OSPF to the customer

Why, how and what about security

Presenter information

Tomas Kirnak

Network design
Security, wireless
Servers
Virtualization

MikroTik Certified Trainer
MikroTik Certified Consultant

Atris, Slovakia

Established 1991

Complete IT solutions
Networking, servers
Virtualization
IP security systems

Goal

- Show peering options for providers to peer with their customers using OSPF

- Test this setup in a network simulator using a virtual simulated network
  - using MikroTik in GNS3

Agenda

- OSPF basics and concepts
- OSPF area and LSA types
- Example topologies
- route-filters and security
- Topology simulation

OSPF (Open Shortest Path First)

- Dynamic routing protocol
- Interior routing based on link-state
- Used for inter-AS prefix distribution

- OSPFv2 for IPv4, OSPFv3 for IPv6

Why OSPF?

- A dynamic routing protocol
- Will give redundancy to the customer

- Can provide easy load-balancing to the customer

Why OSPF and not BGP?

- OSPF is faster
- OSPF is easier to configure

- OSPF is supported on all business-class devices, even on cheap routers these days

OSPF Basics

- Gathers link state information from available routers and constructs a topology map of the network.
- Full CIDR support (opposed to legacy RIP)
- A path through network is formed based on “shortest-path” through a network mesh – the shortest distance
- Each interface has a “distance” parameter.

OSPF Basics

- OSPF routes IP (L3) traffic, but uses IP as its own transport protocol as well.
- Own L4 protocol – proto 89
- Multicast used for packet delivery in a single L2 domain

Link state protocol

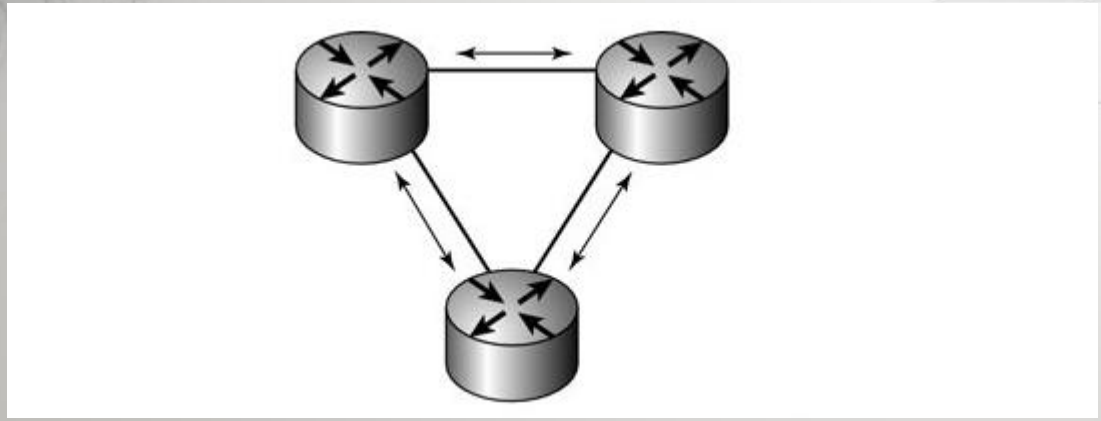
- Each router interface – a link

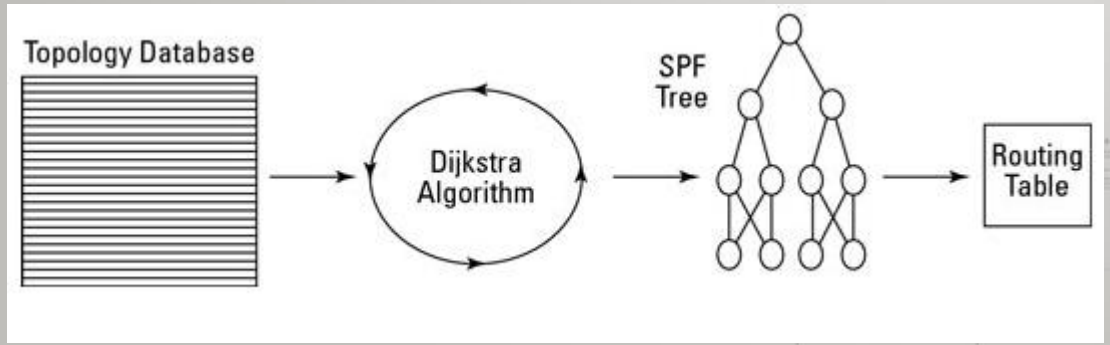
- OSPF sends LSAs to its neighbors:
  - Link State Advertisement (LSA): A simple update on a router's link status, so one will be sent when a link is connected, disconnected, or otherwise changed

