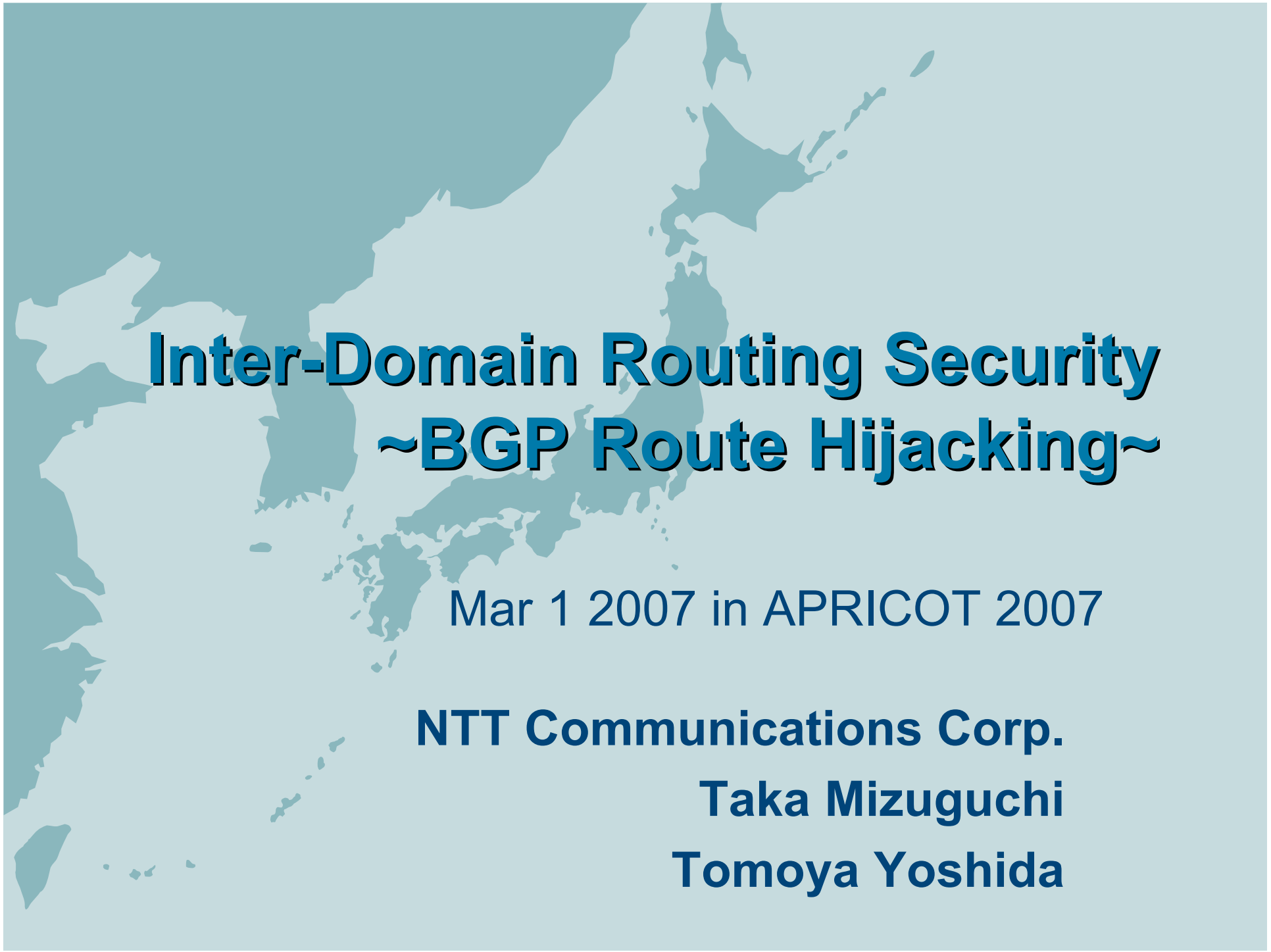


Inter-Domain Routing Security ~BGP Route Hijacking~

Mar 1 2007 in APRICOT 2007

NTT Communications Corp.

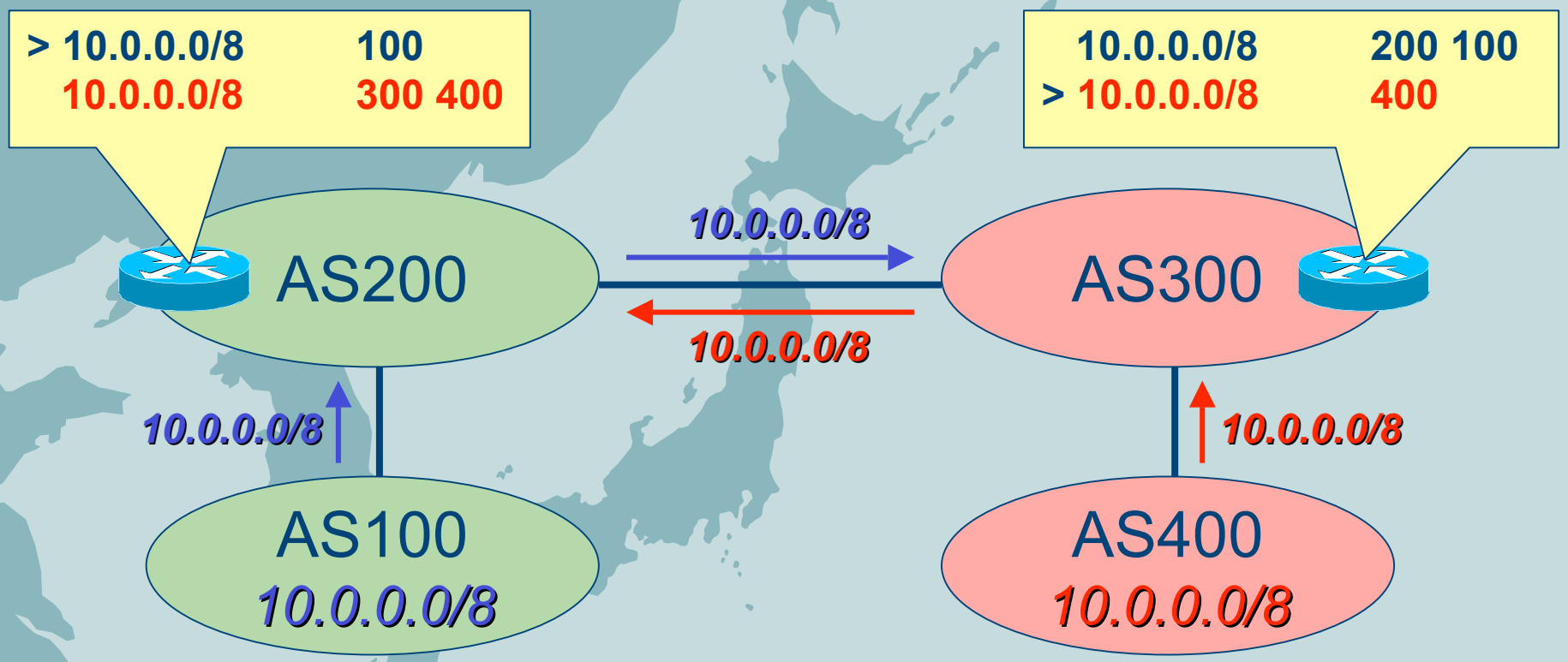
Taka Mizuguchi

Tomoya Yoshida

What's BGP Route Hijacking?

- Invalid BGP route announcement
- Traffic diverting by BGP route hijacking, unreachable…
- Detection is not so easy…
- Recovery is very hard…
- Not frequently, but it occurs
- Easy outbreak, but big impact
- Not only global, but localized outbreak

Definition of Hijacking



- AS100 is advertising their owned route(10.0.0.0/8) : *Victim AS*
- AS400 is advertising invalid route(10.0.0.0/8) : *Hijacking AS*
- AS300 is infected by Hijacking : *Infected AS*
- AS200 is Influenced but not infected by Hijacking : *Influenced AS*

Impact by Hijacking

- Network Unreachable/Service failure
  - Traffic divert to other network (Hijacked Network)
  - Service failure / Failure of Application
    - i.e. DNS: Root-server address hijacking
- Leak of Information
  - By traffic diverting and Packet capture
  - Looks like Phishing…
- Temporary hijacking
  - Generating DoS Traffic
  - Sending SPAM

Impact is not only infected network, but all other user can't access infected sites.

