Welcome to

Security in a Mixed IPv4 and IPv6 World

PROSA

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg

ipv6-security-in-mixed-v4-v6.tex in the repo security-courses

Time schedule

- 17:00 - 18:15 Introduction and basics
- 30min break go be with your family, hang around, get coffee/tea
  Try IPv6 on your phone, laptop, table, at home, your VPN
- 18:45 - 19:15 Walking through the stack
- 10min break
- 19:25 - 20:00 Protection, building secure and robust networks

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: hlk@zencurity.com Mobile: +45 2026 6000
- Run a small network for fun AS57860

You are welcome to drop me an email

❤ THANK you all of the IPv6 Community! ❤

- I have used many references over the years, I have used open source since forever
- I have read papers since the early nineties, so grateful for information sharing
- Note: this presentation is open source! You may remix, re-use, steal and copy
- I have deliberately included names and references which are part of this community, like RIPE NCC and APNIC
- Many companies also share information about IPv6 security, Cisco, Juniper, ERNW and others
- This presentation available at kramse@Github ipv6-security-in-mixed-v4-v6.tex in the repo security-courses

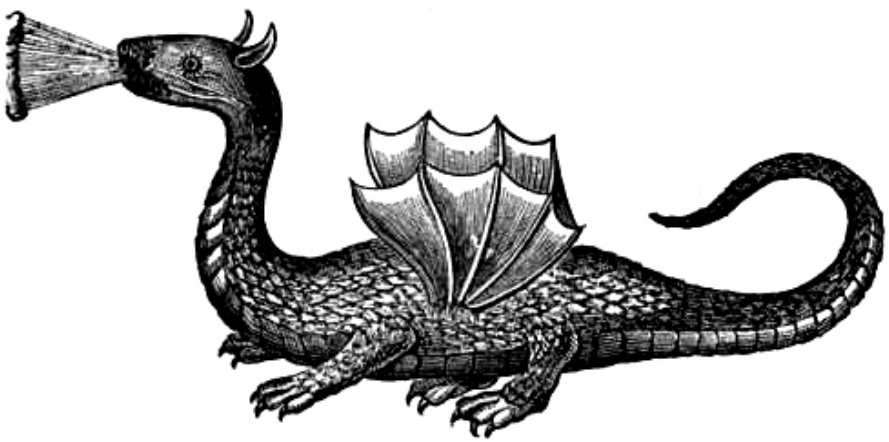
I have included a small list of resources on page 75

Goals for today

- Network security in a mixed IPv4 and IPv6 environment, the title says so ☺
- Introduce security problems that have haunted us in 35 years
- Suggest methods and ways to reduce problems, longer lasting than patching
- Create an understanding of a more paranoid mindset – take control of your networks
- Network configuration of existing equipment, mostly enterprise networks
- Taking control includes configuring IPv6 security, and any IPv4 security you forgot 🚩

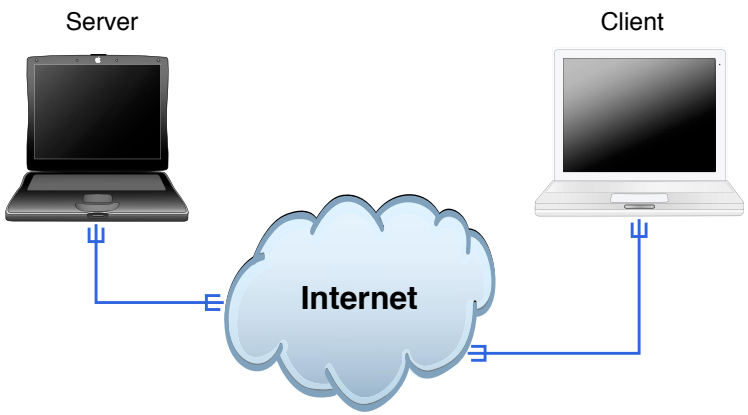
Red flags are considered check points, actions, something I think you should investigate

Networks are trouble



- Networks are constantly evolving
- Threats are constantly increasing
- Vulnerabilities are found daily
- Even more vulnerabilities are *developed* and *installed*
  Sorry developers, but some of you don't care, and it shows!

Internet Today



Clients and servers, roots in the academic world

Protocols are old, some where implemented on the internet around 1983

Not everything is encrypted, mostly HTTPS

TCP/IP Protocol Suite

Security Problems in the TCP/IP Protocol Suite

*S.M. Bellovin**
smb@ulysses.att.com

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

- *Security problems in the TCP/IP protocol suite*, S. M. Bellovin April 1989, https://www.cs.columbia.edu/~smb/papers/ipext.pdf
- *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* 2004, https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf

Security problems in the TCP/IP Suite

> The paper "Security Problems in the TCP/IP Protocol Suite" was originally pub- lished in Computer Communication Review, Vol. 19, No. 2, in April, 1989

Some problems described in the original:

sequence number spoofing

routing attacks,

source address spoofing

authentication attacks

TCP sequence number prediction

> TCP SEQUENCE NUMBER PREDICTION One of the more fascinating security holes was first described by Morris [7] . Briefly, he used TCP sequence number prediction to construct a TCP packet sequence without ever receiving any responses from the server. This allowed him to spoof a trusted host on a local network.

Previously address based authentication was used for many things

Not a realiable security mechanism

Not a problem for generic operating systems, but Internet of Things are a problem again

Better to use real authentication – encryption used for confidentiality and authentication

Additionally using IP filters for restricting access is of course also great

Routing attacks

Problems described in the original from 1989:

- IP Source routing attacks - use a specific source
  Usually not a problem today, ICMP redirect not used much, but layer 2 with ARP spoofing IS a problem
- Routing Information Protocol Attacks
  The Routing Information Protocol [15] (RIP) - RIP is outdated, but using STP, OSPF etc. without authentication is similar
- Border Gateway Protocol (BGP) still used today, still problems
- Domain Name System (DNS) problems
- Simple Network Management Protocol (SNMP) problems

Fun packets with Yersinia could still break a lot of networks https://github.com/tomac/yersinia

Solutions to TCP/IP security problems

Solutions:

- Use RANDOM TCP sequence numbers, Win/Mac/Linux - DO,but IoT?
- Filtering, ingress / egress:
  "reject external packets that claim to be from the local net" BCP38
- Routers and routing protocols must be more skeptical
  Routing filters everywhere, auth routing OSPF/BGP etc.

Has been recommended for some years, but not done in all organisations

BGP routing Resource Public Key Infrastructure RPKI

DNS Problems

5.3 The Domain Name System

The Domain Name System (DNS) [32][33] provides for a distributed database mapping host names to IP addresses. An intruder who interferes with the proper operation of the DNS can mount a variety of attacks, including denial of service and password collection. There are a number of vulnerabilities.

Source: *Security Problems in the TCP/IP Protocol Suite*, S.M. Bellovin 1989
https://www.cs.columbia.edu/~smb/papers/ipext.pdf

We have a lot of the same problems in DNS today

Plus some more caused by middle-boxes, NAT, DNS size, DNS inspection

- DNS must allow both UDP and TCP port 53
- **Your DNS servers must have updated software, see DNS flag days**
  https://dnsflagday.net/ after which kludges will be REMOVED!
- **Use DNSSEC now!**

SNMP Problems

5.5 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) [37] has recently been defined to aid in network management. Clearly, access to such a resource must be heavily protected. The RFC states this, but also allows for a null authentication service; this is a bad idea. **Even a ‘‘read-only’’ mode is dangerous;** it may expose the target host to netstat-type attacks if the particular Management Information Base (MIB) [38] used includes sequence numbers. (The current standardized version does not; however, the MIB is explicitly declared to be extensible.)

Source: *Security Problems in the TCP/IP Protocol Suite*, S.M. Bellovin 1989
https://www.cs.columbia.edu/~smb/papers/ipext.pdf

True - still there, still useful, still dangerous – use SNMPv3!

