authority (CA) creates and digitally signs certificates

Digital Certificate

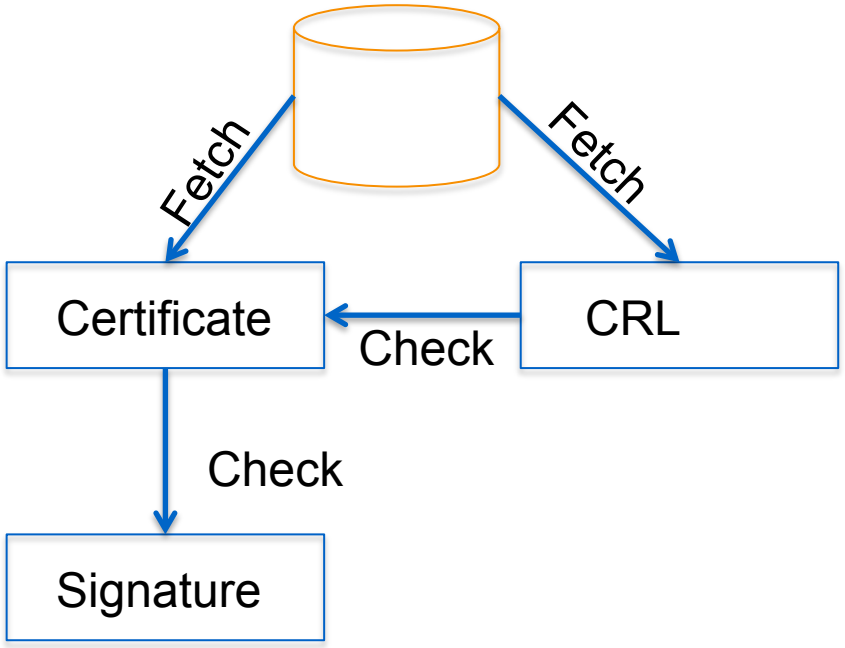
- To obtain a digital certificate, Alice must:
  - Make a certificate signing request to the CA
  - Alice sends to CA:
    - Her identifier IdA
    - Her public key KA_PUB
    - Additional information
- CA returns Alice's digital certificate, cryptographically binding her identity to public key:
  - CertA = {IDA, KA_PUB, info, SigCA(IDA,KA_PUB,info)}

X.509

- An ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI)
- Assumes a strict hierarchical system of Certificate Authorities (CAs)
- RFC 1422 – basis of X.509-based PKI
- Current version X.509v3 provides a common baseline for the Internet
- Structure of a Certificate, certificate revocation (CRLs)

X.509 Certificate Usage

- Fetch certificate
- Fetch certificate revocation list (CRL)
- Check the certificate against the CRL
- Check signature using the certificate



Every certificate contains…

- Body of the certificate
  - Version number, serial number, names of the issuer and subject
  - Public key associated with the subject
  - Expiration date (not before, not after)
  - Extensions for additional tributes
- Signature algorithm
  - Used by the CA to sign the certificate
- Signature
  - Created by applying the certificate body as input to a one-way hash function. The output value is encrypted with the CA's private key to form the signature value

Certificate Authority

- Issuer and signer of the certificate
- Trusted (Third) Party
  - Based on trust model
  - Who to trust?
- Types:
  - Enterprise CA
  - Individual CA (PGP)
  - Global CA (such as VeriSign)
- Functions:
  - Enrolls and Validates Subscribers
  - Issues and Manages Certificates
  - Manages Revocation and Renewal of Certificates
  - Establishes Policies & Procedures

Certificate Revocation Lists

- CA periodically publishes a data structure called a certificate revocation list (CRL).
- Described in X.509 standard.
- Each revoked certificate is identified in a CRL by its serial number.
- CRL might be distributed by posting at known Web URL or from CA's own X.500 directory entry.

Questions?

Resource Registration

Network Security Workshop

APNIC

Resource Registration

- As part of your membership agreement with APNIC, all Members are required to register their resources in the APNIC database.
  - First allocation/assignment, APNIC will create:
    - Inetnum or inet6num object
    - Autnum object (if you received an ASN)
    - Maintainer object (to protect your data)
    - Role object
- Members must keep records up to date:
  - Whenever there is a change in contacts
  - When new resources are received
  - When resources are sub-allocated or assigned

What is the APNIC Database?

- Public network management database
  - Operated by Internet Registries
    - Public data only
    - (For private data, please see “Privacy of customer assignment” module)
- Tracks network resources
  - IP addresses, ASNs, Reverse Domains, Routing policies
- Records administrative information
  - Contact information (persons/roles)
  - Authorization

Whois Database Query - Clients

- Standard whois client
  - Included with many Unix distributions
  - RIPE extended whois client
  - http://ftp.apnic.net/apnic/dbase/tools/ripe-dbase-client.tar.gz
- Query via the APNIC website
  - http://www.apnic.net/apnic-bin/whois2.pl
- Query clients – MS Windows etc

Object Types

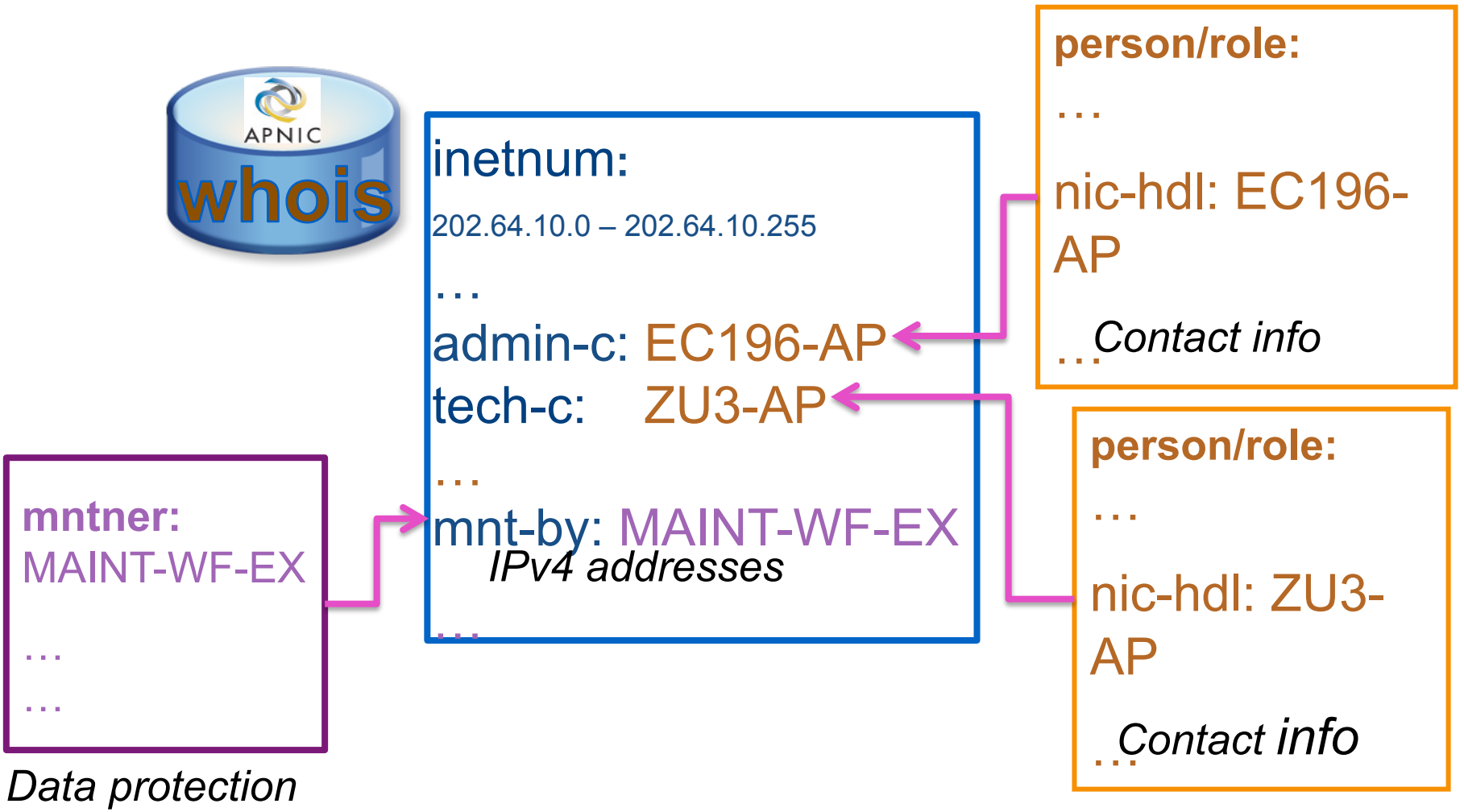
OBJECT	PURPOSE
• person	contact persons
• role	contact groups/roles
• inetnum	IPv4 addresses
• Inet6num	IPv6 addresses
• aut-num	Autonomous System number
• domain	reverse domains
• route	prefixes being announced
• mntner	(maintainer) data protection
• mnt-irt	Incident Response Team

http://www.apnic.net/db/

Database Object

- An object is a set of attributes and values
- Each attribute of an object…
  - Has a value
  - Has a specific syntax
  - Is mandatory or optional
  - Is single or multi-valued
- Some attributes are …
  - Primary (unique) keys
  - Lookup keys for queries
  - Inverse keys for queries
- Object templates illustrate this structure

Inter-Related Objects



New Members

- If you are receiving your first allocation or assignment, APNIC will create the following objects for you:
  - role object
  - inetnum or inet6num object
  - maintainer object (to protect your data)
  - aut-num object (if you received an ASN)
- Information is taken from your application for resources and membership

Inetnum / Inet6num Objects

- Contains IP allocation and assignment information
- APNIC creates an inetnum (or inet6num) object for each allocation or assignment they make to the Member
- All members must create inetnum (or inet6num) objects for each sub-allocation or assignment they make to customers

Whois – Inet6num Example

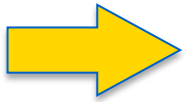
```
inet6num:       2001:0DF0:000A::/48
netname:        APNIC-TRAININGIPv6-DC-20080424
descr:          APNIC Training IPv6 Address for data centre
country:        AU
admin-c:        AT480-AP
tech-c:         AT480-AP
status:         ASSIGNED PORTABLE
mnt-by:         MAINT-AU-APNICTRAINING
mnt-routes:     MAINT-AU-APNICTRAINING
remarks:        -+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:        This object can only be updated by APNIC hostmasters.
remarks:        To update this object, please contact APNIC
remarks:        hostmasters and include your organisation's account
remarks:        name in the subject line.
remarks:        -+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
changed:        hm-changed@apnic.net 20080424
changed:        hm-changed@apnic.net 20100818
source:         APNIC
```

Person Object

- Represents a contact person for an organization
  - Every Member must have at least one contact person registered
  - Large organizations often have several contacts for different purposes
- Is referenced in other objects
- Has a nic-hdl
  - Eg. EC17-AP

What is a ‘nic-hdl’?

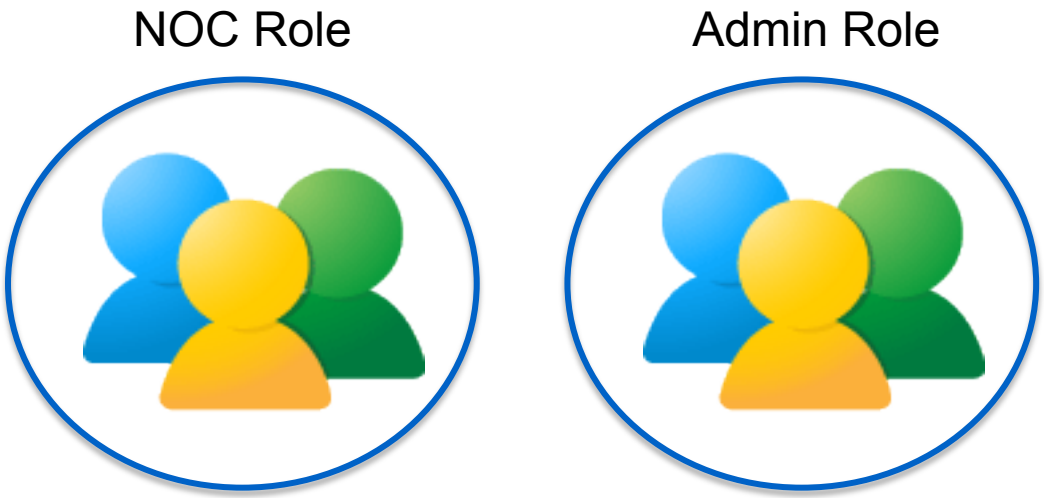
- Unique identifier for a person or role
- Represents a person or role object
  - Referenced in objects for contact details
    - (inetnum, aut-num, domain…)
  - format: <XXXX-AP>
    - Eg: EC196-AP



```
Person: Eric Chu
address:      ExampleNet Service Provider
address:      Level 1 33 Park Road Milton
address:      Wallis and Futuna Islands
country:      WF
phone:        +680-368-0844
fax-no:       +680-367-1797
e-mail:       echu@example.com
nic-hdl: EC196-AP
mnt-by:       MAINT-WF-EX
changed:      echu@example.com 20020731
source:       APNIC
```

Role Object

- Represents a group of contact persons for an organization
  - Eases administration
  - Can be referenced in other objects instead of the person objects for individuals
- Also has a nic-hdl
  - Eg. HM20-AP



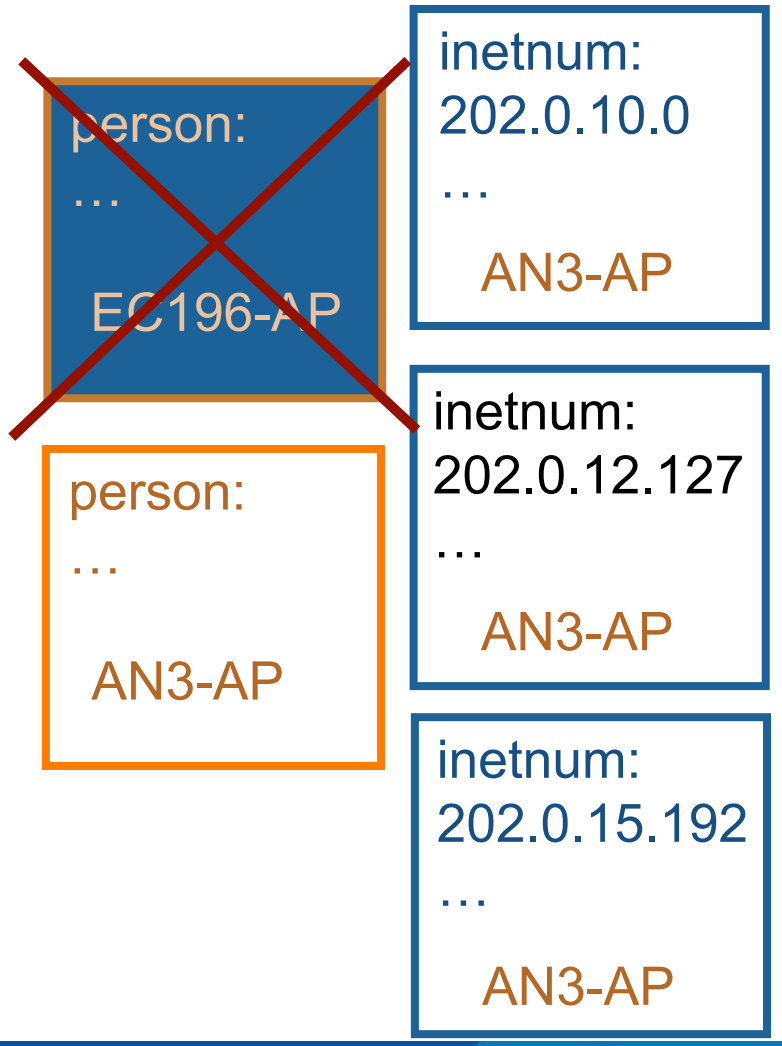
How a Role Object Works

- Role Object is used instead of a Person Object as a reference in other objects
- If a contact leaves the organization:
  - New Person Object is created
  - The nic-hdl of the new contact replaces nic-hdl of the old person in the Role Object
  - Old Person Object is deleted
- This means only a single replacement is required instead of many

Replacing Contacts in the DB - Using Person Objects

E. Chu is leaving my organization.
A. Nagali is replacing him.

1. Create a Person Object for new contact (***E. Chu***)
2. Find all objects containing old contact (***E. Chu***)
3. Update all objects, replacing old contact (EC196-AP) with new contact (AN3-AP)
4. Delete old contact's (EC196-AP) Person Object

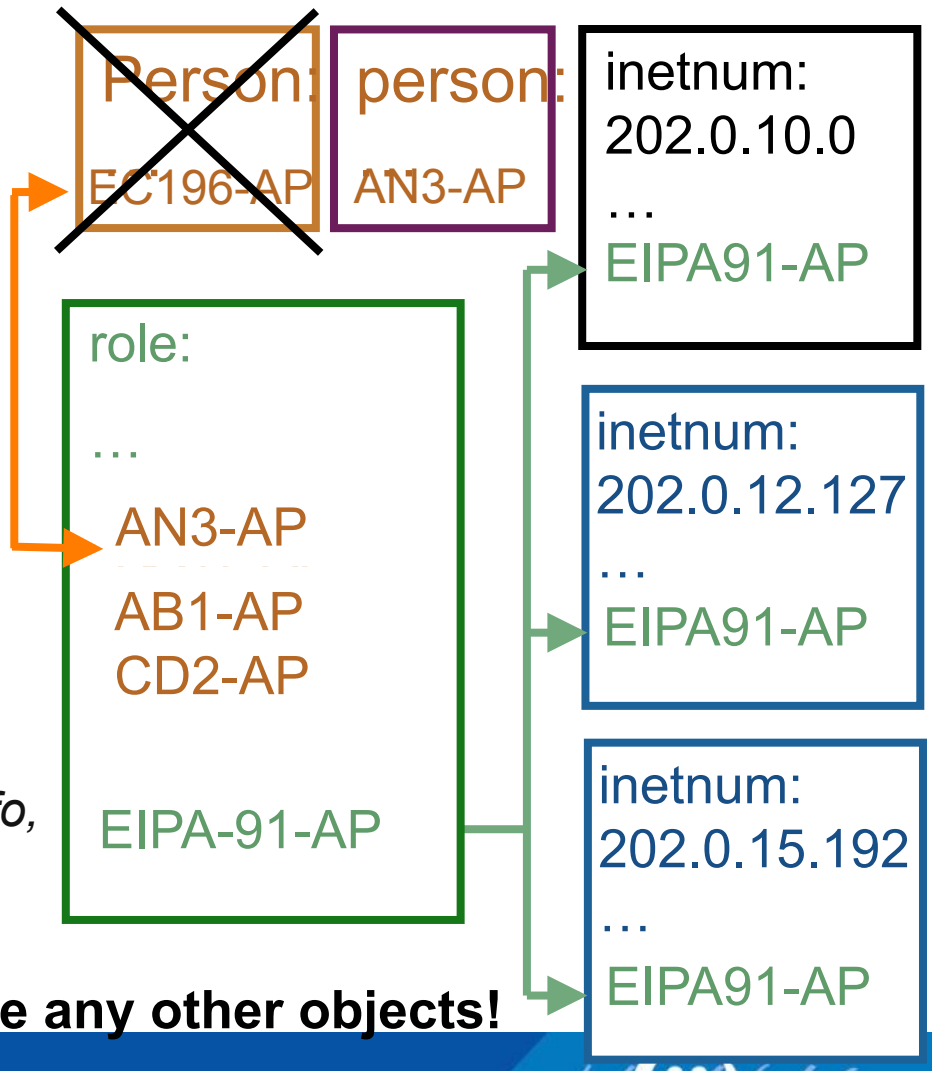


Replacing Contacts in the DB – Using a Role Object

E. Chu is leaving my organization.
A. Nagali is replacing him.

1. Create a Person Object for new contact (A. Nagali)
2. Replace old contact (EC196-AP) with new contact (AN3-AP) in Role Object
3. Delete old contact's Person Object.

My Role Object contains all contact info, that is referenced in all my objects.



No need to update any other objects!

Whois - Role vs Person Objects

```
% APNIC found the following authoritative answer from: whois.apnic.net

% [whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

role:           APNIC Training
address:        Level 1 33 Park Rd. 4064 Milton, Brisbane
country:        AU
phone:          +617 38583100
fax-no:         +617 38583199
e-mail:         training@apnic.net
admin-c:        AA196-AP
tech-c:         AA196-AP
nic-hdl:        AT480-AP
mnt-by:         MAINT-AU-APNICTRAINING
changed:        hm-changed@apnic.net 20080424
source:         APNIC

person:         Amante Alvaran
nic-hdl:        AA196-AP
e-mail:         amante@apnic.net
address:        Level 1 33 Park Road Milton
address:        Brisbane QLD Australia
phone:          +617-3858-3100
fax-no:         +617-3858-3199
country:        AU
mnt-by:         MAINT-AU-APNICTRAINING
changed:        hm-changed@apnic.net 20051025
changed:        hm-changed@apnic.net 20080424
source:         APNIC
```

IRT Object

- Incident Response Team (IRT)
  - Dedicated abuse handling teams (not netops)
- Implemented in Nov 2010 through Prop-079
- Abuse contact information
- Mandatory object reference in inetnum, inet6num, and aut-num objects

IRT Object

- Why provide abuse contact
  - Dedicated contacts or team that specifically resolve computer security incidents
  - Efficient and accurate response
  - Stops the tech-c and admin-c from getting abuse reports
  - Shared response to address abuse

Database Protection - Maintainers

- protects other objects in the APNIC Whois Database
- used to prevent unauthorized persons from changing the details in whois
- Multiple levels of maintainers exist in a hierarchical manner
  - Maint-by
  - Maint-lower
- Applied to any object created directly below that maintainer object

Database Protection

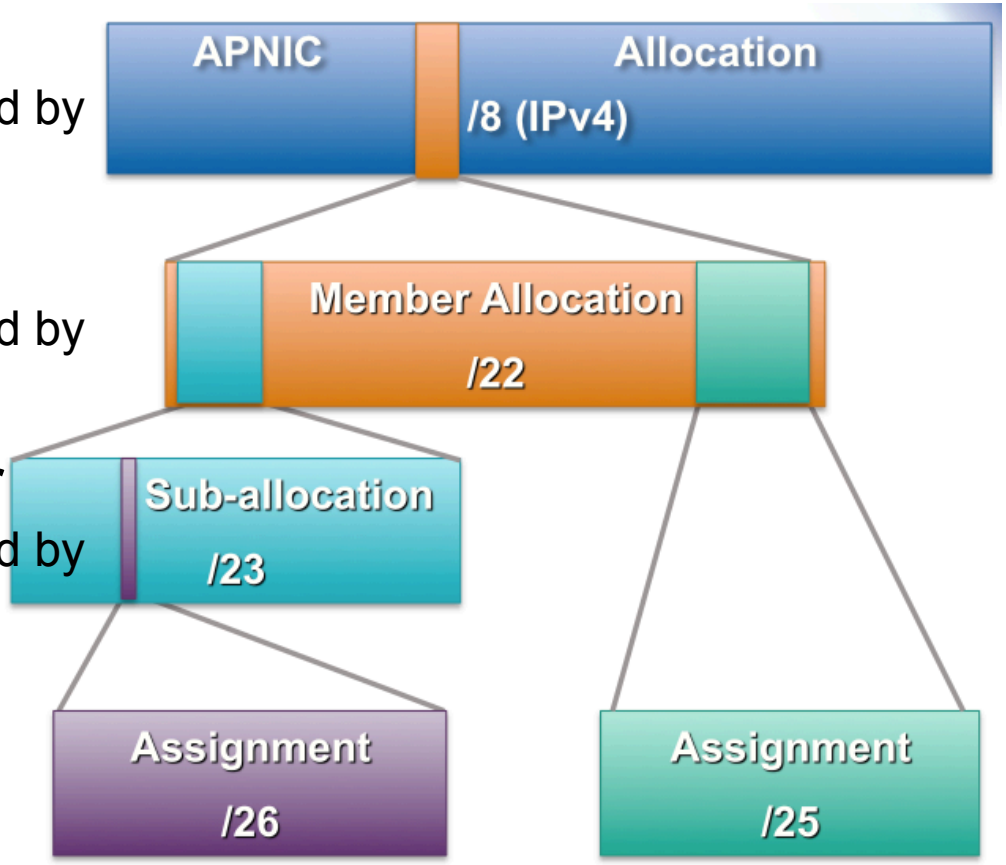
- **Authorisation**
  - "mnt-by" references as maintainer object
    - Can be found in all database objects
    - "mnt-by" should be used with every object
- **Authentication**
  - Updates to an object must pass the authentication rule specified by its maintainer
  - Authentication methods (using 'auth' attribute)
    - Crypt-PW
    - PGP – GNUPG
    - MD5

Database Protection
Maintainer Object

```
mntner:         MAINT-AU-APNICTRAINING
descr:          APNIC Training
country:        AU
admin-c:        AA196-AP
tech-c:         AA196-AP
auth:           MD5-PW $1$FUrnj.4g$sIyzbkZj2XJoDanL/ndXN0
mnt-by:         MAINT-AU-APNICTRAINING
upd-to:         amante@apnic.net
referral-by:    APNIC-HM
changed:        hm-changed@apnic.net 20080424
changed:        hm-changed@apnic.net 20090325
changed:        hm-changed@apnic.net 20090403
changed:        hm-changed@apnic.net 20090702
changed:        hm-changed@apnic.net 20091111
changed:        hm-changed@apnic.net 20091217
changed:        hm-changed@apnic.net 20100528
source:         APNIC
```

Maintainer Hierarchy Diagram

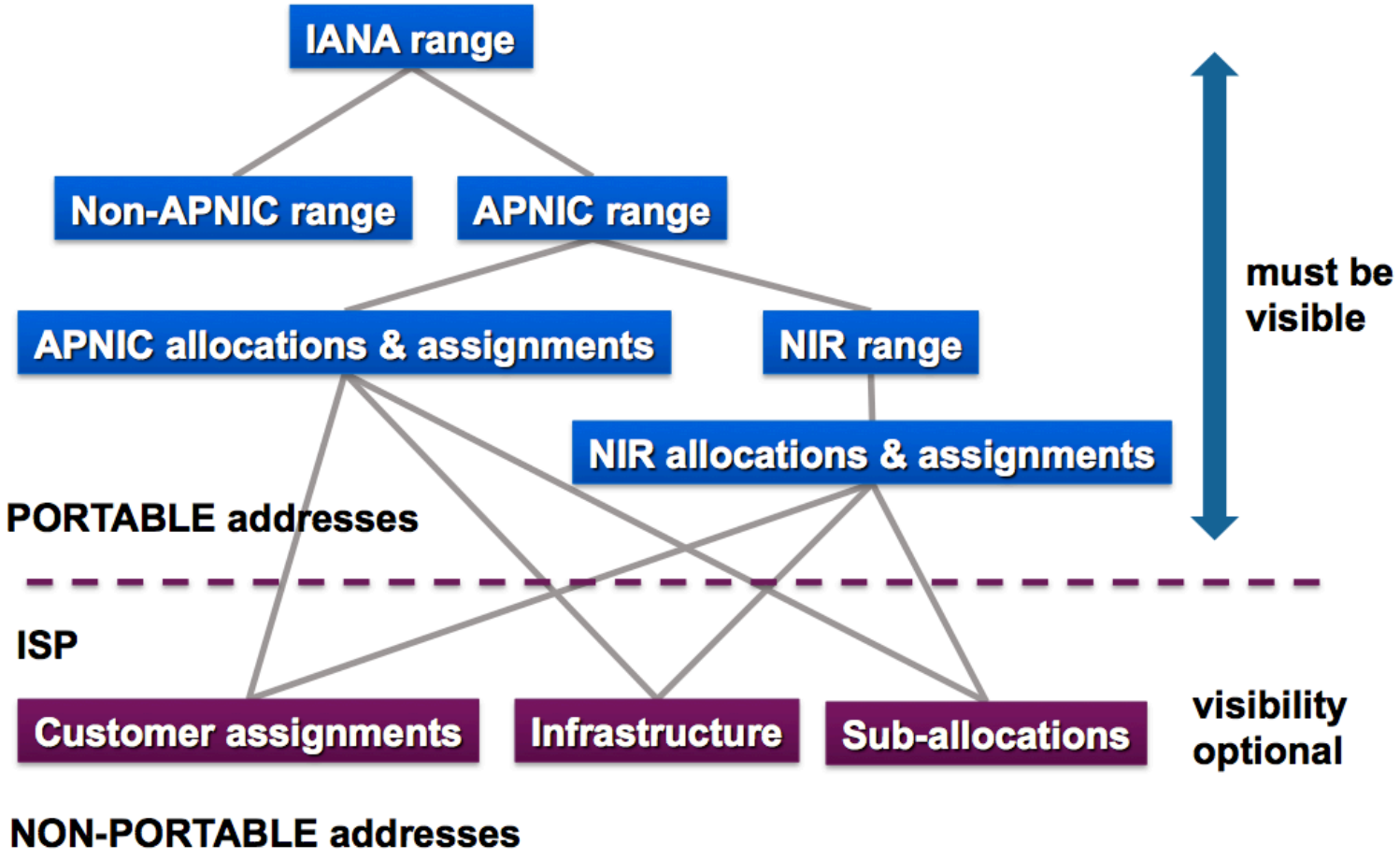
- **Allocated to APNIC**
  - Maint-by can only be changed by IANA
- **Allocated to Member**
  - Maint-by can only be changed by APNIC
- **Sub-allocated to Customer**
  - Maint-by can only be changed by Members



Customer Privacy

- Privacy issues
  - Concerns about publication of customer information
  - Increasing government concern
- APNIC legal risk
  - Legal responsibility for accuracy and advice
  - Damages incurred by maintaining inaccurate personal data
- Customer data is hard to maintain
- Customer assignment registration is still mandatory

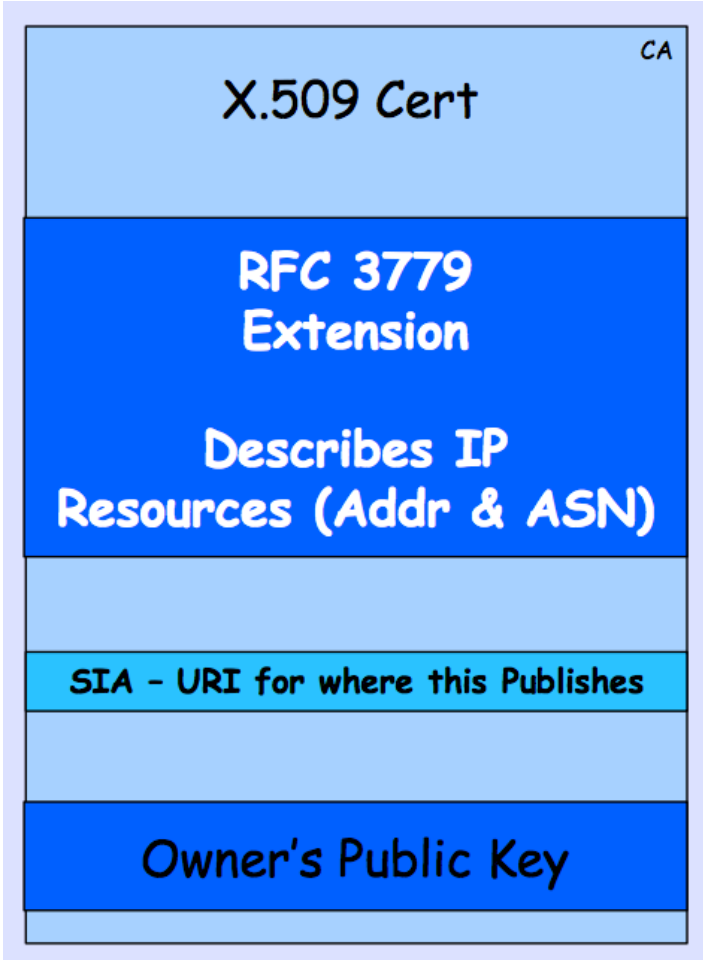
What Needs to be Visible?



RPKI

- Resource Public Key Infrastructure
- verify the authenticity of data that has been digitally signed by the originator of the data
- Based on the X.509 certificate format (RFC5280) and extended by RFC3779
- RPKI is in the process of standardization through the Secure Inter-Domain Routing (SIDR) working group.

X.509 Certificate + 3779 Ext



Resource Certification

- RIRs have been developing a new service for their members
- APNIC has now launched Resource Certification for the AP region
- The goal is to improves the security of inter-domain routing and augmenting the information published in the APNIC Whois Database

Terminologies

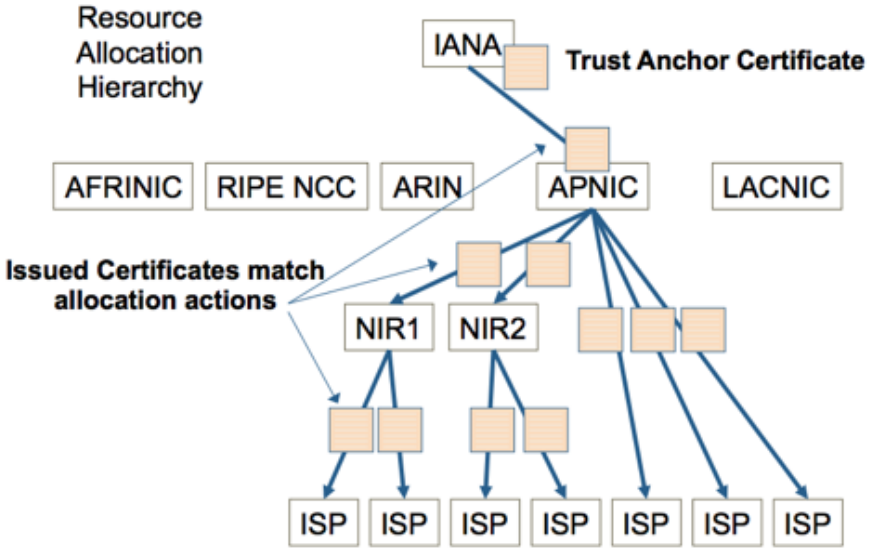
- Resource holders include:
  - Regional Internet Registries (RIRs)
  - Local Internet Registries (LIRs)
  - Internet Service Providers (ISPs)
  - End-user organizations
- Internet resources are:
  - IPv4 and IPv6 address blocks
  - Autonomous System (AS) numbers

Resource Certification Benefits

- Routing information corresponds to properly delegated address resources
- Resource Certification gives resource holders proof that they hold certain resources
- Resource holders can attest to those resources when distributing them
- Resource Certification is a highly robust means of preventing the injection of false information into the Internet's routing system.

Resource Public Key Infrastructure

- RPKI hierarchy is based on the administrative resource allocation hierarchy
  - IANA → RIRs → LIRs → end-users
- Main components:
  - Trust anchors
  - ROAs
  - validators



Route Origin Attestations (ROAs)

- allow entities to verify that an autonomous system (AS) has been given permission by an IP address block holder to advertise routes to one or more prefixes within that block. We call this mechanism a Route Origin Attestation (ROA).
- The certificate holder uses their private key to sign an ROA for specific IP address blocks to be routed by a specific AS, and this can be tested and verified by the public key, and the certificate hierarchy.
  - Example: the ROA might state the following: "ISP 4 permits AS 65000 to originate a route for the prefix 192.2.200.0/24”

More Info on RPKI

- RPKI Origin Validation, Randy Bush
- Securing BGP with BGPsec, Geoff Huston and Randy Bush

Questions?

Device & Infrastructure Security

Network Security Workshop

APNIC

Overview

- Server Hardening
- Layer 2 Security
- Layer 3 Security
- Routing Security

Server Hardening

- Use netstat to check which ports you are currently listening on your Linux machine.
  - Close unnecessary ports
- Remove unused applications. Minimal software means less possible vulnerabilities
- Perform regular software patches and update.
- Disable unwanted services and remove from startup items
- Use TCP wrappers and properly configure hosts.allow and hosts.deny files.
- **Rule of thumb:** *deny all, allow as necessary*

Server Hardening: Accounts

- Disable default accounts and groups that are not needed
- Use strong authentication
- Good password policy
  - Minimum number of characters
  - Combination of alphabets, numbers, special characters, upper and lower case
  - Implement password aging
  - Force users to change password on first login
  - Prevent use of previous passwords
- Lock account after a number of failed logins

Backup and Recovery

- A backup system is a fundamental element of any disaster recovery plan
- Provides for disaster recovery of key network services and any file
- Physical vs Logical backup
  - Physical backup – create copy of the files into some other location, such as disks or tapes
  - Logical backup – remote, cloud services

Backup and Recovery

- Type of Backup
  - Full backup – entire dataset regardless whether it has been altered or not; take longer
  - Incremental backups – only backs up data that has been changed since last backup
  - Differential backups – backups data that has changed since the last full backup
  - Copy backups – full backups without a reset of archive bits
- Backup intervals
  - Daily incremental
- Backup media
  - Offline backups: Magnetic Tapes, Optical drives, Hard disk
  - Offsite backups: Network, NAS, Data center

Backup and Recovery

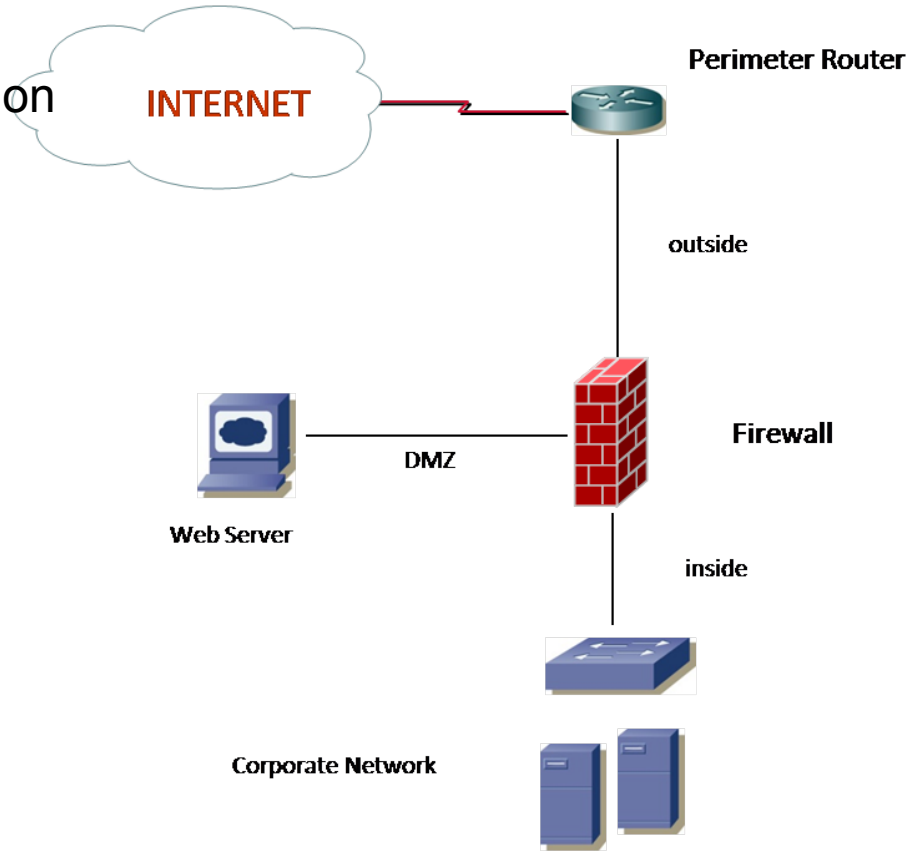
- Always test that your backups are restorable
- Restoration should be within a reasonable period of time
  - time to recover
  - Priority of some files over others

Logging

- All security-related events must be logged
- Audits must be performed on a regular basis
- In a Linux system:
  - monitor log messages using logwatch
  - Perform system accounting using auditd

Network Devices

- Attack areas:
  - Default passwords
  - Broadcasting packets replicated on all ports
  - rogue devices participate in STP and mislead it
  - packet flooding using spoofed MAC addresses
  - Gaining management access



Network Devices

- Change the default settings
- Allow management sessions only from approved sources
- Use AAA server to authenticate administrators, authorize their actions and perform accounting of all actions
- Encrypt sessions
- Limit device access
  - Console sessions should also be authenticated
- Admin actions should be authorized through a AAA server
- Disable password recovery

Network Devices: Routers

- Use strong authentication
- Disable unused services
- Modify insecure default settings
- Authenticate IGP messages
- Check software versions for security-related bugs

Increasing Port Security

- CAM entry aging
- Static or permanent CAM entries
- Limit MAC addresses per port
- Disable unused port
- Port authentication with IEEE 802.1X

Mitigation of ARP Spoofing

- Static ARP entries
- Secure ARP inspection
  - Secure ARP Discovery (SAD)
- Separate VLANs with unique IP subnets
- Private VLAN
- IEEE 802.1X port authentication

Port Authentication using 802.1X

- 802.1X is an IEEE standard defining layer 2 protocol used for authentication purposes
- 3 authentication protocols
  - EAP-MD5 (challenge response auth protocol)
  - EAP-OTP (proprietary one-time password)
  - EAP-TLS (using digital certificates)

Spanning Tree Protocol

- Used to prevent loops in a switched LAN by disabling redundant links (IEEE 802.1D)
- STP takes 30-50 seconds to converge
- Misplacement of the root bridge can cause suboptimal paths
- Loss of the root bridge has the most effect on performance
- STP does not include any security by default

Trunking

- Allows multiple VLANs to be carried over one physical link. This may expose the whole network to a single port if not configured properly.
- An intruder can also interfere with VTP messages and cause VLANs to disappear
- Must disable trunking on a port

VLAN Trunking Protocol (VTP)

- used to make VLAN management easier in large switched LAN environments
- VTP should use authentication to prevent unauthorised devices from participating in VTP
- VTP can use MD5 to authenticate VTP messages
- The same password has to be used on all devices in a VTP domain
- Replay attacks are not possible

Security Best Practices

- For VLANs and Trunking
  - Always use a dedicated VLAN ID for all trunk ports
  - Disable unused ports and put them in an unused vlan
  - Do not use VLAN 1 for anything
  - Disable auto-trunking on user facing ports (DTP off)
  - Explicitly configure trunking on infrastructure ports
  - Use all tagged mode for the native VLAN on trunks
  - Use PC Voice VLAN access on phones that support it
  - Use 802.1q tag on all the trunk ports

VLAN 1

- A special VLAN used as a default vlan assigned to L2 device ports.
- Generic rule: “network administrators should pruse any VLAN, and in particular VLAN 1, from all theports where that VLAN is not strictly needed”

Network Hardening (Layer 3)

- Interior gateway protocol (IGP) - exchange routing information between routers inside the network
  - OSPF, EIGRP, RIPv2, IS-IS
- Exterior Gateway Protocol (EGP) - exchange routes with Internet Service Providers (ISPs)
  - BGP

Threats to Routing Protocols

- Deliberate exposure – attacker takes control of a router and intentionally releases routing information top other entities
- Sniffing – attackers monitor and/or record the routing exchanges between authorized routers to sniff for routing information.
- Traffic analysis – attackers gain routing information by analyzing the characteristics of the data traffic on a subverted link.
- Spoofing – illegitimate device assumes the identity of a legitimate one.
- Falsification – attacker sends false routing information.
- Interference – attacker inhibits the exchanges by legitimate routers.
- Overload – attackers place excess burden on legitimate routers.

