Network-Based Security ISP Current Practices

APNIC22 - Kaohsiung, Taiwan

Merike Kaeo

merike@doubleshotsecurity.com

Author: Designing Network Security

(ISBN# 1587051176)

Agenda

- What Is The Security Problem
- Security Practices in Large ISPs
  - What they do and why
- Configuration Examples

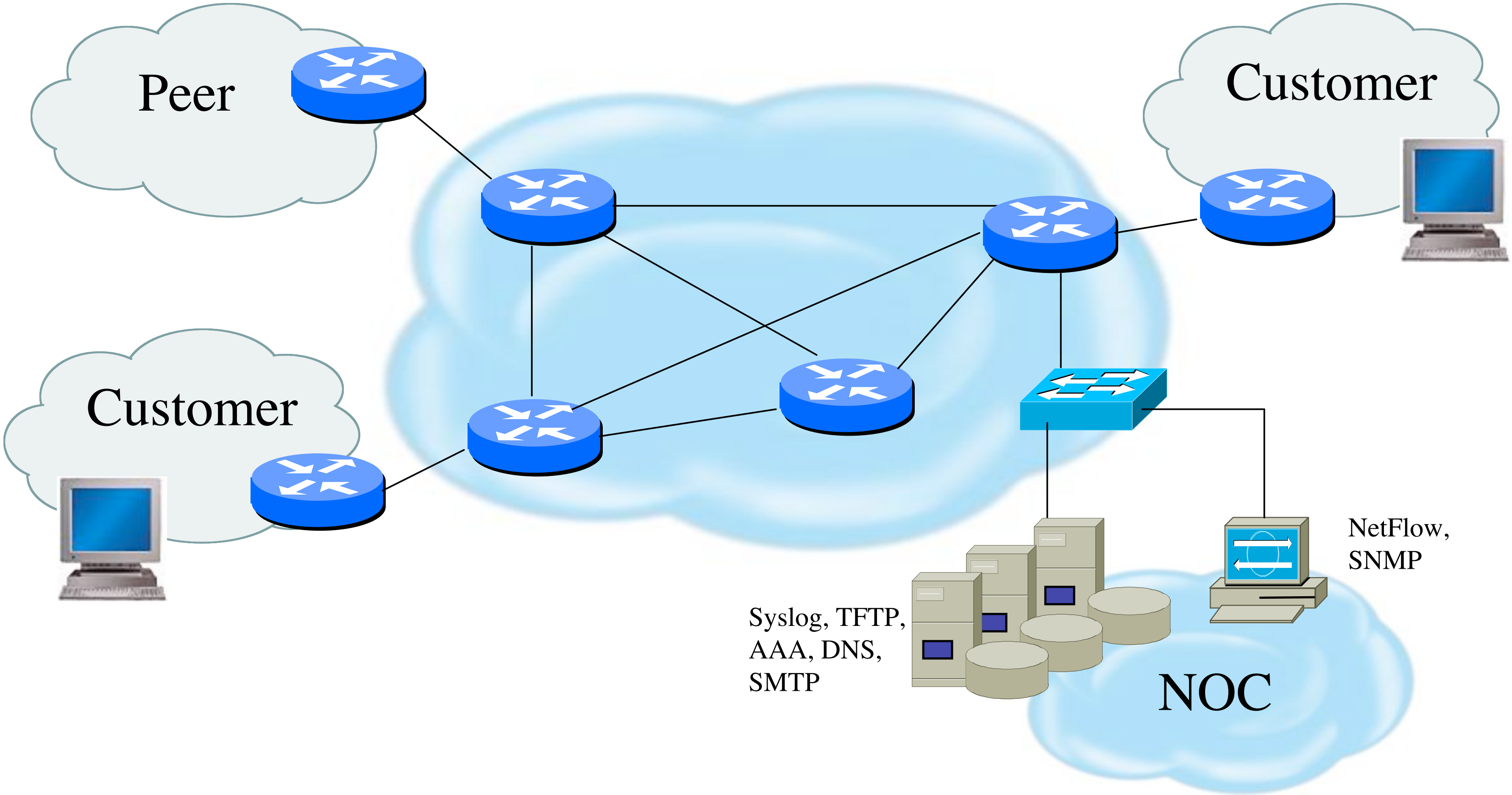
What Are Security Goals?

- Controlling Data / Network Access
- Preventing Intrusions
- Responding to Incidences
- Ensuring Network Availability
- Protecting information in Transit

First Step…..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 can you protect your site?

Infrastructure Security



How Do Large ISPs Protect Their Infrastructures ?

- Understand the Problem
- Establish an Effective Security Policy
  - physical security
  - logical security
  - control/management plane
  - routing plane
  - data plane
- Procedures For Incident Response
  - assessing software vulnerability risk
  - auditing configuration modifications

Risk Mitigation vs Cost of Security

Risk mitigation: the process of selecting appropriate controls to reduce risk to an acceptable level.

The ***level of acceptable risk*** is determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy.

Assess the cost of certain losses and do not spend more to protect something than it is actually worth.

Definitions (rfc 2828)

Threat: A threat is a potential for a security violation, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

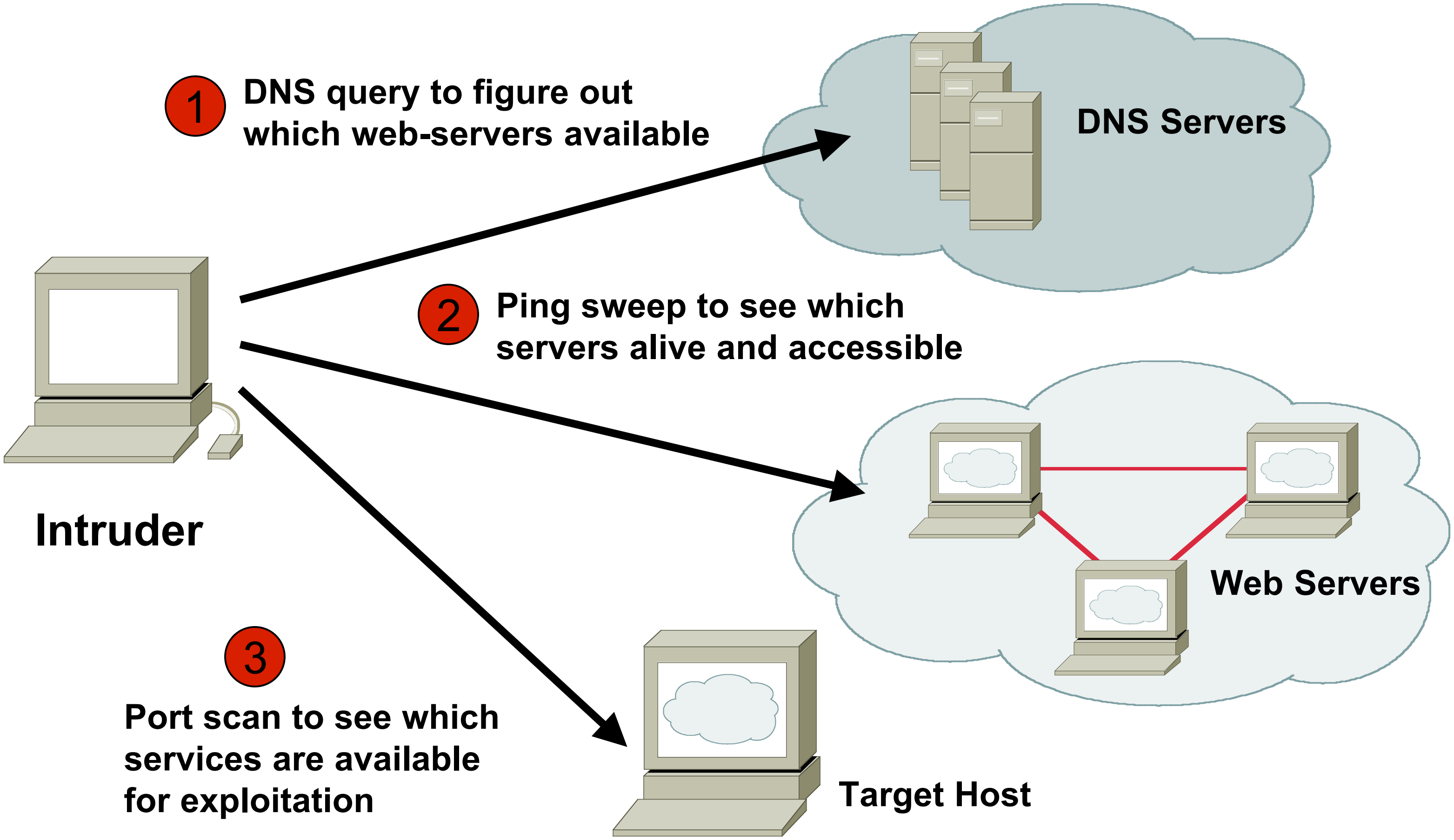
Threat Action (attack): an assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system

Threat Consequence: The threat consequences are the security violations which results from a threat action, i.e. an attack.

Attack Sources

- Passive vs Active
  - Writing and/or reading data on the network
- On-Path vs Off-Path
  - How easy is it to subvert network topology?
- Insider or Outsider
  - What is definition of perimeter?
- Deliberate Attack vs Unintentional Event
  - Configuration errors and software bugs are as harmful as a deliberate malicious network attack

Example Active Reconnaissance Attempt

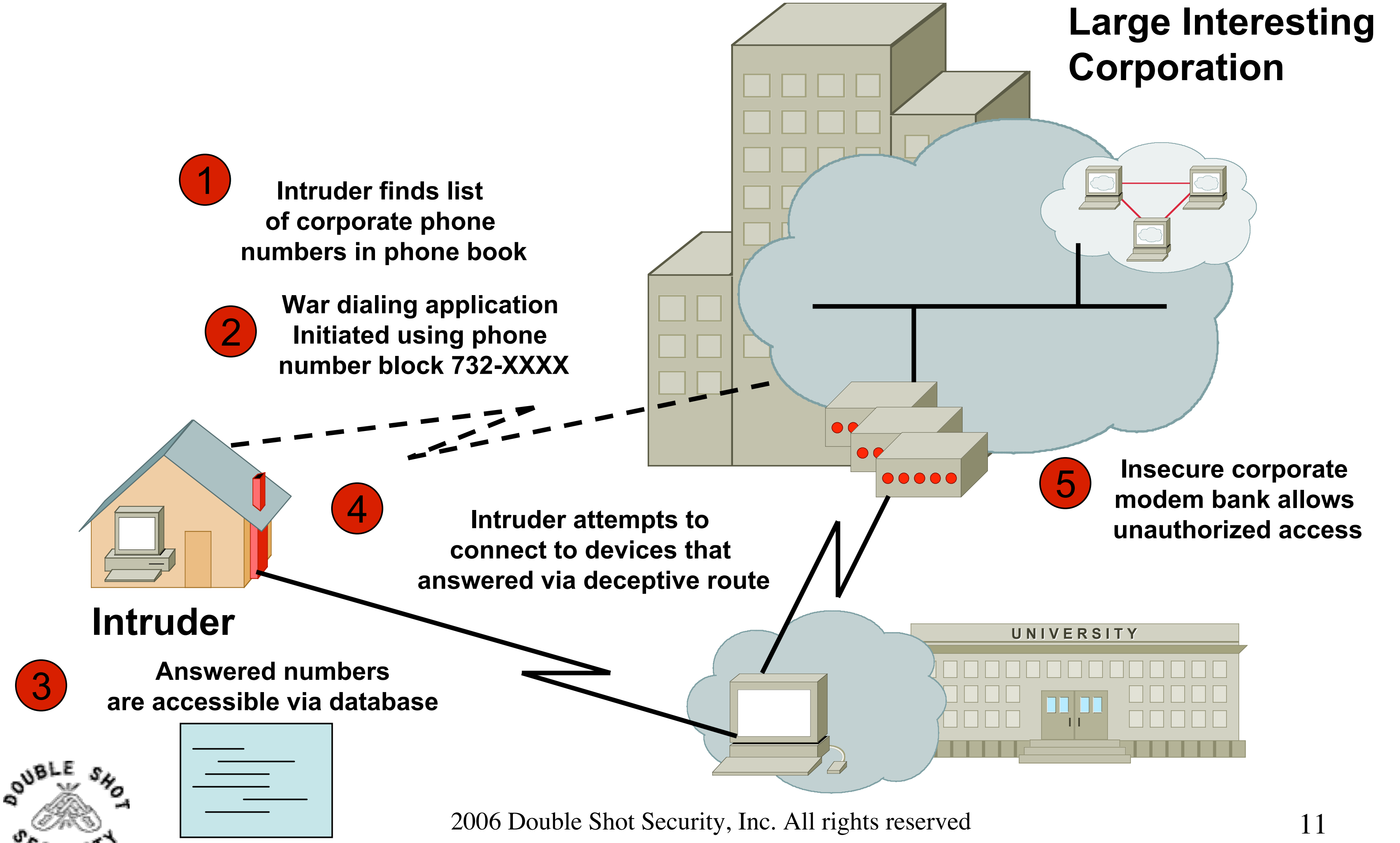


1 DNS query to figure out which web-servers available

2 Ping sweep to see which servers alive and accessible

3 Port scan to see which services are available for exploitation

Off-Path, Outsider Attack: War Dialing



1 Intruder finds list of corporate phone numbers in phone book

2 War dialing application Initiated using phone number block 732-XXXX

3 Answered numbers are accessible via database

4 Intruder attempts to connect to devices that answered via deceptive route

5 Insecure corporate modem bank allows unauthorized access

Operational Security Impact

- Unauthorized Disclosure
  - circumstance or event whereby entity gains access to data for which it is not authorized
- Deception
  - circumstance or event that may result in an authorized entity receiving false data and believing it to be true
- Disruption
  - circumstance or event that interrupts or prevents the correct operation of system services and functions
- Usurpation
  - circumstance or event that results in control of system services or functions by an unauthorized entity

Security Services

- User Authentication
- User Authorization
- Data Origin Authentication
- Access Control
- Data Integrity
- Data Confidentiality
- Auditing / Logging
- DoS Mitigation

Functional Considerations

- Device Physical Access
- Device Management
  - In-band
  - Out-Of-Band (OOB)
- Data Path
- Routing Control Plane
- Software Upgrade / Configuration Integrity

- Logging
- Filtering
- DoS Tracking /Tracing
  - Sink Hole Routing
  - Black-Hole Triggered Routing
  - Unicast Reverse Path Forwarding (uRPF)
  - Rate Limiting

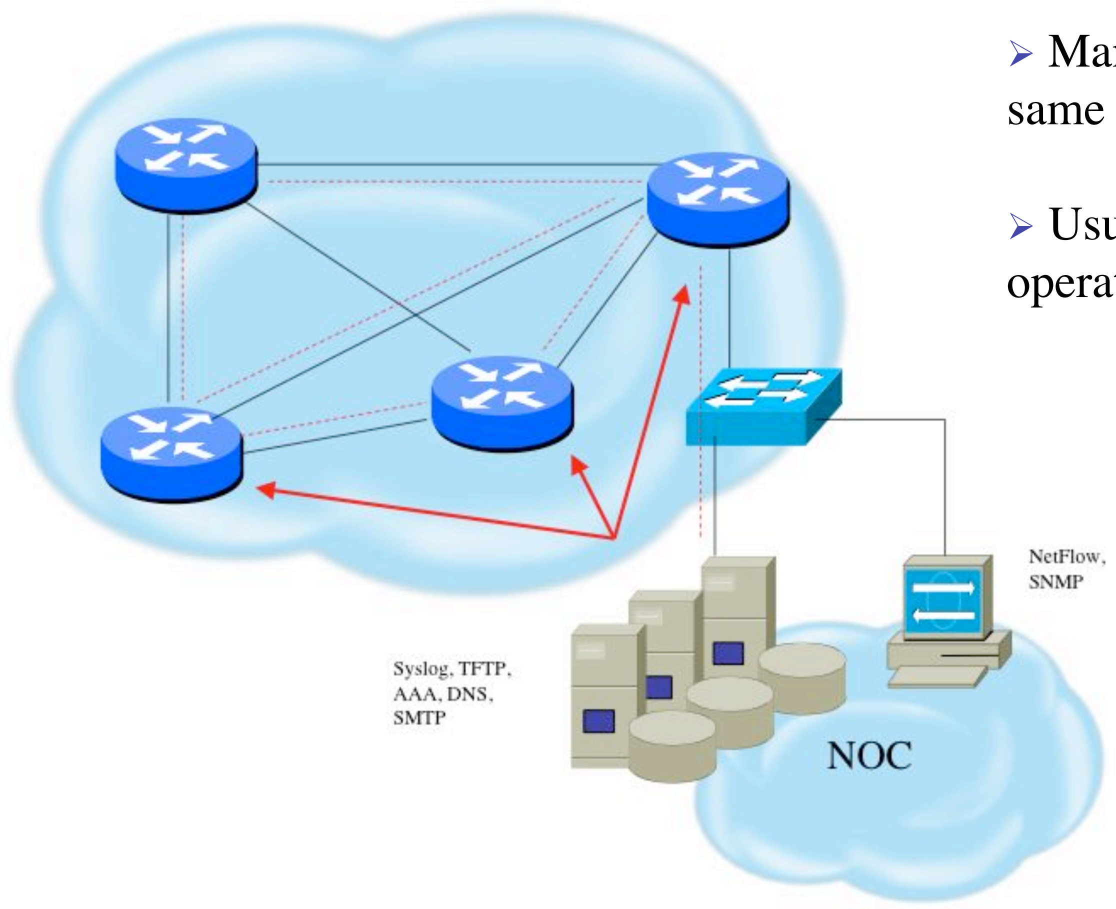
Device Physical Access
(Survey Results)

