



De technische werking van het Internet

1

Intro

- Ramon A.S. Pirbux
- 25+ jaar in ICT
- Eigenaar van NSOC.NL (Network Systems Operations Cyber Security) (voorheen IPTAC.NL)
- Netwerk en Security Consultant
- Cisco Trainer
- www.linkedin.com/in/rpirbux/
- <https://www.credly.com/users/ramon-pirbux/badges>
- www.nsoc.nl
- info@nsoc.nl
- +31 6 10062775 (mobile, whatsapp, telegram)

WWW.NSOC.NL

2

2

NSOC.NL - WEBINAR

Over welke onderwerpen gaan we praten?

Het Internet: een overzicht vanuit de helikopterperspectief.

Stappen van een fysieke internetinstallatie thuis:

- Bekabelde verbindingen
- Draadloze netwerken

Technische aspecten van surfen op het internet: een blik onder de motorkap.

- Protocollen: OSI en TCP/IP model, MAC, IPv4, IPv6, DHCP, ARP, NAT, DNS, ROUTING (IGP/EGP), Cloud, HTTP/HTTPS.

Tips voor beveiliging

Praktische oefeningen en labo's.

Vervolg opties

WWW.NSOC.NL

3

3

NSOC.NL - WEBINAR

De motivatie achter deze sessie(s)

Bewustwording en kennisvergaring.

Tekort aan bekwame ICT-specialisten.

Opkomst van nieuwe technologieën.

Verschillende soorten (nieuwe) cyberaanvallen.

De rol van Kunstmatige Intelligentie (AI).

En voornamelijk het beantwoorden van uw vragen.

WWW.NSOC.NL

4

4

NSOC.NL - WEBINAR

Vragen ?

- Slides komen op www.nsoc.nl/blog/

NSOC.NL - WEBINAR

Basiskennis ICT netwerken - Begrippen

- Protocollen en modellen
- **Protocollen** zijn gestandaardiseerde regels en afspraken die bepalen hoe gegevens worden verzonden, ontvangen en verwerkt binnen een communicatienetwerk.
 - Voorbeelden zijn: DHCP, ARP, RIP, EIGRP, ISIS, OSPF, BGP4 en nog heel veel meer.
- Het **OSI-model** (Open Systems Interconnection) is een conceptueel raamwerk dat wordt gebruikt om de functies van een telecommunicatie- of computersysteem te begrijpen en te standaardiseren.

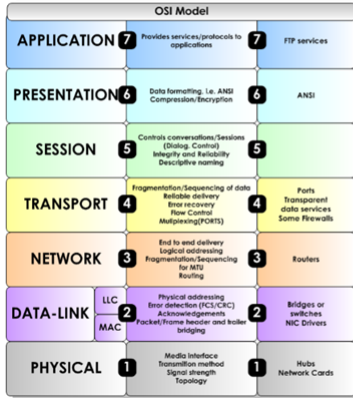
Het model verdeelt deze functies in **zeven** afzonderlijke lagen, waarbij elke laag een specifieke rol speelt in de verwerking en overdracht van gegevens
- Het **TCP/IP-model**, ook wel het Internet Protocol Suite genoemd, is een conceptueel raamwerk voor communicatieprotocollen dat wordt gebruikt in netwerken, vooral op het Internet. Deze bestaat uit **vier** afzonderlijke lagen.

NSOC.NL - WEBINAR

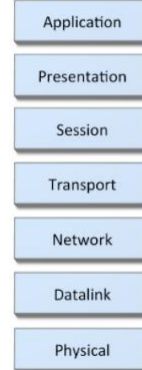
Basiskennis ICT netwerken - Modellen

NSOC.NL
NETWORK AND CYBER SECURITY

The OSI Model (Open Systems Interconnection)



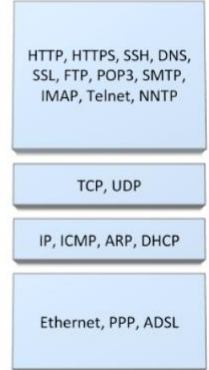
OSI Model



Internet Model



Internet Protocols



WWW.NSOC.NL

7

7

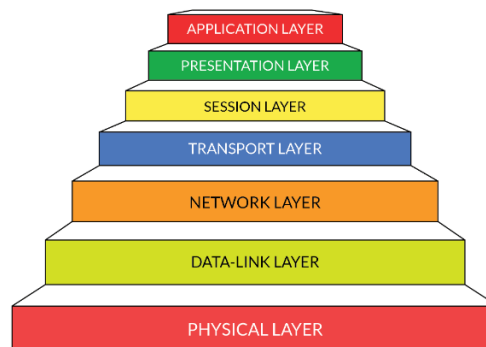
NSOC.NL - WEBINAR

Basiskennis ICT netwerken - communicatie

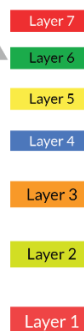
NSOC.NL
NETWORK AND CYBER SECURITY

OSI MODEL

Client Side



Server Side



WWW.NSOC.NL

8

8

NSOC.NL - WEBINAR

Theorie over switching

NSOC.NL
NETWORK AND CYBER SECURITY

- Voor effectieve communicatie binnen je huisnetwerk (LAN) gebruiken zowel de modem als alle aangesloten apparaten, naast het toegekende IP-adres, ook een MAC-adres. Dit proces staat bekend als lokale switching.
- *Elke interface of ethernet-poort van de stations heeft een uniek MAC-adres. Dit **MAC-adres bestaat uit 48 bits** en wordt hexadecimaal uitgedrukt. Dankzij deze unieke MAC-adressen kunnen stations en de modem binnen het LAN zich van elkaar onderscheiden. De communicatie tussen de stations en de modem in het LAN is zo efficiënt, omdat duidelijk is welke stations met elkaar in verbinding staan.*
- Door deze methode van lokale switching binnen je LAN, waarbij zowel het IP- als het MAC-adres worden gebruikt, wordt de communicatie binnen je thuisnetwerk gestroomlijnd en beveiligd
- Dit 48-bits, hexadecimaal weergegeven adres, maakt elk station en de modem binnen het LAN uniek, wat essentieel is voor de onderlinge communicatie.
- **DEMO: MAC adressen laten zien (ipconfig /all)**

WWW.NSOC.NL

9

9

NSOC.NL - WEBINAR

Theorie over IP-adressen

NSOC.NL
NETWORK AND CYBER SECURITY

Om te kunnen surfen op het Internet heeft je station een publieke IP-adres nodig.

Er bestaan 2 type IP-adressen: IPv4 en IPv6

IPv4 is 32 bits en wordt geschreven in decimal.

IPv6 is 128 bits en wordt in hexadecimal geschreven.

