MikroTik User Meeting 2015

Czech republic - Prague

Layer3
High availability
By: Ali Sami

MikroTik Certified trainer
www.mikrotik4me.com
https://www.facebook.com/MikroTik4ME

Presenter

Ali Sami – From Iraq - Baghdad

Almost 11 Year using Mikrotik.

MTCNA (2008) MTCTCE-MTCWE-MTCUME-MTCRE-MTCINE

The First Arab Mikrotik Certified Trainer sine 2011

Professional Certified from other vender.

Working in IT field sine 1999

Current feeling (Mikrotik is morphine in my blood)

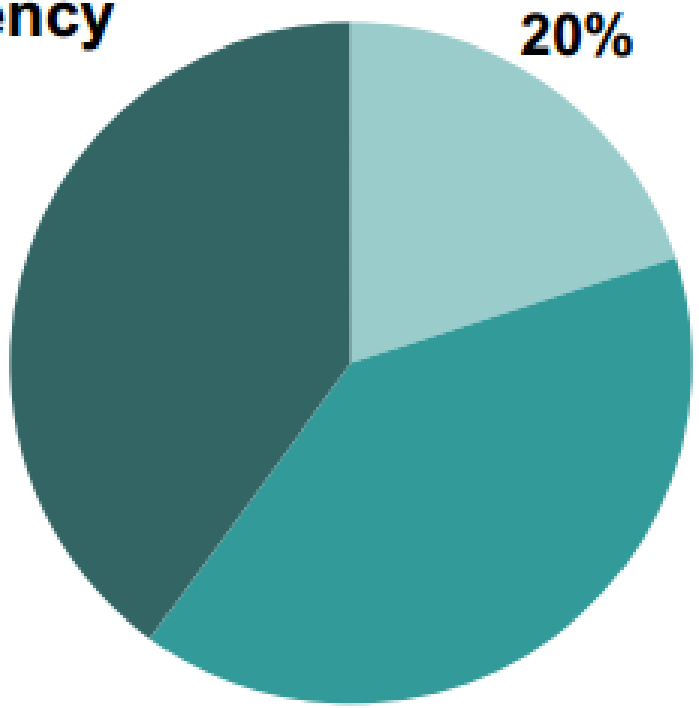
Introduction…

- High availability refers to a system or component that is continuously operational for a desirably long length of time.
- known as "five 9s" (99.999%) availability.

Availability	Downtime per Year (24x7x365)		
99.000%	3 Days	15 Hours	36 Minutes
99.500%	1 Day	19 Hours	48 Minutes
99.900%		8 Hours	46 Minutes
99.950%		4 Hours	23 Minutes
99.990%			53 Minutes
99.999%			5 Minutes

Top case of down time

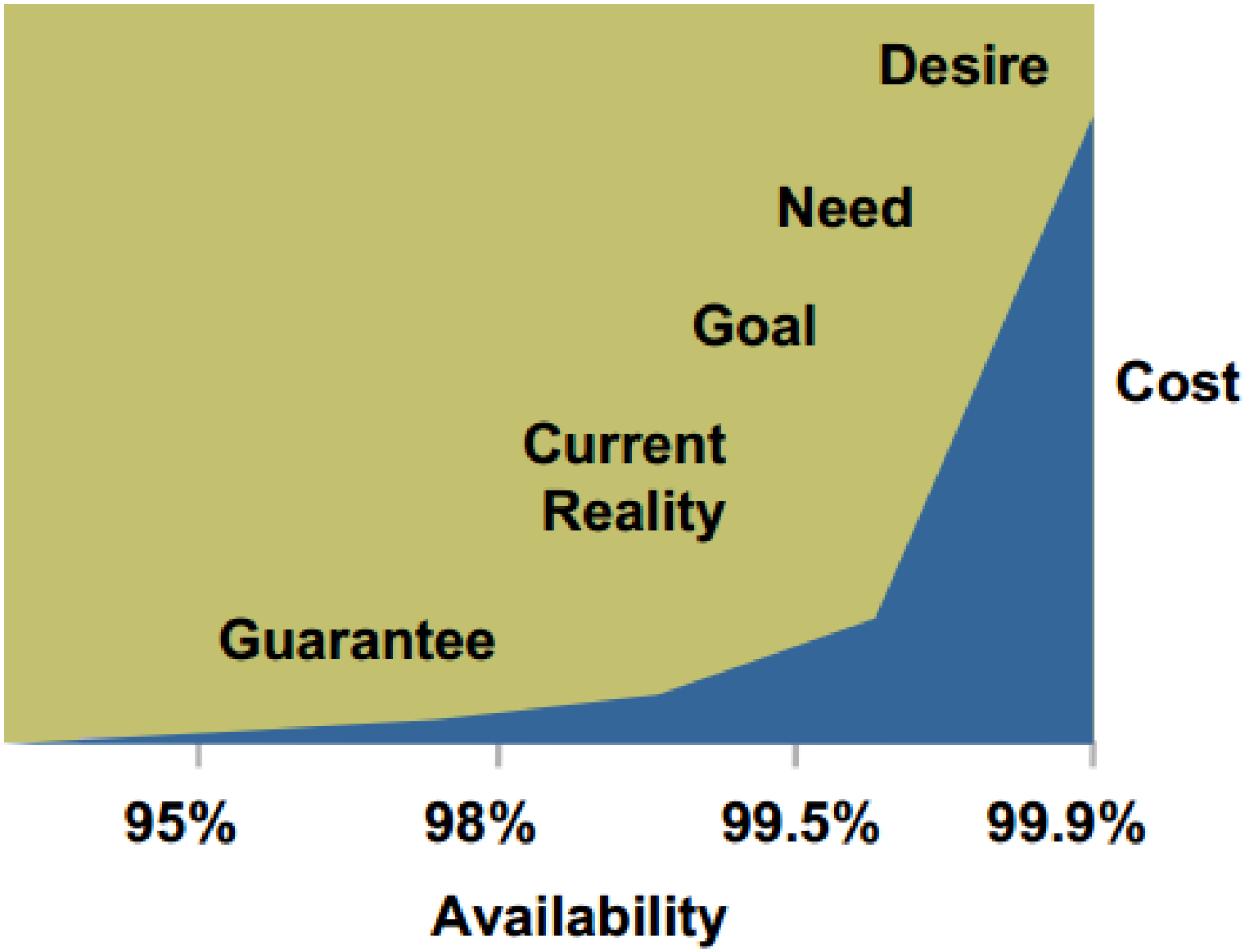
- Change management
- Process consistency
- Methodology
- Communication



- Hardware
- Links
- Design
- Environmental issues
- Natural disasters

- Software issues
- Performance and load
- Scaling

Availability investment



Availability calculation

Calculated Availability based on MTBF and MTTR

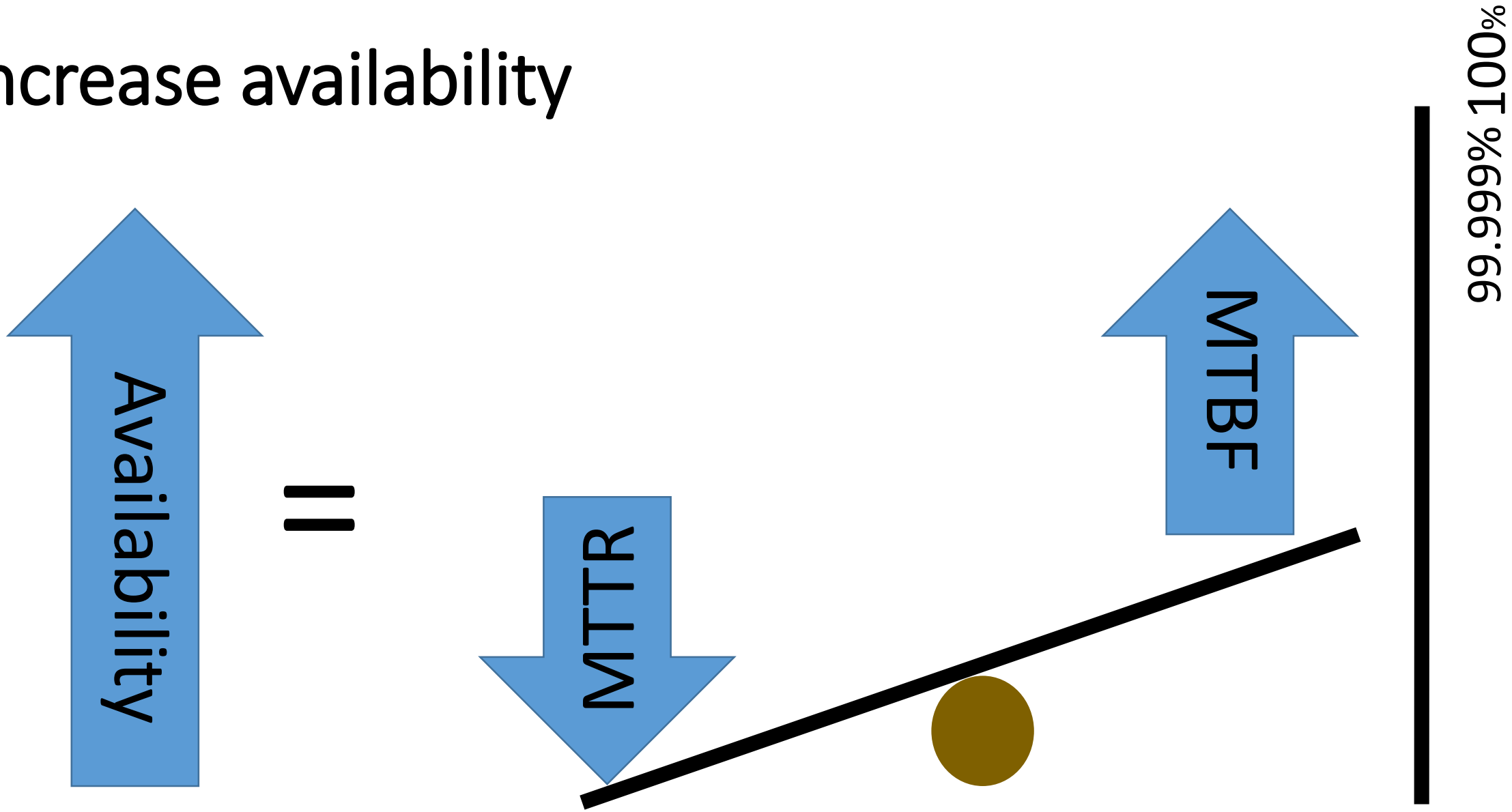
- **Mean time = average time.**
- **MTTR =** Mean Time To Repair.

  The average time required to troubleshoot and repair failure and return network it to normal operating. MTTR=(Total up time / total down time).
- **MTBF=** Mean Time Between Failures

  The average time elapsed from one failure to the next.

  MTBF = (Total UpTime / Total number of failure)
- Availability = (MTBF/(MTBF+MTTR) = availability in %

Increase availability

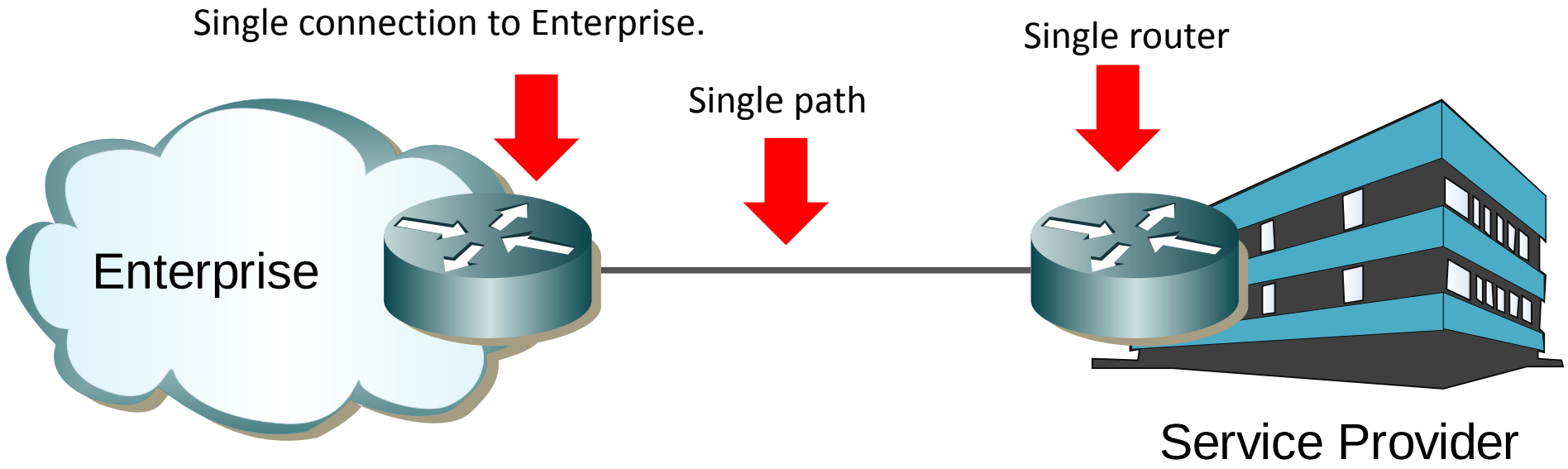


Top case of increase availability (count.)

- **Verified network design**
- **Simplified network design**
- **Less hardware**
- **Physical redundancy**
- **Right management process**
- **Network monitoring tools**

Availability calculation (cont.)

With 3 Single point of Failure



99.925%

Availability calculation Case #1

mpy is minute per Year

Total Enterprise downtime = 10 time maintenance total Time To Repair 120mpy.

Total Path downtime = 6 Time maintenance total Time to Repair 180mpy.

Total Local router downtime = 14 times maintenance total Time To Repair 90mpy.

Total down time = 390mpy (6.5 Hours)

Total repair time per year = 30

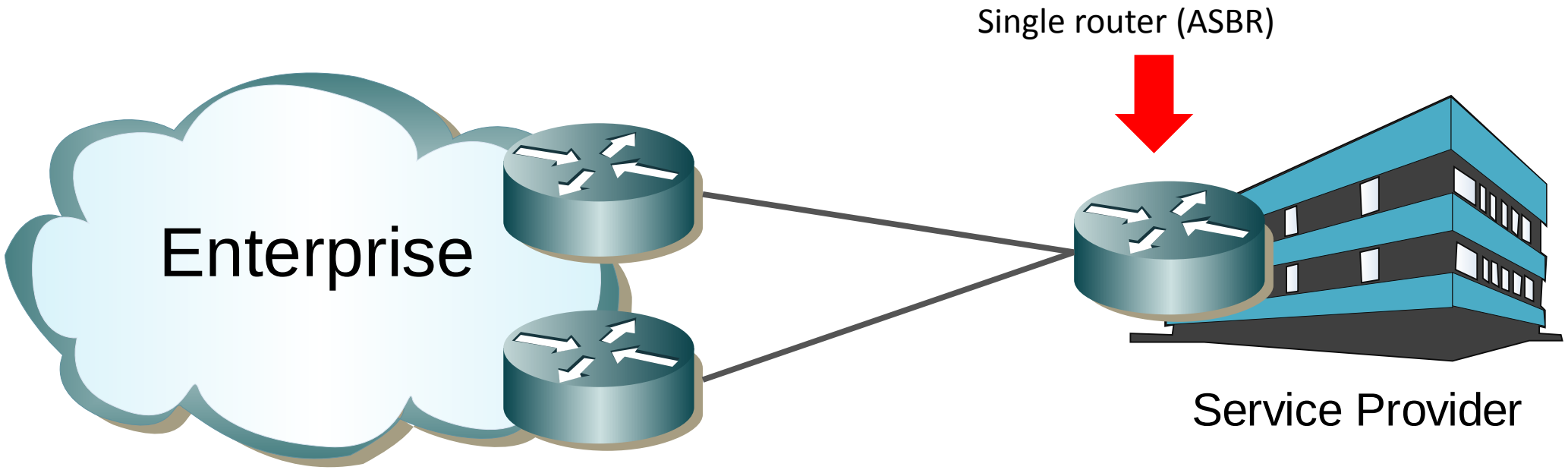
MTTR = 390(total down time per Year)/30 (total repair time per year =13minute

MTBF = 518400 (mpy)/30 = 17280mpy (12 days)

Availability = 1330 mpy (MTBF) / (1330 + 13) * 100 = 99.925%.

Availability calculation (cont.)

With 1 Single point of Failure



99.983%

Availability calculation Case #1

Total Local router downtime = 14 times maintenance total Time To Repair 90mpy.