RFC 4593

Securing Routing Protocols

- an authentication mechanism should be used to prevent accidental or deliberate adjacencies from being established
  - password system should be secret and changed regularly
- authenticate routing updates
- security only verifies the source of the information
  - no encryption of the routing update contents
  - any packet interception will allow read-access

Cisco IOS Features

- **Control Plane Policing**
  - allows users to configure a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks
  - Control plane can help maintain packet forwarding despite an attack or heavy traffic load
- **Unicast RPF**
  - limits malicious traffic by enabling a router to verify the reachability of the source address in packets being forwarded.

Bogons

- Bogons – Martians and netblocks that have not been allocated to an RIR by IANA.
- Fullbogons – a larger set which also includes IP space that has been allocated to an RIR, but not assigned by that RIR to an actual ISP or other end-users.

http://www.team-cymru.org/Services/Bogons/

Bogons (BGP)

```
Cisco Router Traditional bogons
router bgp <your asn>
  neighbor x.x.x.x remote-as 65333
  neighbor x.x.x.x ebgp-multihop 255
  neighbor x.x.x.x description <your description>
  neighbor x.x.x.x prefix-list cymru-out out
  neighbor x.x.x.x route-map CYMRUBOGONS in
  neighbor x.x.x.x password <your password>
  neighbor x.x.x.x maximum-prefix 100 threshold
90
```

http://www.team-cymru.org/Services/Bogons/bgp.html

Bogons (BGP)

```
! Remember to configure your Cisco router to handle the new style
! community syntax.
ip bgp-community new-format
!
! Set a bogon next-hop on all routers that receive the bogons.
ip route 192.0.2.1 255.255.255.255 null0
!
! Configure a community list to accept the bogon prefixes into the
! route-map.
ip community-list 10 permit 65333:888
!
! Configure the route-map.  Remember to apply it to the proper
! peering sessions.
route-map CYMRUBOGONS permit 10
  description Filter bogons learned from cymru.com bogon route-servers
  match community 10
  set ip next-hop 192.0.2.1
!
ip prefix-list cymru-out seq 5 deny 0.0.0.0/0 le 32
```

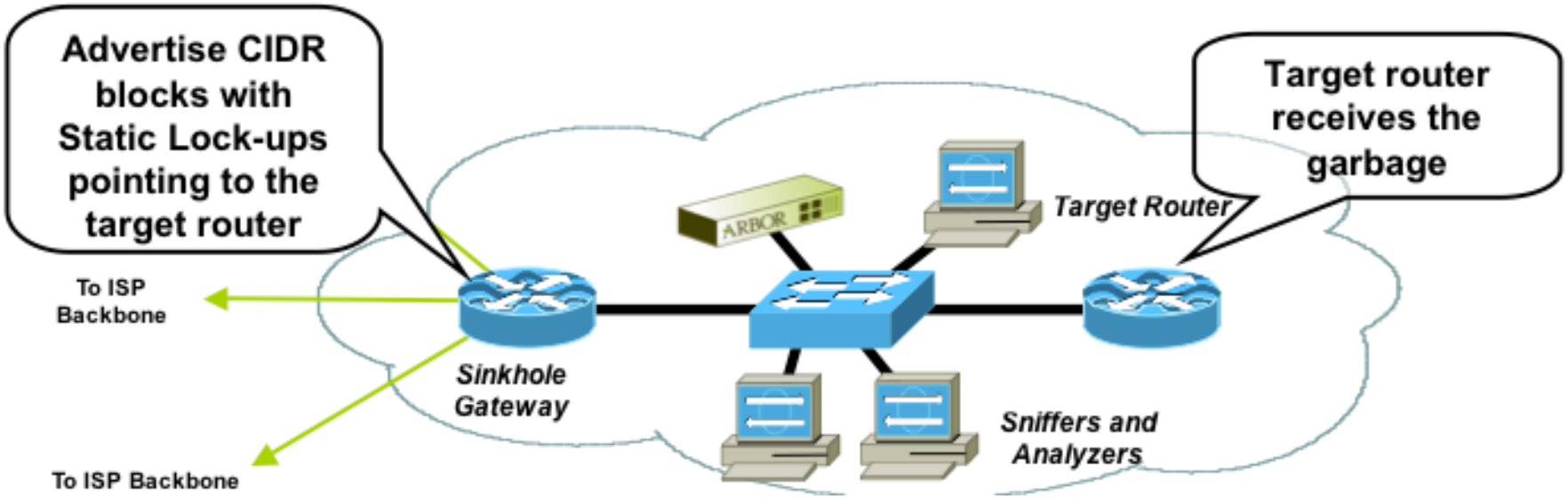
Bogons (BGP Peer-Group)

```
router bgp <your asn>
  neighbor cymru-bogon peer-group
  neighbor cymru-bogon ebgp-multihop 255
  neighbor cymru-bogon description <general description>
  neighbor cymru-bogon prefix-list cymru-out out
  neighbor cymru-bogon route-map CYMRUBOGONS in
  neighbor cymru-bogon maximum-prefix 100 threshold 90
! You'll need to increase the maximum to at least 50000 with
an
! appropriate thresholds if you're receiving one or both
fullbogons
! feeds.
!
  neighbor x.x.x.x remote-as 65333
  neighbor x.x.x.x peer-group cymru-bogon
  neighbor x.x.x.x description <specific description>
  neighbor x.x.x.x password <your password>
```

BGP Security

- **Real-time Blackhole Routing (RTBH)**
  - Packets are forwarded to a router's bit bucket – either a null interface or a discard interface)
  - desired packets are dropped with minimal or no performance impact
  - Employing uRPF in conjunction with RTBH can provide source-based solution vs destination-based
- **BGP Diversion**
  - Uses BGP to divert traffic to sinkholes or any packet "scrubbing" centers for further analysis
  - Divert via resetting BGP next hop to ip address of analysis system(s) or matching community tags that result in different BGP next hops being assigned for a given prefix
- **BGP Route Tagging**
  - Tag routes using BGP communities to apply filtering, rate limiting, QoS, firewall, or any other policy on packets

Sinkholes


Advertise CIDR blocks with Static Lock-ups pointing to the target router
Target router receives the garbage
ARBOR
Target Router
To ISP Backbone
Sinkhole Gateway
Sniffers and Analyzers
To ISP Backbone

Questions?

Operational Security

Network Security Workshop

APNIC

Overview

- Physical and Logical Security
- Security Management
- Security Policies

Physical and Logical Security

- One of the most neglected areas of security
- Equipment access must be restricted
- Password protect (avoid clear-text) console login
- Avoid using telnet

Security Management

- Network security is a part of a bigger information security plan
- Policies vs Standards vs Guidelines
- Must develop and implement comprehensive security policy
  - Minimum password length
  - Frequency of password change
  - Access of devices
  - User creation/deletion process
- Disaster Recovery and Attack Mitigation Plan

Polices, Standards and Guidelines

- Policies are aimed at informing users as well as layout the baseline for security.
- Based on these policies, we can set up standards – including for example use of specific technologies in a uniform way.
- Guidelines are not mandatory, but best practices

First Step….. Security Policy

- Design Policy
  - Study and analyze your network environment
  - Develop a threat model
  - Perform a security vulnerability assessment
- Implement Policy
  - Use appropriate technology
  - Train all employees
- Enforce Policy
  - Automate and audit

Security Policy

- A formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.
- Creates a "baseline" or framework of your network's security implementation
  - Define the allowed behaviors
  - Define roles
  - Define how to handle security incidents

Source: Cisco Introduction to Network Security, 2003

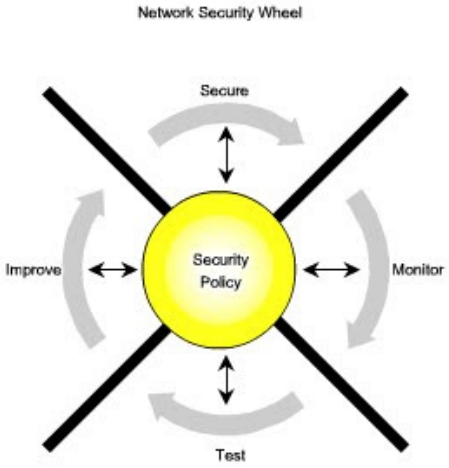
Security Policy: What it Should Contain?

- Definition
  - Define data and assets to be covered by the security policy
- Identity
  - How do you identify the hosts and applications affected by this policy?
- Trust
  - Under what conditions is communication allowed between networked hosts?
- Enforceability
  - How will the policies implementation be verified?
- Risk Assessment
  - What is the impact of a policy violation? How are violations detected?
- Incident Response
  - What actions are required upon a violation of a security policy?

Source: Cisco Introduction to Network Security, 2003

Security Wheel

- Promotes a continuous process of securing, monitoring, auditing, and managing
- Based on the security policy
- Steps:
  1. Secure the network by applying the security policy and implementing the security solutions
  2. Monitor and Respond
  3. Audit/Test
  4. Manage and Improve



Considerations For Security Policy

- What are you trying to protect?
  - What data is confidential?
  - What resources are precious?
- What are you trying to protect against?
  - Unauthorized access to confidential data?
  - Malicious attacks on network resources?
- How do regulatory issues affect your policy?

The Security Policy Should Include…

- Physical security controls
  - Media
  - Equipment location
  - Environmental safeguards

- Logical security controls
  - Subnet boundaries
  - Routing boundaries
  - Logical access control

The Security Policy Should Include…

- System and data integrity
  - Firewalls
  - Network services
- Data confidentiality
- Mechanisms to verify/monitor security controls
  - Accounting
  - Management
  - Intrusion detection

The Security Policy Should Include….

- Policies and procedures for staff
  - Secure backups
  - Equipment certification
  - Use of Portable Tools
  - Audit Trails
  - Incident Handling

- Appropriate security awareness training for users of the corporate network

Security Policy

- “formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.” – RFC 2196
- Purpose: “inform users of their obligatory requirements for protecting technology and information assets”

Organizational Security

- A well-constructed security policy is a great weapon in the fight to preserve the safety and integrity of an organization's technical and intellectual assets.
- The most important part of organizational security is YOU.

Security Audit

- organized technical assessment of the security strengths and weaknesses of an IT infrastructure.
- includes servers and hardware (firewalls, routers, switches, IDSes and IPSes)

Intrusion Detection

- Common Detection Methodologies
  - Signature-based Detection
    - Compares signatures against observed events to identify possible incidents
  - Anomaly-based Detection
    - Comparing definitions of what activity is considered normal against observed events to identify significant deviations.
  - Stateful protocol analysis

Access Control Monitoring

- Intrusion Detection Systems
  - Three Common Components
    - Sensors
    - Analyzers
    - Administrator Interfaces
- Intrusion Prevention Systems
  - The next big thing
  - Is a preventative and proactive technology, IDS is a detective technology.
  - Two types: Network Based (NIPS) and Host Based (HIPS)

Access Control Monitoring

- Two Main Types of Intrusion Detection Systems
  - Network Based (NIDS)
  - Host Based (HIDS)
- HIDS and NIDS can be:
  - Signature Based
    - Model of specific attacks and how they are carried out
  - Statistical Anomaly Based
    - Profile-based systems
    - IDS learns the system's "profile"
  - Rule Based
    - Uses an "expert system"

Access Control Monitoring

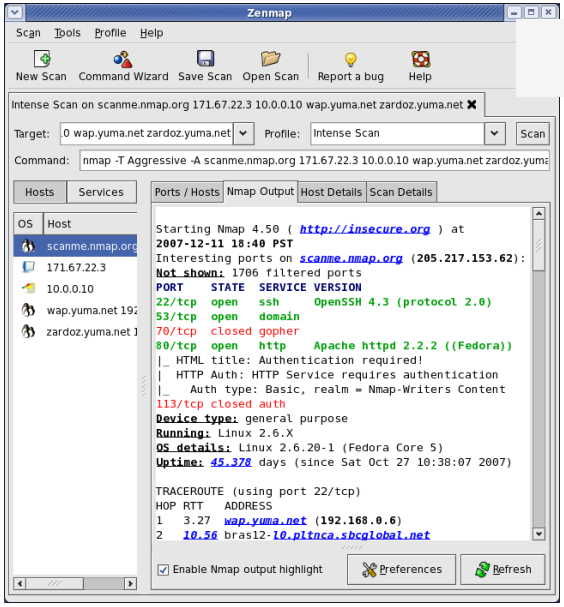
- Honeypots
  - An attractive offering that hopes to lure attackers away from critical systems
- Network sniffers
  - A general term for programs or devices that are able to examine traffic on a LAN segment.

Security Testing Techniques

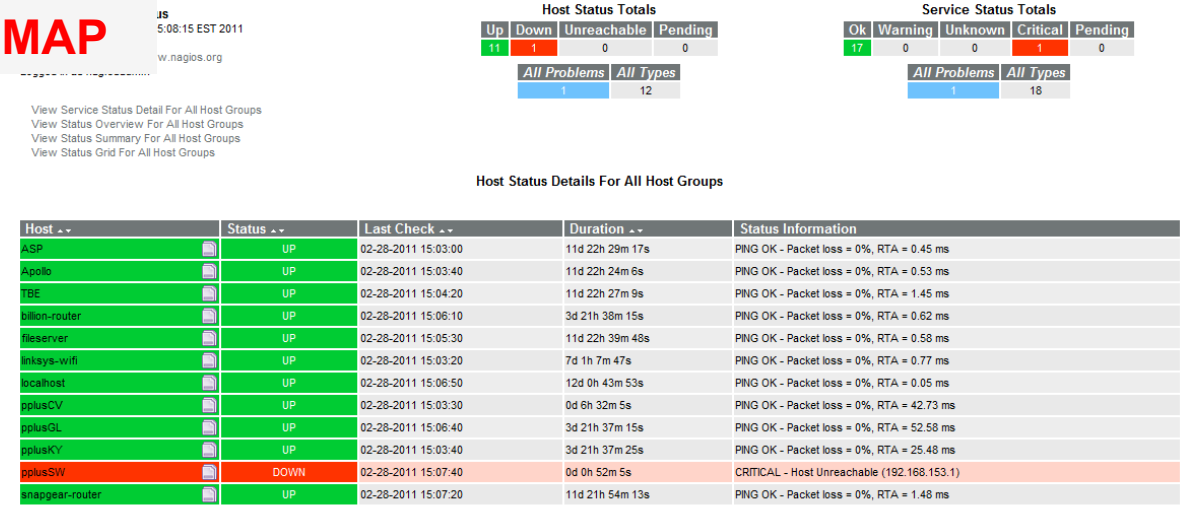
- network scanning
- vulnerability scanning
- password cracking
- log review
- integrity checkers
- virus detection
- war dialing
- war driving
- penetration testing

- Common testing tools
  - NMAP
  - GFI LANguard
  - Tripwire
  - Nessus
  - Metasploit
  - Superscan
- Network protocol analyzer utility for UNIX and Windows

Monitoring IDS/IPS

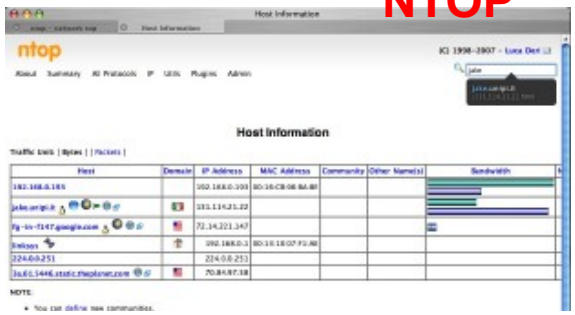


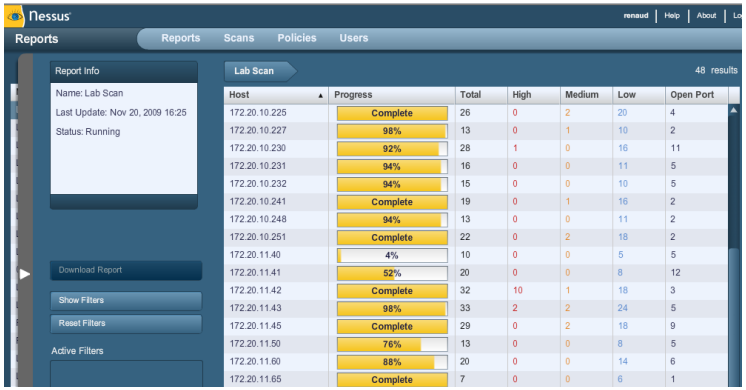
NMAP



NAGIOS

NTOP





NESSUS

LOGWATCH

```
**Unmatched Entries**
Address 91.205.7.19 maps to vhost19.sunline.net.ua, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT! : 65 time(s)
```

Questions?

IP Security (IPSec)

Network Security Workshop

APNIC

Overview

- Introduction to VPN
- IPSec Fundamentals
- Tunnel and Transport Mode IPSec
- Architecture and Components of IPSec
- Internet Key Exchange
- Configuring IPSec for IPv4 and IPv6

Virtual Private Network

- Creates a secure tunnel over a public network
  - Client to firewall
  - Router to router
  - Firewall to firewall
- Uses the Internet as the public backbone to access a secure private network
  - Remote employees can access their office network
- Two types:
  - Remote access
  - Site-to-site VPN

Virtual Private Network

- There are three basic types of VPN:
  - **Remote access VPNs** or virtual private dial-up networks (VPDNs)
  - **Site-to-site VPN**, where multiple fixed sites are connected over a public network i.e. Internet
  - **Point-to-Point VPN**, these are also referred to as "leased-line VPNs." Two or more networks are connected using a dedicated line from an ISP. These lines can be packet or circuit switched. For example, T1's, Metro Ethernet, DS3, ATM or something else

VPN Implementations

- Hardware
  - Usually a VPN-type router
  - Pros: highest network throughput, plug and play, dual purpose
  - Cons: cost and lack of flexibility
- Software
  - Ideal for two end-points in different organisations
  - Pros: flexible, and low relative cost
  - Cons: lack of efficiency, more labor training required, lower productivity; higher labor costs
- Firewall
  - Pros: cost effective, tri-purpose, hardens the operating system
  - Cons: still relatively costly

VPN Protocols

- PPTP (Point-to-Point tunneling Protocol)
  - Developed by Microsoft to secure dial-up connections
  - Operates in the data-link layer
- L2F (Layer 2 Forwarding Protocol)
  - Developed by Cisco
  - Similar as PPTP
- L2TP (Layer 2 Tunneling Protocol)
  - IETF standard
  - Combines the functionality of PPTP and L2F
- IPSec (Internet Protocol Security)
  - Open standard for VPN implementation
  - Operates on the network layer

Advantages of VPN

- Cheaper connection
  - Use the Internet connection instead of a private lease line
- Scalability
  - Flexibility of growth
  - Efficiency with broadband technology
- Availability
  - Available everywhere there is an Internet connection

Disadvantages of VPN

- VPNs require an in-depth understanding of public network security issues and proper deployment precautions
- Availability and performance depends on factors largely outside of their control
- VPNs need to accommodate protocols other than IP and existing internal network technology

IPsec

- Provides Layer 3 security (RFC 2401)
  - Transparent to applications (no need for integrated IPSec support)
- A set of protocols and algorithms used to secure IP data at the network layer
- Combines different components:
  - Security associations (SA)
  - Authentication headers (AH)
  - Encapsulating security payload (ESP)
  - Internet Key Exchange (IKE)
- A security context for the VPN tunnel is established via the ISAKMP

IPsec Standards

- RFC 4301 “The IP Security Architecture”
  - Defines the original IPsec architecture and elements common to both AH and ESP
- RFC 4302
  - Defines authentication headers (AH)
- RFC 4303
  - Defines the Encapsulating Security Payload (ESP)
- RFC 2408
  - ISAKMP
- RFC 5996
  - IKE v2 (Sept 2010)
- RFC 4835
  - Cryptographic algorithm implementation for ESP and AH

Benefits of IPsec

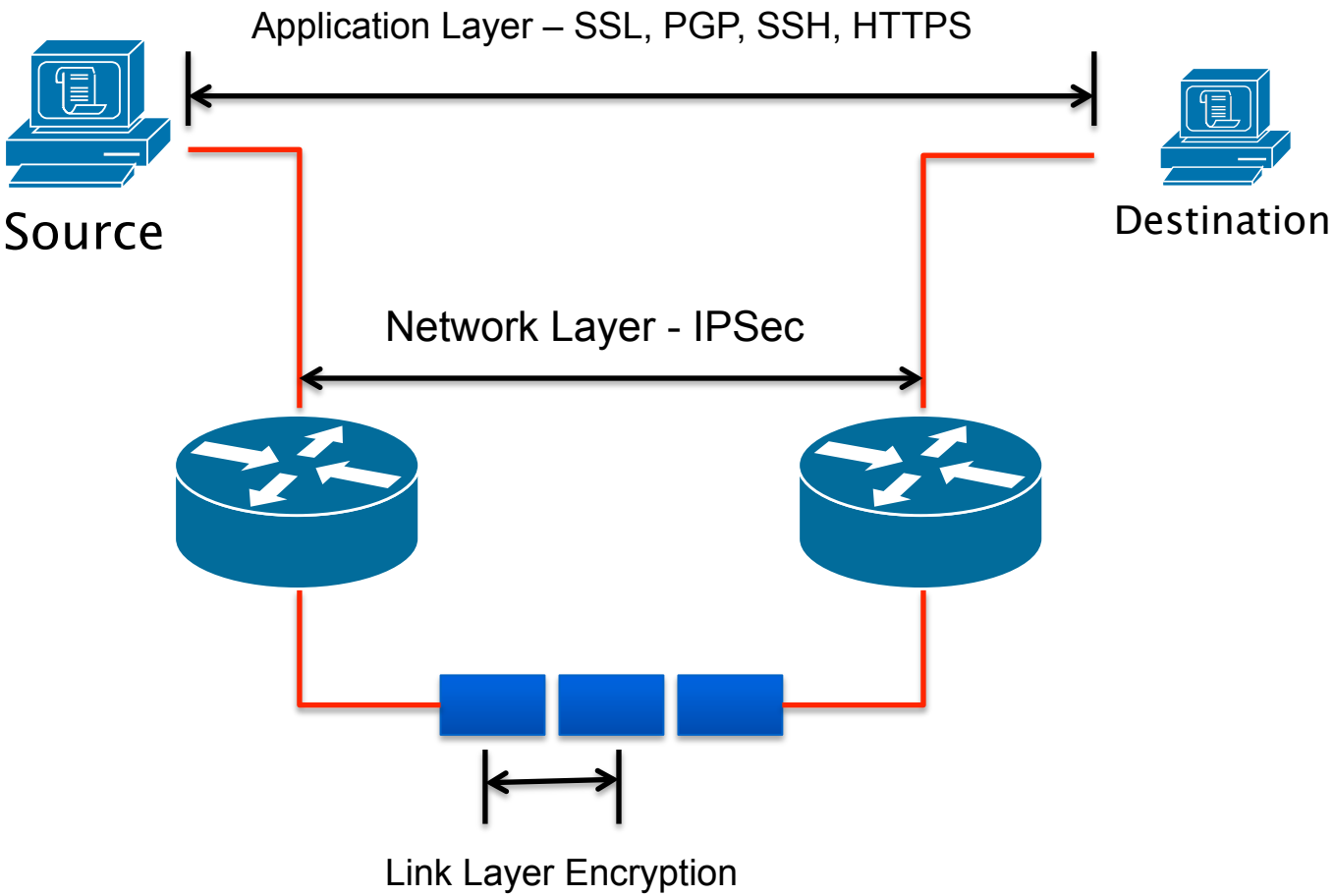
- Confidentiality
  - By encrypting data
- Integrity
  - Routers at each end of a tunnel calculates the checksum or hash value of the data
- Authentication
  - Signatures and certificates
  - All these while still maintaining the ability to route through existing IP networks

"IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6" - (RFC 2401)

Benefits of IPsec

- Data integrity and source authentication
  - Data “signed” by sender and “signature” is verified by the recipient
  - Modification of data can be detected by signature “verification”
  - Because “signature” is based on a shared secret, it gives source authentication
- Anti-replay protection
  - Optional; the sender must provide it but the recipient may ignore
- Key management
  - IKE – session negotiation and establishment
  - Sessions are rekeyed or deleted automatically
  - Secret keys are securely established and authenticated
  - Remote peer is authenticated through varying options

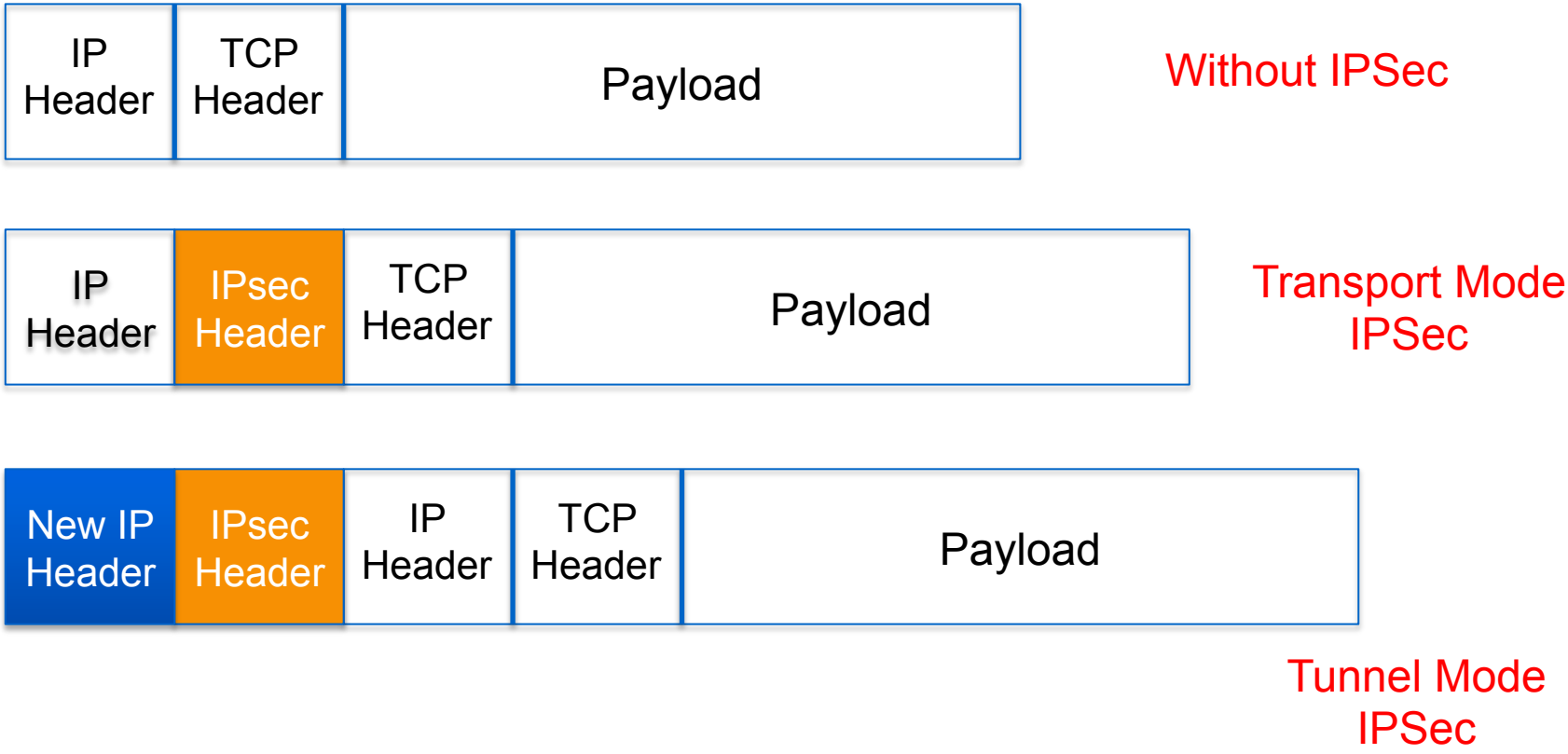
Different Layers of Encryption



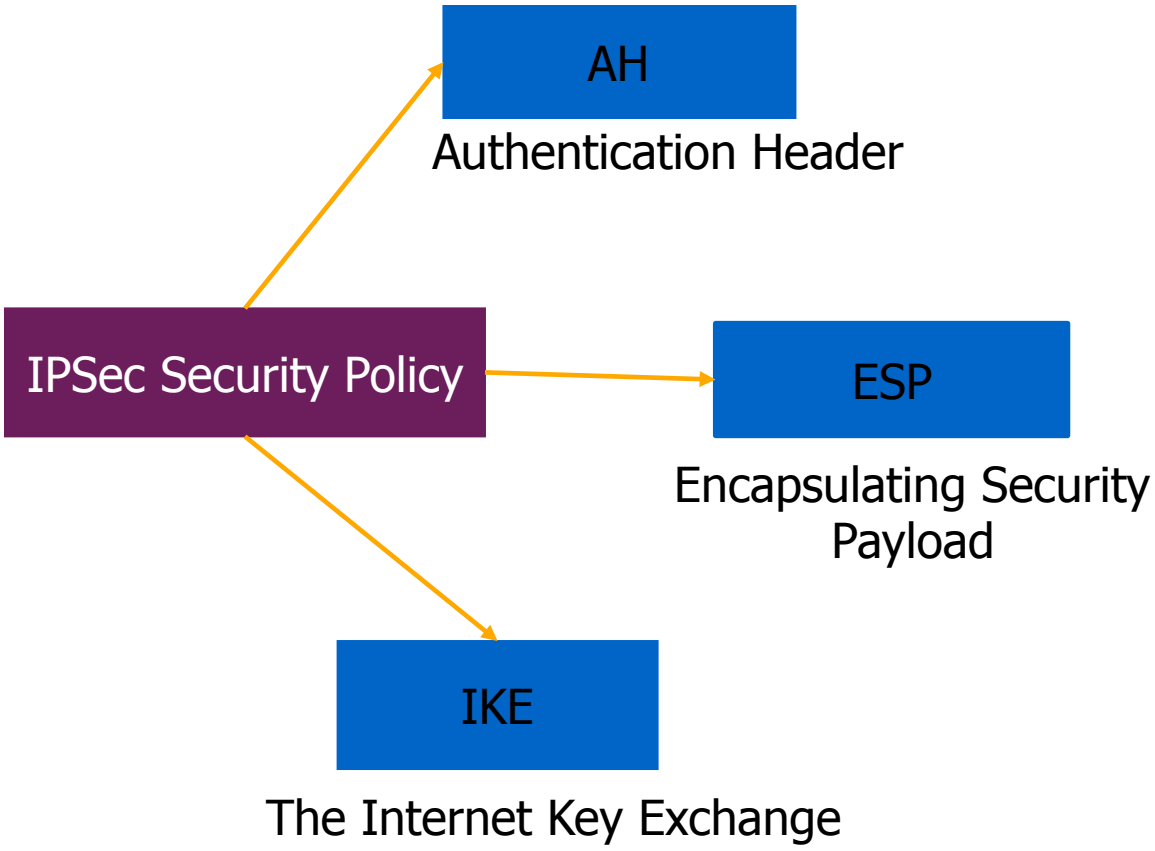
IPsec Modes

- Tunnel Mode
  - Entire IP packet is encrypted and becomes the data component of a new (and larger) IP packet.
  - Frequently used in an IPsec site-to-site VPN
- Transport Mode
  - IPSec header is inserted into the IP packet
  - No new packet is created
  - Works well in networks where increasing a packet's size could cause an issue
  - Frequently used for remote-access VPNs

Tunnel vs. Transport Mode IPsec



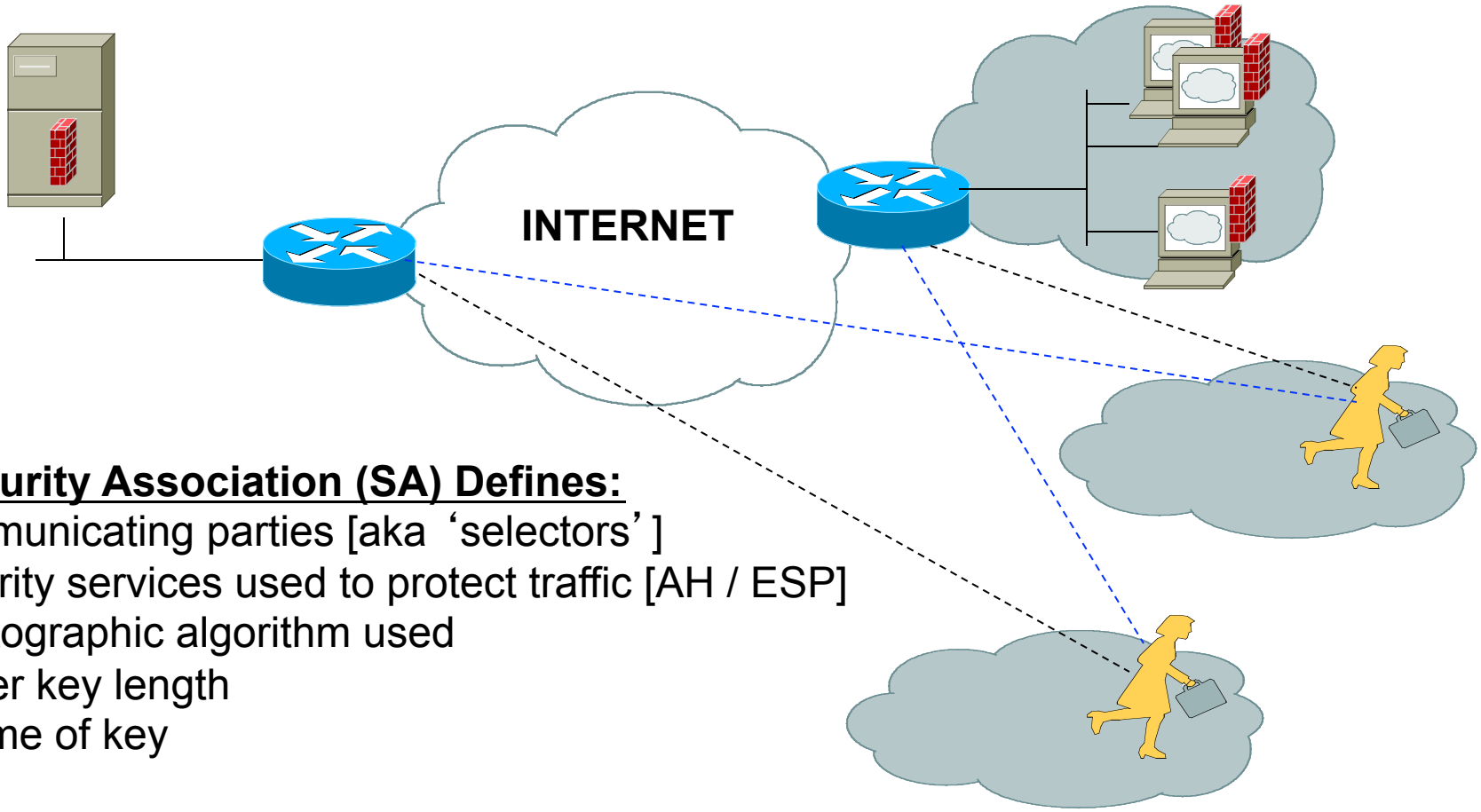
IPsec Architecture



Security Associations (SA)

- A collection of parameters required to establish a secure session
- Uniquely identified by three parameters consisting of
  - Security Parameter Index (SPI)
  - IP destination address
  - Security protocol (AH or ESP) identifier
- An SA is unidirectional
  - Two SAs required for a bidirectional communication
- A single SA can be used for AH or ESP, but not both
  - must create two (or more) SAs for each direction if using both AH and ESP

Security Associations



A Security Association (SA) Defines:

- communicating parties [aka ‘selectors’]
- security services used to protect traffic [AH / ESP]
- cryptographic algorithm used
- cipher key length
- lifetime of key

Security Parameter Index (SPI)

- A unique 32-bit identification number that is part of the Security Association (SA)
- It enables the receiving system to select the SA under which a received packet will be processed.
- Has only local significance, defined by the creator of the SA.
- Carried in the ESP or AH header
- When an ESP/AH packet is received, the SPI is used to look up all of the crypto parameters