If you must use SNMPv2 then at least put it into separate VLAN! 🚩

local networks

> 6.1 Vulnerability of the Local Network Some local-area networks, notably the Ethernet networks, are extremely vulnerable to eavesdropping and host-spoofing. If such networks are used, physical access must be strictly controlled. It is also unwise to trust any hosts on such networks if any machine on the network is accessible to untrusted personnel, unless authentication servers are used. If the local network uses the Address Resolution Protocol (ARP) [42] more subtle forms of host-spoofing are possible. In particular, it becomes trivial to intercept, modify, and forward packets, rather than just taking over the host's role or simply spying on all traffic.

Today we can send VXLAN spoofed packets across the internet layer 3 and inject ARP behind firewalls, in some cloud infrastructure cases ...

A Look Back at "Security Problems in the TCP/IP Protocol Suite" – about 1989 + 15 years = 2004

IPv6 is more/less secure than IPv4

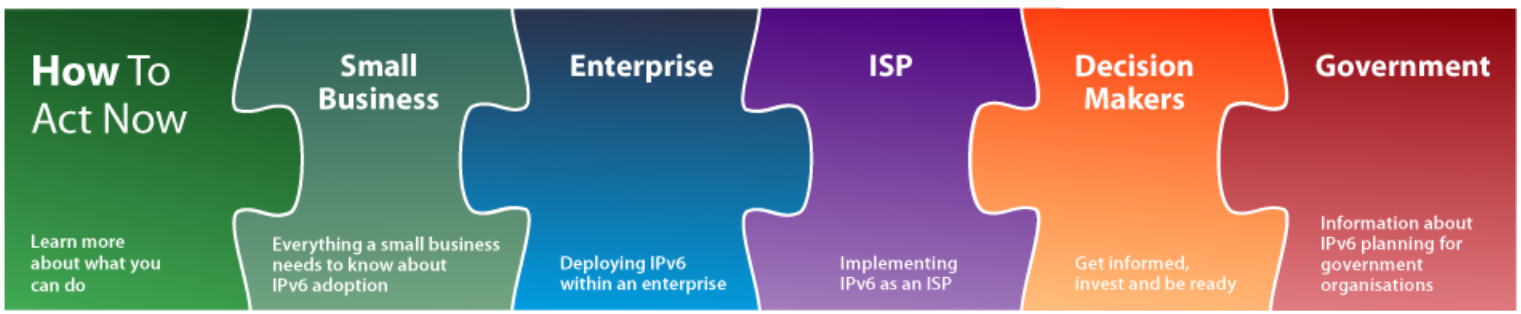
There are two big misconceptions about IPv6 security:

- IPv6 is more secure than IPv4
- IPv6 is less secure than IPv4

  Neither are true. Both assume that comparing IPv6 security with IPv4 security is meaningful. It is not.

Source: David Holder at, https://blog.apnic.net/2019/03/18/common-misconceptions-about-ipv6-security/

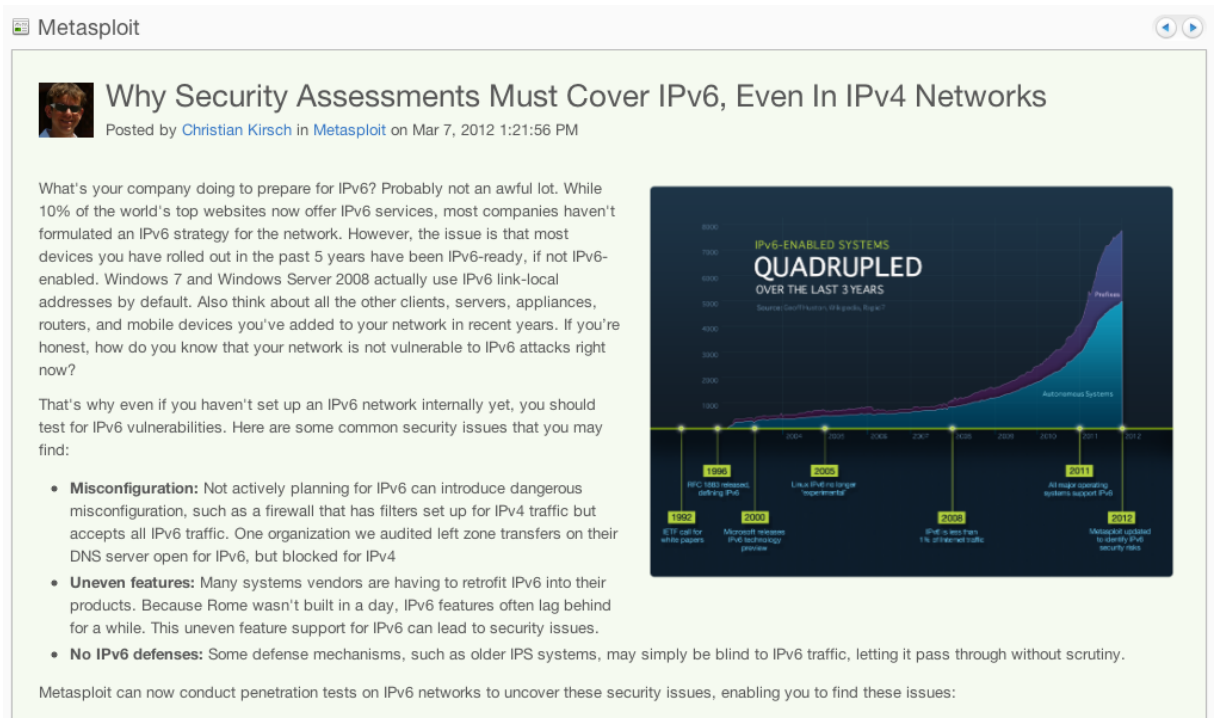
IPv6 is already in your network!



Picture from the IPv6 Act Now web site, RIPE NCC

- You have both, you will keep on having both
- Unless you have very strict control and turn one or the other OFF always, you have both IPv4 and IPv6 in your network!
- My suggestion, realize IPv6 is here, take control

Hacking IPv6



Metasploit

Why Security Assessments Must Cover IPv6, Even In IPv4 Networks

Posted by Christian Kirsch in Metasploit on Mar 7, 2012 1:21:56 PM

What's your company doing to prepare for IPv6? Probably not an awful lot. While 10% of the world's top websites now offer IPv6 services, most companies haven't formulated an IPv6 strategy for the network. However, the issue is that most devices you have rolled out in the past 5 years have been IPv6-ready, if not IPv6-enabled. Windows 7 and Windows Server 2008 actually use IPv6 link-local addresses by default. Also think about all the other clients, servers, appliances, routers, and mobile devices you've added to your network in recent years. If you're honest, how do you know that your network is not vulnerable to IPv6 attacks right now?

That's why even if you haven't set up an IPv6 network internally yet, you should test for IPv6 vulnerabilities. Here are some common security issues that you may find:

- **Misconfiguration:** Not actively planning for IPv6 can introduce dangerous misconfiguration, such as a firewall that has filters set up for IPv4 traffic but accepts all IPv6 traffic. One organization we audited left zone transfers on their DNS server open for IPv6, but blocked for IPv4
- **Uneven features:** Many systems vendors are having to retrofit IPv6 into their products. Because Rome wasn't built in a day, IPv6 features often lag behind for a while. This uneven feature support for IPv6 can lead to security issues.
- **No IPv6 defenses:** Some defense mechanisms, such as older IPS systems, may simply be blind to IPv6 traffic, letting it pass through without scrutiny.

