- mis-operation -

Matsuzaki 'maz' Yoshinobu
<maz@iij.ad.jp>

disclaimer

- This is not:

  to accuse someone, products or vendors

- This is:
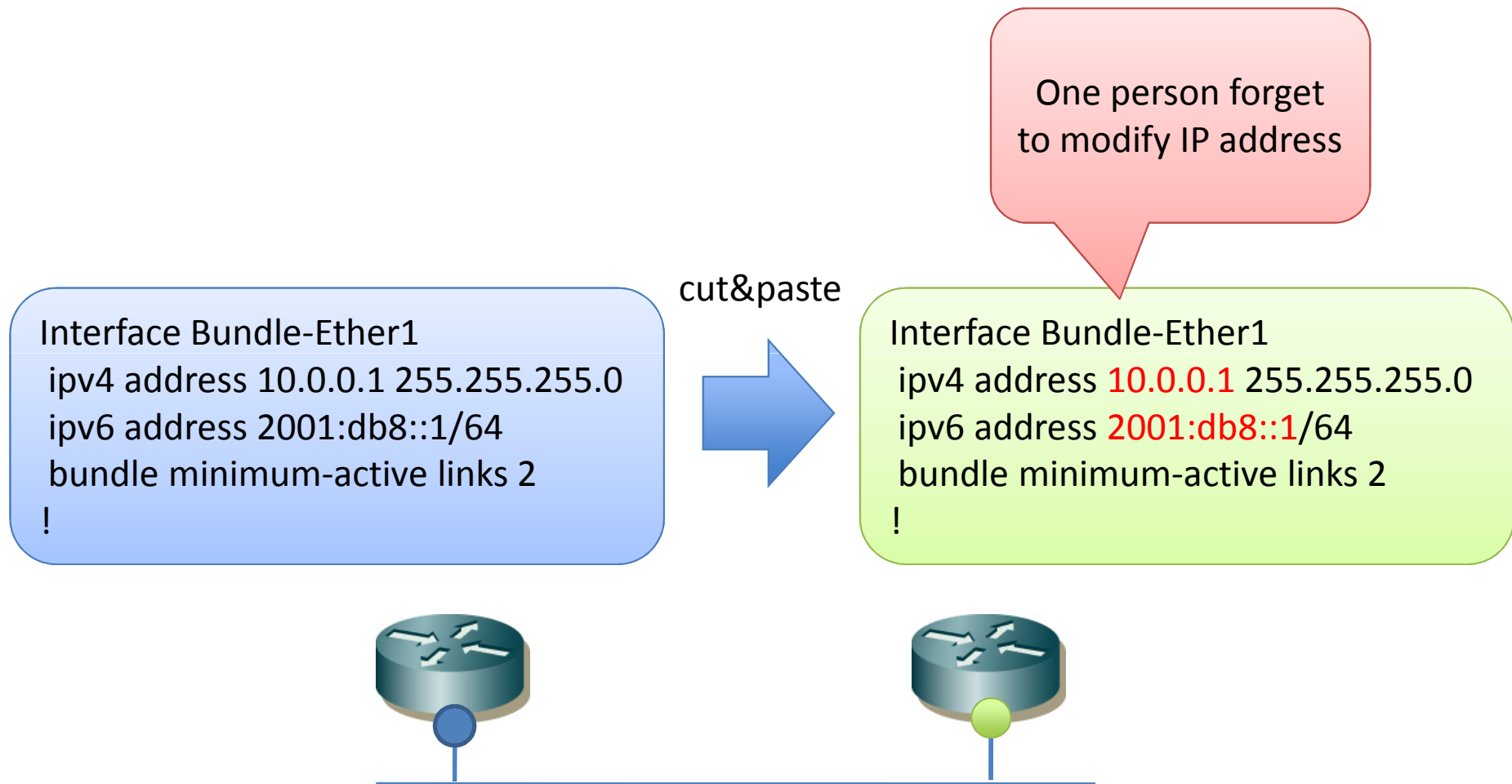
  to learn something from experiences ☺

We have made lots of mistakes

- In many case, its effects are negligible (hopefully), but sometimes even a small mistake could cause a disaster

- Let's look into our mistakes
  - frequent ones and major outages
- These cases are gathered from Japanese operational community. Thanks!

No.1 cut & paste of configuration

- One person was writing a router configuration by cutting & pasting from other routers'.
- but... forgot to modify IP address setting ☹
- caused unwanted routing, IP address duplications

No.1 cut & paste of configuration

One person forget to modify IP address

Interface Bundle-Ether1
 ipv4 address 10.0.0.1 255.255.255.0
 ipv6 address 2001:db8::1/64
 bundle minimum-active links 2
!

cut&paste

Interface Bundle-Ether1
 ipv4 address 10.0.0.1 255.255.255.0
 ipv6 address 2001:db8::1/64
 bundle minimum-active links 2
!

No.2 replacing a router

- One person was asked to replace an existing router to new one

- The person connected the new router to a live network by configuring certain interface though the existing router was still running ☹

- There were 2 routers on the network having the same IP address on their loopback or other interfaces

No.2 replacing a router

existing router

new router

Interface loopback0
 ipv4 address 10.0.0.1 255.255.255.255
 ipv6 address 2001:db8::1/128
 !

Interface loopback0
 ipv4 address 10.0.0.1 255.255.255.255
 ipv6 address 2001:db8::1/128
 !

before removing the existing router, the person connected the new router. even worse ospf was running on the routers

No.3 cable maintenance

- There was a scheduled maintenance at a long distance cable in a network, so one person incremented OSPF link costs on the link

- To avoid flapping on the link, the person disabled OSPF on the link ☹

- During the maintenance window, another cable was down

- … the network was divided

No.3 cable maintenance

There was a scheduled maintenance on this cable, so one person disabled OSPF on this link

But another link was down during the maintenance window, so the network was divided
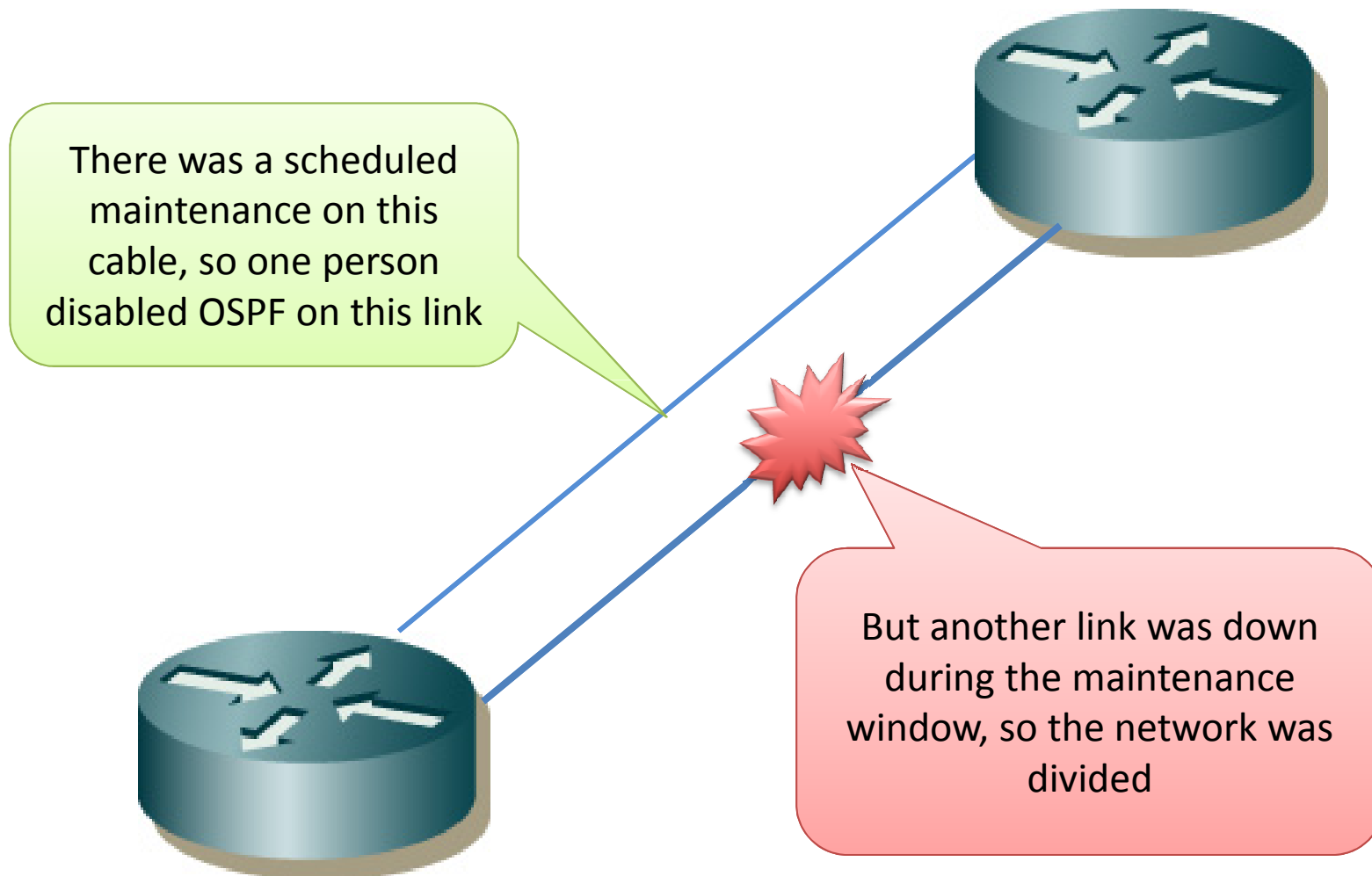
No.4 router reload

