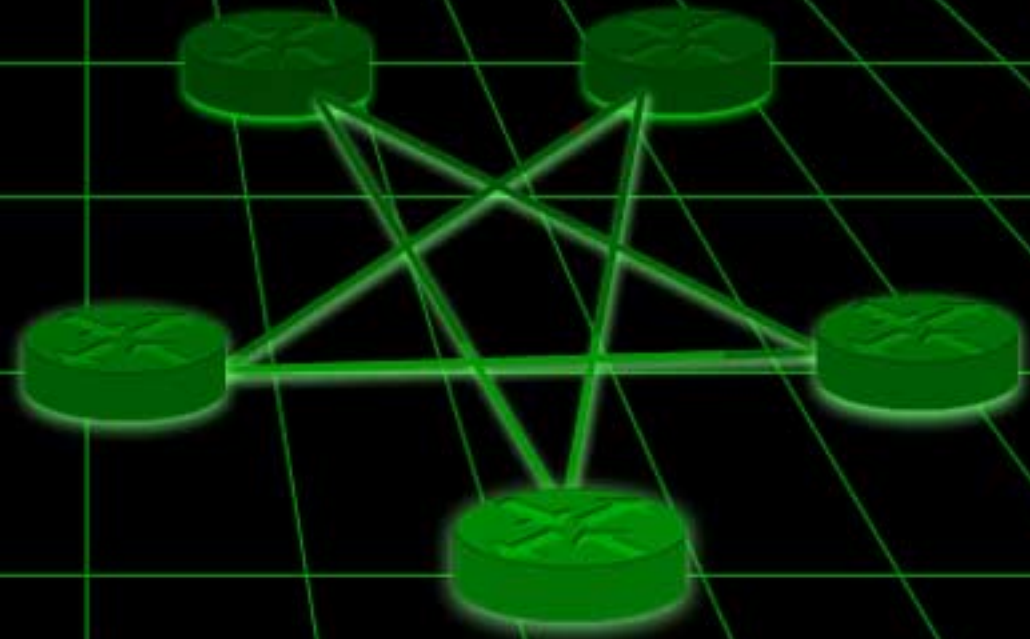
Routing & Tunneling Protocol Attacks

DEFCON 9

FX
Phenoelit



Session Overview

- Introduction
- Layer 2 and 3 attack scenarios
- Hack the cable: ARP attacks
- ICMP abuse
- Discovering & attacking IGPs
- GRE intrusion & RFC-1918 hacking

Why bother with protocols when I have exploits?

Exploits

- Specific software
- Specific version
- Platform dependent
- Exploit awareness
- Patches protect and are easy to apply

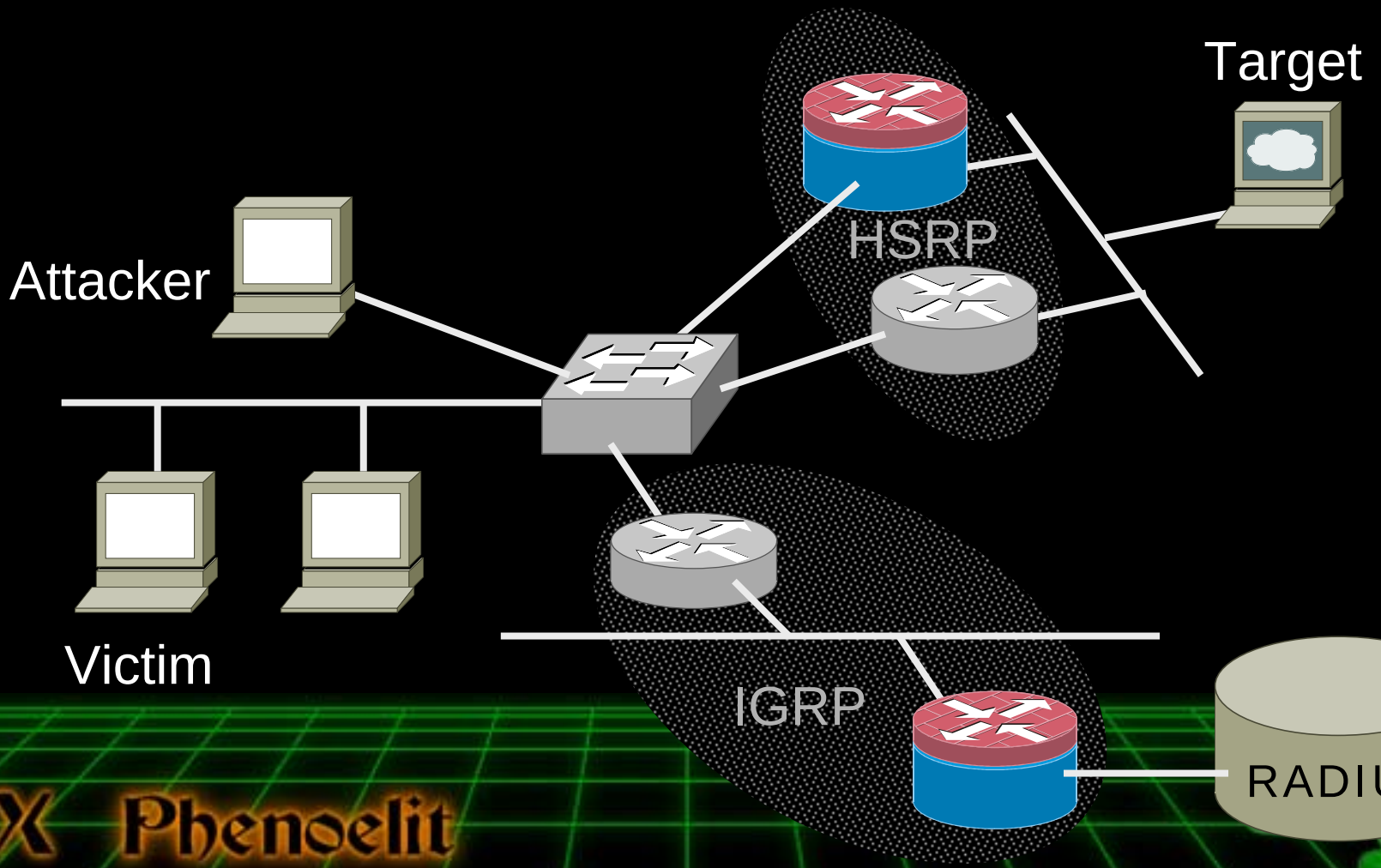
Protocols

- Standards Conformant
- Widely supported
- Platform independent
- Issues are less known
- Only a consistent config and design protects

Use both!

