# Securing Network infrastructure

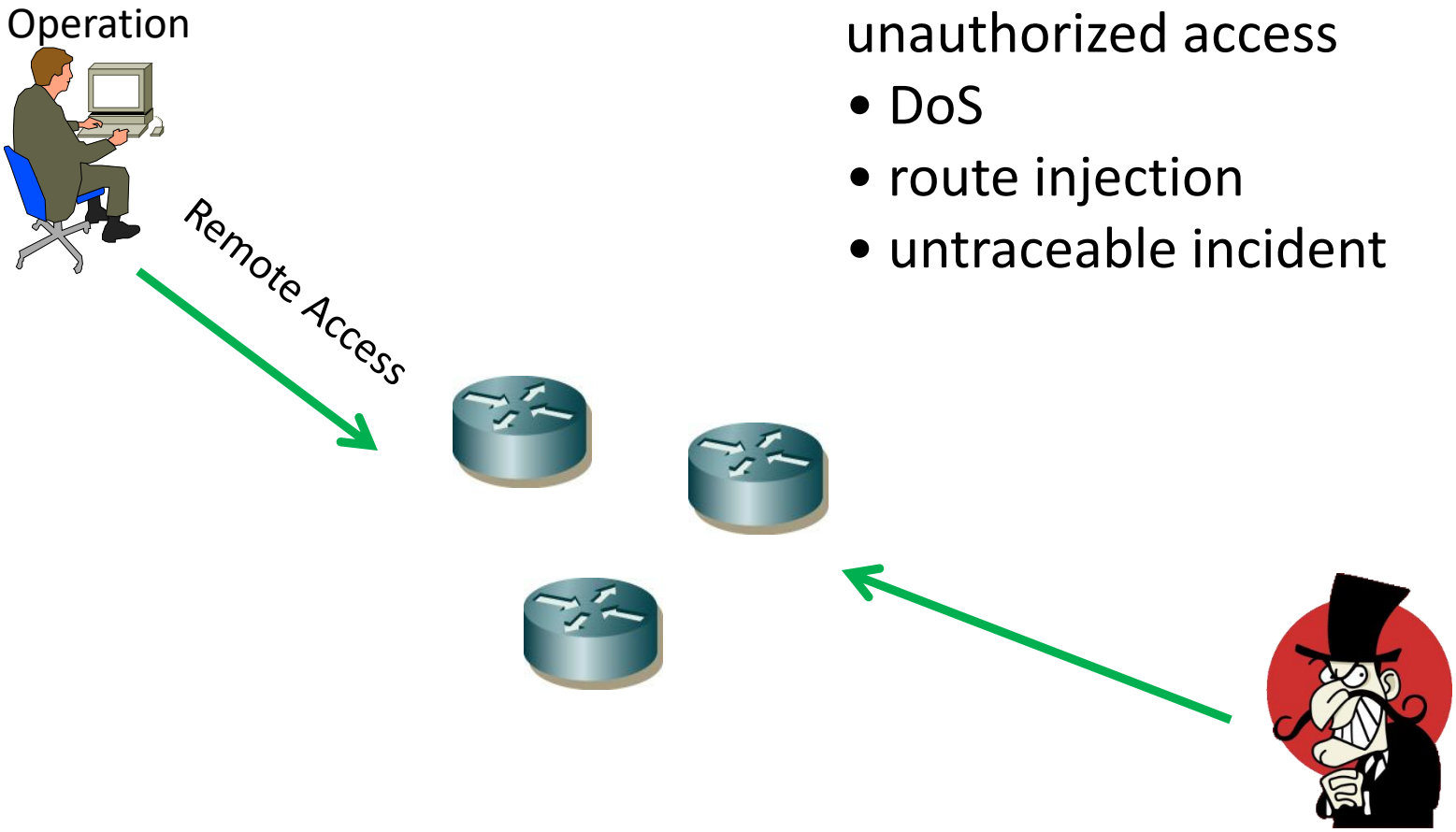
Slides taken from:

Matsuzaki ‘maz’ Yoshinobu

# Our Goals

- Ensuring Network Availability
- Controlling Routing Policy
- Protecting Information
- Preventing Misuse
- Mitigating Attacks
- Responding to Incidents
- etc.

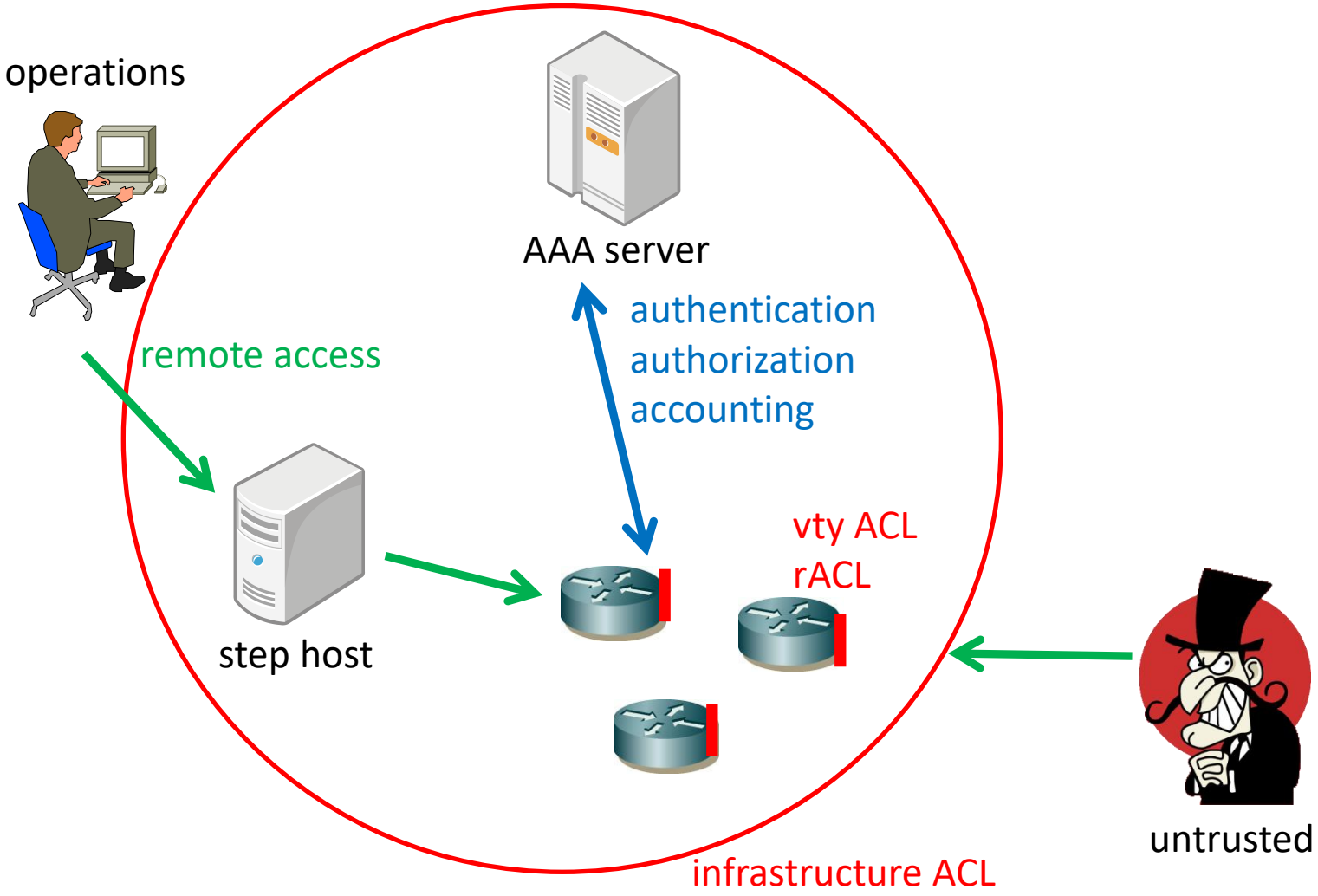
# RISKS




unauthorized access

- DoS
- route injection
- untraceable incident

# protecting devices



# AAA server and remote access

- Authentication, Authorization, Accounting
  - tacacs, radius
- each operators has own login account
  - You can set privileges per tasks of the operator
- logging at AAA servers
  - where (device)
  - who (login account)
  - what (command)