IPv4 kan opgedeeld worden in 3 types:

- APIPA (Automatic Private IP Addressing) – 169.254.x.x/16
- Private (RFC1918) – 10.0.0.0/8, 172.16.0.0/12 en de 192.168.0.0/16)
- Publieke IP-adressen

DEMO:

[Learn Numbering Systems in 1 Minute \(youtube.com\)](#)

IP adres en routing table (ipconfig /all – netstat –rn)

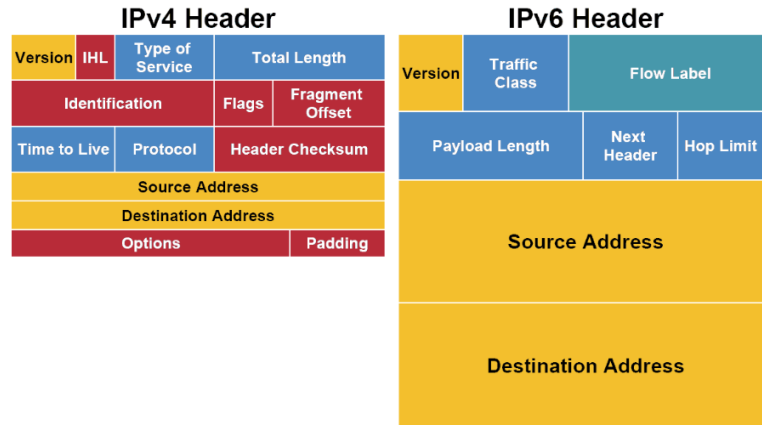
WWW.NSOC.NL

10

10

NSOC.NL - WEBINAR

IPv4 en IPv6 structuren



WWW.NSOC.NL

11

11

Essentieel voor routing

NSOC.NL
 NETWORK AND CYBER SECURITY

Routing is het proces waarbij netwerkapparatuur (routers) data van het ene naar het andere netwerk stuurt door de meest efficiënte route te bepalen.

Het huisnetwerk is het ene netwerk en het Internet is het andere netwerk.

Voor routing hebben stations het volgende nodig:

- IP-adres
- Subnetmasker
- Gateway (default gateway)

Om op internet te surfen, hebben stations ook DNS-servers nodig.

DEMO



WWW.NSOC.NL

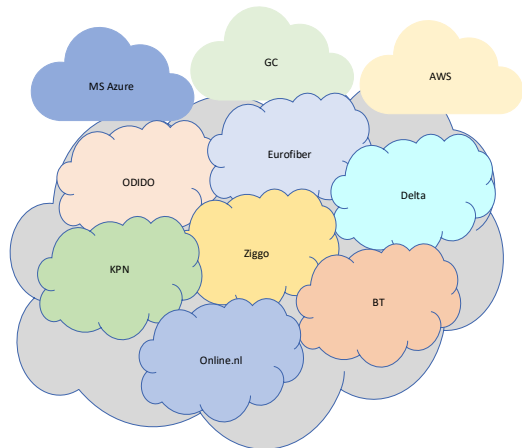
12

12

NSOC.NL - WEBINAR

Wat is het Internet?

- Een netwerk van netwerken
- Netwerken zijn Service Providers
 - Internet Service Providers
 - Levert Internet diensten aan particulieren en/of bedrijven.
 - Providers: KPN, Ziggo, Eurofiber, ODIDO en meer.
 - Diensten: Internet, VoIP en Video(streaming)
 - (optioneel) Private cloud diensten
 - Cloud Service Providers
 - Providers: MS Azure, AWS, GC, Alibaba Cloud
 - Levert diensten zoals IAAS, PAAS en SAAS



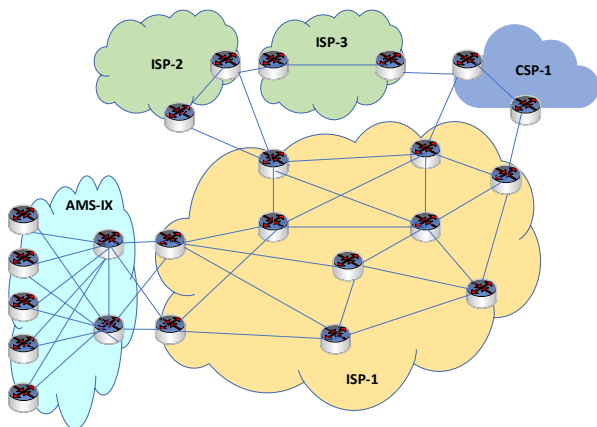
WWW.NSOC.NL

13

13

NSOC.NL - WEBINAR

Het netwerk van een ISP



Total Traffic Statistics

Live statistics showing total aggregate volume of all parties connected to NSOC.NL.

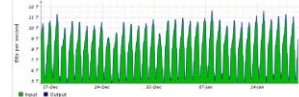
Download Traffic Volume (Gbps)

Legend: Inbound, Outbound



Copyright © 2024 NSOC.NL B.V.

Legend: Inbound, Outbound



Copyright © 2024 NSOC.NL B.V.

Legend: Inbound, Outbound



Copyright © 2024 NSOC.NL B.V.

Legend: Inbound, Outbound



Copyright © 2024 NSOC.NL B.V.

WWW.NSOC.NL

14

14

NSOC.NL - WEBINAR

Routing binnen en tussen ISP's

Routing in het proces waarbij data of netwerkpakketten van de ene netwerkknoop (zoals een computer of router) naar de andere worden gestuurd, meestal via meerdere netwerken. Dit proces omvat het bepalen van de optimale paden langs welke deze gegevens/data kunnen reizen van hun bron naar hun bestemming.

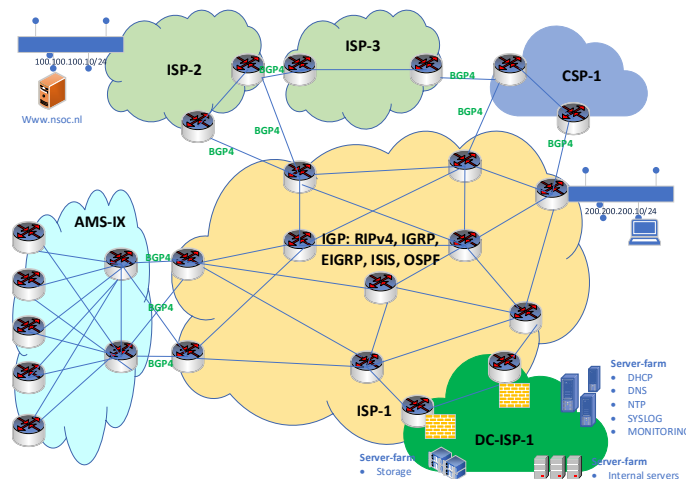
Binnen het netwerk van een ISP worden veelal een of meerdere routeringsprotocollen. Deze worden samengevat IGP genoemd en bepalen de optimale pad van een bron naar een bestemming.

- Voorbeelden van routing protocollen binnen een netwerk zijn: RIPv2, ISIS, OSPF, IGRP, EIGRP.

Om data/verkeer tussen ISP's uit te wisselen voor optimale routing tussen bron en bestemming wordt een EGP gebruikt. De enige EGP tussen de ISP's is BGP4.

NSOC.NL - WEBINAR

Routing binnen en tussen ISP



NSOC.NL - WEBINAR

Afdelingen binnen een ISP

Niet of semi technisch:
marketing, sales,
communicatie...etc.

Technische afdelingen:
Provisioning, Helpdesk,
NOC/NMC, SOC, Netwerk
Engineers, Network Designers,
System Engineer, Solution
Architecten, Security
Engineers, CISO...etc.