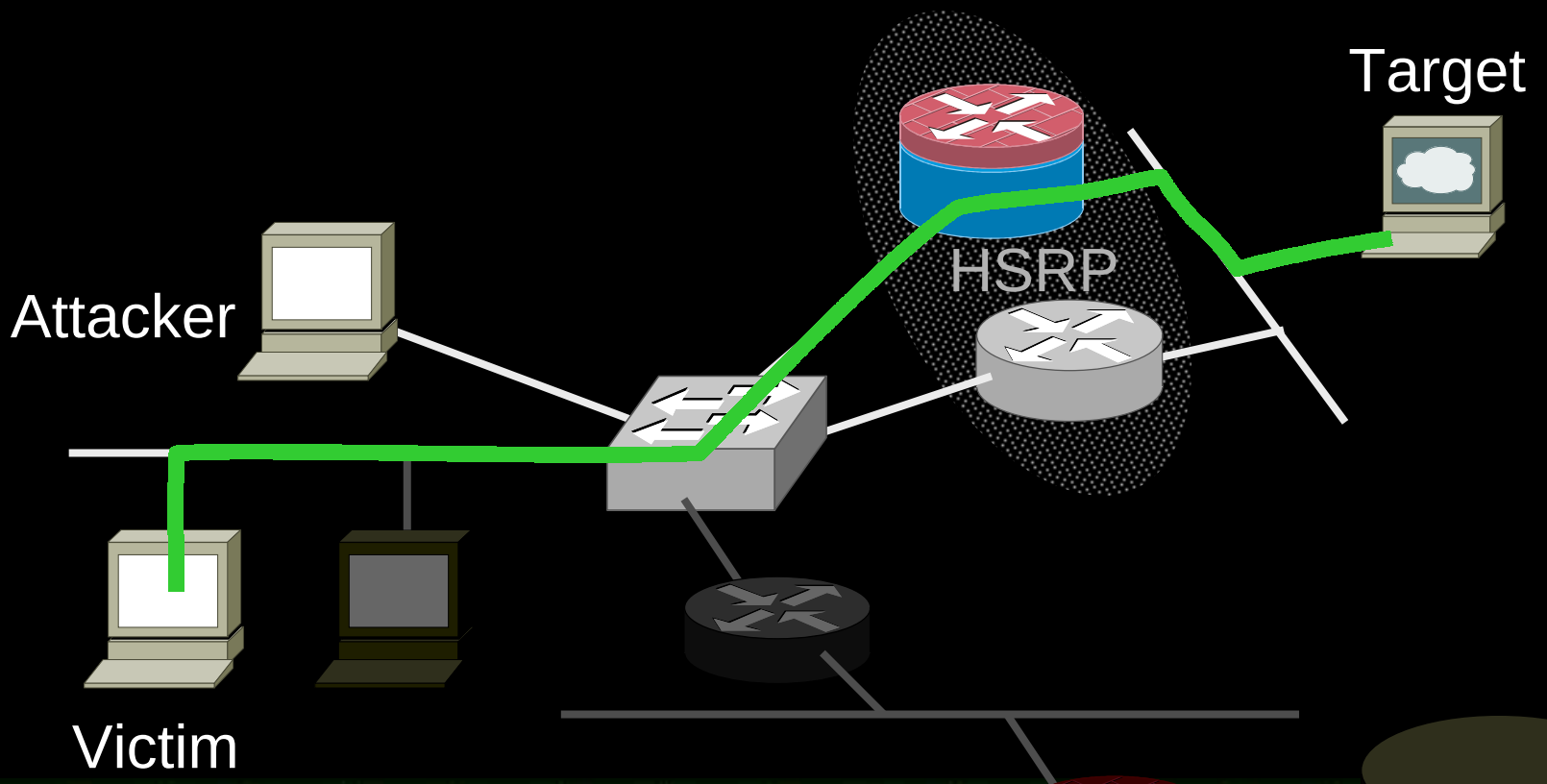
FX Phenoelit

Attack Scenarios [0]
The Network



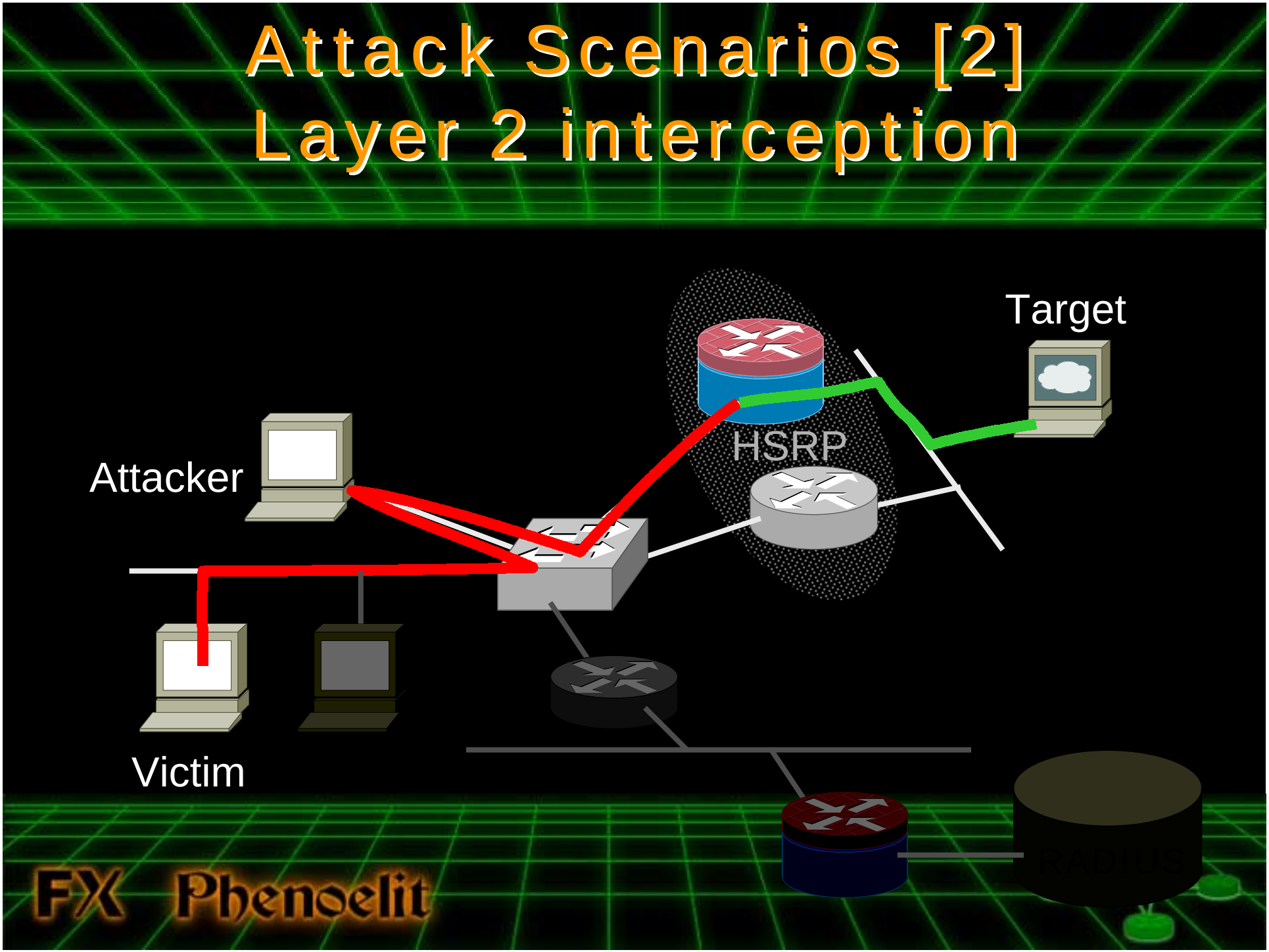
FX Phenoelit

Attack Scenarios [1]
A normal traffic path

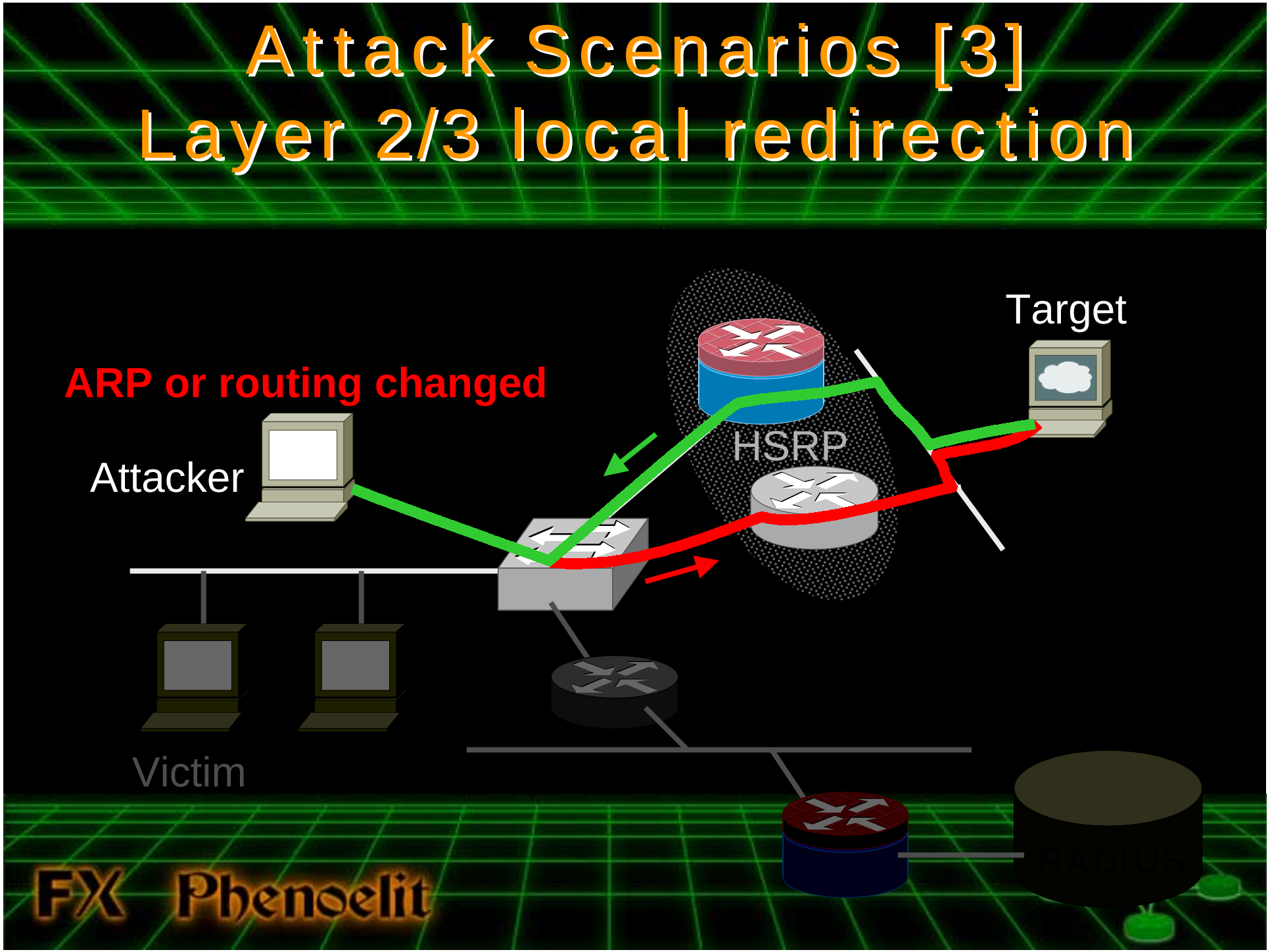


FX Phenoelit

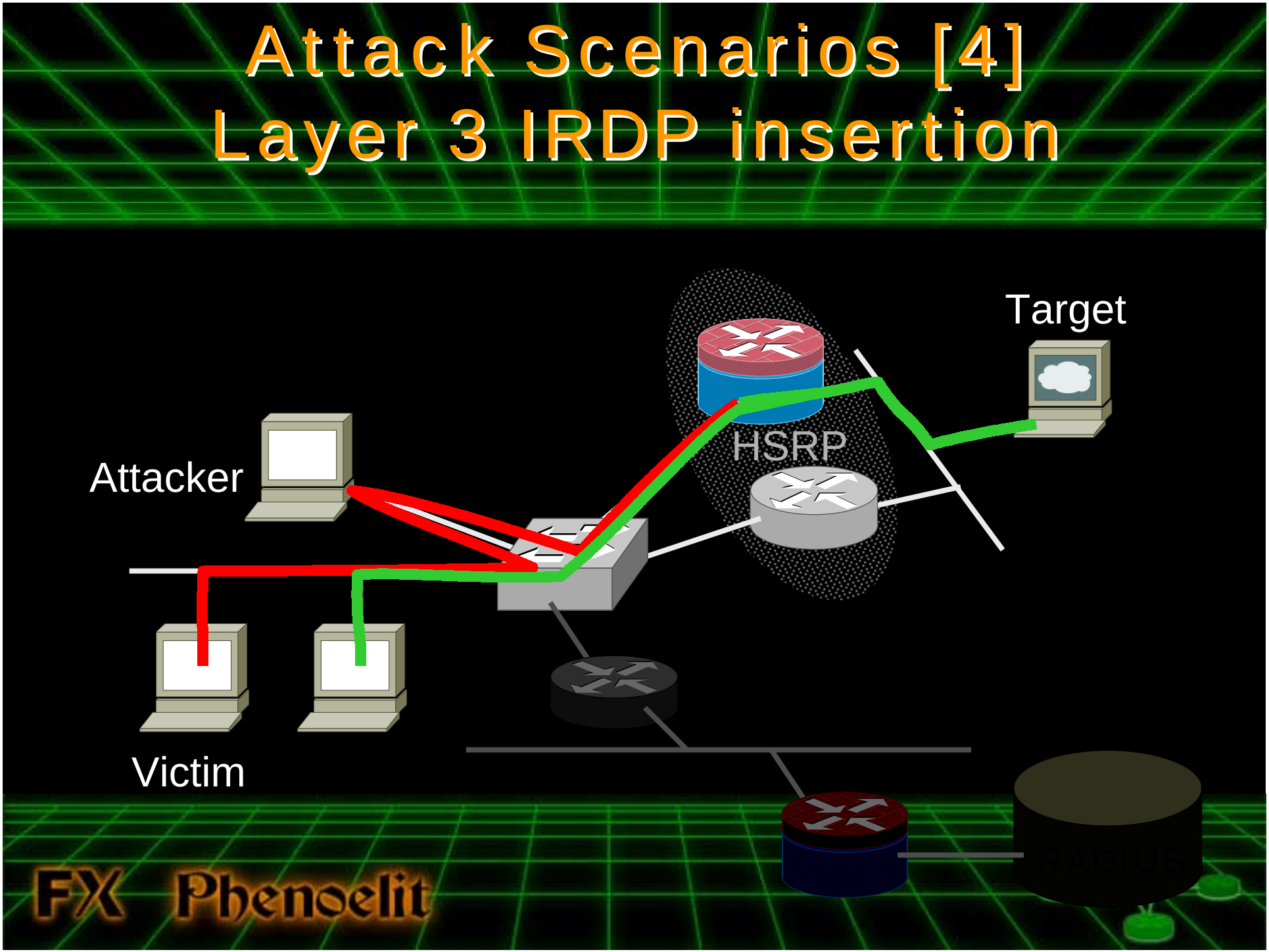
Attack Scenarios [2]
Layer 2 interception