Metasploit can now conduct penetration tests on IPv6 networks to uncover these security issues, enabling you to find these issues:

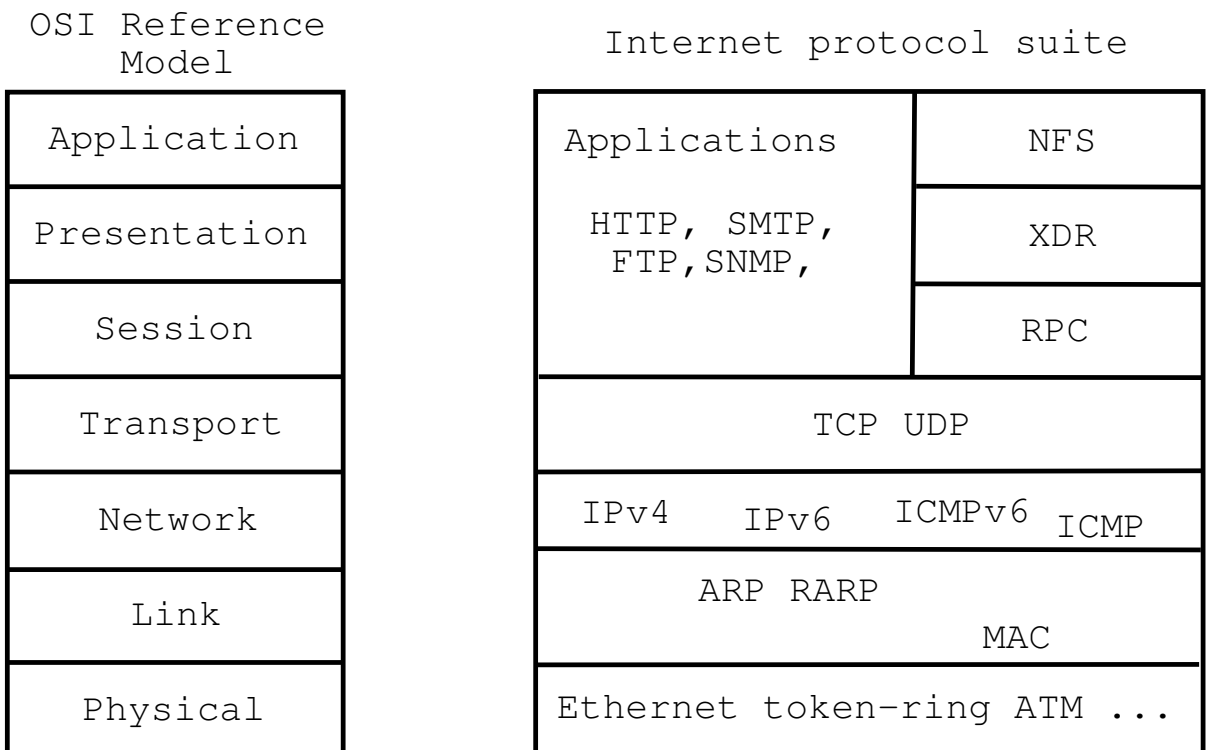
Source: Metasploit – NOTE THE DATE 2012!

Even 10 years ago we had IPv6 enabled systems running and communicating in our IPv4 networks