# Remote Access to Devices

- in-band access
  - vty, snmp, ntp, etc...
  - IP reachability is required
  - useful for daily operations
- out-of-band access
  - serial console
  - workable without IP reachability
  - useful for restoration

# Access Control for in-band access

- operations need to access remote devices

to manage the devices

- packet filtering on vty, snmp and etc

– to protect devices from unauthorized access

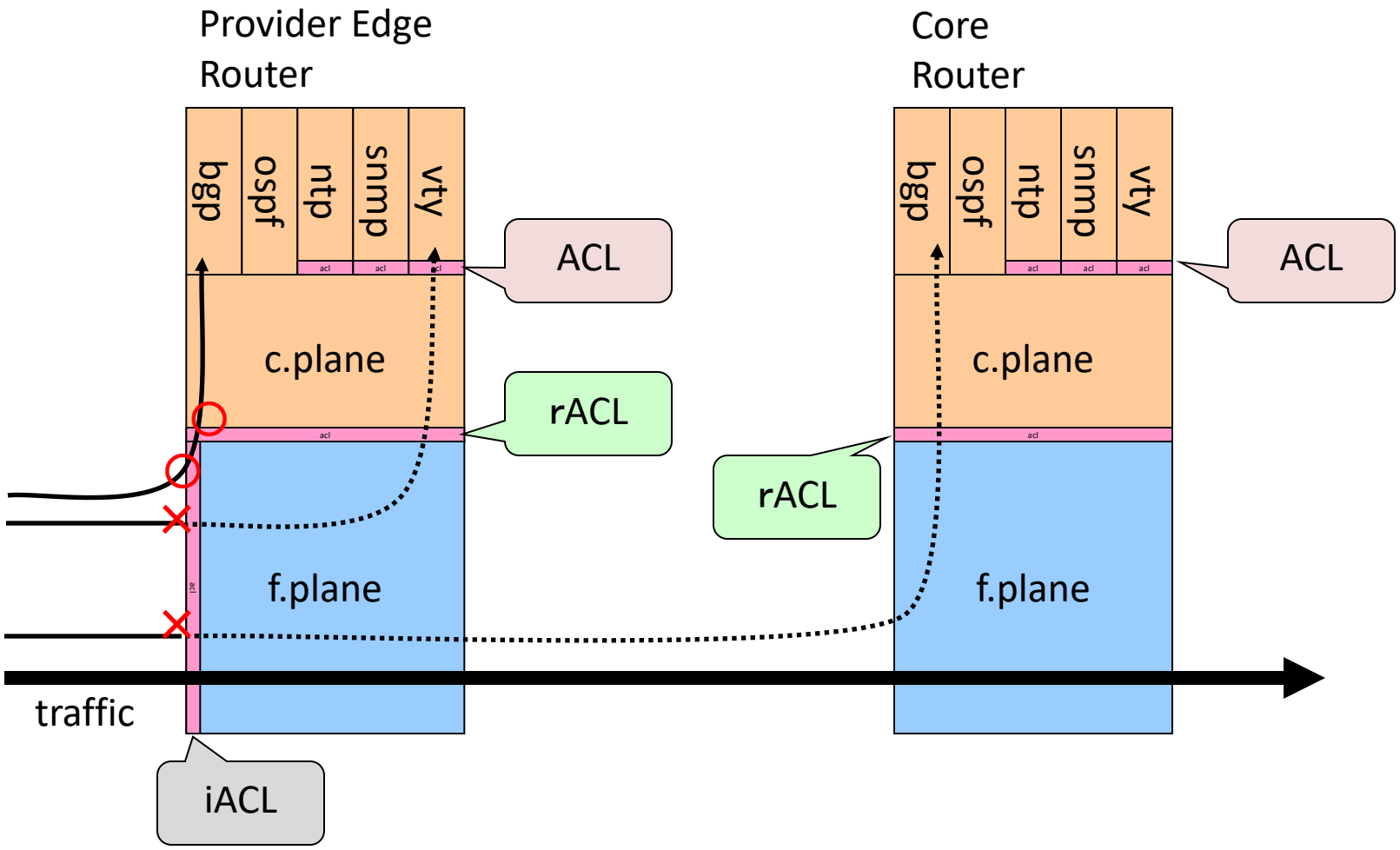
– allow access from trusted network only

    - source IP address based filtering

# Step Hosts

- are placed on a trusted network
- useful to enforce more restricted control
- each operations has own login account

# multiple ACLs to protect Devices

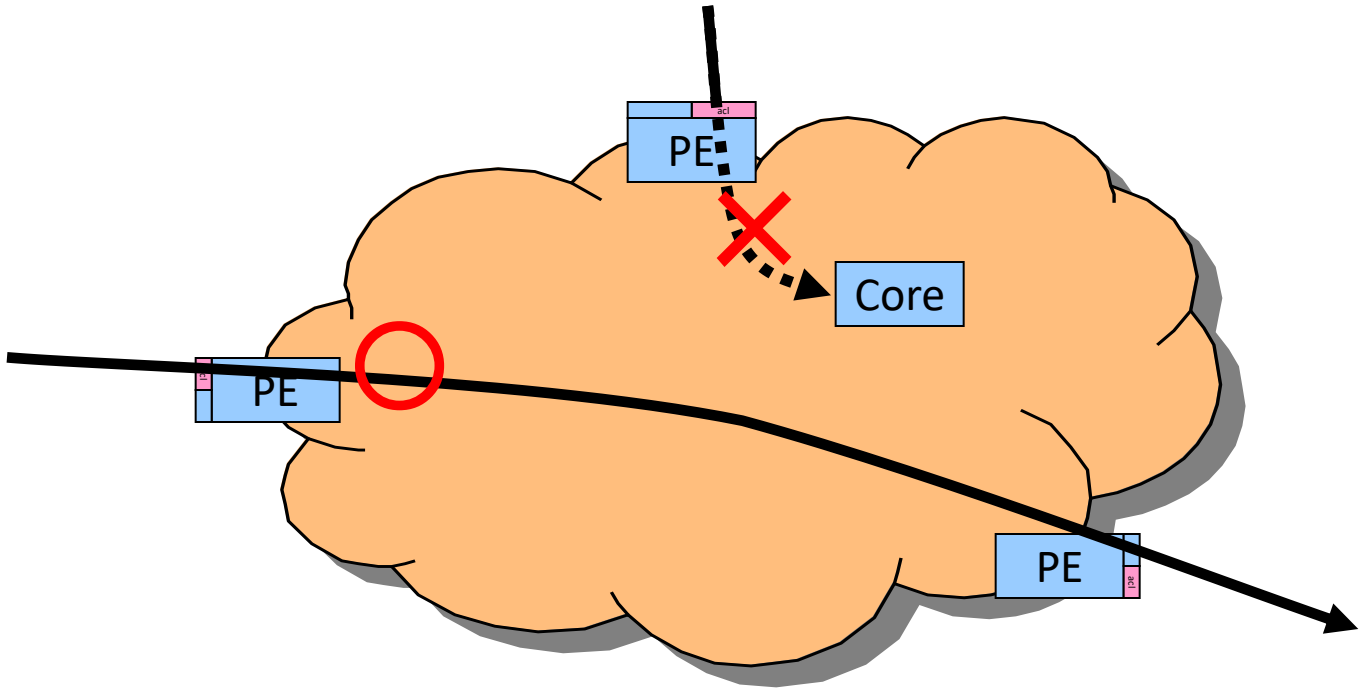


# Infrastructure ACL

- to protect our management traffic
  - not too much
  - ping, traceroute to our devices should be workable
- deny packets from INFRA and to INFRA on edge
  - INFRA: routers, step hosts and so on
    - these ip range should stay inside

# Infrastructure ACL (iACL)

- enforce a policy on the network edge



# Infrastructure Filters

- 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 filters

# Config Audit

- configuration files are periodically gathered
  - by in-house automated tool

- sanity check
  - filtering rules
  - routing configuration
  - and so on

# Monitoring

- what's happened in the past
- syslog
  - to record messages from devices/softwares
- snmp
  - to monitor resources
- netflow
  - to monitor packet flows