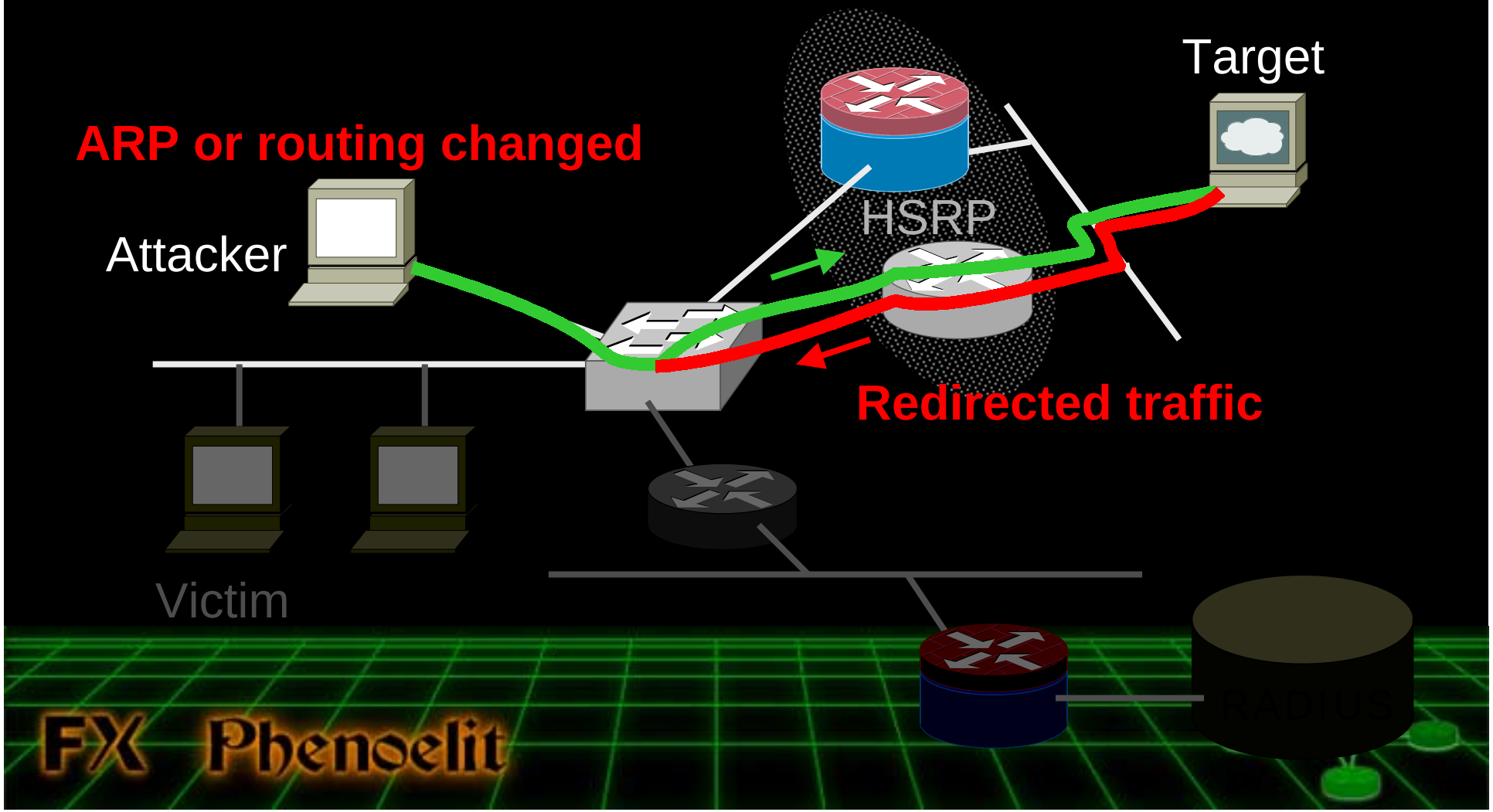
Attack Scenarios [3]
Layer 2/3 local redirection



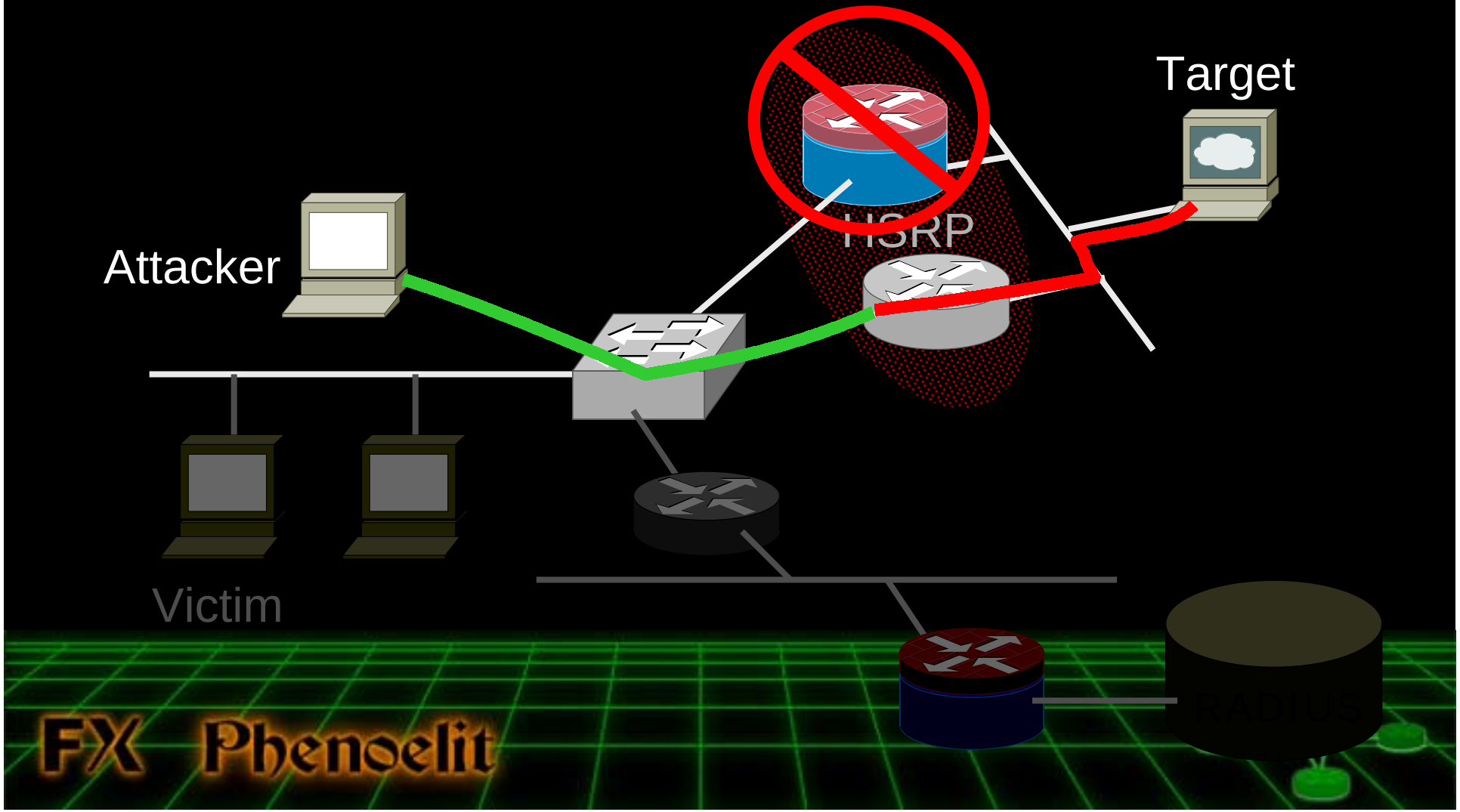
Attack Scenarios [4]
Layer 3 IRDP insertion



