```
--
  ^  ___  ___             http://www.GomoR.org/          <-+
  | / __ |__/          Systems & Security Engineer         |
  | \__/ |  \     ---[ zsh$ alias psed='perl -pe ' ]---    |
  +-->  Net::Frame <=> http://search.cpan.org/~gomor/  <---+
```

ERNW

Wir leben IT-Security.

Routing Protocol Security
IT-Underground, Prague, 2007

Still a problem in 2007?

or

„An example of breaking OSPF“

Who we are

- **Dror-John Roecher**
  - Security Consultant with a faible for enterprise networks and electronic gadgets.
  - Based in Germany. Working for ERNW GmbH.
  - Check this: www.ernw.de
  - no cool nick

- **Patrice <GomoR> Auffret**
  - Security Engineer, Perl network developper
  - Author of SinFP (an active and passive OS fingerprinting tool)
  - Currently employed by a big service company based in France
  - Check this: www.GomoR.org
  - And also this: www.GomoR.org/sinfp

What we will be talking about…

- **Part1 - The (maybe not so) dull theory**
  - The „marketing blah“ – why the stuff we are talking about is important. (very brief!)
  - OSPF operations in some detail.
  - Some ways of breaking OSPF.
  - Mitigating OSPF (again brief)
- **Part2 - The BYOL audience-participation**
  - Show you our tools ☺
  - Attacking OSPF networks

Why this talk?

- **Never found anything real good on „hacking“ OSPF – it was all theory and almost no hands-on.**
- **No tools available. Usually threats are only taken seriously when „tools“ are publicly available. So we need to change the lack of tools.**
- **Attacks on the infrastructure level are still not tapped to their full potential. Just remember yesterdays‘ „Digging into SNMP“ – another interesting „infrastructure level“ hacking technique.**

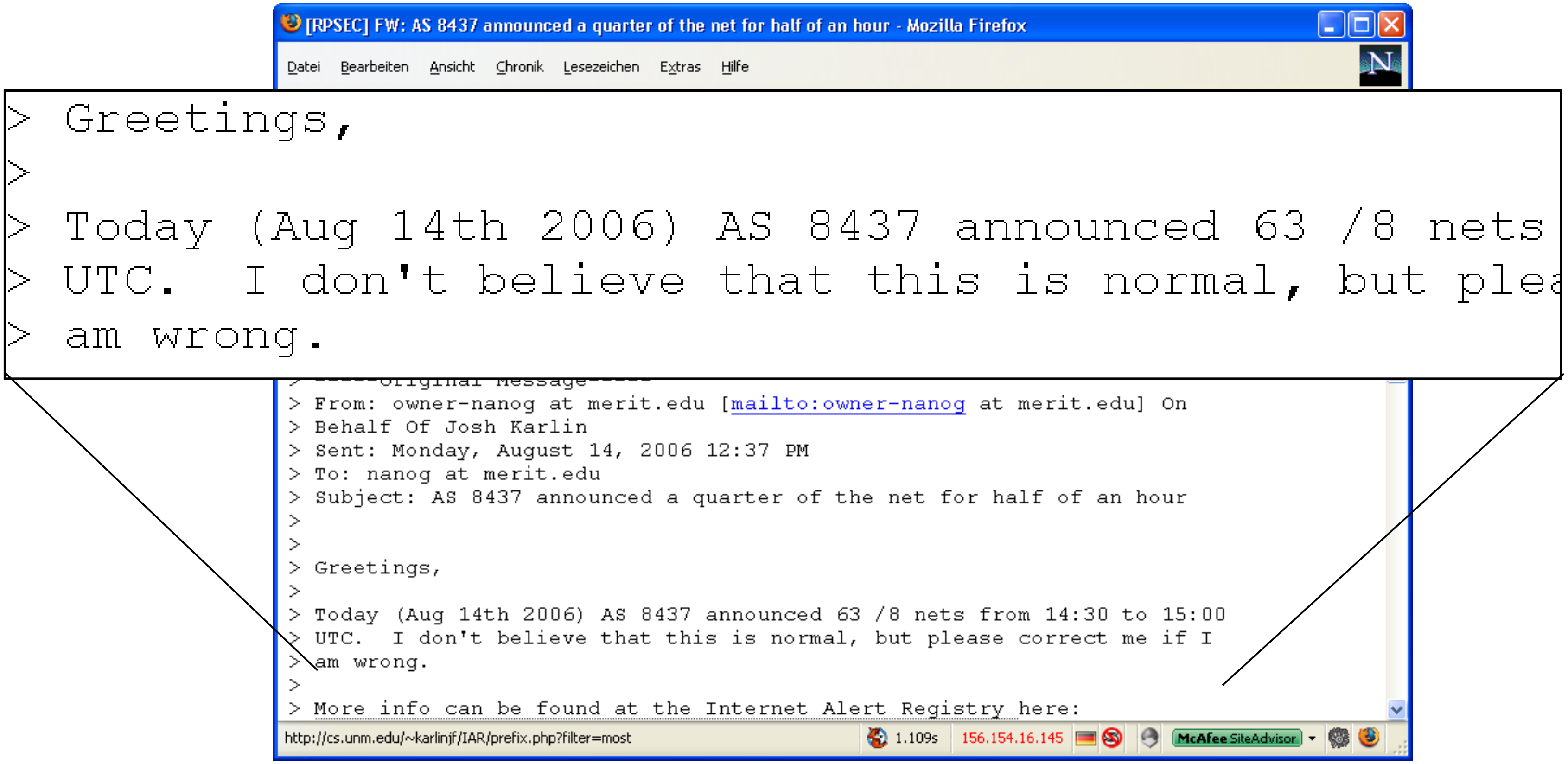
- **Plain old curiosity ,-)**

Brief History of „Routing Protocol Security“

- **Earliest known public discussion: RFC 789, Jan 1981.**
  - Faulty hardware caused faulty network control protocols which in „DoSed“ the ARPANet for a couple of hours…
- **A lot of discussion (with focus on BGP) ever since (just do a google search on „BGP Security“ and be overwhelmed)**
- **Many „add-ons“ [S-BGP, Secure BGP, etc] to BGP – but not much on other protocols.**

- **Structured effort in IETF „rpsec“ working group, but drafts are expired. They are really worth while reading – some guys put a lot of brain into these. Actually the best I have found on the topic so far!**

Scary… but fortunately only a „human error“


[RPSEC] FW: AS 8437 announced a quarter of the net for half of an hour - Mozilla Firefox
Datei
Bearbeiten
Ansicht
Chronik
Lesezeichen
Extras
Hilfe

```
> -----Original Message-----
> From: owner-nanog at merit.edu [mailto:owner-nanog at merit.edu] On
> Behalf Of Josh Karlin
> Sent: Monday, August 14, 2006 12:37 PM
> To: nanog at merit.edu
> Subject: AS 8437 announced a quarter of the net for half of an hour
>
>
> Greetings,
>
> Today (Aug 14th 2006) AS 8437 announced 63 /8 nets from 14:30 to 15:00
> UTC.  I don't believe that this is normal, but please correct me if I
> am wrong.
>
> More info can be found at the Internet Alert Registry here:
```

```
> Greetings,
>
> Today (Aug 14th 2006) AS 8437 announced 63 /8 nets
> UTC.  I don't believe that this is normal, but plea
> am wrong.
```

Routing Protocols in use…

- **BGP runs the internet (besides DNS & caffeine).**
- **OSFP & IS-IS & EIGRP run enterprise networks.**
- **RIP is [mostly] dead.**

- **We will be talking (only) about OSPF (because that is what we will be doing in the BYOL and because it is in wide usage).**