Type of Route Hijacking

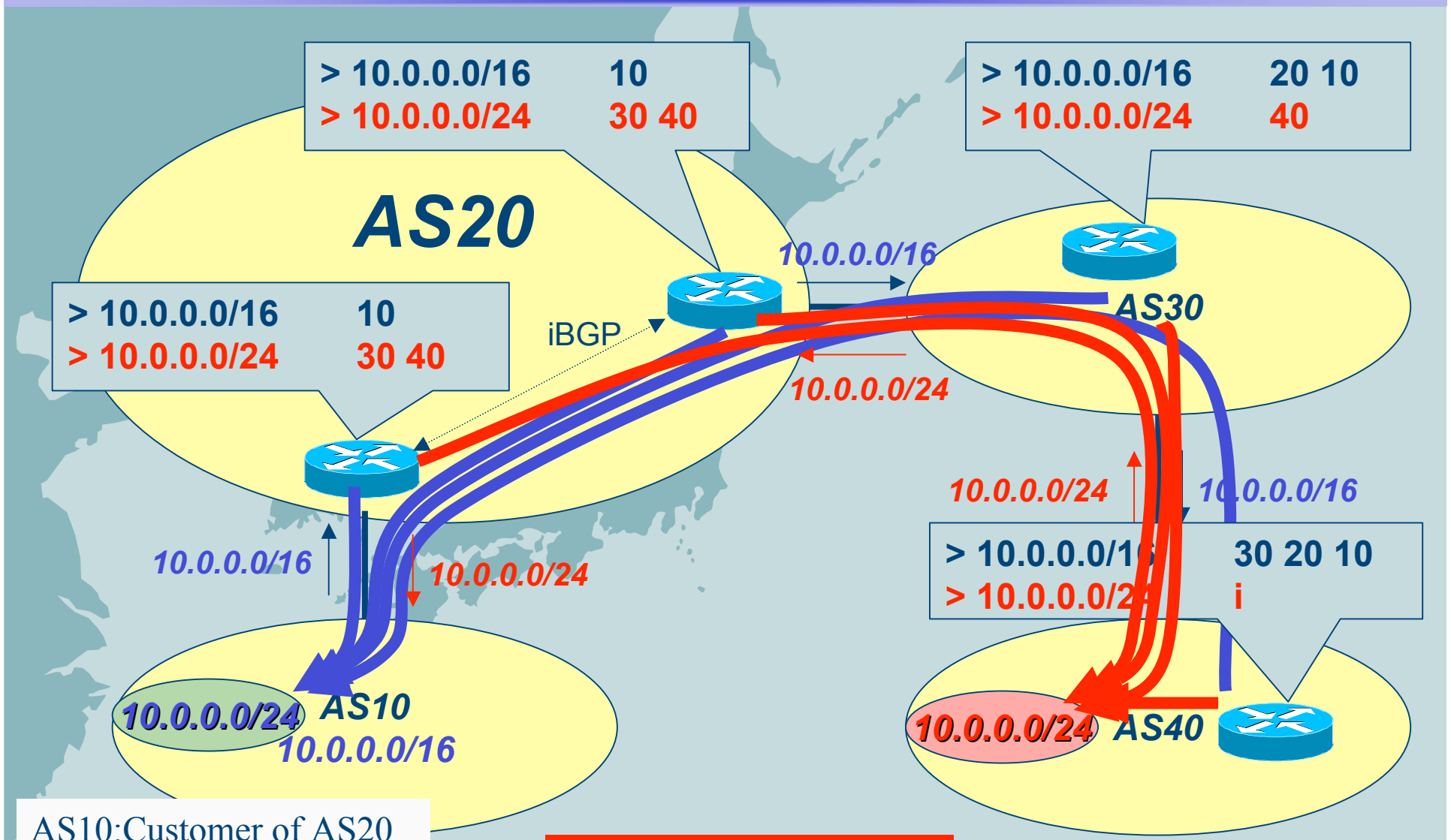
- Prefix Hijack
  - Valid: 10.0.0.0/16 10 i
  - Invalid: 10.0.0.0/16 40 i
- Sub-prefix Hijack
  - Valid: 10.0.0.0/16 10 i
  - Invalid: 10.0.0.0/24 40 i

Extent of the impact by BGP Route Hijacking

- Global impact
  - Invalid longer prefix advertisement
  - Detection is easy
- Local impact
  - Invalid same prefix advertisement
  - Invalid longer prefix, but filtered on peering link
  - Detection is hard
- No impact
  - Invalid shorter prefix advertisement
  - Detection is easy
  - Short lived BGP