- Equipment kept in highly restrictive environments
- Console access
  - password protected
  - access via OOB management
- Individual users authenticated
- Social engineering training and awareness

Securing Device Management

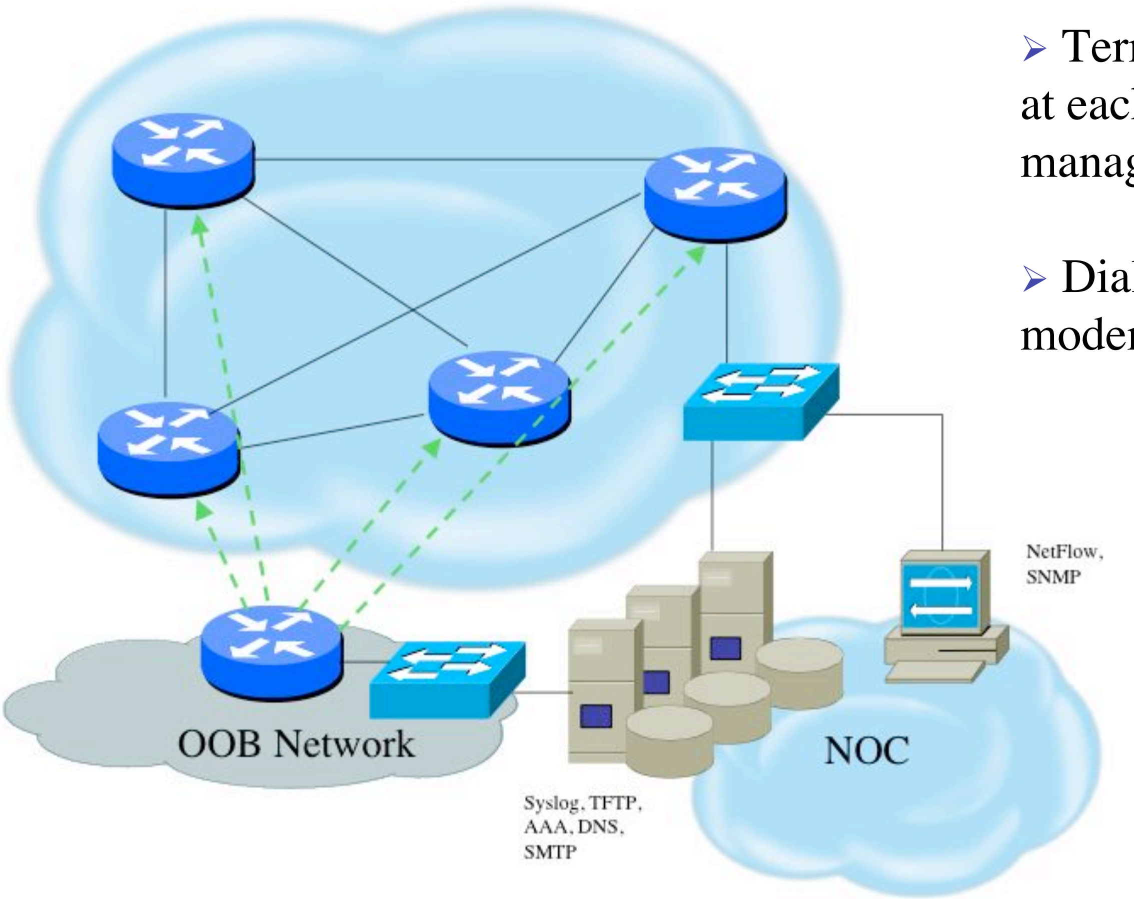
- Miscreants have a far easier time gaining access to devices than you think.
- Ensure that the basic security capabilities have been configured.
- In-band vs Out-of-band management tradeoff

Device In-Band Management



- Management traffic uses same path as transit data
- Usually an issue of operational cost

Device OOB Management



- Terminal servers are used at each location for OOB management

- Dial-back encrypted modems are used as backup

Device Management
(Survey Results)

- SSH primarily used; Telnet only from jumphosts
- HTTP access explicitly disabled
- All access authenticated
  - Varying password mechanisms
  - AAA usually used
    - different servers for in-band vs OOB
    - Different servers for device authentication vs other
    - Static username pw or one-time pw
  - Single local database entry for backup
- Each individual has specific authorization
- Strict access control via filtering
- Access is audited with triggered pager/email notifications
- SNMP is read-only
  - Restricted to specific hosts
  - View restricted if capability exists
  - Community strings updated every 30-90 days

Telnet is Insecure

- Avoid using Telnet
  - Some older devices may require it
- Telnet sends information in clear
  - Username and password can easily be sniffed
- *IF* Telnet used, mitigate risk
  - Limit access
  - Use jumphosts from remote sites

Secure Shell (SSH)

- Username/password information is encrypted
- Host-based authentication
- Flexible authentication methods
  - One-time password, Kerberos, Public key
- Negotiates parameters
  - Key exchange method, public key algorithm, symmetric encryption algorithm, authentication algorithm, hash fcn
- Allows Secure Tunneling
  - TCP port forwarding
  - Forward remote ports to local ones
- Uses TCP port 22

SSH Support

- Two flavors of ssh, ssh1 and ssh2
- Use ssh2 if possible
- Client will either "speak" ssh1 or ssh2
- OpenSSH for UNIX
  - www.openssh.org
  - Supports both ssh1 and ssh2
- Putty client for Windows
  - www.chiark.greenend.org.uk/~sgtatham/putty/

Using SSH on Cisco Routers

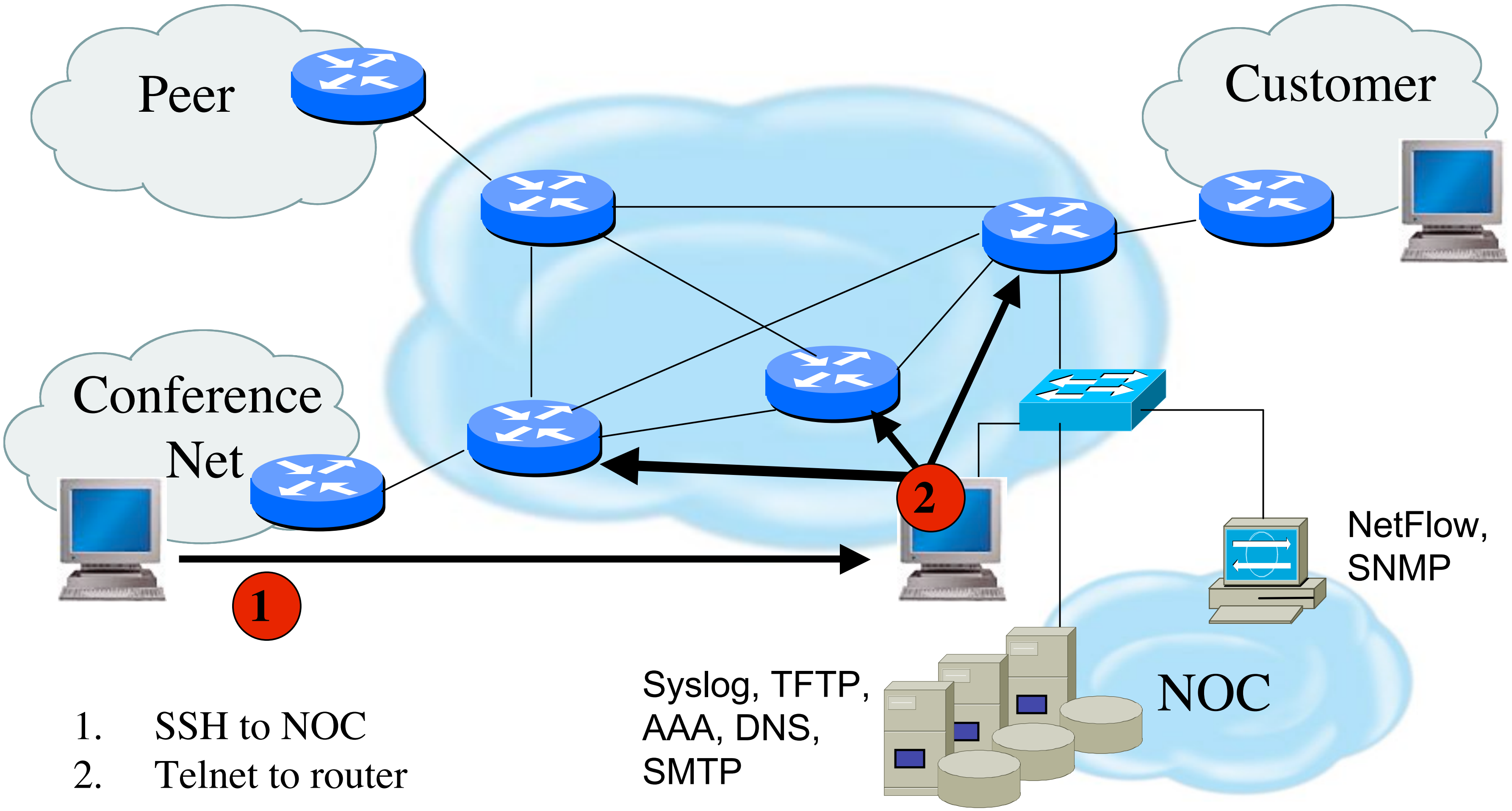
- Supported as of IOS 12.0S
- Ensure you have crypto image
- Set up SSH

```
Router (config)# crypto key generate rsa
```

- Add SSH as input transport

```
line vty 0 4
   transport input ssh
```

Telnet using SSH ‘Jumphost’



1. SSH to NOC
2. Telnet to router

Turn Off Unused Services

Interface-Specific Services

```
no ip redirects
no ip directed-broadcast
no ip proxy-arp
no ip source-route
no ip mask-reply
no cdp enable
```

Global Services

```
no service finger
no ip finger
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no cdp run
```

HTTP Server

- Cisco devices support starting in IOS 11.1CC and 12.0S
- Explicitly disable if not using

```
no ip http server
```

- Example Secure Configuration

```
access-list 36 permit <router 1 IP address>
access-list 36 permit <router 2 IP address>
access-list 36 deny any
ip http server
ip http port 6656
ip http authentication aaa
ip http access-class 36
```

Limiting Device Access

```
access-list 29 permit <NOC subnet>
access-list 29 deny any
line vty 0 4
  access-class 29 in
  exec-timeout 5 0
  transport input telnet ssh
  transport output none
  transport preferred none
  login local
```

- Define specific subnet or hosts which can have telnet or ssh access

- Note that authenticated login is also used

Disabling the AUX Port

```
line aux0
   login local
   no password
   transport input none
   no exec
```

- Will not let anyone log in
- Use this if not using aux port for console access

Authenticate Individual Users

```
service password-encryption
enable secret 5 $1$mgfc$ISYSLeC6ookRSV7sI1vXR.
enable password 7 075F701C1E0F0C0B
!
username merike secret 5 $6$mffc$ImnGLeC67okLOMps
username staff secret 5 $6$ytjc$IchdLeC6o6kImR7s

line con 0
 exec-timeout 1 30
 login local
!
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
```

AAA Authentication

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa accounting exec start-stop tacacs+
!
ip tacacs source-interface loopback0
tacacs-server host <IP address>
tacacs-server key <shared secret>
!
line con 0
 exec-timeout 1 30
 login local
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
```

Secure SNMP Access

- SNMP is primary source of intelligence on a target network!
- Block SNMP from the outside

  access-list 101 deny udp any any eq snmp
- If the router has SNMP, protect it!

  snmp-server community *fO0bAr* RO 1

  access-list 1 permit 127.1.3.5
- Limit the view of the SNMP table

  snmp-server view *limitedforip* ip include

  snmp-server community *newseccret* view *limitedforip*
- Explicitly direct SNMP traffic to an authorized management station.

  snmp-server host *fO0bAr* 127.1.3.5

SNMP Configuration

```
access-list 35 permit <SNMP-server IP address>
access-list deny any
snmp-server community try2brkme RO 35
snmp-server trap-source loopback0
snmp-server trap authentication
snmp-server host <SNMP-server IP address> try2brkme
```

Banner….what's wrong?

```
banner login ^C
            Martini

    2.5 ounces vodka
    1/5 ounce dry vermouth

    Fill mixing glass with ice, add vermouth and
    vodka, and stir to chill.  Strain into a Martini
    glass and garnish with an olive or lemon twist.