Moderne afkortingen:
NetOps, DevOps, SecOps

WWW.NSOC.NL

17

17

NSOC.NL
NETWORK AND CYBER SECURITY

DHCP-servers

DNS-servers

NTP-servers

Syslog-servers

Monitoring-servers

Backup-servers

Bastion-servers

AAA-servers

Provisioning-servers

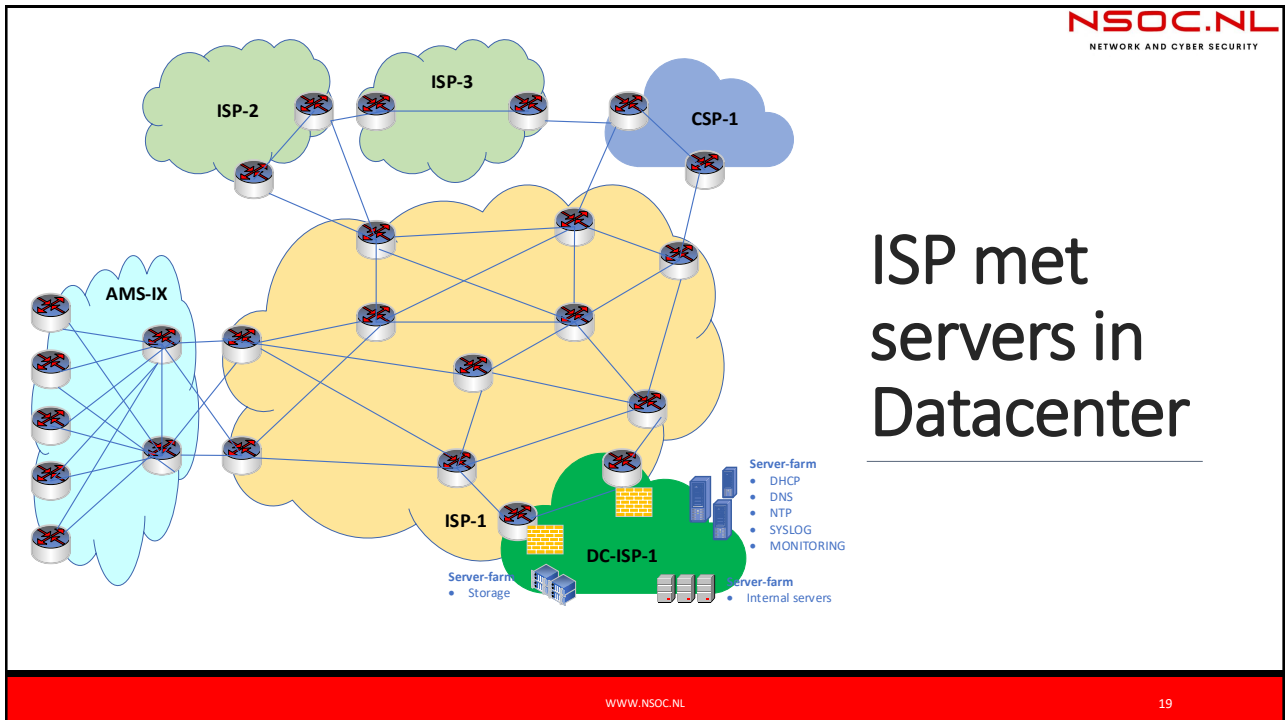
en meer natuurlijk...

Internet
server
services

WWW.NSOC.NL

18

18



19

NSOC.NL
NETWORK AND CYBER SECURITY

NSOC.NL - WEBINAR

Een wandeling door een Datacenter

WWW.NSOC.NL

20

20



NSOC.NL - WEBINAR

Datacenter redundantie (99.999%)

NSOC.NL
NETWORK AND CYBER SECURITY

- Meerdere datacenters in een bepaalde regio.
- Spreiding van hardware over meerdere racks, verdiepingen, ruimtes en datacenters
- Meerdere ISP verbindingen (DC)
- Meerdere Airco units (DC)
- Meerdere stroom aansluitingen (rack)
 - Minimaal 2 directe stroom feeds
 - UPS
 - Generator (DC)
- Meerdere servers
 - Meerdere harddrives
 - Meerdere CPU's
 - Meerdere Netwerkkarten
 - Meer
- Meer switches, routers en firewalls
- Meerdere storage systemen met RAID configuraties.
- Redundantie protocollen: HSRP, VRRP, GLBP
- Dynamische routeringsprotocollen



Availability %	Downtime per year	Downtime per month	Downtime per week	Downtime per day
90% ("one nine")	36.5 days	72 hours	16.8 hours	2.4 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours	14.4 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes	1.44 minutes
99.99% ("four nines")	52.56 minutes	4.38 minutes	1.01 minutes	8.66 seconds
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds	864.3 milliseconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	604.8 milliseconds	86.4 milliseconds
99.99999% ("seven nines")	3.15 seconds	262.07 milliseconds	60.48 milliseconds	8.64 milliseconds
99.999999% ("eight nines")	315.569 milliseconds	26.207 milliseconds	6.048 milliseconds	0.864 milliseconds
99.9999999% ("nine nines")	31.5569 milliseconds	2.6207 milliseconds	0.6048 milliseconds	0.0864 milliseconds

WWW.NSOC.NL

23

23

NSOC.NL - WEBINAR

Publieke Cloud

NSOC.NL
NETWORK AND CYBER SECURITY

- Servers die via het Internet toegankelijk zijn om gegevens op te slaan, te beheren en te verwerken, in plaats van op een lokale server of een persoonlijke computer.
- Cloud computing stelt individuen en organisaties in staat om rekenbronnen, zoals opslag, verwerkingskracht en toepassingen, te gebruiken zonder de noodzaak om fysieke hardware te bezitten of te onderhouden. In plaats daarvan kunnen gebruikers deze bronnen op aanvraag benaderen.
- Cloud computing biedt verschillende voordelen, waaronder schaalbaarheid, flexibiliteit, kostenefficiëntie en de mogelijkheid om bronnen vanaf elke locatie met een internetverbinding te benaderen. Populaire cloudserviceproviders zijn onder andere Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) en anderen.

