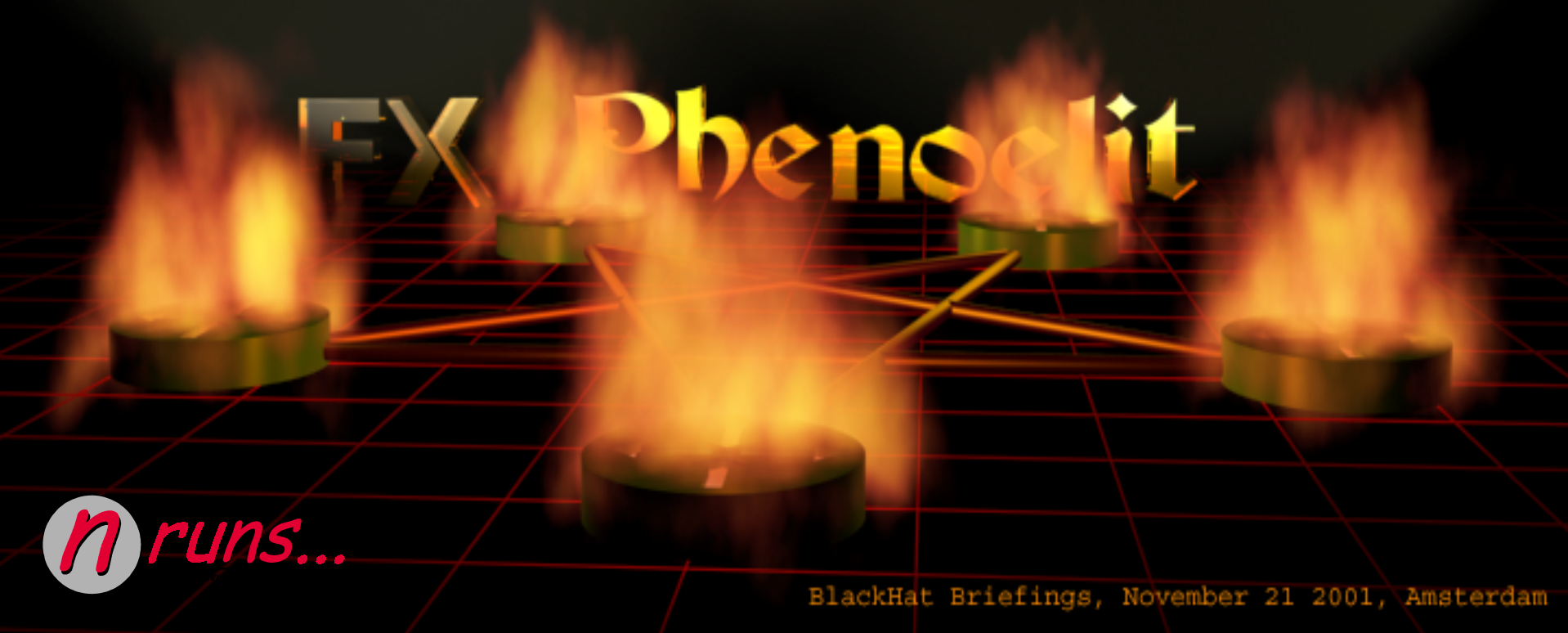
Routing Protocol & Tunneling Attacks



FX Phenoelit

nruns...

BlackHat Briefings, November 21 2001, Amsterdam

Session Overview

- Introduction
- Layer 2 and 3 attack scenarios
- CDP, STP & IEEE 802.1q
- ARP attacks & ICMP abuse
- Discovering & attacking IGPs
  - RIP, IGRP, EIGRP and OSPF
- Attacking tunnels
- GRE intrusion & RFC-1918 hacking

FX Phenoelit

Trends

CERT® Coordination Center

„Trends in Denial of Service Attack Technology“

> Of extreme concern is the potential of routers being used for DoS attacks based on direct attacks against the routing protocols that interconnect the networks comprising the Internet. We believe this to be an eminent and real threat with a potentially high impact. Routing protocol attacks are being actively discussed in some intruder circles and have become agenda items at public conferences such as DefCon and Black Hat Briefings.

http://www.cert.org/archive/pdf/DoS_trends.pdf

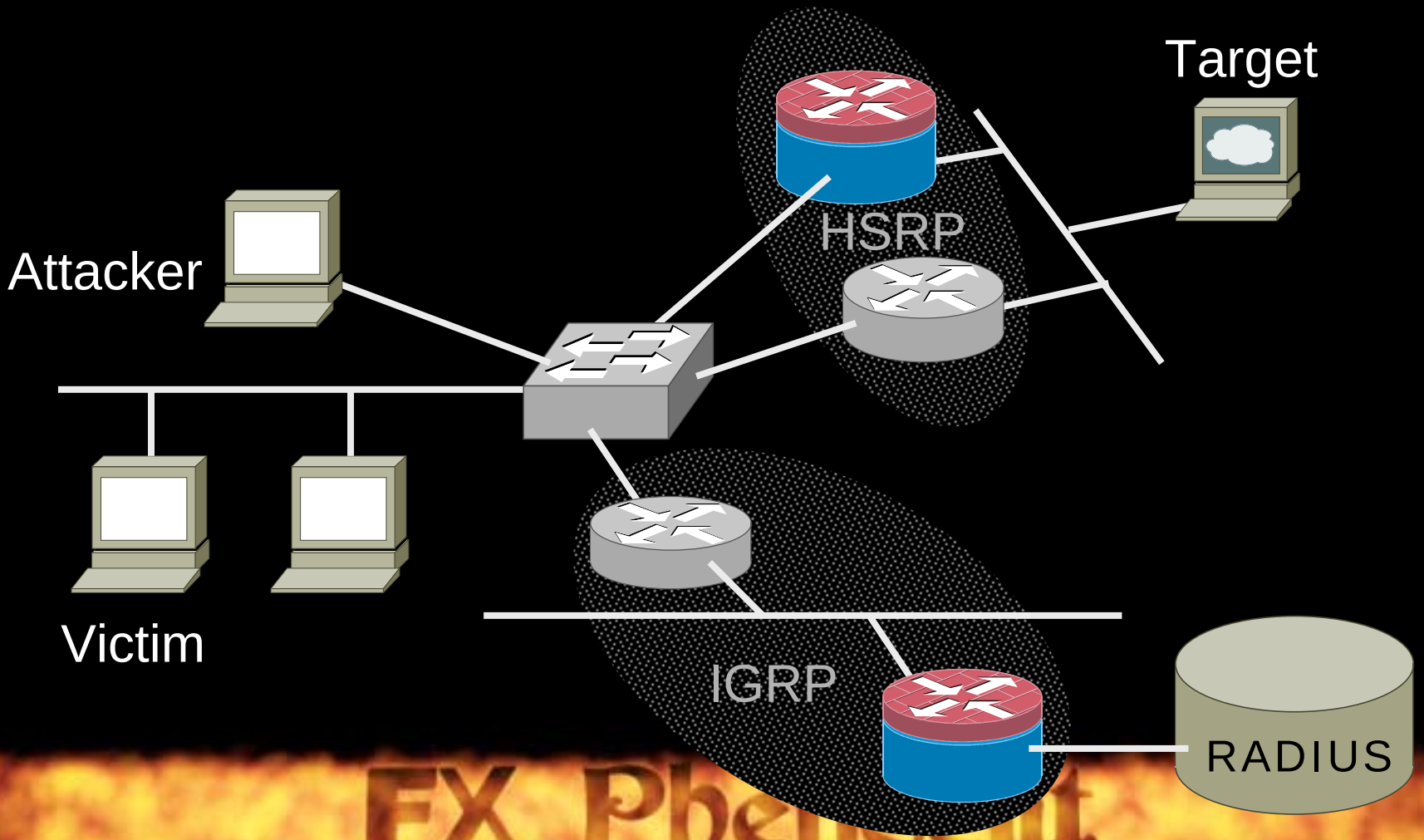
Infrastructure at Risk

What threats are you facing?

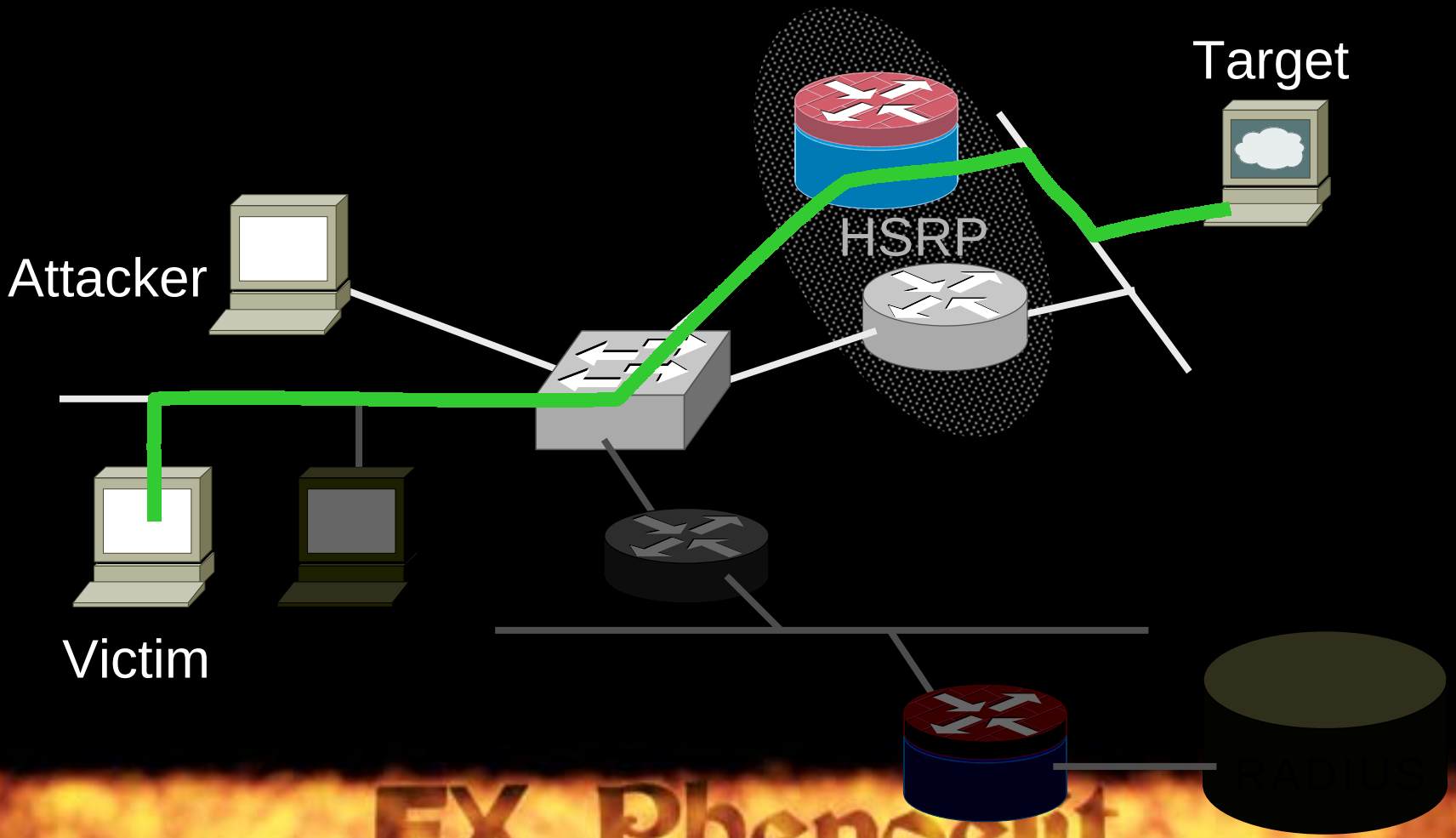
- Sniffing vital information from the network
- Preventing vital information from getting to it‘s destination
- Modifying information on the way from source to destination
- Impersonating source or destination and hereby giving a false sense of security