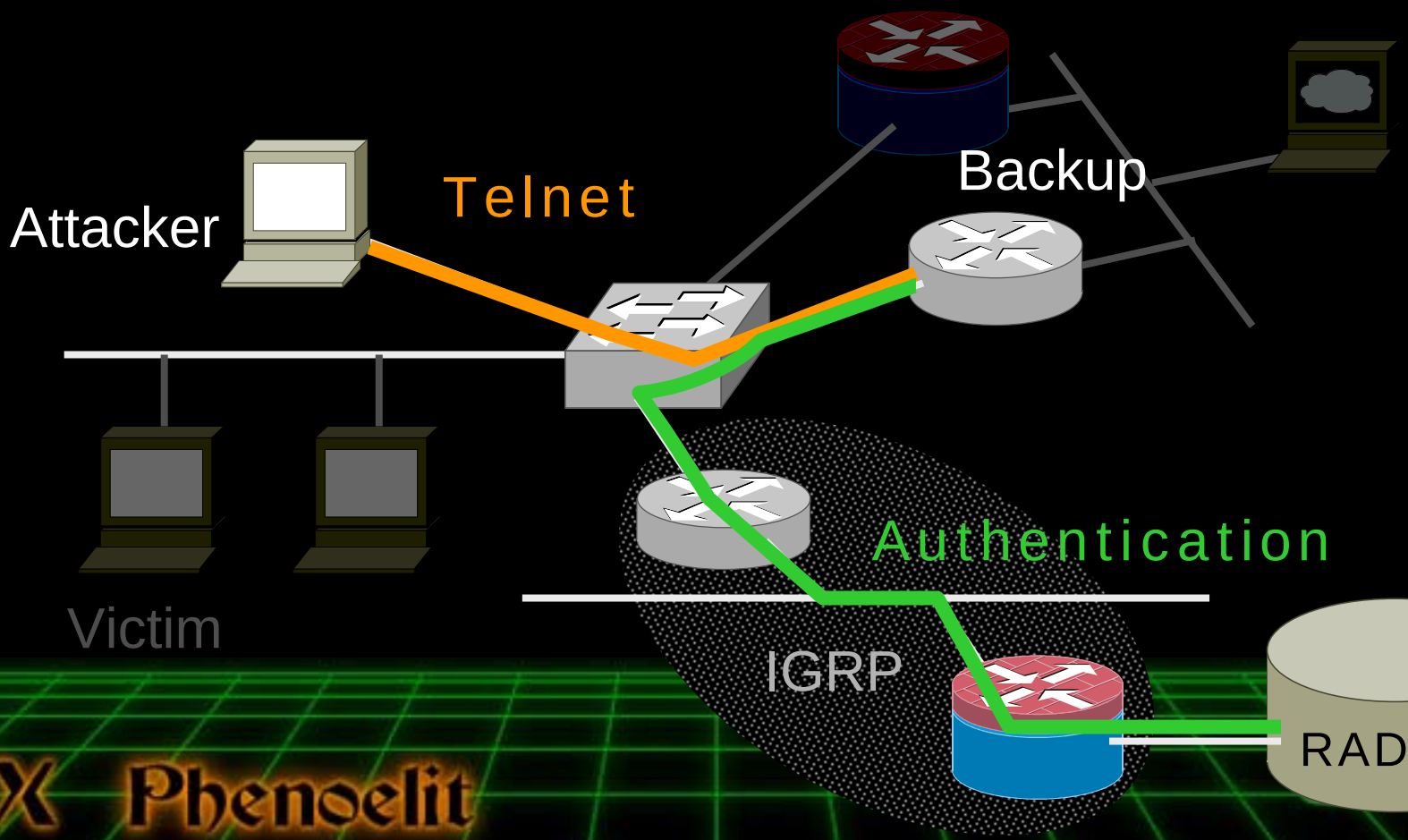
Attack Scenarios [5]
Layer 3 redirection (ICMP)



Attack Scenarios [6]
HSRP switchover & takeover

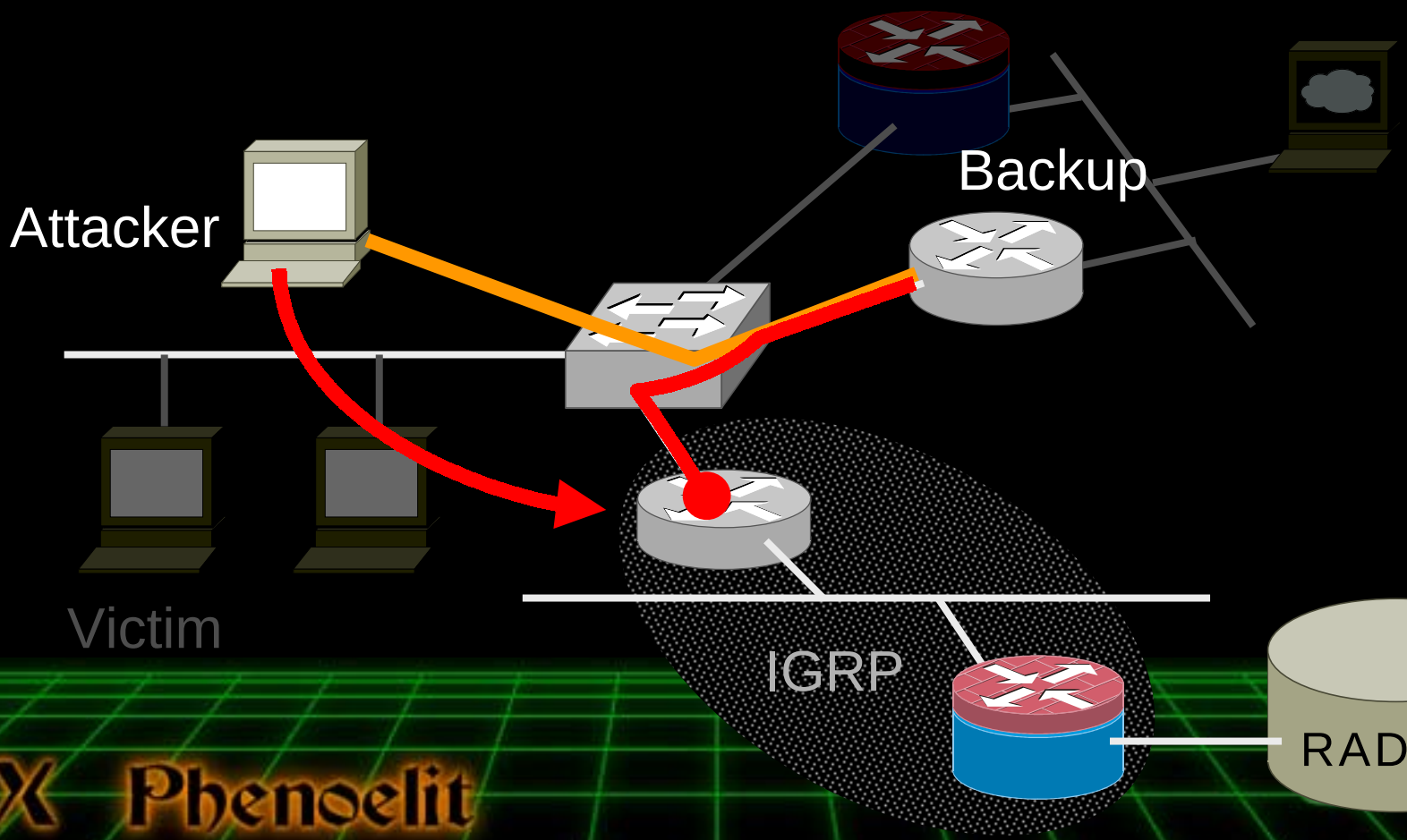


Attack Scenarios [7]
Another normal traffic path



FX Phenoelit

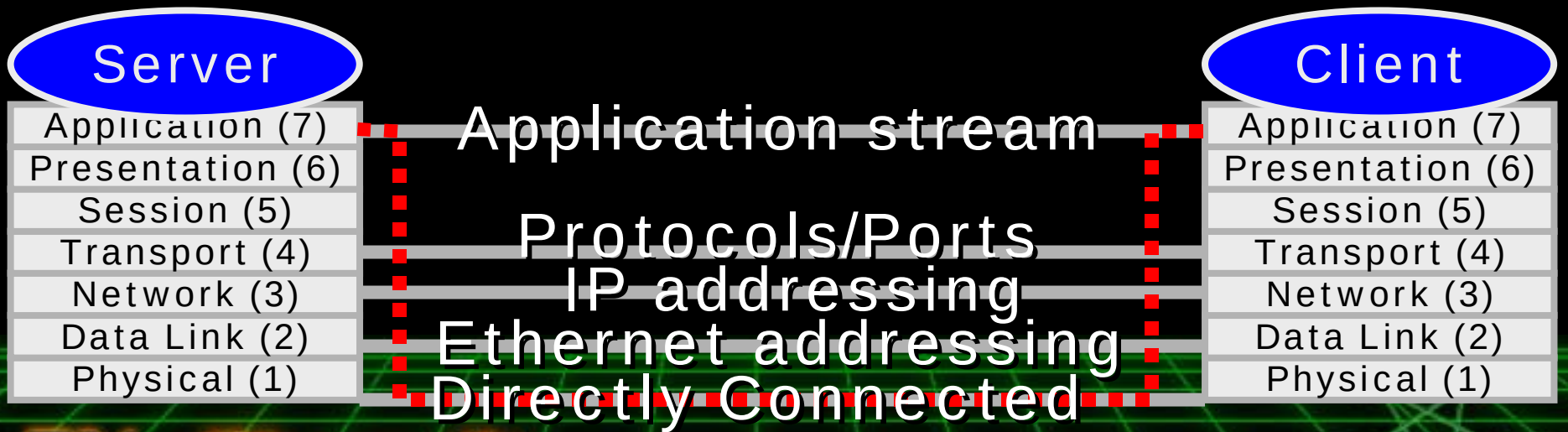
Attack Scenarios [8]
IGRP Routing attack



FX Phenoelit

How do these attacks work in general?

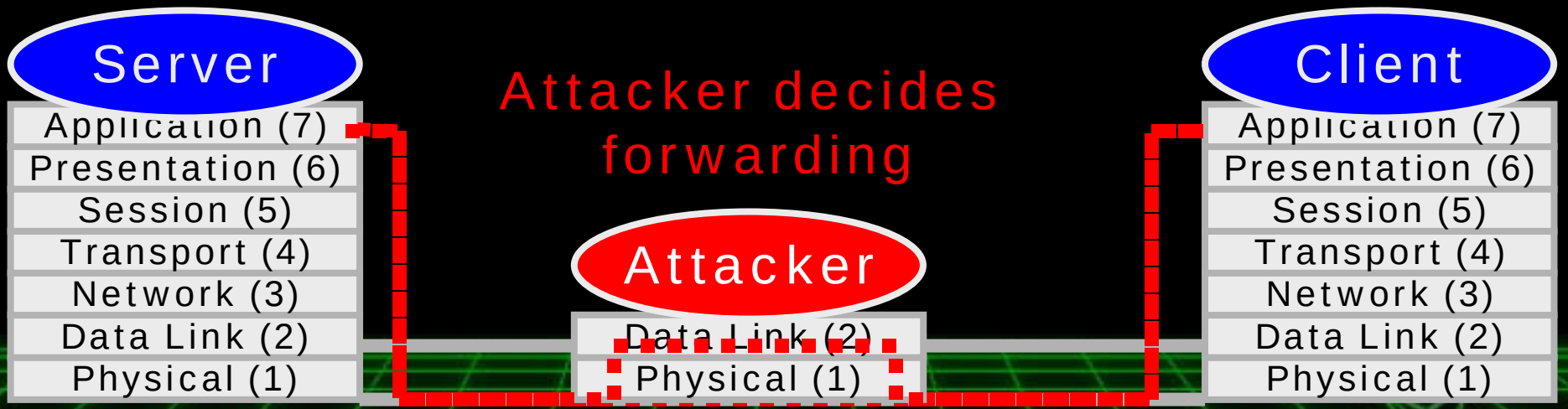
- Normal communication goes down the OSI layers
- All attacks on Layer 2 and Layer 3 work on
  - Modification of the **addressing**
  - Therefore modification of the **traffic path**