    For spam/DoS sending, Phishing

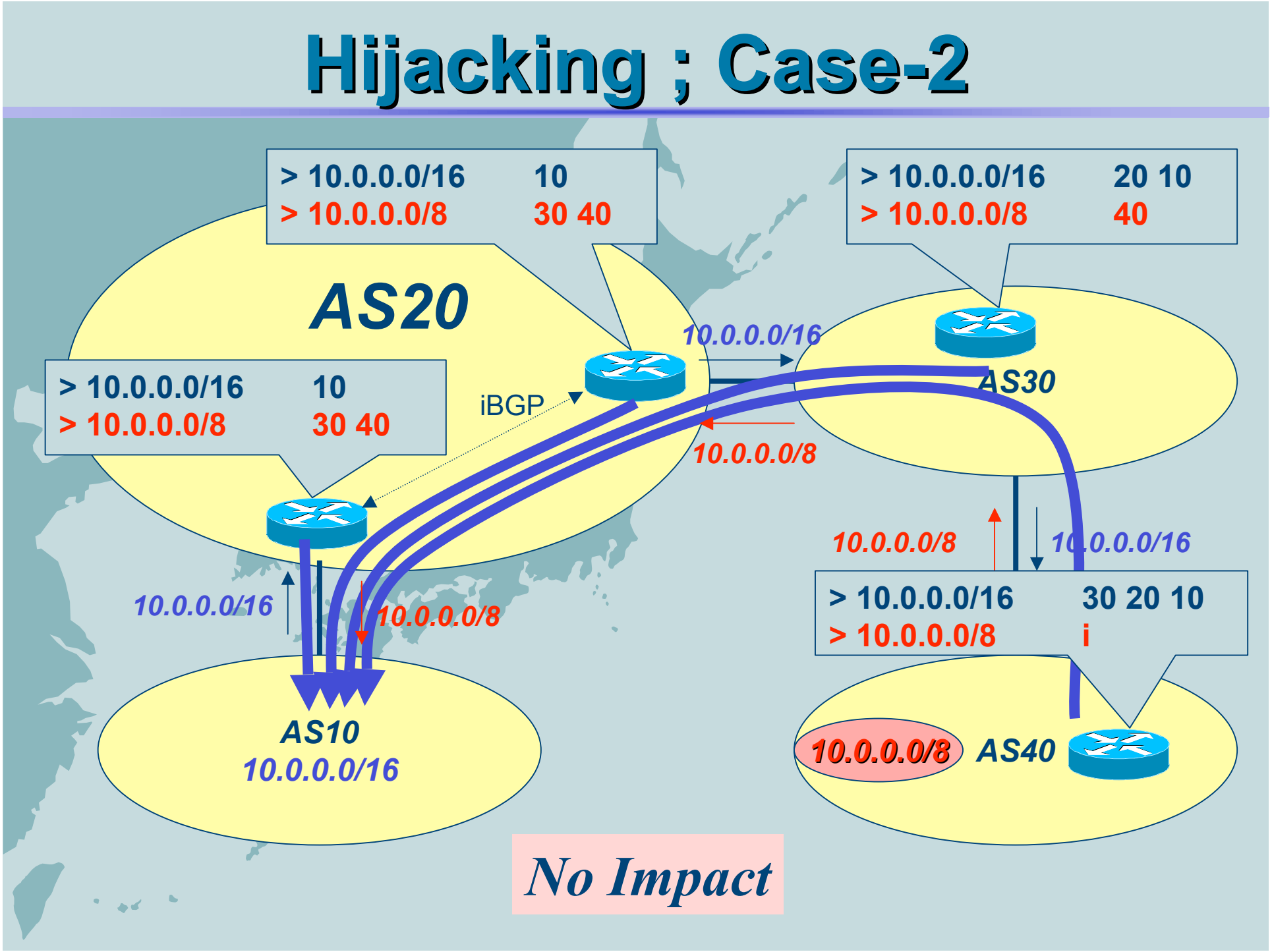
Hijacking ; Case-1



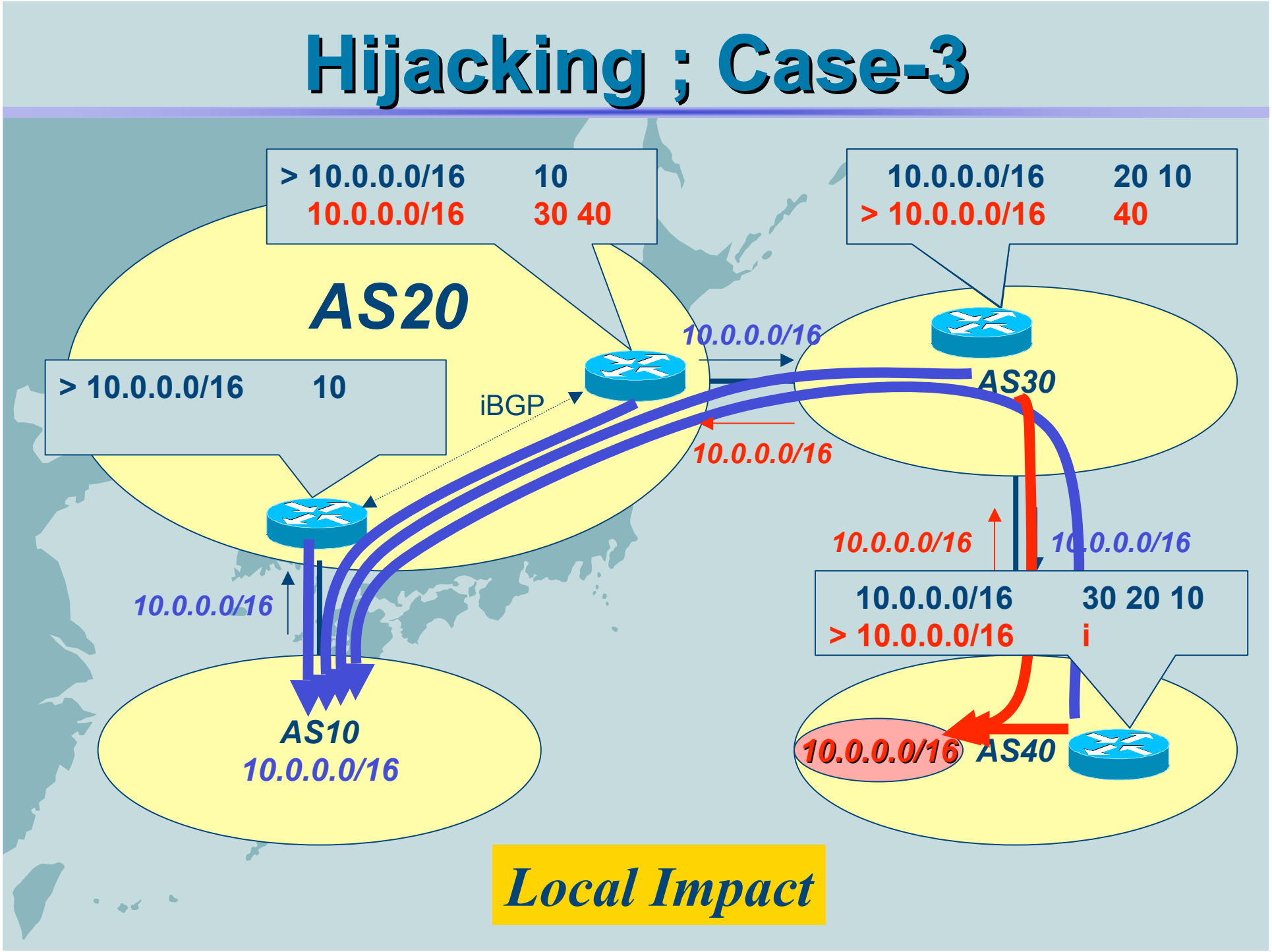
AS10:Customer of AS20
AS40:Customer of AS30
AS20 and AS30 is peering