How a path is calculated

- Each OSPF router keeps a topological DB:
  - Topological database: A table in memory that contains link information about all known routers.
- A SPF algorithm is then user (Dijkstra algorithm) to calculate the shortest path to all destinations.
- SPF tree: A listing all of the routes to any destination with an order of preference

OSPF process





- Exchange LSAs
- Form topology DB
- Calculate SPF
- Inject into routing table

OSPF Areas

- An OSPF domain can (doesn’t have to) be divided into area.
- An OSPF domain needs to have a backbone area
- Each additional area needs to be connected to the backbone area
  - OSPF doesn’t impose a limit on the number of areas in an OSPF domain, only that they need to connect to the backbone area

OSPF Areas

- Each area has a unique area ID
  - Backbone: 0.0.0.0
- Each area has a type:
  - Standard
  - Stubby
    - Totally Stubby
  - NSSA (Not So Stubby Area)
    - Not So Totally Stubby Area

Area types:

- Each area type accepts and forwards different types of LSAs.

- LSA types:
  - *Type 1* - Router LSA
  - *Type 2* - Network LSA
  - *Type 3* - Summary LSA
  - *Type 5* - External LSA
  - *Type 7* - (NSSA) External LSA redistribution

OSPF basic config

- We need a routerID for OSPF
- This should be a reachable IP, on a loopback interface

Adding a loopback IP for routerID

```
/interface bridge
add name="br0 - loopback“

/ip address
add address=10.0.0.1/32 interface="br0 - loopback“

/routing ospf instance
set default router-id=10.0.0.1
```

Making the loopback reachable

- 2 Options:

/routing ospf instance
set default redistribute-connected=as-type-1

/routing ospf network
add area=backbone network=10.0.0.1/32

Default route for our network

- On our edge routes in our provider network, we redistribute a default route to the rest of our infrastructure

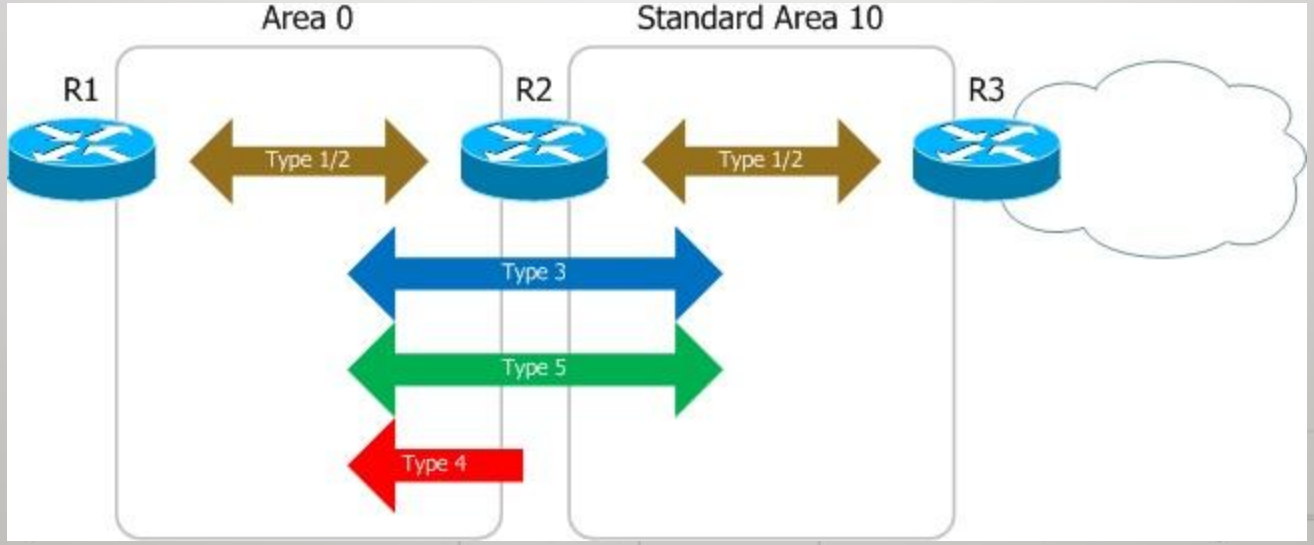
```
/routing ospf instance
set [ find default=yes ] distribute-default=if-installed-as-type-1
```