- One person performed a firmware upgrade of a router.

- The person changed OSPF link costs to reroute traffic, and reloaded the router ... without saving the configuration ☹

- After reloading the router, OSPF was established, and packets are discarded until BGP is converged
  - OSPF Stub Router Advertisement [RFC3137] would solve this

No.4 router reload
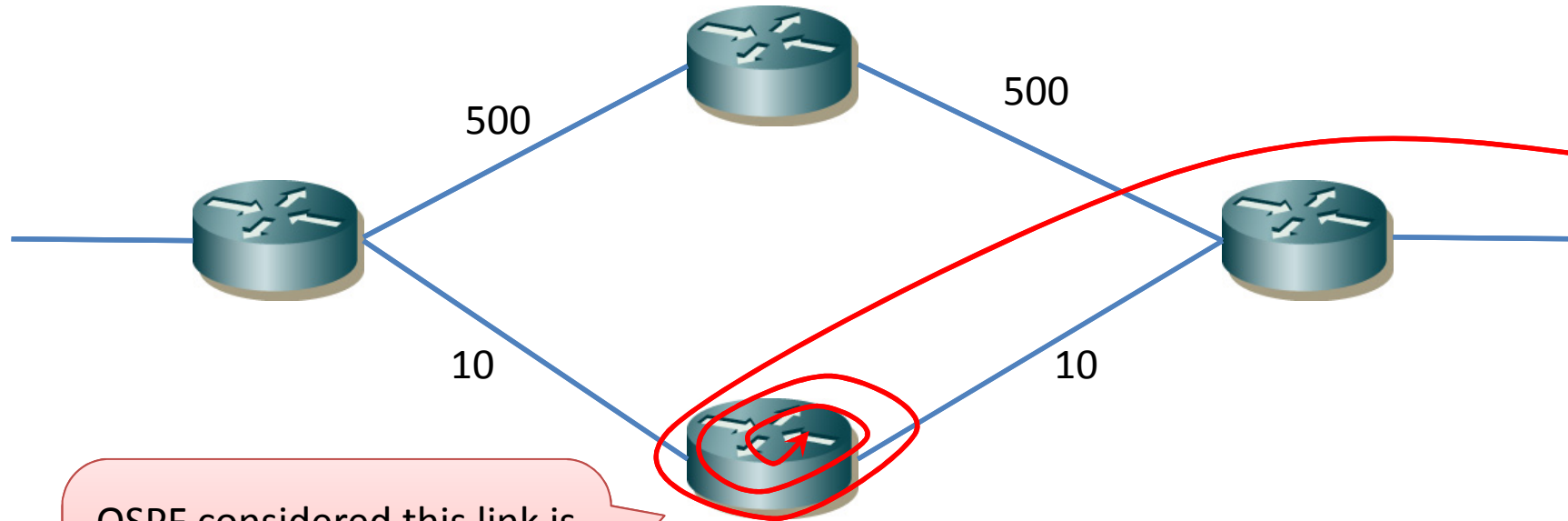
OSPF considered this link is the shortest to go, but packets are discarded until BGP is converged

No.5 port move

- One team performed a maintenance to move a cable from one switch to another
- One person shutdown a port, then another person unplug the cable checking the port number and the port LED.
- The person at the switch misunderstood the port number and port LED relationship, then unplugged an wrong cable ☹
- Unexpected network down

No.5 port move

2010 (c) Internet Initiative Japan Inc.
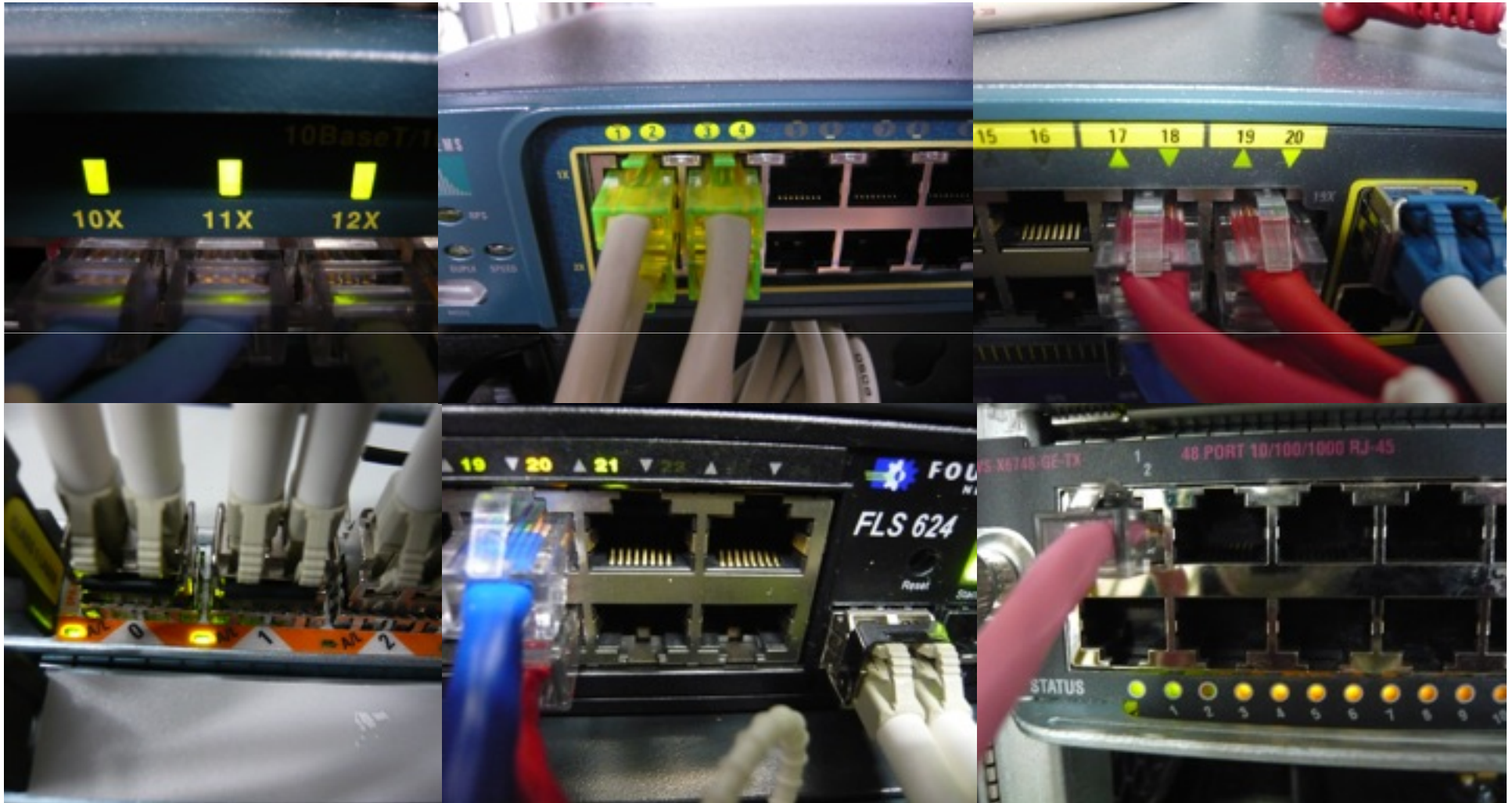
No.6 cable removal

- There were lots of unused cables under racks, so one person tried to remove by cutting down connectors and pulling out cables.