WWW.NSOC.NL

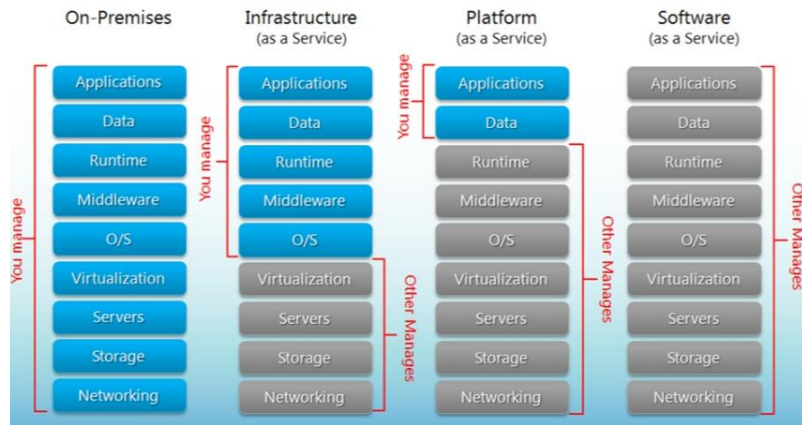
24

24

NSOC.NL - WEBINAR

Cloud Services

NSOC.NL
NETWORK AND CYBER SECURITY



WWW.NSOC.NL

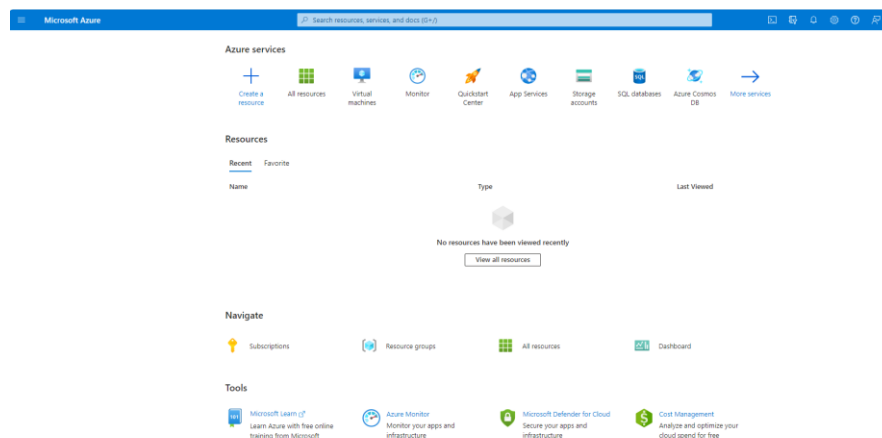
25

25

NSOC.NL - WEBINAR

Microsoft Azure Cloud portal

NSOC.NL
NETWORK AND CYBER SECURITY



WWW.NSOC.NL

26

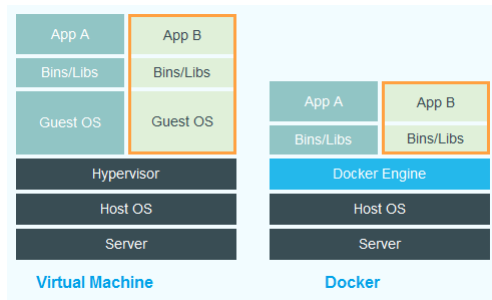
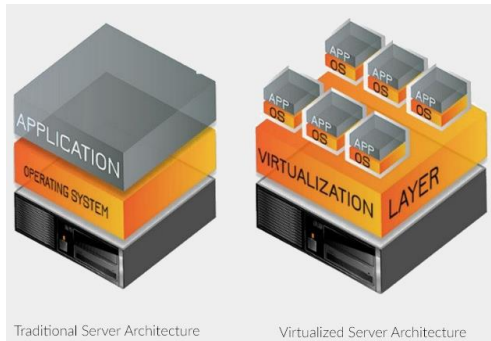
26

NSOC.NL -

Server technologie



NSOC.NL
NETWORK AND CYBER SECURITY
AR



WWW.NSOC.NL

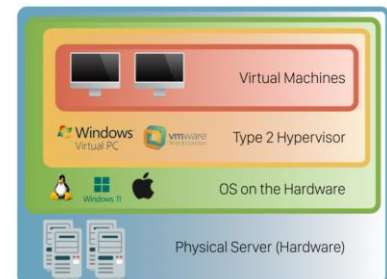
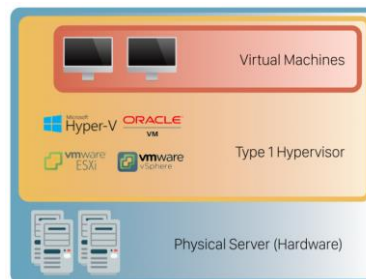
27

27

NSOC.NL - WEBINAR

Hypervisors

- **Type-1:** Bare metal, Native.
 - Microsoft Hyper-V
 - Vmware ESXi
 - Vmware vSphere
 - ORACLE VM
- **Type-2:** Hosted Hypervisors
 - VirtualBox
 - Vmware Workstation
 - Vmware Fusion



WWW.NSOC.NL

28

28

NSOC.NL - WEBINAR

Internetconfiguratie voor thuisgebruik



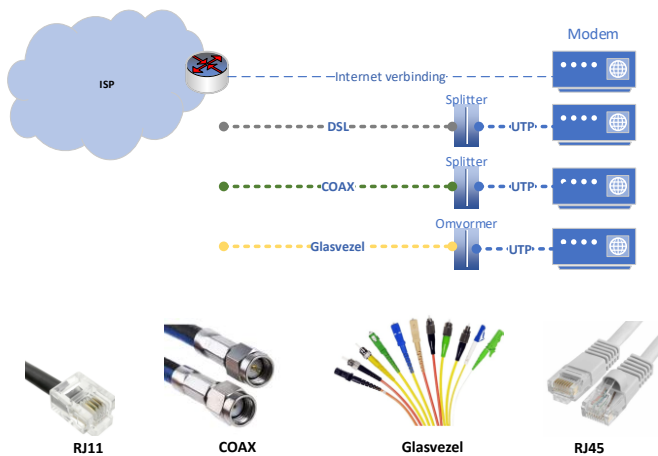
WWW.NSOC.NL

29

29

NSOC.NL - WEBINAR

Van ISP naar huis



Types modems



WWW.NSOC.NL

30

30

NSOC.NL - WEBINAR

NSOC.NL
NETWORK AND CYBER SECURITY

De modem is geïnstalleerd, wat zijn de volgende stappen

- Volg de installatiehandleiding.
- 1. Sluit je laptop/PC aan via een UTP-kabel op een LAN-poort.
- 2. De modem wijst je laptop/PC een IP-adres toe (*dit wordt in detail besproken*).
- 3. Start je internetbrowser en log in op de modem.
- 4. **Wijzig het standaard inlogwachtwoord.**
- 5. **Verander de standaard WIFI-naam (SSID).**
- 6. **Wijzig het standaard WIFI-wachtwoord.**
- 7. Kies uit verschillende beveiligingsopties, variërend van zwak naar sterk:
 - GEEN / OPEN
 - WEP
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK
 - WPA3
- Neem de tijd om de instellingen aan te passen en kies een sterke beveiligingsconfiguratie voor een veilige draadloze verbinding.

WWW.NSOC.NL

31

31

De modem/router (AI0)

NSOC.NL
NETWORK AND CYBER SECURITY

- De modem/router, doorgaans geïnstalleerd in de meterkast, voert diverse taken uit, waaronder:
 - Fungeren als een **DHCP-client** om het publieke IP-adres via de WAN-poort te verkrijgen.
 - Fungeren als een **DHCP-server** om private IP-adressen toe te wijzen aan stations via de LAN-poorten of Wifi.
 - Uitvoeren van adresvertaling (**NAT**) om de private IP-adressen om te zetten naar het publieke WAN-adres. (Van binnen(LAN) naar buiten (WAN))
 - Uitvoeren van **Port Forwarding** (van buiten (WAN) naar binnen (LAN))
 - WiFi access Point (Autonomous AP)

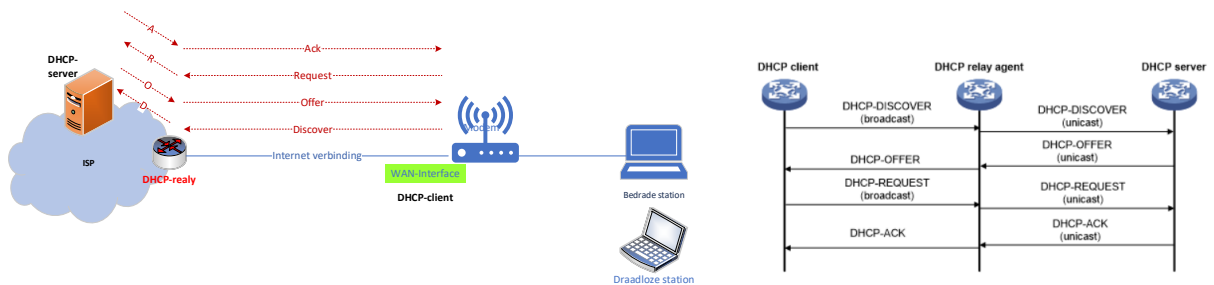
WWW.NSOC.NL

32

32

NSOC.NL - WEBINAR

Het DHCP proces (DHCP-server relay)