# SYSLOG Messages

- Nov 9 15:19:14.390 UTC:config[65775]: %MGBL-SYS-5-CONFIG_I :Configured from console by maz on vty0(2001:db8:120:100:e1dd:97f3:fd98:a51f)

- Nov 12 13:53:38 maz sudo: maz : user NOTin sudoers ; TTY=pts/3 ; PWD=/home/maz ;USER=root ; COMMAND=/bin/bash

# Synced Timestamp

- makes log messages useful
  - to compare incidents among devices
  - to compare time-related events
- Use ntp to sync clocks
  - choose a proper clock source
- national ntp server
- stable clocks
  - ATOM, GPS

# Clock = Oscillation + Counter

- TAI = weighted average of atom clocks
  - TAI: International Atomic Time
- UTC = TAI + leap seconds
  - UTC: Coordinated Universal Time
  - leap seconds: to adjust clock to Earth's rotation
- atom clocks are adjusted to TAI
- localtime = UTC + timezone (+ summer time)

# Leap Second

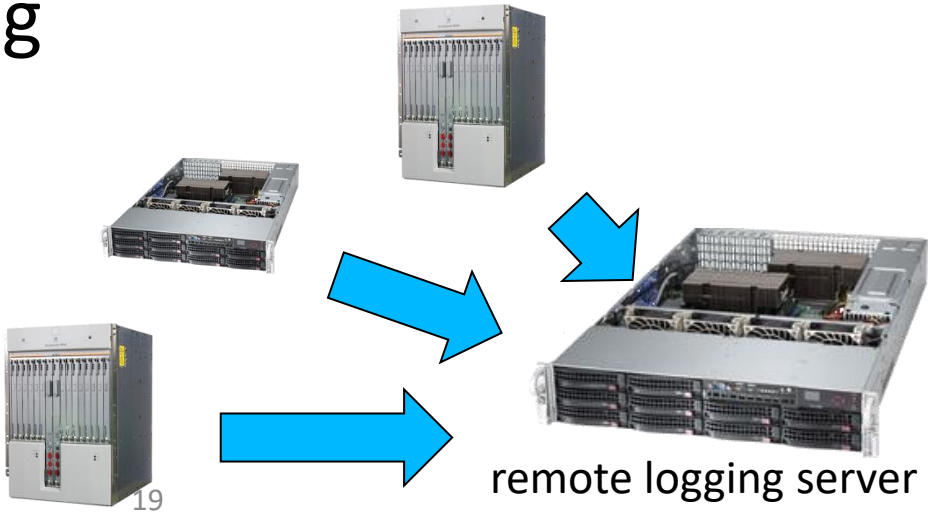
- Based on current predictions, the next leap second should be added on June 30, 2020.

- make sure your applications works as usual even the leap second introduced

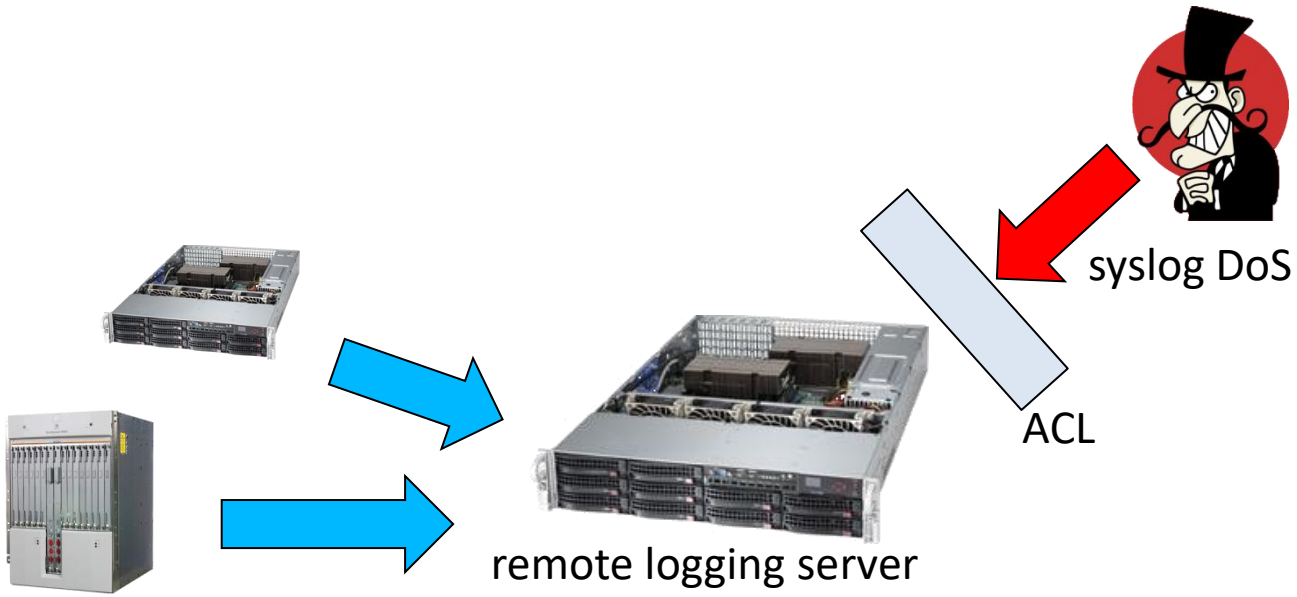
https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6b43ae8a619d17c4935c3320d2ef9e92bdeed05d

# remote logging

- log messages could be modified/deleted
- - if the system is compromised
- remote logging servers
- - receive log messages from other devices
- - syslogd/syslog-ng