Let‘s have a look at how OSPF works

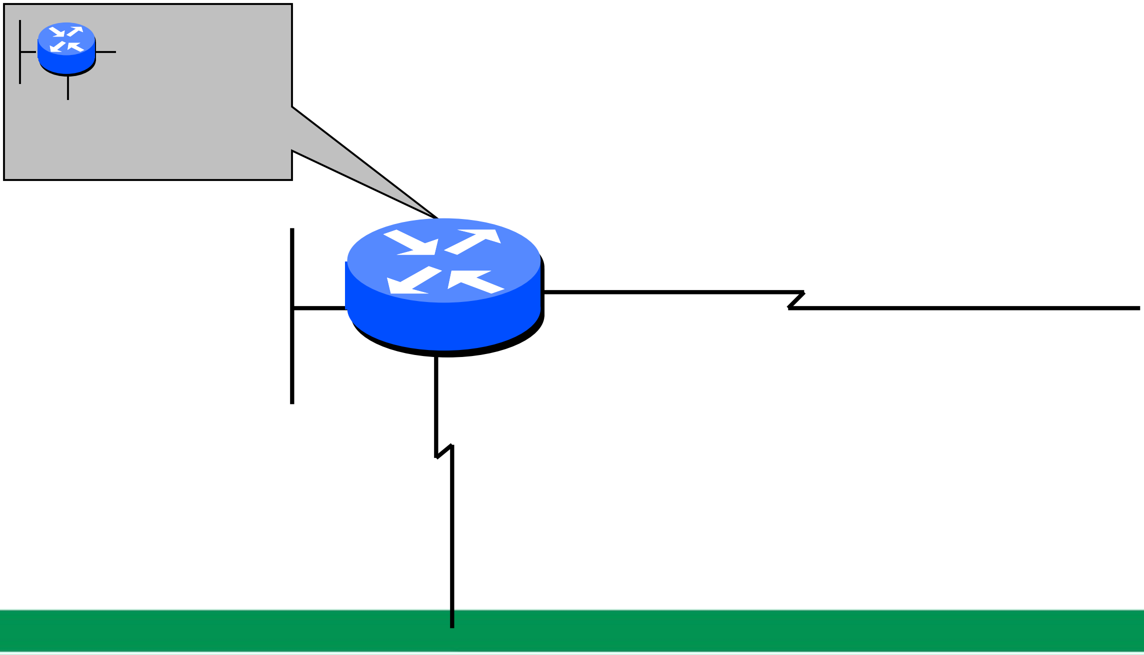
OSPF „quick & dirty“

OSPF „quick & dirty“

1. **All OSPF Routers multicast periodic „Hello“ packets. If a „Hello“ is received from a different router (and if some additional requirements are met), than the routers form a „neighbor“-relationship.**
2. **Certain neighborships are elevated to „adjacencies“. Adjacent routers synchronise their topology information through LSA-packets.**
3. **The topology information is stored in a local database and used to graph the network.**
4. **The graph is used to calculate the „shortest path tree“.**
5. **From this tree routes to all networks are derived and installed into the routing-table.**