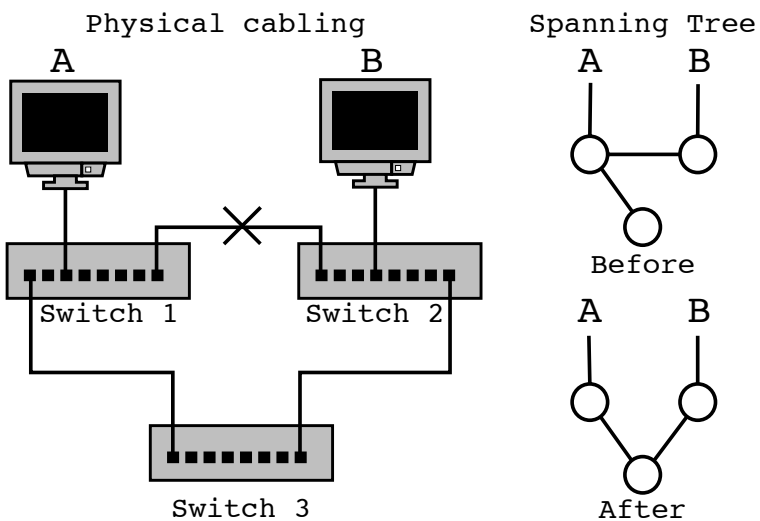
Networks are Built from Components

Photo by Eugen Str on Unsplash

Protocols: OSI and Internet model

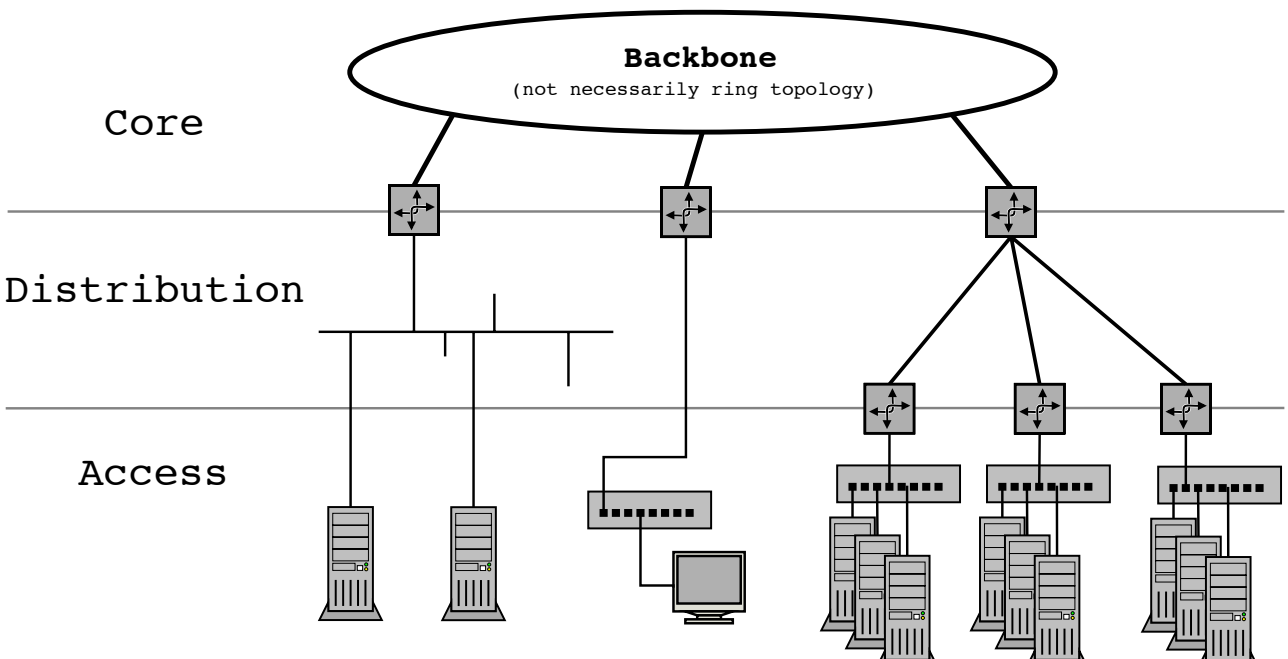


Topologies og Spanning Tree Protocol



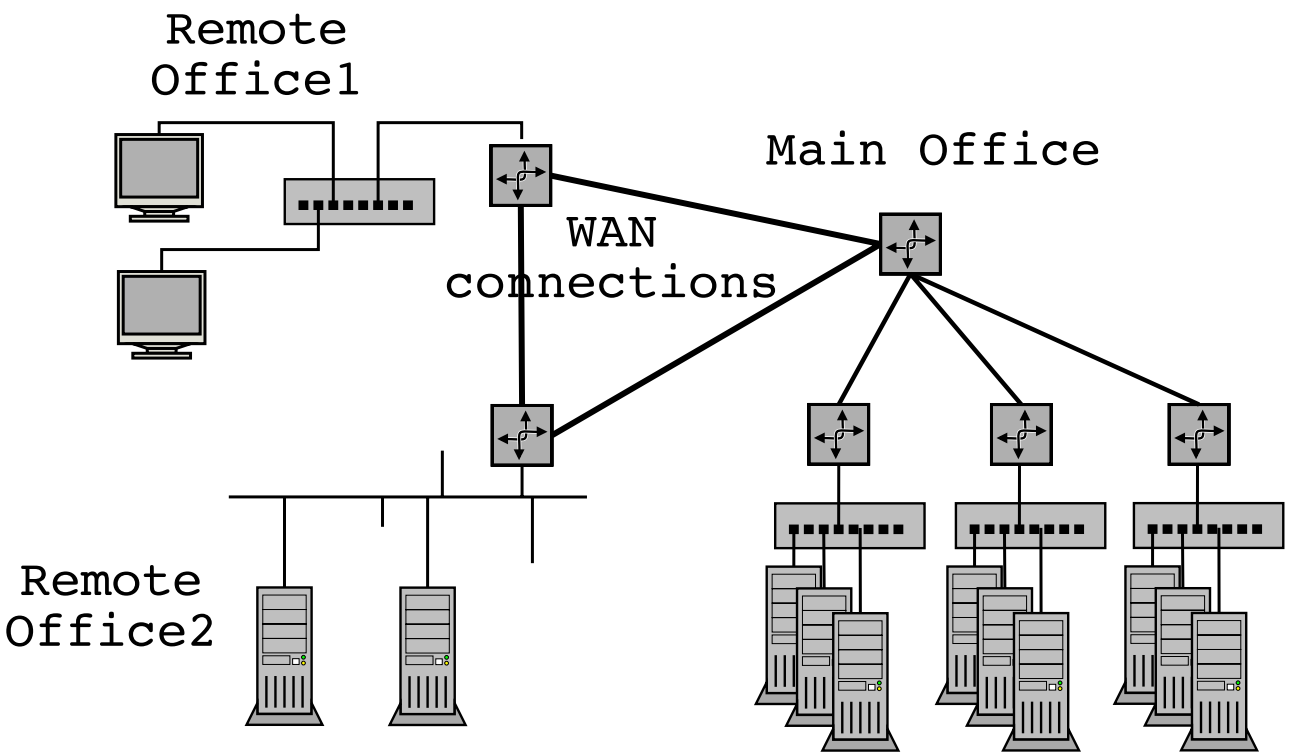
Se more about Ethernet and networks in the classic
Radia Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*

Core, Distribution og Access net



May seem old, and today multiple designs are pushed by vendors

Bridges and routers



Best Current Practice

Lets get this out of the way immediately, you should already be doing

- Network segmentation and filtering – we could write a book about this! 🚩
- Monitor your network – both bandwidth, error, netflow etc. 🚩
- Take control of your network, no more admin/admin logins on core devices 🚩
- Turn on authentication for protocols – routing protocols but also any http service within your org 🚩
- Configure host-based firewalls 🚩
- Control DNS – internally and externally, recursive, authoritative etc. 🚩

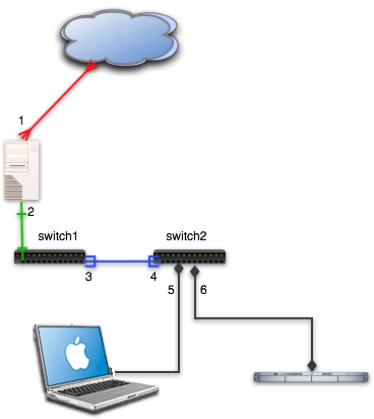
This goes for IPv4-only, IPv6-only, and mixed networks!

Walking through the stack

- Lets try to do this in a more structured way

Photo by Kelly Sikkema on Unsplash

Sample Network



Our network will be similar to regular networks, as found in enterprises

I have an isolated network, allowing us to sniff and mess with hacking tools

Will use a mix of my portable Wi-Fi using provider 3.dk WITH IPv6 and my internet in a box, portable infrastructure

Internet in a Box

The main purposes for bringing this box, is to show

- These are standard devices, Juniper EX3300 cheap oldish, works great
- Managed switches are a must! You can learn by buying cheap ones, like the TP-Link T1500G-10PS shown, VLAN, SNMP, Syslog ...
- Multiple systems created using PC Engines APU2C4 (really D4) running OpenBSD, Unbound, Suricata, Zeek, DHCP, router advertisement, PF firewall - explicit and nice ICMPv6 filtering ...
- Attack systems compact PCs or laptop
- Creating a home lab is not expensive, bought the Arista 7150 24-port 10G used on ebay

You should have similar (or better) devices in your production network, and they can be configured to do a LOT more than you use them for right now

IPv6 Neighbor Discovery Protocol (NDP)

OSI	IPv4	IPv6
Network	IP / ICMP	IPv6 / ICMPv6
Link	ARP	
Physical	Physical	Physical

Address Resolution Protocol (ARP) is replaced

NDP expands on the ARP concept, similar command `arp -an` compared to `ndp -an`

Can do some things we knew from DHCPv4 still DHCPv6 exist

Note ICMPv6 often need to be added to firewall rules for NDP! 🚩

ARP vs NDP

So at the low level, near the hardware we have protocols connecting IP addreses with MAC addresses, Ethernet and Wi-Fi are commonly found

```
hlk@bigfoot:basic-ipv6-new$ arp -an
? (10.0.42.1) at 0:0:24:c8:b2:4c on en1 [ethernet]
? (10.0.42.2) at 0:c0:b7:6c:19:b on en1 [ethernet]

hlk@bigfoot:basic-ipv6-new$ ndp -an
Neighbor                        Linklayer Address  Netif Expire    St Flgs Prbs
::1                             (incomplete)         lo0 permanent R
2001:16d8:ffd2:cf0f:21c:b3ff:fec4:e1b6 0:1c:b3:c4:e1:b6 en1 permanent R
fe80::1%lo0                     (incomplete)         lo0 permanent R
fe80::200:24ff:fec8:b24c%en1  0:0:24:c8:b2:4c      en1 8h54m51s  S  R
fe80::21c:b3ff:fec4:e1b6%en1  0:1c:b3:c4:e1:b6     en1 permanent R
```

ARP and NDP problems

- This mapping is used in your operating system, keep a dynamic ARP/neighbor cache – a table
- Switches map devices to ports – tables
- Routers remember your IP, so it can send responses back – tables
- A table has a maximum size! This can cause problems 🚩
- This is all done without ANY security – you can lie, attackers can lie
- See ARP spoofing and a sample tool https://en.wikipedia.org/wiki/ARP_spoofing and https://en.wikipedia.org/wiki/DSniff

Secure Neighbor Discovery Protocol

> The Secure Neighbor Discovery (SEND) protocol is a security extension of the Neighbor Discovery Protocol (NDP) in IPv6 defined in RFC 3971 and updated by RFC 6494.

Source: https://en.wikipedia.org/wiki/Secure_Neighbor_Discovery

- SEND Secure NDP is available, but quite complex ... who uses it?
- Not widely available, source: RIPE NCC IPv6 Security training April 2021
- *a solution that is non-trivial to deploy*, source: RFC7113
- Cisco IPv6 Secure Neighbor Discovery

  https://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2mt/ip6-send.html
- Juniper Secure IPv6 Neighbor Discovery

  https://www.juniper.net/documentation/us/en/software/junos/neighbor-discovery/topics/topic-map/ipv6-secure-neighbor.html

https://en.wikipedia.org/wiki/Secure_Neighbor_Discovery

Tcpdump and Wireshark demo

"The quieter you become, the more you are able to hear".

Source: Kali Linux

- Lets try to listen a bit

Attacking IPv6

Example toolkits:

- Nmap supports IPv6 https://nmap.org
- THC-IPV6-ATTACK-TOOLKIT https://github.com/vanhauser-thc/thc-ipv6
- SI6 Networks' IPv6 toolkit is a set of IPv6 security assessment and trouble-shooting tools https://www.si6networks.com/research/tools/ipv6toolkit/
- Chiron is an IPv6 Security Assessment Framework, written in Python and employing Scapy https://github.com/aatlasis/Chiron
- Cool little script and concept found recently https://github.com/milo2012/ipv4Bypass

Scanning for IPv6 hosts

- Yes, naive bruteforce may not work when subnets in IPv6 are /64s
- Using tools like Scan6 with predictable patterns work because humans
- If on local network we can wait for NDP traffic, hosts communicating
- In other cases we can lure people to our DNS server, NTP server (Shodan did this), etc.