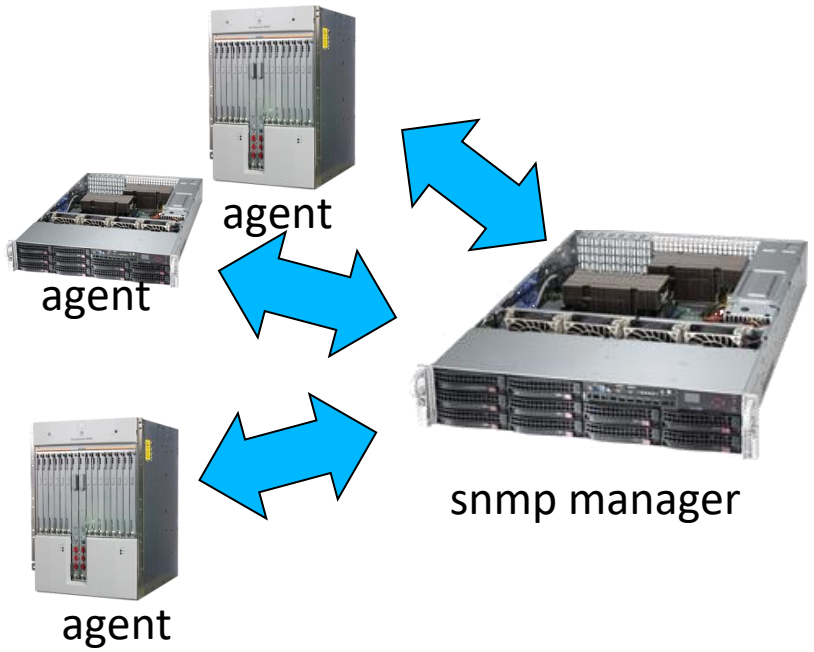
# protecting syslog



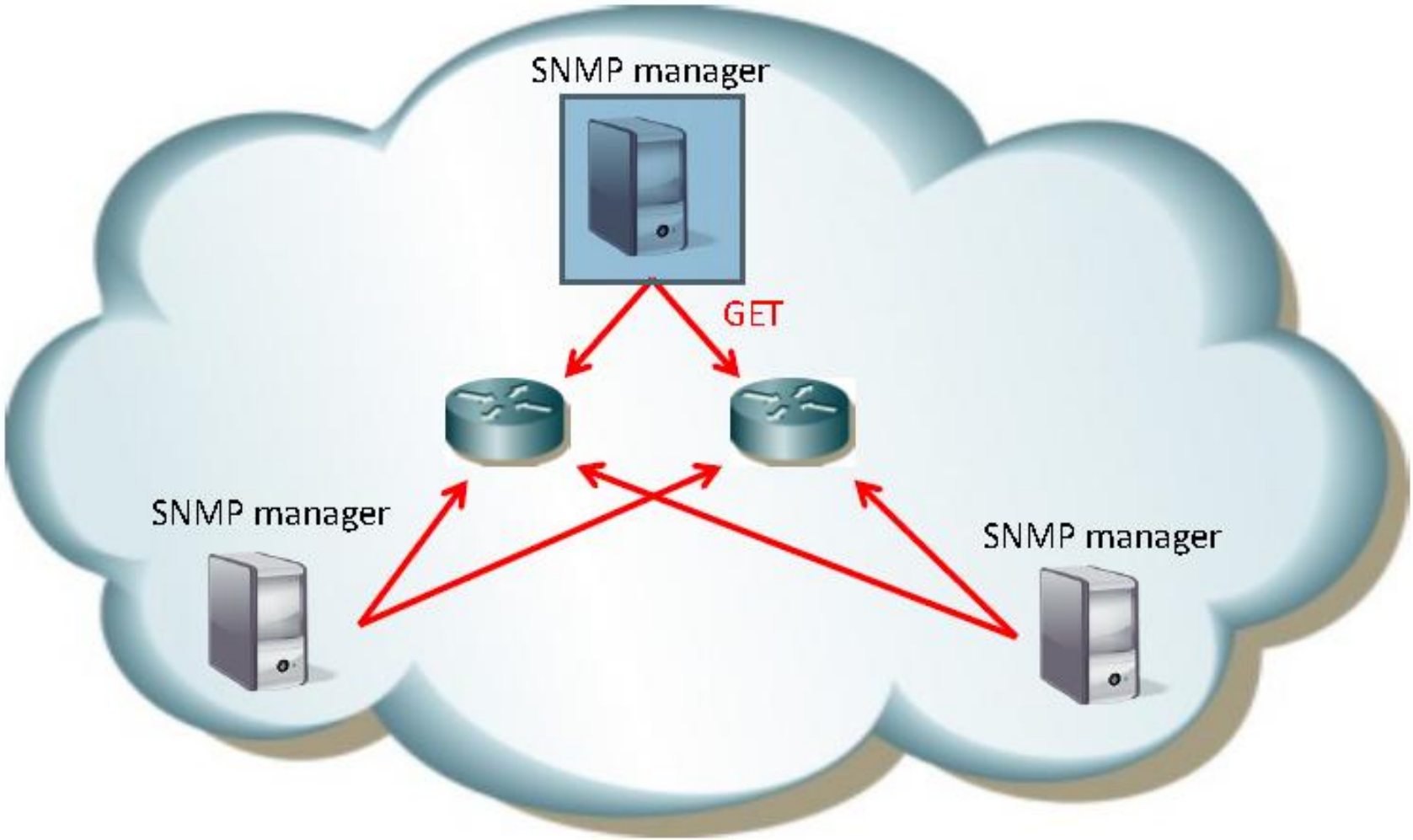

ensure the correctness of log entries

# SNMP

- can read/write information and send a trap
- - use version 3, and set password
- - prevent ‘write’ function, or just disable it on agents
- - snmp agent/manager



# snmp monitoring system



# SNMP Counters

- frequency of updating counters
  - depends on agents (0-30sec)
  - 5min is widely used as snmp polling time
- counter overflow
  - 32bit counters(ifIn/OutOctets) could wrap in 5.7min at 100Mbps
  - consider 64bit counters(ifHCInOctets) for 1Gbps or more interfaces

# Useful information via SNMP MIBs

- interface
  - bytes, packets, errors
- system
  - cpu load
  - memory usage
  - temperature
  - icmp, udp
  - ntp

# SNMP Use Case

- usage monitoring
  - bandwidth and traffic volume
- visualize
  - stackable graph
- useful for multiple links between POPs
  - grouping
- international links

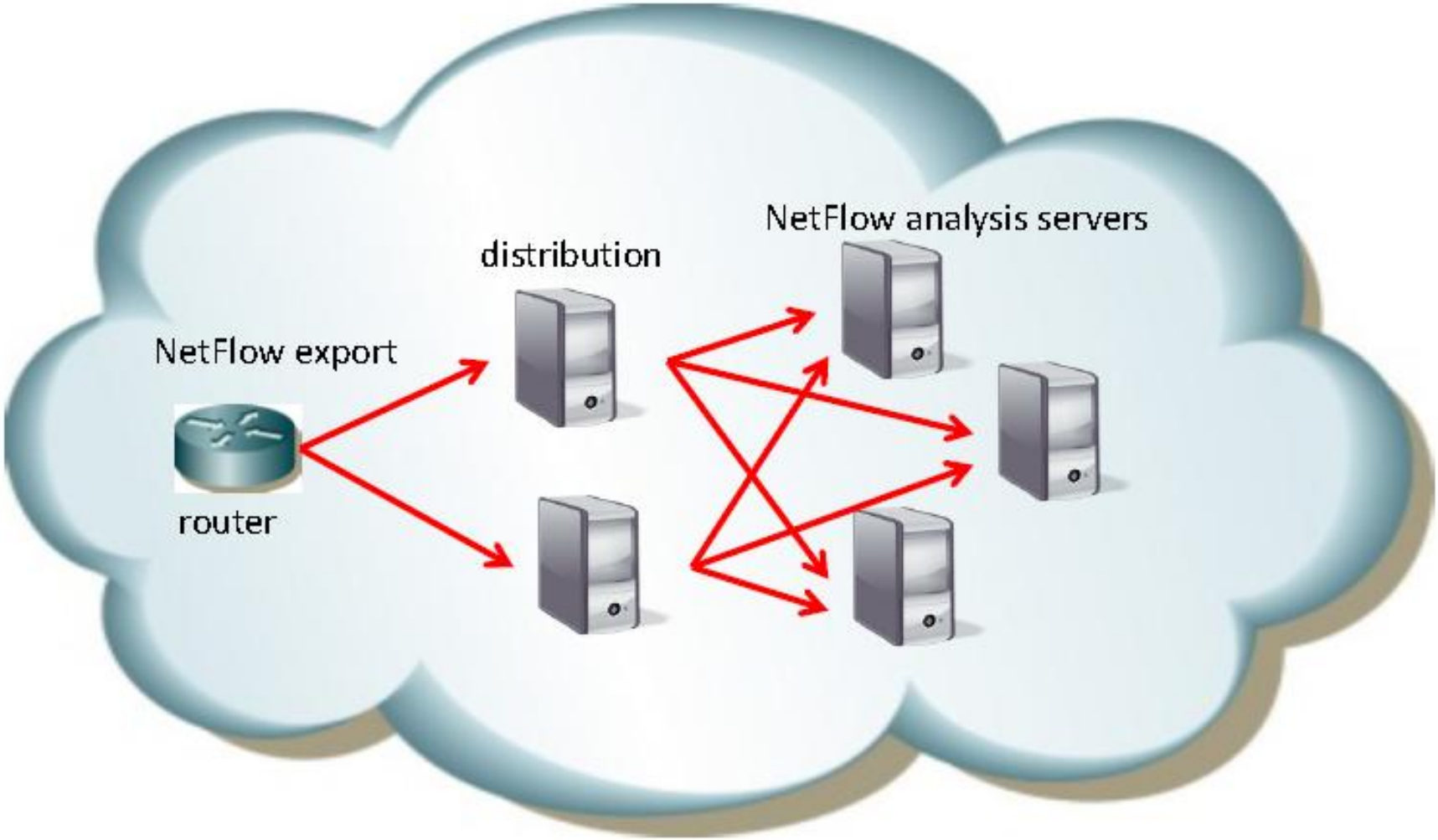
# Netflow

- to monitor flow information
  - packet header
  - most routers support it
- require more storage
  - even with sampling, still need to expect huge data
  - not for long term monitoring
- useful for analysis and anomaly detection