    RELAX....INDULGE.....Get Off My Router!!
^C
```

Better Device Banner

!!!! WARNING !!!!

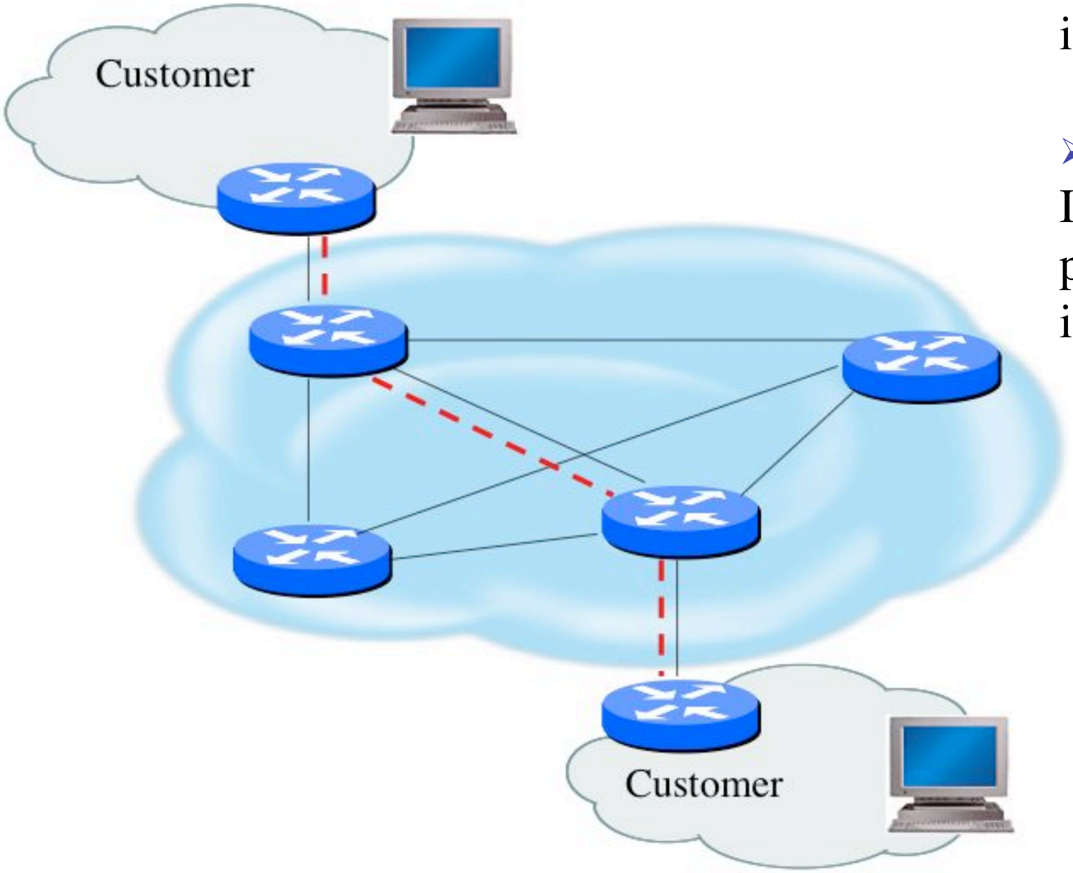
You have accessed a restricted device.

All access is being logged and any unauthorized access will be prosecuted to the full extent of the law.

Fundamental Device Protection Security Practices

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only through ssh
- Disable device access methods that are not used
- Protect SNMP if used
- Shut down unused interfaces
- Shut down unneeded services
- Ensure accurate timestamps for all logging
- Create appropriate banners
- Test device integrity on a regular basis

Data Path



- Protecting traffic that is in transit

- Goal is not to become Internet police but to avoid performance and reliability issues

Data Path

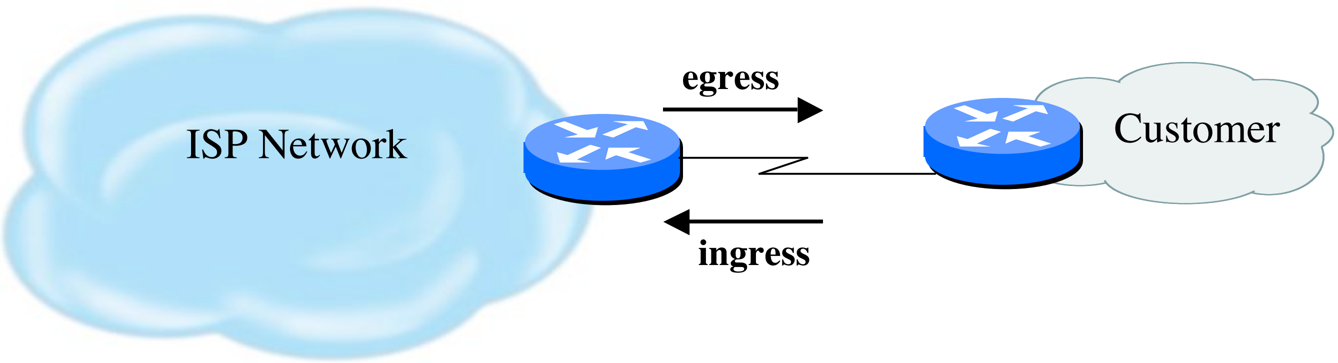
- Filtering and rate limiting are primary mitigation techniques
- BCP-38 guidelines for ingress filtering
- Null-route and black-hole any detected malicious traffic
- Netflow used for tracking traffic flows
- uRPF is not consistently implemented
- Logging of Exceptions

BCP-38 Guidelines

Restrict transit traffic which originates from a downstream network to known, and intentionally advertised, prefix(es)

Description (Martian nets)	**Network**
default	0.0.0.0 /8
loopback	127.0.0.0 /8
RFC 1918	10.0.0.0 /8
RFC 1918	172.16.0.0 /12
RFC 1918	192.168.0.0 /16
Net Test	192.0.2.0 /24
Special use	224.0.0.0/3
Special use	169.254.0.0/16

Sample Egress Filter

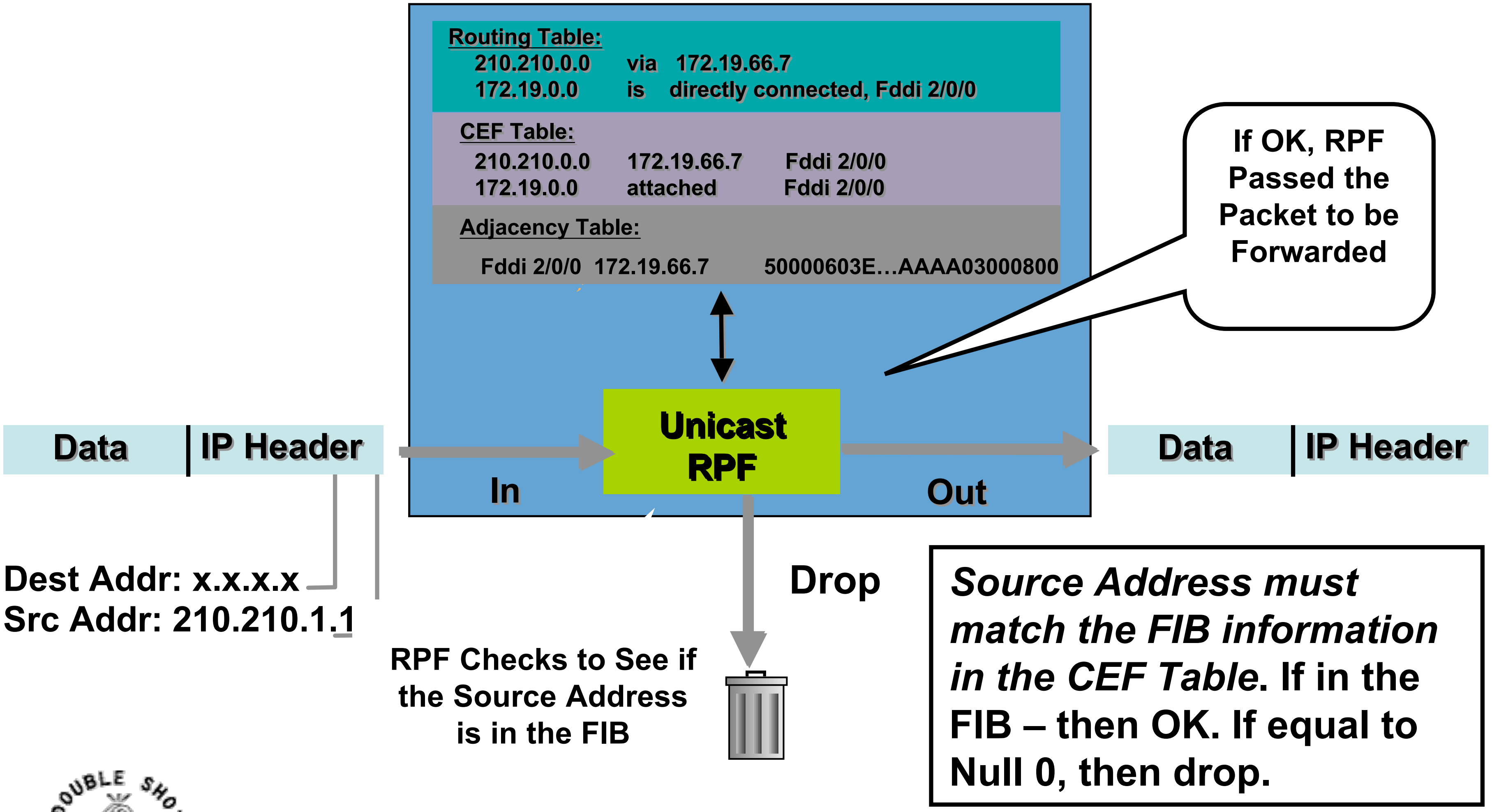


```
access-list 43 permit <my src network> log
access-list 43 deny any ;og
!
interface serial0/0/3
    ip access-group 43 out
```

Sample Ingress Filter

```
access-list 42 deny 0.0.0.0 0.0.0.0 log
access-list 42 deny 127.0.0.0 0.255.255.255 log
access-list 42 deny 10.0.0.0 0.255.255.255.255 log
access-list 42 deny 172.16.0.0 0.15.255.255 log
access-list 42 deny 192.168.0.0 0.0.255.255 log
Access-list 42 deny 192.0.2.0 0.0.0.255 log
access-list 42 deny 224.0.0.0 15.255.255.255 log
access-list 42 deny 169.254.0.0 0.0.255.255 log
access-list 42 deny <my src network> log
access-list 42 permit any
!
interface serial0/0/3
    ip access-group 42 in
```

Unicast Reverse Path Forwarding (uRPF)



Routing Table:

210.210.0.0	via	172.19.66.7
172.19.0.0	is	directly connected, Fddi 2/0/0

CEF Table:

210.210.0.0	172.19.66.7	Fddi 2/0/0
172.19.0.0	attached	Fddi 2/0/0

Adjacency Table:

Fddi 2/0/0	172.19.66.7	50000603E…AAAA03000800

Dest Addr: x.x.x.x
Src Addr: 210.210.1.1

If OK, RPF Passed the Packet to be Forwarded

RPF Checks to See if the Source Address is in the FIB

***Source Address must match the FIB information in the CEF Table*. If in the FIB – then OK. If equal to Null 0, then drop.**

Configuring uRPF

- Cisco IOS

```
Router (config-if)#ip verify unicast reverse-path
or:
Router (config-if)#ip verify unicast source reachable-via [any|rx]
                    [allow-default|allow-self-ping[ACL#]]
```

- Juniper

```
Router (config-if)#ip sa-validate
```

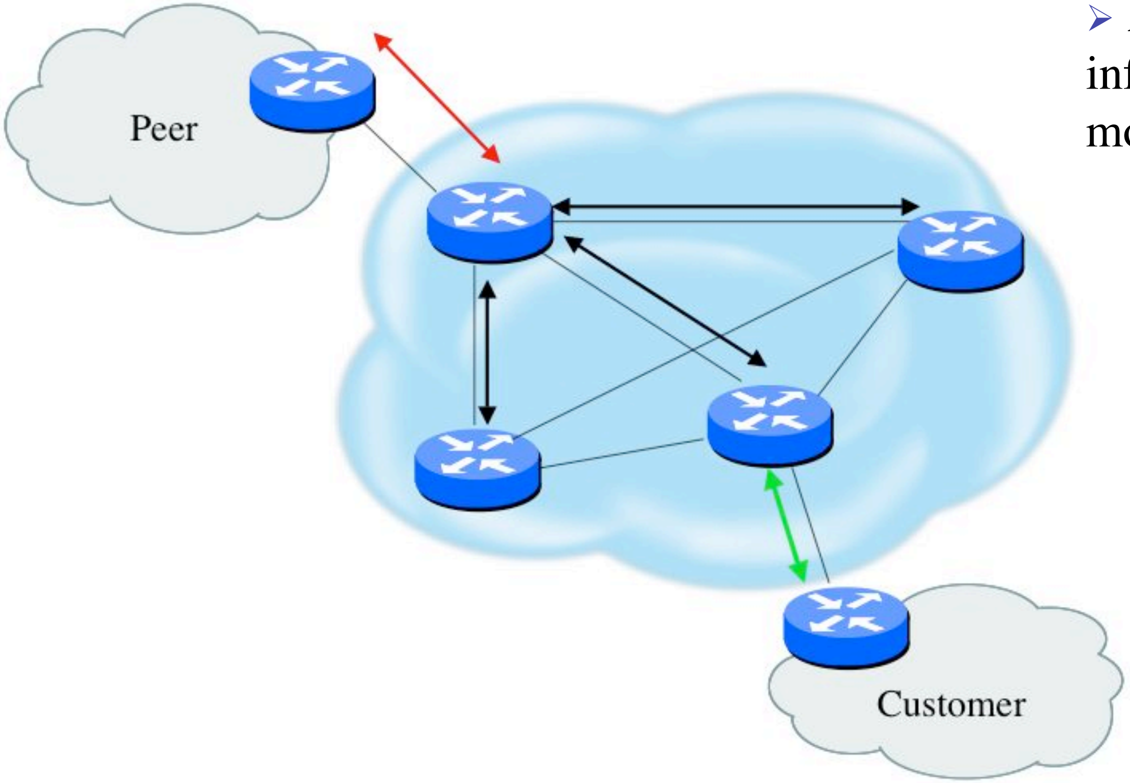
- FreeBSD

```
deny log ip from any to any not (versrcpath|verrevpath) in via em0
```

- Linux

```
echo 1 > /proc/sys/net/ipv4/conf/(all|ethx)/rp_filter
```

Routing Control Plane



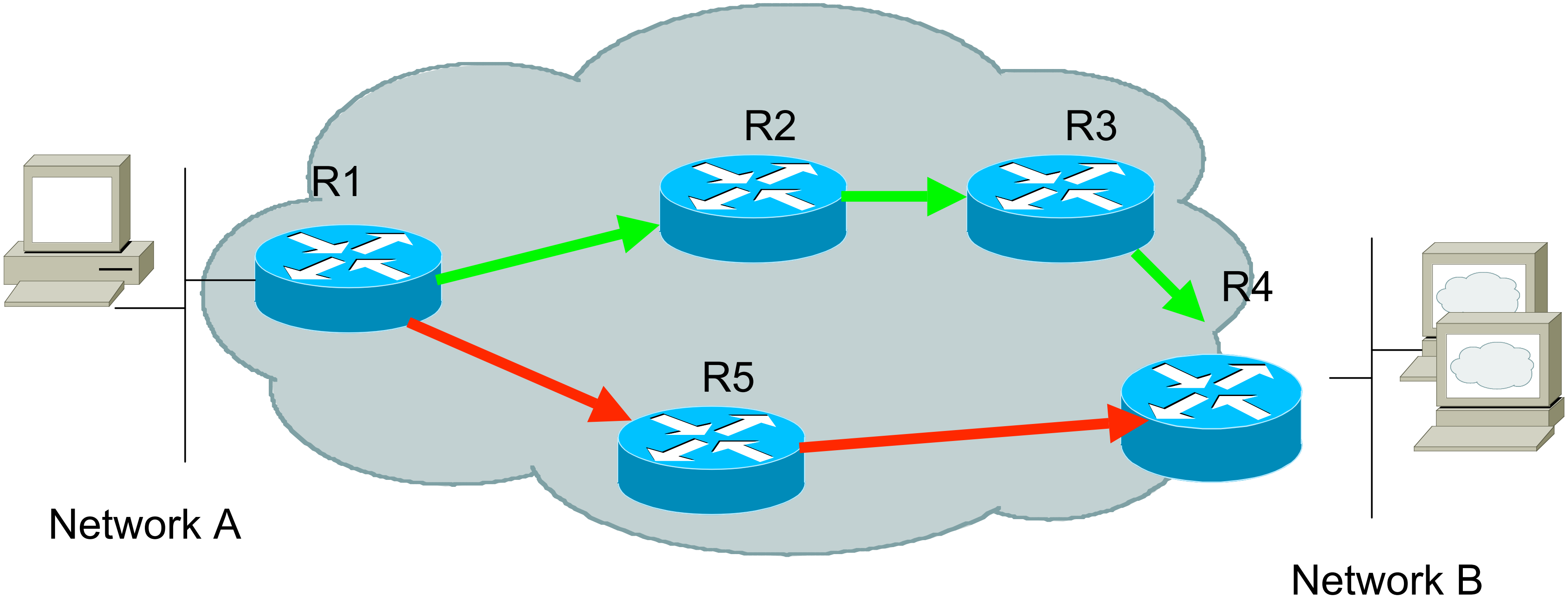
- Attacks on routing infrastructure are becoming more prevalent

How Can Routing Threats Be Realized ?

- Protocol error
  - Routing protocol itself
  - TCP issues for BGP
- Software bugs
  - Is it a bug or feature ?
- Active attack
  - More probable than you think !
- Configuration mistakes
  - Most common form of problem

Routing Threat Consequence

- Traffic is sent along invalid path
- Traffic is dropped



Routing Control Plane
(Survey Results)

- MD-5 authentication
  - Some only deploy this at customer's request
- Route filters limit routes believed from valid peer
- Packet filters limit which devices appear as valid peer
- GTSM (TTL-Hack)
  - Limited iBGP deployment
  - Lack of consistent implementation
- Limiting propagation of invalid routing information
  - Prefix filters
  - AS-PATH filters (trend is leaning towards this)
  - Route dampening (latest consensus is that it causes more harm than good)

BGP Prefix Lists

- Prefix-lists and access-lists are mutually exclusive
- Prefix-list should be used as an alternative to distribute list

```
router bgp 200
  neighbor <IP address> remote-as <eBGP AS>
  neighbor <IP address> prefix-list FILTER-IN in
  neighbor <IP address> prefix-list FILTER-OUT out
```

Prefix List Examples

- Deny default route

```
ip prefix-list MKO deny 0.0.0.0/0
```

- Permit prefix 166.0.0.0/8

```
ip prefix-list MKO permit 166.0.0.0/8
```

- In 192/8 allow up to /24

```
ip prefix-list MKO permit 192.0.0.0/8 le 24
```

- In 192/8 deny /25 and above