OSPF areas

- An OSPF domain can be divided into areas
- Areas are implemented in OSPF for performance, network topology separation and security reasons

Area LSA forwarding

- Default area:



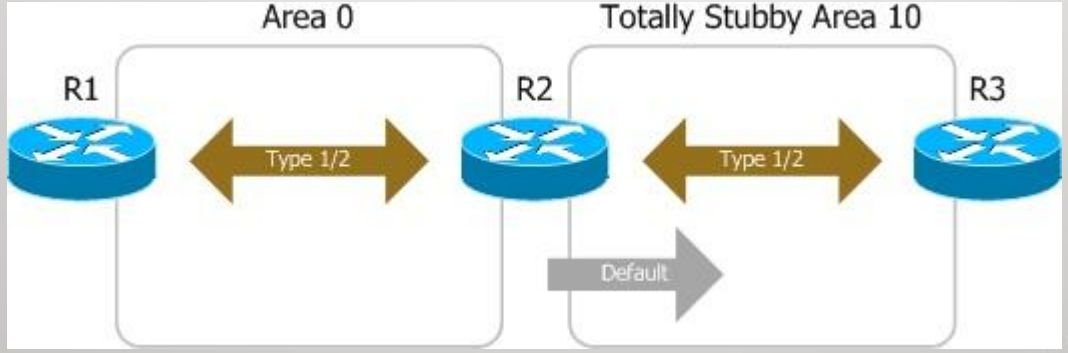
Default area

- Used inside of our network

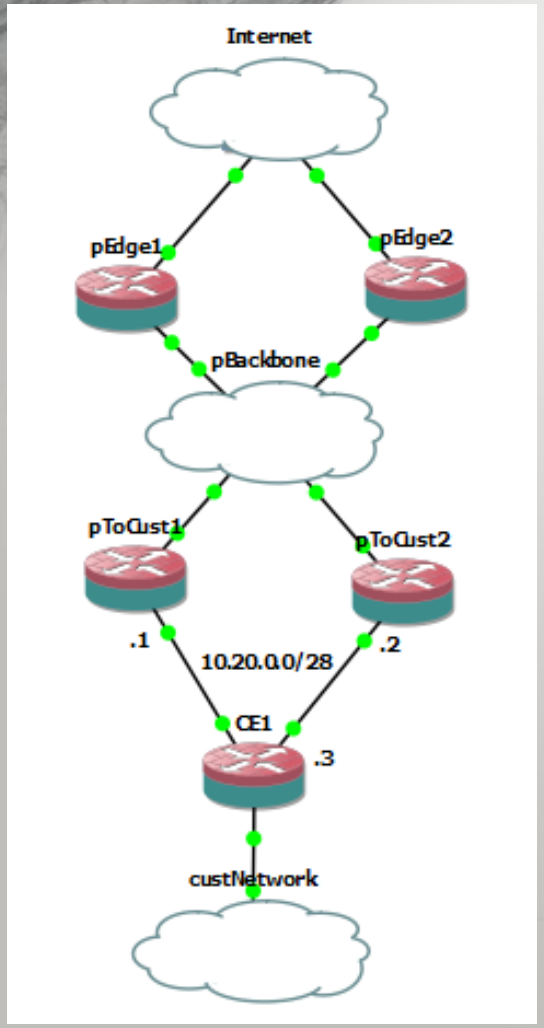
- Not secure to peer with customers
  - Customers can see all our internal routes, could inject routes to us, etc.