Global Impact

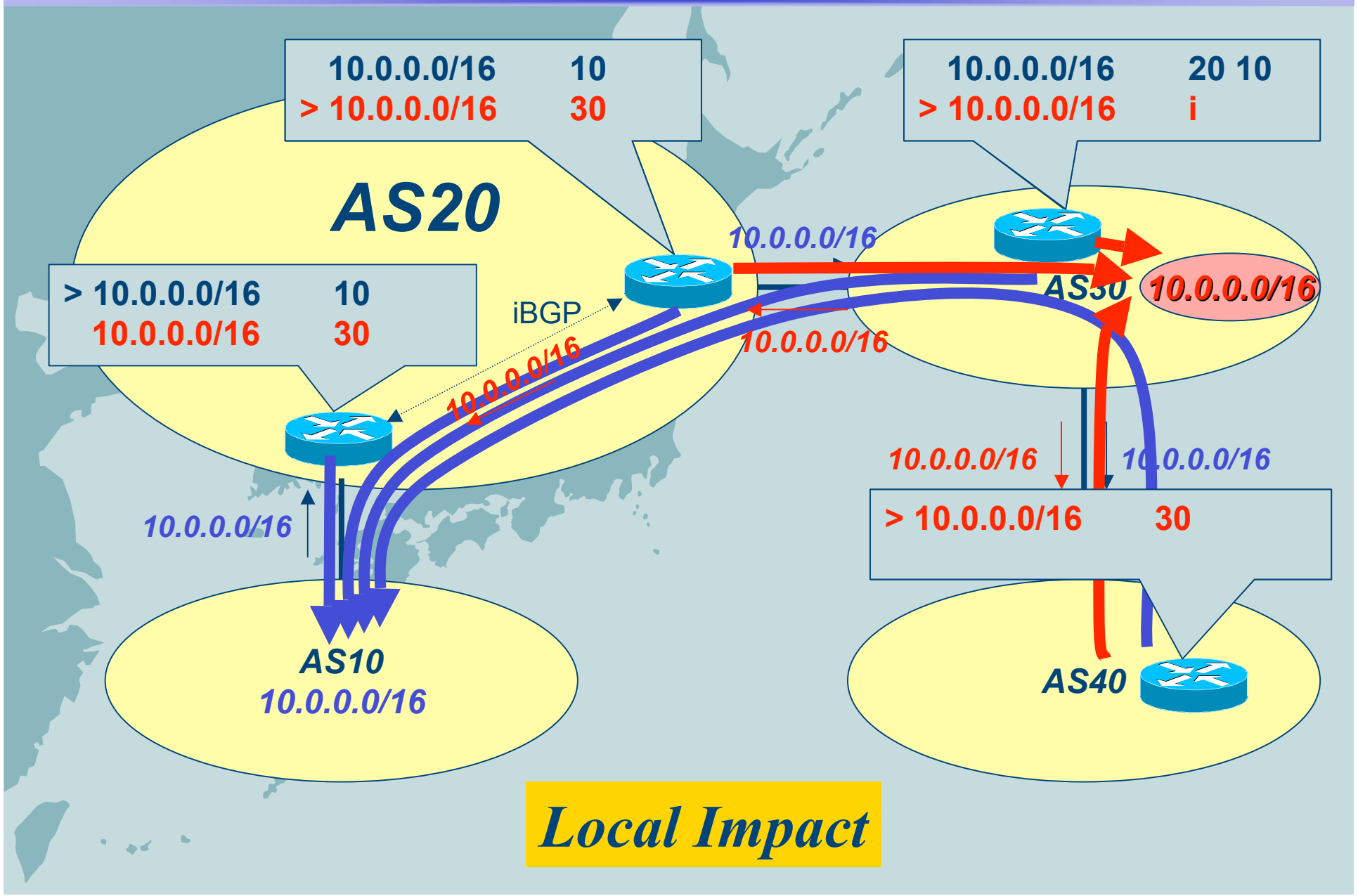
Hijacking ; Case-2



Hijacking ; Case-3



Hijacking ; Case-4



Local Impact

Cause of Route Hijacking

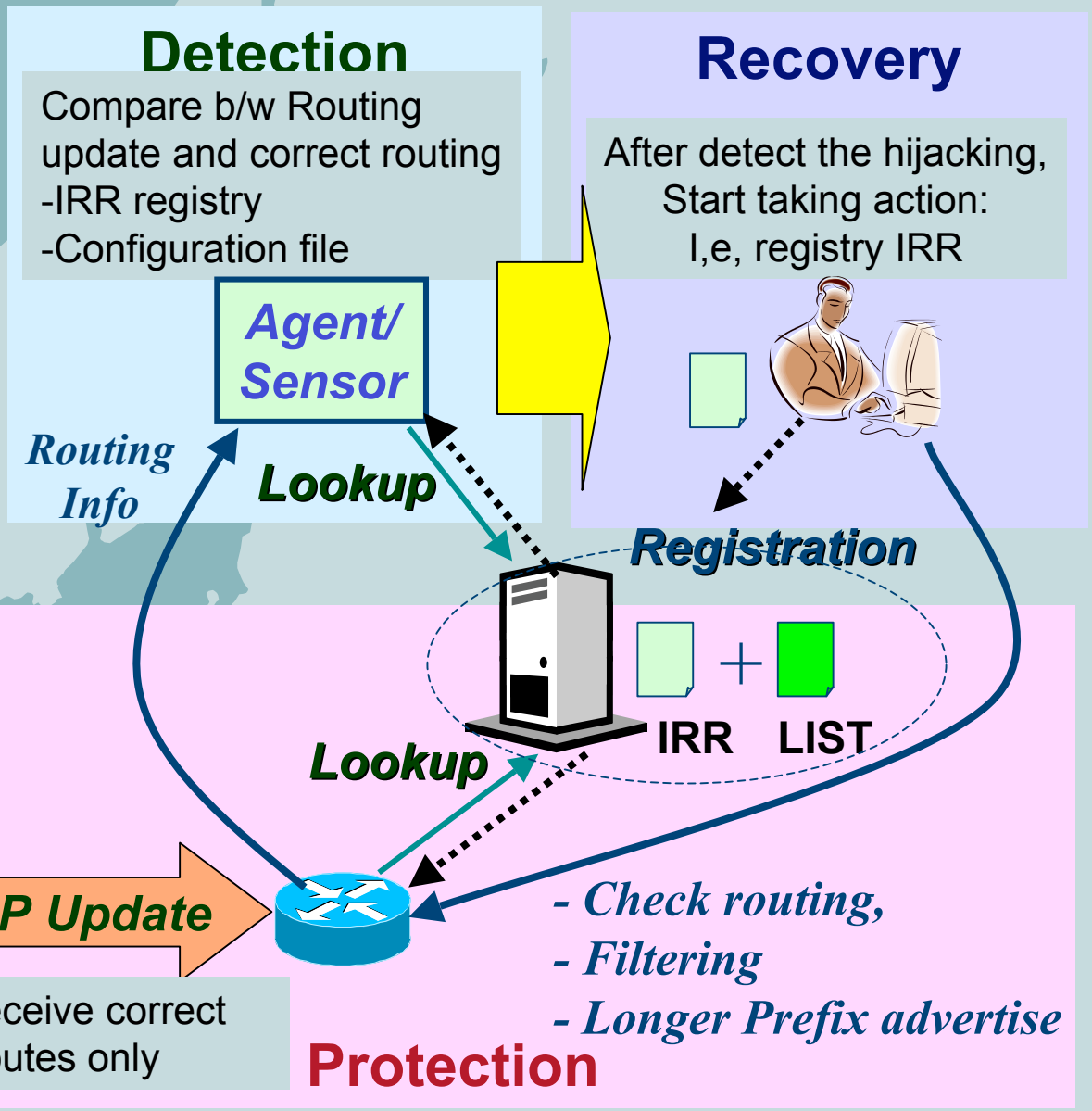
- Operational Fault
  - Automatic route advertisement
  - Configuration error
    - Filtering error (leaking local/private use address)
    - Fat finger ^^); (wrong address/mask)
- Intentional Fault
  - Unfair use of IP address
  - For Spam/DDoS/Phishing….
  - Cyber Terrorism

Research of BGP Route Hijacking in Japan

- **Japanese Government (Ministry of Internal Affairs and Communications) research project**
  - **4 year term ; 2006/4 - 2010/3**
  - **to develop detect/recover/protect function**
  - **NTT Communications in charge of this project**
- **Telecom-ISAC Japan**
  - **Research by volunteers from Japanese ISPs**
  - **Activity of BGP working group since 2004**

Functions of Anti-BGP route hijacking

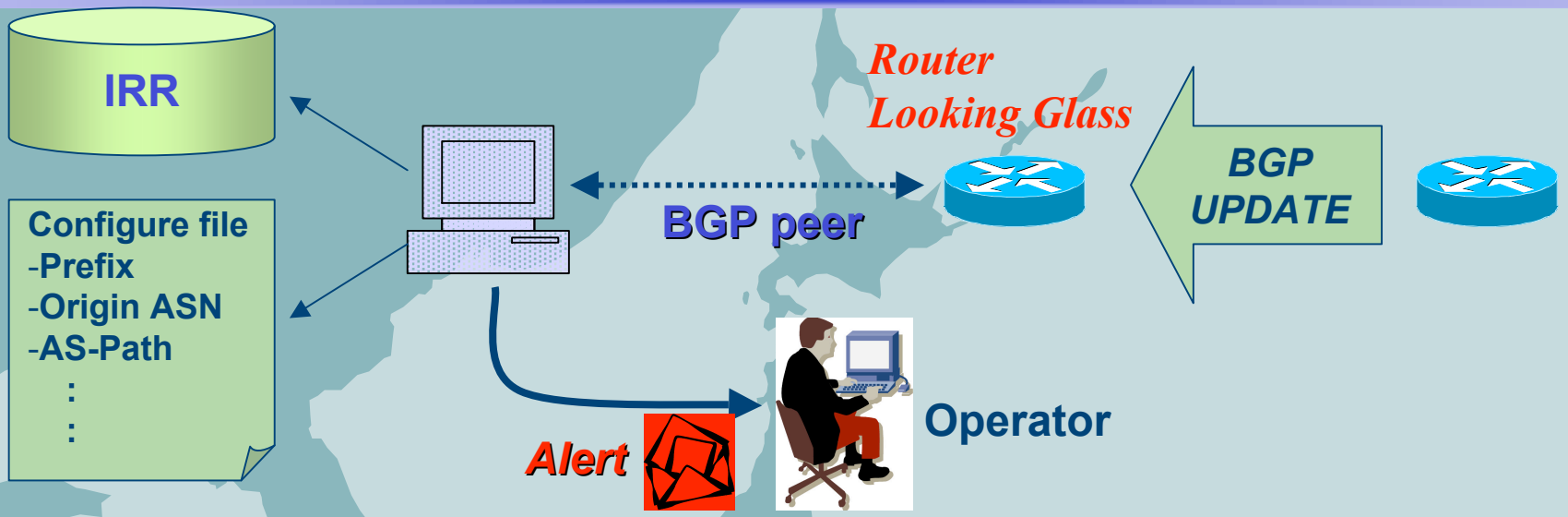
- Detection
- Recovery
- Protection



Detection systems in the World

- RIPE NCC MyASN Service
  - A part of RIPE NCC RIS (Routing Information Service)
  - Checking a prefix is announced with an incorrect AS path.
  - Alerting by email or to your own syslog server
- PHAS (Prefix Hijack Alert System)
  - UCLA
  - uses BGP data (with 3 hours' delay) from Oregon-Univ RouteViews
  - Checking origin, lasthop and sub-allocation set change
  - Alerting by email
- IAR (Internet Alert Registry)
  - Using PGBGP (Pretty Good BGP)
  - Alerting by email or search on the web
- ENCORE (an inter-AS diagnostic ENsemble system using COoperative REflector agents)
  - NTT Media Innovation Laboratories
  - Putting multi-point agents on Multi-AS, Monitoring owned prefixes on the agent
  - Alerting by email
- Keiro-Bygyo (Route magistrate)
  - Telecom-ISAC Japan BGP-WG
  - Comparing local info (from IRR and manual maintain) and BGP UPDATE
  - Alerting by email