```
ip prefix-list MKO deny 192.0.0.0/8 ge 25
```

- Permit all

```
ip prefix-list MKO permit 0.0.0.0/0 le 32
```

Prefix Filter Bogons and RIR Blocks

- Templates available from the Bogon Project:
  - http://www.cymru.com/Bogons/index.html
- Cisco Template by Barry Greene
  - ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/
- Juniper Template by Steven Gill
  - http://www.qorbit.net/documents.html

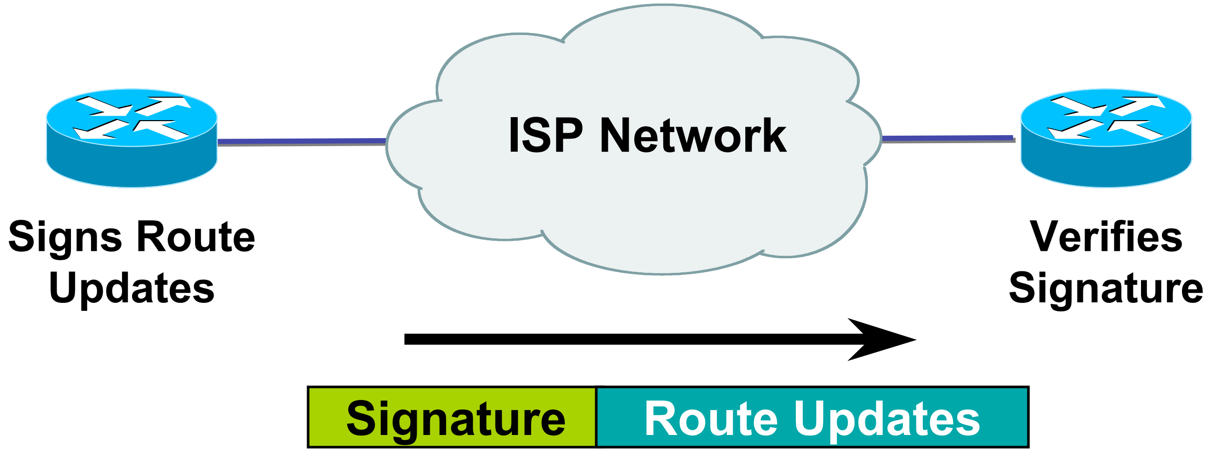
Sample BGP Route Filter

```
router bgp 200
no synchronization
  neighbor <ip address> remote-as <eBGP AS>
  neighbor <ip address> prefix-list bogon-filter in
  neighbor <ip address> prefix-list bogon-filter out
no auto-summary
!
ip prefix-list bogon-filter deny 0.0.0.0/8 le 32
ip prefix-list bogon-filter deny 10.0.0.0/8 le 32
ip prefix-list bogon-filter deny 127.0.0.0/8 le 32
ip prefix-list bogon-filter deny 169.254.0.0/16 le 32
ip prefix-list bogon-filter deny 172.16.0.0/12 le 32
ip prefix-list bogon-filter deny 192.0.2.0/24 le 32
ip prefix-list bogon-filter deny 192.168.0.0/16 le 32
ip prefix-list bogon-filter deny 224.0.0.0/3 le 32
ip prefix-list bogon-filter permit 0.0.0.0/0 le 32
```

BGP Security

- Maximum Prefix Tracking
  - Two level control
    - can log warnings or tear down session
    - Neighbor <IP add> maximum-prefix <max> [<threshold>] [warning-only]
- Maximum AS Path Length
  - Discard prefixes with AS-Path length greater than what is specified
    - Neighbor <IP address> maxas-limit <max>
  - Easier than filter-lists

Route Authentication

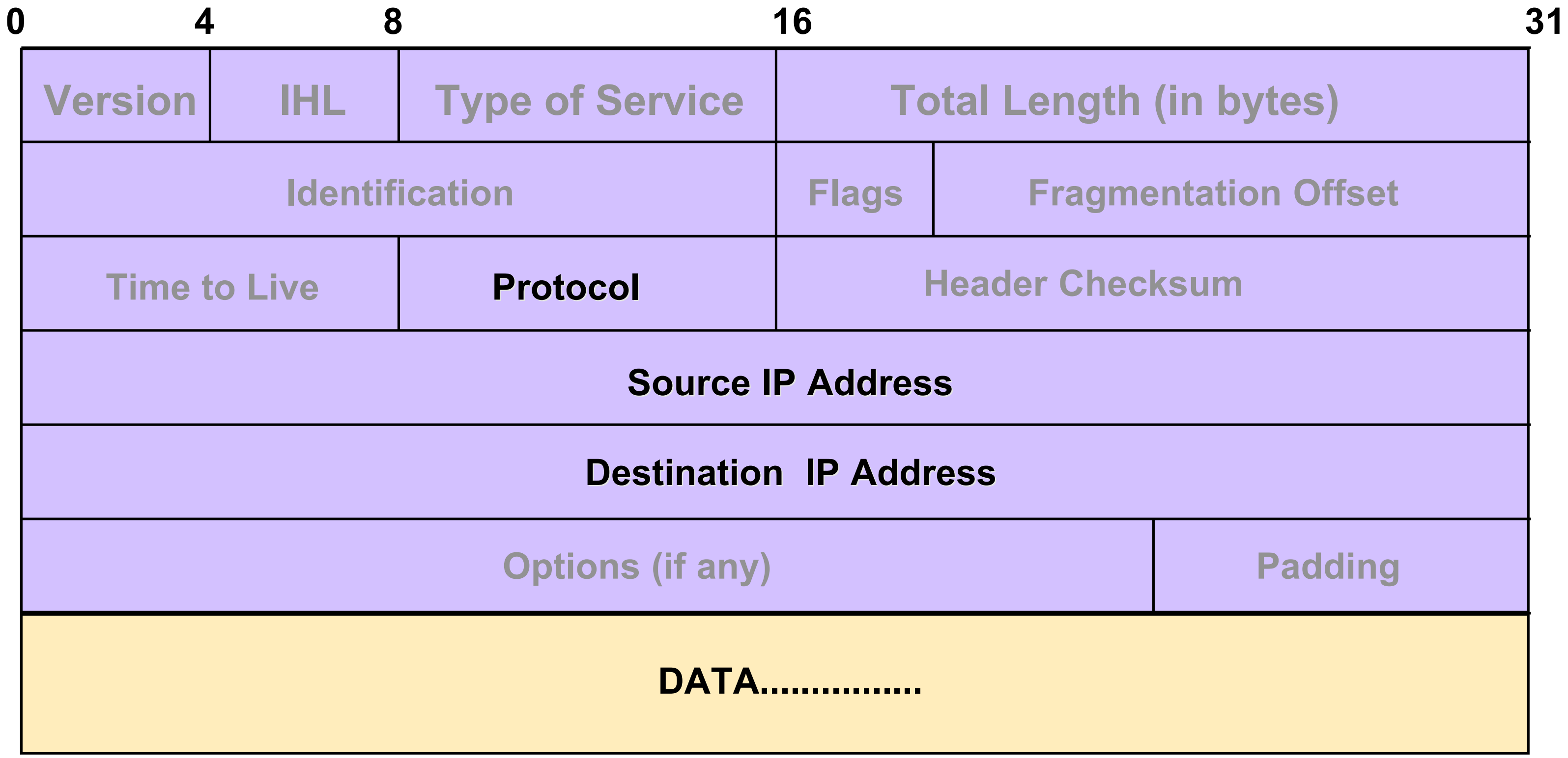


Certifies authenticity of neighbor and integrity of route updates

Why Use Route Authentication

- Route Authentication equates to data origin authentication and data integrity
- In BGP, requires TCP resets to be authenticated so malicious person can't randomly send TCP resets
- In cases where routing information traverses shared networks, someone might be able to alter a packet or send a duplicate packet
- Routing protocols were not initially created with security in mind…..this needs to change….

IP Header Format



0 4 8 16 31

Version | IHL | Type of Service | Total Length (in bytes)

Identification | Flags | Fragmentation Offset

Time to Live | **Protocol** | Header Checksum

Source IP Address

Destination IP Address

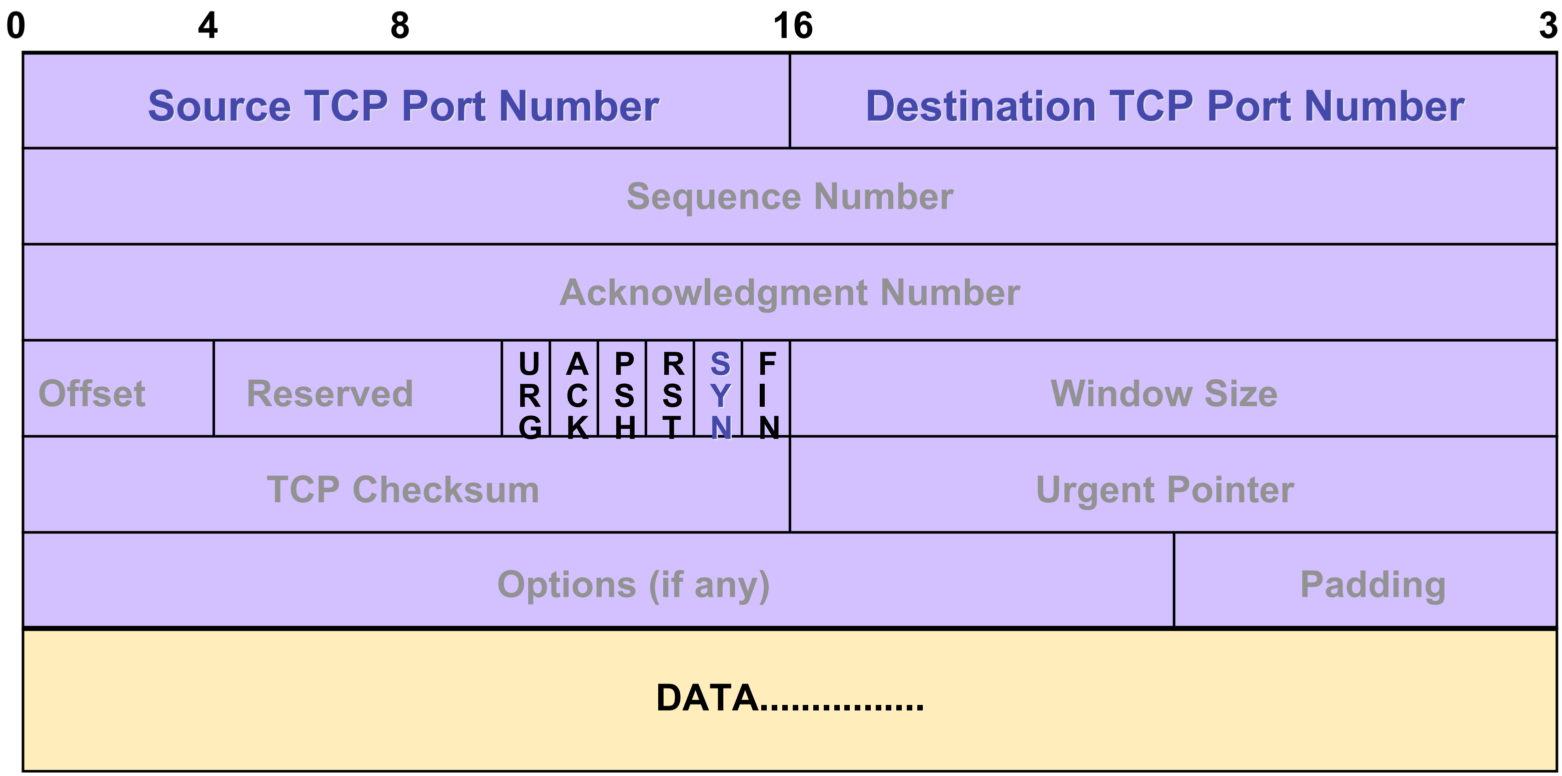
Options (if any) | Padding

DATA................

TCP (Transport Control Protocol)

- Provides reliable virtual circuits to user processes
- Lost or damaged packets are resent
- Sequence numbers maintain ordering
- All packets except first contain ACK #
  - (contains sequence number of last sequential byte successfully received)

TCP Header Format



0 4 8 16 31

Source TCP Port Number | Destination TCP Port Number

Sequence Number

Acknowledgment Number

Offset | Reserved | URG | ACK | PSH | RST | SYN | FIN | Window Size

TCP Checksum | Urgent Pointer

Options (if any) | Padding

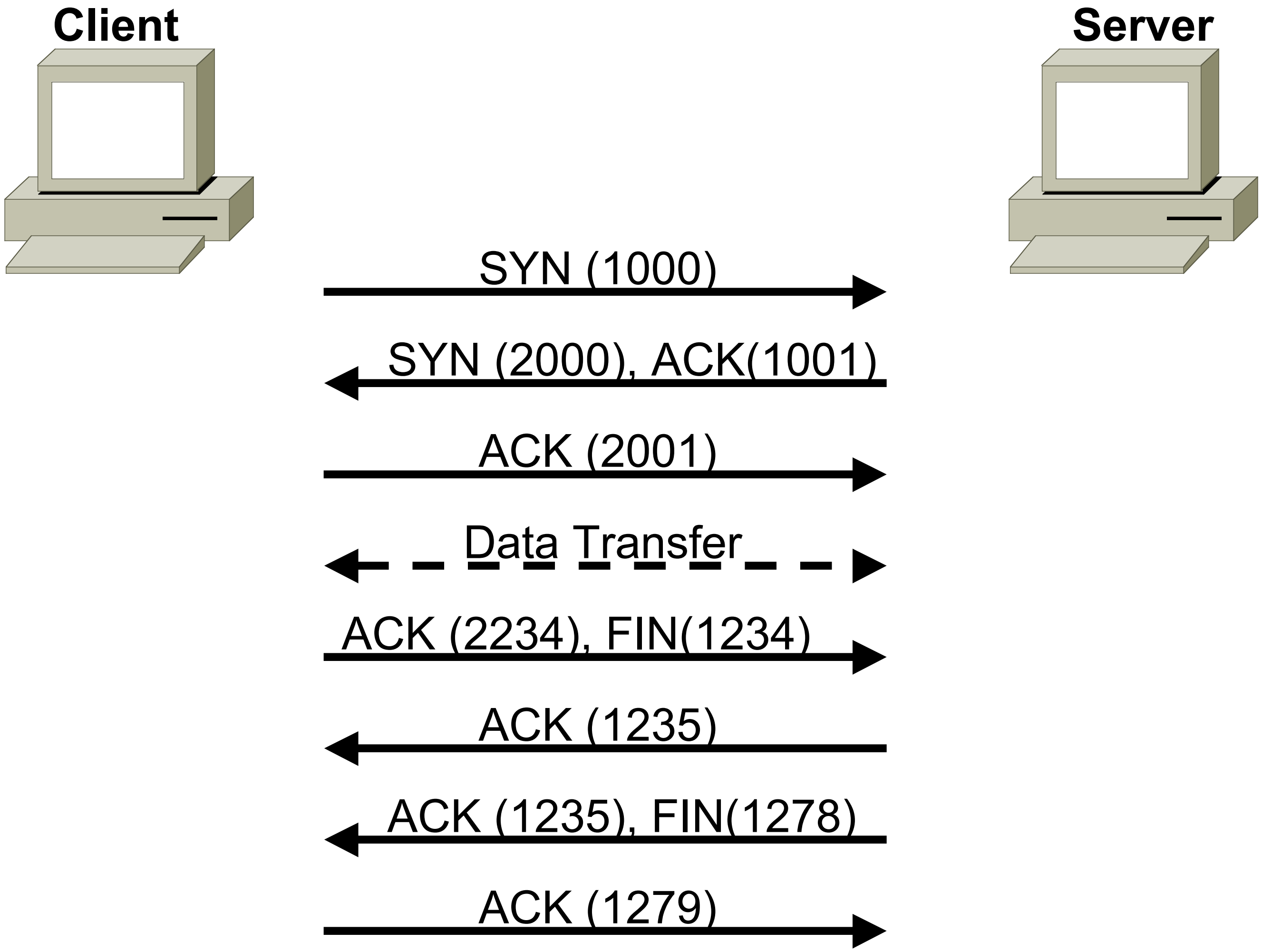
DATA................

TCP Control Flags

URG	ACK	PSH	RST	SYN	FIN

- URG: indicates urgent data in data stream
- ACK: acknowledgement of earlier packet
- PSH: flush packet and not queue for later delivery
- RST: reset connection due to error or other interruption
- SYN: used during session establishment to synchronize sequence numbers
- FIN: used to tear down a session

TCP Session


Client
Server
SYN (1000)
SYN (2000), ACK(1001)
ACK (2001)
Data Transfer
ACK (2234), FIN(1234)
ACK (1235)
ACK (1235), FIN(1278)
ACK (1279)

TCP Reset Attack is a Protocol Flaw

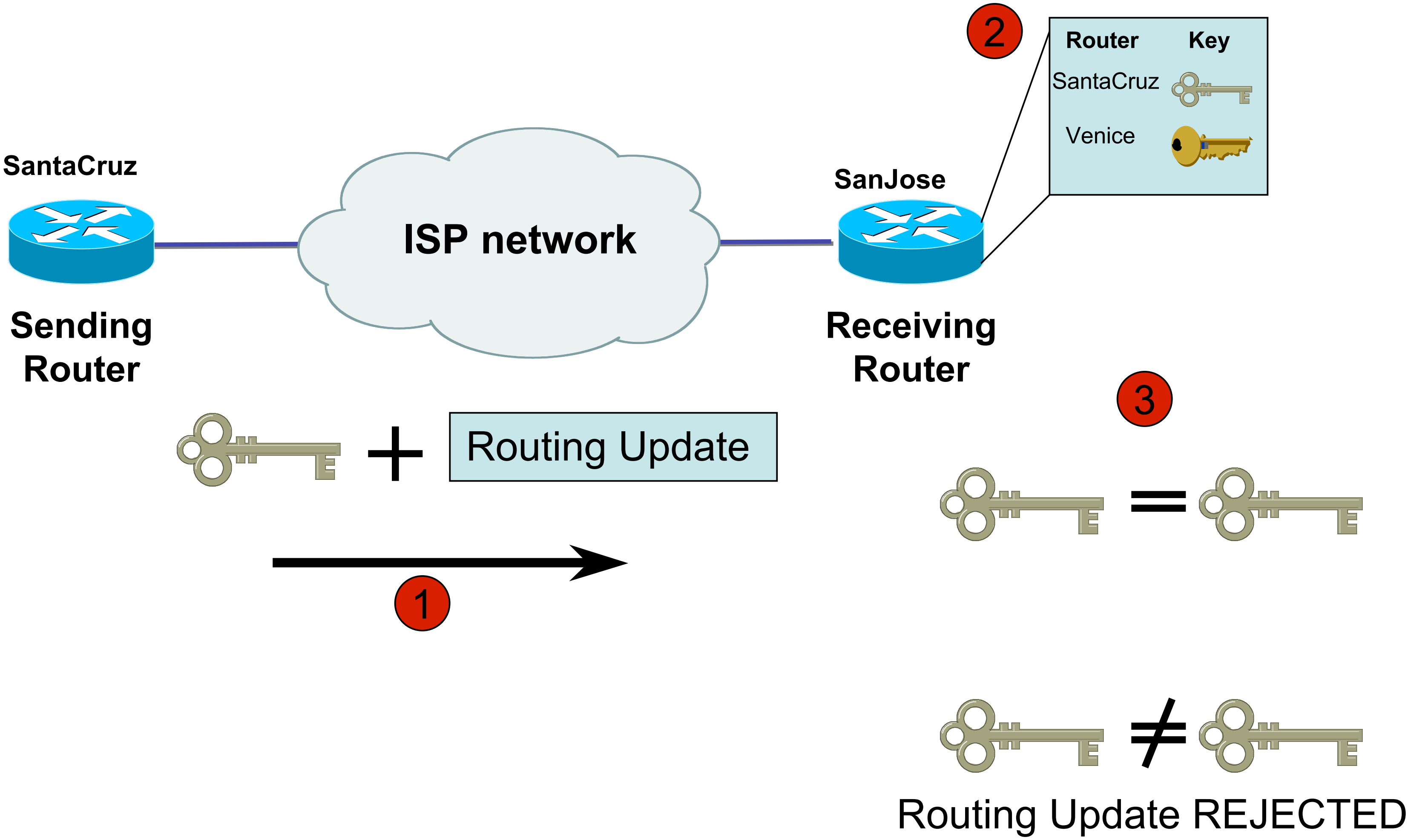
- Attacker predicts the target’s choice of expected sequence number
- Spoofed packet is sent with the reset bit enabled which resets the TCP connection
- BGP routing protocols runs over TCP

Reality Check

- Software will have bugs
- Network devices will be misconfigured
- Security mitigation techniques reduce the risk of an intrusion

BUT….is route authentication useful ?

Plaintext Neighbor Authentication



Hash Functions

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.

Common Algorithms: MD-5 (128), SHA-1 (160)

Computing a Keyed-MAC

- Message broken down into n blocks of 512-bits
- Shared secret key is xor'ed with specified array to produce K1
- Shared secret key is xor'ed a 2nd time with another specified array to produce K2

Hash1 = $(1^{st}$ block of message + $K1)_{MD5}$

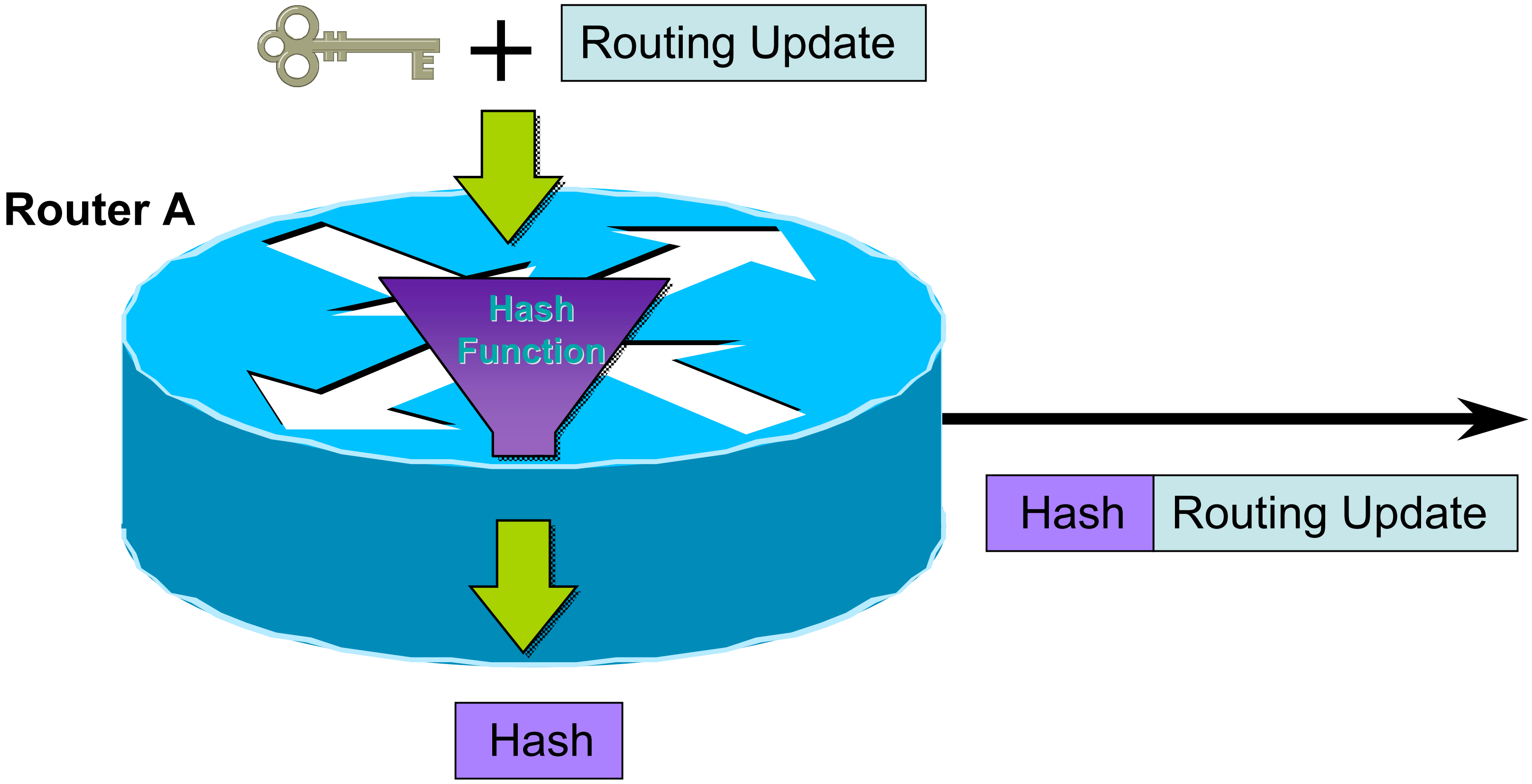
Hash2 = $(hash1 + K2)_{MD5}$

Hash3 = $(2^{nd}$ block of message + $hash2)_{MD5}$

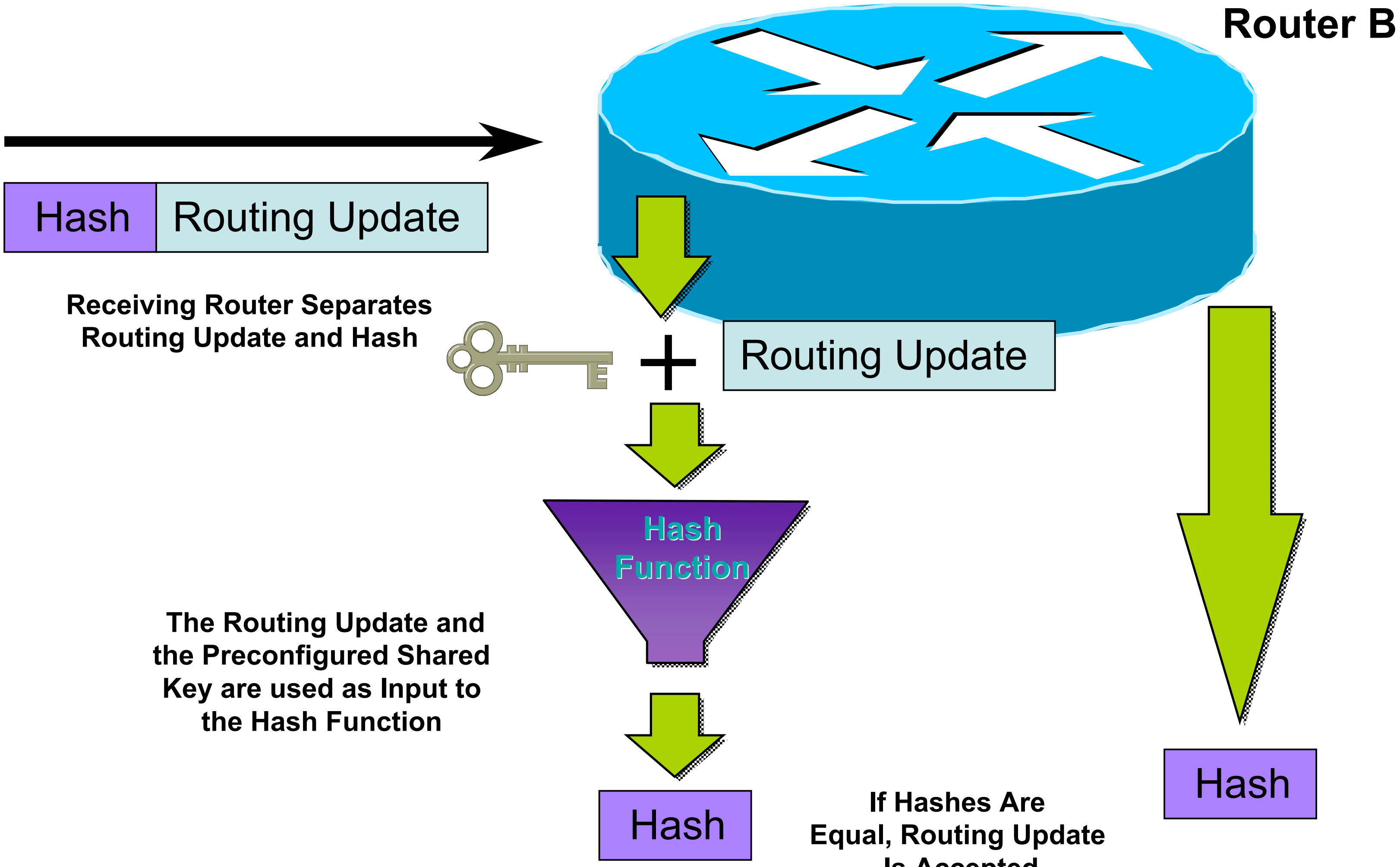
Hash(n+1) = $(n^{th}$ block of message + $hashn)_{MD5}$

HMAC-MD5-96 / HMAC-SHA-96 -> last hash truncated to 96 bits!!

MD-5 Neighbor Authentication: Originating Router



MD-5 Neighbor Authentication: Receiving Router



Router B

Hash

Routing Update

Receiving Router Separates Routing Update and Hash

+

Routing Update

Hash Function

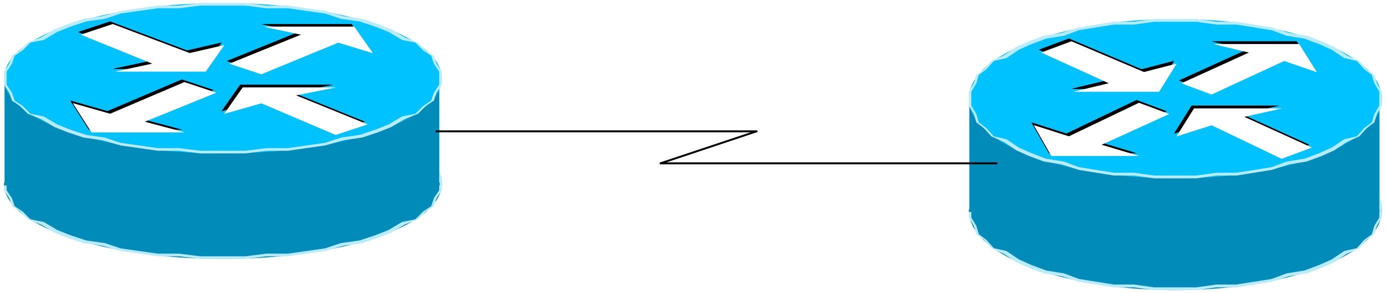
The Routing Update and the Preconfigured Shared Key are used as Input to the Hash Function

Hash

If Hashes Are Equal, Routing Update Is Accepted

Hash

Sample Configuration (OSPF)