FX Phenoelit

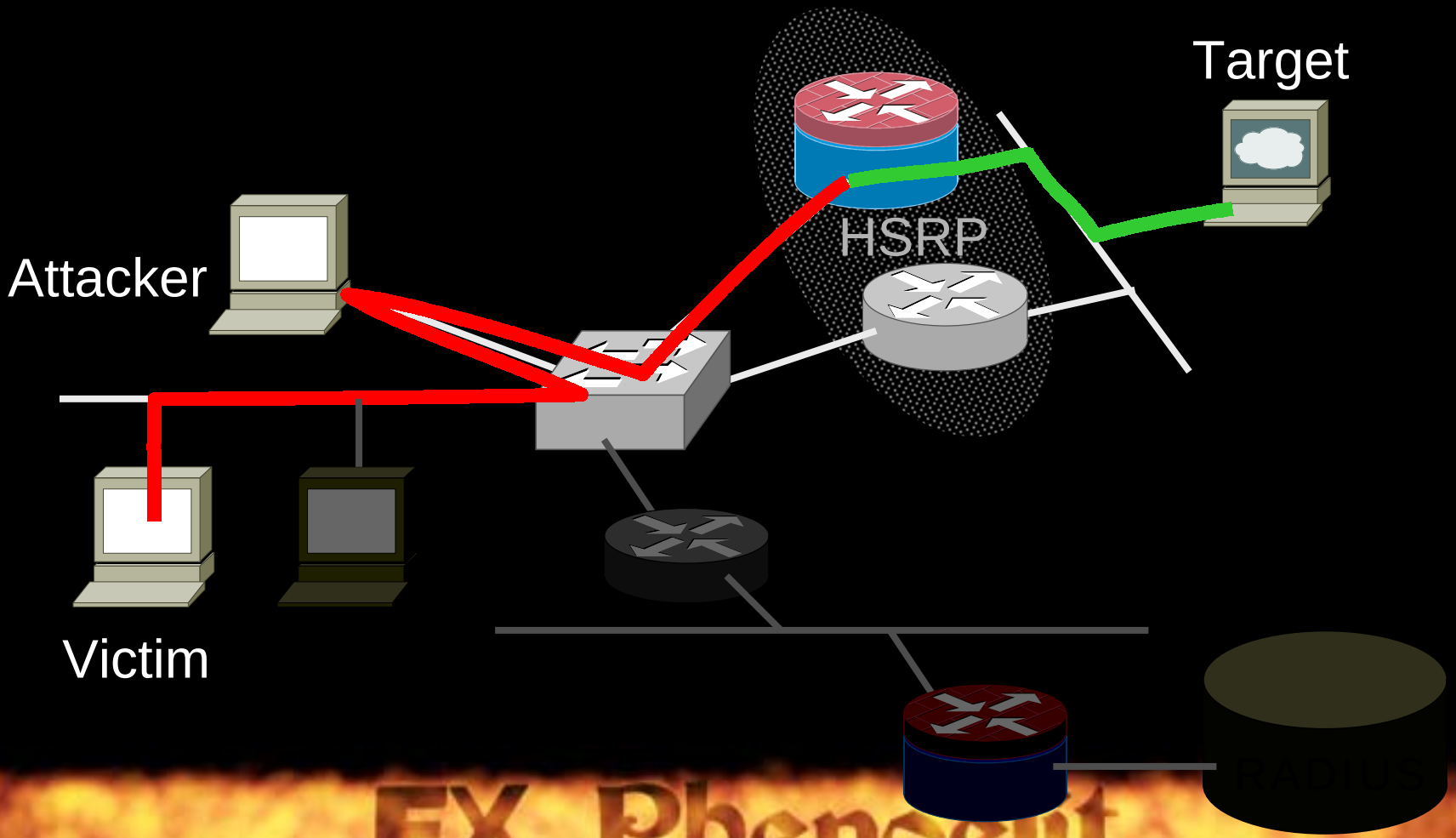
Attack Scenarios [0]
The Network



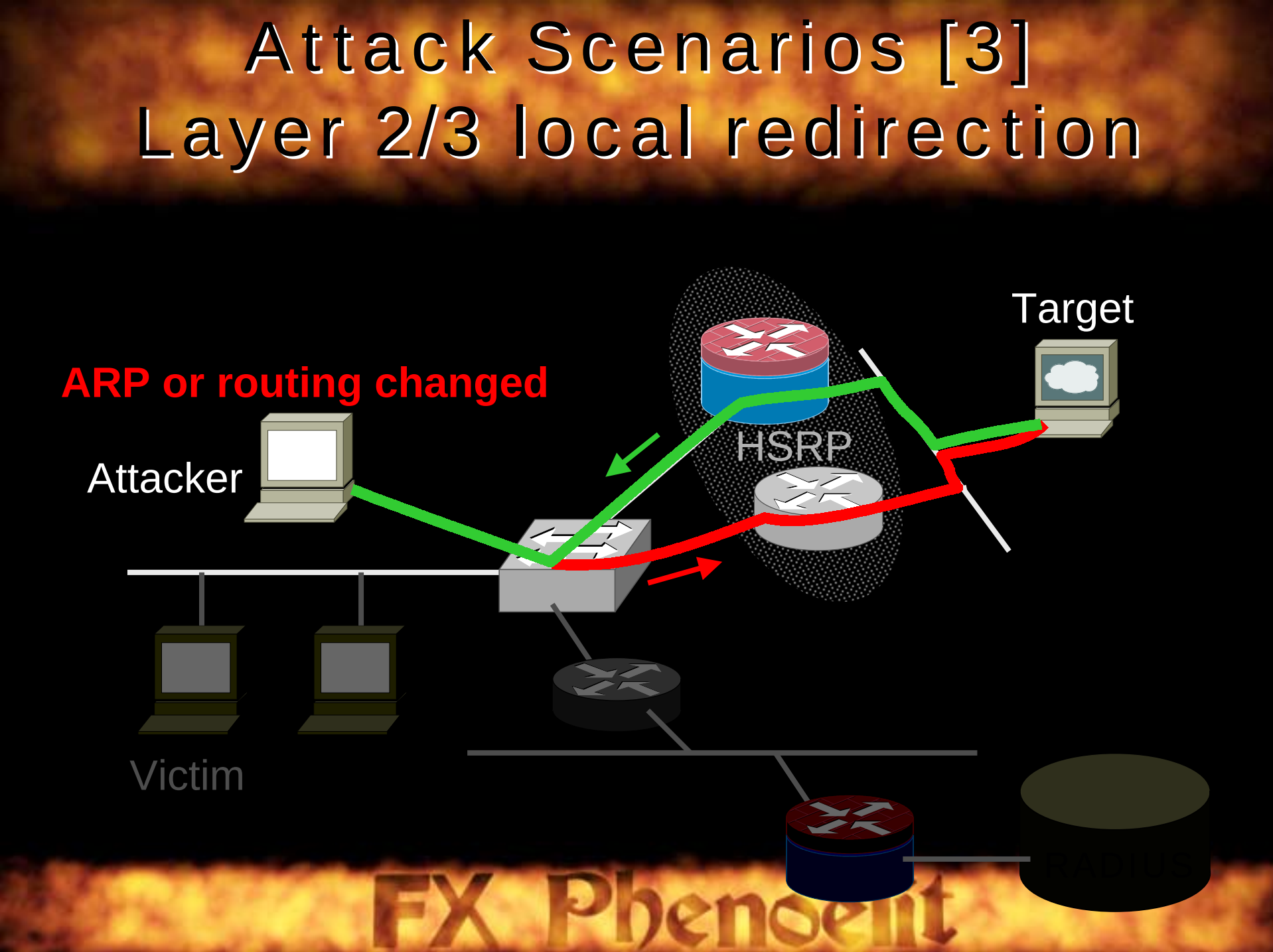
Attack Scenarios [1]
A normal traffic path



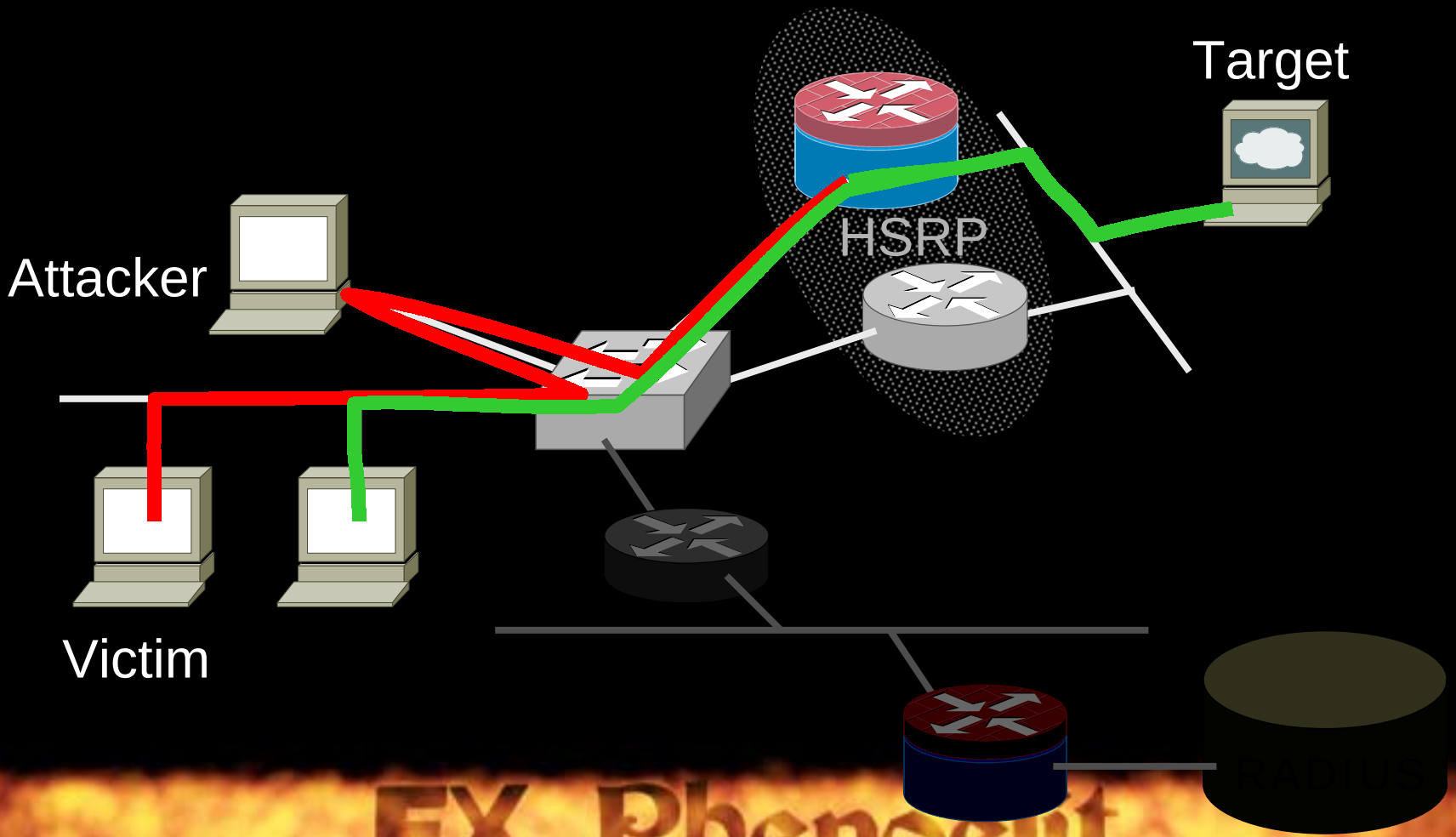
Attack Scenarios [2]
Layer 2 interception



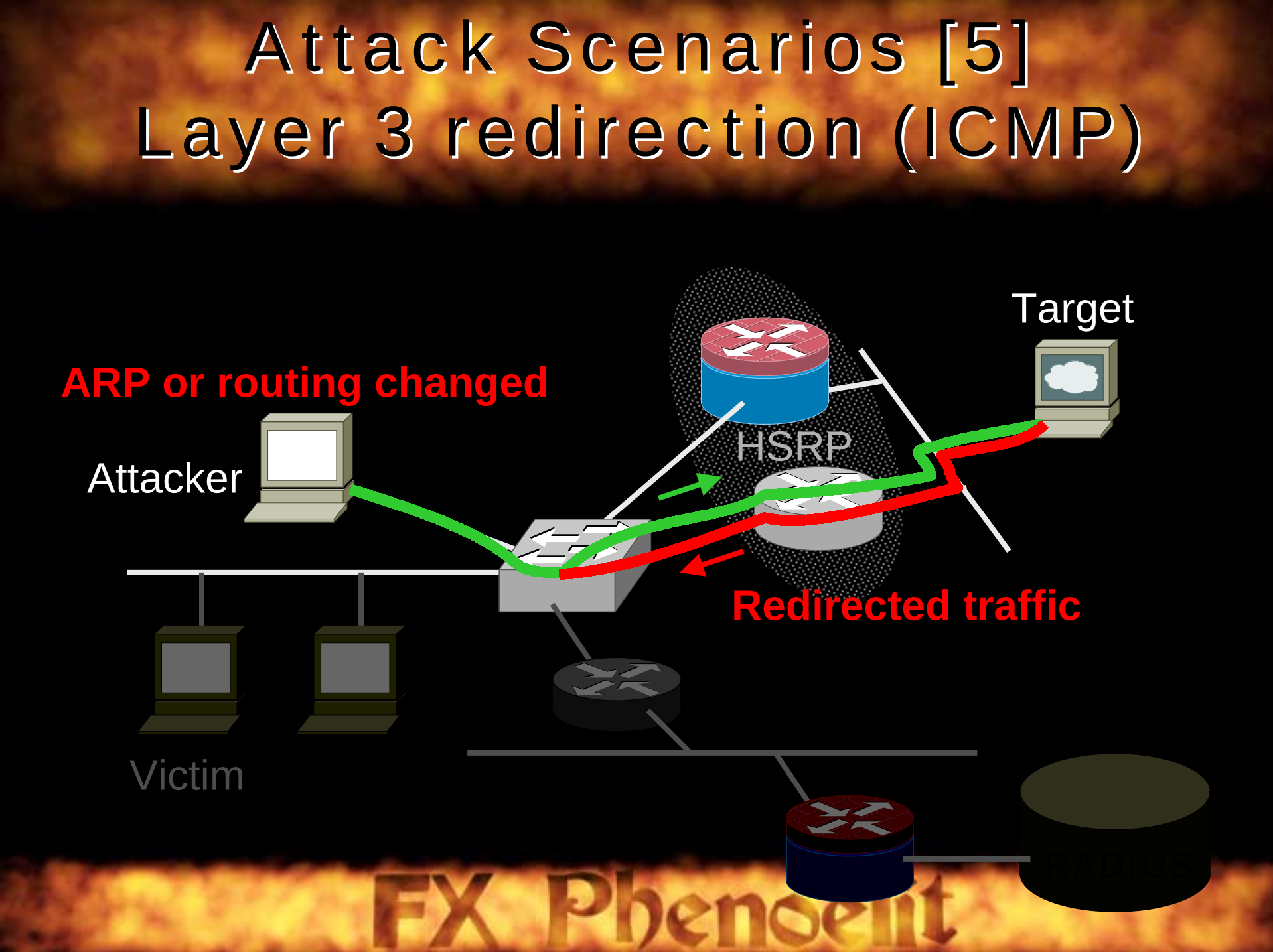
Attack Scenarios [3]
Layer 2/3 local redirection