How to Set Up SA

- Manually
  - Sometimes referred to as “manual keying”
  - You configure on each node:
    - Participating nodes (I.e. traffic selectors)
    - AH and/or ESP [tunnel or transport]
    - Cryptographic algorithm and key
- Automatically
  - Using IKE (Internet Key Exchange)

ISAKMP

- Internet Security Association and Key Management Protocol
- Used for establishing Security Associations (SA) and cryptographic keys
- Only provides the framework for authentication and key exchange, but key exchange is independent
- Key exchange protocols
  - Internet Key Exchange (IKE) and Kerberized Internet Negotiation of Keys (KINK)

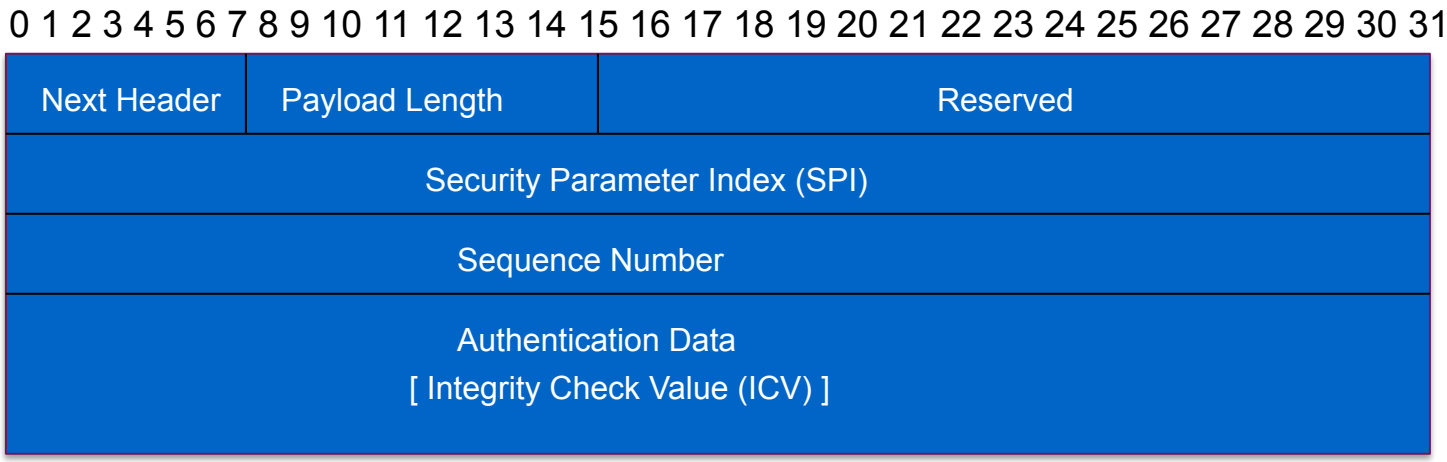
Selectors

- Defines when to create an SA and what the SA will be used for
- Classifies the type of traffic requiring IPsec protection and the kind of protection to be applied.
- Elements of a selector:
  - Source IP address
  - Destination IP address
  - Protocol (TCP or UDP)
  - Upper layer protocol
    - Example: use ESP with NULL encryption and HMAC-SHA1 for routing updates, but use ESP with 3DES and SHA-1 for telnet and TFTP access for a router

Authentication Header (AH)

- Provides source authentication and data integrity
  - Protection against source spoofing and replay attacks
- Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out
- If both AH and ESP are applied to a packet, AH follows ESP
- Operates on top of IP using protocol 51
- In IPv4, AH protects the payload and all header fields except mutable fields and IP options (such as IPSec option)

AH Header Format



Next Header (8 bits): indicates which upper layer protocol is protected (UDP, TCP, ESP)

Payload Length (8 bits): size of AH in 32-bit longwords, minus 2

Reserved (16 bits): for future use; must be set to all zeroes for now

SPI (32 bits): arbitrary 32-bit number that specifies to the receiving device which security association is being used (security protocols, algorithms, keys, times, addresses, etc)

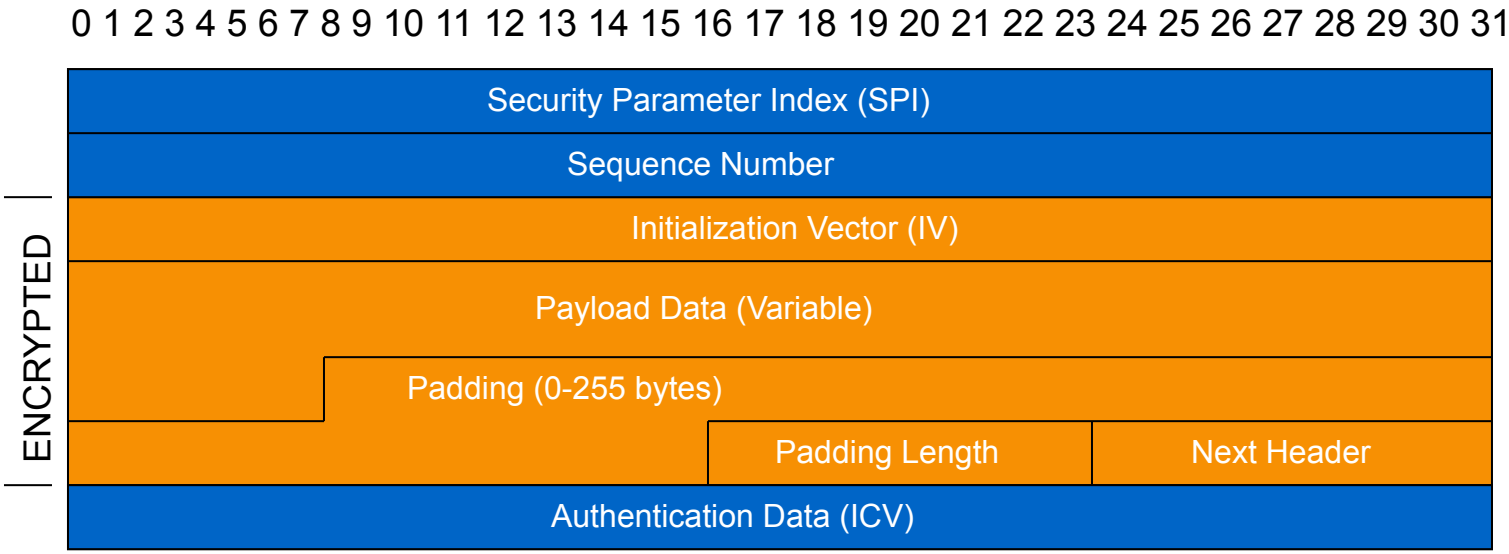
Sequence Number (32 bits): start at 1 and must never repeat. It is always set but receiver may choose to ignore this field

Authentication Data: ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)

Encapsulating Security Payload (ESP)

- Uses IP protocol 50
- Provides all that is offered by AH, plus data confidentiality
  - It uses symmetric key encryption
- Must encrypt and/or authenticate in each packet
  - Encryption occurs before authentication
- Authentication is applied to data in the IPsec header as well as the data contained as payload

ESP Header Format



SPI: arbitrary 32-bit number that specifies SA to the receiving device

Seq #: start at 1 and must never repeat; receiver may choose to ignore

IV: used to initialize CBC mode of an encryption algorithm

Payload Data: encrypted IP header, TCP or UDP header and data

Padding: used for encryption algorithms which operate in CBC mode

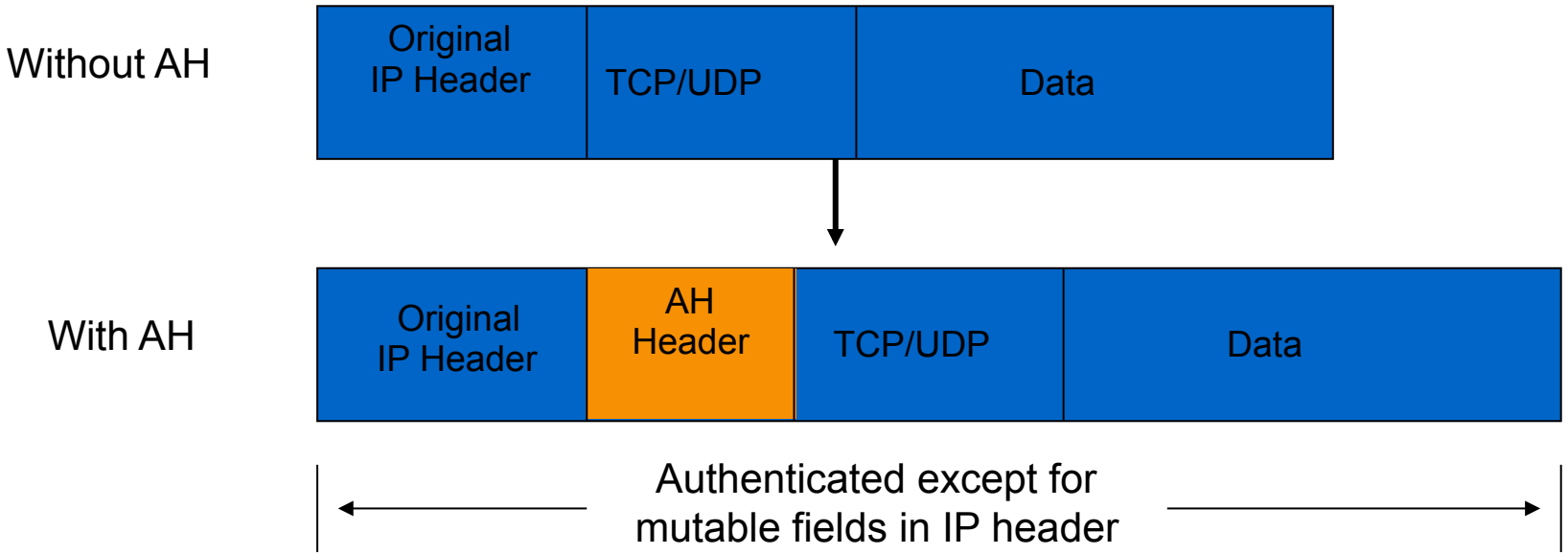
Padding Length: number of bytes added to the data stream (may be 0)

Next Header: the type of protocol from the original header which appears in the encrypted part of the packet

Authentication Header: ICV is a digital signature over the packet and it varies in length depending on the algorithm used (SHA-1, MD5)

Packet Format Alteration for AH Transport Mode

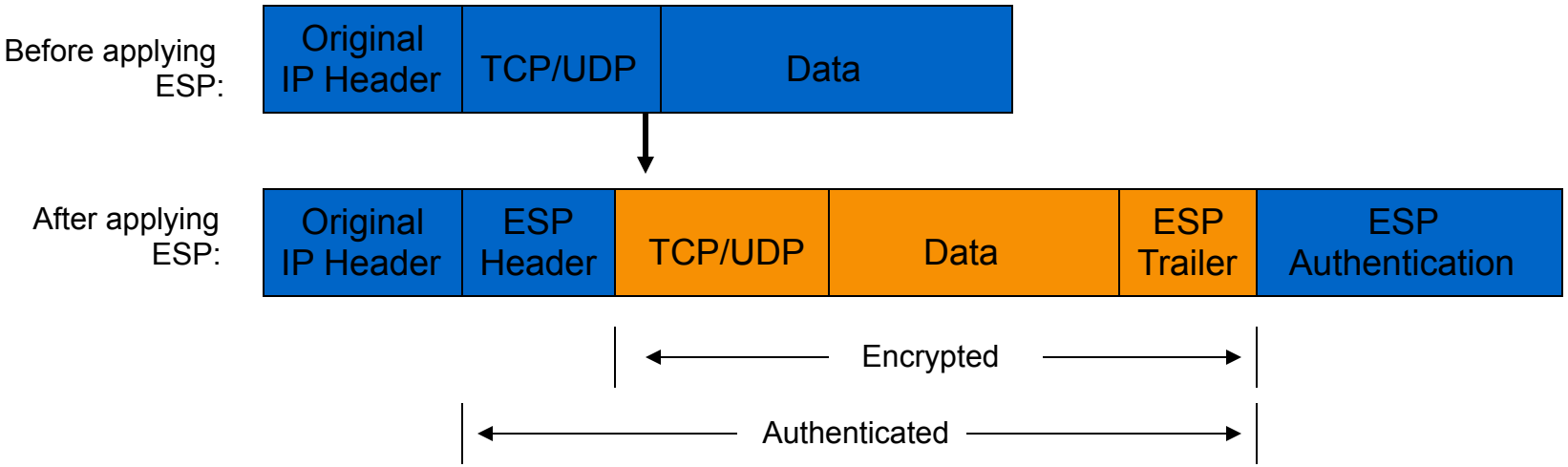
Authentication Header



- ToS
- TTL
- Header Checksum
- Offset
- Flags

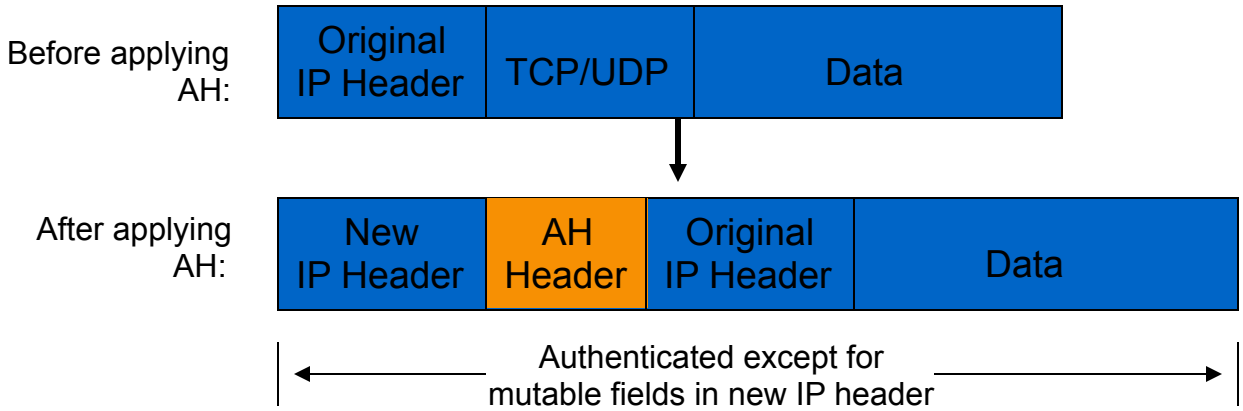
Packet Format Alteration for ESP Transport Mode

Encapsulating Security Payload



Packet Format Alteration for AH Tunnel Mode

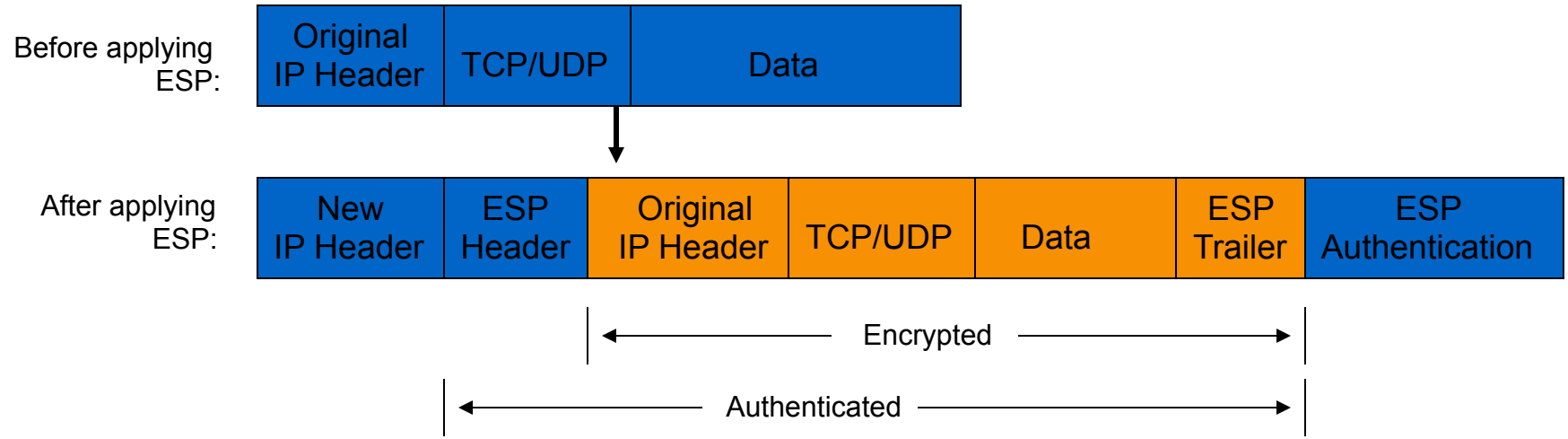
Authentication Header



- ToS
- TTL
- Header Checksum
- Offset
- Flags

Packet Format Alteration for ESP Tunnel Mode

Encapsulating Security Payload



Internet Key Exchange (IKE)

- “An IPSec component used for performing mutual authentication and establishing and maintaining Security Associations.” (RFC 5996)
- Typically used for establishing IPSec sessions
- A key exchange mechanism
- Five variations of an IKE negotiation:
  - Two modes (aggressive and main modes)
  - Three authentication methods (pre-shared, public key encryption, and public key signature)
- Uses UDP port 500

IKE Modes

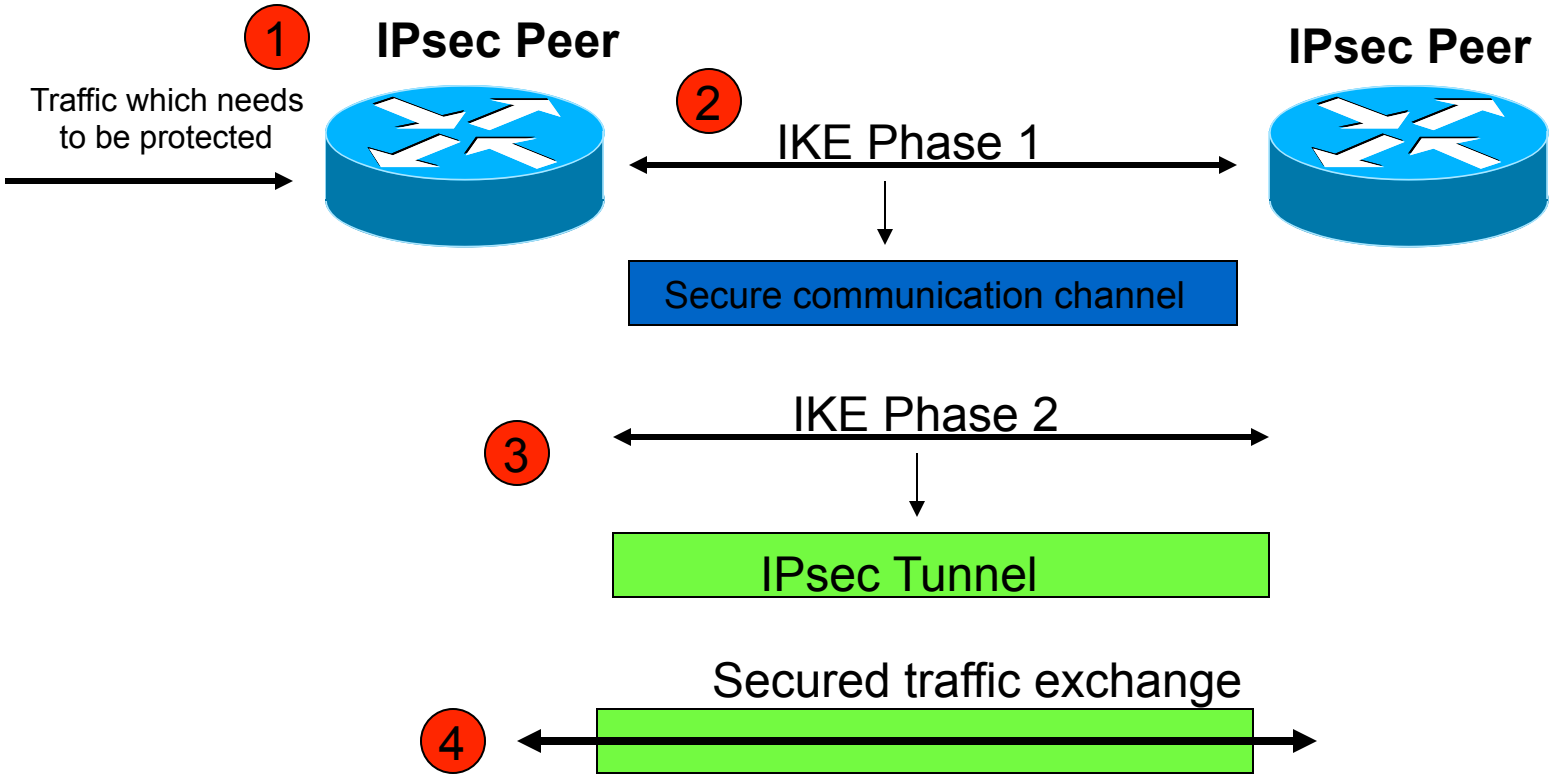
Mode	Description
Main mode	Three exchanges of information between IPsec peers. Initiator sends one or more proposals to the other peer (responder) Responder selects a proposal
Aggressive Mode	Achieves same result as main mode using only 3 packets First packet sent by initiator containing all info to establish SA Second packet by responder with all security parameters selected Third packet finalizes authentication of the ISAKMP session
Quick Mode	Negotiates the parameters for the IPsec session. Entire negotiation occurs within the protection of ISAKMP session

Internet Key Exchange (IKE)

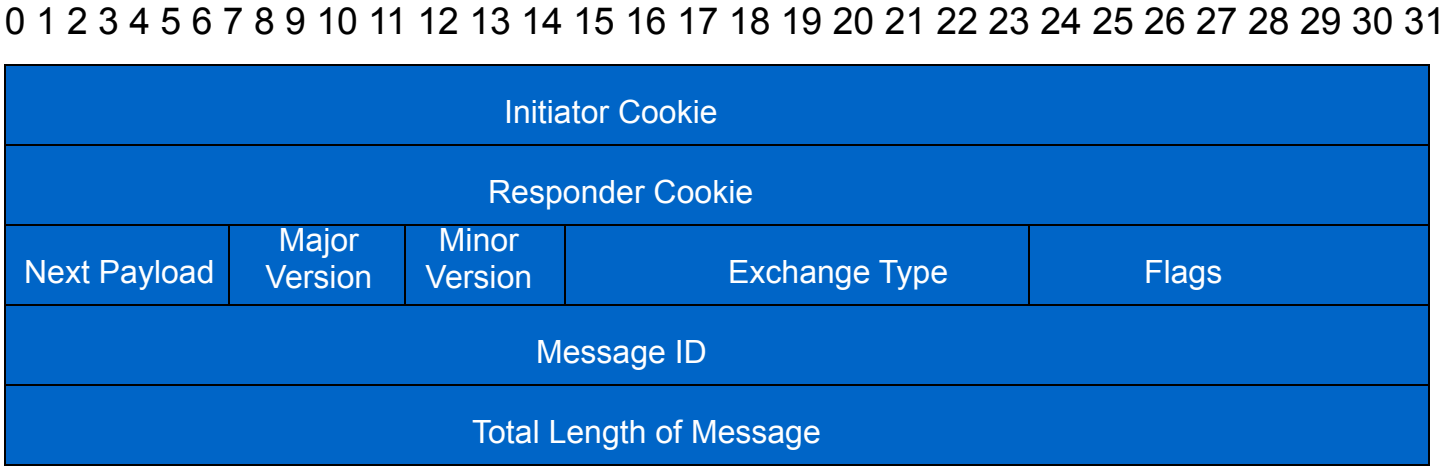
- Phase I
  - Establish a secure channel (ISAKMP SA)
  - Using either main mode or aggressive mode
  - Authenticate computer identity using certificates or pre-shared secret

- Phase II
  - Establishes a secure channel between computers intended for the transmission of data (IPsec SA)
  - Using quick mode

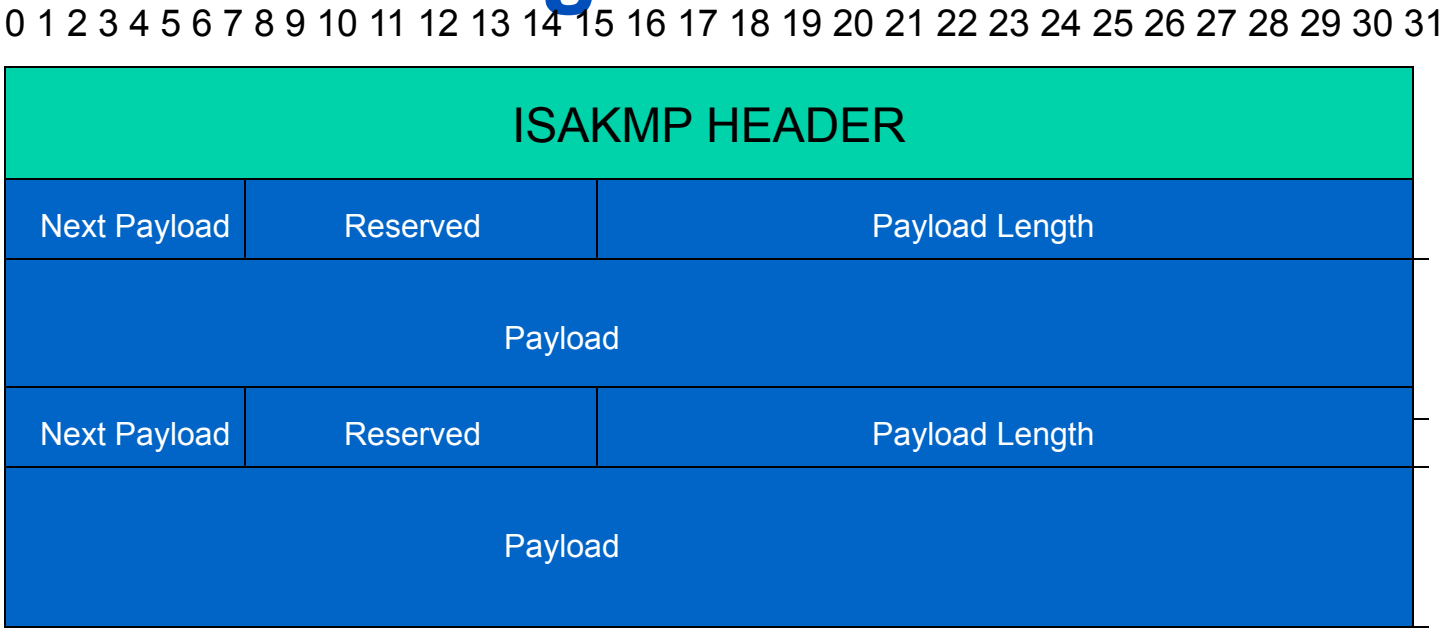
Overview of IKE



ISAKMP Header Format



ISAKMP Message Format



Next Payload: 1byte; identifier for next payload in message. If it is the last payload It will be set to 0

Reserved: 1byte; set to 0

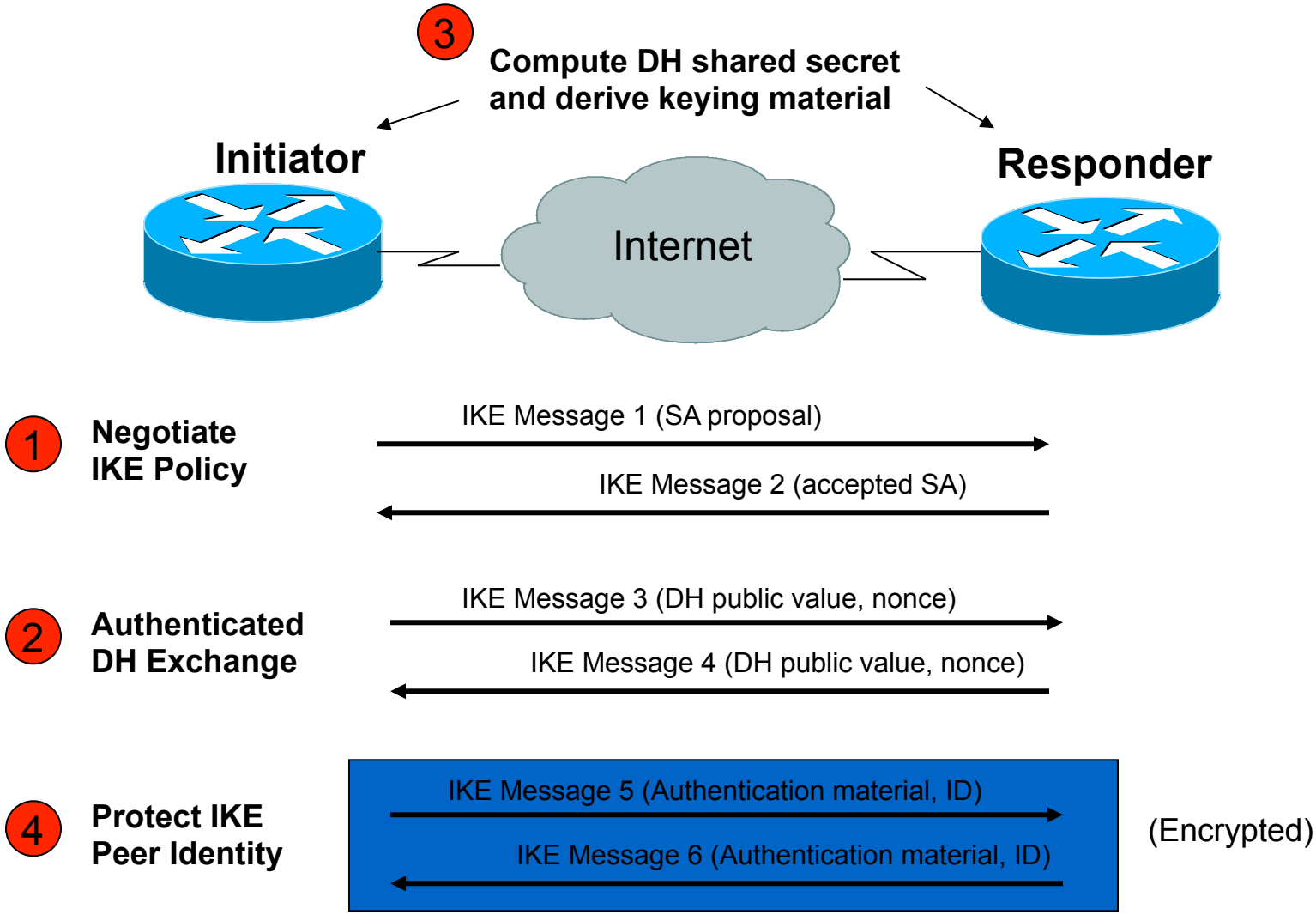
Payload Length: 2 bytes; length of payload (in bytes) including the header

Payload: The actual payload data

IKE Phase 1 (Main Mode)

- Main mode negotiates an ISAKMP SA which will be used to create IPsec SAs
- Three steps
  - SA negotiation (encryption algorithm, hash algorithm, authentication method, which DF group to use)
  - Do a Diffie-Hellman exchange
  - Provide authentication information
  - Authenticate the peer

IKE Phase 1 (Main Mode)



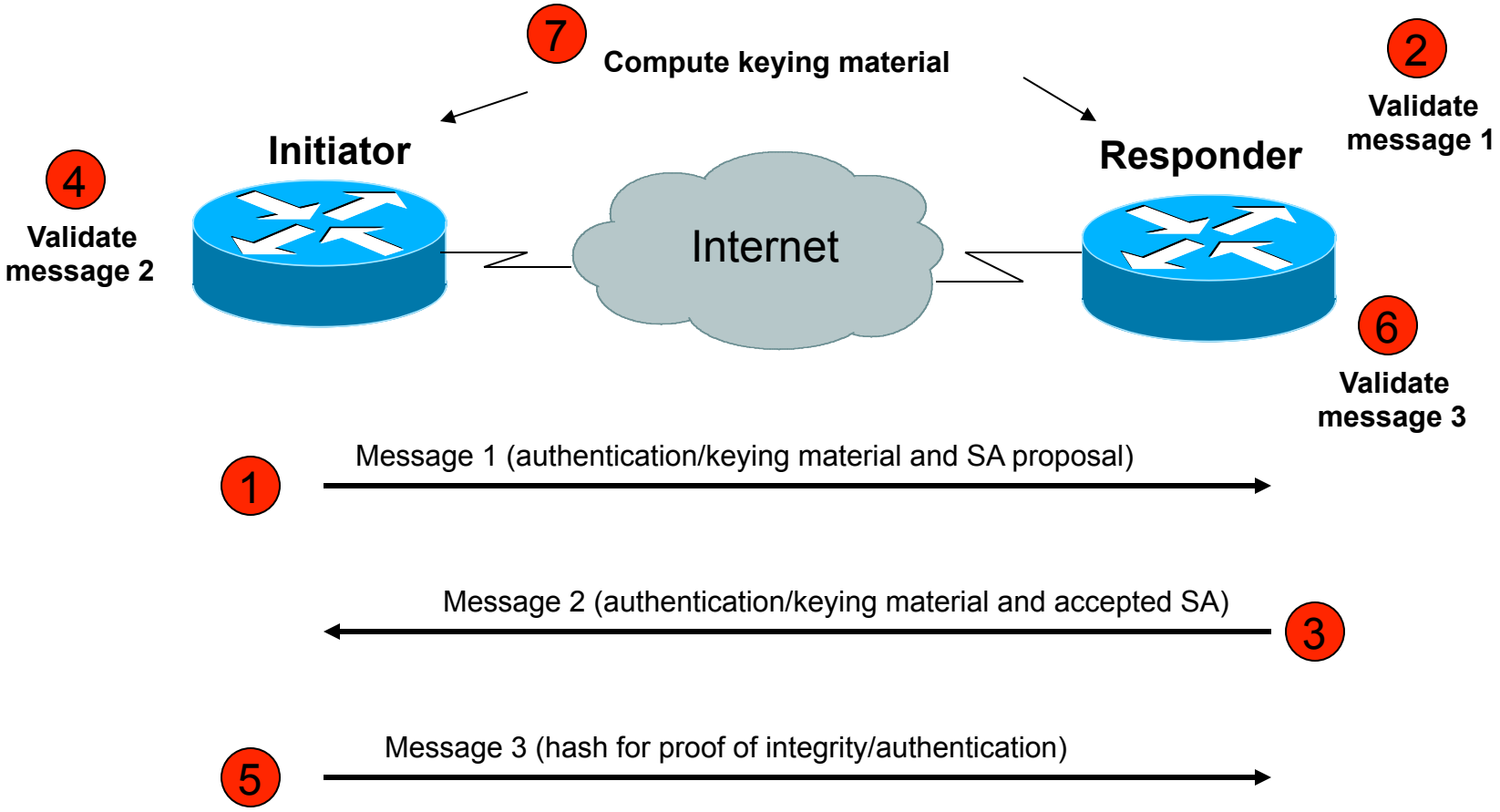
IKE Phase 1 (Aggressive Mode)

- Uses 3 (vs 6) messages to establish IKE SA
- No denial of service protection
- Does not have identity protection
- Optional exchange and not widely implemented

IKE Phase 2 (Quick Mode)

- All traffic is encrypted using the ISAKMP Security Association
- Each quick mode negotiation results in two IPsec Security Associations (one inbound, one outbound)
- Creates/refreshes keys

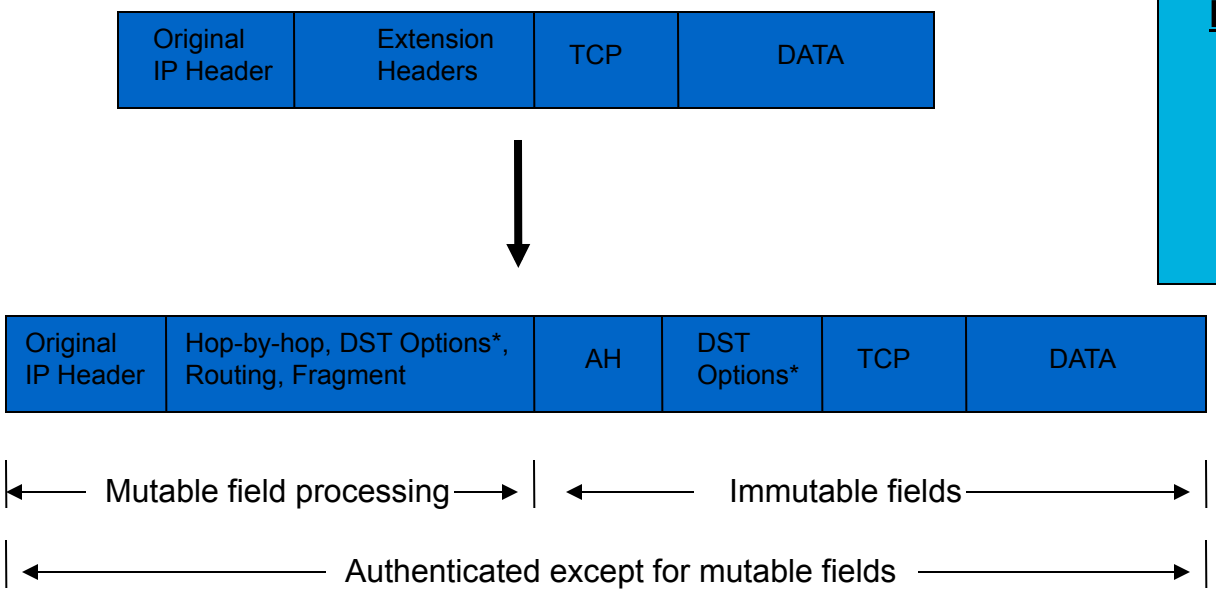
IKE Phase 2 (Quick Mode)



IPv6 and IPsec Standards

- IPv6 node requirements draft
  - ESP and AH must be supported
  - Must support manual configuration of SA
  - Key management SHOULD be supported (IKEv1, IKEv2, Kerberos, etc)
- IKEv1 vs IKEv2
  - IKEv2 incorporates extensions made to IKEv1
  - IKEv2 has support for multiple addresses for traffic selectors which is useful in Mobile scenarios
  - Are vendors supporting IKEv2?

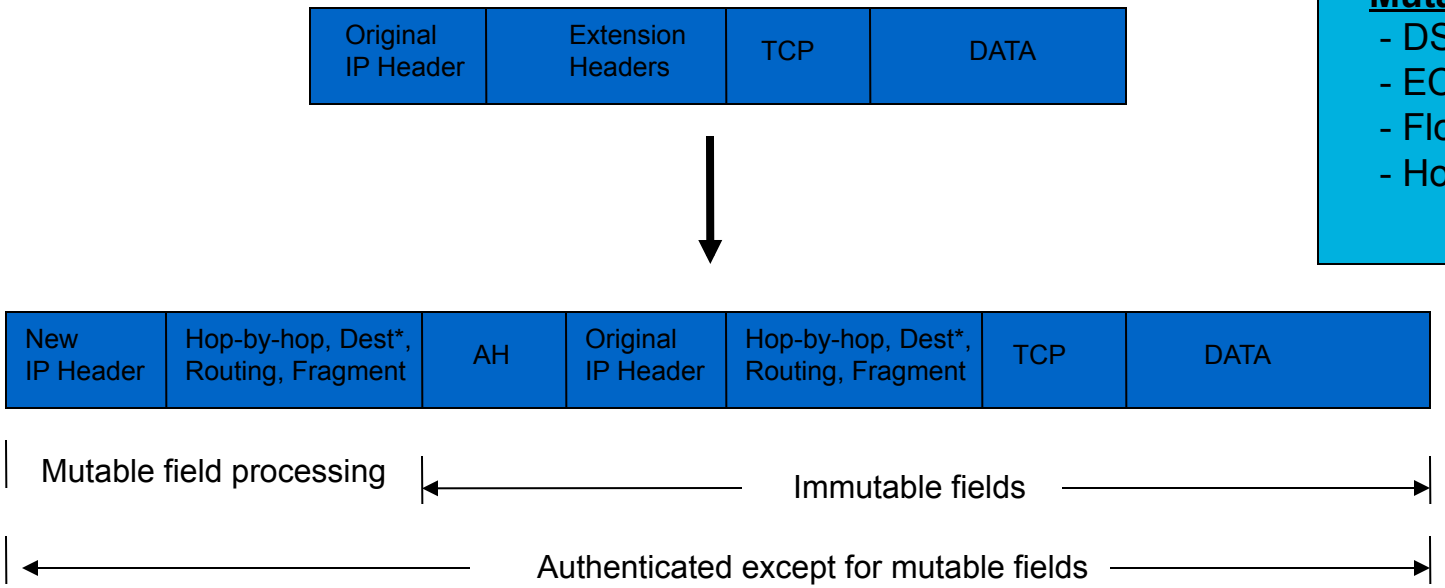
IPv6 AH Transport Mode



Mutable Fields:
- DSCP
- ECN
- Flow Label
- Hop Limit

* DST options extension header could appear before, after, or both before and after the AH header.