Detection system

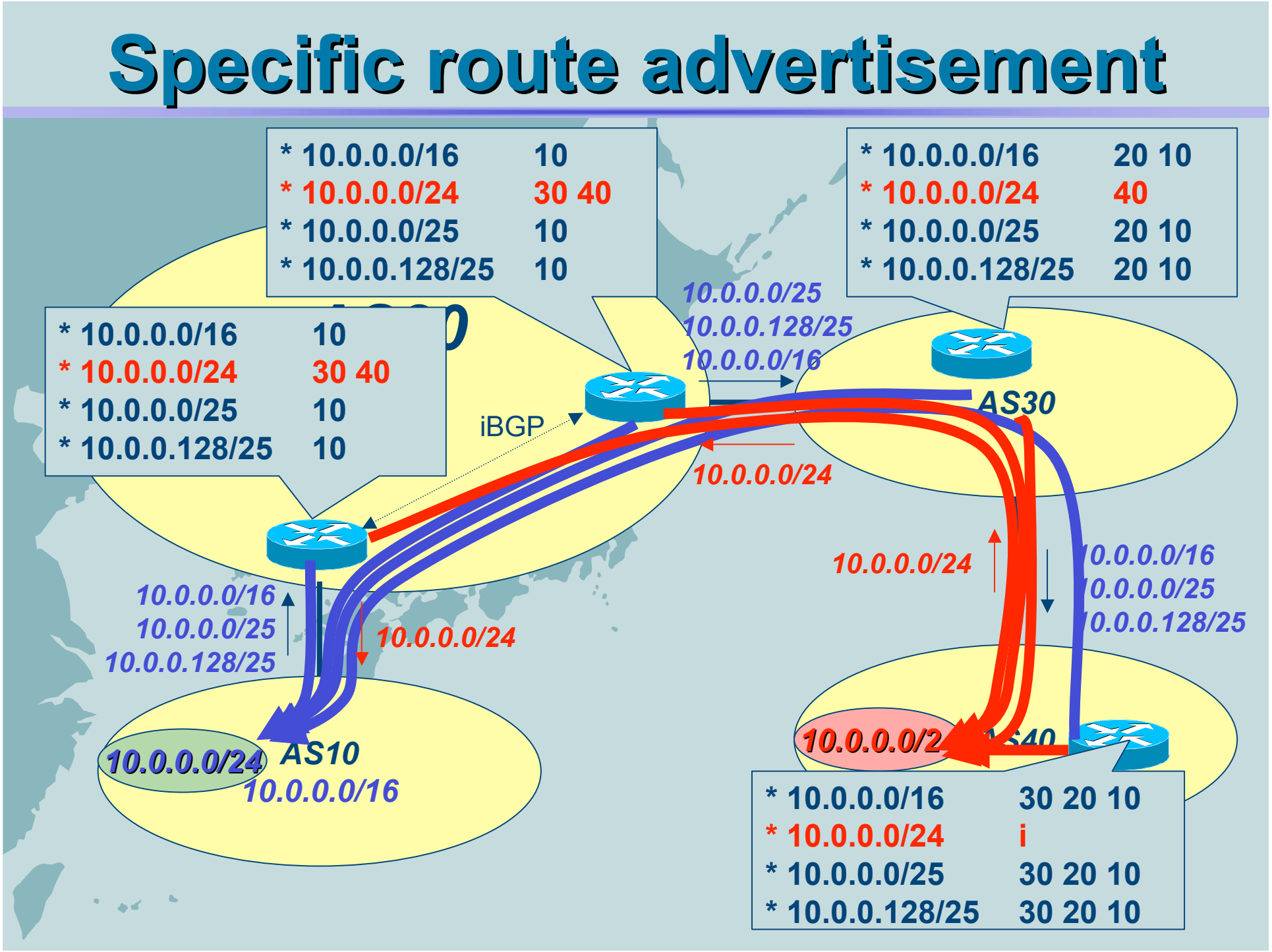


- Monitoring BGP update
  - Having BGP peer with multiple Routers
  - Checking a prefix between last ASN in the AS path attribute announced by BGP and origin AS in IRR
  - When expected to hijack, alerting by email, syslog, SNMP trap etc

Recovery flow

- Checking extent of the impact
  - Global Impact? Local Impact?
- How to recover (temporary and permanent)?
  - Hijacking AS should stop advertising invalid route advertisement (permanent)
  - Request route filtering on infected AS (temporary)
  - Announce more specific route (temporary)

Specific route advertisement



Recovery flow by Reverse Hijacking

- Decision of advertise route （More Specific route)
- IRR registry (*option*)
- Request to upstream ISP for opening prefix route filtering
- Start advertise Specific route
  (Specific prefix advertisement via upstream)
- Checking the trouble resolution as temporary fix
- Request to Hijacked AS
- Stop advertisement from Hijacked AS
- Stop advertisement of Reverse Hijacking route

Problems of Recovery

- Redundancy
  - Detection System/Email receipt address should have redundant
- How to contact/request Hijacked AS
  - Don't have direct connection (Customer/peer/Upstream ISPs)
  - Don't know contact phone/email address
- Problem of specific route advertisement
  - Upstream should open prefix filter(exact match)
    - Request based filter
    - IRR registry based filter
  - Convergence time for global recovery
  - Can't accept specific route
    - ISP has route filtering policy

    i.e. /24

Useful tools for Recovery

- Detection System
  - MyASN, PHAS, IAR, ENCORE, BUGYO….
- Upstream ISP
  - Can contact their peers, then ….
- Operator community
  - nsp-security/nsp-security-xx
  - xNOG (NANOG, JANOG, SANOG, AFNOG …)
- Specific route advertisement

Real Hijacking Case (1)

- 2004/6
- Originated from Japanese ISP
- Longer prefix / Invalid origin
  - /24 x2, /25 x1, /29 x1
- Detected 1/1 AS
- Action
  - Contacted originated AS operator
  - Origin AS stopped invalid announcement
- Impact : about 150 minutes

Real Hijacking Case (2)

- 2004/9
- Originated from Korean ISP
- Longer prefix / Invalid origin
  - /24 x 2
- Detected 1/1 AS
- Action
  - Escalate peer ISP
    - Filtering on peer ISP
    - Origin AS stop announcement
- Impact : about 2 days

Real Hijacking Case (3)

- 2005/2
- Originated from Japanese ISP
- Longer prefix / Invalid origin
  - /22 x 1
- Detected 1/1 AS
- Action
  - Escalate peer ISP
    - Reverse Hijacking
- Impact : about 1 hour

Real Hijacking Case (4)

- 2006/11
- Originated from Korean ISP
- Longer prefix / Invalid origin
  - /27 x 1
- Detected 6/7 ASes on Keiro-Bugyo
- Action
  - Couldn't contact to origin AS operator, escalate own upstream ISP
    - Filtering on Upstream ISP first
    - Origin AS stop announcement
- Impact: about 16 hours

Real Hijacking Case (5)

- 2006/11
- Originated from *Indonesian* ISP
- Same prefix length / invalid origin
  - /17 x 2, /14 x 1
- Detected 1/7 AS on Keiro-Bugyo
- Action
  - Not have been taken any action (Withdrawn soon)
- Impact : about 5 minutes

- By after analysis, we found this AS originated many other invalid routes at the same time

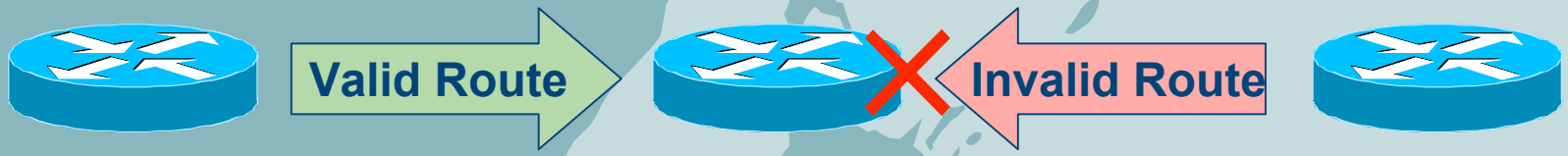
Real Hijacking Case (6)

- 2006/12
- Originated from Japanese ISP
- Longer prefix / Invalid origin
  - /32 x15, /30 x14
- Detected just 1/7 AS on Keiro-Bugyo
  - Almost ISP at Keiro-Bugyo adopted the prefix-length filtering
- Action
  - Contacted originated AS operator
- Impact : about 23 minutes

Summary of these cases

- Detection
  - Longer prefix Hijacking
    - /24 or shorter is almost easy to detect
    - /25 or longer is hard to detect
      - Depends on the ISP filtering policy
  - Same Prefix length Hijacking
    - Hard to detect
  - Many sensors in wide locations would be better
- Recovery
  - It's not takes long time (Less than 2 hours), if operators know contact (Peer/Local ISP)
  - Takes long time, if don't have contact
  - More specific announcement can mitigate the impact as temporary solution