WWW.NSOC.NL

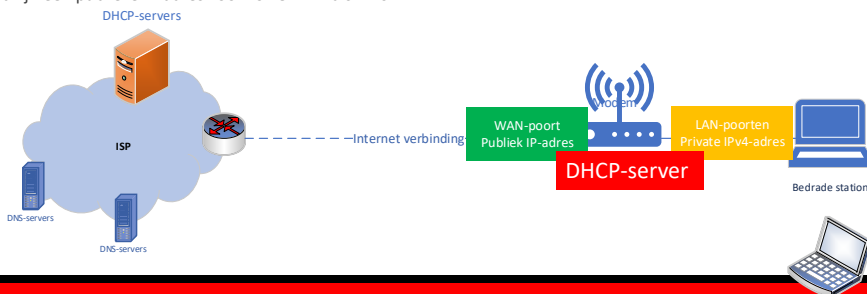
33

33

NSOC.NL - WEBINAR

Hoe worden IP-adressen en DNS-servers toegewezen aan stations?

- De modem draait een DHCP-server software die IP-adressen, subnetmaskering, gateway en DNS-servers toewijst aan de stations. Het gateway IP-adres is vaak voorgedefinieerd en kan aangepast worden.
 - Dit zijn private IPv4-adressen.
 - In geval van IPv6 is dit een publieke IPv6 adres.
- De DHCP-server software werkt alleen voor bedrade en draadloze stations binnen het huis netwerk (LAN-poorten)
- De modem poort die aangesloten zit op het Internet (WAN-poort) fungeert als een "station" en krijgt zijn IP adres gegevens van een DHCP-server die in een datacenter van de ISP staat.
 - Dit zijn een publieke IP adres voor zowel IPv4 als IPv6.



WWW.NSOC.NL

Draadloze station

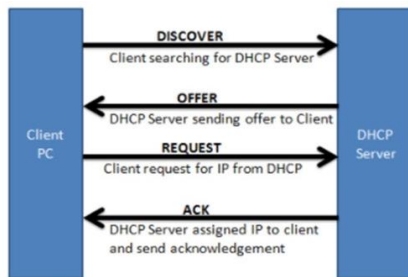
34

34

NSOC.NL - WEBINAR

Het DHCP proces (Local DHCP-server)

NSOC.NL
NETWORK AND CYBER SECURITY



No.	Time	Source	Destination	Protocol	Sequence	Acknowledgment	Next sequence	TCP segment	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP					DHCP Discover - Transaction ID 0x089aeaf9
2	0.002069	192.168.2.1	255.255.255.255	DHCP					DHCP Offer - Transaction ID 0x089aeaf9
3	0.000250	0.0.0.0	255.255.255.255	DHCP					DHCP Request - Transaction ID 0x089aeaf9
4	0.002069	192.168.2.1	255.255.255.255	DHCP					DHCP ACK - Transaction ID 0x089aeaf9


```

Source: Cisco 95:27:e9 (00:1f:6c:95:27:e9)
Type: IPv4 (0x0000)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 255.255.255.255
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 328
Identification: 0x00ed (37101)
Flags: 0x0000
Time to live: 255
Protocol: UDP (17)
Header checksum: 0x670e [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.2.1
Destination: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Bootstrap Protocol (Offer)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x089aeaf9
Seconds elapsed: 0
> Bootp Flags: 0x0000, Broadcast flag (Broadcast)
3.... = Broadcast flag: Broadcast
0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.2.133
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client HWC address: 0x0010:14:7c:59 (00:25:b3:14:7c:59)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
  
```

WWW.NSOC.NL

35

35

NSOC.NL
NETWORK AND CYBER SECURITY

```

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : AC-74-B1-78-40-34
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
IPv6 Address. . . . . : 2a02:a456:a815:1:b266:b37:abf8:e903(Preferred)
Temporary IPv6 Address. . . . . : 2a02:a456:a815:1:bdF9:5c65:753b:7570(Preferred)
Link-local IPv6 Address . . . . : fe80::5963:4497:55c5:6520%24(Preferred)
Autoconfiguration IPv4 Address. : 169.254.235.94(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 296514737
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-07-F8-E1-A0-29-19-2A-3F-0F
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
NetBIOS over Tcpip. . . . . : Enabled
  
```

IPv4 Route Table					
Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0		On-link	127.0.0.1	331
127.0.0.1	255.255.255.255		On-link	127.0.0.1	331
127.255.255.255	255.255.255.255		On-link	127.0.0.1	331
192.168.3.0	255.255.255.0		On-link	192.168.3.1	291
192.168.3.1	255.255.255.255		On-link	192.168.3.1	291
192.168.3.255	255.255.255.255		On-link	192.168.3.1	291
192.168.208.0	255.255.255.0		On-link	192.168.208.1	291
192.168.208.1	255.255.255.255		On-link	192.168.208.1	291
192.168.208.255	255.255.255.255		On-link	192.168.208.1	291
224.0.0.0	240.0.0.0		On-link	127.0.0.1	331
224.0.0.0	240.0.0.0		On-link	192.168.3.1	291
224.0.0.0	240.0.0.0		On-link	192.168.208.1	291
224.0.0.0	240.0.0.0		On-link	18	291
255.255.255.255	255.255.255.255		On-link	127.0.0.1	331
255.255.255.255	255.255.255.255		On-link	192.168.3.1	291
255.255.255.255	255.255.255.255		On-link	192.168.208.1	291
255.255.255.255	255.255.255.255		On-link	18	291

Persistent Routes:					
None					

DHCPclient – Station zonder DHCP

WWW.NSOC.NL

36

36

NSOC.NL - WEBINAR

DHCPclient – station met DHCP

NSOC.NL
NETWORK AND CYBER SECURITY

No.	Time	Source	Destination	Protocol	Length	Info
186	18.386724	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2b2f7e1d
200	18.938722	192.168.2.254	192.168.2.158	DHCP	366	DHCP Offer - Transaction ID 0x2b2f7e1d
201	18.939764	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x2b2f7e1d
202	18.951151	192.168.2.254	192.168.2.158	DHCP	366	DHCP ACK - Transaction ID 0x2b2f7e1d

Wireless LAN adapter Wi-Fi:

```

Connection-specific DNS Suffix . : kpn
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : AC-74-B1-78-A9-34
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2a02:a456:a815:1:b266:b37:abf8:e903(Preferred)
Temporary IPv6 Address. . . . . : 2a02:a456:a815:1:bd49:5c65:753b:7570(Preferred)
Link-local IPv6 Address . . . . . : fe80::5963:4497:55c5:6520%24(Preferred)
IPv4 Address. . . . . : 192.168.2.158(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : zondag 21 januari 2024 16:50:41
Lease Expires . . . . . : maandag 22 januari 2024 16:50:40
Default Gateway . . . . . : 192.168.2.254
DHCP Server . . . . . : 192.168.2.254
DHCPv6 IAID . . . . . : 296514737
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-07-F8-E1-A0-29-19-2A-3F-0F
DNS Servers . . . . . : 192.168.2.254
NetBIOS over Tcpip. . . . . : Enabled
  