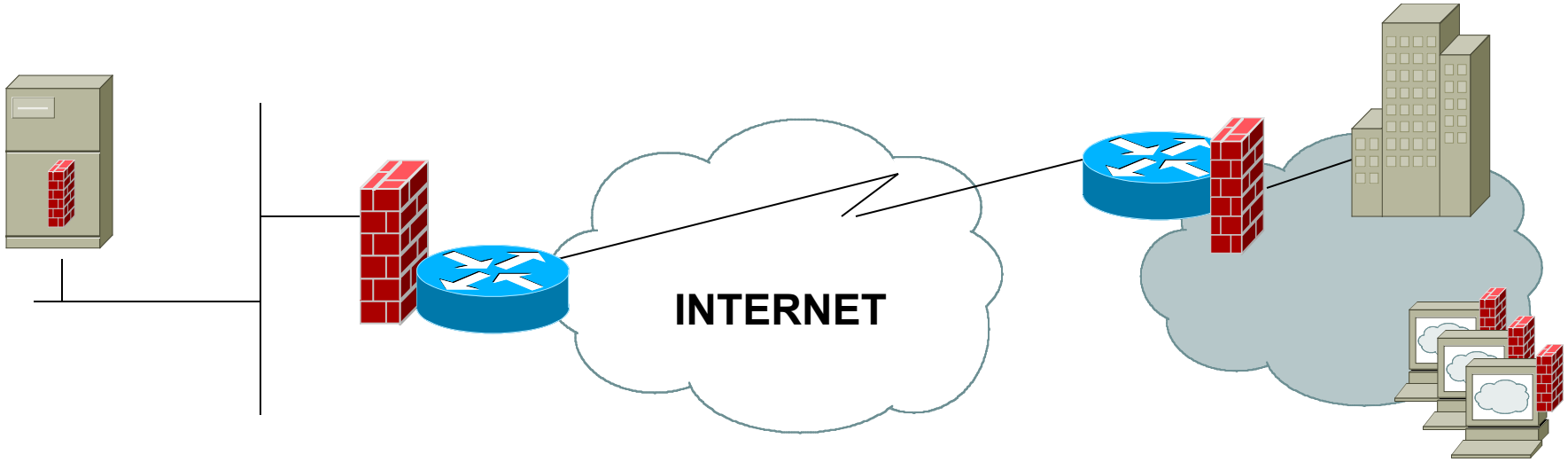
IPv6 AH Tunnel Mode



Mutable Fields:
- DSCP
- ECN
- Flow Label
- Hop Limit

Mixed inner and outer IP versions are allowed (I.e. IPv4 over IPv6 or IPv6 over IPv4)

IPv6 IPsec AH Considerations



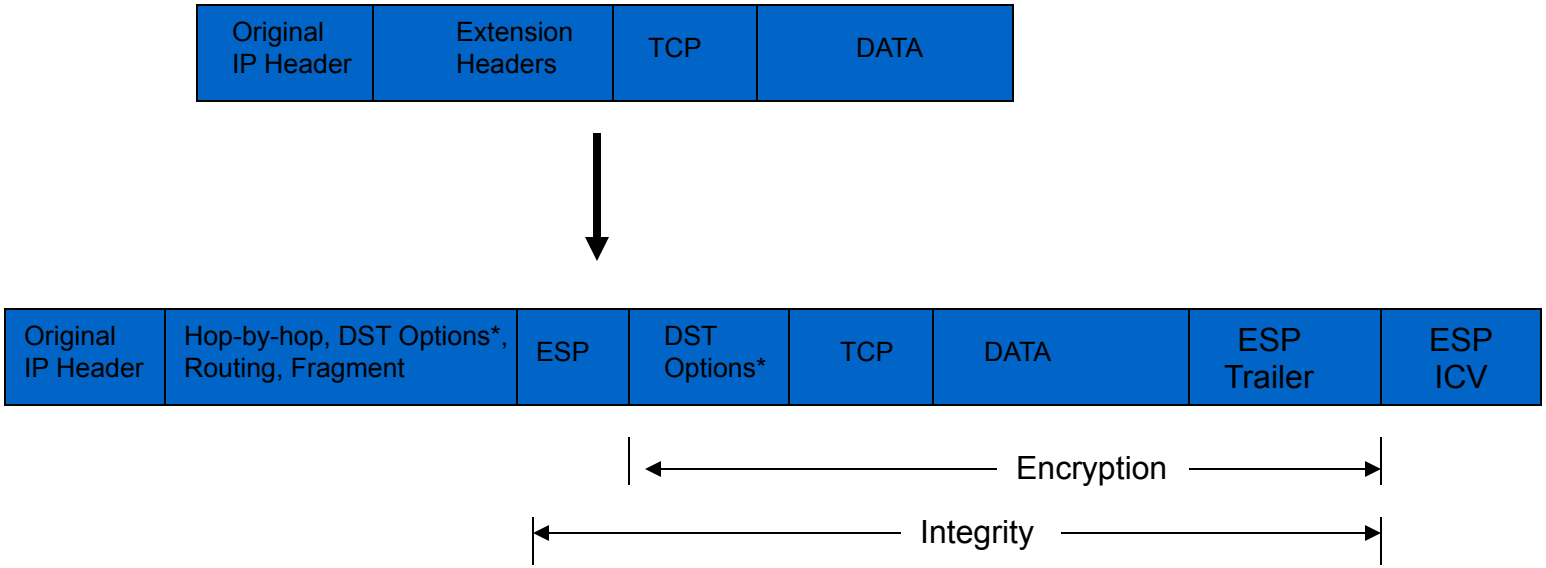
Route authentication:

- OSPFv3 requires IPsec
- Replace MD-5 for other routing protocols?

Most initial host implementations support AH

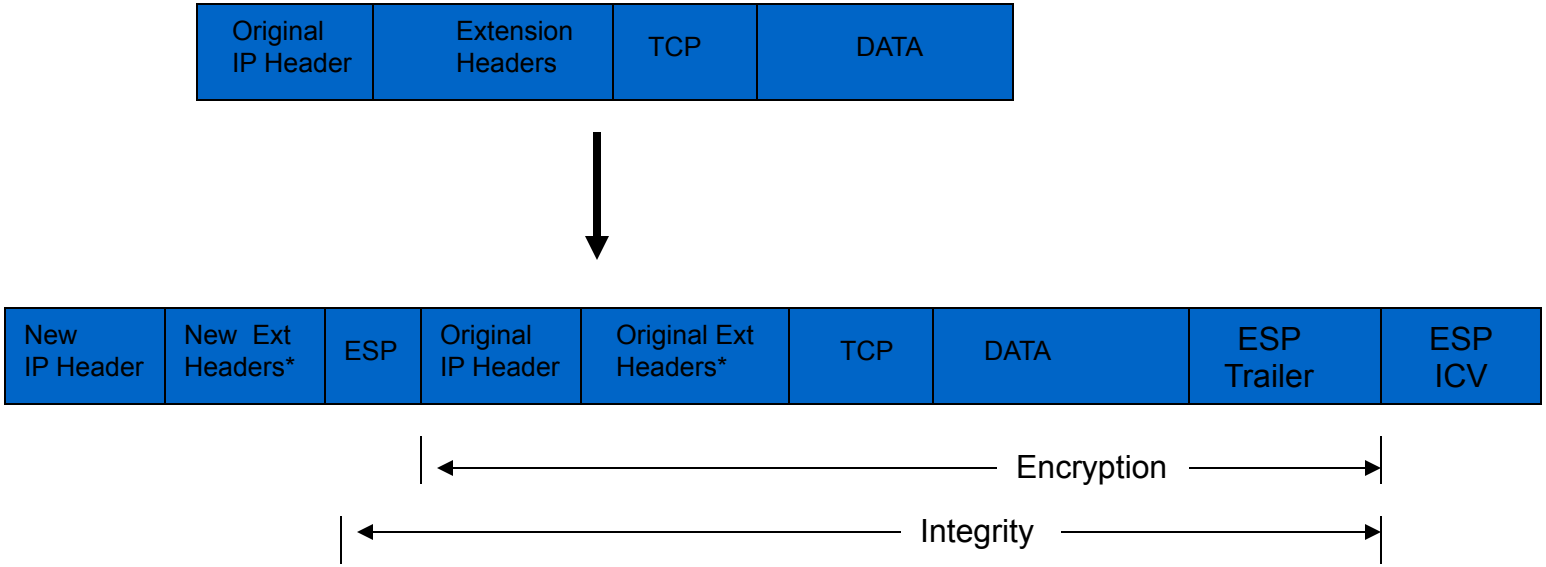
Is AH going to be deprecated?

IPv6 ESP Transport Mode

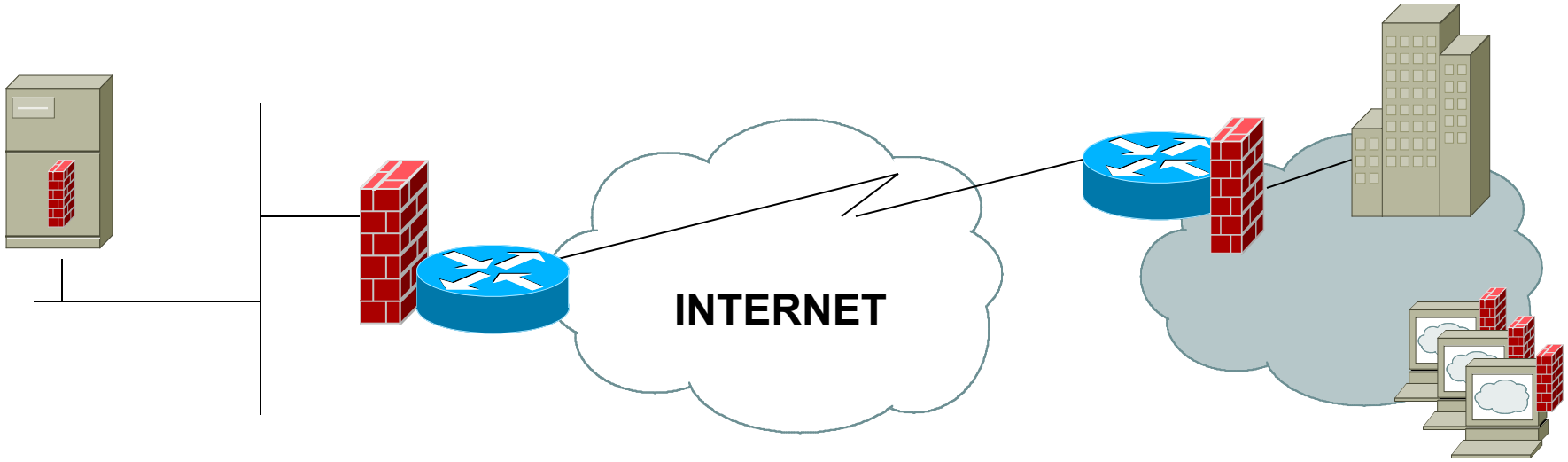


* DST options extension header could appear before, after, or both before and after the ESP header. Since ESP protects only fields after the ESP header, it generally will be desirable to place the destination options header(s) after the ESP header.

IPv6 ESP Tunnel Mode



IPv6 IPsec ESP



- ESP with NULL encryption can be used for router authentication

- National /Corporate policies will dictate where encryption is feasible

- Distributed firewalls with IPsec hooks can still give stateful inspection

IPSec Best Practices

- Use IPsec to provide integrity in addition to encryption
  - Use ESP option
- Use strong encryption algorithms
  - AES instead of DES
- Use a good hashing algorithm
  - SHA instead of MD5
- Reduce the lifetime of the Security Association (SA) by enabling Perfect Forward Secrecy (PFS)
  - Increases processor burden so do this only if data is highly sensitive

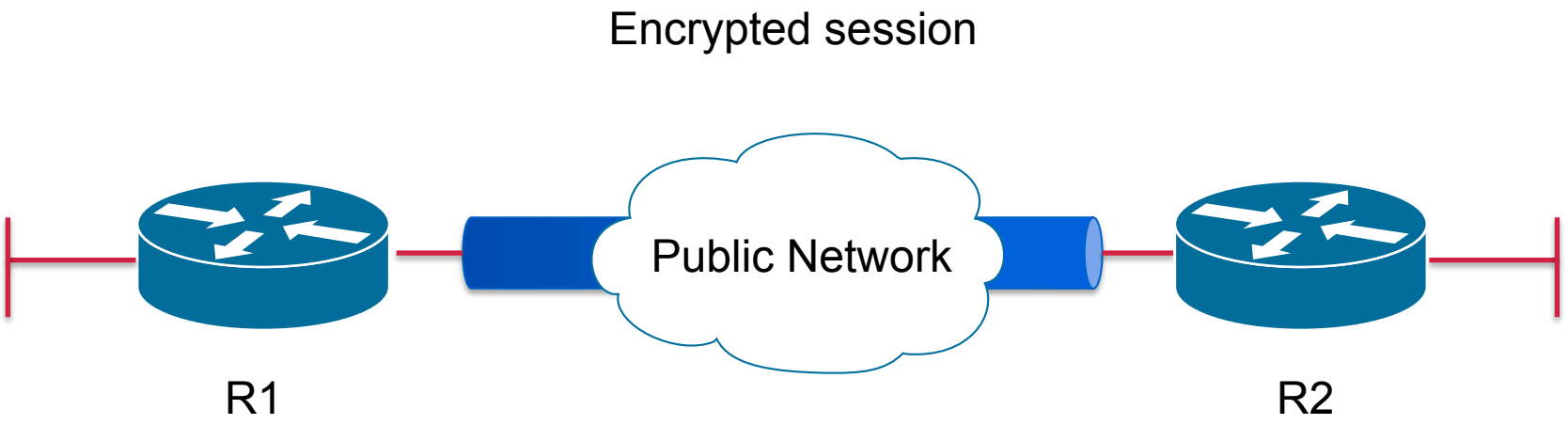
Configuring IPSec

- Step 1: Configure the IKE Phase 1 Policy (ISAKMP Policy)
  - ***crypto isakmp policy [priority]***
- Step 2: Set the ISAKMP Identity
  - **crypto isakmp identity {ipaddress|hostname}**
- Step 3: Configure the IPSec transfer set
  - **crypto ipsec transform-set transform-set-name <transform1> <transform2> mode [tunnel|transport]**
  - **crypto ipsec security-association lifetime seconds seconds**

Configuring IPSec

- Step 5: Creating map with name
  - `Crypto map crypto-map-name seq-num ipsec-isakmp`
  - `Match address access-list-id`
  - `Set peer [ipaddress|hostname]`
  - `Set transform-set transform-set-name`
  - `Set security-association lifetime seconds seconds`
  - `Set pfs [group1|group2]`
- Step 6: Apply the IPsec Policy to an Interface
  - `Crypto map crypto-map-name local-address interface-id`

IPSec Layout



Router Configuration

```
crypto isakmp policy 1
  authentication pre-share
  encryption aes
  hash sha
  group 5
crypto isakmp key Training123 address 172.16.11.66
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map LAB-VPN 10 ipsec-isakmp
  match address 101
  set transform-set ESP-AES-SHA
  set peer 172.16.11.66
```

Phase 1 SA

Encryption and authentication

Phase 2 SA

Router Configuration

```
int fa 0/1
crypto map LAB-VPN
Exit
!
access-list 101 permit ip 172.16.16.0
0.0.0.255 172.16.20.0 0.0.0.255
```

Apply to an outbound interface

Define interesting VPN traffic

IPSec Debug Commands

- sh crypto ipsec sa
- sh crypto isakmp peers
- sh crypto isakmp sa
- sh crypto map

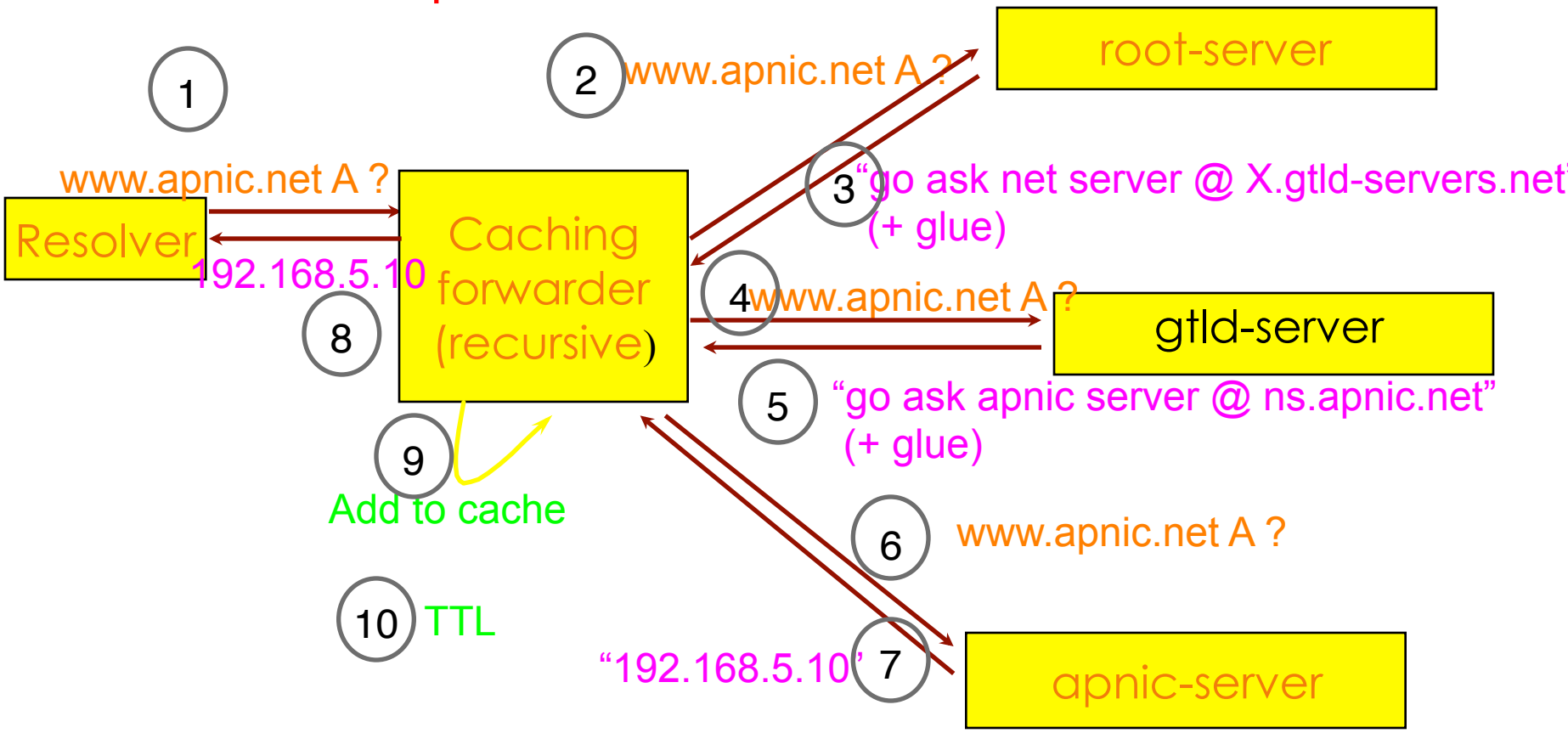
Questions?

DNS Security

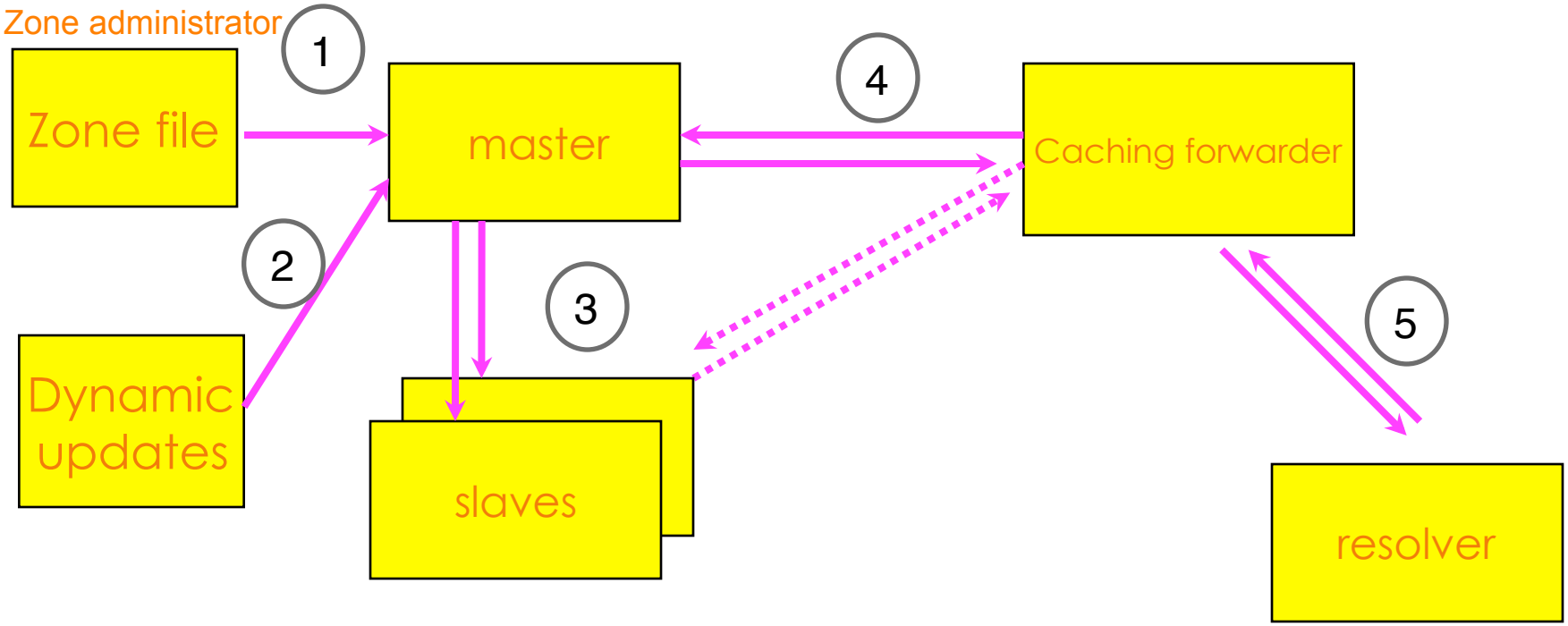
Network Security Workshop

APNIC

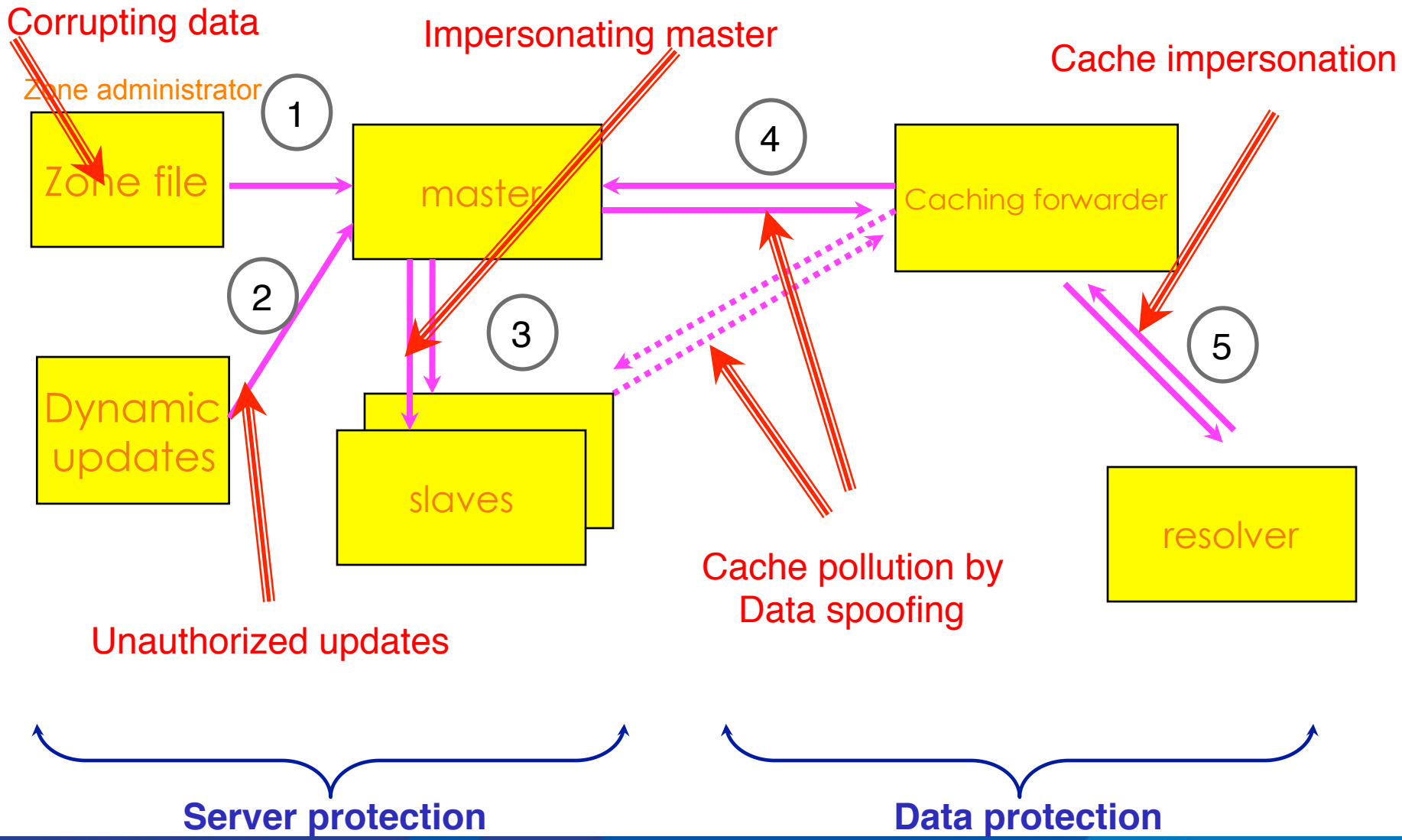
Overview: How DNS Works



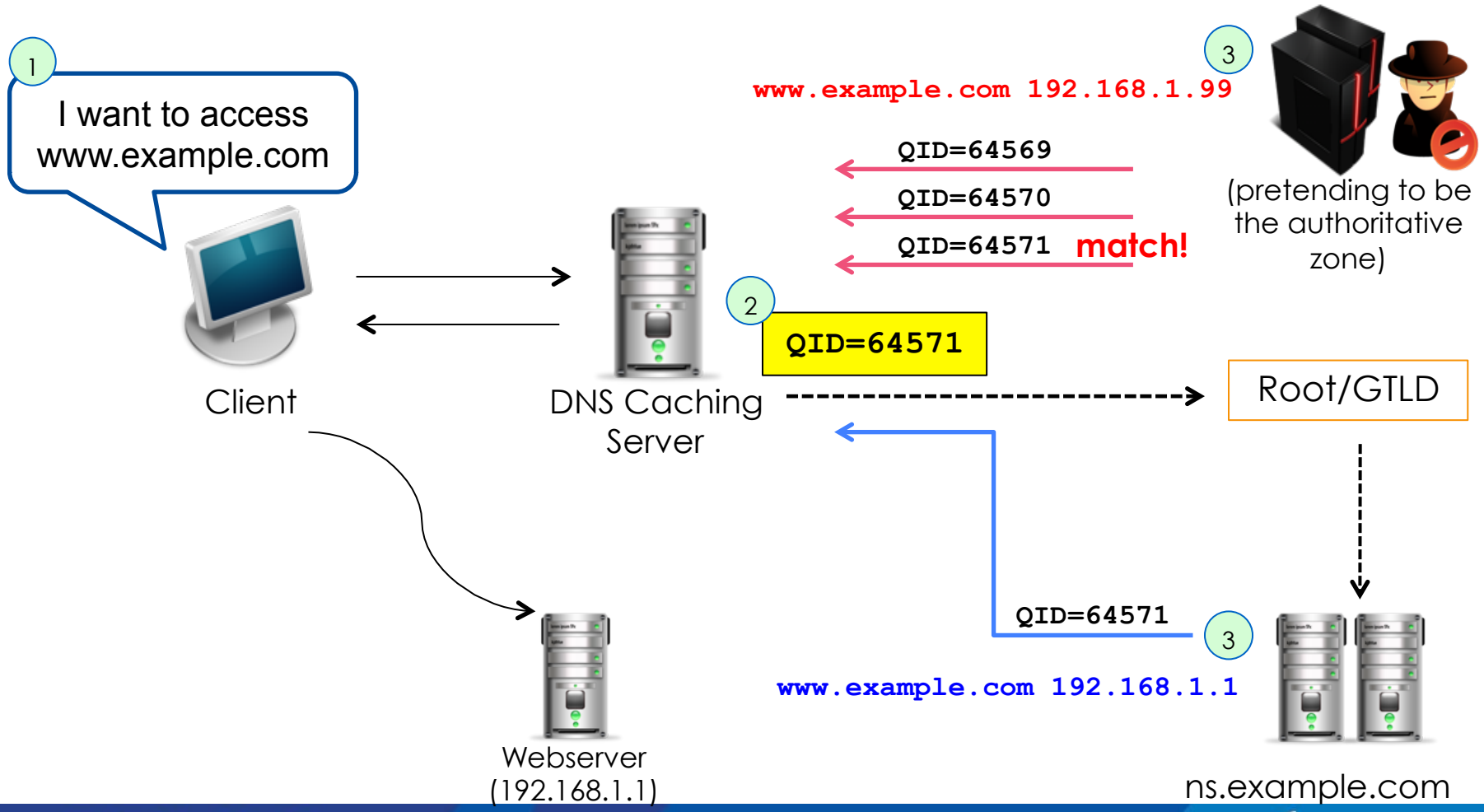
DNS Vulnerabilities



DNS Vulnerabilities



DNS Cache Poisoning



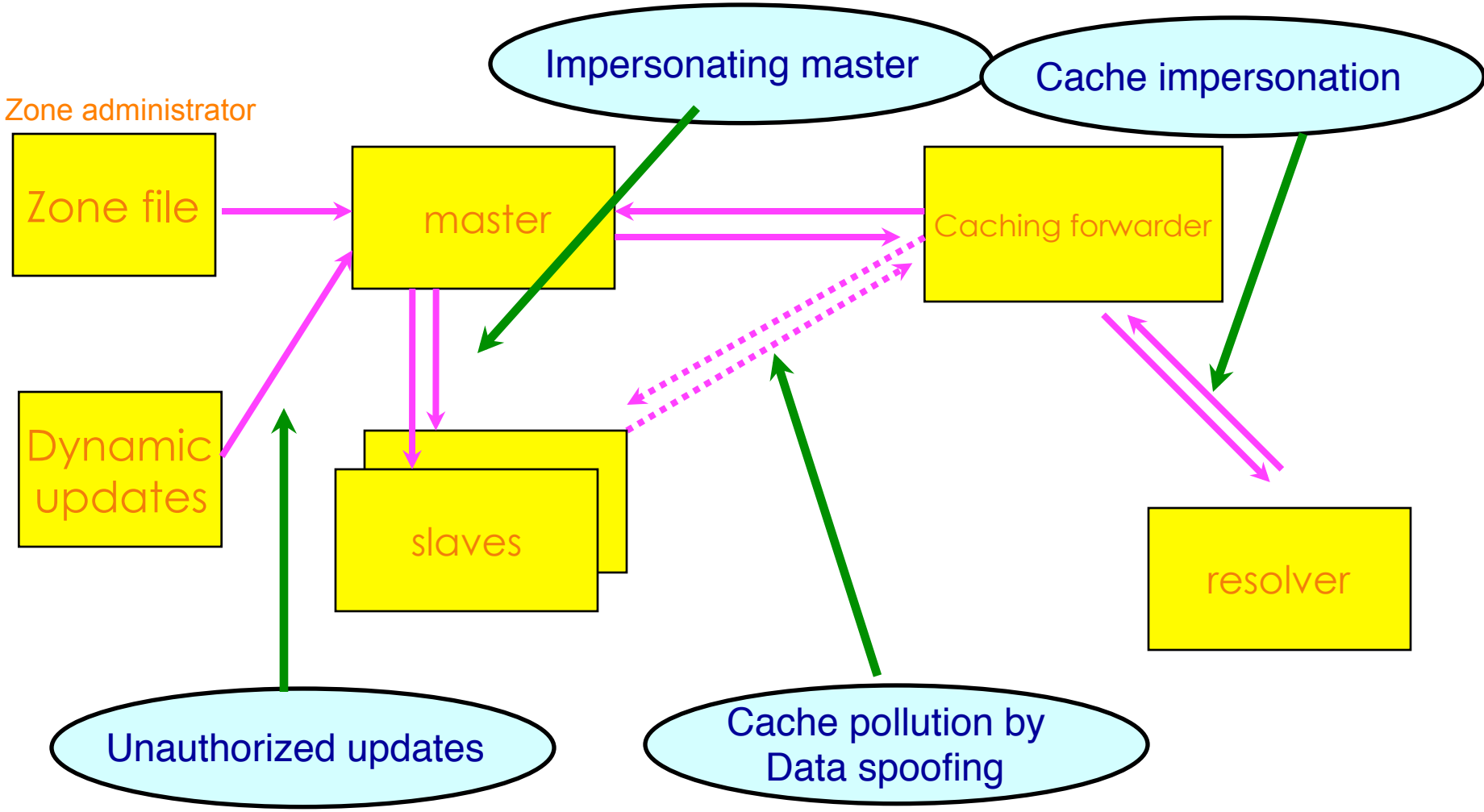
Securing the Nameserver

- Run the most recent version of the DNS software
  - Bind 9.9.1 or Unbound 1.4.16
  - Apply the latest patches
- Hide version
- Restrict queries
  - `Allow-query { acl_match_list; };`
- Prevent unauthorized zone transfers
  - `Allow-transfer { acl_match_list; };`
- Run BIND with the least privilege (use `chroot`)
- Randomize source ports
  - don't use `query-source` option
- Secure the box
- Use TSIG and DNSSEC

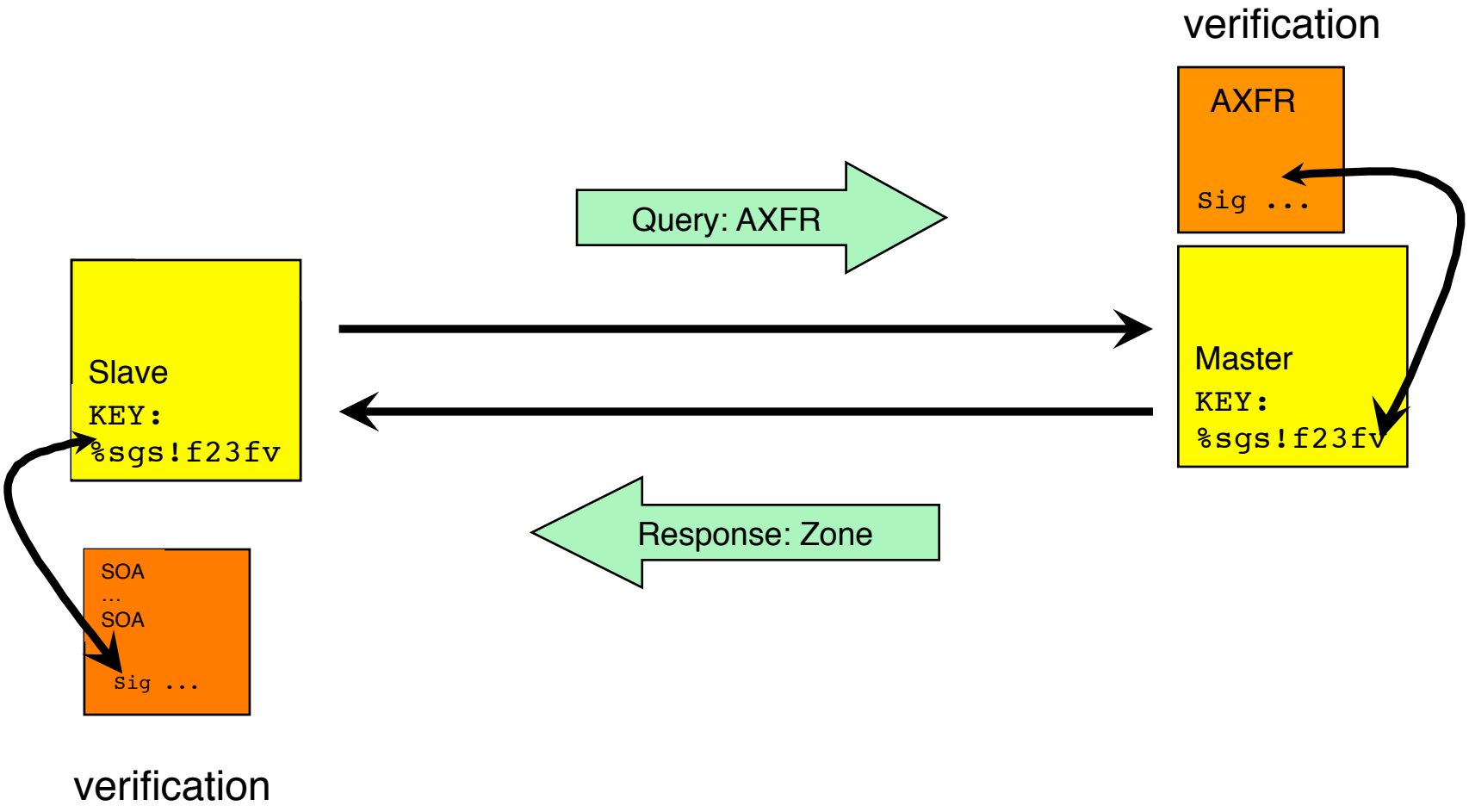
Transaction Signature (TSIG)

- A mechanism for protecting a message from a primary to secondary and vice versa (i.e. transactions)
- A keyed-hash is applied (like a digital signature) so recipient can verify message
  - DNS question or answer & the timestamp
  - Based on a shared secret - both sender and receiver are configured with it
- RFC 2845

TSIG Protected Vulnerabilities



TSIG Example



TSIG Steps

- Generate secret
  - `dnssec-keygen -a <algorithm> -b <bits> -n host <name of the key>`
- Communicate secret
  - Transfer the key securely (ex. SSH/SCP)
- Configure the servers
  - Edit configuration file for primary and secondary
- Test
  - dig @<server> <zone> AXFR -k <TSIG keyfile>

TSIG Configuration – named.conf

Primary server 10.33.40.46

```
key ns1-ns2.pcx. net {
  algorithm hmac-md5;
  secret "APlaceToBe";
};
server 10.33.50.35 {
  keys {ns1-ns2.pcx.net;};
};

allow-transfer {
  key ns1-ns2.pcx.net ;};
```