Area LSA forwarding

- Totally stubby area:



- We can use this to peer with our customers
  - Only default route to the customer



Basic example

- Provider wants to provide redundancy for the customer
- OSPF peer with the customer
- This should remove 95% of outages for the customer (outages caused by provider network problems)

How to configure

/routing ospf area

add area-id=0.0.0.1 inject-summary-lsas=no name=toCustomer1 type=stub

/routing ospf network

add network=10.20.0.0/28 area=toCustomer1

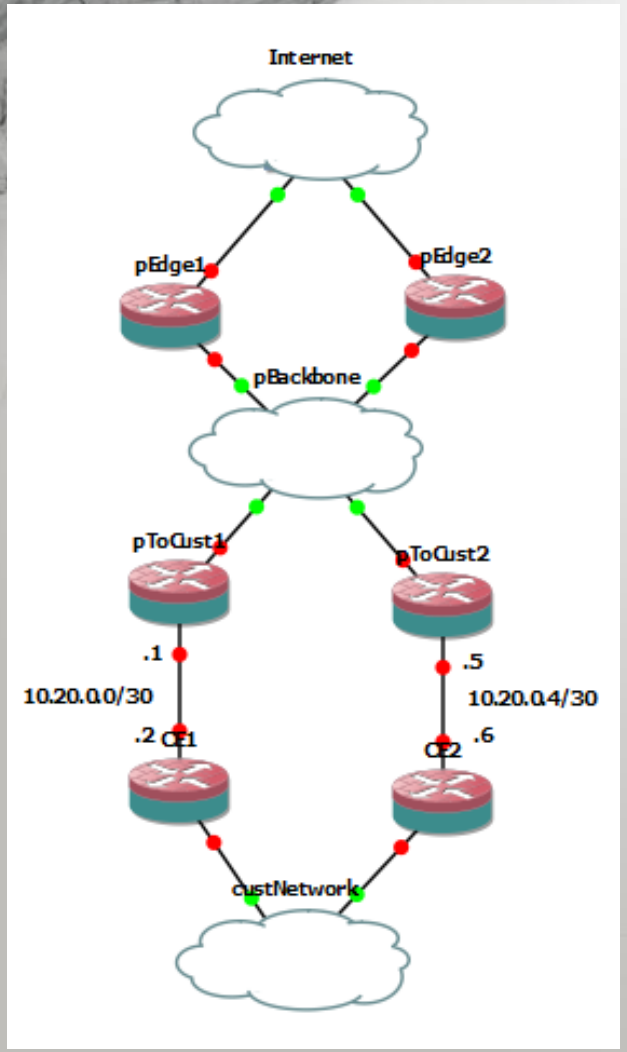
/routing ospf interface

add interface=toCustomer authentication=md5 authentication-key=password

OSPF security part 1

- Always secure your OSPF interfaces with authentication

- Prevents un-authorized routers to establish an OSPF session



Customer redundancy

- Customer can add a second router to his edge
- This provides full redundancy for the customer

Config on provider routers

- On pToCust1 and pToCust2:

```
/routing ospf area
add area-id=0.0.0.1 inject-summary-lsas=no name=toCustomer1 type=stub
/routing ospf network
add network=10.20.0.x/30  area=toCustomer1
/routing ospf interface
add interface=toCustomer authentication=md5 authentication-key=password
```