- The person found a fiber with MIC connector, and considered it as FDDI – it means unused anymore, then cut down the MIC connector. ☹

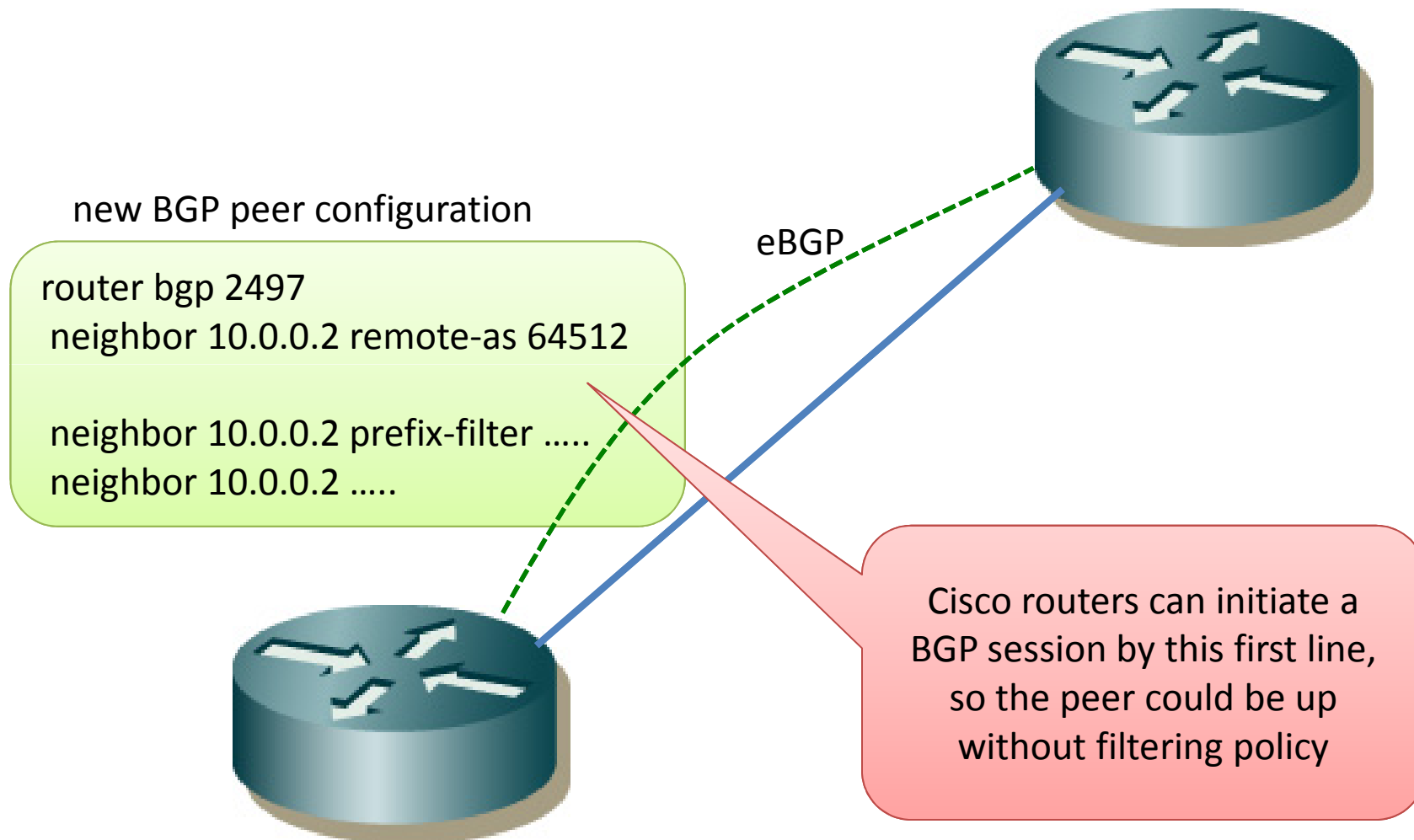- But this fiber was actually used for a GbE link as a multimode fiber, so this caused unexpected fiber cut.

No.6 cable removal
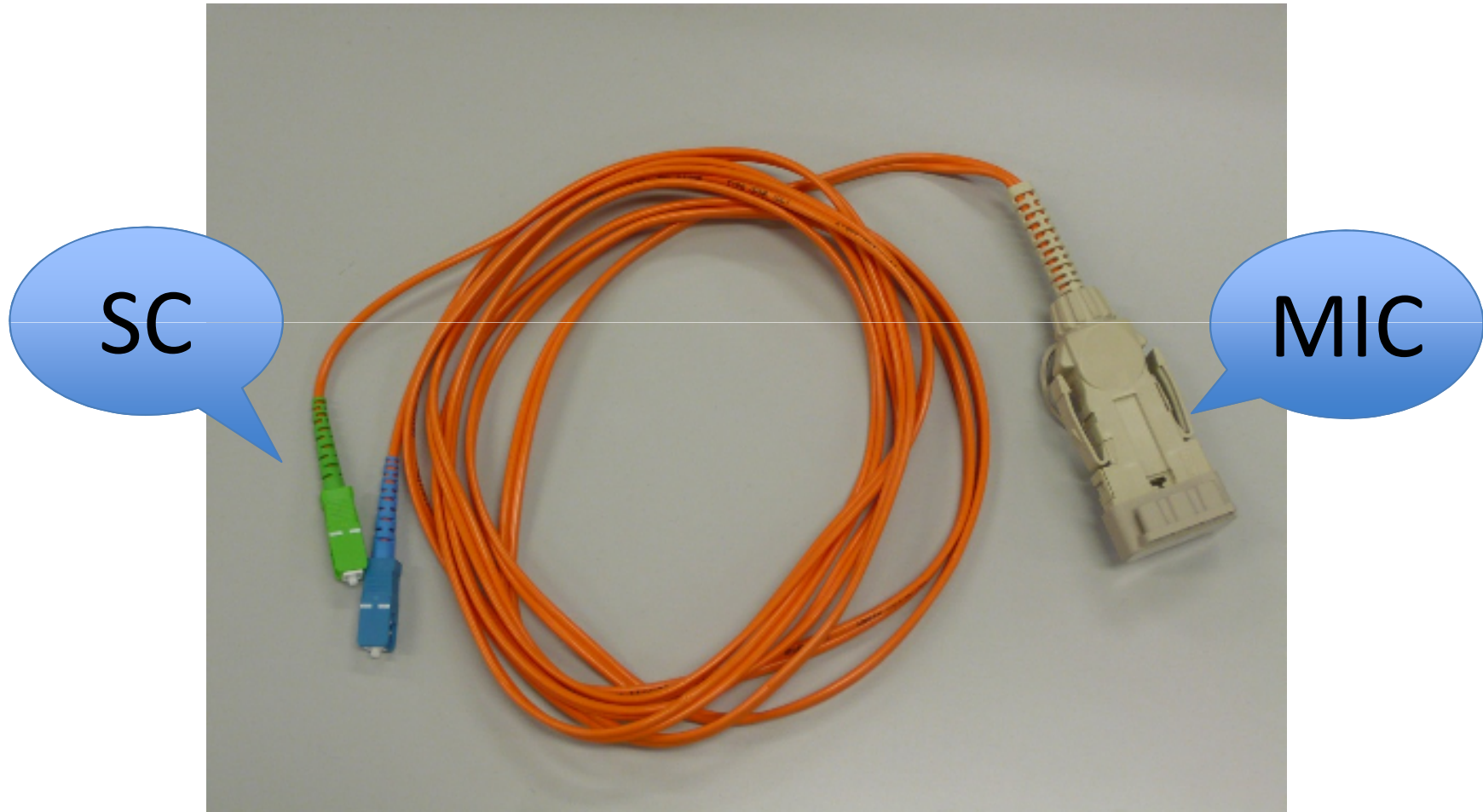
No.7 new BGP session on cisco

- One person were writing a configuration for a new BGP peering session on a Cisco router.