Secondary server 10.33.50.35

```
key ns1-ns2.pcx.net {
  algorithm hmac-md5;
  secret "APlaceToBe";
};
server 10.33.40.46 {
  keys {ns1-ns2.pcx.net;};
};
zone "my.zone.test." {
  type slave;
  file “myzone.backup”;
  masters
       {10.33.40.46;}; };
```

You can save this in a file and refer to it in the config file (named.conf) using ‘include’ statement:

```
include “/var/named/master/tsig-key-ns1-ns2”;
```

TSIG Testing - dig

- You can use dig to check TSIG configuration

```
dig  @<server> <zone> AXFR -k <TSIG keyfile>
```

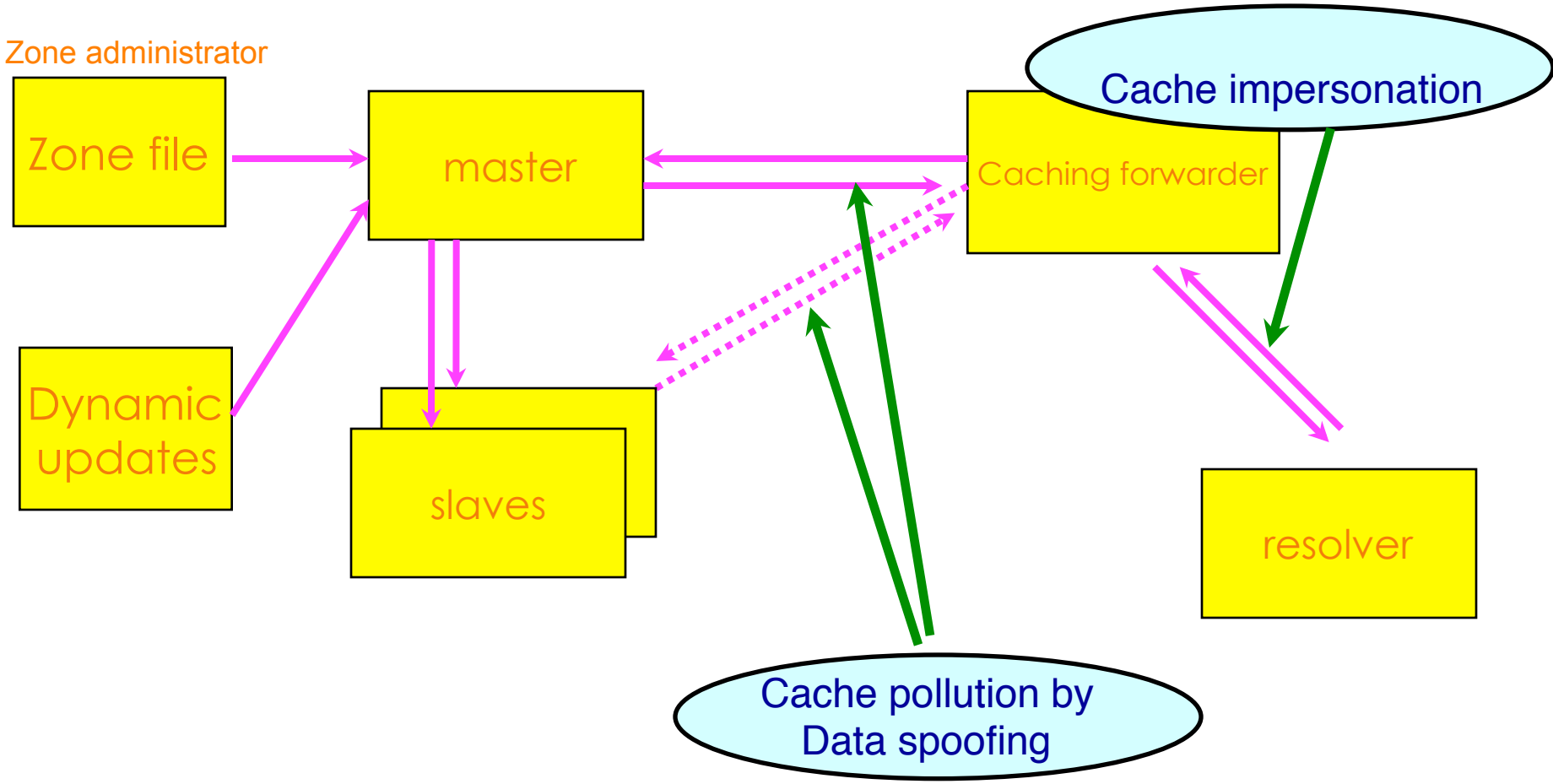
```
$ dig @127.0.0.1 example.net AXFR \
-k Kns1-ns2.pcx.net.+157+15921.key
```

- A wrong key will give “Transfer failed” and on the server the security-category will log this.
- Note: TSIG is time-sensitive

DNS Security Extensions (DNSSEC)

- Protects the integrity of data in the DNS by establishing a chain of trust
- A form of digitally signing the data to attest its validity
- RFC 4033, 4034, 4035
- DNSKEY/RRSIG/NSEC: provides mechanisms to establish authenticity and integrity of data
- DS: provides a mechanism to delegate trust to public keys of third parties

Vulnerabilities protected by DNSSEC



DNSSEC New Resource Records

- 3 Public key crypto related RRs
  - RRSIG = Signature over RRset made using private key
  - DNSKEY = Public key, needed for verifying a RRSIG
  - DS = Delegation Signer; ‘Pointer’ for building chains of authentication
- One RR for internal consistency
  - NSEC = Next Secure; indicates which name is the next one in the zone and which typecodes are available for the current name
    - authenticated non-existence of data

Types of Keys

- Zone Signing Key (ZSK)
  - Sign the RRsets within the zone
  - Public key of ZSK is defined by a DNSKEY RR
- Key Signing Key (KSK)
  - Signed the keys which includes ZSK and KSK and may also be used outside the zone
- Trusted anchor in a security aware server
- Part of the chain of trust by a parent name server
- Using a single key or both keys is an operational choice (RFC allows both methods)

DNSSEC - Setting up a Secure Zone

- Enable DNSSEC in the configuration file (named.conf)
  - `dnssec-enable yes; dnssec-validation yes;`
- Create key pairs (KSK and ZSK)
  - `dnssec-keygen -a rsasha1 -b 1024 -n zone champika.net`
- Publish your public key
- Signing the zone
- Update the config file
  - Modify the zone statement, replace with the signed zone file
- Test with dig

Signing the Zone

- `dnssec-signzone -o champika.net db.champika.net Kchampika.net.+005+33633`
- Once you sign the zone a file with a .signed extension will be created
  - `db.champika.net.signed`
- Note that only authoritative records are signed NS records for the zone itself are signed
  - NS records for delegations are not signed
  - DS RRs are signed!
  - Glue is not signed
- Difference in the file size
  - db.champika.net vs. db.champika.net.signed

Testing with dig: an example

```
dig @localhost www.champika.net
+dnssec +multiline
```

```
; (3 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37425
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.champika.net.      IN A

;; ANSWER SECTION:
www.champika.net.       86400 IN A 192.168.1.2
www.champika.net.       86400 IN RRSIG A 5 3 86400 20091123163643 (
                                20091024163643 22827 champika.net.
                                Eyp1IVyQyYBLKOX2u/LT1+40xjBomXzLrcdwSErgioMb
                                pGyDWDLzP+FTbE3QCfBMLNDt2AGoYcty1cfY4li9sHkw
                                fue6hTQTSm0LhisBkVKQBy6ZD5oGiJQgaIkBGmLtVkPh
                                jGJ8Z1UhbwKcGGK13doAa+5X8mx6MXNCudiNWeg= )

;; AUTHORITY SECTION:
champika.net.           86400 IN NS ns.champika.net.
champika.net.           86400 IN RRSIG NS 5 2 86400 20091123163643 (
                                20091024163643 22827 champika.net.
                                CZsPewlhPWpYTl8wPh09QhD6pWt0If2mLVshviGKq4no
                                ISNVoijmX0LyIns+o3DZz/2+TtwoQCRFLbfI99YMS3fx
                                BHGYqFDeGItyVx3oBpmTuAtMu2+od5WFS+LClsJsEP/N
                                QvUDgtWrj8+ZOwVVj8aLe+I51h29ek7Mzk7+P4E= )

;; ADDITIONAL SECTION:
ns.champika.net.        86400 IN A 192.168.1.1
ns.champika.net.        86400 IN RRSIG A 5 3 86400 20091123163643 (
                                20091024163643 22827 champika.net.
                                eTP05c4GscnoC9V5sR6vgDo02WgCr1T5arU7YZhWctXI
                                vkmU1ni+wguwqW6xezfB/Eu4J69bMnpQoX2zWUDtLUCM
                                +FVLsFx4Bbt+BjPEJKV03g9vv6IdKkR/pxyE1kJWJWmI
                                tR49P2dywlzqqTyvnj3F1yuFRTLHhJvfcVc+n8w= )

;; Query time: 2 msec
```

Questions?

IPv6 Security

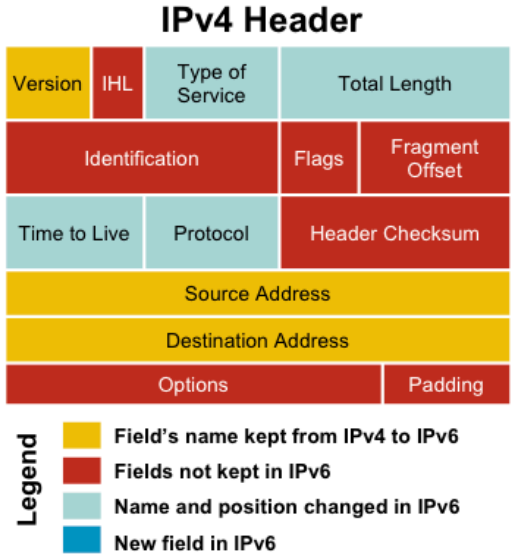
Network Security Workshop

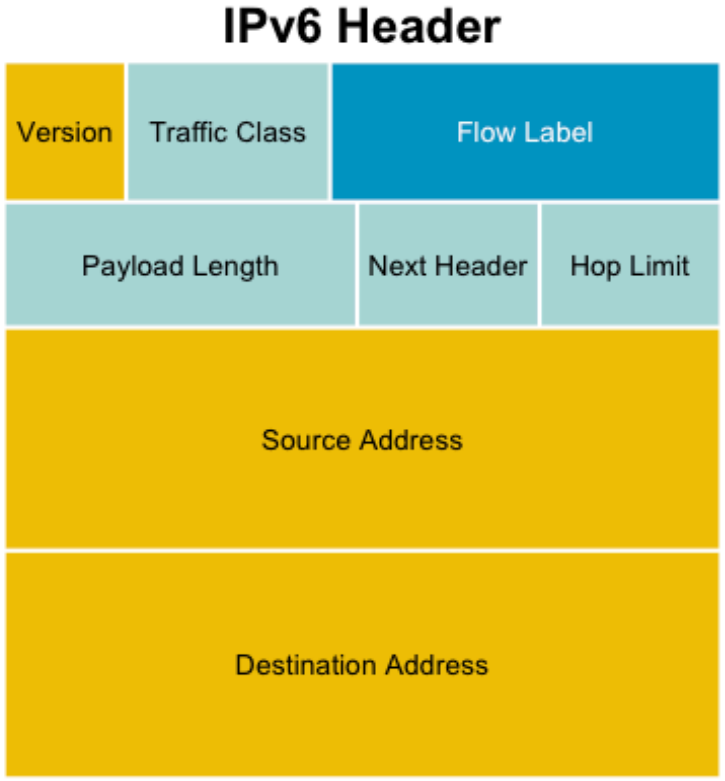
APNIC

IPv6 Security

- IPv6 protocol, where is the big change in TCP/IP protocol stack compared to IPv4
  - On the layer three or network layer of TCP/IP
  - Not much changes on the upper or lower layer from layer 3
- But there can be new threats introduced by IPv6
  - I.e. introduction of new/enhanced header fields
  - The way it interacts with the protocol layers above and below layer 3
  - Newly introduced neighbour discovery process
  - ICMPv6 provide key functionalities in IPv6 protocol operation
  - Elimination of broadcast function and widespread use of multicast in IPv6 protocol operation
  - And so on…

Protocol Header Comparison



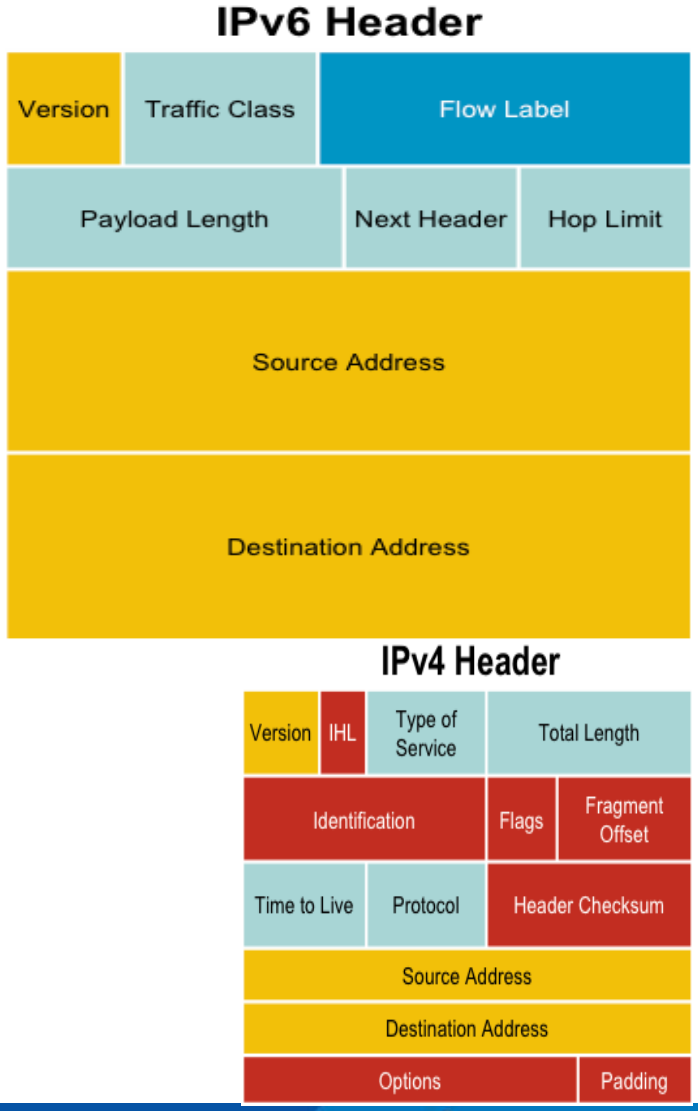


- IPv4 contain 10 basic header field
- IPv6 contain 6 basic header field
- IPv6 header has 40 octets in contrast to the 20 octets in IPv4
- So a smaller number of header fields and the header is 64-bit aligned to enable fast processing by current processors

IPv6 Protocol Header Format

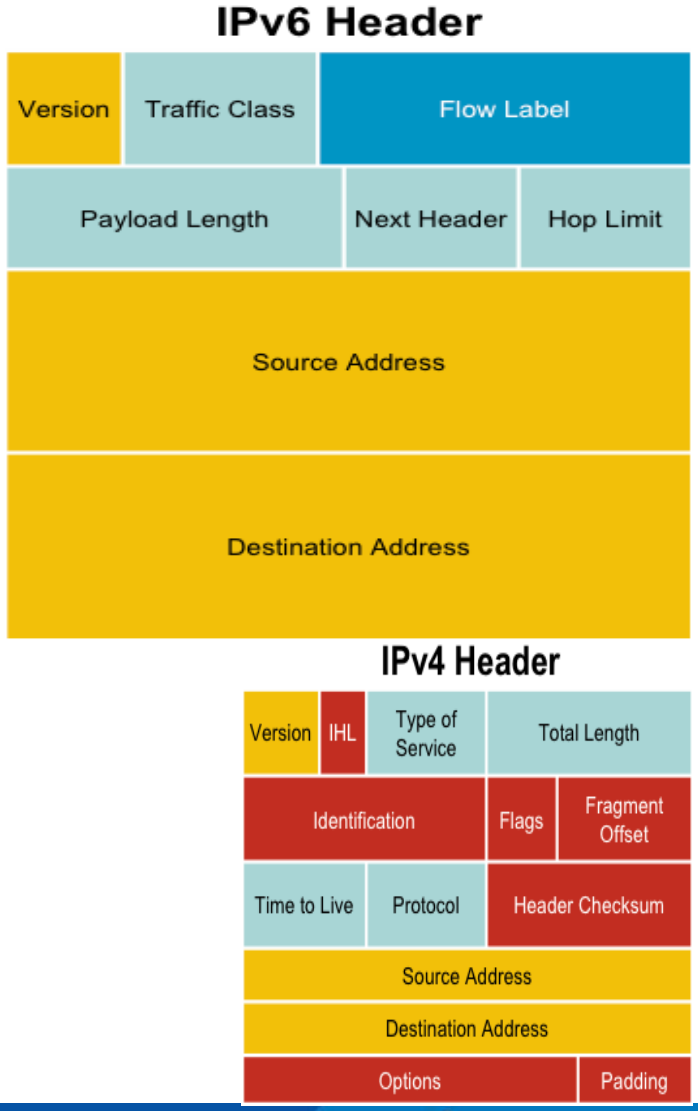
The IPv6 header fields:

- Version:
  - A 4-bit field, same as in IPv4. It contains the number 6 instead of the number 4 for IPv4
- Traffic class:
  - A 8-bit field similar to the type of service (ToS) field in IPv4. It tags packet with a traffic class that it uses in differentiated services (DiffServ). These functionalities are the same for IPv6 and IPv4.
- Flow label:
  - A completely new 20-bit field. It tags a flow for the IP packets. It can be used for multilayer switching techniques and faster packet-switching performance



IPv6 Protocol Header Format

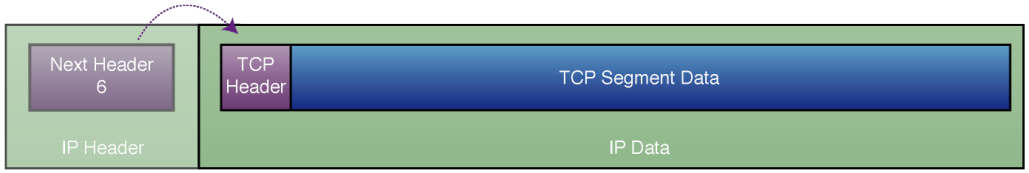
- Payload length:
  - This 16-bit field is similar to the IPv4 Total Length Field, except that with IPv6 the Payload Length field is the length of the data carried after the header, whereas with IPv4 the Total Length Field included the header. 216 = 65536 Octets.
- Next header:
  - The 8-bit value of this field determines the type of information that follows the basic IPv6 header. It can be a transport-layer packet, such as TCP or UDP, or it can be an extension header. The next header field is similar to the protocol field of IPv4.
- Hop limit:
  - This 8-bit field defines by a number which count the maximum hops that a packet can remain in the network before it is destroyed. With the IPv4 TLV field this was expressed in seconds and was typically a theoretical value and not very easy to estimate.



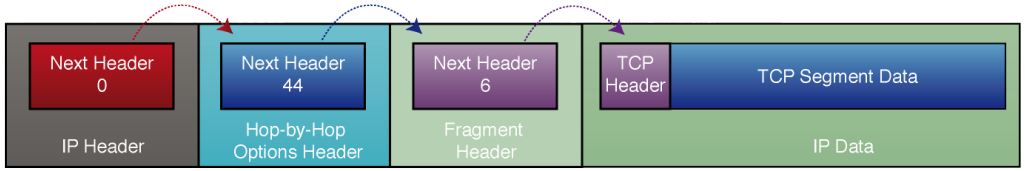
IPv6 Extension Header

- Adding an optional Extension Header in IPv6 makes it simple to add new features in IP protocol in future without a major re-engineering of IP routers everywhere
- The number of extension headers are not fixed, so the total length of the extension header chain is variable
- The extension header will be placed in- between main header and payload in IPv6 packet

Link listed Extension Header



IPv6 Datagram With No Extension Headers Carrying TCP Segment



IPv6 Datagram With Two Extension Headers Carrying TCP Segment

- Link listed extension header can be used by simply using next header code value
- Above example use multiple extension header creating link list by using next header code value i.e 0 44 6
- The link list will end when the next header point to transport header i.e next header code 6

IPv6 Extension Header

- If the Next Header field value (code) is 6 it determine that there is no extension header and the next header field is pointing to TCP header which is the payload of this IPv6 packet
- Possible Code values of Next Header field:
  - 0 Hop-by-hop option
  - 1 ICMPv4
  - 2 IGMPv4
  - 4 IP in IP encapsulation
  - 6 TCP
  - 8 EGP
  - 17 UDP
  - 41 IPv6
  - 43 Routing extension [Source routing]
  - 44 Fragmentation extension
  - 46 Resource Reservation Protocol [RSVP]
  - 50 Encrypted Security Payload [ESP]
  - 51 Authentication Header [AH]
  - 58 ICMPv6
  - 59 Null (No next header)
  - 60 Destination option

Order Of Extension Header

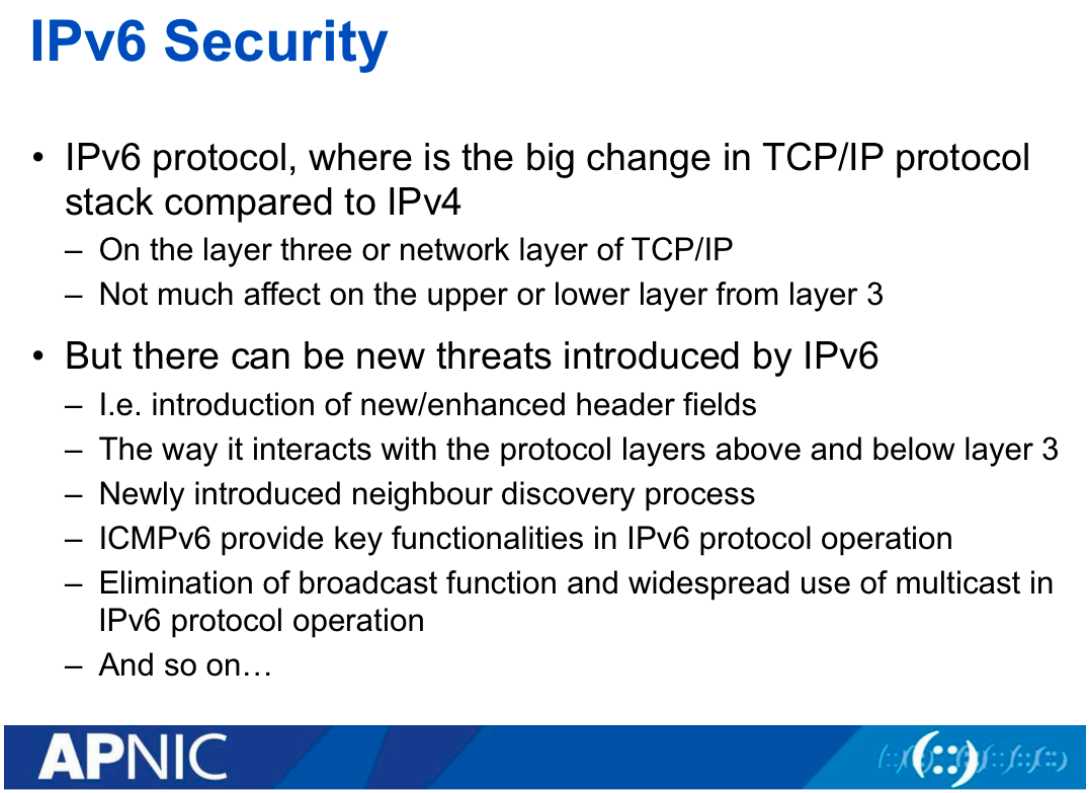
- Source node follow the order:
  - 1. Hop-by-hop
  - 2. Routing
  - 3. Fragment
  - 4. Authentication
  - 5. Encapsulating security payload
  - 6. Destination option
  - 7. Upper-layer
- Order is important because:
  - Only hop-by-hop has to be processed by every intermediate nodes
  - Routing header need to be processed by intermediate routers
  - At the destination fragmentation has to be processed before others
  - This is how it is easy to implement using hardware and make faster processing engine

Fragmentation Handling In IPv6

- Routers handle fragmentation in IPv4 which cause variety of processing performance issues
- IPv6 routers no longer perform fragmentation. IPv6 host use a discovery process [Path MTU Discovery] to determine most optimum MTU size before creating end to end session
- In this discovery process, the source IPv6 device attempts to send a packet at the size specified by the upper IP layers [i.e TCP/Application].
- If the device receives an ICMP packet too big message, it informs the upper layer to discard the packet and to use the new MTU.
- The ICMP packet too big message contains the proper MTU size for the pathway.
- Each source device needs to track the MTU size for each session.

IPv6 Security

- Going back to the previous slide……



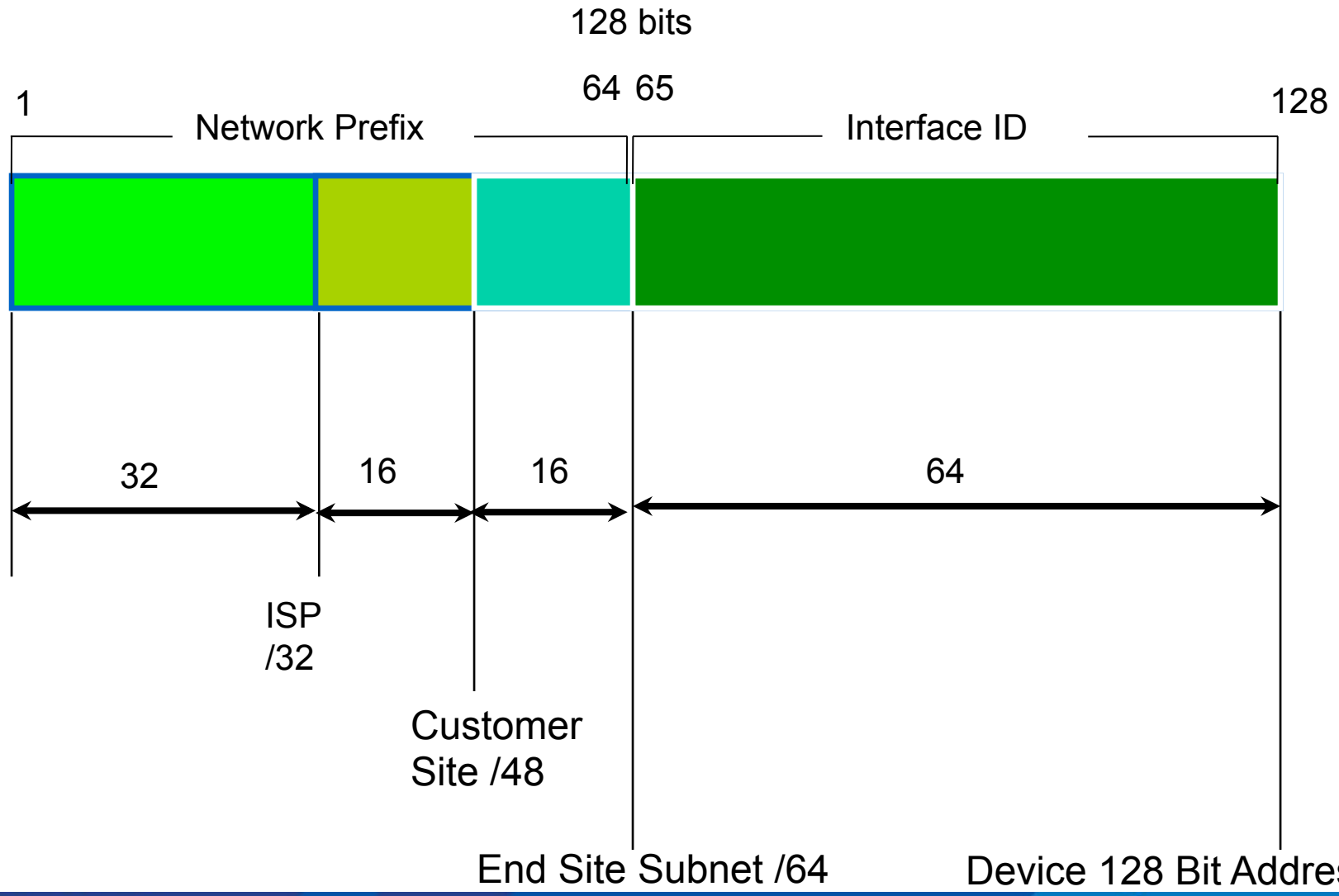
IPv6 Addressing

- An IPv6 address is 128 bits long
- So the number of addresses are 2^128
  =340282366920938463463374607431768211455
  (39 decimal digits)
  =0xffffffffffffffffffffffffffffffff (32 hexadecimal digits)
- In hex 4 bit (nibble) is represented by a hex digit
- So 128 bit is reduced down to 32 hex digit

IPv6 Address Representation

- Hexadecimal values of eight 16 bit fields
  - X:X:X:X:X:X:X:X (X=16 bit number, ex: A2FE)
  - 16 bit number is converted to a 4 digit hexadecimal number
- Example:
  - FE38:DCE3:124C:C1A2:BA03:6735:EF1C:683D
  - Abbreviated form of address
    - 4EED:0023:0000:0000:0000:036E:1250:2B00
    - →4EED:23:0:0:0:36E:1250:2B00
    - →4EED:23::36E:1250:2B00
    - (Null value can be used only once)

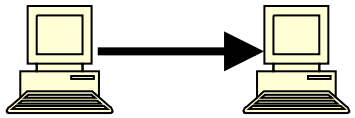
IPv6 addressing structure

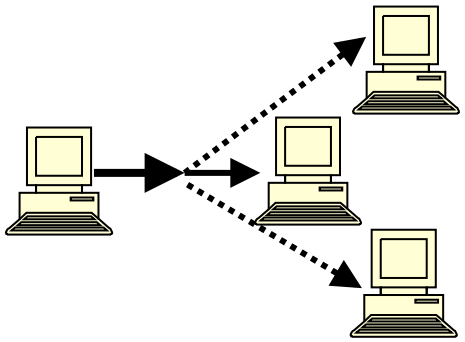


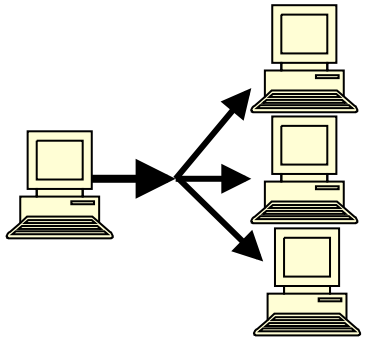
IPv6 addressing model

- **IPv6 Address type**
  - Unicast
    - An identifier for a single interface
  - Anycast
    - An identifier for a set of interfaces
  - Multicast
    - An identifier for a group of nodes

RFC 4291







Addresses Without a Network Prefix

- Localhost ::1/128
- Unspecified Address ::/128
- IPv4-mapped IPv6 address ::ffff/96 [a.b.c.d]
- IPv4-compatible IPv6 address ::/96 [a.b.c.d]

Local Addresses With Network Prefix

- Link Local Address
  - A special address used to communicate within the local link of an interface
  - i.e. anyone on the link as host or router
  - This address in packet destination that packet would never pass through a router
  - fe80::/10

Local Addresses With Network Prefix

- Unique Local IPv6 Unicast Address
  - Addresses similar to the RFC 1918 / private address like in IPv4 but will ensure uniqueness
  - A part of the prefix (40 bits) are generated using a pseudo-random algorithm and it's improbable that two generated ones are equal
  - fc00::/7
  - Example webtools to generate ULA prefix

    http://www.sixxs.net/tools/grh/ula/

    http://www.goebel-consult.de/ipv6/createLULA

Global Addresses With Network Prefix

- IPV6 Global Unicast Address
  - Global Unicast Range: 0010 2000::/3

    0011 3000::/3
  - All five RIRs are given a /12 from the /3 to further distribute within the RIR region
    - APNIC 2400:0000::/12
    - ARIN 2600:0000::/12
    - AfriNIC 2C00:0000::/12
    - LACNIC 2800:0000::/12
    - Ripe NCC 2A00:0000::/12

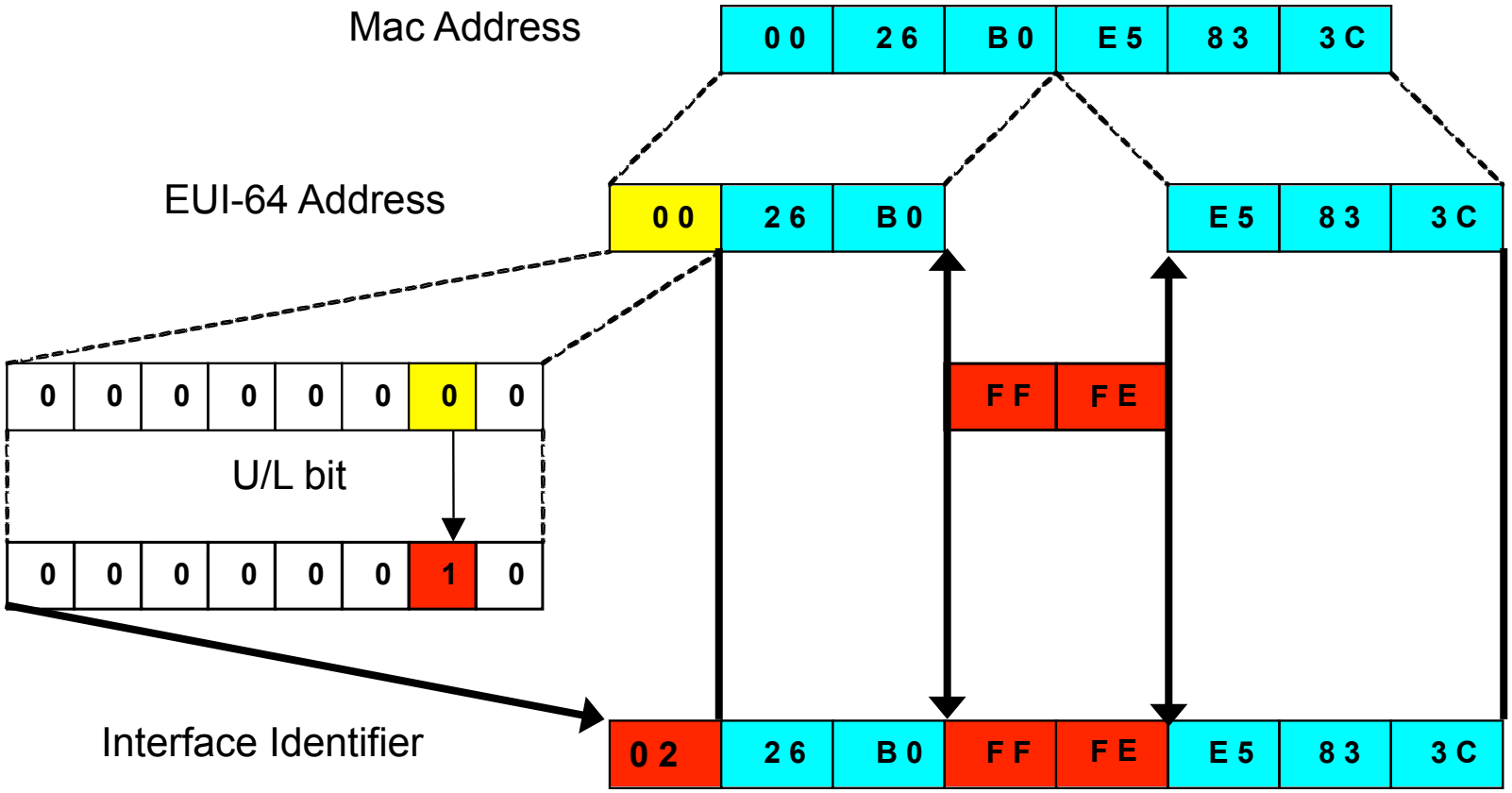
Examples and Documentation Prefix

- Two address ranges are reserved for examples and documentation purpose by RFC 3849
  - For example 3fff:ffff::/32
  - For documentation 2001:0DB8::/32

Interface ID

- The lowest-order 64-bit field addresses may be assigned in several different ways:
  - auto-configured from a 48-bit MAC address expanded into a 64-bit EUI-64
  - assigned via DHCP
  - manually configured
  - auto-generated pseudo-random number
  - possibly other methods in the future

EUI-64


Mac Address
00 26 B0 E5 83 3C
EUI-64 Address
00 26 B0 E5 83 3C
FF FE
0 0 0 0 0 0 0 0
U/L bit
0 0 0 0 0 0 1 0
Interface Identifier
02 26 B0 FF FE E5 83 3C

IPv6 autoconfiguration

- Stateless mechanism
  - For a site not concerned with the exact addresses
  - No manual configuration required
  - Minimal configuration of routers
  - No additional servers
- Stateful mechanism
  - For a site that requires tighter control over exact address assignments
  - Needs a DHCP server
    - DHCPv6

Plug and Play

- IPv6 link local address
  - Even if no servers/routers exist to assign an IP address to a device, the device can still auto-generate an IP address
    - Allows interfaces on the same link to communicate with each other
- Stateless
  - No control over information belongs to the interface with an assigned IP address
    - Possible security issues
- Stateful
  - Remember information about interfaces that are assigned IP addresses

IPv6 Security Features

- IPsec is mandatory in IPv6
- Since IPsec become part of the IPv6 protocol all node can secure their IP traffic if they have required keying infrastructure
- In build IPsec does not replace standard network security requirement but introduce added layer of security with existing IP network

Historical Purpose of ICMP

- **I**nternet **C**ontrol **M**essage **P**rotocol (ICMP) was initially drafted in RFC 791 & 792
  - Allow errors/information to report back to the transmitting device to facilitate testing and debugging in TCP/IP network
  - Originally created to allow the reporting of a small set of error conditions of IPv4 networks
- It work as a protocol on top of IP as an “administrative assistant”
- One of the under-appreciated service of TCP/IP protocol because of its wide spread use by the hackers
- Not all functions are harmful for network though ☺

ICMP Messages

- Most of the firewall administrator would like to block nearly all ICMP messages for IPv4
- IPv4 communication still work
- There are two class of ICMPv4 messages
  - Error messages
    - i.e. Destination unreachable, Source quench, Redirect, Time exceeded, Parameter problem
  - Informational messages
    - i.e. Echo (Request), Echo reply, Router advertisement, Router solicitation, Time stamp (Request), Timestamp reply, Information request, Information reply, Address mask request, address mask reply, Traceroute

ICMP Messages

- Error messages
  - Error message includes the original full IP header and the first 8 bytes of the payload. Beginning of the payload will contain higher-layer header. ICMP message also carries either the full UDP header, or the first 8 bytes of the TCP header. In both cases, the source and destination port numbers are provided

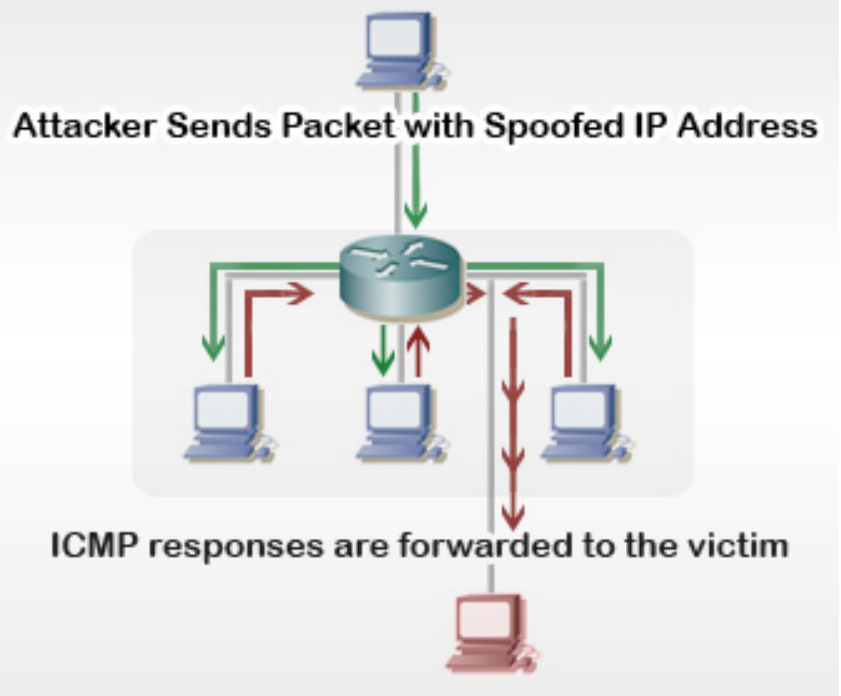
- Informational messages
  - Informational messages are used to let devices exchange information, implement certain IP-related features, and perform testing. They do not indicate errors and are typically not sent in response to a regular datagram transmission. They are generated either when directed by an application, or on a regular basis to provide information to other devices. An informational ICMP message may also be sent in reply to another informational ICMP message, since they often occur in request/reply or solicitation/advertisement functional pairs.