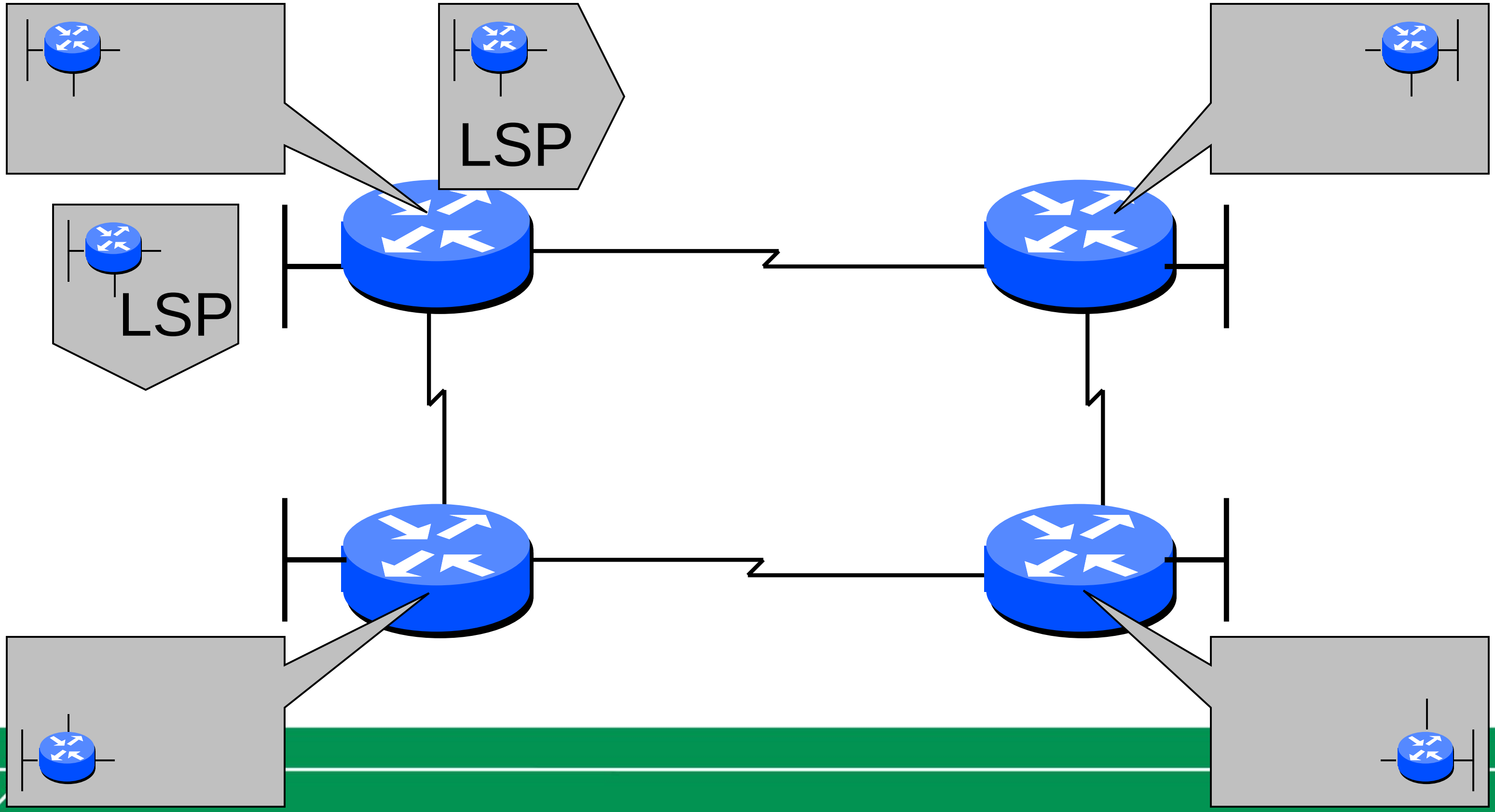
Link State Advertisments

- **Every Router advertises its own links.**



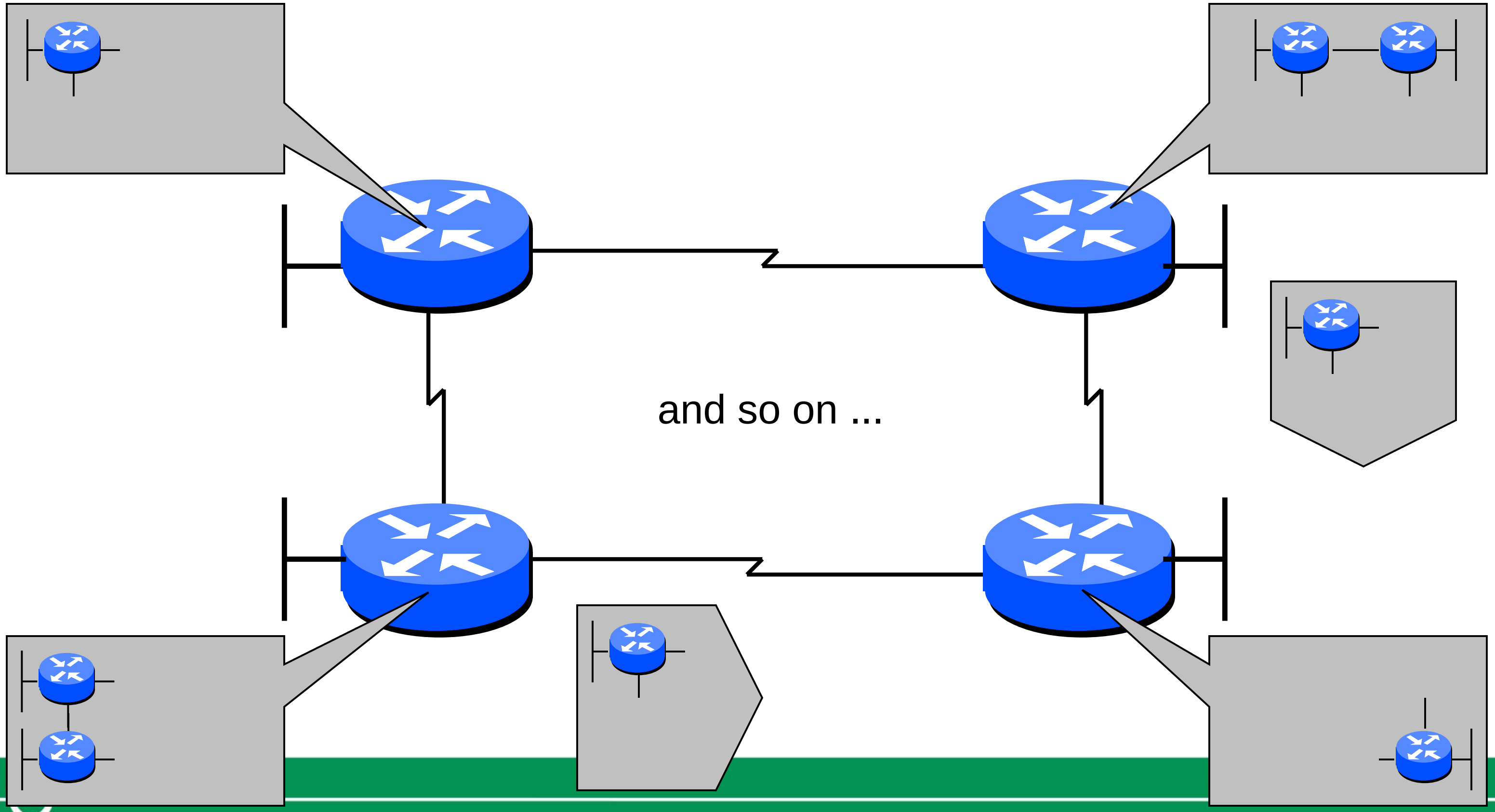
Link State Advertisments

- **These LSAs get flooded through the network**



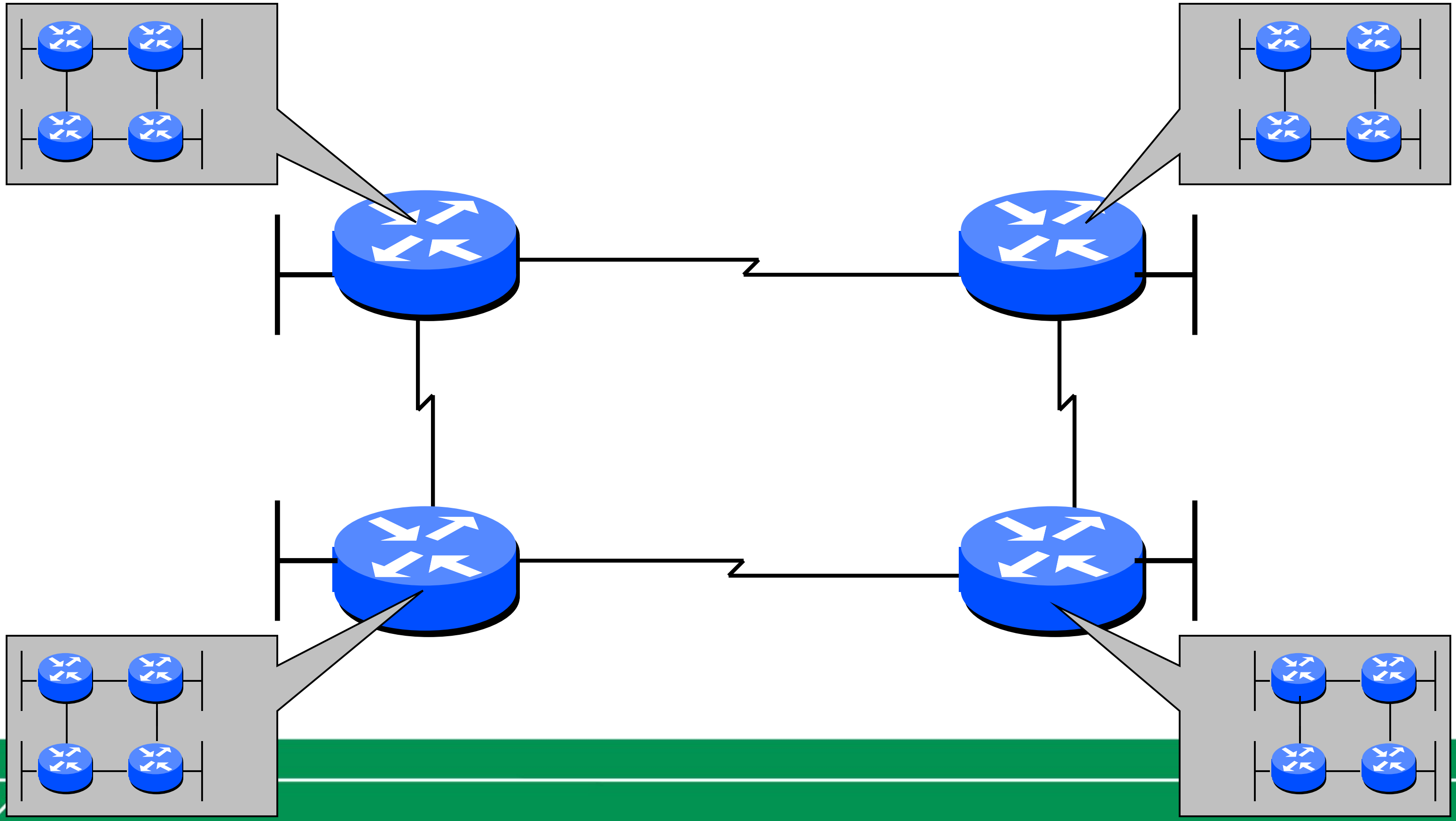
LSA and Flooding

- **Every router stores the received LSAs in its topology database**

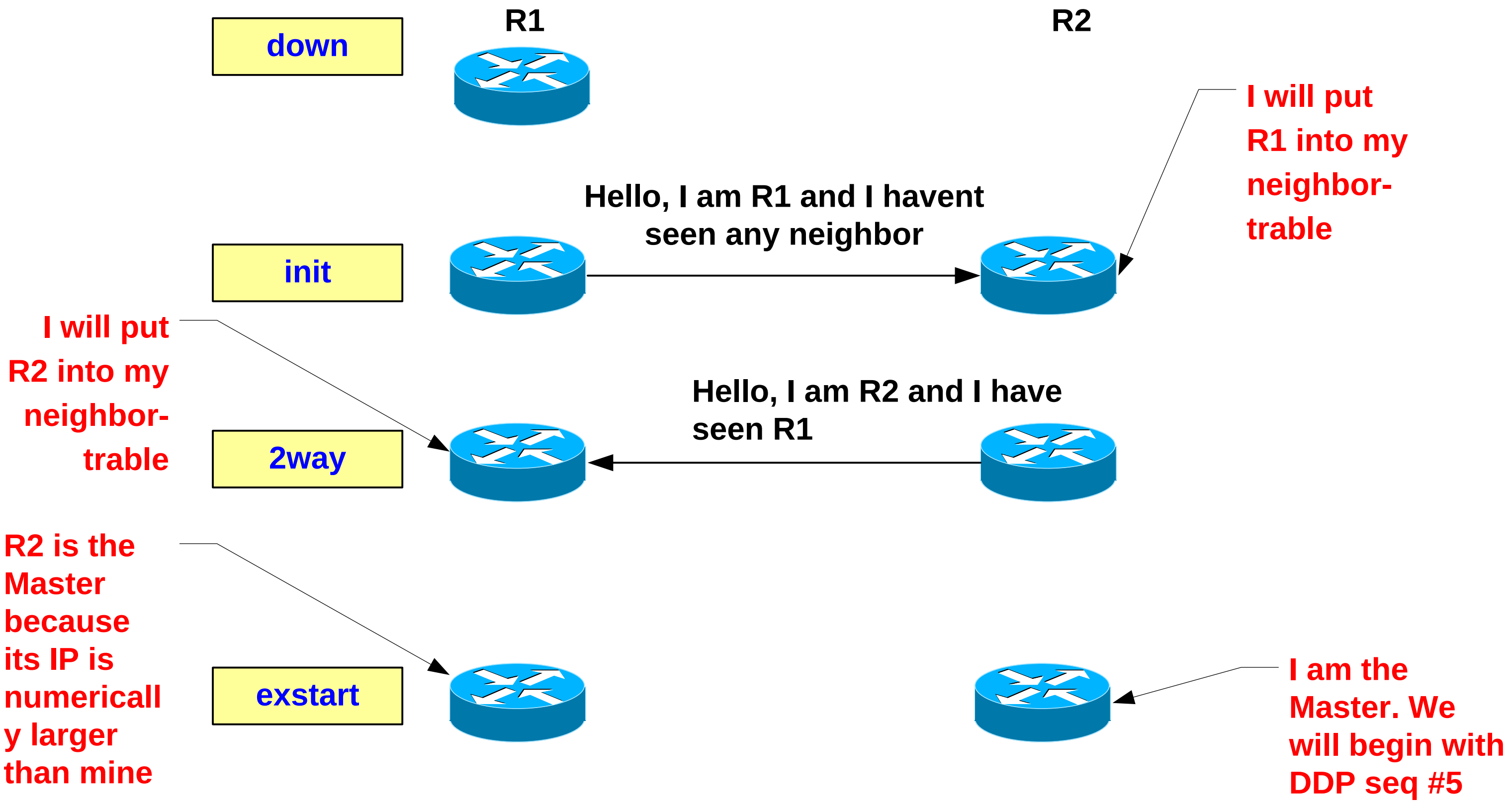


Full Topology

- **Finally every router nows the complete topology**



OSPF State Machine (1/2)