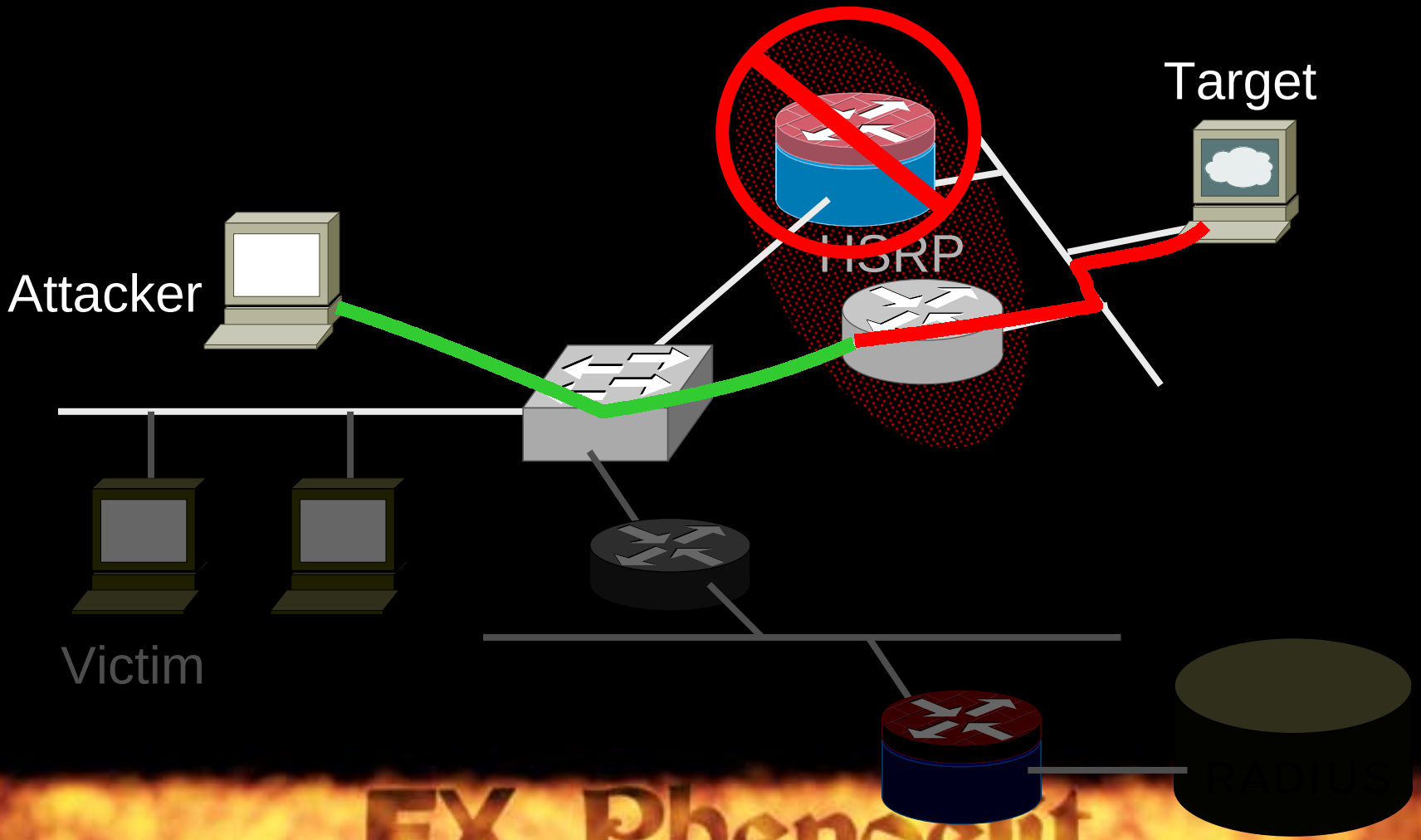
Attack Scenarios [4]
Layer 3 IRDP insertion



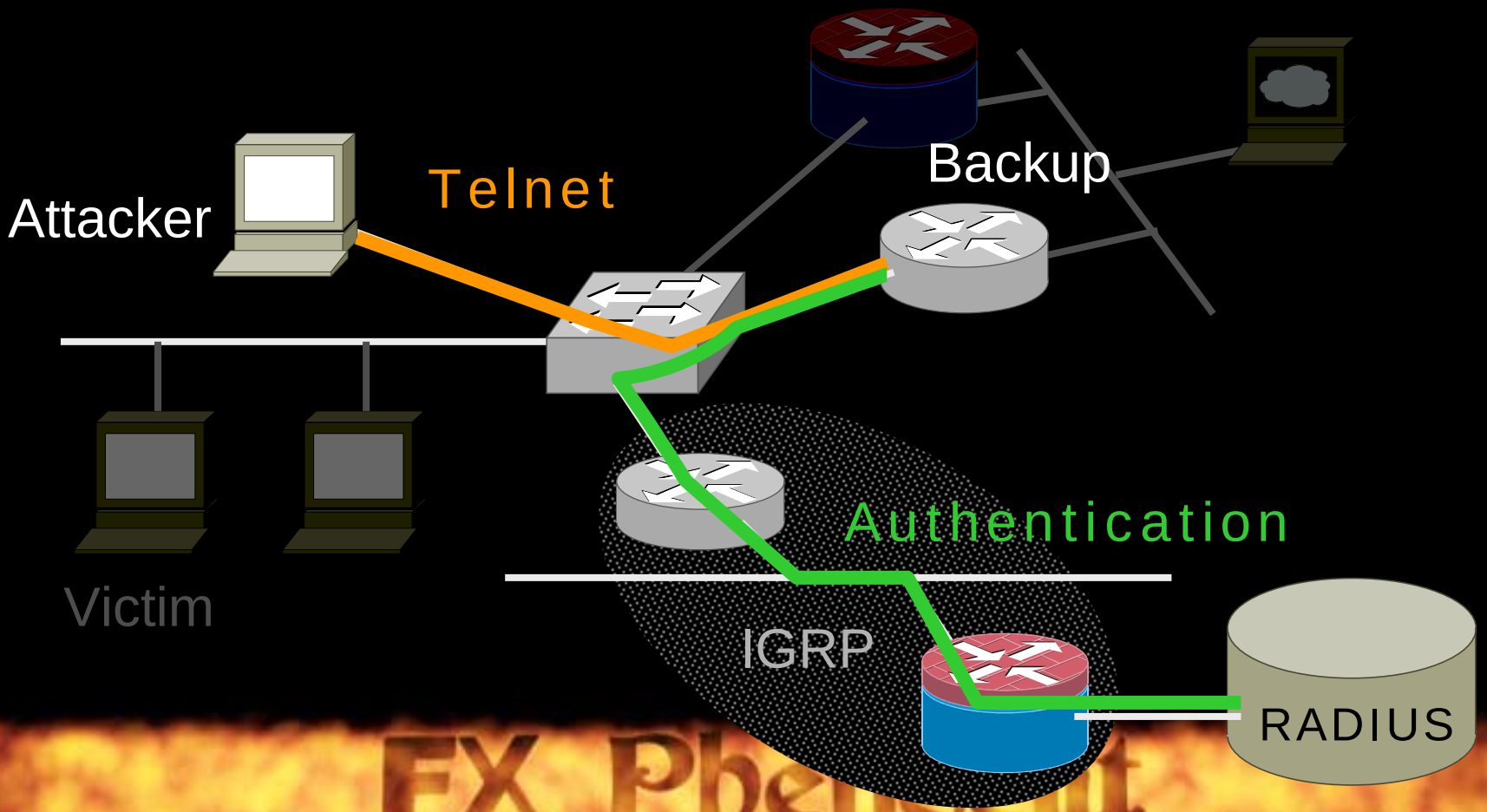
Attack Scenarios [5]
Layer 3 redirection (ICMP)



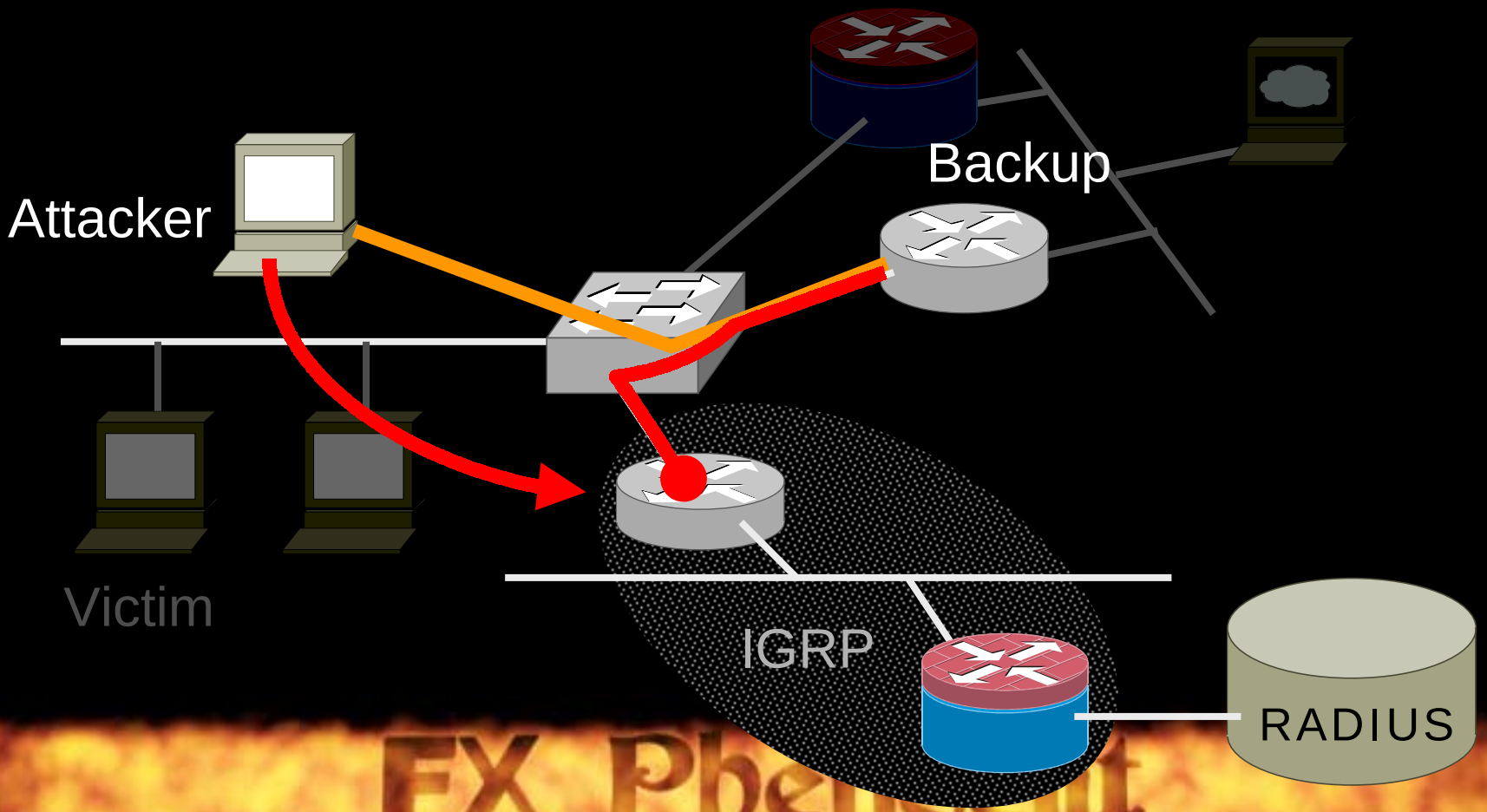
Attack Scenarios [6]
HSRP switchover & takeover



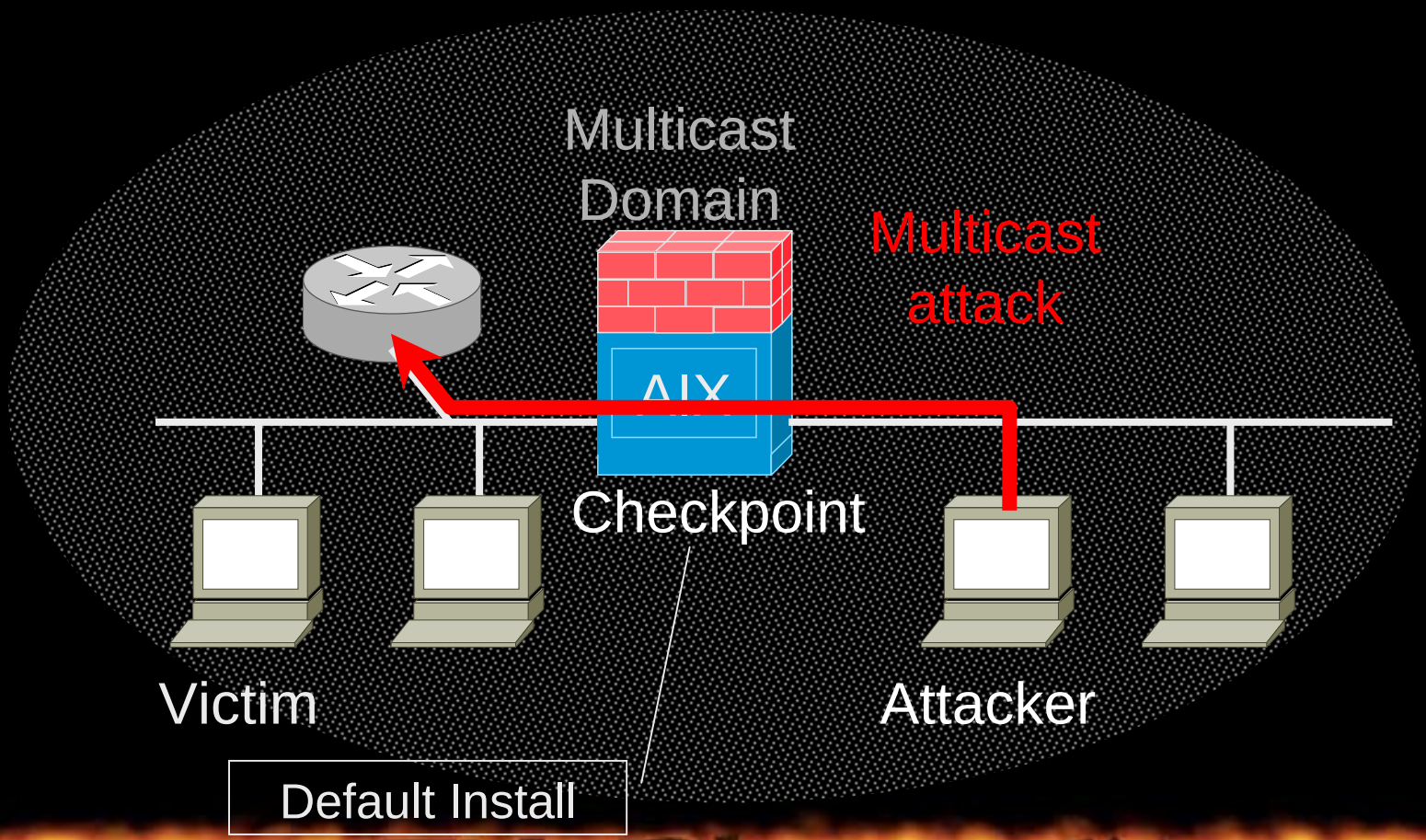
Attack Scenarios [7]
Another normal traffic path