```

IPv4 Route Table

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.2.254	192.168.2.158	35
127.0.0.0	255.0.0.0	On-link		127.0.0.1	331
127.0.0.1	255.255.255.255	On-link		127.0.0.1	331
127.255.255.255	255.255.255.255	On-link		127.0.0.1	331
192.168.2.0	255.255.255.0	On-link		192.168.2.158	291
192.168.2.158	255.255.255.255	On-link		192.168.2.158	291
192.168.2.255	255.255.255.255	On-link		192.168.2.158	291
192.168.3.0	255.255.255.0	On-link		192.168.3.1	291
192.168.3.1	255.255.255.255	On-link		192.168.3.1	291
192.168.3.255	255.255.255.255	On-link		192.168.3.1	291
192.168.208.0	255.255.255.0	On-link		192.168.208.1	291
192.168.208.1	255.255.255.255	On-link		192.168.208.1	291
192.168.208.255	255.255.255.255	On-link		192.168.208.1	291
224.0.0.0	240.0.0.0	On-link		127.0.0.1	331
224.0.0.0	240.0.0.0	On-link		192.168.3.1	291
224.0.0.0	240.0.0.0	On-link		192.168.208.1	291
224.0.0.0	240.0.0.0	On-link		192.168.2.158	291
255.255.255.255	255.255.255.255	On-link		127.0.0.1	331
255.255.255.255	255.255.255.255	On-link		192.168.3.1	291
255.255.255.255	255.255.255.255	On-link		192.168.208.1	291
255.255.255.255	255.255.255.255	On-link		192.168.2.158	291

Persistent Routes:
None

WWW.NSOC.NL

37

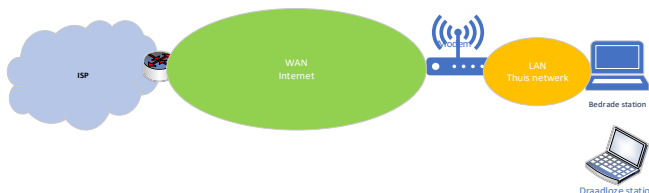
37

NSOC.NL - WEBINAR

Stations/modem hebben IP informatie. Wat nu?

NSOC.NL
NETWORK AND CYBER SECURITY

- Voordat een station het Internet op kan, dient de station het MAC adres van de modem te achterhalen, om data-verkeer naar de modem te kunnen sturen, omdat deze de default gateway is. Het IP-adres van de gateway is vaak voorgedefinieerd en kan aangepast worden.
- Omdat deze beide op het lokale thuisnetwerk(LAN) zitten, verifieer de station eerst zijn lokale geheugen (dit noemen ze de arp cache) (op windows via cmd-prompt te zien met arp -a).
- Als het MAC adres van de modem niet in de arp-cache zit, zal de station het ARP process opstarten om opzoek te gaan naar het MAC-adres van de modem.



WWW.NSOC.NL

38

38

NSOC.NL - WEBINAR

Het ARP Proces

NSOC.NL
NETWORK AND CYBER SECURITY



Een station met MAC-adres X heeft het IP-adres Y gekregen en wil verbinding maken met het Internet door het IP-verkeer naar de modem te sturen.



Helaas is het MAC-adres van de modem niet bekend, maar het IP-adres is wel bekend; dit is het IP-adres van de standaardgateway dat door het DHCP-proces aan het station is toegewezen.



Het station moet het MAC-adres van de modem (standaardgateway) achterhalen.



Dit proces wordt uitgevoerd door ARP (Address Resolution Protocol).

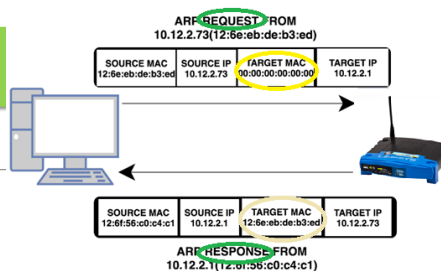
WWW.NSOC.NL

39

39

NSOC.NL

Het ARP Proces



NSOC.NL
NETWORK AND CYBER SECURITY

IAR

No.	Time	Source	Destination	Protocol	Length	Info
183	17.605538	Shenzhen_7c:3d:ed	Broadcast	ARP	60	Who has 192.168.2.254? Tell 192.168.2.6
184	17.704796	Arcadyan_55:a1:87	Broadcast	ARP	52	Who has 192.168.2.254? Tell 192.168.2.192
185	18.114326	cc:00:f1:f8:38:d7	Broadcast	ARP	52	Who has 192.168.2.158? Tell 192.168.2.254
186	18.306724	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2b2f7e1d
187	18.841909	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.100? Tell 192.168.2.2
188	18.841909	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.184? Tell 192.168.2.2
189	18.841909	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.151? Tell 192.168.2.2
190	18.841909	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.174? Tell 192.168.2.2
191	18.841909	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.171? Tell 192.168.2.2
192	18.841909	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.199? Tell 192.168.2.2
193	18.938594	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.180? Tell 192.168.2.2
194	18.938594	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.158? Tell 192.168.2.2
195	18.938594	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.198? Tell 192.168.2.2
196	18.938594	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.227? Tell 192.168.2.2
197	18.938594	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.169? Tell 192.168.2.2
198	18.938594	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.101? Tell 192.168.2.2
199	18.938594	Tp-LinkT_ad:f8:ec	Broadcast	ARP	60	Who has 192.168.2.179? Tell 192.168.2.2
200	18.938722	192.168.2.254	192.168.2.158	DHCP	366	DHCP Offer - Transaction ID 0x2b2f7e1d
201	18.939764	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x2b2f7e1d
202	18.951151	192.168.2.254	192.168.2.158	DHCP	366	DHCP ACK - Transaction ID 0x2b2f7e1d
213	19.115926	IntelCor_78:49:34	Broadcast	ARP	42	Who has 192.168.2.254? Tell 192.168.2.158
224	19.122998	cc:00:f1:f8:38:d7	IntelCor_78:49:34	ARP	52	192.168.2.254 is at cc:00:f1:f8:38:d7

WWW.NSOC.NL

40

40

NSOC.NL - WEBINAR

DHCP en ARP voor gateway

NSOC.NL
NETWORK AND CYBER SECURITY

STATION VOOR ARP REQUEST

```
C:\Users\ramon.pirbux>arp -a

Interface: 192.168.208.1 --- 0x5
Internet Address      Physical Address      Type
192.168.208.255       ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.3.1 --- 0xf
Internet Address      Physical Address      Type
192.168.3.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
239.255.255.250       01-00-5e-7f-ff-fa    static
```