Hello, I am R1 and I havent seen any neighbor

I will put R1 into my neighbor-trable

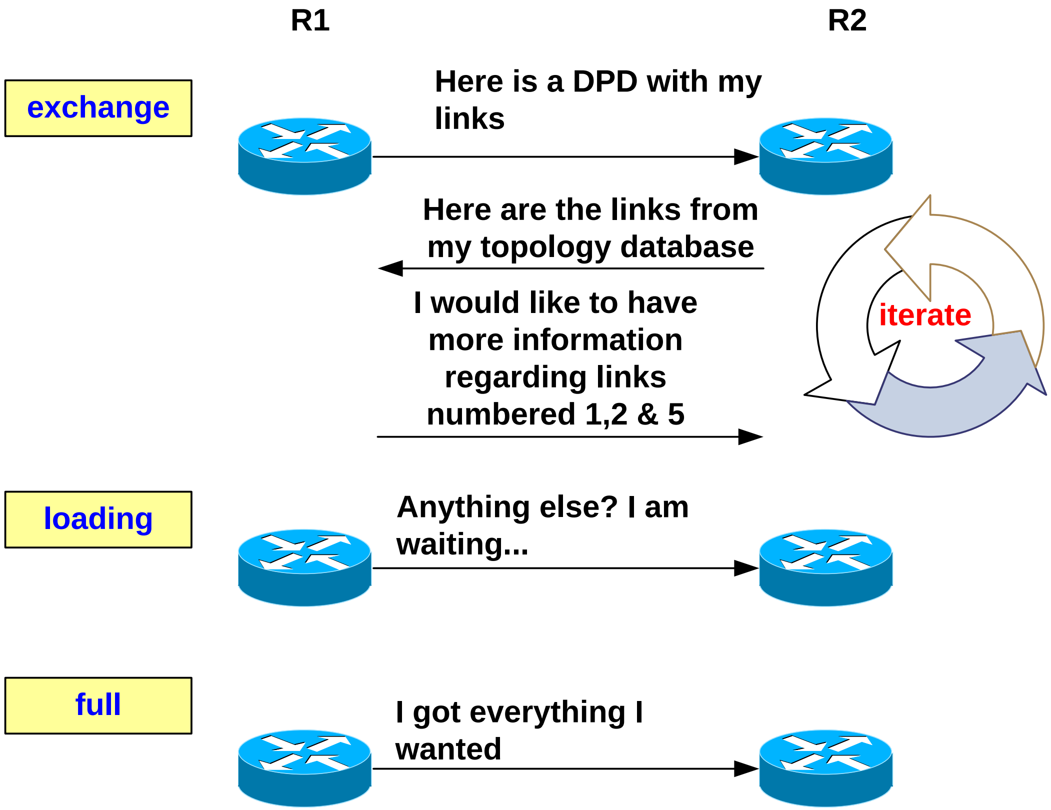
I will put R2 into my neighbor-trable

Hello, I am R2 and I have seen R1

R2 is the Master because its IP is numericall y larger than mine

I am the Master. We will begin with DDP seq #5

OSPF State Machine (2/2)



R1
R2
exchange
Here is a DPD with my links
Here are the links from my topology database
I would like to have more information regarding links numbered 1,2 & 5
iterate
loading
Anything else? I am waiting...
full
I got everything I wanted

OSPF Authentication

- **Per default OSPF has no authentication.**

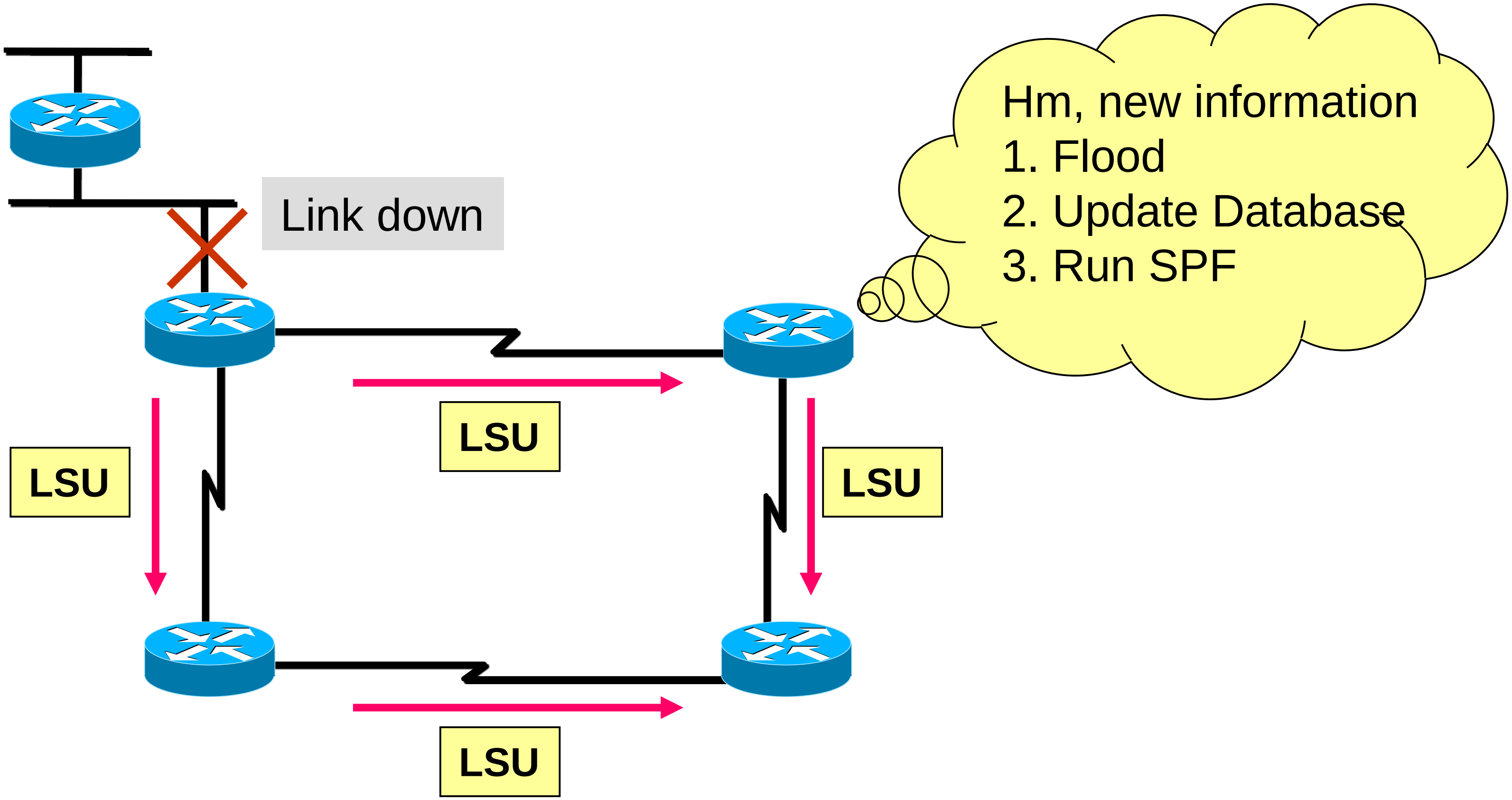
- **Two different authentication-schemes exist, which can be used to increase security:**
  - Simple password authentication (that is plaintext passwords)
  - Message Digest authentication (md5 based)