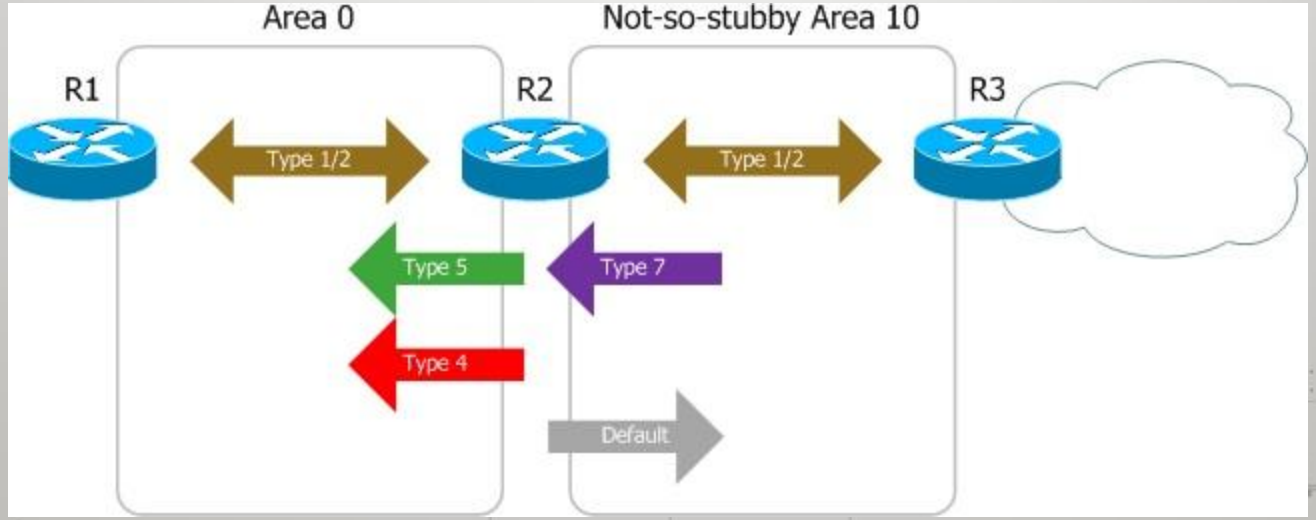
Customer wants more

- We are giving the default route to the customer redundantly

- Customers at this level usually need public IPs
  - these should also be redundant and usable anywhere in the customer network

Area LSA forwarding

- Totally NSSA



Setup on provider routers

- On pToCust1 and pToCust2:

```
/routing ospf area
add area-id=0.0.0.2 inject-summary-lsas=no name=toCust2 \
    type=nssa translator-role=translate-always
/routing ospf network
add network=10.20.0.x/30  area=toCustomer1
/routing ospf interface
add interface=toCustomer authentication=md5 authentication-key=password
```

What we configured

- Customers will get a default route from us
- Customers will be able to inject routes into our OSPF domain now

Security

- Customers could inject routes into our routing tables to route traffic to them that is not supposed to be going to them