ICMP Attack Vector

- Some of the ICMP messages can be used and attack vector by the hacker i.e.
  - ECHO_REQUEST
    - Which will allow network reconnaissance or DoS attack
  - REDIRECT
    - Which could achieve the same result to source routing
  - DESTINATION_ UNREACHABLE
    - This ICMP message can cause a host to drop a connection immediately
  - TIME_EXCEEDED
    - This ICMP message can cause a host to drop a connection immediately

Smurf Attack

- The Smurf attack is named after the source code employed to launch the attack (smurf.c)
- ICMP ECHO_REQUEST packets are sent to the broadcast address of a network.
- Depending on host configuration they may attempt to reply to the ECHO_REQUEST
- The resulting flood of responses may degrade the performance of the network particularly at the destination host.



ICMP DoS Attack

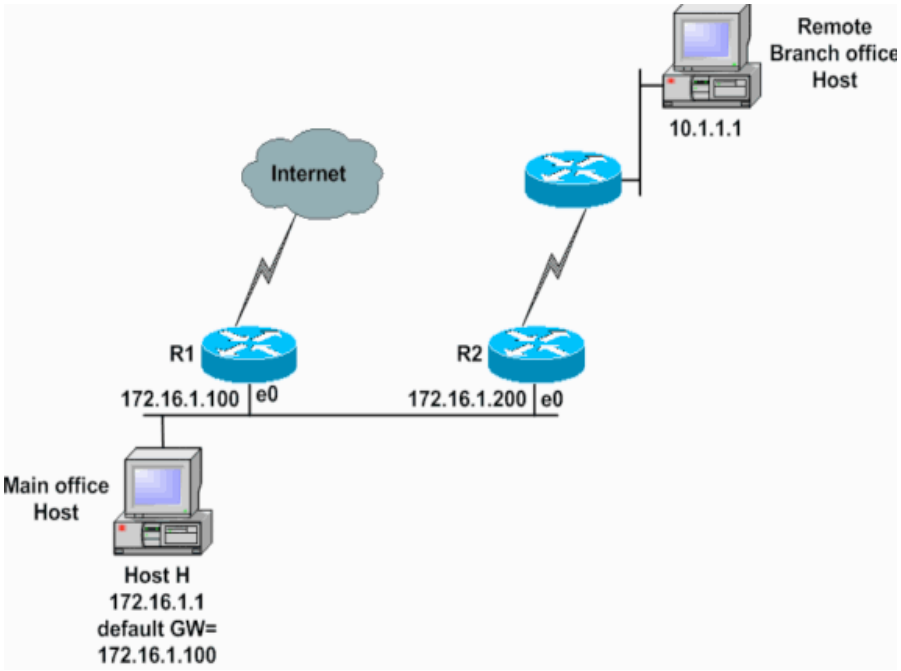
- Attacker could use either TIME_EXCEEDED or DESTINATION_UNREACHABL messages
- By forging one of this ICMP messages and sending it to any of the communicating host
- They will immediately drop a connection

Ping of Death Attack

- An attacker sends an ICMP ECHO_REQUEST packet that is larger than the maximum IP packet size.
- Since the received ICMP echo request packet is larger than the normal IP packet size, it is fragmented
- The target can't reassemble the packets, so the OS crashes or reboots

ICMP Redirect Attack

- Router R1 will send an ICMP REDIRECT message to host H to send packet to R2 directly for destination 10.1.1.1
- Hackers can utilize this behavior and initiate man-in-the-middle attack



How to Stop These?

- Most of the firewall administrator would like to block nearly all ICMP messages for IPv4 on the perimeter ☺
- Use interface command

```
no ip redirects
no ip directed-broadcast
no ip unreachables
```

- Use ACL (Advance ACL using ICMP Type and Code)

ICMPv6 Functions in IPv6

- ICMPv6 defined in RFC 4443
- ICMPv6 has features that are very important for the function of IPv6 protocol [unlike IPv4 where ICMP is used for testing and troubleshooting purpose]
  - i.e. ND, PMTUD etc
- ICMPv6 has its own IPv6 extension header type code which is 58

ICMPv6 Functions in IPv6

- Following functions are very important which is part of ICMPv6:
  - Neighbor Discovery Protocol (NDP) i.e. Neighbor Advertisement (NA) and Neighbor Solicitations (NS)
  - Router Advertisements (RA) and Router Solicitation (RS)
  - Path MTU Discovery (PMTUD)
  - Multicast Listener Discovery (MLD)
  - Multicast Router Discovery (MRD)

IPv6 Neighbor Discovery (ND)

- IPv6 use multicast (L2) instead of broadcast to find out target host MAC address
- It increases network efficiency by eliminating broadcast from L2 network
- IPv6 ND use ICMP6 as transport
  - Compared to IPv4 ARP no need to write different ARP for different L2 protocol i.e. Ethernet etc.

IPv6 Neighbor Discovery (ND)

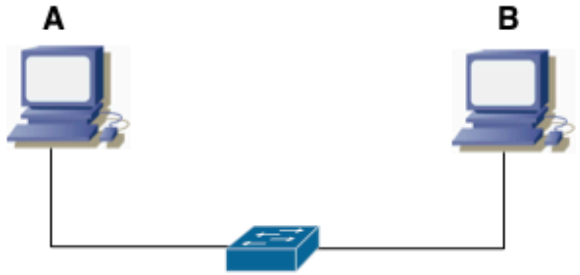
- Solicited Node Multicast Address
  - Start with FF02:0:0:0:0:1:ff::/104
  - Last 24 bit from the interface IPV6 address
- Example Solicited Node Multicast Address
  - IPV6 Address 2406:6400:0:0:0:0:0000:0010
  - Solicited Node Multicast Address is FF02:0:0:0:0:1:ff00:0010
- All host listen to its solicited node multicast address corresponding to its unicast and anycast address (If defined)

IPv6 Neighbor Discovery (ND)

- Host A would like to communicate with Host B
- Host A IPv6 global address 2406:6400::10
- Host A IPv6 link local address fe80::226:bbff:fe06:ff81
- Host A MAC address 00:26:bb:06:ff:81
- Host B IPv6 global address 2406:6400::20
- Host B Link local UNKNOWN [Gateway if outside the link]
- Host B MAC address UNKNOWN
- How Host A will create L2 frame for Host B?

IPv6 Neighbor Discovery (ND)

Host A
IPV6 global address: 2406:6400::0010
IPv6 Link local: fe80::0226:bbff:fe06:ff81
MAC address: 00:26:bb:06:ff:81
Listen to other then above:
FF02::1 [All node multicast]
FF02:0:0:0:0:1:ff00:0010 [Solicited node m.cast unicast]
FF02:0:0:0:0:1:ff06:ff81 [Solicited node m.cast link local]



Multicast enable switch: Unicast by IGMP snooping
Non multicast enable switch: broadcast, PC LAN card filter or discard

Packet S: 2406:6400::0010 D:2406:6400::0020

ICMP6 NS Type 135
S: fe80::0226:bbff:fe06:ff81
D:FF02:0:0:0:0:1:ff00:0020

Frame
S: 00:26:bb:06:ff:81 D 33:33:ff:00:00:20
Ethernet reserved IPv6 m.cast: 33:33:xx:xx:xx:xx

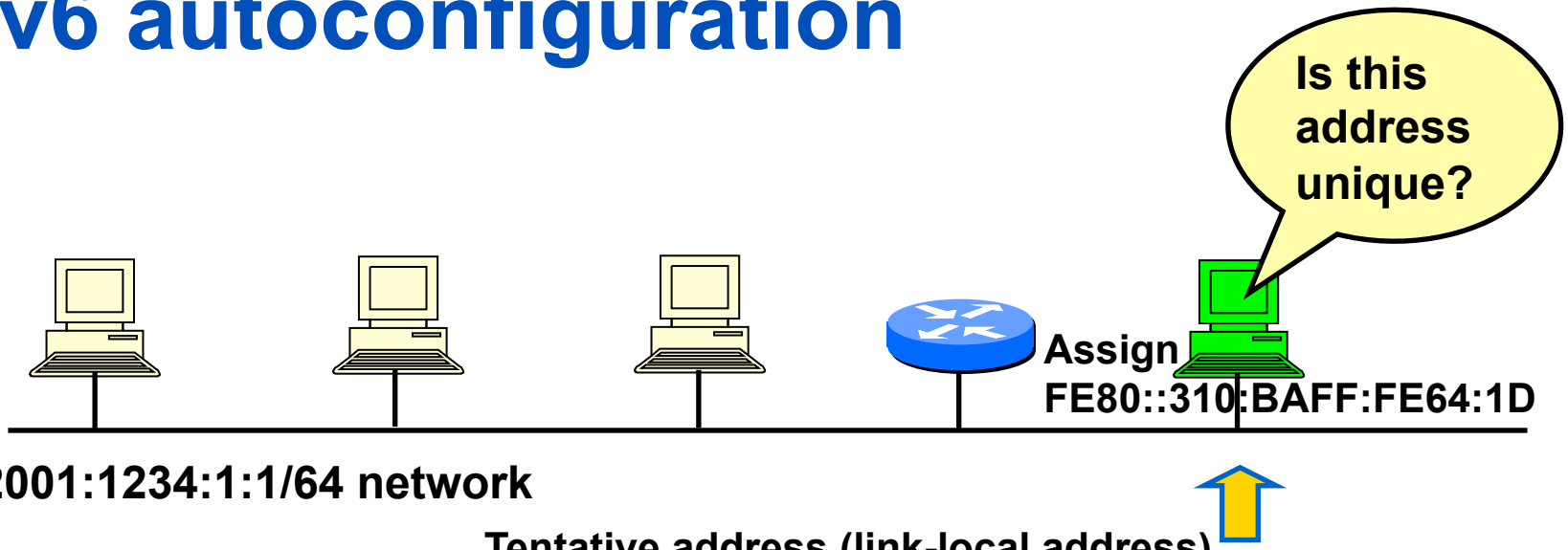
Host B
IPV6 global address: 2406:6400::0020
IPv6 Link local: fe80::0226:bbff:fe06:ff82 [Unknown to A]
MAC address: 00:26:bb:06:ff:82 [Unknown to A]
Listen to other then above:
FF02::1 [All node multicast]
FF02:0:0:0:0:1:ff00:0020 [Solicited node m.cast unicast]
FF02:0:0:0:0:1:ff06:ff82 [Solicited node m.cast link local]

Packet S: 2406:6400::0020 D:2406:6400::0010

ICMP6 NA Type 136
S: fe80::0226:bbff:fe06:ff82
D:fe80::0226:bbff:fe06:ff81

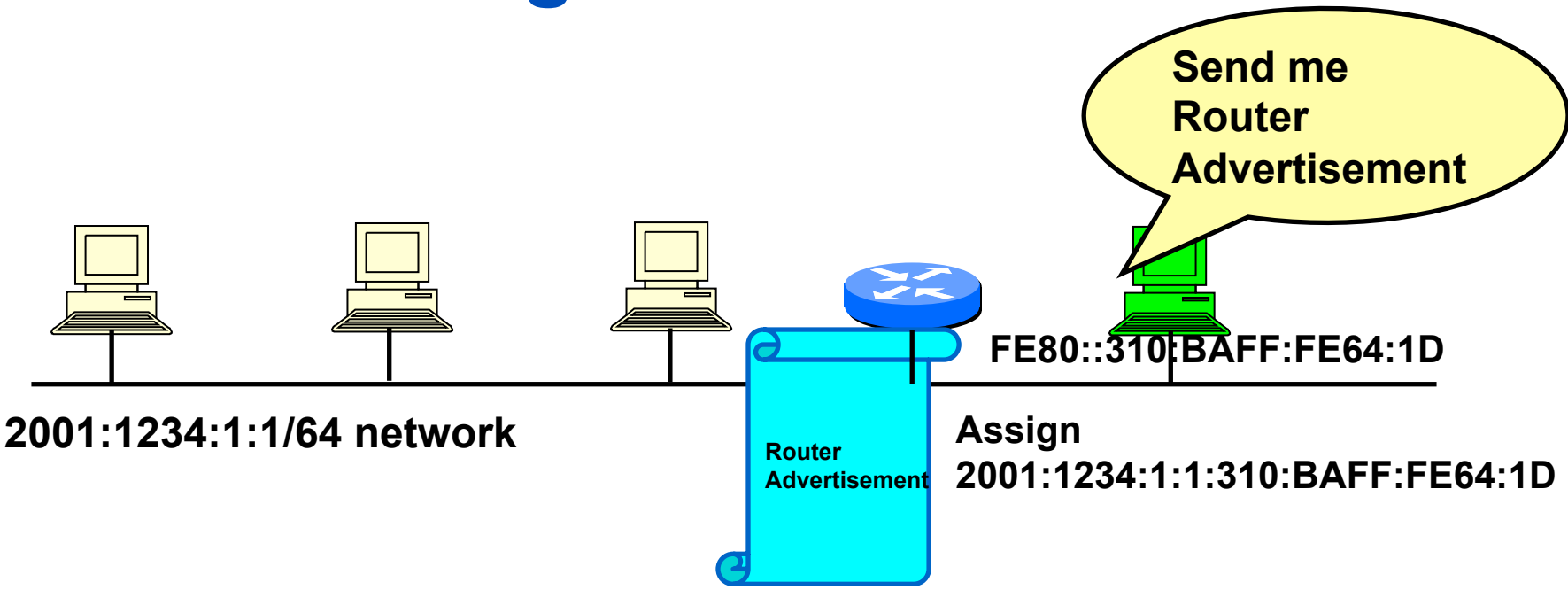
Frame
S: 00:26:bb:06:ff:82 D 00:26:bb:06:ff:81

IPv6 autoconfiguration



1. A new host is turned on.
2. Tentative address will be assigned to the new host.
3. Duplicate Address Detection (DAD) is performed. First the host transmit a Neighbor Solicitation (NS) message to the solicited node multicast address (FF02::1:FF64:001D) corresponding to its to be used address
5. If no Neighbor Advertisement (NA) message comes back then the address is unique.
6. FE80::310:BAFF:FE64:1D will be assigned to the new host.

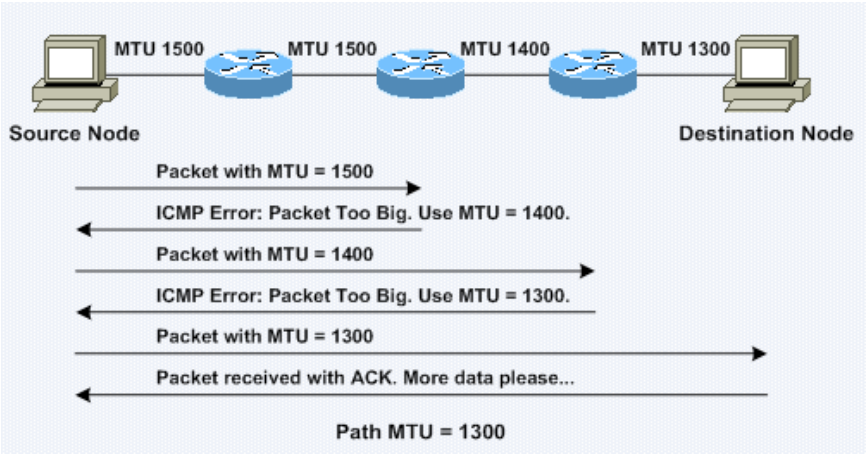
IPv6 autoconfiguration



1. The new host will send Router Solicitation (RS) request to the all-routers multicast group (FF02::2).
2. The router will reply Routing Advertisement (RA).
3. The new host will learn the network prefix. E.g, 2001:1234:1:1/64
4. The new host will assigned a new address Network prefix+Interface ID E.g, 2001:1234:1:1:310:BAFF:FE64:1D

IPv6 Path MTU Discovery

- IPv6 router no longer perform fragmentation
- To make sure there will not be any fragmentation requirement in any router along the path
  - Source host send a Path MTU Discovery message (Per session)
  - Use its default MTU size and wait for “ICMPv6 packet too big” reply message
  - If no reply come back from any router along the path then default MTU is the optimal MTU
  - If “ICMPv6 packet too big” reply message come then adjust with the smallest MTU size from the reply message
  - Each source device needs to track the MTU size for each session



ICMPv6 Messages

- There are two class of ICMPv6 messages (Like ICMPv4)
  - Error messages
    - Destination Unreachable, Packet Too Big, Time Exceeded, Parameter Problem
  - Informational messages
    - Echo request, Echo reply, Router solicitation, Router advertisement, Redirect, Router renumbering

Type	1	***Type:*** Identifies the ICMPv6 message type; for *Destination Unreachable*

- ICMPv6 message contain a type (8 bit) and code (8 bit)
  - Type: Identifies the ICMP message type i.e Destination Unreachable
  - Code: That relate the details (Sub type) of the message to the type of the message i.e. Destination Unreachable (Type 1) has got 4 code (Sub type)

Code Value	Message Subtype
0	*No Route To Destination*
1	*Communication With Destination Administratively Prohibited*
3	*Address Unreachable*
4	*Port Unreachable*

ICMPv6 Messages

- One minor improvement made in ICMPv6 was that the message types were separated
- In IPv6 error messages have type values from 0 to 127 and informational messages have type values from 128 to 255
- List of all ICMPv6 type and code value
  - http://www.iana.org/assignments/icmpv6-parameters
- Some of the type values are defined so far
  - So undefined type should be blocked
    - Unallocated error messages: Type 5-99 and type 102-126
    - Unallocated informational message: Type 156-199 and type 202-254
    - Experimental message: Type 100, 101, 200, 201
    - Extension type message: Type 127, 255
- However if new message are allocated by IANA in future, adjustment need to be made to this filter

ICMPv6 Messages

- ICMPv6 is used for many legitimate purpose so following messages must be permitted through the network perimeter
  - Type 1: Destination Unreachable
  - Type 2: Packet Too Big [PMTUD]
  - Type 3: Time Exceeded
  - Type 4: Parameter Problem
- Following messages can be permitted as an option through the network perimeter (If Source & Destination of the packet can be controlled)
  - Type 128: Echo Request
  - Type 129: Echo Reply

ICMPv6 Messages

- Following messages need to be blocked through the network perimeter if those functions are not used for specific purpose:
  - Type 138: Router Renumbering
  - Type 129: Echo Reply
  - Type 139 & 140: Node Information Query Messages

ICMPv6 Messages

- ICMPv6 error message contain part/full of the original packet in its payload that cause the error at the first place
  - More likely full packet in ICMPv6 as minimum MTU is 1280 byte
- This payload could be used by the hacker as a covert channel to send any malicious code
- So firewall should inspect payload segment in ICMPv6 error packet to make sure it is legitimate
  - If the error packet fragment does not contain legitimate IPv6 address or it is not statefully sent then packet should be dropped

ICMPv6 Messages

- A Denial of Service (DoS) attack can be initiated by generating a stream of illegal packets i.e large packet, expiring hop count etc
  - If enough erred packets are generated it could drive high CPU utilization of the router
- ICMPv6 error message generation can be limited by using following command
  - Router(config)#ipv6 icmp error-interval 10000 [in millisecond]

ICMPv6 Messages

- Rate limiting ICMPv6 traffic from overwhelming the router

```
!
ipv6 access-list ICMPv6
 permit icmp any any
!
class-map match-all ICMPv6
 match protocol ipv6
 match access-group name ICMPv6
!
!
policy-map ICMPv6_RATE_LIMIT
 class ICMPv6
    police 100000 200000 conform-action transmit  exceed-action
drop
!
Interface fa0/0
 service-policy input ICMPv6_RATE_LIMIT
```

Example configuration

- ICMPv6 filter (Undefined ICMPv6 message type)

```
Router#sh ipv6 access-list ICMPV6_UNDEFINE_TYPE
IPv6 access list ICMPV6_UNDEFINE_TYPE
        deny icmp any any 5 99 sequence 10
        deny icmp any any 102 126 sequence 20
        deny icmp any any 156 199 sequence 30
        deny icmp any any 202 254 sequence 40
        deny icmp any any 100 sequence 50
        deny icmp any any 101 sequence 60
        deny icmp any any 200 sequence 70
        deny icmp any any 201 sequence 80
        deny icmp any any 127 sequence 90
        deny icmp any any 255 sequence 100
        permit icmp any any sequence 110
```

Example configuration

- ICMPv6 filter (Specific ICMPv6 message type and code)

```
Router(config)#ipv6 access-list ICMPV6_SPECIFIC_TYPE_CODE
Router(config-ipv6-acl)#deny icmp any any ?
<0-255>                  ICMPv6 message type
auth                     Match on authentication header
beyond-scope             Destination beyond scope
dest-option              Destination Option header (all types)
dest-option-type         Destination Option header with type
destination-unreachable  Destination address is unreachable
dhaad-reply              Home agent address discovery reply
dhaad-request            Home agent address discovery request
dscp                     Match packets with given dscp value
```

Continue next slide…….

Example configuration

```
  echo-reply                Echo reply
  echo-request              Echo request (ping)
  flow-label                Flow label
  header                    Parameter header problems
  hop-limit                 Hop limit exceeded in transit
  log                       Log matches against this entry
  log-input                 Log matches against this entry,
including input
  mld-query                 Multicast Listener Discovery Query
  mld-reduction             Multicast Listener Discovery Reduction
  mld-report                Multicast Listener Discovery Report
  mobility                  Mobility header (all types)
```

Continue next slide…….

Example configuration

mobility-type	*Mobility header with type*
mpd-advertisement	*Mobile prefix advertisement*
mpd-solicitation	*Mobile prefix solicitation*
nd-na advertisements	*Neighbor discovery neighbor*
nd-ns solicitations	*Neighbor discovery neighbor*
next-header	*Parameter next header problems*
no-admin	*Administration prohibited destination*

Continue next slide…….

Example configuration

no-route	*No route to destination*
packet-too-big	*Packet too big*
parameter-option	*Parameter option problems*
parameter-problem	*All parameter problems*
port-unreachable	*Port unreachable*
reassembly-timeout	*Reassembly timeout*
redirect	*Neighbor redirect*

Extension Header Threats

- IPv6 extension headers are used to extend the functionality of the protocol
- An attacker could manipulate this feature to create attack
  - Create an IPv6 packet with long list of extension headers that cause a DoS to the routers along the path or to the destination host
  - Lengthy extension headers could consume system resource or could crash the the host protocol stack
  - Could be use as an attack vector to inject malicious code to the network by avoiding firewall and IDS (Numerous extension header in a single packet could spread the payload in to second fragment that could not be checked by the firewall)

IPv6 Extension Headers

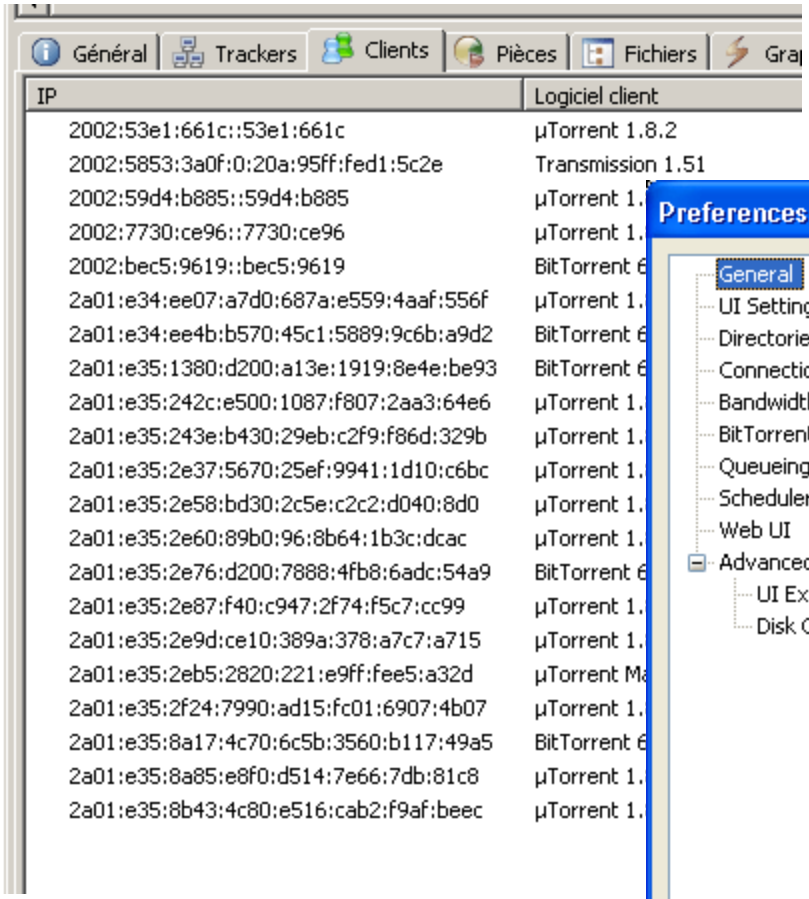
Common IPv6 *Next Header* Values

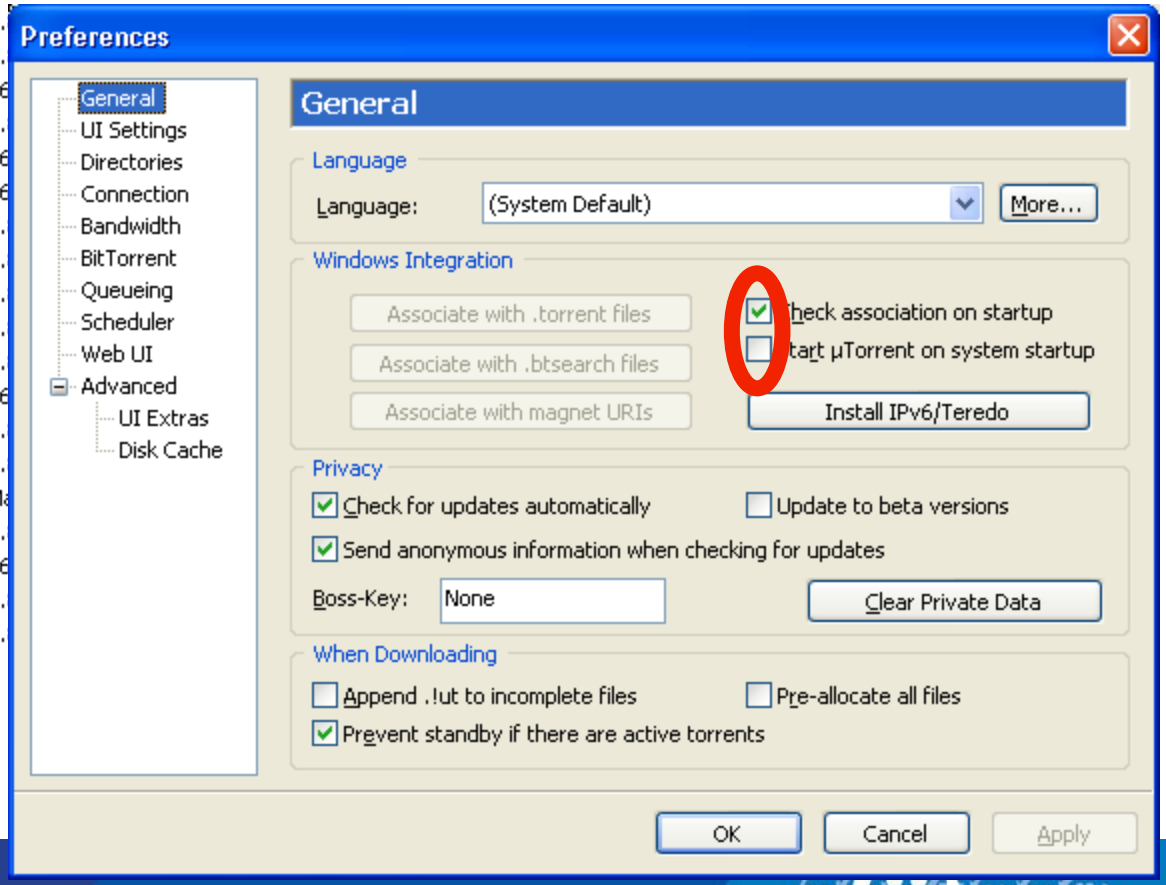
Value (Hexadecimal)	Value (Decimal)	Protocol / Extension Header
00	0	Hop-By-Hop Options Extension Header (note that this value was “Reserved” in IPv4)
01	1	ICMPv4
02	2	IGMPv4
04	4	IP in IP Encapsulation
06	6	TCP
08	8	EGP
11	17	UDP
29	41	IPv6
2B	43	Routing Extension Header
2C	44	Fragmentation Extension Header
2E	46	Resource Reservation Protocol (RSVP)
32	50	Encrypted Security Payload (ESP) Extension Header
33	51	Authentication Header (AH) Extension Header
3A	58	ICMPv6
3B	59	No Next Header
3C	60	Destination Options Extension Header

Should I care?

- Is IPv6 in my IPv4 network?
  - Easy to check!
- Look inside IPv4 NetFlow records
  - Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  - IPv4 address: 192.88.99.1 (6to4 anycast server)
  - UDP 3544, the public part of Teredo, yet another tunnel
- Look into DNS requests log for ‘ISATAP’

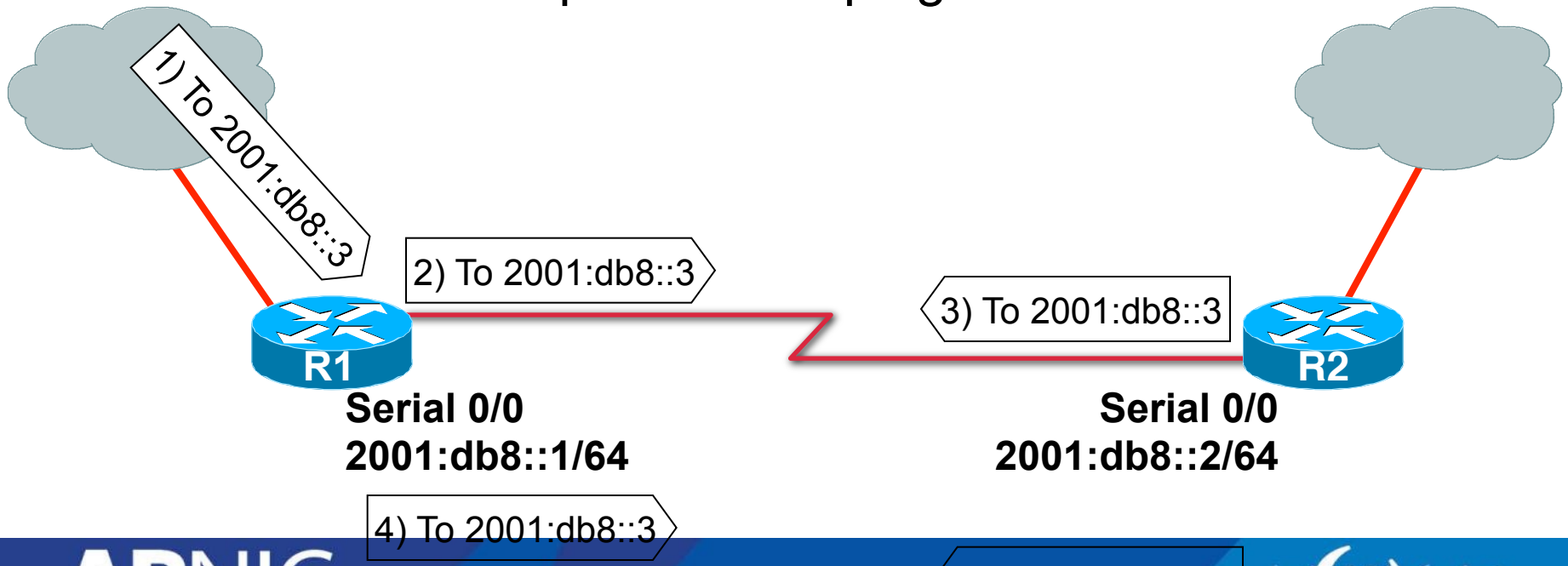
Is it real? May be!
uTorrent 1.8 (released Aug 08)





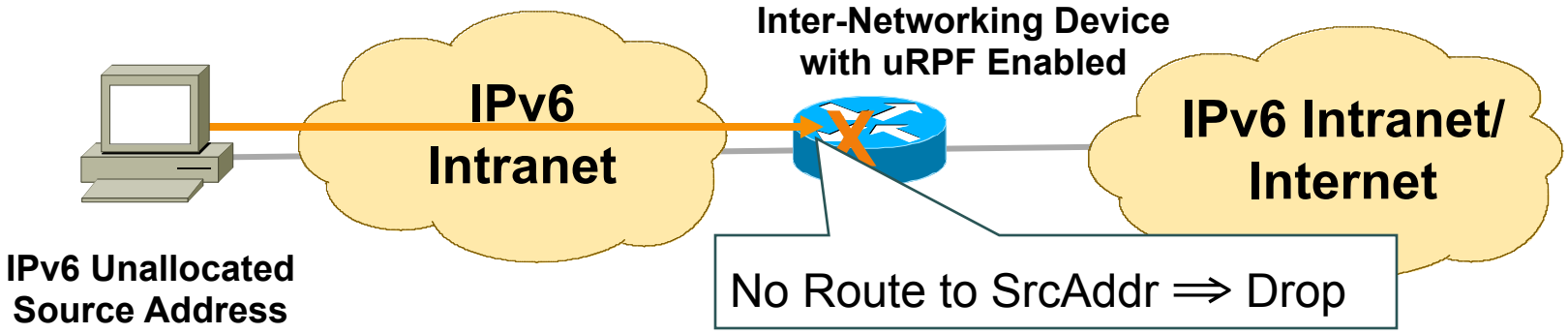
DoS Example
Ping-Pong over Physical Point-to-Point

- Cisco IOS implements RFC 4443 so this is not a threat
- Otherwise use /127 on P2P link (see also RFC 3627)
- Same as in IPv4, on real P2P, if not for me send it on the other side... Could produce looping traffic



IPv6 Bogon Filtering and Anti-Spoofing

- IPv6 nowadays has its bogons:
  - http://www.cymru.com/Bogons/ipv6.txt
- Similar situation as IPv4
  - ⇒ Same technique = uRPF



By the Way: It Is Real ☹ IPv6 Hacking/Lab Tools

- Sniffers/packet capture
  - Snort
  - TCPdump
  - Sun Solaris snoop
  - COLD
  - Wireshark
  - Analyzer
  - Windump
  - WinPcap
- DoS Tools
  - 6tunneldos
  - 4to6ddos
  - Imps6-tools
- Scanners
  - IPv6 security scanner
  - Halfscan6
  - Nmap
  - Strobe
  - Netcat
- Packet forgers
  - Scapy6
  - SendIP
  - Packit
  - Spak6
- Complete toolkit
  - www.thc.org/thc-ipv6/

Candidate Best Practices

- Train your network operators and security managers on IPv6
- Train your network operators and security managers on IPv6
- Selectively filter ICMP (RFC 4890)
- Block Type 0 Routing Header at the edge

Candidate Best Practices Mainly for Enterprise Customers

- Implement privacy extensions carefully
- Filter internal-use IPv6 addresses & ULA at the border routers
- Filter unneeded services at the firewall
- Maintain host and application security
- Use cryptographic protections where critical
- Implement ingress filtering of packets with IPv6 multicast source addresses
- Use static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints

Questions?