Interesting talk about this, applying statistical methods:
TROOPERS19: *IPv666 – Address of the Beast* slides not there, but video is
https://troopers.de/troopers19/agenda/ymwjsm/
Tool at https://github.com/lavalamp-/ipv666

References this: *Target Generation for Internet-wide IPv6 Scanning* Austin Murdock, Frank Li, Paul Bramsen, Zakir Durumeric, Vern Paxson https://austinmurdock.com/6Gen.pdf

Similarities between IPv4 and IPv6 security

- Rogue DHCP servers can be done in both, plus false router advertisements in IPv6
- MAC address overflow can be done in both
- Unfiltered access can be abused
- DNS spoofing can be abused
- Sniffing unencrypted traffic is the same
- MITM Attacks are the same 🚩
- Application attacks are the same! Example Web attack over IPv4/IPv6 - often address family doesn't matter 🚩
- Flooding attacks are possible at various places

Disparities between IPv4 and IPv6 security, example

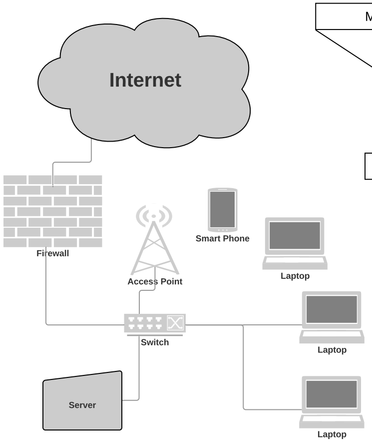
> The functionality provided by IPv6's Type 0 Routing Header can be exploited in order to achieve traffic amplification over a remote path for the purposes of generating denial-of-service traffic. This document updates the IPv6 specification to deprecate the use of IPv6 Type 0 Routing Headers, in light of this security concern.

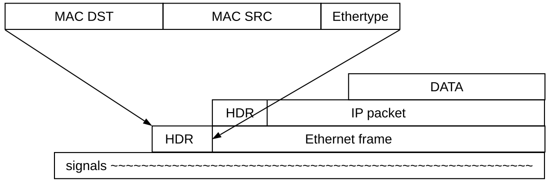
Source RFC5095

- Routing headers – flexible, but hard to filter
  Updated RFC8200 *Internet Protocol, Version 6 (IPv6) Specification* recommend order for those
- IPv6 Type 0 routing header, fixed
  Deprecated officially in RFC 5095 https://www.rfc-editor.org/rfc/rfc5095.txt
- Other stuff better specified, like RFC5722 – see later

We are relying on vendors to create updated software, but must install those updates

Protection, building secure and robust networks





Ethernet frames contain packets

```
 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|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet IPv4 Packet Header

- We should prefer security mechanisms that does NOT require us to keep patching every month
- Can we change our networks to avoid this? Yes!

Internet Network Knowledge

To work with network security the following protocols are the bare minimum to know about.

- ARP Address Resolution Protocol for IPv4
- NDP Neighbor Discovery Protocol for IPv6
- IPv4 & IPv6 – the basic packet fields source, destination,
- ICMPv4 & ICMPv6 Internet Control Message Protocol
- UDP User Datagram Protocol
- TCP Transmission Control Protocol
- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System

These protocols are part of the Internet Protocol suite, or TCP/IP for short.

Operational Security Considerations for IPv6 Networks

Internet Engineering Task Force (IETF)
Request for Comments: 9099
Category: Informational
ISSN: 2070-1721

É. Vyncke
Cisco
K. Chittimaneni

M. Kaeo
Double Shot Security
E. Rey
ERNW

August 2021

Operational Security Considerations for IPv6 Networks

Source: https://www.rfc-editor.org/rfc/rfc9099.txt

- Fantastic reference
- Another from RIPE NCC, 191 slides! IPv6 Security Training Course April 2021, https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf

Get IPv6 prefix!

You can ask RIPE NCC for an IPv6 provider independent prefix, through a LIR – I have a LIR!

- YOU can't request directly, but need to find a RIPE NCC member to request it
  Hint: Zencurity Aps is a member
- It will cost you about EUR 100 per year and you will get minimum /48
- You can move this space from provider to provider
  more easily than migrating from their IP space to some new providers space
- You can have this announced via multiple providers – redundancy
- Read more about this at:
  https://www.ripe.net/manage-ips-and-asns/ipv6/request-ipv6/how-to-request-an-ipv6-pi-assignment

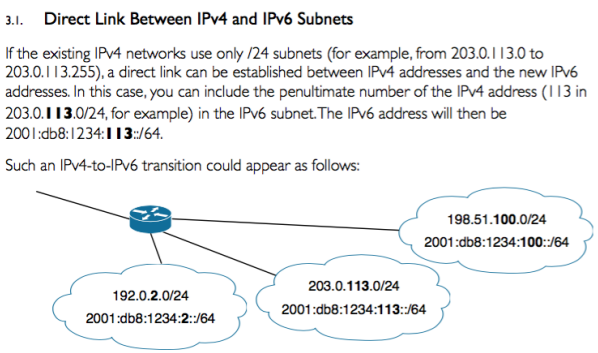
Address planning – helps security for both IPv4 and IPv6!

> IPv6 address allocations and overall architecture are important parts of securing IPv6. Initial designs, even if intended to be temporary, tend to last much longer than expected. Although IPv6 was initially thought to make renumbering easy, in practice, it may be extremely difficult to renumber without a proper IP Address Management (IPAM) system. [RFC7010] introduces the mechanisms that could be utilized for IPv6 site renumbering and tries to cover most of the explicit issues and requirements associated with IPv6 renumbering. **A key task for a successful IPv6 deployment is to prepare an addressing plan. Because an abundance of address space is available, structuring an address plan around both services and geographic locations allows address space to become a basis for more structured security policies to permit or deny services between geographic regions**. [RFC6177] documents some operational considerations of using different prefix sizes for address assignments at end sites.

Source: RFC 9099

- You have space, use it!

Network Architecture and Address planning



3.1. **Direct Link Between IPv4 and IPv6 Subnets**

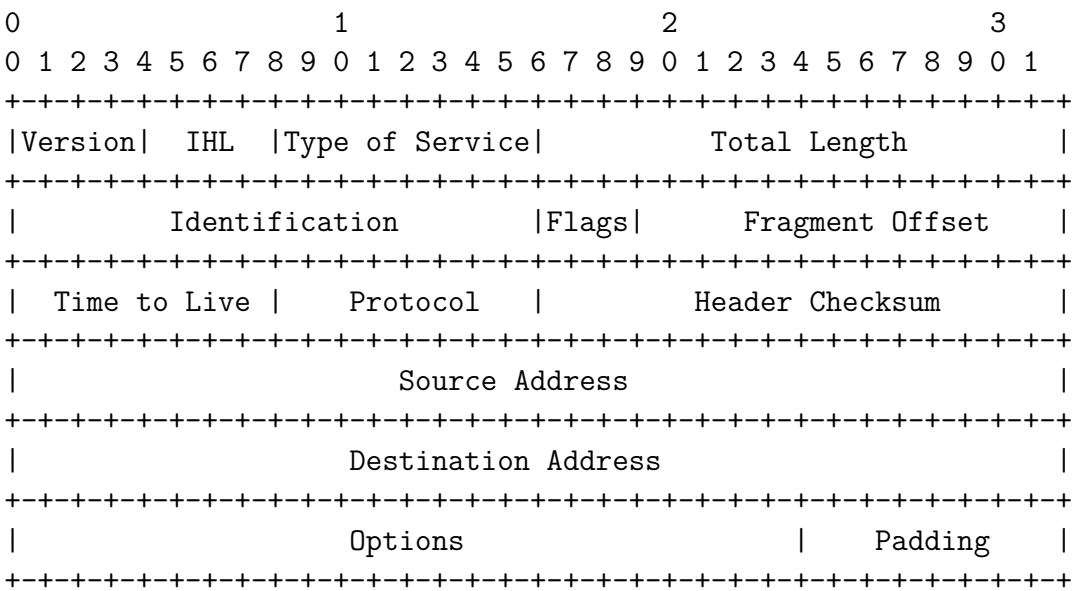
If the existing IPv4 networks use only /24 subnets (for example, from 203.0.113.0 to 203.0.113.255), a direct link can be established between IPv4 addresses and the new IPv6 addresses. In this case, you can include the penultimate number of the IPv4 address (113 in 203.0.**113**.0/24, for example) in the IPv6 subnet. The IPv6 address will then be 2001:db8:1234:**113**::/64.

Such an IPv4-to-IPv6 transition could appear as follows:

Source: picture from Surfnet Preparing and IPv6 Address Plan

- Take the opportunity to re-design your network! Create a design, consider it green field, work towards it!
- Use /127 for point-to-point links, add loopback addresses on routers, allows filtering of access to management
- You can also make parts IPv6-only, Veronika McKillop at TROOPERS19 *Microsoft IT (secure) journey to IPv6-only* https://troopers.de/troopers19/agenda/h7sv7v/

Enable More Packet filtering



Packet filtering can be done one single packets – stateless filtering

We can save information about direction and ongoing traffic – stateful filtering/firewalling

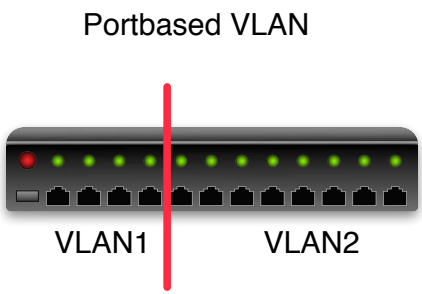
Recommend host based firewalls too!

Example UFW Uncomplicated Firewall