- The person typed the setting line by line, but before completing all of the configuration, the router established a BGP session without filter policy. ☹

- The router announced full-table with internal more specifics.
  - use 'conf net' to avoid this
  - firstly put a fake remote-as setting, and after complete policy setting , overwrite with a real remote-as number

No.7 new BGP session on cisco

new BGP peer configuration

router bgp 2497
 neighbor 10.0.0.2 remote-as 64512

 neighbor 10.0.0.2 prefix-filter .....
 neighbor 10.0.0.2 .....

eBGP

Cisco routers can initiate a
BGP session by this first line,
so the peer could be up
without filtering policy

No.8 new interface for eBGP

- One person configured a new private peering, and the AS has a policy to keep a received nexthop address as is - no nexthop-self.

- The person established a BGP session before announcing the network on the link for eBGP. ☹

- Unexpected best path selection, or unexpected traffic flow.
  - BGP performs recursive route lookup using Routing Table including BGP to find immediate next_hop (RFC4271)

No.8 new interface for eBGP

AS policy: keep a received nexthop address as is

UPDATE

eBGP

iBGP

The person forgot to announce the network on the peering link.
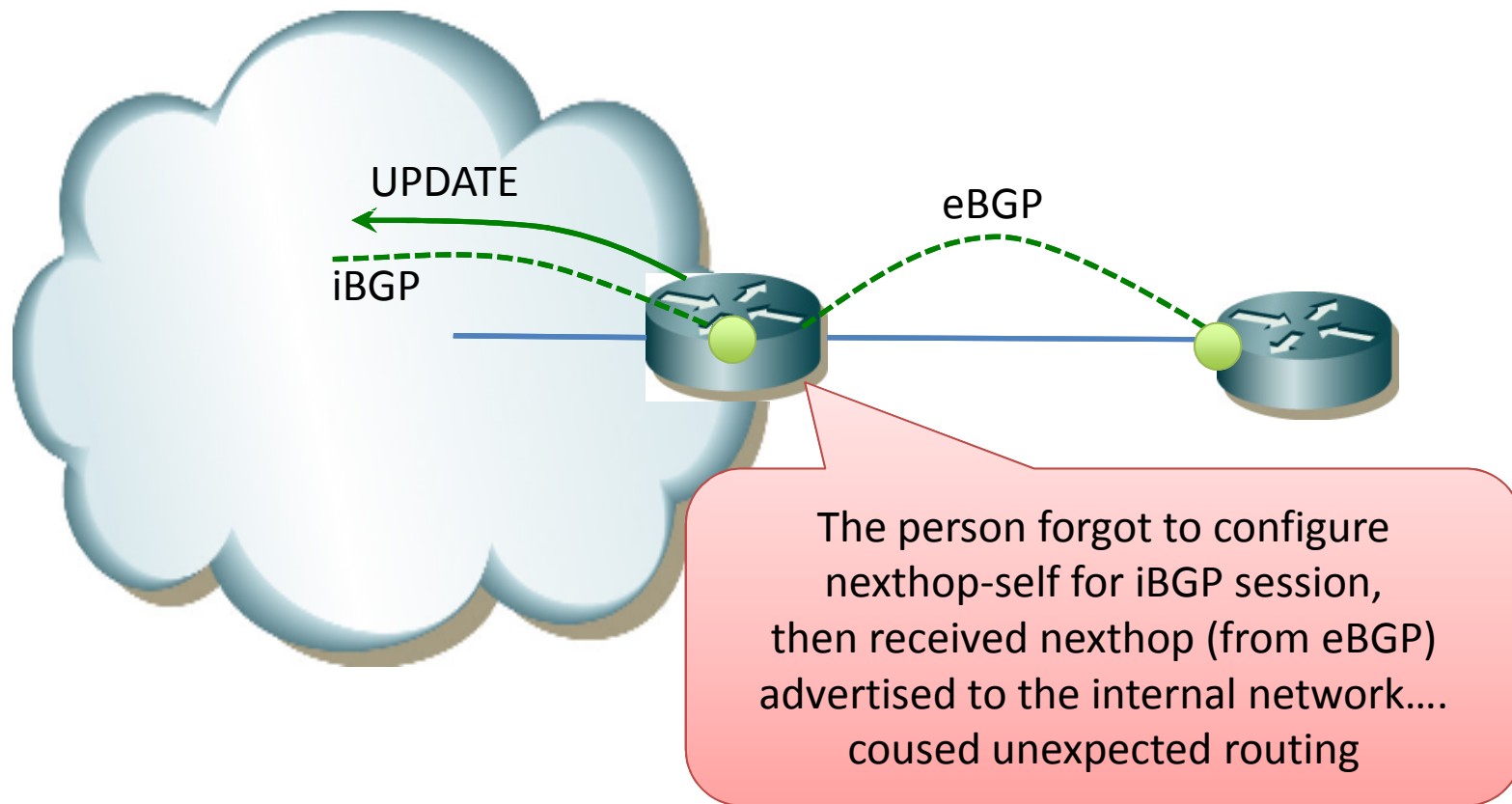…caused unexpected routing
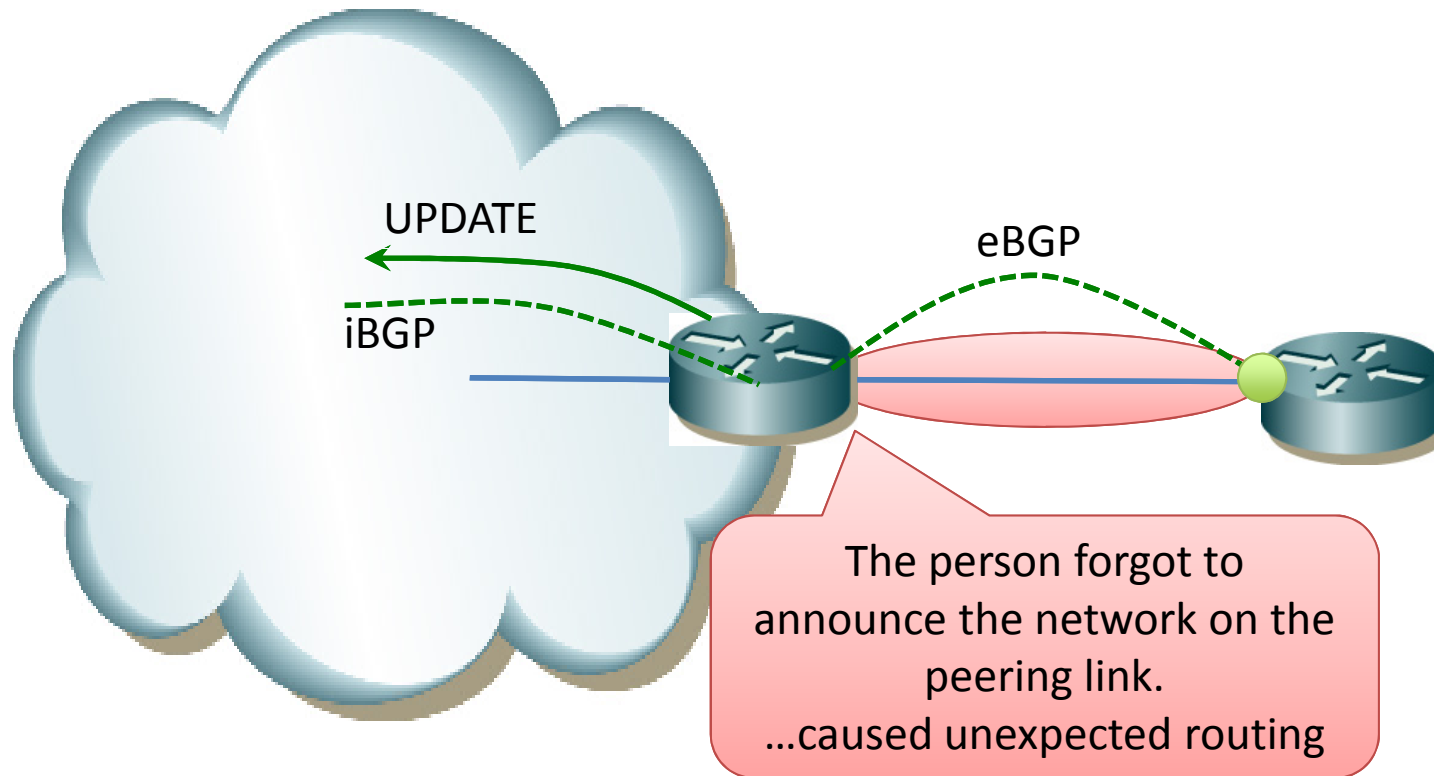
No.9 new router for eBGP

- One person installed a new router to connect an IX, and the AS has a policy to rewrite a received nexthop address to its internal address – performing nexthop-self

- The person forgot to put a nexthop-self policy for iBGP sessions on the router ☹

- After setting up eBGP sessions with other ASes, they met unexpected routing.