Total down time = 90mpy (1.5 Hours)

Total repair time per year = 14

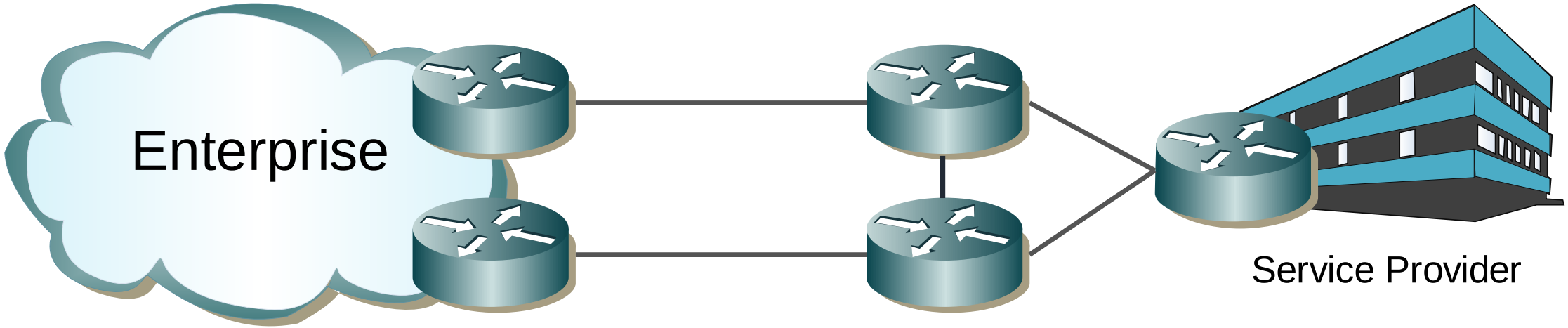
MTTR = 90(total down time per Year)/14 (total repair time per year =6.4minute

MTBF = 518400 (mpy)/14 = 37028mpy (25.5 days)

Availability = 37028 mpy (MTBF) / (37028 + 6.4) * 100 = 99.983%

Availability calculation (cont.)

With NO Single point of Failure



99.999%

Availability calculation Case #1

Total Local router downtime = 14 times maintenance total Time To Repair 7 mpy.

Total down time = 7mpy

Total repair time per year = 14

MTTR = 7(total down time per Year)/ 14 (total repair time per year =0.5 minute

MTBF = 518400 (mpy)/14 = 37028mpy (25.5 days)

Availability = 37028mpy(MTBF) / (37028+ 0.5) * 100 = 99.999%

Network Convergence.

- Converged network : when all routes within network domain operate on unified routing information and forwarding tables are note changing for “some reasonable” amount of time.
- Network convergence: The process of synchronizing network forwarding tables after a topology change. is also known as network restoration.
- **In other word** addresses the manner in which networks recover from problems and network changes.

Presentation Agenda

- Network high availability classification.
- Layer3 High Availability within router.
  - Routing Failover types SO/SSO/(SSO/NSF).
  - RIB and FIB.
  - High availability on OSPF network
  - High availability with BGP.
- Case study
  - Stateful switch over with BGP/SSO.

Network High availability classification

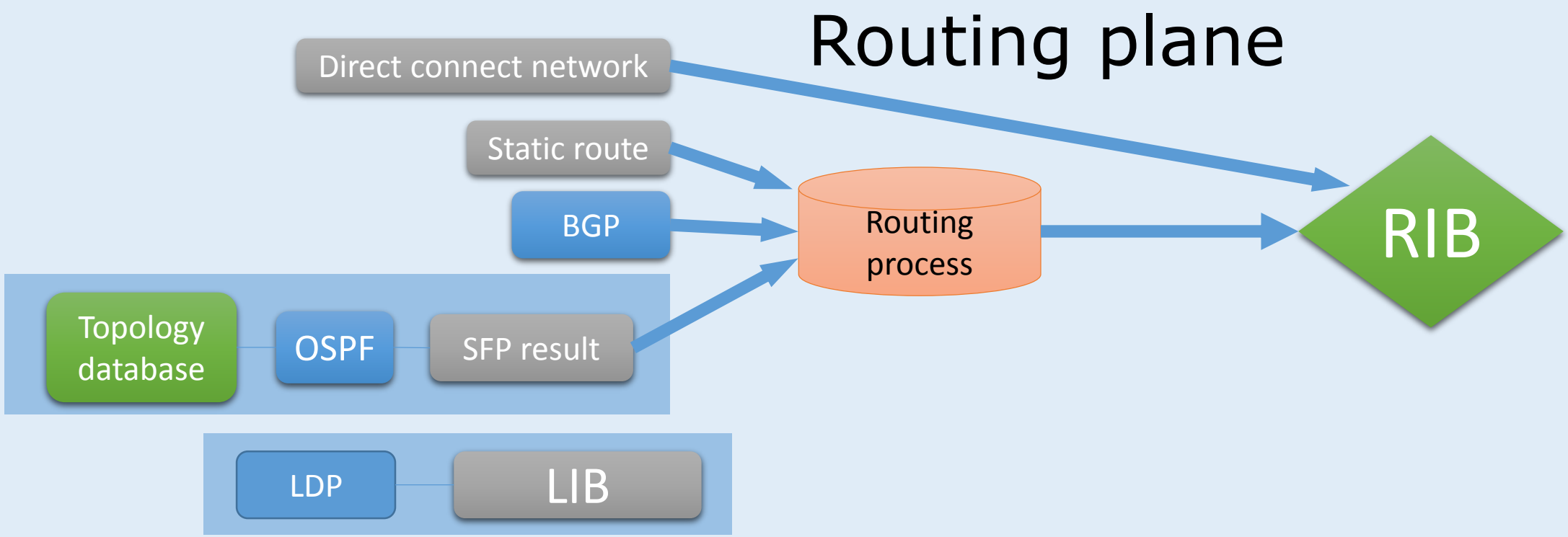
Application Resiliency	**Global Server Loadbalancy CDN – Any Casting**
L3 Resiliency	**Netwatch – ping gatway – AD – OSPF – BGP-VRRP**
L2 Resiliency	**RSTP – LACP (802.3ad) – RSVP-TE**
Physical Resiliency	**Redundant power supply – path diversity**

Layer 3 High availability within router.

- Routing information Base (RIB)
- Forwarding information Base (FIB)
- Switch Over (SO).
- Stateful Switch Over (SSO).
- Stateful Switch Over with none stop forwarding (SSO/NSF).

Routing Information Base (RIB)

- **Placed in routing plane.**
- where all IP Routing information is stored.
- It is not specific to any routing protocol.
- RIB is NOT used for forwarding IP datagrams.
- Entries in RIB are advertised to other routers via Dynamic routing protocols.

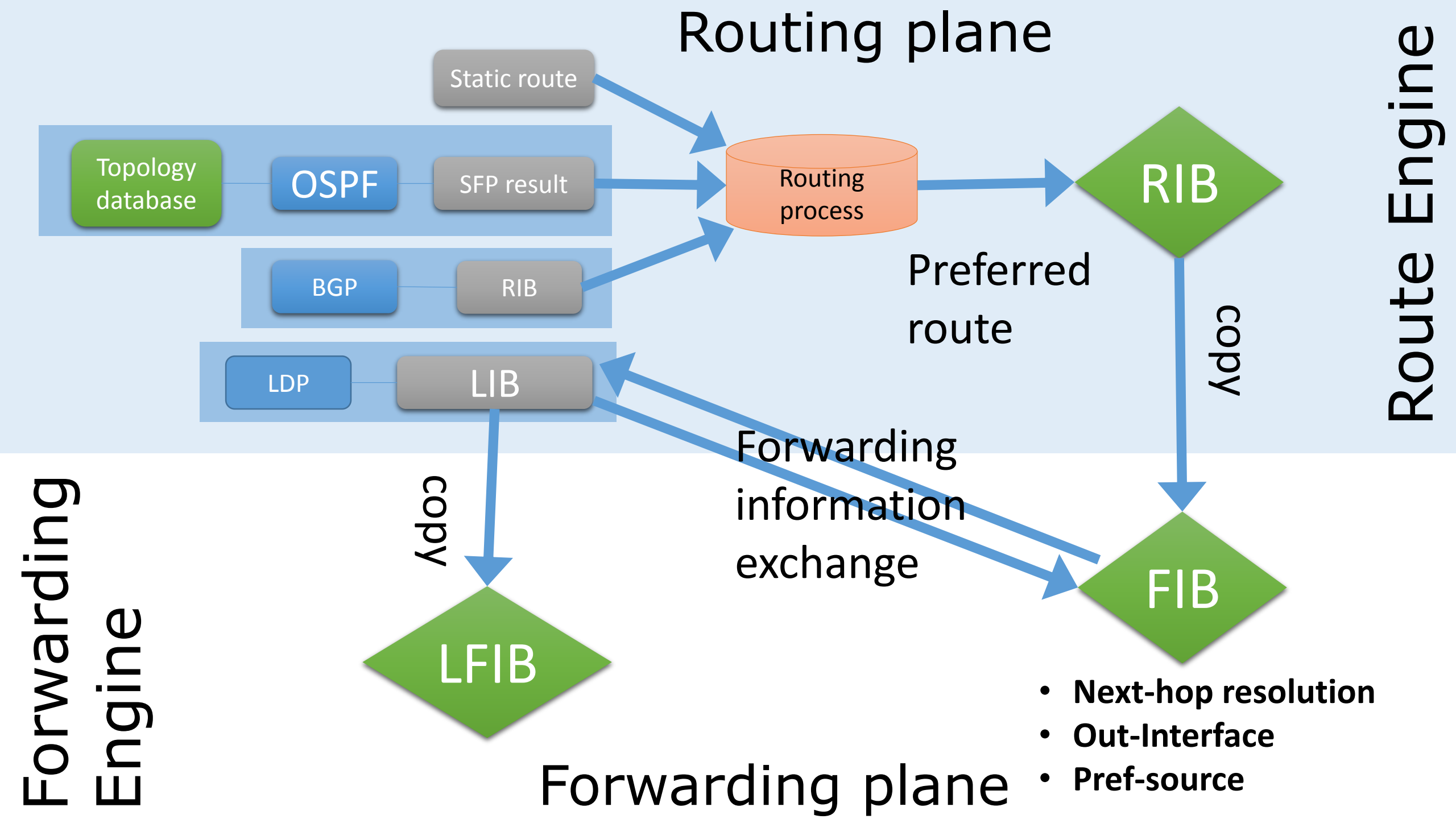


Forwarding Engine

Forwarding plane

Forwarding Information Base (FIB)

- **Placed in Forwarding plane**
- Used to make IP destination prefix-based switching decisions.
- Contains the interface identifier and next hop information for each reachable destination network prefix.
- When IP routes are copied from routing table to FIB, their next hops are resolved with outgoing interfaces and preferred source.
- **The number of entries within a forwarding information base is one of the key elements that may influence the forwarding performance of a router.**

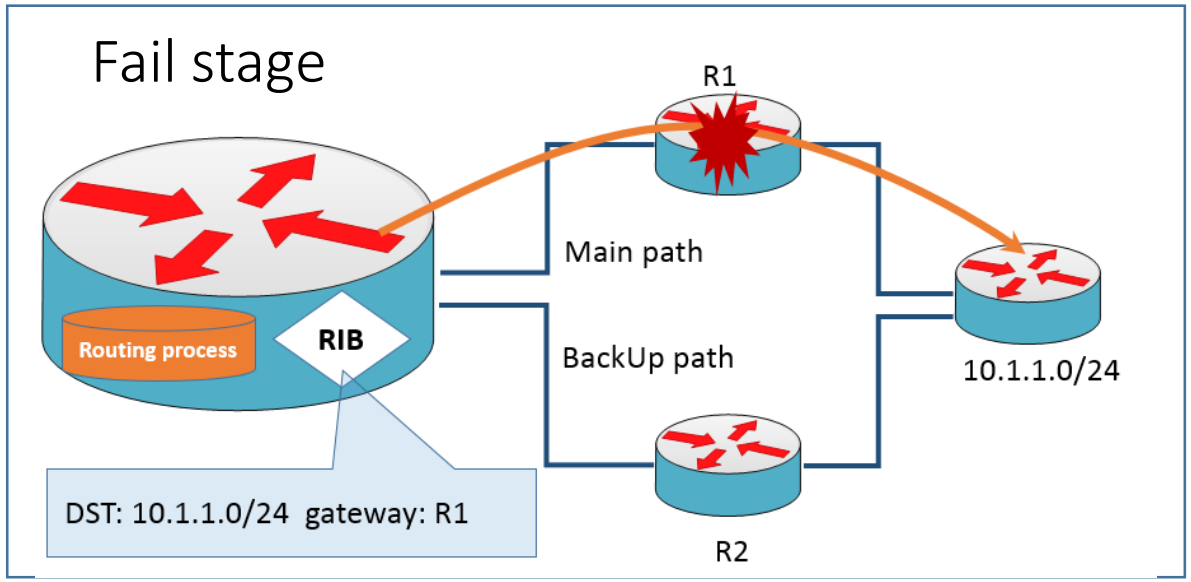

Routing plane
Route Engine
Static route
Topology database
OSPF
SFP result
BGP
RIB
LDP
LIB
Routing process
RIB
Preferred route
copy
Forwarding information exchange
copy
LFIB
FIB
Forwarding Engine
Forwarding plane
• Next-hop resolution
• Out-Interface
• Pref-source

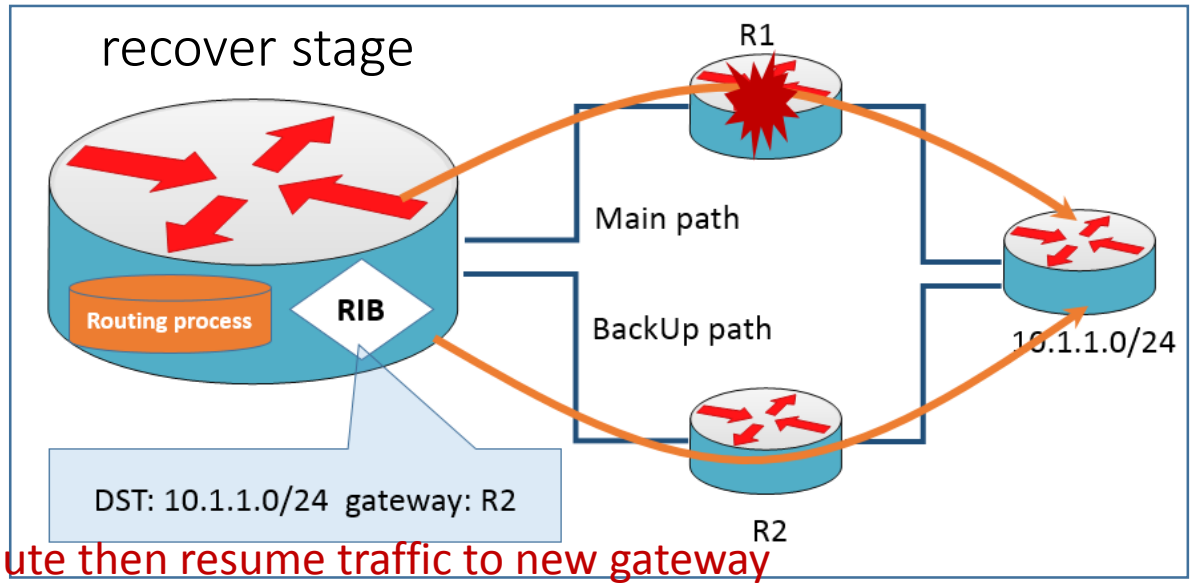
Routing Fail over

- Failover is the process in which networks automatically detect service interruptions and adjustments and switch over to an alternate path.
- Switch Over
- Stateful Switch over
- Stateful switch over with none stop forwarding.

Switch Over

- Switch traffic from Gateway to another.
- Mean new routing calculation process need to be executed, then preferred route will installed in RIB.
- FIB will stop forwarding during this process.