Attack Scenarios [8]
IGRP Routing attack

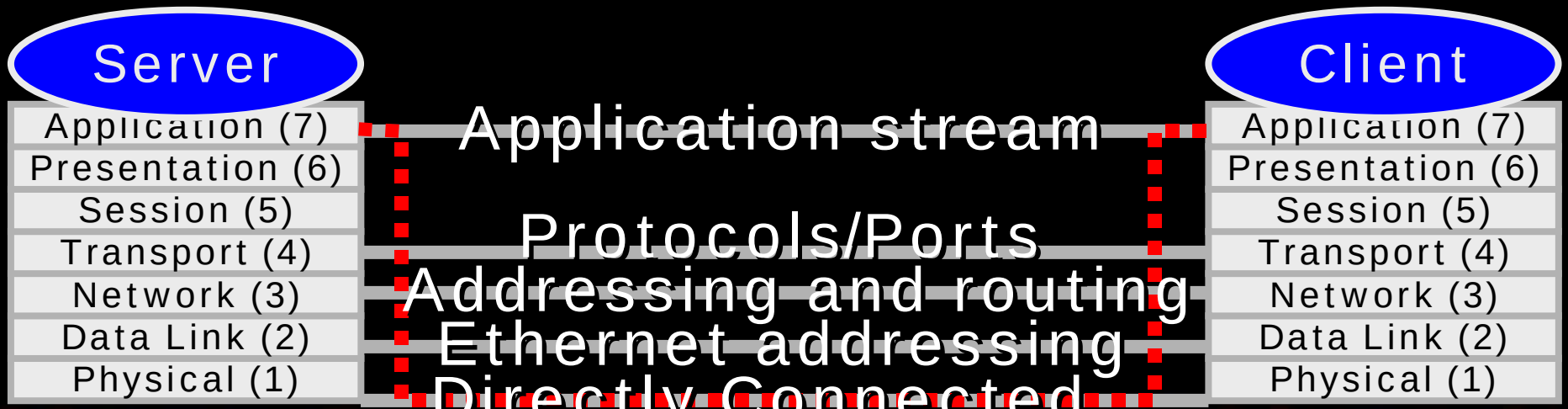


Attack Scenarios [9]
The beauty of multicast



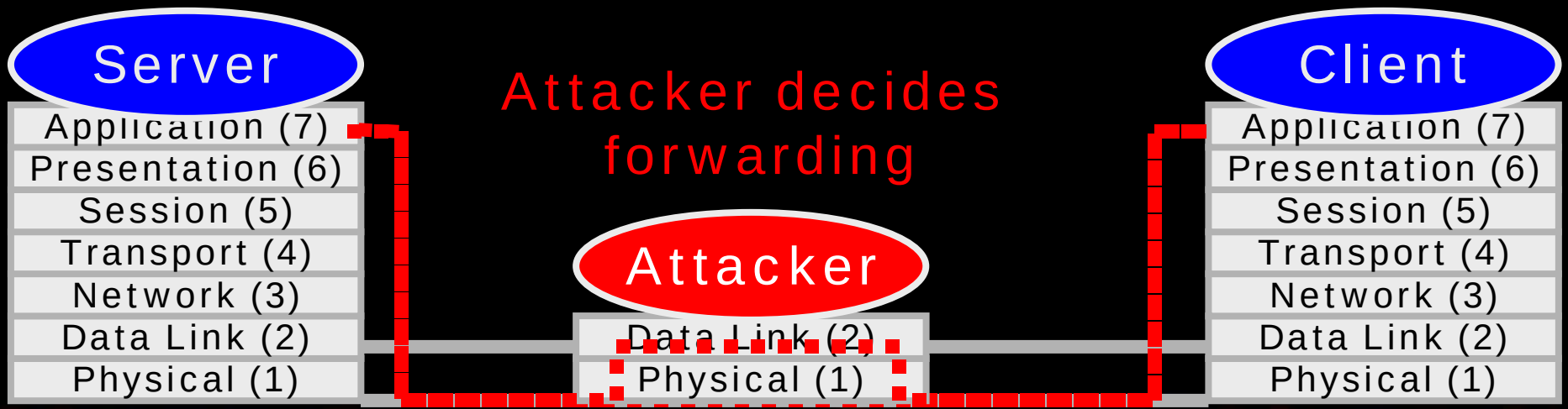
How do these attacks work in general?

- Normal communication goes down the OSI layers
- All attacks on Layer 2 and Layer 3 work on
  - Modification of the **addressing**
  - Therefore modification of the **traffic path**



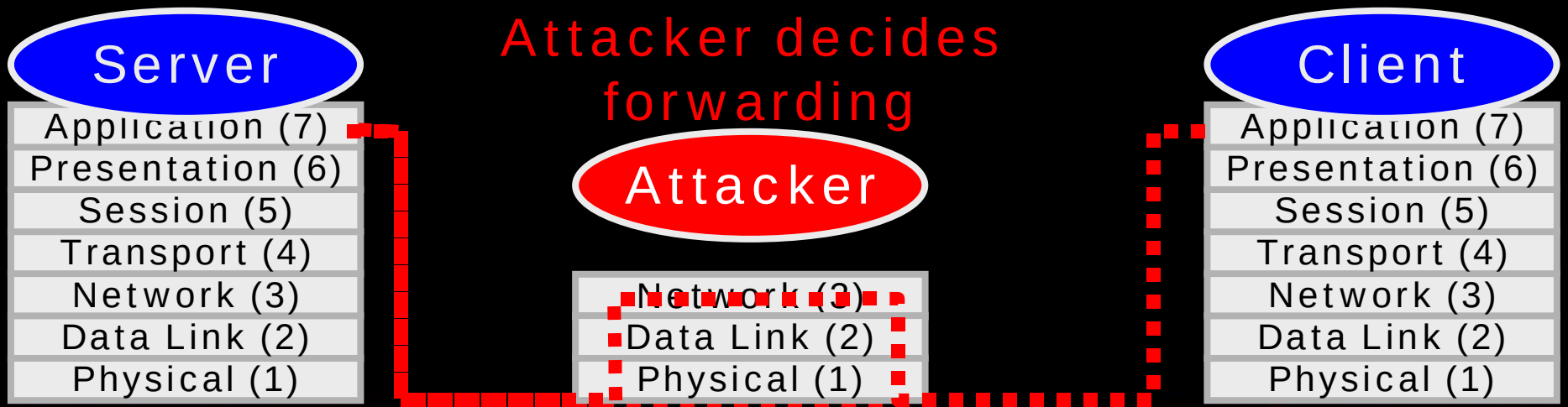
Layer 2 Attack

- Man in the middle attack
- Intercepting traffic by giving false data link address information to both parties
- Layer 3 remains untouched
- Most effective way is ARP interception



Layer 3 Attack

- Man in the middle or remote attack
- Intercepting traffic by giving false next hop information to one or both parties
- Works from remote segments
- There are various methods of applications

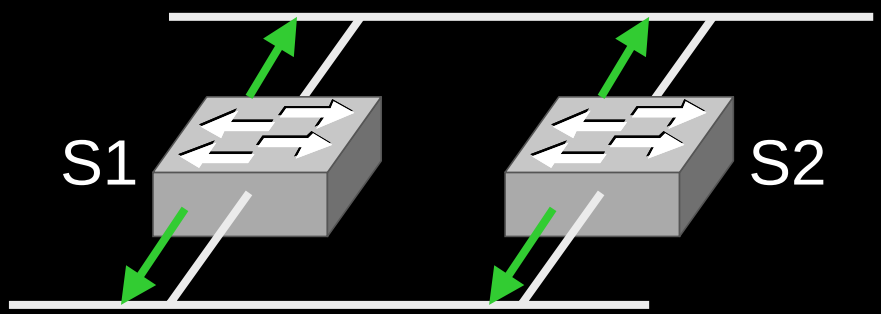


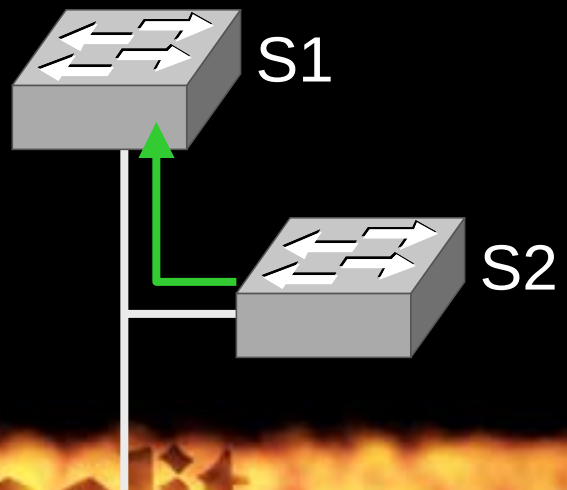
Cisco Discovery Protocol (CDP)

- Cisco proprietary data link layer protocol
- Used for discovery purposes
- Contains valuable information about the router or switch
  - IP address
  - Software Version
  - Platform
  - Capabilities
  - Native VLAN ...
- Can be used for Denial of Service attacks

Spanning Tree (STP)

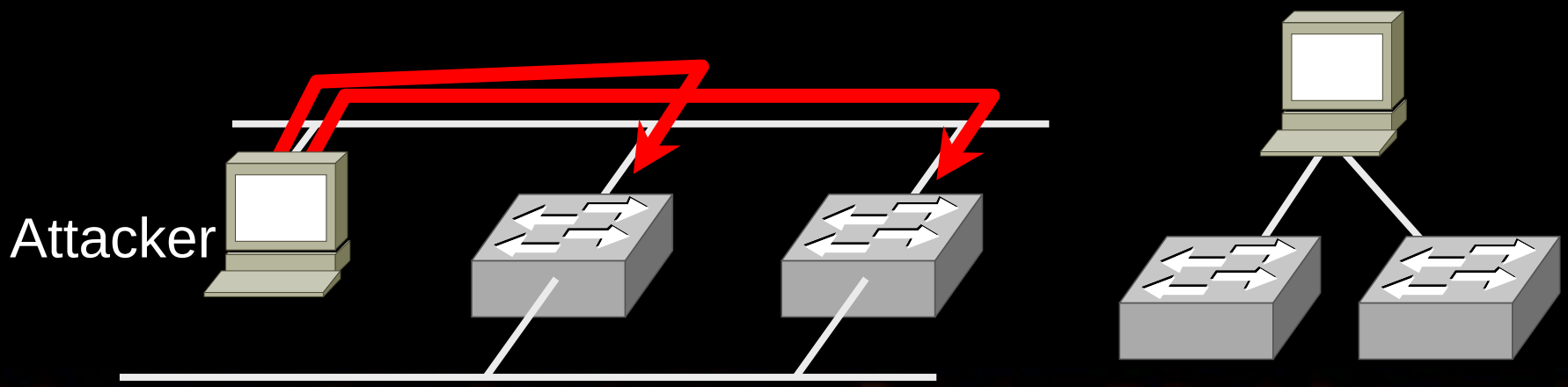
- Provides path calculation for flat earth networks
- Sends out periodic BPDUs (bridge protocol data units) approximately every 4 seconds
- Switch with the lowest priority value becomes root and frames will be forwarded through it





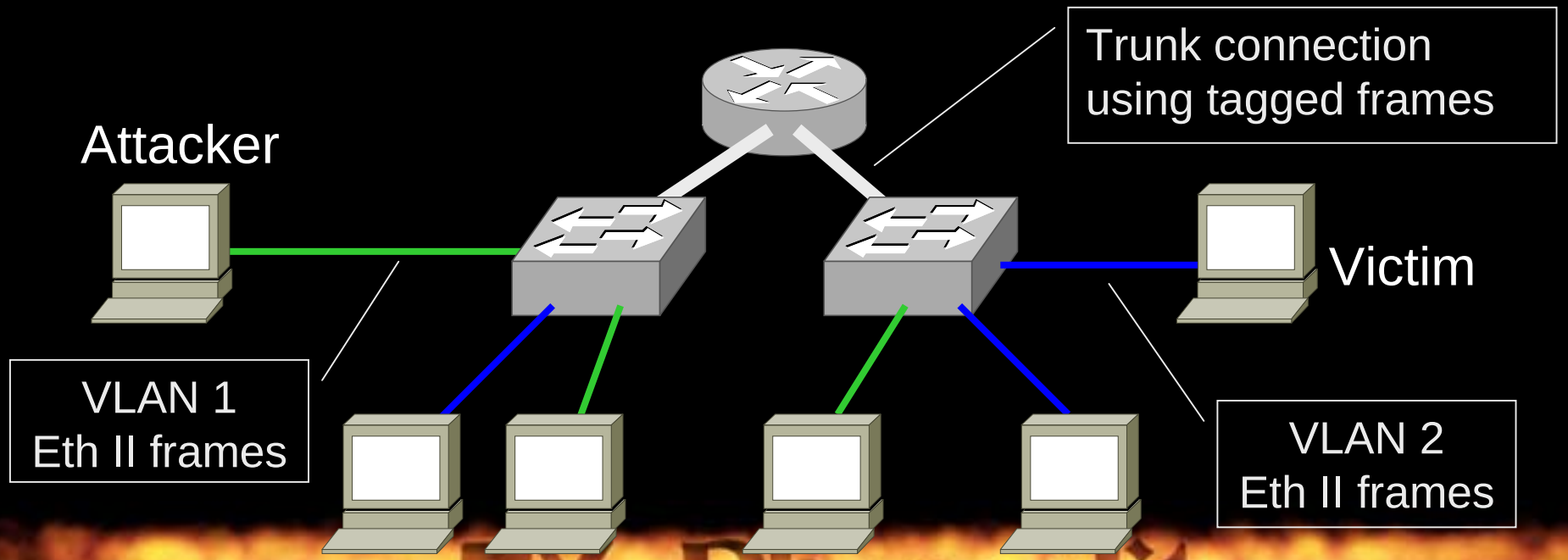
Spanning Tree (STP) attack

- Different BPDUs send out to switches all the time forces spanning tree recalculation
- BPDUs with Attacker as best root switch may result in attacker getting all traffic (attacker becomes tree root)