FX Phenoelit

Layer 2 Attack

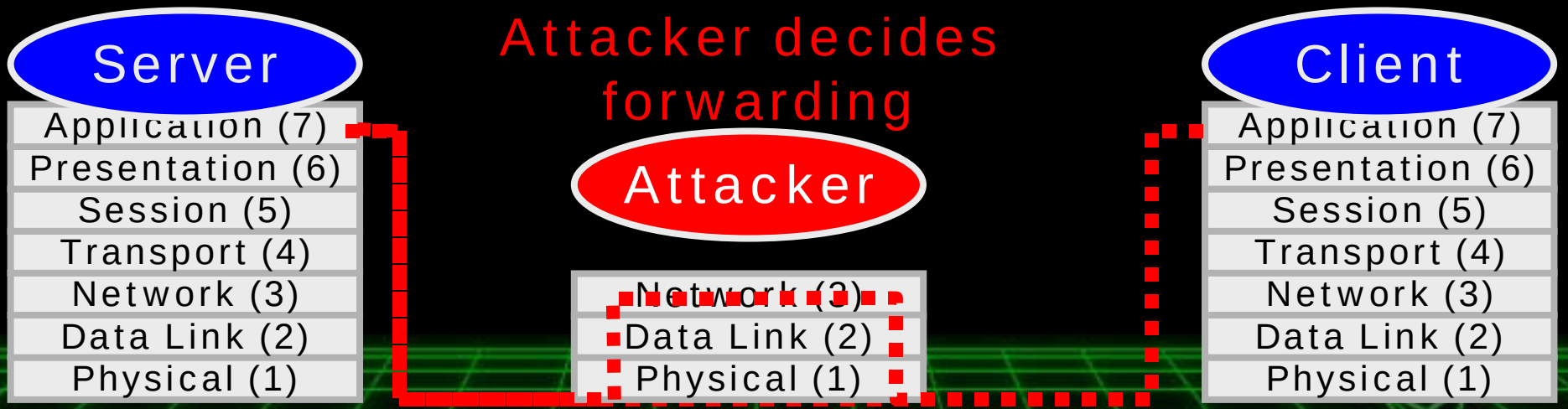
- Man in the middle attack
- Intercepting traffic by giving false data link address information to both parties
- Layer 3 remains untouched
- The only effective way is ARP interception



FX Phenoelit

Layer 3 Attack

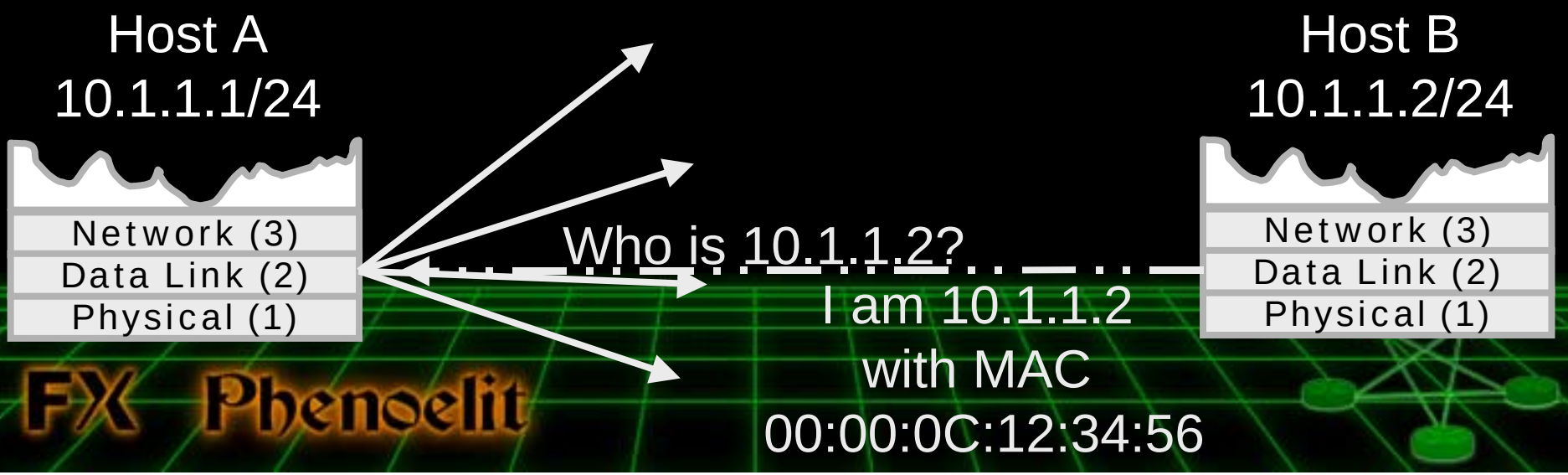
- Man in the middle or remote attack
- Intercepting traffic by giving false next hop information to one or both parties
- Works from remote segments
- There are various methods of applications



FX Phenoelit

Address Resolution Protocol
ARP (RFC 826)

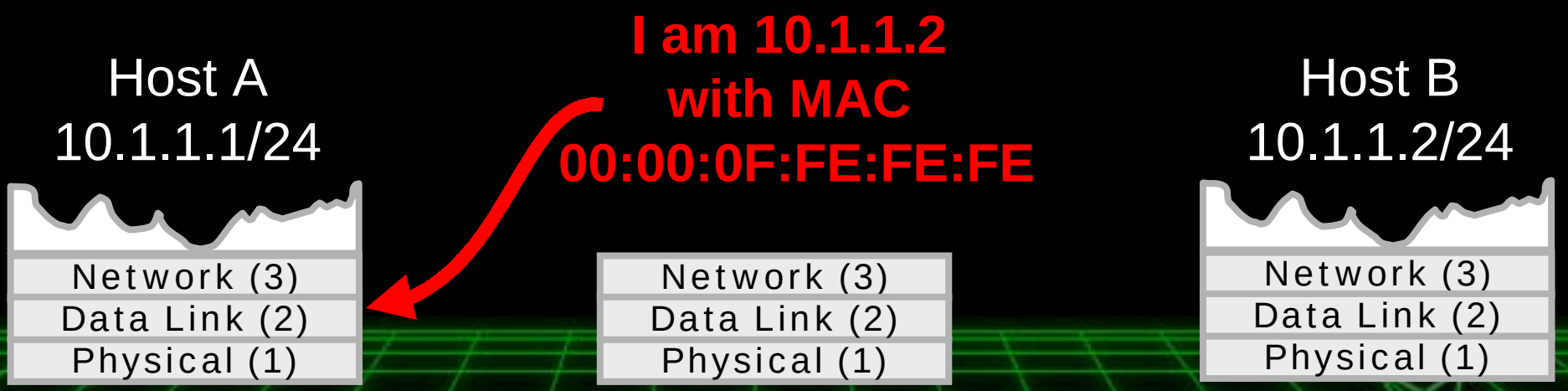
- IP addresses are resolved into Media Addresses
- If the Media Address is unknown, request it via Broadcast
- First or most recent answer is used to communicate
- Address cache times out on most systems



FX Phenoelit

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



FX Phenoelit

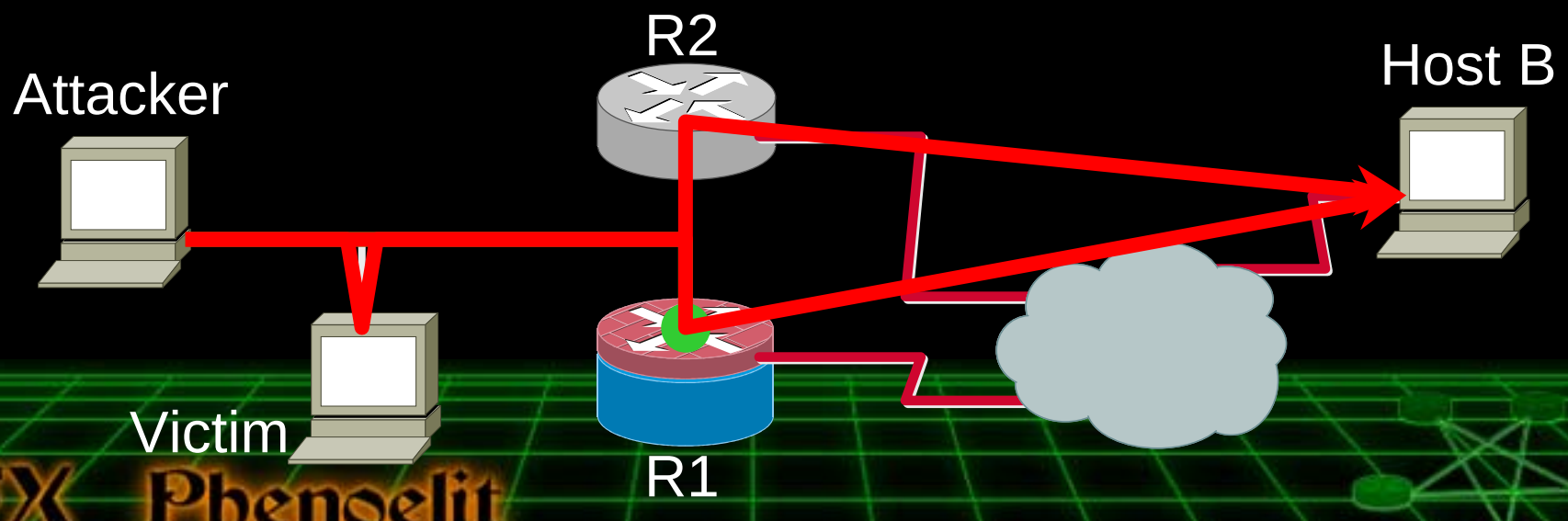
ARP Attack Tools

Tools for ARP attacks

- Phenoelit ARP0c (Linux) & WCI (Windows)
- THC Parasite
- Ettercap by ALoR & NaGA
- arpspoof by Dug Song
- HUNT by Pavel Krauz
- lots of others ...