# Netflow and Sampling

- • sampled netflow is widely used
- – just to know trend
- – to reduce data
- • margin of error
- – sampled netflow and actual traffic
- – depends on routers
- – worst case: 20%
- • IIJ uses magic number as sampling rate
- – 1/16382

# netflow monitoring system



# Netflow Analysis

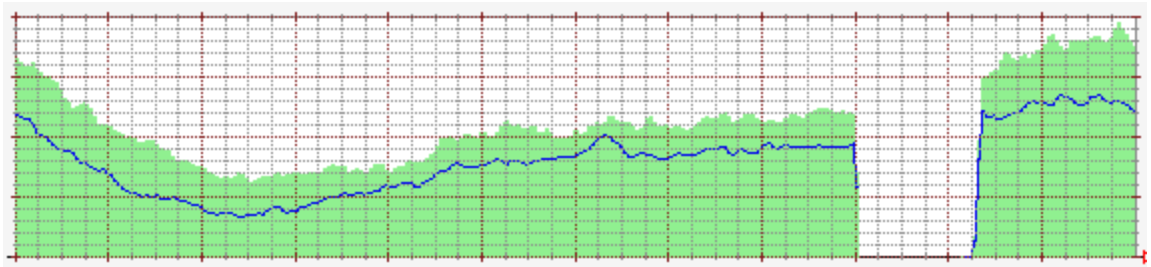
- combination of parameters
  - AS, IP address, protocol, port number
  - too many patterns to pre-generate every graphs