```
interface Loopback0
ip address 70.70.70.70 255.255.255.255

interface Serial2
ip address 192.16.64.2 255.255.255.0

ip ospf message-digest-key 1 md5 mk6
router ospf 10
network 192.16.64.0 0.0.0.255 area 0
network 70.0.0.0 0.255.255.255 area 0
area 0 authentication message-digest
```

```
interface Loopback0
ip address 172.16.10.36 255.255.255.240

interface Serial1/0
ip address 192.16.64.1 255.255.255.0

ip ospf message-digest-key 1 md5 mk6
router ospf 10
network 172.16.0.0 0.0.255.255 area 0
network 192.16.64.0 0.0.0.255 area 0
area 0 authentication message-digest
```

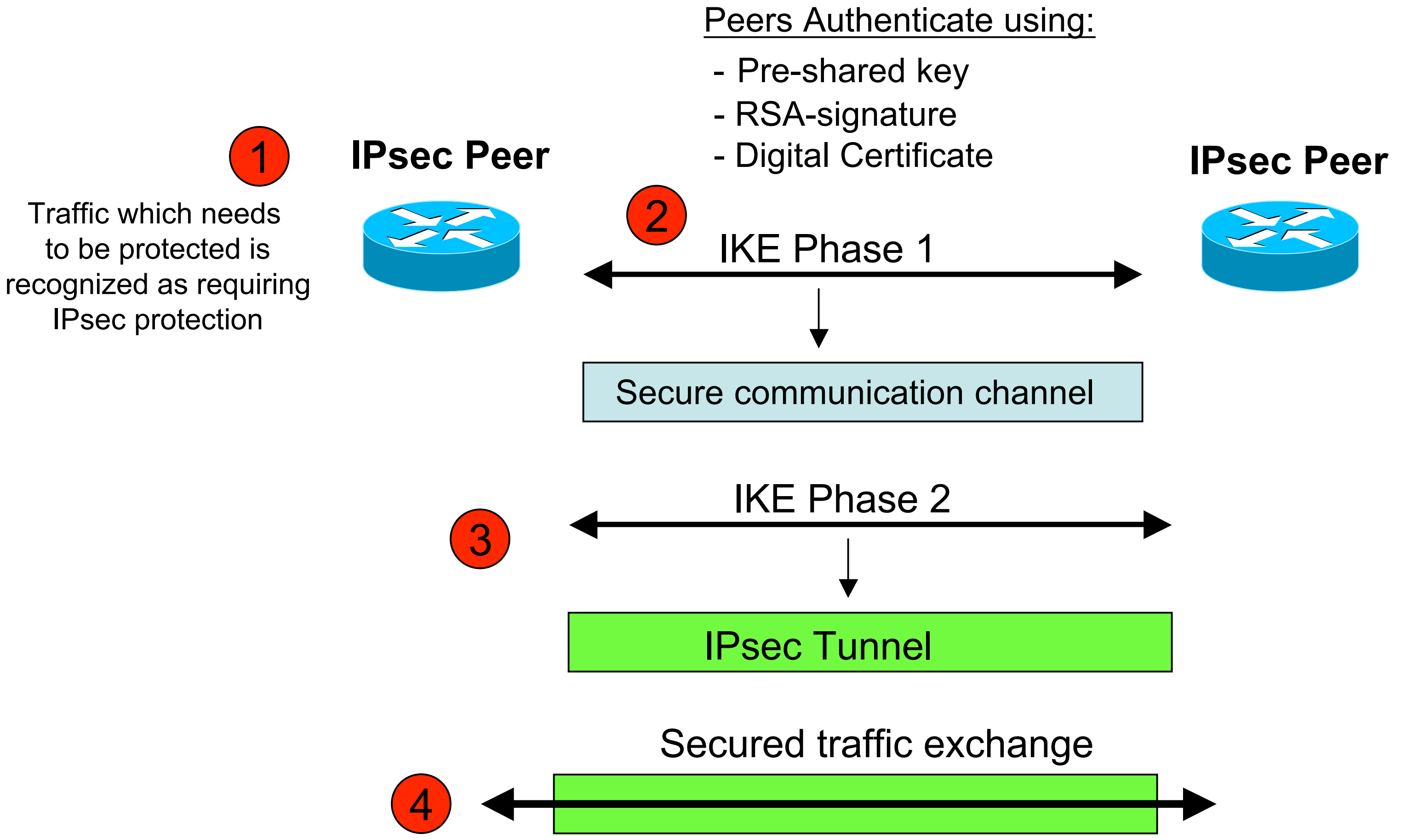
Issues With Current Route Authentication Implementations

- Re-keying is a nightmare
  - session loss
  - route re-computation
- Interoperability issues
- Is SHA-1 a better authentication protocol ?

Another option…..

- Use IPsec to secure routing updates
- Advantages
  - automatic re-keying (sort of…)
  - confidentiality of routing updates
- Disadvantages
  - limited interoperability
  - configuration nightmare

Overview of IPsec w/IKE



1

Traffic which needs
to be protected is
recognized as requiring
IPsec protection

IPsec Peer

Peers Authenticate using:

- Pre-shared key
- RSA-signature
- Digital Certificate

IPsec Peer

2

IKE Phase 1

Secure communication channel

3

IKE Phase 2

IPsec Tunnel

4

Secured traffic exchange

Pretty Good IPsec Policy

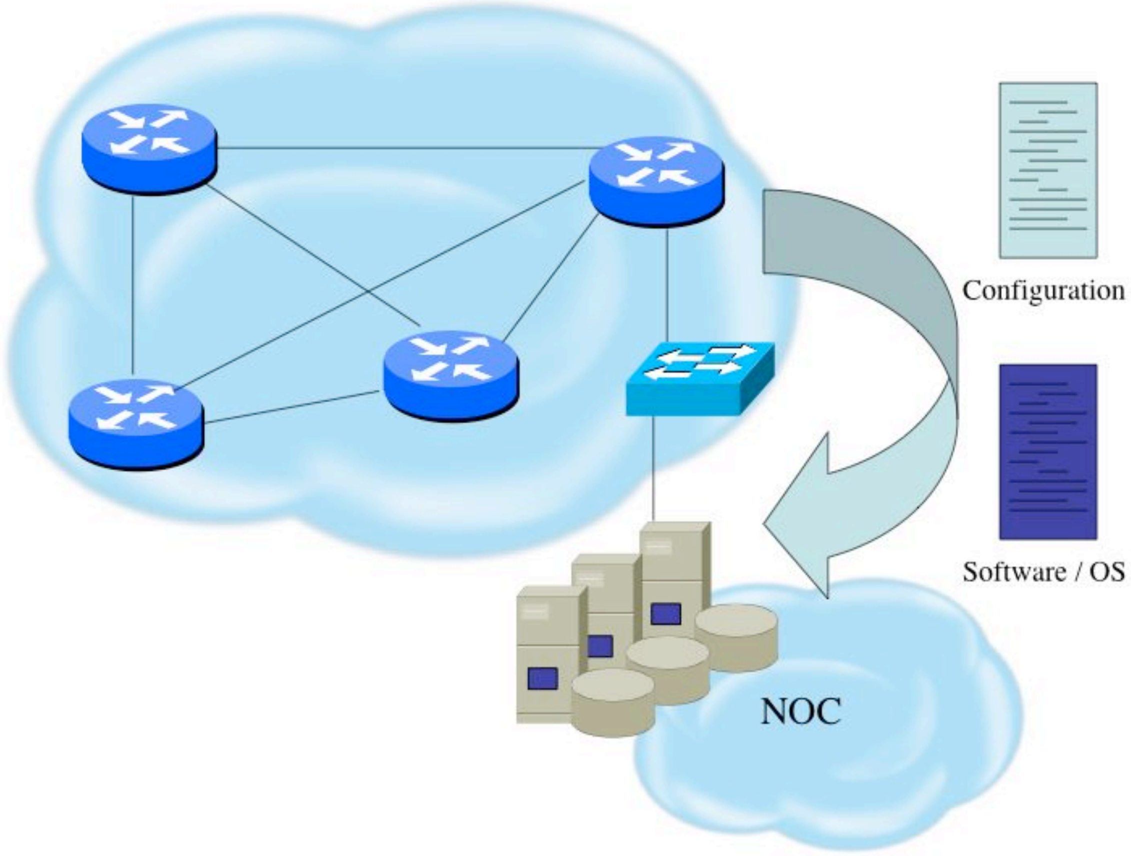
- IKE Phase 1 (aka ISAKMP)
  - 3DES
  - Lifetime (how many seconds in 1 day?)
  - SHA-1
  - DH Group 2 (MODP)
- IKE Phase 2 (aka IPsec)
  - 3DES
  - Lifetime (how many seconds in 1 hour?)
  - SHA-1
  - PFS
  - DH Group 2 (MODP)

Juniper BGP IPsec Example

```
[edit security ipsec]
+   proposal test-proposal {
+       protocol esp;
+       authentication-algorithm hmac-sha1-96;
+       encryption-algorithm 3des-cbc;
+       lifetime-seconds 3600;
+   }
+   policy test-ipsecwike {
+       perfect-forward-secrecy {
+           keys group2;
+       }
+       proposals test-proposal;
+   }
[edit security ipsec]
    security-association bgp-gw8-sa { ... }
+   security-association test-sa {
+       mode transport;
+       dynamic {
+       ipsec-policy test-ipsecwike }
+   }
```

```
[edit security]
+  ike {
+      proposal test-ike {
+          authentication-method pre-shared-keys;
+          dh-group group2;
+          authentication-algorithm sha1;
+          encryption-algorithm 3des-cbc;
+          lifetime-seconds 28880;
+      }
+      policy 198.6.255.32 {
+          mode main;
+          proposals test-ike;
+          pre-shared-key hexadecimal
"$9$QB21F9AuO1hyl0ONdwYoa9AtpRhWLx7db
      ApORSyW8Ndbs2aiHm";
+      }
```

Software Upgrade / Integrity



Software Upgrade / Integrity
(Survey Results)

- Files stored on specific systems with limited access
- All access to these systems are authenticated and audited
- SCP is used where possible and FTP is NEVER used
- Configuration files polled & compared on an hourly basis
- Filters limit uploading / downloading of files
- Many system binaries use MD-5 checks for integrity
- Configuration files are stored with obfuscated passwords

System Image and Configuration File Security

- Careful of sending configurations where people can snoop the wire
  - CRC or MD5 validation
  - Sanitize configuration files
- SCP should be used to copy files
  - TFTP and FTP should be avoided
- Use tools like ‘rancid’ to periodically check against modified config files

Never Leave Passwords in Clear-Text

- ***password*** command
  - Will encrypt all passwords on the Cisco IOS with Cisco-defined encryption type "7"
  - Use "*command* password 7 <password>" for cut/paste operations
  - Cisco proprietary encryption method
- ***secret*** command
  - Uses MD5 to produce a one-way hash
  - Cannot be decrypted
  - Use "*command* secret 5 <password>" to cut/paste another "enable secret" password

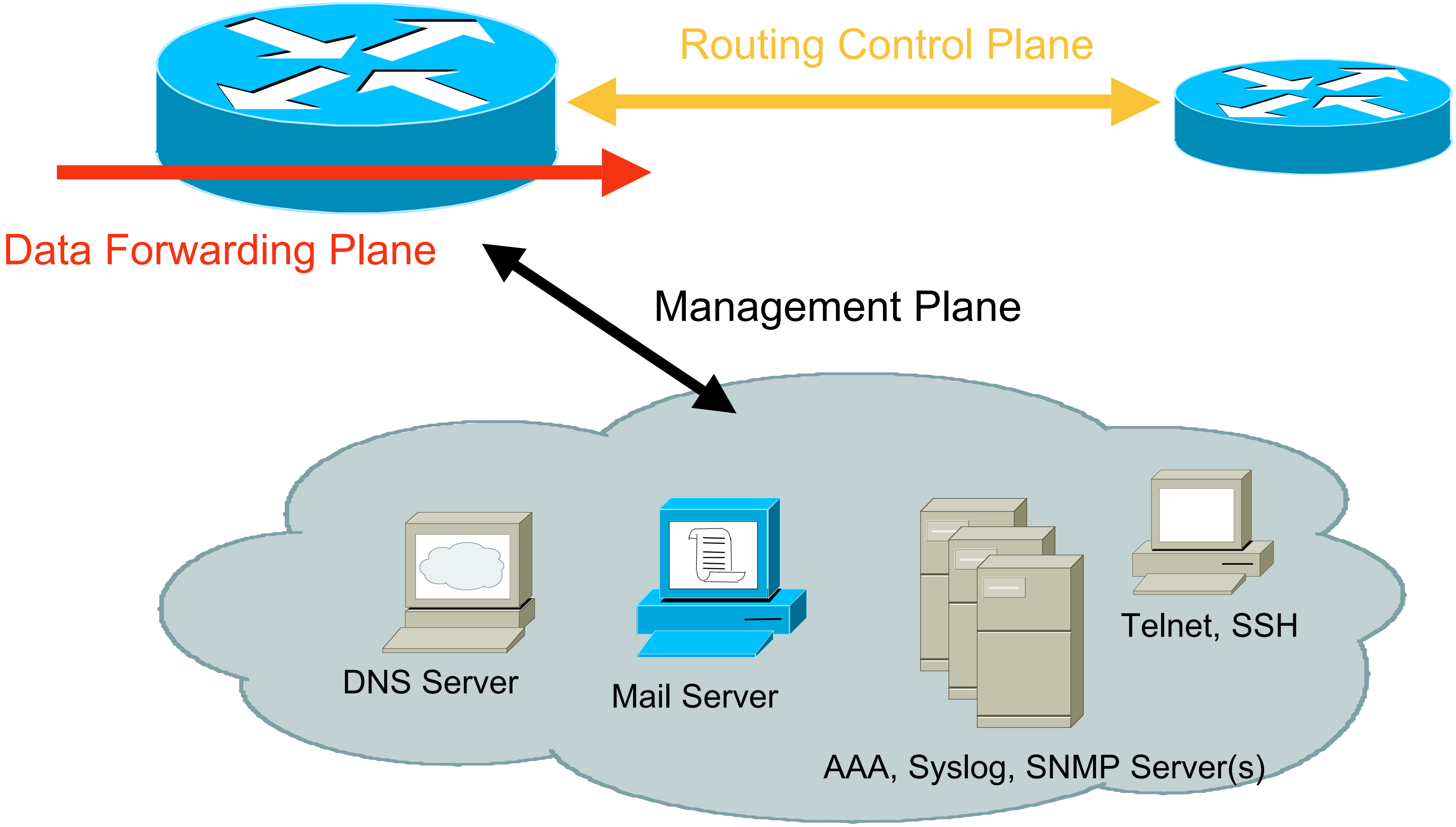
Core Dump Configuration

```
ip ftp username cisco
ip ftp password 7 66CEB8747509
ip ftp source-interface loopback0
exception protocol ftp
exception dump <FTP server IP address>
```

Filtering Consideration

- Data Plane
  - Traffic going through the router
- Management Plane
  - Traffic used to monitor and log information
  - Traffic used to manage device
- Control Plane
  - Traffic specific to routing protocols

Filtering Considerations



Filtering Deployment Considerations

- How does the filter load into the router? Does it interrupt packet flow?
- How many filters can be supported in hardware? In software?
- How does filter depth impact performance?
- How do multiple concurrent features affect performance?

Data Plane (Packet) Filters

- Most common problems
  - Poorly-constructed filters
  - Ordering matters
- Scaling and maintainability issues with filters are commonplace
- Make your filters as modular and simple as possible

Management Plane Filters

- Define Explicit Access To/From Management Stations
  - SNMP, Syslog, TFTP, NTP, AAA Protocols, DNS, SMTP, SSH, Telnet, etc.
- Authenticate Access
- Think of Using Out-of-Band Management Network

Control Plane (Routing) Filters

- Filter traffic destined TO your core routers
- Develop list of required protocols that are sourced from outside your AS and access core routers
  - Example: eBGP peering, GRE, IPSec, etc.
  - Use classification filters as required
- Identify core address block(s)
  - This is the protected address space
  - Summarization is critical for simpler and shorter filter lists

BGP Prefix Filtering

- All BGP Prefixes coming into your network and leaving your network need to be filtered to enforce a policy.
- The problem is most ISPs is that they are **not**:
  - Filtering Comprehensively
  - Filtering their customer’s prefixes
  - Filtering prefixes going out of their network

Secure Logging Infrastructure

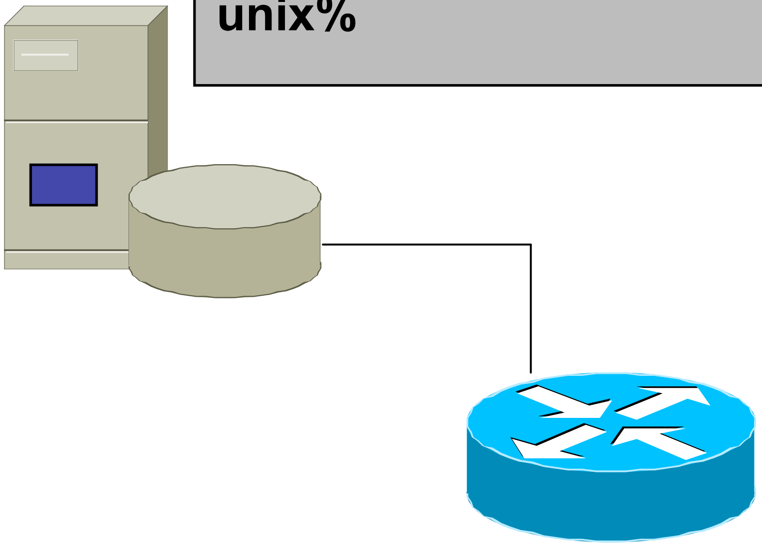
- Log enough information to be useful but not overwhelming.
- Create backup plan for keeping track of logging information should the syslog server be unavailable
- Remove private information from logs
- How accurate are your timestamps?

Logging Configuration

```
service timestamps debug uptime
service timestamps log datetime msec
!
logging console warnings
logging snmp-authfail
logging buffered 3200 notifications
!
logging trap debugging
logging source-interface loopback0
logging 192.168.66.5
logging 192.168.99.5
```

Timestamp Issues

```
unix% tail cisco.log
  Feb 18 21:48:26 [10.1.1.101.9.132] 31: *Mar  2 11:51:55 CST:
     %SYS-5-CONFIG_I: Configured from console by vty0 (10.1.1.2)
unix% date
  Tue Feb 18 21:49:53 CST 2005
unix%
```



```
version 12.2
service timestamps log datetime
localtime show-timezone
!
logging 10.1.1.2
```

```
Router>sho clock
*11:53:44.764 CST Tue Mar 2 1993
Router>
```

Using NTP

- Need to synchronize timestamps
- Network Time Protocol (NTP)
  - External source
    - Upstream ISP, Internet, atomic clock, GPS
  - Internal source
    - Router can act as stratum 1 timesource