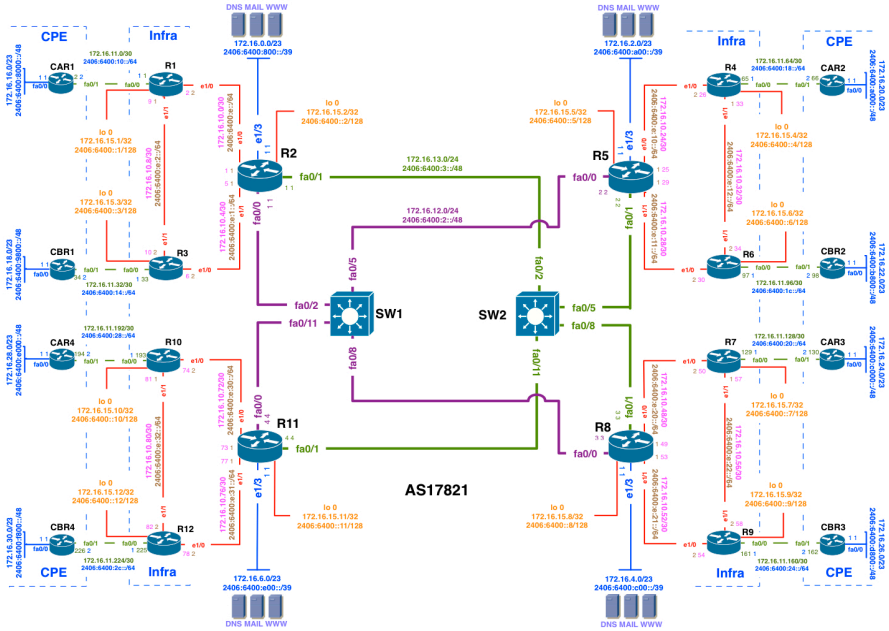
Route Filtering

Network Security Workshop

APNIC

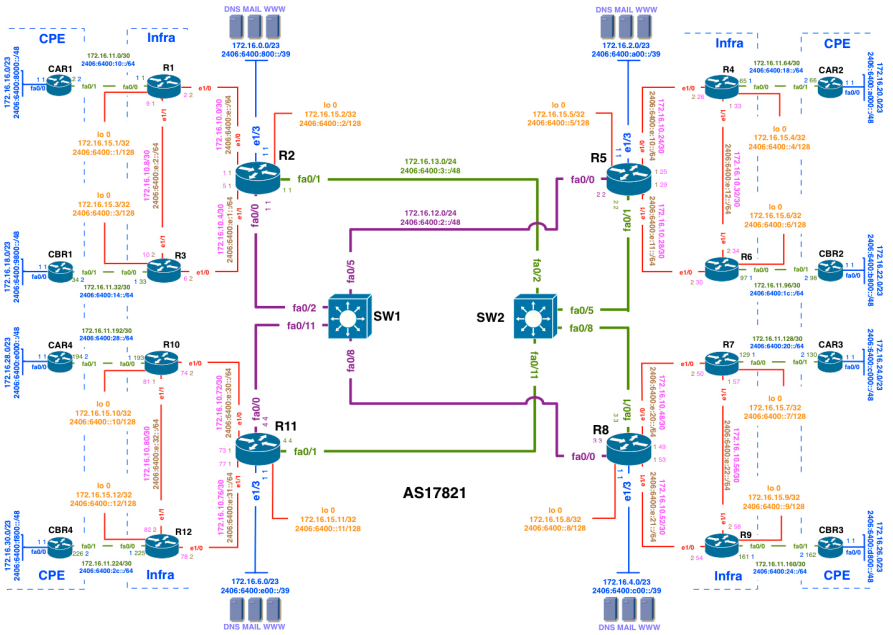
Route Filtering

- Types of prefixes in IP core network:
  - Internal Prefixes
  - External prefixes
    - Downstream customers
    - Internet prefixes



Route Filtering

- Internal prefixes originated in IP core network
  - Loopback
  - Transport
    - Connect inter-regional networks
  - Point-to-point
    - Infrastructure point-to-point
    - Customer side point-to-point
  - Data centre
    - Some ISP originate from separate AS if it is a large public hosting operation and multihome DC



Route Filtering

- Loopback Prefix
  - Prefix size /128
  - Advertised in IGP i.e. OSPF
  - Scope within IP core network
    - Can be summarize in IGP i.e. OSPF if the number of loopback prefixes are large within the region

Route Filtering

Loopback prefixes in Training ISP network:

```
Router1#sh ipv6 route
IPv6 Routing Table - default - 51 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, I - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

LC  2406:6400::1/128 [0/0]
     via Loopback0, receive
OI  2406:6400::2/128 [110/10]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
O   2406:6400::3/128 [110/10]
     via FE80::C802:1FF:FEAE:1D, Ethernet1/1
OI  2406:6400::4/128 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::5/128 [110/11]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::6/128 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::7/128 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::8/128 [110/11]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::9/128 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::10/128 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::11/128 [110/11]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400::12/128 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
```

Route Filtering

- Transport Prefix
  - Prefix size can be /64~/48
  - /48 is preferred if BGP traffic engineering required in future
  - Advertised in IGP i.e. OSPF
  - Scope within IP core network

Route Filtering

Transport prefixes in Training ISP network:

```
Router1#sh ipv6 route
IPv6 Routing Table - default - 51 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, I - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
OI  2406:6400:2::/48 [110/11]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:3::/48 [110/11]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
```

Route Filtering

- Prefixes advertised/originated in IP core network
  - Point-to-point
    - Infrastructure point-to-point
      - Prefix size /64 [/127 on interface configuration according to rfc-6164]
      - Advertised in IGP i.e. OSPF
      - Scope within IP core network
      - Can be summarize in IGP i.e. OSPF if the number of p-to-p prefixes are large within the region
    - Customer side point-to-point
      - Prefix size /64 [/127 on interface configuration according to rfc-6164]
      - Advertise from EGP i.e. iBGP (Not OSPF)
      - Scope within IP core network
      - Summarization in iBGP using network statement and pull up route [Atomic summarization]

Route Filtering

Infrastructure p-to-p prefixes in Training ISP network:

```
Router1#sh ipv6 route
IPv6 Routing Table - default - 51 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

C   2406:6400:E::/64 [0/0]
     via Ethernet1/0, directly connected
O   2406:6400:E:1::/64 [110/20]
     via FE80::C802:1FF:FEAE:1D, Ethernet1/1
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
C   2406:6400:E:2::/64 [0/0]
     via Ethernet1/1, directly connected
OI  2406:6400:E:10::/64 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:11::/64 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:12::/64 [110/31]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:20::/64 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:21::/64 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:22::/64 [110/31]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:30::/64 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:31::/64 [110/21]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
OI  2406:6400:E:32::/64 [110/31]
     via FE80::C801:1FF:FEAE:1C, Ethernet1/0
```

Route Filtering

Customer p-to-p prefixes in Training ISP network:

```
Router1#sh ipv6 route
IPv6 Routing Table - default - 51 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, I - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

S   2406:6400:10::/48 [1/0]
     via Null0, directly connected
B   2406:6400:14::/48 [200/0]
     via 2406:6400::3
B   2406:6400:18::/48 [200/0]
     via 2406:6400::4
B   2406:6400:1C::/48 [200/0]
     via 2406:6400::6
B   2406:6400:20::/48 [200/0]
     via 2406:6400::7
B   2406:6400:24::/48 [200/0]
     via 2406:6400::9
B   2406:6400:28::/48 [200/0]
     via 2406:6400::10
B   2406:6400:2C::/48 [200/0]
     via 2406:6400::12
```

Route Filtering

- Data Centre Prefix
  - Prefix assignment can be /48 or a number of /48 if need more
  - /48 is preferred as it will support specific BGP network advertisement for traffic engineering purpose
  - Usually advertised in iBGP but ISP can prefer to advertise from separate AS using eBGP if DC is multihome, has separate routing policy the IP core and providing public hosting service
  - Scope within IP core network if single home
  - For multihoming case origin AS is different and ISP will allow transit only

Route Filtering

Data center prefixes in Training ISP network:

```
IPv6 Routing Table - default - 51 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, I - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

B   2406:6400:800::/48 [200/0]
    via 2406:6400::2
B   2406:6400:A00::/48 [200/0]
    via 2406:6400::5
B   2406:6400:C00::/48 [200/0]
    via 2406:6400::8
B   2406:6400:E00::/48 [200/0]
    via 2406:6400::11
```

Receiving Prefixes

- There are three scenarios for receiving prefixes from other ASNs
  - Customer talking BGP
  - Peer talking BGP
  - Upstream/Transit talking BGP
- Each has different filtering requirements and need to be considered separately

Receiving Prefixes: From Customers

- ISPs should only accept prefixes which have been assigned or allocated to their downstream customer
- If ISP has assigned address space to its customer, then the customer IS entitled to announce it back to his ISP
- If the ISP has NOT assigned address space to its customer, then:
  - Check in the five RIR databases to see if this address space really has been assigned to the customer. **L**egitimacy of **A**ddress (LoA) check
  - The tool: whois –h jwhois.apnic.net x.x.x.0/24
    - (jwhois queries all RIR database)

Receiving Prefixes: From Customers

- Example use of whois to check if customer is entitled to announce address space:

```
$ whois -h whois.apnic.net 2406:6400::/32

Inet6num:       2406:6400::/32
netname:        APNIC-AP
descr:          Asia Pacific Network Information Centre
descr:          Regional Internet Registry for the Asia-Pacific
descr:          6 Cordelia Street
descr:          South Brisbane, QLD 4101
descr:          Australia
country:        AU
admin-c:        AIC1-AP
tech-c:         NO4-AP
mnt-by:         APNIC-HM
mnt-irt:        IRT-APNIC-AP
changed:        hm-changed@apnic.net
status:         ASSIGNED PORTABLE
changed:        hm-changed@apnic.net 20110309
source:         APNIC
```

Portable – means its an assignment to the customer, the customer can announce it to you

Receiving Prefixes: From Peers

- A peer is an ISP with whom you agree to exchange prefixes you originate into the Internet routing table
  - Prefixes you accept from a peer are only those they have indicated they will announce
  - Prefixes you announce to your peer are only those you have indicated you will announce

Receiving Prefixes: From Peers

- Agreeing what each will announce to the other:
  - Exchange of e-mail documentation as part of the peering agreement, and then ongoing updates

    OR
  - Use of the Internet Routing Registry and configuration tools such as the IRRToolSet

    http://www.isc.org/software/irrtoolset

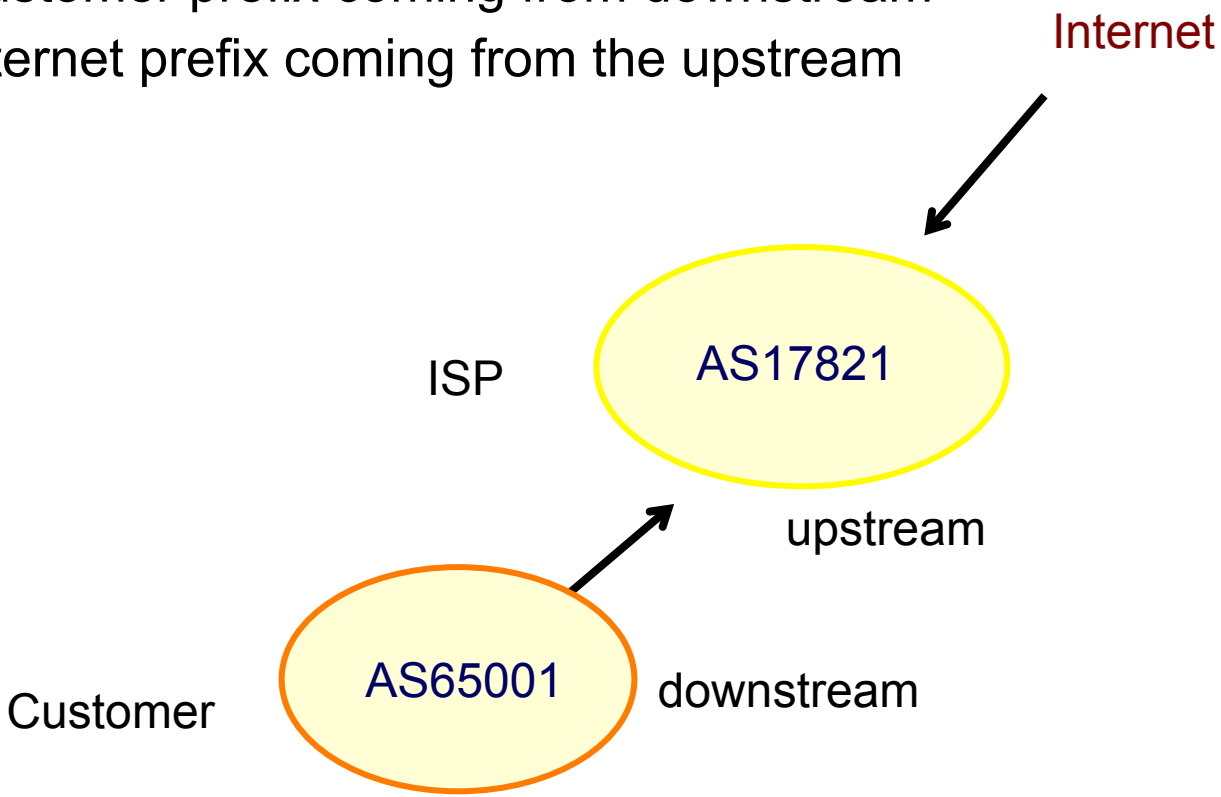
Receiving Prefixes: From Upstream

- Upstream/Transit Provider is an ISP who you pay to give you transit to the WHOLE Internet
- Receiving prefixes from them is not desirable unless really necessary
  - Traffic Engineering – see BGP Multihoming presentations
- Ask upstream/transit provider to either:
  - originate a default-route

    OR
  - announce one prefix you can use as default

Route Filtering Case study

- External Prefixes
  - Customer prefix coming from downstream
  - Internet prefix coming from the upstream



Route Filtering

Downstream customer prefixes in Training ISP network:

```
Router1#sh ipv6 route
IPv6 Routing Table - default - 51 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, I - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

B   2406:6400:8000::/48 [20/0]
     via FE80::C80C:1FF:FEAF:6, FastEthernet0/0
B   2406:6400:9800::/48 [200/0]
     via 2406:6400::3
B   2406:6400:A000::/48 [200/0]
     via 2406:6400::4
B   2406:6400:B800::/48 [200/0]
     via 2406:6400::6
B   2406:6400:C000::/48 [200/0]
     via 2406:6400::7
B   2406:6400:D800::/48 [200/0]
     via 2406:6400::9
B   2406:6400:E000::/48 [200/0]
     via 2406:6400::10
B   2406:6400:F800::/48 [200/0]
     via 2406:6400::12
```

Route Filtering

Upstream Internet prefixes in Training ISP network:

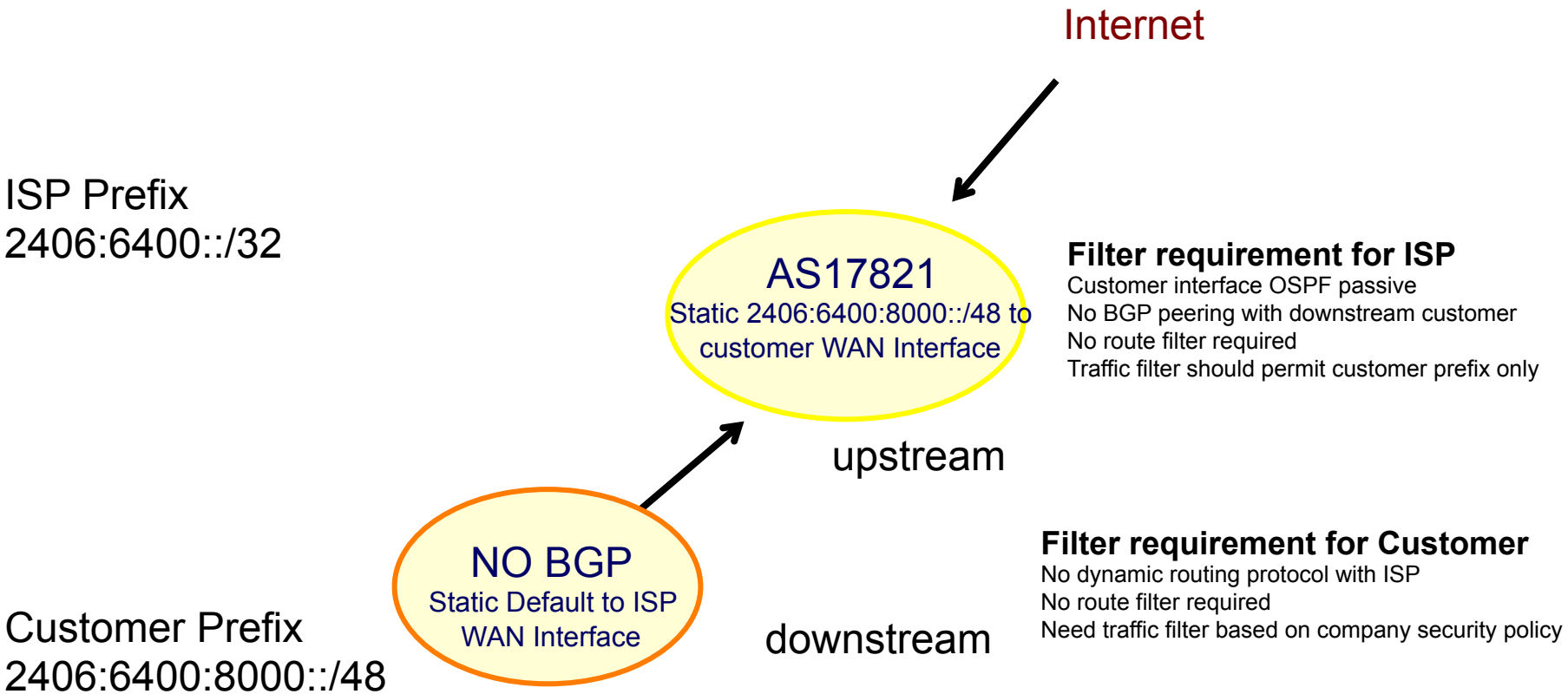
```
Router1#sh ipv6 route
IPv6 Routing Table - default - 51 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery, I - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

B   2406:6400:8000::/48 [20/0]
     via FE80::C80C:1FF:FEAF:6, FastEthernet0/0
B   2406:6400:9800::/48 [200/0]
     via 2406:6400::3
B   2406:6400:A000::/48 [200/0]
     via 2406:6400::4
B   2406:6400:B800::/48 [200/0]
     via 2406:6400::6
B   2406:6400:C000::/48 [200/0]
     via 2406:6400::7
B   2406:6400:D800::/48 [200/0]
     via 2406:6400::9
B   2406:6400:E000::/48 [200/0]
     via 2406:6400::10
B   2406:6400:F800::/48 [200/0]
     via 2406:6400::12
```

Route Filtering

- Customer prefix coming from downstream:
  - Option 1: Customer single home and non portable prefix
    - Customer is not APNIC member prefix received from upstream ISP
  - Option 2: Customer single home and portable prefix
    - Customer is APNIC member receive allocation as service provider but no AS number yet
  - Option 3: Customer multihome and non portable prefix
    - Customer is not APNIC member both prefix and ASN received from upstream ISP
  - Option 4: Customer multihome and portable prefix
    - Customer is APNIC member both prefix and ASN received from APNIC

Route Filtering

- Option 1: Customer single home and non portable prefix

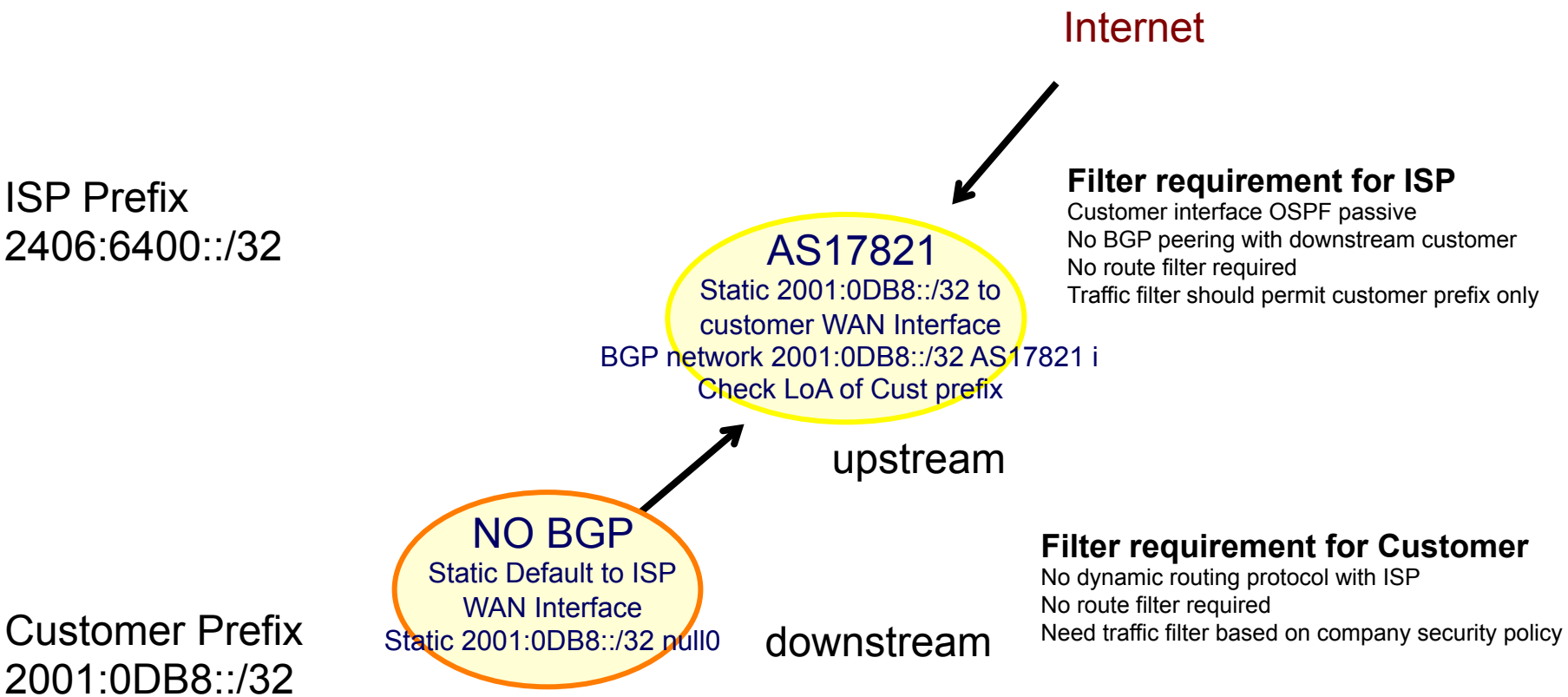


Filter requirement for ISP
Customer interface OSPF passive
No BGP peering with downstream customer
No route filter required
Traffic filter should permit customer prefix only

Filter requirement for Customer
No dynamic routing protocol with ISP
No route filter required
Need traffic filter based on company security policy

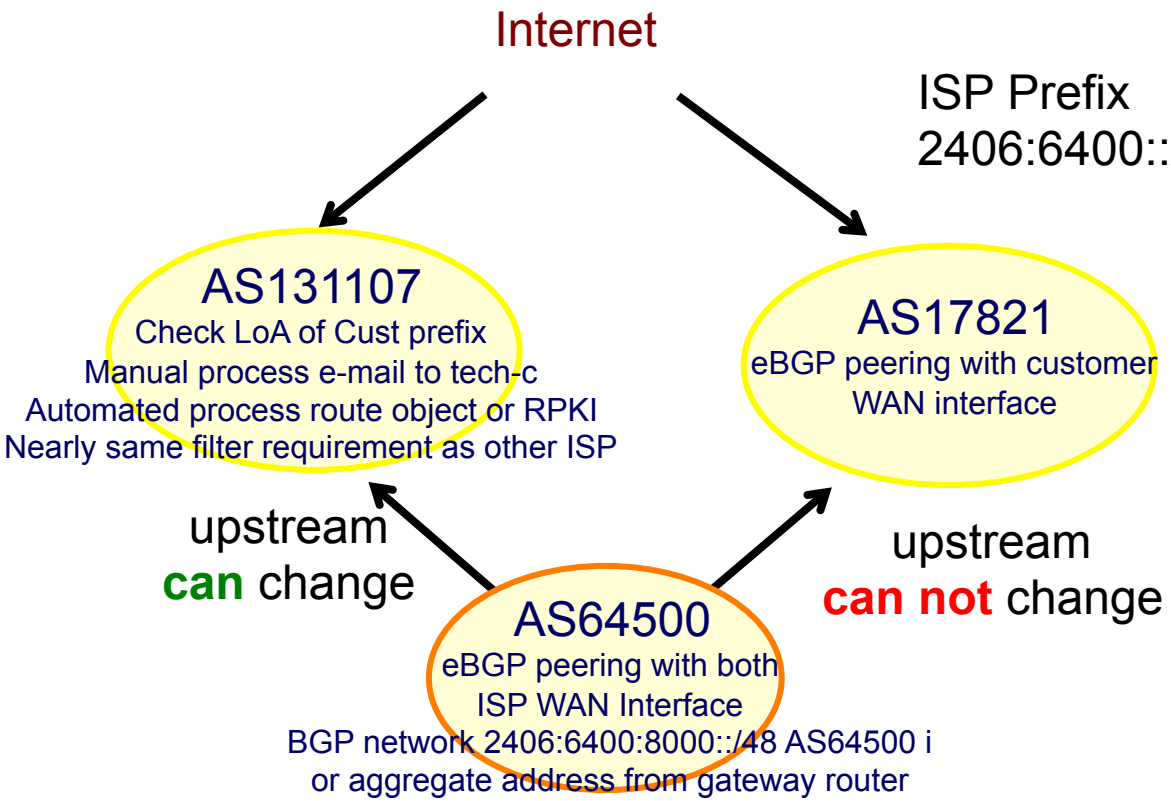
Route Filtering

- Option 2: : Customer single home and portable prefix



Route Filtering

- Option 3: Customer multihome and non portable prefix



Filter requirement for ISP

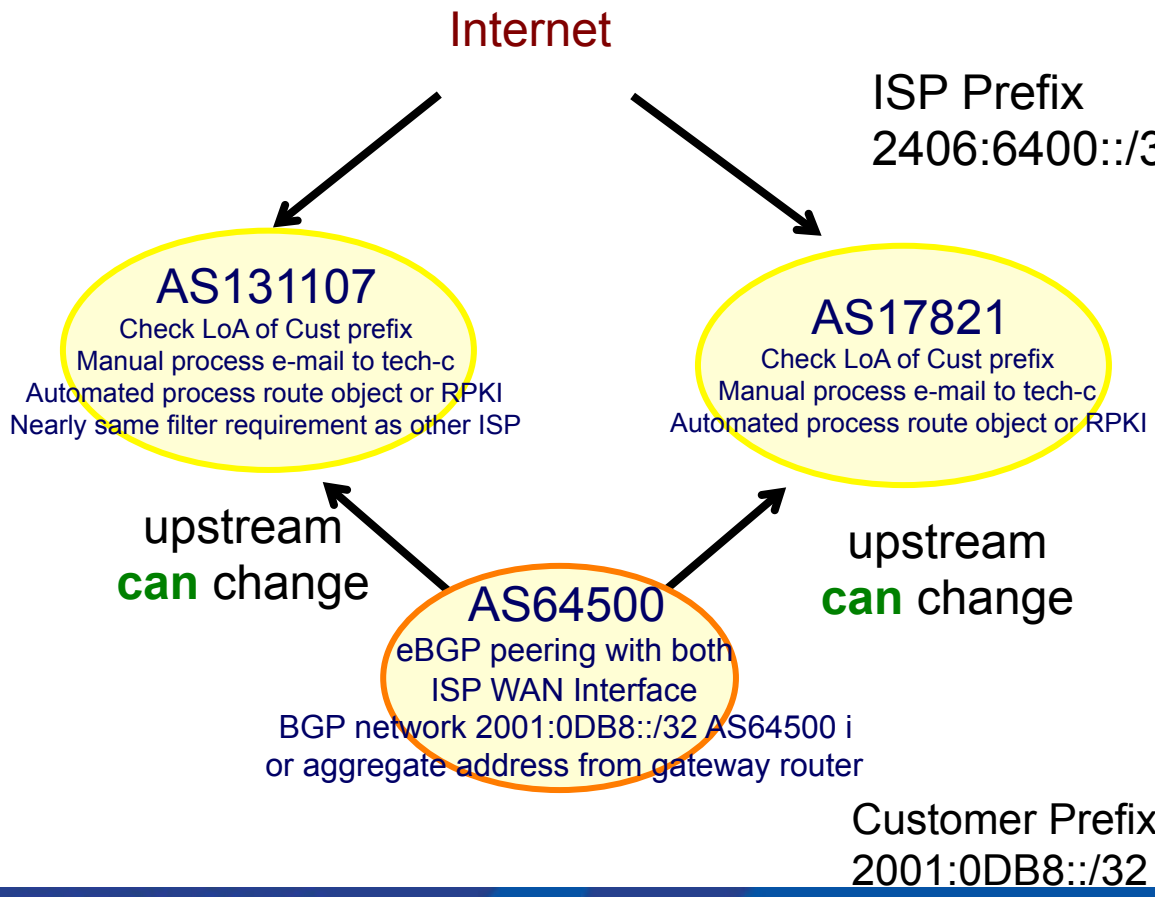
Customer interface OSPF passive
BGP peering with downstream customer
Route filter permit 2406:6400:8000::/48 only in
Route filter permit ::/0, AS17821cust, all /48& /32 out
Or route filter permit ::/0 & AS17821 only out
AS path filter permit _64500$ in
Traffic filter should permit customer prefix in

Filter requirement for Customer

BGP peering with both upstream ISP
Route filter permit 2406:6400:8000::/48 only out
Route filter permit ::/0, AS17821cust, all /48& /32 in
Or route filter permit ::/0 & AS17821 only in
AS path filter permit ^$ out
Need traffic filter based on company security policy

Route Filtering

- Option 4: Customer multihome and portable prefix



Filter requirement for ISP

Customer interface OSPF passive
BGP peering with downstream customer
Route filter permit 2001:0DB8::/32 only in
Route filter permit ::/0, AS17821cust, all /48& /32 out
Or route filter permit ::/0 & AS17821 only out
AS path filter permit _64500$ in
Traffic filter should permit customer prefix in

Filter requirement for Customer

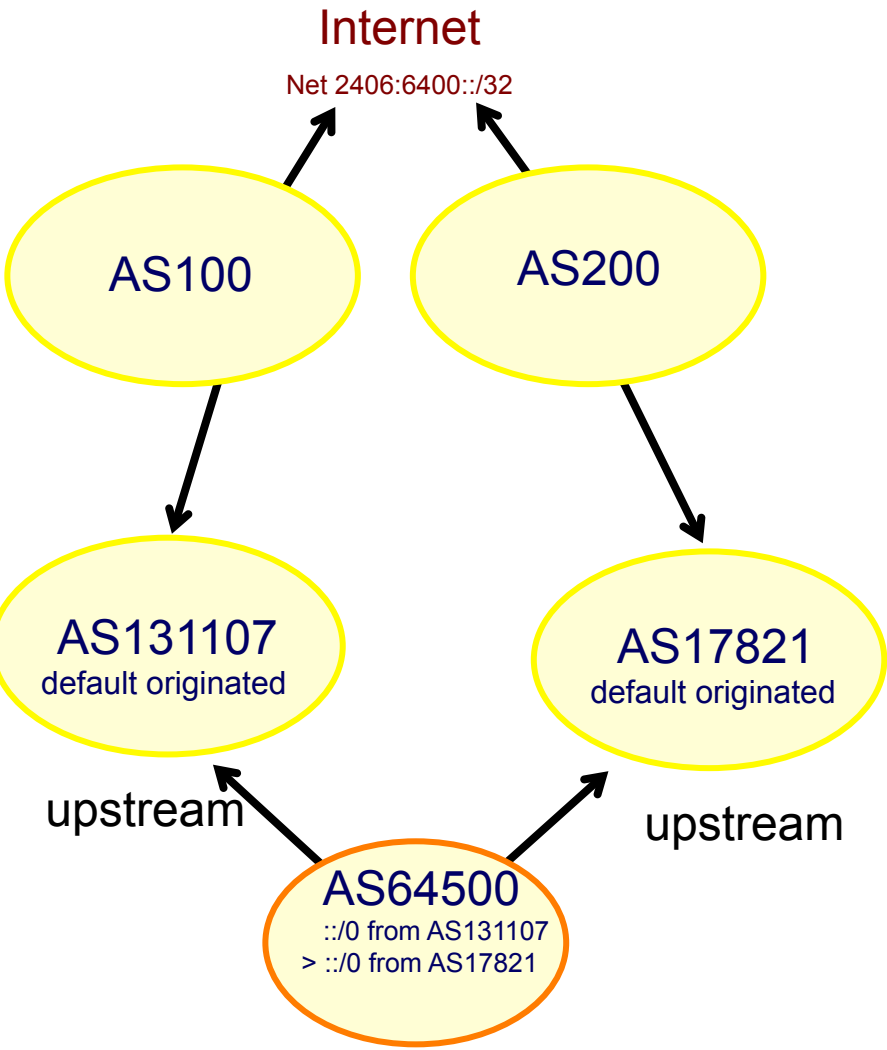
BGP peering with both upstream ISP
Route filter permit 2001:0DB8::/32 only out
Route filter permit ::/0, AS17821cust, all /48& /32 in
Or route filter permit ::/0 & AS17821 only in
AS path filter permit ^$ out
Need traffic filter based on company security policy

Route Filtering

- Downstream Customer BGP In process design issue:
  - Option 1: ISP default only In
    - Customer is accepting ::/0 only from upstream ISP prefix
  - Option 2: ISP default + local In
    - Customer is accepting ::/0 and upstream ISP prefix and their other customer portable prefixes **(Non portable prefixes should not)**
  - Option 3: ISP default + local + all In
    - Customer is accepting ::/0, upstream ISP aggregated prefix and their other customer portable prefixes **(Non portable prefixes should not)** and all other from Internet

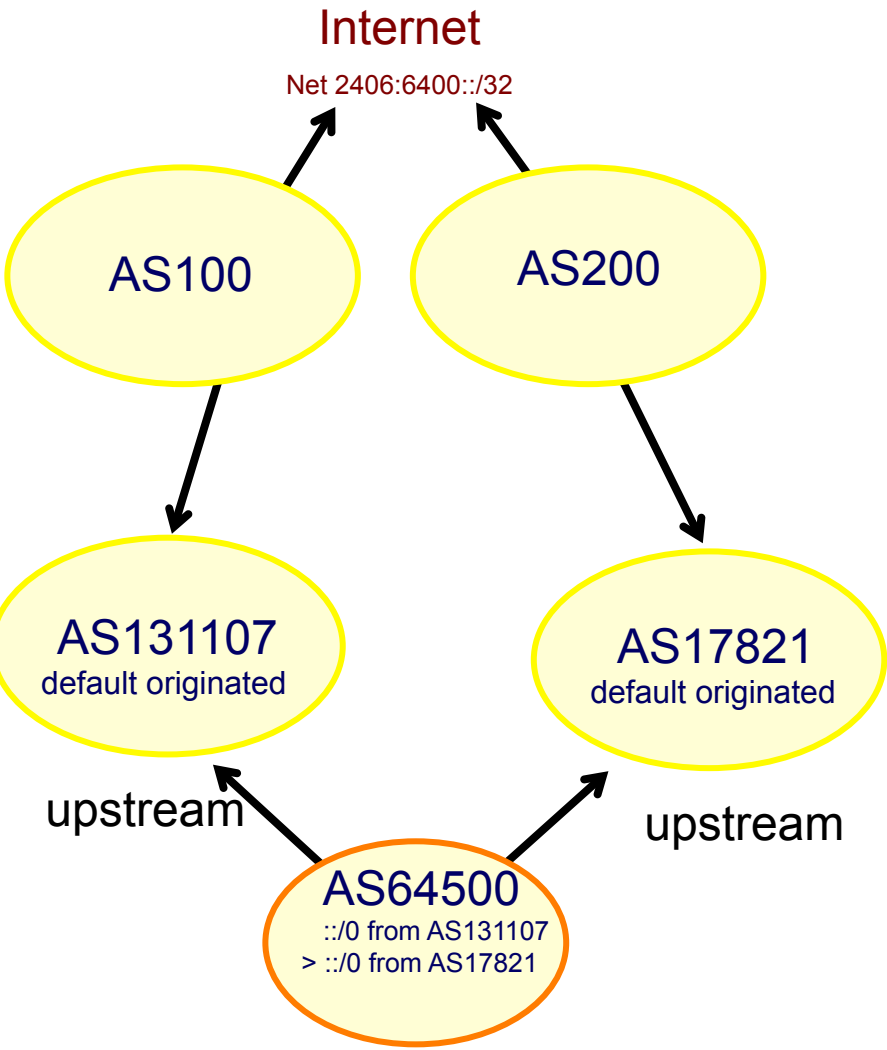
Route Filtering

- Option 1: ISP default only In
  - Can use a low configuration router (CPU/DRAM)



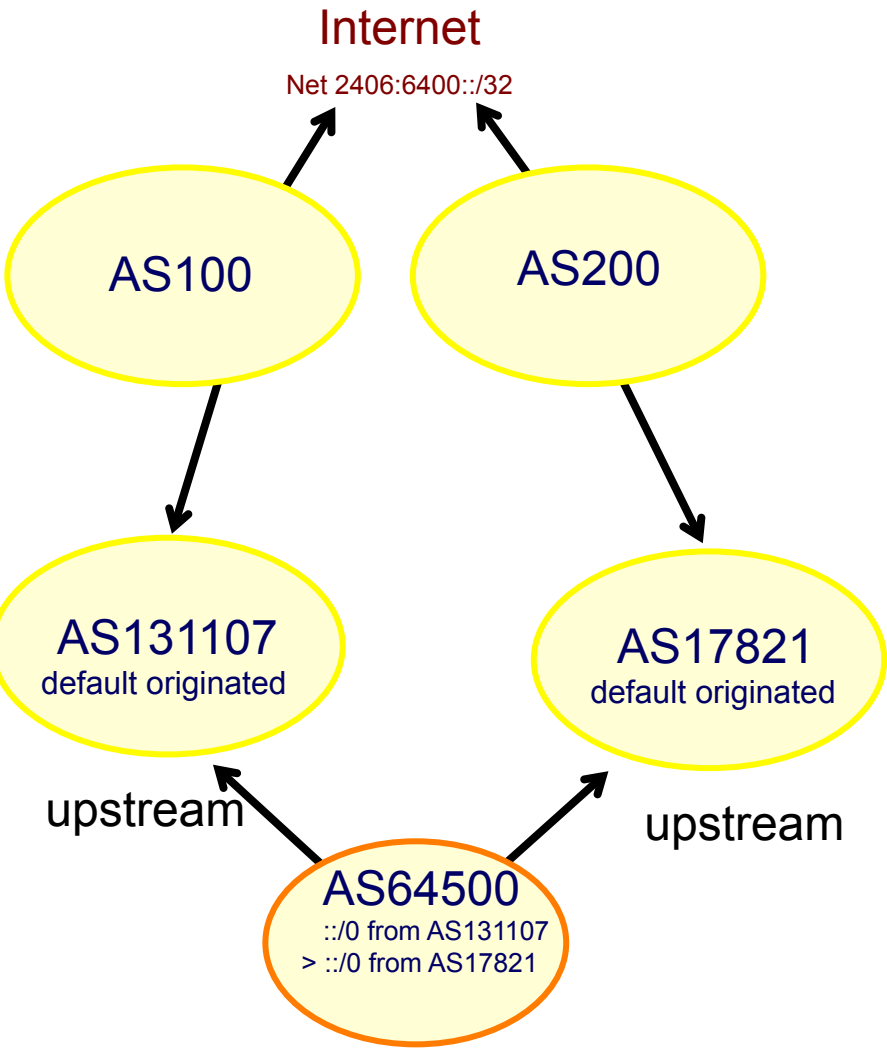
Route Filtering

- Option 1: ISP default only In
  - Can use a low configuration router (CPU/DRAM)
  - Easy to manage small routing table



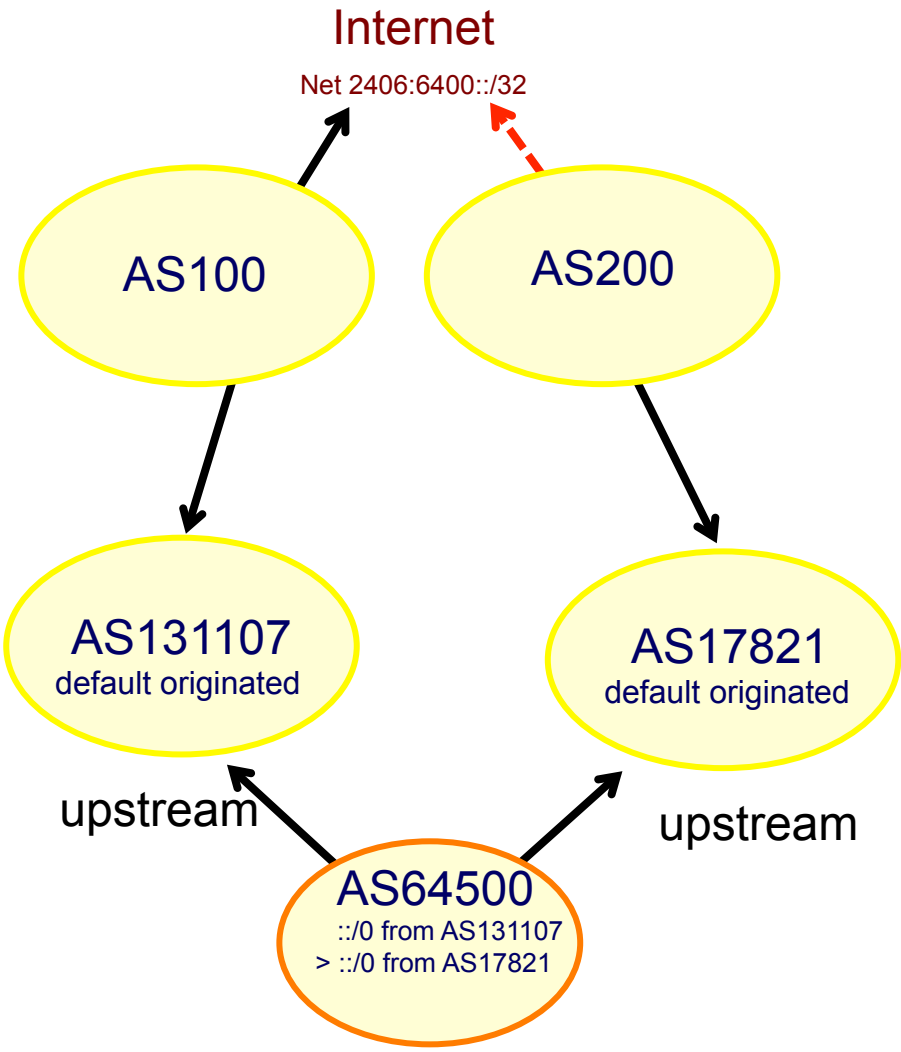
Route Filtering

- Option 1: ISP default only In
  - Can use a low configuration router (CPU/DRAM)
  - Easy to manage small routing table
  - Do not support destination specific traffic engineering