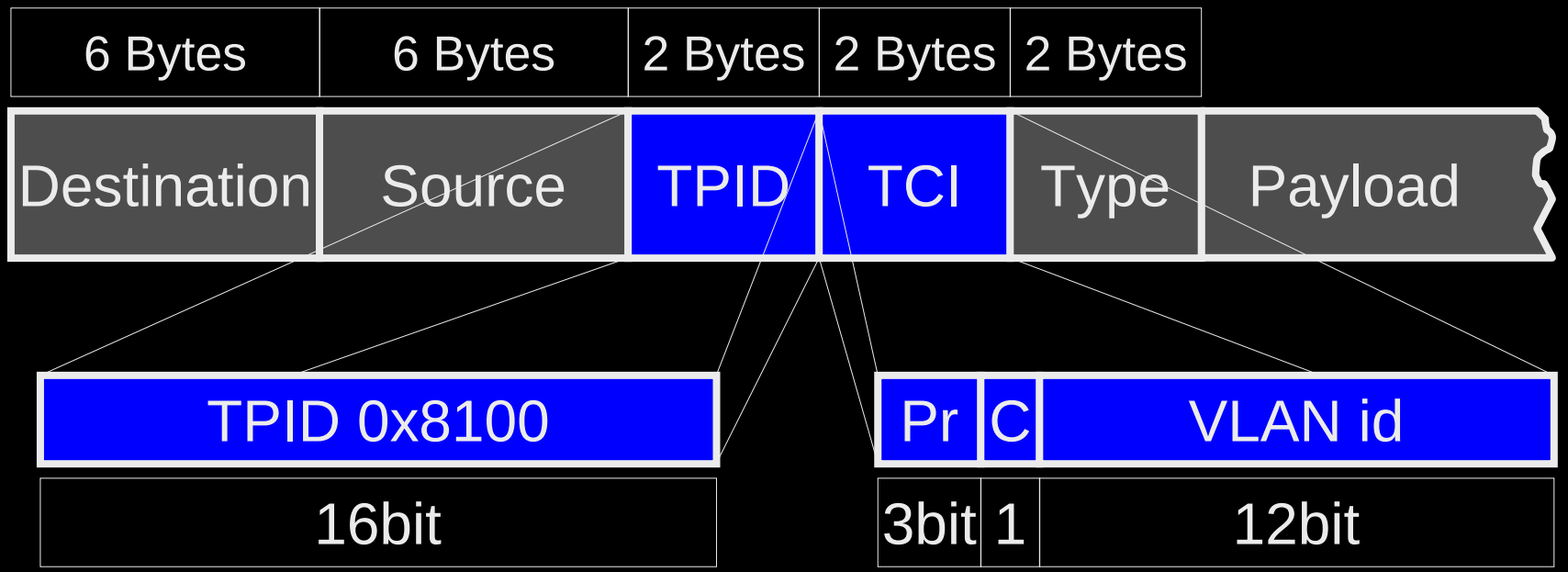
IEEE 802.1q VLAN trunks

- Used to share a VLAN between two switches
- Uses a tag field in frame to identify VLAN
- Trunk transports frames from all „trunked“ VLANs



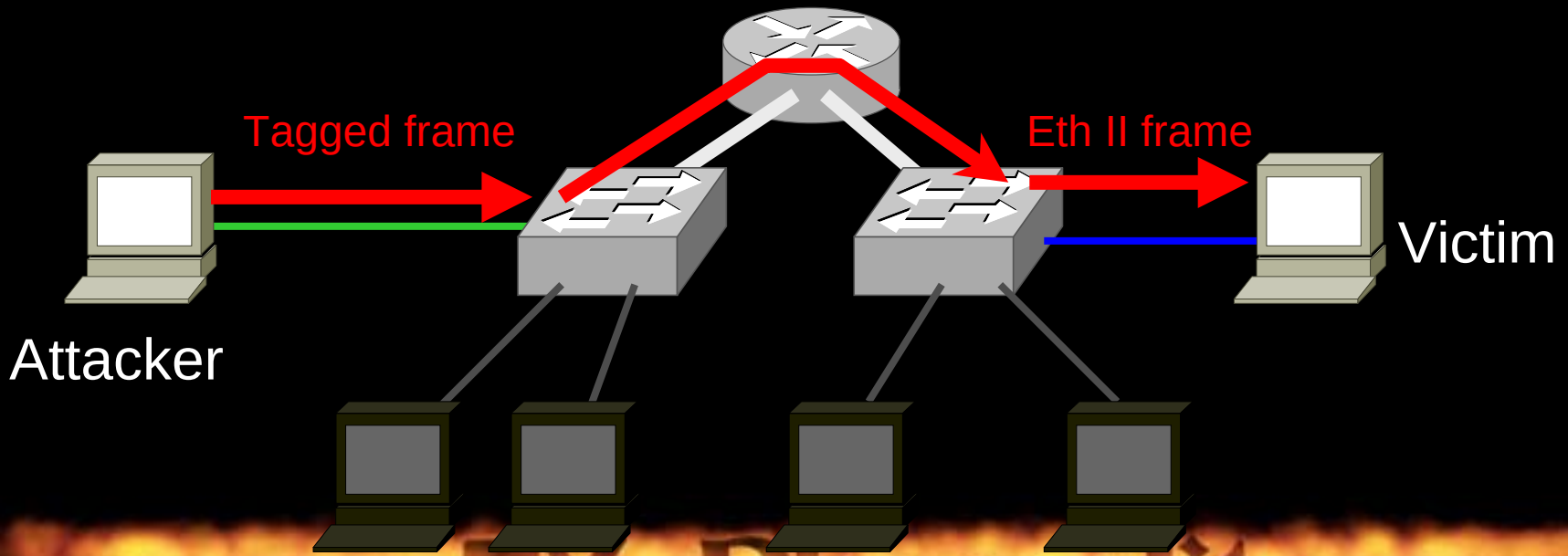
IEEE 802.1q trunk frames

- Frames get „tagged“ for VLAN trunk transport



IEEE 802.1q VLAN hopping

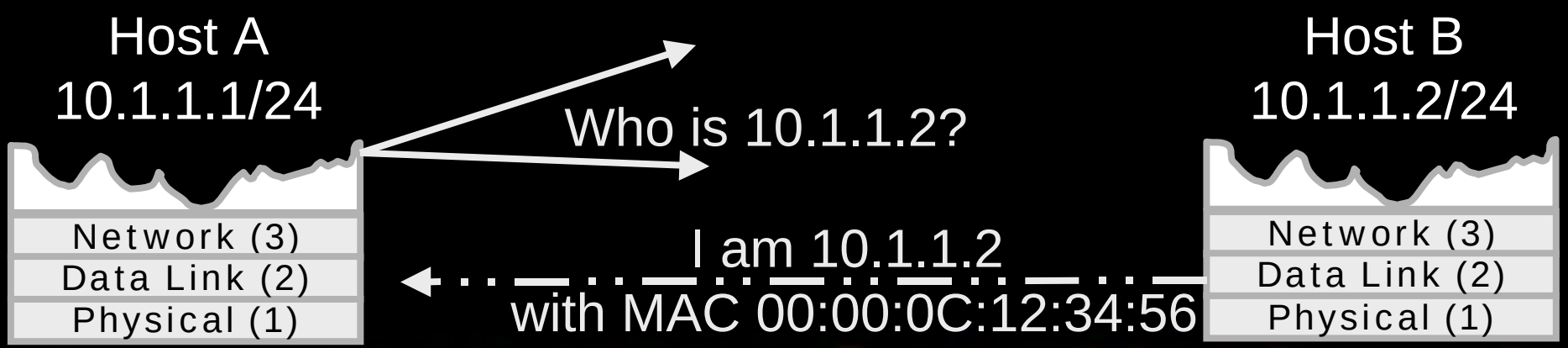
- Attacker sends already tagged frames
- Frames are addressed to Victim‘s MAC
- Tagged frame is forwarded unmodified to trunk port and gets untagged on destination switch



FX Phenoelit

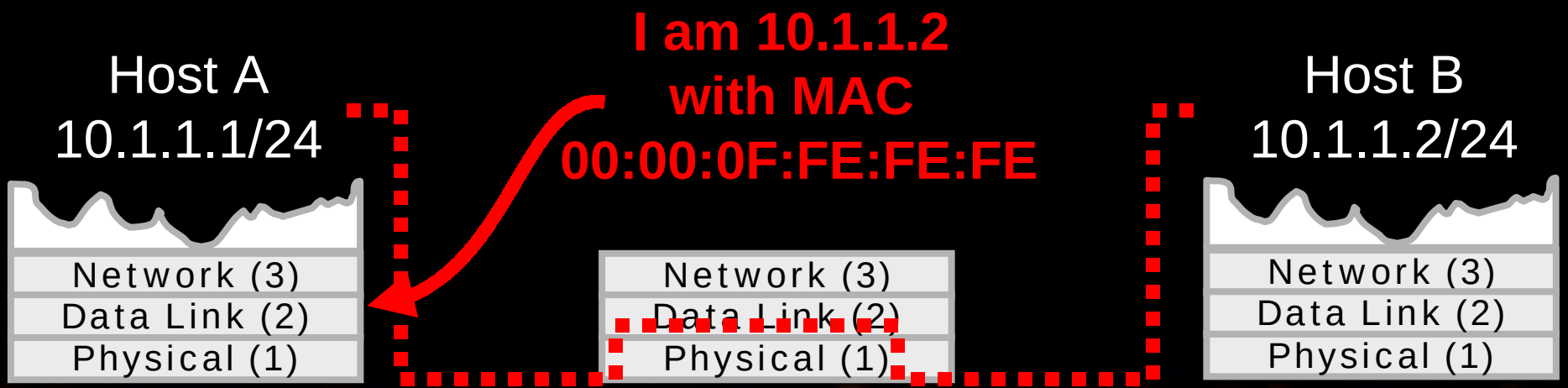
Address Resolution Protocol
ARP (RFC 826)

- IP addresses are resolved into Media Addresses
- If the Media Address is unknown, request it via Broadcast
- First or most recent answer is used to communicate
- Address cache times out on most systems



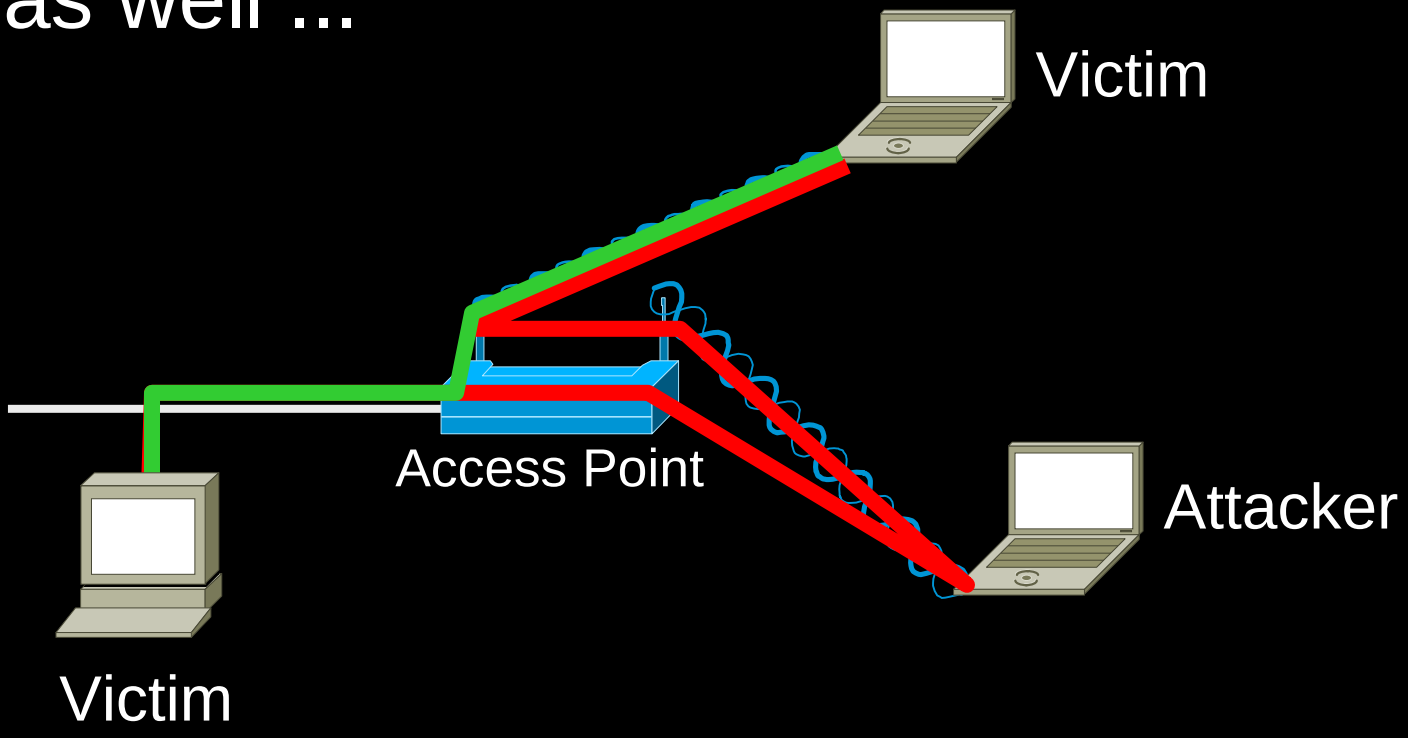
ARP Interception

- Be faster or „more chatty“ than the recipient
- Intercept both directions to prevent direct communication
- Invisible for Layer 3 integrity checks
- Requires bridging/routing (Tool or OS)
- Can be used to insert packets or prevent traffic



Wireless ARP Attack

- The attack works on IEEE 802.11 networks as well ...