- Dangerous, needs to be secured somehow

Routing Filters

/routing filter

add action=accept chain=cust1-out prefix=10.0.0.x/30

add action=accept chain=cust1-out prefix=0.0.0.0/0 prefix-length=0

add action=discard chain=cust1-out

add action=accept chain=cust1-in prefix=10.0.0.x/30

add action=accept chain=cust1-in prefix=22.33.1.0/28 prefix-length=29-32

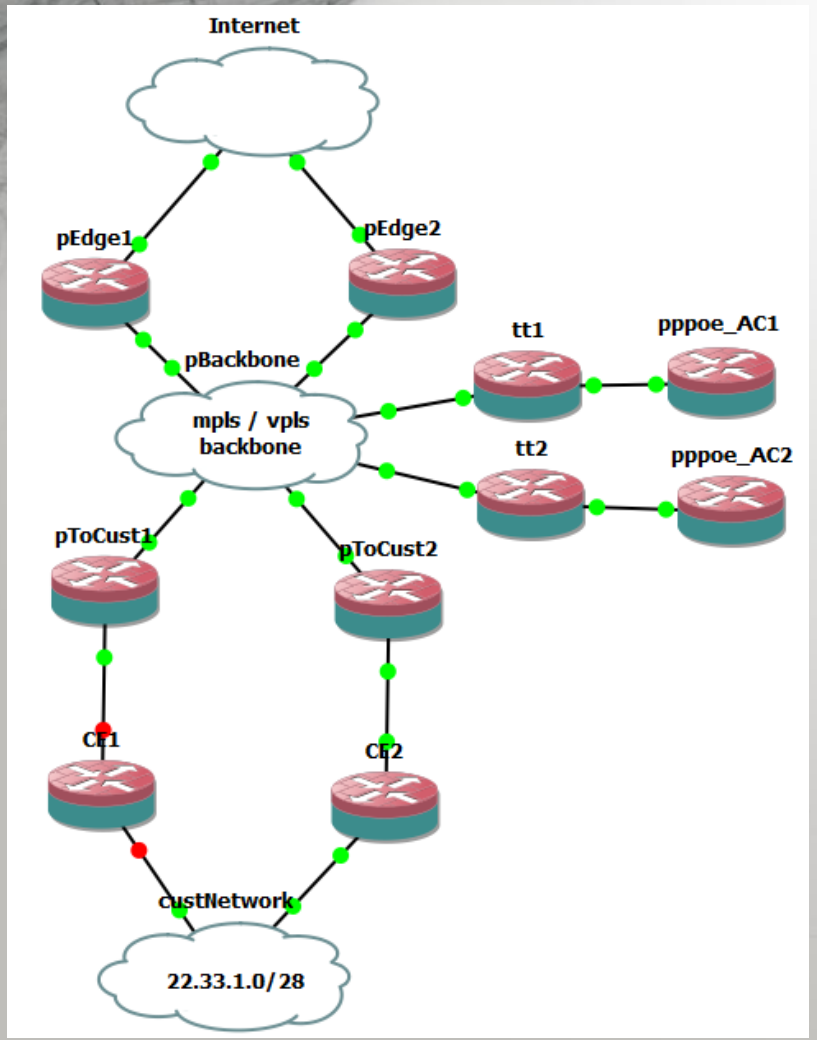
add action=discard chain=cust1-in

Result

- Customers will be able to inject routes for their IP ranges into our routing tables
- Redundancy will work
- OSPF peering with customer is secured

Load balancing using OSPF

- Customers can load-balance their outgoing traffic to us as they likes over the 2 connections
- Customers can load balance their incoming traffic by manipulating the OSPF path costs within their OSPF sessions to us - ECMP
- We achieved full load-balancing, and the customers can configure it how they like and change it without causing reconfiguration on our end – all by manipulating their OSPF interface costs



Complex topology

- ISP provides connectivity over PPPoE
- OSPF peering inside PPPoE
- Works with same config as above

GNS3 with MikroTik example

Simulating MikroTik networks

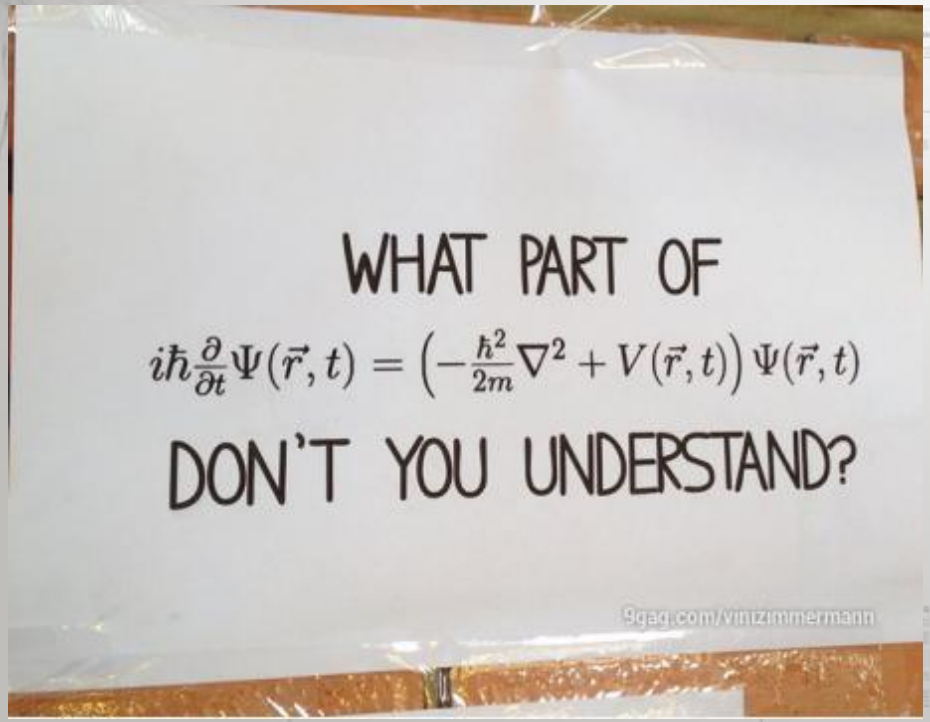
Final notes:

- This presentation is by no means a complete ready-to-implement solution.
- Advances OSPF knowledge is necessary to implement these topologies
- This presentation is not a full copy-paste solution, please test before deploying in production

More material

- US12:
  - Bandwidth-based load-balancing without MPLS TE
- EU13:
  - Building a scalable IPSec infrastructure with MikroTik
- US13:
  - MPLS for ISPs (PPPoE over VPLS)

- Available on www.tiktube.com



If you have any questions, please ask now, or find me after the presentation.

Thanks for listening

Tomas Kirnak

t.kirnak@atris.sk