  – BGP performs recursive route lookup using Routing Table including BGP to find immediate next_hop (RFC4271)
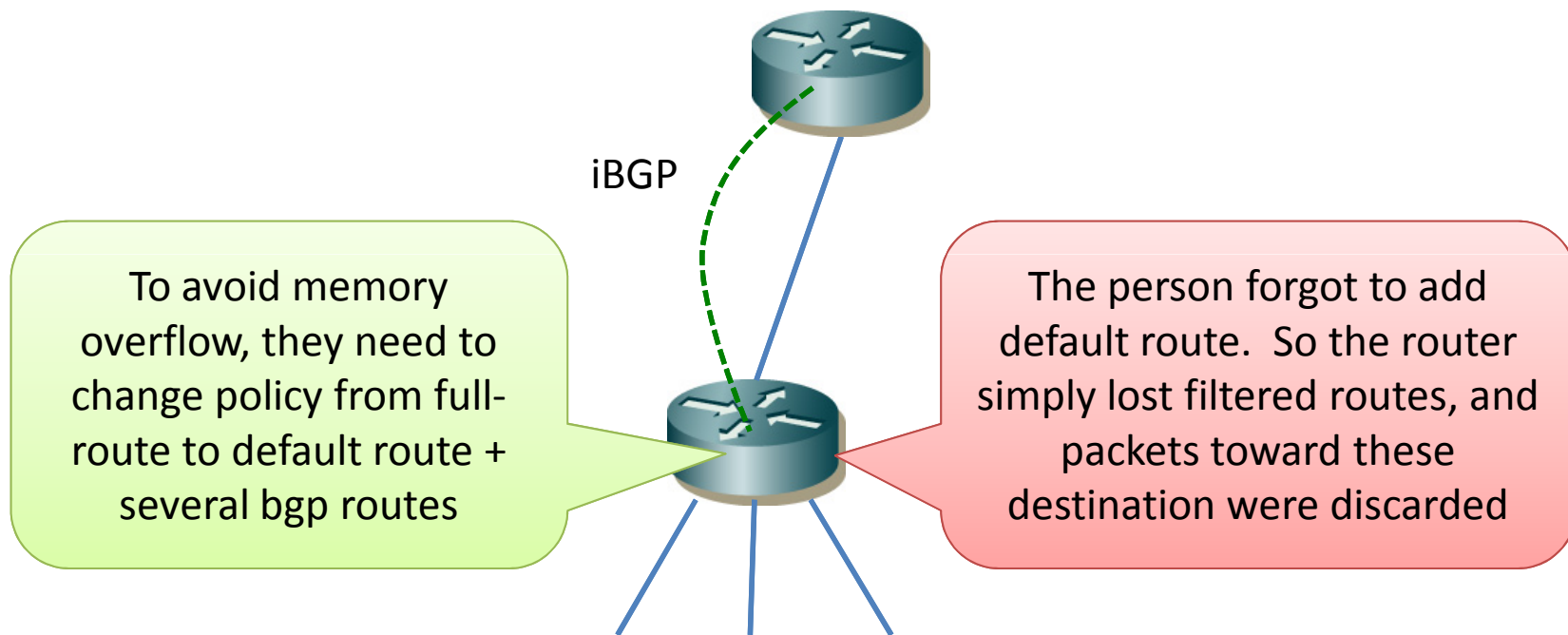
No.9 new router for eBGP

AS policy: always rewrite a received nexthop

UPDATE

eBGP

iBGP

The person forgot to configure
nexthop-self for iBGP session,
then received nexthop (from eBGP)
advertised to the internal network….
coused unexpected routing

No.10 BGP FIB reducing

- One person was asked to filter BGP routes on small routers to avoid memory overflow

- The person forgot to add default route that would cover filtered routes on the routes ☹
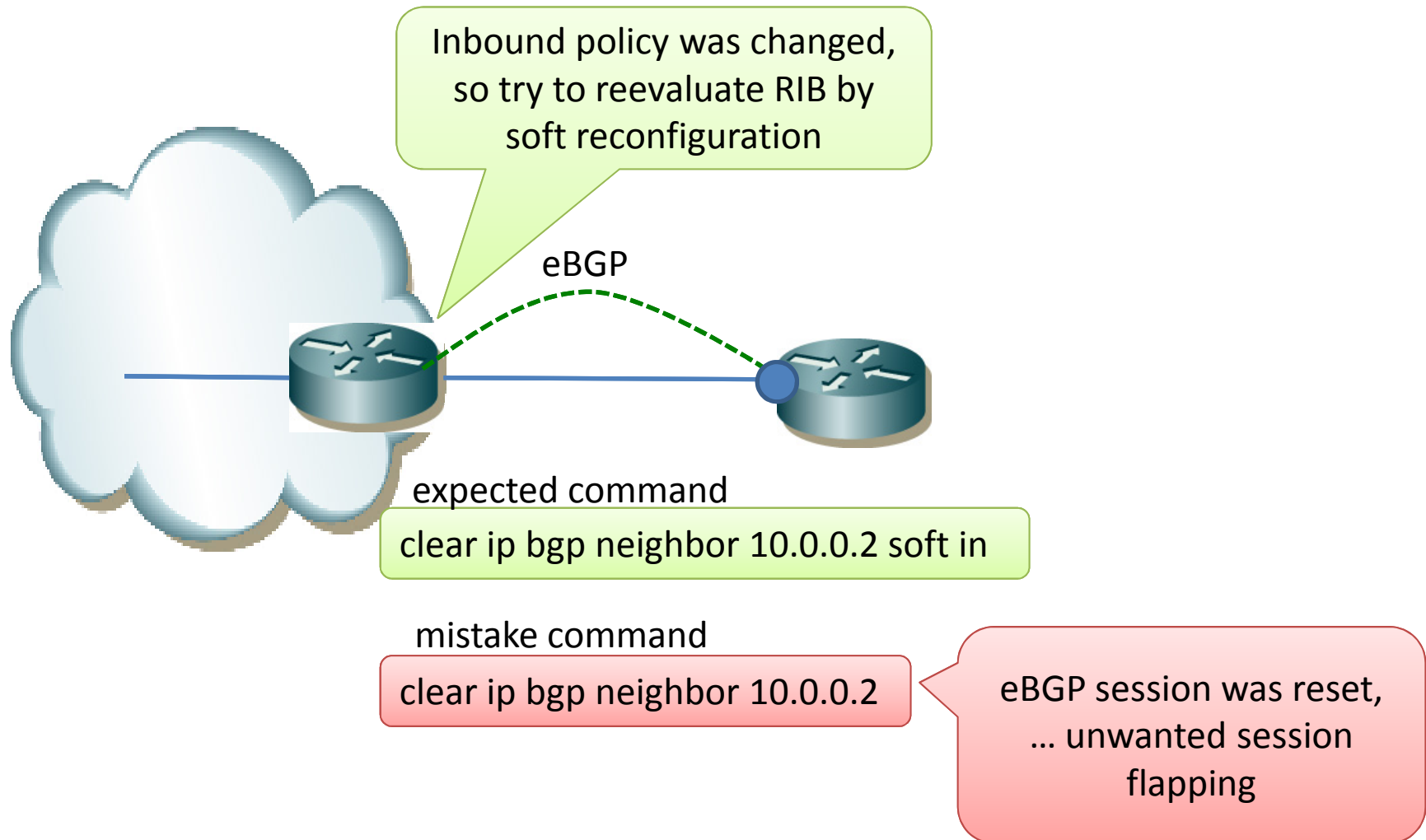
- The router lost routes, caused packets discard

No.10 BGP FIB reducing

iBGP

To avoid memory overflow, they need to change policy from full-route to default route + several bgp routes

The person forgot to add default route. So the router simply lost filtered routes, and packets toward these destination were discarded

No.11 BGP soft reconfiguration

- One person changed a filter policy for eBGP on a cisco router, and tried to perform soft reconfiguration to reevaluate in-RIB.