Link fail

Seq #	Host	Time	Reply Size	TTL	Status
39	192.168.200.1	0ms	50	63	
40	192.168.200.1	0ms	50	63	
41	192.168.200.1	timeout			timeout
42		timeout			no route to host
43		timeout			no route to host
44		timeout			no route to host
45	192.168.200.1	0ms	50	63	
46	192.168.200.1	0ms	50	63	

Old route withdrawal & Routes calculation and install new route then resume traffic to new gateway

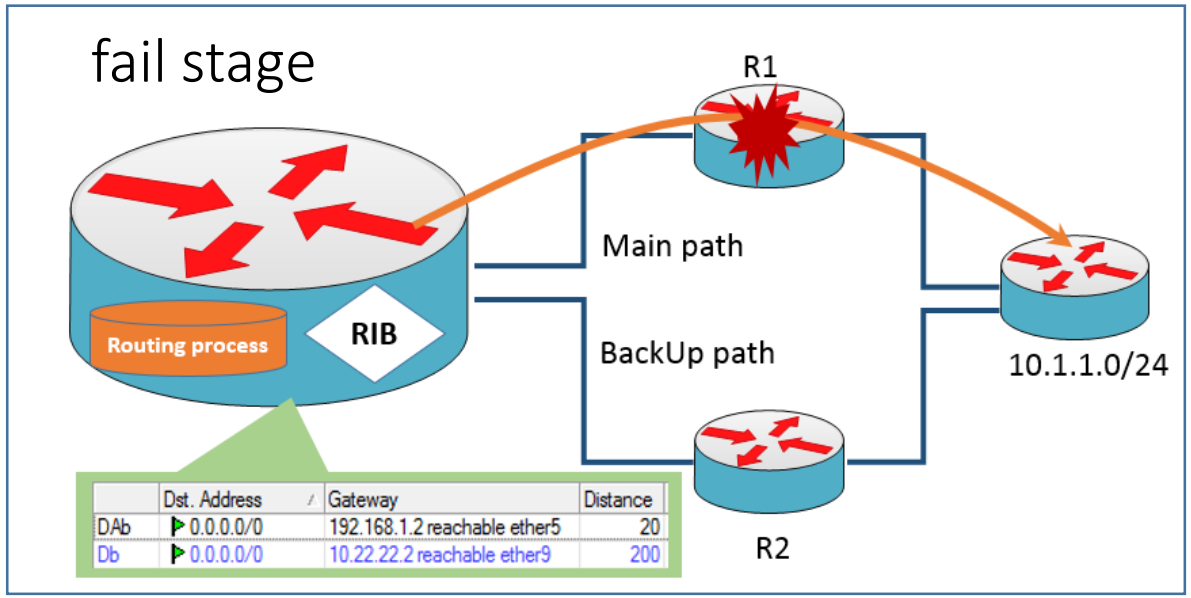
Stateful Switch Over

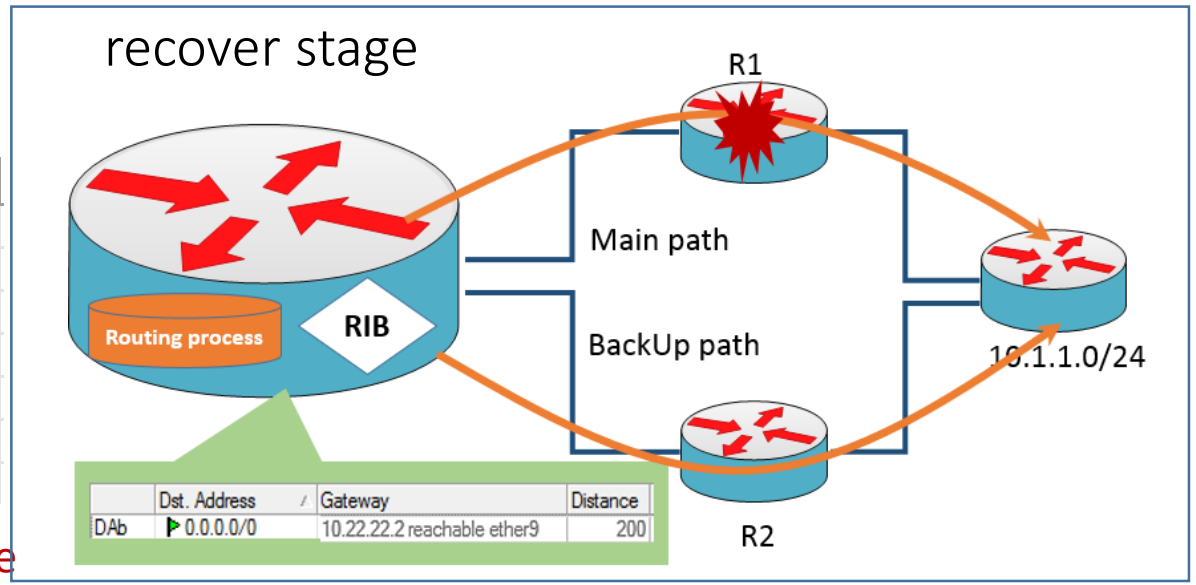
- Switch traffic from Gateway to another.
- There is Already route available in RIB for backup gateway but in Standby mode no need to recalculation.
- Will take less time to activate standby route than install new route.
- FIB will stop forwarding during this process.

Seq #	Host	Time	Reply Size	TTL	Status
15	192.168.200.1	0ms	50	63	
16	192.168.200.1	1ms	50	63	
17	192.168.200.1	timeout			timeout
18	192.168.200.1	timeout			timeout
19	192.168.200.1	timeout			timeout
20	192.168.200.1	1ms	50	63	
21	192.168.200.1	2ms	50	63	

Stateful Switch Over

- Switch traffic from Gateway to another.
- There is Already route available in RIB for backup gateway but in Standby mode no need to recalculation.
- Will take less time to activate standby route than install new route.
- FIB will stop forwarding during this process.



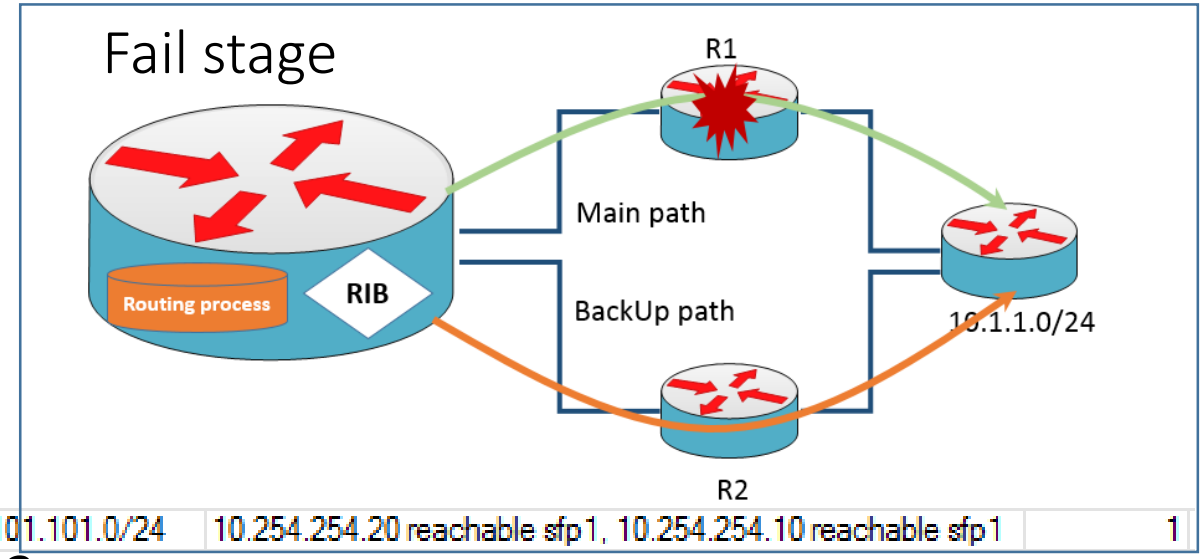


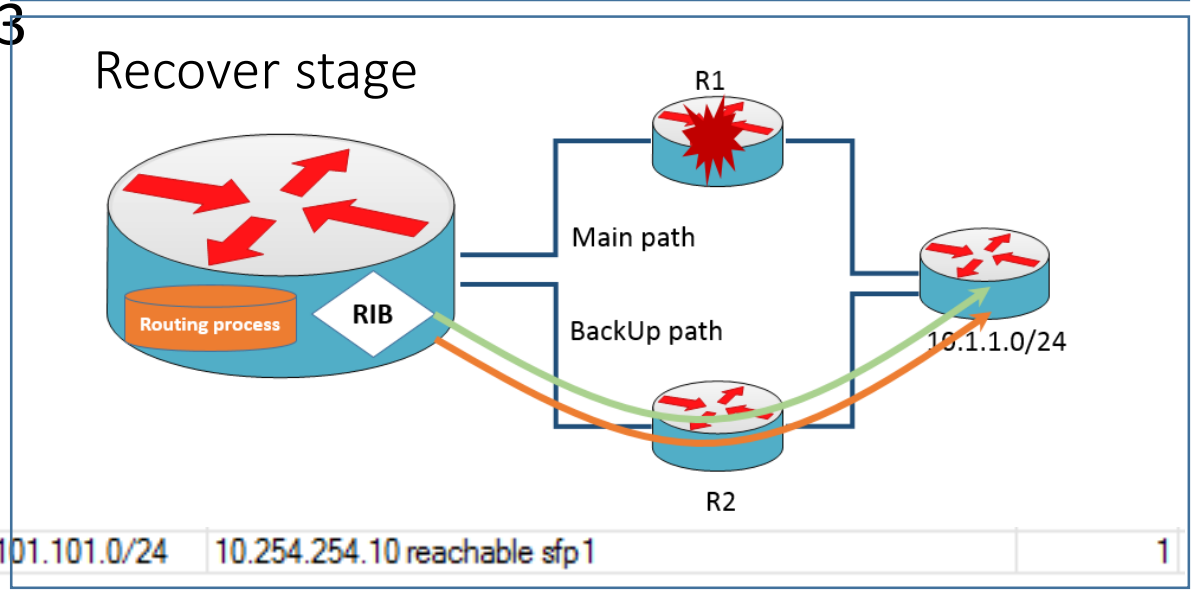
Seq #	Host	Time	Reply Size	TTL	Status
15	192.168.200.1	0ms	50	63	
16	192.168.200.1	1ms	50	63	
17	192.168.200.1	timeout			timeout
18	192.168.200.1	timeout			timeout
19	192.168.200.1	timeout			timeout
20	192.168.200.1	1ms	50	63	
21	192.168.200.1	2ms	50	63	

link fail & Switch over traffic to available route

Stateful Switch Over with none stop forwarding

- Switch traffic from Gateway to another.
- There is Already active route available in RIB for new gateway.
- No calculation no reactivation.
- FIB will keep forwarding during this process.
- For Mikroitk ROS Available only in ECMP and L3 Interface bonding .
- ECMP convergence time its about 200ms.
- LACP convergence time is about 50ms.





High availibitly at OSPF network

- OSPF route Selection.
- OSPF network convergence time
- Tuning OSPF convergent time for high availibitly.

OSPF route Selection

- There are six route types in the OSPF network.
  - Intra-area routes. (Highest preferred)
  - Inter-area routes.
  - External Type-1 routes.
  - External Type-2 routes.
  - NSSA Type-1 routes.
  - NSSA Type-2 routes. (Lowes preferred)

OSPF route Selection

OSPF will choose routes in the following order:

- If there is multiple routes, then routes compared by type.
- If there is Multiple routes same type then compare by cost.
- If there is Multiple routers same type and same cost then will install multiple routes. (router will does ECMP)

Note : Usually only selected routes will be offer to install in RIB

OSPF Network convergence time

- Most of the important operations of OSPF that contribute to convergence, controlled by timers.
- ***Convergence total time = Failure_Detection_Time + Event_Propagation_Time + SPF_Run_Time + RIB_FIB_Update_Time***

The formula reflects the fact that convergence time for a link-state protocol is sum of the following process:

- **Detect the network failure**, e.g. interface down condition.
- **Propagate the event** by flood the LSA across the topology.
- **SPF calculations** on all routers upon reception of the new information.
- **RIB/FIB update** for all routers in the area.

OSPF Network convergence time (cont.)

Seq #	Host	Time	Reply Size	TTL	Status
10	101.101.101.1	0ms	50	62	
11	101.101.101.1	0ms	50	62	
12	101.101.101.1	timeout			timeout
13	101.101.101.1	timeout			timeout
14	5.10.224.5	0ms	78	64	net unreachable
15	5.10.224.5	0ms	78	64	net unreachable
16	5.10.224.5	0ms	78	64	net unreachable
17	5.10.224.5	5ms	78	64	TTL exceeded
18	5.10.224.5	5ms	78	64	TTL exceeded
19	101.101.101.1	0ms	50	62	
20	101.101.101.1	0ms	50	62	

Packet drop due link failure

Network convergence time

- Withdraw route due link failure.
- Failure detection.
- Even propagation
- SPF calculation

- Micro-loop during RIB/FIB update

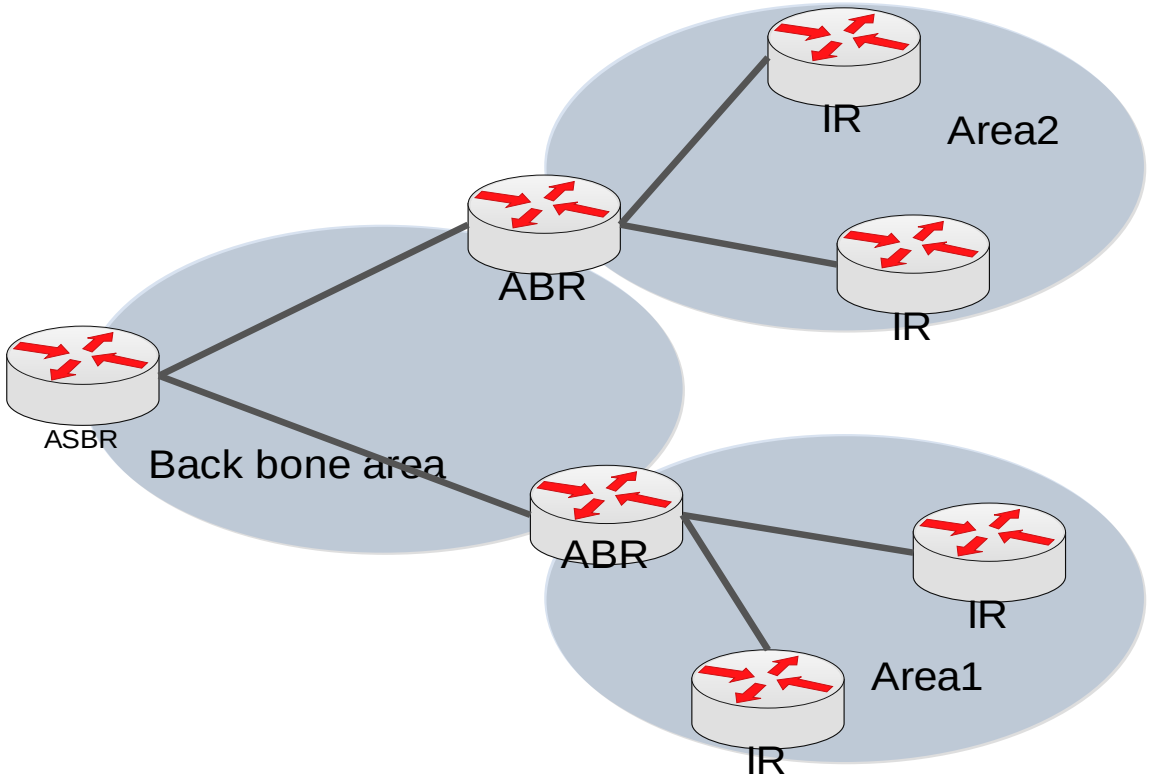
Traffic resumed after install new route

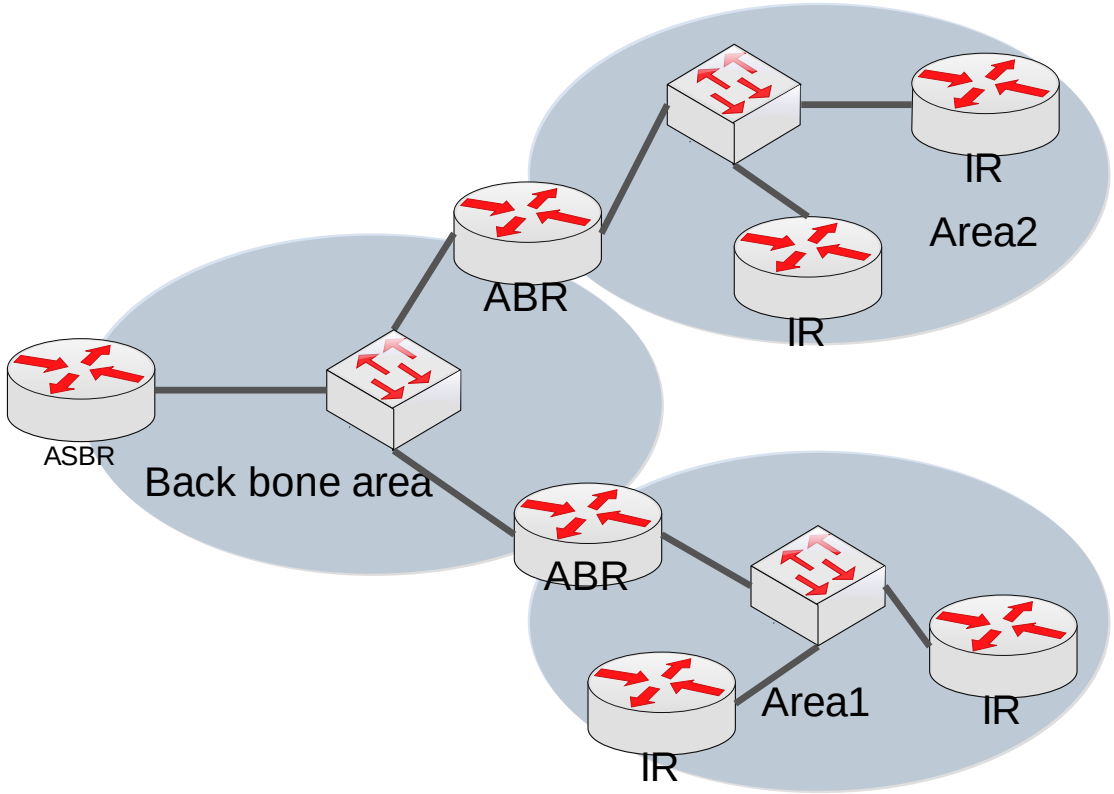
Improve OSPF convergence time with Fast Failure Detection

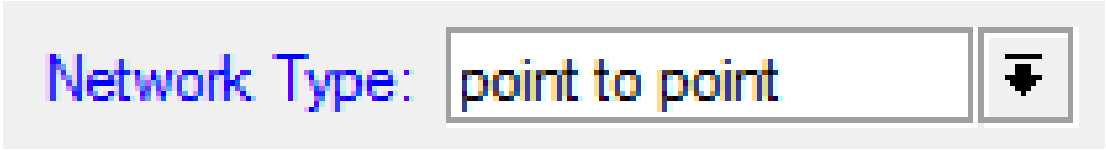
Detecting link and node failures quickly is number one priority for fast convergence.