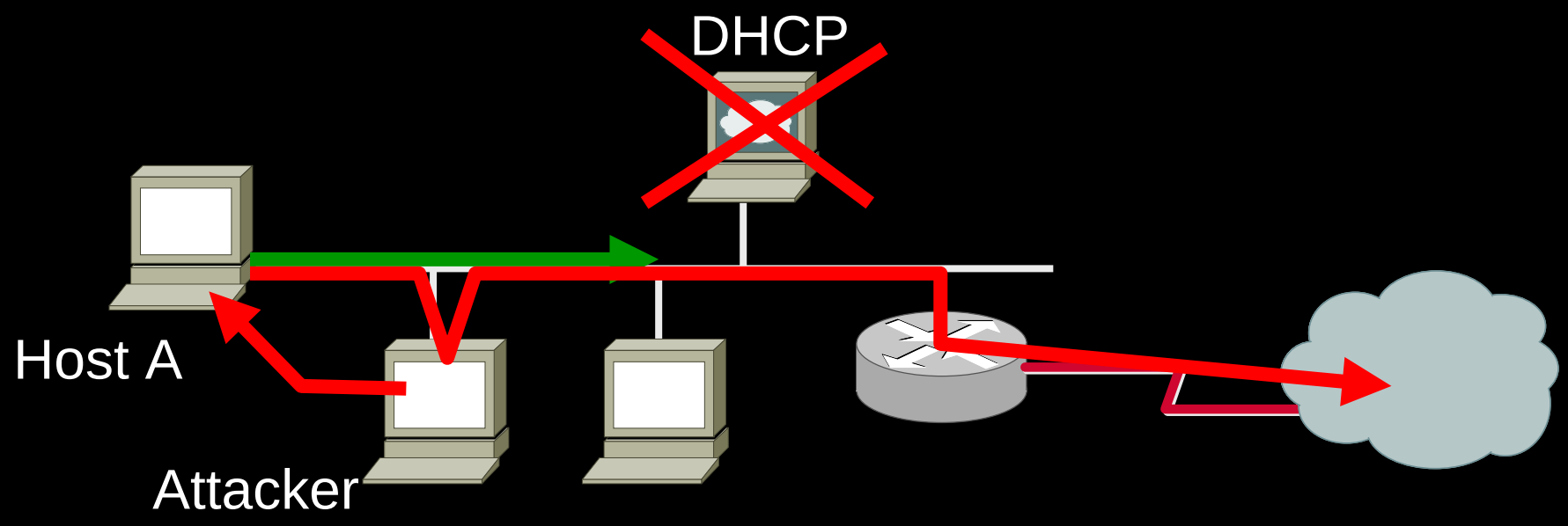


ARP Attack Risks

- Risks
  - Sniffing in switched network environments
  - Can modify packet content on frame level
  - Can prevent traffic from passing
  - Can be used to reroute traffic in a segment
- Requirements
  - Requires attacker to have access to the Ethernet broadcast domain
  - Normally requires attacker‘s interface to be in promiscuous mode

DHCP replaces ARP attacks

- Attacker runs exhaustion attack on DHCP server
- Clients are supplied with evil DHCP config



Discovering Routers

- Routers can be discovered passively by
  - Listening for Multicast emissions (HELLO and Updates)
  - Listening for Router advertisements, redirects and CDP
- Routers can be discovered actively by
  - Querying Routing processes (AS scanning)
  - Router Solicitations
  - OS Fingerprinting
  - Protocol scans
  - Port scans
  - Taking over management systems

Router Discovery Tools

- Autonomous System Scanner (ASS) can be used for active or passive detection
- Ethereal can decode most routing protocols
- ntop can be used to discover central traffic points
- tcpdump‘s -e option shows data link addresses
- Fyodor‘s nmap and Phenoelit‘s protos scan for IP protocols
- DHCP queries reveal router addresses
- NMS database contains router information (HPOV)

ICMP Router Discovery Protocol (IRDP – RFC 1256)

- ICMP Router Discovery Protocol enabled router sends out periodic updates as broadcast
- IRDP requests (called Router Solicitations) are send as broadcast by Hosts that look for a default gateway
- Announcing Router is inserted in Host routing table
  - Metric is higher then the static default for normal routers
  - Metric is lower then anything else
  - Metric depends on „preference“ value of the updates

IRDP Attacks

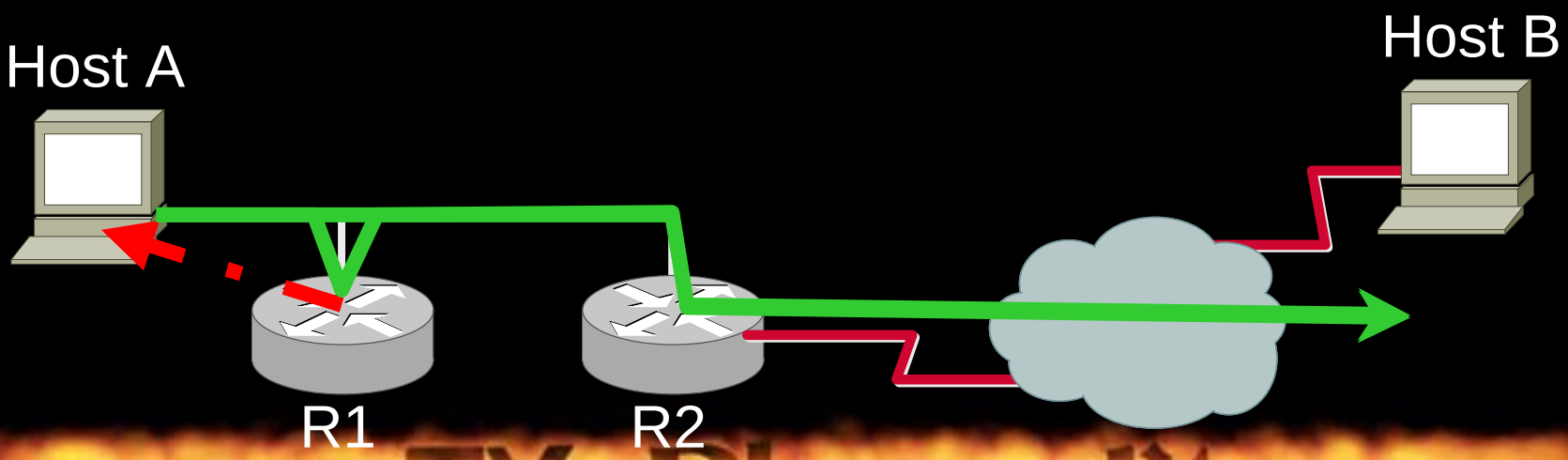
- Attacker sends IRDP updates
- Attacker then makes the default gateway temporary unavailable
  - CDP overflow attacks (Router reboot)
  - Temporary ARP interception
  - Dial on demand routers
- Attacker is now the default router

IRDP Attacks

- Can be used targeted (unicast) or wide (broadcast)
- Lifetime of a route max **18h:12min:15sec**
- Windows 9x
  - does IRDP **all the time**
  - can be forced to use the attacker‘s router by using preference 1000 in the answer and sending an ICMP host unreachable message
- Windows NT4 performs IRDP during boot
- Windows 2000 and Linux don't care

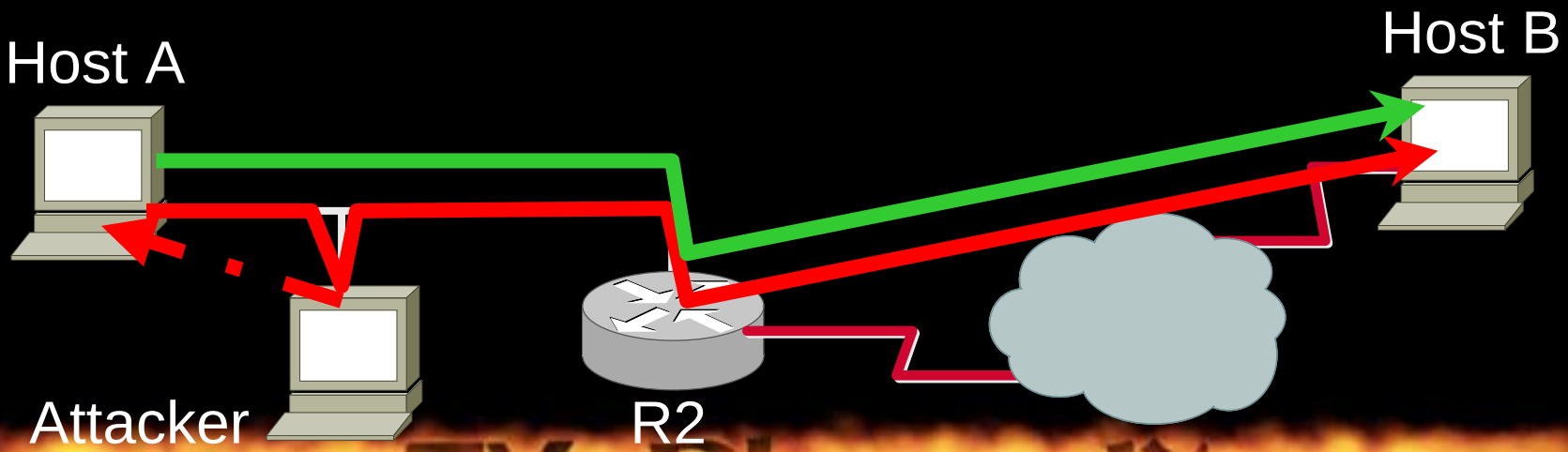
ICMP Redirects (RFC 792)

- Introduced to make routing more effective
- Packet is send from Host A to B through router R1
- R1 finds next hop R2 on same segment and network
- R1 forwards the packet
- R1 sends ICMP Redirect to A



ICMP Redirect Attack

- Packet is sent from Host A to B through router R2
- Attacker sees traffic (A->B) and sends spoofed ICMP redirect to Host A
- Host A adjusts routing and sends traffic through Attacker
- Normally requires copy of the first 64bits of the packet
- Even works across routers !



FX Phenoelit

ICMP Redirect Host Reactions

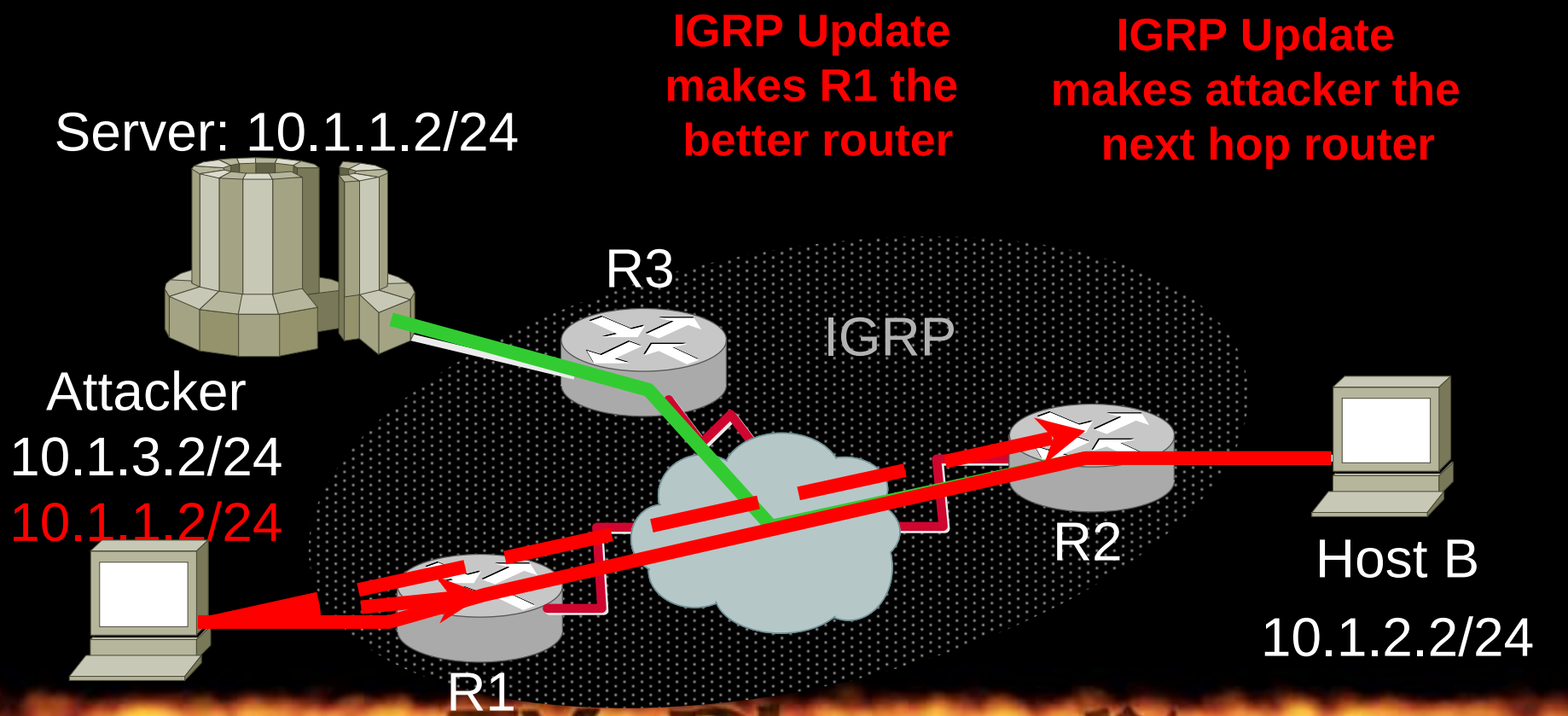
- Windows 9x Hosts
  - Accepts ICMP redirects by default
  - Adds a host route to routing table
- Linux Hosts
  - Accepts ICMP redirects by default in some distributions
  - See /proc/sys/net/ipv4/conf/*/accept_redirects
    Does not show redirects in routing table
- Tools:
  - IRPAS icmp_redirect
  - icmp_redir from Yuri Volobuev