- The person forgot to add 'soft' keyword when typing 'clear ip bgp neighbor XXX soft', the session was actually reset. ☹
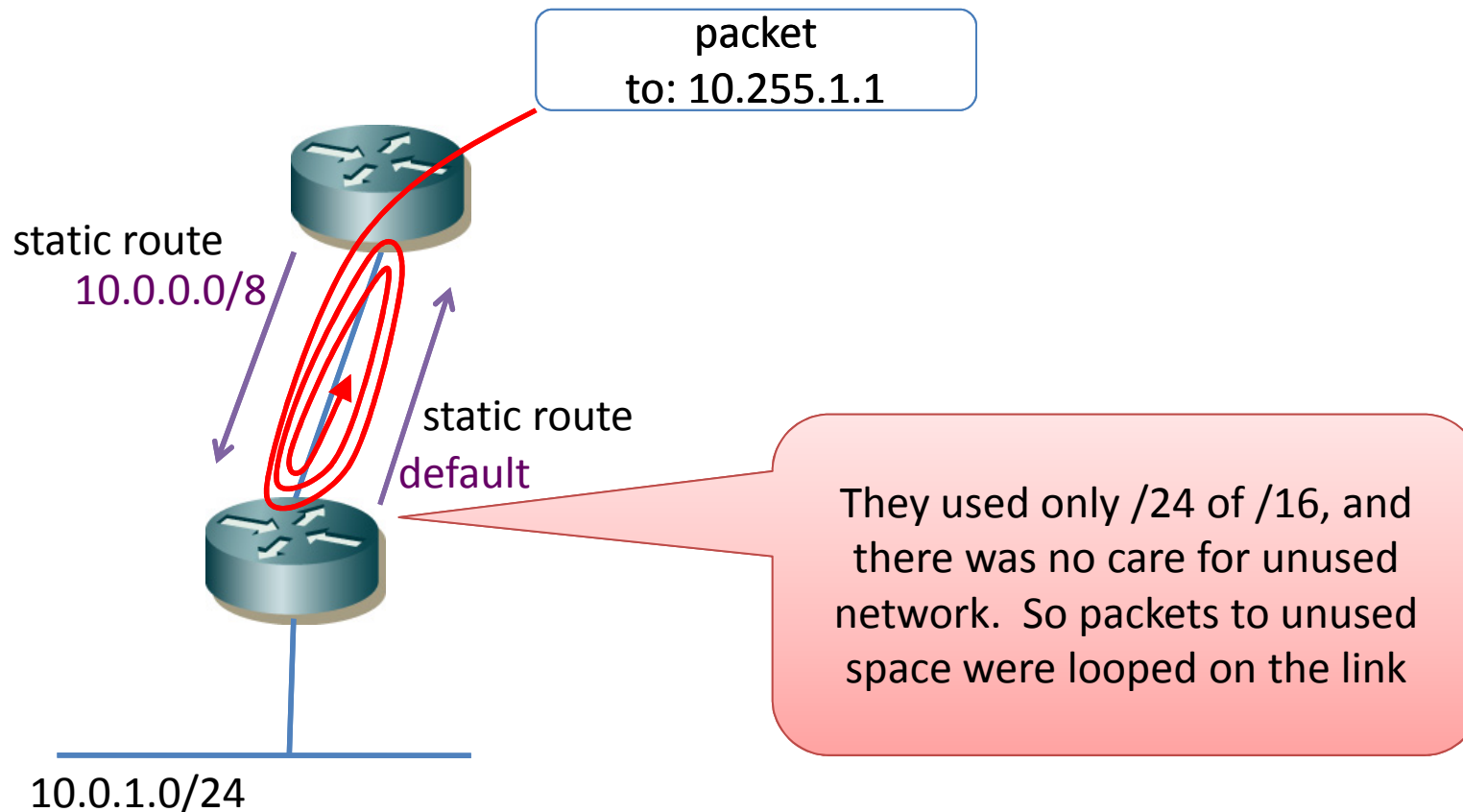
- Unwanted session flapping

No.11 BGP soft reconfiguration

Inbound policy was changed, so try to reevaluate RIB by soft reconfiguration

eBGP

expected command

clear ip bgp neighbor 10.0.0.2 soft in

mistake command

clear ip bgp neighbor 10.0.0.2

eBGP session was reset, ... unwanted session flapping

No.12 route termination

- One prefix was statically routed to a downstream router, and the downstream router had default route to upstream.

- But the downstream network used only a part of the prefix, and no care for unused space. ☹

- Packets to unused space like portscan were looped between 2 routers.
  - they should add a null route to terminate route at the downstream router, or
 - they should adjust the routed prefix as needed

No.12 route termination

packet
to: 10.255.1.1

static route
10.0.0.0/8

static route
default

10.0.1.0/24

They used only /24 of /16, and there was no care for unused network. So packets to unused space were looped on the link

No.13 redistribute

- One person was asked to delete OSPF to BGP redistribution at a router

- The person tried to delete the configuration with leading 'no' keyword, but this deleted filter policy of the redistribution. ☹

- All OSPF routes were redistributed into BGP, and these were announced to other ASes.

No.13 redistribute
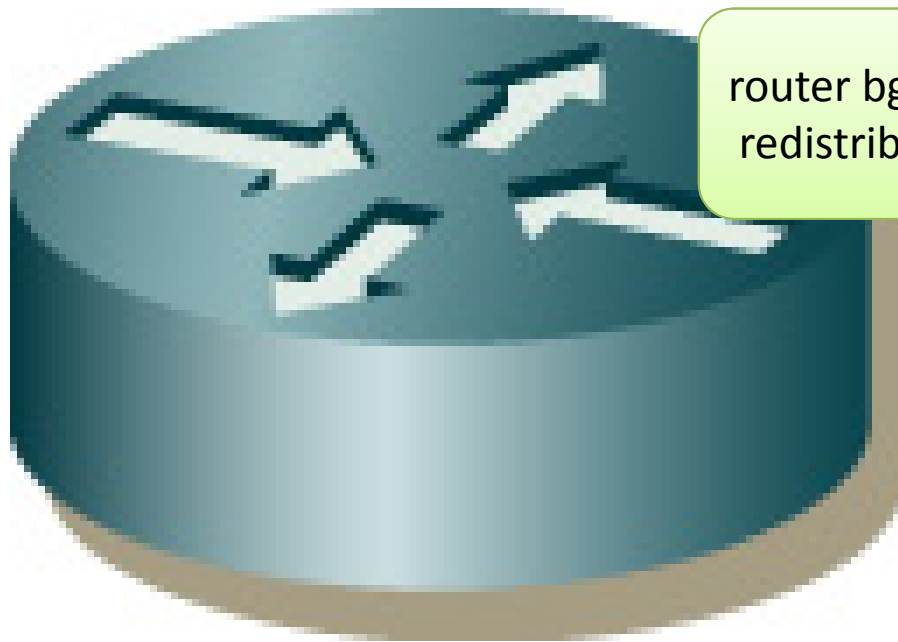
router bgp 65535
 redistribute ospf 65535 route-map ospf-to-bgp

One person was asked to delete entire line, but the person deleted filter policy by leading 'no' keyword

No.14 packet filter

- One person was asked to modify packet filter of a remote router

- The person forgot to permit management access ☹

- After modification, the person was also filtered out, and couldn't control anymore