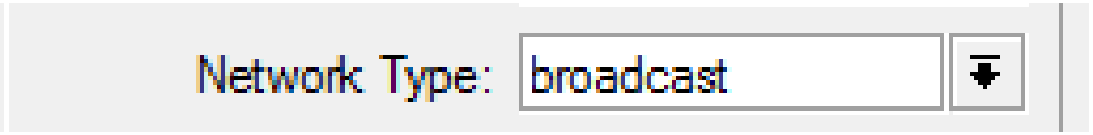
- Use of *physical* point-to-point links whether possible useful at physical failure detection mechanisms.
- Using point-to-point link as network type for faster adjacent, that DR elections are no longer needed.

Improve OSPF convergence time with Fast Failure Detection (cont.)



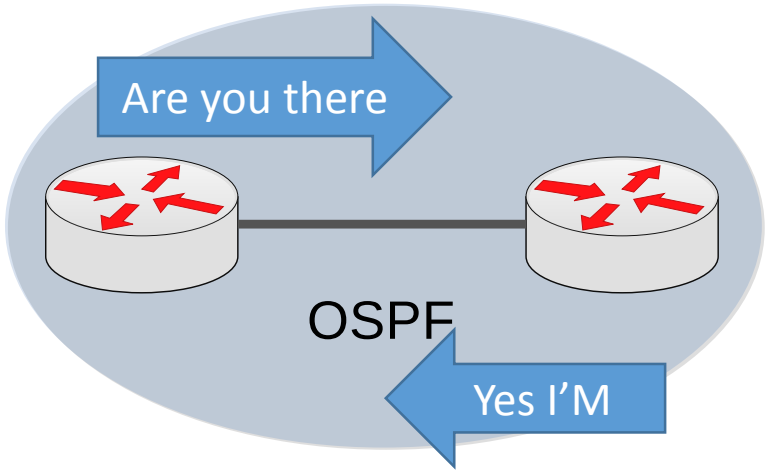






Improve OSPF convergence time with Fast Failure Detection (cont.)

- OSPF routing devices constantly track the status of their neighbors, sending and receiving hello packets that indicate whether each neighbor still is a live.
- Adjusts OSPF hellos with the (Hello-interval/Router-dead-interval) default is 10/40 of seconds change to 1/4 of seconds.



Default parameters

Hello Interval:	10	s
Router Dead Interval:	40	s

Hello Interval:	1	s
Router Dead Interval:	4	s

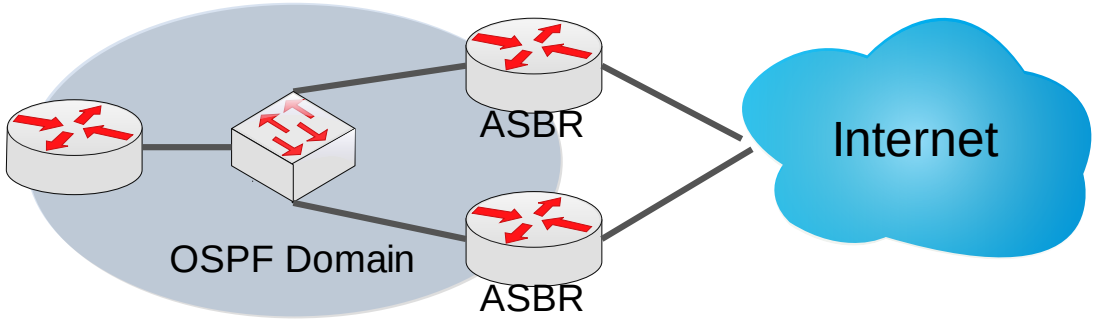
Improve OSPF convergence time with Fast Failure Detection (cont.)

1.

Network Type: broadcast

Hello Interval: 10 s

Router Dead Interval: 40 s

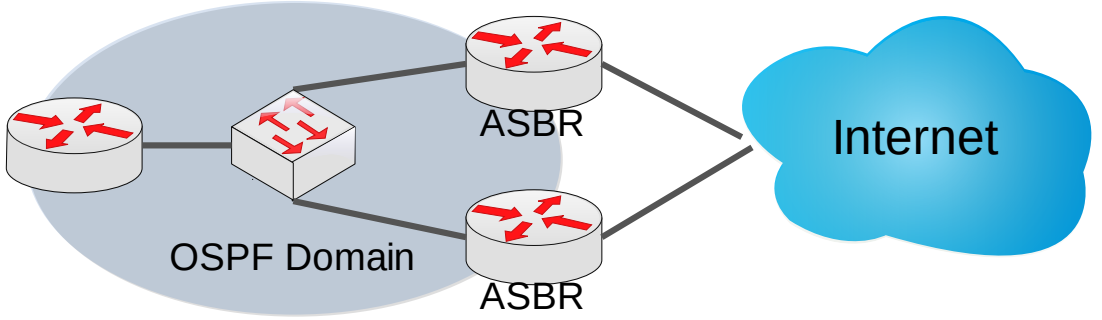


2.

Network Type: broadcast

Hello Interval: 1 s

Router Dead Interval: 4 s

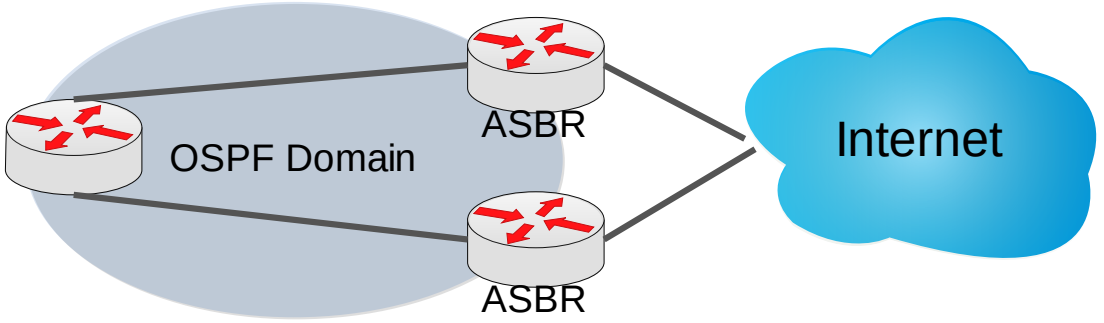


3.

Network Type: point to point

Hello Interval: 1 s

Router Dead Interval: 4 s



Improve OSPF convergence time with Fast Failure Detection (cont.)

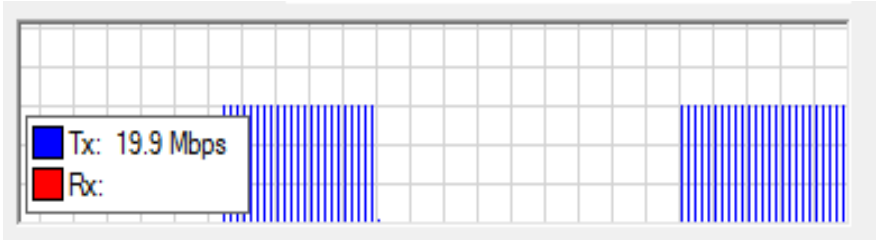
Test:

1- Sending out 40 ICMP packet toward internet. Time-out =1000ms

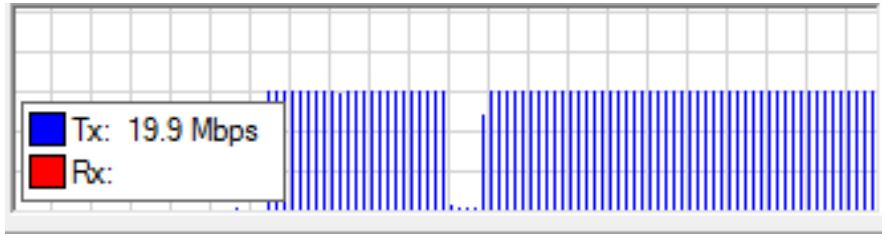
2- Using ROS bandwidth test tool

Result:

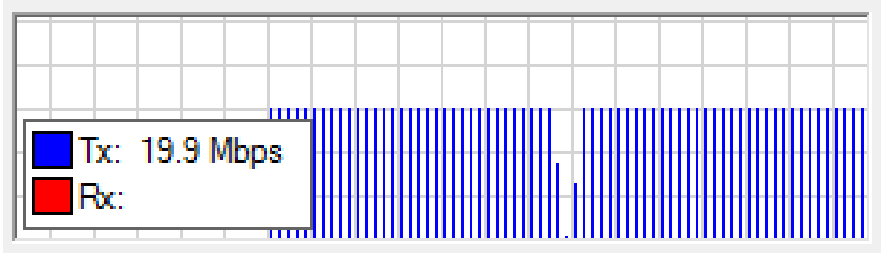
sent=40 received=7 packet-loss=82%



sent=40 received=34 packet-loss=15%



sent=40 received=38 packet-loss=5%



Improve with OSPF convergence time (cont.)

- Event propagation, SPF calculation, RIB/FIB update are Contribute the most of the convergence time in the topologies with large amount of prefixes.

Improve OSPF convergence time (cont.)

Partitioning OSPF network by Areas

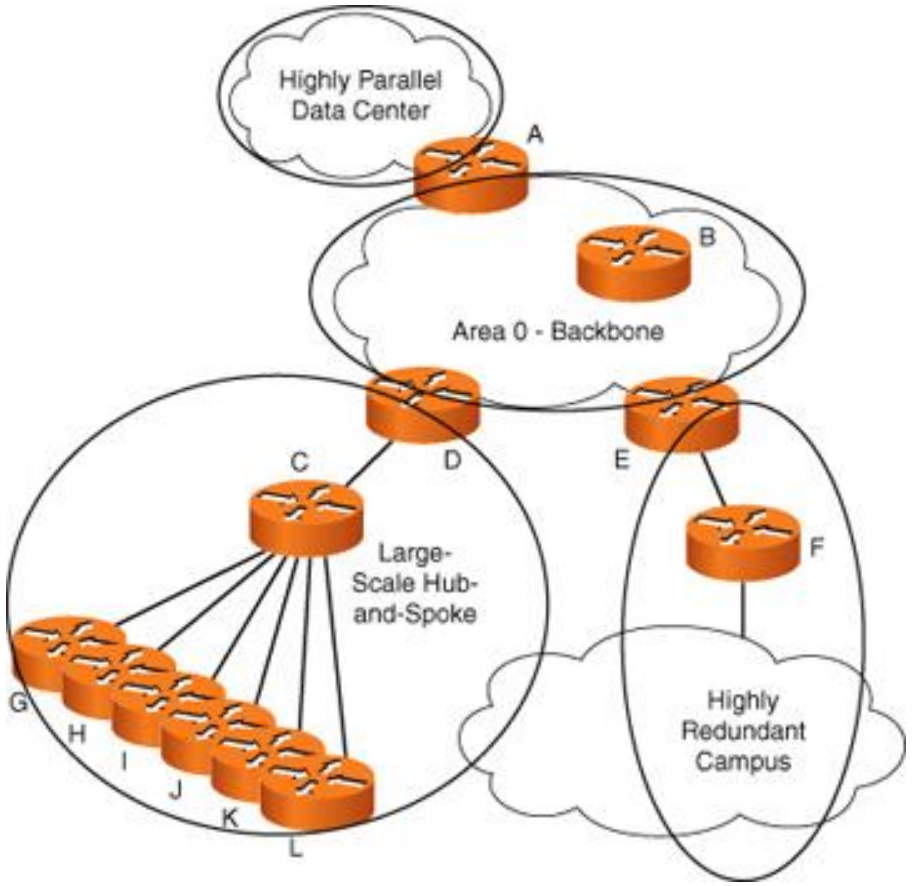
Advantages of OSPF areas

- Suppressing flooding domain.
- Reduced of SPF calculations cause of smaller LSDB.
- Smaller routing table.
- Faster RIB update and propagate to FIB.
- Make noneBackbone area as Stub area or Totally stubby area.

Improve OSPF convergence time (cont.)

Suggestion:

- Make the Backbone Area simple.
- Put the complex network in separated area. such as a full-mesh, a large hub-and-spoke, or a highly redundant topology such as a redundant campus or data center.
- **Route Summarization :** advertise summarized routes into neighbors Area.
- Configure summarization into and out of areas at the ABR or ASBR.



For more about OSPF designing at the Campus please visit:
http://www.mikrotik4me.com/index.php/downloads

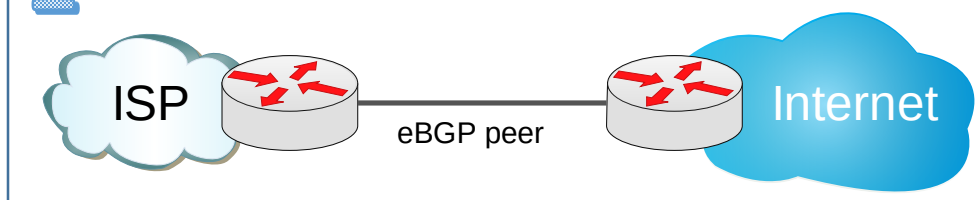
High availability with BGP

- Peering design
- BGP and iBGP and IGP
- High availability at Enterprise.