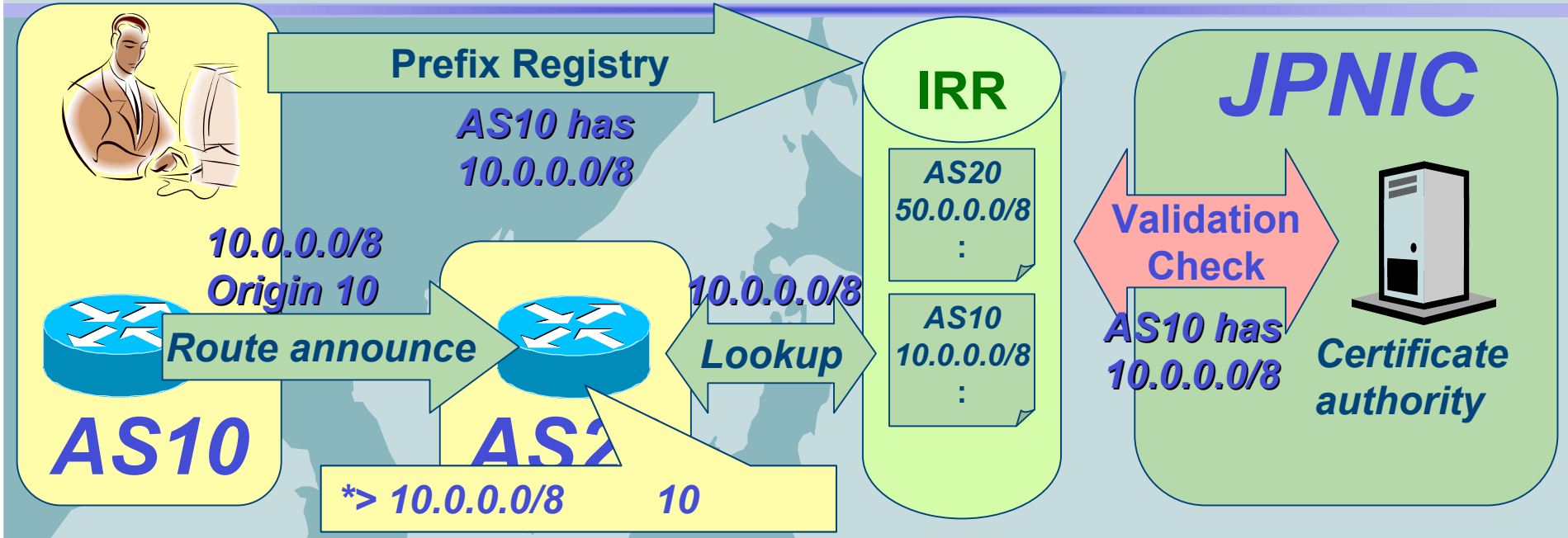
Protection



- Don't received invalid route!!
  - What is valid and what is invalid
  - How to block invalid prefix?
- Protection method
  - IRR base route validation
    - Guarantee origin AS
    - JPIRR (trial)
    - Router lookup IRR (irrzebra is working)
  - BGP base route validation
    - Guarantee Origin AS and AS-PATH
    - sBGP, soBGP, pgBGP, psBGP
    - Router should implement these protocol
      # Router CPU high-load

} Our research

IRR Based Protection



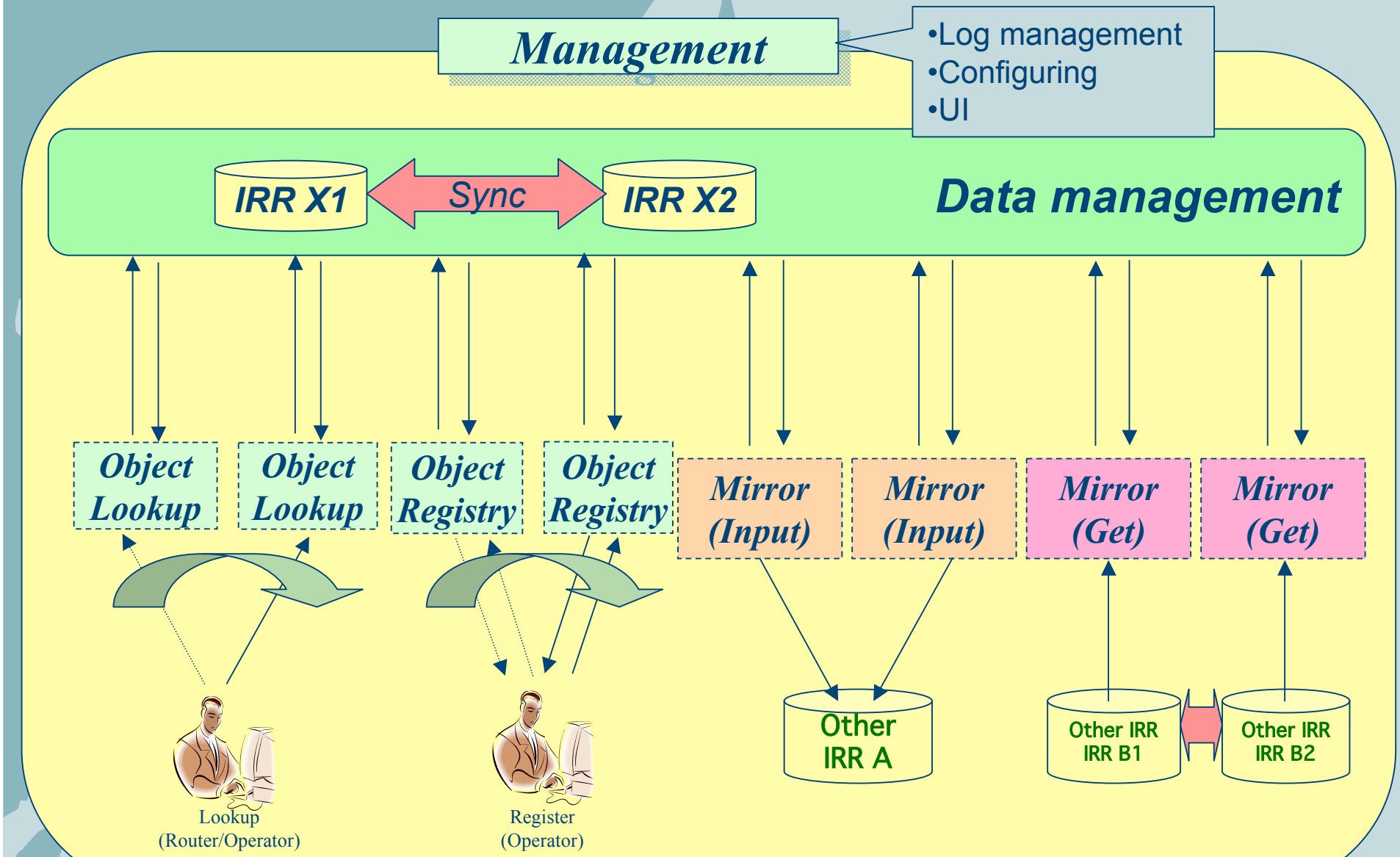
Authentication Process of Route

- Operator
  - registry IRR
  - Announce Valid Route prefix
- IRR
  - Authenticate by CA (JPNIC)
  - Store valid Prefixes only
- Router
  - lookup IRR registry
  - Filtering of invalid Route

Requirement of IRR

- IRR system
  - Stable IRR system (Redundancy)
  - Performance
  - Scalability
  - Secure mirroring
- (Valid) IRR data
  - Authenticate by CA