```
root@debian01:~# ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian01:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@debian01:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Together with Firewalls - VLAN Virtual LAN



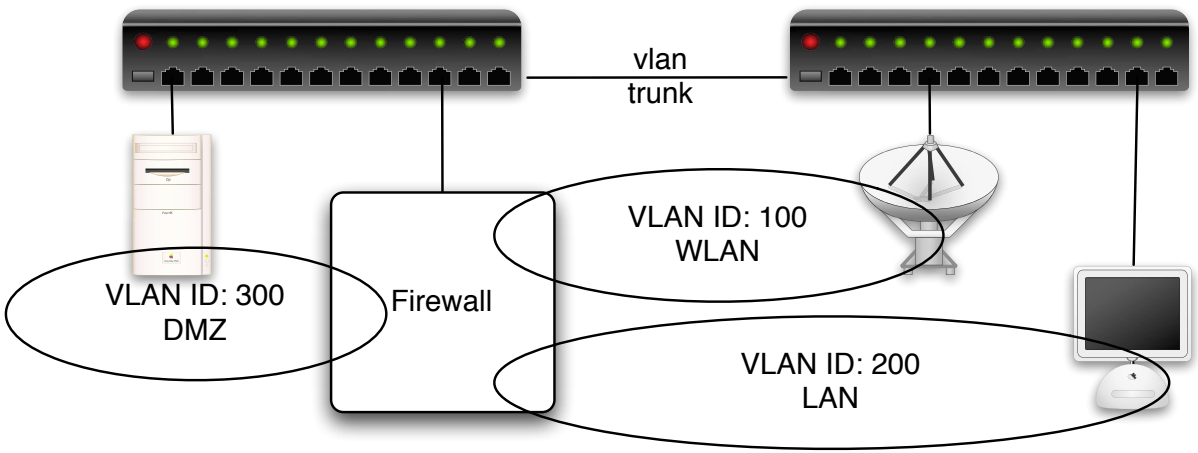
Some ports belong in groups together – cannot communicate between groups

Port 1-4 are a single LAN – virtual LAN

Remaining ports are another VLAN

A router or firewall is needed to transfer packets between VLANs – with filters

IEEE 802.1q – virtual LAN



Standard is named IEEE 802.1q VLAN tagging on Ethernet frames

VLAN trunking allows multiple VLANs to use the same ports, between switches

Take control of your core network services

Core Network Services

- These are critical for the network to operate correctly. IP packets may flow in the network, but if these services don't reply or aren't configured correctly, users and devices won't be able to connect, authentication services may fail, and network applications won't be accessible.
- They are:
  1. DNS
  2. DHCP
  3. NTP

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Source:

https://nsrc.org/workshops/2018/tenet-nsrc-cndo/networking/cndo/en/presentations/Campus_Operations_BCP.pdf

Unbound and NSD

Unbound is a validating, recursive, caching DNS resolver. It is designed to be fast and lean and incorporates modern features based on open standards.

To help increase online privacy, Unbound supports DNS-over-TLS which allows clients to encrypt their communication. In addition, it supports various modern standards that limit the amount of data exchanged with authoritative servers.

https://www.nlnetlabs.nl/projects/unbound/about/

My preferred local DNS server. We will now stop and look at this configuration file and function.

Also check out uncensored DNS and his DNS over TLS setup!
Even has pinning information available:
https://blog.censurfridns.dk/blog/32-dns-over-tls-pinning-information-for-unicastcensurfridnsdk/

Perform Network Management

Network management is the process of administering and managing computer networks. Services provided by this discipline include fault analysis, performance management, provisioning of networks and maintaining the quality of service. Software that enables network administrators to perform their functions is called network management software.

Source:

https://en.wikipedia.org/wiki/Network_management

Step 1: configure devices properly

You should always configure your devices properly

Turn on SNMP, probably SNMPv2

Turn on LLDP Link Layer Discovery Protocol – vendor-neutral

http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

Centralized syslog and SNMP traps

Router protection filters, in general on devices allow only management from specific prefixes/sources

And updated firmware, HTTPS and SSH only etc. the usual stuff

Centralized management SSH, Jump hosts

A jump server, jump host or jumpbox is a computer on a network used to access and manage devices in a separate security zone. The most common example is managing a host in a DMZ from trusted networks or computers.

https://en.wikipedia.org/wiki/Jump_server

OpenSSH client config with jump host

My recommended SSH client settings, put in `$HOME/.ssh/config`:

```
Host *
    ServerAliveInterval=30
    ServerAliveCountMax=30
    NoHostAuthenticationForLocalhost yes
    HashKnownHosts yes
    UseRoaming no

Host jump-01
  Hostname 10.1.2.3
  Port 12345678

Host fw-site-01 10.1.2.5
  User hlk
  Port 34
  Hostname 10.1.2.5
  ProxyCommand ssh -q -a -x jump-01 -W %h:%p
```

I configure fw using both hostname and IP,
then I can use name, and any program using IP get this config too

Config example: SNMP

```
snmp {
    description "SW-CPH-01";
    location "Interxion, Ballerup, Denmark";
    contact "noc@zencurity.com";
    community yourcommunitynotmine {
        authorization read-only;
        clients {
            10.1.1.1/32;
            10.1.2.2/32;
        }
    }
}
```

If you must use SNMPv2 then at least put it into separate VLAN! 🚩

Rogue DHCP servers and devices

Common problem in networks is people connecting devices with DHCPD servers

In general make sure to segment networks

Start to use port security on switches, including DHCP snooping
https://en.wikipedia.org/wiki/DHCP_snooping