Peering to Enterprise

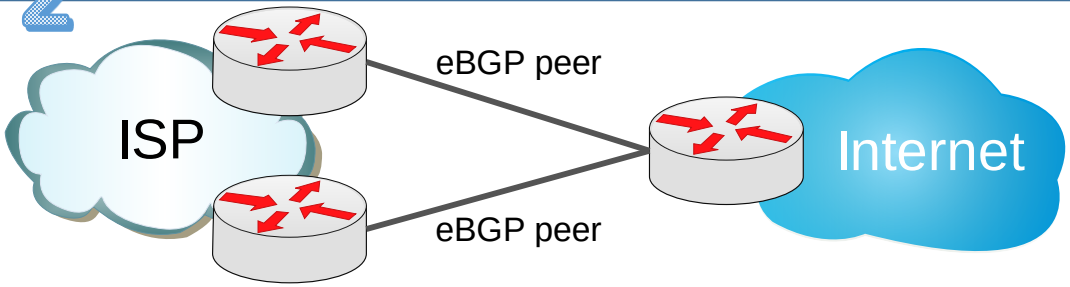
- 4 type of BGP peering is available

1



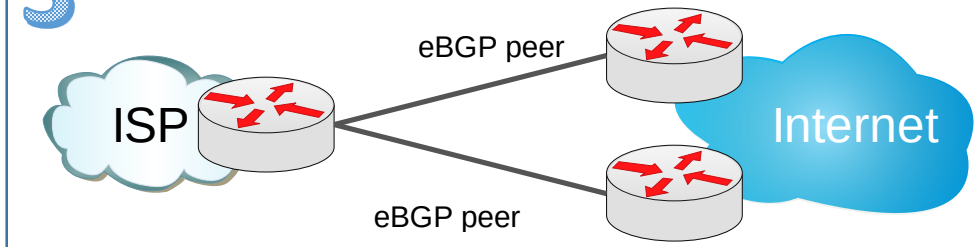
Single homed

2



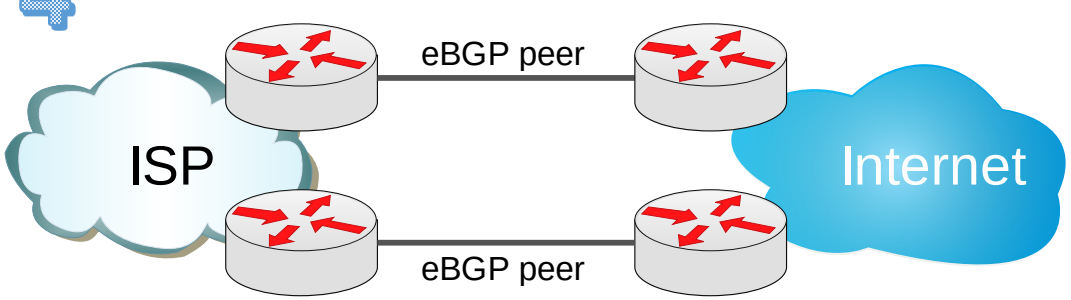
Dual single homed

3



Single Multihomed

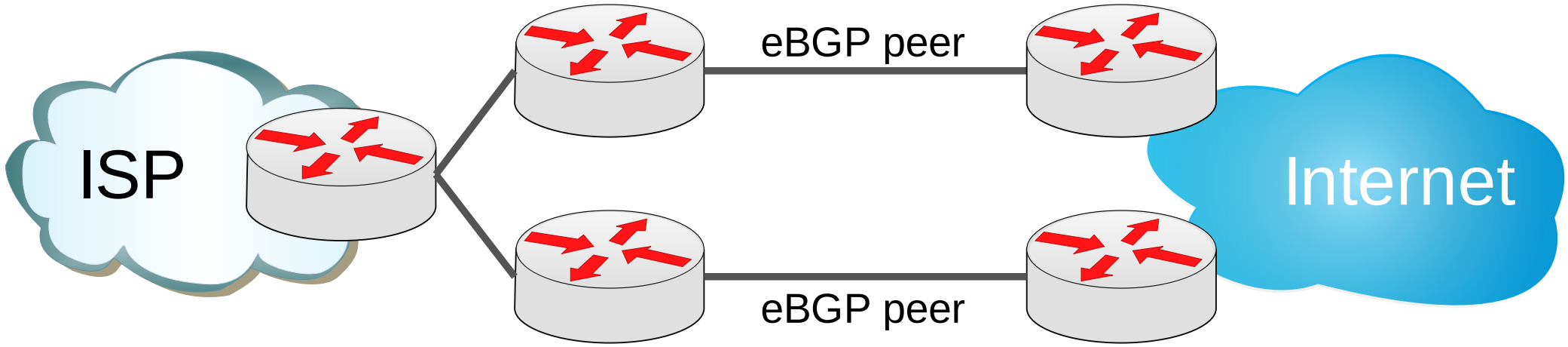
4

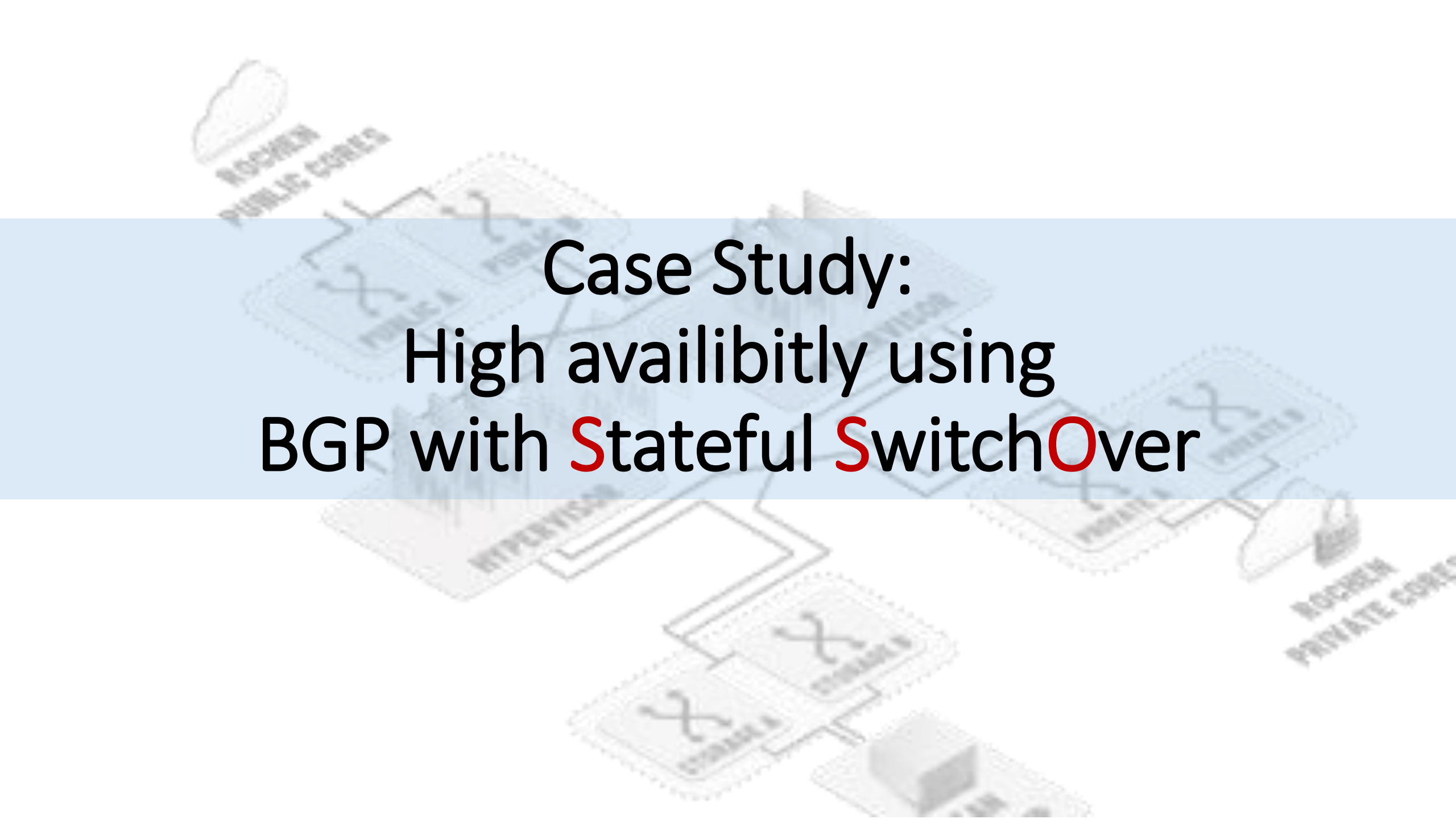


Dual Multihomed

Peering to Enterprise (cont.)

- Dual Multi Homed most in used.
- Upload load balancing using routing policy (Mangle).
- Download balancing using BGP attribute like (prepend).
- Provide redundant connection for upload and download.





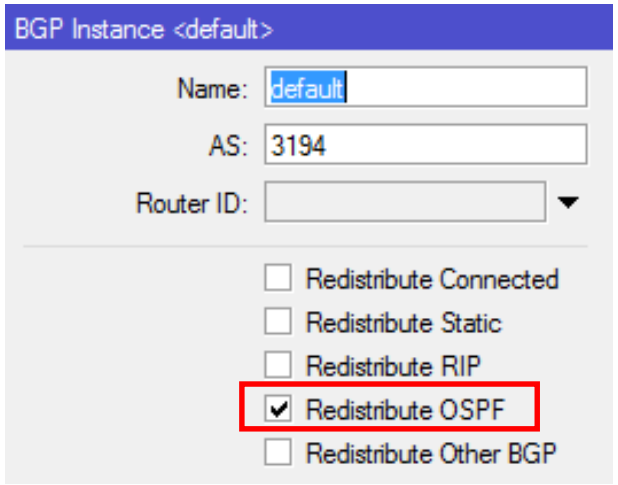
Case Study:
High availibitly using
BGP with Stateful SwitchOver

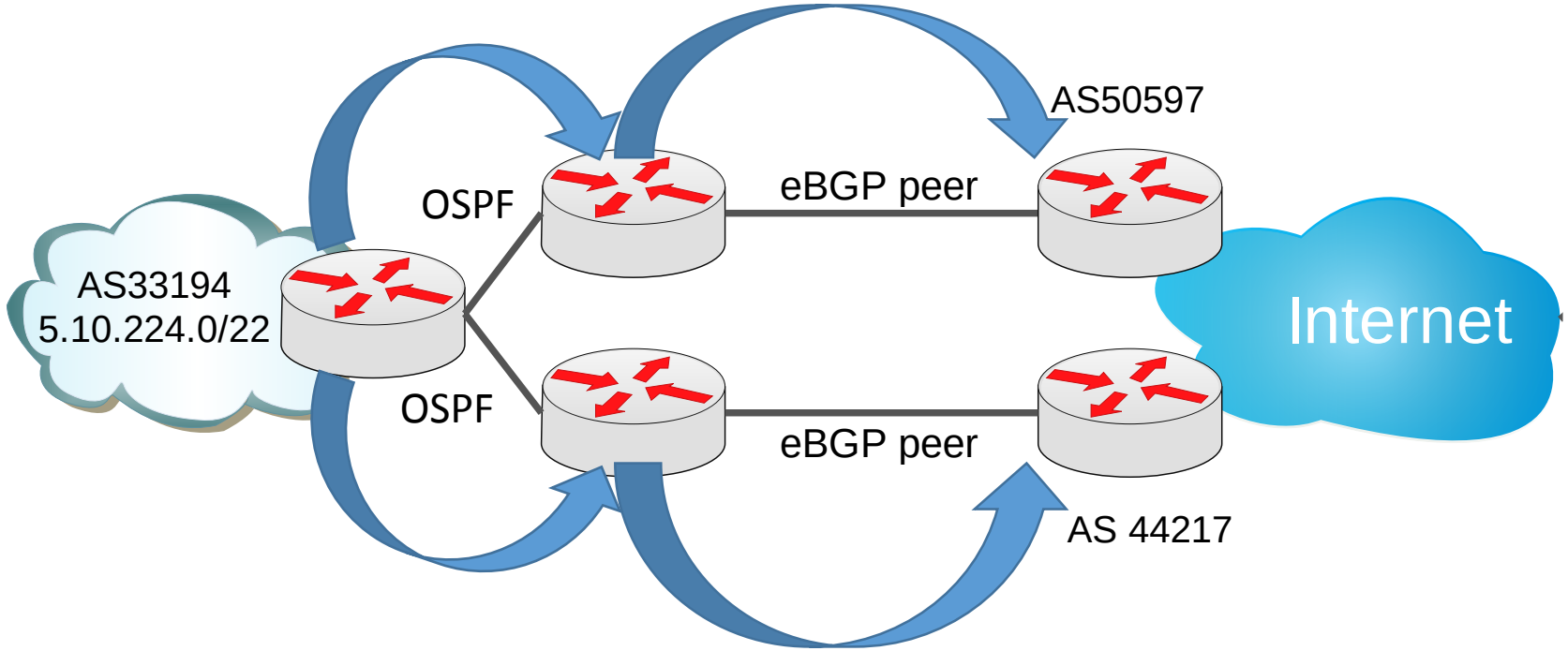
BGP Multi Homed configuration plan

- Available subnet is 5.10.224.0/22.
- UL/DL load sharing between two ISP’s (ASN44217) (ASN50597).
- Divided into four /24 subnet for download load sharing.
- OSPF as IGP for distribute prefix to ASBRs and redistribute default route to internal network.
- Also there is some specific prefix need to be upload from specific path.

Prefixes Redistribution

- For Internal prefix advertise via OSPF to ASBR then via BGP peers will advertised to Enterprise.





BGP Multi Homed configuration (cont.)

Configuration syntax peering to AS44217 : (as reference)

```
/routing bgp instance
set default as=3194 redistribute-ospf=yes
/routing bgp peer
add comment="AS 44217" in-filter=AS44217-bgp-in name=peer1 out-filter=AS44217-Out
remote-address=192.168.50.1 remote-as=44217
/routing filter
```

Out-filter

```
add action=accept chain=AS44217-Out prefix=5.10.224.0/24 prefix-length=24
add action=accept chain=AS44217-Out prefix=5.10.225.0/24 prefix-length=24
add action=accept chain=AS44217-Out prefix=5.10.224.0/22 prefix-length=22
add action=discard chain=AS44217-Out
```

BGP Multi Homed configuration (cont.)

Configuration syntax peering to AS50597 : (as reference)

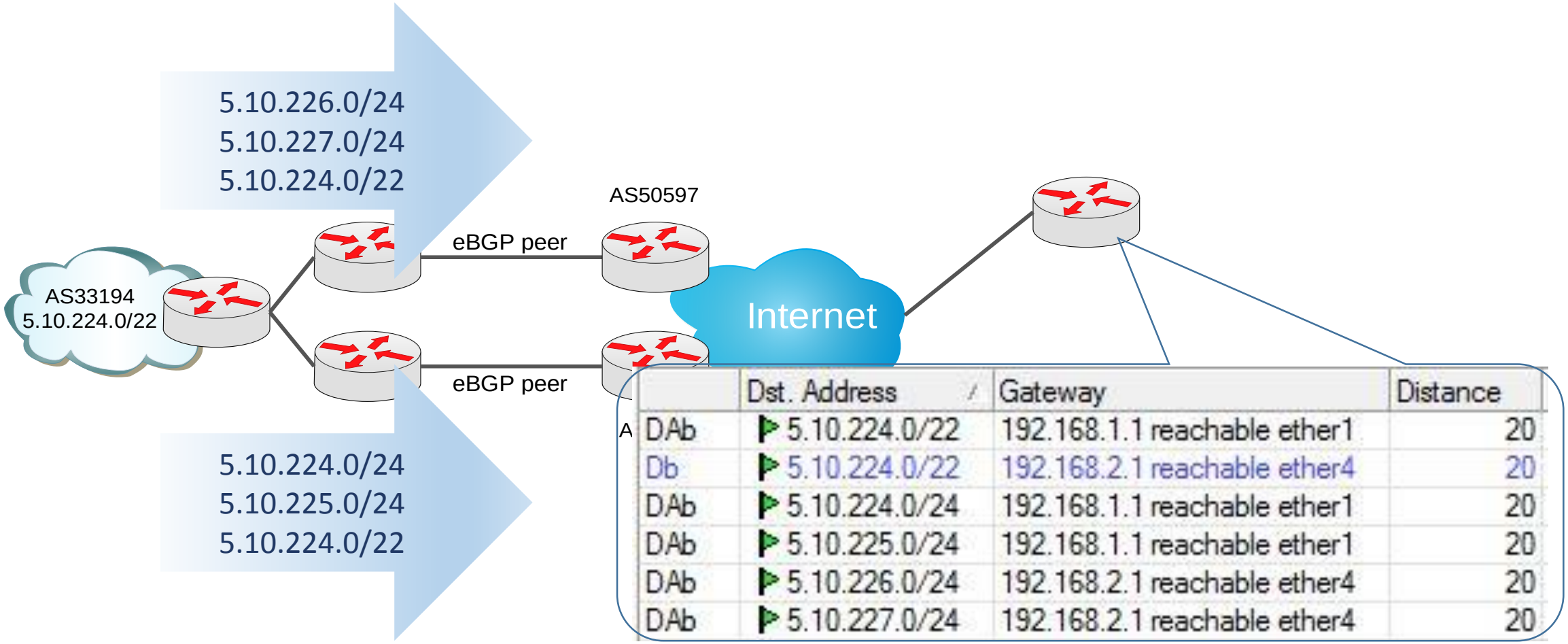
```
/routing bgp instance
set default as=3194 redistribute-ospf=yes
/routing bgp peer
add comment="AS 50598" in-filter=AS50597-bgp-in name=peer1 out-filter=AS50597-Out
remote-address=192.168.50.1 remote-as=50597
/routing filter
```

Out-filter

```
add action=accept chain=AS50597-Out prefix=5.10.226.0/24 prefix-length=24
add action=accept chain=AS50597-Out prefix=5.10.227.0/24 prefix-length=24
add action=accept chain=AS50597-Out prefix=5.10.224.0/22 prefix-length=22
add action=discard chain=AS50597-Out
```

Prefixes Announcement.

- The way that prefixes announce to the Internet in effect on return traffic.
- Four subnet with /24 and one subnet /22 as supernet subnet.