STATION NA ONTVANGST ARP REPLY

```
C:\Users\ramon.pirbux>arp -a

Interface: 192.168.208.1 --- 0x5
Internet Address      Physical Address      Type
192.168.208.255       ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.3.1 --- 0xf
Internet Address      Physical Address      Type
192.168.3.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 192.168.2.158 --- 0x1b
Internet Address      Physical Address      Type
192.168.2.2           08-ff-7b-ad-f8-ec    dynamic
192.168.2.7           2b-a2-5c-cd-04-11    dynamic
192.168.2.102         98-8c-c8-e8-c9-76    dynamic
192.168.2.152         00-02-0b-f7-d8-0b    dynamic
192.168.2.161         00-02-0b-fc-c4-0d    dynamic
192.168.2.178         7c-8a-3f-e1-6b-16    dynamic
192.168.2.190         7b-97-42-55-c8-2c    dynamic
192.168.2.192         7b-97-41-55-a1-47    dynamic
192.168.2.254         c2-80-f1-f8-38-47    dynamic
192.168.2.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

WWW.NSOC.NL

41

41

NSOC.NL - WEBINAR

Het station heeft nu de MAC en IP van de standaardgateway. Wat nu?

NSOC.NL
NETWORK AND CYBER SECURITY

- Het station kan nu verbinding maken met het Internet door gebruik te maken van IP-adressen.
- Het DNS-proces wordt ingeschakeld voor het omzetten van internetnamen.
- De DNS-serveradressen worden door het DHCP-proces aan het station toegewezen.
- DNS staat voor Domain Name System.
Het is een systeem dat leesbare domeinnamen, zoals www.nsoc.com, vertaalt naar numerieke IP-adressen die computers gebruiken om met elkaar te communiceren op het Internet.
DNS fungeert als een soort telefoonboek voor het Internet, waardoor gebruikers gemakkelijk domeinnamen kunnen gebruiken in plaats van het onthouden van complexe IP-adressen.
Het speelt een cruciale rol in het mogelijk maken van de menselijke leesbaarheid van webadressen en het routeren van internetverzoeken naar de juiste servers.
- **DEMO: DNS servers laten zien op de client en DNS cache entries**
 - `Ipconfig /all (/displaydns)/flushdns – (nslookup)`

WWW.NSOC.NL

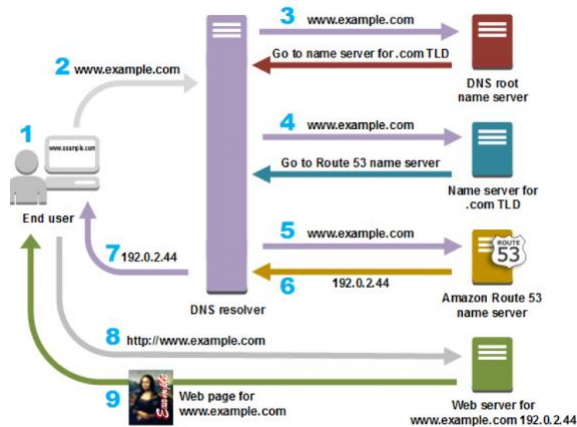
42

42

NSOC.NL - WEBINAR

Hoe functioneert DNS?

NSOC.NL
NETWORK AND CYBER SECURITY



WWW.NSOC.NL

43

43

NSOC.NL - WEBINAR

Hoe functioneert DNS?

NSOC.NL
NETWORK AND CYBER SECURITY

Realtek PCIe GBE Family Controller: Local Area Connection

No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
1	0.000	0.000000000	192.168.77.159	69		192.168.77.1	DNS	Standard query 0x0ae5 A wpad.home
9	0.024	0.024560000	192.168.77.1	108		192.168.77.159	DNS	Standard query response 0x0ae5 No such name A wpad.home SO...
33	14.784	14.759701000	192.168.77.159	88		8.8.8.8	DNS	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
34	14.806	0.021977000	8.8.8.8	124		192.168.77.159	DNS	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PT...
35	14.807	0.000994000	192.168.77.159	78		8.8.8.8	DNS	Standard query 0x0002 A wireshark.org.home
36	14.826	0.018922000	8.8.8.8	153		192.168.77.159	DNS	Standard query response 0x0002 No such name A wireshark.or...
37	14.826	0.000227000	192.168.77.159	78		8.8.8.8	DNS	Standard query 0x0003 AAAA wireshark.org.home
38	14.847	0.020295000	8.8.8.8	153		192.168.77.159	DNS	Standard query response 0x0003 No such name AAAA wireshark...
39	14.847	0.000171000	192.168.77.159	73		8.8.8.8	DNS	Standard query 0x0004 A wireshark.org
40	14.866	0.013070000	8.8.8.8	105		192.168.77.159	DNS	Standard query response 0x0004 A wireshark.org A 104.25.11...
41	14.867	0.000600000	192.168.77.159	73		8.8.8.8	DNS	Standard query 0x0005 AAAA wireshark.org
42	14.906	0.039411000	8.8.8.8	129		192.168.77.159	DNS	Standard query response 0x0005 AAAA wireshark.org AAAA 248...

Class: IN (0x0001)

Answers

- wireshark.org: Type A, class IN, addr 104.25.11.6
 - Name: wireshark.org
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 169
 - Data length: 4
 - Address: 104.25.11.6
- wireshark.org: Type A, class IN, addr 104.25.10.6
 - Name: wireshark.org
 - Type: A (Host Address) (1)

WWW.NSOC.NL

44

44

NSOC.NL - WEBINAR

Tijd om het Internet te verkennen



Het station is nu voorzien van een IP-adres, standaardgateway en DNS-servers, en heeft het MAC-adres van de standaardgateway verkregen. We zijn klaar om te gaan surfen op het internet.



Voor het surfen op het internet maakt een webbrowser gebruik van de HTTP- en HTTPS-protocollen.



De HTTP- en HTTPS-protocollen maken gebruik van het TCP protocol.