Interior Gateway Routing Protocol (IGRP)

- Cisco proprietary protocol
- 2^{16}-1 = 65535 possible autonomous systems
- No authentication
- Delay, bandwidth, reliability, load and hop count used to calculate metric
- Passive or silent hosts possible (protocol scan)
- Spoofed updates have better metric then real links
- Requires spoofed source network to be enabled

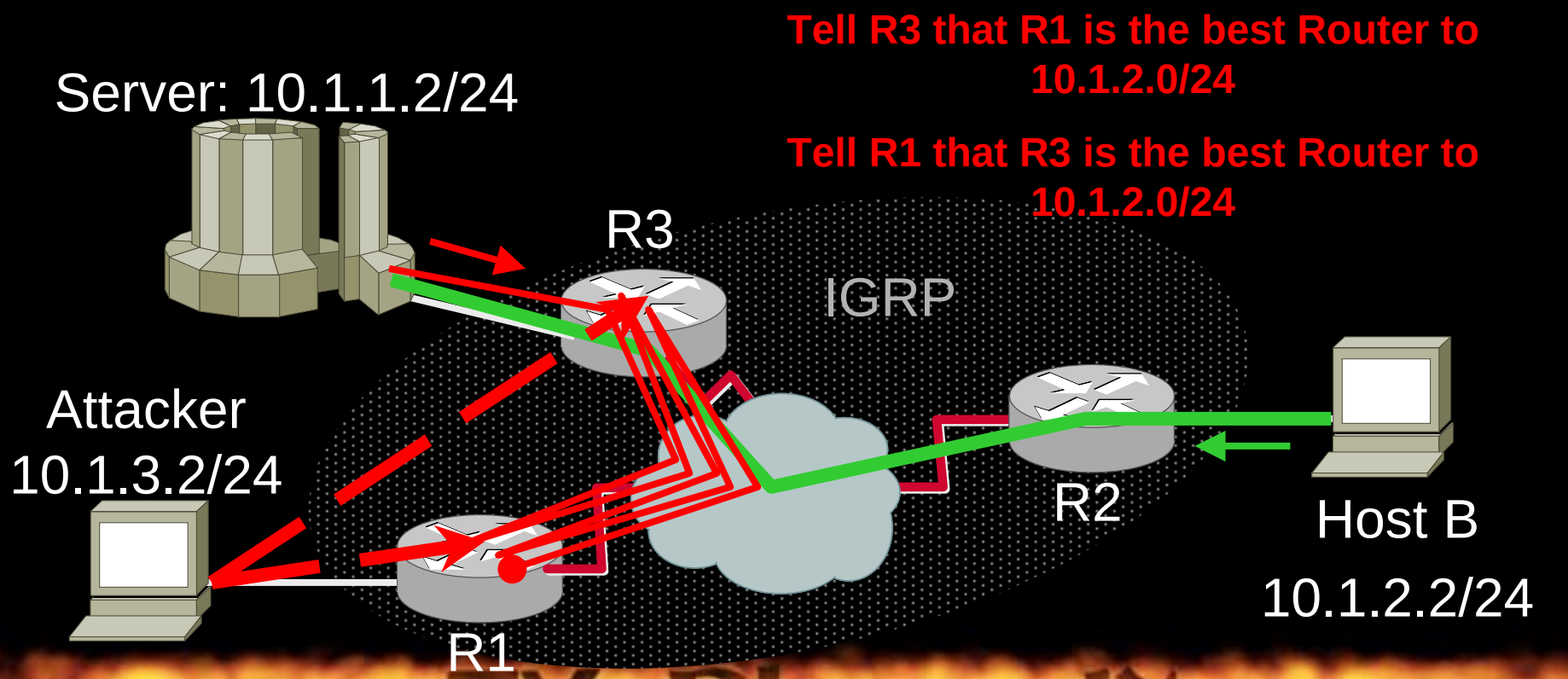
IGRP Attacks

Introducing new routes or modifying routes



IGRP Attacks

Creating routing loops



Routing Information Protocol (RFC 1058, 2453)

- RIP v1 (RFC 1058)
  - Uses fixed subnet/netmask size by class
  - No autonomous systems
  - Runs on UDP port 520
  - Broadcast or unicast traffic
- RIP v2 (RFC 2453)
  - Supports variable subnet size
  - Multicast or unicast traffic
  - Clear text authentication defined
  - Cisco supports MD5 authentication (double authentication block forbidden by the RFC)

RIP Attacks

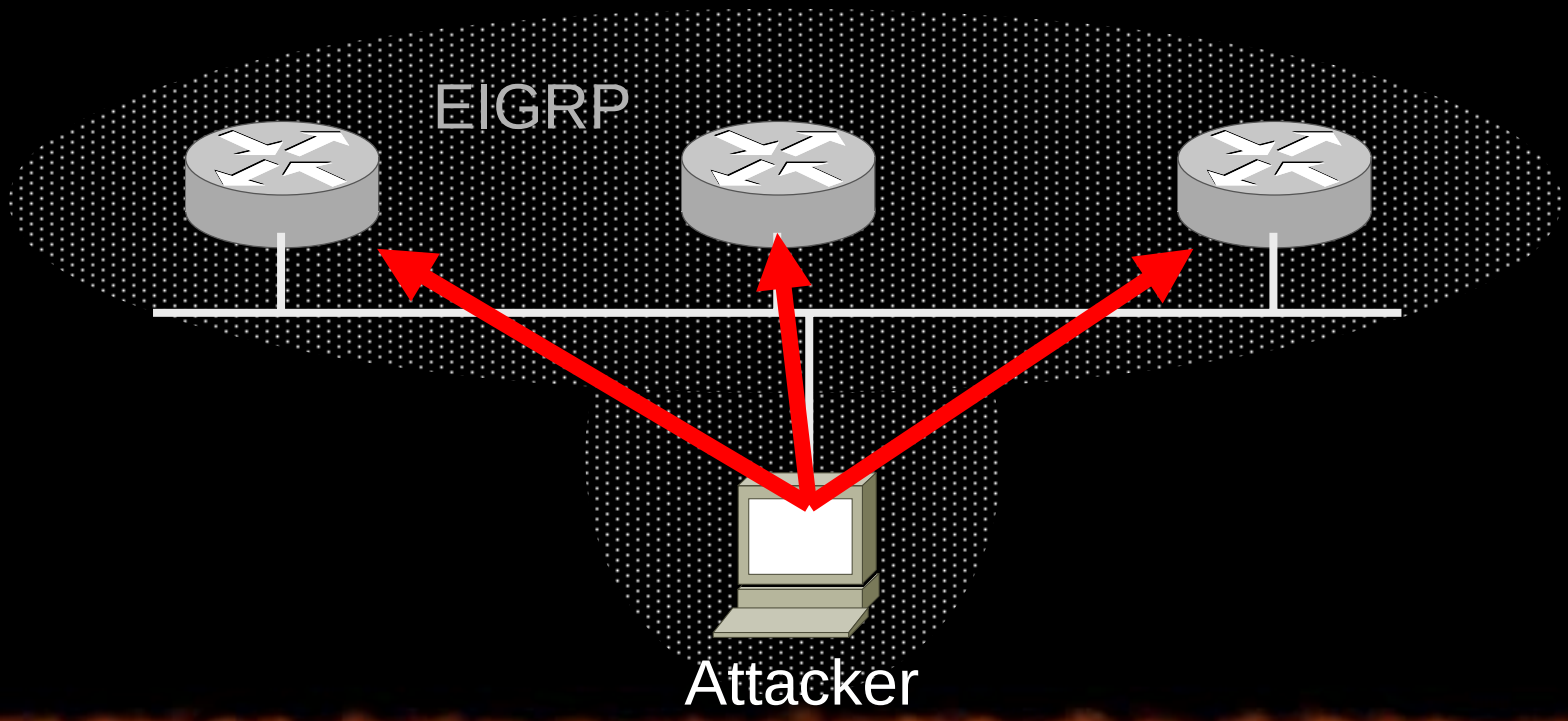
- Same attacks as with IGRP
- Network boundaries are important for RIPv1
- Multicast RIPv2 (224.0.0.9) may be forwarded across segments
- Split Horizon algorithm with poisoned reverse
  - Sends „unreachable“ back to sender of the route (metric 16)
  - May prevent routing loop attacks
  - Protects only if more than 2 routers are in the segment
- Tools:
  - rprobe.c and srip.c from humble
  - Nemesis-rip from Mark Grimes
  - ASS to scan

Enhanced Interior Gateway Routing Protocol (EIGRP)

- Yet another Cisco proprietary protocol
- 2^{32}-1 possible autonomous systems (65535 used)
- No authentication
- Delay, bandwidth, reliability, load and hop count used to calculate metric
- Attacker must become „neighbor“ to exchange routing information with AS
- Requires spoofed source network to be enabled

EIGRP Route Introduction

- Attacker joins as EIGRP neighbor
- Attacker injects new route

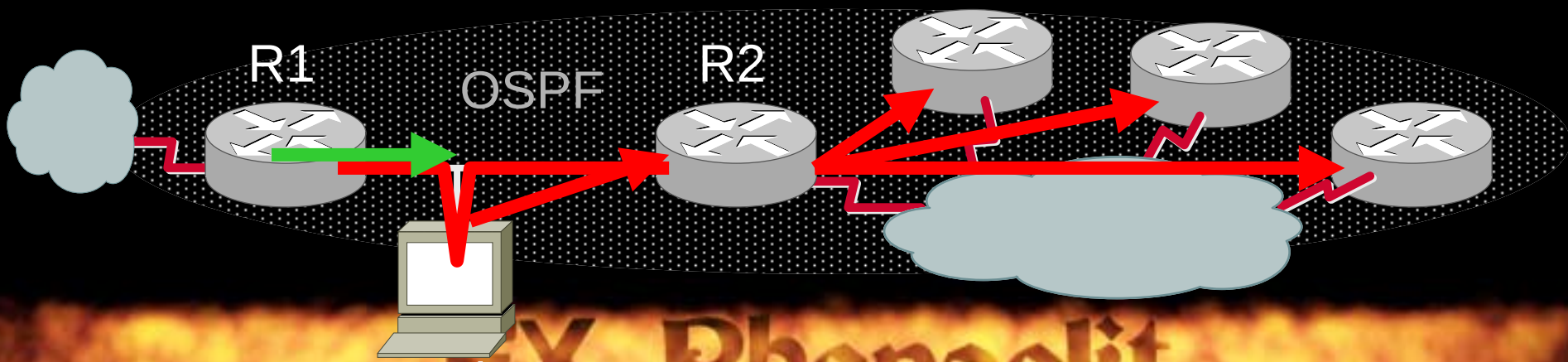


Opens Shortest Path First OSPF (RFC 2328)

- Sends LSA (Link State Advertisements) through the Area
- Uses HELO packets to Multicast (224.0.0.5)
- Every router knows the status of the Area
- No authentication, clear text or md5 defined
- IP Protocol 89 (protocol scan)
- More security features than other routing protocols
- The „hard-to-understand“ factor helps the attacker

OSPF Attacks

- Attacks can become very complex
- Forged LSAs are contested by routers
- For demonstration we use an „extended-Layer 2 attack“
  - Run modified ARP interception software
  - Change OSPF packets while bridging them from R1 to R2
  - Let R2 distribute the false information through the area



Border Gateway Protocol BGP 4 (RFC 1771)

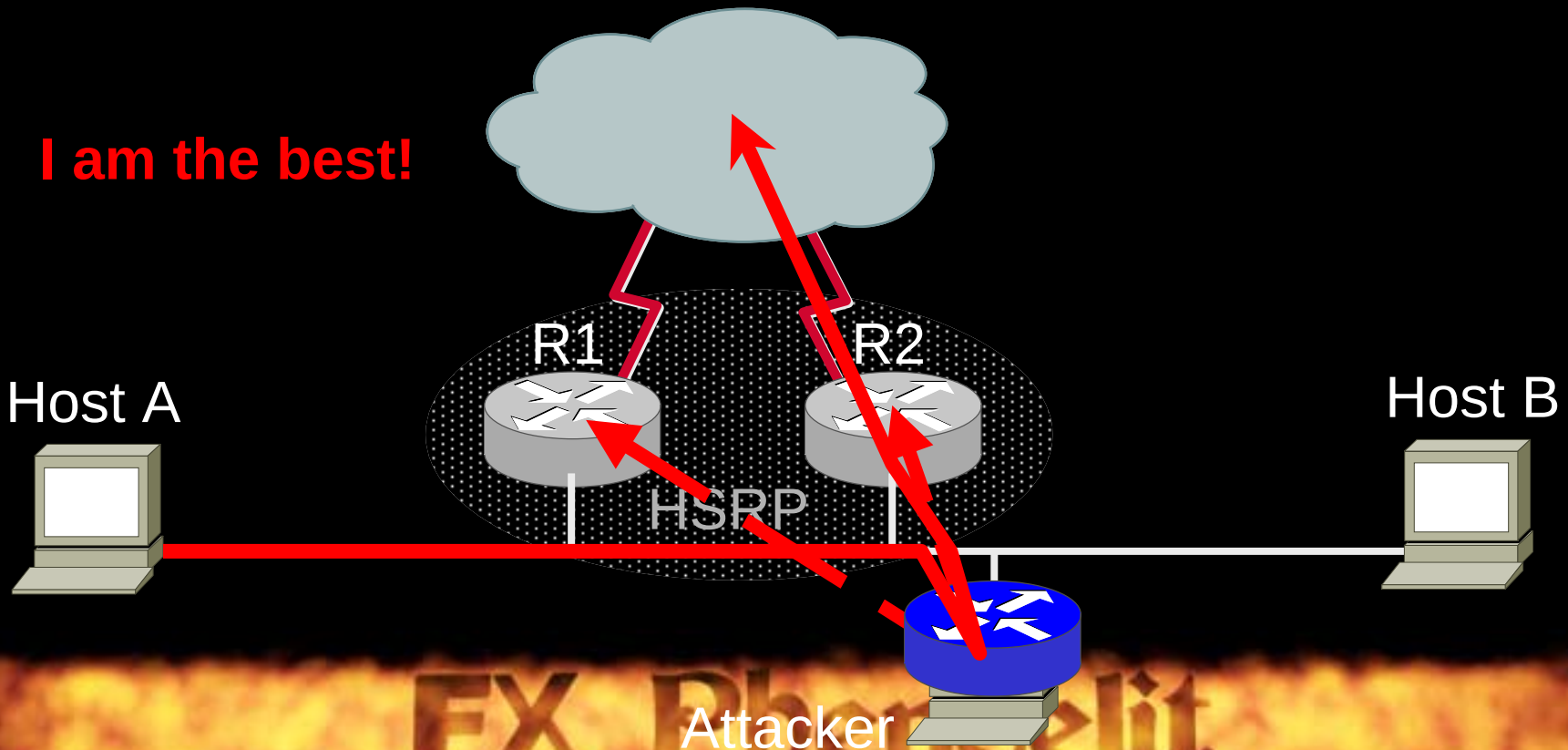
- Exterior Gateway Protocol that connects Autonomous Systems
- Uses TCP Port 179 for communication
- IBGP (interior BGP) needs an IGP or static routes to reach neighbors
- Possible attacks include:
  - Bad updates
  - Abuse of BGP communities
  - TCP Sequence Number and Layer 2 attacks
  - IBGP is a softer target than EBGP