```
access-list 15 permit
    192.168.66.0 0.0.0.255
access-list 17 permit 192.168.1.1
access-list 17 permit 192.168.3.1
!
ntp source loopback0
ntp access-group peer 17
ntp access-group serve-only 15
ntp server 192.168.3.1
ntp server 192.168.1.1 prefer
```

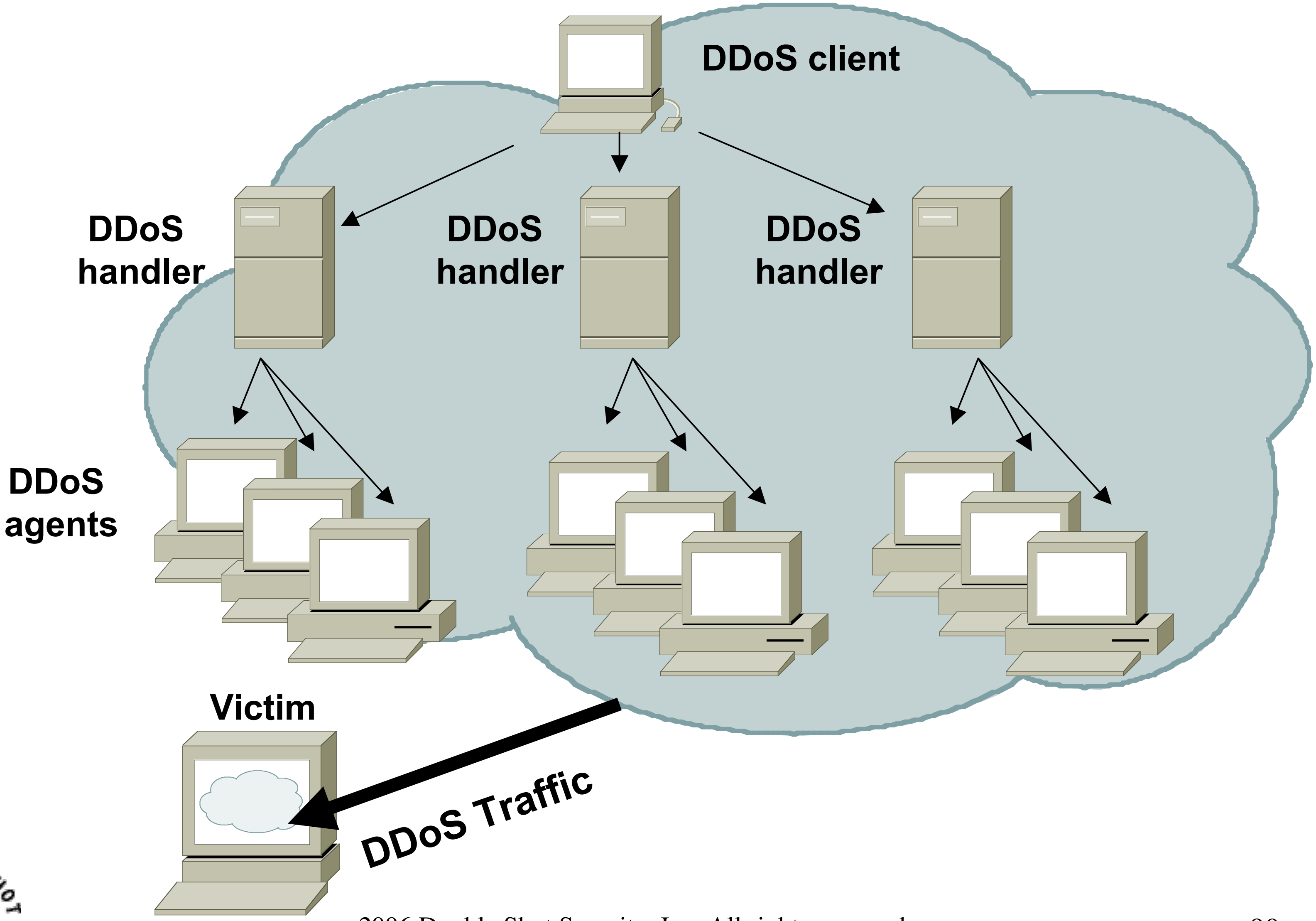
Logging BGP Neighbor Changes

- Get information on up/down events and reason for last peering reset
  - [no] log-neighbor changes
- Useful for analyzing BGP session resets
- Available from *sh ip bgp neighbor*
- Accessible via SNMP

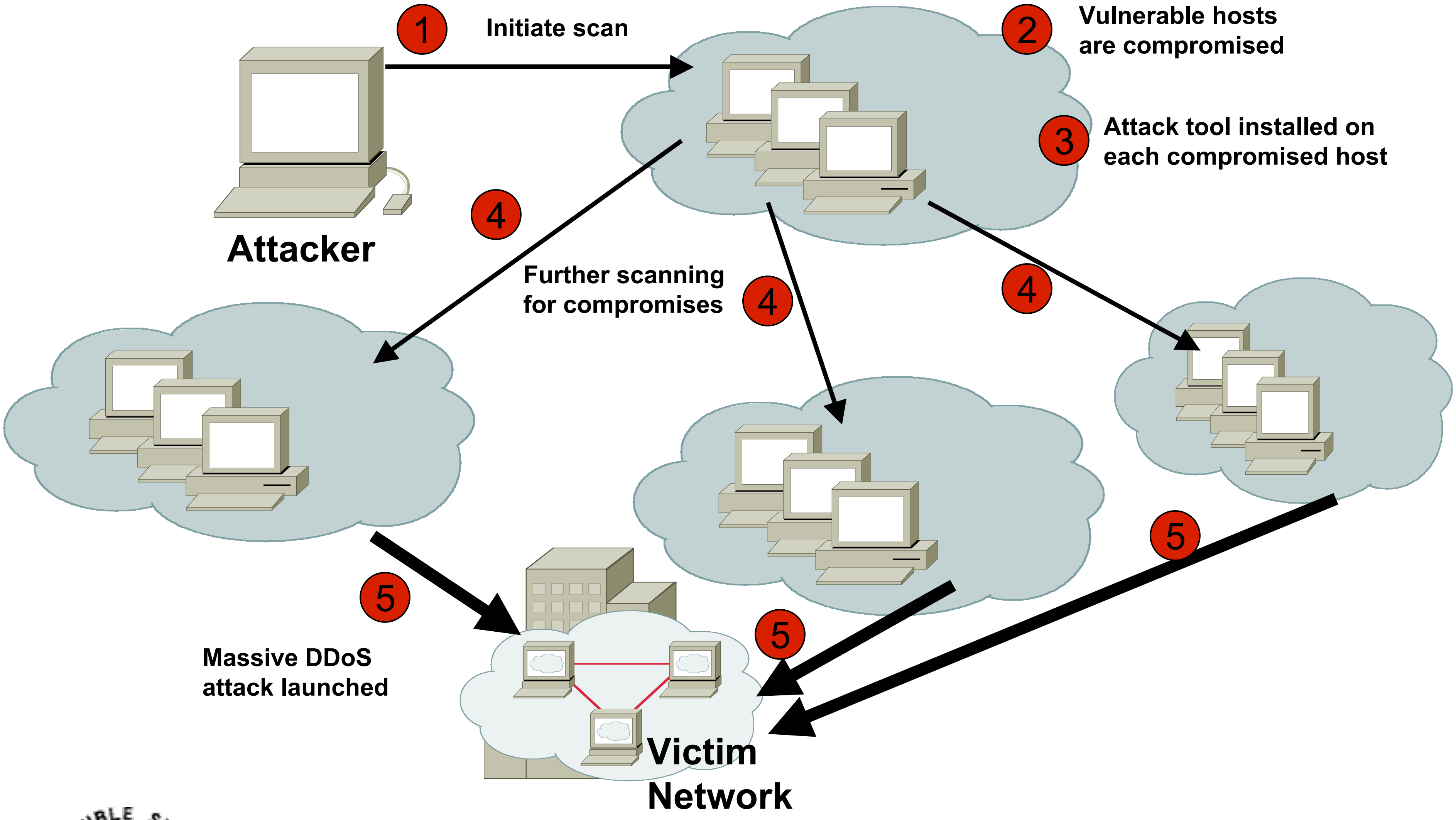
DDoS Is A Huge Problem

- Distributed and/or coordinated attacks
  - Increasing rate and sophistication
- Infrastructure protection
  - Coordinated attack against infrastructure
  - Attacks against multiple infrastructure components
- Overwhelming amounts of data
  - Huge effort required to analyze
  - Lots of uninteresting events

Basics of a DDoS Attack



Automated DDoS Attack



Initiate scan

Vulnerable hosts are compromised

Attack tool installed on each compromised host

Attacker

Further scanning for compromises

Massive DDoS attack launched

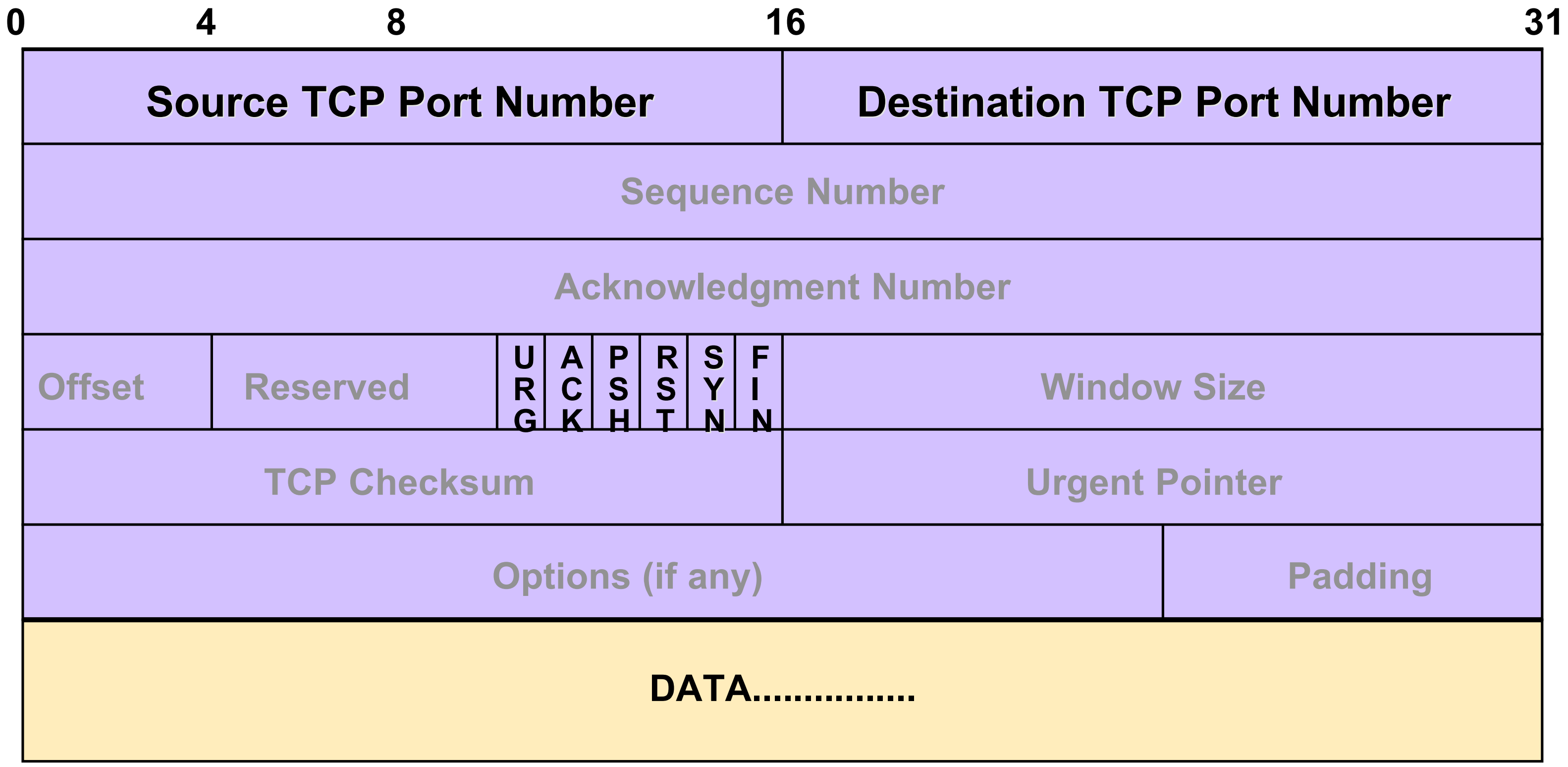
Victim Network

Types of DDoS Attacks

- TCP SYN
- TCP ACK
- UDP, ICMP, TCP floods
- Fragmented Packets
- IGMP flood
- Spoofed and un-spoofed

DoS Attack

Any traffic that causes disruption of service - protocol error exploitation or flooding of traffic



0 4 8 16 31

Source TCP Port Number | Destination TCP Port Number

Sequence Number

Acknowledgment Number

Offset | Reserved | URG | ACK | PSH | RST | SYN | FIN | Window Size

TCP Checksum | Urgent Pointer

Options (if any) | Padding

DATA................

What If Router Becomes Attack Target?

It allows an attacker to:

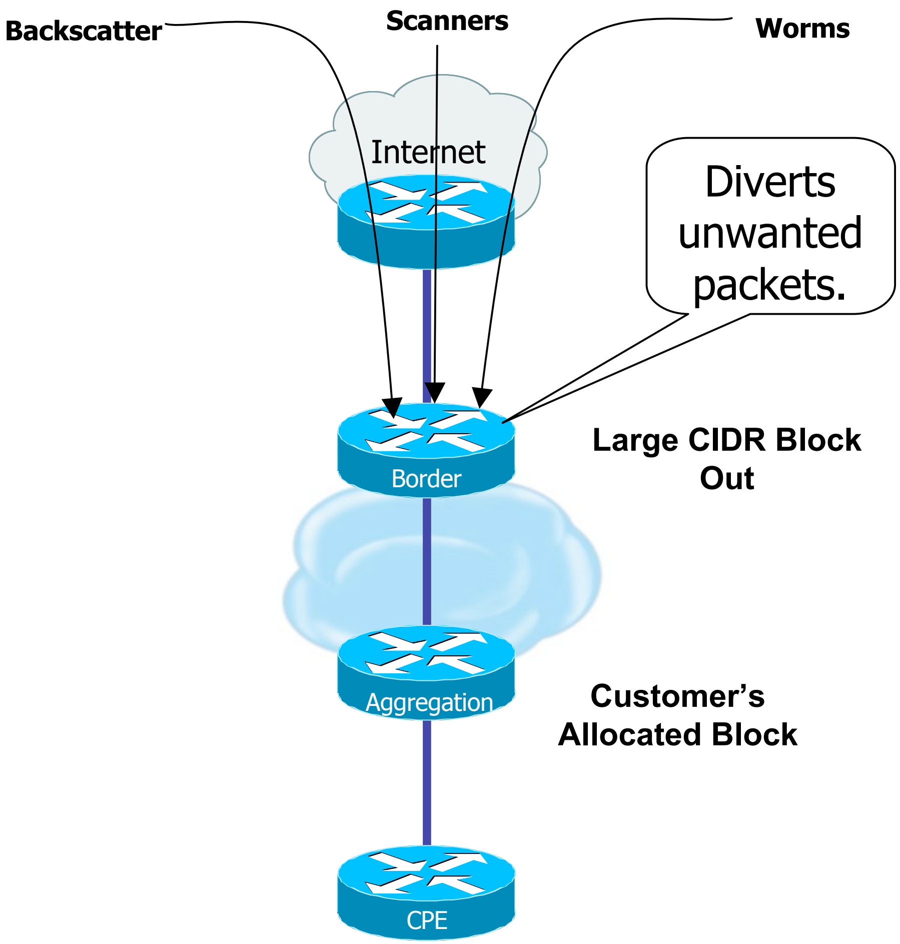
- Disable the router & network…
- Compromise other routers…
- Bypass firewalls, IDS systems, etc…
- Monitor and record all outgoing an incoming traffic…
- Redirect whatever traffic they desire…

Router CPU Vulnerabilities

- Attacks on applications on the Internet have affected router CPU performance leading to some BGP instability
- 100,000+ hosts infected with most hosts attacking routers with forged-source packets
- Small packet processing is taxing on many routers…even high-end
- Filtering useful but has CPU hit

DoS Tracking / Mitigation (Sink Hole)

- Router or workstation built to *divert traffic* and assist in analyzing attacks and determine the source.
- Used to redirect attacks away from the customer – working the attack on a router built to withstand the attack.
- Used to monitor *attack noise, scans, data from mis-configuration* and other activity (via the advertisement of default or unused IP space)