Can also be used to prevent people from adding unmanaged switches

In general, your devices have features – use them

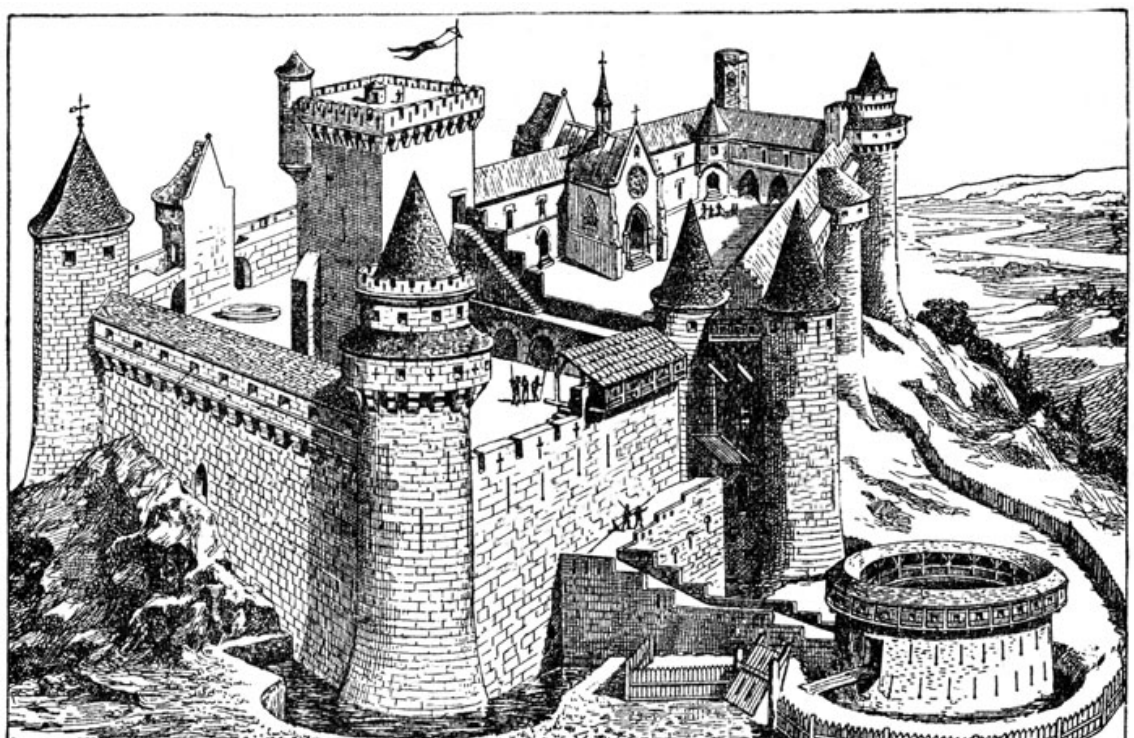
Port Security

Snooping on the network ports, and only allow what is needed

Ideas

- Only allow 0x0800 IPv4 on some ports?
- Only allow 0x86DD IPv6 on some ports?
- Which types SHOULD we allow?

Defense in depth



Picture originally from: http://karenswhimsy.com/public-domain-images

Helpful functions are available

First hop security Cisco

```
ipv6 snooping logging packet drop

interface GigabitEthernet1/0/1
    switchport mode access
    ipv6 nd raguard
    ipv6 dhcp guard
```

- RA Guard RFC6105 *IPv6 Router Advertisement Guard* and
  RFC7113 *Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*
  Only allow router advertisements on configured ports
- DHCPv6 guard only allow DHCP servers on specific ports
- Source and Prefix Guard

Wait a minute, have you turned similar features for IPv4? Many have NOT! 🚩

Example port security MAC and IPv4

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/1 mac-limit 4
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 mac-limit 4
set interface ge-0/0/1 persistent-learning
set interface ge-0/0/8 dhcp-trusted
set vlan employee-vlan arp-inspection
set vlan employee-vlan examine-dhcp
set vlan employee-vlan mac-move-limit 5
```

Source: Overview of Port Security, Juniper

https://www.juniper.net/documentation/en_US/junos/topics/example/overview-port-security.html

IPv6 First-Hop Security Configuration

> IPv6 Source Guard and IPv6 Prefix Guard are Layer 2 snooping features that validate the source of IPv6 traffic. IPv6 Source Guard blocks any data traffic from an unknown source. For example, one that is not already populated in the binding table or previously learned through Neighbor Discovery (ND) or Dynamic Host Configuration Protocol (DHCP) gleaning. IPv6 Prefix Guard prevents home-node sourcing traffic outside of the authorized and delegated traffic.

Source: *IPv6 First-Hop Security Configuration Guide*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6f-xe-16-book/ip6-src-guard.html

- Guard functionality in general are based on understanding some protocol, like RA, DHCP, ARP or NDP
- Without proper communication the device(s) cannot be allowed to send traffic
- So you are a device that got an IP great, you can only use this IP for communication

Limit bad packets from spoofed sources! Avoid rogue devices re-routing traffic on layer 2.

Creating an Access Control List (ACL)

```
(config)#ipv6 access-list RA-GUARD
(config-ipv6-acl)#sequence 3 deny icmp any any router-advertisement
(config-ipv6-acl)#sequence 6 permit ipv6 any any
(config-ipv6-acl)#exit
(config)#interface FastEthernet0/5
(config-if)#ipv6 traffic-filter RA-GUARD in
```

Source: example copied from RIPE NCC IPv6 Security Training materials:
https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf

- Best practice, and not that hard to do
- ACL, filtering and firewalling will create longer lasting protection
- Paired with a nice address plan you can easily put restrictions on traffic flow, without hurting functionaliy or the business
- Does ANY client in ANY office NEEEEEED to connect to ANY UPS, Virtualisation and printer across the world ...

Junos Enabling ND Inspection

To enable neighbor discovery inspection on a VLAN:

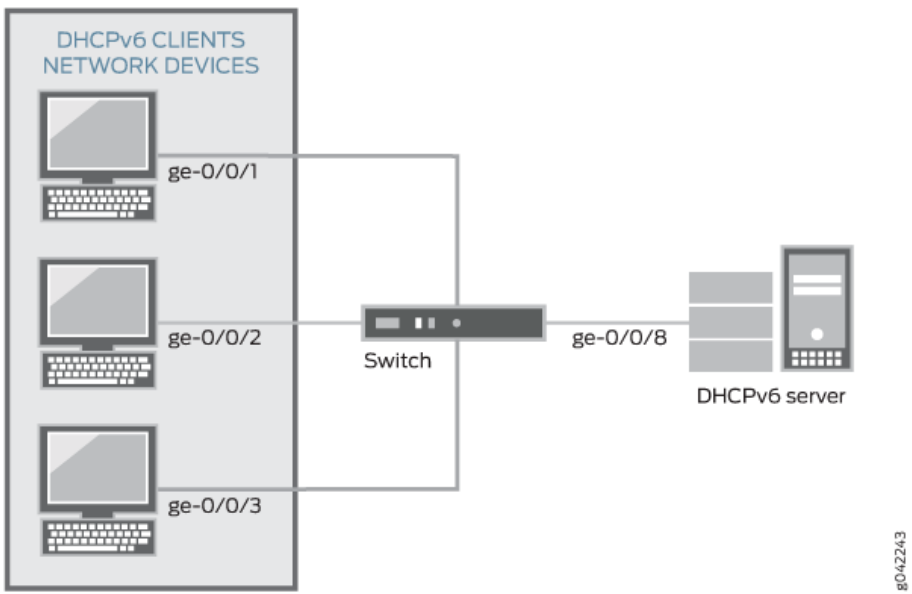
```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set  neighbor-discovery-inspection
```

NOTE: DHCPv6 snooping is enabled automatically when neighbor discovery inspection is configured. There is no explicit configuration required for DHCPv6 snooping.

Source:

https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/port-security-nd-inspection.html

Allowing services to function, eliminate threats from rogue devices



Source: Picture from Juniper

https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/example/port-security-protect-from-ipv6-spoofing.html

- TL;DR Upstream and trunk ports are allowed to have *servers* and *services*

RFC5722: Handling of Overlapping IPv6 Fragments

> IPv6 nodes transmitting datagrams that need to be fragmented MUST NOT create overlapping fragments. When reassembling an IPv6 datagram, if one or more its constituent fragments is determined to be an overlapping fragment, the entire datagram (and any constituent fragments, including those not yet received) MUST be silently discarded.

Source: RFC5722

- Better when expected behaviour is documented

RFC6980: Security Implications of IPv6 Fragmentation with IPv6 ND

> Abstract This document analyzes the security implications of employing IPv6 fragmentation with Neighbor Discovery (ND) messages. **It updates RFC 4861 such that use of the IPv6 Fragmentation Header is forbidden in all Neighbor Discovery messages**, thus allowing for simple and effective countermeasures for Neighbor Discovery attacks. Finally, it discusses the security implications of using IPv6 fragmentation with SEcure Neighbor Discovery (SEND) and formally updates RFC 3971 to provide advice regarding how the aforementioned security implications can be mitigated.

Source: RFC6980 *Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*

- Better when expected behaviour is documented
- This ensures that RA Guard cannot easily be circumvented
- See also RFC6105 *IPv6 Router Advertisement Guard*
  RFC7113 *Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*

Stateless firewall filter throw stuff away

```
hlk@MX-CPH-02> show configuration firewall filter all | no-more
/* This is a sample, better to use BGP flowspec or BGP based RTBH */
term edgeblocker {
    from {
        source-address {
            84.xx.xxx.173/32;
...
            87.xx.xxx.171/32;
        }
        destination-address {
            192.0.2.16/28;
        }
        protocol [ tcp udp icmp ];
    }
    then {
        count edge-block;
        discard;
    }
}
```

Hint: can also leave out protocol and then it will match all protocols

Stateless firewall filter limit protocols

```
term limit-icmp {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-100M;
        accept;
    }
}
term limit-udp {
    from {
        protocol udp;
    }
    then {
        policer UDP-1000M;
        accept;
    }
}
```

Routers also have extensive Class-of-Service (CoS) tools today, and in general rate limiting stuff is nice

Strict filtering for some servers, still stateless!