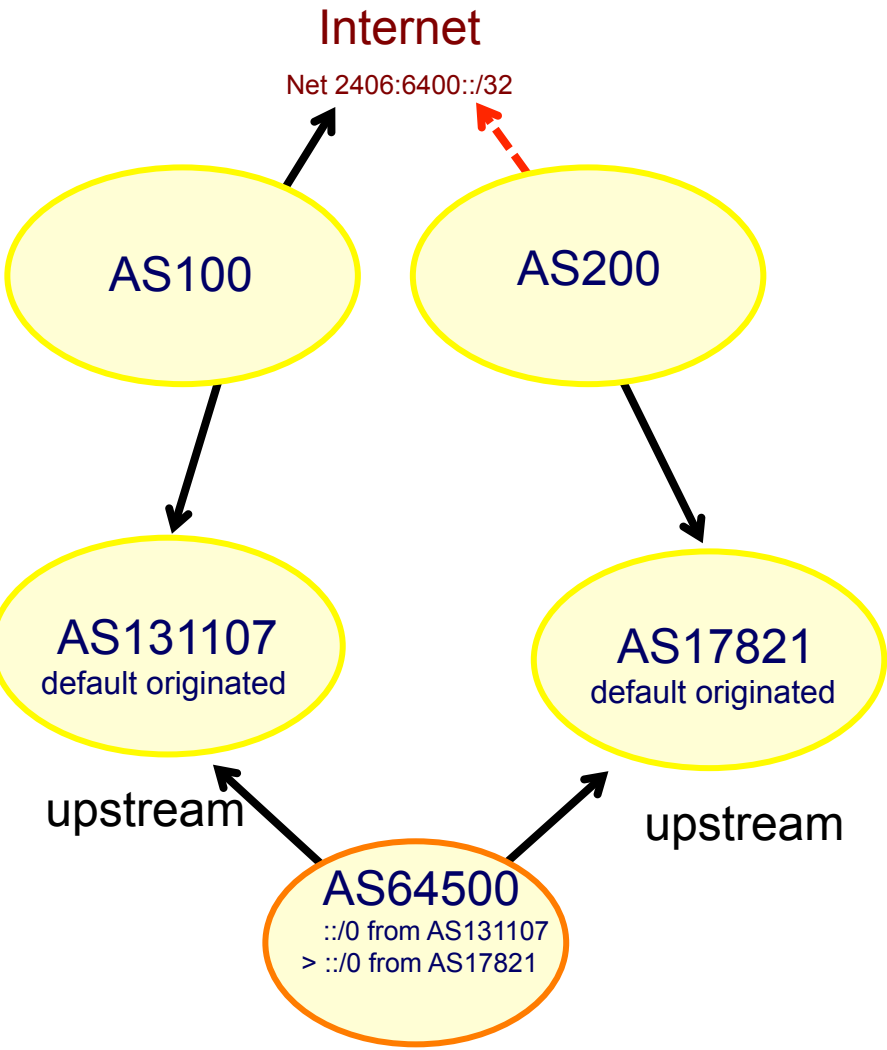
Route Filtering

- Option 1: ISP default only In
  - Can use a low configuration router (CPU/DRAM)
  - Easy to manage small routing table
  - Do not support destination specific traffic engineering
  - Can not re-route traffic if remote transit is down



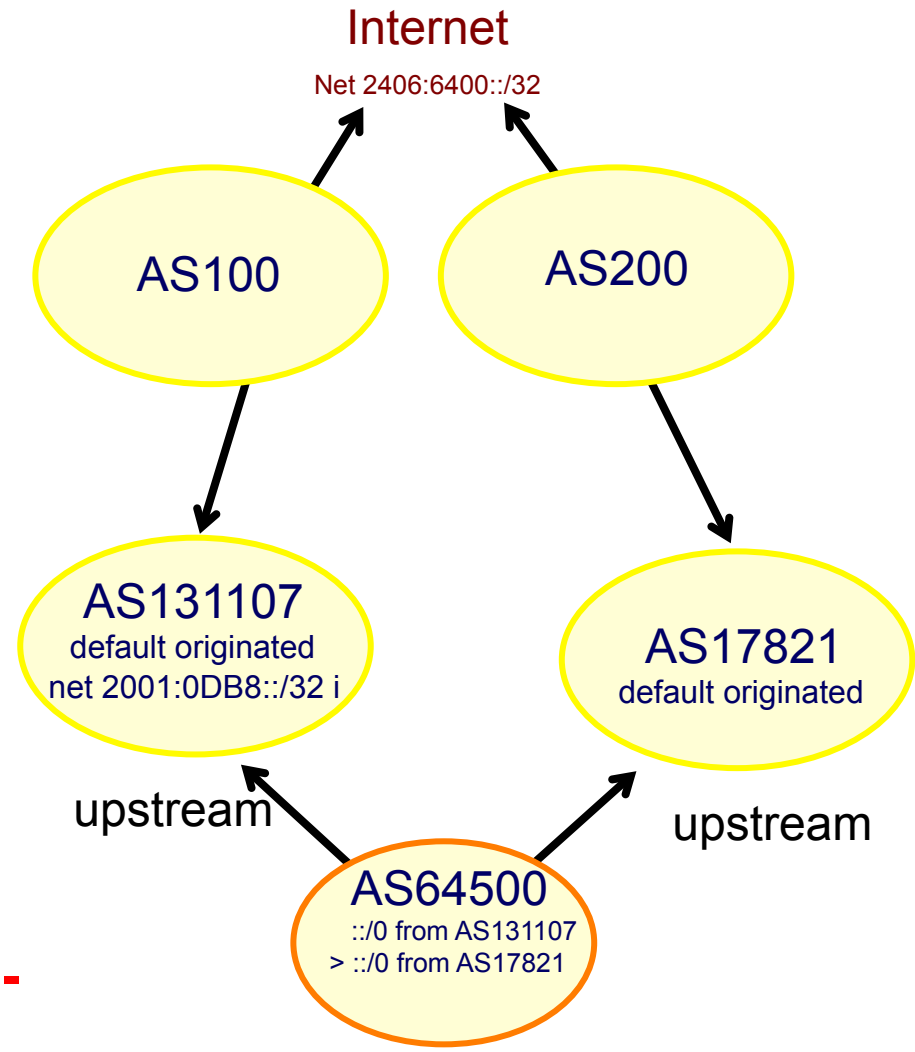
Route Filtering

- Option 1: ISP default only In
  - Can use a low configuration router (CPU/DRAM)
  - Easy to manage small routing table
  - Do not support destination specific traffic engineering
  - Can not re-route traffic if remote transit is down
  - I.e. Network 2406:6400::/32 is withdrawn in AS200 but default path in AS64500 is still sending traffic via AS 17821)



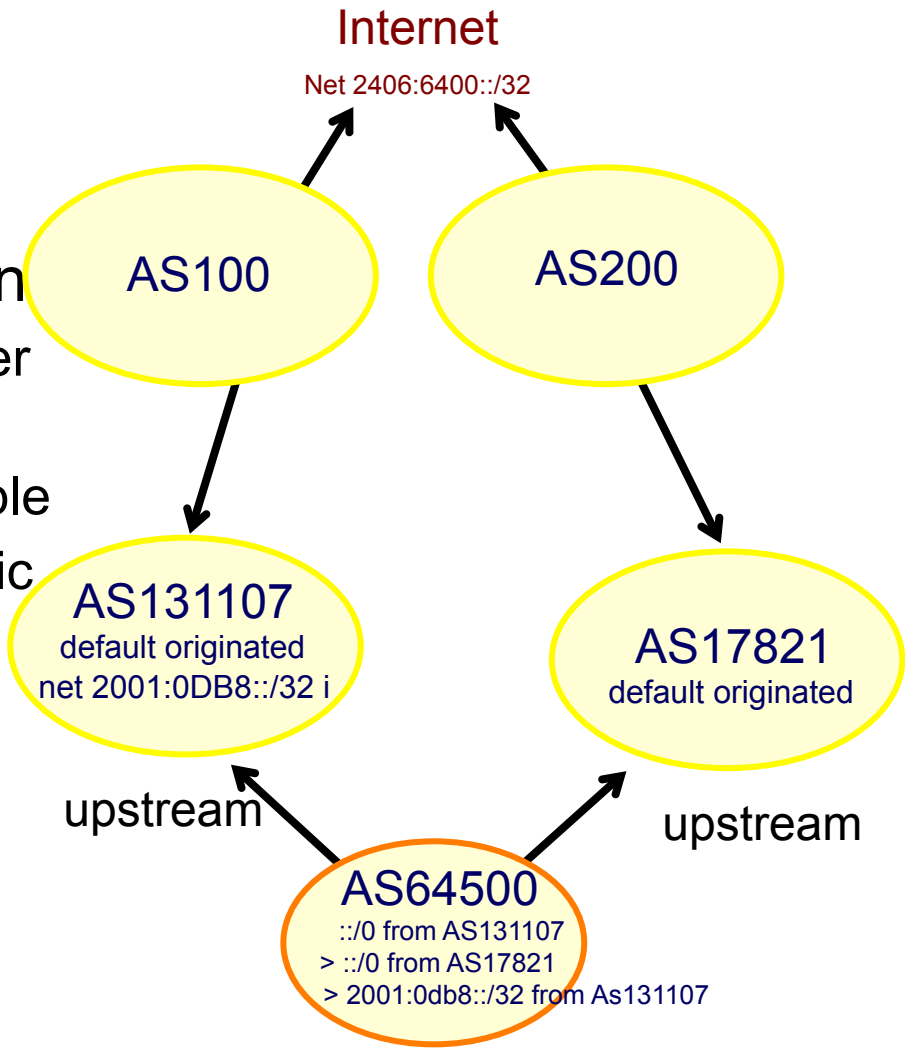
Route Filtering

- Option 1: ISP default only In
  - Can use a low configuration router (CPU/DRAM)
  - Easy to manage small routing table
  - Do not support destination specific traffic engineering
  - Can not re-route traffic if remote transit is down
  - Prefixes originated in AS131107 can be routed via AS17821 **(Sub-optimal path)**



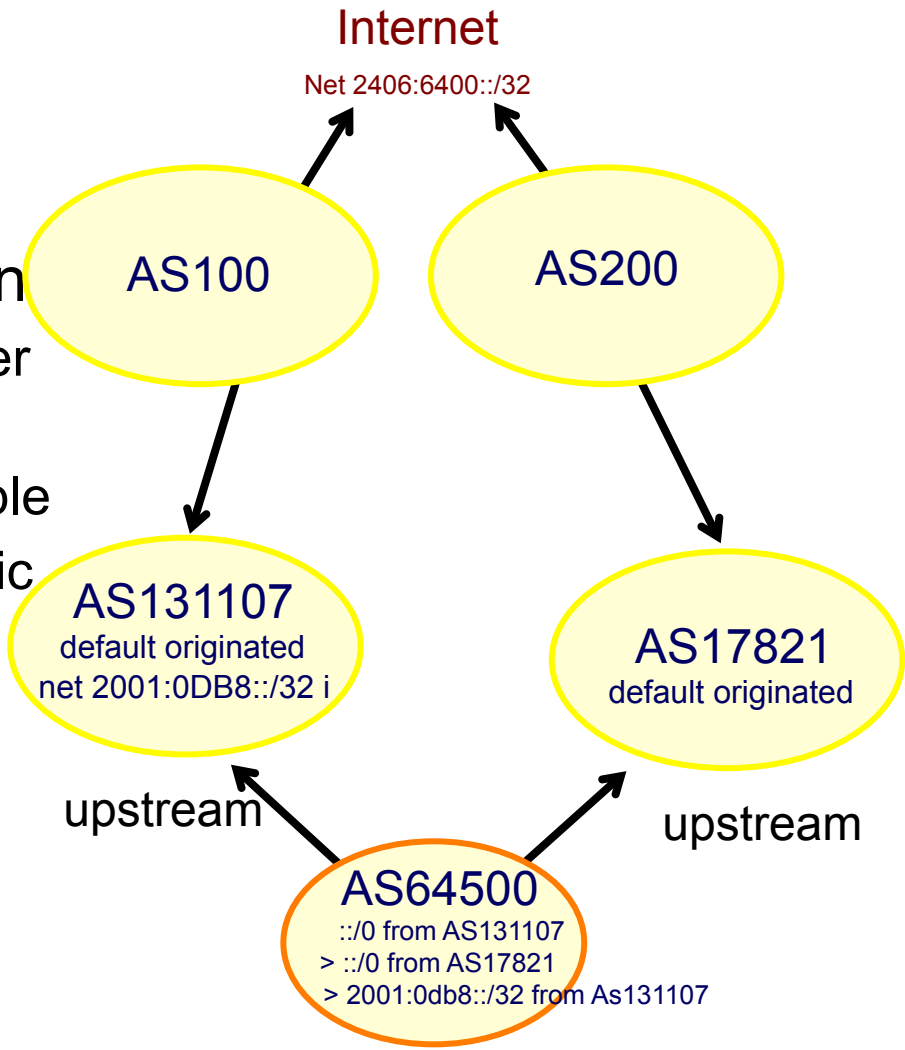
Route Filtering

- Option 2: ISP default + local In
  - Can use a low configuration router (CPU/DRAM)
  - Easy to manage small routing table
  - Do not support destination specific traffic engineering to the remote
  - Can not re-route traffic if remote transit is down
  - AS131107 is sending its portable local route to AS64500



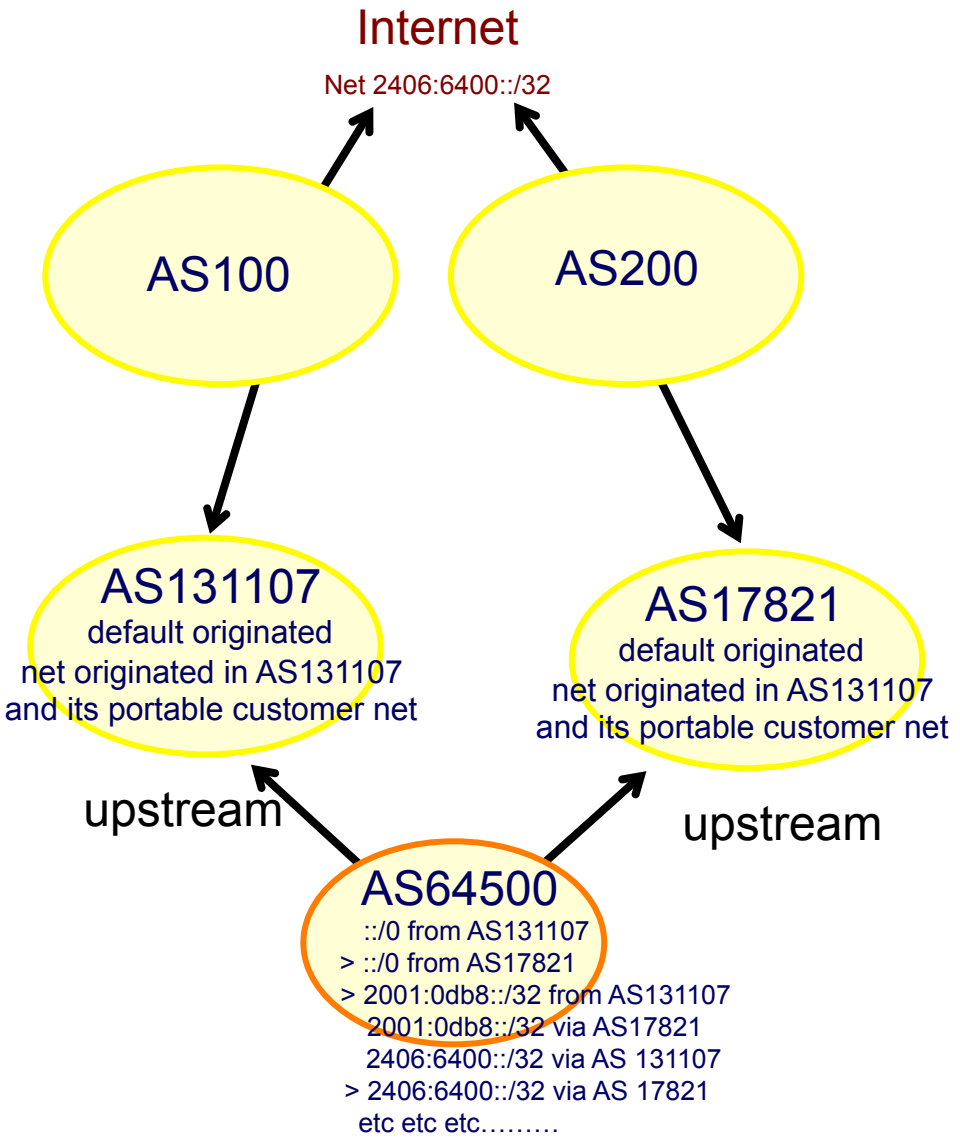
Route Filtering

- Option 2: ISP default + local In
  - Can use a low configuration router (CPU/DRAM)
  - Easy to manage small routing table
  - Do not support destination specific traffic engineering to the remote
  - Can not re-route traffic if remote transit is down
  - AS131107 is sending its portable local route to AS64500
  - Prefixes originated in AS131107 can now be routed via AS131107 **(Optimal Path)**



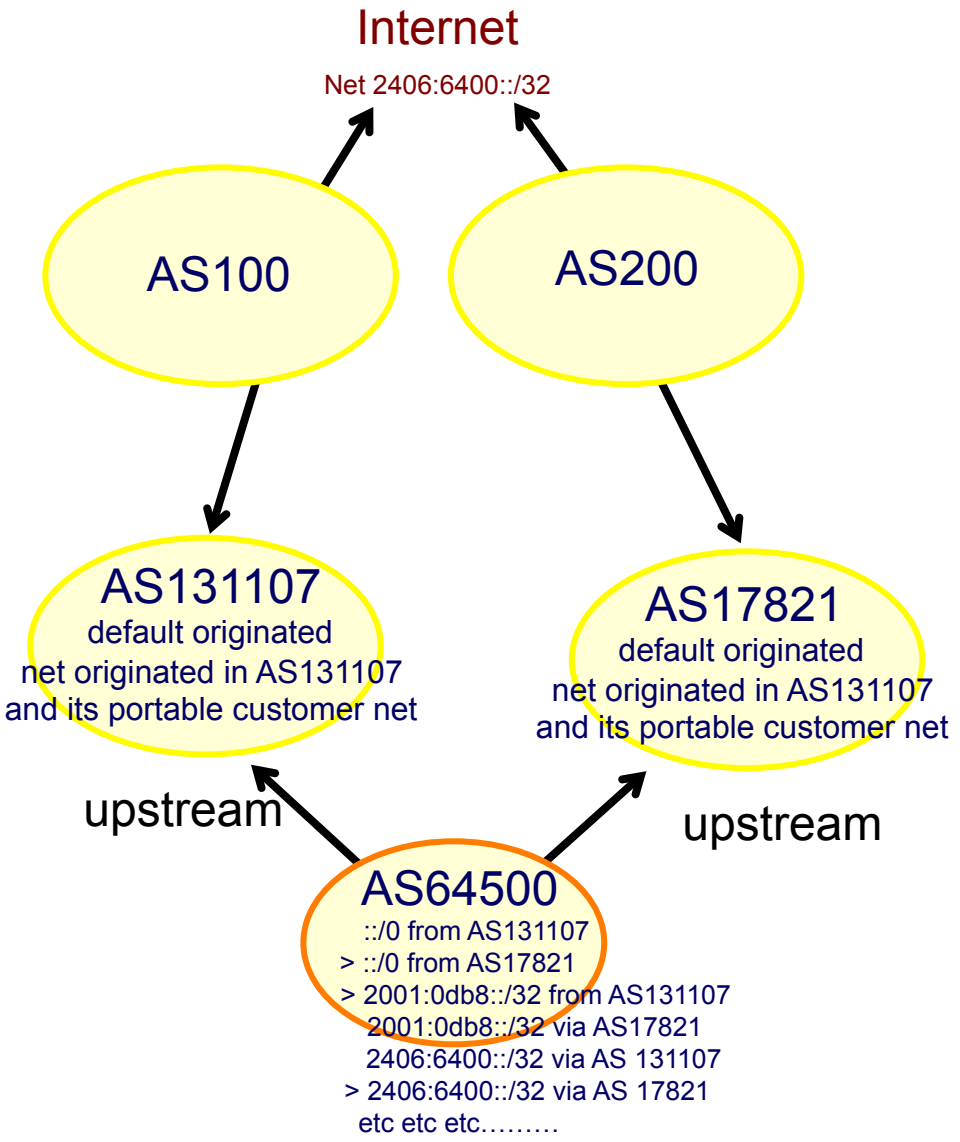
Route Filtering

- Option 3: ISP default + local + all In
  - Need high configuration router (CPU/DRAM)



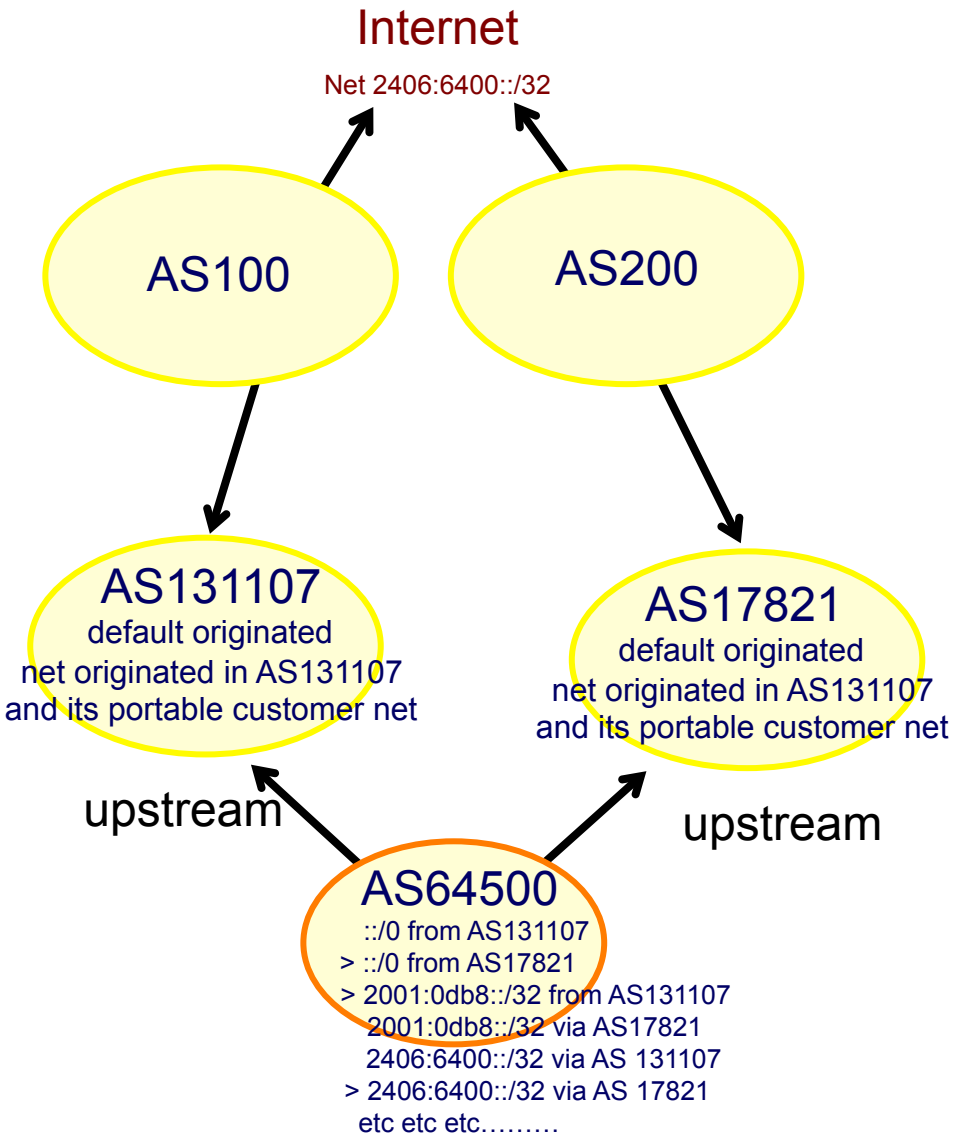
Route Filtering

- Option 3: ISP default + local + all In
  - Need high configuration router (CPU/DRAM)
  - Need skilled people to manage large routing table



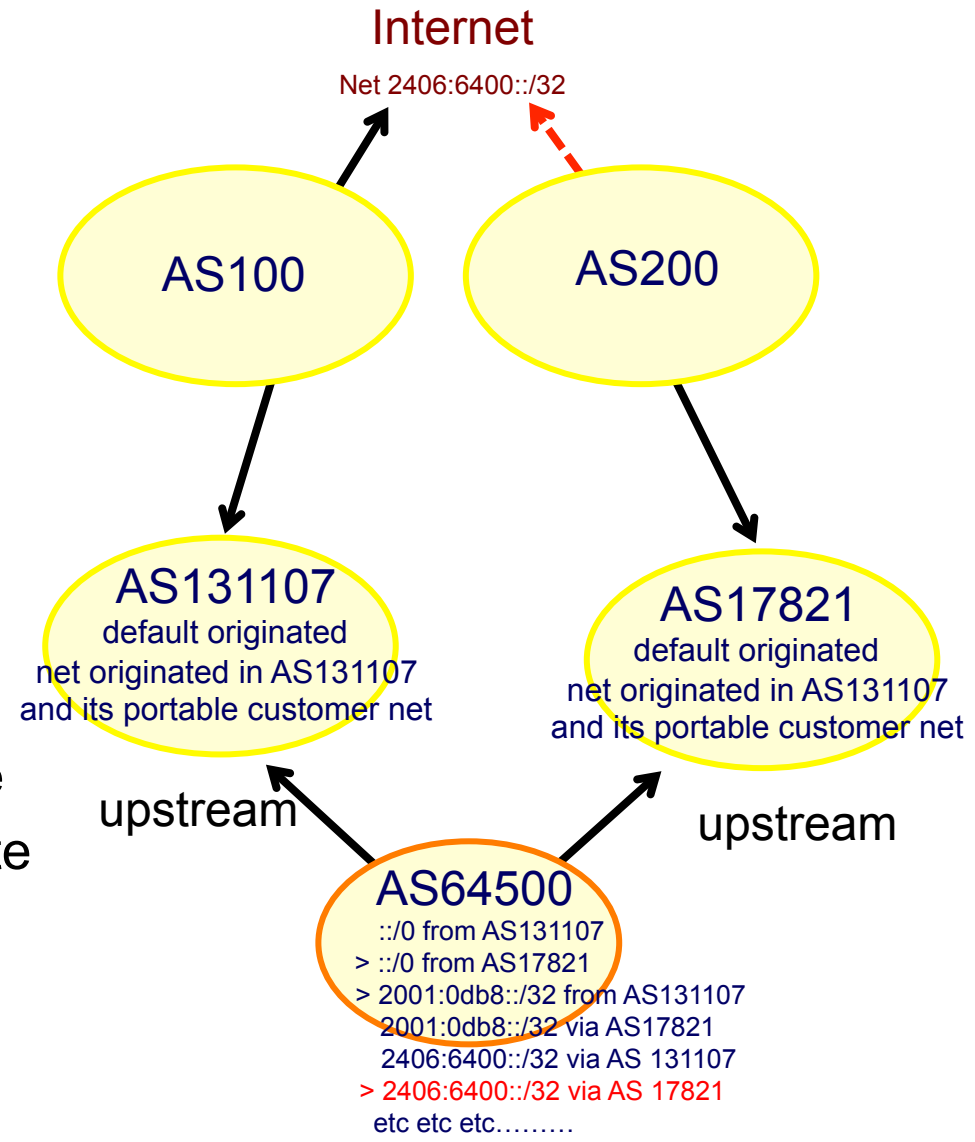
Route Filtering

- Option 3: ISP default + local + all In
  - Need high configuration router (CPU/DRAM)
  - Need skilled people to manage large routing table
  - Support destination specific traffic engineering to the remote



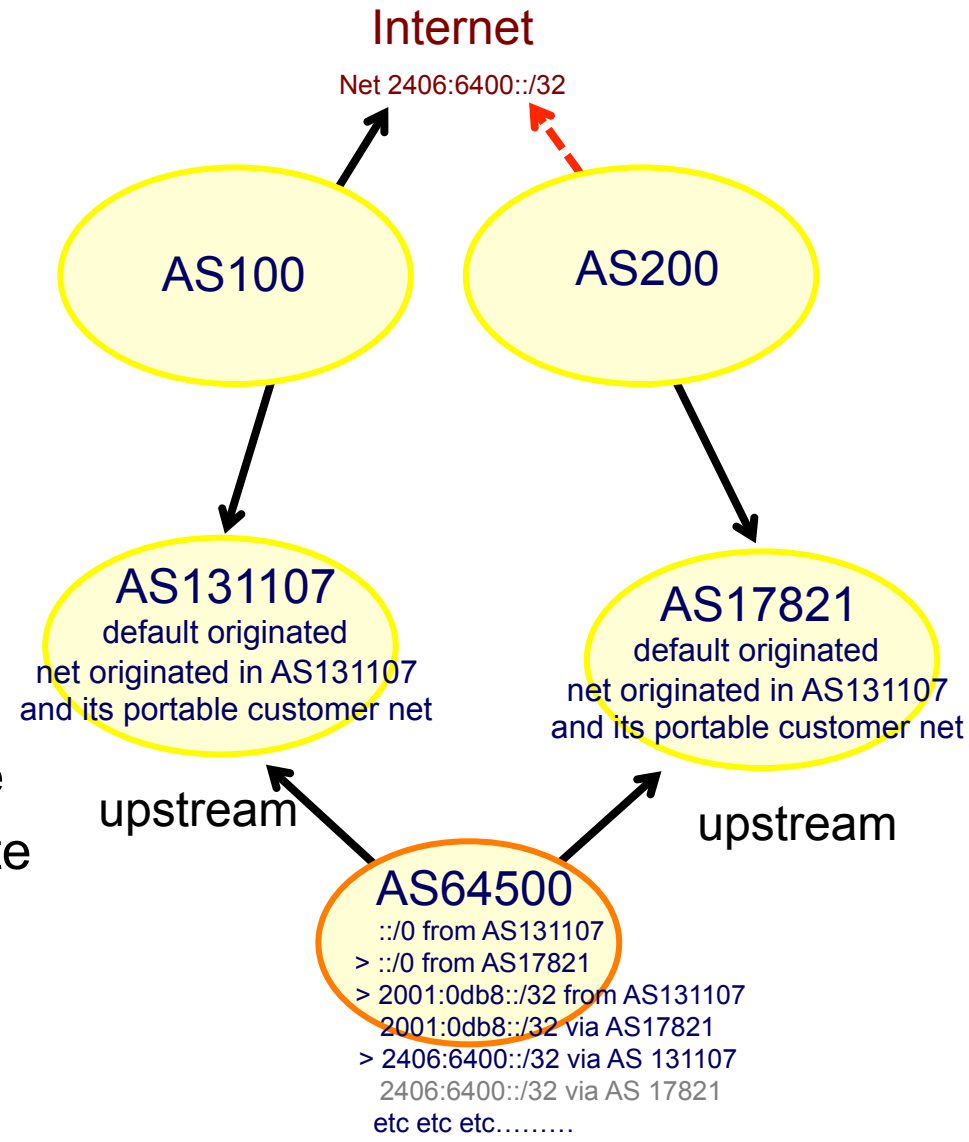
Route Filtering

- Option 3: ISP default + local + all In
  - Need high configuration router (CPU/DRAM)
  - Need skilled people to manage large routing table
  - Support destination specific traffic engineering to the remote
  - Can now re-route traffic if remote transit is down



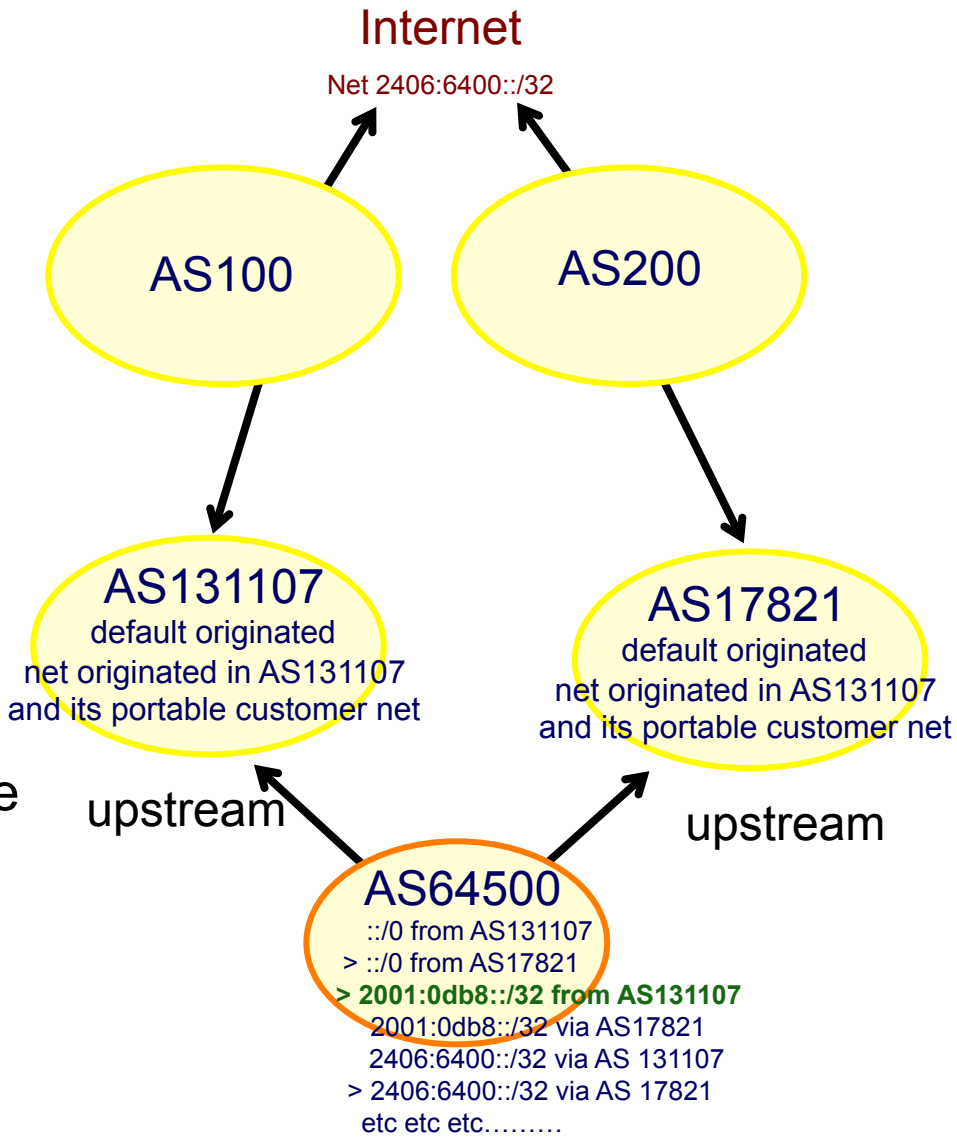
Route Filtering

- Option 3: ISP default + local + all In
  - Need high configuration router (CPU/DRAM)
  - Need skilled people to manage large routing table
  - Support destination specific traffic engineering to the remote
  - Can now re-route traffic if remote transit is down



Route Filtering

- Option 3: ISP default + local + all In
  - Need high configuration router (CPU/DRAM)
  - Need skilled people to manage large routing table
  - Support destination specific traffic engineering to the remote
  - Can now re-route traffic if remote transit is down
  - Prefixes originated in AS131107 or AS17821 can now be routed via AS131107 or AS17821 respectively



Route Filtering BCP

- **Prefixes: From Upstream/Transit Provider**
- If necessary to receive prefixes from any provider, care is required.
  - Don't accept default (unless you need it)
  - Don't accept your own prefixes
- For IPv4:
  - Don't accept private (RFC1918) and certain special use prefixes:
    http://www.rfc-editor.org/rfc/rfc5735.txt
  - Don't accept prefixes longer than /24 (?)
- For IPv6:
  - Don't accept certain special use prefixes:
    http://www.rfc-editor.org/rfc/rfc5156.txt
  - Don't accept prefixes longer than /48 (?)

Route Filtering BCP

- **Prefixes: From Upstream/Transit Provider**
- Check Team Cymru's list of "bogons"

  www.team-cymru.org/Services/Bogons/http.html
- For IPv4 also consult:

  datatracker.ietf.org/doc/draft-vegoda-no-more-unallocated-slash8s
- For IPv6 also consult:

  www.space.net/~gert/RIPE/ipv6-filters.html
- Bogon Route Server:

  www.team-cymru.org/Services/Bogons/routeserver.html
  - Supplies a BGP feed (IPv4 and/or IPv6) of address blocks which should not appear in the BGP table

Route Filtering Plan in Training Lab

- We will use option 3: Config on ISP Edge router (In)
  - Receive individual customer prefix
  - i.e. On R1 From R13 2406:6400:8000::/48
    On R3 From R14 2406:6400:9800::/48
    On R4 From R15 2406:6400:a000::/48
    On R6 From R16 2406:6400:b800::/48
    On R7 From R17 2406:6400:c000::/48
    On R9 From R18 2406:6400:d800::/48
    On R10 From R19 2406:6400:e000::/48
    On R11 From R20 2406:6400:f800::/48
  - And prefix originated by customer AS

Route Filtering Plan in Training Lab

- We will use option 3: Config on ISP Edge router (Out)
  - Send default prefix to customer i.e. ::/0
  - Send aggregated ISP prefix i.e. 2406:6400::/32
  - Send all individual customer prefix i.e. 2406:6400:8000::/48
    2406:6400:9800::/48
    2406:6400:a000::/48
    2406:6400:b800::/48
    2406:6400:c000::/48
    2406:6400:d800::/48
    2406:6400:e000::/48
    2406:6400:f800::/48
  - Send all Internet prefix with prefix length >/32, /32 and /48 only

Route Filtering Plan in Training Lab

- We will use option 3: Config on CPE router (IN)
  - Receive default prefix to customer i.e. ::/0
  - Receive aggregated ISP prefix i.e. 2406:6400::/32
  - Receive all individual cust prefix i.e. 2406:6400:8000::/48
    2406:6400:9800::/48
    2406:6400:a000::/48
    2406:6400:b800::/48
    2406:6400:c000::/48
    2406:6400:d800::/48
    2406:6400:e000::/48
    2406:6400:f800::/48
  - Receive all Internet prefix with prefix length >/32, /32 and /48 only

Route Filtering Plan in Training Lab

- We will use option 3: Config on CPE router (Out)
  - Send individual customer prefix only
  - i.e.

From R13	To	R1	2406:6400:8000::/48
From R14	To	R3	2406:6400:9800::/48
From R15	To	R4	2406:6400:a000::/48
From R16	To	R6	2406:6400:b800::/48
From R17	To	R7	2406:6400:c000::/48
From R18	To	R9	2406:6400:d800::/48
From R19	To	R10	2406:6400:e000::/48
From R20	To	R12	2406:6400:f800::/48

  - Send that prefix originated customer AS number

Questions?

Thank you!

End of Workshop

APNIC