- Graphs
  - pre-defined graphs
  - dynamic graph system

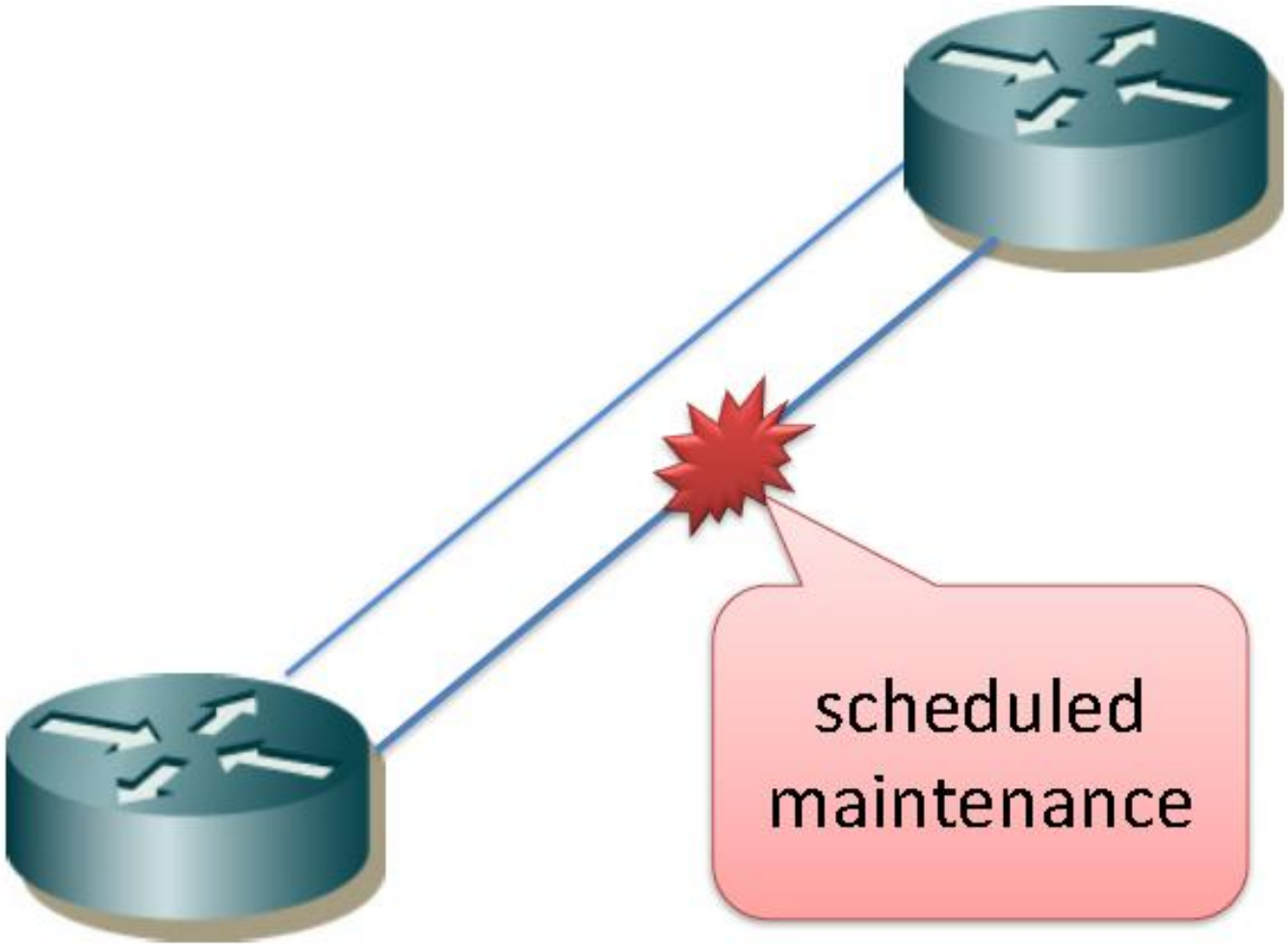
# case 1: bps

- traffic was suddenly doubled on a link

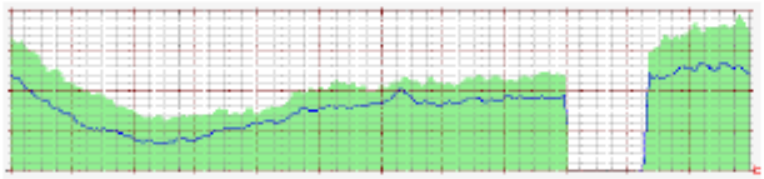
- also found a missing traffic

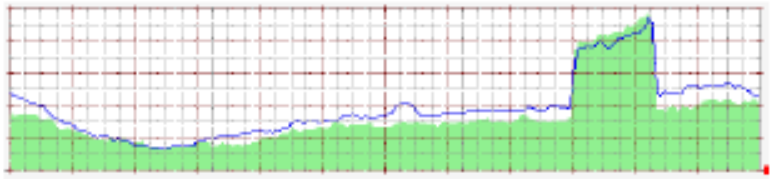


# case 1: 2 links between routers

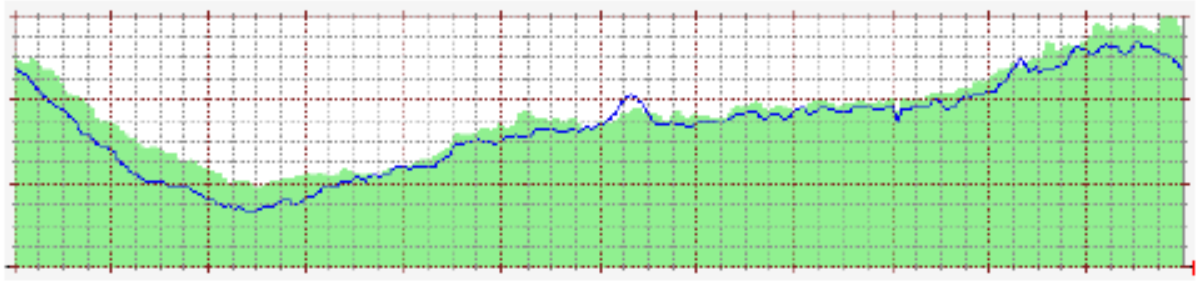


# case 1: total traffic: bps





merge

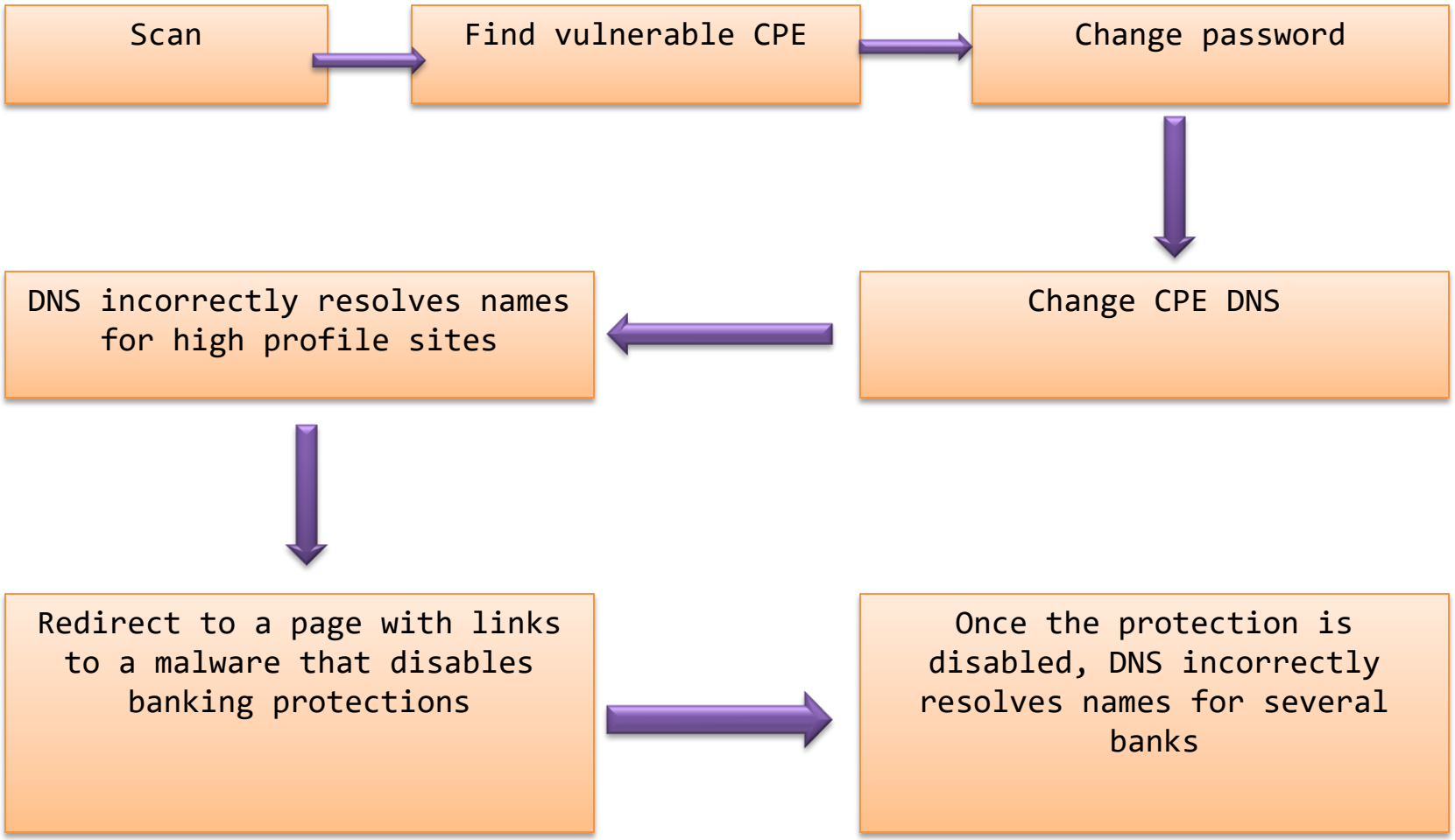


# Monitoring and Detection

- snmp is useful to check
  - trend
  - threshold

- netflow is useful to analysis
  - anomaly
  - change

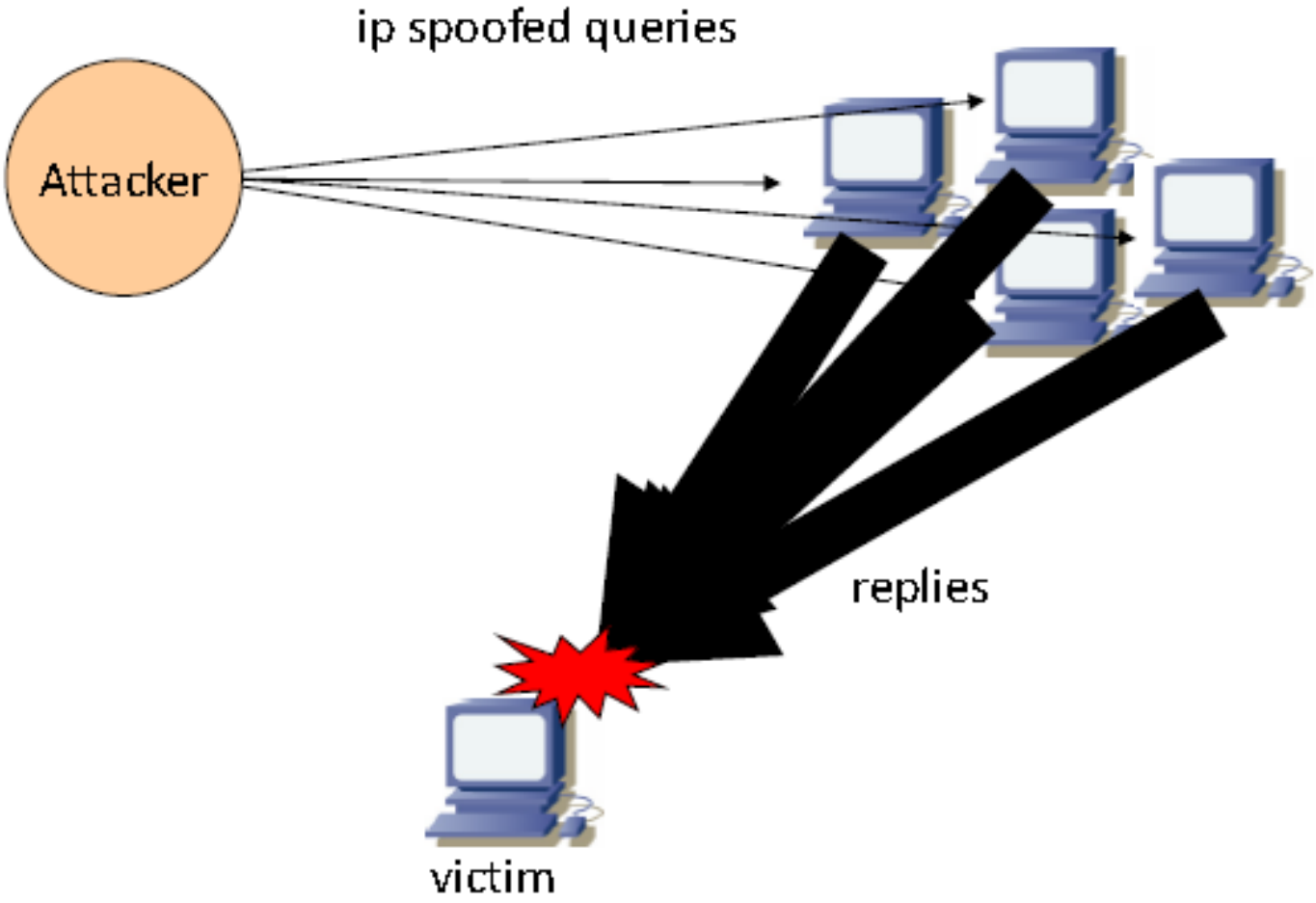
# Implication of CPEs Exploited



# Magnitude of Problem

- 4.5 Million CPEs (ADSL Modems) using a unique malicious DNS
- In early 2012 more than 300,000 CPEs still infected
- 40 malicious DNS servers found