No.14 packet filter

remote access
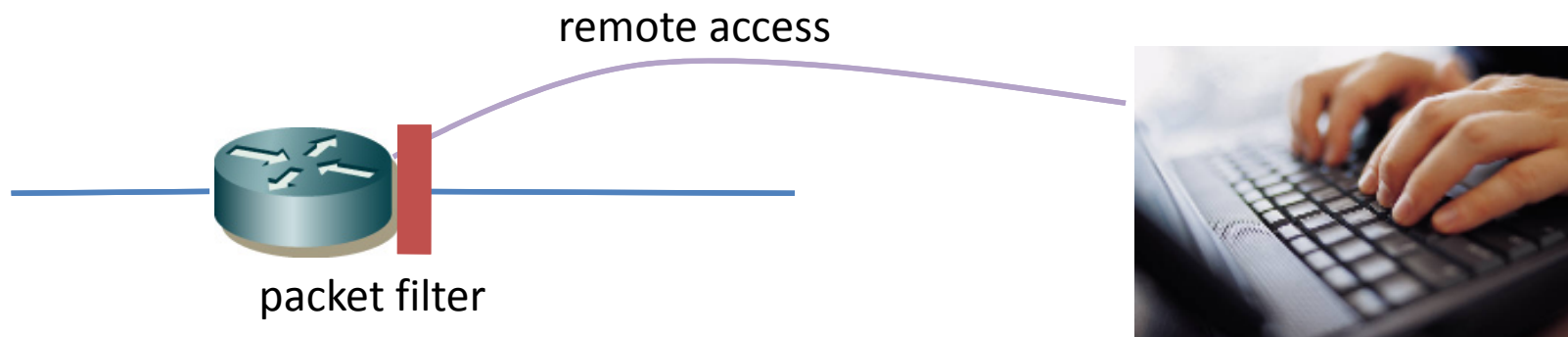
packet filter

One person tried to modify packet filter remotely but the person forgot to permit management access, and lost his remote connection.

No.15 console logging

- A router was configured to send log messages to a serial console port

- One person enabled debug on the router, and tons of messages were sent to console. ☹

- The serial console was low speed like 9600bps, and the tons of messages chewed up the port. The router became unstable…

No.15 console logging

One person enabled debug on a router, and tons of log messages were sent to a serial console.
This was enough to chew up the port, and router became unstable.

serial console   speed=9600

Jul 6 21:50:26 487: LC/0/1/CPU0:Jul 6 21:50:26.275 JST-9: jacket[163]: %L2-SPA-5-STATE_CHANGE : SPA in bay 1 Initing
Jul 6 21:50:29 488: LC/0/1/CPU0:Jul 6 21:50:29.569 JST-9: jacket[163]: %L2-SPA-5-STATE_CHANGE : SPA in bay 1 now is up and running
Jul 6 21:50:30 489: RP/0/RP0/CPU0:Jul 6 21:50:30.017 JST-9: invmgr[206]: %PLATFORM-INV-6-NODE_STATE_CHANGE : Node: 0/1/1, state: OK
 :

No.16 remote login

- One person was asked to change configuration on a certain router.

- The person mistyped the remote hostname, but it was still valid one, so the person changed configuration on a wrong router ☹
  - There was a similar case that typing in a wrong terminal among multi terminal windows.

- ..causes an unexpected routing

No.16 remote login

rt010bb101

rt011bb101

One person was asked to change configuration HERE!

remote access

The person mistyped the hostname, but it was still valid one.
The person changed configuration on a wrong router
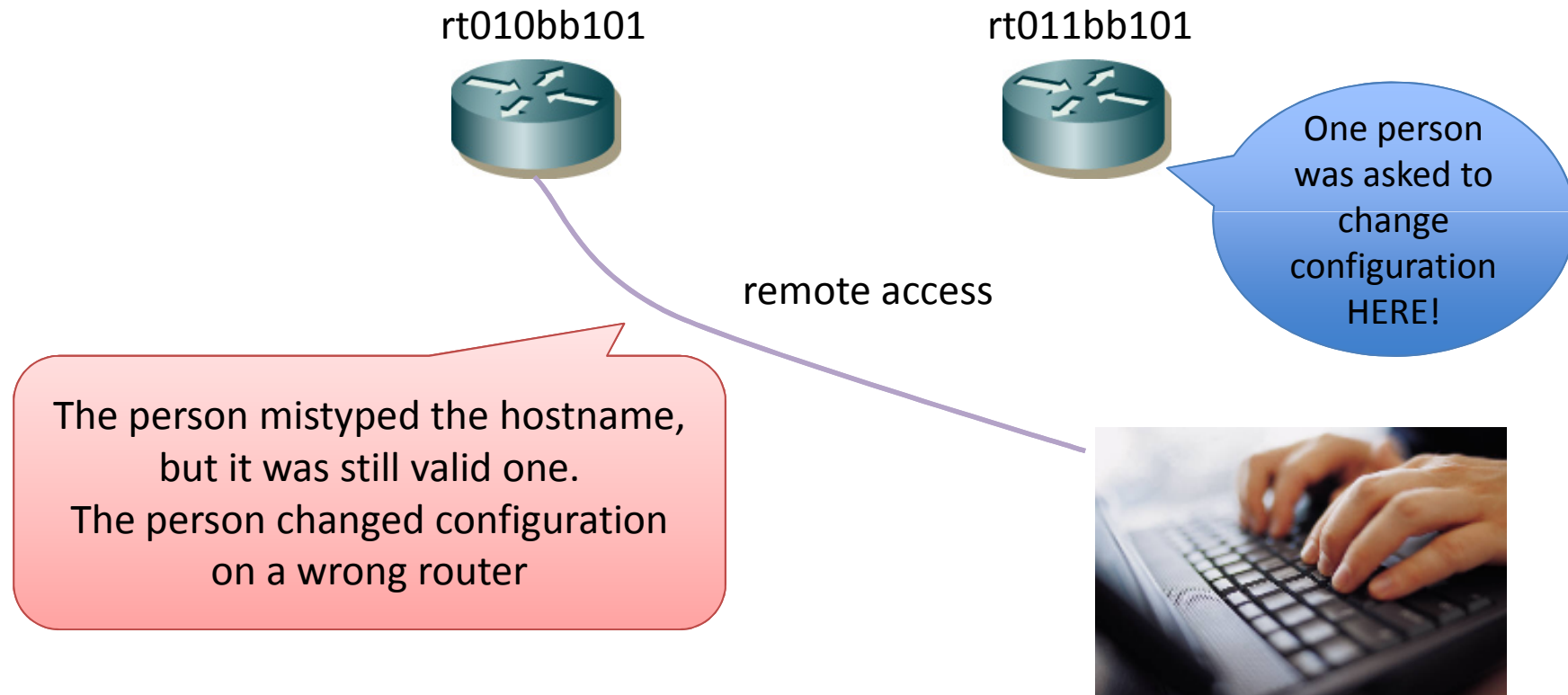
No.17 serial console login

- One person tried to change configuration through serial console, but before that someone used the console terminal to access a remote router, and the session was still there.

- The person was unaware of that and changed configuration on a wrong router ☹
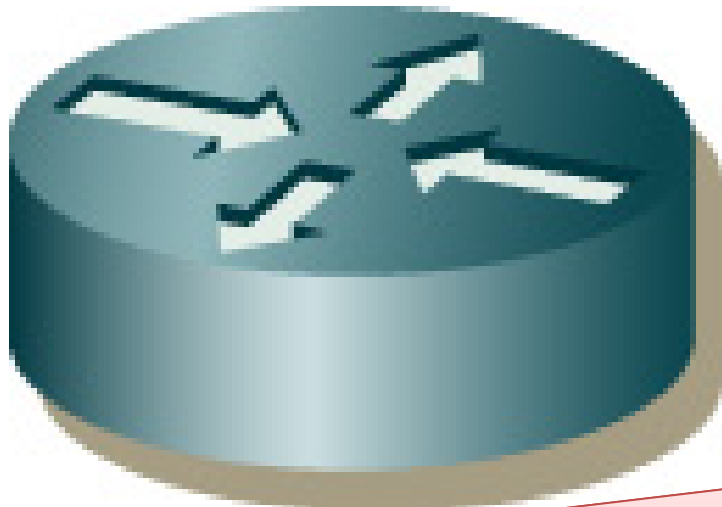
- …. caused unexpected routing

No.17 serial console login

remote access

rt010bb101

rt011bb101

One person was asked to change configuration HERE!