Idealized IRR System



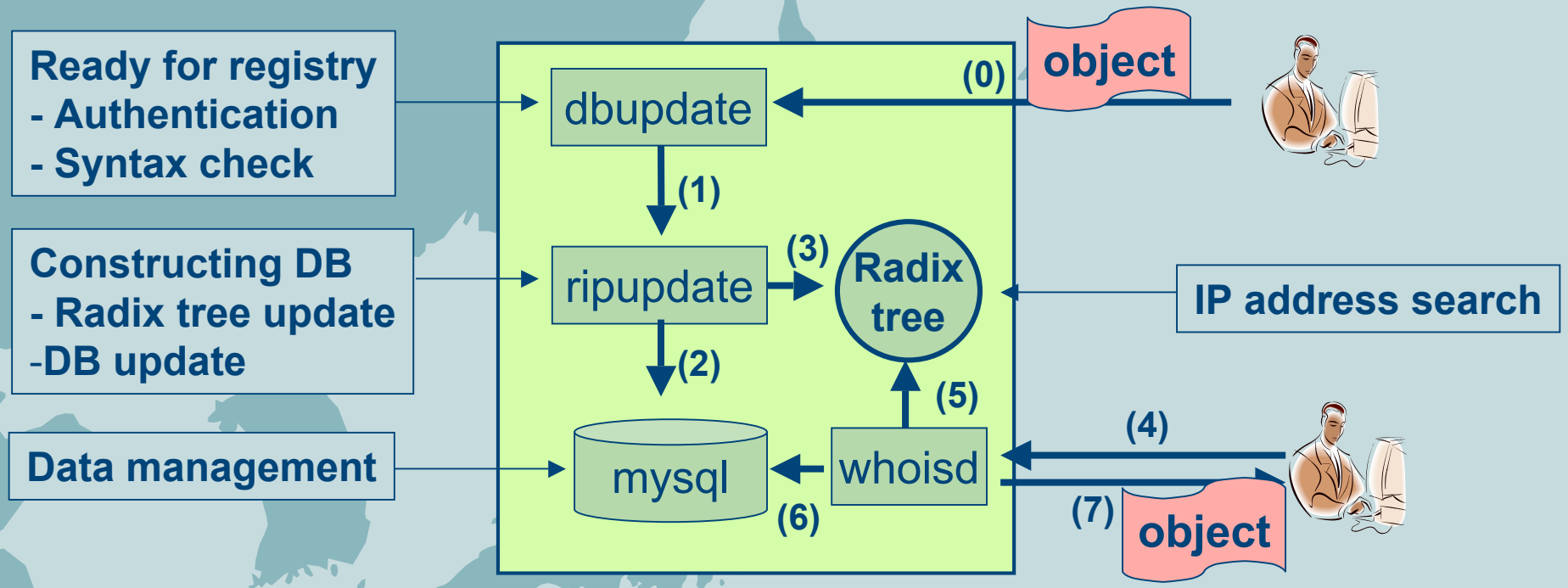
"Reliability" and "Stability" needed

Current IRR system

- **RIPE whoisd** **RIPE, APNIC**
- **Merit IRRd** **RADB, JPIRR , VRR, other ISP's IRR**

Items	*RIPE Whoisd*	*Merit IRR*
Install method	Compile from source	Package install (PORTS)
Structure	Modularized	Monolithic
Data management	RDBMS (MySQL)	Text file
Object registry	Mail, Web (other tool)	Mail, Web (other tool)
Mirroring protocol	NRTM	NRTM
RPSL correspondense	RPSLng (RFC4012)	RPSLng (RFC4012)
Error check	Strict (Sequence check)	Loose
System Scalability	Yes (RDBMS)	No
Backup mechanism	No	No
Latest version	Whoisd-3.3.0 2005/5/25	Irrd-2.3.3 2006/11/6

RIPE whoisd

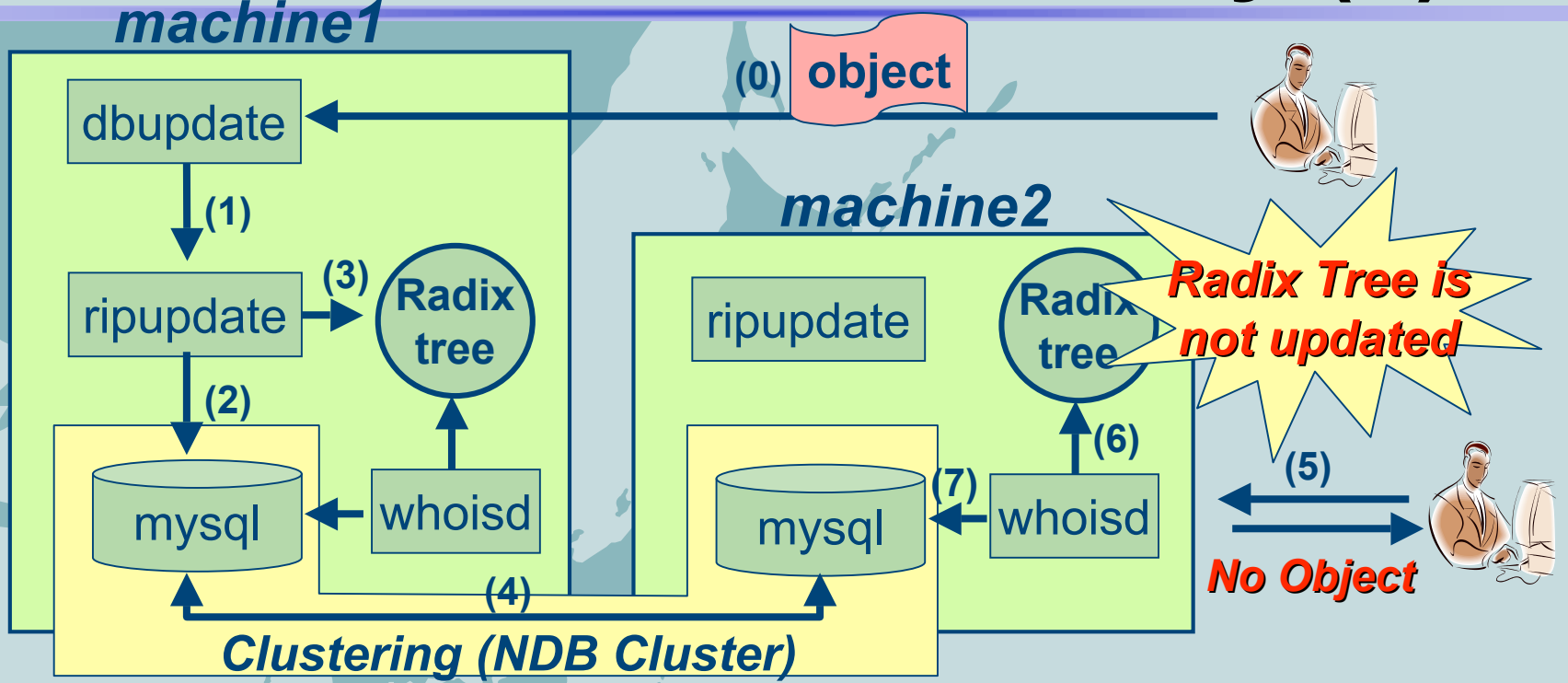


(0) Object registry by Operator
(1) Send Object to ripupdate for Database constructing
(2) Update “MySQL Database”
(3) Constructing “Radix Tree”
(4) Whois query
(5) Check address (IP Prefix check)
(6) Database search
(7) Whois reply

Registry Process

Lookup Process

RIPE whoisd redundancy (1)