	Dst. Address	Gateway	Distance
DAb	5.10.224.0/22	192.168.1.1 reachable ether1	20
Db	5.10.224.0/22	192.168.2.1 reachable ether4	20
DAb	5.10.224.0/24	192.168.1.1 reachable ether1	20
DAb	5.10.225.0/24	192.168.1.1 reachable ether1	20
DAb	5.10.226.0/24	192.168.2.1 reachable ether4	20
DAb	5.10.227.0/24	192.168.2.1 reachable ether4	20

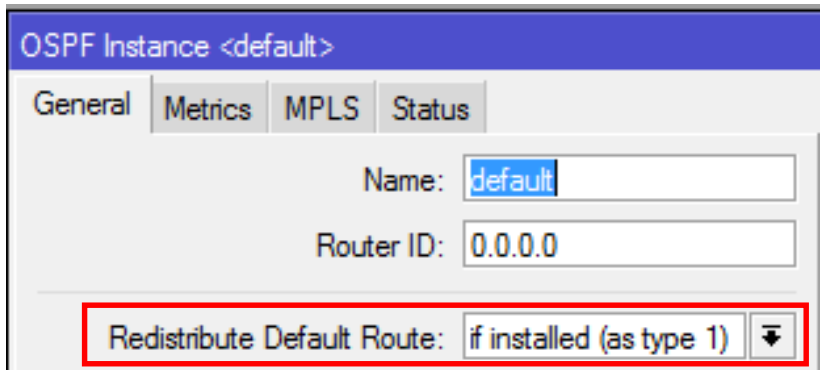
BGP Multi Homed configuration Upload

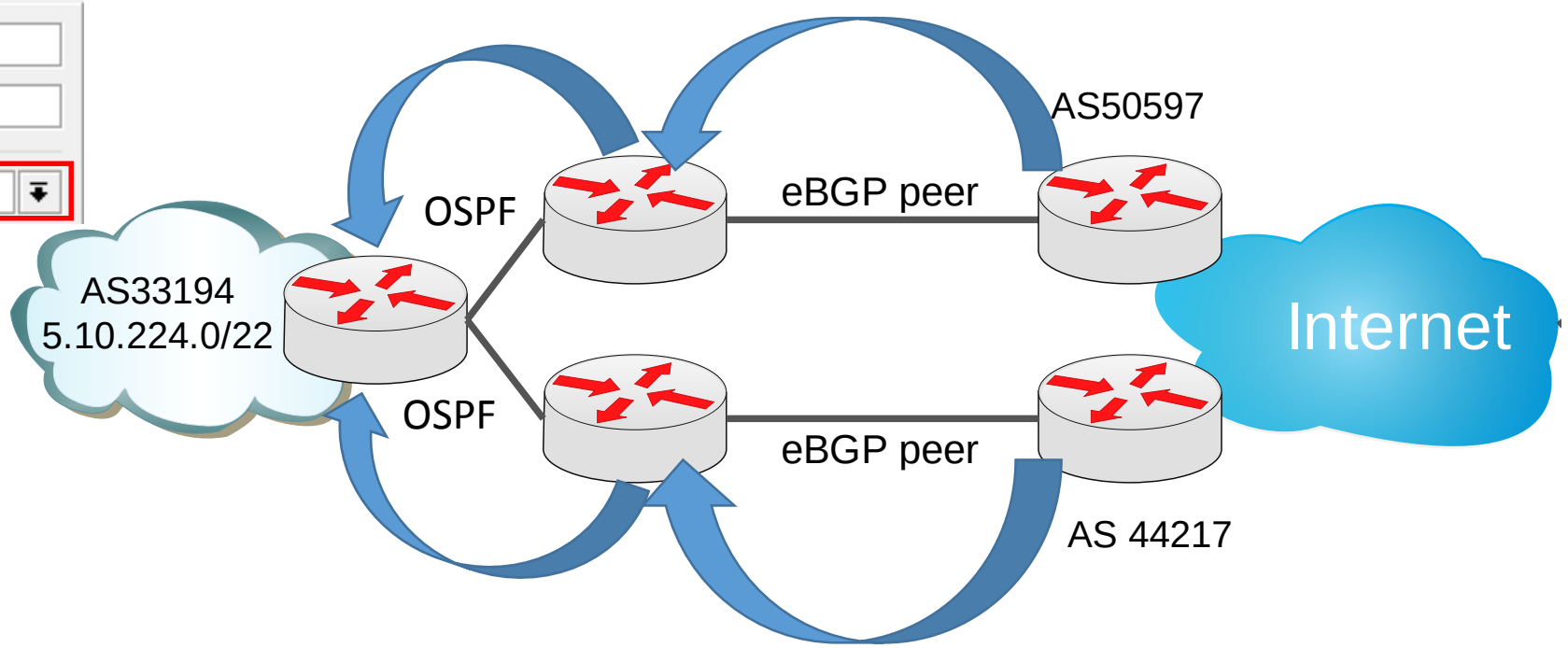
Reaching Internet by:

- full routing update from upstream providers.
  - For redundancy Need to implement iBGP between ASBRs.
  - Over killing for internal router to redistribute 500k routes into IGP.
  - Only default route should to redistribute into IGP .
- Only Default route (Stub network)
  - Most useful for small and medium provider.
  - For redundancy need to implement iBGP between ASBRs.
  - Easy to manage.
  - Can be redistributed to internal routers by IGP protocols.

Default Routes Redistribution

- For default routes the will be receive via BGP peers on ASBR the from ASBR to Internal routers.





BGP Multi Homed configuration Upload (cont.)

Configuration syntax peering to AS44217 : (as reference)

/routing bgp peer

add comment="AS 44217" in-filter=AS44217-bgp-in name=peer1 out-filter=AS44217-Out/

remote-address=192.168.50.1 remote-as=44217

/routing filter

in-filter

```
add action=accept chain=AS44217-bgp-in prefix=0.0.0.0/0
add action=discard chain=AS44217-bgp-in
```

BGP Multi Homed configuration Upload (cont.)

Configuration syntax peering to AS50597 : (as reference)

/routing bgp peer

add comment="AS 50597" in-filter=AS50597-bgp-in name=peer1 out-filter=AS44217-Out/

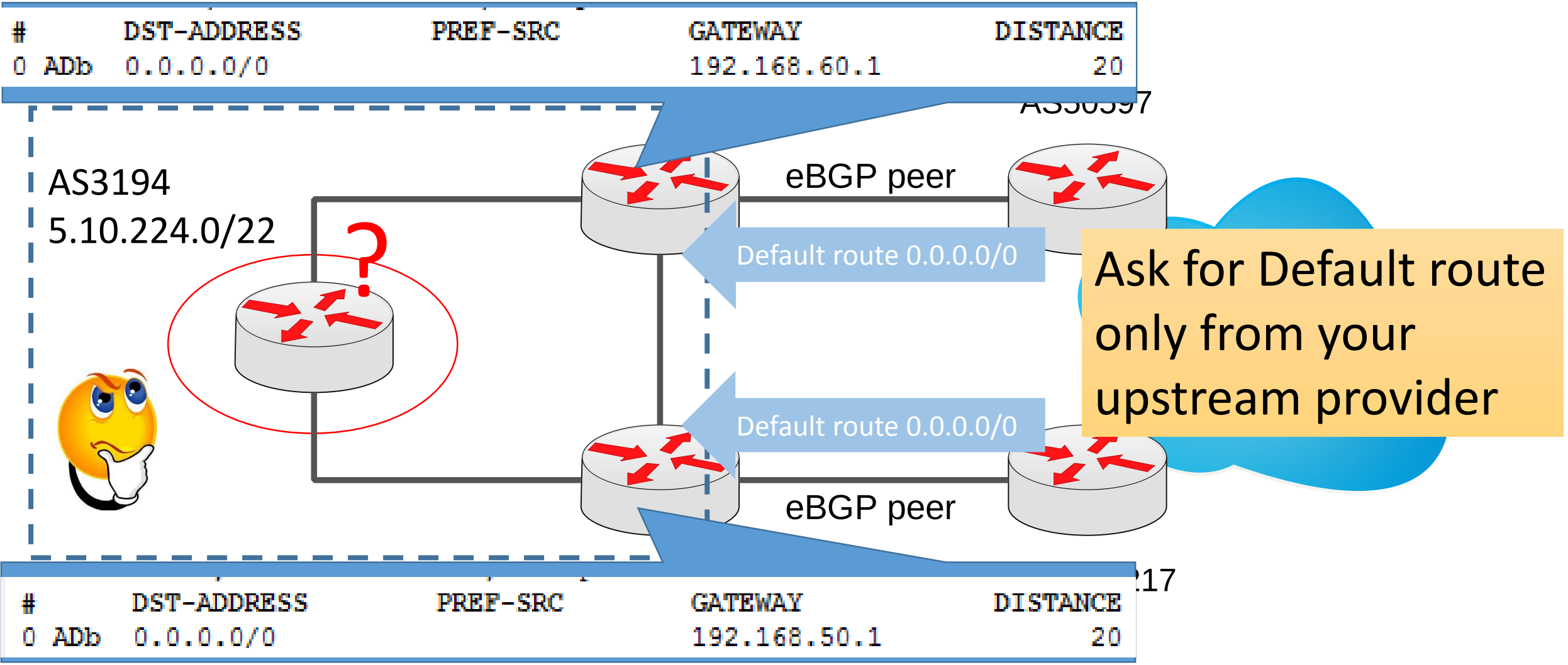
remote-address=192.168.50.1 remote-as=50597

/routing filter

in-filter

```
add action=accept chain=AS50597-bgp-in prefix=0.0.0.0/0
add action=discard chain=AS50597-bgp-in
```

BGP Multi Homed configuration Upload (cont.)



BGP Multi Homed configuration Upload (cont.)

Manually can be add by network administration, but will no provide dynamic failover..!!

Dynamic route (OSPF):

- By default will do ECMP that is undesirable for forwarding traffic to internet.

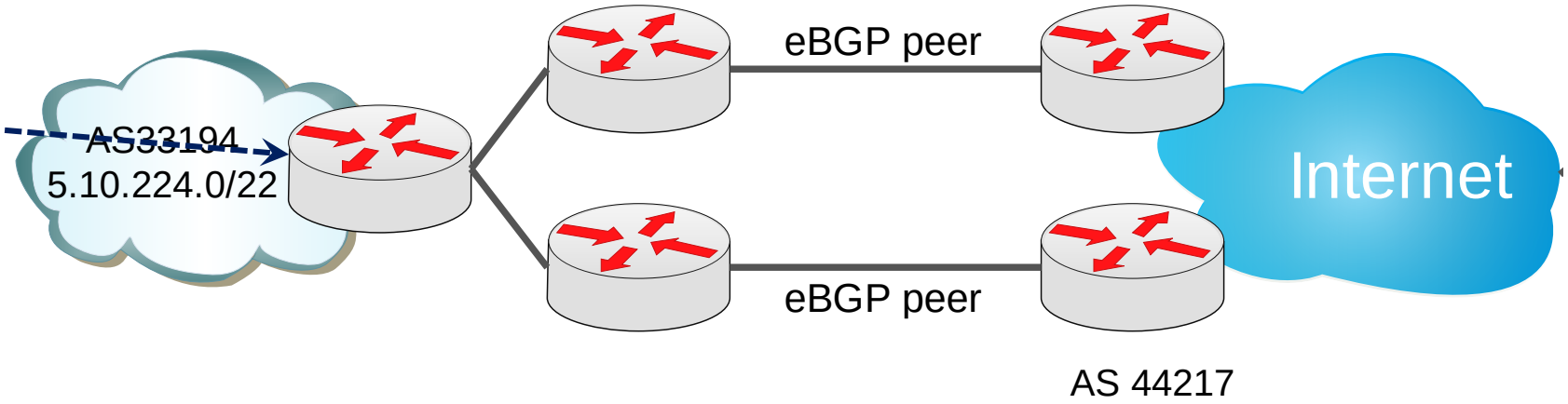
	Dst. Address	Gateway	Distance
DAo	0.0.0.0/0	10.2.2.1 reachable ether10, 10.1.1.1 reachable ether1	110

- Default route at OSPF can be priorities by:
  - Interface Cost.
  - Type1 and Type2.
  - Metric.

BGP Multi Homed configuration Upload load Sharing.

Configuration syntax Local Gateway: (as reference)

```
/ip firewall mangle
add action=mark-routing chain=prerouting new-routing-mark=226 passthrough=no
src-address=5.10.226.0/23
/ip route
add distance=1 gateway=10.2.2.1 routing-mark=226
```

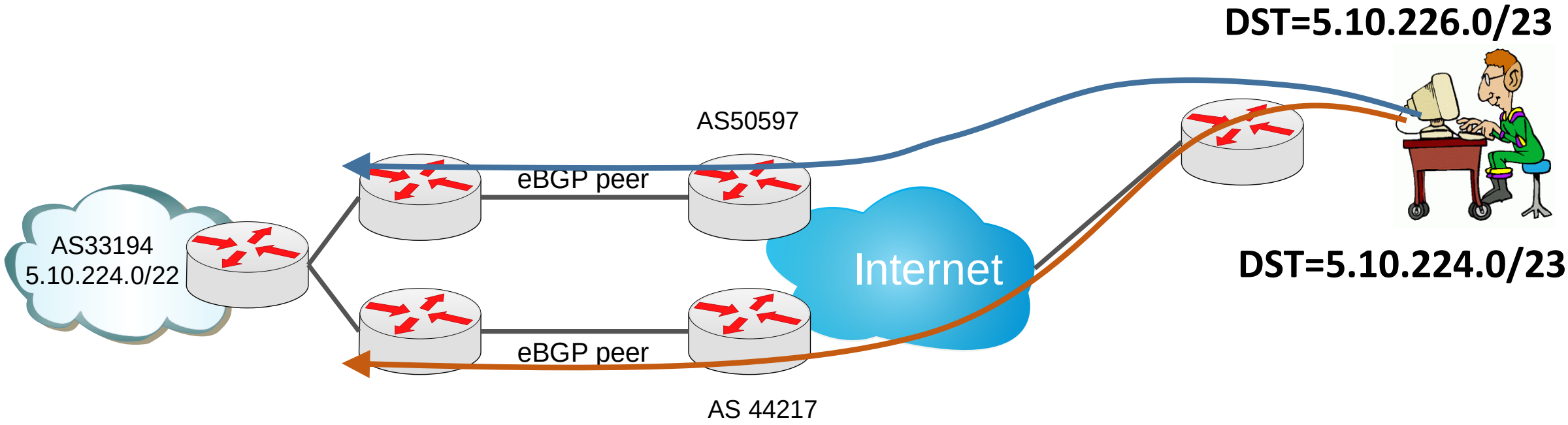


Configuration verification

- Verification the Return Path.
- Verification the Forward path.