- **Both are based on a „pre shared key“.**

Hello Paket Format

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Version #   |       1       |         Packet length         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Router ID                            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Area ID                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           Checksum            |             AuType            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Authentication                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Authentication                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        Network Mask                           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         HelloInterval         |    Options    |    Rtr Pri    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     RouterDeadInterval                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Designated Router                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                   Backup Designated Router                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Neighbor                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Neighbor ...                         |
```

Flooding occurs when topology changes are noticed



Hm, new information
1. Flood
2. Update Database
3. Run SPF

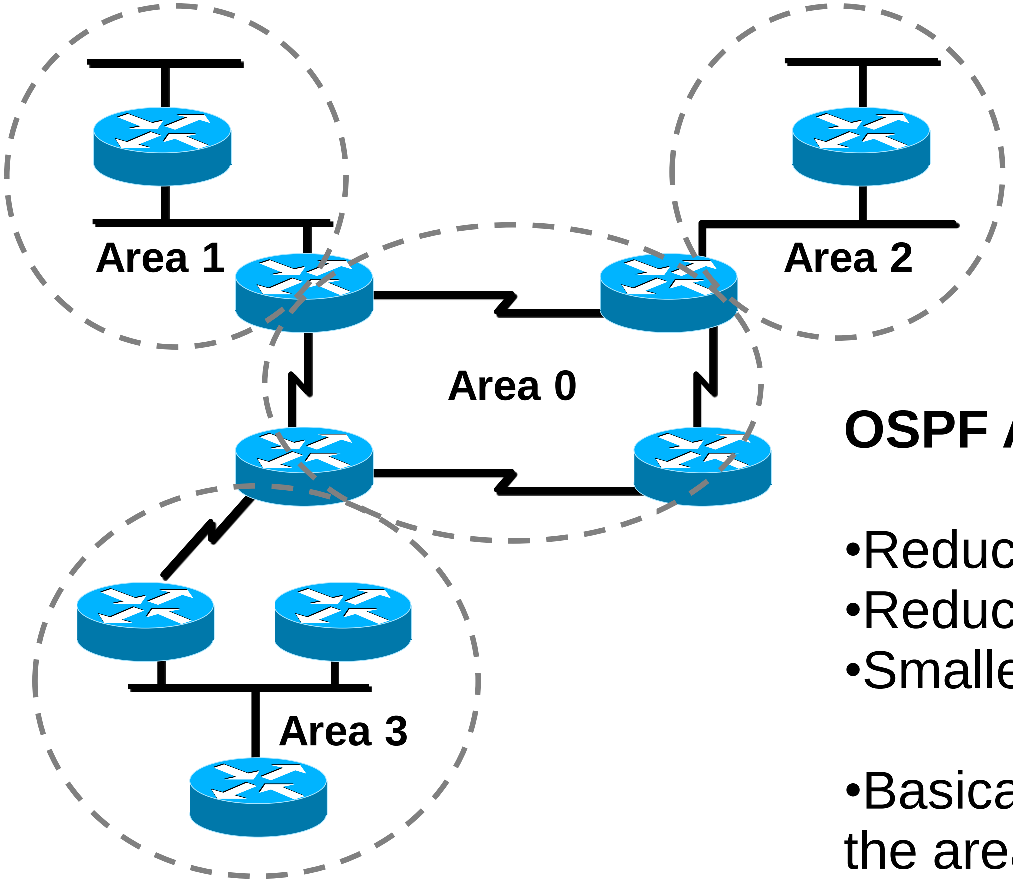
OSPF Fightback mechanism

- **What is Fightback?**
  - Every LSA that is circulating with wrong information will be corrected by its owner. That is if an attacker spoofs an LSA from a different router with wrong information the original owner will correct it by sending „correct“ LSA.

- **Common perception of fightback**
  - Fightback corrects most attacks (and therefor attacks on OSPF are not feasible)
  - Many theoretical attacks will cause only a brief topology change and are therefor not feasible.

  - Tell you something: Theses perceptions are plain wrong - I will show you later why ;-)

OSPF Areas



OSPF Area Konzept:

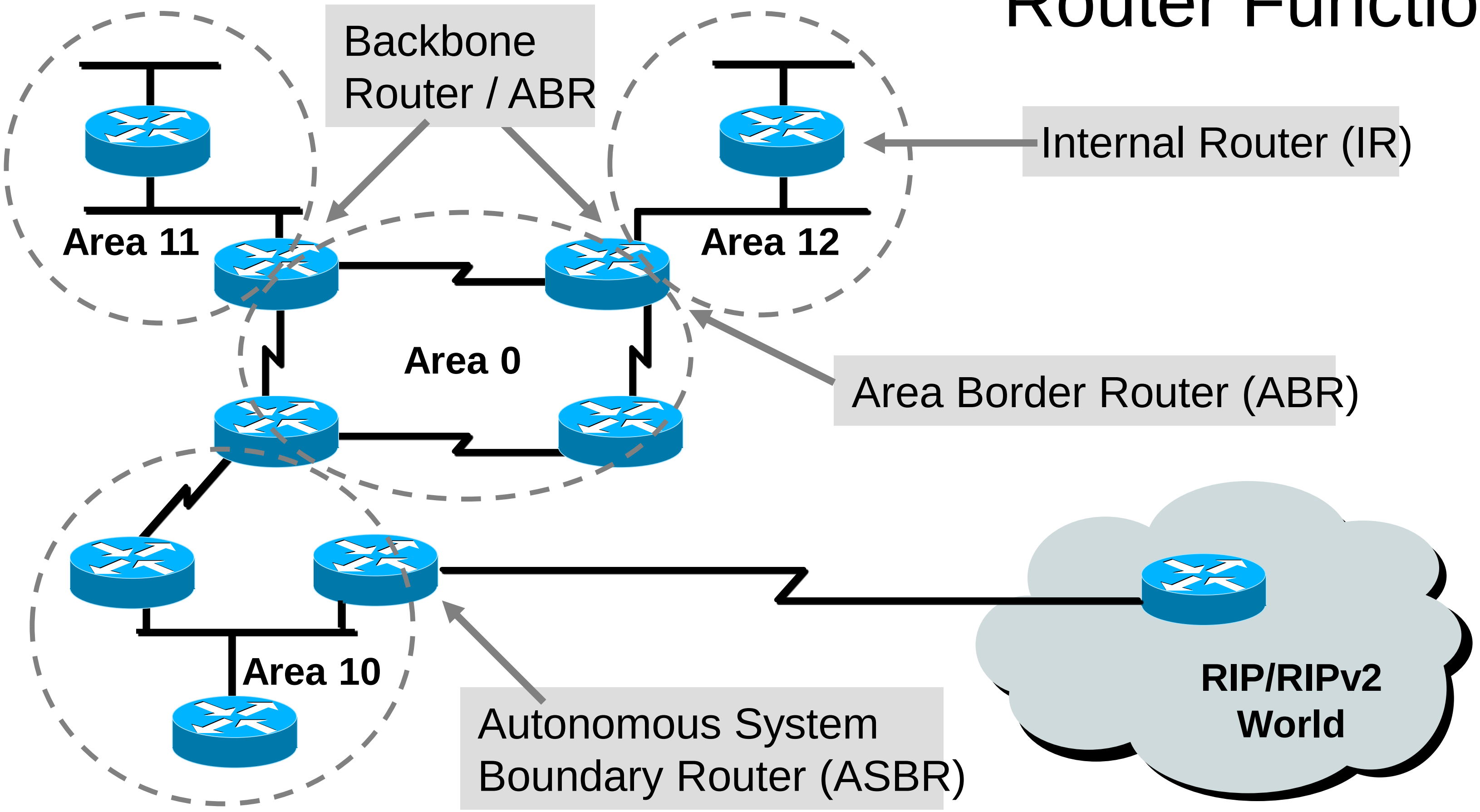
- Reduced Routing information,
- Reduced flooding of LSUs
- Smaller SPF tree – less CPU-cycles

- Basically: keep local changes local (to the area)

Some „rules“ on OSPF Areas

- **Areas are identified by a 32-Bit identifier**
- **Area 0.0.0.0 (or simply Area 0) is always the Backbone Area.**
- **All other Areas must be directly connected to the Backbone Area.**

Router Functions



Different Area Types – different information within

- **Normal Area**
  - All LSA Types are forwarded. (The Backbone Area always falls into this category)
- **Stubby Area**
  - No external LSAs are forwarded in stubby areas. Instead a default pointing to the ABR is inserted. Inter area routes are allowed.
- **Totally Stubby Area**
  - No external and no inter area routes – everything that is not local to the area is handled by a default-route.
- **Not So Stubby Area**
  - These area are basically stubby areas with external routes originating from a router within the area.

Different LSA for different information….

LSA-Type	who?	Content?
Type1:	everyone	Links
Type2:	DR	Network
Type3:	ABR	Network Summaries (interarea)
Type4:	ABR	Routes to the ASBR
Type5:	ASBR	External Routes
Type7:	ASBR	NSSA External Routes (Type7-LSAs are converted by ABRs to Type5-LSAs).

LSA Types

- **Router Links (Type1-LSA)**
- **Every Router** sends information about connected links as **Type1-LSA**.

- **Network Links (Type2-LSA)**
- **DR** send Network Link LSAs as **Type2-LSAs**, these include information about the network (network address, netmask, connected router).

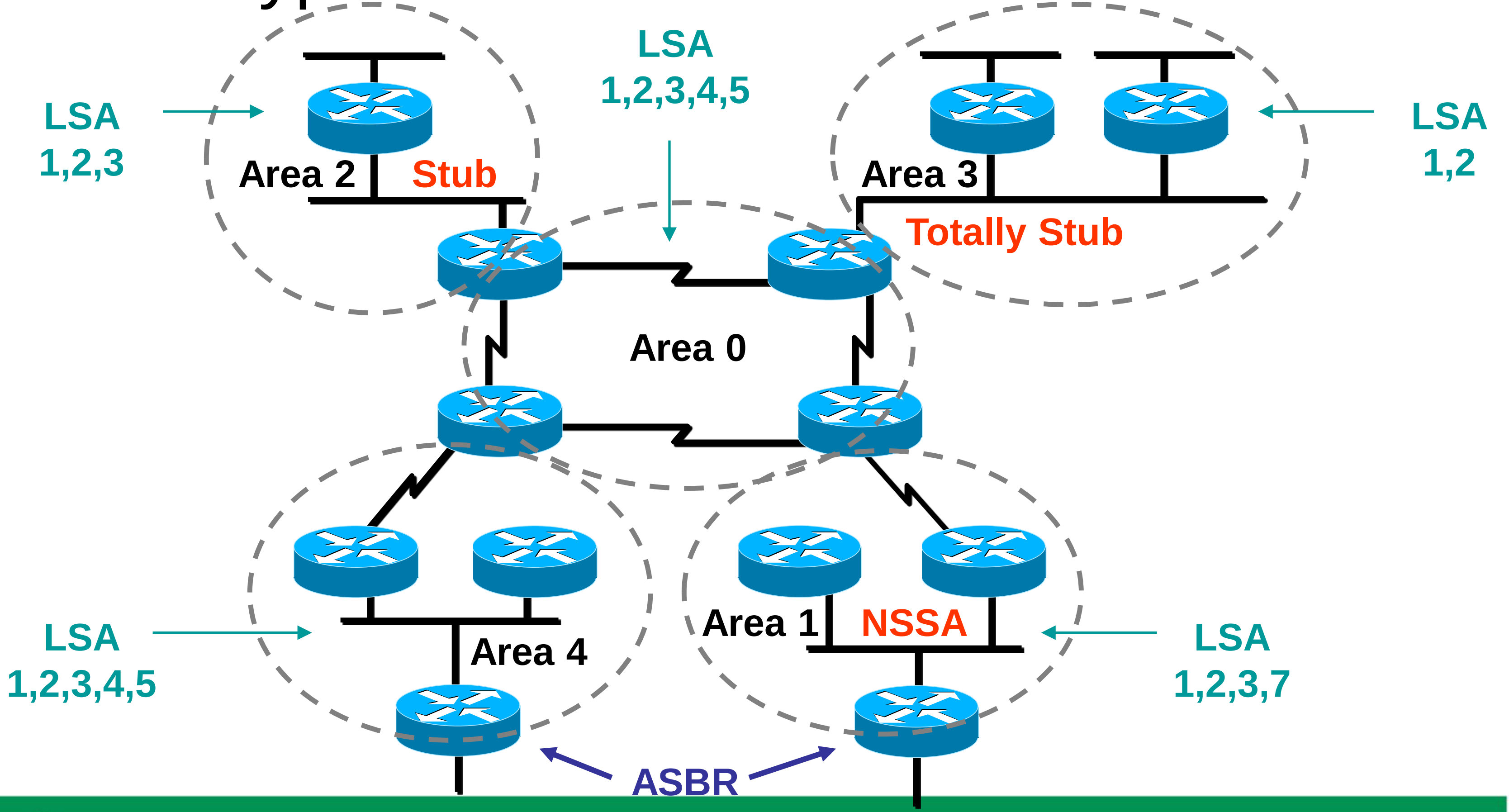
- **Network-Summary (Type3-LSA)**
- **Type3-LSAs** include informationen for networks in other areas and are generated by **ABRs**. (Type3-LSAs are not include in SPF calculation).

LSA Types

- **ASBR Summary (Type4-LSA)**
- **LSA Type4** are generated by **ABRs** and include routes to the ASBRs).

- **ASBR External LSA (Type5-LSA,Type7-LSA)**
- **ASBRs** send ASBR External LSAs (**Type5-LSA)**, including information about networks outside the OSPF AS or a default route to outside the OSPF AS.
- If these Type-5 LSAs are sourced by an ASBR of a NSS, it is send as a **Type7-LSA.** Type7-LSAs are changed to **Type5-LSAs** by the ABR of the NSSA.

LSAs & Area Types



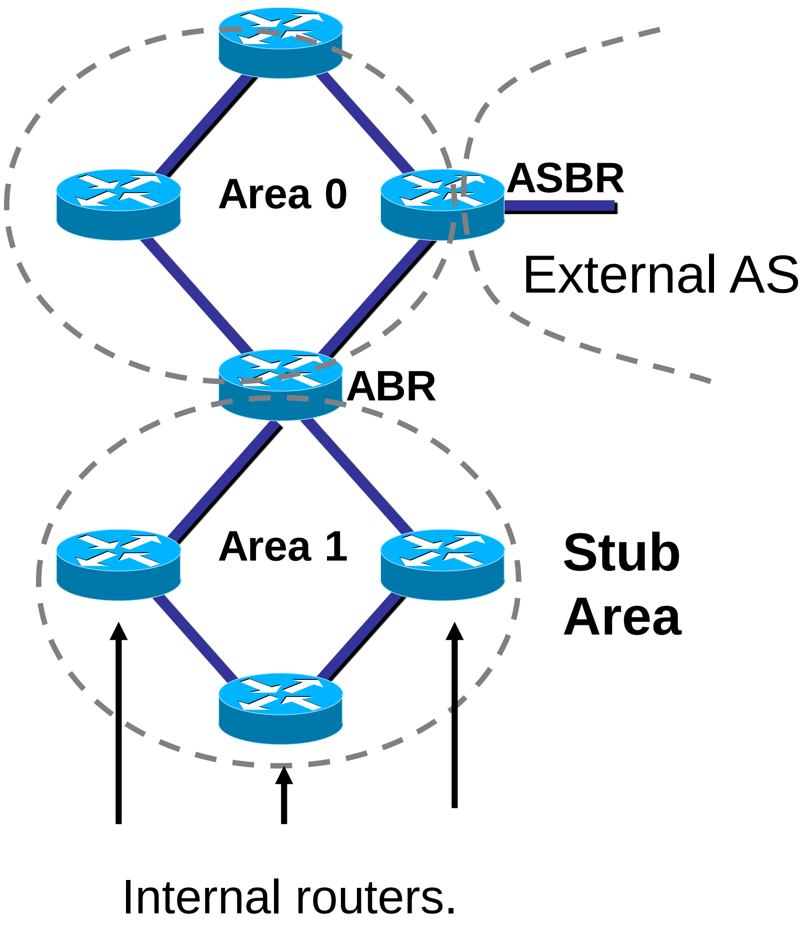
sh ip route - standard area