Hot Standby Router Protocol HSRP (RFC 2281)

- Cisco proprietary protocol for high availability
- „Standby“ IP address and MAC address are bound to the active router
- There are one or more inactive routers
- Multicast driven communication, UDP Port 1985
- Authentication is done in clear text
- If active router no longer says „Hello“ ...
  - Inactive routers send out a request to take over
  - Router with the highest priority „wins“ state ACTIVE

HSRP Attacks

- New routers with high priority can take over the „standby“ addresses



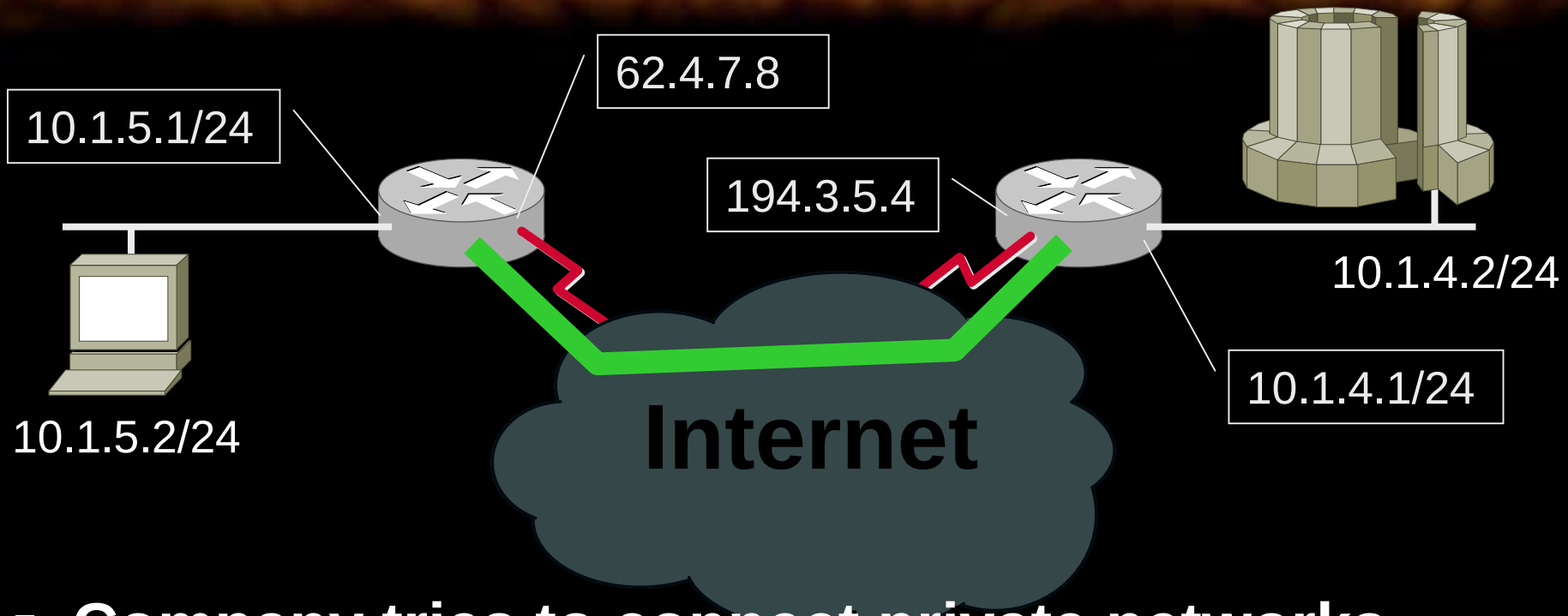
Attacking tunnels

- Theory of unencrypted tunnel attacks:
  - Generate traffic for the inside target network
  - Encapsulate in tunneling protocol
  - Send to tunnel destination router
  - Return path depends on scenario
- Vulnerable protocols:
  - IPX encapsulation (RFC 1234)
  - AX.25 encapsulation (RFC 1226)
  - Internet Encapsulation Protocol (RFC 1241)
  - IPv4 in IPv4 encapsulation (RFC 2003)
  - Generic Routing Encapsulation (RFC 1701, 1702, 2784)

Generic Routing Encapsulation GRE (RFC 1701, 1702, 2784)

- Used to transport protocol A over domain of protocol B in B‘s payload
  - IPv4 in IPv4
  - IPv6 in IPv4
  - IPX in IPv4
  - etc.
- Optional 32bit tunnel key
- Sequence numbers defined but weak
- Supports source routing!

Once upon a time ...



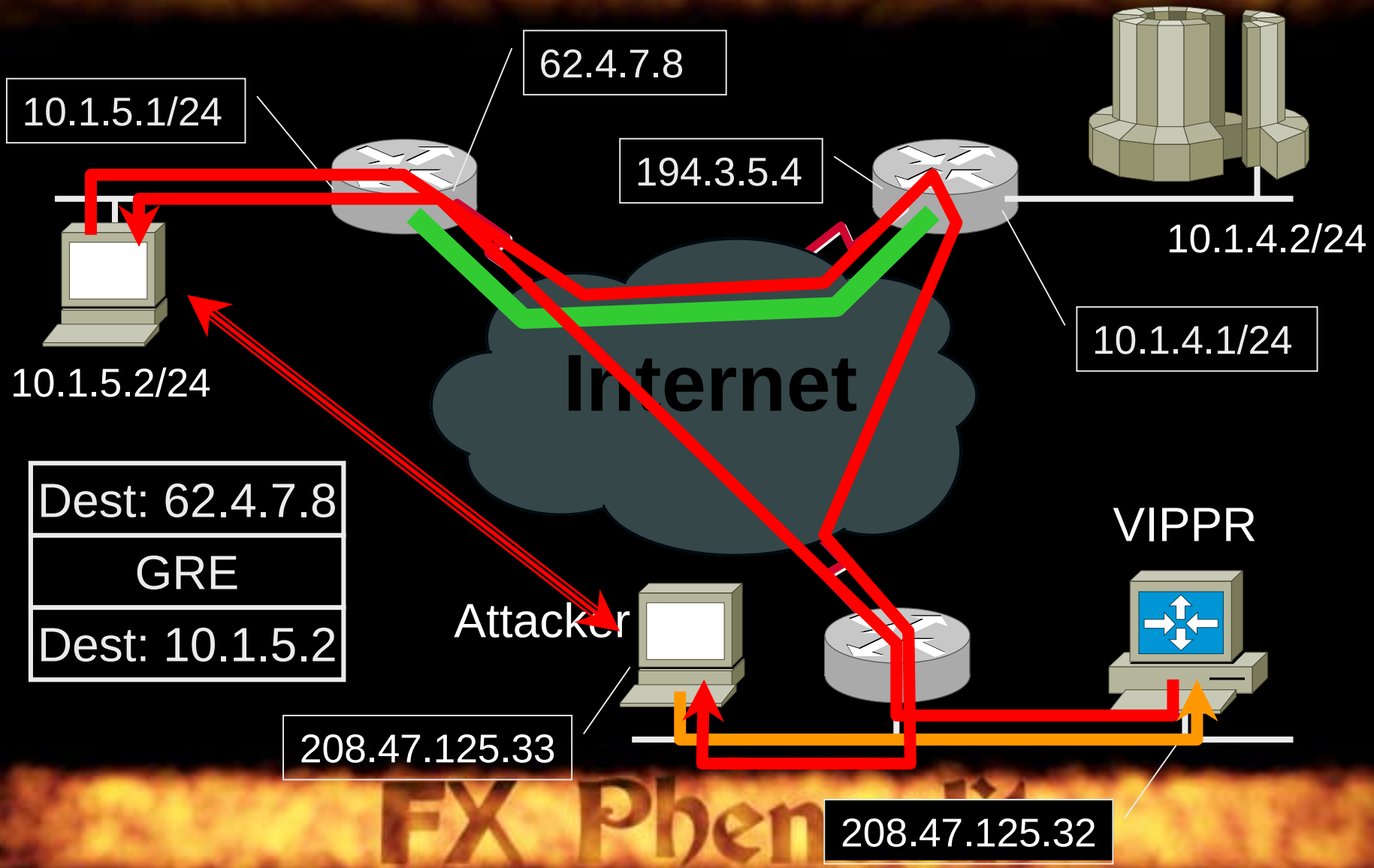
- **Company tries to connect private networks**
- **Carrier offers „VPN“ solution based on GRE**
- **IP traffic from remote location to HQ encapsulated in GRE**

FX Phenoelit

Making the game interesting

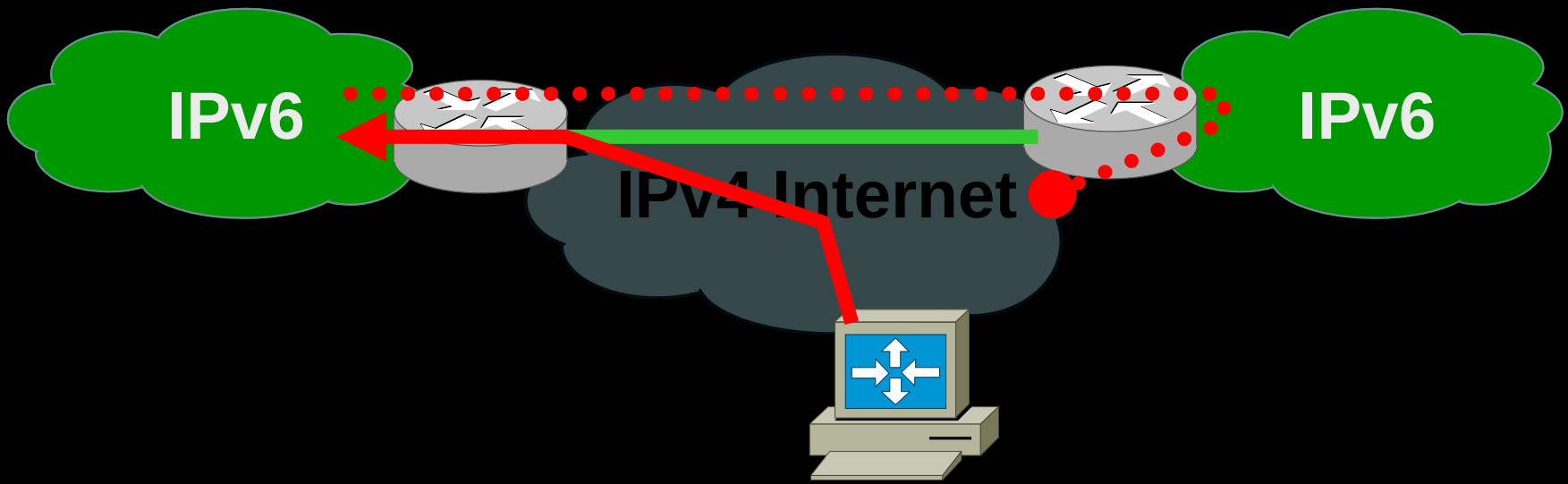
- Branch office router:
  - Does not allow any traffic on outside interface other than GRE from 194.3.5.4
  - Routes all traffic from the internal network (10.1.5.0/24) into the GRE tunnel
- HQ router
  - Does not allow incoming connections on the outside interface
  - Does only allow GRE from branch offices

GRE Tunnel Intrusion



Islands at Risk

- IPv4 islands (IP Encapsulation within IP)
- IPv6 islands connected by GRE tunnels



Phenoelit IRPAS Tools

- Autonomous System Scanner
- Protocol sender:
  icmp_redirect, cdp, hsrp, igrp, irdp, irdpresponder
- Trace programs: itrace & tctrace
- Protocol scanner: protos
- Virtual IP attack router (still 1st beta): VIPPR

Tools and slides available on
http://www.phenoelit.de/

FX Phenoelit

Summary

- There are many ways to alter a traffic path
- Most routing protocols are insufficient protected – this makes routing protocol attacks successful
- Unencrypted tunneling protocols represent a high risk and demonstrate the fact that so-called „private“ IP addresses do not protect!

Thanks go to ...

- FtR, kim0, Zet, DasIch and Bine for being Phenoelit
- Jeff Moss & the BlackHat staff for everything
- Nico/Sécurité.Org for the idea to coordinate the two speeches

n.runs Security Group

The BlackHat audience for being here !