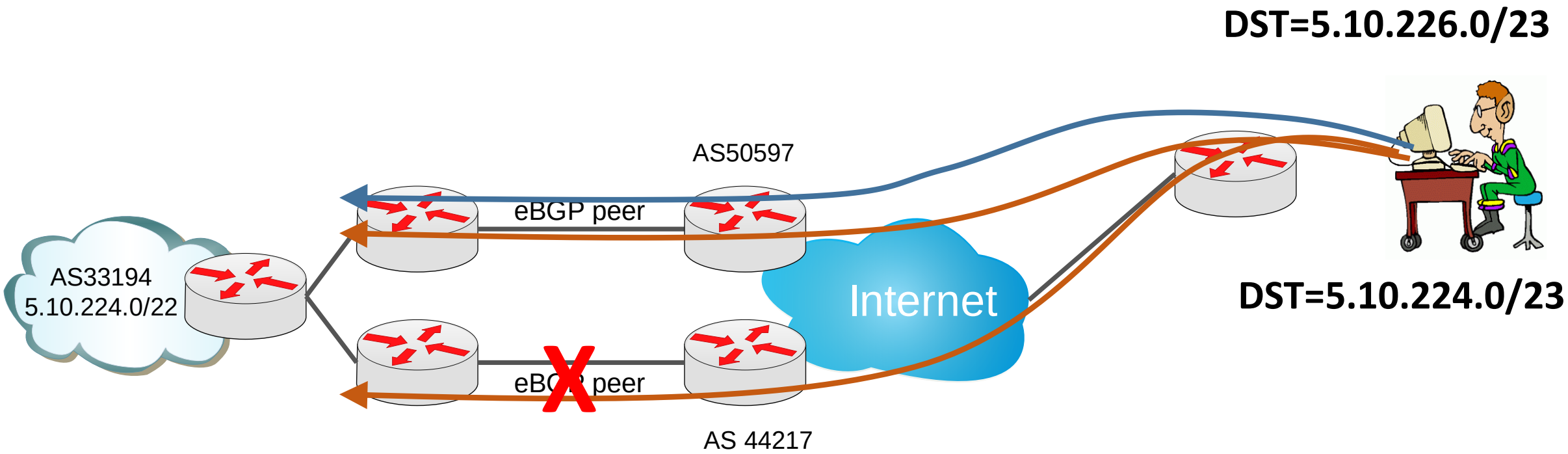
BGP High availability Case scenario #1

bgp prepend attribute for download load balancing normal behavior



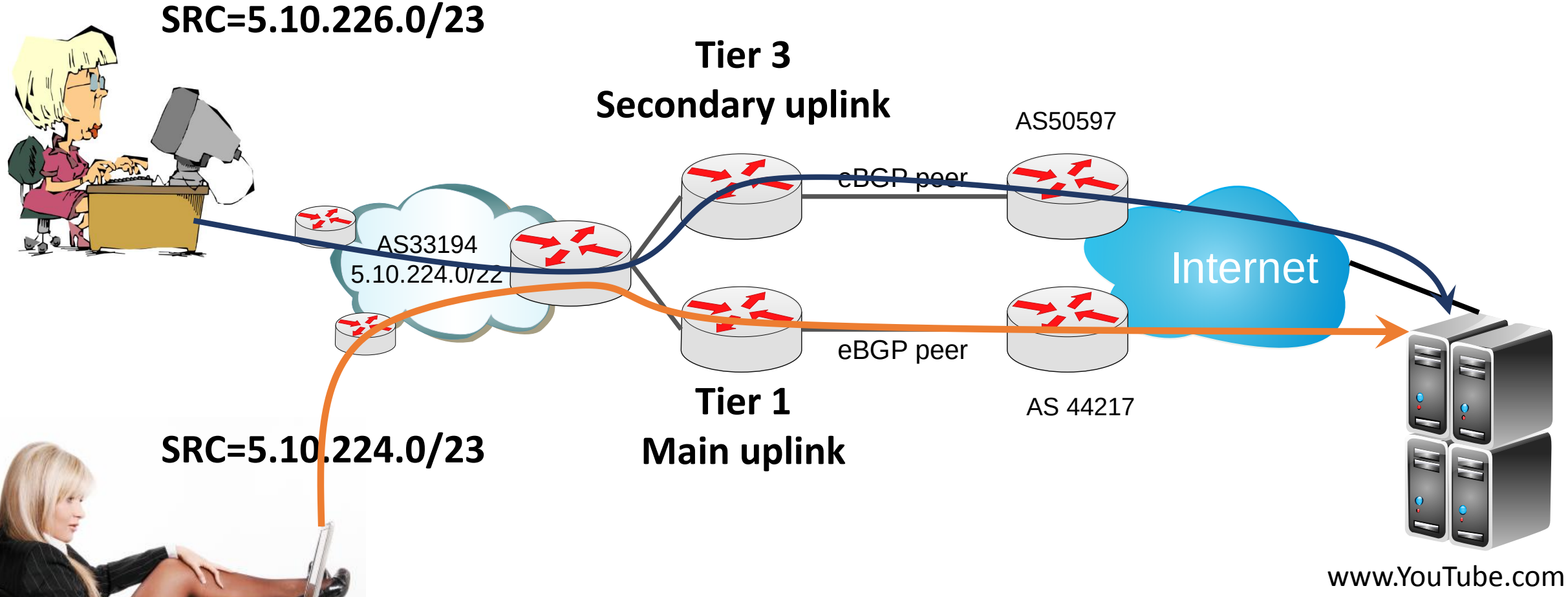
BGP High availability Case scenario #1

bgp prepend attribute for download redundancy normal behavior



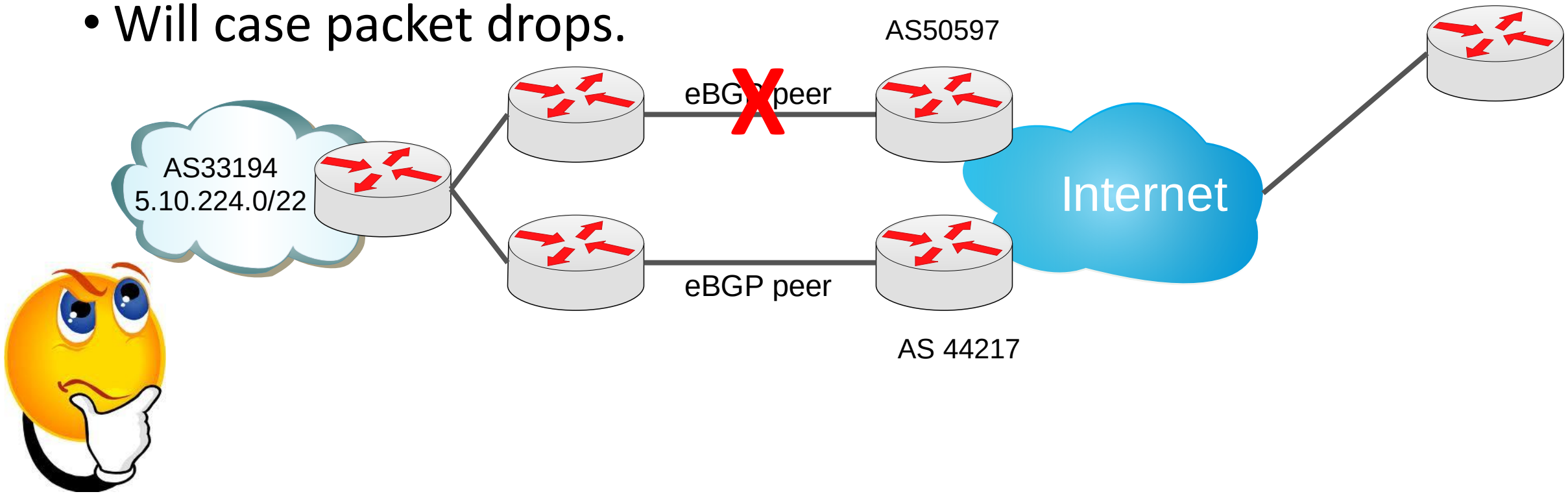
BGP High availability Case scenario #1

bgp prepend attribute for download load balancing normal behavior



Possible fails at this topology 01

- Uplink path that is specified by routing policy.
- When its fail can not be recovered automatically.
- Will case packet drops.



Possible fails at this topology 01 (cont.)

SRC=5.10.226.0/23

2nd Uplink used with routing policy

Packet Drop

AS33194
5.10.224.0/22

eBGP peer

AS50597

Internet

eBGP peer

AS 44217

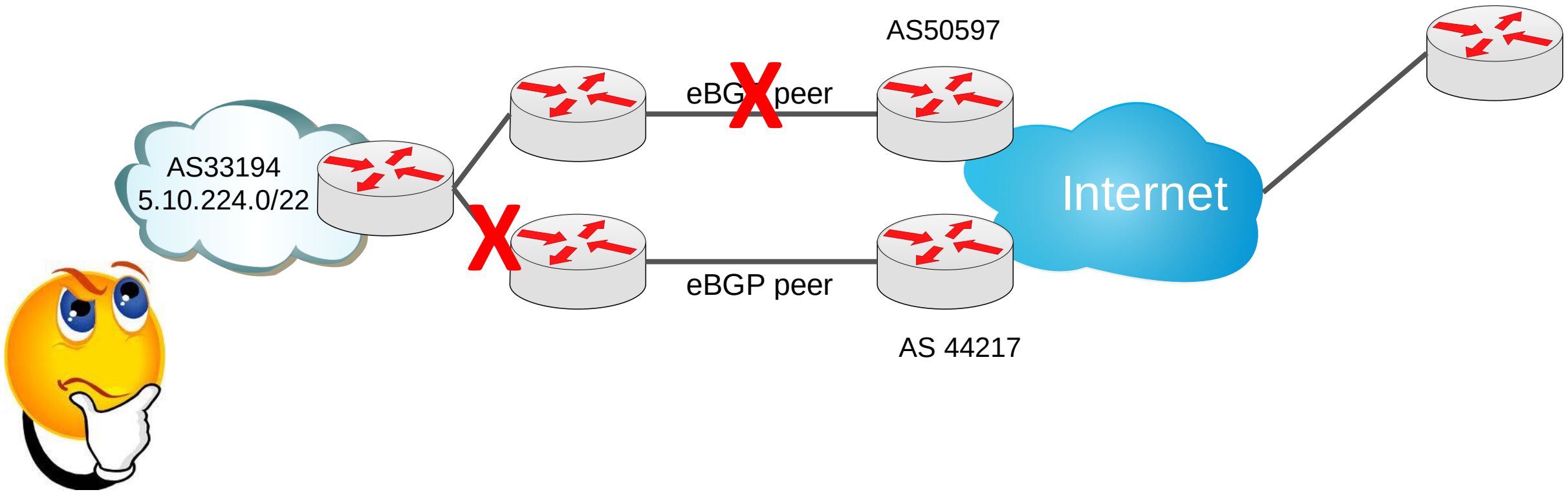
Main uplink used as default route

SRC=5.10.224.0/23

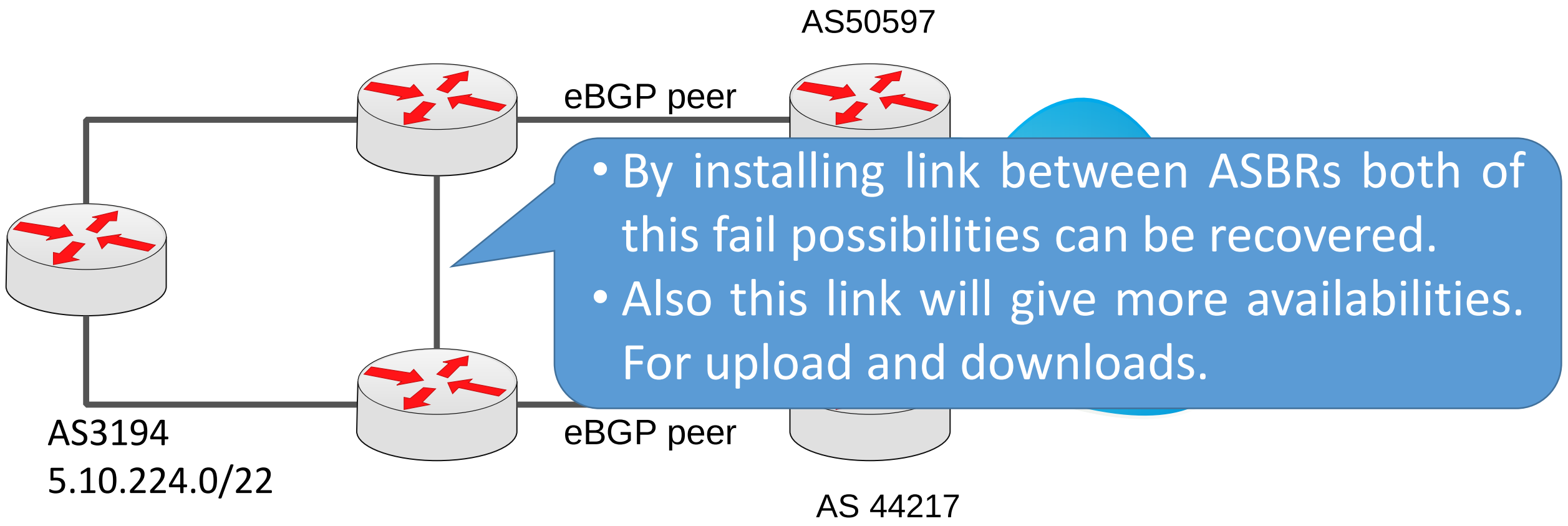
www.YouTube.com

Possible fails at this topology 02

- Internal link fail.
- Case total disconnection.



iBGP between ASBRs for Redundancy



iBGP Or OSPF?

- Both protocols are able to handle the jon.
- As OSPF have its internal routing data base will not install backup route in the RIB.
- BGP have no internal table so its will install all learned route direct to RIB. This will cause to have standby route at RIB for faster recovery.
- Result that iBGP will provide less convergence time.

iBGP Or OSPF (cont.)

iBGP 12% packet loss

Seq #	Host	Time	Reply Size	TTL	Status
0	101.101.101.1	0ms	50	63	
1	101.101.101.1	0ms	50	63	
2	101.101.101.1	0ms	50	63	
3	101.101.101.1	0ms	50	63	
4	101.101.101.1	0ms	50	63	
5	101.101.101.1	0ms	50	63	
6	101.101.101.1	0ms	50	63	
7	101.101.101.1	0ms	50	63	
8	101.101.101.1	0ms	50	63	
9	101.101.101.1	timeout			timeout
10	101.101.101.1	timeout			timeout
11	101.101.101.1	timeout			timeout
12	101.101.101.1	timeout			timeout
13	101.101.101.1	timeout			timeout
14	101.101.101.1	0ms	50	63	
15	101.101.101.1	0ms	50	63	
16	101.101.101.1	0ms	50	63	
17	101.101.101.1	0ms	50	63	

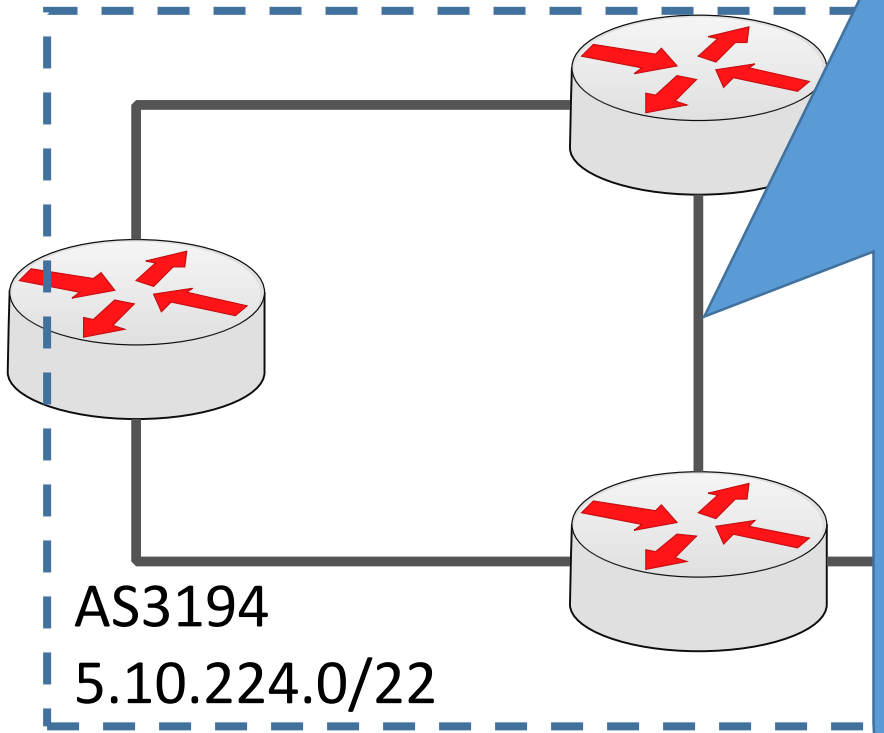
40 items ... | 35 of 40 packets re... | 12% packet loss | Min: 0 ms | Avg: 0 ms | Max: 1 ms

OSPF 30% packet loss

Seq #	Host	Time	Reply Size	TTL	Status
6	101.101.101.1	0ms	50	63	
7	101.101.101.1	0ms	50	63	
8	101.101.101.1	0ms	50	63	
9	101.101.101.1	timeout			timeout
10	101.101.101.1	timeout			timeout
11	101.101.101.1	timeout			timeout
12	101.101.101.1	timeout			timeout
13	101.101.101.1	timeout			timeout
14	10.2.2.1	0ms	78	64	net unreachable
15	10.2.2.1	0ms	78	64	net unreachable
16	10.2.2.1	0ms	78	64	net unreachable
17	10.2.2.1	0ms	78	64	net unreachable
18	10.2.2.1	0ms	78	64	net unreachable
19	10.2.2.1	0ms	78	64	net unreachable
20	101.101.101.1	timeout			timeout
21	101.101.101.1	0ms	50	63	
22	101.101.101.1	0ms	50	63	
23	101.101.101.1	0ms	50	63	

40 items | 28 of 40 packets re... | 30% packet loss | Min: 0 ms | Avg: 0 ms | Max: 0 ms

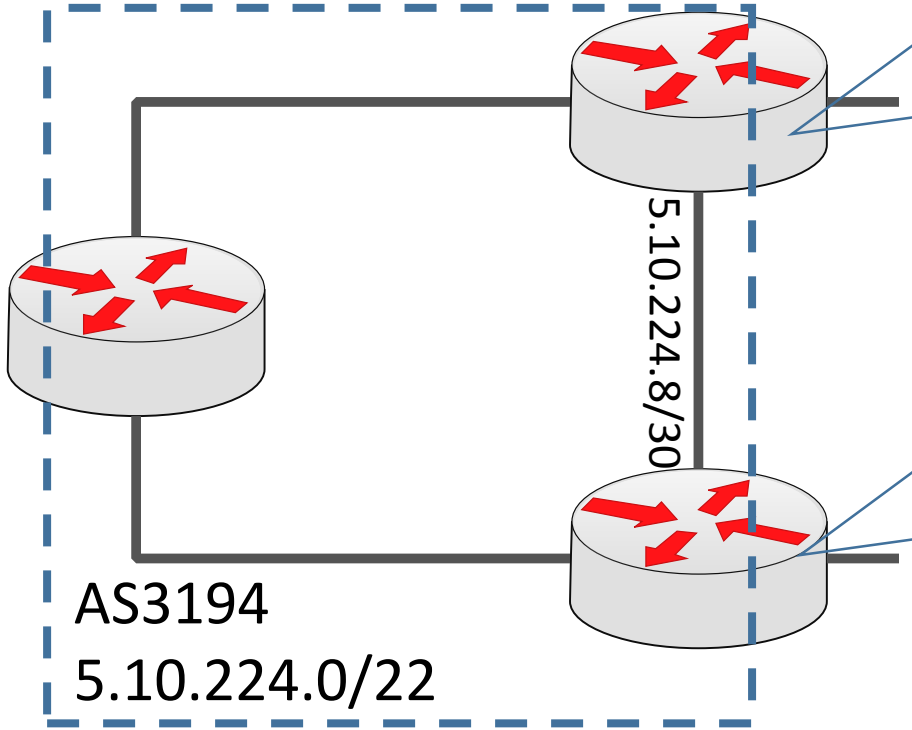
iBGP between ASBRs for Redundancy



iBGP

- Useful to exchange routing information between BGP speakers
- Helpful to switch over for uplink and download.
- Should set next-hop “force self” to insure reachability.
- Possibility of installing routes as standby in routing table that provide stateful switch over link recovery.