Local Redirection

- Fixed ARP entries mapped to other IP address
- Alternative routes to circumvent packet filters
- Adding another local hop
- Can be done by hostile code on target system



FX Phenoelit

Discovering Routers

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

FX Phenoelit

Router Discovery Tools

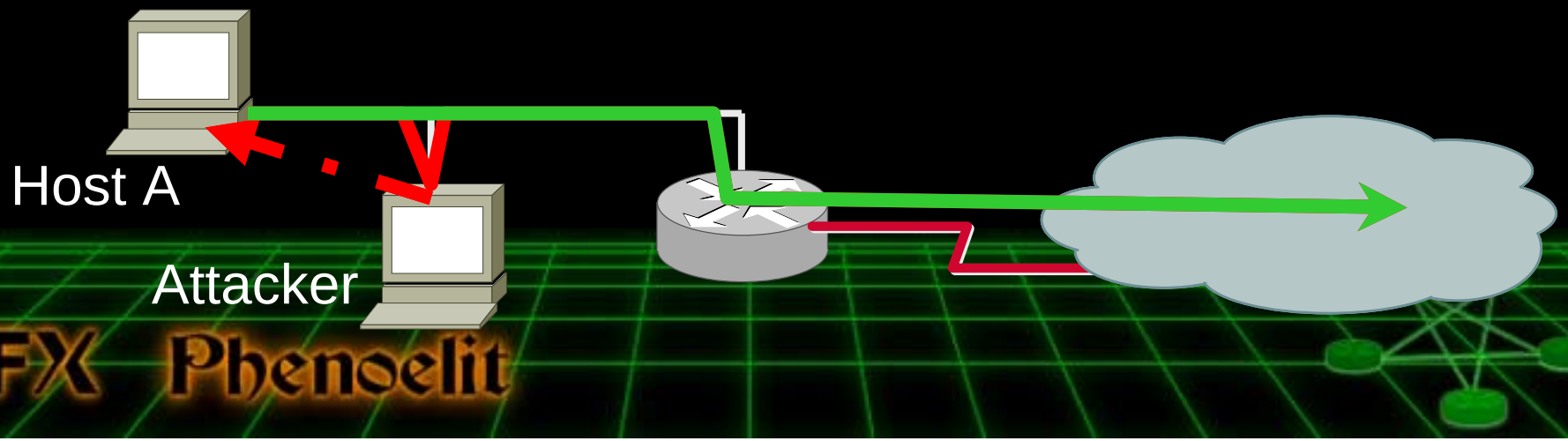
- Autonomous System Scanner (ASS) can be used for active or passive detection
- Ethereal can decode most routing protocols
- ntop can be used to discover central traffic points
- tcpdump‘s -e option shows data link addresses
- Fyodor‘s nmap and Phenoelit‘s protos scan for IP protocols
- DHCP queries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

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
  - 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)
  - ICMP Redirect
  - Temporary ARP interception
- Attacker is now the default router



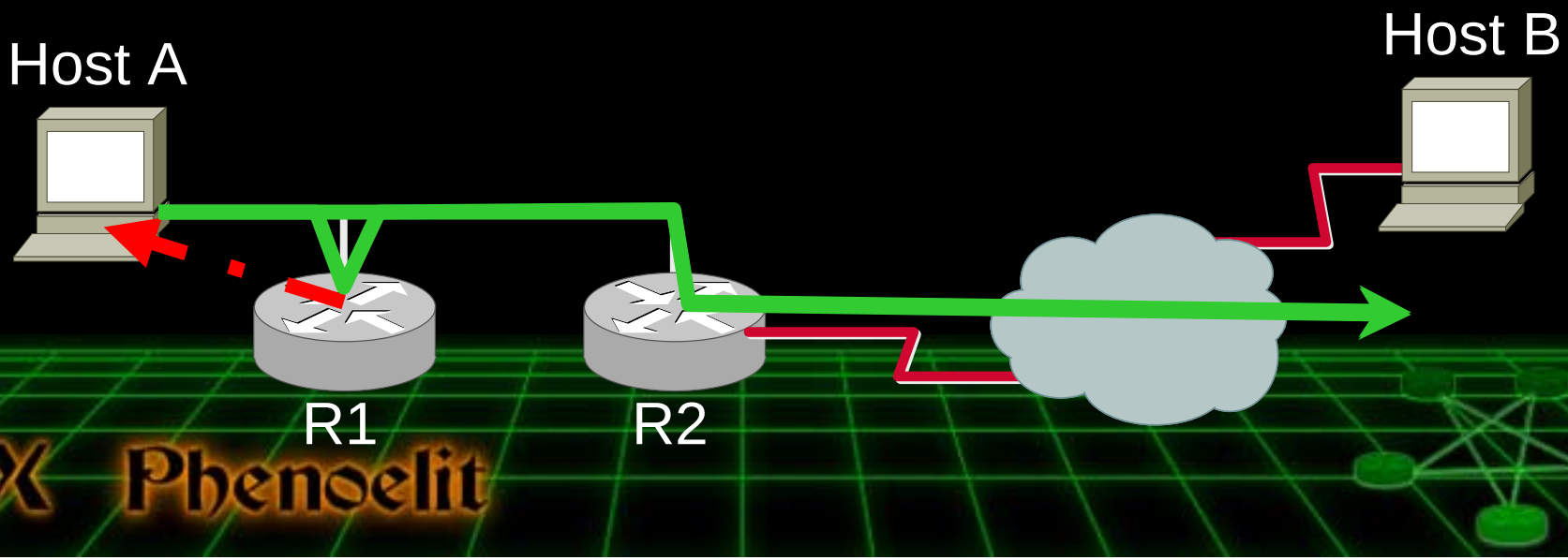
FX Phenoelit

IRDP Attacks

- Phenoelit IRPAS tools
  - Irdp & Irdpresponder
  - ASS
- Best as additional interception because of metric
- Can be used to prevent interception recovery
- Lifetime of a route max **18h:12min:15sec**
- Windows 9x does IRDP **all the time**, NT on boot
- Linux doesn't care

ICMP Redirects (RFC 792)

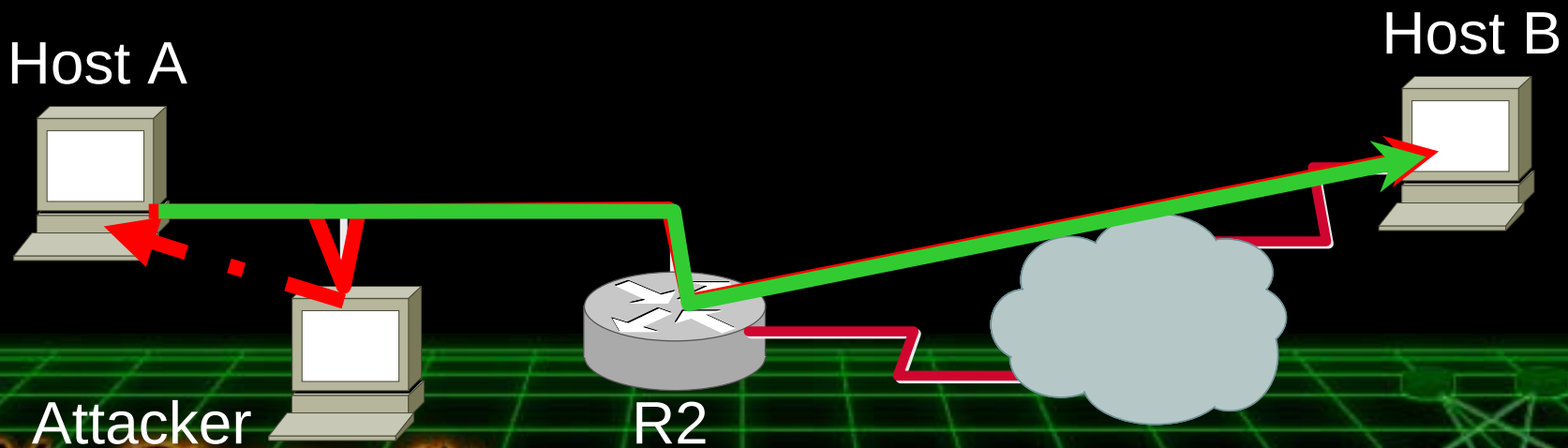
- Introduced to make routing more effective
- Packet is send from Host A to B through router R1
- R1 finds next hop R2 on same segment and network
- R1 forwards the packet
- R1 sends ICMP Redirect to A