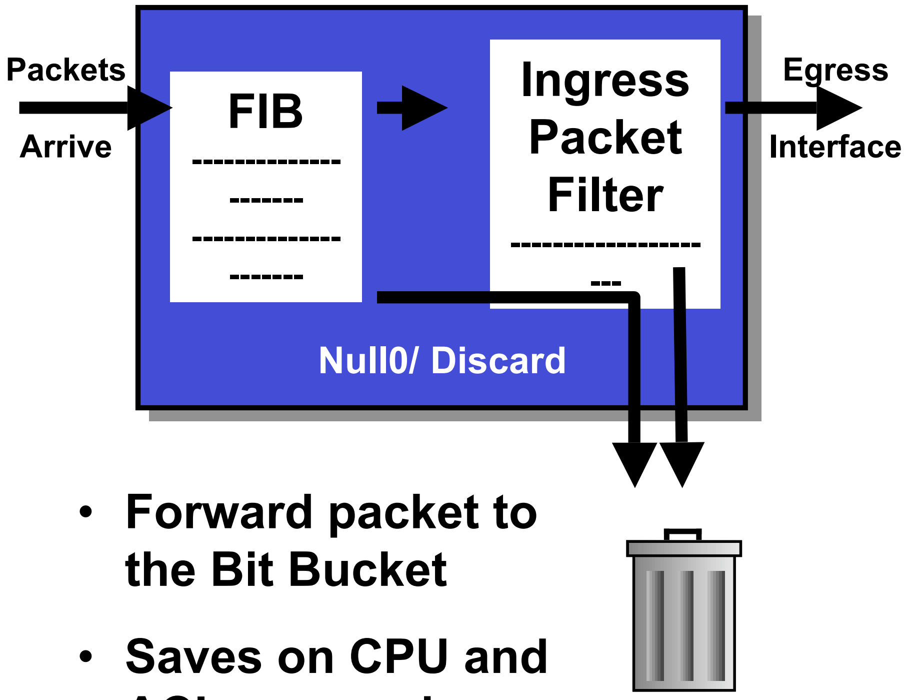
Diverts unwanted packets.

Large CIDR Block Out

Customer's Allocated Block

DoS Tracking / Mitigation
(Black-Hole Triggered Routing)

- Several Techniques:
  - Destination-based BGP Blackhole Routing
  - Source-based BGP Blackhole Routing (coupling uRPF)
  - Customer-triggered
- Exploits router's forwarding logic which typically results in desired packets being dropped with minimal or no performance impact
  - Packets forwarded to NULL interface

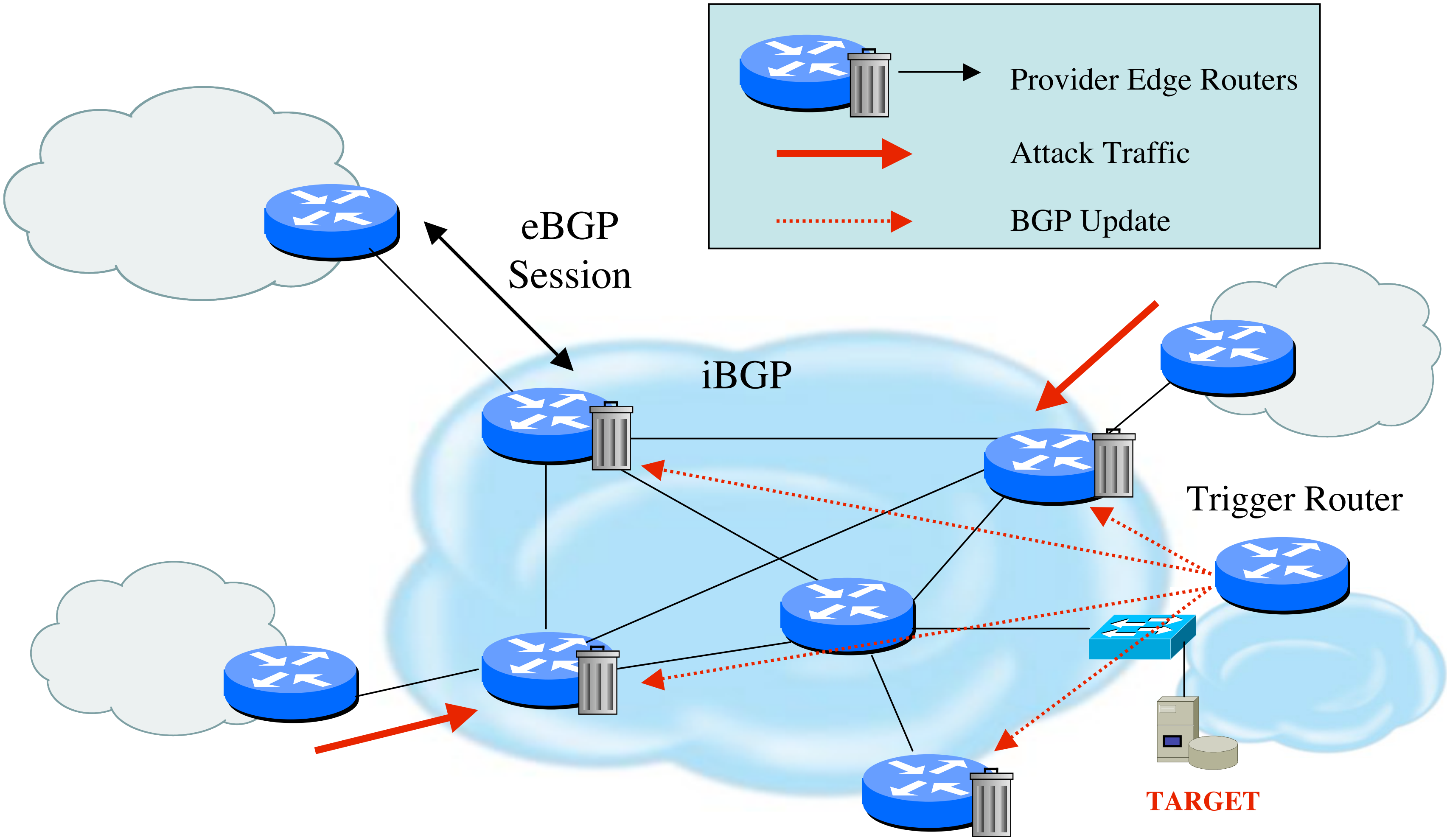


- **Forward packet to the Bit Bucket**
- **Saves on CPU and ACL processing**

RTBH Basics

- Use BGP routing protocol to trigger network wide response to an attack flow.
- Simple static route and BGP allows ISP to trigger network wide black holes as fast as iBGP can update the network.
- Unicast RPF allows for the black hole to include any packet whose source or destination address matches the prefix.
- Effective against spoofed and valid source addresses.

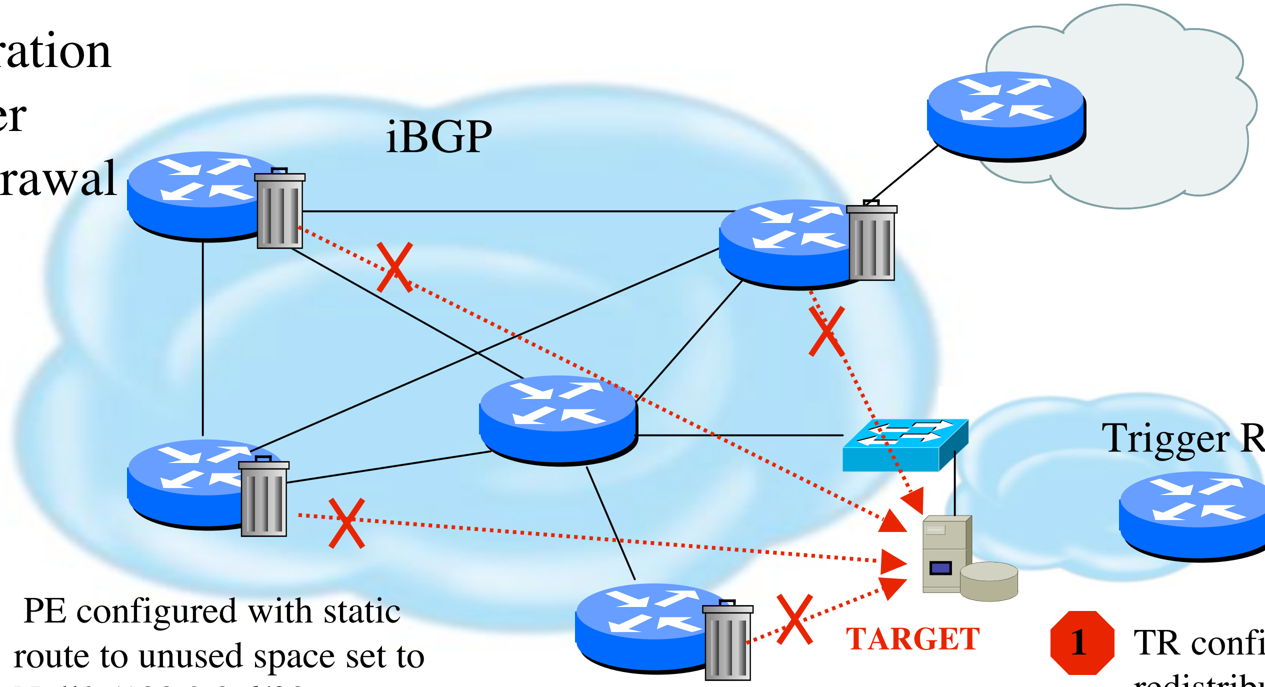
RTBH in the Network



Destination-Based RTBH

Steps:

1. Preparation
2. Trigger
3. Withdrawal



1 PE configured with static route to unused space set to Null0 (192.0.2.6/32 set to Null0)

2 Receives iBGP update which states next hop for target is 192.0.2.6/32

3 Installs new (valid) route to target

N OTE: All traffic to the target is dropped, even legitimate traffic

1 TR configured to redistribute static into every iBGP peer

2 Add static route which sets next hop to target destination (192.0.2.6)

3 Manually remove static route which causes BGP route withdrawl

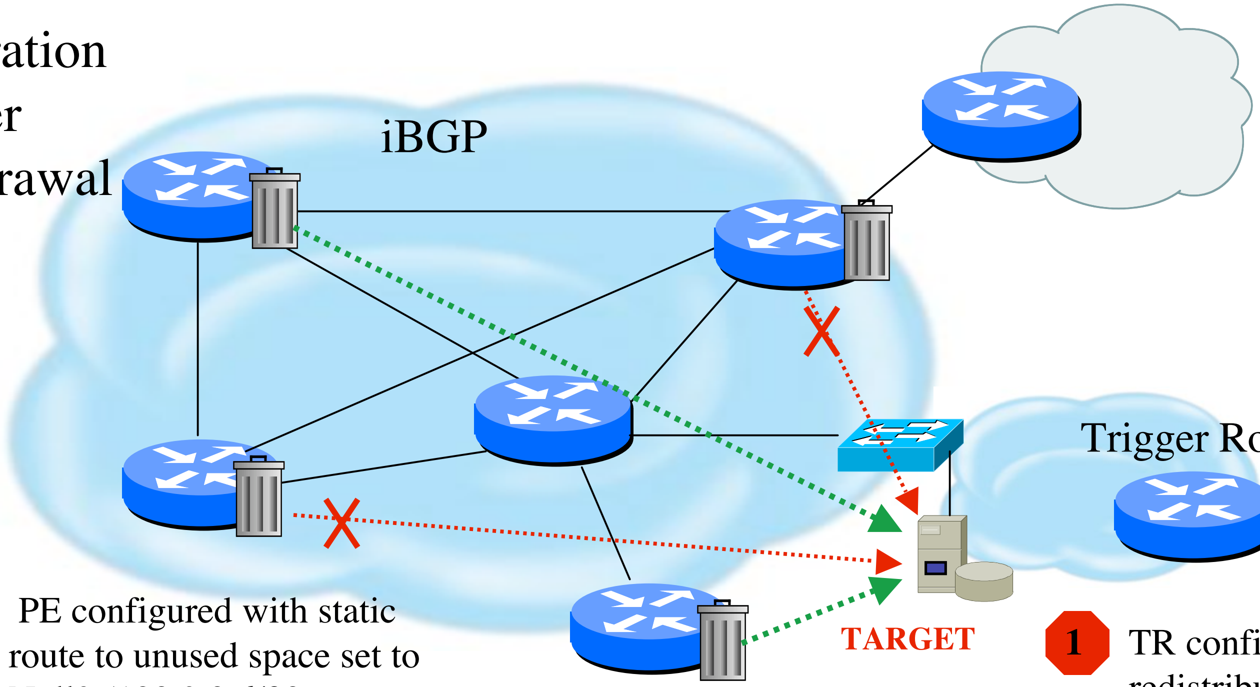
Source-Based RTBH

- Ability to drop packets at network edge based on specific source address
- Permits legitimate traffic from reaching target destination
- Depends on uRPF
- Packet dropped if:
  - If router has no entry for source IP address
  - If source IP address entry points to Null0

Source-Based RTBH

Steps:

1. Preparation
2. Trigger
3. Withdrawal



1 PE configured with static route to unused space set to Null0 (192.0.2.6/32 set to Null0) and loose mode uRPF on external interfaces

2 Receives iBGP update which states next hop for target is 192.0.2.6/32. All traffic from source IP will fail loose uRPF check.

3 Installs new (valid) route to target

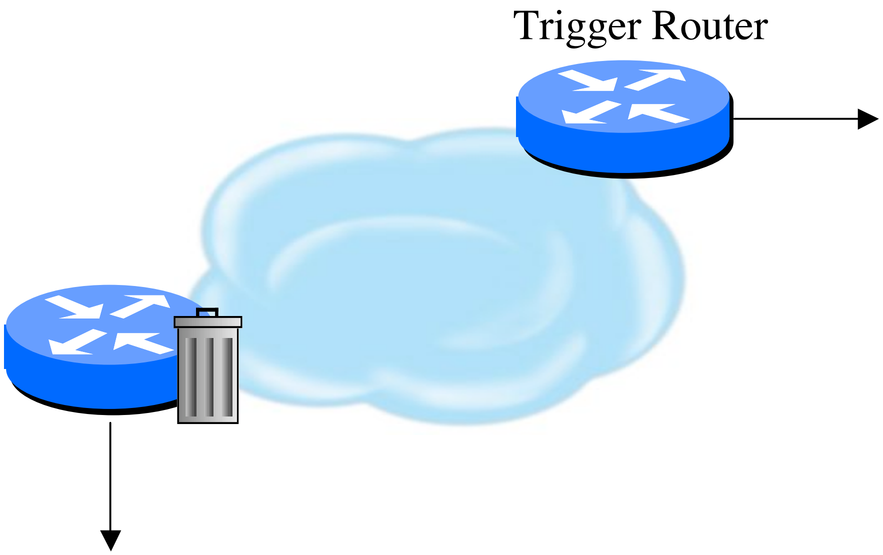
N OTE: Only traffic from the attack sources get dropped

1 TR configured to redistribute static into every iBGP peer

2 Add static route which sets next hop to target destination (192.0.2.6)

3 Manually remove static route which causes BGP route withdrawl

RTBH Configuration Example