TCP initieert eerst een end-to-end sessie, bekend als de 3-way handshake, om data-uitwisseling tussen bron en bestemming mogelijk te maken.



In de transport laag, laag 4, worden twee protocollen gebruikt voor transport:

TCP: biedt betrouwbaar transport

UDP: biedt onbetrouwbaar transport

WWW.NSOC.NL

45

45

NSOC.NL - WEBINAR

TCP en UDP protocollen

• TCP en UDP werken op het transport laag (laag 4) van het OSI-7 en TCP/IP model.

• TCP kenmerken:

- Verbindingsgeoriënteerd
- Full Duplex
- Flow control
- Congestiebeheer
- Betrouwbaar

• UDP kenmerken:

- Verbindingsloos
- Geen flowcontrol
- Niet betrouwbaar
- Sneller dan TCP

TCP Segment Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags			Window Size		
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

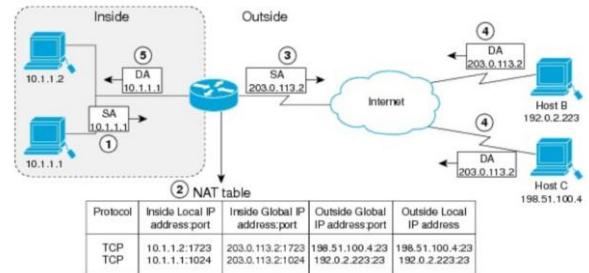
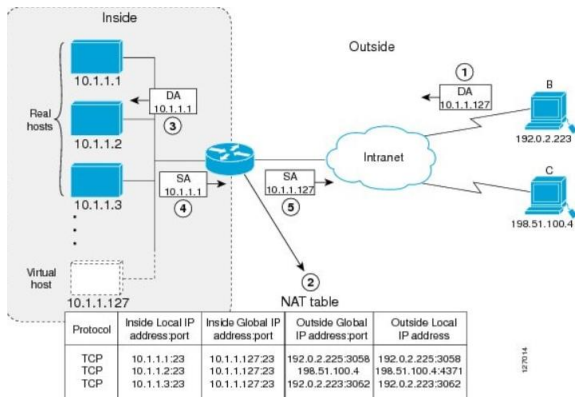
UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

WWW.NSOC.NL

46

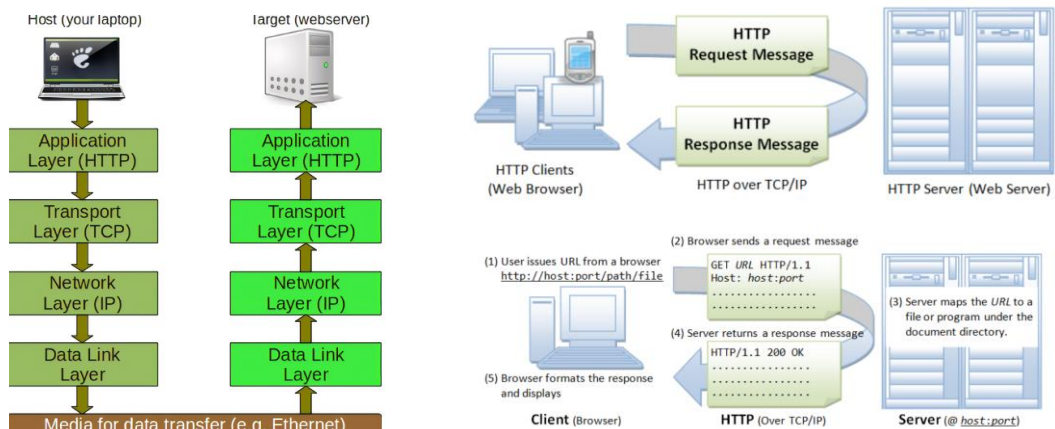
46



Netwerk Adres Translatie (NAT)

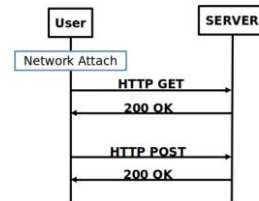
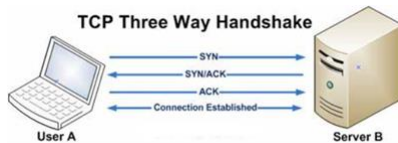
NSOC.NL - WEBINAR

Tijd om het Internet te verkennen



NSOC.NL - WEBINAR

Wat gebeurt er onder de motorkap...



856	18:32:06.176272	10.0.0.31	146.66.71.198	TCP	66 9556 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
863	18:32:06.225084	146.66.71.198	10.0.0.31	TCP	66 80 → 9556 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
864	18:32:06.225212	10.0.0.31	146.66.71.198	TCP	54 9556 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
865	18:32:06.225505	10.0.0.31	146.66.71.198	HTTP	388 GET / HTTP/1.1
871	18:32:06.272074	146.66.71.198	10.0.0.31	TCP	56 80 → 9556 [ACK] Seq=1 Ack=335 Win=30464 Len=0
873	18:32:06.279675	146.66.71.198	10.0.0.31	HTTP	739 HTTP/1.1 200 OK (text/html)
880	18:32:06.320004	10.0.0.31	146.66.71.198	TCP	54 9556 → 80 [ACK] Seq=335 Ack=686 Win=64768 Len=0
886	18:32:06.397447	10.0.0.31	146.66.71.198	HTTP	364 GET /images/netlab-labelled-pod1.jpg HTTP/1.1
889	18:32:06.449118	146.66.71.198	10.0.0.31	TCP	1514 80 → 9556 [ACK] Seq=686 Ack=645 Win=31488 Len=1460 [TCP se
890	18:32:06.449119	146.66.71.198	10.0.0.31	TCP	1514 80 → 9556 [ACK] Seq=2146 Ack=645 Win=31488 Len=1460 [TCP s
891	18:32:06.449120	146.66.71.198	10.0.0.31	TCP	1514 80 → 9556 [ACK] Seq=3606 Ack=645 Win=31488 Len=1460 [TCP s
892	18:32:06.449122	146.66.71.198	10.0.0.31	TCP	1514 80 → 9556 [ACK] Seq=5066 Ack=645 Win=31488 Len=1460 [TCP s

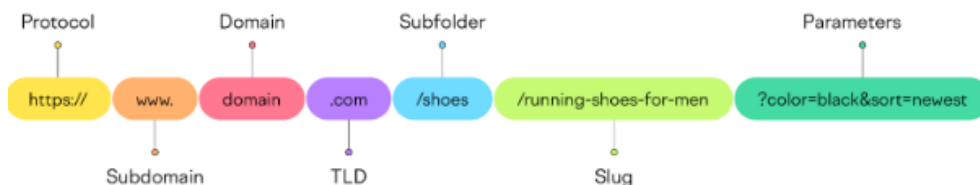
WWW.NSOC.NL

49

49

NSOC.NL - WEBINAR

URL structuur uitgelegd



WWW.NSOC.NL

50

50

NSOC.NL - WEBINAR

Applicatie laag – poort nummers

- Iedere netwerk-applicatie heeft zijn eigen applicatie-laag poort nummer.
- Deze zijn te vinden in RFC1700.
- Een paar voorbeelden van de meest voorkomende zijn:

Port Number	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384-32,767	UDP	RTP-based Voice and Video

WWW.NSOC.NL

51

51

HTTP STATUS CODES

2xx Success

200 Success / OK

3xx Redirection

301 Permanent Redirect

302 Temporary Redirect

304 Not Modified

4xx Client Error

401 Unauthorized Error

403 Forbidden

404 Not Found

405 Method Not Allowed

5xx Server Error

501 Not Implemented

502 Bad Gateway

503 Service Unavailable

504 Gateway Timeout

NSOC.NL
NETWORK AND CYBER SECURITY

HTTP codes

WWW.NSOC.NL

52

52

NSOC.NL - WEBINAR

NSOC.NL
NETWORK AND CYBER SECURITY

Begrippen

ARP	-	Address Resolution Protocol
CSP	-	Cloud Service Provider
DHCP	-	Dynamic Host Configuration Protocol
DNS	-	Domain Name Server
EGP	-	Exterior Gateway Protocol
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
IAAS	-	Infrastructure As A Service
IGP	-	Interior Gateway Protocol
IP	-	Internet Protocol
ISP	-	Internet Service Provider
MAC	-	Media Access Control
NAT	-	Network Address Translation
PAAS	-	Platform As A Service
SAAS	-	Software As A Service
TCP	-	Transmission Control Protocol
UDP	-	User Datagram Protocol

WWW.NSOC.NL

53

53

NSOC.NL - WEBINAR

NSOC.NL
NETWORK AND CYBER SECURITY

Wat is de volgende stap?

- Doe je al een ICT opleiding, dan wens ik je heel veel succes.
- Wil je omgeschoold worden of ben je startende, dan heb je diverse mogelijkheden.
 - Een ICT opleiding gaan volgen.
 - Zelfstudie
 - Je kan ook bij NSOC een opleiding volgen.
 - [Courses & Exams – NSOC.NL](#)
- Mijn doel was om jullie iets te leren, en ik hoop dat dit gelukt is.

WWW.NSOC.NL

54

54

NSOC.NL - WEBINAR

NSOC.NL
NETWORK AND CYBER SECURITY

Vragen of opmerkingen ?