```
RouterA#sh ip route
Codes:   C - connected, O - OSPF, IA - OSPF inter area
         E1 - OSPF external type 1, E2 - OSPF external type 2,
         * - candidate default

Gateway of last resort is not set

         203.250.15.0 255.255.255.252 is subnetted, 1 subnets
C        203.250.15.0 is directly connected, Serial0
O IA     203.250.14.0 [110/74] via 203.250.15.1, 00:06:31, Serial0
         128.213.0.0 is variably subnetted, 2 subnets, 2 masks
O E2     128.213.64.0 255.255.192.0
                       [110/10] via 203.250.15.1, 00:00:29, Serial0
O IA     128.213.63.0 255.255.255.252
                       [110/84] via 203.250.15.1, 00:03:57, Serial0
         131.108.0.0 255.255.255.240 is subnetted, 1 subnets
O        131.108.79.208 [110/74] via 203.250.15.1, 00:00:10, Serial0
```

Stub Area



Stub area

No external LSAs are propagated within stub areas. Internal routers have a default pointing to the ABR.

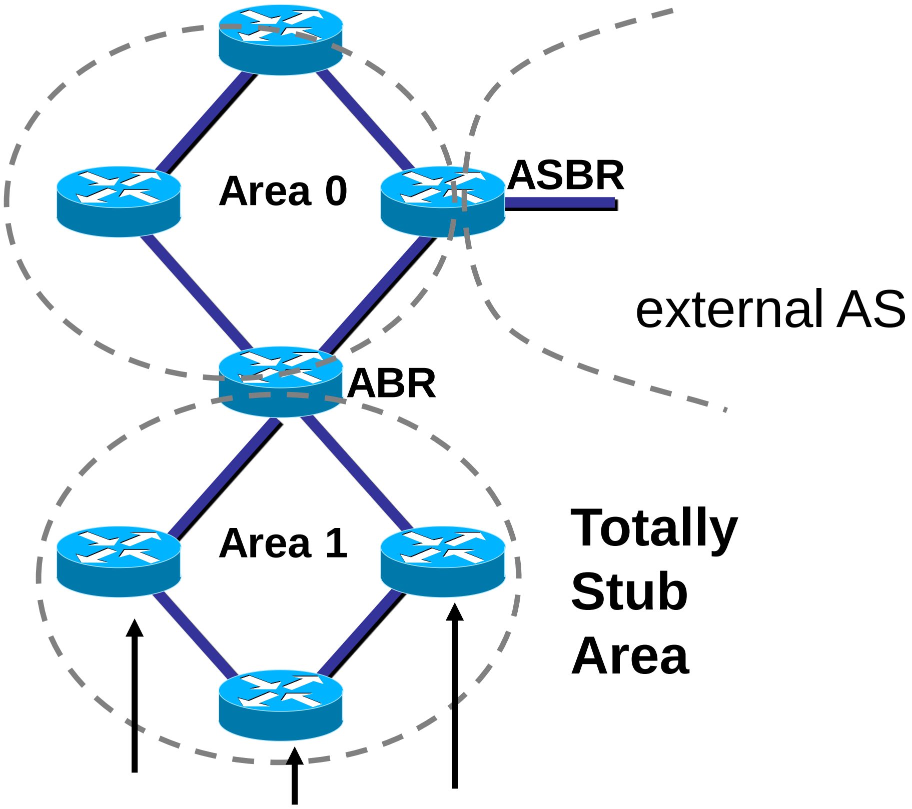
sh ip route - stub area

```
RouterA#sh ip route
Codes:   C - connected, O - OSPF, IA - OSPF inter area
         E1 - OSPF external type 1, E2 - OSPF external type 2,
         * - candidate default