```
interface Null0
! avoid backscatter traffic
no ip unreachables
!
router bgp 6665
redestributre static route-map bh-trig
!
route map bh-trig permit 10
  match tag 66
  set ip next-hop 192.0.2.1
  set local-preference 200
  set origin igp
! ensure edge router does not readvertise
! prefix to any eBGP peer
  set community no-export
!
! make sure no other static routes affected
! by the bh-trig route map
route-map bh-trig deny 22
!
! the manually configured trigger
ip route 192.168.33.0 255.255.255.0 null0 tag66
```

```
interface Null0
no ip unreachables
!
ip route 192.0.2.1 255.255.255.255 null0
```

Additional RTBH Considerations

- Avoid intentionally/unintentionally dropping legitimate traffic
- Deploy secure BGP features
  - Neighbor authentication
  - Prefix filters
  - ‘TTL hack’
- Use prefix filters at edge and trigger routers to ensure essential services (e.g. DNS) not black-holed by mistake

IPv4 vs IPv6

- Same considerations exist for IPv6 networks although the same tools are not yet there for IPv6 transports
- IPv6 / IPv4 tunnels used to hide malicious traffic from filtering rules is a concern
- Flow collection tools are not yet capable of detecting much malicious traffic

Operational Practices Summary

- Risk mitigation techniques similar yet different
  - Similar conceptual safeguards
  - Differences based on performance issues and operational complexity
- Infrastructure products need standardized capabilities for more effective security deployments

THANK YOU!

(draft-ietf-opsec-current-practices-07.txt)