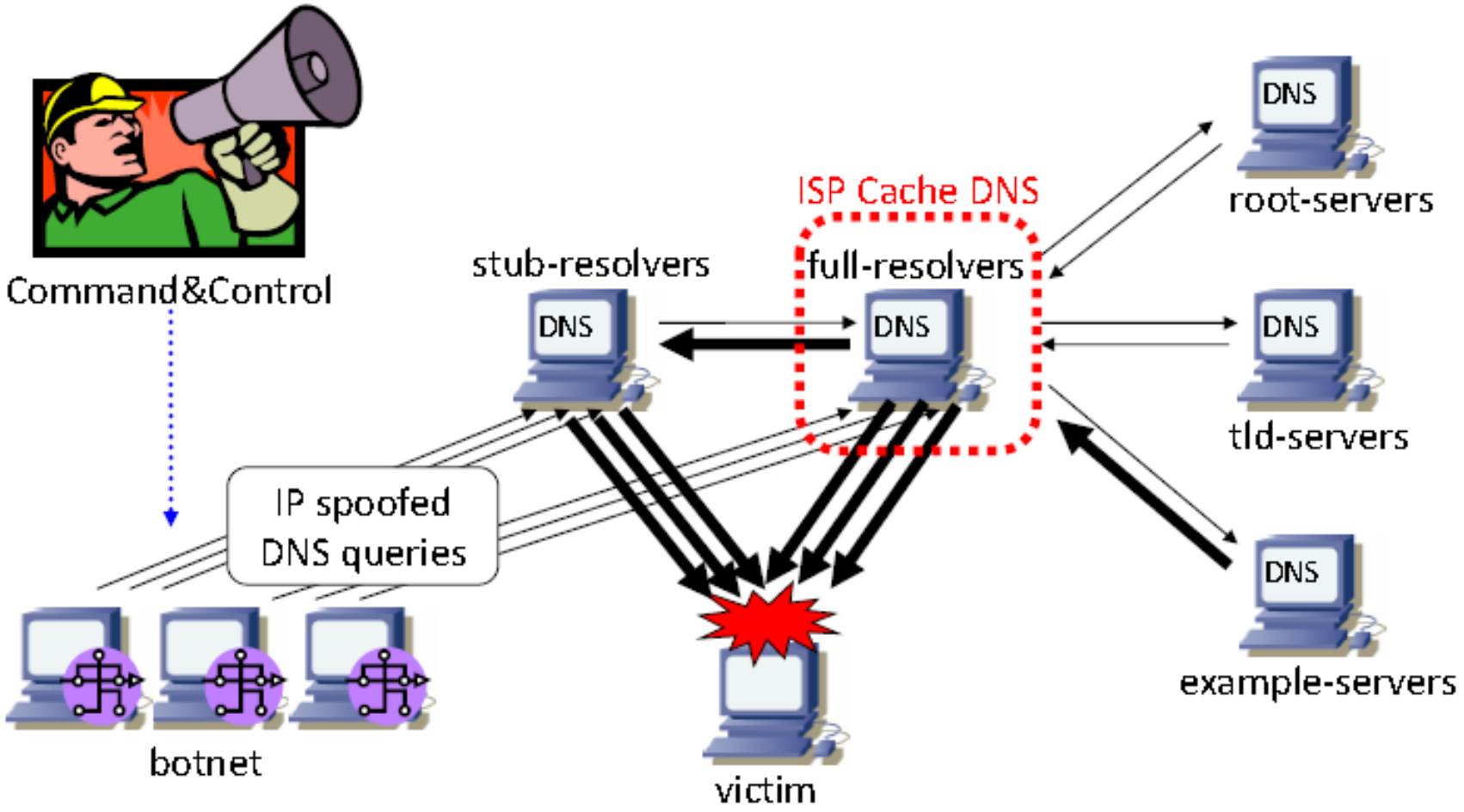
# reflection attacks



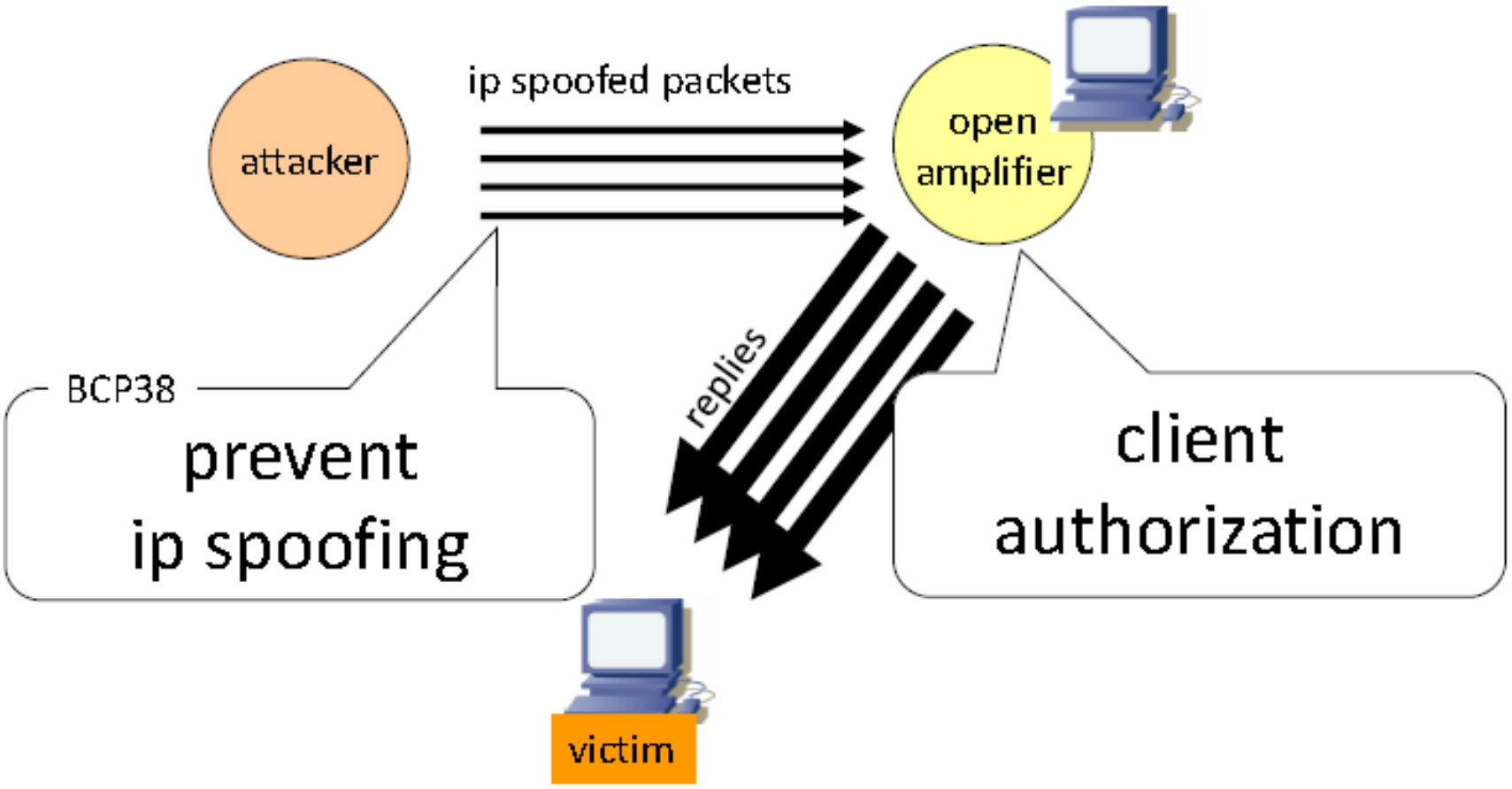
# Amplifiers

- dns amplification attack
  - a huge size record
  - amplification ratio: ~60
- ntp amplification attack
  - amplification ratio: ~200
- Memcached attack
  - amplification ratio: ~10K

# dns amp attack



# solutions against ip reflection attacks



# Client Authorization

- Incoming interface base
  - useful for home users and enterprises
  - allow from inside, deny from outside
- source IP address base
  - useful for service providers
  - allow from customer network
- you can simply disable the service if it’s not necessary

# RFC2827 (BCP38) – Ingress Filtering

- If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.
- The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).
- An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