```
term some-server-allow {
    from {
        destination-address {
            192.0.2.0/24;
        }
        protocol tcp;
        destination-port [ 80 443 ];
    } then accept;
}
term some-server-block-unneeded {
    from {
        destination-address {
            192.0.2.0/24; }
        protocol-except icmp;  }
    then { count some-server-block; discard;
    }
}
```

Wut - no UDP, yes UDP service is not used on these servers

uRPF unicast Reverse Path Forwarding

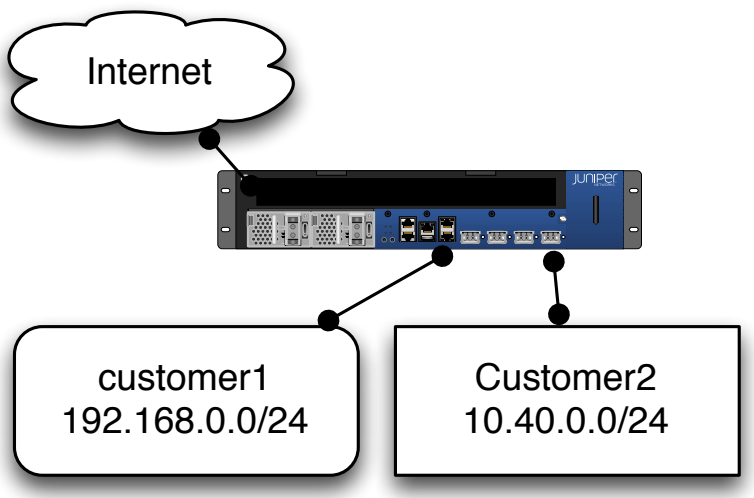
Reverse path forwarding (RPF) is a technique used in modern routers for the purposes of ensuring loop-free forwarding of multicast packets in multicast routing and to help prevent IP address spoofing in unicast routing.

Source: http://en.wikipedia.org/wiki/Reverse_path_forwarding

Configuring Unicast RPF Strict Mode

In strict mode, unicast RPF checks whether the incoming packet has a source address that matches a prefix in the routing table, **and whether the interface expects to receive a packet with this source address prefix.**

Strict vs loose mode RPF




```
user@router# show interfaces
ge-0/0/0 {
        unit 2 {
                family inet {
                        rpf-check fail-filter rpf-special-case-dhcp;
                        address 192.168.0.254/24;
                }
        }
}
ge-0/0/1 {
        unit 2 {
                family inet {
                        rpf-check fail-filter rpf-special-case-dhcp;
                        address 10.40.0.254/24;
                }
        }
}
```

Routing Security

- Use MD5 passwords or better authentication for routing protocols 🚩
- TTL Security – avoid routed packets
- Max prefix – of course, only allow expected networks
- Prefix filtering – only parts of IPv6 space is used
- TCP Authentication Option [RFC 5925] replaces TCP MD5 [RFC 2385]
- Turn ON RPKI for both IPv4 and IPv6 prefixes, 🚩
  https://nlnetlabs.nl/projects/rpki/about/
- Drop bogons on IPv4 and IPv6, article with multiple references YMMV
  https://theinternetprotocolblog.wordpress.com/2020/01/15/some-notes-on-ipv6-bogon-filtering/

Mutually Agreed Norms for Routing Security (MANRS)

> Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

Source: https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf

- Problems related to incorrect routing information
- Problems related to traffic with spoofed source IP addresses
- Problems related to coordination and collaboration between network operators
- Also BCP38 RFC2827 *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

You should all ask your internet providers if they know about MANRS, and follow it. We should ask our government and institutions to support and follow MANRS and good practices for network on the Internet

Conclusion

- Implement IPv6 – take control
- Read the Fine manuals – your devices already has a lot to offer
- Make incremental changes, configure security for new parts and VLANs in the network
  Over time the older ones will be phased out, replaced or can have the same configuration applied with little trouble
- Start from the bottom and from client ports, or from server ports if you like
- Learn some Linux and use open source projects, really, will save you thosands of USD/EUR/DKK

Questions?

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

Email: hlk@zencurity.com

Further literature

Primary literature used in my Communication and Network Security Class are these three books:

- *Applied Network Security Monitoring Collection, Detection, and Analysis*, 2014 Chris Sanders ISBN: 9780124172081 - shortened ANSM
- *Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems*, 3rd edition 2017, Chris Sanders ISBN: 9781593278021 - shortened PPA
- *Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali*. OccupyTheWeb, December 2018, 248 pp. ISBN-13: 978-1-59327-855-7 - shortened LBfH

Resources

Long list of various references follow, YMMV. I have found these useful in some way

- https://theinternetprotocolblog.wordpress.com/2020/11/28/ipv6-security-best-practices/
- https://insinuator.net/2019/02/ipv6-security-in-an-ipv4-only-environment/
  via https://mobile.twitter.com/enno_insinuator/status/1285681172719316992
- https://www.caida.org/catalog/papers/2016_dont_forget_lock/dont_forget_lock.pdf
  via https://twitter.com/Enno_Insinuator/status/1224147916022898689
- https://static.ernw.de/whitepaper/ERNW_Whitepaper68_Vulnerability_Assessment_Cisco_ACI_signed.pdf
  Classic with example of something locked down on IPv4 but not on IPv6
  I have found similar on management interfaces for a large network myself, if you came from a specific source port, you could connect to management on all core routers around the network. Router protection filter for IPv6 was not secure.

Further resources

- *IPv6 and IPv4 Threat Comparison and BestPractice Evaluation (v1.0)* Sean Convery (sean@cisco.com) Darrin Miller (dmiller@cisco.com) https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.7165&rep=rep1&type=pdf 43 pages short enough, nicely structured
- https://www.cisco.com/web/SG/learning/ipv6_seminar/files/02Eric_Vyncke_Security_Best_Practices.pdf Updated? Advanced https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKSEC-3200.pdf
- Mixed resources, maybe not useful
- https://www.varonis.com/blog/ipv6-security - Apply IPv4 best practices when applicable ... and IPv6 Security is not distinct from IPv4 security
- https://www.hpc.mil/images/hpcdocs/ipv6/infoblox-best-practices-for-ipv6-security-excerpt.pdf routing security and stuff
- https://www.nist.gov/publications/guidelines-secure-deployment-ipv6 from 2010, but maybe some good advice - and goes to show IPv6 security advise has been around for some time

Resources LIRs and others

Grateful to be part of such communities! Tried finding recent references, more can be found across their sites:

- RIPE April 2021, 191 pages!
  https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf
- ISOC 2019 https://www.internetsociety.org/deploy360/ipv6/security/faq/
- APNIC 2019 https://blog.apnic.net/2019/03/18/common-misconceptions-about-ipv6-security/
- May 2022 *Apple Platform security guide*, includes IPv6
  https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf
- *JANET IPv6 Technical Guide*, IPv4 security equivalence page 49
  https://repository.jisc.ac.uk/8349/1/janet-ipv6-technical-guide.pdf
- *Network Reconnaissance in IPv6 Networks* https://www.rfc-editor.org/rfc/rfc7707.txt
- RFC6092 2011 *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*
  https://datatracker.ietf.org/doc/html/rfc6092