FX Phenoelit

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

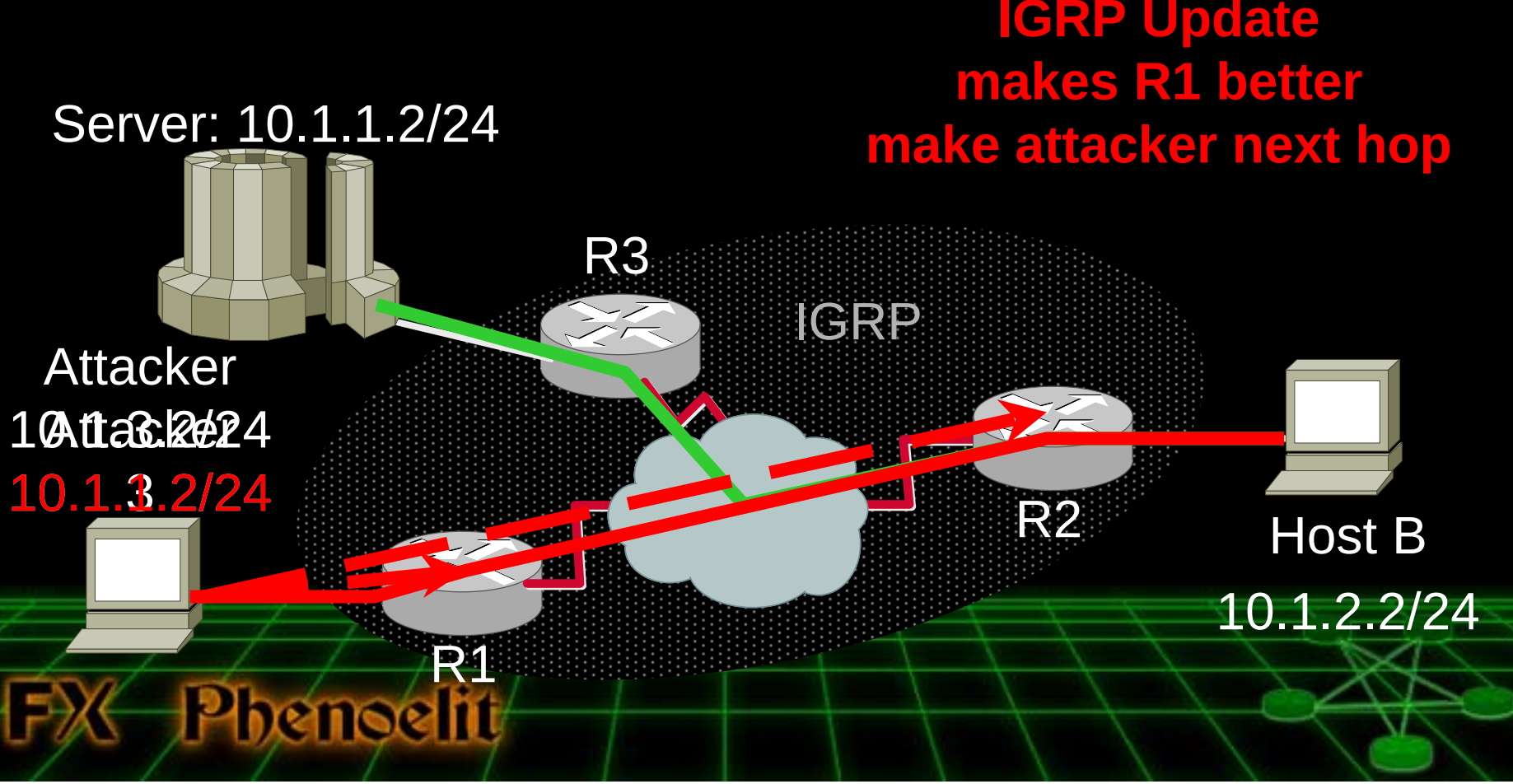
- Windows 9x Hosts
  - Accepts ICMP redirects by default
  - Adds a host route to routing table
- Linux Hosts
  - Accepts ICMP redirects by default in some distributions
  - See /proc/sys/net/ipv4/conf/*/accept_redirects
    Does not show redirects in routing table
- Tools:
  - IRPAS icmp_redirect
 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



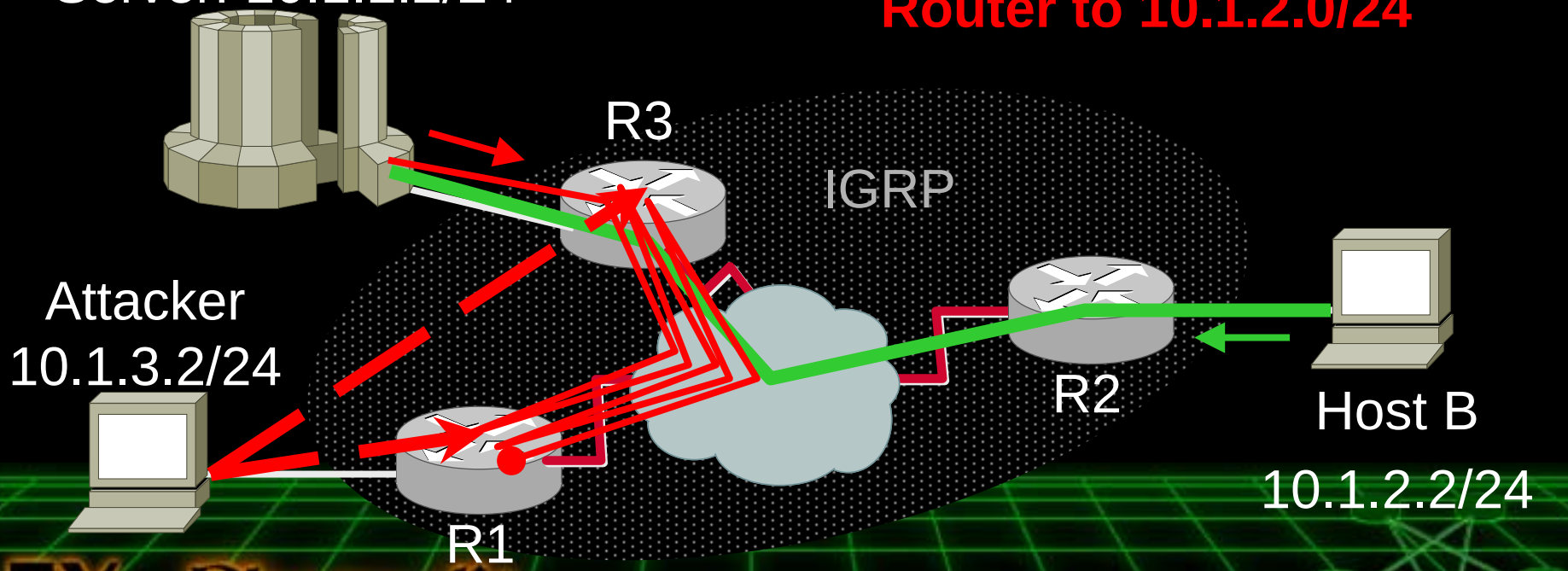
FX Phenoelit

IGRP Attacks

Creating routing loops

Tell R3 that R1 is the best Router to 10.1.2.0/24

Tell R1 that R3 is the best Router to 10.1.2.0/24



FX Phenoelit

Routing Information Protocol Version 1 (RFC 1058)

- RFC published 1988
- Uses fixed network size
  (no subnet information possible)
- No autonomous systems
- Runs on UDP port 520
- Broadcast or unicast traffic
- Passive or silent hosts possible (port scan)

Routing Information Protocol Version 2 (RFC 2453)

- Uses destination network/net mask
- Includes next hop information and net masks
- No autonomous systems
- Runs on UDP port 520
- Multicast or unicast traffic
- Passive or silent hosts possible (port scan)
- Clear text authentication defined
- Cisco supports MD5 authentication (double authentication block forbidden by the RFC)

FX Phenoelit

RIP Attacks

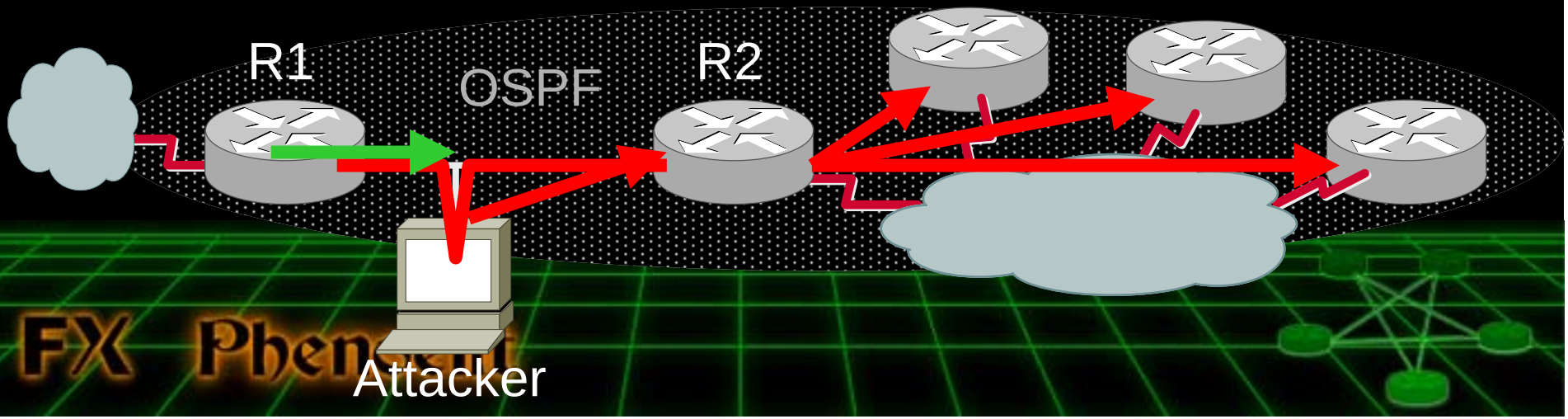
- Same attacks as with IGRP
- Network boundaries are important for RIPv1
- Multicast RIPv2 (224.0.0.9) may be forwarded across segments
- Split Horizon algorithm with poisoned reverse
  - Sends „unreachable“ back to sender of the route (metric 16)
  - May prevent routing loop attacks
  - Protects only 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

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 then other routing protocols
- The „hard-to-understand“ factor helps the attacker

OSPF Attacks

- Attacks tend to be very complex
- Forged LSAs are contested by routers
- Best attack seems to be „extended-Layer 2“
  - 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 targen than EBGP