Gateway of last resort is not set

         203.250.15.0 255.255.255.252 is subnetted, 1 subnets
C        203.250.15.0 is directly connected, Serial0
O IA     203.250.14.0 [110/74] via 203.250.15.1, 00:26:58, Serial0
         128.213.0.0 255.255.255.252 is subnetted, 1 subnets
O IA     128.213.63.0 [110/84] via 203.250.15.1, 00:26:59, Serial0
         131.108.0.0 255.255.255.240 is subnetted, 1 subnets
O        131.108.79.208 [110/74] via 203.250.15.1, 00:26:59, Serial0
O IA    0.0.0.0 0.0.0.0 [110/65] via 203.250.15.1, 00:26:59, Serial0
```

Totally stub Area



Internal routers.

Totally stubby area
No external routes and not inter-area routes are known within a totally stubby area.

Everything which is not local to the area is routed via a default to an ABR.

sh ip route - totally stub area

```
RouterA#sh ip route
Codes:   C - connected, O - OSPF, IA - OSPF inter area
         E1 - OSPF external type 1, E2 - OSPF external type 2,
         * - candidate default

Gateway of last resort is not set

         203.250.15.0 255.255.255.252 is subnetted, 1 subnets
C        203.250.15.0 is directly connected, Serial0
         131.108.0.0 255.255.255.240 is subnetted, 1 subnets
O        131.108.79.208 [110/74] via 203.250.15.1, 00:31:27, Serial0
O IA    0.0.0.0 0.0.0.0 [110/74] via 203.250.15.1, 00:00:00, Serial0
```

Attacking OSPF

What are the consequences of attacking OSPF?

- **Disruption and/or Manipulation of the Routing Domain**

Attack Vectors

OSPF Attack Vectors…

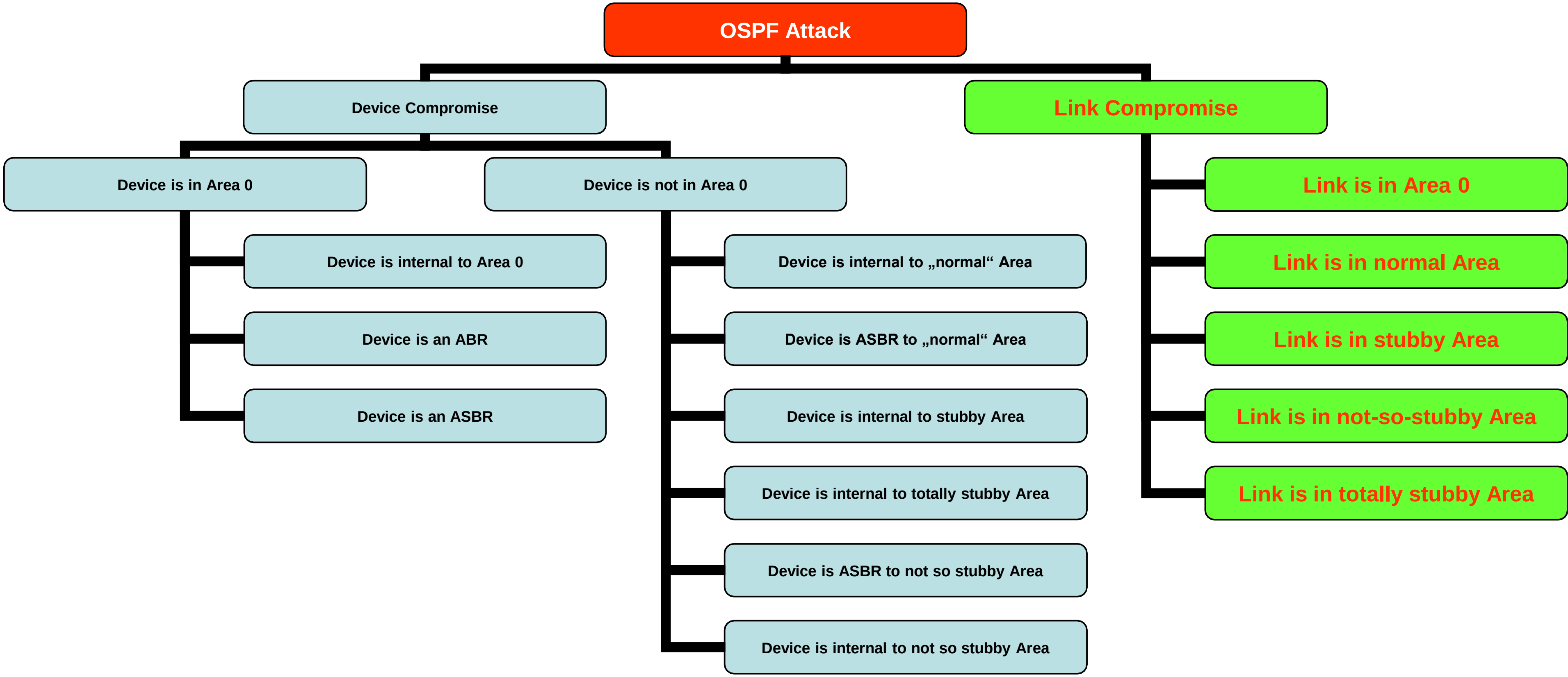
That is what we will talk about today :-)

- **Classification of attack-vectors:**
  - Attacks which originate from the outside of the OSPF network
    - Prerequisite: Attacker is able to send unicast OSPF-packets to an internal OSPF router. This should not be possible, because OSPF packets should not be allowed to enter the network.
  - Attacks which originate from the inside of the OSPF network
    - Device Compromise: Attacker has administrative access (console or ssh) to an OSPF-router.
    - Link Compromise: Attacker has access to a network-link, where OSPF is being spoken by one or more connected routers.
  - Attacks through „broken“ implementations: BOs in ospfd etc. – not in scope for todays‘ talk, even though they may have a huge impact on overall security.

Link Compromise

- **Link is in Area 0**
- **Link is not in Area 0**
  - Link is in „normal“ Area
  - Link is in „stubby“ Area
  - Link is in „not so stubby“ Area
  - Link it in „totally stubby“ Area

The Attack Vectors as a graph



OSPF Attack

Device Compromise

Device is in Area 0

Device is internal to Area 0

Device is an ABR

Device is an ASBR

Device is not in Area 0

Device is internal to „normal“ Area

Device is ASBR to „normal“ Area

Device is internal to stubby Area

Device is internal to totally stubby Area

Device is ASBR to not so stubby Area

Device is internal to not so stubby Area

Link Compromise

Link is in Area 0

Link is in normal Area

Link is in stubby Area

Link is in not-so-stubby Area

Link is in totally stubby Area

Some Threats through Device Compromise

- **We will not go into depth here (mostly for time-reasons and because threats are somewhat obvious).**
- **Some possible threats:**
  - DoS: Dropping of routes
  - DoS: (Partial) Disabling of OSPF
  - DoS: Addition of „bogus“ routes via loopback interfaces (e.g. with /32 mask to have a „longest match“)
  - DoS: Creating Routing loops (which adds congestion besides DoS)

- **These are not very interesting, because any change to OSPF will affect the local routing table, too and the interesting attacks avoid just that.**

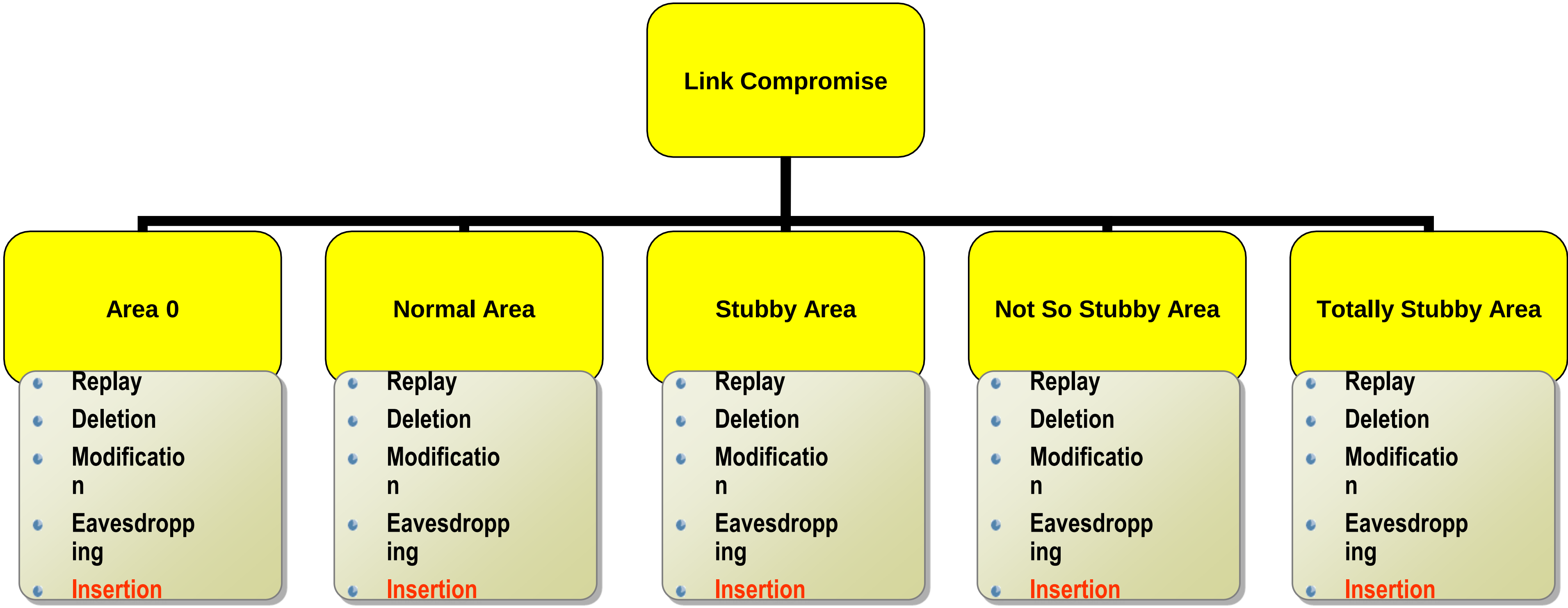
Threats through Link Compromise

- **Denial of Service:**
  - Blackhole: Traffic is directed to a router which cannot handle the load.
  - Starvation: Traffic is forwarded to a part of the network, that can not deliver it.
  - Delay: Traffic is routed via a suboptimal path.
  - Loop: Traffic is forwarded along a looping path.
  - Partition: Some part of the network believes it is partitioned from the rest, when in fact it is not.
  - Churn: Forwarding on the network changes rapidly, resulting in large variations of data-delivery patterns (impacting congestion control mechnisms).
  - Instability: OSPF itself becomes unstable so that global convergence is never achieved.
  - Overload: OSPF messages themself become a significant part of the network traffic.
  - Resource Exhaustion: OSPF messages cause exhaustion of router ressources (queues, memory, cpu).
- **Man in the Middle**
  - Eavesdropping: Carefully crafted insertion of routing information may lead to rerouting through attacker which may put the attacker in the packet-path. These are quite difficult to accomplish. But this is (imho) the most interesting attack scenario.

Attacks on „Link Compromise“ fall into one of these classes

- **Message Replay**
- **Message Insertion (that will be the focus today)**
- **Message Deletion (usually detectable by the sender)**
- **Message Modification**
- **Message Eavesdropping (almost always needed to gain some knowledge about how OSPF is set up)**

Link Compromise



Link Compromise

Area 0
- Replay
- Deletion
- Modification
- Eavesdropping
- Insertion

Normal Area
- Replay
- Deletion
- Modification
- Eavesdropping
- Insertion

Stubby Area
- Replay
- Deletion
- Modification
- Eavesdropping
- Insertion

Not So Stubby Area
- Replay
- Deletion
- Modification
- Eavesdropping
- Insertion

Totally Stubby Area
- Replay
- Deletion
- Modification
- Eavesdropping
- Insertion

Abetting Factors – Link Compromise

- **OSPF Routers on Broadcast, NBMA, PtMP and Virtual Links accept Unicast packets (Section 8.1 in RFC 2328). Therefor many attacks for link-compromise work also „from remote“, as long as the attacker is able to send IP-Protocol-89 packets to a legitimate OSPF router.**
- **Usually same key used on all links (if any at all).**
- **Tools for breaking OSPF-MD5-keys exist (e.g. Cain & Abel)**