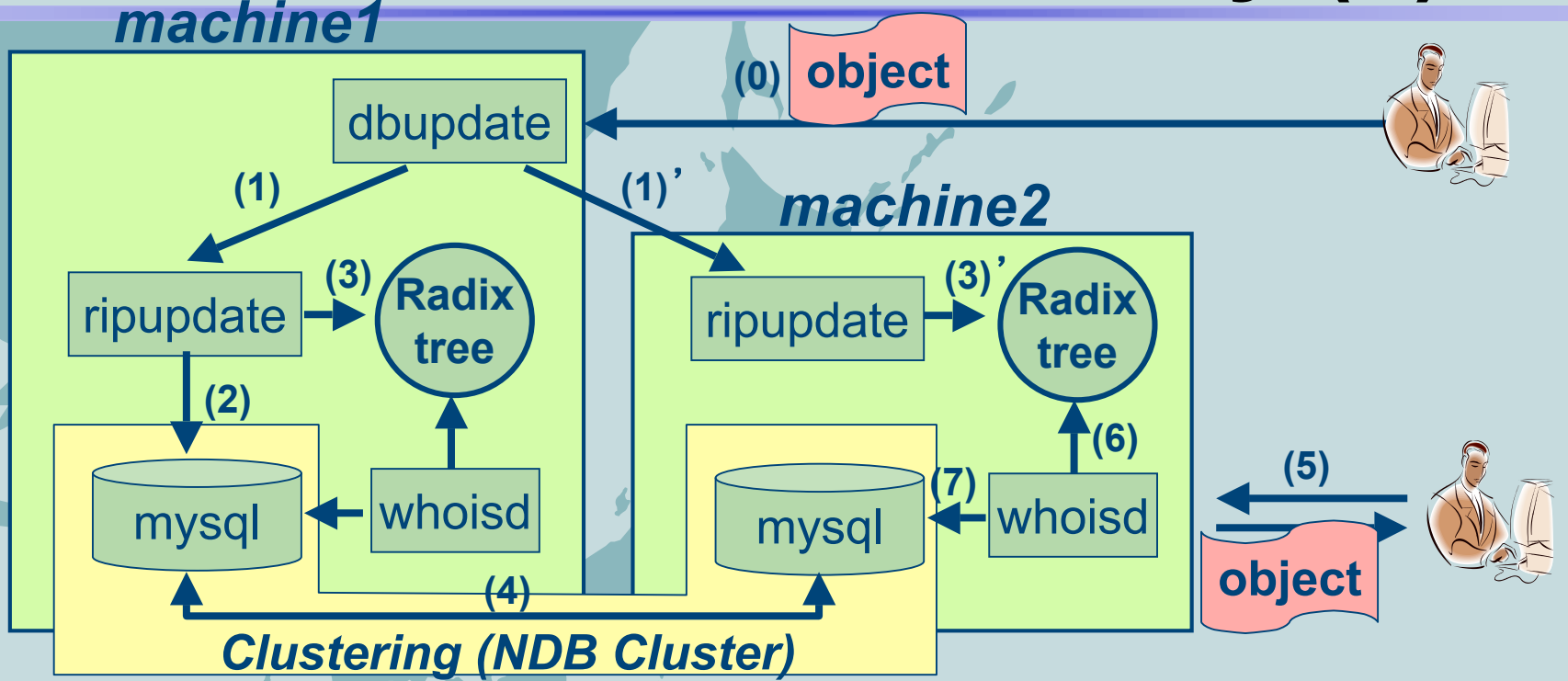


(0) Object registry by Operator
(1) Send Object to ripupdate for Database constructing
(2) Update “MySQL Database”
(3) Constructing “Radix Tree”
(4) Database sync
(5) Whois query
(6) Check address (IP Prefix check)
(7) Database search

Registry Process

Lookup Process

RIPE whoisd redundancy (2)

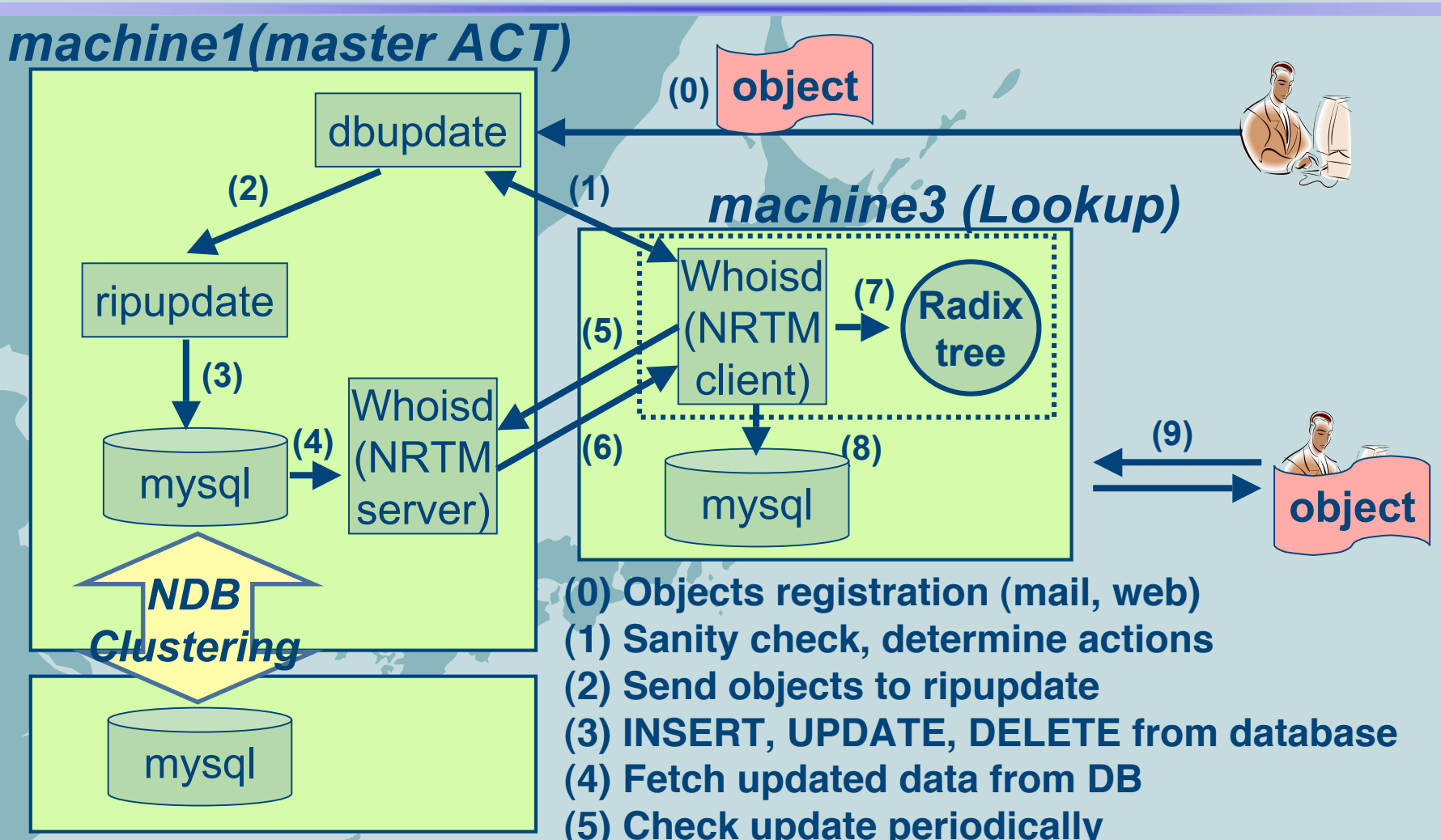


(0) Object registry by Operator
(1) Send Object to ripupdate for Database constructing
(2) Update “MySQL Database”
(3) Constructing “Radix Tree”
(4) Database sync
(5) Whois query
(6) Check address (IP Prefix check)
(7) Database search

Registry Process

Lookup Process

RIPE whoisd redundancy (3)



(0) Objects registration (mail, web)
(1) Sanity check, determine actions
(2) Send objects to ripupdate
(3) INSERT, UPDATE, DELETE from database
(4) Fetch updated data from DB
(5) Check update periodically
(6) Send updates to NRTM client
(7) Update Radix Tree
(8) Updates Radix Tree and store data into local DB
(9) Reply for users' queries

Current Issues of our IRR system

- Performance
  - Memory issue
    4G is not enough for NDB cluster
    ---> change configuration
  - Radix Tree issue
    More than 5 minutes for booting
    ---> Service interruption by blocking
  - Scalability
    - Clustering with many server
    - Redundancy b/w far location
- Field trial
  - IRR lookup function will be separate
  - Redundancy test b/w Tokyo and Osaka
- Router implementation
  - 4byte ASN support…
  - Should start talking with NIR/RIRs and Vender

Summary

- Detection
  - Longer prefix Hijacking is almost easy to detect, but /25 or longer is hard to detect
  - Same Prefix length Hijacking is hard to detect
  - Many sensors in wide locations would be better
- Recovery
  - It's not takes long time , if operators know contact
  - Takes long time, if don't have contact
  - More specific announcement can mitigate the impact as temporary solution
- Protection
  - IRR base route validation, we need stable / redundant IRR
  - For scalability, we are using customized RIPE whoisd
  - We will start field trial and we doing routing implementation

Special Thanks

- Telecom-ISAC BGP-WG
- JPNIC
  - Mr. Kimura, Mr. Okada
- NTT Communications
  - Anti-Route Hijacking team

Reference

- RIPE/NCC
  http://www.ris.ripe.net/myasn.html
- Merit
  http://www.irr.net/
- PHAS
  http://phas.netsec.colostate.edu/
- IAR
  http://www.cs.unm.edu/~karlinjf/IAR/
- NTT Media Innovation Laboratories
  http://www.ntt.co.jp/mirai/organization/organization0204.html (Japanese only)
- JANOG
  http://www.janog.gr.jp/meeting/janog19/2007/01/_meets_jpirr.html
- JPNIC
  http://jpnic.jp/ja/materials/irr/20051207/kimura-20051207.pdf
- NSP-SEC
  http://puck.nether.net/mailman/listinfo/nsp-security
- NSP-SEC-JP
  http://puck.nether.net/mailman/listinfo/nsp-security-jp (Japanese only)
- Telecom-ISAC (Keiro Bugyo)
  https://www.telecom-isac.jp/ (Japanese only)

Thank you

Taka Mizuguchi
Tomoya Yoshida