someone used the console to login the other router, and the session was still there

serial console

The person was unaware of that, and changed configuration on a wrong router
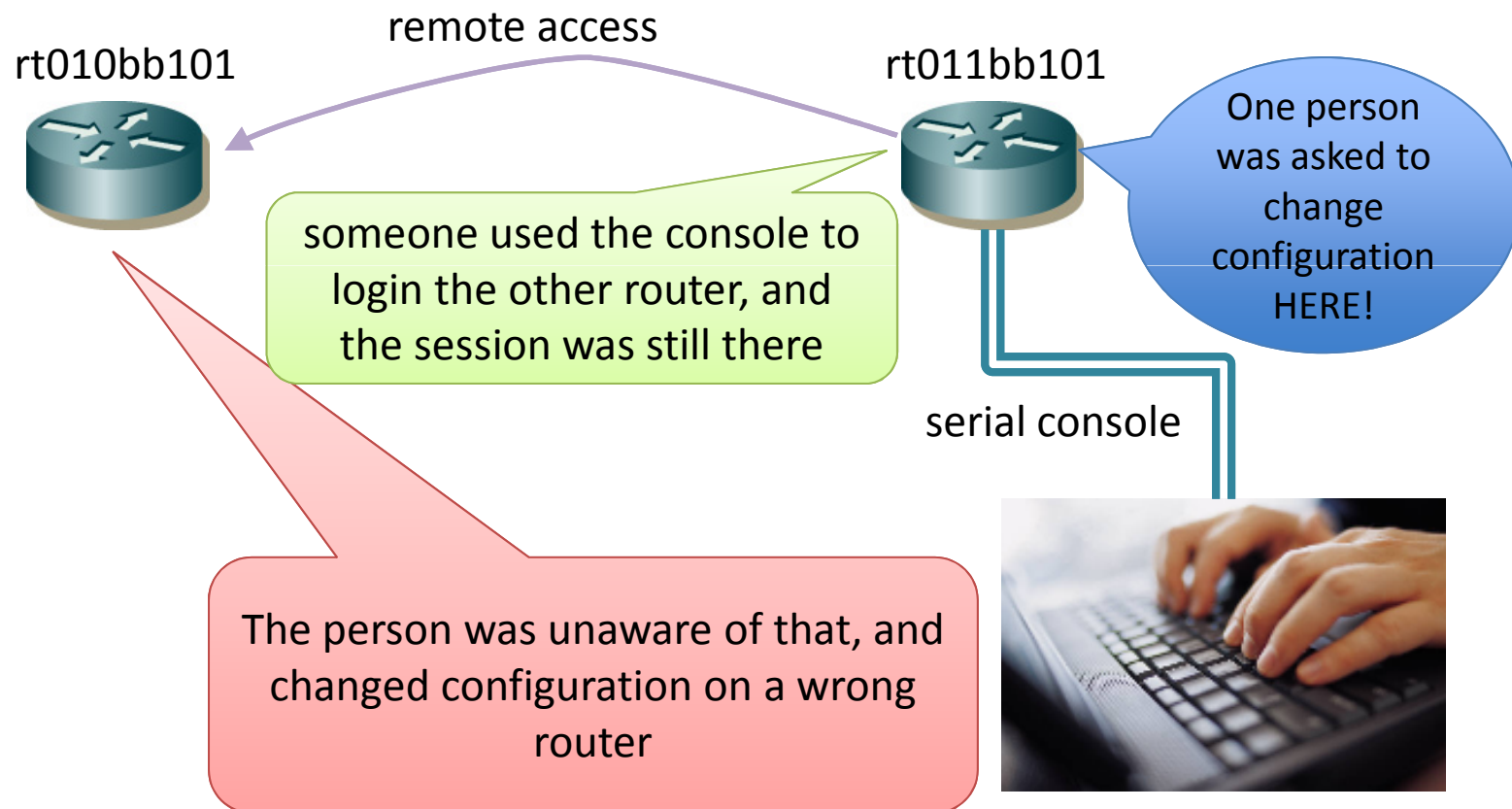
No.18 configuration cleaning

- One person was asked to delete unused configuration of a router

- The person deleted line by line with leading 'no' keyword, and carelessly deleted a routing process. ☹

- The router stopped the routing process as the command said so…..

No.18 configuration cleaning

expected configuration

router ospf 65535
 no network 10.0.0.0 0.0.0.3 area 0

but typed in

no router ospf 65535
 no network 10.0.0.0 0.0.0.3 area 0

The routing process was stopped,
… caused a routing trouble

No.19 bug

- new firmware, new future, new attribute
- It was tested before install, but in a live network sometimes something is different.

No.19 bug

No.20 remote access from home

- One person accessed a router from home.
- Suddenly "Daddy!!!!" – his kid ran into him, and then due to the shock, he pasted buffer to the terminal. ☹
- fortunately, any of the lines were not accepted by the router – just errors.

No.20 remote access from home
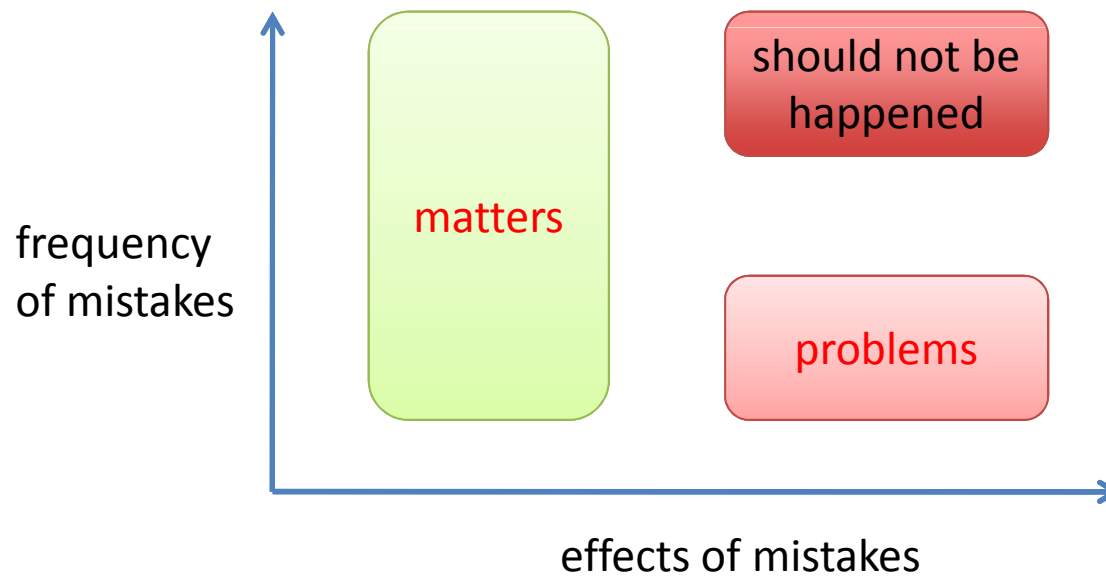
surprise
ひっくり

What we want

- to keep our services available
  - react to anything that causes service deterioration
  - mistake is also a cause of deterioration
  - even more we aim for better services

- minimize the effect of mistakes

react to mistakes

- minimize the effects
- reduce mistakes

minimize the effects of mistakes

- protection
  - straiten the extent of the impact
    - multiple route filters
- restoration
  - detect in early stage
    - monitor of configuration changes, traffic anomaly detection
  - notification properly
    - notify the operator of the mistake
  - recovery from mistake quickly
    - undo the modification, disconnect the wrong part

reduce mistakes

- In many cases, the main reason of mistakes is "careless"
  - more detailed classification would be possible
  - as you might know, to understand others (even yourself) is difficult

mistake, operators and attention

- OK, let's put an assumption

- An attention ability is limited, and it depends on operators and environments
  - If you have enough ability to complete an operation, there would be zero-mistake.

but according to our experiences

- We have made lots of mistakes
  - we don't have enough ability, or have abilities to mistake :P

- So we need a support to reduce mistakes

support for operation

- **minimum hand-operation**
  - automation
- **clear procedure of operation**
  - operation sheet

we have done that, and keep improving

- **support for attention**
  - better user interface to help operations

end

2010 (c) Internet Initiative Japan Inc.