Attack Classification - Message Insertion

Categories of Attacks – Message Insertion (1/2)

- **Setting up phanthom routers (routers that dont exist)**
  - Simple „hello“ suffices to get into neighbor-tables. But that should have no impact – just a „gimmick“
- **Spoofing messages from existing routers**
  - Send „hellos“ with on a link where the router acutally isnt located (not sure if OSPF fightback should come into place).
  - Send „hellos“ on a link where the router is located
  - Send spoofed LSAs (here the OSPF fightback mechanism should come into place) – which can be leveraged for DoS by taking advantage of timer-mechnisms in OSPF.

Categories of Attacks – Message Insertion (2/2)

- **Adding a „real“ router – rerouting to traffic**
  - In the Backbone Area
    - Inject Type 1,2,3,5 LSAs
  - In a normal Area
    - Inject Type 1,2,3,5 LSAs
  - In a stubby Area
    - Inject Type 1,2,3 LSAs
  - In a totally Stubby Area
    - Inject Type 1,2 LSAs
  - In a NSSA
    - Inject Type 1,2,7 LSAs

When adding a „real“ router…

- **Message Insertion aimed at manipulating routing information:**
  - Add „new“ networks (e.g. 194.77.14.0/24) as „internal“ to an Area
  - Add existing networks used in a different Area
  - Add default routes
    - Either as ABR
    - Or as ASBR
  - Add new Areas – with new networks
  - Add new Areas – with networks already used somewhere else in the AS
- **Possibilities depend on where the compromised link is located.**

When sending spoofed LSAs…

- **OSPF „Fightback“ should kick in, but…**
  - Using periodic injection of spoofed LSAs will exploit that there is a MinLSInterval timer (default 5 seconds). The legitimate owner of the LSA will honor that interval, an attacker will not. Resulting in permanent or semi-permanent changes to the topology
  - And the legitimate owner may even help in flooding the spoofed LSA…
    - The spoofed LSA has a higher squence number.
    - A copy of the LSA is already present on the original router in the LSDB and this copy was installed and not received through flooding.
    - Effect: The malicious LSA will be first flooded by the legitimate owner and then checked for „correctnes“.
    - After the error is uncovered, the legitimate router will _try_ to correct. Try, because of MinLSInterval (dont send the same LSA faster than MinLSInterval) – but in the meantime a new spoofed LSA might arrive, which will be flooded immediately…
  - Using Message-Modification or Message-Deletion an attacker may prevent the legitimate owner of ever receiving the spoofed LSA. Then Fightback will never occur.

There are more ways to break OSPF

- **But we havent explored them all yet… more work to do.**
- **We have limited time for the session – so we had to choose which one to show.**
- **Some need very deep OSPF knowledge – again time constraints prevent talking about these.**
- **Some depend on „special“ circumstances / setups – we have neglected these so far.**

- **If you feel like you could contribute and if you would like to contribute – contact us.**
- **If you want to know more – contact us.**

And at the end a few words on the other protocols…

- **RIP makes it even easier than OSPF to manipultae the routing domain – my advice: just dont use it.**
- **IS-IS _should_ be as difficult to hack as OSPF – but there is even less on IS-IS security than on OSPF security. Now that is a topic where one could earn ones‘ first wings… and sites running IS-IS are usually very large.**
- **EIGRP is proprietary Cisco stuff – not too much known on that (FX released „irpas“ some years ago – but as to my knowledge noone followed the lead and expanded on his work)**
- **BGP seems to get the most attention – because it „runs the internet“ and hacking _that_ would have a real global (economic) impact.**

Mitigation

Mitigating attacks on OSPF

- **Preventive**:
  - Use md5-authentication with strong passwords
  - Change passwords periodically
  - Disable OSPF on access-links (dont expose your passwords to clients!)
  - Instead of „passive interface“ consider using „redistribution“ of connected access-networks (dont accept OSPF messages on these interfaces – not sure about this one, needs validation and has impact on routing!)
  - Strict ingress filtering (but make sure not to break your routing)
    - From outside, of course never ever accept OSPF (ip protocol 89)
    - From access-networks, never ever acceept OSPF (ip protocol 89)
    - Multicast Filtering (224.0.0.5 & 224.0.0.6) may come in handy, too.
  - Use Summarization
    - This may keept attacks local to an area (not sure, needs validation!)
- **Detective**:
  - Monitor OSPF neighbor changes (unexpected new neighbor is usually not something you want to see on your network)
  - Monitor routing-changes (changes not related to a link/hardware failure should make you suspicious)
  - Anomaly-based IDS could be tought to detect unnormal OSPF behaviour - need to validate.

References – as a starting point for further reading

- **http://tools.ietf.org/html/draft-ietf-rpsec-ospf-vuln-02**
- **RFC 4953: Generic Threats to Routing Protocols**
- **RFC 2328: OSPFv2**
- **CPAN: Net::Packet::OSPF**

- **And if you want to have the tool-code:**
  - www.ernw.de
  - www.gomor.org

End of Slides-Session
&
Start of BYOL Session

Prerequisites for BYOL

- **Technical**
  - A networked Laptop with VMWare Workstation or Server installed
  - Our prepared VMWare-Image
- **Knowledge & Experience**
  - Some knowledge of Linux & Perl
  - Some experience with Cisco IOS
- **And please follow the instructions, the lab is quite complex and we want to avoid total chaos.**

```
--
  ^  ___  ___             http://www.GomoR.org/          <-+
  | / __ |__/          Systems & Security Engineer         |
  | \__/ |  \     ---[ zsh$ alias psed='perl -pe ' ]---    |
  +-->  Net::Frame <=> http://search.cpan.org/~gomor/  <---+
```

ERNW
Wir leben IT-Security.

děkuji pěkně

dotazy a že odpovědi…