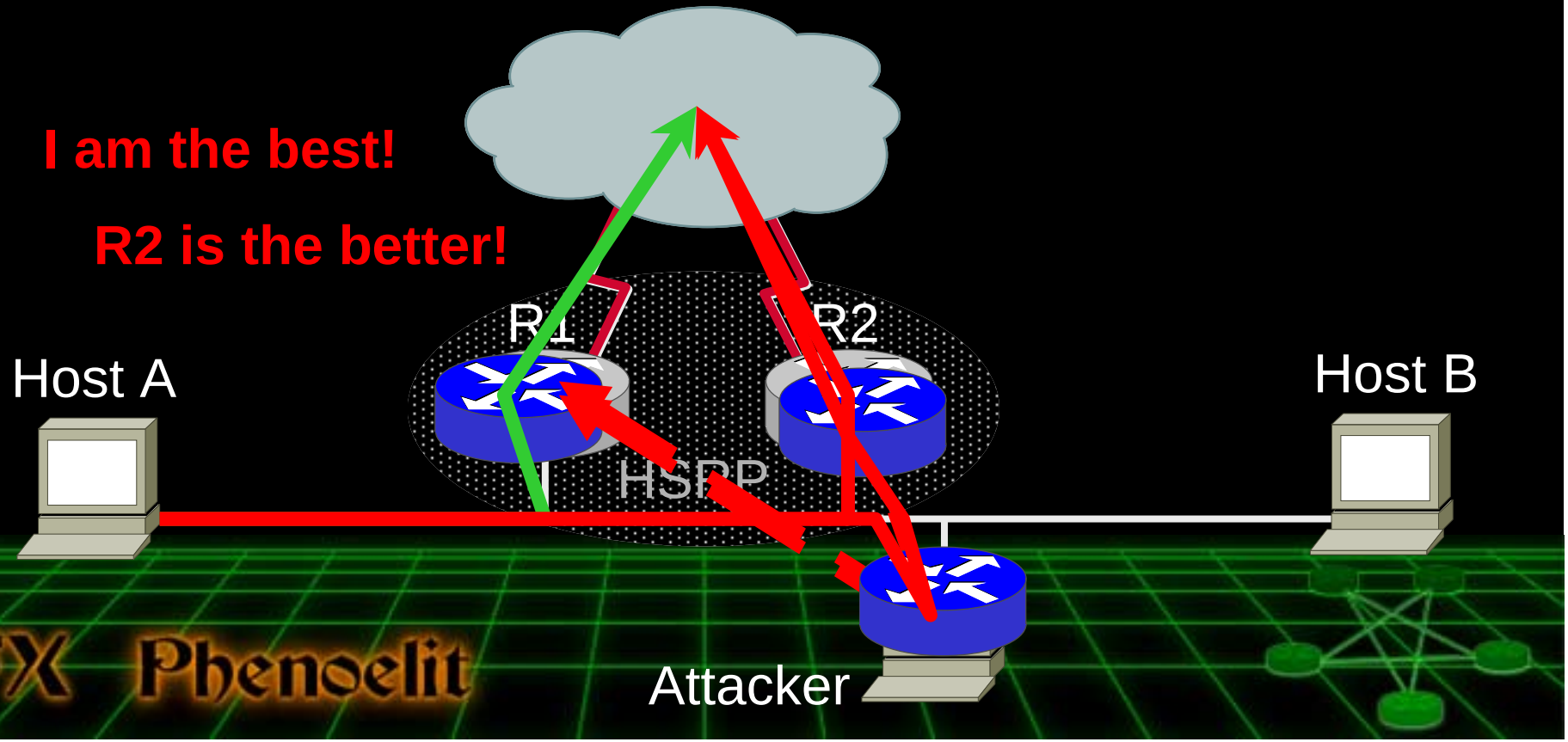
FX Phenoelit

Hot Standby Router Protocol HSRP

- 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

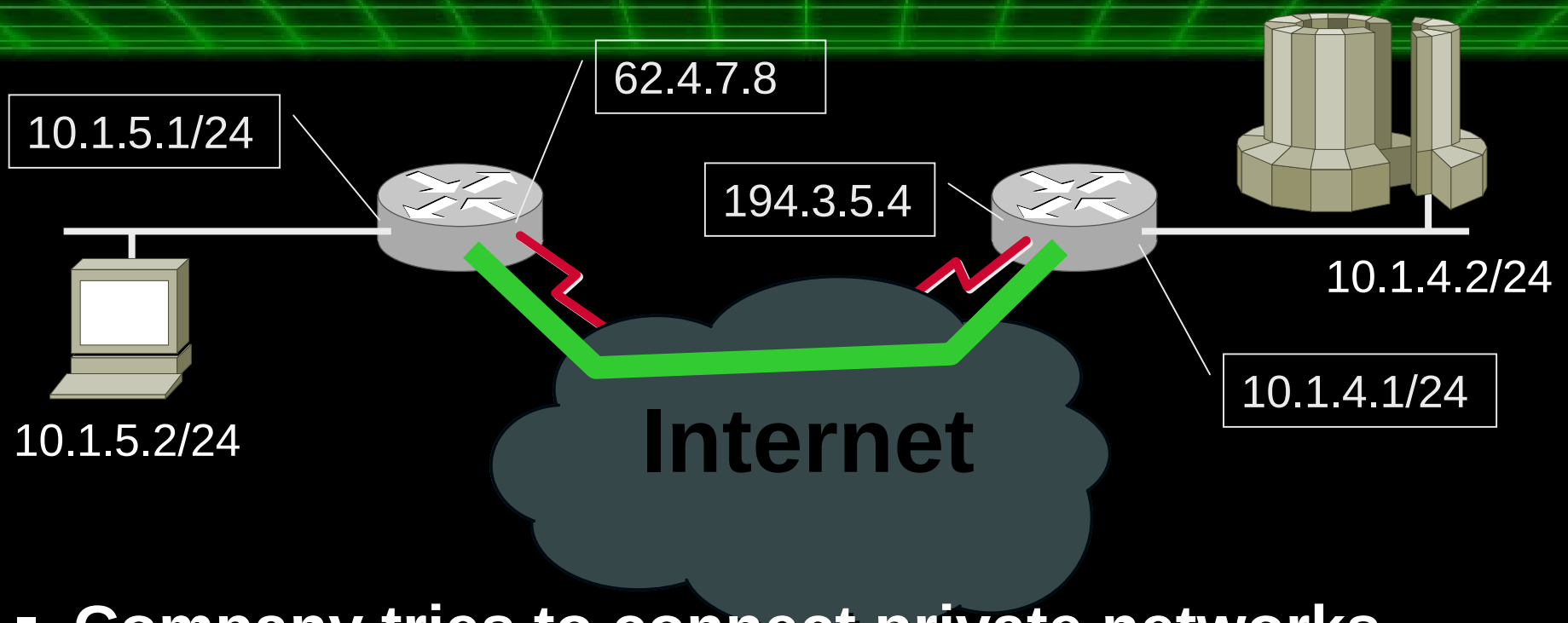
- New routers with high priority can take over the „standby“ addresses



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

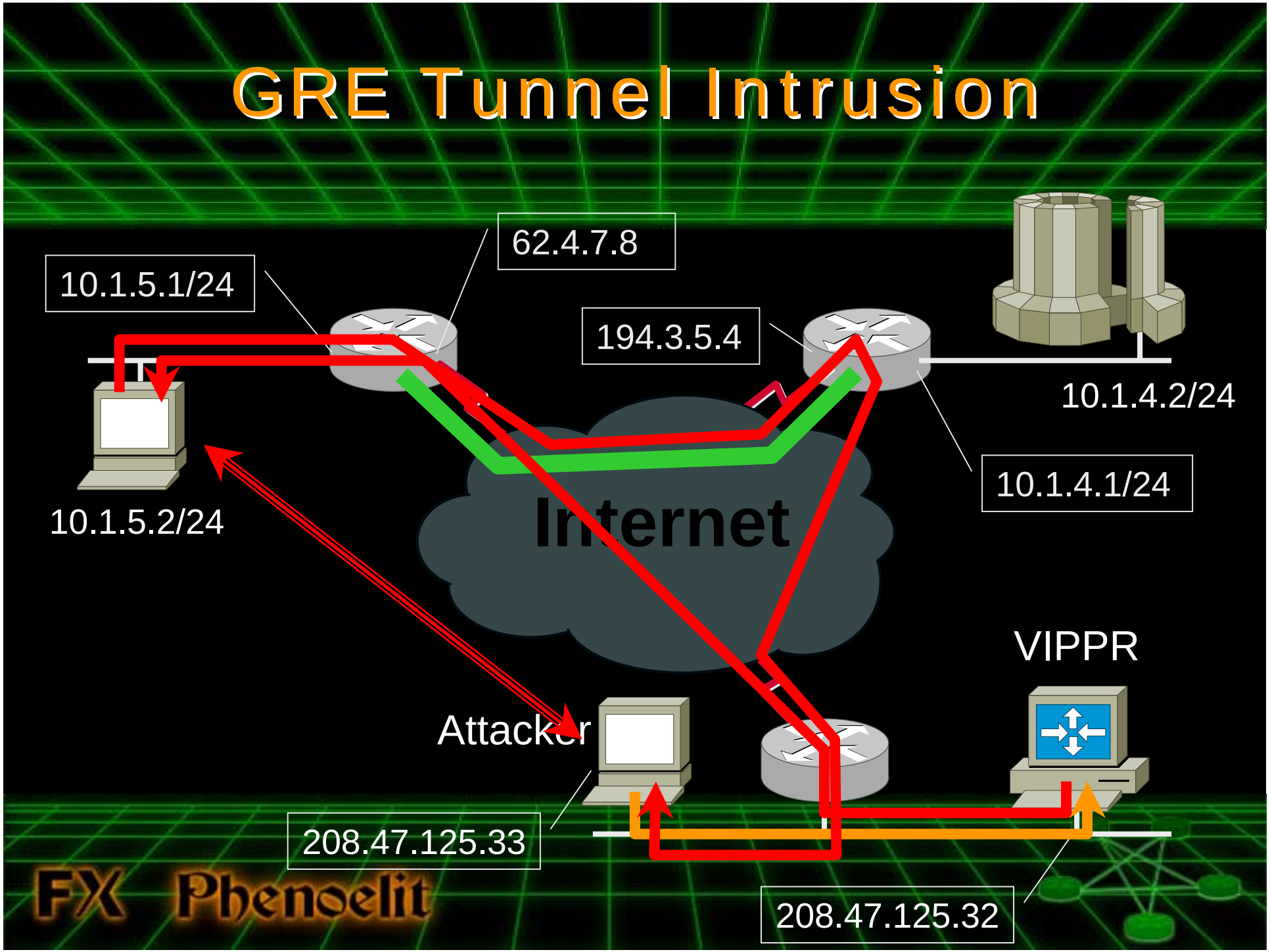
- Used to transport protocol A over domain of protocol B in B‘s payload
  - IPv4 in IPv4
  - IPv6 in IPv4
  - IPX in IPv4
  - etc.
- No authentication or 32bit tunnel key
- Sequence numbers defined but weak
- Supports source routing!

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


GRE Tunnel Intrusion
62.4.7.8
10.1.5.1/24
194.3.5.4
10.1.4.2/24
10.1.4.1/24
10.1.5.2/24
Internet
VIPPR
Attacker
208.47.125.33
208.47.125.32
FX Phenoelit

More Tunnel Attacks

- GRE attack functionality in VIPPR will be extended to support source routing
- Same attack can be applied to
  - IPX encapsulation (RFC 1234)
  - AX.25 encapsulation (RFC 1226)
  - Internet Encapsulation Protocol (RFC 1241)
  - IPv4 in IPv4 encapsulation (RFC 2003)
  - IPv6 in IPv4 encapsulation (mostly GRE)

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 (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
- Curt Wilson for his paper about routing attacks
- smoovB for ideas and support

Lucent Technologies
Bell Labs Innovations

LWS Security Practice

The DEFCON 9 audience for being here !

FX Phenoelit