# Guideline for BCP38

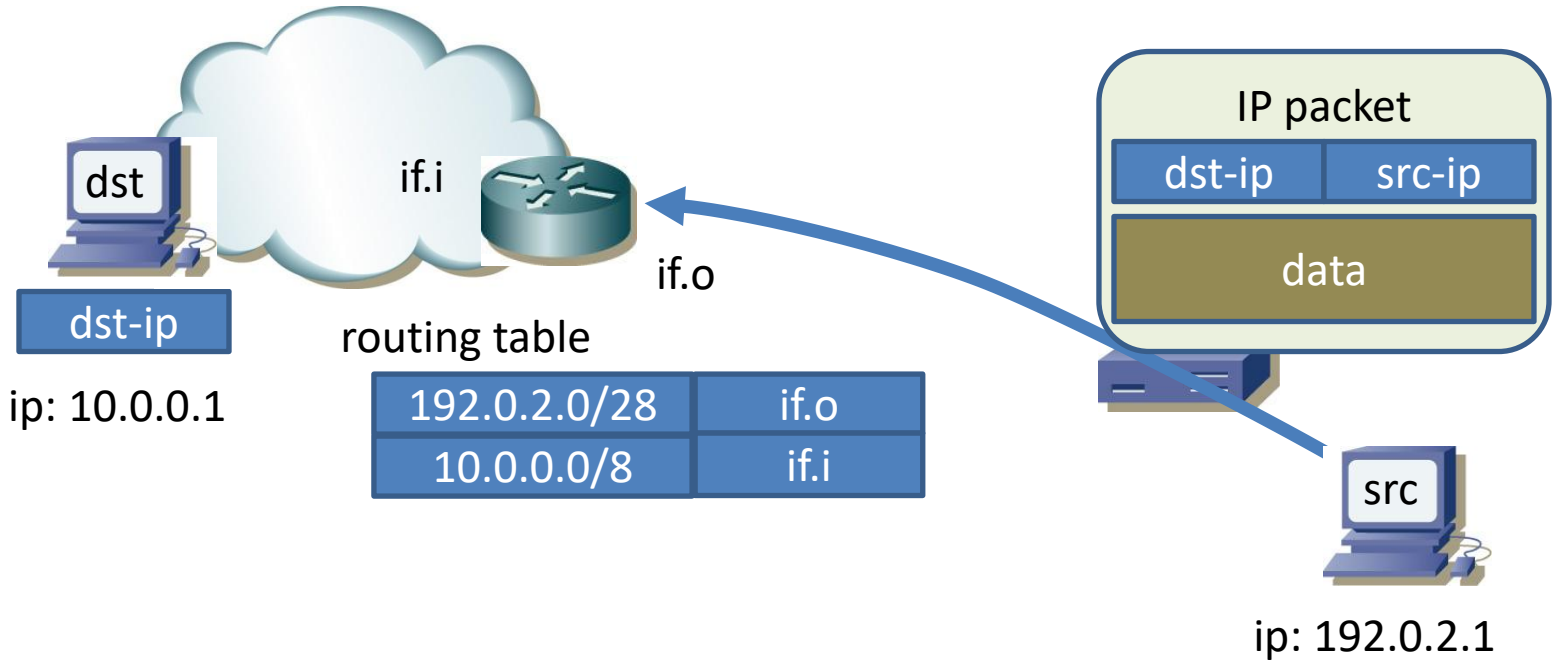
- Networks connecting to the Internet
  - Must use inbound and outbound packet filters to protect network
- Configuration example
  - Outbound—only allow my network source addresses out
  - Inbound—only allow specific ports to specific destinations in

# Techniques for BCP38

- Static ACLs on the edge of the network
- Unicast RPF strict mode

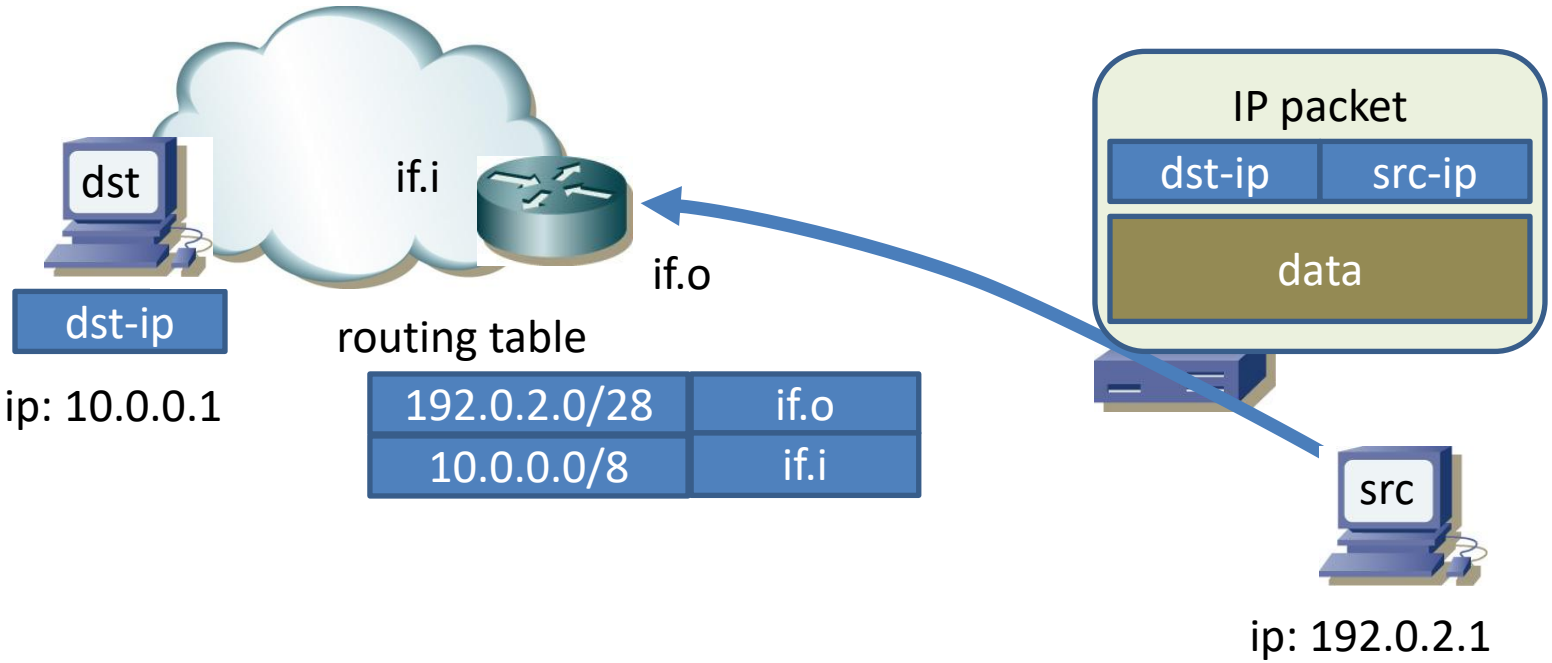
# packet forwarding – dst-ip based

- routing_table(dst-ip) => outgoing interface
  - lookup by 10.0.0.1 => if.i
  - then router forwards the packet



# uRPF – lookup by the src-ip

- routing_table(src-ip) => interface
  - lookup by 192.0.2.1 => if.o
  - The result MUST match the incoming interface



# Blackhole Routing

- routers are good at forwarding
  - not packet filtering
- use the forwarding function to discard packets
  - null routing

# Protecting Routing

- To keep your network working
  - as you designed
  - as you configured
- Static Routing
  - mostly depends on design
- Dynamic Routing
  - possibility of remote attacks

# Threat Model for Routing

- Neighboring Relationship
  - Unexpected Neighboring
  - Shutdown by Someone else
  - Spoofed Neighbor
- Routing Information
  - Propagation of Wrong Information
  - Unintended Routing Policy
  - Hit a Hardware Limitation

# OSPF Neighbors

- Establishing a relationship among trusted neighbors only
- Disabled by default
  - Especially on a link to other parties (IX,customer) to avoid unexpected neighbors

    if you have to enable on these links, use ‘passive’ feature
  - Enabled where it is needed like backbone
- Authentication
  - MD5 authentication (OSPFv2, RFC2328)

# BGP4 Neighbors

- Protecting TCP sessions
  - md5 authentication
- Peering with other parties
  - possibility of injection
  - needs more attention about routing information