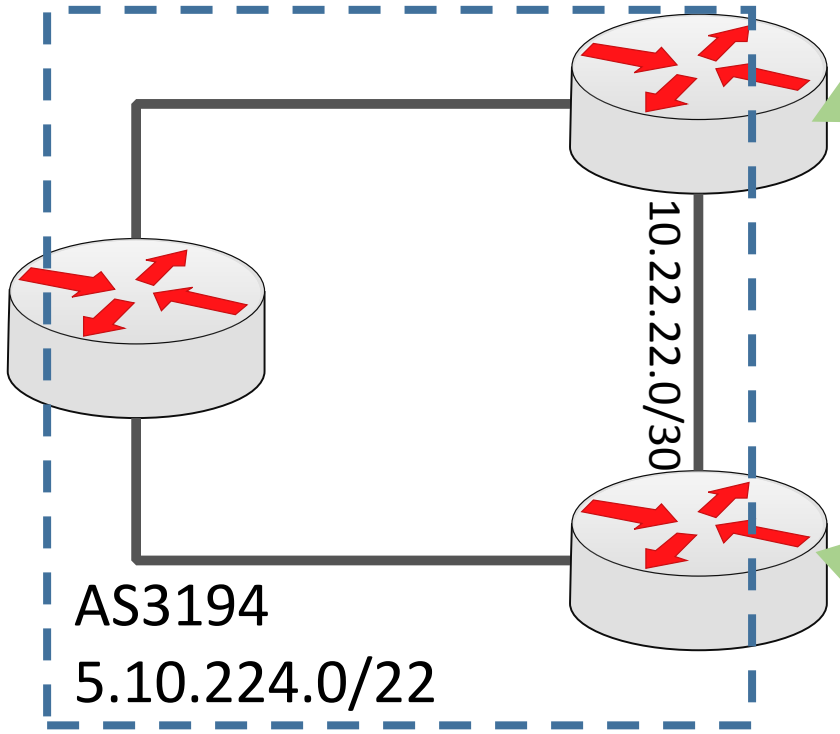
iBGP between ASBRs for Redundancy



add default-originate=**if-installed** name=peer-iBGP nexthop-choice=**force-self** remote-address=5.10.224.9 remote-as=3194

add default-originate=**if-installed** name=peer-iBGP nexthop-choice=**force-self** remote-address=5.10.224.10 remote-as=3194

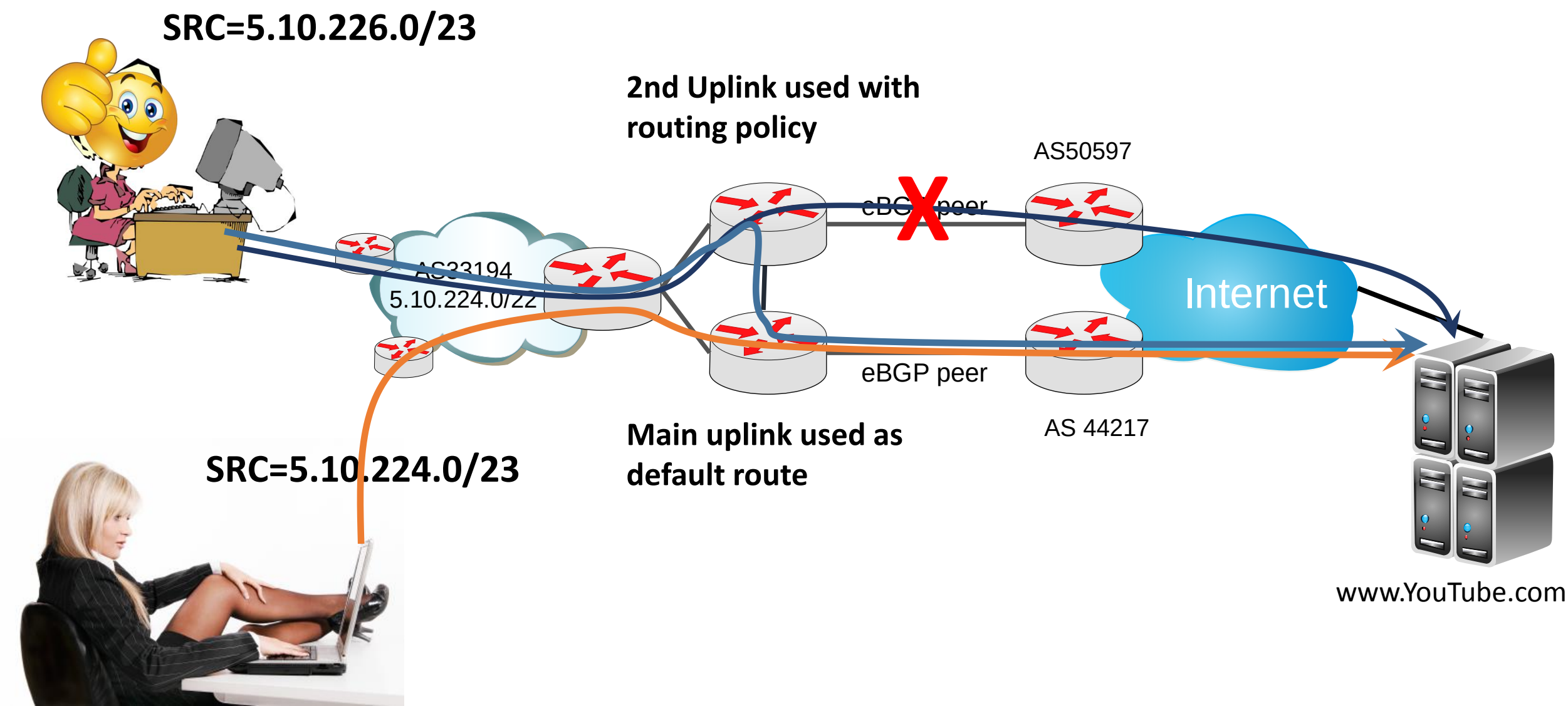
iBGP between ASBRs for Redundancy (cont.)



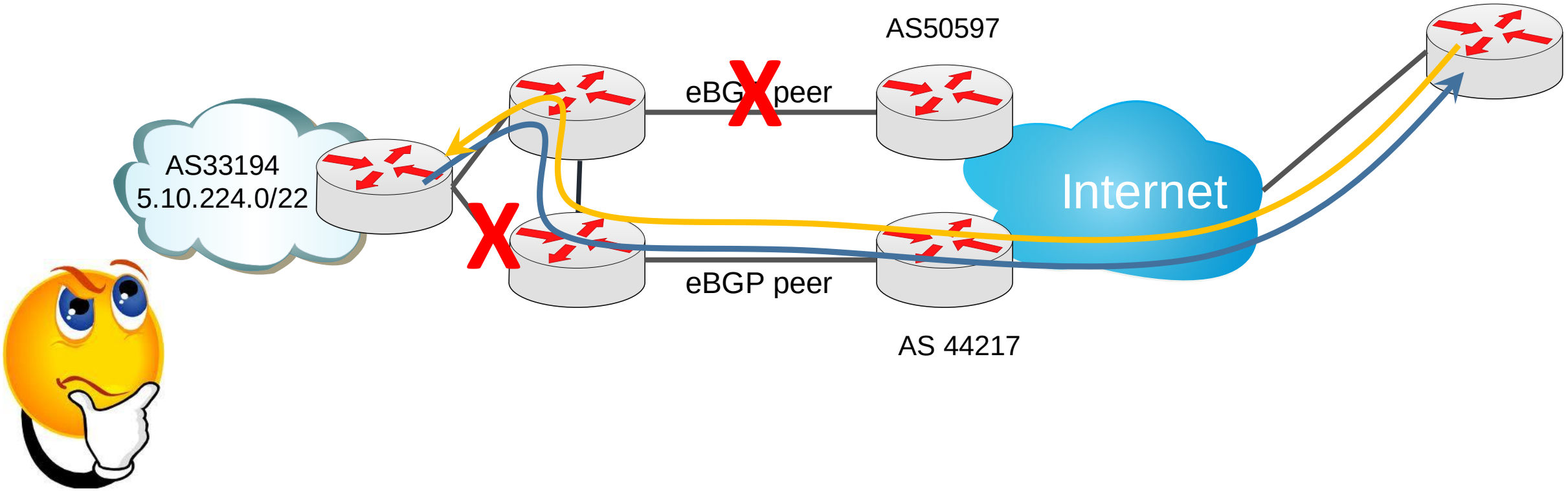
	Dst. Address	Gateway	Distance
Db	0.0.0.0/0	10.22.22.1 reachable ether9	200
DAb	0.0.0.0/0	192.168.2.2 reachable ether5	20

	Dst. Address	Gateway	Distance
DAb	0.0.0.0/0	192.168.1.2 reachable ether5	20
Db	0.0.0.0/0	10.22.22.2 reachable ether9	200
DAb	5.10.224.0/22	10.22.22.2 reachable ether9	200
DAo	5.10.224.0/24	10.1.1.2 reachable ether1	110
Db	5.10.224.0/24	10.22.22.2 reachable ether9	200
DAo	5.10.225.0/24	10.1.1.2 reachable ether1	110
Db	5.10.225.0/24	10.22.22.2 reachable ether9	200
DAo	5.10.226.0/24	10.1.1.2 reachable ether1	110
Db	5.10.226.0/24	10.22.22.2 reachable ether9	200
DAo	5.10.227.0/24	10.1.1.2 reachable ether1	110
Db	5.10.227.0/24	10.22.22.2 reachable ether9	200
DAC	10.1.1.0/30	ether1 reachable	0
Db	10.1.1.0/30	10.22.22.2 reachable ether9	200
DAo	10.2.2.0/30	10.1.1.2 reachable ether1	110

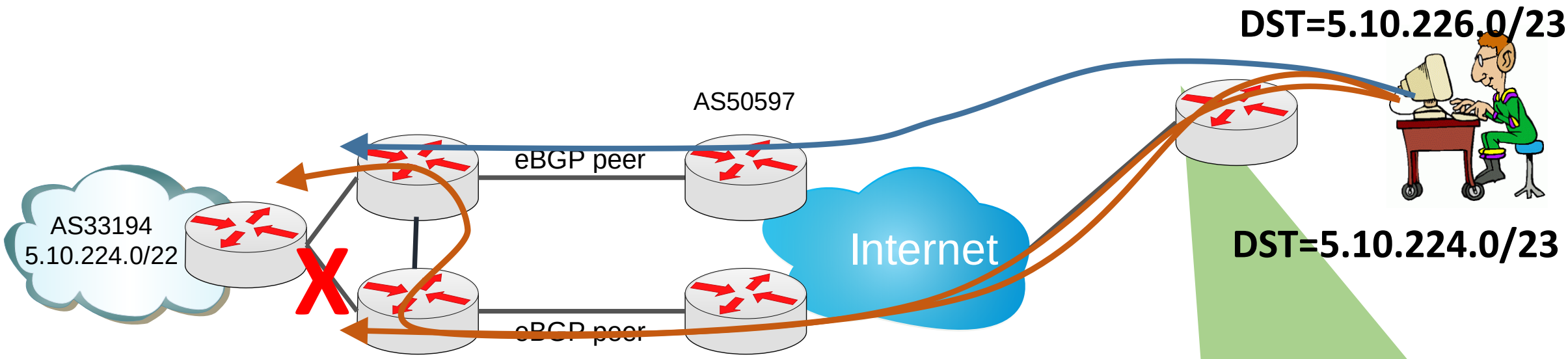
Recovery stage 01



Recovery stage 02



Recovery stage 03



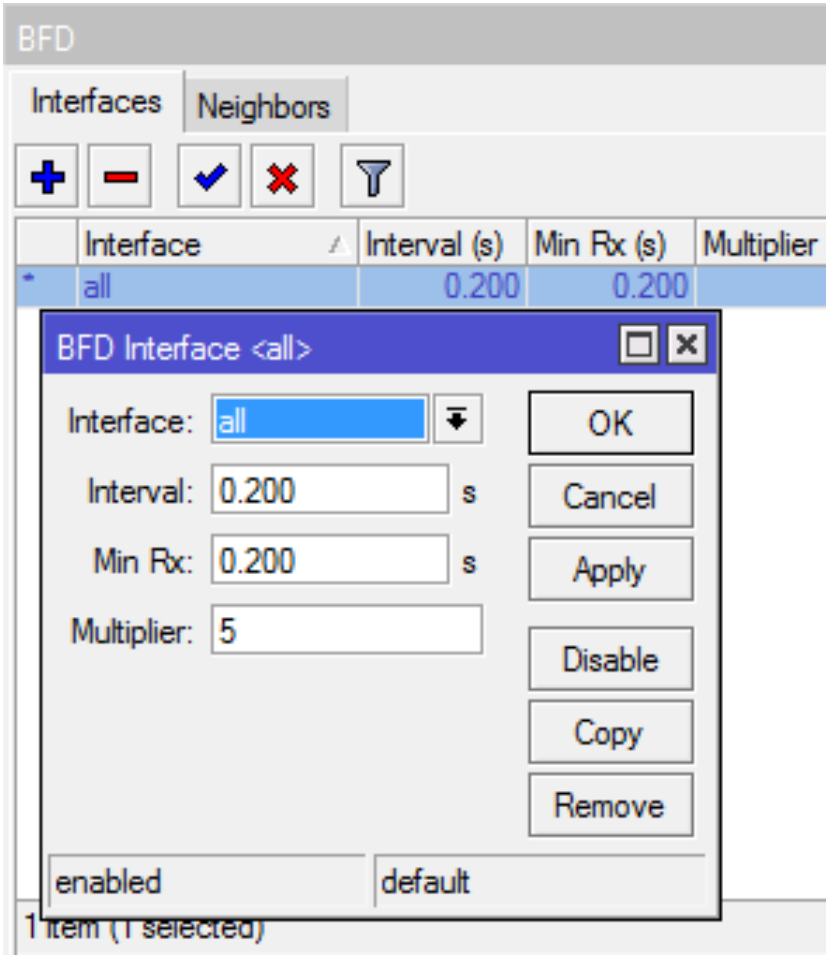
AS

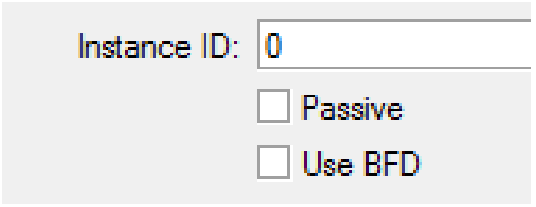
	Dst. Address	Gateway	Distance
DAb	5.10.224.0/22	192.168.2.1 reachable ether4	20
Db	5.10.224.0/22	192.168.1.1 reachable ether1	20
DAb	5.10.224.0/24	192.168.1.1 reachable ether1	20
DAb	5.10.225.0/24	192.168.1.1 reachable ether1	20
DAb	5.10.226.0/24	192.168.2.1 reachable ether4	20
DAb	5.10.227.0/24	192.168.2.1 reachable ether4	20
DAC	101.101.101.1	InterNet-Cloud reachable	0

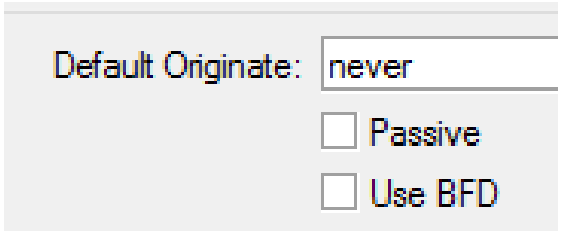
No effect on Global routing information

Bidirectional forwarding detection (BFD).

- is a network protocol used to detect faults between two forwarding engines connected by a link.
- It provides low-overhead detection of faults even on physical media that don't support failure detection of any kind, such as Ethernet, virtual circuits, tunnels and MPLS Label Switched Paths.
- sessions must be explicitly configured between endpoints.
- BFD can provide sub second link fail detection.







www.mikrotik4me.com

https://www.facebook.com/MikroTik4ME